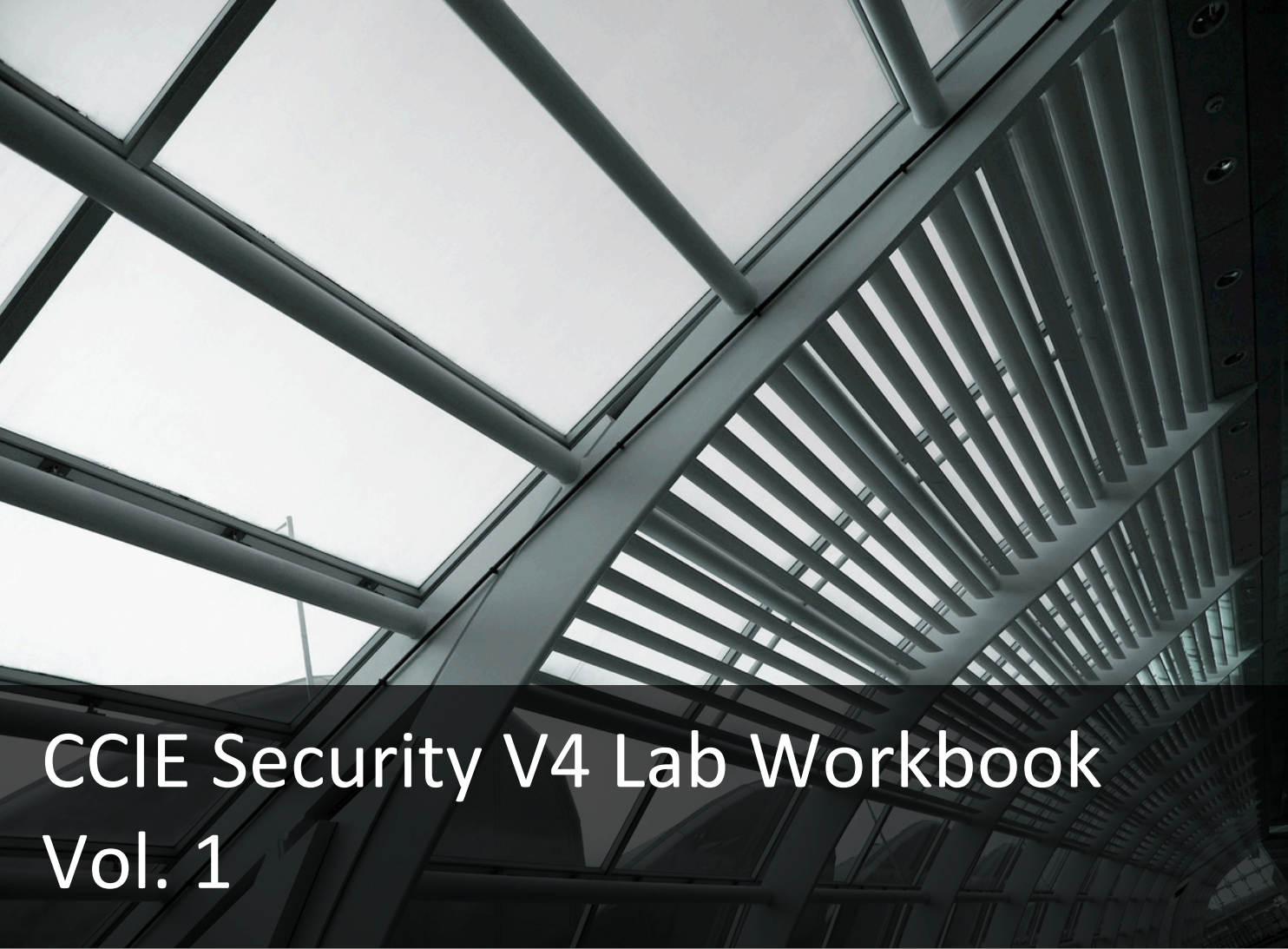




CCIE Security V4 Lab Workbook Vol. 1

Piotr Matusiak

CCIE #19860

R&S, Security

C|EH, CCSI #33705

Narbik Kocharians

CCIE #12410

R&S, Security, SP

CCSI #30832

Table of Content

ASA Firewall

LAB 1.1.	BASIC ASA CONFIGURATION.....	8
LAB 1.2.	BASIC SECURITY POLICY	17
LAB 1.3.	DYNAMIC ROUTING PROTOCOLS.....	29
LAB 1.4.	ASA MANAGEMENT.....	46
LAB 1.5.	STATIC NAT (8.2).....	59
LAB 1.6.	DYNAMIC NAT (8.2).....	67
LAB 1.7.	NAT EXEMPTION (8.2).....	77
LAB 1.8.	STATIC POLICY NAT (8.2)	81
LAB 1.9.	DYNAMIC POLICY NAT (8.2)	91
LAB 1.10.	STATIC NAT (8.3+).....	99
LAB 1.11.	DYNAMIC NAT (8.3+).....	115
LAB 1.12.	BIDIRECTIONAL NAT (8.3+).....	126
LAB 1.13.	MODULAR POLICY FRAMEWORK (MPF)	131
LAB 1.14.	FTP ADVANCED INSPECTION.....	138
LAB 1.15.	HTTP ADVANCED INSPECTION	146
LAB 1.16.	INSTANT MESSAGING ADVANCED INSPECTION	156
LAB 1.17.	ESMTP ADVANCED INSPECTION	159
LAB 1.18.	DNS ADVANCED INSPECTION	164
LAB 1.19.	ICMP ADVANCED INSPECTION	169
LAB 1.20.	CONFIGURING VIRTUAL FIREWALLS	175
LAB 1.21.	ACTIVE/STANDBY FAILOVER.....	198
LAB 1.22.	ACTIVE/ACTIVE FAILOVER.....	212
LAB 1.23.	REDUNDANT INTERFACES.....	239
LAB 1.24.	TRANSPARENT FIREWALL	246
LAB 1.25.	THREAT DETECTION	260
LAB 1.26.	CONTROLLING ICMP AND FRAGMENTED TRAFFIC	264
LAB 1.27.	TIME BASED ACCESS CONTROL.....	270
LAB 1.28.	QOS - PRIORITY QUEUING	276
LAB 1.29.	QOS – TRAFFIC POLICING	280
LAB 1.30.	QOS – TRAFFIC SHAPING	285
LAB 1.31.	QOS – TRAFFIC SHAPING WITH PRIORITIZATION.....	290
LAB 1.32.	SLA ROUTE TRACKING.....	296
LAB 1.33.	ASA IP SERVICES (DHCP).....	303
LAB 1.34.	URL FILTERING AND APPLETS BLOCKING	310
LAB 1.35.	TROUBLESHOOTING USING PACKET TRACER AND CAPTURE TOOLS.....	314

Site-to-Site VPN

LAB 1.36.	BASIC SITE TO SITE IPSEC VPN MAIN MODE (IOS-IOS)	327
LAB 1.37.	BASIC SITE TO SITE IPSEC VPN AGGRESSIVE MODE (IOS-IOS)	353
LAB 1.38.	BASIC SITE TO SITE VPN WITH NAT (IOS-IOS).....	370
LAB 1.39.	IOS CERTIFICATE AUTHORITY.....	386
LAB 1.40.	SITE-TO-SITE IPSEC VPN USING PKI (ASA-ASA)	397
LAB 1.41.	SITE-TO-SITE IPSEC VPN USING PKI (IOS-IOS).....	411
LAB 1.42.	SITE-TO-SITE IPSEC VPN USING PKI (STATIC IP IOS-ASA).....	421
LAB 1.43.	SITE-TO-SITE IPSEC VPN USING PKI (DYNAMIC IP IOS-ASA).....	441
LAB 1.44.	SITE-TO-SITE IPSEC VPN USING PSK (IOS-ASA HAIRPINNING).....	462
LAB 1.45.	SITE-TO-SITE IPSEC VPN USING EASYVPN NEM (IOS-IOS).....	476
LAB 1.46.	SITE-TO-SITE IPSEC VPN USING EASYVPN NEM (IOS-ASA)	485
LAB 1.47.	SITE-TO-SITE IPSEC VPN USING EASYVPN WITH ISAKMP PROFILES (IOS-IOS) 533	
LAB 1.48.	GRE OVER IPSEC	551
LAB 1.49.	DMVPN PHASE 1.....	568
LAB 1.50.	DMVPN PHASE 2 (WITH EIGRP)	585
LAB 1.51.	DMVPN PHASE 2 (WITH OSPF)	604
LAB 1.52.	DMVPN PHASE 3 (WITH EIGRP)	624
LAB 1.53.	DMVPN PHASE 3 (WITH OSPF)	644
LAB 1.54.	DMVPN PHASE 2 DUAL HUB (SINGLE CLOUD)	668
LAB 1.55.	DMVPN PHASE 2 DUAL HUB (DUAL CLOUD)	698
LAB 1.56.	GET VPN (PSK).....	739
LAB 1.57.	GET VPN (PKI)	761
LAB 1.58.	GET VPN COOP (PKI).....	780

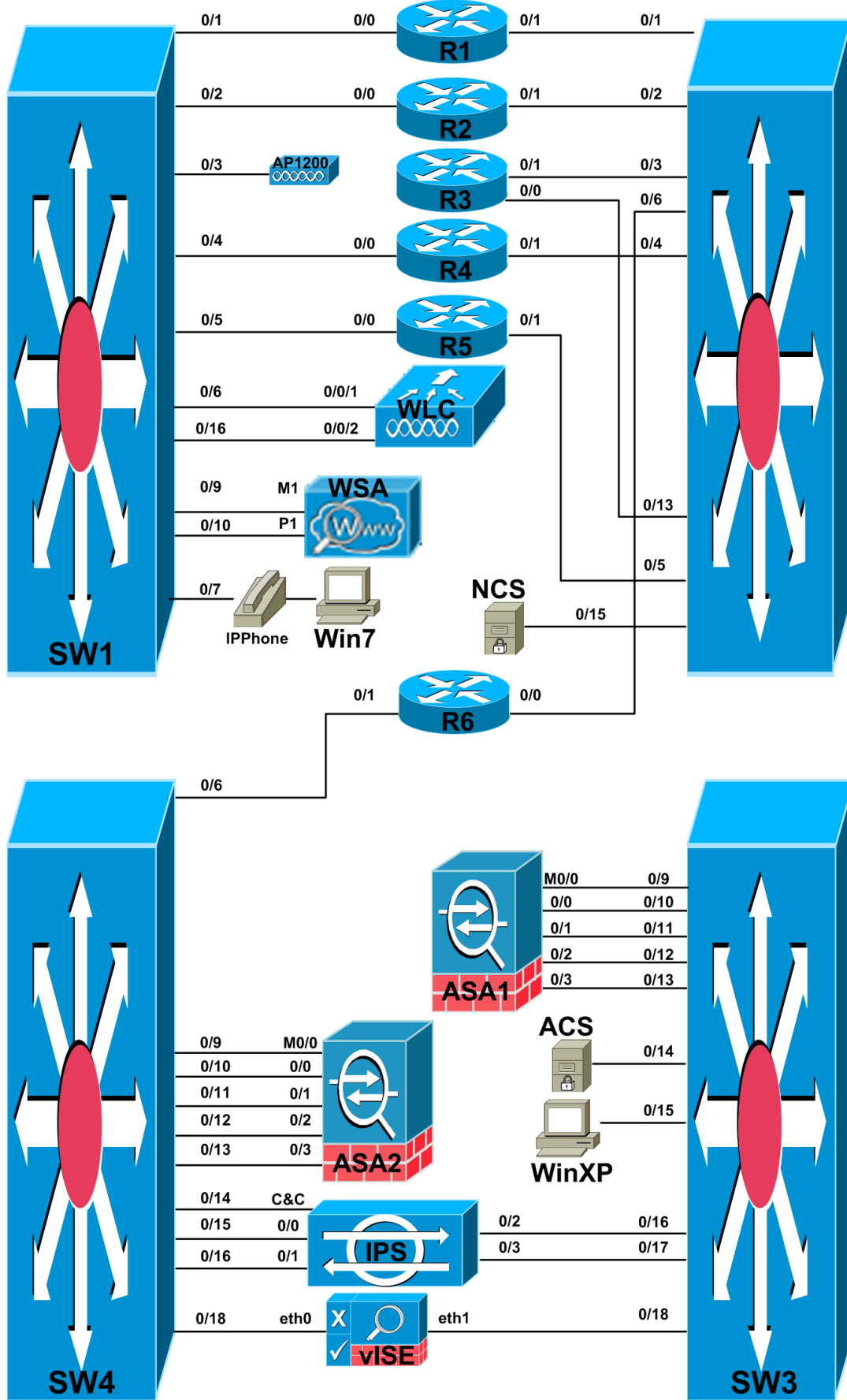
Remote Access VPN

LAB 1.59.	CONFIGURING REMOTE ACCESS IPSEC VPN USING EASYVPN (IOS TO IOS)	814
LAB 1.60.	CONFIGURING REMOTE ACCESS IPSEC VPN USING EASYVPN (IOS TO ASA)	824
LAB 1.61.	CONFIGURING RA VPN USING CISCO VPN CLIENT AND ASA (PSK).....	833
LAB 1.62.	CONFIGURING RA VPN USING CISCO VPN CLIENT AND ASA (PKI)	843
LAB 1.63.	CONFIGURING SSL VPN (IOS).....	867
LAB 1.64.	CONFIGURING SSL VPN (ASA).....	884
LAB 1.65.	ANYCONNECT 3.0 BASIC SETUP	897
LAB 1.66.	ANYCONNECT 3.0 ADVANCED FEATURES	914
LAB 1.67.	EASYVPN SERVER ON ASA WITH LDAP AUTHENTICATION	924

Advanced VPN Features

LAB 1.68.	IPSEC STATEFUL FAILOVER.....	957
LAB 1.69.	IPSEC STATIC VTI	970
LAB 1.70.	IKE ENCRYPTED KEYS.....	979
LAB 1.71.	IPSEC DYNAMIC VTI	984
LAB 1.72.	REVERSE ROUTE INJECTION (RRI).....	994
LAB 1.73.	CALL ADMISSION CONTROL FOR IKE.....	1011
LAB 1.74.	IPSEC LOAD BALANCING (ASA CLUSTER).....	1019

Physical Topology



This page is intentionally left blank.

Advanced CCIE SECURITY v4 LAB WORKBOOK

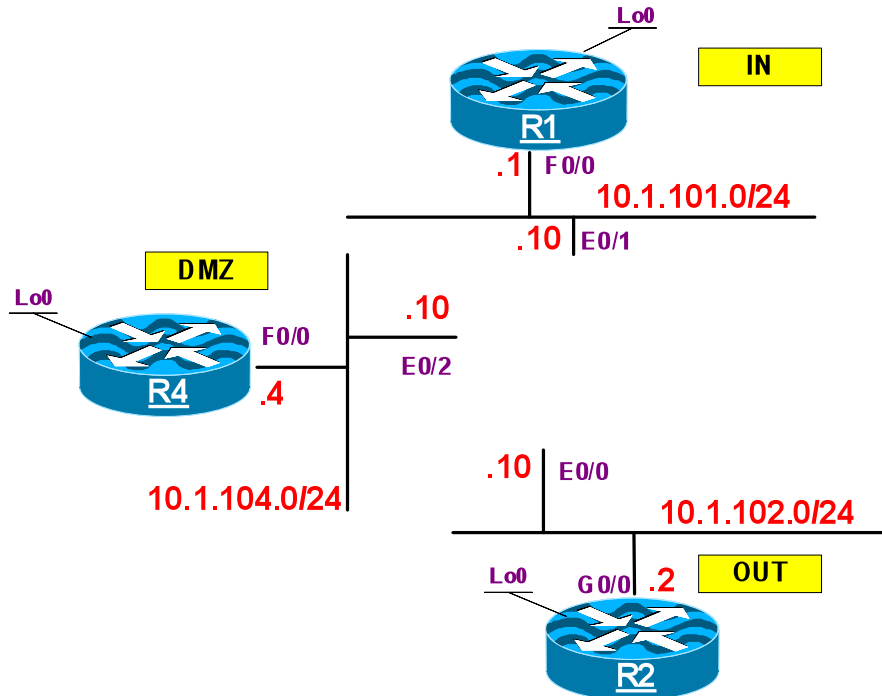
ASA Firewall

Narbik Kocharians
CCIE #12410 (R&S, Security, SP)
CCSI #30832

Piotr Matusiak
CCIE #19860 (R&S, Security)
C|EH, CCSI #33705

www.MicronicsTraining.com

Lab 1.1. Basic ASA configuration



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24

	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Task 1

Configure ASA with the following settings:

Hostname: ASA-FW

Interface E0/0: name OUT, IP address 10.1.102.10/24, security level 0

Interface E0/1: name IN, IP address 10.1.101.10/24, security level 80

On ASA configure default routing pointing to R2 and static routing for the rest of the networks. On routers R1 and R2 configure default routes pointing to the ASA.



Basic configuration of ASA requires port configuration including IP address, interface name and security level. By default the security level is set up automatically when user tries to name the interface. The ASA will use security level of 100 for interface name "inside" and security level of 0 for other interface name (including "outside"). If you need to configure other security level, use "security-level <level>" command to do so.

What is the security level for? The security level defines what connection will be considered as Inbound and what connection is Outbound.

The Outbound connection is a connection originated from the networks behind a higher security level interface towards the networks behind a lower security level interface.

The Inbound connection is a connection originated from the networks behind a lower security level interface towards the networks behind a higher security level interface.

The Outbound connection is automatically being inspected so that it does not require any access list for returning traffic. The Inbound connection is considered unsecure by default and there must be access list allowing that connection.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa# conf term
ciscoasa(config)# hostname ASA-FW

ASA-FW(config)# int e0/0
ASA-FW(config-if)# ip add 10.1.102.10 255.255.255.0
ASA-FW(config-if)# nameif OUT
INFO: Security level for "OUT" set to 0 by default.
ASA-FW(config-if)# no sh

ASA-FW(config-if)# int e0/1
ASA-FW(config-if)# ip add 10.1.101.10 255.255.255.0
ASA-FW(config-if)# nameif IN
INFO: Security level for "IN" set to 0 by default.
ASA-FW(config-if)# security-level 80
ASA-FW(config-if)# no sh
ASA-FW(config-if)# exit
```

Verification

ASA-FW(config)# sh int ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	10.1.102.10	YES	manual	up	up
Ethernet0/1	10.1.101.10	YES	manual	up	up
Ethernet0/2	unassigned	YES	unset	administratively down	up
Ethernet0/3	unassigned	YES	unset	administratively down	up
Management0/0	unassigned	YES	unset	administratively down	down

ASA-FW(config)# ping 10.1.101.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-FW(config)# ping 10.1.102.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

On ASA

```
ASA-FW(config)# route OUT 0 0 10.1.102.2
ASA-FW(config)# route IN 1.1.1.0 255.255.255.0 10.1.101.1
```

To access non-directly connected subnets a static routing (or dynamic) must be configured on the ASA. As the ASA is usually located at the edge of the network the default route points to the edge router using outside interface in most of solutions. Note that you must use interface name (not direction) to configure the static routes.

Verification

ASA-FW(config)# ping 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-FW(config)# ping 2.2.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Routers R1 and R2 must have default routes pointing to the respective ASA interface. After adding those routes, R1 should be able to telnet to R2's loopback interface.

Note that R2 cannot ping R1 - this is because ASA blocks traffic originated from the lower security level interface towards higher security level interface (OUT to IN) without explicit permit in the outbound ACL.

On R1

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.101.10
```

On R2

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.1.102.10
```

Verification

R1#tel 2.2.2.2 /so lo0

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:26	
*578 vty 0		idle	00:00:00	1.1.1.1

The "Location" field shows source address of user session established on the router. It is very useful if we need to determine whether or not a connection goes through NAT or PAT.

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

R1#p 2.2.2.2 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

.....

Success rate is 0 percent (0/5)

This is caused by the ASA default rule of traffic processing. See: remark in the frame above.

Task 2

Configure interface E0/2 on the ASA so that it will connect via dot1q trunk to the switch and will be connected to R4's F0/0 interface using VLAN 104 and IP address of 10.1.104.10/24. Configure static routing on ASA and default routing on R4 to achieve full connectivity.



The interface on ASA can be configured as a trunk to the switch to make more subnets on the one physical interface possible. This is useful when there is a lack of physical interfaces on the ASA and logical segmentation is enough from the security point of view. Remember that you need to bring a physical interface up (no shutdown) first and then configure subinterfaces.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# int e0/2
ASA-FW(config-if)# no sh
ASA-FW(config-if)# int e0/2.104
ASA-FW(config-subif)# vlan 104
ASA-FW(config-subif)# ip add 10.1.104.10 255.255.255.0
ASA-FW(config-subif)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
```

Remember that ASA sets security level to 0 by default for interfaces other than "inside". Don't forget about that during your lab exam.

```
ASA-FW(config-subif)# security-level 50
ASA-FW(config-subif)# no sh

ASA-FW(config-subif)# route DMZ 4.4.4.0 255.255.255.0 10.1.104.4
```

Step 2 R4 configuration.

```
R4(config)#ip route 0.0.0.0 0.0.0.0 10.1.104.10
```

Step 3 SW3 configuration.

```
SW3(config)#int f0/12
SW3(config-if)#switchport trunk encapsulation dot1q
SW3(config-if)#switchport mode trunk
SW3(config-if)#exi
SW3(config)#vlan 104
SW3(config-vlan)#exi
```

Verification**ASA-FW(config)# sh int ip brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	10.1.102.10	YES	manual	up	up
Ethernet0/1	10.1.101.10	YES	manual	up	up
Ethernet0/2	unassigned	YES	unset	up	up
Ethernet0/2.104	10.1.104.10	YES	manual	up	up
Ethernet0/3	unassigned	YES	unset	administratively down	up
Management0/0	unassigned	YES	unset	administratively down	down

ASA-FW(config)# ping 4.4.4.4

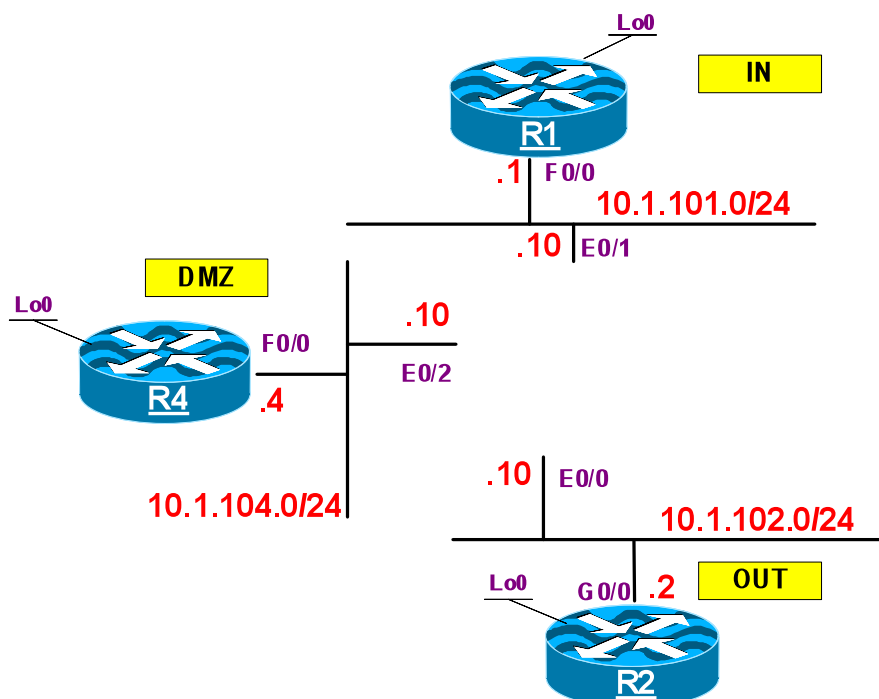
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

Lab 1.2. Basic security policy



This lab is based on the previous lab configuration.

Task 1

Configure ASA with the policy that Ping and Telnet are allowed from the inside subnet (IN) to the outside subnet (OUT) and DMZ.



The main rule on the ASA is to allow traffic coming from the interface with a higher security level towards the interface with a lower security level. However traffic is blocked in opposite direction by default and there is need for an inbound ACL to permit that traffic.

Remember that ICMP traffic is stateless, so there is no session available to track. The ASA has no ICMP inspection enabled by default so that ICMP traffic coming from the interface with higher security level towards the interface with lower security level will be blocked by the lower security level interface (ICMP echo reply will be blocked).

There are two ways to allow that traffic coming through: (1) configure ICMP inspection globally or on the interface or (2) configure inbound ACL on the interface with lower security level.

Configuration

Complete these steps:

Step 1 ASA configuration.

```

ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any echo-
reply
ASA-FW(config)# access-list DMZ_IN permit icmp any any echo-reply

ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
ASA-FW(config)# access-group DMZ_IN in interface DMZ

```

Verification

R1#ping 2.2.2.2 so lo0

Test from IN (inside) to OUT (outside) - ICMP

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

```

R1#ping 4.4.4.4

Test from IN (inside) to DMZ (dmz) - ICMP

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

R1#tel 2.2.2.2 /so lo0

Trying 2.2.2.2 ... Open

Test from IN (inside) to OUT (outside) - TCP

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:13:07	
*578 vty 0		idle	00:00:00	1.1.1.1

Interface	User	Mode	Idle	Peer Address

R2>exi

[Connection to 2.2.2.2 closed by foreign host]

R1#tel 4.4.4.4 /so 1o0

Trying 4.4.4.4 ... Open

Test from IN (inside) to DMZ (dmz) - TCP

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:11:58	
*514 vty 0		idle	00:00:00	1.1.1.1

Interface	User	Mode	Idle	Peer Address

R4>exit

[Connection to 4.4.4.4 closed by foreign host]

R2#ping 1.1.1.1

Test from OUT (outside) to IN (inside) - ICMP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

R4#ping 1.1.1.1

Test from DMZ (dmz) to IN (inside) - ICMP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Note that the ping is not working for the traffic initiated from the interface with a lower security level. This is because ACL allows only ICMP echo-reply. Also note that Telnet traffic is allowed automatically as the ASA has TCP packet inspection enabled by default so all TCP traffic coming from the interface with higher security level to the interface with lower security level will be statefully inspected (returning traffic will be allowed back).

Task 2

Allow SSH and TELNET connections from R2's and R4's loopback0 interface to the R1's loopback0 interface. You are allowed to add only one line to the existing access lists.



As this task requires using only one ACL line there is a need for object grouping. This method allows us to group up similar objects (hosts, ports, subnets, etc.) and then use group names in the ACL. There are different object group types:

- *icmp-type - specifies a group of ICMP types, such as echo*
- *network - specifies a group of host or subnet IP addresses*
- *protocol - specifies a group of protocols, such as TCP, etc*
- *service - specifies a group of TCP/UDP ports/services*

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# object-group network MGMT-HOSTS
ASA-FW(config-network)# network-object host 2.2.2.2
ASA-FW(config-network)# network-object host 4.4.4.4
ASA-FW(config-network)# exit
```

Object group of network type is for grouping hosts and subnets.

```
ASA-FW(config)# object-group service TELNET-and-SSH tcp
ASA-FW(config-service)# port-object eq telnet
ASA-FW(config-service)# port-object eq ssh
ASA-FW(config-service)# exit
```

Object group of service type is for grouping TCP/UDP ports. We need to specify what protocol we're going to match (tcp or udp). We can also use tcp-udp to match both services in one rule. There is also a possibility to not specify the service type and then we can use « service-object » to specify any other protocol (for example GRE, ICMP, ESP, etc).

```
ASA-FW(config)# access-list OUTSIDE_IN permit tcp object-group
MGMT-HOSTS host 1.1.1.1 object-group TELNET-and-SSH
```

```
ASA-FW(config)# access-list DMZ_IN permit tcp object-group MGMT-
HOSTS host 1.1.1.1 object-group TELNET-and-SSH
```

The object groups are then used in ACL building.

Verification

```
ASA-FW(config)# sh run object-group
```

```
object-group network MGMT-HOSTS
  network-object host 2.2.2.2
  network-object host 4.4.4.4
object-group service TELNET-and-SSH tcp
  port-object eq telnet
  port-object eq ssh
```

```
ASA-FW(config)# sh access-list OUTSIDE IN
```

```
access-list OUTSIDE_IN; 5 elements; name hash: 0xe01d8199
access-list OUTSIDE_IN line 1 extended permit icmp any any echo-reply (hitcnt=1)
0xc857b49e
access-list OUTSIDE_IN line 2 extended permit tcp object-group MGMT-HOSTS host 1.1.1.1
object-group TELNET-and-SSH 0xb422f490
  access-list OUTSIDE_IN line 2 extended permit tcp host 2.2.2.2 host 1.1.1.1 eq telnet
(hitcnt=0) 0x939bf78d
  access-list OUTSIDE_IN line 2 extended permit tcp host 2.2.2.2 host 1.1.1.1 eq ssh
(hitcnt=0) 0x8d022728
  access-list OUTSIDE_IN line 2 extended permit tcp host 4.4.4.4 host 1.1.1.1 eq telnet
(hitcnt=0) 0xbf14a304
  access-list OUTSIDE_IN line 2 extended permit tcp host 4.4.4.4 host 1.1.1.1 eq ssh
(hitcnt=0) 0x04c16117
```

```
ASA-FW(config)# sh access-list DMZ IN
```

```
access-list DMZ_IN; 5 elements; name hash: 0x229557de
access-list DMZ_IN line 1 extended permit icmp any any echo-reply (hitcnt=1) 0x7fb4c5b2
access-list DMZ_IN line 2 extended permit tcp object-group MGMT-HOSTS host 1.1.1.1
object-group TELNET-and-SSH 0x909d621e
  access-list DMZ_IN line 2 extended permit tcp host 2.2.2.2 host 1.1.1.1 eq telnet
(hitcnt=0) 0x231b90e2
  access-list DMZ_IN line 2 extended permit tcp host 2.2.2.2 host 1.1.1.1 eq ssh
(hitcnt=0) 0x4284ac66
  access-list DMZ_IN line 2 extended permit tcp host 4.4.4.4 host 1.1.1.1 eq telnet
(hitcnt=0) 0xfd96744e
  access-list DMZ_IN line 2 extended permit tcp host 4.4.4.4 host 1.1.1.1 eq ssh
(hitcnt=0) 0x44528edd
```

Note that access-list entry (ACEs) is expanded and displayed as multiple ACEs with the same line number when grouped objects are used.

```
R2#tel 1.1.1.1
```

```
Trying 1.1.1.1 ...  
% Connection timed out; remote host not responding
```

```
R2#tel 1.1.1.1 /so lo0
```

```
Trying 1.1.1.1 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R1>exit
```

```
[Connection to 1.1.1.1 closed by foreign host]
```

```
R4#tel 1.1.1.1
```

```
Trying 1.1.1.1 ...
```

```
% Connection timed out; remote host not responding
```

```
R4#tel 1.1.1.1 /so lo0
```

```
Trying 1.1.1.1 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R1>exit
```

```
[Connection to 1.1.1.1 closed by foreign host]
```

```
R2#tel 1.1.1.1
```

```
Trying 1.1.1.1 ...
```

```
% Connection timed out; remote host not responding
```

```
R2#tel 1.1.1.1 /so lo0
```

```
Trying 1.1.1.1 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R1>exit
```

```
[Connection to 1.1.1.1 closed by foreign host]
```

```
R4#tel 1.1.1.1
```

```
Trying 1.1.1.1 ...
```

```
% Connection timed out; remote host not responding
```

```
R4#tel 1.1.1.1 /so lo0
```

```
Trying 1.1.1.1 ... Open
```

User Access Verification

Password:

R1>exit

[Connection to 1.1.1.1 closed by foreign host]

Task 3

Configure the following outbound access policy for hosts located in the inside network:

Host/Subnet	Source port	Destination host	Destination port
1.1.1.1	any	10.1.104.4 4.4.4.4	tcp/23 tcp/22 tcp/80
1.1.1.1	4000 – 5000	10.1.102.2	tcp/21
10.1.101.0/24	any	any	tcp/80 tcp/443 tcp/110 icmp/echo

Use object groups where possible to simplify the configuration.



This time we must use object groups as per task requirement. However, it must be considered carefully to use as minimum objects as possible. This task can be done using only three ACL lines.

Note that this is not about how many object groups we can use. It is how many ACEs we can use!

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# object-group network R1-lo0
ASA-FW(config-network)# network-object host 1.1.1.1

ASA-FW(config-network)# object-group network R2-f0
ASA-FW(config-network)# network-object host 10.1.102.2

ASA-FW(config-network)# object-group network Inside-Subnet
ASA-FW(config-network)# network-object 10.1.101.0 255.255.255.0
```

```
ASA-FW(config-network)# object-group network R4
ASA-FW(config-network)# network-object host 4.4.4.4
ASA-FW(config-network)# network-object host 10.1.104.4

ASA-FW(config-network)# object-group service R4-Services tcp
ASA-FW(config-service)# port-object eq telnet
ASA-FW(config-service)# port-object eq ssh
ASA-FW(config-service)# port-object eq http

ASA-FW(config-service)# object-group service FTP-PORT-RANGE
ASA-FW(config-service)# service-object tcp source range 4000 5000
ftp

ASA-FW(config-service)# object-group service ALLOWED
ASA-FW(config-service)# service-object tcp http
ASA-FW(config-service)# service-object tcp https
ASA-FW(config-service)# service-object tcp pop3
ASA-FW(config-service)# service-object icmp echo
ASA-FW(config-service)# exit

ASA-FW(config)# access-list INSIDE_IN permit tcp object-group
R1-lo0 object-group R4 object-group R4-Services
ASA-FW(config)# access-list INSIDE_IN permit object-group FTP-
PORT-RANGE object-group R1-lo0 object-group R2-f0
ASA-FW(config)# access-list INSIDE_IN permit object-group ALLOWED
object-group Inside-Subnet any

ASA-FW(config)# access-group INSIDE_IN in interface IN
```

Verification

```
ASA-FW(config)# sh run object-group
object-group network MGMT-HOSTS
  network-object host 2.2.2.2
  network-object host 4.4.4.4
object-group service TELNET-and-SSH tcp
  port-object eq telnet
  port-object eq ssh
object-group network R1-lo0
  network-object host 1.1.1.1
object-group network R2-f0
  network-object host 10.1.102.2
object-group network Inside-Subnet
  network-object 10.1.101.0 255.255.255.0
object-group network R4
  network-object host 4.4.4.4
```

```

network-object host 10.1.104.4
object-group service R4-Services tcp
port-object eq telnet
port-object eq ssh
port-object eq www
object-group service FTP-PORT-RANGE
service-object tcp source range 4000 5000 eq ftp
object-group service ALLOWED
service-object tcp eq www
service-object tcp eq https
service-object tcp eq pop3
service-object icmp echo

```

ASA-FW(config)# sh access-li INSIDE IN

```

access-list INSIDE_IN; 11 elements; name hash: 0xf4313c68
access-list INSIDE_IN line 1 extended permit tcp object-group R1-lo0 object-group R4
object-group R4-Services 0x8a493604
access-list INSIDE_IN line 1 extended permit tcp host 1.1.1.1 host 4.4.4.4 eq telnet
(hitcnt=0) 0xee9f0a8f
access-list INSIDE_IN line 1 extended permit tcp host 1.1.1.1 host 4.4.4.4 eq ssh
(hitcnt=0) 0x2f408621
access-list INSIDE_IN line 1 extended permit tcp host 1.1.1.1 host 4.4.4.4 eq www
(hitcnt=0) 0x4e8fc6d9
access-list INSIDE_IN line 1 extended permit tcp host 1.1.1.1 host 10.1.104.4 eq
telnet (hitcnt=0) 0x929ae368
access-list INSIDE_IN line 1 extended permit tcp host 1.1.1.1 host 10.1.104.4 eq ssh
(hitcnt=0) 0xf20b6c11
access-list INSIDE_IN line 1 extended permit tcp host 1.1.1.1 host 10.1.104.4 eq www
(hitcnt=0) 0xa6a8ec29
access-list INSIDE_IN line 2 extended permit object-group FTP-PORT-RANGE object-group
R1-lo0 object-group R2-f0 0x5add7170
access-list INSIDE_IN line 2 extended permit tcp host 1.1.1.1 range 4000 5000 host
10.1.102.2 eq ftp (hitcnt=0) 0x12709c5b
access-list INSIDE_IN line 3 extended permit object-group ALLOWED object-group Inside-
Subnet any 0x3aba7b0d
access-list INSIDE_IN line 3 extended permit tcp 10.1.101.0 255.255.255.0 any eq www
(hitcnt=0) 0x2865d7c5
access-list INSIDE_IN line 3 extended permit tcp 10.1.101.0 255.255.255.0 any eq
https (hitcnt=0) 0x8defc473
access-list INSIDE_IN line 3 extended permit tcp 10.1.101.0 255.255.255.0 any eq pop3
(hitcnt=0) 0xb42c48d1
access-list INSIDE_IN line 3 extended permit icmp 10.1.101.0 255.255.255.0 any echo
(hitcnt=0) 0x0a464bf7

```

R1#ping 2.2.2.2 so lo0

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)

```


R1#ping 2.2.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#tel 4.4.4.4

Trying 4.4.4.4 ...

% Connection refused by remote host

R1#tel 4.4.4.4 /so lo0

Trying 4.4.4.4 ... Open

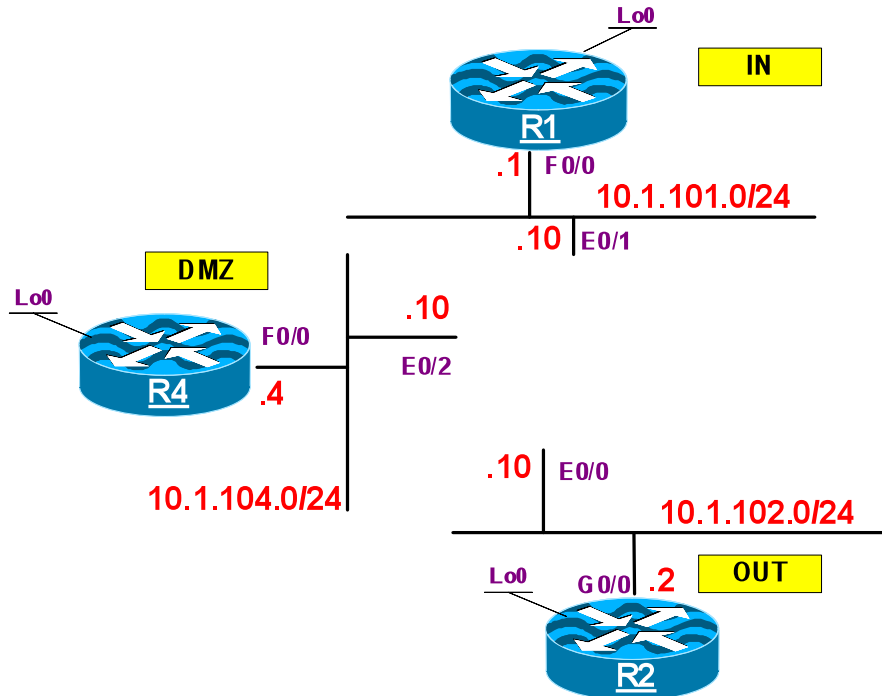
User Access Verification

Password:

R4>exit

[Connection to 4.4.4.4 closed by foreign host]

Lab 1.3. Dynamic routing protocols



This lab is based on the previous lab configuration.

Task 1

Remove static routing for inside networks and configure RIP version 2 between R1 and ASA only. Ensure RIP updates are being authenticated using MD5 with password of "cisco123".



RIPv2 configuration on ASA is pretty simple and very similar to the configuration on routers. Remember that you need to use passive-interface to not advertise on all ASA's interfaces (as all interfaces are in 10.0.0.0/8 network). RIPv2 authentication is configured on the interface (along with a MD5 key) – there is no keychain configuration on the ASA.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# sh run route
route OUT 0.0.0.0 0.0.0.0 10.1.102.2 1
route IN 1.1.1.0 255.255.255.0 10.1.101.1 1
route DMZ 4.4.4.0 255.255.255.0 10.1.104.4 1

ASA-FW(config)# no route IN 1.1.1.0 255.255.255.0 10.1.101.1 1

ASA-FW(config)# router rip
ASA-FW(config-router)# version 2
ASA-FW(config-router)# no auto
ASA-FW(config-router)# network 10.0.0.0
ASA-FW(config-router)# passive-interface default
ASA-FW(config-router)# no passive-interface IN

ASA-FW(config-router)# int e0/1
ASA-FW(config-if)# rip authentication mode MD5
ASA-FW(config-if)# rip authentication key cisco123 key_id 1
ASA-FW(config-if)# exit
```

Note that RIP authentication configuration is different on ASA and IOS router. On the ASA the MD5 key is configured directly on the interface whereas on IOS router there must be a key-chain configured and attached on the interface.

Step 2 R1 configuration.

```
R1#sh run | in route
ip route 0.0.0.0 0.0.0.0 10.1.101.10

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip route 0.0.0.0 0.0.0.0 10.1.101.10

R1(config)#key chain AUTH
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco123

R1(config-keychain-key)#int f0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain AUTH

R1(config-if)#router rip
R1(config-router)#ver 2
R1(config-router)#no auto-summary
```

```
R1(config-router)#network 10.0.0.0
R1(config-router)#network 1.0.0.0
R1(config-router)#end
```

Verification

ASA-FW(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 10.1.102.2 to network 0.0.0.0

```
R 1.1.1.0 255.255.255.0 [120/1] via 10.1.101.1, 0:00:13, IN
```

This prefix has been injected by RIPv2 to the routing table. R1 has sent information about its networks to ASA via authenticated RIPv2 update.

```
S 4.4.4.0 255.255.255.0 [1/0] via 10.1.104.4, DMZ
C 10.1.104.0 255.255.255.0 is directly connected, DMZ
C 10.1.102.0 255.255.255.0 is directly connected, OUT
C 10.1.101.0 255.255.255.0 is directly connected, IN
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.102.2, OUT
```

ASA-FW(config)# ping 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 3 subnets
R    10.1.104.0 [120/1] via 10.1.101.10, 00:00:06, FastEthernet0/0
R    10.1.102.0 [120/1] via 10.1.101.10, 00:00:06, FastEthernet0/0

```

The ASA has sent information about its connected networks to R1 via authenticated RIPv2 updates. Note that routes to R2 and R4 loopbacks are not present in R1's routing table because dynamic routing is configured only on inside interface.

```

C    10.1.101.0 is directly connected, FastEthernet0/0

```

R1#sh ip protocols

```

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 9 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0      2     2                AUTH

```

This indicates that authentication on Fa0/0 is enabled

```

Loopback0          2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    1.0.0.0
    10.0.0.0
  Routing Information Sources:
    Gateway          Distance    Last Update
  10.1.101.10        120         00:00:15
  Distance: (default is 120)

```

Note that even though there is passive interface configured on the ASA, RIPv2 is sending updates to R1 for all ASA's directly connected networks.

Task 2

Configure OSPF Area 0 on the outside interface and authenticate it using interface authentication with password of "cisco456" and key ID 1. Use 10.10.10.10 as OSPF router ID.

Remove static routing between ASA and R2 and ensure that R2 sends a default gateway for ASA outside connections using OSPF. Use 2.2.2.2 as a router-id on R2.



The OSPF configuration on ASA is similar to the configuration on the routers. Remember that on the ASA you need to use network mask when specifying network/interface where OSPF is running on. On the router however, you need to configure wildcard mask to specify the network.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# sh run route
route OUT 0.0.0.0 0.0.0.0 10.1.102.2 1
route DMZ 4.4.4.0 255.255.255.0 10.1.104.4 1

ASA-FW(config)# no route OUT 0.0.0.0 0.0.0.0 10.1.102.2 1

ASA-FW(config)# router ospf 1
ASA-FW(config-router)# router-id 10.10.10.10
ASA-FW(config-router)# network 10.1.102.10 255.255.255.0 area 0

ASA-FW(config-router)# int e0/0
ASA-FW(config-if)# ospf authentication message-digest
ASA-FW(config-if)# ospf message-digest-key 1 MD5 cisco456
ASA-FW(config-if)# exit
```

Step 2 R2 configuration.

```
R2#sh run | in route
ip route 0.0.0.0 0.0.0.0 10.1.102.10

R2#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R2(config)#no ip route 0.0.0.0 0.0.0.0 10.1.102.10
```

```
R2(config)#int g0/0
```

```
R2(config-if)#ip ospf authentication message-digest
```

```
R2(config-if)#ip ospf message-digest-key 1 md5 cisco456
```

```
R2(config-if)#router ospf 1
```

```
R2(config-router)#router-id 2.2.2.2
```

```
R2(config-router)#network 0.0.0.0 0.0.0.0 ar 0
```

```
R2(config-router)#default-information originate always
```

```
R2(config-router)#end
```

```
R2#
```

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on GigabitEthernet0/0
from LOADING to FULL, Loading Done
```

Note that IOS router does not use key-chain when configuring OSPF authentication. The OSPF authentication configuration on the ASA and IOS router is exactly the same.

The R2 must send default route to the ASA so that "default-information" command is used.

Verification

```
ASA-FW(config)# sh ospf 1
```

```
Routing Process "ospf 1" with ID 10.10.10.10 and Domain ID 0.0.0.1
```

This indicates that OSPF process 1 is running and router ID is 10.10.10.10

Supports only single TOS(TOS0) routes

Does not support opaque LSA

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

Number of external LSA 1. Checksum Sum 0x feab

Number of opaque AS LSA 0. Checksum Sum 0x 0

Number of DCbitless external and opaque AS LSA 0

Number of DoNotAge external and opaque AS LSA 0

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

External flood list length 0

Area BACKBONE(0)

Number of interfaces in this area is 1

```
Area has no authentication
```

This indicates that authentication is not enabled for the OSPF.

```

SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x 1520d
Number of opaque link LSA 0. Checksum Sum 0x      0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```

ASA-FW(config)# sh ospf 1 int OUT

```

OUT is up, line protocol is up
Internet Address 10.1.102.10 mask 255.255.255.0, Area 0
Process ID 1, Router ID 10.10.10.10, Network Type BROADCAST, Cost: 10

```

This shows that interface OUT is used by OSPF process 1. OSPF network type for this interface is BROADCAST (the default OSPF network type for Ethernet: DR/BDR election is performed and updates are sent via multicast packets)

```

Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 10.10.10.10, Interface address 10.1.102.10
Backup Designated router (ID) 2.2.2.2, Interface address 10.1.102.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1

```

The authentication is enabled for that interface.

ASA-FW(config)# sh ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/BDR	0:00:38	10.1.102.2	OUT

ASA-FW(config)# sh route

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```


Gateway of last resort is 10.1.102.2 to network 0.0.0.0

```
R  1.1.1.0 255.255.255.0 [120/1] via 10.1.101.1, 0:00:14, IN
O  2.2.2.2 255.255.255.255 [110/11] via 10.1.102.2, 0:01:13, OUT
S  4.4.4.0 255.255.255.0 [1/0] via 10.1.104.4, DMZ
C  10.1.104.0 255.255.255.0 is directly connected, DMZ
C  10.1.102.0 255.255.255.0 is directly connected, OUT
C  10.1.101.0 255.255.255.0 is directly connected, IN
O*E2 0.0.0.0 0.0.0.0 [110/1] via 10.1.102.2, 0:01:13, OUT
```

R2's loopback IP address is in ASA's routing table. Note that this IP address is a 'host' route (255.255.255.255). This is because the default OSPF network type for loopback interfaces is LOOPBACK so that OSPF sends out "host" route. To change that you should use "ip ospf network point-to-point" command on the R2's loopback interface.

Also note there is a default route injected by the OSPF process into the routing table.

R2#sh ip protocols

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    0.0.0.0 255.255.255.255 area 0
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway          Distance      Last Update
  Distance: (default is 110)
```

R2#sh ip ospf interface

```
Loopback0 is up, line protocol is up
  Internet Address 2.2.2.2/24, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.102.2/24, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.10.10.10, Interface address 10.1.102.10
  Backup Designated router (ID) 2.2.2.2, Interface address 10.1.102.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
```

```
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.10.10.10  (Designated Router)
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
  Youngest key id is 1
```

R2#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.10.10.10	1	FULL/DR	00:00:35	10.1.102.10	GigabitEthernet0/0

R2#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
      2.0.0.0/24 is subnetted, 1 subnets
C      2.2.2.0 is directly connected, Loopback0
      10.0.0.0/24 is subnetted, 1 subnets
C      10.1.102.0 is directly connected, GigabitEthernet0/0
```

Task 3

Configure EIGRP AS 104 between ASA and R4. EIGRP messages should be authenticated using MD5 with key of "cisco789". Remove previously configured static routes for that segment.



EIGRP has some similarities to the previous two dynamic routing protocols. It uses keychain on the router (as RIPv2) and requires normal mask to be provided for a network on ASA (as OSPF).

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# sh run route
route DMZ 4.4.4.0 255.255.255.0 10.1.104.4 1

ASA-FW(config)# no route DMZ 4.4.4.0 255.255.255.0 10.1.104.4 1

ASA-FW(config)# router eigrp 104
ASA-FW(config-router)# no auto-summary
ASA-FW(config-router)# network 10.1.104.10 255.255.255.255
ASA-FW(config-router)# int e0/2.104
ASA-FW(config-subif)# authentication mode eigrp 104 md5
ASA-FW(config-subif)# authentication key eigrp 104 cisco789 key-id
1
ASA-FW(config-subif)# exit
```

Note that you must use regular netmask on the ASA and wildcard netmask on the IOS router when configuring networks under EIGRP. Authentication is enabled per interface basis.

Step 2 R4 configuration.

```
R4#sh run | in route
ip source-route
ip route 0.0.0.0 0.0.0.0 10.1.104.10

R4#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R4(config)#no ip route 0.0.0.0 0.0.0.0 10.1.104.10

R4(config)#key chain AUTH
R4(config-keychain)#key 1
R4(config-keychain-key)#key-string cisco789

R4(config-keychain-key)#router eigrp 104
R4(config-router)#no auto
R4(config-router)#network 0.0.0.0 0.0.0.0

R4(config-router)#int f0/0
R4(config-if)#ip authentication mode eigrp 104 md5
R4(config-if)#ip authentication key-chain eigrp 104 AUTH
R4(config-if)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console
R4#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 104: Neighbor 10.1.104.10
(FastEthernet0/0) is up: new adjacency
```

Verification

R4#sh ip eigrp neighbors

IP-EIGRP neighbors for process 104

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q	Seq Cnt Num
0	10.1.104.10	Fa0/0	10 00:00:55	3	200	0	5

R4#sh ip protocols

Routing Protocol is "eigrp 104"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Default networks flagged in outgoing updates

Default networks accepted from incoming updates

EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

EIGRP maximum hopcount 100

EIGRP maximum metric variance 1

Redistributing: eigrp 104

EIGRP NSF-aware route hold timer is 240s

Automatic network summarization is not in effect

Maximum path: 4

Routing for Networks:

0.0.0.0

Routing Information Sources:

Gateway	Distance	Last Update

Distance: internal 90 external 170

EIGRP is enabled on every interface.

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

4.0.0.0/24 is subnetted, 1 subnets
C      4.4.4.0 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.104.0 is directly connected, FastEthernet0/0

```

ASA-FW(config)# sh eigrp 104 int

EIGRP-IPv4 interfaces for process 104

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
DMZ	1	0/0	1	0/1	50	0

On the ASA EIGRP is enabled only on DMZ interface

ASA-FW(config)# sh eigrp 104 neighbors

EIGRP-IPv4 neighbors for process 104

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	10.1.104.4	Et0/2.104	13 00:01:52	1	200	0	3

ASA-FW(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 10.1.102.2 to network 0.0.0.0

```

R      1.1.1.0 255.255.255.0 [120/1] via 10.1.101.1, 0:00:14, IN

```

```
O    2.2.2.2 255.255.255.255 [110/11] via 10.1.102.2, 0:11:03, OUT
D    4.4.4.0 255.255.255.0 [90/156160] via 10.1.104.4, 0:01:58, DMZ
C    10.1.104.0 255.255.255.0 is directly connected, DMZ
C    10.1.102.0 255.255.255.0 is directly connected, OUT
C    10.1.101.0 255.255.255.0 is directly connected, IN
O*E2 0.0.0.0 0.0.0.0 [110/1] via 10.1.102.2, 0:11:03, OUT
```

EIGRP prefix for R4's loopback is in ASA's routing table.

Task 4

On ASA configure route redistribution between all three dynamic routing protocols, so that the network will gain full reachability.



Redistribution should be carefully configured as each of dynamic routing protocols requires specific parameters to successfully redistribute routes. Here are the most important things you should remember:

- *RIPv2 requires metric (hops) to be specified during redistribution;*
- *OSPF requires “subnet” keyword in order to take subnetted networks under consideration;*
- *EIGRP requires metric to be specified during redistribution;*

Remember that you can use more complex redistribution scenarios (like route-maps or other filtering methods) if required.

If no metric is specified in the task you can use any metric you want during redistribution.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# router rip
ASA-FW(config-router)# redistribute ospf 1 metric 2
ASA-FW(config-router)# redistribute eigrp 104 metric 1

ASA-FW(config-router)# router ospf 1
ASA-FW(config-router)# redistribute rip subnets
ASA-FW(config-router)# redistribute eigrp 104 subnets

ASA-FW(config-router)# router eigrp 104
ASA-FW(config-router)# redistribute rip metric 100000 0 255 1 1500
```

```
ASA-FW(config-router)# redistribute ospf 1 metric 100000 0 255 1
1500
ASA-FW(config-router)# exit
```

Verification

ASA-FW(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 10.1.102.2 to network 0.0.0.0

```
R 1.1.1.0 255.255.255.0 [120/1] via 10.1.101.1, 0:00:11, IN
O 2.2.2.2 255.255.255.255 [110/11] via 10.1.102.2, 0:00:11, OUT
D 4.4.4.0 255.255.255.0 [90/156160] via 10.1.104.4, 0:06:58, DMZ
C 10.1.104.0 255.255.255.0 is directly connected, DMZ
C 10.1.102.0 255.255.255.0 is directly connected, OUT
C 10.1.101.0 255.255.255.0 is directly connected, IN
O*E2 0.0.0.0 0.0.0.0 [110/1] via 10.1.102.2, 0:00:11, OUT
```

The ASA sees all networks so that it can redistribute that information into its routing protocols to let other routers know about those networks.

R1#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.101.10 to network 0.0.0.0

```
1.0.0.0/24 is subnetted, 1 subnets
C 1.1.1.0 is directly connected, Loopback0
2.0.0.0/32 is subnetted, 1 subnets
R 2.2.2.2 [120/2] via 10.1.101.10, 00:00:02, FastEthernet0/0
4.0.0.0/24 is subnetted, 1 subnets
R 4.4.4.0 [120/1] via 10.1.101.10, 00:00:02, FastEthernet0/0
10.0.0.0/24 is subnetted, 3 subnets
R 10.1.104.0 [120/1] via 10.1.101.10, 00:00:02, FastEthernet0/0
R 10.1.102.0 [120/1] via 10.1.101.10, 00:00:02, FastEthernet0/0
C 10.1.101.0 is directly connected, FastEthernet0/0
```

```
R* 0.0.0.0/0 [120/2] via 10.1.101.10, 00:00:03, FastEthernet0/0
```

R1 got all information via RIPv2. Note that prefixes redistributed from the OSPF have higher metric (hop count) than prefixes from EIGRP. This is due to "metric" keyword during the redistribution.

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```
1.0.0.0/24 is subnetted, 1 subnets
O E2 1.1.1.0 [110/20] via 10.1.102.10, 00:00:36, GigabitEthernet0/0
2.0.0.0/24 is subnetted, 1 subnets
C 2.2.2.0 is directly connected, Loopback0
4.0.0.0/24 is subnetted, 1 subnets
O E2 4.4.4.0 [110/20] via 10.1.102.10, 00:00:36, GigabitEthernet0/0
10.0.0.0/24 is subnetted, 3 subnets
O E2 10.1.104.0 [110/20] via 10.1.102.10, 00:00:36, GigabitEthernet0/0
C 10.1.102.0 is directly connected, GigabitEthernet0/0
O E2 10.1.101.0 [110/20] via 10.1.102.10, 00:00:37, GigabitEthernet0/0
```

R2 sees all networks as OSPF External type. The cost of a type 2 route is always the external cost, irrespective of the interior cost to reach that route.

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.104.10 to network 0.0.0.0

```
1.0.0.0/24 is subnetted, 1 subnets
D EX 1.1.1.0 [170/28160] via 10.1.104.10, 00:00:45, FastEthernet0/0
2.0.0.0/32 is subnetted, 1 subnets
D EX 2.2.2.2 [170/28160] via 10.1.104.10, 00:00:45, FastEthernet0/0
4.0.0.0/24 is subnetted, 1 subnets
C 4.4.4.0 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 3 subnets
```



```
C      10.1.104.0 is directly connected, FastEthernet0/0
D EX   10.1.102.0 [170/28160] via 10.1.104.10, 00:00:45, FastEthernet0/0
D EX   10.1.101.0 [170/28160] via 10.1.104.10, 00:00:46, FastEthernet0/0
D*EX 0.0.0.0/0 [170/28160] via 10.1.104.10, 00:00:46, FastEthernet0/0
```

R4 has EIGRP External type with AD (Administrative Distance) of 170. This AD is much worse than regular EIGRP which is 90. This is a basic loop prevention mechanism.

R1#p 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

R1#p 10.1.104.4

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.104.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

R1#p 2.2.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

R1#p 4.4.4.4

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

R1#tel 4.4.4.4 /so lo0

```
Trying 4.4.4.4 ... Open
```

User Access Verification

Password:

```
R4>exit
```

```
[Connection to 4.4.4.4 closed by foreign host]
```

R2#tel 1.1.1.1

```
Trying 1.1.1.1 ...
```

```
% Connection timed out; remote host not responding
```

```
R2#tel 1.1.1.1 /so lo0
```

```
Trying 1.1.1.1 ... Open
```

```
User Access Verification
```

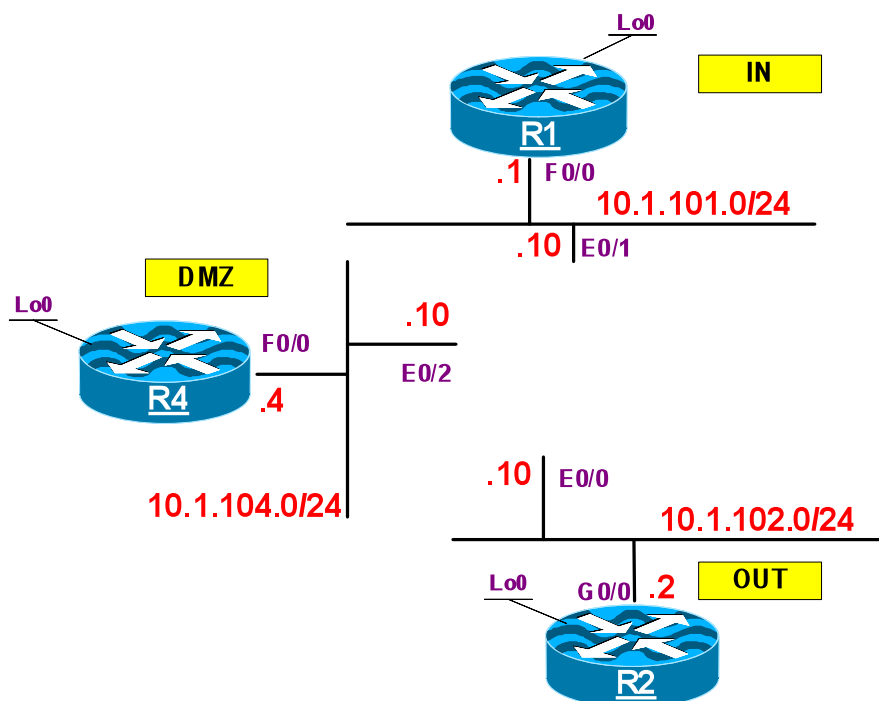
```
Password:
```

```
R1>exit
```

```
[Connection to 1.1.1.1 closed by foreign host]
```

Full network connectivity has been achieved.

Lab 1.4. ASA management



This lab is based on the previous lab configuration.

Task 1

Configure domain name of “micronicstraining.com” and enable Adaptive Security Device Manager (ASDM) access to the ASA from the inside network. To accomplish this put the management station (TestPC, 10.1.101.254/24) in the Inside network (VLAN 101). Create user admin with password of “cisco123”.



ASDM is a graphical user interface (GUI) for managing ASA. Although it is not mentioned in the CCIE SECURITY v4 Lab Exam Blueprint as a configuration tool it is useful to know how to use it. There are some configuration tasks which cannot be done from configuration line interface (CLI) and can be accomplished using ASDM (i.e. bookmark lists for Clientless VPN, etc.)

ASDM image file is located on the flash disk and needs to be configured before first use. Access to the ASDM is via HTTP/HTTPS and some special

configuration needs to be done to enable HTTP server on the ASA.

Configuration

Complete these steps:

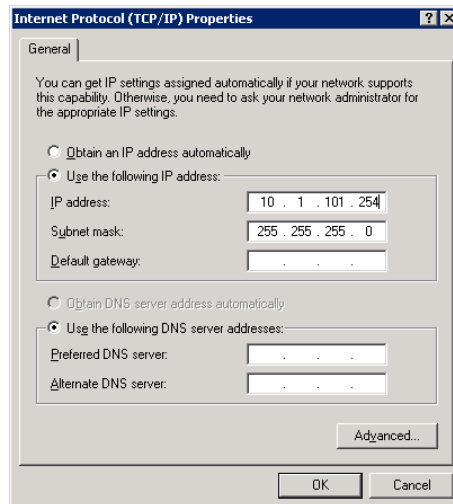
Step 1 ASA configuration.

```
ASA-FW(config)# domain-name micronicstraining.com
ASA-FW(config)# http server enable
ASA-FW(config)# http 10.1.101.254 255.255.255.255 IN

ASA-FW(config)# sh flash | in asdm
108 11348300    May 25 2010 16:51:02  asdm-621.bin

ASA-FW(config)# asdm image flash:/asdm-621.bin
ASA-FW(config)# username admin password cisco123 privilege 15
```

Step 2 Test PC configuration.

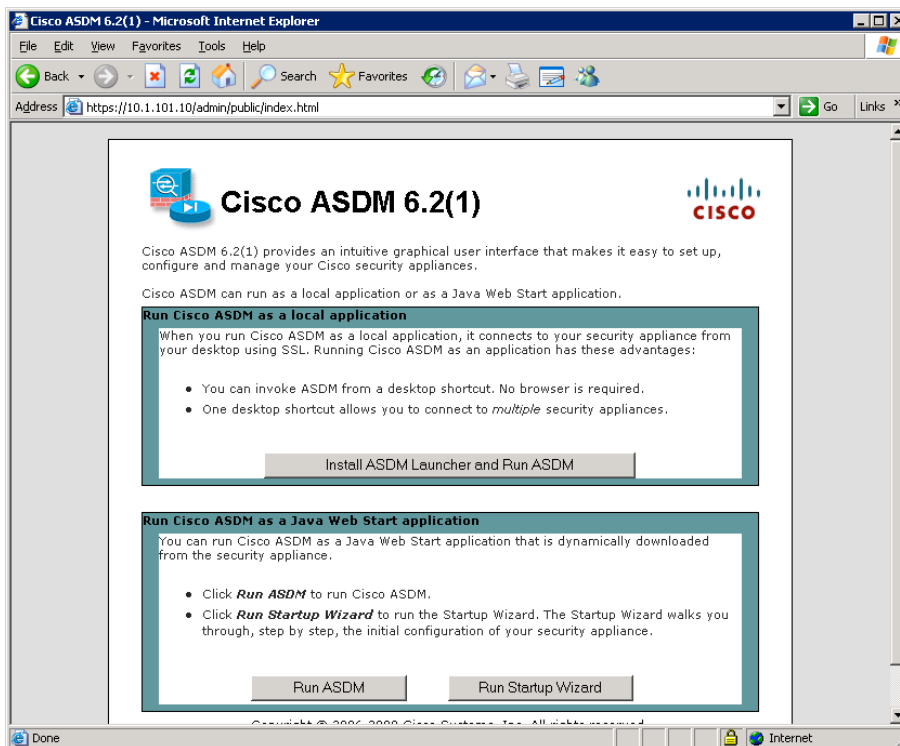


Verification

Step 1: Run a web browser and type <https://10.1.101.10> in an address bar. A security alert should show up which needs to be accepted.



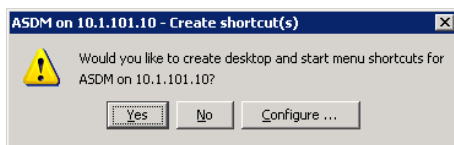
Step 2: You have an option to download and install ASDM software on your local computer or to run it remotely. Click *Run ASDM* to run it on your local machine.



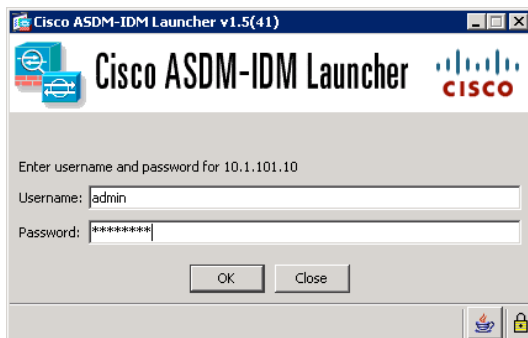
Step 3: Accept a security warning to be able to run ASDM's Java scripts.

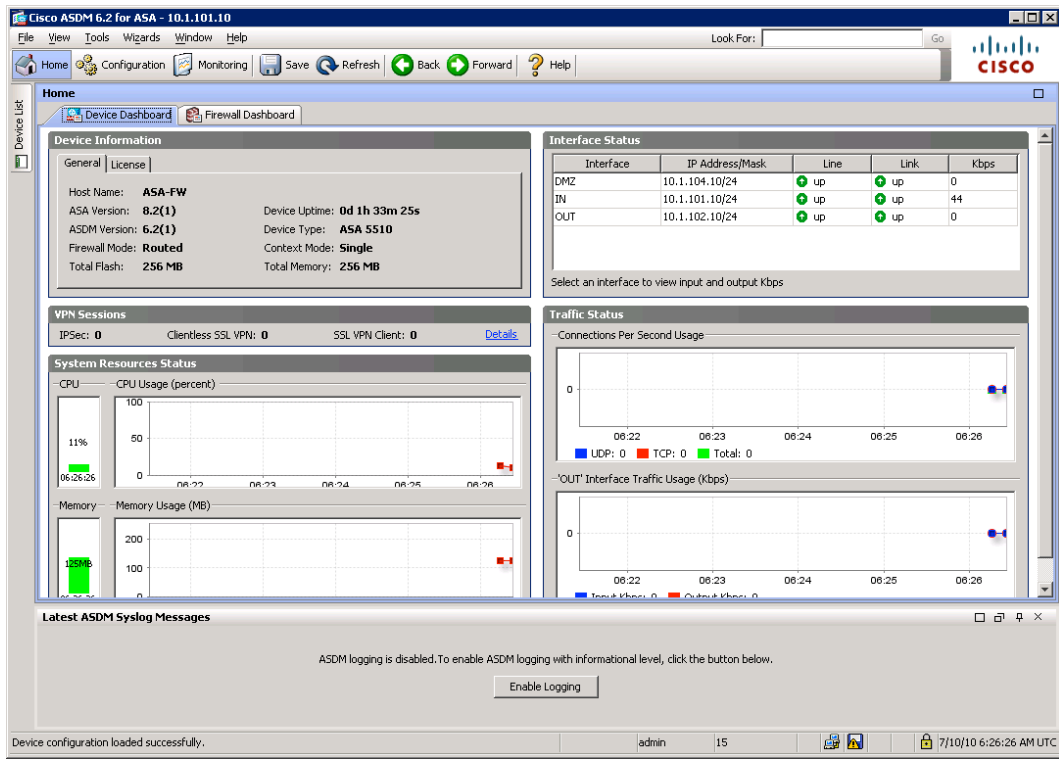


Step 4: You can create shortcut on your desktop and start menu for later use.



Step 5: Once ASDM is downloaded and run you must provide username and password for authentication. After successful authentication ASDM should open configuration GUI.





Task 2

Configure remote management access via SSH version 2 from host IP 1.1.1.1 located in the Inside network. Make sure user is automatically logged out after 12 minutes of inactivity. Use RSA keys of 1024 bits in length to secure management connections and password of "cisco789".



SSH management access requires RSA keys to be generated. You must configure subnets/hosts that will be allowed to connect to the ASA. There is a built-in username of "pix" configured on the ASA which can be used for SSH access. The password for this user is the same as enable password.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# ssh 1.1.1.1 255.255.255.255 IN
ASA-FW(config)# ssh timeout 12
ASA-FW(config)# ssh version 2
```

```
ASA-FW(config)# passwd cisco789
```

```
ASA-FW(config)# crypto key generate rsa modulus 1024
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

Verification

```
ASA-FW(config)# sh ssh
```

```
Timeout: 12 minutes
Version allowed: 2
1.1.1.1 255.255.255.255 IN
```

Note that to test this configuration you must change source IP address for SSH connections on R1. By default source address is an IP address of the outgoing interface. You'll need RSA keys of at least 768 bits size to be able to use SSHv2. If your router has no RSA keys already, you must generate new keys (remember that you need hostname and domain name to be configured before generating keys).

```
R1(config)#ip ssh source-interface lo0
Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
```

```
R1(config)#ip domain-name micronicstraining.com
R1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1.micronicstraining.com
```

```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R1(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
R1#ssh -c 3des -l pix 10.1.101.10
```

```
Password:
Type help or '?' for a list of available commands.
ASA-FW>
```

Task 3

Configure banner message so that it will display for successful remote connection via SSH. The banner should include the following message:

★

Welcome to ASA-FW.micronicstraining.com.

Only authorized users are allowed to connect.

★



In this task a Message of the Day (MOTD) banner should be configured. Remember that you can use some variables to be included in the banner automatically.

The tokens \$(domain) and \$(hostname) are replaced with the hostname and domain name of the ASA.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# banner motd ★
ASA-FW(config)# banner motd Welcome to $(hostname).$(domain).
ASA-FW(config)# banner motd Only authorized users are allowed to
connect.
ASA-FW(config)# banner motd ★
```

Verification

```
ASA-FW(config)# sh banner
```

```
motd:
★
Welcome to $(hostname).$(domain).
Only authorized users are allowed to connect.
★
```

```
R1#ssh -c 3des -l pix 10.1.101.10
```

```
Password:
```

```
★
```

```
Welcome to ASA-FW.micronicstraining.com.
```

```
Only authorized users are allowed to connect.
```

```
★
```

```
Type help or '?' for a list of available commands.
```

ASA-FW>

Task 4

Configure ASA so that it will automatically send configuration file to a TFTP server after issuing “write net” CLI command. The TFTP server is located in the Inside network with IP address of 10.1.101.254 and the file should be stored in the directory named “backups” using the file name of “ASA-FW.cfg”.



This is a one-line simple task. All you need is to configure TFTP server remote location specifying an interface which should be used to connect to the TFTP server, and IP address of the TFTP server and the file name with a full path to store the configuration in. Note that you can be unable to test that configuration on remote racks if there is no TFTP server running on the specified IP address.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# tftp-server IN 10.1.101.254 /backups/ASA-FW.cfg
```

Verification

```
ASA-FW(config)# write net
Building configuration...
Cryptochecksum: d424e00c c58583c2 0c78ad3a 080ed6f9
!!
[OK]
```

Task 5

Enable SYSLOG logging so that it will send all Informational and higher level events to the SYSLOG server located at 10.1.101.254 using UDP port 514 as a transport. The logging queue should be able to hold 100 messages when SYSLOG server is busy.

In addition to that, firewall administrator should be notified by email (fwadmin@micronicstraining.com) of every events regarding AUTH logging subsystem which are higher than or equal to level 3. Use email address of asa-fw@micronicstraining.com as a source and SMTP server located at 10.1.101.254. Also, configure rate limit for all Debug level messages so that no more than 10 messages are generated in 1 second interval in case console logging is used.



SYSLOG logging is a most popular method of sending system logs to the external server. It uses UDP port 514 by default and sends only those logs which are specified by the administrator (log level must be configured). You can also configure other logging methods like sending logs to some email using specified SMTP server.

When configuring SYSLOG logging ensure you use appropriate logging level to not be overwhelmed by lots of unnecessary information. Remember that configured logging level includes all lower levels, for example when you configure critical (2) level it includes alerts (1) and emergencies (0) as well.

There are the following logging levels:

- (0) emergencies - system is unusable
- (1) alerts - immediate action needed
- (2) critical - critical conditions
- (3) errors - error conditions
- (4) warnings - warning conditions
- (5) notifications - normal but significant conditions
- (6) informational - informational messages
- (7) debugging - debugging messages

You must be very careful when enabling logging for level 7 (debugging) as this may generate a lot of SYSLOG messages (depending on system usage). This is very dangerous for ASA stability especially when you enable logging on the console. Thus, there is a good practice to rate limit those messages to not be surprised when debugging is on the console.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# logging host IN 10.1.101.254
WARNING: interface Ethernet1 security level is 80.
```

```
ASA-FW(config)# logging queue 100
ASA-FW(config)# logging trap informational
ASA-FW(config)# logging enable
```

SYSLOG server is to be expected behind the most trusted interface (usually having security level of 100). When this server is specified behind lower security level interface then a warning message is displayed.

Logs are processed sequentially by the queue mechanism. If there are so many logs that the ASA cannot handle, the logs can be discarded. Note that if you specify the logging queue of zero, this means the queue is set to 8192, which is maximum.

SNMP Traps are usually sent to some NMS (Network Management System) but we can also send them to the SYSLOG server, but we need to specify what severity level we want to be sent. Finally, do not forget to enable logging. You can do that using "logging enable" or "logging on" commands.

```
ASA-FW(config)# logging from-address asa-fw@micronicstraining.com
ASA-FW(config)# logging recipient-address
fwadmin@micronicstraining.com level errors
ASA-FW(config)# logging list AUTH-ERR level errors class auth
ASA-FW(config)# logging mail AUTH-ERR
ASA-FW(config)# smtp-server 10.1.101.254
```

There is also a chance to send logs to other destination than SYSLOG. For example, you can send logs to the email address you specify. Doing that is pretty risky as there must be a lot of logs to be send so that an email is not a perfect solution. However, you can create a list of severity levels and classes, which should be sent using that method. In our example we're sending only Severity level of 3 with a class Auth for user authentication events.

Do not forget to configure SMTP server to send the emails to.

```
ASA-FW(config)# logging rate-limit 10 1 level debug
```

Debugging is a really good troubleshooting method. However, it may be really destructive for ASA's performance - Especially when we want to see debugging messages on the console. To lower the risk, we should always limit number of logging messages while debugging.

Verification

ASA-FW(config)# sh logging

```
Syslog logging: enabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: level informational, facility 20, 10 messages logged
  Logging to IN 10.1.101.254 errors: 1  dropped: 7
History logging: disabled
Device ID: disabled
Mail logging: list AUTH-ERR, 0 messages logged
ASDM logging: disabled
```

ASA-FW(config)# sh logging queue

```
Logging Queue length limit : 100 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msg on queue, 1 msgs most on queue
```

After configuring logging features we should always check then using "show logg" command.

Task 6

Configure ASA as NTP client using MD5 authentication with a key of "Cisco_NTP". The NTP server must be configured at 1.1.1.1 with a stratum of 4.



Network Time Protocol (NTP) is used for time synchronization on network devices. Having current time on the ASA is very important from a security audit perspective. It is important to have valid timestamps in the logs to be able to track malicious activity. Time is also very important when the ASA terminates VPNs and uses X.509 certificates for authentication (certificates have validity time and must be checked against reliable time source before usage).

NTP authentication is used to authenticate server to ensure that the ASA gets time from valid source.

The router can be an NTP server by using "ntp master <stratum>" command. The stratum level defines its distance from the reference clock. It is important to

note that the stratum is not an indication of quality or reliability of the NTP server.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# ntp authentication-key 1 md5 Cisco_NTP
ASA-FW(config)# ntp authenticate
ASA-FW(config)# ntp trusted-key 1
ASA-FW(config)# ntp server 1.1.1.1 key 1 source IN
```

Remember that you must specify the trusted key to be used.
Without this the NTP Server does not enable authentication.

Step 2 R1 configuration.

```
R1(config)#ntp authentication-key 1 md5 Cisco_NTP
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
R1(config)#ntp master 4
R1(config)#ntp source lo0
```

Verification

ASA-FW(config)# sh ntp associations

address	ref clock	st	when	poll	reach	delay	offset	disp
*~1.1.1.1	127.127.7.1	4	33	64	37	0.9	-0.95	890.8

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

ASA-FW(config)# sh ntp associations detail

```
1.1.1.1 configured, authenticated, our_master, sane, valid, stratum 4
ref ID 127.127.7.1, time ce822bf1.417e5616 (23:17:05.255 UTC Thu Oct 15 2009)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 37, sync dist 891.235
delay 0.85 msec, offset -0.9517 msec, dispersion 890.78
precision 2**18, version 3
org time ce822c00.8e86d0be (23:17:20.556 UTC Thu Oct 15 2009)
rcv time ce822c00.8eela66d (23:17:20.558 UTC Thu Oct 15 2009)
xmt time ce822c00.8e573047 (23:17:20.556 UTC Thu Oct 15 2009)
filtdelay =      0.85      0.89      0.87      1.08      1.02      0.00      0.00      0.00
```

```
filtoffset =   -0.95   -0.97   -1.09   -1.33   -2.05    0.00    0.00    0.00
filtererror =   15.63   16.60   17.58   18.55   19.53 16000.0 16000.0 16000.0
```

ASA-FW(config)# sh ntp status

Clock is synchronized, stratum 5, reference is 1.1.1.1

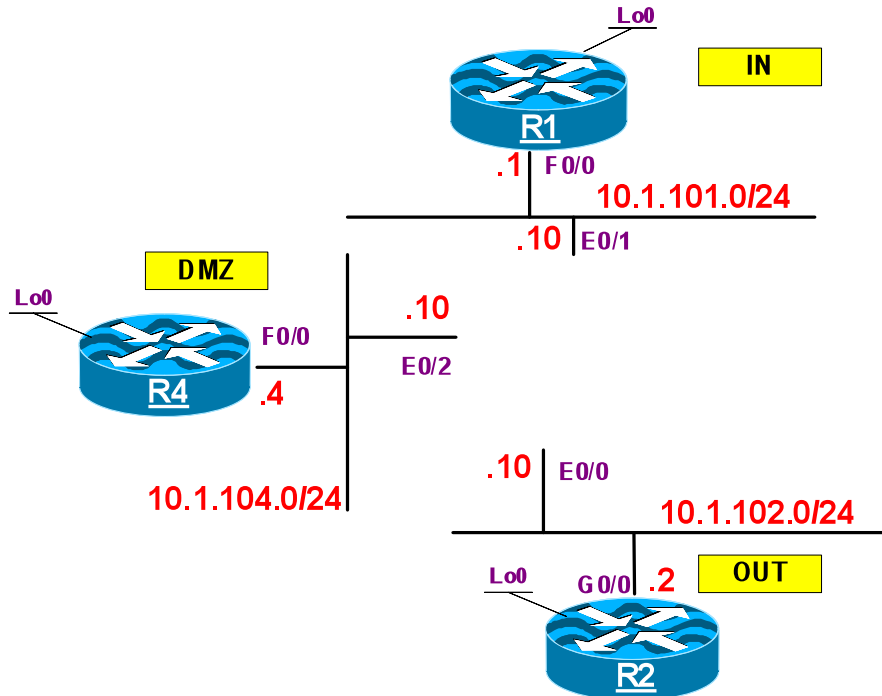
nominal freq is 99.9984 Hz, actual freq is 99.9985 Hz, precision is 2**6

reference time is ce822c00.8ee1a66d (23:17:20.558 UTC Thu Oct 15 2009)

clock offset is -0.9517 msec, root delay is 0.85 msec

root dispersion is 891.77 msec, peer dispersion is 890.78 msec

Lab 1.5. Static NAT (8.2)



This lab is based on ASA 8.2 software version. Make sure you downgrade the ASA code to that version before continuing. Required files should be on flash.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Task 1

Configure ASA so that when someone from the outside (network segment behind ASA's OUT interface) tries to connect to IP address of 10.1.102.1 he/she will be pointed to R1's loopback0 interface. Limit the embryonic connections for hosts using that connection to 2. Ensure all packets need to be translated in order to pass through the ASA.



First of all NAT Control feature must be enabled to control ASA behavior in such way that all packets need to be translated in order to pass between interfaces.

To accomplish this task you need to configure R1's loopback0 IP address to be seen as 10.1.102.1 on the ASA's outside subnet. This can be done by using Static NAT (SNAT) with a parameter of hosts embryonic connections set to 2.

However, this is not enough to pass traffic. The ASA does not allow connections coming from an interface with a lower security level to an interface with a higher security level without an ACL allowing that connections. Thus, you need to configure an ACL in the inbound direction on ASA's outside interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat-control
ASA-FW(config)# static (IN,OUT) 10.1.102.1 1.1.1.1 netmask
255.255.255.255 tcp 0 2

ASA-FW(config)# access-list OUTSIDE_IN permit ip any host
10.1.102.1
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

Verification

```
ASA-FW(config)# sh xlate
1 in use, 1 most used
Global 10.1.102.1 Local 1.1.1.1
```

ASA-FW(config)# sh xlate detail

```

1 in use, 1 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
      r - portmap, s - static
NAT from IN:1.1.1.1 to OUT:10.1.102.1 flags s

```

See the xlate created - there is a flag field indicating that the xlate is due to static translation. This xlate will be in the xlate table all the time.

R2#tel 10.1.102.1

```
Trying 10.1.102.1 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R1>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:03:44	
*514 vty 0		idle	00:00:00	10.1.102.2

Interface	User	Mode	Idle	Peer Address

The location field indicates that the source IP address has been translated in the path.

```
R1>exit
```

```
[Connection to 10.1.102.1 closed by foreign host]
```

R2#ping 10.1.102.1

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

```

R1#tel 2.2.2.2

```

Trying 2.2.2.2 ...
% Connection refused by remote host

```

Connection is refused by the ASA as there is no translation configured for that IP address. There is NAT Control enabled and all packets must have translation rule in place to be allowed through the ASA.

R1#tel 2.2.2.2 /so lo0

```
Trying 2.2.2.2 ... Open
```

```
User Access Verification
```

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:24	
*578 vty 0		idle	00:00:00	10.1.102.1

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

Note that Static NAT works in both ways - no matter if you originate traffic from R2 or R1.

Task 2

Configure ASA so that when someone from the outside (network segment behind ASA's OUT interface) tries to connect to IP address of 10.1.102.4 using TELNET, he/she will be pointed to R4's loopback0 interface.



This task is similar to the previous however there is one difference. The translation must be used only for TELNET traffic. This is called Static PAT (Port Address Translation) and it's useful for "port redirection".

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# static (DMZ,OUT) tcp 10.1.102.4 telnet 4.4.4.4
telnet netmask 255.255.255.255
ASA-FW(config)# access-list OUTSIDE_IN permit tcp any host
10.1.102.4 eq telnet
```

Note that "telnet" keyword can be changed to port number (23 in this case).

Verification

ASA-FW(config)# sh xlate

```
2 in use, 2 most used
Global 10.1.102.1 Local 1.1.1.1
PAT Global 10.1.102.4(23) Local 4.4.4.4(23)
```

ASA-FW(config)# sh xlate detail

```
2 in use, 2 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
      r - portmap, s - static
NAT from IN:1.1.1.1 to OUT:10.1.102.1 flags s
TCP PAT from DMZ:4.4.4.4/23 to OUT:10.1.102.4/23 flags sr
```

The flag field indicates this is "static portmap" rule - port redirection in other words.

R2#tel 10.1.102.4

Trying 10.1.102.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:07:45	
*514 vty 0		idle	00:00:00	10.1.102.2

Interface	User	Mode	Idle	Peer Address

R4>exit

[Connection to 10.1.102.4 closed by foreign host]

R2#ping 10.1.102.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.4, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

R4#tel 10.1.102.2

Trying 10.1.102.2 ...

% Connection refused by remote host

R4#tel 10.1.102.2 /so lo0

Trying 10.1.102.2 ...

% Connection refused by remote host

Note that when Static PAT is used there is only one-way translation.

Task 3

Configure ASA so that when someone from the outside (network segment behind ASA's OUT interface) tries to connect to ASA's OUT interface using port 2323, he/she will be redirected to R1's F0/0 interface using port 23.



This task is similar to the previous however in this case the ASA must "listen" on its outside interface on port 2323 and "redirect" all traffic coming to that interface/port to the IP address of R1's F0/0 interface and port 23.

Note that you still need an ACL entry on the outside interface for those connections.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# static (IN,OUT) tcp interface 2323 10.1.101.1
telnet netmask 255.255.255.255
SA-FW(config)# access-list OUTSIDE_IN permit tcp any host
10.1.102.10 eq 2323
```

Verification

ASA-FW(config)# sh xlate

```
3 in use, 3 most used
Global 10.1.102.1 Local 1.1.1.1
PAT Global 10.1.102.4(23) Local 4.4.4.4(23)
PAT Global 10.1.102.10(2323) Local 10.1.101.1(23)
```

ASA-FW(config)# sh xlate detail

```
3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
      r - portmap, s - static
NAT from IN:1.1.1.1 to OUT:10.1.102.1 flags s
```

TCP PAT from DMZ:4.4.4.4/23 to OUT:10.1.102.4/23 flags sr

TCP PAT from IN:10.1.101.1/23 to OUT:10.1.102.10/2323 flags sr

R2#tel 10.1.102.10 2323

Trying 10.1.102.10, 2323 ... Open

User Access Verification

Password:

R1>sh users

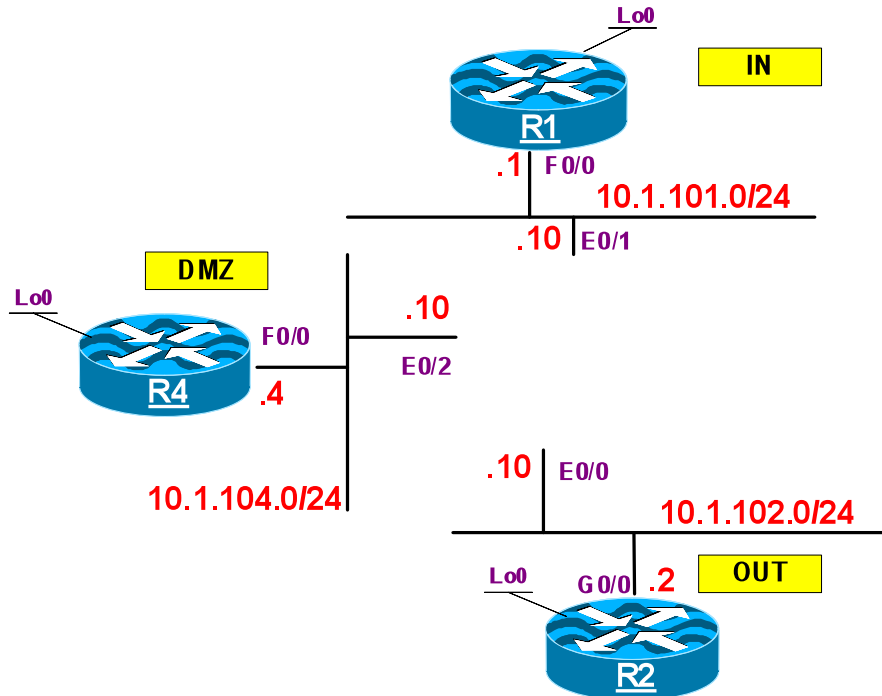
Line	User	Host(s)	Idle	Location
0 con 0		idle	00:08:58	
*514 vty 0		idle	00:00:00	10.1.102.2

Interface	User	Mode	Idle	Peer Address

R1>exit

[Connection to 10.1.102.10 closed by foreign host]

Lab 1.6. Dynamic NAT (8.2)



This lab is based on ASA 8.2 software version. Make sure you downgrade the ASA code to that version before continuing. Required files should be on flash.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the following commands:

```
clear configure static
clear configure access-list
```

Task 1

Ensure all packets need to be translated in order to pass through the ASA. However, when R4 tries to go outside using its loopback0 interface packets should not be translated.



NAT Control ensures that every packet going through the ASA must be translated. If there is no translation rule in place the packet is dropped. However, in this task we need to bypass this rule by configuring feature called NAT 0 (or Identity NAT). When we use ID 0 configuring NAT translation (source IP addresses to be translated) it means that packet matched that rule will NOT be translated. NAT 0 is evaluated before any other NAT statements and you don't need to configure Global statement for ID 0. This kind of NAT is useful in case of VPN configuration where is a need to not translate packets which are subjected to be going through the VPN tunnel.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat-control
ASA-FW(config)# nat (DMZ) 0 4.4.4.4 255.255.255.255
nat 0 4.4.4.4 will be identity translated for outbound
```

Verification

```
R4#tel 2.2.2.2
Trying 2.2.2.2 ...
% Connection refused by remote host
```

No translation rule for that connection.

```
R4#tel 2.2.2.2 /so lo0
Trying 2.2.2.2 ... Open
```

User Access Verification

Password:

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:12:00	
*578 vty 0		idle	00:00:00	4.4.4.4

Interface	User	Mode	Idle	Peer Address

```
R2>exit
```

```
[Connection to 2.2.2.2 closed by foreign host]
```

Note the 4.4.4.4 has not been translated.

```
ASA-FW(config)# sh xlate
```

```
1 in use, 3 most used
```

```
Global 4.4.4.4 Local 4.4.4.4
```

```
ASA-FW(config)# sh xlate detail
```

```
1 in use, 3 most used
```

```
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,  
r - portmap, s - static
```

```
NAT from DMZ:4.4.4.4 to OUT:4.4.4.4 flags iI
```

Note that the above translation is dynamically created when there is connection from R4's Lo0. The Identity NAT creates xlates for all IP addresses even though there is the same IP address used for translation.

The xlate will be present in the translation table for duration of 3 hours by default. This can be configured using timeout xlate <idle_time> command.

Task 2

Configure ASA so that all IP addresses from the inside subnet (10.1.101.0/24) will be translated to the dynamic pool of 10.1.102.100 – 10.1.102.200. If the pool is exhausted, configure ASA to perform dynamic port translation using IP address of 10.1.102.201.



This is the most common NAT configuration in the real world. Dynamic NAT translates all source IP addresses (specified by “nat (ifname) id IP-addresses” command) to the pool of IP addresses (specified by “global (ifname) ID IP-address-range” command). The ID must match NAT and GLOBAL statements. That configuration will dynamically translate each IP address to one GLOBAL IP address (one-to-one translation) so you need to ensure that after exhaustion of GLOBAL IP addresses the communication won’t suffer. This is usually accomplished by configuring one (or more) GLOBAL “backup” IP addresses to translate packets using PAT (ca. 64k ports can be used, so many connections can be covered).

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat (IN) 1 10.1.101.0 255.255.255.0
ASA-FW(config)# global (OUT) 1 10.1.102.100-10.1.102.200 netmask
255.255.255.0
ASA-FW(config)# global (OUT) 1 10.1.102.201 netmask 255.255.255.255
INFO: Global 10.1.102.201 will be Port Address Translated
```

Verification

```
R1#tel 2.2.2.2
```

```
Trying 2.2.2.2 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:18	
*578 vty 0		idle	00:00:00	10.1.102.170

Interface	User	Mode	Idle	Peer Address

Note that the source IP address has been translated to the random IP address from the pool.

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

R1#tel 2.2.2.2 /so lo0

Trying 2.2.2.2 ...

% Connection refused by remote host

R1#tel 4.4.4.4

Trying 4.4.4.4 ...

% Connection refused by remote host

Note that only connections between inside and outside subnets are translated. Since NAT Control is enabled, all packets must be translated. Thus, no connections allowed between inside and DMZ.

ASA-FW(config)# sh xlate

2 in use, 3 most used

Global 4.4.4.4 Local 4.4.4.4

Global 10.1.102.170 Local 10.1.101.1

ASA-FW(config)# sh xlate detail

2 in use, 3 most used

Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
r - portmap, s - static

NAT from DMZ:4.4.4.4 to OUT:4.4.4.4 flags iI

NAT from IN:10.1.101.1 to OUT:10.1.102.170 flags i

Task 3

Configure ASA so that when R1 tries to communicate with hosts in DMZ using its loopback0 interface as a source, it will be dynamically translated to ASA's DMZ interface IP address.



Instead of configuring GLOBAL pool of IP addresses you can specify ASA's interface and all source IP addresses specified by NAT command will be PAted to this IP address. Remember that you need to use different NAT ID for every NAT/GLOBAL pair.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat (IN) 2 1.1.1.1 255.255.255.255
ASA-FW(config)# global (DMZ) 2 interface
INFO: DMZ interface address added to PAT pool
```

Verification

R1#tel 4.4.4.4

Trying 4.4.4.4 ...

% Connection refused by remote host

R1#tel 4.4.4.4 /so lo0

Trying 4.4.4.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:13:23	
*514 vty 0		idle	00:00:00	10.1.104.10

Interface	User	Mode	Idle	Peer Address

R4>exit

[Connection to 4.4.4.4 closed by foreign host]

Do not disconnect from R4 and check ASA's translations. If you close the connection ASA will remove XLATE entry.

```
ASA-FW(config)# sh xlate
```

```
3 in use, 3 most used
Global 4.4.4.4 Local 4.4.4.4
PAT Global 10.1.104.10(29892) Local 1.1.1.1(56160)
Global 10.1.102.170 Local 10.1.101.1
```

```
ASA-FW(config)# sh xlate detail
```

```
3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
      r - portmap, s - static
NAT from DMZ:4.4.4.4 to OUT:4.4.4.4 flags iI
TCP PAT from IN:1.1.1.1/56160 to DMZ:10.1.104.10/29892 flags ri
NAT from IN:10.1.101.1 to OUT:10.1.102.170 flags i
```

Task 4

Configure ASA so that when R1 tries to communicate with hosts on the outside network using its loopback0 interface as a source, it will be dynamically translated to IP address of 10.1.102.202. Use minimal number of commands to accomplish this task.



Note that the NAT statement for IP address of 1.1.1.1 has been configured in the previous task; hence there is just need for GLOBAL statement for the outside interface. The NAT ID must be the same to match with NAT command. In this example the R1's loopback0 interface will be translated to two different IP addresses depends on the outbound interface on the ASA.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# global (OUT) 2 10.1.102.202 netmask 255.255.255.255
INFO: Global 10.1.102.202 will be Port Address Translated
```

Verification

```
R1#tel 2.2.2.2 /so lo0
```

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:19:34	
*578 vty 0		idle	00:00:00	10.1.102.202

Interface	User	Mode	Idle	Peer Address

R2>

When you're using terminal server to access your devices in the rack, use Ctrl+Shift+6+x to get back to the R1 and make another connection to R4's loopback0 using R1's loopback0 interface as a source. Do not disconnect previous sessions in order to see XLATE entries on the ASA.

<Ctrl+Shift+6 X>

R1#tel 4.4.4.4 /so lo0

Trying 4.4.4.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:15:15	
*514 vty 0		idle	00:00:00	10.1.104.10

Interface	User	Mode	Idle	Peer Address

R4>

<Ctrl+Shift+6 X>

R1#tel 2.2.2.2

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:21:24	
578 vty 0		idle	00:01:49	10.1.102.202


```
*579 vty 1          idle          00:00:09 10.1.102.170
```

Interface	User	Mode	Idle	Peer Address

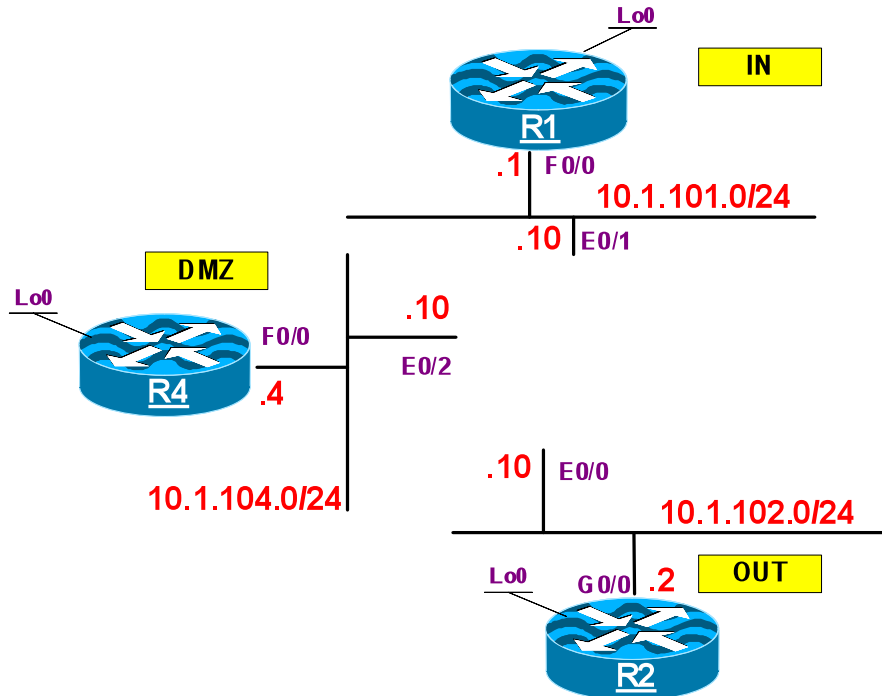
ASA-FW(config)# sh xlate

```
4 in use, 4 most used
Global 4.4.4.4 Local 4.4.4.4
PAT Global 10.1.104.10(4460) Local 1.1.1.1(52849)
PAT Global 10.1.102.202(6995) Local 1.1.1.1(29961)
Global 10.1.102.170 Local 10.1.101.1
```

ASA-FW(config)# sh xlate detail

```
4 in use, 4 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
      r - portmap, s - static
NAT from DMZ:4.4.4.4 to OUT:4.4.4.4 flags iI
TCP PAT from IN:1.1.1.1/52849 to DMZ:10.1.104.10/4460 flags ri
TCP PAT from IN:1.1.1.1/29961 to OUT:10.1.102.202/6995 flags ri
NAT from IN:10.1.101.1 to OUT:10.1.102.170 flags i
```

Lab 1.7. NAT Exemption (8.2)



This lab is based on ASA 8.2 software version. Make sure you downgrade the ASA code to that version before continuing. Required files should be on flash.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the following commands:

```
clear configure nat
clear configure global
clear xlate
```

Task 1

Ensure all packets need to be translated in order to pass through the ASA. Configure ASA so that it will dynamically translate all IP addresses coming from inside subnets (10.1.101.0/24 and 1.1.1.0/24) and destined to the outside networks to the pool of 10.1.102.100 – 10.1.102.200. However, communication between host 1.1.1.1 and 2.2.2.2 should not be translated.



NAT Control feature ensures that every packet going through the ASA will be translated.

This task is very similar to Identity NAT (from lab 1.6) but here we need to bypass NAT for traffic between two hosts (not only sourced from the inside network). To specify both source and destination we need to use an access list which will be used by “NAT 0” statement. This configuration is called NAT Exemption and is useful in VPN scenarios where some flows (usually those going through the VPN tunnel) must bypass translation.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat-control
ASA-FW(config)# nat (IN) 1 1.1.1.0 255.255.255.0
ASA-FW(config)# nat (IN) 1 10.1.101.0 255.255.255.0
```

```
ASA-FW(config)# global (OUT) 1 10.1.102.100-10.1.102.200 netmask  
255.255.255.0
```

```
ASA-FW(config)# access-list NO-NAT permit ip host 1.1.1.1 host  
2.2.2.2
```

```
ASA-FW(config)# nat (IN) 0 access-list NO-NAT
```

Verification

R1#tel 10.1.102.2

Trying 10.1.102.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:35:38	
*578 vty 0		idle	00:00:00	10.1.102.106

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 10.1.102.2 closed by foreign host]

R1#tel 2.2.2.2

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:35:59	
*578 vty 0		idle	00:00:00	10.1.102.106

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

R1#tel 2.2.2.2 /so 1o0

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:36:22	
*578 vty 0		idle	00:00:00	1.1.1.1

Interface	User	Mode	Idle	Peer Address

Note there is no translation (it seems like Identity NAT but it's not). See "sh xlate" to show the difference.

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

R1#tel 4.4.4.4

Trying 4.4.4.4 ...

% Connection refused by remote host

Note that Telnet connection between R1's loopback0 and R2's loopback0 is bypassing the translation (source IP address is the same after connection). However, connections to DMZ are unsuccessful because of NAT Control in place (no NAT/GLOBAL statement for such traffic is configured).

ASA-FW(config)# sh xlate

1 in use, 4 most used

Global 10.1.102.106 Local 10.1.101.1

ASA-FW(config)# sh xlate detail

1 in use, 4 most used

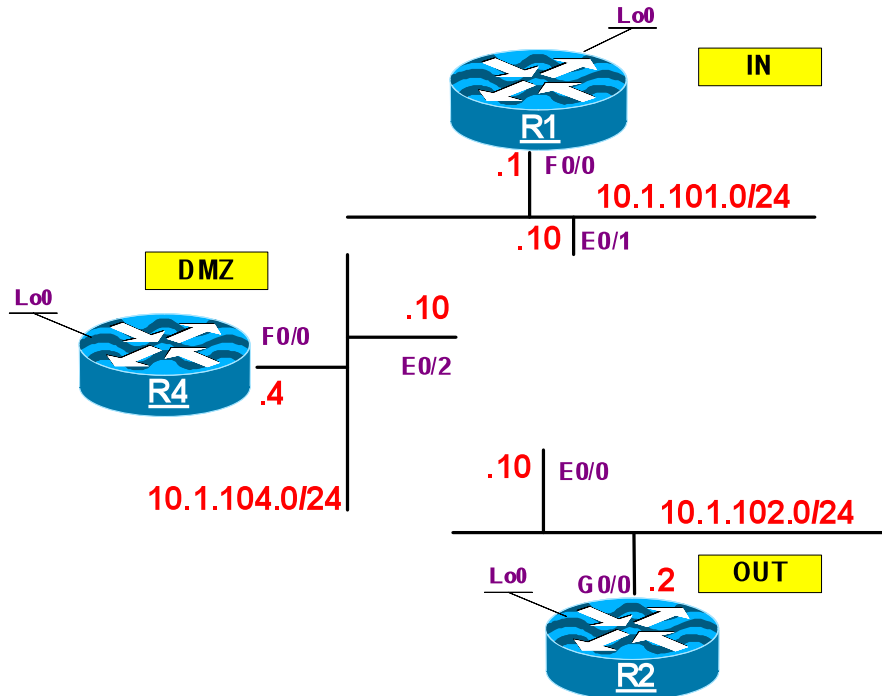
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,

r - portmap, s - static

NAT from IN:10.1.101.1 to OUT:10.1.102.106 flags i

Note that there is no XLATE for NAT Exemption!!! The NAT exemption DOES NOT work like Identity NAT. The Identity NAT creates Identity XLATE (the same Local and Global IP) and allows connections from both sites.

Lab 1.8. Static Policy NAT (8.2)



This lab is based on ASA 8.2 software version. Make sure you downgrade the ASA code to that version before continuing. Required files should be on flash.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the following commands:

```
clear configure nat
clear configure global
clear xlate
```

Task 1

Ensure all packets need to be translated in order to pass through the ASA. Configure ASA so that it statically translates R1's loopback0 IP address to its outside interface's IP address. The translation must be enforced only for traffic going between R1's loopback0 and R2's loopback0 interface.



NAT Control must be enabled in order to translate all packets going through the ASA. From the task we know that there must be STATIC translation in place and it should work only for traffic between two hosts. This leads to only one conclusion: there must be an access list involved.

Remember that even you configure ASA's interface to "serve" global translation IP address, there is a need for ACL in inbound direction to successfully pass the traffic.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat-control
ASA-FW(config)# access-list STATIC-POLICY permit ip host 1.1.1.1
host 2.2.2.2
ASA-FW(config)# static (IN,OUT) interface access-list STATIC-
POLICY
```

WARNING: All traffic destined to the IP address of the OUT interface is being redirected.
WARNING: Users will not be able to access any service enabled on the OUT interface.

```
ASA-FW(config)# access-list OUTSIDE_IN permit ip any host 10.1.102.10
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

Verification

ASA-FW(config)# sh xlate

```
1 in use, 4 most used
Global 10.1.102.10 Local 1.1.1.1
```

ASA-FW(config)# sh xlate detail

```
1 in use, 4 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
      r - portmap, s - static
NAT from IN:1.1.1.1 to OUT(STATIC-POLICY):10.1.102.10 flags s
```

Note the ACL name in the brackets. This XLATE entry is a conditional static.

R1#tel 10.1.102.2

```
Trying 10.1.102.2 ...
% Connection refused by remote host
```

R1#tel 10.1.102.2 /so lo0

```
Trying 10.1.102.2 ...
% Connection refused by remote host
```

R1#tel 2.2.2.2

```
Trying 2.2.2.2 ...
% Connection refused by remote host
```

R1#tel 2.2.2.2 /so lo0

```
Trying 2.2.2.2 ... Open
```

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:43:07	
*578 vty 0		idle	00:00:00	10.1.102.10

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

Only this traffic is translated.

R2#tel 10.1.102.10

Trying 10.1.102.10 ... Open

User Access Verification

Password:

R1>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:21	
*514 vty 0		idle	00:00:00	10.1.102.2

Interface	User	Mode	Idle	Peer Address

R1>exit

[Connection to 10.1.102.10 closed by foreign host]

R2#tel 10.1.102.10 /so 1o0

Trying 10.1.102.10 ... Open

User Access Verification

Password:

R1>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:01:39	
*514 vty 0		idle	00:00:00	2.2.2.2

Interface	User	Mode	Idle	Peer Address

R1>exi

[Connection to 10.1.102.10 closed by foreign host]

Note that only traffic between 1.1.1.1 and 2.2.2.2 is translated, no other traffic is allowed to go through the ASA because of NAT Control in place. However, due to the inbound ACL on the ASA's OUT interface the traffic can be originated from R2's loopback0 interface and destined to R1's loopback0 (destination IP address in this case should be ASA's OUT interface).

Task 2

Configure ASA so that it statically translates to the IP address of 10.1.104.1 all traffic coming from R1's loopback0 interface towards DMZ subnet. The translation rule should be used only for traffic originated from 1.1.1.1 and destined to 4.4.4.4.



*This task is very similar to the previous one. The difference is that here we need to use an arbitrary IP address for translation instead of ASA interface's IP address. Again, there is a need for ACL to specify what flows must be subjected to translation. Read the task carefully to see that the translation must work **ONLY** for traffic originated from 1.1.1.1. To disallow traffic coming (originating) from 4.4.4.4 towards 1.1.1.1 you just do **NOT** need to configure any inbound ACL on ASA's DMZ interface.*

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# access-list STATIC-POLICY-DMZ permit ip host
1.1.1.1 host 4.4.4.4
ASA-FW(config)# static (IN,DMZ) 10.1.104.1 access-list STATIC-
POLICY-DMZ
```

Verification

```
ASA-FW(config)# sh xlate
```

```
2 in use, 4 most used
Global 10.1.104.1 Local 1.1.1.1
Global 10.1.102.10 Local 1.1.1.1
```

```
ASA-FW(config)# sh xlate detail
```

```
2 in use, 4 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
      r - portmap, s - static
NAT from IN:1.1.1.1 to DMZ(STATIC-POLICY-DMZ):10.1.104.1 flags s
NAT from IN:1.1.1.1 to OUT(STATIC-POLICY):10.1.102.10 flags s
```

```
R1#tel 4.4.4.4
```

```
Trying 4.4.4.4 ...
% Connection refused by remote host
```

R1#tel 4.4.4.4 /so lo0

Trying 4.4.4.4 ...

% Connection timed out; remote host not responding

R1#tel 4.4.4.4 /so lo0

Trying 4.4.4.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:47:15	
*514 vty 0		idle	00:00:00	10.1.104.1

Interface	User	Mode	Idle	Peer Address

R4>exit

[Connection to 4.4.4.4 closed by foreign host]

R4#tel 10.1.104.1

Trying 10.1.104.1 ...

% Connection timed out; remote host not responding

R4#tel 10.1.104.1 /so lo0

Trying 10.1.104.1 ...

% Connection timed out; remote host not responding

Note that traffic from R4 to R1 is denied by ASA because there is no access list allowing it on DMZ interface. The ASA displays the following log (when logging is configured):

%ASA-2-106001: Inbound TCP connection denied from 4.4.4.4/46869 to 10.1.104.1/23 flags SYN on interface DMZ

Task 3

Configure static translation on ASA so that when R2 telnets to the IP address of 10.1.102.1 port tcp/2323 using its loopback0 interface as a source it will be automatically redirected to the host 1.1.1.1 port tcp/23. This translation rule should work only for traffic initiated from R2's loopback0 interface and destined to 10.1.102.1.



This task requires “port redirection” but only for traffic between two hosts. Again, there must be ACL involved to specify that hosts and enable translation for that specific flow. Be careful here because ACL must contain “original” IP address (non-translated) and destination port to be effective.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# access-list STATIC-R1 permit tcp host 1.1.1.1 eq telnet
host 2.2.2.2
ASA-FW(config)# static (IN,OUT) tcp 10.1.102.1 2323 access-list STATIC-R1

ASA-FW(config)# access-list OUTSIDE_IN permit tcp host 2.2.2.2 host
10.1.102.1 eq 2323
```

Verification

ASA-FW(config)# sh xlate

```
3 in use, 4 most used
Global 10.1.104.1 Local 1.1.1.1
Global 10.1.102.10 Local 1.1.1.1
PAT Global 10.1.102.1(2323) Local 1.1.1.1(23)
```

ASA-FW(config)# sh xlate detail

```
3 in use, 4 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
NAT from IN:1.1.1.1 to DMZ(STATIC-POLICY-DMZ):10.1.104.1 flags s
NAT from IN:1.1.1.1 to OUT(STATIC-POLICY):10.1.102.10 flags s
TCP PAT from IN:1.1.1.1/23 to OUT(STATIC-R1):10.1.102.1/2323 flags sr
```

R2#tel 10.1.102.1 2323

```
Trying 10.1.102.1, 2323 ...
% Connection timed out; remote host not responding
```

R2#tel 10.1.102.1 2323 /so lo0

```
Trying 10.1.102.1, 2323 ... Open
```

User Access Verification

```

Password:
R1>sh users
      Line          User           Host(s)           Idle           Location
    0 con 0
*514 vty 0           idle             idle             00:05:02
                                idle             00:00:00 2.2.2.2

      Interface      User           Mode           Idle           Peer Address

R1>exit

[Connection to 10.1.102.1 closed by foreign host]

```

Note that it works as expected and only traffic originated from R2's loopback0 interface is translated (redirected). Traffic originated from other IP address is denied by inbound ACL on the OUT interface.

Task 4

Configure ASA so that it statically translate all hosts from the inside network (10.1.101.0/24) to addresses on the 10.1.104.0/24 network making them all accessible from DMZ.



This type of NAT is useful when we want to make two networks fully accessible for each other. We need to translate whole network to another network and allow traffic to be originated from the subnet behind lower security level interface by configuring inbound ACL.

Configuration

Complete these steps:

Step 1 ASA configuration.

```

ASA-FW(config)# access-list STATIC-IN-DMZ permit ip 10.1.101.0
255.255.255.0 10.1.104.0 255.255.255.0
ASA-FW(config)# static (IN,DMZ) 10.1.104.0 access-list STATIC-IN-
DMZ
WARNING: mapped-address conflict with existing static
IN:1.1.1.1 to DMZ:10.1.104.1 netmask 255.255.255.255

ASA-FW(config)# access-list DMZ_IN permit ip any 10.1.104.0
255.255.255.0
ASA-FW(config)# access-group DMZ_IN in interface DMZ

```

Note there is warning message saying that there is conflict with already configured translation. However, this translation is for different source IP address - no big deal in the lab environment, however in the real world you must ensure there are no conflicts and use the same subnet masks for both networks (so that there are sufficient number of IP addresses for translation).

Verification

ASA-FW(config)# sh xlate

```
4 in use, 4 most used
Global 10.1.104.1 Local 1.1.1.1
Global 10.1.104.0 Local 10.1.101.0
Global 10.1.102.10 Local 1.1.1.1
PAT Global 10.1.102.1(2323) Local 1.1.1.1(23)
```

ASA-FW(config)# sh xlate detail

```
4 in use, 4 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
NAT from IN:1.1.1.1 to DMZ(STATIC-POLICY-DMZ):10.1.104.1 flags s
NAT from IN:10.1.101.0 to DMZ(STATIC-IN-DMZ):10.1.104.0 flags s
NAT from IN:1.1.1.1 to OUT(STATIC-POLICY):10.1.102.10 flags s
TCP PAT from IN:1.1.1.1/23 to OUT(STATIC-R1):10.1.102.1/2323 flags sr
```

R4#tel 10.1.104.1

```
Trying 10.1.104.1 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R1>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:10:03	
*514 vty 0		idle	00:00:00	10.1.104.4

Interface	User	Mode	Idle	Peer Address

```
R1>exit
```

```
[Connection to 10.1.104.1 closed by foreign host]
```

R4#tel 10.1.104.1 /so lo0

```
Trying 10.1.104.1 ... Open
```

```
User Access Verification
```

Password:

R1>sh users

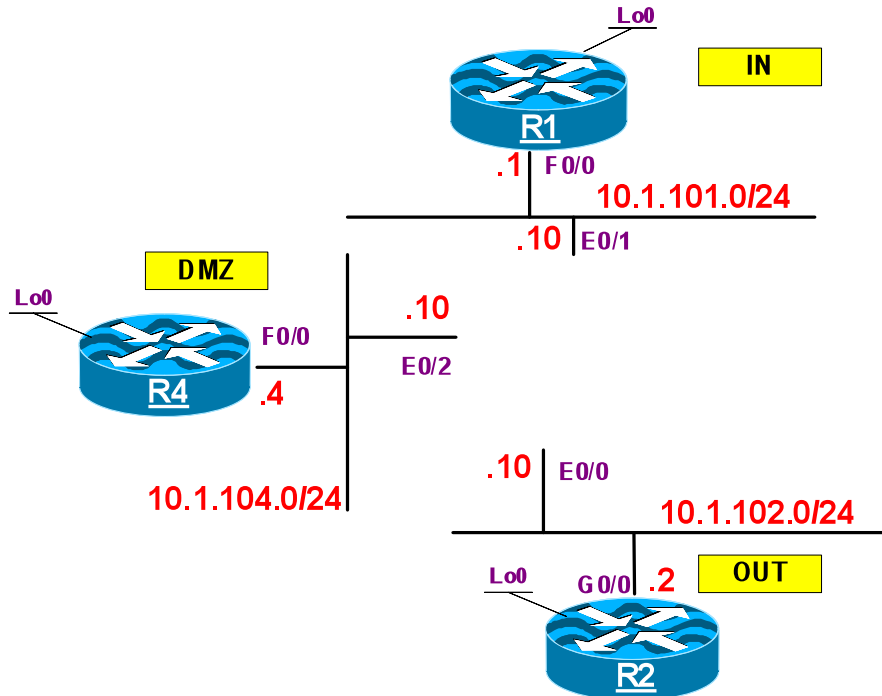
Line	User	Host(s)	Idle	Location
0 con 0		idle	00:10:50	
*514 vty 0		idle	00:00:00	4.4.4.4

Interface	User	Mode	Idle	Peer Address

R1>exit

[Connection to 10.1.104.1 closed by foreign host]

Lab 1.9. Dynamic Policy NAT (8.2)



This lab is based on ASA 8.2 software version. Make sure you downgrade the ASA code to that version before continuing. Required files should be on flash.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the following commands:

```
clear configure static
clear configure access-list
```

Task 1

Ensure all packets need to be translated in order to pass through the ASA. Configure ASA so that it dynamically translates source IP addresses of telnet traffic going between 1.1.1.1 and 2.2.2.2. Use ASA's outside IP address as a global address.



First, configure NAT Control feature to ensure all packets must be translated to pass through ASA. There is a requirement for using dynamic translation, which means we should look at NAT/GLOBAL configuration. Another important thing is that we need translate only packets for specific flows (between two hosts). This should lead us to the final solution that is Dynamic NAT with ACL (called Policy DNAT).

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat-control
ASA-FW(config)# access-list DYNA-NAT permit tcp host 1.1.1.1 host
2.2.2.2 eq telnet
ASA-FW(config)# nat (IN) 1 access-list DYNA-NAT
ASA-FW(config)# global (OUT) 1 interface
INFO: OUT interface address added to PAT pool
```

Verification

```
R1#tel 10.1.102.2
Trying 10.1.102.2 ...
% Connection refused by remote host
```

```
R1#tel 10.1.102.2 /so lo0
Trying 10.1.102.2 ...
% Connection refused by remote host
```

```
R1#tel 2.2.2.2
Trying 2.2.2.2 ...
% Connection refused by remote host
```

All connections are denied by the NAT Control function on the ASA.

```
R1#tel 2.2.2.2 /so lo0
```

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:12:57	
*578 vty 0		idle	00:00:00	10.1.102.10

Interface	User	Mode	Idle	Peer Address

Note that you can't connect from other IP addresses as there is no translation rule in place (and NAT Control is enabled). After establishing telnet session between R1 and R2 do not disconnect to see XLATE on the ASA.

ASA-FW(config)# sh xlate

1 in use, 4 most used

PAT Global 10.1.102.10(23407) Local 1.1.1.1(53426)

ASA-FW(config)# sh xlate detail

1 in use, 4 most used

Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,

r - portmap, s - static

TCP PAT from IN:1.1.1.1/53426 to OUT(DYNA-NAT):10.1.102.10/23407 flags ri

Task 2

Configure ASA so that it translates source IP addresses for traffic going between inside subnet (10.1.101.0/24) and outside subnet (10.1.102.0/24). Use dynamic address pool of 10.1.102.100-200 and ensure it will be backed up by IP address of 10.1.102.201 in case the pool is exhausted.



This task is very similar to the previous one. The difference is we need to dynamically translate whole inside subnet to some IP address pool. In addition to that we should back up this pool with one IP address. Remember that you can also use ASA's outside interface as a backup.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# access-list DYNA-NAT2 permit ip 10.1.101.0
255.255.255.0 10.1.102.0 255.255.255.0

ASA-FW(config)# nat (IN) 2 access-list DYNA-NAT2

ASA-FW(config)# global (OUT) 2 10.1.102.100-10.1.102.200 netmask
255.255.255.0
ASA-FW(config)# global (OUT) 2 10.1.102.201 netmask 255.255.255.255
INFO: Global 10.1.102.201 will be Port Address Translated
```

Verification

R1#tel 2.2.2.2

Trying 2.2.2.2 ...
% Connection refused by remote host

R1#tel 10.1.102.2 /so lo0

Trying 10.1.102.2 ...
% Connection refused by remote host

R1#tel 10.1.102.2

Trying 10.1.102.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:17:45	
*578 vty 0		idle	00:00:00	10.1.102.196

Note there is a random IP address from the pool.

Interface	User	Mode	Idle	Peer Address

ASA-FW(config)# sh xlate

1 in use, 4 most used

Global 10.1.102.196 Local 10.1.101.1

ASA-FW(config)# sh xlate detail

1 in use, 4 most used

Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
r - portmap, s - static

NAT from IN:10.1.101.1 to OUT(DYNA-NAT2):10.1.102.196 flags i

Note that using dynamic translation we can initiate communication from only one direction. In above example we couldn't initiate telnet session from R2 to R1 even though we had inbound ACL on ASA's outside interface configured.

Task 3

Configure ASA so that it translates source IP address for traffic initiated from 1.1.1.1 and destined to 4.4.4.4. Use IP address 10.1.104.1 for this translation.



Here, we are requested for dynamic PAT configuration for traffic between R1's loopback0 and R4's loopback0 interface. Note that the task is very specific and it clearly states that traffic should be initiated from R1. This means we need to use dynamic translation.

Be careful and check what translation IDs you have configured to ensure you won't overwrite or add next NAT statement to the previously configured NAT rule instead of adding new NAT statement. Also, watch out what interfaces you use for NAT and GLOBAL statements.

Remember that you should configure ONLY what you've asked for. Do not configure inbound ACL on DMZ interface in this task as this is not necessary.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# access-list DYNA-NAT3 permit ip host 1.1.1.1 host
4.4.4.4

ASA-FW(config)# nat (IN) 3 access-list DYNA-NAT3
ASA-FW(config)# global (DMZ) 3 10.1.104.1 netmask 255.255.255.255
INFO: Global 10.1.104.1 will be Port Address Translated
```

Verification

```
R1#tel 4.4.4.4
Trying 4.4.4.4 ...
% Connection refused by remote host
```

```
R1#tel 4.4.4.4 /so lo0
Trying 4.4.4.4 ... Open
```

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:17:01	
*514 vty 0		idle	00:00:00	10.1.104.1

Interface	User	Mode	Idle	Peer Address

ASA-FW(config)# sh xlate

2 in use, 4 most used

PAT Global 10.1.104.1(31496) Local 1.1.1.1(63820)

Global 10.1.102.196 Local 10.1.101.1

ASA-FW(config)# sh xlate detail

2 in use, 4 most used

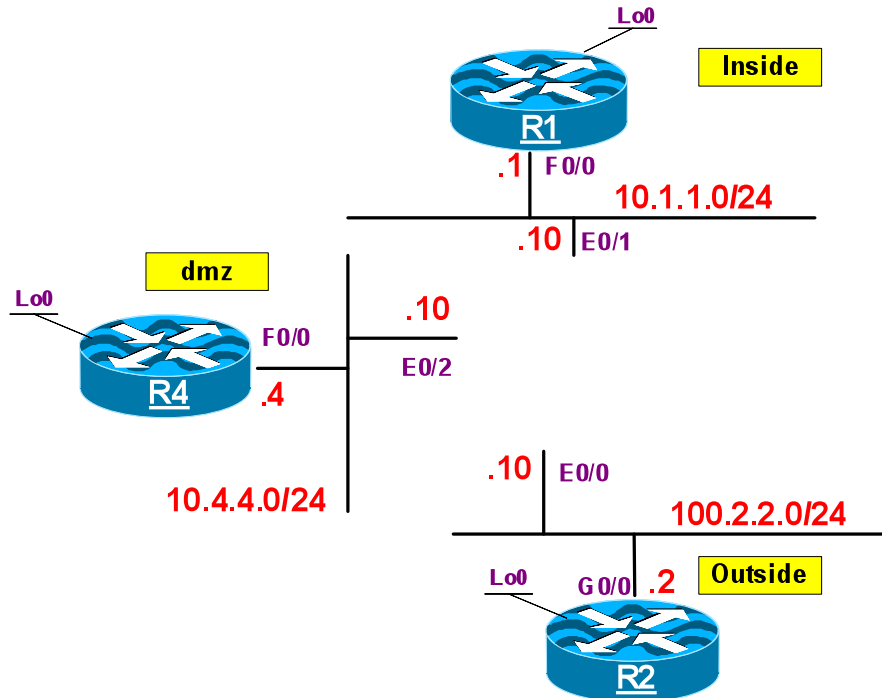
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,

r - portmap, s - static

TCP PAT from IN:1.1.1.1/63820 to DMZ(DYNA-NAT3):10.1.104.1/31496 flags ri

NAT from IN:10.1.101.1 to OUT(DYNA-NAT2):10.1.102.196 flags i

Lab 1.10. Static NAT (8.3+)



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 10
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 20
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 40
- Configure Telnet on all routers using password "cisco"
- Configure default routes on R1/R2 and R4 to point to ASA and static routes to reach router's loopbacks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.1.1/24
R2	Lo0	2.2.2.2/24
	G0/0	100.2.2.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.4.4.4/24
ASA1	E0/0	100.2.2.10/24
	E0/1	10.1.1.10/24
	E0/2	10.4.4.10/24

Task 1

Configure ASA so that when someone from the outside (network segment behind ASA's OUTSIDE interface) tries to connect to IP address of 100.2.2.99 he/she will be pointed to R1's loopback0 interface. Limit the embryonic connections for hosts using that connection to 2 and full connections to 10 per host.



This is new NAT scenario. You must have at least 8.3(1) software version installed on the ASA.

The following commands are no longer supported in 8.3+

- *nat-control*
- *static*
- *global*

Piggybacked options such as max connection, TCP sequence number randomization, embryonic connection and nailed are migrated to MPF.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network R1-loopback
ASA(config-network-object)# host 1.1.1.1
ASA(config-network-object)# ex
ASA(config)# object network R1-loop-translated
ASA(config-network-object)# host 100.2.2.99
ASA(config-network-object)# ex
ASA(config)# object network R1-loopback
ASA(config-network-object)# nat (inside,outside) static R1-loop-
translated

ASA(config)# access-list OUTSIDE_IN permit ip any host 1.1.1.1
ASA(config)# access-group OUTSIDE_IN in interface outside

ASA(config)# route inside 1.1.1.1 255.255.255.255 10.1.1.1
ASA(config)# route outside 2.2.2.2 255.255.255.255 100.2.2.2
ASA(config)# route dmz 4.4.4.4 255.255.255.255 10.4.4.4

ASA(config)# access-list R1-LOOP extended permit tcp any host
1.1.1.1
ASA(config)# class-map CM-R1-LOOP
```

```
ASA(config-cmap)# match access-list R1-LOOP
ASA(config-cmap)# exit
ASA(config)# policy-map OUTSIDE-POLICY
ASA(config-pmap)# class CM-R1-LOOP
ASA(config-pmap-c)# set connection per-client-max 10 per-client-embryonic-max 2
ASA(config-pmap-c)# exit
ASA(config-pmap)# exit
ASA(config)# service-policy OUTSIDE-POLICY interface outside
```

Step 2 R1 configuration.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.10
```

Step 3 R2 configuration.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 100.2.2.10
```

Step 4 R4 configuration.

```
R4(config)# ip route 0.0.0.0 0.0.0.0 10.4.4.10
```

Verification

R2#tel 100.2.2.99

Trying 100.2.2.99 ... Open

User Access Verification

Password:

R1>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:21	
*514 vty 0		idle	00:00:00	100.2.2.2

Interface	User	Mode	Idle	Peer Address

R1>

ASA(config)# sh nat

Auto NAT Policies (Section 2)

```
1 (inside) to (outside) source static R1-loopback R1-loop-translated
  translate_hits = 0, untranslate_hits = 19
```

ASA(config)# sh conn det

```
1 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP outside:100.2.2.2/49617 inside:1.1.1.1/23,
  flags UIOB, idle 1m20s, uptime 1m25s, timeout 1h0m, bytes 403
```

ASA(config)# sh service-policy interface outside

```
Interface outside:
  Service-policy: OUTSIDE-POLICY
  Class-map: CM-R1-LOOP
    Set connection policy: per-client-max 10 per-client-embryonic-max 2
    current conns 3, drop 0
```

Task 2

Configure ASA so that when someone from the outside (network segment behind ASA's OUTSIDE interface) tries to connect to IP address of 100.2.2.4 using TELNET, he/she will be pointed to R4's f0/0 interface.



This task is similar to the previous however there is one difference. The translation must be used only for TELNET traffic. This is called Static PAT (Port Address Translation) and it's useful for "port redirection".

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network R4
ASA(config-network-object)# host 10.4.4.4
ASA(config-network-object)# nat (dmz,outside) static 100.2.2.4
service tcp 23 23

ASA(config)# access-list OUTSIDE_IN extended permit tcp any host
10.4.4.4 eq 23
```

Verification

R2#tel 100.2.2.4

Trying 100.2.2.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	1w4d	
*514 vty 0	piotr	idle	00:00:00	100.2.2.2

Interface	User	Mode	Idle	Peer Address

R4>

ASA(config)# sh nat

Auto NAT Policies (Section 2)

```
1 (inside) to (outside) source static R1-loopback R1-loop-translated
   translate_hits = 0, untranslate_hits = 31
2 (dmz) to (outside) source static R4 100.2.2.4 service tcp telnet telnet
   translate_hits = 0, untranslate_hits = 4
```

ASA(config)# sh conn det

1 in use, 3 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
 B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
 D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
 G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
 i - incomplete, J - GTP, j - GTP data, K - GTP t3-response

```
k - Skinny media, M - SMTP data, m - SIP media, n - GUP
O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
q - SQL*Net data, R - outside acknowledged FIN,
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
V - VPN orphan, W - WAAS,
X - inspected by service module
TCP outside:100.2.2.2/16851 dmz:10.4.4.4/23,
  flags UIOB, idle 44s, uptime 59s, timeout 1h0m, bytes 504
```

Task 3

Configure ASA so that when someone from the outside (network segment behind ASA's OUTSIDE interface) tries to connect to ASA's outside interface using port 2323, he/she will be redirected to R1's F0/0 interface using port 23.



This task is similar to the previous however in this case the ASA must “listen” on its outside interface on port 2323 and “redirect” all traffic coming to that interface/port to the IP address of R1's F0/0 interface and port 23.

Note that you still need an ACL entry on the outside interface for those connections.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network R1
ASA(config-network-object)# host 10.1.1.1
ASA(config-network-object)# nat (inside,outside) static interface
service tcp 23 2323

ASA(config)# access-list OUTSIDE_IN extended permit tcp any host
10.1.1.1 eq 23
```

Note that you must configure Real IP address and Real Port number in the outside ACL.

Verification

R2#tel 100.2.2.10 2323

Trying 100.2.2.10, 2323 ... Open

User Access Verification

Password:

R1>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:40:49	
*514 vty 0		idle	00:00:00	100.2.2.2

Interface	User	Mode	Idle	Peer Address

R1>

ASA(config)# sh nat

Auto NAT Policies (Section 2)

```

1 (inside) to (outside) source static R1-loopback R1-loop-translated
   translate_hits = 0, untranslate_hits = 31
2 (inside) to (outside) source static R1 interface service tcp telnet 2323
   translate_hits = 0, untranslate_hits = 1
3 (dmz) to (outside) source static R4 100.2.2.4 service tcp telnet telnet
   translate_hits = 0, untranslate_hits = 4

```

ASA(config)# sh conn det

1 in use, 3 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
 B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
 D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
 G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
 i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
 k - Skinny media, M - SMTP data, m - SIP media, n - GUP
 O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
 q - SQL*Net data, R - outside acknowledged FIN,
 R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
 s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
 V - VPN orphan, W - WAAS,
 X - inspected by service module

TCP outside:100.2.2.2/57249 inside:10.1.1.1/23,
 flags UIOB, idle 1m22s, uptime 1m27s, timeout 1h0m, bytes 382

Task 4

Configure ASA so that it statically translates R1's loopback0 IP address to its outside interface's IP address. The translation must be enforced only for traffic going between R1's loopback0 and R2's loopback0 interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network R2-loopback
ASA(config-network-object)# host 2.2.2.2
ASA(config-network-object)# ext

ASA(config)# nat (inside,outside) source static R1-loopback
interface destination R2-loopback R2-loopback
WARNING: All traffic destined to the IP address of the outside
interface is being redirected.
WARNING: Users may not be able to access any service enabled on the
outside interface.
```

Verification

R1#tel 2.2.2.2

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:21:21	
*706 vty 0		idle	00:00:00	10.1.1.1

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

R1#tel 2.2.2.2 /so lo0

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:21:32	
*706 vty 0		idle	00:00:00	100.2.2.10

Interface	User	Mode	Idle	Peer Address

R2>

ASA(config)# sh nat

Manual NAT Policies (Section 1)

```
1 (inside) to (outside) source static R1-loopback interface destination static R2-
loopback R2-loopback
    translate_hits = 1, untranslate_hits = 0
```

Auto NAT Policies (Section 2)

```
1 (inside) to (outside) source static R1-loopback R1-loop-translated
    translate_hits = 0, untranslate_hits = 31
2 (inside) to (outside) source static R1 interface service tcp telnet 2323
    translate_hits = 0, untranslate_hits = 1
3 (dmz) to (outside) source static R4 100.2.2.4 service tcp telnet telnet
    translate_hits = 0, untranslate_hits = 4
```

Note that now the translation is going to Manual NAT section and will be triggered first.

ASA(config)# sh conn det

1 in use, 3 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
 B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
 D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
 G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
 i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
 k - Skinny media, M - SMTP data, m - SIP media, n - GUP
 O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
 q - SQL*Net data, R - outside acknowledged FIN,
 R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
 s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
 V - VPN orphan, W - WAAS,
 X - inspected by service module

TCP outside:2.2.2.2/23 inside:1.1.1.1/64664,

flags UIO, idle 47s, uptime 52s, timeout 1h0m, bytes 408

Task 5

Configure ASA so that it statically translates to the IP address of 10.5.5.1 all traffic coming from R1's loopback0 interface towards DMZ subnet. The translation rule should be used only for traffic originated from 1.1.1.1 and destined to 4.4.4.4.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network R4-loopback
ASA(config-network-object)# host 4.4.4.4
ASA(config-network-object)# ext
ASA(config)# object network R1-R4-NAT
ASA(config-network-object)# host 10.5.5.1
ASA(config-network-object)# ext
ASA(config)# nat (inside,dmz) source static R1-loopback R1-R4-NAT
destination static R4-loopback R4-loopback
```

Verification

R1#tel 4.4.4.4

Trying 4.4.4.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	1w4d	
*514 vty 0	piotr	idle	00:00:00	10.1.1.1

Interface	User	Mode	Idle	Peer Address

R4>ext

[Connection to 4.4.4.4 closed by foreign host]

R1#tel 4.4.4.4 /so lo0

Trying 4.4.4.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	1w4d	
*514 vty 0	piotr	idle	00:00:00	10.5.5.1

Interface	User	Mode	Idle	Peer Address

R4>

Task 6

Configure static translation on ASA so that when R2 telnets to the IP address of 100.2.2.11 port tcp/2323 using its loopback0 interface as a source it will be automatically redirected to the host 1.1.1.1 port tcp/23. This translation rule should work only for traffic initiated from R2's loopback0 interface and destined to 100.2.2.11.



This task requires "port redirection" but only for traffic between two hosts.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object service PORT-2323
ASA(config-service-object)# service tcp source eq 2323
ASA(config)# object service PORT-23
ASA(config-service-object)# service tcp source eq telnet
ASA(config)# object network R1-R2-NAT
ASA(config-network-object)# host 100.2.2.11

ASA(config)# nat (inside,outside) source static R1-loopback R1-R2-
NAT destination static R2-loopback R2-loopback service PORT-23
PORT-2323
```

Verification

R2#tel 100.2.2.11 2323

Trying 100.2.2.11, 2323 ...

% Connection timed out; remote host not responding

R2#tel 100.2.2.11 2323 /so lo0

Trying 100.2.2.11, 2323 ... Open

User Access Verification

Password:

R1>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:13:37	
*514 vty 0		idle	00:00:00	2.2.2.2

Interface	User	Mode	Idle	Peer Address

R1>

ASA(config)# sh nat

Manual NAT Policies (Section 1)

1 (inside) to (outside) source static R1-loopback interface destination static R2-loopback R2-loopback

translate_hits = 1, untranslate_hits = 0

2 (inside) to (dmz) source static R1-loopback R1-R4-NAT destination static R4-loopback R4-loopback

translate_hits = 1, untranslate_hits = 0

3 (inside) to (outside) source static R1-loopback R1-R2-NAT destination static R2-loopback R2-loopback service PORT-23 PORT-2323

translate_hits = 0, untranslate_hits = 1

Auto NAT Policies (Section 2)

1 (inside) to (outside) source static R1-loopback R1-loop-translated

translate_hits = 0, untranslate_hits = 31

2 (inside) to (outside) source static R1 interface service tcp telnet 2323

translate_hits = 0, untranslate_hits = 1

3 (dmz) to (outside) source static R4 100.2.2.4 service tcp telnet telnet

translate_hits = 0, untranslate_hits = 4

ASA(config)# sh conn det

1 in use, 3 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
 B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
 D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
 G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
 i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
 k - Skinny media, M - SMTP data, m - SIP media, n - GUP
 O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
 q - SQL*Net data, R - outside acknowledged FIN,
 R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
 s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
 V - VPN orphan, W - WAAS,
 X - inspected by service module

TCP outside:2.2.2.2/13444 inside:1.1.1.1/23,
 flags UIOB, idle 33s, uptime 38s, timeout 1h0m, bytes 380

Task 7

Configure ASA so that it statically translate all hosts from the inside network (10.1.1.0/24) to addresses on the 10.11.11.0/24 network making them all accessible from DMZ.



This type of NAT is useful when we want to make two networks fully accessible for each other. We need to translate whole network to another network and allow traffic to be originated from the subnet behind lower security level interface by configuring inbound ACL.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network NET-10.1.1.0
ASA(config-network-object)# subnet 10.1.1.0 255.255.255.0
ASA(config-network-object)# ex
ASA(config)# object network NET-10.11.11.0
ASA(config-network-object)# subnet 10.11.11.0 255.255.255.0
ASA(config-network-object)# ex

ASA(config)# object network NET-10.1.1.0
ASA(config-network-object)# nat (inside,dmz) static NET-10.11.11.0
```

```
ASA(config)# access-li DMZ_IN permit ip 10.4.4.0 255.255.255.0
10.1.1.0 255.255.255.0
ASA(config)# access-group DMZ_IN in int dmz
```

Verification

R4#tel 10.1.1.1

Trying 10.1.1.1 ...

% Connection timed out; remote host not responding

R4#tel 10.11.11.1

Trying 10.11.11.1 ... Open

User Access Verification

Password:

R1>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:24:41	
*514 vty 0		idle	00:00:00	10.4.4.4

Interface	User	Mode	Idle	Peer Address

R1>

ASA(config)# sh nat

Manual NAT Policies (Section 1)

1 (inside) to (outside) source static R1-loopback interface destination static R2-loopback R2-loopback

translate_hits = 1, untranslate_hits = 0

2 (inside) to (dmz) source static R1-loopback R1-R4-NAT destination static R4-loopback R4-loopback

translate_hits = 1, untranslate_hits = 0

3 (inside) to (outside) source static R1-loopback R1-R2-NAT destination static R2-loopback R2-loopback service PORT-23 PORT-2323

translate_hits = 0, untranslate_hits = 1

Auto NAT Policies (Section 2)

1 (inside) to (outside) source static R1-loopback R1-loop-translated

translate_hits = 0, untranslate_hits = 31

2 (inside) to (outside) source static R1 interface service tcp telnet 2323

translate_hits = 0, untranslate_hits = 1

3 (dmz) to (outside) source static R4 100.2.2.4 service tcp telnet telnet

```
translate_hits = 0, untranslate_hits = 4
4 (inside) to (dmz) source static NET-10.1.1.0 NET-10.11.11.0
translate_hits = 0, untranslate_hits = 1
```

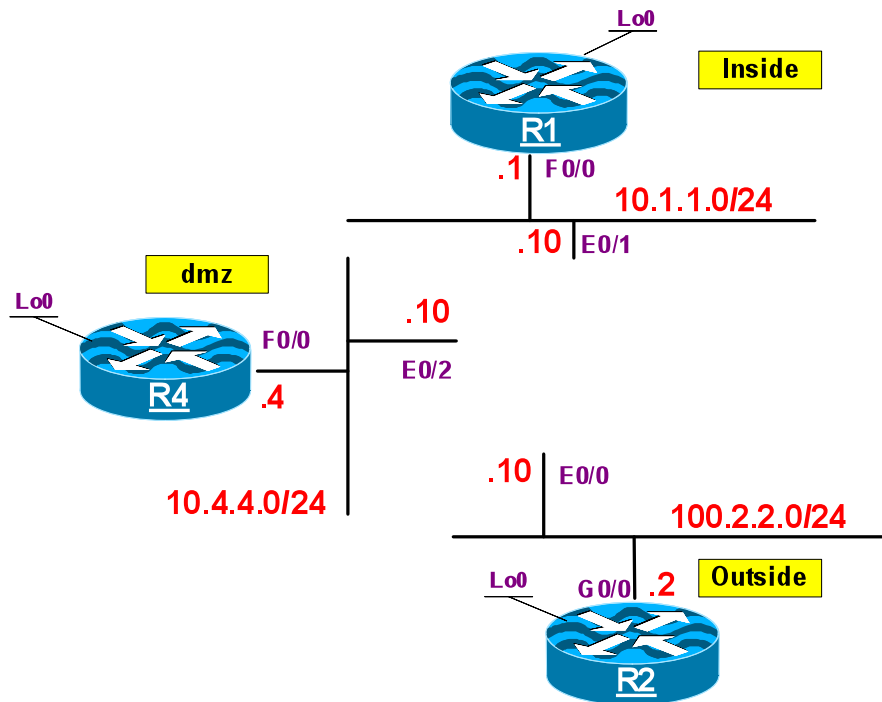
ASA(config)# sh conn det

1 in use, 3 most used

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, M - SMTP data, m - SIP media, n - GUP
O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
q - SQL*Net data, R - outside acknowledged FIN,
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
V - VPN orphan, W - WAAS,
X - inspected by service module

TCP dmz:10.4.4.4/18331 inside:10.1.1.1/23,
flags UIOB, idle 42s, uptime 46s, timeout 1h0m, bytes 402

Lab 1.11. Dynamic NAT (8.3+)



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 10
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 20
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 40
- Configure Telnet on all routers using password "cisco"
- Configure default routes on R1/R2 and R4 to point to ASA and static routes to reach router's loopbacks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.1.1/24
R2	Lo0	2.2.2.2/24
	G0/0	100.2.2.2/24

R4	Lo0 F0/0	4.4.4.4/24 10.4.4.4/24
ASA1	E0/0 E0/1 E0/2	100.2.2.10/24 10.1.1.10/24 10.4.4.10/24

Before you start

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the following commands:

```
clear configure nat
clear configure access-list
```

Task 1

Configure ASA so that when any IP address from DMZ tries to go outside packets will be translated to an IP address of 100.2.2.99.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network ANYNET
ASA(config-network-object)# subnet 0.0.0.0 0.0.0.0
ASA(config-network-object)# nat (dmz,outside) dynamic 100.2.2.99
ASA(config-network-object)# exi
```

Verification

```
R4#tel 100.2.2.2
Trying 100.2.2.2 ... Open
```

User Access Verification

Password:

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	13:43:04	

```
*706 vty 0          idle          00:00:00 100.2.2.99
```

Interface	User	Mode	Idle	Peer Address

```
R2>exit
```

```
[Connection to 100.2.2.2 closed by foreign host]
```

R4#tel 100.2.2.2 /so 1o0

```
Trying 100.2.2.2 ... Open
```

User Access Verification

```
Password:
```

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	13:43:16	
*706 vty 0		idle	00:00:00	100.2.2.99

Interface	User	Mode	Idle	Peer Address

```
R2>
```

ASA(config)# sh nat det

Auto NAT Policies (Section 2)

```
1 (dmz) to (outside) source dynamic ANYNET 100.2.2.99
```

```
translate_hits = 2, untranslate_hits = 0
```

```
Source - Origin: 0.0.0.0/0, Translated: 100.2.2.99/32
```

ASA(config)# sh conn det

```
1 in use, 3 most used
```

```
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
```

```
B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
```

```
D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
```

```
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
```

```
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
```

```
k - Skinny media, M - SMTP data, m - SIP media, n - GUP
```

```
O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
```

```
q - SQL*Net data, R - outside acknowledged FIN,
```

```
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
```

```
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
```

```
V - VPN orphan, W - WAAS,
```

```
X - inspected by service module
```

```
TCP outside:100.2.2.2/23 dmz:4.4.4.4/31078,
```

```
flags UIO, idle 41s, uptime 45s, timeout 1h0m, bytes 404
```

```
ASA(config)# sh xlate
```

```
1 in use, 7 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
TCP PAT from dmz:4.4.4.4/31078 to outside:100.2.2.99/57571 flags ri idle 0:01:04
```

```
timeout 0:00:30
```

Task 2

Configure ASA so that when R4 tries to initiate a session from its loopback IP address, the connection is not translated.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network R4-loopback
```

```
ASA(config-network-object)# host 4.4.4.4
```

```
ASA(config-network-object)# exi
```

```
ASA(config)# nat (dmz,outside) source static R4-loopback R4-  
loopback
```

Note that there is no Identity NAT in ASA 8.3+ Instead,
there is Manual NAT entry for 'exempt' static.

Verification

```
R4#tel 100.2.2.2
```

```
Trying 100.2.2.2 ... Open
```

User Access Verification

Password:

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	13:57:18	
*706 vty 0		idle	00:00:00	100.2.2.99

Interface	User	Mode	Idle	Peer Address

```
R2>exit
```

```
[Connection to 100.2.2.2 closed by foreign host]
```

```
R4#tel 100.2.2.2 /so 1o0
```

```
Trying 100.2.2.2 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	13:57:28	
*706 vty 0		idle	00:00:00	4.4.4.4

Interface	User	Mode	Idle	Peer Address

```
R2>
```

```
ASA(config)# sh nat
```

```
Manual NAT Policies (Section 1)
```

```
1 (dmz) to (outside) source static R4-loopback R4-loopback
    translate_hits = 1, untranslate_hits = 0
```

```
Auto NAT Policies (Section 2)
```

```
1 (dmz) to (outside) source dynamic ANYNET 100.2.2.99
    translate_hits = 3, untranslate_hits = 0
```

```
ASA(config)# sh xlate
```

```
2 in use, 7 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
NAT from dmz:4.4.4.4 to outside:4.4.4.4
```

```
    flags sI idle 0:07:51 timeout 0:00:00
```

```
TCP PAT from dmz:10.4.4.4/31441 to outside:100.2.2.99/8106 flags ri idle 0:00:29
    timeout 0:00:30
```

Task 3

Configure ASA so that all IP addresses from the inside subnet (10.1.1.0/24) will be translated to the dynamic pool of 100.2.2.100 – 100.2.2.200. If the pool is exhausted, configure ASA to perform dynamic port translation using IP address of 100.2.2.201.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network NAT-RANGE
ASA(config-network-object)# range 100.2.2.100 100.2.2.200
ASA(config-network-object)# exi
ASA(config)# object network PAT
ASA(config-network-object)# host 100.2.2.201
ASA(config-network-object)# exi
ASA(config)# object-group network NAT-PAT-GROUP
ASA(config-network-object-group)# network-object object NAT-RANGE
ASA(config-network-object-group)# network-object object PAT
ASA(config-network-object-group)# exi
ASA(config)# object network NET-10.1.1.0
ASA(config-network-object)# subnet 10.1.1.0 255.255.255.0
ASA(config-network-object)# nat (inside,outside) dynamic NAT-PAT-
GROUP
ASA(config-network-object)# exi
```

Verification

R1#tel 100.2.2.2

Trying 100.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	14:13:00	
*706 vty 0		idle	00:00:00	100.2.2.187

Interface	User	Mode	Idle	Peer Address

R2>

ASA(config)# sh nat det

Manual NAT Policies (Section 1)

```
1 (dmz) to (outside) source static R4-loopback R4-loopback
  translate_hits = 1, untranslate_hits = 0
  Source - Origin: 4.4.4.4/32, Translated: 4.4.4.4/32
```

Auto NAT Policies (Section 2)

```

1 (inside) to (outside) source dynamic NET-10.1.1.0 NAT-PAT-GROUP
  translate_hits = 3, untranslate_hits = 0
  Source - Origin: 10.1.1.0/24, Translated: 100.2.2.100/30, 100.2.2.104/29,
100.2.2.112/28, 100.2.2.128/26
  100.2.2.192/29, 100.2.2.200/32, 100.2.2.201/32
2 (dmz) to (outside) source dynamic ANYNET 100.2.2.99
  translate_hits = 3, untranslate_hits = 0
  Source - Origin: 0.0.0.0/0, Translated: 100.2.2.99/32

```

ASA(config)# sh xlate

```

2 in use, 7 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from dmz:4.4.4.4 to outside:4.4.4.4
  flags sI idle 0:23:24 timeout 0:00:00
NAT from inside:10.1.1.1 to outside:100.2.2.187 flags i idle 0:04:10 timeout 3:00:00

```

Task 4

Configure ASA so that when R1 tries to communicate with hosts in DMZ using its loopback0 interface as a source, it will be dynamically translated to ASA's DMZ interface IP address.

Configuration

Complete these steps:

Step 1 ASA configuration.

```

ASA(config)# object network R1-loopback
ASA(config-network-object)# host 1.1.1.1
ASA(config-network-object)# nat (inside,dmz) dynamic interface
ASA(config-network-object)# exi

```

Verification

R1#tel 10.4.4.4

```
Trying 10.4.4.4 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R4>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:20:17	
*514 vty 0	piotr	idle	00:00:00	10.1.1.1

Interface	User	Mode	Idle	Peer Address

```
R4>exit
```

[Connection to 10.4.4.4 closed by foreign host]

R1#tel 10.4.4.4 /so lo0

Trying 10.4.4.4 ... Open

User Access Verification

Password:

```
R4>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:20:33	
*514 vty 0	piotr	idle	00:00:00	10.4.4.10

Interface	User	Mode	Idle	Peer Address

```
R4>
```

ASA(config)# sh nat det

Manual NAT Policies (Section 1)

```
1 (dmz) to (outside) source static R4-loopback R4-loopback
   translate_hits = 1, untranslate_hits = 0
   Source - Origin: 4.4.4.4/32, Translated: 4.4.4.4/32
```

Auto NAT Policies (Section 2)

```
1 (inside) to (dmz) source dynamic R1-loopback interface
   translate_hits = 1, untranslate_hits = 0
   Source - Origin: 1.1.1.1/32, Translated: 10.4.4.10/24
2 (inside) to (outside) source dynamic NET-10.1.1.0 NAT-PAT-GROUP
   translate_hits = 3, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 100.2.2.100/30, 100.2.2.104/29,
100.2.2.112/28, 100.2.2.128/26
   100.2.2.192/29, 100.2.2.200/32, 100.2.2.201/32
3 (dmz) to (outside) source dynamic ANYNET 100.2.2.99
   translate_hits = 3, untranslate_hits = 0
   Source - Origin: 0.0.0.0/0, Translated: 100.2.2.99/32
```

ASA(config)# sh xlate

```
3 in use, 7 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from dmz:4.4.4.4 to outside:4.4.4.4
      flags sI idle 0:28:24 timeout 0:00:00
TCP PAT from inside:1.1.1.1/35710 to dmz:10.4.4.10/32704 flags ri idle 0:00:23 timeout
0:00:30
NAT from inside:10.1.1.1 to outside:100.2.2.187 flags i idle 0:09:10 timeout 3:00:00
```

Task 5

Configure ASA so that when R1 tries to communicate with hosts on the outside network using its loopback0 interface as a source, it will be dynamically translated to IP address of 100.2.2.202. Do not broke your previous configuration.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network PAT-202
ASA(config-network-object)# host 100.2.2.202
ASA(config-network-object)# ext
ASA(config)# nat (inside,outside) source dynamic R1-loopback PAT-
202
```

Note that you cannot add second NAT statement under the object. You must use Manual NAT configuration to accomplish this task.

Verification

```
R1#tel 100.2.2.2
Trying 100.2.2.2 ... Open
```

User Access Verification

Password:

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	21:00:37	
*706 vty 0		idle	00:00:00	100.2.2.176

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 100.2.2.2 closed by foreign host]

R1#tel 100.2.2.2 /so lo0

Trying 100.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	21:01:25	
*706 vty 0		idle	00:00:00	100.2.2.202

Interface	User	Mode	Idle	Peer Address

R2>

ASA(config)# sh nat det

Manual NAT Policies (Section 1)

1 (dmz) to (outside) source static R4-loopback R4-loopback
translate_hits = 1, untranslate_hits = 0
Source - Origin: 4.4.4.4/32, Translated: 4.4.4.4/32

2 (inside) to (outside) source dynamic R1-loopback PAT-202
translate_hits = 2, untranslate_hits = 0
Source - Origin: 1.1.1.1/32, Translated: 100.2.2.202/32

Auto NAT Policies (Section 2)

1 (inside) to (dmz) source dynamic R1-loopback interface
translate_hits = 0, untranslate_hits = 0
Source - Origin: 1.1.1.1/32, Translated: 10.4.4.10/24

2 (inside) to (outside) source dynamic NET-10.1.1.0 NAT-PAT-GROUP
translate_hits = 5, untranslate_hits = 0
Source - Origin: 10.1.1.0/24, Translated: 100.2.2.100/30, 100.2.2.104/29,
100.2.2.112/28, 100.2.2.128/26
100.2.2.192/29, 100.2.2.200/32, 100.2.2.201/32

3 (dmz) to (outside) source dynamic ANYNET 100.2.2.99
translate_hits = 3, untranslate_hits = 0
Source - Origin: 0.0.0.0/0, Translated: 100.2.2.99/32

ASA(config)# sh xlate

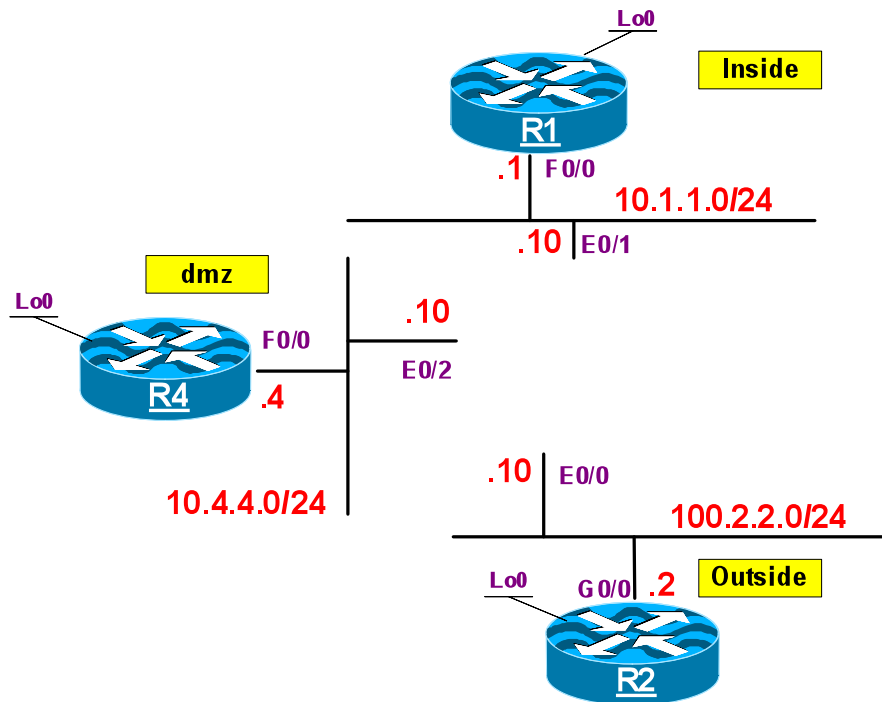
4 in use, 7 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

NAT from dmz:4.4.4.4 to outside:4.4.4.4

```
flags sI idle 7:11:51 timeout 0:00:00
TCP PAT from inside:1.1.1.1/58640 to outside:100.2.2.202/7235 flags ri idle 0:00:20
timeout 0:00:30
NAT from inside:10.1.1.1 to outside:100.2.2.176 flags i idle 0:01:40 timeout 3:00:00
```

Lab 1.12. Bidirectional NAT (8.3+)



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 10
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 20
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 40
- Configure Telnet on all routers using password "cisco"
- Configure default routes on R1/R2 to point to ASA and static routes to reach router's loopbacks
- Do NOT configure static default route on R4

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.11.1/24
R2	Lo0	2.2.2.2/24

	G0/0	100.2.2.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.4.4.4/24
ASA1	E0/0	100.2.2.10/24
	E0/1	10.1.1.10/24
	E0/2	10.4.4.10/24

Before you start

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the following commands:

```
clear configure nat
clear configure access-list
```

Task 1

For security reasons R4 has no default route configured. Configure ASA to redirect all TCP/23 traffic from the outside destined to IP address of 100.2.2.44 to router R4 f0/0 interface. Do not configure default route on R4 to accomplish this task.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# object network R4
ASA(config-network-object)# host 10.4.4.4
ASA(config-network-object)# nat (dmz,outside) static 100.2.2.44
ASA(config-network-object)# exit

ASA(config)# object network ANYNET
ASA(config-network-object)# subnet 0.0.0.0 0.0.0.0
ASA(config-network-object)# nat (outside,dmz) dynamic interface

ASA(config)# access-list OUTSIDE_IN permit tcp any host 10.4.4.4 eq
23
ASA(config)# access-group OUTSIDE_IN in int outside
```

This is called Bidir NAT because we're translating packet SRC and DST at the same time.
It works as expected, however it is not recommended to use

that method as the ASA must do two NAT lookups to translate the packet. It's simply not efficient.

Verification

R2#tel 100.2.2.44

Trying 100.2.2.44 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:06:22	
*514 vty 0	piotr	idle	00:00:00	10.4.4.10

Interface	User	Mode	Idle	Peer Address

R4>

ASA(config)# sh nat det

Auto NAT Policies (Section 2)

```
1 (dmz) to (outside) source static R4 100.2.2.44
   translate_hits = 0, untranslate_hits = 1
   Source - Origin: 10.4.4.4/32, Translated: 100.2.2.44/32
2 (outside) to (dmz) source dynamic ANYNET interface
   translate_hits = 1, untranslate_hits = 0
   Source - Origin: 0.0.0.0/0, Translated: 10.4.4.10/24
```

ASA(config)# sh xlate

3 in use, 7 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

NAT from dmz:10.4.4.4 to outside:100.2.2.44

flags s idle 0:01:01 timeout 0:00:00

TCP PAT from outside:100.2.2.2/48411 to dmz:10.4.4.10/51855 flags ri idle 0:01:01
timeout 0:00:30

Another method (preferred) is called Twice NAT and requires only one lookup and one translation rule. Let's clear previous NAT config and try again.

Configuration

Complete these steps:

Step 2 ASA configuration.

```
clear configure nat

ASA(config)# object network R4-NAT
ASA(config-network-object)# host 100.2.2.44
ASA(config-network-object)# exit
ASA(config)# object network ANYNET
ASA(config-network-object)# subnet 0.0.0.0 0.0.0.0
ASA(config-network-object)# exit
ASA(config)# object network R4
ASA(config-network-object)# host 10.4.4.4
ASA(config-network-object)# exit

ASA(config)# nat (outside,dmz) source dynamic ANYNET interface
destination static R4-NAT R4
```

Verification

R2#tel 100.2.2.44

Trying 100.2.2.44 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:17:27	
*514 vty 0	piotr	idle	00:00:00	10.4.4.10

Interface	User	Mode	Idle	Peer Address

R4>

ASA(config)# sh nat det

Manual NAT Policies (Section 1)

```
1 (outside) to (dmz) source dynamic ANYNET interface destination static R4-NAT R4
translate_hits = 1, untranslate_hits = 1
```

```
Source - Origin: 0.0.0.0/0, Translated: 10.4.4.10/24
```

```
Destination - Origin: 100.2.2.44/32, Translated: 10.4.4.4/32
```

```
ASA(config)# sh xlate
```

```
2 in use, 7 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
NAT from dmz:10.4.4.4 to outside:100.2.2.44
```

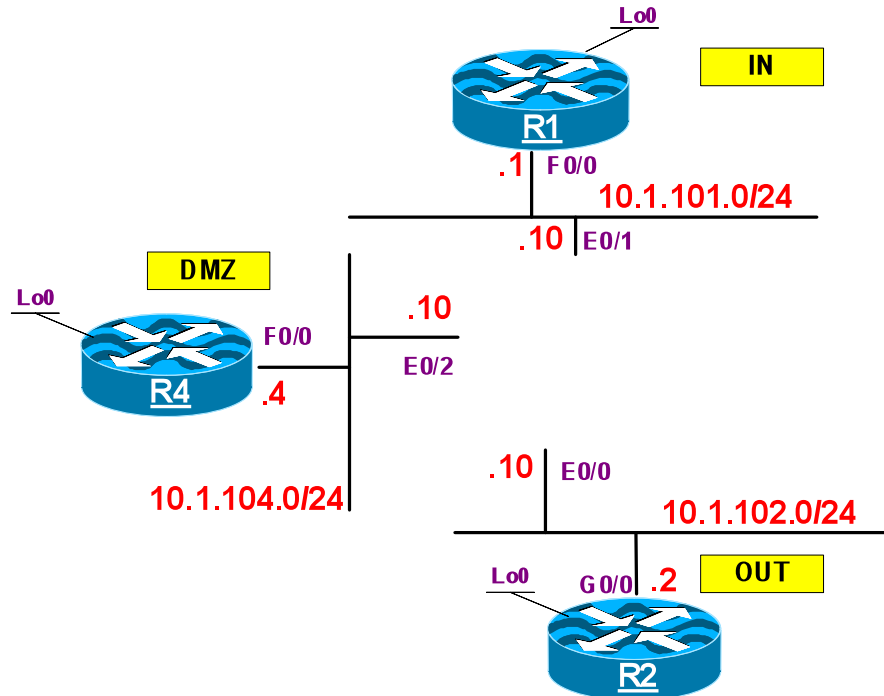
```
flags sT idle 0:00:23 timeout 0:00:00
```

```
TCP PAT from outside:100.2.2.2/17245 to dmz:10.4.4.10/50587 flags ri idle 0:00:23
```

```
timeout 0:00:30
```

Note that we have only one NAT rule configured but it creates two xlates where the static one is 'T - Twice'.

Lab 1.13. Modular Policy Framework (MPF)



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the following commands:

```
clear configure nat
clear configure nat-control
clear configure global
clear configure access-list
```

Task 1

Configure ASA so that it inspects HTTP and ICMP in order to pass that type of traffic in secure manner. All inbound packets traversing ASA secure appliance should be inspected (no matter on what interface traffic come).



Packets inspection allows ASA to look deeper inside the packets when they're traversing the device. It allows ASA to automatically open a hole in the inbound direction on the outgoing interface for returning packets. Thus, configuring an ACL for the returning traffic is no longer required.

This advanced inspection policies allow traffic to pass the device in secure manner disallowing bogus or crafted packets.

There is a global inspection policy enabled by default on every interface in the inbound direction, however you can configure custom policy and apply it on the interface as well.

MPF configuration contains three steps:

- 1. Configure class-map to match interesting traffic (to be inspected)*
- 2. Configure policy-map, attach previously configured class-map to it and enable inspection*
- 3. Apply policy-map globally or on an interface*

MPF can perform deep packet inspection for a number of protocols. Each protocol has its own set of attributes and parameters which can be checked against when such traffic comes into the interface. To perform deep packet inspection (also called L7 inspection) a new class map and policy map type has been introduced. This is an "inspection" type class map and policy map which

is also called L7 maps. Those maps can be used to build up an advanced inspection policy and they can be attached under L3/L4 class map/policy map. More details will be presented later when it comes to advanced inspection on specific protocols (like HTTP or FTP).

The easiest way to accomplish this task is to configure inspection for HTTP and ICMP on a global level. All inbound packets on all ASA interfaces will be inspected automatically. We do not have to match any traffic, as it will be done automatically using inspection_default class map. This class map matches a number of default protocols and includes HTTP (port 80) and ICMP by default.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect http
ASA-FW(config-pmap-c)# inspect icmp
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

Verification

R1#p 2.2.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

ASA-FW(config)# sh service-policy global

Global policy:

Service-policy: global_policy

Class-map: inspection_default

Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0

Inspect: ftp, packet 0, drop 0, reset-drop 0

Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0

```

Inspect: rsh, packet 0, drop 0, reset-drop 0
Inspect: rtsp, packet 0, drop 0, reset-drop 0
      tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
      tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: skinny , packet 0, drop 0, reset-drop 0
      tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: xdmcp, packet 0, drop 0, reset-drop 0
Inspect: sip , packet 0, drop 0, reset-drop 0
      tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: netbios, packet 0, drop 0, reset-drop 0
Inspect: tftp, packet 0, drop 0, reset-drop 0
Inspect: http, packet 0, drop 0, reset-drop 0
Inspect: icmp, packet 10, drop 0, reset-drop 0

```

Why 10 packets? Because the default policy is attached globally, meaning it works on every interface in inbound direction. Hence, ten packets as there were 5 ICMP Echo Request and 5 ICMP Echo Replies.

ASA-FW(config)# sh run class-map inspection default

!

```

class-map inspection_default
  match default-inspection-traffic

```

ASA-FW(config)# class-map inspection default

ASA-FW(config-cmap)# match ?

mpf-class-map mode commands/options:

access-list	Match an Access List
any	Match any packet
default-inspection-traffic	Match default inspection traffic:
	ctiqbe----tcp--2748 dns-----udp--53
	ftp-----tcp--21 gtp-----udp--2123,3386
	h323-h225-tcp--1720 h323-ras--udp--1718-1719
	http-----tcp--80 icmp-----icmp
	ils-----tcp--389 mgcp-----udp--2427,2727
	netbios---udp--137-138 radius-acct---udp--1646
	rpc-----udp--111 rsh-----tcp--514
	rtsp-----tcp--554 sip-----tcp--5060
	sip-----udp--5060 skinny----tcp--2000
	smtp-----tcp--25 sqlnet----tcp--1521
	tftp-----udp--69 waas-----tcp--1-65535
	xdmcp-----udp--177
dscp	Match IP DSCP (DiffServ CodePoints)
flow	Flow based Policy
port	Match TCP/UDP port(s)
precedence	Match IP precedence
rtsp	Match RTP port numbers

tunnel-group

Match a Tunnel Group

ASA-FW(config)# sh conn all

7 in use, 10 most used

UDP DMZ 10.1.104.4:520 NP Identity Ifc 224.0.0.9:520, idle 0:00:20, bytes 15144, flags

-

ICMP OUT 2.2.2.2:0 IN 10.1.101.1:2, idle 0:00:00, bytes 72

UDP IN 10.1.101.1:520 NP Identity Ifc 224.0.0.9:520, idle 0:00:18, bytes 15216, flags -

UDP OUT 10.1.102.2:520 NP Identity Ifc 224.0.0.9:520, idle 0:00:10, bytes 15192, flags

-

UDP OUT 224.0.0.9:520 NP Identity Ifc 10.1.102.10:520, idle 0:00:06, bytes 53280, flags

-

UDP IN 224.0.0.9:520 NP Identity Ifc 10.1.101.10:520, idle 0:00:06, bytes 53280, flags

-

UDP DMZ 224.0.0.9:520 NP Identity Ifc 10.1.104.10:520, idle 0:00:06, bytes 53280, flags

-

Note that you need to start contiguous ping on R1 to see dynamic connection entries on the ASA.

Task 2

There is a SMTP server located on 4.4.4.4. Configure ASA so that it only inspects ESMTP traffic between 1.1.1.1 and 4.4.4.4.



ASA can inspect Simple Mail Transport Protocol (SMTP) allowing this traffic to be checked against a number of checks to ensure there are no malicious packets destined to the mail server. SMTP inspection is enabled by default on a global level (matched by inspection_default class map, all traffic destined to the port 25 is considered to be SMTP), hence there is no need for an ACL for allowing returning traffic and basic checks are enforced to ensure there is no harm in SMTP packets. However, in our case we're asked for SMTP inspection between two hosts only. This cannot be done on a global level and we need to match our traffic using an access list and enable SMTP inspection on the interface.

It is also wise to disable SMTP inspection on a global level if we don't want the inspection to be done on every interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# no inspect esmtp

ASA-FW(config-pmap-c)#access-list R1-to-R4-inspection permit ip host
1.1.1.1 host 4.4.4.4

ASA-FW(config)# class-map CM-R1-to-R4
ASA-FW(config-cmap)# match access-list R1-to-R4-inspection
ASA-FW(config-cmap)# exit

ASA-FW(config)# policy-map PM-R1-to-R4
ASA-FW(config-pmap)# class CM-R1-to-R4
ASA-FW(config-pmap-c)# inspect esmtp
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit

ASA-FW(config)# service-policy PM-R1-to-R4 interface DMZ
```

Verification

ASA-FW(config)# sh service-policy interface DMZ

Interface DMZ:

Service-policy: PM-R1-to-R4

Class-map: CM-R1-to-R4

Inspect: esmtp_default_esmtp_map, packet 0, drop 0, reset-drop 0

ASA-FW(config)# sh run all policy-map type inspect esmtp

```
!
policy-map type inspect esmtp_default_esmtp_map
description Default ESMTP policy-map
parameters
mask-banner
no mail-relay
no special-character
no allow-tls
match cmd line length gt 512
drop-connection log
match cmd RCPT count gt 100
drop-connection log
match body line length gt 998
```

```
log
match header line length gt 998
  drop-connection log
match sender-address length gt 320
  drop-connection log
match MIME filename length gt 255
  drop-connection log
match ehlo-reply-parameter others
mask
```

Note there are many SMTP checks configured by default. Hence, enabling SMTP inspection may cause your mail connections suffer. Be careful and know what you're doing!

ASA-FW(config)# sh service-policy inspect esmtp

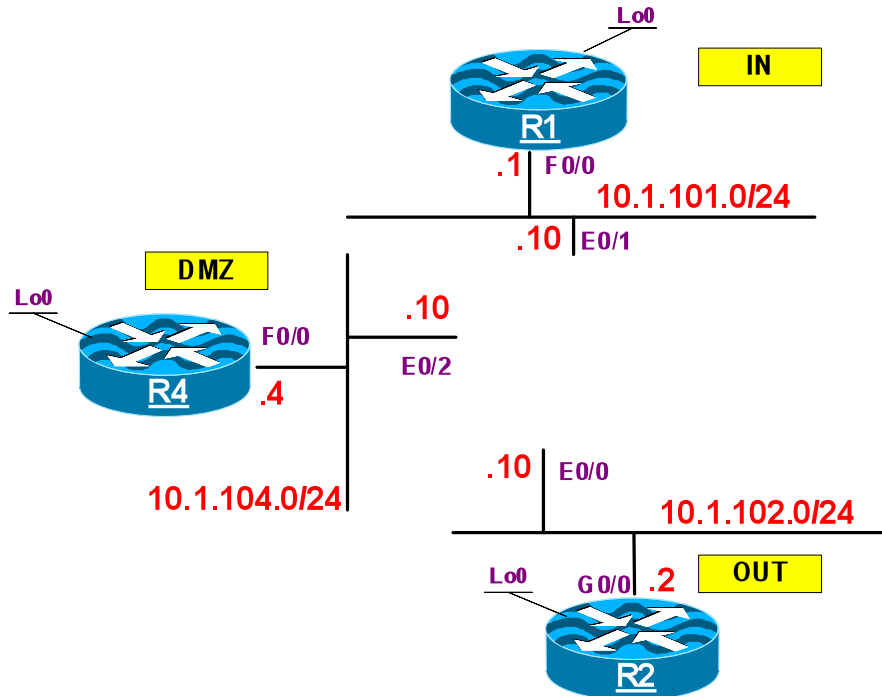
Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
```

Interface DMZ:

```
Service-policy: PM-R1-to-R4
Class-map: CM-R1-to-R4
  inspect: esmtp_default_esmtp_map, packet 0, drop 0, reset-drop 0
  mask-banner, count 0
  match cmd line length gt 512
    drop-connection log, packet 0
  match cmd RCPT count gt 100
    drop-connection log, packet 0
  match body line length gt 998
    log, packet 0
  match header line length gt 998
    drop-connection log, packet 0
  match sender-address length gt 320
    drop-connection log, packet 0
  match MIME filename length gt 255
    drop-connection log, packet 0
  match ehlo-reply-parameter others
    mask, packet 0
```

Lab 1.14. FTP Advanced Inspection



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the command `clear configure all` and then paste the initial config.

Task 1

There is an FTP server located in DMZ at 10.1.104.20. Configure ASA so that it resets any connection from the outside networks to that FTP server containing one of the following commands:

- DELE
- APPE
- PUT
- RMD



This task requires configuration of deep packet inspection for FTP. We're required to reset packets containing some FTP commands. To do that, ASA must be able to properly recognize the traffic (as FTP) and then check some fields inside FTP header/body to perform some actions. When we see a requirement for checking something which is protocol specific we should automatically start thinking about L7 class maps and policy maps.

So, we need to create L7 policy map (type inspect for FTP protocol) and match required commands inside the packets (we can also use L7 class map here and match it under L7 policy map but since we can match FTP commands using only one configuration line we can do that directly under the L7 policy map).

There is also need for L3/L4 class map matching traffic using an access list. The ACL is required here as we need to specify destination IP address (if we'd need to match all FTP traffic, the better option is to use "match port" statement).

L7 policy maps cannot be applied directly to the interface or at the global level. Instead, they first need to be applied under L3/L4 policy map when specifying the inspection.

Last thing is to assign L3/L4 policy map to the interface and since we want to protect our FTP server located in DMZ by resetting some commands which can be sent over from a FTP client (located on the outside networks) we must do it on the outside interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# access-list DMZ_FTP permit tcp any host 10.1.104.20
```

```
eq ftp

ASA-FW(config)# policy-map type inspect ftp PM_FTP
ASA-FW(config-pmap)# match request-command DELE APPE PUT RMD
ASA-FW(config-pmap-c)# reset

ASA-FW(config-pmap-c)# class-map CM_FTP
ASA-FW(config-cmap)# match access-list DMZ_FTP

ASA-FW(config-cmap)# policy-map OUTSIDE_MPF
ASA-FW(config-pmap)# class CM_FTP
ASA-FW(config-pmap-c)# inspect ftp strict PM_FTP

ASA-FW(config-pmap-c)# service-policy OUTSIDE_MPF interface OUT
```

Verification

```
ASA-FW(config)# sh service-policy inspect ftp
```

Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
Inspect: ftp, packet 0, drop 0, reset-drop 0
```

Interface OUT:

```
Service-policy: OUTSIDE_MPF
Class-map: CM_FTP
Inspect: ftp strict PM_FTP, packet 0, drop 0, reset-drop 0
match request-command appe put dele rmd
reset, packet 0
```

Task 2

The FTP server located in DMZ at 10.1.104.20 is managed from the inside network. Configure ASA so that it denies and logs all users except user “admin” from accessing directory “/secret” on all FTP servers located behind DMZ and OUT interfaces.



Here we need to block some users from accessing a directory on FTP servers. This can be done using regular expressions matching those two values (username and directory name) and resetting packets containing those values. Note that we need to disallow all usernames but "admin" username from accessing "/secret" folder. So, the easiest way to do that is to use NOT in the match statement.

Also note that we must use L7 class map here to match both conditions at once. This cannot be done using L7 policy map, as policy maps don't have match-all/match-any keywords available. Thus, first we need to create L7 class map matching two regexs (match-all perfectly suits here) and then nest this class map under the L7 policy map (remember that we can't use L7 class map under L3/L4 policy map).

As we're required to perform that inspection on every FTP connection originated from the inside network, we can simply match port 21 (using ACL is not necessary here) and apply L3/L4 policy map on the inside interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# regex FTP_USER "admin"
ASA-FW(config)# regex FTP_DIR "\/secret"
```

We need to use backslash sign before the "slash" because "slash" is a special character in the regex world, so that, we need to tell the regex engine to treat the "slash" like a normal character.

```
ASA-FW(config)# class-map type inspect ftp match-all CM_FTP_ACCESS
ASA-FW(config-cmap)# match not username regex FTP_USER
ASA-FW(config-cmap)# match filename regex FTP_DIR
```

Class map has match-all/match-any keywords available so that we can use more "match" statements to build more complex policies.

```
ASA-FW(config-cmap)# policy-map type inspect ftp PM_FTP_ACCESS
ASA-FW(config-pmap)# class CM_FTP_ACCESS
ASA-FW(config-pmap-c)# reset log
```

```
ASA-FW(config-pmap-c)# class-map CM_FTP_TRAFFIC
ASA-FW(config-cmap)# match port tcp eq ftp
```

Since we need to inspect FTP traffic the easiest way to do that is to match FTP port. However, this solution does not work for non-standard FTP ports. Be careful!

```
ASA-FW(config-cmap)# policy-map INSIDE_MPF
ASA-FW(config-pmap)# class CM_FTP_TRAFFIC
ASA-FW(config-pmap-c)# inspect ftp strict PM_FTP_ACCESS
```

The "strict" keyword enables enhanced inspection of FTP traffic and forces compliance with RFC standards.

```
ASA-FW(config-pmap-c)# service-policy INSIDE_MPF interface IN
```

Since our FTP server is located in the DMZ network and is managed from the inside network only, the best option is to enable inspection on IN interface. Better than enabling this globally.

Verification

```
ASA-FW(config)# sh service-policy inspect ftp table
```

Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
Inspect: ftp, packet 0, drop 0, reset-drop 0
```

INFO: There is no rule in the table.

Interface OUT:

```
Service-policy: OUTSIDE_MPF
Class-map: CM_FTP
Inspect: ftp strict PM_FTP, packet 0, drop 0, reset-drop 0
Match request-command appe put dele rmd
Number of filters 1, action: reset
Filter id: 2, subid/is_regex: 0x0/0, value_type: VALUE_GENERIC
value: 2625(0xa41), value_high: 0(0x0)
mask_match: ANY, mask_value: 0x0, negate: 0
```

Interface IN:

```
Service-policy: INSIDE_MPF
Class-map: CM_FTP_TRAFFIC
Inspect: ftp strict PM_FTP_ACCESS, packet 0, drop 0, reset-drop 0
Class-map: CM_FTP_ACCESS
Number of filters 2, action: reset log
Filter id: 0, subid/is_regex: 0x0/0, value_type: VALUE_REGEX
value: 21(0x15)/FTP_DIR, value_high: 21(0x15)
mask_match: NONE, mask_value: 0x0, negate: 0
Filter id: 4, subid/is_regex: 0x0/0, value_type: VALUE_REGEX
```

```
value: 20(0x14)/FTP_USER, value_high: 20(0x14)
mask_match: NONE, mask_value: 0x0, negate: 1
```

Task 3

The FTP server in DMZ should NOT disclose any information about software version or system greeting to the users behind OUT interface. You can alter existing configuration to accomplish this task.



To protect our FTP server located in DMZ we can mask some information that is usually disclosed while user connects to the server. That information could be used for a reconnaissance part of an attack.

Since we have some configuration done already (Task 1) we can simply add more lines to existing config. This can be done by configuring “parameters” part under the L7 policy map (remember that this is protocol specific so it must be done using L7 maps) where we just add some checks to be done while inspecting traffic.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# policy-map type inspect ftp PM_FTP
ASA-FW(config-pmap)# parameters
ASA-FW(config-pmap-p)# mask-banner
ASA-FW(config-pmap-p)# mask-syst-reply
ASA-FW(config-pmap-p)# exit
ASA-FW(config-pmap)# exit
```

Verification

```
ASA-FW(config)# sh service-policy inspect ftp
```

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: ftp, packet 0, drop 0, reset-drop 0
```

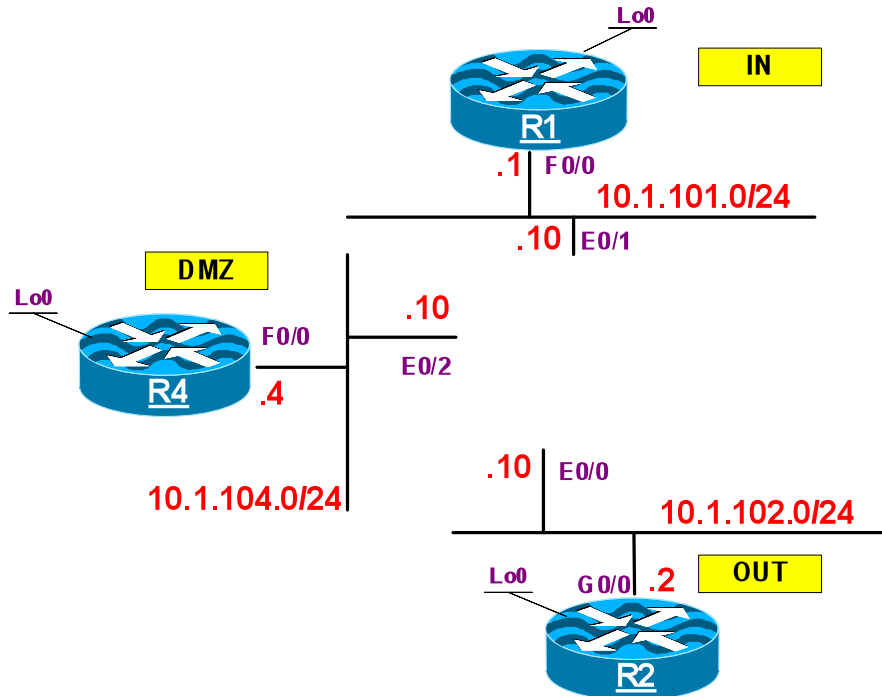
Interface OUT:

```
Service-policy: OUTSIDE_MPF
Class-map: CM_FTP
  Inspect: ftp strict PM_FTP, packet 0, drop 0, reset-drop 0
    mask-banner enabled
    mask-syst-reply enabled
    match request-command appe put dele rmd
    reset, packet 0
```

Interface IN:

```
Service-policy: INSIDE_MPF
Class-map: CM_FTP_TRAFFIC
  Inspect: ftp strict PM_FTP_ACCESS, packet 0, drop 0, reset-drop 0
    class CM_FTP_ACCESS
      reset log, packet 0
```

Lab 1.15.HTTP Advanced Inspection



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the command `clear configure all` and then paste the initial config.

Task 1

You have discovered a new version of peer-to-peer software uses in your network. After sniffing the traffic you have caught a few HTTP packets with User-Agent = "P2P-new-app" in the header. Configure ASA to block that peer-to-peer application and log that activity.



This task requires configuration of deep packet inspection for HTTP. All we need is to recognize some peer-to-peer software which uses HTTP as a transport by matching against User-Agent HTTP header field. This can be done using regular expression and L7 policy map.

As we want to perform the inspection for HTTP traffic comes from every direction, we can use global policy in that case (remember that global policy uses inspection_default class map which matches HTTP by default).

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# regex P2P "P2P-new-app"

ASA-FW(config)# policy-map type inspect http PM_HTTP_P2P
ASA-FW(config-pmap)# match request header user-agent regex P2P
ASA-FW(config-pmap-c)# drop-connection log

ASA-FW(config-pmap-c)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect http PM_HTTP_P2P
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

Verification

```
ASA-FW(config)# sh service-policy inspect http
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: inspection_default
```

```
Inspect: http PM_HTTP_P2P, packet 0, drop 0, reset-drop 0
```

```

protocol violations
packet 0
match request header user-agent regex P2P
drop-connection log, packet 0

```

Task 2

Configure ASA so that it disallows Internet surfing for websites <http://www.yahoo.com> and <http://mail.google.com> using MPF. This policy should be enforced on the inside interface.



Using MPF it is possible to filter out packets containing a specific field's value in HTTP header. In this case we're requested to look after specific URLs to block out users access to some websites. This can be easily done using regular expressions as some header fields may contain additional control characters and it's sometimes hard to match an exact value. Following is an example of HTTP packet capture which depicts most of header fields and their possible values. As you can see the URL is carried by the header field named "Host" so we should match that field in our L7 class map (or L7 policy map if we have only one condition to match).

```

⊞ Frame 4 (533 bytes on wire (533 bytes captured))
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
⊞ Hypertext Transfer Protocol
  ⊞ GET /download.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /download.html
    Request Version: HTTP/1.1
  Host: www.ethereal.com\r\n
  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
  Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,
  Accept-Language: en-us,en;q=0.5\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
  Keep-Alive: 300\r\n
  Connection: keep-alive\r\n
  Referer: http://www.ethereal.com/development.html\r\n
  \r\n

```

Two regex statements must be matched by L7 type "regex" class map (remember that you need to use "match-any" as those two URLs never be seen in one packet). Then this class map must be used in another L7 type "inspect" class map in order to match by specific header field. Next, L7 policy map is used to perform an action on our matched traffic (HTTP traffic containing specific URLs in Host field).

Last thing is to enable deep packet inspection for HTTP traffic using L3/L4

policy map. The L3/L4 class map used in this task can be either "inspection_default" which is pre-configured and we know it matches HTTP using port 80 or it can be a new L3/L4 class map configured (matching port 80 for example). As this task does not specify that this must be done ONLY for HTTP traffic we can use both solutions.

The L3/L4 policy map must be assigned with inside interface, as the HTTP header field (Host) is sent in the very first HTTP packet from the client to the server and we want to match and reset that session as near to the source as possible.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# regex URL_YAHOO "www\.yahoo\.com"
ASA-FW(config)# regex URL_GMAIL "mail\.google\.com"
```

Note that backslash sign must be used to treat the dot "." as a string not a regular expression control sign.

```
ASA-FW(config)# class-map type regex match-any CM_URL_REGEX
ASA-FW(config-cmap)# match regex URL_YAHOO
ASA-FW(config-cmap)# match regex URL_GMAIL
```

We must use class-map type regex here as there are two regex for matching.

```
ASA-FW(config-cmap)# class-map type inspect http CM_HTTP_URLS
ASA-FW(config-cmap)# match request header host regex class
CM_URL_REGEX
```

```
ASA-FW(config-cmap)# policy-map type inspect http PM_BLOCK_URLS
ASA-FW(config-pmap)# class CM_HTTP_URLS
ASA-FW(config-pmap-c)# reset log
```

```
ASA-FW(config-pmap-c)# policy-map INSIDE_MPF
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect http PM_BLOCK_URLS
```

```
ASA-FW(config-pmap-c)# service-policy INSIDE_MPF interface IN
```

Verification

```
ASA-FW(config)# sh service-policy inspect http
```

Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
  Inspect: http PM_HTTP_P2P, packet 0, drop 0, reset-drop 0
    protocol violations
      packet 0
  match request header user-agent regex P2P
  drop-connection log, packet 0
```

Interface IN:

```
Service-policy: INSIDE_MPF
Class-map: inspection_default
  Inspect: http PM_BLOCK_URLS, packet 0, drop 0, reset-drop 0
    protocol violations
      packet 0
  class CM_HTTP_URLS
    reset log, packet 0
```

Task 3

There is a Web Server configured on R4 (10.1.104.4). You need to protect this server from the outside networks by the following policy:

- replace server name in the server banner to “MySecureServer”
- prohibit any HTTP request that does not contain a GET or POST request method and generate SYSLOG message when such a request is detected
- silently drop all connections which violates HTTP protocol specification



Each deep protocol inspection has its own set of additional parameters which can be checked. Those parameters can differ in ASA software depending on version as some additional checks can be added in the future. For HTTP we are requested to mask our server's banner and enforce protocol compliance with HTTP standard. This can be done using L7 policy map with “parameters” subsection. In addition we're requested to allow only GET and POST HTTP methods to be destined to our web server. As there can be more HTTP methods available in protocol specification (and we do not need to know every method available) it is wise to use NOT in match statement to filter out remaining methods.

Finally, as we need to protect our web server which is specified in the task, there is a need for an access list matching traffic destined to the server. The

policy must be enforced on the outside interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# class-map type inspect http match-all CM_METHODS
ASA-FW(config-cmap)# match not request method get
ASA-FW(config-cmap)# match not request method post
```

This will match all HTTP methods but GET and POST.

```
ASA-FW(config-cmap)# policy-map type inspect http
SERVER_PROTECTION
ASA-FW(config-pmap)# parameters
ASA-FW(config-pmap-p)# spoof-server "MySecureServer"
ASA-FW(config-pmap-p)# protocol-violation action drop-connection
ASA-FW(config-pmap-p)# class CM_METHODS
ASA-FW(config-pmap-c)# reset log
```

A web server is usually introduces itself to every client by attaching some information in HTTP header. This can be a risk as a malicious user may get information about software version of the server and search for bugs and security holes for that version. Hence, the best option is to mislead the attacker by spoofing server's banner and pretending this server software is from other vendors.

```
ASA-FW(config-pmap-c)# access-list TO_WEB_SERVER permit tcp any
host 10.1.104.4 eq http
```

```
ASA-FW(config)# class-map CM_WEB_SERVER
ASA-FW(config-cmap)# match access-list TO_WEB_SERVER
```

```
ASA-FW(config-cmap)# policy-map OUTSIDE_MPF
ASA-FW(config-pmap)# class CM_WEB_SERVER
ASA-FW(config-pmap-c)# inspect http SERVER_PROTECTION
```

```
ASA-FW(config-pmap-c)# service-policy OUTSIDE_MPF interface OUT
```

Verification

```
ASA-FW(config)# sh service-policy inspect http
```

Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
  Inspect: http PM_HTTP_P2P, packet 0, drop 0, reset-drop 0
    protocol violations
    packet 0
  match request header user-agent regex P2P
  drop-connection log, packet 0

Interface OUT:
Service-policy: OUTSIDE_MPF
Class-map: CM_WEB_SERVER
  Inspect: http SERVER_PROTECTION, packet 0, drop 0, reset-drop 0
    protocol violations
    packet 0
  server spoofs, packet 0
  class CM_METHODS
    reset log, packet 0

Interface IN:
Service-policy: INSIDE_MPF
Class-map: inspection_default
  Inspect: http PM_BLOCK_URLS, packet 12, drop 2, reset-drop 2
    protocol violations
    packet 0
  class CM_HTTP_URLS
    reset log, packet 0
```

Task 4

There is a Web proxy server located in DMZ at 10.1.104.20. All internal users use this server to surf the Internet. Configure ASA so that it disallows other protocols tunneling through HTTP by configuring strict size and number of headers allowed. Any HTTP request message that containing host field longer than 6 bytes and host field appears more than 3 times in the packet must be dropped.



HTTP tunneling is often used to provide connectivity for applications which have restricted access or with lack of native support for communication. Tunneled application adds additional header information inside the HTTP packet which is processed somehow on the far end.

We can block such applications using simple MPF configuration and looking at number of headers inside HTTP and length of the Host field which is usually

longer than it is in “pure” HTTP traffic.

We must be careful here as the task asks us for checking traffic sourced from the Proxy server located in DMZ, so the inspection policy must be applied on DMZ interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# class-map type inspect http CM_HTTP_HEADER_LENGTH
ASA-FW(config-cmap)# match request header host length gt 6

ASA-FW(config-cmap)# class-map type inspect http CM_HTTP_HEADERS
ASA-FW(config-cmap)# match request header host count gt 3

ASA-FW(config-cmap)# policy-map type inspect http PM_HTTP_CHECK
ASA-FW(config-pmap)# class CM_HTTP_HEADER_LENGTH
ASA-FW(config-pmap-c)# reset
ASA-FW(config-pmap-c)# class CM_HTTP_HEADERS
ASA-FW(config-pmap-c)# reset

ASA-FW(config-pmap-c)# access-list PROXY permit tcp host
10.1.104.20 any eq 80

ASA-FW(config)# class-map CM_PROXY
ASA-FW(config-cmap)# match access-list PROXY

ASA-FW(config-cmap)# policy-map DMZ_MPF
ASA-FW(config-pmap)# class CM_PROXY
ASA-FW(config-pmap-c)# inspect http PM_HTTP_CHECK

ASA-FW(config-pmap-c)# service-policy DMZ_MPF interface DMZ
```

Verification

ASA-FW(config)# sh service-policy inspect http

Global policy:

Service-policy: global_policy

Class-map: inspection_default

Inspect: http PM_HTTP_P2P, packet 0, drop 0, reset-drop 0
protocol violations
packet 0

```
match request header user-agent regex P2P
drop-connection log, packet 0
```

Interface OUT:

```
Service-policy: OUTSIDE_MPF
Class-map: CM_WEB_SERVER
Inspect: http SERVER_PROTECTION, packet 0, drop 0, reset-drop 0
protocol violations
packet 0
server spoofs, packet 0
class CM_METHODS
reset log, packet 0
```

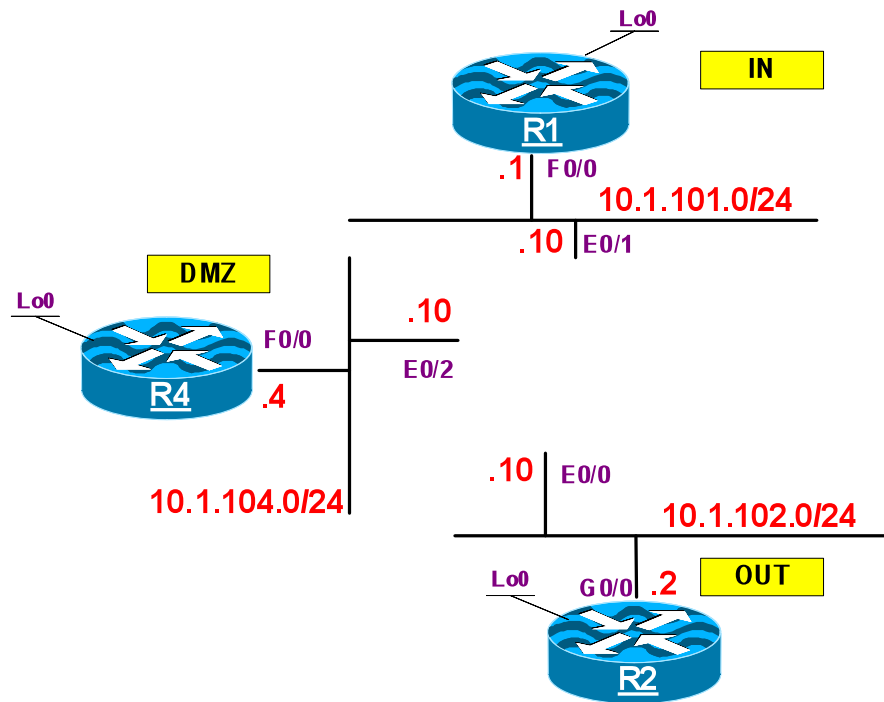
Interface IN:

```
Service-policy: INSIDE_MPF
Class-map: inspection_default
Inspect: http PM_BLOCK_URLS, packet 12, drop 2, reset-drop 2
protocol violations
packet 0
class CM_HTTP_URLS
reset log, packet 0
```

Interface DMZ:

```
Service-policy: DMZ_MPF
Class-map: CM_PROXY
Inspect: http PM_HTTP_CHECK, packet 0, drop 0, reset-drop 0
protocol violations
packet 0
class CM_HTTP_HEADER_LENGTH
reset, packet 0
class CM_HTTP_HEADERS
reset, packet 0
```


Lab 1.16. Instant Messaging Advanced Inspection



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the command `clear configure all` and then paste the initial config.

Task 1

You have discovered that users in your inside network are using Yahoo and/or MSN instant messenger software. Configure ASA to block the following services offered by those applications:

- Conference
- Games
- File transfer
- Webcam

In addition to that, totally block usage of both applications for host 10.1.101.123.



ASA allows us to configure policy settings for Instant Messaging software containing Microsoft's MSN and Yahoo IM. Each of these applications have a number of services which are for example Chat, Conference, Games, File transfer, Webcam, etc. Some of those services could be dangerous for our users as they may be used by skilled attacker to upload and run malicious software on user's computer.

We are requested here to block out some of those services for our internal users. In addition to that one user's IP address must NOT be able to use messaging applications at all.

As you can see, we have two things to do which requires slightly different policy. Thus, we need two L7 class maps. One is to match IM protocols (MSN and Yahoo) and their services (Conference, Games, File transfer and Webcam). Second is to match IM protocols and user's IP address. Both L7 class maps can then be used in one L7 policy map to take an action.

We can use global policy to enforce our IM inspection.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# class-map type inspect im match-all CM_IM_SERVICES
ASA-FW(config-cmap)# match protocol yahoo-im msn-im
ASA-FW(config-cmap)# match service conference games file-transfer
webcam

ASA-FW(config-cmap)# class-map type inspect im match-all CM_IM_HOST
ASA-FW(config-cmap)# match protocol yahoo-im msn-im
ASA-FW(config-cmap)# match ip-address 10.1.101.123 255.255.255.255

ASA-FW(config-cmap)# policy-map type inspect im PM_IM
ASA-FW(config-pmap)# class CM_IM_SERVICES
ASA-FW(config-pmap-c)# reset
ASA-FW(config-pmap-c)# class CM_IM_HOST
ASA-FW(config-pmap-c)# drop-connection

ASA-FW(config-pmap-c)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect im PM_IM
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

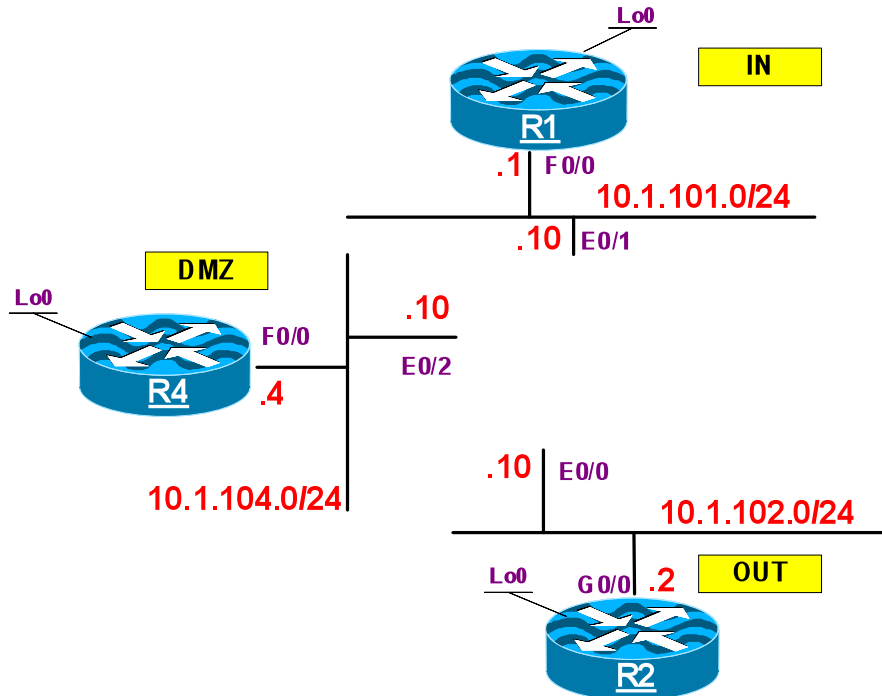
Verification

```
ASA-FW(config)# sh service-policy inspect im
```

Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
Inspect: im PM_IM, packet 0, drop 0, reset-drop 0
class CM_IM_SERVICES
  reset, packet 0
class CM_IM_HOST
  drop-connection, packet 0
```

Lab 1.17.ESMTP Advanced Inspection



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the command `clear configure all` and then paste the initial config.

Task 1

There is a plan to deploy a number of SMTP servers in the DMZ. You are requested to pro-actively configure the following policy to protect the servers against potential attackers (from all directions):

- drop all ESMTP messages longer than 48000 characters and generate log when such incident happen
- limit all EHLO commands to 10 per second
- drop all messages with more than 10 recipients per transaction
- do not allow ESMTP command line to be longer than 600 bytes.



Simple Mail Transport Protocol inspection is complex and can use lot of parameters. Thanks for that, because we can create more flexible policies controlling SMTP traffic before it hits the mail server.

It is possible to control commands which are sent through SMTP and limit their number to ensure some commands can't overwhelm our mail server causing DOS attack.

In this task we do not need L7 class map as all requested checks can be configured directly under L7 policy map. As we are requested to apply the inspection policy on the global level, we first need to disable default SMTP inspection to be able to assign our custom L7 policy map.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# policy-map type inspect esmtp PM_SMTP
```

```
ASA-FW(config-pmap)# match body length gt 48000
ASA-FW(config-pmap-c)# drop-connection log
ASA-FW(config-pmap-c)# match cmd verb EHLO
ASA-FW(config-pmap-c)# rate-limit 10
ASA-FW(config-pmap-c)# match cmd RCPT count gt 10
ASA-FW(config-pmap-c)# drop-connection
ASA-FW(config-pmap-c)# match cmd line length gt 600
ASA-FW(config-pmap-c)# drop-connection

ASA-FW(config-pmap-c)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect esmtp PM_SMTP
ERROR: Inspect configuration of this type exists, first remove
that configuration and then add the new configuration
```

There is a default ESMTP inspection enabled which uses
"_default_esmtp_map" policy map with bunch of checks
preconfigured. We need to disable it first before
configuring our new policy.

```
ASA-FW(config-pmap-c)# no inspect esmtp
ASA-FW(config-pmap-c)# inspect esmtp PM_SMTP
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

Verification

Here is a default SNMP inspection L7 policy map. As you can see, there are lots
of default parameters configured to protect mail servers. Those default
settings can sometimes cause problems and needs to be considered when deploying
ASA in the new environment where mail servers are located.

```
ASA-FW(config)# sh run all policy-map type inspect esmtp default esmtp map
!
policy-map type inspect esmtp _default_esmtp_map
description Default ESMTP policy-map
parameters
mask-banner
no mail-relay
no special-character
no allow-tls
match cmd line length gt 512
drop-connection log
match cmd RCPT count gt 100
drop-connection log
match body line length gt 998
log
```

```
match header line length gt 998
  drop-connection log
match sender-address length gt 320
  drop-connection log
match MIME filename length gt 255
  drop-connection log
match ehlo-reply-parameter others
  mask
!
```

ASA-FW(config)# sh service-policy inspect esmtp

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
  Inspect: esmtp PM_SMTP, packet 0, drop 0, reset-drop 0
    mask-banner, count 0
    match body length gt 48000
      drop-connection log, packet 0
    match cmd verb EHLO
      rate-limit 10, packet 0
    match cmd RCPT count gt 10
      drop-connection, packet 0
    match cmd line length gt 600
      drop-connection, packet 0
```

Task 2

Recently, you have been asked by mail server administrator to help him block senders and domains of malicious mails. You need to block emails coming from the following domains:

- @gmail.com
- @yahoo.com
- specific user with e-mail address of jdoe@hotmail.com

You can alter existing configuration to accomplish this task.



In this task we need to match SMTP packets containing some string values. When it comes to strings the best option to use is regular expressions. We can easily match those strings using L7 class map (remember to use “match-any” keyword as those strings may not appear in SMTP packets together). Then we can match sender address using L7 policy map configured in the previous task.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# regex GMAIL "@gmail\.com"
ASA-FW(config)# regex YAHOO "@yahoo\.com"
ASA-FW(config)# regex HOTMAIL "jdoe@hotmail\.com"

ASA-FW(config)# class-map type regex match-any CM_BLOCK_EMAIL
ASA-FW(config-cmap)# match regex GMAIL
ASA-FW(config-cmap)# match regex YAHOO
ASA-FW(config-cmap)# match regex HOTMAIL
```

There must be class map of type regex as there are three regexs to match.

```
ASA-FW(config-cmap)# policy-map type inspect esmtp PM_SMTP
ASA-FW(config-pmap)# match sender-address regex class
CM_BLOCK_EMAIL
ASA-FW(config-pmap-c)# drop-connection
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

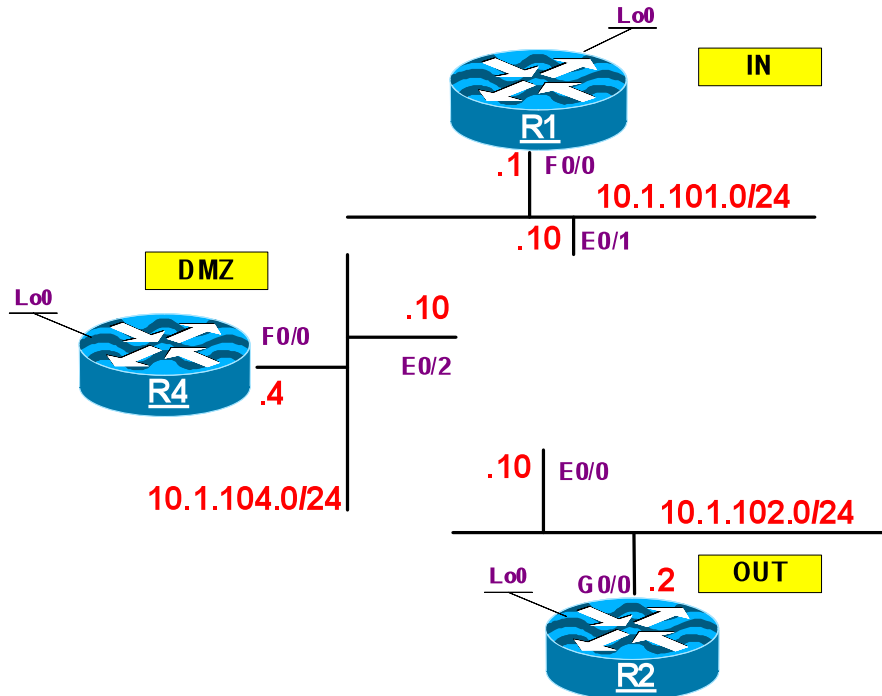
Verification

```
ASA-FW(config)# sh service-policy inspect esmtp
```

Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp PM_SMTP, packet 0, drop 0, reset-drop 0
  mask-banner, count 0
  match body length gt 48000
  drop-connection log, packet 0
  match cmd verb EHLO
  rate-limit 10, packet 0
  match cmd RCPT count gt 10
  drop-connection, packet 0
  match cmd line length gt 600
  drop-connection, packet 0
  match sender-address regex class CM_BLOCK_EMAIL
  drop-connection, packet 0
```


Lab 1.18.DNS Advanced Inspection



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the command `clear configure all` and then paste the initial config.

Task 1

A new DNS server for domain `micronicstraining.com` has been deployed in DMZ. Configure ASA so that it allows only this domain to be queried and mask RD bit in the DNS header to prevent the server from sending recursive queries on behalf of a requester.



DNS cache poisoning attacks use DNS open resolvers when attempting to corrupt the DNS cache of vulnerable systems. The DNS messages sent to open resolvers set the recursion desired (RD) flag in the DNS header. Utilizing the DNS application inspection flag filtering feature, these attacks can be minimized by dropping DNS messages with the RD flag present in the DNS header.

Another useful security control is to ensure that DNS query contains only domain name belonging to us. If other domain name is requested the DNS server might use recursive lookup for this domain and waste resources.

Note that we are asked to mask RD bit inside the DNS query, NOT drop those packets. This can be done using "mask" keyword as an action in L7 policy map. The inspection policy should be applied on the outside interface as most queries come from the outside networks.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# regex DOMAIN "micronicstraining\.com"

ASA-FW(config)# policy-map type inspect dns PM_DNS
ASA-FW(config-pmap)# match not domain-name regex DOMAIN
```

```
ASA-FW(config-pmap-c)# drop
ASA-FW(config-pmap-c)# match header-flag RD
ASA-FW(config-pmap-c)# mask

ASA-FW(config-pmap-c)# class-map CM_DNS_SERVER
ASA-FW(config-cmap)# match port udp eq 53

ASA-FW(config-cmap)# policy-map OUTSIDE_MPF
ASA-FW(config-pmap)# class CM_DNS_SERVER
ASA-FW(config-pmap-c)# inspect dns PM_DNS

ASA-FW(config-pmap-c)# service-policy OUTSIDE_MPF interface OUT
```

Verification

```
ASA-FW(config)# sh service-policy inspect dns
```

Global policy:

```
Service-policy: global_policy
Class-map: inspection_default
Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
message-length maximum 512, drop 0
dns-guard, count 0
protocol-enforcement, drop 0
nat-rewrite, count 0
```

Interface OUT:

```
Service-policy: OUTSIDE_MPF
Class-map: CM_DNS_SERVER
Inspect: dns PM_DNS, packet 0, drop 0, reset-drop 0
dns-guard, count 0
protocol-enforcement, drop 0
nat-rewrite, count 0
match not domain-name regex DOMAIN
drop, packet 0
match header-flag RD
mask, packet 0
```

Task 2

There is a new Web Server hosting www.micronicstraining.com website deployed in the inside network at 10.1.101.25. This server needs to be visible to the outside world as 10.1.102.25. Client workstations located in the inside network must access the

Web Server using its FQDN which has DNS A record pointing to 10.1.102.25 in the external DNS server located in ISP network.

Configure ASA so that it performs dynamic NAT translation for all inside hosts to the pool of 10.1.102.100-200. Ensure that client workstations get private IP address of the Web Server when connecting to www.micronicstraining.com.



The problem here is that internal clients will get public IP address of the Web server from an external DNS server. This can be an issue if the Web server's IP address is translated on the ASA.

Fortunately, there is an additional "dns" keyword in the static command which rewrites the A (address) record in DNS replies that match this static. For DNS replies traversing from a mapped interface to any other interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the A record is rewritten from the real value to the mapped value.

Also note that DNS inspection must be enabled to support this functionality (it is enabled by default in the global policy).

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# nat (IN) 1 0 0 dns
ASA-FW(config)# global (OUT) 1 10.1.102.100-10.1.102.200 netmask
255.255.255.0

ASA-FW(config)# static (IN,OUT) 10.1.102.25 10.1.102.25 dns

ASA-FW(config)# access-list OUTSIDE_IN permit tcp any host
10.1.102.25 eq 80
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

Verification

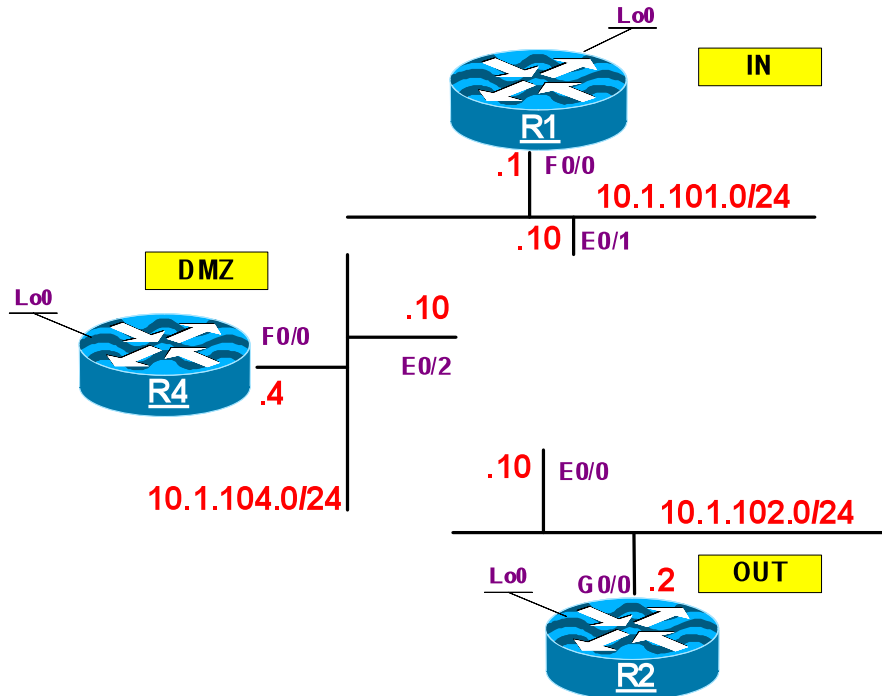
```
ASA-FW(config)# sh xlate detail
1 in use, 1 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
```

```
    r - portmap, s - static
NAT from IN:10.1.102.25 to OUT:10.1.102.25 flags sD
```

ASA-FW(config)# sh nat IN OUT

```
match ip IN host 10.1.102.25 OUT any
static translation to 10.1.102.25
translate_hits = 0, untranslate_hits = 0
match ip IN any OUT any
dynamic translation to pool 1 (10.1.102.100 - 10.1.102.200)
translate_hits = 0, untranslate_hits = 0
```

Lab 1.19. ICMP Advanced Inspection



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1	E0/0	10.1.102.10/24
	E0/1	10.1.101.10/24
	E0/2.104	10.1.104.10/24

Note that the topology is the same so that you can quickly revert to initial config on the ASA by using the command `clear configure all` and then paste the initial config.

Task 1

Configure ASA so that it allows ICMP traffic coming from inside network to DMZ and to outside and to be initiated from the outside to DMZ. You are not allowed using of access list however you can alter initial configuration to accomplish this task.



We have two things to do in this task: (1) allow ICMP traffic from Inside to outside and DMZ and (2) allow ICMP traffic from outside to DMZ but not inside. In addition we are not allowed to use any ACL to accomplish this task. This should direct us to the solution using MPF. It is enough to enable ICMP inspection in the global policy to accomplish first part of the question.

However, ICMP inspection won't work for traffic originated from outside network to DMZ as it is against basic rule that traffic from the interface with lower security level to the interface with higher security level is not allowed by default (there must be an ACL on the outside to allow this traffic).

Fortunately, we're allowed to alter initial configuration. Thus, the best option which meets requirements is to change security level on the outside interface to be higher than security level on DMZ interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect icmp
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

```
ASA-FW(config)# int e0/0
ASA-FW(config-subif)# security-level 60
ASA-FW(config-subif)# exit
```

Verification

R1#ping 2.2.2.2 so lo0 rep 100

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/66/180 ms
```

ASA-FW(config)# sh conn all | in ICMP

```
ICMP OUT 2.2.2.2:0 IN 1.1.1.1:4, idle 0:00:00, bytes 72
```

R1#ping 4.4.4.4 so lo0 rep 100

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/57/204 ms
```

ASA-FW(config)# sh conn all | in ICMP

```
ICMP DMZ 4.4.4.4:0 IN 1.1.1.1:4, idle 0:00:00, bytes 72
```

R2#ping 4.4.4.4 so lo0 rep 10000

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/54/188 ms
```

ASA-FW(config)# sh conn all | in ICMP

```
ICMP DMZ 4.4.4.4:0 OUT 2.2.2.2:2, idle 0:00:00, bytes 72
```



```
ASA-FW(config)# logg buffered 7
ASA-FW(config)# logg on
ASA-FW(config)# clear logg buffer
```

R2#ping 1.1.1.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

ASA-FW(config)# sh logg

```
Syslog logging: enabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: disabled
  Debug-trace logging: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: level debugging, 8 messages logged
  Trap logging: disabled
  History logging: disabled
  Device ID: disabled
  Mail logging: disabled
  ASDM logging: disabled
%ASA-5-111008: User 'enable_15' executed the 'clear logging buffer' command.
%ASA-3-106014: Deny inbound icmp src OUT:10.1.102.2 dst IN:1.1.1.1 (type 8, code 0)
%ASA-3-106014: Deny inbound icmp src OUT:10.1.102.2 dst IN:1.1.1.1 (type 8, code 0)
%ASA-3-106014: Deny inbound icmp src OUT:10.1.102.2 dst IN:1.1.1.1 (type 8, code 0)
%ASA-3-106014: Deny inbound icmp src OUT:10.1.102.2 dst IN:1.1.1.1 (type 8, code 0)
%ASA-3-106014: Deny inbound icmp src OUT:10.1.102.2 dst IN:1.1.1.1 (type 8, code 0)
```

Note that there is no ACL in the logging output so that this traffic has been denied on the OUT interface by the ASA's rules.

Task 2

Statically translate R1's F0/0 interface to be visible on the outside network as 10.1.102.1. Enable traceroute packets to go through the ASA and ensure that inside network's address is hidden when doing traceroute on R2 to the network behind R1 (use R1's loopback0 IP address).



ICMP inspection allows ICMP packets to go through the ASA without configuring ACL on the outbound interface for returning traffic. However, it can also be used for changing some information inside ICMP packets to not disclose sensitive information about the network. This is useful when traceroute is used as it sends UDP packets with increased TTL and waiting for ICMP time-exceeded or ICMP port unreachable packets. When NAT is configured on the ASA a traceroute tools can reveal IP addressing of subnets behind the ASA when tracerouting IP addresses in remote networks.

We can mitigate that issue by enabling ICMP error inspection on the ASA. Then the ASA changes IP address of the translated host (which sends out ICMP time-exceeded or port unreachable) according to the translation configured.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# static (IN,OUT) 10.1.102.1 10.1.101.1

ASA-FW(config)# access-list OUTSIDE_IN permit udp any any
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT

ASA-FW(config)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect icmp error
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

Verification

[before enabling ICMP error inspection]

R2#traceroute 1.1.1.1

Type escape sequence to abort.

Tracing the route to 1.1.1.1

```
1 10.1.101.1 252 msec 212 msec *
```

[after enabling ICMP error inspection]

R2#traceroute 1.1.1.1

Type escape sequence to abort.

Tracing the route to 1.1.1.1

```
1 10.1.102.1 200 msec 120 msec *
```

Note that the IP address in returning ICMP packet has been altered based on configured translation.

ASA-FW(config)# sh service-policy global

Global policy:

Service-policy: global_policy

Class-map: inspection_default

Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0

Inspect: ftp, packet 0, drop 0, reset-drop 0

Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0

Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0

Inspect: netbios, packet 0, drop 0, reset-drop 0

Inspect: rsh, packet 0, drop 0, reset-drop 0

Inspect: rtsp, packet 0, drop 0, reset-drop 0

Inspect: skinny , packet 0, drop 0, reset-drop 0

Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0

Inspect: sqlnet, packet 0, drop 0, reset-drop 0

Inspect: sunrpc, packet 0, drop 0, reset-drop 0

Inspect: tftp, packet 0, drop 0, reset-drop 0

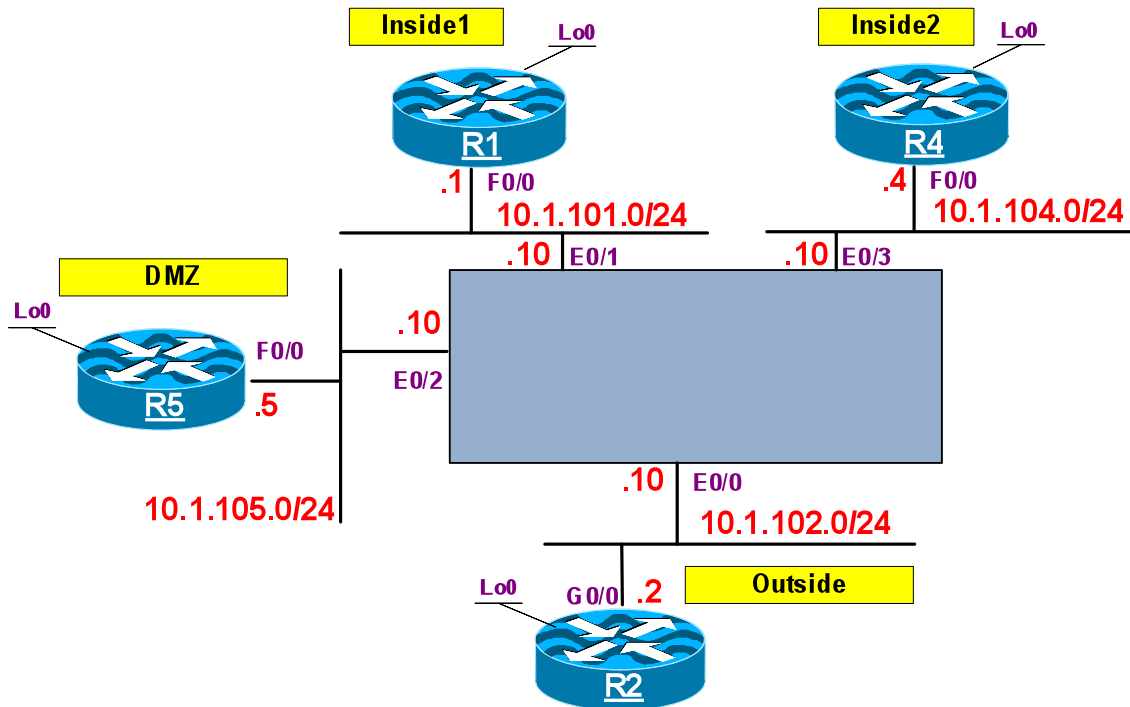
Inspect: sip , packet 0, drop 0, reset-drop 0

Inspect: xdmcp, packet 0, drop 0, reset-drop 0

Inspect: icmp, packet 60, drop 0, reset-drop 0

Inspect: icmp error, packet 2, drop 0, reset-drop 0

Lab 1.20. Configuring Virtual Firewalls



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1's E0/3 interface should be configured in VLAN 104
- R5's F0/0 and ASA1's E0/2 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"
- Configure static default route on all routers pointing to ASA.

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24

Task 1

Configure ASA with the following security contexts:

Context name:	CTX1	CTX2
Interfaces:	E0/0 – Outside E0/1 – Inside E0/2.104 – DMZ	E0/0 – Outside E0/3 – Inside
Context file:	CTX1.CFG	CTX2.CFG

The context configuration should be stored on the Flash memory. Assigned interfaces should be named as showed in the table so that no physical interface name is disclosed inside the context.



You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context acts like an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

You can run all your contexts in routed mode or transparent mode; you cannot run some contexts in one mode and others in another. Multiple context mode supports static routing only.

To enable multiple mode (security contexts), enter command `mode multiple`. You will be prompted to reboot the security appliance.

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files: a new startup configuration that comprises the system configuration, and `admin.cfg` that comprises the admin context (in the root directory of the internal Flash memory). The original running configuration is saved as `old_running.cfg` (in the root directory of the internal Flash memory). The original startup configuration is not saved. The security appliance automatically adds an entry for the admin context to the system configuration with the name `admin`.

The system administrator adds and manages contexts by configuring each

context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context. The system configuration does include a specialized failover interface for failover traffic only.

To create a new security context you must enter command “context <name>” in the system configuration and specify context configuration file (usually on the Flash) and allocate interfaces to the context. Those interfaces will be visible in the context mode. To ensure that an administrator of the context will not see any physical interface’s name, you can name the interface during its allocation.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

Rebooting....

Booting system, please wait...

CISCO SYSTEMS

Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17

Low Memory: 631 KB

High Memory: 256 MB

PCI Device Table.

Bus	Dev	Func	VendID	DevID	Class	Irq
00	00	00	8086	2578	Host Bridge	
00	01	00	8086	2579	PCI-to-PCI Bridge	
00	03	00	8086	257B	PCI-to-PCI Bridge	
00	1C	00	8086	25AE	PCI-to-PCI Bridge	
00	1D	00	8086	25A9	Serial Bus	11
00	1D	01	8086	25AA	Serial Bus	10
00	1D	04	8086	25AB	System	
00	1D	05	8086	25AC	IRQ Controller	
00	1D	07	8086	25AD	Serial Bus	9
00	1E	00	8086	244E	PCI-to-PCI Bridge	
00	1F	00	8086	25A1	ISA Bridge	
00	1F	02	8086	25A3	IDE Controller	11
00	1F	03	8086	25A4	Serial Bus	5
00	1F	05	8086	25A6	Audio	5
02	01	00	8086	1075	Ethernet	11
03	01	00	177D	0003	Encrypt/Decrypt	9
03	02	00	8086	1079	Ethernet	9
03	02	01	8086	1079	Ethernet	9
03	03	00	8086	1079	Ethernet	9
03	03	01	8086	1079	Ethernet	9
04	02	00	8086	1209	Ethernet	11
04	03	00	8086	1209	Ethernet	5

Evaluating BIOS Options ...

Launch BIOS Extension to setup ROMMON

Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST
2006

Platform ASA5510-K8

Use BREAK or ESC to interrupt boot.

Use SPACE to begin boot immediately.

Launching BootLoader...

Default configuration file contains 1 entry.

Searching / for images to boot.

Loading /asa821-k8.bin... Booting...

Loading...

Processor memory 177934336, Reserved memory: 20971520 (DSOs: 0 + kernel: 20971520)

Guest RAM start: 0xd4000080

Guest RAM end: 0xdd400000

Guest RAM brk: 0xd4001000

IO memory 51224576 bytes

IO memory start: 0xd0bff000

IO memory end: 0xd3cd9000

Total SSMS found: 0

Total NICs found: 7

mcwa i82557 Ethernet at irq 11 MAC: 0019.e8d9.6271

mcwa i82557 Ethernet at irq 5 MAC: 0000.0001.0001

i82546GB rev03 Ethernet @ irq09 dev 3 index 00 MAC: 0019.e8d9.6272

i82546GB rev03 Ethernet @ irq09 dev 3 index 01 MAC: 0019.e8d9.6273

i82546GB rev03 Ethernet @ irq09 dev 2 index 02 MAC: 0019.e8d9.6274

i82546GB rev03 Ethernet @ irq09 dev 2 index 03 MAC: 0019.e8d9.6275

i82547GI rev00 Gigabit Ethernet @ irq11 dev 1 index 05 MAC:

0000.0001.0002

Licensed features for this platform:

Maximum Physical Interfaces : Unlimited

Maximum VLANs : 100

Inside Hosts : Unlimited

Failover : Active/Active

VPN-DES : Enabled

VPN-3DES-AES : Enabled

Security Contexts : 5

GTP/GPRS : Disabled

VPN Peers : 250

WebVPN Peers : 100

AnyConnect for Mobile : Disabled

AnyConnect for Linksys phone : Disabled

Advanced Endpoint Assessment : Disabled

UC Proxy Sessions : 2

This platform has an ASA 5510 Security Plus license.

Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)

Boot microcode : CN1000-MC-BOOT-2.00

SSL/IKE microcode: CNLite-MC-SSLm-

PLUS-2.03

IPSec microcode : CNlite-MC-IPSECM-

MAIN-2.05

Creating context 'system'... Done. (0)

Creating context 'null'... Done. (257)

Cisco Adaptive Security Appliance Software Version 8.0(4) <system>

***** Warning

This product contains cryptographic features and is subject to United States and local country laws governing, import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

***** Warning

Copyright (c) 1996-2008 by Cisco Systems, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

INFO: Admin context is required to get the interfaces

*** Output from config line 20, "arp timeout 14400"

Creating context 'admin'... Done. (1)

*** Output from config line 23, "admin-context admin"

Cryptochecksum (changed): cf287bec dd6e8cf1 b96cbba9 ca2251ec

*** Output from config line 25, " config-url flash:/admi..."

```
Cryptochecksum (changed): 6f50b7d4 8539ef8c b6c4265c 7c8ef765
Type help or '?' for a list of available commands.
ciscoasa> en
Password:
ciscoasa#
```

```
ciscoasa# show mode
Security context mode: multiple
ciscoasa#
```

It is very important to create contexts with an exact name as it was specified in the task. Context names are case sensitive.

Also, physical interfaces must be up when allocating to the context. If not, they will not be operative inside the context and it is very common mistake.

Note that you can allocate the same physical interface to difference contexts. It is called "interface sharing" and will be described in more details in the following sections.

```
ciscoasa# conf t
ciscoasa(config)# int e0/0
ciscoasa(config-if)# no sh
ciscoasa(config-if)# int e0/1
ciscoasa(config-if)# no sh
ciscoasa(config-if)# int e0/2
ciscoasa(config-if)# no sh
ciscoasa(config-if)# int e0/3
ciscoasa(config-if)# no sh

ciscoasa(config-if)# int e0/2.105
ciscoasa(config-subif)# vlan 105
ciscoasa(config-subif)# exit

ciscoasa(config)# context CTX1
Creating context 'CTX1'... Done. (2)
ciscoasa(config-ctx)# config-url flash:/CTX1.CFG
INFO: Converting flash:/CTX1.CFG to disk0:/CTX1.CFG

WARNING: Could not fetch the URL disk0:/CTX1.CFG
INFO: Creating context with default config
```

Note that there is no CTX1.CFG file on the flash/disk0 so that the ASA creates a new file with basic configuration template. Be careful here as if there was a file on the flash with the same name already, the ASA would import that file as a configuration of the context. Thus, the best option is to do "sh flash" and check if there is such file

already.

Another thing is that the ASA does not write the file to the flash if you do not save the config either within the context ("write mem") or for all contexts within system mode ("write mem all").

```
ciscoasa(config-ctx)# allocate-interface e0/0 Outside
ciscoasa(config-ctx)# allocate-interface e0/1 Inside
ciscoasa(config-ctx)# allocate-interface e0/2.105 DMZ
```

When allocating interfaces to the context you can specify the name for that interface within the context. This is NOT nameif! This is just a name for the "physical" interface. There is also additional keyword at the end of that command:

- visible - all physical properties for that interface will be visible inside the context ("show interface" shows that info)
- invisible - only limited info will be displayed using "show interface" command, and this is the default.

```
ciscoasa(config-ctx)# context CTX2
Creating context 'CTX2'... Done. (3)
```

```
ciscoasa(config-ctx)# config-url flash:/CTX2.CFG
INFO: Converting flash:/CTX2.CFG to disk0:/CTX2.CFG
```

```
WARNING: Could not fetch the URL disk0:/CTX2.CFG
INFO: Creating context with default config
```

```
ciscoasa(config-ctx)# allocate-interface e0/0 Outside
ciscoasa(config-ctx)# allocate-interface e0/3 Inside
ciscoasa(config-ctx)# exit
```

Step 2 Switchport configuration where ASA DMZ interface is connected.

```
SW3(config)#int f0/12
SW3(config-if)#switchport trunk encapsulation dot1q
SW3(config-if)#switchport mode trunk
SW3(config-if)#exi
SW3(config)#vlan 105
SW3(config-vlan)#exi
```

Verification

```
ciscoasa(config)# sh mode
Security context mode: multiple
```

ciscoasa(config)# sh context

Context Name	Class	Interfaces	URL
*admin	default		disk0:/admin.cfg
CTX1	default	Ethernet0/0,Ethernet0/1, disk0:/CTX1.CFG Ethernet0/2.105	
CTX2	default	Ethernet0/0,Ethernet0/3 disk0:/CTX2.CFG	

Total active Security Contexts: 3

ciscoasa(config)# sh context detail

Context "system", is a system resource

Config URL: startup-config

Real Interfaces:

Mapped Interfaces: Ethernet0/0, Ethernet0/1, Ethernet0/2,
Ethernet0/2.105, Ethernet0/3, Management0/0, Virtual254

Class: default, Flags: 0x00000819, ID: 0

Context "admin", has been created

Config URL: disk0:/admin.cfg

Real Interfaces:

Mapped Interfaces:

Real IPS Sensors:

Mapped IPS Sensors:

Class: default, Flags: 0x00000813, ID: 1

Context "CTX1", has been created

Config URL: disk0:/CTX1.CFG

Real Interfaces: Ethernet0/0, Ethernet0/1, Ethernet0/2.105

Mapped Interfaces: DMZ, Inside, Outside

Real IPS Sensors:

Mapped IPS Sensors:

Class: default, Flags: 0x00000811, ID: 2

Context "CTX2", has been created

Config URL: disk0:/CTX2.CFG

Real Interfaces: Ethernet0/0, Ethernet0/3

Mapped Interfaces: Inside, Outside

Real IPS Sensors:

Mapped IPS Sensors:

Class: default, Flags: 0x00000811, ID: 3

Context "null", is a system resource

Config URL: ... null ...

Real Interfaces:

Mapped Interfaces:

Real IPS Sensors:

Mapped IPS Sensors:

Class: default, Flags: 0x00000809, ID: 257

Task 2

Configure ASA so that it will assign the following resources to the newly created contexts:

Context CTX1 Policy	ASDM Connections	2
	Connections	1000
	SSH Sessions	2
	Telnet Sessions	1
	XLATE Objects	300
Context CTX2 Policy	ASDM Connections	4
	Connections	2000
	SSH Sessions	5
	Telnet Sessions	1
	XLATE Objects	1000



Sharing hardware resources is always risky and may lead to performance issues when one context uses more resources than the others. In that case it is wise to limit resources per context. ASA by default limits some resources which are allocated to the contexts. However, those limits can be too lax for some organizations and the administrator can change them.

Here's the list of resources which can be limited:

- *mac-address - the number of MAC addresses allowed in the MAC address table (only on transparent firewall)*
- *conns - TCP/UDP connections between any two hosts*
- *inspects - application inspections rate*
- *hosts - the number of hosts that can connect through the ASA*
- *asdm - concurrent ASDM management sessions*
- *ssh - concurrent SSH sessions*
- *syslogs - system logs messages rate*
- *telnet - concurrent telnet sessions*
- *xlates - concurrent address translations*

Limiting the resources is nothing else like configuration of special class where the above resources are allocated. This class is then assigned to the context using "member <class-name>" command.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa(config)# class CTX1
ciscoasa(config-class)# limit-resource ASDM 2
ciscoasa(config-class)# limit-resource Conns 1000
ciscoasa(config-class)# limit-resource SSH 2
ciscoasa(config-class)# limit-resource Telnet 1
ciscoasa(config-class)# limit-resource xlate 300

ciscoasa(config-class)# class CTX2
ciscoasa(config-class)# limit-resource ASDM 4
ciscoasa(config-class)# limit-resource conn 2000
ciscoasa(config-class)# limit-resource telnet 1
ciscoasa(config-class)# limit-resource xlate 1000
```

Note that you do not need to configure SSH resources as this number will be inherited from the default class. All resources are set to unlimited, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions - 5 sessions,
- SSH sessions - 5 sessions,
- IPSec sessions - 5 sessions,
- MAC addresses - 65,535 entries.

```
ciscoasa(config-class)# context CTX1
ciscoasa(config-ctx)# member CTX1
ciscoasa(config-ctx)# context CTX2
ciscoasa(config-ctx)# member CTX2
ciscociscoasa(config-ctx)# exit
```

Verification

```
ciscoasa(config)# sh run all class
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

class CTX1
  limit-resource ASDM 2
  limit-resource Conns 1000
```

```

limit-resource SSH 2
limit-resource Telnet 1
limit-resource Xlates 300
!

```

```

class CTX2
  limit-resource ASDM 4
  limit-resource Conns 2000
  limit-resource Telnet 1
  limit-resource Xlates 1000
!

```

ciscoasa(config)# sh class default

Class Name	Members	ID	Flags
default	All	1	0001

ciscoasa(config)# sh class CTX1

Class Name	Members	ID	Flags
CTX1	1	2	0000

ciscoasa(config)# sh class CTX2

Class Name	Members	ID	Flags
CTX2	1	3	0000

ciscociscoasa(config)# sh context detail CTX1

```

Context "CTX1", has been created
  Config URL: disk0:/CTX1.CFG
  Real Interfaces: Ethernet0/0, Ethernet0/1, Ethernet0/2.105
  Mapped Interfaces: DMZ, Inside, Outside
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: CTX1, Flags: 0x00000811, ID: 2

```

ciscociscoasa(config)# sh context detail CTX2

```

Context "CTX2", has been created
  Config URL: disk0:/CTX2.CFG
  Real Interfaces: Ethernet0/0, Ethernet0/3
  Mapped Interfaces: Inside, Outside
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: CTX2, Flags: 0x00000811, ID: 3

```

Task 3

Configure interfaces for new contexts as follow:

Context	Interface name	Security level	IP address
CTX1	Inside	100	10.1.101.10/24

	Outside	0	10.1.102.10/24
	DMZ	50	10.1.105.10/24
CTX2	Inside	80	10.1.104.10/24
	Outside	40	10.1.102.11/24



Now it's time to configure context. This is done exactly in the same way as it is in a single mode configuration. The one difference is the administrator needs to go to the respective context's config mode before entering command. Using command of "changeto context <context-name>" the administrator can move between contexts.

Note that in the context configuration you have access to all configuration command as it is in single config mode. In our case there are no physical interfaces visible inside the context, manually configured logical names are showed instead of that.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa(config)# changeto context CTX1
ciscoasa/CTX1(config)# int Inside
ciscoasa/CTX1(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.
ciscoasa/CTX1(config-if)# ip add 10.1.101.10 255.255.255.0
ciscoasa/CTX1(config-if)# int Outside
ciscoasa/CTX1(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
ciscoasa/CTX1(config-if)# ip add 10.1.102.10 255.255.255.0
ciscoasa/CTX1(config-if)# int DMZ
ciscoasa/CTX1(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa/CTX1(config-if)# security-level 50
ciscoasa/CTX1(config-if)# ip add 10.1.105.10 255.255.255.0

ciscoasa/CTX1(config-if)# changeto context CTX2
ciscoasa/CTX2(config)# int Inside
ciscoasa/CTX2(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.
ciscoasa/CTX2(config-if)# security-level 80
ciscoasa/CTX2(config-if)# ip add 10.1.104.10 255.255.255.0
ciscoasa/CTX2(config-if)# int Outside
```

```
ciscoasa/CTX2(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
ciscoasa/CTX2(config-if)# security-level 40
ciscoasa/CTX2(config-if)# ip add 10.1.102.11 255.255.255.0
ciscoasa/CTX2(config-if)# exit
```

Verification

ciscoasa/CTX2(config)# changeto context CTX1

ciscoasa/CTX1(config)# ping 10.1.101.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ciscoasa/CTX1(config)# ping 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ciscoasa/CTX1(config)# ping 10.1.105.5

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.105.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ciscoasa/CTX1(config)# changeto context CTX2

ciscoasa/CTX2(config)# ping 10.1.104.4

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.104.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ciscoasa/CTX2(config)# ping 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ciscoasa/CTX2(config)# ping 10.1.101.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:
No route to host 10.1.101.1
```

Success rate is 0 percent (0/1)

There is no route to this network as this is behind context CTX1.

Task 4

Ensure that R4 can ping R2 without configuring any access list. You are not allowed to configure any type of address translation to accomplish this task.



As you can see, you cannot ping R2 from R4. This is because there is no inspection for ICMP enabled or ACL on the outside interface allowing ICMP echo-reply packets back.

However, after enabling ICMP inspection in the CTX2 context, you'll see that you are still not able to ping R2. Let's do some quick troubleshooting to see the issue.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa(config)# changeto context CTX2

ciscoasa/CTX2(config)# policy-map global_policy
ciscoasa/CTX2(config-pmap)# class inspection_default
ciscoasa/CTX2(config-pmap-c)# inspect icmp
ciscoasa/CTX2(config-pmap-c)# exit
ciscoasa/CTX2(config-pmap)# exit
```

Verification

What's the problem?

R4#ping 10.1.102.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

ciscoasa/CTX2(config)# sh int Outside

Interface Outside "Outside", is up, line protocol is up

MAC address 0019.e8d9.6272, MTU 1500

IP address 10.1.102.11, subnet mask 255.255.255.0

Traffic Statistics for "Outside":

9 packets input, 630 bytes

17 packets output, 1556 bytes

0 packets dropped

ciscoasa/CTX2(config)# changeto context CTX1

ciscoasa/CTX1(config)# sh int Outside

Interface Outside "Outside", is up, line protocol is up

MAC address 0019.e8d9.6272, MTU 1500

IP address 10.1.102.10, subnet mask 255.255.255.0

Traffic Statistics for "Outside":

9 packets input, 630 bytes

7 packets output, 556 bytes

0 packets dropped

ciscoasa/CTX1(config)# changeto system

ciscoasa(config)# sh int e0/0

Interface Ethernet0/0 "", is up, line protocol is up

Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec

Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)

Available for allocation to a context

MAC address 0019.e8d9.6272, MTU not set

IP address unassigned

22 packets input, 2488 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 L2 decode drops

24 packets output, 2616 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 babbles, 0 late collisions, 0 deferred

0 lost carrier, 0 no carrier

input queue (curr/max packets): hardware (1/1) software (0/0)

output queue (curr/max packets): hardware (0/1) software (0/0)

Ping from R4 does not work. Take a quick look at the interface in both contexts and in the system context. As you can see the Outside interface in the contexts inherits MAC address from the physical interface. This is normal behavior and everything should work smooth as long as contexts are not sharing interfaces.

The problem with shared interface is that ASA must be able to properly classify incoming traffic and send it to an appropriate context. There are three methods to make it work:

Using unique interfaces

If only one context is associated with the ingress interface, the security appliance classifies the packet into that context. In transparent firewall mode, unique interfaces for contexts are required, so this method is used to classify packets at all times.

Unique MAC Addresses

If multiple contexts share an interface, then the classifier uses the interface MAC address. The ASA lets you assign a different MAC address in each context to the same shared interface, whether it is a shared physical interface or a shared subinterface. An upstream router cannot route directly to a context without unique MAC addresses. You can set the MAC addresses manually when you configure each interface, or you can automatically generate MAC addresses using "mac-address auto" command.

NAT Configuration

If you do not have unique MAC addresses, then the classifier intercepts the packet and performs a destination IP address lookup. All other fields are ignored; only the destination IP address is used. To use the destination address for classification, the classifier must have knowledge about the subnets located behind each security context. The classifier relies on the NAT configuration to determine the subnets in each context. The classifier matches the destination IP address to either a static command or a global command. In the case of the global command, the classifier does not need a matching nat command or an active NAT session to classify the packet.

As we are not allowed to use any NAT in our solution, the only choice left is to use different MAC addresses for each security context. We can use an automatic method configuring "mac-address auto" command in the system context.

Configuration

Complete these steps:

Step 2 ASA configuration.

```
ciscoasa/CTX2(config)# changeto system  
  
ciscoasa(config)# mac-address auto
```

Verification

```
ciscoasa(config)# changeto context CTX1  
  
ciscoasa/CTX1(config)# sh int Outside
```

```
Interface Outside "Outside", is up, line protocol is up
    MAC address 1200.0000.0200, MTU 1500
    IP address 10.1.102.10, subnet mask 255.255.255.0
Traffic Statistics for "Outside":
    11 packets input, 686 bytes
    8 packets output, 584 bytes
    0 packets dropped
```

ciscoasa/CTX1(config)# changeto context CTX2

ciscoasa/CTX2(config)# sh int Outside

```
Interface Outside "Outside", is up, line protocol is up
    MAC address 1200.0000.0300, MTU 1500
    IP address 10.1.102.11, subnet mask 255.255.255.0
Traffic Statistics for "Outside":
    11 packets input, 686 bytes
    18 packets output, 1584 bytes
    0 packets dropped
```

R2#sh arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.1.102.2	-	001b.533b.ea58	ARPA	FastEthernet0/0
Internet	10.1.102.10	0	1200.0000.0200	ARPA	FastEthernet0/0
Internet	10.1.102.11	0	1200.0000.0300	ARPA	FastEthernet0/0

As you can see, ASA uses different MAC addresses for each context. R2 also sees those addresses in its ARP table. However, R2 has no information how to route the traffic to R4, so we need to add static route.

Configuration

Complete these steps:

Step 3 R2 configuration.

```
R2(config)#ip route 10.1.104.0 255.255.255.0 10.1.102.11
```

Verification

R4#ping 10.1.102.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 5

Disable automatic MAC address generation and accomplish the same using network address translation.



OK, it is always good to see how it works with NAT. Hence, first disable MAC autogeneration and configure simple Dynamic PAT in CTX2 context. Let's translate all inside IP addresses to the address of the outside interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa/CTX2(config)# changeto system
ciscoasa(config)# no mac-address auto
```

Verification

R4#ping 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

It does not work when there are the same MAC addresses.

On ASA

```
ciscoasa(config)# changeto context CTX2

ciscoasa/CTX2(config)# nat (Inside) 1 0 0
ciscoasa/CTX2(config)# global (Outside) 1 interface
INFO: Outside interface address added to PAT pool
```

Verification

```
R4#ping 10.1.102.2 rep 10000
```

```
Type escape sequence to abort.
```

```
Sending 10000, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
ciscoasa/CTX2(config)# sh xlate detail
```

```
1 in use, 1 most used
```

```
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
```

```
      r - portmap, s - static
```

```
ICMP PAT from Inside:10.1.104.4/8 to Outside:10.1.102.11/63477 flags ri
```

Task 6

Assign IP address of 10.254.254.8/24 to the management interface of ASA.

Configure following limits for system resources on the admin context:

- limit ASDM connections 1
- limit SSH connections 1
- limit TELNET connections 1

Configure SSH and Telnet access to the device from anywhere on management interface. Authenticate users using local username/password of admin/cisco.



ASA has dedicated management interface which can be used for management only or in some cases it can be “converted” to the normal interface. It is recommended to use this interface for management of ASA, so it must be allocated to the admin context. Each of contexts configured can be set as admin context. If a context is marked as admin context administrators logging onto that context have rights to administer other contexts as well (including system context).

The admin context is created automatically when an administrator converts ASA to multi-context mode.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa/CTX2(config)# changeto system
```



```
ciscoasa(config)# admin-context admin
ciscoasa(config)# int m0/0
ciscoasa(config-if)# no sh

ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface Management0/0
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

WARNING: Could not fetch the URL disk0:/admin.cfg
INFO: Creating context with default config
INFO: Admin context will take some time to come up .... please
wait.

ciscoasa(config)# class CL-ADMIN
ciscoasa(config-class)# limit-resource ASDM 1
ciscoasa(config-class)# limit-resource SSH 1
ciscoasa(config-class)# limit-resource Telnet 1
ciscoasa(config-class)# context admin
ciscoasa(config-ctx)# member CL-ADMIN
ciscoasa(config-ctx)# changeto context admin

ciscoasa/admin(config)# int management0/0
ciscoasa/admin(config-if)# nameif management
INFO: Security level for "management" set to 0 by default.
ciscoasa/admin(config-if)# security 100
ciscoasa/admin(config-if)# ip add 10.254.254.8 255.255.255.0
ciscoasa/admin(config-if)# management-only

ciscoasa/admin(config)# username admin password cisco privilege 15

ciscoasa/admin(config)# aaa authentication ssh console LOCAL
ciscoasa/admin(config)# aaa authentication telnet console LOCAL

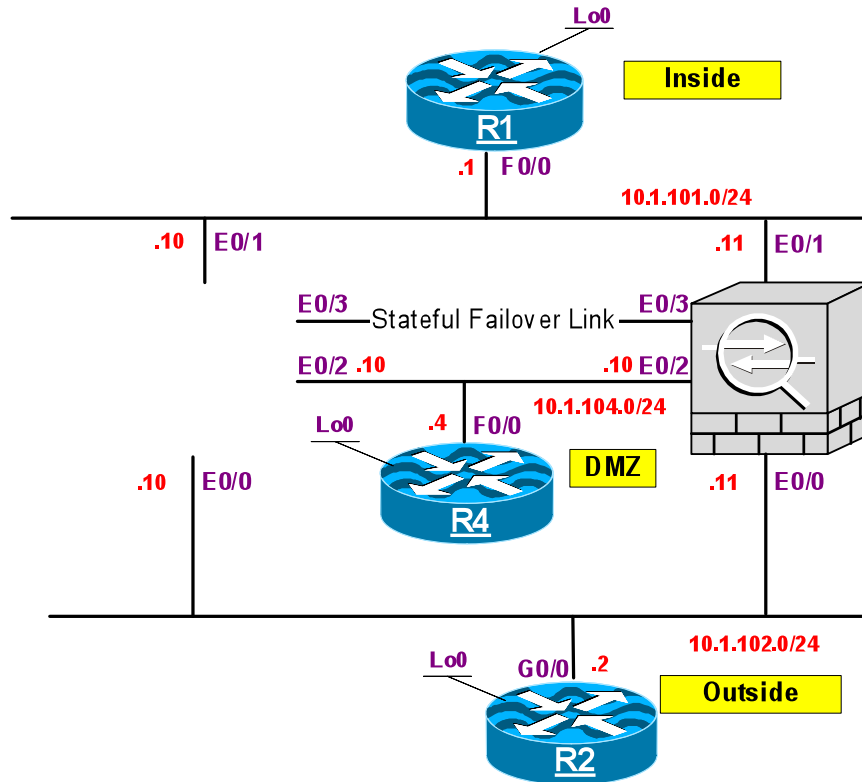
ciscoasa/admin(config)# telnet 0 0 management
ciscoasa/admin(config)# ssh 0 0 management
```

Verification

```
ciscoasa(config)# sh context detail admin
```

```
Context "admin", has been created
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: CL-ADMIN, Flags: 0x00000813, ID: 1
```


Lab 1.21. Active/Standby Failover



Lab Setup

- R1's F0/0 and ASA1/ASA2 E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1/ASA2 E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA1/ASA2 E0/2 interface should be configured in VLAN 104
- ASA1 and ASA2 E0/3 interface should be configured in VLAN 254
- Configure Telnet on all routers using password "cisco"
- Configure static default route on all routers pointing to ASA.

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24

Task 1

Configure ASA interfaces as follow:

Physical Interface	Interface name	Security level	IP address
E0/0	IN	80	Pri 10.1.101.10/24 Sby 10.1.101.11/24
E0/1	OUT	0	Pri 10.1.102.10/24 Sby 10.1.102.11/24
E0/2	DMZ	50	Pri 10.1.104.10/24 Sby 10.1.104.11/24

Configure ASA2 device to back up ASA1 firewall in the event of failure. Configure interface E0/3 as the Failover Link. This interface will be used to transmit failover control messages. Assign a name of LAN_FO and active IP address of 10.1.254.10/24 with a standby address of 10.1.254.11. Authenticate the failover control messages using a key of "cisco987". Configure host name of ASA-FW.



ASA failover uses a special link which must be configured appropriately to successfully monitor state of primary ASA device. This link is a dedicated physical Ethernet interface. The best practice is to use the fastest ASA interface possible as an amount of data traversing this link may be significant and usually depends on the amount of data traverses all remaining interfaces. This link may have two things to do (1) it must synchronize configuration, monitor ASA interfaces and send those information to second ASA to continue working if primary ASA fails (2) it may carry stateful information (like state table and translation table) to maintain all connections by second ASA in case of failure. Although, the first task does not require fast interface, the second may require significant bandwidth of the interface. In addition to that, this link shouldn't be set up using crossover cable. It is highly recommended to use switch for interconnection with PortFast configured on the switch port. In case of configuration, the interface used as failover link should be in UP state, meaning an administrator must enter "no shutdown" command on that interface. No other configuration is required. All failover configuration is done using "failover...." command. Two very important commands are required (1) "failover lan..." which is used for specifying what interface will be used as failover link and (2) "failover interface ip..." which configures IP address of that link (note the IP address is

configured here, not under the physical interface).

Note that all ASA interfaces must have standby IP addresses configured. It is usually omitted when ASA is already pre-configured and we need to add failover to the existing configuration. Those standby IP addresses will be used on secondary ASA as all interfaces must send out heartbeat information on their subnet to check if there is standby interface ready on a given subnet.

The first ASA must be "marked" as primary unit and second ASA as secondary unit. A good practice mandates usage of "encryption" key for securing failover communication.

Configuration of secondary ASA is similar to that it was on primary unit. All you need is to unshut failover interface and configure it in the same way as it was on primary device. The one difference is that secondary device must be marked as secondary unit.

The very last configuration command is simple "failover" which enables failover and starts communication between ASAs.

Note that you do not need to configure any IP addresses (except for failover link) on the secondary ASA. After enabling failover, all configuration should be sent to the second device.

Configuration

Complete these steps:

Step 1 Primary ASA configuration.

```
ciscoasa(config)# hostname ASA-FW

ASA-FW(config)# interface e0/0
ASA-FW(config-if)# nameif OUT
INFO: Security level for "OUT" set to 0 by default.
ASA-FW(config-if)# ip address 10.1.102.10 255.255.255.0 standby
10.1.102.11
ASA-FW(config-if)# no shut

ASA-FW(config-if)# interface e0/1
ASA-FW(config-if)# nameif IN
INFO: Security level for "IN" set to 0 by default.
ASA-FW(config-if)# security-level 80
ASA-FW(config-if)# ip address 10.1.101.10 255.255.255.0 standby
10.1.101.11
ASA-FW(config-if)# no shut

ASA-FW(config-if)# interface e0/2
```

```
ASA-FW(config-subif)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ASA-FW(config-subif)# security-level 50
ASA-FW(config-subif)# ip address 10.1.104.10 255.255.255.0 standby
10.1.104.11
ASA-FW(config-subif)# no shut
ASA-FW(config-subif)# exit

ASA-FW(config)# int e0/3
ASA-FW(config-if)# no sh
```

Do not forget to unshut that interface!

```
ASA-FW(config)# failover lan unit primary
ASA-FW(config)# failover lan interface LAN_FO e0/3
INFO: Non-failover interface config is cleared on Ethernet0/3 and
its sub-interfaces
ASA-FW(config)# failover interface ip LAN_FO 10.1.254.10
255.255.255.0 standby 10.1.254.11
ASA-FW(config)# failover key cisco987
ASA-FW(config)# failover
```

You must enable failover at the end of the configuration using "failover" command.

Step 2 Secondary ASA configuration.

```
ciscoasa(config)# int e0/3
ciscoasa(config-if)# no sh
```

Same on the secondary ASA. You must manually unshut the interface for LAN failover.

```
ciscoasa(config)# failover lan unit secondary
ciscoasa(config-if)# failover lan interface LAN_FO e0/3
INFO: Non-failover interface config is cleared on Ethernet0/3 and
its sub-interfaces
ciscoasa(config)# failover interface ip LAN_FO 10.1.254.10
255.255.255.0 standby 10.1.254.11
ciscoasa(config)# failover key cisco987
ciscoasa(config)# failover
ciscoasa(config)# .
```

```
Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.
```

```
ASA-FW(config)#

ASA-FW(config)# int e0/0
```

**** WARNING ****

Configuration Replication is NOT performed from Standby unit to Active unit.

Configurations are no longer synchronized.

Note that you cannot configure the ASA using being on the Standby unit. Although, it is possible to enable commands the config will NOT be synchronized between devices.

Verification

On Active ASA

ASA-FW(config)# sh failover

Failover On

Failover unit Primary

Failover LAN Interface: LAN_FO Ethernet0/3 (up)

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 250 maximum

Version: Ours 8.2(1), Mate 8.2(1)

Last Failover at: 17:08:59 UTC Jul 10 2010

This host: Primary - Active

Active time: 105 (sec)

slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)

Interface OUT (10.1.102.10): Normal

Interface IN (10.1.101.10): Normal

Interface DMZ (10.1.104.10): Normal

slot 1: empty

Other host: Secondary - Standby Ready

Active time: 291 (sec)

slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)

Interface OUT (10.1.102.11): Normal

Interface IN (10.1.101.11): Normal

Interface DMZ (10.1.104.11): Normal

slot 1: empty

Note the IP addresses in the brackets and "normal" state of those interfaces. The IP addresses are simply Active and Standby IP address configured on the interface. If you see 0.0.0.0 there, it means you do not have Standby IP address configured on a particular interface.

Also the state may be different. There may be Waiting, Non-Monitored and Normal states. Since the ASA does not monitor subinterfaces by default you may see Non-Monitored state very often when using subinterfaces. However, a Waiting state means there is a process of communicating between interfaces in the same subnet on both ASA units. If this state is displayed for too long (couple of

minutes) that means the ASA has communication issues with other ASA device - meaning issues with L2 (switch) in most cases.

Stateful Failover Logical Update Statistics

Link : Unconfigured.

It is highly recommended to perform failover test after configuration. Below is an example test which can easily verify if failover works fine.

1. Enable ICMP inspection to allow ICMP traffic go through the ASA
2. Start pinging R2 from R1 (Inside to Outside)
3. Make Standby ASA to become Active
4. Verify that failover took place and everything is OK in means of verification commands and check if ping is still going on.

FAILOVER TEST

1. Enable ICMP inspection on ASA (just to allow ICMP traffic to pass through the ASA)

```
ASA-FW(config)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect icmp
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

2. Perform repeated ping from R1

R1#ping 10.1.102.2 rep 1000

3. On standby ASA enter command "failover active" to become an active device

ASA-FW(config)# failover active

Switching to Active

ASA-FW(config)# sh failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Version: Ours 8.0(4), Mate 8.0(4)
Last Failover at: 23:14:41 UTC Oct 17 2009
This host: Secondary - Active
Active time: 22 (sec)
```

```

slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
  Interface OUT (10.1.102.10): Normal (Waiting)
  Interface IN (10.1.101.10): Normal (Waiting)
  Interface DMZ (10.1.104.10): Normal (Waiting)
slot 1: empty
Other host: Primary - Standby Ready
Active time: 740 (sec)
slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
  Interface OUT (10.1.102.11): Normal
  Interface IN (10.1.101.11): Normal
  Interface DMZ (10.1.104.11): Normal
slot 1: empty

Stateful Failover Logical Update Statistics
Link : Unconfigured.

```

Note that some of monitored interfaces have Waiting status. Do not worry. Just wait a bit and run "show failover" command again. This may takes a while for interfaces to see each other and update their status.

ASA-FW(config)# sh failover

```

Failover On
Failover unit Secondary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Version: Ours 8.0(4), Mate 8.0(4)
Last Failover at: 23:14:41 UTC Oct 17 2009
  This host: Secondary - Active
    Active time: 37 (sec)
    slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
      Interface OUT (10.1.102.10): Normal
      Interface IN (10.1.101.10): Normal
      Interface DMZ (10.1.104.10): Normal
    slot 1: empty
  Other host: Primary - Standby Ready
    Active time: 740 (sec)
    slot 0: ASA5510 hw/sw rev (2.0/8.0(4)) status (Up Sys)
      Interface OUT (10.1.102.11): Normal
      Interface IN (10.1.101.11): Normal
      Interface DMZ (10.1.104.11): Normal
    slot 1: empty

Stateful Failover Logical Update Statistics
Link : Unconfigured.

```

4. Check R1 ping:

[illegible]

Note that only one ping is lost. The failover is working quite fast.
Also keep in mind that you can use redundant interfaces along with failover.

Configure ASA so that it will maintain TCP connections (including HTTP) in the event of active device failure. Use the same interface which is already used for LAN Failover.



To use Stateful Failover, you must configure a Stateful Failover link to pass all state information. You have three options for configuring a Stateful Failover link:

- By default, ASA does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss.*

Configuration

Complete these steps:

Step 1 Active ASA configuration.

```
ASA-FW(config)# failover link LAN_FO
```

```
ASA-FW(config)# failover replication http
```

Verification

```
ASA-FW(config)# sh failover
```

```
Failover On
Failover unit Primary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
failover replication http
Version: Ours 8.2(1), Mate 8.2(1)
Last Failover at: 17:08:59 UTC Jul 10 2010

  This host: Primary - Active
    Active time: 695 (sec)
    slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
      Interface OUT (10.1.102.10): Normal
      Interface IN (10.1.101.10): Normal
      Interface DMZ (10.1.104.10): Normal
    slot 1: empty

  Other host: Secondary - Bulk Sync
    Active time: 291 (sec)
    slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
      Interface OUT (10.1.102.11): Normal
      Interface IN (10.1.101.11): Normal
      Interface DMZ (10.1.104.11): Normal
    slot 1: empty
```

Stateful Failover Logical Update Statistics

```
Link : LAN_FO Ethernet0/3 (up)
```

Stateful Obj	xmit	xerr	rcv	rerr
General	3	0	3	0
sys cmd	3	0	3	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	0	0	0	0

ARP tbl	0	0	0	0
Xlate_Timeout	0	0	0	0
VPN IKE upd	0	0	0	0
VPN IPSEC upd	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	8	3
Xmit Q:	0	26	36

ASA-FW(config)# sh failover interface

```
interface LAN_FO Ethernet0/3
    System IP Address: 10.1.254.10 255.255.255.0
    My IP Address      : 10.1.254.10
    Other IP Address   : 10.1.254.11
```

ASA-FW(config)# sh run all monitor

```
monitor-interface OUT
monitor-interface IN
monitor-interface DMZ
```

By default ASA monitors only physical interfaces; it does not monitor logical interfaces of subinterfaces. This must be manually enabled using "monitor-interface" command.

There is also a feature called Remote Command Execution which is very useful when making changes to the configuration in failover environment.

Because configuration commands are replicated from the active unit or context to the standby unit or context, you can use the "failover exec" command to enter configuration commands on the correct unit, no matter which unit you are logged-in to. For example, if you are logged-in to the standby unit, you can use the "failover exec active" command to send configuration changes to the active unit. Those changes are then replicated to the standby unit.

Task 3

Configure ASA so that it will use static MAC address on the outside interface in case standby device boots first. Use MAC address of 0011.0011.0011 as Active and 0022.0022.0022 as Standby.



MAC addresses for the interfaces on the primary unit are used for the interfaces on the active unit.

However, if both units are not brought online at the same time and the secondary unit boots first and becomes active, it uses the burned-in MAC addresses for its own interfaces. When the primary unit comes online, the secondary unit will obtain the MAC addresses from the primary unit. This change can disrupt network traffic. Configuring virtual MAC addresses for the interfaces ensures that the secondary unit uses the correct MAC address when it is the active unit, even if it comes online before the primary unit.

This command has no effect when ASA is configured for Active/Active failover. In A/A failover there is a command "mac address" under failover group.

Configuration

Complete these steps:

Step 1 Active ASA configuration.

```
ASA-FW(config)# failover mac address e0/0 0011.0011.0011
0022.0022.0022
```

Verification (on Active unit)

```
ASA-FW(config)# sh int out
```

```
Interface Ethernet0/0 "OUT", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 0011.0011.0011, MTU 1500
    IP address 10.1.102.10, subnet mask 255.255.255.0
    1440 packets input, 173626 bytes, 0 no buffer
    Received 50 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 L2 decode drops
    1401 packets output, 167906 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max packets): hardware (0/25) software (0/0)
    output queue (curr/max packets): hardware (0/3) software (0/0)
Traffic Statistics for "OUT":
  1400 packets input, 142518 bytes
  1401 packets output, 142508 bytes
```

```

0 packets dropped
1 minute input rate 0 pkts/sec, 24 bytes/sec
1 minute output rate 0 pkts/sec, 23 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 20 bytes/sec
5 minute output rate 0 pkts/sec, 20 bytes/sec
5 minute drop rate, 0 pkts/sec

```

Verification (on Standby unit)

ASA-FW(config)# sh int out

```

Interface Ethernet0/0 "OUT", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 0022.0022.0022, MTU 1500
    IP address 10.1.102.11, subnet mask 255.255.255.0
    10413 packets input, 1231356 bytes, 0 no buffer
    Received 9 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 L2 decode drops
    10427 packets output, 1232128 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max packets): hardware (1/5) software (0/0)
    output queue (curr/max packets): hardware (0/3) software (0/0)
Traffic Statistics for "OUT":
  10413 packets input, 1043922 bytes
  10427 packets output, 1043956 bytes
  0 packets dropped
  1 minute input rate 0 pkts/sec, 21 bytes/sec
  1 minute output rate 0 pkts/sec, 21 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec, 20 bytes/sec
  5 minute output rate 0 pkts/sec, 20 bytes/sec
  5 minute drop rate, 0 pkts/sec

```

ASA-FW(config)# failover exec mate sh failover

```

Failover On
Failover unit Secondary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
failover replication http
Version: Ours 8.2(1), Mate 8.2(1)
Last Failover at: 17:04:18 UTC Jul 10 2010
  This host: Secondary - Standby Ready

```

```
Active time: 291 (sec)
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
  Interface OUT (10.1.102.11): Normal
  Interface IN (10.1.101.11): Normal
  Interface DMZ (10.1.104.11): Normal
slot 1: empty
Other host: Primary - Active
Active time: 855 (sec)
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
  Interface OUT (10.1.102.10): Normal
  Interface IN (10.1.101.10): Normal
  Interface DMZ (10.1.104.10): Normal
slot 1: empty
```

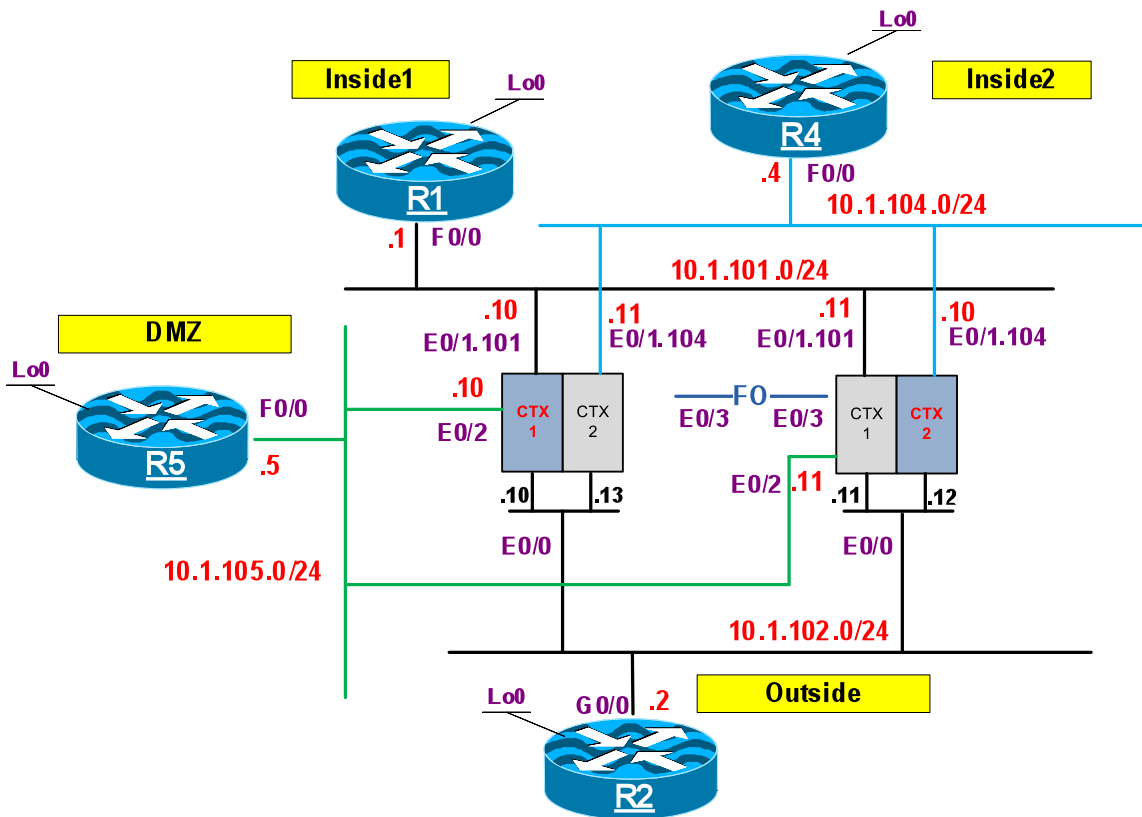
Stateful Failover Logical Update Statistics

```
Link : LAN_FO Ethernet0/3 (up)
Stateful Obj   xmit      xerr      rcv       rerr
General        24         0         24         0
sys cmd        24         0         24         0
up time        0         0         0         0
RPC services   0         0         0         0
TCP conn       0         0         0         0
UDP conn       0         0         0         0
ARP tbl        0         0         0         0
Xlate_Timeout  0         0         0         0
VPN IKE upd    0         0         0         0
VPN IPSEC upd  0         0         0         0
VPN CTCP upd   0         0         0         0
VPN SDI upd    0         0         0         0
VPN DHCP upd   0         0         0         0
SIP Session    0         0         0         0
```

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	5	219
Xmit Q:	0	1	24

Lab 1.22. Active/Active Failover



Lab Setup

- R2's G0/0 and ASA's' E0/0 interface should be configured in VLAN 102
- R5's F0/0 and ASA's' E0/2 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"
- Configure static default route on all routers pointing to ASA

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	G0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24

R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24

Task 1

Configure ASA1 with a hostname of ASA-FW and the following security contexts:

Context name:	CTX1	CTX2
Interfaces:	E0/0 – Outside E0/1.101 – Inside E0/2 – DMZ	E0/0 – Outside E0/1.104 – Inside
Context file:	CTX1.cfg	CTX2.cfg

The context configuration should be stored on the Flash memory.

Configure interfaces for new contexts as follow:

Context	Interface name	Security level	IP address
CTX1	Inside	100	10.1.101.10/24
	Outside	0	10.1.102.10/24
	DMZ	50	10.1.105.10/24
CTX2	Inside	100	10.1.104.10/24
	Outside	0	10.1.102.12/24



In the Active/Active (A/A) implementation of failover, both appliances in the failover pair process

traffic. To accomplish this, two contexts are needed, as is depicted in the diagram above. On the left appliance, CTX1 performs an active role and CTX2 a standby role. On the right appliance, CTX1 is standby and CTX2 is active.

The configuration required in this task is very similar to the configuration of single ASA device. The ASA must be converted to multiple mode, security contexts must be created and appropriate interfaces allocated. Then interfaces must be configured as requested inside respective context.

Configuration

Complete these steps:

Step 1 Switchport configuration where ASA inside interface is connected to.

```
SW3(config-if)#int f0/11
SW3(config-if)#sw tru enca dot
```

```
SW3(config-if)#sw mo tru
```

```
SW3(config)#vlan 101
SW3(config-vlan)#exi
SW3(config)#vlan 104
SW3(config-vlan)#exit
```

Step 2 On both ASA devices.

```
ciscoasa# conf t
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

<...output omitted...>
```

Step 3 ASA1 configuration.

```
ciscoasa(config)# hostname ASA-FW
ASA-FW(config)# int e0/0
ASA-FW(config-if)# no sh
ASA-FW(config-if)# int e0/1
ASA-FW(config-if)# no sh
ASA-FW(config-if)# int e0/1.101
ASA-FW(config-subif)# vlan 101
ASA-FW(config-subif)# no sh
ASA-FW(config-subif)# int e0/1.104
```

```
ASA-FW(config-subif)# vlan 104
ASA-FW(config-subif)# no sh
ASA-FW(config-subif)# int e0/2
ASA-FW(config-if)# no sh
ASA-FW(config-if)# context CTX1
Creating context 'CTX1'... Done. (2)
```

Depends on your previous configuration you may get a message saying:

ERROR: Identify admin context first, using the 'admin-context' command

Then, you need to create "admin" context first and tell the ASA to use that context for administrative purposes. Both things can be done using the following command:

```
ASA-FW(config)# admin-context admin
Creating context 'admin'... Done. (2)
```

Unfortunately, the above command does not specify when admin context is going to write its configuration. Hence, we need to specify that manually:

```
ASA-FW(config)# context admin
ASA-FW(config-ctx)# config-url disk0:/admin.ctx
```

```
WARNING: Could not fetch the URL disk0:/admin.ctx
INFO: Creating context with default config
INFO: Admin context will take some time to come up ....
please wait.
```

Note that it is wise to check if there is no file with previous configuration stored on the flash before configuring config URL. If there is a file with the same name already, it will be imported and used inside the context.

```
ASA-FW(config-ctx)# sh disk0: | in cfg|CFG
164 724          Oct 19 2009 18:38:50  admin.cfg
166 1437         Oct 19 2009 18:38:50  old_running.cfg
```

```
ASA-FW(config-ctx)# config-url disk0:CTX1.cfg
INFO: Converting disk0:CTX1.cfg to disk0:/CTX1.cfg
```

```
WARNING: Could not fetch the URL disk0:/CTX1.cfg
INFO: Creating context with default config
ASA-FW(config-ctx)# allocate-interface e0/1.101
ASA-FW(config-ctx)# allocate-interface e0/0
ASA-FW(config-ctx)# allocate-interface e0/2
```

```
ASA-FW(config-ctx)# context CTX2
Creating context 'CTX2'... Done. (3)
ASA-FW(config-ctx)# config-url disk0:CTX2.cfg
INFO: Converting disk0:CTX2.cfg to disk0:/CTX2.cfg

WARNING: Could not fetch the URL disk0:/CTX2.cfg
INFO: Creating context with default config
ASA-FW(config-ctx)# allocate-interface e0/1.104
ASA-FW(config-ctx)# allocate-interface e0/0

ASA-FW(config-ctx)# changeto context CTX1
ASA-FW/CTX1(config)# int e0/1.101
ASA-FW/CTX1(config-if)# ip add 10.1.101.10 255.255.255.0
ASA-FW/CTX1(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.

ASA-FW/CTX1(config-if)# int e0/0
ASA-FW/CTX1(config-if)# ip add 10.1.102.10 255.255.255.0
ASA-FW/CTX1(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.

ASA-FW/CTX1(config-if)# int e0/2
ASA-FW/CTX1(config-if)# ip add 10.1.105.10 255.255.255.0
ASA-FW/CTX1(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ASA-FW/CTX1(config-if)# security-level 50

ASA-FW/CTX1(config-if)# changeto context CTX2

ASA-FW/CTX2(config)# int e0/1.104
ASA-FW/CTX2(config-if)# ip add 10.1.104.10 255.255.255.0
ASA-FW/CTX2(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.

ASA-FW/CTX2(config-if)# int e0/0
ASA-FW/CTX2(config-if)# ip add 10.1.102.12 255.255.255.0
ASA-FW/CTX2(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
ASA-FW/CTX2(config-if)# exit
```

Verification

```
ASA-FW/CTX2(config)# ping 10.1.104.4
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 10.1.104.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ASA-FW/CTX2(config)# ping 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ASA-FW/CTX2(config)# sh int ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/1.104	10.1.104.10	YES	manual	up	up
Ethernet0/0	10.1.102.12	YES	manual	up	up

ASA-FW/CTX2(config)# changeto context CTX1

ASA-FW/CTX1(config)# ping 10.1.101.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ASA-FW/CTX1(config)# ping 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ASA-FW/CTX1(config)# ping 10.1.105.5

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.105.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ASA-FW/CTX1(config)# sh int ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/1.101	10.1.101.10	YES	manual	up	up
Ethernet0/2	10.1.105.10	YES	manual	up	up
Ethernet0/0	10.1.102.10	YES	manual	up	up

Task 2

Configure Active/Active failover between ASA1 and ASA2 so that the context CTX1 is active on ASA1 and standby on ASA2 whilst the context CTX2 is active on ASA2 and standby on ASA1. As there is a shared interface among both devices, ensure that packet classification is based on MAC addresses. Use interface E0/3 as failover

LAN and stateful link with IP address of 10.1.254.10/24 (VLAN 254). All standby IP addresses should be derived from the last octet of primary IP address plus one (e.g. if primary IP address is 10.1.1.10 the standby IP address will be 10.1.1.11). Secure failover transmission with a key of "cisco456".

Change the command line prompt to show hostname, context and current state of the context for better visibility.



In Active/Standby failover, failover is performed on a unit basis. One unit is active while the other unit is standby. In Active/Active, one context is active while the same context on the other ASA is in standby state.

ASA uses failover groups to manage contexts. Each ASA supports up to two failover groups as there can only be two ASAs in the failover pair. By default all security contexts are assigned to the failover group 1.

You can control the distribution of active contexts between the ASAs by controlling each context's membership in a failover group. Within the failover group configuration mode the "primary" command gives the primary ASA higher priority for failover group 1. However, the "secondary" command under failover group 2 gives secondary ASA higher priority for this failover group. Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously. If one unit boots before the other, both failover groups become active on that unit. When the other unit comes online, any failover groups that have the secondary unit as a priority do not become active on the second unit unless the failover group is configured with the "preempt" command or is manually forced using "no failover active" command.

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```
ASA-FW/CTX1(config)# changeto system
ASA-FW(config)# failover group 1
ASA-FW(config-fover-group)# primary
ASA-FW(config-fover-group)# preempt

ASA-FW(config-fover-group)# failover group 2
ASA-FW(config-fover-group)# secondary
ASA-FW(config-fover-group)# preempt
```



```
ASA-FW(config-fover-group)# context CTX1
ASA-FW(config-ctx)# join-failover-group 1
```

```
ASA-FW(config-ctx)# context CTX2
ASA-FW(config-ctx)# join-failover-group 2
ASA-FW(config-ctx)# exit
```

```
ASA-FW(config)# failover lan unit primary
ASA-FW(config)# int e0/3
ASA-FW(config-if)# no sh
ASA-FW(config)# failover lan interface LAN_FO e0/3
INFO: Non-failover interface config is cleared on Ethernet0/3 and
its sub-interfaces
ASA-FW(config)# failover interface ip LAN_FO 10.1.254.10
255.255.255.0 standby 10.1.254.11
ASA-FW(config)# failover key cisco456
ASA-FW(config)# failover link LAN_FO
ASA-FW(config)# failover
```

The failover configuration is exactly the same as it was for Active/Standby failover. Remember that when adding failover to the existing configuration, you must configure standby IP addresses for all interfaces inside the security contexts.

```
ASA-FW(config)# changeto con CTX2
```

```
ASA-FW/CTX2(config)# int e0/1.104
ASA-FW/CTX2(config-if)# ip add 10.1.104.10 255.255.255.0 standby
10.1.104.11
ASA-FW/CTX2(config-if)# int e0/0
ASA-FW/CTX2(config-if)# ip add 10.1.102.12 255.255.255.0 standby
10.1.102.13
```

```
ASA-FW(config)# changeto con CTX1
ASA-FW/CTX1(config)# int e0/1.101
ASA-FW/CTX1(config-if)# ip add 10.1.101.10 255.255.255.0 standby
10.1.101.11
ASA-FW/CTX1(config-if)# int e0/0
ASA-FW/CTX1(config-if)# ip add 10.1.102.10 255.255.255.0 standby
10.1.102.11
ASA-FW/CTX1(config-if)# int e0/2
ASA-FW/CTX1(config-if)# ip add 10.1.103.10 255.255.255.0 standby
10.1.103.11
ASA-FW/CTX1(config-if)# changeto system
```

In multiple context mode, you can view the extended prompt

when you log in to the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name. The ability to add information to a prompt allows you to see at-a-glance which adaptive security appliance you are logged into when you have multiple modules. During a failover, this feature is useful when both adaptive security appliances have the same hostname.

```
ASA-FW(config)# prompt hostname context priority state
ASA-FW/pri/act(config)#
```

Note that in Active/Active failover the ASA automatically generates different MAC addresses on shared interfaces. You do NOT need to configure "mac-address auto" in A/A failover scenario.

Step 2 Switchport configuration where ASA1 failover interface is connected to.

```
SW3(config)#int f0/13
SW3(config-if)#sw mo acc
SW3(config-if)#sw acc vl 254
% Access VLAN does not exist. Creating vlan 254
SW3(config-if)#exi
```

Step 3 Switchport configuration where ASA2 failover interface is connected to.

```
Switch(config)#ho SW4
SW4(config)#int f0/10
SW4(config-if)#sw mo acc
SW4(config-if)#sw acc vl 102
% Access VLAN does not exist. Creating vlan 102

SW4(config-if)#int f0/11
SW4(config-if)#sw tru enca dot
SW4(config-if)#sw mo tru

SW4(config-if)#int f0/12
SW4(config-if)#sw mo acc
SW4(config-if)#sw acc vl 105
% Access VLAN does not exist. Creating vlan 105

SW4(config-if)#int f0/13
SW4(config-if)#sw mo acc
SW4(config-if)#sw acc vl 254
% Access VLAN does not exist. Creating vlan 254
```

```
SW4(config-if)#int ran f0/19 - 24
SW4(config-if-range)#sw tru enca dot
SW4(config-if-range)#sw mo tru
SW4(config-if-range)#exi
```

```
SW4(config)#vlan 101
SW4(config-vlan)#exi
SW4(config)#vlan 104
SW4(config-vlan)#exi
```

Step 4 ASA2 configuration.

On secondary ASA there is only basic failover configuration required. After configuring and enabling failover, the secondary unit contacts the primary unit and copies configuration for all contexts and system execution space. As you can see both failover groups are active on the primary ASA at the beginning. However, after configuration replication the secondary ASA "preempts" failover group 2.

```
ciscoasa(config)# no failover
ciscoasa(config)# failover lan unit secondary
ciscoasa(config)# int e0/3
ciscoasa(config-if)# no sh
ciscoasa(config-if)# failover lan interface LAN_FO e0/3
INFO: Non-failover interface config is cleared on Ethernet0/3 and
its sub-interfaces
ciscoasa(config)# failover interface ip LAN_FO 10.1.254.10
255.255.255.0 standby 10.1.254.11
ciscoasa(config)# failover key cisco456
ciscoasa(config)# failover link LAN_FO
ciscoasa(config)# failover
ciscoasa(config)# .
```

Detected an Active mate

```
ciscoasa(config)# Removing context 'admin' (1)... Done
INFO: Admin context is required to get the interfaces
Creating context 'admin'... Done. (2)

WARNING: Skip fetching the URL disk0:/admin.cfg
INFO: Creating context with default config
INFO: Admin context will take some time to come up .... please
wait.
Creating context 'CTX1'... Done. (3)

WARNING: Skip fetching the URL disk0:/CTX1.cfg
INFO: Creating context with default config
Creating context 'CTX2'... Done. (4)
```

```
WARNING: Skip fetching the URL disk0:/CTX2.cfg
INFO: Creating context with default config
```

```
Group 1 Detected Active mate
```

```
Group 2 Detected Active mate
End configuration replication from mate.
```

```
Group 2 preempt mate
ASA-FW/sec/stby(config)#
```

Verification

```
ASA-FW/pri/act(config)# sh failover
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 3 of 250 maximum
```

```
Version: Ours 8.2(1), Mate 8.2(1)
```

```
Group 1 last failover at: 05:37:45 UTC Jul 17 2010
```

```
Group 2 last failover at: 05:47:42 UTC Jul 17 2010
```

```
This host: Primary
```

```
Group 1 State: Active
```

```
Active time: 701 (sec)
```

```
Group 2 State: Standby Ready
```

```
Active time: 597 (sec)
```

```
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
```

```
CTX1 Interface Inside (10.1.101.10): Normal (Not-Monitored)
```

```
CTX1 Interface Outside (10.1.102.10): Normal
```

```
CTX1 Interface DMZ (10.1.105.10): Normal
```

```
CTX2 Interface Inside (10.1.104.11): Normal (Not-Monitored)
```

```
CTX2 Interface Outside (10.1.102.13): Normal
```

```
slot 1: empty
```

```
Other host: Secondary
```

```
Group 1 State: Standby Ready
```

```
Active time: 0 (sec)
```

```
Group 2 State: Active
```

```
Active time: 103 (sec)
```

```
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
```

```
CTX1 Interface Inside (10.1.101.11): Normal (Not-Monitored)
```

```
CTX1 Interface Outside (10.1.102.11): Normal
CTX1 Interface DMZ (10.1.105.11): Normal
CTX2 Interface Inside (10.1.104.10): Normal (Not-Monitored)
CTX2 Interface Outside (10.1.102.12): Normal
slot 1: empty
```

Stateful Failover Logical Update Statistics

```
Link : LAN_FO Ethernet0/3 (up)
Stateful Obj   xmit      xerr      rcv       rerr
General        15         0         15         0
sys cmd         15         0         15         0
up time         0          0          0          0
RPC services    0          0          0          0
TCP conn        0          0          0          0
UDP conn        0          0          0          0
ARP tbl         0          0          0          0
Xlate_Timeout   0          0          0          0
SIP Session     0          0          0          0
```

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	1	16
Xmit Q:	0	1	16

Note that the status for Inside interface in both contexts is "Normal (Not-Monitored)". This is because by default ASA does not monitor subinterfaces or logical interfaces. To enable monitoring for those interfaces there should be "monitor-interface Inside" command configured in each of security contexts.

ASA-FW/pri/act(config)# sh failover group 1

Last Failover at: 05:37:45 UTC Jul 17 2010

This host: Primary
State: Active
Active time: 829 (sec)

```
CTX1 Interface Inside (10.1.101.10): Normal (Not-Monitored)
CTX1 Interface Outside (10.1.102.10): Normal
CTX1 Interface DMZ (10.1.105.10): Normal
```

Other host: Secondary
State: Standby Ready
Active time: 0 (sec)

```
CTX1 Interface Inside (10.1.101.11): Normal (Not-Monitored)
CTX1 Interface Outside (10.1.102.11): Normal
CTX1 Interface DMZ (10.1.105.11): Normal
```

Stateful Failover Logical Update Statistics

```
Status: Configured.
RPC services      0          0          0          0
TCP conn          0          0          0          0
UDP conn          0          0          0          0
ARP tbl           0          0          0          0
Xlate_Timeout     0          0          0          0
SIP Session       0          0          0          0
```

ASA-FW/pri/act(config)# sh failover group 2

Last Failover at: 05:47:42 UTC Jul 17 2010

This host: Primary
 State: Standby Ready
 Active time: 597 (sec)

CTX2 Interface Inside (10.1.104.11): Normal (Not-Monitored)
 CTX2 Interface Outside (10.1.102.13): Normal

Other host: Secondary
 State: Active
 Active time: 248 (sec)

CTX2 Interface Inside (10.1.104.10): Normal (Not-Monitored)
 CTX2 Interface Outside (10.1.102.12): Normal

Stateful Failover Logical Update Statistics

```
Status: Configured.
RPC services      0          0          0          0
TCP conn          0          0          0          0
UDP conn          0          0          0          0
ARP tbl           0          0          0          0
Xlate_Timeout     0          0          0          0
SIP Session       0          0          0          0
```

ASA-FW/pri/act(config)# sh failover interface

```
interface LAN_FO_Ethernet0/3
  System IP Address: 10.1.254.10 255.255.255.0
  My IP Address      : 10.1.254.10
  Other IP Address   : 10.1.254.11
```

ASA-FW/pri/act(config)# changeto context CTX1

ASA-FW/CTX1/pri/act(config)# sh int e0/0

Interface Ethernet0/0 "Outside", is up, line protocol is up
 MAC address 1200.0000.a300, MTU 1500
 IP address 10.1.102.10, subnet mask 255.255.255.0
 Traffic Statistics for "Outside":
 99 packets input, 7632 bytes

```
72 packets output, 6696 bytes
0 packets dropped
```

ASA-FW/CTX1/pri/act(config)# sh int e0/1.101

```
Interface Ethernet0/1.101 "Inside", is up, line protocol is up
  MAC address 1200.0165.03b0, MTU 1500
  IP address 10.1.101.10, subnet mask 255.255.255.0
  Traffic Statistics for "Inside":
    9 packets input, 684 bytes
    20 packets output, 920 bytes
    0 packets dropped
```

ASA-FW/CTX1/pri/act(config)# changeto context CTX2**ASA-FW/CTX2/pri/stby(config)# sh int e0/0**

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
  MAC address 1200.0000.04b5, MTU 1500
  IP address 10.1.102.13, subnet mask 255.255.255.0
  Traffic Statistics for "Outside":
    99 packets input, 7872 bytes
    81 packets output, 7268 bytes
    0 packets dropped
```

ASA-FW/CTX2/pri/stby(config)# sh int e0/1.104

```
Interface Ethernet0/1.104 "Inside", is up, line protocol is up
  MAC address 1200.0168.04b6, MTU 1500
  IP address 10.1.104.11, subnet mask 255.255.255.0
  Traffic Statistics for "Inside":
    12 packets input, 822 bytes
    25 packets output, 1060 bytes
    0 packets dropped
```

Note: Enable ICMP inspection in both security contexts to ease the verification. Since we are on Primary ASA in CTX2 security context (which is standby), we cannot configure any commands. However we can use Remote Command Execution feature to configure remotely Active context on the second device. Unfortunately, this tool cannot be used for changing security context ("changeto" command does not work). Hence, to make changes to CTX1 we need to do it manually.

ASA-FW/CTX2/pri/stby(config)# policy-map global_policy

```
**** WARNING ****
```

```
Configuration Replication is NOT performed from Standby unit to Active unit.
Configurations are no longer synchronized.
```

```
ASA-FW/CTX2/pri/stby(config-pmap)#
```

```
ASA-FW/CTX2/pri/stby(config-pmap)# exi
```

```
**** WARNING ****
```

```
Configuration Replication is NOT performed from Standby unit to Active unit.
Configurations are no longer synchronized.
```

ASA-FW/CTX2/pri/stby(config)# sh run policy-map

```
!  
policy-map type inspect dns preset_dns_map  
  parameters  
    message-length maximum 512  
policy-map global_policy  
  class inspection_default  
    inspect dns preset_dns_map  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect netbios  
    inspect rsh  
    inspect rtsp  
    inspect skinny  
    inspect esmtp  
    inspect sqlnet  
    inspect sunrpc  
    inspect tftp  
    inspect sip  
    inspect xdmcp
```

!
← Note: No ICMP Inspection

```
ASA-FW/CTX2/pri/stby(config)# failover exec mate policy-map global_policy  
ASA-FW/CTX2/pri/stby(config)# failover exec mate class inspection_default  
ASA-FW/CTX2/pri/stby(config)# failover exec mate inspect icmp
```

ASA-FW/CTX2/pri/stby(config)# sh run policy-map

```
!  
policy-map type inspect dns preset_dns_map  
  parameters  
    message-length maximum 512  
policy-map global_policy  
  class inspection_default  
    inspect dns preset_dns_map  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect netbios  
    inspect rsh  
    inspect rtsp  
    inspect skinny  
    inspect esmtp  
    inspect sqlnet  
    inspect sunrpc  
    inspect tftp  
    inspect sip  
    inspect xdmcp  
    inspect icmp ← ICMP Inspection is now enabled (configured on Active and synchronized  
                  over the Failover link)
```


!

ASA-FW/CTX2/pri/stby(config)# sh failover exec mate

Active unit Failover EXEC is at mpf-policy-map-class sub-command mode

ASA-FW/CTX2/pri/stby(config)# failover exec mate show run policy-map

!

policy-map type inspect dns preset_dns_map

parameters

message-length maximum 512

policy-map global_policy

class inspection_default

inspect dns preset_dns_map

inspect ftp

inspect h323 h225

inspect h323 ras

inspect netbios

inspect rsh

inspect rtsp

inspect skinny

inspect esmtp

inspect sqlnet

inspect sunrpc

inspect tftp

inspect sip

inspect xdmcp

inspect icmp

!

ASA-FW/CTX2/pri/stby(config)# changeto context CTX1

ASA-FW/CTX1/pri/act(config)# policy-map global_policy

ASA-FW/CTX1/pri/act(config-pmap)# class inspection_default

ASA-FW/CTX1/pri/act(config-pmap-c)# inspect icmp

ASA-FW/CTX1/pri/act(config-pmap-c)# exit

ASA-FW/CTX1/pri/act(config-pmap)# exit

R1#p 10.1.102.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#p 10.1.105.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.105.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R5#p 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

R4#p 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Ping on R4 is not successful because there is no route back on R2. It has nothing to do with ASA packets classification. After adding a route back, the ping is successful.

```
R2(config)#ip route 10.1.104.0 255.255.255.0 10.1.102.12
```

R4#p 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

It is highly recommended to perform failover test after configuration. The best test in this situation would be shutting down switch port for DMZ interface of CTX1 security context and check if failover "moves" CTX1 over to the secondary ASA.

FAILOVER TEST:

```
SW23#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#int f0/12
SW3(config-if)#shut
```

ASA-FW/CTX1/pri/stby(config)# changeto system**ASA-FW/pri/stby(config)# sh failover**

```
Failover On
Failover unit Primary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
```

Version: Ours 8.2(1), Mate 8.2(1)

Group 1 last failover at: 06:03:55 UTC Jul 17 2010

Group 2 last failover at: 05:47:42 UTC Jul 17 2010

This host: Primary

Group 1 State: Failed

Active time: 1570 (sec)

Group 2 State: Standby Ready

Active time: 597 (sec)

slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)

CTX1 Interface Inside (10.1.101.11): Normal (Not-Monitored)

CTX1 Interface Outside (10.1.102.11): Normal

CTX1 Interface DMZ (10.1.105.11): No Link (Waiting)

CTX2 Interface Inside (10.1.104.11): Normal (Not-Monitored)

CTX2 Interface Outside (10.1.102.13): Normal

slot 1: empty

Other host: Secondary

Group 1 State: Active

Active time: 40 (sec)

Group 2 State: Active

Active time: 1012 (sec)

slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)

CTX1 Interface Inside (10.1.101.10): Normal (Not-Monitored)

CTX1 Interface Outside (10.1.102.10): Normal

CTX1 Interface DMZ (10.1.105.10): Normal (Waiting)

CTX2 Interface Inside (10.1.104.10): Normal (Not-Monitored)

CTX2 Interface Outside (10.1.102.12): Normal

slot 1: empty

Stateful Failover Logical Update Statistics

Link : LAN_FO Ethernet0/3 (up)

Stateful Obj	xmit	xerr	rcv	rerr
General	139	0	138	0
sys cmd	136	0	136	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	0	0	0	0
ARP tbl	3	0	2	0
Xlate_Timeout	0	0	0	0
SIP Session	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	1	138
Xmit Q:	0	1	139

Note that now both security contexts are active on the secondary ASA.

We can bring the switch port back up now and see if primary ASA preempts CTX1 context.

Bring the switch port back up.

```
SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#int f0/12
SW3(config-if)#no shut
```

```
ASA-FW/pri/act(config)#
    Group 1 preempt mate
```

ASA-FW/pri/act(config)# sh failover

```
Failover On
Failover unit Primary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Version: Ours 8.2(1), Mate 8.2(1)
Group 1 last failover at: 06:07:48 UTC Jul 17 2010
Group 2 last failover at: 05:47:42 UTC Jul 17 2010
```

```
This host:    Primary
Group 1      State:      Active
              Active time: 1601 (sec)
Group 2      State:      Standby Ready
              Active time: 597 (sec)
```

```
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
  CTX1 Interface Inside (10.1.101.10): Normal (Not-Monitored)
  CTX1 Interface Outside (10.1.102.10): Normal (Waiting)
  CTX1 Interface DMZ (10.1.105.10): Normal (Waiting)
  CTX2 Interface Inside (10.1.104.11): Normal (Not-Monitored)
  CTX2 Interface Outside (10.1.102.13): Normal
slot 1: empty
```

```
Other host:   Secondary
Group 1      State:      Standby Ready
              Active time: 210 (sec)
Group 2      State:      Active
              Active time: 1215 (sec)
```

```
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
  CTX1 Interface Inside (10.1.101.11): Normal (Not-Monitored)
  CTX1 Interface Outside (10.1.102.11): Normal (Waiting)
  CTX1 Interface DMZ (10.1.105.11): Normal (Waiting)
  CTX2 Interface Inside (10.1.104.10): Normal (Not-Monitored)
```

```

    CTX2 Interface Outside (10.1.102.12): Normal
slot 1: empty

```

Stateful Failover Logical Update Statistics

```

Link : LAN_FO Ethernet0/3 (up)
Stateful Obj   xmit      xerr      rcv       rerr
General       166        0        165        0
sys cmd       163        0        163        0
up time        0         0         0         0
RPC services   0         0         0         0
TCP conn       0         0         0         0
UDP conn       0         0         0         0
ARP tbl        3         0         2         0
Xlate_Timeout  0         0         0         0
SIP Session    0         0         0         0

```

Logical Update Queue Information

```

           Cur      Max      Total
Recv Q:    0        1       165
Xmit Q:    0        1       166

```

You may see "Normal (Waiting)" state for DMZ link for a while. This is because the ASA uses keepalives between the interfaces to detect failure. Wait a bit and re-issue the command again.

If you see "waiting" state for a long time this may indicate problem with L2 configuration. Check if both interfaces are reachable and switchports are configured correctly.

ASA-FW/pri/act(config)# sh failover

```

Failover On
Failover unit Primary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Version: Ours 8.2(1), Mate 8.2(1)
Group 1 last failover at: 06:07:48 UTC Jul 17 2010
Group 2 last failover at: 05:47:42 UTC Jul 17 2010

```

```

This host:    Primary
Group 1      State:          Active
              Active time:   1711 (sec)
Group 2      State:          Standby Ready
              Active time:   597 (sec)

```

```

slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
  CTX1 Interface Inside (10.1.101.10): Normal (Not-Monitored)
  CTX1 Interface Outside (10.1.102.10): Normal
  CTX1 Interface DMZ (10.1.105.10): Normal
  CTX2 Interface Inside (10.1.104.11): Normal (Not-Monitored)

```

```

        CTX2 Interface Outside (10.1.102.13): Normal
slot 1: empty

Other host:   Secondary
Group 1       State:           Standby Ready
              Active time:    210 (sec)
Group 2       State:           Active
              Active time:    1325 (sec)

slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
        CTX1 Interface Inside (10.1.101.11): Normal (Not-Monitored)
        CTX1 Interface Outside (10.1.102.11): Normal
        CTX1 Interface DMZ (10.1.105.11): Normal
        CTX2 Interface Inside (10.1.104.10): Normal (Not-Monitored)
        CTX2 Interface Outside (10.1.102.12): Normal
slot 1: empty

Stateful Failover Logical Update Statistics
Link : LAN_FO Ethernet0/3 (up)
Stateful Obj   xmit      xerr      rcv       rerr
General        188        0         187        0
sys cmd        185        0         185        0
up time        0         0         0         0
RPC services   0         0         0         0
TCP conn       0         0         0         0
UDP conn       0         0         0         0
ARP tbl        3         0         2         0
Xlate_Timeout  0         0         0         0
SIP Session    0         0         0         0

Logical Update Queue Information
              Cur      Max      Total
Recv Q:      0       1       187
Xmit Q:      0       1       188

```

Task 3

To improve failover speed between two ASAs, configure both, unit and interface poll time to exchange hello packets on every 500ms. Set the hold time to 5sec. Also, ensure that the ASA will perform switchover for context CTX1 if minimum two interfaces fail. Configure ASA to monitor all its interfaces.



If you want failover to occur faster, decrease the failover unit poll time, which specifies how often hello messages are sent on the failover link. The hold time value specifies the amount of time that ASA will wait (after lost three consecutive hellos) before declaring the peer unit failed and triggering a failover.

You can also specify those parameters for monitored interfaces, as ASA sends hello packets out of each monitored data interface to monitor interface health.

Also, there is a default failover policy which specifies a percentage or a number of the interfaces which must failed before ASA triggers a failover. The default is 1 meaning the failover will trigger when only one interface fails.

Configuration

Complete these steps:

Step 1 Primary ASA configuration.

```
ASA-FW/pri/act(config)# changeto system

ASA-FW/pri/act(config)# failover polltime unit msec 500 holdtime 5

ASA-FW/pri/act(config)# failover group 1
ASA-FW/pri/act(config-fover-group)# interface-policy 2
ASA-FW/pri/act(config-fover-group)# polltime interface msec 500
holdtime 5

ASA-FW/pri/act(config-fover-group)# failover group 2
ASA-FW/pri/act(config-fover-group)# polltime interface msec 500
holdtime 5
ASA-FW/pri/act(config-fover-group)# exit
```

Note that Unit Polltime and Interface Policy are configured under the failover groups.

```
ASA-FW/pri/act(config)# changeto context CTX1
ASA-FW/CTX1/pri/act(config)# monitor-interface Inside
```

Interface monitoring is configured in each security context and this is only one command related to the failover configured in this place. This is because this is the place where the ASA has access to the IP address of the interface.

Rest of failover commands are configured under the system context.

```
ASA-FW/CTX1/pri/act(config)# changeto context CTX2
ASA-FW/CTX2/pri/stby(config)# failover exec active monitor-
```

```
interface Inside
```

Verification

ASA-FW/CTX2/pri/stby(config)# changeto system

ASA-FW/pri/act(config)# sh failover

```
Failover On
Failover unit Primary
Failover LAN Interface: LAN_FO Ethernet0/3 (up)
Unit Poll frequency 500 milliseconds, holdtime 5 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 250 maximum
Version: Ours 8.2(1), Mate 8.2(1)
Group 1 last failover at: 06:07:48 UTC Jul 17 2010
Group 2 last failover at: 05:47:42 UTC Jul 17 2010
```

```
This host:      Primary
Group 1         State:          Active
                  Active time:   3114 (sec)
Group 2         State:          Standby Ready
                  Active time:   597 (sec)
```

```
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
  CTX1 Interface Inside (10.1.101.10): Normal
  CTX1 Interface Outside (10.1.102.10): Normal
  CTX1 Interface DMZ (10.1.105.10): Normal
  CTX2 Interface Inside (10.1.104.11): Normal
  CTX2 Interface Outside (10.1.102.13): Normal
slot 1: empty
```

```
Other host:     Secondary
Group 1         State:          Standby Ready
                  Active time:   210 (sec)
Group 2         State:          Active
                  Active time:   2728 (sec)
```

```
slot 0: ASA5510 hw/sw rev (1.1/8.2(1)) status (Up Sys)
  CTX1 Interface Inside (10.1.101.11): Normal
  CTX1 Interface Outside (10.1.102.11): Normal
  CTX1 Interface DMZ (10.1.105.11): Normal
  CTX2 Interface Inside (10.1.104.10): Normal
  CTX2 Interface Outside (10.1.102.12): Normal
slot 1: empty
```

Stateful Failover Logical Update Statistics

Link : LAN_FO Ethernet0/3 (up)

Stateful Obj	xmit	xerr	rcv	rerr
General	368	0	367	0
sys cmd	365	0	365	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	0	0	0	0
ARP tbl	3	0	2	0
Xlate_Timeout	0	0	0	0
SIP Session	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	1	367
Xmit Q:	0	1	368

ASA-FW/pri/act(config)# changeto context CTX1

ASA-FW/CTX1/pri/act(config)# sh monitor-interface

```
This host: Primary - Active
  Interface Inside (10.1.101.10): Normal
  Interface Outside (10.1.102.10): Normal
  Interface DMZ (10.1.105.10): Normal
Other host: Secondary - Standby Ready
  Interface Inside (10.1.101.11): Normal
  Interface Outside (10.1.102.11): Normal
  Interface DMZ (10.1.105.11): Normal
```

ASA-FW/CTX1/pri/act(config)# changeto context CTX2

ASA-FW/CTX2/pri/stby(config)# sh monitor-interface

```
This host: Primary - Standby Ready
  Interface Inside (10.1.104.11): Normal
  Interface Outside (10.1.102.13): Normal
Other host: Secondary - Active
  Interface Inside (10.1.104.10): Normal
  Interface Outside (10.1.102.12): Normal
```

Task 4

You have been noticed by you company's networking team that they plan to deploy another router on the outside network to connect to another ISP for redundancy and load sharing. You must act proactively and ensure that any asymmetric traffic (including HTTP) caused by redundant ISPs will be handled by the ASA in both contexts.



In Active/Active designs, there is a greater chance for asymmetric routing. This means that one unit may receive a return packet for a connection originated through its peer unit. Because this unit does not have any connection information for this packet, the packet is dropped. This is most common when there are two ISPs with BGP and packet can return from a different ISP.

This can be prevented on the ASA by using ASR Groups (Asynchronous Routing Groups) configured on the interface inside the context. When an asr-group is configured on the interface and it receives a packet for which it has no session information, it checks the session information for the other interfaces that are in the same ASR Group. Then, instead of being dropped, the Layer 2 header is re-written and the packet is redirected to the other unit.

Configuration

Complete these steps:

Step 1 Primary ASA configuration.

```
ASA-FW/CTX2/pri/stby(config)# changeto system
ASA-FW/pri/act(config)# failover group 1
ASA-FW/pri/act(config-fover-group)# replication http
ASA-FW/pri/act(config-fover-group)# failover group 2
ASA-FW/pri/act(config-fover-group)# replication http
ASA-FW/pri/act(config-fover-group)# changeto context CTX1

ASA-FW/CTX1/pri/act(config)# interface e0/0
ASA-FW/CTX1/pri/act(config-if)# asr-group 1

ASA-FW/CTX1/pri/act(config-if)# changeto context CTX2
ASA-FW/CTX2/pri/stby(config)# failover exec active interface e0/0
ASA-FW/CTX2/pri/stby(config)# failover exec active asr-group 1
```

Verification

```
ASA-FW/CTX2/pri/stby(config)# failover exec active sh interface e0/0 detail
```

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
  MAC address 1200.0000.0400, MTU 1500
  IP address 10.1.102.12, subnet mask 255.255.255.0
  Traffic Statistics for "Outside":
    4015 packets input, 432772 bytes
    4012 packets output, 432696 bytes
    0 packets dropped
  Control Point Interface States:
    Interface number is 1
```

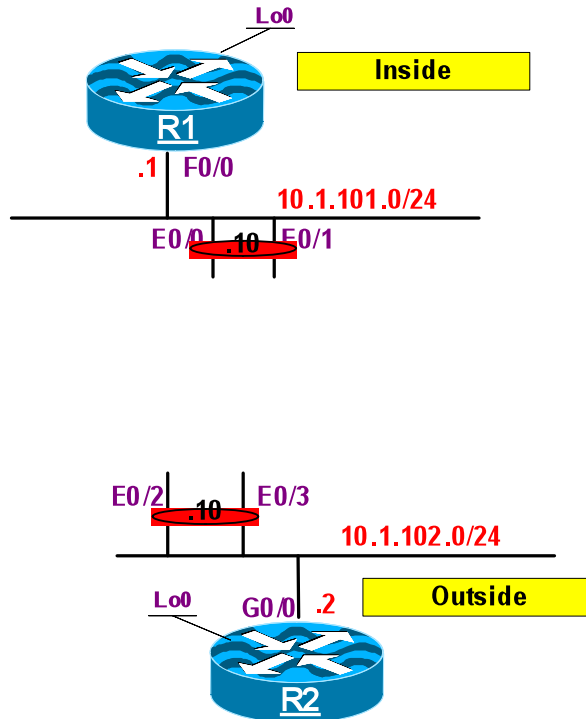
```
Interface config status is active
Interface state is active
Asymmetrical Routing Statistics:
  Received 0 packets
  Transmitted 0 packets
  Dropped 0 packets
```

ASA-FW/CTX2/pri/stby(config)# changeto context CTX1

ASA-FW/CTX1/pri/act(config)# sh interface e0/0 detail

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
  MAC address 1200.0000.0500, MTU 1500
  IP address 10.1.102.10, subnet mask 255.255.255.0
Traffic Statistics for "Outside":
  6088 packets input, 539738 bytes
  4105 packets output, 442420 bytes
  1955 packets dropped
Control Point Interface States:
  Interface number is 2
  Interface config status is active
  Interface state is active
Asymmetrical Routing Statistics:
  Received 0 packets
  Transmitted 0 packets
  Dropped 0 packets
```

Lab 1.23. Redundant Interfaces



Lab Setup

- R1's F0/0 and ASA1 E0/0 & E0/1 interfaces should be configured in VLAN 101.
- R2's G0/0 and ASA1 E0/2 & E0/3 interfaces should be configured in VLAN 102
- Configure Telnet on all routers using password "cisco"
- Configure static default route on all routers pointing to ASA.

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24

Task 1

Configure the following redundant interfaces on ASA1:

Interface name	Redundant1	Redundant2
Member physical interfaces	E0/0, E0/1	E0/2, E0/3
IP address	10.1.101.10/24	10.1.102.10/24
nameif	Inside	Outside
Security	100	0

Configure ASA1 with a hostname of ASA-FW.



A redundant interface is a logical interface made up of two physical interfaces. One physical interface serves as the active interface while the other serves as the standby. When active interface fails, the standby interface becomes active and starts passing traffic. It does not load share across both interfaces at the same time. A redundant interface is considered in failure state only when both of the underlying physical interfaces fail.

Up to eight redundant interface pairs can be configured. Both member interfaces must be of the same physical type (i.e. Ethernet) and have similar parameters configured (i.e. duplex, speed). There must not be any other logical parameters configured on member interfaces like nameif, security level or IP address. Those parameters must be first removed before adding physical interface to the redundant pair.

You can use redundant interface for failover link between two ASA devices. There must be switch between the ASAs and the same active link (redundant interface member) must be up on both sides of the link.

Be careful because when the active interface fails over to the standby interface, the redundant interface does not appear to be failed when being monitored for device-level failover.

The redundant interface uses the MAC address of the first physical interface you add. If you change the order of the member interfaces in the configuration, the MAC address changes to match the MAC address of the interface that is now listed first. You can assign a MAC address to the redundant interface, which is regardless of the member interface MAC address.

Also remember that there is no preemption between redundant interface members. If one member fails and then come back, it will not become an active member automatically.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa(config)# hostname ASA-FW
ASA-FW(config)# int e0/0
ASA-FW(config-if)# no sh
ASA-FW(config-if)# int e0/1
ASA-FW(config-if)# no sh
ASA-FW(config-if)# int e0/2
ASA-FW(config-if)# no sh
ASA-FW(config-if)# int e0/3
ASA-FW(config-if)# no sh

ASA-FW(config-if)# interface redundant 1
ASA-FW(config-if)# member-interface e0/0
INFO: security-level and IP address are cleared on Ethernet0/0.
ASA-FW(config-if)# member-interface e0/1
INFO: security-level and IP address are cleared on Ethernet0/1.
ASA-FW(config-if)# ip add 10.1.101.10 255.255.255.0
ASA-FW(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.
ASA-FW(config-if)# no sh

ASA-FW(config-if)# interface redundant 2
ASA-FW(config-if)# member-interface e0/2
INFO: security-level and IP address are cleared on Ethernet0/2.
ASA-FW(config-if)# member-interface e0/3
INFO: security-level and IP address are cleared on Ethernet0/3.
ASA-FW(config-if)# ip add 10.1.102.10 255.255.255.0
ASA-FW(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
ASA-FW(config-if)# no sh
ASA-FW(config-if)# exit
```

Verification

```
ASA-FW(config)# sh int red1
```

```
Interface Redundant1 "Inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 0019.e8d9.6272, MTU 1500
    IP address 10.1.101.10, subnet mask 255.255.255.0
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
358 L2 decode drops
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carrier, 0 no carrier
input queue (curr/max packets): hardware (8/25) software (0/0)
output queue (curr/max packets): hardware (0/0) software (0/0)

Traffic Statistics for "Inside":
0 packets input, 0 bytes
0 packets output, 0 bytes
0 packets dropped

1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec

Redundancy Information:
Member Ethernet0/0(Active), Ethernet0/1
Last switchover at 20:50:29 UTC Oct 19 2009
```

ASA-FW(config)# sh int e0/0

```
Interface Ethernet0/0 "", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
Active member of Redundant1
MAC address 0019.e8d9.6272, MTU not set
IP address unassigned
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
1 packets output, 64 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/255)
output queue (blocks free curr/low): hardware (255/254)
```

ASA-FW(config)# sh int red2

```
Interface Redundant2 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps, DLY 100 usec
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 0019.e8d9.6274, MTU 1500
IP address 10.1.102.10, subnet mask 255.255.255.0
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
33 L2 decode drops
0 packets output, 0 bytes, 0 underruns
```

```

0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carrier, 0 no carrier
input queue (curr/max packets): hardware (8/25) software (0/0)
output queue (curr/max packets): hardware (0/0) software (0/0)
Traffic Statistics for "Outside":
0 packets input, 0 bytes
0 packets output, 0 bytes
0 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
Redundancy Information:
Member Ethernet0/2(Active), Ethernet0/3
Last switchover at 20:51:11 UTC Oct 19 2009

```

See the Active member is by default first member added to the redundant interface pair. Also note that the MAC address of the redundant interface is inherited from the first member added to the configuration.

Now, it's time to test. Shut down switch port where E0/0 interface is connected.

TEST:

```

SW3(config)#int f0/10
SW3(config-if)#shut
SW3(config-if)#

```

ASA-FW(config)# sh int red1

```

Interface Redundant1 "Inside", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 0019.e8d9.6272, MTU 1500
IP address 10.1.101.10, subnet mask 255.255.255.0
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
358 L2 decode drops
1 packets output, 64 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carrier, 0 no carrier
input queue (curr/max packets): hardware (0/25) software (0/0)
output queue (curr/max packets): hardware (0/1) software (0/0)
Traffic Statistics for "Inside":
0 packets input, 0 bytes

```



```

    1 packets output, 28 bytes
    0 packets dropped
  1 minute input rate 0 pkts/sec,  0 bytes/sec
  1 minute output rate 0 pkts/sec,  0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec,  0 bytes/sec
  5 minute output rate 0 pkts/sec,  0 bytes/sec
  5 minute drop rate, 0 pkts/sec

```

Redundancy Information:

```

Member Ethernet0/1(Active), Ethernet0/0
Last switchover at 20:58:09 UTC Oct 19 2009

```

The second member interface has been promoted to Active state. Note that MAC address has not been changed. This is because it is inherited from the first member in the configuration - not from the Active member!

Now, bring the switch port back up.

```

SW3(config)#int f0/10
SW3(config-if)#no sh
SW3(config-if)#
%LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to up
SW3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up

```

ASA-FW(config)# sh int red1

```

Interface Redundant1 "Inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 0019.e8d9.6272, MTU 1500
    IP address 10.1.101.10, subnet mask 255.255.255.0
    109 packets input, 6985 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    358 L2 decode drops
    124 packets output, 8788 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max packets): hardware (1/25) software (0/0)
    output queue (curr/max packets): hardware (0/1) software (0/0)
Traffic Statistics for "Inside":
  109 packets input, 4503 bytes
  124 packets output, 6078 bytes
  0 packets dropped
  1 minute input rate 0 pkts/sec,  23 bytes/sec
  1 minute output rate 0 pkts/sec,  41 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec,  0 bytes/sec
  5 minute output rate 0 pkts/sec,  0 bytes/sec
  5 minute drop rate, 0 pkts/sec

```

Redundancy Information:

```
Member Ethernet0/1(Active), Ethernet0/0
Last switchover at 20:58:09 UTC Oct 19 2009
```

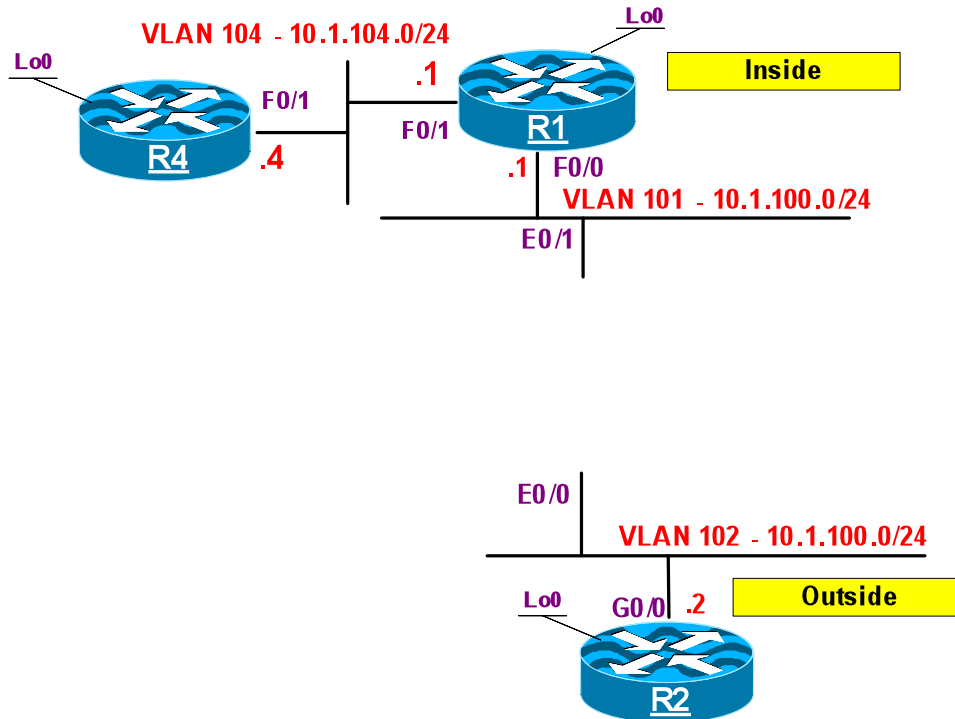
See that the Active interface did not change. This is because there is no preempt in the redundant interfaces. Active interface in the redundant pair can be changed using command "redundant-interface red1 active-member".

ASA-FW(config)# redundant-interface red1 active-member ethernet0/0

ASA-FW(config)# sh int red1

```
Interface Redundant1 "Inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 0019.e8d9.6272, MTU 1500
    IP address 10.1.101.10, subnet mask 255.255.255.0
    110 packets input, 7049 bytes, 0 no buffer
    Received 1 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    359 L2 decode drops
    125 packets output, 8852 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max packets): hardware (2/25) software (0/0)
    output queue (curr/max packets): hardware (0/2) software (0/0)
Traffic Statistics for "Inside":
  109 packets input, 4503 bytes
  125 packets output, 6106 bytes
  0 packets dropped
  1 minute input rate 0 pkts/sec,  0 bytes/sec
  1 minute output rate 0 pkts/sec,  0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec,  15 bytes/sec
  5 minute output rate 0 pkts/sec,  20 bytes/sec
  5 minute drop rate, 0 pkts/sec
Redundancy Information:
  Member Ethernet0/0(Active), Ethernet0/1
  Last switchover at 21:05:15 UTC Oct 19 2009
```

Lab 1.24. Transparent Firewall



Lab Setup

- R1's F0/0 and ASA1's E0/1 interfaces should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interfaces should be configured in VLAN 102
- R1's F0/1 and R4's F0/1 interfaces should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"

IP Addressing

Router	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.100.1/24
	F0/1	10.1.104.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.100.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24

Task 1

Configure the ASA as transparent firewall. Use interface E0/0 as the Outside and interface E0/1 as the Inside. Assign management IP address of 10.1.100.10/24 and allow connections via SSH from the inside networks only. Set SSH access password to "cisco123". Configure domain name of MicronicsTraining.com.



Traditionally, a firewall is a routed hop and acts as a default gateway for hosts in the local network. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire" and it not seen as a router hop to other devices. The ASA connects the same network on its inside and outside ports, but each interface resides on a different broadcast domain (different VLAN is used), so that the ASA performs secured transparent bridging between the two VLANs.

It is very useful and allows us to deploy a firewall in the network without IP readdressing or changing routing domain. However, the ASA in transparent mode differs from the routed mode in the following ways:

- *Supports only two data interfaces - you can use only Inside and Outside, no DMZ is allowed*
- *Require only one IP address - this IP address is assigned to the entire device and it's used for management purposes and to communicate the ASA with external services like AAA servers or SYSLOG.*
- *Bridges packets from one interface/VLAN to the other - there is no routing decision taking place, packets are bridged based on Layer 2 addresses.*
- *Can pass traffic that cannot be passed by a security appliance in routed mode - for example Layer 2 traffic like BPDU, IPX or MPLS.*

In addition to that ASA in transparent mode does not support:

- *Dynamic Domain Name System (DynDNS)*
 - *Dynamic routing protocols - however, you can use static routes for traffic originated on the ASA; dynamic routing protocols can be allowed to go through the ASA if ACL permits*
 - *IPv6*
 - *DHCP relay - the transparent ASA can act as DHCP server, but cannot act as DHCP relay, simply because it is no longer necessary as you can pass DHCP traffic through the ASA using ACL*
 - *Quality of Service (QoS)*
 - *Multicast - you can, however, allow multicast traffic through the ASA*
-

- *Virtual private network (VPN) termination - the transparent ASA supports only site-to-site VPN tunnels for management connections. It does not terminate remote access VPNs but it passes VPN traffic through using ACL.*

To set the firewall mode to transparent mode, use the "firewall transparent" command in global configuration mode. For multiple context mode, you can use only one firewall mode for all contexts (no mix of routed and transparent is possible). Hence, this command is located in the system execution space (however, it also appears in each context configuration just for informational purposes).

After changing the mode, the ASA clears the configuration because many commands are not supported in the transparent mode.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ciscoasa(config)# firewall transparent
```

Note that to change the firewall type back to Routed you must enter "no firewall transparent" command.

```
ciscoasa(config)# int e0/0
ciscoasa(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
ciscoasa(config-if)# no sh
```

```
ciscoasa(config-if)# int e0/1
ciscoasa(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.
ciscoasa(config-if)# no sh
```

```
ciscoasa(config-if)# ip add 10.1.100.10 255.255.255.0
```

```
ciscoasa(config)# domain-name MicronicsTraining.com
```

```
ciscoasa(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

```
ciscoasa(config)# ssh 0 0 inside
ciscoasa(config)# passwd cisco123
```

Verification

R1#ssh -l pix -c 3des 10.1.100.10

Password:
Type help or '?' for a list of available commands.
ciscoasa> exit

[Connection to 10.1.100.10 closed by foreign host]

There is a built-in username of "pix" which can be use for remote access. The password of this user is the same as enable password for the device.

R1#tel 10.1.100.2

Trying 10.1.100.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:39	
*514 vty 0		idle	00:00:00	10.1.100.1

Interface	User	Mode	Idle	Peer Address

R2>exit

[Connection to 10.1.100.2 closed by foreign host]

R1#sh arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.1.100.1	-	0012.8031.dcf8	ARPA	FastEthernet0/0
Internet	10.1.100.2	0	0011.9368.b380	ARPA	FastEthernet0/0
Internet	10.1.100.10	0	0018.7317.b0e1	ARPA	FastEthernet0/0
Internet	10.1.104.1	-	0012.8031.dcf9	ARPA	FastEthernet0/1

ciscoasa(config)# sh arp

Outside 10.1.100.2 0011.9368.b380 40
Inside 10.1.100.1 0012.8031.dcf8 40

Note that we see ARP table on the ASA but it is not used for traffic crossing the device.

Task 2

Configure a BGP neighbor relationship between R1 and R2 in AS 100. The neighbor relationship should be authenticated using key of "bgp123".



Just like any other routing protocol, BGP can be configured for authentication. You can configure MD5 authentication between two BGP peers, which means that each packet sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers. When you are configuring BGP peers with MD5 authentication that pass through an ASA, it is important to disable sequence number randomization because the sequence number is used by BGP peers to calculate the MD5 hash value.

The 16-bit hash value is produced using the following items:

- *the TCP pseudo-header (in the order: source IP address, destination IP address, zero-padded protocol number, and segment length)*
- *the TCP header, excluding options, and assuming a checksum of zero*
- *the TCP segment data (if any)*
- *an independently-specified key or password, known to both peers (BGP password)*

Then this MD5 hash is send over the BGP peer using TCP Option 19 in the TCP header. And here is another issue as the ASA automatically clears all TCP Options and forwards packets to the destination.

So, just to summarize up, two things must be done on the ASA to successfully establish BGP peering:

- *Sequence number randomization for BGP packets must be disabled*
- *TCP option 19 must be allowed in the BGP packets*

This can be done using so called TCP normalization features. Using tcp-map we can specify/match advanced options inside TCP header (it works like class-map but it is designed for TCP) and then in the policy-map we use "set connection" command (instead of "inspect") to perform an action on our matched traffic.

Without that configuration on ASA, the BGP authentication is broken and BGP peers display the following error message on the console:

%TCP-6-BADAUTH: No MD5 digest from 10.1.100.2(179) to 10.1.100.1(54787) (RST)

Configuration

Complete these steps:

Step 1 R1 BGP configuration.

```
R1(config)#router bgp 100
R1(config-router)#neighbor 10.1.100.2 remote-as 100
R1(config-router)#neighbor 10.1.100.2 password bgp123
```


Step 2 R2 BGP configuration.

```
R2(config)#router bgp 100
R2(config-router)#neighbor 10.1.100.1 remote-as 100
R2(config-router)#neighbor 10.1.100.1 password bgp123
```

Step 3 ASA configuration.

```
ciscoasa(config)# tcp-map BGPMAP
ciscoasa(config-tcp-map)# tcp-options range 19 19 allow

ciscoasa(config-tcp-map)# class-map BGP
ciscoasa(config-cmap)# match port tcp eq 179

ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class BGP
ciscoasa(config-pmap-c)# set connection random-sequence-number
disable
ciscoasa(config-pmap-c)# set connection advanced-options BGPMAP
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

Verification

```
R1(config-router)#
%TCP-6-BADAUTH: No MD5 digest from 10.1.100.2(179) to 10.1.100.1(21762) (RST)
R1(config-router)#
%TCP-6-BADAUTH: No MD5 digest from 10.1.100.2(179) to 10.1.100.1(21762) (RST)
```

R1#sh ip bgp summary

```
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1, main routing table version 1
```

```
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.100.2    4   100      0       0        0   0   0 never      Active
R1#
%BGP-5-ADJCHANGE: neighbor 10.1.100.2 Up
```

Be careful here as Active state in "show ip bgp summary" means that BGP actively trying to connect to its peer. There must be status of zero or any other number to be sure that BGP works fine.

R1#sh ip bgp summary

```
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1, main routing table version 1
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.100.2	4	100	5	5	1	0	0	00:01:52	0

Task 3

Configure the ASA so that it examines each ARP packet on the inside and outside interfaces before forwarding the packet. It should look in the static ARP table for a matching entry and if there is no match it should drop the packet. Create a static ARP entry for R1 and R2 Ethernet interfaces.



ARP packets are allowed through the transparent ASA in both directions by default without any ACL. However, you can control ARP packets by enabling ARP inspection.

This feature prevents malicious users from doing "man-in-the-middle" attack. For example, a host sends an ARP request to its default gateway, the default gateway router responds with its MAC address. The attacker can send another ARP response to the host with the attacker's MAC address instead of router's MAC address. Thus, the attacker can intercept traffic and forward it to the real default gateway, so that it is completely transparent to the user.

ARP inspection ensures that attacker cannot send an ARP response with its MAC address, as long as the correct MAC address and the associated IP address are in the static ARP table on the ASA.

You must configure static ARP entries before enabling ARP inspection. When you enable ARP inspection, the ASA compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table. The following rules are enforced:

- if the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.*
- if there is a mismatch between the MAC address, the IP address, or the interface, the ASA drops the packet.*
- if the ARP packet does not match any entries in the static ARP table, you can configure the ASA to either forward the packet out all interfaces (flood), or to drop the packet (no-flood).*

Configuration

Complete these steps:

Step 1 Check MAC address of R1.

```
R1#sh int f0/0 | in bia
Hardware is MV96340 Ethernet, address is 001b.533b.ce68 (bia
001b.533b.ce68)
```

Step 2 Check MAC address on R2.

```
R2#sh int g0/0 | in bia
Hardware is BCM1125 Internal MAC, address is 001b.533b.ea58 (bia
001b.533b.ea58)
```

First, we need to know MAC addresses for both hosts communicating. Then we need to configure those MAC addresses on the ASA and enable ARP inspection feature.

Step 3 Configure DAI on ASA.

```
ciscoasa(config)# arp inside 10.1.100.1 001b.533b.ce68
ciscoasa(config)# arp outside 10.1.100.2 001b.533b.ea58

ciscoasa(config)# arp-inspection inside enable no-flood
ciscoasa(config)# arp-inspection outside enable no-flood
```

Verification

```
ciscoasa(config)# sh arp-inspection
interface          arp-inspection      miss
-----
Outside            enabled              no-flood
Inside             enabled              no-flood
```

```
ciscoasa(config)# sh arp
Outside 10.1.100.2 001b.533b.ea58 -
Inside 10.1.100.1 001b.533b.ce68 -
```

```
R1#tel 10.1.100.2
Trying 10.1.100.2 ... Open
```

User Access Verification

```
Password:
R2>exit
```

[Connection to 10.1.100.2 closed by foreign host]

To verify, let's change MAC address on R1. Telnet connection does not work after MAC changing. Logs on the ASA indicate that ARP inspection blocked the traffic:

%ASA-3-322002: ARP inspection check failed for ARP response received from host 0011.0011.0011 on interface Inside. This host is advertising MAC Address 0011.0011.0011 for IP Address 10.1.100.1, which is statically bound to MAC Address 001b.533b.ce68

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#mac-address 0011.0011.0011
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#tel 10.1.100.2
Trying 10.1.100.2 ...
% Connection timed out; remote host not responding
```

Task 4

Remove the static MAC address from R1's F0/0 interface.

Configure R1 and R2 interface to be a part of OSPF Area 0. Ensure that routers successfully establish OSPF neighbor relationship.



By default only Layer 3 unicast traffic is passed through the ASA (from the interface with higher security level to the interface with lower security level). To permit Layer 3 broadcast or multicast packets through the ASA, you must configure an ACL with a Layer 3 destination address of 255.255.255.255 for broadcast or 224.x.x.x for multicast. The ACL must be applied in both directions (inside and outside) to allow adjacency forming for routing protocols like OSPF or EIGRP.

For OSPF you need to permit OSPF traffic (IP protocol 89) destined to the multicast address 224.0.0.5 and 224.0.0.6. As the OSPF updates are sending between DR and OTHER router using unicast it is needed to allow that traffic as well.

OSPF configuration on the routers may be different in real world and hence

there must be different ACL entries configured. Thus, it is recommended to enable logging on the ASA to see what OSPF packets are getting dropped and then build proper ACL base on that information.

Configuration

Complete these steps:

Step 1 Revert MAC addres on R1 and configure OSPF.

```
R1(config)#int f0/0
R1(config-if)#no mac-address 0011.0011.0011
R1(config-if)#router ospf 1
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0
```

Step 2 Configure OSPF on R2.

```
R2(config)#router ospf 1
R2(config-router)#network 0.0.0.0 0.0.0.0 area 0
```

Step 3 Allow OSPF to go through the ASA.

```
ciscoasa(config)# access-list OUTSIDE_IN permit 89 host 10.1.100.2
host 224.0.0.5
ciscoasa(config)# access-list OUTSIDE_IN permit 89 host 10.1.100.2
host 224.0.0.6
ciscoasa(config)# access-list OUTSIDE_IN permit 89 host 10.1.100.2
host 10.1.100.1
ciscoasa(config)# access-group OUTSIDE_IN in interface outside

ciscoasa(config)# access-list INSIDE_IN permit 89 host 10.1.100.1
host 224.0.0.5
ciscoasa(config)# access-list INSIDE_IN permit 89 host 10.1.100.1
host 224.0.0.6
ciscoasa(config)# access-list INSIDE_IN permit 89 host 10.1.100.1
host 10.1.100.2
ciscoasa(config)# access-group INSIDE_IN in interface inside
```

Verification

Message on R1

```
%OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from LOADING to FULL, Loading
Done
```

R1#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/DR	00:00:35	10.1.100.2	FastEthernet0/0

R2#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	1	FULL/BDR	00:00:35	10.1.100.1	FastEthernet0/0

Note that above access-list breaks BGP relationship previously configured as it blocks TCP/179 traffic. As BGP relation can be establish from both directions, there should be access-list entries allowing this.

Configuration

Complete these steps:

Step 4 Allow BGP to go through the ASA.

```
ciscoasa(config)# access-list OUTSIDE_IN permit tcp host 10.1.100.2
host 10.1.100.1 eq 179
ciscoasa(config)# access-list INSIDE_IN permit tcp host 10.1.100.1
host 10.1.100.2 eq 179
```

Verification

R1#sh ip bgp summ

BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1, main routing table version 1

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.100.2	4	100	33	37	1	0	0	00:00:43	0

Task 5

Configure ASA so that it translates R1's F0/0 IP address to the IP address of 10.1.105.1. Also, R4's F0/0 IP address should be translated to the IP address of 10.1.125.4. Ensure that Telnet works from R1 and R4 to R2's F0/0 interface and the translation takes place.



The ASA (version 8.0 and later) in transparent mode allows us to configure NAT for Layer 3 addresses traversing the firewall. This can be done in the same way as it is in routed mode. However, you must configure static routing on the ASA to upstream router if there is translation of not directly connected subnet. Also remember that you cannot configure interface PAT in the transparent mode as the ASA has no IP addresses on the interfaces.

Configuration

Complete these steps:

Step 1 Add default route on R4.

```
R4(config)#ip route 0.0.0.0 0.0.0.0 10.1.104.1
```

Step 2 Add static routes on R2.

```
R2(config)#ip route 10.1.125.4 255.255.255.255 10.1.100.1
R2(config)#ip route 10.1.105.1 255.255.255.255 10.1.100.1
```

Step 3 Configure ASA.

```
ciscoasa(config)# static (in,out) 10.1.105.1 10.1.100.1
ciscoasa(config)# static (in,out) 10.1.125.4 10.1.104.4

ciscoasa(config)# route inside 10.1.104.0 255.255.255.0 10.1.100.1

ciscoasa(config)# access-list INSIDE_IN permit tcp any any eq 23
```

Verification

R1#tel 10.1.100.2

Trying 10.1.100.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:23	

```
*514 vty 0          idle          00:00:00 10.1.105.1
```

Interface	User	Mode	Idle	Peer Address

```
R2>exit
```

```
[Connection to 10.1.100.2 closed by foreign host]
```

```
R4#tel 10.1.100.2
```

```
Trying 10.1.100.2 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R2>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:01:19	
*514 vty 0		idle	00:00:00	10.1.125.4

Interface	User	Mode	Idle	Peer Address

```
R2>exit
```

```
[Connection to 10.1.100.2 closed by foreign host]
```

```
ciscoasa(config)# sh xlate
```

```
2 in use, 2 most used
```

```
Global 10.1.105.1 Local 10.1.100.1
```

```
Global 10.1.125.4 Local 10.1.104.4
```

```
ciscoasa(config)# sh xlate detail
```

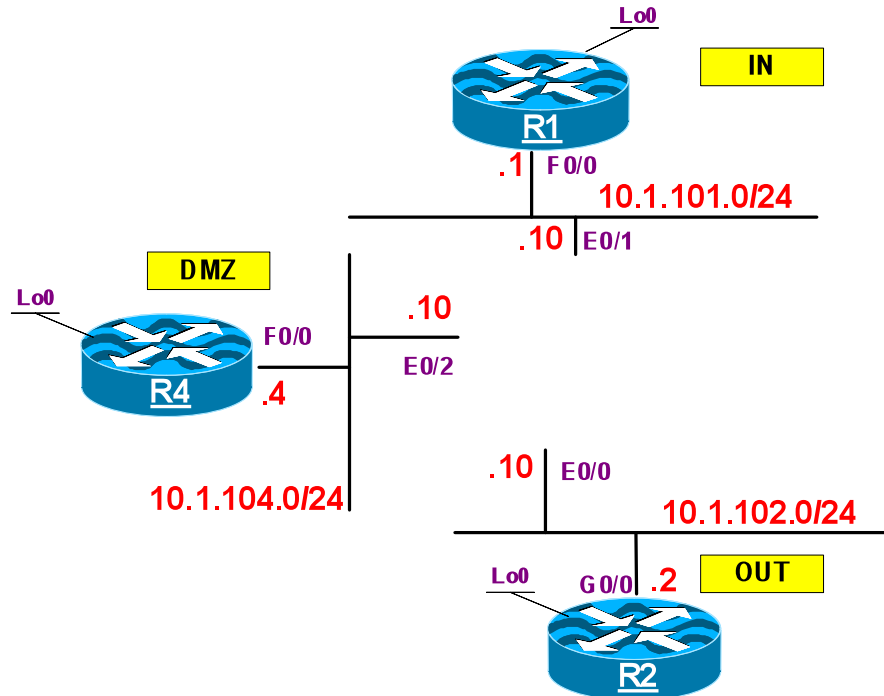
```
2 in use, 2 most used
```

```
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,  
       r - portmap, s - static
```

```
NAT from Inside:10.1.100.1 to Outside:10.1.105.1 flags s
```

```
NAT from Inside:10.1.104.4 to Outside:10.1.125.4 flags s
```


Lab 1.25. Threat Detection



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

On ASA configure Threat Detection feature so that it collects information about used protocols and hosts. Configure this feature to generate SYSLOG message when access-list drops packets at rate of 1000pkt/sec through 20 minutes or at 100pkt/sec burst rate.

If the attack is discovered block the attacker's host for 30 minutes.



The Threat Detection feature can help an administrator determine the level of severity for packets that are detected and dropped by the ASA. There are two types of threat detection:

- *Basic threat detection - tracks the rate at which threat-related packets are dropped and generates a SYSLOG message when rates exceed their thresholds*
- *Scanning thread detection - detects network sweeps and scans and optionally takes appropriate preventive action*

In addition the threat detection feature provides statistics for host-based, port-based and protocol-based information. Those statistics can help you detect activity that might be related to an attack, such as denial of service (DoS) attack. The basic threat detection is enabled by default on the ASA and can slightly affect performance when there are lots of drops.

Basic threat detection provides threat-related drop statistics by monitoring the following events:

- *Access list drops*
- *Bad packet format*
- *Exceeded connection limits*
- *Detection of DoS attacks*
- *Failed basic firewall checks*
- *Detection of suspicious ICMP packets*

- *Packets failing application inspection*
- *Interface overload*
- *Detection of scanning attacks*
- *Detection of incomplete sessions, such as TCP SYN attacks or no data UDP sessions attacks*

Each of these monitored events has a default rate limit (threshold). When this is exceeded a SYSLOG message (733100) is generated. The ASA tracks two types of rates for each monitored event: (1) the average event rate over an interval and (2) the burst event rate over a shorter burst interval (which is 1/60th of the average rate interval or 10 seconds, whichever is higher).

In our example the rate interval must be 20 minutes (1200 seconds), the average rate is 1000 packet drops per second and the burst rate is 100 drops per second. The calculated burst rate interval is 1/60 of 1200, which equals 20.

Scanning threat detection determines whether a scan is in progress by correlating the host database statistics over a specified host or subnet. If the default scanning threat rate threshold is exceeded, the ASA generates SYSLOG message 733101, which indicates that a host has been identified as a target or an attacker. You can configure scanning threat detection to perform automatic shunning (blocking a host), the ASA terminates connections from hosts identified as attackers and generates SYSLOG message. You can exempt host IP address from being shunned. Use "show threat-detection shun" command to view the shunned hosts and release a host from being shunned using "clear threat-detection shun" command.

You can configure the ASA to collect extensive threat detection statistics for hosts, protocols, ports and access lists. Statistics for access lists are enabled by default.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# threat-detection rate acl-drop rate-interval 1200
average-rate 1000 burst-rate 100
ASA-FW(config)# threat-detection scanning-threat shun duration 1800

ASA-FW(config)# threat-detection statistics host
ASA-FW(config)# threat-detection statistics protocol
```

Verification

R2#pi 10.1.101.1 rep 10000 time 0

Type escape sequence to abort.

Sending 10000, 100-byte ICMP Echos to 10.1.101.1, timeout is 0 seconds:

.....

<...output ommited...>

ASA-FW(config)# sh threat-detection statistics

Current monitored hosts:0 Total not monitored hosts:0

			Average(eps)	Current(eps)	Trigger	Total events
Top	Name	Id	Average(eps)	Current(eps)	Trigger	Total events
Top	Name	Id	Average(eps)	Current(eps)	Trigger	Total events
			Average(eps)	Current(eps)	Trigger	Total events
ICMP * 1: tot-ses:3 act-ses:0						
1-hour	Sent byte:		196	0	0	708600
8-hour	Sent byte:		24	738	0	708600
24-hour	Sent byte:		8	246	0	708600
1-hour	Sent pkts:		1	0	0	7086
8-hour	Sent pkts:		0	7	0	7086
24-hour	Sent pkts:		0	2	0	7086

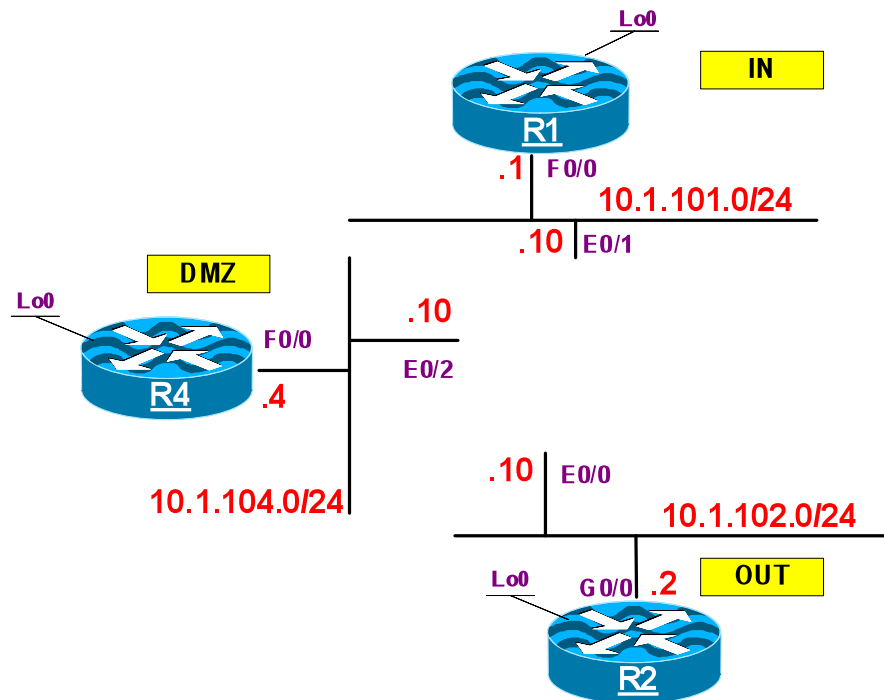
ASA-FW(config)# sh threat-detection rate acl-drop

		Average(eps)	Current(eps)	Trigger	Total events
10-min	ACL drop:	16	500	0	10000
20-min	ACL drop:	8	0	1	10000
1-hour	ACL drop:	2	0	0	10000

ASA-FW(config)# sh threat-detection shun

Shunned Host List:

Lab 1.26. Controlling ICMP and fragmented traffic



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

Configure ASA so that it can ping all outside networks, but nobody can ping ASA from the outside. Do not use ACL to accomplish this task.



ASA controls ICMP messages which are direct to the firewall in the other way than IOS router. There are special commands available to accept or not ICMP messages on the interfaces. By default ASA can be pinged from every side, however, pings directed to the broadcast address are dropped.

ICMP control works in inbound direction only, meaning you can configure what networks/hosts are allowed to send ICMP specified messages and on which ASA interface.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# icmp permit any echo-reply OUT
```

Simply speaking this command permits ICMP Echo Reply packets on outside interface. This means the ASA can send out ICMP Echo Request and will permit ICMP Echo Reply messages only.

Verification

```
ASA-FW(config)# sh run all icmp
icmp unreachable rate-limit 1 burst-size 1
icmp permit any echo-reply OUT
```

ASA-FW(config)# ping 10.1.102.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-FW(config)# ping 10.1.101.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R2#ping 10.1.102.10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.10, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

R1#ping 10.1.101.10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.101.10, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Task 2

Ensure that pMTU discovery and traceroute work successfully with the firewall. All other ICMP messages terminating on firewall interfaces should be discarded.



Traceroute tools uses ICMP time-exceeded and ICMP unreachable messages to determine the hops in the network. To make that tool work the ASA must be able to pass that traffic through, so you need to configure ACL on the outside to allow that traffic.

Configuration

Complete these steps:

Step 1 Verify how traceroute is going through the ASA before any

configuration.

```
R1#traceroute 10.1.102.2
```

Type escape sequence to abort.

Tracing the route to 10.1.102.2

```
 1  *  *  *
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  *  *  *
 8  *  *  *
 9  *  *  *
10  *  *
```

Step 2 Configure ASA.

```
ASA-FW(config)# icmp permit any time-exceeded OUT
```

```
ASA-FW(config)# icmp permit any unreachable OUT
```

```
ASA-FW(config)# !
```

```
ASA-FW(config)# icmp permit any time-exceeded IN
```

```
ASA-FW(config)# icmp permit any unreachable IN
```

```
ASA-FW(config)# !
```

```
ASA-FW(config)# icmp permit any time-exceeded DMZ
```

```
ASA-FW(config)# icmp permit any unreachable DMZ
```

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any
unreachable
```

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any
time-exceeded
```

```
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

Verification

```
R1#traceroute 10.1.102.2
```

Type escape sequence to abort.

Tracing the route to 10.1.102.2

```
1 10.1.102.2 0 msec 0 msec *
```


Task 3

Disable fragment reassembling on the ASA's outside interface. You can allow ICMP traffic to pass through the ASA to validate the solution.



By default, the ASA accepts up to 24 fragments to reconstruct full IP packet. So, the easiest way to prevent packets reassembling on the ASA is to change that value to 1. This means, no fragments can be accepted. There is also limit of packets that can be buffered for reassembly which is 200 by default. Changing this value to a large number can make the ASA more vulnerable to a DoS attack by fragment flooding.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any
ASA-FW(config)# fragment chain 1 OUT
```

Verification

```
ASA-FW(config)# sh run all fragment
```

```
fragment size 200 OUT
fragment chain 1 OUT
fragment timeout 5 OUT
no fragment reassembly full OUT
fragment size 200 IN
fragment chain 24 IN
fragment timeout 5 IN
no fragment reassembly full IN
fragment size 200 DMZ
fragment chain 24 DMZ
fragment timeout 5 DMZ
no fragment reassembly full DMZ
```

```
R2#ping 10.1.101.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2#ping 10.1.101.1 size 1600

Type escape sequence to abort.

Sending 5, 1600-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

ASA-FW(config)# logg con 7

ASA-FW(config)# logg on

ASA-FW(config)# %ASA-5-111008: User 'enable_15' executed the 'logging on' command.

R2#ping 10.1.101.1 size 1600

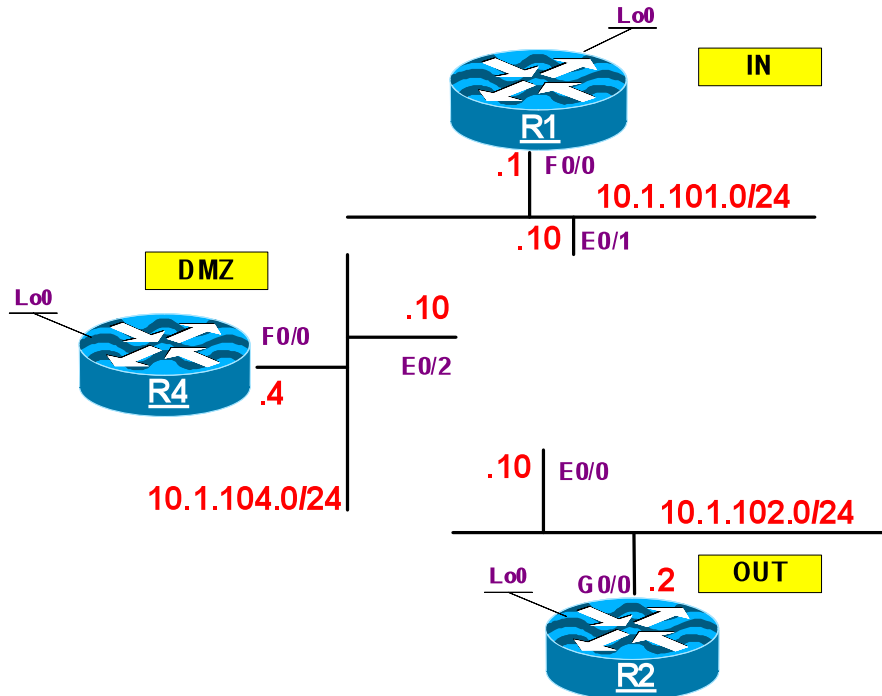
Type escape sequence to abort.

Sending 5, 1600-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

ASA#

%ASA-4-209005: Discard IP fragment set with more than 1 elements: src = 10.1.102.2,
dest = 10.1.101.1, proto = ICMP, id = 15

Lab 1.27. Time based access control



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

Your company uses outsourced services for maintaining the network infrastructure. Configure ASA to allow telnet and SSH connections to R1's F0/0 from the outside. Connections should be allowed only during the contract time, starting from 1 Jan 2010 at 8 a.m. to 31 Dec 2010 at 6 p.m.



Time ranged access lists can be used to control traffic passing ASA in regards to the current time and date on the device. There must be time range object configured first and then it must be attached to specific ACE (Access Control Entry). The time range can be defined by one of two types:

- (1) absolute – the start and the end time and date must be fixed and must describe contiguous range*
- (2) periodic – describes repeatable periods like day-by-day, weekends, days of week, etc.*

As this feature solely depends on time on the device, you must ensure that the time is current – the best option is to use reliable NTP source of course. However, in our case we're not asked to do so.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# time-range Outsourced
ASA-FW(config-time-range)# absolute start 8:00 1 January 2010 end
18:00 31 December 2010

ASA-FW(config-time-range)# access-list OUTSIDE_IN permit tcp any
host 10.1.101.1 eq 22 time-range Outsourced
ASA-FW(config)# access-list OUTSIDE_IN permit tcp any host
10.1.101.1 eq 23 time-range Outsourced
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

Verification

ASA-FW(config)# sh access-list

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list OUTSIDE_IN; 2 elements
access-list OUTSIDE_IN line 1 extended permit tcp any host 10.1.101.1 eq ssh time-range
Outsourced (hitcnt=0) 0xdb76f8a9
access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.101.1 eq telnet time-
range Outsourced (hitcnt=0) 0x4861ab27
```

Note that there are no hits in our ACL. Check the time on the ASA before testing.

ASA-FW(config)# sh clock

```
22:37:25.169 UTC Fri Jan 22 2010
```

R2#tel 10.1.101.1

```
Trying 10.1.101.1 ... Open
```

```
User Access Verification
```

```
Password:
```

```
Password:
```

```
Password:
```

```
% Bad passwords
```

```
[Connection to 10.1.101.1 closed by foreign host]
```

```
R2#
```

ASA-FW(config)# sh access-list

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list OUTSIDE_IN; 2 elements
access-list OUTSIDE_IN line 1 extended permit tcp any host 10.1.101.1 eq ssh time-range
Outsourced (hitcnt=0) 0xdb76f8a9
access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.101.1 eq telnet time-
range Outsourced (hitcnt=1) 0x4861ab27
```

Telnet works fine and there is a hit in the ACL.

ASA-FW(config)# sh time-range

```
time-range entry: Outsourced (active)
      absolute start 08:00 01 January 2010 end 18:00 31 December 2010
      used in: IP ACL entry
```

used in: IP ACL entry

Change the clock on the ASA to see the difference.

```
ASA-FW(config)# clock set 10:00:00 1 Jun 2011
```

```
ASA-FW(config)# sh access-list
```

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list OUTSIDE_IN; 2 elements
access-list OUTSIDE_IN line 1 extended permit tcp any host 10.1.101.1 eq ssh time-range
Outsourced (hitcnt=0) (inactive) 0xdb76f8a9
access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.101.1 eq telnet time-
range Outsourced (hitcnt=0) (inactive) 0x4861ab27
```

Note that when the configured time range is out of current time on the device, the ACL entry is marked as "inactive" in the output of "show access-list" command. This can be useful in troubleshooting and gives us instant information if our configuration is correct or not.

```
R2#tel 10.1.101.1
```

```
Trying 10.1.101.1 ...
```

```
% Connection timed out; remote host not responding
```

Task 2

Users in all you internal network (10.1.101.0/24) should have access to the Internet (HTTP and HTTPS) only during business hours (9am to 5pm) on workdays (Mon-Fri). However, an administrator from IP address of 1.1.1.1 should not have any limits. Ensure that other services are not affected by this policy.



This task clearly states that we should allow traffic in some periodic timeslots only. Hence, the best option here is to use periodic type of time range object. There is also requirement that admin workstation is not getting blocked by this policy, thus we need to specify it at the beginning of the ACL.

Configuration

Complete these steps:

Step 1 ASA configuration.

```

ASA-FW(config)# time-range Users_Internet
ASA-FW(config-time-range)# periodic weekdays 9:00 to 17:00
ASA-FW(config-time-range)# exit

ASA-FW(config)# access-list INSIDE_IN permit ip host 1.1.1.1 any
ASA-FW(config)# access-list INSIDE_IN permit tcp any any eq 80
time-range Users_Internet
ASA-FW(config)# access-list INSIDE_IN permit tcp any any eq 443
time-range Users_Internet
ASA-FW(config)# access-list INSIDE_IN deny tcp any any eq 80
ASA-FW(config)# access-list INSIDE_IN deny tcp any any eq 443
ASA-FW(config)# access-list INSIDE_IN permit ip any any
ASA-FW(config)# access-group INSIDE_IN in interface IN

```

Verification

To verify we can change the clock on the ASA to point to some weekend day. Once it is done, we should see that respective ACEs are inactive and Web traffic will be blocked by the next ACEs.

We do not need to use web browser to make the test. It is enough to enable (if not enabled by default) HTTP server on R2 and telnet to it using "telnet 10.1.102.2 80" command on R1.

```
ASA-FW(config)# clock set 10:00:00 5 Jun 2010
```

```
ASA-FW(config)# sh clock
```

```
10:00:03.399 UTC Sat Jun 5 2010
```

```
ASA-FW(config)# sh access-list
```

```

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list OUTSIDE_IN; 2 elements
access-list OUTSIDE_IN line 1 extended permit tcp any host 10.1.101.1 eq ssh time-range
Outsourced (hitcnt=0) 0xdb76f8a9
access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.101.1 eq telnet time-
range Outsourced (hitcnt=0) 0x4861ab27
access-list INSIDE_IN; 6 elements
access-list INSIDE_IN line 1 extended permit ip host 1.1.1.1 any (hitcnt=0) 0x0abd7ebf
access-list INSIDE_IN line 2 extended permit tcp any any eq www time-range
Users_Internet (hitcnt=0) (inactive) 0x49796a57
access-list INSIDE_IN line 3 extended permit tcp any any eq https time-range
Users_Internet (hitcnt=0) (inactive) 0x4af8d6f5
access-list INSIDE_IN line 4 extended deny tcp any any eq www (hitcnt=0) 0x83fa0440
access-list INSIDE_IN line 5 extended deny tcp any any eq https (hitcnt=0) 0x28e2c45f
access-list INSIDE_IN line 6 extended permit ip any any (hitcnt=0) 0x96858cf8
ASA-FW(config)#

```

R1#tel 10.1.102.2 80

Trying 10.1.102.2, 80 ...

% Connection refused by remote host

R1#tel 10.1.102.2 80 /so lo0

Trying 10.1.102.2, 80 ... Open

GET \

HTTP/1.1 400 Bad Request

Date: Sat, 23 Jan 2010 01:13:05 GMT

Server: cisco-IOS

Accept-Ranges: none

400 Bad Request

[Connection to 10.1.102.2 closed by foreign host]

ASA-FW(config)# sh access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)

alert-interval 300

access-list OUTSIDE_IN; 2 elements

access-list OUTSIDE_IN line 1 extended permit tcp any host 10.1.101.1 eq ssh time-range Outsourced (hitcnt=0) 0xdb76f8a9

access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.101.1 eq telnet time-range Outsourced (hitcnt=0) 0x4861ab27

access-list INSIDE_IN; 6 elements

access-list INSIDE_IN line 1 extended permit ip host 1.1.1.1 any (hitcnt=2) 0x0abd7ebf

access-list INSIDE_IN line 2 extended permit tcp any any eq www time-range

Users_Internet (hitcnt=0) (inactive) 0x49796a57

access-list INSIDE_IN line 3 extended permit tcp any any eq https time-range

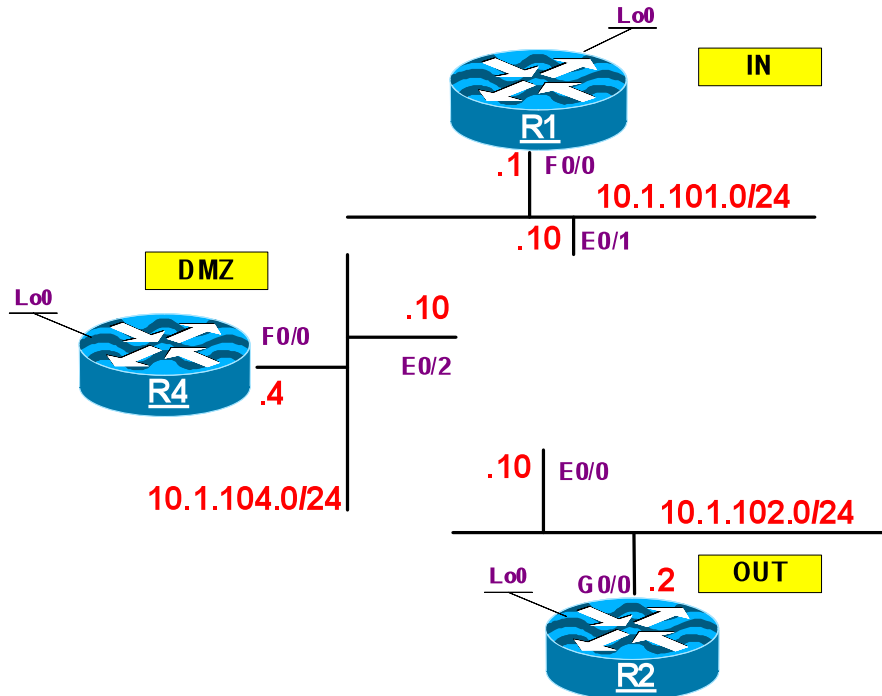
Users_Internet (hitcnt=0) (inactive) 0x4af8d6f5

access-list INSIDE_IN line 4 extended deny tcp any any eq www (hitcnt=1) 0x83fa0440

access-list INSIDE_IN line 5 extended deny tcp any any eq https (hitcnt=0) 0x28e2c45f

access-list INSIDE_IN line 6 extended permit ip any any (hitcnt=0) 0x96858cf8

Lab 1.28. QoS - Priority queuing



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

Your company extensively uses Cisco IP Phones (traffic marked DSCP EF) and some business critical application (TCP port range 15000 to 15200). You need to ensure that ASA will prioritize that traffic going to the outside networks.



Each interface has two levels of queuing available. One is a hardware queue (called tx-ring) which is serviced by FIFO (First In First Out) method. Second is a software queue which is configurable (default serviced by FIFO as well).

As Voice and business critical application's traffic is more important than other corporate traffic (like Web traffic) it is recommended to make use from software queue and prioritize some traffic over the other. Prioritize in software queue will allow important traffic to go sooner to the hardware queue than non-important traffic. This is most useful for latency-dependant traffic like Voice or Video.

Voice traffic is usually marked by EF (Expedited Forwarding) bit in the Layer 3 header. We can use this information to match the traffic and prioritize it. We can also use an ACL to mark the traffic.

It is important to enable priority queuing on the respective interface before configuring action for class map. Finally, our policy map must be attached globally or on the interface. Attaching it globally has effect on every interface where priority queuing is enabled.

Also note that priority queuing is an outbound only solution. We cannot prioritize inbound traffic.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# priority-queue OUT
```

```
ASA-FW(config-priority-queue)# access-list APP extended permit tcp
any any range 15000 15200
```

```
ASA-FW(config)# class-map APP
ASA-FW(config-cmap)# match access-list APP
ASA-FW(config-cmap)# class-map VOICE
ASA-FW(config-cmap)# match dscp ef

ASA-FW(config-cmap)# policy-map LLQ-POLICY
ASA-FW(config-pmap)# class VOICE
ASA-FW(config-pmap-c)# priority
ASA-FW(config-pmap-c)# class APP
ASA-FW(config-pmap-c)# priority

ASA-FW(config-pmap-c)# service-policy LLQ-POLICY interface OUT
```

Verification

ASA-FW(config)# sh service-policy priority

```
Interface OUT:
Service-policy: LLQ-POLICY
Class-map: VOICE
Priority:
Interface OUT: aggregate drop 0, aggregate transmit 0
Class-map: APP
Priority:
Interface OUT: aggregate drop 0, aggregate transmit 0
```

To test our solution, we can configure HTTP server on R2 listening on TCP port 15000. This traffic coming from R1 towards R2 should be prioritized.

R2(config)#ip http port 15000

R2(config)#ip http server

R1#tel 10.1.102.2 15000

```
Trying 10.1.102.2, 15000 ... Open
GET /
HTTP/1.1 400 Bad Request
Date: Wed, 03 Feb 2010 20:34:37 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.102.2 closed by foreign host]
R1#
```

ASA-FW(config)# sh service-policy priority

```
Interface OUT:
  Service-policy: LLQ-POLICY
  Class-map: VOICE
    Priority:
      Interface OUT: aggregate drop 0, aggregate transmit 11
  Class-map: APP
    Priority:
      Interface OUT: aggregate drop 0, aggregate transmit 11
```

ASA-FW(config)# sh priority-queue config

```
Priority-Queue Config interface OUT
      current      default      range
queue-limit      2048          2048          0 - 2048
tx-ring-limit     80            80            3 - 256
```

```
Priority-Queue Config interface IN
      current      default      range
queue-limit       0            2048          0 - 2048
tx-ring-limit     -1           80            3 - 256
```

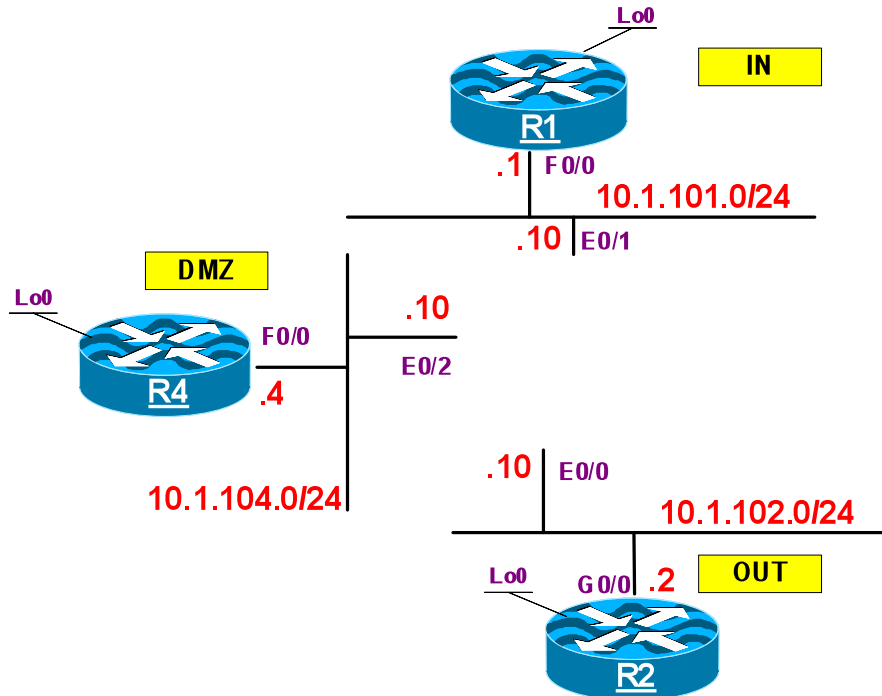
ASA-FW(config)# sh priority-queue statistics

```
Priority-Queue Statistics interface OUT
```

```
Queue Type      = BE          ← Best Effort
Tail Drops      = 0
Reset Drops     = 0
Packets Transmit = 15
Packets Enqueued = 0
Current Q Length = 0
Max Q Length    = 0
```

```
Queue Type      = LLQ          ← Low Latency Queuing
Tail Drops      = 0
Reset Drops     = 0
Packets Transmit = 11
Packets Enqueued = 0
Current Q Length = 0
Max Q Length    = 0
```

Lab 1.29. QoS – Traffic Policing



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

Configure ASA1 so that it limits ICMP traffic on the outside interface. This traffic should be limited to 32kbps in both directions and dropped if this level is exceeded.



This task requires configuring traffic policing on the ASA. It clearly states that we should “limit” the traffic (two technologies should come to your mind right now: policing and shaping) and drop packets which are above configured limit (which leaves us with only one solution: policing). Policing can be configured in both directions on the interface. If it is configured globally it affects all ASA interfaces.

Policing does not buffer packets; it just drops non-conformed packets. Thus, it should be carefully used with TCP traffic (as TCP rapidly slowing down when seeing packets drop) and UDP (as UDP is connectionless and has no mechanisms to confirm that packets reached the destination).

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# access-list ICMP permit icmp any any

ASA-FW(config)# class-map ICMP
ASA-FW(config-cmap)# match access-list ICMP

ASA-FW(config-cmap)# policy-map OUT-POLICY
ASA-FW(config-pmap)# class ICMP
ASA-FW(config-pmap-c)# police input 32000
ASA-FW(config-pmap-c)# police output 32000

ASA-FW(config-pmap-c)# service-policy OUT-POLICY interface OUT
```

Verification

Reconfigure ASA to allow ICMP traffic

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

ASA-FW(config)# sh service-policy police

Interface OUT:

Service-policy: OUT-POLICY

Class-map: ICMP

Input police Interface OUT:

cir 32000 bps, bc 1500 bytes

conformed 0 packets, 0 bytes; actions: transmit

exceeded 0 packets, 0 bytes; actions: drop

conformed 0 bps, exceed 0 bps

Output police Interface OUT:

cir 32000 bps, bc 1500 bytes

conformed 0 packets, 0 bytes; actions: transmit

exceeded 0 packets, 0 bytes; actions: drop

conformed 0 bps, exceed 0 bps

ASA-FW(config)#

Test from R1

R1#pi 10.1.102.2 size 5000 rep 10

Type escape sequence to abort.

Sending 10, 5000-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

!.!.!.!.!.!

Success rate is 50 percent (5/10), round-trip min/avg/max = 4/4/4 ms

R1#

ASA-FW(config)# sh service-policy police

Interface OUT:

Service-policy: OUT-POLICY

Class-map: ICMP

Input police Interface OUT:

cir 32000 bps, bc 1500 bytes

conformed 5 packets, 7570 bytes; actions: transmit

exceeded 0 packets, 0 bytes; actions: drop

conformed 144 bps, exceed 0 bps

Output police Interface OUT:

cir 32000 bps, bc 1500 bytes

conformed 20 packets, 25580 bytes; actions: transmit

exceeded 20 packets, 25580 bytes; actions: drop

conformed 976 bps, exceed 488 bps

Note that there are packets matched by Input and Output policer. As the policer may work for both directions it matches returning ICMP packets. We used ICMP packets of 5000 bytes in size, so the ASA must fragment that traffic and hence there are 40 packets out instead of 10.

Test from R2

ASA-FW(config)# clear service-policy interface OUT

ASA-FW(config)# sh service-policy police

Interface OUT:

Service-policy: OUT-POLICY

Class-map: ICMP

Input police Interface OUT:

cir 32000 bps, bc 1500 bytes

conformed 0 packets, 0 bytes; actions: transmit

exceeded 0 packets, 0 bytes; actions: drop

conformed 0 bps, exceed 0 bps

Output police Interface OUT:

cir 32000 bps, bc 1500 bytes

conformed 0 packets, 0 bytes; actions: transmit

exceeded 0 packets, 0 bytes; actions: drop

conformed 0 bps, exceed 0 bps

R2#pi 10.1.101.1 size 1500 rep 10

Type escape sequence to abort.

Sending 10, 1500-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

!!!!.!!!!!!

Success rate is 80 percent (8/10), round-trip min/avg/max = 1/3/4 ms

R2#

ASA-FW(config)# sh service-policy police

Interface OUT:

Service-policy: OUT-POLICY

Class-map: ICMP

Input police Interface OUT:

cir 32000 bps, bc 1500 bytes

conformed 0 packets, 0 bytes; actions: transmit

exceeded 0 packets, 0 bytes; actions: drop

conformed 0 bps, exceed 0 bps

Output police Interface OUT:

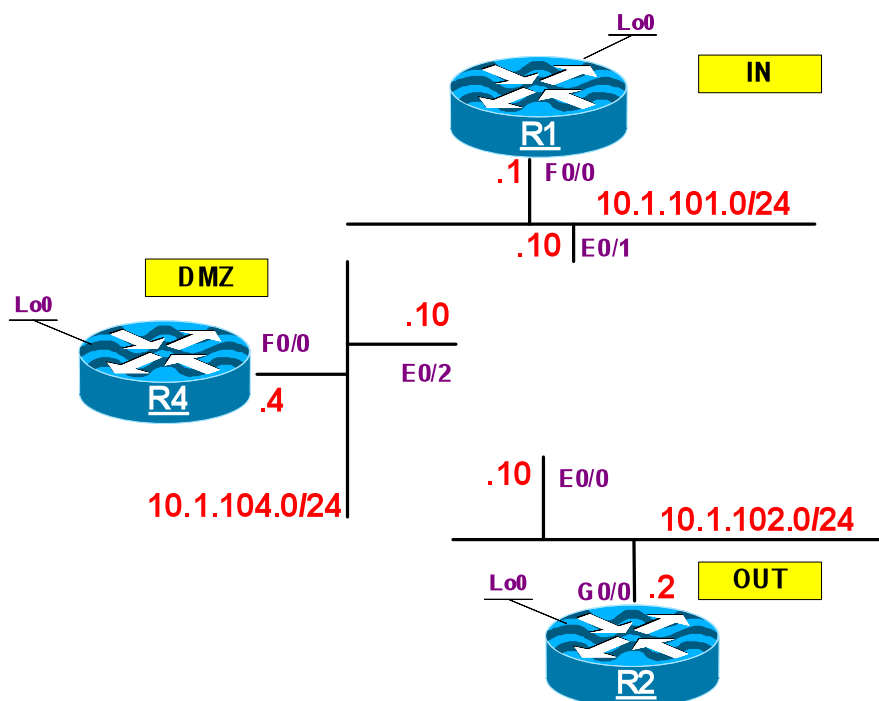
cir 32000 bps, bc 1500 bytes

conformed 8 packets, 12112 bytes; actions: transmit

exceeded 2 packets, 3028 bytes; actions: drop

conformed 2208 bps, exceed 552 bps

Lab 1.30. QoS – Traffic Shaping



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

Users in the inside network uses ASA to connect to the Internet. Although, you have 10Mbps outside connection on the ASA you must ensure that traffic going to the Internet takes no more than 1Mbps (1024kbps with a burst of 10240).



ASA can only send out data with its full interface speed (this is AIR – Access Information Rate). To limit the speed on which packets are sending out we can use policing or shaping. Policing usually drops excessive packets causing problems with TCP/UDP based applications and services. Shaping is more polite and it buffers excessive traffic to send it out later. This results in less packets dropping and smoother traffic flows.

Shaping uses four values to calculate the shaper:

- *CIR - Committed Information Rate (a contracted value to which we should shape our traffic)*
- *Bc – Committed Burst (an amount of bits that can be buffered for later use)*
- *Be – Excessive Burst (an limit of bits that can be buffered)*
- *Tc – Time Interval (usually 1/8th of a second, equals 125ms)*

*Typical shaper sends no more than CIR*Tc in each Tc slot. However, there can be some Tc without data, so that shaper can use it to send out buffered packets. This buffer is described by Bc value and the shaper can accommodate no more than Bc+Be data in the buffer. The ASA sets Be=Bc by default. The Tc is not explicitly configured, rather it is calculated by the following formula $Tc=CIR/Bc$.*

Also note that Bc and Be are in bytes (CIR/Rate is in bits).

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# policy-map SHAPE-POLICY
ASA-FW(config-pmap)# class class-default
ASA-FW(config-pmap-c)# shape average 1024000 10240

ASA-FW(config-pmap-c)# service-policy SHAPE-POLICY interface OUT
```

Verification

Reconfigure ASA to allow ICMP traffic

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

```
ASA-FW(config)# sh service-policy shape
```

Interface OUT:

```
Service-policy: SHAPE-POLICY
  Class-map: class-default
```

```
Shape (average) cir 1024000, bc 10240, be 10240
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

```
R1#pi 10.1.102.2 size 1500 rep 1000
```

Type escape sequence to abort.

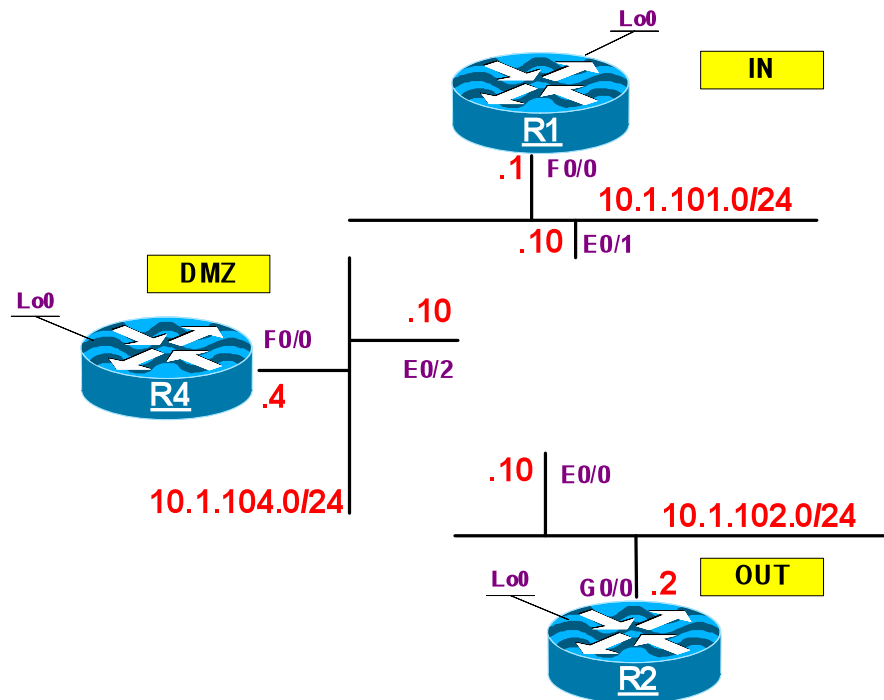
Sending 1000, 1500-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

[illegible]

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/11/36 ms

Page 289 of 1033

Lab 1.31. QoS – Traffic Shaping with Prioritization



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

Configure ASA to enforce QoS policy for outside traffic so that traffic marked with DSCP EF is shaped up to 2Mbps and prioritized. All other traffic should be best-effort serviced.



In this task we need ensure that our Voice traffic will not get more than 2Mbps and it will be prioritized at the same time. Unfortunately, we cannot configure LLQ (Low Latency Queuing) and shaping on the same interface. This can be done however, by prioritizing traffic inside shaped queue. This will effectively create two sub-queues: (1) priority queue and (2) best effort queue inside shaped parent queue. To configure that, we need to nest priority queue (policy map for LLQ) using service-policy command under shaper policy map.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# priority-queue OUT

ASA-FW(config-priority-queue)# class-map VOICE
ASA-FW(config-cmap)# match dscp ef

ASA-FW(config-cmap)# policy-map VOICE
ASA-FW(config-pmap)# class VOICE
ASA-FW(config-pmap-c)# priority

ASA-FW(config-pmap-c)# policy-map SHAPE-OUTSIDE
ASA-FW(config-pmap)# class class-default
ASA-FW(config-pmap-c)# shape average 2048000
ASA-FW(config-pmap-c)# service-policy VOICE
```



```
ASA-FW(config-pmap-c)# service-policy SHAPE-OUTSIDE interface OUT
```

Verification

```
ASA-FW(config)# sh service-policy interface OUT
```

```
Interface OUT:
```

```
Service-policy: SHAPE-OUTSIDE
```

```
Class-map: class-default
```

```
shape (average) cir 2048000, bc 8192, be 8192
```

```
(pkts output/bytes output) 0/0
```

```
(total drops/no-buffer drops) 0/0
```

```
Service-policy: VOICE
```

```
Class-map: VOICE
```

```
priority
```

```
Queueing
```

```
queue limit 64 packets
```

```
(queue depth/total drops/no-buffer drops) 0/0/0
```

```
(pkts output/bytes output) 0/0
```

```
Class-map: class-default
```

```
Default Queueing
```

```
queue limit 64 packets
```

```
(queue depth/total drops/no-buffer drops) 0/0/0
```

```
(pkts output/bytes output) 0/0
```

To test our solution we need to mark some traffic with DSCP EF bit. This can be quickly done on R1 by using MQC. In addition to that we need to allow ICMP on the ASA either by configuring ACL or ICMP inspection.

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any
```

```
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

```
R1(config)#class-map ICMP
```

```
R1(config-cmap)#match protocol icmp
```

```
R1(config-cmap)#exi
```

```
R1(config)#policy-map ICMP-EF
```

```
R1(config-pmap)#class ICMP
```

R1#pi 10.1.102.2 size 1500 rep 1000

```
ASA-FW(config)# sh service-policy interface OUT
```

Page 293 of 1033

Default Queueing

```
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

As you can see there are some packets prioritized and no packets in the default class. To ensure that only packets with DSCP EF bit set are prioritized, let's make another test.

R1#tel 10.1.102.2

Trying 10.1.102.2 ... Open

User Access Verification

Password:

R2>exi

[Connection to 10.1.102.2 closed by foreign host]

R1#

ASA-FW(config)# sh service-policy interface OUT

Interface OUT:

Service-policy: SHAPE-OUTSIDE

Class-map: class-default

shape (average) cir 2048000, bc 8192, be 8192

(pkts output/bytes output) 1008/1479926

(total drops/no-buffer drops) 0/0

Service-policy: VOICE

Class-map: VOICE

priority

Queueing

queue limit 64 packets

(queue depth/total drops/no-buffer drops) 0/28/0

(pkts output/bytes output) 986/1479000

Class-map: class-default

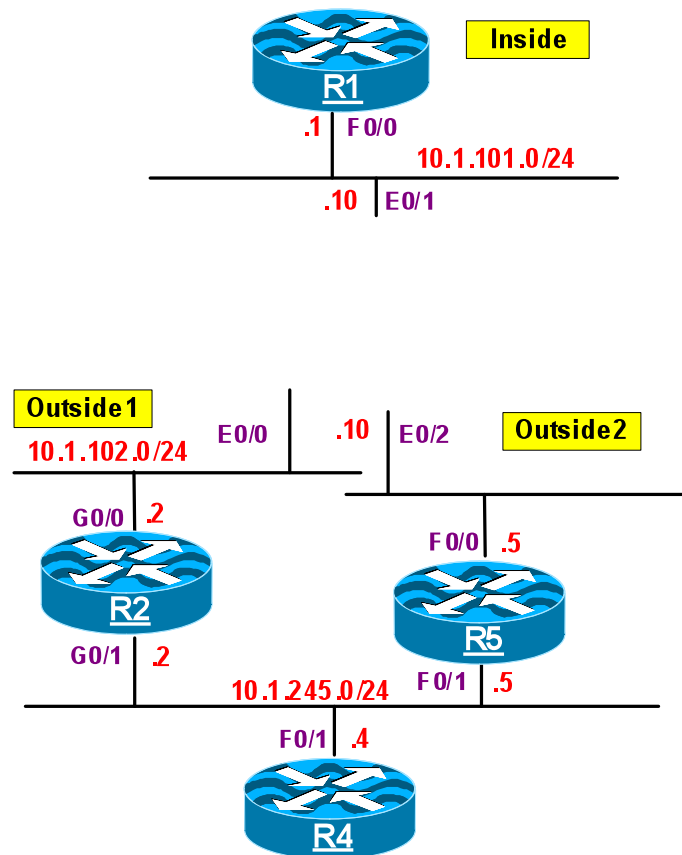
Default Queueing

queue limit 64 packets

(queue depth/total drops/no-buffer drops) 0/0/0

(pkts output/bytes output) 22/926

Lab 1.32. SLA Route Tracking



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R5's F0/0 and ASA's E0/2 interface should be configured in VLAN 105
- R2's G0/1, R5's F0/1 and R4's F0/1 interface should be configured in VLAN 245
- Configure Telnet on all routers using password "cisco"
- Configure default gateway on R1/R2/R5 pointing to the ASA

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	F0/0	10.1.101.1/24
R2	G0/0	10.1.102.2/24

	G0/1	10.1.245.2/24
R4	F0/1	10.1.245.4 /24
R5	F0/0	10.1.105.5 /24
	F0/1	10.1.245.5 /24
ASA1/ASA-FW	E0/0 (Outside1, Security 0)	10.1.102.10 /24
	E0/1 (Inside, Security 100)	10.1.101.10 /24
	E0/2 (Outside2, Security 0)	10.1.105.10 /24

Task 1

You have installed second connection to the outside networks to achieve redundancy. Configure ASA so that it uses R2 as a default gateway as long as its F0/1 interface IP address is reachable. If three ICMP packets fail within 10 seconds the ASA should withdraw the static route from its routing table and use IP address of R5's F0/1 interface as a new default gateway.



Static route tracking provides a method for tracking the availability of a static route and for making a backup route available if the primary route fails.

The ASA associates a static route with monitoring target that you define. If this target becomes unavailable the ASA removes the route associated with the target from its routing table and start using backup route instead. To ensure the backup route will not be visible in the routing table along with primary route (two default gateways would force the ASA to load sharing packets) there should be higher AD (Administrative Distance) associated with the backup route.

The SLA (Service Level Agreement) operation monitors the target with periodic ICMP echo requests. If an echo reply is not received within a specified period of time, the object is considered down, and the associated route for that target is removed from the routing table. A previously configured backup route is used instead of the route that is removed. While the backup route is in use, the SLA monitor operation continues to try to reach the monitoring target. Once the target is available again, the first route is returned to the routing table and the backup route is removed.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# sla monitor 1
ASA-FW(config-sla-monitor)# type echo protocol ipIcmpEcho
10.1.102.2 interface outside1
ASA-FW(config-sla-monitor-echo)# num-packets 3
ASA-FW(config-sla-monitor-echo)# frequency 10
ASA-FW(config-sla-monitor-echo)# exi
ASA-FW(config)# sla monitor schedule 1 start-time now life forever
ASA-FW(config)# track 1 rtr 1 reachability
ASA-FW(config)# route outside1 0.0.0.0 0.0.0.0 10.1.102.2 track 1
ASA-FW(config)# route outside2 0.0.0.0 0.0.0.0 10.1.105.5 254
```

Verification

ASA-FW(config)# sh route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is 10.1.102.2 to network 0.0.0.0

```
C    10.1.105.0 255.255.255.0 is directly connected, Outside2
C    10.1.102.0 255.255.255.0 is directly connected, Outside1
C    10.1.101.0 255.255.255.0 is directly connected, Inside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.1.102.2, Outside1
```

ASA-FW(config)# sh sla monitor configuration

```
SA Agent, Infrastructure Engine-II
Entry number: 1
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.102.2
Interface: Outside1
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 10
```

```
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

ASA-FW(config)# sh sla monitor operational-state

```
Entry number: 1
Modification time: 10:57:46.666 UTC Sat Jul 17 2010
Number of Octets Used by this Entry: 1480
Number of operations attempted: 36
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 11:03:36.667 UTC Sat Jul 17 2010
Latest operation return code: OK
RTT Values:
RTTAvg: 1          RTTMin: 1          RTTMax: 1
NumOfRTT: 3       RTTSum: 3          RTTSum2: 3
```

ASA-FW(config)# sh track 1

```
Track 1
  Response Time Reporter 1 reachability
  Reachability is Up
  1 change, last change 00:02:08
  Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

Test

We can test our solution by running traceroute to the R4's IP address from R1. To make it work, we need to apply an ACL on both ASA's outside interfaces allowing ICMP (type 3, code 3) back from R4.

In addition to that, R4 will need to have a route back to R1. So the best option here is to configure dynamic NAT on R2 and R5 translating all source IP addresses to their interfaces towards R4.

As we can see ASA routes the traffic through R2 as it is in its routing table as default gateway. As long as R2's G0/0 IP address is responding on SLA ICMP packets, the default route points to R2. Once we shut R2's interface down, the default route is deleted from the routing table and the default route with AD of 254 is used instead.

On ASA

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any
ASA-FW(config)# access-group OUTSIDE_IN in interface Outside1
ASA-FW(config)# access-group OUTSIDE_IN in interface Outside2
```

On R2

```
R2(config)#ip nat inside source list 140 interface g0/1
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R2(config)#access-list 140 permit ip any any
R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config-if)#int g0/1
R2(config-if)#ip nat outside
R2(config-if)#exi
```

On R5

```
R5(config)#ip nat inside source list 140 interface f0/1

R5(config)#access-list 140 permit ip any any
R5(config)#int f0/0
R5(config-if)#ip nat inside
%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R5(config-if)#int f0/1
R5(config-if)#ip nat outside
R5(config-if)#exi
```

R1#ping 10.1.245.4

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.245.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

R1#trace 10.1.245.4

```
Type escape sequence to abort.
Tracing the route to 10.1.245.4
```

```
  1 10.1.102.2 0 msec 0 msec 0 msec
  2 10.1.245.4 4 msec 0 msec *
```

```
R2(config)#int g0/0
R2(config-if)#sh
```

```
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
down
```

ASA-FW(config)# sh route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

```
Gateway of last resort is 10.1.105.5 to network 0.0.0.0
```

```
C    10.1.105.0 255.255.255.0 is directly connected, Outside2
C    10.1.102.0 255.255.255.0 is directly connected, Outside1
C    10.1.101.0 255.255.255.0 is directly connected, Inside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.1.105.5, Outside2
```

ASA-FW(config)# sh sla monitor operational-state

```
Entry number: 1
Modification time: 09:48:02.952 UTC Sun Jul 18 2010
Number of Octets Used by this Entry: 1480
Number of operations attempted: 36
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 09:53:42.953 UTC Sun Jul 18 2010
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0          RTTMin: 0          RTTMax: 0
NumOfRTT: 0        RTTSum: 0          RTTSum2: 0
```

ASA-FW(config)# clear conn

```
6 connection(s) deleted.
```

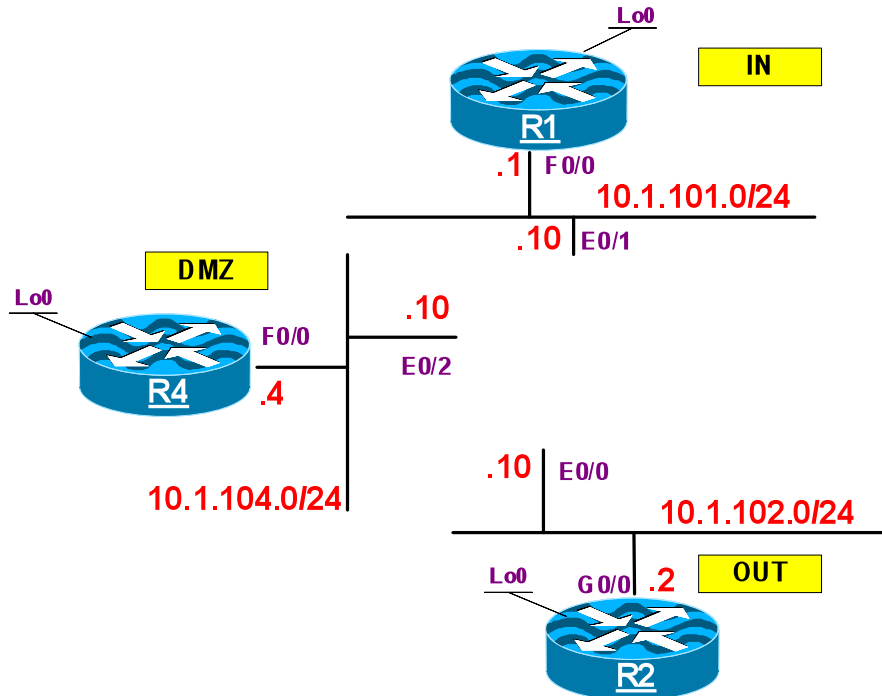
R1#trace 10.1.245.4

```
Type escape sequence to abort.
Tracing the route to 10.1.245.4
```

```
 1 10.1.105.5 0 msec 0 msec 4 msec
 2 10.1.245.4 0 msec 0 msec *
```

Because traceroute uses UDP packets, the ASA creates flows in its connections (state) table. UDP has a default timeout of 2 minutes on the ASA, so we need to wait at least 2 minutes before checking again (tracerouting from R1) or we can clear connections table manually.

Lab 1.33. ASA IP Services (DHCP)



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24

	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (OUT, Security 0)	10.1.102.10 /24
	E0/1 (IN, Security 80)	10.1.101.10 /24
	E0/2.104 (DMZ, Security 50)	10.1.104.10 /24

Task 1

Configure ASA to give out IP addresses for inside hosts automatically using the following information:

IP address range: 10.1.101.100-10.1.101.200

DNS Server: 10.1.101.5

WINS Server 10.1.101.6

Domain Name: MicronicsTraining.com

Lease time: 8h



The ASA may work as a DHCP server in both routed and transparent mode. It may serve IP addresses to the hosts on the network (usually inside network), configure additional DHCP options like DNS/WINS server and configure itself as a default gateway for the clients.

DHCP lease time is 3600 seconds (1h) by default.

In addition to that, the ASA can serve additional DHCP options for its clients like different default gateway (useful in transparent mode as the ASA does not have an IP address and the default gateway usually lays on the other side of the ASA), TFTP server IP address and so on.

Note that you must enable DHCP server on the ASA after configuring it by using "dhcpd enable <interface>" command.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# dhcpd address 10.1.101.100-10.1.101.200 IN
ASA-FW(config)# dhcpd dns 10.1.101.5
```

```
ASA-FW(config)# dhcpd wins 10.1.101.6
ASA-FW(config)# dhcpd domain MicronicsTraining.com
ASA-FW(config)# dhcpd lease 28800
ASA-FW(config)# dhcpd enable IN
```

Verification

ASA-FW(config)# sh dhcpd state

```
Context   Configured as DHCP Server
Interface OUT, Not Configured for DHCP
Interface IN, Configured for DHCP SERVER
Interface DMZ, Not Configured for DHCP
```

ASA-FW(config)# sh dhcpd binding

IP address	Hardware address	Lease expiration	Type

```
R1(config)#int f0/0
R1(config-if)#ip address dhcp
%DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 10.1.101.100,
mask 255.255.255.0, hostname R1
```

R1#sh ip int f0/0

```
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.101.100/24
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
```

```
IP CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
```

R1#sh ip dns view

```
DNS View default parameters:
Logging is off
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: MicronicsTraining.com
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    10.1.101.5
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder timeout: 3 seconds
  Forwarder retries: 2
  Forwarder addresses:
```

ASA-FW(config)# sh dhcpd binding

IP address	Hardware address	Lease expiration	Type
10.1.101.100	0063.6973.636f.2d30. 3031.392e.3330.3130. 2e38.3631.382d.4661. 302f.30	28648 seconds	Automatic

ASA-FW(config)# sh dhcpd statistics

```
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
```

```
Address pools      1
Automatic bindings 1
Expired bindings   0
```

Malformed messages	0
Message	Received
BOOTREQUEST	0
DHCPDISCOVER	1
DHCPREQUEST	1
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Message	Sent
BOOTREPLY	0
DHCPOFFER	1
DHCPACK	1
DHCPNAK	0

Task 2

Clear previous DHCP server configuration on ASA.

There is a DHCP server located on R4. Configure ASA so that it forwards all DHCP messages coming from inside hosts to that server. The ASA should be a default gateway for inside network.



The ASA can also be used as DHCP Relay Agent in case the DHCP server is located on different network. In that mode the ASA relays all DHCP messages to the configured DHCP server and can set itself as a default gateway in the DHCP messages returned to the clients.

Note that the DHCP Relay Agent feature is unavailable in transparent firewall mode as there is no reason to relay DHCP messages in this mode. The ASA passes DHCP messages natively when working in transparent mode.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# clear configure dhcpd

ASA-FW(config)# dhcprelay server 10.1.104.4 DMZ
ASA-FW(config)# dhcprelay enable IN
ASA-FW(config)# dhcprelay setroute IN
```


Verification

ASA-FW(config)# sh dhcprelay state

```
Context    Configured as DHCP Relay
Interface OUT, Not Configured for DHCP
Interface IN, Configured for DHCP RELAY SERVER
Interface DMZ, Configured for DHCP RELAY
```

ASA-FW(config)# sh dhcprelay statistics

```
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
```

Packets Relayed

```
BOOTREQUEST      0
DHCPDISCOVER      0
DHCPREQUEST       0
DHCPDECLINE       0
DHCPRELEASE       0
DHCPINFORM        0

BOOTREPLY         0
DHCPOFFER         0
DHCPACK           0
DHCPNAK           0
```

```
R1(config)#int f0/0
```

```
R1(config-if)#shut
```

```
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
R1(config-if)#no shut
```

```
R1(config-if)#
```

```
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
R1(config-if)#
```

```
%DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 10.1.101.1,
mask 255.255.255.0, hostname R1
```

R4#sh ip dhcp binding

```
Bindings from all pools not associated with VRF:
```

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
10.1.101.1	0063.6973.636f.2d30. 3031.392e.3330.3130. 2e38.3631.382d.4661. 302f.30	Feb 04 2010 09:13 PM	Automatic

ASA-FW(config)# sh dhcprelay statistics

DHCP UDP Unreachable Errors: 0

DHCP Other UDP Errors: 0

Packets Relayed

BOOTREQUEST 0

DHCPDISCOVER 1

DHCPREQUEST 1

DHCPDECLINE 0

DHCPRELEASE 0

DHCPINFORM 0

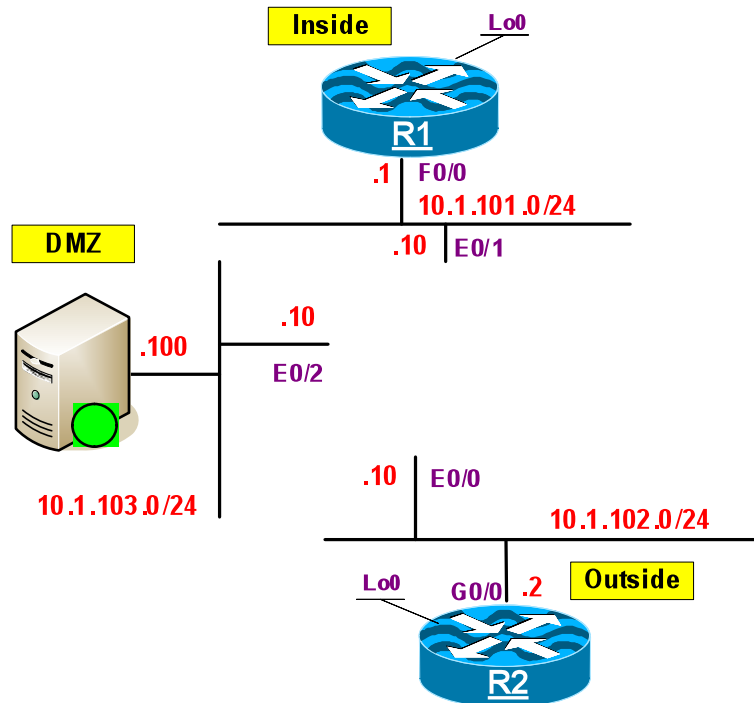
BOOTREPLY 0

DHCPOFFER 1

DHCPACK 1

DHCPNAK 0

Lab 1.34. URL filtering and applets blocking



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101.
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- Websense server's NIC (installed on ACS) and ASA's E0/2 interface should be configured in VLAN 103
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24
	F0/0	10.1.102.2/24

WebSense	NIC	10.1.103.100/24
ASA1/ASA-FW	E0/0 (Outside, Security 0)	10.1.102.10/24
	E0/1 (Inside, Security 100)	10.1.101.10/24
	E0/2 (DMZ, Security 50)	10.1.103.10/24

Task 1

Configure ASA to cooperate with WebSense server to filter out URL's blocked by WebSense policy. The policy should be enforced for HTTP/HTTPS traffic from every IP address and in case of WebSense server failure, ASA should pass traffic without URL filtering.

In addition to that, configure ASA so that it blocks all ActiveX and Java objects embedded into HTTP packets.

The FTP access should also be blocked for IP addresses from subnet 10.1.10.0/24 except the Administrator's workstation on 10.1.10.100.



Java applets and ActiveX controls are executable programs that can be dangerous for end user. Some applets contain hidden code that can destroy data on the internal network. This can be downloaded when you permit access to HTTP port 80.

The ASA can prevent users from downloading applets from the websites by using "filter" command. This can be configured for some users/subnets only allowing other users downloading applets when surfing the Internet.

In addition to applets filtering, the ASA can filter URLs in conjunction with Websense and Secure Computing URL-filtering software. It works this way so that when the ASA receives a request from a user to access a URL, it queries the URL-filtering server to determine whether to allow, or block, the requested web page. Before you enable URL filtering, you must designate at least one server on which the Websense or SmartFilter URL-filtering application is installed.

Configuring URL-filtering software is out of scope for CCIE Security lab exam, so in case of such question, the grading script (or person) will probably look after appropriate commands in the ASA configuration.

The command of "filter url" enables URL filtering and has some additional

options at the end to specify the following:

- *allow - this keyword allows outbound traffic when URL server is down*
- *cgi_truncate - if question mark is found in the URL, this will remove all characters after the question mark*
- *longurl-deny - denies oversized URL requests*
- *longurl-truncate - sends only simple URL (e.g. domain.com) to the URL-filtering server oversized URL is found*

The URL filtering features extend web-based URL filtering to HTTPS and FTP as well. However in case of HTTPS the header is encrypted and the ASA cannot retrieve URL information. The ASA will send an IP address of the Web server to the URL-filtering server for checking. For FTP there is an additional option (interact-block) which prevents users from using interactive FTP sessions.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA-FW(config)# url-server (DMZ) vendor websense host 10.1.103.100
timeout 30 protocol TCP version 4 connections 5

ASA-FW(config)# filter ftp except 10.1.10.100 255.255.255.255
0.0.0.0 0.0.0.0
ASA-FW(config)# filter ftp 21 10.1.10.0 255.255.255.0 0.0.0.0
0.0.0.0 interact-block
ASA-FW(config)# filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
ASA-FW(config)# filter url 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
allow
ASA-FW(config)# filter ActiveX 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
ASA-FW(config)# filter https 443 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
allow
```

Verification

```
ASA-FW(config)# sh url-server statistics
```

```
Global Statistics:
-----
URLs total/allowed/denied          0/0/0
URLs allowed by cache/server        0/0
URLs denied by cache/server         0/0
```

HTTPSs total/allowed/denied	0/0/0
HTTPSs allowed by cache/server	0/0
HTTPSs denied by cache/server	0/0
FTPps total/allowed/denied	0/0/0
FTPps allowed by cache/server	0/0
FTPps denied by cache/server	0/0
Requests dropped	0
Server timeouts/retries	0/0
Processed rate average 60s/300s	0/0 requests/second
Denied rate average 60s/300s	0/0 requests/second
Dropped rate average 60s/300s	0/0 requests/second

Server Statistics:

```
-----
10.1.103.100 DOWN
Vendor websense
Port 15868
Requests total/allowed/denied 0/0/0
Server timeouts/retries 0/0
Responses received 0
Response time average 60s/300s 0/0
```

URL Packets Sent and Received Stats:

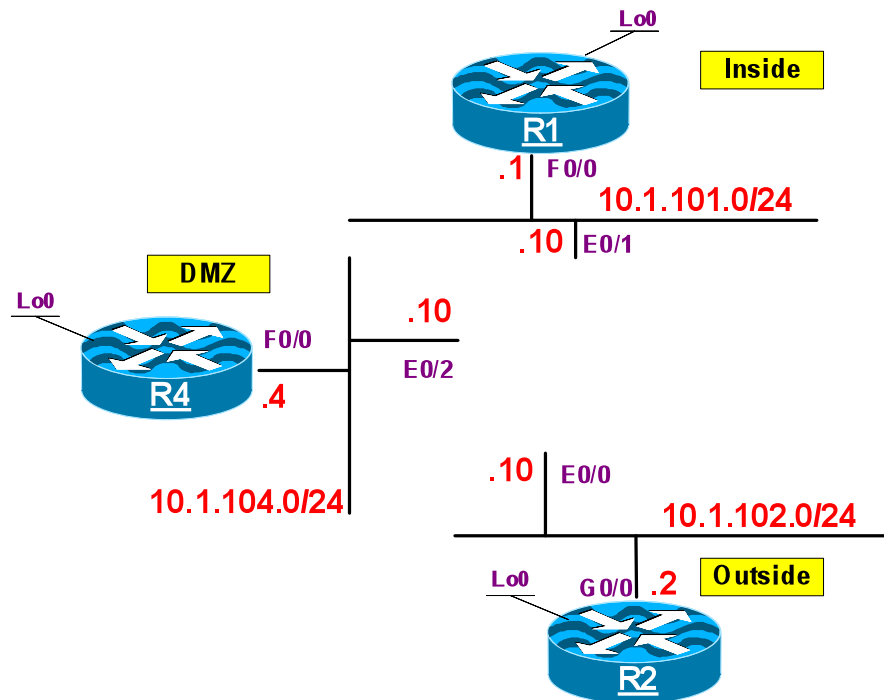
```
-----
Message Sent Received
STATUS_REQUEST 7 0
LOOKUP_REQUEST 0 0
LOG_REQUEST 0 NA
```

Errors:

```
-----
RFC noncompliant GET method 0
URL buffer update failure 0
```

Note that the Websense server is in DOWN state. This is because there is no Websense software installed on the ACS. In the lab, however, it is possible to install trial Websense software on the ACS server and check the configuration.

Lab 1.35. Troubleshooting using Packet Tracer and Capture tools



Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/2 interface should be configured in VLAN 104
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices and advertise their all directly connected networks.

IP Addressing

Device/Hostname	Interface (ifname)	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	Lo0	2.2.2.2/24

	F0/0	10.1.102.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.104.4/24
ASA1/ASA-FW	E0/0 (Outside, Security 0)	10.1.102.10 /24
	E0/1 (Inside, Security 100)	10.1.101.10 /24
	E0/2 (DMZ, Security 50)	10.1.104.10 /24

Task 1

You are trying to ping R1 from R2's F0/0 interface. The ping fails. Using available ASA tools troubleshoot and resolve the issue.

```
R1#ping 10.1.102.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

Troubleshooting

```
ASA-FW(config)# packet-tracer input Inside icmp 10.1.101.1 0 0 10.1.102.2 detailed
```

```
Phase: 1
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0xd78c48c0, priority=1, domain=permit, deny=false
```

```
hits=22, user_data=0x0, cs_id=0x0, l3_type=0x8
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=0000.0000.0000, mask=0000.0000.0000
```

```
Phase: 2
```

```
Type: FLOW-LOOKUP
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Found no matching flow, creating a new flow
```


Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 10.1.102.0 255.255.255.0 Outside

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0xd7c4e720, priority=0, domain=permit-ip-option, deny=true
hits=3, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Phase: 5
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0xd7cb61f0, priority=66, domain=inspect-icmp-error, deny=false
hits=2, user_data=0xd78c1080, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 728, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...

Result:
input-interface: Inside

```
input-status: up
input-line-status: up
output-interface: Outside
output-status: up
output-line-status: up
Action: allow
```

Hmm, seems everything is OK. Take a closer look to the above output - this is ONLY for unidirectional flow. The ICMP packet has flown by Inside and Outside interface. We need to check the same for returning traffic. Let's look...

ASA-FW(config)# packet-tracer input Outside icmp 10.1.102.2 8 0 10.1.101.1 detailed

```
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow
```

```
Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in  10.1.101.0      255.255.255.0   Inside
```

```
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x330f848, priority=0, domain=permit, deny=true
    hits=6, user_data=0x9, cs_id=0x0, flags=0x1000, protocol=0
    src ip=0.0.0.0, mask=0.0.0.0, port=0
    dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
```

```
Result:
input-interface: Outside
input-status: up
input-line-status: up
output-interface: Inside
output-status: up
output-line-status: up
Action: drop
```

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

As you can see, the packet has been denied by the ACL (implicit rule). Let's confirm that by enabling logging at Debug (7) level.

```
ASA-FW(config)# logging buffered 7
```

```
ASA-FW(config)# logging on
```

```
ASA-FW(config)# clear logging buffer
```

```
R2#pi 10.1.101.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

```
.....
```

Success rate is 0 percent (0/5)

```
ASA-FW(config)# sh logging
```

Syslog logging: enabled

Facility: 20

Timestamp logging: disabled

Standby logging: disabled

Debug-trace logging: disabled

Console logging: disabled

Monitor logging: disabled

Buffer logging: level debugging, 6 messages logged

Trap logging: disabled

History logging: disabled

Device ID: disabled

Mail logging: disabled

ASDM logging: disabled

User 'enable_15' executed the 'clear logging buffer' command.

```
Deny inbound icmp src Outside:10.1.102.2 dst Inside:10.1.101.1 (type 8, code 0)
```

```
Deny inbound icmp src Outside:10.1.102.2 dst Inside:10.1.101.1 (type 8, code 0)
```

```
Deny inbound icmp src Outside:10.1.102.2 dst Inside:10.1.101.1 (type 8, code 0)
```

```
Deny inbound icmp src Outside:10.1.102.2 dst Inside:10.1.101.1 (type 8, code 0)
```

```
Deny inbound icmp src Outside:10.1.102.2 dst Inside:10.1.101.1 (type 8, code 0)
```

Confirmed! Five packets (Echo Requests) have been denied by the outside interface.

We can also use another tool to check what happened. Capture - is the packet sniffer on the ASA which can "trace" the packets to see what happened on the device. Let's capture traffic on the outside interface with "trace" option enabled.

```
ASA-FW(config)# capture ISSUE trace interface outside
```

R2#pi 10.1.101.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.101.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

ASA-FW(config)# sh capture ISSUE trace

5 packets captured

```
1: 14:22:20.842348 10.1.102.2 > 10.1.101.1: icmp: echo request
2: 14:22:20.854386 10.1.102.2 > 10.1.101.1: icmp: echo request
3: 14:22:20.855073 10.1.102.2 > 10.1.101.1: icmp: echo request
4: 14:22:20.867905 10.1.102.2 > 10.1.101.1: icmp: echo request
5: 14:22:20.885055 10.1.102.2 > 10.1.101.1: icmp: echo request
```

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found no matching flow, creating a new flow

Phase: 4

Type: ROUTE-LOOKUP

Subtype: input

Result: ALLOW

Config:

Additional Information:

in 10.1.101.0 255.255.255.0 Inside

```

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
output-interface: Inside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule

5 packets shown

```

ASA-FW(config)# no capture ISSUE

Similar output as it was for Packet Tracer. Again, we see that the packets have been dropped by the outside ACL.

However, the main difference between Packet Tracer and Capture is that the capture sees existing flow but Packet Tracer only injects the packet into the traffic plane. Capture is more useful as it may show bidirectional flows - meaning you can check if returning packets are not getting dropped for some reason.

Let's look at ping in the other direction, from R1 towards R2. Assuming default ASA configuration, the Echo Request should pass the ASA as this packet is going from Inside (100) to Outside (0). However, returning packet, which is Echo Reply should be dropped due to lack of flow information (there is no inspect enable for ICMP by default) nor ACL on the outside. Let's check this out then...

ASA-FW(config)# capture ICMP-I trace detail interface Inside

ASA-FW(config)# capture ICMP-O trace detail interface Outside

ASA-FW(config)# sh capture ICMP-I

```

1 packet captured
  1: 14:41:26.596404 10.1.101.1 > 10.1.102.2: icmp: echo request
1 packet shown

```

ASA-FW(config)# sh capture ICMP-O

```

2 packets captured
  1: 14:41:26.597259 10.1.101.1 > 10.1.102.2: icmp: echo request
  2: 14:41:26.603774 10.1.102.2 > 10.1.101.1: icmp: echo reply
2 packets shown

```

Huh! See that there are two packets captured on the Outside interface and only one on the Inside. This should make you suspicious that something is not right

here. The Echo Reply packet should be seen on the Inside interface if everything works perfect.
Let's "trace" that capture to see what ASA has done with those packets.

ASA-FW(config)# sh capture ICMP-O trace

2 packets captured

1: 14:41:26.597259 10.1.101.1 > 10.1.102.2: icmp: echo request
2: 14:41:26.603774 10.1.102.2 > 10.1.101.1: icmp: echo reply

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x333b008, priority=12, domain=capture, deny=false
hits=1, user_data=0x32f33b0, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x330f5d8, priority=1, domain=permit, deny=false
hits=168, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found no matching flow, creating a new flow

← This is because ICMP is stateless

Phase: 4

Type: ROUTE-LOOKUP

Subtype: input

Result: ALLOW

Config:

Additional Information:

in 10.1.101.0 255.255.255.0 Inside

Phase: 5

```
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
  Forward Flow based lookup yields rule:
    in  id=0x330f848, priority=0, domain=permit, deny=true
        hits=35, user_data=0x9, cs_id=0x0, flags=0x1000, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Result:
output-interface: Inside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

ASA-FW(config)# sh capture

```
capture ICMP-I type raw-data trace detail interface Inside [Capturing - 212 bytes]
capture ICMP-O type raw-data trace detail interface Outside [Capturing - 342 bytes]
```

ASA-FW(config)# no cap ICMP-I**ASA-FW(config)# no cap ICMP-O**

Again, we see the returning packet has been denied by the ACL. This is because ICMP is stateless and there is no ICMP inspection enabled on the ASA. To make it work we should either configure ICMP inspection or permit ICMP echo reply in the inbound ACL on the Outside interface.

Another useful tool is DEBUG. However it is not recommended to enable it in production as this may overwhelm your device. A very quick check we can use here by enabling "debug icmp trace".

R1#ping 10.1.102.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

ASA-FW(config)# deb icmp trace

```
debug icmp trace enabled at level 1
ASA-FW(config)# ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=18
seq=0 len=72
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=18 seq=1 len=72
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=18 seq=2 len=72
```

```
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=18 seq=3 len=72
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=18 seq=4 len=72
```

From the output we see that ICMP packets get routed out of Outside interface but never return back.

Let's fix the issue by enabling ICMP inspection.

```
ASA-FW(config)# policy-map global_policy
ASA-FW(config-pmap)# class inspection_default
ASA-FW(config-pmap-c)# inspect icmp
ASA-FW(config-pmap-c)# exit
ASA-FW(config-pmap)# exit
```

R1#ping 10.1.102.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

ASA-FW(config)# sh debug

debug icmp trace enabled at level 1

```
ASA-FW(config)# ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=19
seq=0 len=72
ICMP echo reply from Outside:10.1.102.2 to Inside:10.1.101.1 ID=19 seq=0 len=72
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=19 seq=1 len=72
ICMP echo reply from Outside:10.1.102.2 to Inside:10.1.101.1 ID=19 seq=1 len=72
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=19 seq=2 len=72
ICMP echo reply from Outside:10.1.102.2 to Inside:10.1.101.1 ID=19 seq=2 len=72
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=19 seq=3 len=72
ICMP echo reply from Outside:10.1.102.2 to Inside:10.1.101.1 ID=19 seq=3 len=72
ICMP echo request from Inside:10.1.101.1 to Outside:10.1.102.2 ID=19 seq=4 len=72
ICMP echo reply from Outside:10.1.102.2 to Inside:10.1.101.1 ID=19 seq=4 len=72
```


This page is intentionally left blank.

Advanced CCIE SECURITY v4 LAB WORKBOOK

Site-to-Site VPN

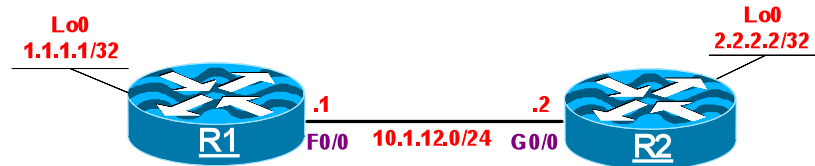
Narbik Kocharians
CCIE #12410 (R&S, Security, SP)
CCSI #30832

Piotr Matusiak
CCIE #19860 (R&S, Security)
C|EH, CCSI #33705

www.MicronicsTraining.com

Lab 1.36. Basic Site to Site IPSec VPN

Main Mode (IOS-IOS)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 120
- Configure Telnet on all routers using password "cisco"
- Configure static routing on R1 and R2 to be able to reach Loopback IP addresses

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/32
	F0/0	10.1.12.1/24
R2	F0/0	10.1.12.2/24
	Lo0	2.2.2.2/32

Task 1

Configure basic Site to Site IPSec VPN to protect traffic between IP addresses 1.1.1.1 and 2.2.2.2 using the following policy:

ISAKMP Policy	IPSec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Encryption: 3DES	Hash: MD5
Hash: MD5	Proxy ID: 1.1.1.1 ↔ 2.2.2.2
DH Group: 2	
PSK: cisco123	



ISAKMP (Internet Security Association and Key Management Protocol) is defined in RFC 2408 and it a framework which defines the following:

- procedures to authenticate a communicating peer*
- how to create and manage SAs (Security Associations)*
- key generation techniques*
- threat mitigation (like DoS and replay attacks)*

ISAKMP does not specify any details of key management or key exchange and is not bound to any key generation technique. Inside of ISAKMP, Cisco uses Oakley for the key exchange protocol. Oakley enables you to choose between different well-known DH (Diffie-Hellman) groups.

ISAKMP and Oakley create an authenticated, secure tunnel between two entities, and then negotiate the SA for IPSec. Both peers must authenticate each other and establish shared key. There are three authentication methods available: (1) RSA signatures (PKI), (2) RSA encrypted pseudo-random numbers (NONCES), and pre-shared keys (PSK). The DH protocol is used to agree on a common session key.

IPSec uses a different shared key from ISAKMP and Oakley. The IPSec shared key can be derived by using DH again to ensure PFS (Perfect Forward Secrecy) or by refreshing the shared secret derived from the original DH exchange.

IKE is a hybrid protocol which establishes a shared security policy and authenticated keys for services that require keys, such as IPSec. Before IPSec tunnel is established, each device must be able to identify its peer. ISAKMP and IKE are both used interchangeably, however these two items are somewhat different.

IKE Phase 1 - two ISAKMP peers establish a secure, authenticated channel. This channel is known as teh ISAKMP SA. There are two modes defined by ISAKMP: Main Mode and Aggressive Mode.

IKE Phase 2 - SAs are negotiated on behalf of services such as IPSec that needs keying material. This phase is called Quick Mode.

To configure IKE Phase 1 you need to create ISAKMP policies. It is possible to configure multiple policy statements with different configuration statements, and then let the two hosts come to an agreement.

You can use two methods to configure ISAKMP (IKE Phase 1):

I. Using PSK:

- 1. Configure ISAKMP protection suite (policy)*
 - Specify what size modulus to use for DH calculation (group1: 768bits; group2: 1024bits; group5: 1536bits)*

- Specify a hashing algorithm (MD5 or SHA)
 - Specify the lifetime of the SA (in seconds)
 - Specify the authentication method (PSK)
 - Specify encryption algorithm (DES, 3DES, AES)
2. Configure the ISAKMP pre-shared key (one per peer)

II. Using PKI

1. Create an RSA key for the router
2. Request certificate of the CA
3. Enroll certificates for the client router (certify your keys)
4. Configure ISAKMP protection suite (policy) like it is for PSK but specify *rsa-sig* as the authentication method

To configure IPsec (IKE Phase 2) do the following:

1. Create an extended ACL (determines interesting traffic - the traffic that should be protected by IPsec)
 2. Create IPsec transform set - like ISAKMP policies, transform sets are the setting suites to choose from
 3. Create crypto map to bind all components together:
 - Specify peer IP address
 - Specify SA lifetime (for IPsec SAs)
 - Specify transform sets
 - Specify the ACL to match interesting traffic
 4. Apply the crypto map to an egress interface
-

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# encr 3des
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2

R1(config-isakmp)#crypto isakmp key cisco123 address 10.1.12.2
```

Be careful of using leading spaces in pre-shared key value.
It may complicate seriously your lab exam. Remember that
the pre-shared key value must be the same at the both side
of a IPSEC tunnel.

```
R1(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac

R1(cfg-crypto-trans)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)# set peer 10.1.12.2
R1(config-crypto-map)# set transform-set TSET
R1(config-crypto-map)# match address 120

R1(config-crypto-map)#access-list 120 permit ip host 1.1.1.1 host
2.2.2.2

R1(config)#int f0/0
R1(config-if)#crypto map CMAP
R1(config-if)#exit
R1(config)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

ISAKMP is enabled and working. The router will be processing IKE packets (UDP protocol, port 500) for establishing ISAKMP "auxiliary" tunnel which will be used to negotiate securely parameters of an IPSec tunnel.

Step 2 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2

R2(config-isakmp)#crypto isakmp key cisco123 address 10.1.12.1

R2(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac

R2(cfg-crypto-trans)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R2(config-crypto-map)# set peer 10.1.12.1
R2(config-crypto-map)# set transform-set TSET
R2(config-crypto-map)# match address 120

R2(config-crypto-map)#access-list 120 permit ip host 2.2.2.2 host
1.1.1.1

R2(config)#int g0/0
R2(config-if)#crypto map CMAP
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Detailed verification on R1

Let's perform some debugging to see what's exactly going on during IPSec tunnel establishment. The best two debugs are: debug crypto isakmp and debug crypto ipsec.

To actually see something we need to pass 'interesting' traffic (defined by crypto ACL) which will trigger ISAKMP process.

```
R1#deb crypto isakmp
Crypto ISAKMP debugging is on
R1#deb crypto ipsec
Crypto IPSEC debugging is on
```

R1#ping 2.2.2.2 so 100

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
R1#
```

The first ICMP packet triggers ISAKMP process as this is our interesting traffic matching our ACL. Before actually start sending IKE packets to the peer the router first checks if there is any local SA (Security Association) matching that traffic. Note that this check is against IPSec SA not IKE SA. OK, no SA means there must be IKE packet send out.

```
IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 10.1.12.1, remote= 10.1.12.2,
local_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),
remote_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
```

```
ISAKMP:(0): SA request profile is (NULL)
```

The router has tried to find any IPSec SA matching outgoing connection but no valid SA has been found in Security Association Database (SADB) on the router.

```
ISAKMP: Created a peer struct for 10.1.12.2, peer port 500
ISAKMP: New peer created peer = 0x49E25A08 peer_handle = 0x80000003
ISAKMP: Locking peer struct 0x49E25A08, refcount 1 for isakmp_initiator
ISAKMP: local port 500, remote port 500
ISAKMP: set new node 0 to QM_IDLE
```




IKE Phase 1 (Main Mode) message 1

By default, IKE Main Mode is used so we should expect 6 packets for Phase 1. There is a message saying that Aggressive Mode cannot start, however it does not mean that there is some error, it just means that Aggressive Mode is not configured on the local router.

Then, the router checks ISAKMP policy configured and sees that there is PSK (Pre-Shared Key) authentication configured. It must check if there is a key for the peer configured as well.

After that the 1st IKE packet is sent out to the peer's IP address on port UDP 500 which is default.

The packet contains locally configured ISAKMP policy (or policies if many) to be chosen by the peer.

```
ISAKMP:(0):insert sa successfully sa = 48C5EC5C
```

```
ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
```

The router has started IKE Main Mode (it is a default)

```
ISAKMP:(0):found peer pre-shared key matching 10.1.12.2
```

Pre-shared key for remote peer has been found. ISAKMP will use it to authenticate the peer during one of the last stages of IKE Phase 1.

```
ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
```

```
ISAKMP:(0): constructed NAT-T vendor-07 ID
```

```
ISAKMP:(0): constructed NAT-T vendor-03 ID
```

```
ISAKMP:(0): constructed NAT-T vendor-02 ID
```

```
ISAKMP:(0):Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
```

```
ISAKMP:(0):Old State = IKE_READY New State = IKE_I_MM1
```

```
ISAKMP:(0): beginning Main Mode exchange
```

```
ISAKMP:(0): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) MM_NO_STATE
```

The router initiating IKE exchange is called "the initiator".
The router responding to IKE request is called "the responder".
The initiator (R1) has sent ISAKMP policy along with vendor specific IDs which are a part of IKE packet payload. MM_NO_STATE indicates that ISAKMP SA has been created, but nothing else has happened yet.

```
ISAKMP:(0):Sending an IKE IPv4 Packet.
```



IKE Phase 1 (Main Mode) message 2

OK, seems everything is going smooth, we have got a response packet from the peer. This is the first place where something could go wrong and this is most common issue when configuring VPNs. The received packet contains SA chosen by the peer and some other useful information like Vendor IDs. Those vendor specific payloads are used to discover NAT along the path and maintain keepalives (DPD). The router matches ISAKMP policy from the packet to one locally configured. If there is a match, the tunnel establishment process continues. If the policy configured on both routers is not the same, the cross-check process fails and the tunnel is down.

```
ISAKMP (0): received packet from 10.1.12.2 dport 500 sport 500 Global (I) MM_NO_STATE
```

The responder (R2) has responded with IKE packet that contains negotiated ISAKMP policy along with its vendor specific IDs. Note that the IKE Main Mode state is still MM_NO_STATE.

```
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
```

```
ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2
```

```
ISAKMP:(0): processing SA payload. message ID = 0
```

```
ISAKMP:(0): processing vendor id payload
```

```
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
```

```
ISAKMP (0): vendor ID is NAT-T RFC 3947
```

```
ISAKMP:(0):found peer pre-shared key matching 10.1.12.2
```

```
ISAKMP:(0): local preshared key found
```

```
ISAKMP : Scanning profiles for xauth ...
```

```
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
```

```
ISAKMP: encryption 3DES-CBC
```

```
ISAKMP: hash MD5
```

```
ISAKMP: default group 2
```

```
ISAKMP: auth pre-share
```

```
ISAKMP: life type in seconds
```

```
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
```

```
ISAKMP:(0):atts are acceptable. Next payload is 0
```

The router is processing ISAKMP parameters that have been sent as the reply.

Vendor IDs are processed to determine if peer supports e.g. NAT-Traversal, Dead Peer Detection feature. ISAKMP policy is checked against policies defined locally.

"atts are acceptable" indicates that ISAKMP policy matches with remote peer. Remember that comparing the policy that has been obtained from remote peer with locally defined policies starting from the lowest index (number) of policy defined in the running config.

```
ISAKMP:(0):Acceptable atts:actual life: 0
```

```
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.
```

The lifetime timer has been started. Note that default value of "lifetime" is used (86400 seconds). This is lifetime for ISAKMP SA. Note that IPSEC SAs have their own lifetime parameters which may be defined as number of seconds or kilobytes of transmitted traffic.

```
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2
```



IKE Phase 1 (Main Mode) message 3

The third message is sent out containing KE (Key Exchange) information for DH (Diffie-Hellman) secure key exchange process.

```
ISAKMP:(0): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3
```



IKE Phase 1 (Main Mode) message 4

4th message has been received from the peer. This message contains KE payload and based on that information both peers can generate a common session key to be used in securing further communication. The pre-shared key configured locally for the peer is used in this calculation.

After receiving this message peers can also be able to determine if there is a NAT along the path.

```
ISAKMP (0): received packet from 10.1.12.2 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4
```

"MM_SA_SETUP" indicates that the peers have agreed on parameters for the ISAKMP SA.

```

ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0): found peer pre-shared key matching 10.1.12.2
ISAKMP:(1002): processing vendor id payload
ISAKMP:(1002): vendor ID is Unity
ISAKMP:(1002): processing vendor id payload
ISAKMP:(1002): vendor ID is DPD
ISAKMP:(1002): processing vendor id payload
ISAKMP:(1002): speaking to another IOS box!
ISAKMP:received payload type 20
ISAKMP (1002): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1002): No NAT Found for self or peer
ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_I_MM4 New State = IKE_I_MM4

```



IKE Phase 1 (Main Mode) message 5

Fifth message is used for sending out authentication information the peer. This information is transmitted under the protection of the common shared secret.

```

ISAKMP:(1002):Send initial contact
ISAKMP:(1002):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1002): ID payload
    next-payload : 8
    type          : 1
    address       : 10.1.12.1
    protocol      : 17
    port          : 500
    length        : 12
ISAKMP:(1002):Total payload length: 12
ISAKMP:(1002): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) MM_KEY_EXCH

```

"MM_KEY_EXCH" indicates that the peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated. Note that the process of authentication has been just started.

```

ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Old State = IKE_I_MM4 New State = IKE_I_MM5

```



IKE Phase 1 (Main Mode) message 6

The peer identity is verified by the local router and SA is established.

*This message finishes ISAKMP Main Mode (Phase I) and the status is changed to **IKE_P1_COMPLETE**.*

```
ISAKMP (1002): received packet from 10.1.12.2 dport 500 sport 500 Global (I)
MM_KEY_EXCH
```

Note that the process of peer authentication is still in progress (MM_KEY_EXCH). Remember that there is also one IKE Main Mode state which is not visible in the debug output. It is "MM_KEY_AUTH" which indicates that the ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE and a Quick mode exchange begins.

```
ISAKMP:(1002): processing ID payload. message ID = 0
ISAKMP (1002): ID payload
    next-payload : 8
    type         : 1
    address      : 10.1.12.2
    protocol     : 17
    port         : 500
    length       : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1002): processing HASH payload. message ID = 0
ISAKMP:(1002):SA authentication status:
    authenticated
ISAKMP:(1002):SA has been authenticated with 10.1.12.2
ISAKMP: Trying to insert a peer 10.1.12.1/10.1.12.2/500/, and inserted successfully
49E25A08.
```

The peer has been authenticated now. Note that SA number has been generated and inserted into SADB along with the information relevant to the peer which has been agreed during IKE Main Mode.

```
ISAKMP:(1002):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_I_MM6

ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_I_MM6 New State = IKE_I_MM6

ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE
```



IKE Phase 2 (Quick Mode) message 1

Now it's time for Phase II which is Quick Mode (QM). The router sends out the packet containing local Proxy IDs (network/hosts addresses to be protected by the IPSec tunnel) and security policy defined by the Transform Set.

```
ISAKMP:(1002):beginning Quick Mode exchange, M-ID of 680665262
ISAKMP:(1002):QM Initiator gets spi
ISAKMP:(1002): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Node 680665262, Input = IKE_MSG_INTERNAL, IKE_INIT_QM
ISAKMP:(1002):Old State = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1002):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
```



IKE Phase 2 (Quick Mode) message 2

Second QM message is a response from the peer. It contains IPSec policy chosen by the peer and peer's proxy ID. This is a next place where something can go wrong if the Proxy IDs are different on both sides of the tunnel. The router cross-checks if its Proxy ID is a mirrored peer's Proxy ID.

```
ISAKMP (1002): received packet from 10.1.12.2 dport 500 sport 500 Global (I) QM_IDLE
```

The state of IKE is "QM_IDLE". This indicates that the ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

```
ISAKMP:(1002): processing HASH payload. message ID = 680665262
ISAKMP:(1002): processing SA payload. message ID = 680665262
ISAKMP:(1002):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 3600
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:(1002):atts are acceptable.
```

The routers are negotiating parameters for IPSec tunnel which will be used for traffic transmission. These parameters are defined by "crypto ipsec transform-set" command. Note that lifetime values of IPSec SA are visible

at this moment. You are able to set it both: globally or in the crypto map entry.

"Attr are acceptable" indicates that IPSec parameters defined as IPSec transform-set match at the both sides.

```
IPSEC(validate_proposal_request): proposal part #1
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.1.12.1, remote= 10.1.12.2,
local_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),
remote_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= NONE (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
Crypto mapdb : proxy_match
src addr      : 1.1.1.1
dst addr      : 2.2.2.2
protocol      : 0
src port      : 0
dst port      : 0
```

The local and remote proxy are defined. This indicates sources and destinations set in crypto ACL which defines the interesting traffic for the IPSec tunnel. Remember that the crypto ACL at the both sides of the tunnel must be "mirrored". If not, you may get the following entry in the debug output: IPSEC(initialize_sas): invalid proxy IDs.

```
ISAKMP:(1002): processing NONCE payload. message ID = 680665262
ISAKMP:(1002): processing ID payload. message ID = 680665262
ISAKMP:(1002): processing ID payload. message ID = 680665262
ISAKMP:(1002): Creating IPSec SAs
inbound SA from 10.1.12.2 to 10.1.12.1 (f/i) 0/0
(proxy 2.2.2.2 to 1.1.1.1)
has spi 0xB7629AFD and conn_id 0
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
outbound SA from 10.1.12.1 to 10.1.12.2 (f/i) 0/0
(proxy 1.1.1.1 to 2.2.2.2)
has spi 0xC486083C and conn_id 0
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
```

The IPSec SA have been created and inserted in the router's security associations database (SADB). SAs are distinguished by SPI values which are also used to differentiate many tunnels terminated on the same router. Note that two SPI values are generated for one tunnel: one SPI for inbound SA and one SPI for outbound SA. SPI value is inserted in the ESP header of the packet leaving the router. At the second side of the tunnel, SPI value inserted into the ESP header enables the router to reach parameters and keys which have been dynamically agreed during IKE negotiations or session key refreshment in case of lifetime timeout. The SPI value is an index of entities in the router's SADB.



IKE Phase 2 (Quick Mode) message 3

The last message finishes QM. Upon completion of Phase II IPsec session key is derived from new DH shared secret. This session key will be used for encryption until IPSec timer expires.

```
ISAKMP:(1002): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):deleting node 680665262 error FALSE reason "No Error"
ISAKMP:(1002):Node 680665262, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1002):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event with 1 KMI message(s)
Crypto mapdb : proxy_match
    src addr      : 1.1.1.1
    dst addr      : 2.2.2.2
    protocol      : 0
    src port      : 0
    dst port      : 0
IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer
10.1.12.2
IPSEC(policy_db_add_ident): src 1.1.1.1, dest 2.2.2.2, dest_port 0

IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.12.1, sa_proto= 50,
    sa_spi= 0xB7629AFD(3076692733),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
    sa_lifetime(k/sec)= (4449173/3600)
IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.12.2, sa_proto= 50,
    sa_spi= 0xC486083C(3297118268),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2004
    sa_lifetime(k/sec)= (4449173/3600)
IPSEC(update_current_outbound_sa): updated peer 10.1.12.2 current outbound sa to SPI
C486083C
R1#
```

All the negotiations have been completed. The tunnel is up and ready to pass the traffic.

Detailed verification on R2



IKE Phase 1 (Main Mode) message 1

First ISAKMP packet hits the router. It comes from port 500 to the port 500. The transport is UDP.

This packet contains ISAKMP policy (or policies) which are configured on remote peer. The local router needs to choose one which matches locally configured policy. This process is going until first match, so from a security perspective it is important to put more secure policy suites at the beginning (the crypto isakmp policy <ID> determines the order).

This debug output presents the IKE negotiation from the responder point of view. Only the most interesting entires or non-present in debug of the initiator are remarked and commented.

```
ISAKMP (0): received packet from 10.1.12.1 dport 500 sport 500 Global (N) NEW SA
ISAKMP: Created a peer struct for 10.1.12.1, peer port 500
ISAKMP: New peer created peer = 0x48AE852C peer_handle = 0x80000002
ISAKMP: Locking peer struct 0x48AE852C, refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500
ISAKMP:(0):insert sa successfully sa = 487BE048
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1

ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0): found peer pre-shared key matching 10.1.12.1
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ...
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
```

```

ISAKMP:(0):Fillatts in sa vpi_length:4
ISAKMP:(0):Fillatts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.

ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM1

```



IKE Phase 1 (Main Mode) message 2

The router sends back ISAKMP packet containing chosen ISAKMP policy. There are also other payloads attached to that message like Vendor ID (DPD, NAT-T).

```

ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(0): sending packet to 10.1.12.1 my_port 500 peer_port 500 (R) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM2

```



IKE Phase 1 (Main Mode) message 3

Now router receives packet containing KE payload. This is Diffie-Hellman exchange taking place to generate session key in secure manner. After receiving this packet the routers knows if there is NAT Traversal aware device on the other end and if NAT has been discovered along the path.

```

ISAKMP (0): received packet from 10.1.12.1 dport 500 sport 500 Global (R) MM_SA_SETUP
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_R_MM2 New State = IKE_R_MM3

ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 10.1.12.1

```

```
ISAKMP:(1001): processing vendor id payload
ISAKMP:(1001): vendor ID is DPD
ISAKMP:(1001): processing vendor id payload
ISAKMP:(1001): speaking to another IOS box!
```

Vendor specific IDs in the IKE packet payload tell the router that it is negotiating the ISAKMP SA with IOS router.

```
ISAKMP:(1001): processing vendor id payload
ISAKMP:(1001): vendor ID seems Unity/DPD but major 166 mismatch
ISAKMP:(1001): vendor ID is XAUTH
ISAKMP:received payload type 20
ISAKMP (1001): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1001): No NAT Found for self or peer
```

NAT-D payloads exchanged during NAT Discovery process tell the routers at the both ends that no NAT device has been found between the peers.

```
ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1001):Old State = IKE_R_MM3 New State = IKE_R_MM3
```



IKE Phase 1 (Main Mode) message 4

Local router sends out message with its KE payload to finish DH exchange.

```
ISAKMP:(1001): sending packet to 10.1.12.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1001):Old State = IKE_R_MM3 New State = IKE_R_MM4
```



IKE Phase 1 (Main Mode) message 5

Peer authentication taking place upon receiving 5th message.

```
ISAKMP (1001): received packet from 10.1.12.1 dport 500 sport 500 Global (R)
MM_KEY_EXCH
ISAKMP:(1001):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1001):Old State = IKE_R_MM4 New State = IKE_R_MM5

ISAKMP:(1001): processing ID payload. message ID = 0
ISAKMP (1001): ID payload
```

```

    next-payload : 8
    type         : 1
    address      : 10.1.12.1
    protocol     : 17
    port         : 500
    length       : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1001): processing HASH payload. message ID = 0
ISAKMP:(1001): processing NOTIFY INITIAL_CONTACT protocol 1
                spi 0, message ID = 0, sa = 487BE048
ISAKMP:(1001):SA authentication status:
                authenticated
ISAKMP:(1001):SA has been authenticated with 10.1.12.1
ISAKMP:(1001):SA authentication status:
                authenticated
ISAKMP:(1001): Process initial contact,
bring down existing phase 1 and 2 SA's with local 10.1.12.2 remote 10.1.12.1 remote
port 500
ISAKMP: Trying to insert a peer 10.1.12.2/10.1.12.1/500/, and inserted successfully
48AE852C.
ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1001):Old State = IKE_R_MM5  New State = IKE_R_MM5

```



IKE Phase 1 (Main Mode) message 6

The peer identity is verified by the local router and SA is established.

This message finishes ISAKMP Main Mode (Phase I) and the status is changed to IKE_P1_COMPLETE.

```

IPSEC(key_engine): got a queue event with 1 KMI message(s)
ISAKMP:(1001):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1001): ID payload
    next-payload : 8
    type         : 1
    address      : 10.1.12.2
    protocol     : 17
    port         : 500
    length       : 12
ISAKMP:(1001):Total payload length: 12
ISAKMP:(1001): sending packet to 10.1.12.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1001):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1001):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

```



IKE Phase 2 (Quick Mode) message 1

After completing Phase 1 the router receives first packet for Quick Mode (Phase 2).

The packet contains peer's Proxy IDs (network/hosts addresses to be protected by the IPSec tunnel) and security policy defined by the Transform Set. This must be checked against local configuration. If there is a match (crypto ACLs are mirrored and the IPSec encryption and authentication algorithms are agreed) the router continues Phase 2.

```
ISAKMP (1001): received packet from 10.1.12.1 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP: set new node -584676094 to QM_IDLE
ISAKMP:(1001): processing HASH payload. message ID = -584676094
ISAKMP:(1001): processing SA payload. message ID = -584676094
ISAKMP:(1001):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 3600
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:(1001):atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1
IPSEC(validate_proposal_request): proposal part #1,
    (key eng. msg.) INBOUND local= 10.1.12.2, remote= 10.1.12.1,
    local_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
    remote_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= NONE (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
Crypto mapdb : proxy_match
    src addr      : 2.2.2.2
    dst addr      : 1.1.1.1
    protocol      : 0
    src port      : 0
    dst port      : 0
ISAKMP:(1001): processing NONCE payload. message ID = -584676094
ISAKMP:(1001): processing ID payload. message ID = -584676094
ISAKMP:(1001): processing ID payload. message ID = -584676094
ISAKMP:(1001):QM Responder gets spi
ISAKMP:(1001):Node -584676094, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1001):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
ISAKMP:(1001): Creating IPSec SAs
    inbound SA from 10.1.12.1 to 10.1.12.2 (f/i)  0/ 0
    (proxy 1.1.1.1 to 2.2.2.2)
```

```
has spi 0xE272C715 and conn_id 0
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
outbound SA from 10.1.12.2 to 10.1.12.1 (f/i) 0/0
(proxy 2.2.2.2 to 1.1.1.1)
has spi 0x3E8C462 and conn_id 0
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
```



IKE Phase 2 (Quick Mode) message 2

The local router sends out its Proxy IDs and IPSec policy to the remote peer.

```
ISAKMP:(1001): sending packet to 10.1.12.1 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Node -584676094, Input = IKE_MSG_INTERNAL, IKE_GOT_SPI
ISAKMP:(1001):Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
IPSEC(key_engine): got a queue event with 1 KMI message(s)
Crypto mapdb : proxy_match
    src addr      : 2.2.2.2
    dst addr      : 1.1.1.1
    protocol      : 0
    src port      : 0
    dst port      : 0
IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer
10.1.12.1
IPSEC(policy_db_add_ident): src 2.2.2.2, dest 1.1.1.1, dest_port 0

IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.12.2, sa_proto= 50,
    sa_spi= 0xE272C715(3799172885),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
    sa_lifetime(k/sec)= (4595027/3600)
IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.12.1, sa_proto= 50,
    sa_spi= 0x3E8C462(65586274),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
    sa_lifetime(k/sec)= (4595027/3600)
```



IKE Phase 2 (Quick Mode) message 3

The last message finishes QM. Upon completion of Phase II IPSec session key is derived from new DH shared secret. This session key will be used for encryption until IPSec timer expires.

```

ISAKMP (1001): received packet from 10.1.12.1 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP:(1001):deleting node -584676094 error FALSE reason "QM done (await)"
ISAKMP:(1001):Node -584676094, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1001):Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event with 1 KMI message(s)
IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
IPSEC(key_engine_enable_outbound): enable SA with spi 65586274/50
IPSEC(update_current_outbound_sa): updated peer 10.1.12.1 current outbound sa to SPI
3E8C462
R2#

```

Verification



After establishing IPsec tunnel, we should see one ISAKMP SA and two IPsec SAs. This can be easily seen when entering the command "show crypto engine connections active". There are two useful commands to verify IPsec VPNs:

"show crypto isakmp sa" – displays ISAKMMP SA and gives us information about state of the tunnel establishment. QM_IDLE state means Quick Mode (Phase 2) has been finished. If something goes wrong, the state should give us information what phase or message has generated an error.

"show crypto ipsec sa" – displays IPsec SAs (inbound and outbound) and gives us information about Proxy IDs and number of packets being encrypted/decrypted. Inbound and outbound SA are described by SPI (Security Parameters Index) which is carried in ESP/AH header and allows router to differentiate between IPsec tunnels. Inbound SPI must be the same as Outbound SPI on the peer router.

R1#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.2	10.1.12.1	QM_IDLE	1002	ACTIVE

This is the normal state of established IKE tunnel.

IPv6 Crypto ISAKMP SA

R1#sh crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

```

    psk - Preshared key, rsig - RSA signature
    renc - RSA encryption
IPv4 Crypto ISAKMP SA

```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.12.1	10.1.12.2		ACTIVE	3des	md5	psk	2	23:57:08	

```

Engine-id:Conn-id = SW:2

```

Negotiated ISAKMP policy is visible. This command is useful to figure out which policy has been used for establishing the IKE tunnel when there are several policies matching at the both sides.

```
IPv6 Crypto ISAKMP SA
```

R1#sh crypto ipsec sa

```

interface: FastEthernet0/0
Crypto map tag: CMAP, local addr 10.1.12.1

```

This command shows information regarding the interfaces and defined crypto.

```

protected vrf: (none)
local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
current_peer 10.1.12.2 port 500

```

The proxies (source and destination of interesting traffic) are displayed. "0/0" after IP address and netmask indicates that IP protocol is transported in the tunnel.

```

PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

```

Very important output useful for the IPSec debugging and troubleshooting. This indicates that outgoing packets are: encapsulated by ESP, encrypted and digested (the hash has been made to discover any alterations). The second marked line indicates that incoming packets are: decapsulated (the IPSec header have been extracted), decrypted and hash/digest has been verified.

```

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

```

This output is relevant only when compression of IPSec packets is enabled in the transform-set.

```

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.12.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

```



```
current outbound spi: 0xC486083C(3297118268)
PFS (Y/N): N, DH group: none
```

If PFS (Perfect Forward Secrecy) has been enabled then the line above indicates that along with configured Diffie-Hellman group.

```
inbound esp sas:
```

```
spi: 0xB7629AFD(3076692733)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
```

```
conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4449172/3420)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

This output contains useful information relevant to unidirectional SA. This shows the following: used IPsec protocol (ESP), SPI value, used transform-set (encryption algorithm along with hash function), ESP mode (tunnel or transport), connection ID, crypto map and lifetime values in second and kilobytes which remains to session key refreshment (tunnel will be terminated instead of key refreshment if no packets need to be transported via tunnel when SA expired).

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
```

```
spi: 0xC486083C(3297118268)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4449172/3420)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R1#sh crypto ipsec sa identity

```
interface: FastEthernet0/0
Crypto map tag: CMAP, local addr 10.1.12.1

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer (none) port 500
  DENY, flags={ident_is_root,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

protected vrf: (none)
local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.0/0)
remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.0/0)
current_peer 10.1.12.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

```

R1#sh crypto ipsec sa address

```

fvrf/address: (none)/10.1.12.1
  protocol: ESP
    spi: 0xB7629AFD(3076692733)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: CMAP
      sa timing: remaining key lifetime (k/sec): (4449172/3386)
      IV size: 8 bytes
      replay detection support: Y
      Status: ACTIVE

fvrf/address: (none)/10.1.12.2
  protocol: ESP
    spi: 0xC486083C(3297118268)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: CMAP
      sa timing: remaining key lifetime (k/sec): (4449172/3386)
      IV size: 8 bytes
      replay detection support: Y
      Status: ACTIVE

```

R1#sh crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1002	IKE	MD5+3DES	0	0	10.1.12.1

2003	IPsec	3DES+MD5	0	4	10.1.12.1
2004	IPsec	3DES+MD5	4	0	10.1.12.1

One IPSec tunnel has three SA - one of IKE tunnel and two of IPSec tunnel used for traffic encryption.

R1#sh crypto engine connections dh

Number of DH's pregenerated = 2

DH lifetime = 86400 seconds

Software Crypto Engine:

Conn	Status	Group	Time left
1	Used	Group 2	85948

The Diffie-Hellman group and the time that remains to next DH key generation.

Verification performed on R2 (The responder).

R2#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.2	10.1.12.1	QM_IDLE	1002	ACTIVE

IPv6 Crypto ISAKMP SA

R2#sh crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.12.2	10.1.12.1		ACTIVE	3des md5	psk	2		23:55:03	

Engine-id:Conn-id = SW:2

IPv6 Crypto ISAKMP SA

R2#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: CMAP, local addr 10.1.12.2

protected vrf: (none)

local ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)

current_peer 10.1.12.1 port 500

```
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.1.12.2, remote crypto endpt.: 10.1.12.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xB7629AFD(3076692733)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
spi: 0xC486083C(3297118268)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4445162/3296)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
spi: 0xB7629AFD(3076692733)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4445162/3296)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R2#sh crypto ipsec sa address

```
fvr/f/address: (none)/10.1.12.2
```

```
protocol: ESP
spi: 0xC486083C(3297118268)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4445162/3287)
IV size: 8 bytes
replay detection support: Y
```

Status: ACTIVE

fvr/f/address: (none)/10.1.12.1

protocol: ESP

```
spi: 0xB7629AFD(3076692733)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4445162/3287)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

R2#sh crypto ipsec sa identity

interface: FastEthernet0/0

Crypto map tag: CMAP, local addr 10.1.12.2

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer (none) port 500
DENY, flags={ident_is_root,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

protected vrf: (none)
local  ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
current_peer 10.1.12.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

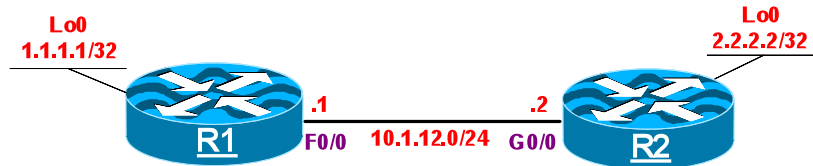
R2#sh crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1002	IKE	MD5+3DES	0	0	10.1.12.2
2003	IPsec	3DES+MD5	0	4	10.1.12.2
2004	IPsec	3DES+MD5	4	0	10.1.12.2

Lab 1.37. Basic Site to Site IPSec VPN

Aggressive Mode (IOS-IOS)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 120
- Configure Telnet on all routers using password "cisco"
- Configure static routing on R1 and R2 to be able to reach Loopback IP addresses

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/32
	F0/0	10.1.12.1/24
R2	F0/0	10.1.12.2/24
	Lo0	2.2.2.2/32

Task 1

Configure basic Site to Site IPSec VPN to protect traffic between IP addresses 1.1.1.1 and 2.2.2.2 using the following policy:

ISAKMP Policy	IPSec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Encryption: 3DES	Hash: MD5
Hash: MD5	Proxy ID: 1.1.1.1 ↔ 2.2.2.2
DH Group: 2	

Your solution must use only three messages during IKE Phase 1 SA establishment. Peer authentication should use password of "Aggressive123".



Aggressive Mode squeezes the IKE SA negotiation into three packets, with all data required for the SA passed by the initiator. The responder sends the proposal, key material and ID, and authenticates the session in the next packet. The initiator replies by authenticating the session. Negotiation is quicker, and the initiator and responder ID pass in the clear.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2

R1(config)#crypto isakmp peer address 10.1.12.2
R1(config-isakmp-peer)#set aggressive-mode client-endpoint ipv4-
address 10.1.12.2
R1(config-isakmp-peer)#set aggressive-mode password Aggressive123
```

The tunnel-password and the client endpoint type ID for IKE Aggressive Mode.

The "client-endpoint" parameter may be the following: ipv4-address (the ip address, ID: ID_IPV4), fqdn (the fully qualified domain name, ID: ID_FQDN), user-fqdn (e-mail address, ID: ID_USER_FQDN). These types of client-endpoint IDs are translated to the corresponding ID type in the Internet Key Exchange (IKE).

```
R1(config-isakmp-peer)#crypto ipsec transform-set TSET esp-3des
esp-md5-hmac

R1(cfg-crypto-trans)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.1.12.2
R1(config-crypto-map)#set transform-set TSET
R1(config-crypto-map)#match address 120

R1(config-crypto-map)#access-list 120 permit ip host 1.1.1.1 host
2.2.2.2
```

```

R1(config)#int f0/0
R1(config-if)#crypto map CMAP
R1(config-if)#exi
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON

```

Step 2 R2 configuration.

```

R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encr 3des
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2

R2(config)#crypto isakmp peer address 10.1.12.1
R2(config-isakmp-peer)#set aggressive-mode client-endpoint ipv4-
address 10.1.12.1
R2(config-isakmp-peer)#set aggressive-mode password Aggressive123

R2(config-isakmp-peer)#crypto ipsec transform-set TSET esp-3des
esp-md5-hmac

R2(cfg-crypto-trans)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R2(config-crypto-map)#set peer 10.1.12.1
R2(config-crypto-map)#set transform-set TSET
R2(config-crypto-map)#match address 120

R2(config-crypto-map)#access-list 120 permit ip host 2.2.2.2 host
1.1.1.1

R2(config)#int g0/0
R2(config-if)#crypto map CMAP
R2(config-if)#exi
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON

```

Verification

R1#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.2	10.1.12.1	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

ISAKMP SA has been negotiated and IKE tunnel is set up and active.

R1#sh crypto ipsec sa

```
interface: FastEthernet0/0
  Crypto map tag: CMAP, local addr 10.1.12.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
current_peer 10.1.12.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.12.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xD18E8F5F(3515780959)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xE40153C8(3825292232)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4534905/3541)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xD18E8F5F(3515780959)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4534905/3541)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

IPSec SAs have been negotiated. The tunnel is up.

R1#sh crypto ipsec sa identity

```
interface: FastEthernet0/0
  Crypto map tag: CMAP, local addr 10.1.12.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer (none) port 500
  DENY, flags={ident_is_root,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

protected vrf: (none)
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
current_peer 10.1.12.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0
```

R1#sh crypto ipsec sa address

```
fvr/f/address: (none)/10.1.12.1
  protocol: ESP
    spi: 0xE40153C8(3825292232)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4534905/3520)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

fvr/f/address: (none)/10.1.12.2
  protocol: ESP
    spi: 0xD18E8F5F(3515780959)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: CMAP
```

```

sa timing: remaining key lifetime (k/sec): (4534905/3520)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

R1#sh crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1001	IKE	MD5+3DES	0	0	10.1.12.1
2001	IPsec	3DES+MD5	0	4	10.1.12.1
2002	IPsec	3DES+MD5	4	0	10.1.12.1

R2#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.2	10.1.12.1	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

R2#sh crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
 K - Keepalives, N - NAT-traversal
 T - cTCP encapsulation, X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.12.2	10.1.12.1		ACTIVE	3des	md5	psk	2	23:52:03	

Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

R2#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: CMAP, local addr 10.1.12.2

protected vrf: (none)

local ident (addr/mask/prot/port): (2.2.2.2/255.255.255.0/0)

remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.0/0)

current_peer 10.1.12.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

```
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.2, remote crypto endpt.: 10.1.12.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xE40153C8(3825292232)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xD18E8F5F(3515780959)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4607831/3116)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xE40153C8(3825292232)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4607831/3116)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R2#sh crypto ipsec sa identity

```
interface: FastEthernet0/0
  Crypto map tag: CMAP, local addr 10.1.12.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer (none) port 500
  DENY, flags={ident_is_root,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0

protected vrf: (none)
local  ident (addr/mask/prot/port): (2.2.2.2/255.255.255.0/0)
remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.0/0)
current_peer 10.1.12.1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

R2#sh crypto ipsec sa address

```
fvr/f/address: (none)/10.1.12.2
  protocol: ESP
    spi: 0xD18E8F5F(3515780959)
      transform: esp-3des esp-md5-hmac ,
      in use settings = {Tunnel, }
      conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: CMAP
      sa timing: remaining key lifetime (k/sec): (4607831/3099)
      IV size: 8 bytes
      replay detection support: Y
      Status: ACTIVE

fvr/f/address: (none)/10.1.12.1
  protocol: ESP
    spi: 0xE40153C8(3825292232)
      transform: esp-3des esp-md5-hmac ,
      in use settings = {Tunnel, }
      conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: CMAP
      sa timing: remaining key lifetime (k/sec): (4607831/3099)
      IV size: 8 bytes
      replay detection support: Y
      Status: ACTIVE
```

R2#sh crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1001	IKE	MD5+3DES	0	0	10.1.12.2
2001	IPsec	3DES+MD5	0	4	10.1.12.2
2002	IPsec	3DES+MD5	4	0	10.1.12.2

Detailed verification on R1**R1#deb cry isak**

Crypto ISAKMP debugging is on

R1#deb cry ips

Crypto IPSEC debugging is on

R1#

R1#ping 2.2.2.2 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R1#

IPSEC(sa_request): ,

(key eng. msg.) OUTBOUND local= 10.1.12.1, remote= 10.1.12.2,
local_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),
remote_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0

ISAKMP:(0): SA request profile is (NULL)

ISAKMP: Created a peer struct for 10.1.12.2, peer port 500

ISAKMP: New peer created peer = 0x48AAB8D0 peer_handle = 0x80000004

ISAKMP: Locking peer struct 0x48AAB8D0, refcount 1 for isakmp_initiator

ISAKMP: local port 500, remote port 500

ISAKMP: set new node 0 to QM_IDLE

ISAKMP:(0):insert sa successfully sa = 49F4F45C

ISAKMP:(0):SA has tunnel attributes set.

ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID

ISAKMP:(0): constructed NAT-T vendor-07 ID

ISAKMP:(0): constructed NAT-T vendor-03 ID

ISAKMP:(0): constructed NAT-T vendor-02 ID

ISAKMP:(0):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR

ISAKMP (0): ID payload

next-payload : 13
type : 1
address : 10.1.12.2
protocol : 17
port : 0
length : 12

ISAKMP:(0):Total payload length: 12

ISAKMP:(0):Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_AM

ISAKMP:(0):Old State = IKE_READY New State = IKE_I_AM1

ISAKMP:(0): beginning Aggressive Mode exchange

ISAKMP:(0): sending packet to 10.1.12.2 my port 500 peer port 500 (I) AG_INIT_EXCH

IKE Aggressive Mode has been started. The state of ISAKMP SA is AG_INIT_EXCH which indicates that the peers have done the first exchange in aggressive mode, but the SA is not yet authenticated.

ISAKMP:(0):Sending an IKE IPv4 Packet.

ISAKMP (0): received packet from 10.1.12.2 dport 500 sport 500 Global (I) AG_INIT_EXCH

The remote peer (R2) responds with IKE packet that contains the following: its ISAKMP policy (proposal), key material and its ID. The state of ISAKMP SA is still AG_INIT_EXCH.

ISAKMP:(0): processing SA payload. message ID = 0

ISAKMP:(0): processing ID payload. message ID = 0

ISAKMP (0): ID payload

next-payload : 10
type : 1
address : 10.1.12.2
protocol : 0
port : 0
length : 12

ISAKMP:(0):: peer matches *none* of the profiles

ISAKMP:(0): processing vendor id payload

ISAKMP:(0): vendor ID is Unity

ISAKMP:(0): processing vendor id payload

ISAKMP:(0): vendor ID is DPD

ISAKMP:(0): processing vendor id payload

ISAKMP:(0): speaking to another IOS box!

ISAKMP:(0):SA using tunnel password as pre-shared key.

ISAKMP:(0): local preshared key found

ISAKMP : Scanning profiles for xauth ...

ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy

ISAKMP: encryption 3DES-CBC

ISAKMP: hash MD5

ISAKMP: default group 2

ISAKMP: auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80

ISAKMP:(0):atts are acceptable. Next payload is 0

The password configured for the peer as "aggressive-mode password" has been used for the peer authentication. ISAKMP proposal has been checked against locally defined ISAKMP policies.

ISAKMP:(0):Acceptable atts:actual life: 86400

ISAKMP:(0):Acceptable atts:life: 0

ISAKMP:(0):Fill atts in sa vpi_length:4

ISAKMP:(0):Fill atts in sa life_in_seconds:86400

ISAKMP:(0):Returning Actual lifetime: 86400

ISAKMP:(0)::Started lifetime timer: 86400.

```

ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):SA using tunnel password as pre-shared key.
ISAKMP:(1001): processing HASH payload. message ID = 0
ISAKMP:received payload type 20
ISAKMP (1001): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1001): No NAT Found for self or peer
ISAKMP:(1001):SA authentication status:
    authenticated
ISAKMP:(1001):SA has been authenticated with 10.1.12.2
ISAKMP: Trying to insert a peer 10.1.12.1/10.1.12.2/500/, and inserted successfully
48AAB8D0.
ISAKMP:(1001):Send initial contact
ISAKMP:(1001): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) AG_INIT_EXCH

```

The ISAKMP SA has been negotiated, authenticated and insterted into SADB. The peer has been informed that the connection has been authenticated. Phase 1 is completed. The ISAKMP SA state will be transited to QM_IDLE. The IKE tunnel is established and ready for IPSec parameters and SAs negotiations.

```

ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
ISAKMP:(1001):Old State = IKE_I_AM1 New State = IKE_P1_COMPLETE

ISAKMP:(1001):beginning Quick Mode exchange, M-ID of 1329820426
ISAKMP:(1001):QM Initiator gets spi
ISAKMP:(1001): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Node 1329820426, Input = IKE_MSG_INTERNAL, IKE_INIT_QM
ISAKMP:(1001):Old State = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1001):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (1001): received packet from 10.1.12.2 dport 500 sport 500 Global (I) QM_IDLE
ISAKMP:(1001): processing HASH payload. message ID = 1329820426
ISAKMP:(1001): processing SA payload. message ID = 1329820426
ISAKMP:(1001):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 3600
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:(1001):atts are acceptable. IPSec parameters have been agreed upon.
IPSEC(validate_proposal_request): proposal part #1
IPSEC(validate_proposal_request): proposal part #1,
    (key eng. msg.) INBOUND local= 10.1.12.1, remote= 10.1.12.2,

```



```
local_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),
remote_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= NONE (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
Crypto mapdb : proxy_match
    src addr      : 1.1.1.1
    dst addr      : 2.2.2.2
    protocol      : 0
    src port      : 0
    dst port      : 0
ISAKMP:(1001): processing NONCE payload. message ID = 1329820426
ISAKMP:(1001): processing ID payload. message ID = 1329820426
ISAKMP:(1001): processing ID payload. message ID = 1329820426
ISAKMP:(1001): Creating IPsec SAs
    inbound SA from 10.1.12.2 to 10.1.12.1 (f/i)  0/ 0
    (proxy 2.2.2.2 to 1.1.1.1)
    has spi 0xE40153C8 and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    outbound SA from 10.1.12.1 to 10.1.12.2 (f/i) 0/0
    (proxy 1.1.1.1 to 2.2.2.2)
    has spi 0xD18E8F5F and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
ISAKMP:(1001): sending packet to 10.1.12.2 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):deleting node 1329820426 error FALSE reason "No Error"
ISAKMP:(1001):Node 1329820426, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1001):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event with 1 KMI message(s)
Crypto mapdb : proxy_match
    src addr      : 1.1.1.1
    dst addr      : 2.2.2.2
    protocol      : 0
    src port      : 0
    dst port      : 0
IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer
10.1.12.2
IPSEC(policy_db_add_ident): src 1.1.1.1, dest 2.2.2.2, dest_port 0

IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.1.12.1, sa_proto= 50,
    sa_spi= 0xE40153C8(3825292232),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
    sa_lifetime(k/sec)= (4534906/3600)
IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.1.12.2, sa_proto= 50,
    sa_spi= 0xD18E8F5F(3515780959),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
    sa_lifetime(k/sec)= (4534906/3600)
```

```
IPSEC(update_current_outbound_sa): updated peer 10.1.12.2 current outbound sa to SPI
D18E8F5F
ISAKMP:(1001): no outgoing phase 1 packet to retransmit. QM_IDLE
```

IKE Phase 2 (Quick Mode) has been completed. ESP tunnel has been established.

Detailed verificatin on R2

```
ISAKMP (0): received packet from 10.1.12.1 dport 500 sport 500 Global (N) NEW SA
```

The responder has received the initial IKE packet from the initiator (R1). The payload contains ISAKMP proposal, key material and ID.

```
ISAKMP: Created a peer struct for 10.1.12.1, peer port 500
ISAKMP: New peer created peer = 0x49BD96B8 peer_handle = 0x80000003
ISAKMP: Locking peer struct 0x49BD96B8, refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500
ISAKMP:(0):insert sa successfully sa = 48B8E45C
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing ID payload. message ID = 0
ISAKMP (0): ID payload
    next-payload : 13
    type          : 1
    address       : 10.1.12.2
    protocol      : 17
    port          : 0
    length        : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0):SA using tunnel password as pre-shared key.
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ...
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
```

```
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.
```

The proposal has been processed by the responder and ISAKMP policy has been accepted.

```
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):SA using tunnel password as pre-shared key.
ISAKMP:(1001): processing vendor id payload
ISAKMP:(1001): vendor ID is DPD
ISAKMP:(1001): processing vendor id payload
ISAKMP:(1001): vendor ID seems Unity/DPD but major 151 mismatch
ISAKMP:(1001): vendor ID is XAUTH
ISAKMP:(1001): processing vendor id payload
ISAKMP:(1001): claimed IOS but failed authentication
ISAKMP:(1001): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(1001):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1001): ID payload
    next-payload : 10
    type         : 1
    address      : 10.1.12.2
    protocol     : 0
    port         : 0
    length       : 12
ISAKMP:(1001):Total payload length: 12
ISAKMP:(1001): sending packet to 10.1.12.1 my_port 500 peer_port 500 (R) AG_INIT_EXCH
```

The reply has been sent to the initiator. ISAKMP SA state is still AG_INIT_EXCH.

```
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
ISAKMP:(1001):Old State = IKE_READY New State = IKE_R_AM2
```

```
ISAKMP (1001): received packet from 10.1.12.1 dport 500 sport 500 Global (R)
AG_INIT_EXCH
```

The responder has got the information that SA has been authenticated

```
ISAKMP:(1001): processing HASH payload. message ID = 0
ISAKMP:received payload type 20
ISAKMP (1001): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1001): No NAT Found for self or peer
```

It has been determined by NAT discovery process that there is no NAT between the peers.

```
ISAKMP:(1001): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 48B8E45C
ISAKMP:(1001):SA authentication status:
authenticated
ISAKMP:(1001):SA has been authenticated with 10.1.12.1
ISAKMP:(1001):SA authentication status:
authenticated
ISAKMP:(1001): Process initial contact,
bring down existing phase 1 and 2 SA's with local 10.1.12.2 remote 10.1.12.1 remote
port 500
ISAKMP: Trying to insert a peer 10.1.12.2/10.1.12.1/500/, and inserted successfully
49BD96B8.
ISAKMP:(1001):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
ISAKMP:(1001):Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
```

IKE Phase 1 completed, SA is negotiated. The ISAKMP SA state has been changed to QM_IDLE.

```
IPSEC(key_engine): got a queue event with 1 KMI message(s)
ISAKMP (1001): received packet from 10.1.12.1 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP: set new node 1329820426 to QM_IDLE
ISAKMP:(1001): processing HASH payload. message ID = 1329820426
ISAKMP:(1001): processing SA payload. message ID = 1329820426
ISAKMP:(1001):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 3600
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:(1001):atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.1.12.2, remote= 10.1.12.1,
local_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
```

```
remote_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= NONE (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
Crypto mapdb : proxy_match
    src addr      : 2.2.2.2
    dst addr      : 1.1.1.1
    protocol      : 0
    src port      : 0
    dst port      : 0
ISAKMP:(1001): processing NONCE payload. message ID = 1329820426
ISAKMP:(1001): processing ID payload. message ID = 1329820426
ISAKMP:(1001): processing ID payload. message ID = 1329820426
ISAKMP:(1001):QM Responder gets spi
ISAKMP:(1001):Node 1329820426, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1001):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
ISAKMP:(1001): Creating IPsec SAs
    inbound SA from 10.1.12.1 to 10.1.12.2 (f/i)  0/ 0
    (proxy 1.1.1.1 to 2.2.2.2)
    has spi 0xD18E8F5F and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    outbound SA from 10.1.12.2 to 10.1.12.1 (f/i) 0/0
    (proxy 2.2.2.2 to 1.1.1.1)
    has spi 0xE40153C8 and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
ISAKMP:(1001): sending packet to 10.1.12.1 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Node 1329820426, Input = IKE_MSG_INTERNAL, IKE_GOT_SPI
ISAKMP:(1001):Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
IPSEC(key_engine): got a queue event with 1 KMI message(s)
Crypto mapdb : proxy_match
    src addr      : 2.2.2.2
    dst addr      : 1.1.1.1
    protocol      : 0
    src port      : 0
    dst port      : 0
IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer
10.1.12.1
IPSEC(policy_db_add_ident): src 2.2.2.2, dest 1.1.1.1, dest_port 0

IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.1.12.2, sa_proto= 50,
    sa_spi= 0xD18E8F5F(3515780959),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
    sa_lifetime(k/sec)= (4607832/3600)
IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.1.12.1, sa_proto= 50,
    sa_spi= 0xE40153C8(3825292232),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
```

```
sa_lifetime(k/sec)= (4607832/3600)
ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1001):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (1001): received packet from 10.1.12.1 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP:(1001):deleting node 1329820426 error FALSE reason "QM done (await)"
ISAKMP:(1001):Node 1329820426, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1001):Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event with 1 KMI message(s)
IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
IPSEC(key_engine_enable_outbound): enable SA with spi 3825292232/50
IPSEC(update_current_outbound_sa): updated peer 10.1.12.1 current outbound sa to SPI
E40153C8
ISAKMP:(1001):purging node 1329820426
```

The IPSec tunnel has been established.

Lab 1.38. Basic Site to Site VPN with NAT (IOS-IOS)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 120
- R2's G0/1 and R4's F0/0 interface should be configured in VLAN 240
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all routers to establish full connectivity

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/32
	F0/0	10.1.12.1/24
R2	G0/0	10.1.12.2/24
	G0/1	10.1.24.2/24
R4	F0/0	10.1.24.4/24
	Lo0	4.4.4.4/32

Task 1

Configure static NAT translation on R2 so that IP address of 10.1.12.1 will be seen on R4 as 10.1.24.1.

Configure basic Site to Site IPSec VPN to protect IP traffic between IP addresses 1.1.1.1 and 4.4.4.4 using the following policy:

ISAKMP Policy

IPSec Policy

Authentication: Pre-shared	Encryption: ESP-3DES
Encryption: 3DES	Hash: MD5
Hash: MD5	Proxy ID: 1.1.1.1 ↔ 4.4.4.4
DH Group: 2	
PSK: cisco123	

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip nat inside source static 10.1.12.1 10.1.24.1

%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed
state to up

Static network address translation (R1's Fa0/0: 10.1.12.1
-> 10.1.24.1)

R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config-if)#int g0/1
R2(config-if)#ip nat outside
```

Step 2 R1 configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2

R1(config-isakmp)#crypto isakmp key cisco123 address 10.1.24.4

From R1's perspective the peer (R4) is seen as 10.1.24.4.

R1(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac

R1(cfg-crypto-trans)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.1.24.4
R1(config-crypto-map)#set transform-set TSET
R1(config-crypto-map)#match address 140
```



```
R1(config-crypto-map)#access-list 140 permit ip host 1.1.1.1 ho
4.4.4.4
```

```
R1(config)#int f0/0
R1(config-if)#crypto map CMAP
R1(config-if)#exi
R1(config)#
%CRYPTO-6-ISA KMP_ON_OFF: ISAKMP is ON
```

Step 3 R4 configuration.

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)#encr 3des
R4(config-isakmp)#hash md5
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#group 2

R4(config-isakmp)#crypto isakmp key cisco123 address 10.1.24.1
```

From R4's perspective the peer (R1) is seen as 10.1.24.1
(this address R1's Fa0/0 is translated to by R2)

```
R4(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac

R4(cfg-crypto-trans)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R4(config-crypto-map)#set peer 10.1.24.1
R4(config-crypto-map)#set transform-set TSET
R4(config-crypto-map)#match address 140

R4(config-crypto-map)#access-list 140 permit ip ho 4.4.4.4 host
1.1.1.1

R4(config)#int f0/0
R4(config-if)#crypto map CMAP
R4(config-if)#exi
R4(config)#
%CRYPTO-6-ISA KMP_ON_OFF: ISAKMP is ON
```

Verification

R1#tel 10.1.24.4

Trying 10.1.24.4 ... Open

User Access Verification

Password:

R4>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:01:03	
*514 vty 0		idle	00:00:00	10.1.24.1

Translation is working.

Interface	User	Mode	Idle	Peer Address
R4>exit				

[Connection to 10.1.24.4 closed by foreign host]

R2#sh ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	10.1.24.1:13083	10.1.12.1:13083	10.1.24.4:23	10.1.24.4:23
---	10.1.24.1	10.1.12.1	---	---

Translation is working.

R1#ping 4.4.4.4 so lo0 rep 4

Type escape sequence to abort.

Sending 4, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

.!!!

Success rate is 75 percent (3/4), round-trip min/avg/max = 4/4/4 ms

Interesting traffic has started the tunnel negotiation.

R2#sh ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
udp	10.1.24.1:500	10.1.12.1:500	10.1.24.4:500	10.1.24.4:500
udp	10.1.24.1:4500	10.1.12.1:4500	10.1.24.4:4500	10.1.24.4:4500
---	10.1.24.1	10.1.12.1	---	---

Note that IKE traffic (UDP port 500) has been translated. During IKE Phase 1 NAT discovery has determined that traffic between the peer is translated, so that it enforces NAT Traversal. From this moment the peers transmit ESP packets encapsulated into UDP packets. The NAT-T traffic uses UDP port 4500.

R1#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.24.4	10.1.12.1	QM_IDLE	1003	ACTIVE

IPv6 Crypto ISAKMP SA

R1#sh crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1003	10.1.12.1	10.1.24.4		ACTIVE	3des	md5	psk	2	23:57:11	N
Engine-id:Conn-id = SW:3										

IPv6 Crypto ISAKMP SA

R1#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: CMAP, local addr 10.1.12.1

protected vrf: (none)

local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)

current_peer 10.1.24.4 port 4500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 10, #recv errors 0

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.24.4

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xE1815114(3783348500)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x65D0096B(1708132715)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 2005, flow_id: NETGX:5, sibling_flags 80000046, crypto map: CMAP

sa timing: remaining key lifetime (k/sec): (4378448/3532)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcsp sas:

```
outbound esp sas:
  spi: 0xE1815114(3783348500)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    conn id: 2006, flow_id: NETGX:6, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4378448/3532)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R1#sh crypto ipsec sa identity

```
interface: FastEthernet0/0
  Crypto map tag: CMAP, local addr 10.1.12.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer (none) port 500
  DENY, flags={ident_is_root,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

protected vrf: (none)
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)
current_peer 10.1.24.4 port 4500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 10, #recv errors 0
```

R1#sh crypto ipsec sa address

```
fvr/f/address: (none)/10.1.12.1
protocol: ESP
  spi: 0x65D0096B(1708132715)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
```

```

conn id: 2005, flow_id: NETGX:5, sibling_flags 80000046, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4378448/3510)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

```
fvr/f/address: (none)/10.1.24.4
```

```
protocol: ESP
```

```
spi: 0xE1815114(3783348500)
```

```
transform: esp-3des esp-md5-hmac ,
```

```
in use settings ={Tunnel UDP-Encaps, }
```

```
conn id: 2006, flow_id: NETGX:6, sibling_flags 80000046, crypto map: CMAP
```

```
sa timing: remaining key lifetime (k/sec): (4378448/3510)
```

```
IV size: 8 bytes
```

```
replay detection support: Y
```

```
Status: ACTIVE
```

R1#sh crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1003	IKE	MD5+3DES	0	0	10.1.12.1
2005	IPsec	3DES+MD5	0	3	10.1.12.1
2006	IPsec	3DES+MD5	3	0	10.1.12.1

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.24.4	10.1.24.1	QM_IDLE	1001	ACTIVE

Note that R4's ISAKMP SA is negotiated with translated R1's IP address.

IPv6 Crypto ISAKMP SA

R4#sh crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.24.4	10.1.24.1		ACTIVE	3des	md5	psk	2	23:49:57	N
Engine-id:Conn-id = SW:1										

IPv6 Crypto ISAKMP SA

R4#sh crypto ipsec sa

```
interface: FastEthernet0/0
  Crypto map tag: CMAP, local addr 10.1.24.4

protected vrf: (none)
local  ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
current_peer 10.1.24.1 port 4500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.24.4, remote crypto endpt.: 10.1.24.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x65D0096B(1708132715)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xE1815114(3783348500)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4581780/3076)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x65D0096B(1708132715)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4581780/3076)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R4#sh crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1001	IKE	MD5+3DES	0	0	10.1.24.4
2001	IPsec	3DES+MD5	0	3	10.1.24.4
2002	IPsec	3DES+MD5	3	0	10.1.24.4

Detailed verification on R1

R1#deb cry isak

Crypto ISAKMP debugging is on

R1#pi 4.4.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

ISAKMP:(0): SA request profile is (NULL)

ISAKMP: Created a peer struct for 10.1.24.4, peer port 500

ISAKMP: New peer created peer = 0x489472CC peer_handle = 0x8000000A

ISAKMP: Locking peer struct 0x489472CC, refcount 1 for isakmp_initiator

ISAKMP: local port 500, remote port 500

ISAKMP: set new node 0 to QM_IDLE

ISAKMP:(0):insert sa successfully sa = 483BFC34

ISAKMP:(0):Can not start Aggressive mode, trying Main mode.

ISAKMP:(0):found peer pre-shared key matching 10.1.24.4

ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID

ISAKMP:(0): constructed NAT-T vendor-07 ID

ISAKMP:(0): constructed NAT-T vendor-03 ID

ISAKMP:(0): constructed NAT-T vendor-02 ID

ISAKMP:(0):Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM

ISAKMP:(0):Old State = IKE_READY New State = IKE_I_MM1

ISAKMP:(0): beginning Main Mode exchange

ISAKMP:(0): sending packet to 10.1.24.4 my_port 500 peer_port 500 (I) MM_NO_STATE

ISAKMP:(0):Sending an IKE IPv4 Packet.

ISAKMP (0): received packet from 10.1.24.4 dport 500 sport 500 Global (I) MM_NO_STATE

ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH

ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2

ISAKMP:(0): processing SA payload. message ID = 0

ISAKMP:(0): processing vendor id payload

ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch

ISAKMP (0): vendor ID is NAT-T RFC 3947

ISAKMP:(0):found peer pre-shared key matching 10.1.24.4

ISAKMP:(0): local preshared key found

ISAKMP : Scanning profiles for xauth ...

ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable .!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
R1#atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.

ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM2

ISAKMP:(0): sending packet to 10.1.24.4 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3

ISAKMP (0): received packet from 10.1.24.4 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3  New State = IKE_I_MM4

ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 10.1.24.4
ISAKMP:(1005): processing vendor id payload
ISAKMP:(1005): vendor ID is Unity
ISAKMP:(1005): processing vendor id payload
ISAKMP:(1005): vendor ID is DPD
ISAKMP:(1005): processing vendor id payload
ISAKMP:(1005): speaking to another IOS box!
ISAKMP:received payload type 20
ISAKMP (1005): NAT found, both nodes inside NAT
ISAKMP:received payload type 20
ISAKMP (1005): My hash no match -  this node inside NAT
```

R1 has analyzed the results of NAT discovery. It has determined that its IP address is NATed in the path because received hash (NAT-D payload) does not match the locally calculated hash.

```
ISAKMP:(1005):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1005):Old State = IKE_I_MM4  New State = IKE_I_MM4
```



```
ISAKMP:(1005):Send initial contact
ISAKMP:(1005):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1005): ID payload
    next-payload : 8
    type          : 1
    address       : 10.1.12.1
    protocol      : 17
    port          : 0
    length        : 12
ISAKMP:(1005):Total payload length: 12
ISAKMP:(1005): sending packet to 10.1.24.4 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH
```

Note that from this moment the peers are exchanging the packets using UDP protocol and port 4500 (NAT-T).

```
ISAKMP:(1005):Sending an IKE IPv4 Packet.
ISAKMP:(1005):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1005):Old State = IKE_I_MM4 New State = IKE_I_MM5

ISAKMP (1005): received packet from 10.1.24.4 dport 4500 sport 4500 Global (I)
MM_KEY_EXCH
ISAKMP:(1005): processing ID payload. message ID = 0
ISAKMP (1005): ID payload
    next-payload : 8
    type          : 1
    address       : 10.1.24.4
    protocol      : 17
    port          : 0
    length        : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1005): processing HASH payload. message ID = 0
ISAKMP:(1005):SA authentication status:
    authenticated
ISAKMP:(1005):SA has been authenticated with 10.1.24.4
ISAKMP:(1005):Setting UDP ENC peer struct 0x49383A9C sa= 0x483BFC34
ISAKMP: Trying to insert a peer 10.1.12.1/10.1.24.4/4500/, and inserted successfully
489472CC.
ISAKMP:(1005):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1005):Old State = IKE_I_MM5 New State = IKE_I_MM6

ISAKMP:(1005):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1005):Old State = IKE_I_MM6 New State = IKE_I_MM6

ISAKMP:(1005):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1005):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE

ISAKMP:(1005):beginning Quick Mode exchange, M-ID of -1428024928
ISAKMP:(1005):QM Initiator gets spi
ISAKMP:(1005): sending packet to 10.1.24.4 my_port 4500 peer_port 4500 (I) QM_IDLE
ISAKMP:(1005):Sending an IKE IPv4 Packet.
```

```

ISAKMP:(1005):Node -1428024928, Input = IKE_MSG_INTERNAL, IKE_INIT_QM
ISAKMP:(1005):Old State = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP:(1005):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1005):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (1005): received packet from 10.1.24.4 dport 4500 sport 4500 Global (I) QM_IDLE
ISAKMP:(1005): processing HASH payload. message ID = -1428024928
ISAKMP:(1005): processing SA payload. message ID = -1428024928
ISAKMP:(1005):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 3 (Tunnel-UDP)

```

Note that this indicates that tunnel is encapsulated into UDP

```

ISAKMP:   SA life type in seconds
ISAKMP:   SA life duration (basic) of 3600
ISAKMP:   SA life type in kilobytes
ISAKMP:   SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:   authenticator is HMAC-MD5
ISAKMP:(1005):atts are acceptable.
ISAKMP:(1005): processing NONCE payload. message ID = -1428024928
ISAKMP:(1005): processing ID payload. message ID = -1428024928
ISAKMP:(1005): processing ID payload. message ID = -1428024928
ISAKMP:(1005): Creating IPSec SAs
    inbound SA from 10.1.24.4 to 10.1.12.1 (f/i) 0/ 0
    (proxy 4.4.4.4 to 1.1.1.1)
    has spi 0xE219E9BB and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    outbound SA from 10.1.12.1 to 10.1.24.4 (f/i) 0/0
    (proxy 1.1.1.1 to 4.4.4.4)
    has spi 0xE481597 and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
ISAKMP:(1005): sending packet to 10.1.24.4 my_port 4500 peer_port 4500 (I) QM_IDLE
ISAKMP:(1005):Sending an IKE IPv4 Packet.
ISAKMP:(1005):deleting node -1428024928 error FALSE reason "No Error"
ISAKMP:(1005):Node -1428024928, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1005):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
R1#
R1#un all
All possible debugging has been turned off

```

Detailed verification on R4

```

R4#deb cry isak
Crypto ISAKMP debugging is on

ISAKMP (0): received packet from 10.1.24.1 dport 500 sport 500 Global (N) NEW SA
ISAKMP: Created a peer struct for 10.1.24.1, peer port 500

```

```
ISAKMP: New peer created peer = 0x49CEE97C peer_handle = 0x80000004
ISAKMP: Locking peer struct 0x49CEE97C, refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500
ISAKMP:(0):insert sa successfully sa = 489FDD70
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1

ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vend
R4#or id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0):found peer pre-shared key matching 10.1.24.1
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ...
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.

ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
```

```
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM1

ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(0): sending packet to 10.1.24.1 my_port 500 peer_port 500 (R) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM2

ISAKMP (0): received packet from 10.1.24.1 dport 500 sport 500 Global (R) MM_SA_SETUP
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_R_MM2 New State = IKE_R_MM3

ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 10.1.24.1
ISAKMP:(1003): processing vendor id payload
ISAKMP:(1003): vendor ID is DPD
ISAKMP:(1003): processing vendor id payload
ISAKMP:(1003): speaking to another IOS box!
ISAKMP:(1003): processing vendor id payload
ISAKMP:(1003): vendor ID seems Unity/DPD but major 50 mismatch
ISAKMP:(1003): vendor ID is XAUTH
ISAKMP:received payload type 20
ISAKMP (1003): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1003): His hash no match - this node outside NAT
ISAKMP:(1003):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1003):Old State = IKE_R_MM3 New State = IKE_R_MM3
```

R4 has analyzed the results of NAT discovery. It has determined that R1's IP address is NATed in the path because received hash (NAT-D payload) does not match the locally calculated hash.

```
ISAKMP:(1003): sending packet to 10.1.24.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH
ISAKMP:(1003):Sending an IKE IPv4 Packet.
ISAKMP:(1003):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1003):Old State = IKE_R_MM3 New State = IKE_R_MM4

ISAKMP (1003): received packet from 10.1.24.1 dport 4500 sport 4500 Global (R)
MM_KEY_EXCH
ISAKMP:(1003):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1003):Old State = IKE_R_MM4 New State = IKE_R_MM5

ISAKMP:(1003): processing ID payload. message ID = 0
ISAKMP (1003): ID payload
    next-payload : 8
    type         : 1
    address      : 10.1.12.1
    protocol     : 17
```

```
        port          : 0
        length        : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1003): processing HASH payload. message ID = 0
ISAKMP:(1003): processing NOTIFY INITIAL_CONTACT protocol 1
        spi 0, message ID = 0, sa = 489FDD70
ISAKMP:(1003):SA authentication status:
        authenticated
ISAKMP:(1003):SA has been authenticated with 10.1.24.1
ISAKMP:(1003):Detected port floating to port = 4500
ISAKMP: Trying to find existing peer 10.1.24.4/10.1.24.1/4500/
ISAKMP:(1003):SA authentication status:
        authenticated
ISAKMP:(1003): Process initial contact,
bring down existing phase 1 and 2 SA's with local 10.1.24.4 remote 10.1.24.1 remote
port 4500
ISAKMP: Trying to insert a peer 10.1.24.4/10.1.24.1/4500/, and inserted successfully
49CEE97C.
ISAKMP:(1003):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1003):Old State = IKE_R_MM5 New State = IKE_R_MM5

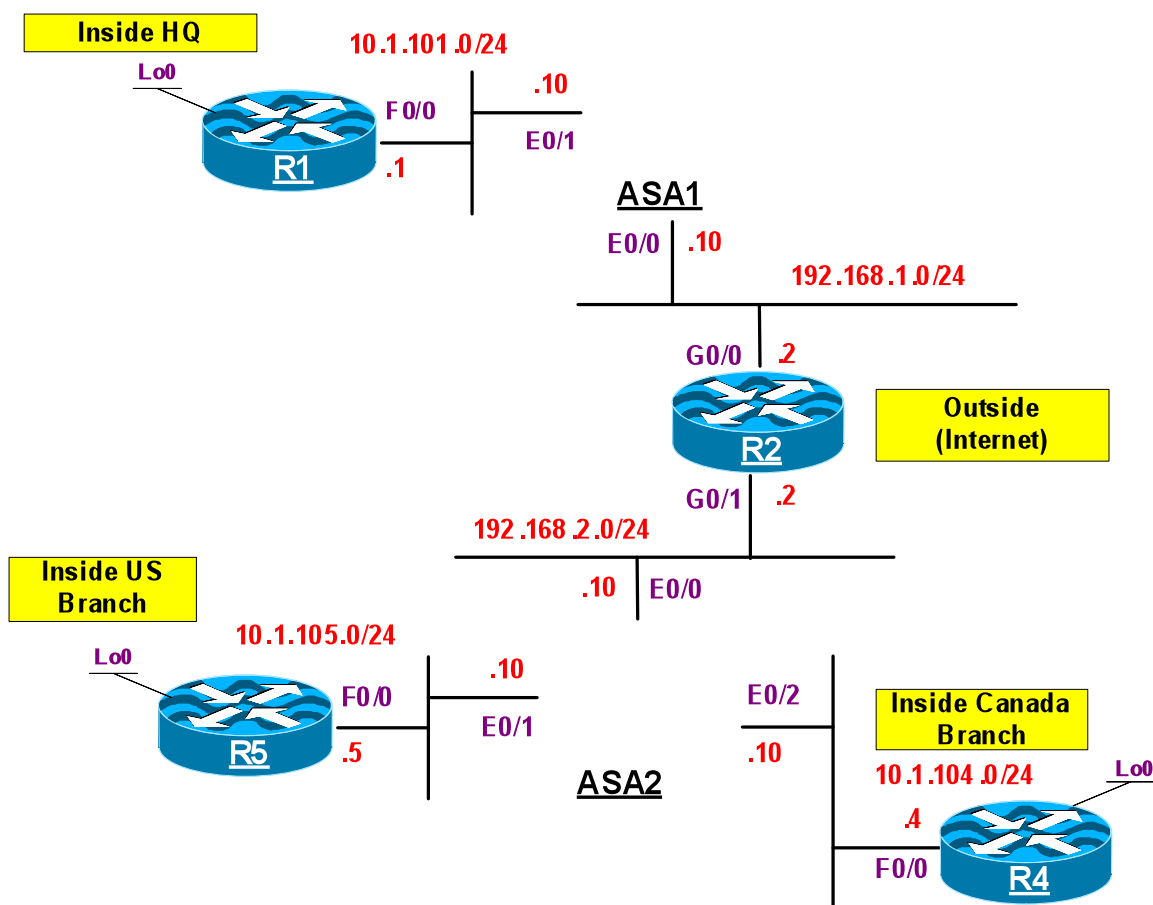
ISAKMP:(1003):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1003): ID payload
        next-payload : 8
        type          : 1
        address        : 10.1.24.4
        protocol       : 17
        port           : 0
        length         : 12
ISAKMP:(1003):Total payload length: 12
ISAKMP:(1003): sending packet to 10.1.24.1 my_port 4500 peer_port 4500 (R) MM_KEY_EXCH
ISAKMP:(1003):Sending an IKE IPv4 Packet.
ISAKMP:(1003):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1003):Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

ISAKMP:(1003):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1003):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (1003): received packet from 10.1.24.1 dport 4500 sport 4500 Global (R) QM_IDLE
ISAKMP: set new node -1428024928 to QM_IDLE
ISAKMP:(1003): processing HASH payload. message ID = -1428024928
ISAKMP:(1003): processing SA payload. message ID = -1428024928
ISAKMP:(1003):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 3 (Tunnel-UDP)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 3600
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
```

```
ISAKMP:(1003):atts are acceptable.
ISAKMP:(1003): processing NONCE payload. message ID = -1428024928
ISAKMP:(1003): processing ID payload. message ID = -1428024928
ISAKMP:(1003): processing ID payload. message ID = -1428024928
ISAKMP:(1003):QM Responder gets spi
ISAKMP:(1003):Node -1428024928, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1003):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
ISAKMP:(1003): Creating IPSec SAs
    inbound SA from 10.1.24.1 to 10.1.24.4 (f/i)  0/ 0
    (proxy 1.1.1.1 to 4.4.4.4)
    has spi 0xE481597 and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    outbound SA from 10.1.24.4 to 10.1.24.1 (f/i) 0/0
    (proxy 4.4.4.4 to 1.1.1.1)
    has spi 0xE219E9BB and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
ISAKMP:(1003): sending packet to 10.1.24.1 my_port 4500 peer_port 4500 (R) QM_IDLE
ISAKMP:(1003):Sending an IKE IPv4 Packet.
ISAKMP:(1003):Node -1428024928, Input = IKE_MESG_INTERNAL, IKE_GOT_SPI
ISAKMP:(1003):Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
ISAKMP (1003): received packet from 10.1.24.1 dport 4500 sport 4500 Global (R) QM_IDLE
ISAKMP:(1003):deleting node -1428024928 error FALSE reason "QM done (await)"
ISAKMP:(1003):Node -1428024928, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1003):Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
R4#
R4#un all
All possible debugging has been turned off
```

Lab 1.39. IOS Certificate Authority



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure IOS Certificate Authority server on R1. The server should have self-signed certificate with a lifetime of 5 years and grant certificates to the clients with a lifetime of 3 years. Store all certificates on the flash using PEM 64-base encryption with password of "Cisco_CA". The server should service all certificate requests automatically.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#ip http server
```

HTTP server must be enabled. It will be used for the automatic certificate enrollment. This feature uses SCEP (Simple Certificate Enrollment Protocol).

```
R1(config)#crypto pki server IOS_CA
```

```
R1(cs-server)#lifetime certificate 1095
```


The lifetime of client certificates (3 years).

```
R1(cs-server)#lifetime ca-certificate 1825
R1(cs-server)#database archive pem password Cisco_CA
R1(cs-server)#database url pem flash:/IOS_CA
R1(cs-server)#grant auto
%PKI-6-CS_GRANT_AUTO: All enrollment requests will be
automatically granted.
R1(cs-server)#no shutdown
Certificate server 'no shut' event has been queued for
processing.

R1(cs-server)#
%Some server settings cannot be changed after CA certificate
generation.
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

%SSH-5-ENABLED: SSH 1.99 has been enabled
% Exporting Certificate Server signing certificate and keys...

%PKI-6-CS_ENABLED: Certificate server now enabled.
R1(cs-server)#exit
```

CA is up after issuing "no shutdown" command. Remember
that at the lab exam.

Verification

R1#sh crypto pki server

```
Certificate Server IOS_CA:
  Status: enabled
  State: enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name: CN=IOS_CA
  CA cert fingerprint: 2CCFEC44 8B1FA216 4B9CA190 024184A0
  Granting mode is: auto
  Last certificate issued serial number: 0x1
  CA certificate expiration timer: 21:37:39 UTC Oct 19 2014
  CRL NextUpdate timer: 03:37:40 UTC Oct 21 2009
  Current primary storage dir: nvram:
  Current storage dir for .pem files: flash:/IOS_CA
  Database Level: Minimum - no cert data written to storage
```

R1#sh flash | in IOS CA

22 1714 Oct 20 2009 21:37:42 +00:00 IOS_CA_00001.pem

The password-protected certificate store has been created on the router flash.

Task 2

To ensure all devices in the network have the same time configure NTP server on R1 with a stratum of 4. The server should authenticate the clients with a password of "Cisco_NTP". Configure rest of devices as NTP clients to the R1's NTP source.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#ntp authentication-key 1 md5 Cisco_NTP
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate
R1(config)#ntp master 4
```

Step 2 ASA1 configuration.

```
ASA1(config)# ntp authentication-key 1 md5 Cisco_NTP
ASA1(config)# ntp authenticate
ASA1(config)# ntp trusted-key 1
ASA1(config)# ntp server 10.1.101.1 key 1

ASA1(config)# access-list OUTSIDE_IN permit udp any host
10.1.101.1 eq 123
ASA1(config)# access-group OUTSIDE_IN in interface Outside
```

The access from the NTP peers to NTP master (R1).

Step 3 ASA2 configuration.

```
ASA2(config)# ntp authentication-key 1 md5 Cisco_NTP
ASA2(config)# ntp authenticate
ASA2(config)# ntp trusted-key 1
ASA2(config)# ntp server 10.1.101.1 key 1
```

Step 4 R2 configuration.

```
R2(config)#ntp authentication-key 1 md5 Cisco_NTP
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
```

```
R2(config)#ntp server 10.1.101.1 key 1
```

```
R2(config)#ip route 10.1.101.0 255.255.255.0 192.168.1.10
```

```
R2(config)#ip route 10.1.105.0 255.255.255.0 192.168.2.10
```

```
R2(config)#ip route 10.1.104.0 255.255.255.0 192.168.2.10
```

Step 5 R4 configuration.

```
R4(config)#ntp authentication-key 1 md5 Cisco_NTP
```

```
R4(config)#ntp authenticate
```

```
R4(config)#ntp trusted-key 1
```

```
R4(config)#ntp server 10.1.101.1 key 1
```

Step 6 R5 configuration.

```
R5(config)#ntp authentication-key 1 md5 Cisco_NTP
```

```
R5(config)#ntp authenticate
```

```
R5(config)#ntp trusted-key 1
```

```
R5(config)#ntp server 10.1.101.1 key 1
```

Verification

R1#sh ntp status

```
Clock is synchronized, stratum 4, reference is 127.127.7.1
```

```
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
```

```
reference time is CE88ADA8.1FB35E7B (21:44:08.123 UTC Tue Oct 20 2009)
```

```
clock offset is 0.0000 msec, root delay is 0.00 msec
```

```
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

Note that R1 (the master) is synchronized with 127.127.7.1. This is an internally created IP address of internal NTP server which instance has been created after issuing "ntp master" command. With this internal address the R1's clock is synchronized. Remember, if you would be asked to enable a peer authentication on NTP master then you have to configure an peer ACLs and permit 127.127.7.1. Without doing that the NTP server will be always out of sync.

R1#sh ntp associations

address	ref clock	st	when	poll	reach	delay	offset	disp
*~127.127.7.1	127.127.7.1	3	2	64	377	0.0	0.00	0.0

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

ASA1(config)# sh ntp status

```
Clock is synchronized, stratum 5, reference is 10.1.101.1
```

```
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
```

```
reference time is ce88af37.bc6be95a (21:50:47.736 UTC Tue Oct 20 2009)
```

clock offset is -0.5972 msec, root delay is 0.98 msec
 root dispersion is 3891.33 msec, peer dispersion is 3890.69 msec

Note that ASA is associated with R1.

ASA1(config)# sh ntp associations

address	ref clock	st	when	poll	reach	delay	offset	disp
*~10.1.101.1	127.127.7.1	4	50	64	7	1.0	-0.60	3890.7

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

R1 is the NTP master and ASA is synced with it. The asterisk indicates that. Address field contains an IP address of the NTP peer. Ref clock field (reference clock) contains an IP address of reference clock of peer. Note that stratum for this peer is 5 (every next NTP peer in the NTP path will results of increased stratum value).

ASA2(config)# sh ntp status

Clock is synchronized, stratum 5, reference is 10.1.101.1
 nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
 reference time is ce88b2ee.eb59aae0 (22:06:38.919 UTC Tue Oct 20 2009)
 clock offset is 0.5964 msec, root delay is 1.27 msec
 root dispersion is 7891.36 msec, peer dispersion is 7890.73 msec

ASA2(config)# sh ntp associations

address	ref clock	st	when	poll	reach	delay	offset	disp
*~10.1.101.1	127.127.7.1	4	11	64	3	1.3	0.60	7890.7

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

R2#sh ntp status

Clock is synchronized, stratum 5, reference is 10.1.101.1
 nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
 reference time is CE88B210.397BFBDE (22:02:56.224 UTC Tue Oct 20 2009)
 clock offset is 1.3123 msec, root delay is 1.77 msec
 root dispersion is 15876.36 msec, peer dispersion is 15875.02 msec

R2#sh ntp associations

address	ref clock	st	when	poll	reach	delay	offset	disp
*~10.1.101.1	127.127.7.1	4	28	64	1	1.8	1.31	15875.

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

R4#sh ntp status

Clock is synchronized, stratum 5, reference is 10.1.101.1
 nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
 reference time is CE8B342F.39971B35 (19:42:39.224 UTC Thu Oct 22 2009)
 clock offset is 1.5869 msec, root delay is 2.15 msec
 root dispersion is 15876.62 msec, peer dispersion is 15875.02 msec

R4#sh ntp associations

```

address      ref clock    st  when  poll reach  delay  offset  disp
*~10.1.101.1 127.127.7.1    4   26    64    1    2.2    1.59 15875.
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configure

```

R5#sh ntp status

```

Clock is synchronized, stratum 5, reference is 10.1.101.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is CE88B28F.63FAD3D2 (22:05:03.390 UTC Tue Oct 20 2009)
clock offset is 2.5238 msec, root delay is 2.12 msec
root dispersion is 3877.93 msec, peer dispersion is 3875.38 msec

```

R5#sh ntp associations

```

address      ref clock    st  when  poll reach  delay  offset  disp
*~10.1.101.1 127.127.7.1    4   24    64    7    2.1    2.52 3875.4
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

```

Task 3

On both ASAs enroll a certificate for IPSec peer authentication. Ensure that FQDN and certificate attributes like Common Name and Country are used. Certificate uses for IPSec authentication should have at least 1024 bytes keys. Configure domain name of MicronicsTraining.com

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```

ASA1(config)# domain-name MicronicsTraining.com
ASA1(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-
RSA-Key>.

```

```

Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
ASA1(config)# crypto ca trustpoint IOS_CA
ASA1(config-ca-trustpoint)# id-usage ssl-ipsec

```

The certificate will be used for SSL or IPSec authentication.

```

ASA1(config-ca-trustpoint)# subject-name CN=ASA1, C=US
ASA1(config-ca-trustpoint)# fqdn ASA1.MicronicsTraining.com
ASA1(config-ca-trustpoint)# enrollment url http://10.1.101.1

```

```
ASA1(config-ca-trustpoint)# exit
ASA1(config)# crypto ca authenticate IOS_CA
```

```
INFO: Certificate has the following attributes:
Fingerprint:      2ccfec44 8b1fa216 4b9ca190 024184a0
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

The CA configured at 10.1.101.1 has been authenticated.
Authentication of the CA results of the root CA
certificate retrieval and writing it in the router's
configuration after the acceptance.

```
ASA1(config)# crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this password to the CA Administrator in order to revoke your
certificate. For security reasons your password will not be saved
in the configuration. Please make a note of it.
Password: *****
Re-enter password: *****

% The subject name in the certificate will be: CN=ASA1, C=US

% The fully-qualified domain name in the certificate will be:
ASA1.MicronicsTraining.com

% Include the device serial number in the subject name? [yes/no]:
no

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ASA1(config)# The certificate has been granted by CA!
```

The certificate has been issued automatically. Auto
enrollment is working

```
ASA1(config)# access-list OUTSIDE_IN permit tcp host 192.168.2.10
host 10.1.101.1 eq 80
```

SCEP (it uses HTTP protocol) for ASA2 should be allowed.

Step 2 ASA2 configuration.

```
ASA2(config)# domain-name MicronicsTraining.com
ASA2(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-
RSA-Key>.
```

```
Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
ASA2(config)# crypto ca trustpoint IOS_CA
ASA2(config-ca-trustpoint)# id-usage ssl-ipsec
ASA2(config-ca-trustpoint)# subject-name CN=ASA2, C=US
ASA2(config-ca-trustpoint)# fqdn ASA2.MicronicsTraining.com
ASA2(config-ca-trustpoint)# enrollment url http://10.1.101.1
ASA2(config-ca-trustpoint)# exit
ASA2(config)# crypto ca authenticate IOS_CA

INFO: Certificate has the following attributes:
Fingerprint:      2ccfec44 8b1fa216 4b9ca190 024184a0
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

ASA2(config)# crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this password to the CA Administrator in order to revoke your
certificate. For security reasons your password will not be saved
in the configuration. Please make a note of it.
Password: *****
Re-enter password: *****

% The subject name in the certificate will be: CN=ASA2, C=US

% The fully-qualified domain name in the certificate will be:
ASA2.MicronicsTraining.com

% Include the device serial number in the subject name? [yes/no]:
no

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ASA2(config)# The certificate has been granted by CA!
```

Verification

```
ASA1(config)# sh crypto ca trustpoints
```

```
Trustpoint IOS_CA:
  Subject Name:
  cn=IOS_CA
  Serial Number: 01
  Certificate configured.
```

CEP URL: http://10.1.101.1

ASA1(config)# sh crypto ca certificates

Certificate
Status: Available
Certificate Serial Number: 02
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Issuer Name:
 cn=IOS_CA
Subject Name:
 hostname=ASA1.MicronicsTraining.com
 cn=ASA1
 c=US
Validity Date:
 start date: 22:14:31 UTC Oct 20 2009
 end date: 22:14:31 UTC Oct 19 2012
Associated Trustpoints: IOS_CA

CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Public Key Type: RSA (1024 bits)
Issuer Name:
 cn=IOS_CA
Subject Name:
 cn=IOS_CA
Validity Date:
 start date: 21:37:39 UTC Oct 20 2009
 end date: 21:37:39 UTC Oct 19 2014
Associated Trustpoints: IOS_CA

This is the CA root certificate accepted during the trustpoint authentication.

ASA2(config)# sh crypto ca trustpoints

Trustpoint IOS_CA:
Subject Name:
 cn=IOS_CA
 Serial Number: 01
Certificate configured.
CEP URL: http://10.1.101.1

ASA2(config)# sh crypto ca certificates

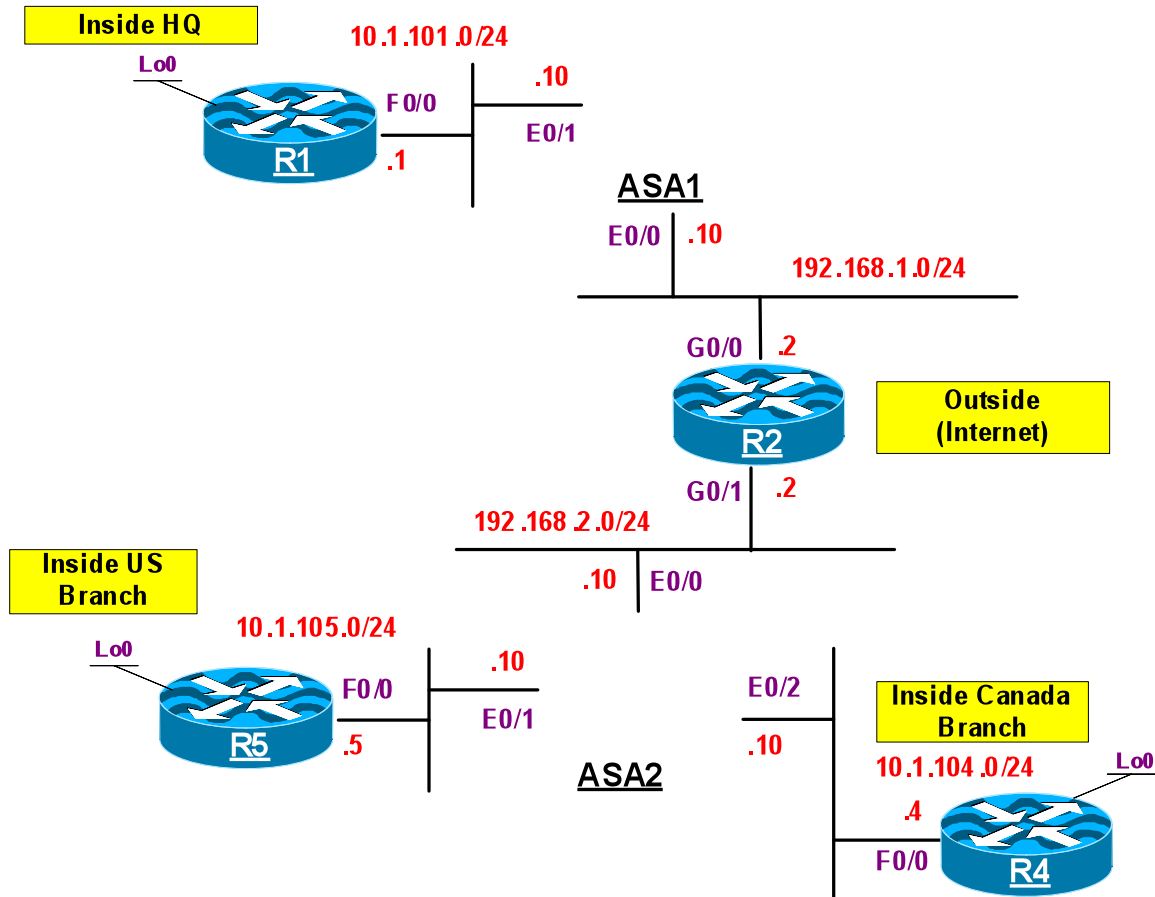
Certificate
Status: Available
Certificate Serial Number: 03

Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Issuer Name:
 cn=IOS_CA
Subject Name:
 hostname=ASA2.MicronicsTraining.com
 cn=ASA2
 c=US
Validity Date:
 start date: 22:19:48 UTC Oct 20 2009
 end date: 22:19:48 UTC Oct 19 2012
Associated Trustpoints: IOS_CA

CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Public Key Type: RSA (1024 bits)
Issuer Name:
 cn=IOS_CA
Subject Name:
 cn=IOS_CA
Validity Date:
 start date: 21:37:39 UTC Oct 20 2009
 end date: 21:37:39 UTC Oct 19 2014
Associated Trustpoints: IOS_CA

Lab 1.40. Site-to-Site IPSec VPN using PKI (ASA-ASA)

This lab is based on the previous lab configuration.



Task 1

Configure Site to Site IPSec VPN between ASA1 and ASA2. Ensure that only traffic between hosts 1.1.1.1 and 5.5.5.5 gets encrypted. Use Certificate Authority and keys/certificates enrolled in the previous lab.

Use the following setting for building the VPN:

ISAKMP Policy:

- Authentincation: RSA signatures
- Encryption 3DES
- Hash MD5

- DH Group 2

IPSec Policy:

- Encryption 3DES
- Hash MD5
- Enable PFS.

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```
ASA1(config)# crypto isakmp enable outside
```

```
ASA1(config)# access-list CRYPTO_ACL permit ip host 1.1.1.1 host  
5.5.5.5
```

```
ASA1(config)# tunnel-group 192.168.2.10 type ipsec-l2l  
ASA1(config)# tunnel-group 192.168.2.10 ipsec-attributes  
ASA1(config-tunnel-ipsec)# trust-point IOS_CA
```

The special arrangements for IPSec on ASA are configured in the tunnel-group configuration. The tunnel group has been pointed to valid CA. This CA will be used for peer authentication.

```
ASA1(config-tunnel-ipsec)# crypto isakmp policy 10  
ASA1(config-isakmp-policy)# auth rsa-sig
```

For peer authentication based on X509v3 certificates the authentication with RSA signatures has to be enabled in the ISAKMP policy.

```
ASA1(config-isakmp-policy)# encry 3des  
ASA1(config-isakmp-policy)# hash md5  
ASA1(config-isakmp-policy)# group 2
```

```
ASA1(config-isakmp-policy)# crypto ipsec transform-set TSET esp-  
3des esp-md5-hmac
```

```
ASA1(config)# crypto map ENCRYPT_OUT 1 match address CRYPTO_ACL  
ASA1(config)# crypto map ENCRYPT_OUT 1 set peer 192.168.2.10  
ASA1(config)# crypto map ENCRYPT_OUT 1 set pfs group2
```

The Perfect Forward Secrecy will be used along with 1024-bits RSA keys (DH Group 2).

```
ASA1(config)# crypto map ENCRYPT_OUT 1 set transform-set TSET
ASA1(config)# crypto map ENCRYPT_OUT 1 set trustpoint IOS_CA

ASA1(config)# crypto map ENCRYPT_OUT interface Outside

ASA1(config)# route inside 1.1.1.1 255.255.255.255 10.1.101.1
```

Step 2 ASA2 configuration.

```
ASA2(config)# crypto isakmp enable outside

ASA2(config)# access-list CRYPTO_ACL permit ip host 5.5.5.5 host
1.1.1.1

ASA2(config)# tunnel-group 192.168.1.10 type ipsec-l2l
ASA2(config)# tunnel-group 192.168.1.10 ipsec-attributes
ASA2(config-tunnel-ipsec)# trust-point IOS_CA

ASA2(config-tunnel-ipsec)# crypto isakmp policy 10
ASA2(config-isakmp-policy)# auth rsa-sig
ASA2(config-isakmp-policy)# encry 3des
ASA2(config-isakmp-policy)# hash md5
ASA2(config-isakmp-policy)# group 2

ASA2(config-isakmp-policy)# crypto ipsec transform-set TSET esp-
3des esp-md5-hmac

ASA2(config)# crypto map ENCRYPT_OUT 1 match address CRYPTO_ACL
ASA2(config)# crypto map ENCRYPT_OUT 1 set peer 192.168.1.10
ASA2(config)# crypto map ENCRYPT_OUT 1 set pfs group2
ASA2(config)# crypto map ENCRYPT_OUT 1 set transform-set TSET
ASA2(config)# crypto map ENCRYPT_OUT 1 set trustpoint IOS_CA

ASA2(config)# crypto map ENCRYPT_OUT interface Outside

ASA2(config)# route Inside_US 5.5.5.5 255.255.255.255 10.1.105.5
```

Verification

R1#ping 5.5.5.5 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

ASA1(config)# sh crypto isakmp

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1  IKE Peer: 192.168.2.10
    Type    : L2L           Role    : initiator
    Rekey   : no           State   : MM_ACTIVE
```

IKE tunnel has been established. Note that command outputs on ASA differ from command output from IOS router. The ASA distinguishes the role of the device in ISAKMP SA negotiation. Also Main Mode state is named differently. In this case MM_ACTIVE has the same meaning as QM_IDLE on the router.

```
Global IKE Statistics
Active Tunnels: 1
Previous Tunnels: 4
In Octets: 9216
In Packets: 50
In Drop Packets: 3
In Notifys: 27
In P2 Exchanges: 0
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 9724
Out Packets: 53
Out Drop Packets: 0
Out Notifys: 54
Out P2 Exchanges: 4
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 3
Initiator Tunnels: 4
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
```

Global IPSec over TCP Statistics

```
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
```

```
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Received ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
```

ASA1(config)# sh crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.2.10
    Type    : L2L                Role    : initiator
    Rekey    : no                State    : MM_ACTIVE
```

ASA1(config)# sh crypto ipsec sa

```
interface: Outside
Crypto map tag: ENCRYPT_OUT, seq num: 1, local addr: 192.168.1.10

access-list CRYPTO_ACL permit ip host 1.1.1.1 host 5.5.5.5
local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.0/0)
remote ident (addr/mask/prot/port): (5.5.5.5/255.255.255.0/0)
current_peer: 192.168.2.10

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.10, remote crypto endpt.: 192.168.2.10

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 5C4F95C0

inbound esp sas:
spi: 0x1AC28131 (448954673)
transform: esp-3des esp-md5-hmac no compression
in use settings = {L2L, Tunnel, PFS Group 2, }
slot: 0, conn_id: 16384, crypto-map: ENCRYPT_OUT
sa timing: remaining key lifetime (kB/sec): (3914999/28641)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
```

```

0x00000000 0x0000001F
outbound esp sas:
spi: 0x5C4F95C0 (1548719552)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 2, }
slot: 0, conn_id: 16384, crypto-map: ENCRYPT_OUT
sa timing: remaining key lifetime (kB/sec): (3914999/28641)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

ASA1(config)# sh vpn-sessiondb

Active Session Summary

Sessions:

	Active	Cumulative	Peak Concurrent	Inactive
SSL VPN	0	0	0	
Clientless only	0	0		0
With client	0	0		0 : 0
Email Proxy	0	0	0	
IPsec LAN-to-LAN	1	4		1
IPsec Remote Access	0	0	0	
VPN Load Balancing	0	0	0	
Totals	1	4		

License Information:

IPsec	: 250	Configured : 250	Active : 1	Load : 0%
SSL VPN	: 2	Configured : 2	Active : 0	Load : 0%

	Active	Cumulative	Peak Concurrent
IPsec	1	4	1
SSL VPN	0	0	0
AnyConnect Mobile	0	0	0
Linksys Phone	0	0	0
Totals	1	4	

Tunnels:

	Active	Cumulative	Peak Concurrent
IKE	1	4	1
IPsec	1	4	1
Totals	2	8	

Active NAC Sessions:

No NAC sessions to display

Active VLAN Mapping Sessions:

No VLAN Mapping sessions to display

ASA1(config)# sh vpn-sessiondb 121

Session Type: LAN-to-LAN

Connection : 192.168.2.10
Index : 4 IP Addr : 5.5.5.5
Protocol : IKE IPsec
Encryption : 3DES Hashing : MD5
Bytes Tx : 400 Bytes Rx : 400
Login Time : 10:03:25 UTC Sun Jul 18 2010
Duration : 0h:06m:18s

ASA2(config)# sh crypto isakmp

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 192.168.1.10
Type : L2L Role : responder
Rekey : no State : MM_ACTIVE

Global IKE Statistics

Active Tunnels: 1
Previous Tunnels: 4
In Octets: 12112
In Packets: 82
In Drop Packets: 3
In Notifys: 55
In P2 Exchanges: 4
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 3
Out Octets: 11028
Out Packets: 71
Out Drop Packets: 0
Out Notifys: 104
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0

Global IPSec over TCP Statistics

```
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Received ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
```

ASA2(config)# sh crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.1.10
    Type    : L2L                Role    : responder
    Rekey    : no                State    : MM_ACTIVE
```

ASA2(config)# sh crypto ipsec sa

```
interface: Outside
Crypto map tag: ENCRYPT_OUT, seq num: 1, local addr: 192.168.2.10

access-list CRYPTO_ACL permit ip host 5.5.5.5 host 1.1.1.1
local ident (addr/mask/prot/port): (5.5.5.5/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
current_peer: 192.168.1.10

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.2.10, remote crypto endpt.: 192.168.1.10

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 1AC28131

inbound esp sas:
spi: 0x5C4F95C0 (1548719552)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 2, }
```

```

slot: 0, conn_id: 16384, crypto-map: ENCRYPT_OUT
sa timing: remaining key lifetime (kB/sec): (4373999/28441)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x0000001F
outbound esp sas:
spi: 0x1AC28131 (448954673)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 2, }
slot: 0, conn_id: 16384, crypto-map: ENCRYPT_OUT
sa timing: remaining key lifetime (kB/sec): (4373999/28441)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x00000001

```

ASA2(config)# sh vpn-sessiondb detail

Active Session Summary

Sessions:

	Active	Cumulative	Peak Concurrent	Inactive
SSL VPN	0	0	0	0
Clientless only	0	0	0	0
With client	0	0	0	0
Email Proxy	0	0	0	0
IPsec LAN-to-LAN	1	4	1	1
IPsec Remote Access	0	0	0	0
VPN Load Balancing	0	0	0	0
Totals	1	4		

License Information:

IPsec	: 250	Configured : 250	Active : 1	Load : 0%
SSL VPN	: 2	Configured : 2	Active : 0	Load : 0%

	Active	Cumulative	Peak Concurrent
IPsec	1	4	1
SSL VPN	0	0	0
AnyConnect Mobile	0	0	0
Linksys Phone	0	0	0
Totals	1	4	

Tunnels:

	Active	Cumulative	Peak Concurrent
IKE	1	4	1
IPsec	1	4	1
Totals	2	8	

Active NAC Sessions:

No NAC sessions to display

Active VLAN Mapping Sessions:

No VLAN Mapping sessions to display

ASA2(config)# sh vpn-sessiondb 121

Session Type: LAN-to-LAN

```

Connection      : 192.168.1.10
Index           : 4                      IP Addr        : 1.1.1.1
Protocol        : IKE IPsec
Encryption      : 3DES                   Hashing         : MD5
Bytes Tx        : 400                     Bytes Rx        : 400
Login Time      : 10:03:25 UTC Sun Jul 18 2010
Duration        : 0h:06m:34s

```

Verification (detailed)

```

ASA1(config)# deb cry isakmp 9
ASA1(config)#
ASA1(config)# Jul 18 10:03:25 [IKEv1 DEBUG]: Pitcher: received a key acquire message,
spi 0x0
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE Initiator: New Phase 1, Intf Inside,
IKE Peer 192.168.2.10 local Proxy Address 1.1.1.1, remote Proxy Address 5.5.5.5,
Crypto map (ENCRYPT_OUT)
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing ISAKMP SA payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing NAT-Traversal VID ver 02
payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing NAT-Traversal VID ver 03
payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing NAT-Traversal VID ver
RFC payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing Fragmentation VID +
extended capabilities payload
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE
(0) total length : 168
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 128

```

Layout of IKE packet payloads presented (the both: sent and received)

```

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing SA payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Oakley proposal is acceptable
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Received NAT-Traversal ver 02 VID
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Received Fragmentation VID
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, IKE Peer included IKE fragmentation
capability flags: Main Mode:          True Aggressive Mode: True
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing ke payload

```

```
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing nonce payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing certreq payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing Cisco Unity VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing xauth V6 VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Send IOS VID
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Constructing ASA spoofing IOS Vendor
ID payload (version: 1.0.0, capabilities: 20000001)
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Send Altiga/Cisco VPN3000/Cisco ASA
GW VID
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing NAT-Discovery payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, computing NAT Discovery hash
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing NAT-Discovery payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, computing NAT Discovery hash
```

NAT-D payload has been prepared.

```
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 320
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 320
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing ke payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing ISA_KE payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing nonce payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing cert request payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Received Cisco Unity client VID
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Received xauth V6 VID
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Processing VPN3000/ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing VID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Received Altiga/Cisco VPN3000/Cisco
ASA GW VID
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing NAT-Discovery payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, computing NAT Discovery hash
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing NAT-Discovery payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, computing NAT Discovery hash
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Generating keys for Initiator...
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing ID payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing cert payload
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing RSA signature
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Computing hash for ISAKMP
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, constructing dpd vid payload
```

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + CERT (6) + SIG (9) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 865

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

NAT Discovery process has been performed. The devices are not behind the NAT.

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Rcv'd fragment from a new fragmentation set. Deleting any old fragments.

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Successfully assembled an encrypted pkt from rcv'd fragments!

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + CERT (6) + SIG (9) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 865

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing ID payload

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing cert payload

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing RSA signature

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Computing hash for ISAKMP

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Processing IOS keep alive payload: proposal=32767/32767 sec.

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, processing VID payload

Jul 18 10:03:25 [IKEv1 DEBUG]: IP = 192.168.2.10, Received DPD VID

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, Trying to find group via OU...

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, No Group found by matching OU(s) from ID payload: Unknown

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, Trying to find group via IKE ID...

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, No Group found by matching OU(s) from ID payload: Unknown

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, Trying to find group via IP ADDR...

The ASA has searched the ID for identify locally configured tunnel group. The IP address has been chosen.

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, Connection landed on tunnel_group 192.168.2.10

Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, peer ID type 9 received (DER_ASN1_DN)

Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Oakley begin quick mode

Jul 18 10:03:25 [IKEv1]: Group = 192.168.2.10, IP = 192.168.2.10, PHASE 1 COMPLETED

Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, Keep-alive type for this connection: DPD

Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Starting P1 rekey timer: 73440 seconds.

Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, IKE got SPI from key engine: SPI = 0x1ac28131

Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, oakley constructing quick mode

Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing blank hash payload

```
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing
IPSec SA payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing
IPSec nonce payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing
pfs ke payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing
proxy ID
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Transmitting
Proxy Id:
  Local host:  1.1.1.1  Protocol 0  Port 0
  Remote host: 5.5.5.5  Protocol 0  Port 0
```

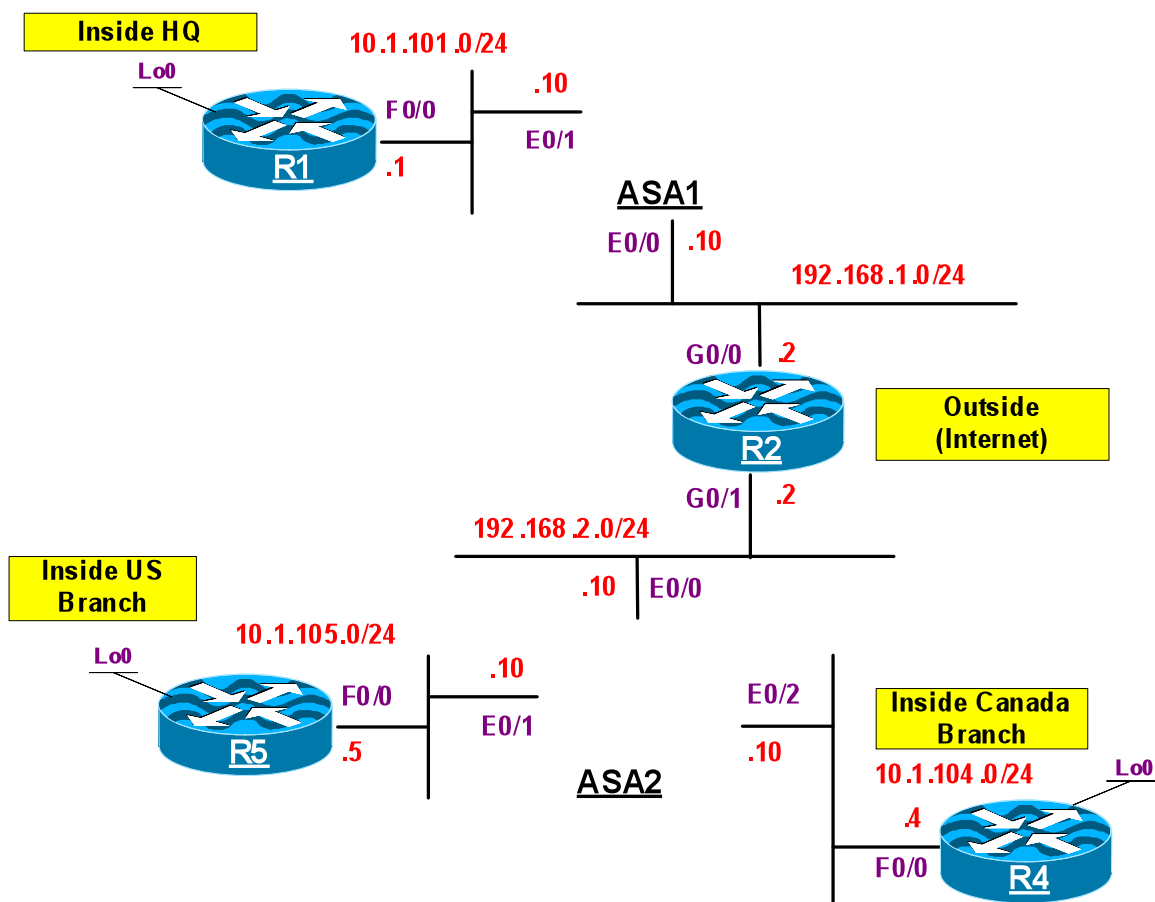
Local and remote proxies. The ip protocol between 1.1.1.1 and 5.5.5.5 will be encrypted.

```
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing qm
hash payload
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE SENDING Message (msgid=a0018003)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 320
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE RECEIVED Message
(msgid=a0018003) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + KE (4) + ID (5)
+ ID (5) + NONE (0) total length : 292
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing hash
payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing SA
payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing
nonce payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing ke
payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing
ISA_KE for PFS in phase 2
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing ID
payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing ID
payload
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, loading all
IPSEC SAs
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Generating
Quick Mode Key!
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, NP encrypt rule
look up for crypto map ENCRYPT_OUT 1 matching ACL CRYPTO_ACL: returned cs_id=d7cf5238;
rule=d79baf10
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Generating
Quick Mode Key!
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, NP encrypt rule
look up for crypto map ENCRYPT_OUT 1 matching ACL CRYPTO_ACL: returned cs_id=d7cf5238;
rule=d79baf10
```

```
Jul 18 10:03:25 [IKEv1]: Group = 192.168.2.10, IP = 192.168.2.10, Security negotiation
complete for LAN-to-LAN Group (192.168.2.10) Initiator, Inbound SPI = 0xlac28131,
Outbound SPI = 0x5c4f95c0
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, oakley
constructing final quick mode
Jul 18 10:03:25 [IKEv1]: IP = 192.168.2.10, IKE_DECODE SENDING Message (msgid=a0018003)
with payloads : HDR + HASH (8) + NONE (0) total length : 72
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, IKE got a
KEY_ADD msg for SA: SPI = 0x5c4f95c0
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Pitcher:
received KEY_UPDATE, spi 0xlac28131
Jul 18 10:03:25 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Starting P2
rekey timer: 24480 seconds.
Jul 18 10:03:25 [IKEv1]: Group = 192.168.2.10, IP = 192.168.2.10, PHASE 2 COMPLETED
(msgid=a0018003)
Jul 18 10:03:40 [IKEv1]: IP = 192.168.2.10, IKE_DECODE RECEIVED Message
(msgid=30705dbc) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length :
80
Jul 18 10:03:40 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing hash
payload
Jul 18 10:03:40 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, processing
notify payload
Jul 18 10:03:40 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Received keep-
alive of type DPD R-U-THERE (seq number 0x3990fdb6)
Jul 18 10:03:40 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, Sending keep-
alive of type DPD R-U-THERE-ACK (seq number 0x3990fdb6)
Jul 18 10:03:40 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing
blank hash payload
Jul 18 10:03:40 [IKEv1 DEBUG]: Group = 192.168.2.10, IP = 192.168.2.10, constructing qm
hash payload
Jul 18 10:03:40 [IKEv1]: IP = 192.168.2.10, IKE_DECODE SENDING Message (msgid=f34536d8)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80

ASA1(config)# un all
ASA1(config)#
```

Lab 1.41. Site-to-Site IPsec VPN using PKI (IOS-IOS)



This lab is based on previous lab configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"

- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure Site-to-Site IPSec Tunnel between R4 and R5 to encrypt traffic flows going between IP address of 4.4.4.4 and IP address of 5.5.5.5.

Use the following parameters for the tunnel:

- ISAKMP Parameters
 - Authentication: RSA Certificate
 - Encryption: 3DES
 - Group: 2
 - Hash: MD5
- IPSec Parameters
 - Encryption: ESP/3DES
 - Authentication: ESP/MD5

Use IOS CA server configured on R1 for certificate enrollment. Configure domain name of MicronicsTraining.com and ensure that FQDN and Country (US) are included in the certificate request.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config)#ip domain-name MicronicsTraining.com
R5(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R5.MicronicsTraining.com
```

```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
```

```
R5(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
R5(config)#crypto ca trustpoint IOS_CA
R5(ca-trustpoint)#usage ike
```

The usage of the certificate has been defined. The certificate is intended to use for IKE peer authentication.

```
R5(ca-trustpoint)#subject-name CN=R5, C=US
R5(ca-trustpoint)#enrollment url http://10.1.101.1
R5(ca-trustpoint)#exit
R5(config)#crypto ca authenticate IOS_CA
% Error in receiving Certificate Authority certificate: status =
FAIL, cert length = 0
%PKI-3-SOCKETSEND: Failed to send out message to CA server.
```

The above error indicates that there is a problem with connection to the CA. It seems like ASA is blocking that connection. Let's configure appropriate ACE in access list of OUTSIDE_IN (for R4 and R5)

Step 2 ASA1 configuration.

```
ASA1(config)# access-list OUTSIDE_IN permit tcp host 10.1.105.5
host 10.1.101.1 eq 80
ASA1(config)# access-list OUTSIDE_IN permit tcp host 10.1.104.4
host 10.1.101.1 eq 80
```

The SCEP has been allowed through ASA1.

Step 3 Certificate enrollment on R5.

```

R5(config)#crypto ca authenticate IOS_CA
Certificate has the following attributes:
    Fingerprint MD5: 01973E0C A51F6B10 CB074127 C07C60BC
    Fingerprint SHA1: 24A01750 51D02F6B 9BB419DE B6F40C72
B9E43EDD

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R5(config)#crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this password to the CA Administrator in order to revoke your
certificate. For security reasons your password will not be saved
in the configuration. Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: CN=R5, C=US
% The subject name in the certificate will include:
R5.MicronicsTraining.com
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOS_CA verbose' command will
show the fingerprint.

R5(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: 05D7E98F
E04055D7 AA68622D B48D6C92
CRYPTO_PKI: Certificate Request Fingerprint SHA1: 302D643E
69C6FECF 71984DF1 D29DB5ED C110B64F
R5(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority

R5(config)#crypto isakmp policy 10
R5(config-isakmp)#encr 3des
R5(config-isakmp)#hash md5
R5(config-isakmp)#authentication rsa-sig
R5(config-isakmp)#group 2

R5(config-isakmp)#crypto ipsec transform-set TSET esp-3des esp-

```

```
md5-hmac
R5(cfg-crypto-trans)#exit

R5(config)#access-list 120 permit ip host 5.5.5.5 host 4.4.4.4

R5(config)#crypto map ENCRYPT 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R5(config-crypto-map)#set peer 10.1.104.4
R5(config-crypto-map)#set transform-set TSET
R5(config-crypto-map)#match address 120
R5(config-crypto-map)#exit

R5(config)#int f0/0
R5(config-if)#crypto map ENCRYPT
```

Step 4 Certificate enrollment on R4.

```
R4(config)#ip domain-name MicronicsTraining.com
R4(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R4.MicronicsTraining.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable... [OK]

R4(config)#
Oct 22 19:45:14.441: %SSH-5-ENABLED: SSH 1.99 has been enabled

R4(config)#crypto ca trustpoint IOS_CA
R4(ca-trustpoint)#usage ike
R4(ca-trustpoint)#subject-name CN=R4, C=CA
R4(ca-trustpoint)#enrollment url http://10.1.101.1
R4(ca-trustpoint)#exit

R4(config)#crypto ca authenticate IOS_CA
Certificate has the following attributes:
    Fingerprint MD5: 01973E0C A51F6B10 CB074127 C07C60BC
    Fingerprint SHA1: 24A01750 51D02F6B 9BB419DE B6F40C72
B9E43EDD

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R4(config)#crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this password to the CA Administrator in order to revoke your
certificate. For security reasons your password will not be saved
```

in the configuration. Please make a note of it.

Password:

Re-enter password:

% The subject name in the certificate will include: CN=R4, C=CA

% The subject name in the certificate will include:

R4.MicronicsTraining.com

% Include the router serial number in the subject name? [yes/no]:

no

% Include an IP address in the subject name? [no]: no

Request certificate from CA? [yes/no]: yes

% Certificate request sent to Certificate Authority

% The 'show crypto ca certificate IOS_CA verbose' command will show the fingerprint.

R4(config)#

CRYPTO_PKI: Certificate Request Fingerprint MD5: D709C725

A0D9081A D8FA55B4 EAF866C6

CRYPTO_PKI: Certificate Request Fingerprint SHA1: A82A6373

70FEA31E AE3B1933 4965B8C0 41695706

R4(config)#

%PKI-6-CERTRET: Certificate received from Certificate Authority

R4(config)#crypto isakmp policy 10

R4(config-isakmp)#encr 3des

R4(config-isakmp)#hash md5

R4(config-isakmp)#authentication rsa-sig

R4(config-isakmp)#group 2

R4(config-isakmp)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac

R4(cfg-crypto-trans)#access-list 120 permit ip host 4.4.4.4 host 5.5.5.5

R4(config)#crypto map ENCRYPT 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

R4(config-crypto-map)#set peer 10.1.105.5

R4(config-crypto-map)#set transform-set TSET

R4(config-crypto-map)#match address 120

R4(config-crypto-map)#int f0/0

R4(config-if)#crypto map ENCRYPT

%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

Step 5 ASA2 configuration.

Since IPSec tunnel needs to be established between two peers which are on different interfaces of ASA but with the same security level of 100, this must be explicitly allowed.

```
ASA2(config)# same-security-traffic permit inter-interface
```

Verification

Run ping from R5's loopback0 towards R4's loopback0.

```
R5#pi 4.4.4.4 so lo0
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 5.5.5.5

```
.!!!!
```

Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms

```
R5#sh cry engine conn act
```

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1001	IKE	MD5+3DES	0	0	10.1.105.5
2001	IPsec	3DES+MD5	0	4	10.1.105.5
2002	IPsec	3DES+MD5	4	0	10.1.105.5

The tunnels have been established.

```
R5#sh crypto isakmp sa
```

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.104.4	10.1.105.5	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

```
R5#sh crypto ipsec sa
```

interface: FastEthernet0/0

Crypto map tag: ENCRYPT, local addr 10.1.105.5

protected vrf: (none)

```
local ident (addr/mask/prot/port): (5.5.5.5/255.255.255.0/0)
```

```
remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.0/0)
```

current_peer 10.1.104.4 port 500

PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 10.1.104.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xF1BDE182(4055753090)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xF37CEB79(4085050233)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4599543/3585)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xF1BDE182(4055753090)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4599543/3585)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R5#sh crypto session

Crypto session current status

```
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 10.1.104.4 port 500
IKE SA: local 10.1.105.5/500 remote 10.1.104.4/500 Active
IPSEC FLOW: permit ip host 5.5.5.5 host 4.4.4.4
Active SAs: 2, origin: crypto map
```

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.104.4	10.1.105.5	QM_IDLE	1004	ACTIVE

IPv6 Crypto ISAKMP SA

R4#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: ENCRYPT, local addr 10.1.104.4

protected vrf: (none)

local ident (addr/mask/prot/port): (4.4.4.4/255.255.255/0/0)

remote ident (addr/mask/prot/port): (5.5.5.5/255.255.255/0/0)

current_peer 10.1.105.5 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 10.1.105.5

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xF37CEB79(4085050233)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xF1BDE182(4055753090)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 2007, flow_id: NETGX:7, sibling_flags 80000046, crypto map: ENCRYPT

sa timing: remaining key lifetime (k/sec): (4417938/3561)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xF37CEB79(4085050233)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 2008, flow_id: NETGX:8, sibling_flags 80000046, crypto map: ENCRYPT

sa timing: remaining key lifetime (k/sec): (4417938/3561)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

R4#sh crypto session

Crypto session current status

Interface: FastEthernet0/0

Session status: UP-ACTIVE

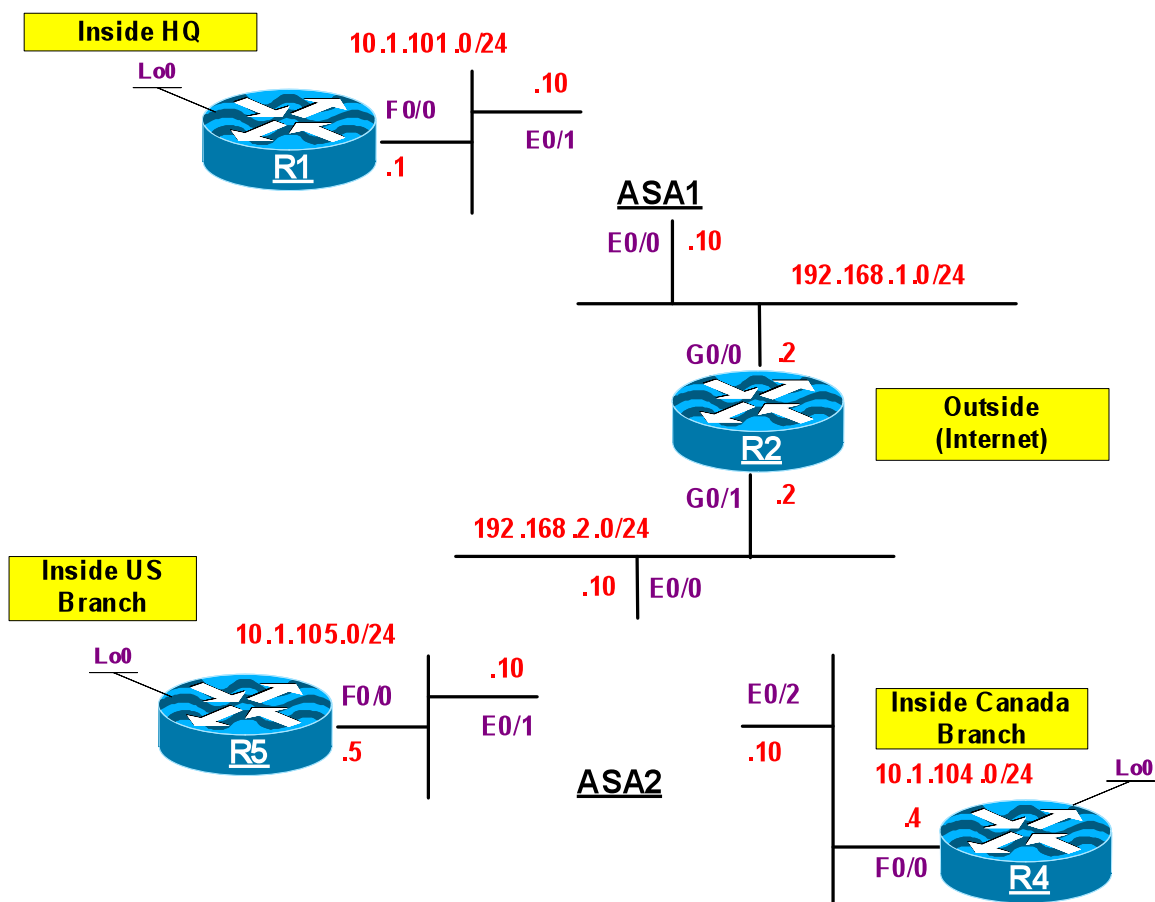
Peer: 10.1.105.5 port 500

IKE SA: local 10.1.104.4/500 remote 10.1.105.5/500 Active

IPSEC FLOW: permit ip host 4.4.4.4 host 5.5.5.5

Active SAs: 2, origin: crypto map

Lab 1.42. Site-to-Site IPsec VPN using PKI (Static IP IOS-ASA)



This lab is based on previous lab configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"

- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

There is Company's Headquarters in US consists of ASA1 and R1. The Company has two branch offices: one in US (R5) and other in Canada (R4). All routers use static IP while connecting to the Internet.

Configure the following Site-to-Site IPSec Tunnels:

Tunnel Endpoint	SRC Network	DST Network	ISAKMP Policy	IPSec Policy
R5 – ASA1	5.5.5.5	1.1.1.1	Authentication: RSA Encryption: 3DES Group: 2 Hash: MD5	Encryption: ESP/3DES Authentication: ESP/MD5

R4 – ASA1	4.4.4.4	1.1.1.1	Authentication: RSA Encryption: DES Group: 2 Hash: SHA	Encryption: ESP/DES Authentication: ESP/SHA

Use IOS CA server configured on R1 for certificate enrollment. Configure domain name of MicronicsTraining.com and ensure that FQDN and Country are included in the certificate request. Enable Perfect Forward Secrecy feature.

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```
ASA1(config)# domain-name MicronicsTraining.com
ASA1(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-
Key>.
```

```
Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
```

```
ASA1(config)# crypto ca trustpoint IOS_CA
ASA1(config-ca-trustpoint)# id-usage ssl-ipsec
ASA1(config-ca-trustpoint)# subject-name CN=ASA1, C=US
ASA1(config-ca-trustpoint)# fqdn ASA1.MicronicsTraining.com
ASA1(config-ca-trustpoint)# enrollment url http://10.1.101.1
ASA1(config-ca-trustpoint)# exit
ASA1(config)# crypto ca authenticate IOS_CA
```

```
INFO: Certificate has the following attributes:
Fingerprint:      01973e0c a51f6b10 cb074127 c07c60bc
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

```
ASA1(config)# crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
password to the CA Administrator in order to revoke your
certificate.
For security reasons your password will not be saved in the
configuration.
Please make a note of it.
```

```
Password: *****
Re-enter password: *****

% The subject name in the certificate will be: CN=ASA1, C=US

% The fully-qualified domain name in the certificate will be:
ASA1.MicronicsTraining.com

% Include the device serial number in the subject name? [yes/no]:
no

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ASA1(config)# The certificate has been granted by CA!

ASA1(config)# crypto isakmp enable outside

ASA1(config)# crypto isakmp policy 10
ASA1(config-isakmp-policy)# auth rsa-sig
ASA1(config-isakmp-policy)# enc 3des
ASA1(config-isakmp-policy)# has md5
ASA1(config-isakmp-policy)# gr 2

ASA1(config-isakmp-policy)# crypto isakmp policy 20
ASA1(config-isakmp-policy)# auth rsa-sig
ASA1(config-isakmp-policy)# enc des
ASA1(config-isakmp-policy)# ha sha
ASA1(config-isakmp-policy)# gr 2
ASA1(config-isakmp-policy)# exit

ASA1(config)# tunnel-group 10.1.105.5 type ipsec-l2l
ASA1(config)# tunnel-group 10.1.105.5 ipsec-attr
ASA1(config-tunnel-ipsec)# peer-id-validate nocheck
```

The "peer-id-validate" command has three options:

- * Required = Enable the IKE peer identity validation feature. If a peer's certificate does not provide sufficient information to perform an identity check, drop the tunnel.
- * If supported by certificate = Enable the IKE peer identity validation feature. If a peer's certificate does not provide sufficient information to perform an identity check, allow the tunnel.
- * Do not check = Do not check the peer's identity at all. Selecting this option disables the feature.

The default option is "required", meaning that if the remote peer does not provide correct identity information during IKE Phase 1, the tunnel will fail. What does the ASA do? It checks if peer's identity (default is an IP address)

is included in certificate's Subject Alt Name.

Hence, we have two options here:

- (1) Disable this feature on the ASA by issuing "peer-id-validate nocheck" command
- (2) Send correct identity info from peers, by issuing "crypto isakmp identity dn" command on R4 and R5

```
ASA1(config-tunnel-ipsec)# trust-point IOS_CA
```

```
ASA1(config-tunnel-ipsec)# tunnel-group 10.1.104.4 type ipsec-l2l
```

```
ASA1(config)# tunnel-group 10.1.104.4 ipsec-attr
```

```
ASA1(config-tunnel-ipsec)# peer-id-validate nocheck
```

```
ASA1(config-tunnel-ipsec)# trust-point IOS_CA
```

```
ASA1(config-tunnel-ipsec)# exit
```

```
ASA1(config)# crypto ipsec transform-set TSET_US esp-3des esp-md5-hmac
```

```
ASA1(config)# crypto ipsec transform-set TSET_CA esp-des esp-sha-hmac
```

```
ASA1(config)# access-list ACL_US permit ip ho 1.1.1.1 ho 5.5.5.5
```

```
ASA1(config)# access-list ACL_CA permit ip ho 1.1.1.1 ho 4.4.4.4
```

The crypto ACLs that enable the ASA and its peers to traffic encryption throughout tunnels terminated on ASA's outside interface.

```
ASA1(config)# crypto map ENCRYPT_OUT 1 match address ACL_US
```

```
ASA1(config)# crypto map ENCRYPT_OUT 1 set transform TSET_US
```

```
ASA1(config)# crypto map ENCRYPT_OUT 1 set trustpoint IOS_CA
```

```
ASA1(config)# crypto map ENCRYPT_OUT 1 set peer 10.1.105.5
```

```
ASA1(config)# crypto map ENCRYPT_OUT 1 set pfs group2
```

```
ASA1(config)# crypto map ENCRYPT_OUT 2 match address ACL_CA
```

```
ASA1(config)# crypto map ENCRYPT_OUT 2 set transform TSET_CA
```

```
ASA1(config)# crypto map ENCRYPT_OUT 2 set trustpoint IOS_CA
```

```
ASA1(config)# crypto map ENCRYPT_OUT 2 set peer 10.1.104.4
```

```
ASA1(config)# crypto map ENCRYPT_OUT 2 set pfs group2
```

```
ASA1(config)# crypto map ENCRYPT_OUT interface Outside
```

```
ASA1(config)# route Inside 1.1.1.1 255.255.255.255 10.1.101.1
```

```
ASA1(config)# access-list OUTSIDE_IN permit tcp host 10.1.105.5  
host 10.1.101.1 eq 80
```

```
ASA1(config)# access-list OUTSIDE_IN permit tcp host 10.1.104.4  
host 10.1.101.1 eq 80
```

The SCEP from R5 and R4 has been allowed to inside (R1).

Step 2 ASA2 configuration.

We need to take care of ESP traffic going through ASA2 from both branches. As ESP is not Stateful we either need to allow it in the outside ACL or just enable inspection.

```
ASA2(config)# policy-map global_policy
ASA2(config-pmap)# class inspection_default
ASA2(config-pmap-c)# inspect ipsec-pass-thru
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
```

Step 3 R5 configuration.

```
R5(config)#ip domain-name MicronicsTraining.com
R5(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R5.MicronicsTraining.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R5(config)#crypto ca trustpoint IOS_CA
R5(ca-trustpoint)#usage ike
R5(ca-trustpoint)#subject-name CN=R5, C=US
R5(ca-trustpoint)#enrollment url http://10.1.101.1
R5(ca-trustpoint)#fqdn R5.MicronicsTraining.com
R5(ca-trustpoint)#exit

R5(config)#crypto ca authenticate IOS_CA
Certificate has the following attributes:
    Fingerprint MD5: 01973E0C A51F6B10 CB074127 C07C60BC
    Fingerprint SHA1: 24A01750 51D02F6B 9BB419DE B6F40C72
B9E43EDD

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R5(config)#crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this password to the CA Administrator in order to revoke your
certificate. For security reasons your password will not be saved
in the configuration. Please make a note of it.

Password:
Re-enter password:
```

```
% The subject name in the certificate will include: CN=R5, C=US
% The subject name in the certificate will include:
R5.MicronicsTraining.com
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOS_CA verbose' command will show
the fingerprint.
```

```
R5(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: CB51F487 829E24AB
160BA244 F0256E9B
CRYPTO_PKI: Certificate Request Fingerprint SHA1: 362D19EC
4865EC2E 06915FC0 A45A9551 3B7F4A58
R5(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority
```

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)#encr 3des
R5(config-isakmp)#authentication rsa-sig
R5(config-isakmp)#hash md5
R5(config-isakmp)#group 2
```

```
R5(config-isakmp)#crypto ipsec transform-set TSET esp-3des esp-md5-
hmac
```

```
R5(cfg-crypto-trans)#access-list 120 permit ip host 5.5.5.5 host
1.1.1.1
```

```
R5(config)#crypto map ENCRYPT 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R5(config-crypto-map)#set peer 192.168.1.10
R5(config-crypto-map)#set transform-set TSET
R5(config-crypto-map)#set pfs group2
R5(config-crypto-map)#match address 120
```

```
R5(config-crypto-map)#int f0/0
R5(config-if)#crypto map ENCRYPT
R5(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Step 4 R4 configuration.

```
R4(config)#ip domain-name MicronicsTraining.com
R4(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R4.MicronicsTraining.com
```



```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R4(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
R4(config)#crypto ca trustpoint IOS_CA
R4(ca-trustpoint)#usage ike
R4(ca-trustpoint)#subject-name CN=R4, C=CA
R4(ca-trustpoint)#enrollment url http://10.1.101.1
R4(ca-trustpoint)#fqdn R4.MicronicsTraining.com
R4(ca-trustpoint)#exit
```

```
R4(config)#crypto ca authenticate IOS_CA
Certificate has the following attributes:
    Fingerprint MD5: 01973E0C A51F6B10 CB074127 C07C60BC
    Fingerprint SHA1: 24A01750 51D02F6B 9BB419DE B6F40C72
B9E43EDD
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

```
R4(config)#crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this password to the CA Administrator in order to revoke your
certificate. For security reasons your password will not be saved
in the configuration. Please make a note of it.
```

```
Password:
Re-enter password:
```

```
% The subject name in the certificate will include: CN=R4, C=CA
% The subject name in the certificate will include:
R4.MicronicsTraining.com
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOS_CA verbose' command will show
the fingerprint.
```

```
R4(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: C37B49A5 39B60647
3928452D CB501CFF
```

```
CRYPTO_PKI:      Certificate Request Fingerprint SHA1:  7E096059
984DF493 DC68F185 4325FDDF 5C9D9F7C
R4(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority

R4(config)#crypto isakmp policy 10
R4(config-isakmp)#encr des
R4(config-isakmp)#ha sha
R4(config-isakmp)#authentication rsa-sig
R4(config-isakmp)#group 2

R4(config-isakmp)#crypto ipsec transform-set TSET esp-des esp-sha-
hmac

R4(cfg-crypto-trans)#access-list 120 permit ip host 4.4.4.4 host
1.1.1.1

R4(config)#crypto map ENCRYPT 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R4(config-crypto-map)#set peer 192.168.1.10
R4(config-crypto-map)#set transform-set TSET
R4(config-crypto-map)#set pfs group2
R4(config-crypto-map)#match address 120

R4(config-crypto-map)#int f0/0
R4(config-if)# crypto map ENCRYPT
R4(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Verification

R4#ping 1.1.1.1 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

R4#sh crypto isakmp sa

```
IPv4 Crypto ISAKMP SA

dst          src          state          conn-id status
192.168.1.10 10.1.104.4    QM_IDLE       1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

R4#sh crypto ipsec sa

```
interface: FastEthernet0/0
  Crypto map tag: ENCRYPT, local addr 10.1.104.4

protected vrf: (none)
local  ident (addr/mask/prot/port): (4.4.4.4/255.255.255.0/0)
remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.0/0)
current_peer 192.168.1.10 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 192.168.1.10
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xF2B4FC1B(4071947291)
PFS (Y/N): Y, DH group: group2

inbound esp sas:
  spi: 0xE63FC84A(3862939722)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4405037/3512)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xF2B4FC1B(4071947291)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4405037/3512)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R4#sh crypto session

Crypto session current status

Interface: FastEthernet0/0

Session status: UP-ACTIVE

Peer: 192.168.1.10 port 500

IKE SA: local 10.1.104.4/500 remote 192.168.1.10/500 Active

IPSEC FLOW: permit ip host 4.4.4.4 host 1.1.1.1

Active SAs: 2, origin: crypto map

R5#ping 1.1.1.1 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 5.5.5.5

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

R5#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
192.168.1.10	10.1.105.5	QM_IDLE	1002	ACTIVE

IPv6 Crypto ISAKMP SA

R5#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: ENCRYPT, local addr 10.1.105.5

protected vrf: (none)

local ident (addr/mask/prot/port): (5.5.5.5/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x89B0F77C(2310076284)

PFS (Y/N): Y, DH group: group2

inbound esp sas:

spi: 0xB4192B2C(3021548332)

```

transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4407895/3499)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```

spi: 0x89B0F77C(2310076284)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4407895/3499)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

outbound ah sas:

outbound pcg sas:

R5#sh crypto session

Crypto session current status

Interface: FastEthernet0/0

Session status: UP-ACTIVE

Peer: 192.168.1.10 port 500

IKE SA: local 10.1.105.5/500 remote 192.168.1.10/500 Active

IPSEC FLOW: permit ip host 5.5.5.5 host 1.1.1.1

Active SAs: 2, origin: crypto map

ASA1(config)# un all

ASA1(config)# sh crypto isakmp sa

Active SA: 2

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 2

1 IKE Peer: 10.1.105.5

Type : L2L Role : responder

Rekey : no State : MM_ACTIVE

2 IKE Peer: 10.1.104.4

Type : L2L Role : responder

Rekey : no State : MM_ACTIVE

ASA1(config)# sh crypto ipsec sa

```
interface: Outside
  Crypto map tag: ENCRYPT_OUT, seq num: 2, local addr: 192.168.1.10

  access-list ACL_CA permit ip host 1.1.1.1 host 4.4.4.4
  local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)
  current_peer: 10.1.104.4

  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.104.4

  path mtu 1500, ipsec overhead 58, media mtu 1500
  current outbound spi: E63FC84A

inbound esp sas:
  spi: 0xF2B4FC1B (4071947291)
    transform: esp-des esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, PFS Group 2, }
    slot: 0, conn_id: 24576, crypto-map: ENCRYPT_OUT
    sa timing: remaining key lifetime (kB/sec): (4373999/3556)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x0000001F

outbound esp sas:
  spi: 0xE63FC84A (3862939722)
    transform: esp-des esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, PFS Group 2, }
    slot: 0, conn_id: 24576, crypto-map: ENCRYPT_OUT
    sa timing: remaining key lifetime (kB/sec): (4373999/3556)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001

Crypto map tag: ENCRYPT_OUT, seq num: 1, local addr: 192.168.1.10

  access-list ACL_US permit ip host 1.1.1.1 host 5.5.5.5
  local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (5.5.5.5/255.255.255.255/0/0)
  current_peer: 10.1.105.5

  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

```
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.105.5
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: B4192B2C
```

inbound esp sas:

```
spi: 0x89B0F77C (2310076284)
  transform: esp-3des esp-md5-hmac no compression
  in use settings = {L2L, Tunnel, PFS Group 2, }
  slot: 0, conn_id: 20480, crypto-map: ENCRYPT_OUT
  sa timing: remaining key lifetime (kB/sec): (4373999/3469)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x0000001F
```

outbound esp sas:

```
spi: 0xB4192B2C (3021548332)
  transform: esp-3des esp-md5-hmac no compression
  in use settings = {L2L, Tunnel, PFS Group 2, }
  slot: 0, conn_id: 20480, crypto-map: ENCRYPT_OUT
  sa timing: remaining key lifetime (kB/sec): (4373999/3468)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

ASA1(config)# sh vpn-sessiondb

Active Session Summary

Sessions:

	Active	Cumulative	Peak Concurrent	Inactive
SSL VPN	0	0	0	0
Clientless only	0	0	0	0
With client	0	0	0	0
Email Proxy	0	0	0	0
IPsec LAN-to-LAN	2	6	2	2
IPsec Remote Access	0	0	0	0
VPN Load Balancing	0	0	0	0
Totals	2	6		

License Information:

IPsec	: 250	Configured : 250	Active : 2	Load : 1%
SSL VPN	: 2	Configured : 2	Active : 0	Load : 0%

	Active	Cumulative	Peak Concurrent
IPsec	2	6	2
SSL VPN	0	0	0
AnyConnect Mobile	0	0	0
Linksys Phone	0	0	0
Totals	2	6	

Tunnels:

	Active	Cumulative	Peak Concurrent
IKE	2	6	2
IPsec	2	6	2
Totals	4	12	

Active NAC Sessions:

No NAC sessions to display

Active VLAN Mapping Sessions:

No VLAN Mapping sessions to display

ASA1(config)# sh vpn-sessiondb 121

Session Type: LAN-to-LAN

```

Connection   : 10.1.105.5
Index        : 5                      IP Addr      : 5.5.5.5
Protocol     : IKE IPsec
Encryption   : 3DES                   Hashing      : MD5
Bytes Tx     : 400                     Bytes Rx     : 400
Login Time   : 11:18:19 UTC Sun Jul 18 2010
Duration     : 0h:02m:27s
Connection   : 10.1.104.4
Index        : 6                      IP Addr      : 4.4.4.4
Protocol     : IKE IPsec
Encryption   : DES                    Hashing      : SHA1
Bytes Tx     : 400                     Bytes Rx     : 400
Login Time   : 11:19:43 UTC Sun Jul 18 2010
Duration     : 0h:01m:03s
ASA1(config)#

```

Verification (detailed)**ASA1(config)# deb cry isak 9**

```

ASA1(config)# Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 164
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing SA payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Oakley proposal is acceptable
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Received NAT-Traversal RFC VID
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload

```



```
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Received NAT-Traversal ver 03 VID
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Received NAT-Traversal ver 02 VID
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing IKE SA payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, IKE SA Proposal # 1, Transform # 1
acceptable Matches global IKE entry # 3
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing ISAKMP SA payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing NAT-Traversal VID ver 02
payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing Fragmentation VID +
extended capabilities payload
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 128
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 300
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing ke payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing ISA_KEY payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing nonce payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing cert request payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Received DPD VID
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Processing IOS/PIX Vendor ID payload
(version: 1.0.0, capabilities: 00000f6f)
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Received xauth V6 VID
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing NAT-Discovery payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, computing NAT Discovery hash
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing NAT-Discovery payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, computing NAT Discovery hash
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing ke payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing nonce payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing certreq payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing Cisco Unity VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing xauth V6 VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Send IOS VID
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Constructing ASA spoofing IOS Vendor ID
payload (version: 1.0.0, capabilities: 20000001)
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing VID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Send Altiga/Cisco VPN3000/Cisco ASA GW
VID
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing NAT-Discovery payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, computing NAT Discovery hash
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, constructing NAT-Discovery payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, computing NAT Discovery hash
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Generating keys for Responder...
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 320
```

```
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + ID (5) + CERT (6) + SIG (9) + NOTIFY (11) + NONE (0) total length :
766
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing ID payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing cert payload
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing RSA signature
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Computing hash for ISAKMP
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, processing notify payload
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, Automatic NAT Detection Status:      Remote
end is NOT behind a NAT device      This end is NOT behind a NAT device
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, Trying to find group via OU...
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, No Group found by matching OU(s) from ID
payload:      Unknown
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, Trying to find group via IKE ID...
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, Trying to find group via IP ADDR...
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, Connection landed on tunnel_group 10.1.105.5
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, peer ID type 2
received (FQDN)
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Peer ID check
bypassed
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing ID
payload
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing cert
payload
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing RSA
signature
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Computing hash for
ISAKMP
Jul 18 11:18:19 [IKEv1 DEBUG]: IP = 10.1.105.5, Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing dpd
vid payload
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + CERT (6) + SIG (9) + IOS KEEPALIVE (128) + VENDOR (13) + NONE
(0) total length : 818
Jul 18 11:18:19 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, PHASE 1 COMPLETED
Jul 18 11:18:19 [IKEv1]: IP = 10.1.105.5, Keep-alive type for this connection: DPD
Jul 18 11:18:19 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Starting P1 rekey
timer: 64800 seconds.
Jul 18 11:18:20 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=64bdc5ed)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE
(0) total length : 292
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing hash
payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing SA
payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing nonce
payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing ke
payload
```

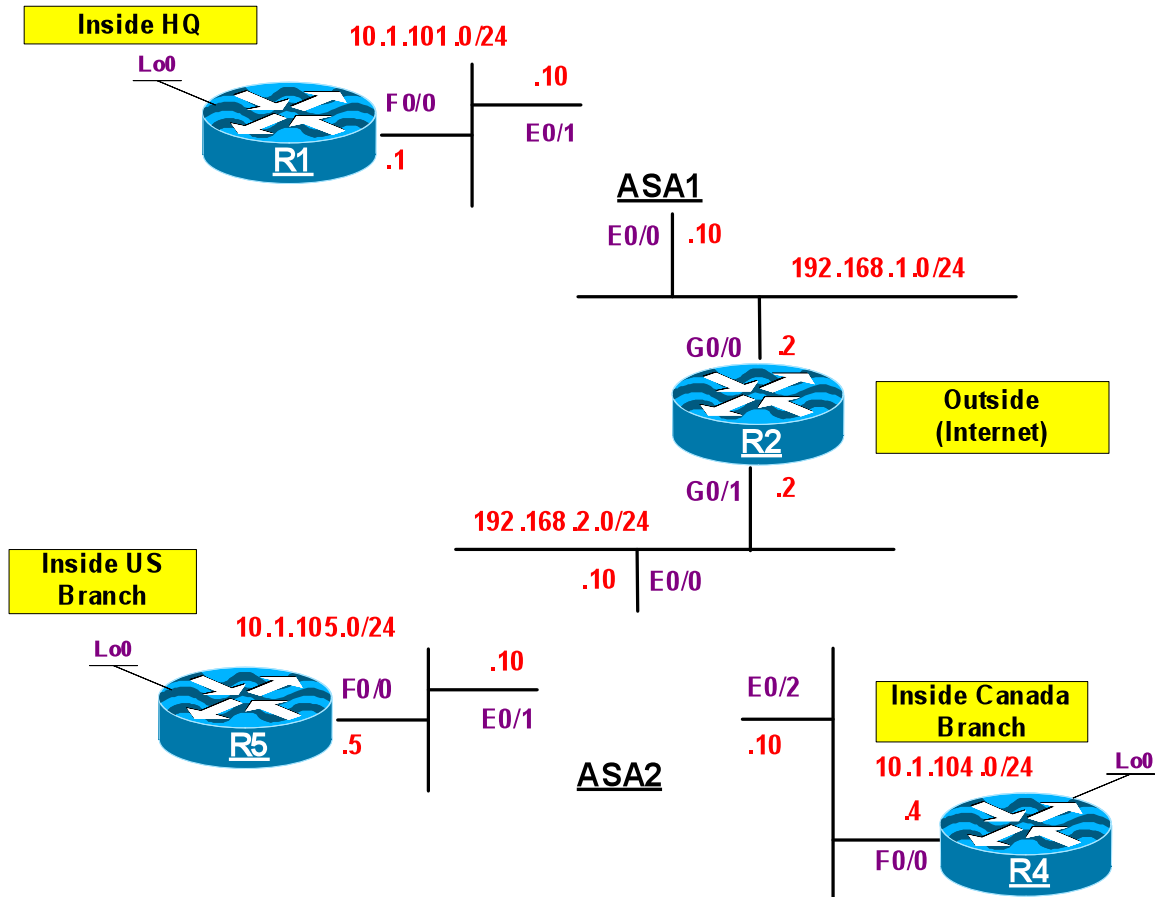
```
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing ISA_KE
for PFS in phase 2
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing ID
payload
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, Received remote Proxy
Host data in ID Payload: Address 5.5.5.5, Protocol 0, Port 0
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing ID
payload
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, Received local Proxy Host
data in ID Payload: Address 1.1.1.1, Protocol 0, Port 0
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, QM IsRekeyed old sa not
found by addr
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, Static Crypto Map check,
checking map = ENCRYPT_OUT, seq = 1...
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, Static Crypto Map check,
map ENCRYPT_OUT, seq = 1 is a successful match
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, IKE Remote Peer
configured for crypto map: ENCRYPT_OUT
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing IPsec SA
payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, IPsec SA Proposal #
1, Transform # 1 acceptable Matches global IPsec SA entry # 1
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, IKE: requesting SPI!
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, IKE got SPI from
key engine: SPI = 0x89b0f77c
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, oakley constructing
quick mode
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing blank
hash payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing IPsec
SA payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing IPsec
nonce payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing pfs ke
payload
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing proxy
ID
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Transmitting Proxy
Id:
    Remote host: 5.5.5.5 Protocol 0 Port 0
    Local host: 1.1.1.1 Protocol 0 Port 0
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing qm
hash payload
Jul 18 11:18:20 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=64bdc5ed)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE
(0) total length : 292
Jul 18 11:18:20 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=64bdc5ed)
with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing hash
payload
```

```
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, loading all IPSEC
SAs
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Generating Quick
Mode Key!
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, NP encrypt rule
look up for crypto map ENCRYPT_OUT 1 matching ACL ACL_US: returned cs_id=d7cb38c0;
rule=d7c9fc68
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Generating Quick
Mode Key!
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, NP encrypt rule
look up for crypto map ENCRYPT_OUT 1 matching ACL ACL_US: returned cs_id=d7cb38c0;
rule=d7c9fc68
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, Security negotiation
complete for LAN-to-LAN Group (10.1.105.5) Responder, Inbound SPI = 0x89b0f77c,
Outbound SPI = 0xb4192b2c
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, IKE got a KEY_ADD
msg for SA: SPI = 0xb4192b2c
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Pitcher: received
KEY_UPDATE, spi 0x89b0f77c
Jul 18 11:18:20 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Starting P2 rekey
timer: 3420 seconds.
Jul 18 11:18:20 [IKEv1]: Group = 10.1.105.5, IP = 10.1.105.5, PHASE 2 COMPLETED
(msgid=64bdc5ed)
Jul 18 11:18:38 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Sending keep-alive
of type DPD R-U-THERE (seq number 0x22ad78e5)
Jul 18 11:18:38 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing blank
hash payload
Jul 18 11:18:38 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing qm
hash payload
Jul 18 11:18:38 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=81cb2dd5)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Jul 18 11:18:38 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=6e139995)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Jul 18 11:18:38 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing hash
payload
Jul 18 11:18:38 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing notify
payload
Jul 18 11:18:38 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Received keep-alive
of type DPD R-U-THERE-ACK (seq number 0x22ad78e5)
Jul 18 11:18:48 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Sending keep-alive
of type DPD R-U-THERE (seq number 0x22ad78e6)
Jul 18 11:18:48 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing blank
hash payload
Jul 18 11:18:48 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing qm
hash payload
Jul 18 11:18:48 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=530ce865)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Jul 18 11:18:48 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=11faf851)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Jul 18 11:18:48 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing hash
payload
```

```
Jul 18 11:18:48 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing notify
payload
Jul 18 11:18:48 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Received keep-alive
of type DPD R-U-THERE-ACK (seq number 0x22ad78e6)
Jul 18 11:18:58 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Sending keep-alive
of type DPD R-U-THERE (seq number 0x22ad78e7)
Jul 18 11:18:58 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing blank
hash payload
Jul 18 11:18:58 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, constructing qm
hash payload
Jul 18 11:18:58 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=dlcf7f74)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Jul 18 11:18:58 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=fcf96857)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Jul 18 11:18:58 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing hash
payload
Jul 18 11:18:58 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, processing notify
payload
Jul 18 11:18:58 [IKEv1 DEBUG]: Group = 10.1.105.5, IP = 10.1.105.5, Received keep-alive
of type DPD R-U-THERE-ACK (seq number 0x22ad78e7)

ASA1(config)# un all
```

Lab 1.43. Site-to-Site IPsec VPN using PKI (Dynamic IP IOS-ASA)



This lab is based on previous lab configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"

- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

There is Company's Headquarters in US consists of ASA1 and R1. The Company has two branch offices: one in US (R5) and other in Canada (R4). To cut leased lines cost you decided to migrate from static IP routers at branches to dynamic IP DSLs. The IP address of DSL modems in branches is changing every day.

Configure the following Site-to-Site IPSec Tunnels:

Tunnel	SRC	DST	ISAKMP Policy	IPSec Policy
Endpoint	Network	Network		
R5 – ASA1	5.5.5.5	1.1.1.1	Authentication: RSA Encryption: 3DES Group: 2	Encryption: ESP/3DES Authentication:

			Hash: MD5	ESP/MD5
R4 – ASA1	4.4.4.4	1.1.1.1	Authentication: RSA Encryption: DES Group: 2 Hash: SHA	Encryption: ESP/DES Authentication: ESP/SHA

Use IOS CA server configured on R1 for certificate enrollment. Configure domain name of MicronicsTraining.com and ensure that FQDN and Country are included in the certificate request. Enable Perfect Forward Secrecy feature. You should assign proper IPSec Profile for every branch peer using Country field in the peer's Certificate.

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```
ASA1(config)# domain-name MicronicsTraining.com
ASA1(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-
Key>.

Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
ASA1(config)# crypto ca trustpoint IOS_CA
ASA1(config-ca-trustpoint)# id-usage ssl-ipsec
ASA1(config-ca-trustpoint)# subject-name CN=ASA1, C=US
ASA1(config-ca-trustpoint)# fqdn ASA1.MicronicsTraining.com
ASA1(config-ca-trustpoint)# enrollment url http://10.1.101.1
ASA1(config-ca-trustpoint)# exit
ASA1(config)# crypto ca authenticate IOS_CA

INFO: Certificate has the following attributes:
Fingerprint:      2ccfec44 8b1fa216 4b9ca190 024184a0
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
ASA1(config)# crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
      password to the CA Administrator in order to revoke your
certificate.
```


For security reasons your password will not be saved in the configuration.

Please make a note of it.

Password: *****

Re-enter password: *****

% The subject name in the certificate will be: CN=ASA1, C=US

% The fully-qualified domain name in the certificate will be:
ASA1.MicronicsTraining.com

% Include the device serial number in the subject name? [yes/no]:
no

Request certificate from CA? [yes/no]: **yes**

% Certificate request sent to Certificate Authority

ASA1(config)# The certificate has been granted by CA!

ASA1(config)# crypto isakmp enable outside

ASA1(config)# crypto isakmp policy 10

ASA1(config-isakmp-policy)# auth rsa-sig

ASA1(config-isakmp-policy)# enc 3des

ASA1(config-isakmp-policy)# has md5

ASA1(config-isakmp-policy)# gr 2

ASA1(config-isakmp-policy)# crypto isakmp policy 20

ASA1(config-isakmp-policy)# auth rsa-sig

ASA1(config-isakmp-policy)# enc des

ASA1(config-isakmp-policy)# ha sha

ASA1(config-isakmp-policy)# gr 2

ASA1(config-isakmp-policy)# exit

ASA1(config)# tunnel-group US_VPN type ipsec-l2l

WARNING: L2L tunnel-groups that have names which are not an IP address may only be used if the tunnel authentication method is Digital Certificates and/or The peer is configured to use Aggressive Mode

ASA1(config)# tunnel-group US_VPN ipsec-attr

ASA1(config-tunnel-ipsec)# peer-id-validate nocheck

ASA1(config-tunnel-ipsec)# trust-point IOS_CA

ASA1(config-tunnel-ipsec)# exit

ASA1(config)# tunnel-group CA_VPN type ipsec-l2l

WARNING: L2L tunnel-groups that have names which are not an IP address may only be used if the tunnel authentication method is Digital Certificates and/or The peer is configured to use Aggressive Mode

ASA1(config)# tunnel-group CA_VPN ipsec-attr

ASA1(config-tunnel-ipsec)# peer-id-validate nocheck

ASA1(config-tunnel-ipsec)# trust-point IOS_CA

ASA1(config-tunnel-ipsec)# exit

We use named tunnel group (instead of IP address). This is because our branch routers have dynamic IP addresses and we cannot rely on them. Hence, we use certificates for authentication. By default, the ASA uses OU field from the certificate to match (pick) the correct tunnel group, however, we use certificate maps later in the configuration to achieve the same.

```
ASA1(config)# crypto ipsec transform-set TSET_US esp-3des esp-md5-hmac
ASA1(config)# crypto ipsec transform-set TSET_CA esp-des esp-sha-hmac

ASA1(config)# access-list ACL_US permit ip ho 1.1.1.1 ho 5.5.5.5
ASA1(config)# access-list ACL_CA permit ip ho 1.1.1.1 ho 4.4.4.4

ASA1(config)# crypto dynamic-map US_VPN 1 match address ACL_US
ASA1(config)# crypto dynamic-map US_VPN 1 set transform TSET_US
ASA1(config)# crypto dynamic-map US_VPN 1 set pfs group2

ASA1(config)# crypto dynamic-map CA_VPN 2 match address ACL_CA
ASA1(config)# crypto dynamic-map CA_VPN 2 set transform TSET_CA
ASA1(config)# crypto dynamic-map CA_VPN 2 set pfs group2
```

This configuration is based on dynamic crypto maps which are used when peer IP address is unknown or other IPSec parameters are intended to be negotiated (i.e. EasyVPN).

```
ASA1(config)# crypto map CRYPTO_OUT 1 ipsec-isakmp dynamic US_VPN
ASA1(config)# crypto map CRYPTO_OUT 2 ipsec-isakmp dynamic CA_VPN

ASA1(config)# crypto map CRYPTO_OUT interface Outside
```

The crypto map has been attached to the outside interface. Note that the peer IP address has not been specified in the crypto map.

```
ASA1(config)# tunnel-group-map enable rules

ASA1(config)# crypto ca certificate map CERT_MAP 10
ASA1(config-ca-cert-map)# subject-name attr C eq US
ASA1(config-ca-cert-map)# crypto ca certificate map CERT_MAP 20
ASA1(config-ca-cert-map)# subject-name attr C eq CA
ASA1(config-ca-cert-map)# exit

ASA1(config)# tunnel-group-map CERT_MAP 10 US_VPN
ASA1(config)# tunnel-group-map CERT_MAP 20 CA_VPN
```

The tunnel-group-maps have tied respective crypto maps and certificate maps that allow to fulfilling the task

requirements (Country field in the certificate must be present and set).

```
ASA1(config)# route Inside 1.1.1.1 255.255.255.255 10.1.101.1
```

```
ASA1(config)# access-list OUTSIDE_IN permit tcp host 10.1.105.5  
host 10.1.101.1 eq 80
```

```
ASA1(config)# access-list OUTSIDE_IN permit tcp host 10.1.104.4  
host 10.1.101.1 eq 80
```

Step 2 ASA2 configuration.

```
ASA2(config)# policy-map global_policy  
ASA2(config-pmap)# class inspection_default  
ASA2(config-pmap-c)# inspect ipsec-pass-thru  
ASA2(config-pmap-c)# exit  
ASA2(config-pmap)# exit
```

Step 3 R5 configuration.

```
R5(config)#ip domain-name MicronicsTraining.com  
R5(config)#crypto key generate rsa modulus 1024  
The name for the keys will be: R5.MicronicsTraining.com
```

```
% The key modulus size is 1024 bits  
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R5(config)#crypto ca trustpoint IOS_CA  
R5(ca-trustpoint)#usage ike  
R5(ca-trustpoint)#subject-name CN=R5, C=US  
R5(ca-trustpoint)#enrollment url http://10.1.101.1  
R5(ca-trustpoint)#fqdn R5.MicronicsTraining.com  
R5(ca-trustpoint)#exit
```

```
R5(config)#crypto ca authenticate IOS_CA  
Certificate has the following attributes:  
    Fingerprint MD5: 01973E0C A51F6B10 CB074127 C07C60BC  
    Fingerprint SHA1: 24A01750 51D02F6B 9BB419DE B6F40C72  
B9E43EDD
```

```
% Do you accept this certificate? [yes/no]: yes  
Trustpoint CA certificate accepted.
```

```
R5(config)#crypto ca enroll IOS_CA  
%  
% Start certificate enrollment ..  
% Create a challenge password. You will need to verbally provide  
this  
    password to the CA Administrator in order to revoke your  
certificate.
```

For security reasons your password will not be saved in the configuration.

Please make a note of it.

Password:

Re-enter password:

```
% The subject name in the certificate will include: CN=R5, C=US
% The subject name in the certificate will include:
R5.MicronicsTraining.com
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOS_CA verbose' command will show
the fingerprint.
```

```
R5(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: CB51F487 829E24AB
160BA244 F0256E9B
CRYPTO_PKI: Certificate Request Fingerprint SHA1: 362D19EC
4865EC2E 06915FC0 A45A9551 3B7F4A58
R5(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority
```

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)#encr 3des
R5(config-isakmp)#authentication rsa-sig
R5(config-isakmp)#hash md5
R5(config-isakmp)#group 2
```

```
R5(config-isakmp)#crypto ipsec transform-set TSET esp-3des esp-md5-
hmac
```

```
R5(cfg-crypto-trans)#access-list 120 permit ip host 5.5.5.5 host
1.1.1.1
```

```
R5(config)#crypto map ENCRYPT 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R5(config-crypto-map)#set peer 192.168.1.10
R5(config-crypto-map)#set transform-set TSET
R5(config-crypto-map)#set pfs group2
R5(config-crypto-map)#match address 120
```

```
R5(config-crypto-map)#int f0/0
R5(config-if)#crypto map ENCRYPT
R5(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Step 4 R4 configuration.

```
R4(config)#ip domain-name MicronicsTraining.com
R4(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R4.MicronicsTraining.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R4(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled


R4(config)#crypto ca trustpoint IOS_CA
R4(ca-trustpoint)#usage ike
R4(ca-trustpoint)#subject-name CN=R4, C=CA
R4(ca-trustpoint)#enrollment url http://10.1.101.1
R4(ca-trustpoint)#fqdn R4.MicronicsTraining.com
R4(ca-trustpoint)#exit


R4(config)#crypto ca authenticate IOS_CA
Certificate has the following attributes:
    Fingerprint MD5: 01973E0C A51F6B10 CB074127 C07C60BC
    Fingerprint SHA1: 24A01750 51D02F6B 9BB419DE B6F40C72
B9E43EDD

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.


R4(config)#crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: CN=R4, C=CA
% The subject name in the certificate will include:
R4.MicronicsTraining.com
% Include the router serial number in the subject name? [yes/no]:
```

```
no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOS_CA verbose' command will show
the fingerprint.

R4(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: C37B49A5 39B60647
3928452D CB501CFF
CRYPTO_PKI: Certificate Request Fingerprint SHA1: 7E096059
984DF493 DC68F185 4325FDDF 5C9D9F7C
R4(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority


R4(config)#crypto isakmp policy 10
R4(config-isakmp)#encr des
R4(config-isakmp)#ha sha
R4(config-isakmp)#authentication rsa-sig
R4(config-isakmp)#group 2


R4(config-isakmp)#crypto ipsec transform-set TSET esp-des esp-sha-
hmac


R4(cfg-crypto-trans)#access-list 120 permit ip host 4.4.4.4 host
1.1.1.1


R4(config)#crypto map ENCRYPT 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R4(config-crypto-map)#set peer 192.168.1.10
R4(config-crypto-map)#set transform-set TSET
R4(config-crypto-map)#set pfs group2
R4(config-crypto-map)#match address 120


R4(config-crypto-map)#int f0/0
R4(config-if)# crypto map ENCRYPT
R4(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Verification

R4#pin 1.1.1.1 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 4.4.4.4

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

R5#ping 1.1.1.1 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 5.5.5.5

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

R4#sh cry isak sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime
1001	10.1.104.4	192.168.1.10		ACTIVE	des	sha	rsig	2	23:58:20

Engine-id:Conn-id = SW:1

The peers have been authenticated by using certificates - "rsig" indicates that. "show crypto isakmp sa detail" may be used to determine which ISAKMP policy has been chosen by the peers.

IPv6 Crypto ISAKMP SA

R4#sh cry eng conn ac

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1001	IKE	SHA+DES	0	0	10.1.104.4
2001	IPsec	DES+SHA	0	4	10.1.104.4
2002	IPsec	DES+SHA	4	0	10.1.104.4

R4#sh cry sess

Crypto session current status

Interface: FastEthernet0/0

Session status: UP-ACTIVE

Peer: 192.168.1.10 port 500

IKE SA: local 10.1.104.4/500 remote 192.168.1.10/500 Active

IPSEC FLOW: permit ip host 4.4.4.4 host 1.1.1.1

Active SAs: 2, origin: crypto map

This command shows the peers, status of the tunnel and definition of interesting traffic.

R4#sh cry ips sa

```
interface: FastEthernet0/0
  Crypto map tag: ENCRYPT, local addr 10.1.104.4

protected vrf: (none)
local ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
current_peer 192.168.1.10 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 192.168.1.10
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x21D3F08A(567537802)
PFS (Y/N): Y, DH group: group2

inbound esp sas:
  spi: 0x13B6803F(330727487)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4492988/3479)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x21D3F08A(567537802)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4492988/3479)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:
```


outbound pcp sas:

R5#sh cry isak sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1005	10.1.105.5	192.168.1.10		ACTIVE	3des	md5	rsig	2	23:58:54	
Engine-id:Conn-id = SW:5										

IPv6 Crypto ISAKMP SA

R5#sh cry eng conn ac

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1005	IKE	MD5+3DES	0	0	10.1.105.5
2003	IPsec	3DES+MD5	0	4	10.1.105.5
2004	IPsec	3DES+MD5	4	0	10.1.105.5

R5#sh cry sess

Crypto session current status

Interface: FastEthernet0/0

Session status: UP-ACTIVE

Peer: 192.168.1.10 port 500

IKE SA: local 10.1.105.5/500 remote 192.168.1.10/500 Active

IPSEC FLOW: permit ip host 5.5.5.5 host 1.1.1.1

Active SAs: 2, origin: crypto map

R5#sh cry ips sa

interface: FastEthernet0/0

Crypto map tag: ENCRYPT, local addr 10.1.105.5

protected vrf: (none)

local ident (addr/mask/prot/port): (5.5.5.5/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

```

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 192.168.1.10
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xF539870C(4114188044)
PFS (Y/N): Y, DH group: group2

inbound esp sas:
spi: 0x5FF3F295(1609822869)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4446487/3522)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcsp sas:

outbound esp sas:
spi: 0xF539870C(4114188044)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4446487/3522)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcsp sas:

```

ASA1(config)# sh cry isak

```

Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1  IKE Peer: 10.1.104.4
   Type    : L2L           Role    : responder
   Rekey    : no           State    : MM_ACTIVE
2  IKE Peer: 10.1.105.5
   Type    : L2L           Role    : responder
   Rekey    : no           State    : MM_ACTIVE

```

```
Global IKE Statistics
Active Tunnels: 2
Previous Tunnels: 6
In Octets: 73056
In Packets: 501
In Drop Packets: 54
In Notifys: 376
In P2 Exchanges: 6
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 2
Out Octets: 50884
Out Packets: 472
Out Drop Packets: 0
Out Notifys: 768
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 2
Initiator Tunnels: 1
Initiator Fails: 1
Responder Fails: 21
System Capacity Fails: 0
Auth Fails: 5
Decrypt Fails: 0
Hash Valid Fails: 1
No Sa Fails: 10
```

```
Global IPSec over TCP Statistics
-----
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Received ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
```

ASA1(config)# sh cry isak sa detail

```
Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
```

Total IKE SA: 2

```

1  IKE Peer: 10.1.104.4
    Type      : L2L                Role      : responder
    Rekey      : no                 State      : MM_ACTIVE
    Encrypt    : des                Hash       : SHA
    Auth       : rsa                Lifetime: 86400
    Lifetime Remaining: 86029

2  IKE Peer: 10.1.105.5
    Type      : L2L                Role      : responder
    Rekey      : no                 State      : MM_ACTIVE
    Encrypt    : 3des               Hash       : MD5
    Auth       : rsa                Lifetime: 86400
    Lifetime Remaining: 86112

```

ASA1(config)# sh cry ips sa

```

interface: Outside
  Crypto map tag: CA_VPN, seq num: 2, local addr: 192.168.1.10

  access-list ACL_CA permit ip host 1.1.1.1 host 4.4.4.4
  local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)
  current_peer: 10.1.104.4

  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.104.4

  path mtu 1500, ipsec overhead 58, media mtu 1500
  current outbound spi: 13B6803F

inbound esp sas:
  spi: 0x21D3F08A (567537802)
    transform: esp-des esp-sha-hmac no compression
    in use settings = {L2L, Tunnel, PFS Group 2, }
    slot: 0, conn_id: 36864, crypto-map: CA_VPN
    sa timing: remaining key lifetime (kB/sec): (4373999/3219)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x0000001F
outbound esp sas:
  spi: 0x13B6803F (330727487)
    transform: esp-des esp-sha-hmac no compression

```

```
in use settings ={L2L, Tunnel, PFS Group 2, }
slot: 0, conn_id: 36864, crypto-map: CA_VPN
sa timing: remaining key lifetime (kB/sec): (4373999/3219)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

Crypto map tag: US_VPN, seq num: 1, local addr: 192.168.1.10

access-list ACL_US permit ip host 1.1.1.1 host 5.5.5.5
local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (5.5.5.5/255.255.255.255/0/0)
current_peer: 10.1.105.5

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.105.5

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 5FF3F295

inbound esp sas:
spi: 0xF539870C (4114188044)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 2, }
slot: 0, conn_id: 40960, crypto-map: US_VPN
sa timing: remaining key lifetime (kB/sec): (4373999/3300)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0x5FF3F295 (1609822869)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 2, }
slot: 0, conn_id: 40960, crypto-map: US_VPN
sa timing: remaining key lifetime (kB/sec): (4373999/3298)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA1(config)# sh vpn-sessiondb 121

Session Type: LAN-to-LAN

Connection : CA_VPN

```

Index      : 9                      IP Addr    : 4.4.4.4
Protocol    : IKE IPsec
Encryption  : DES                   Hashing     : SHA1
Bytes Tx    : 400                   Bytes Rx    : 400
Login Time  : 03:43:19 UTC Fri Jul 23 2010
Duration    : 0h:06m:34s

```

Connection : US_VPN

```

Index      : 10                     IP Addr    : 5.5.5.5
Protocol    : IKE IPsec
Encryption  : 3DES                  Hashing     : MD5
Bytes Tx    : 400                   Bytes Rx    : 400
Login Time  : 03:44:42 UTC Fri Jul 23 2010
Duration    : 0h:05m:11s

```

Verification (detailed)

```

ASA1(config)# deb cry isak 20
ASA1(config)# Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE RECEIVED Message
(msgsid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 164
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing SA payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Oakley proposal is acceptable
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Received NAT-Traversal RFC VID
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Received NAT-Traversal ver 03 VID
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Received NAT-Traversal ver 02 VID
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing IKE SA payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, IKE SA Proposal # 1, Transform # 1
acceptable Matches global IKE entry # 5
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing ISAKMP SA payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing NAT-Traversal VID ver 02
payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing Fragmentation VID +
extended capabilities payload
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 128
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 308
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing ke payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing ISA_KE payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing nonce payload

```

```

Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing cert request payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Received DPD VID
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Processing IOS/PIX Vendor ID payload
(version: 1.0.0, capabilities: 00000f6f)
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Received xauth V6 VID
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing NAT-Discovery payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, computing NAT Discovery hash
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing NAT-Discovery payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, computing NAT Discovery hash
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing ke payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing nonce payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing certreq payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing Cisco Unity VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing xauth V6 VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Send IOS VID
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Constructing ASA spoofing IOS Vendor ID
payload (version: 1.0.0, capabilities: 20000001)
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing VID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Send Altiga/Cisco VPN3000/Cisco ASA GW
VID
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing NAT-Discovery payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, computing NAT Discovery hash
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, constructing NAT-Discovery payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, computing NAT Discovery hash
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Generating keys for Responder...
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 328
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + ID (5) + CERT (6) + SIG (9) + NOTIFY (11) + NONE (0) total length :
766
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing ID payload
Jul 23 03:43:19 [IKEv1 DECODE]: IP = 10.1.104.4, ID_FQDN ID received, len 24
0000: 52342E4D 6963726F 6E696373 54726169      R4.MicronicsTrai
0010: 6E696E67 2E636F6D      ning.com

```

Note that ID_FQDN ID type has been received by the ASA. ID_FQDN is written in the certificate used for peer authentication.

```

Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing cert payload
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing RSA signature
Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Computing hash for ISAKMP
Jul 23 03:43:19 [IKEv1 DECODE]: Dump of received Signature, len 128:
0000: 31F1AF7C 7B266908 92DFF3AB C547EEAE      1..|{&i.....G..
0010: AF8853FF F4082F91 2D78869C A38BBF41      ..S.../.-x.....A
0020: 63185454 A7E6B250 00BFBF6A 36F1EACD      c.TT...P...j6...
0030: 849CA235 908F61FA EC4D8BBE 0D7ADBBA      ...5..a..M...z..
0040: 0A83E023 7E22EEB6 677034C2 D17E04ED      ...#"..gp4...~..

```

```

0050: 97621F26 13A12C1C 1497D0B9 2AE52E03      .b.&...,*...
0060: 532B7B90 4F67F6F4 3C954E8E 2D9E0B66      S+{.Og..<.N.-..f
0070: A85A1EEE 216F86A9 1CDF4EFA 81FE317C      .Z...!o....N...l|

```

```

Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, processing notify payload
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, Automatic NAT Detection Status:      Remote
end is NOT behind a NAT device      This      end is NOT behind a NAT device
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, Trying to find group via cert rules...
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, Connection landed on tunnel_group CA_VPN

```

"tunnel-group-map" has caused that the connection has been properly assigned to the configured tunnel-group. This assignment has been based on certificate-map which examines the certificate's field values.

```

Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, peer ID type 2 received
(FQDN)
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Peer ID check bypassed
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing ID payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing cert
payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing RSA
signature
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Computing hash for
ISAKMP
Jul 23 03:43:19 [IKEv1 DECODE]: Constructed Signature Len: 128
Jul 23 03:43:19 [IKEv1 DECODE]: Constructed Signature:
0000: 09458DE0 978EE65F FA3A7075 14E03532      .E....._:pu..52
0010: 73AD3FFF 2820C912 4EF30FB1 A48A91F7      s.?.( ..N.....
0020: 8D042A8B 884D571C D1FED0FB 53271E43      ..*..MW.....S'.C
0030: 29217A90 C9BDC3E3 BAE510EE 9CCEA703      )!z.....
0040: 673D0A25 DCE4A48E FF73B4A4 8C0B963F      g=.%.....s.....?
0050: 389C842A 83C2ADB4 1153CACC E3E246C8      8..*.....S....F.
0060: 7C0F8A22 F4E43654 60CDD30A D16BD027      |.."..6T`....k.'
0070: A5A94979 99F6B8FE 4920B5DA 0C95A677      ..Iy....I .....w

```

```

Jul 23 03:43:19 [IKEv1 DEBUG]: IP = 10.1.104.4, Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing dpd vid
payload
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + CERT (6) + SIG (9) + IOS KEEPALIVE (128) + VENDOR (13) + NONE
(0) total length : 818
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, PHASE 1 COMPLETED

```

Phase 1 completed - the Quick Mode has begun.

```

Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, Keep-alive type for this connection: DPD
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Starting P1 rekey
timer: 64800 seconds.

```



```
Jul 23 03:43:19 [IKEv1 DECODE]: IP = 10.1.104.4, IKE Responder starting QM: msg id =
9b5f88d8
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE RECEIVED Message (msgid=9b5f88d8)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE
(0) total length : 296
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing hash payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing SA payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing nonce
payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing ke payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing ISA_KE for
PFS in phase 2
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing ID payload
Jul 23 03:43:19 [IKEv1 DECODE]: Group = CA_VPN, IP = 10.1.104.4, ID_IPV4_ADDR ID
received
4.4.4.4
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, Received remote Proxy Host
data in ID Payload: Address 4.4.4.4, Protocol 0, Port 0
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing ID payload
Jul 23 03:43:19 [IKEv1 DECODE]: Group = CA_VPN, IP = 10.1.104.4, ID_IPV4_ADDR ID
received
1.1.1.1
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, Received local Proxy Host
data in ID Payload: Address 1.1.1.1, Protocol 0, Port 0
```

Local and remote proxies presented by the remote peer match locally configured proxies.

```
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, QM IsRekeyed old sa not found
by addr
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, Mismatch: P1 Authentication
algorithm in the crypto map entry different from negotiated algorithm for the L2L
connection
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, IKE Remote Peer configured
for crypto map: CA_VPN
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing IPsec SA
payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, IPsec SA Proposal # 1,
Transform # 1 acceptable Matches global IPsec SA entry # 2
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, IKE: requesting SPI!
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, IKE got SPI from key
engine: SPI = 0x21d3f08a
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, oakley constructing
quick mode
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing blank hash
payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing IPsec SA
payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing IPsec
nonce payload
```

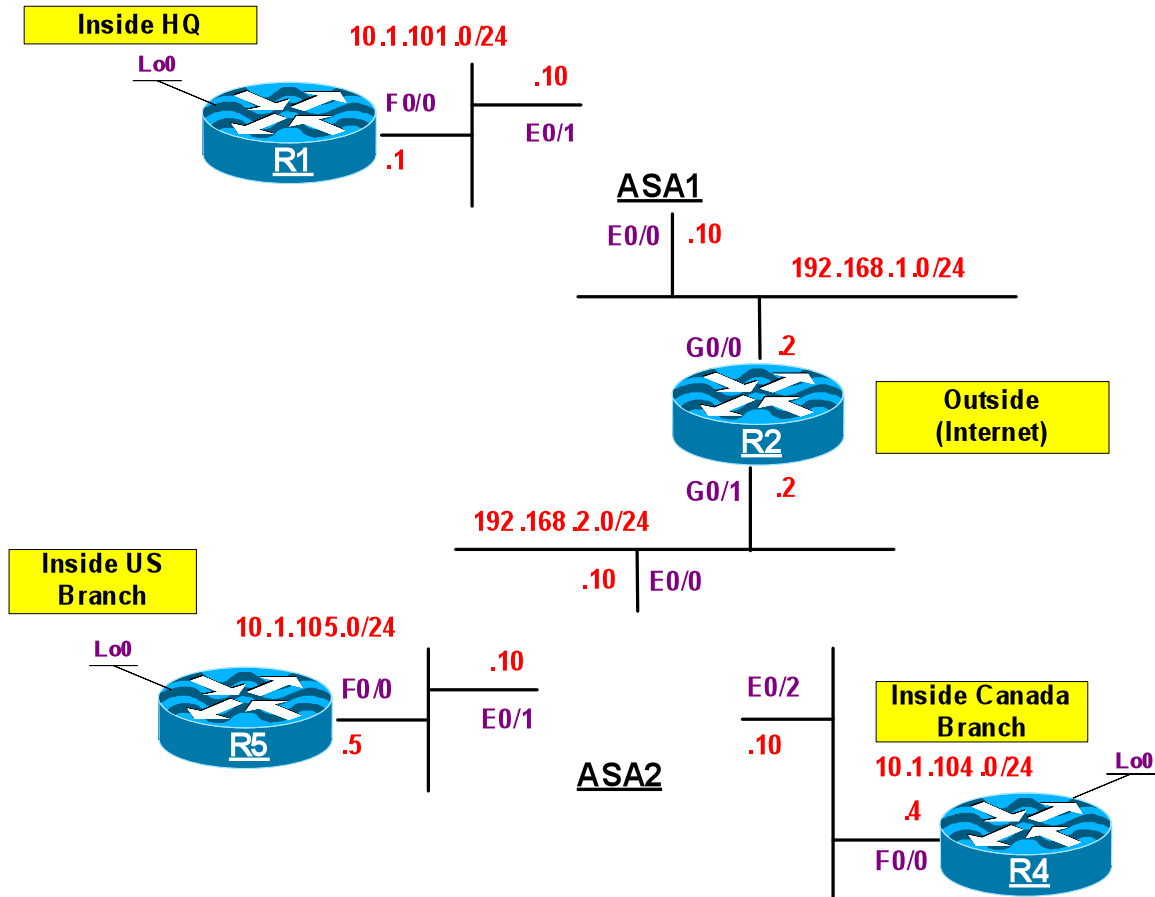
```
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing pfs ke
payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing proxy ID
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Transmitting Proxy Id:
    Remote host: 4.4.4.4  Protocol 0  Port 0
    Local host:  1.1.1.1  Protocol 0  Port 0
```

The ASA has presented its proxy to the remote peer (R4).

```
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, constructing qm hash
payload
Jul 23 03:43:19 [IKEv1 DECODE]: Group = CA_VPN, IP = 10.1.104.4, IKE Responder sending
2nd QM pkt: msg id = 9b5f88d8
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE SENDING Message (msgid=9b5f88d8)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE
(0) total length : 296
Jul 23 03:43:19 [IKEv1]: IP = 10.1.104.4, IKE_DECODE RECEIVED Message (msgid=9b5f88d8)
with payloads : HDR + HASH (8) + NONE (0) total length : 52
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, processing hash payload
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, loading all IPSEC SAs
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Generating Quick Mode
Key!
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, NP encrypt rule look up
for crypto map CA_VPN 2 matching ACL ACL_CA: returned cs_id=d7beba18; rule=d7bef8f8
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Generating Quick Mode
Key!
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, NP encrypt rule look up
for crypto map CA_VPN 2 matching ACL ACL_CA: returned cs_id=d7beba18; rule=d7bef8f8
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, Security negotiation complete
for LAN-to-LAN Group (CA_VPN) Responder, Inbound SPI = 0x21d3f08a, Outbound SPI =
0x13b6803f
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, IKE got a KEY_ADD msg
for SA: SPI = 0x13b6803f
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Pitcher: received
KEY_UPDATE, spi 0x21d3f08a
Jul 23 03:43:19 [IKEv1 DEBUG]: Group = CA_VPN, IP = 10.1.104.4, Starting P2 rekey
timer: 3420 seconds.
Jul 23 03:43:19 [IKEv1]: Group = CA_VPN, IP = 10.1.104.4, PHASE 2 COMPLETED
(msgid=9b5f88d8)
```

```
ASA1(config)# un all
```

Lab 1.44. Site-to-Site IPSec VPN using PSK (IOS-ASA Hairpinning)



This lab is based on previous lab configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"

- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

There is Company's Headquarters in US consists of ASA1 and R1. The Company has two branch offices: one in US (R5) and other in Canada (R4). All routers have static IP addresses. Configure the following Site-to-Site IPSec Tunnels:

Tunnel Endpoint	SRC Network	DST Network	ISAKMP Policy	IPSec Policy
R5 – ASA1	5.5.5.5	1.1.1.1	Authentication: PSK Encryption: 3DES Group: 2 Hash: MD5 Key: R5-ASA	Encryption: ESP/3DES Authentication: ESP/MD5

R4 – ASA1	4.4.4.4	1.1.1.1	Authentication: PSK Encryption: DES Group: 2 Hash: SHA Key: R4-ASA	Encryption: ESP/DES Authentication: ESP/SHA

Configure the above IPSec tunnels and ensure branch networks can communicate between each other using Headquarters' hub device.

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```
ASA1(config)# crypto isakmp enable outside

ASA1(config)# crypto isakmp policy 5
ASA1(config-isakmp-policy)# authentication pre-share
ASA1(config-isakmp-policy)# encryption 3des
ASA1(config-isakmp-policy)# hash md5
ASA1(config-isakmp-policy)# group 2

ASA1(config-isakmp-policy)# crypto isakmp policy 10
ASA1(config-isakmp-policy)# authentication pre-share
ASA1(config-isakmp-policy)# encryption des
ASA1(config-isakmp-policy)# hash sha
ASA1(config-isakmp-policy)# group 2
ASA1(config-isakmp-policy)# exit

ASA1(config)# tunnel-group 10.1.105.5 type ipsec-l2l
ASA1(config)# tunnel-group 10.1.105.5 ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key R5-ASA
ASA1(config-tunnel-ipsec)# exit

ASA1(config)# tunnel-group 10.1.104.4 type ipsec-l2l
ASA1(config)# tunnel-group 10.1.104.4 ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key R4-ASA
ASA1(config-tunnel-ipsec)# exit

ASA1(config)# access-list CRYPTO-ACL-R5 extended permit ip host
1.1.1.1 host 5.5.5.5
ASA1(config)# access-list CRYPTO-ACL-R5 extended permit ip host
4.4.4.4 host 5.5.5.5
```

```
ASA1(config)# access-list CRYPTO-ACL-R4 extended permit ip host
1.1.1.1 host 4.4.4.4
ASA1(config)# access-list CRYPTO-ACL-R4 extended permit ip host
5.5.5.5 host 4.4.4.4
```

Additional ACEs allow to communicate IPSec-protected IP addresses of R4 and R5 throughout "hairpinned" tunnels on ASA's outside interface.

```
ASA1(config)# crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-
md5-hmac
```

```
ASA1(config)# crypto ipsec transform-set ESP-DES-SHA esp-des esp-
sha-hmac
```

```
ASA1(config)# crypto map ENCRYPT_OUT 1 match address CRYPTO-ACL-R5
ASA1(config)# crypto map ENCRYPT_OUT 1 set peer 10.1.105.5
ASA1(config)# crypto map ENCRYPT_OUT 1 set transform-set ESP-3DES-
MD5
```

```
ASA1(config)# crypto map ENCRYPT_OUT 2 match address CRYPTO-ACL-R4
ASA1(config)# crypto map ENCRYPT_OUT 2 set peer 10.1.104.4
ASA1(config)# crypto map ENCRYPT_OUT 2 set transform-set ESP-DES-
SHA
```

```
ASA1(config)# crypto map ENCRYPT_OUT interface Outside
```

```
ASA1(config)# route Inside 1.1.1.1 255.255.255.255 10.1.101.1 1
```

```
ASA1(config)# same-security-traffic permit intra-interface
```

The capability to route a traffic in and out of the same interface has been enabled

Step 2 R5 configuration.

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)#encr 3des
R5(config-isakmp)#hash md5
R5(config-isakmp)#authentication pre-share
R5(config-isakmp)#group 2
```

```
R5(config-isakmp)#crypto isakmp key R5-ASA address 192.168.1.10
```

```
R5(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac
R5(cfg-crypto-trans)#exi
```

```
R5(config)#access-list 120 permit ip host 5.5.5.5 host 1.1.1.1
R5(config)#access-list 120 permit ip host 5.5.5.5 host 4.4.4.4
```

```

R5(config)#crypto map ENCRYPT 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R5(config-crypto-map)#set peer 192.168.1.10
R5(config-crypto-map)#set transform-set TSET
R5(config-crypto-map)#match address 120
R5(config-crypto-map)#exit

R5(config)#int f0/0
R5(config-if)#crypto map ENCRYPT
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R5(config-if)#exit

```

Step 3 R4 configuration.

```

R4(config)#crypto isakmp policy 30
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#group 2

R4(config-isakmp)#crypto isakmp key R4-ASA address 192.168.1.10

R4(config)#crypto ipsec transform-set TSET esp-des esp-sha-hmac

R4(cfg-crypto-trans)#access-list 120 permit ip host 4.4.4.4 host
1.1.1.1
R4(config)#access-list 120 permit ip host 4.4.4.4 host 5.5.5.5

R4(config)#crypto map ENCRYPT 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R4(config-crypto-map)# set peer 192.168.1.10
R4(config-crypto-map)# set transform-set TSET
R4(config-crypto-map)# match address 120
R4(config-crypto-map)#exit

R4(config)#int f0/0
R4(config-if)# crypto map ENCRYPT

```

Step 4 ASA2 configuration.

```

ASA2(config)# policy-map global_policy
ASA2(config-pmap)# class inspection_default
ASA2(config-pmap-c)# inspect ipsec-pass-thru
ASA2(config)# access-list OUTSIDE_IN permit udp host 192.168.1.10
eq 500 host 10.1.104.4 eq 500
ASA2(config)# access-list OUTSIDE_IN permit udp host 192.168.1.10
eq 500 host 10.1.105.5 eq 500
ASA2(config)# access-group OUTSIDE_IN in interface outside

```

The above ACL is created to allow IKE tunnel setup from

ASA1 to R4/R5 because there may be a case where R4 is sending something behind R5 and there is no tunnel between R5 and ASA1 already established. In that case, the ASA1 must be able to establish a tunnel to R5 to handle that traffic.

Verification

R4#pi 1.1.1.1 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 4.4.4.4

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R4#pi 5.5.5.5 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:

Packet sent with a source address of 4.4.4.4

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R4#sh cry isa sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.104.4	192.168.1.10		ACTIVE	des	sha	psk	2	23:41:30	
Engine-id:Conn-id = SW:2										

IPv6 Crypto ISAKMP SA

R4#sh cry eng conn ac

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1002	IKE	SHA+DES	0	0	10.1.104.4

2003	IPsec	DES+SHA	0	5	10.1.104.4
2004	IPsec	DES+SHA	5	0	10.1.104.4
2005	IPsec	DES+SHA	0	5	10.1.104.4
2006	IPsec	DES+SHA	19	0	10.1.104.4

Note that two IPSec SAs (inbound and outbound) have been created for every local-remote proxy pair.

R4#sh cry sess

Crypto session current status

Interface: FastEthernet0/0

Session status: UP-ACTIVE

Peer: 192.168.1.10 port 500

IKE SA: local 10.1.104.4/500 remote 192.168.1.10/500 Active

IPSEC FLOW: permit ip host 4.4.4.4 host 1.1.1.1

Active SAs: 2, origin: crypto map

IPSEC FLOW: permit ip host 4.4.4.4 host 5.5.5.5

Active SAs: 2, origin: crypto map

Two active SAs for every IPSec flow mentioned above are visible when crypto sessions have been displayed.

R4#sh cry ips sa

interface: FastEthernet0/0

Crypto map tag: ENCRYPT, local addr 10.1.104.4

protected vrf: (none)

local ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x880857A4(2282248100)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x55652A60(1432693344)

transform: esp-des esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: ENCRYPT

sa timing: remaining key lifetime (k/sec): (4607369/2454)

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```
spi: 0x880857A4(2282248100)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4607369/2454)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

One pair of SAs have been created for 4.4.4.4/32 and 1.1.1.1/32.

outbound ah sas:

outbound pcg sas:

protected vrf: (none)

```
local ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (5.5.5.5/255.255.255.255/0/0)
```

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

```
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
```

```
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xAFFA8D8D(2952433037)

PFS (Y/N): N, DH group: none

inbound esp sas:

```
spi: 0xFC97ED38(4237815096)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: NETGX:5, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4587626/2496)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xAFFA8D8D(2952433037)
  transform: esp-des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2006, flow_id: NETGX:6, sibling_flags 80000046, crypto map: ENCRYPT
  sa timing: remaining key lifetime (k/sec): (4587624/2496)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

The second pair of SAs have been created for 4.4.4.4/32 and 5.5.5.5/32.

R5#sh cry isak sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection
 K - Keepalives, N - NAT-traversal
 T - cTCP encapsulation, X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.105.5	192.168.1.10		ACTIVE	3des	md5	psk	2	23:57:07	
Engine-id:Conn-id = SW:1										

IPv6 Crypto ISAKMP SA

R5#sh cry sess

Crypto session current status

Interface: FastEthernet0/0

Session status: UP-ACTIVE

Peer: 192.168.1.10 port 500

IKE SA: local 10.1.105.5/500 remote 192.168.1.10/500 Active

IPSEC FLOW: permit ip host 5.5.5.5 host 1.1.1.1

Active SAs: 0, origin: crypto map

IPSEC FLOW: permit ip host 5.5.5.5 host 4.4.4.4

Active SAs: 2, origin: crypto map

R5#sh cry ips sa

interface: FastEthernet0/0

Crypto map tag: ENCRYPT, local addr 10.1.105.5

protected vrf: (none)

local ident (addr/mask/prot/port): (5.5.5.5/255.255.255.0/0)

remote ident (addr/mask/prot/port): (1.1.1.1/255.255.255.0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

← No traffic for that flow

yet

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x0(0)

PFS (Y/N): N, DH group: none

inbound esp sas:

inbound ah sas:

inbound pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (5.5.5.5/255.255.255.0/0)

remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x8689FE2F(2257190447)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xD396C0D5(3549872341)

```

transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4563711/3425)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```

spi: 0x8689FE2F(2257190447)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: ENCRYPT
sa timing: remaining key lifetime (k/sec): (4563711/3425)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

outbound ah sas:

outbound pcg sas:

ASA1(config)# sh cry isa sa det

```

Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1  IKE Peer: 10.1.104.4
    Type    : L2L                Role    : responder
    Rekey    : no                 State    : MM_ACTIVE
    Encrypt  : des                Hash     : SHA
    Auth     : preshared          Lifetime: 86400
    Lifetime Remaining: 85180

2  IKE Peer: 10.1.105.5
    Type    : L2L                Role    : initiator
    Rekey    : no                 State    : MM_ACTIVE
    Encrypt  : 3des              Hash     : MD5
    Auth     : preshared          Lifetime: 86400
    Lifetime Remaining: 86186

```

Note that because R4 pinged R5 the ASA1 is an Initiator for the second L2L tunnel.

ASA1(config)# sh cry ips sa

```

interface: Outside

```

Crypto map tag: ENCRYPT_OUT, seq num: 2, local addr: 192.168.1.10

access-list CRYPTO-ACL-R4 permit ip host 1.1.1.1 host 4.4.4.4

local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)

current_peer: 10.1.104.4

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0

#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.104.4

path mtu 1500, ipsec overhead 58, media mtu 1500

current outbound spi: 55652A60

inbound esp sas:

spi: 0x880857A4 (2282248100)

transform: esp-des esp-sha-hmac no compression

in use settings ={L2L, Tunnel, }

slot: 0, conn_id: 45056, crypto-map: ENCRYPT_OUT

sa timing: remaining key lifetime (kB/sec): (4373999/2373)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x0000003F

outbound esp sas:

spi: 0x55652A60 (1432693344)

transform: esp-des esp-sha-hmac no compression

in use settings ={L2L, Tunnel, }

slot: 0, conn_id: 45056, crypto-map: ENCRYPT_OUT

sa timing: remaining key lifetime (kB/sec): (4373999/2373)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

Crypto map tag: ENCRYPT_OUT, seq num: 2, local addr: 192.168.1.10

access-list CRYPTO-ACL-R4 permit ip host 5.5.5.5 host 4.4.4.4

local ident (addr/mask/prot/port): (5.5.5.5/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (4.4.4.4/255.255.255.255/0/0)

current_peer: 10.1.104.4

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

```
#pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.104.4
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: FC97ED38
```

```
inbound esp sas:
```

```
spi: 0xAFFA8D8D (2952433037)
  transform: esp-des esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 45056, crypto-map: ENCRYPT_OUT
  sa timing: remaining key lifetime (kB/sec): (4373998/2413)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x000FFFFF
```

```
outbound esp sas:
```

```
spi: 0xFC97ED38 (4237815096)
  transform: esp-des esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 45056, crypto-map: ENCRYPT_OUT
  sa timing: remaining key lifetime (kB/sec): (4373999/2411)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

```
Crypto map tag: ENCRYPT_OUT, seq num: 1, local addr: 192.168.1.10
```

```
access-list CRYPTO-ACL-R5 permit ip host 4.4.4.4 host 5.5.5.5
local ident (addr/mask/prot/port): (4.4.4.4/255.255.255.0/0)
remote ident (addr/mask/prot/port): (5.5.5.5/255.255.255.0/0)
current_peer: 10.1.105.5
```

```
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.105.5
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: D396C0D5
```

```

inbound esp sas:
  spi: 0x8689FE2F (2257190447)
    transform: esp-3des esp-md5-hmac no compression
    in use settings ={L2L, Tunnel, }
    slot: 0, conn_id: 49152, crypto-map: ENCRYPT_OUT
    sa timing: remaining key lifetime (kB/sec): (4373999/3372)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x0000003F
outbound esp sas:
  spi: 0xD396C0D5 (3549872341)
    transform: esp-3des esp-md5-hmac no compression
    in use settings ={L2L, Tunnel, }
    slot: 0, conn_id: 49152, crypto-map: ENCRYPT_OUT
    sa timing: remaining key lifetime (kB/sec): (4373999/3372)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001

```

ASA1(config)# sh vpn-sessiondb 121

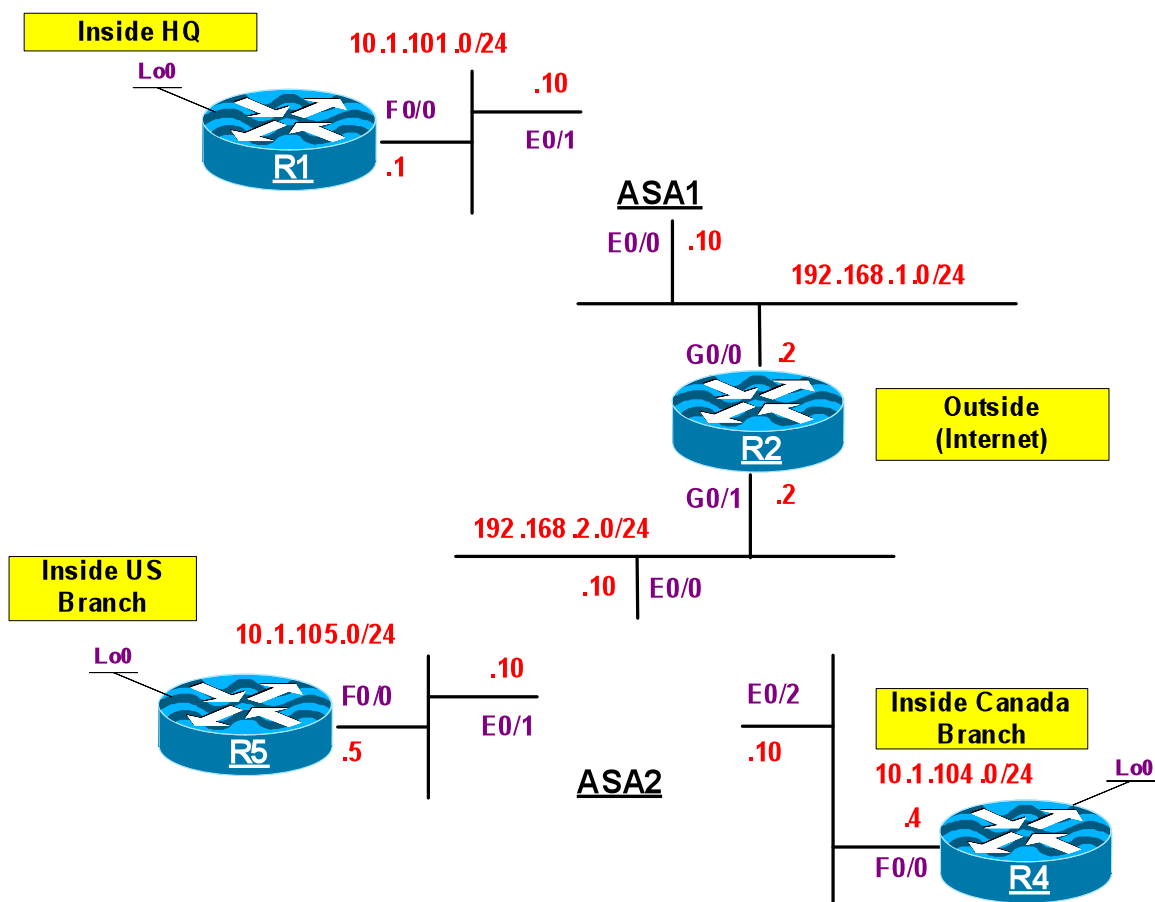
Session Type: LAN-to-LAN

```

Connection   : 10.1.104.4
Index        : 11                      IP Addr      : 4.4.4.4
Protocol     : IKE IPsec
Encryption   : DES                     Hashing      : SHA1
Bytes Tx     : 1000                    Bytes Rx     : 2400
Login Time   : 04:12:23 UTC Fri Jul 23 2010
Duration     : 0h:20m:54s
Connection   : 10.1.105.5
Index        : 12                      IP Addr      : 5.5.5.5
Protocol     : IKE IPsec
Encryption   : 3DES                    Hashing      : MD5
Bytes Tx     : 500                     Bytes Rx     : 500
Login Time   : 04:29:09 UTC Fri Jul 23 2010
Duration     : 0h:04m:08s

```


Lab 1.45. Site-to-Site IPsec VPN using EasyVPN NEM (IOS-IOS)



This lab is based on previous labs configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"

- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure IPSec VPN tunnel between branch routers with the following parameters:

Tunnel Endpoint	SRC Network	DST Network	ISAKMP Policy	IPSec Policy
R5 – R4	5.5.5.5	4.4.4.4	Authentication: PSK Encryption: 3DES Group: 2 Hash: SHA	Encryption: ESP/3DES Authentication: ESP/SHA

Use Easy VPN to configure the tunnel in network extension mode. Router R5 should act as EasyVPN Remote and router R4 should be EasyVPN Server. Use group name of "BRANCH_US" with the password of "cisco123". Configure a new user name of

“easy” with password of “vpn123” in R4’s local database and use it for extended authentication.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#username easy password vpn123
```

```
R4(config)#aaa new-model
```

```
R4(config)#aaa authentication login USER-AUTH local
```

```
R4(config)#aaa authorization network GR-AUTH local
```

AAA on the router must be enabled because EasyVPN feature may use additional peer authentication which is named “XAUTH” (Extended authentication). Authorization list (network) specifies where session parameters which should be populated to a client are stored.

```
R4(config)#crypto isakmp policy 3
```

```
R4(config-isakmp)# encr 3des
```

```
R4(config-isakmp)# authentication pre-share
```

```
R4(config-isakmp)# group 2
```

```
R4(config-isakmp)#exit
```

```
R4(config)#crypto isakmp client configuration group BRANCH_US
```

```
R4(config-isakmp-group)# key cisco123
```

```
R4(config-isakmp-group)#exit
```

This is a configuration item which enables to specify parameters which are populated to the client during “Config Mode”. Config Mode (often called IKE Phase 1.5) is a special stage of IKE during which client requests configuration parameters for the session that is being negotiated. The EasyVPN Server populates these parameters to EasyVPN client.

```
R4(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
```

```
R4(cfg-crypto-trans)#exit
```

```
R4(config)#crypto dynamic-map DYN-CMAP 10
```

```
R4(config-crypto-map)# set transform-set TSET
```

```
R4(config-crypto-map)#exit
```

The peer IP address and other IPSec parameters are unknown at the moment of crypto map configuration. Dynamic crypto map enables to negotiate proper values during tunnel

establishment.

```
R4(config)#crypto map EASY-VPN client authentication list USER-AUTH
R4(config)#crypto map EASY-VPN isakmp authorization list GR-AUTH
R4(config)#crypto map EASY-VPN 10 ipsec-isakmp dynamic DYN-CMAP

R4(config)#interface f0/0
R4(config-if)# crypto map EASY-VPN
R4(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
```

Step 2 R5 configuration.

```
R5(config)#crypto ipsec client ezvpn EZ
R5(config-crypto-ezvpn)# connect auto
```

The connection will be initiated automatically.

```
R5(config-crypto-ezvpn)# group BRANCH_US key cisco123
```

EasyVPN group authentication - it is similar to peer authentication in L2L tunnel negotiations. This is a device authentication.

```
R5(config-crypto-ezvpn)# mode network-extension
```

NEM (Network Extension Mode) enables EasyVPN client to preserve its IP address as tunnel endpoint. The traffic initiated from the client inside network is not NATed so that it allows to connect to this network from the networks behind the EasyVPN server.

```
R5(config-crypto-ezvpn)# peer 10.1.104.4
```

EasyVPN Server IP address.

```
R5(config-crypto-ezvpn)# xauth userid mode interactive
```

Interactive entering of the user credential that will be used during Extended Authentication (XAUTH). These credentials have to be entered during every IKE negotiations. The credential storage in the EasyVPN client configuration have to be exclusively enabled in the EasyVPN Server configuration (save-password command in the group configuration).

```
R5(config-crypto-ezvpn)#exit
```

```
R5(config)#int lo0
R5(config-if)# crypto ipsec client ezvpn EZ inside
```

```
R5(config-if)#exit
```

```
R5(config)#int f0/0
```

```
R5(config-if)# crypto ipsec client ezvpn EZ outside
```

```
R5(config-if)#
```

These commands define the inside and outside interfaces of the EasyVPN Client. Outside interface is used for IPSec tunnel termination.

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

After a while the following error message appears on R5. Since IPSec tunnel needs to be established between two peers who are on different interfaces of ASA but with the same security level of 100. This must be explicitly allowed on the ASA.

```
%CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client)  User=  Group=BRANCH_US  
Client_public_addr=10.1.105.5  Server_public_addr=10.1.104.4
```

Step 3 ASA2 configuration.

```
ASA2(config)# same-security-traffic permit inter-interface
```

Step 4 R5 configuration.

```
R5#
```

```
EZVPN(EZ): Pending XAuth Request, Please enter the following  
command:
```

```
EZVPN: crypto ipsec client ezvpn xauth
```

```
R5#
```

```
R5#crypto ipsec client ezvpn xauth
```

```
Username: easy
```

```
Password:
```

```
R5#
```

```
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=BRANCH_US  
Client_public_addr=10.1.105.5  Server_public_addr=10.1.104.4  
NEM_Remote_Subnets=5.5.5.0/255.255.255.0
```

The user and the password have been provided for XAUTH. Note that EasyVPN connection is up. The client informs the server about its inside networks. These networks may be injected into the server's routing table when reverse route feature is.

Verification

R5#ping 4.4.4.4 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The connection is established. R5 is able to ping R4's loopback through the IPsec tunnel.

R5#sh crypto ipsec client ezvpn

```
Easy VPN Remote Phase: 8

Tunnel name : EZ
Inside interface list: Loopback0
Outside interface: FastEthernet0/0
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Save Password: Disallowed
Current EzVPN Peer: 10.1.104.4
```

EasyVPN session status. Note that saving XAUTH password is disabled (this is a default setting).

R5#sh crypto isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
-----
1002  10.1.105.5        10.1.104.4          ACTIVE 3des sha 2 23:59:10 CX
      Engine-id:Conn-id = SW:2

IPv6 Crypto ISAKMP SA
```

R5#sh crypto ipsec sa

```
interface: FastEthernet0/0
  Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.105.5

protected vrf: (none)
local  ident (addr/mask/prot/port): (5.5.5.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer 10.1.104.4 port 500
```

Note that remote proxy identity is 0.0.0.0/0 that means "any". By default EasyVPN disallow the client to transmit unencrypted traffic apart from established IPSec tunnel. This may be changed when split-tunnel feature is enabled on the EasyVPN server.

```
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 10.1.104.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xB33E0E9(187949289)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x428A6416(1116365846)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
    sa timing: remaining key lifetime (k/sec): (4603441/3543)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xB33E0E9(187949289)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
    sa timing: remaining key lifetime (k/sec): (4603441/3543)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R4#pi 5.5.5.5 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:

Packet sent with a source address of 4.4.4.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Note that inside network of the client is accessible from the server inside network. It is an advantage of network-extension mode. In case of using the "client mode" accessing the inside client network is not feasible due to PAT enabled on the IPSec tunnel endpoint that translates the client inside network.

R4#sh cry isak sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.104.4	10.1.105.5		ACTIVE	3des	sha		2	23:58:35	CX
Engine-id:Conn-id = SW:2										

IPv6 Crypto ISAKMP SA

R4#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: EASY-VPN, local addr 10.1.104.4

protected vrf: (none)

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (5.5.5.0/255.255.255.0/0/0)

current_peer 10.1.105.5 port 500

PERMIT, flags={}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 10.1.105.5

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x428A6416(1116365846)

PFS (Y/N): N, DH group: none

inbound esp sas:


```
spi: 0xB33E0E9(187949289)
```

R4#sh crypto map

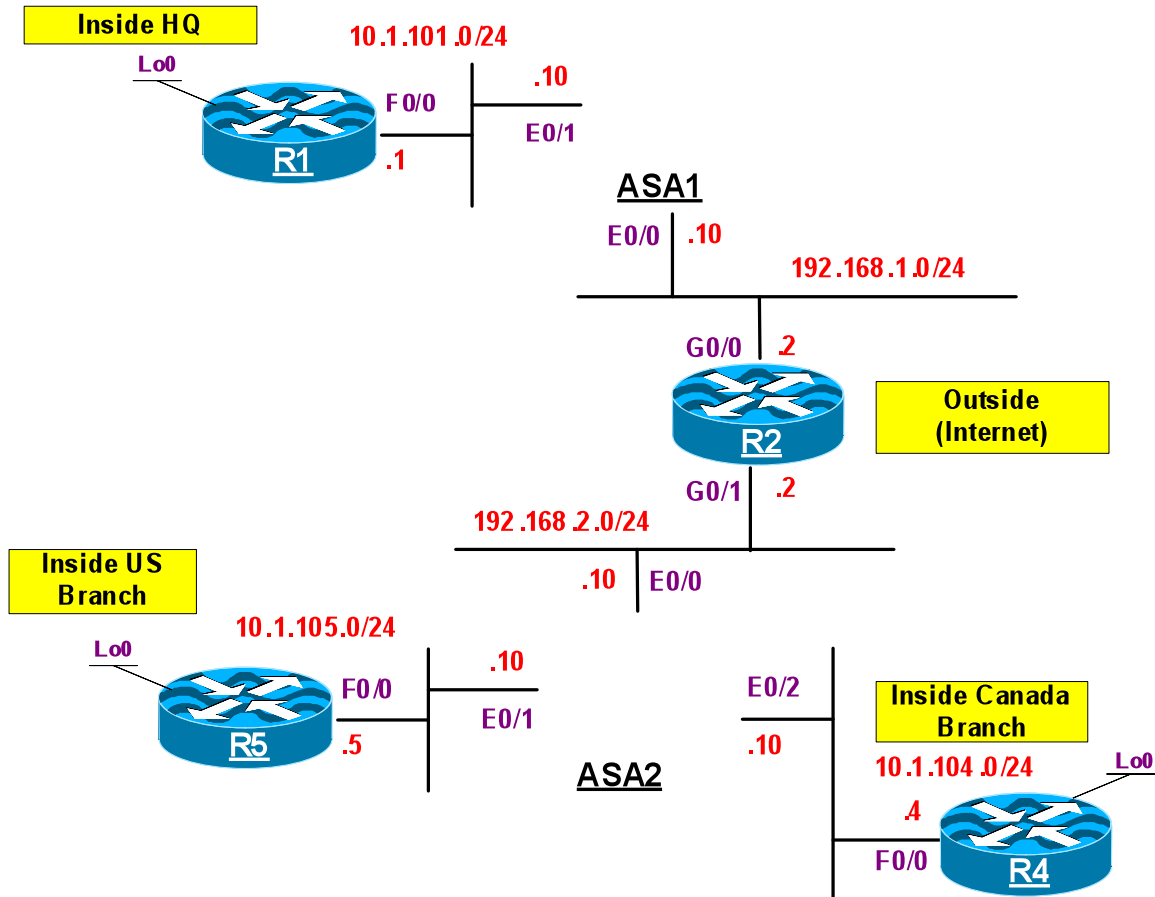
```
Crypto Map "EASY-VPN" 10 ipsec-isakmp
    Dynamic map template tag: DYN-CMAP
```

```
Crypto Map "EASY-VPN" 65536 ipsec-isakmp
    Peer = 10.1.105.5
    Extended IP access list
        access-list permit ip any 5.5.5.0 0.0.0.255
        dynamic (created from dynamic map DYN-CMAP/10)
```

Note that definition of interesting traffic has been configured dynamically by dynamic-crypto map. Information relevant to the client inside networks is passed to the server during IKE negotiation.

```
Current peer: 10.1.105.5
Security association lifetime: 4608000 kilobytes/3600 seconds
Responder-Only (Y/N): N
PFS (Y/N): N
Transform sets={
    TSET: { esp-3des esp-sha-hmac } ,
}
Interfaces using crypto map EASY-VPN:
    FastEthernet0/0
```

Lab 1.46. Site-to-Site IPsec VPN using EasyVPN NEM (IOS-ASA)



This lab is based on previous labs configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"

- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure IPSec VPN tunnel between ASA1 and R5/R4 with the following parameters:

Tunnel	SRC	DST	ISAKMP Policy	IPSec Policy
Endpoint	Network	Network		
ASA1 – R5/R4	1.1.1.1	5.5.5.5 4.4.4.4	Authentication: PSK Encryption: 3DES Group: 2 Hash: SHA	Encryption: ESP/3DES Authentication: ESP/SHA

Use Easy VPN to configure the tunnel in network extension mode. R5 should act as EasyVPN Remote and ASA1 should be an EasyVPN Server. Use group name of "BRANCHES" with the password of "cisco123".

Do not use extended authentication, the branch routers should connect using only group credentials. Ensure that branch routers will tunnel traffic only destined to the network of 1.1.1.0/24.

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```
ASA1(config)# access-list EZVPN-TRAFFIC permit ip host 1.1.1.1 host
5.5.5.5
ASA1(config)# access-list EZVPN-TRAFFIC permit ip host 1.1.1.1 host
4.4.4.4

ASA1(config)# access-list ST standard permit 1.1.1.0 255.255.255.0

ASA1(config)# group-policy EZ-POLICY internal
```

The group-policy contains parameters that are passed down to the client or such parameters may be requirements that the client have to fulfill before IPSec session is established. Note that this is an internally configured group-policy. Group-policies may be provided from ACS Server. Note that group-policy definition is based on Attribute-Value pairs.

```
ASA1(config)# group-policy EZ-POLICY attributes
ASA1(config-group-policy)# split-tunnel-policy tunnelspecified
ASA1(config-group-policy)# split-tunnel-network-list value ST
ASA1(config-group-policy)# nem enable
```

Network Extension Mode has been enabled. This policy includes also the definition of split tunneling. This feature enables the server to define the exceptions of default rule that enforcing full traffic encryption between the client and the server. The traffic definition is made by an ACL which is tied to group-policy by the command of "split-tunnel-network-list".

"split-tunnel-policy" defines the policy which is applied for a traffic chosen by the split-tunnel ACL. The traffic may be encrypted if "tunnelspecified" is enabled or the traffic is excluded from encryption if "excludespecified" is enabled. A "tunnelall" option may also be used but encryption of all the traffic is the default. Note that from the client perspective the network defined by the ACL in split-tunneling in fact defines a destination of the traffic rather than the source.

```
ASA1(config-group-policy)# exit

ASA1(config)# isakmp enable Outside

ASA1(config)# crypto isakmp policy 1 authentication pre-share
ASA1(config)# crypto isakmp policy 1 encryption 3des
ASA1(config)# crypto isakmp policy 1 hash sha
ASA1(config)# crypto isakmp policy 1 group 2

ASA1(config)# tunnel-group BRANCHES type remote-access
ASA1(config)# tunnel-group BRANCHES general-attributes
ASA1(config-tunnel-general)# default-group-policy EZ-POLICY
ASA1(config-tunnel-general)# exit
```

Tunnel-group for EasyVPN clients has been defined. Note that group-policy has been tied to tunnel-group as its general attribute.

```
ASA1(config)# tunnel-group BRANCHES ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key cisco123
ASA1(config-tunnel-ipsec)# isakmp ikev1-user-authentication none
ASA1(config-tunnel-ipsec)# exit
```

XAUTH has been disabled (by default ASA requires XAUTH). Only the peer authentication will be performed.

```
ASA1(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac

ASA1(config)# crypto dynamic-map DYN-MAP 5 set transform-set TSET

ASA1(config)# crypto map ENCRYPT_OUT 1 ipsec-isakmp dynamic DYN-MAP

ASA1(config)# crypto map ENCRYPT_OUT interface Outside

ASA1(config)# route Inside 1.1.1.1 255.255.255.255 10.1.101.1
```

Step 2 ASA2 configuration.

```
ASA2(config)# policy-map global_policy
ASA2(config-pmap)# class inspection_default
ASA2(config-pmap-c)# inspect ipsec-pass-thru
```

The IPSec-related traffic through ASA2 has been allowed.

Step 3 R5 configuration.

```
R5(config)#crypto ipsec client ezvpn HQ
R5(config-crypto-ezvpn)#connect auto
R5(config-crypto-ezvpn)#group BRANCHES key cisco123
R5(config-crypto-ezvpn)#mode network-extension
```

```
R5(config-crypto-ezvpn)#peer 192.168.1.10

R5(config-crypto-ezvpn)#int f0/0
R5(config-if)# crypto ipsec client ezvpn HQ outside

R5(config-if)#int lo0
R5(config-if)# crypto ipsec client ezvpn HQ inside
R5(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=BRANCHES
Client_public_addr=10.1.105.5  Server_public_addr=192.168.1.10
NEM_Remote_Subnets=5.5.5.0/255.255.255.0
```

The tunnel has been established. Note that entering the user and password interactively is no longer needed.

Step 4 R4 configuration.

```
R4(config)#crypto ipsec client ezvpn HQ
R4(config-crypto-ezvpn)#connect auto
R4(config-crypto-ezvpn)#group BRANCHES key cisco123
R4(config-crypto-ezvpn)#mode network-extension
R4(config-crypto-ezvpn)#peer 192.168.1.10
R4(config-crypto-ezvpn)#exit

R4(config)#int f0/0
R4(config-if)#crypto ipsec client ezvpn HQ outside

R4(config-if)#int lo0
R4(config-if)#crypto ipsec client ezvpn HQ inside
R4(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=BRANCHES
Client_public_addr=10.1.104.4  Server_public_addr=192.168.1.10
NEM_Remote_Subnets=4.4.4.0/255.255.255.0
```

Verification

R4#ping 1.1.1.1 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 4.4.4.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R4#sh cry isak sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1003	10.1.104.4	192.168.1.10		ACTIVE	3des	sha	psk	2	23:57:23	C

Engine-id:Conn-id = SW:3

Note that authentication by using tunnel-group name and the password is treated as pre-shared ISAKMP peer authentication.

IPv6 Crypto ISAKMP SA

R4#sh cry ips sa

interface: FastEthernet0/0

Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.104.4

protected vrf: (none)

local ident (addr/mask/prot/port): (4.4.4.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x63FABD04(1677376772)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xD3631C04(3546487812)

transform: esp-3des esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2005, flow_id: NETGX:5, sibling_flags 80000046, crypto map:

FastEthernet0/0-head-0

sa timing: remaining key lifetime (k/sec): (4483637/28677)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

```
inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0x63FABD04(1677376772)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2006, flow_id: NETGX:6, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4483637/28677)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcg sas:
```

R4#sh cry sess

Crypto session current status

```
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 192.168.1.10 port 500
IKE SA: local 10.1.104.4/500 remote 192.168.1.10/500 Active
IPSEC FLOW: permit ip 4.4.4.0/255.255.255.0 1.1.1.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

R4#sh crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

```
Tunnel name : HQ
Inside interface list: Loopback0
Outside interface: FastEthernet0/0
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Save Password: Disallowed
Split Tunnel List: 1
  Address      : 1.1.1.0
  Mask         : 255.255.255.0
  Protocol     : 0x0
  Source Port  : 0
  Dest Port    : 0
Current EzVPN Peer: 192.168.1.10
```

The client has obtained split-tunnel configuration from the server during Mode Config. Protocol value 0x0 means that all IP traffic to 1.1.1.0/24 will be encrypted.

R5#ping 1.1.1.1 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 5.5.5.5

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R5#sh cry isa sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1003	10.1.105.5	192.168.1.10		ACTIVE	3des	sha	psk	2	23:58:00	C

Engine-id:Conn-id = SW:3

IPv6 Crypto ISAKMP SA

R5#sh cry ips sa

interface: FastEthernet0/0

Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.105.5

protected vrf: (none)

local ident (addr/mask/prot/port): (5.5.5.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x8AD193D1(2328990673)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xDAA2BC9A(3668098202)

transform: esp-3des esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2005, flow_id: NETGX:5, sibling_flags 80000046, crypto map:

FastEthernet0/0-head-0

sa timing: remaining key lifetime (k/sec): (4494113/28711)

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0x8AD193D1(2328990673)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2006, flow_id: NETGX:6, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
sa timing: remaining key lifetime (k/sec): (4494113/28711)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcg sas:
```

R5#sh cry sess

Crypto session current status

```
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 192.168.1.10 port 500
IKE SA: local 10.1.105.5/500 remote 192.168.1.10/500 Active
IPSEC FLOW: permit ip 5.5.5.0/255.255.255.0 1.1.1.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

R5#sh crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

```
Tunnel name : HQ
Inside interface list: Loopback0
Outside interface: FastEthernet0/0
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Save Password: Disallowed
Split Tunnel List: 1
Address      : 1.1.1.0
Mask         : 255.255.255.0
Protocol     : 0x0
Source Port: 0
Dest Port    : 0
Current EzVPN Peer: 192.168.1.10
```

ASA1(config)# sh cry isak sa det

Active SA: 2
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 2

```
1  IKE Peer: 10.1.105.5
    Type      : user          Role      : responder
    Rekey     : no           State     : AM_ACTIVE
    Encrypt   : 3des         Hash      : SHA
    Auth      : preshared    Lifetime: 86400
    Lifetime Remaining: 86245
2  IKE Peer: 10.1.104.4
    Type      : user          Role      : responder
    Rekey     : no           State     : AM_ACTIVE
    Encrypt   : 3des         Hash      : SHA
    Auth      : preshared    Lifetime: 86400
    Lifetime Remaining: 86266
```

Note that ASA plays the role of responder for the both connecton because the tunnels have been initiated from the client side.

ASA1(config)# sh cry ips sa

```
interface: Outside
  Crypto map tag: DYN-MAP, seq num: 5, local addr: 192.168.1.10

  local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (4.4.4.0/255.255.255.0/0/0)
  current_peer: 10.1.104.4, username: BRANCHES
  dynamic allocated peer ip: 0.0.0.0

  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.104.4

  path mtu 1500, ipsec overhead 58, media mtu 1500
  current outbound spi: D3631C04

inbound esp sas:
  spi: 0x63FABD04 (1677376772)
    transform: esp-3des esp-sha-hmac no compression
    in use settings = {RA, Tunnel, }
    slot: 0, conn_id: 73728, crypto-map: DYN-MAP
```

```
sa timing: remaining key lifetime (sec): 28659
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x0000003F
outbound esp sas:
spi: 0xD3631C04 (3546487812)
transform: esp-3des esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 73728, crypto-map: DYN-MAP
sa timing: remaining key lifetime (sec): 28659
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x00000001

Crypto map tag: DYN-MAP, seq num: 5, local addr: 192.168.1.10

local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (5.5.5.0/255.255.255.0/0/0)
current_peer: 10.1.105.5, username: BRANCHES
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.10, remote crypto endpt.: 10.1.105.5

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: DAA2BC9A

inbound esp sas:
spi: 0x8AD193D1 (2328990673)
transform: esp-3des esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 65536, crypto-map: DYN-MAP
sa timing: remaining key lifetime (sec): 28636
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x0000003F
outbound esp sas:
spi: 0xDAA2BC9A (3668098202)
transform: esp-3des esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 65536, crypto-map: DYN-MAP
```

```

sa timing: remaining key lifetime (sec): 28635
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

ASA1(config)# sh vpn-sessiondb ra protocol

```

Filter Group      : All
Total Active Tunnels : 4
Cumulative Tunnels : 29

```

Protocol	Tunnels	Percent
IKE	2	50%
IPsec	2	50%
IPsecLAN2LAN	0	0%
IPsecLAN2LANOverNatT	0	0%
IPsecOverNatT	0	0%
IPsecOverTCP	0	0%
IPsecOverUDP	0	0%
L2TPOverIPsec	0	0%
L2TPOverIPsecOverNatT	0	0%
Clientless	0	0%
Port-Forwarding	0	0%
IMAP4S	0	0%
POP3S	0	0%
SMTPS	0	0%
SSL-Tunnel	0	0%
DTLS-Tunnel	0	0%

Note that vpnsession database indicated that there are four active tunnels: two of IKE and two of IPsec.

ASA1(config)# sh vpn-sessiondb remote

Session Type: IPsec

Username	: BRANCHES	Index	: 16
Assigned IP	: 5.5.5.0	Public IP	: 10.1.105.5
Protocol	: IKE IPsec		
License	: IPsec		
Encryption	: 3DES	Hashing	: SHA1
Bytes Tx	: 500	Bytes Rx	: 500
Group Policy	: EZ-POLICY	Tunnel Group	: BRANCHES
Login Time	: 06:09:57 UTC Fri Jul 23 2010		
Duration	: 0h:03m:26s		
NAC Result	: Unknown		
VLAN Mapping	: N/A	VLAN	: none
Username	: BRANCHES	Index	: 18
Assigned IP	: 4.4.4.0	Public IP	: 10.1.104.4
Protocol	: IKE IPsec		

```

License       : IPsec
Encryption    : 3DES
Bytes Tx      : 500
Bytes Rx      : 500
Group Policy  : EZ-POLICY
Tunnel Group  : BRANCHES
Login Time    : 06:10:18 UTC Fri Jul 23 2010
Duration      : 0h:03m:05s
NAC Result    : Unknown
VLAN Mapping  : N/A
VLAN          : none

```

Show vpn-sessiondb remote displays information relevant to tunnels established with remote peers. Note that Network Extension Mode makes inside client network visible.

Verification (detailed)

```
ASA1(config)# deb cry isak 20
```

```

Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + KE
(4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 1140
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing SA payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, Received NAT-Traversal RFC VID
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, Received NAT-Traversal ver 03 VID
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, Received NAT-Traversal ver 02 VID
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing ke payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing ISA_KE payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing nonce payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing ID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, Received DPD VID
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, Received xauth V6 VID
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, Claims to be IOS but failed
authentication
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, processing VID payload
Jul 23 06:15:33 [IKEv1 DEBUG]: IP = 10.1.105.5, Received Cisco Unity client VID
Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, Connection landed on tunnel group BRANCHES
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, No valid authentication
type found for the tunnel group
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing IKE SA
payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKE SA Proposal # 1,
Transform # 17 acceptable Matches global IKE entry # 3

```

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing ISAKMP SA payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing ke payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing nonce payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Generating keys for Responder...

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing ID payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing hash payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Computing hash for ISAKMP

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing Cisco Unity VID payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing xauth V6 VID payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing dpd vid payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing NAT-Traversal VID ver 02 payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing NAT-Discovery payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, computing NAT Discovery hash

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing NAT-Discovery payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, computing NAT Discovery hash

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing Fragmentation VID + extended capabilities payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing VID payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Send Altiga/Cisco VPN3000/Cisco ASA GW VID

Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 440

Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NAT-D (130) + NAT-D (130) + NOTIFY (11) + NONE (0) total length : 128

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing hash payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Computing hash for ISAKMP

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing NAT-Discovery payload

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, computing NAT Discovery hash

```

Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing NAT-
Discovery payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, computing NAT
Discovery hash
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing notify
payload
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Automatic NAT Detection
Status:      Remote end is NOT behind a NAT device      This end is NOT behind a NAT
device
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
primary DNS = cleared
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
secondary DNS = cleared
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
primary WINS = cleared
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
secondary WINS = cleared
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
split tunneling list = ST
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
IP Compression = disabled
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
Split Tunneling Policy = Split Network
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
Browser Proxy Setting = no-modify
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKEGetUserAttributes:
Browser Proxy Bypass Local = disable

```

The session parameters have been set and prepared for passing them to the client. Note that split-tunnel network list and policy are visible. Undefined parameters in the group-policy have been marked as "cleared".

```

Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=a776bd6d)
with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 380
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, process_attr():
Enter!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Processing cfg
Request attributes
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Received unknown
transaction mode attribute: 28692
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Received unknown
transaction mode attribute: 28693
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received
request for DNS server address!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received
request for DNS server address!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received
request for WINS server address!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received
request for WINS server address!

```



```
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for Split Tunnel List!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for Split DNS!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for Default Domain Name!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for Save PW setting!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for Local LAN Include!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for PFS setting!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for backup ip-sec peer list!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for Application Version!
```

Mode Config has been started. The client has requested a set of parameters which will be passed down from the server. The client has requested the following: DNS server, WINS server, Split tunnel list, Split tunnel DNS (the DNS server which will be used for inquiring about names through the tunnel), allowance for saving the XAUTH password locally on the client, allowance for communication with local lan without an encryption, PFS settings and the list of backup peers (EasyVPN servers).

```
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Client Type: IOS Client Application Version: 12.4(24)T2
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for Banner!
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Received unknown transaction mode attribute: 28695
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, MODE_CFG: Received request for DHCP hostname for DDNS is: R5!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing blank hash payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing qm hash payload
Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=a776bd6d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 172
Jul 23 06:15:33 [IKEv1 DECODE]: IP = 10.1.105.5, IKE Responder starting QM: msg id = 9196d7a4
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, PHASE 1 COMPLETED
Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, Keep-alive type for this connection: DPD
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Starting P1 rekey timer: 82080 seconds.
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, sending notify message
```

```
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing blank
hash payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing qm hash
payload
Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=94a8c6f)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 92
Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=9196d7a4)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total
length : 1280
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing hash
payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing SA payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing nonce
payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing ID payload
Jul 23 06:15:33 [IKEv1 DECODE]: Group = BRANCHES, IP = 10.1.105.5, ID_IPV4_ADDR_SUBNET
ID received--5.5.5.0--255.255.255.0
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Received remote IP Proxy
Subnet data in ID Payload: Address 5.5.5.0, Mask 255.255.255.0, Protocol 0, Port 0
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing ID payload
Jul 23 06:15:33 [IKEv1 DECODE]: Group = BRANCHES, IP = 10.1.105.5, ID_IPV4_ADDR_SUBNET
ID received--1.1.1.0--255.255.255.0
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Received local IP Proxy
Subnet data in ID Payload: Address 1.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0
```

The client has informed the server about its inside network to establish identity of local and remote IPSec proxy.

```
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, QM IsRekeyed old sa not
found by addr
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, IKE Remote Peer configured
for crypto map: DYN-MAP
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing IPSec SA
payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IPSec SA Proposal #
11, Transform # 1 acceptable Matches global IPSec SA entry # 5
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, IKE: requesting SPI!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKE got SPI from key
engine: SPI = 0x592ce8c6
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, oakley constucting
quick mode
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing blank
hash payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing IPSec SA
payload
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Overriding Initiator's
IPSec rekeying duration from 2147483 to 28800 seconds
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing IPSec
nonce payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing proxy ID
```

```
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Transmitting Proxy
Id:
  Remote subnet: 5.5.5.0 Mask 255.255.255.0 Protocol 0 Port 0
  Local subnet: 1.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
```

The server has informed the client about remote and local proxy ID.

```
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Sending RESPONDER
LIFETIME notification to Initiator
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, constructing qm hash
payload
Jul 23 06:15:33 [IKEv1 DECODE]: Group = BRANCHES, IP = 10.1.105.5, IKE Responder
sending 2nd QM pkt: msg id = 9196d7a4
Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE SENDING Message (msgid=9196d7a4)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) +
NONE (0) total length : 196
Jul 23 06:15:33 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=9196d7a4)
with payloads : HDR + HASH (8) + NONE (0) total length : 52
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing hash
payload
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, loading all IPSEC SAs
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Generating Quick Mode
Key!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, NP encrypt rule look
up for crypto map DYN-MAP 5 matching ACL Unknown: returned cs_id=d791a4b0;
rule=00000000
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Generating Quick Mode
Key!
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, NP encrypt rule look
up for crypto map DYN-MAP 5 matching ACL Unknown: returned cs_id=d791a4b0;
rule=00000000
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, Security negotiation
complete for User (BRANCHES) Responder, Inbound SPI = 0x592ce8c6, Outbound SPI =
0xf1e42b1c
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, IKE got a KEY_ADD msg
for SA: SPI = 0xf1e42b1c
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Pitcher: received
KEY_UPDATE, spi 0x592ce8c6
Jul 23 06:15:33 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, Starting P2 rekey
timer: 27360 seconds.
Jul 23 06:15:33 [IKEv1]: Group = BRANCHES, IP = 10.1.105.5, PHASE 2 COMPLETED
(msgid=9196d7a4)
Jul 23 06:15:34 [IKEv1]: IP = 10.1.105.5, IKE_DECODE RECEIVED Message (msgid=2468295b)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 205
Jul 23 06:15:34 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing hash
payload
Jul 23 06:15:34 [IKEv1 DEBUG]: Group = BRANCHES, IP = 10.1.105.5, processing notify
payload
Jul 23 06:15:34 [IKEv1 DECODE]: OBSOLETE DESCRIPTOR - INDEX 1
Jul 23 06:15:34 [IKEv1 DECODE]: 0000: 00000000 75340003 52352E75 32000A43
....u4..R5.u2..C
```

```

0010: 6973636F 20323831 31753500 0B46484B      isco 281lu5..FHK
0020: 30383439 46314241 75300009 32353735      0849F1BAu0..2575
0030: 34303039 36753100 09313330 31353835      40096u1..1301585
0040: 39327536 00093232 38353839 35363875      92u6..228589568u
0050: 39000836 33303139 36303875 33002E66      9..63019608u3..f
0060: 6C617368 3A633238 30306E6D 2D616476      lash:c2800nm-adv
0070: 656E7465 72707269 73656B39 2D6D7A2E      enterprisek9-mz.
0080: 3132342D 32342E54 322E6269 6E             124-24.T2.bin

```

```
ASA1(config)# un all
```

Verification (deep dive)

Alternatively you can use ISAKMP capture to get all IKE packets and analyze their content. The output is pretty long but it's worth to see it.

```
ASA1(config)# capture IKE type isakmp interface outside
ASA1(config)# sho capture IKE
```

```
18 packets captured
```

```

1: 06:37:20.47184260 10.1.105.5.500 > 192.168.1.10.500:  udp 1140
2: 06:37:20.47184270 192.168.1.10.500 > 10.1.105.5.500:  udp 440
3: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500:  udp 132
4: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500:  udp 132
5: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500:  udp 388
6: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500:  udp 388
7: 06:37:20.47184320 192.168.1.10.500 > 10.1.105.5.500:  udp 172
8: 06:37:20.47184320 192.168.1.10.500 > 10.1.105.5.500:  udp 172
9: 06:37:20.47184350 10.1.105.5.500 > 192.168.1.10.500:  udp 1284
10: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500:  udp 92
11: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500:  udp 92
12: 06:37:20.47184350 10.1.105.5.500 > 192.168.1.10.500:  udp 1284
13: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500:  udp 196
14: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500:  udp 196
15: 06:37:20.47184360 10.1.105.5.500 > 192.168.1.10.500:  udp 60
16: 06:37:20.47184360 10.1.105.5.500 > 192.168.1.10.500:  udp 60
17: 06:37:21.47185020 10.1.105.5.500 > 192.168.1.10.500:  udp 212
18: 06:37:21.47185020 10.1.105.5.500 > 192.168.1.10.500:  udp 212

```

```
18 packets shown
```

Note: 18 packets has been captured. Let's see what they contain.

```
ASA1(config)# sho capture IKE decode
```

```
18 packets captured
```

See that R5 sends IKE packet in Aggressive Mode. It contains almost all required information like SA Proposals, Group name, Key Exchange, and identity info – see greyed fields. Remember that the aggressive mode in EasyVPN is used when ISAKMP peer authentication is based on pre-shared-key.

```
1: 06:37:20.47184260 10.1.105.5.500 > 192.168.1.10.500:  udp 1140
ISAKMP Header
  Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
  Responder COOKIE: 00 00 00 00 00 00 00 00
  Next Payload: Security Association
  Version: 1.0
  Exchange Type: Aggressive Mode
  Flags: (none)
  MessageID: 00000000
  Length: 1140
  Payload Security Association
    Next Payload: Vendor ID
    Reserved: 00
    Payload Length: 788
    DOI: IPsec
    Situation: (SIT_IDENTITY_ONLY)
    Payload Proposal
      Next Payload: None
      Reserved: 00
      Payload Length: 776
      Proposal #: 1
      Protocol-Id: PROTO_ISAKMP
      SPI Size: 0
      # of transforms: 20
      Payload Transform
        Next Payload: Transform
        Reserved: 00
        Payload Length: 40
        Transform #: 1
        Transform-Id: KEY_IKE
        Reserved2: 0000
        Encryption Algorithm: AES-CBC
        Key Length: 128
        Hash Algorithm: SHA1
        Group Description: Group 2
        Authentication Method: XAUTH_INIT_PRESHRD
        Life Type: seconds
        Life Duration (Hex): 00 20 c4 9b
```

This and the next Payload Transforms are ISAKMP policies hardcoded into the EasyVPN client software.

```
  Payload Transform
    Next Payload: Transform
    Reserved: 00
    Payload Length: 40
```

Transform #: 2
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: AES-CBC
Key Length: 128
Hash Algorithm: MD5
Group Description: Group 2
Authentication Method: XAUTH_INIT_PRESHRD
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00

Payload Length: 40

Transform #: 3

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: AES-CBC

Key Length: 192

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTH_INIT_PRESHRD

Life Type: seconds

Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00

Payload Length: 40

Transform #: 4

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: AES-CBC

Key Length: 192

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTH_INIT_PRESHRD

Life Type: seconds

Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00

Payload Length: 40

Transform #: 5

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: AES-CBC

Key Length: 256

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTH_INIT_PRESHRD

Life Type: seconds

```
Life Duration (Hex): 00 20 c4 9b
Payload Transform
  Next Payload: Transform
  Reserved: 00
  Payload Length: 40
  Transform #: 6
  Transform-Id: KEY_IKE
  Reserved2: 0000
  Encryption Algorithm: AES-CBC
  Key Length: 256
  Hash Algorithm: MD5
  Group Description: Group 2
  Authentication Method: XAUTH_INIT_PRESHRD
  Life Type: seconds
  Life Duration (Hex): 00 20 c4 9b
Payload Transform
  Next Payload: Transform
  Reserved: 00
  Payload Length: 40
  Transform #: 7
  Transform-Id: KEY_IKE
  Reserved2: 0000
  Encryption Algorithm: AES-CBC
  Key Length: 128
  Hash Algorithm: SHA1
  Group Description: Group 2
  Authentication Method: Preshared key
  Life Type: seconds
  Life Duration (Hex): 00 20 c4 9b
Payload Transform
  Next Payload: Transform
  Reserved: 00
  Payload Length: 40
  Transform #: 8
  Transform-Id: KEY_IKE
  Reserved2: 0000
  Encryption Algorithm: AES-CBC
  Key Length: 128
  Hash Algorithm: MD5
  Group Description: Group 2
  Authentication Method: Preshared key
  Life Type: seconds
  Life Duration (Hex): 00 20 c4 9b
Payload Transform
  Next Payload: Transform
  Reserved: 00
  Payload Length: 40
  Transform #: 9
  Transform-Id: KEY_IKE
  Reserved2: 0000
  Encryption Algorithm: AES-CBC
```

Key Length: 192
Hash Algorithm: SHA1
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform
Reserved: 00
Payload Length: 40
Transform #: 10
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: AES-CBC
Key Length: 192
Hash Algorithm: MD5
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform
Reserved: 00
Payload Length: 40
Transform #: 11
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: AES-CBC
Key Length: 256
Hash Algorithm: SHA1
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform
Reserved: 00
Payload Length: 40
Transform #: 12
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: AES-CBC
Key Length: 256
Hash Algorithm: MD5
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform
Reserved: 00

Payload Length: 36
Transform #: 13
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: 3DES-CBC
Hash Algorithm: SHA1
Group Description: Group 2
Authentication Method: XAUTH_INIT_PRESHRD
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00

Payload Length: 36
Transform #: 14
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: 3DES-CBC
Hash Algorithm: MD5
Group Description: Group 2
Authentication Method: XAUTH_INIT_PRESHRD
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00

Payload Length: 36
Transform #: 15
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: DES-CBC
Hash Algorithm: SHA1
Group Description: Group 2
Authentication Method: XAUTH_INIT_PRESHRD
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00

Payload Length: 36
Transform #: 16
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: DES-CBC
Hash Algorithm: MD5
Group Description: Group 2
Authentication Method: XAUTH_INIT_PRESHRD
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00
Payload Length: 36
Transform #: 17
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: 3DES-CBC
Hash Algorithm: SHA1
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00
Payload Length: 36
Transform #: 18
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: 3DES-CBC
Hash Algorithm: MD5
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: Transform

Reserved: 00
Payload Length: 36
Transform #: 19
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: DES-CBC
Hash Algorithm: SHA1
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Transform

Next Payload: None

Reserved: 00
Payload Length: 36
Transform #: 20
Transform-Id: KEY_IKE
Reserved2: 0000
Encryption Algorithm: DES-CBC
Hash Algorithm: MD5
Group Description: Group 2
Authentication Method: Preshared key
Life Type: seconds
Life Duration (Hex): 00 20 c4 9b

Payload Vendor ID

```
Next Payload: Vendor ID
Reserved: 00
Payload Length: 20
Data (In Hex):
    4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f
Payload Vendor ID
Next Payload: Vendor ID
Reserved: 00
Payload Length: 20
Data (In Hex):
    43 9b 59 f8 ba 67 6c 4c 77 37 ae 22 ea b8 f5 82
Payload Vendor ID
Next Payload: Vendor ID
Reserved: 00
Payload Length: 20
Data (In Hex):
    7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
Payload Vendor ID
Next Payload: Key Exchange
Reserved: 00
Payload Length: 20
Data (In Hex):
    90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
Payload Key Exchange
Next Payload: Nonce
Reserved: 00
Payload Length: 132
Data:
    f0 25 90 d8 3f 81 9c 9a dd 71 3e bb 56 57 24 d0
    81 c7 6e 35 8f 66 03 95 4f 57 6f 00 5b 8b 4b fe
    12 55 4e af 01 19 5b 11 55 60 fd 19 d7 ae 5a c3
    59 75 92 aa 70 bd 13 5b a8 cb d1 a7 60 aa 38 16
    74 65 d6 9c 15 ba 4c b3 09 11 93 48 f4 d5 da 43
    ed ba b8 38 c0 ab 1e 67 5c c2 33 47 0a 9a 44 90
    d2 8d a9 0a f8 a9 8d 63 91 9d e9 09 16 4c 0d 85
    7e 92 04 2e fd 43 e4 3e 6d 8c 0a 1b eb 57 2a f9
Payload Nonce
Next Payload: Identification
Reserved: 00
Payload Length: 24
Data:
    c6 a1 41 66 13 2b e4 aa 7f 28 a4 69 42 76 bb d2
    f6 0f f8 27
```

The nonces used for key generation are visible at this part of IKE packet.

```
Payload Identification
Next Payload: Vendor ID
Reserved: 00
Payload Length: 16
ID Type: ID_KEY_ID (11)
```

```

Protocol ID (UDP/TCP, etc...): 17
Port: 0
ID Data: BRANCHES
Payload Vendor ID
Next Payload: Vendor ID
Reserved: 00
Payload Length: 20
Data (In Hex):
    af ca d7 13 68 a1 f1 c9 6b 86 96 fc 77 57 01 00
Payload Vendor ID
Next Payload: Vendor ID
Reserved: 00
Payload Length: 12
Data (In Hex): 09 00 26 89 df d6 b7 12
Payload Vendor ID
Next Payload: Vendor ID
Reserved: 00
Payload Length: 20
Data (In Hex):
    8d fc 3c f7 4d 00 0b 3f 57 27 fa 9a a4 83 76 02
Payload Vendor ID
Next Payload: None
Reserved: 00
Payload Length: 20
Data (In Hex):
    12 f5 f2 8c 45 71 68 a9 70 2d 9f e2 74 cc 01 00

```

The last part of the packet are as follows: Identification data (the EasyVPN group is visible) and vendor specific IDs which define IPSec features supported by the device.

Second packet is a response from the EasyVPN Server. It contain agreed transform (only one that server agreed to) and data required for Key Exchange.

2: 06:37:20.47184270 192.168.1.10.500 > 10.1.105.5.500: udp 440

```

ISAKMP Header
Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Security Association
Version: 1.0
Exchange Type: Aggressive Mode
Flags: (none)
MessageID: 00000000
Length: 440
Payload Security Association
Next Payload: Key Exchange
Reserved: 00
Payload Length: 56
DOI: IPsec
Situation: (SIT_IDENTITY_ONLY)
Payload Proposal

```

```
Next Payload: None
Reserved: 00
Payload Length: 44
Proposal #: 1
Protocol-Id: PROTO_ISAKMP
SPI Size: 0
# of transforms: 1
Payload Transform
  Next Payload: None
  Reserved: 00
  Payload Length: 36
  Transform #: 17
  Transform-Id: KEY_IKE
  Reserved2: 0000
  Encryption Algorithm: 3DES-CBC
  Hash Algorithm: SHA1
  Group Description: Group 2
  Authentication Method: Preshared key
  Life Type: seconds
  Life Duration (Hex): 00 20 c4 9b
```

Chosen ISAKMP policy has been sent as a reply of EasyVPN server

```
Payload Key Exchange
  Next Payload: Nonce
  Reserved: 00
  Payload Length: 132
  Data:
    1f 65 76 e3 81 7a 55 1e d8 9d 5b 5e 88 8d d8 d9
    ae 69 ba 3a 61 0b 29 4f 54 32 ab fe 02 a9 16 95
    05 7a ec 7e c3 7e dd 50 bf 2b 86 8b 33 5f 5f bf
    65 ef 8e 49 5c 8f 38 48 cd fa 9a f1 ab 18 c7 4b
    0c b5 e8 66 f4 5e 9b dd bb e5 ee 28 c0 2a 8b f3
    ea 00 68 71 88 00 65 d6 0e 0f 8d 85 30 23 87 76
    ac d9 ca 21 6e 73 8e e7 2e d6 c8 2d d4 f7 69 88
    34 8d 11 e9 0e 1b 67 5b f0 20 6a 66 e0 fa 39 41
  Payload Nonce
    Next Payload: Identification
    Reserved: 00
    Payload Length: 24
    Data:
      db f3 19 e4 cb d0 f8 27 47 45 09 11 fe ee dc 12
      6e 8f 04 68
```

Further session key material negotiations.

```
Payload Identification
  Next Payload: Hash
  Reserved: 00
  Payload Length: 12
  ID Type: IPv4 Address (1)
```

Protocol ID (UDP/TCP, etc...): 17

Port: 0

ID Data: 192.168.1.10

Identity of the EasyVPN server.

Payload Hash

Next Payload: Vendor ID

Reserved: 00

Payload Length: 24

Data:

72 a4 56 ac 28 ff 93 c8 f3 de d1 7d 6c fd c6 a7

2e 0a 86 fc

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 00

Payload Length: 20

Data (In Hex):

12 f5 f2 8c 45 71 68 a9 70 2d 9f e2 74 cc 01 00

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 00

Payload Length: 12

Data (In Hex): 09 00 26 89 df d6 b7 12

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 00

Payload Length: 20

Data (In Hex):

af ca d7 13 68 a1 f1 c9 6b 86 96 fc 77 57 01 00

Payload Vendor ID

Next Payload: NAT-D

Reserved: 00

Payload Length: 20

Data (In Hex):

90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f

Payload NAT-D

Next Payload: NAT-D

Reserved: 00

Payload Length: 24

Data:

01 98 6a ce 63 c9 1f 1b 2a 7b 6e bc 2d 84 38 90

3e 65 6c 49

Payload NAT-D

Next Payload: Vendor ID

Reserved: 00

Payload Length: 24

Data:

eb 80 2d 65 2f e0 45 a8 b4 7e 2e 7a 33 b6 0c c2

c0 01 ad 51

NAT Discovery hashes (NAT-D payload) that enable the peer to discover the NAT enabled across the network.

Payload Vendor ID
Next Payload: Vendor ID
Reserved: 00
Payload Length: 24
Data (In Hex):
40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
c0 00 00 00

Payload Vendor ID
Next Payload: None
Reserved: 00
Payload Length: 20
Data (In Hex):
1f 07 f7 0e aa 65 14 d3 b0 fa 96 54 2a 50 01 00

3: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500: udp 132

ISAKMP Header
Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Hash
Version: 1.0
Exchange Type: Aggressive Mode
Flags: (Encryption)
MessageID: 00000000
Length: 132

4: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500: udp 132

ISAKMP Header
Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Hash
Version: 1.0
Exchange Type: Aggressive Mode
Flags: (none)
MessageID: 00000000
Length: 132
Payload Hash
Next Payload: NAT-D
Reserved: 00
Payload Length: 24
Data:
a4 66 61 29 f9 a5 26 66 19 00 a4 a1 9c 7f a0 9d
b1 3b 59 60
Payload NAT-D
Next Payload: NAT-D
Reserved: 00
Payload Length: 24
Data:
eb 80 2d 65 2f e0 45 a8 b4 7e 2e 7a 33 b6 0c c2

```
c0 01 ad 51
Payload NAT-D
  Next Payload: Notification
  Reserved: 00
  Payload Length: 24
  Data:
    01 98 6a ce 63 c9 1f 1b 2a 7b 6e bc 2d 84 38 90
    3e 65 6c 49
Payload Notification
  Next Payload: None
  Reserved: 00
  Payload Length: 28
  DOI: IPsec
  Protocol-ID: PROTO_ISAKMP
  Spi Size: 16
  Notify Type: STATUS_INITIAL_CONTACT
  SPI:
    78 3b 9b ea 4d 01 0b 3f dc 15 82 8e fd f2 7f b7
Extra data: 00 00 00 00
```

5: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500: udp 388

```
ISAKMP Header
  Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
  Responder COOKIE: dc 15 82 8e fd f2 7f b7
  Next Payload: Hash
  Version: 1.0
  Exchange Type: Transaction
  Flags: (Encryption)
  MessageID: 021567B1
  Length: 388
```

Third packet is the last one for Aggressive Mode, but in this case there is an EasyVPN feature which requires Mode Config for the client. Note that config request is sent (required) from the client side.

6: 06:37:20.47184320 10.1.105.5.500 > 192.168.1.10.500: udp 388

```
ISAKMP Header
  Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
  Responder COOKIE: dc 15 82 8e fd f2 7f b7
  Next Payload: Hash
  Version: 1.0
  Exchange Type: Transaction
  Flags: (none)
  MessageID: 021567B1
  Length: 388
  Payload Hash
  Next Payload: Attributes
  Reserved: 00
  Payload Length: 24
  Data:
    5d 28 f7 ad fd 6d ac 4a dc 47 94 b5 76 98 ec 3e
```



```

07 c8 b8 20
Payload Attributes
Next Payload: None
Reserved: 00
Payload Length: 328
type: ISAKMP_CFG_REQUEST
Reserved: 00
Identifier: 0000
Unknown: (empty)
Unknown: (empty)
IPv4 DNS: (empty)
IPv4 DNS: (empty)
IPv4 NBNS (WINS): (empty)
IPv4 NBNS (WINS): (empty)
Cisco extension: Split Include: (empty)
Cisco extension: Split DNS Name: (empty)
Cisco extension: Default Domain Name: (empty)
Cisco extension: Save PWD: (empty)
Cisco extension: Include Local LAN: (empty)
Cisco extension: Do PFS: (empty)
Cisco extension: Backup Servers: (empty)
Application Version:
43 69 73 63 6f 20 49 4f 53 20 53 6f 66 74 77 61
72 65 2c 20 32 38 30 30 20 53 6f 66 74 77 61 72
65 20 28 43 32 38 30 30 4e 4d 2d 41 44 56 45 4e
54 45 52 50 52 49 53 45 4b 39 2d 4d 29 2c 20 56
65 72 73 69 6f 6e 20 31 32 2e 34 28 32 34 29 54
32 2c 20 52 45 4c 45 41 53 45 20 53 4f 46 54 57
41 52 45 20 28 66 63 32 29 0a 54 65 63 68 6e 69
63 61 6c 20 53 75 70 70 6f 72 74 3a 20 68 74 74
70 3a 2f 2f 77 77 77 2e 63 69 73 63 6f 2e 63 6f
6d 2f 74 65 63 68 73 75 70 70 6f 72 74 0a 43 6f
70 79 72 69 67 68 74 20 28 63 29 20 31 39 38 36
2d 32 30 30 39 20 62 79 20 43 69 73 63 6f 20 53
79 73 74 65 6d 73 2c 20 49 6e 63 2e 0a 43 6f 6d
70 69 6c 65 64 20 4d 6f 6e 20 31 39 2d 4f 63 74
2d 30 39 20 31 37 3a 33 38 20 62 79 20 70 72 6f
64 5f 72 65 6c 5f 74 65 61 6d
Cisco extension: Banner: (empty)
Unknown: (empty)
Cisco extension: Dynamic DNS Hostname: 52 35
Extra data: 00 00 00 00 00 00 00 00

```

Server agrees that it supports Client Mode Config and sends out all Mode Config information it has.

```

7: 06:37:20.47184320 192.168.1.10.500 > 10.1.105.5.500:  udp 172
ISAKMP Header
Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Hash

```

```
Version: 1.0
Exchange Type: Transaction
Flags: (none)
MessageID: 021567B1
Length: 172
Payload Hash
  Next Payload: Attributes
  Reserved: 00
  Payload Length: 24
  Data:
    73 24 60 32 dc 32 33 0c 8f a3 57 1a 98 65 a6 b0
    ae 5f b0 ad
```

Payload Attributes

```
  Next Payload: None
  Reserved: 00
  Payload Length: 120
  type: ISAKMP_CFG_REPLY
  Reserved: 00
  Identifier: 0000
  Cisco extension: Save PWD: No
  Cisco extension: Split Include: 1.1.1.0/255.255.255.0/0/0/0
  Cisco extension: Do PFS: No
  Application Version:
    43 69 73 63 6f 20 53 79 73 74 65 6d 73 2c 20 49
    6e 63 20 41 53 41 35 35 31 30 20 56 65 72 73 69
    6f 6e 20 38 2e 32 28 31 29 20 62 75 69 6c 74 20
    62 79 20 62 75 69 6c 64 65 72 73 20 6f 6e 20 54
    75 65 20 30 35 2d 4d 61 79 2d 30 39 20 32 32 3a
    34 35
```

8: 06:37:20.47184320 192.168.1.10.500 > 10.1.105.5.500: udp 172

ISAKMP Header

```
  Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
  Responder COOKIE: dc 15 82 8e fd f2 7f b7
  Next Payload: Hash
  Version: 1.0
  Exchange Type: Transaction
  Flags: (Encryption)
  MessageID: 021567B1
  Length: 172
```

9: 06:37:20.47184350 10.1.105.5.500 > 192.168.1.10.500: udp 1284

ISAKMP Header

```
  Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
  Responder COOKIE: dc 15 82 8e fd f2 7f b7
  Next Payload: Hash
  Version: 1.0
  Exchange Type: Quick Mode
  Flags: (Encryption)
  MessageID: 1D0E05C1
  Length: 1284
```

10: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500: udp 92

ISAKMP Header

Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f

Responder COOKIE: dc 15 82 8e fd f2 7f b7

Next Payload: Hash

Version: 1.0

Exchange Type: Informational

Flags: (none)

MessageID: 8BA99D99

Length: 92

Payload Hash

Next Payload: Notification

Reserved: 00

Payload Length: 24

Data:

1b f2 17 e7 41 11 d2 1f 91 6a c1 90 07 3e 80 65

61 08 64 3c

Payload Notification

Next Payload: None

Reserved: 00

Payload Length: 40

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

Notify Type: STATUS_RESP_LIFETIME

SPI:

78 3b 9b ea 4d 01 0b 3f dc 15 82 8e fd f2 7f b7

Data: 80 0b 00 01 00 0c 00 04 00 01 51 80

11: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500: udp 92

ISAKMP Header

Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f

Responder COOKIE: dc 15 82 8e fd f2 7f b7

Next Payload: Hash

Version: 1.0

Exchange Type: Informational

Flags: (Encryption)

MessageID: 8BA99D99

Length: 92

Here IKE Phase 2 (Quick Mode) starts. Client sends out his SA proposals and Proxy IDs.

12: 06:37:20.47184350 10.1.105.5.500 > 192.168.1.10.500: udp 1284

ISAKMP Header

Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f

Responder COOKIE: dc 15 82 8e fd f2 7f b7

Next Payload: Hash

Version: 1.0

Exchange Type: Quick Mode

Flags: (none)
MessageID: 1D0E05C1
Length: 1284
Payload Hash
Next Payload: Security Association
Reserved: 00
Payload Length: 24
Data:
d9 5e e8 91 75 de f9 af 31 24 e1 12 5f de 51 8c
dd 6f d2 88

Payload Security Association

Next Payload: Nonce
Reserved: 00
Payload Length: 1172
DOI: IPsec
Situation: (SIT_IDENTITY_ONLY)
Payload Proposal
Next Payload: Proposal
Reserved: 00
Payload Length: 56
Proposal #: 1
Protocol-Id: PROTO_IPSEC_ESP
SPI Size: 4
of transforms: 1
SPI: 56 7c 92 a4
Payload Transform
Next Payload: None
Reserved: 00
Payload Length: 44
Transform #: 1
Transform-Id: ESP_AES
Reserved2: 0000
Encapsulation Mode: Tunnel
Life Type: Seconds
Life Duration (Hex): 00 20 c4 9b
Life Type: Kilobytes
Life Duration (Hex): 00 46 50 00
Authentication Algorithm: SHA1
Key Length: 128

Payload Proposal
Next Payload: Proposal
Reserved: 00
Payload Length: 56
Proposal #: 2
Protocol-Id: PROTO_IPSEC_ESP
SPI Size: 4
of transforms: 1
SPI: 31 73 c5 d0
Payload Transform
Next Payload: None
Reserved: 00

Payload Length: 44
Transform #: 1
Transform-Id: ESP_AES
Reserved2: 0000
Encapsulation Mode: Tunnel
Life Type: Seconds
Life Duration (Hex): 00 20 c4 9b
Life Type: Kilobytes
Life Duration (Hex): 00 46 50 00
Authentication Algorithm: MD5
Key Length: 128

Payload Proposal

Next Payload: Proposal
Reserved: 00
Payload Length: 56
Proposal #: 3
Protocol-Id: PROTO_IPSEC_ESP
SPI Size: 4
of transforms: 1
SPI: ce 71 a8 5c

Payload Transform

Next Payload: None
Reserved: 00
Payload Length: 44
Transform #: 1
Transform-Id: ESP_AES
Reserved2: 0000
Encapsulation Mode: Tunnel
Life Type: Seconds
Life Duration (Hex): 00 20 c4 9b
Life Type: Kilobytes
Life Duration (Hex): 00 46 50 00
Authentication Algorithm: SHA1
Key Length: 128

Payload Proposal

Next Payload: Proposal
Reserved: 00
Payload Length: 48
Proposal #: 3
Protocol-Id: PROTO_IPSEC_IPCOMP
SPI Size: 4
of transforms: 1
SPI: 00 00 4b ff

Payload Transform

Next Payload: None
Reserved: 00
Payload Length: 36
Transform #: 1
Transform-Id: IPCOMP_LZS
Reserved2: 0000
Encapsulation Mode: Tunnel

```
    Life Type: Seconds
    Life Duration (Hex): 00 20 c4 9b
    Life Type: Kilobytes
    Life Duration (Hex): 00 46 50 00
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 56
  Proposal #: 4
  Protocol-Id: PROTO_IPSEC_ESP
  SPI Size: 4
  # of transforms: 1
  SPI: bd dc b8 ab
  Payload Transform
    Next Payload: None
    Reserved: 00
    Payload Length: 44
    Transform #: 1
    Transform-Id: ESP_AES
    Reserved2: 0000
    Encapsulation Mode: Tunnel
    Life Type: Seconds
    Life Duration (Hex): 00 20 c4 9b
    Life Type: Kilobytes
    Life Duration (Hex): 00 46 50 00
    Authentication Algorithm: MD5
    Key Length: 128
  Payload Proposal
    Next Payload: Proposal
    Reserved: 00
    Payload Length: 48
    Proposal #: 4
    Protocol-Id: PROTO_IPSEC_IPCOMP
    SPI Size: 4
    # of transforms: 1
    SPI: 00 00 fe 00
    Payload Transform
      Next Payload: None
      Reserved: 00
      Payload Length: 36
      Transform #: 1
      Transform-Id: IPCOMP_LZS
      Reserved2: 0000
      Encapsulation Mode: Tunnel
      Life Type: Seconds
      Life Duration (Hex): 00 20 c4 9b
      Life Type: Kilobytes
      Life Duration (Hex): 00 46 50 00
    Payload Proposal
      Next Payload: Proposal
      Reserved: 00
```

Payload Length: 56
Proposal #: 5
Protocol-Id: PROTO_IPSEC_ESP
SPI Size: 4
of transforms: 1
SPI: 35 06 a3 cb
Payload Transform
 Next Payload: None
 Reserved: 00
 Payload Length: 44
 Transform #: 1
 Transform-Id: ESP_AES
 Reserved2: 0000
 Encapsulation Mode: Tunnel
 Life Type: Seconds
 Life Duration (Hex): 00 20 c4 9b
 Life Type: Kilobytes
 Life Duration (Hex): 00 46 50 00
 Authentication Algorithm: SHA1
 Key Length: 192
Payload Proposal
 Next Payload: Proposal
 Reserved: 00
 Payload Length: 56
 Proposal #: 6
 Protocol-Id: PROTO_IPSEC_ESP
 SPI Size: 4
 # of transforms: 1
 SPI: 90 2c 99 79
 Payload Transform
 Next Payload: None
 Reserved: 00
 Payload Length: 44
 Transform #: 1
 Transform-Id: ESP_AES
 Reserved2: 0000
 Encapsulation Mode: Tunnel
 Life Type: Seconds
 Life Duration (Hex): 00 20 c4 9b
 Life Type: Kilobytes
 Life Duration (Hex): 00 46 50 00
 Authentication Algorithm: MD5
 Key Length: 192
Payload Proposal
 Next Payload: Proposal
 Reserved: 00
 Payload Length: 56
 Proposal #: 7
 Protocol-Id: PROTO_IPSEC_ESP
 SPI Size: 4
 # of transforms: 1

SPI: de 82 91 dd
Payload Transform
 Next Payload: None
 Reserved: 00
 Payload Length: 44
 Transform #: 1
 Transform-Id: ESP_AES
 Reserved2: 0000
 Encapsulation Mode: Tunnel
 Life Type: Seconds
 Life Duration (Hex): 00 20 c4 9b
 Life Type: Kilobytes
 Life Duration (Hex): 00 46 50 00
 Authentication Algorithm: SHA1
 Key Length: 256
Payload Proposal
 Next Payload: Proposal
 Reserved: 00
 Payload Length: 56
 Proposal #: 8
 Protocol-Id: PROTO_IPSEC_ESP
 SPI Size: 4
 # of transforms: 1
 SPI: 03 de d8 0a
 Payload Transform
 Next Payload: None
 Reserved: 00
 Payload Length: 44
 Transform #: 1
 Transform-Id: ESP_AES
 Reserved2: 0000
 Encapsulation Mode: Tunnel
 Life Type: Seconds
 Life Duration (Hex): 00 20 c4 9b
 Life Type: Kilobytes
 Life Duration (Hex): 00 46 50 00
 Authentication Algorithm: MD5
 Key Length: 256
 Payload Proposal
 Next Payload: Proposal
 Reserved: 00
 Payload Length: 56
 Proposal #: 9
 Protocol-Id: PROTO_IPSEC_ESP
 SPI Size: 4
 # of transforms: 1
 SPI: 40 54 5e 23
 Payload Transform
 Next Payload: None
 Reserved: 00
 Payload Length: 44


```
    Transform #: 1
    Transform-Id: ESP_AES
    Reserved2: 0000
    Encapsulation Mode: Tunnel
    Life Type: Seconds
    Life Duration (Hex): 00 20 c4 9b
    Life Type: Kilobytes
    Life Duration (Hex): 00 46 50 00
    Authentication Algorithm: SHA1
    Key Length: 256
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 48
  Proposal #: 9
  Protocol-Id: PROTO_IPSEC_IPCOMP
  SPI Size: 4
  # of transforms: 1
  SPI: 00 00 81 e8
Payload Transform
  Next Payload: None
  Reserved: 00
  Payload Length: 36
  Transform #: 1
  Transform-Id: IPCOMP_LZS
  Reserved2: 0000
  Encapsulation Mode: Tunnel
  Life Type: Seconds
  Life Duration (Hex): 00 20 c4 9b
  Life Type: Kilobytes
  Life Duration (Hex): 00 46 50 00
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 56
  Proposal #: 10
  Protocol-Id: PROTO_IPSEC_ESP
  SPI Size: 4
  # of transforms: 1
  SPI: 3f 55 57 df
Payload Transform
  Next Payload: None
  Reserved: 00
  Payload Length: 44
  Transform #: 1
  Transform-Id: ESP_AES
  Reserved2: 0000
  Encapsulation Mode: Tunnel
  Life Type: Seconds
  Life Duration (Hex): 00 20 c4 9b
  Life Type: Kilobytes
```

```
    Life Duration (Hex): 00 46 50 00
    Authentication Algorithm: MD5
    Key Length: 256
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 48
  Proposal #: 10
  Protocol-Id: PROTO_IPSEC_IPCOMP
  SPI Size: 4
  # of transforms: 1
  SPI: 00 00 d8 81
  Payload Transform
    Next Payload: None
    Reserved: 00
    Payload Length: 36
    Transform #: 1
    Transform-Id: IPCOMP_LZS
    Reserved2: 0000
    Encapsulation Mode: Tunnel
    Life Type: Seconds
    Life Duration (Hex): 00 20 c4 9b
    Life Type: Kilobytes
    Life Duration (Hex): 00 46 50 00
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 52
  Proposal #: 11
  Protocol-Id: PROTO_IPSEC_ESP
  SPI Size: 4
  # of transforms: 1
  SPI: e8 49 67 0b
  Payload Transform
    Next Payload: None
    Reserved: 00
    Payload Length: 40
    Transform #: 1
    Transform-Id: ESP_3DES
    Reserved2: 0000
    Encapsulation Mode: Tunnel
    Life Type: Seconds
    Life Duration (Hex): 00 20 c4 9b
    Life Type: Kilobytes
    Life Duration (Hex): 00 46 50 00
    Authentication Algorithm: SHA1
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 52
  Proposal #: 12
```

```
Protocol-Id: PROTO_IPSEC_ESP
SPI Size: 4
# of transforms: 1
SPI: ac 85 7d 5f
Payload Transform
  Next Payload: None
  Reserved: 00
  Payload Length: 40
  Transform #: 1
  Transform-Id: ESP_3DES
  Reserved2: 0000
  Encapsulation Mode: Tunnel
  Life Type: Seconds
  Life Duration (Hex): 00 20 c4 9b
  Life Type: Kilobytes
  Life Duration (Hex): 00 46 50 00
  Authentication Algorithm: MD5
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 52
  Proposal #: 13
  Protocol-Id: PROTO_IPSEC_ESP
  SPI Size: 4
  # of transforms: 1
  SPI: 06 32 54 41
  Payload Transform
    Next Payload: None
    Reserved: 00
    Payload Length: 40
    Transform #: 1
    Transform-Id: ESP_3DES
    Reserved2: 0000
    Encapsulation Mode: Tunnel
    Life Type: Seconds
    Life Duration (Hex): 00 20 c4 9b
    Life Type: Kilobytes
    Life Duration (Hex): 00 46 50 00
    Authentication Algorithm: SHA1
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 48
  Proposal #: 13
  Protocol-Id: PROTO_IPSEC_IPCOMP
  SPI Size: 4
  # of transforms: 1
  SPI: 00 00 74 a5
  Payload Transform
    Next Payload: None
    Reserved: 00
```

```
Payload Length: 36
Transform #: 1
Transform-Id: IPCOMP_LZS
Reserved2: 0000
Encapsulation Mode: Tunnel
Life Type: Seconds
Life Duration (Hex): 00 20 c4 9b
Life Type: Kilobytes
Life Duration (Hex): 00 46 50 00
Payload Proposal
Next Payload: Proposal
Reserved: 00
Payload Length: 52
Proposal #: 14
Protocol-Id: PROTO_IPSEC_ESP
SPI Size: 4
# of transforms: 1
SPI: e3 5b 48 e2
Payload Transform
Next Payload: None
Reserved: 00
Payload Length: 40
Transform #: 1
Transform-Id: ESP_3DES
Reserved2: 0000
Encapsulation Mode: Tunnel
Life Type: Seconds
Life Duration (Hex): 00 20 c4 9b
Life Type: Kilobytes
Life Duration (Hex): 00 46 50 00
Authentication Algorithm: MD5
Payload Proposal
Next Payload: Proposal
Reserved: 00
Payload Length: 48
Proposal #: 14
Protocol-Id: PROTO_IPSEC_IPCOMP
SPI Size: 4
# of transforms: 1
SPI: 00 00 5a c2
Payload Transform
Next Payload: None
Reserved: 00
Payload Length: 36
Transform #: 1
Transform-Id: IPCOMP_LZS
Reserved2: 0000
Encapsulation Mode: Tunnel
Life Type: Seconds
Life Duration (Hex): 00 20 c4 9b
Life Type: Kilobytes
```

```
    Life Duration (Hex): 00 46 50 00
Payload Proposal
  Next Payload: Proposal
  Reserved: 00
  Payload Length: 52
  Proposal #: 15
  Protocol-Id: PROTO_IPSEC_ESP
  SPI Size: 4
  # of transforms: 1
  SPI: 65 75 36 ff
Payload Transform
  Next Payload: None
  Reserved: 00
  Payload Length: 40
  Transform #: 1
  Transform-Id: ESP_DES
  Reserved2: 0000
  Encapsulation Mode: Tunnel
  Life Type: Seconds
  Life Duration (Hex): 00 20 c4 9b
  Life Type: Kilobytes
  Life Duration (Hex): 00 46 50 00
  Authentication Algorithm: SHA1
Payload Proposal
  Next Payload: None
  Reserved: 00
  Payload Length: 52
  Proposal #: 16
  Protocol-Id: PROTO_IPSEC_ESP
  SPI Size: 4
  # of transforms: 1
  SPI: c0 36 b5 6f
Payload Transform
  Next Payload: None
  Reserved: 00
  Payload Length: 40
  Transform #: 1
  Transform-Id: ESP_DES
  Reserved2: 0000
  Encapsulation Mode: Tunnel
  Life Type: Seconds
  Life Duration (Hex): 00 20 c4 9b
  Life Type: Kilobytes
  Life Duration (Hex): 00 46 50 00
  Authentication Algorithm: MD5
Payload Nonce
  Next Payload: Identification
  Reserved: 00
  Payload Length: 24
  Data:
    c9 9c 07 90 28 9c f0 c6 10 54 01 f2 0e fa ba 4e
```

```
37 74 0e 99
Payload Identification
  Next Payload: Identification
  Reserved: 00
  Payload Length: 16
  ID Type: IPv4 Subnet (4)
  Protocol ID (UDP/TCP, etc...): 0
  Port: 0
  ID Data: 5.5.5.0/255.255.255.0
Payload Identification
  Next Payload: None
  Reserved: 00
  Payload Length: 16
  ID Type: IPv4 Subnet (4)
  Protocol ID (UDP/TCP, etc...): 0
  Port: 0
  ID Data: 1.1.1.0/255.255.255.0
Extra data: 00 00 00 00
```

The EasyVPN Server responds with chosen SA proposal and it's Proxy IDs.

13: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500: udp 196

```
ISAKMP Header
  Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
  Responder COOKIE: dc 15 82 8e fd f2 7f b7
  Next Payload: Hash
  Version: 1.0
  Exchange Type: Quick Mode
  Flags: (none)
  MessageID: 1D0E05C1
  Length: 196
  Payload Hash
    Next Payload: Security Association
    Reserved: 00
    Payload Length: 24
    Data:
      d9 ac 1c 49 2b 2c 55 cc de a0 52 70 5e fc e7 53
      60 31 f3 88
  Payload Security Association
    Next Payload: Nonce
    Reserved: 00
    Payload Length: 64
    DOI: IPsec
    Situation: (SIT_IDENTITY_ONLY)
  Payload Proposal
    Next Payload: None
    Reserved: 00
    Payload Length: 52
    Proposal #: 1
    Protocol-Id: PROTO_IPSEC_ESP
    SPI Size: 4
```

```
# of transforms: 1
SPI: 59 08 47 15
Payload Transform
  Next Payload: None
  Reserved: 00
  Payload Length: 40
  Transform #: 1
  Transform-Id: ESP_3DES
  Reserved2: 0000
  Life Type: Seconds
  Life Duration (Hex): 00 20 c4 9b
  Life Type: Kilobytes
  Life Duration (Hex): 00 46 50 00
  Encapsulation Mode: Tunnel
  Authentication Algorithm: SHA1
Payload Nonce
  Next Payload: Identification
  Reserved: 00
  Payload Length: 24
  Data:
    38 d5 0b 1f 1e c4 15 93 d2 ea 3c 96 ec 67 ef 28
    55 7f 97 6f
Payload Identification
  Next Payload: Identification
  Reserved: 00
  Payload Length: 16
  ID Type: IPv4 Subnet (4)
  Protocol ID (UDP/TCP, etc...): 0
  Port: 0
  ID Data: 5.5.5.0/255.255.255.0
Payload Identification
  Next Payload: Notification
  Reserved: 00
  Payload Length: 16
  ID Type: IPv4 Subnet (4)
  Protocol ID (UDP/TCP, etc...): 0
  Port: 0
  ID Data: 1.1.1.0/255.255.255.0
Payload Notification
  Next Payload: None
  Reserved: 00
  Payload Length: 24
  DOI: IPsec
  Protocol-ID: PROTO_IPSEC_ESP
  Spi Size: 4
  Notify Type: STATUS_RESP_LIFETIME
  SPI: 59 08 47 15
  Data: 80 01 00 01 80 02 70 80
```

14: 06:37:20.47184350 192.168.1.10.500 > 10.1.105.5.500: udp 196

ISAKMP Header

Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Hash
Version: 1.0
Exchange Type: Quick Mode
Flags: (Encryption)
MessageID: 1D0E05C1
Length: 196

15: 06:37:20.47184360 10.1.105.5.500 > 192.168.1.10.500: udp 60

ISAKMP Header

Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Hash
Version: 1.0
Exchange Type: Quick Mode
Flags: (Encryption)
MessageID: 1D0E05C1
Length: 60

16: 06:37:20.47184360 10.1.105.5.500 > 192.168.1.10.500: udp 60

ISAKMP Header

Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Hash
Version: 1.0
Exchange Type: Quick Mode
Flags: (none)
MessageID: 1D0E05C1
Length: 60

Payload Hash

Next Payload: None
Reserved: 00
Payload Length: 24
Data:

82 7a fe 77 fa 45 4d 45 68 1f c9 d4 3f 99 15 d6
b7 ba 07 53

Extra data: 00 00 00 00 00 00 00 00

17: 06:37:21.47185020 10.1.105.5.500 > 192.168.1.10.500: udp 212

ISAKMP Header

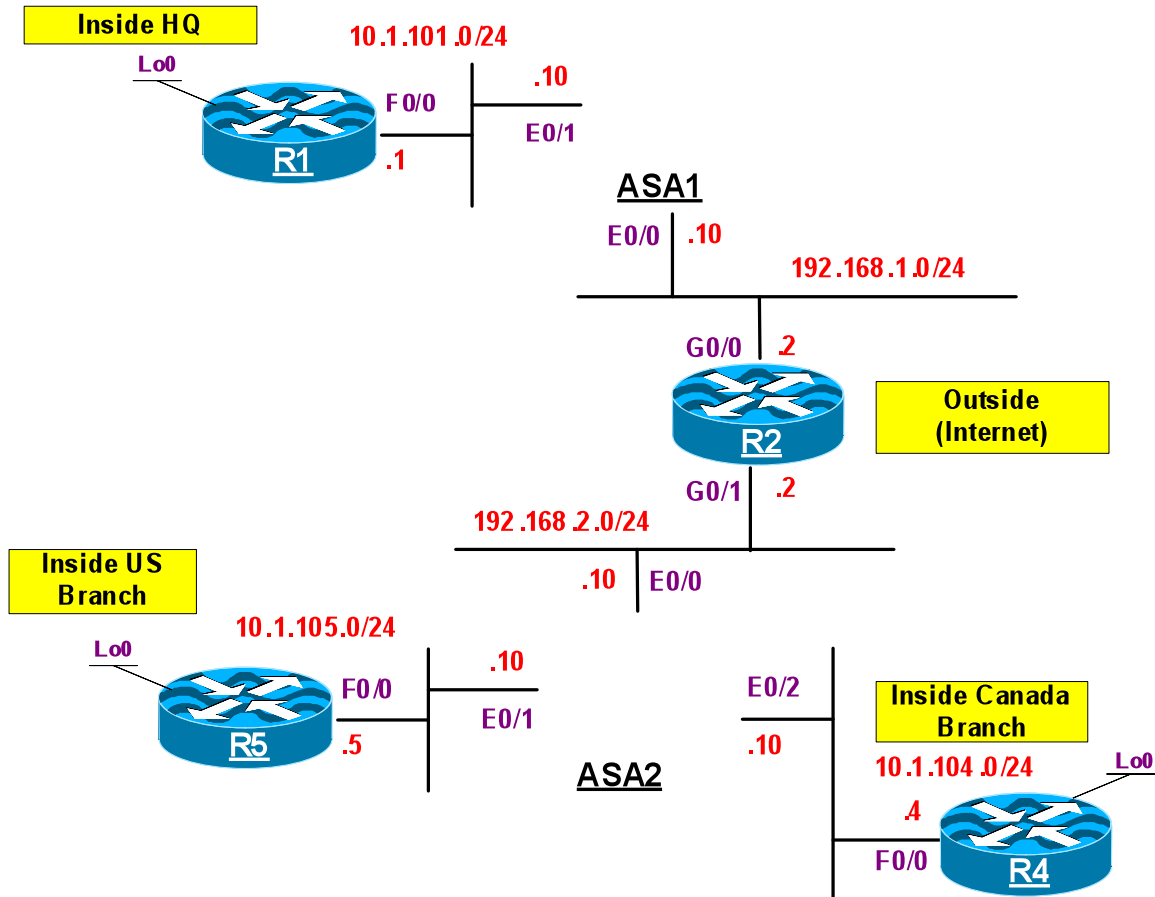
Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
Responder COOKIE: dc 15 82 8e fd f2 7f b7
Next Payload: Hash
Version: 1.0
Exchange Type: Informational
Flags: (Encryption)
MessageID: DD36CA24
Length: 212

18: 06:37:21.47185020 10.1.105.5.500 > 192.168.1.10.500: udp 212


```
ISAKMP Header
  Initiator COOKIE: 78 3b 9b ea 4d 01 0b 3f
  Responder COOKIE: dc 15 82 8e fd f2 7f b7
  Next Payload: Hash
  Version: 1.0
  Exchange Type: Informational
  Flags: (none)
  MessageID: DD36CA24
  Length: 212
  Payload Hash
    Next Payload: Notification
    Reserved: 00
    Payload Length: 24
    Data:
      0d 61 fc 2a 93 01 d7 a0 11 dd ce b5 67 69 6e 91
      60 cd 23 bb
  Payload Notification
    Next Payload: None
    Reserved: 00
    Payload Length: 153
    DOI: IPsec
    Protocol-ID: PROTO_ISAKMP
    Spi Size: 0
    Notify Type: Unknown
    Data:
      00 00 00 00 75 34 00 03 52 35 2e 75 32 00 0a 43
      69 73 63 6f 20 32 38 31 31 75 35 00 0b 46 48 4b
      30 38 34 39 46 31 42 41 75 30 00 09 32 35 37 35
      34 30 30 39 36 75 31 00 09 31 33 30 31 35 38 35
      39 32 75 36 00 09 32 32 38 35 38 39 35 36 38 75
      39 00 08 36 33 30 33 33 33 35 36 75 33 00 2e 66
      6c 61 73 68 3a 63 32 38 30 30 6e 6d 2d 61 64 76
      65 6e 74 65 72 70 72 69 73 65 6b 39 2d 6d 7a 2e
      31 32 34 2d 32 34 2e 54 32 2e 62 69 6e
  Extra data: 00 00 00 00 00 00 00 00
```

18 packets shown

Lab 1.47. Site-to-Site IPsec VPN using EasyVPN with ISAKMP Profiles (IOS-IOS)



This lab is based on previous labs configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"

- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure IPSec VPN tunnel between R5 and R4 with the following parameters:

Tunnel Endpoint	SRC Network	DST Network	ISAKMP Policy	IPSec Policy
R5 – R4	5.5.5.5	4.4.4.4	Authentication: PSK Encryption: 3DES Group: 2 Hash: SHA	Encryption: ESP/3DES Authentication: ESP/SHA

Use Easy VPN to configure the tunnel in network extension mode. R5 should act as EasyVPN Remote and R4 should be an EasyVPN Server. Use group name of "R5" with the password of "cisco123". You should use ISAKMP profile when configuring EasyVPN Server on R4.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#username student5 password student5
R4(config)#aaa new-model
R4(config)#aaa authorization network GROUP-AUTH local

R4(config)#crypto isakmp policy 1
R4(config-isakmp)#encr 3des
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#group 2
R4(config-isakmp)#exit

R4(config)#crypto isakmp client configuration group R5
R4(config-isakmp-group)#key cisco123
R4(config-isakmp-group)#exit

R4(config)#crypto isakmp profile VPN-CLIENTS
% A profile is deemed incomplete until it has match identity
statements
R4(conf-isa-prof)#match identity group R5
R4(conf-isa-prof)#isakmp authorization list GROUP-AUTH

    ISAKMP profile allows to specify an ISAKMP parameters when
    defined identity criteria are matched (e.g. group name, ip
    address, host name, host domain, user name and user
    domain). In this case, for any connection where the name of
    the group (R5) is used as the identity then configuration
    (authorization) for this connection will be processed
    locally from router's database.

R4(conf-isa-prof)#crypto ipsec transform-set TSET esp-3des esp-sha-
hmac

R4(cfg-crypto-trans)#crypto dynamic-map DYN-CMAP 10
R4(config-crypto-map)# set transform-set TSET
R4(config-crypto-map)# set isakmp-profile VPN-CLIENTS

R4(config)#crypto map ENCRYPT 10 ipsec-isakmp dynamic DYN-CMAP

R4(config)#int f0/0
R4(config-if)#crypto map ENCRYPT
R4(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Step 2 R5 configuration.

```
R5(config)#crypto ipsec client ezvpn EZ
R5(config-crypto-ezvpn)#connect auto
R5(config-crypto-ezvpn)#group R5 key cisco123
R5(config-crypto-ezvpn)#mode network-extension
R5(config-crypto-ezvpn)#peer 10.1.104.4

R5(config-crypto-ezvpn)#int f0/0
R5(config-if)# crypto ipsec client ezvpn EZ outside

R5(config-if)#int lo0
R5(config-if)# crypto ipsec client ezvpn EZ inside
R5(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client)  User=  Group=R5
Client_public_addr=10.1.105.5  Server_public_addr=10.1.104.4
NEM_Remote_Subnets=5.5.5.0/255.255.255.0
```

Step 3 ASA2 configuration.

Since IPSec tunnel needs to be established between two peers who are on different interfaces of ASA but with the same security level of 100. This must be explicitly allowed on ASA.

```
ASA2(config)# same-security-traffic permit inter-interface
```

Verification

R5#ping 4.4.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 5.5.5.5

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R5#sh crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

Tunnel name : EZ

Inside interface list: Loopback0

Outside interface: FastEthernet0/0

Current State: IPSEC_ACTIVE

Last Event: MTU_CHANGED

Save Password: Disallowed

Current EzVPN Peer: 10.1.104.4

R5#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.105.5	10.1.104.4		ACTIVE	3des	sha	psk	2	23:56:41	C
Engine-id:Conn-id = SW:1										

IPv6 Crypto ISAKMP SA

R5#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.105.5

protected vrf: (none)

local ident (addr/mask/prot/port): (5.5.5.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 10.1.104.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 10.1.104.4

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xD4F8B509(3573069065)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xD5881B72(3582466930)

transform: esp-3des esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map:

FastEthernet0/0-head-0

sa timing: remaining key lifetime (k/sec): (4448645/3441)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

```

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xD4F8B509(3573069065)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4448645/3441)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

R4#ping 5.5.5.5 so 100

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

```

R4#sh crypto isakmp sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
-----
1001  10.1.104.4        10.1.105.5          ACTIVE 3des sha psk 2  23:57:04 C
      Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

```

R4#sh crypto ipsec sa

```

interface: FastEthernet0/0
  Crypto map tag: ENCRYPT, local addr 10.1.104.4

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (5.5.5.0/255.255.255.0/0/0)

```

```
current_peer 10.1.105.5 port 500
  PERMIT, flags={}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.104.4, remote crypto endpt.: 10.1.105.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xD5881B72(3582466930)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xD4F8B509(3573069065)
    transform: esp-3des esp-sha-hmac ,
    in use settings = {Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4485964/3420)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xD5881B72(3582466930)
    transform: esp-3des esp-sha-hmac ,
    in use settings = {Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: ENCRYPT
    sa timing: remaining key lifetime (k/sec): (4485964/3420)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Verification (detailed)

```
R4#deb cry isak
Crypto ISAKMP debugging is on
R4#
ISAKMP (0): received packet from 10.1.105.5 dport 500 sport 500 Global (N) NEW SA
ISAKMP: Created a peer struct for 10.1.105.5, peer port 500
ISAKMP: New peer created peer = 0x4A0B08AC peer_handle = 0x80000002
```



```
ISAKMP: Locking peer struct 0x4A0B08AC, refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500
ISAKMP:(0):insert sa successfully sa = 499D5A4C
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing ID payload. message ID = 0
ISAKMP (0): ID payload
    next-payload : 13
    type          : 11
    group id      : R5
    protocol      : 17
    port          : 0
    length        : 10
```

The group name has been sent by the client as the identity.

```
ISAKMP:(0):: peer matches VPN-CLIENTS profile
```

The ISAKMP profile criteria has matched.

```
ISAKMP:(0):Setting client config settings 499D4FAC
ISAKMP/xauth: initializing AAA request
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/D
R4#PD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP : Looking for xauth in profile VPN-CLIENTS
ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 128
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 2 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 128
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
```

```
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 192
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 4 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 192
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 5 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 256
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 6 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 256
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 7 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 128
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
```

```
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 8 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 128
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 9 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 192
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 10 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 192
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 11 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 256
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 12 against priority 1 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      keylength of 256
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
```

```
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 13 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Xauth authentication by pre-shared key offered but does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 14 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Hash algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 15 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 16 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth XAUTHInitPreShared
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):Encryption algorithm offered does not match policy!
ISAKMP:(0):atts are not acceptable. Next payload is 3
ISAKMP:(0):Checking ISAKMP transform 17 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:(0):atts are acceptable. Next payload is 3
ISAKMP:(0):Acceptable atts:actual life: 86400
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:2147483
ISAKMP:(0):Returning Actual lifetime: 86400
```

```
ISAKMP:(0)::Started lifetime timer: 86400.

ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID is DPD
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 221 mismatch
ISAKMP:(0): vendor ID is XAUTH
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): claimed IOS but failed authentication
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID is Unity
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
ISAKMP:(0):Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

ISAKMP:(1001): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(1001):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1001): ID payload
    next-payload : 10
    type          : 1
    address       : 10.1.104.4
    protocol      : 0
    port          : 0
    length        : 12
ISAKMP:(1001):Total payload length: 12
ISAKMP:(1001): sending packet to 10.1.105.5 my_port 500 peer_port 500 (R) AG_INIT_EXCH
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
ISAKMP:(1001):Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

ISAKMP (1001): received packet from 10.1.105.5 dport 500 sport 500 Global (R)
AG_INIT_EXCH
ISAKMP:(1001): processing HASH payload. message ID = 0
ISAKMP:received payload type 20
ISAKMP (1001): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1001): No NAT Found for self or peer
ISAKMP:(1001): processing NOTIFY INITIAL_CONTACT protocol 1
```

```
spi 0, message ID = 0, sa = 499D5A4C
ISAKMP:(1001):SA authentication status:
    authenticated
ISAKMP:(1001):SA has been authenticated with 10.1.105.5
ISAKMP:(1001):SA authentication status:
    authenticated
ISAKMP:(1001): Process initial contact,
bring down existing phase 1 and 2 SA's with local 10.1.104.4 remote 10.1.105.5 remote
port 500
ISAKMP:(1001):returning IP addr to the address pool
ISAKMP: Trying to insert a peer 10.1.104.4/10.1.105.5/500/, and inserted successfully
4A0B08AC.
ISAKMP:(1001):Returning Actual lifetime: 86400
ISAKMP: set new node 1434551794 to QM_IDLE
ISAKMP:(1001):Sending NOTIFY RESPONDER_LIFETIME protocol 1
    spi 1234317488, message ID = 1434551794
ISAKMP:(1001): sending packet to 10.1.105.5 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):purging node 1434551794
ISAKMP: Sending phase 1 responder lifetime 86400

ISAKMP:(1001):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP:(1001):Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

ISAKMP (1001): received packet from 10.1.105.5 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP: set new node 793798316 to QM_IDLE
ISAKMP:(1001):processing transaction payload from 10.1.105.5. message ID = 793798316
ISAKMP: Config payload REQUEST
ISAKMP:(1001):checking request:
ISAKMP:  MODECFG_CONFIG_URL
ISAKMP:  MODECFG_CONFIG_VERSION
ISAKMP:  IP4_DNS
ISAKMP:  IP4_DNS
ISAKMP:  IP4_NBNS
ISAKMP:  IP4_NBNS
ISAKMP:  SPLIT_INCLUDE
ISAKMP:  SPLIT_DNS
ISAKMP:  DEFAULT_DOMAIN
ISAKMP:  MODECFG_SAVEPWD
ISAKMP:  INCLUDE_LOCAL_LAN
ISAKMP:  PFS
ISAKMP:  BACKUP_SERVER
ISAKMP:  APPLICATION_VERSION
ISAKMP:  MODECFG_BANNER
ISAKMP:  MODECFG_IPSEC_INT_CONF
ISAKMP:  MODECFG_HOSTNAME
```

The client has requested several parameters.

ISAKMP/author: Author request for group R5successfully sent to AAA

The client request has been directed to the router's AAA process in accordance with AAA authorization list configured in the ISAKMP profile.

```
ISAKMP:(1001):Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
ISAKMP:(1001):Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

ISAKMP:(1001):Receive config attributes requested but config attributes not in crypto
map. Sending empty reply.
ISAKMP:(1001):attributes sent in message:
ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software, 2800 Software (C2800NM-
ADVENTERPRISEK9-M), Version 12.4(24)T2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 19-Oct-09 17:38 by prod_rel_team
ISAKMP: Sending IPsec Interface Config reply value 0
ISAKMP (1001): Unknown Attr: MODECFG_HOSTNAME (0x700A)
ISAKMP:(1001): responding to peer config from 10.1.105.5. ID = 793798316
ISAKMP: Marking node 793798316 for late deletion
ISAKMP:(1001): sending packet to 10.1.105.5 my_port 500 peer_port 500 (R) CONF_ADDR
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Talking to a Unity Client
ISAKMP:(1001):Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
ISAKMP:(1001):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

ISAKMP:FSM error - Message from AAA grp/user.

ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1001):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP:(1001):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1001):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (1001): received packet from 10.1.105.5 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP: set new node -618165756 to QM_IDLE
ISAKMP:(1001): processing HASH payload. message ID = -618165756
ISAKMP:(1001): processing SA payload. message ID = -618165756
ISAKMP:(1001):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1 (Tunnel)
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-SHA
ISAKMP: key length is 128
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPsec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 2
ISAKMP: transform 1, ESP_AES
ISAKMP: attributes in transform:
```

```
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      key length is 128
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 3
ISAKMP: transform 1, ESP_AES
ISAKMP:  attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      key length is 128
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001):Checking IPSec proposal 3
ISAKMP:(1001):transform 1, IPPCP LZS
ISAKMP:  attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 4
ISAKMP: transform 1, ESP_AES
ISAKMP:  attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      key length is 128
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001):Checking IPSec proposal 4
ISAKMP:(1001):transform 1, IPPCP LZS
ISAKMP:  attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
```



```
ISAKMP:(1001):Checking IPSec proposal 5
ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-SHA
ISAKMP:     key length is 192
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 6
ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:     key length is 192
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 7
ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-SHA
ISAKMP:     key length is 256
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 8
ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:     key length is 256
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 9
ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
```

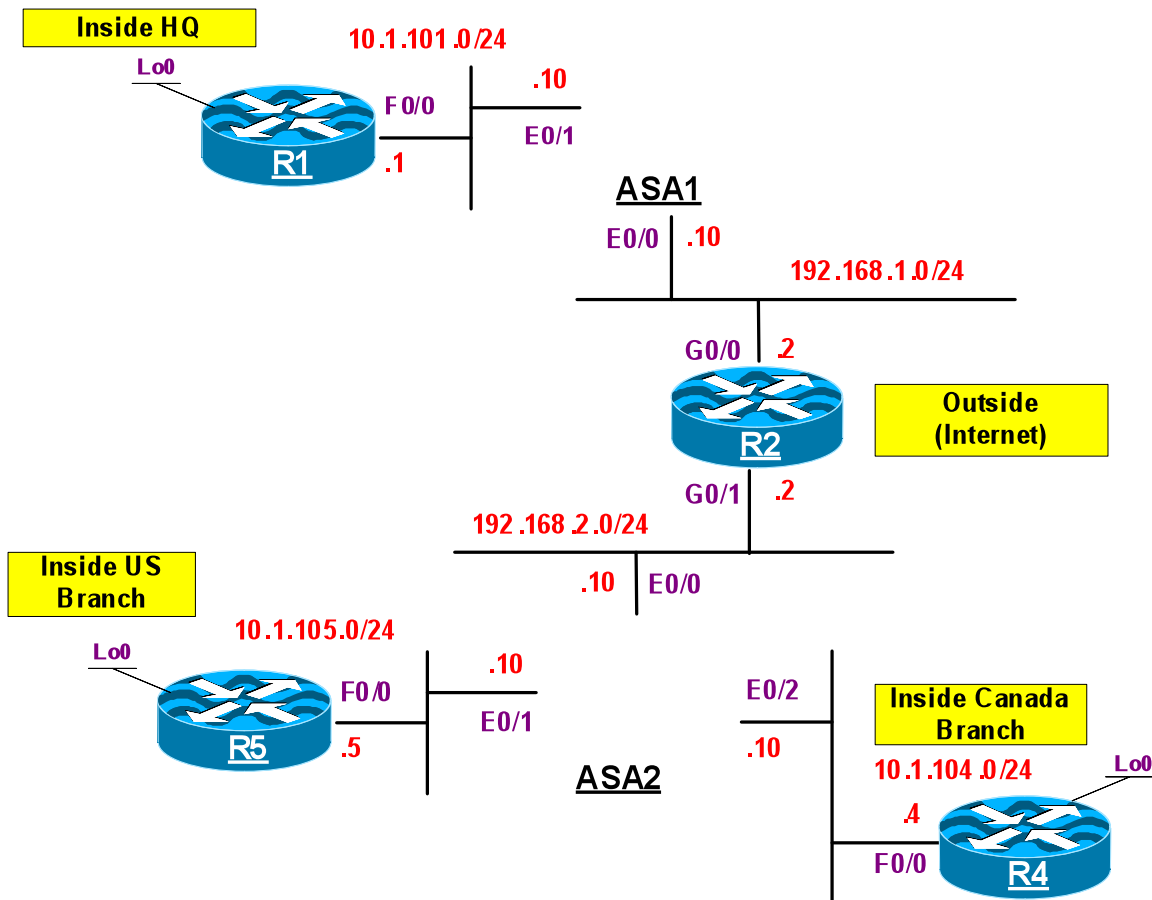
```
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      key length is 256
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001):Checking IPSec proposal 9
ISAKMP:(1001):transform 1, IPPCP LZS
ISAKMP:      attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 10
ISAKMP: transform 1, ESP_AES
ISAKMP:      attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      key length is 256
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001):Checking IPSec proposal 10
ISAKMP:(1001):transform 1, IPPCP LZS
ISAKMP:      attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:(1001):atts are acceptable.
ISAKMP:(1001): IPSec policy invalidated proposal with error 256
ISAKMP:(1001):Checking IPSec proposal 11
ISAKMP: transform 1, ESP_3DES
ISAKMP:      attributes in transform:
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:(1001):atts are acceptable.
```

Negotiating of IPSec transform-sets (hardcoded in the client software).

```
ISAKMP:(1001): processing NONCE payload. message ID = -618165756
ISAKMP:(1001): processing ID payload. message ID = -618165756
ISAKMP:(1001): processing ID payload. message ID = -618165756
ISAKMP:(1001):QM Responder gets spi
ISAKMP:(1001):Node -618165756, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1001):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
ISAKMP:(1001):deleting node 793798316 error FALSE reason "No Error"
ISAKMP:(1001): Creating IPSec SAs
    inbound SA from 10.1.105.5 to 10.1.104.4 (f/i) 0/0
    (proxy 5.5.5.0 to 0.0.0.0)
    has spi 0xD4F8B509 and conn_id 0
    lifetime of 2147483 seconds
    lifetime of 4608000 kilobytes
    outbound SA from 10.1.104.4 to 10.1.105.5 (f/i) 0/0
    (proxy 0.0.0.0 to 5.5.5.0)
    has spi 0xD5881B72 and conn_id 0
    lifetime of 2147483 seconds
    lifetime of 4608000 kilobytes
ISAKMP:(1001): sending packet to 10.1.105.5 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP:(1001):Sending an IKE IPv4 Packet.
ISAKMP:(1001):Node -618165756, Input = IKE_MSG_INTERNAL, IKE_GOT_SPI
ISAKMP:(1001):Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
ISAKMP (1001): received packet from 10.1.105.5 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP:(1001):deleting node -618165756 error FALSE reason "QM done (await)"
ISAKMP:(1001):Node -618165756, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1001):Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

R4#un all
```

Lab 1.48. GRE over IPSec



This lab is based on previous labs configuration. You need to perform actions from Task 1 (IOS CA configuration) and Task 2 (NTP configuration) before going through this lab.

Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface

- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure GRE tunnel between R5 and R4. The tunnel should pass EIGRP AS 34 multicast packets exchanging information about Loopback0 networks. Use 192.168.34.x/24 as tunnel IP addresses and ensure that information passing the tunnel is encrypted. Use the following parameters for IPSec protocol:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Group: 1
 - Encryption: DES
 - Hash : SHA
 - Key: ccie123
- IPSec Parameters
 - Encryption: ESP-DES
 - Authentication: ESP-SHA-HMAC

Make appropriate changes on ASA2 firewall to allow connections.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config)#interface Tunnel0
R5(config-if)#ip address 192.168.34.5 255.255.255.0
R5(config-if)#tunnel source f0/0
R5(config-if)#tunnel destination 10.1.104.4
```

Definition of GRE tunnel interface ("tunnel mode gre ip" is the default).

```
R5(config-if)#crypto isakmp policy 10
R5(config-isakmp)#authentication pre-share
R5(config-isakmp)#exit
```

```
R5(config)#crypto isakmp key cisco123 address 10.1.104.4
```

```
R5(config)#access-list 120 permit gre host 10.1.105.5 host
10.1.104.4
```

Only the GRE traffic between R5 and R4 will be encrypted.

```
R5(config)#crypto ipsec transform-set TSET esp-des esp-sha-hmac
R5(cfg-crypto-trans)#exit
```

```
R5(config)#crypto map GRE-IPSEC 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

```
R5(config-crypto-map)#set peer 10.1.104.4
R5(config-crypto-map)#set transform-set TSET
R5(config-crypto-map)#match address 120
R5(config-crypto-map)#exit
```

```
R5(config)#int f0/0
R5(config-if)#crypto map GRE-IPSEC
R5(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
```

```
R5(config-if)#router eigrp 34
R5(config-router)#no auto
R5(config-router)#network 192.168.34.5 0.0.0.0
R5(config-router)#network 5.5.5.5 0.0.0.0
```

GRE allows transport of multicast traffic so that it

enables using of dynamic routing protocols like EIGRP between R5 and R4. Encrypting the GRE that transport mulitcast packets is the best way of securing such traffic.

Step 2 R4 configuration.

```
R4(config)#interface Tunnel0
R4(config-if)#ip address 192.168.34.4 255.255.255.0
R4(config-if)#tunnel source f0/0
R4(config-if)#tunnel destination 10.1.105.5
R4(config-if)#exit

R4(config)#crypto isakmp policy 10
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#exit

R4(config)#crypto isakmp key cisco123 address 10.1.105.5

R4(config)#access-list 120 permit gre host 10.1.104.4 host
10.1.105.5

R4(config)#crypto ipsec transform-set TSET esp-des esp-sha-hmac
R4(cfg-crypto-trans)#exit

R4(config)#crypto map GRE-IPSEC 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R4(config-crypto-map)#set peer 10.1.105.5
R4(config-crypto-map)#set transform-set TSET
R4(config-crypto-map)#match address 120

R4(config-crypto-map)#int f0/0
R4(config-if)#crypto map GRE-IPSEC
R4(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R4(config-if)#exit

R4(config)#router eigrp 34
R4(config-router)#no auto
R4(config-router)#network 192.168.34.4 0.0.0.0
R4(config-router)#network 4.4.4.4 0.0.0.0
```

Step 3 ASA2 configuration.

```
ASA2(config)# policy-map global_policy
ASA2(config-pmap)# class inspection_default
ASA2(config-pmap-c)# inspect ipsec-pass-thru
ASA2(config-pmap-c)# exi
ASA2(config-pmap)# exi
```

```
ASA2(config)# same-security-traffic permit inter-interface
```

Verification

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 34: Neighbor 192.168.34.4 (Tunnel0) is up: new adjacency
R5#
```

The EIGRP is working between R5 and R4 through GRE tunnel.

R5#ping 4.4.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 5.5.5.5

```
!!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R5#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.105.10 to network 0.0.0.0

4.0.0.0/24 is subnetted, 1 subnets

```
D    4.4.4.0 [90/27008000] via 192.168.34.4, 00:00:30, Tunnel0
```

5.0.0.0/24 is subnetted, 1 subnets

```
C    5.5.5.0 is directly connected, Loopback0
```

10.0.0.0/24 is subnetted, 1 subnets

```
C    10.1.105.0 is directly connected, FastEthernet0/0
```

```
C    192.168.34.0/24 is directly connected, Tunnel0
```

```
S*   0.0.0.0/0 [1/0] via 10.1.105.10
```

Routing information related to R4's network on its loopback has been learnt by EIGRP.

R5#sh int tu0

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 192.168.34.5/24

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Remember that if detection of the IPSec-protected GRE tunnel failure is needed then GRE keepalives must NOT be used. DPD (Dead Peer Detection) IPSec feature should be used instead. If GRE keepalives on IPSec-protected GRE interface are configured then the tunnel will be flapping.

```
Tunnel source 10.1.105.5 (FastEthernet0/0), destination 10.1.104.4
Tunnel protocol/transport GRE/IP
  Key disabled, sequencing disabled
  Checksumming of packets disabled
Tunnel TTL 255
Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:03, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 110
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  21 packets input, 1900 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  21 packets output, 1900 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
```

R5#sh ip protocol

```
Routing Protocol is "eigrp 34"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 34
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    5.5.5.5/32
    192.168.34.5/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.34.4         90          00:00:45
  Distance: internal 90 external 170
```

Information relevant to the routes learnt and the source of the information are presented.

R5#sh ip eigrp neighbor

IP-EIGRP neighbors for process 34

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.34.4	Tu0	12 00:00:58	11	1434	0	3

R4 is the EIGRP neighbour of R5 on the Tunnel0 interface.

R5#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.105.5	10.1.104.4		ACTIVE	des	sha	psk	1	23:58:52	
Engine-id:Conn-id = SW:1										

IPv6 Crypto ISAKMP SA

ISAKMP SA has been established.

R5#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: GRE-IPSEC, local addr 10.1.105.5

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.105.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.104.4/255.255.255.255/47/0)

Local and remote IPsec proxies. Note that only GRE (IP ID 47) is transported through the tunnel.

current_peer 10.1.104.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 27, #pkts encrypt: 27, #pkts digest: 27

#pkts decaps: 27, #pkts decrypt: 27, #pkts verify: 27

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 110, #recv errors 0

local crypto endpt.: 10.1.105.5, remote crypto endpt.: 10.1.104.4

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

```
current outbound spi: 0xD7DDE0F5(3621642485)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x3007AC1D(805809181)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: GRE-IPSEC
    sa timing: remaining key lifetime (k/sec): (4545433/3527)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0xD7DDE0F5(3621642485)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: GRE-IPSEC
    sa timing: remaining key lifetime (k/sec): (4545433/3527)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:
```

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 34: Neighbor 192.168.34.5 (Tunnel0) is up: new adjacency
```

```
R4#
```

```
R4#ping 5.5.5.5 so lo0
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
```

```
Packet sent with a source address of 4.4.4.4
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

```
R4#sh ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 10.1.104.10 to network 0.0.0.0

```
4.0.0.0/24 is subnetted, 1 subnets
C    4.4.4.0 is directly connected, Loopback0
5.0.0.0/24 is subnetted, 1 subnets
D    5.5.5.0 [90/27008000] via 192.168.34.5, 00:01:34, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C    10.1.104.0 is directly connected, FastEthernet0/0
C    192.168.34.0/24 is directly connected, Tunnel0
S*   0.0.0.0/0 [1/0] via 10.1.104.10
```

R4#sh int tu0

```
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.34.4/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.1.104.4 (FastEthernet0/0), destination 10.1.105.5
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:04, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 9
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    41 packets input, 3780 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    41 packets output, 3780 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
```

R4#sh ip protocol

```
Routing Protocol is "eigrp 34"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
```

```

EIGRP maximum metric variance 1
Redistributing: eigrp 34
EIGRP NSF-aware route hold timer is 240s
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  4.4.4.4/32
  192.168.34.4/32
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.34.5          90          00:01:51
Distance: internal 90 external 170

```

R4#sh ip eigrp neighbor

IP-EIGRP neighbors for process 34

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.34.5	Tu0	13 00:01:59	14	1434	0	3

R4#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.104.4	10.1.105.5		ACTIVE	des	sha	psk	1	23:57:50	
Engine-id:Conn-id = SW:1										

IPv6 Crypto ISAKMP SA

R4#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: GRE-IPSEC, local addr 10.1.104.4

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.104.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.105.5/255.255.255.255/47/0)

current_peer 10.1.105.5 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46

#pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 9, #recv errors 0

```
local crypto endpt.: 10.1.104.4, remote crypto endpt.: 10.1.105.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x3007AC1D(805809181)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xD7DDE0F5(3621642485)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: GRE-IPSEC
    sa timing: remaining key lifetime (k/sec): (4512546/3466)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x3007AC1D(805809181)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: GRE-IPSEC
    sa timing: remaining key lifetime (k/sec): (4512546/3466)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Task 2

Configure GRE tunnel between R1 and R2. The tunnel should pass EIGRP AS 12 multicast packets exchanging information about R1's Loopback0 and R2's g0/1 networks. Use 192.168.12.x/24 as tunnel IP addresses and ensure that information passing the tunnel is encrypted using IPSec Profiles:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Group: 1
 - Encryption: DES
 - Hash : SHA
 - Key: ccie123

- IPsec Parameters
 - Encryption: ESP-DES
 - Authentication: ESP-SHA-HMAC

Make appropriate changes on ASA1 firewall to allow connections.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#interface Tunnel0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#tunnel source f0/0
R1(config-if)#tunnel destination 192.168.1.2
R1(config-if)#!
R1(config-if)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#exit
R1(config)#!
R1(config)#crypto isakmp key cisco123 address 192.168.1.2
R1(config)#!
R1(config)#crypto ipsec transform-set TSET esp-des esp-sha-hmac
R1(cfg-crypto-trans)#exit
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R1(config)#crypto ipsec profile GRE-VPN
R1(ipsec-profile)#set transform-set TSET
R1(ipsec-profile)#exit
```

IPsec profile has been configured. In the next step this profile will be tied to the Tunnel0 interface. The crypto ACL that defines the GRE traffic as interesting is no longer required. GRE profile will define interesting traffic automatically.

```
R1(config)#int tu0
R1(config-if)#tunnel protection ipsec profile GRE-VPN
R1(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R1(config-if)#exi
R1(config)#router eigrp 12
R1(config-router)#no auto
R1(config-router)#network 192.168.12.1 0.0.0.0
R1(config-router)#network 1.1.1.1 0.0.0.0
R1(config-router)#exi
```

Step 2 R2 configuration.

```

R2(config)#interface Tunnel0
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#tunnel source g0/0
R2(config-if)#tunnel destination 10.1.101.1
R2(config-if)#!
R2(config-if)#crypto isakmp policy 10
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#exit
R2(config)#!
R2(config)#crypto isakmp key cisco123 address 10.1.101.1
R2(config)#!
R2(config)#crypto ipsec transform-set TSET esp-des esp-sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#!
R2(config)#crypto ipsec profile GRE-VPN
R2(ipsec-profile)#set transform-set TSET
R2(ipsec-profile)#exit
R2(config)#!
R2(config)#int tu0
R2(config-if)#tunnel protection ipsec profile GRE-VPN
R2(config-if)#exit
R2(config)#!
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to down
R2(config)#router eigrp 12
R2(config-router)#no auto
R2(config-router)#network 192.168.12.2 0.0.0.0
R2(config-router)#network 192.168.2.2 0.0.0.0
R2(config-router)#exit

R2(config)#ip route 10.1.101.1 255.255.255.255 192.168.1.10

```

Step 3 ASA1 configuration.

```

ASA1(config)# policy-map global_policy
ASA1(config-pmap)# class inspection_default
ASA1(config-pmap-c)# inspect ipsec-pass-thru
ASA1(config-pmap-c)# exit
ASA1(config-pmap)# exit

ASA1(config)# access-list OUTSIDE_IN permit udp host 192.168.1.2 eq
500 host 10.1.101.1 eq 500
ASA1(config)# access-list OUTSIDE_IN permit esp host 192.168.1.2
host 10.1.101.1
ASA1(config)# access-group OUTSIDE_IN in interface Outside

```


Verification

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 12: Neighbor 192.168.12.2 (Tunnel0) is up: new adjacency
R1#
```

R1#sh cry isak sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
-----
1001  10.1.101.1        192.168.1.2          ACTIVE des sha psk 1  23:59:12
      Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

R1#ping 192.168.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

R1#sh cry ips sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.101.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.101.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.1.2/255.255.255.255/47/0)
```

This has been done by IPSec profile. Local and remote proxy are available without crypto ACL.

```
current_peer 192.168.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
#pkts decaps: 33, #pkts decrypt: 33, #pkts verify: 33
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 11, #recv errors 0

local crypto endpt.: 10.1.101.1, remote crypto endpt.: 192.168.1.2
```

```

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xE0102732(3759154994)
PFS (Y/N): N, DH group: none

```

```

inbound esp sas:
spi: 0x7FF28A80(2146601600)

```

R1#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

```

```

Gateway of last resort is 10.1.101.10 to network 0.0.0.0

```

```

C    192.168.12.0/24 is directly connected, Tunnel0
    1.0.0.0/24 is subnetted, 1 subnets
C      1.1.1.0 is directly connected, Loopback0
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.101.0 is directly connected, FastEthernet0/0
D    192.168.2.0/24 [90/26882560] via 192.168.12.2, 00:01:40, Tunnel0
S*   0.0.0.0/0 [1/0] via 10.1.101.10

```

R1#sh ip eigrp neighbor

```

IP-EIGRP neighbors for process 12

```

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q	Seq
			(sec)		(ms)		Cnt	Num
0	192.168.12.2	Tu0	14	00:01:51	11	1434	0	3

```

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 12: Neighbor 192.168.12.1 (Tunnel0) is up: new adjacency

```

```

R2#

```

R2#sh crypto isak sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection

```

```

        K - Keepalives, N - NAT-traversal
        T - cTCP encapsulation, X - IKE Extended Authentication
        psk - Preshared key, rsig - RSA signature
        renc - RSA encryption

```

```

IPv4 Crypto ISAKMP SA

```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	192.168.1.2	10.1.101.1		ACTIVE	des	sha	psk	1	23:57:16	
	Engine-id:Conn-id = SW:1									

IPv6 Crypto ISAKMP SA

R2#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 192.168.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.101.1/255.255.255.255/47/0)
current_peer 10.1.101.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 58, #pkts encrypt: 58, #pkts digest: 58
  #pkts decaps: 51, #pkts decrypt: 51, #pkts verify: 51
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 192.168.1.2, remote crypto endpt.: 10.1.101.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x7FF28A80(2146601600)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xE0102732(3759154994)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000046, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4467999/3431)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x7FF28A80(2146601600)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000046, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4467999/3431)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:
```

outbound pcp sas:

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

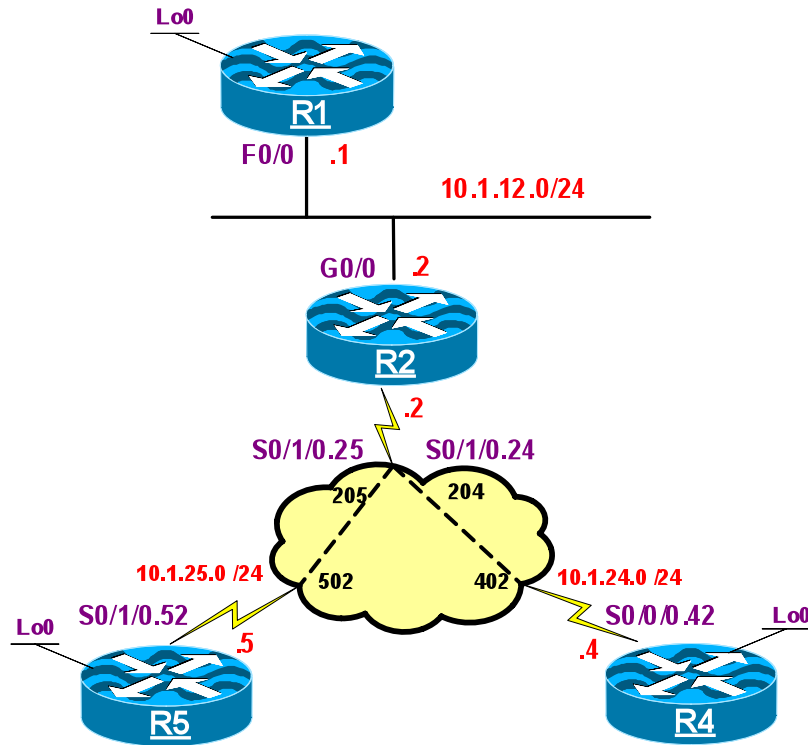
Gateway of last resort is not set

```
C    192.168.12.0/24 is directly connected, Tunnel0
    1.0.0.0/24 is subnetted, 1 subnets
D    1.1.1.0 [90/27008000] via 192.168.12.1, 00:02:29, Tunnel0
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S    10.1.105.0/24 [1/0] via 192.168.2.10
S    10.1.104.0/24 [1/0] via 192.168.2.10
S    10.1.101.0/24 [1/0] via 192.168.1.10
S    10.1.101.1/32 [1/0] via 192.168.1.10
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
C    192.168.2.0/24 is directly connected, GigabitEthernet0/1
```

ASA1(config)# sh access-list

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list OUTSIDE_IN; 2 elements; name hash: 0xe01d8199
access-list OUTSIDE_IN line 1 extended permit udp host 192.168.1.2 eq isakmp host
10.1.101.1 eq isakmp (hitcnt=0) 0xd890bccc ← This is 0 because the tunnel was
initiated from R1
access-list OUTSIDE_IN line 2 extended permit esp host 192.168.1.2 host 10.1.101.1
(hitcnt=1) 0x8ff474ec
```

Lab 1.49.DMVPN Phase 1



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's S0/1/0 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner
- R2's S0/1/0 and R4's S0/0/0 interface should be configured in a frame-relay point-to-point manner
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R4 and R5 pointing to the R2

IP Addressing

Device	Interface	IP address
R1	Lo0	192.168.1.1/24
	F0/0	10.1.12.1/24

R2	F0/0	10.1.12.2/24
	S0/1/0.25	10.1.25.2/24
	S0/1/0.24	10.1.24.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0.42	10.1.24.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0.52	10.1.25.5/24

Task 1

Configure Hub-and-Spoke GRE tunnels between R1, R4 and R5, where R1 is acting as a Hub. Traffic originated from every Spoke's loopback interface should be transmitted securely via the Hub to the other spokes. You must use EIGRP dynamic routing protocol to let other spokes know about protected networks. Use the following settings when configuring tunnels:

- Tunnel Parameters
 - IP address: 172.16.145.0/24
 - IP MTU: 1400
 - Tunnel Authentication Key: 12345
- NHRP Parameters
 - NHRP ID: 12345
 - NHRP Authentication key: cisco123
 - NHRP Hub: R1
- Routing Protocol Parameters
 - EIGRP 145

Encrypt the GRE traffic using the following parameters:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Encryption: 3DES
 - Hashing: SHA
 - DH Group: 2

- Pre-Shared Key: cisco123
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC



Dynamic Multipoint Virtual Private Network (DMVPN) has been introduced by Cisco in late 2000. This technology has been developed to address needs for automatically created VPN tunnels when dynamic IP addresses on the spokes are in use.

In GRE over IPSec (described in the previous lab) both ends of the connection must have static/unchangeable IP address. It is possible however, to create many GRE Site-to-Site tunnels from company's branches to the Headquarters. This is pure Hub-and-Spoke topology where all branches may communicate with each other securely through the Hub.

In DMVPN may have dynamic IP addresses on the spokes, but there must be static IP address on the Hub. There is also an additional technology used to let the hub know what dynamic IP addresses are in use by the spokes. This is NHRP (Next Hop Resolution Protocol) which works like ARP but for layer 3. All it does is building a dynamic database stored on the hub with information about spokes' IP addresses. Now the Hub knows IPSec peers and can build the tunnels with them.

The Hub must be connected to many spokes at the same time so there was another issue to solve: how to configure the Hub to not have many Tunnel interfaces (each for Site-to-Site tunnel with spoke). The answer is: use GRE multipoint type of tunnel, where we do not need to specify the other end of the tunnel statically.

That being said, there are three DMVPN mutations called phases:

- *Phase 1: simple Hub and Spoke topology where dynamic IP addresses on the spokes may be used*
- *Phase 2: Hub and Spoke with Spoke to Spoke direct communication allowed*
- *Phase 3: Hub and Spoke with Spoke to Spoke direct communication allowed with better scalability using NHRP Redirects*

All above phases will be described in more detail in the next few labs.

Configuration

Complete these steps:

Step 1 R1 configuration.

First we need ISAKMP Policy with pre-shared key configured. Note that in DMVPN we need to configure so-called "wildcard PSK" because there may be many peers. This is why more common solution in DMVPN is to use certificates and PKI. In DMVPN Phase 1 there is no need for wildcard PSK as there is only Hub to Spoke tunnel, so that we know the peers.

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr 3des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R1(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)# mode transport
```

The "mode transport" is used for decreasing IPSec packet size (an outer IP header which is present in tunnel mode is not added in the transport mode).

```
R1(cfg-crypto-trans)#crypto ipsec profile DMVPN
R1(ipsec-profile)#set transform-set TSET
R1(ipsec-profile)#exit
```

There is only one interface Tunnel on every DMVPN router. This is because we use GRE multipoint type of the tunnel.

```
R1(config)#interface Tunnel0
R1(config-if)#ip address 172.16.145.1 255.255.255.0

R1(config-if)#ip mtu 1400
```

Maximum Transmission Unit is decreased to ensure that DMVPN packet would not exceed IP MTU set on non-tunnel IP interfaces - usually a 1500 bytes (When "transport mode" is used then DMVPN packet consists of original IP Packet, GRE header, ESP header and outer IPSec IP header. If original IP packet size is close to the IP MTU set on real IP interface then adding GRE and IPSec headers may lead to exceeding that value)

```
R1(config-if)#ip nhrp authentication cisco123
R1(config-if)#ip nhrp map multicast dynamic
R1(config-if)#ip nhrp network-id 12345
```

The Hub works as NHS (Next Hop Server). The NHRP configuration on the Hub is straight forward. First, we

need NHRP network ID to identify the instance and authenticate key to secure NHRP registration. There is a need for NHRP static mapping on the Hub. The Hub must be able to send down all multicast traffic so that dynamic routing protocols can distribute routes between spokes. The line "ip nhrp map multicast dynamic" simply tells the NHRP server to replicate all multicast traffic to all dynamic entries in the NHRP table (entries with flag "dynamic").

```
R1(config-if)#no ip split-horizon eigrp 145
```

Since we use EIGRP between the Hub and the Spokes, we need to disable Split Horizon for that protocol to be able to send routes gathered from one Spoke to the other Spoke. The Split Horizon rule says: "information about the routing is never sent back in the direction from which it was received". This is basic rule for loop prevention.

```
R1(config-if)#tunnel source FastEthernet0/0
R1(config-if)#tunnel mode gre multipoint
R1(config-if)#tunnel key 12345
R1(config-if)#tunnel protection ipsec profile DMVPN
```

A regular GRE tunnel usually needs source and destination of the tunnel to be specified. However in the GRE multipoint tunnel type, there is no need for a destination. This is because there may be many destinations, as many Spokes are out there. The actual tunnel destination is derived from NHRP database.

The tunnel has a key for identification purposes, as there may be many tunnels on one router and the router must know what tunnel the packet is destined to.

Finally, we must encrypt the traffic. This is done by using IPSec Profile attached to the tunnel. I recommend to leave that command aside for a while when configuring DMVPN and add it to the configuration once we know the tunnels work fine. DMVPN may work without any encryption, so no worries.

```
R1(config-if)#exi
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Tunnel0 has changed its state to "UP". ISAKMP protocol is enabled and operates on the router.

```
R1(config)#router eigrp 145
R1(config-router)#network 172.16.145.0 0.0.0.255
R1(config-router)#network 192.168.1.0
R1(config-router)#no auto-summary
R1(config-router)#exi
```

Finally we need a routing protocol over the tunnel. Remember, this protocol will be used to carry the info about networks behind the Spokes (or Hub). Be careful when configuring it as there is a chance to get into "recursive loop". This means we shouldn't use the same dynamic routing protocol instance for prefixes available over the tunnel and to achieve underlaying connectivity between Hub and Spokes.

Step 2 R5 configuration.

R5 is our first Spoke. Again, we need ISAKMP Policy configuration and PSK.

```
R5(config)#crypto isakmp policy 1
R5(config-isakmp)# encr 3des
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# group 2
R5(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R5(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R5(cfg-crypto-trans)# mode transport

R5(cfg-crypto-trans)#crypto ipsec profile DMVPN
R5(ipsec-profile)# set transform-set TSET
R5(ipsec-profile)#exi
```

The tunnel interface configuration is slightly different on the Spoke than on the Hub. This is because the Spoke works as NHRP Client to the Hub (NHS). Most of below commands have been described already.

```
R5(config)#interface Tunnel0
R5(config-if)# ip address 172.16.145.5 255.255.255.0
R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco123
R5(config-if)# ip nhrp map 172.16.145.1 10.1.12.1
R5(config-if)# ip nhrp network-id 12345
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.145.1
```

NHRP Client configuration. We need our Spoke to register in NHS, so that we need to configure the following:

- NHRP authentication key - to authenticate successfully to the NHS
- NHRP Network ID - to be authenticated to correct NHS instance
- NHRP Holdtime - to tell the NHS for how long

it should treat the registered spokes' IP address as valid

- NHS - IP address of NHRP Server; note this is its Private (tunnel) IP address. To resolve this address to the Public (Physical) IP address of the NHS, we need the last command which is:
- NHRP static mapping - to resolve NHS' Physical IP address

This mapping is very important as it causes the Spoke to initiate the GRE tunnel to the Hub. Without this the Spoke has no clue how to register to the NHS.

```
R5(config-if)# tunnel source Serial0/1/0.52
R5(config-if)# tunnel destination 10.1.12.1
R5(config-if)# tunnel key 12345
R5(config-if)# tunnel protection ipsec profile DMVPN
```

The tunnel configuration is also different. On the Spoke there is no reason for using GRE multipoint tunnel mode. This is because there is only one tunnel (Spoke to Hub) in DMVPN Phase 1. Hence, we are obligated to provide both: source and destination of the tunnel.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R5(config-if)#exi

R5(config)#router eigrp 145
R5(config-router)# network 172.16.145.0 0.0.0.255
R5(config-router)# network 192.168.5.0
R5(config-router)# no auto-summary
R5(config-router)#ex
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.1 (Tunnel0)
is up: new adjacency
R5(config-router)#exi
```

The router has established EIGRP adjacency through the tunnel. Note that the adjacency has been established with the DMVPN hub (172.16.145.1).

Step 3 R4 configuration.

The beauty of this technology is that there is exactly the same configuration on all Spokes!

```
R4(config)#crypto isakmp policy 1
```

```
R4(config-isakmp)# encr 3des
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R4(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R4(cfg-crypto-trans)# mode transport

R4(cfg-crypto-trans)#crypto ipsec profile DMVPN
R4(ipsec-profile)# set transform-set TSET
R4(ipsec-profile)#exi

R4(config)#interface Tunnel0
R4(config-if)# ip address 172.16.145.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco123
R4(config-if)# ip nhrp map 172.16.145.1 10.1.12.1
R4(config-if)# ip nhrp network-id 12345
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.145.1
R4(config-if)# tunnel source Serial0/0/0.42
R4(config-if)# tunnel destination 10.1.12.1
R4(config-if)# tunnel key 12345
R4(config-if)# tunnel protection ipsec profile DMVPN
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config-if)#exi

R4(config)#router eigrp 145
R4(config-router)# network 172.16.145.0 0.0.0.255
R4(config-router)# network 192.168.4.0
R4(config-router)# no auto-summary
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.1 (Tunnel0)
is up: new adjacency
R4(config-router)#exi
```

Verification

R1#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route

- o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.145.0 is directly connected, Tunnel0

D 192.168.4.0/24 [90/27008000] via 172.16.145.4, 00:00:17, Tunnel0

D 192.168.5.0/24 [90/27008000] via 172.16.145.5, 00:00:55, Tunnel0

**Spokes have sent updates about their networks (loopback interfaces) to the Hub.
Now Hub must send that information down to the other Spokes. The Hub may do
that as long as Split Horizon rule is disabled for the routing protocol.**

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.12.0 is directly connected, FastEthernet0/0

C 192.168.1.0/24 is directly connected, Loopback0

S* 0.0.0.0/0 [1/0] via 10.1.12.2

R1#sh ip nhrp

172.16.145.4/32 via 172.16.145.4

Tunnel0 created 00:00:33, expire 00:05:26

Type: dynamic, Flags: unique registered

NBMA address: 10.1.24.4

172.16.145.5/32 via 172.16.145.5

Tunnel0 created 00:01:08, expire 00:04:51

Type: dynamic, Flags: unique registered

NBMA address: 10.1.25.5

**NHRP database displayed on the DMVPN hub. Note that "sh ip nhrp" shows mapping
between Tunnel0 ip address and ip address of Serial interface which is used for
reaching the tunnel endpoint. The entries in NHRP database on the hub are
dynamic (dynamically obtained from the spokes).**

R1#sh ip eigrp neighbor

IP-EIGRP neighbors for process 145

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
1	172.16.145.4	Tu0	11	00:00:38	10	1362	0	3
0	172.16.145.5	Tu0	11	00:01:16	29	1362	0	3

EIGRP adjacency established with the spokes.

R1#sh ip eigrp interface

IP-EIGRP interfaces for process 145

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu0	2	0/0	19	6/227	80	0
Lo0	0	0/0	0	0/1	0	0

R1#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.1	10.1.25.5	QM_IDLE	1001	ACTIVE
10.1.12.1	10.1.24.4	QM_IDLE	1002	ACTIVE

IPv6 Crypto ISAKMP SA

R1#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.12.1

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.24.4/255.255.255.255/47/0)

Local and remote identities used for the tunnel. Note that GRE protocol is transported in the tunnel (IP protocol 47). It is automatically achieved by assigning IPSec profile to the tunnel interface (configuring crypto ACLs is no longer needed)

current_peer 10.1.24.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19

#pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19

Note that traffic is going through the tunnel established between the hub (R1) and the spoke (R4).

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.24.4

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x97564348(2539012936)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x2A3D155F(708646239)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2003, flow_id: NETGX:3, sibling_flags 80000006, crypto map: Tunnel0-

head-0

sa timing: remaining key lifetime (k/sec): (4568792/3536)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

Inbound SPI (Security Parameter Index) has been negotiated.

```
inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0x97564348(2539012936)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2004, flow_id: NETGX:4, sibling_flags 80000006, crypto map: Tunnel0-
head-0
  sa timing: remaining key lifetime (k/sec): (4568792/3536)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

Outbound SPI (Security Parameter Index) has been negotiated.

```
outbound ah sas:

outbound pcg sas:
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)
```

Local and remote identities used for tunnel established between hub (R1) and one of the spokes (R5).

```
current_peer 10.1.25.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
#pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.25.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x423D37C6(1111308230)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xE65FFF26(3865050918)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2001, flow_id: NETGX:1, sibling_flags 80000006, crypto map: Tunnel0-
head-0
  sa timing: remaining key lifetime (k/sec): (4492833/3501)
  IV size: 8 bytes
```

```

    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
    spi: 0x423D37C6(1111308230)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000006, crypto map: Tunnel0-
head-0
    sa timing: remaining key lifetime (k/sec): (4492832/3501)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.24.2 to network 0.0.0.0

```

    172.16.0.0/24 is subnetted, 1 subnets
C       172.16.145.0 is directly connected, Tunnel0
C       192.168.4.0/24 is directly connected, Loopback0
D       192.168.5.0/24 [90/28288000] via 172.16.145.1, 00:03:22, Tunnel0
    10.0.0.0/24 is subnetted, 1 subnets
C       10.1.24.0 is directly connected, Serial0/0/0.42
D       192.168.1.0/24 [90/27008000] via 172.16.145.1, 00:03:22, Tunnel0
S*     0.0.0.0/0 [1/0] via 10.1.24.2

```

**The networks of R1 and R5 loopbacks are present in the R4's routing table.
 These networks are reachable through the hub (R1) over the DMVPN network.**

R4#sh ip route 192.168.5.0

```

Routing entry for 192.168.5.0/24
  Known via "eigrp 145", distance 90, metric 28288000, type internal
  Redistributing via eigrp 145

```


Last update from 172.16.145.1 on Tunnel0, 00:03:34 ago

Routing Descriptor Blocks:

* 172.16.145.1, from 172.16.145.1, 00:03:34 ago, via Tunnel0

Next hop IP address followed by the information source (R1 - the hub)

Route metric is 28288000, traffic share count is 1

Total delay is 105000 microseconds, minimum bandwidth is 100 Kbit

Reliability 255/255, minimum MTU 1400 bytes

Loading 1/255, Hops 2

R4#sh ip cef 192.168.5.0

192.168.5.0/24

nexthop 172.16.145.1 Tunnel0

The CEF entries displayed for R5 loopback network. This indicates an IP address of next hop which have to be used for reaching 192.168.5.0/24.

R4#sh ip nhrp

172.16.145.1/32 via 172.16.145.1

Tunnel0 created 00:04:04, never expire

Type: static, Flags:

NBMA address: 10.1.12.1

The NHRP database entries displayed. This shows the mapping between hub's tunnel interface IP address and hub's real interface IP address through which the tunnel endpoint is reachable. Note that NHRP database entries related to the hub are static and never expires (the hub must be always reachable for the spoke and cannot be dynamic).

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id status
10.1.12.1	10.1.24.4	QM_IDLE	1001 ACTIVE

This indicates that ISAKMP tunnel is established and active (QM_IDLE means that ISAKMP SA is authenticated and Quick Mode - IPsec Phase 2 is finished).

IPv6 Crypto ISAKMP SA

R4#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.24.4

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.24.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)

current_peer 10.1.12.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 67, #pkts encrypt: 67, #pkts digest: 67

```
#pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

IPSec proxy IDs on the spoke indicates that traffic between tunnel endpoint will be encrypted/decrypted. Also, packet counters are incrementing as there are routing updates crossing the tunnel.

```
local crypto endpt.: 10.1.24.4, remote crypto endpt.: 10.1.12.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.42
current outbound spi: 0x2A3D155F(708646239)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
spi: 0x97564348(2539012936)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2001, flow_id: NETGX:1, sibling_flags 80000006, crypto map: Tunnel0-
head-0
  sa timing: remaining key lifetime (k/sec): (4571034/3344)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
spi: 0x2A3D155F(708646239)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2002, flow_id: NETGX:2, sibling_flags 80000006, crypto map: Tunnel0-
head-0
  sa timing: remaining key lifetime (k/sec): (4571034/3344)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R4#pi 192.168.5.5 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:

Packet sent with a source address of 192.168.4.4

```
!!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

Now ping the other spoke using its loopback IP address as source. This should simulate end-to-end connectivity through the DMVPN network.

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.1	10.1.24.4	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

Note: No new ISAKMP SA or NHRP mappings created.

R4#sh ip nhrp

```
172.16.145.1/32 via 172.16.145.1
  Tunnel0 created 00:04:40, never expire
  Type: static, Flags:
  NBMA address: 10.1.12.1
```

The same bunch of commands should be run on the other spoke.

R5#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.25.2 to network 0.0.0.0

```
172.16.0.0/24 is subnetted, 1 subnets
C      172.16.145.0 is directly connected, Tunnel0
D      192.168.4.0/24 [90/28288000] via 172.16.145.1, 00:01:24, Tunnel0
C      192.168.5.0/24 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.25.0 is directly connected, Serial0/1/0.52
D      192.168.1.0/24 [90/27008000] via 172.16.145.1, 00:02:02, Tunnel0
S*    0.0.0.0/0 [1/0] via 10.1.25.2
```

R5#sh ip cef 192.168.4.0

```
192.168.4.0/24
  nexthop 172.16.145.1 Tunnel0
```

R5#sh ip nhrp

```
172.16.145.1/32 via 172.16.145.1
  Tunnel0 created 00:02:11, never expire
  Type: static, Flags:
```

NBMA address: 10.1.12.1

R5#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.1	10.1.25.5	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

R5#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.25.5

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)

current_peer 10.1.12.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40

#pkts decaps: 46, #pkts decrypt: 46, #pkts verify: 46

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 10.1.25.5, remote crypto endpt.: 10.1.12.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.52

current outbound spi: 0xE65FFF26(3865050918)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x423D37C6(1111308230)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2001, flow_id: NETGX:1, sibling_flags 80000006, crypto map: Tunnel0-

head-0

sa timing: remaining key lifetime (k/sec): (4430458/3455)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xE65FFF26(3865050918)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

```
conn id: 2002, flow_id: NETGX:2, sibling_flags 80000006, crypto map: Tunnel0-  
head-0  
sa timing: remaining key lifetime (k/sec): (4430459/3455)  
IV size: 8 bytes  
replay detection support: Y  
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R5#pi 192.168.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:

Packet sent with a source address of 192.168.5.5

```
!!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/40 ms

Note: No new ISAKMP SA or NHRP mappings created.

R5#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.1	10.1.25.5	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

R5#sh ip nhrp

172.16.145.1/32 via 172.16.145.1

Tunnel0 created 00:03:01, never expire

Type: static, Flags:

NBMA address: 10.1.12.1

IP Addressing

Device	Interface	IP address
R1	Lo0	192.168.1.1/24
	F0/0	10.1.12.1/24
R2	F0/0	10.1.12.2/24
	S0/1/0.25	10.1.25.2/24
	S0/1/0.24	10.1.24.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0.42	10.1.24.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0.52	10.1.25.5/24

Task 1

Configure Hub-and-Spoke GRE tunnels between R1, R4 and R5, where R1 is acting as a Hub. Traffic originated from every Spoke's loopback interface should be transmitted securely directly to the other spokes. You must use EIGRP dynamic routing protocol to let other spokes know about protected networks. Use the following settings when configuring tunnels:

- Tunnel Parameters
 - IP address: 172.16.145.0/24
 - IP MTU: 1400
 - Tunnel Authentication Key: 12345
- NHRP Parameters
 - NHRP ID: 12345
 - NHRP Authentication key: cisco123
 - NHRP Hub: R1
- Routing Protocol Parameters
 - EIGRP 145

Encrypt the GRE traffic using the following parameters:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Encryption: 3DES

- Hashing: SHA
- DH Group: 2
- Pre-Shared Key: cisco123
- IPsec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC



DMVPN Phase 2 introduces a new feature which is direct Spoke to Spoke communication through the DMVPN network. It is useful for companies who have communication between branches and want to lessen the Hub's overhead. This lab describes DMVPN Phase 2 when EIGRP is in use. This is important to understand the difference between routing protocols used in DMVPN solution. They must be especially configured/tuned to work in most scalable and efficient way.

However, there are some disadvantages of using one protocol or another so that I'll try to describe those in the upcoming labs.

As most of the commands have been already described in the previous lab, I will focus on the new commands and on differences between DMVPN Phase 1 and 2.

Configuration

Complete these steps:

Step 1 R1 configuration.

The Hub's configuration for DMVPN Phase 2 is almost the same as for Phase 1.

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)# encr 3des
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R1(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)# mode transport
```



```

R1(cfg-crypto-trans)#crypto ipsec profile DMVPN
R1(ipsec-profile)# set transform-set TSET
R1(ipsec-profile)#exit

R1(config)#interface Tunnel0
R1(config-if)# ip address 172.16.145.1 255.255.255.0
R1(config-if)# ip mtu 1400
R1(config-if)# ip nhrp authentication cisco123
R1(config-if)# ip nhrp map multicast dynamic
R1(config-if)# ip nhrp network-id 12345
R1(config-if)# no ip split-horizon eigrp 145
R1(config-if)# no ip next-hop-self eigrp 145

```

The difference is in routing protocol behavior. The DMVPN Phase 2 allows for direct Spoke to Spoke communication. Hence, one spoke must send the traffic to the other spoke using its routing table information. In DMVPN Phase 1 the spoke sends all traffic up to the Hub and uses the Hub for Spoke to Spoke communication. However, in DMVPN Phase 2 a spoke must point to the other spoke directly. This is achieved by changing the routing protocol behavior. The EIGRP changes next hop in the routing update when sending it further. So that, the Hub changes the next hop to itself when sending down the routing updates to the Spokes. This behavior can be changed by the command "no ip next-hop-self eigrp AS".

```

R1(config-if)# tunnel source FastEthernet0/0
R1(config-if)# tunnel mode gre multipoint

```

Note that in DMVPN Phase 2 the Hub is in GRE Multipoint mode as it was in Phase 1.

```

R1(config-if)# tunnel key 12345
R1(config-if)# tunnel protection ipsec profile DMVPN
R1(config-if)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

R1(config)#router eigrp 145
R1(config-router)# network 172.16.145.0 0.0.0.255
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
R1(config-router)#exit

```

Step 2 R5 configuration.

```

R5(config)#crypto isakmp policy 1
R5(config-isakmp)# encr 3des

```

```
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# group 2
R5(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R5(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R5(cfg-crypto-trans)# mode transport

R5(cfg-crypto-trans)#crypto ipsec profile DMVPN
R5(ipsec-profile)# set transform-set TSET
R5(ipsec-profile)#exi

R5(config)#interface Tunnel0
R5(config-if)# ip address 172.16.145.5 255.255.255.0
R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco123
R5(config-if)# ip nhrp map 172.16.145.1 10.1.12.1
R5(config-if)# ip nhrp map multicast 10.1.12.1
```

One additional command on the Spoke is about sending multicast traffic to the Hub. This is because on spokes we use GRE Multipoint tunnel type so that we need to tell the router where to send multicast and broadcast traffic.

```
R5(config-if)# ip nhrp network-id 12345
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.145.1
R5(config-if)# tunnel source Serial0/1/0.52
R5(config-if)# tunnel mode gre multipoint
```

Note that on DMVPN Phase 2 we use GRE multipoint tunnel type as we require many tunnels with many spokes.

```
R5(config-if)# tunnel key 12345
R5(config-if)# tunnel protection ipsec profile DMVPN
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R5(config-if)#exi

R5(config)#router eigrp 145
R5(config-router)# network 172.16.145.0 0.0.0.255
R5(config-router)# network 192.168.5.0
R5(config-router)# no auto-summary
R5(config-router)#ex
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.1 (Tunnel0)
is up: new adjacency
R5(config-router)#exi
```

Step 3 R4 configuration.

The DMVPN configuration on all spokes is the same.

```
R4(config)#crypto isakmp policy 1
R4(config-isakmp)# encr 3des
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R4(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R4(cfg-crypto-trans)# mode transport

R4(cfg-crypto-trans)#crypto ipsec profile DMVPN
R4(ipsec-profile)# set transform-set TSET
R4(ipsec-profile)#exit

R4(config)#interface Tunnel0
R4(config-if)# ip address 172.16.145.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco123
R4(config-if)# ip nhrp map 172.16.145.1 10.1.12.1
R4(config-if)# ip nhrp map multicast 10.1.12.1
R4(config-if)# ip nhrp network-id 12345
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.145.1
R4(config-if)# tunnel source Serial0/0/0.42
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# tunnel key 12345
R4(config-if)# tunnel protection ipsec profile DMVPN
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config-if)#exit

R4(config)#router eigrp 145
R4(config-router)# network 172.16.145.0 0.0.0.255
R4(config-router)# network 192.168.4.0
R4(config-router)# no auto-summary
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.1 (Tunnel0)
is up: new adjacency
R4(config-router)#exit
```

Verification

R1#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

```

172.16.0.0/24 is subnetted, 1 subnets
C      172.16.145.0 is directly connected, Tunnel0
D      192.168.4.0/24 [90/297372416] via 172.16.145.4, 00:00:12, Tunnel0
D      192.168.5.0/24 [90/297372416] via 172.16.145.5, 00:00:14, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.12.0 is directly connected, FastEthernet0/0
C      192.168.1.0/24 is directly connected, Loopback0
S*    0.0.0.0/0 [1/0] via 10.1.12.2

```

The Hub has routing information about the networks behind the spokes.

R1#sh ip nhrp

```

172.16.145.4/32 via 172.16.145.4, Tunnel0 created 00:00:22, expire 00:05:37
Type: dynamic, Flags: unique registered
NBMA address: 10.1.24.4
172.16.145.5/32 via 172.16.145.5, Tunnel0 created 00:00:25, expire 00:05:34
Type: dynamic, Flags: unique registered
NBMA address: 10.1.25.5

```

The spokes are registered in NHS successfully.

R1#sh crypto isakmp sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.12.1	10.1.24.4		ACTIVE	3des	sha	psk	2	23:59:19	
Engine-id:Conn-id = SW:2										
1001	10.1.12.1	10.1.25.5		ACTIVE	3des	sha	psk	2	23:59:27	
Engine-id:Conn-id = SW:1										

IPv6 Crypto ISAKMP SA

The Hub set up ISAKMP SA and IPsec SA with both spokes.

R1#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.12.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.24.4/255.255.255.255/47/0)
current_peer 10.1.24.4 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
#pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

The traffic is going through the tunnel between the Hub and the Spoke. This traffic is an EIGRP updates as we have not initiated any traffic yet.

```
local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.24.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x49DC5EAF(1239178927)
```

```
inbound esp sas:
  spi: 0xF483377E(4102240126)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4524624/3565)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
  spi: 0x49DC5EAF(1239178927)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4524622/3565)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

```
protected vrf: (none)
```

```

local ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)
current_peer 10.1.25.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 17, #pkts encrypt: 17, #pkts digest: 17
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

```

The traffic is going through the tunnel between the Hub and the Spoke. This traffic is an EIGRP updates as we have not initiated any traffic yet.

```

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.25.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x1FB68E8D(532057741)

```

```

inbound esp sas:
  spi: 0xE487940A(3834090506)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4411380/3563)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

```

```
inbound ah sas:
```

```
inbound pcsp sas:
```

```

outbound esp sas:
  spi: 0x1FB68E8D(532057741)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4411379/3563)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

```

```
outbound ah sas:
```

```
outbound pcsp sas:
```

R1#sh ip eigrp neighbor

IP-EIGRP neighbors for process 145

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
1	172.16.145.5	Tu0	14 00:00:50	34	5000	0	3

```
0 172.16.145.4 Tu0 11 00:00:50 83 5000 0 3
```

EIGRP neighbor adjacency is established with both spokes via the tunnel.

R1#sh ip eigrp interface

IP-EIGRP interfaces for process 145

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu0	2	0/0	58	71/2524	320	0
Lo0	0	0/0	0	0/1	0	0

R5#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.25.2 to network 0.0.0.0

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.145.0 is directly connected, Tunnel0

D 192.168.4.0/24 [90/310172416] via 172.16.145.4, 00:09:17, Tunnel0

C 192.168.5.0/24 is directly connected, Loopback0

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.25.0 is directly connected, Serial0/1/0.52

D 192.168.1.0/24 [90/297372416] via 172.16.145.1, 00:09:17, Tunnel0

S* 0.0.0.0/0 [1/0] via 10.1.25.2

The Spoke has routing information for the networks behind other spoke and the Hub. Note that in DMVPN Phase 2 the Spoke must point to the other Spoke (not the Hub). This is achieved by configuring "no ip next-hop-self eigrp" command on the Hub.

R5#sh ip route 192.168.4.4

Routing entry for 192.168.4.0/24

Known via "eigrp 145", distance 90, metric 310172416, type internal

Redistributing via eigrp 145

Last update from 172.16.145.4 on Tunnel0, 00:09:25 ago

Routing Descriptor Blocks:

* 172.16.145.4, from 172.16.145.1, 00:09:25 ago, via Tunnel0

Route metric is 310172416, traffic share count is 1

Total delay is 1005000 microseconds, minimum bandwidth is 9 Kbit

Reliability 255/255, minimum MTU 1400 bytes

Loading 1/255, Hops 2

Detailed view of the prefix indicates that R5 got routing information from the Hub but has next hop of R4.

```
R5#sh ip cef 192.168.4.4
192.168.4.0/24, version 20, epoch 0
0 packets, 0 bytes
  via 172.16.145.4, Tunnel0, 0 dependencies
    next hop 172.16.145.4, Tunnel0
    invalid adjacency
```

When CEF is enabled (enabled by default on every router) the router uses CEF database (called FIB) to "switch" the packets. The FIB is built up based on the information from the routing table (RIB). The CEF database indicates that next hop router for that prefix is R4, but it also shows that this entry is "invalid". This is because the router has no clue how to get to that address (what physical interface use to route the traffic out).

```
R5#sh ip cef 10.1.24.4
0.0.0.0/0, version 18, epoch 0, cached adjacency to Serial0/1/0.52
0 packets, 0 bytes
  via 10.1.25.2, 0 dependencies, recursive
    next hop 10.1.25.2, Serial0/1/0.52 via 10.1.25.0/24
    valid cached adjacency
```

```
R5#sh ip cef 172.16.145.4
172.16.145.0/24, version 17, epoch 0, attached, connected
0 packets, 0 bytes
  via Tunnel0, 0 dependencies
    valid punt adjacency
```

Note that there are valid CEF entries for logical and physical tunnel endpoint.

```
R5#sh ip nhrp
172.16.145.1/32 via 172.16.145.1, Tunnel0 created 00:10:24, never expire
  Type: static, Flags: used
  NBMA address: 10.1.12.1
```

NHRP has only static entry for the Hub. This entry is used to register the spoke to the NHS.

```
R5#sh crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
-----
1001  10.1.25.5         10.1.12.1      ACTIVE 3des sha psk 2 23:56:35
```



```
Engine-id:Conn-id = SW:1
```

```
IPv6 Crypto ISAKMP SA
```

R5#sh crypto ipsec sa

```
interface: Tunnel0
```

```
  Crypto map tag: Tunnel0-head-0, local addr 10.1.25.5
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)
```

```
current_peer 10.1.12.1 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  #pkts encaps: 67, #pkts encrypt: 67, #pkts digest: 67
```

```
  #pkts decaps: 56, #pkts decrypt: 56, #pkts verify: 56
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

```
  #pkts not compressed: 0, #pkts compr. failed: 0
```

```
  #pkts not decompressed: 0, #pkts decompress failed: 0
```

```
  #send errors 20, #recv errors 0
```

The spoke has ISKAMP SA and IPSec SA with the Hub. It does not have any tunnels with the other spoke yet.

```
local crypto endpt.: 10.1.25.5, remote crypto endpt.: 10.1.12.1
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.52
```

```
current outbound spi: 0xE487940A(3834090506)
```

```
inbound esp sas:
```

```
  spi: 0x1FB68E8D(532057741)
```

```
    transform: esp-3des esp-sha-hmac ,
```

```
    in use settings ={Transport, }
```

```
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
```

```
    sa timing: remaining key lifetime (k/sec): (4482147/3389)
```

```
    IV size: 8 bytes
```

```
    replay detection support: Y
```

```
    Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
```

```
  spi: 0xE487940A(3834090506)
```

```
    transform: esp-3des esp-sha-hmac ,
```

```
    in use settings ={Transport, }
```

```
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
```

```
    sa timing: remaining key lifetime (k/sec): (4482145/3389)
```

```
    IV size: 8 bytes
```

```
    replay detection support: Y
```

```
    Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

R5#ping 192.168.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:

Packet sent with a source address of 192.168.5.5

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/42/52 ms

R5#ping 192.168.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:

Packet sent with a source address of 192.168.5.5

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms

The ping to the network behind R4 is successful.

R5#sh ip nhrp

172.16.145.1/32 via 172.16.145.1, Tunnel0 created 00:05:05, never expire

Type: static, Flags: used

NBMA address: 10.1.12.1

172.16.145.4/32 via 172.16.145.4, Tunnel0 created 00:00:10, expire 00:05:50

Type: dynamic, Flags: router used

NBMA address: 10.1.24.4

Now after the ping, there are dynamic NHRP mappings and additional spoke-to-spoke IPsec SA.

R5#sh ip cef 192.168.4.4

192.168.4.0/24, version 20, epoch 0

0 packets, 0 bytes

via 172.16.145.4, Tunnel0, 0 dependencies

next hop 172.16.145.4, Tunnel0

valid adjacency

Note that CEF entry is valid now.

R5#sh adjacency tun0 det

Protocol	Interface	Address
IP	Tunnel0	172.16.145.4(5)
		0 packets, 0 bytes
		4500000000000000FF2F76C40A011905
		0A01180420000800000003039
		Tun endpt never
		Epoch: 0

```

IP          Tunnel0          172.16.145.1(5)
                                0 packets, 0 bytes
                                4500000000000000FF2F82C70A011905
                                0A010C0120000800000003039
                                Tun endpt  never
                                Epoch: 0

```

R5#sh crypto isakmp sa

```

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.1.12.1    10.1.25.5    QM_IDLE       1001      0 ACTIVE
10.1.25.5    10.1.24.4    QM_IDLE       1002      0 ACTIVE

```

```
IPv6 Crypto ISAKMP SA
```

The R5 has ISAKMP SA with R4 established. Note that R4 is an Initiator of this tunnel.

R5#sh crypto isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
```

```
      K - Keepalives, N - NAT-traversal
```

```
      X - IKE Extended Authentication
```

```
      psk - Preshared key, rsig - RSA signature
```

```
      renc - RSA encryption
```

```
IPv4 Crypto ISAKMP SA
```

```

C-id  Local          Remote          I-VRF          Status Encr Hash Auth DH Lifetime Cap.
1001  10.1.25.5        10.1.12.1          ACTIVE 3des sha  psk  2  23:55:04
      Engine-id:Conn-id = SW:1
1002  10.1.25.5        10.1.24.4          ACTIVE 3des sha  psk  2  23:58:46
      Engine-id:Conn-id = SW:2

```

```
IPv6 Crypto ISAKMP SA
```

R5#sh crypto ipsec sa

```
interface: Tunnel0
```

```
  Crypto map tag: Tunnel0-head-0, local addr 10.1.25.5
```

```
protected vrf: (none)
```

```
local  ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)
```

```
current_peer 10.1.12.1 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 99, #pkts encrypt: 99, #pkts digest: 99
```

```
#pkts decaps: 82, #pkts decrypt: 82, #pkts verify: 82
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 20, #recv errors 0

local crypto endpt.: 10.1.25.5, remote crypto endpt.: 10.1.12.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.52
current outbound spi: 0xE487940A(3834090506)

inbound esp sas:
spi: 0x1FB68E8D(532057741)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4482143/3300)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xE487940A(3834090506)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4482141/3300)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcg sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.24.4/255.255.255.255/47/0)
current_peer 10.1.24.4 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

This is IPSec SA with R4. Note that for 10 pings sent only 5-6 of them have
been encrypted. This is because the tunnel between R5 and R4 is takes some time
to come up.

local crypto endpt.: 10.1.25.5, remote crypto endpt.: 10.1.24.4
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.52
current outbound spi: 0x541C9A19(1411160601)
```

```
inbound esp sas:
```

```
spi: 0xD15B10C(219525388)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4475056/3522)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
```

```
spi: 0x541C9A19(1411160601)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4475056/3522)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R4#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 10.1.24.2 to network 0.0.0.0
```

```
172.16.0.0/24 is subnetted, 1 subnets
C      172.16.145.0 is directly connected, Tunnel0
C      192.168.4.0/24 is directly connected, Loopback0
D      192.168.5.0/24 [90/310172416] via 172.16.145.5, 00:05:12, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.24.0 is directly connected, Serial0/0/0.42
D      192.168.1.0/24 [90/297372416] via 172.16.145.1, 00:05:12, Tunnel0
S*    0.0.0.0/0 [1/0] via 10.1.24.2
```

R4 has routing information for the networks behind R5 and R1.

R4#sh ip route 192.168.5.5

```
Routing entry for 192.168.5.0/24
  Known via "eigrp 145", distance 90, metric 310172416, type internal
  Redistributing via eigrp 145
  Last update from 172.16.145.5 on Tunnel0, 00:05:18 ago
  Routing Descriptor Blocks:
  * 172.16.145.5, from 172.16.145.1, 00:05:18 ago, via Tunnel0
    Route metric is 310172416, traffic share count is 1
    Total delay is 1005000 microseconds, minimum bandwidth is 9 Kbit
    Reliability 255/255, minimum MTU 1400 bytes
    Loading 1/255, Hops 2
```

R4#sh ip cef 192.168.5.5

```
192.168.5.0/24, version 20, epoch 0
0 packets, 0 bytes
  via 172.16.145.5, Tunnel0, 0 dependencies
    next hop 172.16.145.5, Tunnel0
    valid adjacency
```

The CEF is valid as it has been already resolved during tunnel set up process between R5 and R4.

R4#sh ip nhrp

```
172.16.145.1/32 via 172.16.145.1, Tunnel0 created 00:06:29, never expire
  Type: static, Flags: used
  NBMA address: 10.1.12.1
172.16.145.4/32 via 172.16.145.4, Tunnel0 created 00:01:59, expire 00:04:00
  Type: dynamic, Flags: router unique local
  NBMA address: 10.1.24.4
  (no-socket)
172.16.145.5/32 via 172.16.145.5, Tunnel0 created 00:01:59, expire 00:04:00
  Type: dynamic, Flags: router implicit
  NBMA address: 10.1.25.5
```

R4#sh crypto isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA
```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.24.4	10.1.25.5		ACTIVE	3des	sha	psk	2	23:57:52	
	Engine-id:Conn-id = SW:2									
1001	10.1.24.4	10.1.12.1		ACTIVE	3des	sha	psk	2	23:54:13	

Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

R4#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.24.4

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.24.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.12.1/255.255.255.255/47/0)

current_peer 10.1.12.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 94, #pkts encrypt: 94, #pkts digest: 94

#pkts decaps: 96, #pkts decrypt: 96, #pkts verify: 96

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 13, #recv errors 0

local crypto endpt.: 10.1.24.4, remote crypto endpt.: 10.1.12.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.42

current outbound spi: 0xF483377E(4102240126)

inbound esp sas:

spi: 0x49DC5EAF(1239178927)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4394861/3249)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xF483377E(4102240126)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4394863/3249)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.24.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.25.5/255.255.255.255/47/0)
current_peer 10.1.25.5 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
```

The IPSec SA is already established between R4 and R5. Note that the packet counters are not incrementing as there is no support for dynamic routing protocol between the spokes in DMVPN.

```
local crypto endpt.: 10.1.24.4, remote crypto endpt.: 10.1.25.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.42
current outbound spi: 0xD15B10C(219525388)
```

```
inbound esp sas:
  spi: 0x541C9A19(1411160601)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2005, flow_id: NETGX:5, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4539686/3468)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

inbound ah sas:

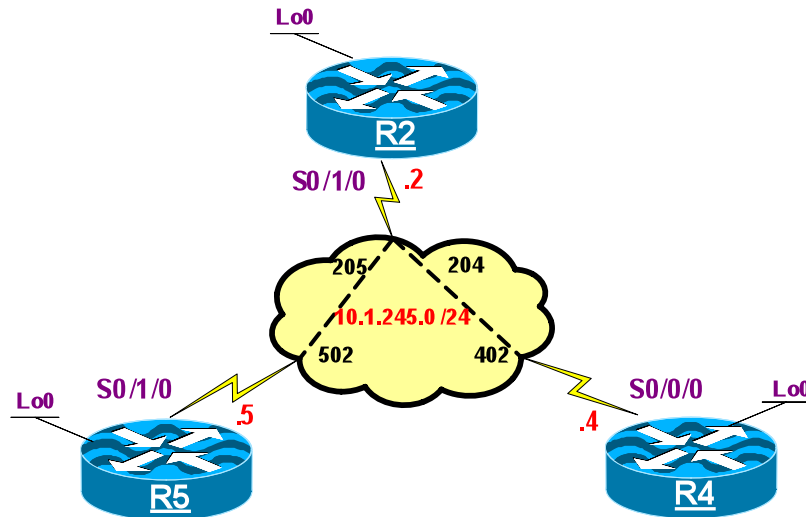
inbound pcp sas:

```
outbound esp sas:
  spi: 0xD15B10C(219525388)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2006, flow_id: NETGX:6, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4539686/3468)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

Lab 1.51.DMVPN Phase 2 (with OSPF)



Depending on IOS software version you may get slightly different command outputs. This is because CEF code has changed in IOS 12.2(20)T.

Lab Setup

- R2's S0/1/0, R4's S0/0/0 and R5's S0/1/0 interfaces should be configured in a frame-relay manner using physical interfaces
- Configure Telnet on all routers using password "cisco"

IP Addressing

Device	Interface	IP address
R2	Lo0	192.168.2.2/24
	S0/1/0	10.1.245.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0	10.1.245.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0	10.1.245.5/24

Task 1

Configure Hub-and-Spoke GRE tunnels between R2, R4 and R5, where R2 is acting as a Hub. Traffic originated from every Spoke's loopback interface should be transmitted securely directly to the other spokes. You must use OSPF dynamic routing protocol to let other spokes know about protected networks. You are not allowed to use NHRP Redirects to accomplish this task. Use the following settings when configuring tunnels:

- Tunnel Parameters
 - IP address: 172.16.245.0/24
 - IP MTU: 1400
 - Tunnel Authentication Key: 123
- NHRP Parameters
 - NHRP ID: 123
 - NHRP Authentication key: cisco123
 - NHRP Hub: R2
- Routing Protocol Parameters
 - OSPF Area 0

Encrypt the GRE traffic using the following parameters:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Encryption: 3DES
 - Hashing: SHA
 - DH Group: 2
 - Pre-Shared Key: cisco123
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC



DMVPN Phase 2 with OSPF is very similar to Phase 2 with EIGRP. We need to configure OSPF in a special way to ensure the spokes has next hop pointing to the other spokes not a Hub. In EIGRP it was achieved by the command of "no ip next-hop-self eigrp" on the Hub. Here it is achieved by tuning OSPF network type.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R2(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R2(cfg-crypto-trans)# mode transport

R2(cfg-crypto-trans)#crypto ipsec profile DMVPN
R2(ipsec-profile)# set transform-set TSET
R2(ipsec-profile)#exi

R2(config)#interface Tunnel0
R2(config-if)# ip address 172.16.245.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip nhrp authentication cisco123
R2(config-if)# ip nhrp map multicast dynamic
R2(config-if)# ip nhrp network-id 123
R2(config-if)# tunnel source s0/1/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# tunnel key 123
R2(config-if)# tunnel protection ipsec profile DMVPN
R2(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R2(config-if)# ip ospf priority 255
R2(config-if)# ip ospf network broadcast
```

We need to know that OSPF does not change next hop when operating in "broadcast" type network. This is because OSPF elects DR/BDR on broadcast networks like Ethernet. Every router in that network sends routing information to DR/BDR

and then that router advertises that information to other routers. Since, all routers are connected to the same media on broadcast networks, it is assumed that they have access to each other. Hence, there is no reason to change the next hop in the advertisements. This protocol behavior perfectly suits in this situation.

Another thing is that we still have Hub and Spoke physical topology. Since, the OSPF must elect DR/BDR and all routers must have adjacency with DR/BDR router we need to ensure this role will be taken by the Hub. We use OSPF priorities to do that. The priority of 255 is the highest and 0 is the lowest. Practically, having priority of 0 disables the router from election process. Thus, we set 255 on the Hub and 0 on the Spokes.

```
R2(config-if)# exit

R2(config)#router ospf 1
R2(config-router)#router-id 172.16.245.2
R2(config-router)#network 172.16.245.2 0.0.0.0 area 0
R2(config-router)#network 192.168.2.2 0.0.0.0 area 0
R2(config-router)#exi
```

Step 2 R5 configuration.

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)# encr 3des
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# group 2
R5(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R5(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R5(cfg-crypto-trans)# mode transport

R5(cfg-crypto-trans)#crypto ipsec profile DMVPN
R5(ipsec-profile)# set transform-set TSET
R5(ipsec-profile)#exi

R5(config)#interface Tunnel0
R5(config-if)# ip address 172.16.245.5 255.255.255.0
R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco123
R5(config-if)# ip nhrp map 172.16.245.2 10.1.245.2
R5(config-if)# ip nhrp map multicast 10.1.245.2
R5(config-if)# ip nhrp network-id 123
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.245.2
R5(config-if)# tunnel source Serial0/1/0
R5(config-if)# tunnel mode gre multipoint
```

```
R5(config-if)# tunnel key 123
R5(config-if)# tunnel protection ipsec profile DMVPN
R5(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R5(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R5(config-if)#ip ospf priority 0
R5(config-if)#ip ospf network broadcast
R5(config-if)#exi
```

No changes on the Spokes but OSPF network type and priority of 0. The priority disables the router participation in DR/BDR election.

```
R5(config)#router ospf 1
R5(config-router)#router-id 172.16.245.5
R5(config-router)#net 172.16.245.5 0.0.0.0 area 0
R5(config-router)#
%OSPF-5-ADJCHG: Process 1, Nbr 172.16.245.2 on Tunnel0 from LOADING
to FULL, Loading Done
R5(config-router)#net 192.168.5.5 0.0.0.0 area 0
R5(config-router)#exi
```

Step 3 R4 configuration.

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)# encr 3des
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R4(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R4(cfg-crypto-trans)# mode transport

R4(cfg-crypto-trans)#crypto ipsec profile DMVPN
R4(ipsec-profile)# set transform-set TSET
R4(ipsec-profile)#exi

R4(config)#interface Tunnel0
R4(config-if)# ip address 172.16.245.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco123
R4(config-if)# ip nhrp map 172.16.245.2 10.1.245.2
R4(config-if)# ip nhrp map multicast 10.1.245.2
R4(config-if)# ip nhrp network-id 123
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.245.2
R4(config-if)# tunnel source Serial0/0/0
```

```

R4(config-if)# tunnel mode gre multipoint
R4(config-if)# tunnel key 123
R4(config-if)# tunnel protection ipsec profile DMVPN
R4(config-router)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R4(config-router)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config-if)# ip ospf priority 0
R4(config-if)# ip ospf network broadcast
R4(config-if)# exi

```

No changes on the Spokes but OSPF network type and priority of 0. The priority disables the router participation in DR/BDR election.

```

R4(config)#router ospf 1
R4(config-router)#router-id 172.16.245.4
R4(config-router)#net 172.16.245.4 0.0.0.0 area 0
R4(config-router)#net 192.168.4.4 0.0.0.0 area 0
R4(config-router)#exi
%OSPF-5-ADJCHG: Process 1, Nbr 172.16.245.2 on Tunnel0 from LOADING
to FULL, Loading Done

```

Verification

R2#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.245.4	0	FULL/DROTHER	00:00:39	172.16.245.4	Tunnel0
172.16.245.5	0	FULL/DROTHER	00:00:34	172.16.245.5	Tunnel0

The Hub has OSPF adjacencies with the Spokes. Note that the Spokes have DROTHER roles in the network - meaning they are not DR/BDR.

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

172.16.0.0/24 is subnetted, 1 subnets
C      172.16.245.0 is directly connected, Tunnel0

```

```

192.168.4.0/32 is subnetted, 1 subnets
O    192.168.4.4 [110/11112] via 172.16.245.4, 00:01:01, Tunnel0
192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.5 [110/11112] via 172.16.245.5, 00:00:43, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C    10.1.245.0 is directly connected, Serial0/1/0
C    192.168.2.0/24 is directly connected, Loopback0

```

The Hub has routing information for networks behind the Spokes.

R2#sh ip nhrp

```

172.16.245.4/32 via 172.16.245.4, Tunnel0 created 00:03:47, expire 00:04:11
Type: dynamic, Flags: unique registered
NBMA address: 10.1.245.4
172.16.245.5/32 via 172.16.245.5, Tunnel0 created 00:04:38, expire 00:05:21
Type: dynamic, Flags: unique registered
NBMA address: 10.1.245.5

```

The Hub works as NHS in the network and has spokes registered.

R2#sh crypto session

```

Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.245.4 port 500
IKE SA: local 10.1.245.2/500 remote 10.1.245.4/500 Active
IPSEC FLOW: permit 47 host 10.1.245.2 host 10.1.245.4
Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.245.5 port 500
IKE SA: local 10.1.245.2/500 remote 10.1.245.5/500 Active
IPSEC FLOW: permit 47 host 10.1.245.2 host 10.1.245.5
Active SAs: 2, origin: crypto map

```

R2#sh crypto isakmp sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.

1002  10.1.245.2        10.1.245.4      ACTIVE 3des sha psk 2 23:55:55
      Engine-id:Conn-id = SW:2

1001  10.1.245.2        10.1.245.5      ACTIVE 3des sha psk 2 23:55:04

```

```
Engine-id:Conn-id = SW:1
```

```
IPv6 Crypto ISAKMP SA
```

For the crypto part, the Hub has IPSec tunnels (encrypting GRE) between all spokes.

R2#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
current_peer 10.1.245.4 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
  #pkts decaps: 43, #pkts decrypt: 43, #pkts verify: 43
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.2, remote crypto endpt.: 10.1.245.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0xD3CA593(222078355)

inbound esp sas:
  spi: 0xB000E51C(2952848668)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: Onboard VPN:3, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4507274/3349)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0xD3CA593(222078355)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: Onboard VPN:4, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4507274/3349)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```


outbound ah sas:

outbound pcg sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)

current_peer 10.1.245.5 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52

#pkts decaps: 38, #pkts decrypt: 38, #pkts verify: 38

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.2, remote crypto endpt.: 10.1.245.5

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x558438AB(1434728619)

inbound esp sas:

spi: 0x83D966D1(2212062929)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2001, flow_id: Onboard VPN:1, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4449171/3298)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0x558438AB(1434728619)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2002, flow_id: Onboard VPN:2, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4449169/3298)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcg sas:

R4#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.245.2	255	FULL/DR	00:00:34	172.16.245.2	Tunnel0

The spoke has OSPF adjacency with the Hub. Note that the Hub is DR (Designated Router).

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

172.16.0.0/24 is subnetted, 1 subnets
C    172.16.245.0 is directly connected, Tunnel0
C    192.168.4.0/24 is directly connected, Loopback0
    192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.5 [110/11112] via 172.16.245.5, 00:01:47, Tunnel0
    10.0.0.0/24 is subnetted, 1 subnets
C    10.1.245.0 is directly connected, Serial0/0/0
    192.168.2.0/32 is subnetted, 1 subnets
O    192.168.2.2 [110/11112] via 172.16.245.2, 00:02:15, Tunnel0

```

Routing to the network behind other spokes should be pointed to the other spoke's IP address. This is achieved by changing OSPF network type to "broadcast".

R4#sh ip route 192.168.5.5

Routing entry for 192.168.5.5/32

Known via "ospf 1", distance 110, metric 11112, type intra area

Last update from 172.16.245.5 on Tunnel0, 00:02:11 ago

Routing Descriptor Blocks:

* 172.16.245.5, from 172.16.245.5, 00:02:11 ago, via Tunnel0

Route metric is 11112, traffic share count is 1

R4#sh ip cef 192.168.5.5

192.168.5.5/32, version 21, epoch 0

0 packets, 0 bytes

via 172.16.245.5, Tunnel0, 0 dependencies

next hop 172.16.245.5, Tunnel0

invalid adjacency

Same situation here, the router has no information about physical interface to route the packet out for that network.

R4#sh ip cef 172.16.245.5

172.16.245.0/24, version 15, epoch 0, attached, connected
0 packets, 0 bytes
via Tunnel0, 0 dependencies
valid punt adjacency

R4#sh ip nhrp

172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:05:35, never expire
Type: static, Flags: used
NBMA address: 10.1.245.2

R4#sh crypto session

Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.245.2 port 500
IKE SA: local 10.1.245.4/500 remote 10.1.245.2/500 Active
IPSEC FLOW: permit 47 host 10.1.245.4 host 10.1.245.2
Active SAs: 2, origin: crypto map

The router has IPSec tunnel to the Hub only.

R4#ping 192.168.5.5 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/47/56 ms

Ping to the network behind the other spoke is successful. After that the CEF entry is "valid" and the packets can be CEF-switched.

R4#sh ip cef 192.168.5.5

192.168.5.5/32, version 21, epoch 0
0 packets, 0 bytes
via 172.16.245.5, Tunnel0, 0 dependencies
next hop 172.16.245.5, Tunnel0
valid adjacency

R4#sh ip cef 172.16.245.5

172.16.245.5/32, version 22, epoch 0, connected
0 packets, 0 bytes
via 172.16.245.5, Tunnel0, 0 dependencies
next hop 172.16.245.5, Tunnel0
valid adjacency

R4#sh ip nhrp

172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:06:08, never expire
Type: static, Flags: used

```

NBMA address: 10.1.245.2
172.16.245.4/32 via 172.16.245.4, Tunnel0 created 00:00:17, expire 00:05:43
  Type: dynamic, Flags: router unique local
NBMA address: 10.1.245.4
  (no-socket)
172.16.245.5/32 via 172.16.245.5, Tunnel0 created 00:00:18, expire 00:05:43
  Type: dynamic, Flags: router used
NBMA address: 10.1.245.5

```

The router got NHRP information from the other spoke so that it can validate CEF entry and use it to switch the packets.

R4#sh crypto session

```

Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.245.2 port 500
  IKE SA: local 10.1.245.4/500 remote 10.1.245.2/500 Active
  IPSEC FLOW: permit 47 host 10.1.245.4 host 10.1.245.2
    Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.245.5 port 500
  IKE SA: local 10.1.245.4/500 remote 10.1.245.5/500 Active
  IKE SA: local 10.1.245.4/500 remote 10.1.245.5/500 Active
  IPSEC FLOW: permit 47 host 10.1.245.4 host 10.1.245.5
    Active SAs: 4, origin: crypto map

```

The direct IPSec tunnel has been built between the spokes.

R4#sh crypto isakmp sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.245.4	10.1.245.5		ACTIVE	3des	sha	psk	2	23:59:23	
	Engine-id:Conn-id = SW:2									
1003	10.1.245.4	10.1.245.5		ACTIVE	3des	sha	psk	2	23:59:23	
	Engine-id:Conn-id = SW:3									
1001	10.1.245.4	10.1.245.2		ACTIVE	3des	sha	psk	2	23:53:33	
	Engine-id:Conn-id = SW:1									

IPv6 Crypto ISAKMP SA

R4#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 65, #pkts encrypt: 65, #pkts digest: 65
#pkts decaps: 70, #pkts decrypt: 70, #pkts verify: 70
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0xB000E51C(2952848668)

inbound esp sas:
  spi: 0xD3CA593(222078355)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4438379/3207)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xB000E51C(2952848668)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4438380/3207)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
current_peer 10.1.245.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

Note that only 2 packets out of 5 has been encrypted/decrypted. This does not mean 3 packets has lost. Those packets has been sent to the other spoke through the Hub in the first step. Then, when the direct tunnel came up, rest of the packets used the encrypted tunnel.

```
local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x723E68C3(1916692675)
```

```
inbound esp sas:
  spi: 0x8C779DEA(2356649450)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4388330/3558)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
  spi: 0x723E68C3(1916692675)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4388330/3558)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R5#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

172.16.0.0/24 is subnetted, 1 subnets
C      172.16.245.0 is directly connected, Tunnel0
192.168.4.0/32 is subnetted, 1 subnets
O      192.168.4.4 [110/11112] via 172.16.245.4, 00:04:18, Tunnel0
C      192.168.5.0/24 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.245.0 is directly connected, Serial0/1/0
192.168.2.0/32 is subnetted, 1 subnets
O      192.168.2.2 [110/11112] via 172.16.245.2, 00:04:28, Tunnel0

```

Same on the other spoke - the routing points to the remote spoke.

R5#sh ip cef 192.168.4.4

```

192.168.4.4/32, version 17, epoch 0
0 packets, 0 bytes
via 172.16.245.4, Tunnel0, 0 dependencies
next hop 172.16.245.4, Tunnel0
valid adjacency

```

CEF entry is "valid" because it was validated by the tunnel establishment process between R4 and R5. Same for NHRP entries below.

R5#sh ip nhrp

```

172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:08:04, never expire
Type: static, Flags: used
NBMA address: 10.1.245.2
172.16.245.4/32 via 172.16.245.4, Tunnel0 created 00:01:24, expire 00:04:37
Type: dynamic, Flags: router
NBMA address: 10.1.245.4
172.16.245.5/32 via 172.16.245.5, Tunnel0 created 00:01:23, expire 00:04:37
Type: dynamic, Flags: router unique local
NBMA address: 10.1.245.5
(no-socket)

```

R5#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection
 K - Keepalives, N - NAT-traversal
 X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.245.5	10.1.245.4		ACTIVE	3des	sha	psk	2	23:58:30	
Engine-id:Conn-id = SW:2										
1001	10.1.245.5	10.1.245.2		ACTIVE	3des	sha	psk	2	23:51:49	
Engine-id:Conn-id = SW:1										
1003	10.1.245.5	10.1.245.4		ACTIVE	3des	sha	psk	2	23:58:30	
Engine-id:Conn-id = SW:3										

IPv6 Crypto ISAKMP SA

R5#sh crypto ipsec sa

```

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.5

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 67, #pkts encrypt: 67, #pkts digest: 67
  #pkts decaps: 80, #pkts decrypt: 80, #pkts verify: 80
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x83D966D1(2212062929)

inbound esp sas:
  spi: 0x558438AB(1434728619)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4486614/3104)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```



```
spi: 0x83D966D1(2212062929)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4486616/3104)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)

current_peer 10.1.245.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2

#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

Tunnel between spokes works!

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.4

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x8C779DEA(2356649450)

inbound esp sas:

```
spi: 0x723E68C3(1916692675)
```

```
  transform: esp-3des esp-sha-hmac ,
```

```
  in use settings ={Transport, }
```

```
  conn id: 2005, flow_id: NETGX:5, crypto map: Tunnel0-head-0
```

```
  sa timing: remaining key lifetime (k/sec): (4422335/3505)
```

```
  IV size: 8 bytes
```

```
  replay detection support: Y
```

```
  Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x8C779DEA(2356649450)
```

```
  transform: esp-3des esp-sha-hmac ,
```

```
  in use settings ={Transport, }
```

```
  conn id: 2006, flow_id: NETGX:6, crypto map: Tunnel0-head-0
```

```
  sa timing: remaining key lifetime (k/sec): (4422335/3505)
```

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

R5#ping 192.168.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:

Packet sent with a source address of 192.168.5.5

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms

Try to ping to see if the tunnel statistics are incrementing.

R5#sh crypto ipsec sa

```
interface: Tunnel0
```

```
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.5
```

```
protected vrf: (none)
```

```
local  ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
```

```
current_peer 10.1.245.2 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 71, #pkts encrypt: 71, #pkts digest: 71
```

```
#pkts decaps: 85, #pkts decrypt: 85, #pkts verify: 85
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.2
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
```

```
current outbound spi: 0x83D966D1(2212062929)
```

```
inbound esp sas:
```

```
  spi: 0x558438AB(1434728619)
```

```
    transform: esp-3des esp-sha-hmac ,
```

```
    in use settings ={Transport, }
```

```
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
```

```
    sa timing: remaining key lifetime (k/sec): (4486613/3059)
```

```
    IV size: 8 bytes
```

```
    replay detection support: Y
```

```
    Status: ACTIVE
```

```
inbound ah sas:
```

inbound pcp sas:

outbound esp sas:

```
spi: 0x83D966D1(2212062929)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4486615/3059)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)

current_peer 10.1.245.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7

#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

See 5 more packets encrypted/decrypted.

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.4

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x8C779DEA(2356649450)

inbound esp sas:

```
spi: 0x723E68C3(1916692675)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2005, flow_id: NETGX:5, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4422334/3459)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

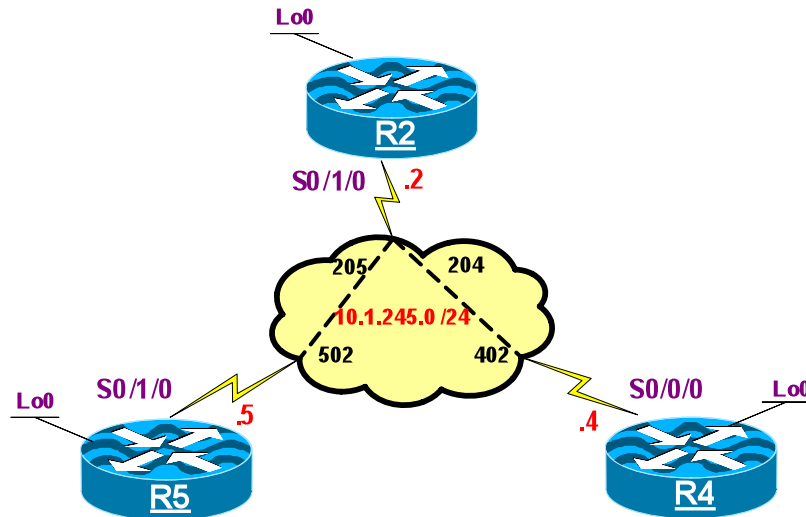
```
spi: 0x8C779DEA(2356649450)
transform: esp-3des esp-sha-hmac ,
```

```
in use settings ={Transport, }  
conn id: 2006, flow_id: NETGX:6, crypto map: Tunnel0-head-0  
sa timing: remaining key lifetime (k/sec): (4422334/3459)  
IV size: 8 bytes  
replay detection support: Y  
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

Lab 1.52. DMVPN Phase 3 (with EIGRP)



Depending on IOS software version you may get slightly different command outputs. This is because CEF code has changed in IOS 12.2(20)T.

Lab Setup

- R2's S0/1/0, R4's S0/0/0 and R5's S0/1/0 interfaces should be configured in a frame-relay manner using physical interfaces
- Configure Telnet on all routers using password "cisco"

IP Addressing

Device	Interface	IP address
R2	Lo0	192.168.2.2/24
	S0/1/0	10.1.245.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0	10.1.245.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0	10.1.245.5/24

Task 1

Configure Hub-and-Spoke GRE tunnels between R2, R4 and R5, where R2 is acting as a Hub. Traffic originated from every Spoke's loopback interface should be transmitted securely directly to the other spokes. You must use EIGRP dynamic routing protocol to let other spokes know about protected networks. You must ensure that every traffic is CEF switched. Use the following settings when configuring tunnels:

- Tunnel Parameters
 - IP address: 172.16.245.0/24
 - IP MTU: 1400
 - Tunnel Authentication Key: 123
- NHRP Parameters
 - NHRP ID: 123
 - NHRP Authentication key: cisco123
 - NHRP Hub: R2
- Routing Protocol Parameters
 - EIGRP AS 245

Encrypt the GRE traffic using the following parameters:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Encryption: 3DES
 - Hashing: SHA
 - DH Group: 2
 - Pre-Shared Key: cisco123
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC



DMVPN Phase 3 is the latest method of configuration. It was introduced by Cisco to fix some disadvantages of Phase 2 like:

- *Scalability: Phase 2 allows Hubs daisy-chaining, OSPF single area, limited number of hubs due to OSPF DR/BDR election*
- *Scalability: Phase 2 does not allow route summarization on the Hub, all prefixes must be distributed to all spokes to be able to set up direct spoke to spoke tunnels.*
- *Performance: Phase 2 sends first packets through the Hub using process-switching (not CEF) causing CPU spikes.*

DMVPN Phase 3 uses two NHRP "hacks" to make it happen:

- *NHRP Redirect – a new messages send from the Hub to the Spoke to let the Spoke know that there is a better path to the other spoke than through the Hub*
- *NHRP Shortcut – a new way of changing (overwriting) CEF information on the Spoke*

In DMVPN Phase 3 all Spokes must point to the Hub for the networks behind the other spokes (just like it was in Phase 1).

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R2(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R2(cfg-crypto-trans)# mode transport

R2(cfg-crypto-trans)#crypto ipsec profile DMVPN
R2(ipsec-profile)# set transform-set TSET
R2(ipsec-profile)#exit

R2(config)#int Tunnel0
R2(config-if)# ip address 172.16.245.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip nhrp authentication cisco123
R2(config-if)# ip nhrp map multicast dynamic
R2(config-if)# ip nhrp network-id 123
```

```
R2(config-if)# ip nhrp redirect
```

NHRP Redirect is a special NHRP message sent by the Hub to the spoke to tell the spoke that there is a better path to the remote spoke than through the Hub. All it does is enforces the spoke to trigger an NHRP resolution request to IP destination.

The "ip nhrp redirect" command should be configured on the Hub only!

```
R2(config-if)# tunnel source s0/1/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# tunnel key 123
R2(config-if)# tunnel protection ipsec profile DMVPN
R2(config-if)# no ip split-horizon eigrp 245
```

Note that we do not need "no ip next-hop-self eigrp" command in the DMVPN Phase 3.

```
R2(config-if)# exit
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON

R2(config)#router eigrp 245
R2(config-router)#no auto
R2(config-router)#net 172.16.245.2 0.0.0.0
R2(config-router)#net 192.168.2.2 0.0.0.0
R2(config-router)#exit
```

Step 2 R4 configuration.

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)# encr 3des
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R4(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R4(cfg-crypto-trans)# mode transport

R4(cfg-crypto-trans)#crypto ipsec profile DMVPN
R4(ipsec-profile)# set transform-set TSET
R4(ipsec-profile)#exit

R4(config)#int Tunnel0
R4(config-if)# ip address 172.16.245.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco123
R4(config-if)# ip nhrp map 172.16.245.2 10.1.245.2
```



```
R4(config-if)# ip nhrp map multicast 10.1.245.2
R4(config-if)# ip nhrp network-id 123
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.245.2
R4(config-if)# ip nhrp shortcut
```

The only difference on the spoke is that the spoke has NHRP Shortcut configured. This will work together with NHRP Redirect on the Hub to send a new Resolution Request NHRP message and overwrite CEF entry to use direct spoke to spoke tunnel instead of the Hub.
This command should be configured on spokes only.

```
R4(config-if)# tunnel source Serial0/0/0
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# tunnel key 123
R4(config-if)# tunnel protection ipsec profile DMVPN
R4(config-router)#exi
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up

R4(config-if)#router eigrp 245
R4(config-router)#no auto
R4(config-router)#net 172.16.245.4 0.0.0.0
R4(config-router)#net 192.168.4.4 0.0.0.0
R4(config-router)#exi
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 245: Neighbor 172.16.245.2 (Tunnel0)
is up: new adjacency
```

Step 3 R5 configuration.

Same configuration on all spokes.

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)# encr 3des
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# group 2
R5(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R5(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R5(cfg-crypto-trans)# mode transport

R5(cfg-crypto-trans)#crypto ipsec profile DMVPN
R5(ipsec-profile)# set transform-set TSET
R5(ipsec-profile)#exi

R5(config)#int Tunnel0
R5(config-if)# ip address 172.16.245.5 255.255.255.0
```

```

R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco123
R5(config-if)# ip nhrp map 172.16.245.2 10.1.245.2
R5(config-if)# ip nhrp map multicast 10.1.245.2
R5(config-if)# ip nhrp network-id 123
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.245.2
R5(config-if)# ip nhrp shortcut
R5(config-if)# tunnel source Serial0/1/0
R5(config-if)# tunnel mode gre multipoint
R5(config-if)# tunnel key 123
R5(config-if)# tunnel protection ipsec profile DMVPN
R5(config-if)# exit
R5(config)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R5(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up

R5(config-if)#router eigrp 245
R5(config-router)#no auto
R5(config-router)#net 172.16.245.5 0.0.0.0
R5(config-router)#net 192.168.5.5 0.0.0.0
R5(config-router)#exit
R5(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 245: Neighbor 172.16.245.2 (Tunnel0)
is up: new adjacency

```

Verification

R2#sh ip eigr neighbors

IP-EIGRP neighbors for process 245

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q	Seq Cnt Num
1	172.16.245.5	Tu0	10 00:04:57	1608	5000	0	3
0	172.16.245.4	Tu0	11 00:05:48	51	1362	0	4

R2#sh ip eigr interfaces

IP-EIGRP interfaces for process 245

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu0	2	0/0	829	6/227	148	0
Lo0	0	0/0	0	0/1	0	0

The Hub has neighbor adjacencies with the spokes.

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

172.16.0.0/24 is subnetted, 1 subnets
C      172.16.245.0 is directly connected, Tunnel0
D      192.168.4.0/24 [90/27008000] via 172.16.245.4, 00:06:53, Tunnel0
D      192.168.5.0/24 [90/27008000] via 172.16.245.5, 00:00:07, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.245.0 is directly connected, Serial0/1/0
C      192.168.2.0/24 is directly connected, Loopback0

```

Routing information for network behind the spokes is on the Hub.

R2#sh ip nhrp

```

172.16.245.4/32 via 172.16.245.4
Tunnel0 created 00:07:38, expire 00:04:21
Type: dynamic, Flags: unique registered
NBMA address: 10.1.245.4
172.16.245.5/32 via 172.16.245.5
Tunnel0 created 00:06:11, expire 00:05:48
Type: dynamic, Flags: unique registered used
NBMA address: 10.1.245.5

```

The Spokes are registered in the NHRP database successfully.

R2#sh crypto session

```

Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.245.4 port 500
IKE SA: local 10.1.245.2/500 remote 10.1.245.4/500 Active
IPSEC FLOW: permit 47 host 10.1.245.2 host 10.1.245.4
Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.245.5 port 500
IKE SA: local 10.1.245.2/500 remote 10.1.245.5/500 Active
IPSEC FLOW: permit 47 host 10.1.245.2 host 10.1.245.5
Active SAs: 2, origin: crypto map

```

R2#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal
 T - cTCP encapsulation, X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.245.2	10.1.245.4		ACTIVE	3des	sha	psk	2	23:52:08	
	Engine-id:Conn-id = SW:1									
1002	10.1.245.2	10.1.245.5		ACTIVE	3des	sha	psk	2	23:53:35	
	Engine-id:Conn-id = SW:2									

IPv6 Crypto ISAKMP SA

The Hub has ISAKMP SA and IPSec SA with the spokes. This is to encrypt GRE tunnel traffic.

R2#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
current_peer 10.1.245.4 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 118, #pkts encrypt: 118, #pkts digest: 118
  #pkts decaps: 108, #pkts decrypt: 108, #pkts verify: 108
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.2, remote crypto endpt.: 10.1.245.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x655C5AD2(1700551378)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x9B622E0(162931424)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000006, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4495822/3124)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x655C5AD2(1700551378)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000006, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4495820/3124)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
current_peer 10.1.245.5 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 95, #pkts encrypt: 95, #pkts digest: 95
  #pkts decaps: 97, #pkts decrypt: 97, #pkts verify: 97
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.2, remote crypto endpt.: 10.1.245.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0xD73908D9(3610839257)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x2CB7F3F4(750253044)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000006, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4587098/3210)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:
```

```

outbound esp sas:
  spi: 0xD73908D9(3610839257)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000006, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4587098/3210)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

R4#sh ip eigrp neighbors

IP-EIGRP neighbors for process 245

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q	Seq Cnt Num
0	172.16.245.2	Tu0	13 00:07:47	12	5000	0	7

The Spoke has neighbor adjacency with the Hub.

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

172.16.0.0/24 is subnetted, 1 subnets
C      172.16.245.0 is directly connected, Tunnel0
C      192.168.4.0/24 is directly connected, Loopback0
D      192.168.5.0/24 [90/298652416] via 172.16.245.2, 00:01:10, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.245.0 is directly connected, Serial0/0/0
D      192.168.2.0/24 [90/297372416] via 172.16.245.2, 00:07:57, Tunnel0

```

The routing information for remote network is pointing to the Hub's IP address.

R4#sh ip cef 192.168.5.0

```

192.168.5.0/24, version 25, epoch 0
0 packets, 0 bytes

```

```
via 172.16.245.2, Tunnel0, 0 dependencies
next hop 172.16.245.2, Tunnel0
valid adjacency
```

R4#sh ip cef 192.168.5.5

```
192.168.5.0/24, version 25, epoch 0
0 packets, 0 bytes
via 172.16.245.2, Tunnel0, 0 dependencies
next hop 172.16.245.2, Tunnel0
valid adjacency
```

The CEF entry is valid as the spoke has all information how to reach Hubs physical IP address.

R4#sh ip nhrp

```
172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:09:05, never expire
Type: static, Flags: used
NBMA address: 10.1.245.2
```

There is a static entry in the NHRP database on the spoke. This entry is used in NHRP registration process.

R4#sh crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.1.245.2   10.1.245.4   QM_IDLE        1001      0 ACTIVE

IPv6 Crypto ISAKMP SA
```

The ISKAMP SA and IPSec SAs are built up with the Hub only. There are no spoke to Spoke IPSec tunnels yet.

R4#sh crypto ipsec sa

```
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.1.245.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 128, #pkts encrypt: 128, #pkts digest: 128
#pkts decaps: 137, #pkts decrypt: 137, #pkts verify: 137
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
```

```

current outbound spi: 0x9B622E0(162931424)

inbound esp sas:
  spi: 0x655C5AD2(1700551378)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4388606/3040)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x9B622E0(162931424)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4388607/3040)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

R4#ping 192.168.5.5 so lo0

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/43/56 ms

```

Test by pinging the network behind the other spoke.

R4#sh ip cef 192.168.5.0

```

192.168.5.0/24, version 25, epoch 0
0 packets, 0 bytes
  via 172.16.245.2, Tunnel0, 0 dependencies
    next hop 172.16.245.2, Tunnel0
      valid adjacency

```

R4#sh ip nhrp

```

172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:09:48, never expire
  Type: static, Flags: used
  NBMA address: 10.1.245.2

```



```

172.16.245.5/32 via 172.16.245.5, Tunnel0 created 00:00:15, expire 00:05:46
  Type: dynamic, Flags: router implicit used
  NBMA address: 10.1.245.5
192.168.4.0/24 via 172.16.245.4, Tunnel0 created 00:00:14, expire 00:05:46
  Type: dynamic, Flags: router unique local
  NBMA address: 10.1.245.4
    (no-socket)
192.168.5.0/24 via 172.16.245.5, Tunnel0 created 00:00:13, expire 00:05:46
  Type: dynamic, Flags: router
  NBMA address: 10.1.245.5

```

The NHRP database shows new dynamic entries for the remote spoke and the "local" entry for R4 which is created when sending an NHRP resolution reply.

R4#sh crypto isakmp sa

```

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.1.245.4    10.1.245.5    QM_IDLE        1002     0 ACTIVE
10.1.245.5    10.1.245.4    QM_IDLE        1003     0 ACTIVE
10.1.245.2    10.1.245.4    QM_IDLE        1001     0 ACTIVE

IPv6 Crypto ISAKMP SA

```

R4#sh crypto ipsec sa

```

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
  #pkts decaps: 165, #pkts decrypt: 165, #pkts verify: 165
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x9B622E0(162931424)

inbound esp sas:
  spi: 0x655C5AD2(1700551378)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4388602/2954)
    IV size: 8 bytes

```

```
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x9B622E0(162931424)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4388604/2954)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
current_peer 10.1.245.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

Note that only one ICMP packet out of 5 has been sent through the direct Spoke-to-Spoke tunnel. Rest of the packets has been sent through the Hub.

```
local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x3CAEA65A(1018078810)
```

```
inbound esp sas:
spi: 0xD962CE1F(3647131167)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2005, flow_id: NETGX:5, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4384325/3528)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:
```

inbound pcg sas:

outbound esp sas:

```
spi: 0x3CAEA65A(1018078810)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2006, flow_id: NETGX:6, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4384325/3528)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

Same information on the other spoke.

R5#sh ip eigrp neighbors

IP-EIGRP neighbors for process 245

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	172.16.245.2	Tu0	12 00:09:43	20	5000	0	7

R5#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.245.0 is directly connected, Tunnel0

D 192.168.4.0/24 [90/298652416] via 172.16.245.2, 00:09:50, Tunnel0

C 192.168.5.0/24 is directly connected, Loopback0

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.245.0 is directly connected, Serial0/1/0

D 192.168.2.0/24 [90/297372416] via 172.16.245.2, 00:09:50, Tunnel0

The spoke has routing information for remote networks pointing to the Hub.

R5#sh ip cef 192.168.4.0

192.168.4.0/24, version 21, epoch 0

0 packets, 0 bytes

via 172.16.245.2, Tunnel0, 0 dependencies

```
next hop 172.16.245.2, Tunnel0
valid adjacency
```

R5#sh ip nhrp

```
172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:10:09, never expire
  Type: static, Flags: used
  NBMA address: 10.1.245.2
172.16.245.4/32 via 172.16.245.4, Tunnel0 created 00:02:02, expire 00:03:59
  Type: dynamic, Flags: router implicit
  NBMA address: 10.1.245.4
192.168.4.0/24 via 172.16.245.4, Tunnel0 created 00:02:00, expire 00:03:59
  Type: dynamic, Flags: router
  NBMA address: 10.1.245.4
192.168.5.0/24 via 172.16.245.5, Tunnel0 created 00:02:01, expire 00:03:59
  Type: dynamic, Flags: router unique local
  NBMA address: 10.1.245.5
  (no-socket)
```

NHRP entries has been resolved and cached already.

R5#sh crypto isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA
```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.245.5	10.1.245.2		ACTIVE	3des	sha	psk	2	23:49:44	
	Engine-id:Conn-id = SW:1									
1003	10.1.245.5	10.1.245.4		ACTIVE	3des	sha	psk	2	23:57:51	
	Engine-id:Conn-id = SW:3									
1002	10.1.245.5	10.1.245.4		ACTIVE	3des	sha	psk	2	23:57:51	
	Engine-id:Conn-id = SW:2									

```
IPv6 Crypto ISAKMP SA
```

R5#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.5

  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
  current_peer 10.1.245.2 port 500
    PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 156, #pkts encrypt: 156, #pkts digest: 156
#pkts decaps: 155, #pkts decrypt: 155, #pkts verify: 155
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x2CB7F3F4(750253044)

inbound esp sas:
  spi: 0xD73908D9(3610839257)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4475924/2980)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0x2CB7F3F4(750253044)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4475924/2980)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
current_peer 10.1.245.4 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

The IPSec SA is built and used for encrypting packets between the spokes.

```
local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0xD962CE1F(3647131167)
```

```
inbound esp sas:
spi: 0x3CAEA65A(1018078810)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4564186/3468)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcsp sas:
```

```
outbound esp sas:
spi: 0xD962CE1F(3647131167)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4564186/3468)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcsp sas:
```

R5#ping 192.168.4.4 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.5
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
```

Let's ping to see if the traffic goes through the tunnel.

R5#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.5

  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 160, #pkts encrypt: 160, #pkts digest: 160
#pkts decaps: 158, #pkts decrypt: 158, #pkts verify: 158
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x2CB7F3F4(750253044)

inbound esp sas:
  spi: 0xD73908D9(3610839257)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4475923/2962)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcsp sas:

outbound esp sas:
  spi: 0x2CB7F3F4(750253044)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4475923/2962)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcsp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
current_peer 10.1.245.4 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

Yes, the traffic is crossing the tunnel as we see 5 more packets encrypted/decrypted.

```
local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0xD962CE1F(3647131167)
```

inbound esp sas:

```
spi: 0x3CAEA65A(1018078810)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4564186/3449)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

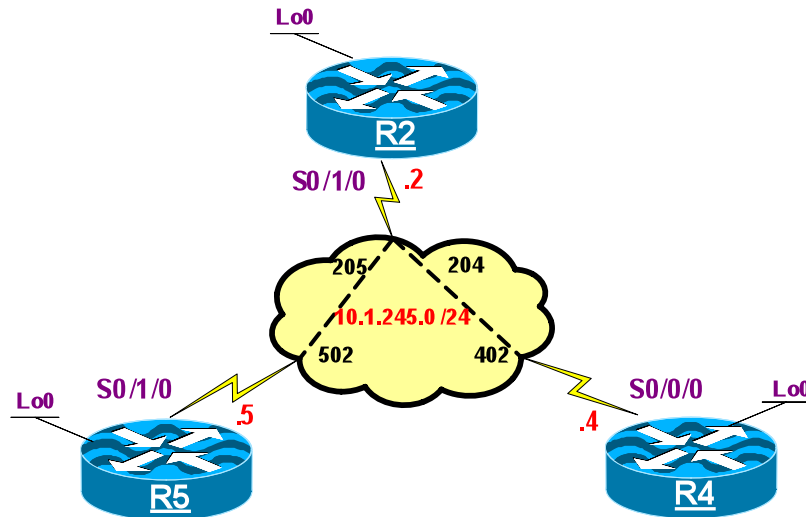
outbound esp sas:

```
spi: 0xD962CE1F(3647131167)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4564186/3449)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

Lab 1.53.DMVPN Phase 3 (with OSPF)



Depending on IOS software version you may get slightly different command outputs. This is because CEF code has changed in IOS 12.2(20)T.

Lab Setup

- R2's S0/1/0, R4's S0/0/0 and R5's S0/1/0 interfaces should be configured in a frame-relay manner using physical interfaces
- Configure Telnet on all routers using password "cisco"

IP Addressing

Device	Interface	IP address
R2	Lo0	192.168.2.2/24
	S0/1/0	10.1.245.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0	10.1.245.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0	10.1.245.5/24

Task 1

Configure Hub-and-Spoke GRE tunnels between R2, R4 and R5, where R2 is acting as a Hub. Traffic originated from every Spoke's loopback interface should be transmitted securely directly to the other spokes. You must use OSPF dynamic routing protocol to let other spokes know about protected networks. You must ensure that every traffic is CEF switched. Use the following settings when configuring tunnels:

- Tunnel Parameters
 - IP address: 172.16.245.0/24
 - IP MTU: 1400
 - Tunnel Authentication Key: 123
- NHRP Parameters
 - NHRP ID: 123
 - NHRP Authentication key: cisco123
 - NHRP Hub: R2
- Routing Protocol Parameters
 - OSPF Area 0

Encrypt the GRE traffic using the following parameters:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Encryption: 3DES
 - Hashing: SHA
 - DH Group: 2
 - Pre-Shared Key: cisco123
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC



OSPF is always tricky when used in DMVPN scenarios. In DMVPN Phase 3 we need to care of OSPF network type to ensure the Spokes point to the Hub's IP address for remote networks.

To achieve that the OSPF network type must be changed to point-to-multipoint as this type has no DR/BDR election process and changes next hop when advertising the routes further.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)#crypto isakmp key cisco123 address
0.0.0.0 0.0.0.0

R2(config)#crypto ipsec transform-set TSET esp-3des esp-
sha-hmac
R2(cfg-crypto-trans)# mode transport

R2(cfg-crypto-trans)#crypto ipsec profile DMVPN
R2(ipsec-profile)# set transform-set TSET
R2(ipsec-profile)#exi

R2(config)#int Tunnel0
R2(config-if)# ip address 172.16.245.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip nhrp authentication cisco123
R2(config-if)# ip nhrp map multicast dynamic
R2(config-if)# ip nhrp network-id 123
R2(config-if)# ip nhrp redirect

This is DMVPN Phase 3, so do not forget of NHRP
Redirect.

R2(config-if)# tunnel source s0/1/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# tunnel key 123
R2(config-if)# tunnel protection ipsec profile DMVPN
R2(config-if)# ip ospf network point-to-multipoint
```

Here's the change. We need to have 'point-to-multipoint' OSPF network type in DMVPN Phase 3 to

make it work. This will allow the Hub sending summarizing routes to the spokes, as the spokes must contact the Hub in the first step to route the packets to the remote network.

Note that we do not configure OSPF priorities as there is no DR/BDR election process in OSPF point-to-multipoint network type. This is also very important in more advanced scenarios when we'd need more hubs in the DMVPN Phase 3 network.

```
R2(config-if)# exit
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON

R2(config)#router ospf 1
R2(config-router)#router-id 172.16.245.2
R2(config-router)#network 172.16.245.2 0.0.0.0 area 0
R2(config-router)#network 192.168.2.2 0.0.0.0 area 0
R2(config-router)#exit
```

Step 2 R4 configuration.

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)# encr 3des
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)#crypto isakmp key cisco123 address
0.0.0.0 0.0.0.0

R4(config)#crypto ipsec transform-set TSET esp-3des esp-
sha-hmac
R4(cfg-crypto-trans)# mode transport

R4(cfg-crypto-trans)#crypto ipsec profile DMVPN
R4(ipsec-profile)# set transform-set TSET
R4(ipsec-profile)#exit

R4(config)#int Tunnel0
R4(config-if)# ip address 172.16.245.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco123
R4(config-if)# ip nhrp map 172.16.245.2 10.1.245.2
R4(config-if)# ip nhrp map multicast 10.1.245.2
R4(config-if)# ip nhrp network-id 123
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.245.2
R4(config-if)# ip nhrp shortcut
```

NHRP Shortcut should be enabled on spokes in DMVPN Phase 3.

```
R4(config-if)# tunnel source Serial0/0/0
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# tunnel key 123
R4(config-if)# tunnel protection ipsec profile DMVPN
R4(config-if)# ip ospf network point-to-multipoint
```

Same on the spokes - OSPF point-to-multipoint
network type.

```
R4(config-router)#exi
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up

R4(config)#router ospf 1
R4(config-router)#router-id 172.16.245.4
R4(config-router)#network 172.16.245.4 0.0.0.0 area 0
R4(config-router)#network 192.168.4.4 0.0.0.0 area 0
R4(config-router)#exi
R4(config)#
%OSPF-5-ADJCHG: Process 1, Nbr 172.16.245.2 on Tunnel0 from
LOADING to FULL, Loading Done
```

Step 3 R5 configuration.

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)# encr 3des
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# group 2
R5(config-isakmp)#crypto isakmp key cisco123 address
0.0.0.0 0.0.0.0

R5(config)#crypto ipsec transform-set TSET esp-3des esp-
sha-hmac
R5(cfg-crypto-trans)# mode transport

R5(cfg-crypto-trans)#crypto ipsec profile DMVPN
R5(ipsec-profile)# set transform-set TSET
R5(ipsec-profile)#exi

R5(config)#int Tunnel0
R5(config-if)# ip address 172.16.245.5 255.255.255.0
R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco123
R5(config-if)# ip nhrp map 172.16.245.2 10.1.245.2
R5(config-if)# ip nhrp map multicast 10.1.245.2
R5(config-if)# ip nhrp network-id 123
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.245.2
R5(config-if)# ip nhrp shortcut
```

```

R5(config-if)# tunnel source Serial0/1/0
R5(config-if)# tunnel mode gre multipoint
R5(config-if)# tunnel key 123
R5(config-if)# tunnel protection ipsec profile DMVPN
R5(config-if)# ip ospf network point-to-multipoint

```

Same on the spokes - OSPF point-to-multipoint network type.

```

R5(config-if)# exit
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R5(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up

R5(config)#router ospf 1
R5(config-router)#router-id 172.16.245.5
R5(config-router)#network 172.16.245.5 0.0.0.0 area 0
R5(config-router)#network 192.168.5.5 0.0.0.0 area 0
R5(config-router)#exit
R5(config)#
%OSPF-5-ADJCHG: Process 1, Nbr 172.16.245.2 on Tunnel0 from
LOADING to FULL, Loading Done

```

Verification

R2#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.245.5	0	FULL/ -	00:01:59	172.16.245.5	Tunnel0
172.16.245.4	0	FULL/ -	00:01:49	172.16.245.4	Tunnel0

The Hub has neighbor adjacency with the spokes.

R2#sh ip ospf interface

```

Loopback0 is up, line protocol is up
  Internet Address 192.168.2.2/24, Area 0
  Process ID 1, Router ID 172.16.245.2, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Tunnel0 is up, line protocol is up
  Internet Address 172.16.245.2/24, Area 0
  Process ID 1, Router ID 172.16.245.2, Network Type POINT_TO_MULTIPOINT, Cost: 1000
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:24
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled

```

```

IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 172.16.245.5
  Adjacent with neighbor 172.16.245.4
Suppress hello for 0 neighbor(s)

```

The network type on the Hub is Point-to-Multipoint

R2#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

Gateway of last resort is not set

```

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.16.245.0/24 is directly connected, Tunnel0
O    172.16.245.5/32 [110/1000] via 172.16.245.5, 00:01:22, Tunnel0
O    172.16.245.4/32 [110/1000] via 172.16.245.4, 00:02:39, Tunnel0
192.168.4.0/32 is subnetted, 1 subnets
O    192.168.4.4 [110/1001] via 172.16.245.4, 00:00:53, Tunnel0
192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.5 [110/1001] via 172.16.245.5, 00:00:43, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C    10.1.245.0 is directly connected, Serial0/1/0
C    192.168.2.0/24 is directly connected, Loopback0

```

The Hub has remote networks in its routing table. Note that those networks are "host" prefixes. This is because the loopback interfaces has OSPF "loopback" type and thus, they are advertised as "host" routes. To change that, configure "ip ospf network point-to-point" on the loopback interfaces.

R2#sh ip nhrp

```

172.16.245.4/32 via 172.16.245.4
  Tunnel0 created 00:03:10, expire 00:04:48
  Type: dynamic, Flags: unique registered
  NBMA address: 10.1.245.4
172.16.245.5/32 via 172.16.245.5
  Tunnel0 created 00:01:45, expire 00:04:14
  Type: dynamic, Flags: unique registered
  NBMA address: 10.1.245.5

```

Both spokes are redistered in NHS successfully.

R2#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.245.2	10.1.245.4		ACTIVE	3des	sha	psk	2	23:56:43	
	Engine-id:Conn-id = SW:1									
1002	10.1.245.2	10.1.245.5		ACTIVE	3des	sha	psk	2	23:58:08	
	Engine-id:Conn-id = SW:2									

IPv6 Crypto ISAKMP SA

The Hub has ISAKMP SA and IPsec SA established with the spokes.

R2#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.245.2

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)

current_peer 10.1.245.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26

#pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.2, remote crypto endpt.: 10.1.245.4

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0xD90CFE(227594238)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x6E5FC564(1851770212)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000006, crypto map:

Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4393718/3399)

IV size: 8 bytes


```
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
    spi: 0xD90CFFE(227594238)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000006, crypto map:
Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4393717/3399)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
current_peer 10.1.245.5 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 22
    #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.2, remote crypto endpt.: 10.1.245.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0xC52C4105(3308011781)
PFS (Y/N): N, DH group: none

inbound esp sas:
    spi: 0xFAEAE72E(4209698606)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000006, crypto map:
Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4388665/3484)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:
```

inbound pcp sas:

outbound esp sas:

```
spi: 0xC52C4105(3308011781)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000006, crypto map:
```

Tunnel0-head-0

```
sa timing: remaining key lifetime (k/sec): (4388664/3484)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

R4#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.245.2	0	FULL/ -	00:01:44	172.16.245.2	Tunnel0

The spoke has neighbor adjacency with the Hub. Note the Hub is NOT DR/BDR in this case.

R4#sh ip ospf interface

```
Loopback0 is up, line protocol is up
  Internet Address 192.168.4.4/24, Area 0
  Process ID 1, Router ID 172.16.245.4, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Tunnel0 is up, line protocol is up
  Internet Address 172.16.245.4/24, Area 0
  Process ID 1, Router ID 172.16.245.4, Network Type POINT_TO_MULTIPOINT, Cost: 11111
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:24
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.245.2
  Suppress hello for 0 neighbor(s)
```

OSPF network type "point-to-multipoint" is configured.

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.16.245.0/24 is directly connected, Tunnel0
O    172.16.245.2/32 [110/11111] via 172.16.245.2, 00:03:23, Tunnel0
O    172.16.245.5/32 [110/12111] via 172.16.245.2, 00:02:05, Tunnel0
C    192.168.4.0/24 is directly connected, Loopback0
    192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.5 [110/12112] via 172.16.245.2, 00:01:27, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C    10.1.245.0 is directly connected, Serial0/0/0
    192.168.2.0/32 is subnetted, 1 subnets
O    192.168.2.2 [110/11112] via 172.16.245.2, 00:01:48, Tunnel0

```

The Spoke has routing to the networks behind other spokes via the Hub. This is achieved by configured OSPF network type.

R4#sh ip cef 192.168.5.5

```

192.168.5.5/32, version 25, epoch 0
0 packets, 0 bytes
via 172.16.245.2, Tunnel0, 0 dependencies
next hop 172.16.245.2, Tunnel0
valid adjacency

```

CEF entry is "valid" as the spoke has all information about how to get to the hub.

R4#sh ip nhrp

```

172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:04:05, never expire
Type: static, Flags: used
NBMA address: 10.1.245.2

```

R4#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection
 K - Keepalives, N - NAT-traversal
 X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption
 IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.245.4	10.1.245.2		ACTIVE	3des	sha	psk	2	23:55:48	

Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

There is ISAKMP SA and IPSec SA established with the Hub only. There are no SAs with other spoke yet.

R4#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
  #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x6E5FC564(1851770212)

inbound esp sas:
  spi: 0xD90CFE(227594238)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4481079/3341)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x6E5FC564(1851770212)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4481080/3341)
```

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

R4#ping 192.168.5.5 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/43/60 ms
```

Test by pinging the remote network. Remember to source that ping from the network behind the spoke.

R4#sh ip nhrp

```
172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:04:52, never expire
  Type: static, Flags: used
  NBMA address: 10.1.245.2
172.16.245.5/32 via 172.16.245.5, Tunnel0 created 00:00:21, expire 00:05:39
  Type: dynamic, Flags: router implicit
  NBMA address: 10.1.245.5
192.168.4.0/24 via 172.16.245.4, Tunnel0 created 00:00:20, expire 00:05:39
  Type: dynamic, Flags: router unique local
  NBMA address: 10.1.245.4
    (no-socket)
192.168.5.0/24 via 172.16.245.5, Tunnel0 created 00:00:20, expire 00:05:39
  Type: dynamic, Flags: router
  NBMA address: 10.1.245.5
```

NHRP has added dynamic entries for the other spoke.

R4#sh ip cef 192.168.5.5

```
192.168.5.5/32, version 25, epoch 0
0 packets, 0 bytes
  via 172.16.245.2, Tunnel0, 0 dependencies
    next hop 172.16.245.2, Tunnel0
      valid adjacency
```

R4#sh crypto isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA
```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1003	10.1.245.4	10.1.245.5		ACTIVE	3des	sha	psk	2	23:59:25	
	Engine-id:Conn-id = SW:3									
1001	10.1.245.4	10.1.245.2		ACTIVE	3des	sha	psk	2	23:54:53	
	Engine-id:Conn-id = SW:1									
1002	10.1.245.4	10.1.245.5		ACTIVE	3des	sha	psk	2	23:59:25	
	Engine-id:Conn-id = SW:2									

IPv6 Crypto ISAKMP SA

The ISAKMP and IPsec SAs has been negotiated with the other spoke.

R4#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.245.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 32, #pkts encrypt: 32, #pkts digest: 32
  #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x6E5FC564(1851770212)

inbound esp sas:
  spi: 0xD90CFFE(227594238)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4481078/3289)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
```

```
spi: 0x6E5FC564(1851770212)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4481079/3289)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)

current_peer 10.1.245.5 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

Note that this time no packets have been sent through the direct tunnel. All packets have been sent through the Hub. However, next packets should use the direct Spoke-to-Spoke tunnel.

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.5

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0

current outbound spi: 0xB8BE4200(3099476480)

inbound esp sas:

spi: 0x7ACB8793(2060158867)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4472866/3561)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

spi: 0x4CD42BBF(1288973247)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2007, flow_id: NETGX:7, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4474527/3591)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x81623FED(2170699757)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4472866/3561)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
spi: 0xB8BE4200(3099476480)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2008, flow_id: NETGX:8, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4474527/3591)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

R4#ping 192.168.5.5 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:

Packet sent with a source address of 192.168.4.4

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms

Try to ping again.

R4#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.245.4

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)
current_peer 10.1.245.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 33, #pkts encrypt: 33, #pkts digest: 33
#pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```



```
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x6E5FC564(1851770212)

inbound esp sas:
  spi: 0xD90CFE(227594238)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4481078/3266)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x6E5FC564(1851770212)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4481079/3266)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
current_peer 10.1.245.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.4, remote crypto endpt.: 10.1.245.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0xB8BE4200(3099476480)
```

See that all ICMP packets have been sent through the spoke-to-spoke tunnel.

```
inbound esp sas:
spi: 0x4CD42BBF(1288973247)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2007, flow_id: NETGX:7, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4474526/3568)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
spi: 0xB8BE4200(3099476480)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2008, flow_id: NETGX:8, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4474526/3568)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

Same bunch of command on the other spoke.

R5#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.245.2	0	FULL/ -	00:01:39	172.16.245.2	Tunnel0

R5#sh ip ospf interface

```
Loopback0 is up, line protocol is up
  Internet Address 192.168.5.5/24, Area 0
  Process ID 1, Router ID 172.16.245.5, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Tunnel0 is up, line protocol is up
  Internet Address 172.16.245.5/24, Area 0
  Process ID 1, Router ID 172.16.245.5, Network Type POINT_TO_MULTIPOINT, Cost: 11111
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:23
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
```

```

Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.245.2
Suppress hello for 0 neighbor(s)

```

R5#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

```

Gateway of last resort is not set

```

```

      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C      172.16.245.0/24 is directly connected, Tunnel0
O      172.16.245.2/32 [110/11111] via 172.16.245.2, 00:04:34, Tunnel0
O      172.16.245.4/32 [110/12111] via 172.16.245.2, 00:04:34, Tunnel0
      192.168.4.0/32 is subnetted, 1 subnets
O      192.168.4.4 [110/12112] via 172.16.245.2, 00:04:04, Tunnel0
C      192.168.5.0/24 is directly connected, Loopback0
      10.0.0.0/24 is subnetted, 1 subnets
C      10.1.245.0 is directly connected, Serial0/1/0
      192.168.2.0/32 is subnetted, 1 subnets
O      192.168.2.2 [110/11112] via 172.16.245.2, 00:04:15, Tunnel0

```

R5#sh ip cef 192.168.4.4

```

192.168.4.4/32, version 21, epoch 0
0 packets, 0 bytes
  via 172.16.245.2, Tunnel0, 0 dependencies
    next hop 172.16.245.2, Tunnel0
    valid adjacency

```

R5#sh ip nhrp

```

172.16.245.2/32 via 172.16.245.2, Tunnel0 created 00:05:03, never expire
  Type: static, Flags: used
  NBMA address: 10.1.245.2
172.16.245.4/32 via 172.16.245.4, Tunnel0 created 00:01:56, expire 00:04:03
  Type: dynamic, Flags: router implicit
  NBMA address: 10.1.245.4
192.168.4.0/24 via 172.16.245.4, Tunnel0 created 00:01:56, expire 00:04:03
  Type: dynamic, Flags: router
  NBMA address: 10.1.245.4
192.168.5.0/24 via 172.16.245.5, Tunnel0 created 00:01:56, expire 00:04:03
  Type: dynamic, Flags: router unique local
  NBMA address: 10.1.245.5

```

(no-socket)

R5#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.245.5	10.1.245.2		ACTIVE	3des	sha	psk	2	23:54:50	
	Engine-id:Conn-id = SW:1									
1003	10.1.245.5	10.1.245.4		ACTIVE	3des	sha	psk	2	23:57:57	
	Engine-id:Conn-id = SW:3									
1002	10.1.245.5	10.1.245.4		ACTIVE	3des	sha	psk	2	23:57:57	
	Engine-id:Conn-id = SW:2									

IPv6 Crypto ISAKMP SA

R5#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.245.5

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)

current_peer 10.1.245.2 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 33, #pkts encrypt: 33, #pkts digest: 33

#pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0xFAEAE72E(4209698606)

inbound esp sas:

spi: 0xC52C4105(3308011781)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4522359/3286)

IV size: 8 bytes

```
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xFAEAE72E(4209698606)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4522360/3286)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)
current_peer 10.1.245.4 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

Those are packets sent from R4.

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x4CD42BBF(1288973247)

inbound esp sas:
spi: 0xB8BE4200(3099476480)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2007, flow_id: NETGX:7, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4551728/3503)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
```

inbound pcp sas:

outbound esp sas:

```
spi: 0x4CD42BBF(1288973247)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2008, flow_id: NETGX:8, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4551728/3503)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

R5#ping 192.168.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:

Packet sent with a source address of 192.168.5.5

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms

Try to ping R4's network to see if the packets get encrypted/decrypted.

R5#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.245.5

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.2/255.255.255.255/47/0)

current_peer 10.1.245.2 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 33, #pkts encrypt: 33, #pkts digest: 33

#pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0xFAEAE72E(4209698606)

inbound esp sas:

```
spi: 0xC52C4105(3308011781)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
```

```
conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4522358/3268)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```
spi: 0xFAEAE72E(4209698606)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4522360/3268)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.245.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.245.4/255.255.255.255/47/0)

current_peer 10.1.245.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

Seems everything is working!

local crypto endpt.: 10.1.245.5, remote crypto endpt.: 10.1.245.4

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x4CD42BBF(1288973247)

inbound esp sas:

```
spi: 0xB8BE4200(3099476480)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2007, flow_id: NETGX:7, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4551727/3485)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

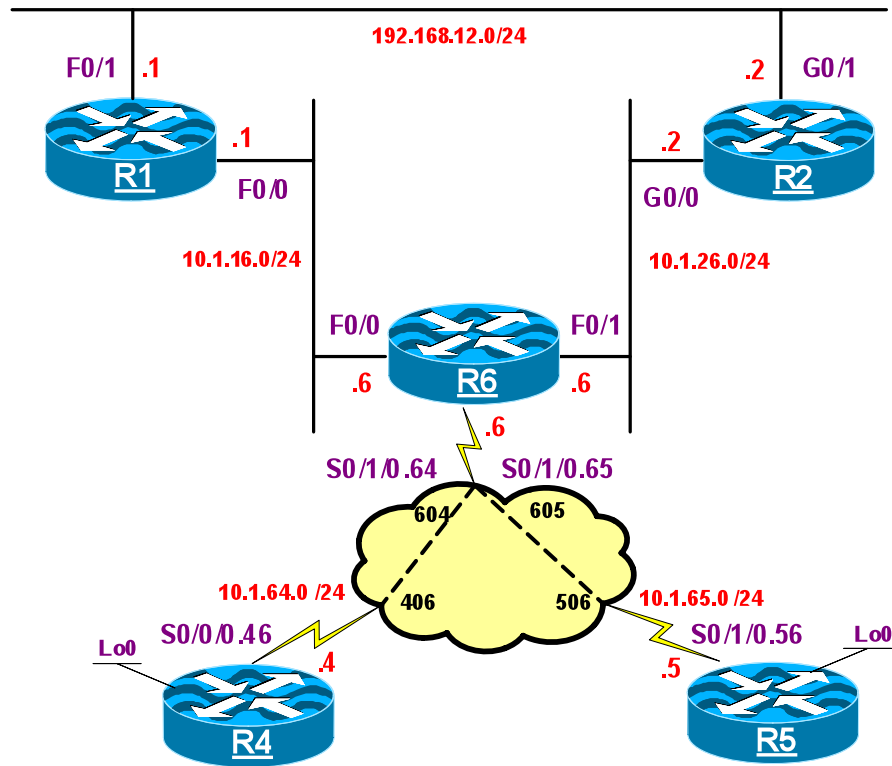
outbound esp sas:

```
spi: 0x4CD42BBF(1288973247)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2008, flow_id: NETGX:8, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4551727/3485)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

Lab 1.54. DMVPN Phase 2 Dual Hub (Single Cloud)



Depending on IOS software version you may get slightly different command outputs. This is because CEF code has changed in IOS 12.2(20)T.

Lab Setup

- R1's F0/0 and R6's F0/0 interface should be configured in VLAN 16
- R1's F0/1 and R2's G0/1 interface should be configured in VLAN 12
- R2's G0/0 and R6's F0/1 interface should be configured in VLAN 26
- R6's S0/1/0 and R4's S0/0/0 interface should be configured in a frame-relay point-to-point manner.
- R6's S0/1/0 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R2, R4 and R5 pointing to the R6

IP Addressing

Device	Interface	IP address
R1	F0/0	10.1.16.1/24
	F0/1	192.168.12.1/24
R2	G0/0	10.1.26.2/24
	G0/1	192.168.12.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0.46	10.1.64.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0.56	10.1.65.5/24
R6	F0/0	10.1.16.6/24
	F0/1	10.1.26.6/24
	S0/1/0.64	10.1.64.6/24
	S0/1/0.65	10.1.65.6/24

Task 1

Configure Hub-and-Spoke GRE tunnels between R1, R2, R4 and R5, where R1 and R2 are acting as Hubs. High availability must be achieved by configuring two NHS on the spokes. Traffic originated from every Spoke's loopback interface and Hub's F0/1 (G0/1) interface should be transmitted securely directly to the other spokes. You must use EIGRP dynamic routing protocol to let other spokes know about protected networks. Use the following settings when configuring tunnels:

- Tunnel Parameters
 - IP address: 172.16.145.0/24
 - IP MTU: 1400
 - Tunnel Authentication Key: 145
- NHRP Parameters
 - NHRP ID: 145
 - NHRP Authentication key: cisco123
 - NHRP Hub: R1

- Routing Protocol Parameters
 - EIGRP 145

Encrypt the GRE traffic using the following parameters:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Encryption: 3DES
 - Hashing: SHA
 - DH Group: 2
 - Pre-Shared Key: cisco123
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC



With a few additional configuration lines to the spoke routers you can set up dual (or multiple) hub routers, for redundancy. There are two ways to configure dual hub DMVPNs:

- 1. A single DMVPN network with each spoke using a single multipoint GRE tunnel interface and pointing to two different hubs as its Next-Hop-Server (NHS). The hub routers will only have a single multipoint GRE tunnel interface.*
- 2. Dual DMVPN networks with each spoke having two GRE tunnel interfaces (either point-to-point or multipoint) and each GRE tunnel connected to a different hub router. Again, the hub routers will only have a single multipoint GRE tunnel interface.*

Dual Hub - Single DMVPN Layout

The dual hub with a single DMVPN layout is fairly easy to set up, but it does not give you as much control over the routing across the DMVPN as the dual hub with dual DMVPNs layout does. The idea in this case is to have a single DMVPN "cloud" with all hubs (two in this case) and all spokes connected to this single subnet ("cloud"). The static NHRP mappings from the spokes to the hubs define the static IPsec+mGRE links over which the dynamic routing protocol will run. The dynamic routing protocol will not run over the dynamic IPsec+mGRE links between spokes. Since the spoke routers are routing neighbors with the hub routers over the same mGRE tunnel interface, you cannot use link or interfaces

differences (like metric, cost, delay, or bandwidth) to modify the dynamic routing protocol metrics to prefer one hub over the other hub when they are both up. If this preference is needed, then techniques internal to the configuration of the routing protocol must be used. For this reason, it may be better to use EIGRP rather than OSPF for the dynamic routing protocol.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# encr 3des
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R1(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)# mode transport

R1(cfg-crypto-trans)#crypto ipsec profile DMVPN
R1(ipsec-profile)# set transform-set TSET
```

There is only one Tunnel interface (GRE multipoint type) on each Hub.

```
R1(ipsec-profile)#interface Tunnel0
R1(config-if)# ip address 172.16.145.1 255.255.255.0
R1(config-if)# ip mtu 1400
R1(config-if)# ip nhrp authentication cisco145
R1(config-if)# ip nhrp map multicast dynamic
R1(config-if)# ip nhrp network-id 145
R1(config-if)# no ip split-horizon eigrp 145
R1(config-if)# no ip next-hop-self eigrp 145
```

This is DMVPN Phase 2 with EIGRP scenario so that we need to turn off Split Horizon and next hop changing on the Hub.

```
R1(config-if)# tunnel source FastEthernet0/0
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# tunnel key 145
R1(config-if)# tunnel protection ipsec profile DMVPN
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R1(config-if)# exi
```

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

```
R1(config)#router eigrp 145
R1(config-router)# network 172.16.145.1 0.0.0.0
R1(config-router)# network 192.168.12.1 0.0.0.0
R1(config-router)# no auto-summary
R1(config-router)# exi
```

Step 2 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# encr 3des
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R2(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R2(cfg-crypto-trans)# mode transport

R2(cfg-crypto-trans)#crypto ipsec profile DMVPN
R2(ipsec-profile)# set transform-set TSET
R2(ipsec-profile)#exi
```

There is only one Tunnel interface (GRE multipoint type) on each Hub.

```
R2(config)#interface Tunnel0
R2(config-if)# ip address 172.16.145.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip nhrp authentication cisco145
R2(config-if)# ip nhrp map multicast dynamic
R2(config-if)# ip nhrp network-id 145
R2(config-if)# no ip split-horizon eigrp 145
R2(config-if)# no ip next-hop-self eigrp 145
```

This is DMVPN Phase 2 with EIGRP scenario so that we need to turn off Split Horizon and next hop changing on the Hub.

```
R2(config-if)# tunnel source GigabitEthernet0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# tunnel key 145
R2(config-if)# tunnel protection ipsec profile DMVPN
R2(config-if)# exi
R2(config)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
```

```
R2(config)#router eigrp 145
R2(config-router)# no auto-summary
R2(config-router)# network 172.16.145.2 0.0.0.0
R2(config-router)# network 192.168.12.2 0.0.0.0
R2(config-router)# exit
R2(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 192.168.12.1
(FastEthernet0/1) is up: new adjacency
```

Step 3 R4 configuration.

```
R4(config)#crypto isakmp policy 1
R4(config-isakmp)# encr 3des
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R4(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R4(cfg-crypto-trans)# mode transport

R4(cfg-crypto-trans)#crypto ipsec profile DMVPN
R4(ipsec-profile)# set transform-set TSET
```

Note that all tunnels are in teh same subnet!

```
R4(ipsec-profile)#interface Tunnel0
R4(config-if)# ip address 172.16.145.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco145
R4(config-if)# ip nhrp map 172.16.145.1 10.1.16.1
R4(config-if)# ip nhrp map 172.16.145.2 10.1.26.2
R4(config-if)# ip nhrp map multicast 10.1.16.1
R4(config-if)# ip nhrp map multicast 10.1.26.2
```

Since we use two NHSes we need two static mappings on the spoke.

```
R4(config-if)# ip nhrp network-id 145
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.145.1
R4(config-if)# ip nhrp nhs 172.16.145.2
```

The spoke has only one multipoint tunnel, but two NHSes specified in the configuration. The spoke tries to register in both NHSes. When one NHS is down the spoke always has another NHS to use.

```
R4(config-if)# tunnel source Serial0/0/0.46
R4(config-if)# tunnel mode gre multipoint
```

```
R4(config-if)# tunnel key 145
R4(config-if)# tunnel protection ipsec profile DMVPN
R4(config-if)# exit
R4(config)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up

R4(config)#router eigrp 145
R4(config-router)# no auto-summary
R4(config-router)# network 172.16.145.4 0.0.0.0
R4(config-router)# network 192.168.4.4 0.0.0.0
R4(config-router)# exit
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.1 (Tunnel0)
is up: new adjacency
R4(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.2 (Tunnel0)
is up: new adjacency
```

Note that two EIGRP adjacencies are built.

Step 4 R5 configuration.

```
R5(config)#crypto isakmp policy 1
R5(config-isakmp)# encr 3des
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# group 2
R5(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R5(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R5(cfg-crypto-trans)# mode transport

R5(cfg-crypto-trans)#crypto ipsec profile DMVPN
R5(ipsec-profile)# set transform-set TSET

R5(ipsec-profile)#interface Tunnel0
R5(config-if)# ip address 172.16.145.5 255.255.255.0
R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco145
R5(config-if)# ip nhrp map 172.16.145.1 10.1.16.1
R5(config-if)# ip nhrp map 172.16.145.2 10.1.26.2
R5(config-if)# ip nhrp map multicast 10.1.16.1
R5(config-if)# ip nhrp map multicast 10.1.26.2
```

Since we use two NHSEs we need two static mappings on the spoke.

```
R5(config-if)# ip nhrp network-id 145
```

```
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.145.1
R5(config-if)# ip nhrp nhs 172.16.145.2
```

The spoke has only one multipoint tunnel, but two NHSes specified in the configuration. The spoke tries to register in both NHSes. When one NHS is down the spoke always has another NHS to use.

```
R5(config-if)# tunnel source Serial0/1/0.56
R5(config-if)# tunnel mode gre multipoint
R5(config-if)# tunnel key 145
R5(config-if)# tunnel protection ipsec profile DMVPN
R5(config-if)# exit
R5(config)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R5(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up

R5(config)#router eigrp 145
R5(config-router)# no auto-summary
R5(config-router)# network 172.16.145.5 0.0.0.0
R5(config-router)# network 192.168.5.5 0.0.0.0
R5(config-router)# exit
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.2 (Tunnel0)
is up: new adjacency
R5(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 145: Neighbor 172.16.145.1 (Tunnel0)
is up: new adjacency
```

Note that two EIGRP adjacencies are built.

Verification

R1#sh ip eigrp neighbors

IP-EIGRP neighbors for process 145

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q	Seq Cnt Num
2	172.16.145.5	Tu0	11 00:00:53	183	5000	0	6
1	172.16.145.4	Tu0	13 00:03:07	107	5000	0	10
0	192.168.12.2	Fa0/1	11 00:06:33	1	200	0	16

The hub has three EIGRP neighbors. Two of them are spokes and one is the other Hub. This is because we advertise a common network behind both Hubs to be accessible to the Spokes.

R1#sh ip eigrp interfaces

IP-EIGRP interfaces for process 145

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu0	2	0/0	145	71/2524	568	0
Fa0/1	1	0/0	1	0/1	50	0

R1#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.16.6 to network 0.0.0.0

```
C    192.168.12.0/24 is directly connected, FastEthernet0/1
    172.16.0.0/24 is subnetted, 1 subnets
C      172.16.145.0 is directly connected, Tunnel0
D    192.168.4.0/24 [90/27010560] via 192.168.12.2, 00:03:18, FastEthernet0/1
D    192.168.5.0/24 [90/27010560] via 192.168.12.2, 00:01:03, FastEthernet0/1
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.16.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.16.6
```

Note that R1 sees remote networks behind the Spokes through R2. This is expected as EIGRP metric is better for that path. This is certainly not the best path and need to be manually changed as described in the next lab. See the below output:

R1#sh int tu0 | in BW

MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,

R1#sh int f0/1 | in BW

MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

Note that the default bandwidth and delay of Tunnel interface is 9Kb/s and 500000usec. However, the default values on the FastEthernet interface are much better: 100000Kb/s and 100usec. This is why we see better metric to the network behind the spokes through the R2.

R1#sh ip route 192.168.4.0

Routing entry for 192.168.4.0/24

Known via "eigrp 145", distance 90, metric 27010560, type internal

Redistributing via eigrp 145

Last update from 192.168.12.2 on FastEthernet0/1, 00:00:14 ago

Routing Descriptor Blocks:

* 192.168.12.2, from 192.168.12.2, 00:00:14 ago, via FastEthernet0/1

```

Route metric is 27010560, traffic share count is 1
Total delay is 55100 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 2

```

R1#sh ip nhrp

```

172.16.145.4/32 via 172.16.145.4, Tunnel0 created 00:03:26, expire 00:05:41
  Type: dynamic, Flags: unique registered
  NBMA address: 10.1.64.4
172.16.145.5/32 via 172.16.145.5, Tunnel0 created 00:01:13, expire 00:04:46
  Type: dynamic, Flags: unique registered
  NBMA address: 10.1.65.5

```

First Hub has both Spokes registered via NHRP.

R1#sh crypto isakmp sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.16.1	10.1.64.4		ACTIVE	3des	sha	psk	2	23:56:28	
Engine-id:Conn-id = SW:1										
1002	10.1.16.1	10.1.65.5		ACTIVE	3des	sha	psk	2	23:58:40	
Engine-id:Conn-id = SW:2										

```
IPv6 Crypto ISAKMP SA
```

R1 has ISAKMP SA and IPSec SAs set up with both spokes. No IPSec between the Hubs.

R1#sh crypto ipsec sa

```

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.16.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
  current_peer 10.1.64.4 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 64, #pkts encrypt: 64, #pkts digest: 64
    #pkts decaps: 65, #pkts decrypt: 65, #pkts verify: 65
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0

```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.16.1, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x56A0EB85(1453386629)

inbound esp sas:
  spi: 0xEFBE50D1(4022227153)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4446287/3383)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x56A0EB85(1453386629)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4446287/3383)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
current_peer 10.1.65.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.16.1, remote crypto endpt.: 10.1.65.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xFAC2EC42(4207078466)
```

```

inbound esp sas:
spi: 0xD892939A(3633484698)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4579213/3515)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xFAC2EC42(4207078466)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4579213/3515)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```

R2#sh ip eigrp neighbors

IP-EIGRP neighbors for process 145

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
2	172.16.145.5	Tu0	11 00:01:39	135	1362	0	7
1	172.16.145.4	Tu0	14 00:03:52	160	1362	0	10
0	192.168.12.1	Gi0/1	13 00:07:19	1	200	0	16

The second Hub has neighbor adjacencies with two Spokes and the first Hub.

R2#sh ip eigrp interfaces

IP-EIGRP interfaces for process 145

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu0	2	0/0	147	6/227	348	0
Gi0/1	1	0/0	1	0/1	50	0

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.26.6 to network 0.0.0.0

```

C    192.168.12.0/24 is directly connected, GigabitEthernet0/1
    172.16.0.0/24 is subnetted, 1 subnets
C    172.16.145.0 is directly connected, Tunnel0
D    192.168.4.0/24 [90/27008000] via 172.16.145.4, 00:04:03, Tunnel0
D    192.168.5.0/24 [90/27008000] via 172.16.145.5, 00:01:49, Tunnel0
    10.0.0.0/24 is subnetted, 1 subnets
C    10.1.26.0 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.26.6
  
```

Since it has better metric to the remote networks than R1 it sees them by the Tunnel interface.

R2#sh ip nhrp

```

172.16.145.4/32 via 172.16.145.4
    Tunnel0 created 00:04:09, expire 00:04:57
    Type: dynamic, Flags: unique registered
    NBMA address: 10.1.64.4
172.16.145.5/32 via 172.16.145.5
    Tunnel0 created 00:01:57, expire 00:04:02
    Type: dynamic, Flags: unique registered
    NBMA address: 10.1.65.5
  
```

R2 has both Spokes registered in the NHS.

R2#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection
 K - Keepalives, N - NAT-traversal
 T - cTCP encapsulation, X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.26.2	10.1.64.4		ACTIVE	3des	sha	psk	2	23:55:44	
	Engine-id:Conn-id = SW:1									
1002	10.1.26.2	10.1.65.5		ACTIVE	3des	sha	psk	2	23:57:56	
	Engine-id:Conn-id = SW:2									

IPv6 Crypto ISAKMP SA

ISAKMP SA and IPSec SAs are built with both Spokes.

R2#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.26.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
current_peer 10.1.64.4 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 75, #pkts encrypt: 75, #pkts digest: 75
  #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.26.2, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x790BF682(2030827138)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x4D4D0F27(1296895783)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000006, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4411126/3339)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x790BF682(2030827138)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000006, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4411125/3339)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:
```

```
outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
current_peer 10.1.65.5 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 41, #pkts encrypt: 41, #pkts digest: 41
  #pkts decaps: 41, #pkts decrypt: 41, #pkts verify: 41
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.26.2, remote crypto endpt.: 10.1.65.5
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x73CE7CBE(1942912190)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x3454DCB6(877976758)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000006, crypto map:
Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4516057/3471)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x73CE7CBE(1942912190)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000006, crypto map:
Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4516057/3471)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R4#sh ip eigrp neighbors

IP-EIGRP neighbors for process 145

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
1	172.16.145.2	Tu0	13 00:04:38	22	5000	0	15
0	172.16.145.1	Tu0	12 00:04:38	71	5000	0	15

R4 is the Spoke. It has EIGRP adjacencies with both Hubs.

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.64.6 to network 0.0.0.0

```

D    192.168.12.0/24 [90/297246976] via 172.16.145.2, 00:04:44, Tunnel0
    [90/297246976] via 172.16.145.1, 00:04:44, Tunnel0
    172.16.0.0/24 is subnetted, 1 subnets
C    172.16.145.0 is directly connected, Tunnel0
C    192.168.4.0/24 is directly connected, Loopback0
D    192.168.5.0/24 [90/298652416] via 172.16.145.5, 00:02:29, Tunnel0
    10.0.0.0/24 is subnetted, 1 subnets
C    10.1.64.0 is directly connected, Serial0/0/0.46
S*   0.0.0.0/0 [1/0] via 10.1.64.6

```

The Spoke sees the network behind other Spoke (R5) through R5. This is because of "no ip next-hop-self eigrp" command configured on the Hubs. The network behind the Hubs is accessible equally via both Hubs.

R4#sh ip cef 192.168.5.0

192.168.5.0/24, version 25, epoch 0

0 packets, 0 bytes

via 172.16.145.5, Tunnel0, 0 dependencies

next hop 172.16.145.5, Tunnel0

invalid adjacency

The CEF entry is "invalid" as the router has no clue how to route the packet out (what physical interface to use).

R4#sh ip nhrp

172.16.145.1/32 via 172.16.145.1, Tunnel0 created 00:08:20, never expire

Type: static, Flags: used

NBMA address: 10.1.16.1

172.16.145.2/32 via 172.16.145.2, Tunnel0 created 00:08:20, never expire

Type: static, Flags: used

NBMA address: 10.1.26.2

Static NHRP entries are configured on the spoke to make registration happen in the NHSEs.

R4#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.64.4	10.1.26.2		ACTIVE	3des	sha	psk	2	23:54:24	
	Engine-id:Conn-id = SW:1									
1002	10.1.64.4	10.1.16.1		ACTIVE	3des	sha	psk	2	23:54:24	
	Engine-id:Conn-id = SW:2									

IPv6 Crypto ISAKMP SA

The spoke has ISAKMP Sa and IPSec SAs set up with both Hubs.

R4#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.64.4

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)

current_peer 10.1.16.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 93, #pkts encrypt: 93, #pkts digest: 93

#pkts decaps: 92, #pkts decrypt: 92, #pkts verify: 92

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 4, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.16.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46

current outbound spi: 0xEFBE50D1(4022227153)

inbound esp sas:

spi: 0x56A0EB85(1453386629)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4551007/3258)

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
```

```
spi: 0xEFBE50D1(4022227153)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4551007/3258)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
```

```
current_peer 10.1.26.2 port 500
```

```
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 92, #pkts encrypt: 92, #pkts digest: 92
```

```
#pkts decaps: 94, #pkts decrypt: 94, #pkts verify: 94
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 3, #recv errors 0
```

```
local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.26.2
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
```

```
current outbound spi: 0x4D4D0F27(1296895783)
```

```
inbound esp sas:
```

```
spi: 0x790BF682(2030827138)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4590970/3258)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
spi: 0x4D4D0F27(1296895783)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4590971/3258)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

R4# ping 192.168.5.5 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:

Packet sent with a source address of 192.168.4.4

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 84/96/108 ms

Test it by pinging the remote network behind the other Spoke. The ping is successful.

R4#sh ip cef 192.168.5.0

192.168.5.0/24, version 25, epoch 0

0 packets, 0 bytes

via 172.16.145.5, Tunnel0, 0 dependencies

next hop 172.16.145.5, Tunnel0

valid adjacency

The CEF entry is "valid" now, so that the router can use it to switch the packets through the direct spoke-to-spoke tunnel.

R4#sh ip nhrp

172.16.145.1/32 via 172.16.145.1, Tunnel0 created 00:08:55, never expire

Type: static, Flags: used

NBMA address: 10.1.16.1

172.16.145.2/32 via 172.16.145.2, Tunnel0 created 00:08:55, never expire

Type: static, Flags: used

NBMA address: 10.1.26.2

172.16.145.4/32 via 172.16.145.4, Tunnel0 created 00:00:09, expire 00:05:51

Type: dynamic, Flags: router unique local

NBMA address: 10.1.64.4

(no-socket)

172.16.145.5/32 via 172.16.145.5, Tunnel0 created 00:00:10, expire 00:05:51

Type: dynamic, Flags: router

NBMA address: 10.1.65.5

NHRP cache now has an entry for the other spoke.

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
10.1.64.4	10.1.65.5	QM_IDLE	1003	0	ACTIVE
10.1.26.2	10.1.64.4	QM_IDLE	1001	0	ACTIVE
10.1.65.5	10.1.64.4	QM_IDLE	1004	0	ACTIVE
10.1.16.1	10.1.64.4	QM_IDLE	1002	0	ACTIVE

IPv6 Crypto ISAKMP SA

The Spoke has new ISAKMP SA and IPsec SAs negotiated with the other Spoke.

R4#sh crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.64.4

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)

current_peer 10.1.16.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 106, #pkts encrypt: 106, #pkts digest: 106

#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 4, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.16.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46

current outbound spi: 0xEFBE50D1(4022227153)

inbound esp sas:

spi: 0x56A0EB85(1453386629)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4551006/3225)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xEFBE50D1(4022227153)

```
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4551006/3225)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
current_peer 10.1.26.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 99, #pkts encrypt: 99, #pkts digest: 99
#pkts decaps: 106, #pkts decrypt: 106, #pkts verify: 106
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 3, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.26.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x4D4D0F27(1296895783)
```

inbound esp sas:

```
spi: 0x790BF682(2030827138)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4590968/3225)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```
spi: 0x4D4D0F27(1296895783)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4590970/3225)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)

current_peer 10.1.65.5 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2

#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

Two packets out of 5 have been sent through the tunnel.

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.65.5

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46

current outbound spi: 0xA576BA01(2776021505)

inbound esp sas:

spi: 0xBBA03823(3147839523)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2005, flow_id: NETGX:5, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4584005/3578)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

spi: 0x28F30861(687016033)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2007, flow_id: NETGX:7, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4403135/3579)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xA576BA01(2776021505)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2006, flow_id: NETGX:6, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4584005/3578)

```

    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
spi: 0x1659D9A5(374987173)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2008, flow_id: NETGX:8, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4403135/3579)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

Same bunch of commands on the other Spoke.

R5#sh ip eigrp neighbors

IP-EIGRP neighbors for process 145

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
1	172.16.145.1	Tu0	10 00:04:23	69	5000	0	15
0	172.16.145.2	Tu0	13 00:04:23	842	5000	0	15

R5#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.65.6 to network 0.0.0.0

```

D    192.168.12.0/24 [90/297246976] via 172.16.145.2, 00:04:33, Tunnel0
      [90/297246976] via 172.16.145.1, 00:04:33, Tunnel0
    172.16.0.0/24 is subnetted, 1 subnets
C      172.16.145.0 is directly connected, Tunnel0
D    192.168.4.0/24 [90/298652416] via 172.16.145.4, 00:04:33, Tunnel0
C    192.168.5.0/24 is directly connected, Loopback0
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.65.0 is directly connected, Serial0/1/0.56
S*   0.0.0.0/0 [1/0] via 10.1.65.6

```

R5#sh ip route 192.168.4.0

Routing entry for 192.168.4.0/24

Known via "eigrp 145", distance 90, metric 298652416, type internal

```
Redistributing via eigrp 145
Last update from 172.16.145.4 on Tunnel0, 00:04:38 ago
Routing Descriptor Blocks:
* 172.16.145.4, from 172.16.145.2, 00:04:38 ago, via Tunnel0
  Route metric is 298652416, traffic share count is 1
  Total delay is 555000 microseconds, minimum bandwidth is 9 Kbit
  Reliability 255/255, minimum MTU 1400 bytes
  Loading 28/255, Hops 2
```

R5#sh ip nhrp

```
172.16.145.1/32 via 172.16.145.1, Tunnel0 created 00:04:48, never expire
  Type: static, Flags: used
  NBMA address: 10.1.16.1
172.16.145.2/32 via 172.16.145.2, Tunnel0 created 00:04:48, never expire
  Type: static, Flags: used
  NBMA address: 10.1.26.2
172.16.145.4/32 via 172.16.145.4, Tunnel0 created 00:01:06, expire 00:04:54
  Type: dynamic, Flags: router
  NBMA address: 10.1.64.4
172.16.145.5/32 via 172.16.145.5, Tunnel0 created 00:01:06, expire 00:04:54
  Type: dynamic, Flags: router unique local
  NBMA address: 10.1.65.5
(no-socket)
```

Since we have already built up the direct spoke-to-spoke tunnel, the router has NHRP mappings and CEF entry which are used to move the packets through that tunnel.

R5#sh ip cef 192.168.4.0

```
192.168.4.0/24, version 23, epoch 0
0 packets, 0 bytes
  via 172.16.145.4, Tunnel0, 0 dependencies
    next hop 172.16.145.4, Tunnel0
    valid adjacency
```

R5#sh crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	slot	status
10.1.65.5	10.1.64.4	QM_IDLE	1003	0	ACTIVE
10.1.64.4	10.1.65.5	QM_IDLE	1004	0	ACTIVE
10.1.26.2	10.1.65.5	QM_IDLE	1001	0	ACTIVE
10.1.16.1	10.1.65.5	QM_IDLE	1002	0	ACTIVE

```
IPv6 Crypto ISAKMP SA
```

R5#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.65.5

protected vrf: (none)
```



```
local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
current_peer 10.1.16.1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
#pkts decaps: 76, #pkts decrypt: 76, #pkts verify: 76
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.16.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0xD892939A(3633484698)

inbound esp sas:
  spi: 0xFAC2EC42(4207078466)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4605793/3299)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xD892939A(3633484698)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4605792/3299)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
current_peer 10.1.26.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 79, #pkts encrypt: 79, #pkts digest: 79
#pkts decaps: 84, #pkts decrypt: 84, #pkts verify: 84
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.26.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0x3454DCB6(877976758)

inbound esp sas:
  spi: 0x73CE7CBE(1942912190)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4455804/3299)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x3454DCB6(877976758)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4455805/3299)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
current_peer 10.1.64.4 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

Note that only two packets has been sent.

```
local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.64.4
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0xBBA03823(3147839523)

inbound esp sas:
  spi: 0xA576BA01(2776021505)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2007, flow_id: NETGX:7, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4493287/3520)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xBBA03823(3147839523)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2008, flow_id: NETGX:8, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4493287/3520)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R5#ping 192.168.4.4 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.5
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/78/80 ms
```

Let's ping and generate some traffic.

R5#sh crypto ipsec sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.65.5

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
current_peer 10.1.16.1 port 500
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 89, #pkts encrypt: 89, #pkts digest: 89
#pkts decaps: 80, #pkts decrypt: 80, #pkts verify: 80
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.16.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0xD892939A(3633484698)

inbound esp sas:
  spi: 0xFAC2EC42(4207078466)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4605793/3278)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0xD892939A(3633484698)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4605792/3278)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
current_peer 10.1.26.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
#pkts decaps: 89, #pkts decrypt: 89, #pkts verify: 89
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.26.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0x3454DCB6(877976758)
```

inbound esp sas:

```
spi: 0x73CE7CBE(1942912190)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4455804/3278)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```
spi: 0x3454DCB6(877976758)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4455805/3278)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

current_peer 10.1.64.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7

#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

See the ICMP packets are crossing the tunnel.

```
local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0xBBA03823(3147839523)
```

inbound esp sas:

```
spi: 0xA576BA01(2776021505)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2007, flow_id: NETGX:7, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4493286/3499)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

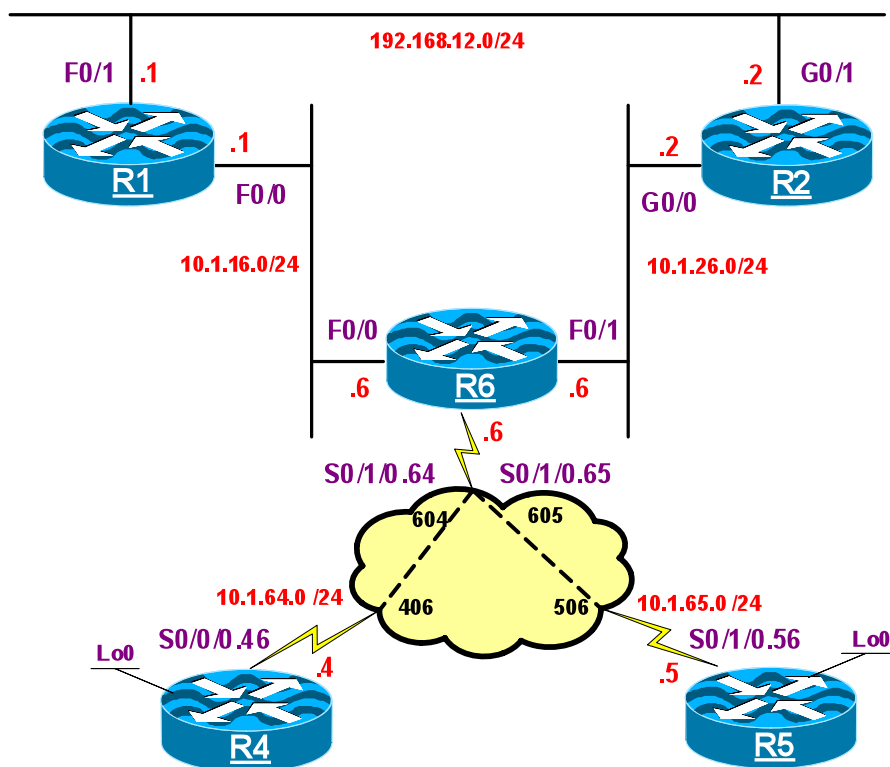
outbound esp sas:

```
spi: 0xBBA03823(3147839523)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2008, flow_id: NETGX:8, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4493286/3499)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

Lab 1.55. DMVPN Phase 2 Dual Hub (Dual Cloud)



Depending on IOS software version you may get slightly different command outputs. This is because CEF code has changed in IOS 12.2(20)T.

Lab Setup

- R1's F0/0 and R6's F0/0 interface should be configured in VLAN 16
- R1's F0/1 and R2's G0/1 interface should be configured in VLAN 12
- R2's G0/0 and R6's F0/1 interface should be configured in VLAN 26
- R6's S0/1/0 and R4's S0/0/0 interface should be configured in a frame-relay point-to-point manner.
- R6's S0/1/0 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R2, R4 and R5 pointing to the R6

IP Addressing

Device	Interface	IP address
R1	F0/0	10.1.16.1/24
	F0/1	192.168.12.1/24
R2	G0/0	10.1.26.2/24
	G0/1	192.168.12.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0.46	10.1.64.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0.56	10.1.65.5/24
R6	F0/0	10.1.16.6/24
	F0/1	10.1.26.6/24
	S0/1/0.64	10.1.64.6/24
	S0/1/0.65	10.1.65.6/24

Task 1

Configure Hub-and-Spoke GRE tunnels between R1, R2, R4 and R5, where R1 and R2 are acting as Hubs. High availability must be achieved by configuring two DMVPN clouds, meaning each spoke has two connections, one for each hub, where tunnel to R1 has better preference than R2. Traffic originated from every Spoke's loopback interface should be transmitted securely directly to the other spokes. You must use EIGRP dynamic routing protocol to let other spokes know about protected networks.

Use the following settings when configuring tunnels:

DMVPN Cloud 1	DMVPN Cloud 2
Topology • Hub: R1 • Spokes: R4, R5	Topology • Hub: R2 • Spokes: R4, R5

Tunnel Parameters • IP address: 172.16.145.0/24 • IP MTU: 1400 • Tunnel Authentication Key: 145 NHRP Parameters • NHRP ID: 145 • NHRP Authentication key: cisco145 • NHRP Hub: R1 Routing Protocol Parameters • EIGRP AS 1 • Delay 1000	Tunnel Parameters • IP address: 172.16.245.0/24 • IP MTU: 1400 • Tunnel Authentication Key: 245 NHRP Parameters • NHRP ID: 245 • NHRP Authentication key: cisco245 • NHRP Hub: R2 Routing Protocol Parameters • EIGRP AS 1 • Delay 2000

Encrypt the GRE traffic using the following parameters:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Encryption: 3DES
 - Hashing: SHA
 - DH Group: 2
 - Pre-Shared Key: cisco123
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC



The dual hub with dual DMVPN layout is slightly more difficult to set up, but it does give you better control of the routing across the DMVPN. The idea is to have a two separate DMVPN "clouds". Each hub (two in this case) is connected to one DMVPN subnet ("cloud") and the spokes are connected to both DMVPN subnets ("clouds"). Since the spoke routers are routing neighbors with both hub routers over the two GRE tunnel interfaces, you can use interface configuration differences (such as bandwidth, cost and delay) to modify the dynamic routing protocol metrics to prefer one hub over the other hub when they are both up.

Configuration

Complete these steps:

Step 1 R1 configuration.

Almost nothing has changed on the first Hub in comparison to DMVPN Single Cloud scenario described in the previous lab.

The one difference here is to use different IP subnets for Tunnel interface on both Hubs. This is because we create two "clouds" which must be separated.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# encr 3des
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R1(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)# mode transport

R1(cfg-crypto-trans)#crypto ipsec profile DMVPN
R1(ipsec-profile)# set transform-set TSET

R1(ipsec-profile)#interface Tunnel0
R1(config-if)# ip address 172.16.145.1 255.255.255.0
R1(config-if)# ip mtu 1400
R1(config-if)# ip nhrp authentication cisco145
R1(config-if)# ip nhrp map multicast dynamic
R1(config-if)# ip nhrp network-id 145
R1(config-if)# no ip split-horizon eigrp 1
R1(config-if)# no ip next-hop-self eigrp 1
R1(config-if)# tunnel source FastEthernet0/0
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# tunnel key 145
R1(config-if)# tunnel protection ipsec profile DMVPN
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R1(config-if)# exi
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

R1(config)#router eigrp 1
R1(config-router)# network 172.16.145.1 0.0.0.0
R1(config-router)# network 192.168.12.1 0.0.0.0
R1(config-router)# no auto-summary
R1(config-router)# exi
```

Note that we used EIGRP AS 1 which will be "shared" between both DMVPN clouds. This may be achieved by configuring two EIGRP Autonomous Systems as well.

Step 2 R2 configuration.

Almost nothing has changed on the second Hub in comparison to DMVPN Single Cloud scenario described in the previous lab.

The one difference here is to use different IP subnets for Tunnel interface on both Hubs. This is because we create two "clouds" which must be separated.

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)# encr 3des
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R2(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R2(cfg-crypto-trans)# mode transport

R2(cfg-crypto-trans)#crypto ipsec profile DMVPN
R2(ipsec-profile)# set transform-set TSET
R2(ipsec-profile)#exit

R2(config)#interface Tunnel0
R2(config-if)# ip address 172.16.245.2 255.255.255.0
R2(config-if)# no ip redirects
R2(config-if)# ip mtu 1400
R2(config-if)# no ip next-hop-self eigrp 1
R2(config-if)# no ip split-horizon eigrp 1
R2(config-if)# ip nhrp authentication cisco245
R2(config-if)# ip nhrp map multicast dynamic
R2(config-if)# ip nhrp network-id 245
R2(config-if)# tunnel source FastEthernet0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# tunnel key 245
R2(config-if)# tunnel protection ipsec profile DMVPN
R2(config-if)# exit
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

R2(config)#router eigrp 1
R2(config-router)# no auto-summary
R2(config-router)# network 172.16.245.2 0.0.0.0
R2(config-router)# network 192.168.12.2 0.0.0.0
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.12.1
(GigabitEthernet0/1) is up: new adjacency
```

```
R2(config-router)#exi
```

Note that we used EIGRP AS 1 which will be "shared" between both DMVPN clouds. This may be achieved by configuring two EIGRP Autonomous Systems as well.

The second Hub has built neighbor relationship with the first Hub.

Step 3 R4 configuration.

```
R4(config)#crypto isakmp policy 1
R4(config-isakmp)# encr 3des
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# group 2
R4(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R4(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R4(cfg-crypto-trans)# mode transport

R4(cfg-crypto-trans)#crypto ipsec profile DMVPN
R4(ipsec-profile)# set transform-set TSET
```

On the spokes we need two Tunnel interfaces: one for each DMVPN cloud. The first cloud will be using R1 as a Hub, the second cloud will be using R2 as a Hub.

```
R4(config)#interface Tunnel1
R4(config-if)# ip address 172.16.145.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco145
R4(config-if)# ip nhrp map 172.16.145.1 10.1.16.1
R4(config-if)# ip nhrp map multicast 10.1.16.1
R4(config-if)# ip nhrp network-id 145
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.145.1
R4(config-if)# tunnel source Serial0/0/0.46
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# tunnel key 145
R4(config-if)# tunnel protection ipsec profile DMVPN shared
```

Note that we need different NHRP ID and Tunnel Keys for both clouds. This is to separate the traffic (as it is terminated on the same Hub).

Although, the tunnel key can separate the traffic at GRE level, the IPSec Profile is "shared" in this case. This means the one profile is used to secure two tunnel interfaces. Hence, there must be "shared" keyword added on the spokes.

```

R4(config-if)# exit

R4(config)#interface Tunnel2
R4(config-if)# ip address 172.16.245.4 255.255.255.0
R4(config-if)# ip mtu 1400
R4(config-if)# ip nhrp authentication cisco245
R4(config-if)# ip nhrp map 172.16.245.2 10.1.26.2
R4(config-if)# ip nhrp map multicast 10.1.26.2
R4(config-if)# ip nhrp network-id 245
R4(config-if)# ip nhrp holdtime 360
R4(config-if)# ip nhrp nhs 172.16.245.2
R4(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R4(config-if)# tunnel source Serial0/0/0.46
R4(config-if)# tunnel mode gre multipoint
R4(config-if)# tunnel key 245
R4(config-if)# tunnel protection ipsec profile DMVPN shared
R4(config-if)# exit

```

Note that we need different NHRP ID and Tunnel Keys for both clouds. This is to separate the traffic (as it is terminated on the same Hub).

Although, the tunnel key can separate the traffic at GRE level, the IPSec Profile is "shared" in this case. This means the one profile is used to secure two tunnel interfaces. Hence, there must be "shared" keyword added on the spokes.

```

R4(config)#router eigrp 1
R4(config-router)# network 172.16.145.4 0.0.0.0
R4(config-router)# network 172.16.245.4 0.0.0.0
R4(config-router)# network 192.168.4.4 0.0.0.0
R4(config-router)# no auto-summary
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.145.1 (Tunnel1)
is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.245.2 (Tunnel2)
is up: new adjacency
R4(config-router)#exit

```

Step 4 R5 configuration.

```

R5(config)#crypto isakmp policy 1
R5(config-isakmp)# encr 3des
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)# group 2
R5(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0

R5(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R5(cfg-crypto-trans)# mode transport

```

```
R5(cfg-crypto-trans)#crypto ipsec profile DMVPN
R5(ipsec-profile)# set transform-set TSET
R5(ipsec-profile)#exi
```

```
R5(config)#interface Tunnel1
R5(config-if)# ip address 172.16.145.5 255.255.255.0
R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco145
R5(config-if)# ip nhrp map 172.16.145.1 10.1.16.1
R5(config-if)# ip nhrp map multicast 10.1.16.1
R5(config-if)# ip nhrp network-id 145
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.145.1
R5(config-if)# tunnel source Serial0/1/0.56
R5(config-if)# tunnel mode gre multipoint
R5(config-if)# tunnel key 145
R5(config-if)# tunnel protection ipsec profile DMVPN shared
```

Note that we need different NHRP ID and Tunnel Keys for both clouds. This is to separate the traffic (as it is terminated on the same Hub).

Although, the tunnel key can separate the traffic at GRE level, the IPSec Profile is "shared" in this case. This means the one profile is used to secure two tunnel interfaces. Hence, there must be "shared" keyword added on the spokes.

```
R5(config-if)# exi
```

```
R5(config)#interface Tunnel2
R5(config-if)# ip address 172.16.245.5 255.255.255.0
R5(config-if)# ip mtu 1400
R5(config-if)# ip nhrp authentication cisco245
R5(config-if)# ip nhrp map 172.16.245.2 10.1.26.2
R5(config-if)# ip nhrp map multicast 10.1.26.2
R5(config-if)# ip nhrp network-id 245
R5(config-if)# ip nhrp holdtime 360
R5(config-if)# ip nhrp nhs 172.16.245.2
R5(config-if)# tunnel source Serial0/1/0.56
R5(config-if)# tunnel mode gre multipoint
R5(config-if)# tunnel key 245
R5(config-if)# tunnel protection ipsec profile DMVPN shared
```

Note that we need different NHRP ID and Tunnel Keys for both clouds. This is to separate the traffic (as it is terminated on the same Hub).

Although, the tunnel key can separate the traffic at GRE level, the IPSec Profile is "shared" in this case. This means the one profile is used to secure two tunnel interfaces. Hence, there must be "shared" keyword added on

the spokes.

```
R5(config)#router eigrp 1
R5(config-router)# network 172.16.145.5 0.0.0.0
R5(config-router)# network 172.16.245.5 0.0.0.0
R5(config-router)# network 192.168.5.5 0.0.0.0
R5(config-router)# no auto-summary
R5(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.145.1 (Tunnel1)
is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.245.2 (Tunnel2)
is up: new adjacency
R5(config-router)#exi
```

Note that we have not configured “delay” parameters yet. This is just to show you what happen and how to troubleshoot that issues.

Verification

R4#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 10.1.64.6 to network 0.0.0.0

```
D 192.168.12.0/24 [90/297246976] via 172.16.245.2, 00:10:28, Tunnel2
   [90/297246976] via 172.16.145.1, 00:10:28, Tunnel1
172.16.0.0/24 is subnetted, 2 subnets
C    172.16.145.0 is directly connected, Tunnel1
C    172.16.245.0 is directly connected, Tunnel2
C    192.168.4.0/24 is directly connected, Loopback0
D 192.168.5.0/24 [90/298652416] via 172.16.245.5, 00:09:03, Tunnel2
10.0.0.0/24 is subnetted, 1 subnets
C    10.1.64.0 is directly connected, Serial0/0/0.46
S*  0.0.0.0/0 [1/0] via 10.1.64.6
```

See that network 192.168.5.0/24 is accessible through R2 (Tunnel2) only. Why is that? Let's see what EIGRP tells us.

R4#sh ip route 192.168.5.0

```
Routing entry for 192.168.5.0/24
  Known via "eigrp 1", distance 90, metric 298652416, type internal
  Redistributing via eigrp 1
```

Last update from 172.16.245.5 on Tunnel2, 00:09:17 ago

Routing Descriptor Blocks:

* 172.16.245.5, from 172.16.245.2, 00:09:17 ago, via Tunnel2

Route metric is 298652416, traffic share count is 1

Total delay is 555000 microseconds, minimum bandwidth is 9 Kbit

Reliability 255/255, minimum MTU 1400 bytes

Loading 1/255, Hops 2

R4#sh ip eigrp topology 192.168.5.0

IP-EIGRP (AS 1): Topology entry for 192.168.5.0/24

State is Passive, Query origin flag is 1, 1 Successor(s), FD is 298652416

Routing Descriptor Blocks:

172.16.245.5 (Tunnel2), from 172.16.245.2, Send flag is 0x0

Composite metric is (298652416/27008000), Route is Internal

Vector metric:

Minimum bandwidth is 9 Kbit

Total delay is 555000 microseconds

Reliability is 255/255

Load is 1/255

Minimum MTU is 1400

Hop count is 2

172.16.145.1 (Tunnell), from 172.16.145.1, Send flag is 0x0

Composite metric is (298654976/27010560), Route is Internal

Vector metric:

Minimum bandwidth is 9 Kbit

Total delay is 555100 microseconds

Reliability is 255/255

Load is 1/255

Minimum MTU is 1400

Hop count is 3

EIGRP topology table contains both paths to 192.168.5.0/24, however it only installs the first one in the routing table. See the Delay parameter, it is higher for the second path (through Tunnell). See also Hop parameter which is again higher for the second path. Although, the EIGRP does not use that parameter for metric calculation it indicates that the path is longer. Let's take a look at R1:

R1#sh ip route 192.168.5.0

Routing entry for 192.168.5.0/24

Known via "eigrp 1", distance 90, metric 27010560, type internal

Redistributing via eigrp 1

Last update from 192.168.12.2 on FastEthernet0/1, 00:17:44 ago

Routing Descriptor Blocks:

* 192.168.12.2, from 192.168.12.2, 00:17:44 ago, via FastEthernet0/1

Route metric is 27010560, traffic share count is 1

Total delay is 55100 microseconds, minimum bandwidth is 100 Kbit

Reliability 255/255, minimum MTU 1400 bytes

Loading 1/255, Hops 2

The R1 sees 192.168.5.0/24 through R2, not through its Tunnel interface. Hence, the metric on R4 is higher as the packet must traverse 3 hops to reach the destination.

R4#sh ip route 192.168.12.0

```
Routing entry for 192.168.12.0/24
  Known via "eigrp 1", distance 90, metric 297246976, type internal
  Redistributing via eigrp 1
  Last update from 172.16.245.2 on Tunnel2, 00:11:00 ago
  Routing Descriptor Blocks:
    172.16.245.2, from 172.16.245.2, 00:11:00 ago, via Tunnel2
      Route metric is 297246976, traffic share count is 1
      Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 1
    * 172.16.145.1, from 172.16.145.1, 00:11:00 ago, via Tunnel1
      Route metric is 297246976, traffic share count is 1
      Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 1
```

R4#sh int tu1 | in BW

```
MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
```

R4#sh int tu2 | in BW

```
MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
```

R5#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 10.1.65.6 to network 0.0.0.0
```

```
D    192.168.12.0/24 [90/297246976] via 172.16.245.2, 00:10:31, Tunnel2
      [90/297246976] via 172.16.145.1, 00:10:31, Tunnel1
    172.16.0.0/24 is subnetted, 2 subnets
C      172.16.145.0 is directly connected, Tunnel1
C      172.16.245.0 is directly connected, Tunnel2
D    192.168.4.0/24 [90/298652416] via 172.16.245.4, 00:10:31, Tunnel2
C    192.168.5.0/24 is directly connected, Loopback0
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.65.0 is directly connected, Serial0/1/0.56
S*    0.0.0.0/0 [1/0] via 10.1.65.6
```

R5#sh ip route 192.168.4.0

```
Routing entry for 192.168.4.0/24
  Known via "eigrp 1", distance 90, metric 298652416, type internal
  Redistributing via eigrp 1
  Last update from 172.16.245.4 on Tunnel2, 00:10:39 ago
  Routing Descriptor Blocks:
    * 172.16.245.4, from 172.16.245.2, 00:10:39 ago, via Tunnel2
      Route metric is 298652416, traffic share count is 1
      Total delay is 555000 microseconds, minimum bandwidth is 9 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 2
```

Same situation here. The 192.168.4.0/24 is accessible through Tunnel2 interface rather than Tunnel1.

R5#sh ip eigrp topology 192.168.4.0

```
IP-EIGRP (AS 1): Topology entry for 192.168.4.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 298652416
  Routing Descriptor Blocks:
    172.16.245.4 (Tunnel2), from 172.16.245.2, Send flag is 0x0
      Composite metric is (298652416/27008000), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 555000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 2
    172.16.145.1 (Tunnel1), from 172.16.145.1, Send flag is 0x0
      Composite metric is (298654976/27010560), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 555100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 3
```

R5#sh ip route 192.168.12.0

```
Routing entry for 192.168.12.0/24
  Known via "eigrp 1", distance 90, metric 297246976, type internal
  Redistributing via eigrp 1
  Last update from 172.16.245.2 on Tunnel2, 00:11:00 ago
  Routing Descriptor Blocks:
    172.16.245.2, from 172.16.245.2, 00:11:00 ago, via Tunnel2
      Route metric is 297246976, traffic share count is 1
      Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 1
    * 172.16.145.1, from 172.16.145.1, 00:11:00 ago, via Tunnel1
      Route metric is 297246976, traffic share count is 1
      Total delay is 500100 microseconds, minimum bandwidth is 9 Kbit
```

Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1

R5#sh int tu1 | in BW

MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,

R5#sh int tu2 | in BW

MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,

Configuration

To optimize that we need to reconfigure Delay parameter on tunnel interfaces. It affects EIGRP protocol algorithm so that the better path will always be through R1 (as long as R1 is up and running). We could also affect EIGRP decision by reconfiguring Bandwidth parameters but this should be done on every interface as BW parameter is NOT cumulative. This means the minimum bandwidth on the path is taken for metric calculation. Delay is cumulative so that less delay on one interface affects every EIGRP router.

Complete these steps:

Step 5 R1 configuration.

```
R1(config)#interface Tunnel0
R1(config-if)#delay 1000
R1(config-if)#exi
```

Step 6 R2 configuration.

```
R2(config)#interface Tunnel0
R2(config-if)#delay 2000
R2(config-if)#exi
```

Step 7 R4 configuration.

```
R4(config)#interface Tunnel1
R4(config-if)#delay 1000
R4(config-if)#exi

R4(config)#interface Tunnel2
R4(config-if)#delay 2000
R4(config-if)#exi
```

Step 8 R5 configuration.

```
R5(config)#interface Tunnel1
R5(config-if)#delay 1000
R5(config-if)#exi
```

```
R5(config)#interface Tunnel2
R5(config-if)#delay 2000
R5(config-if)#exi
```

Verification

R1#sh ip ro

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.16.6 to network 0.0.0.0

```
C    192.168.12.0/24 is directly connected, FastEthernet0/1
    172.16.0.0/24 is subnetted, 2 subnets
C      172.16.145.0 is directly connected, Tunnel0
D      172.16.245.0
        [90/284958976] via 192.168.12.2, 00:11:23, FastEthernet0/1
D    192.168.4.0/24 [90/284828416] via 172.16.145.4, 00:11:37, Tunnel0
D    192.168.5.0/24 [90/284828416] via 172.16.145.5, 00:11:37, Tunnel0
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.16.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.1.16.6
```

Now both spokes are accessible through the tunnel interface (not through R2).

R1#sh ip nhrp

```
172.16.145.4/32 via 172.16.145.4, Tunnel0 created 00:13:08, expire 00:04:30
  Type: dynamic, Flags: unique registered
  NBMA address: 10.1.64.4
172.16.145.5/32 via 172.16.145.5, Tunnel0 created 00:13:12, expire 00:04:46
  Type: dynamic, Flags: unique registered
  NBMA address: 10.1.65.5
```

Both spokes are registered in NHS.

R1#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
10.1.16.1	10.1.65.5	QM_IDLE	1001	0	ACTIVE
10.1.16.1	10.1.64.4	QM_IDLE	1002	0	ACTIVE

IPv6 Crypto ISAKMP SA

The Hub has ISAKMP SA and IPSec SAs set up with the spokes.**R1#sh crypto ipsec sa**

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 10.1.16.1

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

current_peer 10.1.64.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 185, #pkts encrypt: 185, #pkts digest: 185

#pkts decaps: 188, #pkts decrypt: 188, #pkts verify: 188

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.16.1, remote crypto endpt.: 10.1.64.4

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xE5EB2CDE(3857394910)

inbound esp sas:

spi: 0x84A95ADB(2225691355)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2003, flow_id: NETGX:3, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4454946/2801)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xE5EB2CDE(3857394910)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2004, flow_id: NETGX:4, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4454946/2801)

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
current_peer 10.1.65.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 189, #pkts encrypt: 189, #pkts digest: 189
#pkts decaps: 190, #pkts decrypt: 190, #pkts verify: 190
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.1.16.1, remote crypto endpt.: 10.1.65.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x34369DE1(875994593)
```

inbound esp sas:

```
spi: 0x2E6FCA3E(779078206)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4407002/2796)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```
spi: 0x34369DE1(875994593)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4407002/2796)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.26.6 to network 0.0.0.0

```
C    192.168.12.0/24 is directly connected, GigabitEthernet0/1
    172.16.0.0/24 is subnetted, 2 subnets
D    172.16.145.0
        [90/284702976] via 192.168.12.1, 00:13:06, GigabitEthernet0/1
C    172.16.245.0 is directly connected, Tunnel0
D    192.168.4.0/24
        [90/284830976] via 192.168.12.1, 00:13:06, GigabitEthernet0/1
D    192.168.5.0/24
        [90/284830976] via 192.168.12.1, 00:13:06, GigabitEthernet0/1
    10.0.0.0/24 is subnetted, 1 subnets
C    10.1.26.0 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.26.6
```

Now the second Hub is less preferred. It has networks behind the spokes accessible via R1. This is because EIGRP metric was affected and recalculated.

R2#sh ip eigr top 192.168.4.0

```
IP-EIGRP (AS 1): Topology entry for 192.168.4.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 284830976
Routing Descriptor Blocks:
192.168.12.1 (GigabitEthernet0/1), from 192.168.12.1, Send flag is 0x0
  Composite metric is (284830976/284828416), Route is Internal
  Vector metric:
    Minimum bandwidth is 9 Kbit
    Total delay is 15100 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1400
    Hop count is 2
172.16.245.5 (Tunnel0), from 172.16.245.5, Send flag is 0x0
  Composite metric is (285596416/285084416), Route is Internal
  Vector metric:
    Minimum bandwidth is 9 Kbit
    Total delay is 45000 microseconds
    Reliability is 255/255
    Load is 28/255
```

```

    Minimum MTU is 1400
    Hop count is 3
172.16.245.4 (Tunnel0), from 172.16.245.4, Send flag is 0x0
    Composite metric is (285084416/128256), Route is Internal
Vector metric:
    Minimum bandwidth is 9 Kbit
    Total delay is 25000 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1400
    Hop count is 1

```

R2#sh ip nhrp

```

172.16.245.4/32 via 172.16.245.4, Tunnel0 created 00:13:28, expire 00:05:50
    Type: dynamic, Flags: unique registered used
    NBMA address: 10.1.64.4
172.16.245.5/32 via 172.16.245.5, Tunnel0 created 00:13:22, expire 00:05:56
    Type: dynamic, Flags: unique registered used
    NBMA address: 10.1.65.5

```

Both spokes are registered in the NHS.

R2#sh crypto isakmp sa

```

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.1.26.2    10.1.65.5    QM_IDLE        1002     0 ACTIVE
10.1.26.2    10.1.64.4    QM_IDLE        1001     0 ACTIVE

IPv6 Crypto ISAKMP SA

```

It also maintains ISAKMP SA nad IPSec SAs with the spokes.

R2#sh crypto ipsec sa

```

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.26.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
current_peer 10.1.64.4 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 194, #pkts encrypt: 194, #pkts digest: 194
    #pkts decaps: 193, #pkts decrypt: 193, #pkts verify: 193
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

```



```
local crypto endpt.: 10.1.26.2, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x6A0C9367(1779209063)

inbound esp sas:
  spi: 0x77BC473A(2008827706)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2003, flow_id: Onboard VPN:3, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4411618/2779)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x6A0C9367(1779209063)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2004, flow_id: Onboard VPN:4, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4411618/2779)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
current_peer 10.1.65.5 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 189, #pkts encrypt: 189, #pkts digest: 189
  #pkts decaps: 191, #pkts decrypt: 191, #pkts verify: 191
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 10.1.26.2, remote crypto endpt.: 10.1.65.5
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0xE70EAE04(3876498948)

inbound esp sas:
  spi: 0xE97C1EE8(3917225704)
    transform: esp-3des esp-sha-hmac ,
```

```

in use settings ={Transport, }
conn id: 2007, flow_id: Onboard VPN:7, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4433019/2785)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xE70EAE04(3876498948)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2008, flow_id: Onboard VPN:8, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4433019/2785)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.64.6 to network 0.0.0.0

```

D 192.168.12.0/24 [90/284702976] via 172.16.145.1, 00:13:53, Tunnel1
  172.16.0.0/24 is subnetted, 2 subnets
C    172.16.145.0 is directly connected, Tunnel1
C    172.16.245.0 is directly connected, Tunnel2
C    192.168.4.0/24 is directly connected, Loopback0
D 192.168.5.0/24 [90/285084416] via 172.16.145.5, 00:13:53, Tunnel1
  10.0.0.0/24 is subnetted, 1 subnets
C    10.1.64.0 is directly connected, Serial0/0/0.46
S*  0.0.0.0/0 [1/0] via 10.1.64.6

```

The Spoke preffers R1 for 192.168.12.0/24 network and it points to R5 for 192.168.5.0/24 network.

R4#sh ip eigrp topology 192.168.5.0

```

IP-EIGRP (AS 1): Topology entry for 192.168.5.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 285084416
  Routing Descriptor Blocks:
    172.16.145.5 (Tunnel1), from 172.16.145.1, Send flag is 0x0
      Composite metric is (285084416/284828416), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 2
    172.16.245.2 (Tunnel2), from 172.16.245.2, Send flag is 0x0
      Composite metric is (285342976/284830976), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 35100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 3

```

R4#sh ip nhrp

```

172.16.145.1/32 via 172.16.145.1, Tunnel1 created 00:15:16, never expire
  Type: static, Flags: used
  NBMA address: 10.1.16.1
172.16.245.2/32 via 172.16.245.2, Tunnel2 created 00:15:16, never expire
  Type: static, Flags: used
  NBMA address: 10.1.26.2

```

It has static NHRP entries to reach and register in both NHSes.

R4#sh ip cef 192.168.5.0

```

192.168.5.0/24, version 25, epoch 0
0 packets, 0 bytes
  via 172.16.145.5, Tunnel1, 0 dependencies
    next hop 172.16.145.5, Tunnel1
    invalid adjacency

```

CEF entry is invalid as expected in DMVPN Phase 2.

R4#sh crypto isakmp sa

```

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.1.26.2    10.1.64.4    QM_IDLE        1002     0 ACTIVE
10.1.16.1    10.1.64.4    QM_IDLE        1001     0 ACTIVE

IPv6 Crypto ISAKMP SA

```

ISKAMP SA and IPSec SAs are set up with both Hubs. No IPSec tunnel with the other spoke yet.

R4#sh crypto ipsec sa

interface: Tunnel1

Crypto map tag: DMVPN-head-1, local addr 10.1.64.4

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)

current_peer 10.1.16.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 214, #pkts encrypt: 214, #pkts digest: 214

#pkts decaps: 210, #pkts decrypt: 210, #pkts verify: 210

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.16.1

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46

current outbound spi: 0x84A95ADB(2225691355)

inbound esp sas:

spi: 0xE5EB2CDE(3857394910)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2001, flow_id: NETGX:1, crypto map: DMVPN-head-1

sa timing: remaining key lifetime (k/sec): (4463855/2688)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0x84A95ADB(2225691355)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2002, flow_id: NETGX:2, crypto map: DMVPN-head-1

sa timing: remaining key lifetime (k/sec): (4463855/2688)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
current_peer 10.1.26.2 port 500
  PERMIT, flags={origin_is_acl,}
    #pkts encaps: 209, #pkts encrypt: 209, #pkts digest: 209
    #pkts decaps: 210, #pkts decrypt: 210, #pkts verify: 210
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 12, #recv errors 0
```

```
local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.26.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x77BC473A(2008827706)
```

```
inbound esp sas:
  spi: 0x6A0C9367(1779209063)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2005, flow_id: NETGX:5, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4503000/2708)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
  spi: 0x77BC473A(2008827706)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2006, flow_id: NETGX:6, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4503000/2708)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

interface: Tunnel2

```
Crypto map tag: DMVPN-head-1, local addr 10.1.64.4
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
```

```
current_peer 10.1.16.1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 214, #pkts encrypt: 214, #pkts digest: 214
#pkts decaps: 210, #pkts decrypt: 210, #pkts verify: 210
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 6, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.16.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x84A95ADB(2225691355)

inbound esp sas:
  spi: 0xE5EB2CDE(3857394910)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4463855/2688)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x84A95ADB(2225691355)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4463855/2688)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
current_peer 10.1.26.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 209, #pkts encrypt: 209, #pkts digest: 209
#pkts decaps: 210, #pkts decrypt: 210, #pkts verify: 210
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 12, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.26.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x77BC473A(2008827706)

inbound esp sas:
spi: 0x6A0C9367(1779209063)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2005, flow_id: NETGX:5, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4503000/2708)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x77BC473A(2008827706)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2006, flow_id: NETGX:6, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4503000/2708)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R4#ping 192.168.5.5 so lo0 rep 10

```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
!!!!.!!!!
Success rate is 90 percent (9/10), round-trip min/avg/max = 76/92/120 ms
```

Ping between the spokes is successful. Note that there is one packet missed in the middle of the ping. This is the exact moment when the traffic switched over to the direct spoke-to-spoke tunnel.

R4#sh ip cef 192.168.5.0

```
192.168.5.0/24, version 25, epoch 0
0 packets, 0 bytes
```

```
via 172.16.145.5, Tunnel1, 0 dependencies
next hop 172.16.145.5, Tunnel1
valid adjacency
```

CEF entry is valid now.

R4#sh ip nhrp

```
172.16.145.1/32 via 172.16.145.1, Tunnel1 created 00:16:51, never expire
Type: static, Flags: used
NBMA address: 10.1.16.1
172.16.145.4/32 via 172.16.145.4, Tunnel1 created 00:00:54, expire 00:05:07
Type: dynamic, Flags: router unique local
NBMA address: 10.1.64.4
(no-socket)
172.16.145.5/32 via 172.16.145.5, Tunnel1 created 00:00:54, expire 00:05:07
Type: dynamic, Flags: router
NBMA address: 10.1.65.5
172.16.245.2/32 via 172.16.245.2, Tunnel2 created 00:16:51, never expire
Type: static, Flags: used
NBMA address: 10.1.26.2
```

NHRP database has information about other spoke.

R4#sh crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.1.65.5    10.1.64.4    QM_IDLE        1004     0 ACTIVE
10.1.26.2    10.1.64.4    QM_IDLE        1002     0 ACTIVE
10.1.64.4    10.1.65.5    QM_IDLE        1003     0 ACTIVE
10.1.16.1    10.1.64.4    QM_IDLE        1001     0 ACTIVE

IPv6 Crypto ISAKMP SA
```

ISAKMP SA and IPSec SAs are negotiated between the spokes.

R4#sh crypto ipsec sa

```
interface: Tunnel1
Crypto map tag: DMVPN-head-1, local addr 10.1.64.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
current_peer 10.1.16.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 242, #pkts encrypt: 242, #pkts digest: 242
#pkts decaps: 239, #pkts decrypt: 239, #pkts verify: 239
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```



```
#send errors 6, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.16.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x84A95ADB(2225691355)

inbound esp sas:
  spi: 0xE5EB2CDE(3857394910)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2001, flow_id: NETGX:1, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4463851/2592)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0x84A95ADB(2225691355)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2002, flow_id: NETGX:2, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4463851/2592)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
current_peer 10.1.26.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 230, #pkts encrypt: 230, #pkts digest: 230
#pkts decaps: 232, #pkts decrypt: 232, #pkts verify: 232
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 12, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.26.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x77BC473A(2008827706)

inbound esp sas:
```

```
spi: 0x6A0C9367(1779209063)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2005, flow_id: NETGX:5, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4502997/2612)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0x77BC473A(2008827706)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2006, flow_id: NETGX:6, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4502998/2612)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcg sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
current_peer 10.1.65.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.65.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0xBEABEE07(3198938631)

inbound esp sas:
spi: 0xB554FCF8(3042245880)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2009, flow_id: NETGX:9, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4443171/3529)
  IV size: 8 bytes
  replay detection support: Y
```

```
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xBEABEE07(3198938631)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2010, flow_id: NETGX:10, crypto map: DMVPN-head-1
sa timing: remaining key lifetime (k/sec): (4443171/3529)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcg sas:

interface: Tunnel2
Crypto map tag: DMVPN-head-1, local addr 10.1.64.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.16.1/255.255.255.255/47/0)
current_peer 10.1.16.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 242, #pkts encrypt: 242, #pkts digest: 242
#pkts decaps: 239, #pkts decrypt: 239, #pkts verify: 239
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 6, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.16.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x84A95ADB(2225691355)

inbound esp sas:
spi: 0xE5EB2CDE(3857394910)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2001, flow_id: NETGX:1, crypto map: DMVPN-head-1
sa timing: remaining key lifetime (k/sec): (4463851/2592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
```

inbound pcp sas:

outbound esp sas:

```
spi: 0x84A95ADB(2225691355)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2002, flow_id: NETGX:2, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4463851/2592)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.26.2/255.255.255.255/47/0)
current_peer 10.1.26.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 230, #pkts encrypt: 230, #pkts digest: 230
#pkts decaps: 232, #pkts decrypt: 232, #pkts verify: 232
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 12, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.26.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0x77BC473A(2008827706)
```

inbound esp sas:

```
spi: 0x6A0C9367(1779209063)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2005, flow_id: NETGX:5, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4502997/2612)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x77BC473A(2008827706)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2006, flow_id: NETGX:6, crypto map: DMVPN-head-1
```

```
sa timing: remaining key lifetime (k/sec): (4502998/2612)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
current_peer 10.1.65.5 port 500
  PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0
```

```
local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.65.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
current outbound spi: 0xBEABEE07(3198938631)
```

inbound esp sas:

```
spi: 0xB554FCF8(3042245880)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2009, flow_id: NETGX:9, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4443171/3529)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xBEABEE07(3198938631)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2010, flow_id: NETGX:10, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4443171/3529)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

Same bunch of commands on the other spoke.

R5#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.65.6 to network 0.0.0.0

```
D    192.168.12.0/24 [90/284702976] via 172.16.145.1, 00:17:10, Tunnel1
    172.16.0.0/24 is subnetted, 2 subnets
C      172.16.145.0 is directly connected, Tunnel1
C      172.16.245.0 is directly connected, Tunnel2
D    192.168.4.0/24 [90/285084416] via 172.16.145.4, 00:17:10, Tunnel1
C    192.168.5.0/24 is directly connected, Loopback0
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.65.0 is directly connected, Serial0/1/0.56
S*   0.0.0.0/0 [1/0] via 10.1.65.6
```

R5#sh ip eigrp topology 192.168.4.0

```
IP-EIGRP (AS 1): Topology entry for 192.168.4.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 285084416
  Routing Descriptor Blocks:
    172.16.145.4 (Tunnel1), from 172.16.145.1, Send flag is 0x0
      Composite metric is (285084416/284828416), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 2
    172.16.245.2 (Tunnel2), from 172.16.245.2, Send flag is 0x0
      Composite metric is (285342976/284830976), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 35100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 3
```

R5#sh ip cef 192.168.4.0

```
192.168.4.0/24, version 25, epoch 0
0 packets, 0 bytes
  via 172.16.145.4, Tunnel1, 0 dependencies
    next hop 172.16.145.4, Tunnel1
    valid adjacency
```

CEF entry is valid and NHRP database has information about R4.

R5#sh ip nhrp

```
172.16.145.1/32 via 172.16.145.1, Tunnel1 created 00:18:03, never expire
  Type: static, Flags: used
  NBMA address: 10.1.16.1
172.16.145.4/32 via 172.16.145.4, Tunnel1 created 00:02:22, expire 00:03:39
  Type: dynamic, Flags: router
  NBMA address: 10.1.64.4
172.16.145.5/32 via 172.16.145.5, Tunnel1 created 00:02:21, expire 00:03:39
  Type: dynamic, Flags: router unique local
  NBMA address: 10.1.65.5
  (no-socket)
172.16.245.2/32 via 172.16.245.2, Tunnel2 created 00:18:12, never expire
  Type: static, Flags: used
  NBMA address: 10.1.26.2
```

R5#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
10.1.65.5	10.1.64.4	QM_IDLE	1003	0	ACTIVE
10.1.26.2	10.1.65.5	QM_IDLE	1002	0	ACTIVE
10.1.16.1	10.1.65.5	QM_IDLE	1001	0	ACTIVE
10.1.64.4	10.1.65.5	QM_IDLE	1004	0	ACTIVE

IPv6 Crypto ISAKMP SA

R5#sh crypto ipsec sa peer 10.1.64.4

interface: Tunnel2

Crypto map tag: DMVPN-head-1, local addr 10.1.65.5

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

current_peer 10.1.64.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

```
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0xB554FCF8(3042245880)

inbound esp sas:
  spi: 0xBEABEE07(3198938631)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2007, flow_id: NETGX:7, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4476782/3441)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xB554FCF8(3042245880)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2008, flow_id: NETGX:8, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4476782/3441)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

interface: Tunnel1
  Crypto map tag: DMVPN-head-1, local addr 10.1.65.5

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
current_peer 10.1.64.4 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
```



```
current outbound spi: 0xB554FCF8(3042245880)

inbound esp sas:
spi: 0xBEABEE07(3198938631)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2007, flow_id: NETGX:7, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4476782/3441)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xB554FCF8(3042245880)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  conn id: 2008, flow_id: NETGX:8, crypto map: DMVPN-head-1
  sa timing: remaining key lifetime (k/sec): (4476782/3441)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Once again ping the remote spoke to see if the traffic gets encrypted.

R5#ping 192.168.4.4 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.5
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/79/80 ms
```

R5#sh crypto ipsec sa peer 10.1.64.4

```
interface: Tunnel2
  Crypto map tag: DMVPN-head-1, local addr 10.1.65.5

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
current_peer 10.1.64.4 port 500
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0xB554FCF8(3042245880)

inbound esp sas:
  spi: 0xBEABEE07(3198938631)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2007, flow_id: NETGX:7, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4476781/3413)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xB554FCF8(3042245880)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2008, flow_id: NETGX:8, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4476781/3413)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

interface: Tunnell
  Crypto map tag: DMVPN-head-1, local addr 10.1.65.5

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
current_peer 10.1.64.4 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.65.5, remote crypto endpt.: 10.1.64.4
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.56
current outbound spi: 0xB554FCF8(3042245880)

inbound esp sas:
  spi: 0xBEABEE07(3198938631)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2007, flow_id: NETGX:7, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4476781/3413)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xB554FCF8(3042245880)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2008, flow_id: NETGX:8, crypto map: DMVPN-head-1
    sa timing: remaining key lifetime (k/sec): (4476781/3413)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

TEST: shutdown R1's tunnel0 interface

The best test in this scenario is to shutdown R1's tunnel0 interface and see if everything is working fine.

```
R1(config)#int tu0
R1(config-if)#shut
R1(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
R1(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.145.5 (Tunnel0) is down: interface
down
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.145.4 (Tunnel0) is down: interface
down
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
```

R4#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 10.1.64.6 to network 0.0.0.0

```
D    192.168.12.0/24 [90/284958976] via 172.16.245.2, 00:01:32, Tunnel2
    172.16.0.0/24 is subnetted, 2 subnets
C    172.16.145.0 is directly connected, Tunnel1
C    172.16.245.0 is directly connected, Tunnel2
C    192.168.4.0/24 is directly connected, Loopback0
D    192.168.5.0/24 [90/285596416] via 172.16.245.5, 00:01:32, Tunnel2
    10.0.0.0/24 is subnetted, 1 subnets
C    10.1.64.0 is directly connected, Serial0/0/0.46
S*   0.0.0.0/0 [1/0] via 10.1.64.6
```

Now, the Tunnel2 (to the second Hub) is preferred.

R4#sh ip cef 192.168.5.0

```
192.168.5.0/24, version 28, epoch 0
0 packets, 0 bytes
  via 172.16.245.5, Tunnel2, 0 dependencies
    next hop 172.16.245.5, Tunnel2
    invalid adjacency
```

The CEF entry is invalid again, as the next hop changed.

R4#sh ip nhrp

```
172.16.145.1/32 via 172.16.145.1, Tunnel1 created 00:23:27, never expire
  Type: static, Flags: used
  NBMA address: 10.1.16.1
172.16.245.2/32 via 172.16.245.2, Tunnel2 created 00:23:27, never expire
  Type: static, Flags: used
  NBMA address: 10.1.26.2
```

No dynamic entries, as the old entries has been flushed.

R4#ping 192.168.5.5 so lo0 rep 10

```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
```

Packet sent with a source address of 192.168.4.4

!!!!.!!!!

Success rate is 90 percent (9/10), round-trip min/avg/max = 76/90/112 ms

Ping is successful.

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
10.1.65.5	10.1.64.4	QM_IDLE	1006	0	ACTIVE
10.1.26.2	10.1.64.4	QM_IDLE	1002	0	ACTIVE
10.1.64.4	10.1.65.5	QM_IDLE	1005	0	ACTIVE
10.1.16.1	10.1.64.4	MM_NO_STATE	0	0	ACTIVE
10.1.16.1	10.1.64.4	MM_NO_STATE	0	0	ACTIVE (deleted)

IPv6 Crypto ISAKMP SA

The R4 tries to set up an IPSec tunnel with R1 (which is down).

R4#sh crypto ipsec sa peer 10.1.65.5

interface: Tunnell

Crypto map tag: DMVPN-head-1, local addr 10.1.64.4

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)

current_peer 10.1.65.5 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 2, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.65.5

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46

current outbound spi: 0xD165CD2A(3513109802)

inbound esp sas:

spi: 0x25118EF2(621907698)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2011, flow_id: NETGX:11, crypto map: DMVPN-head-1

sa timing: remaining key lifetime (k/sec): (4464565/3577)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

spi: 0xAAB232EA(2863805162)

```
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2013, flow_id: NETGX:13, crypto map: DMVPN-head-1
sa timing: remaining key lifetime (k/sec): (4514894/3577)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xB43D28C4(3023907012)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2012, flow_id: NETGX:12, crypto map: DMVPN-head-1
sa timing: remaining key lifetime (k/sec): (4464565/3577)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
spi: 0xD165CD2A(3513109802)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2014, flow_id: NETGX:14, crypto map: DMVPN-head-1
sa timing: remaining key lifetime (k/sec): (4514894/3577)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

interface: Tunnel2
Crypto map tag: DMVPN-head-1, local addr 10.1.64.4

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.64.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.1.65.5/255.255.255.255/47/0)
current_peer 10.1.65.5 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 10.1.64.4, remote crypto endpt.: 10.1.65.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.46
```

current outbound spi: 0xD165CD2A(3513109802)

inbound esp sas:

spi: 0x25118EF2(621907698)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2011, flow_id: NETGX:11, crypto map: DMVPN-head-1

sa timing: remaining key lifetime (k/sec): (4464565/3577)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

spi: 0xAAB232EA(2863805162)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2013, flow_id: NETGX:13, crypto map: DMVPN-head-1

sa timing: remaining key lifetime (k/sec): (4514894/3577)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xB43D28C4(3023907012)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2012, flow_id: NETGX:12, crypto map: DMVPN-head-1

sa timing: remaining key lifetime (k/sec): (4464565/3577)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

spi: 0xD165CD2A(3513109802)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

conn id: 2014, flow_id: NETGX:14, crypto map: DMVPN-head-1

sa timing: remaining key lifetime (k/sec): (4514894/3577)

IV size: 8 bytes

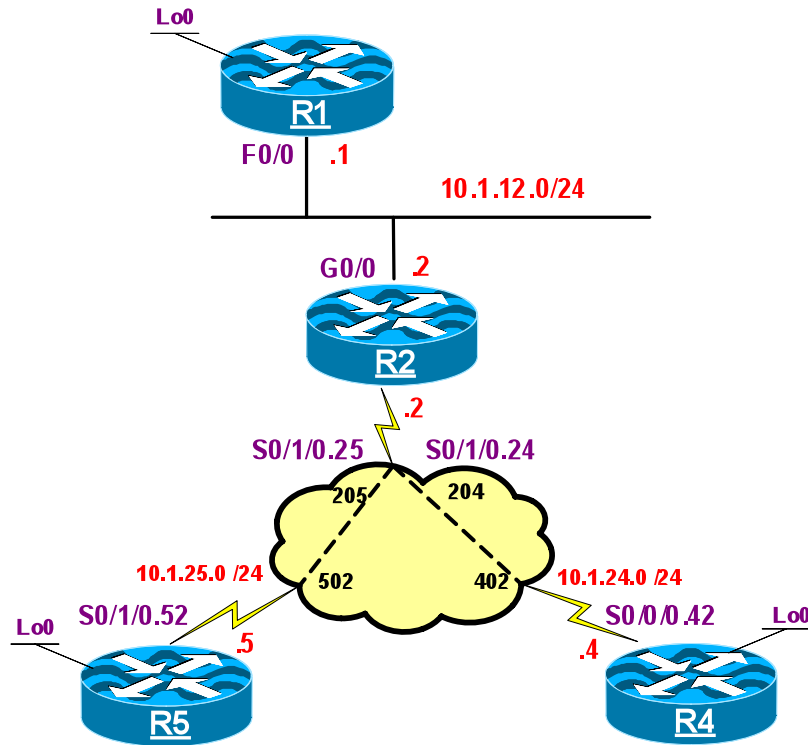
replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcg sas:

Lab 1.56. GET VPN (PSK)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's S0/1/0 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner
- R2's S0/1/0 and R4's S0/0/0 interface should be configured in a frame-relay point-to-point manner
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R4 and R5 pointing to the R2

IP Addressing

Device	Interface	IP address
R1	Lo0	192.168.1.1/24
	F0/0	10.1.12.1/24

R2	F0/0	10.1.12.2/24
	S0/1/0.25	10.1.25.2/24
	S0/1/0.24	10.1.24.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0.42	10.1.24.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0.52	10.1.25.5/24

Task 1

Configure GET VPN solution for traffic going between 192.168.0.0/16 networks (LANs behind R4 and R5). R1 must be used as Key Server and R5 and R4 are Group Members.

Use the following parameters for KS configuration:

Group name:	GETVPN
Server:	Identity 1 IP address 10.1.12.1
Rekey:	Unicast 2 retransmits, every 10 seconds RSA key name R1.micronicstraining.com
Authorization:	Only R5 and R4 GM routers
IPSec SA:	Time-based anti replay window: 64 Policy: 192.168.0.0/16, do not encrypt GDOI Encryption: AES-128 Integrity: SHA
ISAKMP Policy	Authentication: PSK Encryption: DES Hashing: SHA Pre-shared key: GETVPN-R5 (for R5), GETVPN-R4 (for R4)

Do not encrypt SSH traffic between 192.168.5.0/24 and 192.168.4.0/24 networks.
This exception must be configured on GMs only.



GET VPN is a technology used to encrypt traffic going through unsecured networks. It leverages IPsec protocol suite to enforce Integrity and Confidentiality of data. Typical GET deployment consists a router called Key Server (KS) and a couple of routers called Group Members (GMs). The KS is used to create, maintain and send a “policy” to GMs. The policy is an information what traffic should be encrypted by GM and what encryption algorithms must be used. The most important function of KS is generation of encryption keys. There are two keys used:

TEK – Transport Encryption Key – used by GM to encrypt the data

KEK – Key Encryption Key – used to encrypt information between KS and GM

A very important aspect of GET is that it does not set up any IPsec tunnels between GMs! It is NOT like DMVPN. Every GM has the policy (what to encrypt, what encryption algorithm to use, what key is used by the encryption algorithm) and just encrypt every packet conforming its policy and sends it out to the network using ESP (Encapsulated Security Payload). Note that it uses original IP addresses to route the packet out (this is called IP Header Preservation mechanism), hence the packet can be routed towards every other router in the network as long as the routing table has such information.

Configuration

Complete these steps:

Step 1 R1 configuration.

First we need RSA keys to be used by our KS for Rekey process. The KS must send out a new TEK (and KEK) before TEK is expired (default is 3600 seconds). It does this in so-called Rekey phase. This phase is authenticated and secured by ISAKMP SA which is established between KS and GM. This ISAKMP uses GDOI messages (think of this like a mutation of IKE) to build SA and encrypt GM registration. The GDOI uses UDP/848 instead of UDP/500 like IKE does. The RSA keys are used to authenticated the KS to GM in the Rekey process.

Remember that to generate new RSA keys you must have Hostname and Domain-name configured on the router.

```
R1(config)#ip domain-name micronictstraining.com  
R1(config)#crypto key generate rsa modulus 1024
```

The name for the keys will be: R1.micronicstraining.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#

%SSH-5-ENABLED: SSH 1.99 has been enabled

Then we need ISAKMP paramaters, just like in regular IPSec configuration. Pre-shared key must be specified on both KS and GM to be able to authenticate. This will be used to establish ISAKMP SA to secure further GDOI messages.

R1(config)#crypto isakmp policy 10

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# exi

R1(config)#crypto isakmp key GETVPN-R5 address 10.1.25.5

R1(config)#crypto isakmp key GETVPN-R4 address 10.1.24.4

The IPSec paramaters must be configured on KS. These parameters are not used by KS itself. They are part of policy that will be send down to the GMs. The IPSec profile tells the GM what encryption algorithm use.

R1(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac

R1(cfg-crypto-trans)#crypto ipsec profile GETVPN-PROF

R1(ipsec-profile)# set transform-set TSET

Now it's time to configure KS. To do that we need to specify The Group. One KS may have many groups and each group may have different security policy.

R1(ipsec-profile)#crypto gdoi group GETVPN

R1(config-gdoi-group)# identity number 1

R1(config-gdoi-group)# server local

%CRYPTO-6-GDOI_ON_OFF: GDOI is ON

Here we need to specify Rekey parameters. The Rekey phase can be performed in two ways:

- Unicast Rekey - when we do not have multicast support in our infrastructure (may be a case when ISP does not support multicast in its IP VPN cloud). The KS sends down a Rekey packet to every GM it knows of.
- Multicast Rekey - when we have multicast ready infrastructure, then we can enable multicast Rekey and the KS generates only one packet and sends it down to all GMs at one time

```
R1(gdoi-local-server)# rekey authentication mypubkey rsa
R1.micronicstraining.com
R1(gdoi-local-server)# rekey retransmit 10 number 2
R1(gdoi-local-server)# rekey transport unicast
```

By default every GM can register to KS as long as it has correct PSK configured (or valid Certificate in case of PKI). To authorize GMs to be able to register in this group on KS, you need to specify a standard ACL with GM's IP addresses. Our ACL is named GM-LIST.

```
R1(gdoi-local-server)# authorization address ipv4 GM-LIST
```

Now it's time to configure policy for our GMs. Encryption policy is created by IPSec Profile configured earlier. To tell the GMs what packets they should encrypt, we need another ACL (extended this time). Our ACL is named LAN-LIST. We can also specify window size for Time-based Anti-Replay protection. The last parameter important is KS's IP address. This parameter must as well be send don to the GMs as KS may be run on different IP address (like Loopback).

```
R1(gdoi-local-server)# sa ipsec 1
R1(gdoi-sa-ipsec)# profile GETVPN-PROF
R1(gdoi-sa-ipsec)# match address ipv4 LAN-LIST
R1(gdoi-sa-ipsec)# replay counter window-size 64
R1(gdoi-sa-ipsec)# address ipv4 10.1.12.1
R1(gdoi-local-server)#
%GDOI-5-KS_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
R1(gdoi-local-server)#exi
R1(config-gdoi-group)#exi

R1(config)#ip access-list standard GM-LIST
R1(config-std-nacl)# permit 10.1.25.5
R1(config-std-nacl)# permit 10.1.24.4
R1(config-std-nacl)#exi
```

Here's our "policy ACL". Note that we must exclude GDOI (UDP/848) from this policy as there is not much sense to encrypt something already encrypted.

```
R1(config)#ip access-list extended LAN-LIST
R1(config-ext-nacl)# deny udp any eq 848 any eq 848
R1(config-ext-nacl)# permit ip 192.168.0.0 0.0.255.255 192.168.0.0
0.0.255.255
R1(config-ext-nacl)#exi
```

Step 2 R5 configuration.

R5 is our first GM. We need the following to be configured on every GM:

- ISAKMP policy and pre-shared key (in case of PSK)
- the Group to which the GM needs to be registered to
- (optional) ACL to exclude some traffic from encryption
- crypto map type GDOI

```
R5(config)#crypto isakmp policy 10
```

```
R5(config-isakmp)# authentication pre-share
```

```
R5(config-isakmp)# exit
```

```
R5(config)#crypto isakmp key GETVPN-R5 address 10.1.12.1
```

```
R5(config)#crypto gdoi group GETVPN
```

```
R5(config-gdoi-group)# identity number 1
```

```
R5(config-gdoi-group)# server address ipv4 10.1.12.1
```

```
R5(config-gdoi-group)# exit
```

This ACL is optional. In general we should configure our policy on KS only, but there are some situations when we need to exclude some flows from encryption. Like here, we were asked for excluding SSH traffic between 192.168.4.0/24 AND 192.168.5.0/24 networks.

When policy is configured on both KS and GM, the concatenated policy looks like follow:

- Denied traffic on KS
- Permitted traffic on KS
- Denied traffic on GM

We can only DENY (exclude) the traffic on GM, we cannot PERMIT it to be encrypted. To display that concatenated policy use "sh crypto gdoi gm acl" command on GM.

```
R5(config)#ip access-list extended DO-NOT-ENCRYPT
```

```
R5(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 eq 22  
192.168.5.0 0.0.0.255
```

```
R5(config-ext-nacl)#deny tcp 192.168.5.0 0.0.0.255 192.168.4.0  
0.0.0.255 eq 22
```

```
R5(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 192.168.5.0  
0.0.0.255 eq 22
```

```
R5(config-ext-nacl)#deny tcp 192.168.5.0 0.0.0.255 eq 22  
192.168.4.0 0.0.0.255
```

```
R5(config-ext-nacl)#exit
```

```
R5(config)#crypto map CMAP-GETVPN 10 gdoi
```

% NOTE: This new crypto map will remain disabled until a valid group has been configured.

```
R5(config-crypto-map)# set group GETVPN
```

```
R5(config-crypto-map)# match address DO-NOT-ENCRYPT
```

```
R5(config-crypto-map)# exit
```

```
R5(config)#int s0/1/0.52
R5(config-subif)# crypto map CMAP-GETVPN
R5(config-subif)# exi
R5(config)#
%CRYPTO-5-GM_REGISTER: Start registration to KS 10.1.12.1 for group
GETVPN using address 10.1.25.5
R5(config)#
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R5(config)#
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.1 complete for
group GETVPN using address 10.1.25.5
```

See above SYSLOG messages. They indicate that GM has started registration process with KS and registered successfully.

Step 3 R4 configuration.

Same configuration for next GM.

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)# authentication pre-share
R4(config-isakmp)# exi

R4(config)#crypto isakmp key GETVPN-R4 address 10.1.12.1

R4(config)#crypto gdoi group GETVPN
R4(config-gdoi-group)# identity number 1
R4(config-gdoi-group)# server address ipv4 10.1.12.1
R4(config-gdoi-group)# exi

R4(config)#ip access-list extended DO-NOT-ENCRYPT
R4(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 eq 22
192.168.5.0 0.0.0.255
R4(config-ext-nacl)#deny tcp 192.168.5.0 0.0.0.255 192.168.4.0
0.0.0.255 eq 22
R4(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 192.168.5.0
0.0.0.255 eq 22
R4(config-ext-nacl)#deny tcp 192.168.5.0 0.0.0.255 eq 22
192.168.4.0 0.0.0.255

R4(config-ext-nacl)#crypto map CMAP-GETVPN 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R4(config-crypto-map)# set group GETVPN
R4(config-crypto-map)# match address DO-NOT-ENCRYPT
R4(config-crypto-map)# exi
```

```

R4(config)#int s0/0/0.42
R4(config-subif)# crypto map CMAP-GETVPN
R4(config-subif)# exit
%CRYPTO-5-GM_REGISTER: Start registration to KS 10.1.12.1 for group
GETVPN using address 10.1.24.4
R4(config)#
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R4(config)#
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.1 complete for
group GETVPN using address 10.1.24.4

```

Verification

R1#sh crypto gdoi group GETVPN

```

Group Name           : GETVPN (Unicast)
Group Identity       : 1
Group Members        : 2
IPSec SA Direction   : Both
Active Group Server   : Local
Group Rekey Lifetime : 86400 secs
Group Rekey
    Remaining Lifetime : 86361 secs
Rekey Retransmit Period : 10 secs
Rekey Retransmit Attempts: 2
Group Retransmit
    Remaining Lifetime : 0 secs

IPSec SA Number      : 1
IPSec SA Rekey Lifetime: 3600 secs
Profile Name         : GETVPN-PROF
Replay method        : Count Based
Replay Window Size   : 64
SA Rekey
    Remaining Lifetime : 3562 secs
ACL Configured       : access-list LAN-LIST

Group Server list     : Local

```

R1#sh crypto gdoi ks policy

```

Key Server Policy:
For group GETVPN (handle: 2147483650) server 10.1.12.1 (handle: 2147483650):

# of teks : 1  Seq num : 0
KEK POLICY (transport type : Unicast)
spi : 0x76749A6D99B3C0A3827FA26F1558ED63

```

```

management alg      : disabled      encrypt alg       : 3DES
crypto iv length    : 8              key size           : 24
orig life(sec): 86400      remaining life(sec): 86355
sig hash algorithm  : enabled        sig key length      : 162
sig size            : 128
sig key name        : R1.micronicstraining.com

```

```

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi                : 0xAF4FA6F8      access-list         : LAN-LIST
# of transforms    : 0              transform           : ESP_AES
hmac alg           : HMAC_AUTH_SHA
alg key size       : 16              sig key size        : 20
orig life(sec)     : 3600            remaining life(sec) : 3556
tek life(sec)      : 3600            elapsed time(sec)   : 44
antireplay window size: 64

```

See both keys: TEK and KEK.

KEK - for Rekey encryption, default lifetime 24 hours, default encryption algorithm 3DES

TEK - for traffic encryption between GMs, default lifetime 1 hour, encryption algorithm depends on configured policy (no defaults).

R1#sh crypto gdoi ks acl

Group Name: GETVPN

Configured ACL:

access-list LAN-LIST deny udp any port = 848 any port = 848

access-list LAN-LIST permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

Here's the ACL which tells the GMs what traffic they should encrypt.

R1#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group GETVPN : 1

```

Group Member ID    : 10.1.24.4
Group ID           : 1
Group Name          : GETVPN
Key Server ID      : 10.1.12.1
Rekeys sent        : 0
Rekeys retries     : 0
Rekey Acks Rcvd    : 0
Rekey Acks missed  : 0

```

```

Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

```

```

Group Member ID    : 10.1.25.5

```



```

Group ID          : 1
Group Name        : GETVPN
Key Server ID     : 10.1.12.1
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0

Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0

```

Registered members on KS. Keep in mind you may have thousands of members registered to different groups. One member can register to two groups at the same time.

R1#sh crypto gdoi ks rekey

```

Group GETVPN (Unicast)
  Number of Rekeys sent           : 1
  Number of Rekeys retransmitted  : 0
  KEK rekey lifetime (sec)        : 86400
  Remaining lifetime (sec)        : 86335
  Retransmit period               : 10
  Number of retransmissions       : 2
  IPSec SA 1 lifetime (sec)       : 3600
  Remaining lifetime (sec)        : 3536

```

We have configured that for Rekey phase. It is very important for Unicast Rekey that KS will retransmit Rekey message if it didn't receive ACK from the GM.

R1#sh crypto isakmp sa

```

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.1.12.1    10.1.24.4    GDOI_IDLE    1002 ACTIVE
10.1.12.1    10.1.25.5    GDOI_IDLE    1001 ACTIVE

```

```
IPv6 Crypto ISAKMP SA
```

Note that ISAKMP SA is established between KS and GMs only. There is no ISAKMP SA between GMs.

R1#sh crypto ipsec sa

```
No SAs found
```

There are no IPSec SA between KS and GMs. All is done using ISAKMP SA. After IKE Phase 1 establishes the SA, the GDOI protocol uses it for GM Registration and Rekey.

The same bunch of commands are on GMs.

R4#sh crypto gdoi gm

Group Member Information For Group GETVPN:

```

IPSec SA Direction      : Both
ACL Received From KS    : gdoi_group_GETVPN_temp_acl
Last rekey seq num      : 0
Re-register
Remaining time          : 3389 secs
Retry Timer
                        :NOT RUNNING

```

R4#sh crypto gdoi gm acl

Group Name: GETVPN

ACL Downloaded From KS 10.1.12.1:

```

access-list deny udp any port = 848 any port = 848
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

```

ACL Configured Locally:

Map Name: CMAP-GETVPN

```

access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 port = 22 192.168.5.0
0.0.0.255
access-list DO-NOT-ENCRYPT deny tcp 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255 port
= 22
access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 port
= 22
access-list DO-NOT-ENCRYPT deny tcp 192.168.5.0 0.0.0.255 port = 22 192.168.4.0
0.0.0.255

```

Here's the current Policy on GM. See this is concatenated ACL (KS ACL + GM ACL) .

R4#sh crypto gdoi gm rekey

Group GETVPN (Unicast)

```

Number of Rekeys received (cumulative)      : 0
Number of Rekeys received after registration : 0
Number of Rekey Acks sent                    : 0

```

Rekey (KEK) SA information :

	dst	src	conn-id	my-cookie	his-cookie
New	: 10.1.24.4	10.1.12.1	1004	827FA26F	76749A6D
Current	: ---	---	---	---	---
Previous:	---	---	---	---	---

R4#sh crypto gdoi group GETVPN

```

Group Name          : GETVPN
Group Identity       : 1
Rekeys received     : 0
IPSec SA Direction  : Both
Active Group Server  : 10.1.12.1

```

Group Server list : 10.1.12.1

GM Reregisters in : 3371 secs

Rekey Received(hh:mm:ss) : 00:15:45

Rekeys received

Cumulative : 0

After registration : 0

Rekey Acks sent : 0

ACL Downloaded From KS 10.1.12.1:

access-list deny udp any port = 848 any port = 848

access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

KEK POLICY:

Rekey Transport Type : Unicast

Lifetime (secs) : 86394

Encrypt Algorithm : 3DES

Key Size : 192

Sig Hash Algorithm : HMAC_AUTH_SHA

Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:

Serial0/0/0.42:

IPsec SA:

spi: 0xAF4FA6F8(2941232888)

transform: esp-aes esp-sha-hmac

sa timing:remaining key lifetime (sec): (3494)

Anti-Replay : Disabled

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.1	10.1.24.4	GDOI_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

GM maintains ISAKMP SA with KS only!

R4#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.

```
1001 10.1.24.4      10.1.12.1      ACTIVE des sha psk 1 23:43:50
      Engine-id:Conn-id = SW:1
```

```
IPv6 Crypto ISAKMP SA
```

**The below is IPSec SA. This is built upon policy received from KS. Hence, there are as many Proxy IDs as permit ACEs in ACL downloaded from the KS.
Note that there is NO peer!**

R4#sh crypto ipsec sa

```
interface: Serial0/0/0.42
      Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
current peer 0.0.0.0 port 848
      PERMIT, flags={origin_is_acl,}
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts compr. failed: 0
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.42
current outbound spi: 0xAF4FA6F8(2941232888)
PFS (Y/N): N, DH group: none

inbound esp sas:
      spi: 0xAF4FA6F8(2941232888)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2007, flow_id: NETGX:7, sibling_flags 80000040, crypto map: CMAP-
GETVPN
      sa timing: remaining key lifetime (sec): (3474)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
      spi: 0xAF4FA6F8(2941232888)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
```

```

      conn id: 2008, flow_id: NETGX:8, sibling_flags 80000040, crypto map: CMAP-
GETVPN
      sa timing: remaining key lifetime (sec): (3474)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE

```

```
outbound ah sas:
```

```
outbound pcp sas:
```

Note the Inbound and Outbound SPI is the same. This is because every GM understands that SPI (it is configured on KS and sends down to all GMs).

R4#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

```
Gateway of last resort is 10.1.24.2 to network 0.0.0.0
```

```

C    192.168.4.0/24 is directly connected, Loopback0
    10.0.0.0/24 is subnetted, 1 subnets
C    10.1.24.0 is directly connected, Serial0/0/0.42
S*  0.0.0.0/0 [1/0] via 10.1.24.2

```

See, there is only default route configured on GM. Let's try to ping network behind R5 and source the traffic from Lo0.

R4#ping 192.168.5.5 so lo0

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
.....
Success rate is 0 percent (0/5)

```

Unsuccessful! Why? Let's look at crypto.

R4#sh crypto ipsec sa

```

interface: Serial0/0/0.42
  Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)

```

```
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
current_peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.42
current outbound spi: 0xAF4FA6F8(2941232888)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xAF4FA6F8(2941232888)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2007, flow_id: NETGX:7, sibling_flags 80000040, crypto map: CMAP-
GETVPN
    sa timing: remaining key lifetime (sec): (3434)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0xAF4FA6F8(2941232888)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2008, flow_id: NETGX:8, sibling_flags 80000040, crypto map: CMAP-
GETVPN
    sa timing: remaining key lifetime (sec): (3434)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:
```

Seems like ICMP packets have been encrypted and sent out. Hence, the problem must lay somewhere else. Since GET VPN uses IP Header Preservation mechanism, the original source and destination IP addresses are not changed (there is no tunneling). Let's look at R2 if there are correct routes to that networks and add the missing routes.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 192.168.4.0 255.255.255.0 10.1.24.4
R2(config)#ip route 192.168.5.0 255.255.255.0 10.1.25.5
```

R4#ping 192.168.5.5 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
```

Success! Let's look at crypto again.

R4#sh crypto ipsec sa

```
interface: Serial0/0/0.42
  Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
  current_peer 0.0.0.0 port 848
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

  local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.42
  current outbound spi: 0xAF4FA6F8(2941232888)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
    spi: 0xAF4FA6F8(2941232888)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2007, flow_id: NETGX:7, sibling_flags 80000040, crypto map: CMAP-
GETVPN
      sa timing: remaining key lifetime (sec): (3372)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE
```

inbound ah sas:

inbound pcg sas:

outbound esp sas:

```
spi: 0xAF4FA6F8(2941232888)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2008, flow_id: NETGX:8, sibling_flags 80000040, crypto map: CMAP-
```

GETVPN

```
sa timing: remaining key lifetime (sec): (3372)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcg sas:

All packets have been encrypted and decrypted.

Now take a look at R5. The same bunch of commands for GDOI.

R5#sh crypto gdoi gm

Group Member Information For Group GETVPN:

```
IPSec SA Direction      : Both
ACL Received From KS    : gdoi_group_GETVPN_temp_acl
Last rekey seq num      : 0
Re-register
Remaining time          : 3222 secs
Retry Timer
                        :NOT RUNNING
```

R5#sh crypto gdoi gm acl

Group Name: GETVPN

ACL Downloaded From KS 10.1.12.1:

```
access-list deny udp any port = 848 any port = 848
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
```

ACL Configured Locally:

Map Name: CMAP-GETVPN

```
access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 port = 22 192.168.5.0
0.0.0.255
access-list DO-NOT-ENCRYPT deny tcp 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255 port
= 22
access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 port
= 22
access-list DO-NOT-ENCRYPT deny tcp 192.168.5.0 0.0.0.255 port = 22 192.168.4.0
0.0.0.255
```

R5#sh crypto gdoi gm rekey

Group GETVPN (Unicast)


```

Number of Rekeys received (cumulative)      : 0
Number of Rekeys received after registration : 0
Number of Rekey Acks sent                   : 0

```

Rekey (KEK) SA information :

	dst	src	conn-id	my-cookie	his-cookie
New	: 10.1.25.5	10.1.12.1	1004	827FA26F	76749A6D
Current	: ---	---	---	---	---
Previous	: ---	---	---	---	---

R5#sh crypto gdoi group GETVPN

```

Group Name           : GETVPN
Group Identity       : 1
Rekeys received      : 0
IPSec SA Direction   : Both
Active Group Server   : 10.1.12.1
Group Server list     : 10.1.12.1

GM Reregisters in    : 3206 secs
Rekey Received(hh:mm:ss) : 00:18:14

```

```

Rekeys received
  Cumulative          : 0
  After registration   : 0
Rekey Acks sent       : 0

```

ACL Downloaded From KS 10.1.12.1:

```

access-list deny udp any port = 848 any port = 848
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

```

KEK POLICY:

```

Rekey Transport Type   : Unicast
Lifetime (secs)        : 86400
Encrypt Algorithm       : 3DES
Key Size                : 192
Sig Hash Algorithm      : HMAC_AUTH_SHA
Sig Key Length (bits)   : 1024

```

TEK POLICY for the current KS-Policy ACEs Downloaded:

Serial0/1/0.52:

```

IPsec SA:
  spi: 0xAF4FA6F8(2941232888)
  transform: esp-aes esp-sha-hmac
  sa timing:remaining key lifetime (sec): (3344)
  Anti-Replay : Disabled

```

R5#sh crypto isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

```

K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.

1001  10.1.25.5         10.1.12.1          ACTIVE des  sha  psk  1  23:40:56
      Engine-id:Conn-id =  SW:1

IPv6 Crypto ISAKMP SA

```

R5#sh crypto ipsec sa

```

interface: Serial0/1/0.52
  Crypto map tag: CMAP-GETVPN, local addr 10.1.25.5

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
current peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.25.5, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.52
current outbound spi: 0xAF4FA6F8(2941232888)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xAF4FA6F8(2941232888)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2007, flow_id: NETGX:7, sibling_flags 80000040, crypto map: CMAP-
GETVPN
    sa timing: remaining key lifetime (sec): (3331)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

```

```
outbound esp sas:
  spi: 0xAF4FA6F8(2941232888)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2008, flow_id: NETGX:8, sibling_flags 80000040, crypto map: CMAP-
GETVPN
  sa timing: remaining key lifetime (sec): (3331)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Test

To verify the policy configured on GMs, we need to enable SSH server on R4 and R5 and configure local user database. Note that you must test SSH traffic between 192.168.[4-5].0/24 networks, so you need to inform the routers what interface use as SSH source.

```
R4(config)#ip ssh source-interface lo0

R4(config)#ip domain-name micronicstraining.com
R4(config)#cry key gen rsa mod 1024
The name for the keys will be: R4.micronicstraining.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R4(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
R4(config)#line vty 0 4
R4(config-line)#login local


R5(config)#username student password student123
R5(config)#line vty 0 4
R5(config-line)#login local
R5(config-line)#exit


R5(config)#ip ssh source-interface lo0
Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
R5(config)#ip domain-name micronicstraining.com
R5(config)#crypto key generate rsa mod 1024
The name for the keys will be: R5.micronicstraining.com
```

```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R5(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
R5(config)#end
```

First, check the encryption/decryption counters.

```
R5#sh cry ips sa | in local|remot|enca|deca

Crypto map tag: CMAP-GETVPN, local addr 10.1.25.5
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 57, #pkts encrypt: 57, #pkts digest: 57
#pkts decaps: 82, #pkts decrypt: 82, #pkts verify: 82
local crypto endpt.: 10.1.25.5, remote crypto endpt.: 0.0.0.0
```

Connect to r4 using SSH to generate the traffic.

```
R5#ssh -l student 192.168.4.4
```

```
Password:
```

```
R4>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:03:29	
*514 vty 0	student	idle	00:00:00	192.168.5.5

Interface	User	Mode	Idle	Peer Address

```
R4>exit
```

```
[Connection to 192.168.4.4 closed by foreign host]
```

Check the encryption/decryption counters.

```
R5#sh cry ips sa | in local|remot|enca|deca

Crypto map tag: CMAP-GETVPN, local addr 10.1.25.5
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 57, #pkts encrypt: 57, #pkts digest: 57
#pkts decaps: 82, #pkts decrypt: 82, #pkts verify: 82
local crypto endpt.: 10.1.25.5, remote crypto endpt.: 0.0.0.0
```

No encryption counters incremented!!! This is because SSH between those networks is excluded from encryption.

Same test on R4:

R4#sh cry ips sa | in local|remot|enca|deca

```
Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 87, #pkts encrypt: 87, #pkts digest: 87
#pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0
```

R4#ssh -l student 192.168.5.5

Password:

R5>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:01:00	
*514 vty 0	student	idle	00:00:00	192.168.4.4

Interface	User	Mode	Idle	Peer Address

R5>exit

[Connection to 192.168.5.5 closed by foreign host]

R4#sh cry ips sa | in local|remot|enca|deca

```
Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 87, #pkts encrypt: 87, #pkts digest: 87
#pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0
```

No encryption counters incremented!! Let's verify by doing ping.

R4#ping 192.168.5.5 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:

Packet sent with a source address of 192.168.4.4

!!!!!!

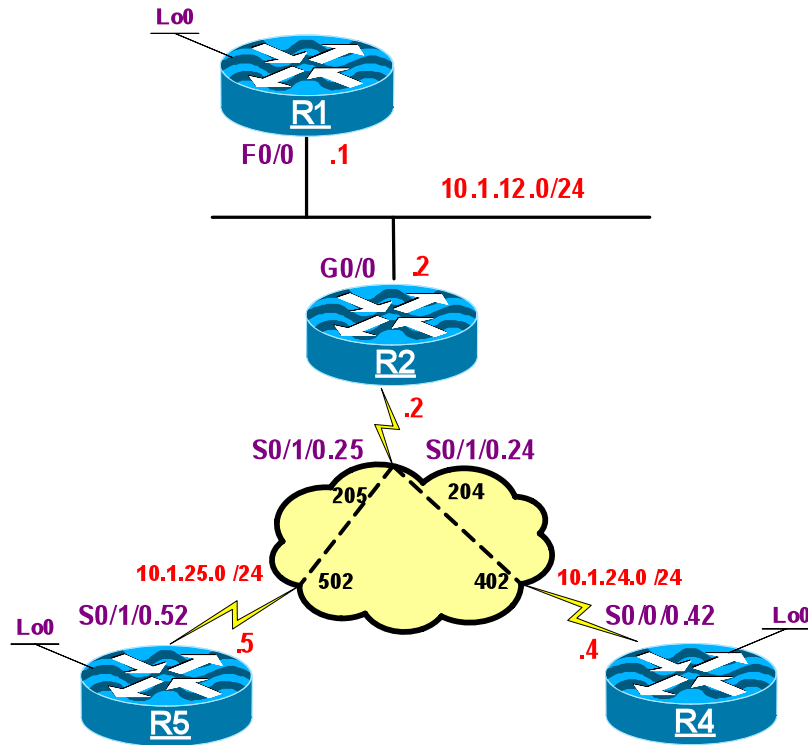
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

R4#sh cry ips sa | in local|remot|enca|deca

```
Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 92, #pkts encrypt: 92, #pkts digest: 92
#pkts decaps: 62, #pkts decrypt: 62, #pkts verify: 62
local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0
```

Counters have been incremented by 5 packets!

Lab 1.57. GET VPN (PKI)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's S0/1/0 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner
- R2's S0/1/0 and R4's S0/0/0 interface should be configured in a frame-relay point-to-point manner
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R4 and R5 pointing to the R2

IP Addressing

Device	Interface	IP address
R1	Lo0	192.168.1.1/24
	F0/0	10.1.12.1/24

R2	F0/0	10.1.12.2/24
	S0/1/0.25	10.1.25.2/24
	S0/1/0.24	10.1.24.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0.42	10.1.24.4/24
R5	Lo0	192.168.5.5/24
	S0/1/0.52	10.1.25.5/24

Task 1

Configure NTP server with MD5 authentication (cisco123) and CA server on R1. It will be used for enrolling certificates for GET VPN Group Members.

Configure GET VPN solution for traffic going between 192.168.0.0/16 networks (LANs behind R5 and R4). R1 must be used as Key Server and R5 and R4 are Group Members.

Use the following parameters for KS configuration:

Group name:	GETVPN
Server:	Identity 1 IP address 10.1.12.1
Rekey:	Unicast No retransmits Lifetime 400 seconds RSA key name KS-KEYS
Authorization:	Only R5 and R4 GM routers
IPSec SA:	Time-based anti replay window: 64 Policy: 192.168.0.0/16, do not encrypt GDOI Encryption: AES-128 Integrity: SHA
ISAKMP Policy	Authentication: Certificates Encryption: DES Hashing: SHA

Do not encrypt TELNET traffic between 192.168.5.0/24 and 192.168.4.0/24 networks. This exception must be configured on GMs.



This lab is very similar to the previous one. Here, we're asked for certificate authentication between KS and GMs. When certificates are in use, we need to be careful about time so that we are asked to configure NTP server on R1 and NTP clients on R4 and R5.

R1 must work as Certificate Authority to give out the certificates to all routers. The CA configuration has been described in details in the lab 2.4.

Note that since the R1 must work as KS it must have its own certificate as well. Hence, we need to create trustpoint on R1 and enroll a certificate as we do on every other router.

Configuration

Complete these steps:

Step 1 Configure R1 as NTP server.

```
R1(config)#ntp master 4
R1(config)#ntp authentication-key 1 md5 cisco123
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate
```

Step 2 Configure R5 as NTP client to R1.

```
R5(config)#ntp authentication-key 1 md5 cisco123
R5(config)#ntp trusted-key 1
R5(config)#ntp authenticate
R5(config)#ntp server 10.1.12.1 key 1
```

Step 3 Configure R4 as NTP client to R1.

```
R4(config)#ntp authentication-key 1 md5 cisco123
R4(config)#ntp trusted-key 1
R4(config)#ntp authenticate
R4(config)#ntp server 10.1.12.1 key 1
```

Step 4 Configure CA and KS n R1.

```
R1(config)#do sh ntp status
```



```
Clock is synchronized, stratum 4, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision
is 2**18
reference time is CEA97CF5.2B02C9E8 (19:01:09.168 UTC Sat Nov 14
2009)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

```
R1(config)#ip domain-name micronictstraining.com
```

```
R1(config)#crypto key generate rsa mod 1024 label KS-KEYS
exportable
```

```
The name for the keys will be: KS-KEYS
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be exportable...[OK]
```

```
R1(config)#
```

```
%SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
R1(config)#ip http server
```

```
R1(config)#crypto pki server IOS-CA
```

```
R1(cs-server)#database url nvram:
```

```
% Server database url was changed. You need to move the
```

```
% existing database to the new location.
```

```
R1(cs-server)#database level minimum
```

```
R1(cs-server)#grant auto
```

```
R1(cs-server)#
```

```
%PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically
granted.
```

```
R1(cs-server)#no shut
```

```
%Some server settings cannot be changed after CA certificate
generation.
```

```
% Please enter a passphrase to protect the private key
```

```
% or type Return to exit
```

```
Password:
```

```
Re-enter password:
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
% Exporting Certificate Server signing certificate and keys...
```

```
% Certificate Server enabled.
```

```
R1(cs-server)#
```

```
%PKI-6-CS_ENABLED: Certificate server now enabled.
```

```
R1(cs-server)#exi
```

Here's the trustpoint to enroll the certificate from CA
installed on R1.

```
R1(config)#crypto ca trustpoint R1-IOS-CA
```

```
R1(ca-trustpoint)#enrollment url http://10.1.12.1:80
R1(ca-trustpoint)#revocation-check none
R1(ca-trustpoint)#exi

R1(config)#crypto ca authenticate R1-IOS-CA
Certificate has the following attributes:
    Fingerprint MD5: 1EDBC58C C0EC6E6A 30277787 757F752B
    Fingerprint SHA1: AC5AAD4E 6F972239 CD46EE23 45265D7A
A756B2C5

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R1(config)#crypto ca enroll R1-IOS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.

Password:
%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:

% The subject name in the certificate will include:
R1.micronicstraining.com
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate R1-IOS-CA verbose' command will
show the fingerprint.

R1(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: BAFB1982 AD56FE4E
7A13792F A30D12FF
CRYPTO_PKI: Certificate Request Fingerprint SHA1: D4D7E9C1
58521229 DABAAD4B 88A19A2B 2A5CFB27
R1(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority
```

The configuration is very similar to that presented in the previous lab. The one difference is in ISAKMP policy. We do not need to specify RSA-SIG as it is enabled by default. Another thing is that we do not configure ISAKMP Keys since

we do not use PSK anymore.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# authentication rsa-sig
R1(config-isakmp)# exit

R1(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R1(cfg-crypto-trans)#exit
R1(config)#crypto ipsec profile GETVPN-PROF
R1(ipsec-profile)# set transform-set TSET
R1(ipsec-profile)#exit

R1(config)#ip access-list standard GM-LIST
R1(config-std-nacl)# permit 10.1.25.5
R1(config-std-nacl)# permit 10.1.24.4
R1(config-std-nacl)# exit

R1(config)#ip access-list extended LAN-LIST
R1(config-ext-nacl)# deny udp any eq 848 any eq 848
R1(config-ext-nacl)# permit ip 192.168.0.0 0.0.255.255 192.168.0.0
0.0.255.255
R1(config-ext-nacl)#exit

R1(config)#crypto gdoi group GETVPN
R1(config-gdoi-group)# identity number 1
R1(config-gdoi-group)# server local
R1(gdoi-local-server)#
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R1(gdoi-local-server)# rekey lifetime seconds 400
R1(gdoi-local-server)# no rekey retransmit
R1(gdoi-local-server)# rekey authentication mypubkey rsa KS-KEYS
R1(gdoi-local-server)# rekey transport unicast
R1(gdoi-local-server)# authorization address ipv4 GM-LIST
R1(gdoi-local-server)#
%GDOI-5-KS_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
R1(gdoi-local-server)# sa ipsec 1
R1(gdoi-sa-ipsec)# profile GETVPN-PROF
R1(gdoi-sa-ipsec)# match address ipv4 LAN-LIST
R1(gdoi-sa-ipsec)# replay counter window-size 64
R1(gdoi-sa-ipsec)# address ipv4 10.1.12.1
R1(gdoi-local-server)#exit
R1(config-gdoi-group)#exit
```

Step 5 Configure R5 as GM.

Before configuring GM, ensure the time is synchronized.

```
R5(config)#do sh ntp status
Clock is synchronized, stratum 5, reference is 10.1.12.1
```

```
nominal freq is 250.0000 Hz, actual freq is 250.0001 Hz, precision
is 2**18
reference time is CEA97E83.4F5E1788 (19:07:47.310 UTC Sat Nov 14
2009)
clock offset is -5.0428 msec, root delay is 56.63 msec
root dispersion is 5.94 msec, peer dispersion is 0.85 msec
```

You need a trustpoint to be able to enroll the certificate
form CA.

```
R5(config)#crypto ca trustpoint R1-IOS-CA
R5(ca-trustpoint)#enrollment url http://10.1.12.1:80
R5(ca-trustpoint)#revocation-check none
R5(ca-trustpoint)#exi
```

Whe the trustpoint is ready, we need to download CA
certificate.

```
R5(config)#crypto ca authenticate R1-IOS-CA
Certificate has the following attributes:
    Fingerprint MD5: 1EDBC58C C0EC6E6A 30277787 757F752B
    Fingerprint SHA1: AC5AAD4E 6F972239 CD46EE23 45265D7A
A756B2C5
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Once we have the CA certificate, we can request a
certificate for the router itself. You do not need to
generate RSA keys. The keys will be automatically generated
during the enrollment process.

```
R5(config)#crypto ca enroll R1-IOS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.
```

```
Password:
RSA key size needs to be atleast 768 bits for ssh version 2
%SSH-5-ENABLED: SSH 1.5 has been enabled
%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:
```

```
% The subject name in the certificate will include: R5
```

```
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate R1-IOS-CA verbose' command will
show the fingerprint.

R5(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: C9AFC720 731E7669
48B60A5C 66A96152
CRYPTO_PKI: Certificate Request Fingerprint SHA1: 6384402D
15D72B7D 8E733C1A C6151667 B9E74C77
R5(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority

GM configuration is very similar to that presented in
previous lab, except authentication method.

R5(config)#crypto isakmp policy 10
R5(config-isakmp)# authentication rsa-sig
R5(config-isakmp)#exit

R5(config)#crypto gdoi group GETVPN
R5(config-gdoi-group)# identity number 1
R5(config-gdoi-group)# server address ipv4 10.1.12.1
R5(config-gdoi-group)#exit

R5(config)#ip access-list extended DO-NOT-ENCRYPT
R5(config-ext-nacl)# deny tcp 192.168.5.0 0.0.0.255 192.168.4.0
0.0.0.255 eq telnet
R5(config-ext-nacl)# deny tcp 192.168.4.0 0.0.0.255 eq telnet
192.168.5.0 0.0.0.255
R5(config-ext-nacl)# deny tcp 192.168.5.0 0.0.0.255 eq telnet
192.168.4.0 0.0.0.255
R5(config-ext-nacl)# deny tcp 192.168.4.0 0.0.0.255 192.168.5.0
0.0.0.255 eq telnet
R5(config-ext-nacl)#exit

R5(config)#crypto map CMAP-GETVPN 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R5(config-crypto-map)# set group GETVPN
R5(config-crypto-map)# match address DO-NOT-ENCRYPT
R5(config-crypto-map)#exit

R5(config)#int s0/1/0.52
R5(config-subif)#crypto map CMAP-GETVPN
R5(config-subif)#
%CRYPTO-5-GM_REGISTER: Start registration to KS 10.1.12.1 for group
GETVPN using address 10.1.25.5
```

```
R5(config-subif)#
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R5(config-subif)#exi
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.1 complete for
group GETVPN using address 10.1.25.5
```

See that R5 has sent registration request and registered successfully.

Step 6 Configure R4 as GM.

Same bunch of commands on second GM.

```
R4(config)#do sh ntp status
Clock is synchronized, stratum 5, reference is 10.1.12.1
nominal freq is 250.0000 Hz, actual freq is 249.9996 Hz, precision
is 2**18
reference time is CEA981C9.A89DB4CF (19:21:45.658 UTC Sat Nov 14
2009)
clock offset is 6.6896 msec, root delay is 56.52 msec
root dispersion is 6.76 msec, peer dispersion is 0.05 msec
```

```
R4(config)#crypto ca trustpoint R1-IOS-CA
R4(ca-trustpoint)#enrollment url http://10.1.12.1:80
R4(ca-trustpoint)#revocation-check none
R4(ca-trustpoint)#exi
```

```
R4(config)#crypto ca authenticate R1-IOS-CA
Certificate has the following attributes:
    Fingerprint MD5: 1EDBC58C C0EC6E6A 30277787 757F752B
    Fingerprint SHA1: AC5AAD4E 6F972239 CD46EE23 45265D7A
A756B2C5
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

```
R4(config)#cry ca enr R1-IOS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.
```

```
Password:
```

```
RSA key size needs to be atleast 768 bits for ssh version 2
%SSH-5-ENABLED: SSH 1.5 has been enabled
%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:

% The subject name in the certificate will include: R4
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate R1-IOS-CA verbose' command will
show the fingerprint.

R4(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: 9B4F4499 CC69D4F5
686DF42C 93D66C71
CRYPTO_PKI: Certificate Request Fingerprint SHA1: A53AE9D9
B2EF40C3 BC54FBC1 7FDB65B5 66A4A88E
R4(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority

R4(config)#crypto isakmp policy 10
R4(config-isakmp)# authentication rsa-sig
R4(config-isakmp)#exit

R4(config)#crypto gdoi group GETVPN
R4(config-gdoi-group)# identity number 1
R4(config-gdoi-group)# server address ipv4 10.1.12.1
R4(config-gdoi-group)#exit

R4(config)#ip access-list extended DO-NOT-ENCRYPT
R4(config-ext-nacl)# deny tcp 192.168.5.0 0.0.0.255 192.168.4.0
0.0.0.255 eq telnet
R4(config-ext-nacl)# deny tcp 192.168.4.0 0.0.0.255 eq telnet
192.168.5.0 0.0.0.255
R4(config-ext-nacl)# deny tcp 192.168.5.0 0.0.0.255 eq telnet
192.168.4.0 0.0.0.255
R4(config-ext-nacl)# deny tcp 192.168.4.0 0.0.0.255 192.168.5.0
0.0.0.255 eq telnet
R4(config-ext-nacl)#exit

R4(config)#crypto map CMAP-GETVPN 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R4(config-crypto-map)# set group GETVPN
R4(config-crypto-map)# match address DO-NOT-ENCRYPT
R4(config-crypto-map)#exit

R4(config)#int s0/0/0.42
R4(config-subif)#crypto map CMAP-GETVPN
```

```

R4(config-subif)#
%CRYPTO-5-GM_REGSTER: Start registration to KS 10.1.12.1 for group
GETVPN using address 10.1.24.4
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R4(config-subif)#exi
R4(config)#
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.1 complete for
group GETVPN using address 10.1.24.4

```

Verification

On KS check what GMs have been registered.

R1#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group GETVPN : 1

Group Member ID : 10.1.24.4

Group ID : 1

Group Name : GETVPN

Key Server ID : 10.1.12.1

Rekeys sent : 0

Rekeys retries : 0

Rekey Acks Rcvd : 0

Rekey Acks missed : 0

Sent seq num : 0 0 0 0

Rcvd seq num : 0 0 0 0

Group Member ID : 10.1.25.5

Group ID : 1

Group Name : GETVPN

Key Server ID : 10.1.12.1

Rekeys sent : 0

Rekeys retries : 0

Rekey Acks Rcvd : 0

Rekey Acks missed : 0

Sent seq num : 0 0 0 0

Rcvd seq num : 0 0 0 0

What group is configured on KS and what's the policy.

R1#sh crypto gdoi ks

Total group members registered to this box: 2

Key Server Information For Group GETVPN:

```

Group Name           : GETVPN
Group Identity       : 1
Group Members        : 2
IPSec SA Direction   : Both
ACL Configured:
    access-list LAN-LIST

```

R1#sh crypto gdoi ks acl

Group Name: GETVPN

Configured ACL:

```

access-list LAN-LIST deny udp any port = 848 any port = 848
access-list LAN-LIST permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

```

R1#sh crypto gdoi ks policy

Key Server Policy:

For group GETVPN (handle: 2147483650) server 10.1.12.1 (handle: 2147483650):

of teks : 1 Seq num : 0

KEK POLICY (transport type : Unicast)

```

spi : 0x9B0C69C0246B33C2A011A4E8A0C41ED5
management alg      : disabled      encrypt alg      : 3DES
crypto iv length    : 8              key size         : 24
orig life(sec): 400      remaining life(sec): 365
sig hash algorithm  : enabled        sig key length    : 162
sig size            : 128
sig key name        : KS-KEYS

```

TEK POLICY (encaps : ENCAPS_TUNNEL)

```

spi                : 0x325AC16C      access-list       : LAN-LIST
# of transforms     : 0              transform         : ESP_AES
hmac alg            : HMAC_AUTH_SHA
alg key size        : 16              sig key size       : 20
orig life(sec)      : 3600            remaining life(sec) : 3566
tek life(sec)       : 3600            elapsed time(sec)  : 34
antireplay window size: 64

```

R1#sh crypto gdoi ks rekey

Group GETVPN (Unicast)

```

Number of Rekeys sent           : 0
Number of Rekeys retransmitted  : 0
KEK rekey lifetime (sec)      : 400
    Remaining lifetime (sec)     : 355
Retransmit period               : 0
Number of retransmissions       : 0
IPSec SA 1 lifetime (sec)    : 3600

```

Remaining lifetime (sec) : 3556

R1#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.1	10.1.25.5	GDOI_IDLE	1001	ACTIVE
10.1.12.1	10.1.24.4	GDOI_IDLE	1002	ACTIVE

IPv6 Crypto ISAKMP SA

ISAKMP Sa has been established between KS and GMs.

R1#sh crypto ipsec sa

No SAs found

Note that there is no IPsec SA between KS and GM. The IPsec SAs are only on GMs.

R5#sh crypto gdoi gm

Group Member Information For Group GETVPN:

IPSec SA Direction	: Both
ACL Received From KS	: gdoi_group_GETVPN_temp_acl
Last rekey seq num	: 0
Re-register	
Remaining time	: 3412 secs ← default is 3600 secs (1 hour)
Retry Timer	
	:NOT RUNNING

R5#sh crypto gdoi gm acl

Group Name: GETVPN

ACL Downloaded From KS 10.1.12.1:

```
access-list deny udp any port = 848 any port = 848
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
```

ACL Configured Locally:

Map Name: CMAP-GETVPN

```
access-list DO-NOT-ENCRYPT deny tcp 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255 port
= 23
access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 port = 23 192.168.5.0
0.0.0.255
access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 port
= 23
access-list DO-NOT-ENCRYPT deny tcp 192.168.5.0 0.0.0.255 port = 23 192.168.4.0
0.0.0.255
```

R5#sh crypto gdoi gm rekey

Group GETVPN (Unicast)

```

Number of Rekeys received (cumulative)      : 0
Number of Rekeys received after registration : 0
Number of Rekey Acks sent                    : 0

```

Rekey (KEK) SA information :

	dst	src	conn-id	my-cookie	his-cookie
New	: 10.1.25.5	10.1.12.1	1005	A011A4E8	9B0C69C0
Current	: ---	---	---	---	---
Previous	: ---	---	---	---	---

R5#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.1	10.1.25.5	GDOI_IDLE	1001	ACTIVE
10.1.25.5	10.1.12.1	GDOI_REKEY	1005	ACTIVE

IPv6 Crypto ISAKMP SA

R5#sh crypto ipsec sa

interface: Serial0/1/0.52

Crypto map tag: CMAP-GETVPN, local addr 10.1.25.5

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)

remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)

current_peer 0.0.0.0 port 848

← there is no peer IP address

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.25.5, remote crypto endpt.: 0.0.0.0

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.52

current outbound spi: 0x325AC16C(844808556)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x325AC16C(844808556)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2011, flow_id: NETGX:11, sibling_flags 80000040, crypto map: CMAP-

GETVPN

sa timing: remaining key lifetime (sec): (3499)

IV size: 16 bytes

replay detection support: Y

```

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x325AC16C(844808556)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2012, flow_id: NETGX:12, sibling_flags 80000040, crypto map: CMAP-
GETVPN
  sa timing: remaining key lifetime (sec): (3499)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

R5#ping 192.168.4.4 so lo0

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.5
.....
Success rate is 0 percent (0/5)

```

R5#sh crypto ipsec sa | inc loca|remot|enca|deca

```

Crypto map tag: CMAP-GETVPN, local addr 10.1.25.5
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
local crypto endpt.: 10.1.25.5, remote crypto endpt.: 0.0.0.0

```

Note that ping is unsuccessful. However, packets are leaving the router and get encrypted. It means somewhere on the way to R4 packets are dropped. Take a look at R2.

R2#sh ip ro

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

Gateway of last resort is not set

```

10.0.0.0/24 is subnetted, 3 subnets
C      10.1.12.0 is directly connected, GigabitEthernet0/0
C      10.1.25.0 is directly connected, Serial0/1/0.25
C      10.1.24.0 is directly connected, Serial0/1/0.24

```

See, no routing to 192.168.4.0/24 and 192.168.5.0/24 networks. Those routes are necessary as GET VPN uses IPSec tunnel mode with IP header preservation, so the original IP header is used to route packets.

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 192.168.4.0 255.255.255.0 10.1.24.4
R2(config)#ip route 192.168.5.0 255.255.255.0 10.1.25.5
R2(config)#exi

```

R5#ping 192.168.4.4 so lo0

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.5
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

```

R5#sh crypto ipsec sa | inc loca|remot|enca|deca

```

Crypto map tag: CMAP-GETVPN, local addr 10.1.25.5
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
local crypto endpt.: 10.1.25.5, remote crypto endpt.: 0.0.0.0

```

Now all packets get encrypted and decrypted.

Same bunch of commands on the second GM.

R4#sh crypto gdoi

GROUP INFORMATION

```

Group Name          : GETVPN
Group Identity      : 1
Rekeys received     : 0
IPSec SA Direction  : Both
Active Group Server : 10.1.12.1
Group Server list    : 10.1.12.1

GM Reregisters in   : 3251 secs
Rekey Received(hh:mm:ss) : 00:05:08

```

```
Rekeys received
  Cumulative           : 0
  After registration   : 0
Rekey Acks sent        : 0
```

ACL Downloaded From KS 10.1.12.1:

```
access-list deny udp any port = 848 any port = 848
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
```

KEK POLICY:

```
Rekey Transport Type      : Unicast
Lifetime (secs)           : 394
Encrypt Algorithm         : 3DES
Key Size                  : 192
Sig Hash Algorithm        : HMAC_AUTH_SHA
Sig Key Length (bits)     : 1024
```

TEK POLICY for the current KS-Policy ACEs Downloaded:

Serial0/0/0.42:

```
IPsec SA:
  spi: 0x325AC16C(844808556)
  transform: esp-aes esp-sha-hmac
  sa timing:remaining key lifetime (sec): (3381)
  Anti-Replay : Disabled
```

R4#sh crypto gdoi gm rekey

Group GETVPN (Unicast)

```
Number of Rekeys received (cumulative)      : 0
Number of Rekeys received after registration : 0
Number of Rekey Acks sent                    : 0
```

Rekey (KEK) SA information :

	dst	src	conn-id	my-cookie	his-cookie
New	: 10.1.24.4	10.1.12.1	1005	A011A4E8	9B0C69C0
Current	: ---	---	---	---	---
Previous	: ---	---	---	---	---

TEST: Telnet from R5's loopback interface to R4's loopback interface.

1. Disable CEF switching on R2 to see packets going through the router.

```
R2(config)#int s0/1/0.25
R2(config-subif)#no ip route-cache
R2(config-subif)#int s0/1/0.24
R2(config-subif)#no ip route-cache
```

```
R2(config-subif)#exi
```

2. Enable debugging for all TELNET packets. Log to the buffer.

```
R2(config)#access-list 123 permit tcp any any eq telnet
R2(config)#access-list 123 permit tcp any eq telnet any
R2(config)#do deb ip pac det 123
IP packet debugging is on (detailed) for access list 123
```

```
R2(config)#logg buffered 7
R2(config)#logg on
```

```
R2(config)#do clear logg
Clear logging buffer [confirm]
R2(config)#
```

3. Telnet from R5's loopback0 to R4's loopback0.

```
R5#tel 192.168.4.4 /so lo0
Trying 192.168.4.4 ... Open
```

User Access Verification

Password:

```
R4>sh users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:06:21	
*514 vty 0		idle	00:00:00	192.168.5.5

Interface	User	Mode	Idle	Peer Address

```
R4>exit
```

[Connection to 192.168.4.4 closed by foreign host]

4. Back to R2 to see if any packets have been captured.

R2#sh logg

```
Syslog logging: enabled (12 messages dropped, 1 messages rate-limited,
                  0 flushes, 0 overruns, xml disabled, filtering disabled)
```

No Active Message Discriminator.

No Inactive Message Discriminator.

```
Console logging: level debugging, 564 messages logged, xml disabled,
                  filtering disabled
```

```
Monitor logging: level debugging, 0 messages logged, xml disabled,
                  filtering disabled
Buffer logging:  level debugging, 516 messages logged, xml disabled,
                  filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

No active filter modules.

ESM: 0 messages dropped

Trap logging: level informational, 55 message lines logged

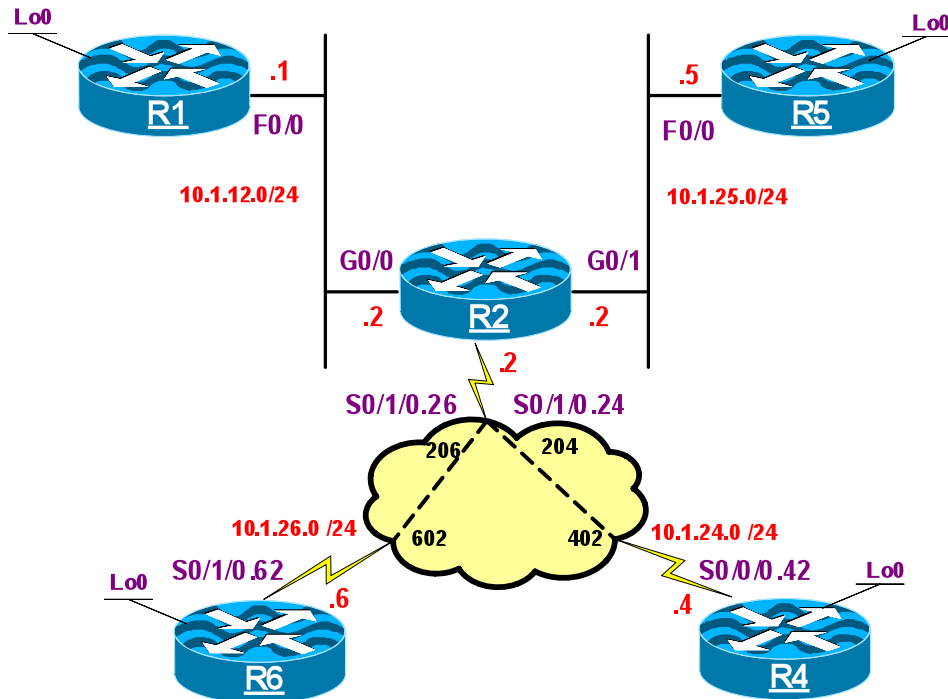
Log Buffer (4096 bytes):

```
IP: s=192.168.5.5 (Serial0/1/0.25), d=192.168.4.4 (Serial0/1/0.24), g=10.1.24.4, len
41, forward
TCP src=56259, dst=23, seq=1588224466, ack=5056452141, win=5768 ACK PSH
IP: tableid=0, s=192.168.4.4 (Serial0/0/0.24), d=192.168.5.5 (Serial0/0/0.25), routed
via FIB
IP: s=192.168.4.4 (Serial0/1/0.24), d=192.168.5.5 (Serial0/1/0.25), g=10.1.25.5, len
41, forward
TCP src=23, dst=56259, seq=5056452141, ack=1588224467, win=4078 ACK PSH
```

< output omitted >

See the source and destination IP addresses. Note the TELNET traffic is not encrypted (as there is port 23 seen in the capture).

Lab 1.58. GET VPN COOP (PKI)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's G0/1 and R5's F0/0 interface should be configured in VLAN 25
- R2's S0/1/0 and R6's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- R2's S0/1/0 and R4's S0/0/0 interface should be configured in a frame-relay point-to-point manner.
- Configure Telnet on all routers using password "cisco"
- Configure RIP version 2 dynamic routing on all routers (all directly connected interfaces).

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24

	F0/0	10.1.12.1/24
R2	G0/0	10.1.12.2/24
	G0/1	10.1.25.2/24
	S0/1/0.26	10.1.26.2/24
	S0/1/0.24	10.1.24.2/24
R4	Lo0	192.168.4.4/24
	S0/0/0.42	10.1.24.4/24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.25.5/24
R6	Lo0	192.168.6.6/24
	S0/1/0.62	10.1.26.6/24

Task 1

Configure NTP server with MD5 authentication (cisco123) and CA server on R1. It will be used for enrolling certificates for GET VPN Group Members.

Configure GET VPN solution for traffic going between 192.168.0.0/16 networks (LANs behind R6 and R4). R1 and R5 must be used as Key Servers and R6 and R4 are Group Members. Enable COOP protocol and ensure that R1 becomes Primary KS.

Use the following parameters for KS configuration:

Group name:	GETVPN
Server:	Identity 1 Primary KS IP address: 1.1.1.1 Secondary KS IP address: 5.5.5.5
Rekey:	Unicast 3 retransmits, every 10 seconds Lifetime 400 seconds RSA key name KS-KEYS
Authorization:	Only R6 and R4 GM routers
IPSec SA:	Time-based anti replay window 64

	Policy: 192.168.0.0/16, do not encrypt GDOI Encryption: AES-128 Integrity: SHA
ISAKMP Policy	Authentication: Certificates Encryption: DES Hashing: SHA

Do not encrypt TELNET traffic between 192.168.6.0/24 and 192.168.4.0/24 networks. This exception must be configured on GMs.



When designing and deploying GET VPN solution it is obvious that the Key Server is the most important component as it creates and maintains security policy for all GMs. If KS is down a new TEK cannot be delivered to GMs on time and when TEK's lifetime is over the GMs start dropping packets.

To address that issue, more KS servers should be deployed. However, it is not enough to just set up another KS as it would give out different TEK to its members. Thus, members of one KS couldn't send packets to members of second KS.

To resolve that issue, Cisco developed a new protocol called COOP (CO-OPERative KS protocol). This protocol is designed to synchronize both KS in terms of GMs info, keys (TEK, KEK), policy (ACL), pseudotime (for Time-based anti-replay protection).

Although all Key Servers accept registration from GMs, only one KS will be responsible for the rekey operation. This KS is called the Primary KS. The Primary KS is decided through an election process among all the co-operative Key Servers. In order to aid this process a priority number should be configured in each KS. If more than one Key Servers have the same highest priority, then the one with highest IP address will be selected.

Election process will be repeated whenever the existing primary KS goes down. It should be noted that when a new KS joins the group, election process will not be triggered even if the new KS has a higher priority than the existing primary.

Configuration

Complete these steps:

Step 1 Configure R1 as NTP server.

```
R1(config)#ntp master 4
R1(config)#ntp authentication-key 1 md5 cisco123
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate
```

Step 2 Configure R5 as NTP client to R1.

```
R5(config)#ntp authentication-key 1 md5 cisco123
R5(config)#ntp trusted-key 1
R5(config)#ntp authenticate
R5(config)#ntp server 10.1.12.1 key 1
```

Step 3 Configure R4 as NTP client to R1.

```
R4(config)#ntp authentication-key 1 md5 cisco123
R4(config)#ntp trusted-key 1
R4(config)#ntp authenticate
R4(config)#ntp server 10.1.12.1 key 1
```

Step 4 Configure R6 as NTP client to R1.

```
R6(config)#ntp authentication-key 1 md5 cisco123
R6(config)#ntp trusted-key 1
R6(config)#ntp authenticate
R6(config)#ntp server 10.1.12.1 key 1
```

Step 5 Configure CA and KS n R1.

```
R1(config)#do sh ntp status
Clock is synchronized, stratum 4, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision
is 2**18
reference time is CEA9949F.DC28907D (20:42:07.859 UTC Sat Nov 14
2009)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

```
R1(config)#do sh ntp asso
```

address	ref clock	st	when	poll	reach	delay
offset disp						
*~127.127.1.1	.LOCL.	3	10	16	77	0.000
0.000 187.72						

```
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
```

configured

R1 must have RSA keys for Rekey authentication. However, when there are more than one KS in the network, all KS must look the same for all GMS. Hence, we need to have the same RSA keys on both Kses. Keep in mind that you need to mark new RSA keys as "exportable" to be able to export them and import on another KS.

```
R1(config)#ip domain-name micronictstraining.com
```

```
R1(config)#crypto key generate rsa mod 1024 label KS-KEYS
exportable
```

The name for the keys will be: KS-KEYS

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be exportable...[OK]

```
R1(config)#
```

%SSH-5-ENABLED: SSH 1.99 has been enabled

```
R1(config)#ip http server
```

```
R1(config)#crypto pki server IOS-CA
```

```
R1(cs-server)#database url nvram:
```

% Server database url was changed. You need to move the
% existing database to the new location.

```
R1(cs-server)#database level minimum
```

```
R1(cs-server)#grant auto
```

```
R1(cs-server)#
```

%PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically
granted.

```
R1(cs-server)#no shut
```

%Some server settings cannot be changed after CA certificate
generation.

% Please enter a passphrase to protect the private key
% or type Return to exit

Password:

Re-enter password:

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.

```
R1(cs-server)#
```

%PKI-6-CS_ENABLED: Certificate server now enabled.

```
R1(cs-server)#crypto ca trustpoint R1-IOS-CA
```

```
R1(ca-trustpoint)# enrollment url http://10.1.12.1:80
```

```
R1(ca-trustpoint)# revocation-check none
```

```
R1(ca-trustpoint)#exi
```

```
R1(config)#cry ca auth R1-IOS-CA
Certificate has the following attributes:
    Fingerprint MD5: 4C94A45D 5200C2CF 99D4804C 34C1F733
    Fingerprint SHA1: BDE3C493 3A9A0B17 9A0AA601 3C7819DB
96F4220C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R1(config)#cry ca enr R1-IOS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.

Password:
%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:

% The subject name in the certificate will include:
R1.micronicstraining.com
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate R1-IOS-CA verbose' command will
show the fingerprint.

R1(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: E37524AF 52D5C9E7
AE626E90 C113B2F7
CRYPTO_PKI: Certificate Request Fingerprint SHA1: 424B180D
C8858DB2 CE02D530 1D29388E B7759993
R1(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority

    Configure RSA-SIG authentication for ISAKMP.

R1(config)#crypto isakmp policy 10
R1(config-isakmp)# authentication rsa-sig
R1(config-isakmp)#exi

R1(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R1(cfg-crypto-trans)#exi
```

```
R1(config)#crypto ipsec profile GETVPN-PROF
R1(ipsec-profile)# set transform-set TSET
R1(ipsec-profile)#exit

R1(config)#ip access-list standard GM-LIST
R1(config-std-nacl)# permit 10.1.26.6
R1(config-std-nacl)# permit 10.1.24.4
R1(config-std-nacl)#exit

R1(config)#ip access-list extended LAN-LIST
R1(config-ext-nacl)# deny udp any eq 848 any eq 848
R1(config-ext-nacl)# permit ip 192.168.0.0 0.0.255.255 192.168.0.0
0.0.255.255
R1(config-ext-nacl)#exit

R1(config)#crypto gdoi group GETVPN
R1(config-gdoi-group)# identity number 1
R1(config-gdoi-group)# server local
R1(gdoi-local-server)# rekey lifetime seconds 400
R1(gdoi-local-server)# rekey retransmit 10 number 3
R1(gdoi-local-server)# rekey authentication mypubkey rsa KS-KEYS
R1(gdoi-local-server)# rekey transport unicast
R1(gdoi-local-server)# authorization address ipv4 GM-LIST
R1(gdoi-local-server)#
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R1(gdoi-local-server)#
%GDOI-5-KS_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
R1(gdoi-local-server)# sa ipsec 1
R1(gdoi-sa-ipsec)# profile GETVPN-PROF
R1(gdoi-sa-ipsec)# match address ipv4 LAN-LIST
R1(gdoi-sa-ipsec)# replay counter window-size 64
R1(gdoi-sa-ipsec)# address ipv4 1.1.1.1
```

Here's the COOP configuration. We need to specify the priority of the KS (1-255, default is 1). The KS with higher priority wins. We need to specify the peer which is other KS. This IP address must be accessible on the network.

```
R1(gdoi-local-server)# redundancy
R1(gdoi-coop-ks-config)# local priority 100
R1(gdoi-coop-ks-config)# peer address ipv4 5.5.5.5
R1(gdoi-coop-ks-config)#
%GDOI-5-COOP_KS_ADD: 5.5.5.5 added as COOP Key Server in group
GETVPN.
R1(gdoi-coop-ks-config)#exit
R1(gdoi-local-server)#exit
R1(config-gdoi-group)#exit
```

Export RSA self-signed keys for using them on the second KS.

```
R1(config)#crypto key export rsa KS-KEYS pem terminal 3des cisco123
% Key name: KS-KEYS
Usage: General Purpose Key
Key data:
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmct4j/ecTlPumBNGlfWPMn1RE
/Rt/gTlWdhRDWwKmt8ftVFMU6rqjwjUqhn7hLRPortnBGS14t4UjK6IXzPLuxUbI
pgAlPn+PlDbpbpgZP4Iv9VDP7xbU+9AVVkJZpnYZLjo6aGQxBvHuLPA1S31+jSgXw
tDkjpNA1w48fHDAgYwIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,4C0424B43DE3EAC5

PjSONv50zJZWwAUA5vTRRdRffJmi5cn9yH+eTlSg1A5G1lKXmT5UhKucVMzHb1ep
XMaBacqt6QiJnib/MEHQAYjrbKSg5AyvplhTap+Vw/reOyMJovrDcCRmt3hzynz9
r/LXN/ykNKWeQvCr+YFglzMtptdEwQfhBA1P4eSMLCozP/r8Sd+oABMBIh4Im8kZ
Z3skBIKUT8CiNTmKDA3B/QMe2F1bcEeaA7r0CvoMQNWG9kLwhyQnnZzMjIPZ/yG8
4RrxmpWxrL3VOnAbAXxYu/fe597JKQEcp3XnURYnNHsh4dIphemlAAegPRHLCJQR
pd2an5I/Q4vAuVLaXgRRCuwe75fLUSZtk8UKAJXS3ZiOKbuABQ5QiLFS+S9Unnb2
1MLe3szgMKg6eyswYTFcXRNLauEyNhA4PMSxxLCPDeDaQr4XilB/iKMXy6ROMUhQ
OenTlu3vhjUzqxX+b/2IWYARvly+rKahA4XkRhXwctsYB2Gs9a+dvuC+n19JI5ys
zv++hUvrxAP1xfi/YM9tVMN91Rd8kZamIPwGFHgMk7wMwqwmDLljD2Qs+2wa8AtM
q+TvgQNUtqq9il0YHcRDZEiA5NWyNvcFFZKGN/+EqlalSX5VAKfnvndnQEY5RNcN9
BUpP7mLApWOBvAZz7vHC7/ZYaPeHtpabPaEvcqTXGc5mah6HLYPS0YhjWXs3XwRz
1czJ+cnBo6YXkvvTo4HefIfnnZHO+it8Y/chbny+/aVw1/fcdBwQ8137XL+b6jzG
sdHa5IyBbs+kIeNELJTg9W1NLNaxEUhXjTh525CEXnU=
-----END RSA PRIVATE KEY-----
```

Step 6 Configure R5 as secondary KS.

As the RSA keys for Rekey must be the same you must first import KS-KEYS on R5.

```
R5(config)#crypto key import rsa KS-KEYS pem exportable terminal
cisco123
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmct4j/ecTlPumBNGlfWPMn1RE
/Rt/gTlWdhRDWwKmt8ftVFMU6rqjwjUqhn7hLRPortnBGS14t4UjK6IXzPLuxUbI
pgAlPn+PlDbpbpgZP4Iv9VDP7xbU+9AVVkJZpnYZLjo6aGQxBvHuLPA1S31+jSgXw
tDkjpNA1w48fHDAgYwIDAQAB
-----END PUBLIC KEY-----

% Enter PEM-formatted encrypted private General Purpose key.
```



```
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,4C0424B43DE3EAC5

PjSONv50zJZWwAUA5vTRRdRffJmi5cn9yH+eTlSglA5GIlKXmT5UhKucVMzHb1ep
XMaBacqt6QiJnib/MEHQAYjrbKSg5AyvplhTap+Vw/reOyMJovrDcCRmt3hzynz9
r/LXN/ykNKWeQvCr+YFglzMtptdEwQfhBA1P4eSMLCozP/r8Sd+oABMBIh4Im8kZ
Z3skBIKUT8CiNtmKDA3B/QMe2F1bcEeaA7r0CvoMQNWG9kLwhyQnnZzmjIPZ/yG8
4RrxmpWxrL3VOnAbAXxYu/fe597JKQEcp3XnURYnNHsh4dIphemlAAegPRHLCJQR
pd2an5I/Q4vAuVLaXgRRCuwe75fLUSZtk8UKAJXS3ZiOKbuABQ5QiLFS+S9Unnb2
1MLe3szgMKg6eyswYTFcxRNLauEyNhA4PMSxxLCPDeDaQr4XilB/iKMXy6ROMuHQ
OenTlu3vhjUzqxX+b/2IWYARvly+rKahA4XkRhXwctsYB2Gs9a+dvuC+nl9JI5ys
zv++hUvrxAP1xfi/YM9tVMN91Rd8kZamIPwGFHgMk7wMwqwmdLljD2Qs+2wa8AtM
q+TvgQNUtqq9il0YHcRDZEiA5NWyNvcFFZKGn/+Eqla1SX5VAKfnvndnQEY5RncN9
BUpP7mLApWOBvAZz7vHC7/ZYaPeHtpabPaEvcqTXGc5mah6HLyPS0YhjWXs3XwRz
1czJ+cnBo6YXkvvTo4HefIfnnZHO+it8Y/chbny+/aVw1/fcdBwQ8137XL+b6jzG
sdHa5IyBbs+kIeNELJtg9W1NLNaxEUhXjTh525CEXnU=
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.
```

```
R5(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
R5(config)#ip domain-name micronicstraining.com
```

```
R5(config)#crypto ca trustpoint R1-IOS-CA
R5(ca-trustpoint)# enrollment url http://10.1.12.1:80
R5(ca-trustpoint)# revocation-check none
R5(ca-trustpoint)#exi
```

```
R5(config)#cry ca auth R1-IOS-CA
Certificate has the following attributes:
    Fingerprint MD5: 4C94A45D 5200C2CF 99D4804C 34C1F733
    Fingerprint SHA1: BDE3C493 3A9A0B17 9A0AA601 3C7819DB
96F4220C
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

```
R5(config)#cry ca enr R1-IOS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
```

Please make a note of it.

Password:

%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair

Re-enter password:

% The subject name in the certificate will include:

R5.micronicstraining.com

% Include the router serial number in the subject name? [yes/no]:

no

% Include an IP address in the subject name? [no]:

Request certificate from CA? [yes/no]: yes

% Certificate request sent to Certificate Authority

% The 'show crypto ca certificate R1-IOS-CA verbose' command will show the fingerprint.

R5(config)#

CRYPTO_PKI: Certificate Request Fingerprint MD5: B9ED0BDD 1450D537
91494EAD 94409D25

CRYPTO_PKI: Certificate Request Fingerprint SHA1: 40380C2E
F606F036 A678EAA9 1989B2AB 32EF79B1

R5(config)#

%PKI-6-CERTRET: Certificate received from Certificate Authority

R5(config)#crypto isakmp policy 10

R5(config-isakmp)# authentication rsa-sig

R5(config-isakmp)#exit

R5(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac

R5(cfg-crypto-trans)#exit

R5(config)#crypto ipsec profile GETVPN-PROF

R5(ipsec-profile)# set transform-set TSET

R5(ipsec-profile)#exit

R5(config)#ip access-list standard GM-LIST

R5(config-std-nacl)# permit 10.1.26.6

R5(config-std-nacl)# permit 10.1.24.4

R5(config-std-nacl)#exit

R5(config)#ip access-list extended LAN-LIST

R5(config-ext-nacl)# deny udp any eq 848 any eq 848

R5(config-ext-nacl)# permit ip 192.168.0.0 0.0.255.255 192.168.0.0
0.0.255.255

R5(config-ext-nacl)#exit

R5(config)#crypto gdoi group GETVPN

R5(config-gdoi-group)# identity number 1

R5(config-gdoi-group)# server local

R5(gdoi-local-server)#

%CRYPTO-6-GDOI_ON_OFF: GDOI is ON

```

R5(gdoi-local-server)# rekey lifetime seconds 400
R5(gdoi-local-server)# rekey retransmit 10 number 3
R5(gdoi-local-server)# rekey authentication mypubkey rsa KS-KEYS
R5(gdoi-local-server)# rekey transport unicast
R5(gdoi-local-server)# authorization address ipv4 GM-LIST
R5(gdoi-local-server)#
%GDOI-5-KS_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
R5(gdoi-local-server)#
%GDOI-4-COOP_KS_UNAUTH: Contact from unauthorized KS 1.1.1.1 in
group GETVPN at local address 5.5.5.5 (Possible MISCONFIG of
peer/local address)

```

No COOP configuration on R5 yet, so this message is displayed.

```

R5(gdoi-local-server)# sa ipsec 1
R5(gdoi-sa-ipsec)# profile GETVPN-PROF
R5(gdoi-sa-ipsec)# match address ipv4 LAN-LIST
R5(gdoi-sa-ipsec)# replay counter window-size 64
R5(gdoi-sa-ipsec)#exi
R5(gdoi-local-server)# address ipv4 5.5.5.5

```

COOP configuration on R5 - this KS has lower priority so that it will become Secondary KS.

```

R5(gdoi-local-server)# redundancy
R5(gdoi-coop-ks-config)# local priority 50
R5(gdoi-coop-ks-config)# peer address ipv4 1.1.1.1
R5(gdoi-coop-ks-config)#
%GDOI-5-COOP_KS_ADD: 1.1.1.1 added as COOP Key Server in group
GETVPN.
%GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GETVPN
(Previous Primary = NONE)
R5(gdoi-coop-ks-config)#exi
R5(gdoi-local-server)#exi
R5(config-gdoi-group)#exi
R5(config)#
%GDOI-5-COOP_KS_TRANS_TO_PRI: KS 1.1.1.1 in group GETVPN
transitioned to Primary (Previous Primary = NONE)

```

Note that the above message says that KS 1.1.1.1 has become Primary KS.

Step 7 Configure R6 as GM.

```

R6(config)#crypto ca trustpoint R1-IOS-CA
R6(ca-trustpoint)#enrollment url http://10.1.12.1:80

```

```
R6(ca-trustpoint)#revocation-check none
R6(ca-trustpoint)#exi

R6(config)#cry ca auth R1-IOS-CA
Certificate has the following attributes:
    Fingerprint MD5: 4C94A45D 5200C2CF 99D4804C 64C1F766
    Fingerprint SHA1: BDE6C496 6A9A0B17 9A0AA601 6C7819DB
96F4220C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R6(config)#cry ca enr R1-IOS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.

Password:
RSA key size needs to be atleast 768 bits for ssh version 2
%SSH-5-ENABLED: SSH 1.5 has been enabled
%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:

% The subject name in the certificate will include: R6
% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate R1-IOS-CA verbose' command will
show the fingerprint.

R6(config)#
CRYPTO_PKI: Certificate Request Fingerprint MD5: 5EBA522C FFA2108C
7ACEB4AD 28F16066
CRYPTO_PKI: Certificate Request Fingerprint SHA1: E10B1672
6EC20657 169EC6D1 109F612E 64BD8EE0
R6(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority

R6(config)#crypto isakmp policy 10
R6(config-isakmp)# authentication rsa-sig
R6(config-isakmp)#exi
```

```

R6(config)#crypto gdoi group GETVPN
R6(config-gdoi-group)# identity number 1
R6(config-gdoi-group)# server address ipv4 1.1.1.1
R6(config-gdoi-group)# server address ipv4 5.5.5.5
R6(config-gdoi-group)#exit

R6(config)#ip access-list extended DO-NOT-ENCRYPT
R6(config-ext-nacl)#deny tcp 192.168.6.0 0.0.0.255 192.168.4.0
0.0.0.255 eq telnet
R6(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 eq telnet
192.168.6.0 0.0.0.255
R6(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 192.168.6.0
0.0.0.255 eq telnet
R6(config-ext-nacl)#deny tcp 192.168.6.0 0.0.0.255 eq telnet
192.168.4.0 0.0.0.255
R6(config-ext-nacl)#exit

R6(config)#crypto map CMAP-GETVPN 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R6(config-crypto-map)# set group GETVPN
R6(config-crypto-map)# match address DO-NOT-ENCRYPT
R6(config-crypto-map)#exit

R6(config)#int s0/1/0.62
R6(config-subif)#crypto map CMAP-GETVPN
R6(config-subif)#
%CRYPTO-5-GM_REGISTER: Start registration to KS 1.1.1.1 for group
GETVPN using address 10.1.26.6
R6(config-subif)#exit
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R6(config)#
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 1.1.1.1 complete for
group GETVPN using address 10.1.26.6

```

GM has successfully registered to the Primary KS.

Step 8 Configure R4 as GM.

```

R4(config)#crypto ca trustpoint R1-IOS-CA
R4(ca-trustpoint)#enrollment url http://10.1.12.1:80
R4(ca-trustpoint)#revocation-check none
R4(ca-trustpoint)#exit

R4(config)#cry ca auth R1-IOS-CA
Certificate has the following attributes:
    Fingerprint MD5: 4C94A45D 5200C2CF 99D4804C 34C1F733
    Fingerprint SHA1: BDE3C493 3A9A0B17 9A0AA601 3C7819DB

```

96F4220C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R4(config)#cry ca enr R1-IOS-CA

%

% Start certificate enrollment ..

% Create a challenge password. You will need to verbally provide
this

password to the CA Administrator in order to revoke your
certificate.

For security reasons your password will not be saved in the
configuration.

Please make a note of it.

Password:

RSA key size needs to be atleast 768 bits for ssh version 2

%SSH-5-ENABLED: SSH 1.5 has been enabled

%CRYPTO-6-AUTOGEN: Generated new 512 bit key pair

Re-enter password:

% The subject name in the certificate will include: R4

% Include the router serial number in the subject name? [yes/no]:
no

% Include an IP address in the subject name? [no]:

Request certificate from CA? [yes/no]: yes

% Certificate request sent to Certificate Authority

% The 'show crypto ca certificate R1-IOS-CA verbose' command will
show the fingerprint.

R4(config)#

CRYPTO_PKI: Certificate Request Fingerprint MD5: 4F88B593 4469B0CE
91C579DB D454D96A

CRYPTO_PKI: Certificate Request Fingerprint SHA1: A3A48B4C
EC2BE242 50EF7B22 31ED7CEB EE5744AA

R4(config)#

%PKI-6-CERTRET: Certificate received from Certificate Authority

R4(config)#crypto isakmp policy 10

R4(config-isakmp)# authentication rsa-sig

R4(config-isakmp)#exi

R4(config)#crypto gdoi group GETVPN

R4(config-gdoi-group)# identity number 1

R4(config-gdoi-group)# server address ipv4 1.1.1.1

R4(config-gdoi-group)# server address ipv4 5.5.5.5

R4(config-gdoi-group)#exi

R4(config)#ip access-list extended DO-NOT-ENCRYPT

```

R4(config-ext-nacl)#deny tcp 192.168.6.0 0.0.0.255 192.168.4.0
0.0.0.255 eq telnet
R4(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 eq telnet
192.168.6.0 0.0.0.255
R4(config-ext-nacl)#deny tcp 192.168.4.0 0.0.0.255 192.168.6.0
0.0.0.255 eq telnet
R4(config-ext-nacl)#deny tcp 192.168.6.0 0.0.0.255 eq telnet
192.168.4.0 0.0.0.255
R4(config-ext-nacl)#exi

R4(config)#crypto map CMAP-GETVPN 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R4(config-crypto-map)# set group GETVPN
R4(config-crypto-map)# match address DO-NOT-ENCRYPT
R4(config-crypto-map)#exi

R4(config)#int s0/0/0.42
R4(config-subif)#crypto map CMAP-GETVPN
R4(config-subif)#
%CRYPTO-5-GM_REGISTER: Start registration to KS 1.1.1.1 for group
GETVPN using address 10.1.24.4
%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R4(config-subif)#exi
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GETVPN transitioned to Unicast
Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 1.1.1.1 complete for
group GETVPN using address 10.1.24.4

```

GM has successfully registered to the Primary KS.

Verification

R1#sh crypto gdoi ks

Total group members registered to this box: 2

Key Server Information For Group GETVPN:

```

Group Name           : GETVPN
Group Identity        : 1
Group Members         : 2
IPSec SA Direction    : Both
ACL Configured:
  access-list LAN-LIST
Redundancy            : Configured
  Local Address        : 1.1.1.1
  Local Priority        : 100
  Local KS Status      : Alive

```

Local KS Role : Primary

R1#sh crypto gdoi ks coop

Crypto Gdoi Group Name :GETVPN

Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 1.1.1.1

Local Priority: 100

Local KS Role: Primary , Local KS Status: Alive

Primary Timers:

Primary Refresh Policy Time: 20

Remaining Time: 10

Antireplay Sequence Number: 9

Peer Sessions:

Session 1:

Server handle: 2147483651

Peer Address: 5.5.5.5

Peer Priority: 50

Peer KS Role: Secondary , Peer KS Status: Alive

Antireplay Sequence Number: 3

IKE status: Established

Counters:

Ann msgs sent: 7

Ann msgs sent with reply request: 1

Ann msgs rcv: 1

Ann msgs rcv with reply request: 1

Packet sent drops: 1

Packet Recv drops: 0

Total bytes sent: 3713

Total bytes rcv: 591

Note that COOP leverages ISAKMP SA to securely transfer all information. Hence, when you use PSK for authentication you must remember to configure pre-shared key for Peer KS.

R1#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group GETVPN : 1

Group Member ID : 10.1.24.4

Group ID : 1

Group Name : GETVPN

Key Server ID : 1.1.1.1

Rekeys sent : 0

Rekeys retries : 0

Rekey Acks Rcvd : 0

Rekey Acks missed : 0

Sent seq num : 0 0 0 0

Rcvd seq num : 0 0 0 0

Group Member ID : 10.1.26.6

Group ID : 1

Group Name : GETVPN

Key Server ID : 1.1.1.1

Rekeys sent : 0

Rekeys retries : 0

Rekey Acks Rcvd : 0

Rekey Acks missed : 0

Sent seq num : 0 0 0 0

Rcvd seq num : 0 0 0 0

R1#sh crypto gdoi ks policy

Key Server Policy:

For group GETVPN (handle: 2147483650) server 1.1.1.1 (handle: 2147483650):

of teks : 1 Seq num : 0

KEK POLICY (transport type : Unicast)

spi : 0x3A67598E27379BA8F7613793A7A03C2F

management alg : disabled encrypt alg : 3DES

crypto iv length : 8 key size : 24

orig life(sec): 400 remaining life(sec): 294

sig hash algorithm : enabled sig key length : 162

sig size : 128

sig key name : KS-KEYS

TEK POLICY (encaps : ENCAPS_TUNNEL)

spi : 0xA175D05E access-list : LAN-LIST

of transforms : 0 transform : ESP_AES

hmac alg : HMAC_AUTH_SHA

alg key size : 16 sig key size : 20

orig life(sec) : 3600 remaining life(sec) : 3495

tek life(sec) : 3600 elapsed time(sec) : 105

antireplay window size: 64

For group GETVPN (handle: 2147483650) server 5.5.5.5 (handle: 2147483651):

R1#sh crypto gdoi ks rekey

Group GETVPN (Unicast)

Number of Rekeys sent : 1

Number of Rekeys retransmitted : 0

KEK rekey lifetime (sec) : 400

Remaining lifetime (sec) : 284

Retransmit period : 10

```
Number of retransmissions      : 3
IPSec SA 1  lifetime (sec)     : 3600
    Remaining lifetime (sec)   : 3485
```

R1#sh crypto gdoi ks replay

Anti-replay Information For Group GETVPN:

```
Timebased Replay:
    is not enabled
```

R1#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
1.1.1.1	10.1.24.4	GDOI_IDLE	1007	ACTIVE
1.1.1.1	10.1.26.6	GDOI_IDLE	1006	ACTIVE
5.5.5.5	1.1.1.1	GDOI_IDLE	1005	ACTIVE

IPv6 Crypto ISAKMP SA

See an additional ISAKMP SA between KSeS.

R1#sh crypto ipsec sa

No SAs found

R1#sh crypto ca certificates

Certificate

Status: Available

Certificate Serial Number (hex): 02

Certificate Usage: General Purpose

Issuer:

cn=IOS-CA

Subject:

Name: R1.micronicstraining.com

hostname=R1.micronicstraining.com

Validity Date:

start date: 04:58:59 UTC Jul 31 2010

end date: 04:58:59 UTC Jul 31 2011

Associated Trustpoints: R1-IOS-CA

CA Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=IOS-CA

Subject:

cn=IOS-CA

Validity Date:

```
start date: 04:57:49 UTC Jul 31 2010
end   date: 04:57:49 UTC Jul 30 2013
Associated Trustpoints: R1-IOS-CA IOS-CA
```

R5#sh crypto gdoi ks

Total group members registered to this box: 2

Key Server Information For Group GETVPN:

```
Group Name           : GETVPN
Group Identity       : 1
Group Members        : 2
IPSec SA Direction   : Both
ACL Configured:
  access-list LAN-LIST
Redundancy           : Configured
Local Address        : 5.5.5.5
Local Priority        : 50
Local KS Status      : Alive
Local KS Role        : Secondary
```

**Note the secondary KS has 2 members registered! This info has been sent from
Primary KS - no GMs has registered directly to that KS.**

R5#sh crypto gdoi ks coop

```
Crypto Gdoi Group Name :GETVPN
  Group handle: 2147483650, Local Key Server handle: 2147483650

  Local Address: 5.5.5.5
  Local Priority: 50
  Local KS Role: Secondary , Local KS Status: Alive
  Secondary Timers:
    Sec Primary Periodic Time: 30
    Remaining Time: 28, Retries: 0
    Invalid ANN PST recvd: 0
    New GM Temporary Blocking Enforced?: No
    Antireplay Sequence Number: 4

  Peer Sessions:
  Session 1:
    Server handle: 2147483651
    Peer Address: 1.1.1.1
    Peer Priority: 100
    Peer KS Role: Primary , Peer KS Status: Alive
    Antireplay Sequence Number: 12

    IKE status: Established
  Counters:
    Ann msgs sent: 1
```

```
Ann msgs sent with reply request: 1
Ann msgs rcv: 11
Ann msgs rcv with reply request: 1
Packet sent drops: 2
Packet Recv drops: 0
Total bytes sent: 591
Total bytes rcv: 5821
```

R5#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group GETVPN : 0

Group Member ID : 10.1.24.4

```
Group ID      : 1
Group Name    : GETVPN
Key Server ID : 1.1.1.1
Rekeys sent   : 0
Rekeys retries : 0
Rekey Acks Rcvd : 0
Rekey Acks missed : 0
```

```
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0
```

Group Member ID : 10.1.26.6

```
Group ID      : 1
Group Name    : GETVPN
Key Server ID : 1.1.1.1
Rekeys sent   : 0
Rekeys retries : 0
Rekey Acks Rcvd : 0
Rekey Acks missed : 0
```

```
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0
```

R5#sh crypto gdoi ks replay

Anti-replay Information For Group GETVPN:

```
Timebased Replay:
    is not enabled
```

R5#sh crypto gdoi ks rekey

Group GETVPN (Unicast)

```
Number of Rekeys sent           : 0
Number of Rekeys retransmitted  : 0
KEK rekey lifetime (sec)       : 400
Remaining lifetime (sec)       : 222
```

```
Retransmit period           : 10
Number of retransmissions   : 3
IPSec SA 1 lifetime (sec)   : 3600
    Remaining lifetime (sec) : 3423
```

R5#sh crypto gdoi ks policy

Key Server Policy:

For group GETVPN (handle: 2147483650) server 5.5.5.5 (handle: 2147483650):

For group GETVPN (handle: 2147483650) server 1.1.1.1 (handle: 2147483651):

of teks : 1 Seq num : 0

KEK POLICY (transport type : Unicast)

```
spi : 0x3A67598E27379BA8F7613793A7A03C2F
management alg      : disabled   encrypt alg      : 3DES
crypto iv length    : 8          key size             : 24
orig life(sec): 400      remaining life(sec): 215
sig hash algorithm  : enabled    sig key length    : 162
sig size            : 128
sig key name        : KS-KEYS
```

TEK POLICY (encaps : ENCAPS_TUNNEL)

```
spi           : 0xA175D05E   access-list      : LAN-LIST
# of transforms : 0          transform          : ESP_AES
hmac alg       : HMAC_AUTH_SHA
alg key size   : 16          sig key size      : 20
orig life(sec) : 3600        remaining life(sec) : 3416
tek life(sec)  : 3600        elapsed time(sec)  : 184
antireplay window size: 64
```

Compare the policy on the Secondary KS - it is exactly the same as it is on the Primary KS.

R5#sh crypto gdoi group GETVPN

```
Group Name           : GETVPN (Unicast)
Group Identity        : 1
Group Members         : 2
IPSec SA Direction    : Both
Active Group Server   : Local
Redundancy            : Configured
    Local Address     : 5.5.5.5
    Local Priority     : 50
    Local KS Status    : Alive
    Local KS Role      : Secondary
Group Rekey Lifetime  : 400 secs
Group Rekey
    Remaining Lifetime : 207 secs
Rekey Retransmit Period : 10 secs
Rekey Retransmit Attempts: 3
```

```
Group Retransmit
  Remaining Lifetime    : 0 secs

IPSec SA Number        : 1
IPSec SA Rekey Lifetime: 3600 secs
Profile Name           : GETVPN-PROF
Replay method          : Count Based
Replay Window Size     : 64
SA Rekey
  Remaining Lifetime    : 3408 secs
ACL Configured         : access-list LAN-LIST

Group Server list      : Local
```

R5#sh crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
5.5.5.5      10.1.24.4      GDOI_IDLE   1004 ACTIVE
5.5.5.5      1.1.1.1        GDOI_IDLE   1002 ACTIVE
5.5.5.5      10.1.26.6      GDOI_IDLE   1003 ACTIVE
```

```
IPv6 Crypto ISAKMP SA
```

See that Secondary KS has ISAKMP SA for every GM.

R5#sh crypto ipsec sa

```
No SAs found
```

R5#sh crypto ca certificates

```
Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
  cn=IOS-CA
Subject:
  Name: R5.micronicstraining.com
  hostname=R5.micronicstraining.com
Validity Date:
  start date: 05:01:24 UTC Jul 31 2010
  end   date: 05:01:24 UTC Jul 31 2011
Associated Trustpoints: R1-IOS-CA
```

```
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
```

```

Issuer:
  cn=IOS-CA
Subject:
  cn=IOS-CA
Validity Date:
  start date: 04:57:49 UTC Jul 31 2010
  end   date: 04:57:49 UTC Jul 30 2013
Associated Trustpoints: R1-IOS-CA

```

On GM we should see that it has been registered to Primary KS only.

R4#sh crypto gdoi gm

```

Group Member Information For Group GETVPN:
  IPSec SA Direction      : Both
  ACL Received From KS    : gdoi_group_GETVPN_temp_acl
  Last rekey seq num      : 0
  Re-register
    Remaining time        : 3206 secs
  Retry Timer
    :NOT RUNNING

```

R4#sh crypto gdoi gm acl

```

Group Name: GETVPN
ACL Downloaded From KS 1.1.1.1:
  access-list deny udp any port = 848 any port = 848
  access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
ACL Configured Locally:
  Map Name: CMAP-GETVPN
  access-list DO-NOT-ENCRYPT deny tcp 192.168.6.0 0.0.0.255 192.168.4.0 0.0.0.255 port
= 23
  access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 port = 23 192.168.6.0
0.0.0.255
  access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 192.168.6.0 0.0.0.255 port
= 23
  access-list DO-NOT-ENCRYPT deny tcp 192.168.6.0 0.0.0.255 port = 23 192.168.4.0
0.0.0.255

```

R4#sh crypto gdoi gm rekey

```

Group GETVPN (Unicast)
  Number of Rekeys received (cumulative)      : 0
  Number of Rekeys received after registration : 0
  Number of Rekey Acks sent                    : 0

Rekey (KEK) SA information :
      dst          src          conn-id  my-cookie  his-cookie
New      : 10.1.24.4      1.1.1.1      1007      F7613793      3A67598E
Current : ---            ---            ---      ---          ---
Previous: ---            ---            ---      ---          ---

```

R4#sh crypto gdoi gm replay

Anti-replay Information For Group GETVPN:

Timebased Replay:
is not enabled

R4#sh crypto gdoi group GETVPN

```

Group Name           : GETVPN
Group Identity       : 1
Rekeys received      : 0
IPSec SA Direction   : Both
Active Group Server   : 1.1.1.1
Group Server list     : 1.1.1.1
                     : 5.5.5.5

GM Reregisters in    : 3187 secs
Rekey Received(hh:mm:ss) : 00:08:49

```

```

Rekeys received
  Cumulative          : 0
  After registration   : 0
Rekey Acks sent       : 0

```

ACL Downloaded From KS 1.1.1.1:

```

access-list deny udp any port = 848 any port = 848
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

```

KEK POLICY:

```

Rekey Transport Type   : Unicast
Lifetime (secs)        : 330
Encrypt Algorithm       : 3DES
Key Size                : 192
Sig Hash Algorithm      : HMAC_AUTH_SHA
Sig Key Length (bits)   : 1024

```

TEK POLICY for the current KS-Policy ACEs Downloaded:

Serial0/0/0.42:

```

IPsec SA:
  spi: 0xA175D05E(2708852830)
  transform: esp-aes esp-sha-hmac
  sa timing:remaining key lifetime (sec): (3360)
  Anti-Replay : Disabled

```

R4#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id status
10.1.24.4	1.1.1.1	GDOI_REKEY	1007 ACTIVE

1.1.1.1	10.1.24.4	GDOI_IDLE	1006 ACTIVE
5.5.5.5	10.1.24.4	GDOI_IDLE	1004 ACTIVE

IPv6 Crypto ISAKMP SA

R4 does maintain ISKAMP SA with Primary and Secondary KS. This is because in case of Primary KS failure the KS does not need to renegotiate IKE Phase 1 to send Rekey messages.

R4#sh crypto ipsec sa

```
interface: Serial0/0/0.42
  Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4

protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
current peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0.42
current outbound spi: 0xA175D05E(2708852830)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xA175D05E(2708852830)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2009, flow_id: NETGX:9, sibling_flags 80000040, crypto map: CMAP-
GETVPN
    sa timing: remaining key lifetime (sec): (3346)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xA175D05E(2708852830)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
```

```

      conn id: 2010, flow_id: NETGX:10, sibling_flags 80000040, crypto map: CMAP-
GETVPN
      sa timing: remaining key lifetime (sec): (3346)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

```

R4#ping 192.168.6.6 so lo0

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.6, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/121/124 ms

```

Ping works fine because there is RIPv2 enabled in the network so that R2 knows about all networks.

R4#sh crypto ipsec sa | inc loca|remot|enca|deca

```

Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0

```

Counters has incremented. Let's try TELNET. It should be excluded from encryption.

R4#tel 192.168.6.6 /so lo0

```
Trying 192.168.6.6 ... Open
```

```
User Access Verification
```

```
Password:
```

```
R6>exit
```

```
[Connection to 192.168.6.6 closed by foreign host]
```

R4#sh crypto ipsec sa | inc loca|remot|enca|deca

```

Crypto map tag: CMAP-GETVPN, local addr 10.1.24.4
local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

```

local crypto endpt.: 10.1.24.4, remote crypto endpt.: 0.0.0.0

No counters are incremented! That's good.

R4#sh crypto ca certificates

Certificate

Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
 cn=IOS-CA
Subject:
 Name: R4
 hostname=R4
Validity Date:
 start date: 05:06:53 UTC Jul 31 2010
 end date: 05:06:53 UTC Jul 31 2011
Associated Trustpoints: R1-IOS-CA

CA Certificate

Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
 cn=IOS-CA
Subject:
 cn=IOS-CA
Validity Date:
 start date: 04:57:49 UTC Jul 31 2010
 end date: 04:57:49 UTC Jul 30 2013
Associated Trustpoints: R1-IOS-CA

Same bunch of commands on R6.

R6#sh crypto gdoi gm

Group Member Information For Group GETVPN:
 IPSec SA Direction : Both
 ACL Received From KS : gdoi_group_GETVPN_temp_acl
 Last rekey seq num : 0
 Re-register
 Remaining time : 3159 secs
 Retry Timer
 :NOT RUNNING

R6#sh crypto gdoi gm acl

Group Name: GETVPN
ACL Downloaded From KS 1.1.1.1:
 access-list deny udp any port = 848 any port = 848
 access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
ACL Configured Locally:
Map Name: CMAP-GETVPN

```

access-list DO-NOT-ENCRYPT deny tcp 192.168.6.0 0.0.0.255 192.168.4.0 0.0.0.255 port
= 23
access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 port = 23 192.168.6.0
0.0.0.255
access-list DO-NOT-ENCRYPT deny tcp 192.168.4.0 0.0.0.255 192.168.6.0 0.0.0.255 port
= 23
access-list DO-NOT-ENCRYPT deny tcp 192.168.6.0 0.0.0.255 port = 23 192.168.4.0
0.0.0.255

```

R6#sh crypto gdoi gm rekey

Group GETVPN (Unicast)

```

Number of Rekeys received (cumulative)      : 0
Number of Rekeys received after registration : 0
Number of Rekey Acks sent                    : 0

```

Rekey (KEK) SA information :

	dst	src	conn-id	my-cookie	his-cookie
New	: 10.1.26.6	1.1.1.1	1007	F7613793	3A67598E
Current	: ---	---	---	---	---
Previous	: ---	---	---	---	---

R6#sh crypto gdoi group GETVPN

```

Group Name           : GETVPN
Group Identity       : 1
Rekeys received      : 0
IPSec SA Direction   : Both
Active Group Server   : 1.1.1.1
Group Server list     : 1.1.1.1
                     : 5.5.5.5

```

```

GM Reregisters in    : 3144 secs
Rekey Received(hh:mm:ss) : 00:10:37

```

```

Rekeys received
Cumulative           : 0
After registration   : 0
Rekey Acks sent      : 0

```

ACL Downloaded From KS 1.1.1.1:

```

access-list deny udp any port = 848 any port = 848
access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

```

KEK POLICY:

```

Rekey Transport Type : Unicast
Lifetime (secs)      : 344
Encrypt Algorithm     : 3DES
Key Size              : 192

```

```
Sig Hash Algorithm      : HMAC_AUTH_SHA
Sig Key Length (bits)  : 1024
```

TEK POLICY for the current KS-Policy ACEs Downloaded:

Serial0/1/0.62:

IPsec SA:

```
spi: 0xA175D05E(2708852830)
transform: esp-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (3252)
Anti-Replay : Disabled
```

R6#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.26.6	1.1.1.1	GDOI_REKEY	1007	ACTIVE
1.1.1.1	10.1.26.6	GDOI_IDLE	1006	ACTIVE
5.5.5.5	10.1.26.6	GDOI_IDLE	1004	ACTIVE

IPv6 Crypto ISAKMP SA

R6#sh crypto ipsec sa

interface: Serial0/1/0.62

Crypto map tag: CMAP-GETVPN, local addr 10.1.26.6

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)

remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)

current_peer 0.0.0.0 port 848

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.26.6, remote crypto endpt.: 0.0.0.0

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0.62

current outbound spi: 0xA175D05E(2708852830)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xA175D05E(2708852830)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2009, flow_id: NETGX:9, sibling_flags 80000040, crypto map: CMAP-

GETVPN

sa timing: remaining key lifetime (sec): (3240)

```
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xA175D05E(2708852830)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2010, flow_id: NETGX:10, sibling_flags 80000040, crypto map: CMAP-
GETVPN
sa timing: remaining key lifetime (sec): (3240)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Same SPI number for Inbound and Outbound. This SPI is exactly the same on every GM.

R6#sh crypto ca certificates

```
Certificate
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
Issuer:
cn=IOS-CA
Subject:
Name: R6
hostname=R6
Validity Date:
start date: 05:05:54 UTC Jul 31 2010
end date: 05:05:54 UTC Jul 31 2011
Associated Trustpoints: R1-IOS-CA
```

```
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=IOS-CA
Subject:
cn=IOS-CA
Validity Date:
```

start date: 04:57:49 UTC Jul 31 2010
end date: 04:57:49 UTC Jul 30 2013
Associated Trustpoints: R1-IOS-CA

This page is intentionally left blank.

**Advanced
CCIE SECURITY v4
LAB WORKBOOK**

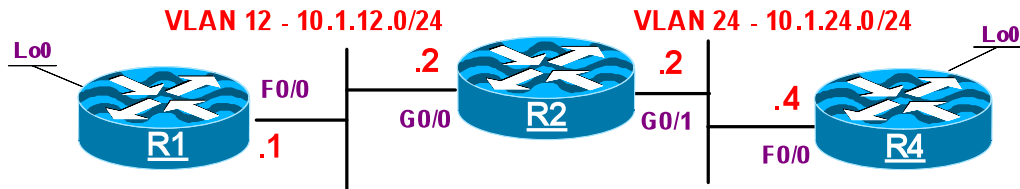
Remote Access VPN

**Narbik Kocharians
CCIE #12410 (R&S, Security, SP)
CCSI #30832**

**Piotr Matusiak
CCIE #19860 (R&S, Security)
C|EH, CCSI #33705**

www.MicronicsTraining.com

Lab 1.59. Configuring Remote Access IPsec VPN using EasyVPN (IOS to IOS)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's G0/1 and R4's F0/0 interface should be configured in VLAN 24
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1 and R4 pointing to the R2

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.12.1/24
R2	G0/0	10.1.12.2/24
	G0/1	10.1.24.2/24
R4	Lo0	4.4.4.4/24
	F0/0	10.1.24.4/24

Task 1

Configure R4 as the EasyVPN Server. Enable AAA on the router and configure network authorization based on the local database. Use MicronicsTraining.com as a domain name. Configure the following ISAKMP and IPsec Policies:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Group: 2

- Encryption: 3DES
- IPsec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-MD5-HMAC

Configure IP address pool named VPN_POOL and give out IP addresses from the range of 192.168.25.1 to 192.168.25.10.

Create ISAKMP client group of SALES and allow VPN connections for Sales Department with the following parameters:

Key = cisco123

DNS address = 10.1.12.5

WINS address = 10.1.12.6

Domain Name = MicronicsTraining.com

Pool = VPN_POOL

Use dynamic crypto map and configure it to inject route information from connected VPN Clients into the routing table.

Configure R1 as EasyVPN Remote and connect to the R4 using automatic Client Mode.



Easy VPN is a Cisco way of doing Remote Access VPNs. The idea behind it is to configure Secure Gateway (the device which terminates Remote Access VPNs) and minimize configuration burden on the Client.

This technology has been developed for Cisco IPsec Client and so-called hardware clients i.e. ASA 5505 or IOS routers.

In EasyVPN the Client does not need to configure any ISAKMP or IPsec parameters, all those parameters are negotiated during the connection. The EasyVPN Server must use Diffie-Hellman Group 2 to be able to negotiate parameters with the client. Because the first aggressive mode packet contains the Diffie-Hellman public value, only a single Diffie-Hellman group may be specified in the proposal. Each client must however supply EasyVPN Group name and password to be used for authentication and policy configuration. The policy is a bunch of attributes that may be sent down to the clients during the connection. Those attributes/parameters include DNS/WINS server, domain name, IP address pool, etc.

Easy VPN uses IKE Aggressive mode for connection, so that the group name is sent to the EasyVPN Server in the very first message. The group name is not encrypted so that it is easy to sniff. Hence, there was another security

mechanism configured called Extended Authentication (XAuth for short). This requires supplying additional user credentials during IKE Phase 1.5. This phase is already secured by ISAKMP SA so that all information is encrypted.

Configuration

Complete these steps:

Step 1 R4 configuration.

First configure AAA to allow ISAKMP key lookup in the local routers database. This is required for EasyVPN only. It is not required for Site-to-Site VPNs.

```
R4(config)#aaa new-model
R4(config)#aaa authorization network VPN_AUTH local

R4(config)#ip domain-name MicronicsTraining.com
```

Configure ISAKMP policy with DH Group 2.

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)# auth pre-share
R4(config-isakmp)# gr 2
R4(config-isakmp)# enc 3des
R4(config-isakmp)#exi

R4(config)#crypto ipsec transform-set TSET esp-3des esp-md5-hmac
R4(cfg-crypto-trans)#exi
```

A pool of IP addresses for remote clients must be configured on the router. The client will get next free IP address from the pool and use it on its VPNC interface.

```
R4(config)#ip local pool VPN_POOL 192.168.25.1 192.168.25.10
```

EasyVPN group with all parameters used in IKE Phase 1.5 must be configured on the EasyVPN Server. The client will use the group name and the password during connection. The very first ISAKMP packet will contain group name so that it will land in the correct group on the server.

```
R4(config)#crypto isakmp client configuration group SALES
R4(config-isakmp-group)#key cisco123
R4(config-isakmp-group)#dns 10.1.12.5
R4(config-isakmp-group)#wins 10.1.12.6
R4(config-isakmp-group)#domain MicronicsTraining.com
R4(config-isakmp-group)#pool VPN_POOL
```

```
R4(config-isakmp-group)#exi
```

The Remote Access networks are Hub-and-Spoke by design. Hence, the regular crypto map cannot be used in this case. To address that, a dynamic crypto map has been introduced. It specifies IPSec policy and is attached to regular crypto map. This is because only regular (static) crypto map can be attached to the interface.

```
R4(config)#crypto dynamic-map DYNMAP 10
R4(config-crypto-map)#set transform-set TSET
R4(config-crypto-map)#reverse-route
R4(config-crypto-map)#exi
```

We need to configure the crypto map so that it may consult local database for pre shared keys. The second command is to send out an IP address to the client. The Cisco IPSec Client asks the server for a bunch of attributes during IKE Phase 1.5 so that the server must "respond" to that request. One of those attributes is IP address.

```
R4(config)#crypto map VPN isakmp authorization list VPN_AUTH
R4(config)#crypto map VPN client configuration address respond
```

```
R4(config)#crypto map VPN 10 ipsec-isakmp dynamic DYNMAP
```

Finally we need to attach dynamic crypto map to static crypto map and then to the interface.

```
R4(config)#int f0/0
R4(config-if)#crypto map VPN
R4(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R4(config-if)#exi
```

Step 2 R1 configuration.

Client configuration is minimal by design. It is even more minimalistic when using software IPSec Client. All we need is to configure EasyVPN Group, specify the password and EasyVPN server's IP address. There are three modes:

- Client - default option, the EasyVPN Client gets an IP address from the server but all traffic from this client is translated (PAT) to that address, the mode is secure and is appropriate for most remote access clients
- Network Extension - the client works like it is a part of the company's network. The client's IP address (not assigned by the server) must be routable in the company's network.
- Network Extension Plus - similar to the previous one but in

this case the client gets an IP address from the server and assigns it to its loopback interface. This IP address may be used for management purposes.

There are three connection methods:

- Auto - means that the client initiates the tunnel setup as soon as the EasyVPN is enabled on the interfaces.
- Manual - the client waits for a command to set up the tunnel
- ACL - tunnel will be initiated as soon as interesting traffic (ACL) is seen on the network

```
R1(config)#crypto ipsec client ezvpn EZ
R1(config-crypto-ezvpn)#group SALES key cisco123
R1(config-crypto-ezvpn)#peer 10.1.24.4
R1(config-crypto-ezvpn)#connect auto
R1(config-crypto-ezvpn)#mode client
```

EasyVPN on hardware clients must be attached to the interfaces. Like NAT there must be Inside interface and Outside interface. Traffic coming from the Inside to the Outside triggers EasyVPN tunnel.

```
R1(config-crypto-ezvpn)#int loopback0
R1(config-if)#crypto ipsec client ezvpn EZ inside

R1(config-if)#int f0/0
R1(config-if)#crypto ipsec client ezvpn EZ outside
R1(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client) User= Group=SALES
Client_public_addr=10.1.12.1 Server_public_addr=10.1.24.4
Assigned_client_addr=192.168.25.1
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback10000, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to
up
```

See that NVI0 interface. It is for NAT as the EasyVPN is in Client mode.

Verification

```
R1#sh int lo10000
```

Loopback10000 is up, line protocol is up

Hardware is Loopback

```
Description: *** Internally created by EzVPN ***
```

```
Internet address is 192.168.25.1/32
```

```

MTU 1514 bytes, BW 8000000 Kbit/sec, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation LOOPBACK, loopback not set
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out

```

R1#sh crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

```

Tunnel name : EZ
Inside interface list: Loopback0
Outside interface: FastEthernet0/0
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Address: 192.168.25.1 (applied on Loopback10000)
Mask: 255.255.255.255
DNS Primary: 10.1.12.5
NBMS/WINS Primary: 10.1.12.6
Default Domain: MicronicsTraining.com
Save Password: Disallowed
Current EzVPN Peer: 10.1.24.4

```

All parameters have been downloaded from the server.

R1#sh crypto isakmp sa

```

IPv4 Crypto ISAKMP SA

```

dst	src	state	conn-id	status
10.1.24.4	10.1.12.1	QM_IDLE	1001	ACTIVE

```

IPv6 Crypto ISAKMP SA

```

R1#ping 4.4.4.4

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

```


The ping is unsuccessful. This is because the traffic must come from Inside interface (Loopback0).

R1#ping 4.4.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R1#sh crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.12.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.25.1/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 10.1.24.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

The packets have been encrypted/decrypted. Note the Proxy IDs. All from client's IP address towards any network will be encrypted.

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.24.4

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x5C5F537B(1549751163)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x122946D2(304694994)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map:

FastEthernet0/0-head-0

sa timing: remaining key lifetime (k/sec): (4481002/3479)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

```

outbound esp sas:
  spi: 0x5C5F537B(1549751163)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4481002/3479)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

R1#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

1.0.0.0/24 is subnetted, 1 subnets
C      1.1.1.0 is directly connected, Loopback0
192.168.25.0/32 is subnetted, 1 subnets
C      192.168.25.1 is directly connected, Loopback10000
10.0.0.0/24 is subnetted, 1 subnets
C      10.1.12.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.1.12.2

```

There is a new interface on the router. This interface is used for NAT.

R4#sh crypto isakmp sa

```

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.1.24.4    10.1.12.1    QM_IDLE       1001 ACTIVE

IPv6 Crypto ISAKMP SA

```

R4#sh crypto ipsec sa

```

interface: FastEthernet0/0
  Crypto map tag: VPN, local addr 10.1.24.4

```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.25.1/255.255.255.255/0/0)
current_peer 10.1.12.1 port 500
  PERMIT, flags={}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.24.4, remote crypto endpt.: 10.1.12.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x122946D2(304694994)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x5C5F537B(1549751163)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: VPN
    sa timing: remaining key lifetime (k/sec): (4547943/3455)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0x122946D2(304694994)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: VPN
    sa timing: remaining key lifetime (k/sec): (4547943/3455)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:
```

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.24.2 to network 0.0.0.0

```

192.168.25.0/32 is subnetted, 1 subnets
S    192.168.25.1 [1/0] via 10.1.12.1
4.0.0.0/24 is subnetted, 1 subnets
C    4.4.4.0 is directly connected, Loopback0
10.0.0.0/24 is subnetted, 1 subnets
C    10.1.24.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.24.2

```

There is a "dynamic" static route on the server. This static route is automatically created for every client. This is necessary for R4 to know how to route packets to that network. This static route may be redistributed to you dynamic routing protocol to let the client access rest of your network. This has been described in detail in the lab for RRI.

R4#tel 192.168.25.1

Trying 192.168.25.1 ... Open

User Access Verification

Password:

R1>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:45	
*514 vty 0		idle	00:00:00	10.1.24.4

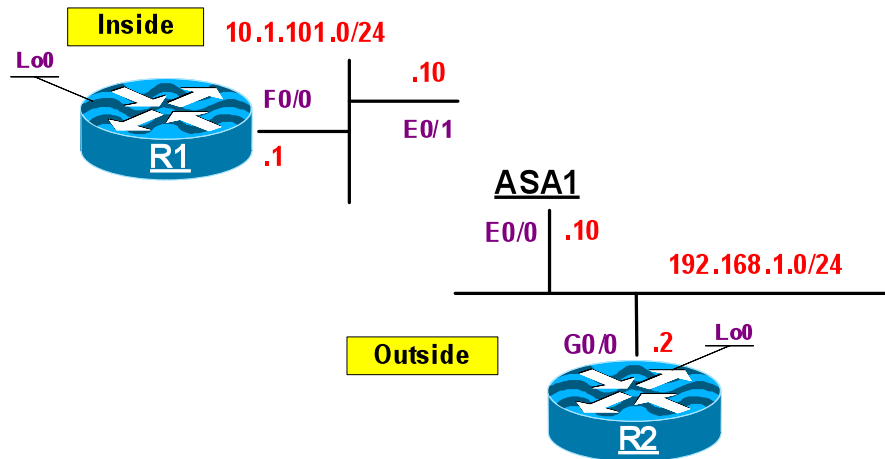
Interface	User	Mode	Idle	Peer Address

R1>exit

[Connection to 192.168.25.1 closed by foreign host]

Note that we can connect to the R1 from R4 using this IP address. However, connection to the clients behind R1 (if any) cannot be established. This is because of PAT performed on R1.

Lab 1.60. Configuring Remote Access IPSec VPN using EasyVPN (IOS to ASA)



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1 and R2 pointing to the respective ASA interface
- Configure default routing on ASA1 to the R2

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	Lo0	2.2.2.2/24
ASA1	E0/0, Outside, Security 0	192.168.1.10/24
	E0/1, Inside, Security 100	10.1.101.10/24

Task 1

Configure ASA1 as the EasyVPN Server. Users connecting to the ASA1 should be authenticated using local database with a username of “salesman” and password of “sales123”. Configure the following ISAKMP and IPSec Policies:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Group: 2
 - Encryption: 3DES
 - Hash : SHA
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC

Configure IP address pool named VPN_POOL and give out IP addresses from the range of 192.168.25.1 to 192.168.25.10.

Create ISAKMP client group of SALES and allow VPN connections for Sales Department with the following parameters:

Key = cisco123

Pool = VPN_POOL

Configure R2 as EasyVPN Remote and connect to the ASA1 using Client Mode.



Cisco ASA is secure gateway by design. It is created to terminate Site-to-Site and Remote Access VPNs. However, the configuration is slightly different than on IOS. The ASA uses so-called Tunnel Groups and Group Policies to configure EasyVPN Server. The Tunnel Group term has been taken from VPN Concentrator and is called Connection Profile in the ASDM.

Configuration

Complete these steps:

Step 1 ASA configuration.

First of all, remember that the ASA has NO ISAKMP enabled by default! We are asked to enable user authentication (xauth) so that we need a user account in the local database on the ASA.

```
ASA1(config)# username salesman password sales123
ASA1(config)# isakmp enable Outside
```

ISAKMP Policy is configured in the same way as it is in IOS. Alternatively we can configure every parameter in a new line as showed below. Remember to configure DH Group 2 or higher.

```
ASA1(config)# crypto isakmp policy 1 authentication pre-share
ASA1(config)# crypto isakmp policy 1 encryption 3des
ASA1(config)# crypto isakmp policy 1 hash sha
ASA1(config)# crypto isakmp policy 1 group 2
```

Next, configure a pool of IP addresses to be given out to the clients.

```
ASA1(config)# ip local pool VPN_POOL 10.1.25.1-10.1.25.10 mask
255.255.255.0
```

There are two types of Tunnel Group: (1) remote-access and ipsec-l2l. The type must be specified at the beginning as this defines a list of attributes available for configuration.

In our case we need to specify at least one general attribute, which is IP address pool. There are also "ipsec-attributes" which are related to IPSec, like PSK, Trustpoint, etc. All IKE Phase 1.5 attributes can be configured under Group Policy which can be specified under "general-attributes".

```
ASA1(config)# tunnel-group SALES type remote-access
ASA1(config)# tunnel-group SALES general-attributes
ASA1(config-tunnel-general)# address-pool VPN_POOL
ASA1(config-tunnel-general)# exit
```

```
ASA1(config)# tunnel-group SALES ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key cisco123
ASA1(config-tunnel-ipsec)# exit
```

Do you remember that there must be dynamic crypto map used for Remote Access VPNs? Hence, we need to configure dynamic crypto map first to specify the IPSec parameters (transform set) and then assign it to static crypto map. The static crypto map can be applied to the interface.

```
ASA1(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac

ASA1(config)# crypto dynamic-map DYN-MAP 5 set transform-set TSET

ASA1(config)# crypto map ENCRYPT_OUT 1 ipsec-isakmp dynamic DYN-MAP
```

```
ASA1(config)# crypto map ENCRYPT_OUT interface Outside

ASA1(config)# route Inside 1.1.1.1 255.255.255.255 10.1.101.1
```

Step 2 R2 configuration.

EasyVPN Client (officially called Cisco EasyVPN Remote) configuration is straight forward and has been described in the previous lab.

```
R2(config)#crypto ipsec client ezvpn EZ
R2(config-crypto-ezvpn)#group SALES key cisco123
R2(config-crypto-ezvpn)#peer 192.168.1.10
R2(config-crypto-ezvpn)#connect auto
R2(config-crypto-ezvpn)#mode client

R2(config-crypto-ezvpn)#int loopback0
R2(config-if)#crypto ipsec client ezvpn EZ inside

R2(config-if)#int g0/0
R2(config-if)#crypto ipsec client ezvpn EZ outside
R2(config-if)#end

%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
```

As soon as you apply the crypto map on the interface you'll notice the following message on the console:

```
EZVPN(EZ): Pending XAuth Request, Please enter the following
command:
EZVPN: crypto ipsec client ezvpn xauth
```

This message appears only then there is "auto" connection configured on the EasyVPN Remote. You must use the following command and provide username and password for XAUTH authentication.

```
R2#crypto ipsec client ezvpn xauth
Username: salesman
Password:
R2#
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client) User= Group=SALES
Client_public_addr=192.168.1.2 Server_public_addr=192.168.1.10
Assigned_client_addr=10.1.25.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback10000,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state
to up
```

After successful authentication, the client gets an IP

address from the pool and brings up its logical interfaces.
From now on, the traffic going between inside and outside interface will be encrypted.

Verification

R2#pi 1.1.1.1 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 2.2.2.2

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

2.0.0.0/24 is subnetted, 1 subnets

C 2.2.2.0 is directly connected, Loopback0

10.0.0.0/32 is subnetted, 1 subnets

C 10.1.25.1 is directly connected, Loopback10000

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

S* 0.0.0.0/0 [1/0] via 192.168.1.10

The ping is successful. Note that the client has only default route configured.

Thus, all traffic to the other networks will be sending out using this next hop.

R2#sh crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

Tunnel name : EZ

Inside interface list: Loopback0

Outside interface: GigabitEthernet0/0

Current State: IPSEC_ACTIVE

Last Event: MTU_CHANGED

Address: 10.1.25.1 (applied on Loopback10000)

Mask: 255.255.255.255

Save Password: Disallowed
 Current EzVPN Peer: 192.168.1.10

R2#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
192.168.1.10	192.168.1.2	QM_IDLE	1001	ACTIVE

IPv6 Crypto ISAKMP SA

R2#sh crypto ipsec sa

interface: GigabitEthernet0/0

Crypto map tag: GigabitEthernet0/0-head-0, local addr 192.168.1.2

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.25.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 192.168.1.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

Traffic has been encrypted. Note that proxy IDs are for any destination - this is because by default the EasyVPN Remote will encrypt all traffic. You must use Split-Tunneling feature to change that behavior.

local crypto endpt.: 192.168.1.2, remote crypto endpt.: 192.168.1.10

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0

current outbound spi: 0xA422A55(172108373)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xB7ED79A2(3085793698)

transform: esp-3des esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000046, crypto map:

GigabitEthernet0/0-head-0

sa timing: remaining key lifetime (k/sec): (4442797/28679)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

```

inbound pcp sas:

outbound esp sas:
  spi: 0xA422A55(172108373)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000046, crypto map:
GigabitEthernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4442797/28679)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

ASA1(config)# sh crypto isakmp sa detail

```

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.1.2
   Type    : user                Role    : responder
   Rekey    : no                 State    : AM_ACTIVE
   Encrypt  : 3des               Hash     : SHA
   Auth     : preshared          Lifetime: 86400
   Lifetime Remaining: 86363

```

The ASA is a headend of the EasyVPN so that it acts as "responder" for the clients. Note that in EasyVPN we use Aggressive Mode when PSK is used for authentication.

ASA1(config)# sh route

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

```

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

```

S    1.1.1.1 255.255.255.255 [1/0] via 10.1.101.1, Inside
S    10.1.25.1 255.255.255.255 [1/0] via 192.168.1.2, Outside
C    10.1.101.0 255.255.255.0 is directly connected, Inside

```

```
C    192.168.1.0 255.255.255.0 is directly connected, Outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.1.2, Outside
```

The ASA has static route injected to its routing table by EASYVPN Server. This route is there to reach remote client. When client is disconnected, the route is withdrawn from the routing table.

ASA1(config)# sh crypto ipsec sa detail

```
interface: Outside
  Crypto map tag: DYN-MAP, seq num: 5, local addr: 192.168.1.10

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.1.25.1/255.255.255.255/0/0)
  current_peer: 192.168.1.2, username: salesman
  dynamic allocated peer ip: 10.1.25.1

  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
  #pkts invalid pad (rcv): 0,
  #pkts invalid ip version (rcv): 0,
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

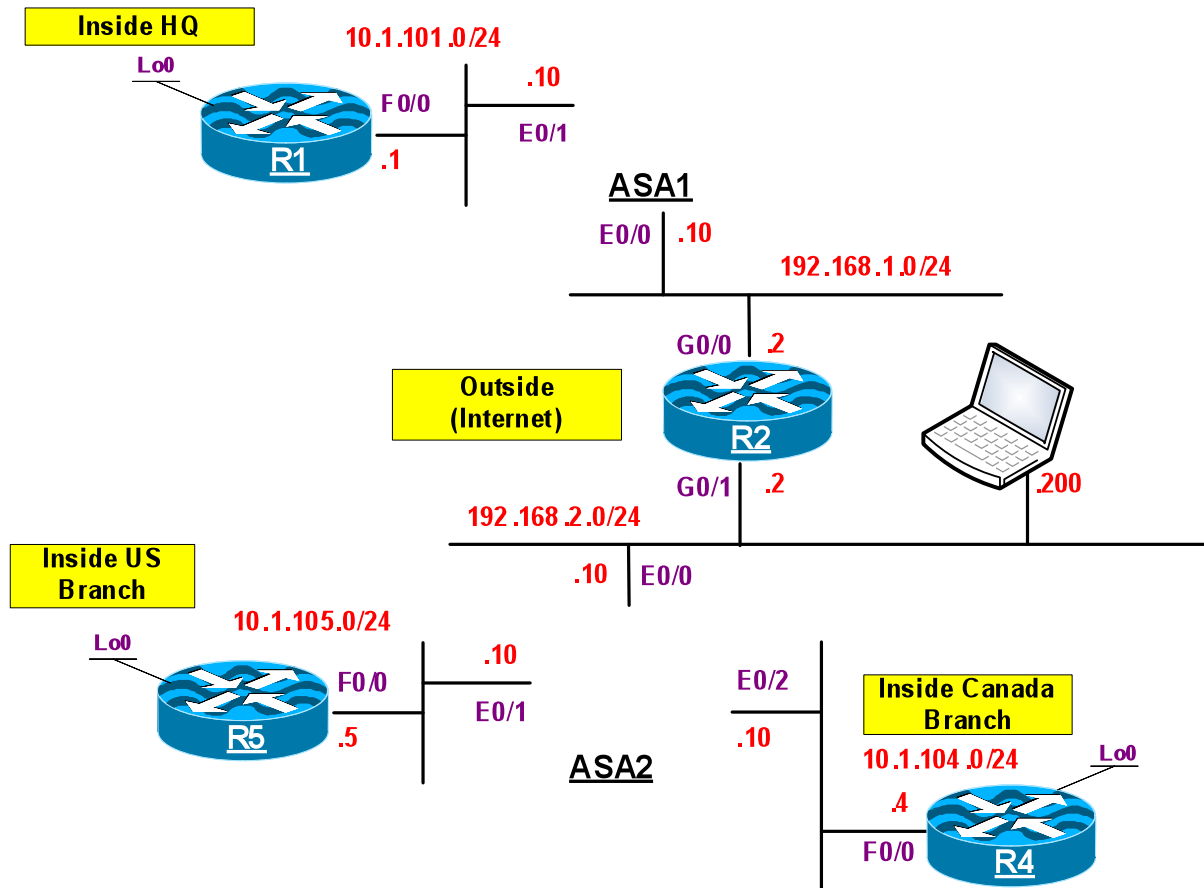
  local crypto endpt.: 192.168.1.10, remote crypto endpt.: 192.168.1.2

  path mtu 1500, ipsec overhead 58, media mtu 1500
  current outbound spi: B7ED79A2

inbound esp sas:
  spi: 0x0A422A55 (172108373)
    transform: esp-3des esp-sha-hmac no compression
    in use settings = {RA, Tunnel, }
    slot: 0, conn_id: 4096, crypto-map: DYN-MAP
    sa timing: remaining key lifetime (sec): 28644
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x0000003F
outbound esp sas:
  spi: 0xB7ED79A2 (3085793698)
    transform: esp-3des esp-sha-hmac no compression
```

```
in use settings ={RA, Tunnel, }  
slot: 0, conn_id: 4096, crypto-map: DYN-MAP  
sa timing: remaining key lifetime (sec): 28644  
IV size: 8 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001
```

Lab 1.61. Configuring RA VPN using Cisco VPN Client and ASA (PSK)



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure ASA1 as the EasyVPN Server. Place Test PC with Cisco VPN Client software into VLAN 122 and use it for remote access connections. Configure the following ISAKMP and IPSec Policies:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Group: 2
 - Encryption: 3DES
 - Hash : SHA
- IPSec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC
 - PFS Group 2

User named “remoteuser” with a password of ‘user123’ should be able to authenticate to the SALES group and get an IP address from the pool of 192.168.21.0/24.

The user should get the following additional attributes from the VPN Server:

WINS: 10.1.101.6

DNS: 10.1.101.5

Domain: micronicstraining.com

User’s traffic destined to an IP address of 1.1.1.1 should be encrypted; all other traffic should be sent out clear.



The most common EasyVPN deployment is with Cisco IPSec software client. This is typical remote access design where many clients accessing a headend and terminating IPSec tunnels to have access to corporate network.

Configuration

Complete these steps:

Step 1 Switchport configuration where Windows host is connected to.

```
SW3(config)#int f0/15
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 122
```

We’re placing WinXP client in VLAN 122.

Step 2 ASA1 configuration.

```
ASA1(config)# crypto isakmp enable outside
```

Remember, you must explicitly enable ISAKMP on the ASA to be able to terminate the IPSec tunnel.

```
ASA1(config)# crypto isakmp policy 10
ASA1(config-isakmp-policy)# auth pre-share
ASA1(config-isakmp-policy)# encr 3des
ASA1(config-isakmp-policy)# hash sha
ASA1(config-isakmp-policy)# group 2
ASA1(config-isakmp-policy)# exit
```

```
ASA1(config)# ip local pool VPN-CLIENTS 10.1.21.1-10.1.21.254 mask
```


255.255.255.0

```
ASA1(config)# access-list ST permit host 1.1.1.1
```

In the task, we are asked to tunnel traffic to 1.1.1.1 address only so that we need to configure Split Tunneling feature. We need to define that using standard ACL.

```
ASA1(config)# group-policy SALES-POLICY internal
ASA1(config)# group-policy SALES-POLICY attributes
ASA1(config-group-policy)# vpn-tunnel-protocol ipsec
ASA1(config-group-policy)# dns-server value 10.1.101.5
ASA1(config-group-policy)# wins-server value 10.1.101.6
ASA1(config-group-policy)# default-domain value
micronicstraining.com
ASA1(config-group-policy)# split-tunnel-policy tunnelspecified
ASA1(config-group-policy)# split-tunnel-network-list value ST
```

The Group Policy is a container for different attributes which will be shared between different tunnel groups or users. That policy usually specified all Phase 1.5 configuration attributes like DNS server, domain name and split tunneling. This Group Policy can be an "internal" or "external"; meaning can be configured on the ASA or on ACS. The Group Policy is then attached under a Tunnel Group or user profile.

The Split Tunneling ACL is used to specify Tunnel Network List. We must change Split Tunnel Policy to "tunnelspecified" to make it work.

```
ASA1(config-group-policy)# exit
```

```
ASA1(config)# tunnel-group SALES type remote-access
ASA1(config)# tunnel-group SALES ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key cisco123
ASA1(config-tunnel-ipsec)# exit
```

IPSec attributes are an authentication configuration in most cases. Here we use PSK.

```
ASA1(config)# tunnel-group SALES general-attributes
ASA1(config-tunnel-general)# default-group-policy SALES-POLICY
ASA1(config-tunnel-general)# address-pool VPN-CLIENTS
ASA1(config-tunnel-general)# exit
```

General attributes are used for client configuration. Here we can assign a new Group Policy which may be "shared" between different tunnel groups. This is the best way to configure that.

```
ASA1(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac
```

```

ASA1(config)# crypto dynamic-map DYN-CMAP 10 set pfs group2
ASA1(config)# crypto dynamic-map DYN-CMAP 10 set transform-set TSET

ASA1(config)# crypto map ENCRYPT_OUT 10 ipsec-isakmp dynamic DYN-
CMAP
ASA1(config)# crypto map ENCRYPT_OUT interface Outside

ASA1(config)# username remoteuser password user123
ASA1(config)# username remoteuser attributes
ASA1(config-username)# vpn-group-policy SALES-POLICY
ASA1(config-username)# exit

ASA1(config)# route inside 1.1.1.1 255.255.255.255 10.1.101.1

```

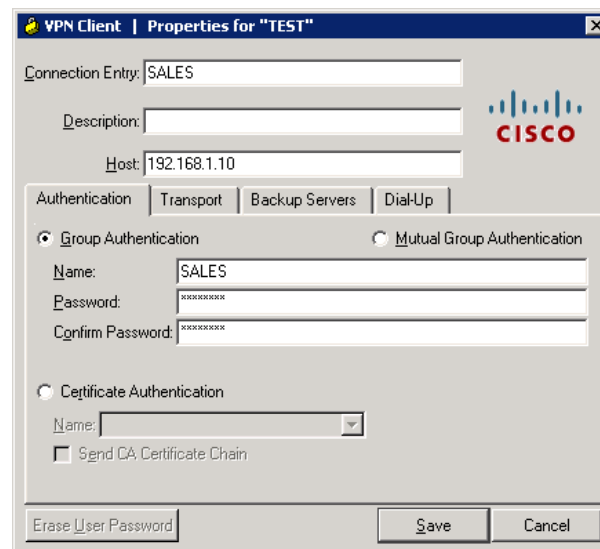
This static route is required for ASA to access 1.1.1.1 network.

Step 3 VPN Client configuration.

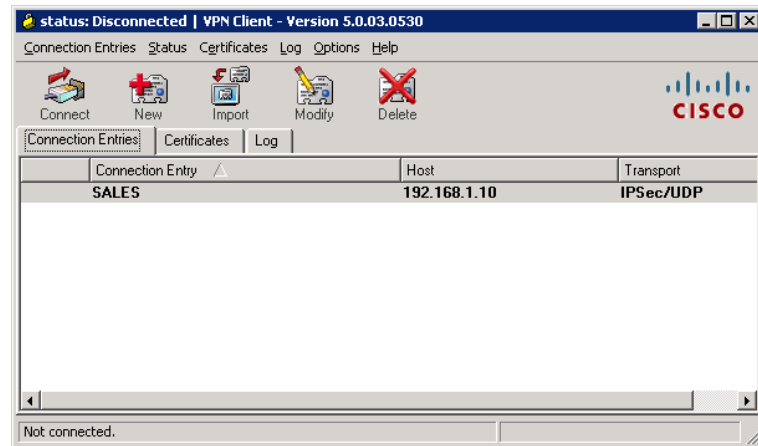
1. Assign IP address of 192.168.2.200/24 to Client workstation and add a static route

```
route add 192.168.1.0 mask 255.255.255.0 192.168.2.2
```

2. Configure Cisco VPN Client software

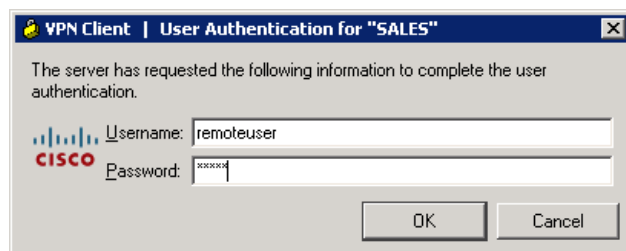


All we need is to specify an IP address for the EasyVPN Server, the Group Name (Tunnel Group name) and password.

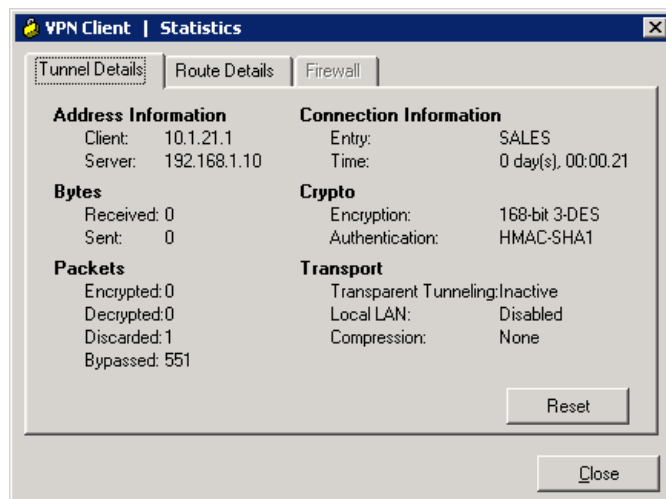


Verification

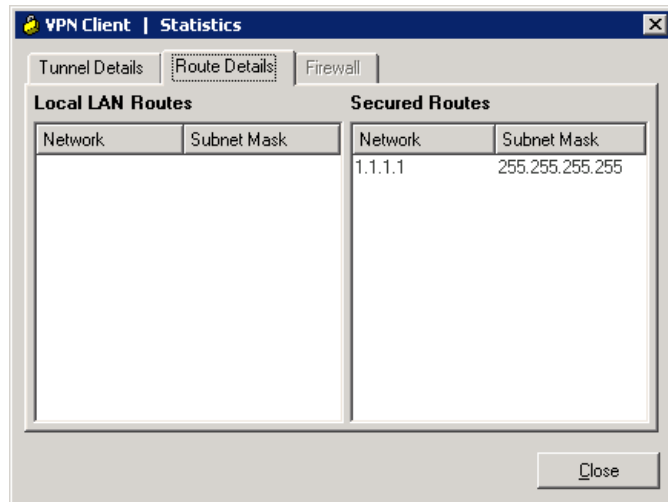
1. Verify on the client (connect to the VPN Server)



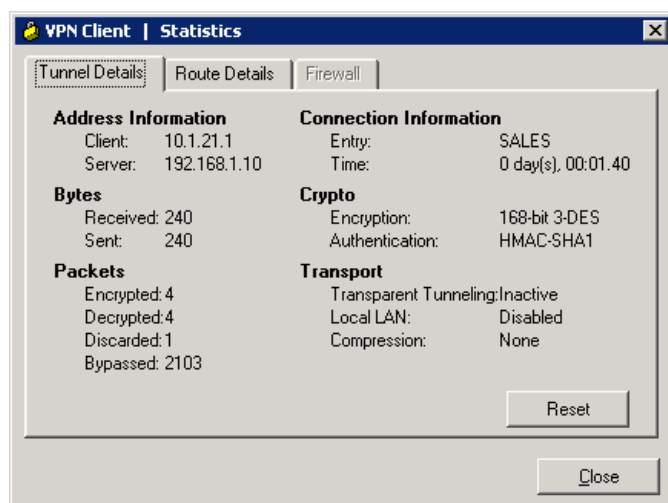
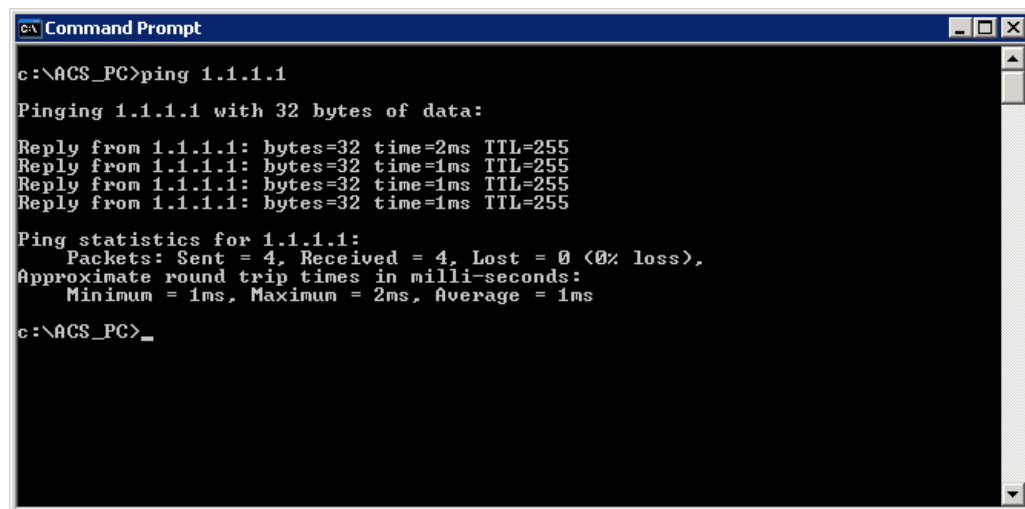
Here is our XAUTH phase. We need to authenticate with user's credentials.



After connection we see the Statistics and split tunneling. The IPSec client only secures 1.1.1.1/32 route.



We can test by pinging the 1.1.1.1 address.



See the encryption/decryption counters incremented.

2. Verify on ASA

ASA1(config)# sh crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1  IKE Peer: 192.168.2.200
    Type      : user          Role      : responder
    Rekey     : no           State     : AM ACTIVE
```

ASA1(config)# sh crypto ipsec sa

```
interface: Outside
```

```
Crypto map tag: DYN-CMAP, seq num: 10, local addr: 192.168.1.10
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.1.21.1/255.255.255.0/0/0)
current_peer: 192.168.2.200, username: remoteuser
dynamic allocated peer ip: 10.1.21.1
```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

On the ASA we see that it has terminated the tunnel (using Aggressive Mode) and received the traffic.

```
local crypto endpt.: 192.168.1.10, remote crypto endpt.: 192.168.2.200
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: FBB1C55E
```

```
inbound esp sas:
```

```
spi: 0x2A6A2E30 (711601712)
  transform: esp-3des esp-sha-hmac no compression
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 12288, crypto-map: DYN-CMAP
  sa timing: remaining key lifetime (sec): 28633
  IV size: 8 bytes
  replay detection support: Y
```

```
Anti replay bitmap:
```

```
0x00000000 0x0000001F
```

```
outbound esp sas:
```

```
spi: 0xFBB1C55E (4222731614)
  transform: esp-3des esp-sha-hmac no compression
  in use settings ={RA, Tunnel, }
```

```

slot: 0, conn_id: 12288, crypto-map: DYN-CMAP
sa timing: remaining key lifetime (sec): 28633
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

ASA1(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

```

S    1.1.1.1 255.255.255.255 [1/0] via 10.1.101.1, Inside
S    10.1.21.1 255.255.255.255 [1/0] via 192.168.1.2, Outside
C    10.1.101.0 255.255.255.0 is directly connected, Inside
C    192.168.1.0 255.255.255.0 is directly connected, Outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.1.2, Outside

```

There is a static route for the client injected into ASA's routing table.

ASA1(config)# sh vpn-sessiondb detail

Active Session Summary

Sessions:

	Active	Cumulative	Peak Concurrent	Inactive
SSL VPN	0	0		0
Clientless only	0	0		0
With client	0	0		0
Email Proxy	0	0		0
IPsec LAN-to-LAN	0	0		0
IPsec Remote Access	1	2		1
VPN Load Balancing	0	0		0
Totals	1	2		

License Information:

IPsec	250	Configured	250	Active	1	Load	0%
SSL VPN	100	Configured	100	Active	0	Load	0%

	Active	Cumulative	Peak Concurrent
IPsec	1	3	1
SSL VPN	0	0	0
AnyConnect Mobile	0	0	0
Linksys Phone	0	0	0

Totals : 1 : 3

Tunnels:

	Active	Cumulative	Peak	Concurrent
IKE :	1 :	2 :		1
IPsec :	1 :	2 :		1
Totals :	2 :	4		

Active NAC Sessions:

No NAC sessions to display

Active VLAN Mapping Sessions:

No VLAN Mapping sessions to display

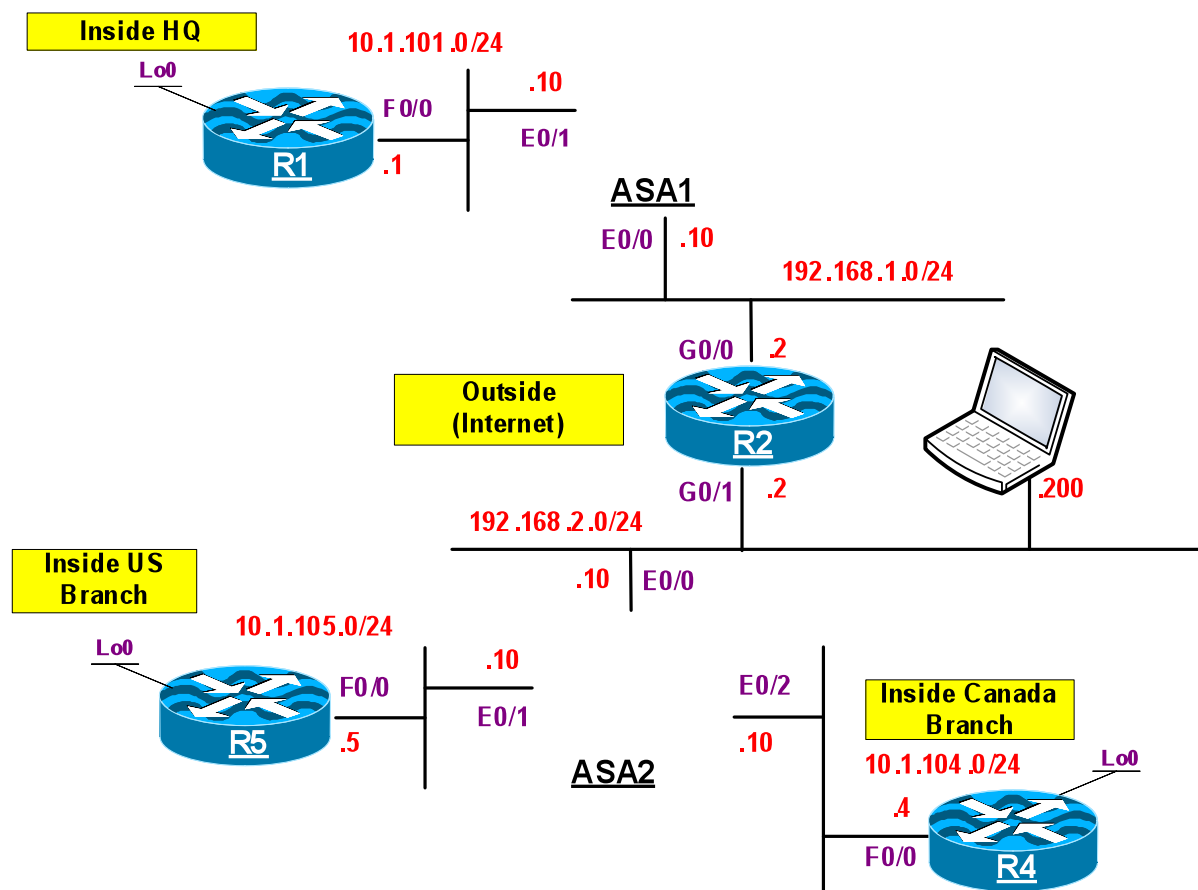
ASA1(config)# sh vpn-sessiondb remote

Session Type: IPsec

Username	: remoteuser	Index	: 3
Assigned IP	: 10.1.21.1	Public IP	: 192.168.2.200
Protocol	: IKE IPsec		
License	: IPsec		
Encryption	: 3DES	Hashing	: SHA1
Bytes Tx	: 240	Bytes Rx	: 240
Group Policy	: SALES-POLICY	Tunnel Group	: SALES
Login Time	: 22:47:22 UTC Mon Oct 26 2009		
Duration	: 0h:03m:45s		
NAC Result	: Unknown		
VLAN Mapping	: N/A	VLAN	: none

To see EasyVPN information you must use "show vpn-sessiondb remote" command. There is an information about Group Policy and Tunnel Group which have been used for that client.

Lab 1.62. Configuring RA VPN using Cisco VPN Client and ASA (PKI)



Lab Setup

- R1's F0/0 and ASA1's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA1's E0/0 interface should be configured in VLAN 102
- R2's G0/1 and ASA2's E0/0 interface should be configured in VLAN 122
- R4's F0/0 and ASA2's E0/2 interface should be configured in VLAN 104
- R5's F0/0 and ASA2's E0/1 interface should be configured in VLAN 105
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1, R4 and R5 pointing to the respective ASA's interface
- Configure default routing on both ASAs pointing to the respective R2 interface

IP Addressing

Device	Interface / ifname / sec level	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.101.1/24
R2	G0/0	192.168.1.2/24
	G0/1	192.168.2.2/24
R4	Lo0	4.4.4.4 /24
	F0/0	10.1.104.4 /24
R5	Lo0	5.5.5.5/24
	F0/0	10.1.105.5/24
ASA1	E0/0, Outside, Security 0	192.168.1.10 /24
	E0/1, Inside, Security 100	10.1.101.10 /24
ASA2	E0/0, Outside, Security 0	192.168.2.10 /24
	E0/1, Inside_US, Security 100	10.1.105.10 /24
	E0/2, Inside_CA, Security 100	10.1.104.10 /24

Task 1

Configure IOS Certificate Authority server on R1. The server should have self-signed certificate with a lifetime of 5 years and be able to grant certificates to the clients with a lifetime of 3 years. Store all certificates on the flash using PEM 64-base excryption with password of "Cisco_CA". The server should service all certificate requests automatically.



The EasyVPN remote access is very popular these days. However, using pre-shared key for authentication is not the best way to secure access to the company's network. Hence, in most cases we should use PKI and certificates for group authentication.

Using certificates is very flexible so that we can provide different network access and different security polices depending on some fields in the user's certificate.

Configuration

Complete these steps:

Step 1 R1 configuration.

Configuration of IOS CA has been described in section 2 already.

```
R1(config)#ip http server
R1(config)#crypto pki server IOS_CA
R1(cs-server)#lifetime certificate 1095
R1(cs-server)#lifetime ca-certificate 1825
R1(cs-server)#database archive pem password Cisco_CA
R1(cs-server)#database url pem flash:/IOS_CA
R1(cs-server)#grant auto
%PKI-6-CS_GRANT_AUTO: All enrollment requests will be
automatically granted.
R1(cs-server)#no shutdown
Certificate server 'no shut' event has been queued for
processing.
R1(cs-server)#
%Some server settings cannot be changed after CA
certificate generation.
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

%SSH-5-ENABLED: SSH 1.99 has been enabled
% Exporting Certificate Server signing certificate and
keys...

%PKI-6-CS_ENABLED: Certificate server now enabled.
R1(cs-server)#exit
```

Verification

R1#sh crypto pki server

Certificate Server IOS_CA:

Status: enabled

State: enabled

Server's configuration is locked (enter "shut" to unlock it)

Issuer name: CN=IOS_CA

CA cert fingerprint: 2CCFEC44 8B1FA216 4B9CA190 024184A0

Granting mode is: auto

Last certificate issued serial number: 0x1

CA certificate expiration timer: 21:37:39 UTC Oct 19 2014

```
CRL NextUpdate timer: 03:37:40 UTC Oct 21 2009
Current primary storage dir: nvram:
Current storage dir for .pem files: flash:/IOS_CA
Database Level: Minimum - no cert data written to storage
```

R1#sh flash | in IOS CA

```
22      1714 Oct 20 2009 21:37:42 +00:00 IOS_CA_00001.pem
```

Task 2

To ensure R1 and ASA1 have the same time configure NTP server on R1 with a stratum of 4. The server should authenticate the clients with a password of "Cisco_NTP".

Configure devices as NTP clients to the R1's NTP source.



Time is very important factor when using certificates. This is because a certificate has a lifetime and its validation is based on the time. Hence, we need to be sure the time is accurate on every device which has certificates (or request certificates).

The best option to synchronize the time in the network is to use NTP server on one of the routers and configure all other systems as a clients.

Configuration

Complete these steps:

Step 1 R1 NTP Server configuration.

```
R1(config)#ntp authentication-key 1 md5 Cisco_NTP
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate
R1(config)#ntp master 4
```

Step 2 ASA as NTP client.

```
ASA1(config)# ntp authentication-key 1 md5 Cisco_NTP
ASA1(config)# ntp authenticate
ASA1(config)# ntp trusted-key 1
ASA1(config)# ntp server 10.1.101.1 key 1
```

Verification

R1#sh ntp status

```
Clock is synchronized, stratum 4, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is CE9B2538.42900269 (21:55:04.260 UTC Tue Nov 3 2009)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
R1#sh ntp ass
R1#sh ntp associations
```

address	ref clock	st	when	poll	reach	delay	offset	disp
*~127.127.7.1	127.127.7.1	3	21	64	377	0.0	0.00	0.0

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

ASA1(config)# sh ntp status

```
Clock is synchronized, stratum 5, reference is 10.1.101.1
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is ce9b256c.dff18b1c (21:55:56.874 UTC Tue Nov 3 2009)
clock offset is -0.8338 msec, root delay is 0.98 msec
root dispersion is 15891.49 msec, peer dispersion is 15890.63 msec
ASA1(config)# sh ntp associations
```

address	ref clock	st	when	poll	reach	delay	offset	disp
*~10.1.101.1	127.127.7.1	4	15	64	1	1.0	-0.83	15890.

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

Task 3

On ASA1 enroll a certificate for IPsec peer authentication. Ensure that FQDN and certificate attributes like Common Name (ASA1) and Country (US) are used. Certificate uses for IPsec authentication should have at least 1024 bits keys.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA1(config)# domain-name MicronicsTraining.com
ASA1(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-
Key>.
```

```
Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
```

Every device must have a key pair generated before it can "ask" for signing. To generate keys we need to have hostname and domain name configured.

```
ASA1(config)# crypto ca trustpoint IOS_CA
ASA1(config-ca-trustpoint)# id-usage ssl-ipsec
ASA1(config-ca-trustpoint)# subject-name CN=ASA1, C=US
ASA1(config-ca-trustpoint)# fqdn ASA1.MicronicsTraining.com
ASA1(config-ca-trustpoint)# enrollment url http://10.1.101.1
ASA1(config-ca-trustpoint)# exit
```

A trustpoint is an object which is used for connection with a Certificate Authority (CA). It is used when a device wants its key to be signed or when a certificate must be validated.

After configuring a trustpoint we need to first get a certificate of the CA and then ask for signing device's key.

```
ASA1(config)# crypto ca authenticate IOS_CA

INFO: Certificate has the following attributes:
Fingerprint:      2ccfec44 8b1fa216 4b9ca190 024184a0
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

This is CA certificate which must be stored in device configuration to validate other certificates signed by this CA.

```
ASA1(config)# crypto ca enroll IOS_CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.
Password: *****
Re-enter password: *****

% The subject name in the certificate will be: CN=ASA1, C=US

% The fully-qualified domain name in the certificate will be:
ASA1.MicronicsTraining.com
```

```
% Include the device serial number in the subject name? [yes/no]:  
no
```

```
Request certificate from CA? [yes/no]: yes  
% Certificate request sent to Certificate Authority  
ASA1(config)# The certificate has been granted by CA!
```

Note that above information has been inherited from the trustpoint's configuration and the certificate has been granted to the ASA.

```
ASA1(config)# access-list OUTSIDE_IN permit tcp host 192.168.2.200  
host 10.1.101.1 eq 80  
ASA1(config)# access-group OUTSIDE_IN in interface Outside
```

The above ACL must be configured on the ASA to allow certificate enrollment by the client.

Verification

```
ASA1(config)# sh crypto ca trustpoints
```

```
Trustpoint IOS_CA:  
  Subject Name:  
    cn=IOS_CA  
      Serial Number: 01  
  Certificate configured.  
  CEP URL: http://10.1.101.1
```

```
ASA1(config)# sh crypto ca certificates
```

```
Certificate  
Status: Available  
Certificate Serial Number: 02  
Certificate Usage: General Purpose  
Public Key Type: RSA (1024 bits)  
Issuer Name:  
  cn=IOS_CA  
Subject Name:  
  hostname=ASA1.MicronicsTraining.com  
  cn=ASA1  
  c=US  
Validity Date:  
  start date: 22:14:31 UTC Oct 20 2009  
  end   date: 22:14:31 UTC Oct 19 2012  
Associated Trustpoints: IOS_CA
```

CA Certificate

```
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Public Key Type: RSA (1024 bits)
Issuer Name:
  cn=IOS_CA
Subject Name:
  cn=IOS_CA
Validity Date:
  start date: 21:37:39 UTC Oct 20 2009
  end   date: 21:37:39 UTC Oct 19 2014
Associated Trustpoints: IOS_CA
```

Both certificates are in ASA configuration. The first certificate is a device's certificate which is valid for 3 years. The ASA must have CA certificate as well to validate its certificate and any other certificates signed by this CA.

Task 3

Configure ASA1 as the EasyVPN Server. Place Test PC with Cisco VPN Client software into VLAN 122 and use it for remote access connections. Configure the following ISAKMP and IPsec Policies:

- ISAKMP Parameters
 - Authentication: Pre-shared
 - Group: 2
 - Encryption: 3DES
 - Hash : SHA
- IPsec Parameters
 - Encryption: ESP-3DES
 - Authentication: ESP-SHA-HMAC

User named “salesman” with a password of ‘sales123’ should be able to authenticate to the Sales group and get an IP address from the pool of 192.168.25.1 – 192.168.25.10.

User's traffic destined to the network 1.1.1.0/24 should be encrypted; all other traffic should be sent out clear.

Configuration

Complete these steps:

Step 1 Place Test PC in VLAN 122.

```
SW3(config)#int f0/15
SW3(config-if)#sw mo acc
SW3(config-if)#sw acc vl 122
```

Step 2 ASA1 configuration.

```
ASA1(config)# isakmp enable Outside
ASA1(config)# crypto isakmp policy 1 authentication rsa-sig
ASA1(config)# crypto isakmp policy 1 encryption 3des
ASA1(config)# crypto isakmp policy 1 hash sha
ASA1(config)# crypto isakmp policy 1 group 2
```

There is one change in the configuration comparing to the PSK authentication. Now we need to enable certificate's authentication (rsa-sig) in the ISAKMP policy.

```
ASA1(config)# tunnel-group SALES type remote-access

ASA1(config)# ip local pool VPN_POOL 10.1.25.1-10.1.25.10 mask
255.255.255.0

ASA1(config)# access-list ST standard permit 1.1.1.0 255.255.255.0
ASA1(config)# group-policy RA-POLICY internal
ASA1(config)# group-policy RA-POLICY attributes
ASA1(config-group-policy)# split-tunnel-policy tunnelspecified
ASA1(config-group-policy)# split-tunnel-network-list value ST

ASA1(config)# tunnel-group Sales general-attributes
ASA1(config-tunnel-general)# address-pool VPN_POOL
ASA1(config-tunnel-general)# default-group-policy RA-POLICY
ASA1(config-tunnel-general)# exit

ASA1(config)# tunnel-group Sales ipsec-attributes
ASA1(config-tunnel-ipsec)# trust-point IOS_CA
ASA1(config-tunnel-ipsec)# exit
```

In order to validate client's certificate we need to specify the trustpoint used to do that.

```
ASA1(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac
ASA1(config)# crypto dynamic-map DYN-MAP 5 set transform-set TSET
ASA1(config)# crypto map ENCRYPT_OUT 1 ipsec-isakmp dynamic DYN-MAP
ASA1(config)# crypto map ENCRYPT_OUT interface Outside

ASA1(config)# username salesman password sales123 privilege 0

ASA1(config)# route inside 1.1.1.1 255.255.255.255 10.1.101.1
```


Verification

On VPN Client

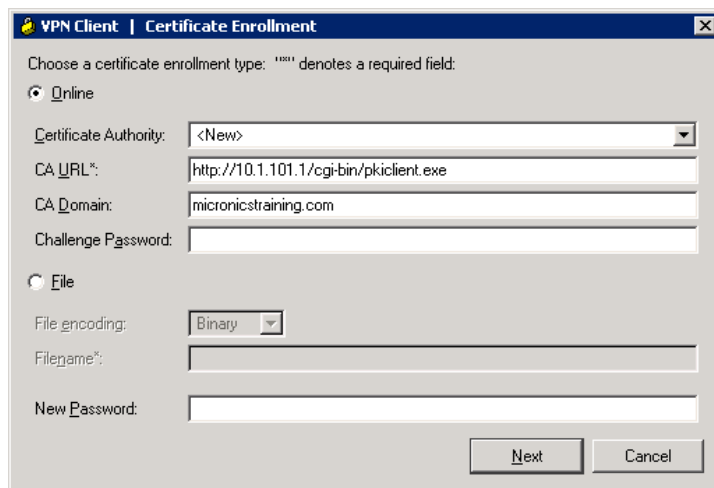
1. Assign IP address of 192.168.2.200/24 to Client workstation and add a static routes

```
route add 192.168.1.0 mask 255.255.255.0 192.168.2.2
route add 10.1.101.1 mask 255.255.255.255 192.168.2.2
```

2. Request a certificate from R1. Click on Certificates tab and then on Enroll button.

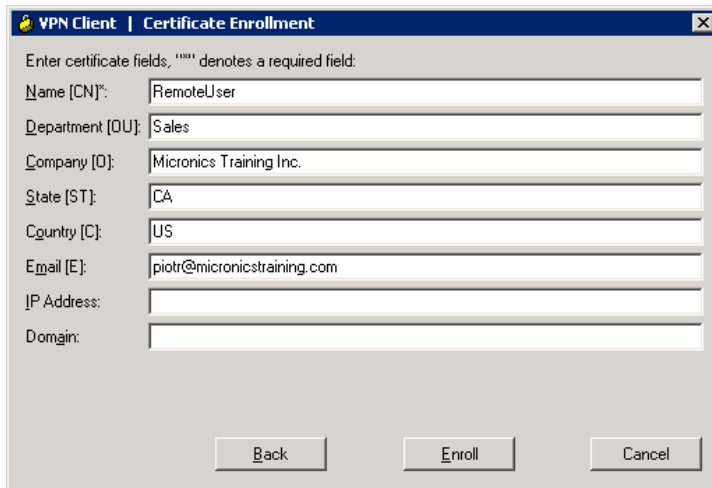
Requesting a new certificate for EasyVPN Client requires providing some information which will be used to generate keys and signing request on the client.

The client uses SCEP (Simple Certificate Enrollment Protocol) for certificate enrollment. In case of IOS CA the SCEP URL is the following: <http://<IOS-CA-IP-ADDR>/cgi-bin/pkiclient.exe>



Click Next

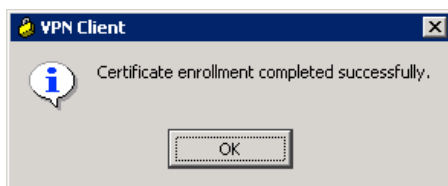
Ensure you provide as much information as you can as that information can be useful for client recognition on the secure gateway. The Name (CN - Common Name) and Department (OU - Organizational Unit) are required. The ASA will land the connection in the Tunnel Group of the same name as OU in the certificate (it is case sensitive)!



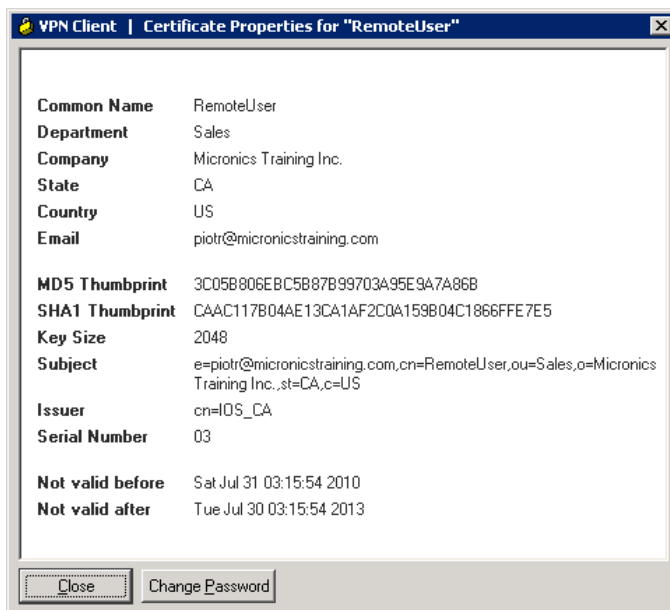
Enter certificate fields, "*" denotes a required field:

Name [CN]:	RemoteUser
Department [OU]:	Sales
Company [O]:	Micronics Training Inc.
State [ST]:	CA
Country [C]:	US
Email [E]:	piotr@micronicstraining.com
IP Address:	
Domain:	

Back Enroll Cancel



Click on the certificate to see its details:

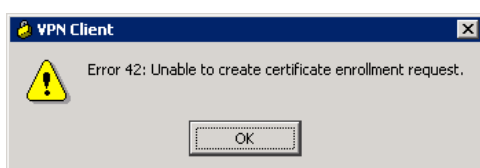


VPN Client | Certificate Properties for "RemoteUser"

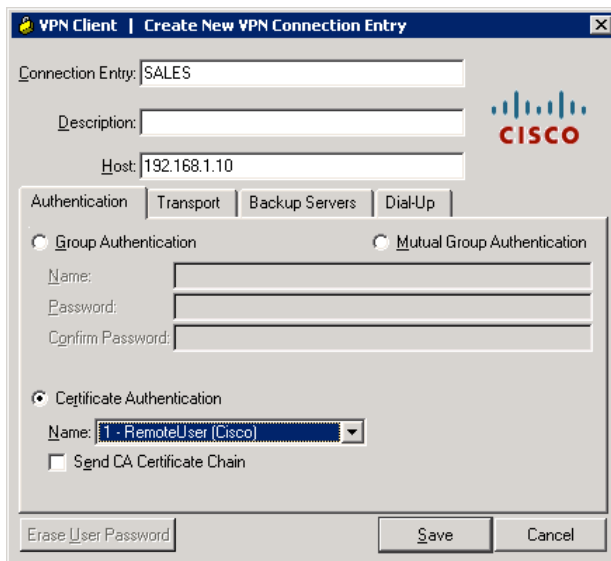
Common Name	RemoteUser
Department	Sales
Company	Micronics Training Inc.
State	CA
Country	US
Email	piotr@micronicstraining.com
MD5 Thumbprint	3C05B806EBC5B87B99703A95E9A7A86B
SHA1 Thumbprint	CAAC117B04AE13CA1AF2C0A159B04C1866FFE7E5
Key Size	2048
Subject	e=piotr@micronicstraining.com,cn=RemoteUser,ou=Sales,o=Micronics Training Inc.,st=CA,c=US
Issuer	cn=IOS_CA
Serial Number	03
Not valid before	Sat Jul 31 03:15:54 2010
Not valid after	Tue Jul 30 03:15:54 2013

Close Change Password

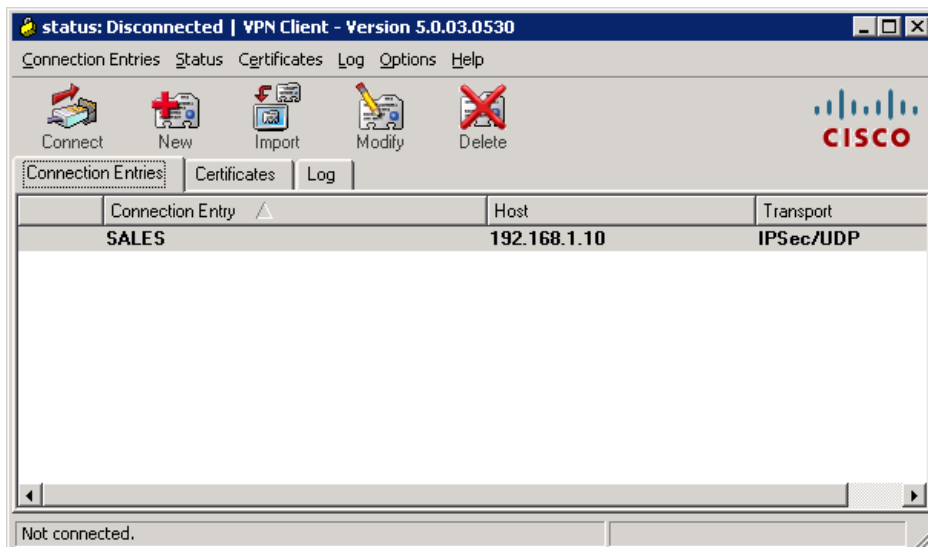
If you see the following error, make sure you have time synchronized between R1 and Client's workstation. Then try again.



3. Configure Cisco VPN Client software. Make sure you choose Certificate Authentication.



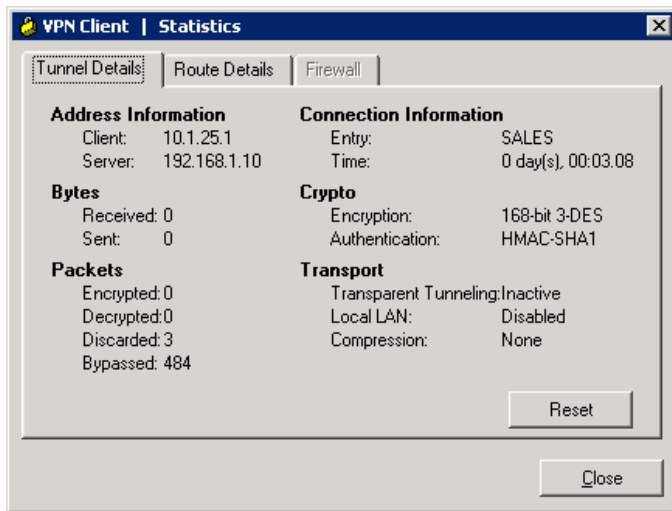
We must create a new connection in the VPN client. The connection should have IP address of the ASA and certificate for authentication specified.



4. Connect to the VPN Server and authenticate the user.



Note that in case of certificate authentication we still have XAUTH enabled. This means we'll be asked for user credentials to set up the tunnel. There is no way to authenticate the user using a certificate.



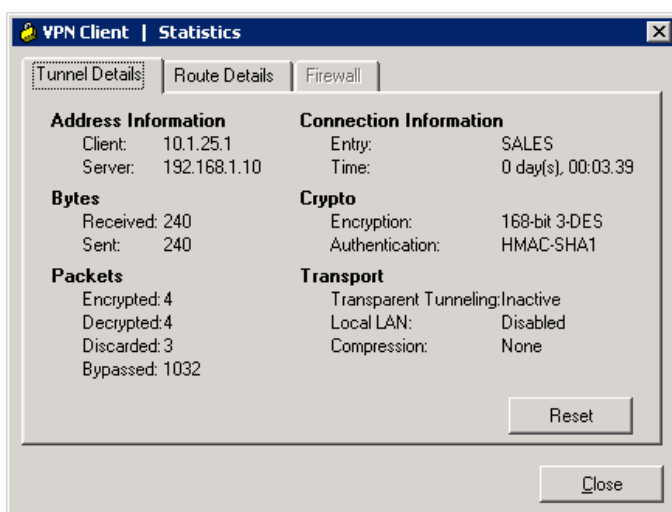
C:\>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:

```
Reply from 1.1.1.1: bytes=32 time=19ms TTL=255
Reply from 1.1.1.1: bytes=32 time=2ms TTL=255
Reply from 1.1.1.1: bytes=32 time=1ms TTL=255
Reply from 1.1.1.1: bytes=32 time=1ms TTL=255
```

Ping statistics for 1.1.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 19ms, Average = 5ms



Traffic to the address of 1.1.1.1 is getting encrypted/decrypted. Note that Bypassed counted is incrementing meaning there are some packets not encrypted - this is because of Split Tunneling used.

On ASA

ASA1(config)# sh crypto isakmp sa detail

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.2.200
    Type    : user                Role    : responder
    Rekey    : no                  State    : MM ACTIVE
    Encrypt  : 3des                 Hash     : SHA
    Auth     : rsa                  Lifetime: 86400
    Lifetime Remaining: 86120
```

Note the very important information. When certificate authentication is used the ISAKMP is using Main Mode instead of Aggressive Mode.

ASA1(config)# sh crypto ipsec sa

```
interface: Outside
Crypto map tag: DYN-MAP, seq num: 5, local addr: 192.168.1.10

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.1.25.1/255.255.255.255/0/0)
current_peer: 192.168.2.200, username: salesman
dynamic allocated peer ip: 10.1.25.1

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

Packets are getting encrypted/decrypted on the ASA.

local crypto endpt.: 192.168.1.10, remote crypto endpt.: 192.168.2.200

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: F0F7B35C

inbound esp sas:
spi: 0x1091008C (277938316)
transform: esp-3des esp-sha-hmac no compression
```

```

in use settings ={RA, Tunnel, }
slot: 0, conn_id: 16384, crypto-map: DYN-MAP
sa timing: remaining key lifetime (sec): 28500
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x0000001F
outbound esp sas:
spi: 0xF0F7B35C (4042765148)
transform: esp-3des esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 16384, crypto-map: DYN-MAP
sa timing: remaining key lifetime (sec): 28500
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x00000001

```

ASA1(config)# sh vpn-sessiondb remote

Session Type: IPsec

Username	: salesman	Index	: 4
Assigned IP	: 10.1.25.1	Public IP	: 192.168.2.200
Protocol	: IKE IPsec		
License	: IPsec		
Encryption	: 3DES	Hashing	: SHA1
Bytes Tx	: 240	Bytes Rx	: 240
Group Policy	: RA-POLICY	Tunnel Group	: Sales
Login Time	: 07:42:50 UTC Sat Jul 31 2010		
Duration	: 0h:05m:49s		
NAC Result	: Unknown		
VLAN Mapping	: N/A	VLAN	: none

Note that tunnel group of "Sales" has been chosen. This is because the client's certificate has OU=Sales.

ASA1(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

```
S    1.1.1.1 255.255.255.255 [1/0] via 10.1.101.1, Inside
```

```
S    10.1.25.1 255.255.255.255 [1/0] via 192.168.1.2, Outside
C    10.1.101.0 255.255.255.0 is directly connected, Inside
C    192.168.1.0 255.255.255.0 is directly connected, Outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.1.2, Outside
```

The static route to the client's IP address is injected into the ASA's routing table.

Verification (detailed)

ASA1(config)# deb cry isak 50

```
ASA1(config)#
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 1144
```

The ASA has received first ISAKMP packet containing ISAKMP policies from the client.

```
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing SA payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Oakley proposal is acceptable
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Received xauth V6 VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Received DPD VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Received Fragmentation VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: False
```

The mode is the Main Mode.

```
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Received NAT-Traversal ver 02 VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Received Cisco Unity client VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing IKE SA payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, IKE SA Proposal # 1, Transform # 21
acceptable Matches global IKE entry # 1
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing ISAKMP SA payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing NAT-Traversal VID ver
02 payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing Fragmentation VID +
extended capabilities payload
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 128
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 272
```

The ASA sent a message with accepted proposal and received a packet with keying material from the client.

```
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing ke payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing ISA_KE payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing nonce payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing NAT-Discovery payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, computing NAT Discovery hash
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing NAT-Discovery payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, computing NAT Discovery hash
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Processing IOS/PIX Vendor ID payload
(version: 1.0.0, capabilities: 00000408)
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Received Cisco Unity client VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing ke payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing nonce payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing certreq payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing Cisco Unity VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing xauth V6 VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Send IOS VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Constructing ASA spoofing IOS Vendor
ID payload (version: 1.0.0, capabilities: 20000001)
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing VID payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Send Altiga/Cisco VPN3000/Cisco ASA
GW VID
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing NAT-Discovery payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, computing NAT Discovery hash
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, constructing NAT-Discovery payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, computing NAT Discovery hash
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Generating keys for Responder...
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 328
```

The ASA sent a message to the client with its keying material.

```
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Rcv'd fragment from a new
fragmentation set. Deleting any old fragments.
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Successfully assembled an encrypted
pkt from rcv'd fragments!
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + ID (5) + CERT (6) + CERT_REQ (7) + SIG (9) + NOTIFY (11) + NONE (0)
total length : 1272
```

The ASA received a message with Identification information from the client.
Note the size of the message (1272 bytes) - it's huge comparing to the other messages. This is because this message contains peer's certificate which will be used for authentication.

```
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing ID payload
```



```
Jul 31 07:42:50 [IKEv1 DECODE]: IP = 192.168.2.200, DER_ASN1_DN ID received, len 144
0000: 30818D31 0B300906 03550406 13025553      0..1.0...U....US
0010: 310B3009 06035504 08130243 41312030      1.0...U....CA1 0
0020: 1E060355 040A1317 4D696372 6F6E6963      ...U....Micronic
0030: 73205472 61696E69 6E672049 6E632E31      s Training Inc.1
0040: 0E300C06 0355040B 13055361 6C657331      .0...U....Sales1
0050: 13301106 03550403 130A5265 6D6F7465      .0...U....Remote
0060: 55736572 312A3028 06092A86 4886F70D      User1*0(..*.H...
0070: 01090116 1B70696F 7472406D 6963726F      .....piotr@micro
0080: 6E696373 74726169 6E696E67 2E636F6D      nicstraining.com
```

```
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing cert payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing cert request payload
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing RSA signature
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, Computing hash for ISAKMP
Jul 31 07:42:50 [IKEv1 DECODE]: Dump of received Signature, len 256:
0000: 3A4A4EAF FD057478 46460649 6B20C527      :JN...txFF.Ik .'
0010: AAFBE23F 918B3102 8C04E6FB 3305F07C      ...?...1.....3..|
0020: 4EEF228C CB679323 7BFC3B43 A5557004      N"...g.#{.;C.Up.
0030: 22CA29CD 19740247 29530E69 AD09EDF7      ".)...t.G)S.i....
0040: D3A528C5 06729150 375221B7 04512A63      ..(..r.P7R!..Q*c
0050: 04ACCD4C 4119885E A0578794 B07DFBAF      ...LA..^..W...)..
0060: 8272474D A1528EE5 5A0D2CA8 39837FCB      .rGM.R..Z.,.9...
0070: EDBEC28B 47F91C39 72062D74 C4CAB28B      ....G..9r.-t....
0080: DC161756 85BE54B6 1D5FF896 22E740A9      ...V..T...".@.
0090: 3992DAE8 F43682A3 BFE85FAC 6B92B71E      9....6....._k...
00A0: 446A6D62 C64794FD FD57A36A 4BC79319      Djmb.G...W.jK...
00B0: 9EE2B9A5 7CFA1B12 B136E228 C6B19D14      ....|....6.(....
00C0: 337ED613 22DD8187      3~..."...
```

```
Jul 31 07:42:50 [IKEv1 DEBUG]: IP = 192.168.2.200, processing notify payload
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, Automatic NAT Detection Status:      Remote
end is NOT behind a NAT device      This      end is NOT behind a NAT device
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, Trying to find group via OU...
Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, Connection landed on tunnel_group Sales
```

The tunnel group has been chosen based on OU in the certificate. This is a default behavior.

```
Jul 31 07:42:50 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, peer ID type 9
received (DER_ASN1_DN)
Jul 31 07:42:50 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, constructing ID
payload
Jul 31 07:42:50 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, constructing cert
payload
Jul 31 07:42:50 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, constructing RSA
signature
Jul 31 07:42:50 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, Computing hash for
ISAKMP
```

```

Jul 31 07:42:50 [IKEv1 DECODE]: Constructed Signature Len: 128
Jul 31 07:42:50 [IKEv1 DECODE]: Constructed Signature:
0000: 38033BC3 BAD78D0A 2193953C BB41722C      8.;.....!...<.Ar,
0010: 04AE90D2 DA211A5C A1208678 ADA7218B      .....!\. .x...!.
0020: 44348C24 C301D12C B8B52560 CA3A87C8      D4.$...,%`.:...
0030: 44C21CB2 D5D67163 AE1B91CB C1C1F3C7      D.....qc.....
0040: 50342BD9 EB89E012 87DE0405 AE3E7B34      P4+.....>{4
0050: E66F31E9 31EA0087 25772895 AB85ACA7      .o1.1...%w(.....
0060: 12F388C6 29E8D02C 2B574B37 DCD8C80C      ....)..,WK7....
0070: DA1F09B2 2BB3F891 F0F4856A 57CEE4C8      ....+.....jW...

```

Jul 31 07:42:50 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, constructing dpd vid payload

```

Jul 31 07:42:50 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0) total length :
853

```

Jul 31 07:42:51 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, constructing blank hash payload

The ASA sent a final message (#6) to the client containing its certificate.

Jul 31 07:42:51 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, constructing qm hash payload

```

Jul 31 07:42:51 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message
(msgid=5a278fca) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
72

```

```

Jul 31 07:42:56 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message
(msgid=5a278fca) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
88

```

The ASA starts Phase 1.5 - Configuration Mode. The ASA sends out first packet asking for user's credentials. The client replies with "salesman" username as showed below.

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, process_attr(): Enter!

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, IP = 192.168.2.200, Processing MODE_CFG Reply attributes.

```

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: primary DNS = cleared

```

```

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: secondary DNS = cleared

```

```

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: primary WINS = cleared

```

```

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: secondary WINS = cleared

```

```

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: split tunneling list = ST

```

```

Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: IP Compression = disabled

```

```
Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: Split Tunneling Policy = Split Network
Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKEGetUserAttributes: Browser Proxy Bypass Local = disable
```

The client sent a bunch of attributes it wants to get from the server. The server prepares a reply message with all attributes it has configured for that group/user.

```
Jul 31 07:42:56 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, User
(salesman) authenticated.
```

User has been authenticated by the server.

```
Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing blank hash payload
Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing qm hash payload
Jul 31 07:42:56 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message
(msgid=51d17a8e) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
64
Jul 31 07:42:56 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message
(msgid=51d17a8e) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
60
Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
process_attr(): Enter!
Jul 31 07:42:56 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Processing cfg ACK attributes
Jul 31 07:42:57 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message
(msgid=ee87f4da) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
188
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
process_attr(): Enter!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Processing cfg Request attributes
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for IPV4 address!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for IPV4 net mask!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for DNS server address!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for WINS server address!
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Received unsupported transaction mode attribute: 5
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Banner!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Save PW setting!
```

```
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Default Domain Name!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Split Tunnel List!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Split DNS!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for PFS setting!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Client Browser Proxy Setting!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for backup ip-sec peer list!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Client Smartcard Removal Disconnect Setting!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for Application Version!
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, Client
Type: WinNT Client Application Version: 5.0.04.0300
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for FWTYPE!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for DHCP hostname for DDNS is: XP!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
MODE_CFG: Received request for UDP Port!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Obtained IP addr (10.1.25.1) prior to initiating Mode Cfg (XAuth enabled)
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Sending subnet mask (255.255.255.0) to remote client
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Assigned private IP address 10.1.25.1 to remote user
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing blank hash payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Send Client Browser Proxy Attributes!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Browser Proxy set to No-Modify. Browser Proxy data will NOT be included in the mode-cfg
reply
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Send Cisco Smartcard Removal Disconnect enable!!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing qm hash payload
Jul 31 07:42:57 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message
(msgid=ee87f4da) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
192
Jul 31 07:42:57 [IKEv1 DECODE]: IP = 192.168.2.200, IKE Responder starting QM: msg id =
812a9a29
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
```

```

Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, PHASE
1 COMPLETED
Jul 31 07:42:57 [IKEv1]: IP = 192.168.2.200, Keep-alive type for this connection: DPD
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Starting P1 rekey timer: 82080 seconds.
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
sending notify message
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing blank hash payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing qm hash payload
Jul 31 07:42:57 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message
(msgid=5cdcd9de) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length :
92
Jul 31 07:42:57 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message
(msgid=812a9a29) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5)
+ NONE (0) total length : 1026

```

Here's IKE Phase 2 (Quick mode) started. The goal here is to negotiate IPSec policy and Proxy IDs.

```

Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
processing hash payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
processing SA payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
processing nonce payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
processing ID payload
Jul 31 07:42:57 [IKEv1 DECODE]: Group = Sales, Username = salesman, IP = 192.168.2.200,
ID_IPV4_ADDR ID received
10.1.25.1
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Received remote Proxy Host data in ID Payload: Address 10.1.25.1, Protocol 0, Port 0
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
processing ID payload
Jul 31 07:42:57 [IKEv1 DECODE]: Group = Sales, Username = salesman, IP = 192.168.2.200,
ID_IPV4_ADDR_SUBNET ID received--0.0.0.0--0.0.0.0
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0,
Protocol 0, Port 0
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, QM
IsRekeyed old sa not found by addr
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, IKE
Remote Peer configured for crypto map: DYN-MAP
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
processing IPSec SA payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IPSec SA Proposal # 12, Transform # 1 acceptable Matches global IPSec SA entry # 5

```

IPSec policy has been agreed.

```
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, IKE:
requesting SPI!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKE got SPI from key engine: SPI = 0x1091008c
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
oakley constructing quick mode
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing blank hash payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing IPsec SA payload
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing IPsec nonce payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing proxy ID
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Transmitting Proxy ID:
  Remote host: 10.1.25.1 Protocol 0 Port 0
  Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Sending RESPONDER LIFETIME notification to Initiator
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
constructing qm hash payload
Jul 31 07:42:57 [IKEv1 DECODE]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKE Responder sending 2nd QM pkt: msg id = 812a9a29
Jul 31 07:42:57 [IKEv1]: IP = 192.168.2.200, IKE_DECODE SENDING Message
(msgid=812a9a29) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5)
+ NOTIFY (11) + NONE (0) total length : 180
Jul 31 07:42:57 [IKEv1]: IP = 192.168.2.200, IKE_DECODE RECEIVED Message
(msgid=812a9a29) with payloads : HDR + HASH (8) + NONE (0) total length : 52
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
processing hash payload
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
loading all IPSEC SAs
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Generating Quick Mode Key!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
NP encrypt rule look up for crypto map DYN-MAP 5 matching ACL Unknown: returned
cs_id=d78ee498; rule=00000000
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Generating Quick Mode Key!
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
NP encrypt rule look up for crypto map DYN-MAP 5 matching ACL Unknown: returned
cs_id=d78ee498; rule=00000000
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Security negotiation complete for User (salesman) Responder, Inbound SPI = 0x1091008c,
Outbound SPI = 0xf0f7b35c
```

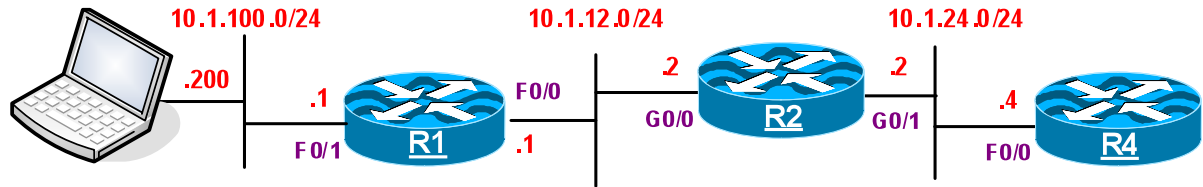
IPsec negotiation is complete.

```
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
IKE got a KEY_ADD msg for SA: SPI = 0xf0f7b35c
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Pitcher: received KEY_UPDATE, spi 0x1091008c
Jul 31 07:42:57 [IKEv1 DEBUG]: Group = Sales, Username = salesman, IP = 192.168.2.200,
Starting P2 rekey timer: 27360 seconds.
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, Adding
static route for client address: 10.1.25.1
Jul 31 07:42:57 [IKEv1]: Group = Sales, Username = salesman, IP = 192.168.2.200, PHASE
2 COMPLETED (msgid=812a9a29)
```

```
ASA1(config)# un all
```

```
ASA1(config)#
```

Lab 1.63. Configuring SSL VPN (IOS)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's G0/1 and R4's F0/0 interface should be configured in VLAN 24
- R1's F0/1 and VPN Client PC (SW3 – F0/15) should be in VLAN 100
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1 and R4 pointing to the R2

IP Addressing

Device	Interface	IP address
R1	F0/0	10.1.12.1/24
R2	G0/0	10.1.12.2/24
	G0/1	10.1.24.2/24
R4	F0/0	10.1.24.4/24
PC	NIC	10.1.100.200/24

Task 1

Configure Clientless SSL VPN on R2 so that it allows users accessing R4's HTTP server after successful authentication using local user database located on R2. The user named "student1" with a password of "student123" should see an URL named "R4-Config" located under "Device Configuration" section.

Use self signed SSL certificate for server's authentication and data security with the following parameters:

- Organization: micronicstrainig.com
- State: CA

- Country: US
- No IP address and serial number included
- RSA Keys name: MY-KEYS
- RSA Keys length: 1024 bits

R2 should accept HTTP connections on its G0/0 interface and redirect them to SSL default port.

User connected to the WebVPN shouldn't be able to enter custom URLs and see "real" URLs when connecting to R4. Maximum of 10 users should be able to use this connection method at one time.

You may need to enable HTTP server on R4 and configure local administrator account (admin/admin123) to verify this task.



SSL VPN is a basic service which can be enabled on the IOS router to make your corporate resources be accessible for remote users without using any sophisticated client software. All the client need is a web browser (Internet Explorer, Firefox, etc.). The user connects to the IP address of your IOS router and authenticates on the website presented to him. This authentication can be against local user database configured on the router itself or against remote database (via ACS or LDAP server). After successful authentication, the user has access to the portal where he/she can see some links to corporate resources. Those resources can be for example: files on remote server, other services available through the web browser (like web accessible management software or application). The user can also surf the Internet via this gateway. The SSL VPN is an access method uses SSL certificates for authentication and security mechanisms built into SSL. It leverages the same mechanism like we use for web surfing and thus it is called Clientless Mode.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#aaa new-model
R2(config)#aaa authentication login AUTH-LOCAL local
```

We are asked for SSL VPN user authentication via local user database, so that we need to enable AAA and tell the router it should look for users in its local database.

```
R2(config)#ip http server
R2(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

SSL VPN must have HTTPS server enabled on the router. Once we enable it, the router generates self signed SSL certificate. This will also create a trustpoint in the routers configuration.

```
R2(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#
%PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write
memory" to save new certificate

R2(config)#crypto ca trustpoint SELF-CA
R2(ca-trustpoint)# rsakeypair MY-KEYS 1024
R2(ca-trustpoint)# subject-name O=MicronicsTrainnig.com, ST=CA,
C=US
R2(ca-trustpoint)# ip-address none
R2(ca-trustpoint)# enrollment selfsigned
R2(ca-trustpoint)# serial-number none
R2(ca-trustpoint)# exit
```

However, for SSL VPN we need to have our custom trustpoint to generate self signed certificate and use it for securing sessions. We were requested to configure named keys and use special fields in the certificate.

```
R2(config)#crypto ca enroll SELF-CA
The router has already generated a Self Signed Certificate for
trustpoint TP-self-signed-2253035440.
If you continue the existing trustpoint and Self Signed Certificate
will be deleted.

Do you want to continue generating a new Self Signed Certificate?
[yes/no]: yes
Generate Self Signed Router Certificate? [yes/no]: yes
%CRYPTO-6-AUTOGEN: Generated new 1024 bit key pair
```

Router Self Signed Certificate successfully created

We need to request self signed certificate from our local trustpoint. To do that we use the same command as for enrolling from remote CA server.

Note that there is already created trustpoint which has generated a self signed certificate. This trustpoint should be overwritten by our custom trustpoint.

```
R2(config)#webvpn gateway SSL-GATEWAY
```

```
R2(config-webvpn-gateway)# ip address 10.1.12.2 port 443
R2(config-webvpn-gateway)# http-redirect port 80
R2(config-webvpn-gateway)# ssl trustpoint SELF-CA
R2(config-webvpn-gateway)# inservice
R2(config-webvpn-gateway)# exit
```

The SSL VPN solution has two parts of the configuration. One is a gateway and another is a context. The gateway specifies general network properties like IP address and port of the server, associated trustpoint for certificate use and port redirection feature.

```
R2(config)#webvpn context SSL-CONTEXT
R2(config-webvpn-context)# aaa authentication list AUTH-LOCAL
R2(config-webvpn-context)# gateway SSL-GATEWAY
R2(config-webvpn-context)# max-users 10
R2(config-webvpn-context)# url-list Device-Configuration
R2(config-webvpn-url)# heading "Device Configuration"
R2(config-webvpn-url)# url-text R4-Config url-value
http://10.1.24.4
R2(config-webvpn-url)# exit
```

A context specifies a "portal" view for users connecting to the device. The user establishes SSL VPN to the router and sees a website prepared by the administrator and used for connections to the corporate network. The context must have an associated gateway and a policy. Policy describes what a user may see on the portal.

```
R2(config-webvpn-context)# policy group SSL-POLICY
R2(config-webvpn-group)# mask-urls
R2(config-webvpn-group)# hide-url-bar
R2(config-webvpn-group)# url-list Device-Configuration
R2(config-webvpn-group)# exit

R2(config-webvpn-context)# default-group-policy SSL-POLICY
R2(config-webvpn-context)# inservice
R2(config-webvpn-context)# exit
```

The SSL VPN context and gateway must be enabled using "inservice" command. Do not forget that!

```
R2(config)#username student1 password student123

R2(config)#ip route 10.1.100.0 255.255.255.0 10.1.12.1
```

Step 2 R4 configuration.

```
R4(config)#ip http server
```

```
R4(config)#ip http authentication local
```

```
R4(config)#username admin privilege 15 password admin123
```

To be able to verify our task we need to enable HTTP server on R4 and use local database authentication.

Verification:

On PC connect to R2 using SSL enabled web browser.

1. Check if you have connectivity. If no default route is used, configure static route.

Ethernet adapter Rack:

```
Connection-specific DNS Suffix  . :  
IP Address. . . . . : 10.1.100.200  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

```
c:\>route add 10.1.12.0 mask 255.255.255.0 10.1.100.1
```

```
c:\>ping 10.1.100.1
```

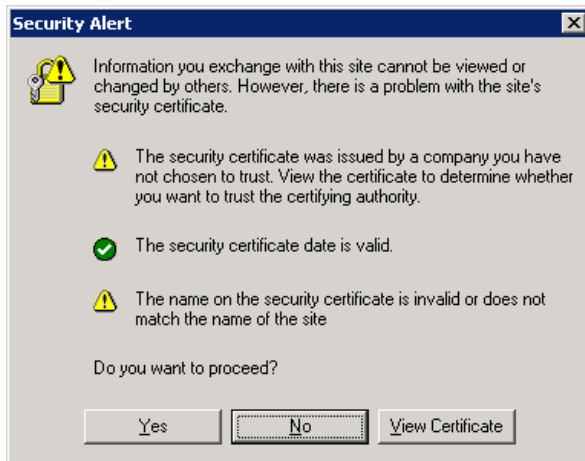
Pinging 10.1.100.1 with 32 bytes of data:

```
Reply from 10.1.100.1: bytes=32 time=2ms TTL=255  
Reply from 10.1.100.1: bytes=32 time<1ms TTL=255  
Reply from 10.1.100.1: bytes=32 time<1ms TTL=255  
Reply from 10.1.100.1: bytes=32 time<1ms TTL=255
```

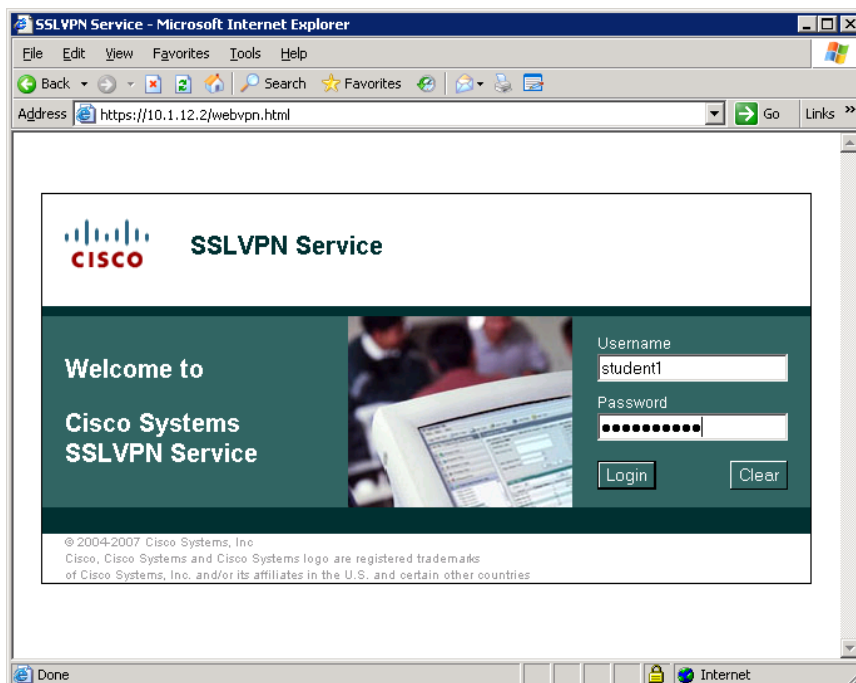
Ping statistics for 10.1.100.1:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

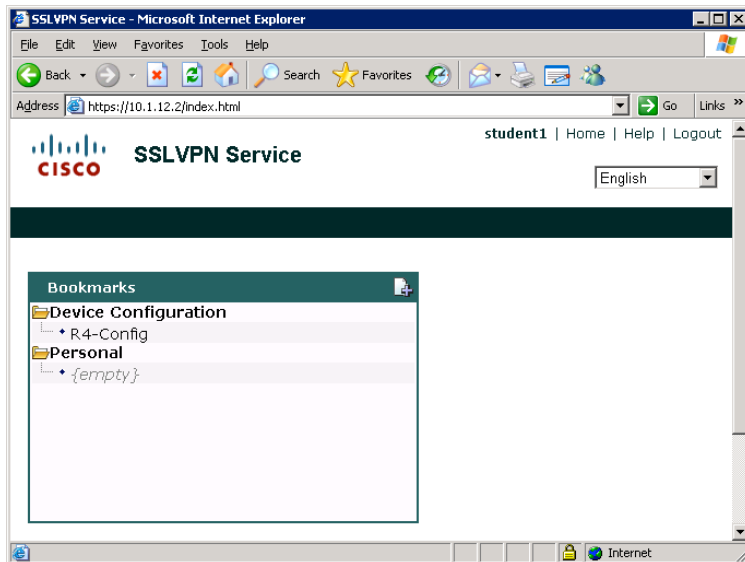
2. Run web browser and type in the address bar: http://10.1.12.2. The SSL certificate warning window should appear. Click Yes to accept the certificate.



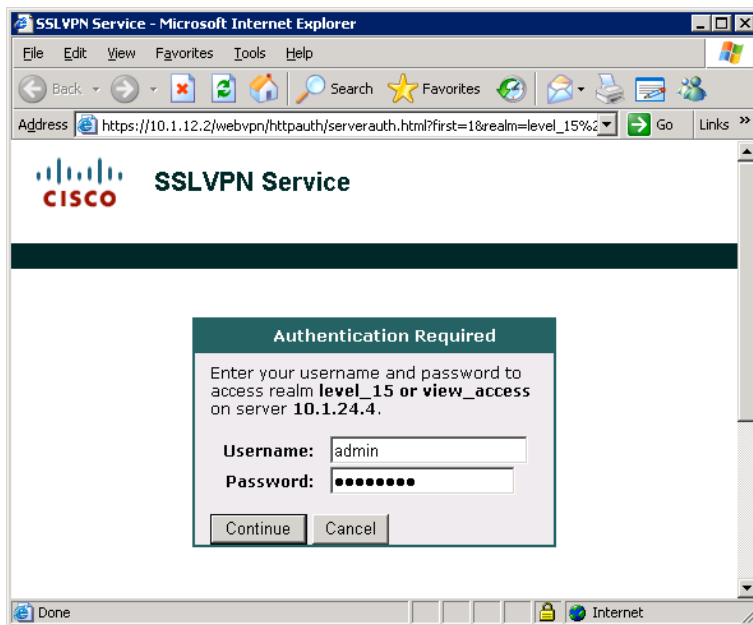
3. WebVPN website should be loaded. Use your credentials to log in.



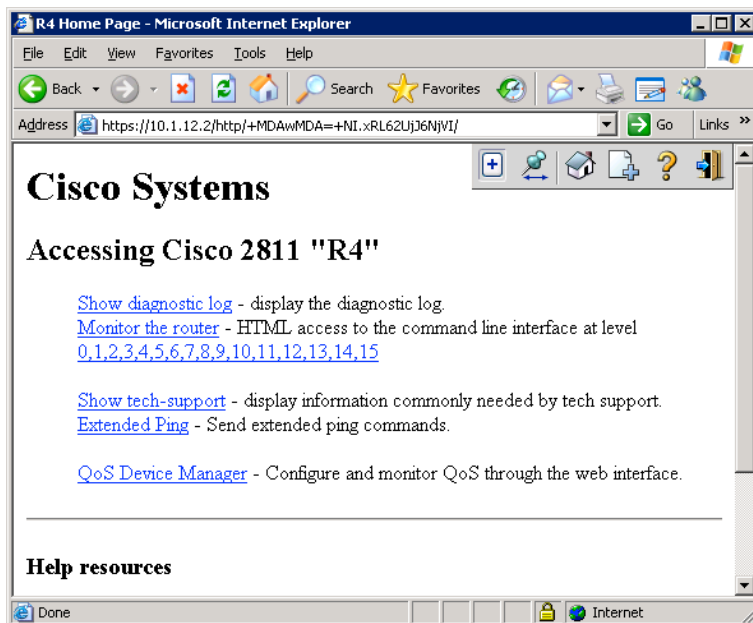
4. After successful login you should see configured bookmark. Click on it to connect to the R4's web management GUI.



5. As R4 management interface requires admin privileges, log in using administrator (priv 15) account.



6. It works!



Task 2

Add Thin Client WebVPN option to the previous configuration so that authenticated users will be forwarded to R4 router when connecting to their local ports:

Local Port	Remote Port (on R4)	Description
2200	22	SSH to R4
2300	23	TELNET to R4

The Java plugin must run automatically after user's login.



Using SSL VPN we can access corporate resources in a secure way. However, in the previous task we configured basic access to the "application" accessed by the web browser.

What if we have an application installed on our local system which must connect to the other ports than HTTP/HTTPS? Such application must be "tunneled" somehow through our SSL VPN. This can be done using a feature called Port Forwarding and available in SSL VPN by some JAVA plug-in runs on our web browser. The main advantage of it is that the user does not need administrative privileges on the system to run the plug-in.

We will use two applications to show how it works: TELNET and SSH client.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#webvpn context SSL-CONTEXT
R2(config-webvpn-context)#port-forward Applications-List
R2(config-webvpn-port-fwd)#local-port 2200 remote-server 10.1.24.4
remote-port 22 description "SSH on R4"
R2(config-webvpn-port-fwd)#local-port 2300 remote-server 10.1.24.4
remote-port 23 description "TELNET on R4"
```

We need to add Port Forwarding feature to our context. This is configured by enabling a «container» for our applications. This feature runs JAVA plug-in on the client and start listening on a local port and loopback IP address of 127.0.0.1. This port is then redirected by the plug-in to the real IP/port on the corporate network.

```
R2(config-webvpn-port-fwd)#exit
R2(config-webvpn-context)#policy group SSL-POLICY
R2(config-webvpn-group)#port-forward Applications-List auto-
download
R2(config-webvpn-group)#exit
R2(config-webvpn-context)#exit
```

Configuring the Port Forward application list is not enough. We need to enable it by associating it with our Policy. The policy is already associated with the context. We can specify the JAVA plug-in behavior - it may run automatically when client gets access to the portal or may be run manually.

Step 2 R4 configuration.

```
R4(config)#ip domain-name micronicstraining.com
R4(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R4.micronicstraining.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

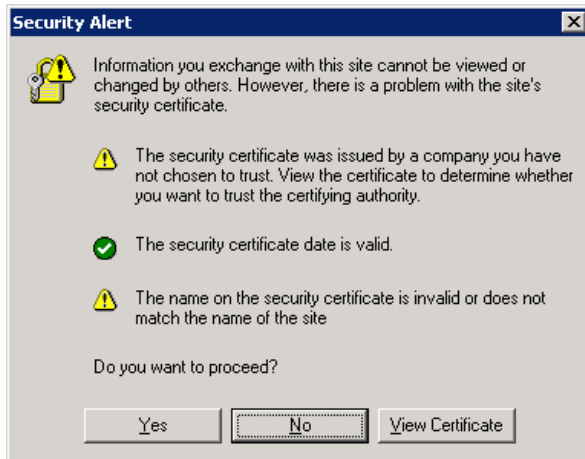
R4(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
R4(config)#line vty 0 4
R4(config-line)#login local
```

We'll need SSH server on R4 for verification purposes. To enable it there must be hostname/domain-name configured and RSA keys generated.

Verification:

Connect using SSL web browser from PC to R2.

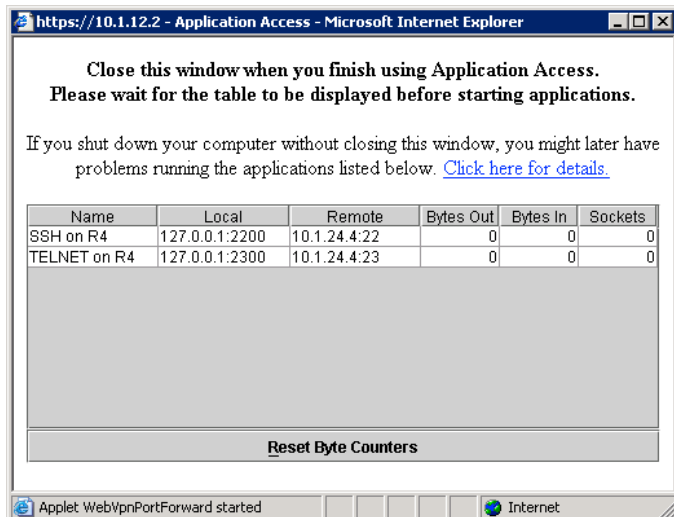
1. Run web browser and type in the address bar: `http://10.1.12.2`. The SSL certificate warning window should appear. Click Yes to accept the certificate.



2. WebVPN website should be loaded. Use your credentials to log in.

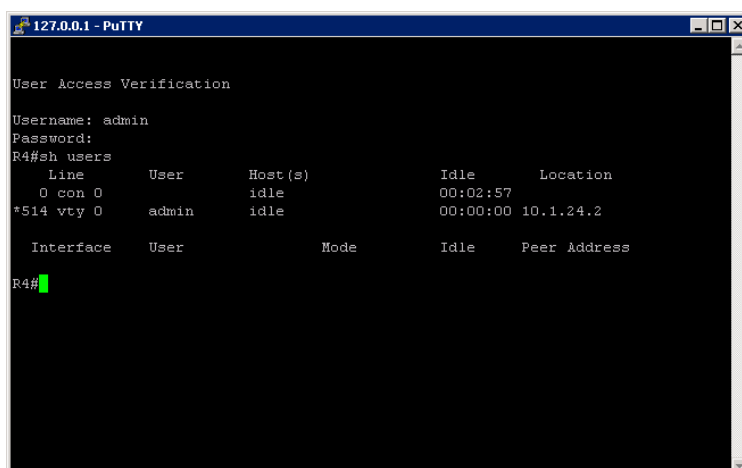
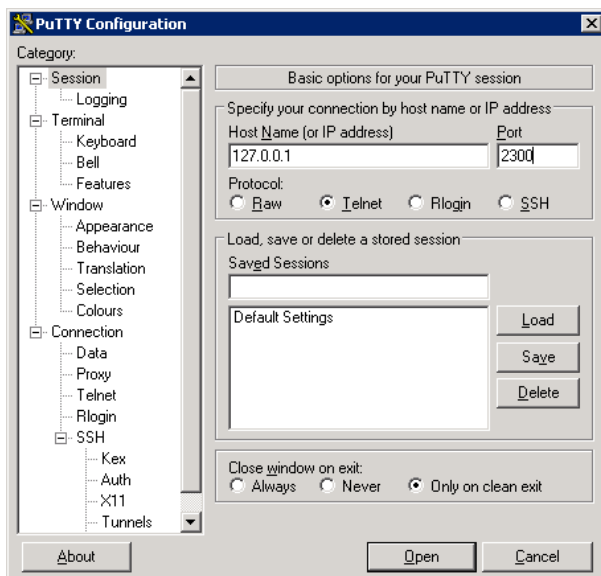


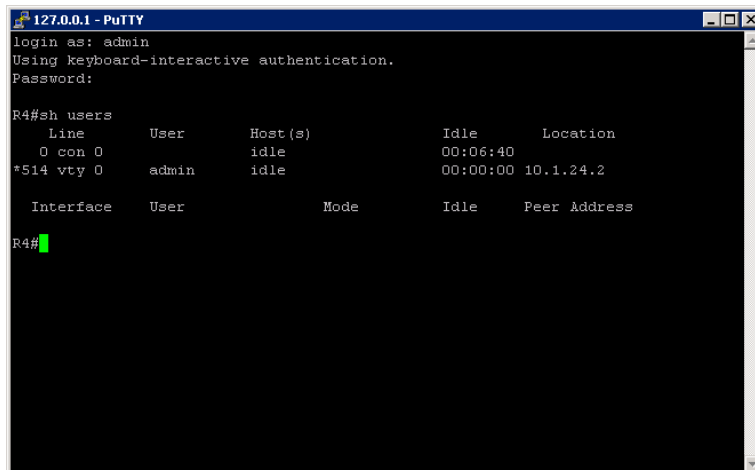
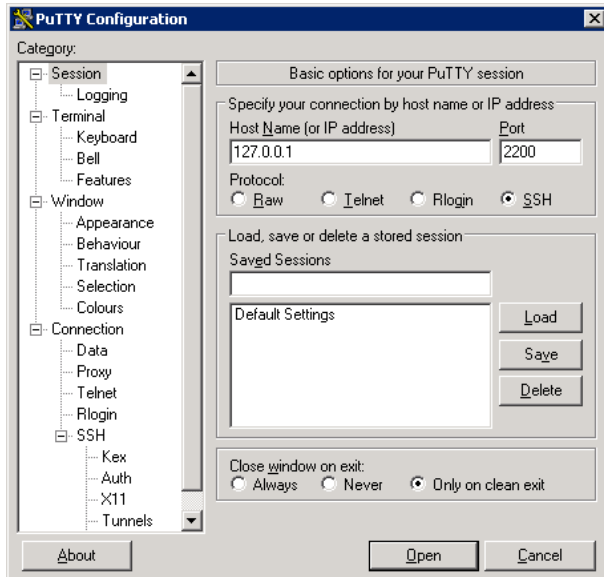
3. After successful login you should see configured bookmark and Port Forwarding Java applet should automatically start. Depends on your browser security level configuration you should accept some security warnings regarding running an unsigned applets.



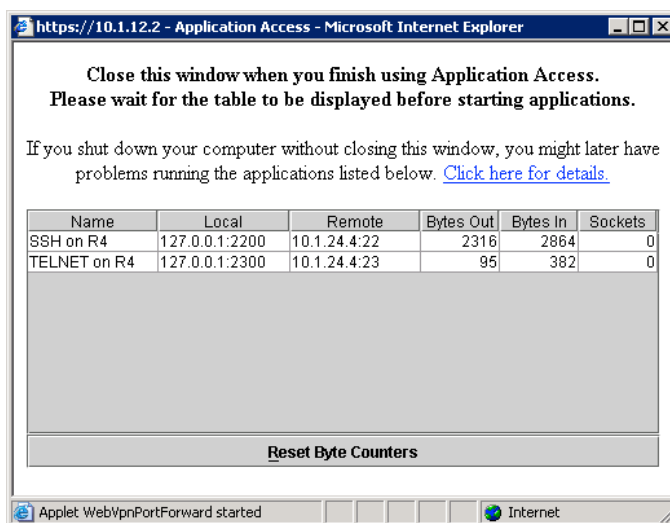
4. Telnet using your favorite terminal software to the IP address of 127.0.0.1 and port 2300. You should be tunneled to the R4. Note that source IP address of this connection is R2's interface (10.1.24.2).

Do the same for SSH connection to the IP address of 127.0.0.1 and port 2200.





5. Check Java applet window and see there are packets tunneled for both connections.



Task 3

Configure full SSL VPN client on the R2 router. User should be able manually run Tunnel connection after successful authentication to WebVPN. The SSL VPN Client package (sslclient-win-1.1.4.176.pkg) is located on the Flash memory. User's workstation should get IP address from a pool of 192.168.2.10 – 192.168.2.60. After tunnel set up the user should be able to connect R4's F0/0 interface using SSH and TELNET natively. Rest of user's traffic should be sent out without any encryption.



Now, what if we have an application which has this server IP address embedded in the code? That application must connect directly to its server. To make it happen we need full SSL Client software installed on the client's machine. To run and install this software the client must have administrative privileges on the system.

We also need full client software (called SVC – SSL VPN Client) installed on the router to make it available to the client for download. Hence, it is called Full Client mode or Tunnel Mode.

The SVC works similar to the IPSec client but the SVC uses SSL for securing the connection.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#webvpn      install      svc      flash:sslclient-win-  
1.1.4.176.pkg  
SSLVPN Package SSL-VPN-Client : installed successfully
```

*The SVC software image must be already on the flash.
To use it with SSL VPN we must install it first.*

```
R2(config)#ip access-list extended SSL-VPN-ACL  
R2(config-ext-nacl)# permit tcp 192.168.2.0 0.0.0.255 host  
10.1.24.4 eq telnet  
R2(config-ext-nacl)# permit tcp 192.168.2.0 0.0.0.255 host  
10.1.24.4 eq 22  
R2(config-ext-nacl)# exit
```

*This is an ACL specifying what traffic will tunneled
by tha SVC. This is not a split tunnel list! This is*

an ACL applied on the tunnel to make only certain services available for a client.

```
R2(config)#ip local pool SSL-VPN-POOL 192.168.2.10
192.168.2.60
```

This is a pool of IP addresses for a client. Just like it is with IPSec client, the full client software must get an IP address to use during the connections.

```
R2(config)#webvpn context SSL-CONTEXT
R2(config-webvpn-context)# policy group SSL-POLICY
R2(config-webvpn-group)# filter tunnel SSL-VPN-ACL
R2(config-webvpn-group)# svc split include 10.1.24.0
255.255.255.0
```

The tunnel policy must be configured under the Policy Group. The same for Split Tunnel list, which is configured without any ACL.

```
R2(config-webvpn-group)# functions svc-enabled
R2(config-webvpn-group)# svc address-pool SSL-VPN-POOL
```

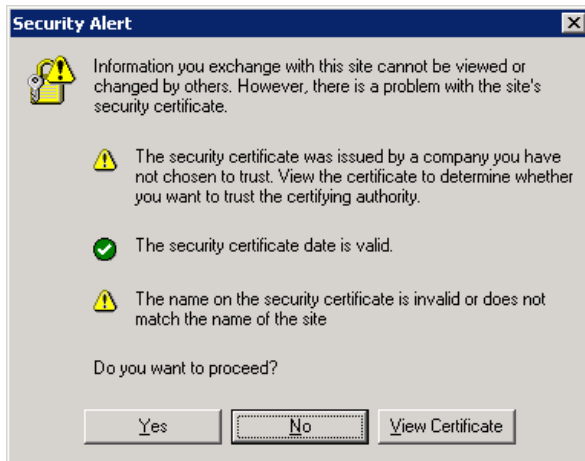
We need to enable SVC in the policy and specify the IP address pool to be given out to the client.

```
R2(config-webvpn-group)# exit
R2(config-webvpn-context)# exit
```

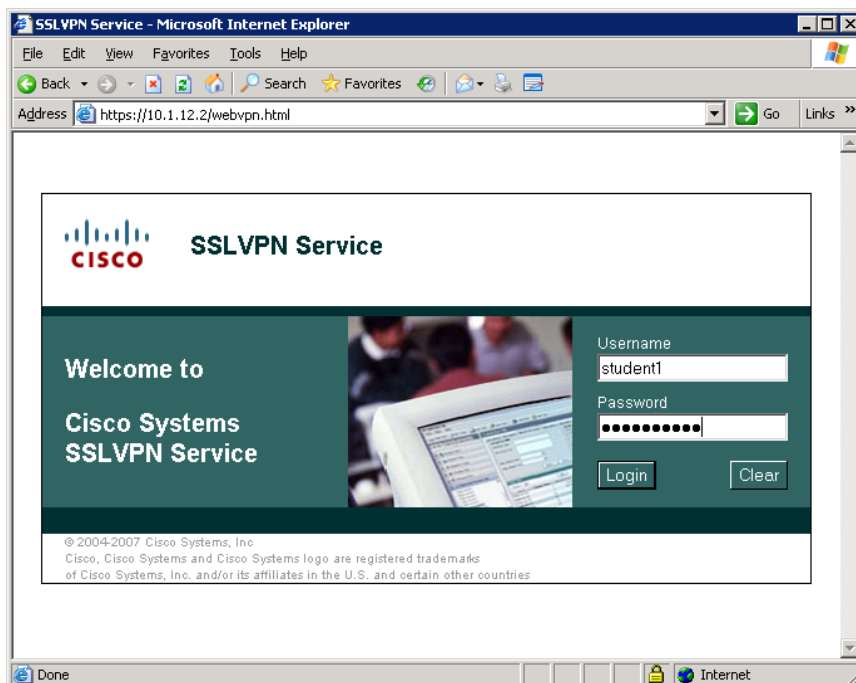
Verification:

Connect using SSL web browser from PC to R2.

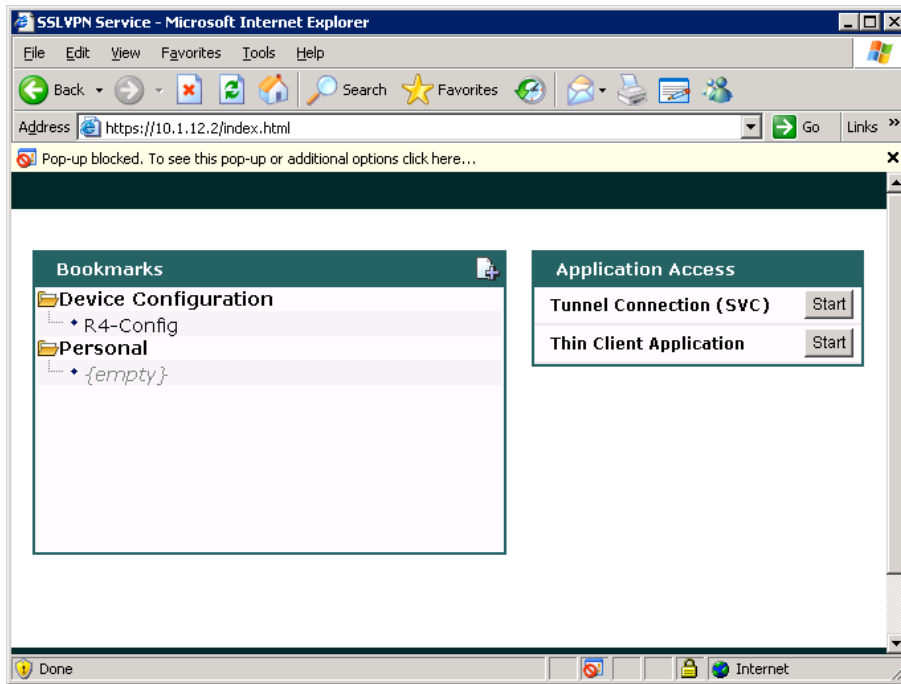
1. Run web browser and type in the address bar: http://10.1.12.2. The SSL certificate warning window should appear. Click Yes to accept the certificate.



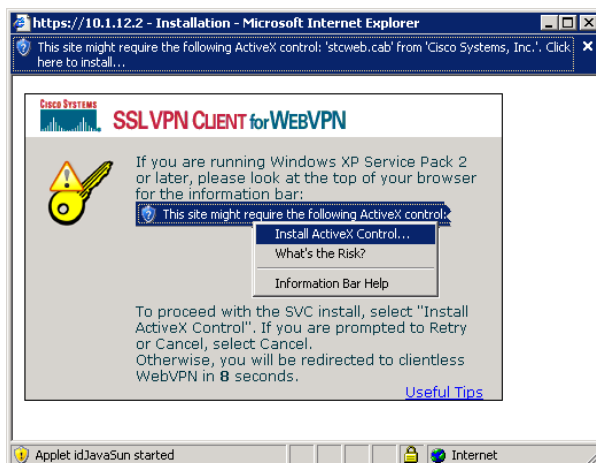
2. WebVPN website should be loaded. Use your credentials to log in.



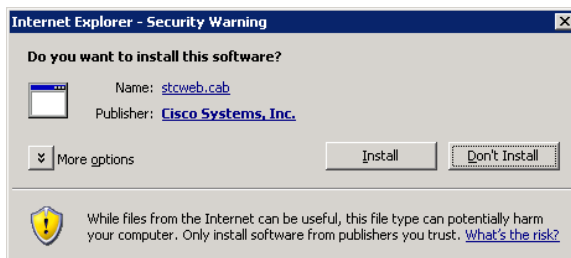
3. After successful log in you should see Tunnel Connection (SVC) available. Click Start button.



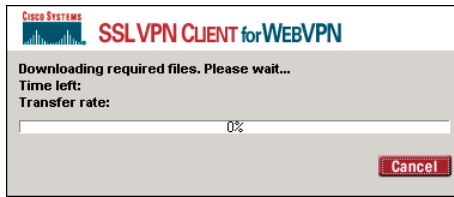
4. Allow running of ActiveX applet in your web browser and install it.



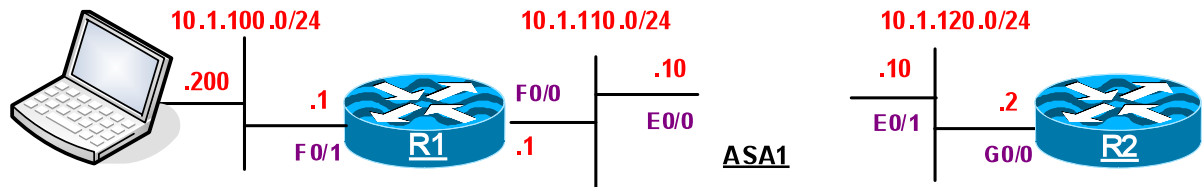
5. You must have administrator right to be able to install the applet



6. After successful installation, the SSL VPN Client runs and establishes the tunnel.



Lab 1.64. Configuring SSL VPN (ASA)



Lab Setup

- R1's F0/0 and ASA1's E0/0 interface should be configured in VLAN 110
- R2's G0/0 and ASA1's E0/1 interface should be configured in VLAN 120
- R1's F0/1 and VPN Client PC (SW3 – F0/15) should be in VLAN 100
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1 and R2 pointing to the ASA

IP Addressing

Device	Interface	IP address
R1	F0/0	10.1.110.1 /24
	F0/1	10.1.100.1 /24
ASA1	E0/0	10.1.110.10 /24
	E0/1	10.1.120.10 /24
R2	F0/0	10.1.120.2 /24
PC	NIC	10.1.100.200 /24

Task 1

Configure Clientless SSL VPN on ASA1 so that it allows users accessing R2's HTTP server after successful authentication using local user database located on the ASA. The user named "student1" with a password of "student123" should be able to enter custom URL to go to R2.

You may need to enable HTTP server on R2 and configure local administrator account (admin/admin123) to verify this task.



Same SSL VPN functionality is available on the ASA. The configuration on the ASA is much simpler than on IOS. We do not use gateways and contexts here. We just configure everything using “webvpn” configuration mode and group policy to specify all user properties.

The functionality is pretty the same comparing to the IOS.

Configuration

Complete these steps:

Step 1 ASA1 configuration.

```
ASA1(config)# webvpn
ASA1(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
```

All SSL VPN headend configuration we perform under “webvpn” mode. First we need enable it on an interface (usually on the outside interface).

```
ASA1(config-webvpn)# group-policy CL-SSL-VPN-GP internal
ASA1(config)# group-policy CL-SSL-VPN-GP attributes
ASA1(config-group-policy)# vpn-tunnel-protocol webvpn
ASA1(config-group-policy)# exit
```

The client connection (what does he/she see after connecting to the ASA) is performed under Group Policy which is associated with a user account. The Group Policy may be internal (configured on the ASA) or external (configured on the ACS).

```
ASA1(config)# username student1 pass student123
ASA1(config)# username student1 attributes
ASA1(config-username)# vpn-group-policy CL-SSL-VPN-GP
ASA1(config-username)# exit
```

Step 2 Configure static route on client PC.

```
route add 10.1.110.0 mask 255.255.255.0 10.1.100.1
```

Step 3 R2 configuration.

```
R2(config)#ip http server
R2(config)#ip http authentication local
R2(config)#username admin privilege 15 password admin123
R2(config)#line vty 0 4
```

```
R2(config-line)#login local
R2(config)#end
```

We need to enable HTTP server on R2 to verify this task.

Verification

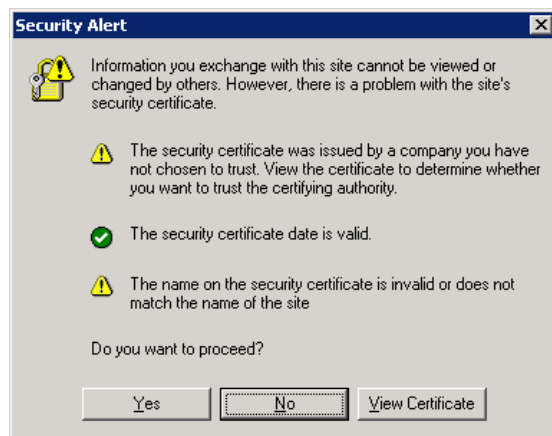
1. ***(Optional) If R2 has no internal HTTP server software (depends on IOS version), you can store some file on the flash memory and then try to access it using SSL VPN terminated on the ASA***

```
R2#copy run flash:run.txt
Destination filename [run.txt]?

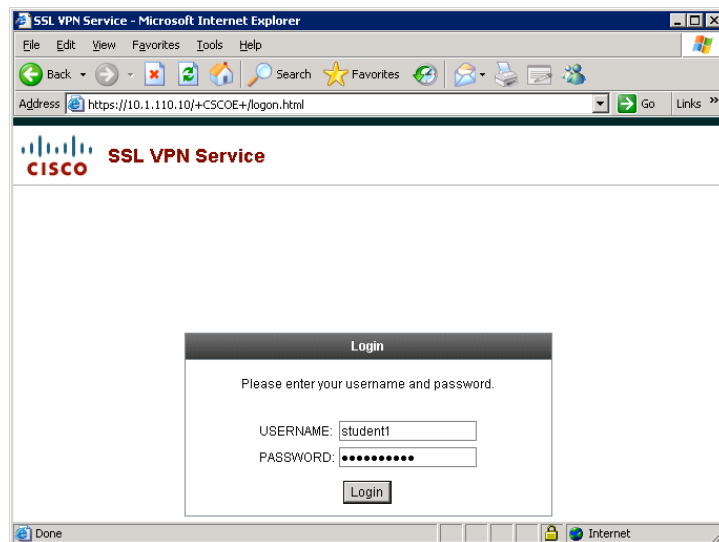
1152 bytes copied in 3.956 secs (291 bytes/sec)
```

You can access that file by going to `http://10.1.120.2/flash:run.txt` (see step 4).

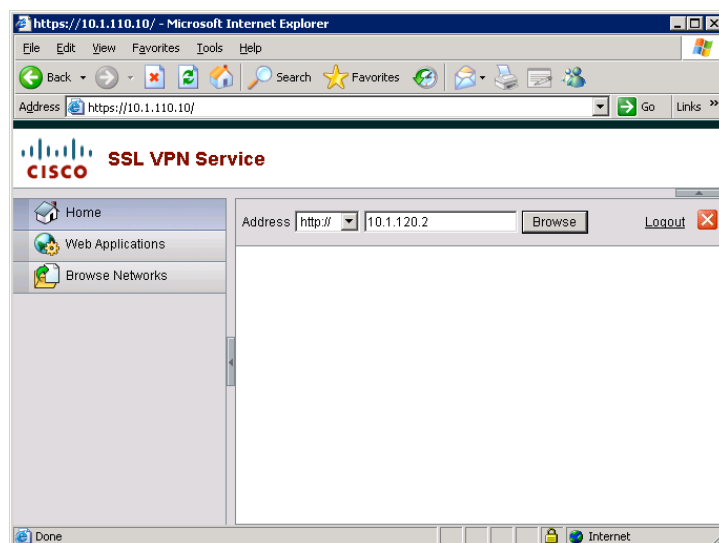
2. ***Run web browser and type in the address bar: `https://10.1.110.10`. The SSL certificate warning window should appear. Click Yes to accept the certificate.***



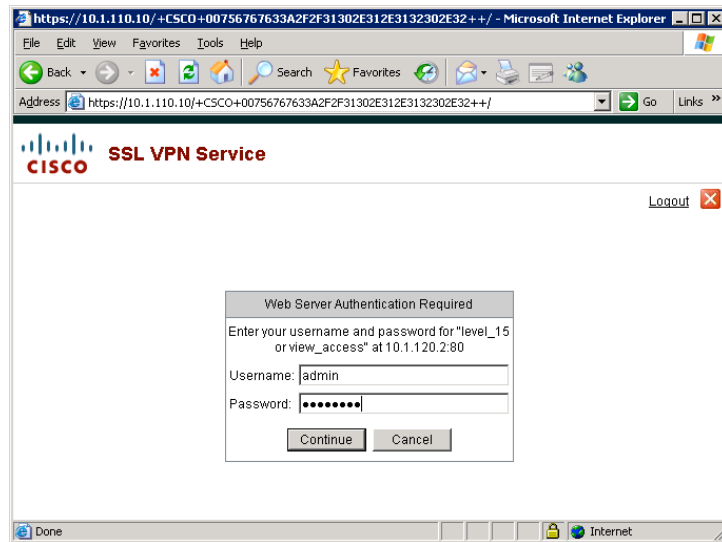
3. ***WebVPN website should be loaded. Use your credentials to log in.***



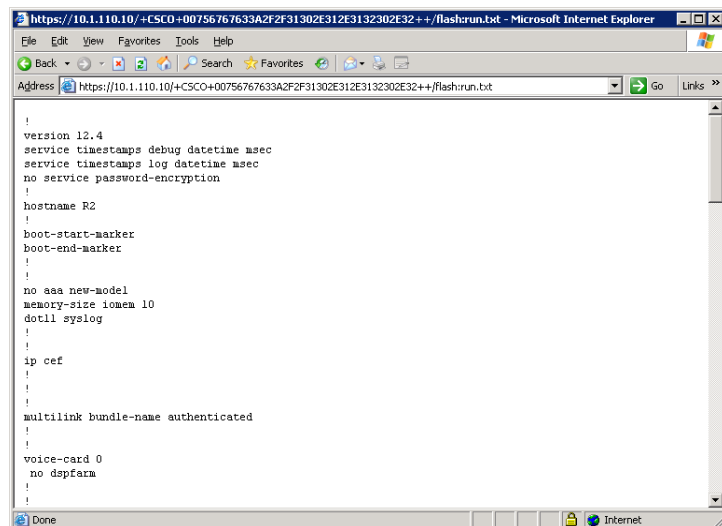
4. Enter the custom URL to access the file stored on R2 (or R2's Web Server page if existed). To access file on R2's flash you need to enter 10.1.120.2/flash:run.txt. To access R2's Web Server, just enter 10.1.120.2 and click on Browse.



5. You need to first authenticate as an admin user to R2



6. The file is loaded (or Web Server's start page is loaded). It works!



OR



ASA1(config)# sh webvpn statistics

```
Total number of objects served      242
      html                          95
      js                            83
      css                           0
      vb                            0
      java archive                   7
      java class                     0
      image                          17
      undetermined                   40
```

ASA1(config)# sh crypto protocol statistics ssl

```
[SSL statistics]
  Encrypt packet requests: 8636
  Encapsulate packet requests: 8636
  Decrypt packet requests: 4755
  Decapsulate packet requests: 4755
  HMAC calculation requests: 13391
  SA creation requests: 145
  SA rekey requests: 0
  SA deletion requests: 145
  Next phase key allocation requests: 0
  Random number generation requests: 0
  Failed requests: 0
```

ASA1(config)# sh vpn-sessiondb webvpn

Session Type: WebVPN

```
Username      : student1          Index      : 14
Public IP     : 10.1.100.200
Protocol      : Clientless
```

```

License      : SSL VPN
Encryption   : RC4                      Hashing      : SHA1
Bytes Tx     : 66668                    Bytes Rx     : 16035
Group Policy : CL-SSL-VPN-GP            Tunnel Group : DefaultWEBVPNGroup
Login Time   : 09:51:04 UTC Sat Jul 31 2010
Duration     : 0h:00m:20s
NAC Result   : Unknown
VLAN Mapping : N/A                      VLAN         : none

```

Note that we are using Clientless mode. There was a default tunnel group used for terminating this connection. However, the user "student1" has group policy attached to his profile.

Task 2

Add Port Forwarding feature to the previous configuration so that authenticated users will be forwarded to R2 router when connecting to their local ports:

Local Port	Remote Port (on R2)	Description
2200	22	SSH to R2
2300	23	TELNET to R2

In addition to that, allow the user to run "telnet.exe" application natively (directly connecting to R2's real IP address). Disable file browsing over the network.



The same feature of Port Forwarding is available on the ASA. However, here is another feature called Smart Tunneling which "certifies" an application to be able to tunnel traffic through the SSL VPN no matter what IP address or port the traffic is destined to.

Configuration

Complete these steps:

Step 1 ASA configuration.

```

ASA1(config)# webvpn
ASA1(config-webvpn)# port-forward Devices 2200 10.1.120.2 22 SSH to
R2
ASA1(config-webvpn)# port-forward Devices 2300 10.1.120.2 23 TELNET
to R2

```

Configuration of Port Forwarding and Smart Tunneling is performed under "webvpn" mode. However, both features must be enabled under Group Policy to be accessible to the user.

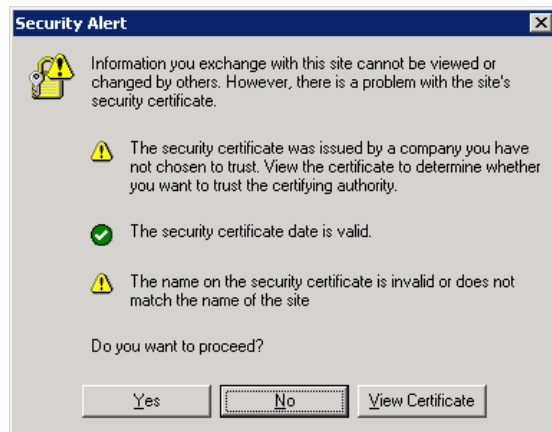
```
ASA1(config-webvpn)# smart-tunnel list Applications TELNET  
"telnet.exe"
```

```
ASA1(config-webvpn)# group-policy CL-SSL-VPN-GP attributes  
ASA1(config-group-policy)# webvpn  
ASA1(config-group-webvpn)# smart-tunnel enable Applications  
ASA1(config-group-webvpn)# port-forward enable Devices  
ASA1(config-group-webvpn)# file-entry disable  
ASA1(config-group-webvpn)# file-browsing disable
```

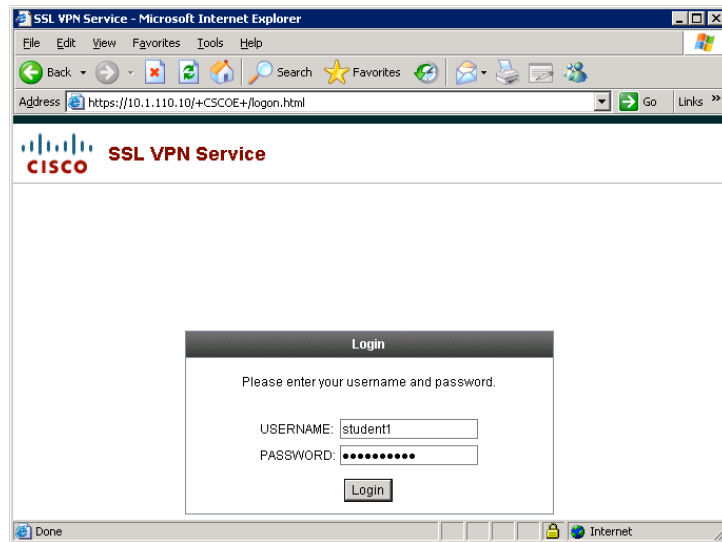
Here we need enable Port Forwarding and Smart Tunneling. In addition to that we have been asked to disable File Browsing on the network.

Verification

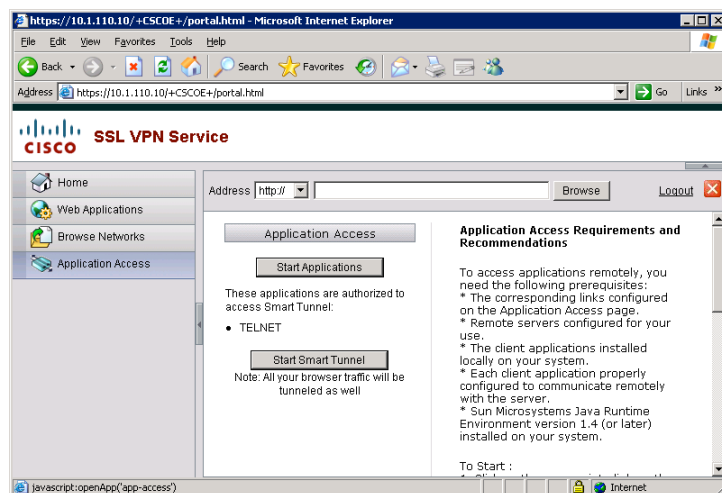
1. Run web browser and type in the address bar: <https://10.1.110.10>. The SSL certificate warning window should appear. Click Yes to accept the certificate.



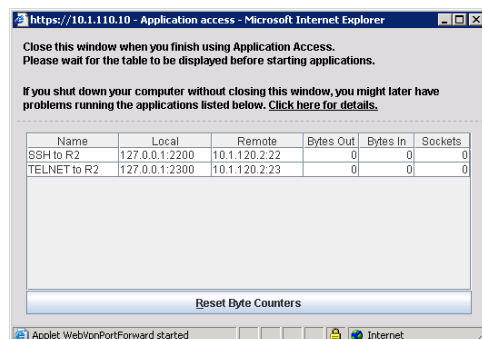
2. WebVPN website should be loaded. Use your credentials to log in.



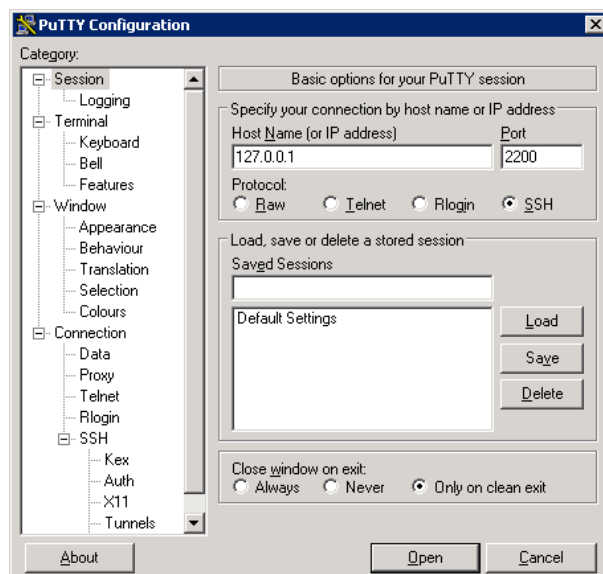
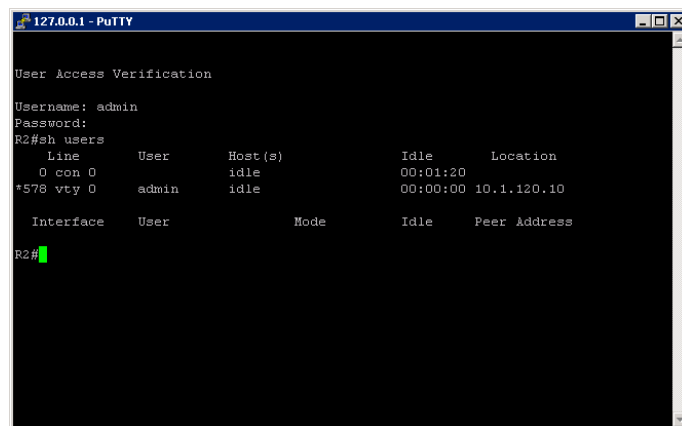
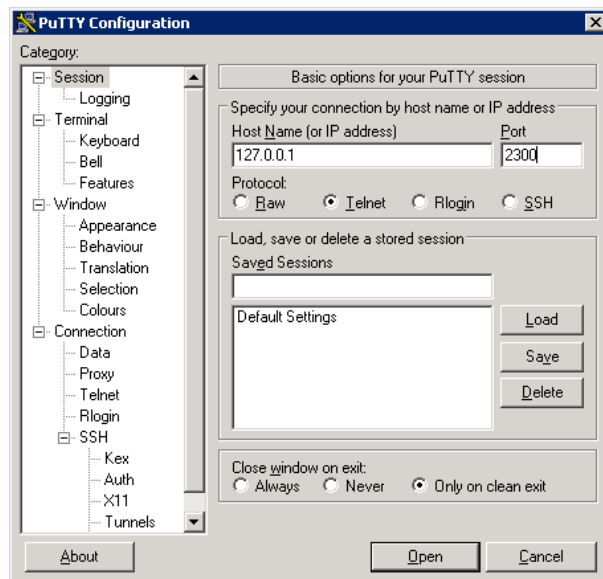
3. After successful authentication, click on Start Application button to run java-based Port Forwarding.

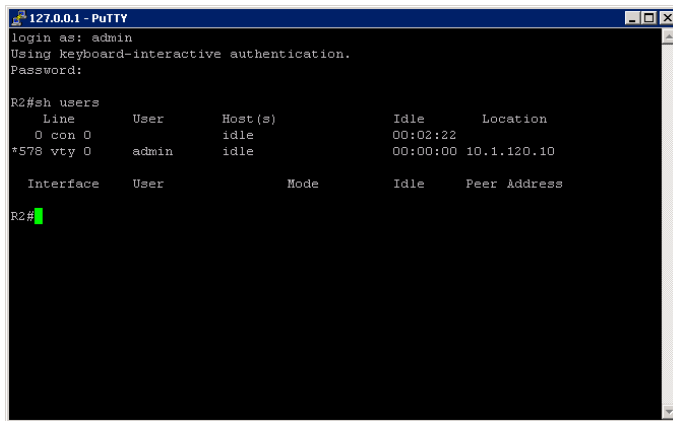


4. Java applet is running and starts listening on specified ports.



5. You can connect to R2's using your favorite terminal software. You should use local loopback IP address (127.0.0.1) and port 2300 to be forwarded to R2 on port 23.



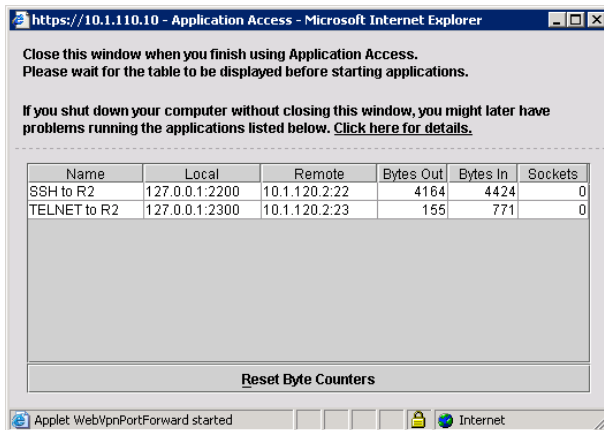


```
127.0.0.1 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:

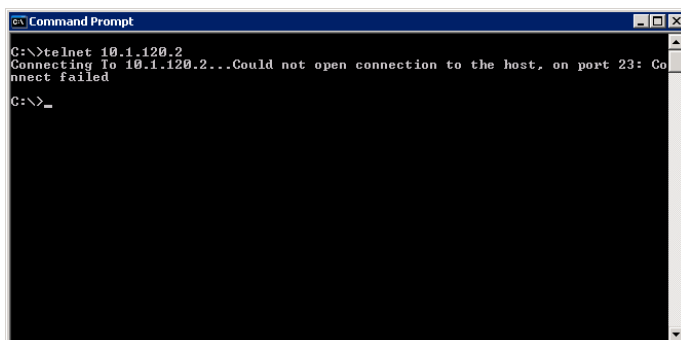
R2#sh users
  Line   User      Host(s)      Idle      Location
  0 con 0           idle        00:02:22
+578 vty 0   admin     10.1.120.10  00:00:00
  Interface  User      Mode      Idle      Peer Address

R2#
```

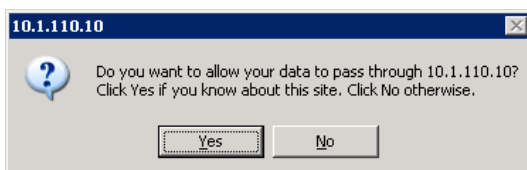
6. See the counters incrementing.

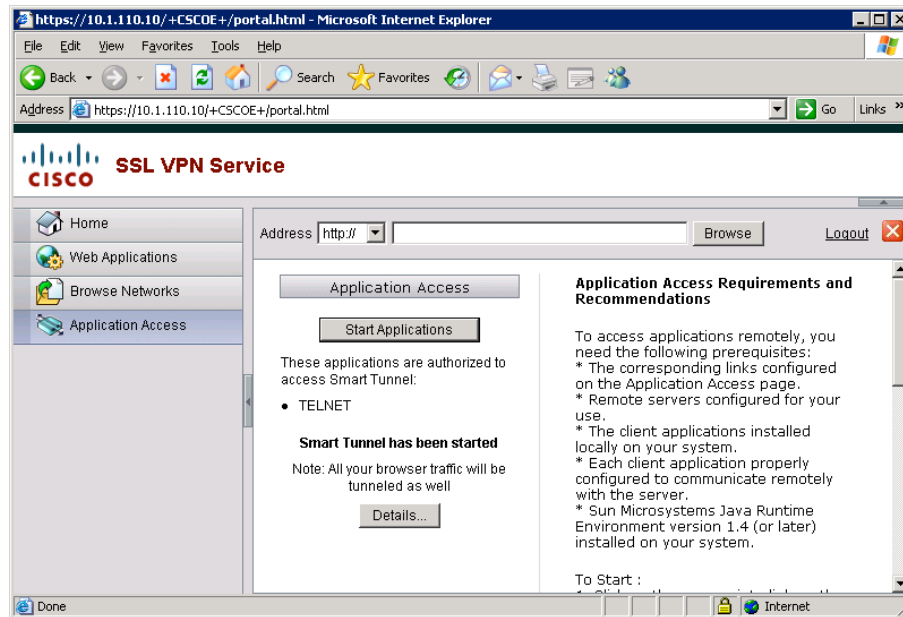


7. Try to connect directly to R2 using telnet.

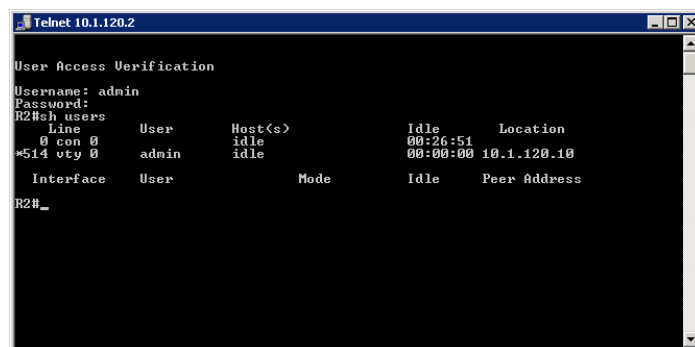


Now, click on Start Smart Tunnel button.

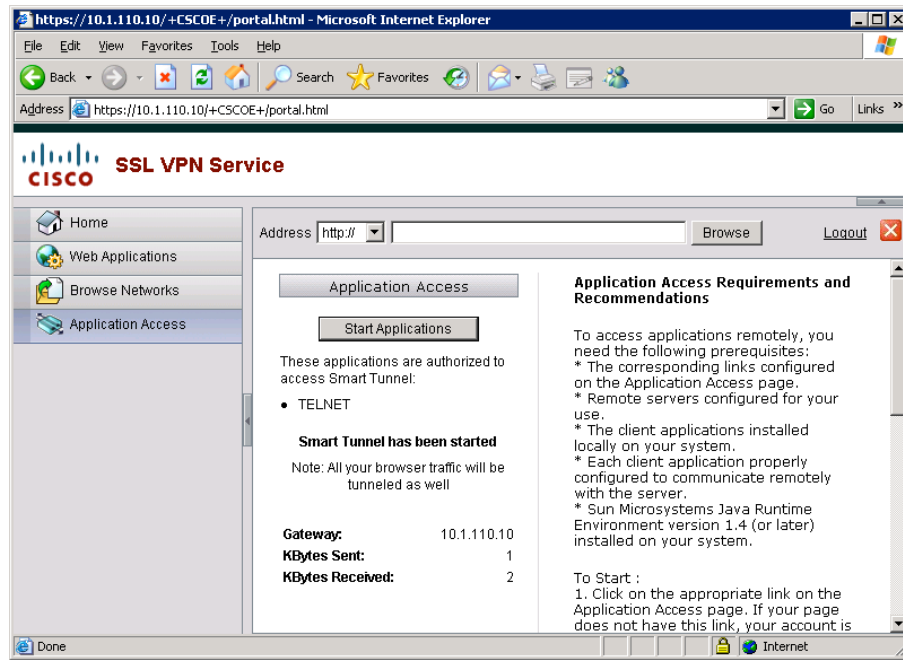




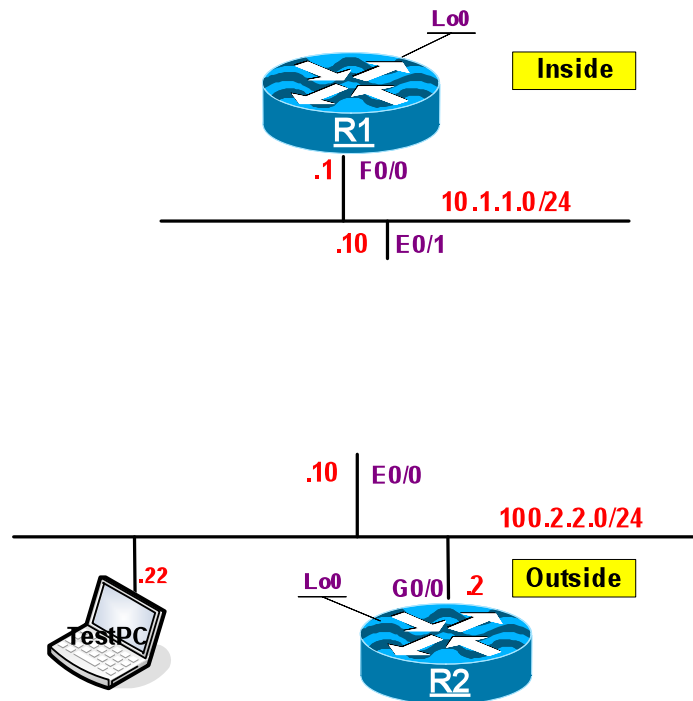
8. You can connect to R2's IP address natively using telnet.exe application. Go to Start → Run, then enter "telnet 10.1.120.2" to connect directly to R2.



9. Click on Details button to see that counters for this connection are increasing.



Lab 1.65. AnyConnect 3.0 Basic Setup



Lab Setup

- R1's F0/0 and ASA84 E0/1 interface should be configured in VLAN 10
- R2's G0/0 and ASA84 E0/0 interface should be configured in VLAN 20
- Configure Telnet on all routers using password "cisco"
- Configure default routes on R1/R2 to point to ASA and static routes to reach router's loopbacks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.11.1/24
R2	Lo0	2.2.2.2/24
	G0/0	100.2.2.2/24
PC	NIC	100.2.2.22/24

ASA84	E0/0	100.2.2.10/24
	E0/1	10.1.1.10/24

Task 1

Configure AnyConnect 3.0 on the ASA so that it is possible to login on the Portal and download AnyConnect client. Then, the user should be able to setup a full DTLS tunnel authenticating to the group CCIE with username/password of ccie/ccie123.

Give out to the client an IP address from the pool 192.168.15.1 – 254.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA84(config)# webvpn
ASA84(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
ASA84(config-webvpn)# anyconnect image disk0:/anyconnect-win-
3.0.2052-k9.pkg
ASA84(config-webvpn)# anyconnect enable
ASA84(config-webvpn)# exit

ASA84(config)# username ccie password ccie123

ASA84(config)# ip local pool VPN-POOL 192.168.15.1-192.168.15.254

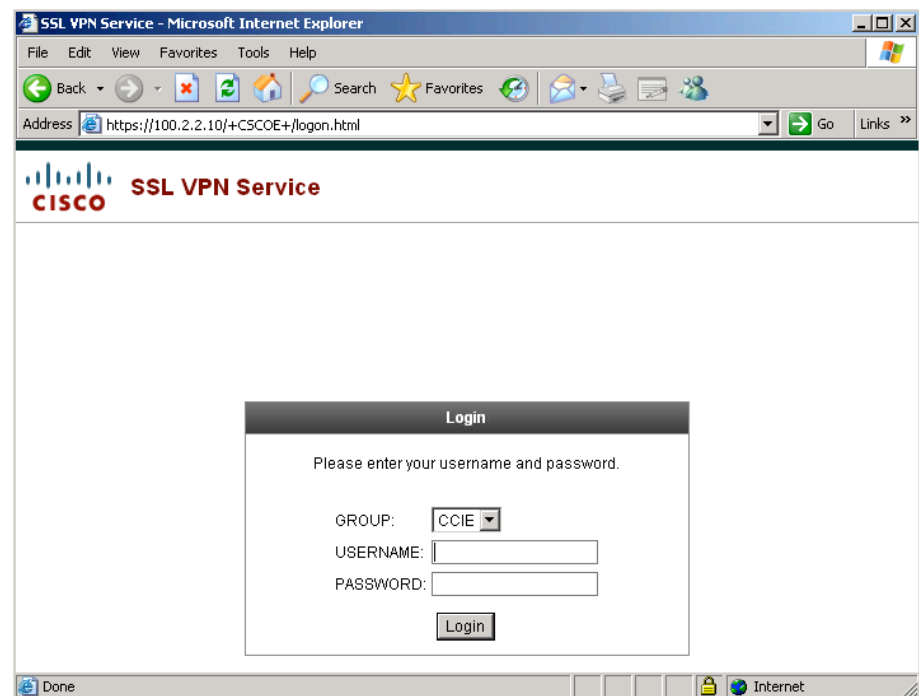
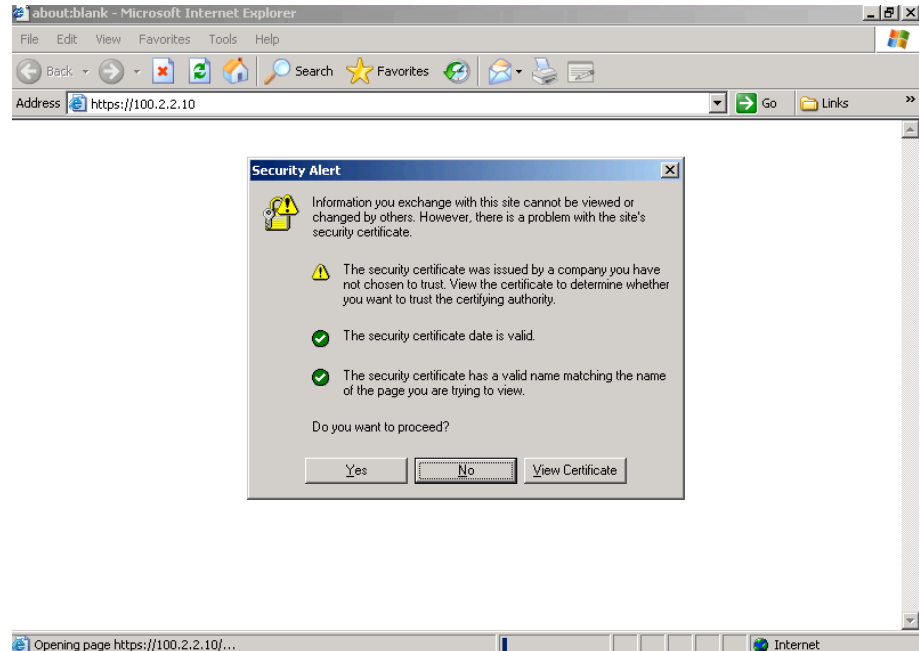
ASA84(config)# group-policy CCIE internal
ASA84(config)# group-policy CCIE attributes
ASA84(config-group-policy)# vpn-tunnel-protocol ssl-client ssl-
clientless
ASA84(config-group-policy)# address-pools value VPN-POOL
ASA84(config-group-policy)# exit

ASA84(config)# tunnel-group CCIE type remote-access
ASA84(config)# tunnel-group CCIE general-attributes
ASA84(config-tunnel-general)# default-group-policy CCIE
ASA84(config-tunnel-general)# exit
ASA84(config)# tunnel-group CCIE webvpn-attributes
ASA84(config-tunnel-webvpn)# group-alias CCIE
ASA84(config-tunnel-webvpn)# exit

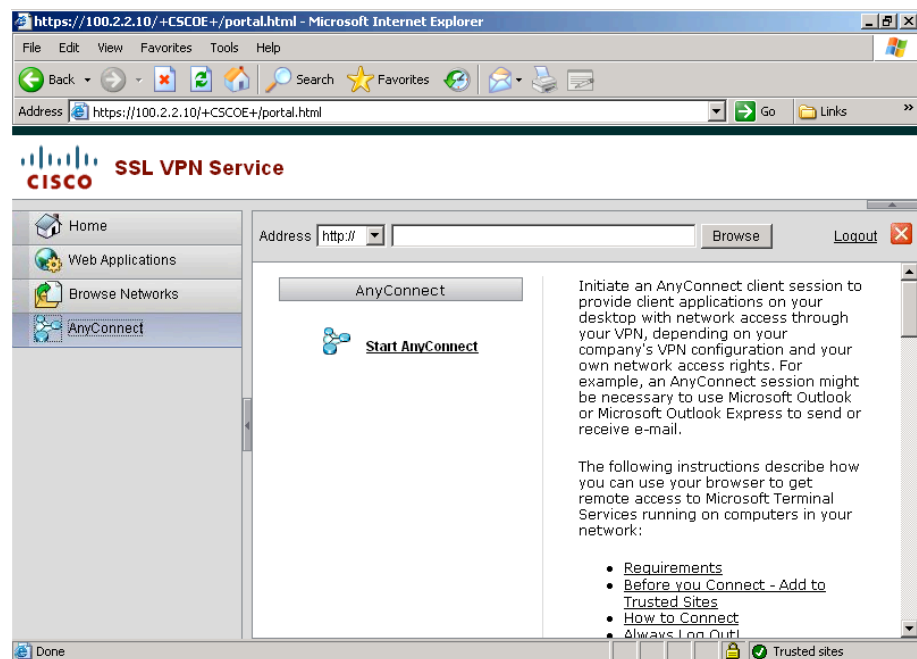
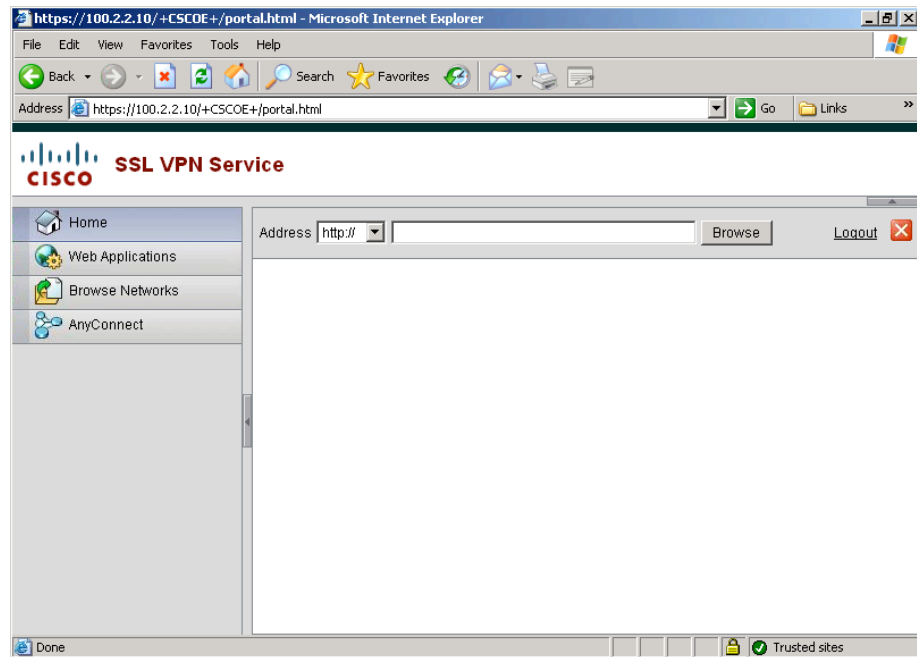
ASA84(config)# webvpn
ASA84(config-webvpn)# tunnel-group-list enable
ASA84(config-webvpn)# exit
```

Step 2 Client PC configuration.

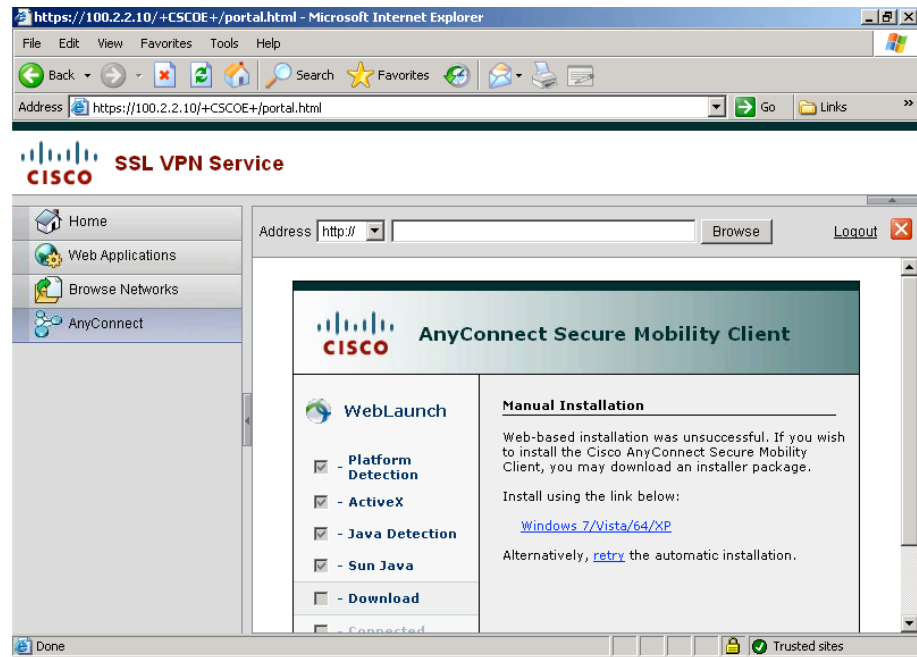
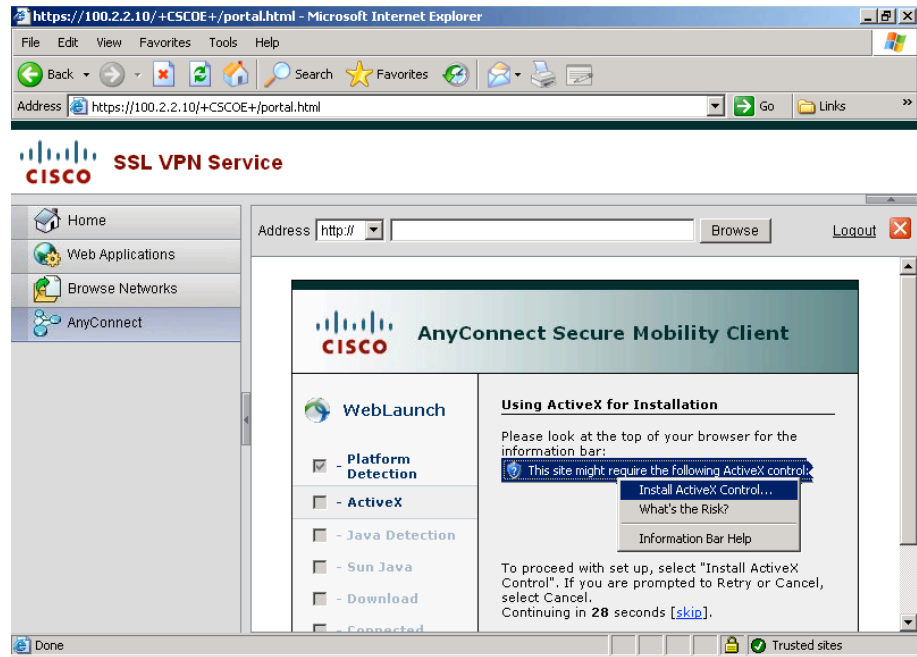
Go to the **PORTAL** using the address <https://100.2.2.10>, accept the certificate and authenticate to the group **CCIE**.



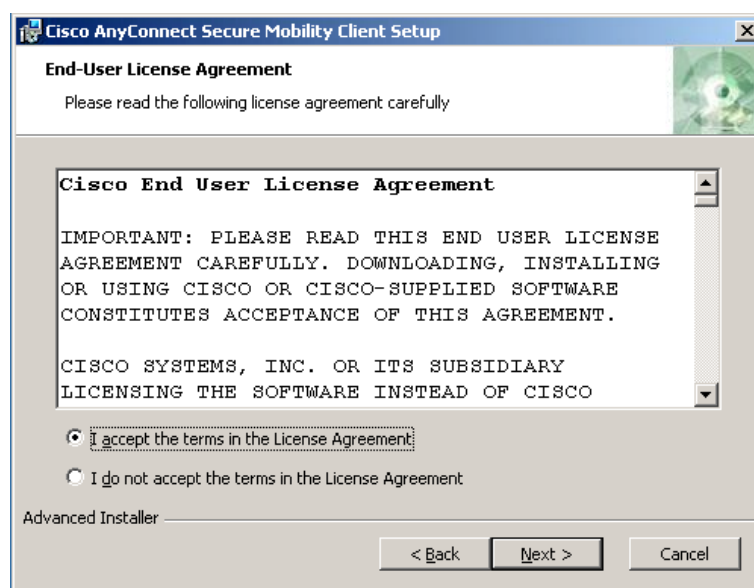
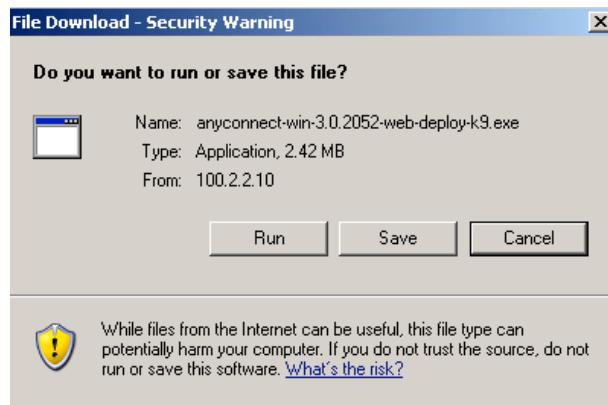
Then go to the **AnyConnect** tab (on the left pane) and click on **Start**

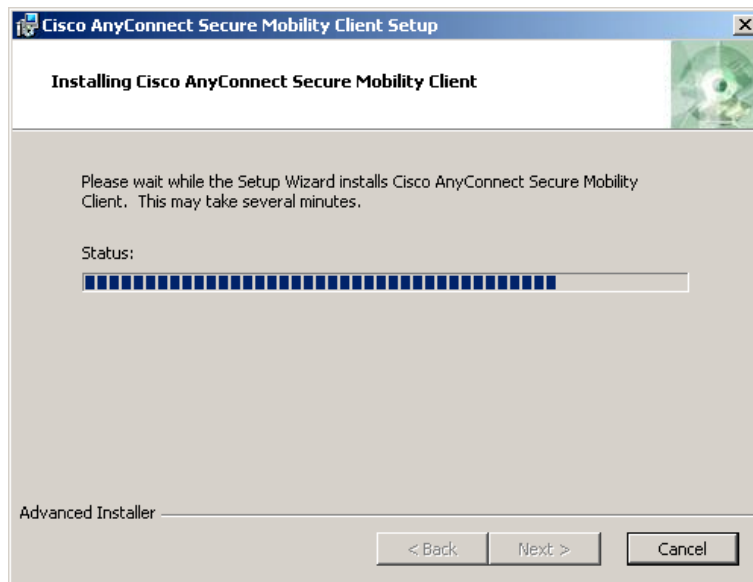
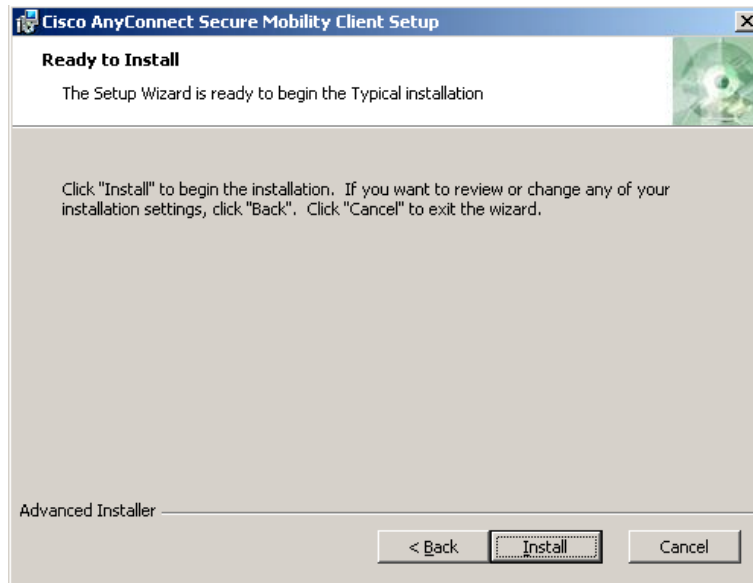
AnyConnect link.

Note that this site was added to trusted Sites in IE. This is useful to not see warning messages.



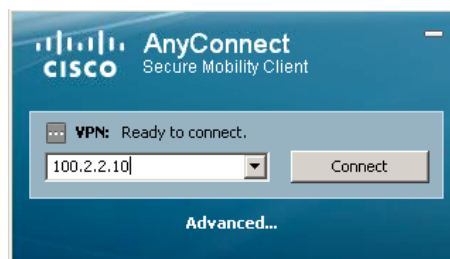
The web installation can be unsuccessful for Windows XP OS. Then you must click on the link, download the installer and manually install it.





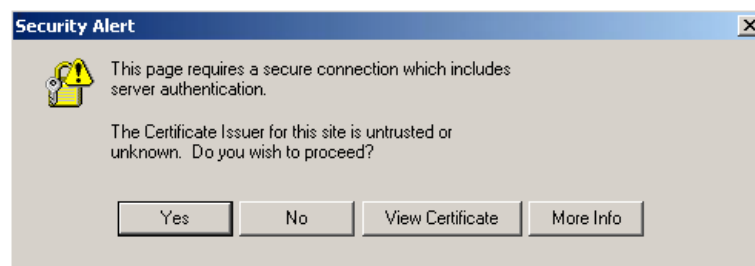


Run Cisco Anyconnect Secure Mobility Client from the Windows Start Menu.



Notice that if you do not have correct DNS configuration on the host, the AnyConnect displays an error message. It is not required to have DNS but it may help.

Click Connect button



The above message is displayed when ASA uses its default Identity Certificate generated based on ASA's IP address. This certificate is self-signed and can be installed in Windows local store.

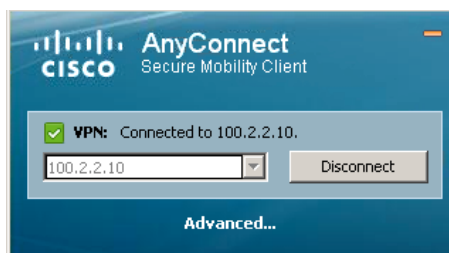
However, this certificate will be regenerated every ASA restart, so it is not worth to store it. Better, enroll for an external PKI certificate and use command 'ssl trust-point <TRUSTPOINT-NAME>' to specify what Identity certificate use for SSL connections.

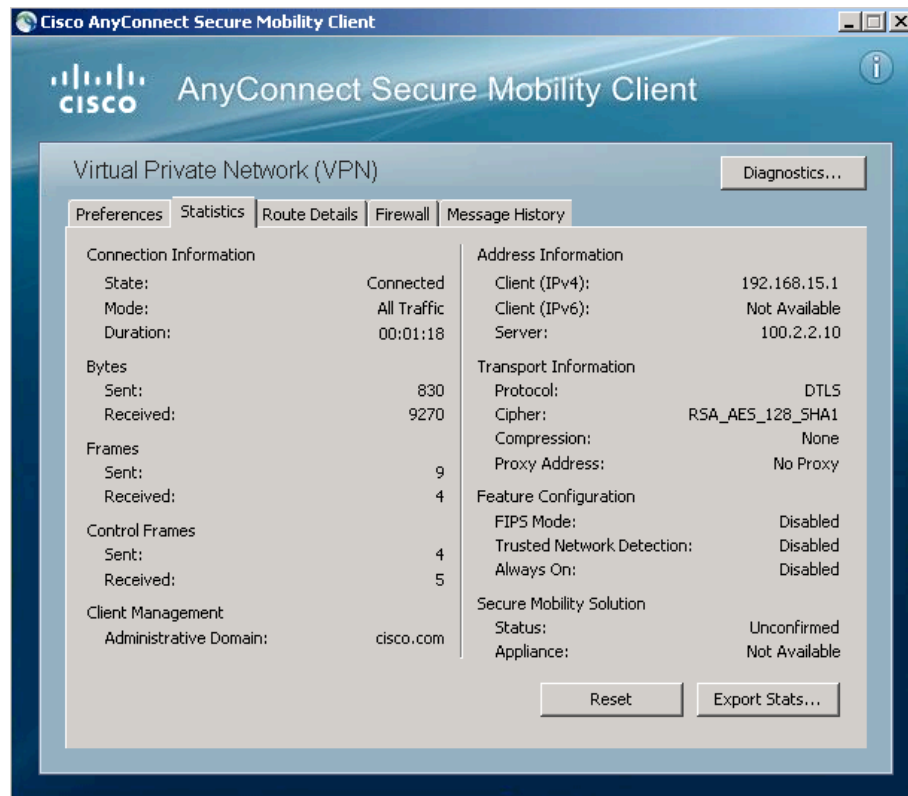
Provide a username and password for the CCIE group and hit OK.



Verification

Anyconnect has connected successfully. You can click on Advanced... button to see more details.





Try to ping IP address behind the ASA. Note that you can ping R1's f0/0 interface but not Loppback. Why? (for the answer go to the next task).

```

C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cisco>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=35ms TTL=255
Reply from 10.1.1.1: bytes=32 time=6ms TTL=255
Reply from 10.1.1.1: bytes=32 time=2ms TTL=255
Reply from 10.1.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 35ms, Average = 11ms

C:\Documents and Settings\cisco>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\cisco>

```

Below is the debug taken on the ASA during the connection. It is very useful to use logging filtering feature to just display what's really important. The following commands will display only useful information on the console:

```

logging enable
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging

```

logging class svc console debugging

```

%ASA-6-725001: Starting SSL handshake with client outside:100.2.2.22/1072 for TLSv1
session.
%ASA-7-725010: Device supports the following 4 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:100.2.2.22/1072 proposes the following 6 cipher(s).
%ASA-7-725011: Cipher[1] : AES256-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : DES-CBC3-SHA
%ASA-7-725011: Cipher[4] : RC4-SHA
%ASA-7-725011: Cipher[5] : RC4-MD5
%ASA-7-725011: Cipher[6] : DES-CBC-SHA
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:100.2.2.22/1072
%ASA-6-725002: Device completed SSL handshake with client outside:100.2.2.22/1072
%ASA-5-722033: Group <CCIE> User <ccie> IP <100.2.2.22> First TCP SVC connection
established for SVC session.
%ASA-6-722022: Group <CCIE> User <ccie> IP <100.2.2.22> TCP SVC connection established
without compression
%ASA-4-722051: Group <CCIE> User <ccie> IP <100.2.2.22> Address <192.168.15.1> assigned
to session
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: asa84.cisco.com'
Processing CSTP header line: 'Host: asa84.cisco.com'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.0.07059'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.0.07059'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.0.07059'
webvpn_cstp_parse_request_field()
...input: 'Cookie:
webvpn=369230436@24576@1075410852@427A1A2DFBFE94AE61D7BF5BC6EC169EC0E4BA1E'
Processing CSTP header line: 'Cookie:
webvpn=369230436@24576@1075410852@427A1A2DFBFE94AE61D7BF5BC6EC169EC0E4BA1E'
Found WebVPN cookie:
'webvpn=369230436@24576@1075410852@427A1A2DFBFE94AE61D7BF5BC6EC169EC0E4BA1E'
WebVPN Cookie:
'webvpn=369230436@24576@1075410852@427A1A2DFBFE94AE61D7BF5BC6EC169EC0E4BA1E'
IPADDR: '369230436', INDEX: '24576', LOGIN: '1075410852'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'

```



```
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: changem1'
Processing CSTP header line: 'X-CSTP-Hostname: changem1'
Setting hostname to: 'changem1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1406'
Processing CSTP header line: 'X-CSTP-MTU: 1406'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret:
AD9F29FCBB9A377D9EC677B49948B78A342BF2DE7F950FD9D0775A4A8F43D4FE3F43A8BBF41C97959A0AE8B
CB618678E'
Processing CSTP header line: 'X-DTLS-Master-Secret:
AD9F29FCBB9A377D9EC677B49948B78A342BF2DE7F950FD9D0775A4A8F43D4FE3F43A8BBF41C97959A0AE8B
CB618678E'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-
SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.15.1/255.255.255.0
CSTP state = HAVE_ADDRESS
SVC: NP setup
np_svc_create_session(0x6000, 0xa92b1640, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

```
CSTP state = CONNECTED
%ASA-6-725001: Starting SSL handshake with client outside:100.2.2.22/1077 for DTLSv1
session.
%ASA-6-725003: SSL client outside:100.2.2.22/1077 request to resume previous session.
%ASA-6-725002: Device completed SSL handshake with client outside:100.2.2.22/1077
%ASA-5-722033: Group <CCIE> User <ccie> IP <100.2.2.22> First UDP SVC connection
established for SVC session.
%ASA-6-722022: Group <CCIE> User <ccie> IP <100.2.2.22> UDP SVC connection established
without compression
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

Task 2

Configure AnyConnect so that you can ping R1's loopback IP address (only ICMP is allowed) and you can TELNET only to R1's f0/0 IP address. All user traffic should go to the VPN tunnel and should be able to reach all internal hosts. Configure Login Message for the users with a text of 'Welcome to the Micronics Training network! Please behave.'

Do not configure any dynamic routing protocol to accomplish this task.

Configuration

Complete these steps:

Step 1 ASA configuration.

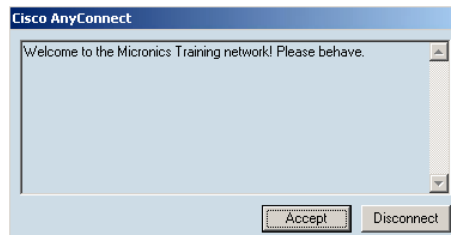
```
ASA84(config)# access-list CCIE-FILTER permit icmp any host 1.1.1.1
ASA84(config)# access-list CCIE-FILTER permit tcp any host 10.1.1.1
eq 23

ASA84(config)# group-policy CCIE attributes
ASA84(config-group-policy)# vpn-filter value CCIE-FILTER
ASA84(config-group-policy)# banner value Welcome to the Micronics
Training network! Please behave.
ASA84(config-group-policy)# exit

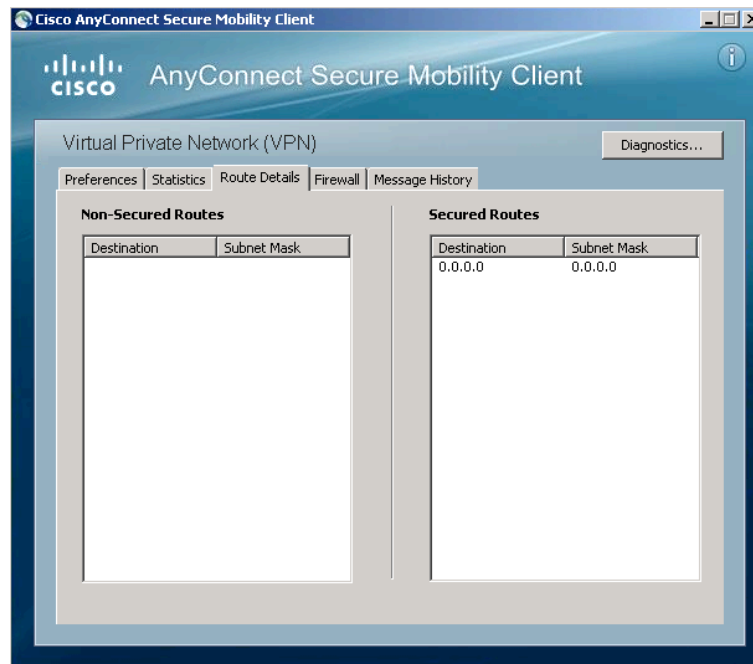
ASA84(config)# route inside 0 0 10.1.1.1 tunneled
```

Verification

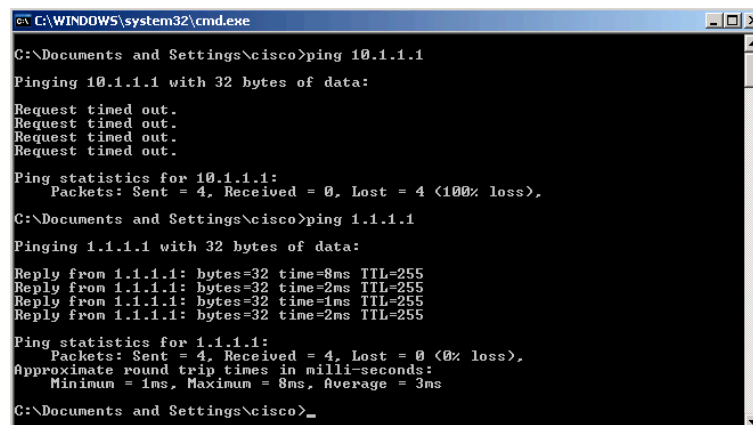
```
// Banner message is displayed.
```



// All user traffic is going through the tunnel



// can ping 1.1.1.1, cannot ping 10.1.1.1



// can telnet to 10.1.1.1

```

c:\Telnet 10.1.1.1

User Access Verification
Password:
R1>sh users
      Line          User           Host(s)           Idle           Location
  *514 vty 0
      idle
      idle
      00:00:00 192.168.15.1
      Interface  User           Mode           Idle           Peer Address
R1>_

```

ASA84(config)# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

```

Username       : ccie                      Index          : 9
Assigned IP    : 192.168.15.1              Public IP       : 100.2.2.22
Protocol       : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License        : AnyConnect Premium
Encryption     : RC4 AES128                Hashing         : none SHA1
Bytes Tx       : 10910                     Bytes Rx        : 4860
Group Policy   : CCIE                      Tunnel Group    : CCIE
Login Time     : 22:32:19 UTC Thu Jan 29 2004
Duration       : 0h:04m:27s
Inactivity     : 0h:00m:00s
NAC Result     : Unknown
VLAN Mapping   : N/A                      VLAN            : none

```

ASA84(config)# sh uauth

```

Current      Most Seen
Authenticated Users      1          1
Authen In Progress      0          0
remote access VPN user 'ccie' at 192.168.15.1, authenticated
access-list CCIE-FILTER (*)

```

Task 3

Configure ASA device so that all internal users (behind ASA's Inside interface) are able to reach the Internet by translating their IP addresses to the ASA's Outside IP address.

Configure the AnyConnect client so that the user can ping it's local network devices (i.e. 100.2.2.2). Do not brake any previous tasks.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA84(config)# object network ANYNET
ASA84(config-network-object)# subnet 0.0.0.0 0.0.0.0
ASA84(config-network-object)# nat (inside,outside) dynamic
interface
ASA84(config-network-object)# exi
```

Note that after configuring this, all Inside traffic will be translated when going out through Outside interface. Also, traffic returning to the AnyConnect VPN user. You must exclude VPN traffic from translation.

Note the following SYSLOG message indicating the issue:
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for tcp src outside:192.168.15.1/1139(LOCAL\ccie) dst inside:10.1.1.1/23 denied due to NAT reverse path failure

```
ASA84(config)# object network VPN-POOL
ASA84(config-network-object)# subnet 192.168.15.0 255.255.255.0
ASA84(config-network-object)# exi
```

```
ASA84(config)# nat (inside,outside) source static ANYNET ANYNET
destination static VPN-POOL VPN-POOL
```

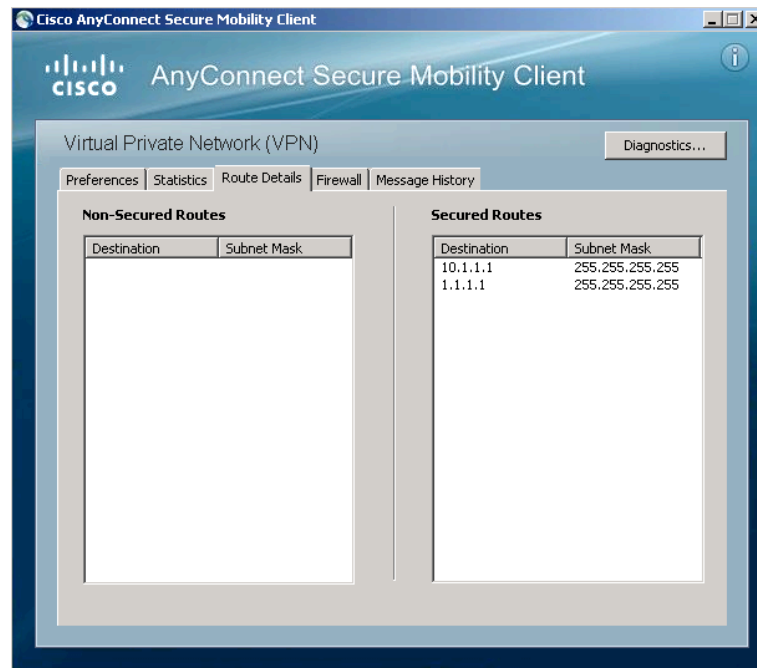
Now, we can connect to to network behind the ASA as returning traffic is NOT subjected to the NAT. but, still cannot ping IPs in local subnet. To make it work we need to configure Split Tunneling feature for AnyConnect.

```
ASA84(config)# access-list ST standard permit host 10.1.1.1
ASA84(config)# access-list ST standard permit host 1.1.1.1

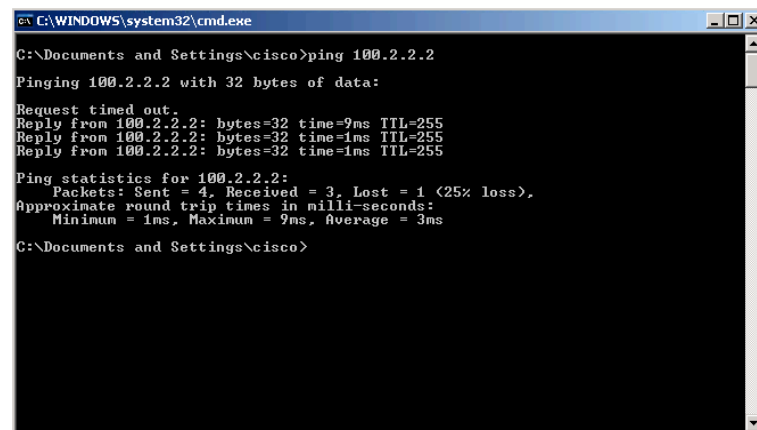
ASA84(config)# group-policy CCIE attributes
ASA84(config-group-policy)# split-tunnel-network-list value ST
ASA84(config-group-policy)# split-tunnel-policy tunnelspecified
ASA84(config-group-policy)# exi
```

Verification

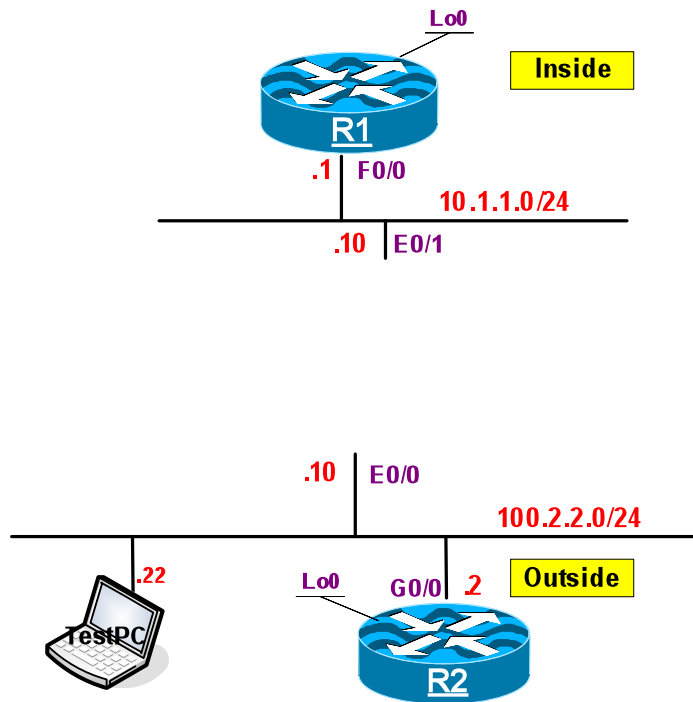
```
// reconnect to the ASA and check AnyConnect routing table
```



// try to ping local IP address



Lab 1.66. AnyConnect 3.0 Advanced Features



Lab Setup

- R1's F0/0 and ASA84 E0/1 interface should be configured in VLAN 10
- R2's G0/0 and ASA84 E0/0 interface should be configured in VLAN 20
- Configure Telnet on all routers using password "cisco"
- Configure default routes on R1/R2 to point to ASA and static routes to reach router's loopbacks

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/24
	F0/0	10.1.11.1/24
R2	Lo0	2.2.2.2/24
	G0/0	100.2.2.2/24

PC	NIC	100.2.2.22/24
ASA84	E0/0	100.2.2.10/24
	E0/1	10.1.1.10/24

Before you start

This lab is based on the previous configuration. Do not erase the config!

Task 1

Configure DNS and DHCP Server on R1 and R2 for their local networks as follows:

```

!                                     !
ip dhcp pool VLAN10                 ip dhcp pool VLAN20
  network 10.1.1.0 /24                network 100.2.2.0 /24
  domain-name cisco.local            domain-name cisco.com
  default-router 10.1.1.10           default-router 100.2.2.10
  dns-server 10.1.1.1                dns-server 100.2.2.2
!                                     !
ip domain lookup                     ip domain lookup
ip domain name cisco.local           ip domain name cisco.com
ip host asa84.cisco.com 100.2.2.10  ip host asa84.cisco.com 100.2.2.10
ip dns server                         ip dns server
!                                     !

```

Reconfigure WinXP PC to assign IP address automatically.

Generate self-signed Identity Certificate for ASA with the following Subject Name:

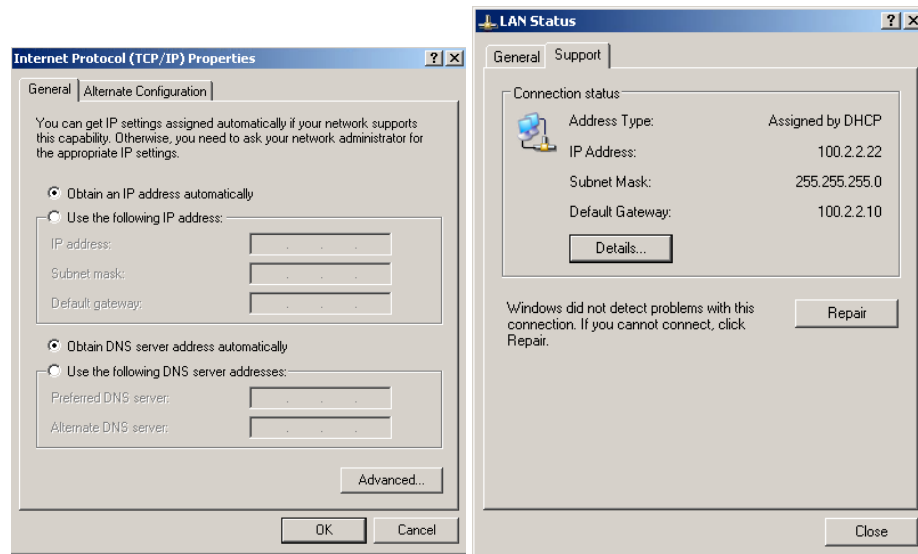
- Common Name=asa84.cisco.com
- Organization=Cisco
- Organizational Unit=CCIE

Use that newly created certificate for SSL. Configure AnyConnect 3.0 so that the user cannot disconnect the VPN tunnel and the AnyConnect automatically tries to connect to the ASA headend whenever it is in Outside network (behind ASA's Outside interface, VLAN 20). You can use DNS/DHCP Servers configured on R1 and R2 to accomplish this task. Use WinXP PC as a management station. Create administrator account with the credentials of admin/admin123.

Configuration

Complete these steps:

- Step 1** Configure interface on client PC to obtain an IP address from DHCP.



- Step 2** ASA CLI configuration.

To configure advanced Anyconnect Features like Always-On or customize user experience of AnyConnect Client you must use ASDM and Profile Editor.

First generate keys and create Identity Certificate for SSL

```
ASA84(config)# crypto key generate rsa label KEYS modulus 1024
<key generation process omitted>

ASA84(config)# crypto ca trustpoint SSL-TRUST
ASA84(config-ca-trustpoint)# enrollment self
ASA84(config-ca-trustpoint)# subject-name
CN=asa84.cisco.com,OU=ccie,O=cisco
ASA84(config-ca-trustpoint)# keypair KEYS

ASA84(config)# crypto ca enroll SSL-TRUST
<enrollment process omitted>

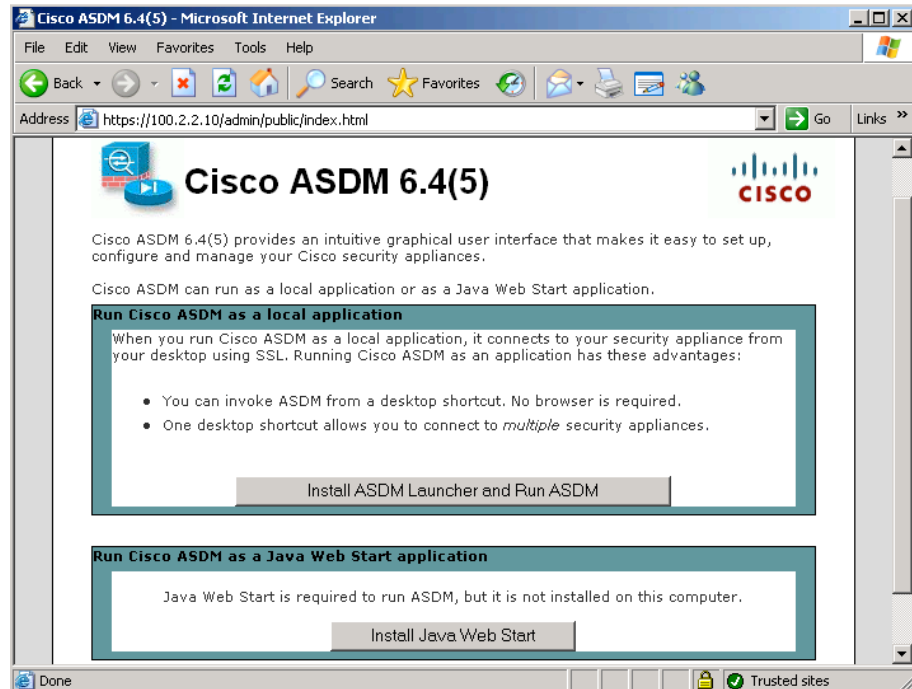
ASA84(config)# ssl trust-point SSL-TRUST
```

You must then configure ASDM access.

```
ASA84(config)# http server enable
ASA84(config)# http 100.2.2.22 255.255.255.255 outside
ASA84(config)# username admin password admin123 priv 15
```

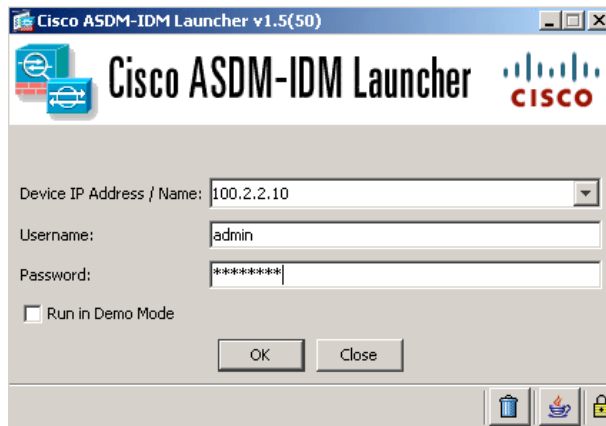
Step 3 ASA ASDM configuration.

Go to <https://100.2.2.10/admin>

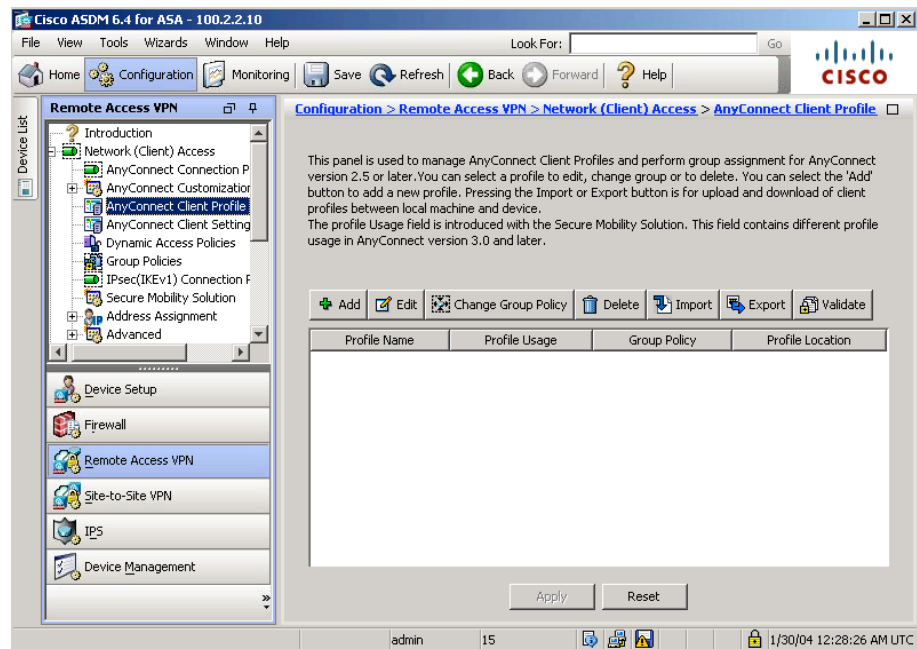


Click on *Install ASDM Launcher and Run ASDM*, authenticate as admin and run installer.



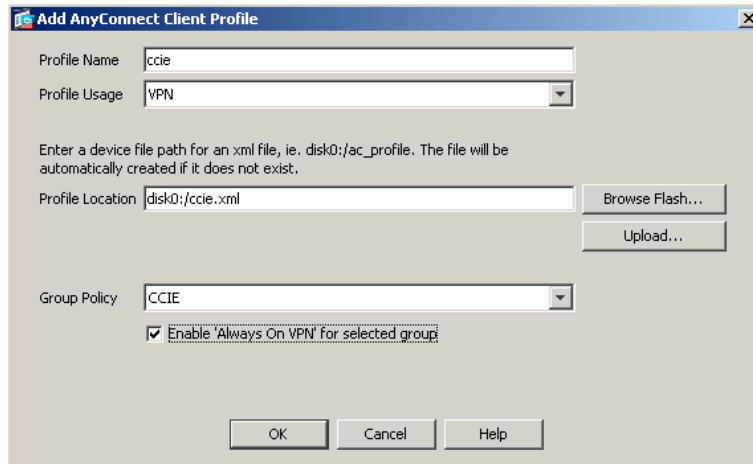


**Go to Configuration --> Remote Access VPN --> AnyConnect Client Profile.
Click Add button and create new profile.**



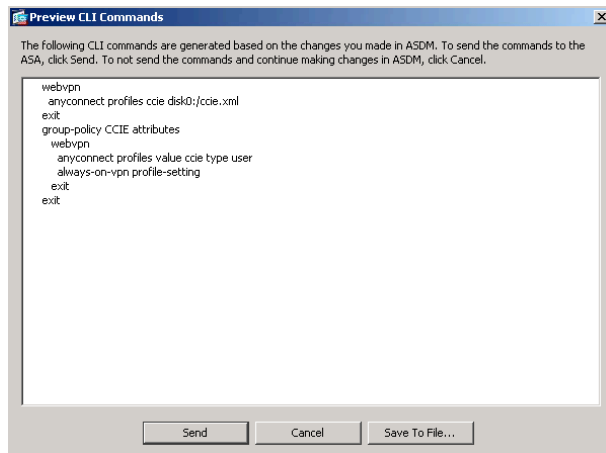
Name the new profile 'ccie' and assign it to the group CCIE. Check the option to enable Always ON VPN feature.

Note that ASDM has a very nice feature that shows all commands generated by the ASDM and send to the ASA device. Using this you can see what commands are required on CLI to configure a particular feature. To enable command preview go to Tools --> Preferences and check 'Preview commands before sending them to the device' option.



The 'Add AnyConnect Client Profile' dialog box is shown. It has a title bar with a close button. The 'Profile Name' field contains 'ccie'. The 'Profile Usage' dropdown is set to 'VPN'. Below these fields is a text instruction: 'Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.' The 'Profile Location' field contains 'disk0:/ccie.xml'. To the right of this field are two buttons: 'Browse Flash...' and 'Upload...'. Below the 'Profile Location' field is a 'Group Policy' dropdown set to 'CCIE'. Underneath the dropdown is a checked checkbox labeled 'Enable 'Always On VPN' for selected group'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Click OK and then Apply. You should see commands preview if this option is enabled. Click Send button.



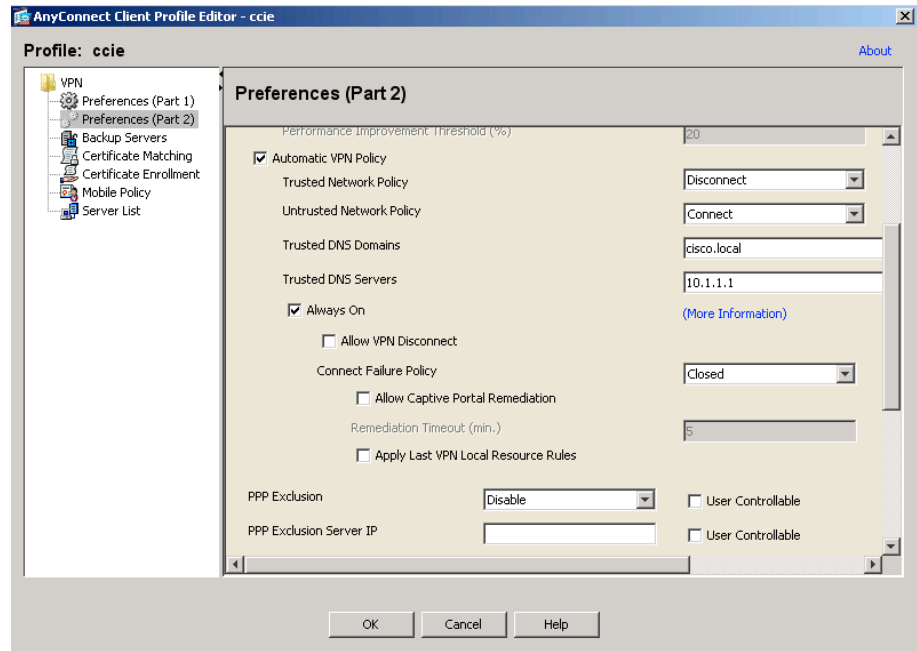
The 'Preview CLI Commands' dialog box is shown. It has a title bar with a close button. The main area contains a text box with the following CLI commands:

```
webvpn
 anyconnect profiles ccie disk0:/ccie.xml
exit
group-policy CCIE attributes
 webvpn
  anyconnect profiles value ccie type user
  always-on-vpn profile-setting
exit
exit
```

Below the text box are three buttons: 'Send', 'Cancel', and 'Save To File...'. Above the text box is a small text block: 'The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.'

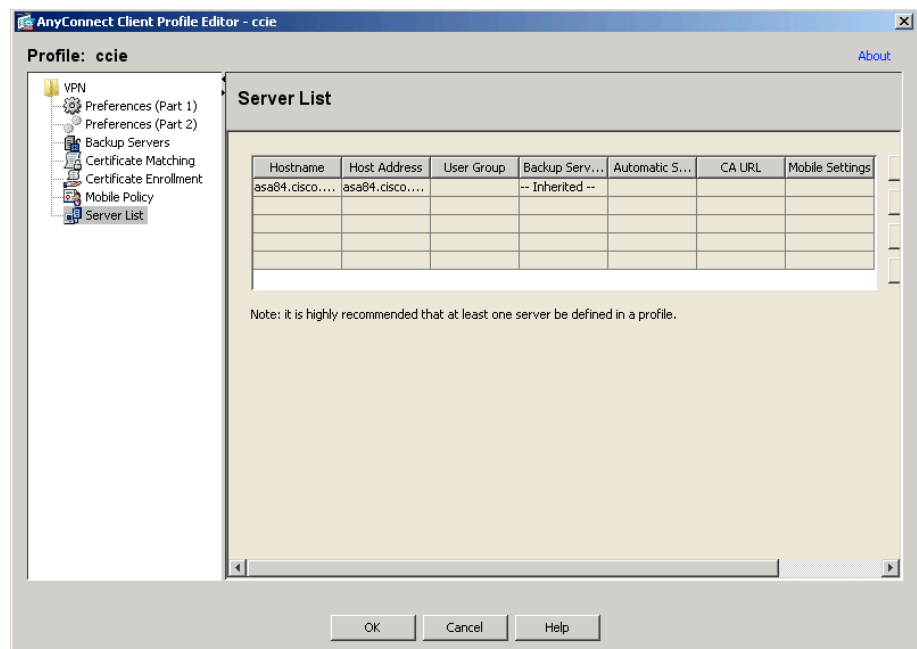
Click on Edit button to configure AC3 Profile and go to Preferences (Part 2) section. Configure it as follows:

- **Check Automatic VPN Policy**
 - **Trusted Network Policy = Disconnect**
 - **Untrusted Network Policy = Connect**
 - **Trusted DNS Domains = cisco.local**
 - **Trusted DNS Servers = 10.1.1.1**
- **Check Always On**
 - **Uncheck Allow VPN Disconnect**



Go to Server List and Add new server with the following information:

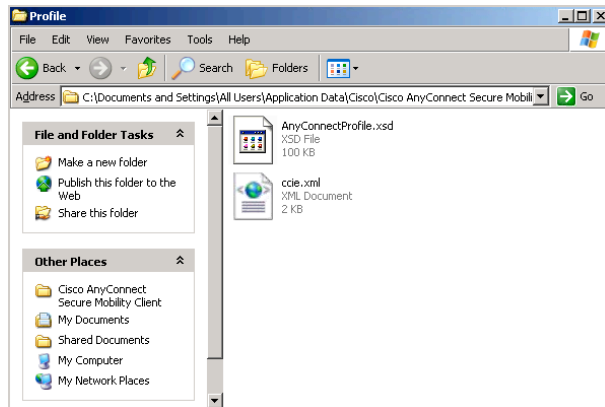
- **Host Display Name (required) = asa84.cisco.com**
- **FQDN or IP Address = asa84.cisco.com**



Click OK and then Apply the settings.

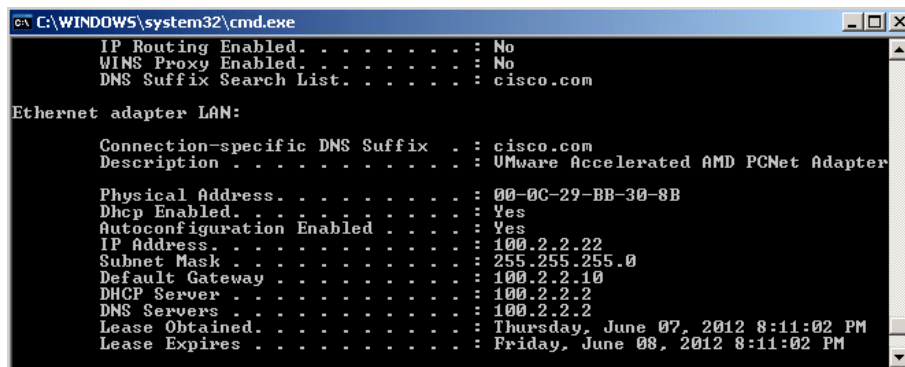
Now when connecting to the ASA headend, the Anyconnect Client will download the Profile config file (ccie.xml) to the client and apply all options configured on it.

The profile is stored on Windows XP in the folder C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

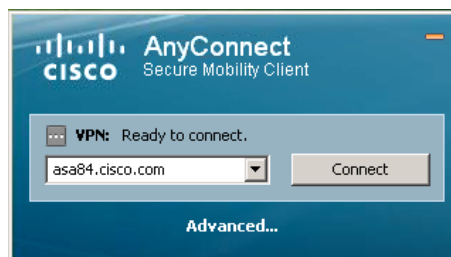


Verification

Now go to the WinXP PC and connect to `asa84.cisco.com` (the FQDN should be resolved against R2 DNS server).



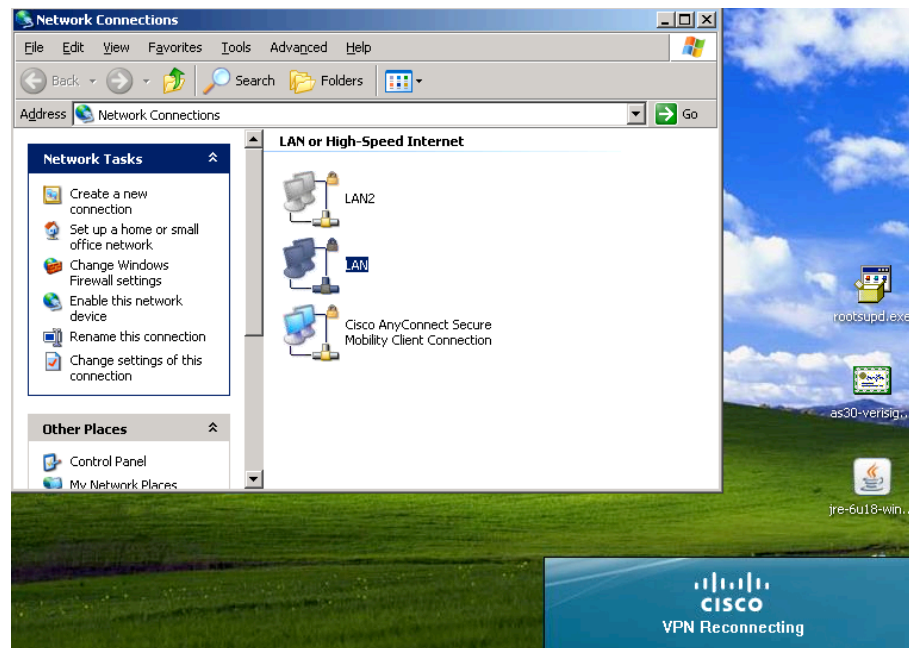
Note that the host is in domain `cisco.com` and DNS server is R2.



Note that after connecting the Disconnect button is greyed out.

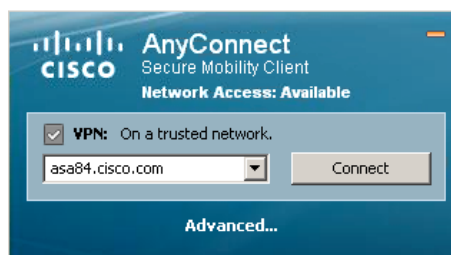


Let's make a test. Now the WinXP PC is in VLAN20 and gets all network settings from R2. Try to disable NIC and reassign the switchport to VLAN 10 and re-enable NIC.



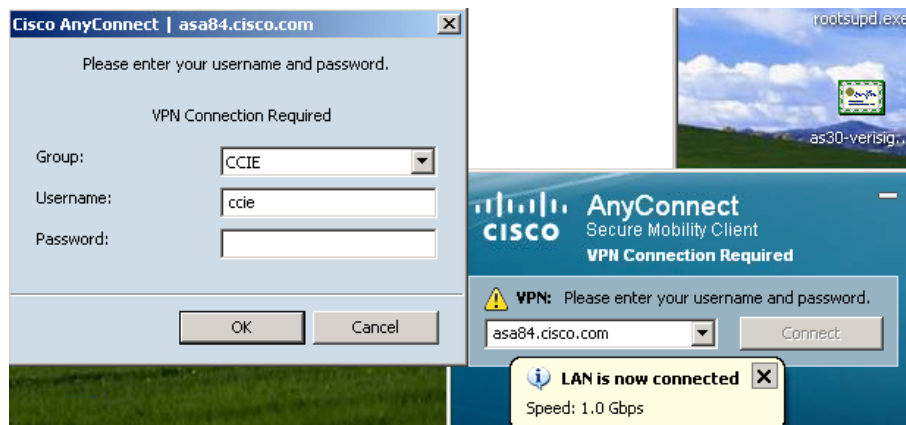
Note that the AC3 tries to reconnect automatically.
Change the VLAN assignment.
Re-enable NIC.

```
SW3(config)#int g1/0/15  
SW3(config-if)#sw acc vl 10
```



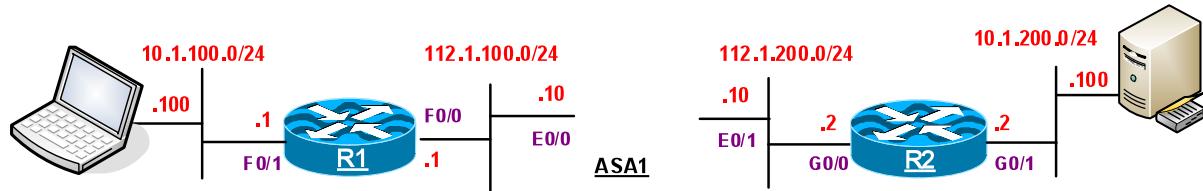
After a while the AC3 realized based on DNS settings that it is now in Trusted Network and there is no need for VPN setup. This feature is called TND - Trusted Network Detection.

Let's revert to correct VLAN (20). Disable NIC, change VLAN on port, Enable NIC,



The AC3 automatically reconnect to the ASA.

Lab 1.67. EasyVPN Server on ASA with LDAP authentication



Lab Setup

- R1's F0/0 and ASA1's E0/0 interface should be configured in VLAN 110
- R2's G0/0 and ASA1's E0/1 interface should be configured in VLAN 120
- R1's F0/1 and VPN Client PC (SW3 – F0/15) should be in VLAN 100
- R2's G0/1 and ACS server (SW3 – F0/14) should be in VLAN 200
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R1 and R2 pointing to the ASA

IP Addressing

Device	Interface	IP address
R1	F0/0	112.1.100.1/24
	F0/1	10.1.100.1/24
ASA1	E0/0	112.1.100.10/24
	E0/1	112.1.200.10/24
R2	G0/0	112.1.200.2/24
	G0/1	10.1.200.2/24
PC	NIC	10.1.100.100/24
ACS	NIC	10.1.200.100/24

Task 1

Configure EasyVPN Server on ASA and authenticate user "student" with a password of "cisco123!" to LDAP server (Microsoft AD) configured on the ACS server.

Configure LDAP mapping so that Active Directory user's "Dial in" permission ("msNPAllowDialin" LDAP attribute) will affect Simultaneous-Logins ASA EasyVPN parameter. If AD user has no dial in permission (FALSE) set the Simultaneous-Logins to 0, if he/she has dial in permission (TRUE) set the Simultaneous-Logins to 1.

1. Active Directory connection properties:

- Server IP: 10.1.200.100
- LDAP DN: micronictstraining.com
- LDAP administrator name/password: Administrator/cisco123!
- LDAP user container name: Users
- Domain name: micronictstraining.com

Use the following ISAKMP parameters:

- Phase 1:
 - Authentication: PSK
 - Encryption: 3DES
 - Hashing: MD5
 - Group: 2
- Phase 2:
 - Encryption: 3DES
 - Hashing: MD5

The user should get an IP address from a pool of 10.1.21.1 – 10.1.21.254 addresses. Configure RIP version 2 between ASA1 and R2 and make sure the correct route back to VPN Client is injected to R2's routing table.

EasyVPN group named "SALES" with a password of "cisco123" should be configured on the ASA. The group should use internal policy so that it assigns an IP address from the pool and tells the VPN client to encrypt traffic to the network 10.1.200.0/24 only.

Configure TestPC with software VPN Client to connect to the EasyVPN server.



An EasyVPN user can be authenticates against different user databases. One of the most popular user dB is an LDAP database. The most common LDAP database is Microsoft's Active Directory which is often used by the companies. The Active Directory stores a lot of different user attributes so that we can use

them in EasyVPN scenario.

For example, each AD user has Dial In permission configured. This defines if the particular user may or may not Dial In to the network. We can use that attribute in our policy.

The ASA has native LDAP support – this means it can directly contact LDAP server and ask for user properties. In the previous versions of the ASA there must be ACS server configured with external LDAP database to make it happen. The LDAP database has its own structure so we need to know that structure to find appropriate fields and values in the database.

Another thing is how to connect to the LDAP database? The structure of the LDAP database is like a X.509 certificate. A user account is often described like DN from the certificate. For example:

CN=User1,CN=IT,DC=micronicstraining.com,DC=com means that there is a user named “User1” with an Organizational Unit container named “IT” in the Active Directory database for a domain of “micronicstraining.com”.

EasyVPN config mode attributes are incompatible with LDAP attributes. To be able to use LDAP user attributes, we need to map those attributes to the EasyVPN attributes.

Configuration

Complete these steps:

Step 1 ASA configuration.

```
ASA(config)# crypto isakmp enable outside
ASA(config)# crypto isakmp policy 10
ASA(config-isakmp-policy)# auth pre-share
ASA(config-isakmp-policy)# encr 3des
ASA(config-isakmp-policy)# hash md5
ASA(config-isakmp-policy)# group 2
ASA(config-isakmp-policy)# exi

ASA(config)# ip local pool EZVPN-POOL 10.1.21.1-10.1.21.254

ASA(config)# access-list ST standard permit 10.1.200.0
255.255.255.0

ASA(config)# ldap attribute-map LDAP-MAP
ASA(config-ldap-attribute-map)# map-name msNPAllowDialin
Simultaneous-Logins
ASA(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 0
ASA(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 1
ASA(config-ldap-attribute-map)# exi
```

We need to map LDAP attributes to the corresponding EasyVPN attributes. In this example we're mapping LDAP attribute named "msNPAllowDialin" to the EasyVPN attribute named Simultaneous-Logins. This EasyVPN attribute is responsible for configuring how many simultaneous logins can be accepted by the ASA for a particular group/user. As we know that the "msNPAllowDialin" attribute can have a value of TRUE or FALSE, we can decide a number of simultaneous logins for each of these values.

```
ASA(config)# aaa-server LDAP-SVR protocol ldap
ASA(config-aaa-server-group)# aaa-server LDAP-SVR (inside) host
10.1.200.100
ASA(config-aaa-server-host)# ldap-base-dn
DC=micronicstraining,DC=com
ASA(config-aaa-server-host)# ldap-scope subtree
ASA(config-aaa-server-host)# ldap-login-dn
CN=Administrator,CN=Users,DC=micronicstraining,DC=com
ASA(config-aaa-server-host)# ldap-login-password cisco123!
ASA(config-aaa-server-host)# server-type microsoft
ASA(config-aaa-server-host)# ldap-attribute-map LDAP-MAP
ASA(config-aaa-server-host)# exit
```

The LDAP server access is configured on the ASA as for any other AAA server. This time the protocol used is not RADIUS/TACACS+ but LDAP. The authentication for that server must be provided using DN notation. We need to assign LDAP mapping configured previously to the LDAP server.

```
ASA(config)# group-policy SALES-POLICY internal
ASA(config)# group-policy SALES-POLICY attributes
ASA(config-group-policy)# vpn-tunnel-protocol IPSec
ASA(config-group-policy)# address-pools value EZVPN-POOL
ASA(config-group-policy)# split-tunnel-policy tunnelspecified
ASA(config-group-policy)# split-tunnel-network-list value ST
ASA(config-group-policy)# exit
```

```
ASA(config)# tunnel-group SALES type remote-access
ASA(config)# tunnel-group SALES general-attributes
ASA(config-tunnel-general)# authentication-server-group LDAP-SVR
ASA(config-tunnel-general)# default-group-policy SALES-POLICY
```

Under the tunnel group we need to specify our LDAP server as an authentication method for users.

```
ASA(config-tunnel-general)# tunnel-group SALES ipsec-attributes
ASA(config-tunnel-ipsec)# pre-shared-key cisco123
ASA(config-tunnel-ipsec)# exit
```

```
ASA(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

```
ASA(config)# crypto dynamic-map DYN-CMAP 10 set transform-set TS
ASA(config)# crypto dynamic-map DYN-CMAP 10 set reverse-route

ASA(config)# crypto map Ezee 100 ipsec-isakmp dynamic DYN-CMAP

ASA(config)# crypto map Ezee interface outside

ASA(config)# route outside 0 0 112.1.100.1
ASA(config)# route inside 10.1.200.0 255.255.255.0 112.1.200.2

ASA(config)# router rip
ASA(config-router)# ver 2
ASA(config-router)# no aut
ASA(config-router)# passive-interface default
ASA(config-router)# no passive-interface inside
ASA(config-router)# network 112.0.0.0
ASA(config-router)# redistribute static
ASA(config-router)# exi
```

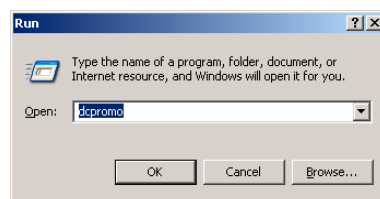
Step 2 R2 configuration.

```
R2(config)#router rip
R2(config-router)#ver 2
R2(config-router)#no aut
R2(config-router)#net 112.0.0.0
R2(config-router)#exi
```

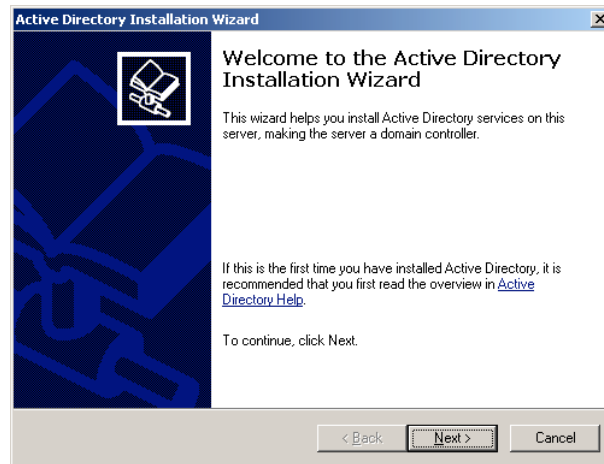
Step 3 Optionally install Actice Diectory as an LDAP server. (optional)

These steps are optional and depend on your Active Directory existence and configuration.

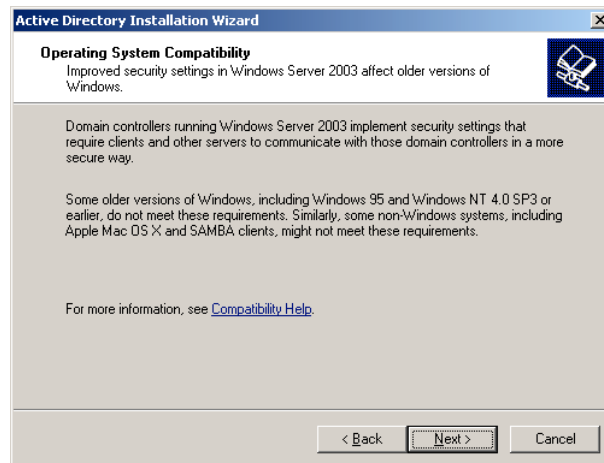
Install and pre-configure Active Directory on the ACS server by running “dcpromo” command.



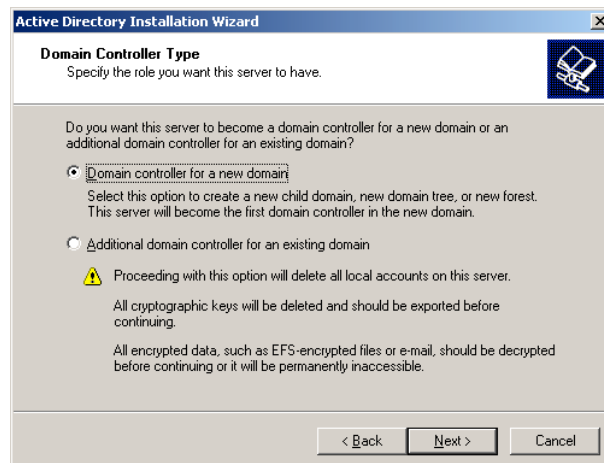
The configuration wizard will run. Hit the Next button.



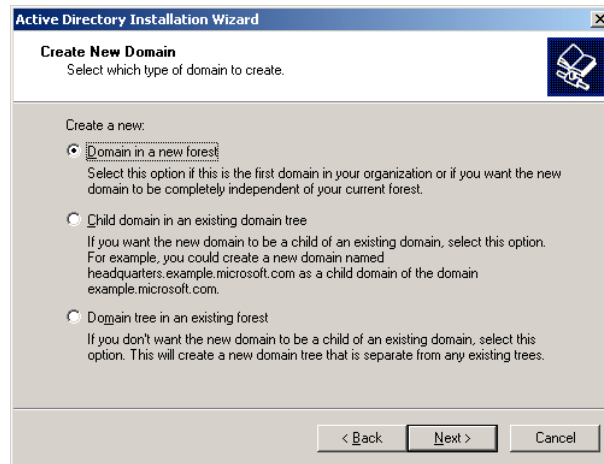
Hit the Next button again.



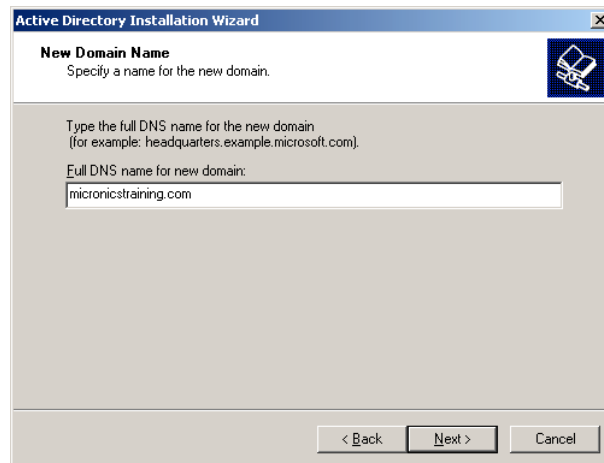
Select "Domain controller for a new domain" and hit Next.



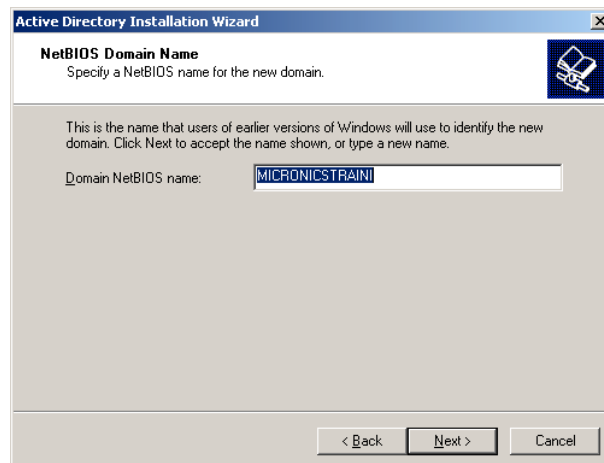
Select "Domain in a new forest" and hit Next.



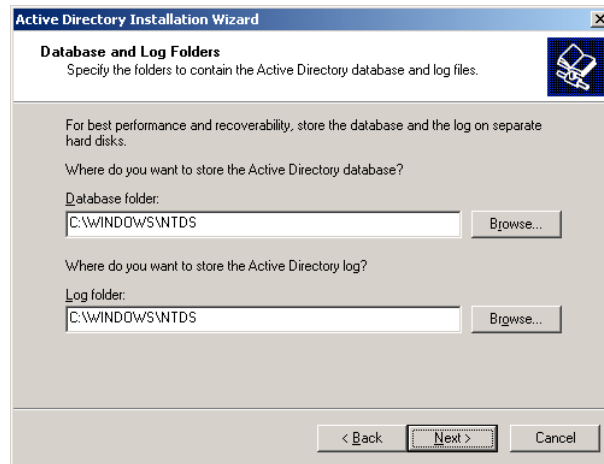
Enter “micronicstraining.com” as a name for a new domain and hit Next.



Leave a default name for NetBIOS domain name. Hit Next.



Leave a default setting for paths. Hit Next.



Active Directory Installation Wizard

Database and Log Folders
Specify the folders to contain the Active Directory database and log files.

For best performance and recoverability, store the database and the log on separate hard disks.

Where do you want to store the Active Directory database?

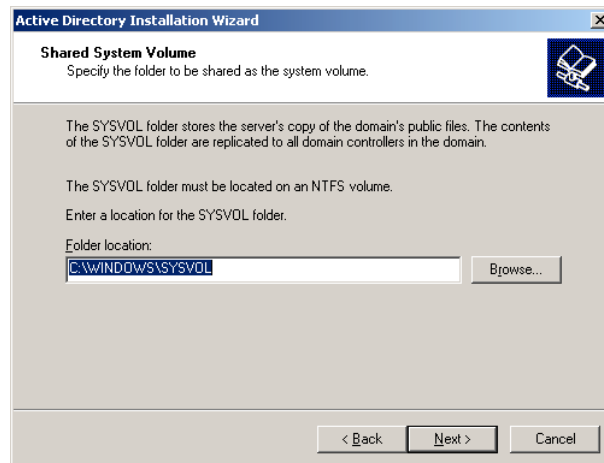
Database folder:
C:\WINDOWS\NTDS Browse...

Where do you want to store the Active Directory log?

Log folder:
C:\WINDOWS\NTDS Browse...

< Back Next > Cancel

Leave a default path for SYSVOL folder. Hit Next.



Active Directory Installation Wizard

Shared System Volume
Specify the folder to be shared as the system volume.

The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.

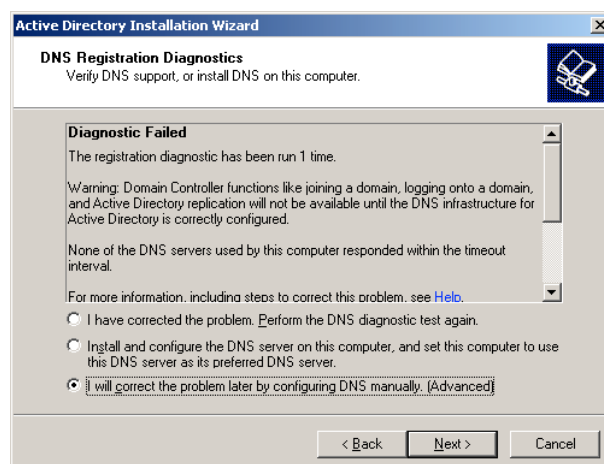
The SYSVOL folder must be located on an NTFS volume.

Enter a location for the SYSVOL folder.

Folder location:
C:\WINDOWS\SYSVOL Browse...

< Back Next > Cancel

This step can be a bit different depending on your DNS configuration. Select option to NOT configure DNS. Hit Next.



Active Directory Installation Wizard

DNS Registration Diagnostics
Verify DNS support, or install DNS on this computer.

Diagnostic Failed
The registration diagnostic has been run 1 time.

Warning: Domain Controller functions like joining a domain, logging onto a domain, and Active Directory replication will not be available until the DNS infrastructure for Active Directory is correctly configured.

None of the DNS servers used by this computer responded within the timeout interval.

For more information, including steps to correct this problem, see [Help](#).

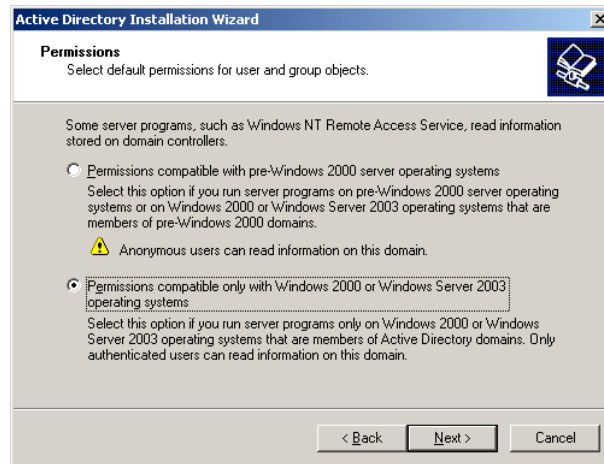
☐ I have corrected the problem. Perform the DNS diagnostic test again.

☐ Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.

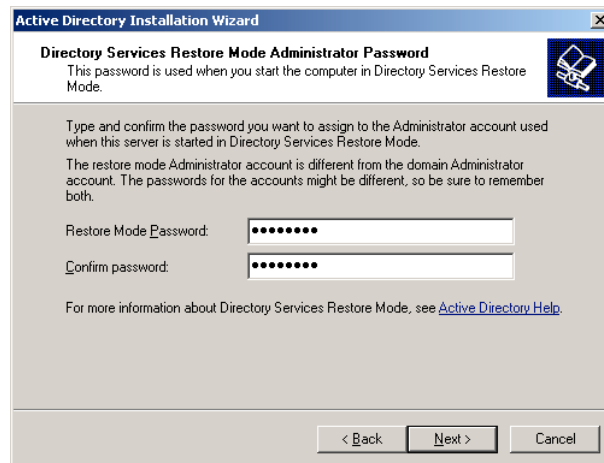
☒ I will correct the problem later by configuring DNS manually. (Advanced)

< Back Next > Cancel

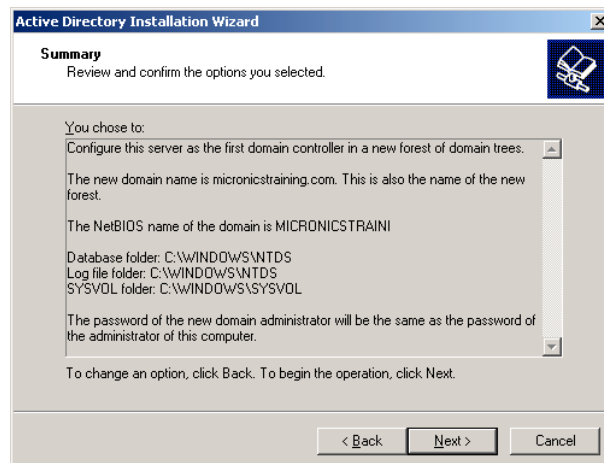
Select permissions compatible with Windows 2000 and Windows 2003. Hit Next.



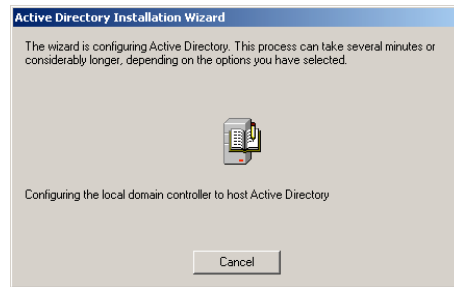
Enter some password for AD restore mode. Hit Next.



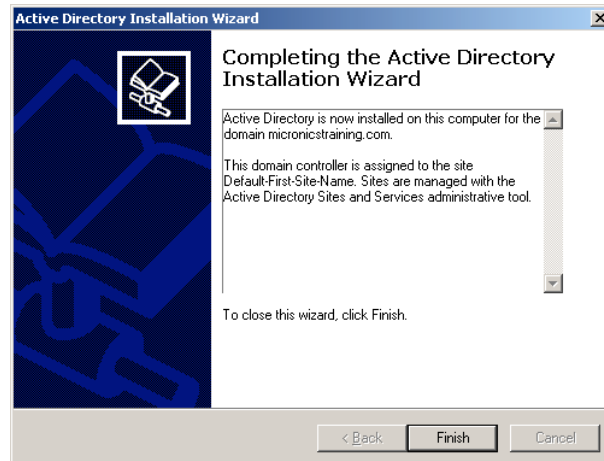
Hit Next on summary page.



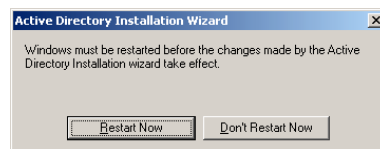
The wizard is finished and is installing and configuring Active Directory. It may take some time. Be patient.



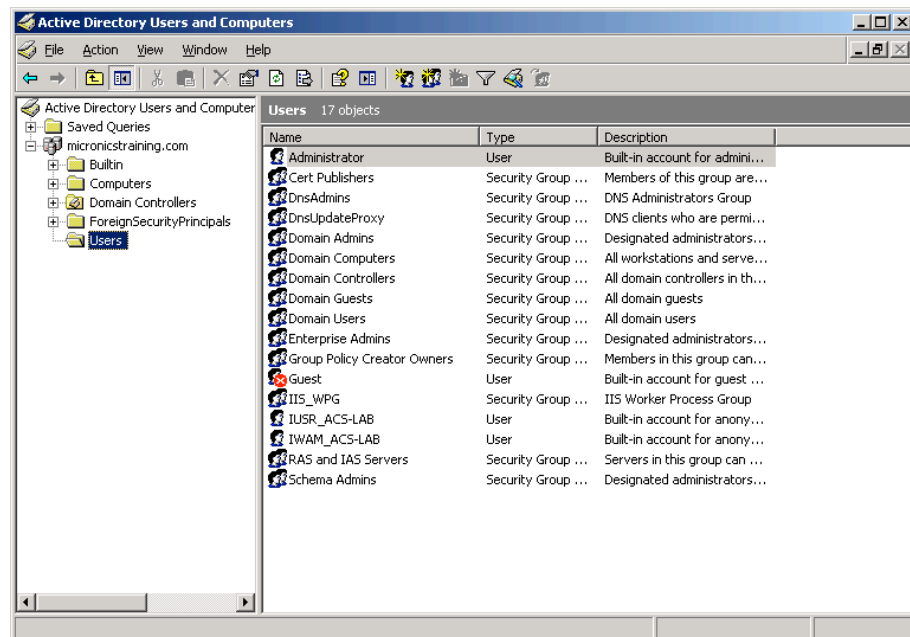
It displays some summary upon completing the task. Hit Finish.



The system must be restarted after AD installation.



After restarting the system, go to Start → Administrative Tools → AD Users and Computers and select Users container.



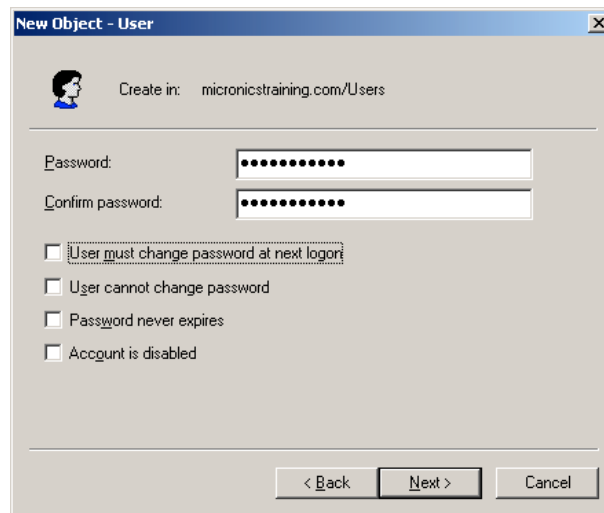
Click on “Create a new user in the current container” icon and enter the following settings for a “student” user.

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'micronicstraining.com/Users'. The fields are filled with the following information:

Field	Value
First name	student
Initials	
Last name	
Full name	student
User logon name	student
Domain (dropdown)	@micronicstraining.com
User logon name (pre-Windows 2000)	MICRONICSTRAINI\student

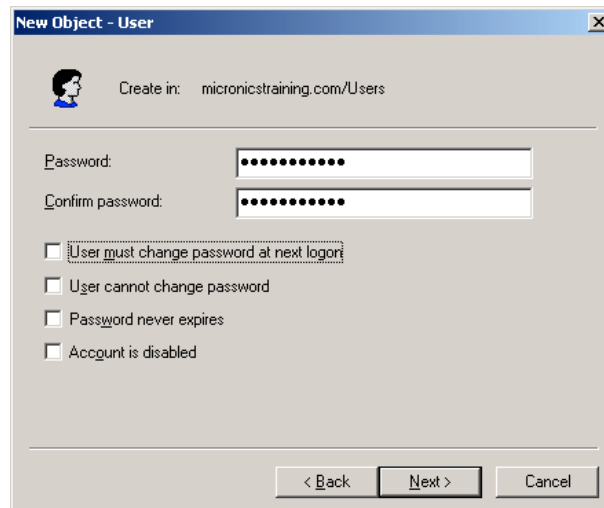
At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

Enter password of “student123!” for the user. And hit Next.



The image shows a Windows-style dialog box titled "New Object - User". At the top, it says "Create in: micronitraining.com/Users". Below this, there are two password fields: "Password:" and "Confirm password:", both containing ten dots. Underneath the password fields are four unchecked checkboxes with the following labels: "User must change password at next login", "User cannot change password", "Password never expires", and "Account is disabled". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Click finish to create new user.



This image is identical to the one above, showing the "New Object - User" dialog box. It contains the same fields for password creation and selection of user properties, with the "Next >" button highlighted.

Double click the new user and go to Dial-in tab. Select Allow access option and hit OK.

student Properties

Remote control | Terminal Services Profile | CDM+
 General | Address | Account | Profile | Telephones | Organization
 Member Of | Dial-in | Environment | Sessions

Remote Access Permission (Dial-in or VPN)

☒ Allow access
☐ Deny access
☐ Control access through Remote Access Policy

☐ Verify Caller ID:

Callback Options

☒ No Callback
☐ Set by Caller (Routing and Remote Access Service only)
☐ Always Callback to:

☐ Assign a Static IP Address:

☐ Apply Static Routes:

Define routes to enable for this Dial-in connection.

Verification

Go to TestPC and configure new connection to the EasyVPN Server.

VPN Client - Create New VPN Connection Entry

Connection Entry: ASA EasyVPN LDAP

Description:

Host: 112.1.100.10

Authentication | Transport | Backup Servers | Dial-Up

☒ Group Authentication ☐ Mutual Group Authentication

Name: SALES

Password:

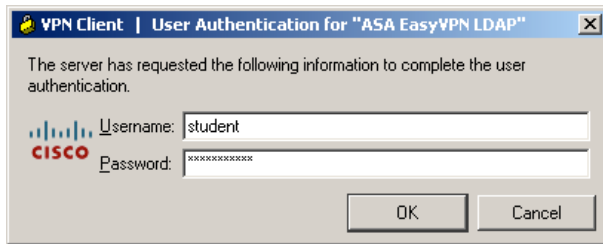
Confirm Password:

☐ Certificate Authentication

Name:

☐ Send CA Certificate Chain

Authenticate using “student” user credentials.



Ping R2 to see if the traffic goes through the tunnel.

C:\>ping 112.1.200.2

Pinging 112.1.200.2 with 32 bytes of data:

Reply from 112.1.200.2: bytes=32 time=110ms TTL=255

Reply from 112.1.200.2: bytes=32 time=64ms TTL=255

Reply from 112.1.200.2: bytes=32 time=127ms TTL=255

Reply from 112.1.200.2: bytes=32 time=140ms TTL=255

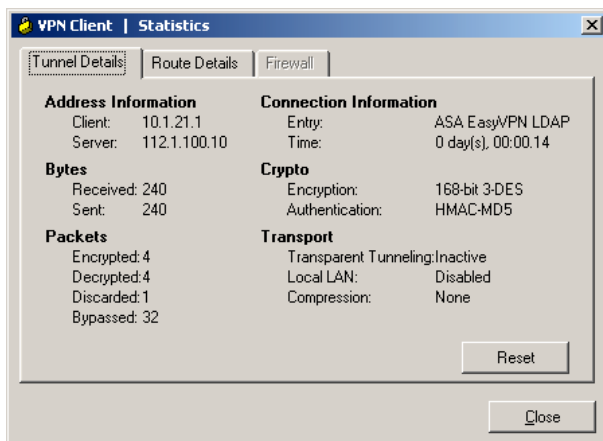
Ping statistics for 112.1.200.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

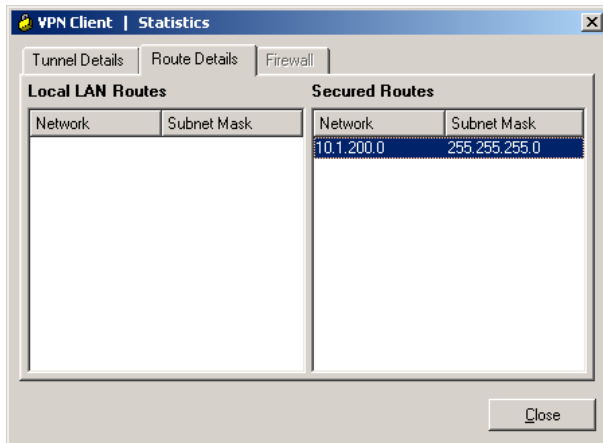
Approximate round trip times in milli-seconds:

Minimum = 64ms, Maximum = 140ms, Average = 110ms

See the Statistics after the connection.



See if there is a correct split tunneling configured.



ASA# sh cryp isak sa detail

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 10.1.100.100
   Type    : user          Role    : responder
   Rekey   : no           State   : AM_ACTIVE
   Encrypt : 3des         Hash    : MD5
   Auth    : preshared    Lifetime: 86400
   Lifetime Remaining: 86321
```

ASA# sh cry ips sa

```
interface: outside
Crypto map tag: DYN-CMAP, seq num: 10, local addr: 112.1.100.10

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.1.21.1/255.255.255.255/0/0)
current_peer: 10.1.100.100, username: student
dynamic allocated peer ip: 10.1.21.1

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

Packets are getting encrypted/decrypted by the ASA

local crypto endpt.: 112.1.100.10, remote crypto endpt.: 10.1.100.100

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 71387A50
```

```

inbound esp sas:
  spi: 0x082E7C0B (137264139)
    transform: esp-3des esp-md5-hmac no compression
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 20480, crypto-map: DYN-CMAP
    sa timing: remaining key lifetime (sec): 28720
    IV size: 8 bytes
    replay detection support: Y
Anti replay bitmap:
  0x00000000 0x0000001F
outbound esp sas:
  spi: 0x71387A50 (1899526736)
    transform: esp-3des esp-md5-hmac no compression
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 20480, crypto-map: DYN-CMAP
    sa timing: remaining key lifetime (sec): 28720
    IV size: 8 bytes
    replay detection support: Y
Anti replay bitmap:
  0x00000000 0x00000001

```

ASA# sh vpn-sessiondb remote

Session Type: IPsec

Username	: student	Index	: 5
Assigned IP	: 10.1.21.1	Public IP	: 10.1.100.100
Protocol	: IKE IPsec		
License	: IPsec		
Encryption	: 3DES	Hashing	: MD5
Bytes Tx	: 240	Bytes Rx	: 240
Group Policy	: SALES-POLICY	Tunnel Group	: SALES
Login Time	: 19:07:55 UTC Mon Jun 21 2010		
Duration	: 0h:01m:23s		
NAC Result	: Unknown		
VLAN Mapping	: N/A	VLAN	: none

The user has been authenticated against LDAP server and got attributes based on SALES-POLICY.

ASA# sh aaa-server protocol ldap

```

Server Group:    LDAP-SVR
Server Protocol: ldap
Server Address:  10.1.200.100
Server port:     0
Server status:   ACTIVE, Last transaction at unknown
Number of pending requests      0
Average round trip time         0ms
Number of authentication requests 7

```


Number of authorization requests	0
Number of accounting requests	0
Number of retransmissions	0
Number of accepts	4
Number of rejects	0
Number of challenges	0
Number of malformed responses	0
Number of bad authenticators	0
Number of timeouts	3
Number of unrecognized responses	0

The LDAP server is active and has been consulted for authentication.

ASA# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 112.1.100.1 to network 0.0.0.0

```
C    112.1.100.0 255.255.255.0 is directly connected, outside
C    112.1.200.0 255.255.255.0 is directly connected, inside
S    10.1.21.1 255.255.255.255 [1/0] via 112.1.100.1, outside
S    10.1.200.0 255.255.255.0 [1/0] via 112.1.200.2, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 112.1.100.1, outside
```

There is a static route in the ASA's routing table for the connected user.

ASA(config)# sh rip database

```
0.0.0.0 0.0.0.0    auto-summary
0.0.0.0 0.0.0.0    redistributed
    [1] via 0.0.0.0,
10.0.0.0 255.0.0.0    auto-summary
10.1.21.1 255.255.255.255 redistributed
    [1] via 0.0.0.0,
10.1.200.0 255.255.255.0 redistributed
    [1] via 0.0.0.0,
112.0.0.0 255.0.0.0    auto-summary
112.1.100.0 255.255.255.0    directly connected, Ethernet0
112.1.200.0 255.255.255.0    directly connected, Ethernet1
ASA(config)#
```

The static route has been redistributed into the RIP domain.

R2#sh ip rou

```
*Jun 21 22:04:44.167: %SYS-5-CONFIG_I: Configured from console by console
R2#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 112.1.200.10 to network 0.0.0.0

```
112.0.0.0/24 is subnetted, 2 subnets
R    112.1.100.0 [120/1] via 112.1.200.10, 00:00:04, GigabitEthernet0/0
C    112.1.200.0 is directly connected, GigabitEthernet0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    10.1.21.1/32 [120/1] via 112.1.200.10, 00:00:04, GigabitEthernet0/0
C    10.1.200.0/24 is directly connected, GigabitEthernet0/1
S*   0.0.0.0/0 [1/0] via 112.1.200.10
```

The prefix is visible on R2 now.

Verification (detailed)

ASA# sh deb

```
debug ldap enabled at level 9
debug crypto isakmp enabled at level 9
```

The first packet of Aggressive Mode contains group name. The connection is matching correct tunnel group.

```
Jun 21 19:07:54 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 849
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing SA payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing ke payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing ISA_KE payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing nonce payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing ID payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, Received xauth V6 VID
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, Received DPD VID
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, Received Fragmentation VID
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: False
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, Received NAT-Traversal ver 02 VID
```

```
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:07:54 [IKEv1 DEBUG]: IP = 10.1.100.100, Received Cisco Unity client VID
Jun 21 19:07:54 [IKEv1]: IP = 10.1.100.100, Connection landed on tunnel_group SALES
Jun 21 19:07:54 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing IKE SA
payload
Jun 21 19:07:54 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, IKE SA Proposal # 1,
Transform # 10 acceptable Matches global IKE entry # 1
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing ISAKMP SA
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing ke
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing nonce
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Generating keys for
Responder...
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing ID
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing hash
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Computing hash for
ISAKMP
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing Cisco
Unity VID payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing xauth V6
VID payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing dpd vid
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing NAT-
Traversal VID ver 02 payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing NAT-
Discovery payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT
Discovery hash
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing NAT-
Discovery payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT
Discovery hash
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing
Fragmentation VID + extended capabilities payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing VID
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Send Altiga/Cisco
VPN3000/Cisco ASA GW VID
Jun 21 19:07:55 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 428
Jun 21 19:07:55 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 156
```

```
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing hash
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Computing hash for
ISAKMP
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing notify
payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing NAT-
Discovery payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT
Discovery hash
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing NAT-
Discovery payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT
Discovery hash
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing VID payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Processing IOS/PIX
Vendor ID payload (version: 1.0.0, capabilities: 00000408)
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing VID payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Received Cisco Unity
client VID
Jun 21 19:07:55 [IKEv1]: Group = SALES, IP = 10.1.100.100, Automatic NAT Detection
Status:      Remote end is NOT behind a NAT device      This end is NOT behind a NAT
device
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing blank
hash payload
Jun 21 19:07:55 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing qm hash
payload
Jun 21 19:07:55 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=f715d9ad)
with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message
(msgid=f715d9ad) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
86
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, process_attr(): Enter!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Processing MODE_CFG
Reply attributes.
```

LDAP connection must verify the user credentials and send back all user's attributes.

```
[10] Session Start
[10] New request Session, context 0x4792f78, reqType = 1
[10] Fiber started
[10] Creating LDAP context with uri=ldap://10.1.200.100:389
[10] Connect to LDAP server: ldap://10.1.200.100:389, status = Successful
[10] supportedLDAPVersion: value = 3
[10] supportedLDAPVersion: value = 2
[10] Binding as administrator
[10] Performing Simple authentication for Administrator to 10.1.200.100
[10] LDAP Search:
      Base DN = [DC=MICRONICSTRAINING,DC=COM]
      Filter  = [sAMAccountName=student]
```

```
Scope = [SUBTREE]
[10] User DN = [CN=student,CN=Users,DC=micronicstraining,DC=com]
[10] Talking to Active Directory server 10.1.200.100
[10] Reading password policy for student,
dn:CN=student,CN=Users,DC=micronicstraining,DC=com
[10] Read bad password count 0
[10] Binding as user
[10] Performing Simple authentication for student to 10.1.200.100
[10] Processing LDAP response for user student
[10] Checking password policy
[10] Authentication successful for student to 10.1.200.100
[10] Retrieved User Attributes:
[10]   objectClass: value = top
[10]   objectClass: value = person
[10]   objectClass: value = organizationalPerson
[10]   objectClass: value = user
[10]   cn: value = student
[10]   givenName: value = student
[10]   distinguishedName: value = CN=student,CN=Users,DC=micronicstraining,DC=com
[10]   instanceType: value = 4
[10]   whenCreated: value = 20100622045216.0Z
[10]   whenChanged: value = 20100622045305.0Z
[10]   displayName: value = student
[10]   uSNCreated: value = 13790
[10]   uSNChanged: value = 13799
[10]   name: value = student
[10]   objectGUID: value = .h9"j.B@....b...
[10]   userAccountControl: value = 512
[10]   badPwdCount: value = 0
[10]   codePage: value = 0
[10]   countryCode: value = 0
[10]   badPasswordTime: value = 0
[10]   lastLogoff: value = 0
[10]   lastLogon: value = 0
[10]   pwdLastSet: value = 129216559364531250
[10]   primaryGroupID: value = 513
[10]   userParameters: value = m: d.
[10]   objectSid: value = .....n.L{..OLT~/XR...
[10]   accountExpires: value = 9223372036854775807
[10]   logonCount: value = 0
[10]   sAMAccountName: value = student
[10]   sAMAccountType: value = 805306368
[10]   userPrincipalName: value = student@micronicstraining.com
[10]   objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=micronicstraining,DC=com
[10]   msNPAllowDialin: value = TRUE
[10]   mapped to Simultaneous-Logins: value = 1
[10] Fiber exit Tx=693 bytes Rx=2654 bytes, status=1
[10] Session End
```

Seems the correct user's attribute is matched and mapped to Simultaneous-Logins EasyVPN attribute.

```
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: primary DNS = cleared
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: secondary DNS = cleared
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: primary WINS = cleared
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: secondary WINS = cleared
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: split tunneling list = ST
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: IP Compression = disabled
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: Split Tunneling Policy = Split Network
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKEGetUserAttributes: Browser Proxy Bypass Local = disable
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, User
(student) authenticated.
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing blank hash payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing qm hash payload
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=4a727d34)
with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message
(msgid=4a727d34) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
56
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
process_attr(): Enter!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Processing cfg ACK attributes
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message (msgid=535785e)
with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 177
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
process_attr(): Enter!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Processing cfg Request attributes
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for IPV4 address!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for IPV4 net mask!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for DNS server address!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for WINS server address!
```

```
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Received
unsupported transaction mode attribute: 5
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Banner!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Save PW setting!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Default Domain Name!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Split Tunnel List!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Split DNS!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for PFS setting!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Client Browser Proxy Setting!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for backup ip-sec peer list!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Client Smartcard Removal Disconnect Setting!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for Application Version!
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Client
Type: WinNT Client Application Version: 5.0.05.0290
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for FWTYPE!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for DHCP hostname for DDNS is: acs-lab!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
MODE_CFG: Received request for UDP Port!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Obtained IP addr (10.1.21.1) prior to initiating Mode Cfg (XAuth enabled)
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Assigned
private IP address 10.1.21.1 to remote user
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing blank hash payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Send Client Browser Proxy Attributes!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Browser Proxy set to No-Modify. Browser Proxy data will NOT be included in the mode-cfg
reply
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Send Cisco Smartcard Removal Disconnect enable!!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing qm hash payload
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=535785e)
with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 180
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
```

```
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, PHASE 1
COMPLETED
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, Keep-alive type for this connection: DPD
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Starting P1 rekey timer: 82080 seconds.
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
sending notify message
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing blank hash payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing qm hash payload
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=291ddb51)
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 88
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message
(msgid=e4373f07) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5)
+ NONE (0) total length : 1022
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
processing hash payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
processing SA payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
processing nonce payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
processing ID payload
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Received
remote Proxy Host data in ID Payload: Address 10.1.21.1, Protocol 0, Port 0
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
processing ID payload
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Received
local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0,
Port 0
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, QM
IsRekeyed old sa not found by addr
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, IKE
Remote Peer configured for crypto map: DYN-CMAP
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
processing IPsec SA payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IPsec SA Proposal # 11, Transform # 1 acceptable Matches global IPsec SA entry # 10
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, IKE:
requesting SPI!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKE got SPI from key engine: SPI = 0x082e7c0b
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
oakley constructing quick mode
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing blank hash payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing IPsec SA payload
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100,
Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds
```

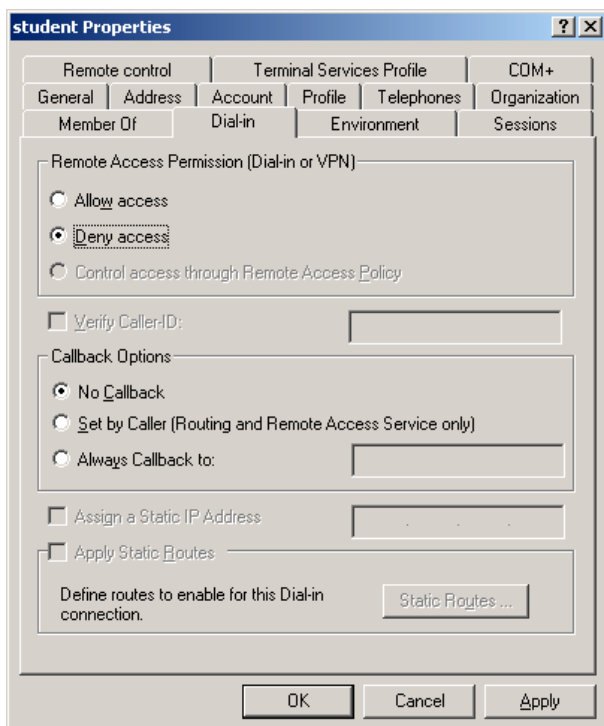


```
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing IPSec nonce payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing proxy ID
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Transmitting Proxy Id:
Remote host: 10.1.21.1 Protocol 0 Port 0
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Sending RESPONDER LIFETIME notification to Initiator
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing qm hash payload
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=e4373f07)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) +
NONE (0) total length : 176
Jun 21 19:07:56 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message
(msgid=e4373f07) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
processing hash payload
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
loading all IPSEC SAs
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Generating Quick Mode Key!
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Generating Quick Mode Key!
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Security
negotiation complete for User (student) Responder, Inbound SPI = 0x082e7c0b, Outbound
SPI = 0x71387a50
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKE got a KEY_ADD msg for SA: SPI = 0x71387a50
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Pitcher: received KEY_UPDATE, spi 0x82e7c0b
Jun 21 19:07:56 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Starting P2 rekey timer: 27360 seconds.
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Adding
static route for client address: 10.1.21.1
Jun 21 19:07:56 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, PHASE 2
COMPLETED (msgid=e4373f07)
```

```
ASA# un all
ASA#
```

Test

To test, let's disable Dial-in permission for the "student" username and connect again.



The connection failed and the Xauth login window keeps displaying.



```
ASA# deb crypto isakmp 9
ASA# deb ldap 9
debug ldap  enabled at level 9
```

```
Jun 21 19:11:41 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 849
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing SA payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing ke payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing ISA_KE payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing nonce payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing ID payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, Received xauth V6 VID
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, Received DPD VID
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, Received Fragmentation VID
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: False
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, Received NAT-Traversal ver 02 VID
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, processing VID payload
Jun 21 19:11:41 [IKEv1 DEBUG]: IP = 10.1.100.100, Received Cisco Unity client VID
Jun 21 19:11:41 [IKEv1]: IP = 10.1.100.100, Connection landed on tunnel_group SALES
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing IKE SA
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, IKE SA Proposal # 1,
Transform # 10 acceptable Matches global IKE entry # 1
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing ISAKMP SA
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing ke
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing nonce
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Generating keys for
Responder...
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing ID
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing hash
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Computing hash for
ISAKMP
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing Cisco
Unity VID payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing xauth V6
VID payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing dpd vid
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing NAT-
Traversal VID ver 02 payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing NAT-
Discovery payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT
Discovery hash
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing NAT-
Discovery payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT
Discovery hash
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing
Fragmentation VID + extended capabilities payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing VID
payload
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Send Altiga/Cisco
VPN3000/Cisco ASA GW VID
Jun 21 19:11:41 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) +
```

```
VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (13) +  
VENDOR (13) + NONE (0) total length : 428
```

```
Jun 21 19:11:41 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message (msgid=0) with  
payloads : HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + VENDOR (13) +  
VENDOR (13) + NONE (0) total length : 156
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing hash  
payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Computing hash for  
ISAKMP
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing notify  
payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing NAT-  
Discovery payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT  
Discovery hash
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing NAT-  
Discovery payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, computing NAT  
Discovery hash
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing VID payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Processing IOS/PIX  
Vendor ID payload (version: 1.0.0, capabilities: 00000408)
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, processing VID payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Received Cisco Unity  
client VID
```

```
Jun 21 19:11:41 [IKEv1]: Group = SALES, IP = 10.1.100.100, Automatic NAT Detection  
Status:      Remote end is NOT behind a NAT device      This end is NOT behind a NAT  
device
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing blank  
hash payload
```

```
Jun 21 19:11:41 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, constructing qm hash  
payload
```

```
Jun 21 19:11:41 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=9f26ceb8)  
with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68
```

```
Jun 21 19:11:43 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message  
(msgid=9f26ceb8) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :  
86
```

```
Jun 21 19:11:43 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, process_attr(): Enter!
```

```
Jun 21 19:11:43 [IKEv1 DEBUG]: Group = SALES, IP = 10.1.100.100, Processing MODE_CFG  
Reply attributes.
```

```
[12] Session Start
```

```
[12] New request Session, context 0x4792f78, reqType = 1
```

```
[12] Fiber started
```

```
[12] Creating LDAP context with uri=ldap://10.1.200.100:389
```

```
[12] Connect to LDAP server: ldap://10.1.200.100:389, status = Successful
```

```
[12] supportedLDAPVersion: value = 3
```

```
[12] supportedLDAPVersion: value = 2
```

```
[12] Binding as administrator
```

```
[12] Performing Simple authentication for Administrator to 10.1.200.100
```

```
[12] LDAP Search:
```

```

Base DN = [DC=MICRONICSTRAINING,DC=COM]
Filter   = [sAMAccountName=student]
Scope    = [SUBTREE]
[12] User DN = [CN=student,CN=Users,DC=micronicstraining,DC=com]
[12] Talking to Active Directory server 10.1.200.100
[12] Reading password policy for student,
dn:CN=student,CN=Users,DC=micronicstraining,DC=com
[12] Read bad password count 0
[12] Binding as user
[12] Performing Simple authentication for student to 10.1.200.100
[12] Processing LDAP response for user student
[12] Checking password policy
[12] Authentication successful for student to 10.1.200.100
[12] Retrieved User Attributes:
[12]   objectClass: value = top
[12]   objectClass: value = person
[12]   objectClass: value = organizationalPerson
[12]   objectClass: value = user
[12]   cn: value = student
[12]   givenName: value = student
[12]   distinguishedName: value = CN=student,CN=Users,DC=micronicstraining,DC=com
[12]   instanceType: value = 4
[12]   whenCreated: value = 20100622045216.0Z
[12]   whenChanged: value = 20100622050649.0Z
[12]   displayName: value = student
[12]   uSNCreated: value = 13790
[12]   uSNChanged: value = 13817
[12]   name: value = student
[12]   objectGUID: value = .h9"j.B@....b...
[12]   userAccountControl: value = 512
[12]   badPwdCount: value = 0
[12]   codePage: value = 0
[12]   countryCode: value = 0
[12]   badPasswordTime: value = 0
[12]   lastLogoff: value = 0
[12]   lastLogon: value = 0
[12]   pwdLastSet: value = 129216559364531250
[12]   primaryGroupID: value = 513
[12]   userParameters: value = m:                                d.
[12]   objectSid: value = .....n.L{.OLT~/XR...
[12]   accountExpires: value = 9223372036854775807
[12]   logonCount: value = 0
[12]   sAMAccountName: value = student
[12]   sAMAccountType: value = 805306368
[12]   userPrincipalName: value = student@micronicstraining.com
[12]   objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=micronicstraining,DC=com
[12]   msNPAllowDialin: value = FALSE
[12]   mapped to Simultaneous-Logins: value = 0

```

This time the attribute has FALSE value so that it is mapped to zero.

```

[12] Fiber exit Tx=693 bytes Rx=2655 bytes, status=1
[12] Session End
Jun 21 19:11:43 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing blank hash payload
Jun 21 19:11:43 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing qm hash payload
Jun 21 19:11:43 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=91334584)
with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 93
Jun 21 19:11:47 [IKEv1]: IP = 10.1.100.100, IKE_DECODE RECEIVED Message
(msgid=91334584) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length :
64
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
process_attr(): Enter!
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
Processing MODE_CFG Reply attributes.
Jun 21 19:11:47 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Error
processing payload: Payload ID: 14
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKE TM V6 FSM error history (struct &0x48036d8) <state>, <event>: TM_DONE, EV_ERROR--
>TM_WAIT_REPLY, EV_PROC_MSG-->TM_WAIT_REPLY, EV_HASH_OK-->TM_WAIT_REPLY, NullEvent--
>TM_WAIT_REPLY, EV_COMP_HASH-->TM_WAIT_REPLY, EV_VALIDATE_MSG-->TM_WAIT_REPLY,
EV_DECRYPT_OK-->TM_WAIT_REPLY, NullEvent
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKE AM Responder FSM error history (struct &0x49253a8) <state>, <event>: AM_DONE,
EV_ERROR-->AM_TM_INIT_XAUTH_V6H, EV_TM_FAIL-->AM_TM_INIT_XAUTH_V6H, NullEvent--
>AM_TM_INIT_XAUTH_V6H, EV_ACTIVATE_NEW_SA-->AM_TM_INIT_XAUTH_V6H, NullEvent--
>AM_TM_INIT_XAUTH_V6H, EV_START_TM-->AM_TM_INIT_XAUTH, EV_START_TM-->AM_PROC_MSG3,
EV_TEST_TM_H6
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
IKE SA AM:ee83af8c terminating: flags 0x0105c001, refcnt 0, tuncnt 0

```

The user authentication has been terminated due to Simultaneous Logins = 0

```

Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
sending delete/delete with reason message
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing blank hash payload
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing IKE delete payload
Jun 21 19:11:47 [IKEv1 DEBUG]: Group = SALES, Username = student, IP = 10.1.100.100,
constructing qm hash payload
Jun 21 19:11:47 [IKEv1]: IP = 10.1.100.100, IKE_DECODE SENDING Message (msgid=52a01bc8)
with payloads : HDR + HASH (8) + DELETE (12) + NONE (0) total length : 76
Jun 21 19:11:47 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Removing
peer from peer table failed, no match!
Jun 21 19:11:47 [IKEv1]: Group = SALES, Username = student, IP = 10.1.100.100, Error:
Unable to remove PeerTblEntry
Jun 21 19:11:47 [IKEv1]: IP = 10.1.100.100, Received encrypted packet with no matching
SA, dropping

```

This page is intentionally left blank.

Advanced CCIE SECURITY v4 LAB WORKBOOK

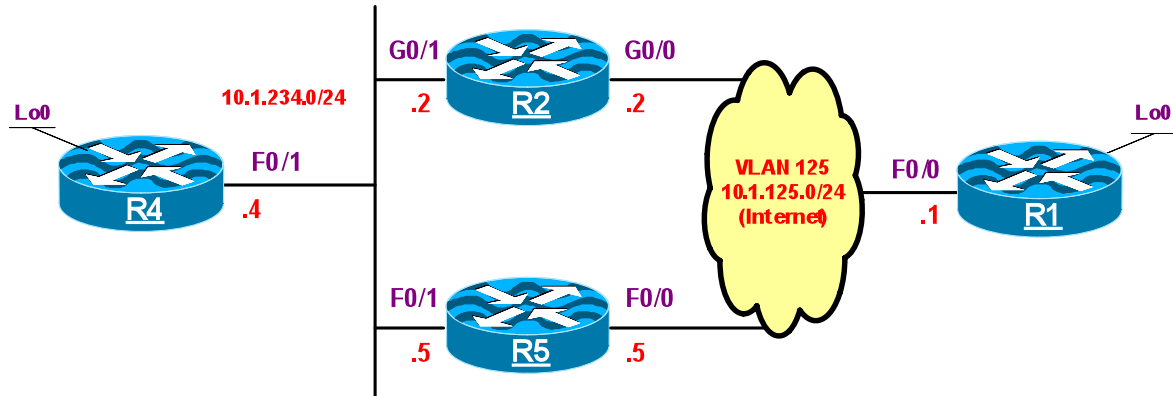
Advanced VPN Features

Narbik Kocharians
CCIE #12410 (R&S, Security, SP)
CCSI #30832

Piotr Matusiak
CCIE #19860 (R&S, Security)
C|EH, CCSI #33705

www.MicronicsTraining.com

Lab 1.68. IPSec Stateful Failover



Lab Setup

- R1's F0/0, R2's G0/0 and R5's F0/0 interface should be configured in VLAN 125
- R2's G0/1, R5's F0/1 and R4's F0/1 interface should be configured in VLAN 245
- Configure Telnet on all routers using password "cisco"

IP Addressing

Device	Interface	IP address
R1	F0/0	10.1.125.1/24
	Lo0	1.1.1.1/24
R2	G0/0	10.1.125.2/24
	G0/1	10.1.245.2/24
R4	F0/1	10.1.245.4/24
	Lo0	4.4.4.4/24
R5	F0/0	10.1.125.5/24
	F0/1	10.1.245.5/24

Task 1

Configure Site to Site IPSec VPN between R1 and R2-R5 pair to protect traffic going between networks 1.1.1.0/24 and 4.4.4.0/24. The R1 must be configured to establish IKE with a VIP address of R2/R5 HA pair. Use 254 in the 4th octet of VIP address

and enable tracking of all interfaces. R2 should be Active HSRP peer. Ensure that all IPSec information (sessions, states, etc.) are exchanged between R2 and R5 using Stream Control Transmission Protocol (SCTP) as the transport protocol.

Use the following ISAKMP parameters:

- Phase 1:
 - Authentication: PSK
 - Encryption: DES
 - Hashing: SHA
 - Group: 1
 - Key: cisco123
- Phase 2:
 - Encryption: 3DES
 - Hashing: SHA



Stateful Failover for IPSec is designed to work in conjunction with Stateful Switchover (SSO) and Hot Standby Router Protocol (HSRP).

HSRP is configured on two routers and enables Virtual IP address (VIP) to be used as a tunnel endpoint. The configuration is straight forward and requires configuring “standby” properties on the interface pair (on two different routers). If we need to use two standby groups for two interface pairs (one for outside and one for inside interfaces) we need to ensure that both HSRP group will become unavailable in case of one interface failure. This can be done by enabling interface tracking feature. There is also a need for “standby name” command which is used later to configure SSO and crypto map redundancy.

SSO is necessary for IPsec and IKE to learn about the redundancy state of the network and to synchronize its internal application state with its redundant peers. SSO feature uses Inter-Process Communication (IPC) and Stream Control Transmission Protocol (SCTP) as the transport protocol to send all IPSec information to the backup router.

Using HSRP and SSO we can configure Stateful IPSec solution with High Availability as all IPSec dynamic information is send over to the backup router and used in case of primary router failure. This should be transparent for the user as no tunnel re-negotiation should occur.

Configuration

Complete these steps:

Step 1 R2 IPsec configuration.

```
R2(config)#int g0/0
R2(config-if)#standby 1 ip 10.1.125.254
R2(config-if)#standby 1 preempt
R2(config-if)#standby 1 name VPN-HA
R2(config-if)#standby 1 track g0/1
R2(config-if)#
%HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 1 state Standby ->
Active
R2(config-if)#exi
```

This is configuration of the "outside" interface, meaning the interface where IPsec tunnel will be terminated on. The HSRP has priority of 100 by default so we need to ensure that the other router has lower priority. We should track our "inside" interface to make sure that whole router will become unavailable in case of only one interface failure. Finally there must be a name for HSRP group which will be used later in the crypto and SSO configuration.

```
R2(config)#int g0/1
R2(config-if)#standby 2 ip 10.1.245.254
R2(config-if)#standby 2 preempt
R2(config-if)#standby 2 track g0/0
R2(config-if)#standby 2 track g0/0
%HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 2 state Standby ->
Active
R2(config-if)#exi
```

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#auth pre
R2(config-isakmp)#exi
```

```
R2(config)#crypto isakmp key cisco123 address 10.1.125.1
```

```
R2(config)#access-list 120 permit ip 4.4.4.0 0.0.0.255 1.1.1.0
0.0.0.255
```

```
R2(config)#crypto ipsec transform-set TSET esp-3des esp-sha
R2(cfg-crypto-trans)#exi
```

```
R2(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

```
R2(config-crypto-map)#set transform-set TSET
R2(config-crypto-map)#match address 120
```

```
R2(config-crypto-map)#reverse-route
R2(config-crypto-map)#exit
```

Crypto configuration is a standard config for typical Site to Site IPsec VPN.

```
R2(config)#int g0/0
R2(config-if)#crypto map CMAP redundancy VPN-HA stateful
R2(config-if)#
%CRYPTO-5-IKE_SA_HA_STATUS: IKE sa's if any, for vip 10.1.125.254
will change from STANDBY to ACTIVE
R2(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

The crypto map is attached to the "outside" interface with two additional keywords:

- "redundancy <HSRP-Gr-Name>" - binds the standby IP address as the local tunnel endpoint and, at the same time, ensures that stateless (without "stateful" keyword) HSRP failover is facilitated between an active and standby device that belongs to the same standby group.
- "stateful" - enables IPsec state information to be sent over to the other device using SSO.

```
R2(config)#ip route 4.4.4.0 255.255.255.0 10.1.245.4
```

Step 2 R5 IPsec configuration.

The same configuration must be done on both routers.

```
R5(config)#int f0/0
R5(config-if)#standby 1 ip 10.1.125.254
R5(config-if)#standby 1 priority 90
```

One difference is on the backup router the HSRP priority must be lower than on primary router.

```
R5(config-if)#standby 1 preempt
R5(config-if)#standby 1 name VPN-HA
R5(config-if)#standby 1 track f0/1
R5(config-if)#exit
```

```
R5(config)#int f0/1
R5(config-if)#standby 2 ip 10.1.245.254
R5(config-if)#standby 2 preempt
R5(config-if)#standby 2 priority 90
R5(config-if)#standby track f0/0
R5(config-if)#exit
```

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)# authentication pre-share
R5(config-isakmp)#exi

R5(config)#crypto isakmp key cisco123 address 10.1.125.1

R5(config)#access-list 120 permit ip 4.4.4.0 0.0.0.255 1.1.1.0
0.0.0.255

R5(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R5(cfg-crypto-trans)#exi
R5(config)#
%HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

R5(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.

R5(config-crypto-map)#set transform-set TSET
R5(config-crypto-map)#match address 120
R5(config-crypto-map)#reverse-route
R5(config-crypto-map)#exi

R5(config)#int f0/0
R5(config-if)#crypto map CMAP redundancy VPN-HA stateful
R5(config-if)#
%CRYPTO-5-IKE_SA_HA_STATUS: IKE sa's if any, for vip 10.1.125.254
will change from STANDBY to ACTIVE
R5(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

R5(config)#ip route 4.4.4.0 255.255.255.0 10.1.245.4
```

Step 3 R2 IPSec HA configuration.

The SSO configuration must have HSRP group name used to be able to notice other device that primary device has failed. The SCTP protocol uses TCP as a transport with source and destination ip/port configurable.

```
R2(config)#redundancy inter-device
R2(config-red-interdevice)#scheme standby VPN-HA
R2(config-red-interdevice)#exi
R2(config)#ipc zone default
R2(config-ipczone)#association 1
R2(config-ipczone-assoc)#protocol sctp
R2(config-ipc-protocol-sctp)#local-port 12345
R2(config-ipc-local-sctp)#local-ip 10.1.125.2
R2(config-ipc-local-sctp)#ex
```

```
R2(config-ipc-protocol-sctp)#remote-port 12345
R2(config-ipc-remote-sctp)#remote-ip 10.1.125.5
R2(config-ipc-remote-sctp)#exi
R2(config-ipc-protocol-sctp)#exi
R2(config-ipczone-assoc)#exi
R2(config-ipczone)#exi
```

Step 4 R5 IPsec HA configuration.

```
R5(config)#redundancy inter-device
R5(config-red-interdevice)#scheme standby VPN-HA
% Standby scheme configuration cannot be processed now group VPN-HA
is not in active state
R5(config-red-interdevice)#exi
R5(config)#ipc zone default
R5(config-ipczone)#association 1
R5(config-ipczone-assoc)#protocol sctp
R5(config-ipc-protocol-sctp)#local-port 12345
R5(config-ipc-local-sctp)#local-ip 10.1.125.5
R5(config-ipc-local-sctp)#ex
R5(config-ipc-protocol-sctp)#remote-port 12345
R5(config-ipc-remote-sctp)#remote-ip 10.1.125.2
R5(config-ipc-remote-sctp)#exi
R5(config-ipc-protocol-sctp)#exi
R5(config-ipczone-assoc)#exi
R5(config-ipczone)#exi
```

Quick Verification

R5#sh redundancy inter-device

```
Redundancy inter-device state: RF_INTERDEV_STATE_INIT
  Pending Scheme: Standby (Will not take effect until next reload)
    Pending Groupname: VPN-HA
  Scheme: <NOT CONFIGURED>
  Peer present: UNKNOWN
  Security: Not configured
```

Unfortunately, enabling SSO requires device reboot to be operational.

```
R5#wr
Building configuration...

[OK]
R5#relo
Proceed with reload? [confirm]
```

After R5 reloading (do not forget to save your config)

R5#sh redundancy inter-device

```
Redundancy inter-device state: RF_INTERDEV_STATE_STDBY
Scheme: Standby
  Groupname: VPN-HA Group State: Standby
Peer present: RF_INTERDEV_PEER_COMM
Security: Not configured
```

R2#sh redundancy inter-device

```
Redundancy inter-device state: RF_INTERDEV_STATE_ACT
Scheme: Standby
  Groupname: VPN-HA Group State: Active
Peer present: RF_INTERDEV_PEER_COMM
Security: Not configured
```

After reload, the SSO monitors HSRP group and sends IPSec information between devices.

Now, we need to configure R1 to be able to set up IPSec tunnel and verify our solution.

Configuration

Complete these steps:

Step 5 R1 IPSec configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#auth pre
R1(config-isakmp)#exi

R1(config)#crypto isakmp key cisco123 address 10.1.125.254

R1(config)#crypto ipsec transform-set TSET esp-3des esp-sha
R1(cfg-crypto-trans)#exi

R1(config)#access-list 120 permit ip 1.1.1.0 0.0.0.255 4.4.4.0
0.0.0.255

R1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set transform-set TSET
R1(config-crypto-map)#match address 120
R1(config-crypto-map)#set peer 10.1.125.254
R1(config-crypto-map)#exi

R1(config)#int f0/0
R1(config-if)#crypto map CMAP
R1(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```


Step 6 R4 routing.

```
R4(config)#ip route 0.0.0.0 0.0.0.0 10.1.245.254
```

Step 7 R1 routing.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.125.254
```

Verification

```
R1#pi 4.4.4.4 so lo0
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

```
.!!!!
```

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

We need some interesting traffic to trigger our IPSec VPN. Let's make a ping between R1 and R4.

```
R1#sh cryp ips sa
```

```
interface: FastEthernet0/0
```

```
  Crypto map tag: CMAP, local addr 10.1.125.1
```

```
protected vrf: (none)
```

```
local  ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (4.4.4.0/255.255.255.0/0/0)
```

```
current_peer 10.1.125.254 port 500
```

```
  PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

```
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 1, #recv errors 0
```

The traffic has been encrypted/decrypted. Note that peer IP address is the HSRP VIP.

```
local crypto endpt.: 10.1.125.1, remote crypto endpt.: 10.1.125.254
```

```
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
```

```
current outbound spi: 0xE757BC0F(3881286671)
```

```
PFS (Y/N): N, DH group: none
```

```

inbound esp sas:
spi: 0xAB00724C(2868933196)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: CMAP
  sa timing: remaining key lifetime (k/sec): (4524905/3588)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```

outbound esp sas:
spi: 0xE757BC0F(3881286671)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: CMAP
  sa timing: remaining key lifetime (k/sec): (4524905/3588)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

```
outbound ah sas:
```

```
outbound pcg sas:
```

R1#sh cry isakmp sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

```

```
IPv4 Crypto ISAKMP SA
```

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1001	10.1.125.1	10.1.125.254		ACTIVE	des	sha	psk	1	23:59:35	

```

  Engine-id:Conn-id = SW:1

```

```
IPv6 Crypto ISAKMP SA
```

R2#sh redundancy inter-device

```

Redundancy inter-device state: RF_INTERDEV_STATE_ACT
Scheme: Standby
  Groupname: VPN-HA Group State: Active
Peer present: RF_INTERDEV_PEER_COMM
Security: Not configured

```

R2#sh crypto ipsec sa

```
interface: GigabitEthernet0/0
  Crypto map tag: CMAP, local addr 10.1.125.254

protected vrf: (none)
local  ident (addr/mask/prot/port): (4.4.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)
current_peer 10.1.125.1 port 500
  PERMIT, flags={}
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
```

Same on R2, we see traffic is going through the tunnel.

```
local crypto endpt.: 10.1.125.254, remote crypto endpt.: 10.1.125.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0xAB00724C(2868933196)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xE757BC0F(3881286671)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4438095/3562)
      HA KB life last checkpointed at (k): (4438096)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xAB00724C(2868933196)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000046, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4438095/3562)
      HA KB life last checkpointed at (k): (4438096)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

R2#show crypto ha

IKE VIP: 10.1.125.254

stamp: 9E 08 4C 2E 83 07 FE 77 91 F8 29 1F 6C 9B F9 88

IPSec VIP: 10.1.125.254

Note that IKE is using HSRP VIP address. This is due to "redundancy" keyword in the crypto map.

R2#show redundancy states

my state = 13 -ACTIVE

peer state = 8 -STANDBY HOT

Mode = Duplex

Unit ID = 0

Maintenance Mode = Disabled

Manual Swact = Enabled

Communications = Up

client count = 12

client_notification_TMR = 30000 milliseconds

RF debug mask = 0x0

R2#show redundancy inter

Redundancy inter-device state: RF_INTERDEV_STATE_ACT

Scheme: Standby

Groupname: VPN-HA Group State: Active

Peer present: RF_INTERDEV_PEER_COMM

Security: Not configured

R2#show crypto session

Crypto session current status

Interface: GigabitEthernet0/0

Session status: UP-ACTIVE

Peer: 10.1.125.1 port 500

IKE SA: local 10.1.125.254/500 remote 10.1.125.1/500 Active

IPSEC FLOW: permit ip 4.4.4.0/255.255.255.0 1.1.1.0/255.255.255.0

Active SAs: 2, origin: dynamic crypto map

R5#sh redundancy inter-device

Redundancy inter-device state: RF_INTERDEV_STATE_STDBY

Scheme: Standby

Groupname: VPN-HA Group State: Standby

Peer present: RF_INTERDEV_PEER_COMM

Security: Not configured

R5#show redundancy states

```
my state = 8 -STANDBY HOT
peer state = 13 -ACTIVE
Mode = Duplex
Unit ID = 0

Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up

client count = 12
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
```

R5#show crypto isakmp sa det

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.

1001  10.1.125.254      10.1.125.1      STDBY   des  sha  psk  1  23:58:02
      Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

R5#show crypto ipsec sa

No active IPSec SAs

R5#show crypto ha

```
IKE VIP: 10.1.125.254
stamp: 9E 08 4C 2E 83 07 FE 77 91 F8 29 1F 6C 9B F9 88
IPSec VIP: 10.1.125.254
```

R5#show crypto session

```
Crypto session current status

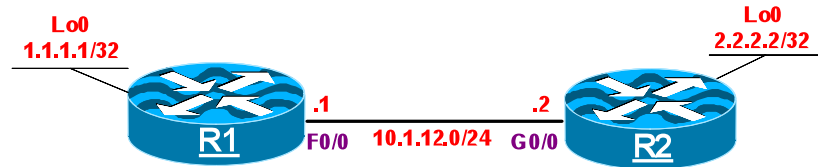
Interface: FastEthernet0/0
Session status: UP-IDLE-STANDBY
Peer: 10.1.125.1 port 500
IKE SA: local 10.1.125.254/500 remote 10.1.125.1/500 Active

R5#
```

Note: You may get the following error message which indicated your hardware does not support IPSec HA. Only specified HW support that feature.

```
%CRYPTO_HA_IPSEC-4-CRYPTO_HA_NOT_SUPPORTED_BY_HW: Crypto hardware is enabled and it  
does not support HA operation 'IPSec - extract keys'
```

Lab 1.69. IPSec Static VTI



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 120
- Configure Telnet on all routers using password "cisco"

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/32
	F0/0	10.1.12.1/24
R2	G0/0	10.1.12.2/24
	Lo0	2.2.2.2/32

Task 1

Configure IPSec VPN between R1 and R2 using Static VTI interface. Use the following ISAKMP parameters:

- Phase 1:
 - Authentication: PSK
 - Encryption: DES
 - Hashing: SHA
 - Group: 1
 - Key: cisco123
- Phase 2:
 - Encryption: 3DES
 - Hashing: SHA

Use IP addresses of 192.168.12.1 and 192.168.12.2 for tunnel addressing for R1 and R2 respectively. Ensure that all traffic destined to unknown networks will be routed through the VPN tunnel.



Static Virtual Tunnel Interface (sVTI) has been developed as a successor for GRE over IPSec. GRE itself is very popular because it carries multicast traffic over the network and has small overhead and performance impact. However, GRE alone it is not secure. That's why we use IPSec to secure GRE traffic. There are two ways to do that:

- (1) using crypto map and specifying GRE as an interesting traffic in a crypto ACL; and*
- (2) using IPSec profiles and applying tunnel protection command on the tunnel interface.*

In addition to that we got into trouble with MTU size and fragmentation as GRE + IPSec may add something between 56 and 76 bytes to the packet.

Static VTI addresses most of the issues with GRE and IPSec. This is nothing more than tunnel interface with IPSec encapsulation. What does it mean for us?

- *it carries multicast traffic natively*
 - *there is no GRE involved so no additional overhead (the MTU for VTI is set to 1442 by IOS)*
 - *no need for crypto map on physical interface*
 - *no need for crypto ACL , IOS encrypts all traffic sourced from tunnel interface (IPSec SA has 0.0.0.0 as source and destination)*
 - *features like NAT or QoS are natively supported on the VTI interface like on any other physical interface*
-

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#exi

R1(config)#crypto isakmp key cisco123 address 10.1.12.2
```



```
R1(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)#exi
```

```
R1(config)#crypto ipsec profile SVTI
R1(ipsec-profile)#set transform-set TSET
R1(ipsec-profile)#exi
```

```
R1(config)#interface Tunnel0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#tunnel source FastEthernet0/0
R1(config-if)#tunnel destination 10.1.12.2
R1(config-if)#tunnel mode ipsec ipv4
R1(config-if)#tunnel protection ipsec profile SVTI
R1(config-if)#
```

Interface Tunnel is configured in the same way as for GRE except on command. We must change tunnel mode to be IPSec (by default tunnel mode is GRE). That's it.

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to down
R1(config-if)#exi
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2
```

Note that we did not configure Crypto ACL. All we need is IPSec Profile attached to the tunnel and an appropriate routing pointing through the tunnel.

Step 2 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#exi
```

```
R2(config)#crypto isakmp key cisco123 address 10.1.12.1
```

```
R2(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R2(cfg-crypto-trans)#exi
```

```
R2(config)#crypto ipsec profile SVTI
R2(ipsec-profile)#set transform-set TSET
R2(ipsec-profile)#exi
```

```
R2(config)#interface Tunnel0
R2(config-if)#ip address 192.168.12.2 255.255.255.0
```

```

R2(config-if)#tunnel source GigabitEthernet0/0
R2(config-if)#tunnel destination 10.1.12.1
R2(config-if)#tunnel mode ipsec ipv4
R2(config-if)#tunnel protection ipsec profile SVTI
R2(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R2(config-if)#exi

R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.1

```

Verification

R1#ping 2.2.2.2 so lo0

Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
 Packet sent with a source address of 1.1.1.1
 !!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Ping is successful.

R1#sh cryp isa sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
1003  10.1.12.1         10.1.12.2      ACTIVE des  sha  psk  1  23:58:22
      Engine-id:Conn-id = SW:3

```

IPv6 Crypto ISAKMP SA

R1#sh cryp ips sa

```

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.12.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

```

```

current_peer 10.1.12.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

```

ICMP packets have been encrypted/decrypted. Note the PROXY IDs - 0/0 means all packets from every source to every destination will be encrypted. This is equivalent to the Crypto ACL of "permit ip any any".

```

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.12.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xA9FBBAF(178240431)
PFS (Y/N): N, DH group: none

```

inbound esp sas:

```

spi: 0x3DACD141(1034735937)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2009, flow_id: NETGX:9, sibling_flags 80000046, crypto map: Tunnel0-

```

head-0

```

sa timing: remaining key lifetime (k/sec): (4477670/3492)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```

spi: 0xA9FBBAF(178240431)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2010, flow_id: NETGX:10, sibling_flags 80000046, crypto map: Tunnel0-

```

head-0

```

sa timing: remaining key lifetime (k/sec): (4477670/3492)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

outbound ah sas:

outbound pcp sas:

R1#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.12.2 to network 0.0.0.0

```
C    192.168.12.0/24 is directly connected, Tunnel0
    1.0.0.0/32 is subnetted, 1 subnets
C      1.1.1.1 is directly connected, Loopback0
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.12.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 192.168.12.2
```

The default routing is pointing to the other end of the tunnel. Hence, packets must go through the tunnel in order to reach remote networks.

R1#sh int tu0

```
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.12.1/24
  MTU 17883 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.1.12.1 (FastEthernet0/0), destination 10.1.12.2
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1443 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "SVTI")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5 packets input, 500 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  20 packets output, 1920 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
```

R2#sh cry isak sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection
 K - Keepalives, N - NAT-traversal
 T - cTCP encapsulation, X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1002	10.1.12.2	10.1.12.1		ACTIVE	des	sha	psk	1	23:56:46	

Engine-id:Conn-id = SW:2

IPv6 Crypto ISAKMP SA

R2#sh cryp ips sa

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.1.12.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.1.12.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.2, remote crypto endpt.: 10.1.12.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x3DACD141(1034735937)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xA9FBBAF(178240431)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2007, flow_id: Onboard VPN:7, sibling_flags 80000046, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4550510/3402)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:
```

```

outbound esp sas:
  spi: 0x3DACD141(1034735937)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2008, flow_id: Onboard VPN:8, sibling_flags 80000046, crypto map:
Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4550510/3402)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```

R2#sh cryp sess

```
Crypto session current status
```

```

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.12.1 port 500
IKE SA: local 10.1.12.2/500 remote 10.1.12.1/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map

```

R2#sh cryp eng conn act

```
Crypto Engine Connections
```

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
1002	IKE	SHA+DES	0	0	10.1.12.2
2007	IPsec	3DES+SHA	0	5	10.1.12.2
2008	IPsec	3DES+SHA	5	0	10.1.12.2

R2#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

```

```
Gateway of last resort is 192.168.12.1 to network 0.0.0.0
```

```

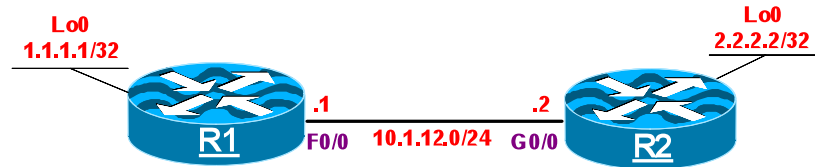
C    192.168.12.0/24 is directly connected, Tunnel0
    2.0.0.0/32 is subnetted, 1 subnets
C      2.2.2.2 is directly connected, Loopback0
    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.12.0 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.12.1

```

R2#sh int tu0

```
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.12.2/24
  MTU 17883 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.1.12.2 (GigabitEthernet0/0), destination 10.1.12.1
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1443 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "SVTI")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    20 packets input, 2000 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5 packets output, 500 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
```

Lab 1.70. IKE encrypted keys



This lab setup is based on the previous lab configuration. You do not need to erase configs before configuring this lab.

Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 120
- Configure Telnet on all routers using password "cisco"

IP Addressing

Device	Interface	IP address
R1	Lo0	1.1.1.1/32
	F0/0	10.1.12.1/24
R2	G0/0	10.1.12.2/24
	Lo0	2.2.2.2/32

Task 1

Configure IPsec VPN between R1 and R2 using Static VTI interface. Use the following ISAKMP parameters:

- Phase 1:
 - Authentication: PSK
 - Encryption: DES
 - Hashing: SHA
 - Group: 1
 - Key: cisco123
- Phase 2:

- Encryption: 3DES
- Hashing: SHA

Use IP addresses of 192.168.12.1 and 192.168.12.2 for tunnel addressing for R1 and R2 respectively. Ensure that all traffic destined to unknown networks will be routed through the VPN tunnel.

Ensure that IKE pre-shared keys are encrypted using most secure algorithm with a master password of "Cisco!1234".



The problem with pre-shared key (PSK) authentication is not that it is weak comparing to the authentication using certificates. The problem is that those keys are stored in configuration in clear text so that an attacker will get information about used PSK by seeing the configuration. The configuration may be stored on a backup media or on TFTP server in a clear format so getting that information is relatively easy.

To resolve that issue we should either use certificates for authentication or enable strong encryption of PSK in the configuration. The second option is available from IOS version 12.3(2)T.

To enable this feature we first need a Master Key configured for the router. The Master Key is used by AES cryptographic protocol to encrypt all PSKs in the configuration. The master key is not stored in the router configuration and cannot be seen or obtained in any way while connected to the router.

For security reasons, neither the removal of the master key, nor the removal of the "password encryption aes" command decrypts the passwords in the router configuration. Once passwords are encrypted, they cannot be decrypted!

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#exit

R1(config)#crypto isakmp key cisco123 address 10.1.12.2

R1(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)#exit

R1(config)#crypto ipsec profile SVTI
```

```
R1(ipsec-profile)#set transform-set TSET
R1(ipsec-profile)#exi

R1(config)#interface Tunnel0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#tunnel source FastEthernet0/0
R1(config-if)#tunnel destination 10.1.12.2
R1(config-if)#tunnel mode ipsec ipv4
R1(config-if)#tunnel protection ipsec profile SVTI
R1(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to down
R1(config-if)#exi

R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2

R1(config)#key config-key password-encrypt Cisco!1234
R1(config)#password encryption aes
```

The first command configures Master Key. If not specified in the command, then the router asks for it interactively via command line.

The second command actually encrypts PSKs in the configuration.

Step 2 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#exi

R2(config)#crypto isakmp key cisco123 address 10.1.12.1

R2(config)#crypto ipsec transform-set TSET esp-3des esp-sha-hmac
R2(cfg-crypto-trans)#exi

R2(config)#crypto ipsec profile SVTI
R2(ipsec-profile)#set transform-set TSET
R2(ipsec-profile)#exi

R2(config)#interface Tunnel0
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#tunnel source GigabitEthernet0/0
R2(config-if)#tunnel destination 10.1.12.1
R2(config-if)#tunnel mode ipsec ipv4
R2(config-if)#tunnel protection ipsec profile SVTI
R2(config-if)#
```

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
R2(config-if)#exi

R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.1

R2(config)#key config-key password-encrypt Cisco!1234
R2(config)#password encryption aes
```

Verification

[Before key encryption]

R2#sh run | in crypto

```
crypto isakmp policy 10
crypto isakmp key cisco123 address 10.1.12.1
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
crypto ipsec profile SVTI
```

[After key encryption]

R2#sh run | in crypto

```
crypto isakmp policy 10
crypto isakmp key 6 `ABgQCubUODNbNOMXLYU\ZXgVQfXfc]HF` address 10.1.12.1
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
crypto ipsec profile SVTI
```

The master key is very important to decrypt the password for crypto use. We can delete the master key but then all passwords become unusable. You must then reissue the command with a new password in clear text to make it work.

R2(config)#no key config-key password-encrypt

```
WARNING: All type 6 encrypted keys will become unusable
Continue with master key deletion ? [yes/no]: yes
```

```
R2(config)#do clear cry isak
R2(config)#do clear cry sa
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down

R2(config)#do sh run | in key
crypto isakmp key 6 `ABgQCubUODNbNOMXLYU\ZXgVQfXfc]HF` address 10.1.12.1
```

R2(config)#do sh cry isa sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
10.1.12.1	10.1.12.2	MM_KEY_EXCH	1004	0	ACTIVE

The IKE cannot exchange Keying Material as the PSK is not accessible

IPv6 Crypto ISAKMP SA

Delete the encrypted PSK and create a new one in clear text.

R2(config)#no crypto isakmp key 6 `ABgQCUBuODNbNOMXLYU\ZXgVQfXfc]HF address 10.1.12.1

R2(config)#crypto isakmp key cisco123 address 10.1.12.1

Can not encrypt password.

Please configure a configuration-key with 'key config-key'

R2(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

R2(config)#do sh cry isa sa

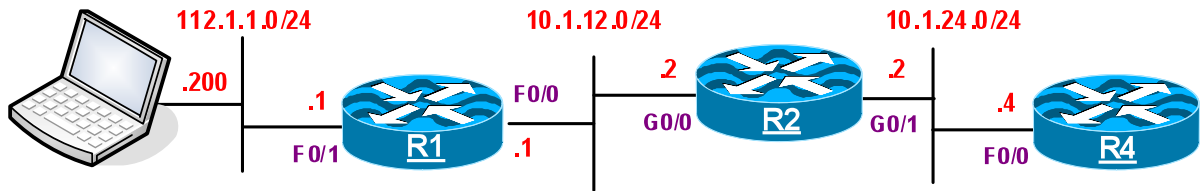
IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
10.1.12.1	10.1.12.2	QM_IDLE	1005	0	ACTIVE

fine!

IPv6 Crypto ISAKMP SA

Lab 1.71. IPSec Dynamic VTI



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's G0/1 and R4's F0/0 interface should be configured in VLAN 24
- R1's F0/1 and PC NIC (SW3 F0/15) should be configured in VLAN 112
- Configure Telnet on all routers using password "cisco"
- Configure default routing on R4 pointing to R2 and R2 pointing to R1

IP Addressing

Device	Interface	IP address
R1	F0/0	10.1.12.1/24
	F0/1	112.1.1.1/24
R2	G0/0	10.1.12.2/24
	G0/1	10.1.24.2/24
R4	F0/0	10.1.24.4/24
PC	NIC	112.1.1.200 /24

Task 1

Configure EasyVPN Server on R2 using Dynamic VTI interface. Use the following ISAKMP parameters:

- Phase 1:
 - Authentication: PSK
 - Encryption: AES
 - Hashing: SHA
 - Group: 2

➤ Phase 2:

- Encryption: AES 128
- Hashing: SHA

Local user named “student1” with a password of “student123” should be able to connect to SALES group using “cisco123” as a group password. The user should get an IP address from a pool of 10.1.21.1 – 10.1.21.10 addresses. After connection, only traffic destined to the network 10.1.24.0/24 should be encrypted.



Cisco Enhanced Easy VPN is a new method for configuring Easy VPN using Dynamic Virtual Tunnel Interface (DVTI) instead of a crypto map, which is used by traditional Easy VPN deployment.

DVTI can be used on both the Easy VPN Server and Easy VPN Remote scenarios. DVTI relies on the virtual tunnel interface to create a virtual access interface for every new Easy VPN tunnel. The configuration of the virtual access interface is cloned from a virtual template configuration. The cloned configuration includes the IPsec configuration and any Cisco IOS feature configured on the virtual template interface, such as QoS, NAT, CBAC or ACLs.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#aaa new-model
R2(config)#aaa authentication login AUTH-LOCAL local
R2(config)#aaa authorization network AUTHOR-LOCAL local

R2(config)#username student1 password student123

R2(config)#crypto isakmp policy 5
R2(config-isakmp)#encr aes
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#exi

R2(config)#crypto isakmp client configuration group SALES
R2(config-isakmp-group)#key cisco123
R2(config-isakmp-group)#pool RA-VPN
R2(config-isakmp-group)#acl 124
R2(config-isakmp-group)#exi
```

Like in every EasyVPN Server scenario we need to configure

Group with a password and a pool of addresses which will be used for clients. The split Tunneling feature is enabled by assigning an ACL to the group.

```
R2(config)#crypto isakmp profile IKE-RA
% A profile is deemed incomplete until it has match identity
statements
R2(conf-isa-prof)#match identity group SALES
R2(conf-isa-prof)#client authentication list AUTH-LOCAL
R2(conf-isa-prof)#isakmp authorization list AUTHOR-LOCAL
R2(conf-isa-prof)#client configuration address respond
R2(conf-isa-prof)#virtual-template 1
R2(conf-isa-prof)#exi
```

ISAKMP Profile is consulted for every new ISAKMP packet which is coming to the router. The profile has at least one "match" statement which must be true in order to use this profile. In EasyVPN deployment we often matching using EasyVPN group name. We need to configure EasyVPN authentication and authorization in the ISAKMP profile and an ability to serve IP addresses to the clients by the EasyVPN server.

The very important thing is to assign a special interface with ISAKMP profile. This interface is called Virtual Template and is used to dynamically build an interface which will be used to terminate the EasyVPN clients on. This interface is called Virtual Access. We do not use any crypto map in this deployment and this is very useful in case that we do not want any crypto map on the interface.

```
R2(config)#crypto ipsec transform-set TS-RA esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#exi
```

On the EasyVPN server we need to configure ISAKMP policy and IPSec policy. Those policies are then used by ISAKMP and IPSec profile respectively. Those profiles are used to "catch" ISAKMP packets and start EasyVPN negotiation.

```
R2(config)#crypto ipsec profile DVTI
R2(ipsec-profile)#set transform-set TS-RA
R2(ipsec-profile)#set isakmp-profile IKE-RA
R2(ipsec-profile)#exi
```

The IPSec Profile specifies IPSec policies by attaching transform set to that profile. We can also attach ISAKMP Profile here but this is not necessary here as we have only one ISAKMP Profile configured on the router.

```
R2(config)#interface Virtual-Template1 type tunnel
R2(config-if)#ip unnumbered GigabitEthernet0/0
R2(config-if)#tunnel mode ipsec ipv4
```

```
R2(config-if)#tunnel protection ipsec profile DVTI
```

The Virtual Template interface must be a type of "tunnel" and has a mode of IPSec IPv4. This is crucial to configure that correctly as a default tunnel type is GRE. If we do not specify the Virtual Template type of tunnel, the default encapsulation is PPP and there is no way to configure "tunnel mode". Always check that using "show interface virtual-template 1" command.

The IP address is used from the G0/0 interface and finally there is IPSec profile attached to it for tunnel traffic encryption.

```
R2(config-if)#
```

```
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
```

```
R2(config-if)#exit
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Template1,
changed state to down
```

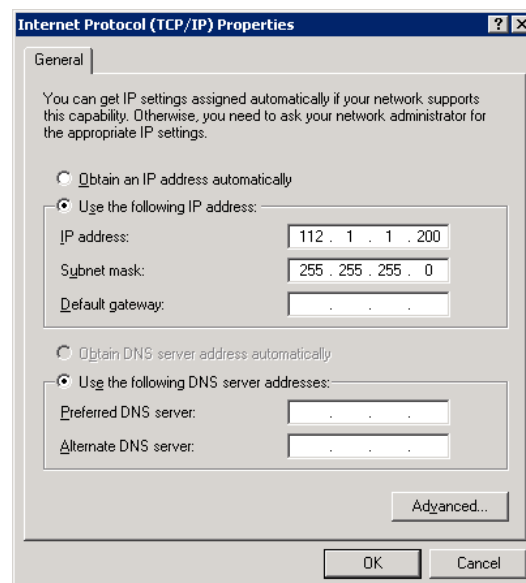
```
R2(config)#ip local pool RA-VPN 10.1.21.1 10.1.21.10
```

Finally we need to create a pool of IP addresses to serve to the clients and our Split Tunnel ACL.

```
R2(config)#access-list 124 permit ip 10.1.24.0 0.0.0.255 any
```

Step 2 Client PC configuration.

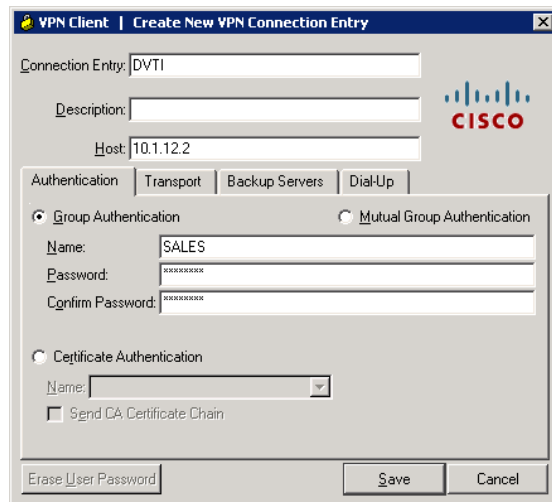
Configure IP address of 112.1.1.200/24 on the PC and add a route to reach R2.




```
c:\>route add 10.1.12.0 mask 255.255.255.0 112.1.1.1
```

Verification

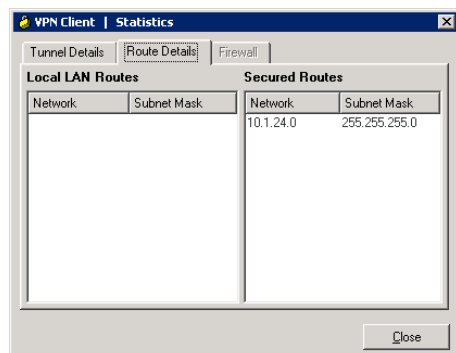
1. Run Cisco IPsec VPN client software and create a new connection entry.



2. Click connect and enter user's credentials.



3. VPN tunnel should be established and an appropriate network secured.



C:\>ping 10.1.24.4

Pinging 10.1.24.4 with 32 bytes of data:

Reply from 10.1.24.4: bytes=32 time=59ms TTL=254

Reply from 10.1.24.4: bytes=32 time=2ms TTL=254

Reply from 10.1.24.4: bytes=32 time=1ms TTL=254

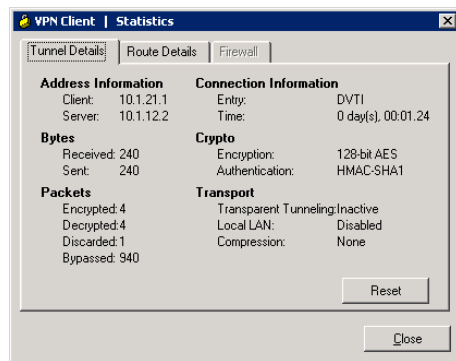
Reply from 10.1.24.4: bytes=32 time=2ms TTL=254

Ping statistics for 10.1.24.4:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 59ms, Average = 16ms



R2#

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up
```

Note that interface Virtual-Access2 is up but Virtual-Templat1 is down. This is because Virtual-Template is only used to build up Virtual-Access.

R2#sh int virtual-templatel

```
Virtual-Templat1 is down, line protocol is down
```

Hardware is Virtual Template interface

```
Interface is unnumbered. Using address of GigabitEthernet0/0 (10.1.12.2)
```

MTU 17940 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source UNKNOWN

```
Tunnel protocol/transport IPSEC/IP
```

```
Tunnel TOS/Traffic Class Configuration: test tos configuration (alt: 0x0), Tunnel TTL 255
```

Tunnel transport MTU 1500 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Tunnel protection via IPSec (profile "DVTI")

Last input never, output never, output hang never

Last clearing of "show interface" counters never

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
```

The interface Virtual-Template has correct tunnel protocol of IPSec/IP. Note that it has no tunnel source destination specified. This information will be derived from IPSec and used on Virtual-Access interface. In Remote Access VPNs we have many remote clients so that tunnel destination is always different.

R2#sh int Virtual-Access2

```
Virtual-Access2 is up, line protocol is up
Hardware is Virtual Access interface
Interface is unnumbered. Using address of GigabitEthernet0/0 (10.1.12.2)
MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL
Tunnel vaccess, cloned from Virtual-Template1
Vaccess status 0x0, loopback not set
Keepalive not set
Tunnel source 10.1.12.2, destination 112.1.1.200
Tunnel protocol/transport IPSEC/IP
Tunnel TOS/Traffic Class Configuration: test tos configuration (alt: 0x0), Tunnel TTL
255
Tunnel transport MTU 1427 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPSec (profile "DVTI")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  4 packets input, 240 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  4 packets output, 480 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
```

Virtual-Access interface has all information required to tunnel the traffic. Also note that MTU is automatically changed to lower value to accommodate IPSec headers.

R2#sh cry isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection
 K - Keepalives, N - NAT-traversal
 T - cTCP encapsulation, X - IKE Extended Authentication
 psk - Preshared key, rsig - RSA signature
 renc - RSA encryption
 IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1003	10.1.12.2	112.1.1.200		ACTIVE	aes	sha		2	23:57:19	CX

Engine-id:Conn-id = SW:3

IPv6 Crypto ISAKMP SA

R2#sh crypto ipsec sa

interface: Virtual-Access2

Crypto map tag: Virtual-Access2-head-0, local addr 10.1.12.2

protected vrf: (none)

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (10.1.21.1/255.255.255.255/0/0)

current_peer 112.1.1.200 port 1286

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

ICMP packets have been encrypted/decrypted. Note that Proxy ID is different for every EasyVPN client.

local crypto endpt.: 10.1.12.2, remote crypto endpt.: 112.1.1.200

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0

current outbound spi: 0xE0C449C7(3770960327)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x4675F596(1182135702)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2009, flow_id: Onboard VPN:9, sibling_flags 80000046, crypto map:

Virtual-Access2-head-0

sa timing: remaining key lifetime (k/sec): (4548296/3442)

```

    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0xE0C449C7(3770960327)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2010, flow_id: Onboard VPN:10, sibling_flags 80000046, crypto map:
Virtual-Access2-head-0
  sa timing: remaining key lifetime (k/sec): (4548296/3442)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```

R2#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.1.12.1 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.12.0/24 is directly connected, GigabitEthernet0/0
C       10.1.24.0/24 is directly connected, GigabitEthernet0/1
S       10.1.21.1/32 [1/0] via 112.1.1.200, Virtual-Access2
S*     0.0.0.0/0 [1/0] via 10.1.12.1

```

**Static route is injected to the routing table to reach remote client IP address.
This static route can be redistributed into dynamic routing protocol if RRI feature
is enabled.**

R2#sh ip int brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.1.12.2	YES	manual	up	up
GigabitEthernet0/1	10.1.24.2	YES	manual	up	up
Serial0/1/0	unassigned	YES	NVRAM	administratively down	down
Serial0/2/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet1/0	unassigned	YES	unset	administratively down	down

FastEthernet1/1	unassigned	YES	unset	administratively down	down
FastEthernet1/2	unassigned	YES	unset	administratively down	down
FastEthernet1/3	unassigned	YES	unset	administratively down	down
FastEthernet1/4	unassigned	YES	unset	administratively down	down
FastEthernet1/5	unassigned	YES	unset	administratively down	down
FastEthernet1/6	unassigned	YES	unset	administratively down	down
FastEthernet1/7	unassigned	YES	unset	administratively down	down
FastEthernet1/8	unassigned	YES	unset	administratively down	down
FastEthernet1/9	unassigned	YES	unset	administratively down	down
FastEthernet1/10	unassigned	YES	unset	administratively down	down
FastEthernet1/11	unassigned	YES	unset	administratively down	down
FastEthernet1/12	unassigned	YES	unset	administratively down	down
FastEthernet1/13	unassigned	YES	unset	administratively down	down
FastEthernet1/14	unassigned	YES	unset	administratively down	down
FastEthernet1/15	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	NVRAM	up	down
Virtual-Access1	unassigned	YES	unset	down	down
Virtual-Template1	10.1.12.2	YES	TFTP	down	down
Virtual-Access2	10.1.12.2	YES	TFTP	up	up

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

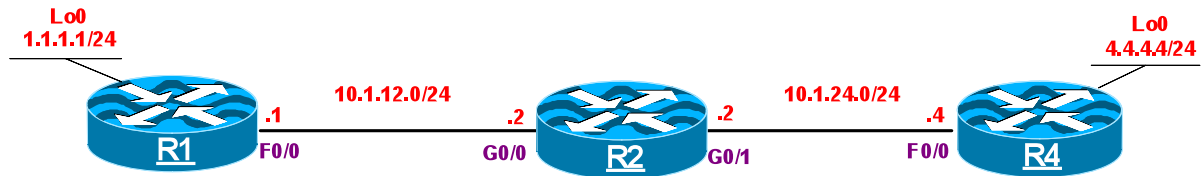
Gateway of last resort is 10.1.24.2 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.24.0 is directly connected, FastEthernet0/0

S* 0.0.0.0/0 [1/0] via 10.1.24.2

Lab 1.72. Reverse Route Injection (RRI)



Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 12
- R2's G0/1 and R4's F0/0 interface should be configured in VLAN 24
- Configure Telnet on all routers using password "cisco"

IP Addressing

Router	Interface	IP address
R1	F0/0	10.1.12.1/24
	Lo0	1.1.1.1/24
R2	G0/0	10.1.12.2/24
	G0/1	10.1.24.2/24
R4	F0/0	10.1.24.4/24
	Lo0	4.4.4.4/24

Task 1

Configure EIGRP AS 24 between R2 and R4 routers and advertise R4's loopback address. R1 should have only static default route pointing to R2.

Configure EasyVPN Server on R2 using Dynamic VTI interface. Use the following ISAKMP parameters:

- Phase 1:
 - Authentication: PSK
 - Encryption: AES
 - Hashing: SHA

- Group: 2
- Phase 2:
 - Encryption: AES 128
 - Hashing: SHA

Local user named “student1” with a password of “student123” should be able to connect to DVTI group using “cisco123” as a group password. The user should get an IP address from a pool of 10.1.21.1 – 10.1.21.10 addresses. After connection, only traffic destined to the network 4.4.4.0/24 (R4’s Loopback0 interface) should be encrypted.

Configure R1 as an EasyVPN Remote using client mode. The username and password should be configured on the client and used automatically to connect. Client should encrypt traffic sourced from R1’s Loopback0 interface.

Ensure that R1 can ping IP address of 4.4.4.4 using its Loopback0 interface by automatically injecting static route for EasyVPN Client’s IP address on R2 and redistribute ONLY that prefix into EIGRP.

Configuration

Complete these steps:

Step 1 R2 configuration.

Configure EIGRP AS 24 on R2’s G0/1.

```
R2(config)#router eigrp 24
R2(config-router)#no au
R2(config-router)#net 10.1.24.2 0.0.0.0
```

Configure EasyVPN Server on R2 using DVTI technology.

```
R2(config)#aaa new-model
R2(config)#aaa authentication login AUTH-LOCAL local
R2(config)#aaa authorization network AUTHOR-LOCAL local

R2(config)#username student password student123

R2(config)#crypto isakmp policy 5
R2(config-isakmp)#encr aes
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#exi
```



```

R2(config)#ip local pool RA-VPN 10.1.21.1 10.1.21.10

R2(config)#access-list 124 permit ip 4.4.4.0 0.0.0.255 any

R2(config)#crypto isakmp client configuration group DVTI
R2(config-isakmp-group)#key cisco123
R2(config-isakmp-group)#pool RA-VPN
R2(config-isakmp-group)#acl 124
R2(config-isakmp-group)#save-password
R2(config-isakmp-group)#exit

R2(config)#crypto isakmp profile IKE-RA
% A profile is deemed incomplete until it has match identity
statements
R2(conf-isa-prof)#match identity group DVTI
R2(conf-isa-prof)#client authentication list AUTH-LOCAL
R2(conf-isa-prof)#isakmp authorization list AUTHOR-LOCAL
R2(conf-isa-prof)#client configuration address respond
R2(conf-isa-prof)#virtual-template 1 ← do not forget about this!!!
R2(conf-isa-prof)#exit

R2(config)#crypto ipsec transform-set TS-RA esp-aes esp-sha-hmac

R2(cfg-crypto-trans)#crypto ipsec profile DVTI
R2(ipsec-profile)#set transform-set TS-RA
R2(ipsec-profile)#set isakmp-profile IKE-RA
R2(ipsec-profile)#exit

R2(config)#interface Virtual-Template1 type tunnel
R2(config-if)#ip unnumbered GigabitEthernet0/0
R2(config-if)#tunnel mode ipsec ipv4
R2(config-if)#tunnel protection ipsec profile DVTI
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Template1,
changed state to down
R2(config-if)#tunnel protection ipsec profile DVTI
R2(config-if)#exit
R2(config)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

```

Step 2 R4 configuration.

Configure EIGRP AS 24 on R4 and advertise its Loopback0 network.

```

R4(config)#router eigrp 24
R4(config-router)#no au
R4(config-router)#net 4.4.4.4 0.0.0.0
R4(config-router)#net 10.1.24.4 0.0.0.0
R4(config-router)#exit

```

```
R4(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 24: Neighbor 10.1.24.2
(FastEthernet0/0) is up: new adjacency
```

Step 3 R1 configuration.

Configure default static route on R1 pointing on R2. Then, configure EasyVPN Remote using client mode. Use appropriate interfaces to encrypt traffic sourced from Loopback0.

```
R1(config-if)#ip route 0.0.0.0 0.0.0.0 10.1.12.2

R1(config)#crypto ipsec client ezvpn EZ
R1(config-crypto-ezvpn)#connect auto
R1(config-crypto-ezvpn)#group DVTI key cisco123
R1(config-crypto-ezvpn)#mode client
R1(config-crypto-ezvpn)#peer 10.1.12.2
R1(config-crypto-ezvpn)#username student password student123
R1(config-crypto-ezvpn)#xauth userid mode local
R1(config-crypto-ezvpn)#exit

R1(config)#int lo0
R1(config-if)#crypto ipsec client ezvpn EZ inside

R1(config-if)#int f0/0
R1(config-if)#crypto ipsec client ezvpn EZ outside
R1(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exi
```

NOTE: this is not a solution yet!!! For full solution see rest of this task.

Verification

R1#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

```

1.0.0.0/24 is subnetted, 1 subnets
C      1.1.1.0 is directly connected, Loopback0
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.12.0/24 is directly connected, FastEthernet0/0
C      10.1.21.1/32 is directly connected, Loopback10000
S* 0.0.0.0/0 [1/0] via 10.1.12.2

```

← R1 has only default route

R1#sh cry ipsec client ezvpn

Easy VPN Remote Phase: 8

Tunnel name : EZ

Inside interface list: Loopback0

Outside interface: FastEthernet0/0

Current State: IPSEC_ACTIVE

Last Event: MTU_CHANGED

Address: 10.1.21.1 (applied on Loopback10000)

← Client got this IP address

Mask: 255.255.255.255

Save Password: Allowed

Split Tunnel List: 1

```

Address      : 4.4.4.0
Mask         : 255.255.255.0
Protocol     : 0x0
Source Port  : 0
Dest Port    : 0

```

Current EzVPN Peer: 10.1.12.2

R1#sh cry isakmp sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.2	10.1.12.1	QM_IDLE	1004	ACTIVE

IPv6 Crypto ISAKMP SA

R1#sh cry isakmp sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.
1004	10.1.12.1	10.1.12.2		ACTIVE	aes	sha		2	23:58:49	CX

Engine-id:Conn-id = SW:4

IPv6 Crypto ISAKMP SA

R1#sh cryp ipsec sa

```
interface: FastEthernet0/0
  Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.12.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.1.21.1/255.255.255.0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0)
current_peer 10.1.12.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

  No traffic has been sent through the tunnel yet.

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.12.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xD3960772(3549824882)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x732BF69F(1932261023)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2011, flow_id: NETGX:11, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
    sa timing: remaining key lifetime (k/sec): (4405245/3540)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xD3960772(3549824882)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2012, flow_id: NETGX:12, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
    sa timing: remaining key lifetime (k/sec): (4405245/3540)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:
```

outbound pcp sas:

R1#ping 4.4.4.4 so lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

.....

← Ping is not successful, see if traffic goes through the VPN

Success rate is 0 percent (0/5)

R1#sh cryp ipsec sa

interface: FastEthernet0/0

Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.12.1

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.21.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 10.1.12.2 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

Seems traffic is sent out thru the tunnel but is not returning

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.12.2

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xD3960772(3549824882)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x732BF69F(1932261023)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2011, flow_id: NETGX:11, sibling_flags 80000046, crypto map:

FastEthernet0/0-head-0

sa timing: remaining key lifetime (k/sec): (4405245/3511)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```

spi: 0xD3960772(3549824882)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2012, flow_id: NETGX:12, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4405244/3511)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

R2#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

4.0.0.0/24 is subnetted, 1 subnets
D      4.4.4.0 [90/156160] via 10.1.24.4, 00:02:13, GigabitEthernet0/1
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.1.12.0/24 is directly connected, GigabitEthernet0/0
C      10.1.24.0/24 is directly connected, GigabitEthernet0/1
S      10.1.21.1/32 [1/0] via 10.1.12.1, Virtual-Access2

```

R2 has a correct route back to the Client

R2#sh cry isak sa det

```

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.

1001  10.1.12.2         10.1.12.1      ACTIVE aes  sha    2    23:58:08 CX
      Engine-id:Conn-id = SW:1

```

IPv6 Crypto ISAKMP SA

R2#sh cry ips sa

interface: Virtual-Access2

Crypto map tag: Virtual-Access2-head-0, local addr 10.1.12.2

protected vrf: (none)

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (10.1.21.1/255.255.255.255/0/0)

current_peer 10.1.12.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

Packets came to R2 but has not been sent back

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.2, remote crypto endpt.: 10.1.12.1

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0

current outbound spi: 0x732BF69F(1932261023)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xD3960772(3549824882)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000046, crypto map:

Virtual-Access2-head-0

sa timing: remaining key lifetime (k/sec): (4601019/3484)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0x732BF69F(1932261023)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000046, crypto map:

Virtual-Access2-head-0

sa timing: remaining key lifetime (k/sec): (4601020/3484)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcg sas:

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

4.0.0.0/24 is subnetted, 1 subnets

C 4.4.4.0 is directly connected, Loopback0

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.24.0 is directly connected, FastEthernet0/0

R4 has no clue about EasyVPN Client's IP address. That's not good :-)

To make it work we need to send routing information over to R4. We could NOT just simply redistribute that static route because we are not allowed to. To allow R2 redistribute that route into EIGRP we need a feature called RRI. This can be configured using "set reverse-route" under the IPsec Profile or "reverse-route" under the dynamic crypto map (in case you use it instead of DVTI). In addition to that, we're asked to redistribute ONLY this prefix. To do that we'll need a route map where we'll match prefixes based on some conditions. Most natural (and easy) way to do that is to use route tagging.

Configuration

Complete these steps:

Step 4 R2 RRI configuration.

```
R2(config)#crypto ipsec profile DVTI
```

```
R2(ipsec-profile)#set reverse-route tag 124
```

This will remove previously installed VPN routes and SAs

```
R2(ipsec-profile)#exit
```

```
R2(config)#route-map DVTI-RRI permit 10
```

```
R2(config-route-map)#match tag 124
```



```

R2(config-route-map)#exi

R2(config)#router eigrp 24
R2(config-router)#redistribute static route-map DVTI-RR1
R2(config-router)#ex

```

Verification

Reconnect to EasyVPN Server to refresh the configuration.

R1#cle cryp isak

```

%CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client) User=student Group=DVTI
Client_public_addr=10.1.12.1 Server_public_addr=10.1.12.2
R1#
%CRYPTO-6-EZVPN_CONNECTION_UP: (Client) User=student Group=DVTI
Client_public_addr=10.1.12.1 Server_public_addr=10.1.12.2
Assigned_client_addr=10.1.21.2

```

R1#sh cry ipsec client ezvpn

```

Easy VPN Remote Phase: 8

Tunnel name : EZ
Inside interface list: Loopback0
Outside interface: FastEthernet0/0
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Address: 10.1.21.2 (applied on Loopback10000) ← This time, client got different IP
address
Mask: 255.255.255.255
Save Password: Allowed
Split Tunnel List: 1
    Address      : 4.4.4.0
    Mask         : 255.255.255.0
    Protocol     : 0x0
    Source Port  : 0
    Dest Port    : 0
Current EzVPN Peer: 10.1.12.2

```

R1#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route

```

- o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

```

1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.12.0/24 is directly connected, FastEthernet0/0
C    10.1.21.2/32 is directly connected, Loopback10000
S*  0.0.0.0/0 [1/0] via 10.1.12.2

```

R1#sh cryp isak sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.12.2	10.1.12.1	QM_IDLE	1005	ACTIVE
10.1.12.2	10.1.12.1	MM_NO_STATE	1004	ACTIVE (deleted)

IPv6 Crypto ISAKMP SA

R1#sh cryp ips sa

interface: FastEthernet0/0

Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.12.1

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.21.2/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 10.1.12.2 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.12.2

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0xED619BF8(3982597112)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xA8AA6AA3(2829740707)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2013, flow_id: NETGX:13, sibling_flags 80000046, crypto map:

FastEthernet0/0-head-0

sa timing: remaining key lifetime (k/sec): (4523368/3557)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

```
inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xED619BF8(3982597112)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2014, flow_id: NETGX:14, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4523368/3557)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R1#ping 4.4.4.4 so lo0

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Ping is successful. So far so good.

R1#sh cryp ips sa

```
interface: FastEthernet0/0
  Crypto map tag: FastEthernet0/0-head-0, local addr 10.1.12.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.21.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.1.12.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
```

ICMP packets are encrypted and decrypted

```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```

local crypto endpt.: 10.1.12.1, remote crypto endpt.: 10.1.12.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xED619BF8(3982597112)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xA8AA6AA3(2829740707)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2013, flow_id: NETGX:13, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
    sa timing: remaining key lifetime (k/sec): (4523367/3535)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0xED619BF8(3982597112)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2014, flow_id: NETGX:14, sibling_flags 80000046, crypto map:
FastEthernet0/0-head-0
    sa timing: remaining key lifetime (k/sec): (4523367/3535)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```

R2#sh ip route

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

```

```

Gateway of last resort is not set

```

```

4.0.0.0/24 is subnetted, 1 subnets
D      4.4.4.0 [90/156160] via 10.1.24.4, 00:05:40, GigabitEthernet0/1
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.1.12.0/24 is directly connected, GigabitEthernet0/0

```

```
C      10.1.24.0/24 is directly connected, GigabitEthernet0/1
S      10.1.21.2/32 [1/0] via 10.1.12.1, Virtual-Access2
```

R2 has a route to the client's IP address

R2#sh ip route 10.1.21.2

```
Routing entry for 10.1.21.2/32
  Known via "static", distance 1, metric 0
  Tag 124
  Redistributing via eigrp 24
  Advertised by eigrp 24 route-map DVTI-RR1
  Routing Descriptor Blocks:
  * 10.1.12.1, via Virtual-Access2
    Route metric is 0, traffic share count is 1
    Route tag 124    ← The prefix is tagged
```

R2#sh cry isak sa

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.1.12.2    10.1.12.1    QM_IDLE       1002 ACTIVE

IPv6 Crypto ISAKMP SA
```

R2#sh cry ips sa

```
interface: Virtual-Access2
  Crypto map tag: Virtual-Access2-head-0, local addr 10.1.12.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.1.21.2/255.255.255.255/0/0)
current_peer 10.1.12.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.12.2, remote crypto endpt.: 10.1.12.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0xA8AA6AA3(2829740707)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xED619BF8(3982597112)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046, crypto map:
Virtual-Access2-head-0
```

```
sa timing: remaining key lifetime (k/sec): (4492064/3492)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xA8AA6AA3(2829740707)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046, crypto map:
Virtual-Access2-head-0
sa timing: remaining key lifetime (k/sec): (4492064/3492)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R2#sh ip protocol

Routing Protocol is "eigrp 24"

```
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
```

Redistributing: static, eigrp 24

```
EIGRP NSF-aware route hold timer is 240s
Automatic network summarization is not in effect
Maximum path: 4
```

Routing for Networks:

```
10.1.24.2/32
```

Routing Information Sources:

Gateway	Distance	Last Update
10.1.24.4	90	00:06:13

Distance: internal 90 external 170

R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2

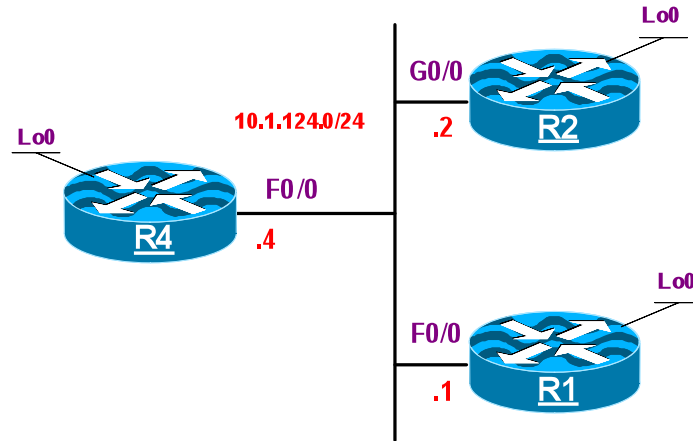
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```
4.0.0.0/24 is subnetted, 1 subnets
C      4.4.4.0 is directly connected, Loopback0
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.24.0/24 is directly connected, FastEthernet0/0
D EX   10.1.21.2/32 [170/26882560] via 10.1.24.2, 00:02:06, FastEthernet0/0
```

See the redistributed route on R4.

Lab 1.73. Call Admission Control for IKE



Lab Setup

- R1's F0/0, R2's G0/0 and R4's F0/0 interface should be configured in VLAN 124
- Configure Telnet on all routers using password "cisco"

IP Addressing

Router	Interface	IP address
R1	F0/0	10.1.124.1/24
	Lo0	1.1.1.1/24
R2	G0/0	10.1.124.2/24
	Lo0	2.2.2.2/24
R4	F0/0	10.1.124.4/24
	Lo0	4.4.4.4/24

Task 1

Configure basic Site to Site IPSec VPN (using Static VTI) between R1/R2 and R4 using the following policy:

ISAKMP Policy	IPSec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Encryption: 3DES	Hash: MD5
Hash: MD5	
DH Group: 2	
PSK for R1: R1-KEY	
PSK for R2: R2-KEY	

Configure IKE protection on R4 so that it cannot accept more than 10 IKE SA's negotiations at the time and no more than 1 IKE SA to be established in total.



Using Call Admission Control (CAC) feature for IKE allows router resource protection and prevents against DoS attacks using IKE protocol. You as an administrator can configure two things:

- (1) Total limit of IKE session which can be terminated on the router ("crypto call admission limit ike sa" command)*
- (2) Limit of IKE negotiations at the same time ("crypto call admission limit ike in-negotiation-sa" command).*

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)#encr 3des
R4(config-isakmp)#hash md5
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#group 2
R4(config-isakmp)#exit

R4(config)#crypto isakmp key R1-KEY address 10.1.124.1
R4(config)#crypto isakmp key R2-KEY address 10.1.124.2

R4(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R4(cfg-crypto-trans)#exit

R4(config)#crypto ipsec profile PROF
R4(ipsec-profile)#set transform-set TS
```

```
R4(ipsec-profile)#exi

R4(config)#interface Tunnel41
R4(config-if)#ip address 172.16.41.4 255.255.255.0
R4(config-if)#tunnel source FastEthernet0/0
R4(config-if)#tunnel destination 10.1.124.1
R4(config-if)#tunnel mode ipsec ipv4
R4(config-if)#tunnel protection ipsec profile PROF

R4(config-if)#interface Tunnel42
R4(config-if)#ip address 172.16.42.4 255.255.255.0
R4(config-if)#tunnel source FastEthernet0/0
R4(config-if)#tunnel destination 10.1.124.2
R4(config-if)#tunnel mode ipsec ipv4
R4(config-if)#tunnel protection ipsec profile PROF
R4(config-if)#exi
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON

R4(config)#crypto call admission limit ike sa 1
R4(config)#crypto call admission limit ike in-negotiation-sa 10
```

Step 2 R1 configuration.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exi

R1(config)#crypto isakmp key R1-KEY address 10.1.124.4

R1(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#exi

R1(config)#crypto ipsec profile PROF
R1(ipsec-profile)#set transform-set TS
R1(ipsec-profile)#exi

R1(config)#interface Tunnel14
R1(config-if)#ip address 172.16.41.1 255.255.255.0
R1(config-if)#tunnel source FastEthernet0/0
R1(config-if)#tunnel destination 10.1.124.4
R1(config-if)#tunnel mode ipsec ipv4
R1(config-if)#tunnel protection ipsec profile PROF
R1(config-if)#
%CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R1(config-if)#exi
R1(config)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel14, changed
state to up
```

Step 3 R2 configuration.

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encr 3des
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#exi

R2(config)#crypto isakmp key R2-KEY address 10.1.124.4

R2(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R2(cfg-crypto-trans)#exi

R2(config)#crypto ipsec profile PROF
R2(ipsec-profile)#set transform-set TS
R2(ipsec-profile)#exi

R2(config)#interface Tunnel24
R2(config-if)#ip address 172.16.42.2 255.255.255.0
R2(config-if)#tunnel source GigabitEthernet0/0
R2(config-if)#tunnel destination 10.1.124.4
R2(config-if)#tunnel mode ipsec ipv4
R2(config-if)#tunnel protection ipsec profile PROF
R2(config-if)#

%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Verification

R1#sh cry isak sa det

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	Status	Encr	Hash	Auth	DH	Lifetime	Cap.

1006	10.1.124.1	10.1.124.4		ACTIVE	3des	md5	psk	2	23:54:00	
Engine-id:Conn-id = SW:6										

IPv6 Crypto ISAKMP SA

R1#sh cry ips sa

```
interface: Tunnel14
  Crypto map tag: Tunnel14-head-0, local addr 10.1.124.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.1.124.4 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 10.1.124.1, remote crypto endpt.: 10.1.124.4
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x8B215125(2334216485)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x3118577C(823678844)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2019, flow_id: NETGX:19, sibling_flags 80000046, crypto map: Tunnel14-
head-0
  sa timing: remaining key lifetime (k/sec): (4403231/3546)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x8B215125(2334216485)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2020, flow_id: NETGX:20, sibling_flags 80000046, crypto map: Tunnel14-
head-0
  sa timing: remaining key lifetime (k/sec): (4403231/3546)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

The IPSec tunnel is up and running between R1 and R4. Let's send traffic through the tunnel.

R1#ping 172.16.41.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.41.4, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R1#sh cry ips sa

interface: Tunnel14

Crypto map tag: Tunnel14-head-0, local addr 10.1.124.1

protected vrf: (none)

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 10.1.124.4 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

Traffic has been encrypted/decrypted.

local crypto endpt.: 10.1.124.1, remote crypto endpt.: 10.1.124.4

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0

current outbound spi: 0x8B215125(2334216485)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x3118577C(823678844)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 2019, flow_id: NETGX:19, sibling_flags 80000046, crypto map: Tunnel14-

head-0

sa timing: remaining key lifetime (k/sec): (4403230/3531)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

```
spi: 0x8B215125(2334216485)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2020, flow_id: NETGX:20, sibling_flags 80000046, crypto map: Tunnel14-
head-0
sa timing: remaining key lifetime (k/sec): (4403230/3531)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

R1#sh cry sess

Crypto session current status

```
Interface: Tunnel14
Session status: UP-ACTIVE
Peer: 10.1.124.4 port 500
IKE SA: local 10.1.124.1/500 remote 10.1.124.4/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

R2#sh cryp isak sa

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	status
10.1.124.4	10.1.124.2	MM_NO_STATE	0	ACTIVE (deleted)

IPv6 Crypto ISAKMP SA

R2 cannot negotiate ISAKMP SA.

R2#sh cry ips sa

interface: Tunnel24

Crypto map tag: Tunnel24-head-0, local addr 10.1.124.2

```
protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.1.124.4 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.1.124.2, remote crypto endpt.: 10.1.124.4
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

There are no SPIs for IPSec.

R2#sh cry sess

```
Crypto session current status
```

```
Interface: Tunnel24
```

```
Session status: DOWN-NEGOTIATING
```

```
Peer: 10.1.124.4 port 500
```

```
IKE SA: local 10.1.124.2/500 remote 10.1.124.4/500 Inactive
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
```

```
Active SAs: 0, origin: crypto map
```

Note that R2 cannot establish IKE SA. See the output on R4's console. It clearly states that IKE request has been denied by CEC feature. Note that it works both ways, so that R4 cannot initiate IKE session towards R2 as well.

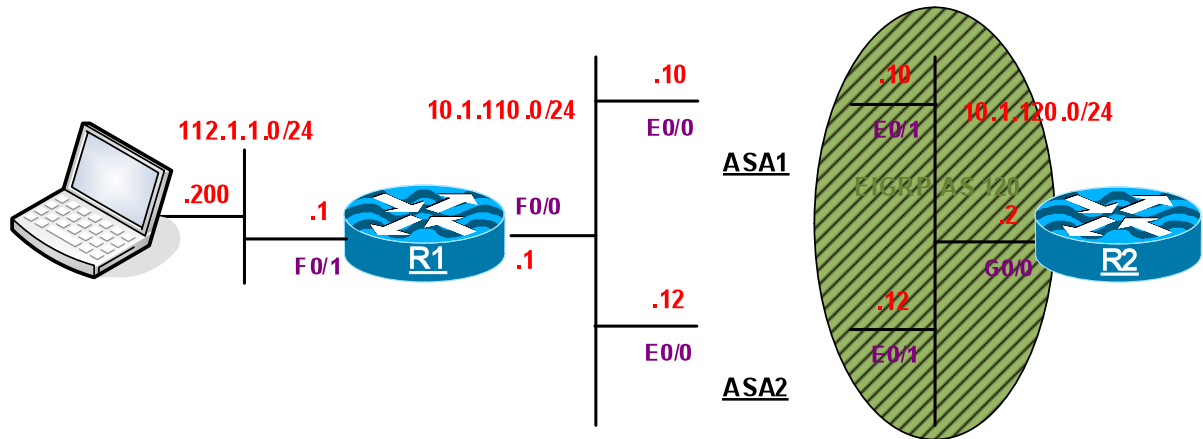
```
R4#
```

```
%CRYPTO-4-IKE_DENY_SA_REQ: IKE denied an INCOMING SA request from 10.1.124.2 to
10.1.124.4 due to IKE SA LIMIT REACHED
```

```
R4#
```

```
%CRYPTO-4-IKE_DENY_SA_REQ: IKE denied an OUTGOING SA request from 10.1.124.4 to
10.1.124.2 due to IKE SA LIMIT REACHED
```

Lab 1.74. IPSec Load Balancing (ASA Cluster)



Lab Setup

- R1's F0/0, ASA1's E0/0 and ASA2's E0/0 interface should be configured in VLAN 110
- R2's G0/0, ASA1's E0/1 and ASA2's E0/1 interface should be configured in VLAN 120
- R1's F0/1 and PC NIC (SW3 F0/15) should be configured in VLAN 112
- Configure Telnet on all routers using password "cisco"
- Configure EIGRP AS 120 in VLAN 120

IP Addressing

Device/Hostname	Interface (ifname, sec)	IP address
R1	F0/0	10.1.110.1/24
	F0/1	112.1.1.1/24
R2	G0/0	10.1.120.2/24
ASA1	E0/0 (Outside, Sec lvl 0)	10.1.110.10/24
	E0/1 (Inside, Sec lvl 100)	10.1.120.10/24
ASA2	E0/0 (Outside, Sec lvl 0)	10.1.110.12/24
	E0/1 (Inside, Sec lvl 100)	10.1.120.12/24
PC	NIC	112.1.1.200/24

Task 1

Configure EasyVPN Server on ASA1/ASA2 VPN Cluster. The ASA1 should have a Master role in the cluster and connection between cluster members should be encrypted and authenticated using key of “cisco123”. Use the following ISAKMP parameters:

- Phase 1:
 - Authentication: PSK
 - Encryption: 3DES
 - Hashing: SHA
 - Group: 2
- Phase 2:
 - Encryption: 3DES
 - Hashing: SHA
 - PSK Group 2

Local user named “student1” with a password of “student123” should be able to connect to the cluster using IP address of 10.1.110.254 and a group SALES with a password of “cisco123”. The user should get an IP address from a pool of 10.1.21.1 – 10.1.21.254 addresses and the following additional information:

- DNS Server: 10.1.120.5
- WINS Server: 10.1.120.6
- Domain name: micronicstraining.com

After connection, only traffic destined to the network 10.1.120.0/24 should be encrypted. Ensure that R2 router gets information about connected user’s IP address using EIGRP routing updates.



If you have a remote access VPN in which you are using two or more ASA devices connected on the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called load balancing. To enable that you must group together logically two or more ASA devices on the same LAN and Internet connection into a virtual cluster.

All devices in the virtual cluster carry session loads. Load balancing directs session traffic to the least loaded device in the cluster, thus distributing the load among all devices.

One device in the virtual cluster has a Master role and directs incoming traffic to the other devices, called Secondary devices. The Master monitors all devices in the cluster, keeps track of how busy each is, and distributes the session load accordingly. The Master role is not tied to a physical device; it can shift among devices. For example, if the current Master fails, one of the secondary devices in the cluster takes over that role and immediately becomes the new Master.

The virtual cluster appears to outside clients as a single virtual cluster IP address. This IP address belongs to the current Master. When a VPN client is attempting to connect to the cluster, the Master sends back to the client the public IP address of the least-loaded available host in the cluster. In a second step, the client connects directly to that host.

If a machine in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The Master then directs these connections to another active device in the cluster. If the Master itself fails, another device in the cluster immediately takes over as the new Master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is up and available.

Configuration

Complete these steps:

Step 1 ASA1 IPSec configuration.

*First we need to configure EasyVPN Server on both devices.
The configuration is typical and has been described in
Remote Access VPN section of the work book.*

```
ASA1(config)# crypto isakmp enable outside
ASA1(config)# crypto isakmp policy 10
ASA1(config-isakmp-policy)# auth pre-share
ASA1(config-isakmp-policy)# encr 3des
ASA1(config-isakmp-policy)# hash sha
ASA1(config-isakmp-policy)# group 2
ASA1(config-isakmp-policy)# exit

ASA1(config)# ip local pool VPN-CLIENTS 10.1.21.1-10.1.21.254 mask
255.255.255.0

ASA1(config)# access-list ST permit ip 10.1.120.0 255.255.255.0 any

ASA1(config)# group-policy SALES-POLICY internal
```

```
ASA1(config)# group-policy SALES-POLICY attributes
ASA1(config-group-policy)# vpn-tunnel-protocol ipsec
ASA1(config-group-policy)# dns-server value 10.1.120.5
ASA1(config-group-policy)# wins-server value 10.1.120.6
ASA1(config-group-policy)# default-domain value
micronicstraining.com
ASA1(config-group-policy)# split-tunnel-policy tunnelspecified
ASA1(config-group-policy)# split-tunnel-network-list value ST
ASA1(config-group-policy)# exit

ASA1(config)# tunnel-group SALES type remote-access
ASA1(config)# tunnel-group SALES ipsec-attributes
ASA1(config-tunnel-ipsec)# pre-shared-key cisco123
ASA1(config-tunnel-ipsec)# exit

ASA1(config)# tunnel-group SALES general-attributes
ASA1(config-tunnel-general)# default-group-policy SALES-POLICY
ASA1(config-tunnel-general)# address-pool VPN-CLIENTS
ASA1(config-tunnel-general)# exit

ASA1(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac

ASA1(config)# crypto dynamic-map DYN-CMAP 10 set pfs group2
ASA1(config)# crypto dynamic-map DYN-CMAP 10 set transform-set TSET
ASA1(config)# crypto dynamic-map DYN-CMAP 10 set reverse-route
ASA1(config)# crypto map ENCRYPT_OUT 10 ipsec-isakmp dynamic DYN-
CMAP
ASA1(config)# crypto map ENCRYPT_OUT interface Outside
ASA1(config)#

ASA1(config)# access-list TO-EIGRP standard permit 10.1.21.0
255.255.255.0
ASA1(config)# route-map REDIST-EIGRP permit 10
ASA1(config-route-map)# match ip address TO-EIGRP
ASA1(config-route-map)# exit

ASA1(config)# router eigrp 120
ASA1(config-router)# redistribute static route-map REDIST-EIGRP
metric 10000 1000 255 1 1500
ASA1(config-router)# exit

ASA1(config)# username student1 password student123
```

Step 2 ASA2 IPSec configuration.

The EasyVPN Server configuration must be exactly the same on both devices.

```
ASA2(config)# crypto isakmp enable outside
```

```
ASA2(config)# crypto isakmp policy 10
ASA2(config-isakmp-policy)# auth pre-share
ASA2(config-isakmp-policy)# encr 3des
ASA2(config-isakmp-policy)# hash sha
ASA2(config-isakmp-policy)# group 2
ASA2(config-isakmp-policy)# exit

ASA2(config)# ip local pool VPN-CLIENTS 10.1.21.1-10.1.21.254 mask
255.255.255.0

ASA2(config)# access-list ST permit ip 10.1.120.0 255.255.255.0 any

ASA2(config)# group-policy SALES-POLICY internal
ASA2(config)# group-policy SALES-POLICY attributes
ASA2(config-group-policy)# vpn-tunnel-protocol ipsec
ASA2(config-group-policy)# dns-server value 10.1.120.5
ASA2(config-group-policy)# wins-server value 10.1.120.6
ASA2(config-group-policy)# default-domain value
micronicstraining.com
ASA2(config-group-policy)# split-tunnel-policy tunnelspecified
ASA2(config-group-policy)# split-tunnel-network-list value ST
ASA2(config-group-policy)# exit

ASA2(config)# tunnel-group SALES type remote-access
ASA2(config)# tunnel-group SALES ipsec-attributes
ASA2(config-tunnel-ipsec)# pre-shared-key cisco123
ASA2(config-tunnel-ipsec)# exit

ASA2(config)# tunnel-group SALES general-attributes
ASA2(config-tunnel-general)# default-group-policy SALES-POLICY
ASA2(config-tunnel-general)# address-pool VPN-CLIENTS
ASA2(config-tunnel-general)# exit

ASA2(config)# crypto ipsec transform-set TSET esp-3des esp-sha-hmac

ASA2(config)# crypto dynamic-map DYN-CMAP 10 set pfs group2
ASA2(config)# crypto dynamic-map DYN-CMAP 10 set transform-set TSET
ASA2(config)# crypto dynamic-map DYN-CMAP 10 set reverse-route

ASA2(config)# crypto map ENCRYPT_OUT 10 ipsec-isakmp dynamic DYN-
CMAP
ASA2(config)# crypto map ENCRYPT_OUT interface Outside

ASA2(config)# access-list TO-EIGRP standard permit 10.1.21.0
255.255.255.0
ASA2(config)# route-map REDIST-EIGRP permit 10
ASA2(config-route-map)# match ip address TO-EIGRP
ASA2(config-route-map)# exit
ASA2(config)# router eigrp 120
ASA2(config-router)# redistribute static route-map REDIST-EIGRP
```

```
metric 10000 1000 255 1 1500
```

```
ASA2(config-router)# exit
```

```
ASA2(config)# username student1 password student123
```

Step 3 ASA1 IPSec clustering configuration.

```
ASA1(config)# cry isakmp enable inside
```

Devices in the cluster communicate with each other using encrypted tunnel when "cluster encryption" is enabled. This tunnel is a regular ISAKMP SA authenticated with a "cluster key". We need to provide a Virtual IP address of the cluster which will be used by EasyVPN clients as a tunnel endpoint.

The priority value is a number between 1 and 10 which dictates which device will become a Master. Higher number wins. Finally we need to enable clustering for each cluster member by issuing "participate" command.

```
ASA1(config)# vpn load-balancing
```

```
ASA1(config-load-balancing)# cluster ip add 10.1.110.254
```

```
ASA1(config-load-balancing)# cluster key cisco123
```

```
ASA1(config-load-balancing)# cluster encryption
```

```
ASA1(config-load-balancing)# priority 10
```

```
ASA1(config-load-balancing)# participate
```

```
ASA1(config-load-balancing)# exit
```

Step 4 ASA2 IPSec clustering configuration.

```
ASA2(config)# cry isakmp enable inside
```

```
ASA2(config)# vpn load-balancing
```

```
ASA2(config-load-balancing)# cluster ip add 10.1.110.254
```

```
ASA2(config-load-balancing)# cluster key cisco123
```

```
ASA2(config-load-balancing)# cluster encryption
```

```
ASA2(config-load-balancing)# priority 5
```

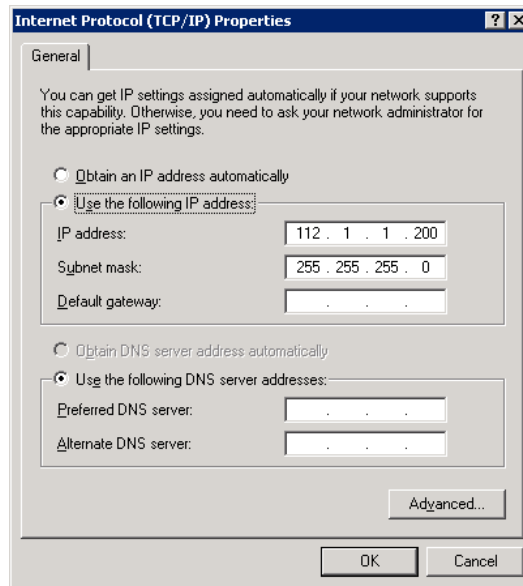
```
ASA2(config-load-balancing)# participate
```

```
ASA2(config-load-balancing)# exit
```

Step 5 Routing on R1.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.110.254
```

Step 6 Client PC configuration.



```
c:\>route add 10.1.110.0 mask 255.255.255.0 112.1.1.1
```

Verification

```
ASA1(config)# sh vpn load-balancing
```

```
Status:      enabled
Role:        Master
Failover:    n/a
Encryption:  enabled
Cluster IP:  10.1.110.254
Peers:       1
```

Public IP	Role	Pri	Model	Load (%)		Sessions	
				IPSec	SSL	IPSec	SSL
* 10.1.110.10	Master	10	ASA-5510	0	0	0	0
10.1.110.12	Backup	5	ASA-5510	0	0	0	0

As we see our ASA1 has become Master for this virtual cluster. This is because of higher priority.

```
ASA1(config)# sh cry isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 10.1.120.12
   Type    : L2L           Role    : responder
```

Rekey : no State : MM_ACTIVE

Master device has ISAKMP SA set up with other devices. Note that this SA has been established using Main Mode with IP addresses from private (inside) network.

ASA2(config)# sh vpn load-balancing

Status: enabled
 Role: Backup
 Failover: n/a
 Encryption: enabled
 Cluster IP: 10.1.110.254
 Peers: 1

Public IP	Role	Pri	Model	Load (%)		Sessions	
				IPSec	SSL	IPSec	SSL
* 10.1.110.12	Backup	5	ASA-5510	0	0	0	0
10.1.110.10	Master	10	ASA-5510	n/a	n/a	n/a	n/a

Same information is on other device. The ASA2 is in Backup role.

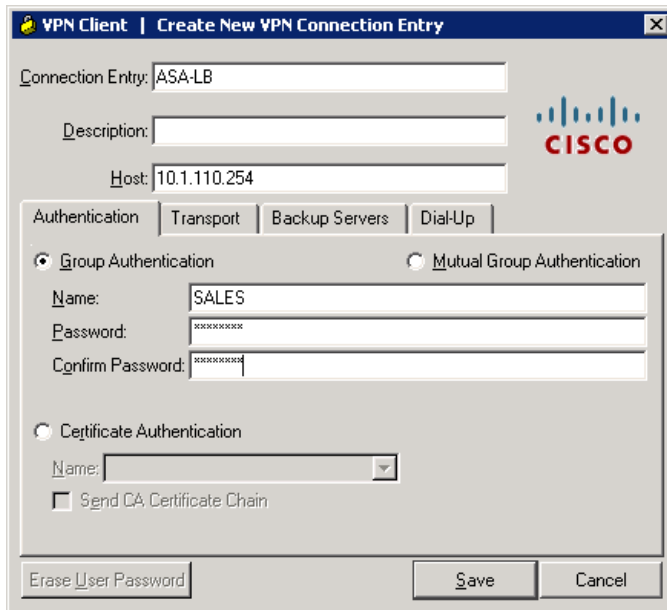
ASA2(config)# sh cry isak sa

Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 1

1 IKE Peer: 10.1.120.10

Type	: L2L	Role	: initiator
Rekey	: no	State	: MM_ACTIVE

Configure a new connection in Cisco VPN Client.



VPN Client | Create New VPN Connection Entry

Connection Entry: ASA-LB

Description:

Host: 10.1.110.254

Authentication | Transport | Backup Servers | Dial-Up

☒ Group Authentication ☐ Mutual Group Authentication

Name: SALES

Password: xxxxxxxx

Confirm Password: xxxxxxxx

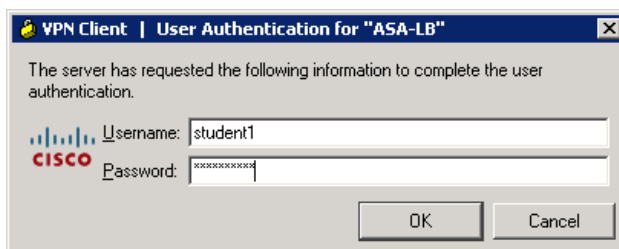
☐ Certificate Authentication

Name:

☐ Send CA Certificate Chain

Erase User Password Save Cancel

Authenticate using local user name.



VPN Client | User Authentication for "ASA-LB"

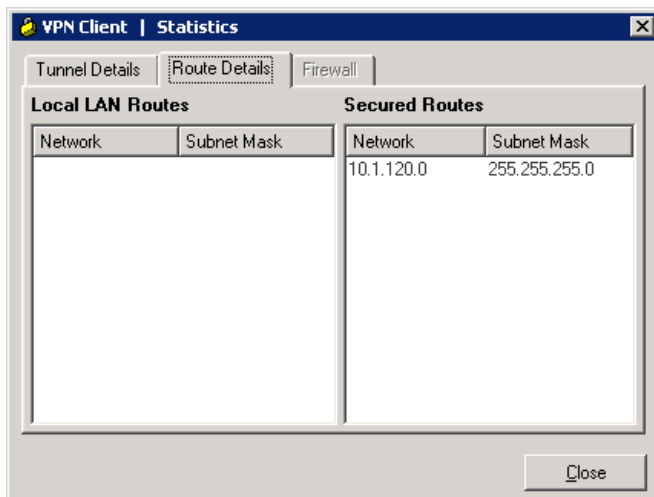
The server has requested the following information to complete the user authentication.

Username: student1

Password: xxxxxxxx

OK Cancel

Check if traffic to the desired network is to be encrypted.



VPN Client | Statistics

Tunnel Details | Route Details | Firewall

Local LAN Routes		Secured Routes	
Network	Subnet Mask	Network	Subnet Mask
		10.1.120.0	255.255.255.0

Close

c:\ACS PC>ping 10.1.120.2

Pinging 10.1.120.2 with 32 bytes of data:


```
Reply from 10.1.120.2: bytes=32 time=14ms TTL=255
```

```
Reply from 10.1.120.2: bytes=32 time=1ms TTL=255
```

```
Reply from 10.1.120.2: bytes=32 time=1ms TTL=255
```

```
Reply from 10.1.120.2: bytes=32 time=1ms TTL=255
```

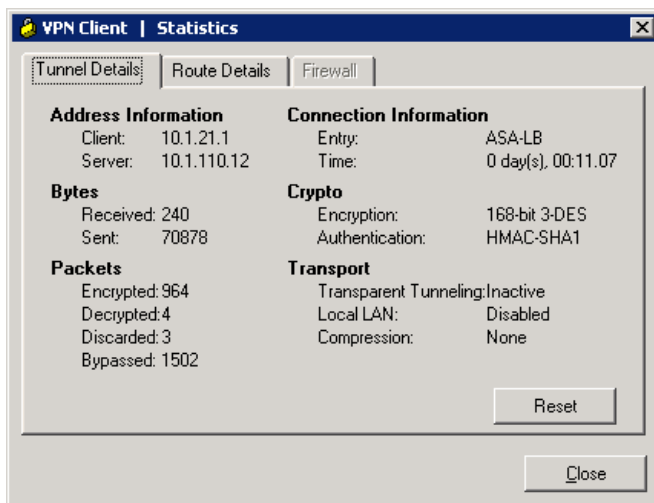
Ping statistics for 10.1.120.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 14ms, Average = 4ms

Tunnel is established and traffic is going through it.



ASA1(config)# sh vpn load-balancing

```
Status:      enabled
Role:        Master
Failover:    n/a
Encryption:  enabled
Cluster IP:  10.1.110.254
Peers:       1
```

Public IP	Role	Pri	Model	Load (%)		Sessions	
				IPSec	SSL	IPSec	SSL
* 10.1.110.10	Master	10	ASA-5510	0	0	0	0
10.1.110.12	Backup	5	ASA-5510	0	0	1	0

We see one IPSec connection on the Backup device.

ASA1(config)# sh crypto isakmp sa

Active SA: 1 ← Only one ISAKMP SA, meaning the client's connection has landed on ASA2

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

```
1  IKE Peer: 10.1.120.12
    Type      : L2L           Role      : responder
    Rekey     : no           State     : MM_ACTIVE
```

ASA1(config)# sh crypto ipsec sa

interface: **inside**

Crypto map tag: __vpn-lb-crypto-map, seq num: 65534, local addr: 10.1.120.10

```
access-list vpnlb-10.1.120.12 permit ip host 10.1.120.10 host 10.1.120.12
local ident (addr/mask/prot/port): (10.1.120.10/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.1.120.12/255.255.255.255/0/0)
current_peer: 10.1.120.12
```

```
#pkts encaps: 547, #pkts encrypt: 547, #pkts digest: 547
#pkts decaps: 529, #pkts decrypt: 529, #pkts verify: 529
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 547, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

local crypto endpt.: 10.1.120.10, remote crypto endpt.: 10.1.120.12

path mtu 1500, ipsec overhead 58, media mtu 1500

current outbound spi: 66A95179

inbound esp sas:

```
spi: 0x6D983B72 (1838693234)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: __vpn-lb-crypto-map
sa timing: remaining key lifetime (kB/sec): (3914973/28268)
IV size: 8 bytes
replay detection support: Y
```

Anti replay bitmap:

```
0xFFFFFFFF 0xFFFFFFFF
```

outbound esp sas:

```
spi: 0x66A95179 (1722372473)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: __vpn-lb-crypto-map
sa timing: remaining key lifetime (kB/sec): (3914967/28268)
IV size: 8 bytes
replay detection support: Y
```

Anti replay bitmap:

```
0x00000000 0x00000001
```

The Master ASA establishes IPSec SA with Backup ASA only. There is no IPSec SA with the client.

ASA1(config)# sh route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is 10.1.110.1 to network 0.0.0.0

```
C    10.1.110.0 255.255.255.0 is directly connected, outside
C    10.1.120.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.1.110.1, outside
```

ASA2(config)# sh vpn load-balancing

```
Status:      enabled
Role:        Backup
Failover:    n/a
Encryption:  enabled
Cluster IP:  10.1.110.254
Peers:       1
```

Public IP	Role	Pri	Model	Load (%)		Sessions	
				IPSec	SSL	IPSec	SSL
* 10.1.110.12	Backup	5	ASA-5510	0	0	1	0
10.1.110.10	Master	10	ASA-5510	n/a	n/a	n/a	n/a

ASA2(config)# sh crypto isakmp sa

Active SA: 2

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 2

```
1  IKE Peer: 10.1.120.10
   Type    : L2L           Role    : initiator
   Rekey    : no           State   : MM_ACTIVE

2  IKE Peer: 112.1.1.200
   Type    : user          Role    : responder
   Rekey    : no           State   : AM_ACTIVE
```

Here's the client's connection. This is because the Master redirects IKE to the backup peer by default.

ASA2(config)# sh crypto ipsec sa

```
interface: outside
  Crypto map tag: DYN-CMAP, seq num: 10, local addr: 10.1.110.12

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.1.21.1/255.255.255.255/0/0)
  current_peer: 112.1.1.200, username: student1
  dynamic allocated peer ip: 10.1.21.1

  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 285, #pkts decrypt: 285, #pkts verify: 285
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0
```

Client's packets are getting encrypted/decrypted.

local crypto endpt.: 10.1.110.12, remote crypto endpt.: 112.1.1.200

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: FA9342C5

inbound esp sas:

```
spi: 0x9423992E (2485360942)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 8192, crypto-map: DYN-CMAP
  sa timing: remaining key lifetime (sec): 28624
  IV size: 8 bytes
  replay detection support: Y
```

Anti replay bitmap:

```
0xFFFFFFFF 0xFFFFFFFF
```

outbound esp sas:

```
spi: 0xFA9342C5 (4203954885)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Tunnel, }
  slot: 0, conn_id: 8192, crypto-map: DYN-CMAP
  sa timing: remaining key lifetime (sec): 28624
  IV size: 8 bytes
  replay detection support: Y
```

Anti replay bitmap:

```
0x00000000 0x00000001
```

interface: inside

Crypto map tag: __vpn-lb-crypto-map, seq num: 65534, local addr: 10.1.120.12

```
access-list vpnlb-10.1.120.10 permit ip host 10.1.120.12 host 10.1.120.10
local ident (addr/mask/prot/port): (10.1.120.12/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.1.120.10/255.255.255.255/0/0)
current_peer: 10.1.120.10

#pkts encaps: 618, #pkts encrypt: 618, #pkts digest: 618
#pkts decaps: 639, #pkts decrypt: 639, #pkts verify: 639
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 618, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.1.120.12, remote crypto endpt.: 10.1.120.10

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 6D983B72

inbound esp sas:
spi: 0x66A95179 (1722372473)
  transform: esp-3des esp-md5-hmac no compression
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: __vpn-lb-crypto-map
  sa timing: remaining key lifetime (kB/sec): (4373961/28182)
  IV size: 8 bytes
  replay detection support: Y
Anti replay bitmap:
  0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:
spi: 0x6D983B72 (1838693234)
  transform: esp-3des esp-md5-hmac no compression
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: __vpn-lb-crypto-map
  sa timing: remaining key lifetime (kB/sec): (4373968/28179)
  IV size: 8 bytes
  replay detection support: Y
Anti replay bitmap:
  0x00000000 0x00000001
```

ASA2(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.1.110.1 to network 0.0.0.0

```
S 10.1.21.1 255.255.255.255 [1/0] via 10.1.110.1, outside
C 10.1.110.0 255.255.255.0 is directly connected, outside
C 10.1.120.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.110.1, outside
```

Here's the static for client's connection. We need to see it redistributed and sent over to R2 via EIGRP.

R2#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

```
D EX 10.1.21.1/32 [170/514560] via 10.1.120.12, 00:03:56, FastEthernet0/0
C 10.1.120.0/24 is directly connected, FastEthernet0/0
```