CCIE Security v6

Authored By:

Khawar Butt

Hepta CCIE # 12353
(R/S, Security, SP, Voice, Storage,Data Center,Wireless)

CCDE # 20110020

Comprehensive coverage of the CCIE Security v6 Exam

Table of Contents

Configuring Destination NAT
Configuring Twice-NAT
Access Control
Module 3 – Configuring High Availability Features
Interface Redundancy
Port Channel
Active/Standby Failover
Stateful Failover
Security Contexts on the ASA using Shared Interface
Active/Active Failover
Clustering – Interface Interface Mode
Clustering – Spanning Interface Mode
Module 4 – Deep Packet Inspection
Configuring System L7 Deep Packet Inspection
Configuring User Defined L7 Deep Packet Inspection
Configuring TCP Normalization
Module 5 – Transparent Firewalls on 9.X
Configuring a Transparent Firewall
Configuring Management on a Transparent FW
ACL's in Transparent Mode
Module 6 – Configuring the Firewall Component of FTD
Initial Configuration of FTD & FMC from CLI
Registering & Initializing the FTD device on FMC
FTD Interface Configuration
Routing Protocol Configuration - Static & Default Routes
Routing Protocol Configuration – RIP
Routing Protocol Configuration – OSPF
Routing Protocol Configuration – BGP
Configuring Access Control Policies – Basic
Configuring Access Control Policies - Advanced
Module 7 – Configuring NAT on FTD
Configuring Dynamic NAT & Dynamic PAT
Configuring Static NAT
Configuring Static PAT
Configuring Twice-NAT
Configuring Destination NAT
Module 8 – Configuring Intrusion Prevention

Configuring ACP for Intrusion using the Default Policies on FTD
Configuring a Customized Intrusion Policy
Configuring an Event Filter
Module 9 – Configuring AMP
Configure AMP Policies to Block Specific File types
Configure AMP Policies to Block Infected Files - Malware
Module 10 – Configuring FTD – Advanced
Configure FTD as a Transparent Firewall
Configure Access Policies on a Transparent Firewall
Configure FTD High Availability – Failover
Configure the FTD High Availability Logical Device
Module 11 – Configuring IOS-Based Firewall
Configuring Zone-based Firewall on a Router
Configuring Port-maps in Zone-based Firewalls
Configuring Nested Classes in Zone-based Firewalls
Module 12 – Configuring VPNs on ASA
Configuring LAN-TO-LAN IPSec VPN on ASA – IKEv1
Configuring LAN-TO-LAN IPSec VPN on ASA – IKEv2
Configuring LAN-TO-LAN thru ASA – with NAT-T
Configuring LAN-TO-LAN thru ASA – without NAT-T
Configuring Web VPN Configuring ASDM on ASA
Configuring ASDM on ASA
Configuring SSL VPN
Configuring Router & Switch Security Features
Module 1 – Control Plane Management
Configuring Control Plane Policing
Configuring Control Plane Protection for Port Filtering
Module 2 – Configuring Router Security Features
Configuring Anti-Spoofing ACLs & the RPF Feature
Configuring NTP with Authentication
Configuring the Router for SNMP
Blocking Unwanted Services on the Router
Configuring Syslog Settings
Module 3 – Configuring Switch Security Features
Configuring the Port-Security Feature on the Switch
Configuring DHCP Snooping

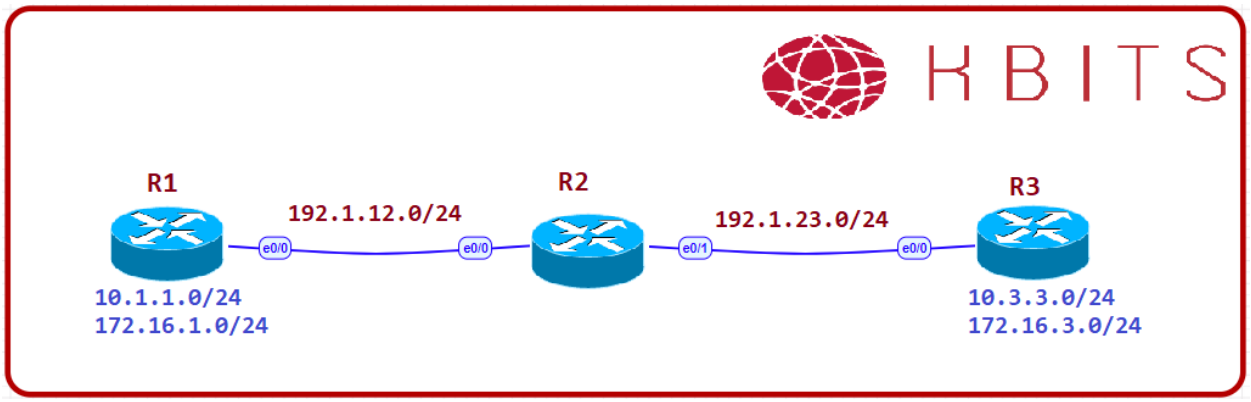
Configuring Static ARP Inspection Using an ARP ACL
Configuring Dynamic ARP Inspection (DAI)
Configuring the Source Guard Feature
Configuring VLAN ACL's
Module 4 – Configuring IPv6
Configuring IPv6 Addressing
Configuring OSPFv3
Configuring EIGRP for IPv6
Configuring IS-IS for IPv6
Configuring BGP for IPv6
Configuring IPv6IP Tunneling
Configuring NAT64

CCIE Security v6 – Advanced VPNs

Module 1 – Basic VPNs

Module 1 – Virtual Private Networks [VPN]

Lab 1 – LAN-To-LAN Tunnel without NAT-T



Lab Scenario:

- Configure an IPSec LAN-to-LAN Tunnel from R1 to a Router on the Internet R3. R2 is your ISP Router.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure the following Static Routes on the appropriate routers:
  - Default Routes on R1 and R3 pointing towards R2.
- Configure the following Loopback addresses on R1 & R3:
  - R1: 10.1.1.0/24
  - R3: 10.3.3.0/24

R1	**R2**
Int Loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int Loopback 1 Ip add 172.16.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.12.1 255.255.255.0	Int E 0/0 Ip add 192.1.12.2 255.255.255.0 No shut ! Int E 0/1 Ip add 192.1.23.2 255.255.255.0 No shut

No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.12.2	
R3 Int E 0/0 Ip address 192.1.23.3 255.255.255.0 No shut ! Int Loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int Loopback 1 Ip add 172.16.3.3 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.1.23.2	

Lab Tasks:

Task 1

Configure an IPSec Tunnel to encrypt traffic from 10.1.1.0/24 on R1 (Loopback 0) to the 10.3.3.0/24 on R3 (Loopback 0) using the following parameters for IPSec:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Group: 2
  - Hash: MD5
  - Pre-Shared Key: **cisco**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-SHA-HMAC

R1

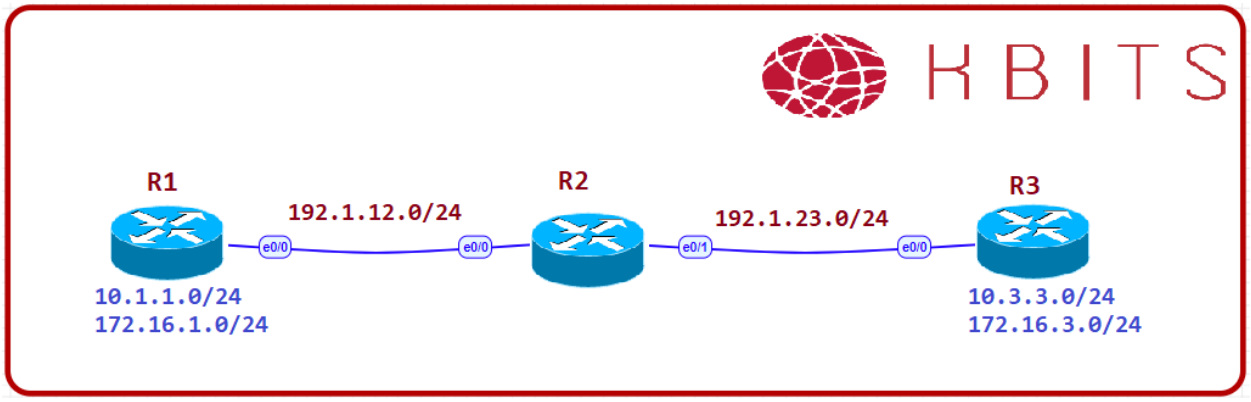
```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 192.1.23.3
!
```

```
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255
!
crypto map I-MAP 10 ipsec-isakmp
 set peer 192.1.23.3
 set transform-set t-set
 match address 101
!
Interface E 0/0
 Crypto map I-MAP
```

R3

```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 192.1.12.2
!
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
!
access-list 101 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map I-MAP 10 ipsec-isakmp
 set peer 192.1.12.1
 set transform-set t-set
 match address 101
!
Interface E 0/0
 Crypto map I-MAP
```

Lab 2 – Point-to-Point GRE



Lab Scenario:

- Configure a Point-to-Point GRE Tunnel from R1 to R3. R2 is your Internet Router.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure Default Routes on R1 and R3 pointing towards R2.
- Configure the following Loopback addresses on R1 & R3:
    - R1: 10.1.1.1/24 and 10.1.2.1/24
    - R3: 10.3.1.1/24 and 10.3.2.1/24

R1	**R2**
Int Loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int Loopback 1 Ip add 172.16.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.12.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.12.2	Int E 0/0 Ip add 192.1.12.2 255.255.255.0 No shut ! Int E 0/1 Ip add 192.1.23.2 255.255.255.0 No shut
R3	

Int Loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int Loopback 1 Ip add 172.16.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.1.23.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.23.2	

Lab Tasks:

Task 1

Configure a Point-to-Point GRE tunnel between R1 and R3. Use 192.168.13.0/24 as the Tunnel Network IP.

R1 Interface Tunnel 1 Ip add 192.168.13.1 255.255.255.0 Tunnel source 192.1.12.1 Tunnel destination 192.1.23.3
R3 Interface Tunnel 1 Ip add 192.168.13.3 255.255.255.0 Tunnel source 192.1.23.3 Tunnel destination 192.1.12.1

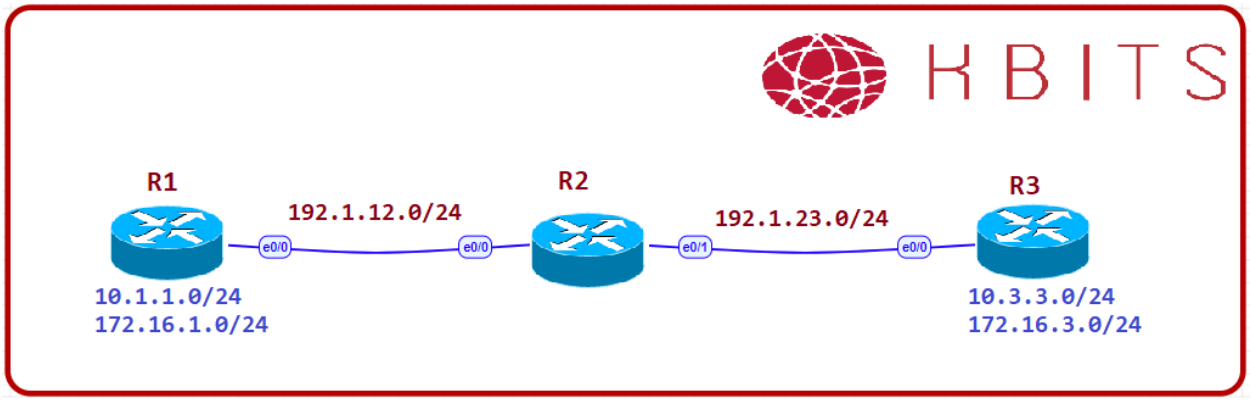
Task 2

Configure EIGRP in AS 13 to route the internal networks (Loopbacks) on the GRE Tunnel between R1 and R3.

R1 Router EIGRP 13 No auto-summary Network 192.168.13.0 Network 10.0.0.0
R3

```
Router EIGRP 13
 No auto-summary
 Network 192.168.13.0
 Network 10.0.0.0
```

Lab 3 – Encrypting GRE Tunnels Using IPSec



Lab Scenario:

- Encrypt the traffic passing thru the GRE Tunnel using IPSec

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure IPSec to encrypt the traffic passing thru the GRE tunnel. Make sure the packet does not duplicate the IP addresses in the Header. Use the following parameters for the IPSec Tunnel:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Group: 2
  - Hash: MD5
  - Pre-Shared Key: **cisco**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-SHA-HMAC

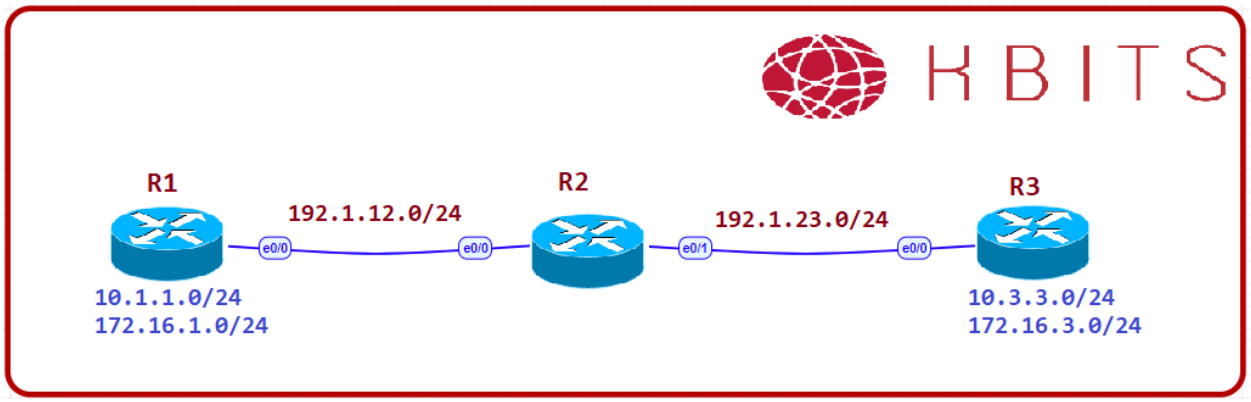
R1
Crypto isakmp policy 10

```
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 192.1.23.3
!
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile IPSEC
 set transform-set t-set
!
Interface Tunnel 1
 Tunnel protection ipsec profile IPSEC
```

R3

```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 192.1.12.1
!
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile IPSEC
 set transform-set t-set
!
Interface Tunnel 1
 Tunnel protection ipsec profile IPSEC
```

Lab 4 – Configuring a P2P VPN using Native IPSec Tunnel Interface – SVTI



Lab Scenario:

- Convert the existing GRE/IPSEC tunnel into a native IPSec tunnel by completely eliminating GRE from the Packets.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Convert the Existing GRE/IPSec tunnel into a Native IPSec tunnel by changing the Tunnel mode to IPSec.

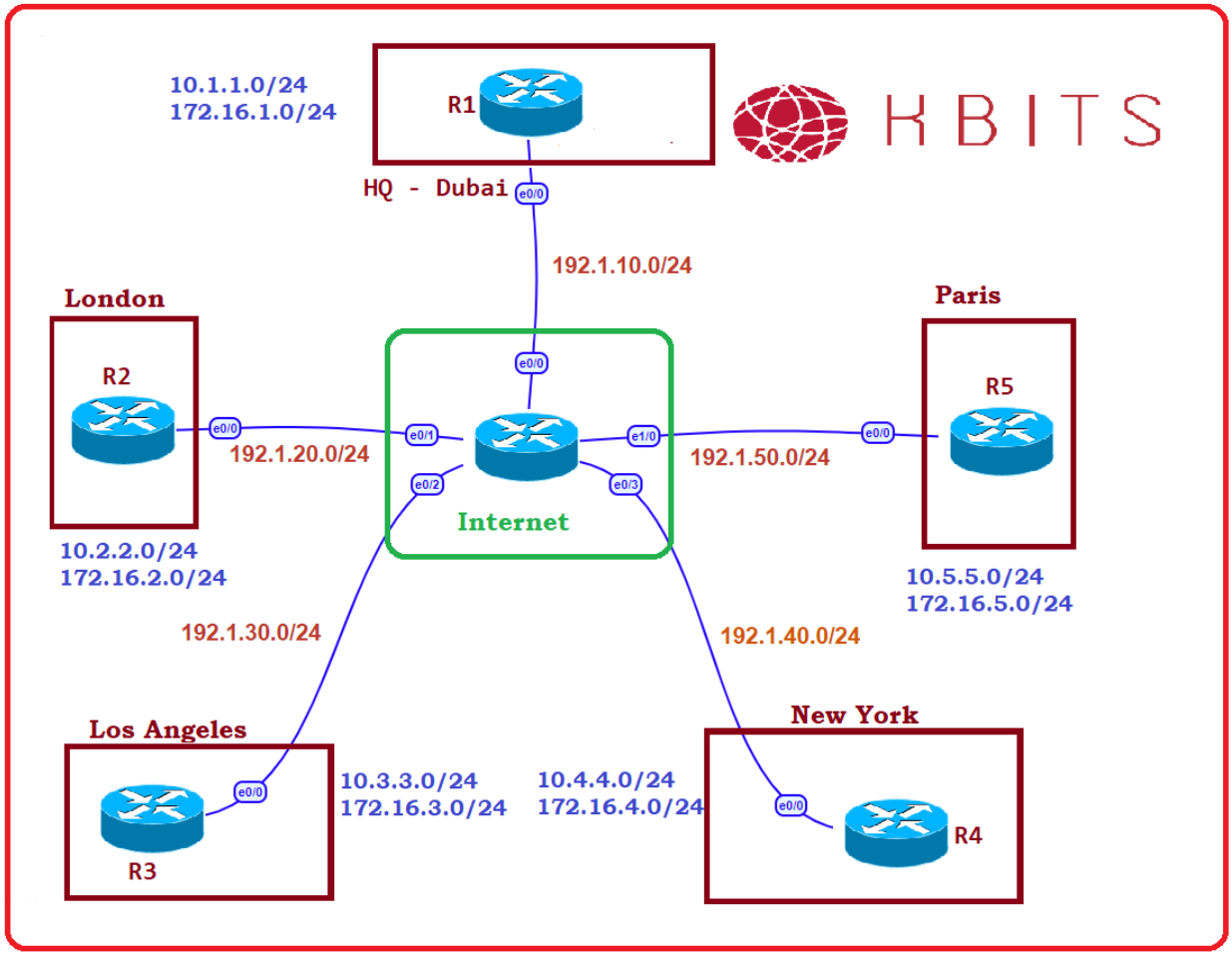
R1 Interface Tunnel 1 Tunnel mode ipsec ipv4
R3 Interface Tunnel 1 Tunnel mode ipsec ipv4

CCIE Security v6 – Advanced VPNs

Module 2 – Advanced VPNs

Module 2 – Advanced VPNs

Lab 1 – Multipoint GRE (MGRE) Tunnel



Lab Scenario:

- Configure a Multipoint GRE Tunnel between R1, R2, R3 & R4. Internet is your Internet Router.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure Default Routes on R1 thru R4 pointing towards R5.
- Configure the following Loopback addresses on R1 thru R4:
  - R1: 10.1.1.1/24 and 172.16.1.1/24
  - R2: 10.2.2.2/24 and 172.16.2.2/24

- R3: 10.3.3.3/24 and 172.16.3.3/24
- R4: 10.4.4.4/24 and 172.16.4.4/24

R1	**R2**
Int Loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int Loopback 1 Ip add 172.16.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.10.6	Int Loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int Loopback 1 Ip add 172.16.2.2 255.255.255.0 ! Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.6
R3	**R4**
Int Loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int Loopback 1 Ip add 172.16.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.1.30.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.30.6	Int Loopback 0 Ip add 10.4.4.4 255.255.255.0 ! Int Loopback 1 Ip add 172.16.4.4 255.255.255.0 ! Int E 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.40.6
R5	**R6**
Int Loopback 0 Ip add 10.5.5.5 255.255.255.0 ! Int Loopback 1 Ip add 172.16.5.5 255.255.255.0 ! Int E 0/0 Ip add 192.1.50.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.50.6	Interface E 0/0 Ip address 192.1.10.6 255.255.255.0 No shut ! Interface E 0/1 Ip address 192.1.20.6 255.255.255.0 No shut ! Interface E 0/2 Ip address 192.1.30.6 255.255.255.0 No shut ! Interface E 0/3 Ip address 192.1.40.6 255.255.255.0

	No shut ! Interface E 1/0 Ip address 192.1.50.6 255.255.255.0 No shut

Lab Tasks:

Task 1

Configure a MultiPoint GRE tunnel between R1, R2, R3 & R4. Use 192.168.1.0/24 as the Tunnel Network IP. The NHRP mapping will be done in the next Task. Use the following parameters for your MGRE Tunnel:

- NHRP Parameters
  - NHRP ID – 1234
  - NHRP Authentication key – cisco
- Tunnel Parameters
  - Tunnel Authentication Key : 1234

R1

```
Interface Tunnel 1
 Ip address 192.168.1.1 255.255.255.0
 Ip nhrp network-id 1234
 Ip nhrp authentication cisco
 Tunnel source E 0/0
 Tunnel mode gre multipoint
 Tunnel key 1234
```

R2

```
Interface Tunnel 1
 Ip address 192.168.1.2 255.255.255.0
 Ip nhrp network-id 1234
 Ip nhrp authentication cisco
 Tunnel source E 0/0
 Tunnel mode gre multipoint
 Tunnel key 1234
```

R3

```
Interface Tunnel 1
 Ip address 192.168.1.3 255.255.255.0
 Ip nhrp network-id 1234
 Ip nhrp authentication cisco
 Tunnel source E 0/0
 Tunnel mode gre multipoint
 Tunnel key 1234
```

R4

```
Interface Tunnel 1
 Ip address 192.168.1.4 255.255.255.0
 Ip nhrp network-id 1234
```

```
Ip nhrp authentication cisco
Tunnel source E 0/0
Tunnel mode gre multipoint
Tunnel key 1234
```

Task 2

Configure NHRP Mapping allowing all devices to connect to each other directly for Unicast traffic. Configure Multicast mappings in such a way that all devices use R1 as the routing hub.

R1

```
Interface Tunnel 1
 Ip nhrp map 192.168.1.2 192.1.20.2
 Ip nhrp map 192.168.1.3 192.1.30.3
 Ip nhrp map 192.168.1.4 192.1.40.4
 Ip nhrp map Multicast 192.1.20.2
 Ip nhrp map Multicast 192.1.30.3
 Ip nhrp map Multicast 192.1.40.4
```

R2

```
Interface Tunnel 1
 Ip nhrp map 192.168.1.1 192.1.10.1
 Ip nhrp map 192.168.1.3 192.1.30.3
 Ip nhrp map 192.168.1.4 192.1.40.4
 Ip nhrp map Multicast 192.1.10.1
```

R3

```
Interface Tunnel 1
 Ip nhrp map 192.168.1.1 192.1.10.1
 Ip nhrp map 192.168.1.2 192.1.20.2
 Ip nhrp map 192.168.1.4 192.1.40.4
 Ip nhrp map Multicast 192.1.10.1
```

R4

```
Interface Tunnel 1
 Ip nhrp map 192.168.1.1 192.1.10.1
 Ip nhrp map 192.168.1.2 192.1.20.2
 Ip nhrp map 192.168.1.3 192.1.30.3
 Ip nhrp map Multicast 192.1.10.1
```

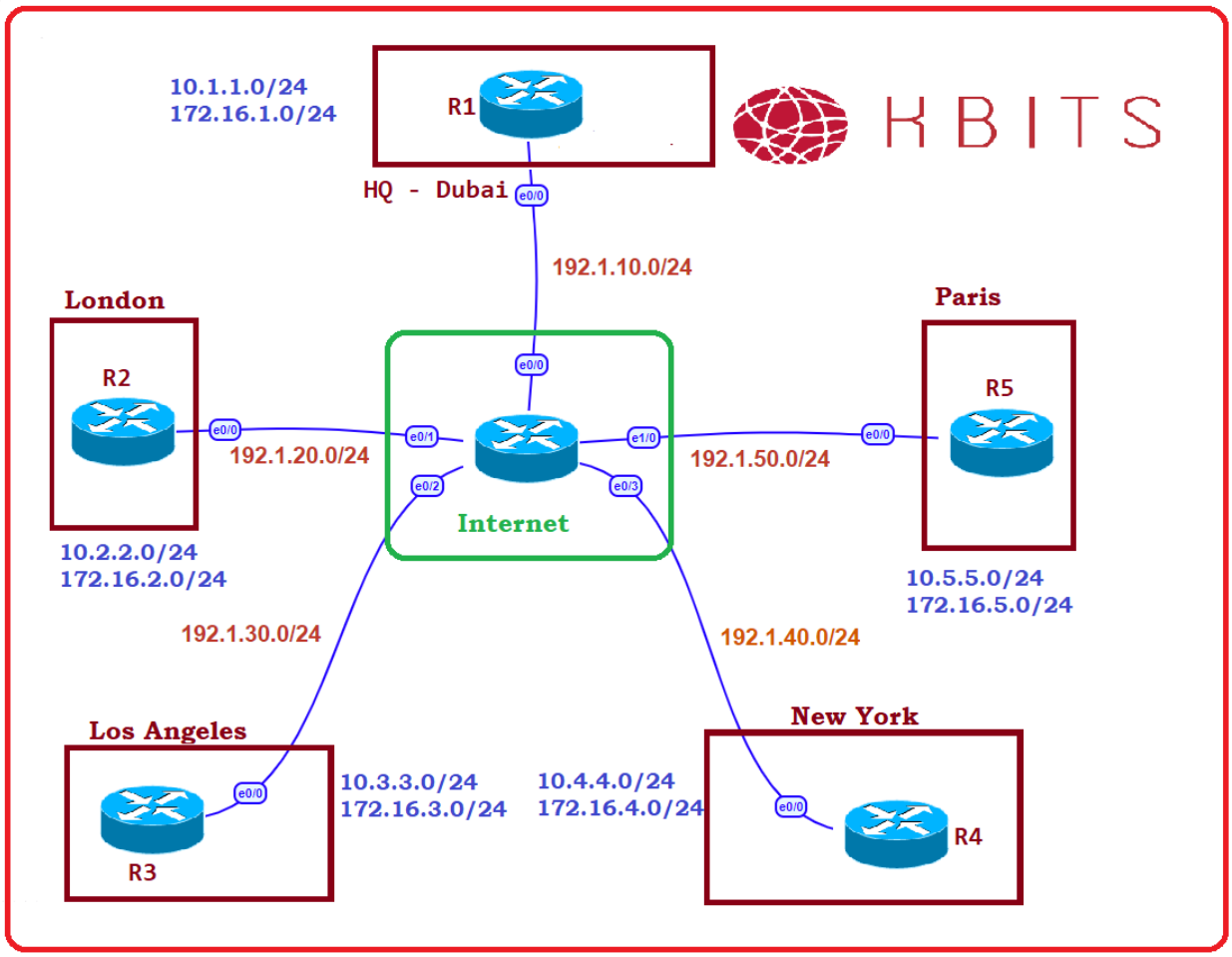
Task 3

Configure EIGRP in AS 1234 to route the internal networks (Loopbacks) on the GRE Tunnel on all the MGRE Routers. Disable Split horizon on R1 to allow it propagate routes from the Spoke routers to the other spoke routers.

Note: You might need to bounce the Tunnel interface to make the Routing work. Bring up the Hub router before the Spoke Routers.

R1 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0
R2 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0
R3 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0
R4 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0

Lab 2 – Configuring DMVPN – Phase I



Lab Scenario:

- Configure DMVPN Phase I. The Spoke-to-Spoke traffic should use a Hub as a hop. Use EIGRP as the Routing Protocol.

Initial Setup:

- **Builds on the previous lab. Disable the Tunnel Interface from the previous lab**

R1 No Interface Tunnel 1	**R2** No Interface Tunnel 1
R3 No Interface Tunnel 1	**R4** No Interface Tunnel 1

Lab Tasks:

Task 1

Configure a MultiPoint GRE tunnel between R1, R2, R3 & R4. Use 192.168.1.0/24 as the Tunnel Network IP. Tunnel:

- NHRP Parameters
  - NHRP ID – 1234
  - NHRP Authentication key – cisco
  - NHS : R1
  - Routing Hub: R1 [Configure the multicast mapping to accommodate routing protocols]
- Tunnel Parameters
  - Tunnel Authentication Key : 1234

R1 Interface Tunnel 1 Ip address 192.168.1.1 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp map multicast dynamic Tunnel source E 0/0 Tunnel mode gre multipoint Tunnel key 1234
R2 Interface Tunnel 1 Ip address 192.168.1.2 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp nhs 192.168.1.1

Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map multicast 192.1.10.1 Tunnel source E 0/0 Tunnel mode gre multipoint Tunnel key 1234
R3 Interface Tunnel 1 Ip address 192.168.1.3 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp nhs 192.168.1.1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map multicast 192.1.10.1 Tunnel source E 0/0 Tunnel mode gre multipoint Tunnel key 1234
R4 Interface Tunnel 1 Ip address 192.168.1.4 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp nhs 192.168.1.1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map multicast 192.1.10.1 Tunnel source E 0/0 Tunnel mode gre multipoint Tunnel key 1234

Task 2

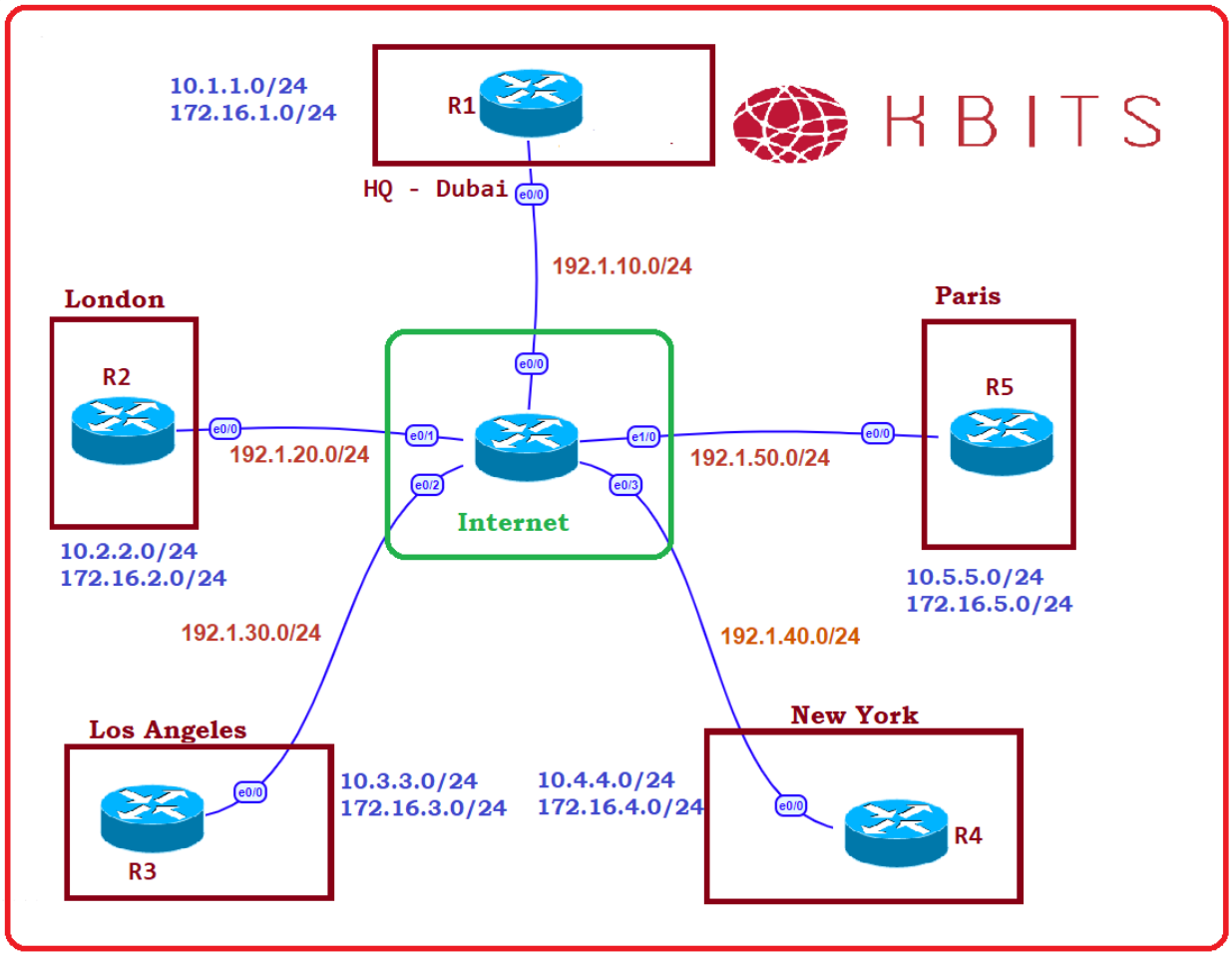
Configure EIGRP in AS 1234 to route the internal networks (Loopbacks) on the GRE Tunnel on all the MGRE Routers. Disable Split horizon on R1 to allow it propagate routes from the Spoke routers to the other spoke routers.

R1 Interface Tunnel 1 No ip split-horizon eigrp 1234 ! Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0
R2

Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0
R3 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0
R4 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0

Note: The default behavior of EIGRP is to change the Next-hop to itself while propagating the spoke routes to other spokes. The result is that the spokes will use the hub route as the next hop for all spoke-to-spoke traffic. **This is DMVPN Phase I [Hub-n-Spoke forwarding]**

Lab 3 – Configuring DMVPN – Phase II



Lab Scenario:

- Configure DMVPN Phase II. The Spoke-to-Spoke traffic should use a direct path. Use the Routing Protocol to accomplish this task.

Initial Setup:

- **Builds on the previous lab.**

Lab Tasks:

Task 1

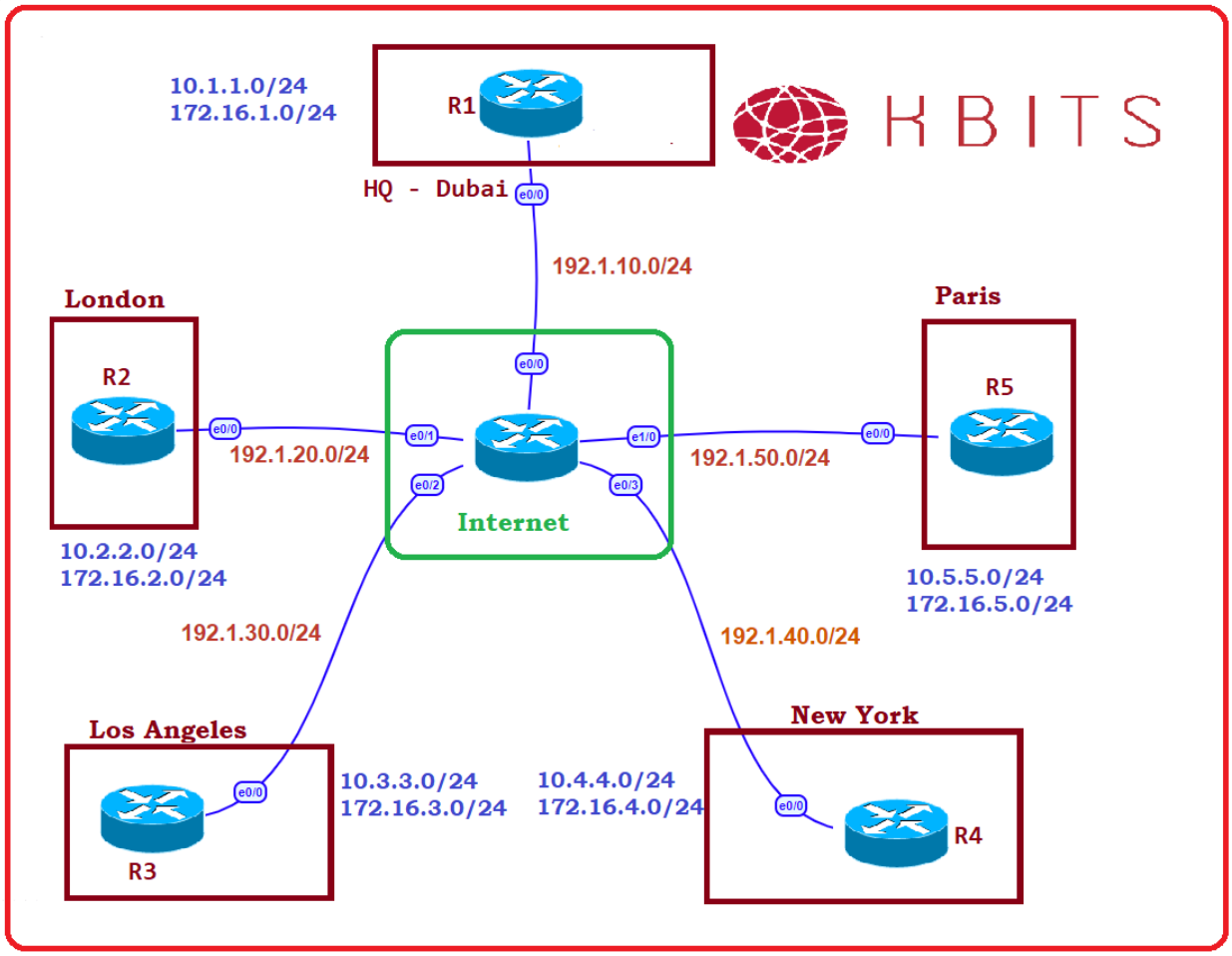
Disable the Hub from changing the next-hop attribute on the hub.

R1
Interface Tunnel 1 No ip next-hop-self eigrp 1234

Note: Check the Routing table. The next-hop attribute for the Spoke-routes is unchanged by the hub and is directly pointing to the spoke Tunnel IP. This causes the spokes to do a NHRP resolution directly for the spoke. Although the resolution packet will go thru the hub, the actual packet will take the direct path. Use the traceroute command to verify this.

This is DMVPN Phase II. In this phase, the spoke-to-spoke traffic is forwarded directly between the spokes. Phase II is accomplished by tweaking the Routing protocol behavior.

Lab 4 – Configuring DMVPN – Phase III



Lab Scenario:

- Configure DMVPN Phase III. The Spoke-to-Spoke traffic should use a direct path. Use the NHRP to accomplish this task.

Initial Setup:

- **Change the Next-hop back to Self. All routes should again have a next-hop pointing to the Hub [DMVPN Phase I]**

R1

```
Interface Tunnel 1
 ip next-hop-self eigrp 1234
```

Lab Tasks:

Task 1

Configure NHRP Redirection on the Hub such that the Hub should push down a dynamic mapping to the spokes for the spoke internal routes. Configure the spokes to accept the mapping.

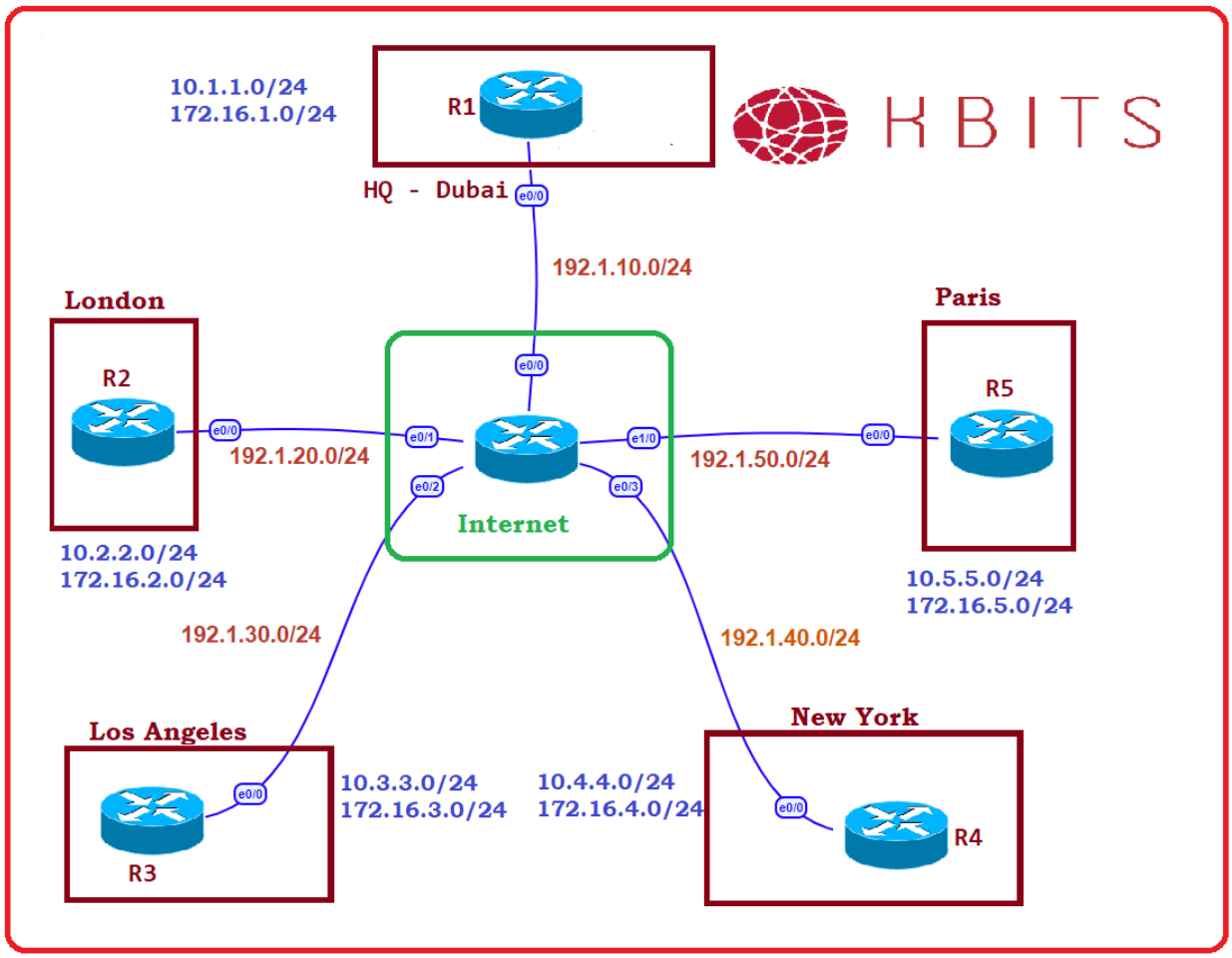
R1 Interface Tunnel 1 Ip nhrp redirect
R2 Interface Tunnel 1 Ip nhrp shortcut
R1 Interface Tunnel 1 Ip nhrp shortcut
R1 Interface Tunnel 1 Ip nhrp shortcut

Note: Check the Routing table. The next-hop attribute is pointing to the hun. Do a traceroute from the R2 to R4. You will notice the first trace goes thru the hub. This is due to the routing table pointing towards the Hub. The hub detects that the spokes are both connected on the same tunnel interface, hence sends a NHRP redirect message to both of them. The NHRP redirect message contains the mapping for the destination public IP for the internal networks.

The subsequent packets will be forwarded directly from spoke to spoke. If you check the routing table entry, it still points to the Hub. If you check the NHRP table, you will see an entry for the destination spoke network with the Spoke public IP.

This is DMVPN Phase III. In this phase, the spoke-to-spoke traffic is forwarded directly between the spokes. Phase III is accomplished by using NHRP redirect messages to override the routing table.

Lab 5 – Configuring a Dual-Hub DMVPN



Lab Scenario:

- Configure R1 & R2 as the NHRP Hub.

Initial Setup:

- **Builds on the previous lab.**

Lab Tasks:

Task 1

Disable the existing tunnel interface on R2.

R2
No Interface Tunnel 1

Task 2

Configure a Static Tunnel between R1 and R2. R2 should be configured with a Tunnel IP address of 192.168.1.2/24 using the same Tunnel parameters as the previous lab.

R2
Interface Tunnel 1 Ip address 192.168.1.2 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp map 192.168.1.1 192.1.10.10 Ip nhrp map multicast 192.1.10.1 Tunnel source E 0/0 Tunnel mode gre multipoint Tunnel key 1234
R1
Interface Tunnel1 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map multicast 192.1.20.2

Task 2

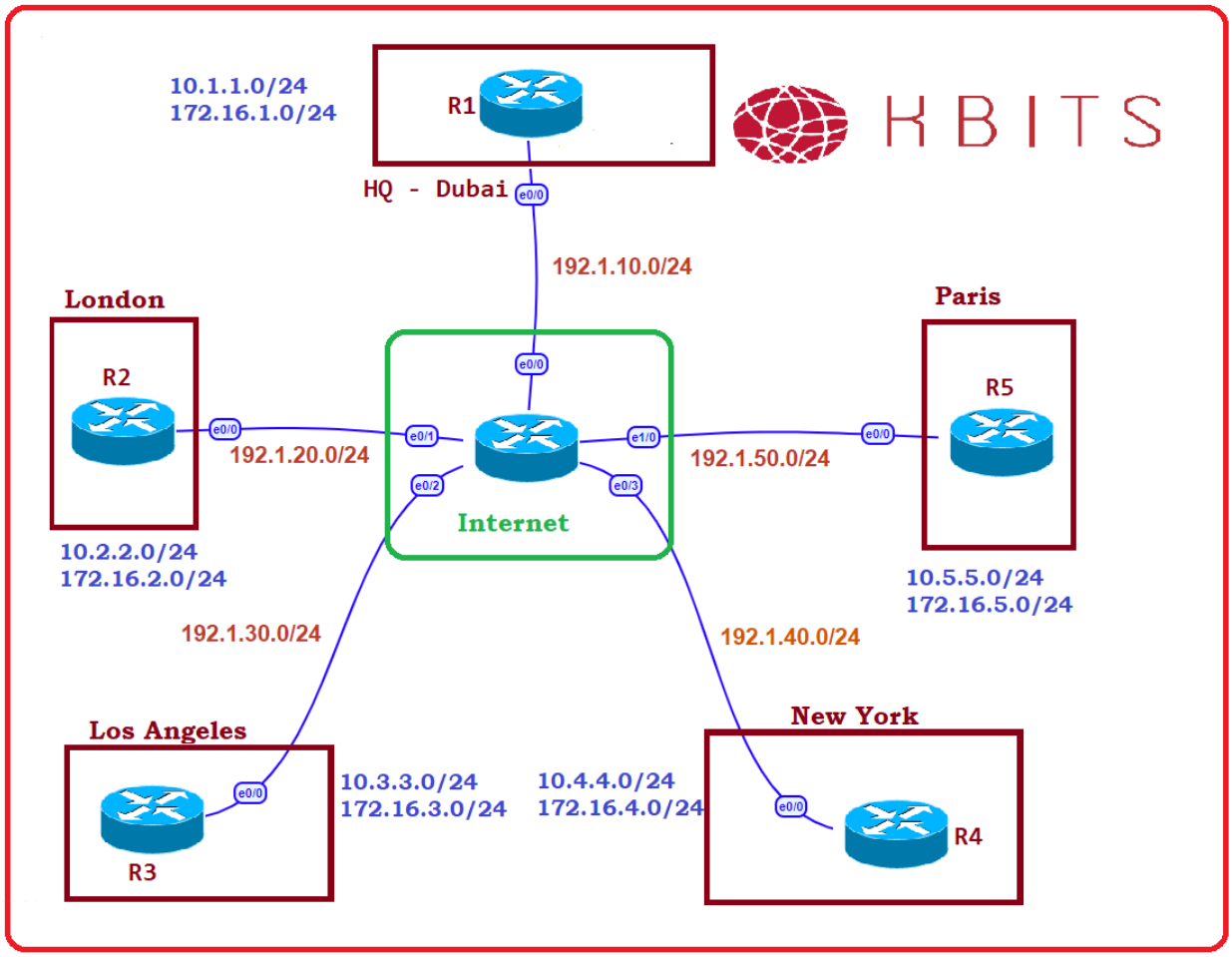
Configure R2 as another NHS in your network. Configure R3 & R4 to use R2 as the NHS Server and a Routing hub as well.

R2
Interface Tunnel 1 Ip nhrp map multicast dynamic No ip split-horizon eigrp 1234 Ip nhrp redirect
R3
Interface Tunnel1 Ip nhrp nhs 192.168.1.2

Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map multicast 192.1.20.2
R4 Interface Tunnel1 Ip nhrp nhs 192.168.1.2 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map multicast 192.1.20.2

Note: You should now see routes from both Routing hubs. Although, it sees 2 entries, the Data path will be direct due to Phase III.

Lab 6 – Encrypting the DMVPN Traffic using IPSec



Lab Scenario:

- Configure IPSec on the Tunnel interfaces to encrypt all Tunnel traffic.

Initial Setup:

- **Builds on the previous lab.**

Lab Tasks:

Task 1

Configure IPSec to encrypt the traffic passing thru the tunnel. Make sure the packet does not duplicate the IP addresses in the Header. Use the following parameters for the IPSec Tunnel:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Group: 2
  - Hash: MD5
  - Pre-Shared Key: **cisco**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-SHA-HMAC

R1

```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 0.0.0.0
!
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile IPSEC
 set transform-set t-set
!
Interface Tunnel 1
 Tunnel protection ipsec profile IPSEC
```

R2

```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 0.0.0.0
!
```

```
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile IPSEC
 set transform-set t-set
!
Interface Tunnel 1
 Tunnel protection ipsec profile IPSEC
```

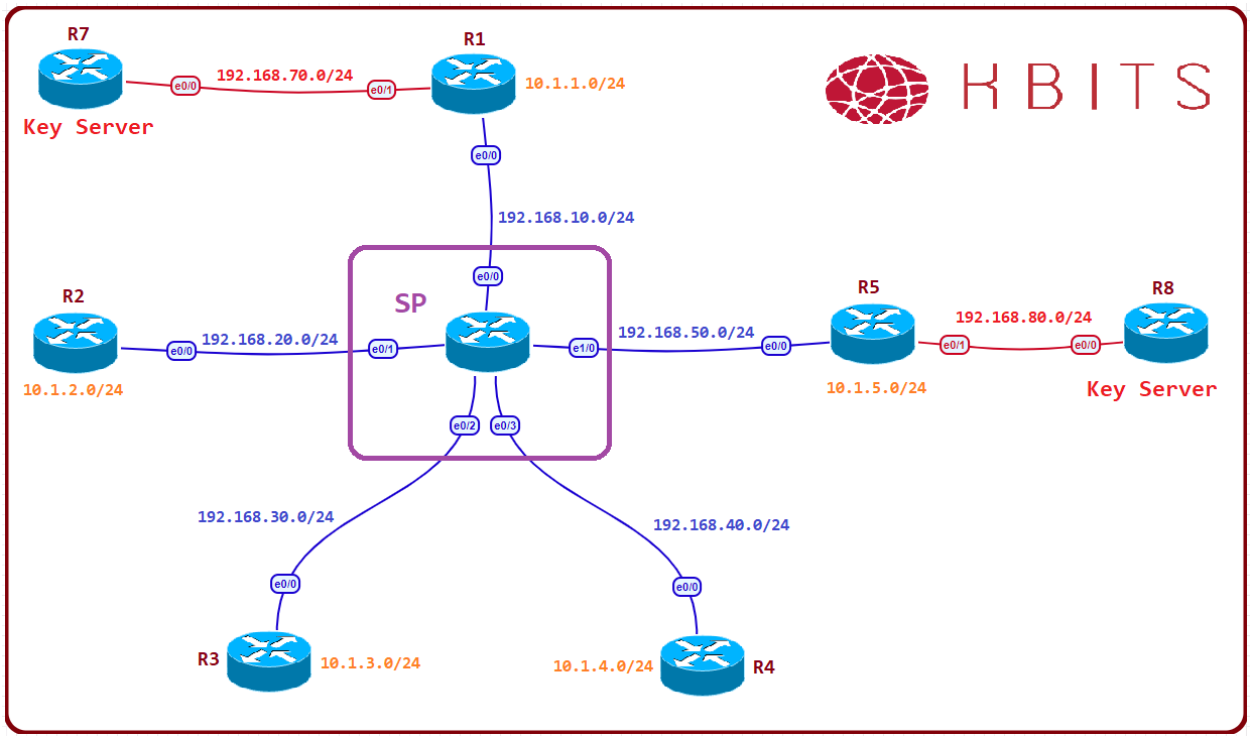
R3

```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 0.0.0.0
!
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile IPSEC
 set transform-set t-set
!
Interface Tunnel 1
 Tunnel protection ipsec profile IPSEC
```

R4

```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco address 0.0.0.0
!
crypto ipsec transform-set t-set esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile IPSEC
 set transform-set t-set
!
Interface Tunnel 1
 Tunnel protection ipsec profile IPSEC
```

Lab 7 – Configuring GET VPN



Lab Scenario:

- Configure GET VPN to encrypt traffic between R1, R2, R3, R4 & R5. R7 is your Key Server. R1 and R7 are located at the Head quarters. R8 will be configured as a Bacup Key Server in a later lab. R2, R3, R4 & R5 are remote sites connecting over a Private WAN.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure the following Loopback addresses on R2 thru R5:
  - R1: 10.1.1.1/24 and 10.1.11.1/24
  - R2: 10.1.2.1/24 and 10.1.22.1/24
  - R3: 10.1.3.1/24 and 10.1.33.1/24
  - R4: 10.1.4.1/24 and 10.1.44.1/24
  - R4: 10.1.5.1/24 and 10.1.55.1/24

- Configure EIGRP in AS 100 as the routing protocol to route all networks in the network. GETVPN requires a full routable network prior to setting up the VPN.

R1	**R2**
Int E 0/0 Ip add 192.168.10.1 255.255.255.0 No shut ! Int E 0/1 Ip add 192.168.70.1 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.1.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.11.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.10.0 Network 192.168.70.0 Network 10.0.0.0	Int E 0/0 Ip add 192.168.20.2 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.2.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.22.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.20.0 Network 10.0.0.0
R3	**R4**
Int E 0/0 Ip add 192.168.30.3 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.3.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.33.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.30.0 Network 10.0.0.0	Int E 0/0 Ip add 192.168.40.4 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.4.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.44.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.40.0 Network 10.0.0.0
R5	**R7**
Int E 0/0 Ip add 192.168.50.5 255.255.255.0	Int E 0/0 Ip add 192.168.70.7 255.255.255.0

No shut ! Int E 0/1 Ip add 192.168.80.5 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.5.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.55.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.50.0 Network 192.168.80.0 Network 10.0.0.0	No shut ! Router EIGRP 100 No auto-summary Network 192.168.70.0
R8 Int E 0/0 Ip add 192.168.80.8 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.168.80.0	**R6 – Service Provider** Int E 0/0 Ip add 192.168.10.6 255.255.255.0 No shut ! Int E 0/1 Ip add 192.168.20.6 255.255.255.0 No shut ! Int E 0/2 Ip add 192.168.30.6 255.255.255.0 No shut ! Int E 0/3 Ip add 192.168.40.6 255.255.255.0 No shut ! Int E 1/0 Ip add 192.168.50.6 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.168.10.0 Network 192.168.20.0 Network 192.168.30.0 Network 192.168.40.0

	Network 192.168.50.0

Lab Tasks:

Task 1

Configure R7 as the Key Server for your GET VPN to encrypt data between R1, R2, R3, R4 and R5. Use the following parameters for the KS.

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Pre-Shared Key: **cisco [Don't use wildcard mask]**
  - Group: 2
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-MD5-HMAC
- Key Server Parameters
  - Identity Number: 100
  - Interesting Traffic: Any traffic on the 10.1.0.0/16 network.
  - Local Address: E 0/0
  - Rekey Transport: Unicast
  - Rekey Key Label: GETVPN
  - Rekey key Encryption: 3des

R7

```
Crypto key generate rsa modulus 1024 label GETVPN exportable
[Exportable is required for Coop Server]
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cisco address 192.168.10.1
crypto isakmp key cisco address 192.168.20.2
crypto isakmp key cisco address 192.168.30.3
crypto isakmp key cisco address 192.168.40.4
crypto isakmp key cisco address 192.168.50.5
!
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

```
crypto ipsec profile G-PROF
 set transform-set TSET
!
crypto gdoi group ABC
 identity number 100
 server local
  address ipv4 192.168.70.7
  sa ipsec 1
    profile G-PROF
    match address ipv4 101
    rekey transport unicast
    rekey authentication mypubkey rsa GETVPN
    rekey algorithm 3des
```

Task 2

Configure R1, R2, R3, R4 and R5 to use R7 as the Key Server. Use the Parameters listed for the Key server to configure the Devices.

R1

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cciesec address 192.168.70.7
!
crypto gdoi group ABC
 identity number 100
 server address ipv4 192.168.70.7
!
crypto map I-MAP 10 gdoi
 set group ABC
!
interface E 0/0
crypto map I-MAP
```

R2

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cciesec address 192.168.70.7
!
```

```
crypto gdoi group ABC
 identity number 100
 server address ipv4 192.168.70.7
!
crypto map I-MAP 10 gdoi
 set group ABC
!
interface E 0/0
crypto map I-MAP
```

R3

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cciesec address 192.168.70.7
!
crypto gdoi group ABC
 identity number 100
 server address ipv4 192.168.70.7
!
crypto map I-MAP 10 gdoi
 set group ABC
!
interface E 0/0
crypto map I-MAP
```

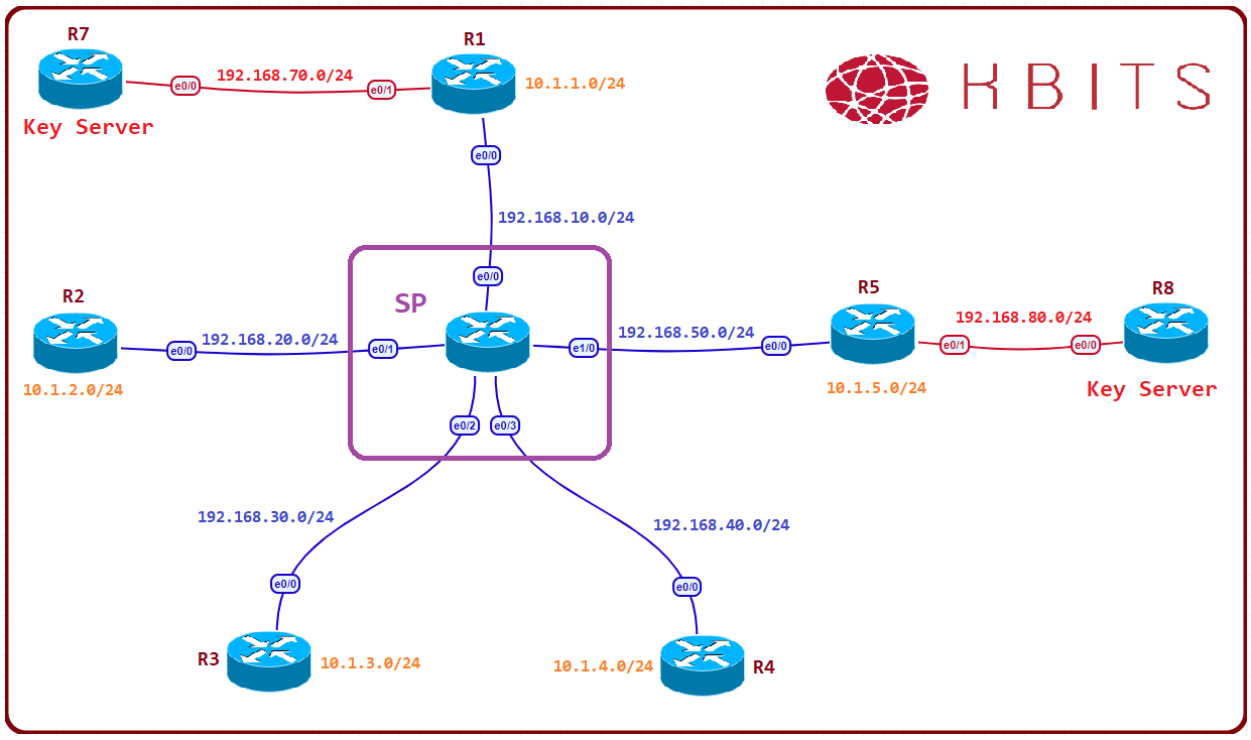
R4

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cciesec address 192.168.70.7
!
crypto gdoi group ABC
 identity number 100
 server address ipv4 192.168.70.7
!
crypto map I-MAP 10 gdoi
 set group ABC
!
interface E 0/0
crypto map I-MAP
```

R5

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cciesec address 192.168.70.7
!
crypto gdoi group ABC
 identity number 100
 server address ipv4 192.168.70.7
!
crypto map I-MAP 10 gdoi
 set group ABC
!
interface E 0/0
crypto map I-MAP
```

Lab 8 – Configuring GET VPN Redundancy



Lab Scenario:

- Configure a Coop server to provide fault tolerance to the Key Server.

Initial Setup:

- **Builds on the previous lab.**

Lab Tasks:

Task 1

Export the RSA keys on R7 so that they can be imported on the Backup server [R7].

- Export Parameters:
  - File Type: PEM
  - Encryption : 3DES
  - Encryption Key: **cisco123**

R7

crypto key export rsa GETVPN pem terminal 3des cisco123

```
---------------------------------------------------------------------------------

% Key name: GETVPN

Usage: General Purpose Key

Key data:  -----BEGIN PUBLIC KEY-----
ABCDi13330GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmct4j/ecT1PumBNG1fWPMm1RE
/Rt/gT1WdhRDWwKmt8ftVFMU6rqjwjUqhn7hLRPortnBGS14t4UjK6IXzPLuxUbI
pgAlPn+PldDbpbgZP4Iv9VDp7xbU+9AVVkZpnYZLjo6aGQxBvHuLPA1S31+jSgXw
tDkjpNA1w48fHDAgYwIDAQAB

-----END PUBLIC KEY-----

 -----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED  DEK-Info: DES-EDE3-CBC,4C0424B43DE3EAC5

PjSOnv50zJZWwAUA5vTRRdRffJmi5cn9yH+eTLSg1A5GilKXmT5UhKucVMzHb1ep
XMaBacqt6QiJnib/MEHQAyjrbKSg5Ayvp1hTap+Vw/reOyMJovrDcCRmt3hzynz9
r/LXN/ykNKWeQvCr+YFglzMtptdEwQfhBA1P4eSMLCozP/r8Sd+oABMBIh4Im8kZ
Z3skBIKUT8CiNTmKDA3B/QMe2F1bcEeaA7r0CvoMQNWG9kLwhyQnnZzMjIPZ/yG8
4RrxmpWxrL3VOnAbAXxYu/fe597JKQEcp3XnURYnNHsh4dIphemlAAegPRHLCJQR
pd2an5I/Q4vAuVLaXgRRCuwe75fLUSZtk8UKAJXS3ZiOKbuABQ5QiLFS+S9Unnb2
1MLe3szgMKg6eyswYTFCXRNLauEyNhA4PMSxxLCPDeDaQr4XilB/iKMXy6ROMUhQ
OenT1u3vhjUzqxX+b/2IWYARvlY+rKahA4XkRhXwctsYB2Gs9a+dvuC+nl9JI5ys
zv++hUvrxAPlxfi/YM9tVMN91Rd8kZamIPwGFHgMk7wMwqwmdLljD2Qs+2wa8AtM
q+TvgQNUtqq9il0YHcRDZEiA5NWyNvcFFZKGn/+EqlalSX5VAKfnvdnQEY5RNcN9
BUpP7mLApWOBvAZz7vHC7/ZYaPeHtpabPaEvcqTXGc5mah6HLyPS0YhjWXs3XwRz
1czJ+cnBo6YXkvvTo4HefIfnnZHO+it8Y/chbny+/aVw1/fcdbWQ8l37XL+b6jzG
sdHa5IyBbs+kIeNELJTg9W1NLNaxEUhXjTh525CEXnU=

-----END RSA PRIVATE KEY-----
```

Task 2

Import the RSA keys from R7 on R8.

- Import Parameters to match:
  - File Type: PEM
  - Encryption: 3DES
  - Encryption Key: **cisco123**

R8

crypto key import rsa KS-KEYS pem exportable terminal cisco123

% Enter PEM-formatted public General Purpose
% End with a blank line or "quit" on a line by itself.

-----BEGIN PUBLIC KEY-----
ABCDi13330GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmct4j/ecT1PumBNG1fWPMm1RE
/Rt/gT1WdhRDWwKmt8ftVFMU6rqjwjUqhn7hLRPortnBGS14t4UjK6IXzPLuxUbI
pgAlPn+PldDbpbgZP4Iv9VDp7xbU+9AVVkZpnYZLjo6aGQxBvHuLPA1S31+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+eTLSg1A5GilKXmT5UhKucVMzHb1ep
XMaBacqt6QiJnib/MEHQAyjrbKSg5Ayvp1hTap+Vw/reOyMJovrDcCRmt3hzynz9
r/LXN/ykNKWeQvCr+YFglzMtptdEwQfhBA1P4eSMLCozP/r8Sd+oABMBIh4Im8kZ
Z3skBIKUT8CiNTmKDA3B/QMe2F1bcEeaA7r0CvoMQNWG9kLwhyQnnZzMjIPZ/yG8
4RrxmpWxrL3VOnAbAXxYu/fe597JKQEcp3XnURYnNHsh4dIphemlAAegPRHLCJQR
pd2an5I/Q4vAuVLaXgRRCuwe75fLUSZtk8UKAJXS3ZiOKbuABQ5QiLFS+S9Unnb2
1MLe3szgMKg6eyswYTFCXRNLauEyNhA4PMSxxLCPDeDaQr4XilB/iKMXy6ROMUhQ
OenT1u3vhjUzqxX+b/2IWYARvlY+rKahA4XkRhXwctsYB2Gs9a+dvuC+nl9JI5ys
zv++hUvrxAPlxfi/YM9tVMN91Rd8kZamIPwGFHgMk7wMwqwmdLljD2Qs+2wa8AtM
q+TvgQNUtqq9il0YHcRDZEiA5NWyNvcFFZKGn/+EqlalSX5VAKfnvdnQEY5RNcN9
BUpP7mLApWOBvAZz7vHC7/ZYaPeHtpabPaEvcqTXGc5mah6HLyPS0YhjWXs3XwRz
1czJ+cnBo6YXkvvTo4HefIfnnZHO+it8Y/chbny+/aVw1/fcdbWQ8l37XL+b6jzG
sdHa5IyBbs+kIeNELJTg9W1NLNaxEUhXjTh525CEXnU=
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.

Task 3

Configure R7 to point to R8 as the Backup redundancy server. R7 should be the preferred KS. Set the Local Priority to 100 on R7. Also enable ISAKMP Keepalives. Set the interval to 10 seconds. Make sure to set the Pre-shared key for the Backup KS.

R7

```
crypto gdoi group ABC
 identity number 100
 server local
  redundancy
   local priority 100
```

```
   peer address ipv4 192.1.80.8
!
Crypto isakmp keepalive 10
Crypto isakmp key cisco address 192.168.80.8
```

Task 4

Configure R8 as the Backup Key Server for your GET VPN to encrypt data between R1, R2, R3, R4 and R5. Use the following parameters for the KS. These are the same ones that were specified on R7. Configure redundancy pointing to R7 as the peer. Set the local priority to 50.

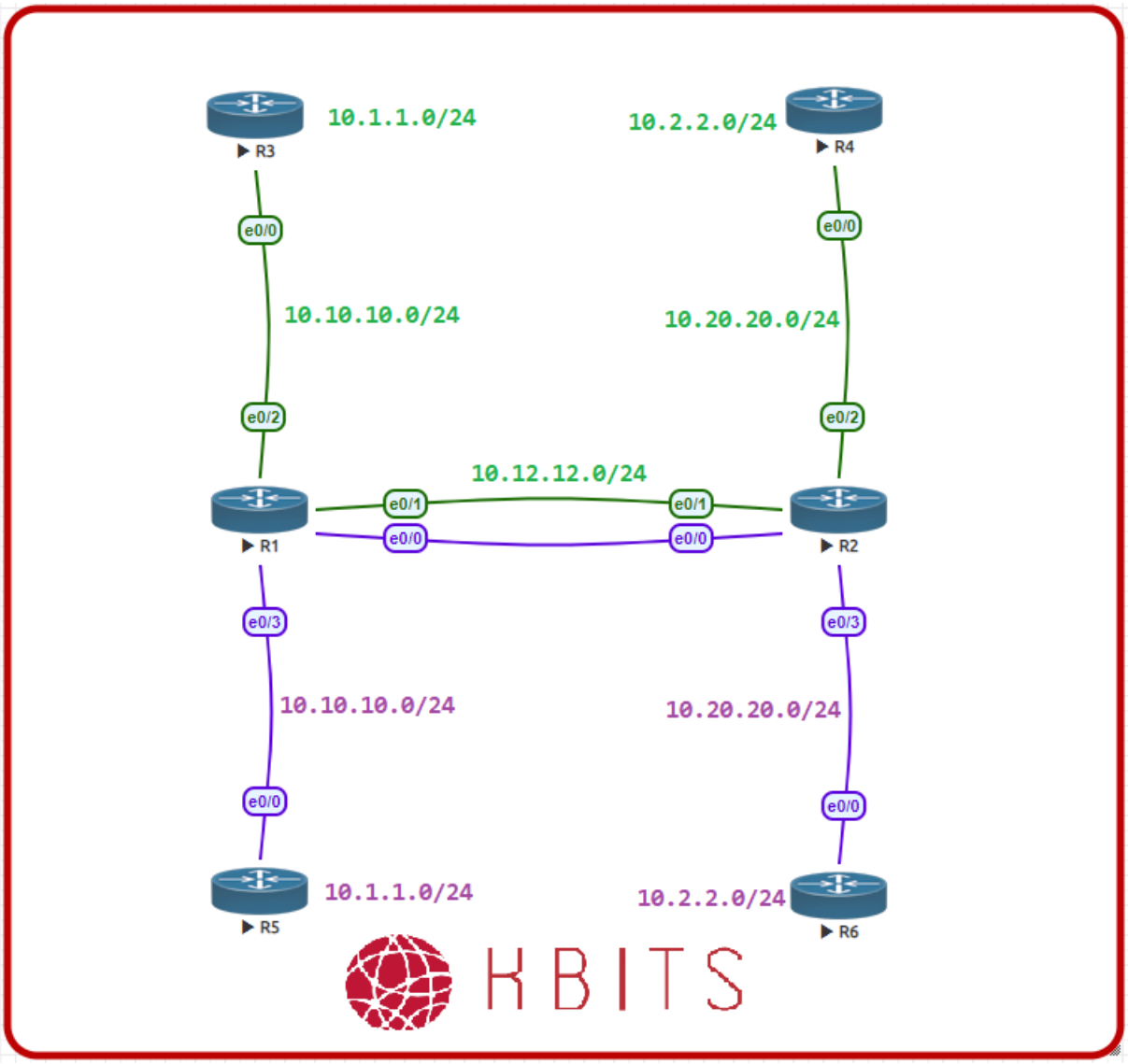
- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Pre-Shared Key: **cisco [Don't use wildcard mask]**
  - Group: 2
  - ISAKMP Keepalive – 10 seconds
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-MD5-HMAC
- Key Server Parameters
  - Identity Number: 100
  - Interesting Traffic: Any traffic on the 10.1.0.0/16 network.
  - Local Address: E 0/0
  - Rekey Transport: Unicast
  - Rekey Key Label: GETVPN
  - Rekey key Encryption: 3des

R8

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cisco address 192.168.10.1
crypto isakmp key cisco address 192.168.20.2
crypto isakmp key cisco address 192.168.30.3
crypto isakmp key cisco address 192.168.40.4
crypto isakmp key cisco address 192.168.50.5
crypto isakmp key cisco address 192.168.70.7
!
Crypto isakmp keepalive 10
!
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
```

```
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
crypto ipsec profile G-PROF
 set transform-set TSET
!
crypto gdoi group ABC
 identity number 100
 server local
  address ipv4 192.168.80.8
  redundancy
    local priority 50
    peer address ipv4 192.1.70.7
  sa ipsec 1
    profile G-PROF
    match address ipv4 101
    rekey transport unicast
    rekey authentication mypubkey rsa GETVPN
    rekey algorithm 3des
```

Lab 9 – Configuring VRF Aware VPN



Lab Scenario:

- Configure VRF-aware IPSec LAN-TO-LAN VPNs.

Initial Setup:

- No Initial Configuration Required.

Lab Tasks:

Task 1

Configure R3, R4, R5 & R6 using normal routing based on the diagram. R3 & R4 are running EIGRP in AS 111. They should enable all interfaces in EIGRP.

R3	**R4**
Int E 0/0 ip address 10.10.10.3 255.255.255.0 no shut ! Int Loopback0 ip address 10.1.1.1 255.255.255.0 ! router eigrp 111 network 10.0.0.0	Int E 0/0 ip address 10.20.20.4 255.255.255.0 no shut ! Int Loopback0 ip address 10.2.2.2 255.255.255.0 ! router eigrp 111 network 10.0.0.0
R5	**R6**
Int E 0/0 ip address 10.10.10.5 255.255.255.0 no shut Int Loopback0 ip address 10.1.1.1 255.255.255.0 ip ospf network point-to-point ! router ospf 1 router-id 0.0.0.5 network 10.0.0.0 0.255.255.255 area 0	Int E 0/0 ip address 10.20.20.6 255.255.255.0 no shut Int Loopback0 ip address 10.2.2.2. 255.255.255.0 ip ospf network point-to-point ! router ospf 1 router-id 0.0.0.6 network 10.0.0.0 0.255.255.255 area 0

Task 2

Creating the VRFs on R1 & R2 based on the following:

- VRF Name: **GREEN**
  - Address-family: IPv4
  - Interfaces: R1
    - E 0/1 – IP Address: 10.12.12.1/24
    - E 0/2 – IP Address: 10.10.10.1/24
  - Interfaces: R2
    - E 0/1 – IP Address: 10.12.12.2/24
    - E 0/2 – IP Address: 10.20.20.2/24
- VRF Name: **BLUE**
  - Address-family: IPv4

- Interfaces: R1
  - E 0/0 – IP Address: 10.12.12.1/24
  - E 0/3 – IP Address: 10.10.10.1/24
- Interfaces: R2
  - E 0/1 – IP Address: 10.12.12.2/24
  - E 0/2 – IP Address: 10.20.20.2/24

R1	**R2**
! VRF: GREEN vrf definition GREEN address-family ipv4 ! Interface E0/1 vrf forwarding GREEN ip address 10.12.12.1 255.255.255.0 no shut ! Interface E 0/2 vrf forwarding GREEN ip add 10.10.10.1 255.255.255.0 no shut **! VRF: BLUE** vrf definition BLUE address-family ipv4 ! Interface E 0/0 vrf forwarding BLUE ip address 10.12.12.1 255.255.255.0 no shut ! Interface E 0/3 vrf forwarding BLUE ip address 10.10.10.1 255.255.255.0 no shut	**! VRF: GREEN** vrf definition GREEN address-family ipv4 ! Interface E0/1 vrf forwarding GREEN ip address 10.12.12.2 255.255.255.0 no shut ! Interface E 0/2 vrf forwarding GREEN ip add 10.20.20.2 255.255.255.0 no shut **! VRF: BLUE** vrf definition BLUE address-family ipv4 ! Interface E 0/0 vrf forwarding BLUE ip address 10.12.12.2 255.255.255.0 no shut ! Interface E 0/3 vrf forwarding BLUE ip address 10.20.20.2 255.255.255.0 no shut

Task 3

Configuring Routing on R1 & R2 based on the following:

- VRF Name: **GREEN**
  - EIGRP AS: 111
- VRF Name: **BLUE**
  - OSPF Area: 0

R1

```
! VRF: GREEN

router eigrp 1
 address-family ipv4 vrf GREEN autonomous-system 111
  network 10.0.0.0

! VRF: BLUE

router ospf 1 vrf BLUE
 network 10.0.0.0 0.255.255.255 area 0 no shut
```

R1

```
! VRF: GREEN

router eigrp 1
 address-family ipv4 vrf GREEN autonomous-system 111
  network 10.0.0.0

! VRF: BLUE

router ospf 1 vrf BLUE
 network 10.0.0.0 0.255.255.255 area 0 no shut
```

Task 4

Encrypt Traffic on R1 towards R2 for VRF-GREEN using the following parameters:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Pre-Shared Key: **Cisco123**
  - Group: 2
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-MD5-HMAC
- Interesting Traffic: 10.1.1.0/24 < - > 10.2.2.0/24

R1

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
 group 2
!
crypto keyring KR1 vrf GREEN
 pre-shared-key address 10.12.12.2 key Cisco123
!
crypto isakmp profile IPROF-GREEN
 match identity address 10.12.12.2 255.255.255.255 GREEN
 vrf GREEN
 keyring KR1
!
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
!
crypto map ABC 10 ipsec-isakmp
 set peer 10.12.12.2
 set transform-set TSET
 match address 101
 set isakmp-profile IPROF-GREEN
!
interface E 0/1
 crypto map ABC
```

R2

```
crypto isakmp policy 10
```

```
 authentication pre-share
 hash md5
 encryption 3des
 group 2
!
crypto keyring KR1 vrf GREEN
 pre-shared-key address 10.12.12.1 key Cisco123
!
crypto isakmp profile IPROF-GREEN
 match identity address 10.12.12.1 255.255.255.255 GREEN
 vrf GREEN
 keyring KR1
!
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
!
access-list 101 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map ABC 10 ipsec-isakmp
 set peer 10.12.12.1
 set transform-set TSET
 match address 101
 set isakmp-profile IPROF-GREEN
!
interface e 0/1
 crypto map ABC
```

Task 4

Encrypt Traffic on R1 towards R2 for VRF-BLUE using the following parameters:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Pre-Shared Key: **Ccie123**
  - Group: 2
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-MD5-HMAC
- Interesting Traffic: 10.1.1.0/24 < - > 10.2.2.0/24

R1

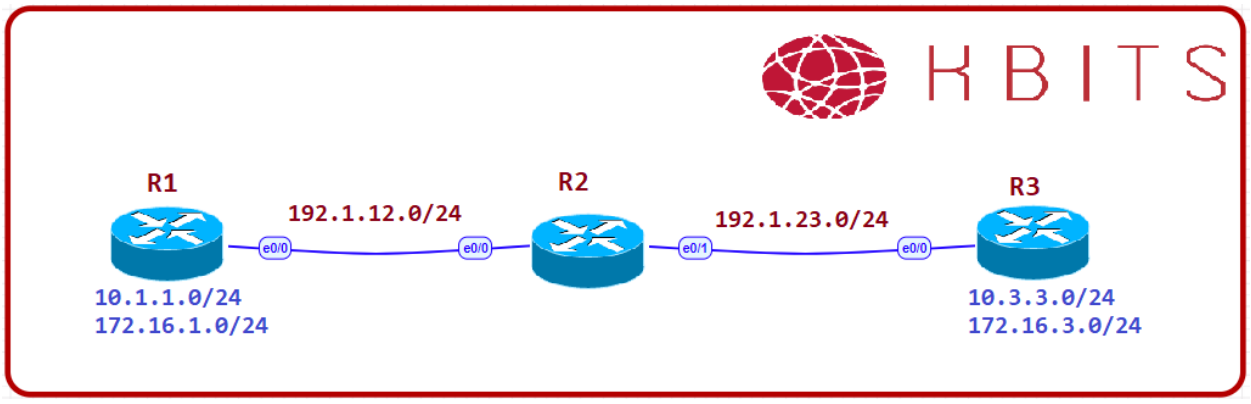
```
crypto keyring KR2 vrf BLUE
 pre-shared-key address 10.12.12.2 key Ccie123
!
```

```
crypto isakmp profile IPROF-BLUE
 match identity address 10.12.12.2 255.255.255.255 BLUE
 vrf BLUE
 keyring KR2
!
access-list 102 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
!
crypto map DEF 10 ipsec-isakmp
 set peer 10.12.12.2
 set transform-set TSET
 match address 102
 set isakmp-profile IPROF-BLUE
!
interface E 0/0
 crypto map DEF
```

R2

```
crypto keyring KR2 vrf BLUE
 pre-shared-key address 10.12.12.1 key Ccie123
!
crypto isakmp profile IPROF-BLUE
 match identity address 10.12.12.1 255.255.255.255 BLUE
 vrf BLUE
 keyring KR2
!
access-list 102 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map DEF 10 ipsec-isakmp
 set peer 10.12.12.1
 set transform-set TSET
 match address 102
 set isakmp-profile IPROF-BLUE
!
interface E 0/0
 crypto map DEF
```

Lab 10 – Configuring a Router as a CA Server



Lab Scenario:

- Configuring R2 as a CA Server. Configuring a VPN Tunnel to encrypt traffic between R1 & R3 using RSA-Signatures. Also, to encrypt traffic from R2 to R3.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure the following Loopback addresses on R1 thru R3.
    - R1: 10.1.1.1/24
    - R2: 10.2.2.2/24
    - R3: 10.3.3.3/24
- Configure EIGRP in AS 100 as the routing protocol to route all networks in the network.

R1	**R2**
Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int loopback 1 Ip add 172.16.1.1 255.255.255.0 ! Int E 0/0	Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int loopback 1 Ip add 172.16.2.2 255.255.255.0 ! Int E 0/0

Ip add 192.1.12.1 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.1.12.0 Network 10.0.0.0	Ip add 192.1.12.2 255.255.255.0 No shut ! Int E 0/1 Ip add 192.1.23.2 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.1.12.0 Network 192.1.23.0 Network 10.0.0.0
R3 Int loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int loopback 1 Ip add 172.16.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.1.23.3 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.1.23.0 Network 10.0.0.0	

Lab Tasks:

Task 1

Assign R2 a domain name of Kbits.live. Also set the timezone and clock to the current timezone and time. Configure R2 to be the CA Server to automatically grant certificates using the following parameters:

- RSA Key Size: 512 Bits
- Key Label: IOS-CA
- Any Passphrase: CCIESEC
- Issuer Name: CN=IOS-CA.kbits.live L=Dubai C=AE

R2 Ip domain-name kbits.live !

```
clock timezone GST 4
!
clock set [Current Time]
!
crypto key generate rsa general-keys label IOS-CA
!
ip http server
!
Crypto pki server IOS-CA
   issuer-name CN=IOS-CA.kbits.live L=Dubai C=AE
   grant auto
   no shut

*** At this point R2 has a Root Certificate that it will use to Sign and
Verify all certificates that it issues.
```

Task 2

Assign R1 and R3 a domain name of Khawarb.com. Also set the timezone and clock to the current timezone and time.

R1

```
Ip domain-name kbits.live
!
clock timezone GST 4
!
clock set [Current Time]
```

R3

```
Ip domain-name kbits.live
!
clock timezone GST 4
!
clock set [Current Time]
```

Task 3

Generate 512 Bit RSA keys on R1 and R3. Configure R1 & R3 to request a certificate from R2, the IOS-based CA Server. Use **CISCO123** as the recovery password. Disable CRL checking.

R1

```
crypto key generate rsa
!
crypto pki trustpoint IOS-CA
```

```
 enrollment url http://10.2.2.2:80
 revocation-check none
!
crypto pki authenticate IOS-CA
!
crypto pki enroll IOS-CA
```

R3

```
crypto key generate rsa
!
crypto pki trustpoint IOS-CA
 enrollment url http://10.2.2.2:80
 revocation-check none
!
crypto pki authenticate IOS-CA
!
crypto pki enroll IOS-CA
```

Task 4

Configure an IPSec Tunnel to encrypt traffic between 10.1.1.0 and 10.3.3.0 networks. Use the following parameters for the tunnel:

- Authentication type = RSA-SIG
- Hash = MD5
- Diffie-Hellman = 2
- Encryption = 3DES
- IPSec Encryption = ESP-3DES
- IPSec Authentication = ESP-MD5-HMAC

R1

```
Crypto isakmp pol 10
 group 2
 hash md5
 encr 3des
!
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
!
access-list 155 permit ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255
!
crypto map I-MAP 10 ipsec-isakmp
 set peer 192.168.23.3
 set transform-set TSET
 match address 155
!
```

```
int E 0/0
 crypto map I-MAP
```

R3

```
Crypto isakmp pol 10
 group 2
 hash md5
 encr 3des
!
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
!
access-list 155 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map I-MAP 10 ipsec-isakmp
 set peer 192.168.12.1
 set transform-set TSET
 match address 155
!
int E 0/0
 crypto map I-MAP
```

Task 5

Configure an IPSec Tunnel to encrypt traffic between 10.2.2.0 and 10.3.3.0 networks. Use the following parameters for the tunnel:

- Authentication type = RSA-SIG
- Hash = MD5
- Diffie-Hellman = 2
- Encryption = 3DES
- IPSec Encryption = ESP-3DES
- IPSec Authentication = ESP-MD5-HMAC

Task 6

As the previous task requires the CA Server to also participate in the Data encryption, it requires to generate a separate key pair for that and request a Identity certificate from itself. So Generate a separate RSA key pair and request a certificate before configuring the IPSec Tunnel.

R2

```
crypto key generate rsa
!
crypto pki trustpoint IOS-ID
 enrollment url http://10.2.2.2:80
 revocation-check none
```

```
!
crypto pki authenticate IOS-ID
!
crypto pki enroll IOS-ID
!
Crypto isakmp pol 10
 group 2
 hash md5
 encr 3des
!
crypto ipsec transform-set TSET esp-3des esp-md5-hmac
!
access-list 155 permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
!
crypto map I-MAP 10 ipsec-isakmp
 set peer 192.168.23.3
 set transform-set TSET
 match address 155
!
int E 0/1
 crypto map I-MAP
```

R3

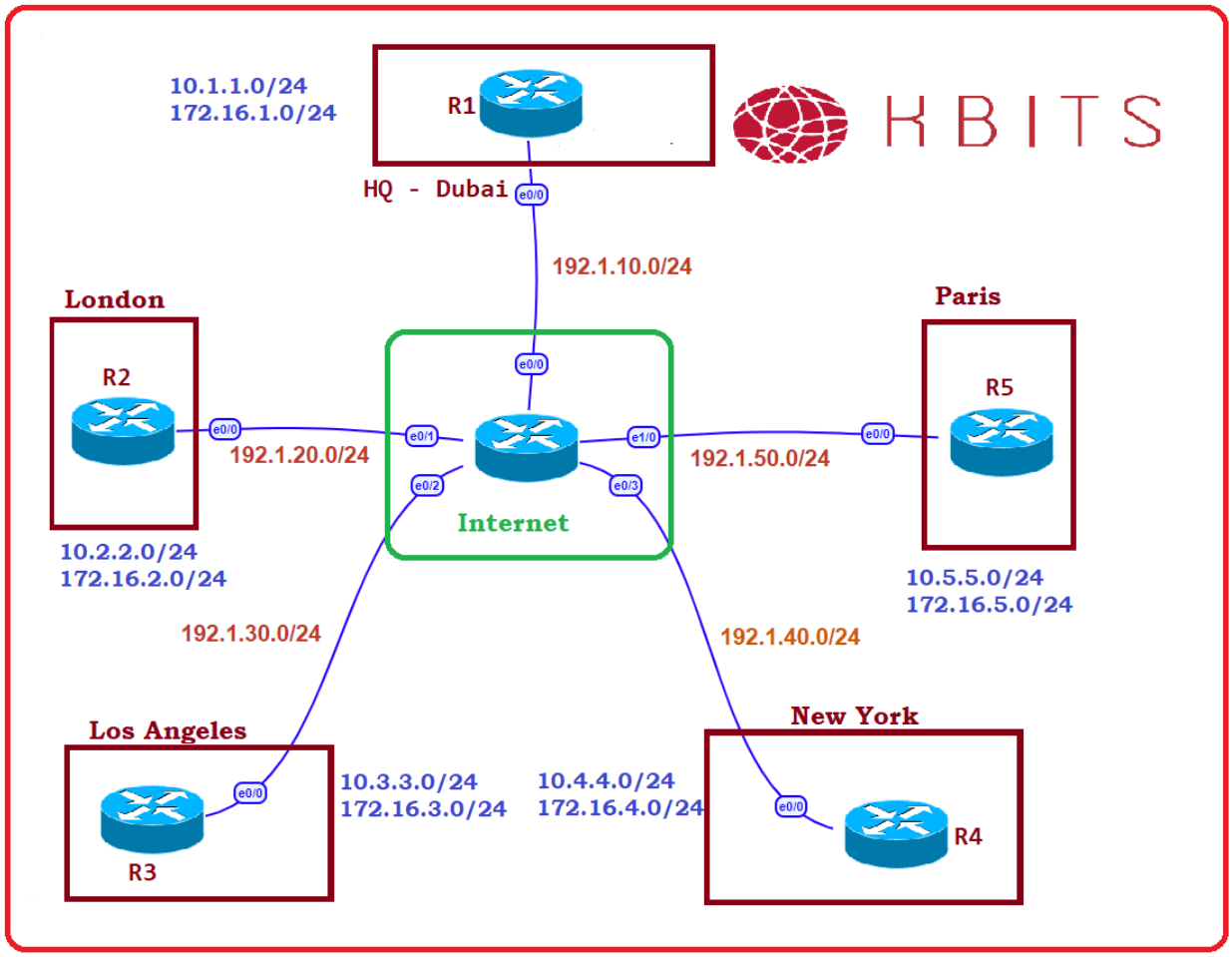
```
! As we are using the same set of parameters for ISAKMP and IPSec that
! were used in the previous tunnel, I don't need to redefine them.
!
access-list 156 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
!
crypto map I-MAP 20 ipsec-isakmp
 set peer 192.168.23.2
 set transform-set TSET
 match address 156
```

CCIE Security v6 – Advanced VPNs

Module 3 – Configuring VPNS Using IKEv2

Module 3 – Configuring VPNs Using IKEv2

Lab 1 – Site-To-Site IPSec VPN Using IKEv2 – Crypto Maps



Lab Scenario:

- Configure IKEv2 using Crypto Maps

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure Default Routes on R1 thru R4 pointing towards R5.
- Configure the following Loopback addresses on R1 thru R4:
  - R1: 10.1.1.1/24 and 172.16.1.1/24

- R2: 10.2.2.2/24 and 172.16.2.2/24
- R3: 10.3.3.3/24 and 172.16.3.3/24
- R4: 10.4.4.4/24 and 172.16.4.4/24

R1	**R2**
Int Loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int Loopback 1 Ip add 172.16.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.10.6	Int Loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int Loopback 1 Ip add 172.16.2.2 255.255.255.0 ! Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.6
R3	**R4**
Int Loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int Loopback 1 Ip add 172.16.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.1.30.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.30.6	Int Loopback 0 Ip add 10.4.4.4 255.255.255.0 ! Int Loopback 1 Ip add 172.16.4.4 255.255.255.0 ! Int E 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.40.6
R5	**R6**
Int Loopback 0 Ip add 10.5.5.5 255.255.255.0 ! Int Loopback 1 Ip add 172.16.5.5 255.255.255.0 ! Int E 0/0 Ip add 192.1.50.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.50.6	Interface E 0/0 Ip address 192.1.10.6 255.255.255.0 No shut ! Interface E 0/1 Ip address 192.1.20.6 255.255.255.0 No shut ! Interface E 0/2 Ip address 192.1.30.6 255.255.255.0 No shut ! Interface E 0/3

	Ip address 192.1.40.6 255.255.255.0 No shut ! Interface E 1/0 Ip address 192.1.50.6 255.255.255.0 No shut

Lab Tasks:

Task 1

Configure a IPSec Tunnel to encrypt traffic from 10.1.1.0/24 on R1 (Loopback 0) to the 10.2.2.0/24 on R2 (Loopback 0).

Task 2

Use the following Parameters for the Tunnel between R1 and R2:

- IKEv2 Proposal Parameters
  - Integrity: SHA1
  - Encryption: 3DES
  - Group: 2
  - Authentication: Pre-share
  - Pre-Shared Key (R1): **cisco1**
  - Pre-Shared Key (R2): **cisco2**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-MD5-HMAC

R1

```
crypto ikev2 proposal PROP1
 integrity sha1
 group 2
 encryption 3des
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR_R2
 peer R2
   address 192.1.20.2
   pre-shared local cisco1
   pre-shared remote cisco2
!
crypto ikev2 profile PROF1
 match identity remote address 192.1.20.2
```

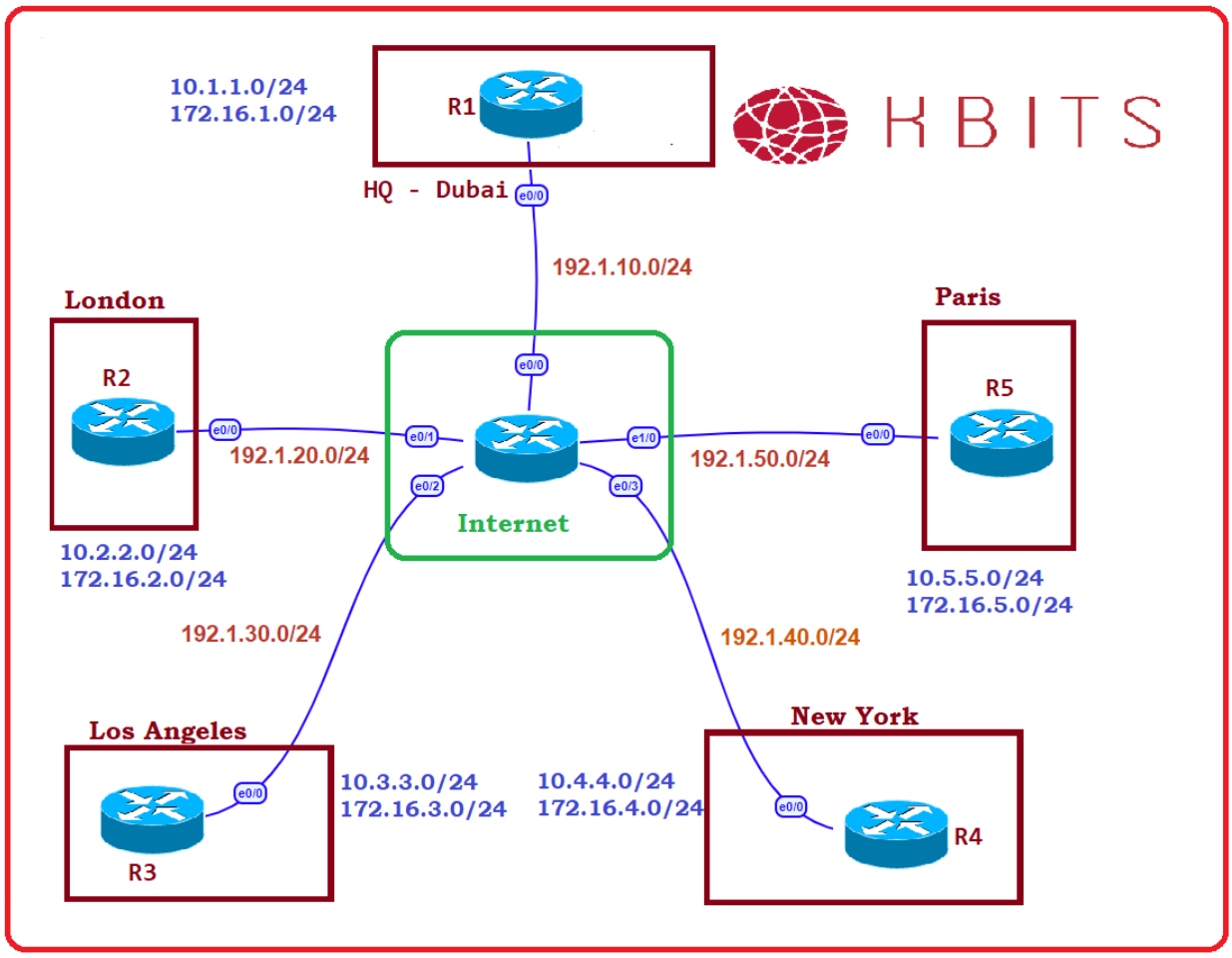
```
 authentication local pre-share
 authentication remote pre-share
 keyring local KR_R2
!
crypto ipsec transform-set ABC esp-3des esp-md5-hmac
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
!
crypto map ABC 10 ipsec-isakmp
 match address 101
 set peer 192.1.20.2
 set transform-set ABC
 set ikev2-profile PROF1
!
Int E 0/0
 crypto map ABC
```

R2

```
crypto ikev2 proposal PROP1
 integrity sha1
 group 2
 encryption 3des
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR_R1
 peer R1
   address 192.1.10.1
   pre-shared local cisco2
   pre-shared remote cisco1
!
crypto ikev2 profile PROF1
 match identity remote address 192.1.10.1
 authentication local pre-share
 authentication remote pre-share
 keyring local KR_R1
!
crypto ipsec transform-set ABC esp-3des esp-md5-hmac
!
access-list 101 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map ABC 10 ipsec-isakmp
 match address 101
 set peer 192.1.10.1
```

```
 set transform-set ABC
 set ikev2-profile PROF1
!
int E 0/0
 crypto map ABC
```

Lab 2 – Site-To-Site IPSec VPN Using IKEv2 – S–VTI



Lab Scenario:

- Configure an IPSec tunnel to encrypt traffic from the R3 to R4 to encrypt traffic from the 10.3.3.0/24 & 172.16.3.0/24 network to the 10.4.4.0/24 & 172.16.4.0/24 using IKEv2. Use Native IPSec Tunnel for this Lab.

Initial Setup:

- **Based on the previous Lab**

Lab Objectives:

Task 1

Configure a Native IPSec Tunnel to Connect R3 to R4. Use the following Parameters for the Tunnel between R3 and R4:

- IKEv2 Proposal Parameters
  - Integrity: SHA1
  - Encryption: 3DES
  - Group: 2
  - Authentication: Pre-share
  - Pre-Shared Key (R3): **cisco3**
  - Pre-Shared Key (R4): **cisco4**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-MD5-HMAC
- Tunnel Parameters
  - Address: 192.168.34.0/24
  - Tunnel Protocol: IPSec

R3

```
crypto ikev2 proposal PROP1
 integrity sha1
 group
 encryption 3des
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR_R4
 peer R4
   address 192.1.40.4
   pre-shared local cisco3
   pre-shared remote cisco4
!
crypto ikev2 profile PROF1
 match identity remote address 192.1.40.4
 authentication remote pre-share
 authentication local pre-share
 keyring local KR_R4
!
crypto ipsec transform-set ABC esp-3des esp-md5-hmac
!
crypto ipsec profile ABC
```

```
 set transform-set ABC
 set ikev2-profile PROF1
!
int tunnel 1
 ip add 192.168.34.3 255.255.255.0
 tunnel source 192.1.30.3
 tunnel destination 192.1.40.4
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ABC
```

R4

```
crypto ikev2 proposal PROP1
 integrity sha1
 group 2
 encryption 3des
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR_R3
 peer R3
   address 192.1.30.3
   pre-shared local cisco4
   pre-shared remote cisco3
!
crypto ikev2 profile PROF1
 match identity remote address 192.1.30.3
 authentication remote pre-share
 authentication local pre-share
 keyring local KR_R3
!
crypto ipsec transform-set ABC esp-3des esp-md5-hmac
!
crypto ipsec profile ABC
 set transform-set ABC
 set ikev2-profile PROF1
!
int tunnel 1
 ip add 192.168.34.4 255.255.255.0
 tunnel source 192.1.40.4
 tunnel destination 192.1.30.3
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ABC
```

Task 2

Configure EIGRP in AS 34 between R3 & R4 on the Tunnel Interface. Injecct the Loopback Networks into EIGRP.

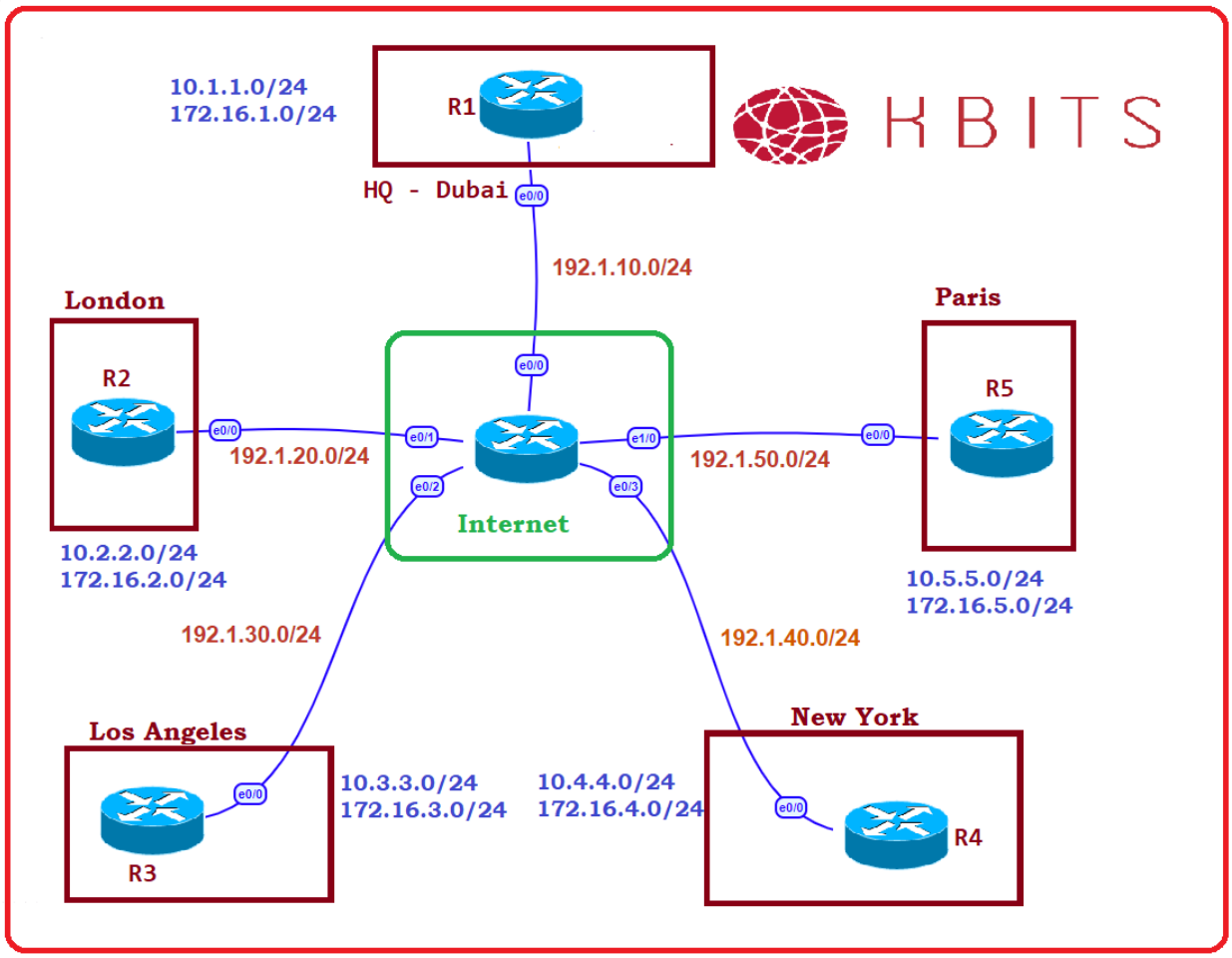
R3 router eigrp 34 network 10.0.0.0 network 172.16.0.0 network 192.168.34.0
R4 router eigrp 34 network 10.0.0.0 network 172.16.0.0 network 192.168.34.0

CCIE Security v6 – Advanced VPNs

Module 4 – Configuring Flex VPNS

Module 4 – Configuring Flex VPNs

Lab 1 – Site-To-Site IPSec VPN Using Flex VPN



Lab Scenario:

- Configure a Site-to-Site IPSec Flex VPN between R1 & R2.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure Default Routes on R1 thru R4 pointing towards R5.
- Configure the following Loopback addresses on R1 thru R4:
  - R1: 10.1.1.1/24 and 172.16.1.1/24

- R2: 10.2.2.2/24 and 172.16.2.2/24
- R3: 10.3.3.3/24 and 172.16.3.3/24
- R4: 10.4.4.4/24 and 172.16.4.4/24

R1	**R2**
Int Loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int Loopback 1 Ip add 172.16.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.10.6	Int Loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int Loopback 1 Ip add 172.16.2.2 255.255.255.0 ! Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.6
R3	**R4**
Int Loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int Loopback 1 Ip add 172.16.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.1.30.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.30.6	Int Loopback 0 Ip add 10.4.4.4 255.255.255.0 ! Int Loopback 1 Ip add 172.16.4.4 255.255.255.0 ! Int E 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.40.6
R5	**R6**
Int Loopback 0 Ip add 10.5.5.5 255.255.255.0 ! Int Loopback 1 Ip add 172.16.5.5 255.255.255.0 ! Int E 0/0 Ip add 192.1.50.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.50.6	Interface E 0/0 Ip address 192.1.10.6 255.255.255.0 No shut ! Interface E 0/1 Ip address 192.1.20.6 255.255.255.0 No shut ! Interface E 0/2 Ip address 192.1.30.6 255.255.255.0 No shut ! Interface E 0/3

	Ip address 192.1.40.6 255.255.255.0 No shut ! Interface E 1/0 Ip address 192.1.50.6 255.255.255.0 No shut

Lab Tasks:

Task 1

Configure a Site-to-Site Flex VPN to encrypt traffic from 10.1.1.0/24 & 172.16.1.0/24 networks on R1 (Loopback 0 & Loopback 1) to the 10.2.2.0/24 & 172.16.2.0/24 on R2 (Loopback 0 & Loopback 1). Do not create a Static VTI on R1. It should be created dynamically based on an incoming connection from R2.

Task 2

Use the following Parameters for the Tunnel between R1 and R5:

- IKEv2 Proposal Parameters
  - Integrity: SHA1
  - Encryption: 3DES
  - Group: 2
  - Authentication: Pre-share
  - Pre-Shared Key: **Cisco123**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-sha-HMAC
- Tunnel IP Address:
  - IP Address for Virtual-template on R1: 192.168.1.1/24
  - Tunnel Interface on R5: 192.168.1.5/24
- EIGRP AS#: 12353

R1

```
crypto ikev2 proposal PROP1
 encryption 3des
 integrity sha1
 group 2
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR1
 peer R2
```

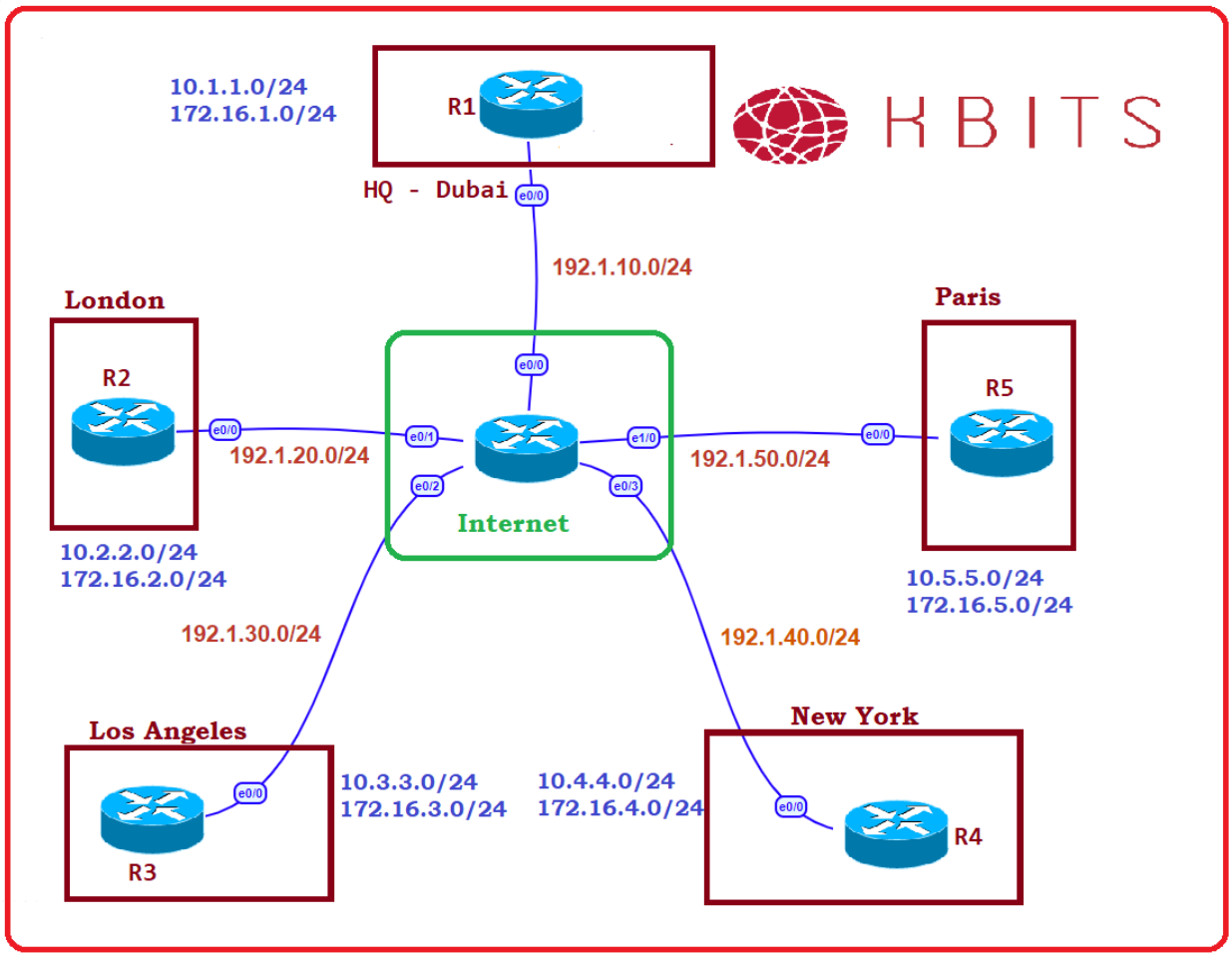
```
  pre-shared-key Cisco123
  address 0.0.0.0
!
crypto ikev2 profile IKEv2-PROF
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local KR1
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile IPROF
 set transform-set TSET
 set ikev2-profile IKEv2-PROF
!
Interface loopback99
 ip address 192.168.1.1 255.255.255.0
!
Interface virtual-template 1 type tunnel
 ip unnumbered Loopback99
 tunnel source E0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPROF
!
crypto ikev2 profile IKEv2-PROF
 virtual-template 1
!
Router eigrp 12353
 network 192.168.1.0
 network 10.0.0.0
 network 172.16.0.0
```

R2

```
crypto ikev2 proposal PROP1
 encryption 3des
 integrity sha1
 group 2
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR1
 peer R1
  pre-shared-key Cisco123
  address 192.1.10.1
```

```
!
crypto ikev2 profile IKEv2-PROF
 match identity remote address 192.1.10.1
 authentication local pre-share
 authentication remote pre-share
 keyring local KR1
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile IPROF
 set transform-set TSET
 set ikev2-profile IKEv2-PROF
!
Interface Tunnel 1
 ip address 192.168.1.2 255.255.255.0
 tunnel source E0/0
 tunnel destination 192.1.10.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPROF
!
router eigrp 12353
 network 192.168.1.0
 network 10.0.0.0
 network 172.16.0.0
```

Lab 2 – Spoke-To-Spoke IPSec VPN Using Flex VPN



Lab Scenario:

- Configure a Spoke-to-Spoke Tunnel between R3, R5 & R5 Using Flex VPN.

Initial Setup:

- **Based on the previous Lab**

Lab Objectives:

Task 1

Configure a Spoke-to-Spoke IPSec tunnel using Flex VPN to encrypt traffic between R3, R4 & R5. R5 is the Hub. Use the following parameters:

- IKEv2 Proposal Parameters
  - Integrity: SHA1
  - Encryption: 3DES
  - Group: 2
  - Authentication: Pre-share
  - Pre-Shared Key: **Cisco123**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-MD5-HMAC
- Tunnel Parameters
  - Pool: FLEX – 192.168.1.101 192.168.1.200
  - NHRP Network ID: 1
  - Tunnel Interface #: 1
  - Virtual-Template #: 1

R5 – Hub

```
crypto ikev2 proposal PROP1
 encryption 3des
 integrity sha1
 group 2
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR1
 peer ALL
  pre-shared-key Cisco123
  address 0.0.0.0
!
crypto ikev2 profile IKEv2-PROF
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local KR1
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile IPROF
```

```
 set transform-set TSET
 set ikev2-profile IKEv2-PROF
!
Interface loopback99
 ip address 192.168.1.1 255.255.255.0
!
Interface virtual-template 1 type tunnel
 ip unnumbered Loopback99
 tunnel source E0/0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile IPROF
!
crypto ikev2 profile IKEv2-PROF
 virtual-template 1
!
router eigrp 12353
 network 192.168.1.0
 network 10.0.0.0
 network 172.16.0.0
!
ip local pool FLEX 192.168.1.21 192.168.1.200
!
crypto ikev2 authorization policy default
 pool FLEX
 route set interface
!
aaa new-model
aaa authorization network default local
!
crypto ikev2 profile IKEv2-PROF
 aaa authorization group override psk list default default
```

R3

```
crypto ikev2 proposal PROP1
 encryption 3des
 integrity sha1
 group 2
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR1
 peer ALL
  pre-shared-key Cisco123
```

```
  address 0.0.0.0
!
crypto ikev2 profile IKEv2-PROF
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local KR1
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile IPROF
 set transform-set TSET
 set ikev2-profile IKEv2-PROF
!
Interface Tunnel 1
 ip address negotiated
 tunnel source E 0/0
 tunnel destination 192.1.50.5
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel protection ipsec profile IPROF
!
Interface virtual-template 1 type tunnel
 ip unnumbered Tunnel1
 tunnel source E0/0
 ip nhrp network-id 1
 ip nhrp shortcut
 tunnel protection ipsec profile IPROF
!
crypto ikev2 profile IKEv2-PROF
 virtual-template 1
!
router eigrp 12353
 network 192.168.1.0
 network 10.0.0.0
 network 172.16.0.0
!
crypto ikev2 authorization policy default
 route set interface
!
aaa new-model
aaa authorization network default local
!
crypto ikev2 profile IKEv2-PROF
 aaa authorization group override psk list default default
```

R4

```
crypto ikev2 proposal PROP1
 encryption 3des
 integrity sha1
 group 2
!
crypto ikev2 policy POL1
 proposal PROP1
!
crypto ikev2 keyring KR1
 peer ALL
  pre-shared-key Cisco123
  address 0.0.0.0
!
crypto ikev2 profile IKEv2-PROF
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring local KR1
!
crypto ipsec transform-set TSET esp-3des esp-sha-hmac
!
crypto ipsec profile IPROF
 set transform-set TSET
 set ikev2-profile IKEv2-PROF
!
Interface Tunnel 1
 ip address negotiated
 tunnel source E 0/0
 tunnel destination 192.1.50.5
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel protection ipsec profile IPROF
!
Interface virtual-template 1 type tunnel
 ip unnumbered Tunnel1
 tunnel source E0/0
 ip nhrp network-id 1
 ip nhrp shortcut
 tunnel protection ipsec profile IPROF
!
crypto ikev2 profile IKEv2-PROF
 virtual-template 1
!
```

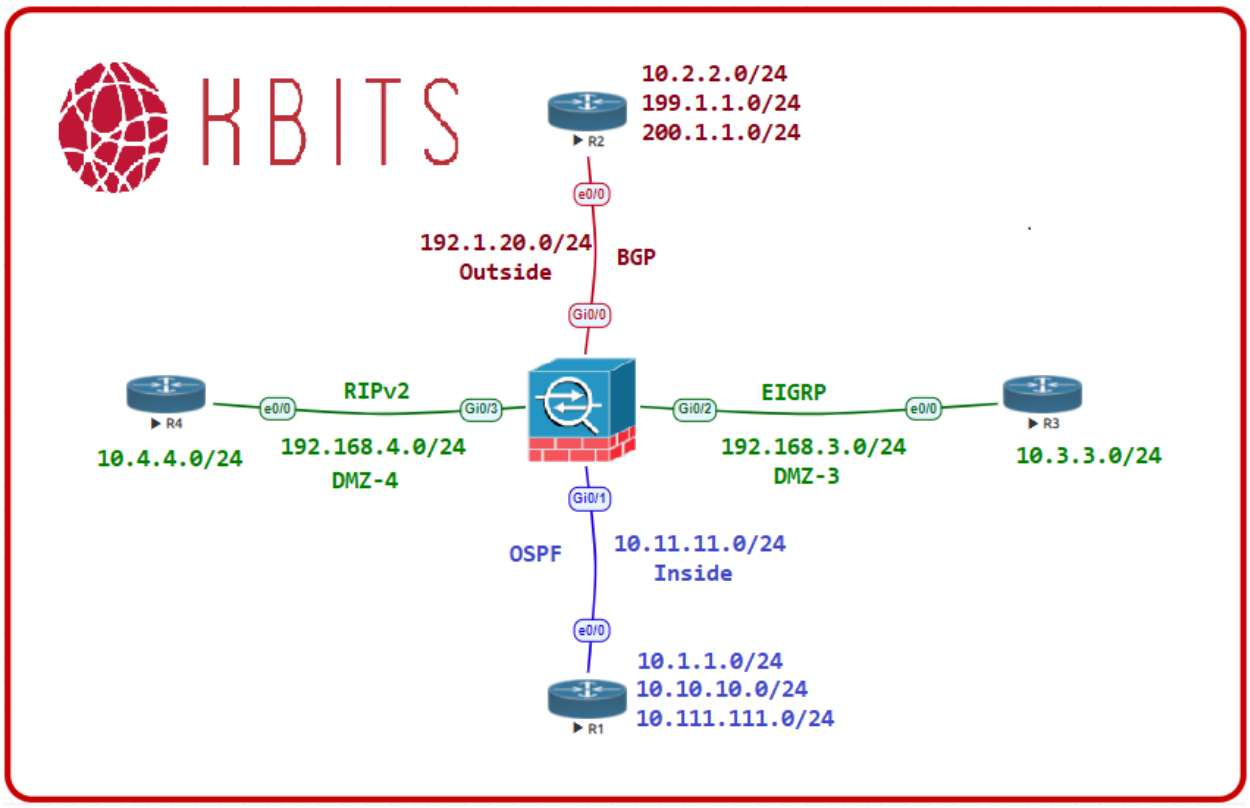
```
router eigrp 12353
 network 192.168.1.0
 network 10.0.0.0
 network 172.16.0.0
!
crypto ikev2 authorization policy default
 route set interface
!
aaa new-model
aaa authorization network default local
!
crypto ikev2 profile IKEv2-PROF
 aaa authorization group override psk list default default
```

CCIE Security v6 – Configuring ASA, FTD, IPS & ZBF

Module 1:
Basic ASA Configurations on 9.X

Module 1 – Basic ASA Configurations on 9.X

Lab 1 – Initializing the FW



Lab Scenario:

- Initialize the Firewall with IP Address, Security Levels and Names of interfaces.
- Configure NTP to synchronize clocks.

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.
- Configure Default Routes on R1, R3 and R4 pointing towards the FW based on the appropriate FW Interface IP.
- Configure the loopbacks on the Routers based on the Network Diagram.

R1	R2

Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int loopback1 Ip address 10.10.10.1 255.255.255.0 ! Int Loopkback2 Ip address 10.111.111.1 255.255.255.0 ! Int E 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10	Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int loopback1 Ip address 199.1.1.1 255.255.255.0 ! Int Loopkback2 Ip address 200.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut
R3 Int E 0/0 Ip address 192.168.3.3 255.255.255.0 No shut ! Int loo0 Ip add 10.3.3.3 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.168.3.10	**R4** Int E 0/0 Ip add 192.168.4.4 255.255.255.0 No shut ! Int loo 0 Ip add 10.4.4.4 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.168.4.10

Lab Tasks:

Task 1

Configure the ASA with the following IP configuration for the Interfaces:

Interface	Name	Security Level	IP Address
G 0/0	Outside	0	192.1.20.10/24
G 0/1	Inside	100	10.11.11.10/24
G 0/2	DMZ3	50	192.168.3.10/24
G 0/3	DMZ4	50	192.168.4.10/24

At this point, the ASA should be able to ping all the surrounding routers.

FW

```
Interface G 0/0
 Nameif Outside
 Ip address 192.1.20.10 255.255.255.0
 No shut
```

```
!
Interface G 0/1
 Nameif Inside
 Ip address 10.11.11.10 255.255.255.0
 No shut
!
Interface G 0/2
 Nameif DMZ3
 Ip address 192.168.3.10 255.255.255.0
 Security-level 50
 No shut
!
Interface G 0/3
 Nameif DMZ4
 Ip address 192.168.4.10 255.255.255.0
 Security-level 50
 No shut
```

Task 2

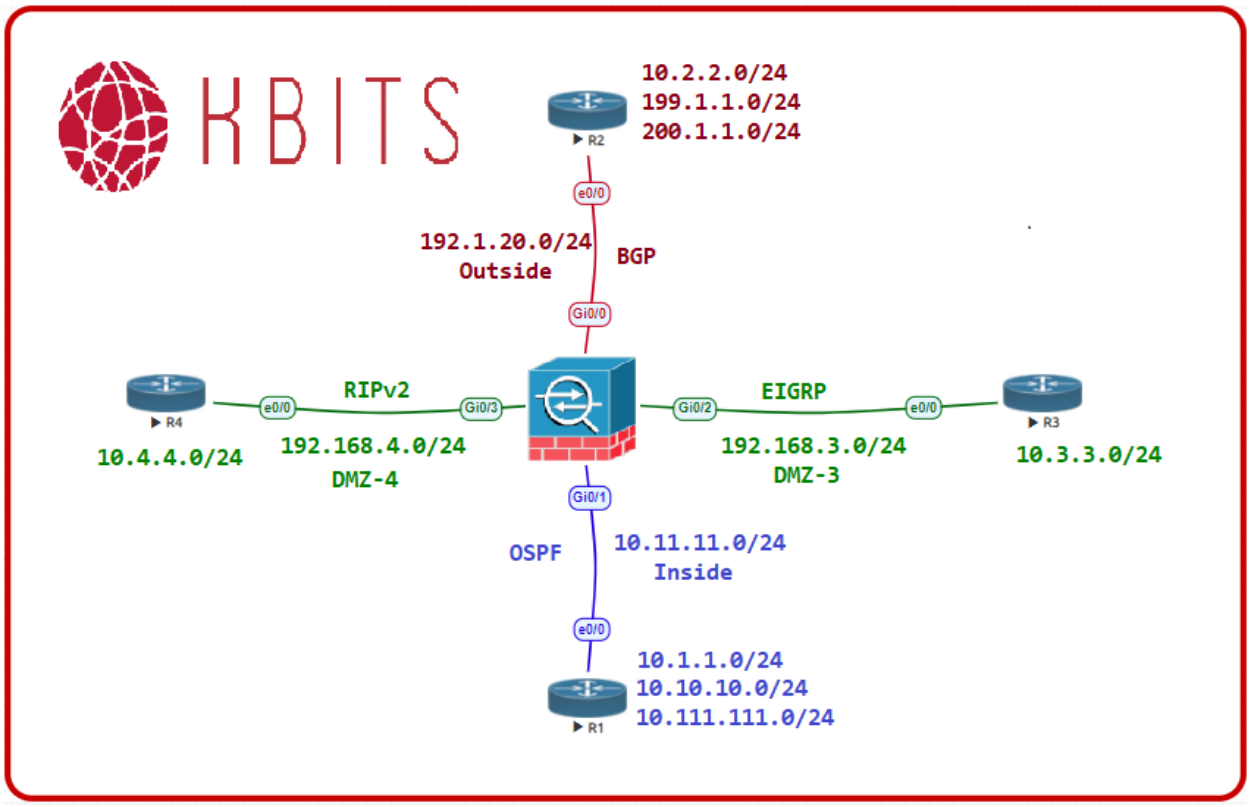
Configure the ASA to give out IP Configuration on the DMZ3 interface using the following information:

- IP Range: 192.168.3.51 – 192.168.3.100
- DNS Server: 192.168.3.35
- WINS Server: 192.168.3.36

FW

```
dhcpd dns 192.168.3.35 interface DMZ3
dhcpd wins 192.168.3.36 interface DMZ3
dhcpd address 192.168.3.51-192.168.3.100 DMZ3
dhcpd enable DMZ3
```

Lab 2 – Static and Default Routes



Lab Scenario:

- Configure Default and Static routes on the Firewall to provide connectivity.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure the Firewall with Static Routes for all internal loopback networks. Internal Networks include networks off of the Inside, DMZ3 and DMZ4 interfaces.

FW

```
Route inside 10.1.1.0 255.255.255.0 10.11.11.1
Route DMZ3 10.3.3.0 255.255.255.0 192.168.3.3
Route DMZ4 10.4.4.0 255.255.255.0 192.168.4.4
```

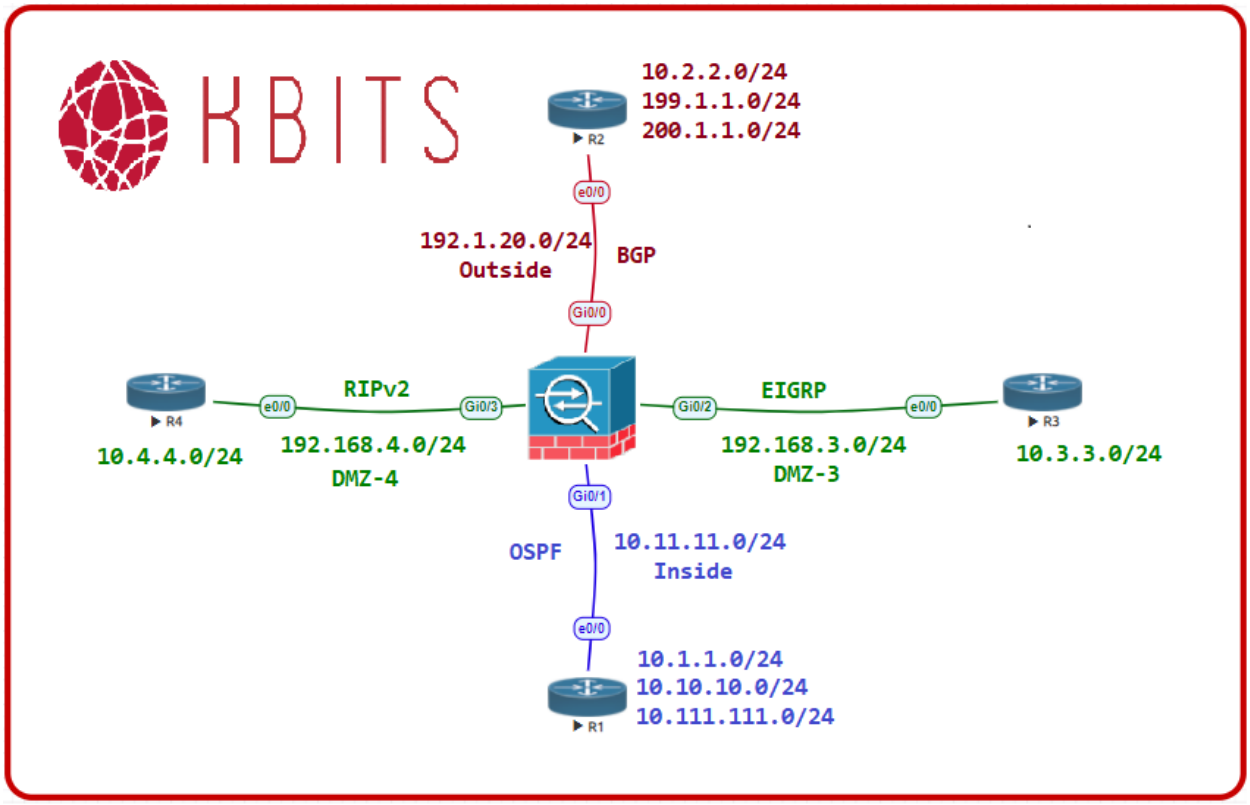
Task 2

Configure a default route on the Firewall pointing towards R2.

FW

```
Route outside 0 0 192.1.20.2
```

Lab 3 – Running RIP V2



Lab Scenario:

- Clear the Static Route configuration on the Routers and the Firewall.
- Configure RIP v2 on the Firewall.
- Configure MD5 authentication for RIP.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Clear all the static routes on the Routers and Firewall. You will be configuring Dynamic Routing protocols on them to learn routes.

FW Clear configure route
R1 No ip route 0.0.0.0 0.0.0.0
R2 No ip route 10.1.1.0 255.255.255.0
R3 No ip route 0.0.0.0 0.0.0.0
R4 No ip route 0.0.0.0 0.0.0.0

Task 2

Configure RIP v2 on the FW on the DMZ3 and DMZ4 interface. Disable auto-summarization of routes. Also, configure RIP v2 on R3 and R4. Advertise the Loopback networks on R3 & R4.

FW Router rip No auto-summary Version 2 Network 192.168.3.0 Network 192.168.4.0
R3 Router rip No auto-summary Version 2 Network 192.168.3.0 Network 10.0.0.0
R4 Router rip

```
No auto-summary
Version 2
Network 192.168.4.0
Network 10.0.0.0
```

Task 3

Configure the Firewall, R3 and R4 with RIP v2 authentication using a Key **1** and password of **cciesec**.

FW

```
Interface G 0/2
 Rip authentication mode md5
 Rip authentication key cciesec key_id 1
```

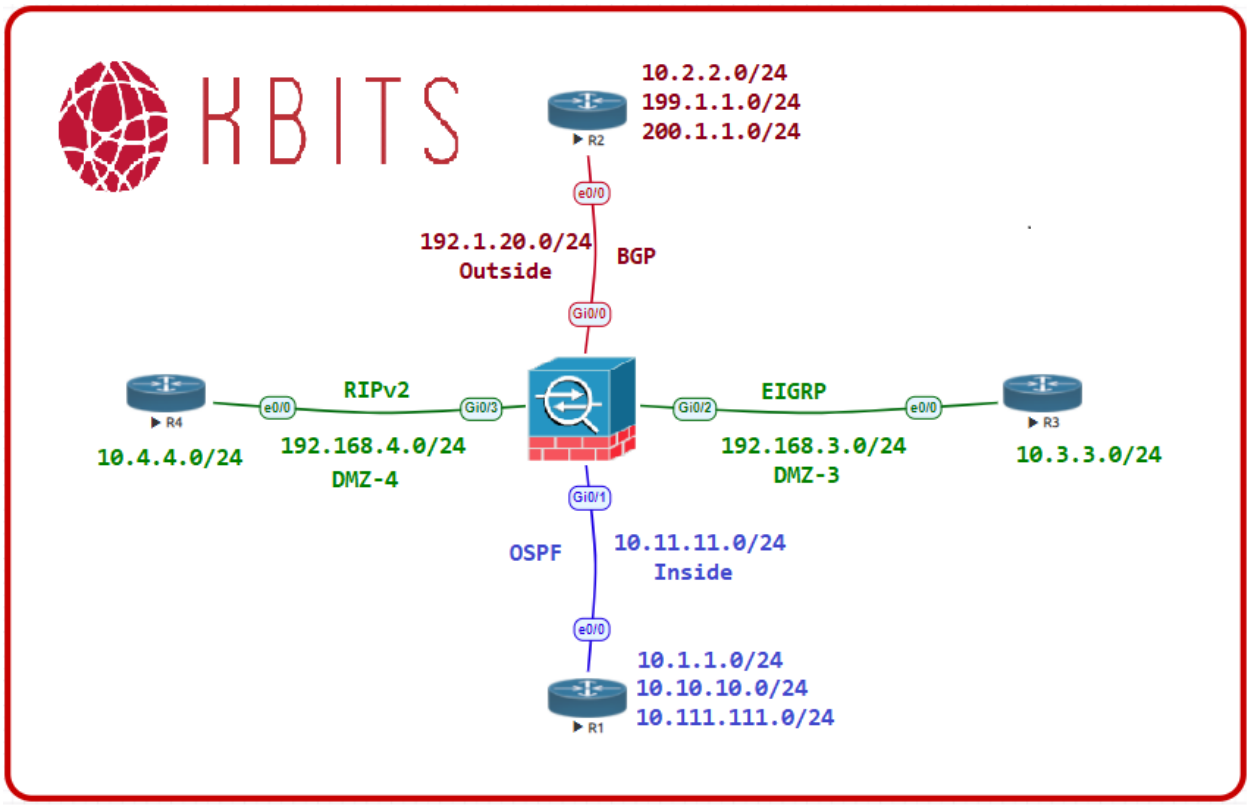
R3

```
Key chain AUTH
 Key 1
   Key-string cciesec
!
Int E 0/0
 Ip rip authentication mode md5
 Ip rip authentication key-chain AUTH
```

R4

```
Key chain AUTH
 Key 1
   Key-string cciesec
!
Int E 0/0
 Ip rip authentication mode md5
 Ip rip authentication key-chain AUTH
```

Lab 4 – Running OSPF



Lab Scenario:

- Configure OSPF on the Firewall.
- Configure MD5 authentication for OSPF.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure OSPF on the outside interface of the ASA in Area 0. Hard-code the Router-id as 10.10.10.10. Also, configure OSPF on R2. Hard-code the router-id as 2.2.2.2. Have R2 advertise the Loopback network in OSPF.

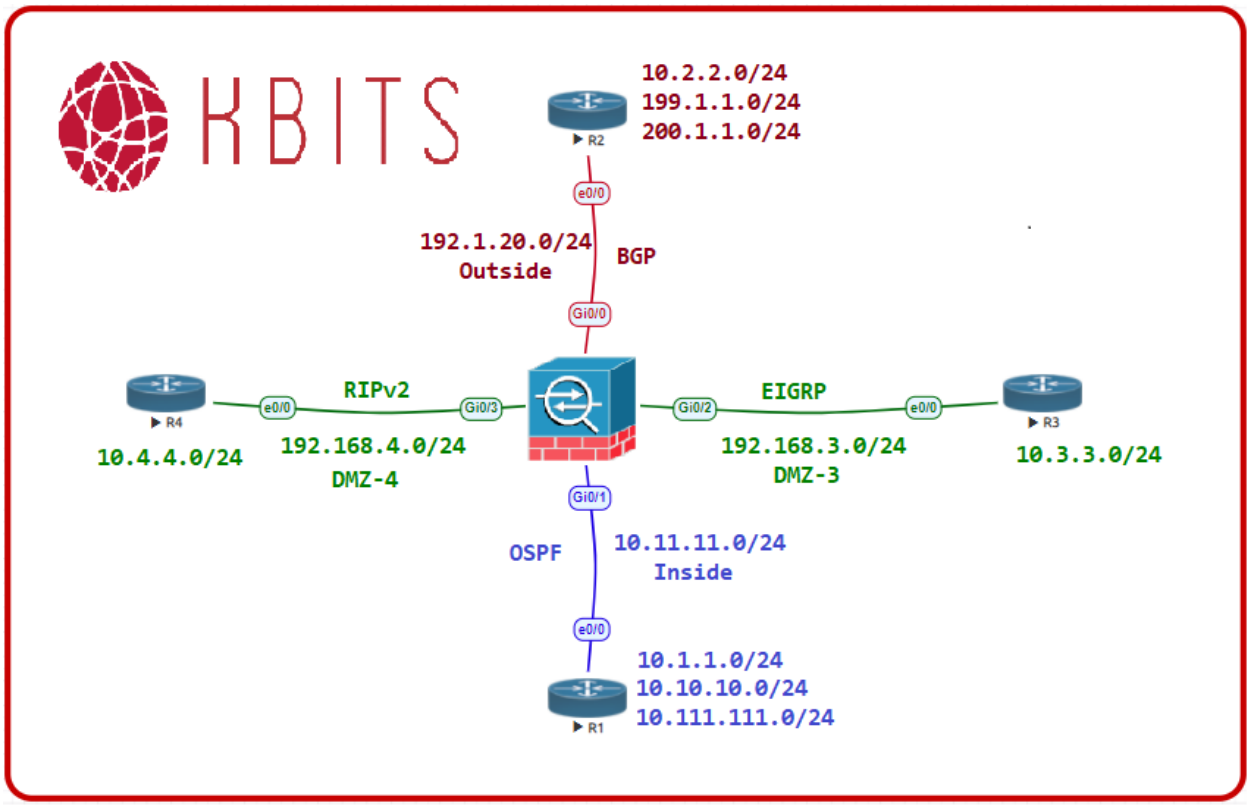
FW
Router OSPF 1 Router-id 10.10.10.10 Network 192.1.20.0 255.255.255.0 area 0
R2
Router OSPF 1 Router-id 2.2.2.2 Network 192.1.20.0 0.0.0.255 area 0 Network 10.2.2.0 0.0.0.255 area 0

Task 2

Configure the Firewall and R2 with a key of **1** and a password of **cciesec**. For MD5 authentication.

FW
Interface G 0/0 Ospf authentication message-digest Ospf message-digeset-key 1 md5 cciesec
R2
Interface E 0/0 ip Ospf authentication message-digest ip Ospf message-digeset-key 1 md5 cciesec

Lab 5 – Running EIGRP



Lab Scenario:

- Configure EIGRP on the Firewall.
- Configure MD5 authentication for EIGRP.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure EIGRP on the inside interface of the Firewall in AS 100 to exchange routes with R1. Disable Auto-summarization. Advertise the R1 Loopbacks in EIGRP.

FW

```
Router EIGRP 100
 No auto-summary
 Network 10.11.11.0 255.255.255.0
```

R1

```
Router EIGRP 100
 No auto-summary
 Network 10.0.0.0
 Network 100.0.0.0
```

Task 2

Configure the Firewall and R2 with EIGRP authentication using a Key **1** and password of **cciesec**.

FW

```
Interface G 0/1
 authentication mode eigrp 100 md5
 authentication key eigrp 100 cciesec key-id 1
```

R1

```
Key chain AUTH
 Key 1
   Key-string cciesec
!
Int E 0/0
 Ip authentication mode eigrp 100 md5
 Ip authentication key-chain eigrp 100 AUTH
```

Task 3

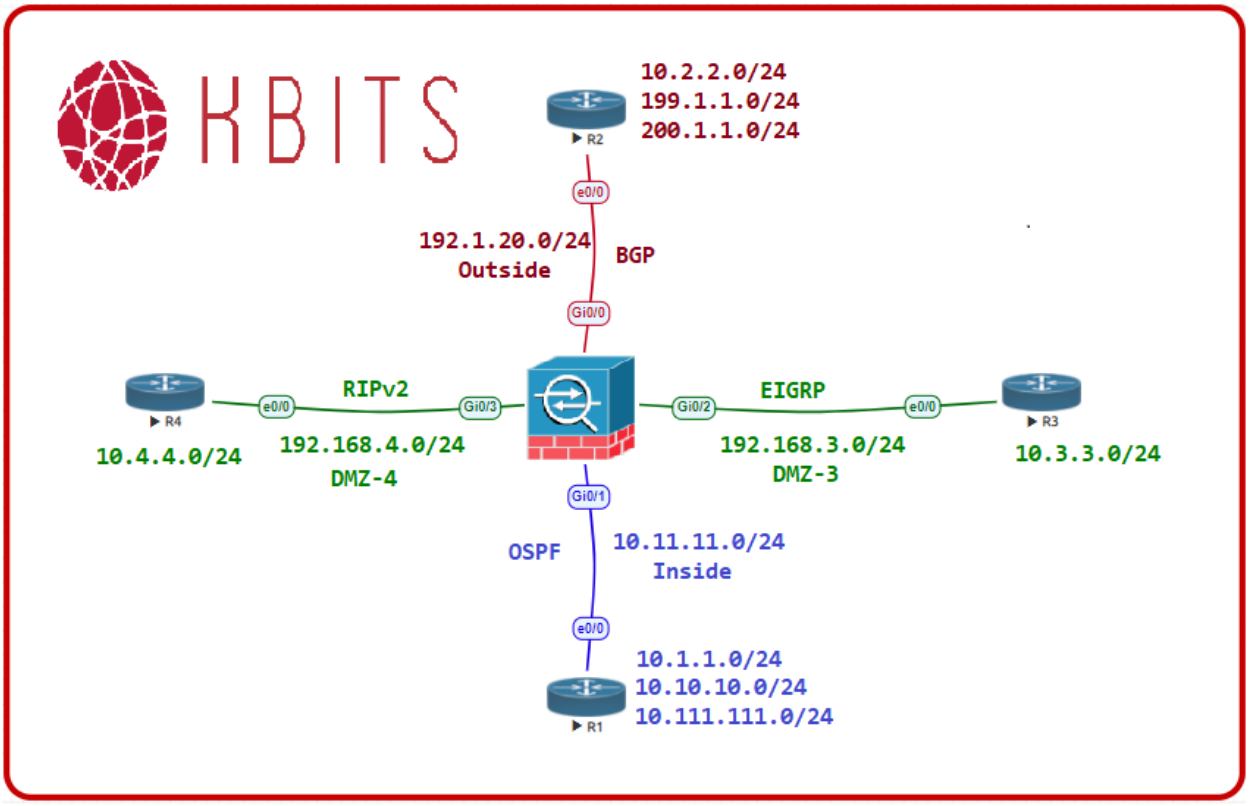
Perform Route Redistribution such that all devices have a complete picture of the entire topology.

FW

```
Router OSPF 1
```

```
 Redistribute Rip subnets
 Redistribute EIGRP 100 subnets
!
Router RIP
 Redistribute ospf 1 metric 1
 Redistribute EIGRP 100 metric 1
!
Router EIGRP 100
 Redistribute ospf 1 metric 1 1 1 1 1
 Redistribute RIP metric 1 1 1 1 1
```

Lab 6 – Configuring Management Protocols



Lab Scenario:

- Configure the Firewall for Remote Management using Telnet and SSH.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure the Firewall for Telnet Management from the Inside interface. The ASA should allow the 10.11.11.0/24 and the 10.1.1.0/24 networks to access it for management.

FW

```
telnet 10.11.11.0 255.255.255.0 inside
telnet 10.1.1.0 255.255.255.0 inside
```

Task 2

Configure the Telnet password as **cciesec** on the Firewall.

FW

```
Passwd cciesec
```

Task 3

Enable SSH on the ASA. Allow R2 to connect to the ASA for Management from the outside interface using SSH Version 2. The idle timeout for SSH connections should be 2 minutes.

FW

```
Domain-name ABC.in
Crypto key generate rsa
!
Ssh version 2
Ssh timeout 2
Ssh 192.1.20.2 255.255.255.255 outside
```

Task 4

Create a username of **ROUTER2** with a password of **cciesec**. Have the ASA authenticate against the Local Username database for ssh connections.

FW

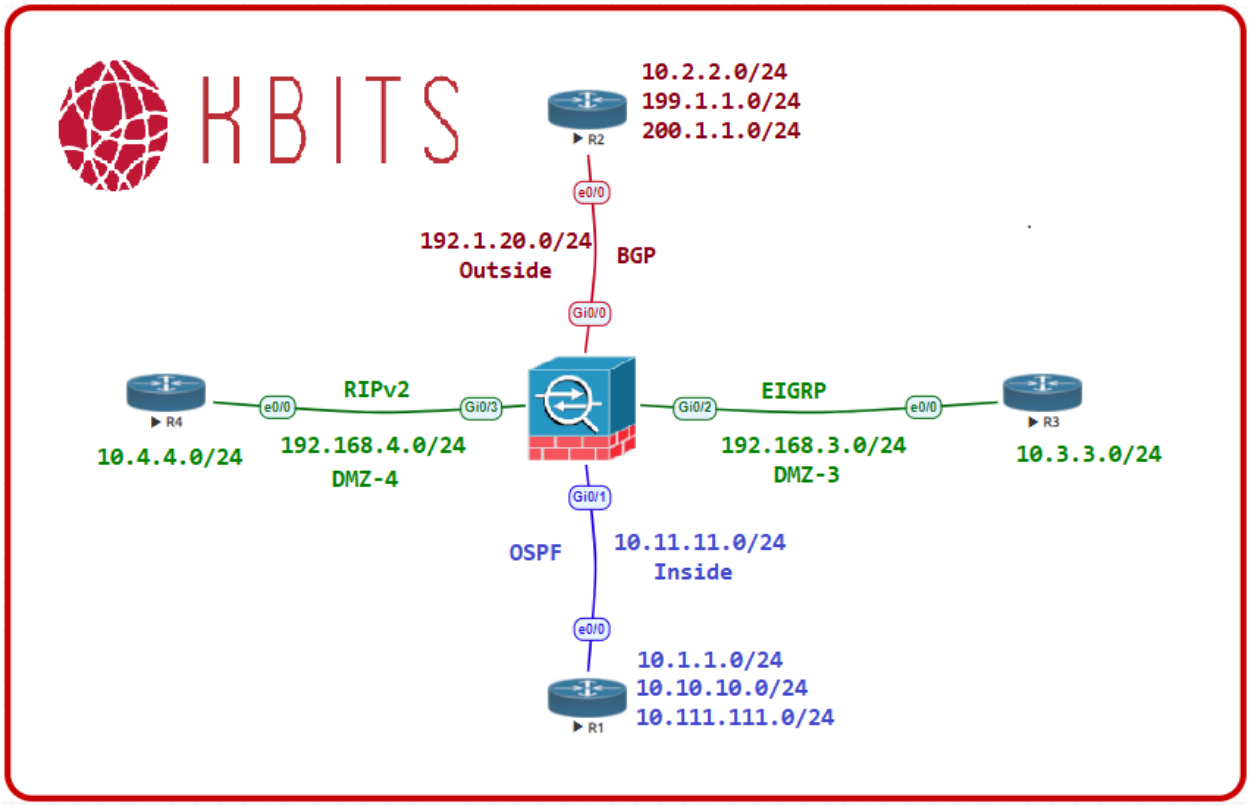
```
Username ROUTER2 password cciesec
!
Aaa  authentication ssh console LOCAL
```

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 2:
NAT & ACLs on 9.X

Module 2 – NAT & ACLs on 9.X

Lab 1 – Configuring Basic NAT Operations



Lab Scenario:

- Configure Object Dynamic NAT on a Firewall
- Configure Object Dynamic PAT on a Firewall

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

The Firewall should translate all traffic going from the DMZ-3 towards the outside using 192.1.20.8 as the Public Address.

FW

```
object network NET-192.168.3.0
 subnet 192.168.3.0 255.255.255.0
 nat (DMZ-3,outside) dynamic 192.1.20.8
```

Task 2

The Firewall should translate all traffic going from 10.11.11.0/24 towards the outside using a pool of 192.1.20.151 – 192.1.20.200.

FW

```
object network POOL-10.11.11.0
 range 192.1.20.151 192.1.20.200
!
object network NET-10.11.11.0
 subnet 10.11.11.0 255.255.255.0
 nat (inside,outside ) dynamic POOL-10.11.11.0
```

Task 3

The Firewall should translate all traffic going from this 10.1.1.0/24 towards outside using a pool of 192.1.20.131-192.1.20.149. Back this pool up by using a PAT address of 192.1.20.150.

FW

```
object network POOL-10.1.1.0
 range 192.1.20.131 192.1.20.149
!
object network POOL-P-10.1.1.0
 host 192.1.20.150
!
object-group network NAT-PAT-10.1.1.0
 network-object object POOL-10.1.1.0
 network-object object POOL-P-10.1.1.0
!
object network NET-10.1.1.0
 subnet 10.1.1.0 255.255.255.0
 nat (inside,outside) dynamic NAT-PAT-10.1.1.0
```

Task 4

The Firewall should translate all traffic going from this 10.111.111.0/24 towards outside using Outside Interface.

FW

```
object network INS-NET
 subnet 10.111.111.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

Lab 2 – Configuring Static NAT, Static Identity NAT & Static PAT

Lab Scenario:

- Configure Object Static NAT on a Firewall
- Configure Object Static Identity NAT on a Firewall to override translation
- Configure Object Static PAT

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Statically translate R1 such that it is seen as itself on the outside. It should not get translated.

FW

```
object network R1
 host 10.11.11.1
 nat (inside,outside) static 10.11.11.1
```

Task 2

Statically translate R3 as 192.1.20.3 on the outside. Also, translate an ISE located at 10.11.11.25 as 192.1.20.25 on the outside.

FW

```
object network R3
 host 192.168.3.3
 nat (DMZ-3,outside) static 192.1.20.3
!
object network ISE
 host 10.11.11.25
 nat (Inside,outside) static 192.1.20.25
```

Task 3

Configure Static PAT on the Firewall such that if a request comes from the outside destined for an IP Address 192.1.20.7 with a port number 25, the firewall should forward the request to a SMTP server located at 192.168.3.11. If a request comes into the Firewall destined for an IP Address 192.1.20.7 with a port number 23, the Firewall should forward the request to a Device located at 192.168.3.12 for 23.

FW

```
object network S1-MAIL
 host 192.168.3.11
 nat (DMZ-3,Outside) static 192.1.20.7 service tcp 25 25
!
object network S2-TELNET
 host 192.168.3.12
 nat (DMZ-3,Outside) static 192.1.20.7 service tcp 23 23
```

Lab 3 – Configuring Destination NAT

Lab Scenario:

- Configure Object Static Destination NAT

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

There is a Mainframe located on the DMZ at 192.168.3.99. Another Mainframe (200.1.1.10) from the outside needs to access it; The local Mainframe should be seen as 192.1.20.29 on the outside. The local Mainframe does not have the ability to point to a default gateway. Allow the Public Mainframe to access the local Mainframe as a local device located at 192.168.3.98.

FW

```
object network MF-LOCAL
 host 192.168.3.99
 nat (DMZ-3,outside) static 192.1.20.29
!
object network MF-REMOTE
 host 200.1.1.10
 nat (outside,DMZ-3) static 192.168.3.98
```

Lab 4 – Configuring Twice-NAT / Manual NAT

Lab Scenario:

- Configure Twice-NAT Policy NAT

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure the ASA such that when a PC 10.1.1.1 communicates with 199.1.1.1, it is seen as 192.1.20.21 and when it communicates with 200.1.1.1, it is seen as 192.1.20.22.

FW

```
object network R1
 host 10.1.1.1
!
object network H-199
 host 199.1.1.1
!
object network H-200
 host 200.1.1.1
!
object network X1
 host 192.1.20.21
!
object network X2
 host 192.1.20.22
!
nat (ins,out) source static R1 H-199 destination static X1 H-199
nat (ins,out) source static R1 H-200 destination static X2 H-200
```

Lab 5 – Access Control

Lab Scenario:

- Allow traffic for the Translations that were configured in the previous lab.
- Configure the ICMP command to restrict pinging on the Firewall interfaces.
- Configure Object Groups for more efficient ACL Management.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Allow traffic in for R3's translated address 192.1.20.3. You should only allow traffic for Telnet, SSH and HTTP. Also allow traffic for the ACS server which was translated to 192.1.20.25 in for HTTP, TACACS+, and the RADIUS ports.

FW

```
Access-list INF permit tcp any host 192.168.3.3 eq 23
Access-list INF permit tcp any host 192.168.3.3 eq 22
Access-list INF permit tcp any host 192.168.3.3 eq 80
Access-list INF permit tcp any host 10.11.11.25 eq 80
Access-list INF permit tcp any host 10.11.11.25 eq 49
Access-list INF permit udp any host 10.11.11.25 eq 1645
Access-list INF permit udp any host 10.11.11.25 eq 1646
Access-list INF permit udp any host 10.11.11.25 eq 1812
Access-list INF permit udp any host 10.11.11.25 eq 1813
!
Access-group INF in interface outside
```

Task 2

Allow traffic destined to an IP Address 192.1.20.7 (already translated) for ports SMTP and Telnet to come in.

FW

```
Access-list INF permit tcp any host 192.168.3.11 eq 25
Access-list INF permit tcp any host 192.168.3.12 eq 23
```

Task 3

Configure the Firewall such that only R2 Loopback 0 should be able to ping R1 E 0/0.

FW

```
Access-list INF permit icmp host 2.2.2.2 host 10.11.11.1 echo
```

Task 4

Configure the Firewall such that it should be able to ping outside but nobody should be able to ping the ASA outside interface.

FW

```
Icmp permit any echo-reply outside
```

Task 5

DMZ-4 contains the following Application Servers and Applications:

Real IP Address	Translated Address	Applications
192.168.4.201	192.1.20.201	HTTP, HTTPS, FTP
192.168.4.202	192.1.20.202	HTTP, HTTPS, FTP
192.168.4.203	192.1.20.203	HTTP, HTTPS, FTP
192.168.4.204	192.1.20.204	SMTP
192.168.4.205	192.1.20.205	SMTP
192.168.4.206	192.1.20.206	DNS, TFTP
192.168.4.207	192.1.20.207	DNS, TFTP

Task 6

Create static one-on-one translations based on the above table.

FW

```
object network S-201
 host 192.168.4.201
 nat (DMZ-4,outside) static 192.1.20.201
!
object network S-202
 host 192.168.4.202
 nat (DMZ-4,outside) static 192.1.20.202
!
object network S-203
```

```
 host 192.168.4.203
 nat (DMZ-4,outside) static 192.1.20.203
!
object network S-204
 host 192.168.4.204
 nat (DMZ-4,outside) static 192.1.20.204
!
object network S-205
 host 192.168.4.205
 nat (DMZ-4,outside) static 192.1.20.205
!
object network S-206
 host 192.168.4.206
 nat (DMZ-4,outside) static 192.1.20.206
!
object network S-207
 host 192.168.4.207
 nat (DMZ-4,outside) static 192.1.20.207
```

Task 7

Allow access to the Application Servers from the following networks:

- 101.1.1.0/24
- 150.1.5.0/24
- 175.4.1.0/24
- 199.1.33.0/24
- 215.5.7.0/24

Use the minimum number of lines possible to accomplish access to these application servers.

FW

```
Object-group network PN
 Network-object 101.1.1.0 255.255.255.0
 Network-object 150.1.5.0 255.255.255.0
 Network-object 175.4.1.0 255.255.255.0
 Network-object 199.1.33.0 255.255.255.0
 Network-object 215.5.7.0 255.255.255.0
!
Object-group network WEB-FTP-N
 Network-object host 192.168.4.201
 Network-object host 192.168.4.202
 Network-object host 192.168.4.203
!
```

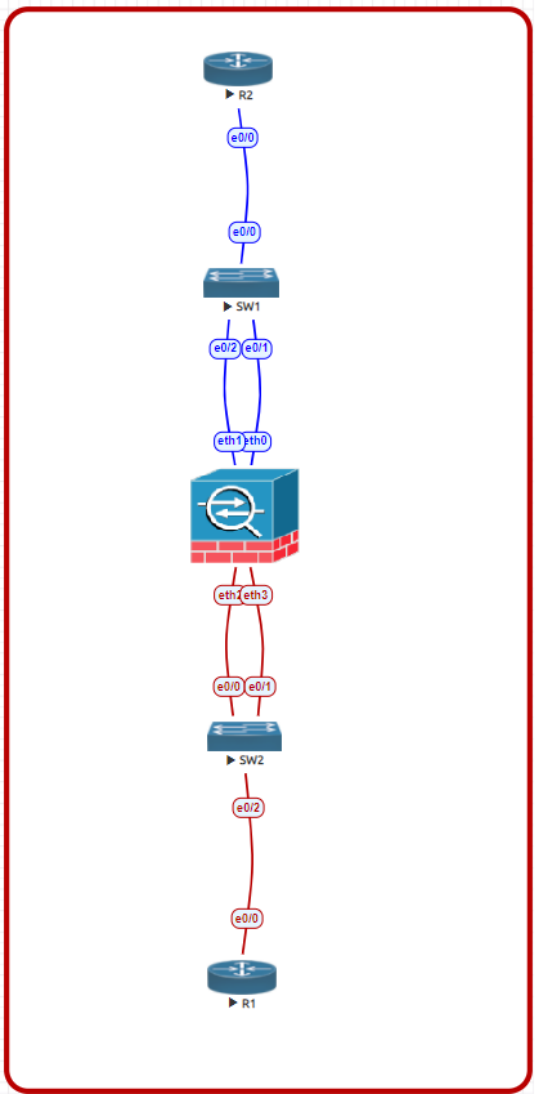
```
Object-group network SMTP-N
 Network-object host 192.168.4.204
 Network-object host 192.168.4.205
!
Object-group network DNS-TFTP-N
 Network-object host 192.168.4.206
 Network-object host 192.168.4.207
!
Object-group service WEB-FTP-P tcp
 Port-object eq 80
 Port-object eq 443
 Port-object eq 21
!
Object-group service DNS-TFTP-P udp
 Port-object eq 69
 Port-object eq 53
!
access-list INF permit tcp object-group PN object-group WEB-FTP-N object-group WEB-FTP-P
access-list INF permit udp object-group PN object-group DNS-TFTP-N object-group DNS-TFTP-P
access-list INF permit tcp object-group PN object-group SMTP-N eq SMTP
```

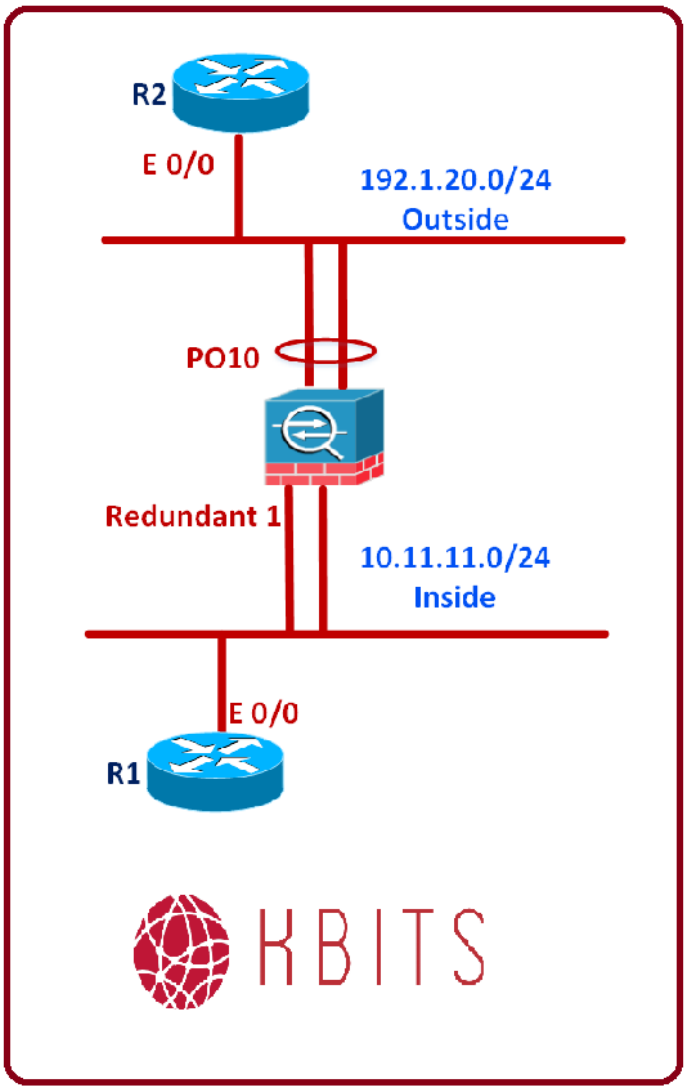
CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 3:
Configuring High Availability Features

Module 3 – Configuring High Availability Features

Lab 1 – Interface Redundancy





Lab Scenario:

- Configure a Redundant Interface on the Firewall to provide Interface Level Redundancy.

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.
- Configure Default Routes on R1 & R2 pointing towards the FW.

R1	**R2**
Int E 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10	Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.10

Lab Tasks:

Task 1

Configure the E2 and E3 as part of Redundant Interface 1 in that order. Assign it a virtual mac-address of your choice.

ASA

```
Interface E2
 No shut
!
Interface E3
 No shut
!
Interface Redundant 1
 Member-interface E2
 Member-interface E3
 Mac-address 0001.AB01.1101
```

Task 2

Configure ASA with the following IP configuration for Redundant Interface:

Interface	**Name**	**Security Level**	**IP Address**
Redundant 1	Inside	100	10.11.11.10/24

ASA

```
Interface Redundant 1
 Nameif inside
```

```
Ip address 10.11.11.10 255.255.255.0
Security-level 100
No shut
```

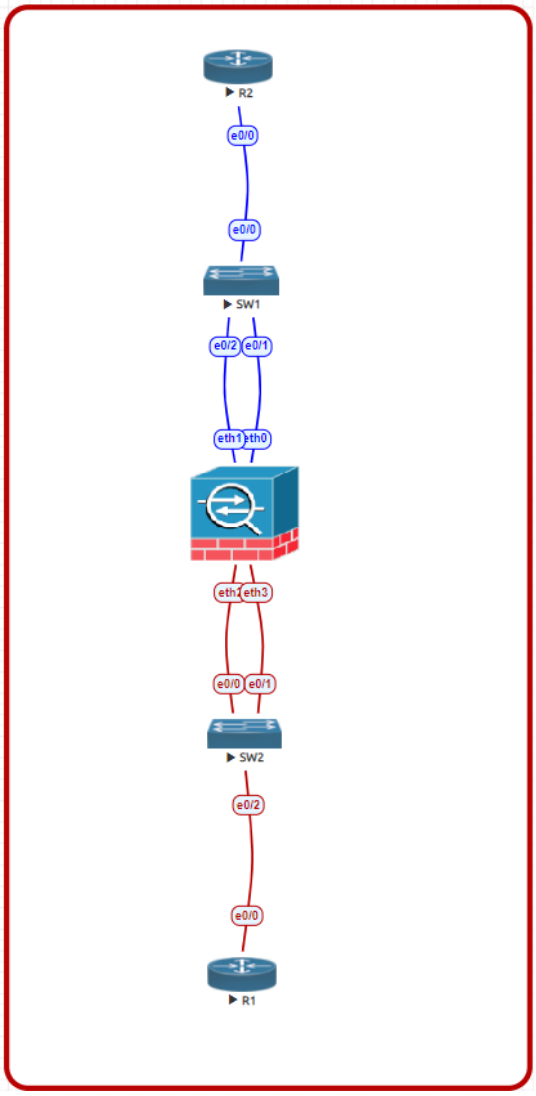
Task 3

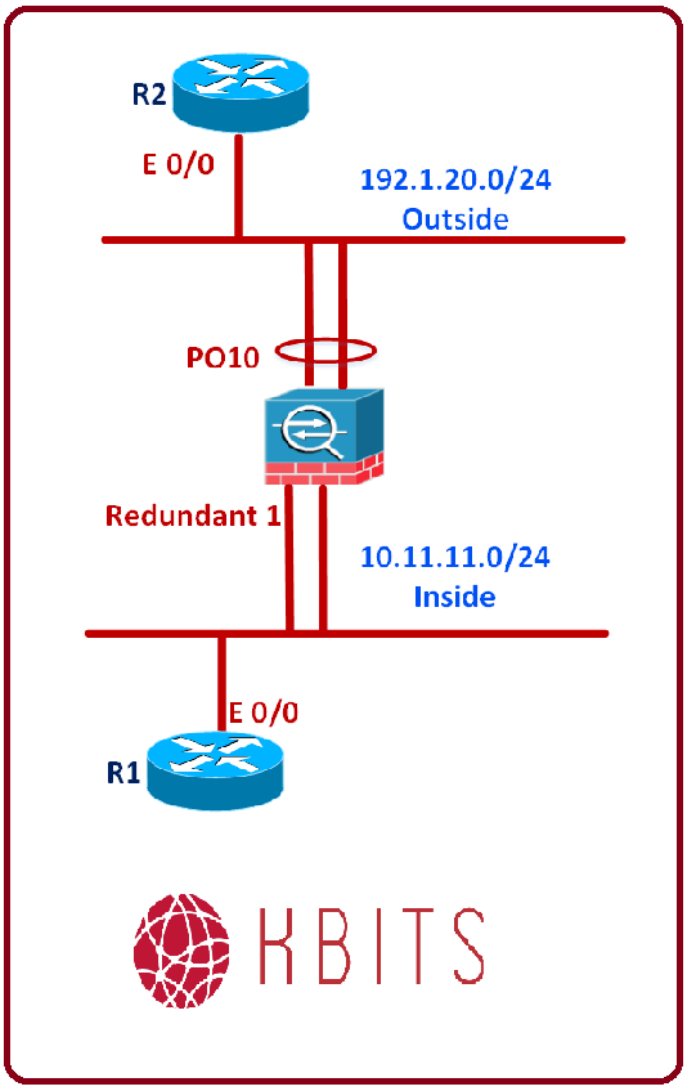
Configure the Outside Switch to Assign the ASA E0/0 & E0/1 ports to VLAN 20.

SW2

```
vlan 10
!
interface range E 0/0-2
 switchport mode access
 switchport access vlan 10
```

Lab 2 – Port Channels





Lab Scenario:

- Configure Port-Channels between the Outside Switch and the ASA Outside ports.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure a Port Channel on the Outside Switch towards the ASA Firewall using LACP. Assign the Port-Channel to VLAN 20. Also, assign the port connecting towards R2 to VLAN 20.

SW1

```
vlan 20
!
interface E 0/0
 switchport mode access
 switchport access vlan 20
!
interface range E 0/1-2
 channel-group 10 mode active
 no shut
!
interface port-channel 10
 switchport mode access
 switchport access vlan 20
```

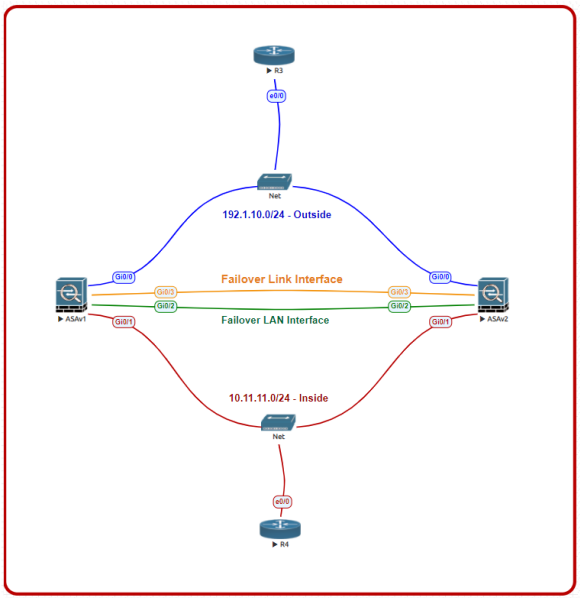
Task 2

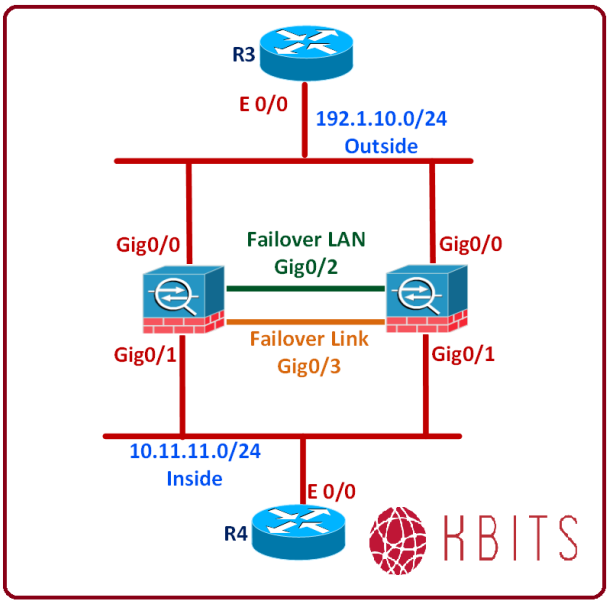
Configure a Port Channel on the ASA Firewall for E0 & E1.

ASA

```
Interface E0
 channel-group 5 mode active
 no shut
!
Interface E1
 channel-group 5 mode active
 no shut
!
Interface Port-channel 5
 nameif Outside
 security-level 0
 ip address 192.1.20.10 255.255.255.0
 no shut
```

Lab 3 – Active / Standby Failover





Lab Scenario:

- Configure Stateless Active/Standby Failover.

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.
- Configure Default Routes on R4 pointing towards the FW.

R4	**R3**
Int E 0/0 Ip add 10.11.11.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10	Int E 0/0 Ip add 192.1.10.3 255.255.255.0 No shut

Lab Tasks:

Task 1

FW-1 and FW-2 will be configured in a Active/Standby Failover Setup. FW-1 will be the Primary Firewall and FW-2 will be the Secondary Firewall. Use the following parameters for the Failover configurations:

- Failover LAN Interface: G 0/2
- Failover Interface Name: FC
- Failover IP Addresses Active: 10.10.10.1/24
- Failover IP Addresses Standby: 10.10.10.2/24
- Failover Key: cisco123

FW-1

```
Interface G 0/2
 No shutdown
!
Failover lan interface FC G0/2
Failover interface IP FC 10.10.10.1 255.255.255.0 standby 10.10.10.2
Failover key cisco123
Failover lan unit primary
Failover
```

FW-2

```
Interface G 0/2
 No shutdown
!
Failover lan interface FC G0/2
Failover interface IP FC 10.10.10.1 255.255.255.0 standby 10.10.10.2
Failover key cisco123
Failover lan unit secondary
Failover
```

Task 2

Configure FW-1 with the following Primary and Standby IP Addresses:

Interface	Name	Security Level	System IP	Standby IP
G 0/0	Outside	0	192.1.10.10/24	192.1.10.11/24
G 0/1	Inside	100	10.11.11.10/24	10.11.11.11/24

FW-1

```
Interface G 0/0
 Ip address 192.1.10.10 255.255.255.0 standby 192.1.10.11
```

```
 Nameif Outside
 No shut
!
Interface G 0/1
 Ip address 10.11.11.10 255.255.255.0 standby 10.11.11.11
 Nameif inside
 No shut
```

Task 3

Configure EIGRP as the routing protocol on both the Routes and the Firewall. Configure a Loopback interface 10.4.4.4/24 on R4 and 10.3.3.3/24 on R3. Advertise them under EIGRP. Use AS 123 for EIGRP.

R3

```
Interface Loopback 0
 Ip address 10.3.3.3 255.255.255.0
!
Router eigrp 123
 Network 10.0.0.0
 Network 192.1.10.0
```

R4

```
Interface Loopback 0
 Ip address 10.4.4.4 255.255.255.0
!
Router eigrp 123
 Network 10.0.0.0
```

FW-1

```
Router Eigrp 123
 Network 10.0.0.0
 Network 192.1.10.0
```

Task 4

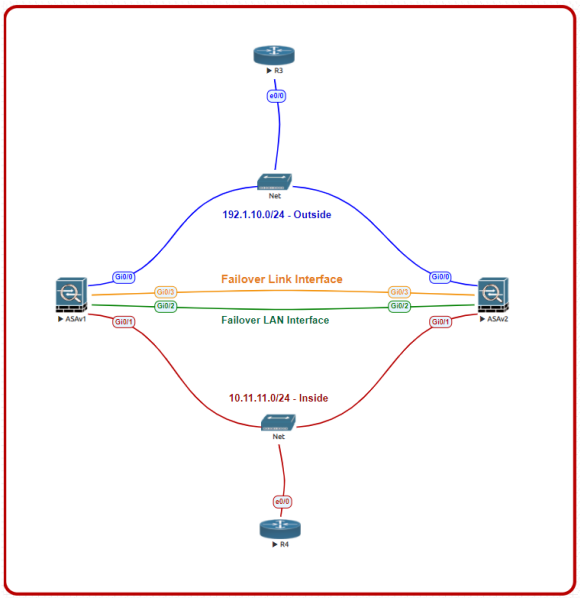
Allow the inside networks to go out using a Outside pool of 192.1.10.51 – 192.1.10.100.

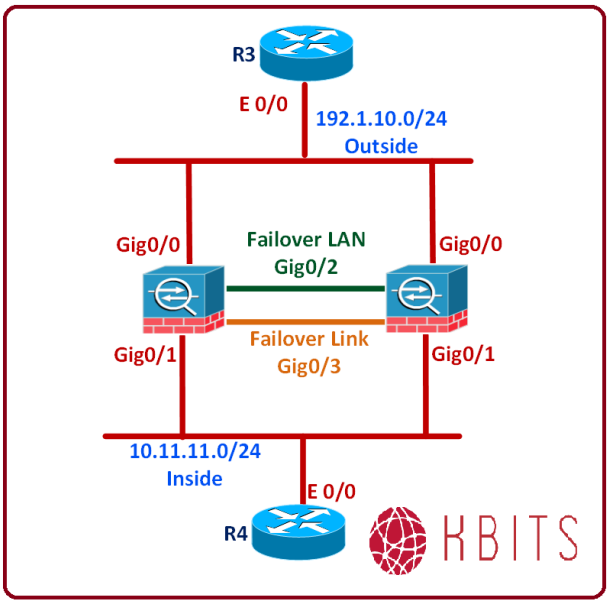
FW-1

```
Object network POOL
 Range 192.1.10.51 192.1.10.100
!
object network INS-NETS
 Subnet 0.0.0.0 0.0.0.0
```

Nat (ins,out) dynamic POOL
Note: If you do Show Run on FW-2, all the configuration should have replicated over to it. Also, do Show Failover to verify the Failover status.

Lab 4 – Stateful Failover





Lab Scenario:

- Configure Statefull Failover between FW-1 & FW-2.

Initial Setup:

- **Based on the previous Lab**

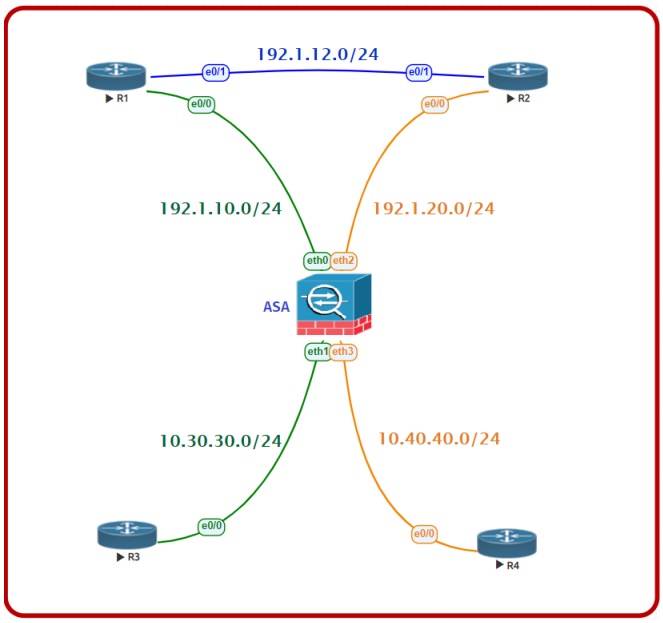
Lab Task:

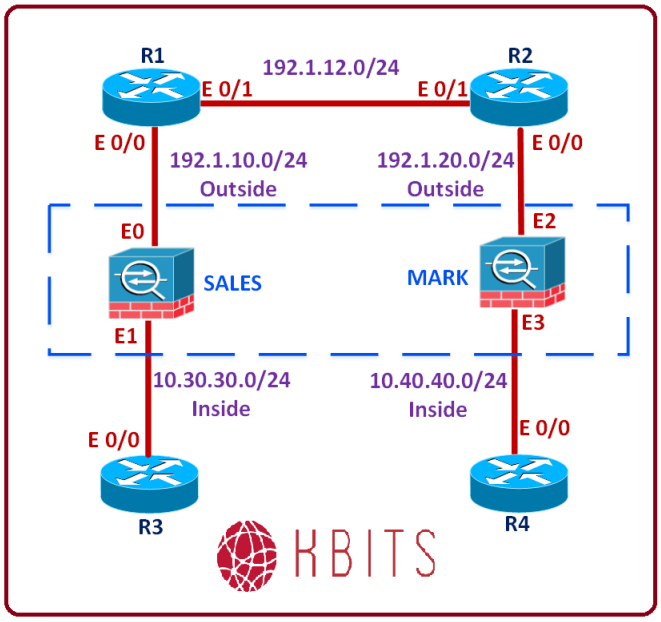
Task 1

Configure G 0/3 as the Failover link to replicate the State and connection information from the Active Firewall to the Standby firewall. Configure G 0/3 with an IP Address of 10.20.20.1/24 as the Active Address and 10.20.20.2/24 as the Standby address. Assign it a name of SFF.

FW-1
Interface G 0/3 No shut ! Failover link SFF G 0/3 Failover interface IP SFF 10.20.20.1 255.255.255.0 standby 10.20.20.2
***Note : This only needs to be done on the Active device as the configuration will be replicated to the standby box**

Lab 5 – Configuring Security Contexts on the ASA





Lab Scenario:

- Configure a FW in Multi-context mode.
- Configure Resource-based class-map to limit the resources to a particular context.

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.
- Configure Default Routes on R3 & R4 pointing towards the appropriate Firewall address.

R1	R2
Int loopback 0 Ip address 1.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Int E 0/1 Ip add 192.1.12.1 255.255.255.0 No shut ! Router eigrp 111 Network 192.1.10.0 Network 192.1.12.0	Int loopback 0 Ip address 1.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Int E 0/1 Ip add 192.1.12.2 255.255.255.0 No shut ! Router eigrp 111 Network 192.1.20.0 Network 192.1.12.0
R3	**R4**
Int E 0/0 Ip address 10.30.30.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.30.30.11	Int E 0/0 Ip address 10.40.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.40.40.21

Lab Tasks:

Task 1

Configure the ASA for Multiple Contexts.

ASA
Mode multiple Note: It will reboot into the System Context.

Task 2

Bring up the interfaces E0, E1, E2 & E3

ASA
Interface E0 no shut !

```
Interface E1
 no shut
!
Interface E2
 no shut
!
Interface E3
 no shut
```

Task 3

Configure two contexts on the ASA. Name them as SALES and MARK. Configure them with configuration files SALES.cfg and MARK.cfg respectively on Flash. Allocate the appropriate interface to the appropriate contexts based on the Network Diagram. (**Note:** Delete any existing .cfg files in flash before creating the context)

FW-1

```
Context SALES
 allocate-interface E0
 allocate-interface E1
 config-url flash:SALES.cfg
!
Context MARK
 allocate-interface E2 OUT
 allocate-interface E3 INS
 config-url flash:MARK.cfg
```

Task 4

Configure the SALES Context Interfaces based on the following table. Configure a default route towards R1:

Interface	Name	Security Level	IP Address
E0	Outside	0	192.1.10.11/24
E 1	Inside	100	10.30.30.11/24

SALES

```
changeto context SALES
!
Interface E0
 Nameif outside
 Ip address 192.1.10.11 255.255.255.0
!
Interface E1
```

```
 Nameif Inside
 Ip address 10.30.30.11 255.255.255.0
!
Route outside 0 0 192.1.10.1
```

Task 5

Configure the MARK Context Interfaces based on the following table. Configure a default route towards R2:

Interface	Name	Security Level	IP Address
E0	Outside	0	192.1.10.11/24
E 1	Inside	100	10.30.30.11/24

MARK

```
changeto context MARK
!
Interface OUT
 nameif Outside
 ip address 192.1.20.21 255.255.255.0
!
Interface INS
 nameif Inside
 ip address 10.40.40.21 255.255.255.0
!
route outside 0 0 192.1.20.2
```

Task 6

Configure SALES to allow the inside network access to the outside networks using Dynamic Translation. Use a pool of 192.1.10.51 – 192.1.10.100. R2 should be seen as 192.1.100.2 on the outside network.

SALES

```
object network POOL-A
 range 192.1.10.51 192.1.10.100
!
object network INS-NET
 subnet 10.30.30.0 255.255.255.0
 nat (inside,outside) dynamic POOL-A
```

Task 7

Configure MARK to allow the inside network access to the outside networks using Dynamic Translation. Use a pool of 192.1.20.51 – 192.1.20.100. R4 should be seen as 192.1.20.4 on the outside network.

MARK

```
object network POOL-A
 range 192.1.20.51 192.1.20.100
!
object network INS-NET
 subnet 10.30.30.0 255.255.255.0
 nat (inside,outside) dynamic POOL-A
!
object network R4
 host 10.40.40.4
 nat (inside,outside) static 192.1.20.4
```

Task 8

Allow Telnet & ICMP Access to R4.

ASA

Changeto context MARK

```
Access-list INF permit tcp any host 10.40.40.4 eq 23
Access-list INF permit icmp any host 10.40.40.4
!
Access-group INF in interface outside
```

Task 9

Configure resource allocation for MARK based on the following:

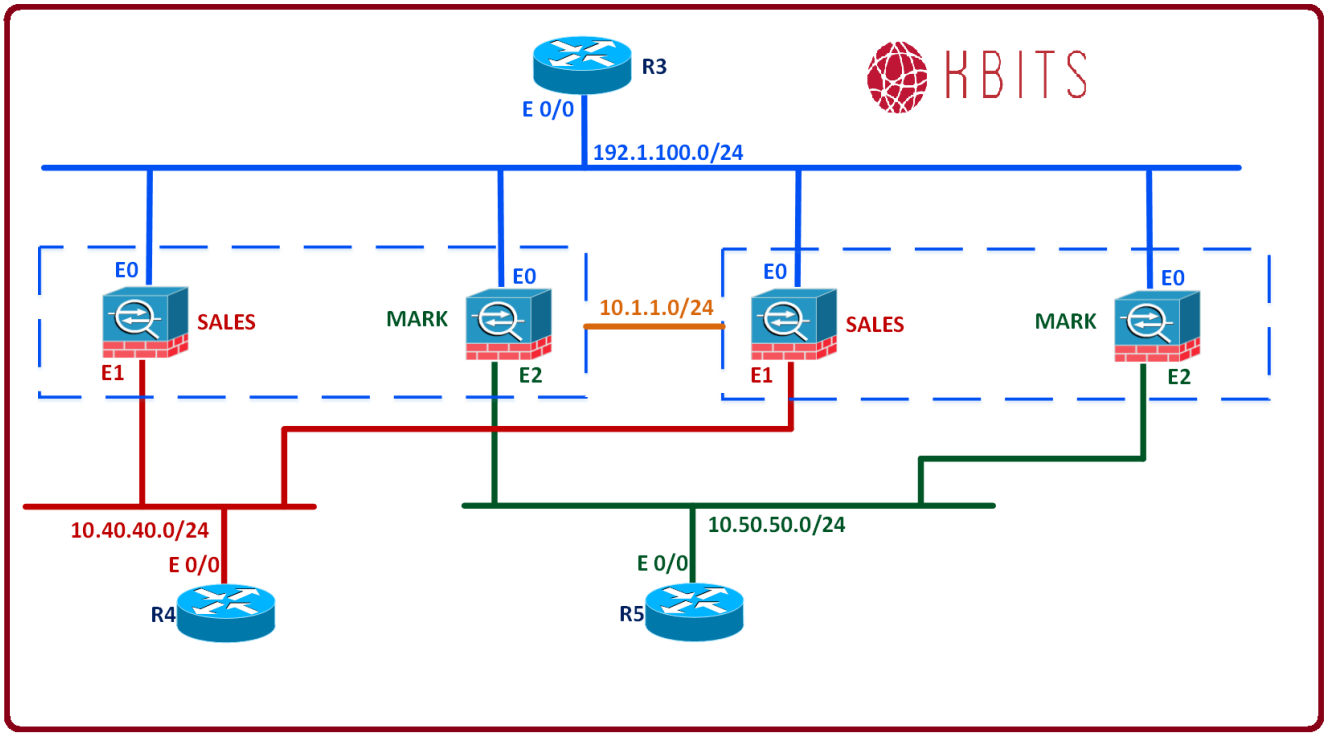
- Maximum Connections: 100
- Maximum Telnet & ASDM Connections each: 3
- Maximum Xlate entries: 100

FW-1

Changeto system

```
class CM-MARK
  limit-resource Conns 100
  limit-resource Telnet 3
  limit-resource ASDM 3
  limit-resource Xlates 100
!
context MARK
  member CM-MARK
```

Lab 6 – Active/Active Failover



Lab Scenario:

- Configure Active/Active Failover with SALES Active on ASA1 & MARK active on ASA2.

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.
- Configure Default Routes on R4 & R5 pointing towards the appropriate Firewall address.

R3	**R4**
Int loopback 0 Ip address 3.3.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.1.100.3 255.255.255.0 No shut	Int E 0/0 Ip add 10.40.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.40.40.11
R5 Int E 0/0 Ip add 10.50.50.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.50.50.21	

Lab Task:

Task 1

Configure Multi-Mode on both ASA firewalls

ASA-1 Mode multiple Note: The Firewall will reboot into the System Context
ASA-2 Mode multiple Note: The Firewall will reboot into the System Context

Task 2

Bring up all the Interfaces on ASA1. We will configure ASA2 later.

ASA-1 interface e0 no shut !

```
interface e1
 no shut
!
interface e2
 no shut
!
interface e3
 no shut
```

Task 3

Configure two contexts on the ASA-1. Name them as SALES and MARK. Configure them with configuration files SALES.cfg and MARK.cfg respectively on Flash. Allocate the appropriate interface to the appropriate contexts based on the Network Diagram. (**Note:** Delete any existing .cfg files in flash before creating the context)

ASA-1

```
context SALES
 allocate-interface E0
 allocate-interface E1
 config-url flash:SALES.cfg
!
context MARK
 allocate-interface E0
 allocate-interface E2
 config-url flash:MARK.cfg
```

Task 4

Configure the SALES Context Interfaces based on the following table. Configure a default route pointing towards R3. Configure the Inside network to go out using a pool of 192.1.100.51-192.1.100.100:

Interface	Name	Security Level	System IP	Standby IP
E0 (Shared)	Outside	0	192.1.100.11/24	192.1.100.12/24
E1	Inside	100	10.40.40.11/24	10.40.40.12/24

ASA-1

Changeto context SALES

```
Interface E0
 nameif Outside
 ip address 192.1.100.11 255.255.255.0 standby 192.1.100.12
!
```

```
Interface E1
 nameif Inside
 ip address 10.40.40.11 255.255.255.0 standby 10.40.40.12
!
route outside 0 0 192.1.100.3
!
object network POOL-A
 range 192.1.100.51 192.1.100.100
!
object network INS-NET
 subnet 10.40.40.0 255.255.255.0
 nat (Inside,outside) dynamic POOL-A
```

Task 5

Configure the MARK Context Interfaces based on the following table. Configure a default route pointing towards R3. Configure the Inside network to go out using a pool of 192.1.100.101-192.1.100.150:

Interface	Name	Security Level	System IP	Standby IP
E0 (Shared)	Outside	0	192.1.100.21/24	192.1.100.22/24
E2	Inside	100	10.50.50.21/24	10.50.50.22/24

ASA-1

Changeto context MARK

```
Interface E0
 nameif Outside
 ip address 192.1.100.21 255.255.255.0 standby 192.1.100.22
!
Interface E2
 nameif Inside
 ip address 10.50.50.21 255.255.255.0 standby 10.50.50.22
!
route outside 0 0 192.1.100.3
!
object network POOL-A
 range 192.1.100.101 192.1.100.150
!
object network INS-NET
 subnet 10.50.50.0 255.255.255.0
 nat (Inside,outside) dynamic POOL-A
```

Task 6

Configure and enable ASA1 for Failover using the following:

- Failover Interface: E3
- Failover Interface Name: FC
- Failover Role: Primary
- Active IP: 10.10.10.1/24
- Standby IP: 10.10.10.2
- Failover Key: Cisco123
- Stateful Link: E3
- Failover Group 1: Active on Primary with Preempt
- Failover Group 2: Active on Secondary with Preempt
- SALES Context: Member of Group 1
- MARK Context: Member of Group 2

ASA-1

Changeto system

```
Interface E3
 no shut
!
failover lan interface FC E3
failover interface ip FC 10.10.10.1 255.255.255.0 standby 10.10.10.2
failover lan unit primary
failover key Cisco123
!
failover link FC E3
!
failover group 1
 primary
 preempt
!
failover group 2
 secondary
 preempt
!
context SALES
 join-failover-group 1
!
context MARK
 join-failover-group 2
!
failover
```

Task 7

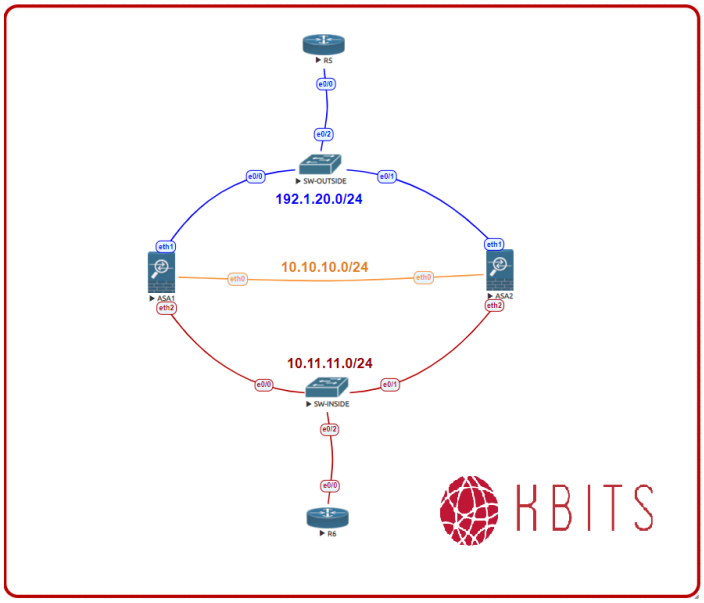
Configure and enable ASA2 for Failover using the following:

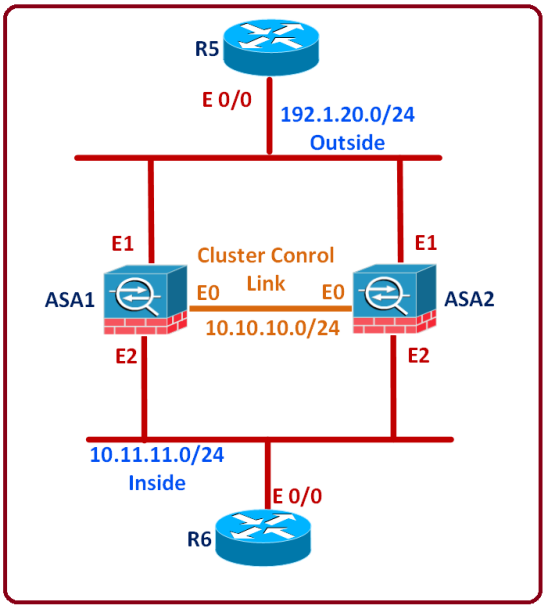
- Failover Interface: E3
- Failover Interface Name: FC
- Failover Role: Secondary
- Active IP: 10.10.10.1/24
- Standby IP: 10.10.10.2
- Failover Key: Cisco123

ASA-2

```
Interface E3
 no shut
!
failover lan interface FC E3
failover interface ip FC 10.10.10.1 255.255.255.0 standby 10.10.10.2
failover lan unit secondary
failover key cisco123
failover
```

Lab 7 – Clustering – Individual Interface Mode





Lab Scenario:

- Configure a Firewall Cluster using Physical Interfaces.

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.

R5	**R6**
Int E 0/0 Ip add 192.1.20.5 255.255.255.0 No shut	Int E 0/0 Ip add 10.11.11.6 255.255.255.0 No shut

Lab Tasks:

Task 1

ASA-1 and ASA-2 will be configured in a Cluster. ASA-1 will be the Master Firewall and ASA-2 will be the Slave Firewall. Use the following parameters for the Failover configurations:

- Cluster Interface Mode: Individual
- Cluster Group Name: CCIEv6
- Failover LAN Interface: E0
- Failover IP Addresses Master: 10.10.10.1/24
- Failover IP Addresses Slave: 10.10.10.2/24
- Failover Key: cisco123

ASA-1

```
Cluster Interface-mode Individual force
!
Interface E0
 No shutdown
!
Cluster group CCIEv6
 local-unit PRI
 cluster-interface E0 ip 10.10.10.1 255.255.255.0
 priority 1
 key cisco123
 enable noconfirm
```

ASA-2

```
Cluster Interface-mode Individual force
!
Interface E0
 No shutdown
!
Cluster group CCIEv6
 local-unit SEC
 cluster-interface E0 ip 10.10.10.2 255.255.255.0
 priority 10
 key cisco123
 enable noconfirm
```

Note: Type show cluster info to see the Status of the devices in the cluster.

Task 2

Configure Switch ports connecting towards the E1 Interfaces of the 2 ASA's and R5 in VLAN 20. Configure Switch ports connecting towards the E2 Interfaces of the 2 ASA's and R6 in VLAN 10.

SW-Outside

```
vlan 20
!
Interface range E 0/0-2
switchport mode access
 switchport access vlan 20
```

SW-Inside

```
vlan 10
!
Interface range E 0/0-2
switchport mode access
 switchport access vlan 10
```

Task 3

Configure FW-1 Interfaces based on the following table:

Interface	Name	Security Level	Master IP/Pool
E1	Outside	0	192.1.20.11/24 Pool: 192.1.20.12-14
E2	Inside	100	10.11.11.11/24 Pool: 10.11.11.12-14

ASA-1

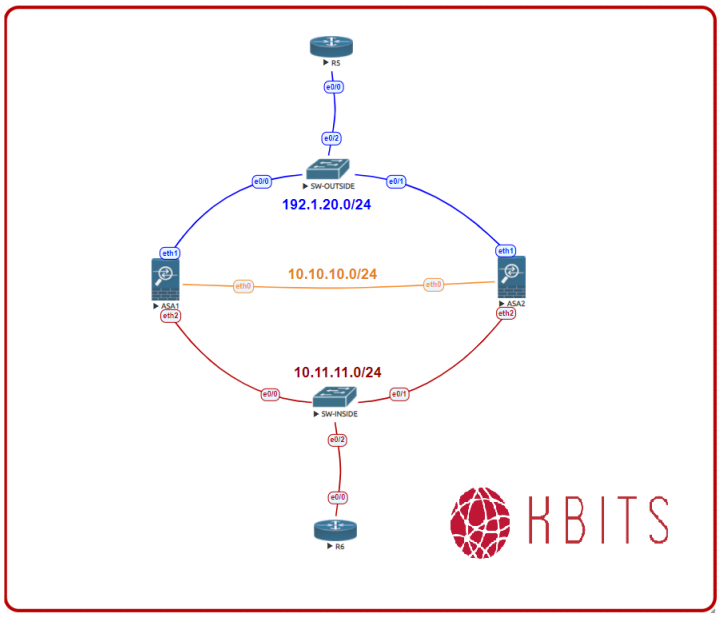
```
Ip local pool OUTSIDE 192.1.20.12-192.1.20.14
Ip local pool INSIDE 10.11.11.12-10.11.11.14
!
Interface E1
 Nameif Outside
 Ip address 192.1.20.11 255.255.255.0 cluster-pool OUTSIDE
 No shut
!
Interface E2
 Nameif Inside
 Ip address 10.11.11.11 255.255.255.0 cluster-pool INSIDE
 No shut
```

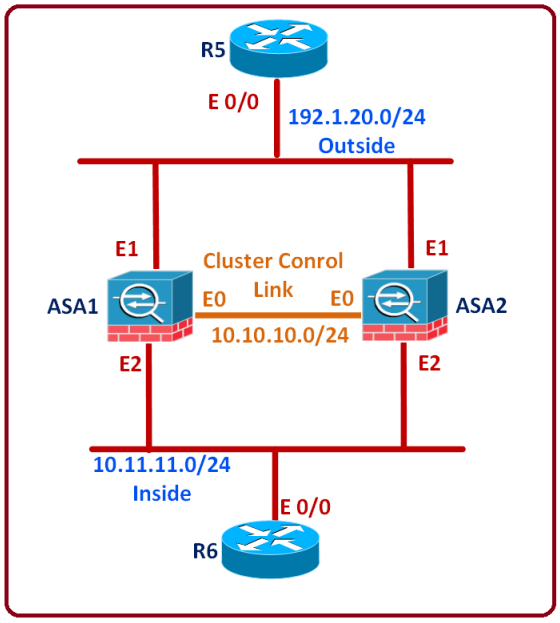
Task 4

Configure EIGRP as the routing protocol is AS 100 on both the Routers and the Firewall. Configure a Loopback interface 5.5.5.5/8 on R5 and 6.6.6.6/8 on R6. Advertise them under EIGRP.

R5
Interface Loopback 0 Ip address 5.5.5.5 255.0.0.0 ! Router EIGRP 100 Network 192.1.20.0 Network 5.0.0.0
R6
Interface Loopback 0 Ip address 6.6.6.6 255.0.0.0 ! Router EIGRP 100 Network 10.0.0.0 Network 6.0.0.0
ASA-1
Router EIGRP 100 Network 10.11.11.0 255.255.255.0 Network 192.1.20.0

Lab 9 – Clustering – Spanned Interface Mode





Lab Scenario:

- Configure a Firewall Cluster using Spanned Port-channel

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.
- Configure Default Routes on R5 & R6 pointing towards the FW.
- Configure the IP Addresses on the Routers based on the Diagram.

R5	**R6**
Int E 0/0 Ip add 192.1.20.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.11	Int E 0/0 Ip add 10.11.11.6 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.11

Lab Tasks:

Task 1

ASA-1 and ASA-2 will be configured in a Cluster. ASA-1 will be the Master Firewall and ASA-2 will be the Slave Firewall. Use the following parameters for the Failover configurations:

- Cluster Interface Mode: Spanned
- Cluster Group Name: CCIEv6
- Failover LAN Interface: E0
- Failover IP Addresses Master: 10.10.10.1/24
- Failover IP Addresses Slave: 10.10.10.2/24
- Failover Key: cisco123

ASA-1

```
cluster interface-mode spanned
!
Interface E0
 no shut
!
cluster group CCIEv6
 key cisco123
 local-unit PRI
 cluster-interface Ethernet0 ip 10.10.10.1 255.255.255.0
 priority 5
 enable
```

ASA-2

```
cluster interface-mode spanned
!
Interface E0
 no shut
!
cluster group CCIEv6
 key cisco123
 local-unit ASA1
 cluster-interface Ethernet0 ip 10.10.10.2 255.255.255.0
 priority 10
 enable
```

Note: Type show cluster info to see the Status of the devices in the cluster.

Task 2

Configure ASA-1 Ports and the correcponding switch ports in a Port-channel based on the following table:

Interface	Port-channel	Protocol	VLAN
E1	20	LACP	20
E2	10	LACP	10

ASA-1

```
Interface E1
 Channel-group 20 mode active
 No shut
!
Interface E2
Channel-group 10 mode active
 No shut
```

SW-OUTSIDE

```
vlan 20
!
Interface E 0/2
 switchport mode access
 switchport access vlan 20
!
Interface range E 0/0-1
 channel-group 20 mode active
 no shut
!
Interface port-channel 20
 switchport mode access
 switchport access vlan 20
```

SW-INSIDE

```
vlan 10
!
Interface E 0/2
 switchport mode access
 switchport access vlan 10
!
Interface range E 0/0-1
 channel-group 10 mode active
 no shut
!
Interface port-channel 10
```

```
switchport mode access
switchport access vlan 10
```

Task 3

Configure ASA-1 Port-channel Interfaces based on the following table

Interface	Name	Security Level	System IP
Port-channel 20	Outside	0	192.1.20.11/24
Port-channel 10	Inside	100	10.11.11.11/24

ASA-1

```
Interface port-channel 20
 port-channel span-cluster
 ip address 192.1.20.11 255.255.255.0
 nameif Outside
 security-level 0
 mac-address aaaa.bbbb.1111
 no shut
!
Interface port-channel 10
 port-channel span-cluster
 ip address 10.11.11.11 255.255.255.0
 nameif Inside
 security-level 100
 mac-address aaaa.bbbb.1212
 no shut
```

Task 4

Configure NAT on ASA-1 to allow the 10.11.11.0/24 network to go out using a pool of 192.1.20.51-192.1.20.200. Configure a default route on the ASA-1 towards R5.

ASA-1

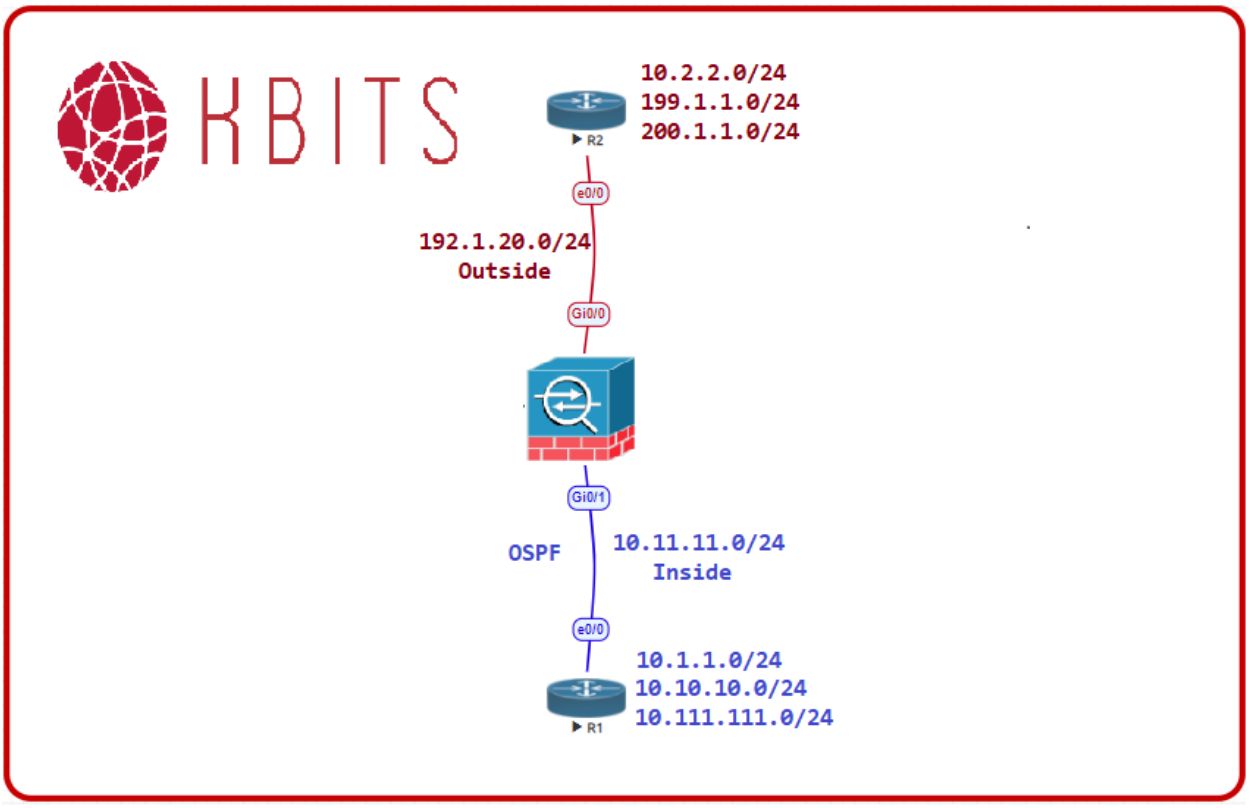
```
object network POOL-A
 range 192.1.20.51 192.1.20.200
!
object network INS-SUB
 subnet 10.11.11.0 255.255.255.0
 nat (inside,outside) dynamic POOL-A
!
route outside 0 0 192.1.20.5
```

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 4:
Deep Packet Inspection

Module 4 – Deep Packet Inspection

Lab 1 – Configuring System L7 Deep Packet Inspection



Lab Scenario:

- Configure System Based Layer 7 Inspection for FTP & EMSTP on Non-Standard Ports.
- Configure ICMP Inspection.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure the following Static Routes on the appropriate routers:
    - Default Routes on R1 pointing towards FW.
    - Default Route on the FW towards R2.

- Configure the following Loopback addresses on R1 & R2:
    - R1 : 200.1.1.1/24
    - R2 : 200.2.2.2/24

R1	**R2**
Int loopback 0 Ip add 200.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10	Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Interface Loo0 Ip address 200.2.2.2 255.255.255.0
ASA Int G 0/0 Nameif Outside Ip add 192.1.20.10 255.255.255.0 No shut ! Int G 0/1 Nameif Inside Ip add 10.11.11.10 255.255.255.0 No shut ! Route outside 0 0 192.1.20.2	

Lab Tasks:

Task 1

Configure Dynamic NAT on the Firewall to allow in the inside users to go out using a pool of 192.1.20.51-192.1.20.100.

FW

```
Object network POOL-A
  Range 192.1.20.51-192.1.20.100
!
Object network INS-NET
 Subnet 10.11.11.0 255.255.255.0
 Nat (inside,outside) dynamic pool POOL-A
```

Task 2

Configure FTP to be inspected on port 2100 in addition to port 21. Do not use any access-list for this task.

FW

```
Class CM4-FTP2100
 Match port tcp eq 2100
!
policy-map global_policy
 class CM4-FTP2100
   inspect ftp
```

Task 3

Configure SMTP to be inspected on port 2500 in addition to port 25. Do not use any access-list for this task.

FW

```
Class CM4-SMTP2500
 Match port tcp eq 2500
!
policy-map global_policy
 class CM4-SMTP2500
   inspect esmtp
```

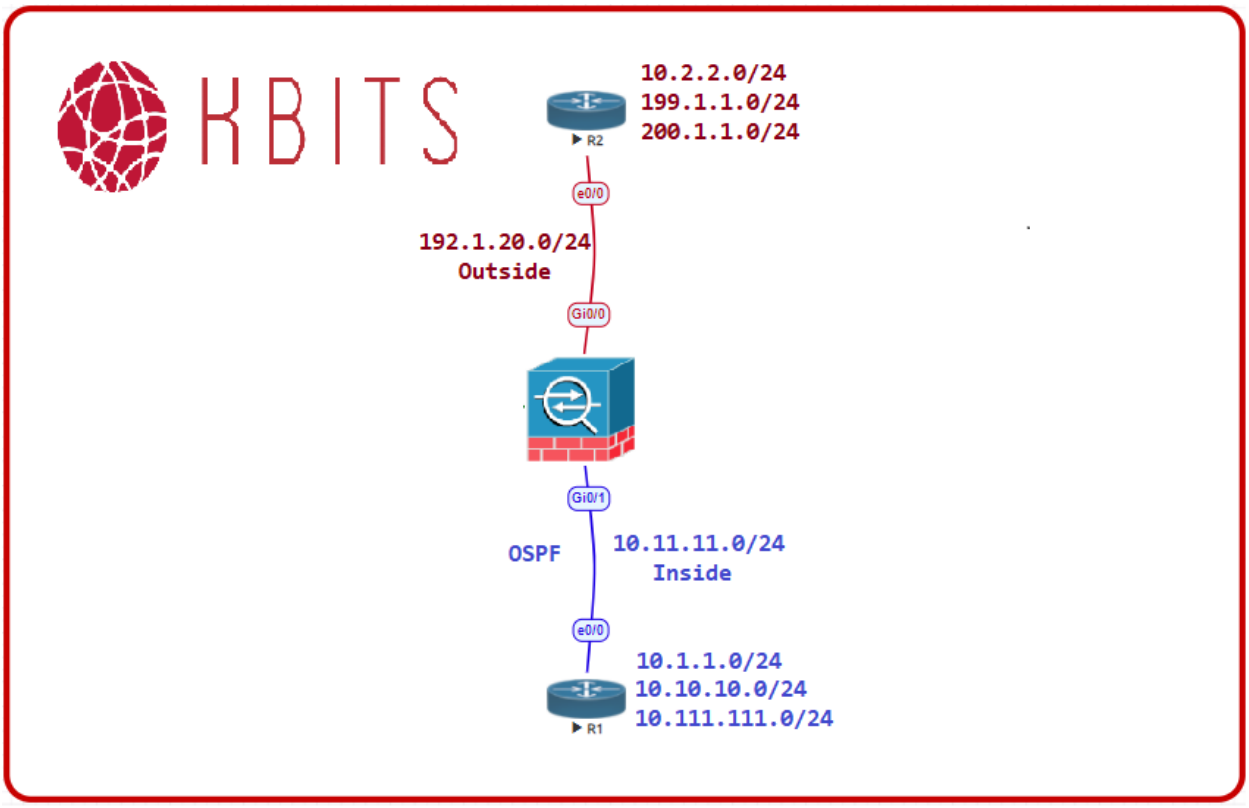
Task 4

Enable Application inspection in the Default inspection policy for the ICMP so that inside users can ping outside the firewall.

ASA

```
policy-map global_policy
 class inspection_default
   inspect icmp
```

Lab 2 – Configuring User Defined L7 Deep Packet Inspection



Lab Scenario:

- Configure User-defined L7 Deep Packet inspection for FTP.
- Configure User-defined L7 Deep Packet inspection for HTTP.
- Configure User-defined L7 Deep Packet inspection for ESMTP.
- Configure User-defined L7 Deep Packet inspection for IPSEC.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

There is a FTP Server located at 10.11.11.221. Translate this server as 192.1.20.221 on the outside. Allow FTP traffic to this Server from the outside.

FW

```
Object network FTP
 Host 10.11.11.221
 Nat (inside,outside) static 192.1.20.221
!
access-list INF permit tcp any host 10.11.11.221 eq 21
!
Access-group INF in interface outside
```

Task 2

FTP traffic connections to this server should be reset if they are trying to execute the following commands:

- Put
- Rmd
- Rnfr
- dele

FW

```
Policy-map type inspect FTP PM7-FTPCMD
  Match-request command put rmd rnfr dele
     Reset
!
access-list FTP-S permit tcp any host 10.11.11.221 eq 21
!
class-map CM4-MYFTP
 match access-list FTP-S
!
policy-map global_policy
 class CM4-MYFTP
   inspect FTP strict PM7-FTPCMD
```

Task 3

There is a HTTP Server located at 10.11.11.222. Translate this server as 192.1.20.222 on the outside. Allow Web traffic to this Server from the outside.

FW

```
Object network WWW
 Host 10.11.11.222
 Nat (inside,outside) static 192.1.20.222
!
access-list INF permit tcp any host 10.11.11.222 eq 80
```

Task 4

Deny any web traffic that has any of the following characteristics coming into the server:

- The word CMD anywhere in the URL.
- The word BOMB anywhere in the URL.
- If the packet has request header length greater than 250 bytes.

FW

```
Regex RE-CMD “CMD”
Regex RE-BOMB “BOMB”
!
Class-map type inspect http match-any CM7-RE-WEB
 Match request URI regex RE-CMD
 Match request URI regex RE-BOMB
 Match request header length gt 250
 !
policy-map type inspect http PM7-RE-WEB
 class CM7-RE-WEB
   reset
!
access-list HTTP-S permit tcp any host 192.1.20.222 eq 80
!
class CM4-RE-WEB
 match access-list HTTP-S
!
policy-map global_policy
 class CM4-RE-WEB
   inspect http PM7-RE-WEB
```

Task 5

Configure your firewall to drop all e-mails that are greater the 1 MB in size. Do not create a new class for this.

FW

```
policy-map type inspect esmtp PM7-MAIL
 match body length gt 1000000
   reset
```

```
!
policy-map global_policy
 class inspection_default
   no inspect esmtp
   inspect esmtp PM7-MAIL
```

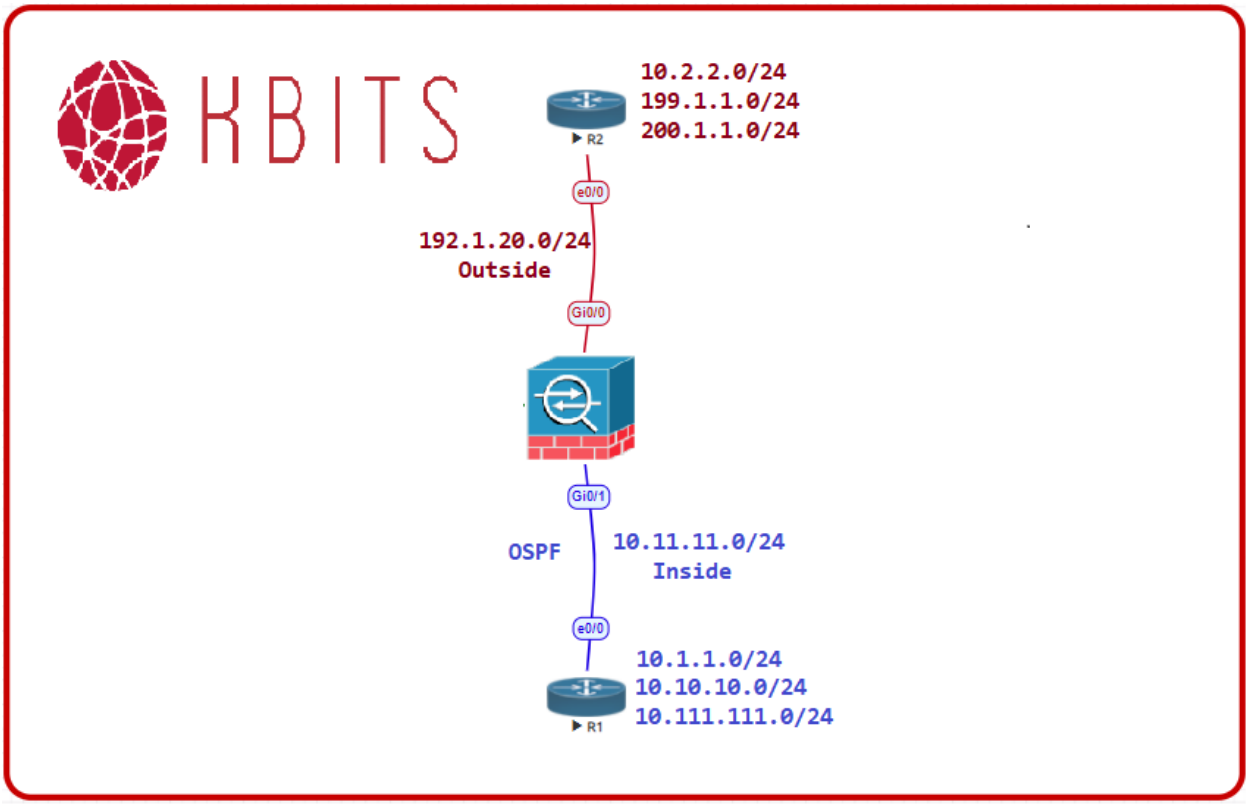
Task 6

Configure your firewall to limit the number of ESP connections from the same client to 25. Do not create a new class for it.

FW

```
policy-map type inspect ipsec-pass-thru PM7-ESP
  parameters
    esp per-client-max 25
!
policy-map global_policy
 class inspection_default
   inspect ipsec-pass-thru PM7-ESP
```

Lab 3 – Configuring TCP Normalization



Lab Scenario:

- Allow BGP neighbor relationship with MD5 authentication to form between 2 Routers thru the Firewall.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure a BGP Neighbor relationship between R1 and R2. They should be in AS 100. They should advertise their local loopback interfaces to each other. Configure a static route on R2 for the 10.11.11.0 network to provide connectivity. Also create a static route for the 192.1.20.0 network. Although, R1 has a default route, BGP needs a non-default route to build a neighbor relationship.

R1 Router BGP 100 Network 200.1.1.0 Neighbor 192.1.20.2 remote-as 100 ! Ip route 192.1.20.0 255.255.255.0 10.11.11.10
R2 Router BGP 100 Network 200.2.2.0 Neighbor 10.11.11.1 remote-as 100 ! Ip route 10.11.11.0 255.255.255.0 192.1.20.10
***** Notice that you did not need to open up any ports on the firewall to accomplish this. This is due to the fact that BGP is tcp-based and the internal neighbor will send a BGP neighbor request to R2. Because of the Implicit TCP inspection, the return packet will be allowed and the neighbor relationship will be formed.**

Task 2

Authenticate the BGP neighbor relationship using a password of cisco.

R1 Router BGP 100 Neighbor 192.1.20.2 password cisco
R2 Router BGP 100 Neighbor 10.11.11.1 password cisco
***** Notice that after specifying the MD5 authentication, the neighbor relationship goes down. To understand this, you need to understand what authentication does. Authentication creates a hash (Like a checksum) of the packet and puts it in a unused TCP header field (Option 19). The hash is used to make sure that the packet was not**

tampered (changed) during transit.

There are 2 reasons for the break.

Number 1: The firewall randomizes (Changes) the TCP sequence number. This breaks the hash.

Number 2: The Option field is cleared by the TCP Normalization process.

To fix it, we modify the default behavior of the TCP Normalization field.

Task 3

Modify the default TCP Randomization parameters to allow the BGP Authentication to take place.

FW

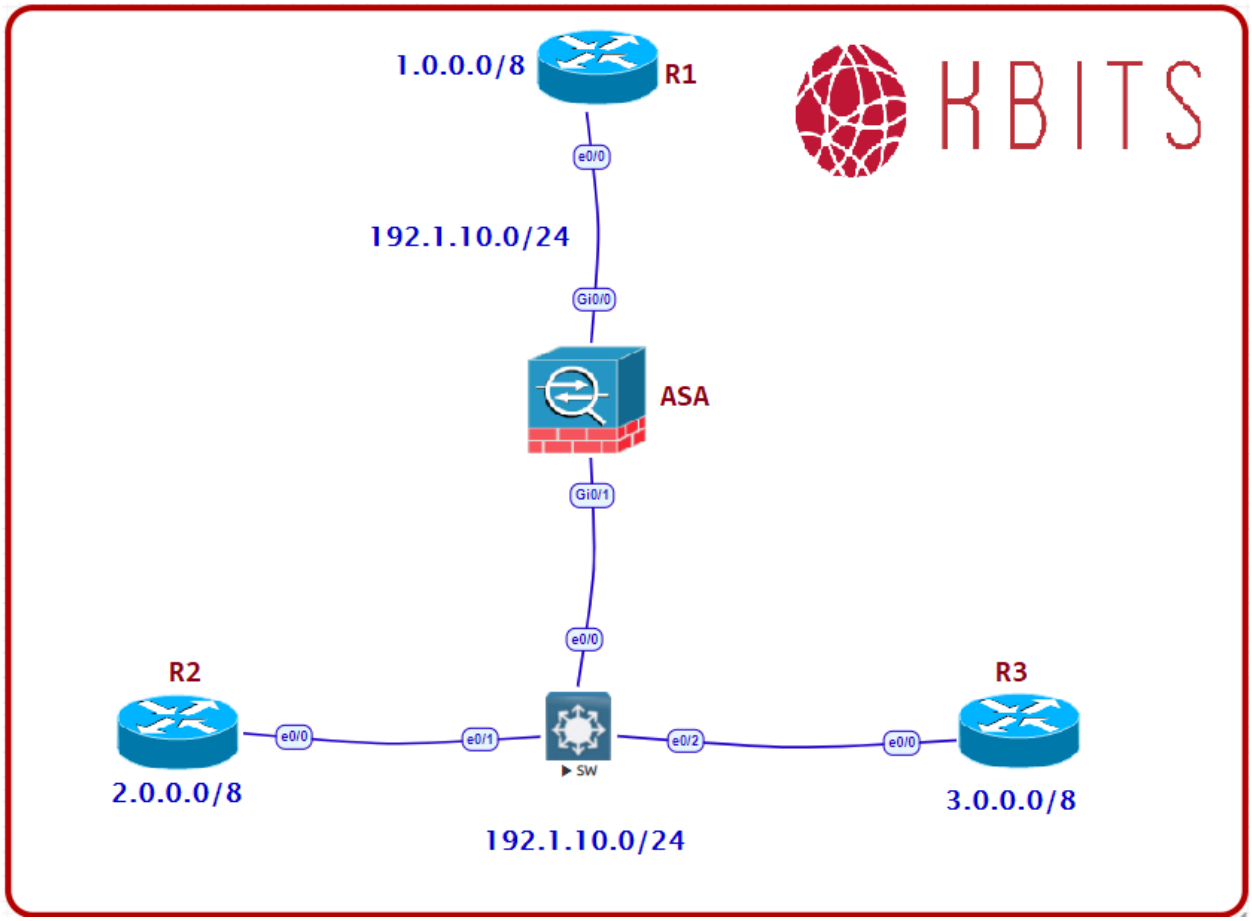
```
TCP-map BGPMAP
 TCP-options range 19 19 allow
!
class-map BGP
 match port tcp eq 179
!
policy-map global_policy
 class BGP
   set connection random-sequence-number disable
   set connection advanced-options BGPMAP
```

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 5:
Transparent Firewalls on 9.X

Module 5 – Transparent Firewalls on 9.X

Lab 1 – Configuring a Transparent Firewall on ASA 9.x



Lab Scenario:

- Initialize the Firewall as Layer 2 Firewall Transparent Firewall.

Initial Setup:

- Configure the IP Addresses on the Routers based on the Diagram.
- Configure the following Loopback addresses on R1, R2 & R3:
  - R1: 10.1.1.0/24
  - R2: 10.2.2.0/24
  - R3: 10.3.3.3/24

- Configure EIGRP in AS 100 on R1, R2 & R3. Enable all the interface in EIGRP.

R1	**R2**
Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Router eigrp 100 Network 192.1.10.0 Network 10.0.0.0	Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int E 0/0 Ip add 192.1.10.2 255.255.255.0 No shut ! Router eigrp 100 Network 192.1.10.0 Network 10.0.0.0
R3 Int loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.1.10.3 255.255.255.0 No shut ! Router eigrp 100 Network 192.1.10.0 Network 10.0.0.0	

Lab Tasks:

Task 1

Configure the Firewall as a Transparent Firewall.

ASA
Firewall Transparent

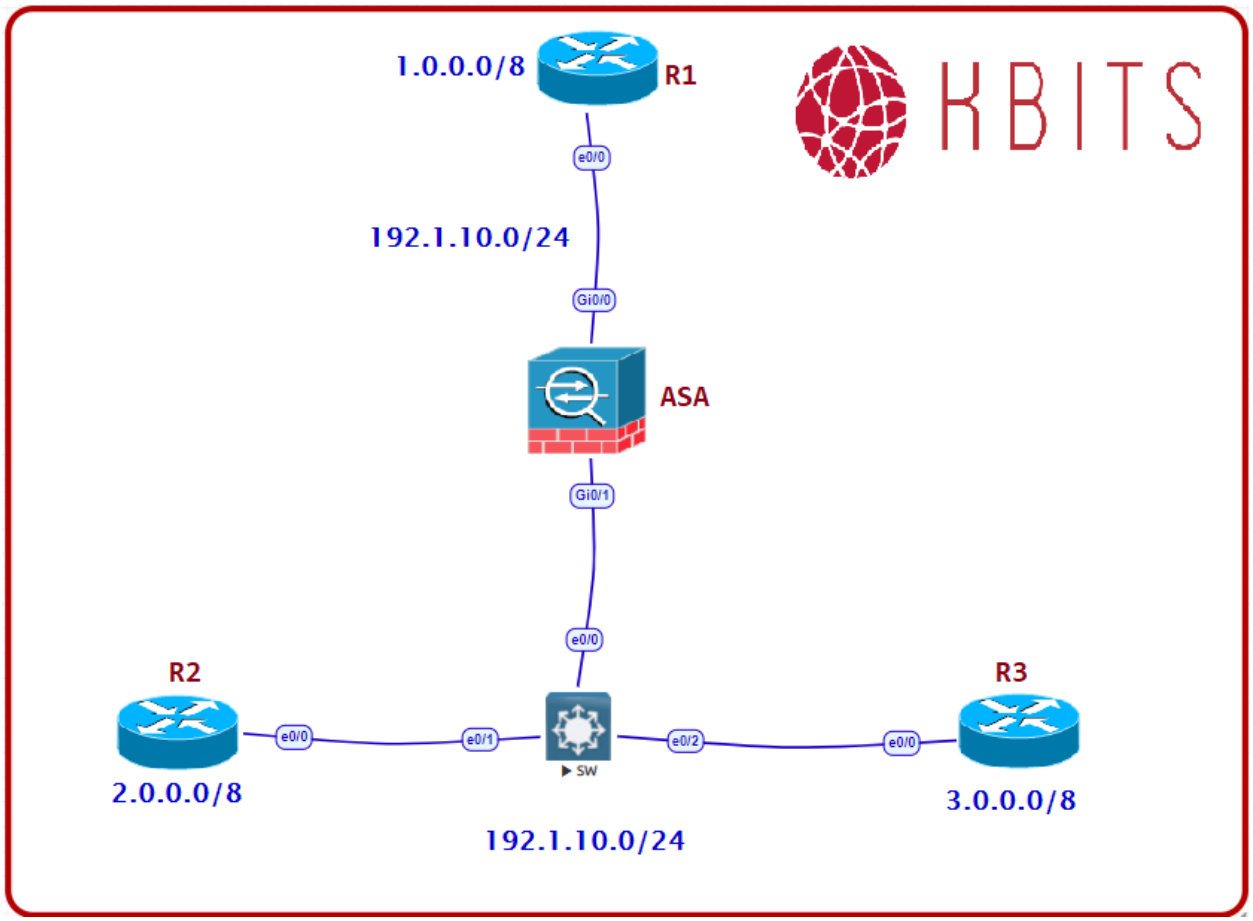
Task 2

Configure G 0/0 as the outside interface with a security level of 0. Bring the Interface up. Configure G 0/1 as the inside interface with a security level of 100. Configure them to be part of the same bridge group. Bring the Interfaces up.

ASA

```
Interface G 0/0
 Nameif outside
 Bridge-group 1
 No shutdown
!
Interface G 0/1
 Nameif inside
 Bridge-group 1
 No shutdown
```

Lab 2 – Configuring Management on a Transparent FW



Lab Scenario:

- Configure the Firewall for Remote Management using Telnet.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Assign the Firewall an IP address of 192.1.10.10/24 to the bridge-group created in the previous lab.

ASA

```
Interface BVI 1
 IP address 192.1.10.10 255.255.255.0
!
Route outside 0 0 10.11.11.2
```

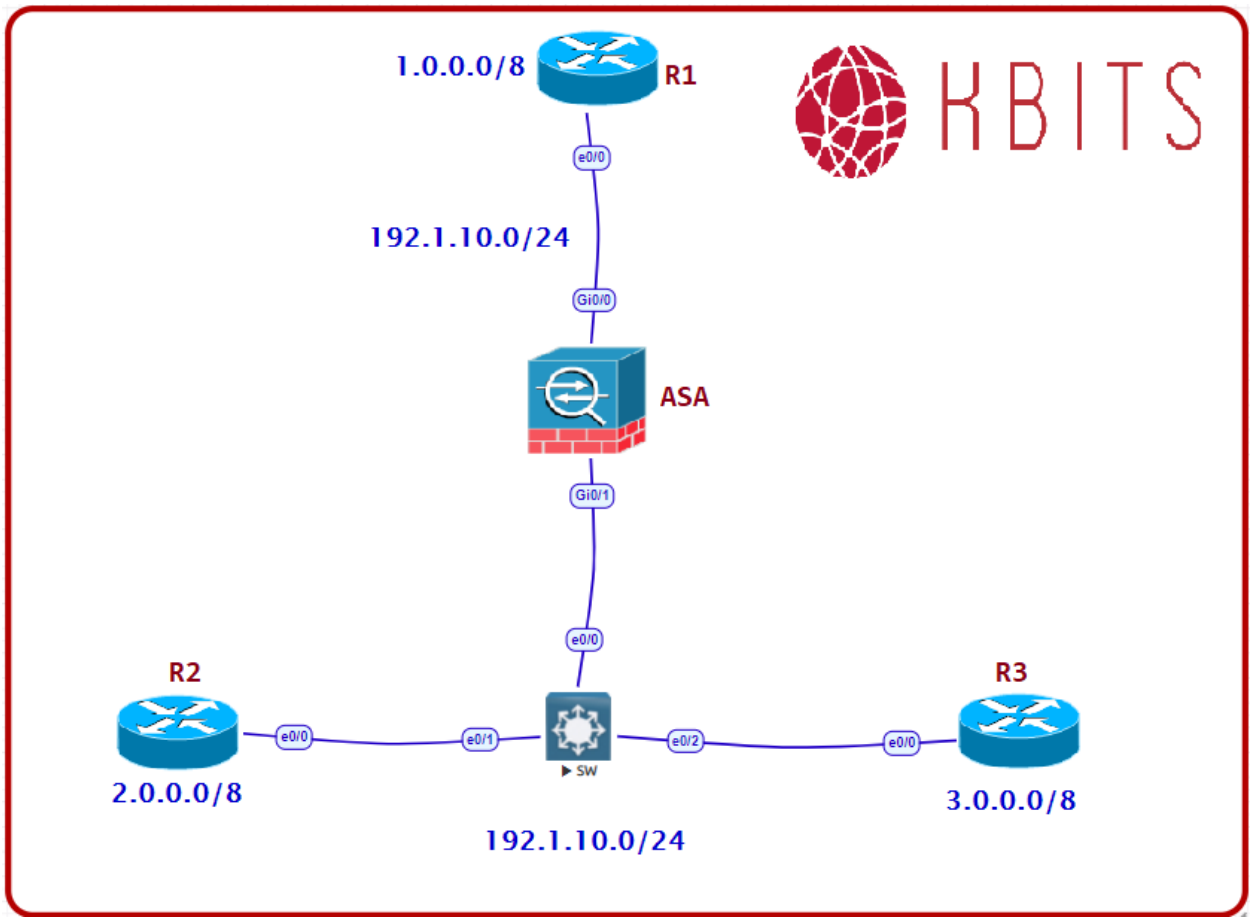
Task 2

Allow Telnet Management of the Firewall only Inside Interface. Configure the authentication based on the Local Database. Create a user named khawar with a password of ccie12353.

FW

```
telnet 192.1.10.0 255.255.255.0 inside
!
Username khawar password ccie12353
Aaa authentication telnet console LOCAL
```

Lab 3 – ACL's in Transparent Mode



Lab Scenario:

- Configure L2 & L3 ACL's on the transparent firewall to control flow of traffic thru it.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure the Firewall to allow R1, R2 and R3 to communicate to each other to exchange Routing information. Allow full access from Inside to Outside.

FW

```
Access-list outside permit eigrp any any
Access-list inside permit ip any any
!
Access-group outside in interface outside
Access-group inside in interface inside
```

Task 2

Allow R1 to Telnet and HTTP into R2.

FW

```
Access-list outside permit tcp host 192.1.10.1 host 192.1.10.2 eq 23
Access-list outside permit tcp host 192.1.10.1 host 192.1.10.2 eq 80
```

Task 3

You will be configuring MPLS-Unicast Routing on R1, R2 and R3 in the future. Make sure the Firewall allows them to communicate to each other. Also, allow BPDU packets and packets with a EtherType 0x2111 thru the Firewall.

FW

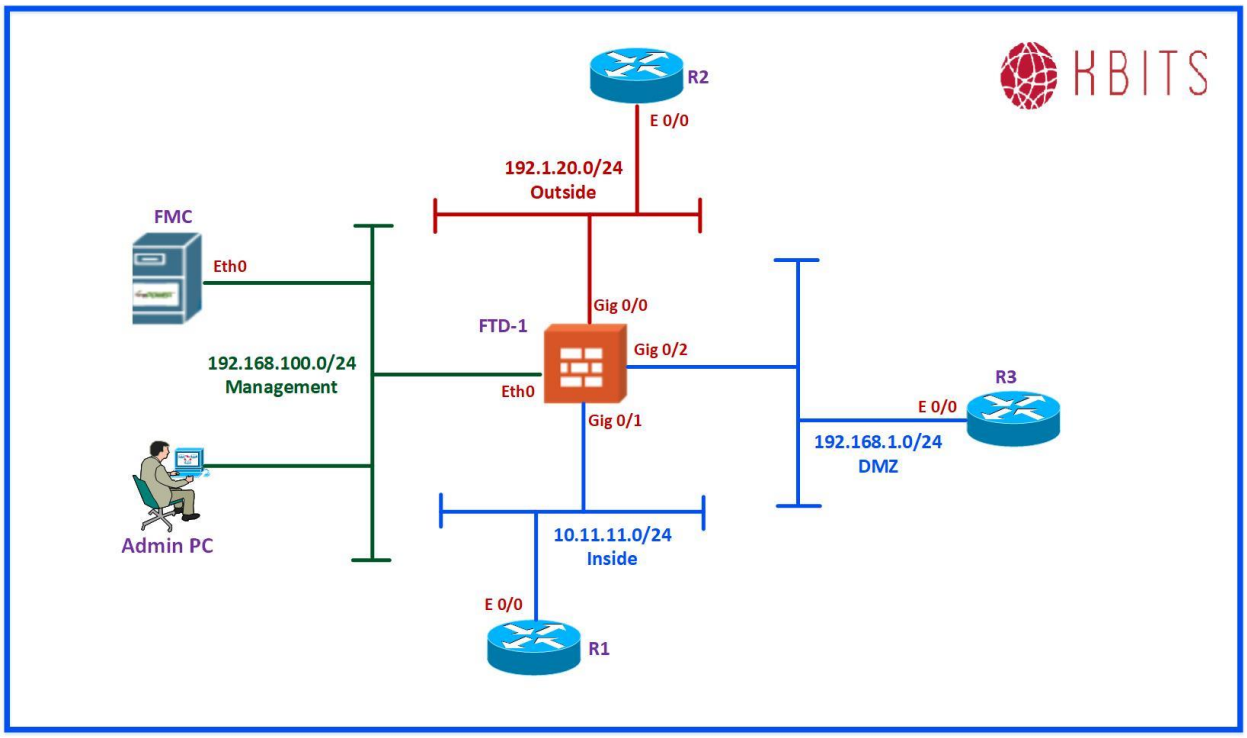
```
access-list E-TYPE ethertype permit bpdu
access-list E-TYPE ethertype permit mpls-unicast
access-list E-TYPE ethertype permit 0x2111
access-group E-TYPE in interface inside
access-group E-TYPE in interface outside
```

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 6:
Configuring the Firewall Component of FTD

Module 6 – Configuring the Firewall Component of FTD

Lab 1 – Initial Configuration of Firepower Threat Defence [FTD] & FMC from CLI



Lab Scenario:

- Initializing the Management parameters of the FTD Device from CLI.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure the following Static Routes on the appropriate routers:
    - Default Routes on R1 pointing towards 10.11.11.10.
    - Default Route on the FW towards 192.1.20.2.
    - Default Route on R2 towards 192.1.20.10.
    - Default Routes on R3 pointing towards 192.168.1.10/24
- Configure the following Loopback addresses on R1,R2 & R3:
    - R1 : 10.1.1.0/24, 100.1.1.1/2
    - R2 : 2.2.2.0/24,199.1.1.1/24,200.1.1.1/24

- R3 : 10.3.3.0/24

R1	**R2**
Int Loopback 1 Ip add 10.1.1.1 255.255.255.0 ! Int loopback 2 Ip add 10.10.10.10 255.255.255.0 ! Int E 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10	Int Loopback 1 Ip add 2.2.2.2 255.255.255.0 ! Int loopback 199 Ip add 199.1.1.1 255.255.255.0 ! Int Loopback 200 Ip add 200.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut
R3 Int Loopback 1 Ip add 10.3.3.3 255.255.255.0 ! Int E 0/0 Ip add 192.168.1.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.168.1.10	

Lab Tasks:

Task 1

Configure the Firepower Management Center [FMC] IP as 192.168.100.50/24 with a default gateway of 192.168.100.254.

FMC CLI

Sudo configure-network

Do you wish to Configure iPv4? [y or n] **y**

Management IP Address>?[] **192.168.100.50**

Management netmask?[] **255.255.255.0**

Management default gateway? [] **192.168.100.254**

Management IP address? **192.168.100.50**

Management netmask? **255.255.255.0**

Management default gateway? **192.168.100.254**

Are these settings correct? (y or n**) y**

Do you wish to configure IPv6 (y or n) **n**

Wait for it to complete the configuration.

Task 2

Initialize the FTD based on the following:

- Admin Password: Kbits@123
- IP Address/Subnet Mask: 192.168.100.51/24
- Default Gateway: 192.168.100.254
- FQDN: FTD-1.kbits.live
- Firewall Mode: Routed

FTD CLI

1. Login using the default creds (admin/Admin123)

2. Accept the EULA

3. Change the default password

4. Configure the IP Address for FTD Management Interface

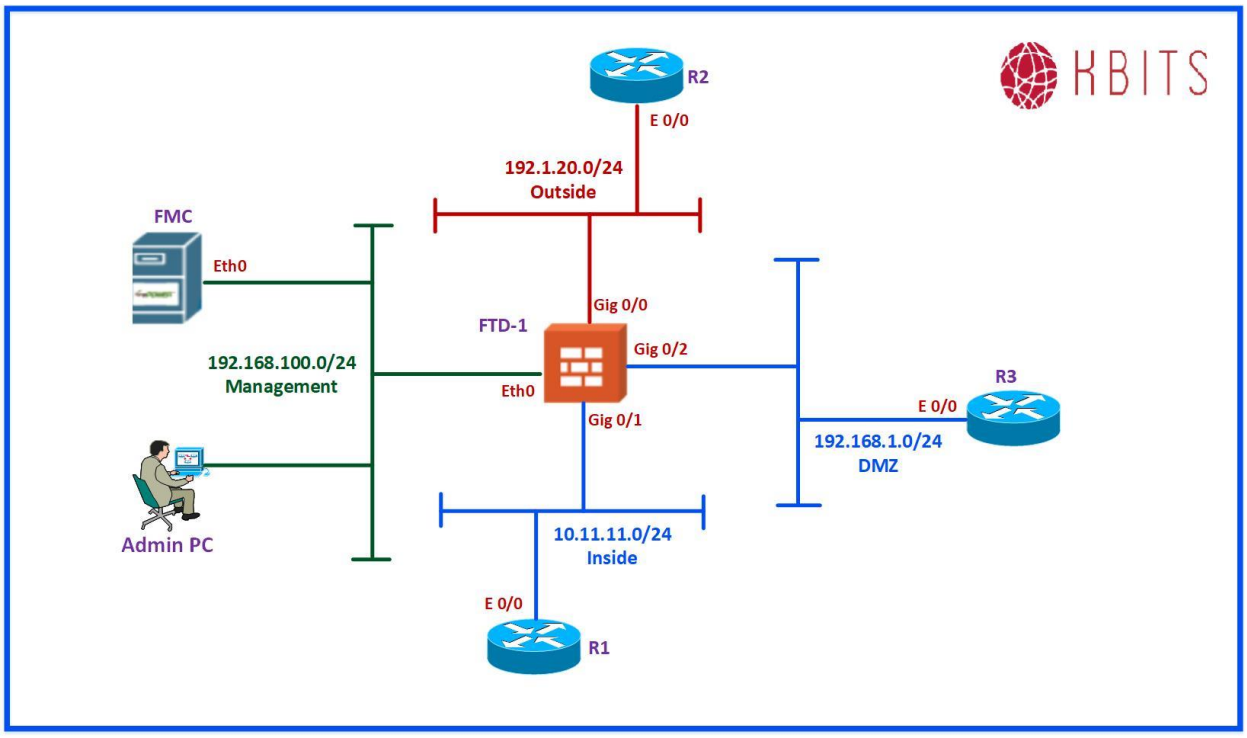
IPv4 Address: 192.168.100.51
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.100.254
Hostname: FTD1.Kbits.live
DNS: None

5. Configure the Firewall Mode (Routed/Transparent) Routed

6. Verifying the connectivity

ping system 192.168.100.50

Lab 2 – Registering & Initializing the FTD Device on FMC



Lab Scenario:

- Configure the FTD to use the FMC as the Manager Device from CLI
- Register the FTD in the FMC Console.
- Configure the Intial Setup of FTD.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Log into the FMC using a browser. The default username is Admin with a password of Admin123.

Management PC

Initializing Page

Change Password:

Password: Kbits@123
Confirm Password: Kbits@123

Network Settings:

IP Address: 192.168.100.50
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.100.254
Hostname: **FMC**
Domain: **Kbits.live**
DNS Server: 8.8.8.8

Time Settings:

Clock: Via **NTP**
Change the Timezone: **Asia/Dubai**

End User Agreement:

Click the checkbox to Accept it

Click "**Apply**" to accept the Changes:

Note: It takes several minutes for it to initialize the FMC.

Task 2

Ensure the FMC is the NTP Server & Initialize the Evaulation License.

Management PC

Licensing

System -> Configuration -> Time Synchronization

-> Serve Time via NTP: **Enabled**

-> Click Save

System -> Licensing -> Smart Licensing -> Evaluation Mode

-> Activate Evaluation Period

Task 3

Configure the relationship between the FTD & FMC.

FTD CLI

configure manager add 192.168.100.50 Kbits123

Task 4

Register the FTD. Create a Default Policy that will Block all the Traffic.

Management PC

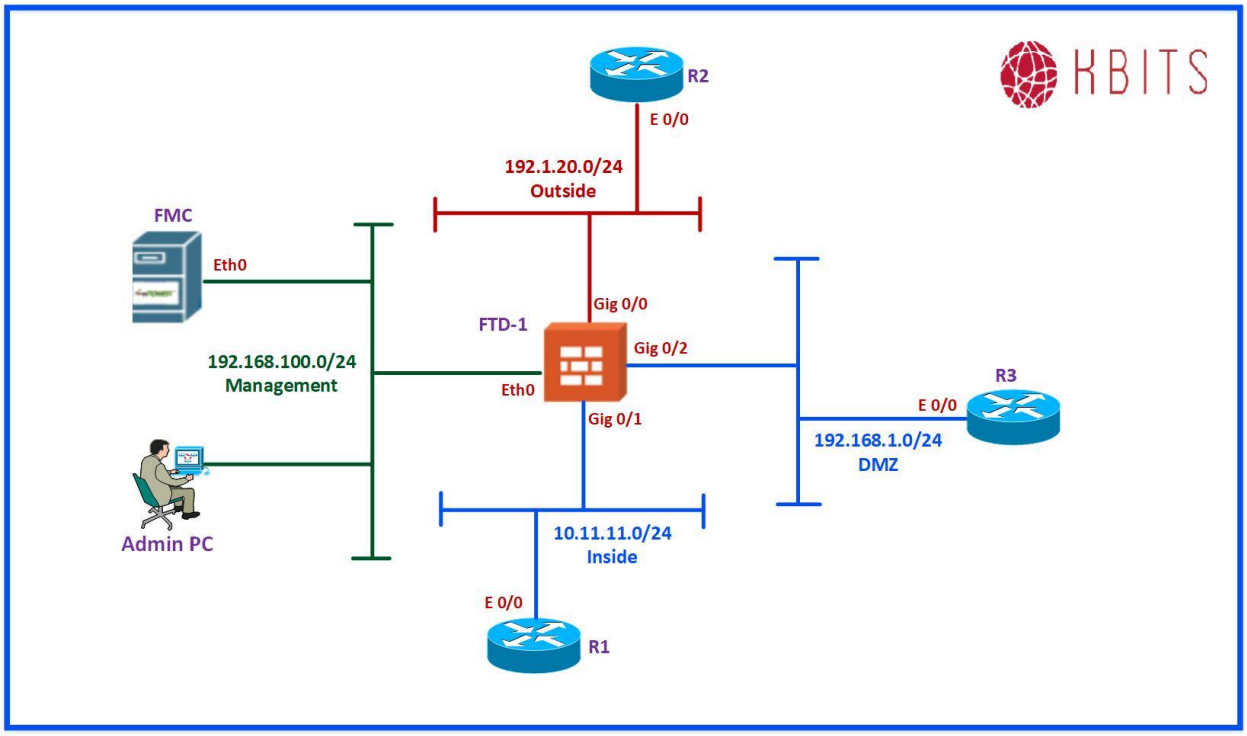
Registration

Devices -> Device Management -> Add Device

Address: 192.168.100.51
Display Name: FTD-1
Registration Key: Kbits123
Default Policy: FTD-1-ACP (Block All traffic)

Enable the licenses and click **Add**

Lab 3 – FTD Interface Configuration



Lab Scenario:

- Configure & Initialize the Interfaces on FTD

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Lab Tasks:

Task 1

Configure the FTD with the following IP configuration for the Interfaces:

Interface	Name	Zone	IP Address
G 0/0	Outside	OUTSIDE	192.1.20.10/24
G 0/1	Inside	INSIDE	10.11.11.10/24
G 0/2	DMZ	DMZ	192.168.1.10/24

FMC

1. Browse to "**Devices -> Device Management -> FTD-1 -> Edit -> Interfaces**"

2. Configure the Interfaces using the following:

Interface: Gig0/0
Name: Outside
Enabled: Check
Zone: OUTSIDE
IP Address: 192.1.20.10/24

Interface: Gig0/1
Name: Inside
Enabled: Check
Zone: INSIDE
IP Address: 10.11.11.10/24

Interface: Gig0/2
Name: DMZ
Enabled: Check
Zone: DMZ
IP Address: 192.168.1.10/24

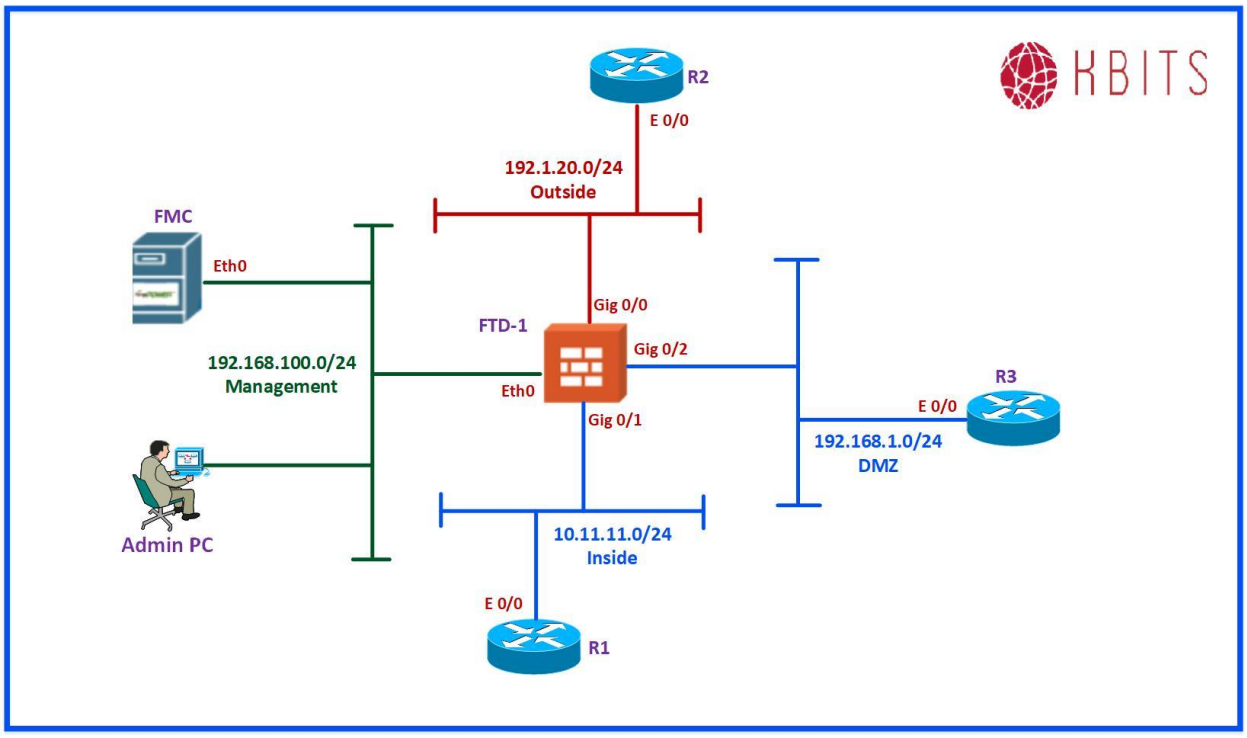
Task 2

Deploy the Changes to the FTD. After the deployment is successful, FTD should be reachable from R1, R2 & R3.

FMC

-> Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

Lab 4 – Routing Protocol Configuration – Static and Default Routes



Lab Scenario:

- Configure Default and Static routes on FTD to provide connectivity.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure the FTD with a Static Routes to the internal loopbacks network 10.1.1.0/24 & 10.10.10.0/24 networks.

FMC

1. Browse to "**Devices -> Device Management -> FTD-1 -> Edit -> Routing**"

2. Configure the Static Routes based on the following:

Route Towards the Internal Network 10.10.10.0/24.

Interface: **Inside**
Network: **10.10.10.0/24** (Object Name: **"NET-10.10.10.0"**)
Gateway: 10.11.11.1 (Object Name: **"R1"**)

3. Click **OK**

Task 2

Configure a default route on the FTD pointing towards R2.

FMC

1. Browse to "**Devices -> Device Management -> FTD-1 -> Edit -> Routing**"

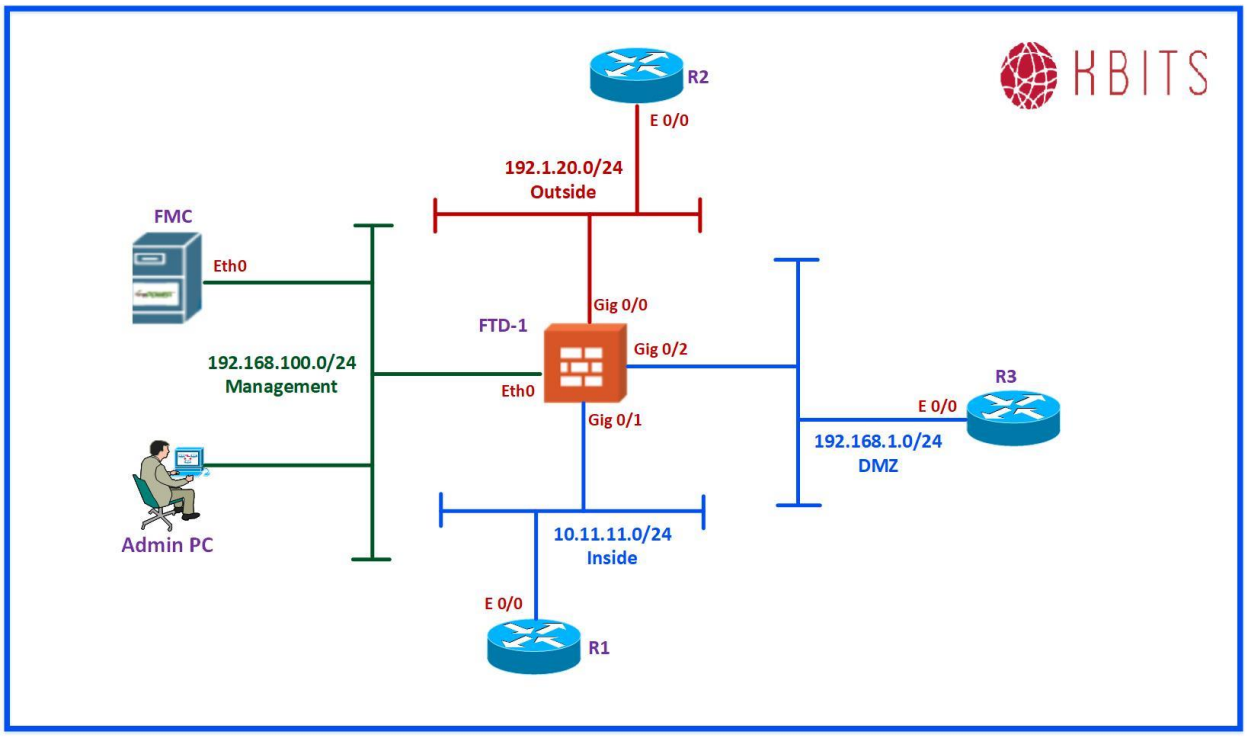
2. Configure the Static Routes based on the following:

Default Route Towards R2

Interface: **Outside**
Network: **any-ipv4**
Gateway: 192.1.20.2 (Object Name: **"R2"**)

3. Click **OK**

Lab 5 – Routing Protocol Configuration - Running RIP V2



Lab Scenario:

- Configure RIP v2 on the Firewall.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure RIP v2 on the FTD on the DMZ interface. Disable auto-summarization of routes. Also, configure RIP v2 on R3. Advertise the Loopback network on R3 under RIP.

FMC

1. Browse to "**Devices -> Device Management -> FTD-1 -> Edit -> Routing**"

2. Configure RIP based on the following:

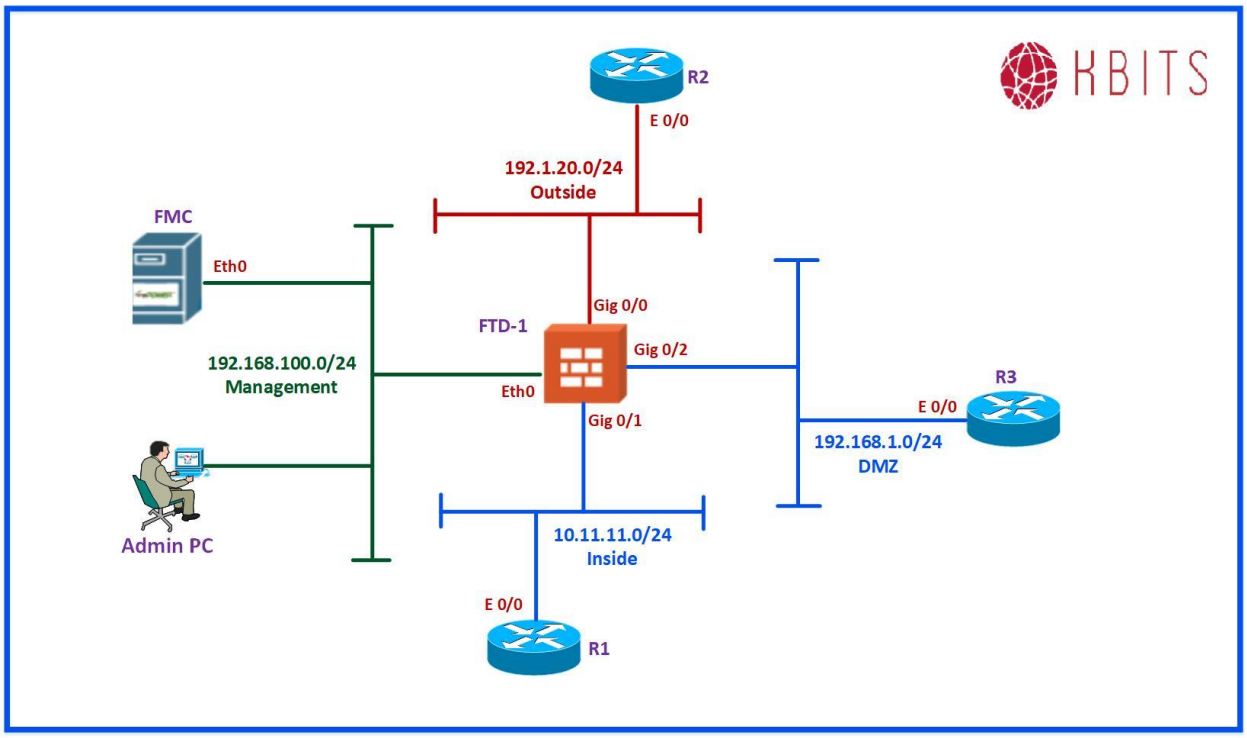
    Version: **Send & Receive Version 2**
    Auto-Summary: **Disable** (Uncheck the Checkbox)
    Network: 192.168.1.0/24 (Object Name: **"NET-192.168.1.0"**)

3. Click **OK**

R3

Router rip
 No auto-summary
 Version 2
 Network 192.168.1.0
 Network 10.0.0.0

Lab 6 – Routing Protocol Configuration – Running OSPF



Lab Scenario:

- Configure OSPF on the Firewall.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure OSPF on the Inside interface of the FTD in Area 0. Hard-code the Router-id as 10.10.10.10. Also, configure OSPF on R1. Hard-code the router-id as 0.0.0.1. Have R1 advertise the Loopback network 10.1.1.0/24 in OSPF. Have the FTD inject a default route towards the Inside network.

FMC

1. Browse to "**Devices -> Device Management -> FTD-1 -> Edit -> Routing**"

2. Configure OSPF based on the following:

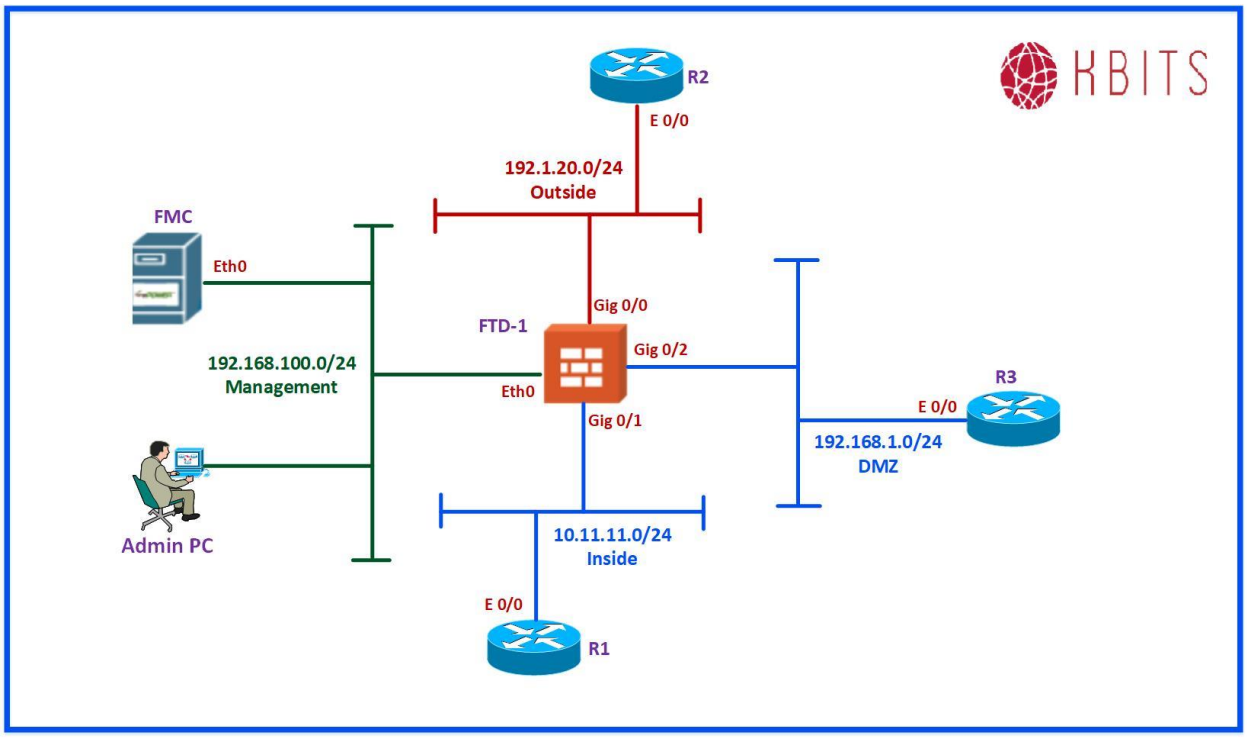
Process ID: 1
Router Type: **ASBR**
Advanced:
Routed-id: **10.10.10.10**
Default-Information Orignate: **Enable**
Default-Information Orignate Always: **Enable**
Network: 10.11.11.0/24 (Object Name: **"NET-10.11.11.0"**)

3. Click **OK**

R1

```
Router OSPF 1
 Router-id 0.0.0.1
 Network 10.11.11.0 0.0.0.255 area 0
 Network 10.1.1.0 0.0.0.255 area 0
```

Lab 7 – Routing Protocol Configuration – Running BGP



Lab Scenario:

- Configure BGP on FTD.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure BGP on the Outside interface of the Firewall in AS 65001 to exchange routes with R2. Advertise the R2 Loopbacks in BGP.

FMC

1. Browse to "**Devices -> Device Management -> FTD-1 -> Edit -> Routing**"

2. Configure BGP based on the following:

    AS #: 65001
    Router Type: **ASBR**
    Address Family: IPv4
        Neighbor: **192.1.20.2**
        Remote-AS: **65001**
        Address-Family: **Enabled**

3. Click **OK**

R2

```
Router BGP 65001
 Network 2.0.0.0
 Network 199.1.1.0
 Network 200.1.1.0
 Neighbor 192.1.20.10 remote-as 65001
```

Task 2

Perform Route Redistribution such that all devices have a complete picture of the entire topology.

FMC

1. Browse to "**Devices -> Device Management -> FTD-1 -> Edit -> Routing**"

Redistribution into BGP

2. Click **"BGP -> IPv4 -> Redistribution -> Add**"

3. Configure Redistribution into BGP based on the following:

    Source: OSPF 1, RIP & Connected Networks

4. Click **OK**

Redistribution into OSPF

5. Click **"OSPF -> Redistribution -> Add**"

6. Configure Redistribution into OSPF based on the following:

    Source: BGP AS # 65001, RIP & Connected Networks
    Subnets: Enable "Use Subnets" for all Sources
    Seed metric: 20 for all Sources

7. Click **OK**

Redistribution into RIP

8. Click **"RIP -> Redistribution -> Add**"

9. Configure Redistribution into RIP based on the following:

    Source: BGP AS # 65001, OSPF 1 & Connected Networks
    Seed metric: 1 for all Sources

10. Click **OK**

Task 3

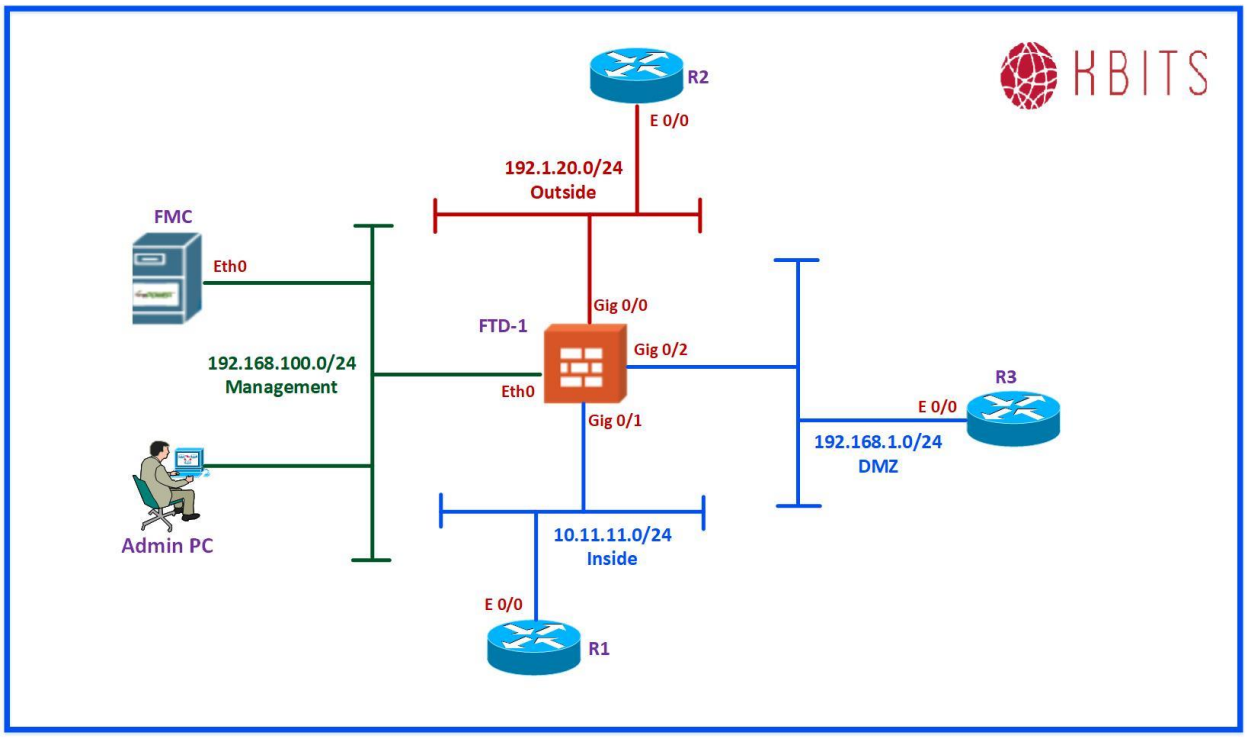
Deploy the Changes to the FTD

FMC

1. Save the changes to the Routing Tab by clicking on the **Save** button.

2. Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

Lab 8 – Configuring Access Control Policies – Basic Filtering



Lab Scenario:

- Configure Access Control Policies on the FTD using FMC Console.
- Configure ACP Policies based on L3 & L4 characteristics.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Allow access to the following DMZ Servers from the OUTSIDE. Allow access to based on the following:

- 192.168.1.11 -> [Web Services – 80 & 443]
- 192.168.1.12 -> [E-Mail Services – 25]
- 192.168.1.13 -> [DNS – 53]
- 192.168.1.3 -> [Telnet & SSH – 22 & 23]

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#1

Name: **WebServer-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks

Source: **Any-IPv4**
Destination: 192.168.1.11 (Object Name: **WebServer**)
Destination Port#s: Objects **(HTTP & HTTPs)**

Policy#2

Name: **MailServer-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks

Source: **Any-IPv4**
Destination: 192.168.1.12 (Object Name: **MailServer**)
Destination Port#s: Objects **(SMTP)**

Policy#3

Name: **DNSServer-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks

Source: **Any-IPv4**
Destination: 192.168.1.13 (Object Name: **DNSServer**)
Destination Port#s: Objects **(DNS_Over_UDP)**

Policy#4

Name: **R3-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks

Source: **Any-IPv4**
Destination: 192.168.1.3 (Object Name: **R3**)
Destination Port#s: Objects **(Telnet & SSH)**
ICMP (Object Name: **PING**)

Task 2

Allow Full access from NET-10.10.10.0/24, NET-10.11.11.0/24 & 10.1.1.0/24 towards any IPv4 address on the outside in the Default Policy

FMC

1. Browse to "Policies -> Access Control -> Access Control -> FTD-ACP -> Edit"

2. Configure the policies based on the following:

Default Policy

Policy#1

Name: **INSIDE-To-ANY**
Action: **Allow**

Zones:

Source Zone: **INSIDE**
Destination Zone: **OUTSIDE, DMZ**

Networks

Source: Objects (**NET-10.10.10.0 & NET-10.11.11.0**)
10.1.1.0/24 (Object Name: **NET-10.1.1.0**)
Destination: **Any-IPv4**

Task 3

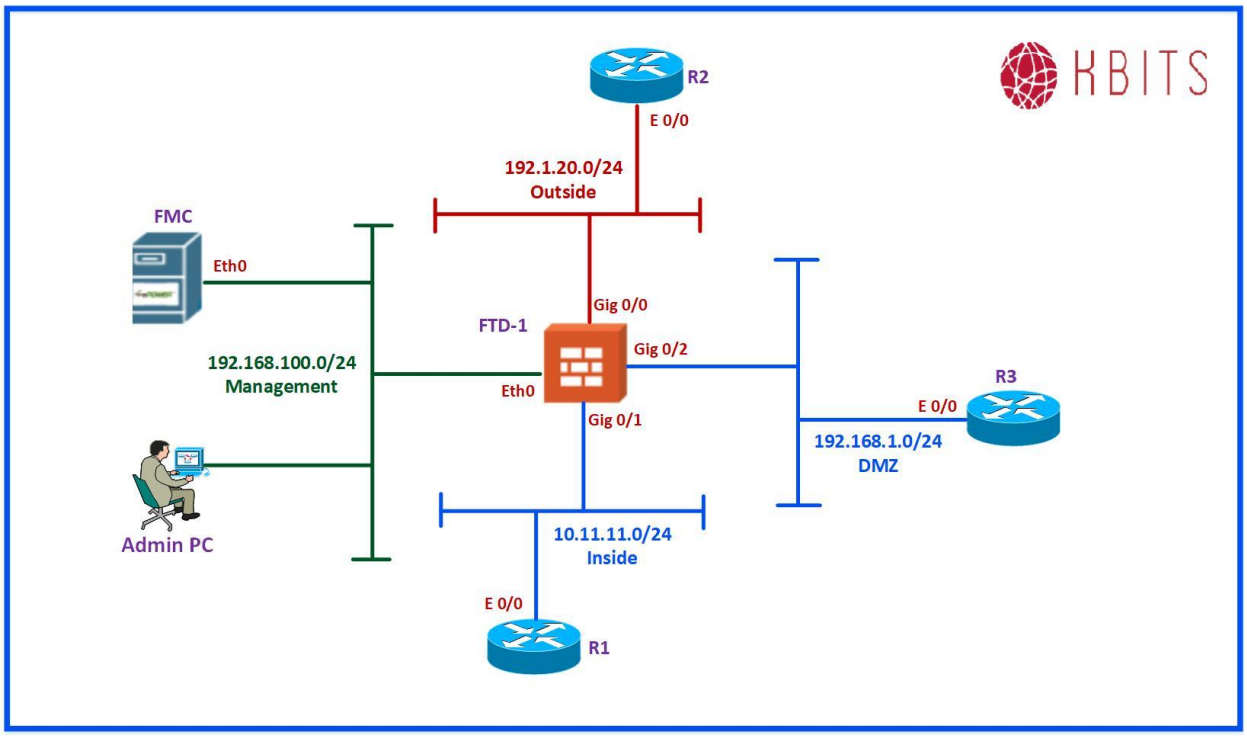
Deploy the Changes to the FTD

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

2. Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

Lab 9 – Configuring Access Control Policies – Advanced Filtering



Lab Scenario:

- Configure Access Control Policies on the FTD using FMC Console.
- Configure ACP Policies based on L3 & L4 characteristics.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Block all RFC-1918 address coming in from the Outside Zone. Put it as the first rule in the Mandatory category.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#1

Name: **Block-RFC-1918**
Action: **Block**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **Any**

Networks

Source: Object (**IPv4-Private-All-RFC1918**)
Destination: any-ipv4

Task 2

Block all traffic coming in from the Outside zone that is sourced from North Korea. Make it the 2nd rule in the Mandatory category.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#2

Name: **Block-North-Korea**
Action: **Block**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **Any**

Networks-Geolocations

Source: Object (**Geolocation:North Korea**)
Destination: any-ipv4

Task 3

Block all Medium, High & Very High Risk applications. This should be applied to traffic from INSIDE to OUTSIDE Zones. Make it the 3rd rule in the Mandatory category.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#3

Name: **Block-Risky-Applications**
Action: **Block**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **Any**

Applications

Filters: Objects (**Risk: Medium, High & Very High**)

Task 4

Block Facebook Video Chats from INSIDE to OUTSIDE Zones. Make it the 4th rule in the Mandatory category.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#4

Name: **Block-FB-Video-Chats**
Action: **Block**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **Any**

Applications

Applications: Objects (**Facebook Video Chats**)

Task 5

Add a rule to the Mandatory Category to block the following URL Categories. Make it the 5th rule in the Mandatory category. This should be done for Traffic from the INSIDE zone to the OUTSIDE zone:

- Adult & Pornography
- Gambling
- Games

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#5

Name: **Block-URLS**
Action: **Block**

Zones:

Source Zone: **INSIDE**
Destination Zone: **OUTSIDE**

URLS:

Categories: Objects (**Adult & Pornography, Gambling, Games**)

Task 6

Deploy the Changes to the FTD

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

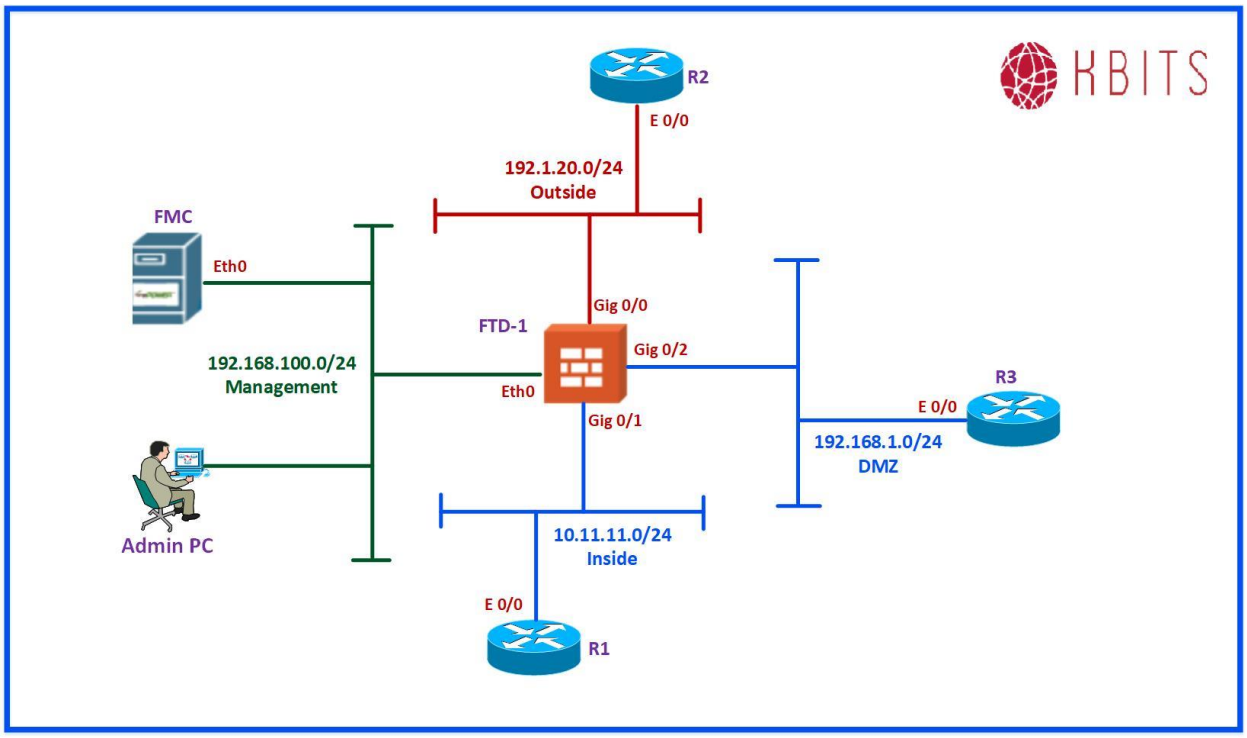
2. Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 7:
Configuring NAT on FTD

Module 7 – Configuring NAT on FTD

Lab 1 – Configuring Dynamic NAT & Dyanmic PAT



Lab Scenario:

- Configure Dynamic NAT
- Configure Dynamic PAT

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

The Firewall should translate all traffic going from 10.11.11.0/24 towards the outside using a pool of 192.1.20.151 – 192.1.20.200.

FMC

1. Browse to "Devices -> NAT -> New Policy -> Threat Defence NAT"

2. Configure using the following:

   Name: **FTD-1-NAT**
   Device: **FTD-1**

3. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Dynamic**

   Interface Objects:

   Source: **INSIDE**
   Destination: **OUTSIDE**

   Translation:

   Original Source: Object (**NET-10.11.11.0)**
   Translated Packet: 192.1.20.51-192.1.20.200 (Object Name: **POOL-A**)

4. Click the **OK**.

Task 2

The Firewall should translate all traffic going from 10.1.1.0/24 towards the outside using an IP Address of 192.1.20.9.

FMC

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Dynamic**

Interface Objects:

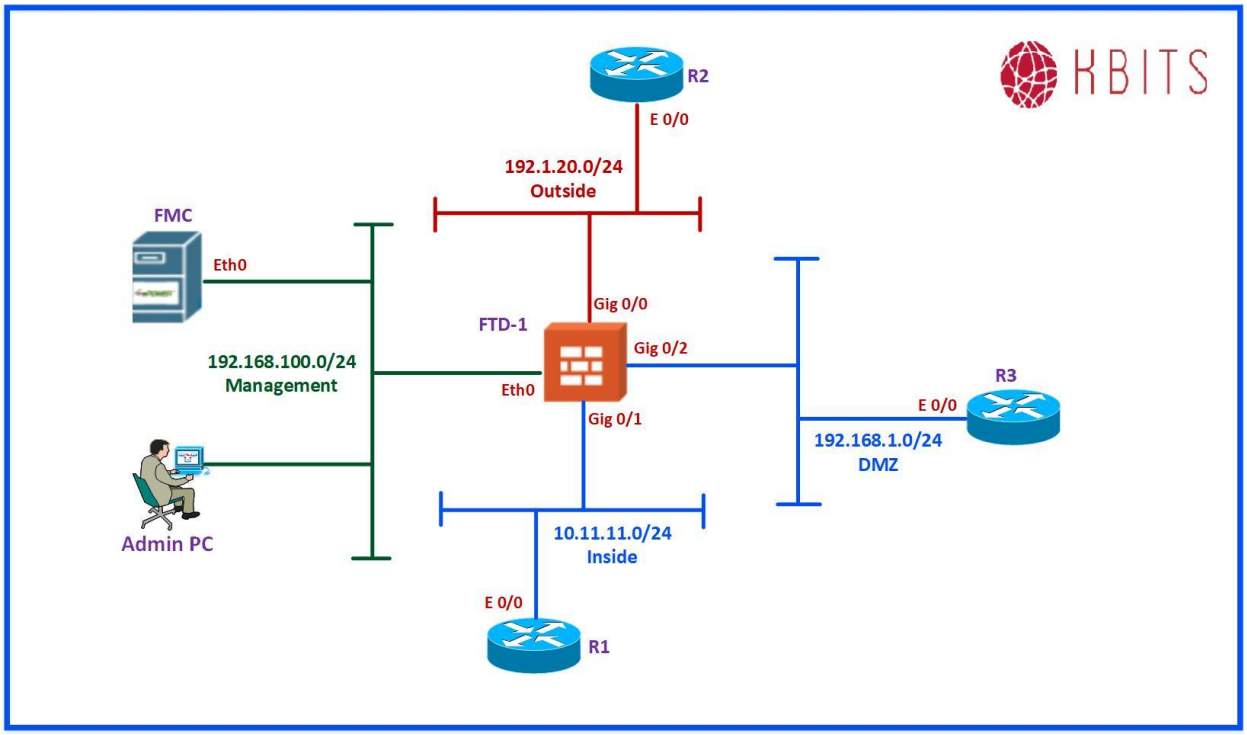
Source: **INSIDE**
Destination: **OUTSIDE**

Translation:

Original Source: Object (**NET-10.1.1.0)**
Translated Packet: 192.1.20.9 (Object Name: **PAT-IP**)

4. Click the **OK**.

Lab 2 – Configuring Static NAT



Lab Scenario:

- Configure Static NAT
- Configure Static Identity NAT

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Statically translate the following devices on the Outside:

- 192.168.1.11 -> 192.1.20.21 [**WebServer**]
- 192.168.1.12 -> 192.1.20.22 [**MailServer**]
- 192.168.1.13 -> 192.1.20.23 [**DNSServer**]
- 192.168.1.3 -> 192.1.20.3 [**R3**]

FMC

NAT for WebServer

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **DMZ**
   Destination: **OUTSIDE**

   Translation:

   Original Source: Object (**WebServer**)
   Translated Source: 192.1.20.21 (Object Name: **WebServer-X**)

2. Click the **OK**.

NAT for MailServer

3. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **DMZ**
   Destination: **OUTSIDE**

   Translation:

Original Source: Object (**MailServer**)
Translated Source: 192.1.20.22 (Object Name: **MailServer-X**)

4. Click the **OK**.

NAT for DNSServer

5. Click **"Add Rule"** and create the rule based on the following:

NAT Rule: **Auto NAT Rule**
Type: **Static**

Interface Objects:

Source: **DMZ**
Destination: **OUTSIDE**

Translation:

Original Source: Object (**DNSServer**)
Translated Source: 192.1.20.23 (Object Name: **DNSServer-X**)

6. Click the **OK**.

NAT for R3

7. Click **"Add Rule"** and create the rule based on the following:

NAT Rule: **Auto NAT Rule**
Type: **Static**

Interface Objects:

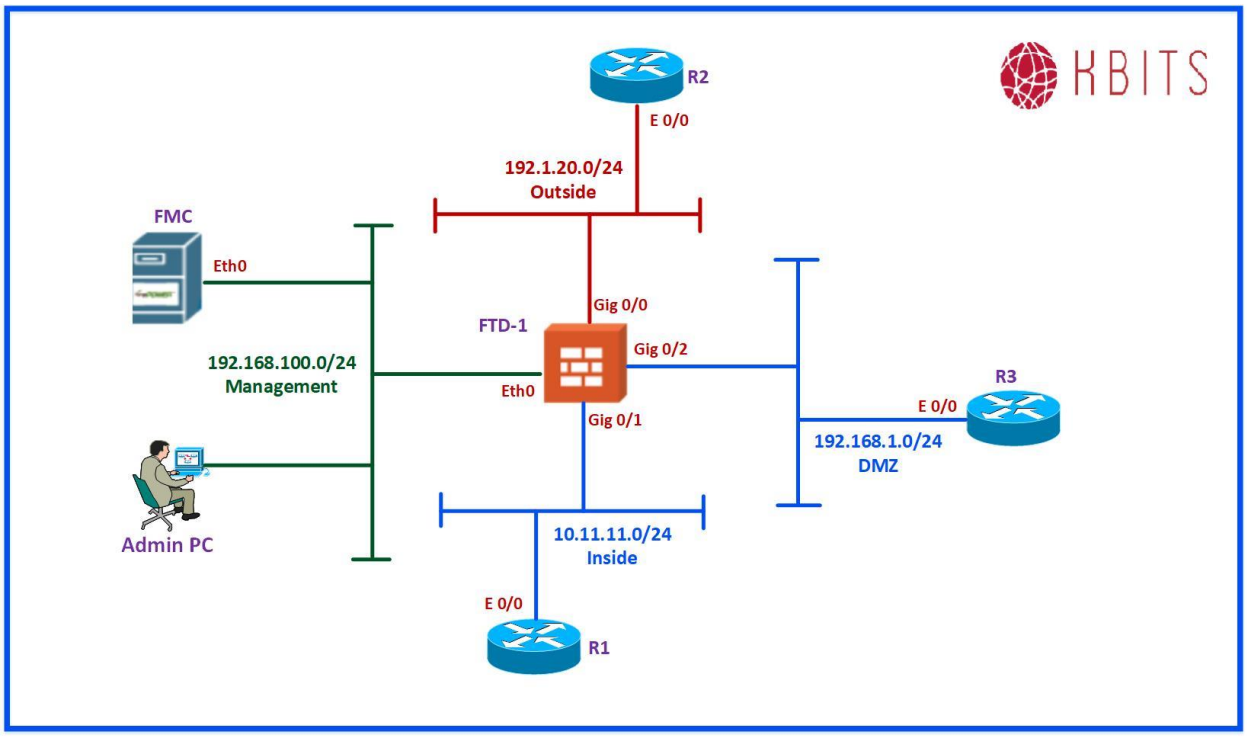
Source: **DMZ**
Destination: **OUTSIDE**

Translation:

Original Source: Object (**R3**)
Translated Source: 192.1.20.3 (Object Name: **R3-X**)

8. Click the **OK**.

Lab 3 – Configuring Static PAT



Lab Scenario:

- Configure Static PAT

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure Static PAT on the Firewall such that if a request comes from the outside destined for an IP Address 192.1.20.7 with a port number 25, the firewall should forward the request to a SMTP server **[MailServer-2]** located at 192.168.1.21

FMC

NAT for MailServer-2

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **DMZ**
   Destination: **OUTSIDE**

   Translation:

   Original Source: 192.168.1.21 (**MailServer-2**)
   Original port: TCP/25
   Translated Source: Object (Name: **PAT-IP**)
   Translated port: TCP/25

2. Click the **OK**.

Task 2

If a request comes into the Firewall destined for an IP Address 192.1.20.7 with a port number 80, the Firewall should forward the request to a Web Server **[WebServer-2]** located at 192.168.1.22 for 80.

FMC

NAT for WebServer-2

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

Interface Objects:

Source: **DMZ**
Destination: **OUTSIDE**

Translation:

Original Source: 192.168.1.22 (**WebServer-2**)
Original port: TCP/80
Translated Source: Object (**PAT-IP**)
Translated port: TCP/80

2. Click the **OK**.

Task 3
Save the Changes to the FTD

FMC

1. Save the changes to the NAT Policy by clicking on the **Save** button.

Task 4
Configure the ACP to allow Access to the Servers defined in the previous task. The policies should the be last ones in the Mandatory Policies.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy – MailServer-2

Name: **MailServer2-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks

Source: **Any-IPv4**

Destination: Object (**MailServer-2**)
Destination Port#s: Objects **(SMTP)**

Mandatory Policy – WebServer-2

Name: **WebServer2-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks

Source: **Any-IPv4**
Destination: Object (**WebServer-2**)
Destination Port#s: Objects **(HTTP)**

3. Click the **OK**.

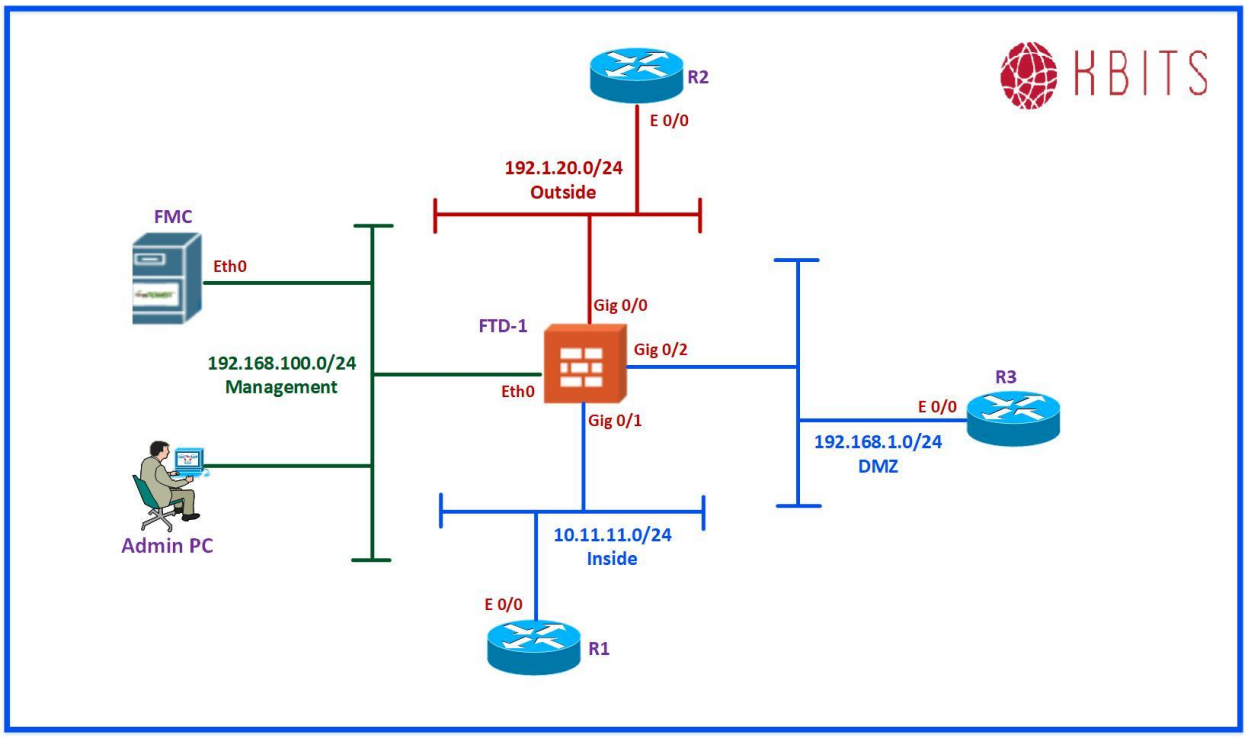
Task 5

Save the Changes to the FTD

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

Lab 4 – Configuring Twice-NAT / Manual NAT



Lab Scenario:

- Configuring Twice-NAT [Policy NAT]

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure FMC such that when a R1 (10.11.11.1) communicates with R2 Loopback199 (199.1.1.1], it is seen as 192.1.20.31.

FMC

NAT for R1 communicating to 199.1.1.1

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Manual NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **INSIDE**
   Destination: **OUTSIDE**

   Translation:

   Original Source: Object (**R1**)
   Original Destination: 199.1.1.1 (Object name: **R2-199**)
   Translated Source: 192.1.20.31 (Object-name: **R1-X1**)
   Translated Destination: Object (**R2-199**)

2. Click the **OK**.

Task 2

Configure the Firewall such that when a R1 (10.1.1.1) communicates with R2 Loopback200 (200.1.1.1], it is seen as 192.1.20.32.

FMC

NAT for R1 communicating to 200.1.1.1

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Manual NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **INSIDE**

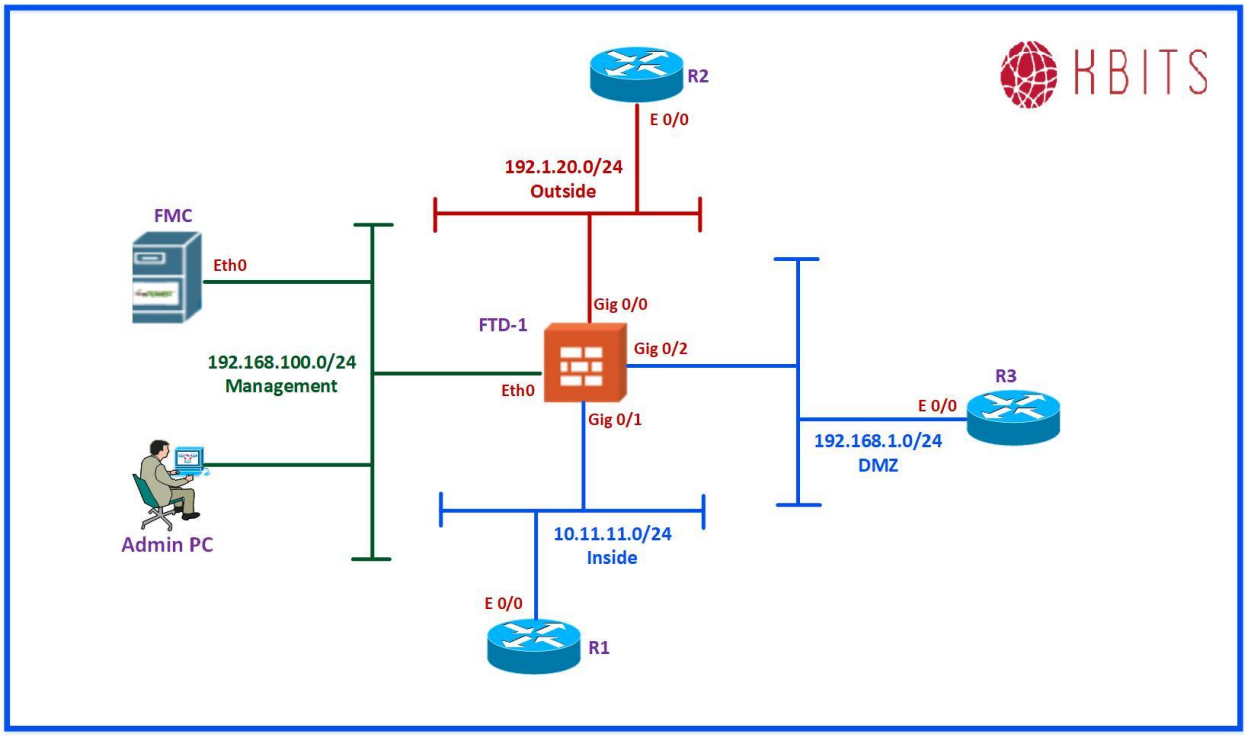
Destination: **OUTSIDE**

Translation:

Original Source: Object (**R1**)
Original Destination: 200.1.1.1 (Object name: **R2-200**)
Translated Source: 192.1.20.32 (Object-name: **R1-X2**)
Translated Destination: Object (**R2-200**)

2. Click the **OK**.

Lab 5 – Configuring Destination NAT



Lab Scenario:

- Configure Destination NAT.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

There is a Mainframe located on the DMZ at 192.168.1.99. Another Mainframe (200.1.1.1) from the outside needs to access it; The local Mainframe should be seen as 192.1.20.29 on the outside. The local Mainframe does not have the ability to point to a default gateway. Allow the Public Mainframe to access the local Mainframe as a local device located at 192.168.1.98.

FMC

NAT for Mainframe Communication

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Manual NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **INSIDE**
   Destination: **OUTSIDE**

   Translation:

   Original Source: 192.168.1.99 (Object name: **Mainframe1-Local**)
   Original Destination: 192.168.1.98 (Object name: **Mainframe2-Local**)
   Translated Source: 192.1.20.29 (Object-name: **Mainframe1-Public**)
   Translated Destination: Object (**R2-200**)

2. Click the **OK**.

Task 2

Save the Changes to the FTD

FMC

1. Save the changes to the NAT Policy by clicking on the **Save** button.

Task 3

Configure the ACP to allow Access from MainFrame-2 towards MainFrame-1. It should be the last policy in the Mandatory Section.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy – Mainframe-Communication

Name: **Mainframe-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks

Source: object (**R2-200)**
Destination: Object (**Mainframe1-Local**)

3. Click the **OK**.

Task 4

Deploy the Changes to the FTD.

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

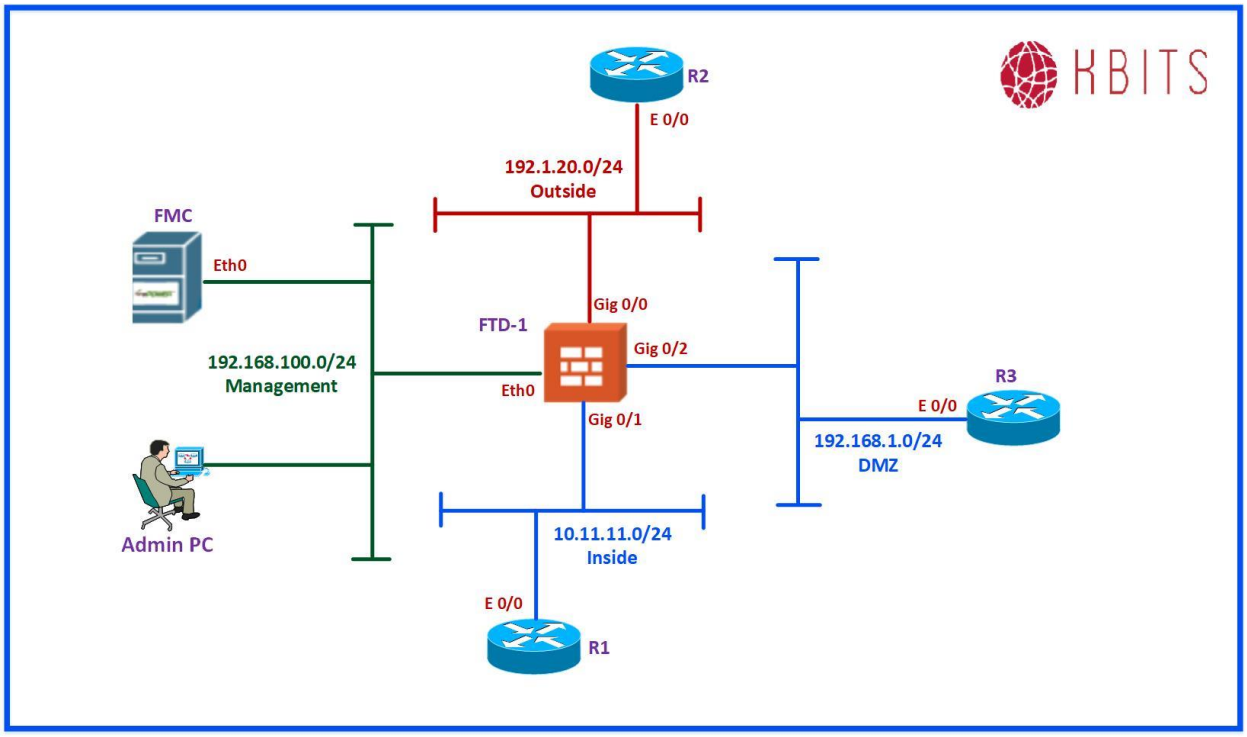
2. Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 8:
Configuring Intrusion Prevention on FTD

Module 8 – Configuring Intrusion Prevention on FTD

Lab 1 – Configuring ACP for Intrusion using the Default Policies on FTD



Lab Scenario:

- Configure a Intrusion Policy on FTD

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Modify the following ACP rules with Intrusion Prevention based on the default Intrusion policies:

- [WebServer & WebServer2 – 80 & 443] **-> Maximum**
- [MailServer & MailServer2 – 25] **-> Balanced**
- [DNSServer – 53] **-> Balanced**
- [R3 – 22 & 23] **-> Security over Connectivity**

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit -> [Policy Name] -> Edit -> Inspection**"

2. Edit the policies based on the following:

Mandatory Policy – WebServer Policies

-> Name: **WebServer-ACCESS**

Intrusion Policy:

-> Intrusion Policy: **Maximum-Detection**

-> Click the **Save**.

Mandatory Policy – WebServer2 Policies

-> Name: **WebServer2-ACCESS**

Intrusion Policy:

-> Intrusion Policy: **Maximum-Detection**

-> Click the **Save**.

Mandatory Policy – MailServer Policies

-> Name: **MailServer-ACCESS**

Intrusion Policy:

-> Intrusion Policy: **Balanced Security and Connectivity**

-> Click the **Save**.

Mandatory Policy – MailServer2 Policies

-> Name: **MailServer2-ACCESS**

Intrusion Policy:

-> Intrusion Policy: **Balanced Security and Connectivity**

-> Click the **Save**.

Mandatory Policy – DNSServer Policies

-> Name: **DNSServer-ACCESS**

Intrusion Policy:

-> Intrusion Policy: **Balanced Security and Connectivity**

-> Click the **Save**.

Mandatory Policy – R3 Policies

-> Name: **R3-ACCESS**

Intrusion Policy:

-> Intrusion Policy: **Security over Connectivity**

-> Click the **Save**.

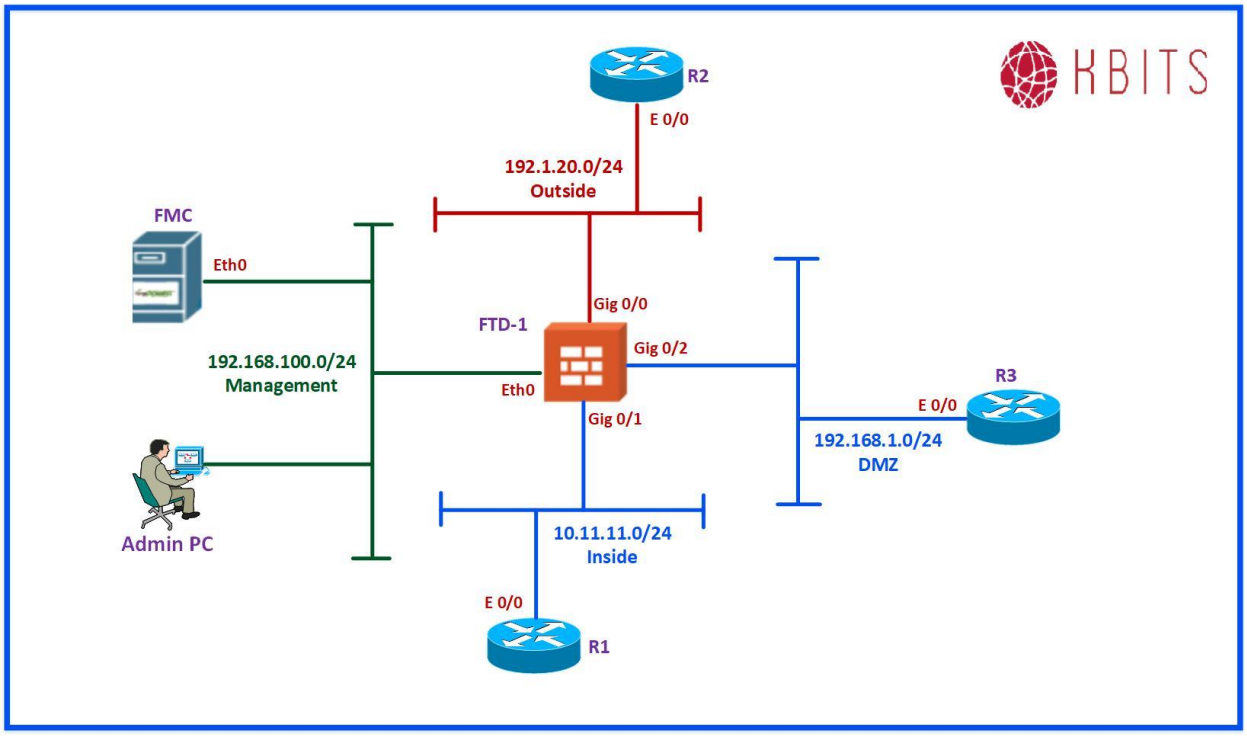
Task 4

Save the Changes to the ACP.

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

Lab 2 – Configuring a Customized Intrusion Policy



Lab Scenario:

- Enabling existing signatures.
- Changing the Actions on Signatures.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure a new Intrusion Policy based on the Balanced default policy. Give it a name of **IPS-FTD-MYPOL**.

FMC

1. Browse to "**Policies -> Access Control -> Intrusion -> Create Policy**"

   Name: **IPS-FTD-MYPOL**
   Base Policy: **Balanced Security and Connectivity**

2. Click the "**Create and Edit Policy**" button.

Task 2

Enable the following signatures in the IPS-FTD-MYPOL policy.

- Signature Name: "APP-DETECT 12P DNS request attempt"
- SignatureID: 5999

FMC

1. Browse to "**Policy Layers -> My Changes -> Rules**"

2. Search for "APP-DETECT 12P DNS request attempt" in the filter field.

3. Click the checkbox to enable the rule and set the action to "**Generate Events**".

4. Click **OK.**

5. Search for Signature ID "**5999**" in the filter field.

6. Click the checkbox next of **5999** to enable the rule and set the action to "**Drop & Generate Events**"

7. Click **OK.**

8. Click "**Policy Information**". (Left Sidebar)

9. Clock "**Commit Changes**" and click "**OK** to apply the new changes.

Task 3

If a request comes into the Firewall destined for PAT-IP object created earlier with a port number 8080, the Firewall should forward the request to a Web Server **[WebServer3]** located at 192.168.1.28 for 80.

FMC

NAT for WebServer3

1. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **DMZ**
   Destination: **OUTSIDE**

   Translation:

   Original Source: 192.168.1.28 (**WebServer3**)
   Original port: TCP/8080
   Translated Source: Object (Name: **PAT-IP**)
   Translated port: TCP/8080

2. Click the **OK**.

Task 4

Save the Changes to the NAT Policy

FMC

1. Save the changes to the NAT Policy by clicking on the **Save** button.

Task 5

Allow HTTP & HTTPS access to this new server. Apply the IPS-FTD-MYPOL Intrusion policy to WWW3. The policies should the be last ones in the Mandatory Policies.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy – MailServer-2

Name: **WebServer3-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **DMZ**

Networks:

Source: **Any-IPv4**
Destination: Object (**WebServer3**)
Destination Port#s: Objects **(HTTP & HTTPS)**

Inspection:

Intrusion Policy: **IPS-FTD-MYPOL**

3. Click the **Save**.

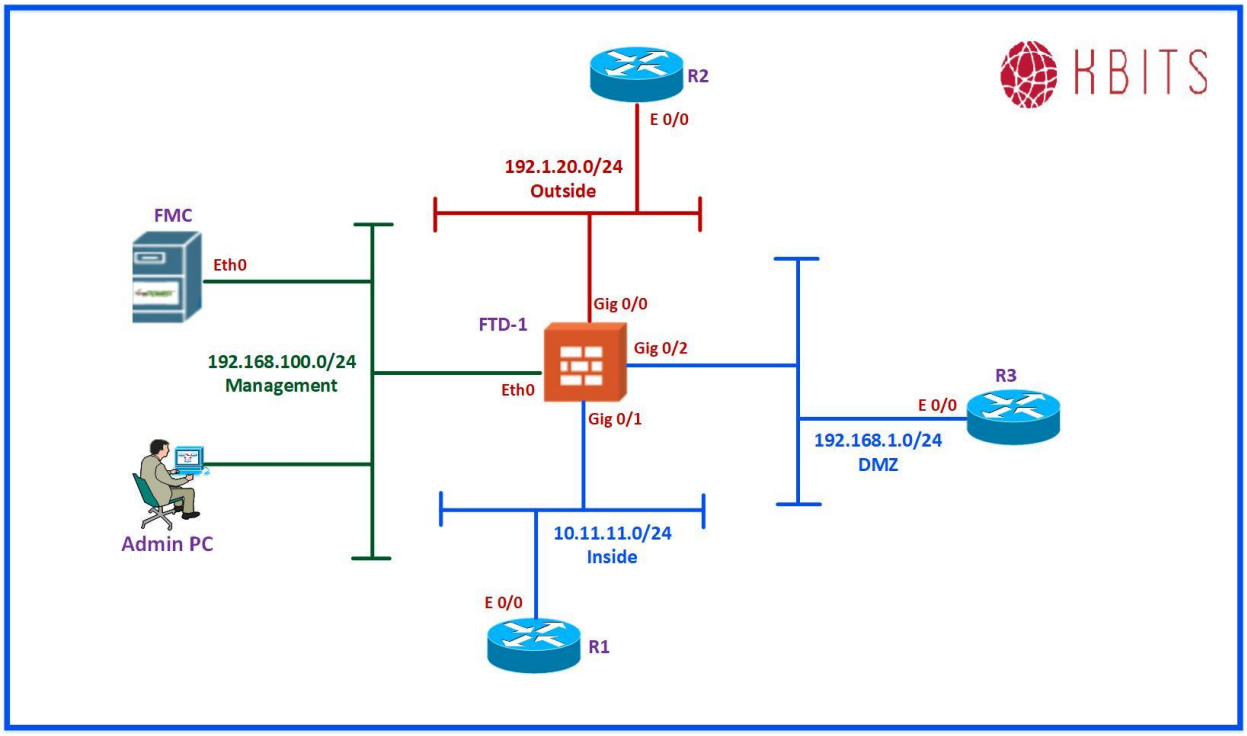
Task 6

Save the Changes to the ACP.

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

Lab 3 – Configuring an Event Filter



Lab Scenario:

- Configuring an Event filter to Bypass a signature

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

The Skype signature enabled in the previous task should not fire for 10.11.11.0/24 Network.

FMC

1. Browse to "**Policies -> Access Control -> Intrusion -> IPS-FTD-MYPOL -> Policy Layers -> My Changes -> Rules**"

2. Search for signature ID 5999" in the filter field.

3. Click the checkbox to edit the rule.

4. Click **Event Filtering -> Suppression.**

5. Set the **Suppression Type** to **Source.**

6. Type **10.11.11.0/24** to suppress signature form the 10.11.11.10/24 network. Click **OK** to create the Event Filter.

7. Click **OK.**

8. Click "**Policy Information**". (Left Sidebar)

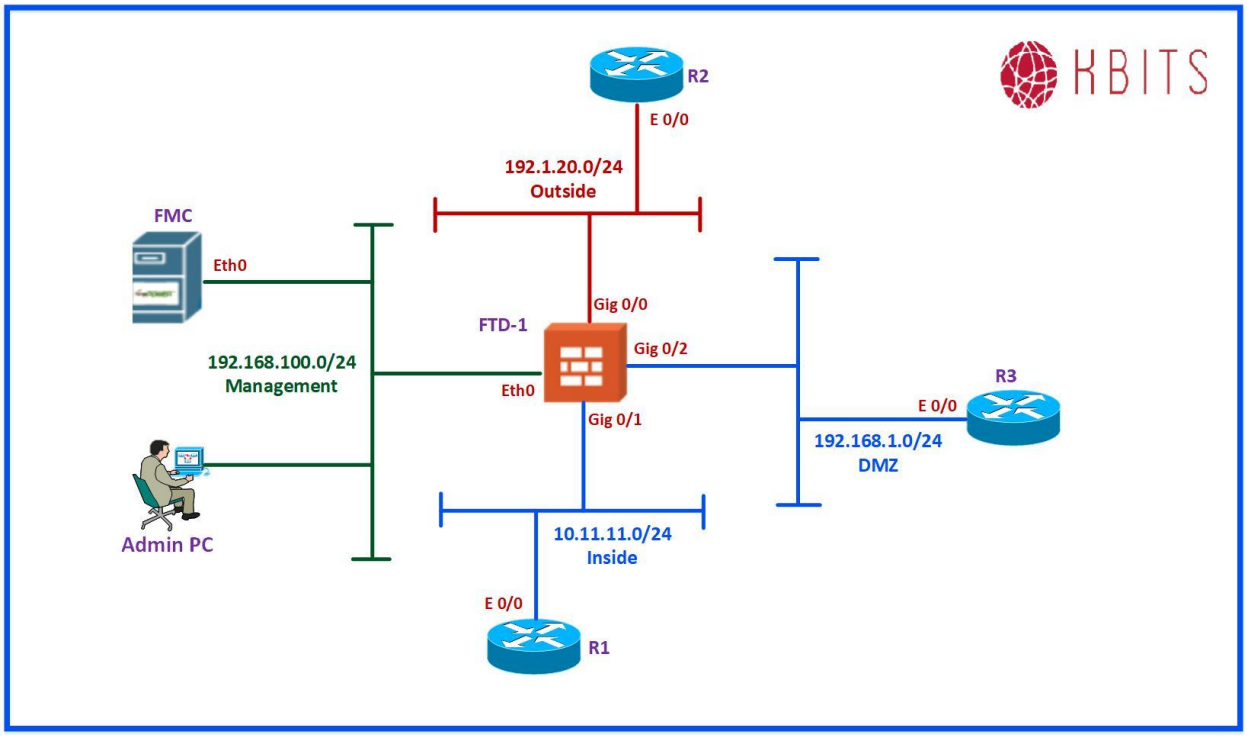
9. Clock "**Commit Changes**" and click "**OK** to apply the new changes.

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 9:
Configuring AMP on FTD

Module 9 – Configuring AMP on FTD

Lab 1 – Configuring AMP to Block Specific File Types



Lab Scenario:

- Configuring the AMP File Policy to block File Types

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure a File & Malware Policy called INSIDE-FILE-POLICY to using the following requirements:

- Download of any Executable using any protocol – Block with Reset.
- Download of any Archive using HTTP – Block with Reset.
- Upload of any Executable or Archive Files using any protocol – Block with Reset.
- Upload of any .MDB file using any protocol – Block File

FMC

1. Browse to "**Policies -> Access Control -> Malware & File Policy -> New File Policy**"

   Name: **INSIDE-FILE-POLICY**

2. Click the "**Save**" button.

3. Click the "**Add Rule**" button to create a new file policy

4. Create the Policies based on the above requirements:

   Policy # 1

   Application Protocol: **Any**
   Direction of Transfer: **Download**
   File Type Category: **Executable** (Select & Click **Add**)
   Action: **Block File** & Click the **Reset Conneciton** checkbox

   Click the "**Save**" button

   Policy # 2

   Application Protocol: **HTTP**
   Direction of Transfer: **Download**
   File Type Category: **Archive** (Select & Click **Add**)
   Action: **Block File** & Click the **Reset Conneciton** checkbox

   Click the "**Save**" button

   Policy # 3

Application Protocol: **Any**
Direction of Transfer: **Upload**
File Type Category: **Archive & Executables** (Select & Click **Add**)
Action: **Block File** & Click the **Reset Conneciton** checkbox

Click the "**Save**" button

Policy # 4

Application Protocol: **Any**
Direction of Transfer: **Upload**
File Type : **MDB** (Select & Click **Add**)
Action: **Block File** & uncheck the **Reset Conneciton** checkbox

Click the "**Save**" button

Task 2

Save the Changes to the File Policy.

FMC

1. Save the changes to the File Policy by clicking on the **Save** button.

Task 3

Configure a File & Malware Policy called DMZ-FILE-POLICY to using the following requirements:

- Upload of any Executable or Archive Files using any protocol – Block with Reset.
- Upload of System File – Block with Reset.

FMC

1. Browse to "**Policies -> Access Control -> Malware & File Policy -> New File Policy**"

   Name: **DMZ-FILE-POLICY**

2. Click the "**Save**" button.

3. Click the "**Add Rule**" button to create a new file policy

4. Create the Policies based on the above requirements:

Policy # 1

Application Protocol: **Any**
Direction of Transfer: **Upload**
File Type Category: **Archive & Executables** (Select & Click **Add**)
Action: **Block File** & Click the **Reset Conneciton** checkbox

Click the "**Save**" button

Policy # 4

Application Protocol: **Any**
Direction of Transfer: **Upload**
File Type Category: **System Fles** (Select & Click **Add**)
Action: **Block File** & Click the **Reset Conneciton** checkbox

Click the "**Save**" button

Task 4
Save the Changes to the File Policy.

FMC

1. Save the changes to the File Policy by clicking on the **Save** button.

Task 5
Configure the **INSIDE-To-ANY** ACP Policy to check Files based on the **INSIDE-FILE-POLICY**.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit -> INSIDE-To-Any -> Edit -> Inspection**"

2. Edit the policies based on the following:

File Policy:

-> File Policy: **INSIDE-FILE-POLICY**

-> Click the **Save**.

Task 6

Configure all the **MailServer-ACCESS** Policy to check the **DMZ-FILE-POLICY**.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit -> MailServer-ACCESS -> Edit -> Inspection**"

2. Edit the policies based on the following:

File Policy:

-> File Policy: **DMZ-FILE-POLICY**

-> Click the **Save**.

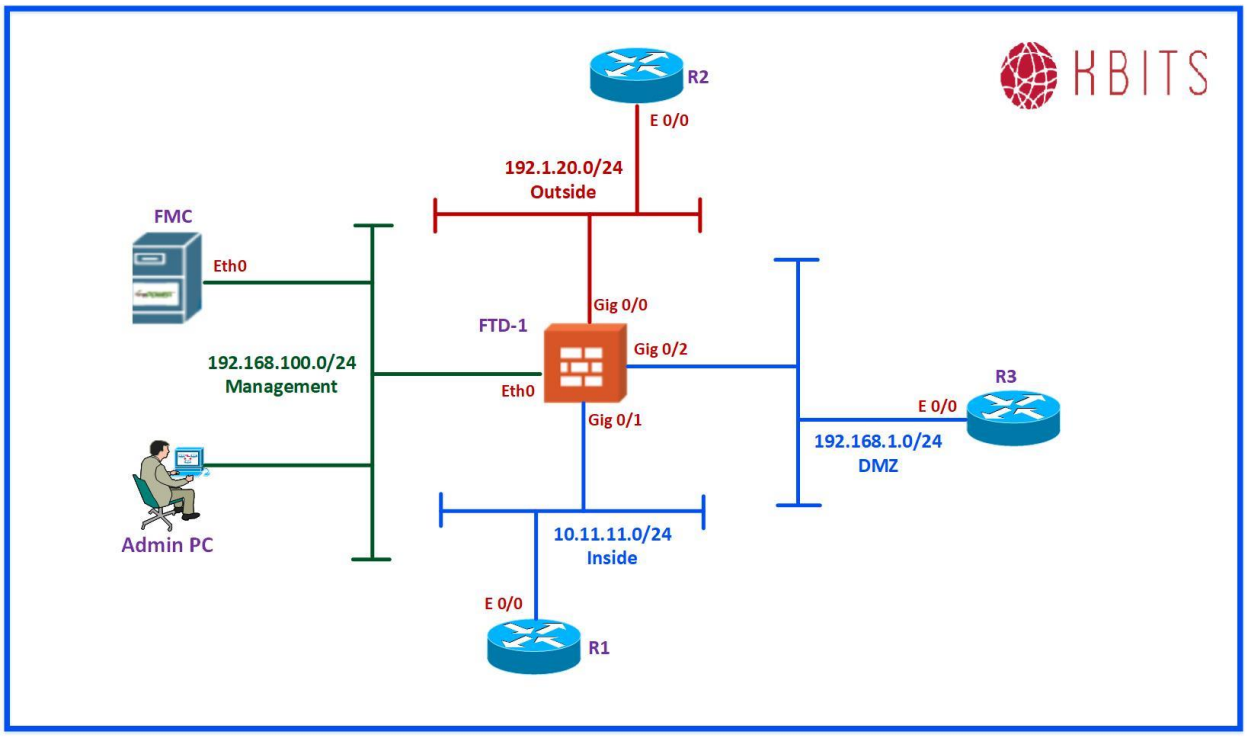
Task 7

Save the Changes to the ACP.

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

Lab 2 – Configure AMP Policies to Block Files Infected with Malware



Lab Scenario:

- Configure AMP Policies for Malware Analysis.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Re-configure INSIDE-FILE-POLICY AMP Policy to using the following requirements:

- Download of any PDF using any protocol – Block Malware with Reset.
- Download of any Office Document using any SMTP – Block Malware with Reset.

FMC

1. Browse to "**Policies -> Access Control -> Malware & File Policy -> INSIDE-FILE-POLICY**

2. Click the "**Add Rule**" button to create a new file policy

4. Create the Policies based on the above requirements:

Policy # 5

Application Protocol: **Any**
Direction of Transfer: **Download**
File Type Category: **PDF Files** (Select & Click **Add**)
Action: **Block Malware** & Click the **Reset Conneciton** checkbox

Click the "**Save**" button

Policy # 6

Application Protocol: **SMTP**
Direction of Transfer: **Download**
File Type Category: **Office Documents** (Select & Click **Add**)
Action: **Block Malware** & Click the **Reset Conneciton** checkbox

Click the "**Save**" button

Task 2

Save the Changes to the File Policy & Deploy.

FMC

1. Save the changes to the File Policy by clicking on the **Save** button.

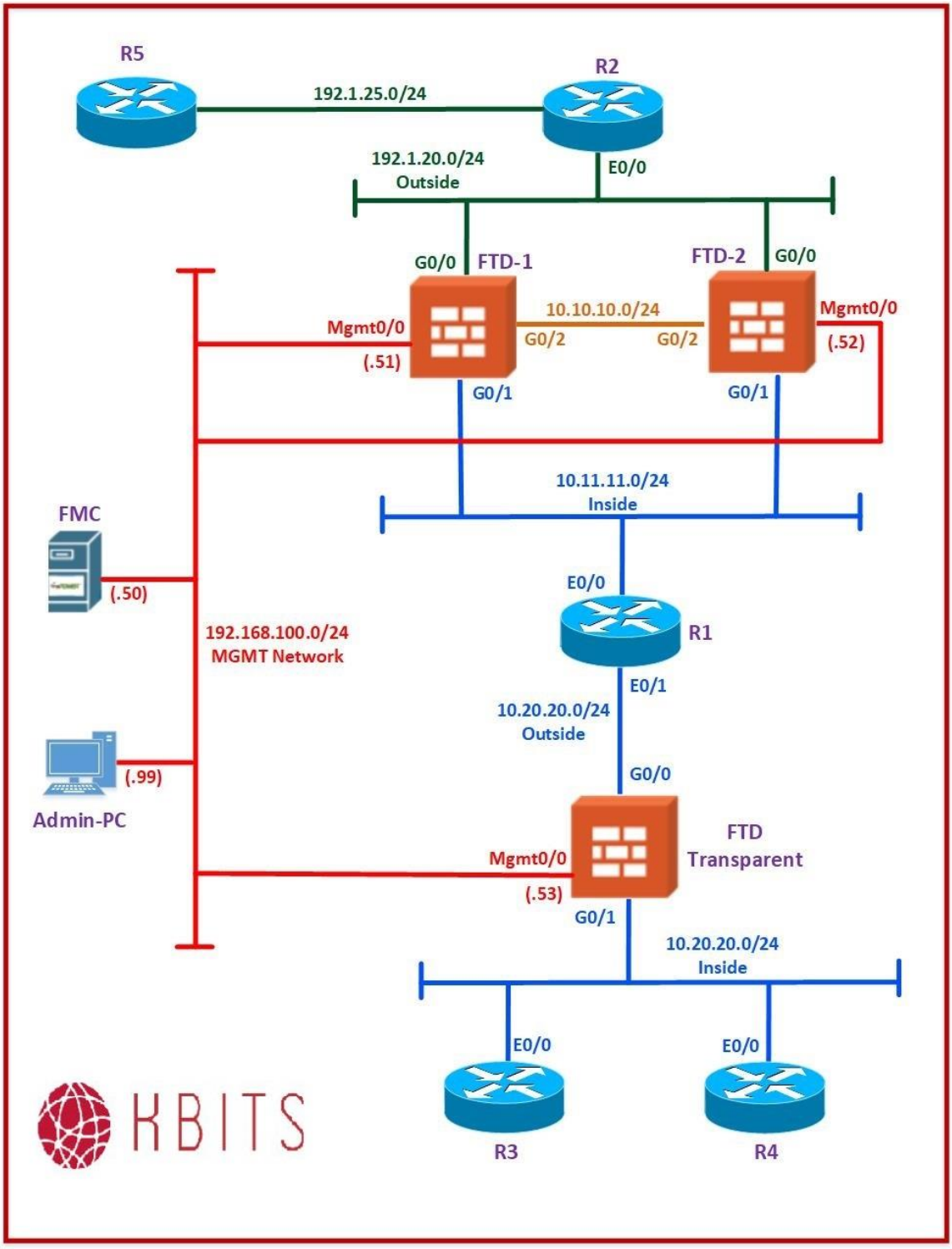
2. Click the **Deploy** button to push all the changes to the FTD.

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 10:
Configuring FTD - Advanced

Module 10 – Configuring FTD - Advanced

Lab1– Configuring FTD - Transparent Firewall Mode



Lab Scenario:

- Intialize the Internal FTD as a Transparent Firewall.
- R2 is acting as the Edge Router and R5 as the Internet. R1, R3 & R4 are internal routers connected on the 10.20.20.0/24 Segment separated by the Transparent Firewall.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure OSPF based on the following:
  - Configure OSPF in Area 0 on R1, R3 & R4.
  - Advertise the Loopback networks on each router.

R1	**R3**
Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Int E 0/1 Ip add 10.20.20.1 255.255.255.0 No shut ! Router ospf 1 Network 10.0.0.0 0.255.255.255 area 0	Int Loopback0 Ip add 10.3.3.3 255.255.255.0 No shut ! Int E 0/0 Ip add 10.20.20.3 255.255.255.0 No shut ! router ospf 1 Network 10.0.0.0 0.255.255.255 area 0
R4	
Int Loopback0 Ip add 10.4.4.4 255.255.255.0 No shut ! Int E 0/0 Ip add 10.20.20.4 255.255.255.0 No shut ! router ospf 1 Network 10.0.0.0 0.255.255.255 area 0	

Lab Tasks:

Task 1

Configure the Firepower Management Center [FMC] IP as 192.168.100.50/24 with a default gateway of 192.168.100.254.

FMC CLI

Sudo configure-network

Do you wish to Configure iPv4? [y or n] **y**

Management IP Address>?[] **192.168.100.50**

Management netmask?[] **255.255.255.0**

Management default gateway? [] **192.168.100.254**

Management IP address? **192.168.100.50**

Management netmask? **255.255.255.0**

Management default gateway?..... **192.168.100.254**

Are these settings correct? (y or n**) y**

Do you wish to configure IPv6 (y or n) **n**

Wait for it to complete the configuration.

Task 2

Initialize the Internal FTD (FTD Transparent) based on the following:

- Admin Password: Kbits@123
- IP Address/Subnet Mask: 192.168.100.53/24
- Default Gateway: 192.168.100.254
- FQDN: FTD3.kbits.live
- Firewall Mode: Transparent

FTD CLI

1. Login using the default creds (admin/Admin123)

2. Accept the EULA

3. Change the default password

4. Configure the IP Address for FTD Management Interface

IPv4 Address: **192.168.100.53**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.100.254**
Hostname: **FTD3.Kbits.live**
DNS: None

5. Configure the Firewall Mode (Routed/Transparent) **Transparent**

6. Verifying the connectivity

ping system 192.168.100.50

Task 3

Log into the FMC using a browser. The default username is Admin with a password of Admin123.

Management PC

Initializing Page

Change Password:

Password: Kbits@123
Confirm Password: Kbits@123

Network Settings:

IP Address: 192.168.100.50
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.100.254
Hostname: **FMC**
Domain: **Kbits.live**
DNS Server: 8.8.8.8

Time Settings:

Clock: Via **NTP**

Change the Timezone: **Asia/Dubai**

End User Agreement:

Click the checkbox to Accept it

Click "**Apply**" to accept the Changes:

Note: It takes several minutes for it to initialize the FMC.

Task 4

Ensure the FMC is the NTP Server & Initialize the Evaulation License.

Management PC

Licensing

System -> Configuration -> Time Synchronization

-> Serve Time via NTP: **Enabled**

-> Click Save

System -> Licensing -> Smart Licensing -> Evaluation Mode

-> Activate Evaluation Period

Task 5

Configure the relationship between the FTD & FMC.

FTD-Transparent CLI

configure manager add 192.168.100.50 Kbits123

Task 6

Register the FTD. Create a Default Policy that will Block all the Traffic.

Management PC

Registration

Devices -> Device Management -> Add Device

Address: 192.168.100.53

Display Name: FTD3
Registration Key: Kbits123
Default Policy: FTD-T-ACP (Block All traffic)

Enable the licenses and click **Add**

Task 7

Assign the Interfaces to the Zones based on the following table:

Interface	Name	Zone
G 0/0	Outside	OUTSIDE-T
G 0/1	Inside	INSIDE

FMC

1. Browse to "**Devices -> Device Management -> FTD3 -> Edit -> Interfaces**"

2. Configure the Interfaces using the following:

Interface: Gig0/0
Name: Outside
Enabled: Check
Zone: OUTSIDE

Interface: Gig0/1
Name: Inside
Enabled: Check
Zone: INSIDE

Task 8

Create a Bridge Group Interface and Assign it an IP Address of 10.20.20.10/24.

FMC

1. Click **"Add Interfaces"** drop-down and select **"Bridge Group Interface".**

2. Configure the BVI using the following:

Interface Name: BVI-10
Bridge Group: 10

Interfaces: Gig 0/0 & Gig0/1

3. Click **OK** and **Save.**

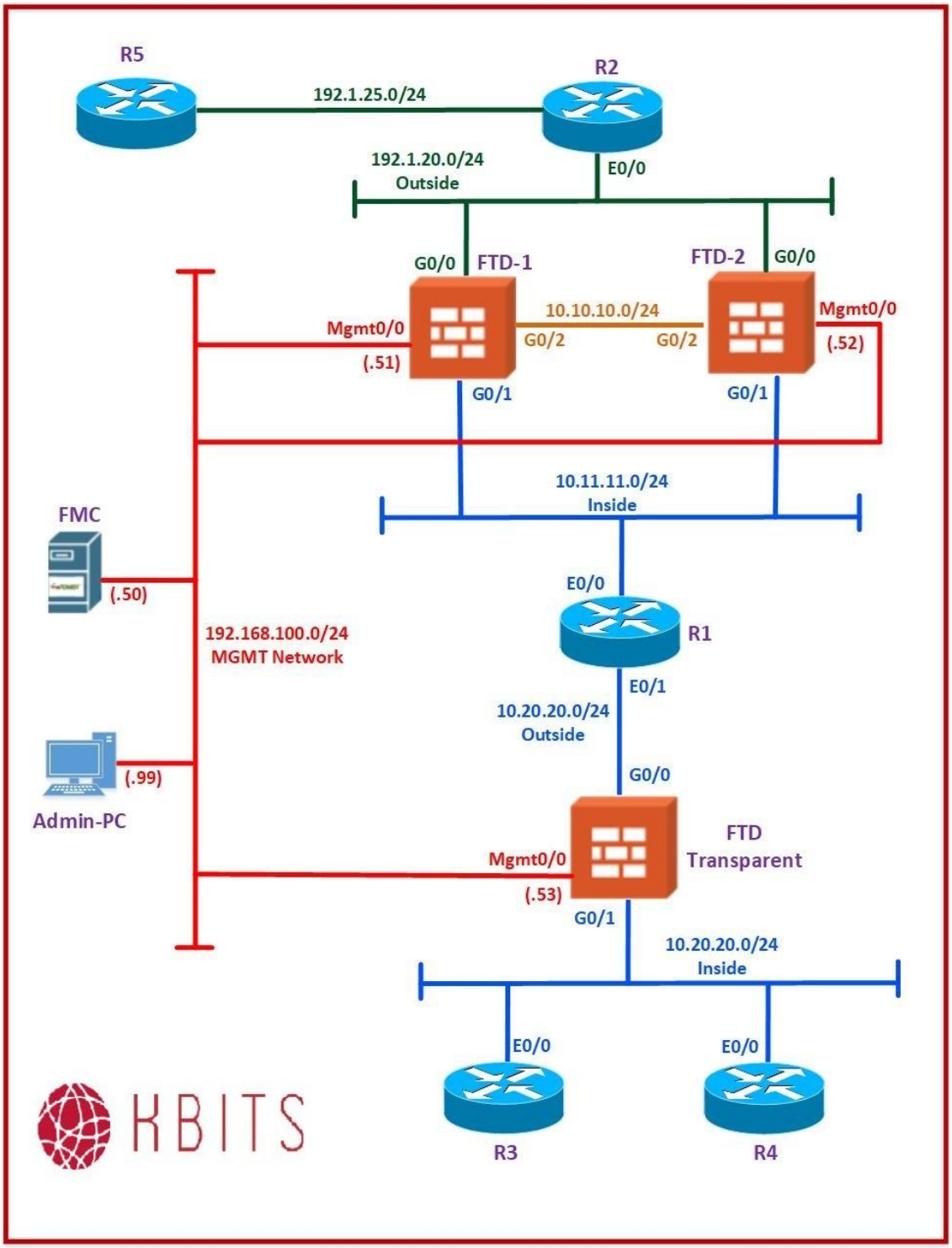
Task 10

Deploy the Changes to FTD3. After the deployment is successful, FTD should be reachable from R1, R3 & R4.

FMC

1. Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

Lab 2 – Configuring Access Policies on a Transparent Firewall



Lab Scenario:

- Configure Access Policies to allow Routing traffic thru the Transparent Firewall.
- Configure Access Policies to allow End-User traffic thru the Transparent firewall.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Allow the following access from OUTSID-T to INSIDE-T zones. These flows should be checked in the mandatory policy.

- OSPF traffic from R1 Towards R3 & R4 from OUTSIDE-T towards INSIDE-T.
- Telnet, SSH & ICMP traffic from R1 towards R3 & R4.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-1-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#1

Name: **OSPF**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE-T**
Destination Zone: **INSIDE-T**

Networks

Source: 10.20.20.1 (Object name: **R1**)
Destination: 10.20.20.3(Object Name: **R3**)
10.20.20.3(Object Name: **R4**)
Destination Ports: protocol 89 (Object Name: **OSPF-89**)

Policy#2

Name: **R1-To-R3-R4**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE-T**
Destination Zone: **INSIDE-T**

Networks

Source: **R1**
Destination: Objects (**R3 & R4**)
Destination Ports: Objects **(Telnet & SSH)**
ICMP (Object Name: **PING**)

Task 2

Allow Full access from the INSIDE-T zone towards the OUTSID-T Zone in the Default Policy.

FMC

1. Browse to "Policies -> Access Control -> Access Control -> FTD-T-ACP -> Edit"

2. Configure the policies based on the following:

Default Policy

Policy#1

Name: **INSIDE-To-ANY**
Action: **Allow**

Zones:

Source Zone: **INSIDE-T**
Destination Zone: **OUTSIDE-T**

Task 3

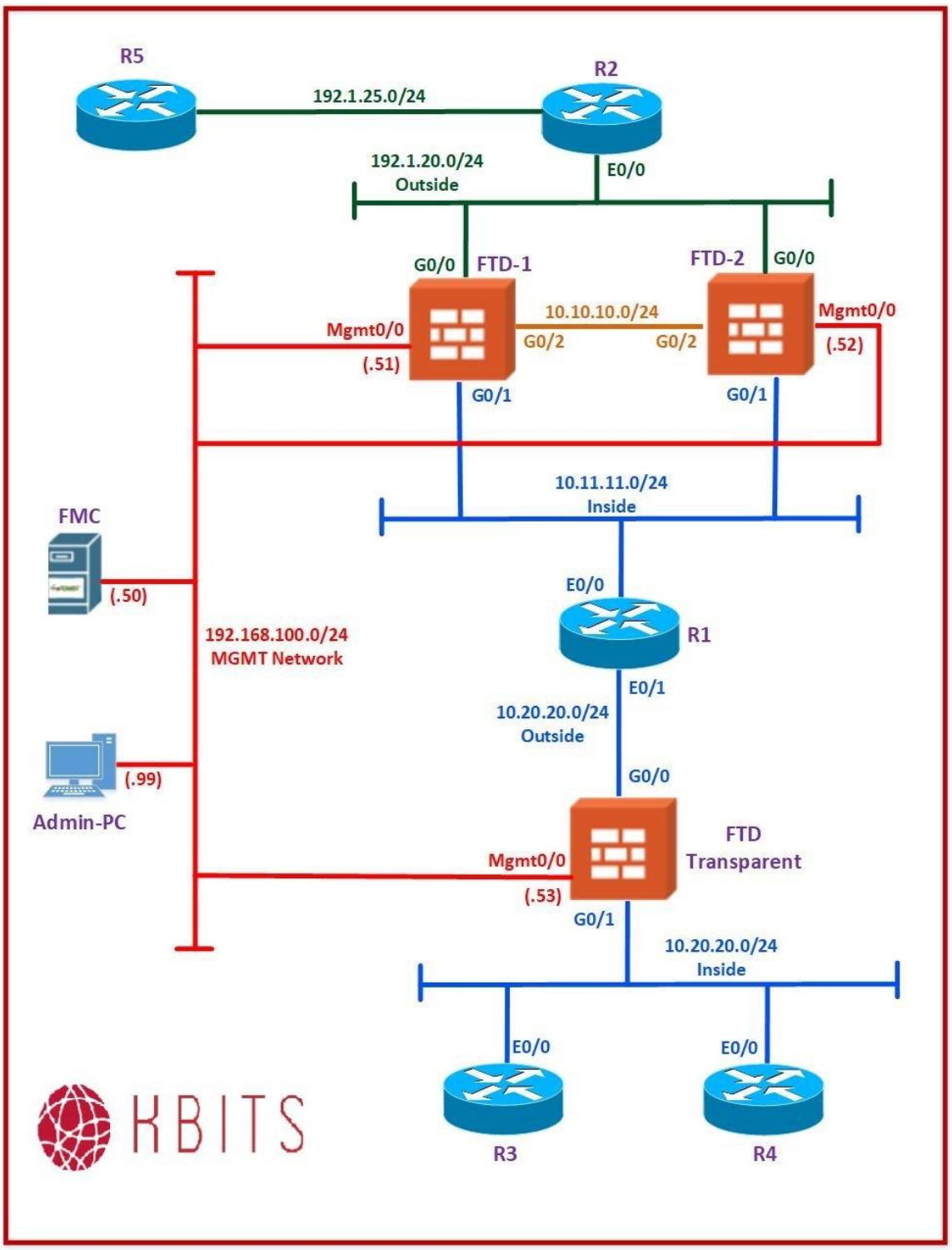
Deploy the Changes to the FTD

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

2. Click the **"Deploy"** button to apply the changes to the FTD3. Wait for the changes to be applied successfully

Lab 3 – Configuring FTP High Availability - Failover



Lab Scenario:

- Configure High Availability (Failover) between FTD-1 & FTD-2.
- R2 is acting as the Edge Router and R5 as the Internet.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure OSPF based on the following:
  - Configure OSPF in Area 0 on R1, R3 & R4.
  - Advertise the Loopback networks on each router.

R2	**R5**
Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int Loopback 199 Ip add 199.1.1.1 255.255.255.0 ! Int E 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Int E 0/1 Ip add 192.1.25.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.25.5	Int Loopback0 Ip add 200.1.1.1 255.255.255.0 No shut ! Int E 0/0 Ip add 192.1.25.5 255.255.255.0 No shut ! ip route 192.1.20.0 255.255.255.0 192.1.25.2

Lab Tasks:

Task 1

Initialize FTD-1 from the CLI based on the following

- Username/Password: admin/Admin123
- Network Configuration:
  - Interface IP:192.168.100.51
  - Subnet Mask: /24
  - Default-Gateway: 192.168.100.254
- Mode: Routed
- FMC/Manager: 192.168.100.50
- Secret Key: cisco123

Initialize FTD-2 from the CLI based on the following

- Username/Password: admin/Admin123
- Network Configuration:
  - Interface IP:192.168.100.52
  - Subnet Mask: /24
  - Default-Gateway: 192.168.100.254
- Mode: Routed
- FMC/Manager: 192.168.100.50
- Secret Key: cisco123

FTD-1

Initializing FTD-1

1. Login using the default creds (admin/Admin123)

2. Accept the EULA

3. Change the default password to Kbits@123.

4. Configure the IP Address for FTD Management Interface

   IPv4 Address: **192.168.100.51**
   Subnet Mask: **255.255.255.0**
   Default Gateway: **192.168.100.254**
   Hostname: **FTD-1**
   Domain: **kbits.live**

5. Configure the Firewall Mode (Routed/Transparent): **Routed**

Configure the relationship with FMC

configure manager add 192.168.100.50 cisco123

Verifying the connectivity

ping system 192.168.100.50

FTD-2

Initializing FTD-2

1. Login using the default creds (admin/Admin123)

2. Accept the EULA

3. Change the default password to Kbits@123.

4. Configure the IP Address for FTD Management Interface

   IPv4 Address: **192.168.100.52**
   Subnet Mask: **255.255.255.0**
   Default Gateway: **192.168.100.254**
   Hostname: **FTD-1**
   Domain: **kbits.live**

5. Configure the Firewall Mode (Routed/Transparent): **Routed**

Configure the relationship with FMC

configure manager add 192.168.100.50 cisco123

Verifying the connectivity

ping system 192.168.100.50

Task 2

Configure the relationship between FMC & FTD by adding FTDs in FMC using the following information:

Add FTD-1 to FMC using the following:

- Host: 192.168.100.51
- Name: FTD-1
- Registration Key: cisco123
- Configure the Default Policy using a Name of FTD-ACP with Block All
- Enable all the Licenses and Add the Device

Add FTD-2 to FMC using the following:

- Host: 192.168.100.52
- Name: FTD-1

- Registration Key: cisco123
- Configure the Default Policy using a Name of FTD-ACP with Block All
- Enable all the Licenses and Add the Device

FMC

Adding FTD-1 to FMC

1. Browse to https://192.168.100.50 and login using the default creds (admin/Admin123)

2. Browse to "Devices -> Device Management -> Add Device"

3. Configure the Device using the following:

   Address: 192.168.100.51
   Display Name: FTD-1
   Registration Key: cisco123
   Default Policy : FTD-ACP (Block All traffic)
   Enable the licenses and click **Add**

Adding FTD-2 to FMC

1. Browse to "Devices -> Device Management -> Add Device"

2. Configure the Device using the following:

   Address: 192.168.100.52
   Display Name: FTD-2
   Registration Key: cisco123
   Default Policy: FTD-ACP (Block All traffic)
   Enable the licenses and click **Add**

Task 3
Create a Management group and add FTD's using the following information:

- Create a management group called Perimeter-FW
- Add FTD-1 & FTD-2 to the new group

FMC

Creating a Device Management Group

1. Browse to "Devices -> Device Management -> Add Group"

2. Configure the Group using the following:

Name: Perimeter-FW
Devices : FTD-1 & FTD-2
Click **Add**

Task 4
Configure High Availability & Add FTDs using the following information:

- Configure High Availability between FTD-1 & FTD-2 in a High Availability group called FTD-HA
- Configure FTD-1 as the Primary Device & FTD-2 as the Secondary Device
- Use the following High Availability parameters:
  - High Availability Link: Gig0/4
  - Stateful Link: Gig0/4 (Same link as High Availability Link)
  - Name: Failover
  - Primary IP: 10.10.10.1
  - Secondary IP: 10.10.10.2
  - Subnet Mask: 255.255.255.0
  - IPSec Encryption Enabled
  - Key: cisco123

FMC

Creating a High Availability Peering

1. Browse to "Devices -> Device Management -> Add High Availability"

2. Configure using the following:

Name: FTD-HA
Device Type: Firepower Threat Defense

Primary: FTD-1
Secondary: FTD-2

High Availability Link: Gig0/4 - Use same link for Stateful Link
Name: Failover
Primary IP: 10.10.10.1
Secondary IP: 10.10.10.2
Subnet Mask: 255.255.255.0

IPSec Encryption Enabled
Key: cisco123

3. **Add** the High Availability Settings.

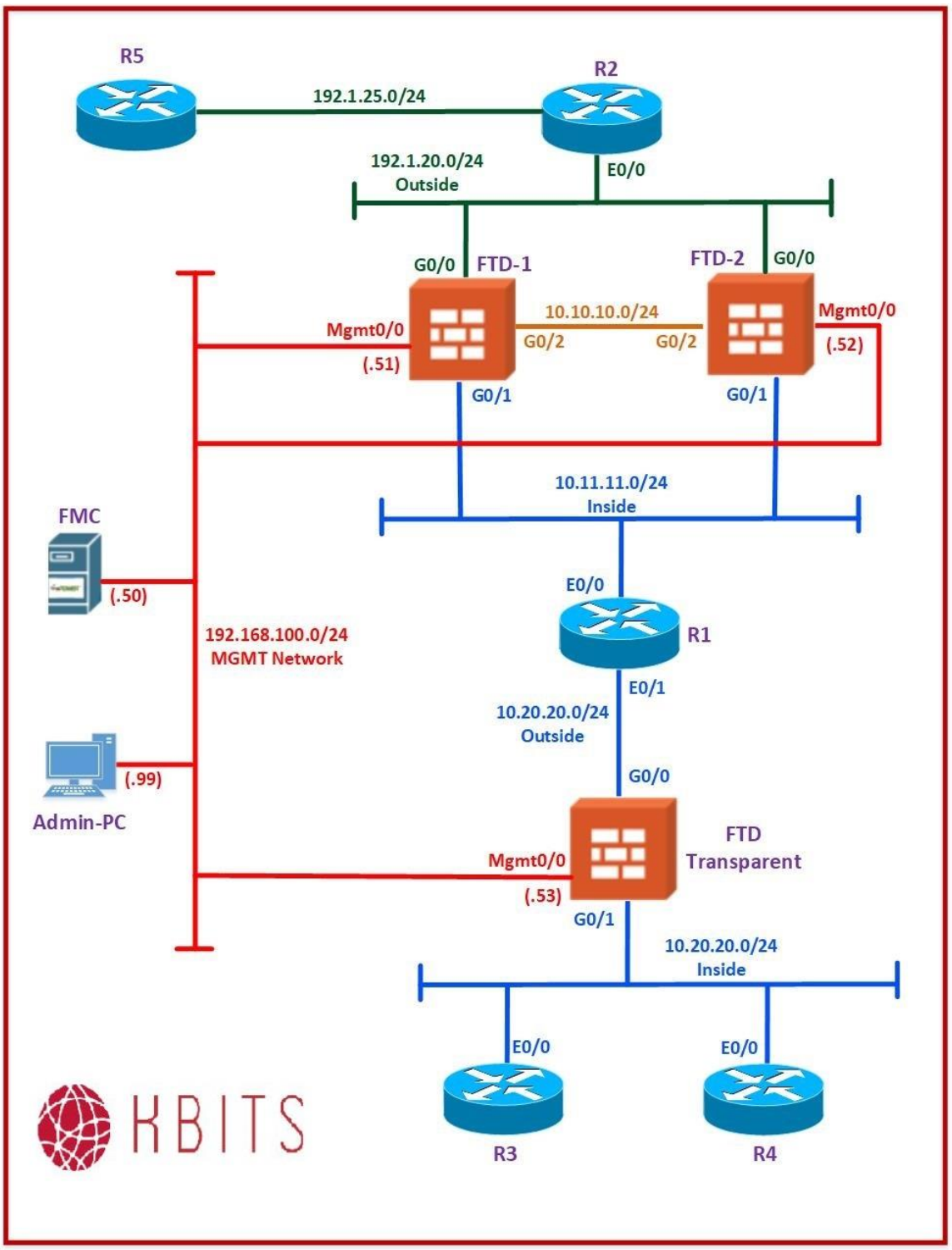
Task 5

Deploy the Changes to FTD-HA.

FMC

1. Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

Lab 4 – Configuring FTP High Availability Logical Device



Lab Scenario:

- Configure the FTD-HA Interfaces, Routing and NAT.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the FTD-HA interfaces based on the following:

Interface	IP Address(A)	IP Address (S)	Name	Zone
G 0/0	192.1.20.10/24	192.1.20.11/24	Outside	OUTSIDE
G 0/1	10.11.11.10/24	10.11.11.11/24	Inside	INSIDE

FMC

Creating the Active Interfaces and their Parameters

1. Browse to "Devices -> Device Management -> FTD-HA -> Edit -> Interfaces"

2. Configure the Interfaces using the following:

Interface: **Gig0/0**
Name: **Outside**
Enabled: **Check**
Zone: **OUTSIDE**
IP Address: **192.1.20.10/24**

Interface: **Gig0/1**
Name: **Inside**
Enabled: **Check**
Zone: **INSIDE**
IP Address: **10.11.11.10/24**

Creating the Standby Interface IPs

1. Browse to "Devices -> Device Management -> FTD-HA -> Edit -> High Availability"

2. Configure the Standby Interface IP's Under the "**Monitored Interface**" Section using the following:

Interface Name: **Outside**
IP Address: **192.1.20.11/24**

Interface Name: **Inside**
IP Address: **10.11.11.11/24**

Task 2

Configure Routing on the FTD-HA Device

- Configure OSPF in Process ID 1 to communicate on the Inside interface.
- Configure a Static Default Route on the FTD-HA R2.

FMC

Creating the Active Interfaces and their Parameters

1. Browse to "Devices -> Device Management -> FTD-HA -> Edit -> Routing"

2. Under OSPF, click Process 1. Select the Internal Role.

3. Under Area, Click **"Add".**

4. Configure using the following:

   OSPF Process: **1**
   Area ID: **0**
   Area Type: **Normal**
   Add & select the following network: 192.1.20.0/24 (Object Name: Outside)

   Click **Save**

5. Configure the Static Route

   Type: **IPv4**
   Interface: **Outside**
   Add & select the following network: object (**any-ipv4**)
   Gateway: 192.1.20.2 (Object Name: **R2**)

   Click **Save**

6. **Save** the Routing Configuration and **Deploy**.

Task 3

Configuring NAT for Internal Users such FTD-HA translates all traffic coming from Inside Subnets (10.0.0.0/8) towards the Outside as 192.1.20.5.

FMC

NAT for Internal Users

1. Browse to "Devices -> NAT -> New Policy -> Threat Defence NAT"

2. Configure using the following:

   Name: **FTD-HA-NAT**
   Device: **FTD-HA**

3. Click **"Add Rule"** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Dynamic**

   Interface Objects:

   Source: **INSIDE**
   Destination: **OUTSIDE**

   Translation:

   Original Source: 10.0.0.0/0 (Object Name: **INS-NETS**)
   Translated Packet: 192.1.20.5 (Object Name: **PAT-IP**)

4. Click the **OK**.

Task 4

Configuring Static NAT based on the using the following:

- R1 (10.11.11.1) should be seen on the outside as 192.1.20.21
- R3 (10.20.20.3) should be seen on the outside as 192.1.20.23
- R3 (10.20.20.4) should be seen on the outside as 192.1.20.24
- WebServer (10.20.20.25) should be seen on the outside as 192.1.20.25.

FMC

NAT for R1

1. Click **“Add Rule”** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

   Interface Objects:

   Source : **INSIDE**
   Destination : **OUTSIDE**

   Translation:

   Original Source: 10.11.11.1 (Object Name: **R1**)
   Translated Source: 192.1.20.21 (Object Name: **R1-X**)

2. Click the **OK**.

NAT for R3

1. Click **“Add Rule”** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

   Interface Objects:

   Source: **INSIDE**
   Destination: **OUTSIDE**

   Translation:

   Original Source: 10.20.20.3 (Object Name: **R3**)
   Translated Source: 192.1.20.23 (Object Name: **R3-X**)

2. Click the **OK**.

NAT for R4

1. Click **“Add Rule”** and create the rule based on the following:

   NAT Rule: **Auto NAT Rule**
   Type: **Static**

   Interface Objects:

Source : **INSIDE**
Destination : **OUTSIDE**

Translation:

Original Source: 10.20.20.4 (Object Name: **R4**)
Translated Source: 192.1.20.24 (Object Name: **R4-X**)

2. Click the **OK**.

NAT for WebServer

1. Click **"Add Rule"** and create the rule based on the following:

NAT Rule: **Auto NAT Rule**
Type: **Static**

Interface Objects:

Source : **INSIDE**
Destination : **OUTSIDE**

Translation:

Original Source: 10.20.20.25 (Object Name: **WebServer**)
Translated Source: 192.1.20.25 (Object Name: **WebServer-X**)

2. Click the **OK** and **Save** to save the NAT Policy.

Task 5

Configure the ACP to allow the following traffic.

- All Inside networks should be able to go out for all traffic. This should be a Default Policy.
- Allow Telnet and SSH Access to the R1, R3 & R4. It should be a Mandatory policy.
- Allow HTTP & HTTPS access to the Web Server (10.20.20.25) from the Outside. This should be a Mandatory Policy.

FMC

1. Browse to "**Policies -> Access Control -> Access Control -> FTD-ACP -> Edit**"

2. Configure the policies based on the following:

Mandatory Policy

Policy#1

Name: **WebServer-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **INSIDE**

Networks

Source: **Any-IPv4**
Destination: Object (**WebServer**)
Destination Port#s: Objects **(HTTP & HTTPs)**

Policy#2

Name: **Router-ACCESS**
Action: **Allow**

Zones:

Source Zone: **OUTSIDE**
Destination Zone: **INSIDE**

Networks

Source: **Any-IPv4**
Destination: Objects (**R1,R3,R4**)
Destination Port#s: Objects **(Telnet,SSH & PING)**

Default Policy

Policy#1

Name: **INSIDE-To-ANY**
Action: **Allow**

Zones:

Source Zone: **INSIDE**

Destination Zone: **OUTSIDE**

Networks

Source: Objects (**INSIDE-NETS**)
Destination: **Any-IPv4**

Task 6
Deploy the Changes to the FTD

FMC

1. Save the changes to the ACP by clicking on the **Save** button.

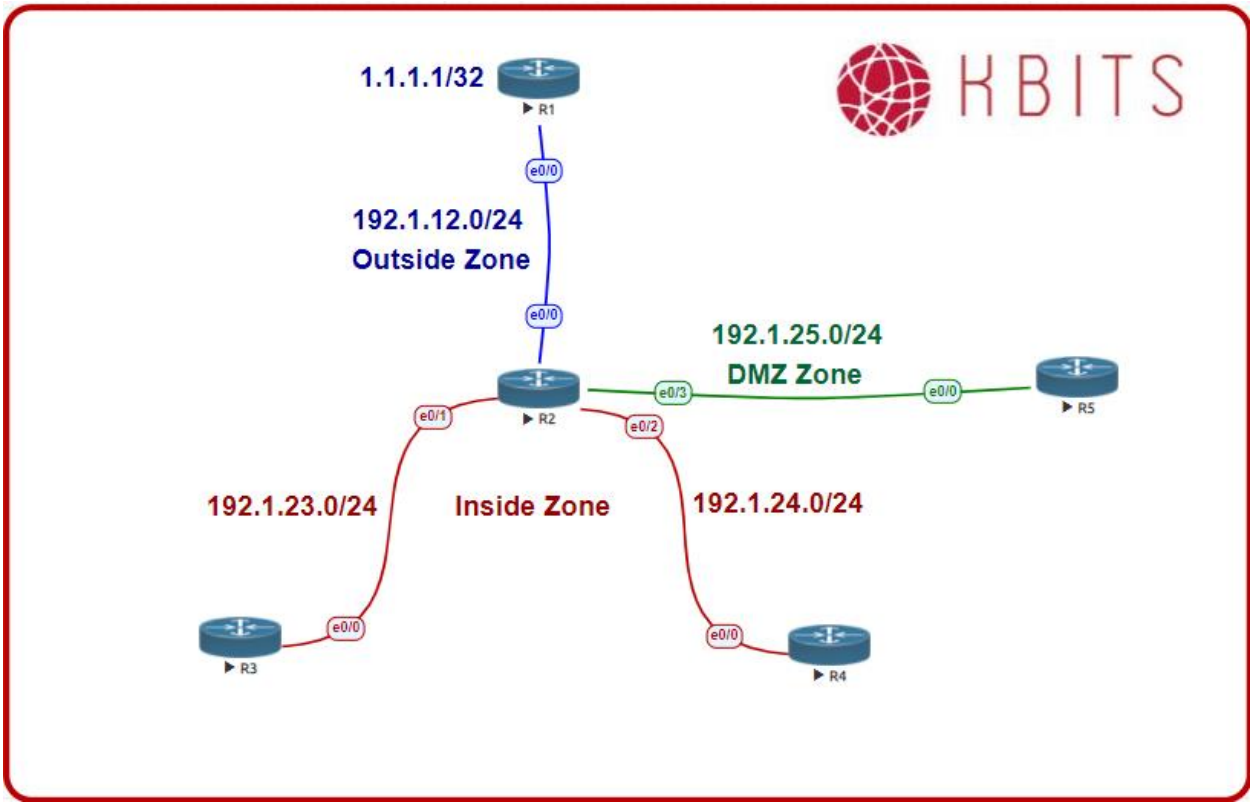
2. Click the **"Deploy"** button to apply the changes to the FTD. Wait for the changes to be applied successfully

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 11:
Configuring Zone-based Firewalls

Module 11 – Configuring Zone-based Firewalls

Lab1– Configuring Zone-based Firewall on a Router



Lab Scenario:

- Configure R2 as a Zone-Based Firewall to control traffic into the Internal and DMZ Segment.
- R1 is acting as the Internet. 192.1.23.0/24 is the Internal Network and the 192.1.24.0/24 is the DMZ network.

Initial Setup:

- Configure the IP Addresses based on the Diagram.
- Configure the 4.2.2.2/24 address on R1.
- Configure the following static and default routes:

- Static routes on R1 for the 192.1.23.0/24 and 192.1.24.0/24 networks pointing to R2 as the Next-hop.
- Default routes on R3 & R4 pointing towards R2.
- Default route on R2 point towards R1.

R1	**R2**
Int loopback 0 Ip add 4.2.2.2 255.255.255.0 ! Int E 0/0 Ip add 192.1.12.1 255.255.255.0 No shut Ip route 192.1.23.0 255.255.255.0 192.1.12.2 Ip route 192.1.24.0 255.255.255.0 192.1.12.2	Int E 0/0 Ip add 192.1.12.2 255.255.255.0 No shut ! Int E 0/1 Ip address 192.1.23.2 255.255.255.0 No shut ! Int E 0/2 Ip address 192.1.24.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.12.1
R3	**R4**
Int E 0/0 Ip address 192.1.23.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.23.2	Int E 0/0 Ip address 192.1.24.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.24.2

Lab Tasks:

Task 1

Configure the zones and apply them based on the following on R2:

- LOCAL : Interface E 0/1
- DMZ : Interface E 0/2
- INTERNET : Interface E 0/0

R2

```
Zone security LOCAL
Zone security DMZ
Zone security INTERNET
!
Interface E 0/0
 Zone-member security INTERNET
!
Interface E 0/1
Zone-member security LOCAL
!
Interface E 0/2
Zone-member security DMZ
```

Task 2

Allow the Following protocols to go from the LOCAL to the INTERNET zone:

- HTTP
- HTTPS
- DNS
- FTP
- TFTP
- SMTP
- ICMP
- RDP

R2

```
ip port-map user-RDP port tcp 3389
!
Class-map type inspect match-any CM-L-I
 Match protocol HTTP
 Match protocol HTTPS
 Match protocol DNS
 Match protocol FTP
 Match protocol TFTP
```

```
 Match protocol SMTP
 Match protocol ICMP
 Match protocol user-RDP
!
policy-map type inspect PM-L-I
 class type inspect CM-L-I
   inspect
!
Zone-pair security L-I source LOCAL destination INTERNET
 Service-policy type inspect PM-L-I
```

Task 3

Allow the Following protocols to go from the LOCAL to the DMZ zone:

- HTTP
- HTTPS
- DNS
- SMTP
- ICMP
- TELNET

R2

```
Class-map type inspect match-any CM-L-D
 Match protocol HTTP
 Match protocol HTTPS
 Match protocol DNS
 Match protocol SMTP
 Match protocol ICMP
 Match protocol TELNET
!
policy-map type inspect PM-L-D
 class type inspect CM-L-D
   inspect
!
Zone-pair security L-D source LOCAL destination DMZ
 Service-policy type inspect PM-L-D
```

Task 4

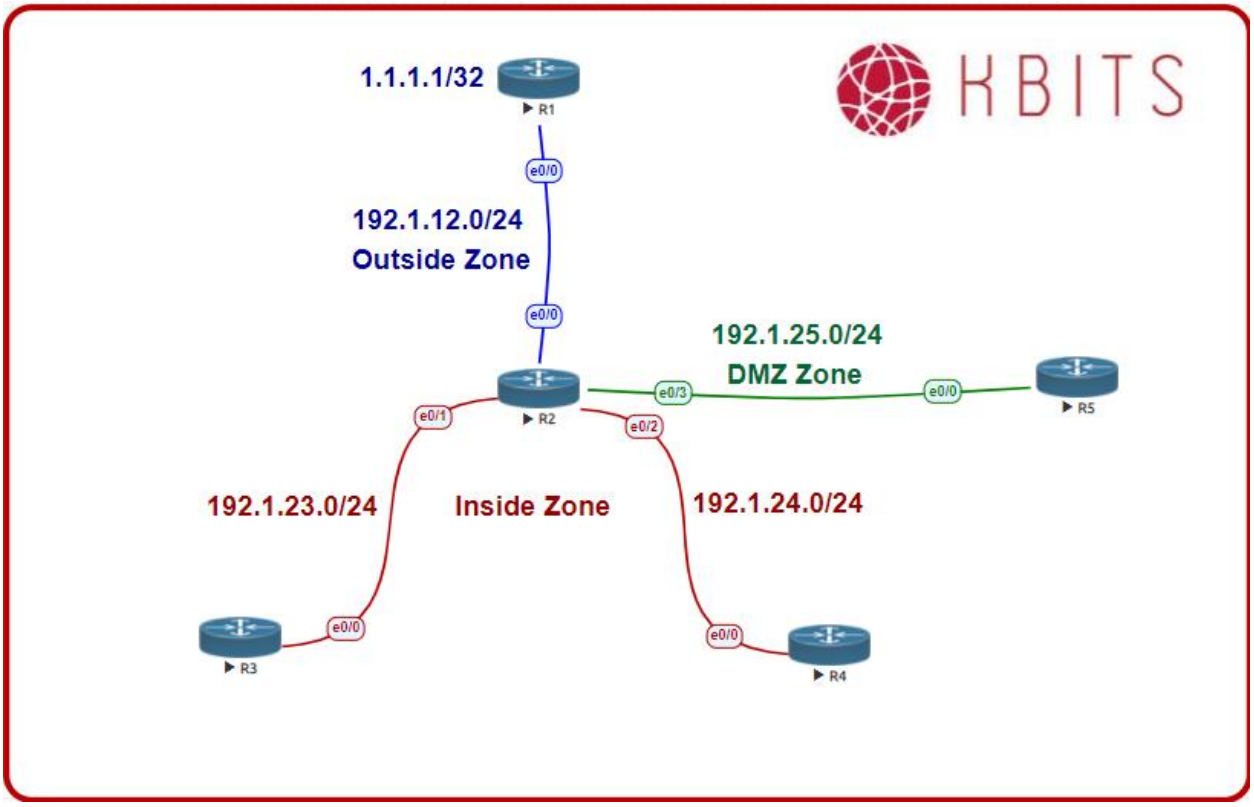
Allow the Following protocols to go from the INTERNET to the DMZ zone:

- Allow SMTP Access to a server 192.1.24.51 located on the DMZ zone
- Allow Telnet Access to a router 192.1.24.4 located on the DMZ zone. Only allow R1 to make this connection.

R2

```
Access-list 142 permit ip any host 192.1.24.51
Access-list 143 permit ip host 192.1.12.1 host 192.1.24.4
!
Class-map type inspect match-all CM-I-D-MAIL
  Access-group 142
  Match protocol SMTP
!
Class-map type inspect match-all CM-I-D-TELNET
  Access-group 143
  Match protocol TELNET
!
Policy-map type inspect PM-I-D
 Class type inspect CM-I-D-WEB
   Inspect
Class type inspect CM-I-D-MAIL
   Inspect
Class type inspect CM-I-D-TELNET
   Inspect
!
zone-pair security I-D source INTERNET destination DMZ
 service-policy type inspect PM-I-D
```

Lab 2 – Configuring Port-Maps in Zone-based Firewall



Lab Scenario:

- Configure Port-maps to allow port/protocols not natively controlled thru Zone-based Firewall.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

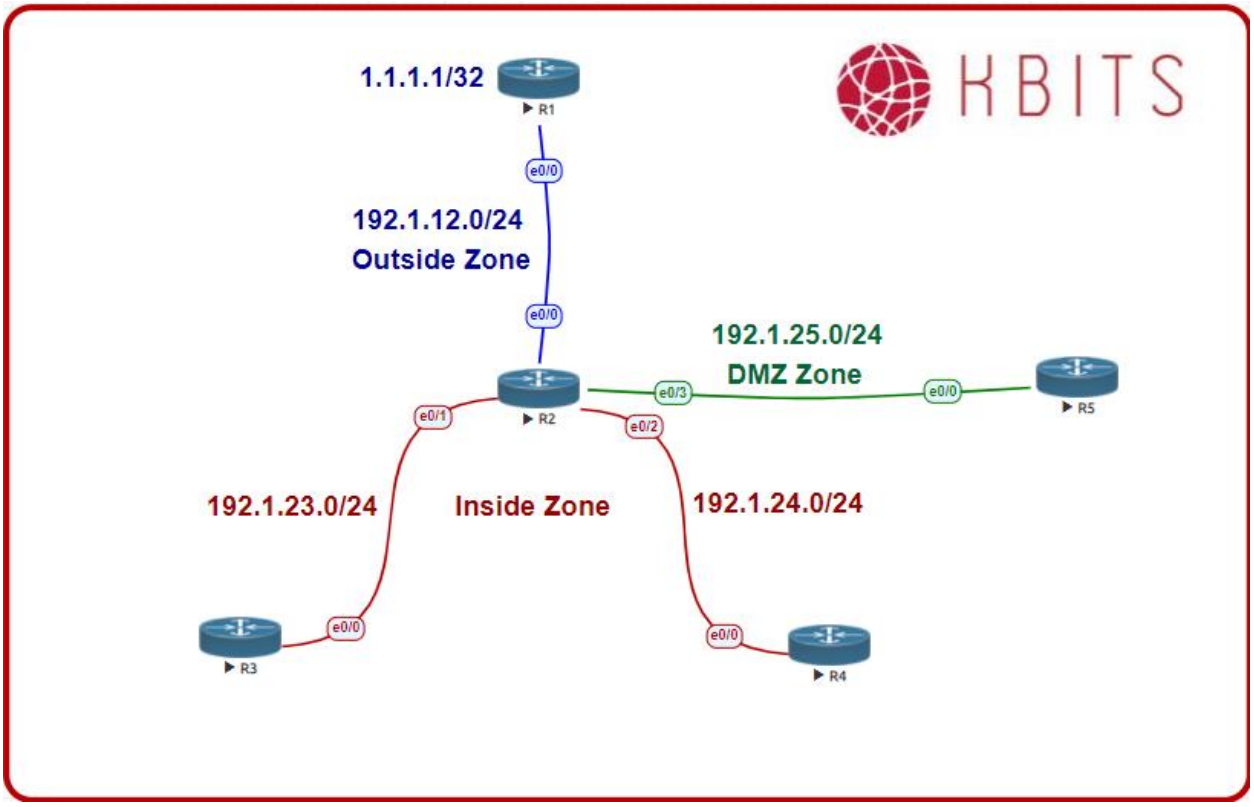
Task 1

Configure Inspection of RDP from LOCAL to DMZ zone.

R2

Class-map type inspect CM-L-D
 Match protocol user-RDP
!
Note: No need to call this Class-map in the policy-map as it is already done in the previous lab. The user-RDP is the same port map created in the previous lab for LOCAL to INTERNET.

Lab 3 – Configuring Nested Classes in Zone-based Firewalls



Lab Scenario:

- Configuring Nested Classes for advanced configurations.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure Access to a server located at 192.1.24.11 for Web Services [HTTP or HTTPS]

R2

```
Access-list 141 permit ip any host 192.1.24.11
!
Class-map type inspect match-any CM-WEB
 Match protocol http
 Match protocol https
!
Class-map type inspect match-all CM-I-D-WEB
 Match class-map CM-WEB
 Match access-group 141
!
Policy-map type inspect PM-I-D
  Class CM-I-D-WEB
    Inspect
```

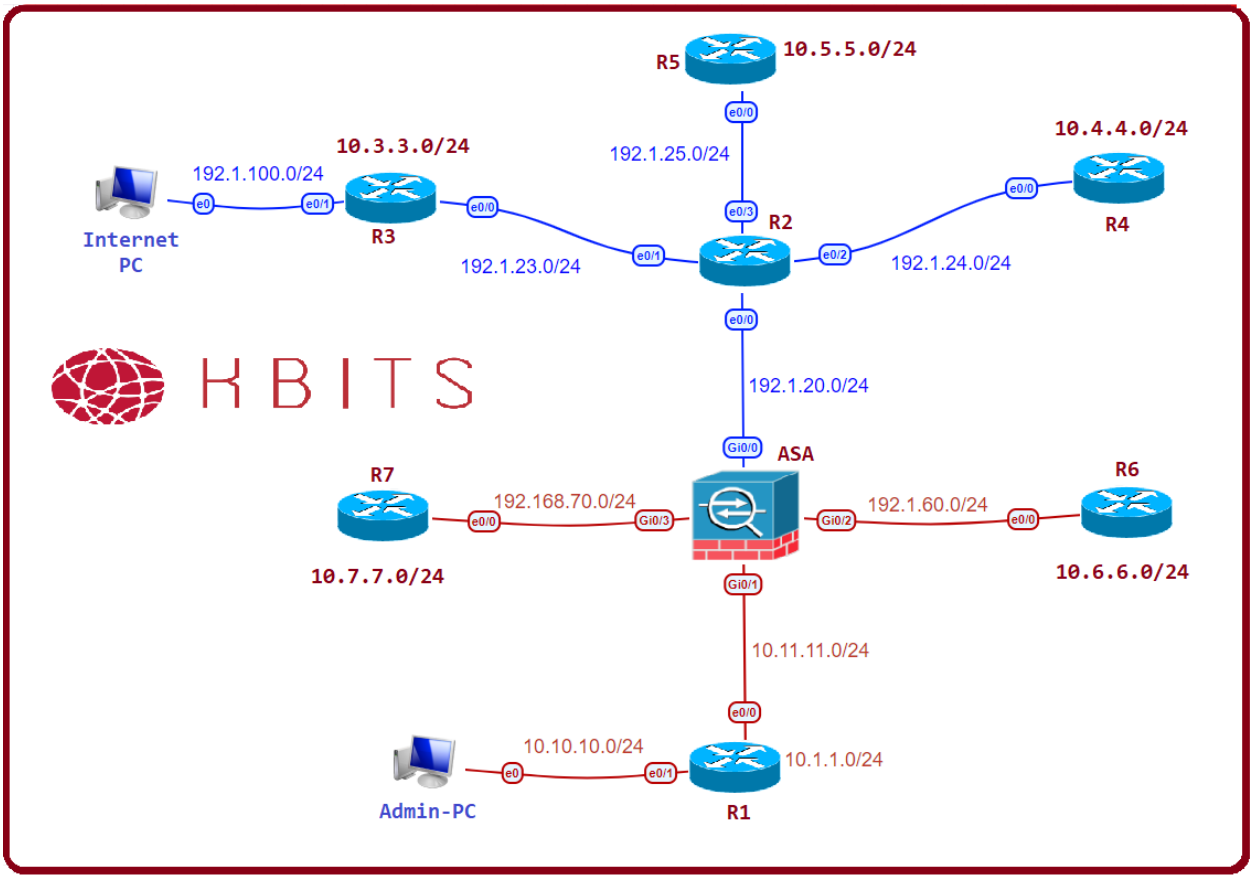
Note: No need to apply this Policy-map as it is already applied in Lab 1

CCIE Security v6 – Configuring ASA, FTD, Intrusion Prevention & AMP

Module 11 – Configuring VPNs on ASA & FTD

Module 11 – Configuring VPNs on ASA & FTD

Lab 1 – Configuring LAN-TO-LAN IPSec VPN on ASA – Router - IKEv1



Lab Scenario:

- Configure a LAN-TO-LAN IPSec VPN using IKEv1.

Initial Setup:

- Configure the IP Addresses on the Routers & FW based on the Diagram.
- Point all the Device to the logical next hop for the Default Gateway.

R1	**R2**
Int E 0/0 Ip add 10.11.11.1 255.255.255.0	Int E 0/0 Ip add 192.1.20.2 255.255.255.0

No shut ! Int E 0/1 Ip add 10.10.10.1 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.1.1 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 10.11.11.1 ! Ip http server ! Line vty 0 4 Password cisco Login Transport input all ! Enable secret cisco	No shut ! Int E 0/1 Ip add 192.1.23.3 255.255.255.0 No shut ! Int E 0/2 Ip add 192.1.24.4 255.255.255.0 No shut ! Int E 0/3 Ip add 192.1.25.5 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.2.2.2 255.255.255.0 ! Ip route 192.1.100.0 255.255.255.0 192.1.23.3
R3 Int E 0/0 Ip add 192.1.23.3 255.255.255.0 No shut ! Int E 0/1 Ip add 192.1.100.3 255.255.255.0 No shut ! Int Loopback1 Ip add 10.3.3.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.23.2	**R4** Int E 0/0 Ip add 192.1.24.4 255.255.255.0 No shut ! Int Loopback1 Ip add 10.4.4.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.24.2
R5 Int E 0/0 Ip add 192.1.25.5 255.255.255.0 No shut ! Int Loopback1 Ip add 10.5.5.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.25.2	**R6** Int E 0/0 Ip add 192.1.60.6 255.255.255.0 No shut ! Int Loopback1 Ip add 10.5.5.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.60.10

R7	ASA
Int E 0/0 Ip add 192.168.70.7 255.255.255.0 No shut ! Int Loopback1 Ip add 10.7.7.7 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.168.70.10	Interface G 0/0 Nameif Outside Ip add 192.1.20.10 255.255.255.0 No shut ! Interface G 0/1 Nameif Inside Ip add 10.11.11.10 255.255.255.0 No shut ! Interface G 0/2 Nameif DMZ-6 Security-level 60 Ip add 192.1.60.10 255.255.255.0 No shut ! Interface G 0/3 Nameif DMZ-7 Security-level 70 Ip add 192.168.70.10 255.255.255.0 No shut ! route Outside 0.0.0.0 0.0.0.0 192.1.20.10 route Inside 10.0.0.0 255.0.0.0 10.11.11.1

Lab Tasks:

Task 1

Configure an IPSec Tunnel on ASA to encrypt traffic from 10.1.1.0/24 to the 10.5.5.0/24 on R5 using the following parameters for IPSec:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Group: 2
  - Hash: MD5
  - Pre-Shared Key: **cisco123**
- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-SHA-HMAC

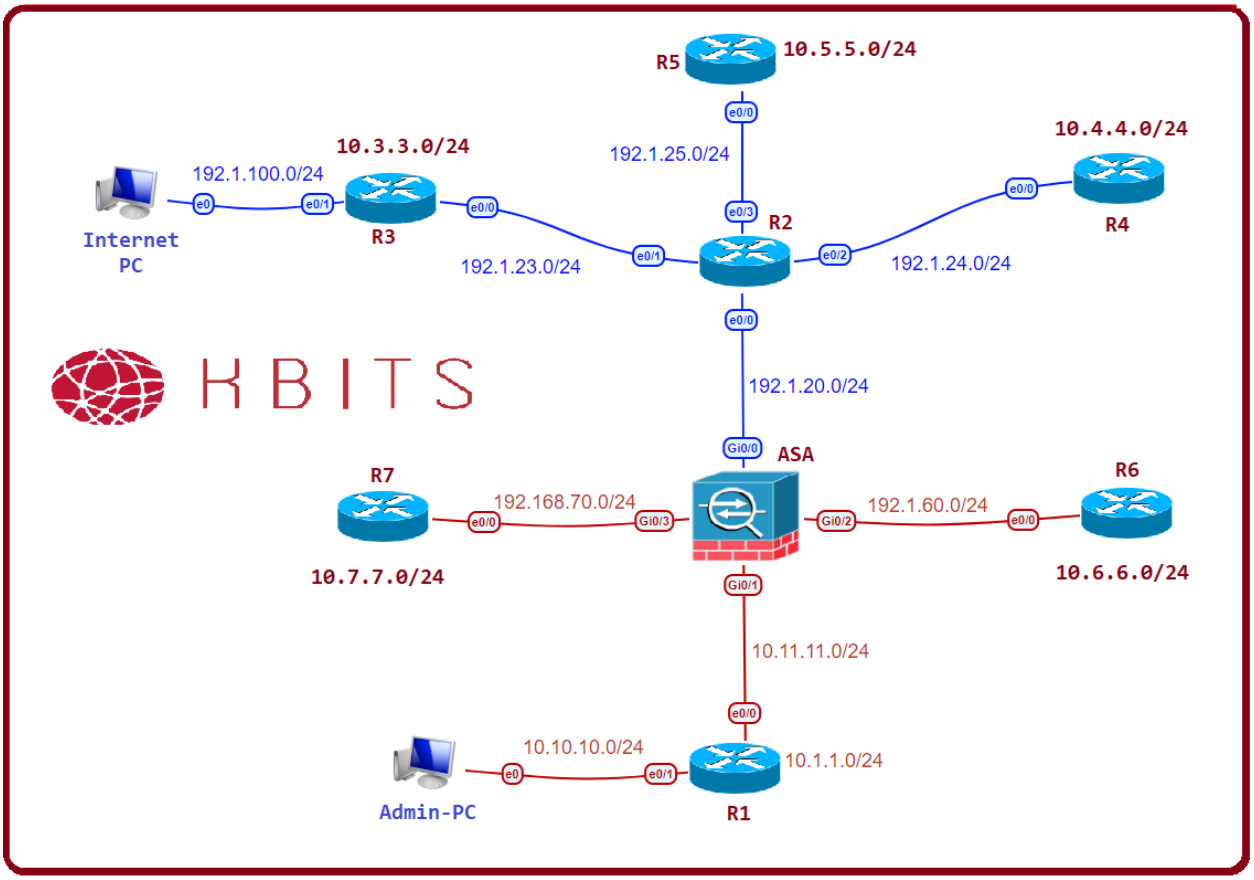
ASA

```
Crypto ikev1 enable outside
!
Crypto ikev1 policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
tunnel-group 192.1.25.5 type ipsec-l2l
tunnel-group 192.1.25.5 ipsec-attributes
 ikev1 pre-shared-key cisco123
!
crypto ipsec ikev1 transform-set T-SET esp-3des esp-sha-hmac
!
access-list 101 permit ip 10.1.1.0 255.255.255.0 10.5.5.0 255.255.255.0
!
crypto map I-MAP 10 set peer 192.1.25.5
crypto map I-MAP 10 set ikev1 transform-set T-SET
crypto map I-MAP 10 match address 101
!
Crypto map I-MAP Interface Outside
```

R5

```
Crypto isakmp policy 10
 Authentication pre-share
 Hash md5
 Group 2
 Encryption 3des
!
Crypto isakmp key cisco123 address 192.1.20.10
!
crypto ipsec transform-set T-SET esp-3des esp-sha-hmac
!
access-list 101 permit ip 10.5.5.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map I-MAP 10 ipsec-isakmp
 set peer 192.1.20.10
 set transform-set T-SET
 match address 101
!
Interface E 0/0
 Crypto map I-MAP
```

Lab 2 – Configuring LAN-TO-LAN IPSec VPN on ASA – Router – IKEv2



Lab Scenario:

- Configure a LAN-TO-LAN IPSec VPN using IKEv2.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure an IPSec Tunnel on ASA to encrypt traffic from 10.1.1.0/24 to the 10.2.2.0/24 on R2 (Loopback 0) using the following parameters for IPSec:

- IKEv2 Parameters
  - Authentication: Pre-shared
  - Encryption: AES-256
  - Group: 2
  - Inegrity: SHA-256
  - PRF: SHA-256
  - Pre-Shared Key: ASA-2-R2 -> **cisco111**
  - Pre-Shared Key: R2-2-ASA -> **cisco222**

- IPSec Parameters
  - Encryption: ESP-3DES
  - Authentication: ESP-SHA1/ESP-SHA-HMAC

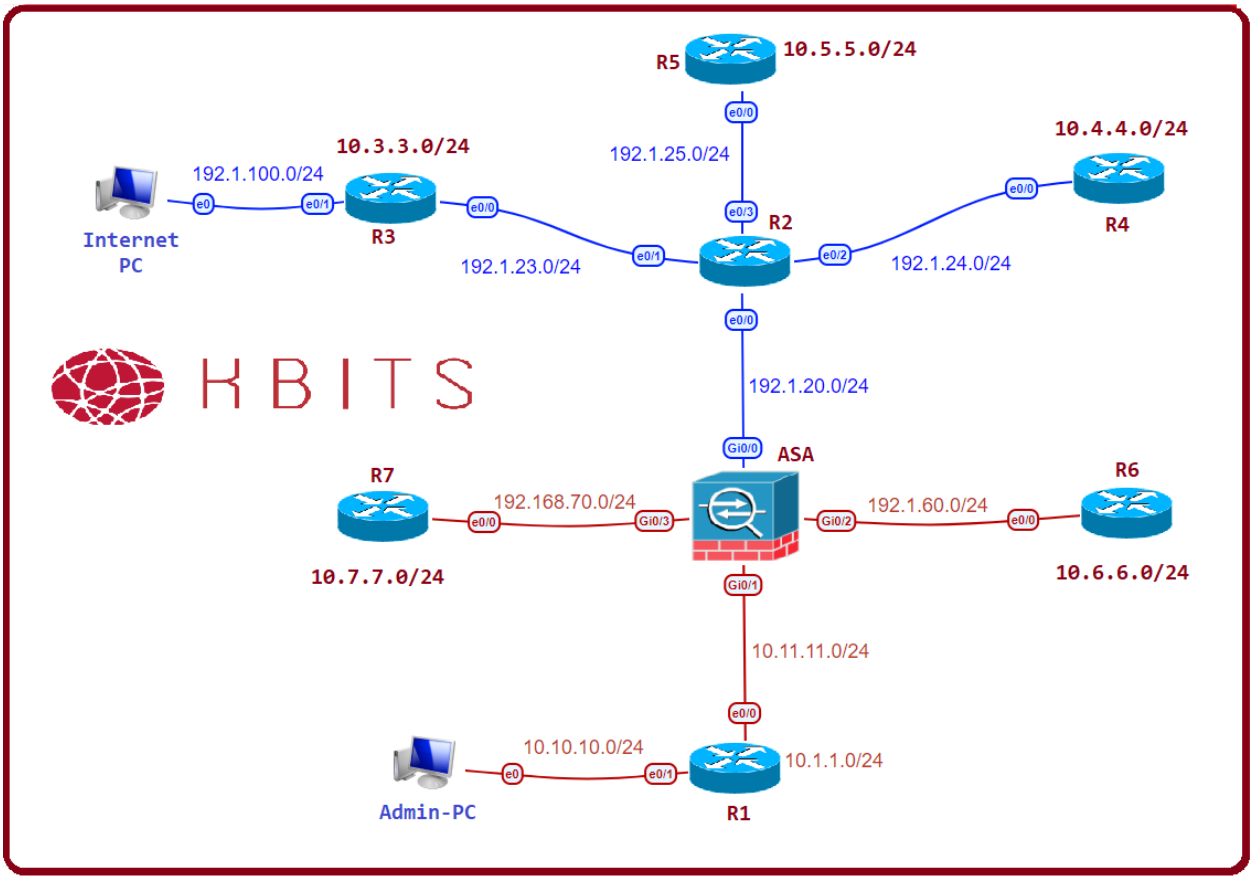
ASA-2

```
Crypto ikev2 enable outside
!
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 2
 prf sha256
!
tunnel-group 192.1.20.2 type ipsec-l2l
tunnel-group 192.1.20.2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco222
 ikev2 local-authentication pre-shared-key cisco111
!
crypto ipsec ikev2 ipsec-proposal IKEv2-TSET
 protocol esp encryption 3des
 protocol esp integrity sha-1
!
access-list 102 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0
255.255.255.0
!
crypto map I-MAP 20 set peer 192.1.20.2
crypto map I-MAP 20 set ikev2 ipsec-proposal IKEv2-TSET
crypto map I-MAP 20 match address 102
```

R2

```
crypto ikev2 proposal PROP-1
 encryption aes-cbc-256
 integrity sha256
 group 2
!
crypto ikev2 policy POL-1
 proposal PROP-1
!
crypto ikev2 keyring KR-1
 peer ASA
  address 192.1.20.10
  pre-shared-key local cisco222
  pre-shared-key remote cisco111
!
crypto ikev2 profile PROF-1
 match identity remote address 192.1.20.10
 authentication remote pre-share
 authentication local pre-share
 keyring local KR-1
!
crypto ipsec transform-set T-SET esp-3des esp-sha-hmac
!
Access-list 102 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto map I-MAP 10 ipsec-isakmp
 set peer 192.1.20.10
 set transform-set T-SET
 set ikev2-profile PROF-1
 match address 102
!
interface E 0/0
 crypto map I-MAP
!
Ip route 10.1.1.0 255.255.255.0 192.1.20.10
```

Lab 3 – Configuring LAN-To-LAN IPSec VPN thru a Firewall – Without NAT-T



Lab Scenario:

- Configure a LAN-To-LAN IPSec VPN from R4 to R6 thru the ASA Firewall.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure an IPSec Tunnel on R4 to encrypt traffic from 10.4.4.0/24 to the 10.6.6.0/24 on R6 using the following parameters for IPSec:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Group: 2
  - Hash: MD5
  - Pre-Shared Key: **cisco123**
- IPSec Parameters
  - Encryption: ESP-AES
  - Authentication: ESP-SHA-HMAC

R4

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
 group 2
crypto isakmp key Cisco123 address 192.1.60.6
!
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
!
Access-list 101 permit ip 10.4.4.0 0.0.0.255 10.6.6.0 0.0.0.255
!
crypto map CMAP 10 ipsec-isakmp
 set peer 192.1.60.6
 set transform-set TSET
 match address 101
!
Interface E 0/0
 crypto map CMAP
```

R6

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
 group 2
crypto isakmp key Cisco123 address 192.1.24.4
!
```

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
!
Access-list 101 permit ip 10.6.6.0 0.0.0.255 10.4.4.0 0.0.0.255
!
crypto map CMAP 10 ipsec-isakmp
 set peer 192.1.24.4
 set transform-set TSET
 match address 101
!
Interface E 0/0
 crypto map CMAP
```

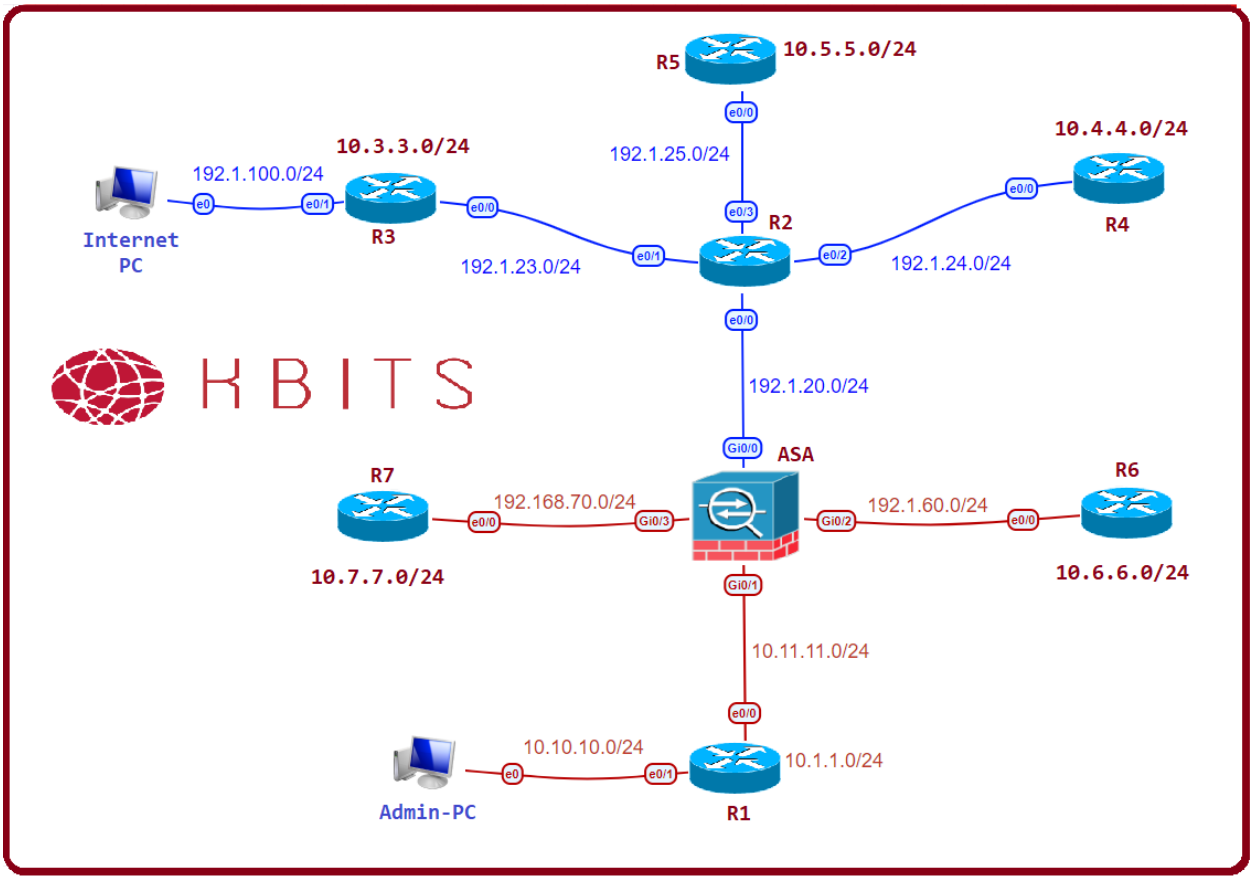
Task 2

Configure the appropriate entries on the ASA Firewall to allow the IPSec Tunnel to form between R4 & R6.

ASA

```
access-list OUTSIDE permit udp host 192.1.24.4 host 192.1.60.6 eq 500
access-list OUTSIDE permit esp host 192.1.24.4 host 192.1.60.6
!
access-group OUTSIDE in interface outside
```

Lab 4 – Configuring LAN-To-LAN IPSec VPN thru a Firewall – With NAT-T



Lab Scenario:

- Configure a LAN-To-LAN IPSec VPN from R3 to R7 thru the ASA Firewall.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Translated R7 on the Outside as 192.1.20.7.

ASA

```
Object network R7
 Host 192.168.70.7
 Nat (DMZ-7,Outside) static 192.1.20.7
```

Task 2

Configure an IPSec Tunnel on R3 to encrypt traffic from 10.3.3.0/24 to the 10.7.7.0/24 on R7 using the following parameters for IPSec:

- ISAKMP Parameters
  - Authentication: Pre-shared
  - Encryption: 3DES
  - Group: 2
  - Hash: MD5
  - Pre-Shared Key: **cisco123**
- IPSec Parameters
  - Encryption: ESP-AES
  - Authentication: ESP-SHA-HMAC

R3

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
 group 2
crypto isakmp key Cisco123 address 192.1.20.7
!
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
!
access-list 101 permit ip 10.3.3.0 0.0.0.255 10.7.7.0 0.0.0.255
!
crypto map CMAP 10 ipsec-isakmp
 set peer 192.1.20.7
 set transform-set TSET
 match address 101
!
Interface E 0/0
 crypto map CMAP
```

R7

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
 group 2
crypto isakmp key Cisco123 address 192.1.23.3
!
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
!
access-list 101 permit ip 10.7.7.0 0.0.0.255 10.3.3.0 0.0.0.255
!
crypto map CMAP 10 ipsec-isakmp
 set peer 192.1.23.3
 set transform-set TSET
 match address 101
!
Interface E 0/0
 crypto map CMAP
```

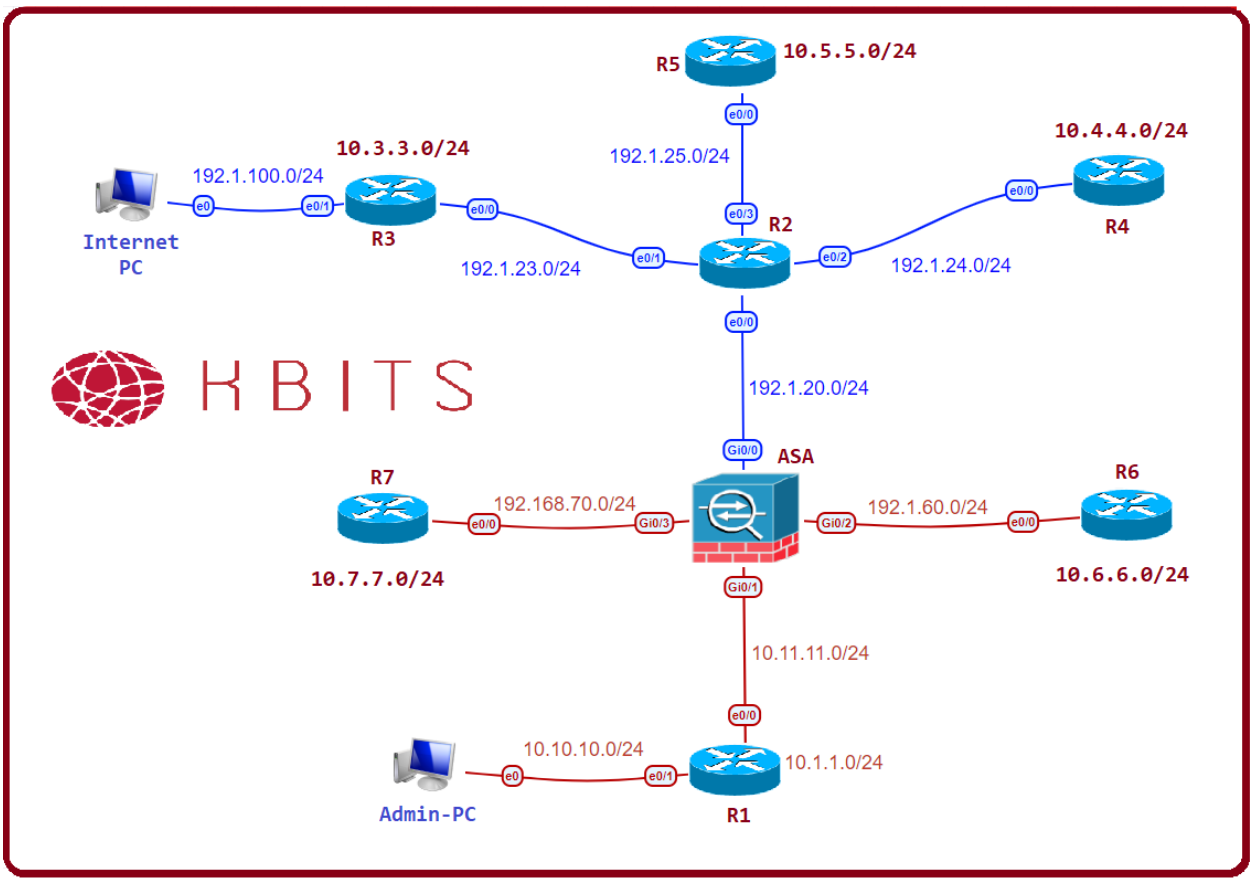
Task 2

Configure the appropriate entries on the ASA Firewall to allow the IPSec Tunnel to form between R3 & R7.

ASA

```
access-list OUTSIDE permit udp host 192.1.23.3 host 192.168.70.7 eq 500
access-list OUTSIDE permit udp host 192.1.23.3 host 192.168.70.7 eq 4500
```

Lab 5 – Configuring Clientless SSL VPN on ASA – Web VPN



Lab Scenario:

- Configure a Remote-Access VPN using Clientless SSL VPN.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

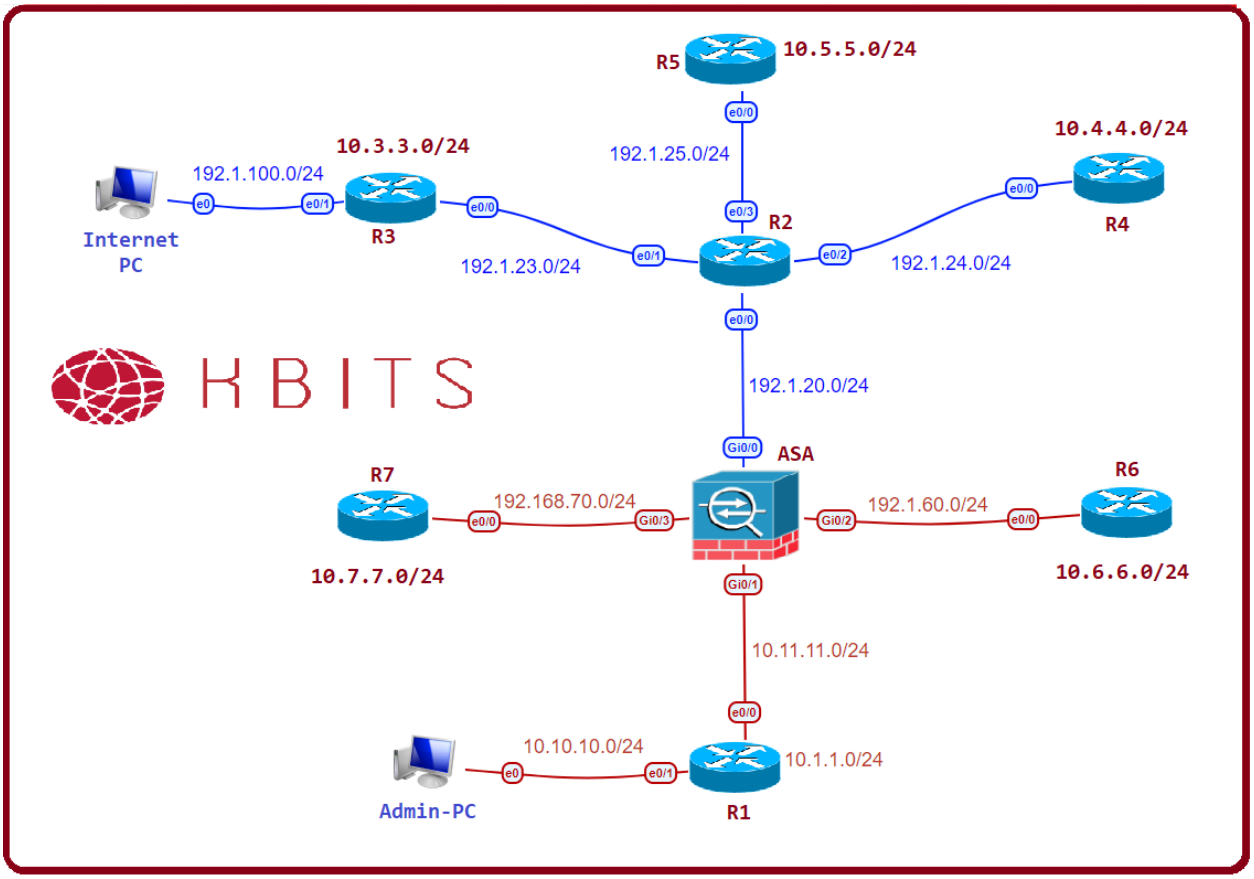
Configure ASA for Clientless WebVPN using the following Parameters:

- Group: SALES
  - VPN-Tunnel-Protoco: SSL-Clientless
  - Banner: Authorized Users Only !!!
  - Port-forward: SALES-APPS
    - 30001:10.11.11.1:23
    - 30002:10.11.11.1:1521
- Users:
  - Jane
    - Password – Cisco123
    - Group-policy - SALES

ASA

```
webvpn
 enable outside
 port-forward SALES-APPS 30001 10.11.11.1 23
 port-forward SALES-APPS 30002 10.11.11.2 1521
!
group-policy SALES internal
group-policy SALES attributes
 vpn-tunnel-protocol ssl-clientless
 banner value "Authorized Users Only !!!"
 webvpn
   port-forward value SALES-APPS
!
username Jane password Cisco123
username Jane attributes
 vpn-group-policy SALES
```

Lab 6 – Configuring ASDM Access on a ASA Firewall



Lab Scenario:

- Configure ASDM Access on a ASA Firewall

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

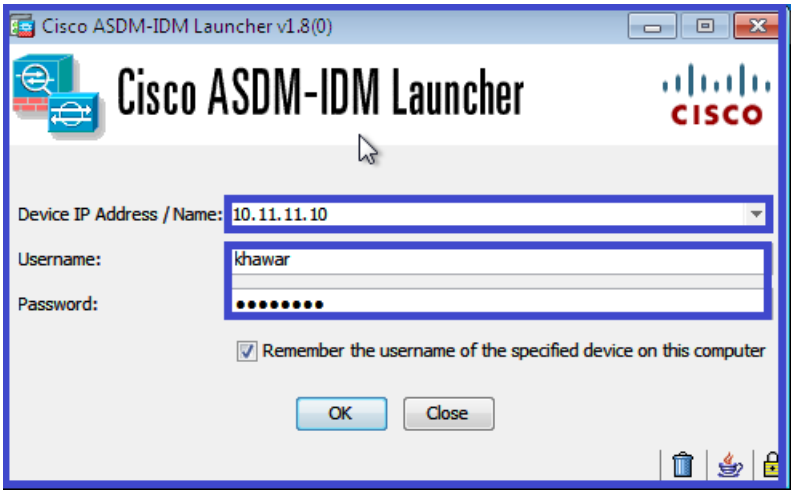
Configure ASA Firewall to allow ASDM Access from the 10.10.10.0/24 Internal Network. Create a local admin user **khawar** with a password of **Cisco123**. Assign it a privilege level of **15**. Configure ASDM authentication using the Local Database.

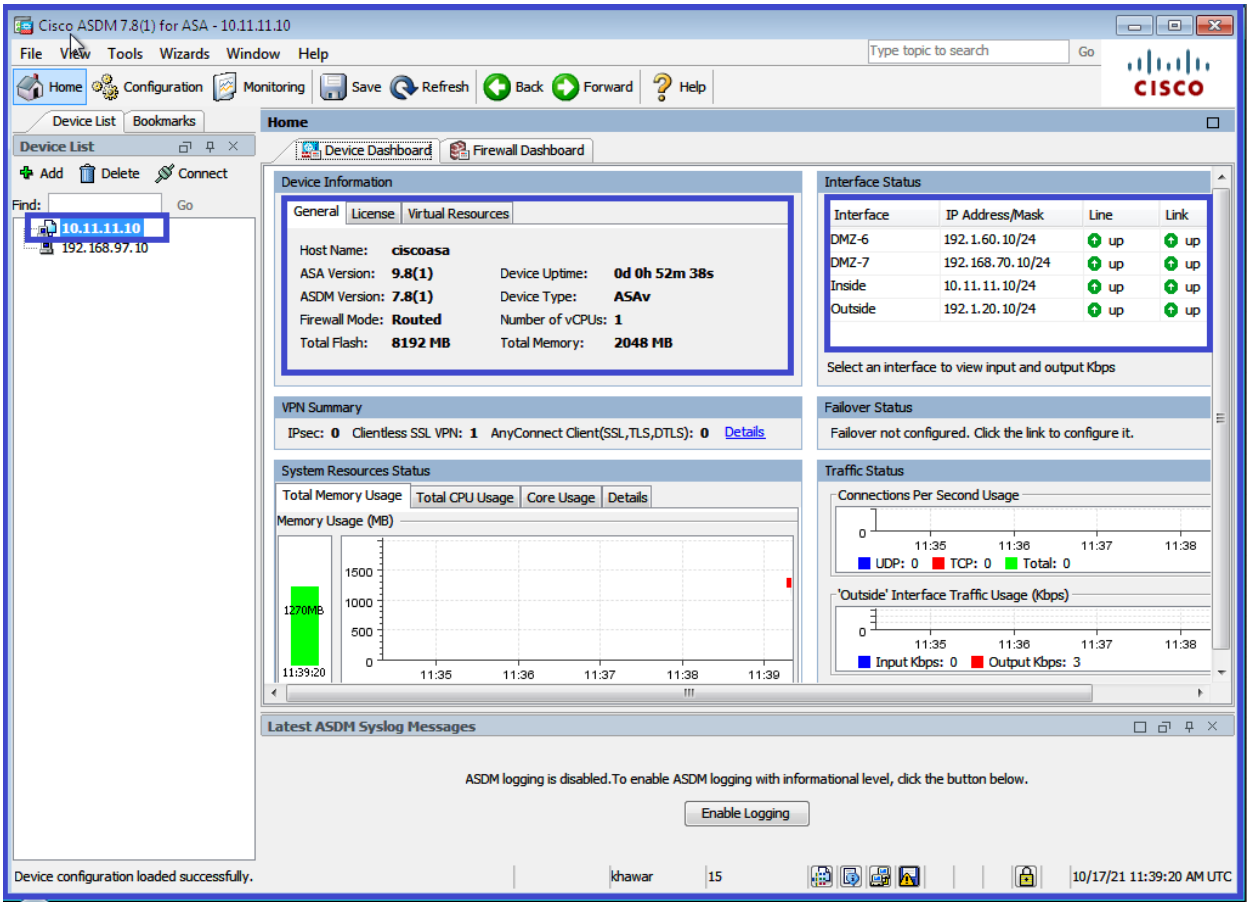
ASA

```
http server enable
http 10.10.10.0 255.255.255.0 inside
username khawar password Cisco123 privilege 15
aaa authentication http console LOCAL
```

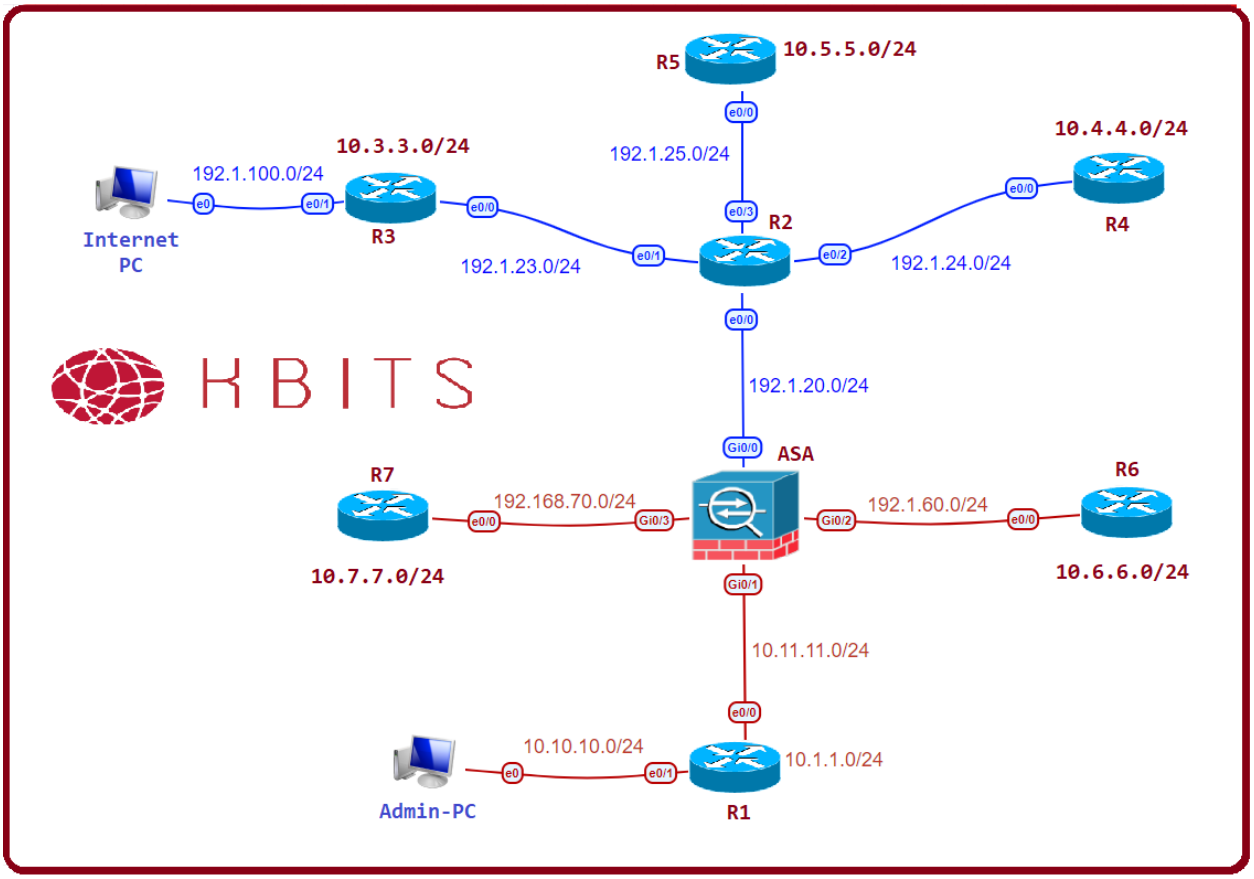
Task 2

Log into the ASA using ASDM on the Internal Admin PC.





Lab 7 – Configuring a SSL VPN using AnyConnect Client



Lab Scenario:

- Configure a SSL VPN using for the AnyConnect Client
-

Initial Setup:

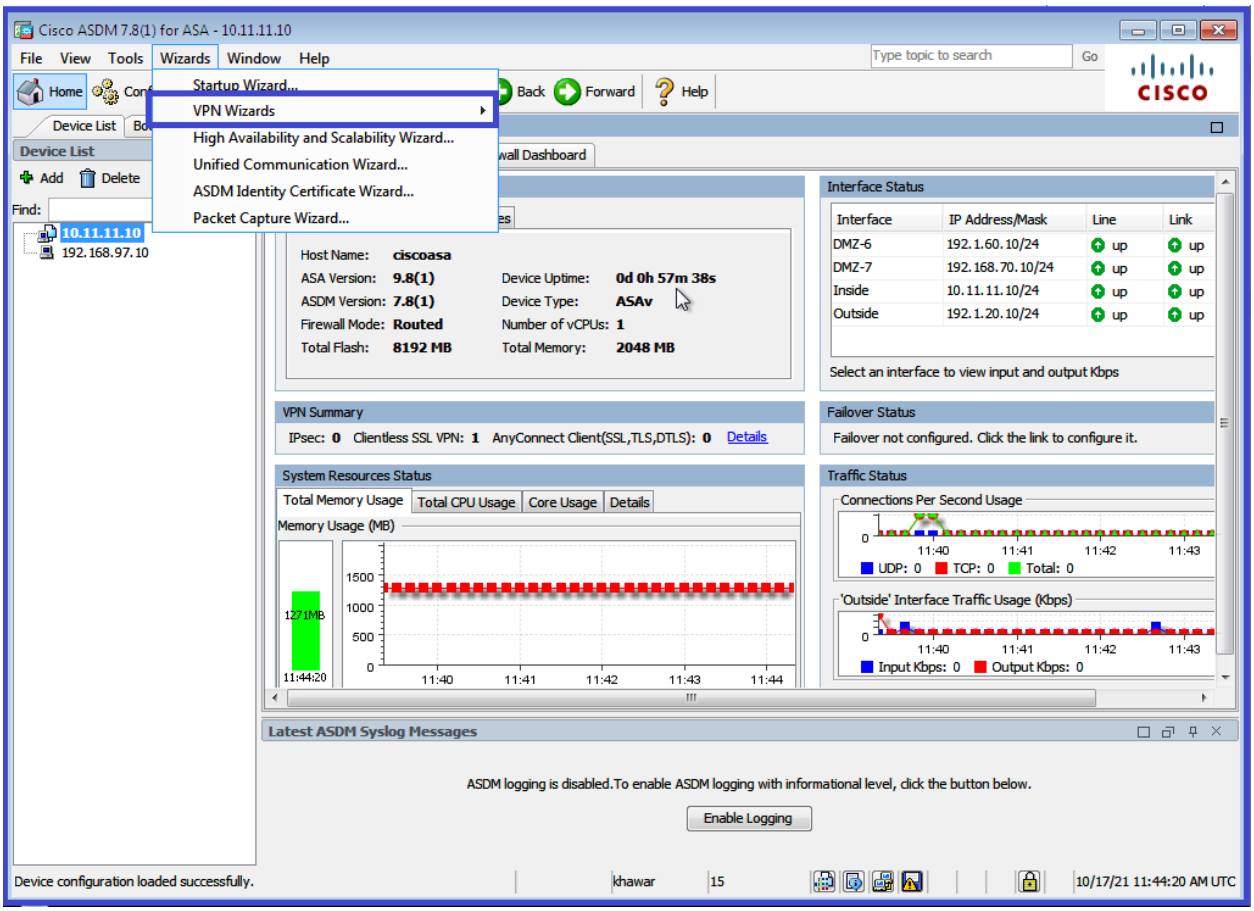
- **Based on the previous Lab**

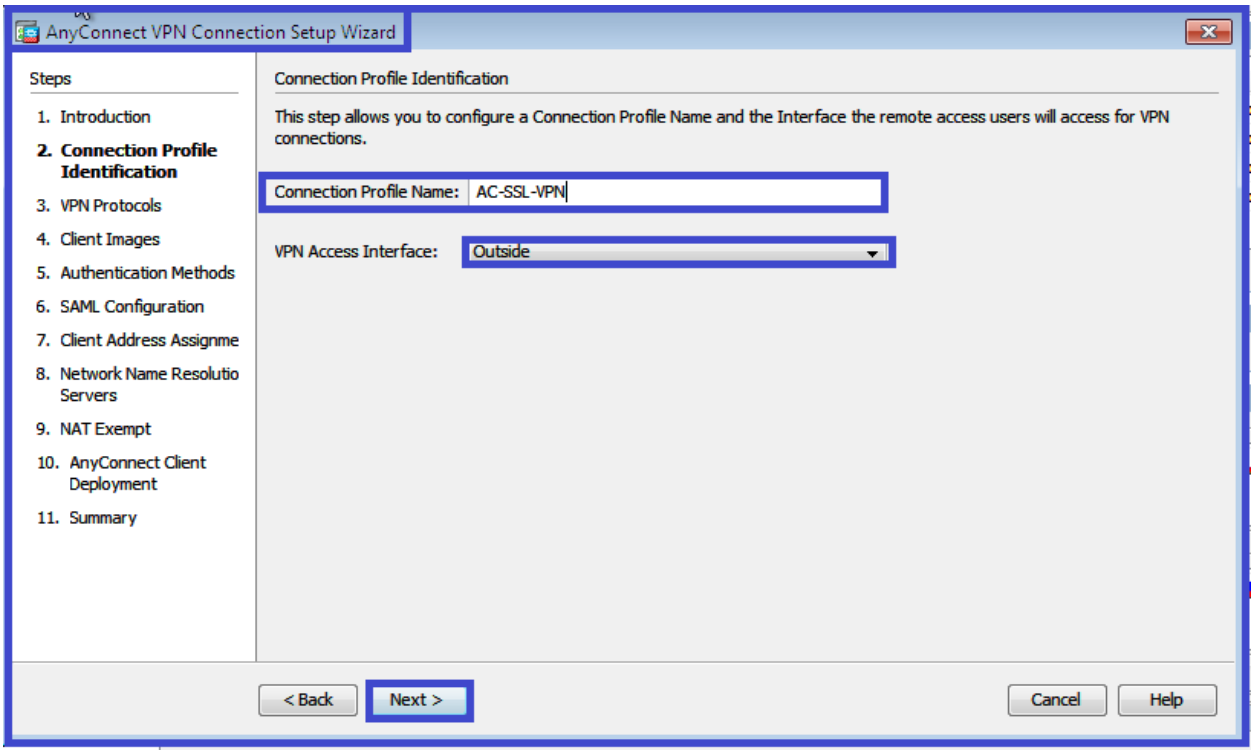
Lab Tasks:

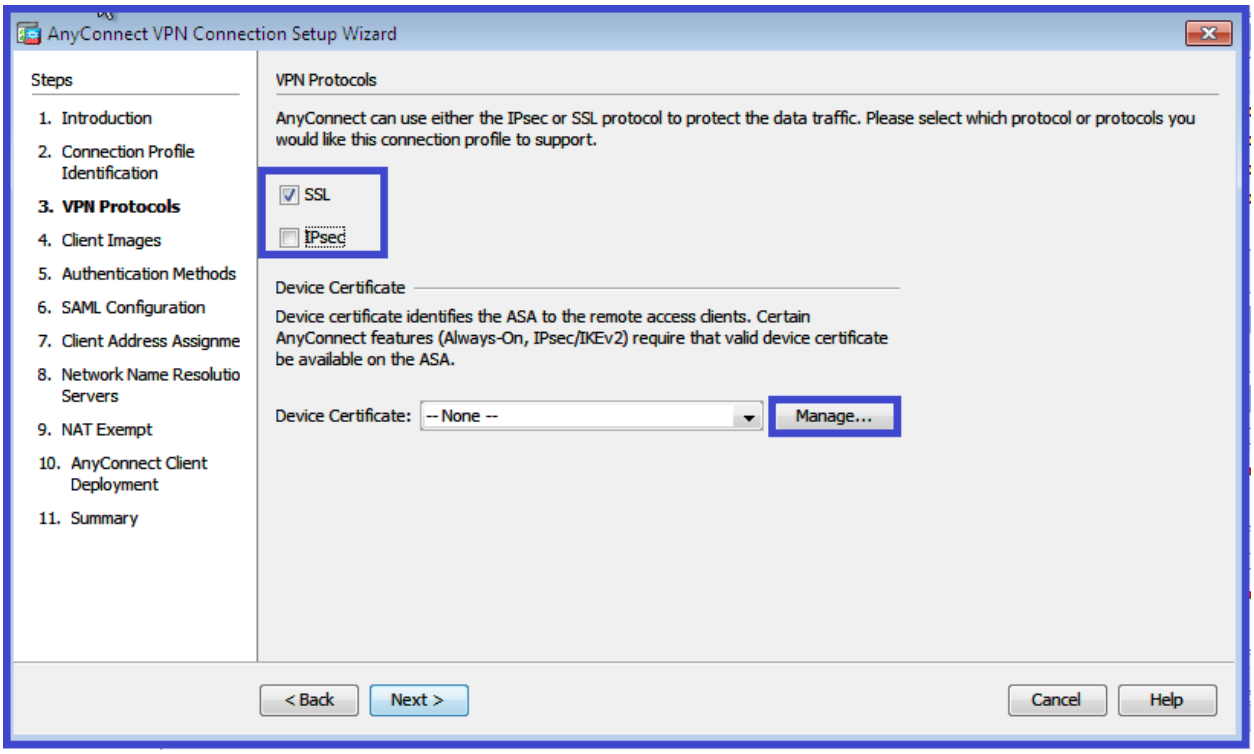
Task 1

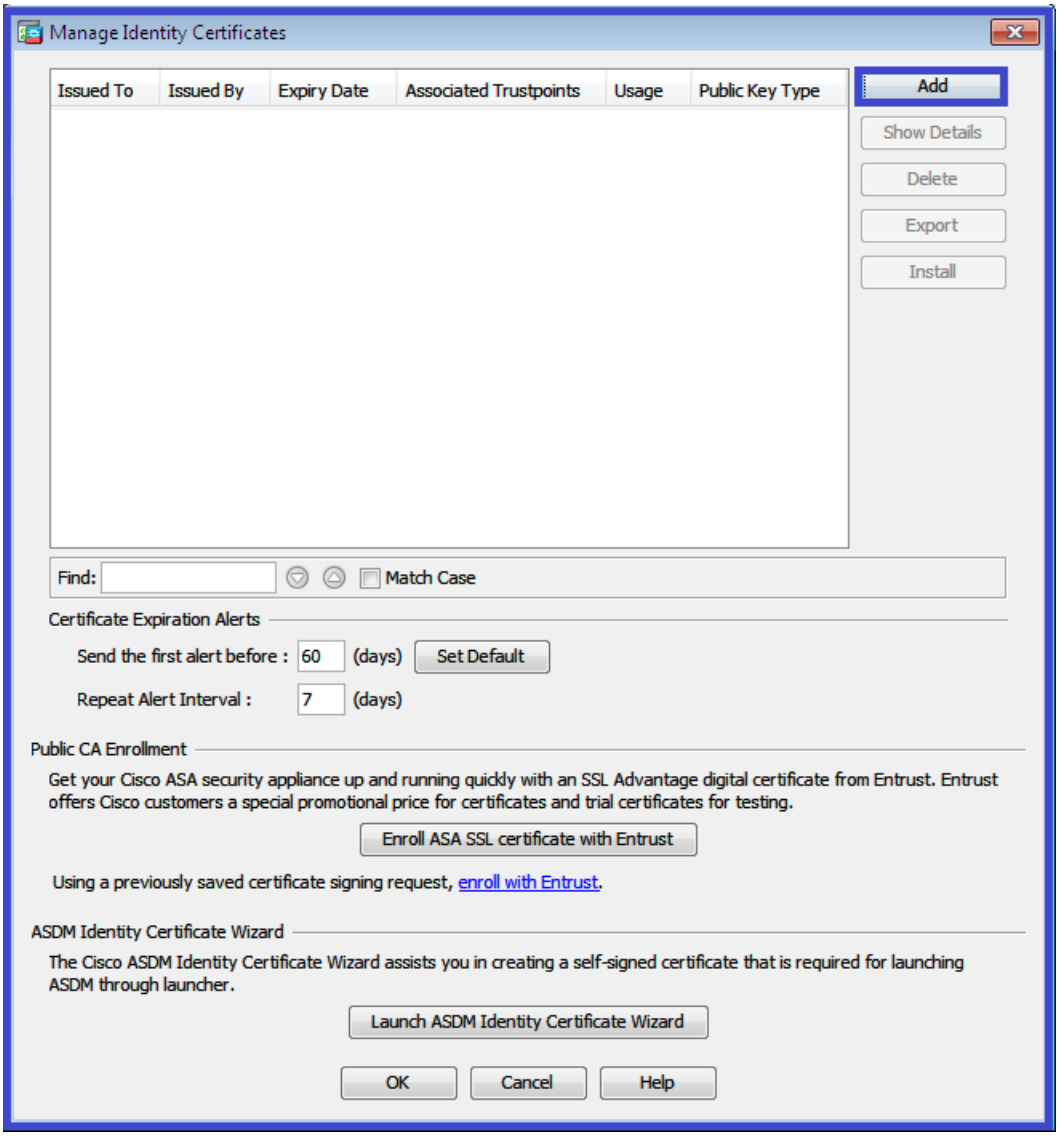
Configure a SSL VPN on the ASA for the AnyConnect Client using the following parameters:

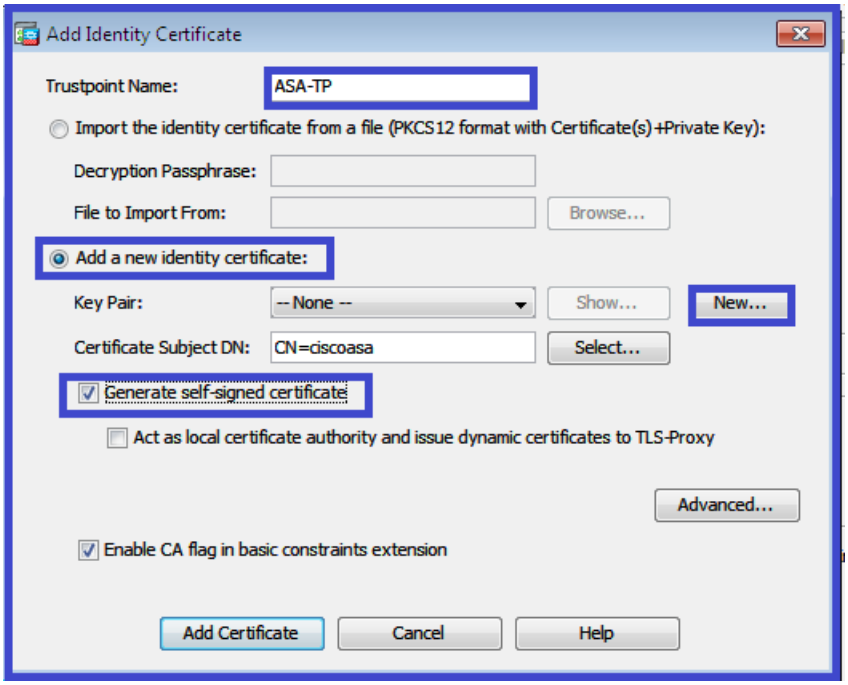
- Connection Profile Name: **AC-SSL-VPN**
- VPN Interface: **Outside**
- VPN Protocols: **SSL Only**
- Device Certificate:
  - Trustpoint Name: **ASA-TP**
- VPN Pool Name: **AC-VPN-POOL**
- VPN Pool Information:
  - Start IP: **192.168.1.1**
  - End IP: **192.168.1.254**
  - Subnet Mask: **255.255.255.0**
- Split Tunneling:
  - Only Send traffic thru the Tunnel specified below:
  - Split-Tunnel List Name: **ST-ACL**
    - 10.1.1.0/24
    - 10.11.11.0/24

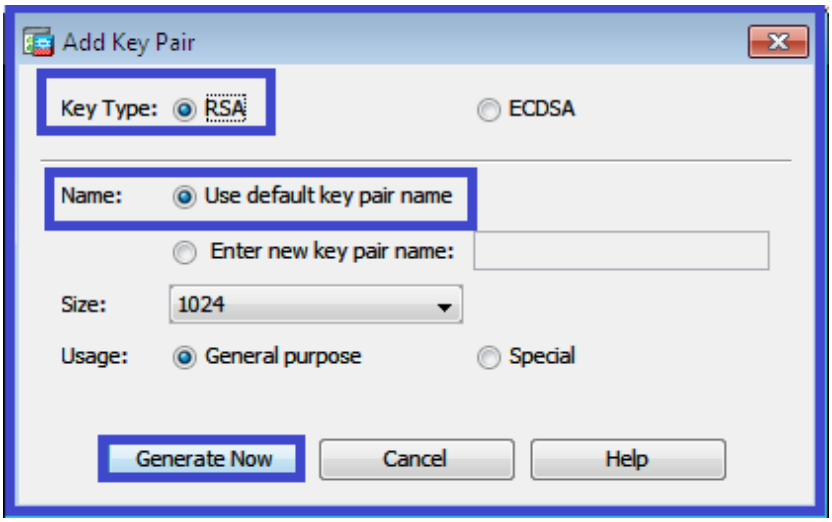


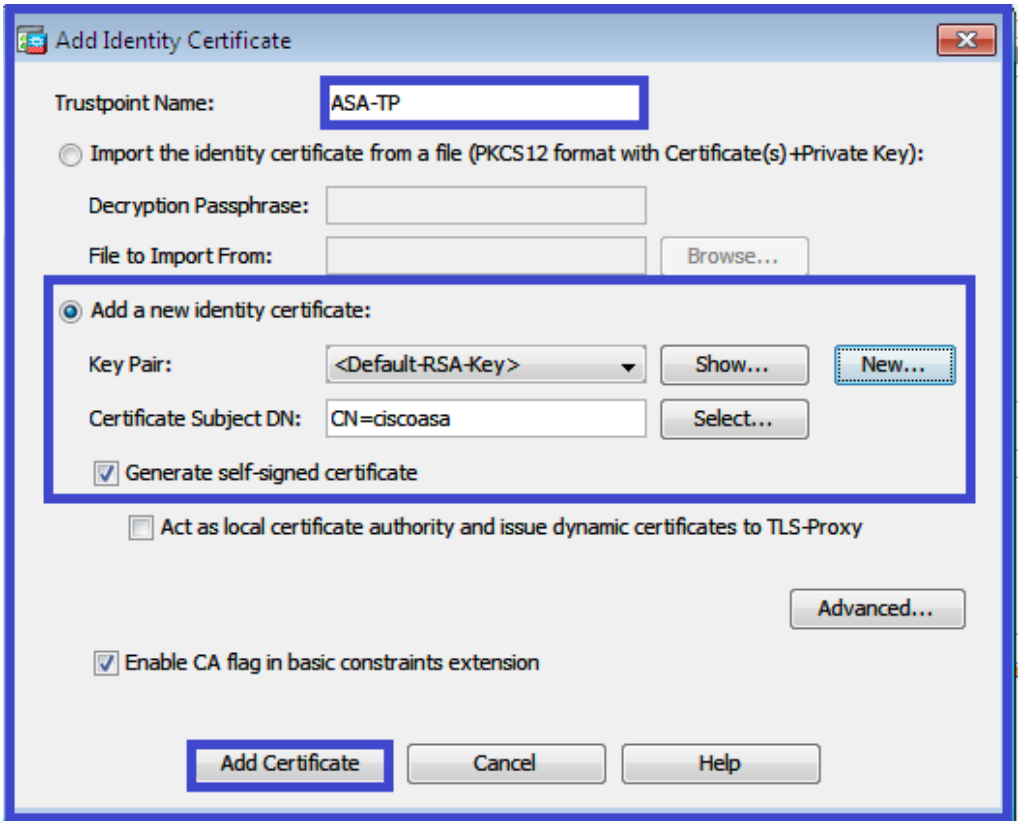


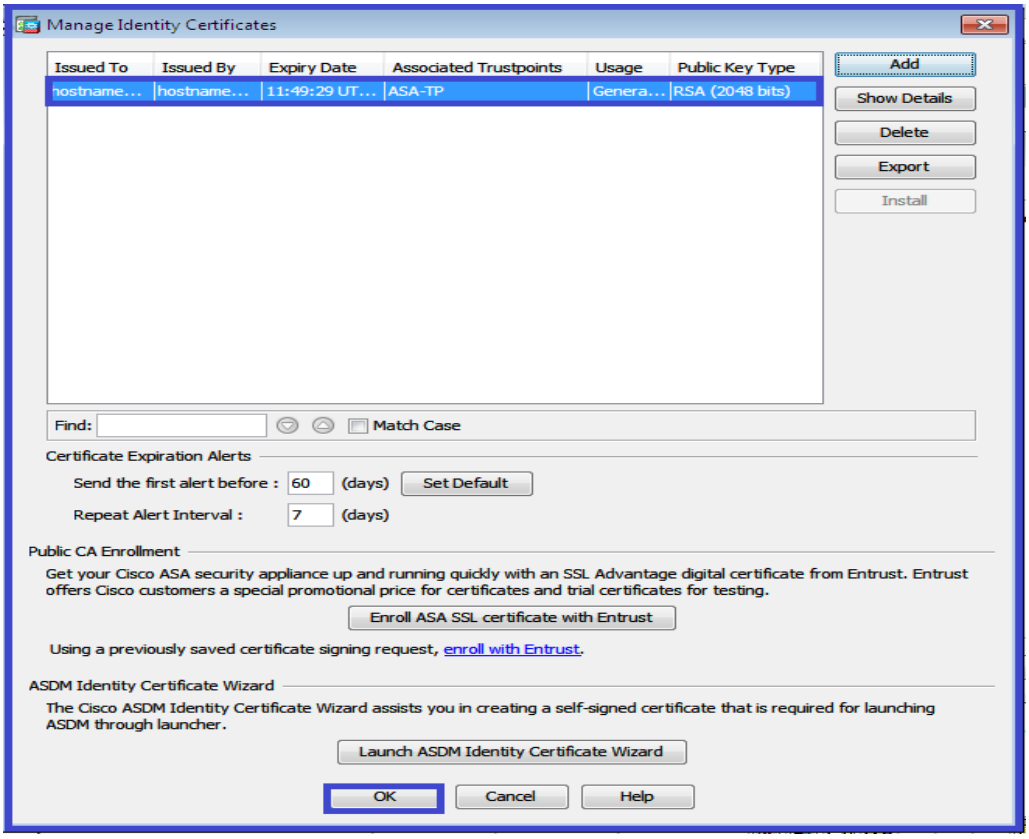


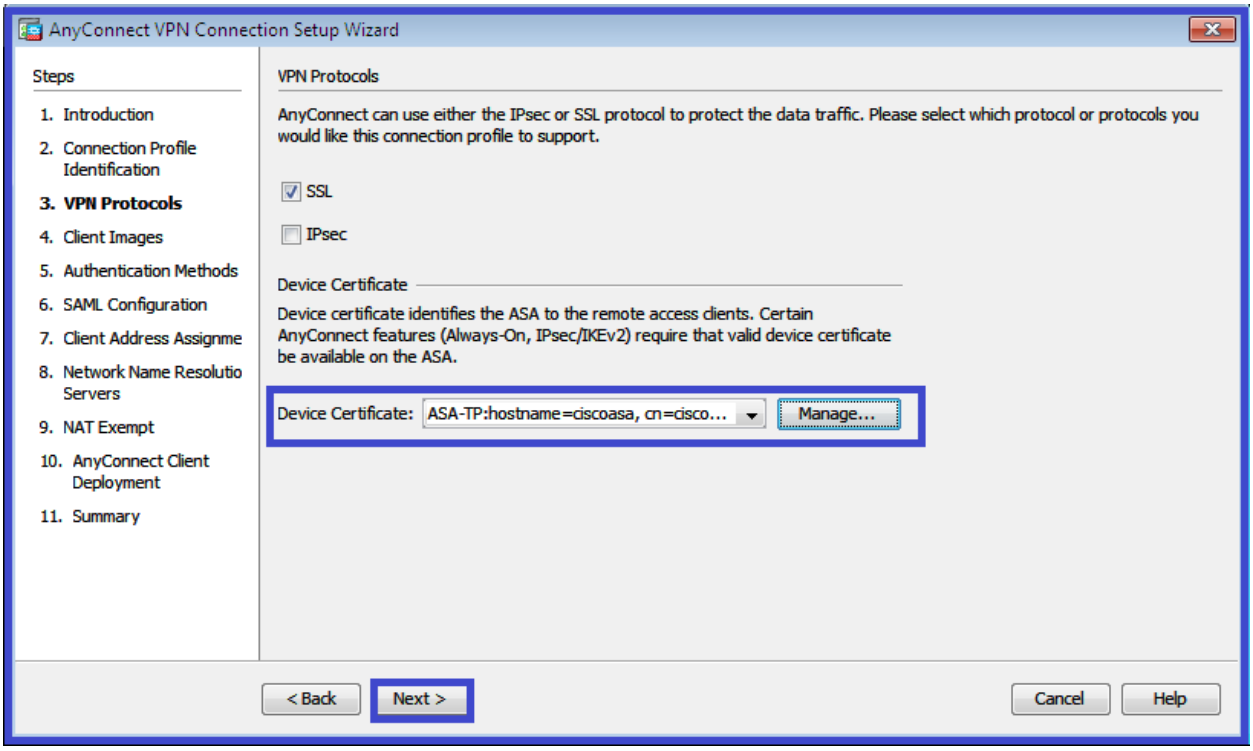


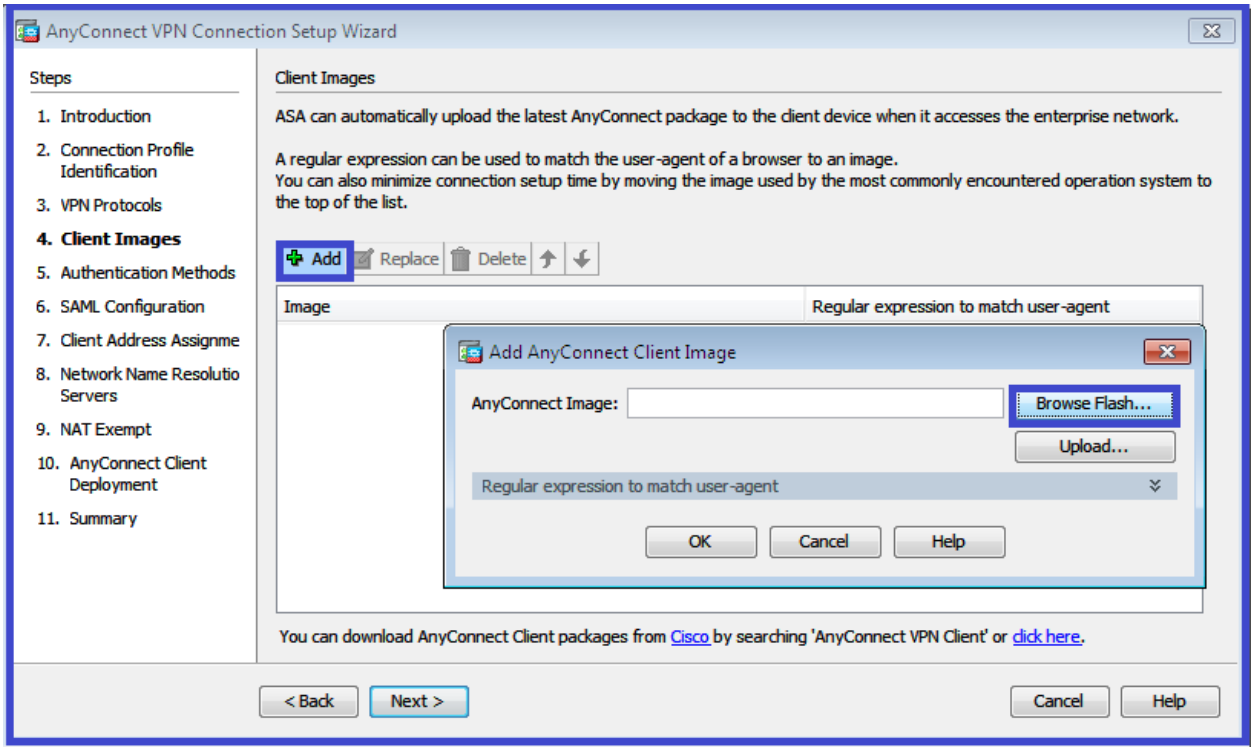










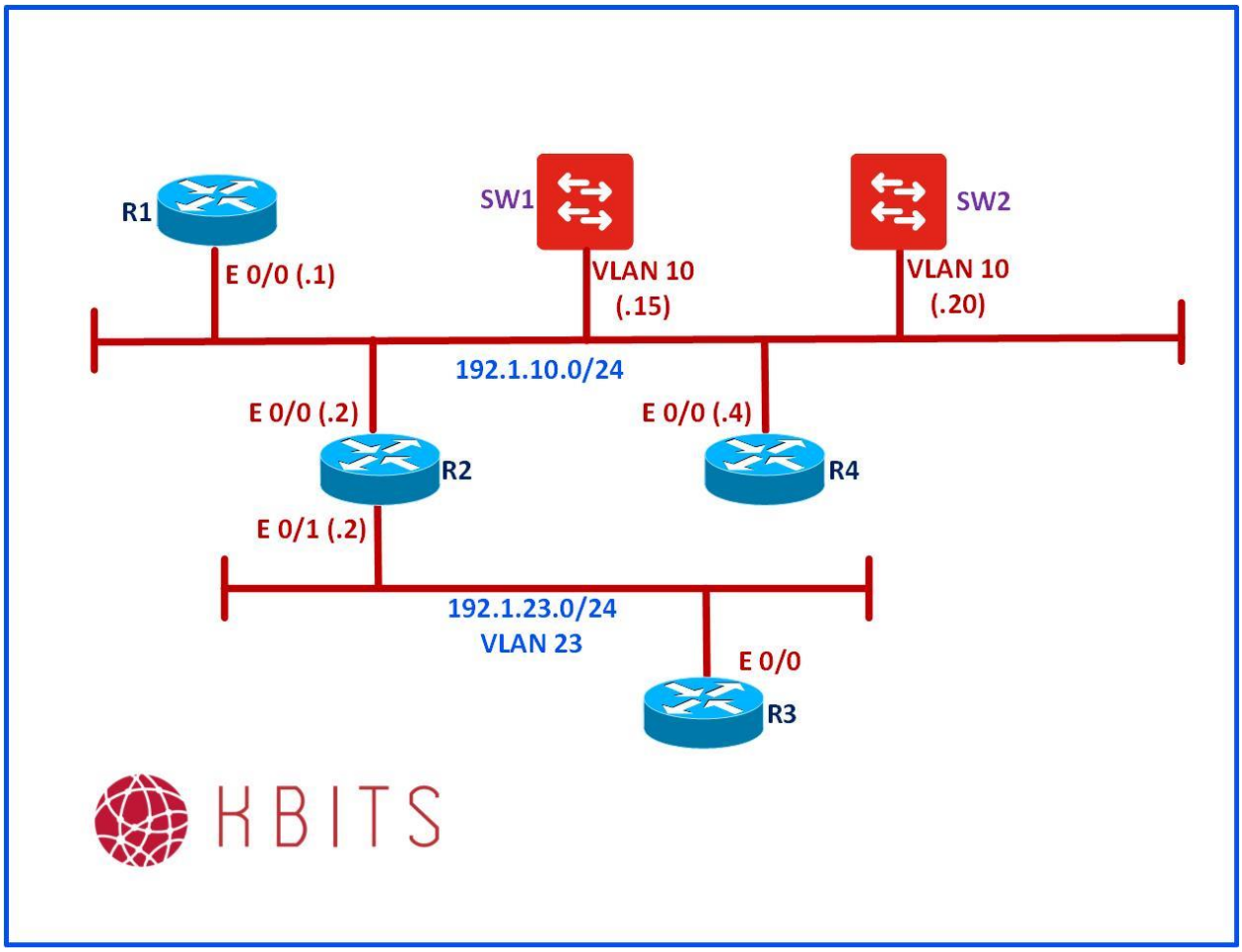


CCIE Security v6 – Configuring Router & Switch Security Features

Module 1 – Control Plane Management

Module 1 – Control Plane Management

Lab 1 – Configuring Control Plane Policing



Lab Scenario:

- Configure the Router for Control Plane Policing for Telnet Traffic.
- The lab is based on the following physical setup:
    - R1 – R4 E 0/0 are connected to SW1 ports E0/0 – E 0/3 respectively. For Example, E 0/0 on R1 is connected to SW1 E 0/0, E 0/0 on R2 is connected to SW1 E 0/2 .....
    - R1 – R4 E 0/1 are connected to SW2 ports E 0/1 – E 0/3 respectively. For Example, E 0/1 on R1 is connected to SW2 E 0/0, F0/1 on R2 is connected to SW2 F 0/2 .....
    - Switches are trunked over on E 1/0 ports on both Switches.

Initial Setup:

- Configure the IP Addresses on the Routers & SW based on the Diagram.
- Configure the 2 switches to trunk using dot1q. Configure SW1 as the VTP Server in domain cisco. Configure SW2 as the VTP Client in domain cisco.
- Configure all the VLANs required on SW1.
- Assign the devices to the appropriate VLANs.
- Run EIGRP in AS 100 on the Routers and SW to have complete routing in the network.

R1	**R2**
Int E 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Router eigrp 100 Network 192.1.10.0	Int E 0/0 Ip add 192.1.10.2 255.255.255.0 No shut ! Int E 0/0 Ip add 192.1.23.2 255.255.255.0 No shut ! Router eigrp 100 Network 192.1.10.0 Network 192.1.23.0
R3	**R4**
Int E 0/0 Ip add 192.1.23.3 255.255.255.0 No shut ! Router eigrp 100 Network 192.1.23.0	Int E 0/0 Ip add 192.1.10.4 255.255.255.0 No shut ! Router eigrp 100 Network 192.1.10.0
SW1 Interface E 1/0 Swithcport trunk encapsulation dot1q Switchport mode trunk ! Vtp mode server Vtp domain cisco ! Vlan 10,23	

```
!
Interface range E 0/0, E 0/1, E 0/3
 Switchport mode access
 Switchport access vlan 10
!
Interface range E 0/2
 Switchport mode access
 Switchport access vlan 23
!
Ip routing
!
Interface VLAN 10
 Ip address 192.1.10.15 255.255.255.0
 No shut
```

SW2

```
Interface E 1/0
 Swithcport trunk encapsulation dot1q
 Switchport mode trunk
!
Vtp mode client
Vtp domain cisco
!
Interface E 0/1
 Switchport mode access
 Switchport access vlan 23
!
Ip routing
!
Interface VLAN 10
 Ip address 192.1.10.20 255.255.255.0
 No shut
```

Lab Tasks:

Task 1

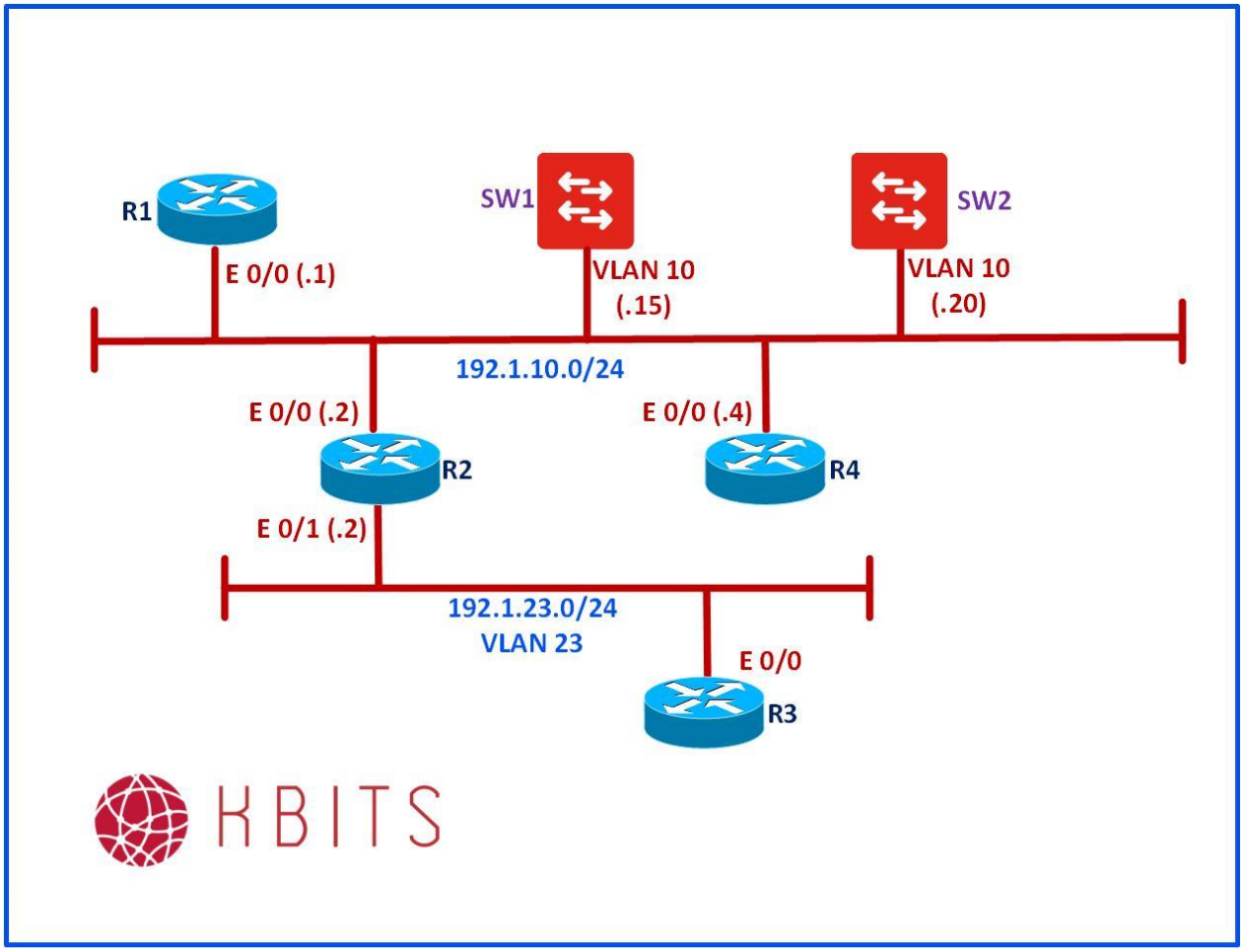
R3 has been configured to allow telnet access for management purposes. Using Control Plane Policing, control the rate of Telnet traffic to 64000 bps.

R3

```
access-list 111 permit tcp any any eq 23
!
class-map TELNET
```

```
 match access-group 101
!
policy-map CP-Police
 class TELNET
   police 64000
!
control-plane
 service-policy input CP-Police
```

Lab 2 – Configuring Control Plane Protection for Port Filtering



Lab Scenario:

- Configure a Router for Control Plane Port-Filtering.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure R3 with a port-filter to drop all traffic destined to a custom udp port 11223. It should also drop traffic to all unused port numbers.

R3

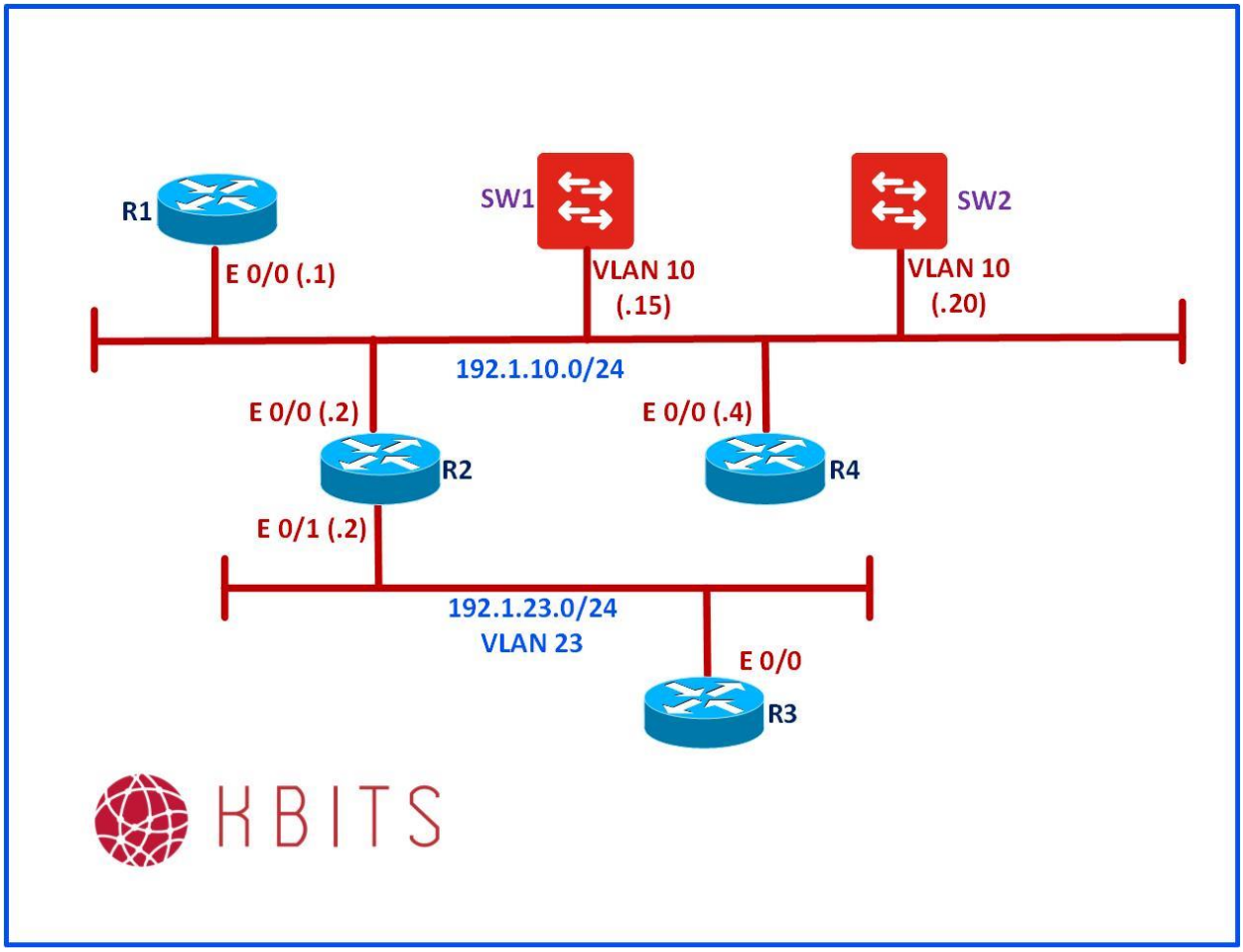
```
class-map type port-filter match-any CM-PF
 match port udp 11223
 match closed-ports
!
policy-map type port-filter PM-PF
 class CM-PF
   drop
!
control-plane host
 service-policy type port-filter input PM-PF
```

CCIE Security v6 – Configuring Router & Switch Security Features

Module 2 – Configuring Router Security Features

Module 2 – Configuring Router Security Features

Lab 1 – Configuring Anti-Spoofing ACL & the RPF Feature



Lab Scenario:

- Configure R2 to block all RFC 1918 addresses coming in from R3.
- R2 should also implement strict RPF to verify that the source is coming in from the valid interface.
- Log all packets that fail the RPF check.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Block any RFC 1918 address coming into R2 from R3.

R2

```
Access-list 121 deny ip 10.0.0.0 0.255.255.255 any
Access-list 121 deny ip 172.16.0.0 0.15.255.255 any
Access-list 121 deny ip 192.168.0.0 0.0.255.255 any
Access-list 121 permit ip any any
!
Interface E 0/1
 Ip access-group 121 in
```

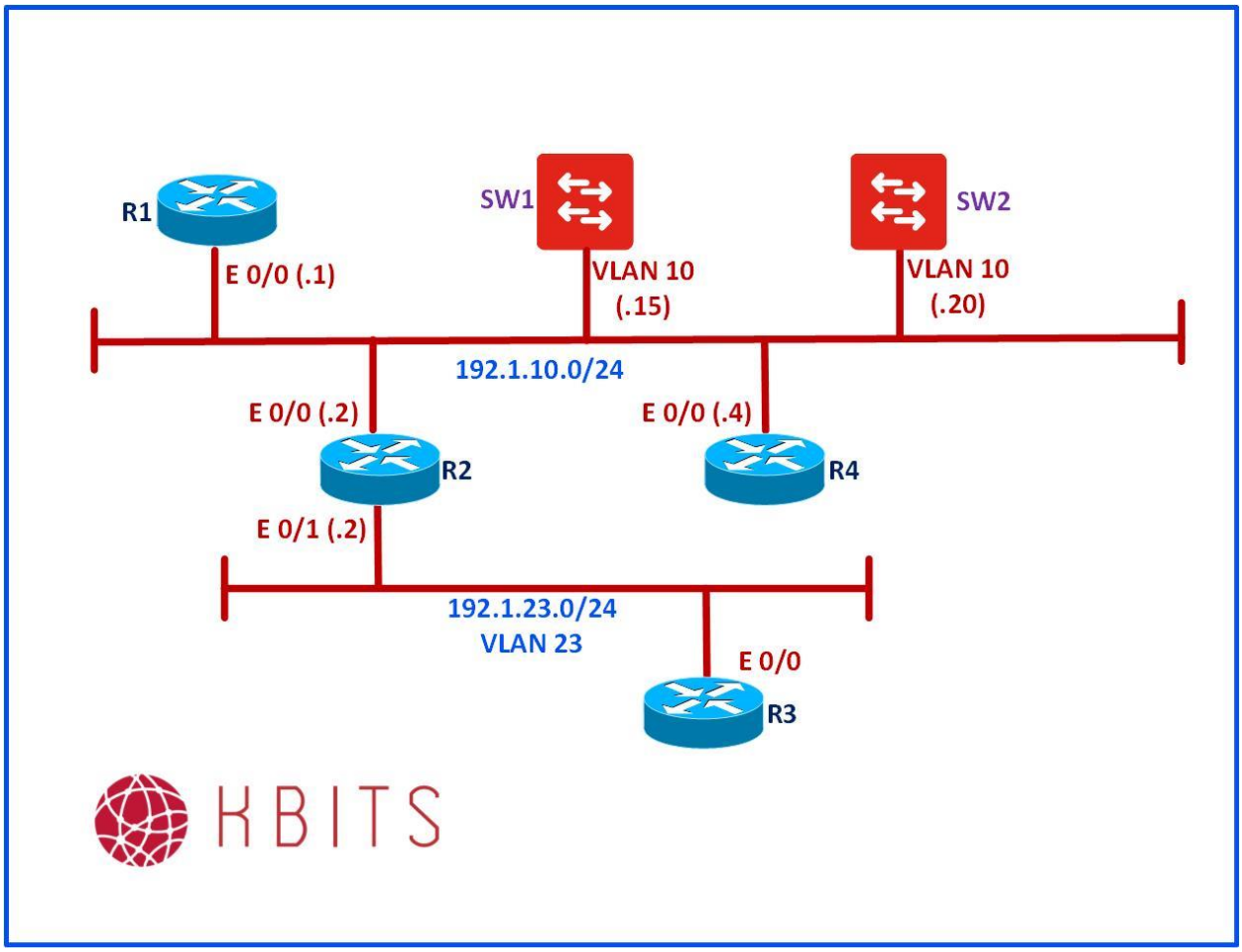
Task 2

Use Strict RPF to prevent IP spoofing using network addresses from the internal networks. The route could use the default gateway to check for the source address. Also make sure all packets that are failing the RPF check get logged.

R2

```
Access-list 131 deny ip any any log
!
Interface E 0/1
 ip verify unicast source reachable-via  rx allow-default 131
```

Lab 2 – Configuring NTP with Authentication



Lab Scenario:

- Configure a Router as Clock Provider using NTP.
- Configure a Router to acquire the time from a remote Time source using NTP.
- Authenticate the NTP Relationship.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure R1 as a NTP Master with a stratum of 2. R1 is in New Delhi (+5:30). Configure the appropriate Time Zone setting. Set the Router clock based on the current date and time.

R1

```
clock timezone IST 5 30
!
Do clock set hh:mm:ss xx Mar 2021
!
ntp master 2
```

Task 2

Configure R2 to receive its clock from R1. R2 is in Dubai (+4). Configure R2 such that it automatically adjusts the clock based on the time zone

R2

```
clock timezone DST 4
!
ntp server 192.1.10.1
```

Task 3

Configure R3 to receive its clock from R2. R3 is located in Rome (+1). Do not use the NTP Server command to receive the clock. Do not configure any commands under the interface to accomplish this task.

R3

```
clock timezone RST 1
!
ntp peer 192.1.23.2
```

Task 4

Authenticate all NTP communications using a key id of 123. The Key string should be **ccie12353.**

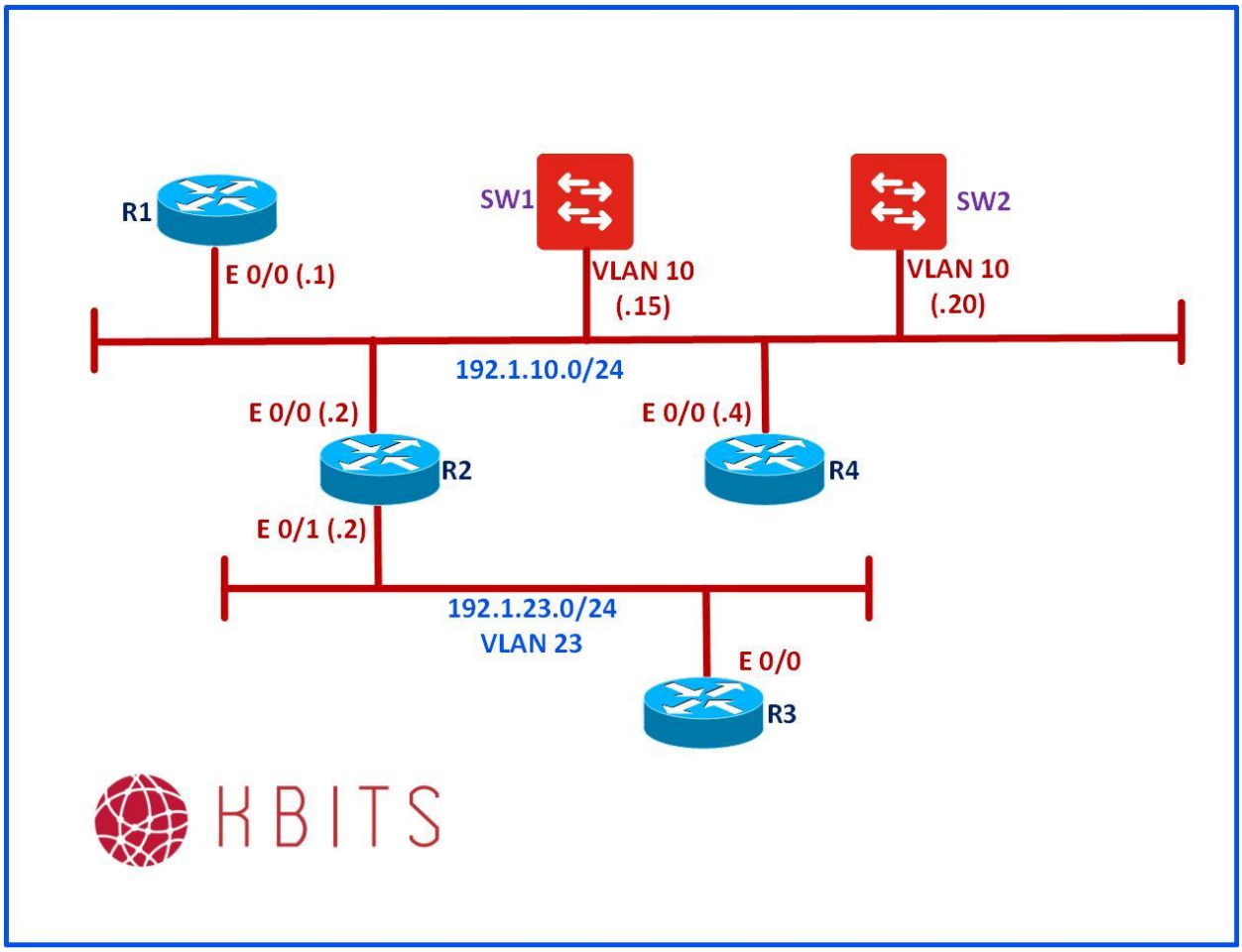
R1

```
ntp authentication-key 123 md5 ccie12353
ntp authenticate
ntp trusted-key 123
```

R2

ntp authentication-key 123 md5 ccie12353 ntp authenticate ntp trusted-key 123 ntp server 192.1.10.1 key 123
R3 ntp authentication-key 123 md5 ccie12353 ntp authenticate ntp trusted-key 123 ntp server 192.1.23.2 key 123

Lab 3 – Configuring the Router for SNMP



Lab Scenario:

- Configure a router to send SNMP traps to a configured SNMP Management Station.
- Limit the traps to ISAKMP and IPSec.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

There is a SNMP Management Station located at 192.1.10.50. Configure R2 to send SNMP Traps for ISAKMP and IPSec only to this management station. It is using a community name of **PublIc**.

R2

```
snmp-server host 192.1.10.50 Pub1Ic  ipsec isakmp
```

Task 2

Configure R2 to send traps to the previously configured SNMP Management station when an ISAKMP tunnel comes up or goes down.

R2

```
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
```

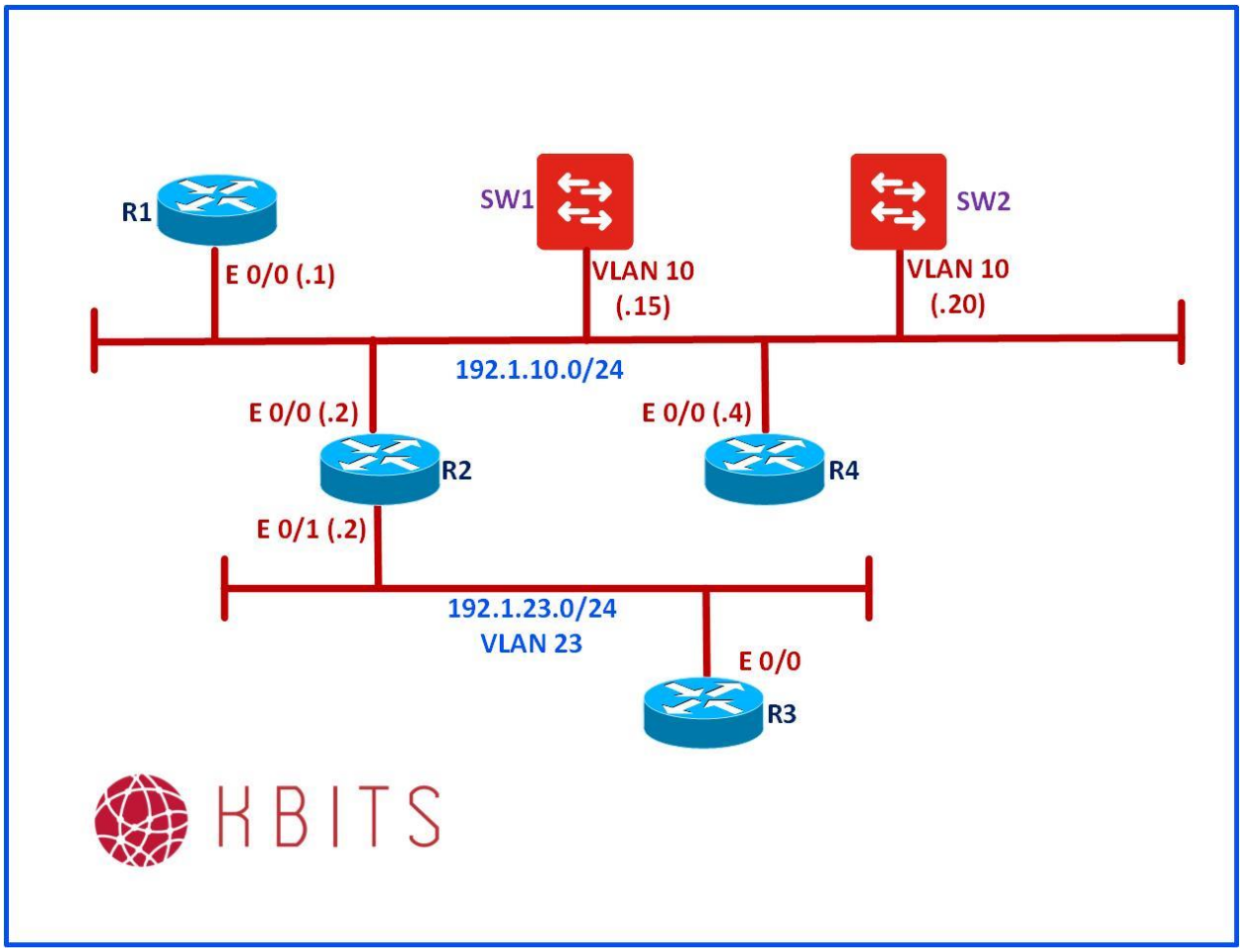
Task 3

Also configure R2 to send traps to the SNMP Management station when an IPSec tunnel comes up or goes down.

R2

```
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
```

Lab 4 – Blocking Unwanted Services on the Router



Lab Scenario:

- Disable the DHCP Server service on a Router.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Disable R4 from being a DHCP Server.

R4

```
No service dhcp
```

Task 2

R2 is sending unreachable messages if a packet is received that it cannot route. It should not send the icmp unreachable messages. Disable it on the Interface facing R3.

R2

```
Interface E 0/1
 No ip unreachables
```

Task 3

R2 is receiving a lot of packets with the IP option fields set. You deem these packets as attack packets. Drop any packet that has the IP option field set.

R2

```
Ip options drop
```

Task 4

R3 is receiving a lot of packets with the IP option fields set. You deem these packets as attack packets. Drop any packet that has the IP option field set. Allow traceroute, record-route & timestamp to work on R3.

R3

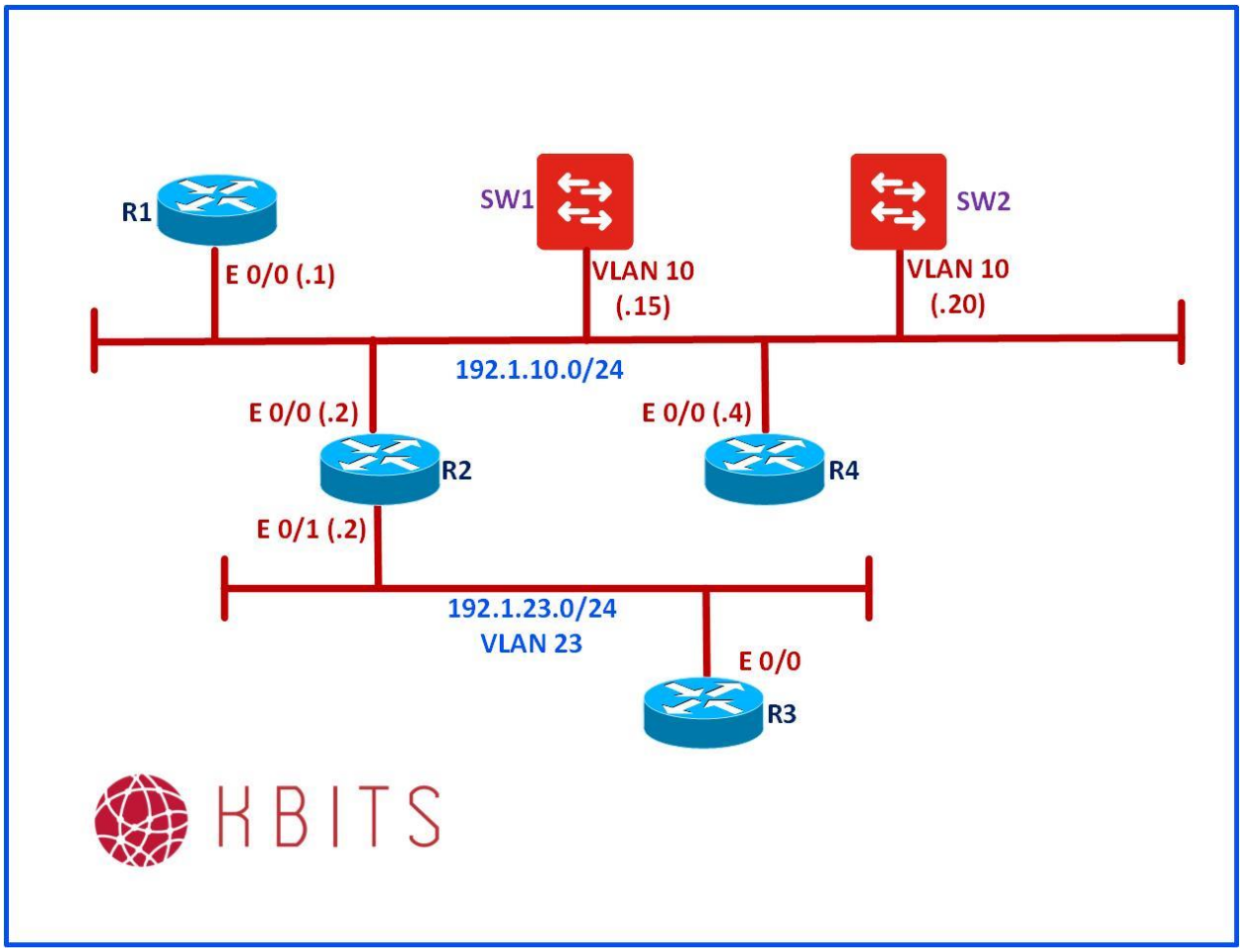
```
Ip access-list extended SEL-OPT
 permit ip any any option traceroute
 permit ip any any option record-route
 permit ip any any option timestamp
 deny ip any any option any-options
 permit ip any any
!
Interface E 0/0
 Ip access-group SEL-OPT in
```

Task 5

R1 is receiving a lot of packets with the source-route ip option used to control return paths. Disable this on R1.

R1
No ip source-route

Lab 5 – Configuring Syslog Settings



Lab Scenario:

- Configure the Archiving Feature on the Router to log Configuration changes to a TFTP Server.
- Enable Logging of changes to the running configuration file.
- Make sure the passwords do not get displayed when viewing the logged commands.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure R1 to create Archives of your configuration files. Store them on a tftp server located at 192.1.10.100. The name of the archive should be **MyConfigFiles**.

R1

```
archive
 path tftp://10.1.1.1/MyConfigFiles
```

Task 2

R1 should also log changes to the running config. Make sure the password are suppressed when displaying logged commands.

R1

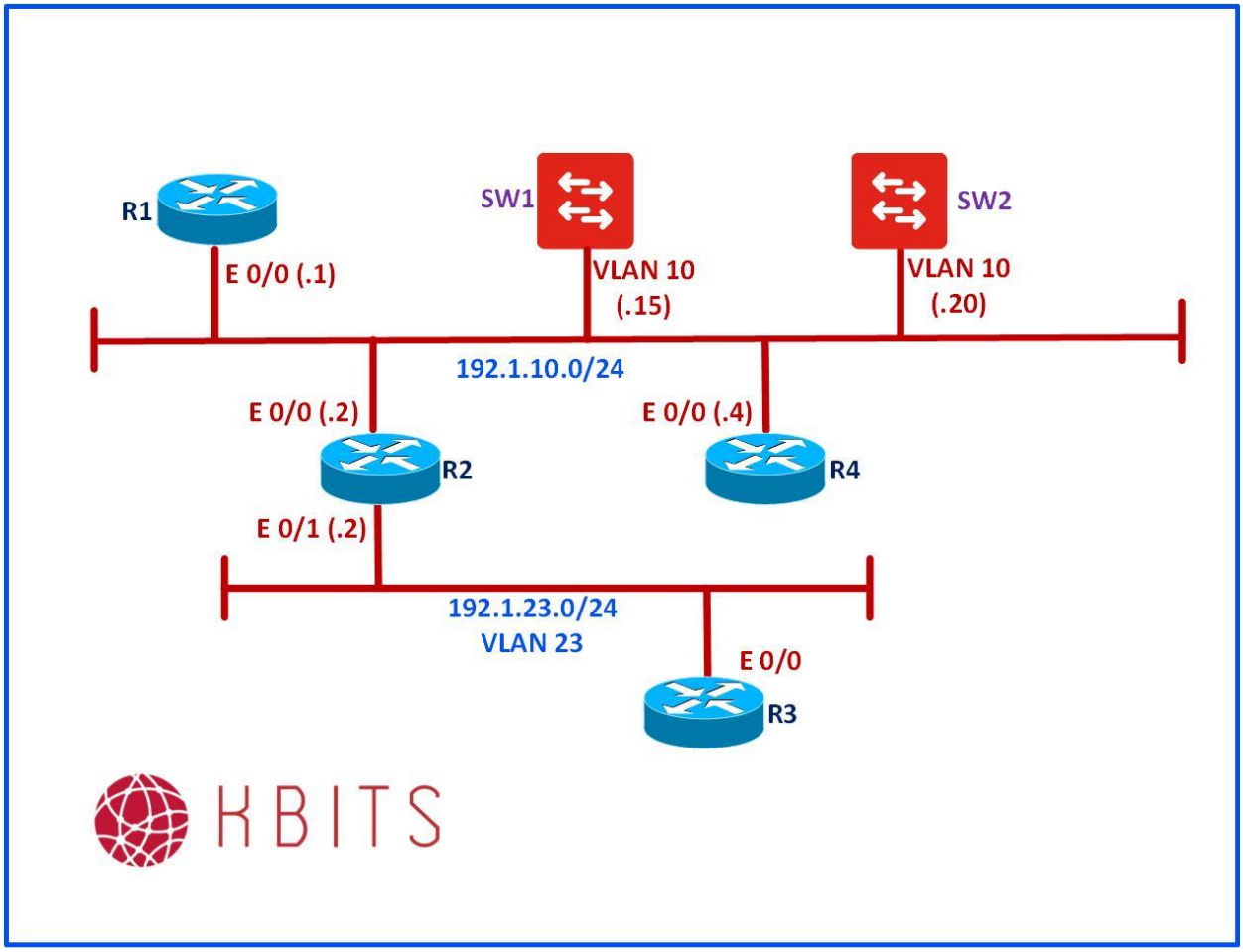
```
archive
 log config
   logging enable
   hidekeys
```

CCIE Security v6 – Configuring Router & Switch Security Features

Module 3 – Configuring Switch Security Features

Module 3 – Configuring Switch Security Features

Lab 1 – Configuring the Port-Security Feature on the Switch



Lab Scenario:

- Configuring the Port-Security feature on the Switch based on Static and Dynamic Mac-address configuration.
- Configure the Error Recovery feature to re-enable an error disabled port automatically.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure SW1 such that only R1 E0/0 and R2 E0/0 can connect to Ports E 0/0 and E 0/1 respectively. If another port tries to connect to these ports, they should be shudown.

SW1

```
Interface E 0/0
 Switchport port-security
 Switchport port-security mac xxxx.xxxx.xxxx
!
Interface E 0/1
 Switchport port-security
 Switchport port-security mac xxxx.xxxx.xxxx
```

Task 2

Configure Port security on Ports E 0/2 – 3. You would like to learn the MAC address dynamically and copy it to the running-configuration file.

SW1

```
Interface range E 0/2-3
 Switchport port-security
 Switchport port-security mac sticky
```

Task 3

Configure E 1/2 in VLAN 10 on SW1. Enable Port security for this port such that 5 MAC address can be connected to it. Configure 2 MAC Address (0001-1010-AB12 and 0001-10101-AB13) statically. The rest of the MAC addresses can be learned dynamically.

SW1

```
Interface E 1/2
 Switchport mode access
 Switchport access vlan 10
 Switchport port-security
 Switchport port-security max 5
 Switchport port-security mac xxxx.xxxx.xxxx
 Switchport port-security mac xxxx.xxxx.xxxx
 Switchport port-security mac sticky
```

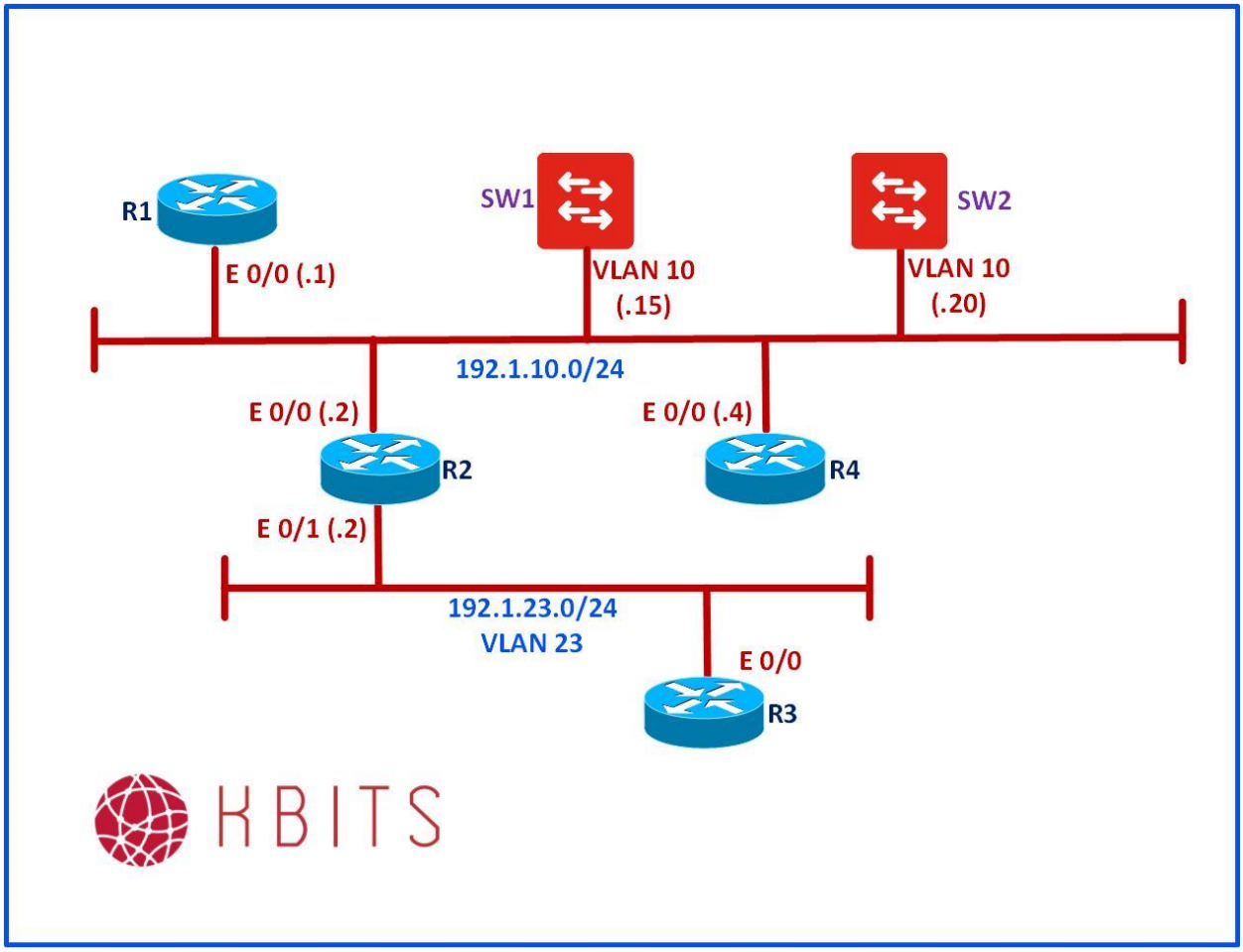
Task 4

Configure the Switch such that it tries to bring up the Port-security error disabled port automatically after 4 minutes.

SW1

```
errdisable recovery cause psecure-violation
errdisable recovery interval 240
```

Lab 2 – Preventing the Rogue DHCP Server Attack using the DHCP Snooping Feature



Lab Scenario:

- Configure the DHCP Snooping feature on the switch.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

All the SALES users will be in the SALES VLAN (100). Create this VLAN. Assign ports E 1/1-2 on SW2 to this VLAN.

SW1

```
VLAN 100
```

SW2

```
Interface range E 1/1-2
 Switchport mode access
 Switchport access vlan 100
```

Task 2

The DHCP server resides on the E1/3 on SW2. Assign this port to the SALES VLAN.

SW2

```
Interface E 1/3
 Switchport mode access
 Switchport access vlan 100
```

Task 3

Make sure the switch only allows DHCP replies from port E 1/3 on SW2.

SW2

```
Ip dhcp snooping
Ip dhcp snooping vlan 100
!
Interface E 1/3
 Ip dhcp snooping trust
```

Lab 3 – Configuring Static ARP Inspection Using an ARP ACL

Lab Scenario:

- Configuring the Switch for Static ARP Inspection to prevent ARP Spoofing attacks.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

There are 2 Servers connected to ports E 2/0 and E 2/1 on SW2 in VLAN 100. Assign ports E 2/0 – 1 to VLAN 100 on SW2 to this VLAN.

SW2

```
Interface range E 2/0-1
 Switchport mode access
 Switchport access vlan 100
```

Task 2

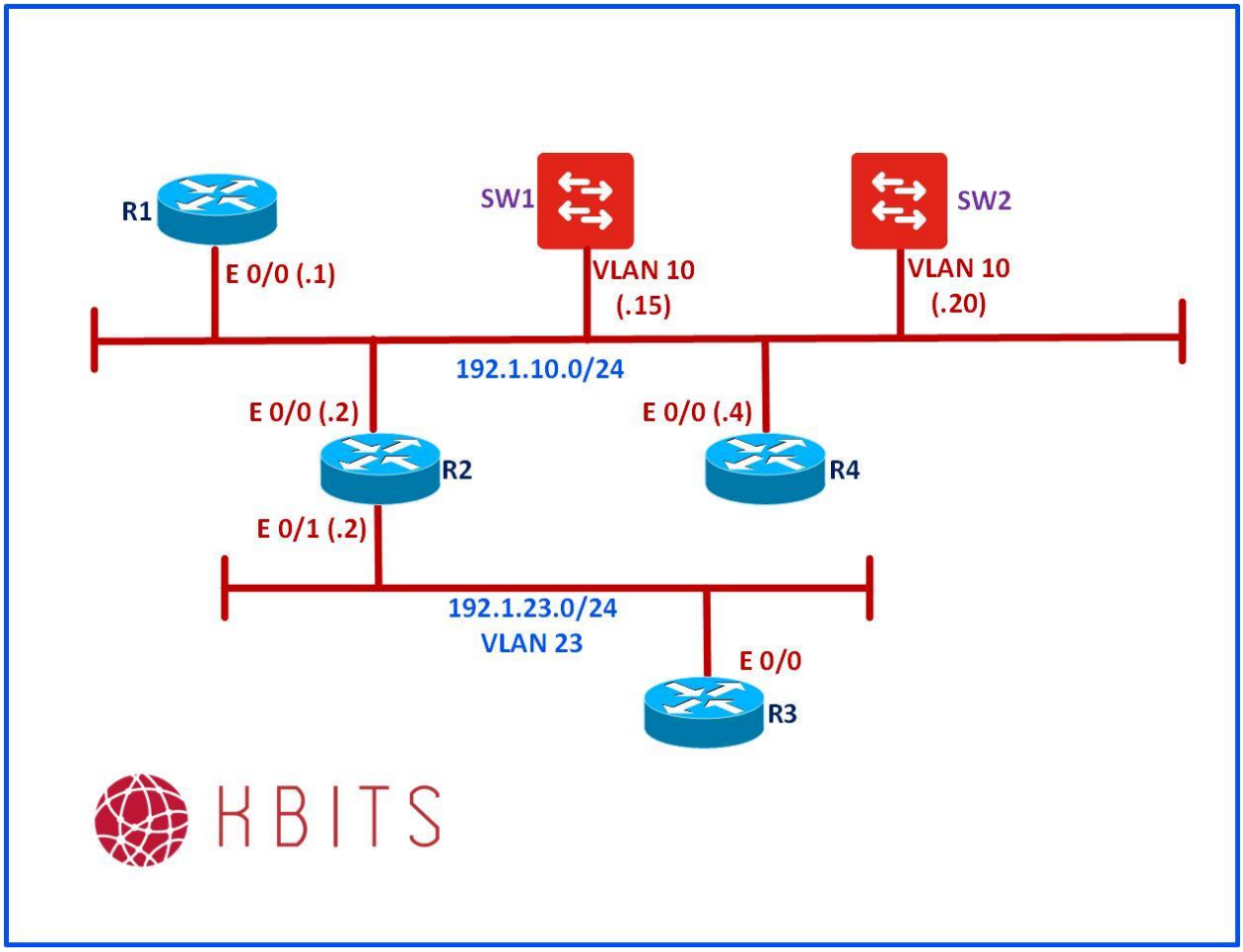
This VLAN is under the ARP Spoofing attack. Make sure that ARP Packets are inspected. The verification should be done based on the following table:

- Server 1: IP Address: 192.1.100.11 – MAC: 0001.1111.1211
- Server 2: IP Address: 192.1.100.12 – MAC: 0001.1111.1212
- Server 3: IP Address: 192.1.100.13 – MAC: 0001.1111.1213

SW2

```
arp access-list VLAN100
 permit ip host 192.1.100.11 mac host 0001.1111.1211
 permit ip host 192.1.100.12 mac host 0001.1111.1212
 permit ip host 192.1.100.13 mac host 0001.1111.1213
!
ip arp inspection vlan 100
ip arp inspection filter VLAN100 vlan 100 static
```

Lab 4 – Configuring Dynamic ARP Inspection (DAI)



Lab Scenario:

- Configuring the ARP Inspection feature using the MAC-IP Address database created by DHCP Snooping.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

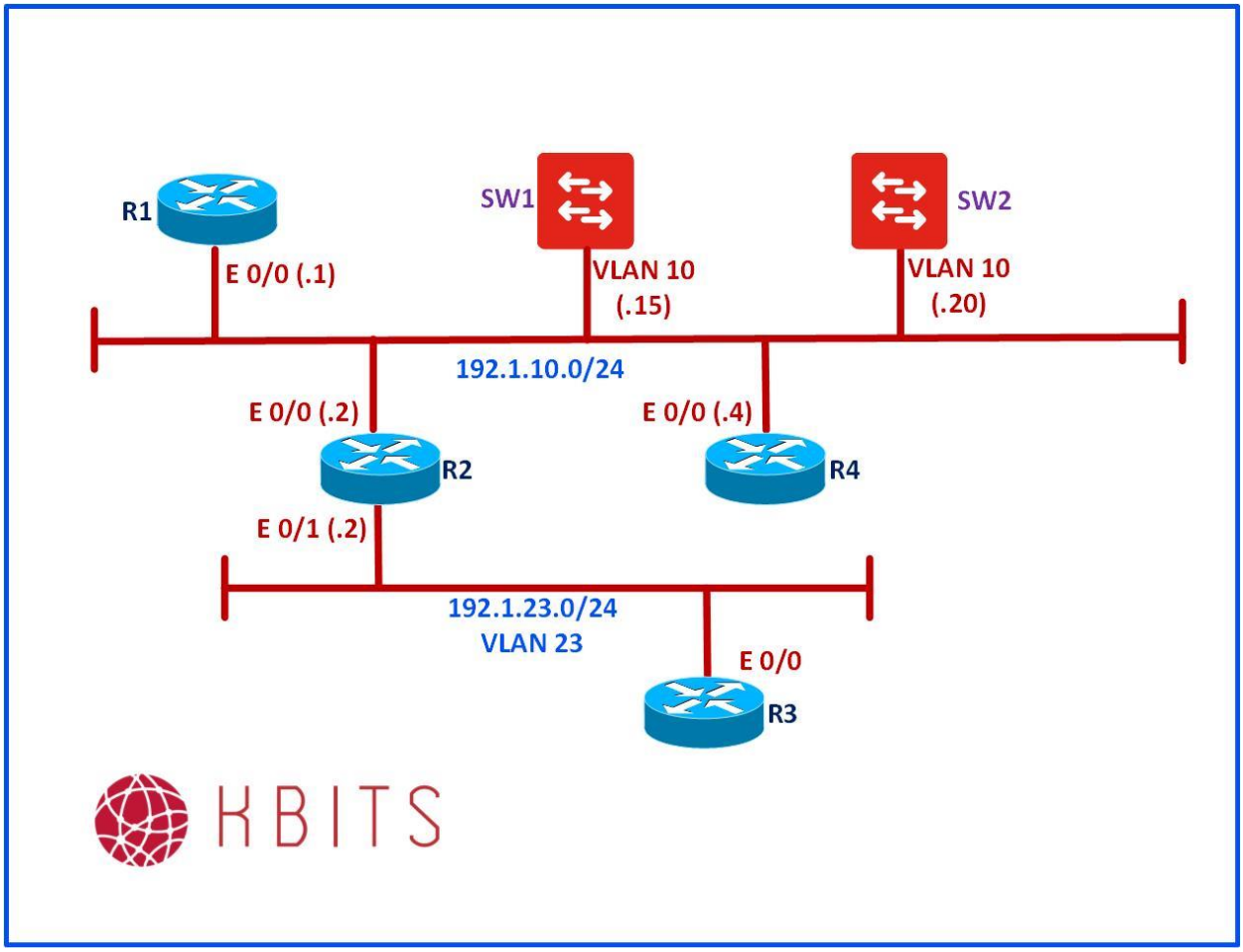
Task 1

Configure SW2 such that it intercepts all packets received on untrusted ports in VLAN 100. It should verify valid IP-MAC mappings against the DHCP Snooping Database. This database was created by enabling DHCP Snooping for VLAN 100 in a previous lab.

SW2

```
Ip arp inspection vlan 100
!
Interface E 1/3
 Ip arp inspection trust
```

Lab 5 – Configuring the Source Guard Feature



Lab Scenario:

- Configuring the Source Guard Feature to validate a device on a Switchport.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

There is a Server connected to port on SW2 in VLAN 100. Turn on the IP Source Guard feature on SW2 such that only this server connects up to E 2/3. This Server has a MAC address of 0001.1010.1020 and an IP address of 192.1.100.7.

SW2

```
ip source binding 0001.1010.1020 vlan 100 192.1.100.7 interface E 2/3
!
Interface E2/3
 Switchport mode access
 Switchport access vlan 100
 ip verify source
```

Lab 6 – Configuring VLAN ACL's

Lab Scenario:

- Configuring a VLAN ACL on the Switch to control traffic by filtering based on Layer 2 & Layer 3 characteristics.

Initial Setup:

- **Based on the previous Lab**

Lab Task:

Task 1

Configure the following policy for VLAN 100 on SW1.

- Hosts should not be able to use the IGMP and the ICMP protocols.
- There is a MAC Address 0001.0012.2222 trying to attack VLAN 100. Block this MAC address from accessing any device on VLAN 100.

Task 2

Use a VLAN ACL for this task.

SW1

```
Access-list 136 permit icmp any any
Access-list 136 permit igmp any any
!
mac access-list extended MAC-ACL
 permit host 0001.0012.2222 any
!
vlan access-map VLAN100 10
 action drop
 match ip address 136
!
vlan access-map VLAN100 20
 action drop
 match mac address MAC-ACL
!
vlan access-map VLAN100 1000
```

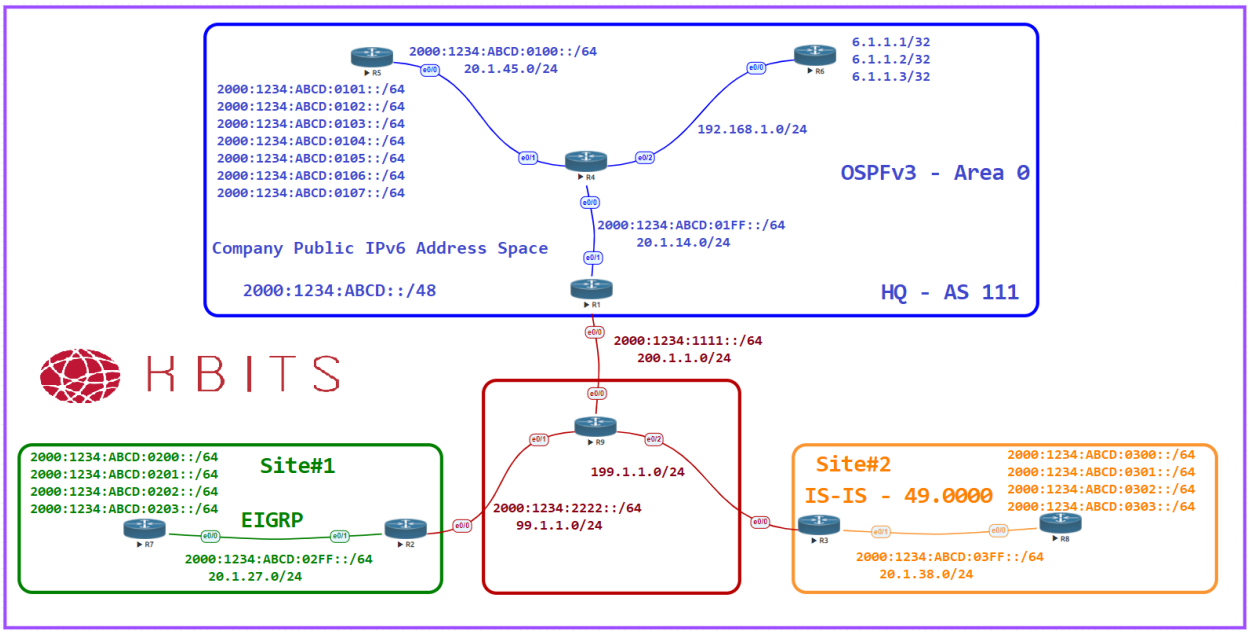
```
 action forward
!
vlan filter VLAN100 vlan-list 100
```

CCIE Security v6 – Configuring Router & Switch Security Features

Module 4 – Configuring IPv6

Module 4 – Configuring IPv6

Lab 2 – Configuring IPv6 Addressing



Task 1

Configure Headquarters with IPv6 addressing based on the Network Diagram. The Network between R4 & R6 will remain as IPv4 only. Configure the rest of the routers with IPv6 addressing based on the Network Diagram. Configure a default route on the Edge Router (R1) towards the ISP.

R1

```
ipv6 unicast-routing
!
Interface E 0/0
 ipv6 address 2000:1234:1111::1/64
 no shut
!
Interface E 0/1
 ipv6 address 2000:1234:ABCD:01FF::1/64
 no shut
!
ipv6 route ::/0 2000:1234:1111::9
```

R4

```
ipv6 unicast-routing
!
Interface E 0/0
 ipv6 address 2000:1234:ABCD:01FF::4/64
```

```
 no shut
!
Interface E 0/1
 ipv6 address 2000:1234:ABCD:0100::4/64
 no shut
```

R5

```
ipv6 unicast-routing
!
Interface E 0/0
 ipv6 address 2000:1234:ABCD:0100::5/64
 no shut
!
Interface Loopback1
 ipv6 address 2000:1234:ABCD:0101::5/64
!
Interface Loopback2
 ipv6 address 2000:1234:ABCD:0102::5/64
!
Interface Loopback3
 ipv6 address 2000:1234:ABCD:0103::5/64
!
Interface Loopback4
 ipv6 address 2000:1234:ABCD:0104::5/64
!
Interface Loopback5
 ipv6 address 2000:1234:ABCD:0105::5/64
!
Interface Loopback6
 ipv6 address 2000:1234:ABCD:0106::5/64
!
Interface Loopback7
 ipv6 address 2000:1234:ABCD:0107::5/64
```

Task 2

Configure **Site#1** with IPv6 addressing based on the Network Diagram. Configure a default route on the Edge Router (R2) towards the ISP.

R2

```
Interface E 0/0
 ipv6 address 2000:1234:2222::2/64
 no shut
!
Interface E 0/1
```

```
 ipv6 address 2000:1234:ABCD:02FF::2/64
 no shut
!
ipv6 route ::/0 2000:1234:2222::9
```

R7

```
ipv6 unicast-routing
!
Interface E 0/0
 ipv6 address 2000:1234:ABCD:02FF::7/64
 no shut
!
Interface Loopback1
 ipv6 address 2000:1234:ABCD:0200::7/64
!
Interface Loopback2
 ipv6 address 2000:1234:ABCD:0201::7/64
!
Interface Loopback3
 ipv6 address 2000:1234:ABCD:0202::7/64
!
Interface Loopback4
 ipv6 address 2000:1234:ABCD:0203::7/64
```

Task 3

Configure **Site#2** with IPv6 addressing based on the Network Diagram.

R3

```
ipv6 unicast-routing
!
Interface E 0/1
 ipv6 address 2000:1234:ABCD:03FF::3/64
 no shut
```

R8

```
ipv6 unicast-routing
!
Interface E 0/0
 ipv6 address 2000:1234:ABCD:03FF::8/64
 no shut
!
Interface Loopback1
 ipv6 address 2000:1234:ABCD:0300::8/64
!
```

```
Interface Loopback2
 ipv6 address 2000:1234:ABCD:0301::8/64
!
Interface Loopback3
 ipv6 address 2000:1234:ABCD:0302::8/64
!
Interface Loopback4
 ipv6 address 2000:1234:ABCD:0303::8/64
```

Task 4

Configure IPv4 IP Addresses based on the network diagram. Configure Static Routing to provide full reachability for IPv4 networks. You are allowed to use static routes.

R1

```
Interface E 0/0
 Ip address 200.1.1.1 255.255.255.0
 No shut
!
Interface E 0/1
 Ip address 20.1.14.1 255.255.255.0
 No shut
!
Ip route 0.0.0.0 0.0.0.0 200.1.1.9
Ip route 20.1.45.0 255.255.255.0 20.1.14.4
Ip route 6.1.1.0  255.255.255.0 20.1.14.4
```

R2

```
Interface E 0/0
 Ip address 99.1.1.2 255.255.255.0
 No shut
!
Interface E 0/1
 Ip address 20.1.27.2 255.255.255.0
 No shut
!
Ip route 0.0.0.0 0.0.0.0 99.1.1.9
```

R3

```
Interface E 0/0
 Ip address 199.1.1.3 255.255.255.0
 No shut
!
Interface E 0/1
```

```
 Ip address 20.1.38.3 255.255.255.0
 No shut
!
Ip route 0.0.0.0 0.0.0.0 199.1.1.9
```

R4

```
Interface E 0/0
 Ip address 20.1.14.4 255.255.255.0
 No shut
!
Interface E 0/1
 Ip address 20.1.45.4 255.255.255.0
 No shut
!
Interface E 0/2
 Ip address 192.168.1.4 255.255.255.0
 No shut
!
Ip route 0.0.0.0 0.0.0.0 20.1.14.1
Ip route 6.1.1.0 255.255.255.0 192.168.1.6
```

R5

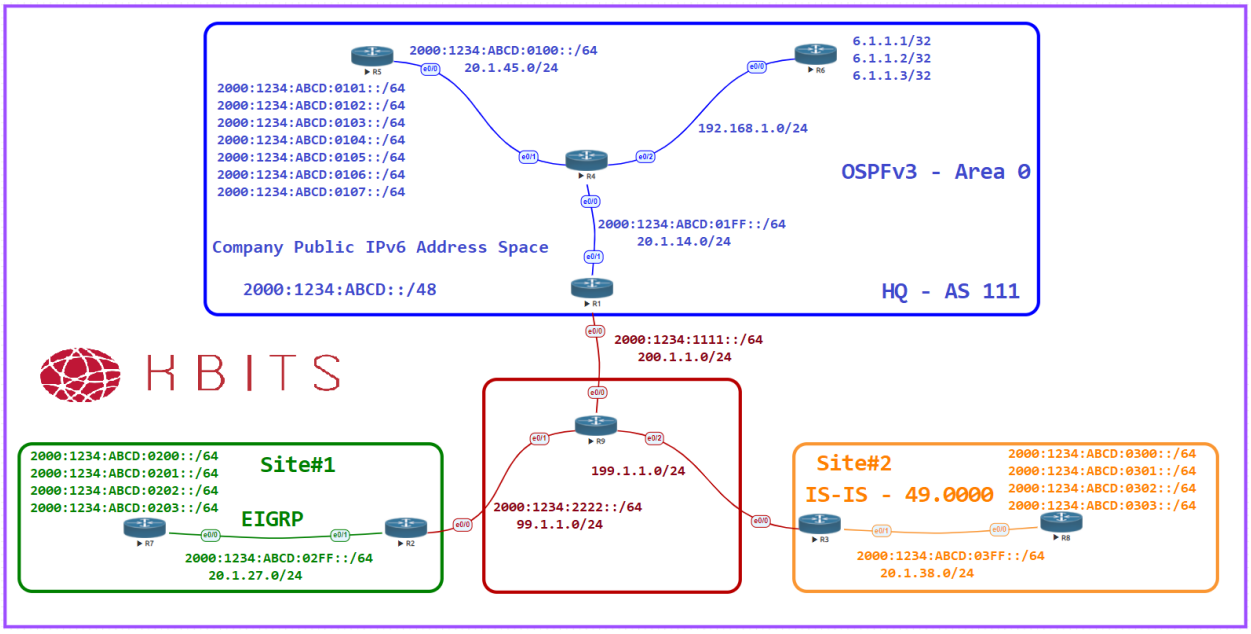
```
Interface E 0/0
 Ip address 20.1.45.5 255.255.255.0
 No shut
!
Ip route 0.0.0.0 0.0.0.0 20.1.45.4
```

R6

```
Interface E 0/0
 Ip address 192.168.1.6 255.255.255.0
 No shut
!
Interface Loo1
 Ip address 6.1.1.1 255.255.255.255
!
Interface Loo2
 Ip address 6.1.1.2 255.255.255.255
!
Interface Loo3
 Ip address 6.1.1.3 255.255.255.255
!
Ip route 0.0.0.0 0.0.0.0 192.168.1.4
!
Line vty 0 4
```

Password cisco Login Transport input all
R7 Interface E 0/0 Ip address 20.1.27.7 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 20.1.27.2
R8 Interface E 0/0 Ip address 20.1.38.8 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 20.1.38.3
R9 Interface E 0/0 Ip address 200.1.1.9 255.255.255.0 No shut ! Interface E 0/1 Ip address 99.1.1.9 255.255.255.0 No shut ! Interface E 0/2 Ip address 199.1.1.9 255.255.255.0 No shut ! Ip route 20.1.14.0 255.255.255.0 200.1.1.1 Ip route 20.1.45.0 255.255.255.0 200.1.1.1 Ip route 6.1.1.0 255.255.255.0 200.1.1.1 Ip route 20.1.27.0 255.255.255.0 99.1.1.2 Ip route 20.1.38.0 255.255.255.0 199.1.1.3

Lab 2 – Configuring OSPFv3



Task 1

Configure Headquarters with OSPFv3 within the HQ Site. Use X.X.X.X. as the router-id. (X stands for the Router #). Enable all the IPv6 addresses within the HQ site in OSPF. Have R1 inject a default route towards R4. The loopback interfaces should appear in the routing table using the interface mask.

R1

```
ipv6 router ospf 1
 router-id 1.1.1.1
 default-information originate always
!
Interface E 0/1
 ipv6 ospf 1 area 0
```

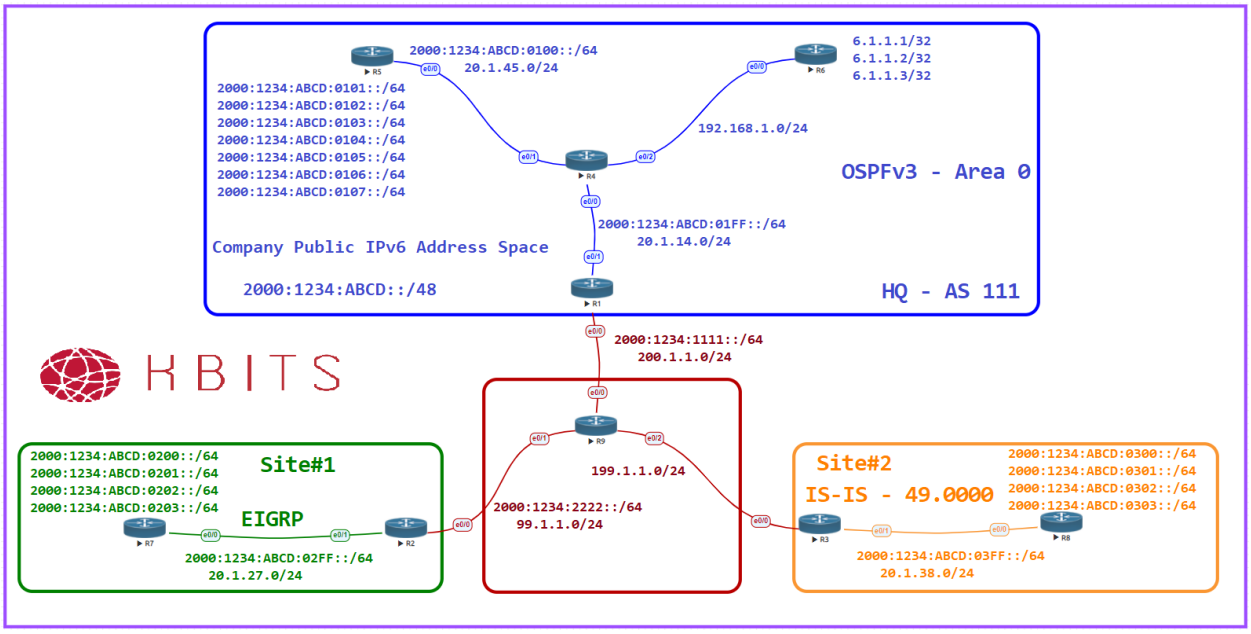
R4

```
ipv6 router ospf 1
 router-id 4.4.4.4
!
Interface E 0/0
 ipv6 ospf 1 area 0
!
Interface E 0/1
 ipv6 ospf 1 area 0
```

R5

```
ipv6 router ospf 1
 router-id 5.5.5.5
!
Interface E 0/0
 ipv6 ospf 1 area 0
!
Interface Loopback 1
 ipv6 ospf 1 area 0
 ipv6 ospf network point-to-point
!
Interface Loopback 2
 ipv6 ospf 1 area 0
 ipv6 ospf network point-to-point
!
Interface Loopback 3
 ipv6 ospf 1 area 0
 ipv6 ospf network point-to-point
!
Interface Loopback 4
 ipv6 ospf 1 area 0
 ipv6 ospf network point-to-point
!
Interface Loopback 5
 ipv6 ospf 1 area 0
 ipv6 ospf network point-to-point
!
Interface Loopback 6
 ipv6 ospf 1 area 0
 ipv6 ospf network point-to-point
!
Interface Loopback 7
 ipv6 ospf 1 area 0
 ipv6 ospf network point-to-point
```

Lab 3 – Configuring EIGRP for IPv6



Task 1

Configure EIGRP 222 within Site#1. Use X.X.X.X. as the router-id. (X stands for the Router #). Enable all the IPv6 addresses within Site#1 in EIGRP. Configure a default route on R7 towards R2.

R2

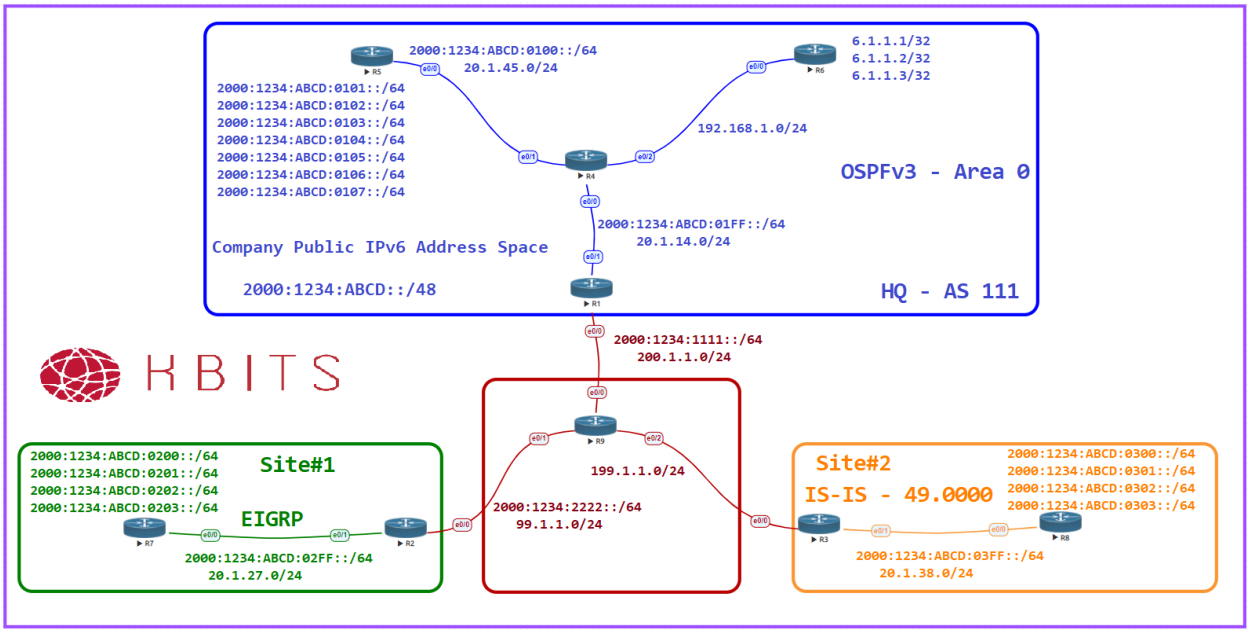
```
ipv6 router eigrp 222
 router-id 2.2.2.2
!
Interface E 0/1
 ipv6 eigrp 222
```

R7

```
ipv6 router eigrp 222
 router-id 7.7.7.7
!
Interface E 0/0
 ipv6 eigrp 222
!
Interface Loopback 1
 ipv6 eigrp 222
!
Interface Loopback 2
 ipv6 eigrp 222
```

```
!
Interface Loopback 3
 ipv6 eigrp 222
!
Interface Loopback 4
 ipv6 eigrp 222
!
Ipv6 route ::/0 2000:1234:ABCD:02FF::2
```

Lab 4 – Configuring IS-IS for IPv6



Task 1

Configure IS-IS within Site#1 based on the diagram. Use XXXX.XXXX.XXXX. as the System-id. (X stands for the Router #). Enable all the IPv6 addresses within Site#1 in IS-IS. Configure the Routers as Level-2 Routers with a metric-style of wide. Configure a default route on R7 towards R2.

R3

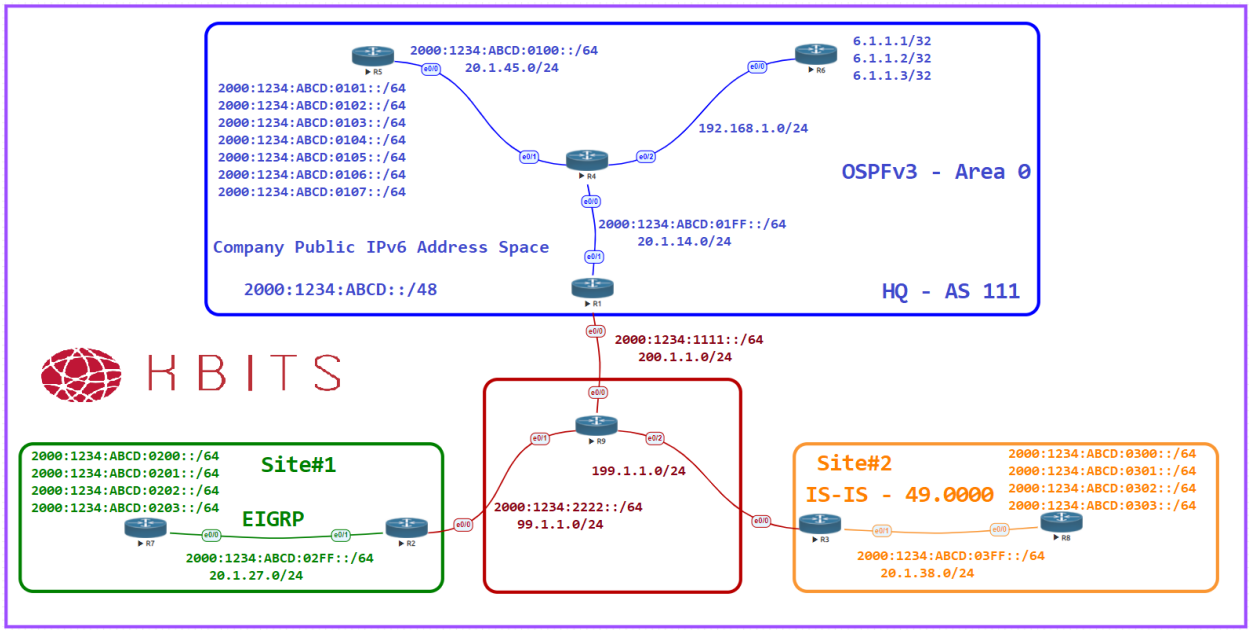
```
router isis
 net 49.0000.3333.3333.3333.00
 is-type level-2-only
 metric-style wide
!
address-family ipv6
  multi-topology
!
Interface E 0/1
 Ipv6 router isis
```

R8

```
router isis
 net 49.0000.8888.8888.8888.00
 is-type level-2-only
 metric-style wide
!
```

```
 address-family ipv6
  multi-topology
!
Interface E 0/0
 Ipv6 router isis
!
Interface Loopback 1
Ipv6 router isis
!
Interface Loopback 2
 Ipv6 router isis
!
Interface Loopback 3
 Ipv6 router isis
!
Interface Loopback 4
 Ipv6 router isis
!
Ipv6 route ::/0 2000:1234:ABCD:03FF::3
```

Lab 5 – Configuring BGP for IPv6



Task 1

Configure BGP between R1 & R9. Configure R1 in AS 111. Redistribute the internal networks to BGP and vice versa.

R1

```
router bgp 111
 neighbor 2000:1234:1111::9 remote-as 1000
 address-family ipv6
  neighbor 2000:1234:1111::9 activate
  redistribute ospf 1
!
ipv6 router ospf 1
 redistribute bgp 111
```

R9

```
router bgp 1000
 neighbor 2000:1234:1111::1 remote-as 111
 address-family ipv6
  neighbor 2000:1234:1111::1 activate
```

Task 2

Configure BGP between R2 & R9. Configure R2 in AS 222. Redistribute the internal networks to BGP and vice versa.

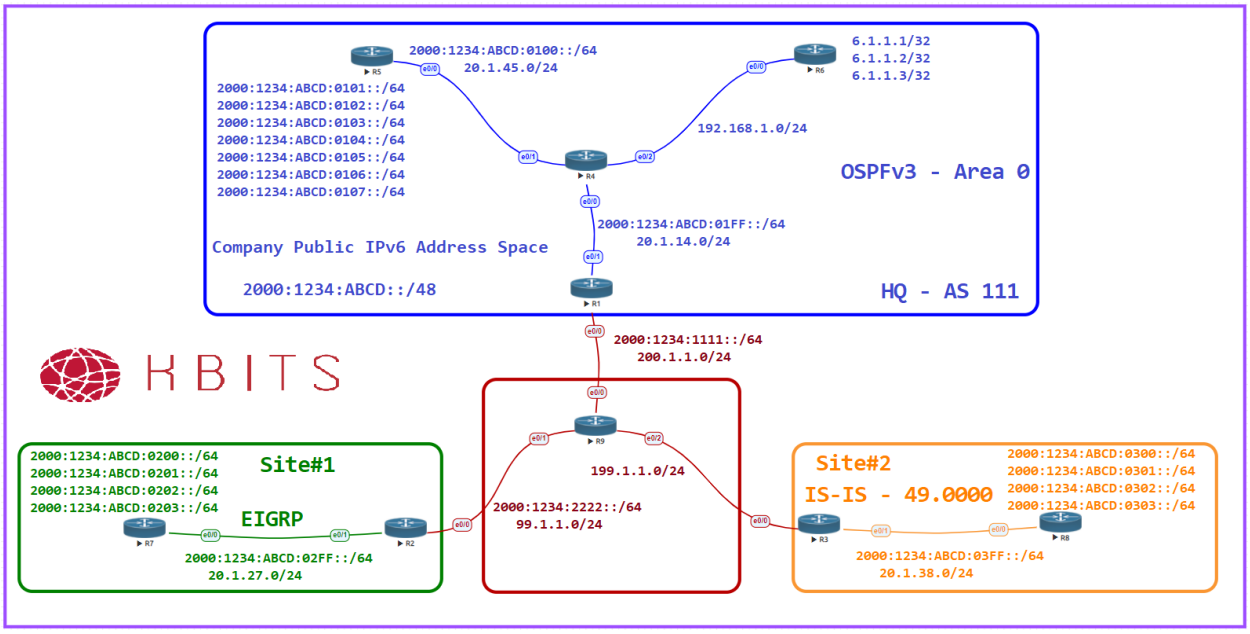
R2

```
router bgp 111
 neighbor 2000:1234:2222::9 remote-as 1000
 address-family ipv6
  neighbor 2000:1234:2222::9 activate
  redistribute eigrp 222
!
ipv6 router eigrp 222
 redistribute bgp 222 metric 10 10 10 10 10
```

R9

```
router bgp 1000
 neighbor 2000:1234:2222::2 remote-as 222
 address-family ipv6
  neighbor 2000:1234:2222::2 activate
```

Lab 6 – Configuring IPv6IP Tunneling



Task 1

Configure a IPv6IP tunnel to connect R1 to R3. Use the 2000:1234:ABCD:01FE::/64 as the Tunnel Network. Enable the Tunnel Interface in OSPF.

R1

```
Interface tunnel 1
 tunnel source 200.1.1.1
 tunnel destination 199.1.1.3
 tunnel mode ipv6ip
 ipv6 address 2000:1234:ABCD:01FE::1/64
 ipv6 ospf 1 area 0
```

R3

```
Interface tunnel 1
 tunnel source 199.1.1.3
 tunnel destination 200.1.1.1
 tunnel mode ipv6ip
 ipv6 address 2000:1234:ABCD:01FE::3/64
 ipv6 ospf 1 area 0
```

Task 2

Configure route redistribution on R3 between OSPF and IS-IS.

R3

```
Ipv6 router ospf 1
 Redistribute isis
!
Router isis
 Address-family ipv6 unicast
  Redistribute ospf 1
```

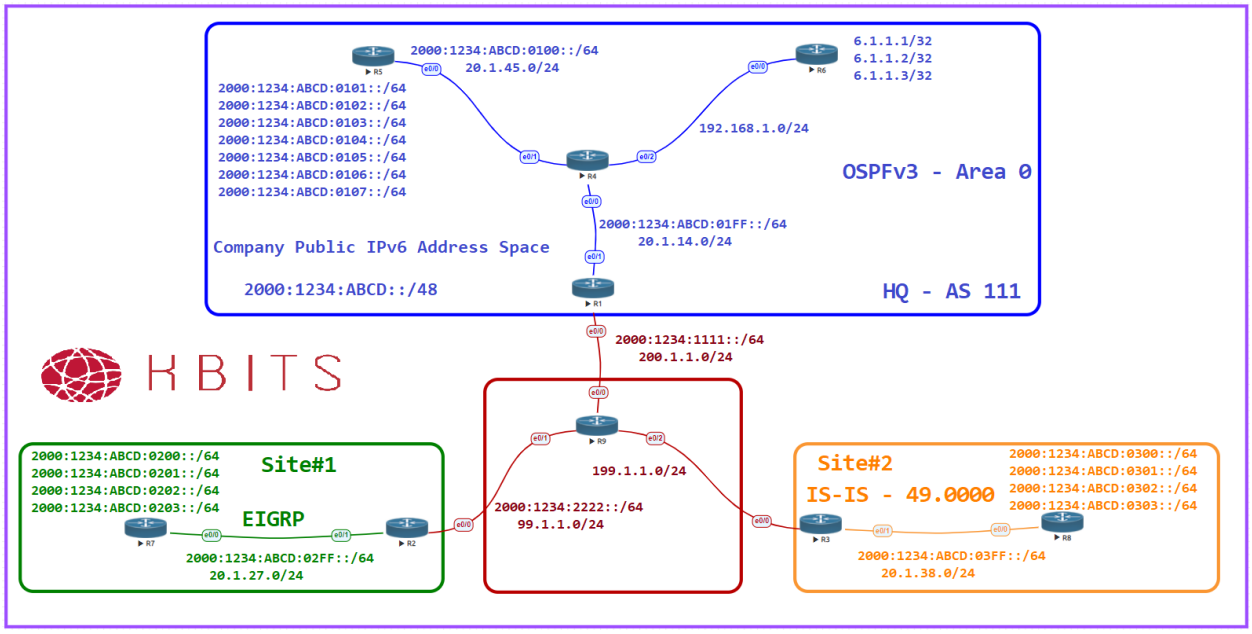
Task 3

Configure route redistribution on R1 between OSPF and BGP for external OSPF routes as well.

R1

```
Router bgp 111
 Address-family ipv6
  Redistribute ospf 1 match internal external
```

Lab 7 – Configuring NAT64



Task 1

Enable NAT64 on all Interfaces on R4.

R4

```
Interface E0/0
 nat64 enable
!
Interface E0/1
 nat64 enable
!
Interface E0/2
 nat64 enable
```

Task 2

Dedicate an IPv6 network prefix for NAT64

R4

```
nat64 prefix stateful 2000:1234:ABCD:0400::/64
```

Task 3

Inject the NAT64 into the IPv6 network by creating a Null 0 route for it and redistributing it into BGP. Allow this route to redistributed into BGP on R1.

R4

```
ipv6 route 2000:1234:ABCD:400::/64 Null0
ipv6 router ospf 1
 redistribute static
```

R1

```
Router bgp 111
 Address-family ipv6
  Redistribute ospf 1 match internal external
```

Task 4

Configure Static NAT for IPv4 Servers. Translate to the following:

- 6.1.1.1 – 2000:1234:ABCD:0400::1
- 6.1.1.2 – 2000:1234:ABCD:0400::2
- 6.1.1.2 – 2000:1234:ABCD:0400::3

R4

```
nat64 v4v6 static 6.1.1.1 2000:1234:ABCD:0400::1
nat64 v4v6 static 6.1.1.2 2000:1234:ABCD:0400::2
nat64 v4v6 static 6.1.1.3 2000:1234:ABCD:0400::3
```

Task 5

Configure Dynamic PAT for your networks (2000:1234:ABCD::/64 to a pool of 10.10.10.1 & 10.10.10.2.

R4

```
ipv6 access-list IPV6LIST
 permit ip 2000:1234:ABCD::/48 any
!
nat64 v4 pool V4POOL 10.10.10.1 10.10.10.2
!
nat64 v6v4 list IPV6LIST pool V4POOL overload
```