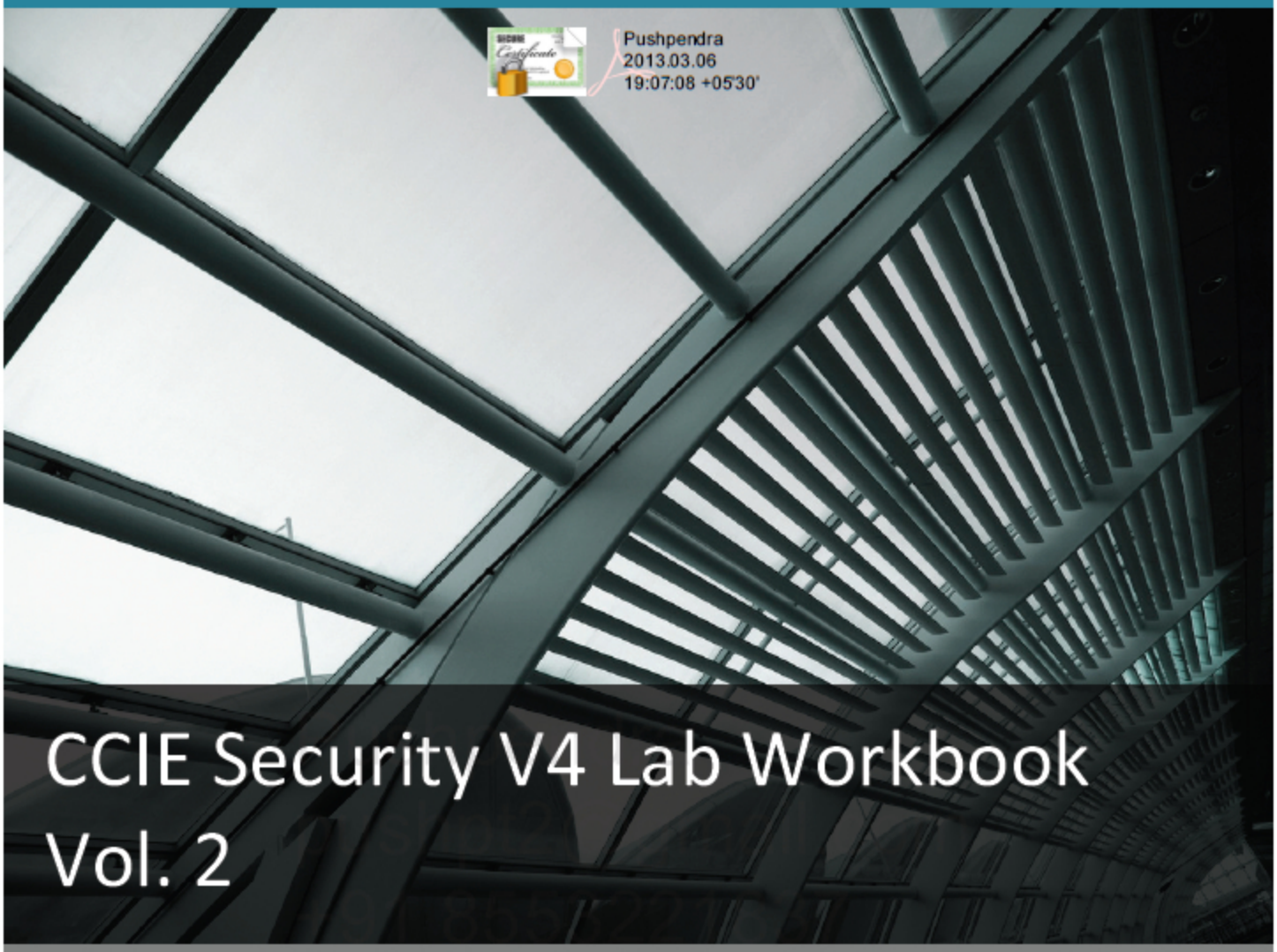



# CCIE Security V4 Lab Workbook Vol. 2

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

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

# Table of Contents

## Content Security - IPS

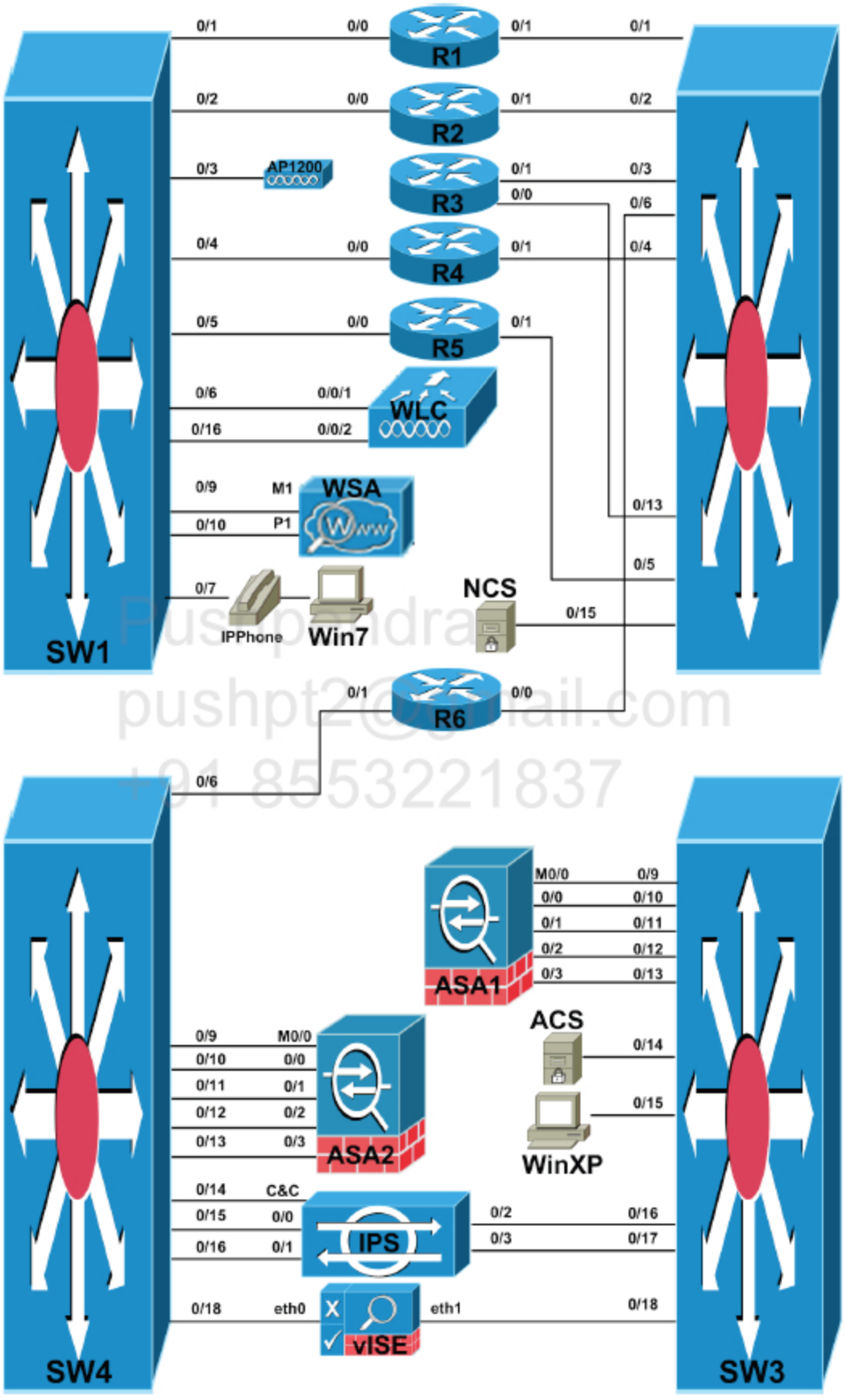




## Content Security - WSA

## Identity Management - ACS

# Physical Topology



# Advanced
# CCIE SECURTY v4
# LAB WORKBOOK

# Content Security

# IPS

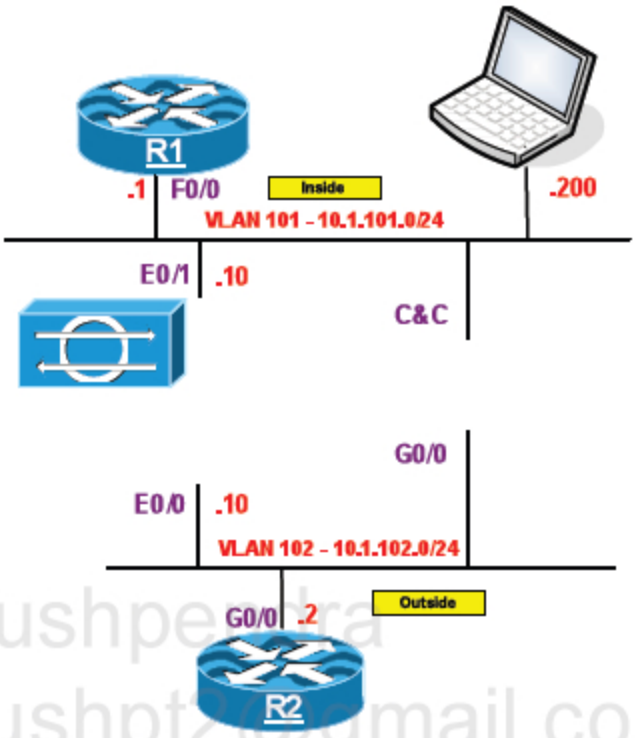


**Narbik Kocharians**
**CCIE #12410 (R&S, Security, SP)**
**CCSI #30832**

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

www.MicronicsTraining.com

# LAB 2.1. Sensor Initialization






## Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- R2's G0/0 and ASA's E0/0 interface should be configured in VLAN 102
- PC should be configured in VLAN 101
- IPS Command and Control (C&C) interface should be configured in VLAN 101
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices (except PC and IPS)

## IP Addressing

| Hostname | Interface (ifname) | IP address |
|---|---|---|
| R1 | F0/0 | 10.1.101.1 /24 |
| R2 | G0/0 | 10.1.102.2 /24 |
| ASA-FW | E0/0 (Outside, Security 0)<br>E0/1 (Inside, Security 100) | 10.1.102.10 /24<br>10.1.101.10 /24 |

## Task 1

Configure IPS Sensor with the following settings:

Hostname: IPS-CCIE

IP address: 10.1.101.100/24

Default Gateway: 10.1.101.10

Allowed Hosts: 10.1.101.200

Configure IPS management interface (m0/0) in VLAN 101.

*The Cisco IPS must be correctly pre-configured in order to make it available in the network and manage it using GUI called IDM (IPS Device Manager). Although, many configuration things may be done from the CLI, the IDM is more user-friendly and easy to use. The IDM is available during the lab exam.*

*A basic configuration must be done from CLI after first connection through the console. Just after login the Setup script launches and asks for basic settings like: management IP address, default gateway (the IPS does not use dynamic nor static routes) and allowed hosts from which we can manage using IDM. After a few basic steps, the IPS is ready to connect to it using IDM.*

*All basic setup configuration is related to C&C (Command & Control) management interface.*



## Configuration

Complete these steps:

**Step 1** IPS first configuration.

```
sensor login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
```

```
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.


    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Sat Feb  6 11:10:51 2010

Setup Configuration last modified: Sat Feb 06 11:03:34 2010

Enter host name[sensor]: IPS-CCIE
Enter IP interface[192.168.1.2/24,192.168.1.1]:
10.1.101.100/24,10.1.101.10

        Note that you must write all information in one line without any
        spaces.

Modify current access list?[no]: yes

        To modify an ACL for management purposes you must answer "yes"
        for above question.

Current access list entries:
  No entries
Permit: 10.1.101.200/32

        If you want to configure only one host, you must provide /32
        mask. If you want to configure whole network use a network
        address with correct mask. Hit enter twice when finished.

Permit:
Modify system clock settings?[no]:

The following configuration was entered.

service host
network-settings
host-ip 10.1.101.100/24,10.1.101.10
host-name IPS-CCIE
telnet-option disabled
access-list 10.1.101.200/32
ftp-timeout 300
```

```
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.

Enter your selection[3]: 2

        Select second option to save basic config and end Setup utility.

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.

sensor#
```



## Verification

```
sensor# exi


IPS-CCIE login: cisco
Password:

        Note that sensor name is refreshed after relogin.

Last login: Sat Feb  6 11:10:50 on ttyS0
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
IPS-CCIE# sh configuration
! ------------------------------
! Current configuration last modified Sat Feb 06 11:11:59 2010
! ------------------------------
! Version 6.1(2)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S372.0   2008-12-10
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.1.101.100/24,10.1.101.10
host-name IPS-CCIE
access-list 10.1.101.200/32
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
```

```
! ------------------------------
service signature-definition sig1
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service analysis-engine
exit
```



```
IPS-CCIE# ping 10.1.101.1
PING 10.1.101.1 (10.1.101.1): 56 data bytes
64 bytes from 10.1.101.1: icmp_seq=0 ttl=255 time=2.8 ms
64 bytes from 10.1.101.1: icmp_seq=1 ttl=255 time=1.4 ms
64 bytes from 10.1.101.1: icmp_seq=2 ttl=255 time=0.7 ms
64 bytes from 10.1.101.1: icmp_seq=3 ttl=255 time=1.4 ms

--- 10.1.101.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.5/2.8 ms
IPS-CCIE#
```

You may ping the sensor from the management station. This ping works only from IP addresses provided in management ACL.

## Task 2

Using graphical user interface (GUI), configure IPS Sensor to allow management via TELNET (port 23) and HTTPS on port 8090. Disable password recovery function.

*The standard IPS management tool is IDM which is available using web browser and uses HTTPS for secure connectivity. It uses standard HTTPS port of 443 but can (should) be altered. Also there is a way for enabling TELNET access (not recommended in real world scenarios). All those settings can be done from CLI but we will use IDM.*

## Configuration

Complete these steps:

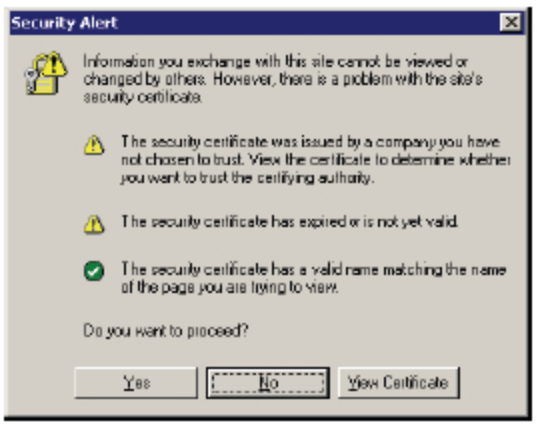
**Step 1** IPS GUI.

1. ***Configure IP address of 10.1.101.200/24 on the ACS/PC host.***

```
C:\>ipconfig

Windows IP Configuration
Ethernet adapter Lab Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 10.1.101.200
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

<output ommited>
```



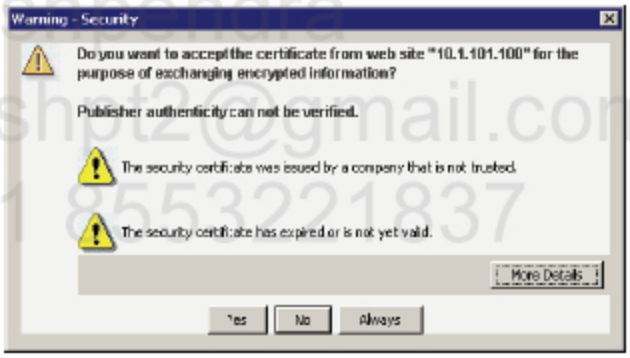
2. ***Run IE/FF (Internet Explorer/FireFox) and go to https://10.1.101.100. Accept security warning message.***



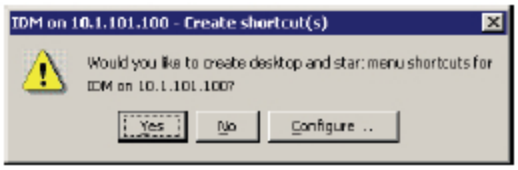

3. ***Click on Run IDM to download and run ActiveX applet.***


**4. *Accept a series of warining messgaes.***



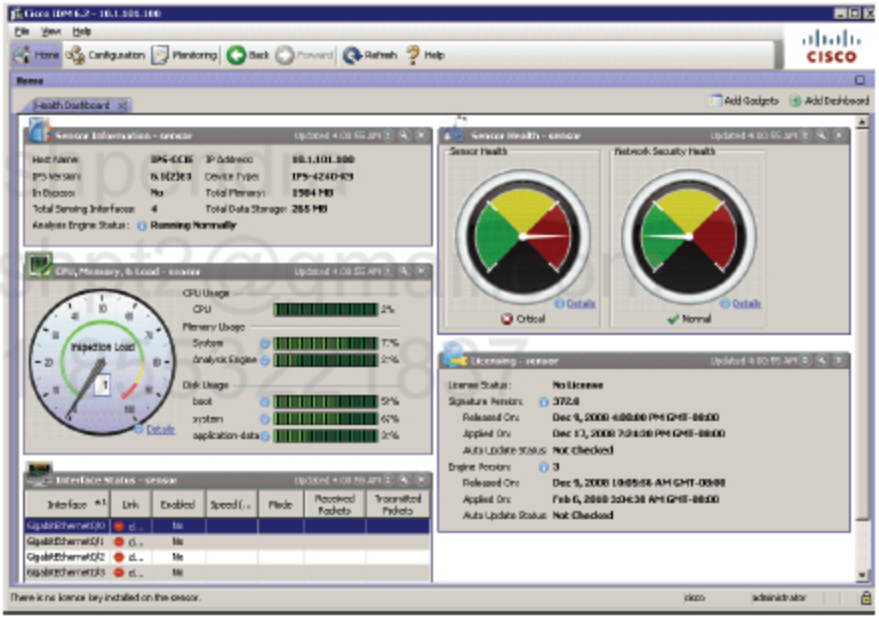




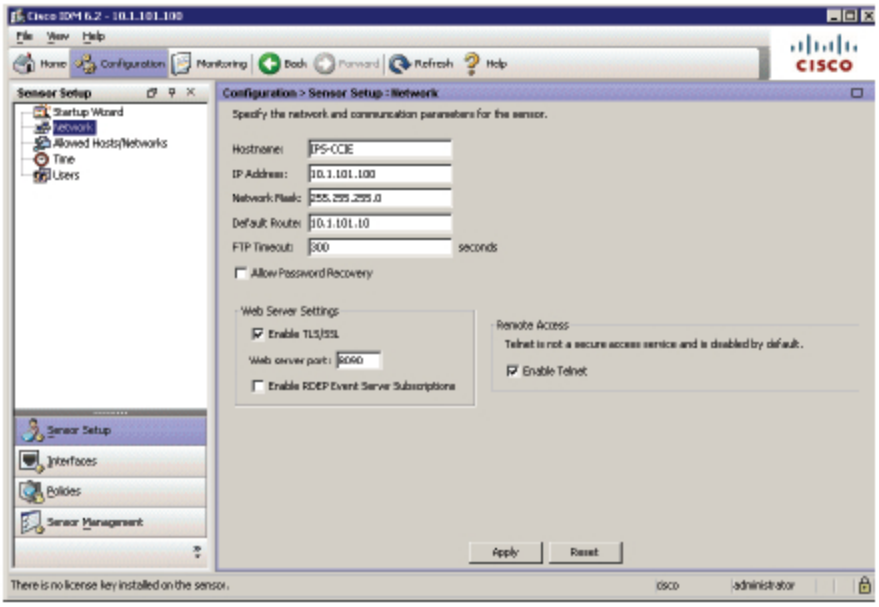


5. *Provide user and password.*


6. *After successful logging you should see IPS Dashboard.*




7. *Click on Configuration → Network and change settings as follows.*




***You must close IDM and open it up again to make changes to the IPS configuration. You will see an error message saying that IME cannot retrieve IPS configuration.***




8. ***Use https://10.1.101.100:8090 in you web browser to connect to the sensor.***




## Task 3

Configure IPS as NTP client to NTP server located on R1 and change the timezone to GMT+1. Add the following users to the sensor:

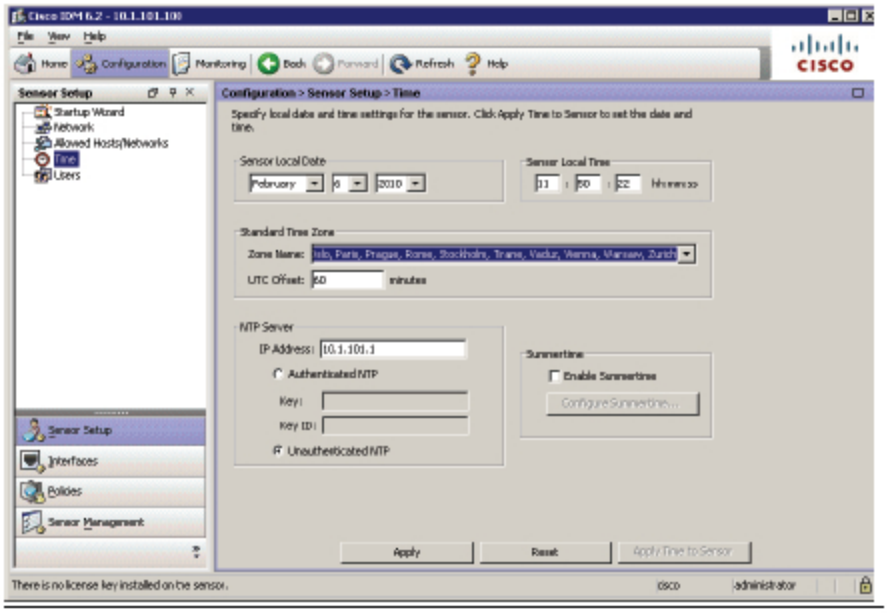
| Username | Role | Password |
|---|---|---|
| ipsadmin | Administrator | Admin1234 |
| ipsoper | Operator | Oper1234 |
| ipsview | Viewer | View1234 |

## Configuration

Complete these steps:

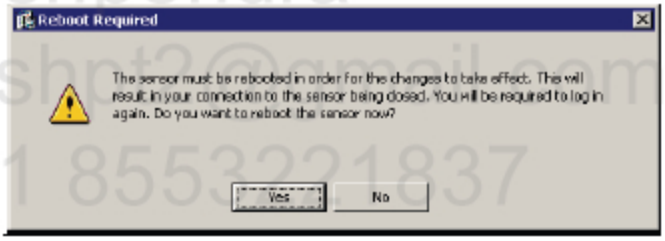
**Step 1** IPS configuration.

1. ***Go to Configuration → Time and set appropriate Zone Name and set NTP server.***



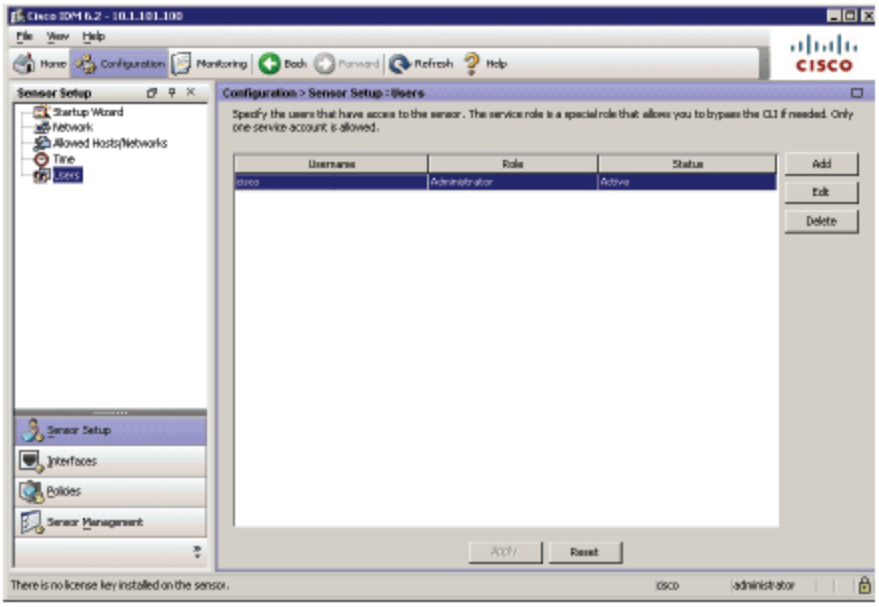

***The sensor must be reloaded for the changes to take effect.***





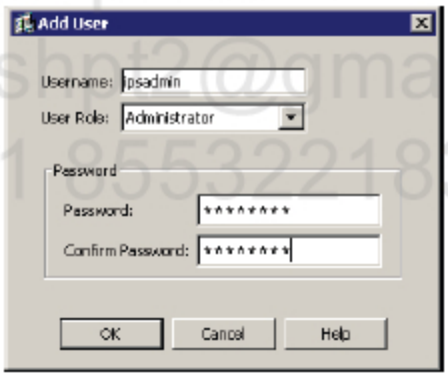


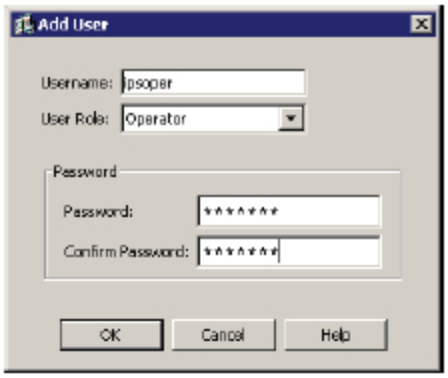
2. ***After the reboot go to Configuration → Users and click on Add button.***




3. ***Provide username and password for all required users. Chose appropriate user role during this step.***



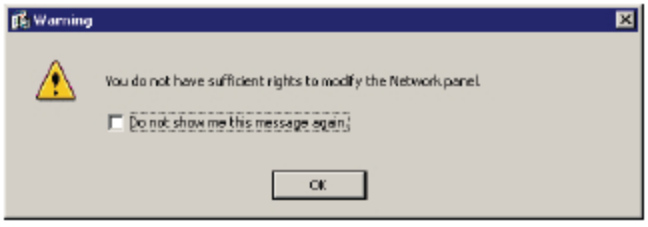


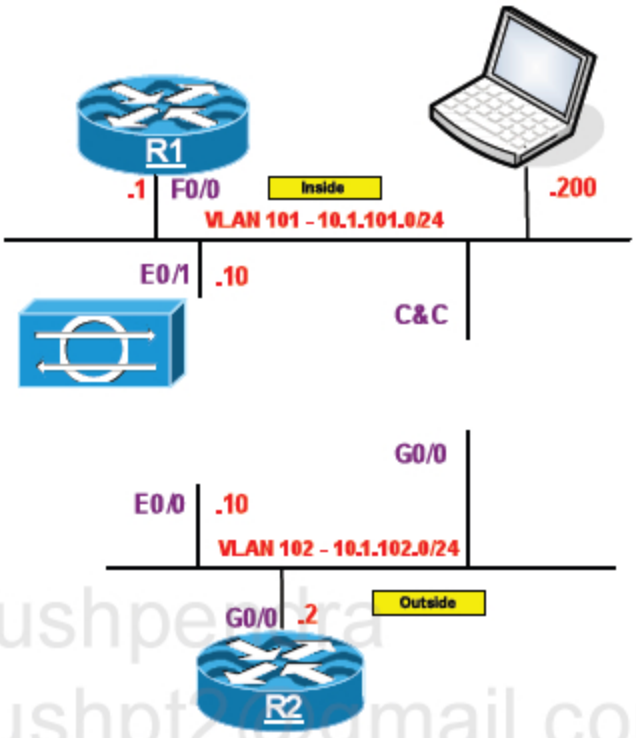

## Verification

1. ***Re-run IDM and authenticate using "ipview" username.***


2. ***Go to Configuration → Network. You should see an error message saying you're not allowed to modify the config.***



# LAB 2.2. Promiscuous Mode






**This lab is based on the topology and configuration from the previous lab.**

## Task 1

Configure the IPS sensor to detect attacks in VLAN 102 using promiscuous mode.

Make sure the IPS sensor can send TCP reset packets into the VLAN 102.

*By default, the monitoring interface of a Cisco sensor works in promiscuous mode, which means that it monitors all traffic on the local network via a network device that captures traffic for the sensor. The network device sends copies of packets to the sensor for analysis. If the traffic matches a signature, the signature fires. The sensor can send an alarm to the management console and take a response action such as initiating a block or resetting the connection.*

*Sensors running in promiscuous mode are IDS (Intrusion Detection Systems).*

*You must configure a switch to capture packets within a VLAN or sourced/destined to a port to the port where IPS sensor is connected. The solution depends on the L2 topology. If the source is connected to different switch than the sensor, there must be RSPAN (Remote Switched Port Analyzer) configured.*

*In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in*

*promiscuous mode is that the sensor does not affect the packet flow.*

## Configuration

Complete these steps:

**Step 1** SW1 configuration.

```
SW1(config)#vlan 666
SW1(config-vlan)#remote-span
SW1(config-vlan)#ex

SW1(config)#monitor session 1 source vlan 102 rx
SW1(config)#monitor session 1 destination remote vlan 666
```

**Step 2** SW3 configuration.

```
SW3(config)#vlan 666
SW3(config-vlan)#remote-span
SW3(config-vlan)#exi

SW3(config)#monitor session 1 source vlan 102 rx
SW3(config)#monitor session 1 destination remote vlan 666
```



**Step 3** SW4 configuration.

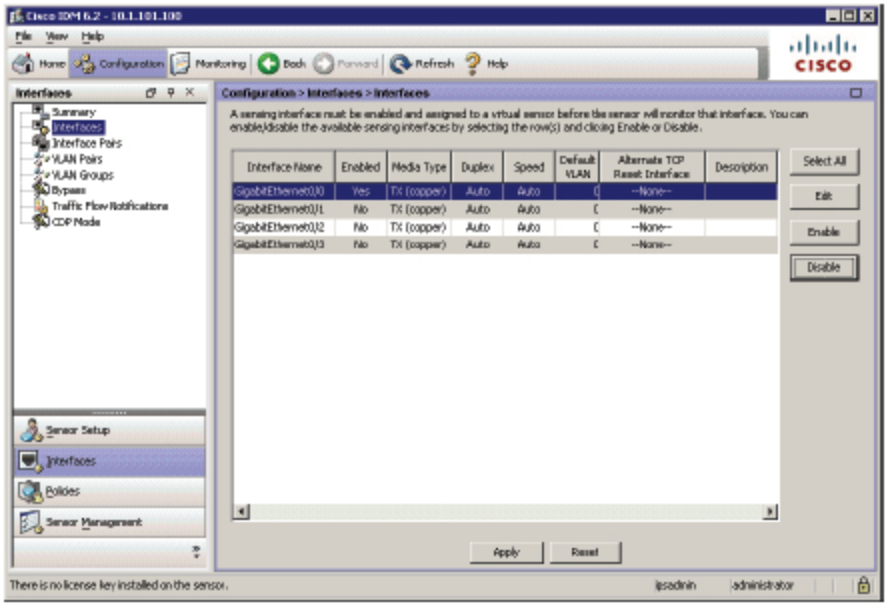
```
SW4(config)#monitor session 1 source remote vlan 666
SW4(config)#monitor session 1 destination interface f0/15 ingress vlan 102
% Warning: specified default VLAN (102) for ingress on dest port does not
exist.
```

Be careful here, as VLAN 102 does not exist on SW4. You must create it if you need to inject traffic into this VLAN (TCP reset packets from the IPS for example).

```
SW4(config)#vlan 102
SW4(config-vlan)#exi
```

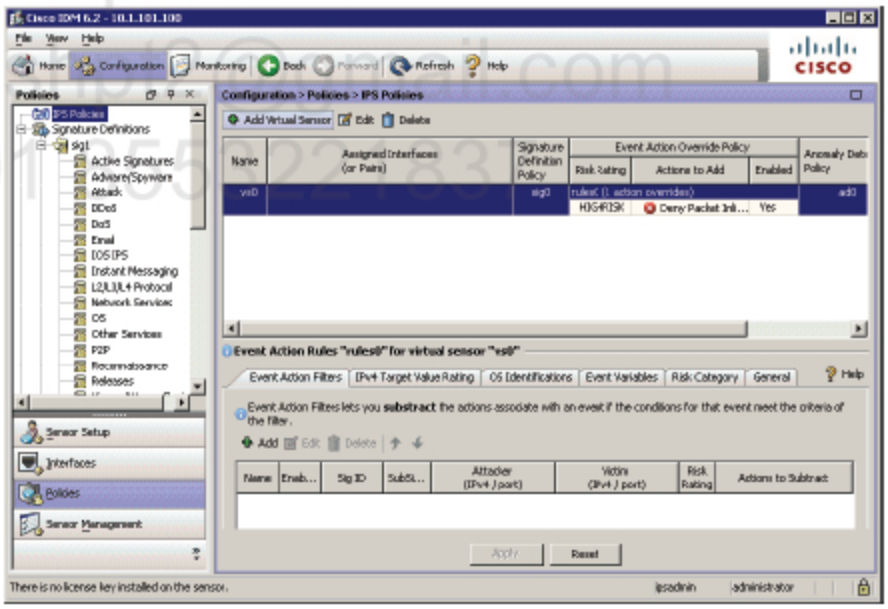
**Step 4** IPS configuration.

1. *Go to Configuration → Interfaces, select GigabitEthernet0/0 interface and click Enable button.*

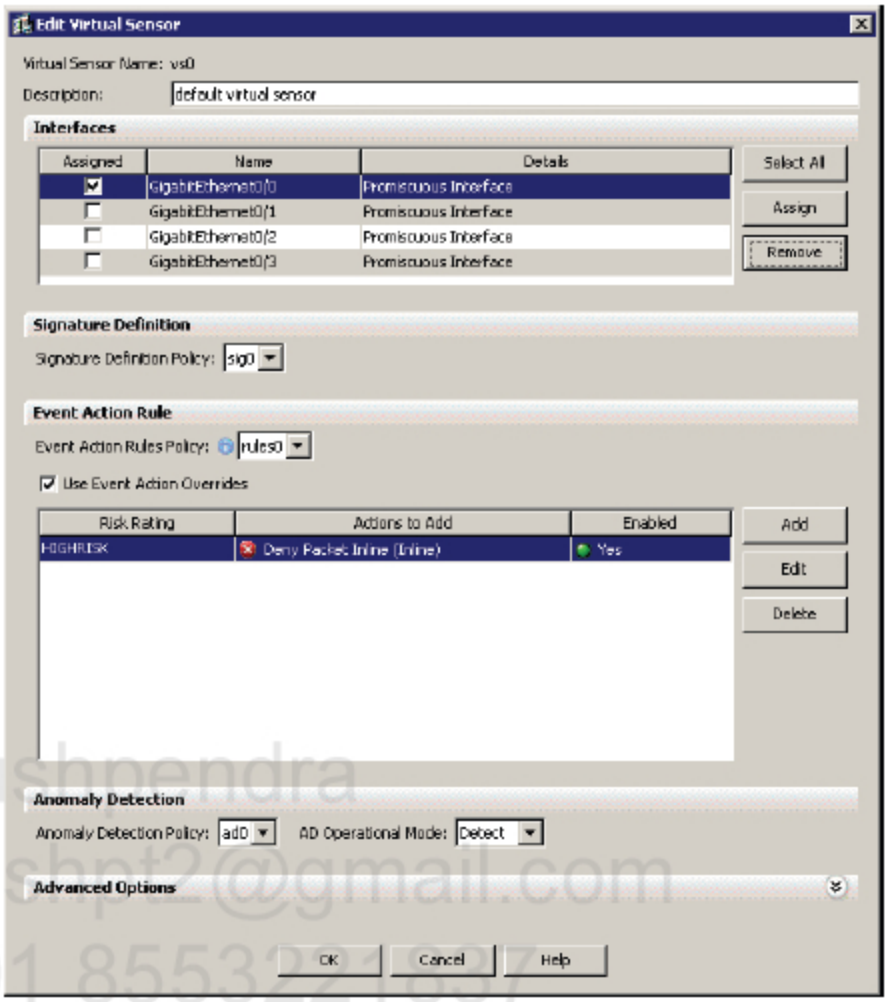



2. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit.***






3. ***Highlight GigabitEthernet0/0 interface on the list and click Assign button. Then click OK and Apply the changes to the sensor.***






## Verification

```
SW1#sh monitor session 1 det
Session 1
---------
Type                   : Remote Source Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source VLANs           :
    RX Only            : 102
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : None
Filter VLANs           : None
```

```
Dest RSPAN VLAN         : 666
```

This port (F0/10) cannot be used on the switch as the asic from this port is now used for IPS purposes.

```
SW1#sh int f0/10
FastEthernet0/10 is up, line protocol is down (monitoring)
  Hardware is Fast Ethernet, address is 0012.0183.3b0a (bia 0012.0183.3b0a)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:17:16, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     158 packets input, 15415 bytes, 0 no buffer
     Received 56 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 56 multicast, 0 pause input
     0 input packets with dribble condition detected
     164 packets output, 15835 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```



```
SW3#sh monitor session 1 det
Session 1
---------
Type                   : Remote Source Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source VLANs           :
    RX Only            : 102
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : None
Filter VLANs           : None
```

```
Dest RSPAN VLAN         : 666


SW4#sh monitor session 1 det
Session 1
---------
Type                    : Remote Destination Session
Description             : -
Source Ports            :
    RX Only             : None
    TX Only             : None
    Both                : None
Source VLANs            :
    RX Only             : None
    TX Only             : None
    Both                : None
Source RSPAN VLAN       : 666
Destination Ports       : Fa0/15
    Encapsulation       : Native
          Ingress       : Enabled, default VLAN = 102
    Ingress encap : Untagged
Filter VLANs            : None
Dest RSPAN VLAN         : None


SW4#sh int f0/15
FastEthernet0/15 is up, line protocol is down (monitoring)
  Hardware is Fast Ethernet, address is 0018.b9ff.ad91 (bia 0018.b9ff.ad91)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:04:36, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     3644 packets output, 363373 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
```

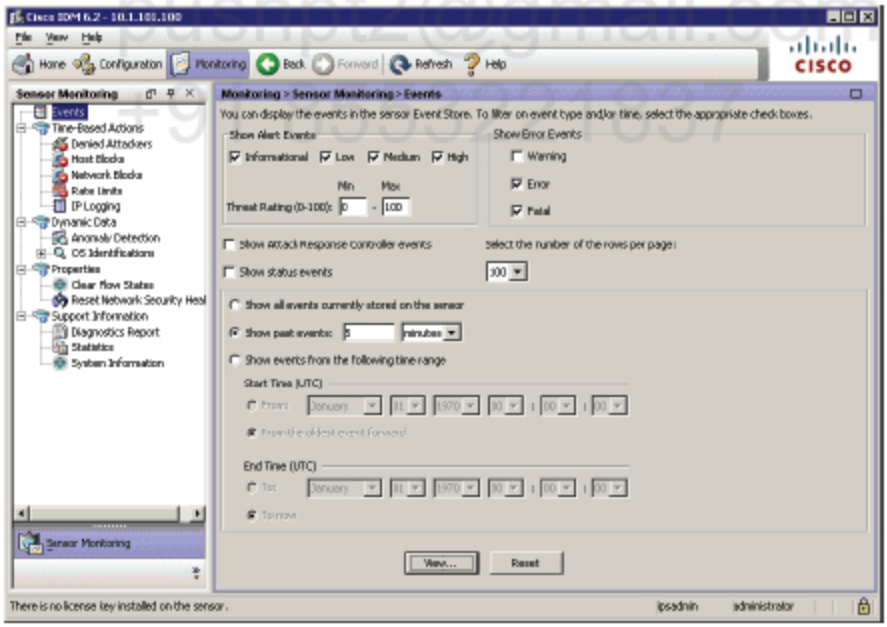
```
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
```

To test it, let's simulate an attack. Connect to HTTP server enabled on R2 and enter the following GET request. It will simulate IIS Unicode attack and should trigger some signature on the IPS if everything is configured correctly.

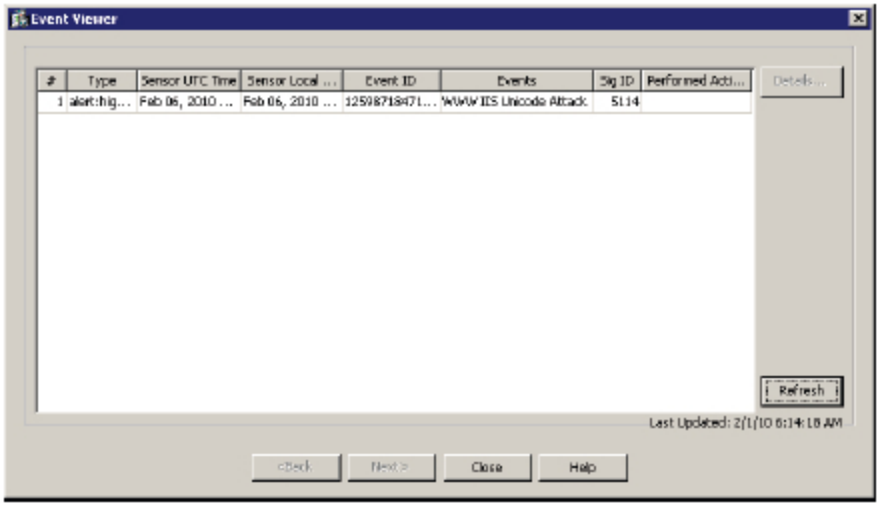
```
R1#tel 10.1.102.2 80
Trying 10.1.102.2, 80 ... Open
GET /..%c0%af../..
HTTP/1.1 400 Bad Request
Date: Sun, 07 Feb 2010 14:29:16 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.102.2 closed by foreign host]
```



***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button.***




***See the fired signature 5114 on the event list.***




***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259871847105390103  vendor=Cisco  severity=high
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 402
  time: Feb 06, 2010 14:11:36 UTC  offset=60  timeZone=GMT+01:00
  signature:  description=WWW IIS Unicode Attack  id=5114  version=S355  type=other
created=20000101
    subsigId: 1
    sigDetails: ..%c0%af..*HTTP
    marsCategory: Penetrate/Evasion/Web
    marsCategory: Penetrate/Nimdaworm
    marsCategory: Penetrate/RemoteCmdExec/Web
    marsCategory: Penetrate/RemoteCmdExec/Web/IIS
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.101.1  locality=OUT
      port: 31997
    target:
      addr: 10.1.102.2  locality=OUT
      port: 80
      os:  idSource=unknown  type=unknown  relevance=unknown
  context:
    fromAttacker:
000000  47 45 54 20 2F 2E 2E 25  63 30 25 61 66 2E 2E     GET /..%c0%af..

  riskRatingValue: 85  targetValueRating=medium
  threatRatingValue: 85
  interface: ge0_0
  protocol: tcp
```

## Task 2

Configure the IPS sensor to detect attacks in VLAN 101 using promiscuous mode. The IPS sensor must monitor this VLAN using its G0/2 interface and be able to inject traffic into VLAN 101.

*The sensor in promiscuous mode sees the traffic copied to the sensor's port but it can also prevent from some attack by sending out a TCP reset packet to the source of the attack. This can be useful in some cases but unfortunately does not protect against some type of attacks as usually the first attacker packet reaches the destination and then the sensor sends the TCP reset. It's hard to block every attacker packet in promiscuous mode.*
*The sensor uses a future of L2 switch called "ingress vlan", when the TCP reset is injected into the sensor port and correctly tagged so that it can reach the attack source within the correct VLAN.*
*The sensor may also send TCP reset using any other monitoring port if configured.*

## Configuration



Complete these steps:

**Step 1** SW1 configuration.

```
Ensure you use different Remote SPAN VLAN and different SPAN session!

SW1(config)#vlan 667
SW1(config-vlan)#remote-span
SW1(config-vlan)#exi

SW1(config)#monitor session 2 source vlan 101 rx
SW1(config)#monitor session 2 destination remote vlan 667
```

**Step 2** SW3 configuration.

```
SW3(config)#vlan 667
SW3(config-vlan)#remote-span
SW3(config-vlan)#exi

SW3(config)#monitor session 2 source vlan 101 rx
SW3(config)#monitor session 2 destination remote vlan 667
```

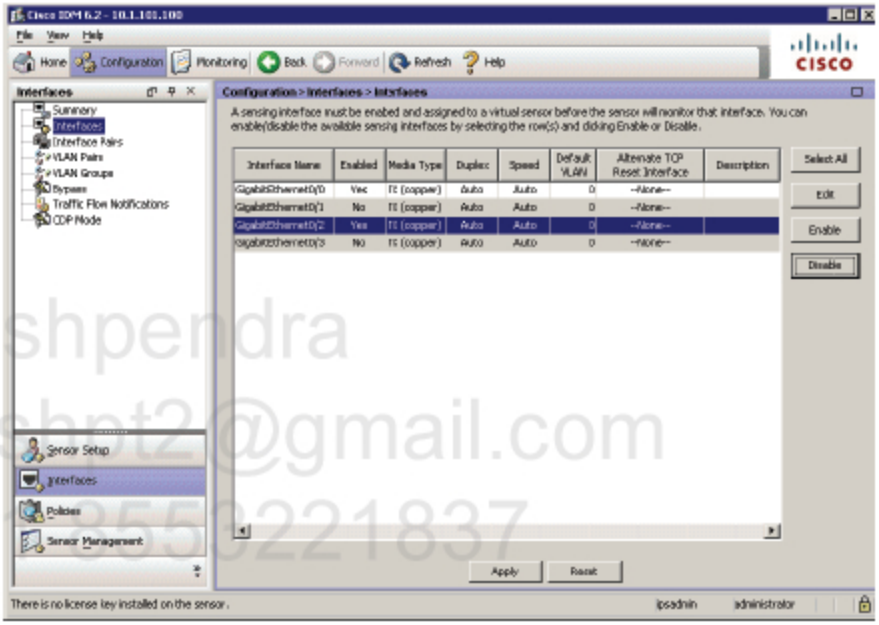
**Step 3** SW4 configuration.

```
SW4(config)#vlan 667
SW4(config-vlan)#remote-span
```

```
SW4(config-vlan)#vlan 101
SW4(config-vlan)#exi

SW4(config)#monitor session 2 source remote vlan 667
SW4(config)#monitor session 2 destination interface f0/17 ingress vlan 101
```

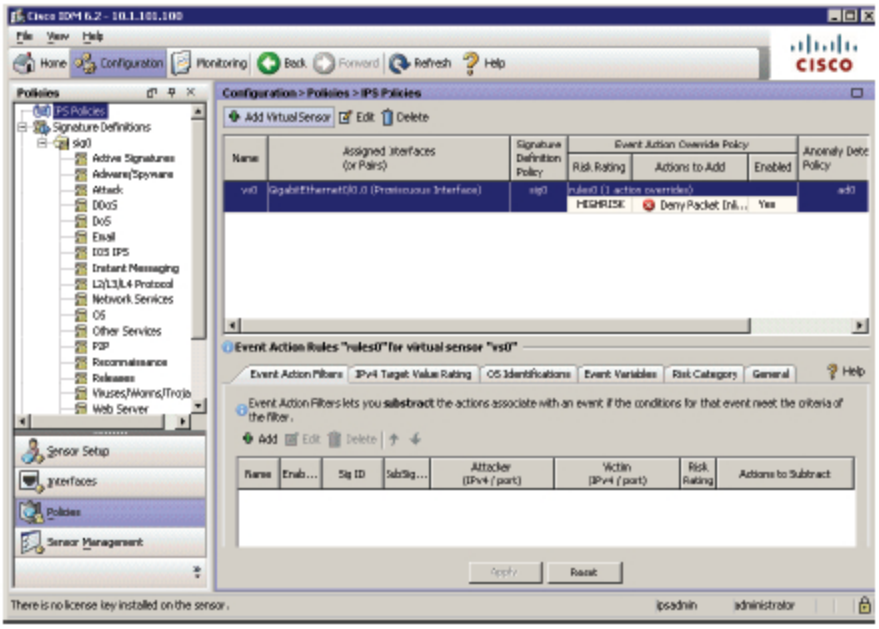
## Step 4 IPS configuration.

1. ***Go to Configuration → Interfaces, select GigabitEthernet0/2 interface and click Enable button.***

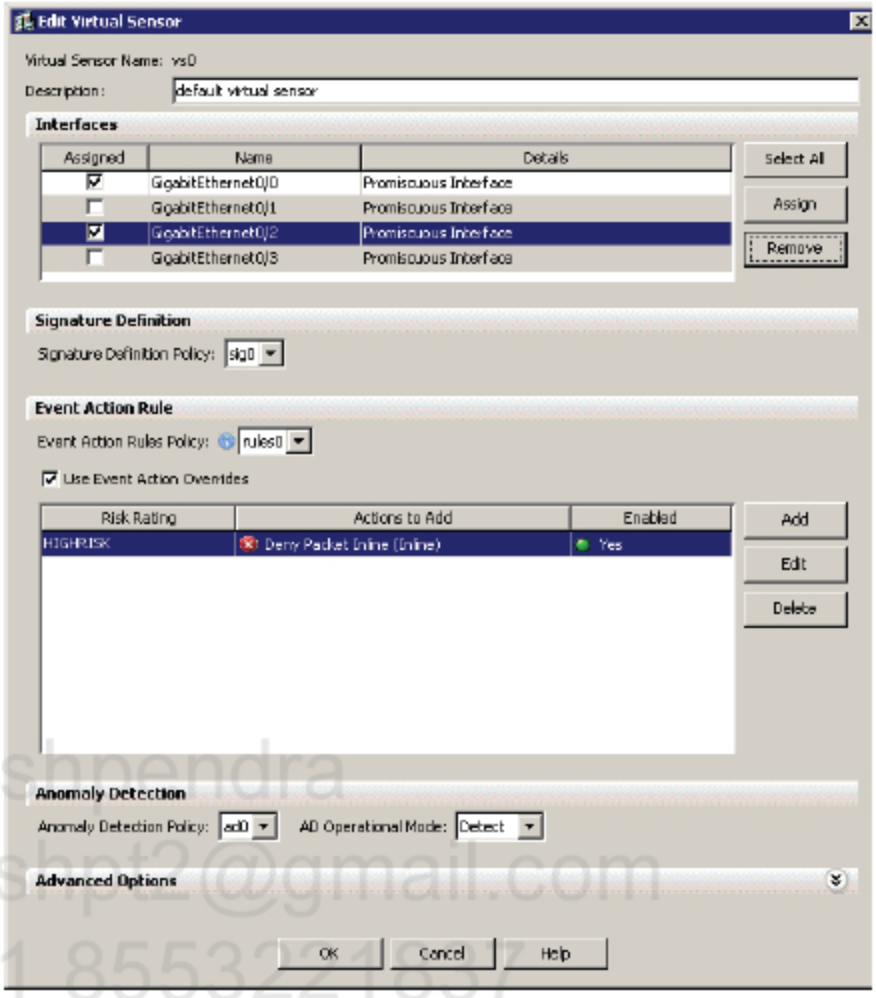





2. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit.***




3. ***Highlight GigabitEthernet0/2 interface on the list and click Assign button. Then click OK and Apply the changes to the sensor.***






## Verification

```
SW1#sh monitor session all
Session 1
---------
Type                   : Remote Source Session
Source VLANs           :
    RX Only            : 102
Reflector Port         : Fa0/10
Dest RSPAN VLAN        : 666


Session 2
---------
Type                   : Remote Source Session
Source VLANs           :
```

```
    RX Only            : 101
Reflector Port         : Fa0/12
Dest RSPAN VLAN        : 667
```

```
SW1#sh monitor session 2 detail
Session 2
---------
Type                   : Remote Source Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source VLANs           :
    RX Only            : 101
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : None
Filter VLANs           : None
Dest RSPAN VLAN        : 667
```



```
SW1#sh int f0/12
FastEthernet0/12 is up, line protocol is down (monitoring)
  Hardware is Fast Ethernet, address is 0012.0183.3b0c (bia 0012.0183.3b0c)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:04:46, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     120 packets input, 17800 bytes, 0 no buffer
     Received 21 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 15 multicast, 0 pause input
     0 input packets with dribble condition detected
     122 packets output, 17958 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
```

```
     0 output buffer failures, 0 output buffers swapped out
```

```
SW3#sh monitor session 2 detail
Session 2
---------
Type                   : Remote Source Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source VLANs           :
    RX Only            : 101
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : None
Filter VLANs           : None
Dest RSPAN VLAN        : 667
```

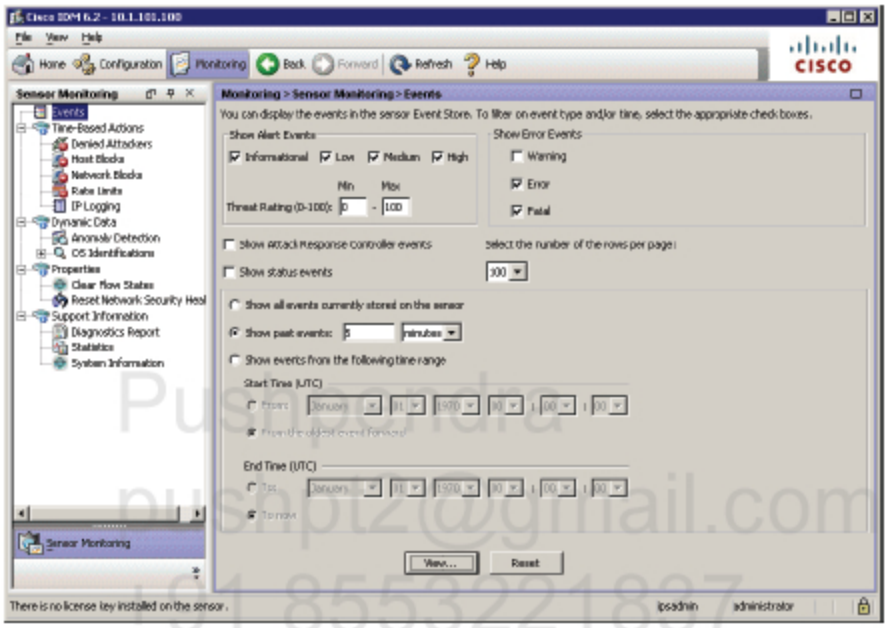


```
SW4#sh monitor session 2 detail
Session 2
---------
Type                   : Remote Destination Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : 667
Destination Ports      : Fa0/17
    Encapsulation      : Native
          Ingress      : Enabled, default VLAN = 101
    Ingress encap : Untagged
Filter VLANs           : None
Dest RSPAN VLAN        : None
```

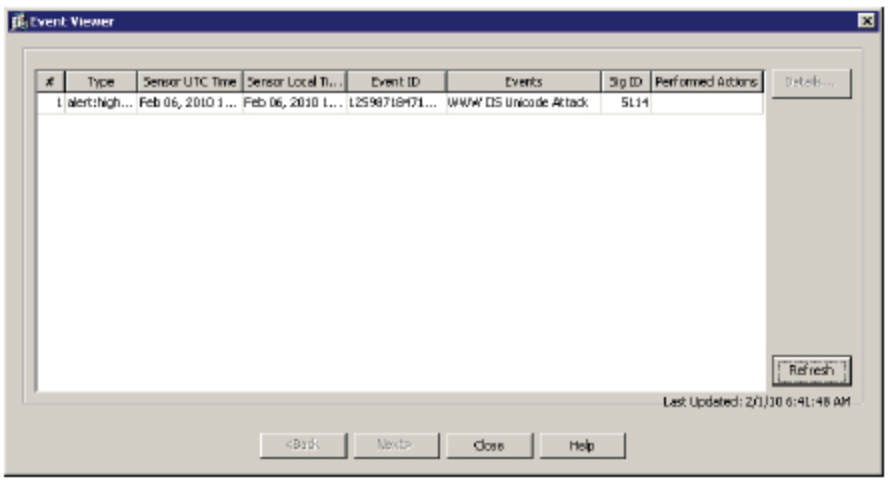
```
R1#tel 10.1.102.2 80
Trying 10.1.102.2, 80 ... Open
GET /..%c0%af../..
HTTP/1.1 400 Bad Request
Date: Sun, 07 Feb 2010 15:15:27 GMT
Server: cisco-IOS
Connection: close
```

```
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.102.2 closed by foreign host]
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button.***




***See the fired signature 5114 on the event list.***



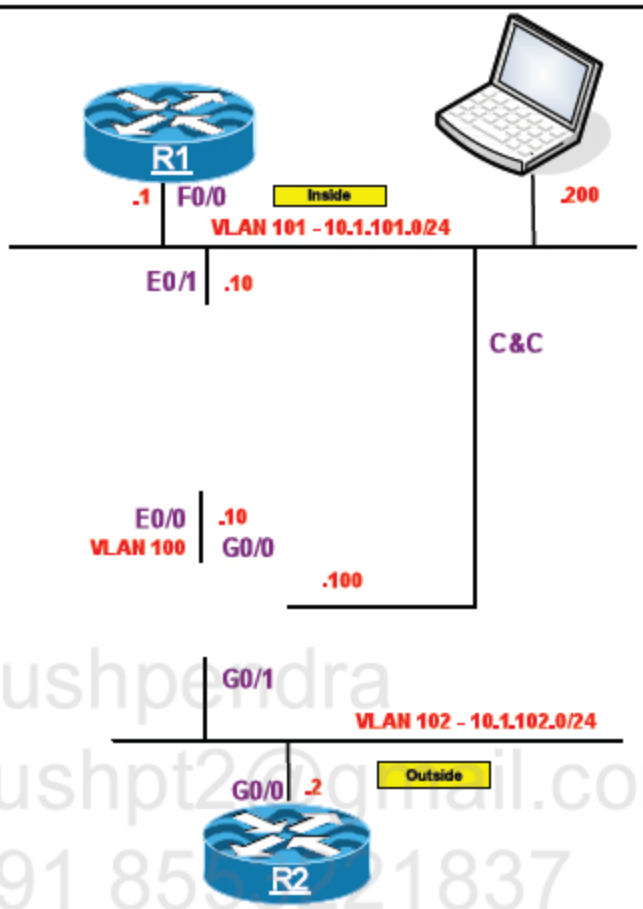

***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259871847105390122  vendor=Cisco  severity=high
```

```
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 402
  time: Feb 06, 2010 14:41:43 UTC  offset=60  timeZone=GMT+01:00
  signature:   description=WWW IIS Unicode Attack  id=5114  version=S355  type=other
created=20000101
    subsigId: 1
    sigDetails: ..%c0%af..*HTTP
    marsCategory: Penetrate/Evasion/Web
    marsCategory: Penetrate/Nimdaworm
    marsCategory: Penetrate/RemoteCmdExec/Web
    marsCategory: Penetrate/RemoteCmdExec/Web/IIS
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.101.1  locality=OUT
      port: 63434
    target:
      addr: 10.1.102.2  locality=OUT
      port: 80
      os:   idSource=unknown  type=unknown  relevance=unknown
  context:
    fromAttacker:
000000  47 45 54 20 2F 2E 2E 25  63 30 25 61 66 2E 2E    GET /..%c0%af..

  riskRatingValue: 85  targetValueRating=medium
  threatRatingValue: 85
  interface: ge0_2
  protocol: tcp
```

**How do we know the attack has been blocked in VLAN 101. The event log indicates it was blocked on IPS interface g0/2.**

# LAB 2.3. Inline Mode






## Lab Setup

- R1's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- ASA's E0/0 and IPS G0/0 interface should be configured in VLAN 100
- R2's G0/0 and IPS G0/1 interface should be configured in VLAN 102
- PC should be configured in VLAN 101
- IPS Command and Control (C&C) interface should be configured in VLAN 101
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices (except PC and IPS)

## IP Addressing

| Hostname | Interface (ifname) | IP address |
|---|---|---|
| R1 | F0/0 | 10.1.101.1/24 |
| R2 | G0/0 | 10.1.102.2/24 |
| ASA-FW | E0/0 (Outside, Security 0) | 10.1.102.10/24 |

| | | |
|---|---|---|
| | E0/1 (Inside, Security 100) | 10.1.101.10/24 |

## Task 1

Configure IPS Sensor in inline mode using its G0/0 and G0/1 interfaces configured in VLAN 100 and VLAN 102 respectively. Use the following initial settings:

Hostname: IPS-CCIE

IP address: 10.1.101.100/24

Default Gateway: 10.1.101.10

Allowed Hosts: 10.1.101.200

Configure IPS management interface (m0/0) in VLAN 101.

*Operating a sensor in inline mode puts the sensor directly into the traffic flow and enables it to prevent attacks by dropping malicious traffic before it reaches the intended target.*
*For a sensor to operate in inline mode, you must configure two monitoring interfaces as a pair. The inline port pair operates in a transparent Layer 2 repeater mode in which packets entering one interface of the port pair are transmitted out the other interface of the port pair, unless a defined signature action results in a packet being dropped. The inline interfaces are transparent and do not have IP addresses.*



## Configuration

Complete these steps:

**Step 1** IPS CLI configuration.

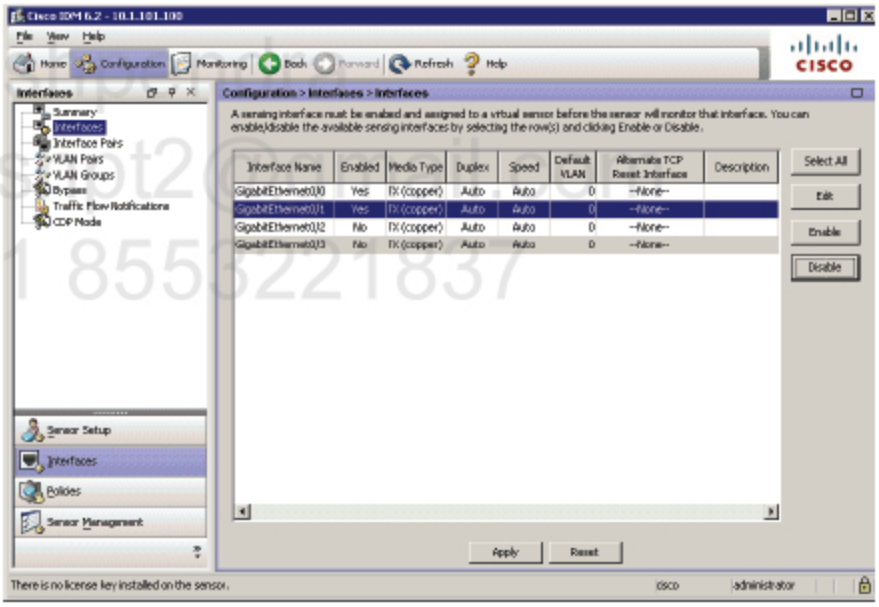
```
sensor login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
```

```
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.


    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Sat Feb  6 21:44:04 2010

Setup Configuration last modified: Sat Feb 06 21:42:16 2010

Enter host name[sensor]: IPS-CCIE
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.101.100/24,10.1.101.10
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.101.200/32
Permit:
Modify system clock settings?[no]:

The following configuration was entered.

service host
network-settings
host-ip 10.1.101.100/24,10.1.101.10
host-name IPS-CCIE
telnet-option disabled
access-list 10.1.101.200/32
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
```

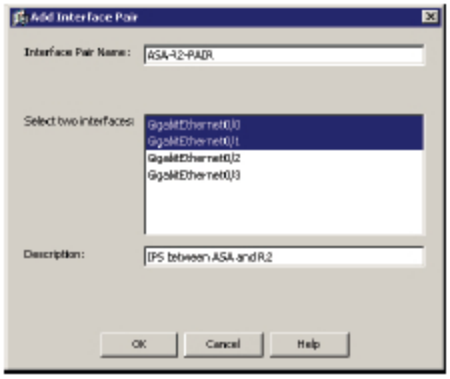
```
[3] Continue to Advanced setup.

Enter your selection[3]: 2

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.

sensor# exit


IPS-CCIE login:
```

## Step 2 IPS GUI configuration.

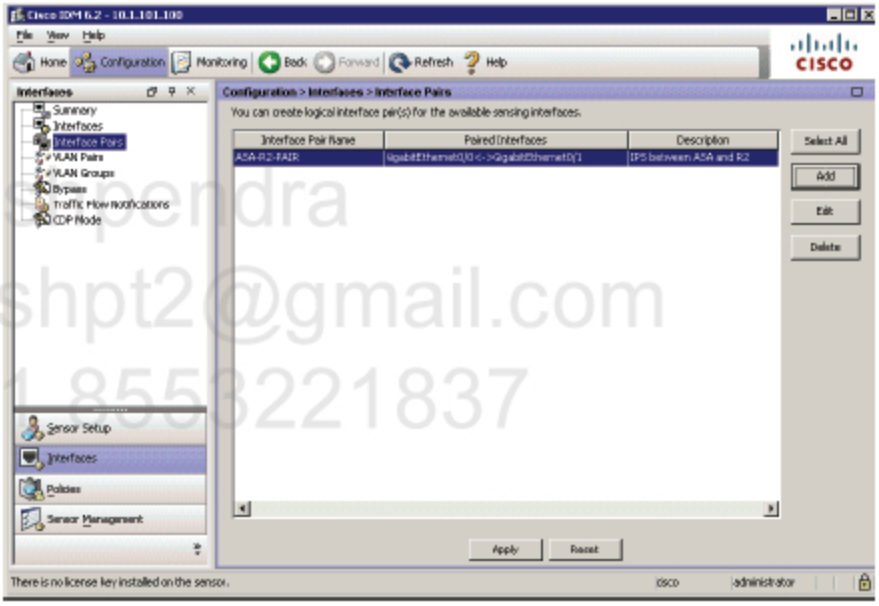
1. ***Go to Configuration → Interfaces, select GigabitEthernet0/0and GigabitEthernet0/1 interfaces and click Enable button.***




2. ***Go to Configuration → Interface Pairs → click on Add. Then enter a name for Interface Pair, select G0/0 and G0/1 interfaces on the list, make some description and click on OK.***

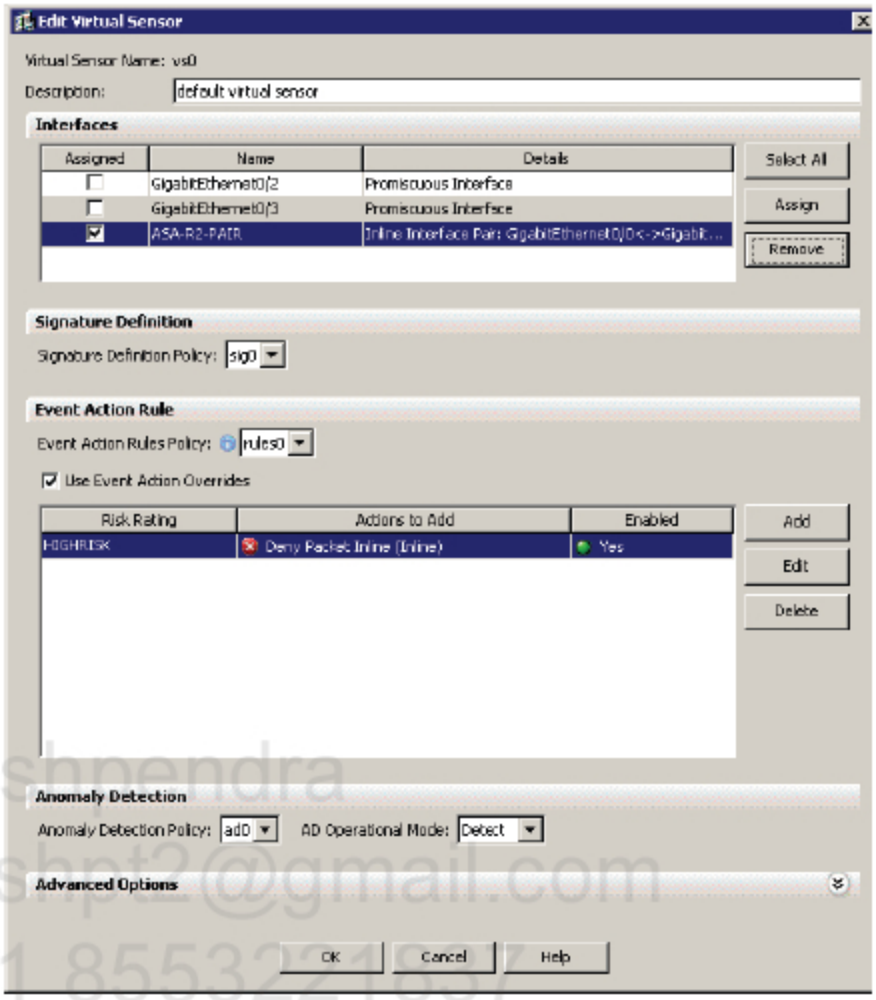



3. ***New Interface Pair is visible on the list, so click on Apply to send changes to the sensor.***






4. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit. Select newly created Interface Pair on the list and click on Assign. Then click OK and Apply the changes to the sensor.***



## Verification

```
ASA-FW(config)# pi 10.1.102.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
ASA-FW(config)#
```

## Task 2

Enable ICMP Echo Request signature to produce an alert when ICMP echo request packet is seen.

*By default some signatures are disabled. This is because it is up to the administrator to tune up and enable signatures that suits his network and will not cause network collapse after enabling them. There are two basic signatures for ICMP traffic which is very useful in testing basic IPS settings and capabilities. Those signatures are:*
*ICMP Echo Request – Sig ID 2004/0*
*ICMP Echo Reply – Sig ID 2000/0*
*Those are Informational signatures with Alert action configured. It is recommended to enable at least one (2004) to see if traffic is going through the IPS in Inline mode.*

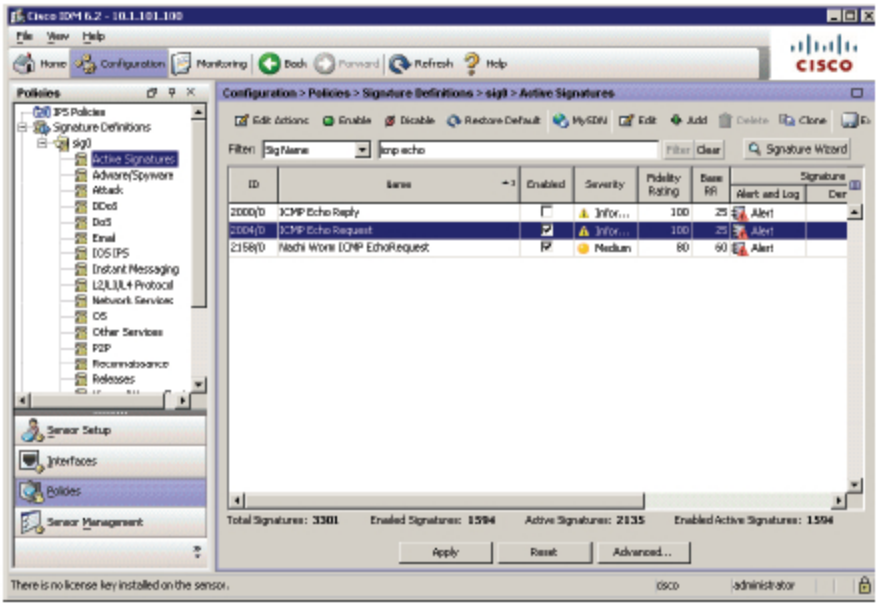


## Configuration

Complete these steps:

**Step 1** IPS configuration.

1. ***Go to Configuration → Policies → sig0 → Active Signatures. From Filter drop-down list select Sig Name and enter "icmp echo" string. Then click on Filter button. Highlight the signature ID 2004/0 and click on Enable. Then Apply the changes to the sensor.***




## Verification

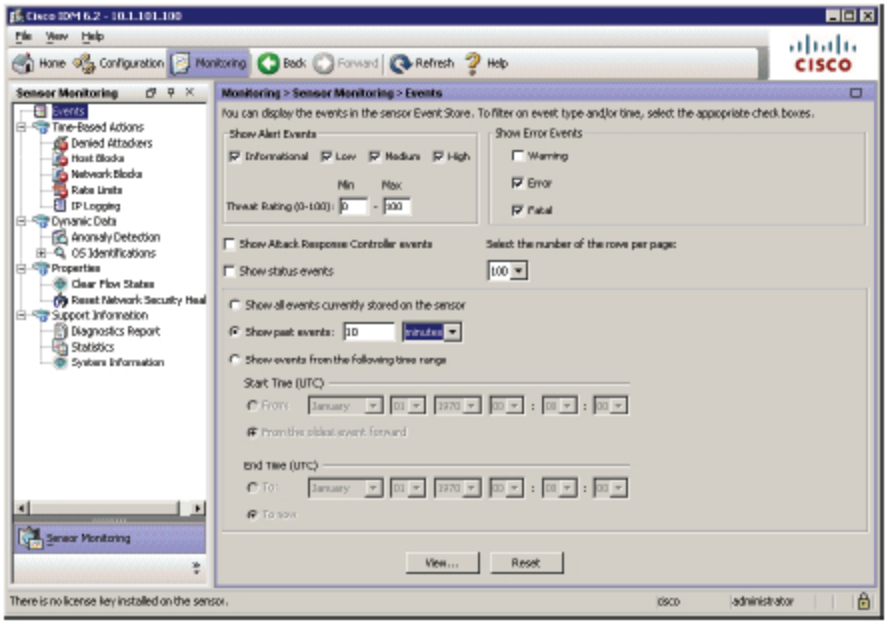


To verify the solution, we need to be able to ping through the ASA. As we already know there are two ways to do that: (1) applying an ACL on the outside in the inbound direction to allow returned ICMP replies; (2) enabling ICMP inspection. The second option is simpler/faster, so we will use it here.

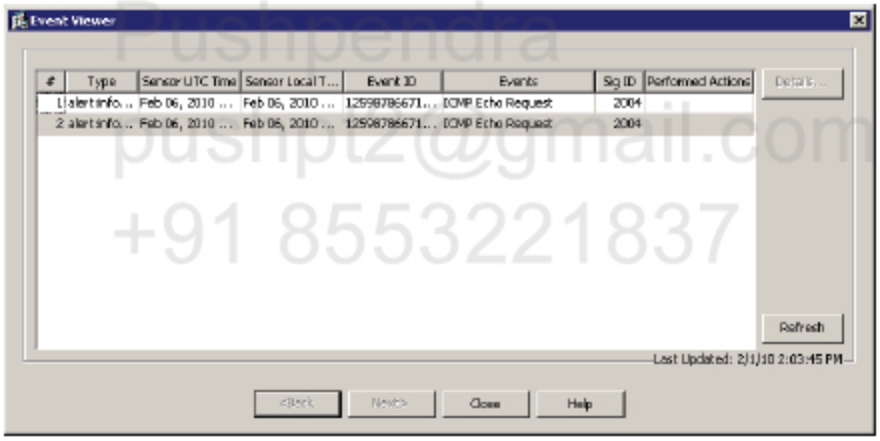
```
ASA-FW(config)# policy-map global_policy
ASA-FW(config-pmap)#  class inspection_default
ASA-FW(config-pmap-c)# inspect icmp
ASA-FW(config-pmap-c)# exi
ASA-FW(config-pmap)# exi
```

```
R1#pi 10.1.102.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.102.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/28 ms
R1#
```

***Go to Monitoring → Events, check Show past events radio button and select 10 minutes. Then click on View button.***




***See the fired signature 2004 on the event list.***




***Double click on the event to see more details. Here's the text output for event details.***

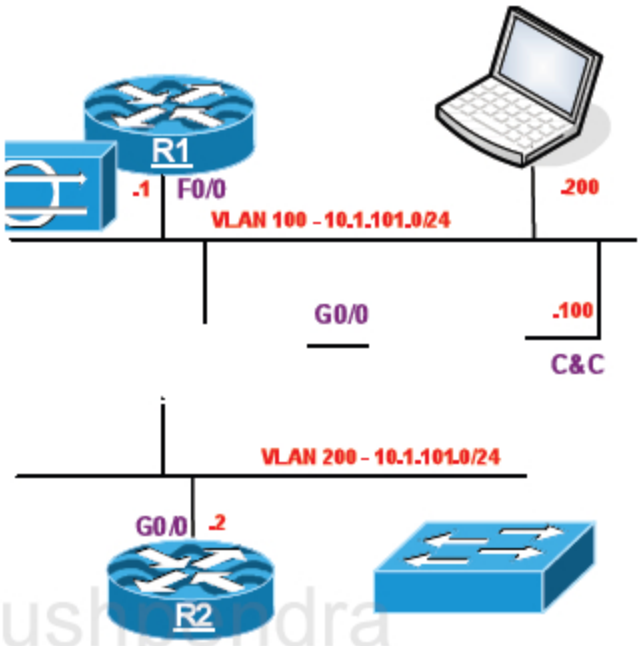
```
evIdsAlert: eventId=1259878667105390098  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 06, 2010 22:04:18 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
```

```
    attacker:
      addr: 10.1.101.1  locality=OUT
    target:
      addr: 10.1.102.2  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_0
  protocol: icmp
```

The second event is a Summary. We will look into that in later labs.

```
evIdsAlert: eventId=1259878667105390099  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 06, 2010 22:04:48 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.101.1  locality=OUT
    target:
      addr: 10.1.102.2  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  summary: 5  final=true  initialAlert=1259878667105390098  summaryType=Regular
  alertDetails: Regular Summary: 5 events this interval ;
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_0
  protocol: icmp
```

# LAB 2.4. Inline VLAN Pair Mode (on-a-stick)






## Lab Setup

- R1's F0/0 interface should be configured in VLAN 100
- R2's G0/0 interface should be configured in VLAN 200
- PC and IPS Command and Control (C&C) interface should be configured in VLAN 100

## IP Addressing

| Hostname | Interface (ifname) | IP address |
|---|---|---|
| R1 | F0/0 | 10.1.101.1/24 |
| R2 | G0/0 | 10.1.101.2/24 |

## Task 1

Configure IPS Sensor to monitor traffic going between VLANs 100 and 200 using only one physical interface (G0/0). Use the following initial settings:

Hostname: IPS-CCIE

IP address: 10.1.101.100/24

Default Gateway: 10.1.101.10

Allowed Hosts: 10.1.101.200

Configure IPS management interface (m0/0) in VLAN 100.

*You can associate VLANS in pairs on a physical interface. This configuration is known as "inline-on-a-stick." Packets received on one of the paired VLANS are analyzed and then forwarded to the other VLAN in the pair.*
*Inline VLAN pair mode is an active monitoring mode where a monitoring interface acts as an IEEE 802.1Q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic that it receives on each VLAN in each pair, and can either forward the packets on the other VLAN in the pair, or drop the packet if an intrusion attempt is detected.*
*You can configure a Cisco IPS sensor to simultaneously bridge up to 255 VLAN pairs on each monitoring interface. The sensor replaces the VLAN ID field in the 802.1Q header of each received packet with the ID of the egress VLAN to which the sensor forwards the packet. The sensor drops all packets received on any VLANs that are not assigned to inline VLAN pairs.*

## Configuration

Complete these steps:

**Step 1** SW4 configuration.

```
SW4(config)#vlan 200
SW4(config-vlan)#exi

SW4(config)#interface FastEthernet0/15
SW4(config-if)#switchport trunk encapsulation dot1q
SW4(config-if)#switchport trunk allowed vlan 100,200
SW4(config-if)#switchport mode trunk
```

We need to have a trunk between the switch and IPS monitoring interface to send a pair of VLANs.

**Step 2** IPS CLI configuration.

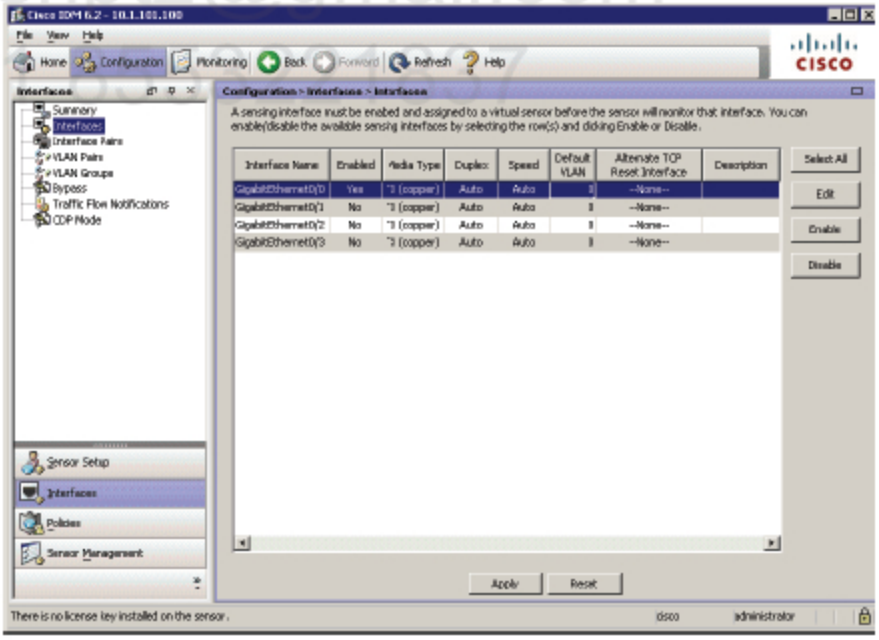
```
sensor login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

```
If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.


    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Sun Feb  7 20:00:22 2010
Setup Configuration last modified: Sun Feb 07 20:00:00 2010

Enter host name[sensor]: IPS-CCIE
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.101.100/24,10.1.101.10
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.101.200/32
Permit:
Modify system clock settings?[no]:

The following configuration was entered.

service host
network-settings
host-ip 10.1.101.100/24,10.1.101.10
host-name IPS-CCIE
telnet-option disabled
access-list 10.1.101.200/32
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
```

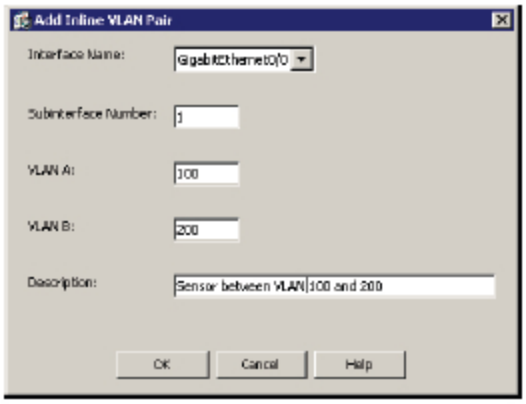
```
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.

Enter your selection[3]: 2

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.

sensor# exi


IPS-CCIE login:
```

**Step 3** IPS GUI configuration.

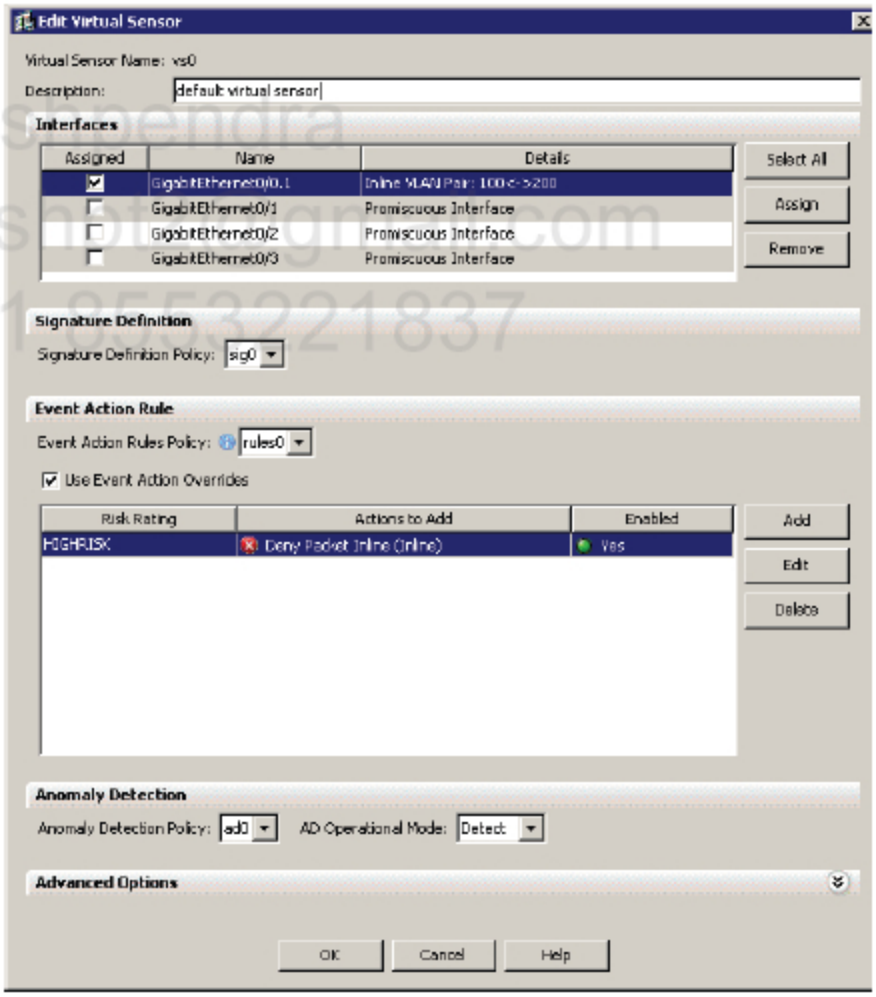
1. ***Go to Configuration → Interfaces, select GigabitEthernet0/0 interface and click Enable button.***




2. ***Then go to configuration → Interfaces → VLAN Pairs and click on Add. Select the GigabitEthernet0/0 interface from the drop-down list and enter the VLAN information as follows:***



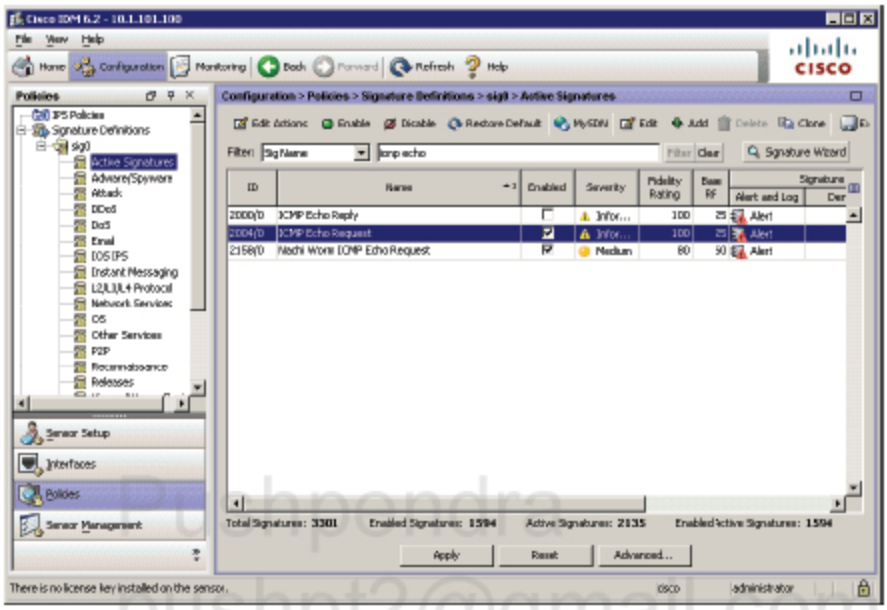

3. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit. Highlight GigabitEthernet0/0.1 interface on the list and click Assign button. Then click OK and Apply the changes to the sensor.***



## Verification

***To verify, enable SIG ID 2004 and ping R2 from R1.***

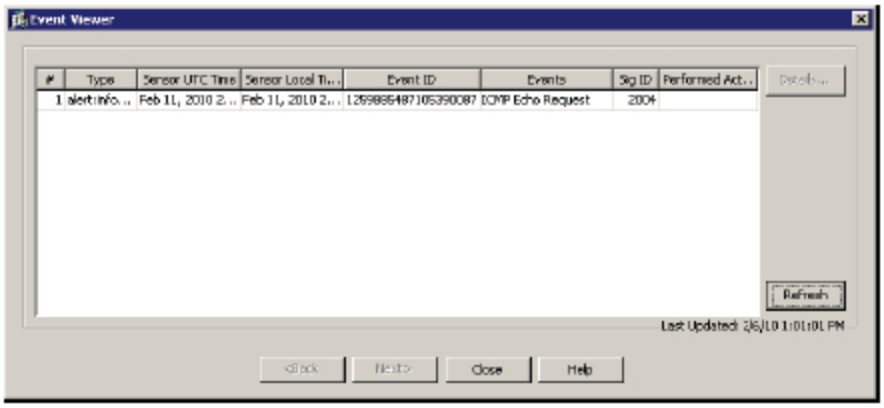
***Go to Configuration → Policies → sig0 → Active Signatures. From Filter drop-down list select Sig Name and enter "icmp echo" string. Then click on Filter button. Highlight the signature ID 2004/0 and click on Enable. Then Apply the changes to the sensor.***






```
R1#pi 10.1.101.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/8/28 ms
R1#
```

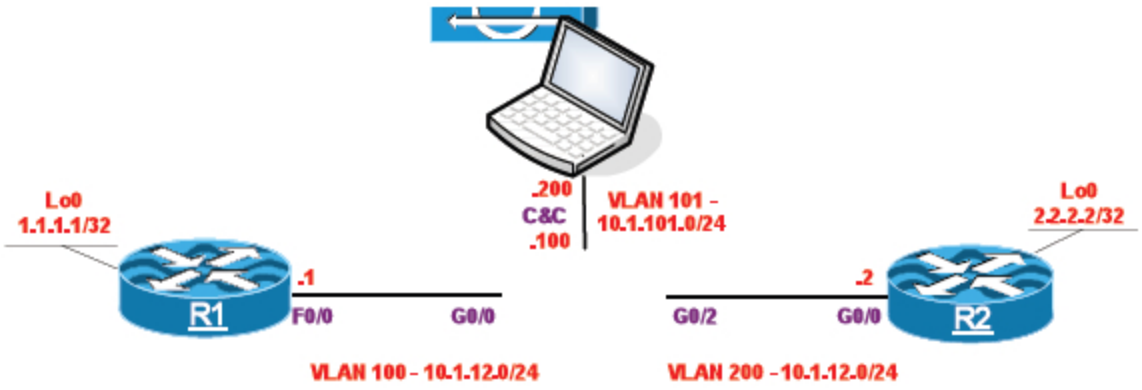
***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the fired signature on the event list.***




***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259885487105390087  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 388
  time: Feb 11, 2010 21:02:16 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 100
  participants:
    attacker:
      addr: 10.1.101.1  locality=OUT
    target:
      addr: 10.1.101.2  locality=OUT
      os:  idSource=unknown  type=unknown  relevance=relevant
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_0
  protocol: icmp
```

# LAB 2.5. Signature tuning




## Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 100 and VLAN 200 respectively
- PC and IPS Command and Control (C&C) interface should be configured in VLAN 101
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices (except PC and IPS)



## IP Addressing

| Hostname | Interface (ifname) | IP address |
|---|---|---|
| R1 | F0/0<br>Lo0 | 10.1.12.1/24<br>1.1.1.1/32 |
| R2 | G0/0<br>Lo0 | 10.1.12.2/24<br>2.2.2.2/32 |

## Task 1

Configure IPS Sensor in inline mode using its G0/0 and G0/1 interfaces configured in VLAN 100 and VLAN 200 respectively. Use the following initial settings:

- Hostname: IPS-CCIE
- IP address: 10.1.101.100/24
- Default Gateway: 10.1.101.10
- Allowed Hosts: 10.1.101.200

- IPS management interface (m0/0) in VLAN 101.

Configure signature named “Fragmented ICMP Traffic” to trigger when fragmented ICMP Echo packets are seen between R1’s F0/0 and R2’s G0/0 interface. You must use existing signature to block the attacker inline and generate an alert.

## Configuration

Complete these steps:

**Step 1** SW4 configuration.

```
SW4(config)#interface FastEthernet0/15
SW4(config-if)#switchport mode access
SW4(config-if)#switchport access vlan 100

SW4(config)#interface FastEthernet0/16
SW4(config-if)#switchport mode access
SW4(config-if)#switchport access vlan 200
```



**Step 2** IPS CLI configuration.

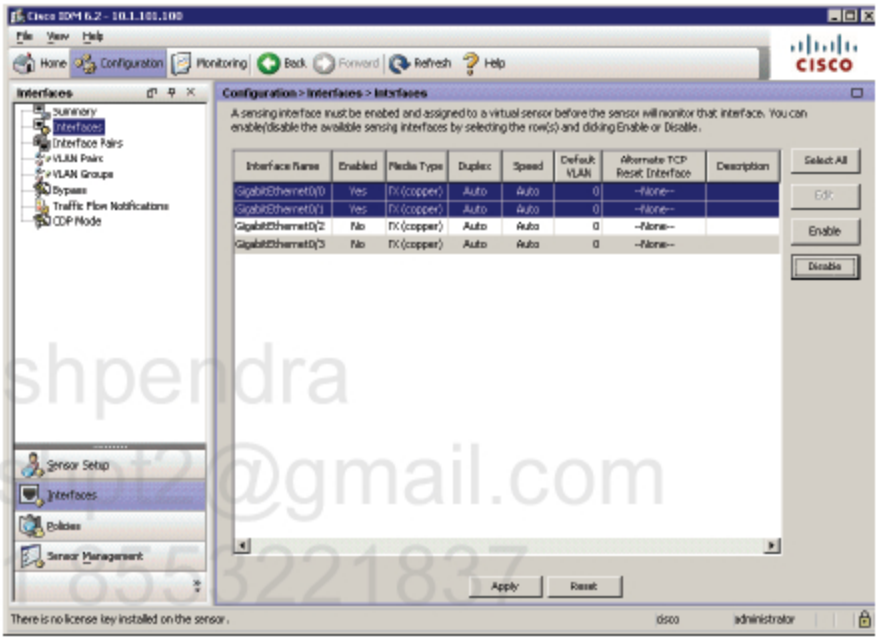
```
sensor login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.


    --- Basic Setup ---

    --- System Configuration Dialog ---
```

```
At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Sun Feb  7 20:00:22 2010

Setup Configuration last modified: Sun Feb 07 20:00:00 2010

Enter host name[sensor]: IPS-CCIE
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.101.100/24,10.1.101.10
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.101.200/32
Permit:
Modify system clock settings?[no]:

The following configuration was entered.

service host
network-settings
host-ip 10.1.101.100/24,10.1.101.10
host-name IPS-CCIE
telnet-option disabled
access-list 10.1.101.200/32
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.

Enter your selection[3]: 2

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.
```

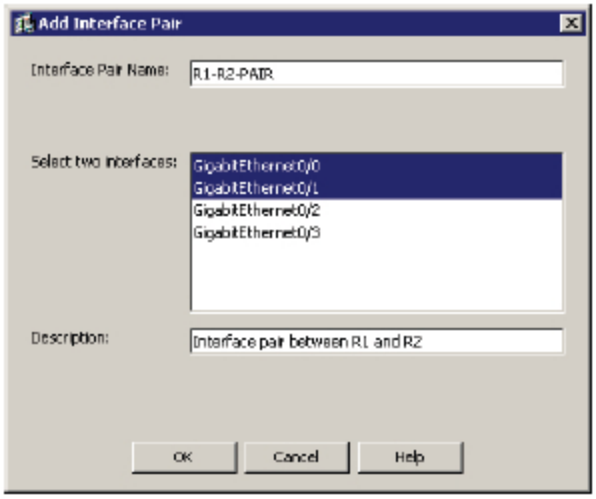
```
sensor# exi


IPS-CCIE login:
```

**Step 3** IPS GUI configuration.

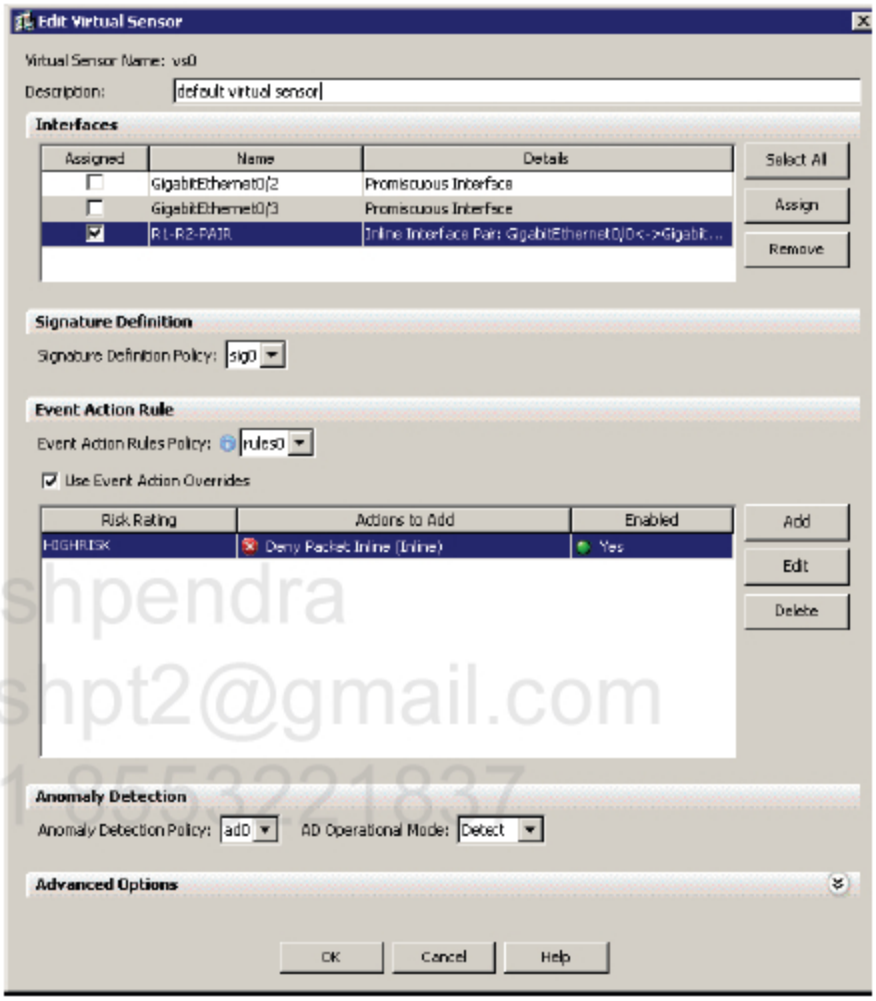
1. ***Go to Configuration → Interfaces → Interfaces, select GigabitEthernet0/0 and GigabitEthernet0/1 interfaces and click Enable button.***




2. ***Go to Configuration → Interfaces → Interface Pairs and click on Add. Enter a name for Inteface Pair, select two interfaces from the list and make some description. Click OK and Apply button.***

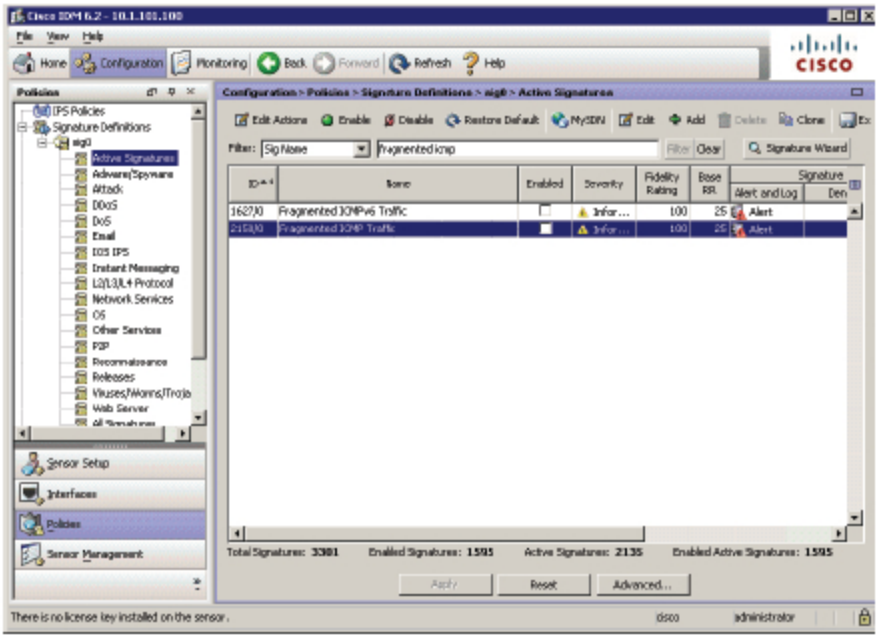


3. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit. Highlight newly created Inline Interface Pair on the list and click Assign button. Then click OK and Apply the changes to the sensor.***

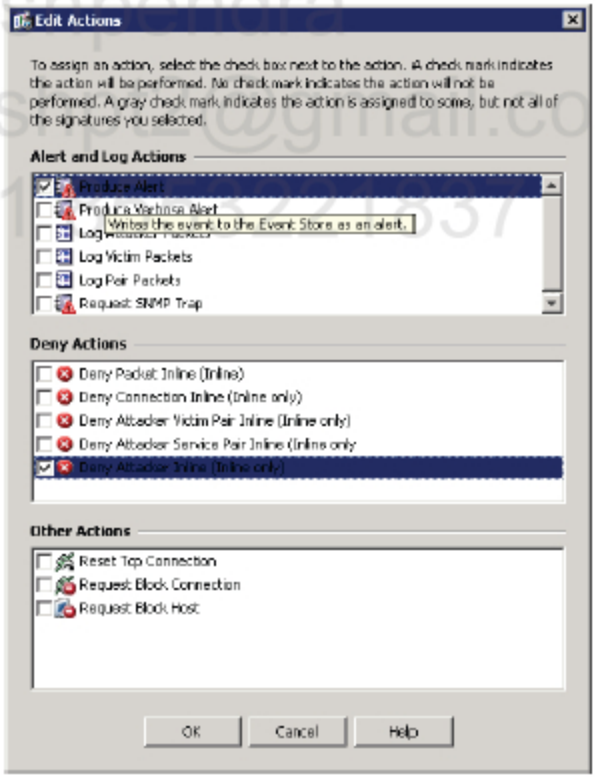




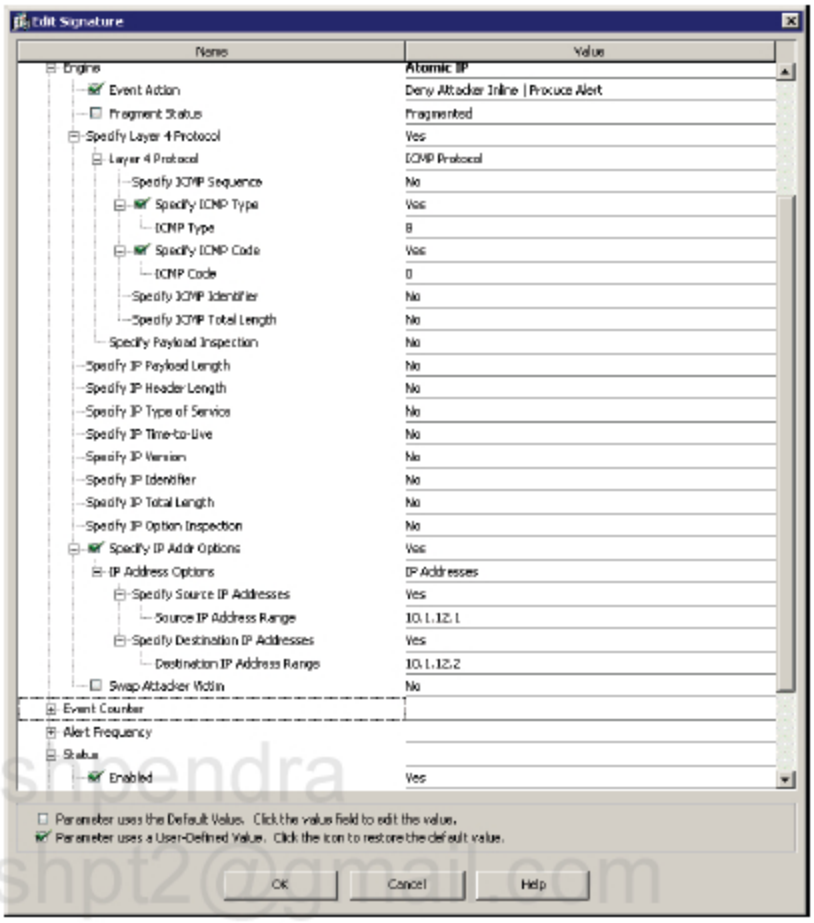

4. ***Go to Configuration → Policies → sig0 → Active Signatures. From Filter drop-down list select Sig Name and enter "fragmented icmp" string. Then click on Filter button. Highlight the signature ID 2150/0 and click on Enable.***




5. ***Then click on Edit Actions button and select Deny Attacker Inline and Produce Alert items on the list. Click on OK.***




6. ***Click on Edit button to see details for selected signature. Enter "8" for ICMP Type and "0" for ICMP Code. Specify Source IP Address Range and Destination IP Address Range as follows:***






## Verification

**R1#pi 10.1.12.2**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

**Standard ping is successful as there is no fragmentation (ICMP packets by default have size of 100 bytes).**

**R1#pi 10.1.12.2 size 2000**

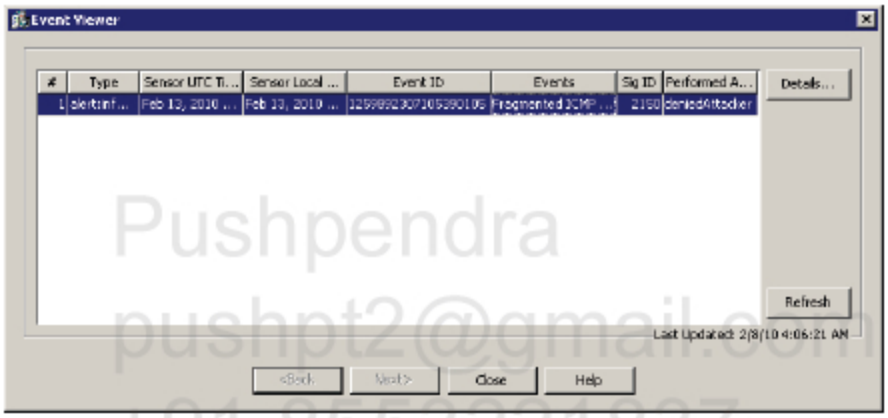
```
Type escape sequence to abort.
Sending 5, 2000-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

**Large ping has been blocked as there are fragments. The default MTU on Ethernet segment is 1500 bytes.**

```
R1#pi 2.2.2.2 so lo0 size 2000

Type escape sequence to abort.
Sending 5, 2000-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

This ping is successful as it does not trigger the signature due to wrong source IP address.

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the fired signature 2150 on the event list.***





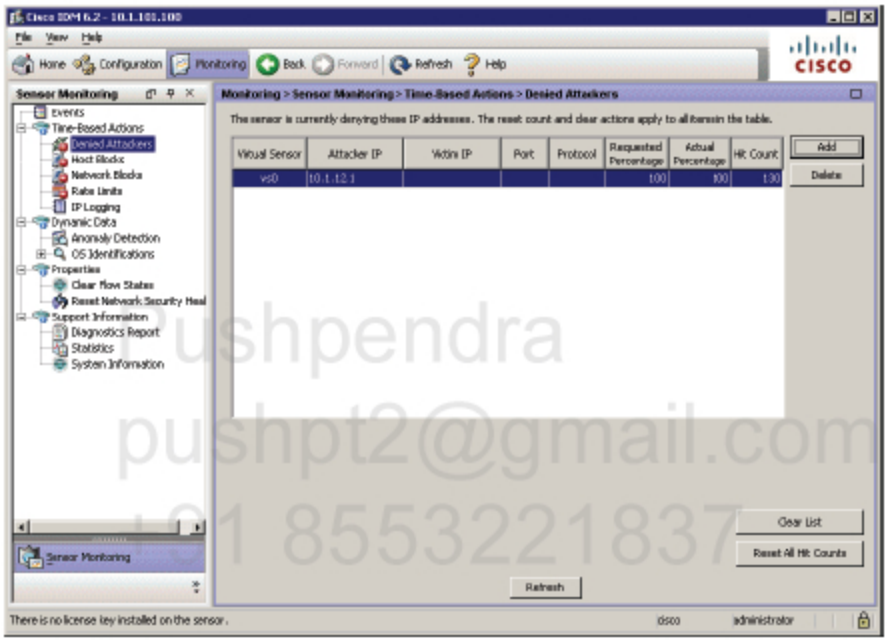

***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259892307105390105  vendor=Cisco  severity=informational
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 13, 2010 12:06:43 UTC  offset=0  timeZone=UTC
  signature:  description=Fragmented ICMP Traffic  id=2150  version=S2  type=other
created=20010202
    subsigId: 0
    marsCategory: DoS/Host
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
    target:
      addr: 10.1.12.2  locality=OUT
      os:  idSource=unknown  type=unknown  relevance=relevant
  actions:
    deniedAttacker: true
```

```
riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
threatRatingValue: 0
interface: ge0_0
protocol: icmp
```

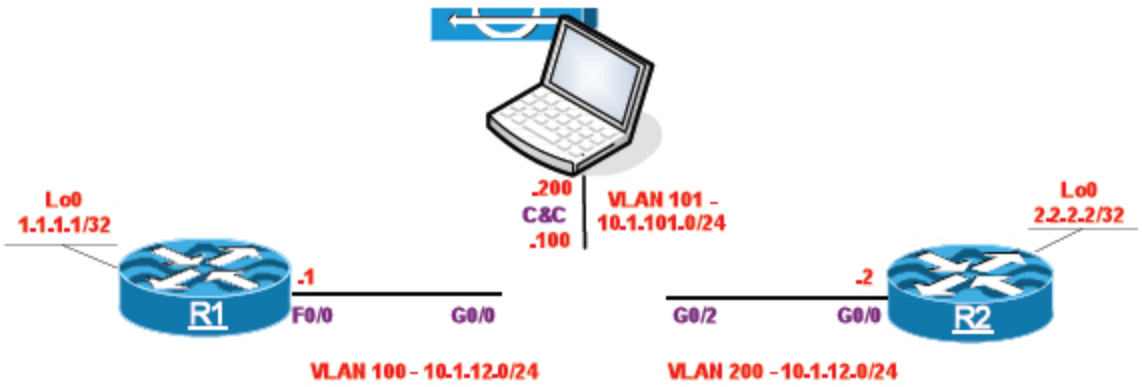
Note that action is available in the event log. This action is available only in Inline mode as the IPS itself must block the traffic. The blocked traffic sources are listed under the following page in IDM:

***Go to Monitoring → Time-Based Actions → Denied Attackers. There should be R1's F0/0 IP address on the list.***



# LAB 2.6. Custom HTTP signature

**This lab is based on the configuration from the previous lab**






## Task 1

Create new signature to reset connections to the HTTP server located on R2. The TCP Reset should be sent to the attacker if there is a string "cisco.com" seen in the URI field and the packet is destined to one of the following ports 80, 8080, 888 and the URI field is no longer than 10 characters.

*Each Cisco IPS signature is created by a signature engine specifically designed for the type of traffic being monitored. A signature engine is a component of the sensor that supports a category of signatures. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values. Cisco IPS signature engines enable network security administrators to tune and create signatures unique to their network environment. Here are some of the general categories of Cisco IPS signature engines:*

- *ATOMIC: Used to perform per-packet inspection (The ATOMIC engines support signatures that trigger on the analysis of a single packet.)*
- *FLOOD: Used to detect attempts to cause a denial of service (DoS)*
- *META: Used to perform event correlation on the sensor*
- *NORMALIZER: Used to detect ambiguities and abnormalities in the traffic stream*
- *SERVICE: Used when services with Layers 5, 6, and 7 require protocol analysis*
- *STATE: Used for state-based and regular expression-based pattern inspection and alarming functionality for TCP streams*
- *STRING: Used for regular expression-based pattern inspection and alarm functionality for multiple transport protocols, including TCP, UDP, and ICMP*
- *SWEEP: Used to detect network reconnaissance*
- *TRAFFIC: Identifies traffic irregularities*
- *TROJAN: Used to detect BackOrifice Trojan horse traffic and Tribe Flood Network 2000*

*(TFN2K), Trojan, or distributed denial of service (DDoS) traffic*

- *AIC (Alarm Interface Controller): Used for deep-packet inspection of FTP and HTTP traffic*

*Signature engines use their parameters to provide the configuration of signatures. An engine parameter is a name and value pair. The parameter name is constant across all signatures in a particular engine, but the value can be different for the various signatures in an engine group. Some parameters are common to all engines while others are engine-specific. Although all signatures have the Event Action parameter, you can select only actions that make sense for that engine.*

## Configuration

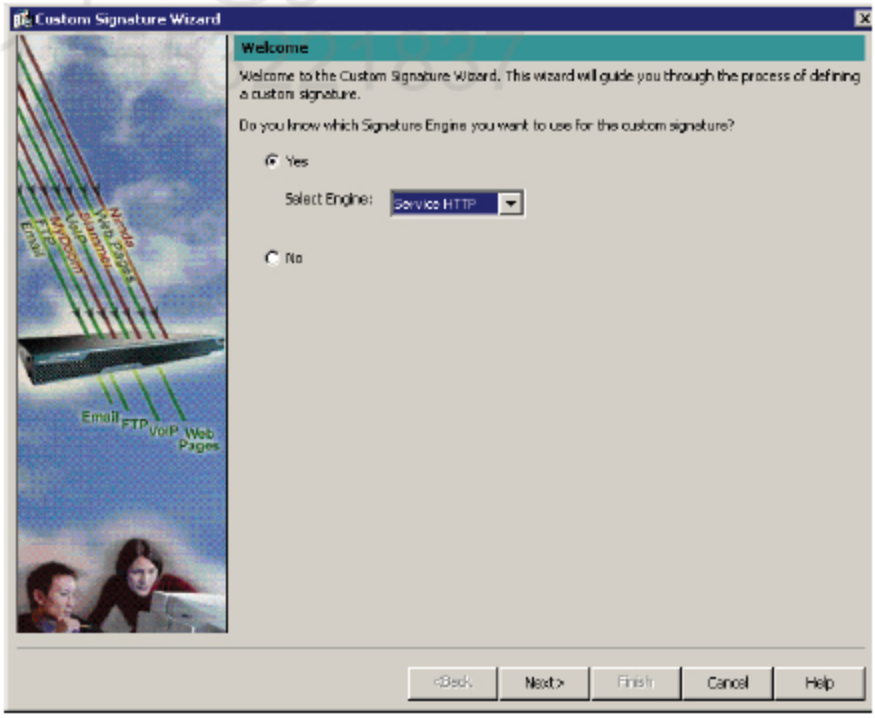
Complete these steps:

**Step 1** IPS configuration.

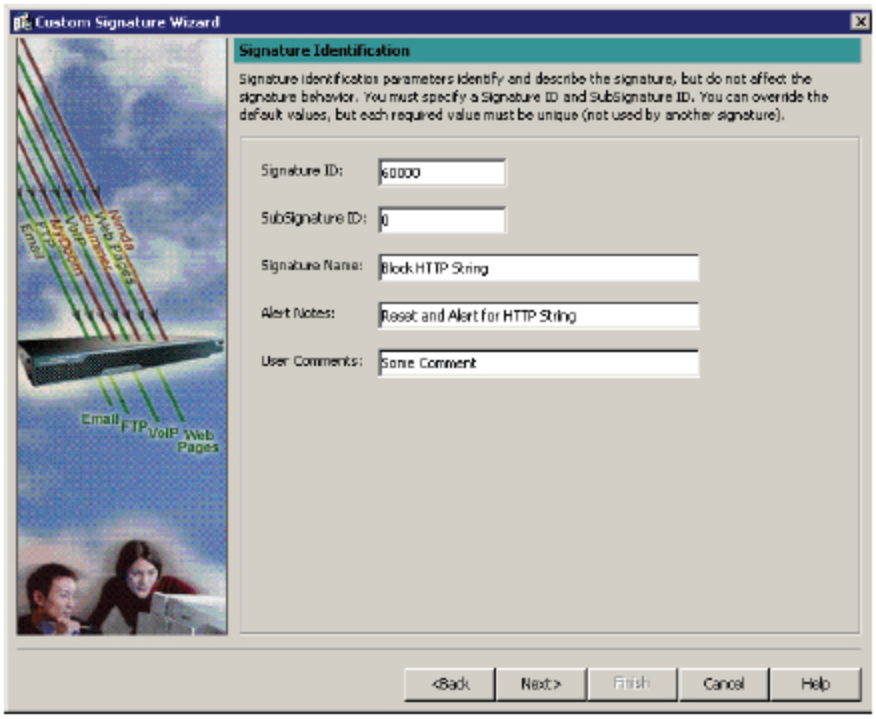
```
The task clearly asks for HTTP deep inspection which can be done using
"Service HTTP" engine. That engine "understands" HTTP traffic (Layer
7) and can be tuned to catch only specific HTTP traffic e.g. specific
URI or port.
```



1. ***Go to Configuration → Policies → sig0 → Active Signatures and click on Signature Wizard. Select Service HTTP from the drop-down list and click Next.***

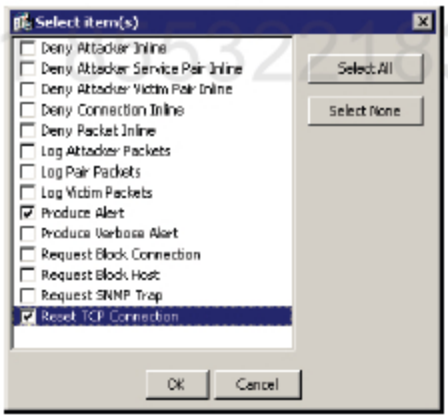



2. ***Enter the name for new signature, make some Notes and Comments and click on Next.***

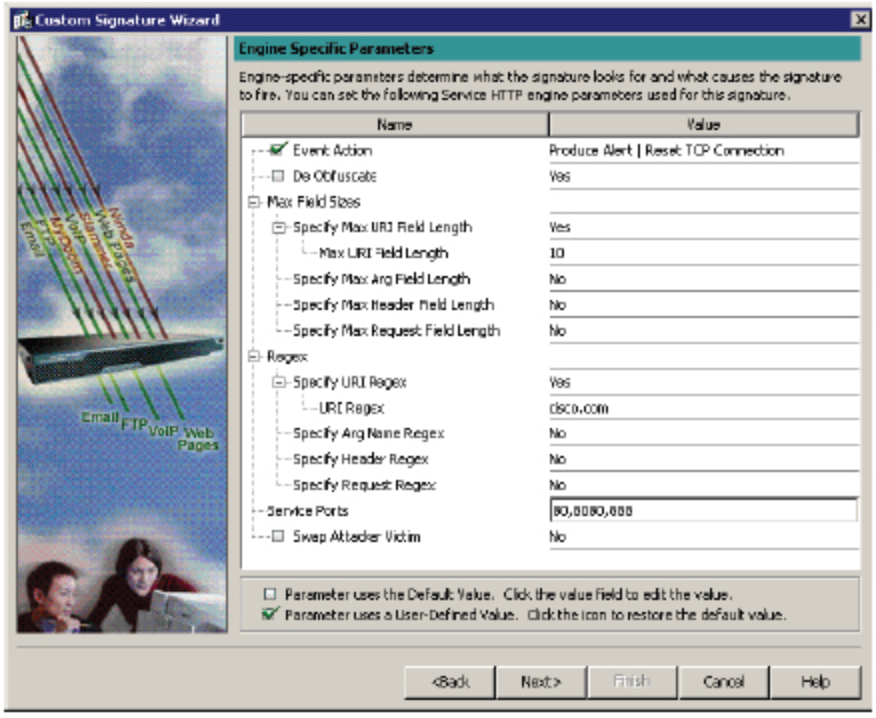





3. ***On the Engine Specific Parameters screen, click on Event Action and select Produce Alert and Reset TCP Connection from the list. Then click OK.***

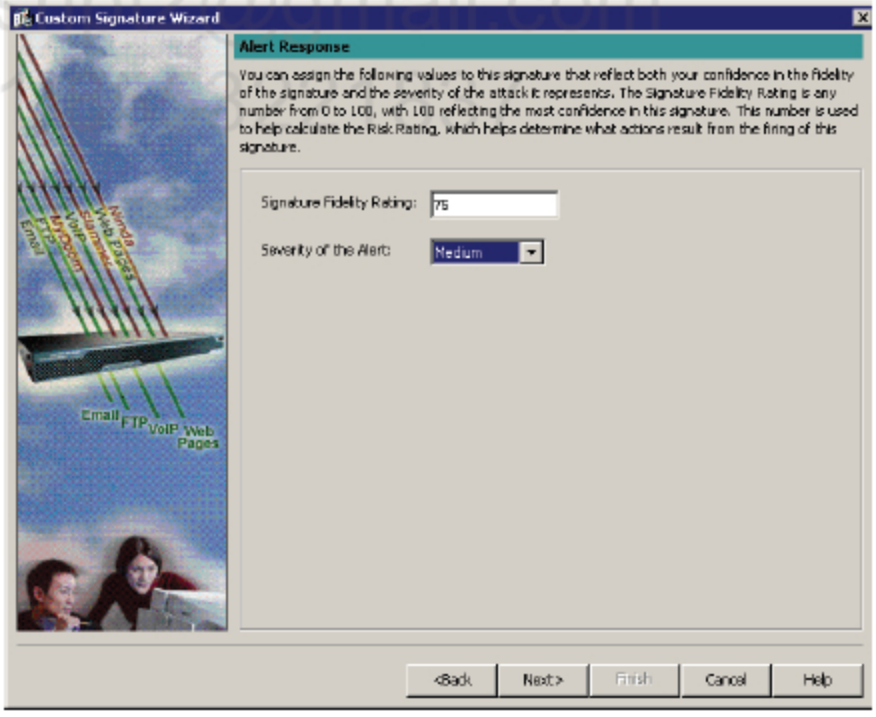



4. ***Set the Max URI Field Length to 10 and URI regex to "cisco.com". Make sure there are Service Ports of 80, 8080 and 888. Then click Next.***

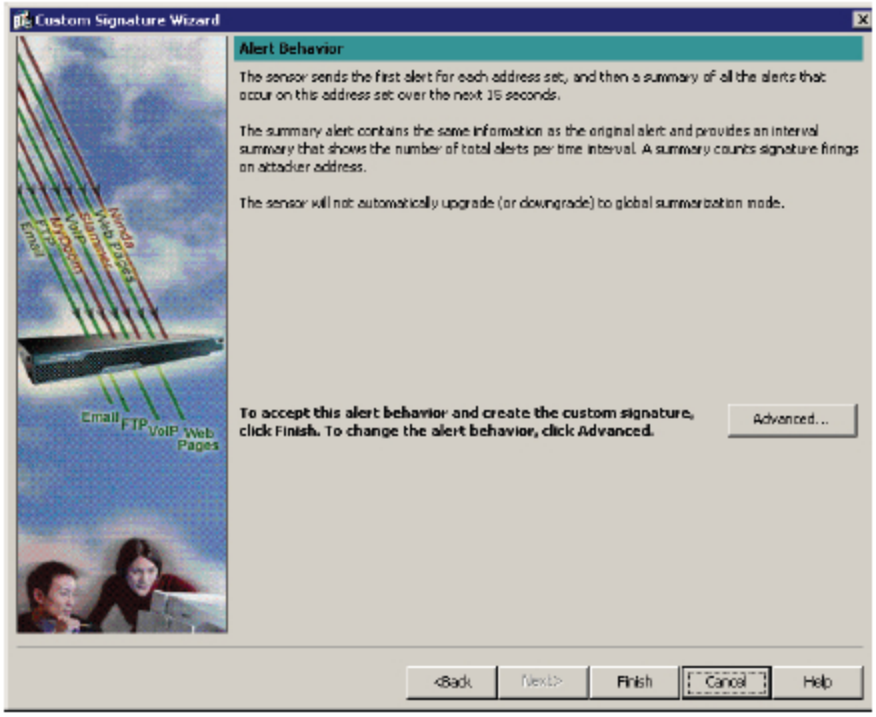





5. ***Set Signature Fidelity Rating to 75 and Action Severity to Medium. Click Next.***




6. ***Leave default settings for Alert Behavior and click Finish to close the wizard.***






## Verification

```
R2(config)#ip http server

R1#tel 10.1.12.2 80
Trying 10.1.12.2, 80 ... Open
GET cisco.com/attack.htm
[Connection to 10.1.12.2 closed by foreign host]
```

Note that the connection has been closed immediately. All conditions have been met: (1) "cisco.com" is in the URI, (2) the URI is longer than 10 characters and (3) the destination port was 80.

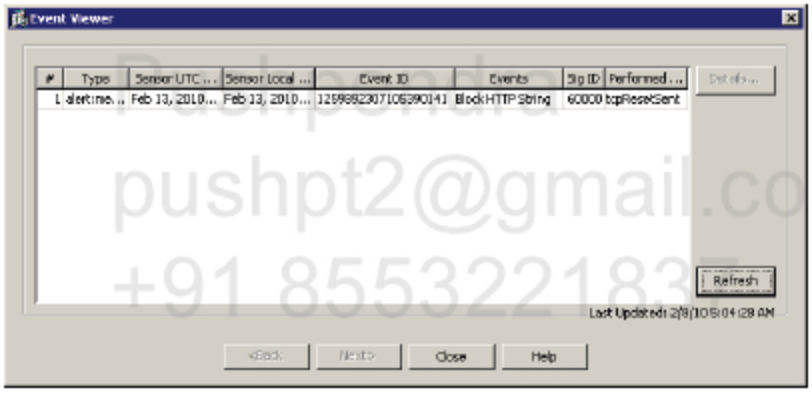
```
R1#tel 10.1.12.2 80
Trying 10.1.12.2, 80 ... Open
GET test.htm
HTTP/1.1 400 Bad Request
Date: Sun, 14 Feb 2010 13:20:51 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.12.2 closed by foreign host]
R1#
```

The packet has reached the destination. There is no "cisco.com" in the URI.

```
R1#tel 10.1.12.2 80
Trying 10.1.12.2, 80 ... Open
GET cisco.com
HTTP/1.1 400 Bad Request
Date: Sun, 14 Feb 2010 13:34:34 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.12.2 closed by foreign host]
```

The packet is allowed as "cisco.com" has only 9 characters.

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the custom signature fired.***



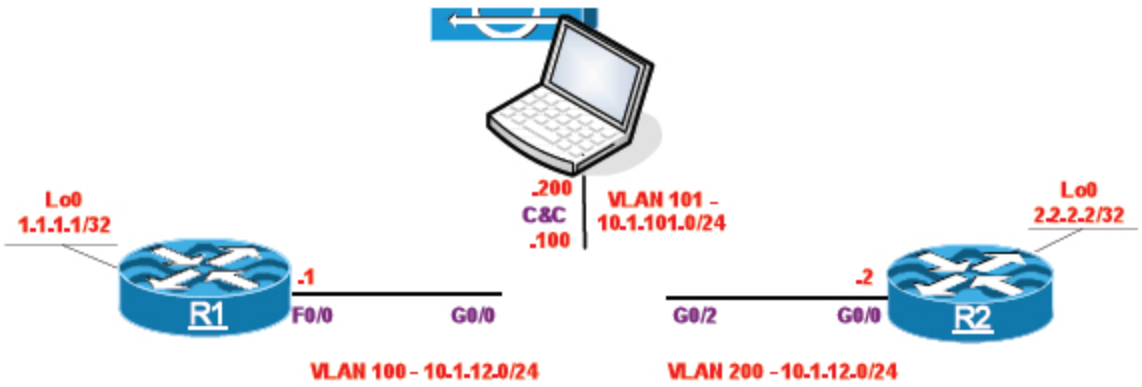

***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259892307105390141  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 13, 2010 13:02:19 UTC  offset=0  timeZone=UTC
  signature:  description=Block HTTP String  id=60000  version=custom  type=other
created=20000101
    subsigId: 0
    sigDetails: Reset and Alert for HTTP String
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
```

```
      port: 62469
    target:
      addr: 10.1.12.2  locality=OUT
      port: 80
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    tcpResetSent: true
  context:
    fromAttacker:
000000  47 45 54 20 63 69 73 63  6F 2E 63 6F 6D 2F 61 74  GET cisco.com/at
000010  74 61 63 6B 2E 68 74 6D                           tack.htm

  riskRatingValue: 66  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 46
  interface: ge0_0
  protocol: tcp
```

# LAB 2.7. Custom String TCP signature

**This lab is based on the configuration from the previous lab**






## Task 1

Create new signature to reset TELNET sessions where string "erase" is found. The signature must ignore the case of that string (case in-sensitive). You must log attacker packets and generate an alert for forensics reasons.

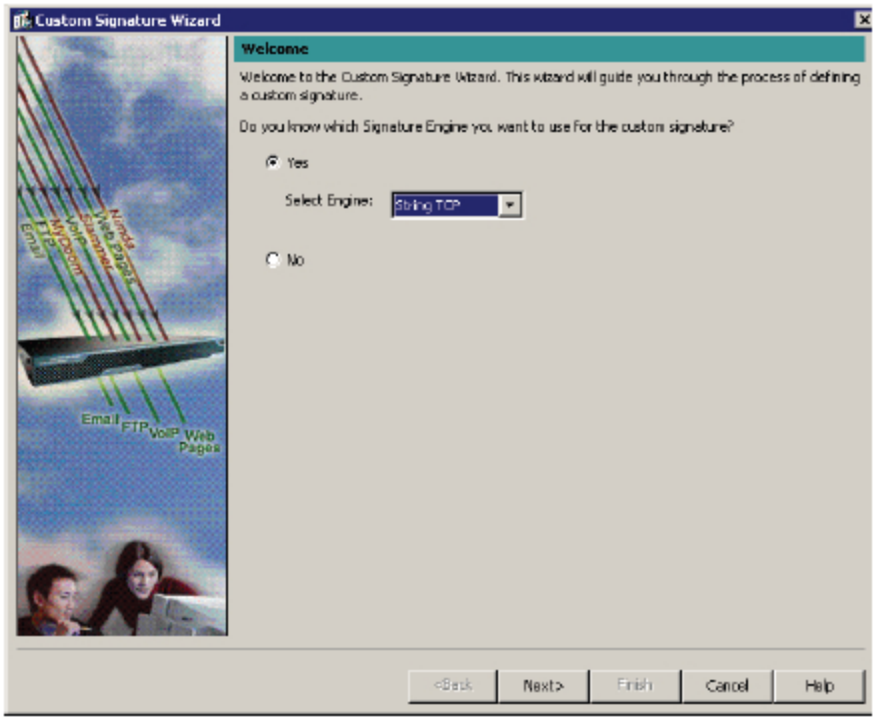
## Configuration

Complete these steps:

**Step 1** IPS configuration.

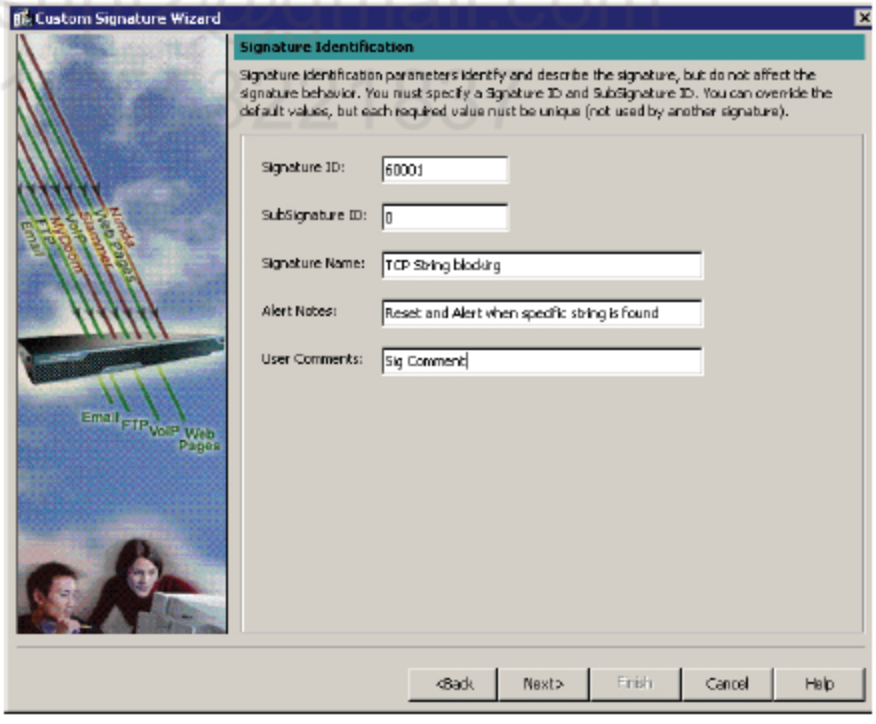
There is no TELNET specific engine so that we need to use a general engine of "String TCP". This is useful for inspecting strings carried by TCP packets.

1. *Go to Configuration → Policies → sig0 → Active Signatures and click on Signature Wizard. Select String TCP from the drop-down list and click Next.*

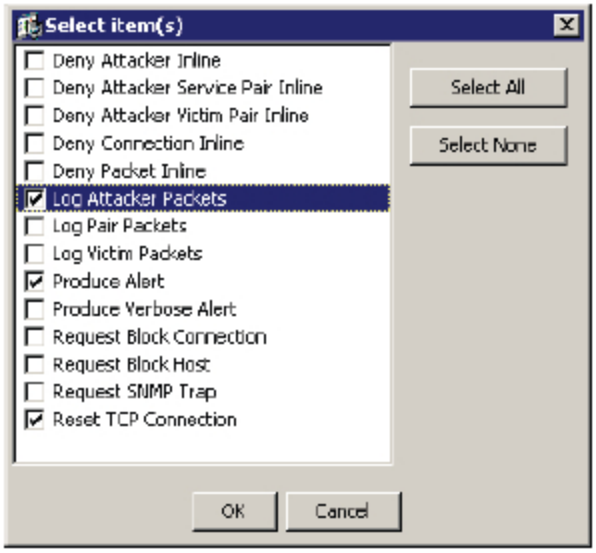




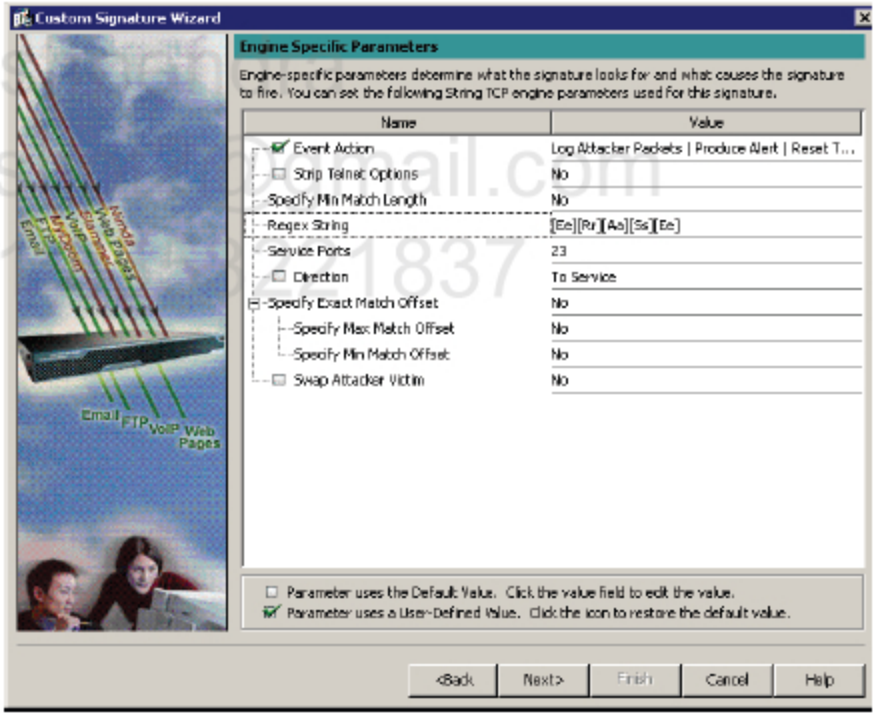

2. ***Enter the name for new signature, make some Notes and Comments and click on Next.***



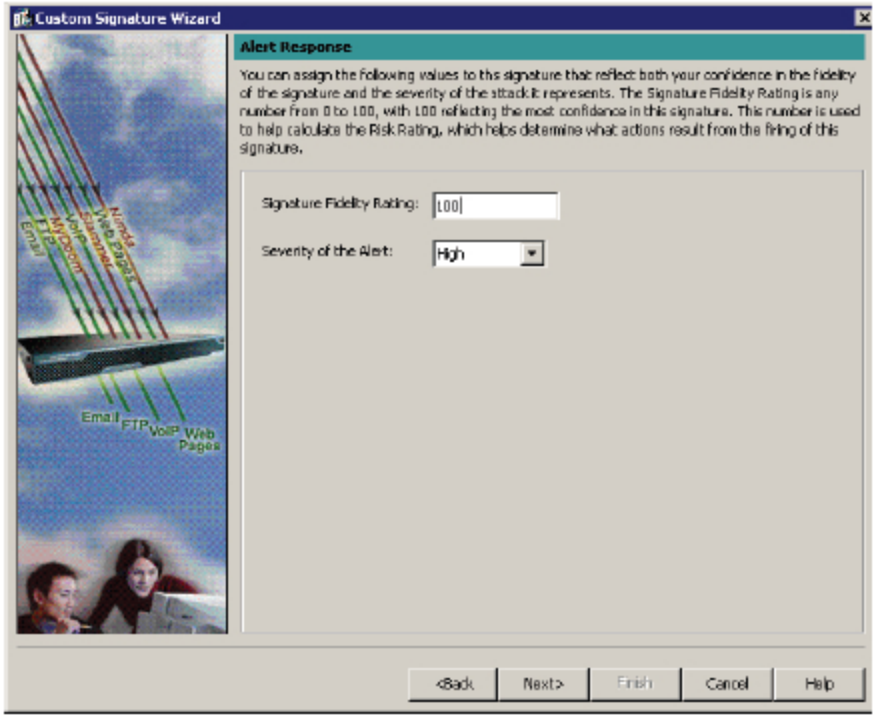

3. ***On the Engine Specific Parameters screen, click on Event Action and select Produce Alert, Log Attacker Packets and Reset TCP Connection from the list. Then click OK.***




4. ***Enter Regex String of "[Ee][Rr][Aa][Ss][Ee]" and set the Service Port to 23. Then click Next.***

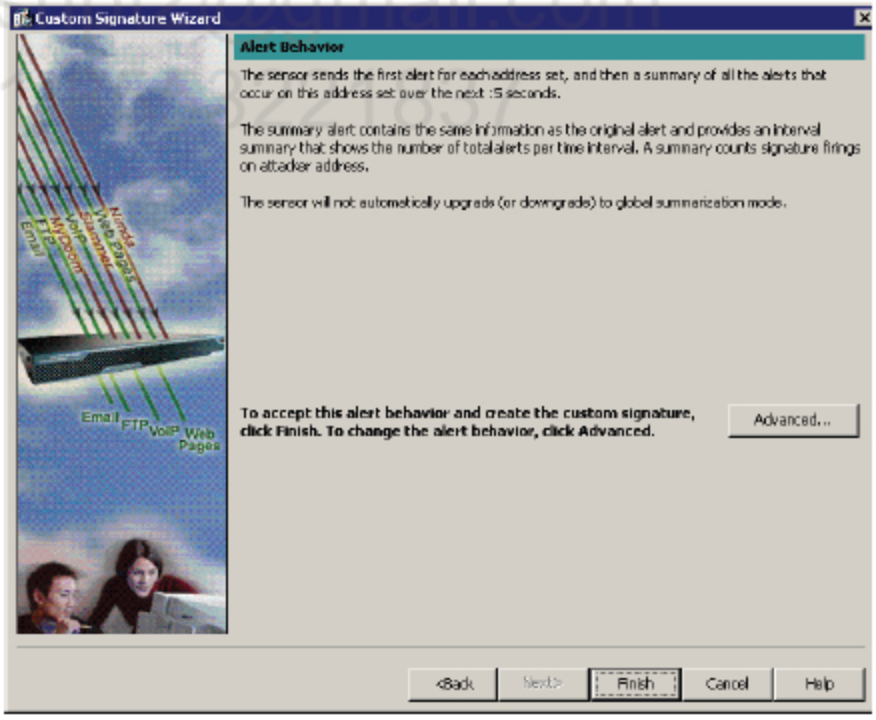


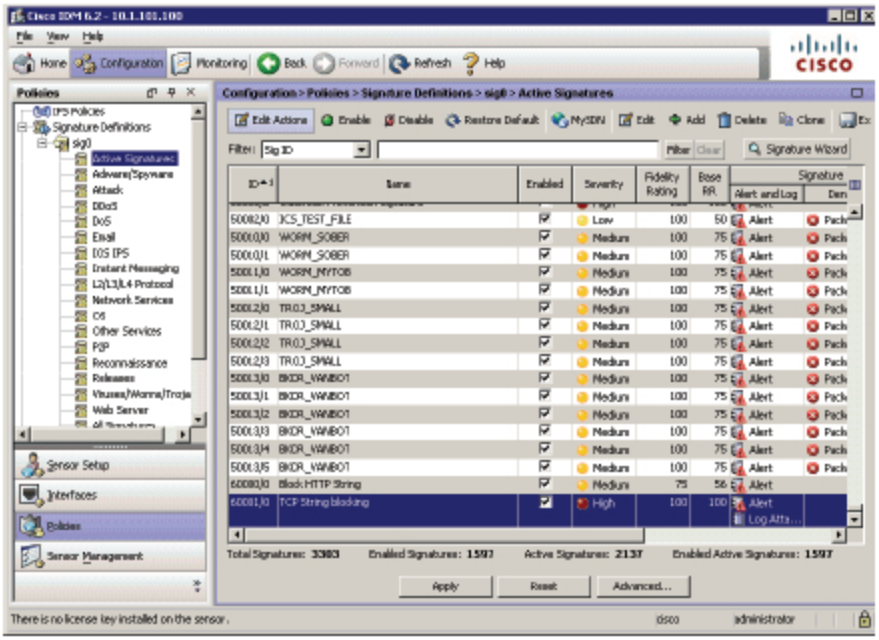

5. ***Set Signature Fidelity Rating to 100 and Action Severity to High. Click Next.***






6. ***Leave default settings for Alert Behavior and click Finish to close the wizard.***





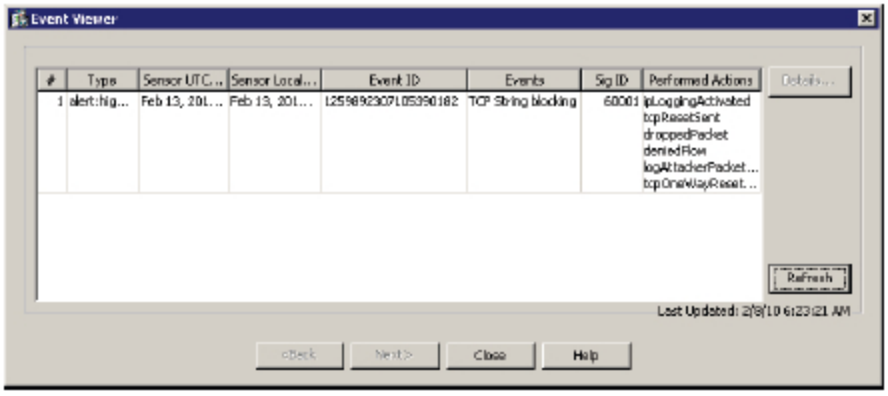



## Verification

```
R1#tel 10.1.12.2
Trying 10.1.12.2 ... Open


User Access Verification

Password:
R2>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:22
*514 vty 0                 idle                 00:00:00 10.1.12.1

  Interface    User               Mode         Idle     Peer Address

R2>eras
[Connection to 10.1.12.2 closed by foreign host]
R1#
```

Note that the connection has been terminated just after last character of the word "erase" has been sent.

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the custom signature fired.***




***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259892307105390182  vendor=Cisco  severity=high
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 13, 2010 14:23:59 UTC  offset=0  timeZone=UTC
  signature:  description=TCP String blocking  id=60001  version=custom  type=other
created=20000101
    subsigId: 0
    sigDetails: Reset and Alert when specific string is found
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
      port: 59742
    target:
      addr: 10.1.12.2  locality=OUT
      port: 23
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    ipLoggingActivated: true
    tcpResetSent: true
    droppedPacket: true
    deniedFlow: true
    logAttackerPacketsActivated: true
    tcpOneWayResetSent: true
  context:
    fromTarget:
000000  20 20 48 6F 73 74 28 73  29 20 20 20 20 20 20 20    Host(s)
000010  20 20 20 20 20 20 20 49  64 6C 65 20 20 20 20 20         Idle
000020  20 20 4C 6F 63 61 74 69  6F 6E 0D 0A 20 20 20 30    Location..   0
000030  20 63 6F 6E 20 30 20 20  20 20 20 20 20 20 20 20   con 0
000040  20 20 20 20 20 20 69 64  6C 65 20 20 20 20 20 20        idle
000050  20 20 20 20 20 20 20 20  20 20 20 30 30 3A 30 30             00:00
```

```
000060  3A 32 32 20 20 20 0D 0A  2A 35 31 34 20 76 74 79  :22   ..*514 vty
000070  20 30 20 20 20 20 20 20  20 20 20 20 20 20 20 20   0
000080  20 20 69 64 6C 65 20 20  20 20 20 20 20 20 20 20    idle
000090  20 20 20 20 20 20 20 30  30 3A 30 30 3A 30 30 20         00:00:00
0000A0  31 30 2E 31 2E 31 32 2E  31 0D 0A 0D 0A 20 20 49  10.1.12.1....  I
0000B0  6E 74 65 72 66 61 63 65  20 20 20 20 55 73 65 72  nterface    User
0000C0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 4D                 M
0000D0  6F 64 65 20 20 20 20 20  20 20 20 20 49 64 6C 65  ode         Idle
0000E0  20 20 20 20 20 50 65 65  72 20 41 64 64 72 65 73       Peer Addres
0000F0  73 0D 0A 0D 0A 52 32 3E  65 08 20 08 65 72 61 73  s....R2>e. .eras

    fromAttacker:
000000  FF FD 03 FF FB 20 FF FB  1F FF FB 21 FF FD 01 FF  ..... .....!....
000010  FC 18 FF FA 1F 00 50 00  18 FF F0 FF FC 20 63 69  ......P...... ci
000020  73 63 6F 0D 0A 73 68 20  75 73 65 72 73 0D 0A 65  sco..sh users..e
000030  7F 65 72 61 73 65                                 .erase

  ipLogIds:
    ipLogId: 1701868398
  riskRatingValue: 100  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 65
  interface: ge0_0
  protocol: tcp
```

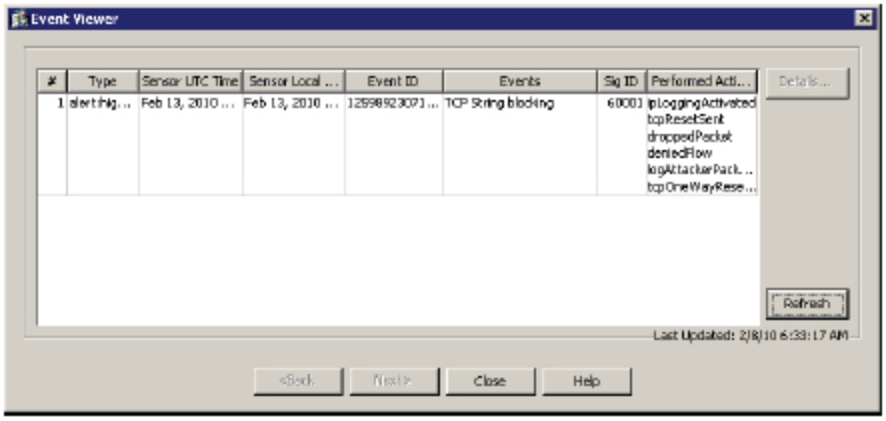


See that target got only "eras" string (fromTarget log) as it is blocked before it hits the destination (fromAttacker log).

```
R1#tel 10.1.12.2
Trying 10.1.12.2 ... Open


User Access Verification

Password:
R2>erAs
[Connection to 10.1.12.2 closed by foreign host]
R1#
```

The signature is not case sensitive.

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the custom signature fired.***



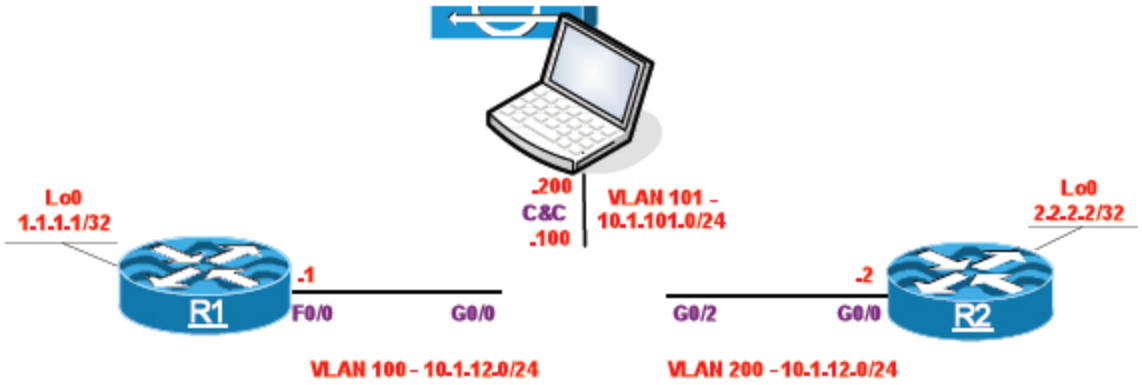

***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259892307105390200  vendor=Cisco  severity=high
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 13, 2010 14:33:50 UTC  offset=0  timeZone=UTC
  signature:  description=TCP String blocking  id=60001  version=custom  type=other
created=20000101
    subsigId: 0
    sigDetails: Reset and Alert when specific string is found
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
      port: 41147
    target:
      addr: 10.1.12.2  locality=OUT
      port: 23
      os:  idSource=unknown  type=unknown  relevance=relevant
  actions:
    ipLoggingActivated: true
    tcpResetSent: true
    droppedPacket: true
    deniedFlow: true
    logAttackerPacketsActivated: true
    tcpOneWayResetSent: true
  context:
    fromTarget:
000000  FF FB 01 FF FB 03 FF FD  18 FF FD 1F 0D 0A 0D 0A  ................
000010  55 73 65 72 20 41 63 63  65 73 73 20 56 65 72 69  User Access Veri
000020  66 69 63 61 74 69 6F 6E  0D 0A 0D 0A 50 61 73 73  fication....Pass
000030  77 6F 72 64 3A 20 FF FE  20 FF FD 21 FF FA 21 00  word: .. ..!..!.
000040  FF F0 FF FE 18 0D 0A 52  32 3E 65 72 41 73        .......R2>erAs
```

```
    fromAttacker:
000000  FF FD 03 FF FB 20 FF FB  1F FF FB 21 FF FD 01 FF  ..... .....!....
000010  FC 18 FF FA 1F 00 50 00  18 FF F0 FF FC 20 63 69  ......P...... ci
000020  73 63 6F 0D 0A 65 72 41  73 65                    sco..erAse

  ipLogIds:
    ipLogId: 1701868399
  riskRatingValue: 100  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 65
  interface: ge0_0
  protocol: tcp
```

# LAB 2.8. Custom ATOMIC IP signature

**This lab is based on the configuration from the previous lab**






## Task 1

Create new signature with ID of 60002 to drop ICMP Echo Requests packets with an IP payload length between 500 and 600 bytes. The signature should be triggered only for RFC1918 IP addresses and should generate alert and save dump of sniffed packets for further investigation.

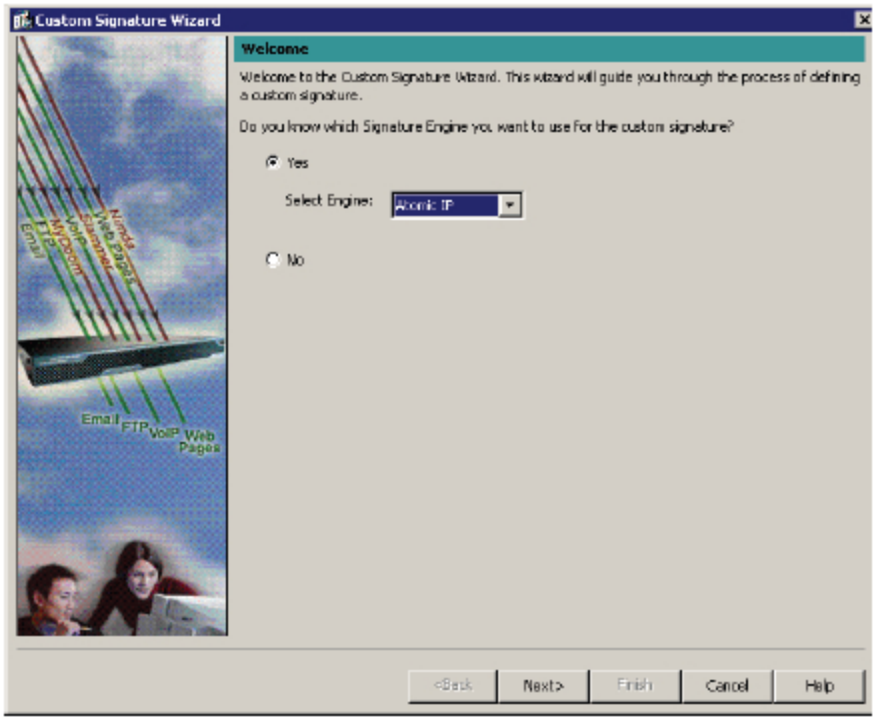
## Configuration

Complete these steps:

**Step 1** IPS configuration.

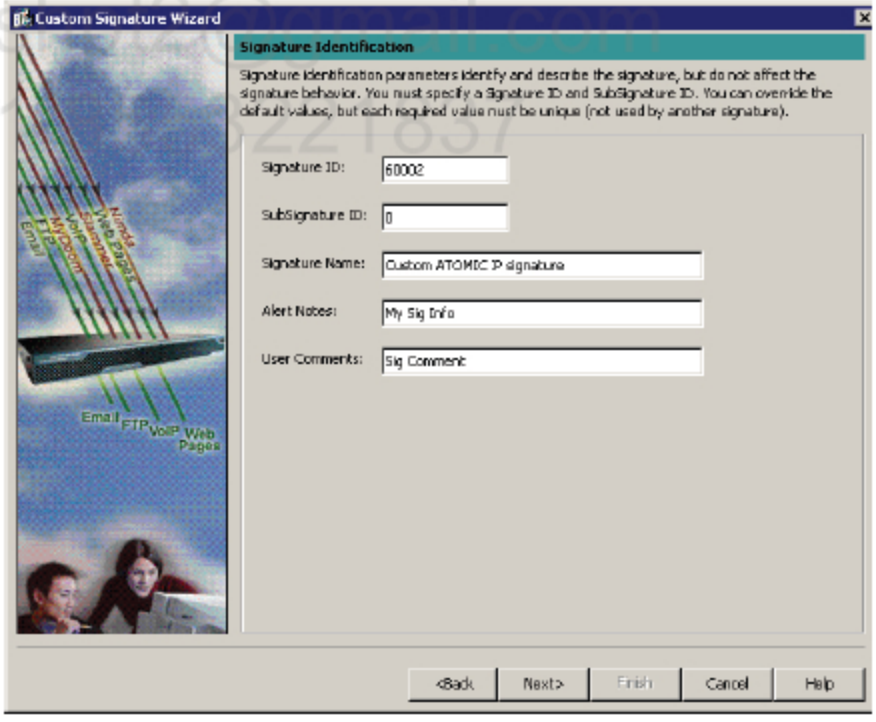
```
Here we're looking for one specific packet so that it is perfect
occasion to use "Atomic IP" engine. This engine is developed to catch
on packets basis and we can use it to use deep packet matching.
```

1. ***Go to Configuration → Policies → sig0 → Active Signatures and click on Signature Wizard. Select Atomic IP from the drop-down list and click Next.***

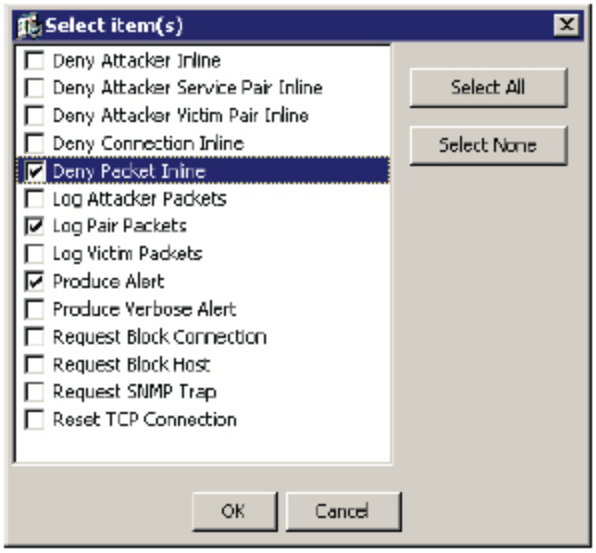




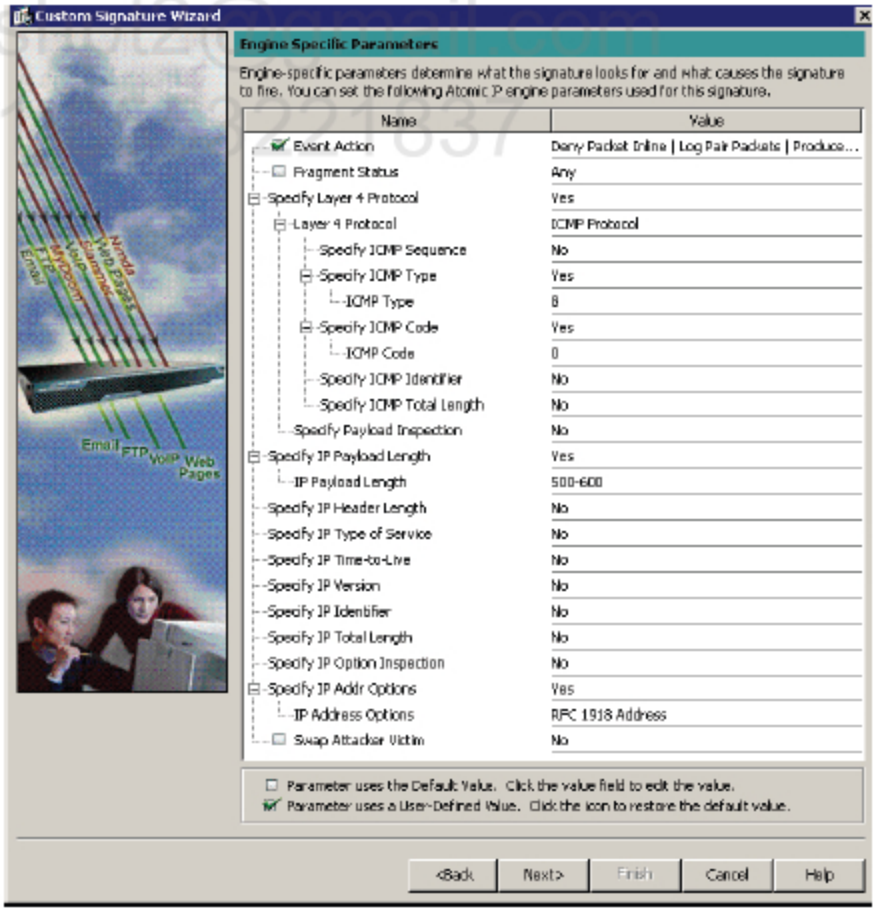

2. ***Set Signature ID to 60002, enter the name for new signature, make some Notes and Comments and click on Next.***



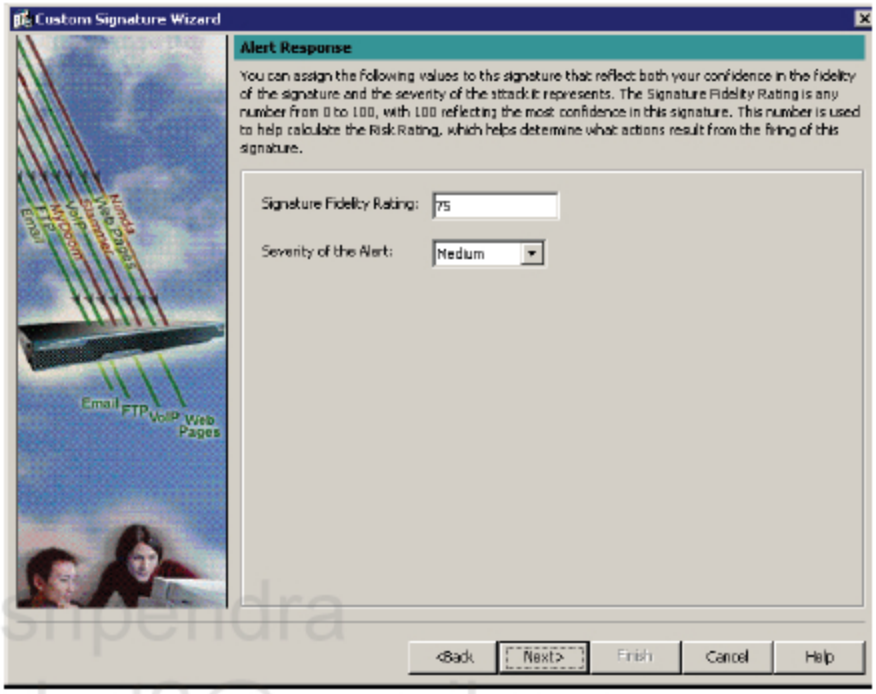

3. ***On the Engine Specific Parameters screen, click on Event Action and select Produce Alert and Deny Packet Inline from the list. Then click OK.***




4. ***Set Specific Layer 4 Protocol item to Yes, and chose ICMP Protocol for Layer 4 Protocol setting. Configure ICMP Type to 8 and ICMP code to 0. Then, set Specify IP Payload Length item to Yes and enter 500-600 in a field for IP Payload Length option. Make sure you also check RFC 1918 Address in IP Address Options item.***

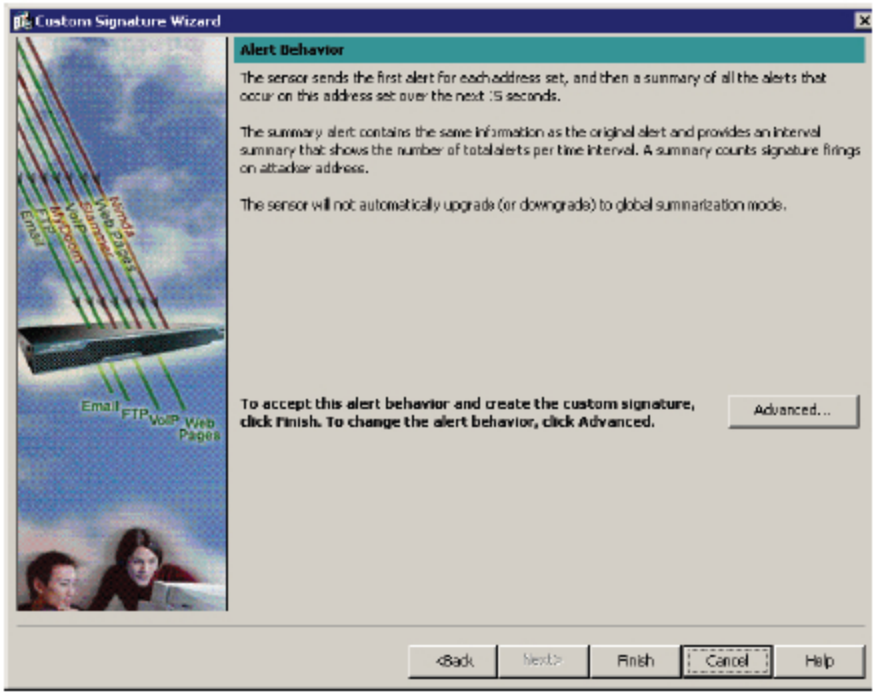


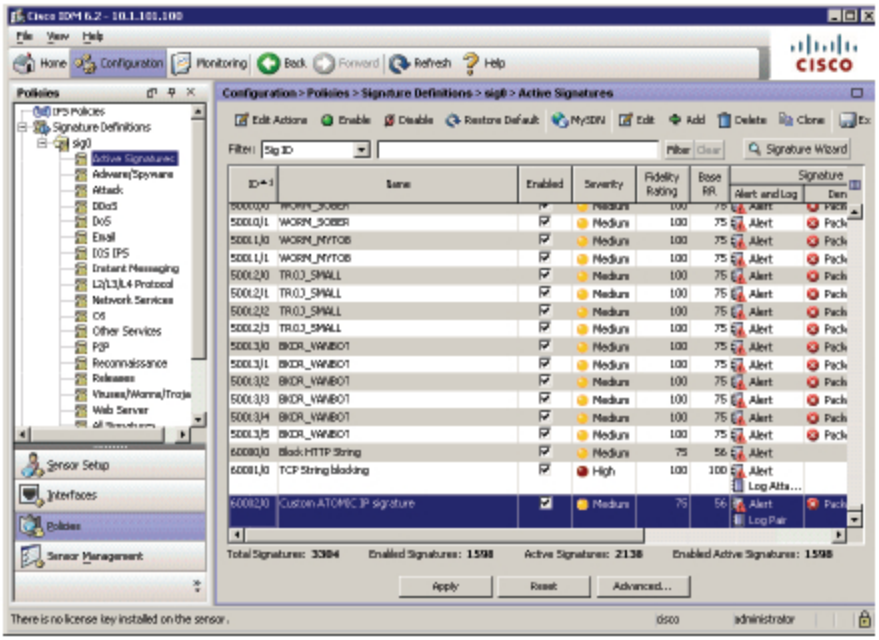
5. **Set Signature Fidelity Rating to 75 and Action Severity to Medium. Click Next.**






6. **Leave default settings for Alert Behavior and click Finish to close the wizard.**








## Verification

```
R1#ping 10.1.12.2 size 500

Type escape sequence to abort.
Sending 5, 500-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 10.1.12.2 size 501

Type escape sequence to abort.
Sending 5, 501-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

The ICMP packets of size 500 bytes and 501 bytes are not getting blocked.

```
R1#ping 10.1.12.2 size 520

Type escape sequence to abort.
Sending 5, 520-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

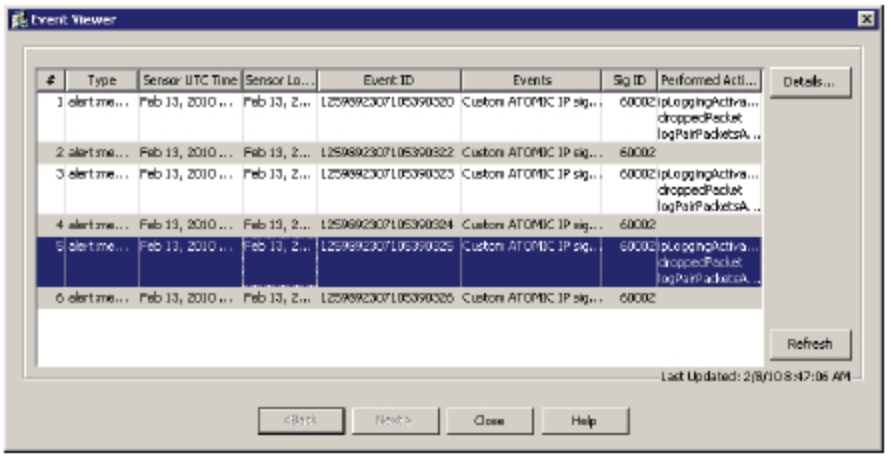
The ICMP packets of size 520 bytes are being blocked. This is because there is additional 20 bytes of IP Header in the packets. Try lower size to see that:

```
R1#ping 10.1.12.2 size 519

Type escape sequence to abort.
Sending 5, 519-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 10.1.12.2 size 620

Type escape sequence to abort.
Sending 5, 620-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#ping 10.1.12.2 size 621

Type escape sequence to abort.
Sending 5, 621-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
```



**Note that there is a difference in ICMP implementation in Cisco and Microsoft Windows. When you ping on Cisco using 1000 bytes packets there will be 980 bytes of data in the ICMP packet so that the overall IP packet length will be 1000 bytes.**
**However, when you ping using MS Windows a 1000 bytes packet will have 1000 bytes of ICMP data and additional 20 bytes of IP Header.**

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the custom signature fired.***



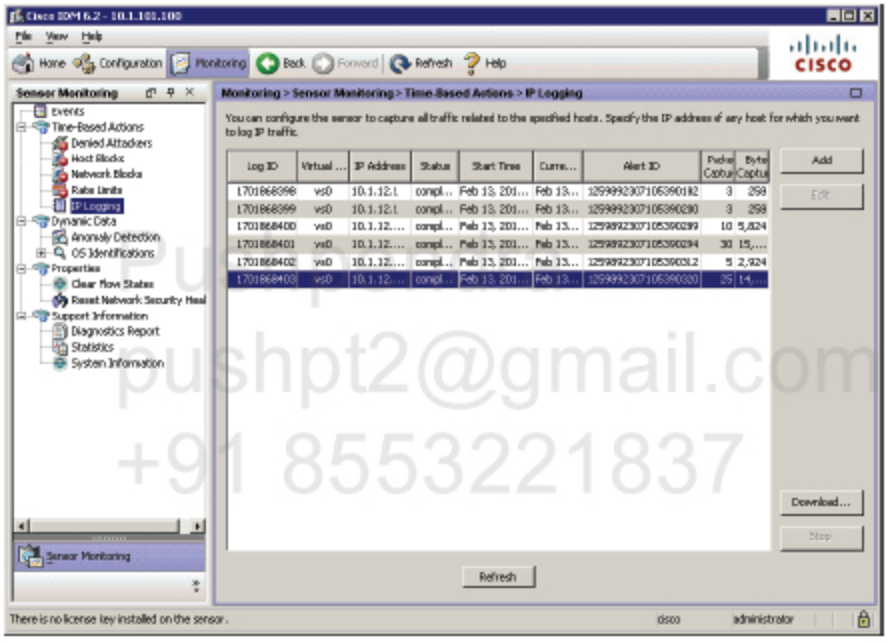
***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259892307105390325  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 13, 2010 16:44:51 UTC  offset=0  timeZone=UTC
  signature:   description=Custom ATOMIC IP signature  id=60002  version=custom
type=other  created=20000101
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
    target:
      addr: 10.1.12.2  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    ipLoggingActivated: true
    droppedPacket: true
    logPairPacketsActivated: true
  ipLogIds:
    ipLogId: 1701868403
  riskRatingValue: 66  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 31
  interface: ge0_0
  protocol: icmp



evIdsAlert: eventId=1259892307105390326  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 13, 2010 16:45:06 UTC  offset=0  timeZone=UTC
  signature:   description=Custom ATOMIC IP signature  id=60002  version=custom
type=other  created=20000101
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
    target:
```

```
    addr: 0.0.0.0  locality=OUT
    os:   idSource=unknown  type=unknown  relevance=unknown
summary: 4  final=true  initialAlert=1259892307105390325  summaryType=Regular
alertDetails: Regular Summary: 4 events this interval ;
riskRatingValue: 56  targetValueRating=medium
threatRatingValue: 56
interface: ge0_0
protocol: icmp
```

This is a summary for 4 ICMP packets. This event is "attached" to the previous event by specifying "initialAlert" number.

***Go to Monitoring → IP Logging and see packet capture triggered by the custom signature. The Alert ID identifies the event which has triggered the IP logging.***

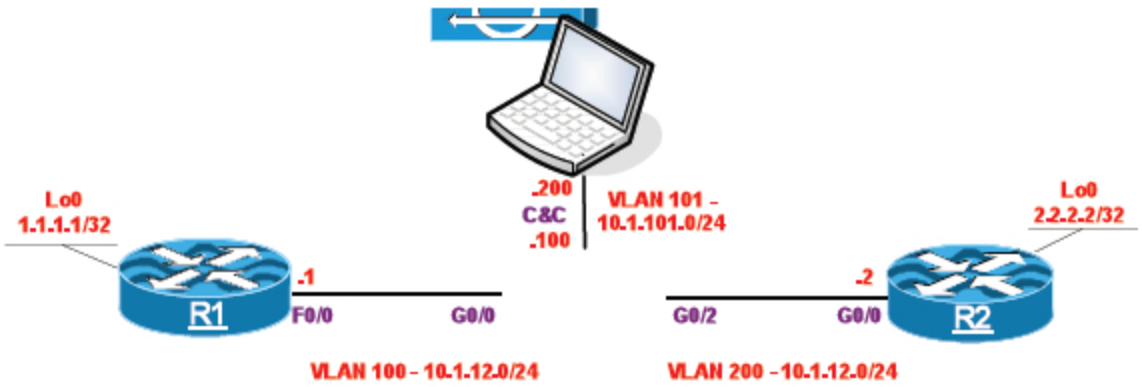



```
R1#pi 2.2.2.2 so lo0 size 550

Type escape sequence to abort.
Sending 5, 550-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
```

This is not RFC1918 IP address! That's why the signature has not been triggered.

# LAB 2.9. META signature

**This lab is based on the configuration from the previous lab**






## Task 1

Configure a new signature so that it triggers when someone pings R2's G0/0 IP address with ICMP Echo Request packet of size bigger than 2000 bytes and in the time window of 30 seconds someone tries to connect to the HTTP server located at R2 and tries to get attack.txt file. You must generate an alert when those conditions are met and block attacker inline for 2 hours.

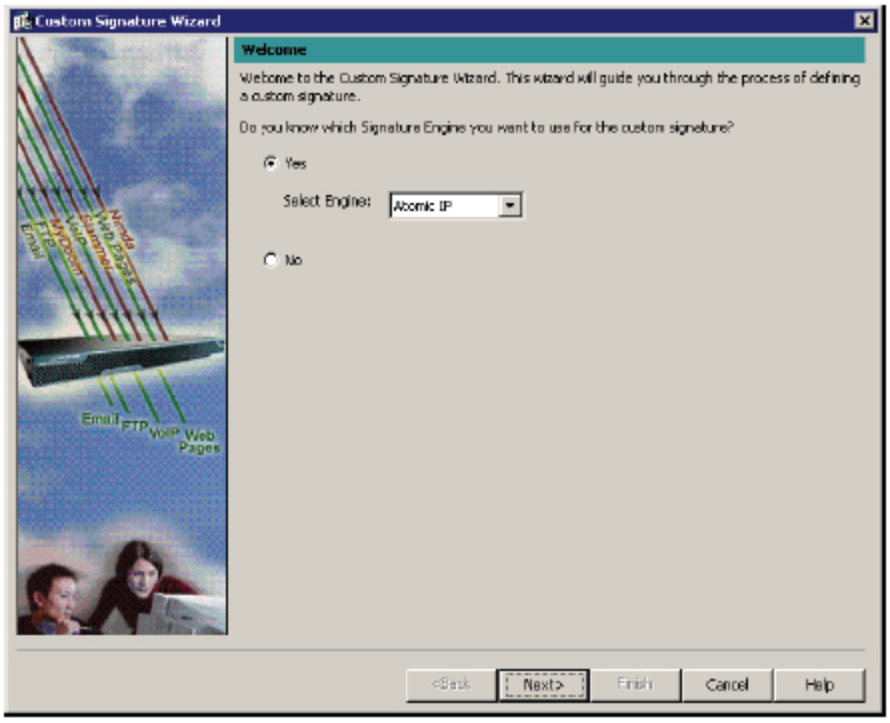
*The META engine provides event correlation on the sensor. Using the META engine can dramatically reduce the number of alerts by combining signatures. The META engine enables you to disable the component signatures, so that they do not generate alerts and receive only a META alert that indicates that the attack is happening. By doing the correlation on the sensor itself rather than at a management console, the sensor can take action immediately.*

## Configuration

Complete these steps:

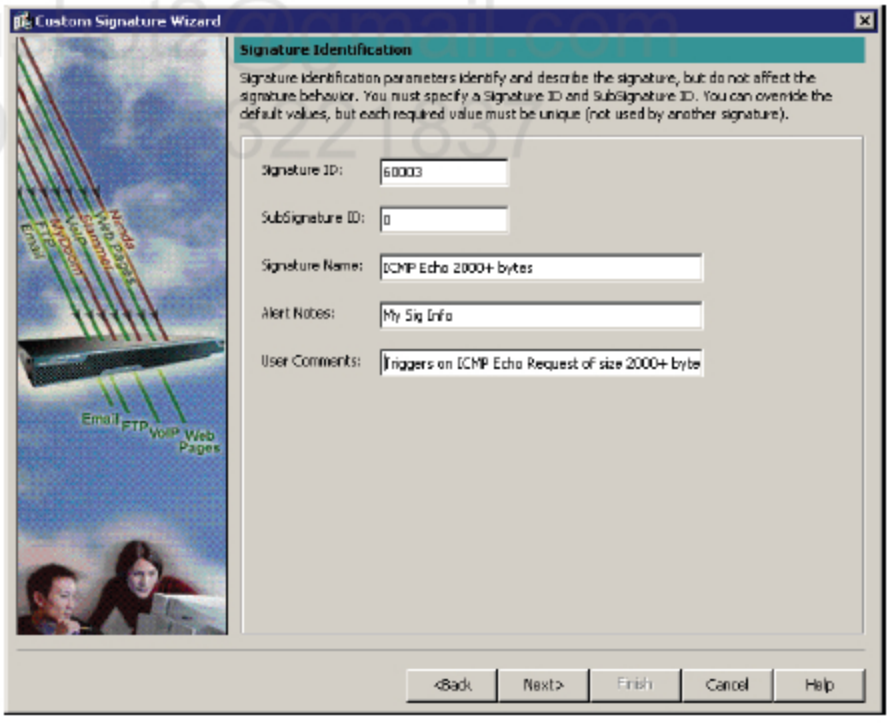
**Step 1** IPS configuration.

1. *Go to Configuration → Policies → sig0 → Active Signatures and click on Signature Wizard. Select Atomic IP from the drop-down list and click Next.*



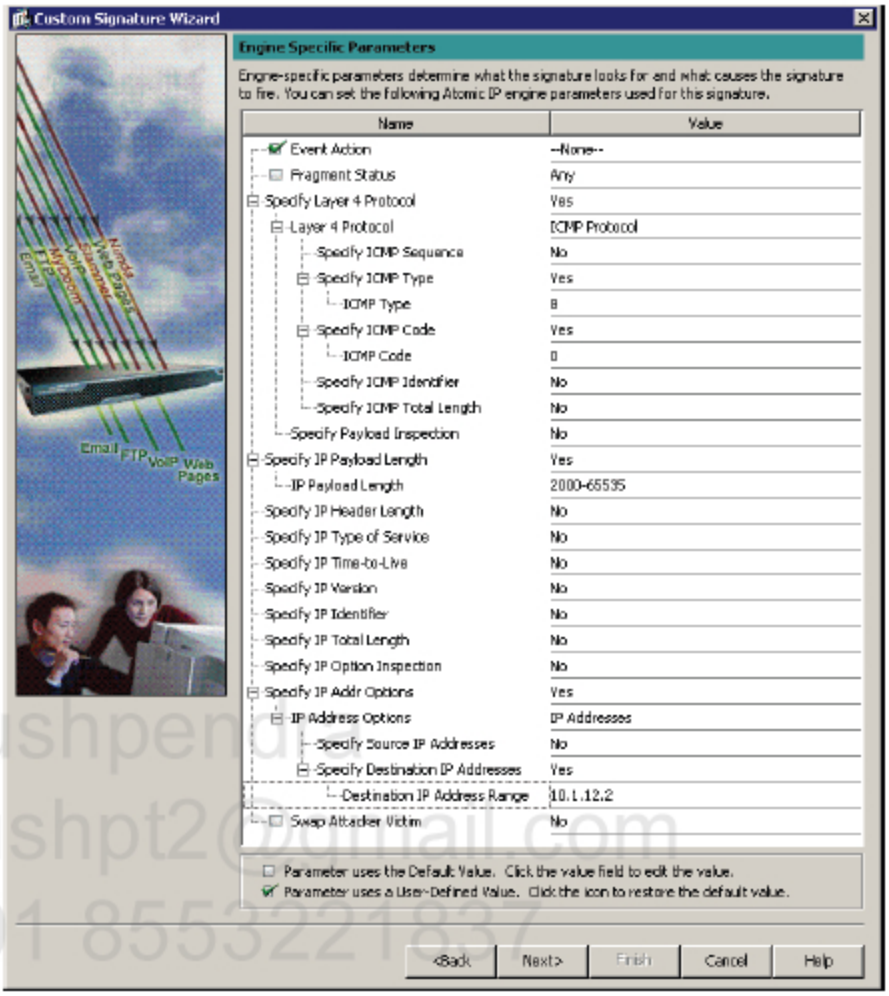



2. ***Enter the name for new signature, make some Notes and Comments and click on Next.***

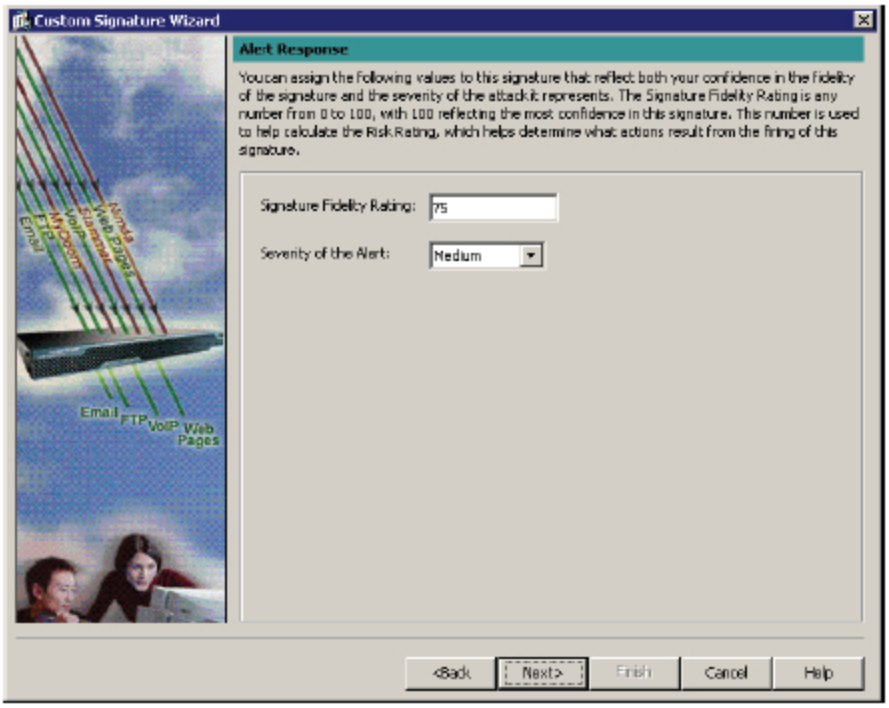



3. ***On the Engine Specific Parameters screen, disable any of Event Actions associated with the signature, select ICMP Protocol as Layer 4 Protocol and use ICMP Type of 8 and ICMP Code of 0. Set IP Payload Length to***

*the range of 2000-65535 and Destination IP Address Range to 10.1.12.2.*

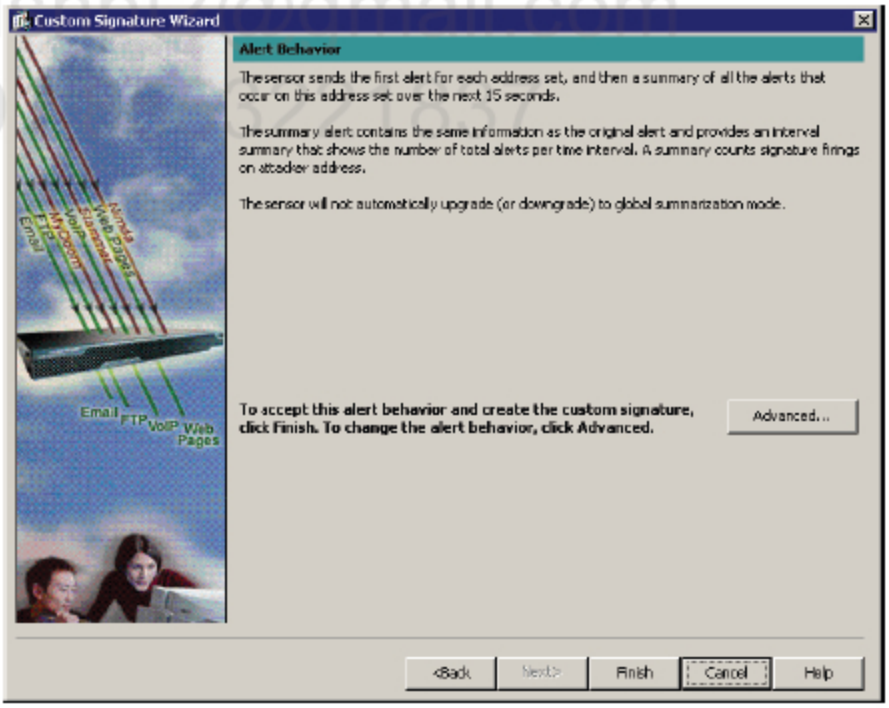



4. ***Set Signature Fidelity Rating to 75 and Action Severity to Medium. Click Next.***

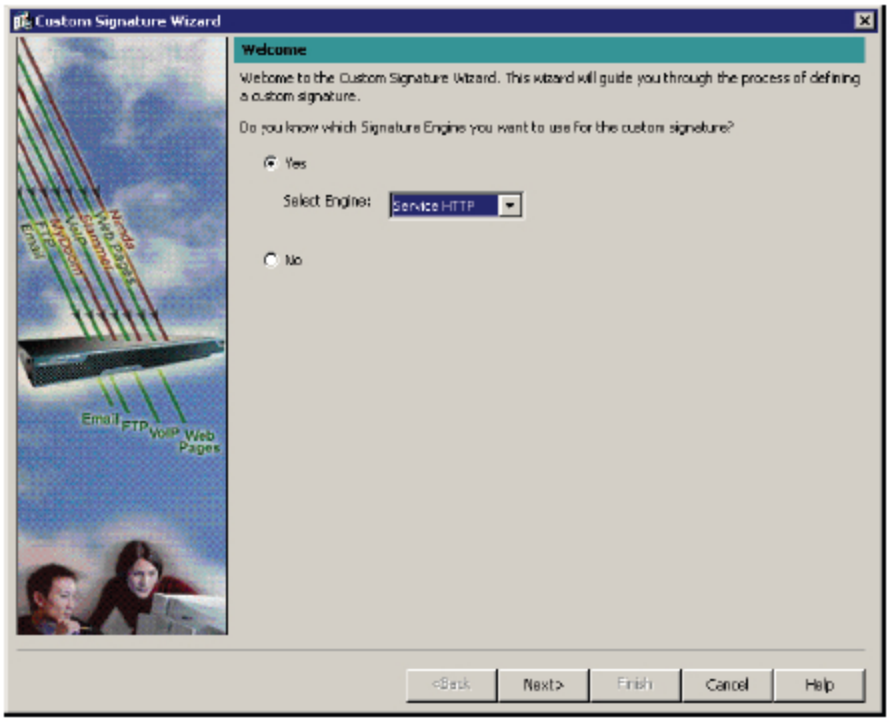





5. ***Leave default settings for Alert Behavior and click Finish to close the wizard.***

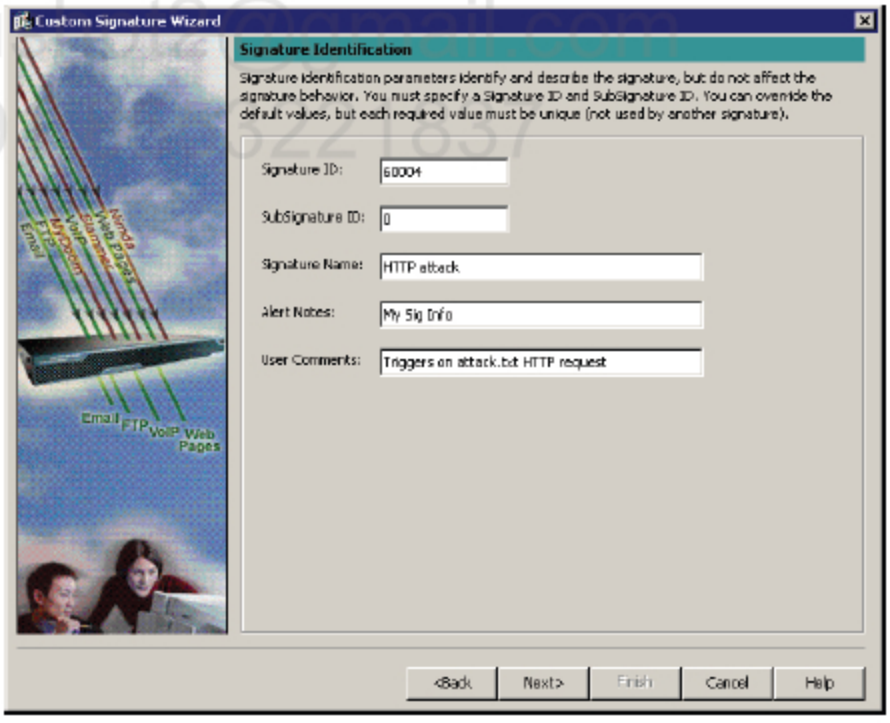



6. ***Open up the Signature Wizard again and select Service HTTP from the drop-down list and click Next.***

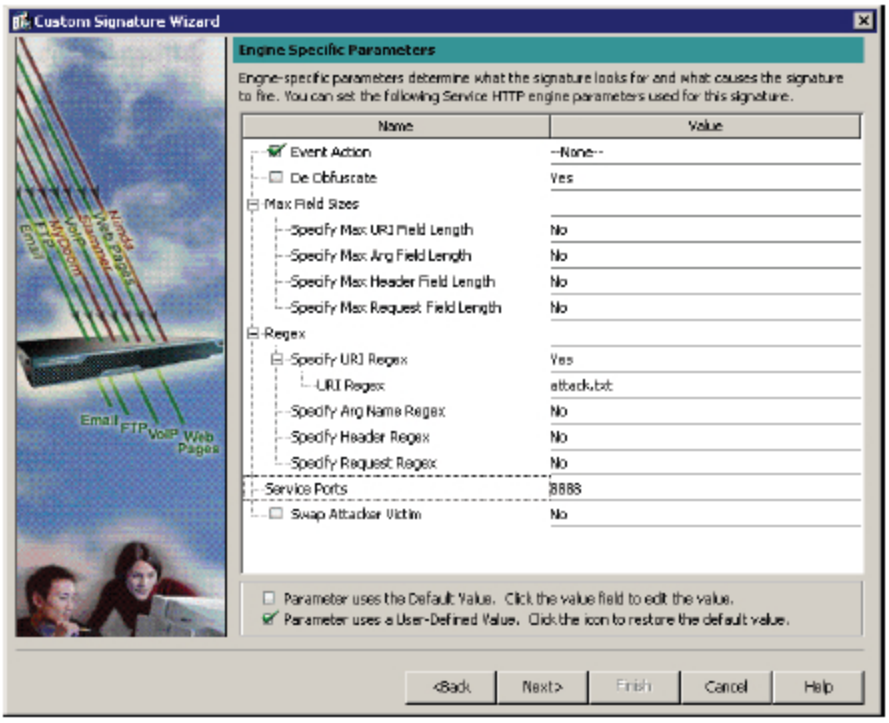




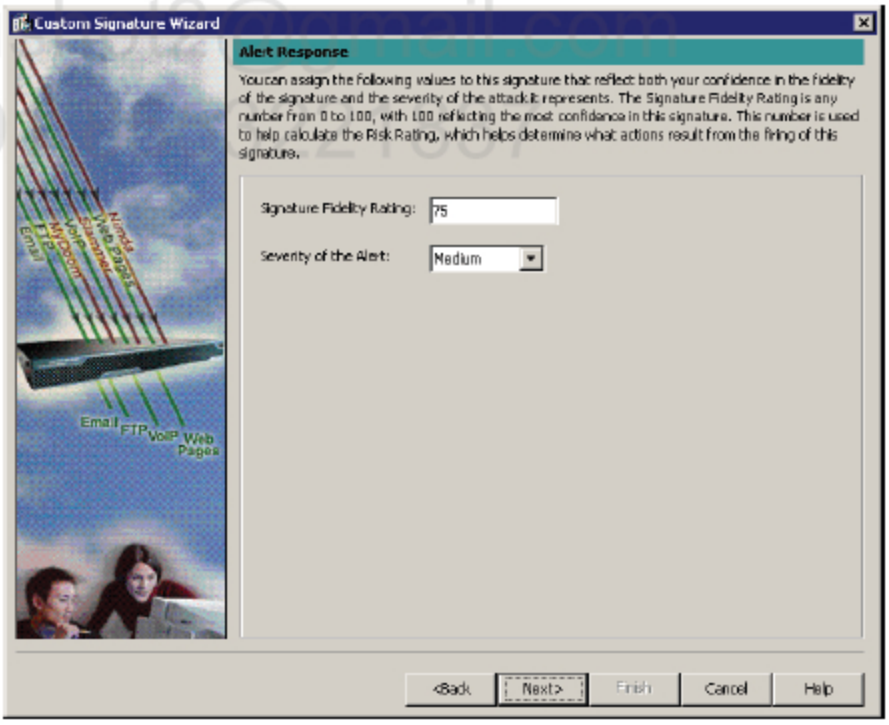

7. ***Enter the name for new signature, make some Notes and Comments and click on Next.***



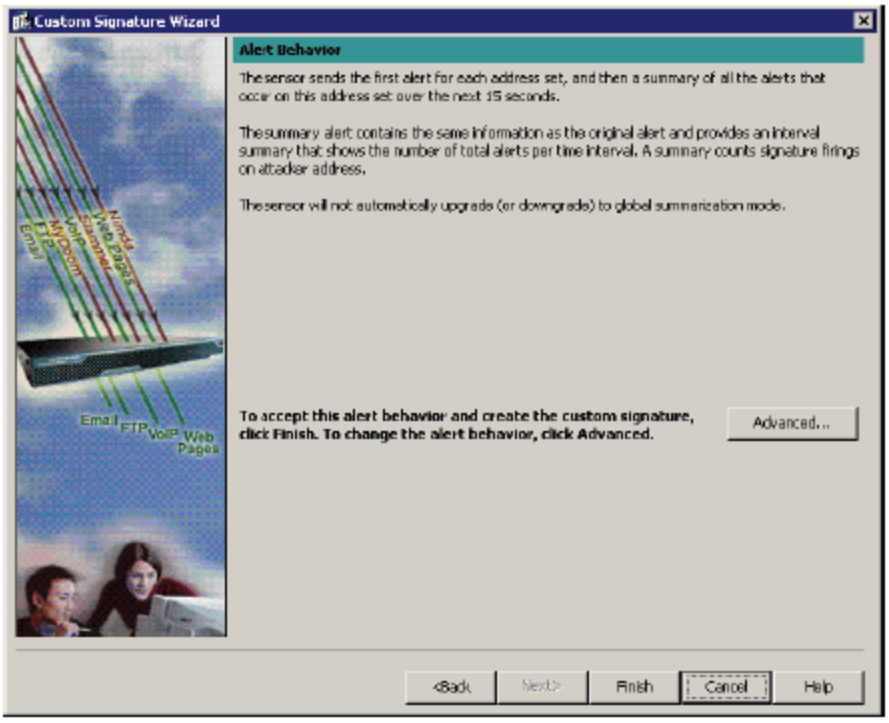

8. ***On the Engine Specific Parameters screen, disable any of Event Actions associated with the signature; configure Regex/Specify URI Regex/URI Regex to "attack.txt" and Service Ports to 8888.***




9. ***Set Signature Fidelity Rating to 75 and Action Severity to Medium. Click Next.***

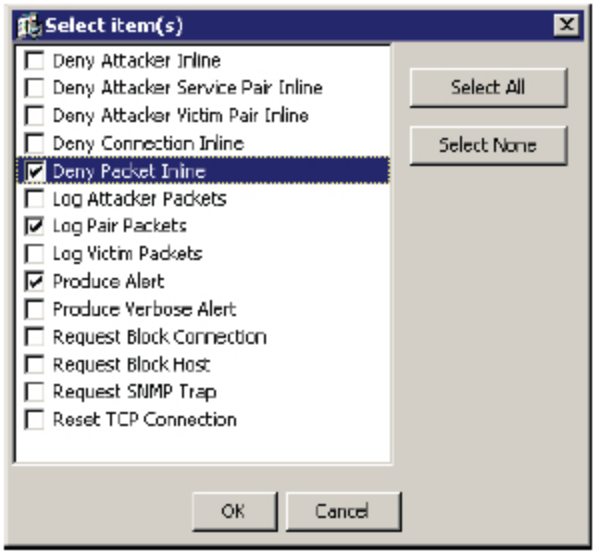



10. ***Leave default settings for Alert Behavior and click Finish to close the wizard.***



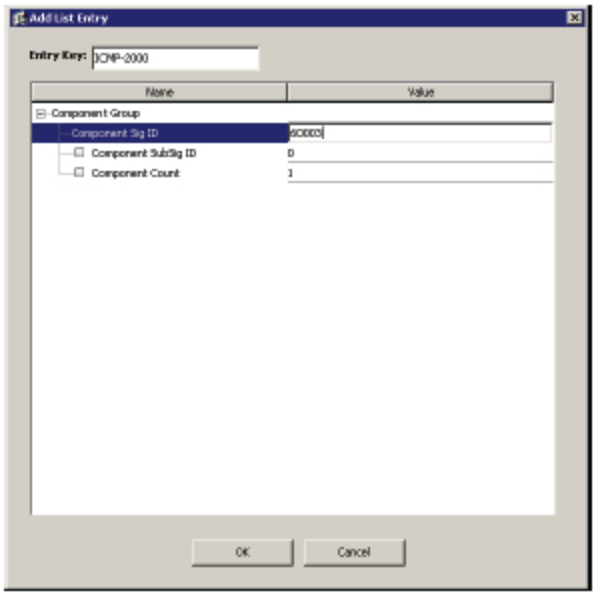



11. ***Go to Configuration → Policies → sig0 → Active Signatures and click on Signature Wizard. Select Meta from the drop-down list and click Next.***
    ***Enter the name for new signature, make some Notes and Comments and click on Next. On the Engine Specific Parameters screen, click on Event Action and select Produce Alert and Deny Packet Inline from the list. Then click OK.***

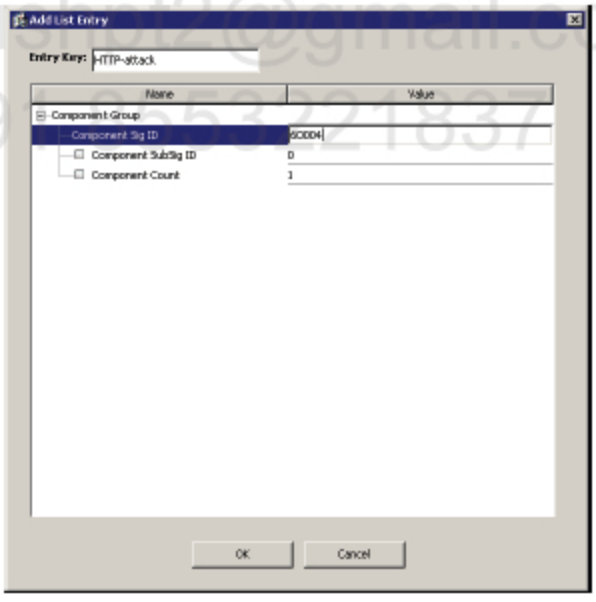



12. ***Click on Component List option and click Add button. Enter the first***

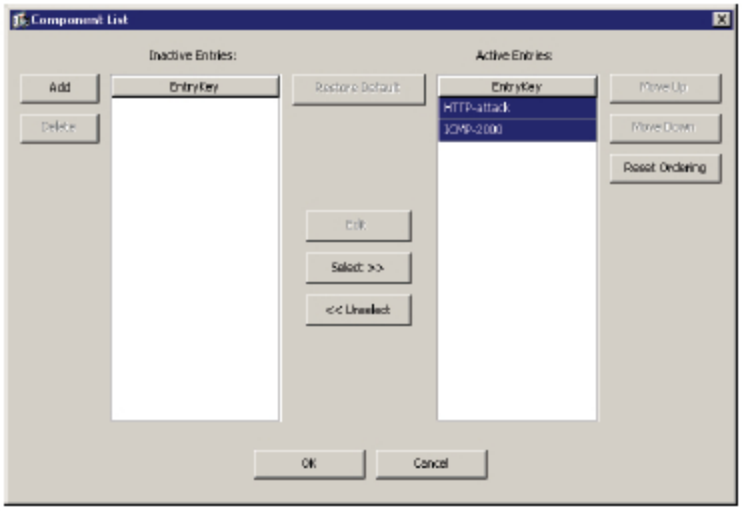
***sub-signature name (it can be some arbitrary name), set Component Sig ID to 60003 (must be real signature ID). Click OK.***



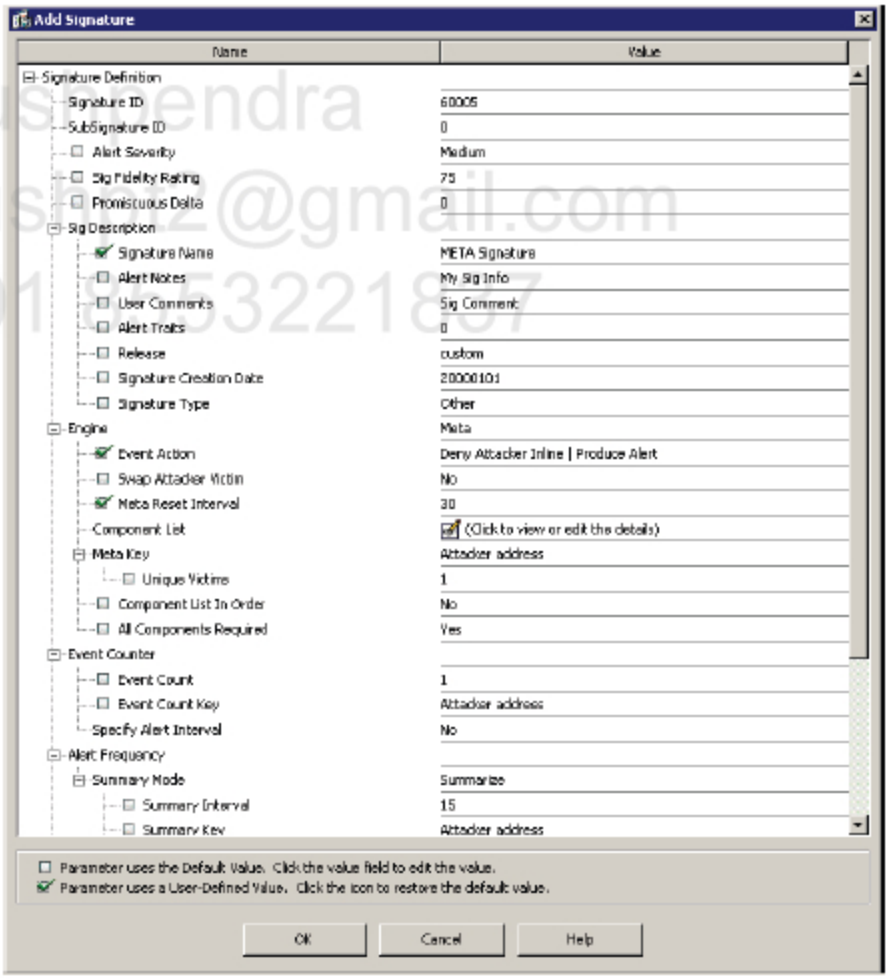

13. ***Click Add button again to add second sub-signature. Enter some name (it can be some arbitrary name), set Component Sig ID to 60004 (must be real signature ID). Click OK.***

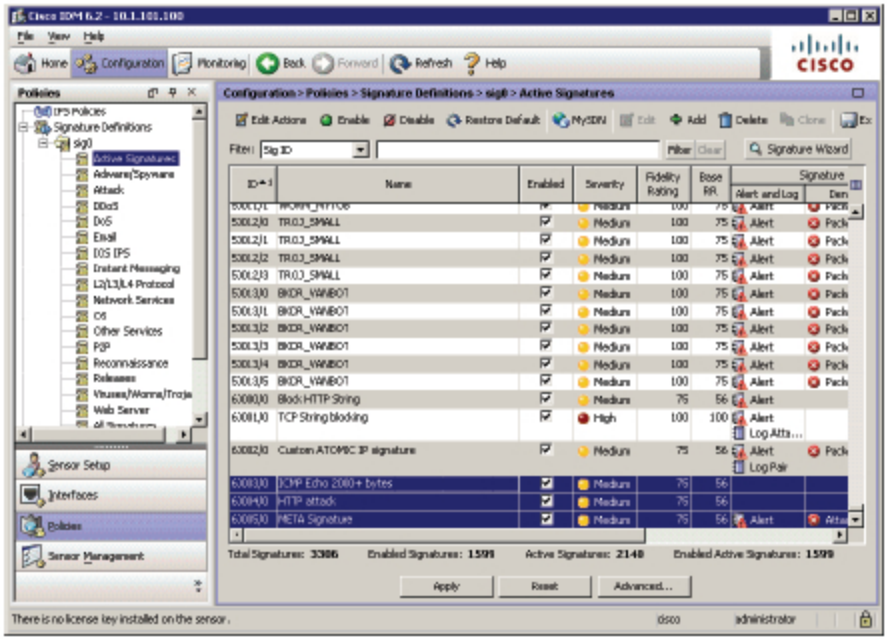



14. ***Both sub-signatures are listed under Inactive Entries column. Highlight them and click on Select button to move them to right column (Active entries). Then click OK.***



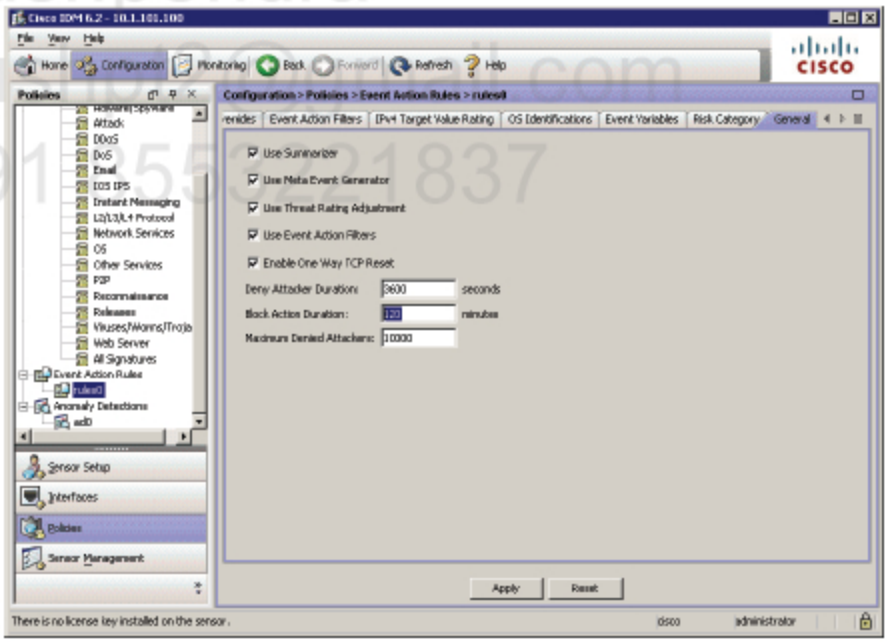

***15. On the Meta signature settings page, set Meta Reset Interval to 30 seconds. Click OK.***






**Note that only META signature has Action configured.**

***16. Go to Configuration → Policies → Event Action Rules → rules0 → (tab) General and set Block Action Duration to 120 minutes.***






## Verification

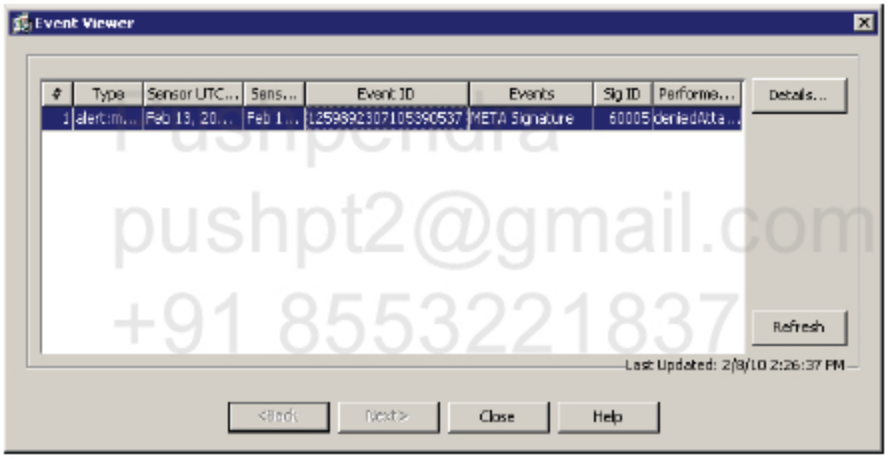
```
R2(config)#ip http port 8888
```

```
R1#pi 10.1.12.2 size 5000
```

```
Type escape sequence to abort.
Sending 5, 5000-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

R1#tel 10.1.12.2 8888
Trying 10.1.12.2, 8888 ... Open
GET attack.txt


<...session hangs...>
```

Two "attacks" have been generated withing 30 seconds.

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the custom META Signature fired.***



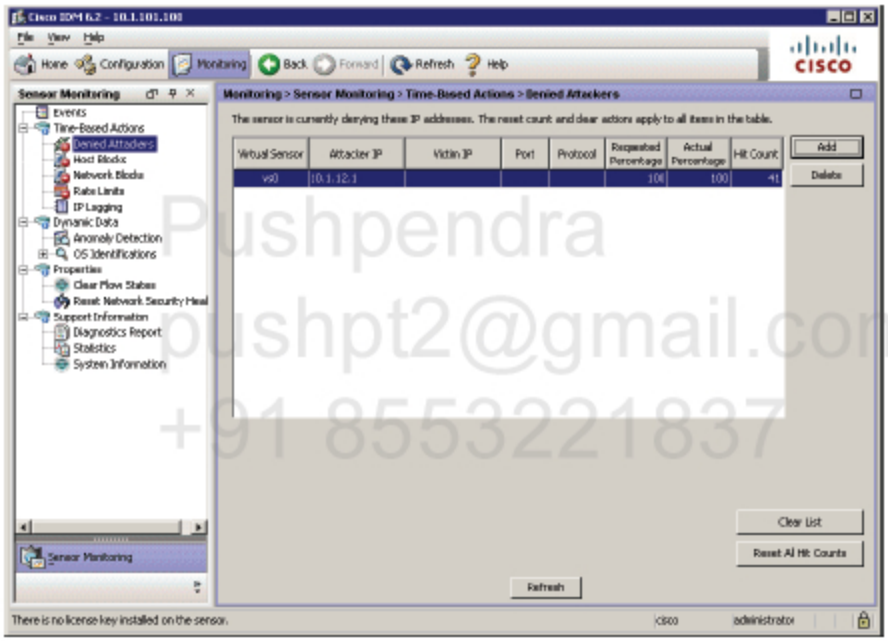

***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259892307105390537  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 13, 2010 22:26:17 UTC  offset=0  timeZone=UTC
  signature:  description=META Signature  id=60005  version=custom  type=other
created=20000101
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
```

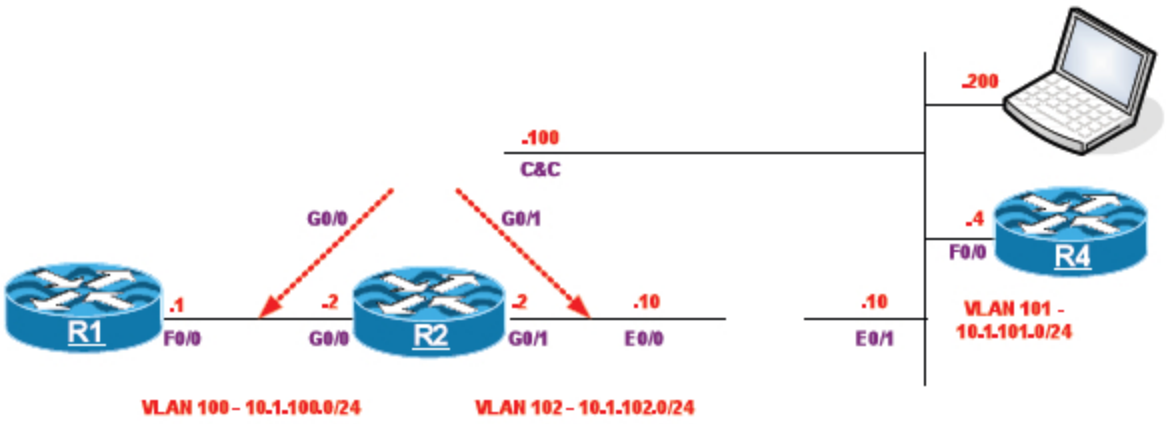
```
    addr: 10.1.12.1  locality=OUT
actions:
  deniedAttacker: true
alertDetails: Component Signature List: 60003.0 60004.0  ;
riskRatingValue: 56  targetValueRating=medium
threatRatingValue: 11
interface: ge0_0
protocol: tcp
```

Two component signatures triggered within 30 seconds so that the META signature has been triggered generating an alert and blocking the attacker.

***Go to Monitoring → Time-Based Actions → Denied Attackers to see if there is R1's F0/0 interface IP address on the list.***



# LAB 2.10. Blocking and rate limiting




## Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 100
- R2's G0/1 and ASA's E0/0 interface should be configured in VLAN 102
- R4's F0/0 and ASA's E0/1 interface should be configured in VLAN 101
- PC and IPS Command and Control (C&C) interface should be configured in VLAN 101
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices (except PC and IPS)



## IP Addressing

| Hostname | Interface (ifname) | IP address |
|---|---|---|
| R1 | F0/0 | 10.1.100.1/24 |
| R2 | G0/1<br>G0/0 | 10.1.100.2/24<br>10.1.102.2/24 |
| R4 | F0/0 | 10.1.101.4/24 |
| ASA-FW | E0/0 (Outside, Security 0)<br>E0/1 (Inside, Security 100) | 10.1.102.10/24<br>10.1.101.10/24 |

## Task 1

Use the following initial settings for IPS sensor configuration:

- Hostname: IPS-CCIE
- IP address: 10.1.101.100/24
- Default Gateway: 10.1.101.10
- Allowed Hosts: 10.1.101.200
- IPS management interface (m0/0) in VLAN 101.

Configure sensor to monitor traffic in VLAN 100 using promiscuous mode and its G0/0 interface. Tune up the ICMP Echo Request signature so that it triggers for packets destined to R4's F0/0 interface IP address. Configure connection blocking for that signature using R2's G0/0 interface (use TELNET connection) and ensure that IPS management station (PC) IP address is not getting accidently blocked.

*Cisco IPS has a blocking feature that prevents packets from reaching their destination. Blocking is initiated by a sensor and performed by another Cisco device at the request of the sensor. A blocking application on the sensor is called Attack Response Controller (ARC). The ARC starts and stops blocks. It monitors the time for the block and removes the block after the time has expired. ARC is also used in rate limiting.*



## Configuration

Complete these steps:

**Step 1** SW1 configuration.

```
SW1(config)#vlan 666
SW1(config-vlan)#remote-span
SW1(config-vlan)#exi

SW1(config)#monitor session 1 source vlan 100 rx
SW1(config)#monitor session 1 destination remote vlan 666
```

**Step 2** SW4 configuration.

```
SW4(config)#vlan 666
SW4(config-vlan)#remote-span
SW4(config-vlan)#exi

SW4(config)#monitor session 1 source remote vlan 666
SW4(config)#monitor session 1 destination interface f0/15
```

## Step 3 IPS CLI configuration.

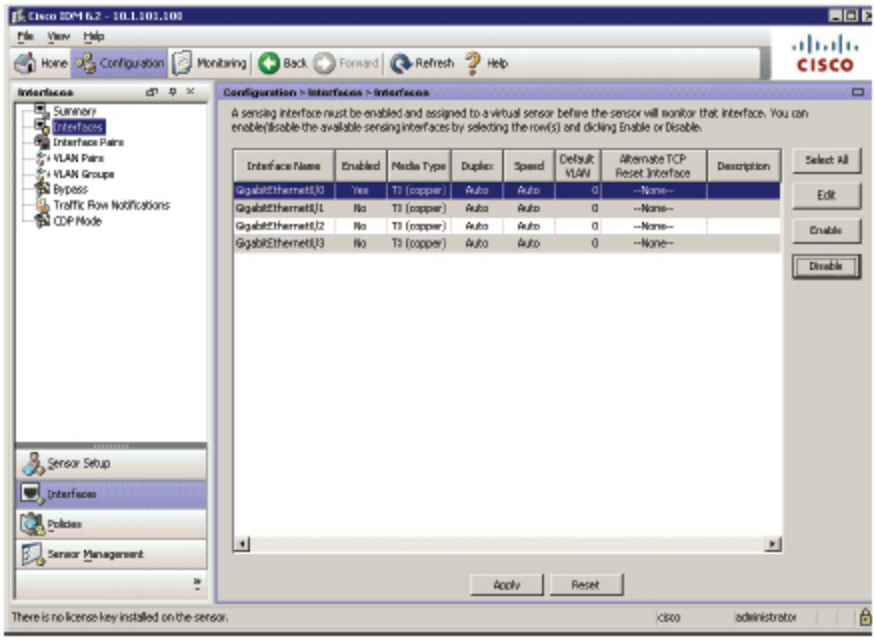
```
sensor login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.

    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Sun Feb  7 20:00:22 2010

Setup Configuration last modified: Sun Feb 07 20:00:00 2010

Enter host name[sensor]: IPS-CCIE
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.101.100/24,10.1.101.10
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.101.200/32
Permit:
Modify system clock settings?[no]:

The following configuration was entered.

service host
network-settings
```

```
host-ip 10.1.101.100/24,10.1.101.10
host-name IPS-CCIE
telnet-option disabled
access-list 10.1.101.200/32
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.

Enter your selection[3]: 2
--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.

sensor# exi


IPS-CCIE login:
```

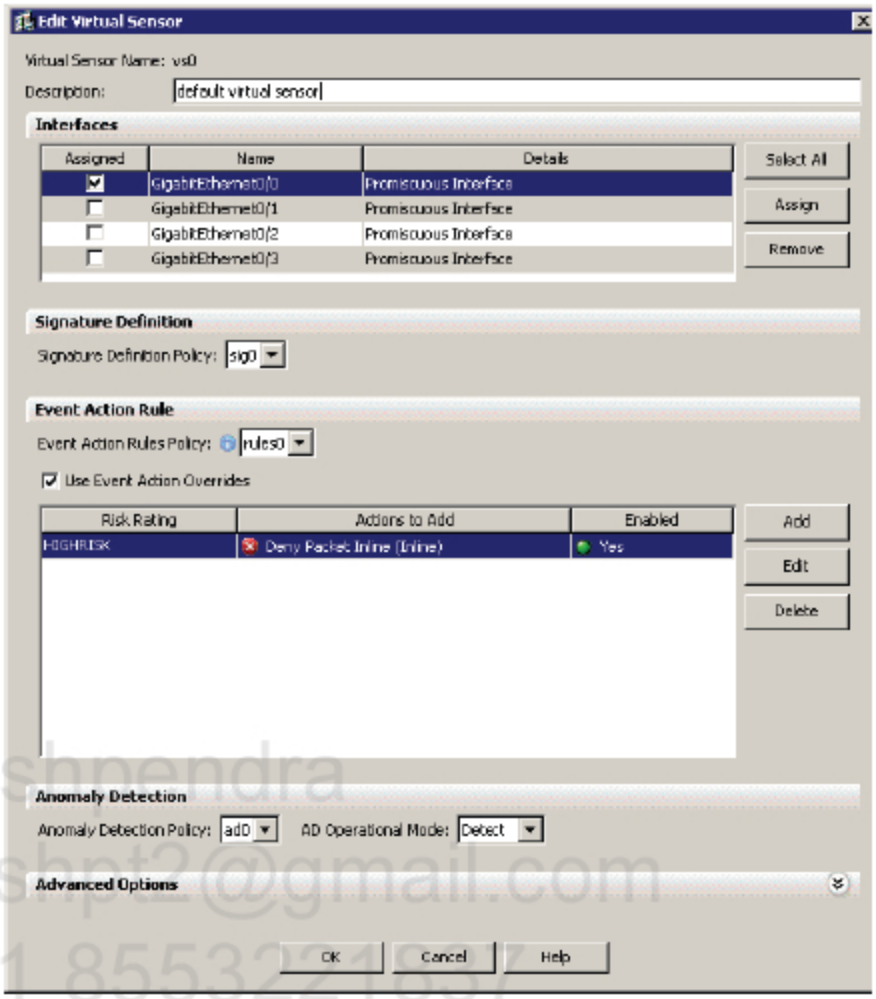


**Step 4** IPS GUI configuration.

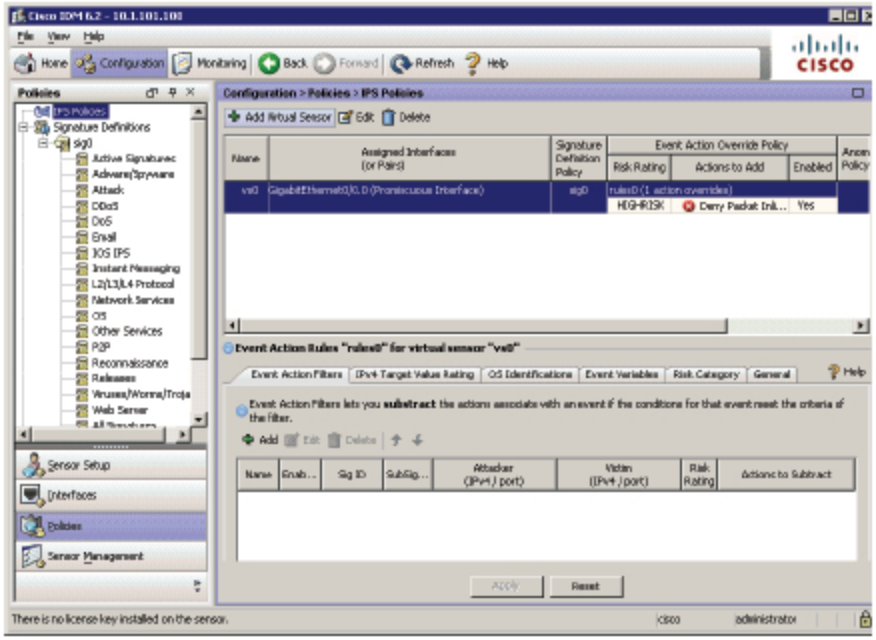
1. *Go to Configuration → Interfaces → Interfaces, select GigabitEthernet0/0 interface and click Enable button.*



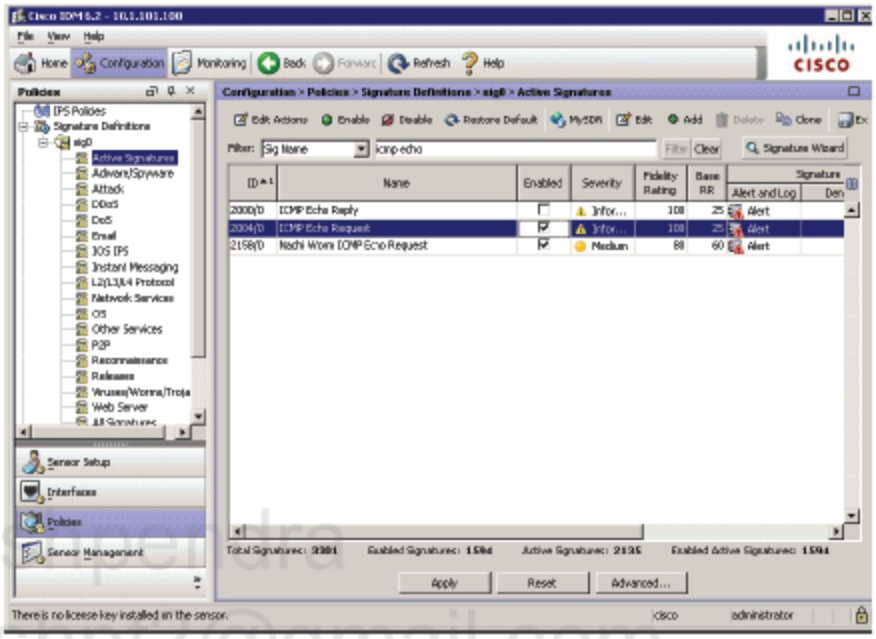

2. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit. Highlight GigabitEthernet0/0 interface on the list and click Assign button. Then click OK and Apply the changes to the sensor.***





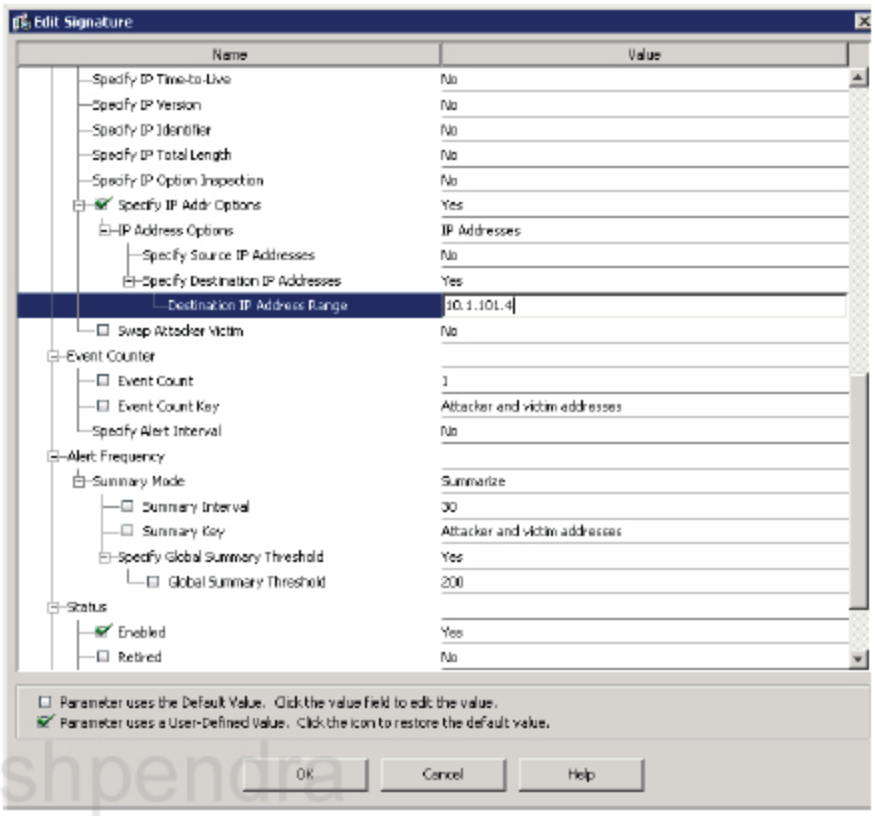



3. *Go to Configuration → Policies → sig0 → Active Signatures. From Filter drop-down list select Sig Name and enter "icmp echo" string. Then click on Filter button. Highlight the signature ID 2004/0 and click on Enable. Then Apply the changes to the sensor.*



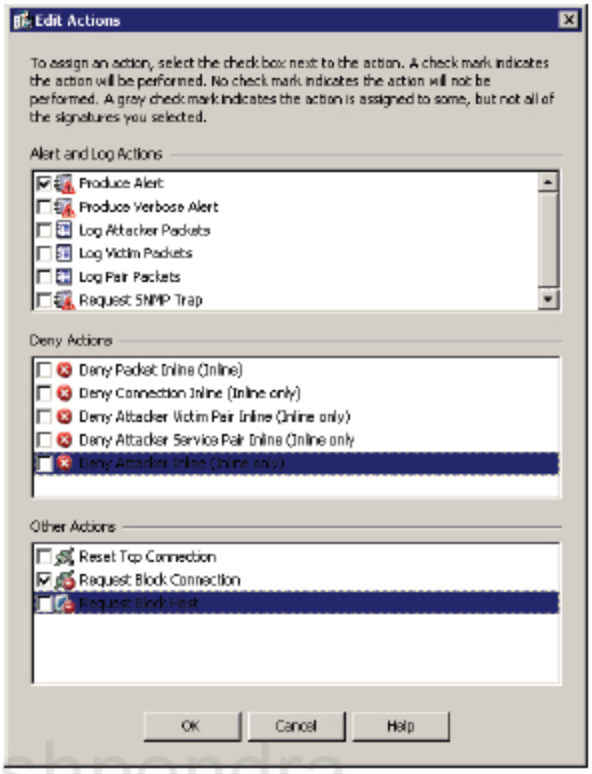



4. *Click on Edit button to see detailed signature settings. Enter 10.1.101.4 as Destination IP Address Range. Click OK.*



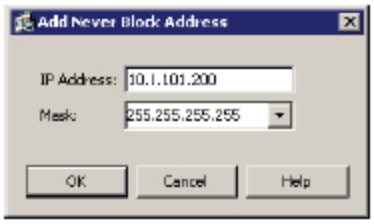



5. ***Click on Edit Actions and check Produce Alert and Request Block Connection items. Click OK.***

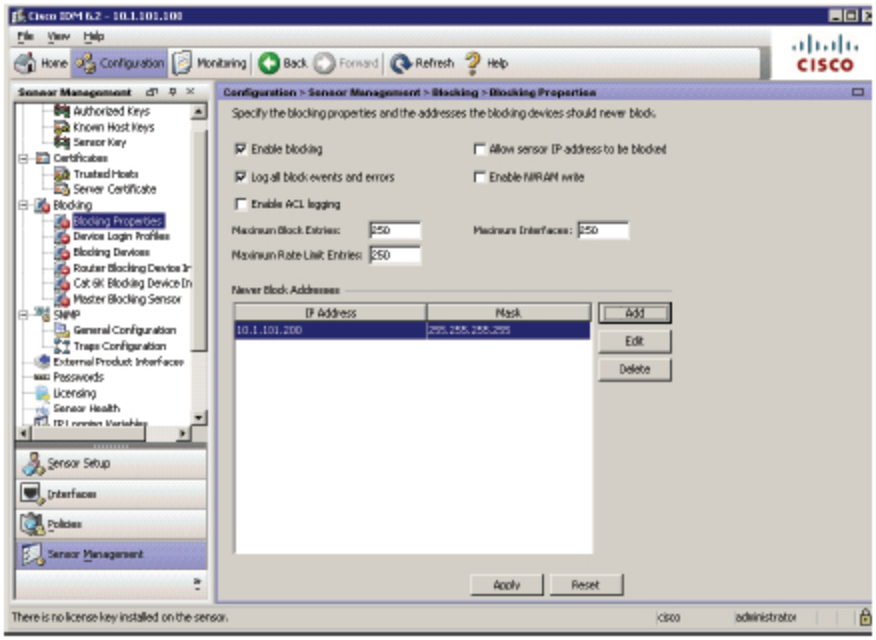





6. ***Go to Configuration → Sensor Management → Blocking → Blocking Properities and click Add button. Enter the IPS management station (PC) IP address and 32 bit mask in the following window. Click OK.***

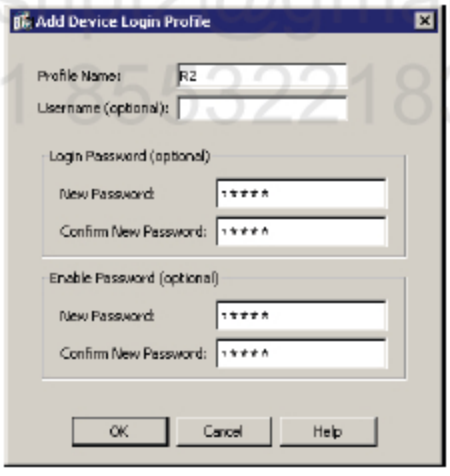


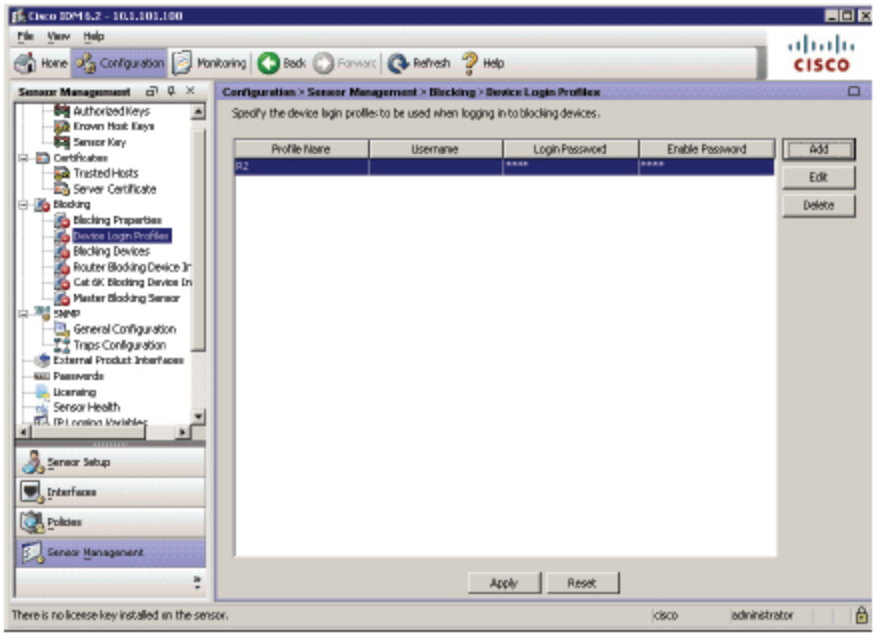

7. ***Make sure that Enable Blocking checkbox is selected.***




8. ***Go to Configuration → Sensor Management → Device Login Profiles and click Add. This login profile will be for R2 router so enter Profile Name (can be arbitrary name) and Login/Enable passwords. Click OK.***

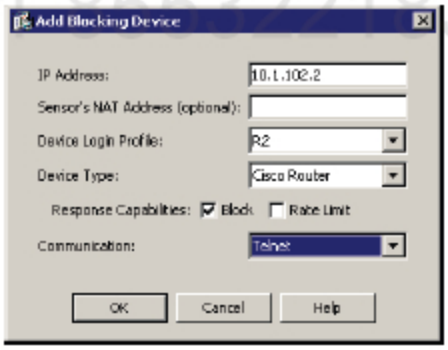


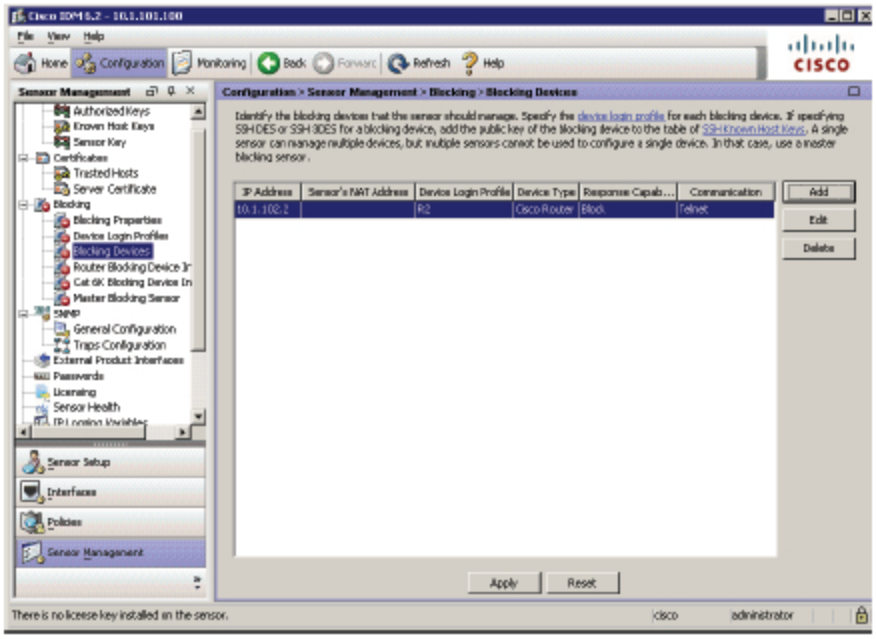





9. ***Go to Configuration → Sensor Management → Blocking Devices and click Add. Configure R2's IP address, select previously configured Device Login Profile and set Device Type to Cisco Router. For Response Capabilities check Block option. Communication must be set to Telnet. Click OK when finished.***

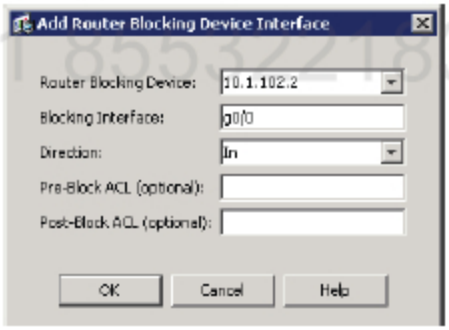







***10. Go to Configuration → Sensor Management → Router Blocking Device Interfaces and click Add. Select R2's IP address form drop-down list and configure g0/0 interface to apply the ACL in the Inbound direction. Click OK when finished.***





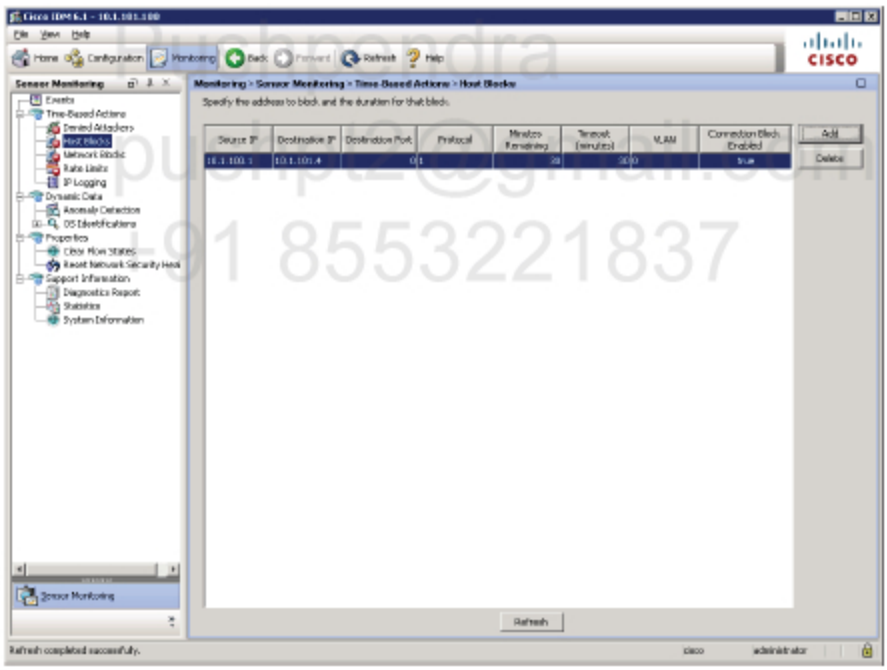

## Verification

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

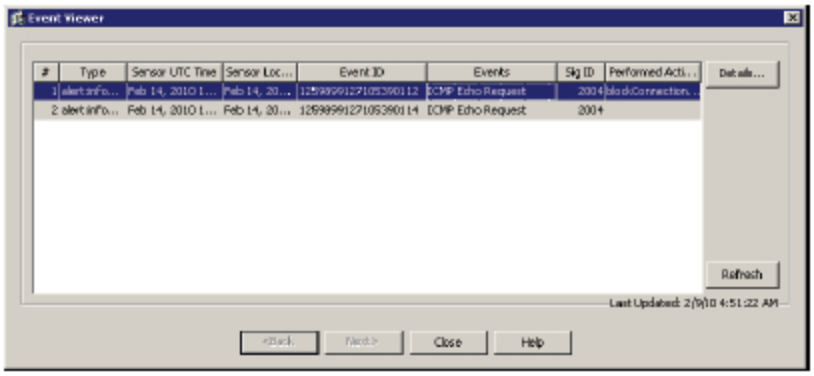
```
R1#pi 10.1.101.4 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.101.4, timeout is 2 seconds:
```

```
!!!!!!.U.U.U.U.U.U.U.U.U.U

<...output omitted...>


R2#
%SYS-5-CONFIG_I: Configured from console by vty0 (10.1.101.100)
R2#
%SYS-5-CONFIG_I: Configured from console by vty0 (10.1.101.100)

R2#sh access-lists
Extended IP access list IDS_g0/0_in_1
    10 permit ip host 10.1.101.100 any       ← This is Never Block Address
    20 deny icmp host 10.1.100.1 host 10.1.101.4     ← This is Request Block Connection
    30 permit ip any any
```

***Go to Monitoring → Time-Based Actions → Host Blocks and check if there is R1's IP address on the list.***




***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the fired signature 2004 on the event list.***




***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105390112  vendor=Cisco  severity=informational
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 14, 2010 12:45:17 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    blockConnectionRequested: true
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 15
  interface: ge0_0
  protocol: icmp


evIdsAlert: eventId=1259899127105390114  vendor=Cisco  severity=informational
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 14, 2010 12:45:47 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
```

```
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 10.1.100.1  locality=OUT
  target:
    addr: 10.1.101.4  locality=OUT
    os:   idSource=unknown  type=unknown  relevance=relevant
summary: 10  final=true  initialAlert=1259899127105390112  summaryType=Regular
alertDetails: Regular Summary: 10 events this interval ;
riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
threatRatingValue: 35
interface: ge0_0
protocol: icmp
```

## Task 2

Configure sensor to monitor traffic in VLAN 102 using promiscuous mode and its G0/1 interface. Create a custom signature so that it blocks host telnetting on port TCP 3005 (SYN packet). The signature must connect to the ASA using SSH and shun the attacker.

Set enable password to “cisco123” on the ASA and configure a new user named “sensor” with password of “sensor123” and use it for shunning.



*The sensor must be able to communicate with the blocking device. The sensor must have a route to (only default route is possible), or must be on the same subnet as, the managed firewall.*
*The blocking device must also have one of the following configured:*
*TELNET: Telnet access should be allowed from the sensor.*
*SSH: SSH access should be allowed from the sensor.*
*SSH is the default communication mechanism between the sensor and the blocking device. If SSH is used, the blocking device must have a software license that supports DES or 3DES encryption.*
*As soon as the blocking device is configured on the sensor, the sensor attempts to log into the blocking device using the specified credentials and access protocol, Telnet or SSH. If the sensor logs in successfully, a user connection is maintained between the sensor and the blocking device. This persistent connection allows the sensor to immediately and dynamically configure blocking rules on the blocking device as required.*
*If local authentication, not AAA, is used for SSH on the ASA, the SSH username is always “pix” and the password is the same as enable password on the device.*
*The ASA uses “shun” to enable blocking. The “shun” command is limited to blocking hosts; it does not support blocking of specific host connections or manual blocking of entire networks or subnetworks.*

## Configuration

Complete these steps:

**Step 1** SW4 configuration.

```
SW4(config)#vlan 888
SW4(config-vlan)#name RSPAN
SW4(config-vlan)#remote-span
SW4(config-vlan)#exi

SW4(config)#monitor session 2 source remote vlan 888
SW4(config)#monitor session 2 destination interface f0/16
```

**Step 2** SW2 and SW3 configuration.

```
SW2(config)#vlan 888
SW2(config-vlan)#name RSPAN
SW2(config-vlan)#remote-span
SW2(config-vlan)#exi

SW2(config)#monitor session 2 source vlan 102
SW2(config)#monitor session 2 destination remote vlan 888
```

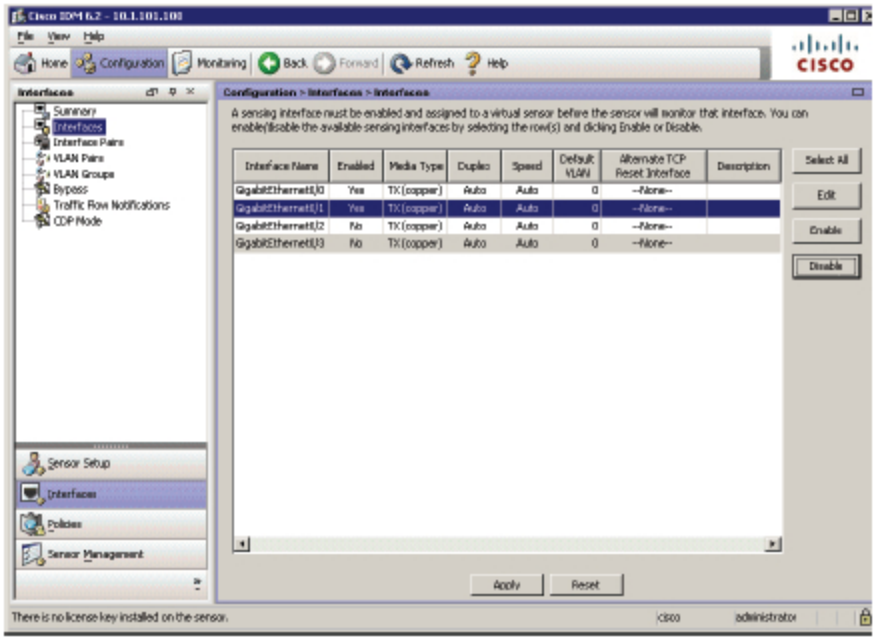
**Step 3** SSH configuration on ASA.

```
ASA-FW(config)# ssh 10.1.101.100 255.255.255.255 Inside
ASA-FW(config)# enable password cisco123
ASA-FW(config)# username sensor password sensor123
ASA-FW(config)# aaa authentication ssh console LOCAL
```

We need to use a specific username and password to enable blocking on the ASA. Hence, we need to configure local AAA.

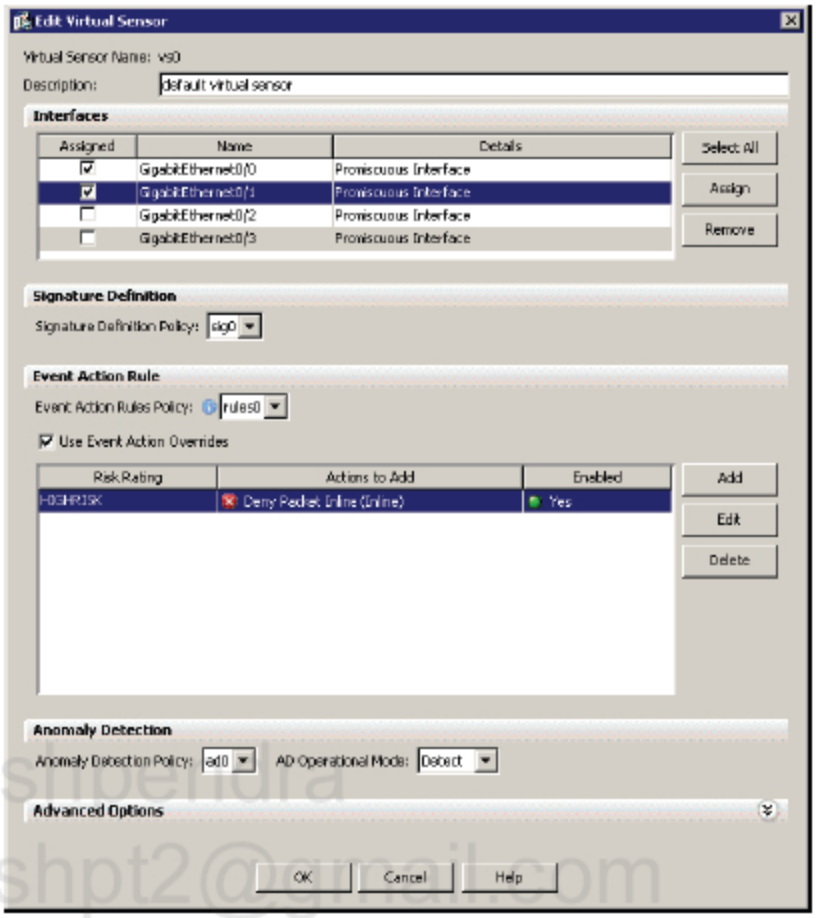
**Step 4** IPS configuration.

1. *Go to Configuration → Interfaces → Interfaces, select GigabitEthernet0/1 interface and click Enable button.*



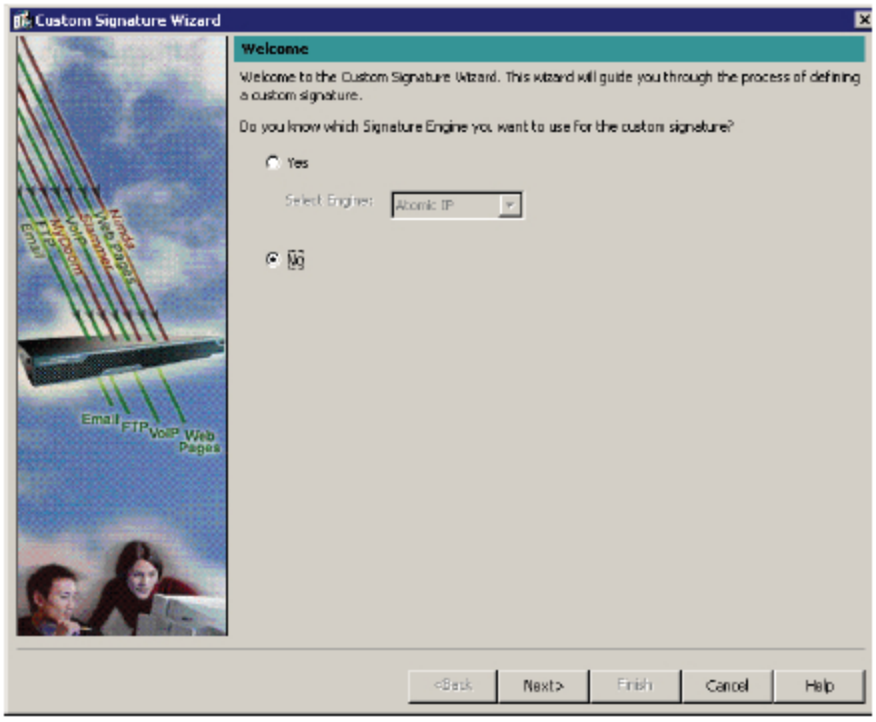



2. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit. Highlight GigabitEthernet0/1 interface on the list and click Assign button. Then click OK and Apply the changes to the sensor.***



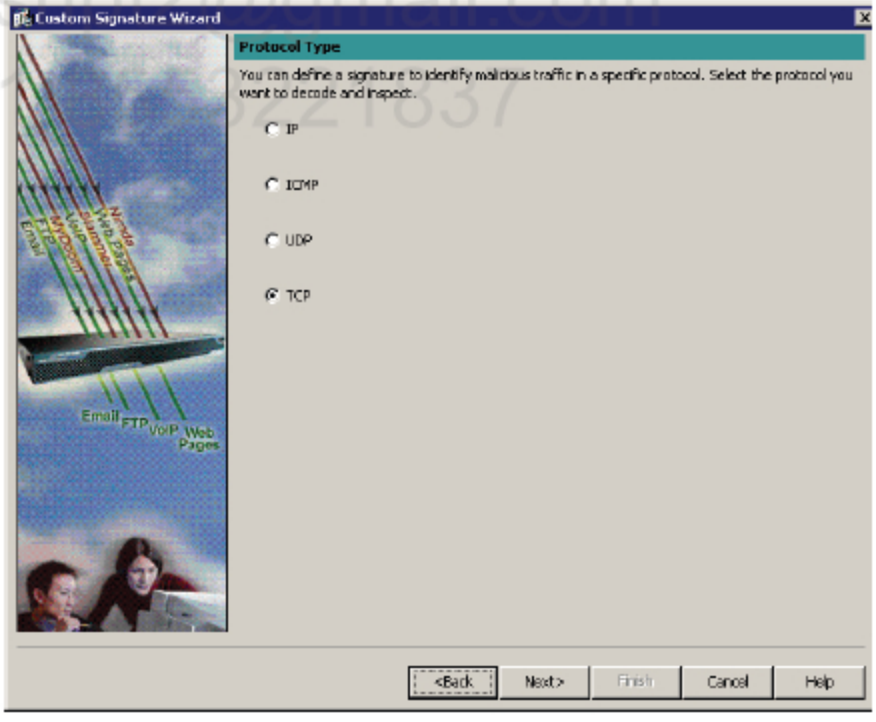



3. ***Go to Configuration → Policies → sig0 → Active Signatures and click on Signature Wizard. Select No option on the first page and click Next.***

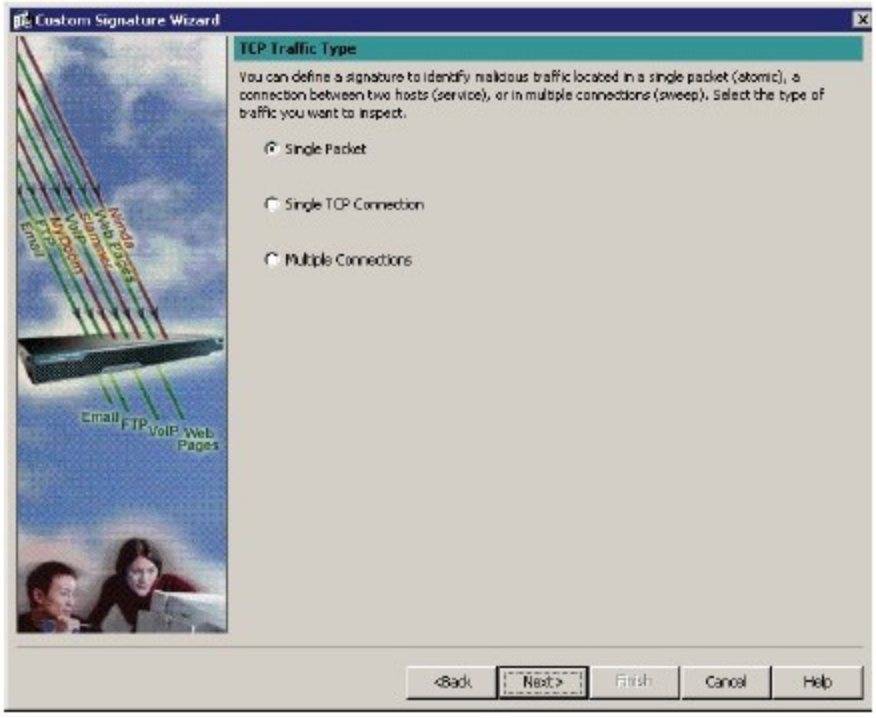





4. ***Check TCP as protocol type and click Next.***

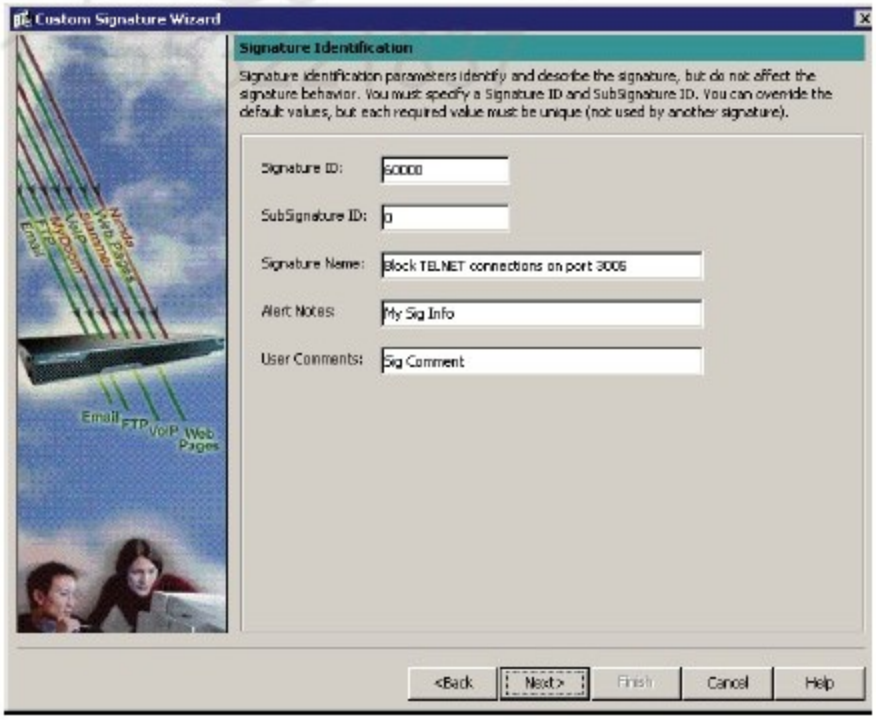



5. ***Select Siingle Packet option to use Atomic IP engine and click on Next.***



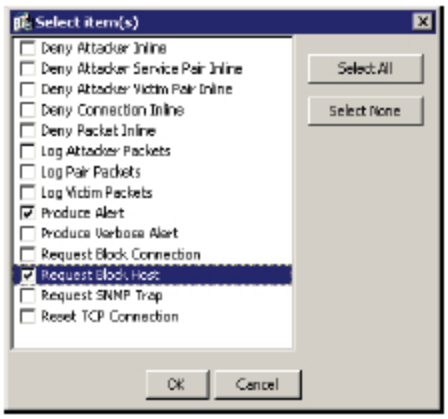



6. ***Enter the name for new signature, make some Notes and Comments and click on Next.***



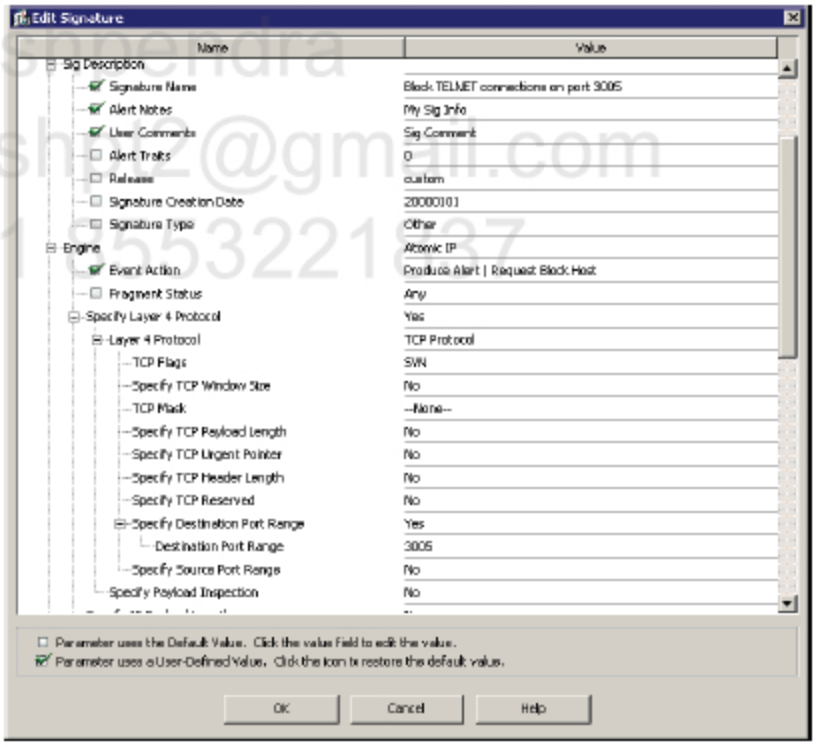

7. ***On the Engine Specific Parameters screen, click on Event Action and select Produce Alert and Request Block Host from the list. Then click***

***OK.***

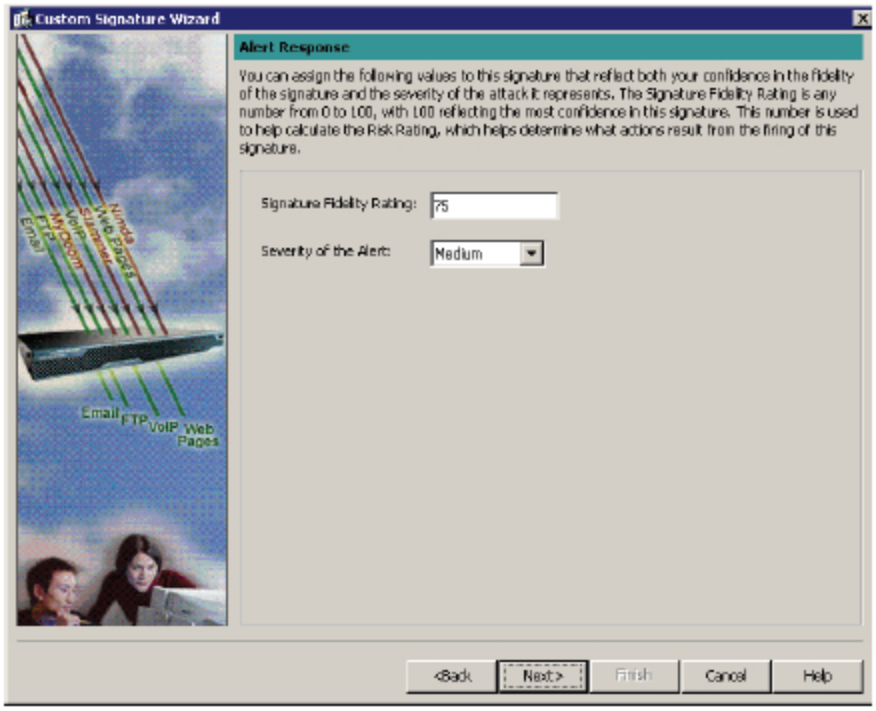



**Remember that ASA does not support connection blocking. Thus, the only option here is to enable "Request Block Host".**

8. ***Set Specify Layer 4 Protocol/Layer 4 Protocol to TCP Protocol and TCP Flags to SYN. Destination Port Range should be set to 3005.***

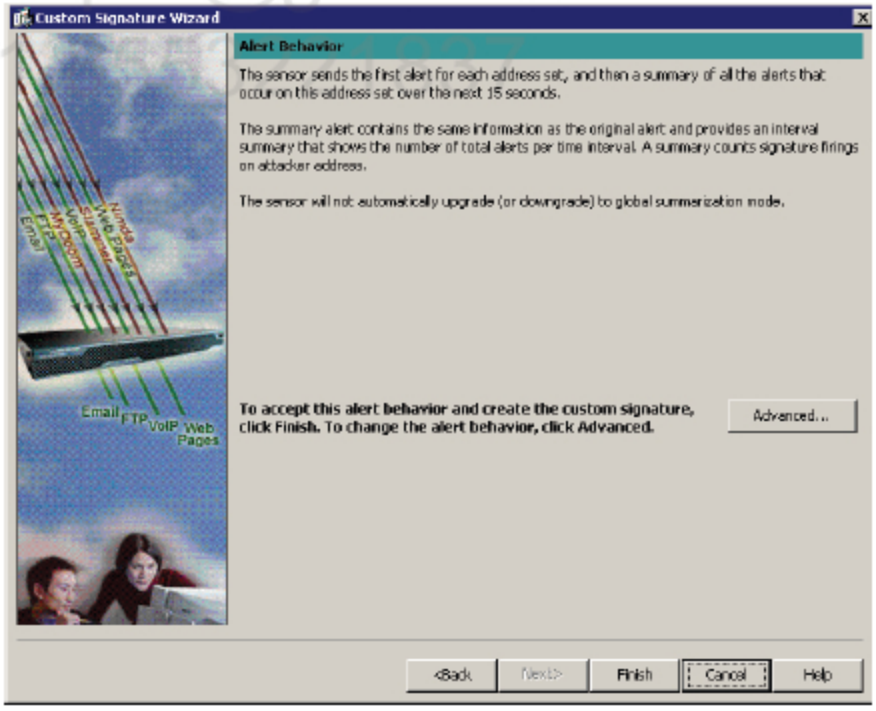


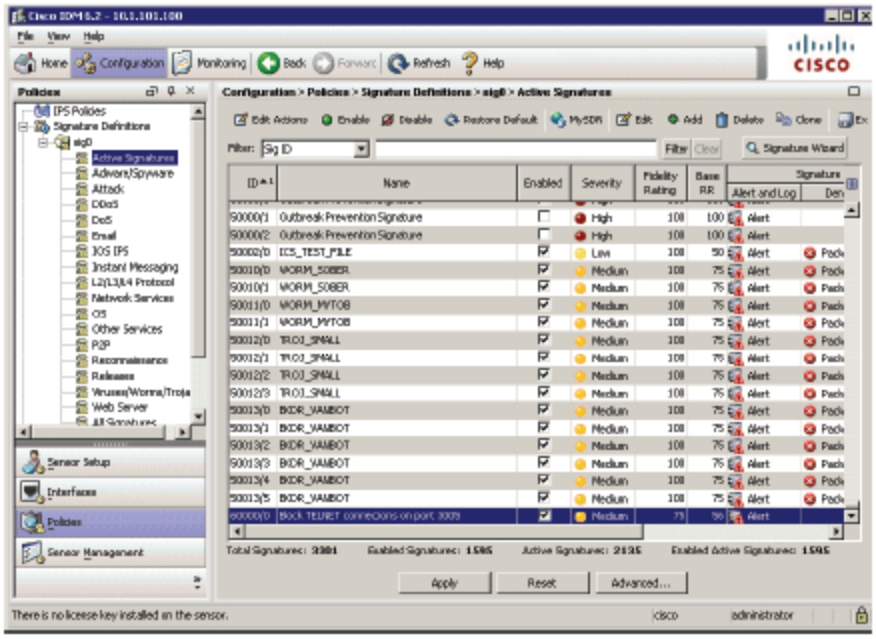

9. ***Set Signature Fidelity Rating to 75 and Action Severity to Medium. Click Next.***





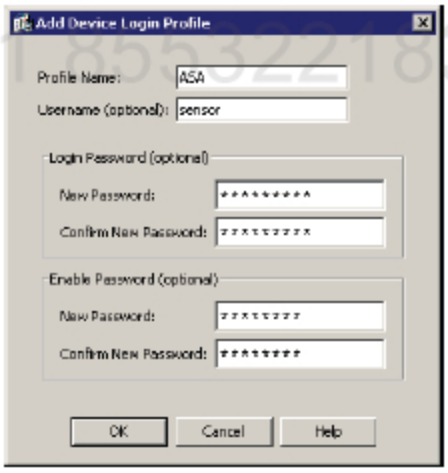

10. ***Leave default settings for Alert Behavior and click Finish to close the wizard.***

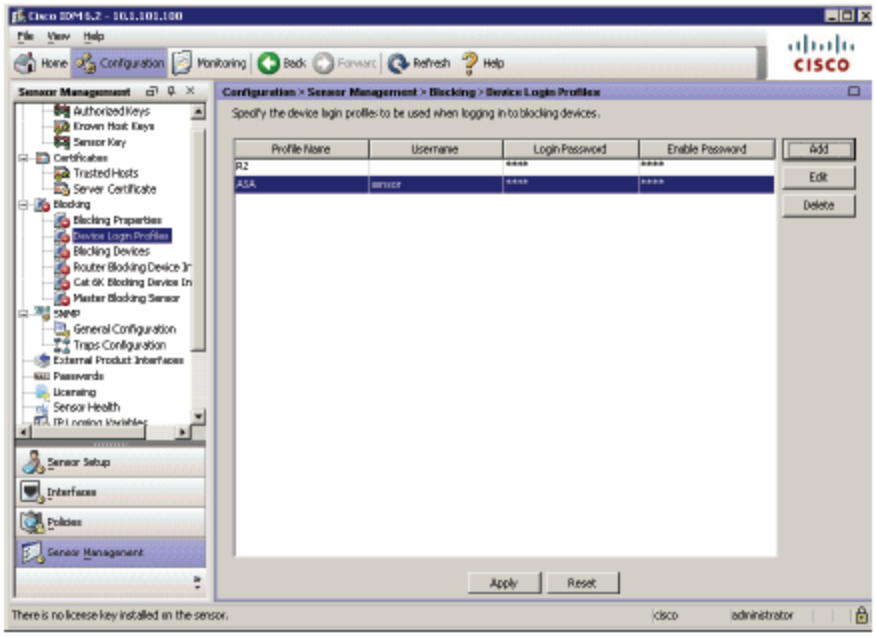




11. **Go to Configuration → Sensor Management → Device Login Profiles and click Add. This login profile will be for ASA so enter Profile Name (can be arbitrary name) and Username of "sensor" and its associate Login/Enable passwords. Click OK.**

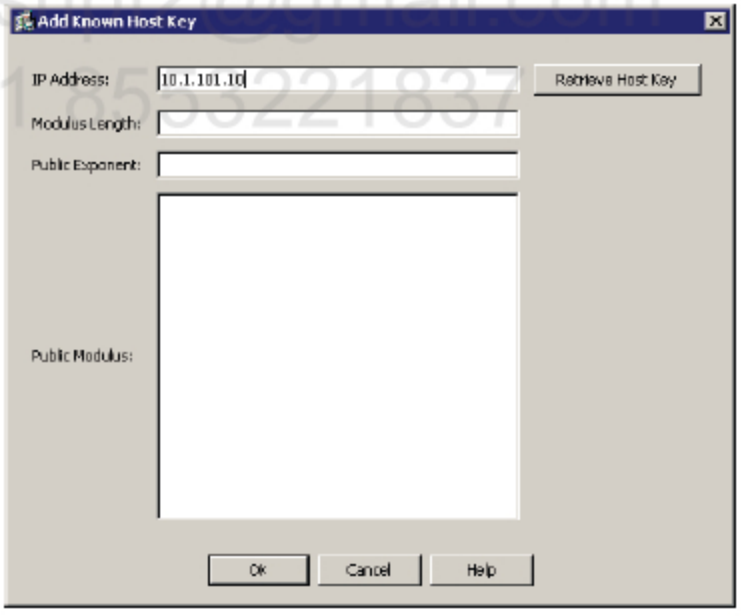






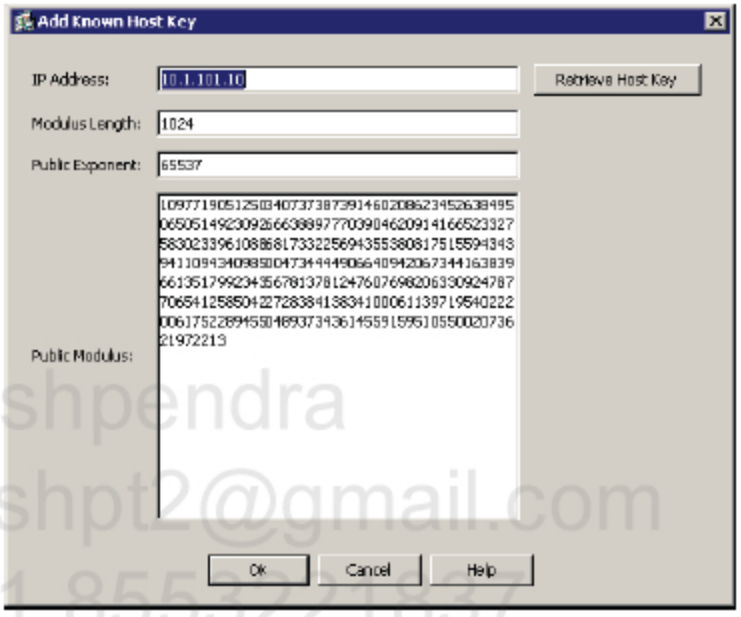

12. ***Go to Configuration --> Sensor management --> SSH --> Known Host Keys and click Add. Enter IP address of ASA device and click Retrieve Host Key button.***

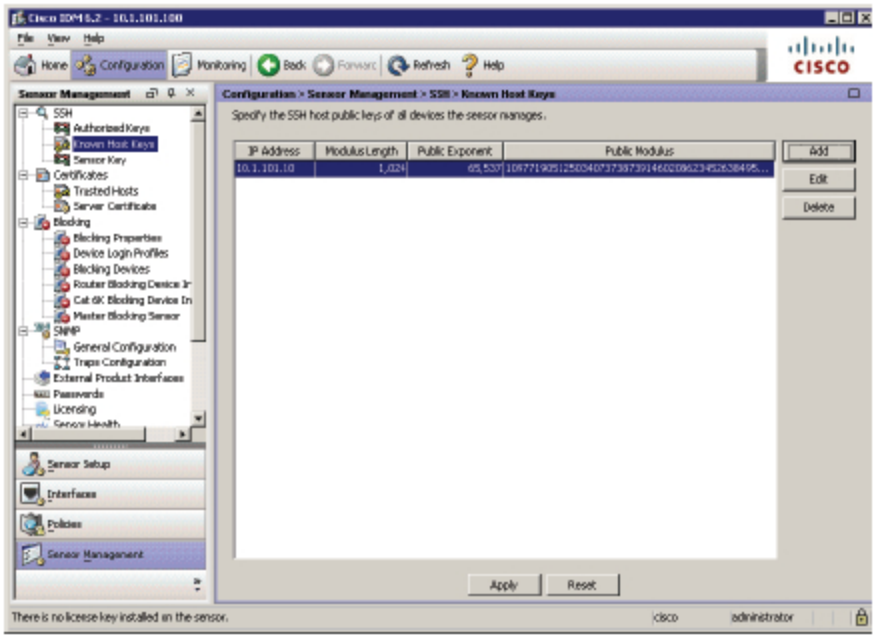




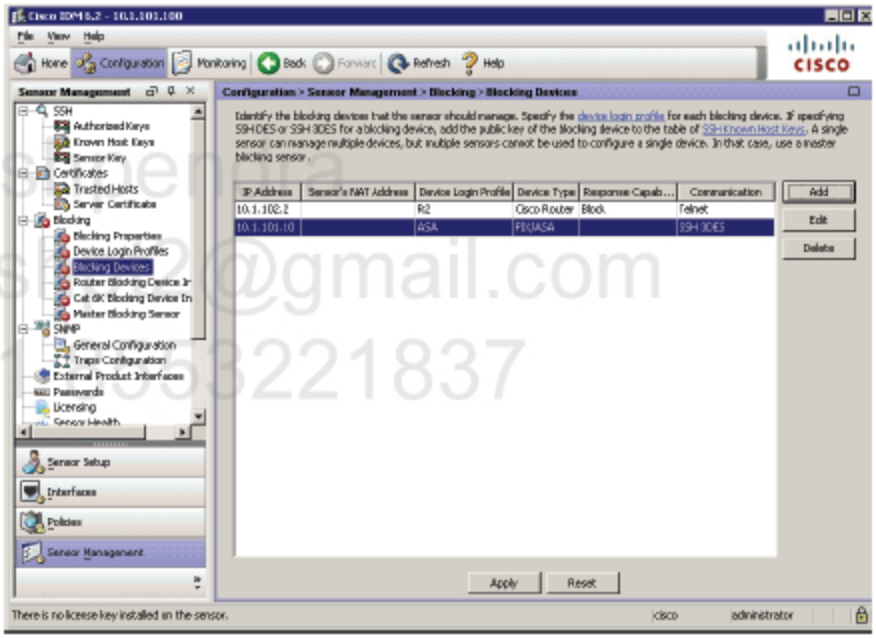

13. ***IPS sensor will try to contact the ASA to get its Public SSH key and store it. After successful key retrieval, the following message appear:***


***14. The key is shown on the window. Click OK to accept it.***



15. ***Go to Configuration → Sensor Management → Blocking Devices and click Add. Configure ASA's IP address, select previously configured Device Login Profile and set Device Type to PIX/ASA. Communication must be set to SSH 3DES. Click OK when finished.***



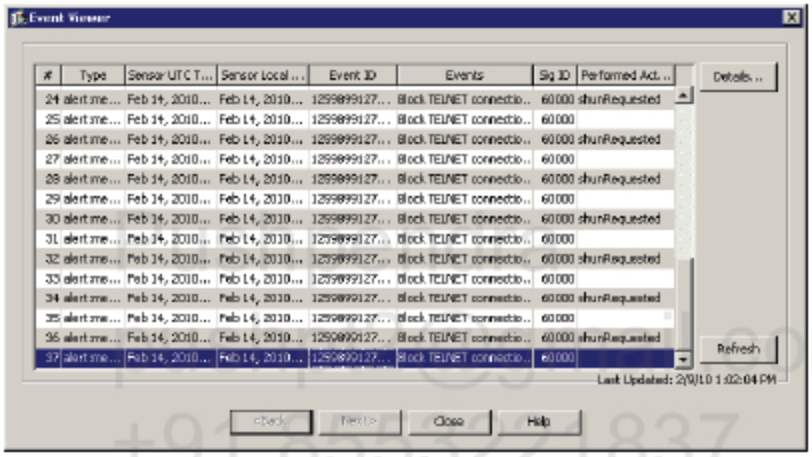

## Verification

```
R2#tel 10.1.101.4 3005
Trying 10.1.101.4, 3005 ... Open


User Access Verification

Password:
```

```
<...session hangs...>

ASA does NOT support Connection Blocking!!! Thus, we see "host" block only.

ASA-FW(config)# sh shun
shun (Outside) 10.1.102.2 0.0.0.0 0 0 0
ASA-FW(config)#
```

***Go to Monitoring → Sensor monitoring → Time-Based Actions → Host Blocks and see if there's R2's IP address.***

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the custom signature fired.***




***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105390843  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 14, 2010 21:02:56 UTC  offset=0  timeZone=UTC
  signature:  description=Block TELNET connections on port 3005  id=60000
version=custom  type=other  created=20000101
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.102.2  locality=OUT
      port: 57266
    target:
      addr: 10.1.101.4  locality=OUT
```

```
      port: 3005
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    shunRequested: true
  riskRatingValue: 66  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 46
  interface: ge0_1
  protocol: tcp
```

Note that "shunRequested: true" does not indicate that the blocking is successful. It only says that the IPS triggered ARC process to block the traffic. If for some reason the IPS cannot contact the blocking device, there is another event saying that.

```
evIdsAlert: eventId=1259899127105390845  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 14, 2010 21:03:11 UTC  offset=0  timeZone=UTC
  signature:  description=Block TELNET connections on port 3005  id=60000
version=custom  type=other  created=20000101
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.102.2  locality=OUT
      port: 0
    target:
      addr: 0.0.0.0  locality=OUT
      port: 0
      os:   idSource=unknown  type=unknown  relevance=unknown
  summary: 12  final=true  initialAlert=1259899127105390843  summaryType=Regular
  alertDetails: Regular Summary: 12 events this interval ;
  riskRatingValue: 56  targetValueRating=medium
  threatRatingValue: 56
  interface: ge0_1
  protocol: tcp
```

## Task 3

Configure signature "ICMP Flood" so that it triggers when level of 50 packets-per-second is reached. R2 should be used to rate limit the connection speed to 10% of its G0/0 interface speed.

*The IPS can also re-configure remote devices to limit the packets going through them. This can be done only on routers and is using MQC (Modular Quality of Service Command Line Interface) to configure that. Simply speaking when the Request Rate Limit action is triggered for the signature, the IPS sends out a couple of commands to the router with traffic policing configuration. There is no option that using traffic shaping non-conformed traffic will be dropped.*

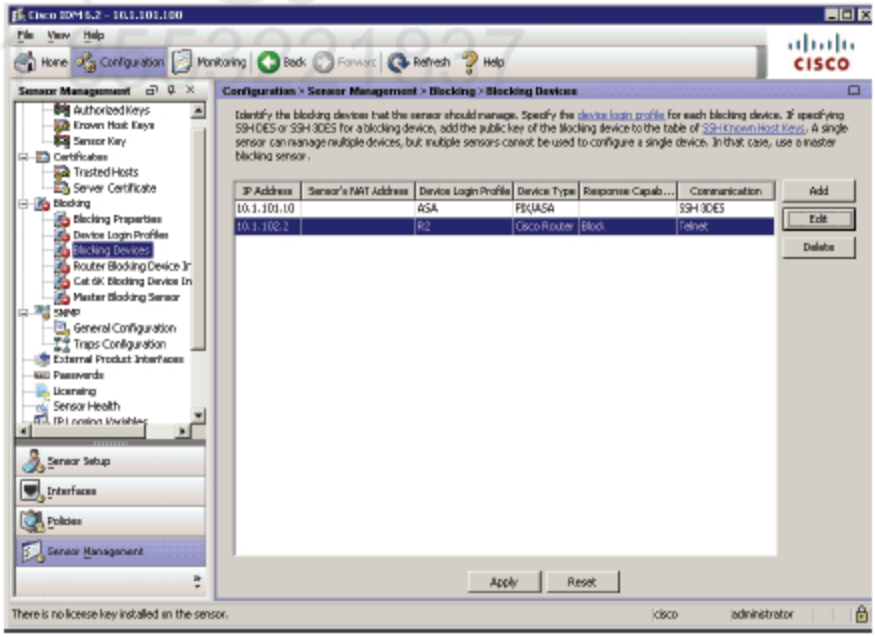
## Configuration

Complete these steps:

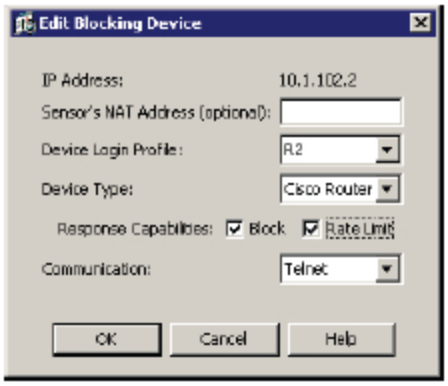
**Step 1** IPS configuration.



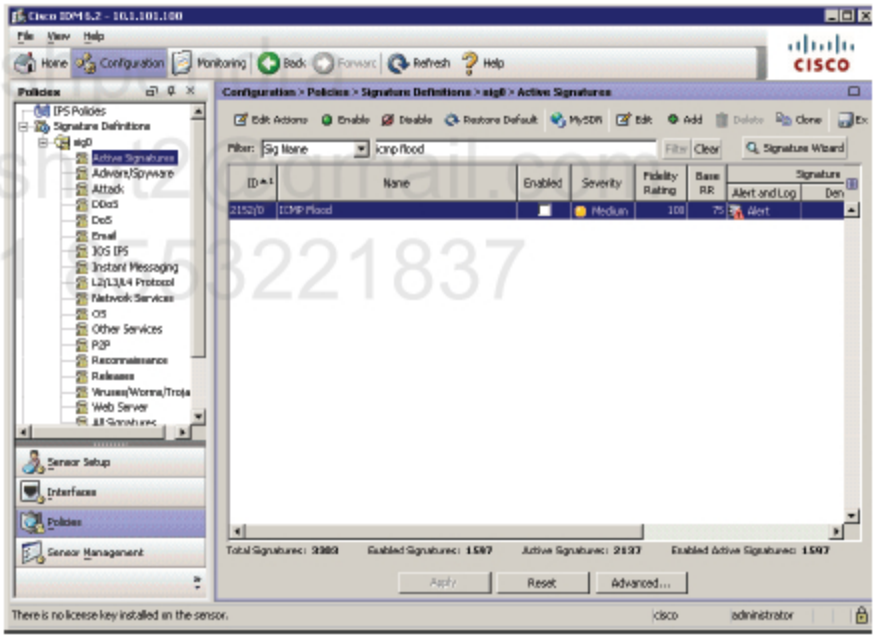
1. ***Go to Configuration → Sensor Management → Blocking Devices, highlight entry for R2 device and click Edit.***



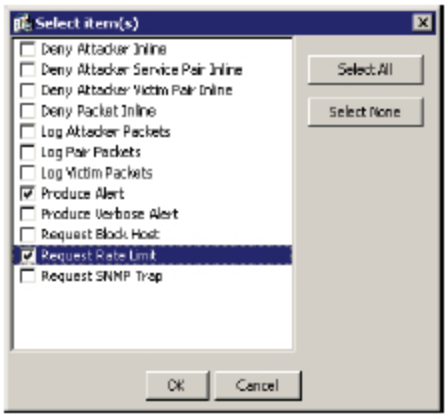

2. ***Select Rate Limit checkbox.***



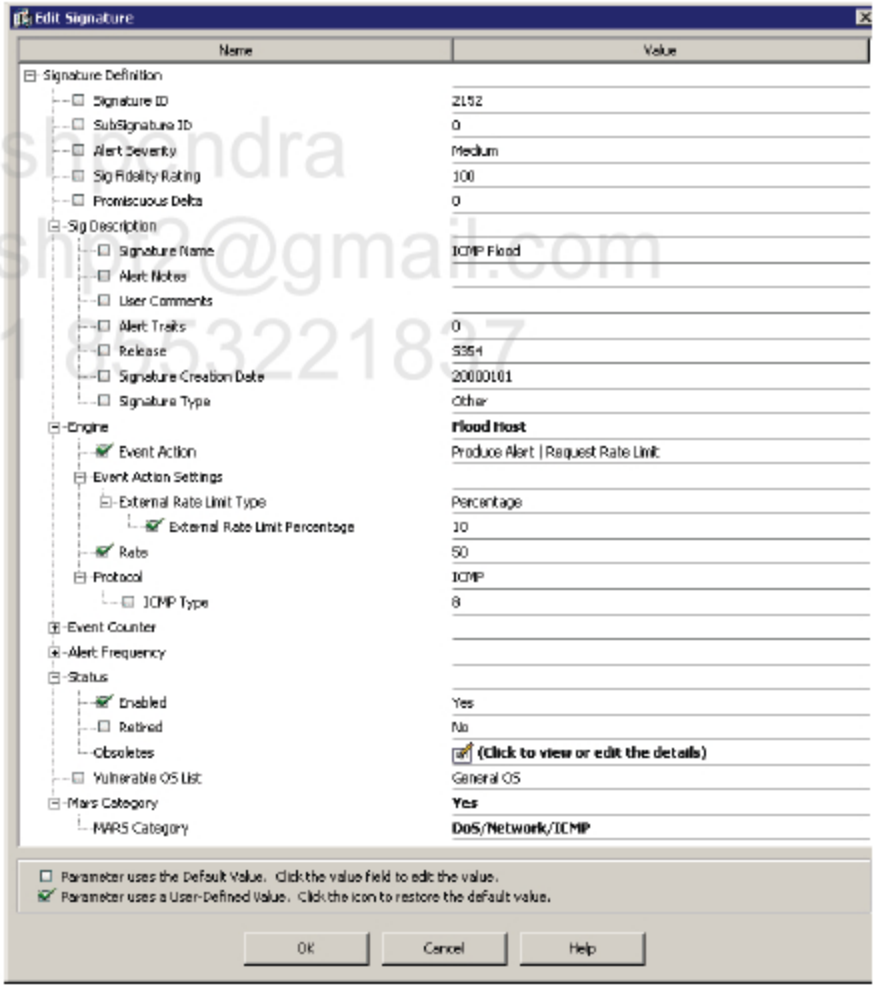

3. ***Go to Configuration → Policies → sig0 → Active Signatures. From Filter drop-down list select Sig Name and enter "icmp flood" string. Then click on Filter button. Highlight the signature ID 2152/0 and click on Enable.***




4. ***Then click on Edit Actions and check Produce Alert and Request Rate Limit actions from the list. Click OK.***




5. ***Click on Edit button and set Engine/Event Action settings/External Rate Limit Type/External Rate Limit Percentage to 10. The Rate item should be set to 50. Click OK and Apply the changes.***



## Verification

```
R1#ping 10.1.102.10 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.102.10, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms
R1#
```

The ping is successful, see if this traffic was matched by the policer.

```
R2#sh policy-map interface g0/0
 GigabitEthernet0/0

  Service-policy input: IDS_RL_POLICY_MAP_1

    Class-map: IDS_RL_CLASS_MAP_icmp-xxBx-8-10_1 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name IDS_RL_ACL_icmp-xxBx-8-10_1
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
          cir 10 %
          cir 100000000 bps, bc 3125000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

No it wasn't! Why? This is because the router was reconfigured by the IPS when the signature was triggered. Thus, it took some time to enable rate limiting on the router.
Try to ping again and see now everything is OK.

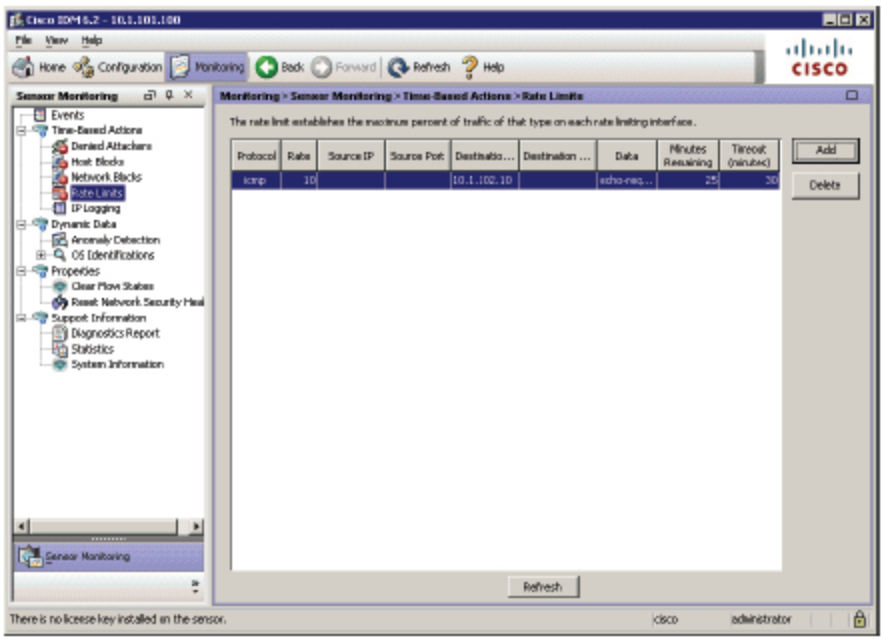
```
R1#ping 10.1.102.10 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.102.10, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
R1#
```

```
R2#sh policy-map interface g0/0
 GigabitEthernet0/0

  Service-policy input: IDS_RL_POLICY_MAP_1

    Class-map: IDS_RL_CLASS_MAP_icmp-xxBx-8-10_1 (match-any)
      100 packets, 11400 bytes
      5 minute offered rate 2000 bps, drop rate 0 bps
      Match: access-group name IDS_RL_ACL_icmp-xxBx-8-10_1
        100 packets, 11400 bytes
        5 minute rate 2000 bps
      police:
          cir 10 %
          cir 100000000 bps, bc 3125000 bytes
        conformed 100 packets, 11400 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 2000 bps, exceed 0 bps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

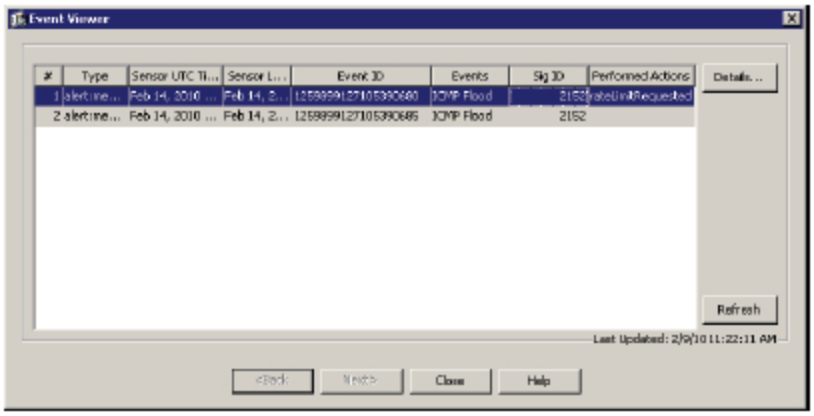


**Now all packets have been matched and conformed to the policy configured.**

***Go to Monitoring → Time-Based Actions → Rate Limits and check if you see the Rate Limit for ICMP.***



***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the fired signature 2152 on the event list.***



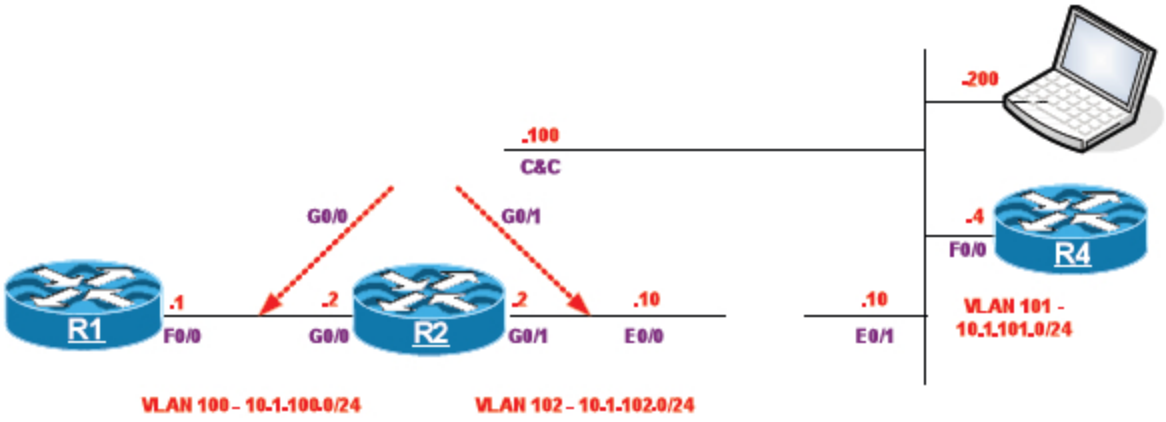

***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105390680  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 14, 2010 19:20:19 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Flood  id=2152  version=S354  type=other
created=20000101
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.102.10  locality=OUT
      os:  idSource=unknown  type=unknown  relevance=relevant
  actions:
    rateLimitRequested: true
  riskRatingValue: 85  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 65
  interface: ge0_1
  protocol: icmp


evIdsAlert: eventId=1259899127105390685  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
```

```
  time: Feb 14, 2010 19:20:49 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Flood  id=2152  version=S354  type=other
created=20000101
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 0.0.0.0  locality=OUT
    target:
      addr: 10.1.102.10  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  summary: 27  final=true  initialAlert=1259899127105390680  summaryType=Regular
  alertDetails: Regular Summary: 27 events this interval ;
  riskRatingValue: 85  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 85
  interface: ge0_1
  protocol: icmp
```

# LAB 2.11. Rules

**This lab is based on the configuration from the previous lab**






## Task 1

R4 is an important asset for your company. Configure rules so that R4 will be treated as High TVR (Target Value Rating) and use risk rating mechanism to enable alerting with packets dump for every signature getting RR (Risk Rating) between 85 and 89.

You may NOT use an IP address in TVR configuration.

Remove blocking actions for the signature 2004 to test your solution.

*IPS Rules is the most common method of IPS tuning and is the best method to decrease false positives. There are a couple of rules to configure depends on what you want to achieve:*

- *Event Action Overrides – use them to change the actions associated with an event based on the calculated risk*
- *Event Action Filters – use them to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. You can also use the variables that you defined on the Event Variables panel to group addresses for your filters.*

*For example, by specifying the source of traffic that is triggering false positives, you can prevent the sensor from generating unnecessary alerts.*

*To make this process more flexible, there are some variables to be defined and used in the "filters" and "overrides". Those variables are:*

- *Event Variables - if you want to use the same value within multiple filters, use a variable. When you change the value of the variable, any filter using that variable is updated with the new value. Note that you must preface the variable with a dollar sign ($) to indicate that you are using a variable rather than a string.*

- *Target Value Rating (TVR) - you can assign a TVR to your network assets. The TVR is one of the factors used to calculate the risk rating value for each alert. Events with a higher risk rating trigger more severe signature event actions. These values are available:*
  - *Low*
  - *Medium*
  - *High*
  - *Mission Critical*
  - *No Value*

*Risk Rating System*

*In contrast to simplistic alert rating models that are commonly used in the industry, Cisco IPS delivers unique risk ratings that are assigned to alerts generated from the IPS sensors. The risk rating is an integer value in the range from 0 to 100. The higher the value, the greater the security risk of the trigger event for the associated alert. The risk rating is a calculated number that is based on several components and is used by event action overrides.*

*There are six values used to calculate the risk rating:*

*Attack Severity Rating (ASR) - this is nothing more than the severity level configured for the signature. The ASR is not a determination of the accuracy of the signature definition. It is only an indication of the seriousness of the attack. Each of severity has an associated numeric value which the risk rating formula uses for the ASR value:*

- *Informational (25)*
- *Low (50)*
- *Medium (75)*
- *High (100)*



*Target Value Rating (TVR) – this is a user-configurable value that identifies the importance of a network asset, through its IP address. The following are the current numeric values for the configured targets:*

- *Zero (50)*
- *Low (75)*
- *Medium (100)*
- *High (150)*
- *Mission Critical (200)*

*Signature Fidelity Rating (SFR) – this is configurable value on a per-signature basis. It is an indication of the confidence that the signature writer has in the signature accuracy; it is not an indication of the seriousness of the potential attack. Valid numbers are 0–100.*

*Attack Relevancy Rating (ARR) - this is a derived value. It is not configurable. It describes how relevant the attack is to the target system. For example, a Microsoft web server (IIS) buffer overflow attack is serious. But if it is launched against an Apache server, it is not relevant. The relevancy of any target operating system is determined at the time of the alert. ARR values are:*

- *Relevant (10)*
- *Unknown (0)*
- *Not Relevant (–10)*

*Promiscuous Delta (PD) - this value lowers the risk rating of certain alerts in promiscuous mode. It is configured on a per-signature basis with numbers of 0–30. The PD is relevant only when the sensor is in promiscuous mode. When the sensor is inline, the PD is subtracted from the risk rating.*

*Watch List Rating (WLR) – this is a value of 0-100 derived from Cisco Security Agent (CSA) Management Center. If the attacker for the alert is found on the watch list, the WLR for that attacker is added to the rating.*

*The risk rating is calculated by the following formula:*

*RR = (ASR * TVR * SFR) / 10000 + ARR - PD + WLR*

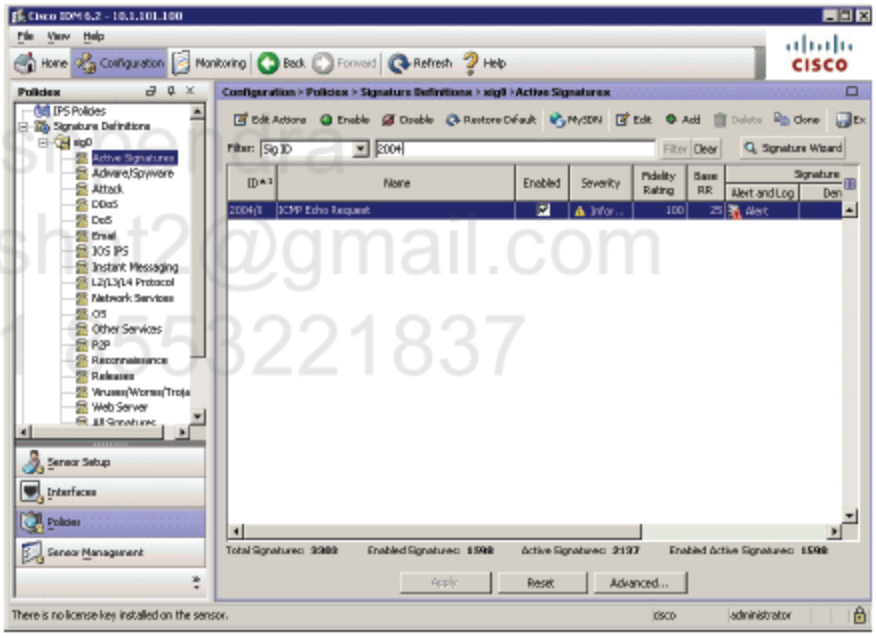
*Valid numbers are from 0–100.*

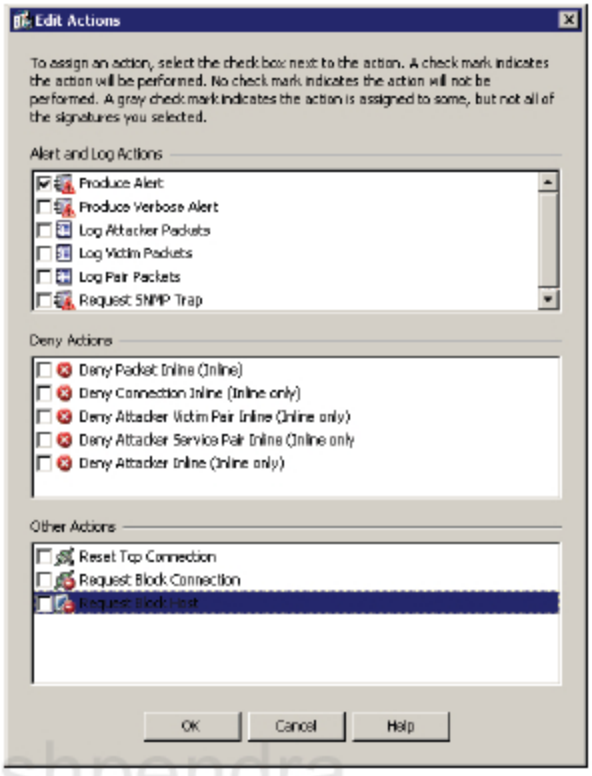
## Configuration

Complete these steps:

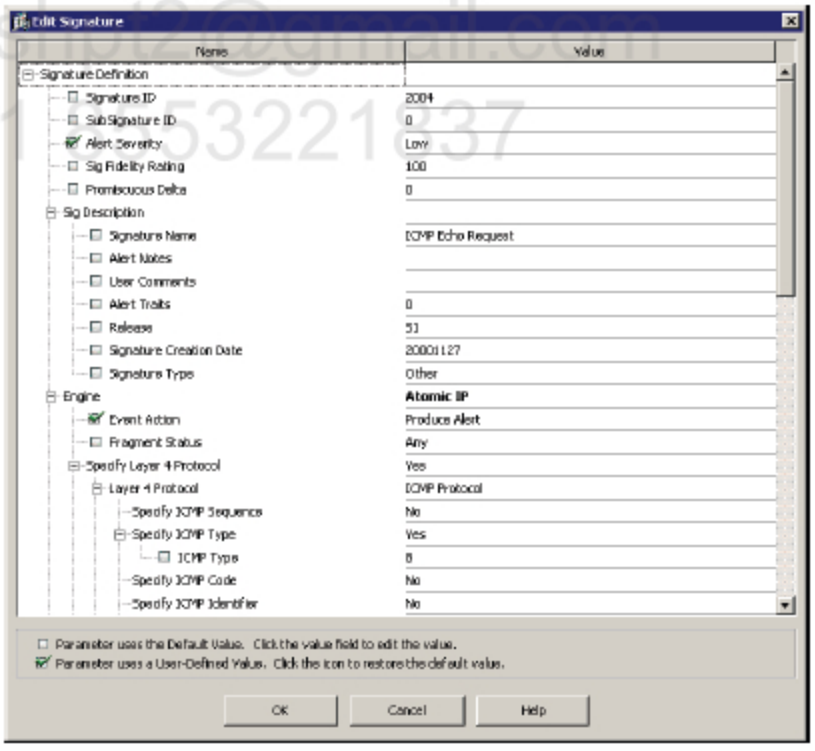
**Step 1** IPS configuration.

1. ***Find out the signature ID 2004 (ICMP Echo Request) by filtering Active Signatures database. Then, click on Edit Actions button and remove blocking actions. Make sure that Alert Severity is Low.***







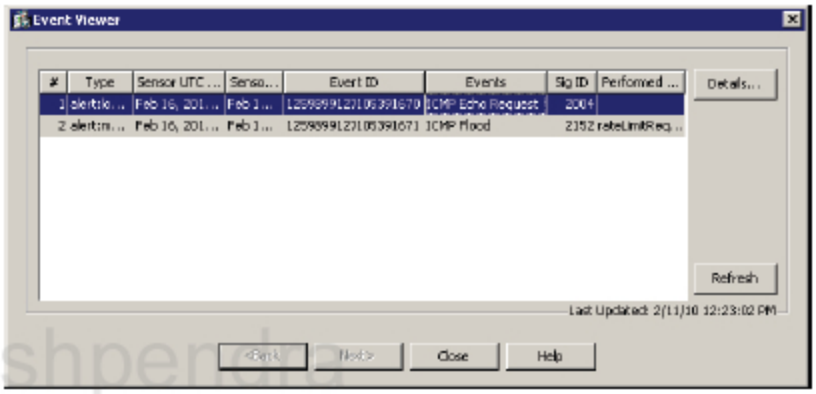




### 2. *Ping R4 from R1 to check if the signature triggers.*

```
R1#ping 10.1.101.4
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the fired signature 2004 on the event list.***





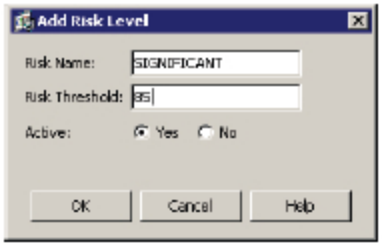

***Double click on the event to see more details. Here's the text output for event details.***

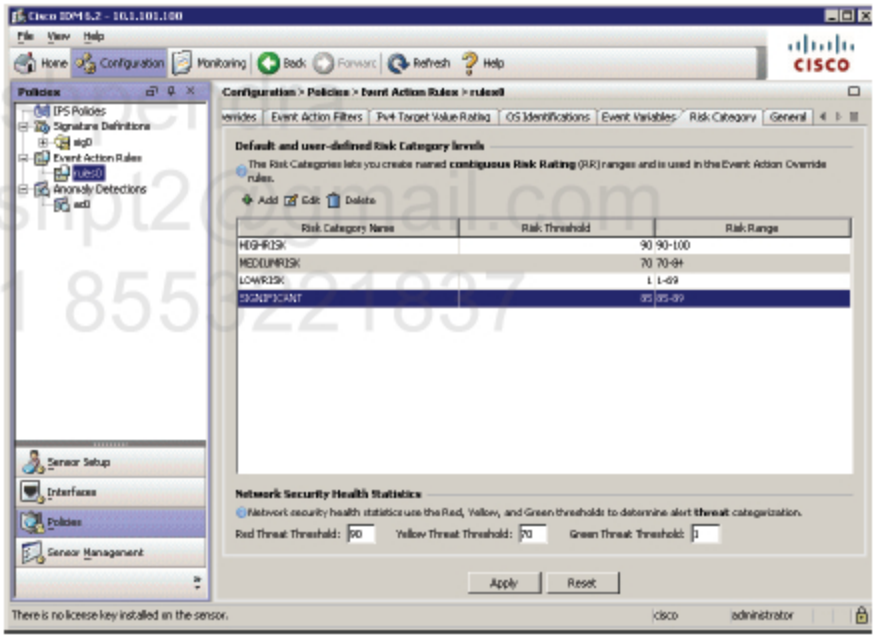
```
evIdsAlert: eventId=1259899127105391670  vendor=Cisco  severity=low
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 16, 2010 20:24:46 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Echo Request  id=2004  version=S1
type=other  created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=OUT
      os:  idSource=unknown  type=unknown  relevance=relevant
  riskRatingValue: 60  targetValueRating=medium
attackRelevanceRating=relevant
  threatRatingValue: 60
  interface: ge0_0
```

```
protocol: icmp
```

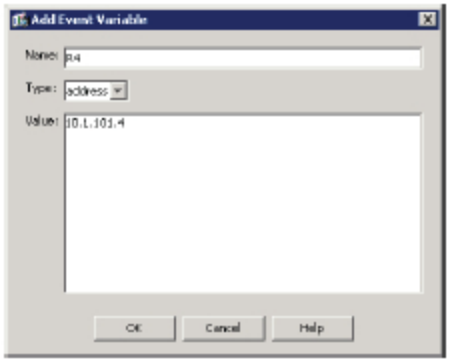
See that Risk Rating is 60 for that alert.

3. *Go to Configuration → Policies → Event Action Rules → rules0 → Risk Category (tab) and click Add. Enter "SIGNIFICANT" for the Risk Name and set the Risk Threshold to 85. Select Yes to activate the risk level and click OK.*

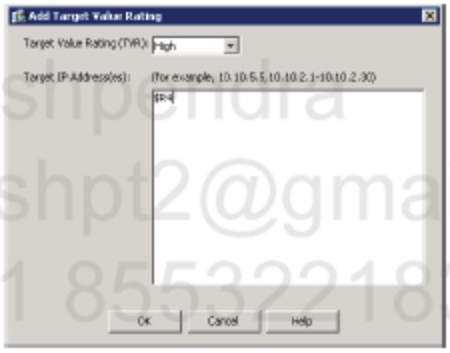



4. *Go to Configuration → Policies → Event Action Rules → rules0 → Event Variables (tab) and click Add. Create the variable named "R4" of a type in Address and the Value of 10.1.101.4. This variable will be used when creating action rules.*



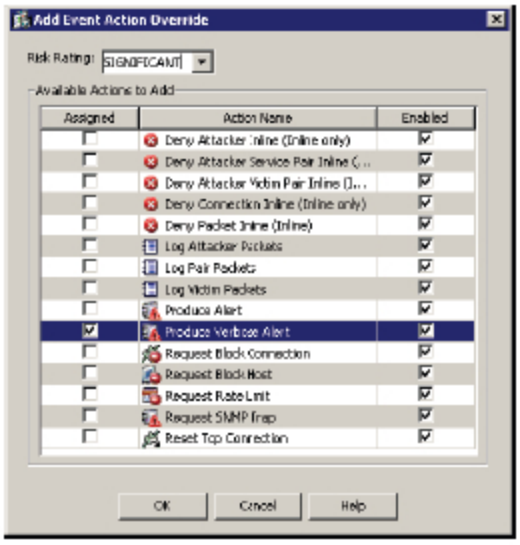

5. ***Go to Configuration → Policies → Event Action Rules → rules0 → IPv4 Target Value Rating (tab) and click Add. From the Target Value Rating (TVR) drop-down list select High and use the variable of "$R4" in the Target IPv4 Address(es) field. Click OK.***

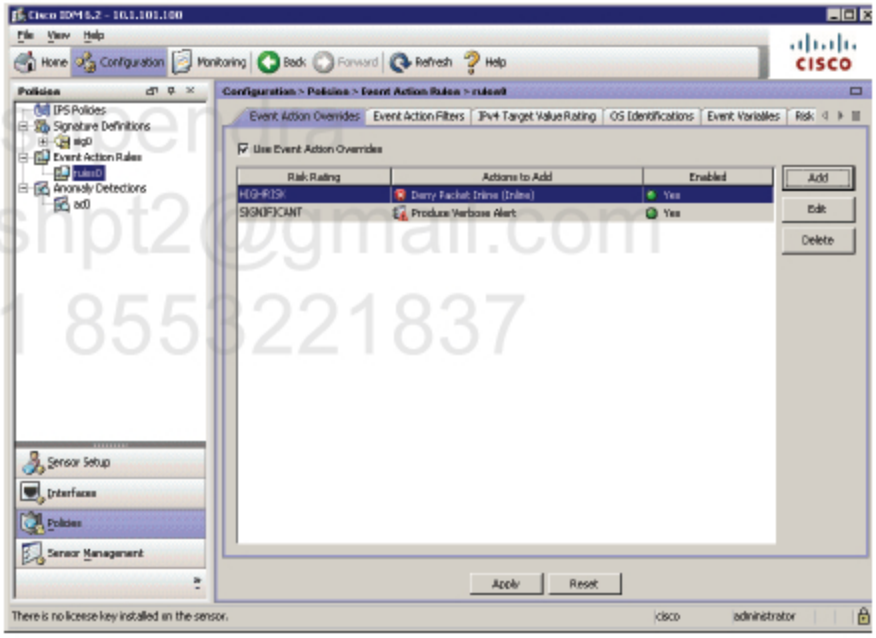





**Remember that you can use variables in the configuration. You must use a dollar sign ($) to use the variable. Also note that you must commit changes on the sensor (Apply the changes) before using the variable so that the sensor knows about it before first use.**

6. ***Go to Configuration → Policies → Event Action Rules → rules0 → Event Action Override (tab) and click Add. For the Risk Rating named SIGNIFICANT add an action of Produce Verbose Alert by selecting Assigned checkbox next to that alert name.***



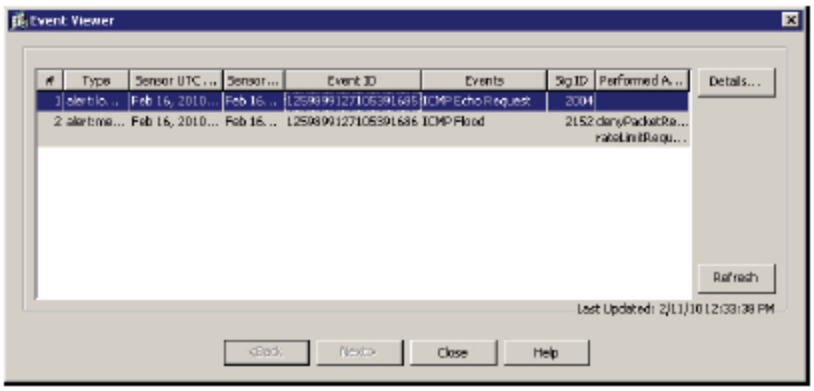



## Verification

```
R1#ping 10.1.101.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
R1#
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the fired signature 2004 on the event list.***




***Double click on the event to see more details. Here's the text output for event details.***



```
evIdsAlert: eventId=1259899127105391685  vendor=Cisco  severity=low
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 16, 2010 20:35:22 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=R4
      os:   idSource=unknown  type=unknown  relevance=relevant
  triggerPacket:
000000  00 1A A1 8F 8C F0 00 19  30 10 86 18 08 00 45 00  ........0.....E.
000010  00 64 75 B1 00 00 FF 01  68 E1 0A 01 64 01 0A 01  .du.....h...d...
000020  65 03 08 00 09 93 00 1F  00 00 00 00 00 00 0C 60  e..............`
000030  68 38 AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  h8..............
000040  AB CD AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  ................
000050  AB CD AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  ................
000060  AB CD AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  ................
000070  AB CD                                            ..
```

```
riskRatingValue: 85  targetValueRating=high  attackRelevanceRating=relevant
threatRatingValue: 85
interface: ge0_0
protocol: icmp
```

Now, as the R4 is treated as a HIGH valued asset, the Risk rating is 85. Hence some action override can be applied.

## Task 2

The ICMP Flood (ID 2152) signature is triggered when pinging R4. Configure Event Action Filters to subtract Rate Limiting action from triggered signature when the ping is issued from R1.

*Action Filters are used to subtract some actions from the signature. If we do not want to trigger some actions on the signatures triggered for specific host, we can subtract those actions here.*



## Configuration

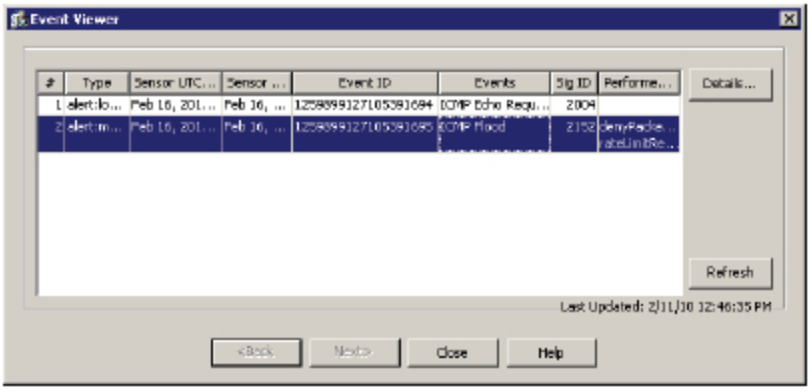
Complete these steps:

**Step 1** Before any configuration.

***Before configuring the solution:***

```
R1#ping 10.1.101.4 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.101.4, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the signature ID 2152 on the event list.***




***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105391695  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 16, 2010 20:48:14 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Flood  id=2152  version=S354  type=other
created=20000101
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=R4
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    denyPacketRequestedNotPerformed: true
```

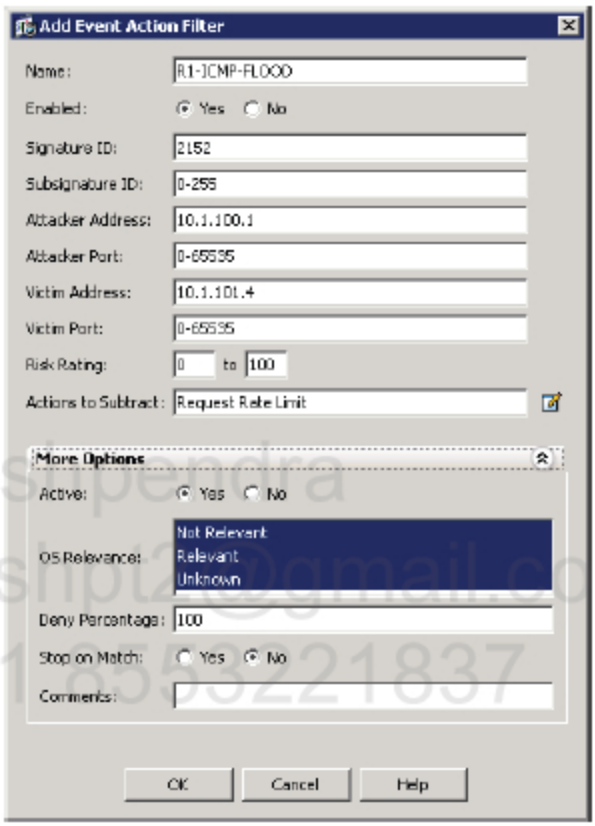
This is because there is Event Action Override configured for HIGHRISK signatures which automatically enforces an action of Deny Packet Inline. As in our example we use promiscuous mode, this request is ignored.

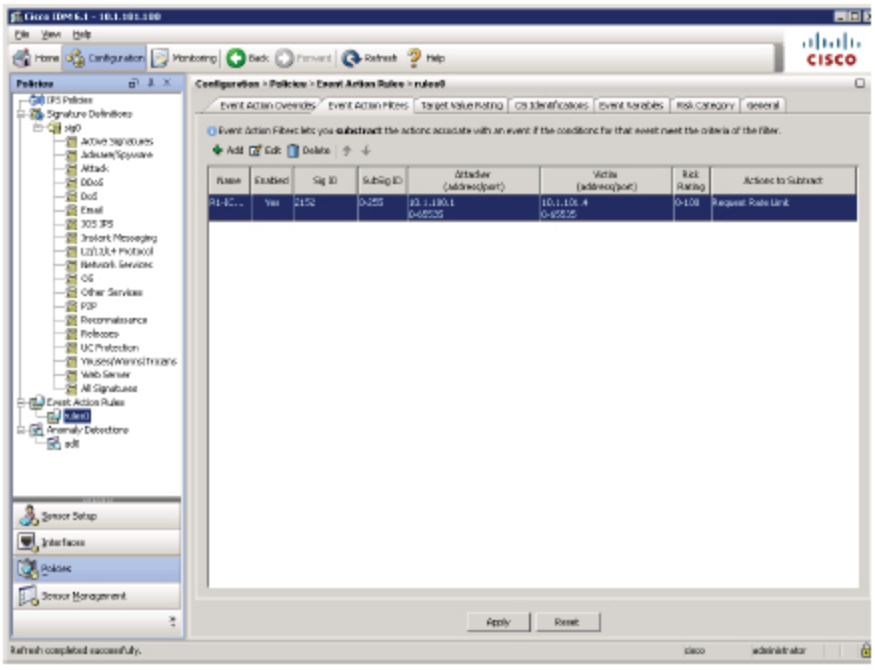
```
    rateLimitRequested: true
  riskRatingValue: 100  targetValueRating=high
attackRelevanceRating=relevant
  threatRatingValue: 80
  interface: ge0_1
  protocol: icmp
```

The Rate Limit action is taking place. Let's change that.

**Step 2** IPS configuration.

1. ***Go to Configuration → Policies → Event Action Rules → rules0 → Event Action Filters (tab) and click Add. Configure the filter for ICMP Flood signature (ID 2152) to substract "Request Rate Limit" action from the signature when trigger due to R1 (10.1.101.1) attack.***



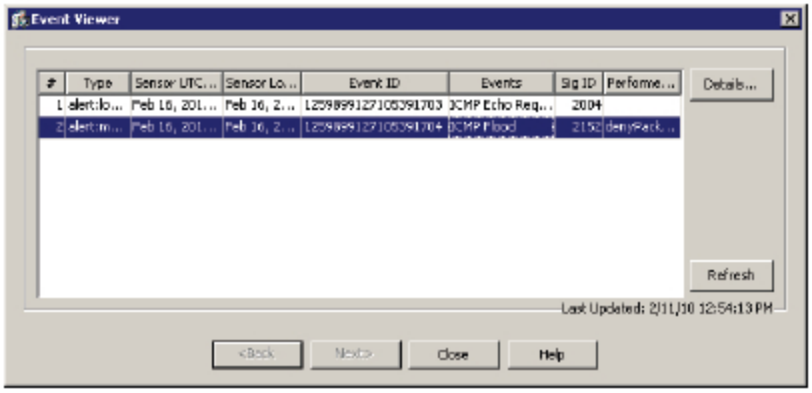




## Verification

```
R1#ping 10.1.101.4 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.101.4, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the signature ID 2152 on the event list.***



***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105391704  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 16, 2010 20:55:56 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Flood  id=2152  version=S354  type=other
created=20000101
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=R4
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    denyPacketRequestedNotPerformed: true
  riskRatingValue: 100  targetValueRating=high  attackRelevanceRating=relevant
  threatRatingValue: 100
  interface: ge0_1
  protocol: icmp
```

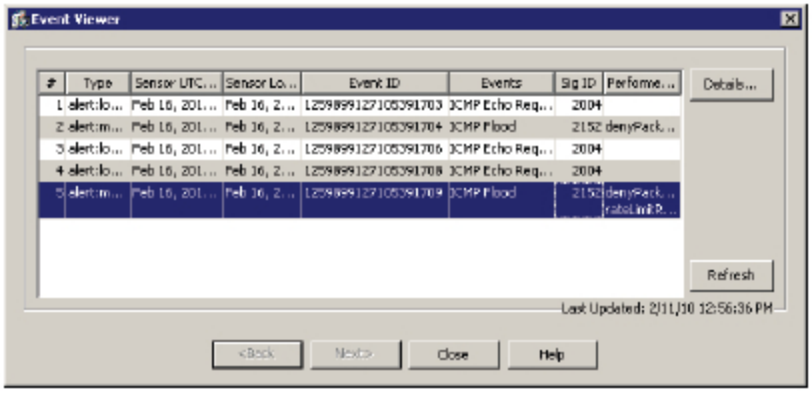


**Note that there is no Rate Limiting action applied!**

**Let's ping from another IP address.**

```
R2#ping 10.1.101.4 rep 100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R2#
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the signature ID 2152 on the event list.***



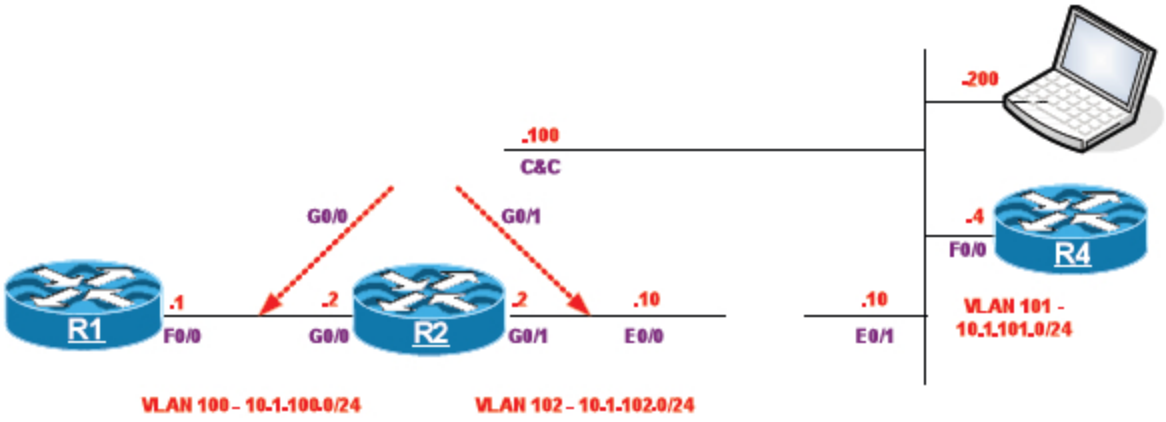

***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105391709  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 16, 2010 20:58:17 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Flood  id=2152  version=S354  type=other
created=20000101
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.102.2  locality=OUT
    target:
      addr: 10.1.101.4  locality=R4
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    denyPacketRequestedNotPerformed: true
    rateLimitRequested: true
  riskRatingValue: 100  targetValueRating=high  attackRelevanceRating=relevant
  threatRatingValue: 80
  interface: ge0_1
  protocol: icmp
```

**Note that there is Rate Limit action applied to the ICMP Flood originated from R2.**

# LAB 2.12. Anomaly Detection

**This lab is based on the configuration from the previous lab**






## Task 1

Configure Anomaly Detection (ad0) engine with the following characteristics:

- Knowledge learing must start every workday (Mo-Fri) at 9am
- A vulnerability assessment tool at IP address of 10.1.100.100 must be excluded from anomaly detection learning and detection
- Your internal zone consists of 10.1.101.0/24 valid host IP addresses
- Scanner threshold for TELNET protocol (TCP/23) must be set to 100 with a custom histogram of L=12 M=8 H=2
- Scanner threshold for ICMP protocol must be set to 50
- Illegal IP addresses in your network are from Class E address space

*Anomaly detection (AD) features allow you to initially set the IPS device into learning mode which samples flows traversing your IPS appliance and establishes a baseline of known normal traffic flows. When traffic flow deviates from what is expected, the anomaly detection engine will respond to the deviation by either dropping traffic or notifying security responders of the anomalous behavior.*

*In general the AD engine looks for behavior on the network that is indicative that scanning worm is present on the network. This detection engine is not based on predefined signatures instead it's based on network behavior.*

*Learning*

*The fundamental objective of learning mode is to establish normal behavior of the network. Learning mode keeps track of behavior that may be attributed to worm scanning behavior such as.*

- *TCP SYN packets that are not followed by a flow*
- *UDP packets that are not followed by flows*
- *ICMP packets that display scanning type behavior*

*Illegal IP address destinations, such as private addresses that aren't part of your network, bogon addresses, addresses that are in predefined zones and should not be accessed by the host sourcing the packet.*

*The network profile, called a histogram, is a table with an entry for every TCP and UDP destination port which carries significant network traffic. An entry in the table describes not just a single threshold, but a complete histogram of the highest scan rates observed on this destination port. This might mean that on HTTP we don't expect any source IP to make failed connection attempts to more than 5 different destination within a single one minute time interval; and that on ports associated with Kazaa, we don't expect to see concurrently more than 3 source IP's each making more than 5 failed connection attempts during a single given one minute interval.*

*By building this histogram profile of the network during quiet periods, when a certain source of set of sources becomes infected with worm, very quick and accurate detection is possible, since the network behavior for that port will immediately differ from the one observed during peace-time.*



*Example for TCP service 80:*

*Default Histogram =*

| | | | |
|---|---|---|---|
| *# Source Ips* | *18* | *6* | *2* |
| *# Destination IPs* | *5* | *20* | *100* |

*Default Scanner threshold = 120*

*This means that:*

- *From a single source we do not expect to see more than 120 un-established connections to different destination IPs.*
- *We do not expect to see more than 18 sources generate un-established connections to 5 or more different destinations*
- *We do not expect to see more than 6 sources generate un-established connections to 20 or more different destinations*
- *We do not expect to see more than 2 sources generate un-established connections to 100 or more different destinations*

*All values are for 60 seconds duration.*

*Detection*

*Basically AD detection mode kicks after a learned baseline is established. Detection uses the following characteristics:*

- *AD monitors the network traffic and looks for worm/scanners by comparing traffic to the Knowledge Base histograms' and scanners' threshold*
- *Once a scanner threshold is violated an alert is triggered for the appropriate signature*
- *Once an histogram threshold is crossed the service is considered to be under worm attack*
- *AD will try to detect and report infected hosts*

*Configuration*

*Each AD configuration incidents contains the following elements:*

- *Scheduler - schedule learning mode and how often you want to save an AD knowledge database.*
- *Zones' IP addresses – define zones and valid IP addresses associated with those zones*
- *IP addresses to ignore - defining IP addresses that can be ignored, such as scanning the workstations that are being used by approved corporate security scanners*
- *Services' histograms and scanner threshold - manually defined thresholds and parameters for each service in histogram*

*AD uses nine signatures for alerts. The signatures are in the range 13000 – 13008. Each signature has two sub signatures:*

*0 – Scanner*

*1 – Scanner during worm*

*AD Zones*

*The concept of zones is used in anomaly detection to help to decrease false positives. Below is a summary of how zones are used by the AD engine:*

- *Zone information is used to sub-divide the network to achieve lower false positives*
- *A zone is a set of destination IP addresses.*
- *An Illegal Zone contains illegal addresses and/or non allocated addresses,*
- *Traffic toward illegal addresses might be a strong indication of worm activity and you may want to allow low thresholds for worm detection when traffic destined to these addresses are detected.*
- *Internal Zone contains addresses within the protected network*
- *External Zone contains valid addresses that are not part of the protected zone*

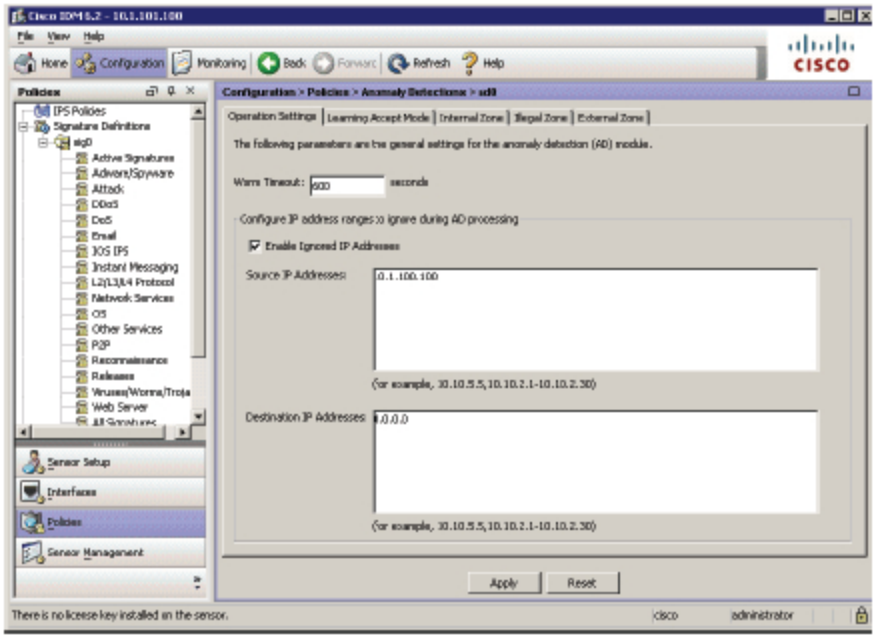


## Configuration

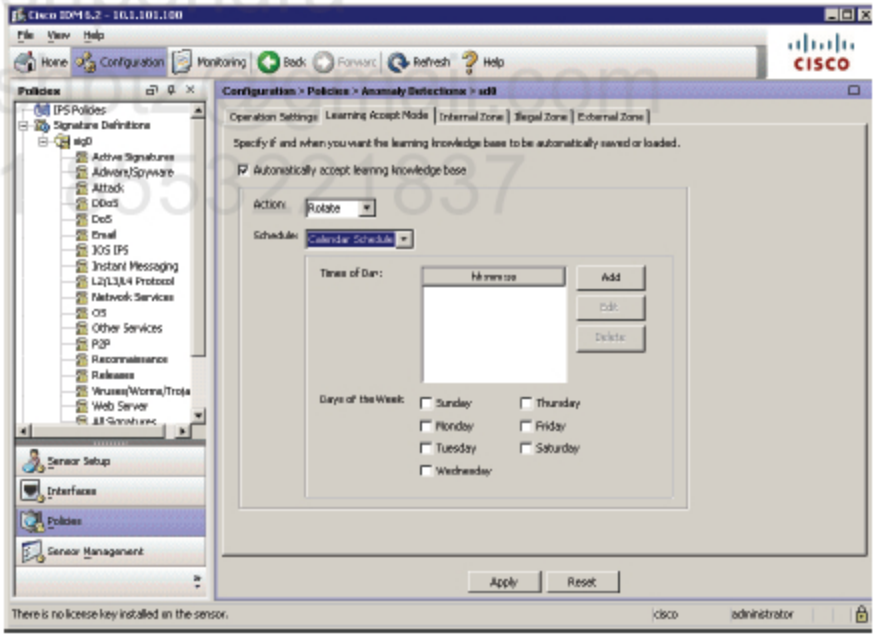
Complete these steps:

**Step 1** IPS configuration.

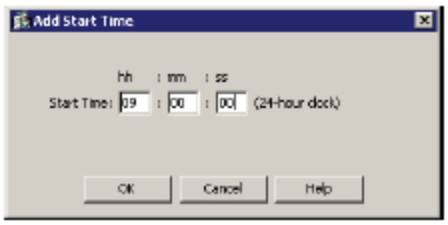
1. ***Go to Configuration → Policies → Anomaly Detections → ad0 → (tab) Operation Settings and configure it as follows:***



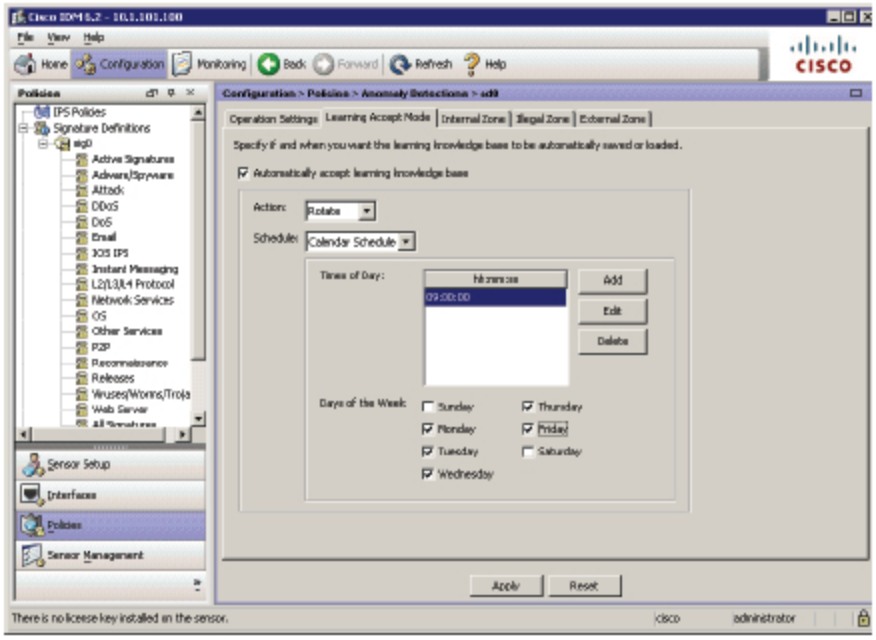

2. ***Go to the (tab) Learning Accept Mode and select "Calendar Schedule" from the drop-down Schedule list.***




3. ***Click Add and set the Start time to 9am.***

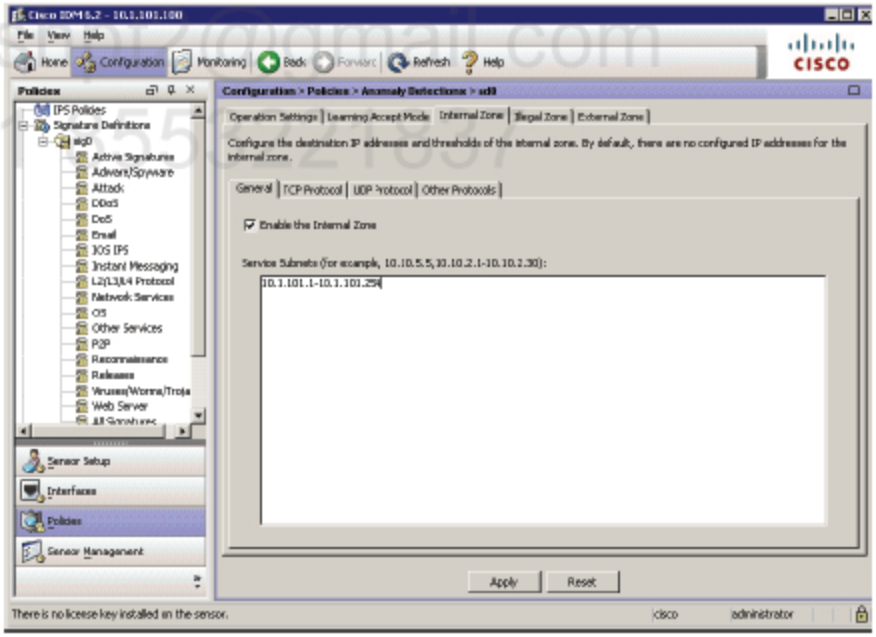


4. **Select workdays (Mo-Fri) from the Days of the Week section.**

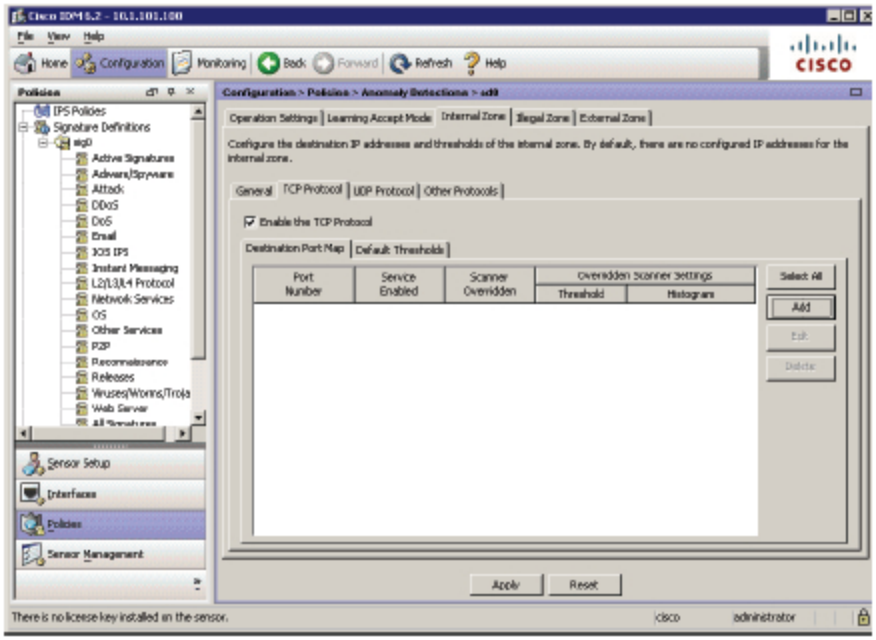




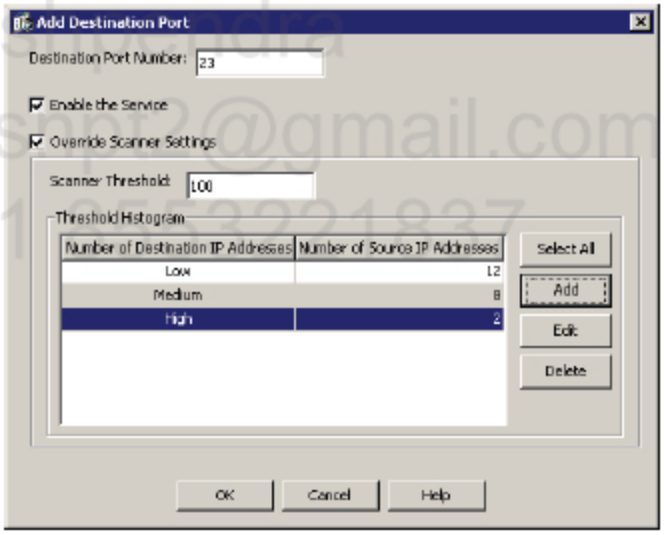

5. **Go to the (tab) Internal Zone and configure the range of 10.1.101.1-10.1.101.254**

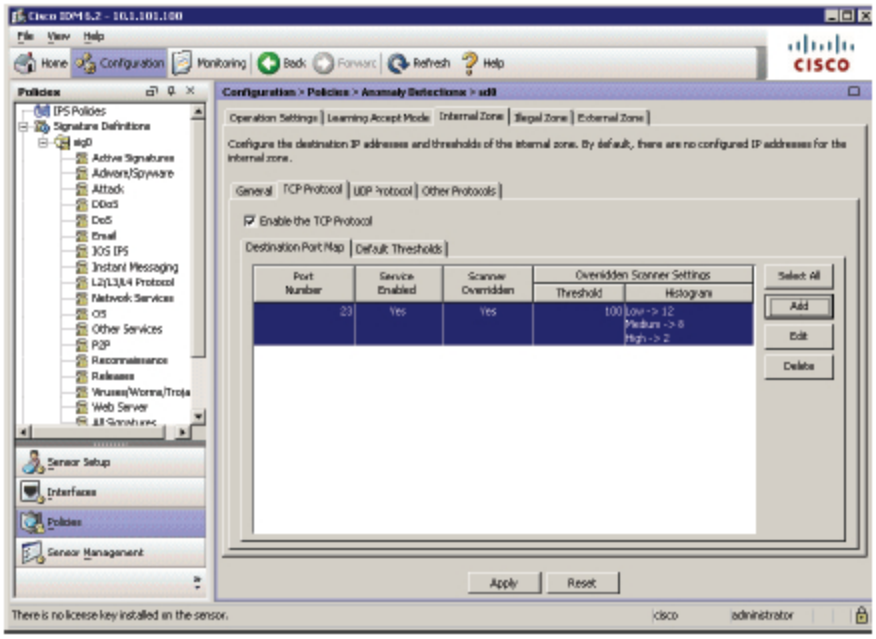



6. **Then click on TCP Protocol tab under the Internal Zone tab and click Add button.**



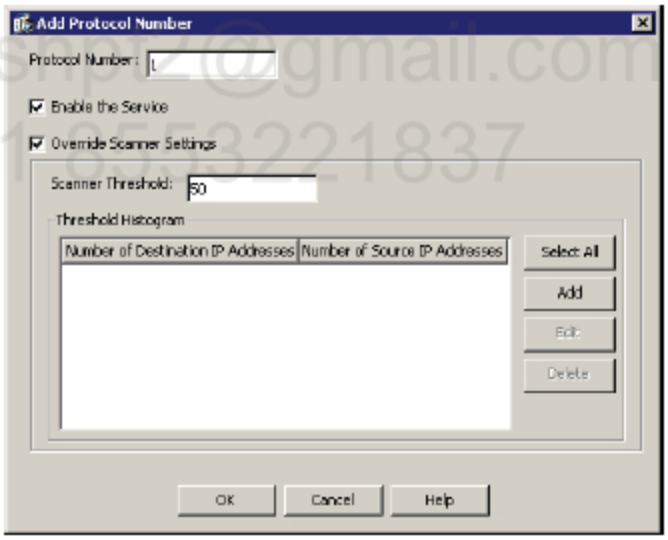

### 7. Configure the options as follows for port 23:

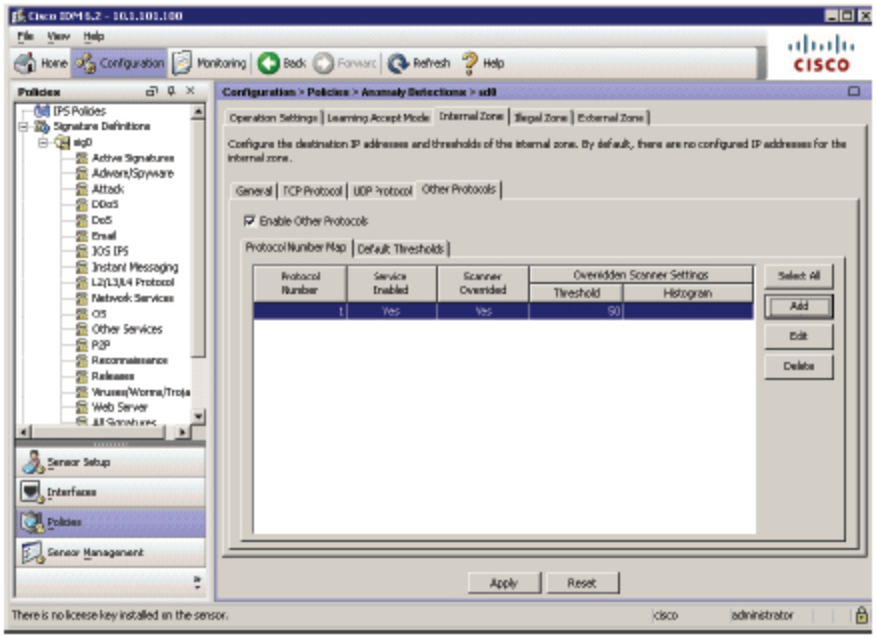




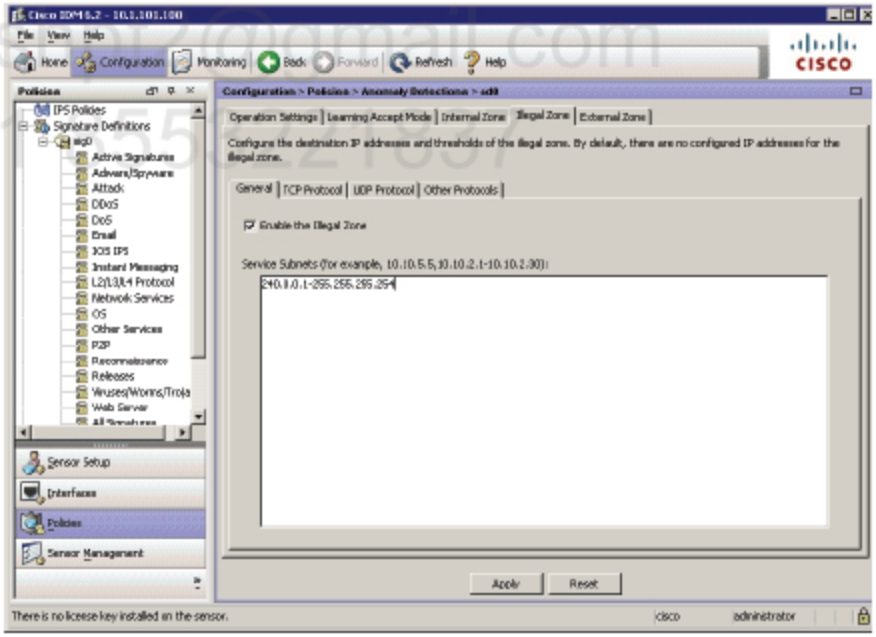

8. ***Change the tab to Other Protcols and click Add to configure the options for protocol 1 (which is ICMP):***





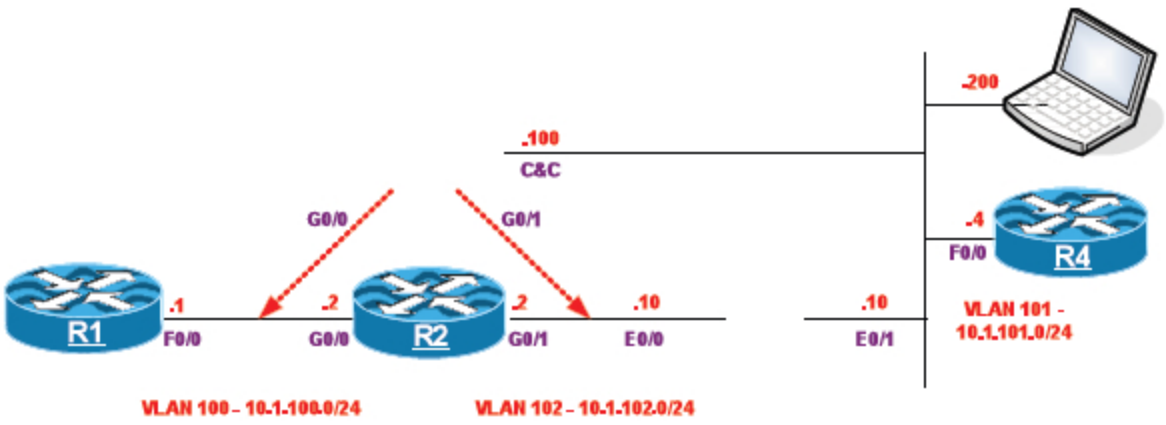



9. ***Go to the (tab) Illegal Zone and configure the range of 240.0.0.1-255.255.255.254 (which is whole Class E).***



# LAB 2.13. Virtual Sensors

**This lab is based on the configuration from the previous lab**






## Task 1

Change the configuration of G0/1 interface so that it belongs to different Virtual Sensor and triggers ICMP Flood signature with a High severity. The new virtual sensor must have separate signature and rules defined. The Anomaly Detection must be disabled in VLAN 102 and no Action Override happens.

*A virtual sensor can monitor multiple segments, and let you apply a different policy or configuration for each virtual sensor within a single physical sensor. You can set up a different policy per monitored segment under analysis. You can also apply the same policy instance, for example, sig0, rules0, or ad0, to different virtual sensors. You can assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a virtual sensor.*

*Virtual sensors have the following advantages:*

- *You can apply different configurations to different sets of traffic.*
- *You can monitor two networks with overlapping IP address spaces with one sensor.*
- *You can monitor both inside and outside of a firewall or NAT device with one physical sensor device.*

*Each virtual sensor consists three components:*

- *Signature definition*
- *Rules*
- *Anomaly detection*

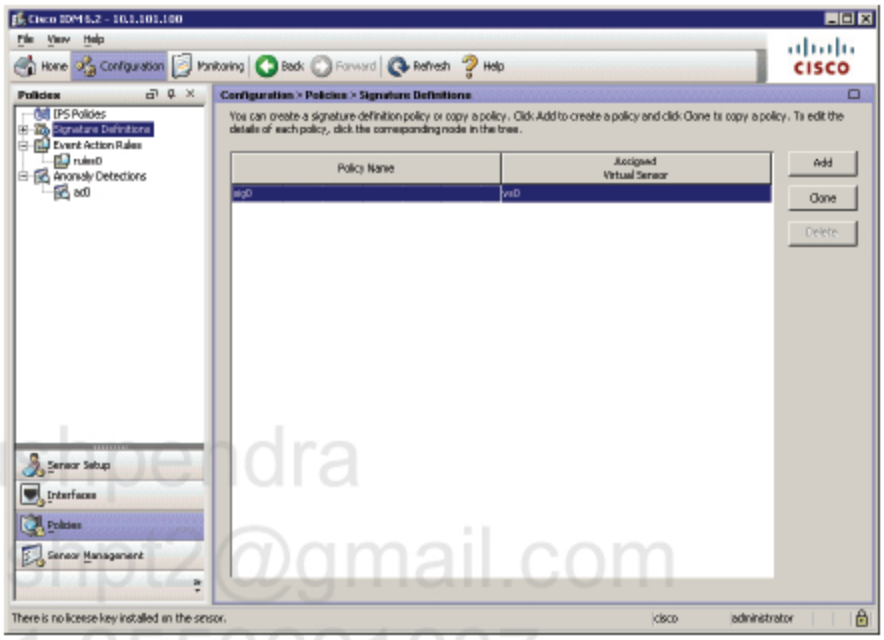
*By default there are sig0, rules0 and ad0 components but you can create new ones with different configuration and then assign them to the new virtual sensor instance. Note that the default virtual sensor is "vs0." You cannot delete the default virtual sensor.*

## Configuration

Complete these steps:

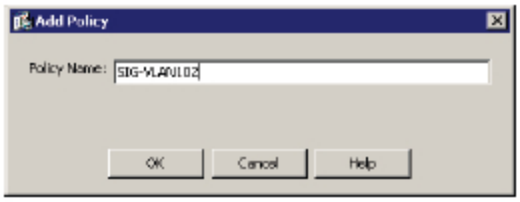
**Step 1** IPS configuration.

1. ***Go to Configuration → Signature Definitions and click Add.***

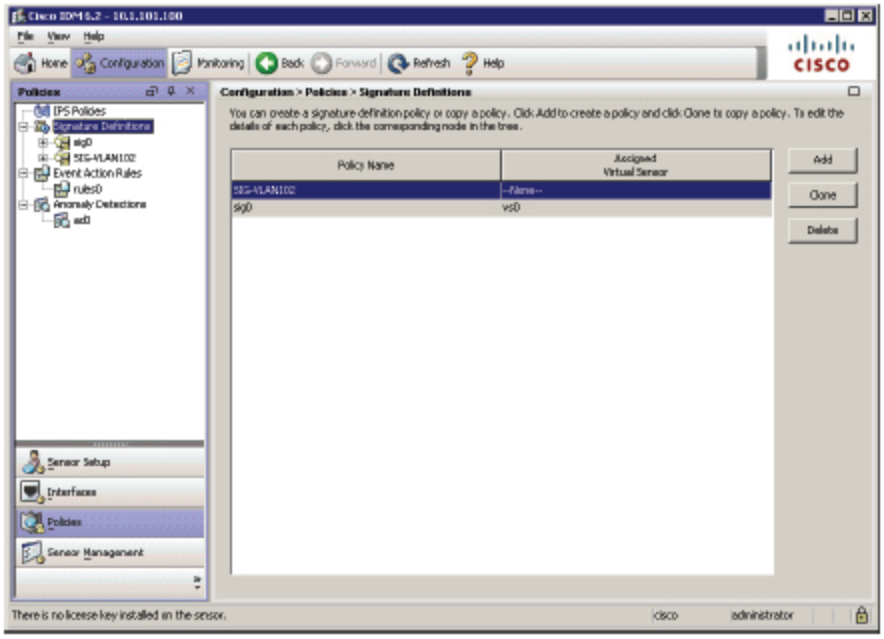




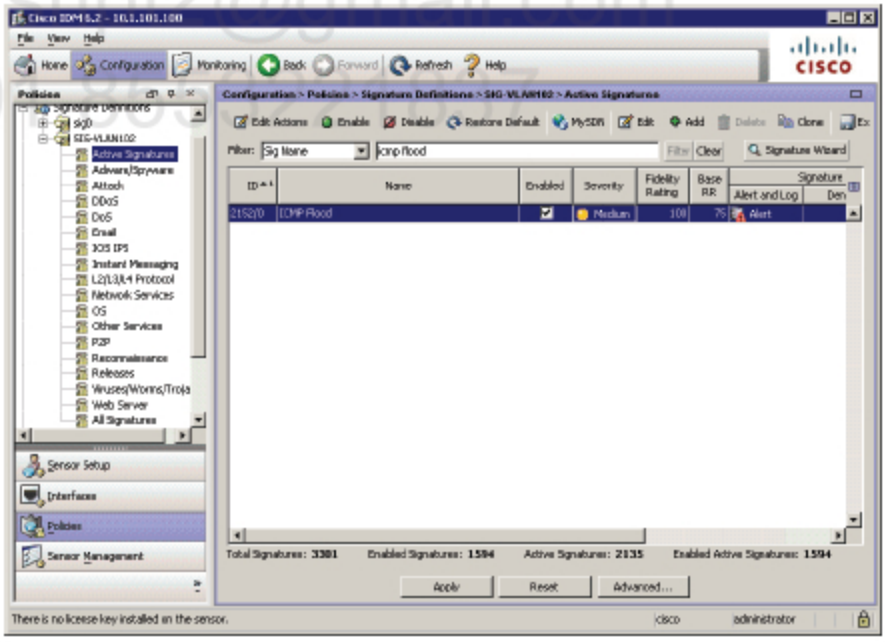

2. ***Enter a name for a new Policy (set of signatures). Click OK to finish.***



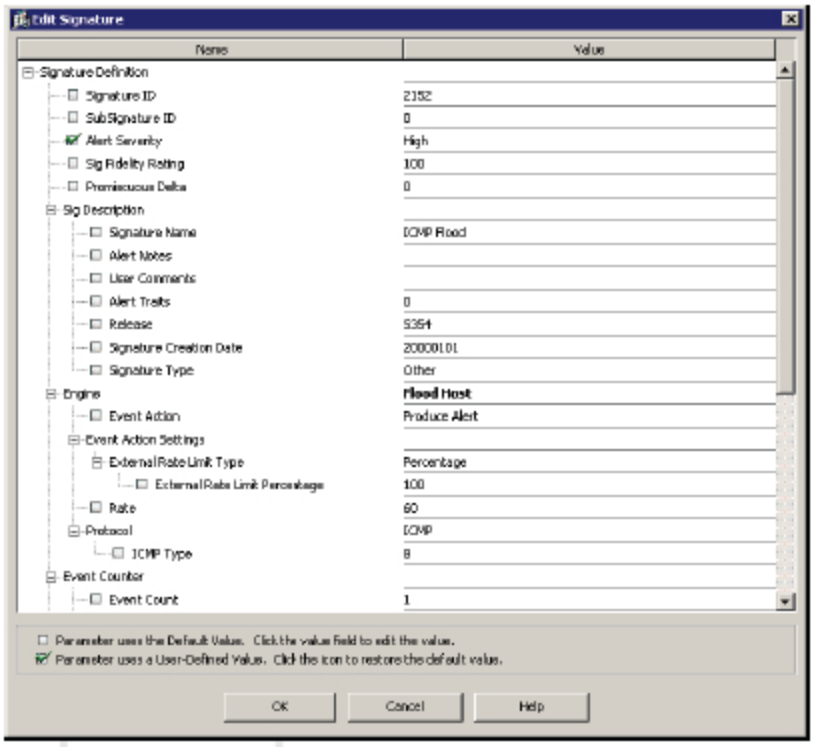

***Note that the newly created signature set is not assigned to any VS yet.***




3. ***Go to Configuration → Policies → SIG-VLAN102 → Active Signatures. From Filter drop-down list select Sig Name and enter "icmp flood" string. Then click on Filter button. Highlight the signature ID 2152/0 and click on Enable.***

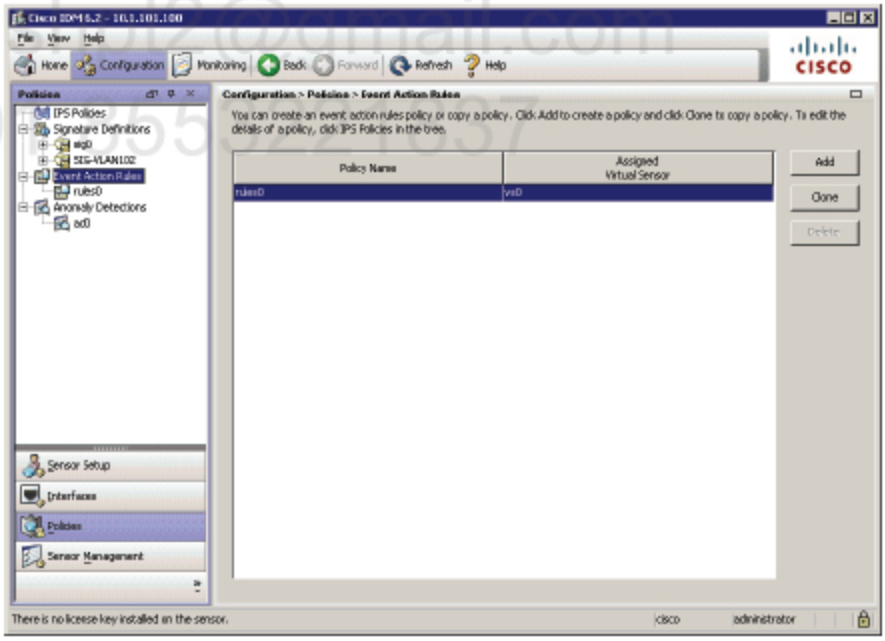



4. ***Select the signature from the list and click Edit. Change the Alert Severity to High.***

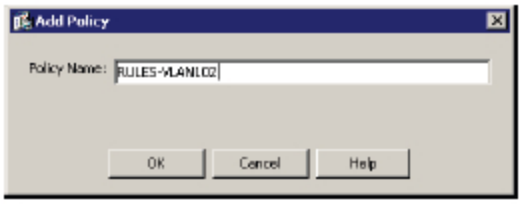




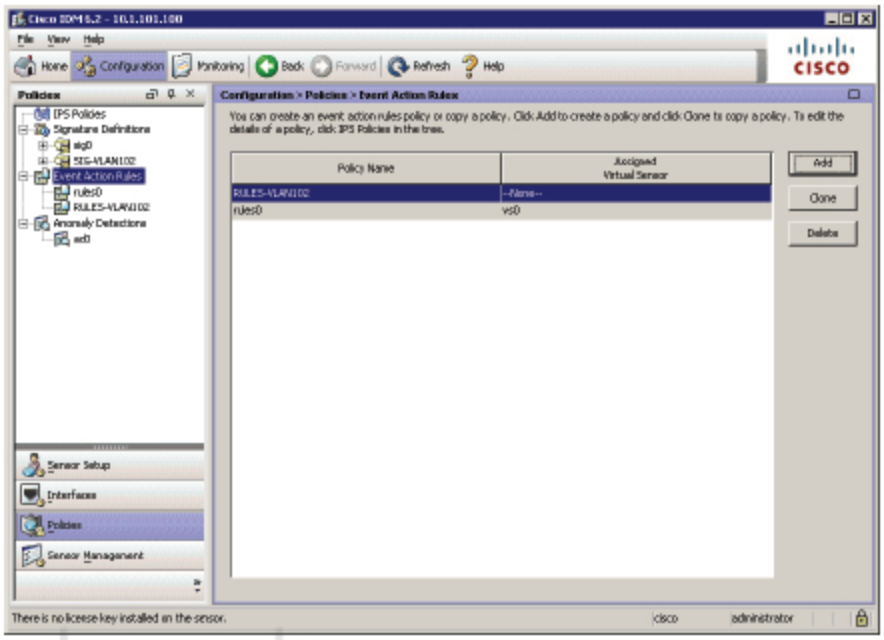

5. **Go to Configuration → Policies → Event Action Rules and click Add.**




6. **Enter a name for the Policy (set of rules) and click OK.**

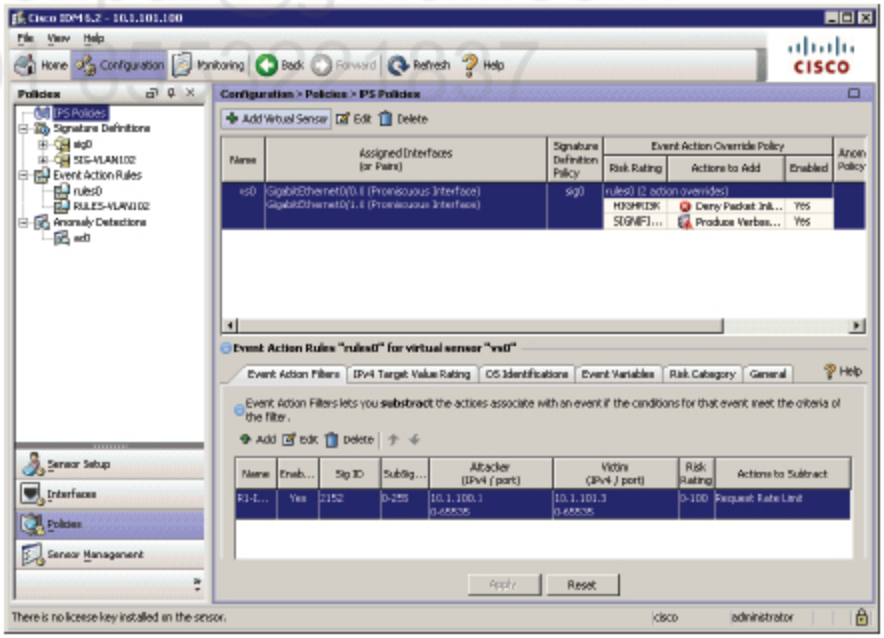


***Note that the newly created ruleset is not assigned to any VS yet.***

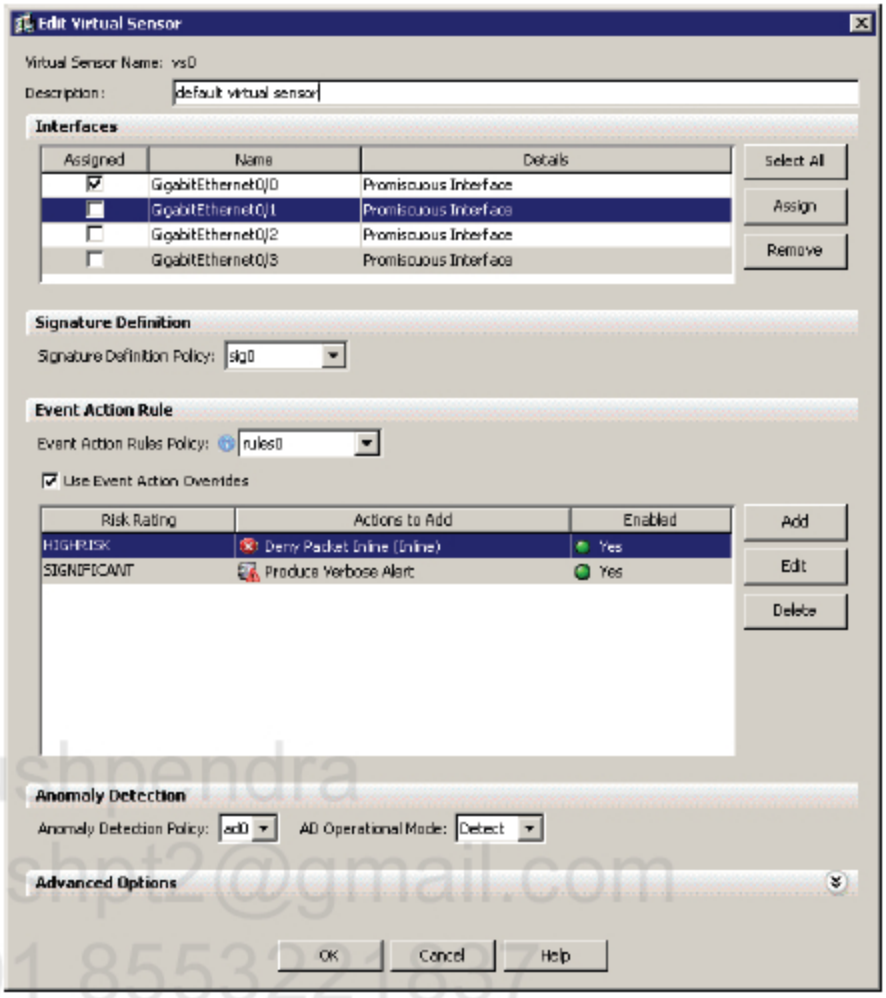





7. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit.***

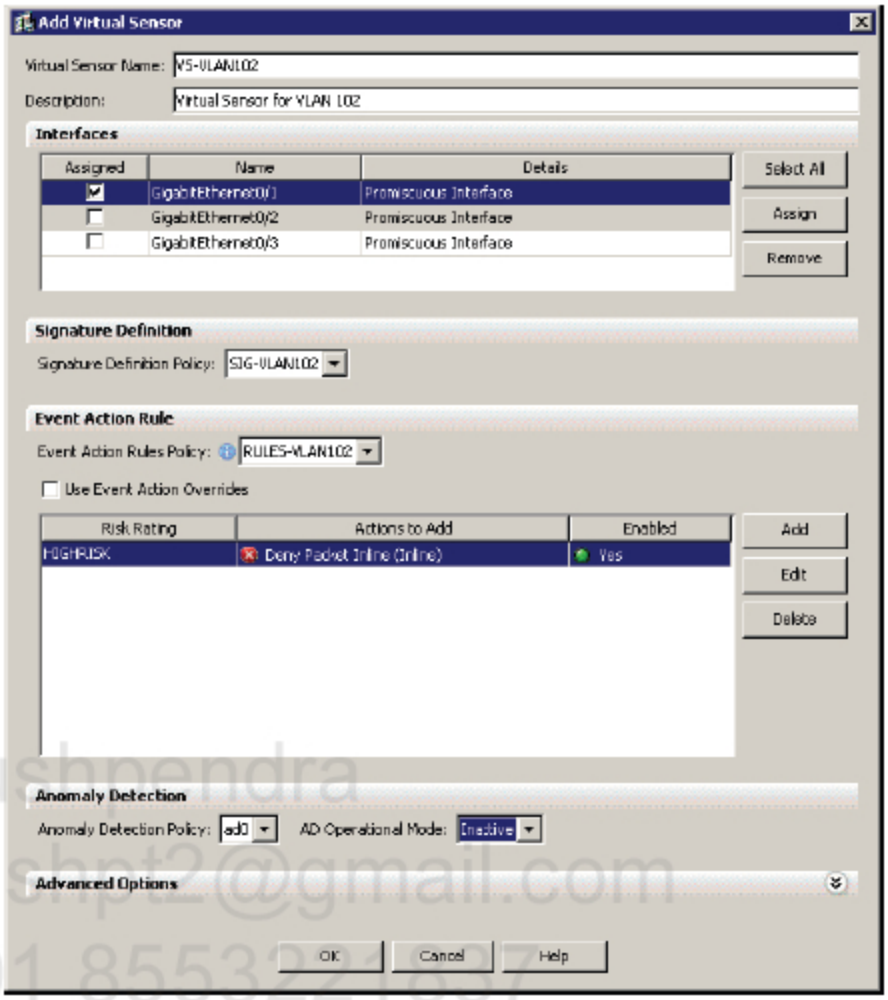



8. ***Highlight GigabitEthernet0/1 interface on the list and click Remove button. Then click OK and Apply the changes to the sensor.***

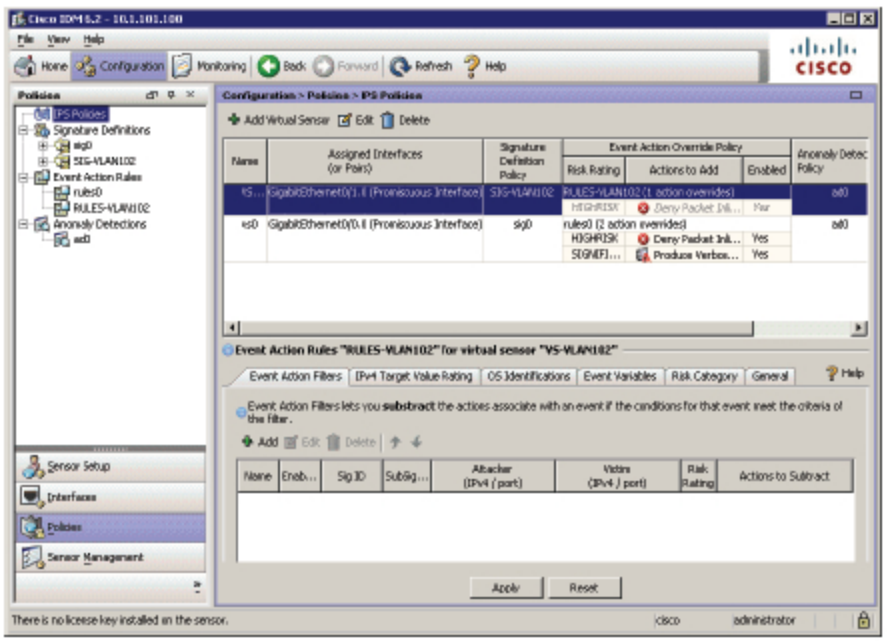





9. ***Go to Configuration → Policies → IPS Policies and click Add Virtual Sensor. Enter a name for virtual sensor i.e. VS-VLAN102. Highlight GigabitEthernet0/1 interface on the list and click Assign button. Select SIG-VLAN102 as Signature Definition Policy and RULES-VLAN102 as Event Action Rules Policy. Uncheck Use Event Action Overrides option and set AD Operational Mode to "Inactive".***



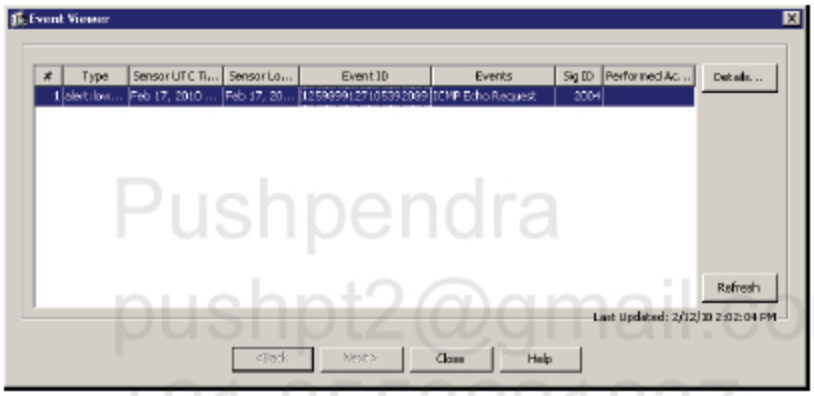


## Verification

```
R1#ping 10.1.101.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.101.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See there is only Signature ID 2004 on the event list.***






***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105392089  vendor=Cisco  severity=low
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 17, 2010 22:03:54 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=R4
      os:   idSource=unknown  type=unknown  relevance=relevant
  triggerPacket:
000000  00 1A A1 8F 8C F0 00 19  30 10 86 18 08 00 45 00  ........0.....E.
```

```
000010  00 64 75 C0 00 00 FF 01  68 D2 0A 01 64 01 0A 01  .du.....h...d...
000020  65 03 08 00 D5 40 00 22  00 00 00 00 00 00 11 D7  e....@."........
000030  97 10 AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  ................
000040  AB CD AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  ................
000050  AB CD AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  ................
000060  AB CD AB CD AB CD AB CD  AB CD AB CD AB CD AB CD  ................
000070  AB CD                                            ..
```

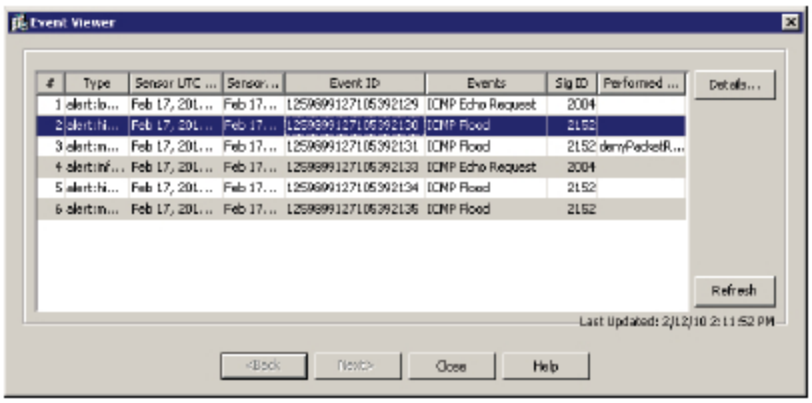
```
  riskRatingValue: 85  targetValueRating=high  attackRelevanceRating=relevant
  threatRatingValue: 85
  interface: ge0_0
  protocol: icmp
```

**The above signature is triggered by VS0 only as VS-VLAN102 has default settings and the signature 2004 is disabled by default.**

```
R1#ping 10.1.101.4 rep 120

Type escape sequence to abort.
Sending 120, 100-byte ICMP Echos to 10.1.101.4, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (120/120), round-trip min/avg/max = 1/2/4 ms
R1#
```



***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the ICMP Flood signature has triggered.***




***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259899127105392130  vendor=Cisco  severity=high
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
```

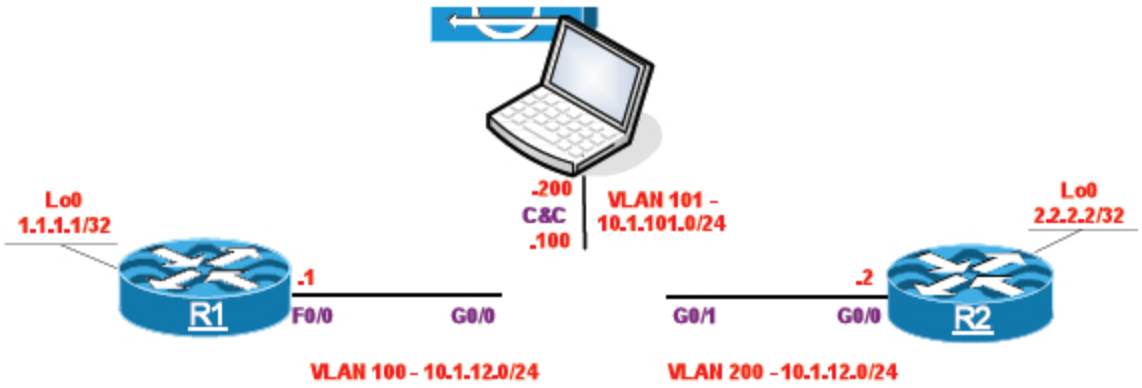
```
    appInstanceId: 386
  time: Feb 17, 2010 22:13:20 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Flood  id=2152  version=S354  type=other
created=20000101
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: VS-VLAN102
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  riskRatingValue: 100  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 100
  interface: ge0_1
  protocol: icmp
```

Note the serverity is High for that signature and it has triggered on VS-VLAN102.



```
evIdsAlert: eventId=1259899127105392131  vendor=Cisco  severity=medium
  originator:
    hostId: CCIE-IPS
    appName: sensorApp
    appInstanceId: 386
  time: Feb 17, 2010 22:13:20 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Flood  id=2152  version=S354  type=other
created=20000101
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.100.1  locality=OUT
    target:
      addr: 10.1.101.4  locality=R4
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    denyPacketRequestedNotPerformed: true
  riskRatingValue: 100  targetValueRating=high  attackRelevanceRating=relevant
  threatRatingValue: 100
  interface: ge0_0
  protocol: icmp
```

# LAB 2.14. Event Summarization




## Lab Setup

- R1's F0/0 and R2's G0/0 interface should be configured in VLAN 100 and VLAN 200 respectively
- PC and IPS Command and Control (C&C) interface should be configured in VLAN 101
- Configure Telnet on all routers using password "cisco"
- Configure RIPv2 on all devices (except PC and IPS)



## IP Addressing

| Hostname | Interface (ifname) | IP address |
|---|---|---|
| R1 | F0/0 | 10.1.12.1/24 |
| | Lo0 | 1.1.1.1/32 |
| R2 | G0/0 | 10.1.12.2/24 |
| | Lo0 | 2.2.2.2/32 |

## Task 1

Configure IPS Sensor in inline mode using its G0/0 and G0/1 interfaces configured in VLAN 100 and VLAN 200 respectively. Use the following initial settings:

Hostname: IPS-CCIE

IP address: 10.1.101.100/24

Default Gateway: 10.1.101.10

Allowed Hosts: 10.1.101.200

Enable ICMP Echo Request (ID 2004) signature so that it generates only one event no matter how many ICMP packets it seen.
Enable ICMP Echo Reply (ID 2000) signature so that it summarize events in 10 sec interval using Victim Address as a key. Also, enable global summarization for this signature so that it generates global summary event after see 100 ICMP Echo Reply packets.

*Signature engines enable you to configure signatures by modifying their parameters. Some parameters are common across all engines, and others are specialized for a specific engine.*
*One of common signature properities is Event Counter. When expanded (in signature's properities) this displays the parameters that determine whether the signature fires. The Event Counter parameters enable you to configure how the sensor counts events. For example, you can specify that you only want the signature to fire if the activity it detects happens five times for the same address set within a specified period of time.*
*The Event Count enables you to prevent the signature from firing until the number of specified events is seen during the specified alert interval on the specified Event Count Key. The default value is 1.*



*Event Count Key - is used for counting multiple firings of the signature. This key influences signature firing by specifying the address sets on which the Event Count parameter is based. It has the following settings:*

- *Attacker address*
- *Attacker address and victim port*
- *Attacker and victim addresses*
- *Attacker and victim addresses and ports*
- *Victim address*

*Alert Interval (2–1000) - is the number of seconds during which the Event Count must be met if the signature is to fire.*

*In addition to event counting we may configure Alert Frequency. When expanded, this displays the parameters for configuring how often the sensor sends an alert to the Event Store when the signature is firing. The Alert Frequency parameters enable you to control the number of alarms generated by a specific signature.*

*Summary Mode - is a technique used to limit alarm firings. The Summary Mode has the following settings:*

- *Fire Once: Sends the first alert and then deletes the inspector*
- *Fire All: Sends all alerts*
- *Summarize: Sends an interval summary alert*
- *Global Summarize: Sends a global summary alert*

*Summary Key - identifies the address set to use for counting events for event summarization. For*

*example, if you want the sensor to count events based on whether they are from the same attacker, choose Attacker address as the Summary Key. Summary Key has the following settings:*

- *Attacker address*
- *Attacker address and victim port*
- *Attacker and victim addresses*
- *Attacker and victim addresses and ports*
- *Victim address*

*Global Summary Threshold (1–65535) - This is the number of events required to automatically change the summary mode to Global Summarize. When the alert rate exceeds this threshold within the summary interval, the sensor changes from sending a summary alert to sending a global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured summary mode behavior. A global summary counts the signature firings on all of the attacker IP addresses and ports and all of the victim IP addresses and ports.*

*Summary Interval (1–65535) - defines the period of time used to control alarm summarization.*

## Configuration

Complete these steps:

**Step 1** SW4 configuration.

```
SW4(config)#interface FastEthernet0/15
SW4(config-if)#switchport mode access
SW4(config-if)#switchport access vlan 100

SW4(config)#interface FastEthernet0/16
SW4(config-if)#switchport mode access
SW4(config-if)#switchport access vlan 200
```

**Step 2** IPS CLI configuration.

```
sensor login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

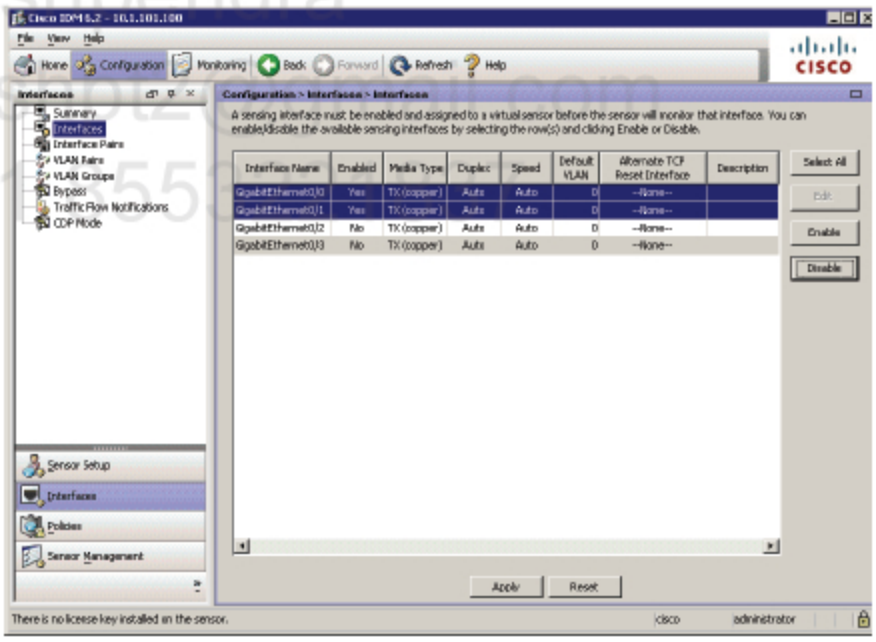
```
***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.


    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Sun Feb  7 20:00:22 2010

Setup Configuration last modified: Sun Feb 07 20:00:00 2010

Enter host name[sensor]: IPS-CCIE
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.101.100/24,10.1.101.10
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.101.200/32
Permit:
Modify system clock settings?[no]:

The following configuration was entered.

service host
network-settings
host-ip 10.1.101.100/24,10.1.101.10
host-name IPS-CCIE
telnet-option disabled
access-list 10.1.101.200/32
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit


[0] Go to the command prompt without saving this config.
```

```
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.

Enter your selection[3]: 2

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.

sensor# exi


IPS-CCIE login:
```

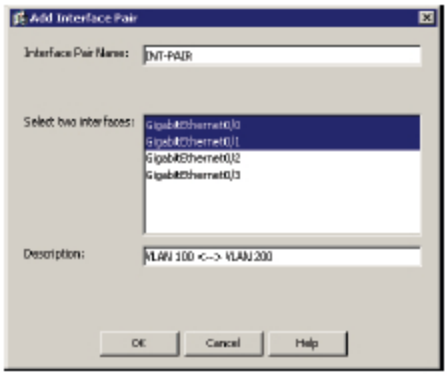
## Step 3 IPS GUI configuration.

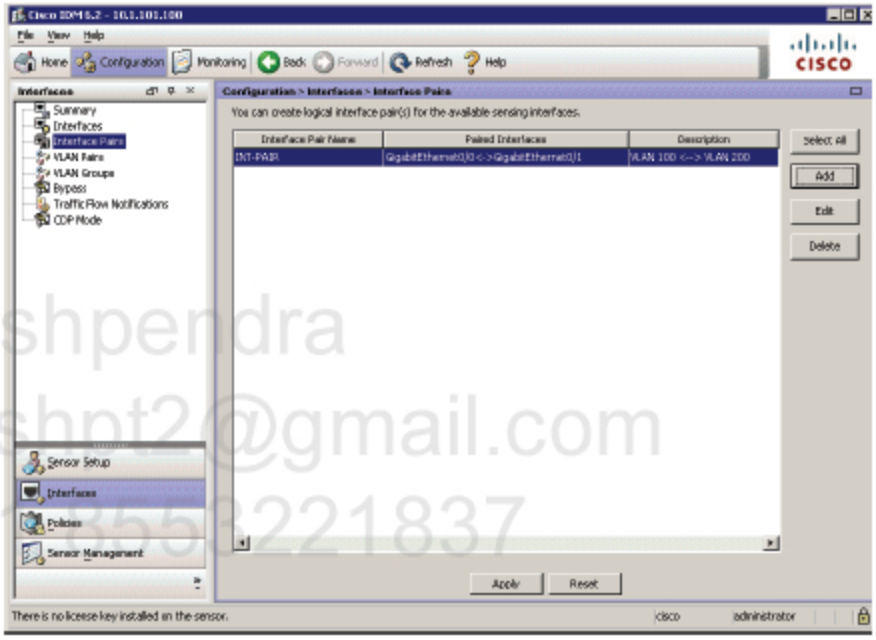
1. ***Go to Configuration → Interfaces → Interfaces, select GigabitEthernet0/0 and GigabitEthernet0/1 interfaces and click Enable button.***





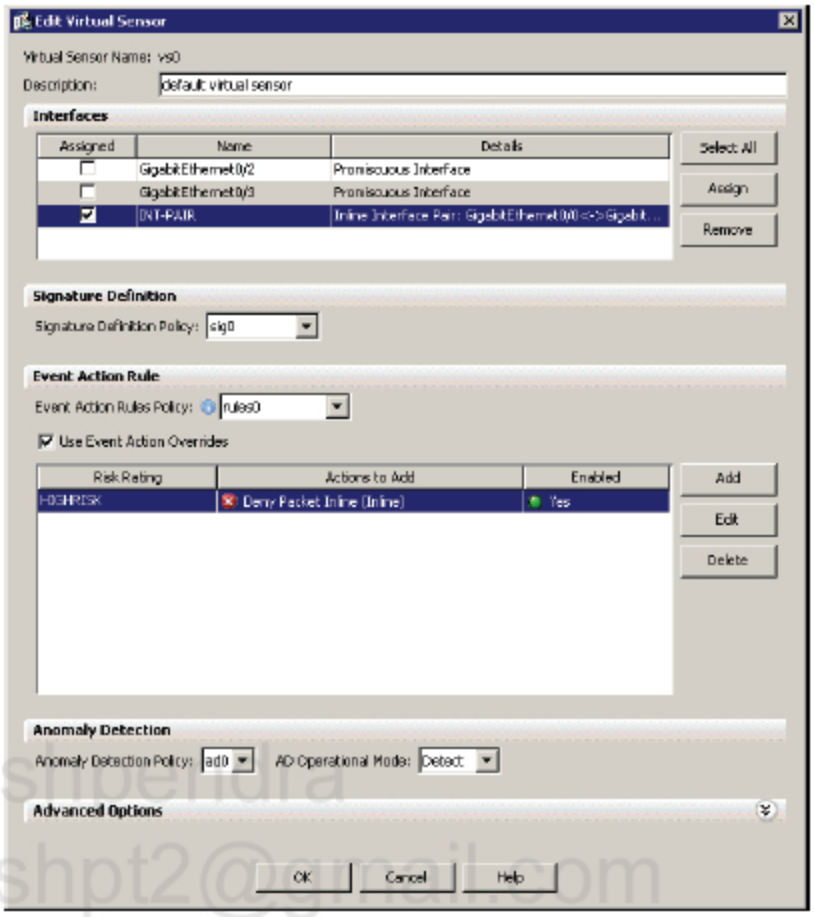

2. ***Go to Configuration → Interfaces → Interface Pairs and click Add. Enter a name for Interface Pair and select G0/0 and G0/1 interface on the list. Click OK.***



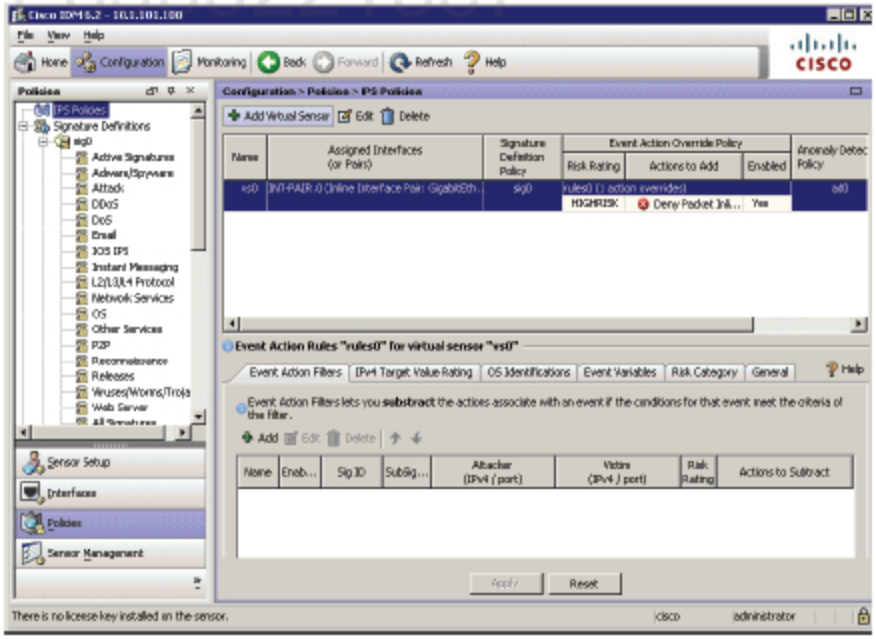






3. ***Go to Configuration → Policies → IPS Policies, select "vs0" virtual sensor on the list and click Edit. Highlight Inline Interface Pair on the list and click Assign button. Then click OK and Apply the changes to the sensor.***

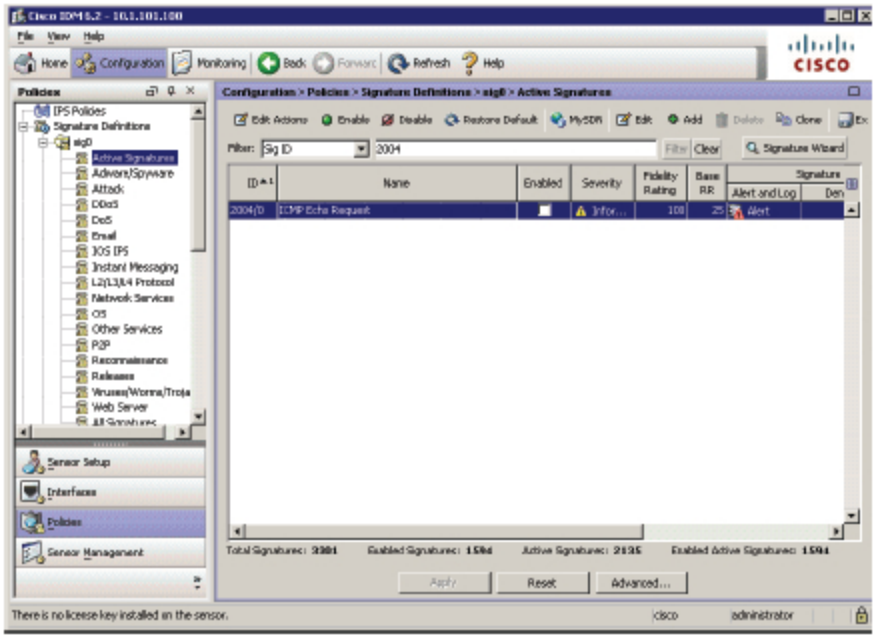




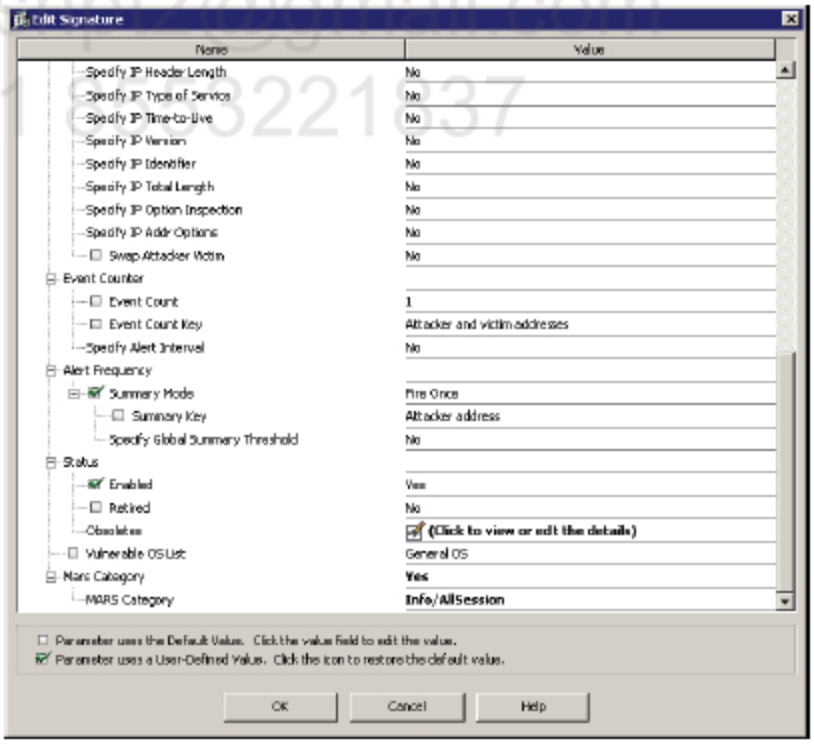

4. ***Go to Configuration → Policies → sig0 → Active Signatures. From Filter drop-down list select Sig ID and enter "2004" string. Then click on Filter button. Highlight the signature ID 2004/0 and click on Enable.***

***Then Apply the changes to the sensor.***






***5. Highlight the signature 2004 on the list and click Edit. Change the Summary Mode to "Fire Once" and click OK.***

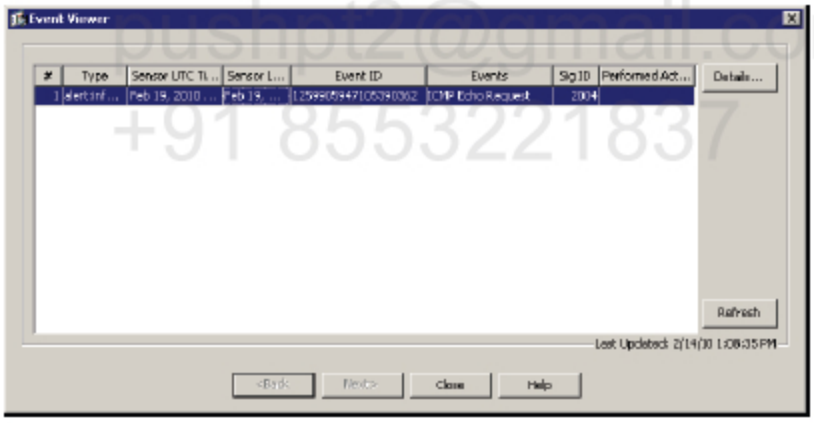


## Verification

```
R1#pi 10.1.12.2 rep 5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms


R1#pi 10.1.12.2 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
R1#
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See that there is only one event for signature ID 2004 on the event list.***






***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259905947105390362  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 19, 2010 21:08:58 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
```

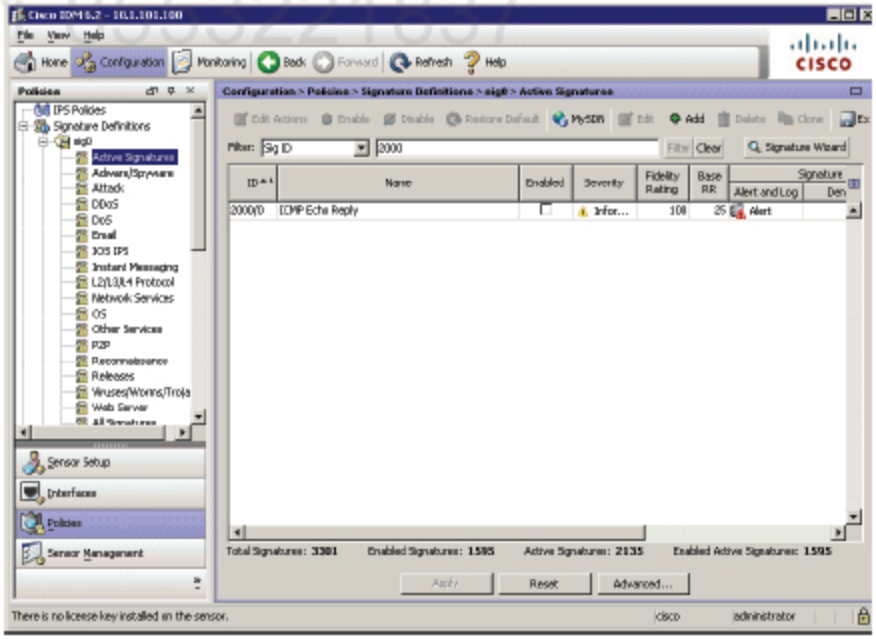
```
vlan: 0
participants:
  attacker:
    addr: 10.1.12.1  locality=OUT
  target:
    addr: 10.1.12.2  locality=OUT
    os:   idSource=unknown  type=unknown  relevance=relevant
riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
threatRatingValue: 35
interface: ge0_0
protocol: icmp
```

## Configuration

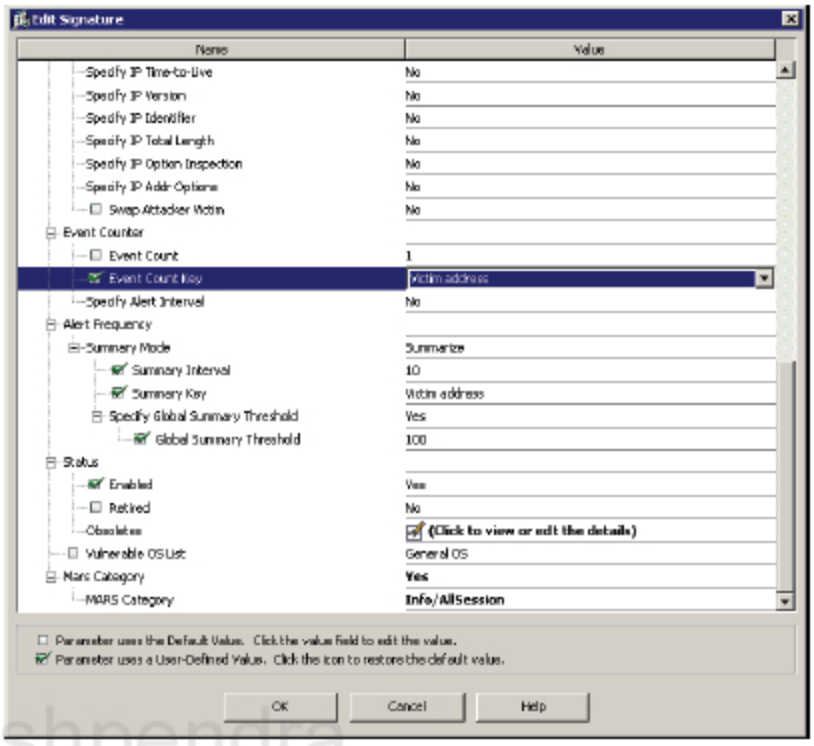
Complete these steps:

**Step 4** IPS GUI configuration.

1. ***Go to Configuration → Policies → sig0 → Active Signatures. From Filter drop-down list select Sig ID and enter "2000" string. Then click on Filter button. Highlight the signature ID 2000/0 and click on Enable. Then Apply the changes to the sensor.***




2. ***Highlight the signature on the list and click Edit. Change Event counter/Event Count Key to "Victim address". Change the settings under Alert Frequency/Summary Mode as follows:***



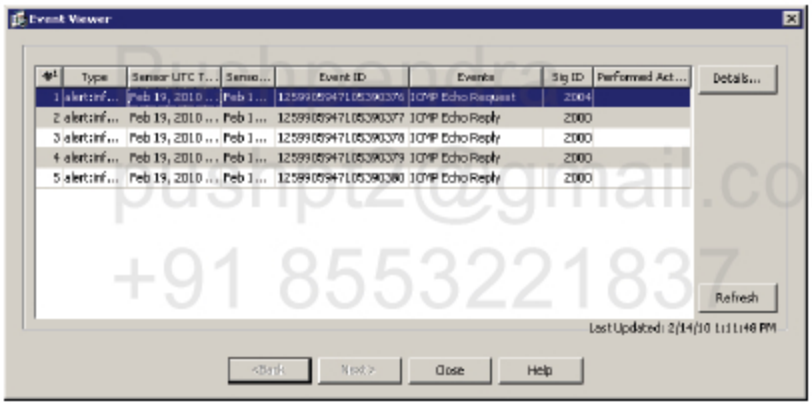



## Verification

```
R1#sh clock
21:13:10.187 UTC Fri Feb 19 2010

R1#pi 10.1.12.2 rep 5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#pi 10.1.12.2 rep 5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#sh clock
21:13:26.203 UTC Fri Feb 19 2010          ← 16 seconds after the first packet

R1#pi 10.1.12.2 rep 5
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#pi 10.1.12.2 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
R1#
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. There is only one event for ICMP Echo Request and four for ICMP Echo Reply..***






**Only one ICMP Echo Request because of Fire Once summary mode:**

```
evIdsAlert: eventId=1259905947105390376  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 19, 2010 21:12:22 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Echo Request  id=2004  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
    target:
```

```
      addr: 10.1.12.2  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_0
  protocol: icmp
```

First ICMP Echo Reply:

```
evIdsAlert: eventId=1259905947105390377  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 19, 2010 21:12:22 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Reply  id=2000  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.2  locality=OUT
    target:
      addr: 10.1.12.1  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_1
  protocol: icmp
```

Summary for first two ping commands (10 packets) because both commands have been entered within 10 seconds Summary Interval. Note that there is only an IP address of the victim. This is because the summary key is set to Victim Address.

```
evIdsAlert: eventId=1259905947105390378  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 19, 2010 21:12:32 UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Reply  id=2000  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
```

```
    attacker:
      addr: 0.0.0.0  locality=OUT
    target:
      addr: 10.1.12.1  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  summary: 10  final=true  initialAlert=1259905947105390377  summaryType=Regular
  alertDetails: Regular Summary: 10 events this interval ;
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_1
  protocol: icmp
```

This is first ICMP Echo Reply packet which has been seen 16 seconds after previous ping commands (Global summary threshold is set to 10 seconds).

```
evIdsAlert: eventId=1259905947105390379  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 19, 2010 21:12:38 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Echo Reply  id=2000  version=S1  type=other
created=20001127
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.2  locality=OUT
    target:
      addr: 10.1.12.1  locality=OUT
      os:   idSource=unknown  type=unknown  relevance=relevant
  riskRatingValue: 35  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 35
  interface: ge0_1
  protocol: icmp
```

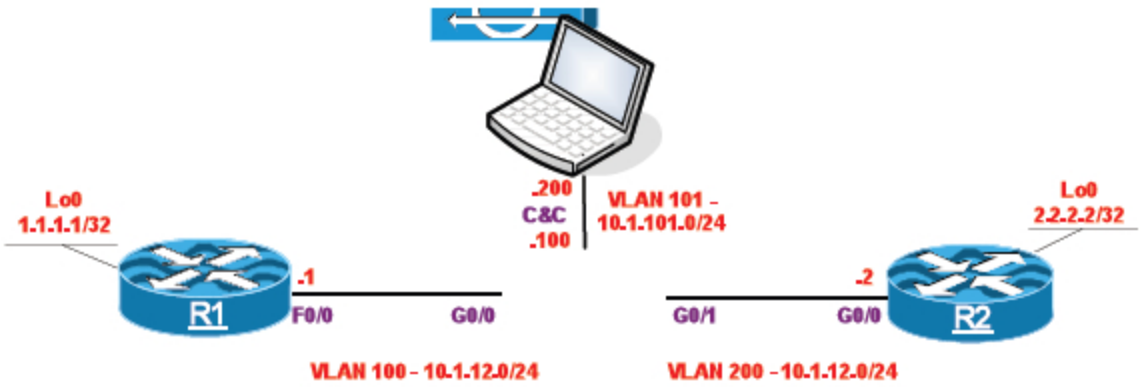
After 10 seconds the IPS starts global summarizing for the signature ID 2000. Hence 5 packets + 100 packets equal 105 ICMP Echo Reply packets summarized. Note that there are no Attacker/Victim IP addresses for Global Summary event.

```
evIdsAlert: eventId=1259905947105390380  vendor=Cisco  severity=informational
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 19, 2010 21:12:48 UTC  offset=0  timeZone=UTC
  signature:  description=ICMP Echo Reply  id=2000  version=S1  type=other
created=20001127
    subsigId: 0
```

```
  marsCategory: Info/AllSession
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 0.0.0.0  locality=OUT
  target:
    addr: 0.0.0.0  locality=OUT
    os:   idSource=unknown  type=unknown  relevance=unknown
summary: 105  final=true  initialAlert=1259905947105390379  summaryType=Global
alertDetails: Global Summary: 105 events this interval ;
riskRatingValue: 25  targetValueRating=medium
threatRatingValue: 25
interface: ge0_1
protocol: icmp
```

# LAB 2.15. Application Inspection and Logging

**This lab is based on the configuration from the previous lab**




## Task 1

Configure deep packets inspection for HTTP so that it blocks CONNECT method used by connections to port TCP/8100 in addition to the standard HTTP ports configured. You may use default signature id of 12678 to accomplish this task. Enable FTP packets inspection as well.



*The AIC engines, AIC HTTP and AIC FTP, provide Layer 4 to Layer 7 packet inspection for HTTP and FTP. By tuning the built-in AIC engine signatures, you can create granular policies for HTTP and FTP. The AIC engines can inspect HTTP traffic when it is received on AIC web ports. If traffic is web traffic but is not received on a designated AIC web port, the SERVICE HTTP engine is executed.*

*To use the AIC engines, you must first enable Application Policy enforcement. Application Policy enforcement is disabled by default for both HTTP and FTP. If you enable Application Policy enforcement for these protocols, the sensor checks to be sure that the traffic is compliant with their respective RFCs. Note that the AIC HTTP engine is a superset of the SERVICE HTTP engine. If enabled, the AIC HTTP engine handles the traditional SERVICE HTTP signatures.*

*AIC FTP Engine Capabilities:*

- *Controls which recognized FTP commands are permitted into the network*
- *Controls whether unrecognized FTP commands are permitted into the network*

*The AIC FTP engine controls the following types of signatures:*

- *Define FTP command: Used to associate an action with a specific FTP command*
- *Unrecognized FTP command: Used to have the sensor take an action when it detects an FTP command that is not recognized*

*AIC HTTP Engine Capabilities:*

- *Enforces RFC compliance*
- *Authorizes and enforces HTTP request methods*
- *Validates response messages*
- *Enforces MIME types*
- *Validates transfer encoding types*
- *Controls content based on message content and type of data being transferred*
- *Enforces URI length*
- *Enforces message size according to policy configured and the header*
- *Enforces tunneling, peer-to-peer, and instant messaging applications*

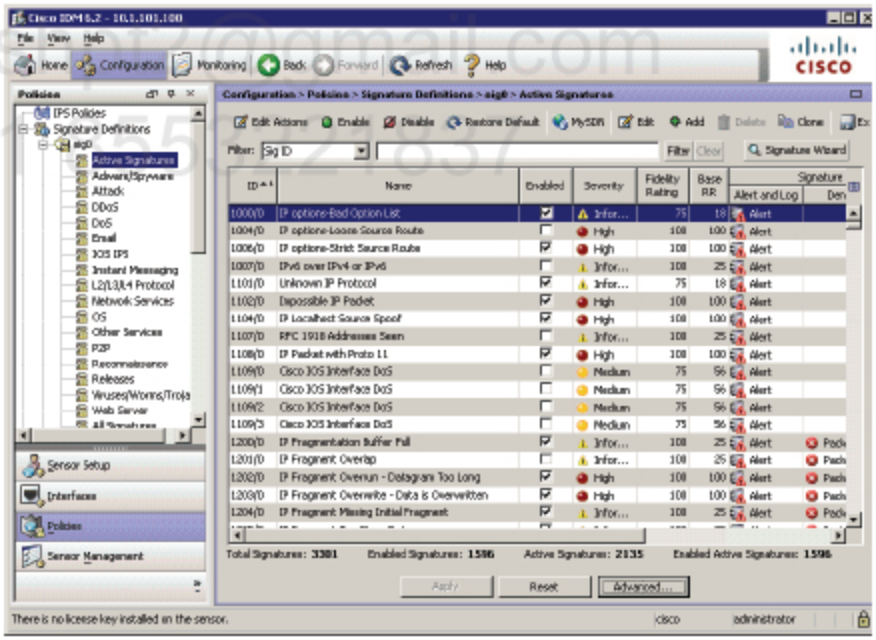
## Configuration

Complete these steps:

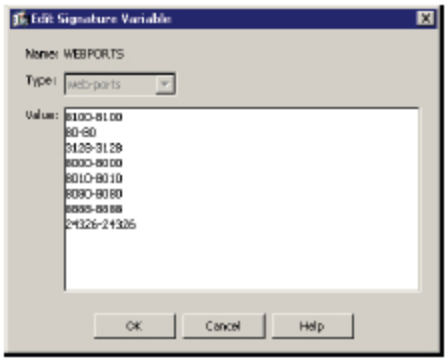
**Step 1** IPS configuration.

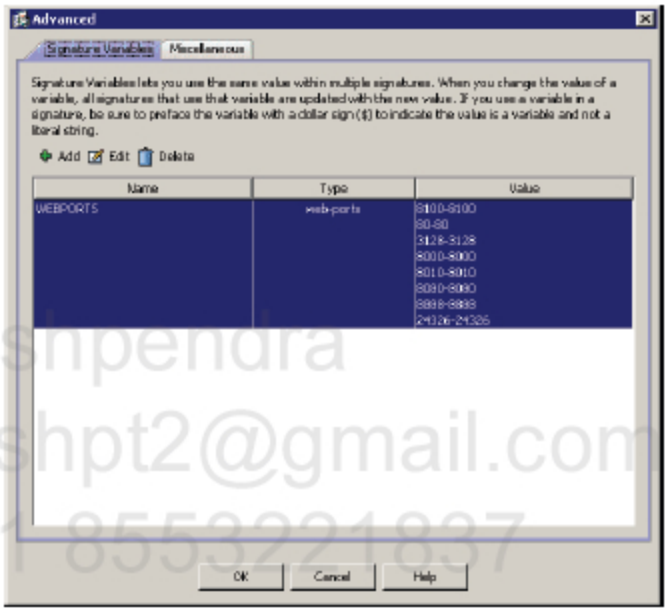
1. ***Go to Configuration → Policies → Signature Definintions → sig0 → Active Signatures → Advanced... → Signature Variables (tab) and click Edit.***





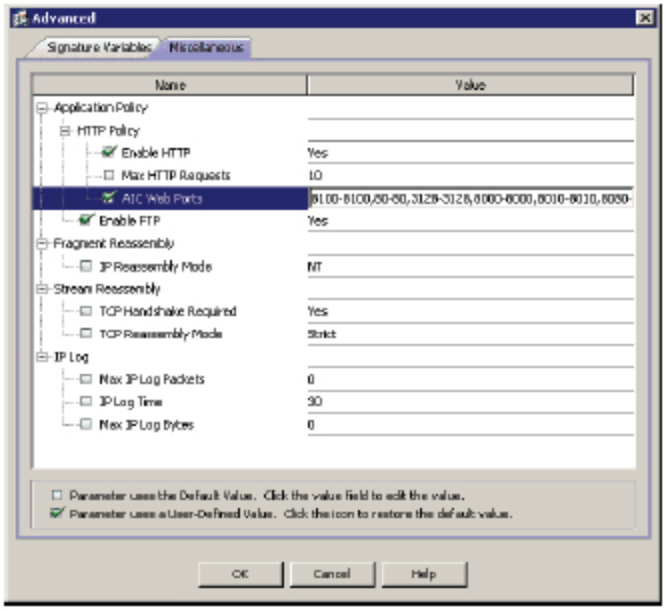

2. ***Add 8100-8100 to the list of ports.***



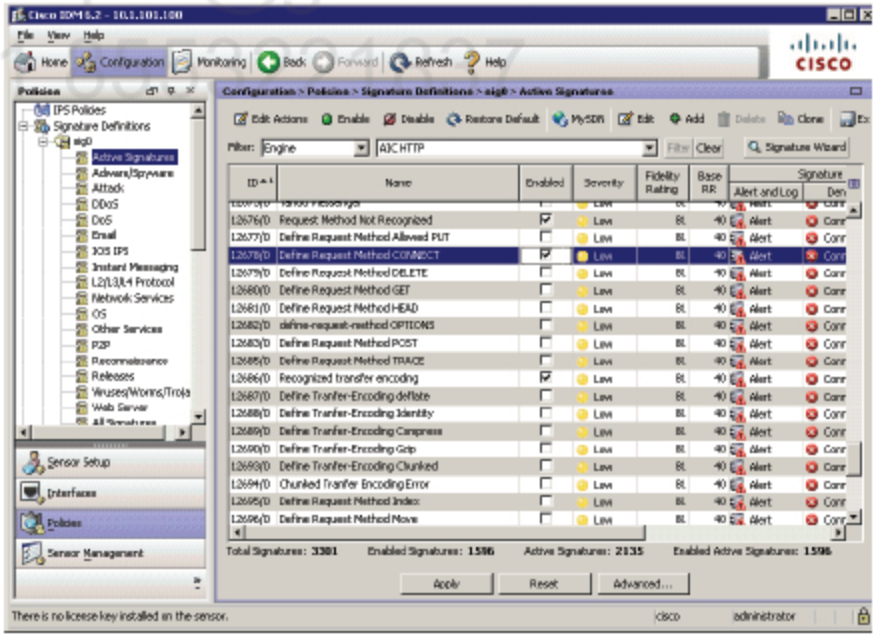



***3. Go to Miscellaneous tab and set "Yes" on Enable FTP option. Click OK.***




4. ***Go to configuration → Policies → Signature Definitions → sig0 → Active Signatures. From Filter drop-down list select "Engine" and "AIC HTTP" from the corresponding drop-down list. Then click on Filter button. Find the signature ID 12678 "Define request Method CONNECT" and enable it.***



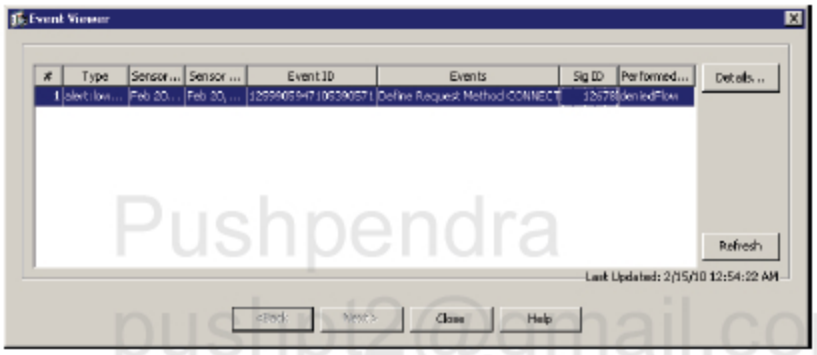



## Verification

***Enable HTTP Server on R2 on port 8100 (to be able to verify the solution).***

```
R2(config)#ip http port 8100
R2(config)#ip http server


R1#tel 10.1.12.2 8100
Trying 10.1.12.2, 8100 ... Open
CONNECT 2.2.2.2:23

<...session freezes...>
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the signature 12678 on the event list.***






***Double click on the event to see more details. Here's the text output for event details.***

```
evIdsAlert: eventId=1259905947105390571  vendor=Cisco  severity=low
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 20, 2010 08:53:46 UTC  offset=0  timeZone=UTC
  signature:  description=Define Request Method CONNECT  id=12678  version=S149
type=other  created=20050304
    subsigId: 0
    sigDetails: Define Request Method CONNECT
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
      port: 49648
    target:
      addr: 10.1.12.2  locality=OUT
      port: 8100
```

```
    os:   idSource=unknown  type=unknown  relevance=relevant
actions:
  deniedFlow: true
riskRatingValue: 50  targetValueRating=medium  attackRelevanceRating=relevant
threatRatingValue: 15
interface: ge0_0
protocol: tcp
```

**Session freezes due to Deny Connection Inline action configured on "Define Request Method CONNECT" signature.**

## Task 2

Configure IPS so that it logs all TELNET sessions (TCP/23) in order to see user passwords and store them in PCAP format on the sensor. Ensure that no more than 100 packets or 100Kb is logged for each session. Packets logging must be finish after 60 seconds. You should create custom signature to accomplish this task.

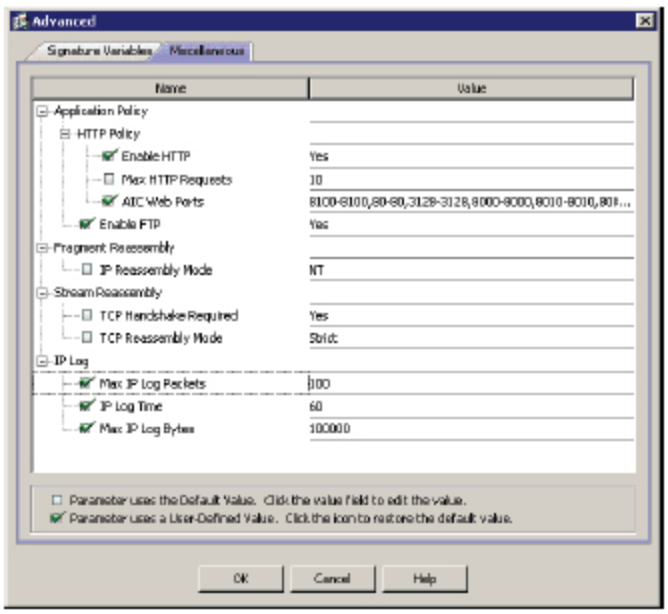


## Configuration

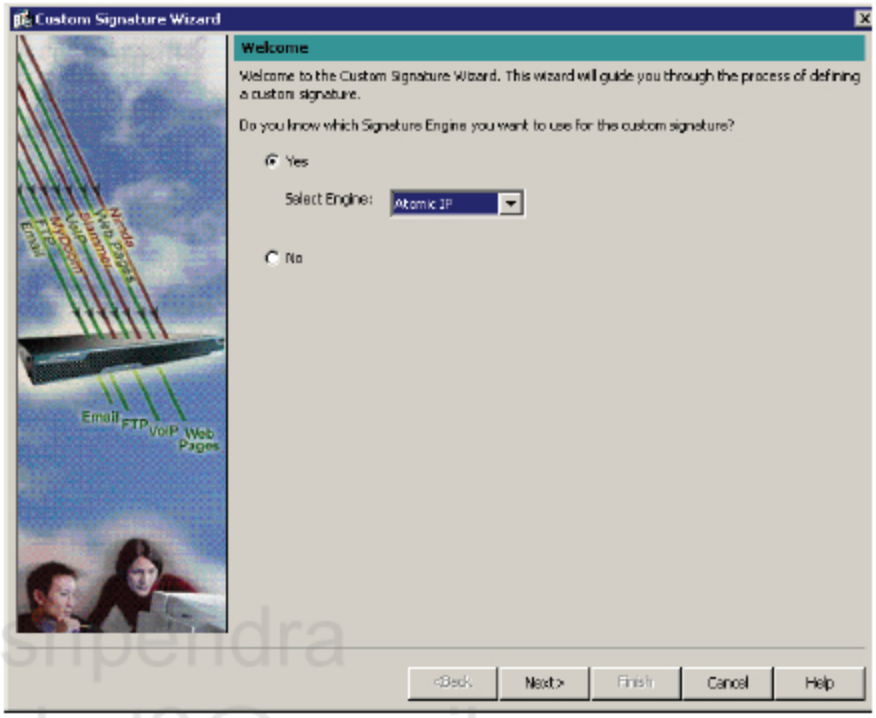
Complete these steps:

**Step 1** IPS configuration.

- ***Go to Configuration → Policies → Signature Definintions → sig0 → Active Signatures → Advanced... → Miscellaneous (tab) and set IP Log settings as follows:***

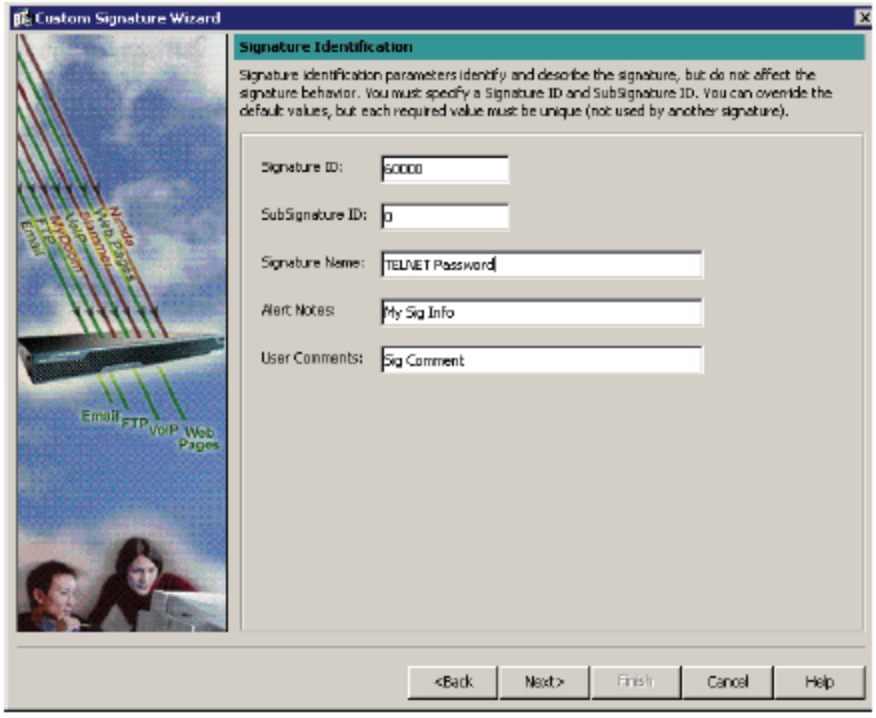


- ***Go to Configuration → Policies → sig0 → Active Signatures and click on Signature Wizard. Select Atomic IP from the drop-down list and click Next.***

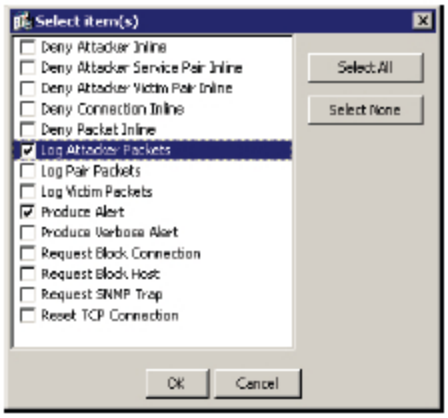




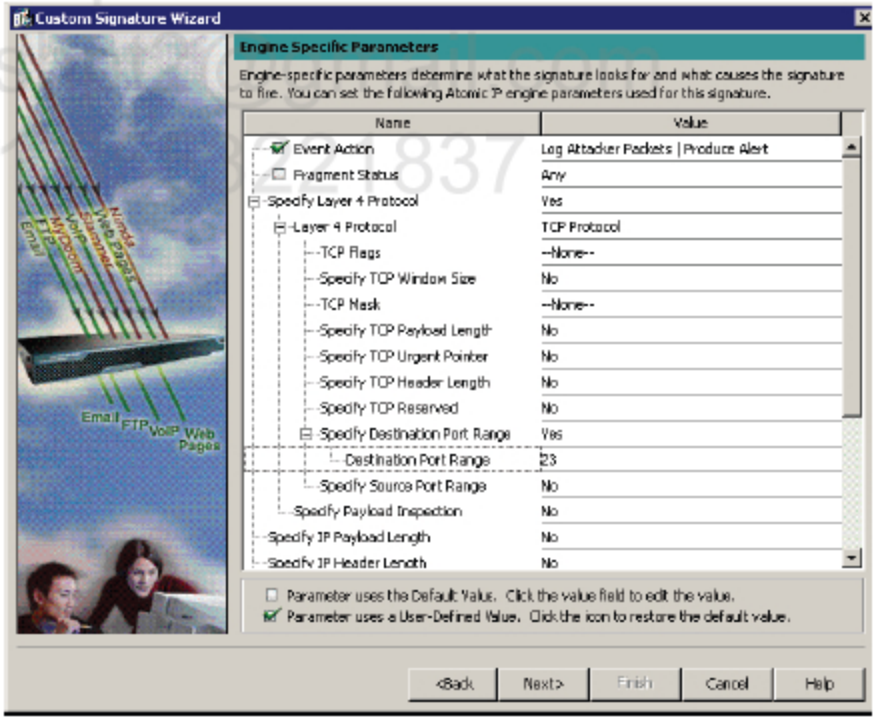

- ***Enter the name for new signature, make some Notes and Comments and click on Next.***



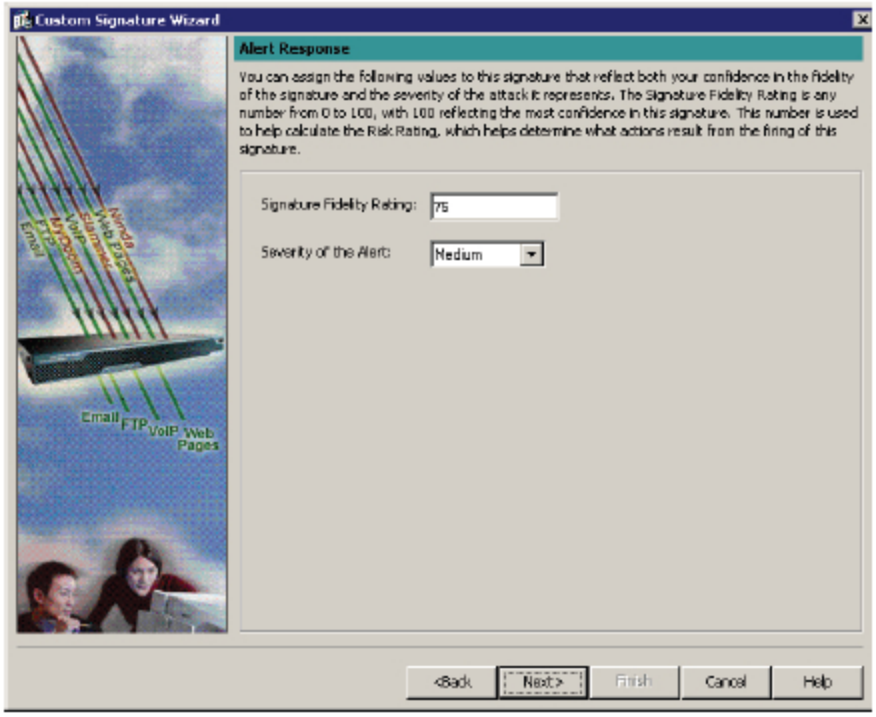
- ***On the Engine Specific Parameters screen, click on Event Action and select Produce Alert and Log Attacker Packets from the list. Then click OK.***




- ***Set Specify Layer 4 Protocol/ Layer 4 Protocol to "TCP Protocol" and port 23 as a Destination Port Range under Specify Layer 4 Protocol/Layer 4 Protocol/Specify Destination Port Range. Click Next.***

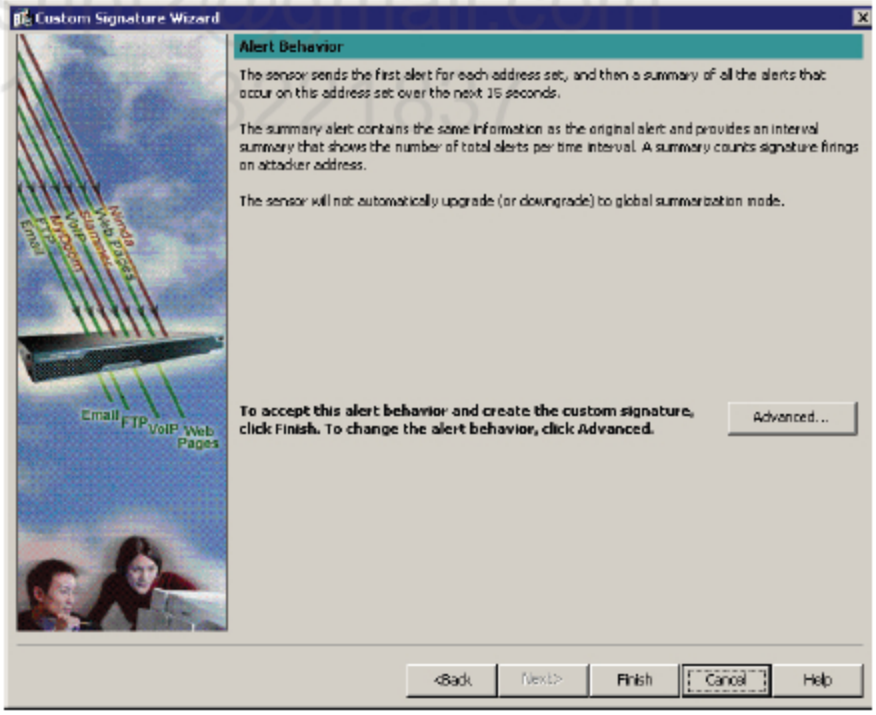



- ***Set Signature Fidelity Rating to 75 and Action Severity to Medium. Click Next.***





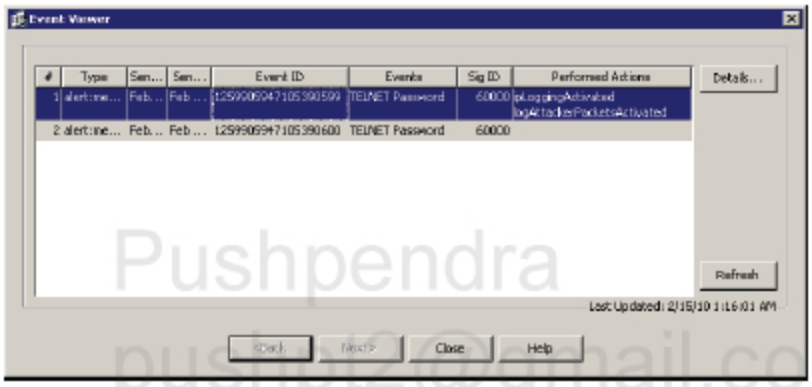

- ***Leave default settings for Alert Behavior and click Finish to close the wizard.***



## Verification

```
R1#telnet 10.1.12.2
Trying 10.1.12.2 ... Open


Password:

R2>
```

***Go to Monitoring → Events, check Show past events radio button and select 5 minutes. Then click on View button. See the newly created signature on the event list.***



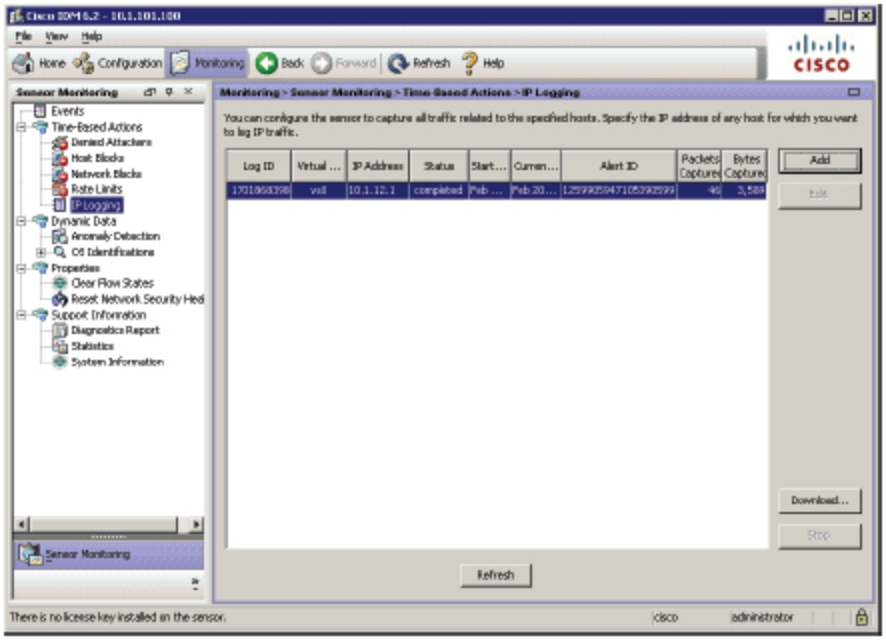



```
evIdsAlert: eventId=1259905947105390599  vendor=Cisco  severity=medium
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 20, 2010 09:16:41 UTC  offset=0  timeZone=UTC
  signature:   description=TELNET Password  id=60000  version=custom  type=other
created=20000101
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
      port: 38652
    target:
      addr: 10.1.12.2  locality=OUT
      port: 23
      os:   idSource=unknown  type=unknown  relevance=relevant
  actions:
    ipLoggingActivated: true
    logAttackerPacketsActivated: true
```

```
  ipLogIds:
    ipLogId: 1701868398
  riskRatingValue: 66  targetValueRating=medium  attackRelevanceRating=relevant
  threatRatingValue: 66
  interface: ge0_0
  protocol: tcp


evIdsAlert: eventId=1259905947105390600  vendor=Cisco  severity=medium
  originator:
    hostId: IPS-CCIE
    appName: sensorApp
    appInstanceId: 386
  time: Feb 20, 2010 09:16:56 UTC  offset=0  timeZone=UTC
  signature:   description=TELNET Password  id=60000  version=custom  type=other
created=20000101
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: 10.1.12.1  locality=OUT
      port: 0
    target:
      addr: 0.0.0.0  locality=OUT
      port: 0
      os:   idSource=unknown  type=unknown  relevance=unknown
  summary: 23  final=true  initialAlert=1259905947105390599  summaryType=Regular
  alertDetails: Regular Summary: 23 events this interval ;
  riskRatingValue: 56  targetValueRating=medium
  threatRatingValue: 56
  interface: ge0_0
  protocol: tcp
```



***Go to Monitoring → Sensor Monitoring → Time-Based Actions → IP Logging and check if there is a capture file associated with our custom signature.***




**You can download the capture file using Download... button and open it with Wireshark.**

**This page is intentionally left blank.**

# Advanced
# CCIE SECURITY v4
# LAB WORKBOOK



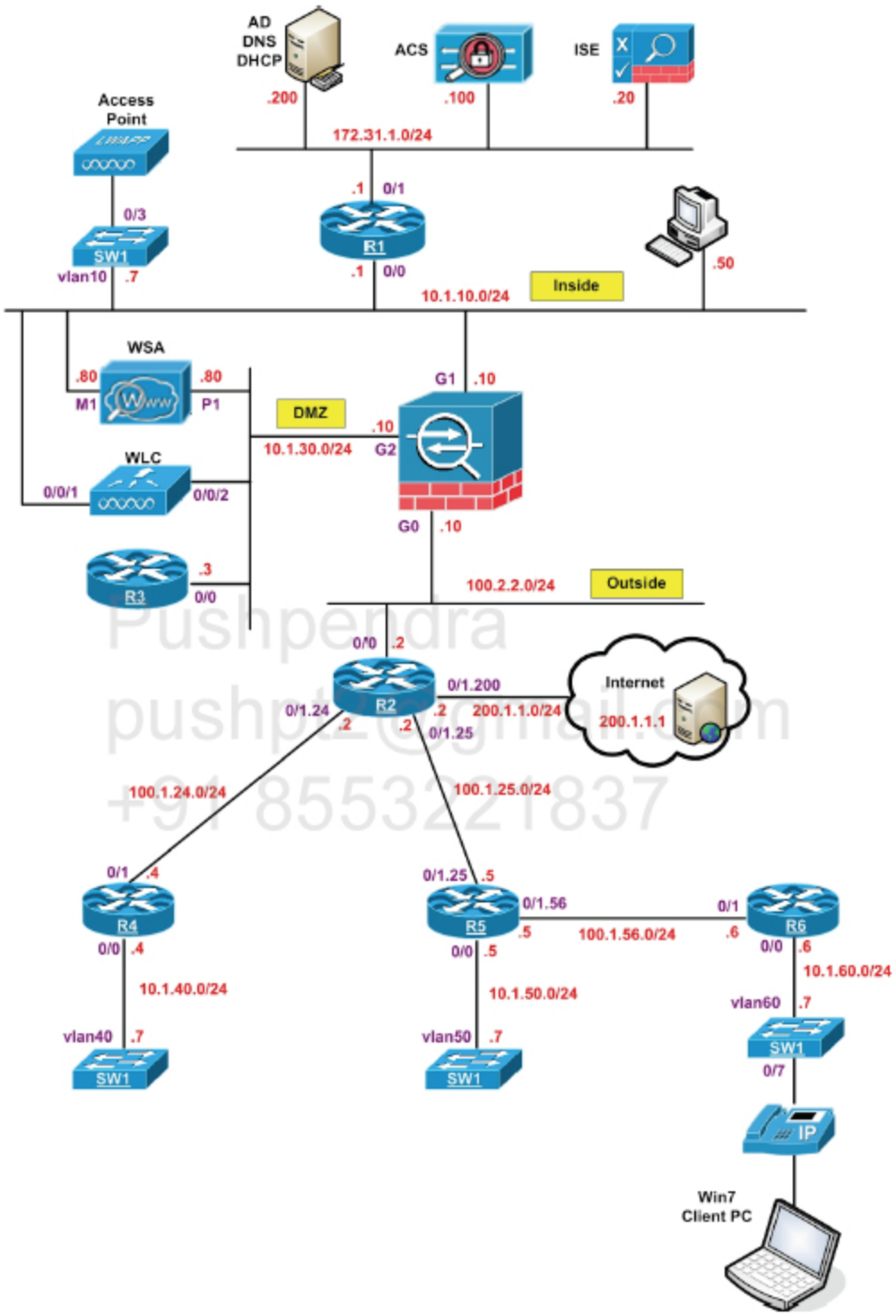
# Content Security
# WSA

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

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

www.MicronicsTraining.com

# Logical Topology for WSA labs






WSA is connected to the network using two interfaces:

- P1 – data interface, placed in VLAN 30 (ASA DMZ)
- M1 – management interface, placed in VLAN 10 (ASA Inside)

Management access to WSA should be allowed from WinXP PC (10.1.10.50).

# LAB 2.16. WSA bootstrapping (optional)

## Objectives

This lab shows how to pre-configure Cisco Web Security Appliance from CLI and GUI.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |



## Task

Perform WSA installation and bootstrapping. Provide the following information during the installation process:

- Hostname: wsa.micronics.local
- Interfaces:

| Interface | IP address & mask | Hostname | Default gateway |
|---|---|---|---|
| M1 | 10.1.10.80/24 | wsa.micronics.local | 10.1.10.1 |
| P1 | 10.1.30.80/24 | proxy.micronics.local | 10.1.30.10 |

- Management access: HTTP/8080, HTTPS/8443, SSH/22
- Separate routing table for management and data
- Nameserver: 8.8.8.8
- NTP server and timezone: default
- Explicit proxy mode
- Administrative user: admin/ironport; email: admin@micronics.local

Configure Win7 PC to use explicit proxy mode in its IE configuration.

## Configuration

Complete these steps:

**Step 1** Log into the WSA console (if you have access to it) or SSH to it. Run **interfaceconfig** command.

```
ironport.example.com> interfaceconfig


Currently configured interfaces:
1. Management (10.1.10.102/24 on Management:
ironport.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP Address (Ex: 192.168.1.2):
[10.1.10.102]> 10.1.10.80

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[0xffffff00]> 255.255.255.0

Hostname:
[ironport.example.com]> wsa.micronics.local

Do you want to enable FTP on this interface? [Y]> n

Do you want to enable SSH on this interface? [Y]> <enter>

Which port do you want to use for SSH?
[22]> <enter>

Do you want to enable HTTP on this interface? [Y]> <enter>

Which port do you want to use for HTTP?
[8080]> <enter>

Do you want to enable HTTPS on this interface? [Y]> <enter>
```

```
Which port do you want to use for HTTPS?
[8443]> <enter>

You have not entered an HTTPS certificate.  To assure privacy,
run "certconfig" first.  You may use the demo, but this will
not be secure.
Do you really wish to use a demo certificate? [Y]> <enter>

Both HTTP and HTTPS are enabled for this interface, should HTTP
requests redirect to the secure service? [Y]> <enter>

You have edited the interface you are currently logged into.
Are you sure you want to change it? [Y]> <enter>


Currently configured interfaces:
1. Management (10.1.10.80/24 on Management:
wsa.micronics.local)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]><enter>

Please run System Setup Wizard at http://10.1.10.80:8080
ironport.example.com> commit

Warning: In order to process these changes, the
proxy process will restart after Commit. This will cause
a brief interruption in service. Additionally, the
authentication cache will be cleared, which might require
some users to authenticate again.

Please enter some comments describing your changes:
[]><enter>
```



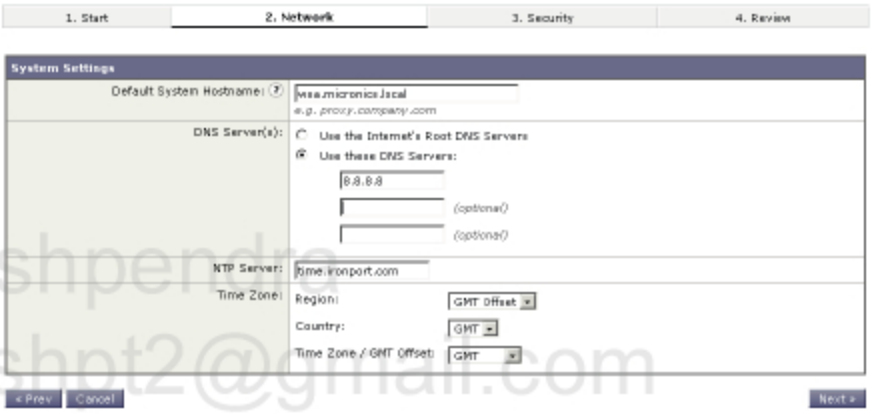
If you're connected through SSH and you've changed IP address then you'll get disconnected. You must reconnect to the new IP address.

**Step 2** Configure WSA using GUI.

- Using web browser, connect to http://wsa.micronics.local:8080 or (preferred) https://wsa.micronics.local:8443 and authenticated using

default **admin/ironport** credentials.

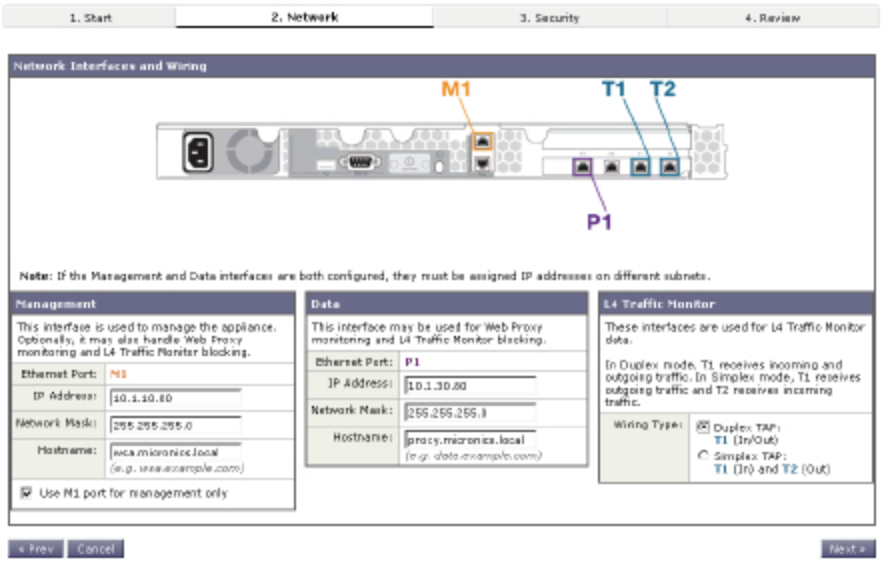

- Run setup wizard at **System Administration > System Setup Wizard**. Provide **Default System Hostname** and **DNS Server**. Leave **NTP Server** and **Time Zone** untouched. Click **Next**.






- Then the configuraton wizard is asking for upstream proxy. There is no upstream proxy in our lab. Click **Next**.

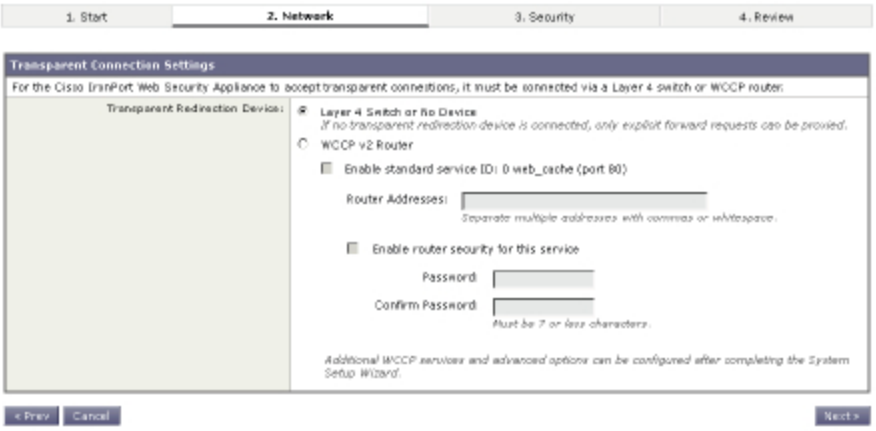

- On **Network Interfaces and Wiring** screen provide correct IP addresses for both **M1** and **P1** interfaces. Pick **Use M1 port for management only** checkbox and click **Next**.



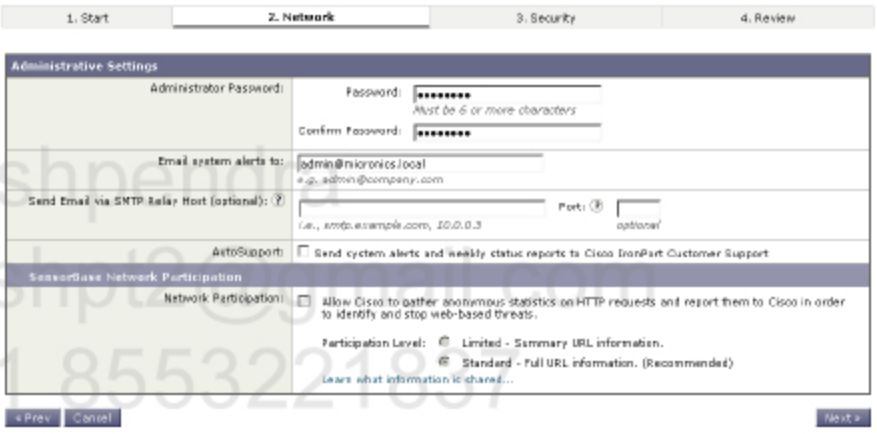

- There are two separate routing tables if 'Use M1 port for management only' checkbox was selected on the previous screen. Configure two different default gateways.




- On **Transparent Connection Settings** screen leave default option. This will allow us to use either 'transparent proxy' or 'explicit proxy' deployments.

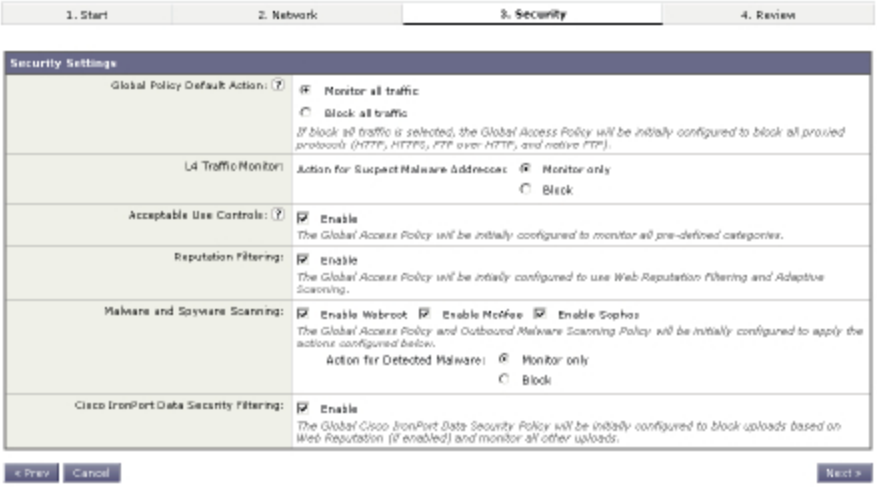



- **If required provide new password for administrator and admin email address. Do not participate in SensorBase and AutoSupport.**

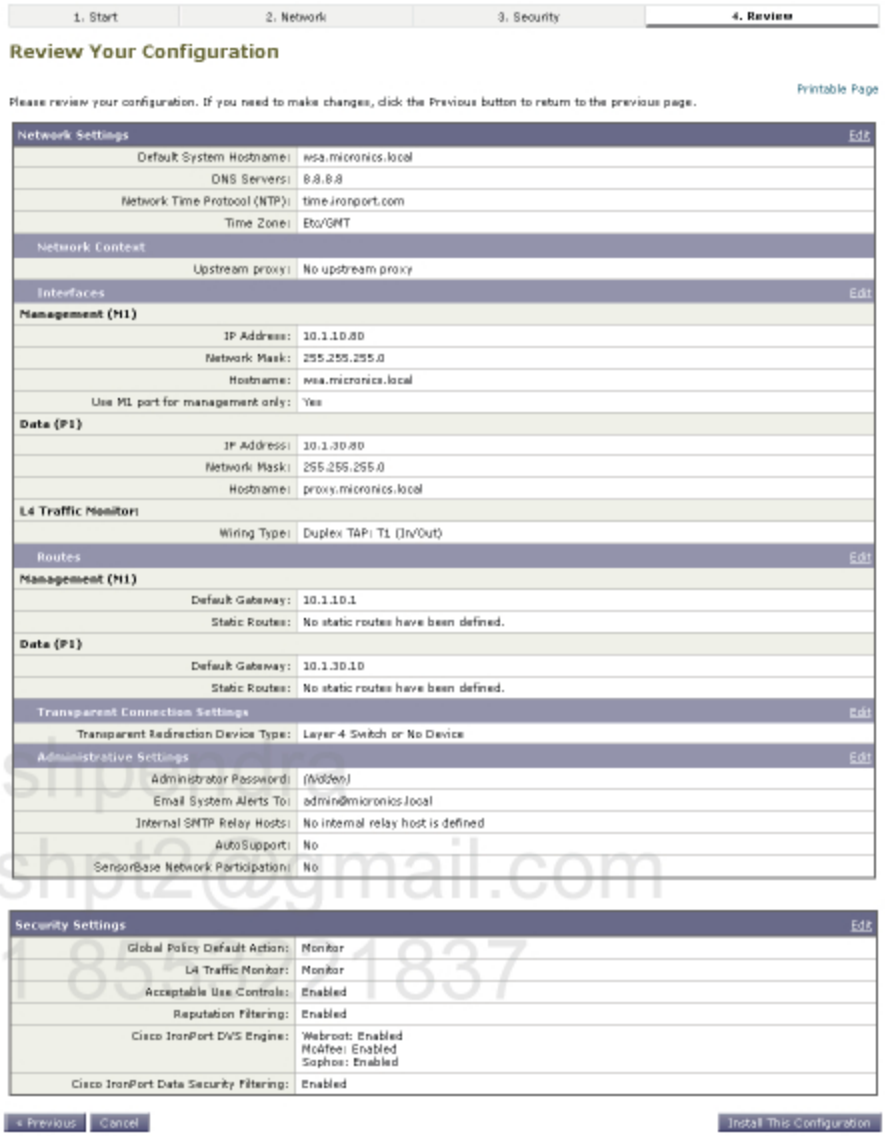





- **On Security Settings screen leave all options default. Click Next.**




**Review the configuration and click Install This Configuration.**



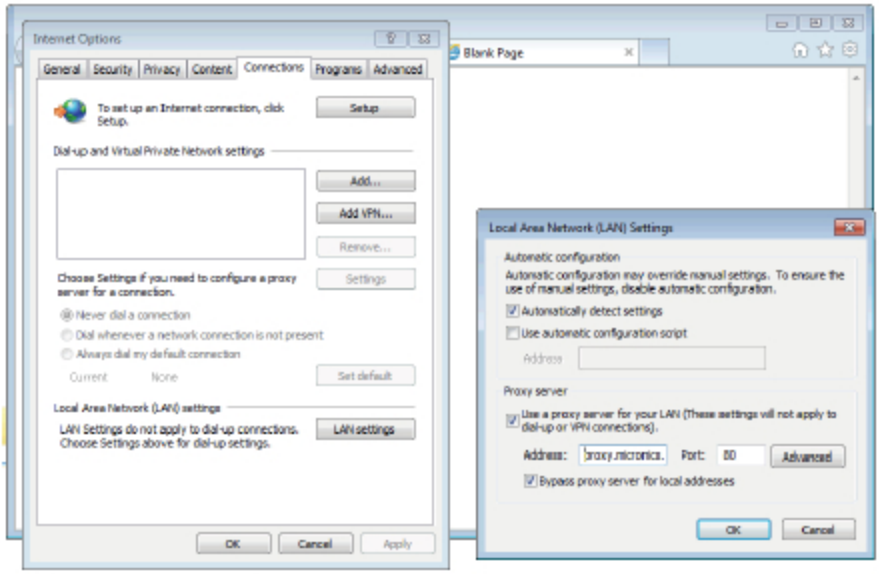



- After a while the following screen should appear. This may fail if you changed management IP address during the configuration wizard.


## Step 3 Win7 client configuration.

- Open up web browser and go to **Tools > Internet Options >**

**Connections > LAN Settings** and enter **proxy.micronics.local** in the **Address** field. Use port **80** and **Bypass proxy server for local addresses**.






## Verification

```
// This lab does not include ASA firewall configuration. It is
assumed in this lab that ASA permits all the traffic.
```

Connect to WSA and go to **System Administration > Policy Trace**. Enter URL www.google.com and Client IP address **10.1.10.104** and hit **Find Policy Match**. If you see something similar to the output below – this means WSA works fine.

### Policy Trace

**Destination**

URL: www.google.com

**Transaction**

*All fields below are optional.*

Client IP Address: 10.1.10.104

User: *No Authentication Realms are defined.*

▸ Advanced

Find Policy Match

**Results**

**User Information**

User Name: None
Group Membership: None
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:17.0) Gecko/20100101 Firefox/17.0

**URL Check**

WBRS Score: 8.4
URL Category: Search Engines and Portals
Scanner "Webroot" Verdict (Request): Unknown
Scanner "AVC" Verdict (Request): Google (Search Engine)
MIME-Type: text/html; charset=UTF-8
Scanner "AVC" Verdict (Response): Google (Search Engine)
Adaptive Scanning Verdict (Response): Unknown
Scanner "McAfee" Verdict (Response): Unknown
Scanner "Sophos" Verdict (Response): Unknown

**Policy Match**

Cisco IronPort Data Security policy: None
Decryption policy: None
Routing policy: Global Routing Policy
Identity policy: Global Identity Policy
Access policy: Global Access Policy

**Final Result**

**Request completed**

Details: Transaction permitted

Trace session complete



Go to the Win7 client PC and try to connect to www.google.com. The connection should be successful.

# LAB 2.17. DNS and routing configration

## Objectives

This lab shows how to configure advanced DNS settings on WSA.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |



## Task

Configure WSA so that it resolves FQDNs against public DNS Server at 8.8.8.8 using its P1 interface. The domain 'micronics.com' must be resolved using DNS Server at 172.31.1.200.

The base ASA firewall configuration is as follows:

```
!
object network INSIDENET
 subnet 10.1.10.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
object network WSA
 host 10.1.30.80
 nat (dmz,outside) static 100.2.2.80
!
```

```
access-list DMZ_IN extended permit icmp any any
access-list OUTSIDE_IN extended permit icmp any any
access-group OUTSIDE_IN in interface outside
access-group DMZ_IN in interface dmz
!
route outside 0.0.0.0 0.0.0.0 100.2.2.2
route inside 172.31.1.0 255.255.255.0 10.1.10.1
!
```

Ensure that WSA is performing DNS resolution and is able to access hosts on the Internet with HTTP and HTTPS.

## Configuration

Complete these steps:

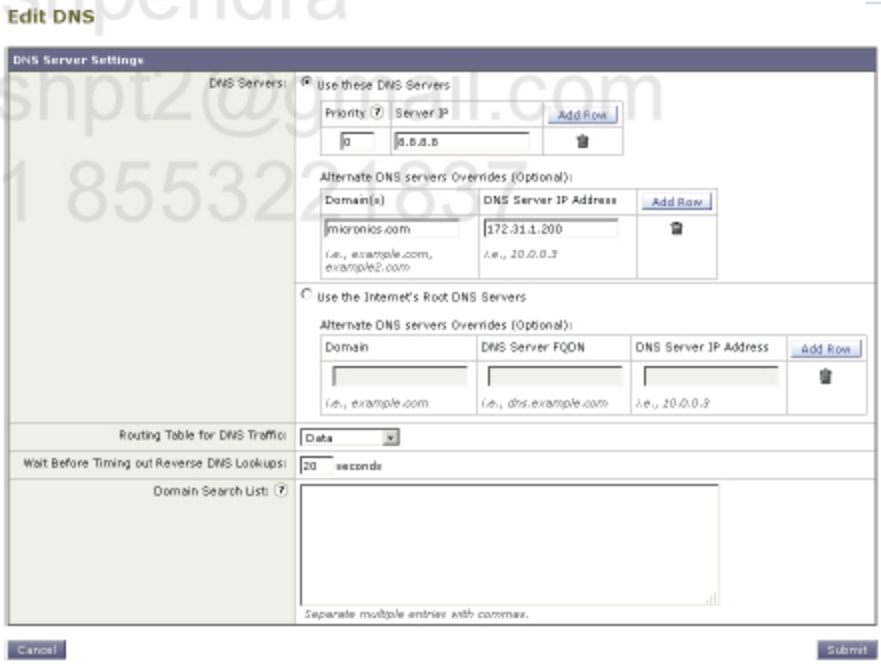
**Step 1** ASA firewall configuration.

```
!
access-list DMZ_IN permit udp host 10.1.30.80 host 8.8.8.8 eq
53
access-list DMZ_IN permit udp host 10.1.30.80 host 172.31.1.200
eq 53
access-list DMZ_IN permit tcp host 10.1.30.80 any eq 443
access-list DMZ_IN permit tcp host 10.1.30.80 any eq 80
!
```

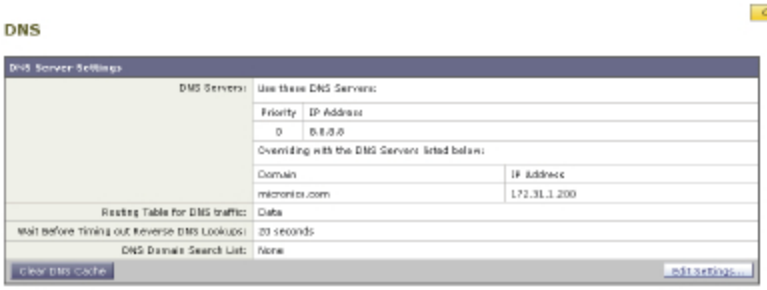
**Step 2** Configure WSA using GUI.

- Go to **Network > DNS** configurationand click **Edit Settings...** Enter **micronics.com** domain name and **172.31.1.200** as **DNS Server IP Address**. From **Routing Table for DNS Traffic** drop-down list select **DATA**. Click **Submit**.



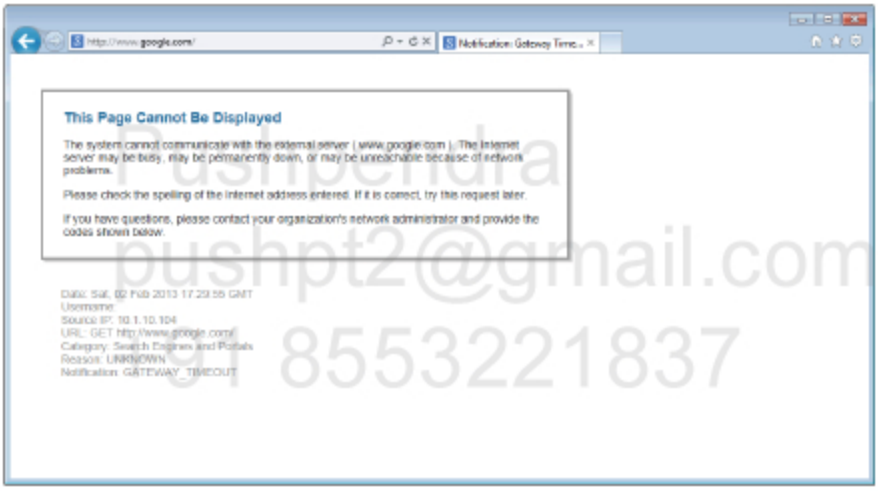



- Click **Commit Changes >**. Enter some description for the change and click **Commit Changes** button.




## Verification

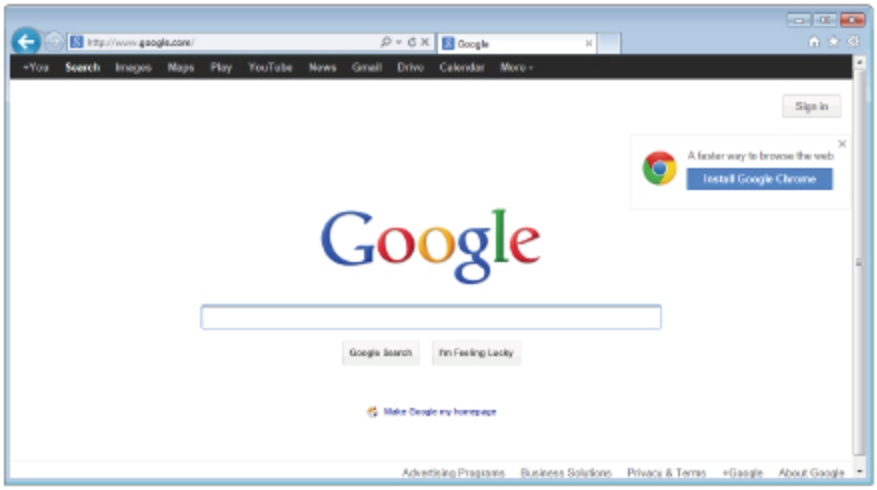
Before ASA configuration it was not possible to resolve FQDN as udp/53 traffic was blocked by DMZ_IN interface ACL. The message in the client's web browser is as follows:



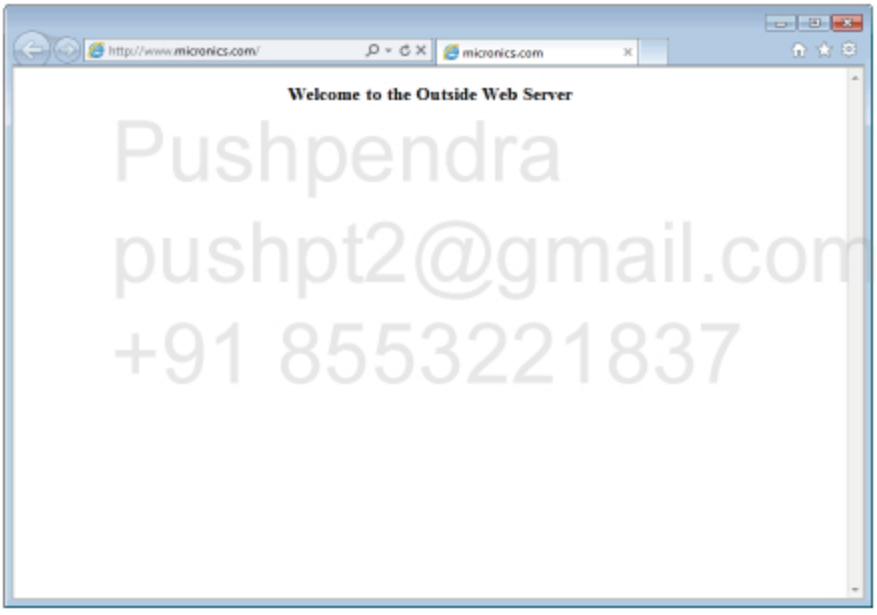



After ASA and WSA configuration check if you can go to the Internet and also to the Internal website.

Internet host resolved by the public DNS




Host resolved by the private DNS.






Check DNS functionality from CLI:

```
wsa.micronics.local> ping

Which interface do you want to send the pings from?
1. Auto
2. Management (10.1.10.80/24: wsa.micronics.local)
3. P1 (10.1.30.80/24: proxy.micronics.local)
[1]> 3

Please enter the host you wish to ping.
[]> www.micronics.com
```

```
Press Ctrl-C to stop.
PING www.micronics.com (200.1.1.1) from 10.1.30.80: 56 data bytes
64 bytes from 200.1.1.1: icmp_seq=0 ttl=127 time=1.590 ms
64 bytes from 200.1.1.1: icmp_seq=1 ttl=127 time=50.220 ms
64 bytes from 200.1.1.1: icmp_seq=2 ttl=127 time=4.046 ms
^C
--- www.micronics.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.590/18.619/50.220/22.368 ms
```

# LAB 2.18. WSA Identities and Access Policies

## Objectives

This lab shows how to use WSA identities and access policies.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |



## Task

Configure the following access policy to allow access to websites:

| From (Identity) | What (URL categories) | When (Time Ranges) |
|---|---|---|
| **10.1.10.104 (Win7 PC)** | Business and Industry | Mon-Fri: 9am – 6pm |
| | Computer Security | |
| | Computers and Internet | |
| | Education | |
| **Any** | Gambilng | Mon-Fri: 6pm – 8am |
| | Shopping | Sat-Sun: all day |

Traffic to uncategorized URLs should be allowed all the time.

## Configuration

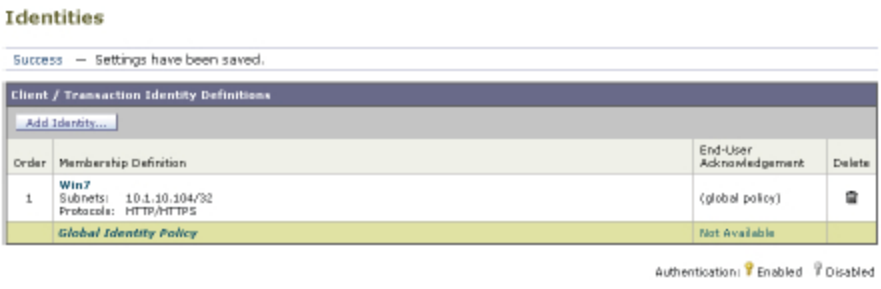
Complete these steps:

**Step 1** Add Identity.

- Go to **Web Security Manager > Identities** and click **Add Identity…** Enter a name for identity e.g. **Win7** and specify subnet/host IP address. Click **Submit.**

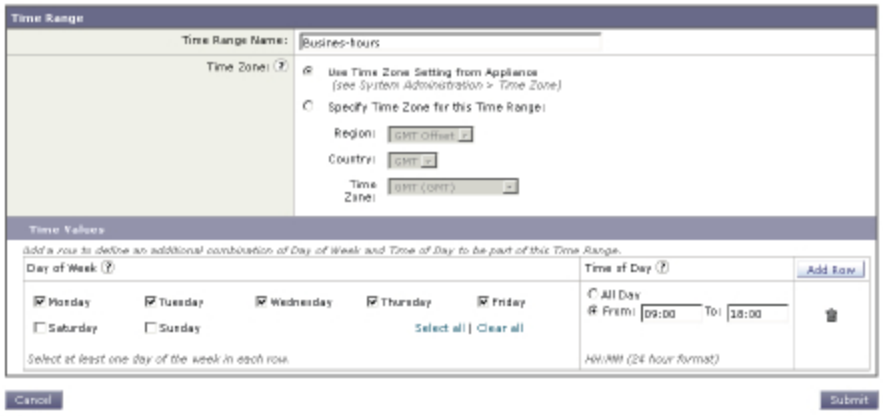



- The new identity is on the list. Click **Commit Changes** or go to next step.



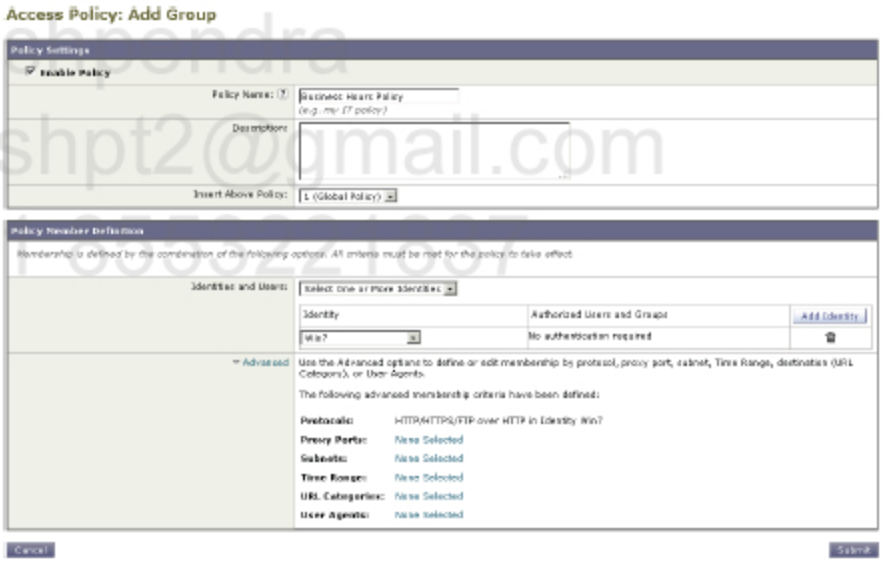

**Step 2** Add Time Range.

- Go to **Web Security Manager > Definied Time Ranges** and click **Add Time Range…** Enter a name for time range e.g. **Business-hours** and pick Monday-Friday with 9:00-18:00 timerange. Click **Submit**.

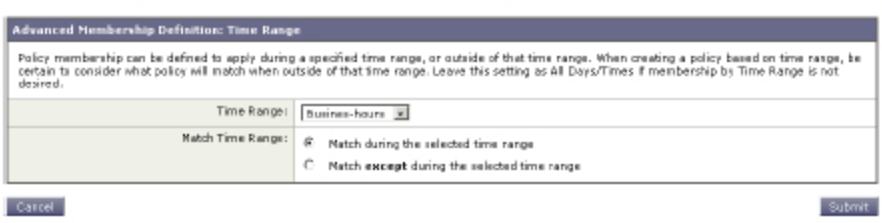



**Step 3** Add Access Policy for business hours.

- Go to **Web Security Manager > Access Policies** and click **Add Policy…** Enter a name for new policy e.g. **Business Hours Policy**, select **Win7** identity and click **None Selected** link next to **Time Range**.




- Pick **Business-hours** time range object and select **Match during the selected time range** option. Click **Submit**.



- Click **None Selected** link next to **URL Categories** and pick the following categories on the list:
    - Business and Industry
    - Computer Security
    - Computers and Internet
    - Education

  Click **Submit**.

**Access Policies: Policy "Business Hours Policy": Membership by URL Categories**

**Advanced Membership Definition: URL Category**

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

**Custom URL Categories**

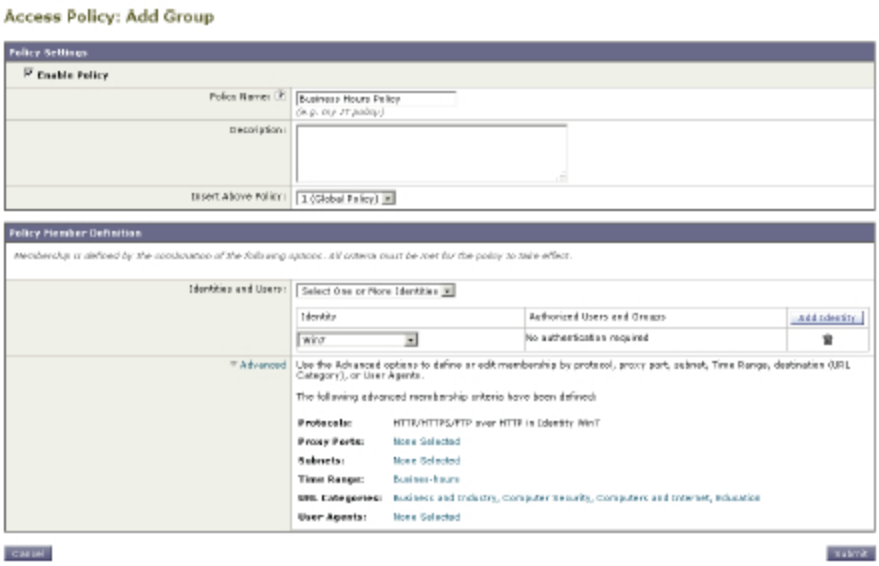
*No Custom Categories are defined. See Web Security Manager > Custom URL Categories.*

**Predefined URL Categories**

| Category | Add<br>Select all |
|---|---|
| Adult | |
| Advertisements | |
| Alcohol | |
| Arts | |
| Astrology | |
| Auctions | |
| Business and Industry | ✓ |
| Chat and Instant Messaging | |
| Cheating and Plagiarism | |
| Child Abuse Content | |
| Computer Security | ✓ |
| Computers and Internet | ✓ |
| Dating | |
| Digital Postcards | |
| Dining and Drinking | |
| Dynamic and Residential | |
| Education | ✓ |
| Entertainment | |



- Review all options selected and click **Submit**.



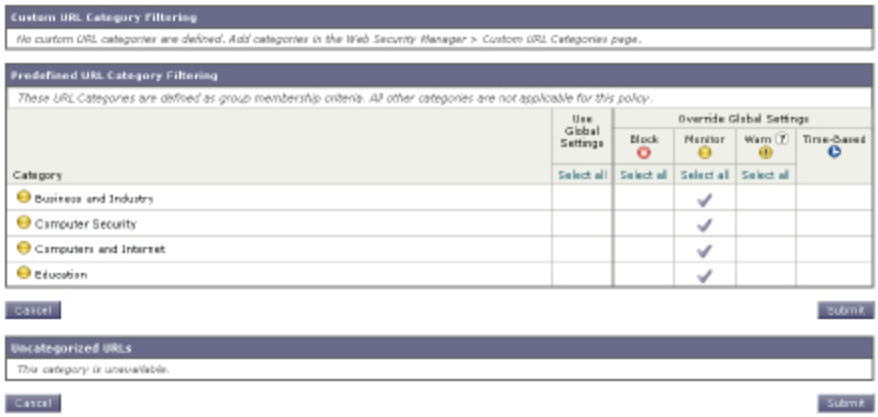

**// The new access policy is added to the list. There are 4 URL categories being monitored. This option is inherited from Global Policy. If we want to really allow those categories but not allow other categories we must change Global Policy to block all categories on the list. This will automatically be inherited by our new policy – hence won't work. We must go to our new policy and statically enable monitoring for 4 URL categories and then go to the Global Policy and explicitly block all categories.**



- Click on **Monitor: 4** in **URL Filtering** column to edit URL filtering policy.


- Click **Select All** in **Monitor** column. Click **Submit**.

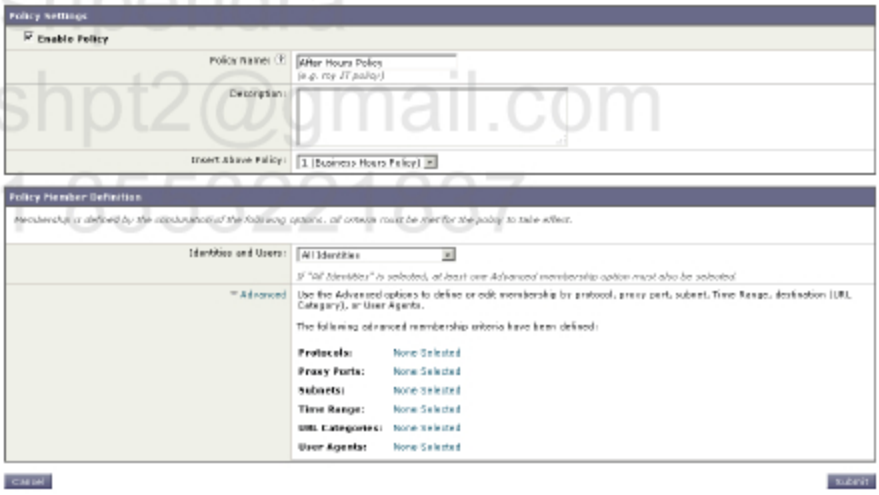
Access Policies: URL Filtering: Business Hours Policy




**Step 4** Add Access Policy for off-business hours.

- Go to **Web Security Manager > Access Policies** and click **Add Policy…** Enter a name for new policy e.g. **After Hours Policy**, select **All Identities** identity and click **None Selected** link next to **Time Range**.

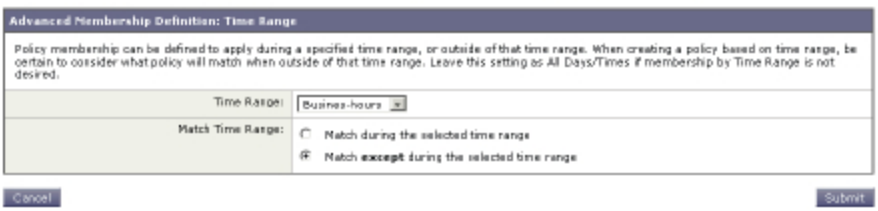
Access Policy: Add Group





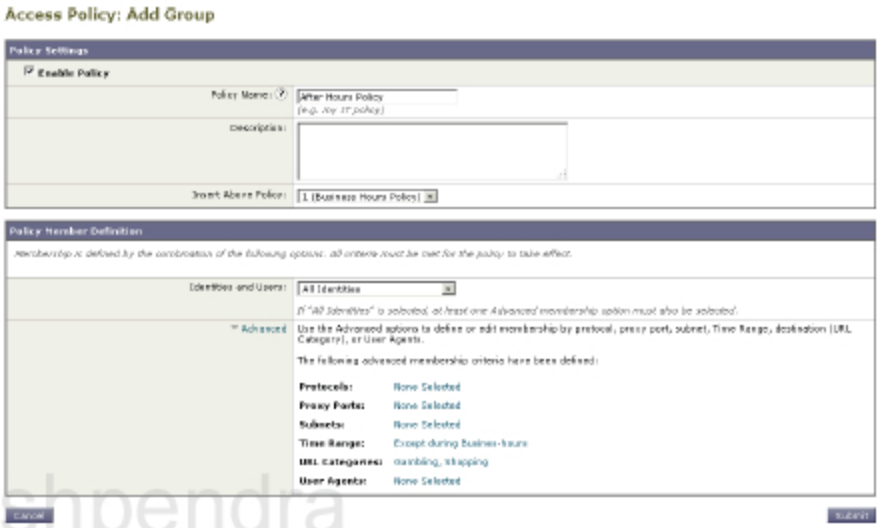

- Pick **Business-hours** time range object and select **Match except during the selected time range** option. Click **Submit**.

Access Policies: Policy "After Hours Policy": Membership by Time Range



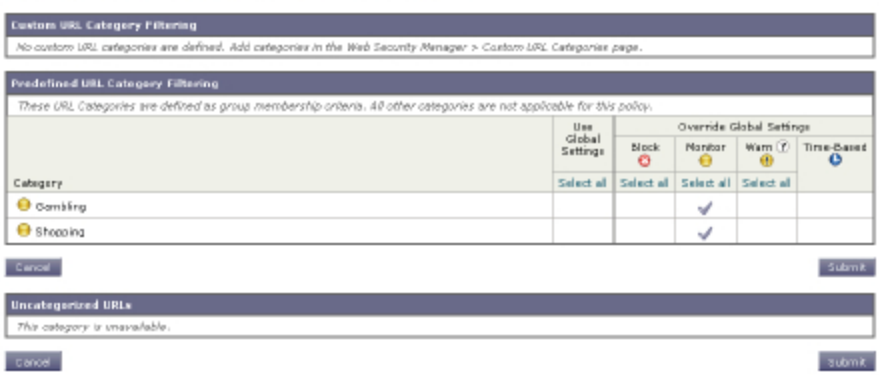
- Click **None Selected** link next to **URL Categories** and pick the following categories on the list:
  - Gambling
  - Shopping

Click **Submit**. Review all options and click **Submit**.



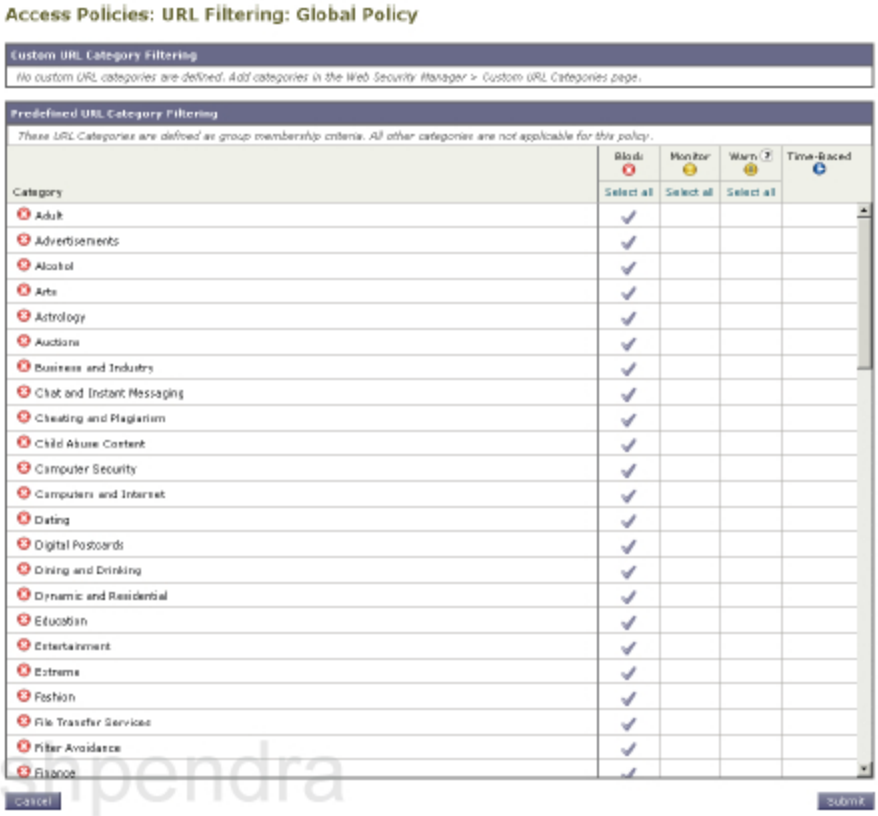



- Click on **Monitor: 2** in **URL Filtering** column for **After Hours Policy** to edit it. Click **Select All** in **Monitor** column. Click **Submit**.




**Step 5** Change Global Access Policy.

- Click on link in **URL Filtering** column for **Global Policy** to edit it. Click **Select All** in **Block** column. Click **Submit**.



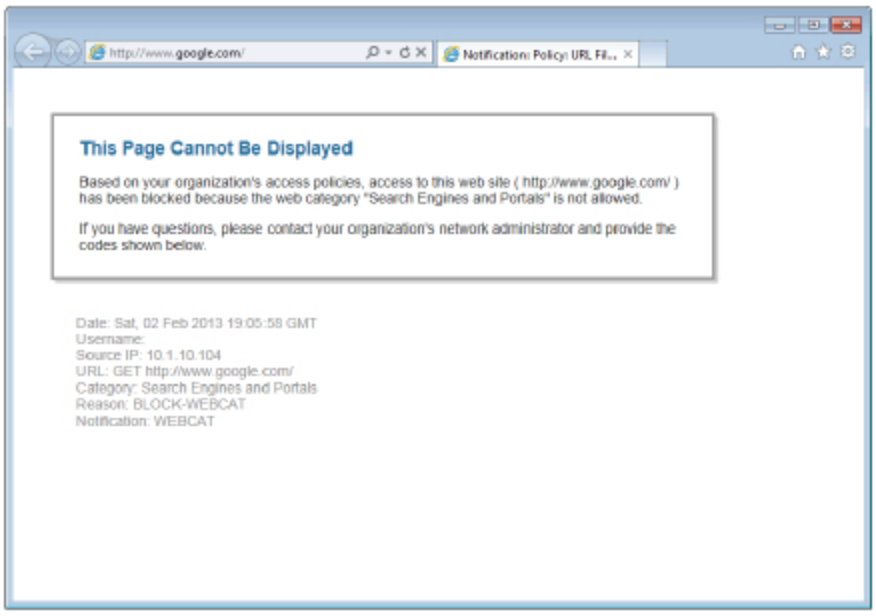



- Review all settings and **Commit Changes**.


## Verification

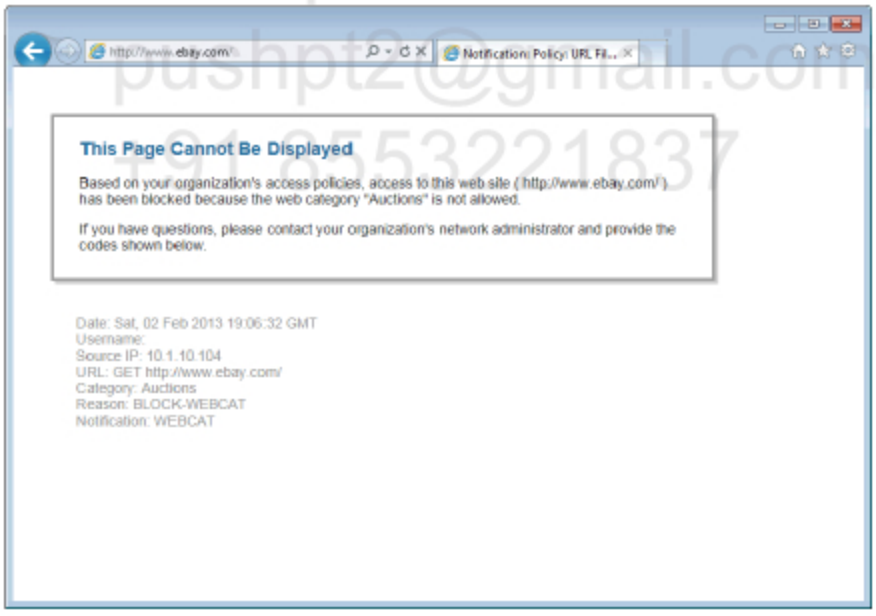
Go to Win7 client PC and test URL filtering by accessing different websites.

- Accessing website from category matched by Global Policy.

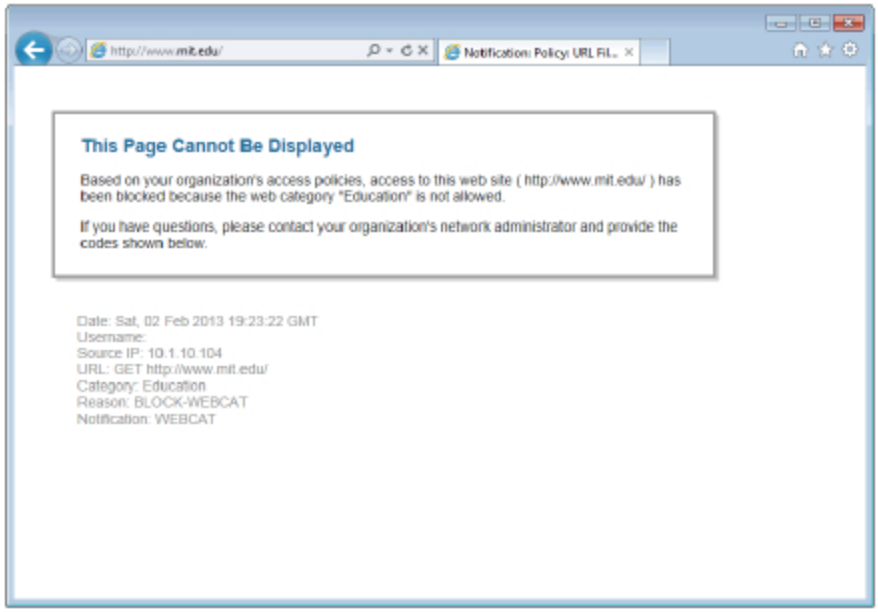



- Accessing website from **Auctions** category (notice that eBAy is NOT in Shopping category).






- Accessing website from **Education** category but outside business hours.




- Accessing website from **Gambilng** category on **Sunday afternoon.**


## Check WSA logs on CLI:

```
1359831958.541 1 10.1.10.104 TCP_DENIED/403 0 GET http://www.google.com/ - NONE/- -
BLOCK_WEBCAT_12-DefaultGroup-Win7-NONE-NONE-NONE-NONE <IW_srch,8.2,-,"-",-,-,-,-,"-",-
,-,-,"-",-,-,"-","-",-,-,IW_srch,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-
"> -

1359831992.661 166 10.1.10.104 TCP_DENIED/403 0 GET http://www.ebay.com/ - NONE/- -
BLOCK_WEBCAT_12-DefaultGroup-Win7-NONE-NONE-NONE-NONE <IW_auct,6.9,-,"-",-,-,-,-,"-",-
```

,-,-,"-",-,-,"-","-",-,-,IW_auct,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-
"> -

1359832018.281 681 10.1.10.104 TCP_MISS/200 9527 GET http://www.poker.com/ -
DIRECT/www.poker.com text/html DEFAULT_CASE_12-After_Hours_Policy-Win7-NONE-NONE-NONE-
DefaultGroup <IW_gamb,0.0,0,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_gamb,-
,"Unknown","-","Unknown","Unknown","-","-",111.92,0,-,"Unknown","-"> -
1359832018.647 232 10.1.10.104 TCP_MISS/403 677 GET

<snip>

1359833002.052 203 10.1.10.104 TCP_DENIED/403 0 GET http://www.mit.edu/ - NONE/- -
BLOCK_WEBCAT_12-DefaultGroup-Win7-NONE-NONE-NONE-NONE <IW_edu,4.9,-,"-",-,-,-,-,"-",-,-
,-,"-",-,-,"-","-",-,-,IW_edu,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-"> -

# LAB 2.19. Active Directory integration

## Objectives

This lab shows how to integrate WSA with Active Directory.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

Create NTLMSSP type of connection between WSA and micronics.local Active Directory domain. Use Domain Controller at IP address 172.31.1.200 and user credentials of caadmin/Micronics1. Make sure that FQDN of all hosts in micronics.local domain is resolved using DNS server at 172.31.1.200.

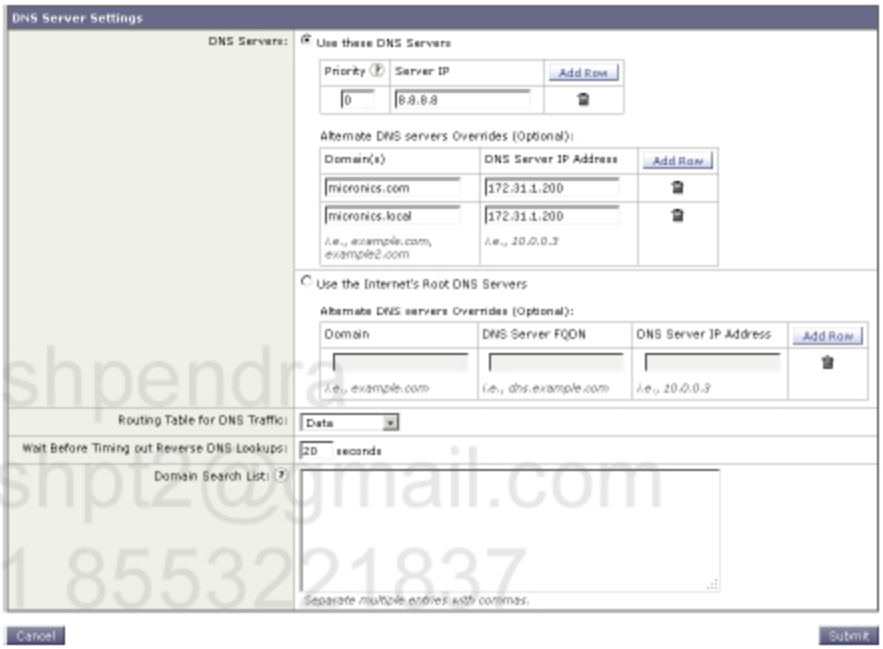
## Configuration

Complete these steps:

**Step 1** Create DNS routing.

- Go to **Network > DNS** and click **Edit Settings...** Add another alternate DNS server by clicking **Add Row** and specifying **micronics.local** domain with IP address of **172.31.1.200**. Click **Submit** and **Commit Changes**.

Edit DNS






**Step 2** Add new Realm for NTLM protocol.

- Go to **Network > Authentication** and click **Add Realm...** Enter a name for new realm e.g. **AD** and specify IP address of Active Directory server. Enter **Micronics.local** for **Active Directory Domain** and click **Join Domain...**



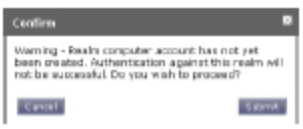

- You must provide credentials for user who can add a computer account to domain. Provide user/pass of **caadmin/Micronics1** and click **Create Account**.


- If process was successful you'll get the following message and new account should be created in AD. Click **Start Test** button to check if it's working.

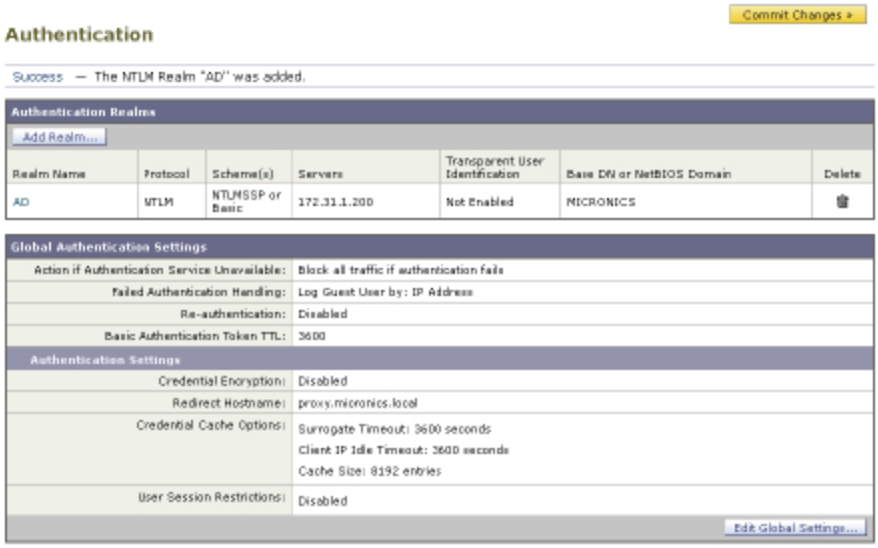



- The test will create a log and should be completed successfully. Click **Submit**.


- You'll get the following message. Click **Submit**.




- Review all settings and click **Commit Changes >**




## Verification

There is no **Verification** for this task.

# LAB 2.20. User authentication

## Objectives

This lab shows how to use user authentication with AD integration.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

Delete all previously created Access Policies and Identities.

Configure WSA to ask users to accept Internet Access Policy before displaying the first website. Configure user authentication and allow access to the following URL categories for users from AD groups:

| AD group | URL categories |
|---|---|
| **Employees** | All |
| **Contractors** | Business and Industry |
| | Computers Security |
| | Computers and Internet |

| Education |
| --- |
| |

Ensure that the user will not be asked to provide credentials after closing and re-opening web browser.

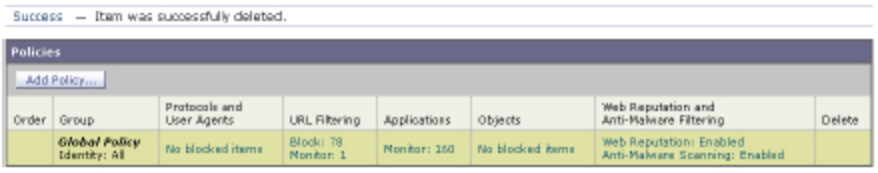
## Configuration

Complete these steps:

**Step 1** Delete all previously created Access Policies and Identities.

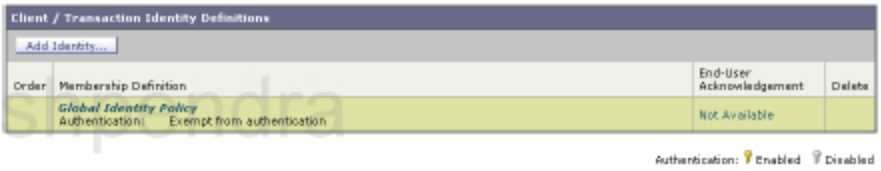
- Go to **Web Security Manager > Access Policies** and click Bin Icon on the right to delete all access policies.

Access Policies




- Go to **Web Security Manager > Identities** and click Bin Icon on the right to delete all identities.

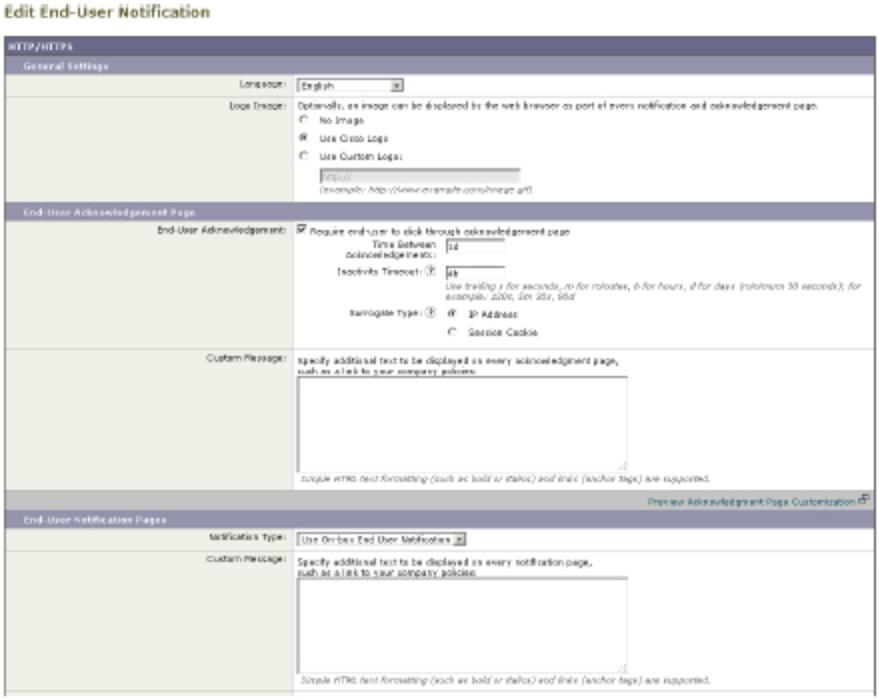
Identities




- Click **Commit Changes**.

**Step 2** Enable End User Notifications (EUN).

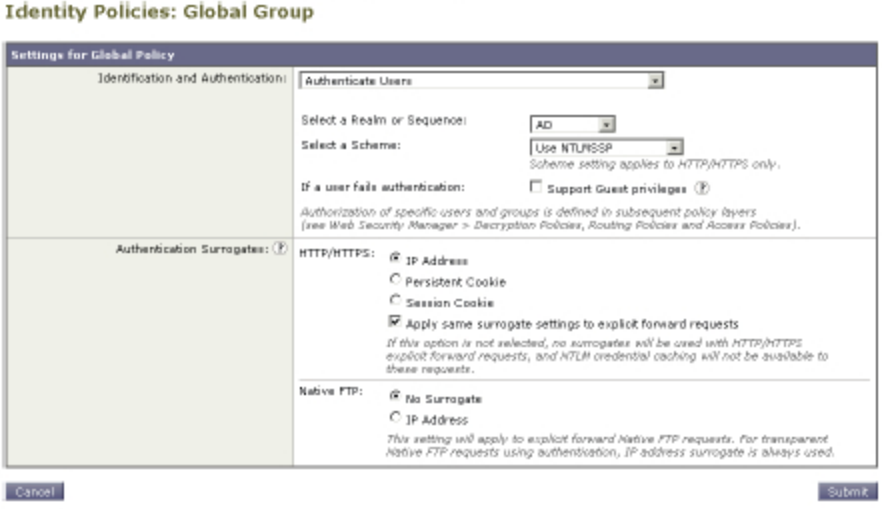
- Go to **Security Services > End-User Notification** and click **Edit Settings…** Check **Use Cisco Logo** radio button and pick **Require end-user to click through acknowledgement page** checkbox. Click **Submit**.




**Step 3** Enable user authentication for Global Identity Policy.

- Go to **Web Security Manager > Identities** and click on **Global Identity Policy** to edit it. Select **Authenticate Users** from **Identification and Authentication** drop-down list and pick **Apply same surrogate settings to explicit forward requests** checkbox. Click **Submit**.





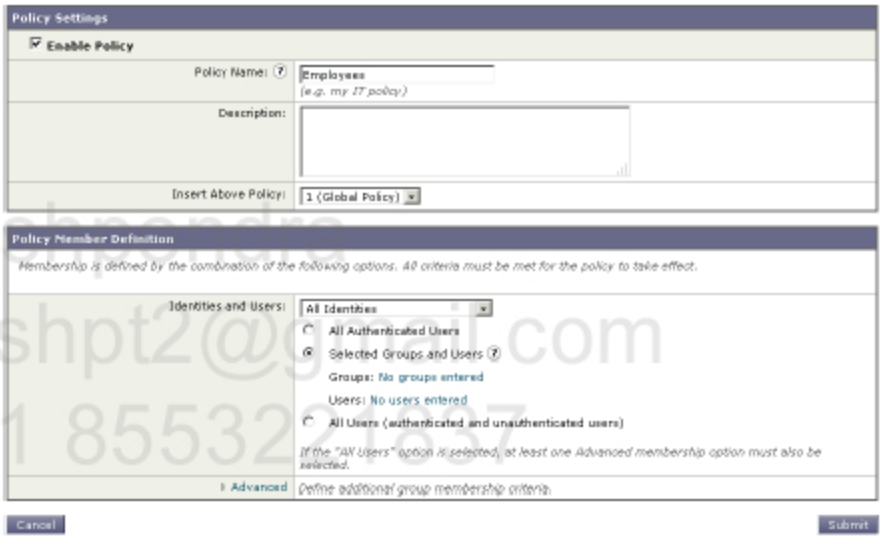

- Verify the Authentication Realm and check if EUN in required. If so, click **Commit Changes**.

Identities


**Step 4** Create access policies for different users groups.

- Go to **Web Security Manager > Access Policies** and click **New Policy…** Enter a name for new policy e.g. **Employees** and check **Selected Groups and Users** radio button. Then click **No groups entered** link to specify AD group.

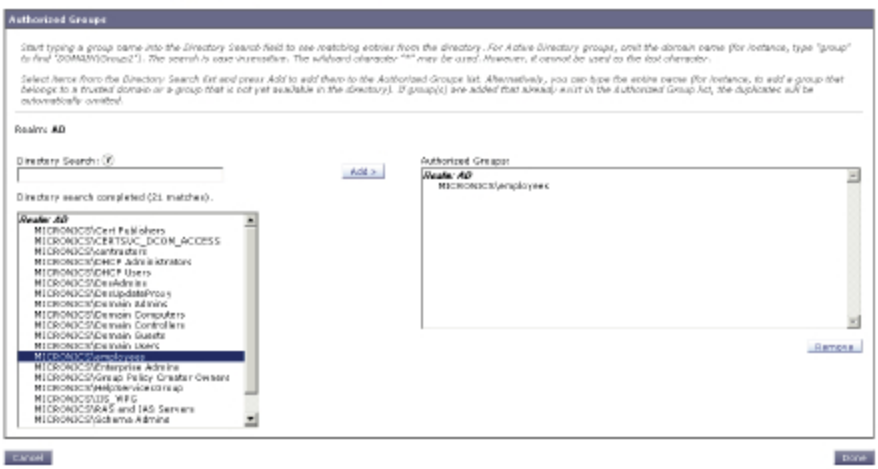
Access Policy: Add Group





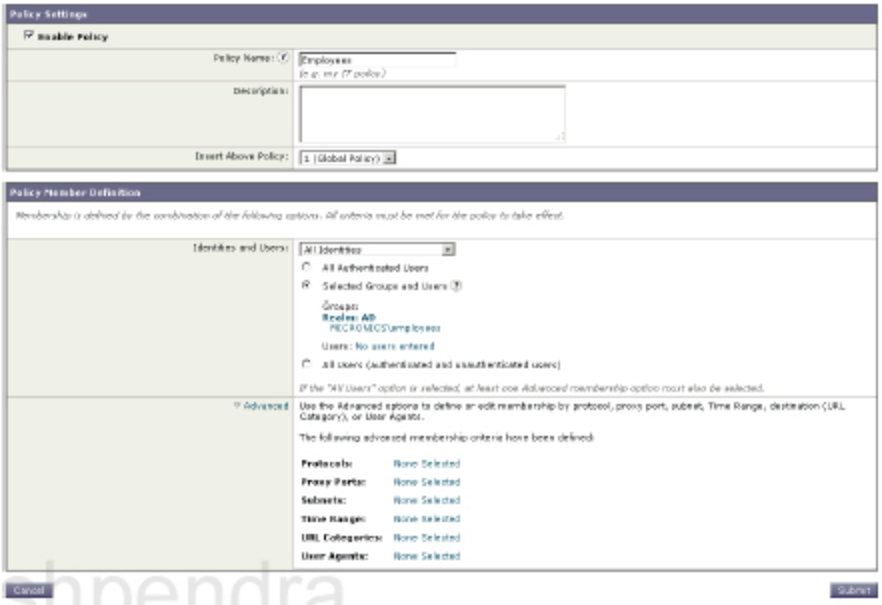

- Select **MICRONICS\employees** group from the left pane and add it to the right pane. Click **Done**.

Access Policies: Policy "Employees": Edit Groups



- Click **Advanced** link to show more optionas and click **None Selected** link next to **URL Categories**.

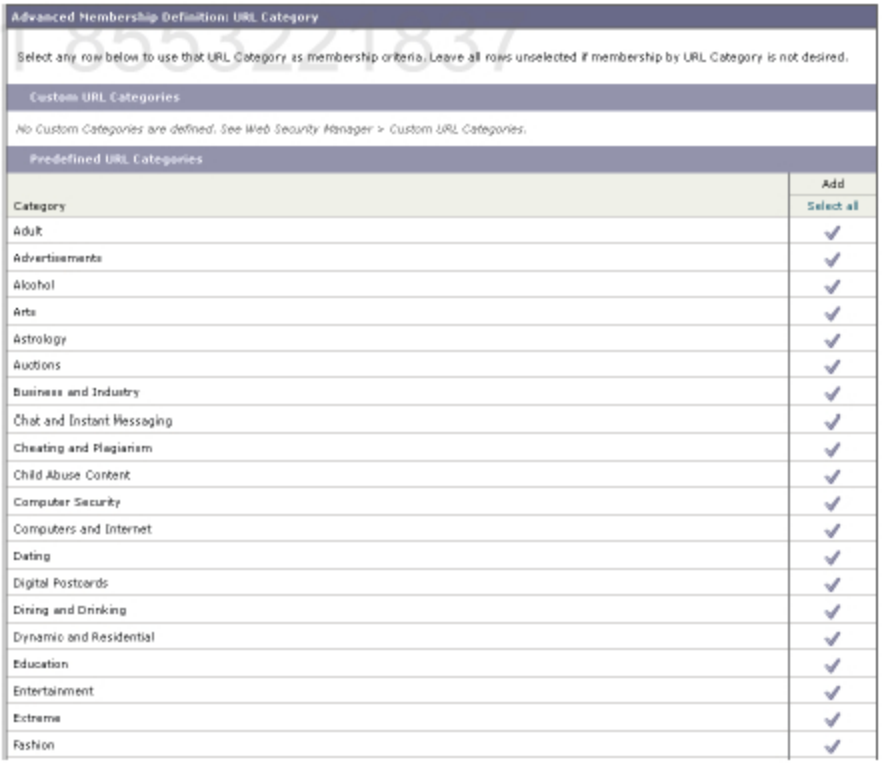
Access Policy: Add Group



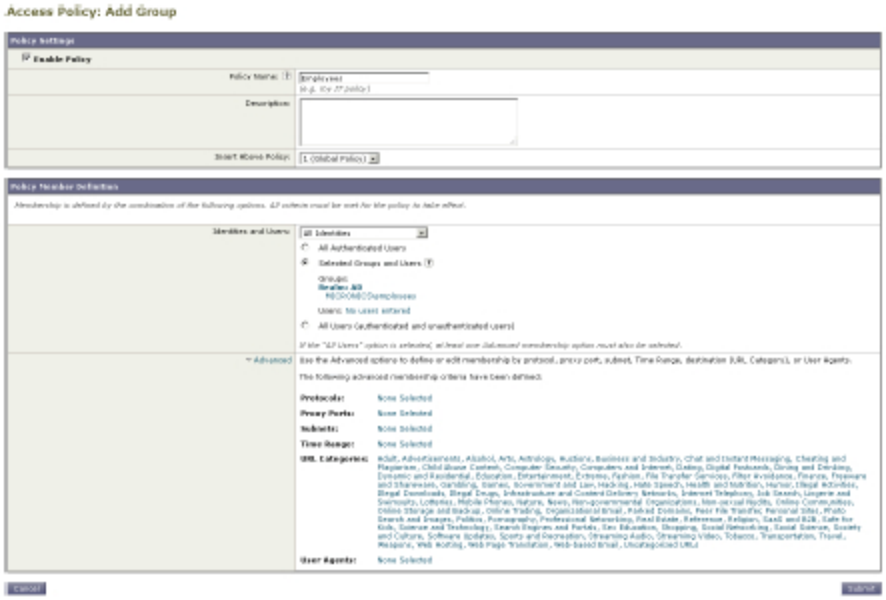



Click **Select all** and then **Submit**.

Access Policies: Policy "Employees": Membership by URL Categories

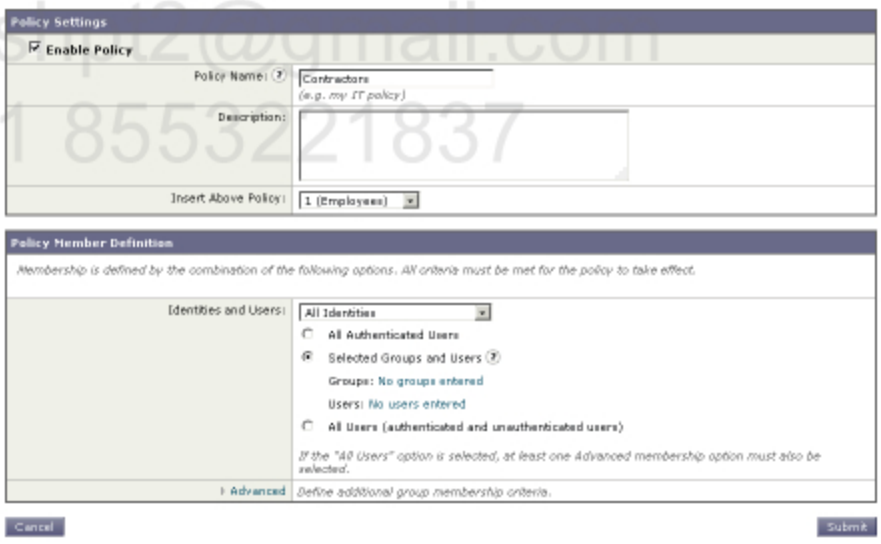



- Review the new access policy and click **Submit**.

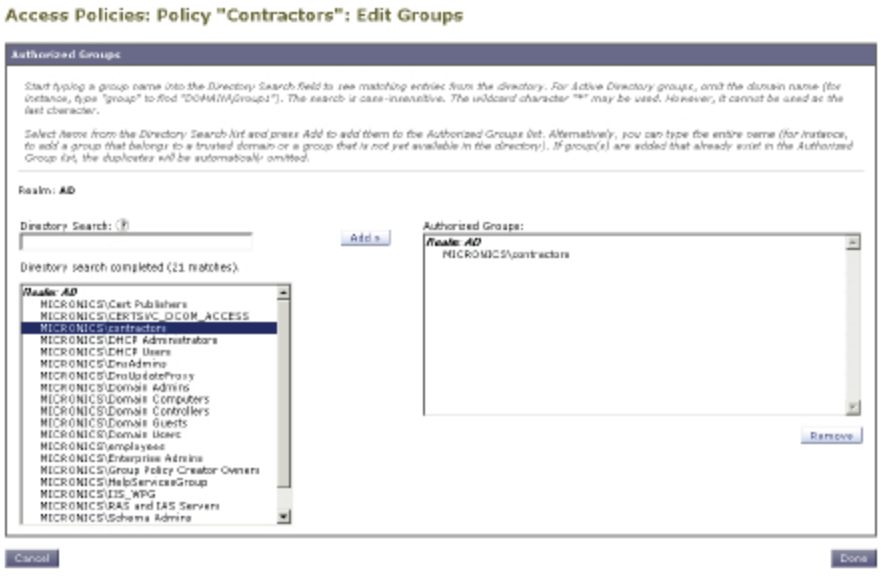



- Add another access policy by clicking **Add Policy…** Enter a name for new policy e.g. **Contractors** and check **Selected Groups and Users** radio button. Then click **No groups entered** link to specify AD group.



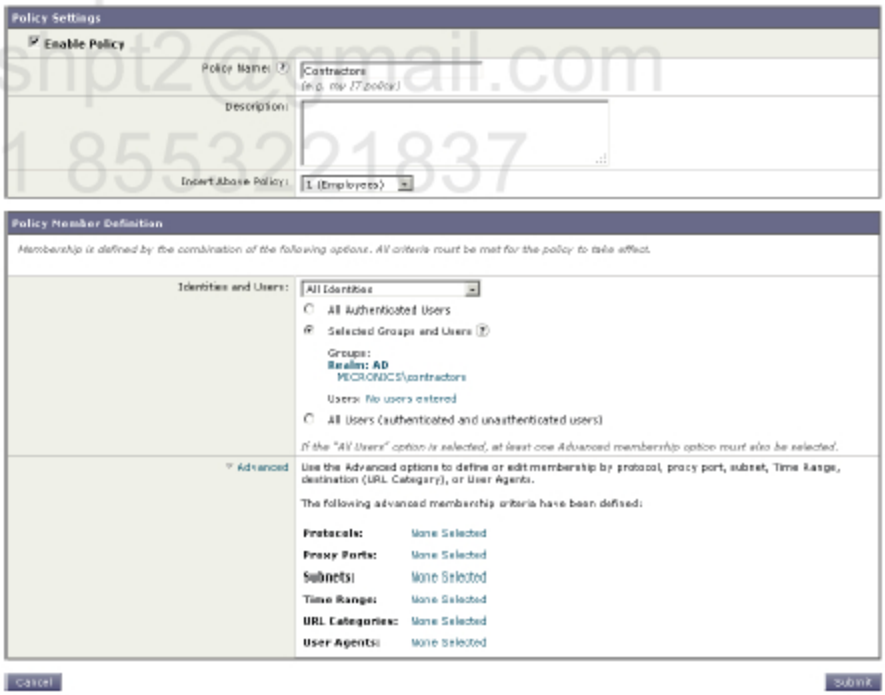



- Select **MICRONICS\contractors** group from the left pane and add it to the right pane. Click **Done**.




- Click **Advanced** link to show more optionas and click **None Selected** link next to **URL Categories**.






- Select the following categories on the list:
  - Business and Industry
  - Computers Security
  - Computers and Internet

- Education

Click **Submit**.

**Access Policies: Policy "Contractors": Membership by URL Categories**

**Advanced Membership Definition: URL Category**

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

**Custom URL Categories**

*No Custom Categories are defined. See Web Security Manager > Custom URL Categories.*

**Predefined URL Categories**

| Category | Add<br>Select all |
|---|---|
| Adult | |
| Advertisements | |
| Alcohol | |
| Arts | |
| Astrology | |
| Auctions | |
| Business and Industry | ✓ |
| Chat and Instant Messaging | |
| Cheating and Plagiarism | |
| Child Abuse Content | |
| Computer Security | ✓ |
| Computers and Internet | ✓ |
| Dating | |
| Digital Postcards | |
| Dining and Drinking | |
| Dynamic and Residential | |
| Education | ✓ |



- Review the new access policy and click **Submit**.

**Access Policy: Add Group**

**Policy Settings**

Enable Policy

Policy Name: Contractors
(e.g. my IT policy)

Description:

Insert Above Policy: 1 (Employees)

**Policy Member Definition**

*Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.*

Identities and Users: All Identities

- All Authenticated Users
- Selected Groups and Users
  - Groups:
    Realm: AD
    MICRONICS\contractors
  - Users: No users entered
- All Users (authenticated and unauthenticated users)

*If the "All Users" option is selected, at least one Advanced membership option must also be selected.*

Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

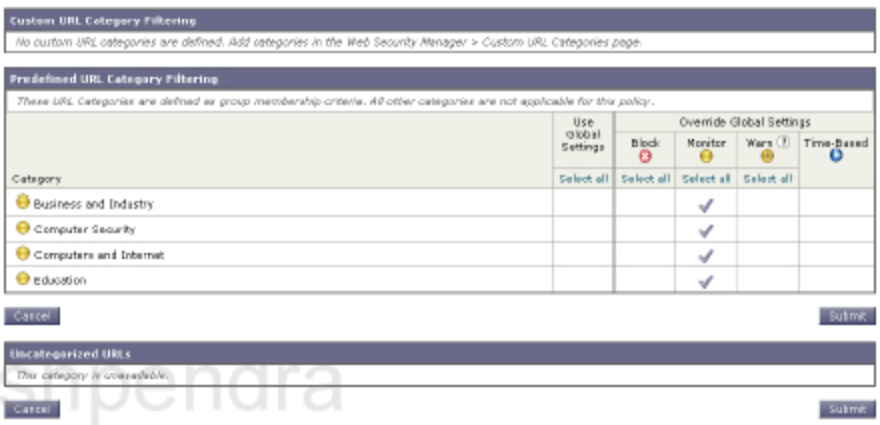
The following advanced membership criteria have been defined:

| | |
|---|---|
| **Protocols:** | None Selected |
| **Proxy Ports:** | None Selected |
| **Subnets:** | None Selected |
| **Time Range:** | None Selected |
| **URL Categories:** | Business and Industry, Computer Security, Computers and Internet, Education |
| **User Agents:** | None Selected |

Cancel Submit

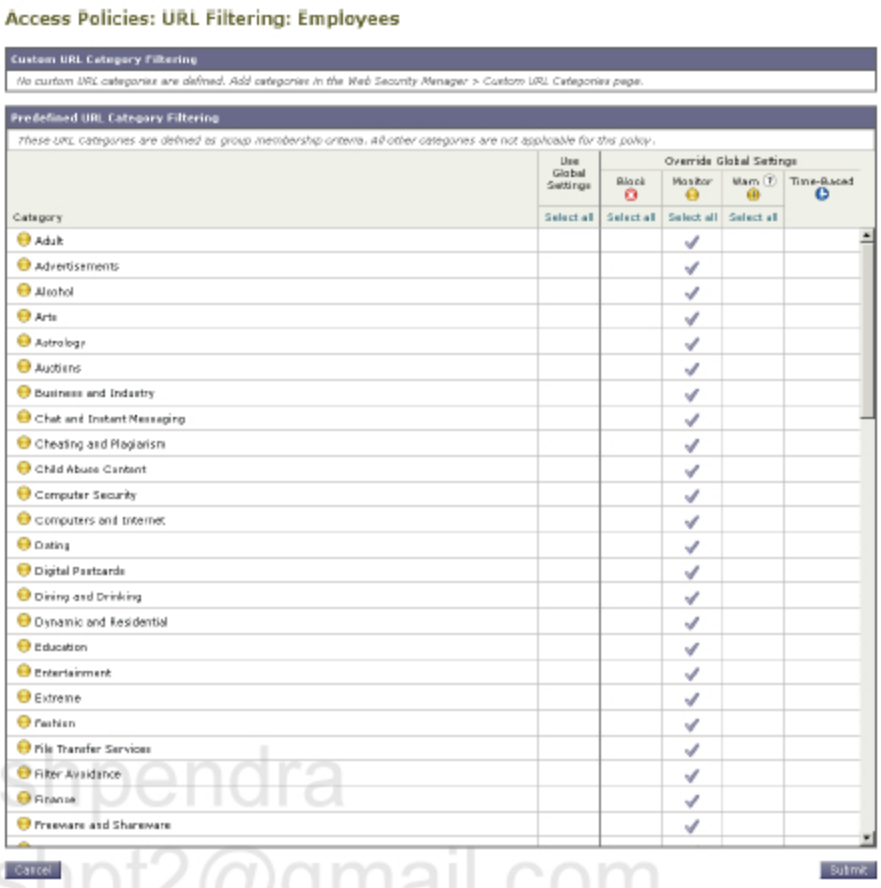
- Two new polices were added. Click link in **URL Filtering** column for **Contractors** policy to edit it.


- Click **Select all** link in **Monitor** column. Click **Submit**.



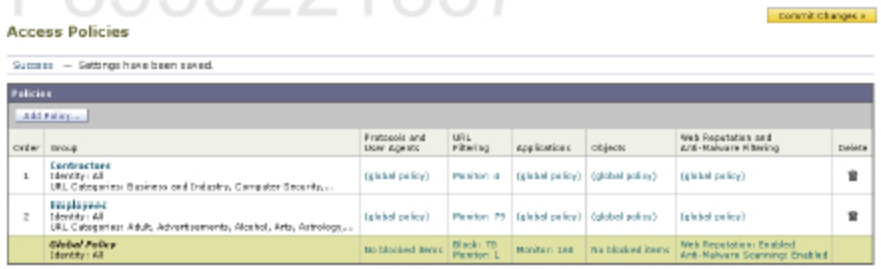



- Click link in **URL Filtering** column for **Employees** policy to edit it. Click **Select all** link in **Monitor** column. Click **Submit**.





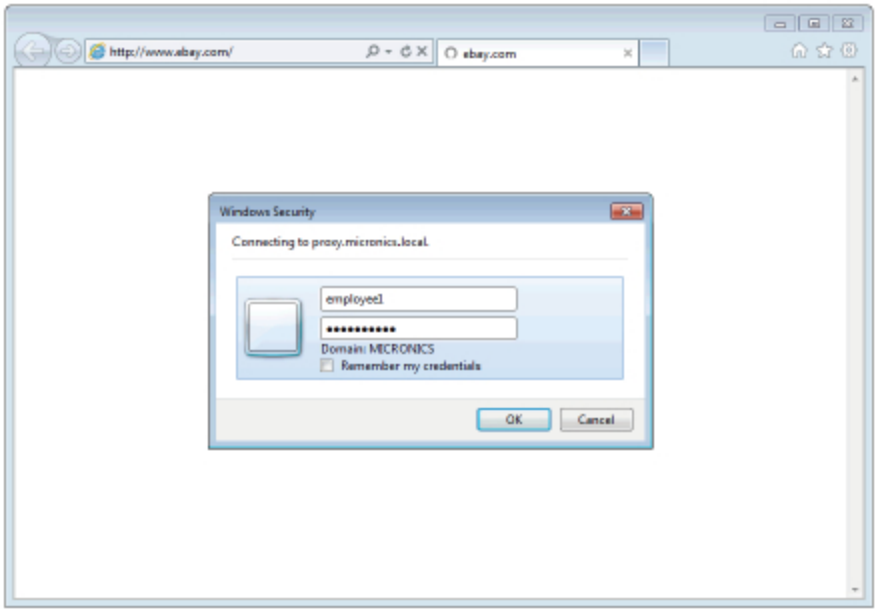

- Review access policies and click **Commit Changes**.



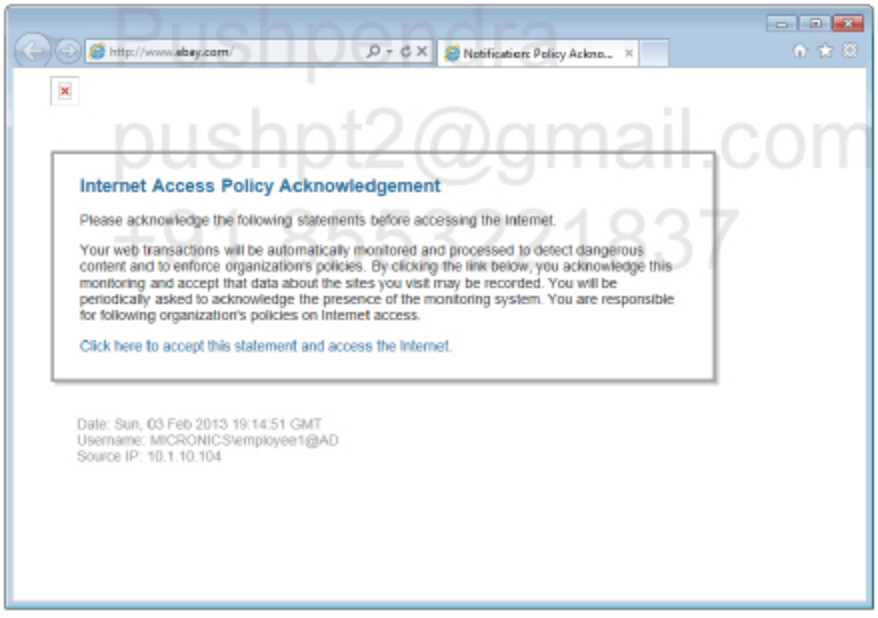

## Verification

Go to Win7 PC client and open up web browser.

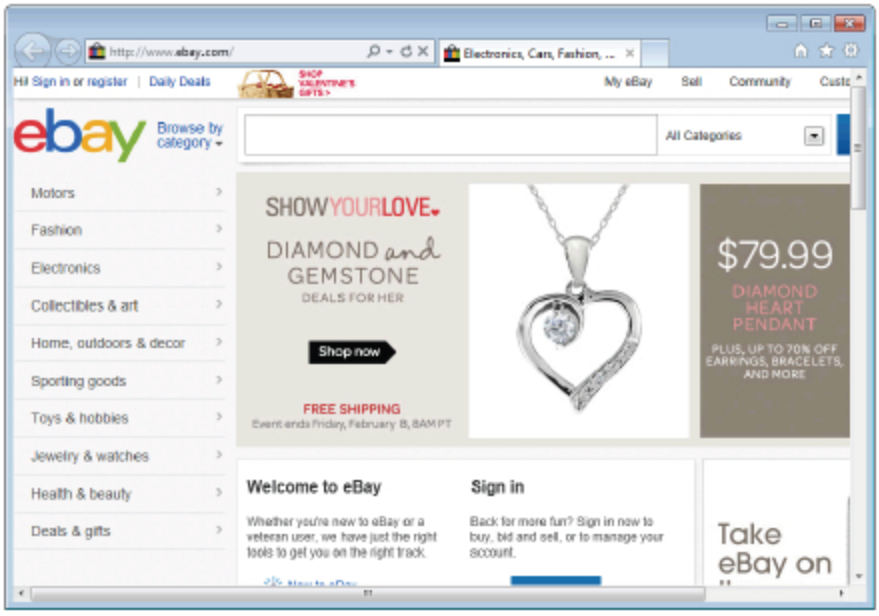
- Go to some website from URL category matching **Emplyees** access policy and authenticate as user **employee1**.




- The user first should be asked to accept access policy.




- Then the user should be allowed to open the webpage.

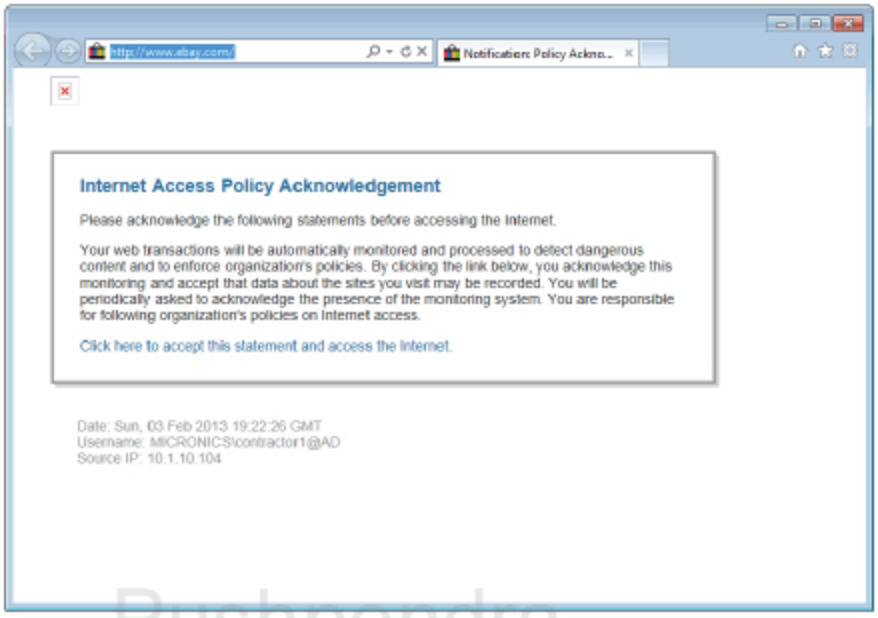



Clear the authentication cache on WSA to re-authenticate with a different user on the client PC.



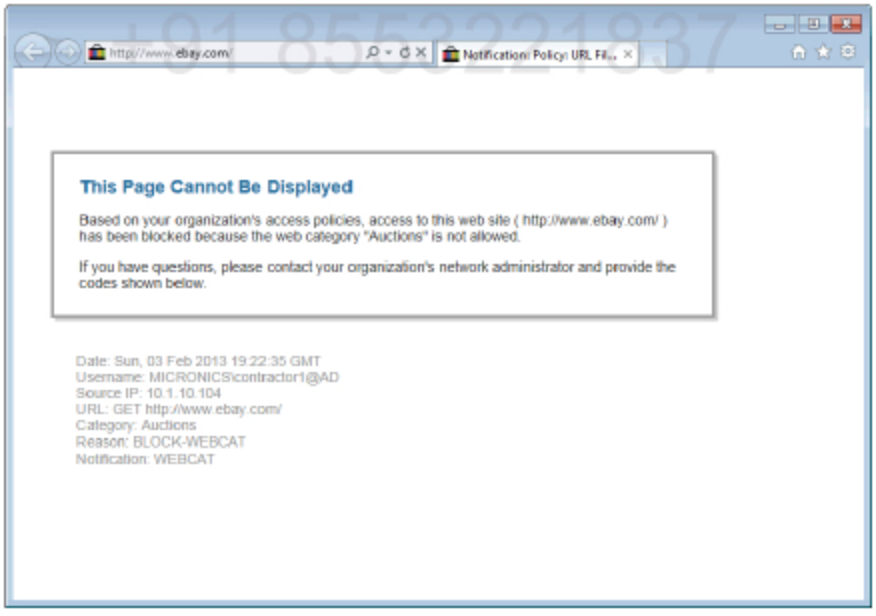
```
wsa.micronics.local> authcache


Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
- SEARCH - Search all entries from auth cache
[]> flushuser

List of Authentication Realms
1. AD
2. GUEST Realm
Enter the auth realm of the user:
[1]> 1

Enter the username to be removed:
[]> employee1

User "MICRONICS\employee1@AD" removed from auth cache.

Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
- SEARCH - Search all entries from auth cache
[]> <enter>
```

- Open up web browser and go to some website from URL category matching **Emplyees** access policy and authenticate as user **contractor1**. The user first should be asked to accept access policy.

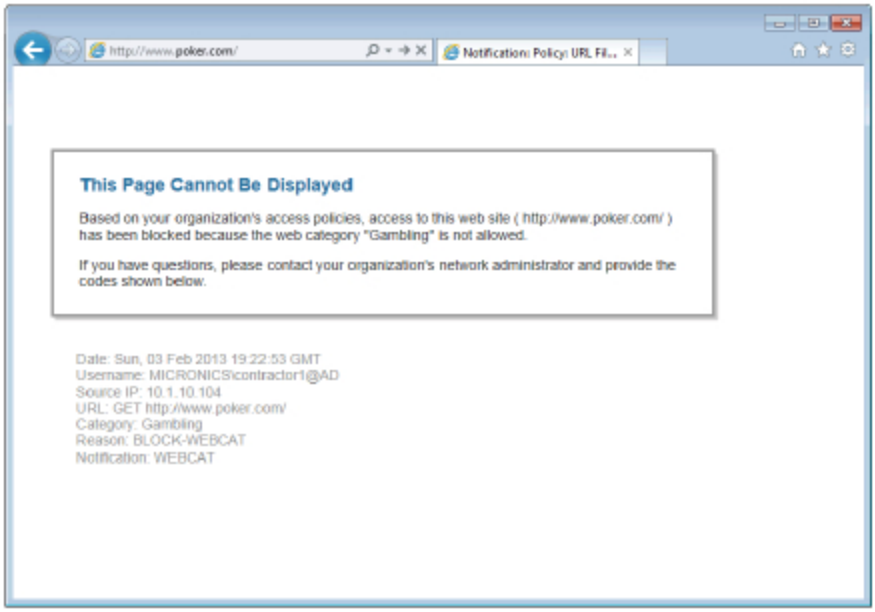




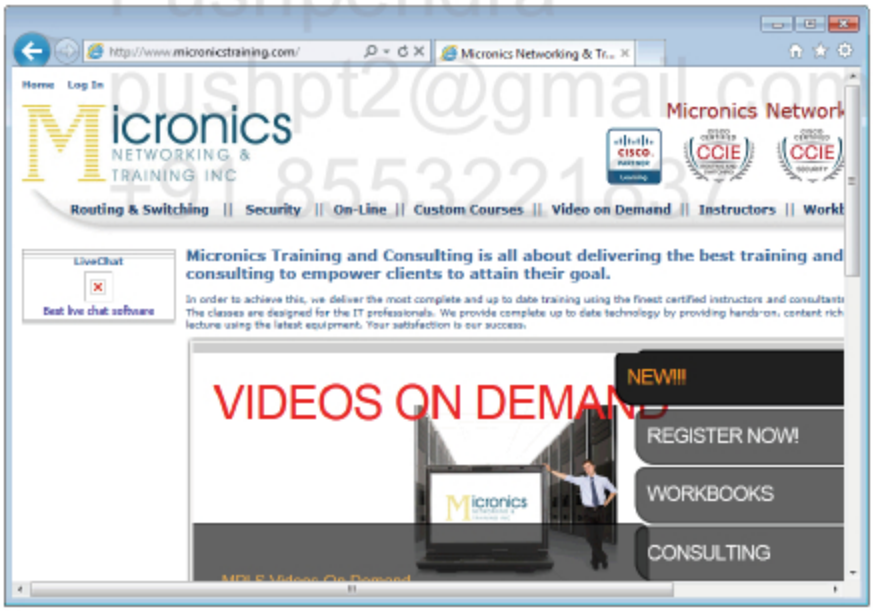

- The page is blocked because contractors group is not allowed to access this URL category.




Try different website from different URL category (e.g. Gambilng) which is not allowed for those users. The website is blocked.




Go to webpage from allowed category e.g. Education. The webpage should be opened.



# LAB 2.21. Custom URL categories

## Objectives

This lab shows how to configure custom URL categories and use them in access policy.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

There is an intranet web server in the company at http://inside.micronics.local. Allow access to that server for Employees based on custom URL category Internal Websites. Also, allow access to the following websites using IP address instead of FQDN:

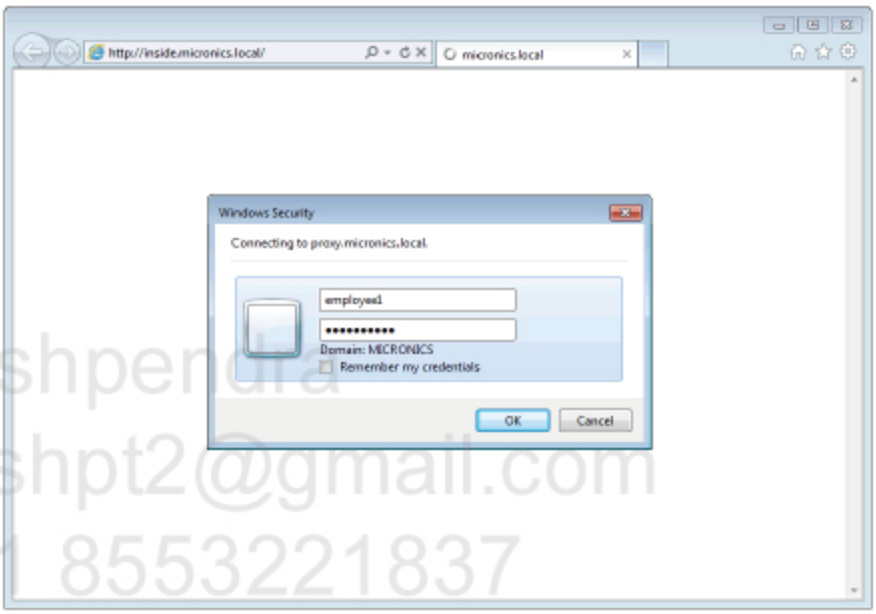
- 200.1.1.1
- 172.31.1.200

## Configuration

Complete these steps:

**Step 1** Check how WSA behavies before re-configuration.

- On Win7 client PC open up web browser and go http://inside.micronics.local. You should be asked for authentication (or not if user's session is there). Then try to access website at http://200.1.1.1. You should be successful.






- Go to WSA CLI and check **accesslogs**. Both requests are allowed based on Global Policy settings for **Uncategorized URLs**.

```
1359963077.038 281 10.1.10.104 TCP_MISS/200 457 GET
http://inside.micronics.local/ "MICRONICS\employee1@AD"
DIRECT/inside.micronics.local text/html DEFAULT_CASE_12-Employees-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <nc,ns,0,"-",0,0,0,0,"-",-
1,0,-1,"-",0,0,"-","-",-,-,nc,nc,"Unknown","-","Unknown","Unknown","-
","-",13.01,0,-,"Unknown","-"> -


1359964383.032 573 10.1.10.104 TCP_MISS/200 267 GET http://200.1.1.1/
"MICRONICS\employee1@AD" DIRECT/200.1.1.1 text/html DEFAULT_CASE_12-
Employees-DefaultGroup-NONE-NONE-NONE-DefaultGroup <nc,-3.5,0,"-
",0,0,0,0,"-",-1,0,-1,"-",0,0,"-","-",-,-,nc,nc,"Unknown","-
","Unknown","Unknown","-","-",3.73,0,-,"Unknown","-"> -
```

**Step 2** Configure new URL Category.

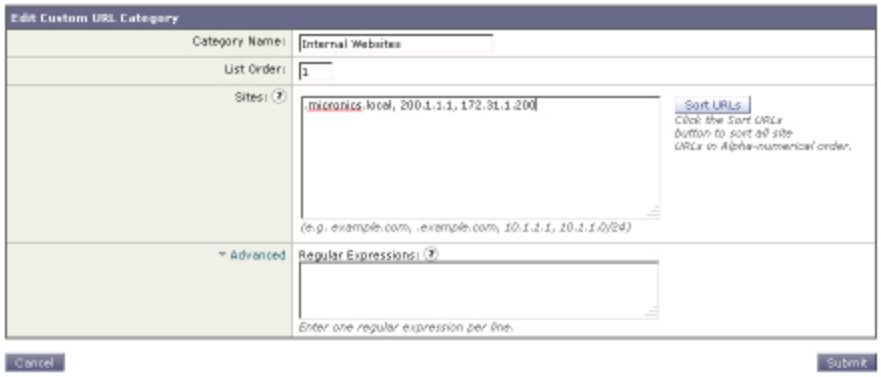
- Go to **Web Security Manager > Custom URL Categories** and click

**Add Custom Category…** Enter **Internal Websites** as category name and in **Sites** field provide the following:

- .micronics.local
- 200.1.1.1
- 172.31.1.200

Click **Submit**.

Custom URL Categories: Add Category



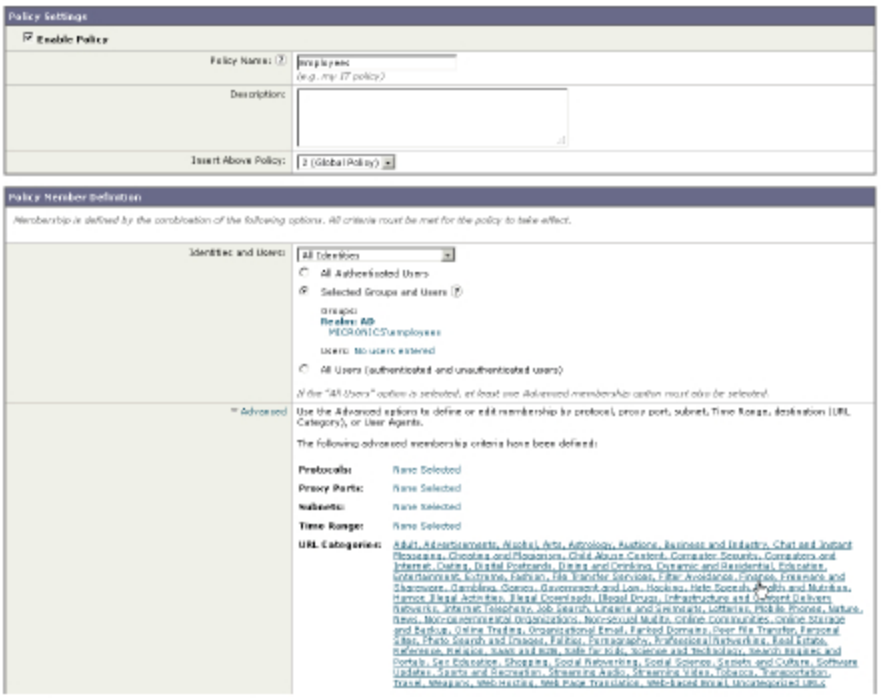



- Go to **Web Security Manager > Access Policies** and click link in **URL Filetring** column for **Employees** policy.

Access Policies


- Click on **URL Categories** to edit them.

Access Policy: Employees





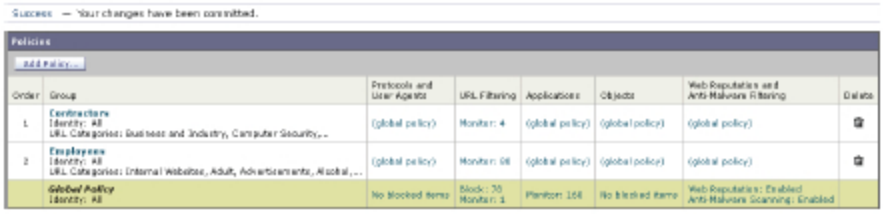

- Pick the **Internal Websites** category in **Custom URL Categories** section. Click **Done.**

Access Policies: Policy "Employees": Membership by URL Categories


- The new category should be on the list. Click **Submit.**

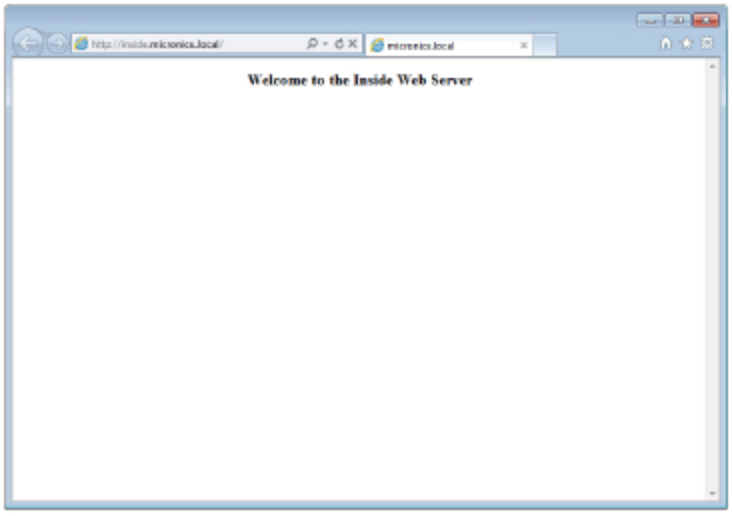

- Review the changes in access policy and commit them.

Access Policies




## Verification

- On Win7 client PC go to the http://inside.micronics.local website.

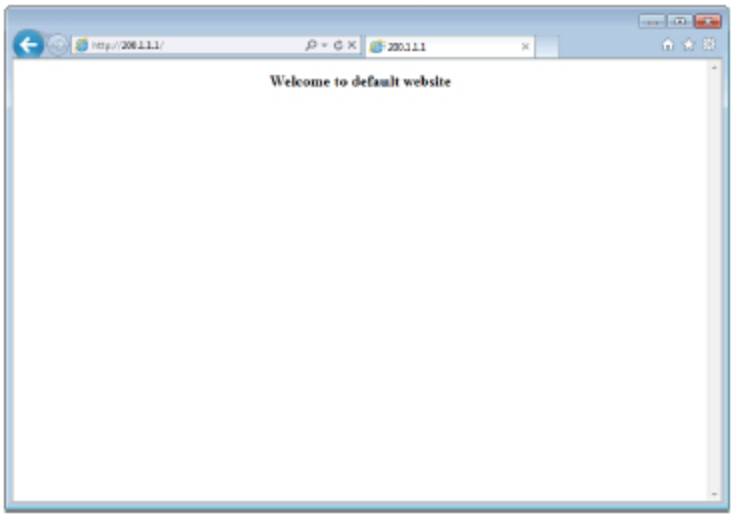



- Check **accesslogs** on CLI.

```
1359964915.129 525 10.1.10.104 TCP_MISS/200 457 GET http://inside.micronics.local/
"MICRONICS\employee1@AD" DIRECT/inside.micronics.local text/html MONITOR_CUSTOMCAT_12-
Employees-DefaultGroup-NONE-NONE-NONE-DefaultGroup <C_Inte,ns,0,"-",0,0,0,0,"-",-1,0,-
1,"-",0,0,"-","-",-,-,IW_comp,-,"Unknown","-","Unknown","Unknown","-","-",28.80,0,-
,"Unknown","-"> -
```



- Go to http://200.1.1.1




- Check logs on CLI.

```
1359964924.538 25 10.1.10.104 TCP_MISS/200 267 GET http://200.1.1.1/
"MICRONICS\employee1@AD" DIRECT/200.1.1.1 text/html MONITOR_CUSTOMCAT_12-Employees-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <C_Inte,-3.5,0,"-",0,0,0,0,"-",-1,0,-1,"-
```

",0,0,"-","-",-,-,nc,nc,"Unknown","-","Unknown","Unknown","-","-",85.44,0,-
,"Unknown","-"> -

# LAB 2.22. Decryption policies

## Objectives

This lab shows how to use decryption policies to handle HTTPS traffic.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

There is an intranet web server in the company at http://inside.micronics.local. Allow access to that server for Employees based on custom URL category Internal Websites. Also, allow access to the following websites using IP address instead of FQDN:

- 200.1.1.1
- 172.31.1.200

## Configuration

Complete these steps:

**Step 1** Check how WSA behavies before re-configuration.

- On Win7 client PC open up web browser and connect to https://www.google.com. Authenticate as user from Employees group. The connection should be successful.
- Go to WSA CLI and check **accesslogs**.

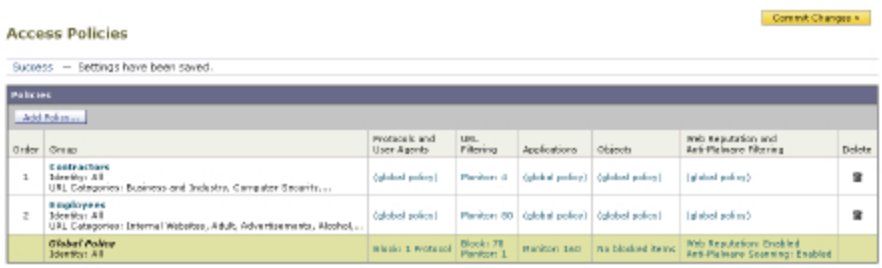
```
1359985729.430 3745 10.1.10.104 TCP_CLIENT_REFRESH_MISS/200 413 CONNECT
tunnel://www.google.com:443/ "MICRONICS\employee1@AD"
DIRECT/www.google.com - DEFAULT_CASE_12-Employees-DefaultGroup-NONE-
NONE-NONE-DefaultGroup <IW_srch,8.2,0,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-
","-",-,-,IW_srch,-,"-","-","Unknown","Unknown","-","-",0.88,0,-
,"Unknown","-"> -
```

**Step 2** Disable HTTP Tunneling for all ports and disable FTP over HTTP.

- Go to **Web Security Manager > Access Policies** and click link for **Protocols and User Agents** column for **Global Policy**. Pick options **FTP over HTTP** and clear all port numbers from **HTTP CONNECT Ports**. Click **Submit**.




- Review the changes and commit them.



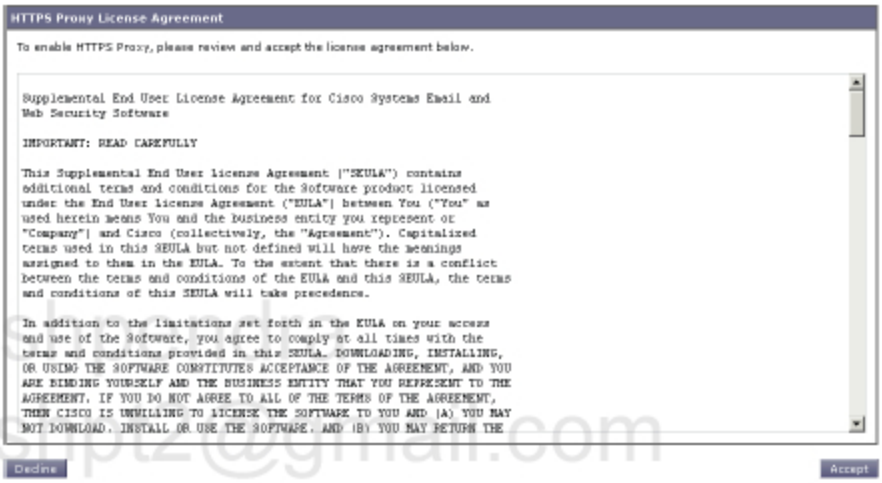
Try to connect to webserver using HTTPS and verify the **accesslog**.

```
1359986616.554  0 10.1.10.104 TCP_DENIED/403 0 CONNECT
tunnel://www.google.com:443/ "MICRONICS\employee1@AD" NONE/- -
BLOCK_ADMIN_CONNECT_12-Employees-DefaultGroup-NONE-NONE-NONE-NONE
<IW_srch,8.2,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_srch,-,"-
","-","Unknown","Unknown","-","-",0.00,0,-,"-","-"> -
```

**Step 3** Enable HTTPS Proxy.

- Go to **Security Services > HTTPS Proxy** and click **Enable and Edit Settings...** Read and **Accept** the license.

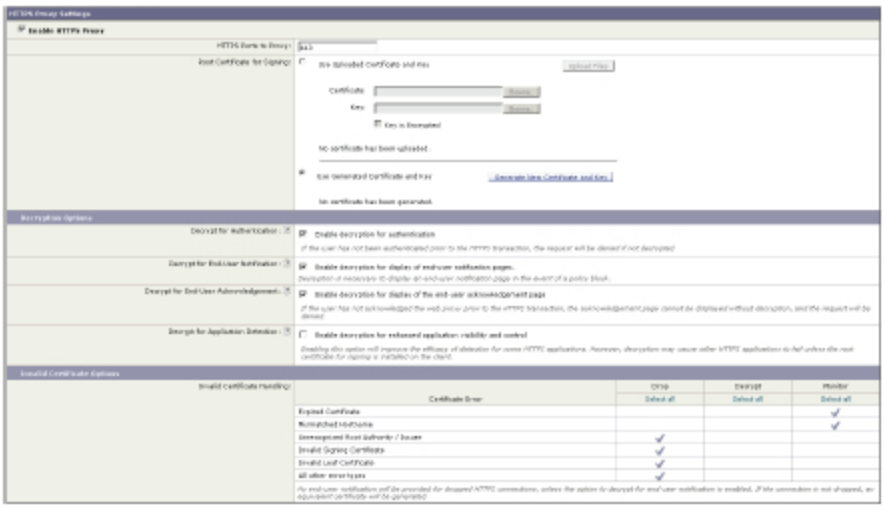
HTTPS Proxy



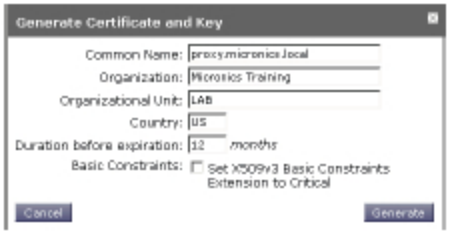



- **Enable HTTPS Proxy** option should be checked. Select **Use Generated Certificate and Key** radio button and click **Generate New Certificate and Key**.

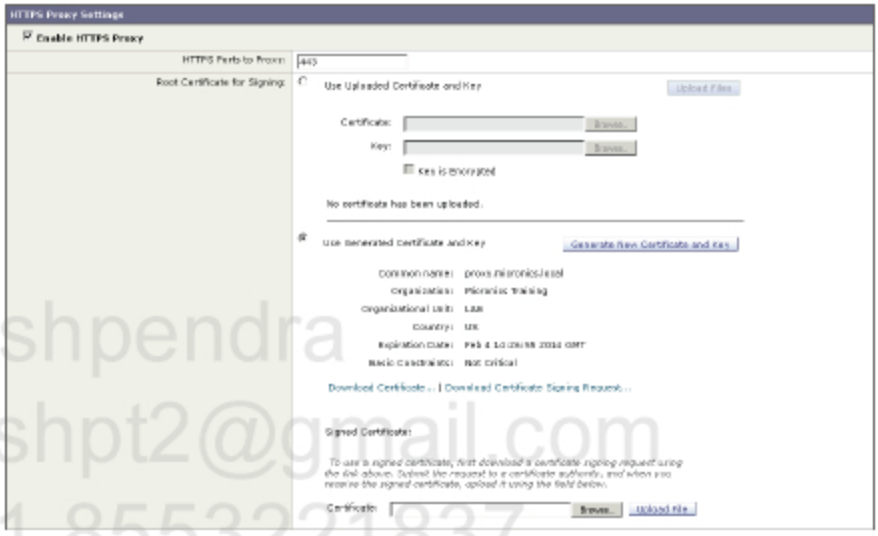
Edit HTTPS Proxy Settings



- Povide information to generate new certificate and click **Generate**.

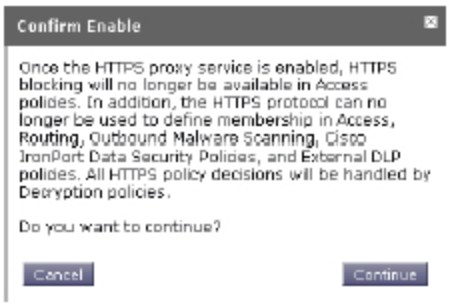



- Information about new certificate will appear. Optionally you can download new certificate and import it to the client web brower. Click **Submit**.






A message appears that enabling HTTPS Proxy causes some changes in WSA policies. Click **Continiue** and **Commit Changes**.

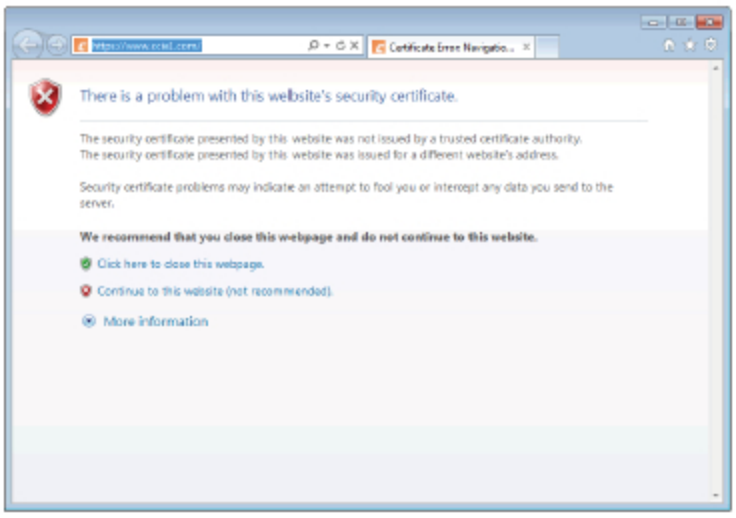



- Try to connect to some webservers using HTTPS and verify the **accesslog**.
  - Go to https://www.google.com

```
1359987764.147  85274 10.1.10.104 TCP_CLIENT_REFRESH_MISS/200
66038 CONNECT tunnel://www.google.com:443/
"MICRONICS\employee1@AD" DIRECT/www.google.com -
PASSTHRU_WBRS_7-DefaultGroup-DefaultGroup-NONE-NONE-NONE-
```

```
DefaultGroup <IW_srch,8.2,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-
",-,-,IW_srch,-,"-","-","Unknown","Unknown","-","-",6.20,0,-,"-
","-"> -
```

- Go to https://www.ccie1.com You should see certificate error.






- View the certificate after connection. Notice that the certificate was issued by WSA.

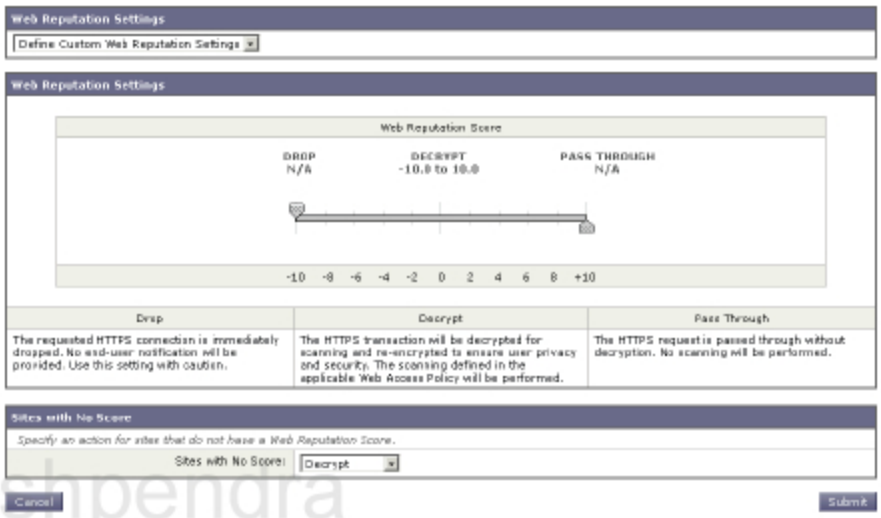

- Check **accesslogs**.

```
1359988179.812 2314 10.1.10.104 TCP_CLIENT_REFRESH_MISS_SSL/200
39 CONNECT tunnel://www.ccie1.com:443/ "MICRONICS\employee1@AD"
DIRECT/www.ccie1.com - DECRYPT_WBRS_7-DefaultGroup-DefaultGroup-
NONE-NONE-NONE-DefaultGroup <IW_comp,0.0,-,"-",-,-,-,-,"-",-,-,-
,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-
","-",0.13,0,-,"-","-"> -
```

**Step 4** Change Web Reputation engine to decrypt all traffic.

- Go to **Web Security Manager > Decryption Policies** and click on link in **Web Reputation** column for **Global Policy**. Edit the Web reputation so that WSA will decrypt all traffic with a score from -10 to +10. Also, select option to **Decrypt** for **Sites with No Score**. Click **Submit** and **Commit Changes**.

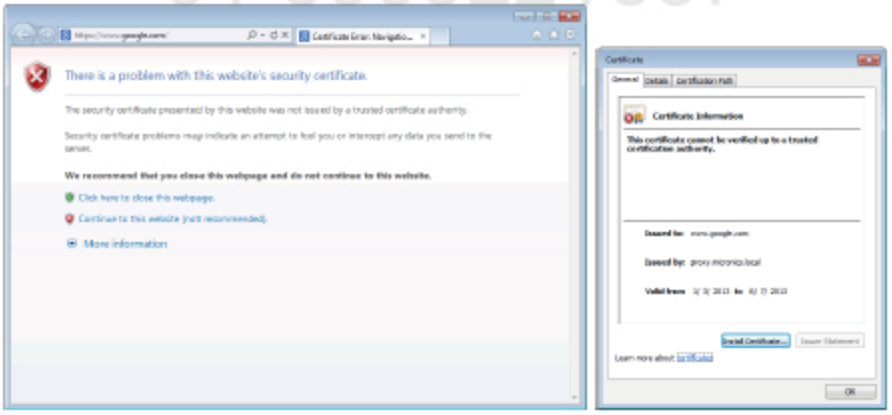
**Decryption Policies: Reputation Settings: Global Policy**






## Verification

On Win7 client PC connect to https://www.google.com




Check access log on CLI.

```
1359988929.257 346 10.1.10.104 TCP_CLIENT_REFRESH_MISS_SSL/200 39 CONNECT
tunnel://www.google.com:443/ "MICRONICS\employee1@AD" DIRECT/www.google.com -
DECRYPT_WBRS_7-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_srch,8.2,-,"-
",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_srch,-,"-","-","Unknown","Unknown","-","-
",0.90,0,-,"-","-"> -
```

# LAB 2.23. Bandwidth and file type limits

## Objectives

This lab shows how to configure different limits on WSA to enforce blocking some file types or MIME types.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

Configure an overall bandwidth limit on WSA to download from teh Internet with a speed of 50 Mbps. For Employees group set up file access limits and block downloading of following files: ZIP archives, RAR archives, EXE files and *.torrent files.

## Configuration

Complete these steps:

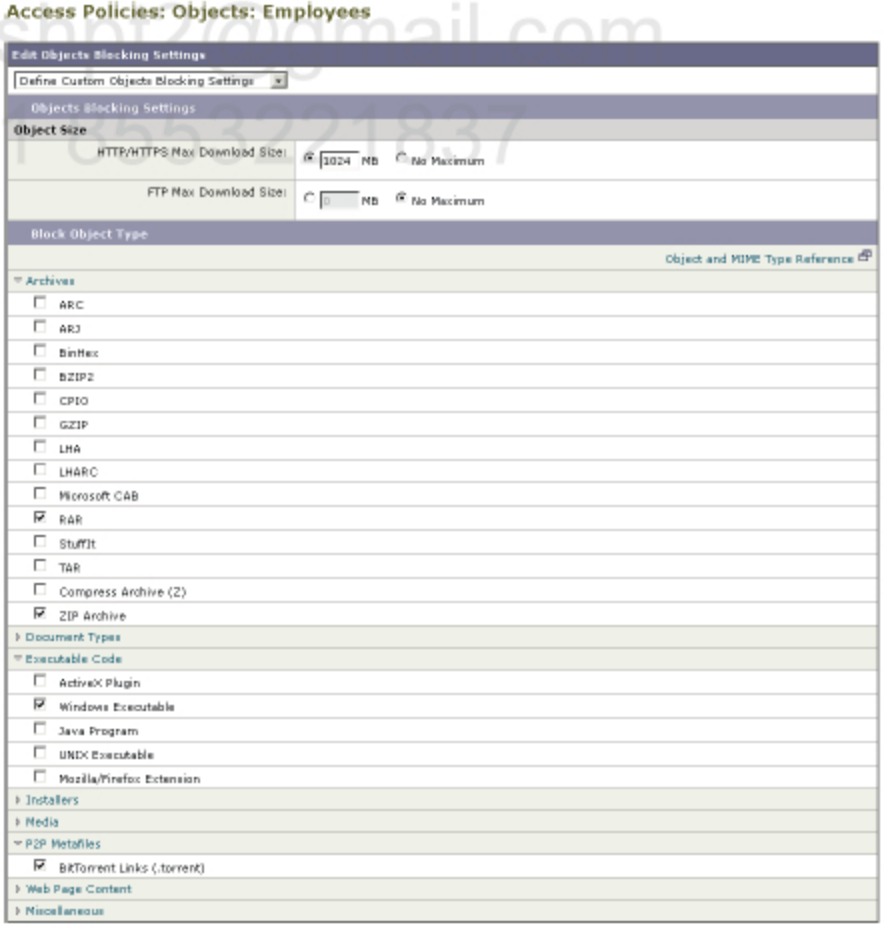
**Step 1** Configure global bandwidth limit for all users.

- Go to **Web Security Manager > Overall Bandwidth Limits** and click **Edit Settings…** Set the limit to **50 Mbps** and click **Submit**.

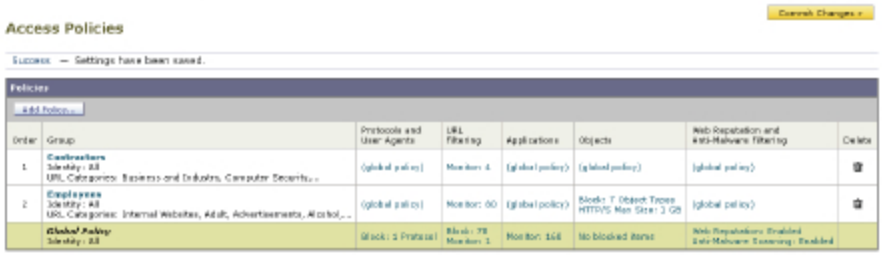

**Step 2** Configure bandwidth and file type limits for Employees policy.

- Go to **Web Security Manager > Access Policies** and click link in **Objects** column for **Employees** policy. From drop-down list select **Define Custom Objects Blocking Settings** and specify maximum object size of **1024 MB**. Pick **RAR, ZIP, Windows Executable** and **BitTorrent Links** from the list and click **Submit**.





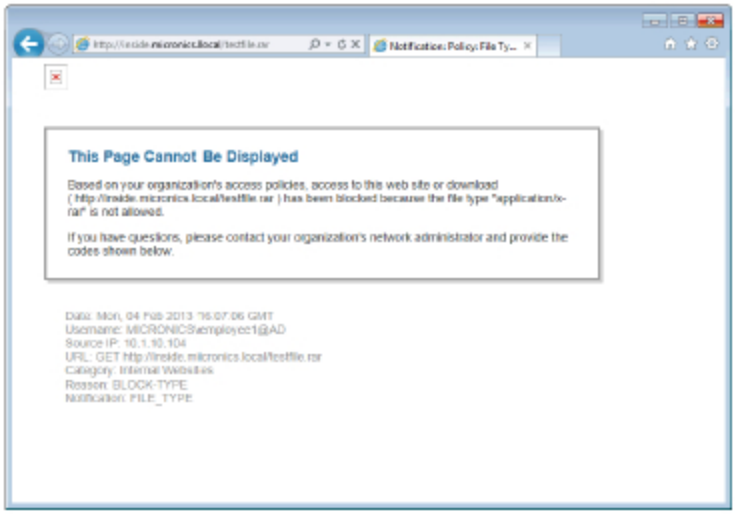
- Review all settings and click **Commit Changes**.




## Verification

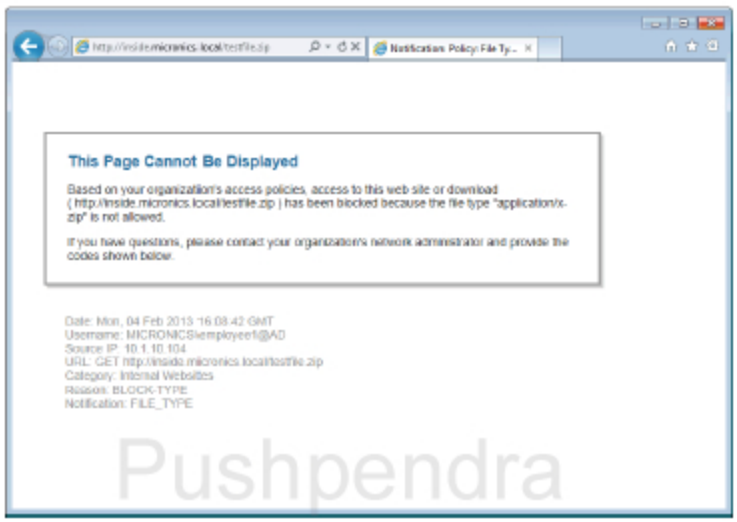
- On Win7 client PC open up web browser and go to http://inside.micronics.local (the URL in custom Internal Websites category allowed to Employees group).


- Click to download RAR Archive. You should be denied.



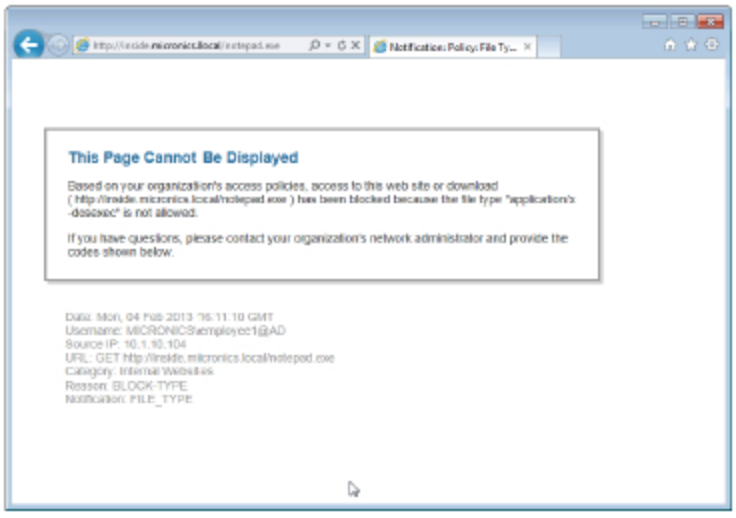
```
1359994026.395 25 10.1.10.104 TCP_DENIED/403 0 GET
http://inside.micronics.local/testfile.rar "MICRONICS\employee1@AD"
DIRECT/inside.micronics.local application/x-rar BLOCK_ADMIN_FILE_TYPE_12-Employees-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <C_Inte,ns,0,"-",0,0,0,-,"-",-,-,-,"-",-,-,"-
","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"Unknown","-"> -
```

- Click to download ZIP Archive. You should be denied.




```
1359994122.454 237 10.1.10.104 TCP_DENIED/403 0 GET
http://inside.micronics.local/testfile.zip "MICRONICS\employee1@AD"
DIRECT/inside.micronics.local application/x-zip BLOCK_ADMIN_FILE_TYPE_12-Employees-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <C_Inte,ns,0,"-",0,0,0,-,"-",-,-,-,"-",-,-,"-
","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"Unknown","-"> -
```

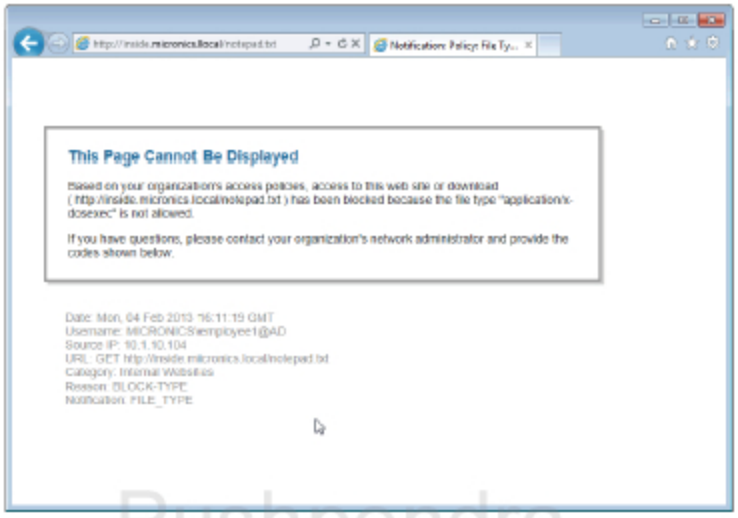
- Click to download Windows Executable. You should be denied.




```
1359994270.344 23 10.1.10.104 TCP_DENIED/403 0 GET
http://inside.micronics.local/notepad.exe "MICRONICS\employee1@AD"
DIRECT/inside.micronics.local application/x-dosexec BLOCK_ADMIN_FILE_TYPE_12-Employees-
```

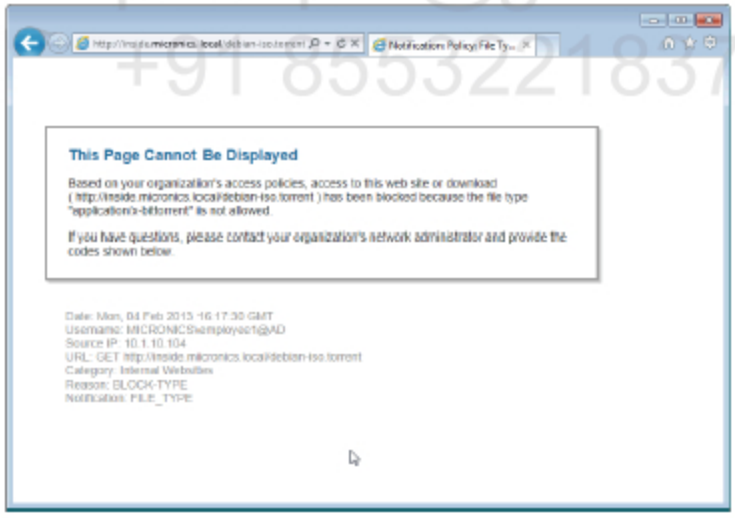
```
DefaultGroup-NONE-NONE-NONE-DefaultGroup <C_Inte,ns,0,"-",0,0,0,-,"-",-,-,-,"-",-,-,"-
","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"Unknown","-"> -
```

- Click to download Windows Executable with changed extension. It is still recognized as dosexec MIME type. You should be denied.






- Click to download BitTorrent file. You should be denied.




```
1359994650.844 26 10.1.10.104 TCP_DENIED/403 0 GET
http://inside.micronics.local/debian-iso.torrent "MICRONICS\employee1@AD"
DIRECT/inside.micronics.local application/x-bittorrent BLOCK_ADMIN_FILE_TYPE_12-
Employees-DefaultGroup-NONE-NONE-NONE-DefaultGroup <C_Inte,ns,0,"-",0,0,0,-,"-",-,-,-
,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","BitTorrent","File Sharing","-","-",0.00,0,-
,"Unknown","-"> -
```

# LAB 2.24. Application Visibility and Control

## Objectives

This lab shows how to use AVC policies to block access to certain web applications.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

Configure an overall bandwidth limit on WSA to download from teh Internet with a speed of 50 Mbps. For Employees group set up file access limits and block downloading of following files: ZIP archives, RAR archives, EXE files and *.torrent files.

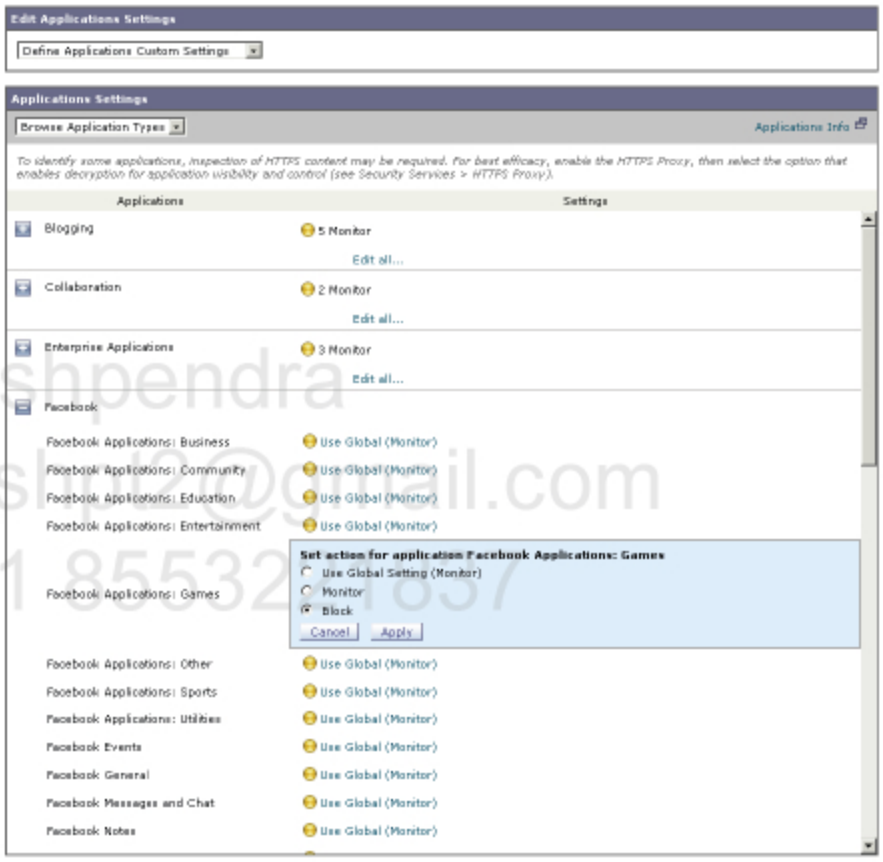
## Configuration

Complete these steps:

**Step 1** Configure global bandwidth limit for all users.

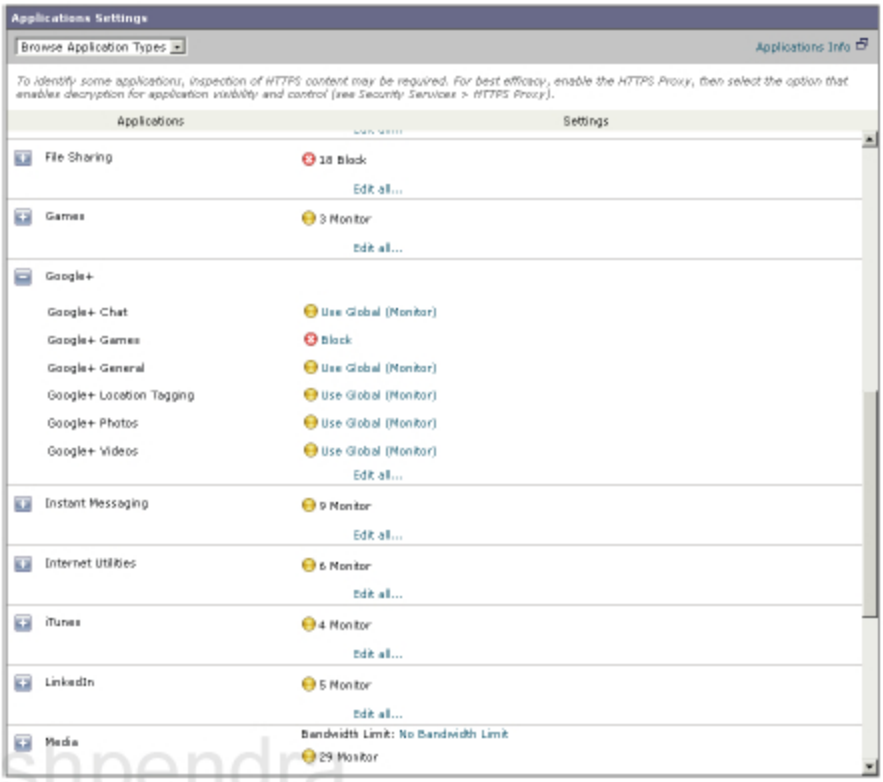
- Go to **Web Security Manager > Access Policies** and link in **Applications** column for **Employees** policy. Expand **Facebook** section and click **Use Global (Monitor)** option next to **Facebook Applications: Games**. Select **Block** option and click **Apply.**

Access Policies: Applications Visibility and Control: Employees



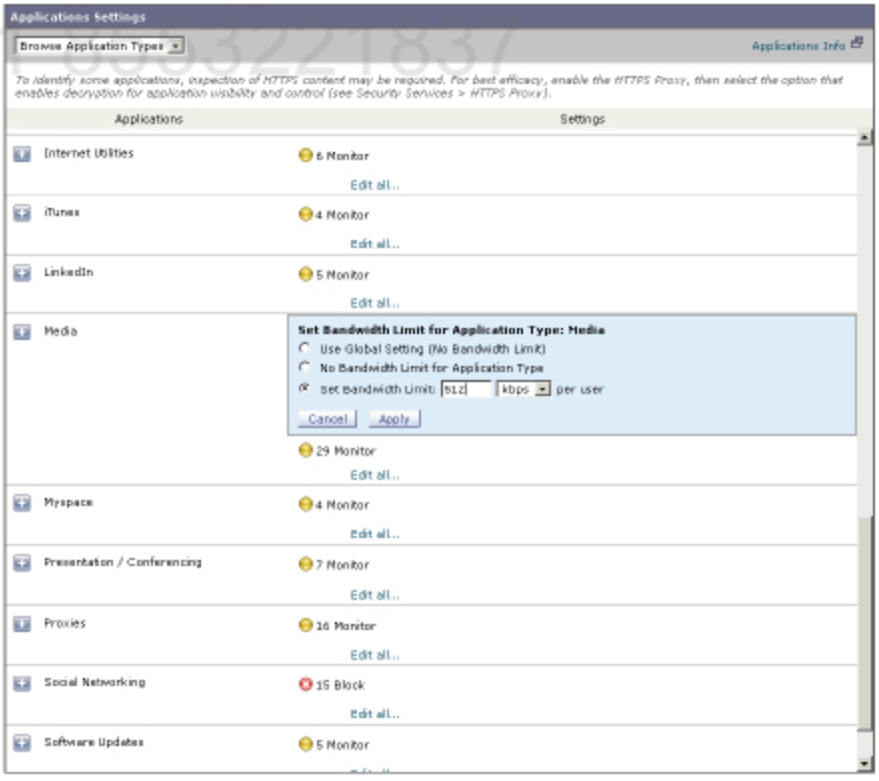



- Click **Edit all...** link next to **File Sharing** category and select **Block** and **Apply**. Do the same for **Google+ Games**.

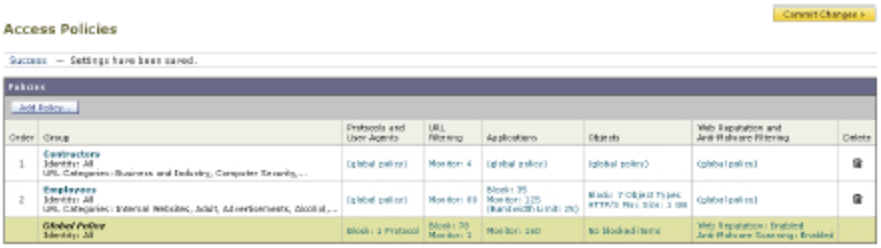





- Click **No Bandwidth Limit** link next to **Media** section and select **Set Bandwidth Limit** option and set it to **512 kbps**. Click **Submit**.

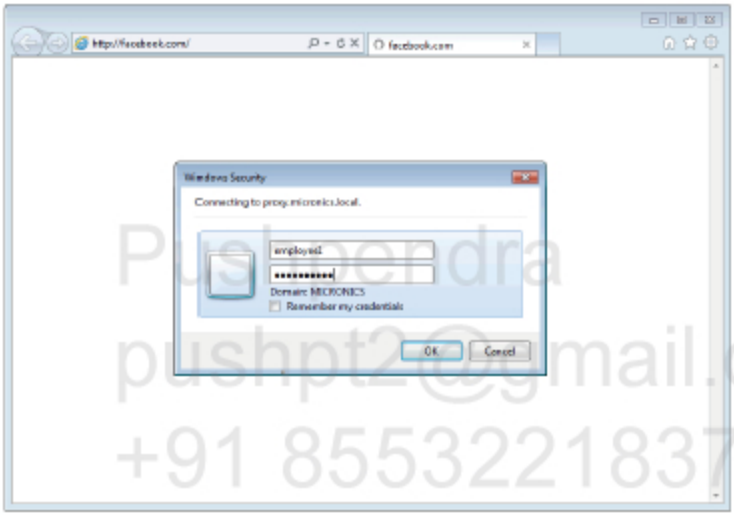



- Review the configuration and click **Commit Changes**.



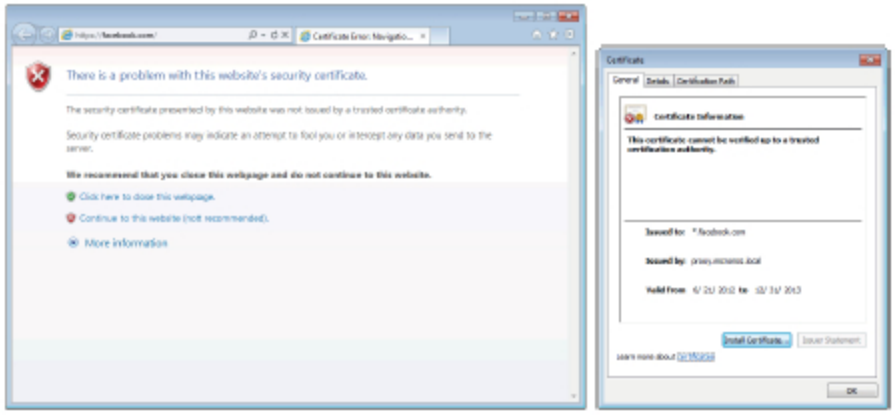

## Verification

- On Win7 client PC open up web browser and go to facebook.com. Authenticate as user from Employees group.

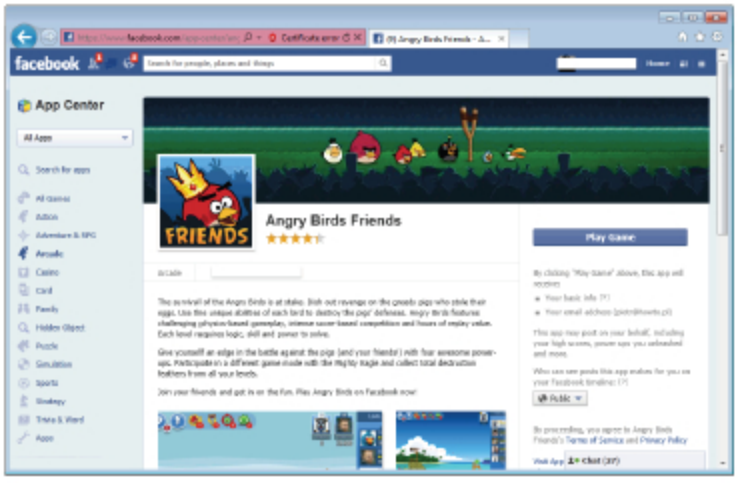




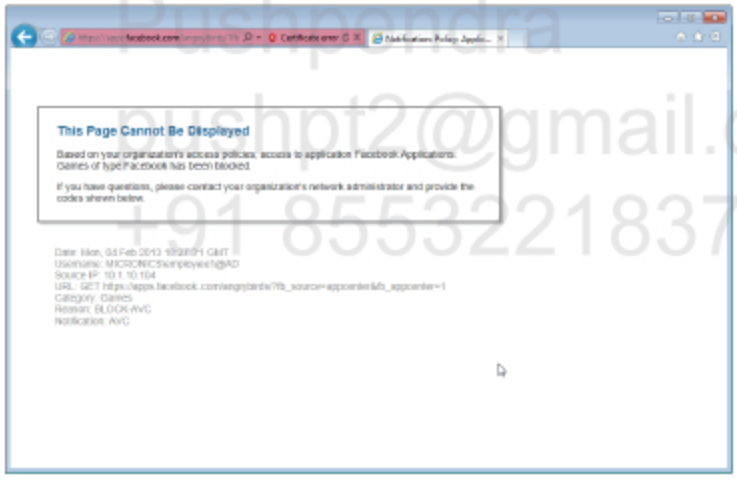

- Facebook redirects all requestst automatically to HTTPS. Hence, having decryption policy for all sites enabled, we should intercept that session. The WSA sends caertificate that is not trusted by the client.



- Go to games section and try to launch a game. You can directly go to facebook.com/appcenter/angrybirds and click **Play Game**.

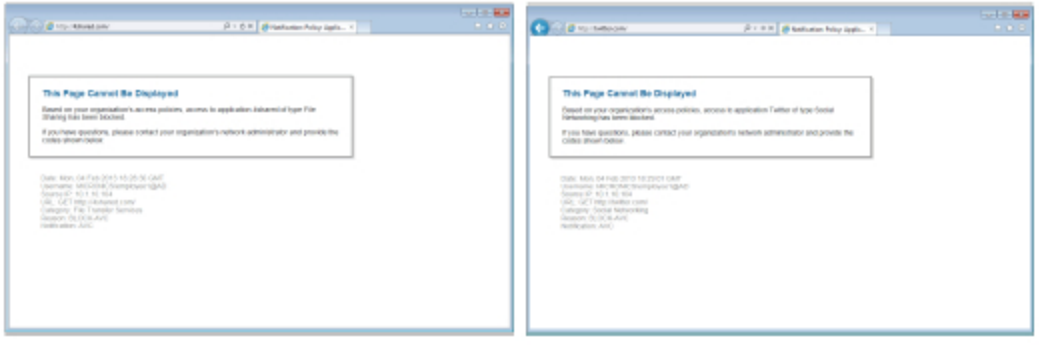



- The connection should not be allowed.






- Try to connect to some File Sharing websites and Social Networking websites. The connections should be denied.



# LAB 2.25. Web Reputation and DVS

## Objectives

This lab shows how to use WBRS and DVS to secure web traffic.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

Configure WSA policy for Employees to automatically block websites if they Web Reputation score is -4 and below (from -4 to -10). Also, if a website provides viruses, encrypted content or is unscannable for whatever reason, block it automatically.

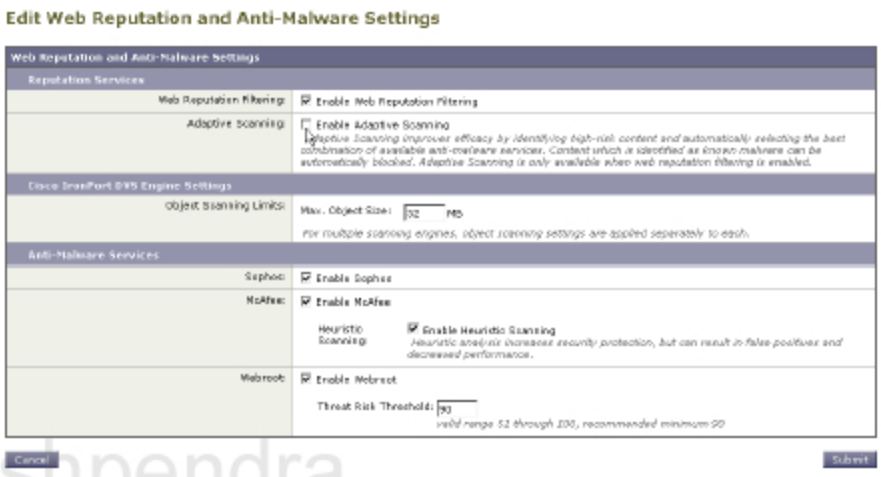
There is a special website www.ihaveabadreputation.com hosted by Cisco to test web repuatation. It's reputation is -9.5 so it should be blocked by WSA. Configure exceltion for all users to allow access to that website.

## Configuration

Complete these steps:

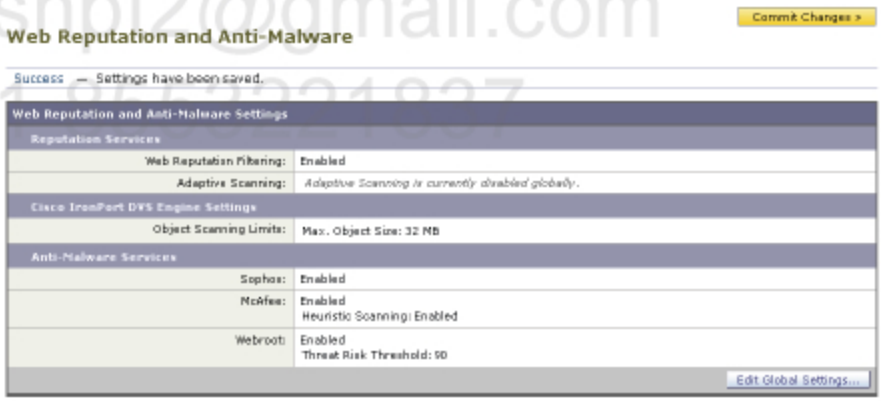
**Step 1** Disable Adaptive Scanning.

- Go to **Security Services > Web Reputation and Anti-Malware** and click **Edit Global Settings...** Uncheck **Enable Adaptive Scanning** option and click **Submit.**



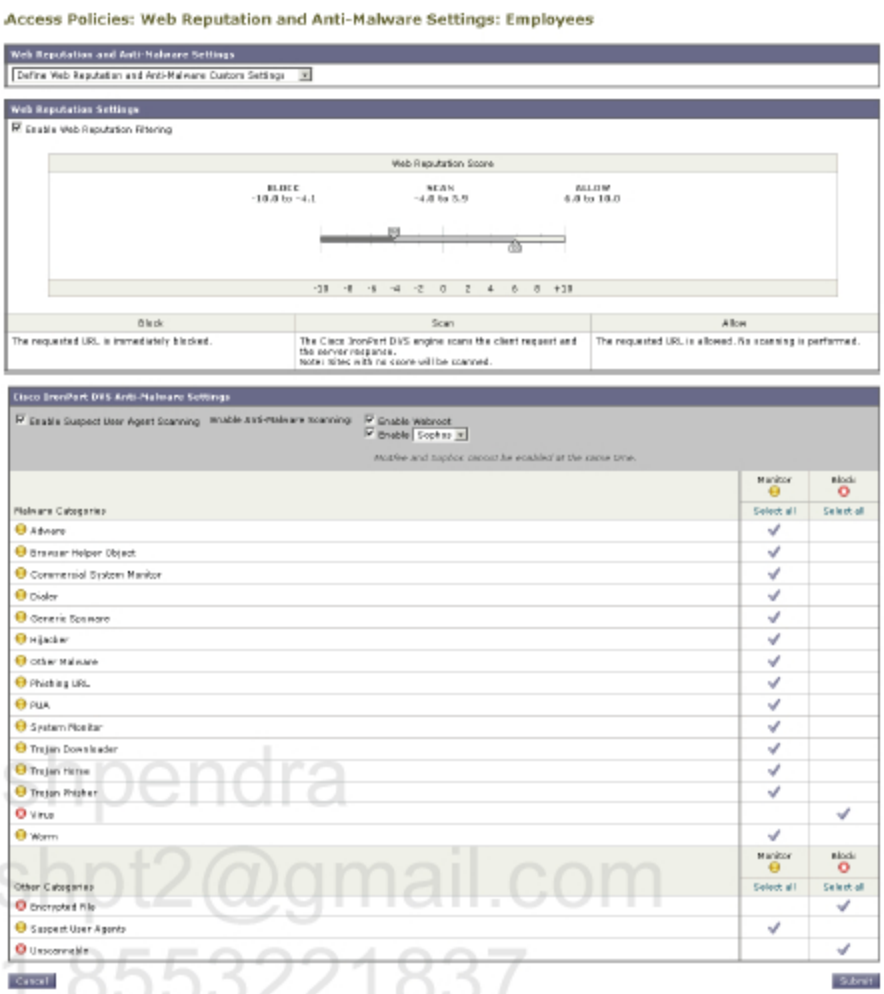



- Review the configuration and click **Commit Changes**.



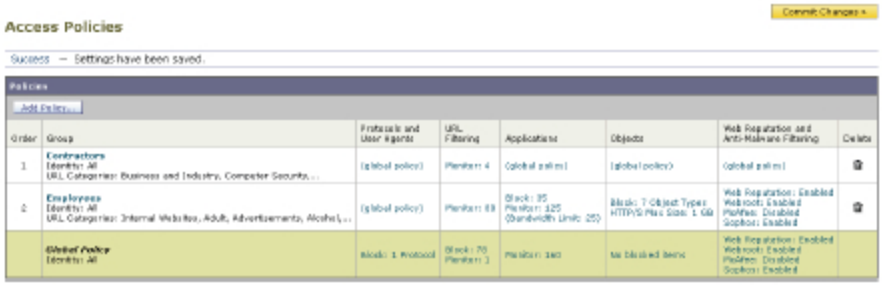

**Step 2** Change WBRS threshold for Employees.

- Go to **Web Security Manager > Access Policies** and click link in **Web Reputation and Anti-Malware Filtering** column for **Employees** policy. Select option **Define WEB Reputation and Anti-Malware Custom Settings** from drop-down list and move the slider from -6 position to -4. Check **Block** option for categories: **Virus, Encrypted file** and **Unscannable**. Click **Submit**.





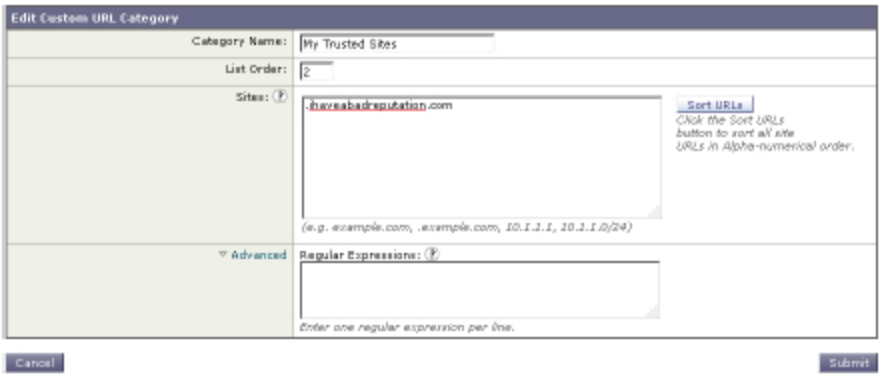

- Review the configuration and click **Commit Changes**.




**Step 3** Configure custom URL category and access policy to whitelist specified URL.

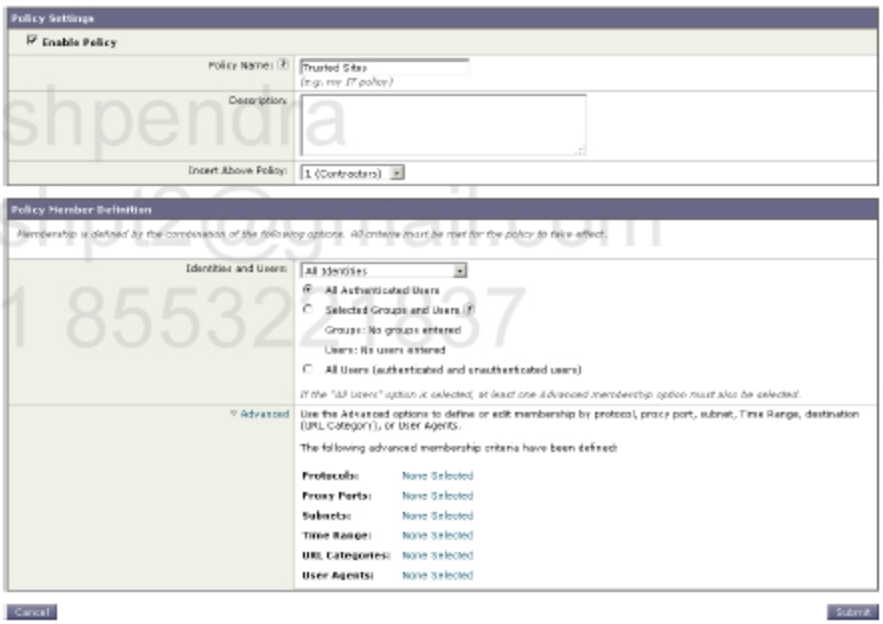
- Go to **Web Security Manager > Custom URL Categories** and click **Add Custom Category…** Enter a name for category e.g. **My Trusted Sites** and add '.ihaveabadreputation.com' domain to the list. Click **Submit**.

Custom URL Categories: Add Category




- Go to **Web Security Manager > Access Polices** and click **Add Policy…** Enter a name for new policy e.g. **Trusted Sites** and insert is at the top of policy list. Click **None Selected** next to **URL Categries**.

Access Policy: Add Group

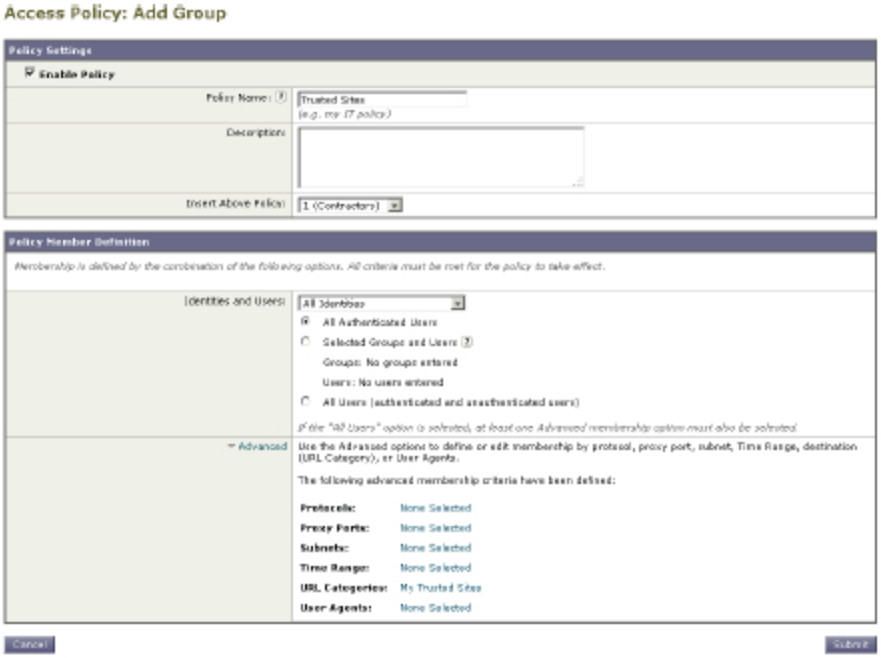





- Pick **My Trusted Sites** category on the list and click **Done**.

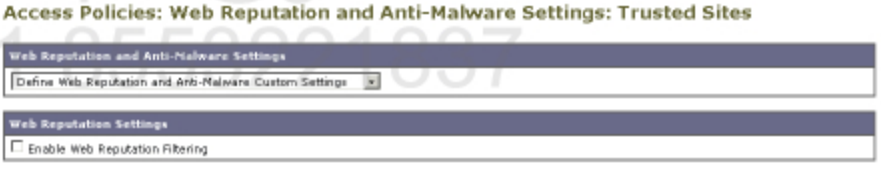
Access Policies: Policy "Trusted Sites": Membership by URL Categories


- Review the policy and click **Submit**.

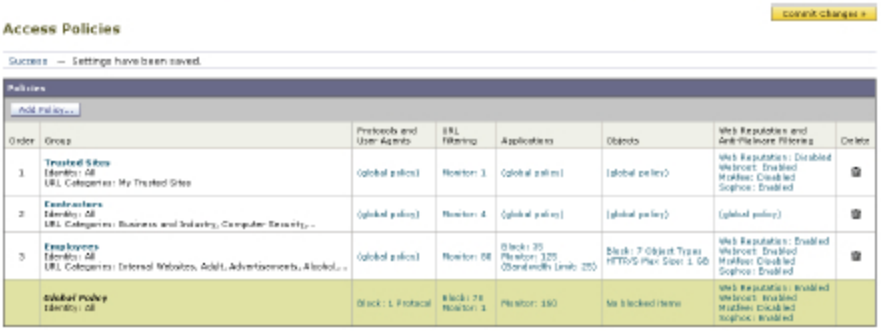



- Click link in **Web Reputation and Anti-Malware Filtering** column for **Trusted Sites** policy. Select option **Define WEB Reputation and Anti-Malware Custom Settings** from drop-down list and uncheck **Enable Web Reputation Filetring** option. Click **Submit**.



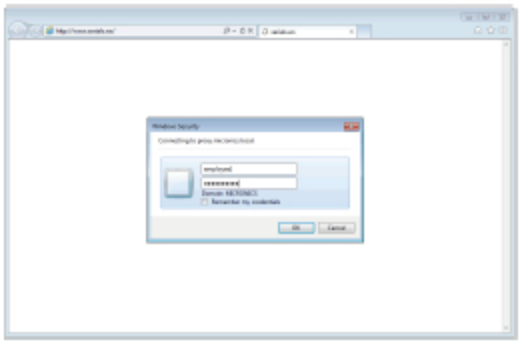


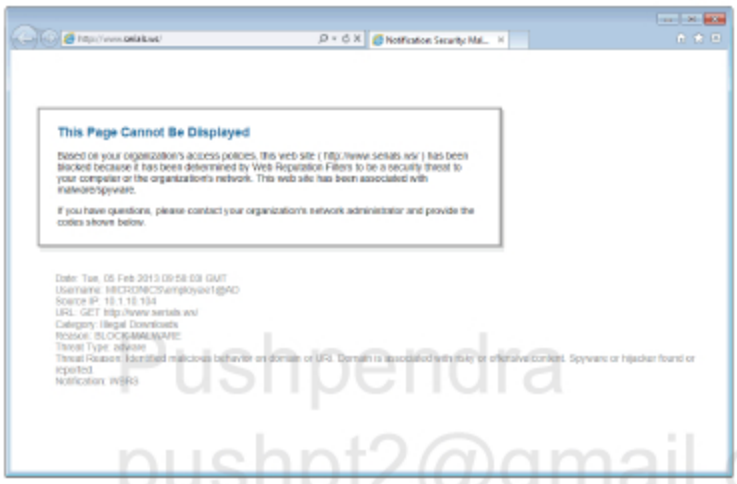

- Review the configuration and click **Commit Changes**.




## Verification

- On Win7 client PC open up web browser and go to some website with bad reputation. Authenticate as user from Employees group. You might need to accept AUP before continueing. This connection should be denied.








```
1360058283.139 1 10.1.10.104 TCP_DENIED/403 0 GET http://www.serials.ws/
"MICRONICS\employee1@AD" NONE/- - BLOCK_WBRS_12-Employees-DefaultGroup-NONE-NONE-NONE-
NONE <IW_ildl,-6.4,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_ildl,-,"-
","adware","Unknown","Unknown","-","-",0.00,0,-,"-","-"> -
```

- Go to www.google.com and see the log.

```
1360058344.078 487 10.1.10.104 TCP_MISS/200 31422 GET http://www.google.com/
"MICRONICS\employee1@AD" DIRECT/www.google.com text/html ALLOW_WBRS_12-Employees-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_srch,8.2,-,"-",-,-,-,-,"-",-,-,-,"-",-,-
,"-","-",-,-,IW_srch,-,"-","-","Google","Search Engine","-","-",516.17,0,-,"-","-"> -
```

- Go to www.ihaveabadreputation.com and see the log.

```
1360058386.537 878 10.1.10.104 TCP_MISS/403 11975 GET
http://www.ihaveabadreputation.com/ "MICRONICS\employee1@AD"
DIRECT/www.ihaveabadreputation.com text/html MONITOR_CUSTOMCAT_12-Trusted_Sites-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <C_My_T,-9.5,0,"-",0,0,0,-,"-",-,-,-,"-",1,-
,"-","-",-,-,IW_csec,-,"-","othermalware","Unknown","Unknown","-","-",109.11,0,-
,"Unknown","-"> -
```

# LAB 2.26. Transparent Proxy with ASA

## Objectives

This lab shows how integrate WSA with ASA to do transparen proxy services for users.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| WSA | M1 | 10.1.10.80/24 |
| | P1 | 10.1.30.80/24 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| ASA | 0/0 (outside) | 100.2.2.10/24 |
| | 0/1 (inside) | 10.1.10.10/24 |
| | 0/2 (dmz) | 10.1.30.10/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |
| Win7 | NIC | 10.1.10.104/24 |
| AD | NIC | 172.31.1.200/24 |



## Task

Reconfigure WSA to provide Transparent Proxy services to all users. THE WSA should use it's M1 interface and talk to ASA using WCCP v2 protocol. Messages exchanged between WSA and ASA should be authenticated using 'cisco123' shared secret. Enable Transparent proxy for http and HTTPS. Disable CONNECT method for explicit proxy.

## Configuration

Complete these steps:

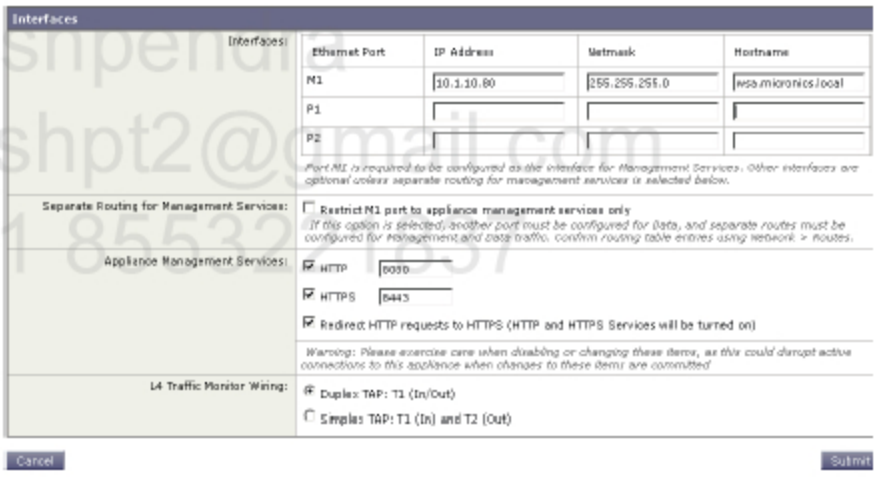
**Step 1** Configure WCCP on ASA.

```
!
access-list WCCP permit tcp 10.1.10.0 255.255.255.0 any eq 80
access-list WCCP permit tcp 10.1.10.0 255.255.255.0 any eq 443
!
wccp 90 redirect-list WCCP password cisco123
wccp interface inside 90 redirect in
!
```

**Step 2** Reconfigure interfaces on WSA.

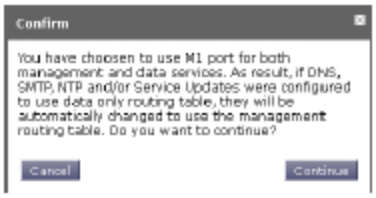
- Go to **Network > Interfaces** and click **Edit Settings…** Uncheck **Restrict M1 port to appliance management services only** option and erase P1 interface configuration. Click **Submit.**

Edit Interfaces

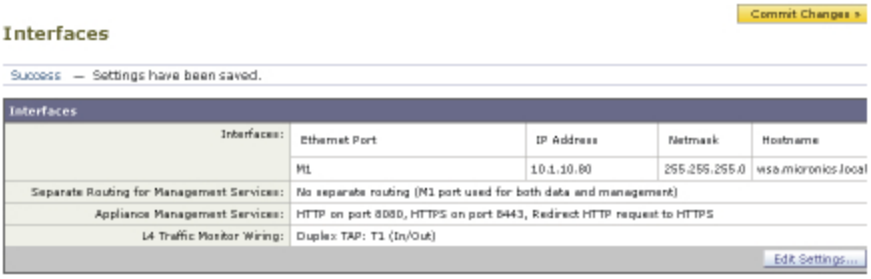





- Note the following message. Click **Continue**.




- Review the configuration and click **Commit Changes**.



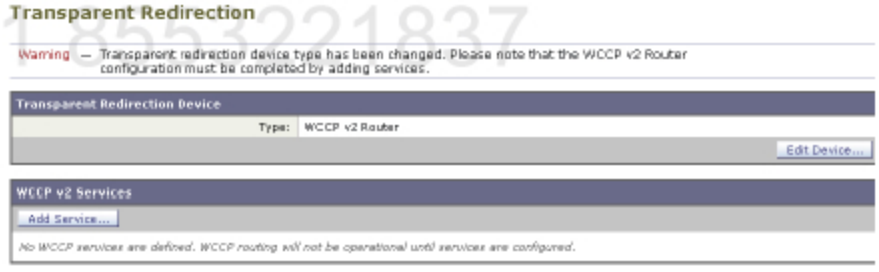

**Step 2** Enable Transparent Proxy services.

- Go to **Network > Transparent Redirection** and click **Edit Device…**

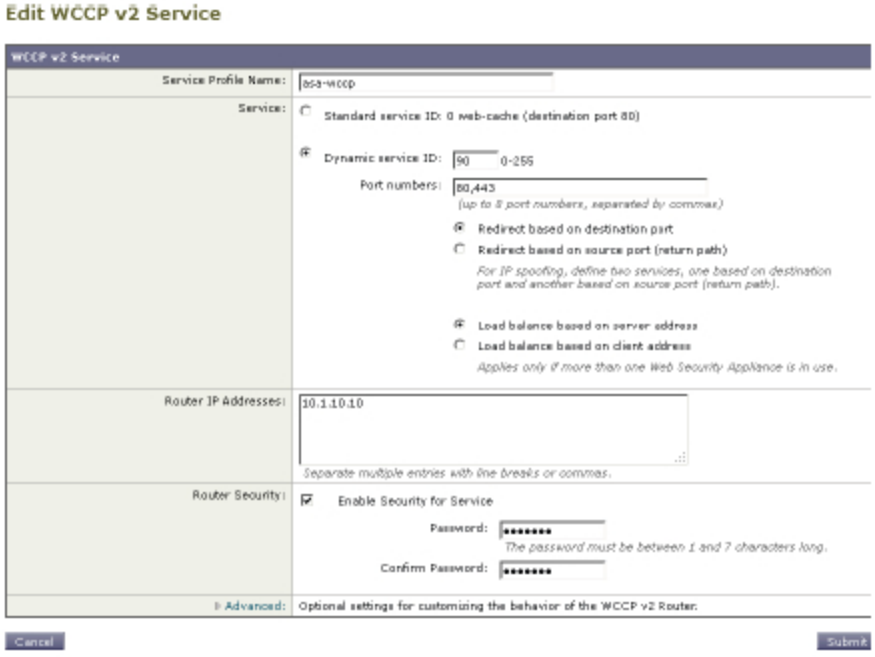

- From the drop-down list select **WCCP v2 Router** and click **Submit**.




- Click **Add Service…**

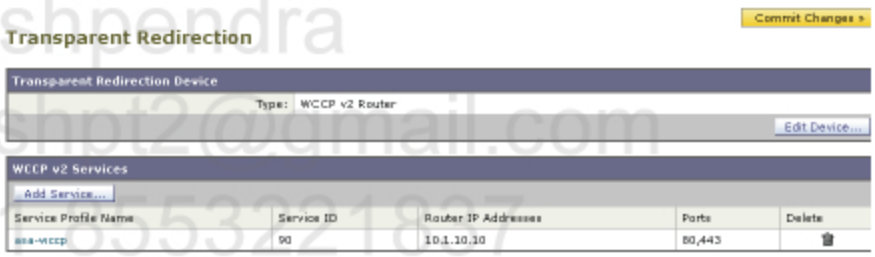



- Provide name for WCCP service e.g. **asa-wccp** and select **Dynamic service ID** option. Set the ID to **90** and associate **Port Numbers** of **80,443**. Put 10.1.10.10 (ASA's inside interface IP) as **Router IP Address** and tick **Enable Security for Service** option configuring 'cisco123' as password. Click **Submit**.



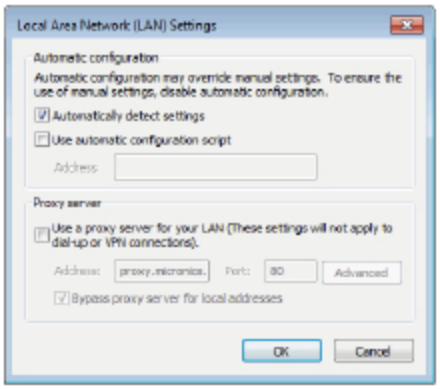

- Review configuration and click **Commit Changes**.





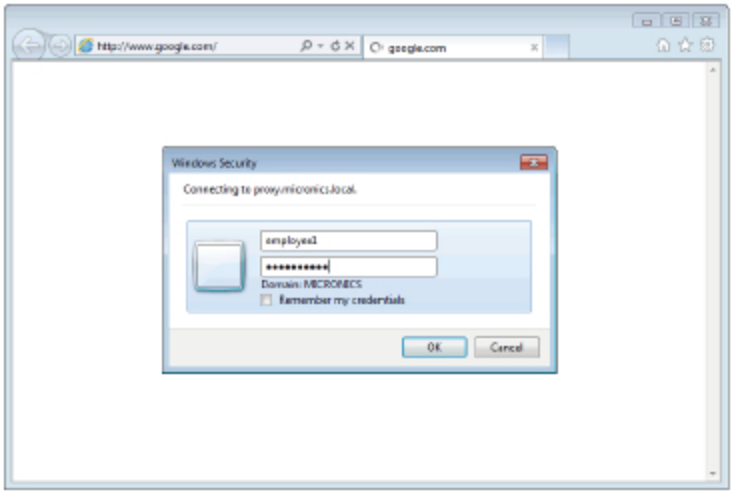

**Step 3** Win7 client PC configuration.

- Open up web browser and go to **Tools > Internet Options > Connections > LAN Settings** and uncheck **Use a proxy server for your LAN** option.



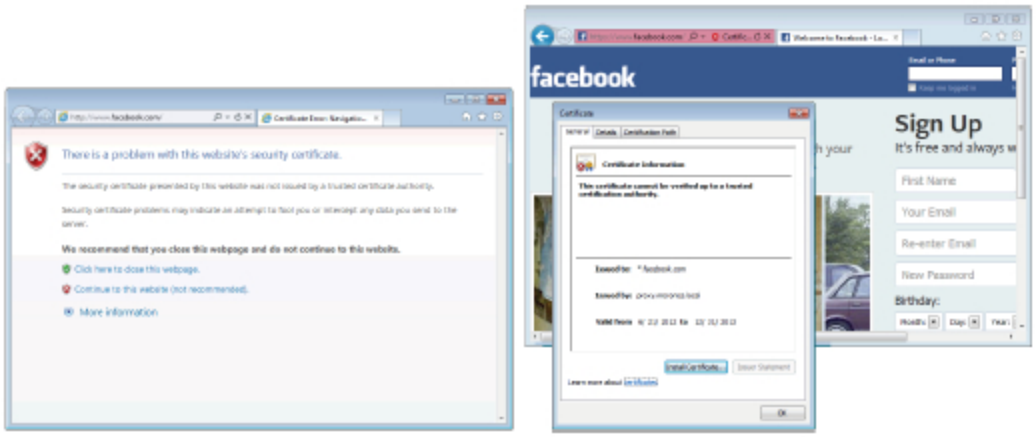
## Verification

- On Win7 client PC open up web browser and go to http://www.google.com. Authenticate as user from Employees group.




```
// there is 401 returned by the proxy which is authentication request.

1360089008.110 0 10.1.10.104 TCP_DENIED/401 0 GET
http://proxy.micronics.local/B0000D0000N0001F0000S0000R0004/http://www.google.com/ -
NONE/- - OTHER-NONE-NONE-NONE-NONE-NONE-NONE <-,-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-
","-",-,-,-,-,"-","-","-","-","-","-",0.00,0,-,"-","-"> -

// after authentication the request is proceeded normally

1360089020.203 413 10.1.10.104 TCP_MISS/200 31422 GET http://www.google.com/
"MICRONICS\employee1@AD" DIRECT/www.google.com text/html ALLOW_WBRS_12-Employees-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_srch,8.2,-,"-",-,-,-,-,"-",-,-,-,"-",-,-
,"-","-",-,-,IW_srch,-,"-","-","Google","Search Engine","-","-",608.66,0,-,"-","-"> -
```

- Connect to http://www.facebook.com. The FB is redirecting the user to HTTPS by default, so you should get certificate error (the certificate is not trusted because it is signed by WSA). You should be connected after accepting the certificate.



```
        // HTTP request to facebook.com
1360089089.513 271 10.1.10.104 TCP_MISS/302 405 GET http://www.facebook.com/
"MICRONICS\employee1@AD" DIRECT/www.facebook.com text/html DEFAULT_CASE_12-Employees-
DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_snet,4.7,0,"-",0,0,0,-,"-",-,-,-,"-",-,-
,"-","-",-,-,IW_snet,-,"-","-","Facebook General","Facebook","-","-",11.96,0,-
,"Unknown","-"> -

        // TCP Connect to 443, redirected to WSA.

1360089089.703 183 10.1.10.104 TCP_MISS_SSL/200 0 TCP_CONNECT 31.13.64.23:443
"MICRONICS\employee1@AD" DIRECT/31.13.64.23 - DECRYPT_AVC_7-DefaultGroup-DefaultGroup-
NONE-NONE-NONE-DefaultGroup <IW_snet,4.7,1,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-
,IW_snet,-,"-","-","Facebook General","Facebook","Encrypted","-",0.00,0,-,"-","-"> -

        // check connection table on ASA - there should be NO connections from Win7 PC

ASA1(config)# sh conn
11 in use, 77 most used
TCP outside 2.16.216.40:443 inside 10.1.10.80:57688, idle 0:00:07, bytes 32361, flags UIO
TCP outside 2.16.216.40:443 inside 10.1.10.80:57686, idle 0:00:07, bytes 27805, flags UIO
TCP outside 2.16.216.40:443 inside 10.1.10.80:57685, idle 0:00:07, bytes 74840, flags UIO
TCP outside 2.16.216.40:443 inside 10.1.10.80:57684, idle 0:00:07, bytes 75426, flags UIO
TCP outside 2.16.216.40:443 inside 10.1.10.80:57683, idle 0:00:08, bytes 11142, flags UIO
TCP outside 2.16.216.40:443 inside 10.1.10.80:57682, idle 0:00:08, bytes 83528, flags UIO
TCP outside 2.16.216.40:443 inside 10.1.10.80:57680, idle 0:00:14, bytes 2593, flags UfFrIO
TCP outside 2.16.216.40:443 inside 10.1.10.80:57679, idle 0:00:14, bytes 45467, flags UfFrIO
TCP outside 195.12.233.137:443 inside 10.1.10.80:57666, idle 0:00:15, bytes 2548, flags UIO
TCP outside 31.13.64.23:443 inside 10.1.10.80:53205, idle 0:00:17, bytes 30380, flags UIO
```



## Check ASA WCCP commands output.

```
ASA1(config)# deb wccp packet
WCCP-PKT:D90: Received valid Here_I_Am packet from 10.1.10.80 w/rcv_id 00000112
WCCP-PKT:D90: Sending I_See_You packet to 10.1.10.80 w/ rcv_id 00000113


ASA1(config)# sh wccp

Global WCCP information:
    Router information:
        Router Identifier:                  100.2.2.10
        Protocol Version:                   2.0

    Service Identifier: 90
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           11464
        Redirect access-list:               WCCP
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           6
```

```
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0


ASA1(config)# sh wccp 90 detail

WCCP Cache-Engine information:
        Web Cache ID:          10.1.10.80
        Protocol Version:      2.0
        State:                 Usable
        Initial Hash Info:     00000000000000000000000000000000
                               00000000000000000000000000000000
        Assigned Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                               FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:        256 (100.00%)
        Packets Redirected:    11464
        Connect Time:          00:00:18


ASA1(config)# sh wccp 90 service

WCCP service information definition:
        Type:           Dynamic
        Id:             90
        Priority:       240
        Protocol:       6
        Options:        0x00000012
        --------
            Hash:       DstIP
            Alt Hash:   -none-
            Ports:      Destination:: 80 443 0 0 0 0 0 0
```

**This page is intentionally left blank.**

# Advanced
# CCIE SECURITY v4
# LAB WORKBOOK

# Identity Management

# ACS

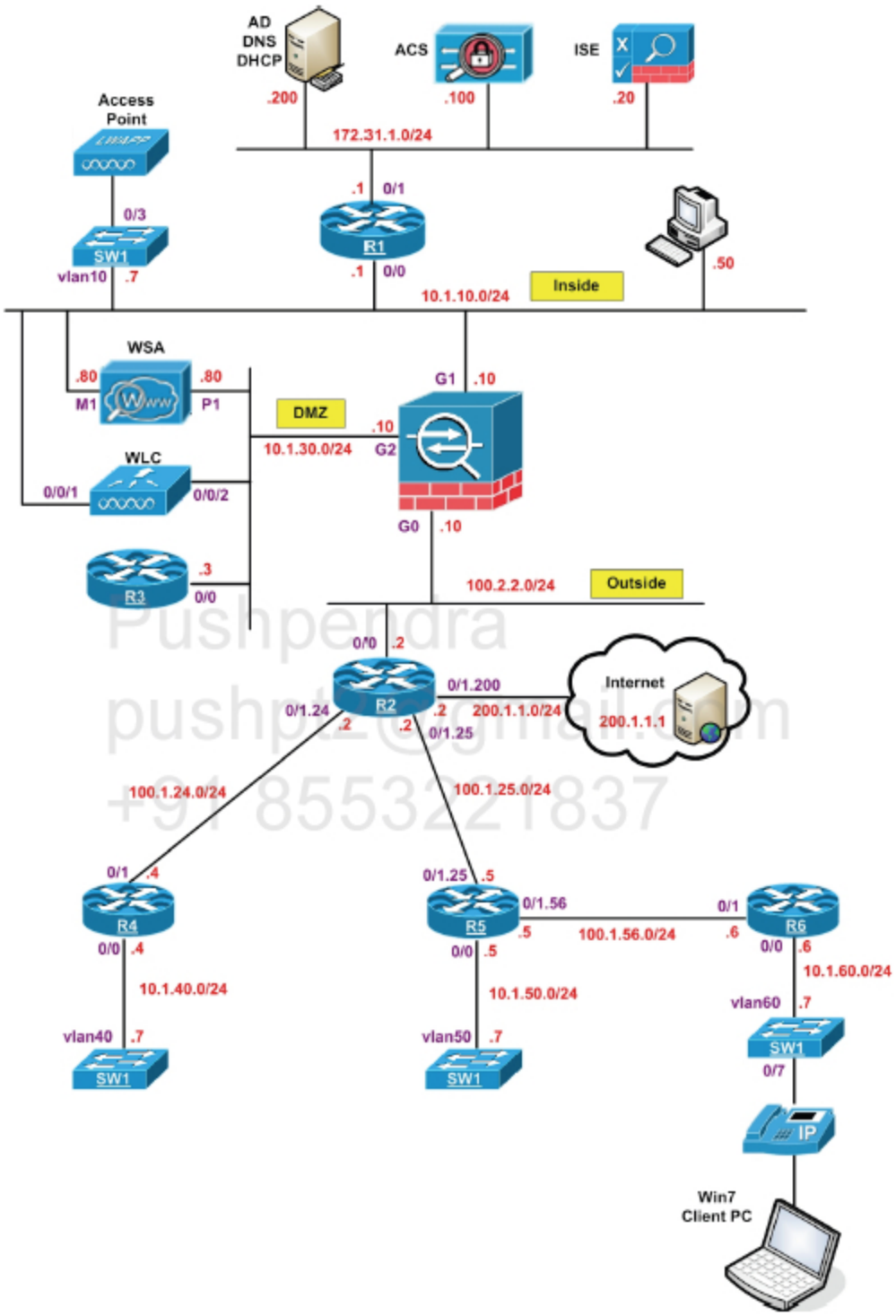


**Narbik Kocharians**
**CCIE #12410 (R&S, Security, SP)**
**CCSI #30832**

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

www.MicronicsTraining.com

# Logical Topology for ACS labs






ACS 5 is connected to the network behind Router1 and has IP address of 172.31.1.100. Default gateway should be set to R1.

Management access to ACS should be allowed from WinXP PC (10.1.10.50).

# LAB 2.27. ACS Bootstrapping

## Objectives

This lab introduces Cisco Secure Access Control Server v5.3 and verifies basic connectivity with other network elements.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| ACS | NIC | 172.31.1.100 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| WinXP | NIC | 10.1.10.50/24 |

# Task 1 – Verify ACS installation

Connect to ACS console using SSH and username/password of **admin/Micronics1**. Check and note the following:

- ACS application version
- ACS daemon status
- Interface configuration
- Routing table (with default gateway)
- Clock configuration
- Timezone configuration

Configure the following:

- NTP server set to 172.31.1.1
- Connect to the GUI and install the license located on WinXP desktop (ACS5.lic)



## Configuration

Complete these steps:

**Step 1** Run Putty and connect to IP address of 172.31.1.100

**Step 2** Verify that ACS is installed properly

```
ACS5/admin# show application
<name>          <Description>
acs             Cisco Secure Access Control System 5.3
```

Cisco ACS is an application installed on underlying operating system called Cisco ADE. Once you're connected to ADE you must check what applications are installed. Then you can use application name (in our case 'acs') in all other commands.

**Step 3** Check ACS version

```
ACS5/admin# show application version acs

Cisco ACS VERSION INFORMATION
```

```
----------------------------
Version : 5.3.0.40
Internal Build ID : B.839.EVAL
```

The main version is 5.3 and the patch level is 40. The build depends on the development stage and also indicates that we use evaluation version of ACS. You can install production license or evaluation license (90 days). Remember that if the ACS was installed with 60GB disk (minimum) there will be no option to run it with no-eval license. The 60GB is a minimum value and can only be used in lab environment.

## Step 4 Check status of ACS processes

```
ACS5/admin# show application status acs

ACS role: PRIMARY

Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'view-database'           running
Process 'view-jobmanager'         running
Process 'view-alertmanager'       running
Process 'view-collector'          running
Process 'view-logprocessor'       running
```



If there is other status than 'running' it means theres something wrong with a particular ACS subsystem/process. To fix that you can try to restart ACS application using 'application stop acs' and then 'application start acs'. Be patient as it may take a while to start all ACS processes.

## Step 5 Check interface configuration and verify IP address and netmask

```
ACS5/admin# show interface
eth0      Link encap:Ethernet  HWaddr 00:50:56:AE:83:F6
          inet addr:172.31.1.100  Bcast:172.31.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feae:83f6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12645 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16627 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1105589 (1.0 MiB)  TX bytes:19717105 (18.8 MiB)
          Interrupt:177 Base address:0x2000
```

Make sure that you see RX and TX packets and no error counters increasing. This is a first indicator that something can be wrong with connectivity. If you do not see eth0 interface that usually means the interface is down.

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1939218 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1939218 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:300253955 (286.3 MiB)  TX bytes:300253955 (286.3 MiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```



## Step 6 Check routing table and default gateway

```
ACS5/admin# show ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
172.31.1.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         172.31.1.1      0.0.0.0         UG    0      0        0 eth0
```

## Step 7 Check basic connectivity to the gateway and to other network elements

```
ACS5/admin# ping 172.31.1.1
PING 172.31.1.1 (172.31.1.1) 56(84) bytes of data.
64 bytes from 172.31.1.1: icmp_seq=0 ttl=255 time=10.0 ms
64 bytes from 172.31.1.1: icmp_seq=1 ttl=255 time=0.642 ms
64 bytes from 172.31.1.1: icmp_seq=2 ttl=255 time=0.690 ms
64 bytes from 172.31.1.1: icmp_seq=3 ttl=255 time=0.784 ms

--- 172.31.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.642/3.049/10.083/4.061 ms, pipe 2

ACS5/admin# ping 10.1.10.10
PING 10.1.10.10 (10.1.10.10) 56(84) bytes of data.
```

```
--- 10.1.10.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3027ms
```

Note that you cannot reach ASA firewall at this stage. This is because the ASA has no route back to network 172.31.1.0/24. You will fix this later.

```
ACS5/admin# ping 10.1.10.50
PING 10.1.10.50 (10.1.10.50) 56(84) bytes of data.
64 bytes from 10.1.10.50: icmp_seq=0 ttl=127 time=0.812 ms
64 bytes from 10.1.10.50: icmp_seq=1 ttl=127 time=1.02 ms
64 bytes from 10.1.10.50: icmp_seq=2 ttl=127 time=1.02 ms
64 bytes from 10.1.10.50: icmp_seq=3 ttl=127 time=10.8 ms

--- 10.1.10.50 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 0.812/3.429/10.860/4.291 ms, pipe 2
```

**Step 8** Check the name server and domain configuration. Verify if DNS works asking to resolve FQDN of **acs5.micronics.local**



```
ACS5/admin# show running-config | inc name
hostname ACS5
ip domain-name micronics.local
ip name-server 172.31.1.200
username admin password hash $1$Vlgou3Zx$hWKQ2lqIKFZF./OlFJ/Wi1 role admin

ACS5/admin# ping 172.31.1.200
PING 172.31.1.200 (172.31.1.200) 56(84) bytes of data.
64 bytes from 172.31.1.200: icmp_seq=0 ttl=128 time=0.551 ms
64 bytes from 172.31.1.200: icmp_seq=1 ttl=128 time=0.331 ms
64 bytes from 172.31.1.200: icmp_seq=2 ttl=128 time=0.401 ms
64 bytes from 172.31.1.200: icmp_seq=3 ttl=128 time=0.415 ms

--- 172.31.1.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.331/0.424/0.551/0.082 ms, pipe 2

ACS5/admin# nslookup acs5.micronics.local
Trying "acs5.micronics.local"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1641
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;acs5.micronics.local.          IN      ANY

;; ANSWER SECTION:
```

```
acs5.micronics.local.   3600    IN      A       172.31.1.100

Received 54 bytes from 172.31.1.200#53 in 0 ms
```

## Step 9 Check clock and timezone configuration

```
ACS5/admin# show clock
Sun Jan  6 12:23:45 UTC 2013

ACS5/admin# show timezone
UTC
```

If there is a different timezone configured you can always change it to the correct value using 'clock timezone UTC' command in the global configurtion. To check what timezone names are available use 'show timezones' command.

## Step 10 Configure NTP



```
ACS5/admin(config)# ntp server 172.31.1.1
The NTP server was modified.
If this action resulted in a clock modification, you must restart ACS.
ACS5/admin(config)# exit

ACS5/admin# write mem
Generating configuration...

ACS5/admin# show ntp
Primary NTP   : 172.31.1.200

unsynchronised
  time server re-starting
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset
jitter
==============================================================================
==
 127.127.1.0     LOCAL(0)        10 l   42   64    7    0.000    0.000
0.002
 172.31.1.1      LOCAL(1)         8 u   44   64   77    0.733    4.846
3.029

Warning: Output results may conflict during periods of changing
synchronization.

ACS5/admin# show ntp
Primary NTP   : 172.31.1.1
```

```
synchronised to NTP server (172.31.1.1) at stratum 9
   time correct to within 452 ms
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset
jitter
==============================================================================
==
 127.127.1.0     LOCAL(0)        10 l   45   64   77    0.000    0.000
0.002
*172.31.1.1      LOCAL(1)         8 u   44   64   77    0.733    4.846
3.029


Warning: Output results may conflict during periods of changing
synchronization.
```

NTP synchronization is very important especially when ACS is a part of Active Directory domain. If you plan to join AD then clock between Domain Controller and ACS must be synchronized. The NTP related issues are causing most problems with AD integration.
You can also check application logs when syncing with NTP.
Note that ACS may not synchronize with a source which is not reliable (the source gets time from its local clock).

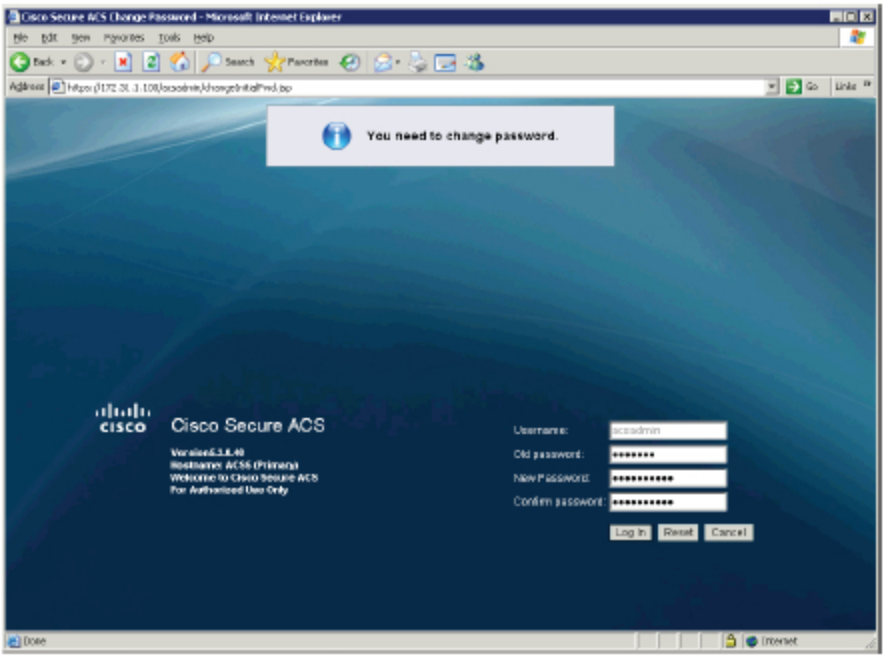


```
ACS5/admin# show logging application | in ntp
Nov  8 11:38:05 ACS5 ntpd[29716]: ntpd 4.2.0a@1.1190-r Mon Jul 28 11:03:50
EDT 2008 (1)
Nov  8 11:38:05 ACS5 ntpd: ntpd startup succeeded
Nov  8 11:38:05 ACS5 ntpd[29716]: precision = 2.000 usec
Nov  8 11:38:05 ACS5 ntpd[29716]: Listening on interface wildcard,
0.0.0.0#123
Nov  8 11:38:05 ACS5 ntpd[29716]: Listening on interface wildcard, ::#123
Nov  8 11:38:05 ACS5 ntpd[29716]: Listening on interface lo, 127.0.0.1#123
Nov  8 11:38:05 ACS5 ntpd[29716]: Listening on interface eth0,
172.31.1.100#123
Nov  8 11:38:05 ACS5 ntpd[29716]: kernel time sync status 0040
Nov  8 11:38:05 ACS5 ntpd[29716]: frequency initialized 0.000 PPM from
/var/lib/ntp/drift
Nov  8 11:41:20 ACS5 ntpd[29716]: synchronized to LOCAL(0), stratum 10
Nov  8 11:41:20 ACS5 ntpd[29716]: kernel time sync disabled 0041
Nov  8 11:42:23 ACS5 ntpd[29716]: synchronized to 172.31.1.1, stratum 8
Nov  8 11:42:24 ACS5 ntpd[29716]: kernel time sync enabled 0001
```

**Step 11** Connect through the GUI and install the license. Open up web browser (IE or FF) and enter the following URL https://172.31.1.100/acsadmin

- Authenticate as **acsadmin/default** and change the default

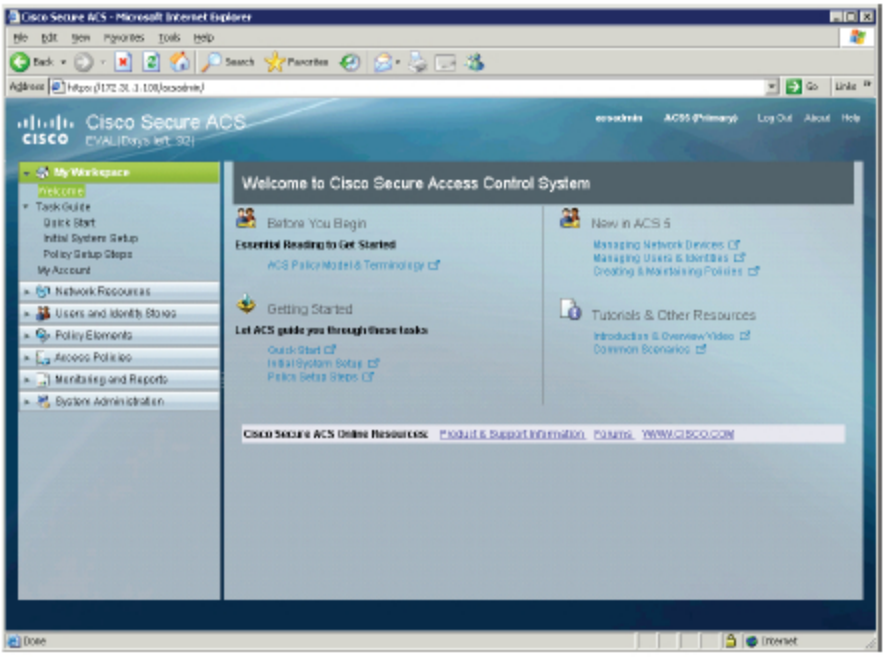
password to **Micronics1**.






- Provide a license file ACS5.lic (should be on WinXP desktop)


- Once license file is installed, the ACS is ready for further configurtion



# LAB 2.28. Setup AAA clients

## Objectives

This lab shows how to configure AAA clients in ACS and perform basic authentication using RADIUS and TACACS+ protocols.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| ACS | NIC | 172.31.1.100 |
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| SW1 | Vlan10 | 10.1.10.7/24 |
| WinXP | NIC | 10.1.10.50/24 |

## Task 1 – Create a user in ACS internal database

Create a new user with username of **student1** with a password of **student123** in ACS Internal Identity Store. The user should belong to **Students** user group.

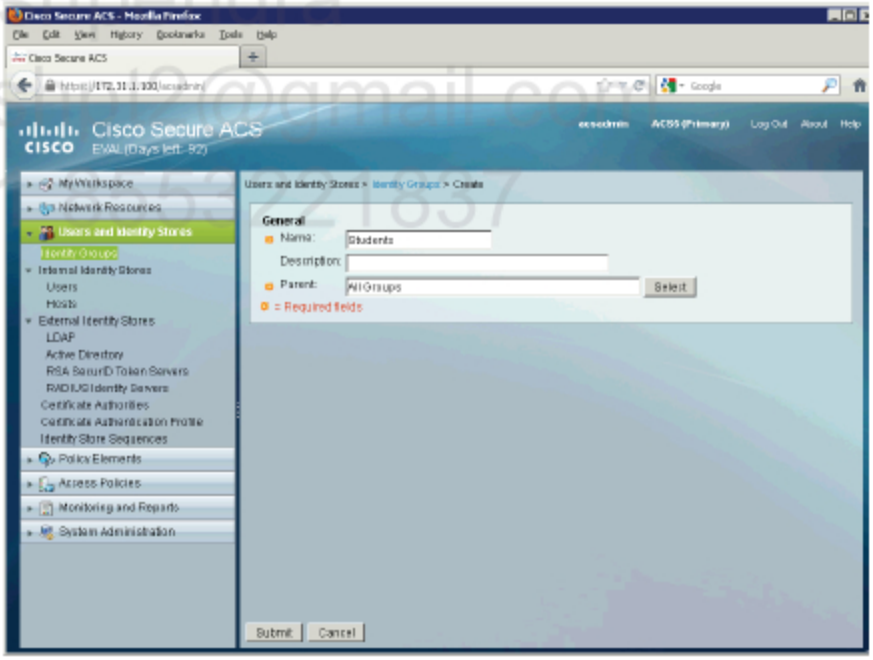
### Configuration

Complete these steps:

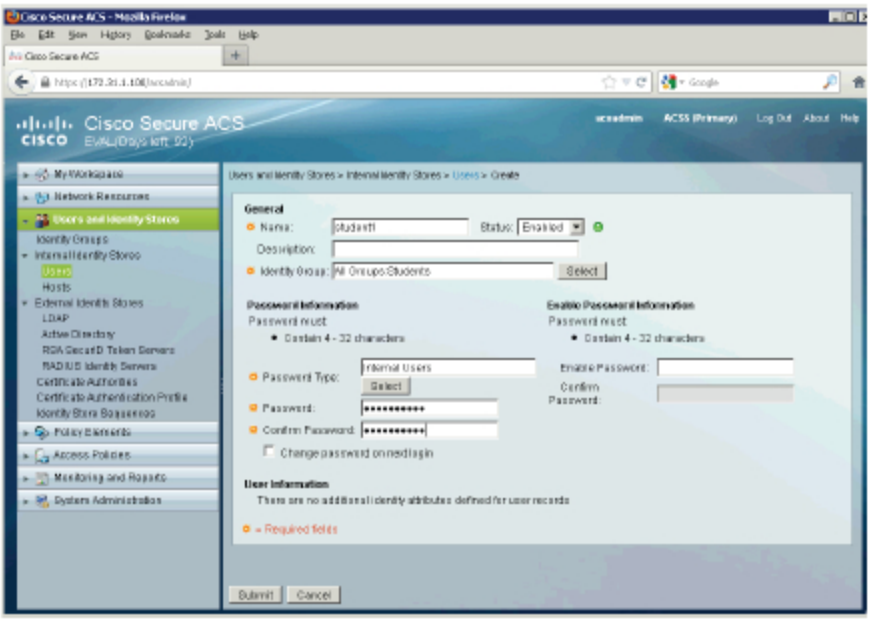
**Step 1** Connect to ACS from WinXP PC and authenticate using **acsadmin**. Add new entry to Device Type and Location NDGs (Network Device Groups).

- Go to **Users and Identity Stores > Identity Groups** and click **Create**. Add name **Students** under **All Groups** and click **Submit**.






- Go to **Users and Identity Stores > Users** and click **Create**. Add new user with a name of **student1** and password of **student123**, select **Students** under **Identity Groups** and click **Submit**.




## Verification

There is no **Verification** for this task.

## Task 2 – Adding the router as AAA client in ACS

Configure R1 router as AAA client in ACS using TACACS+ with secret key of **cisco123.** Make sure the device is sourcing TACACS+ traffic from its loopback0 interface and uses only one TCP connection for whole AAA conversation.

The new AAA client should be added as Device Type = Routers in Location = HQ. Configure AAA on the router and use **test aaa** command to verify your solution.

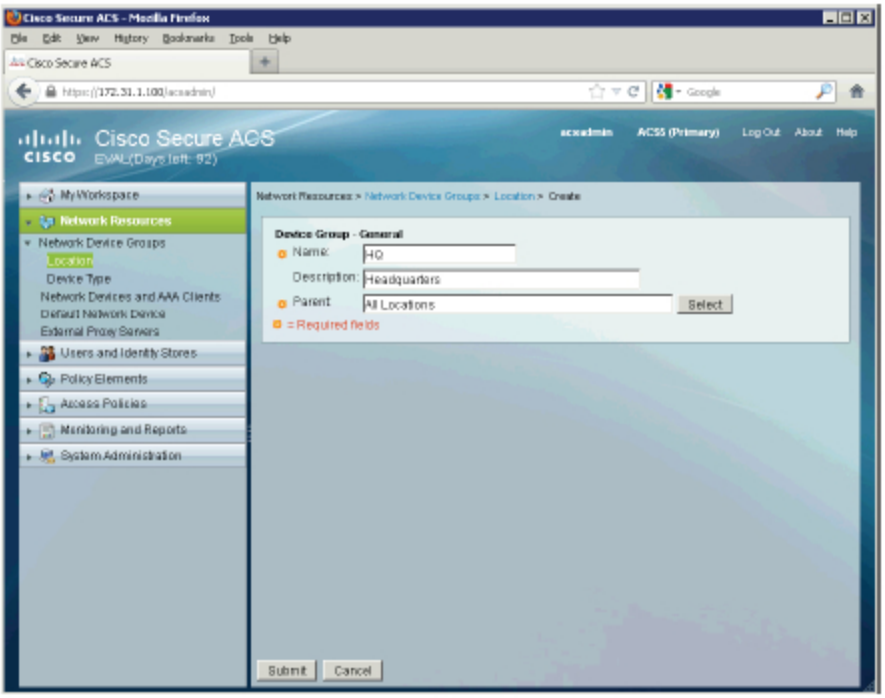
### Configuration

Complete these steps:

**Step 1** Connect to ACS from WinXP PC and authenticate using **acsadmin**. Add new entry to Device Type and Location NDGs (Network Device Groups).

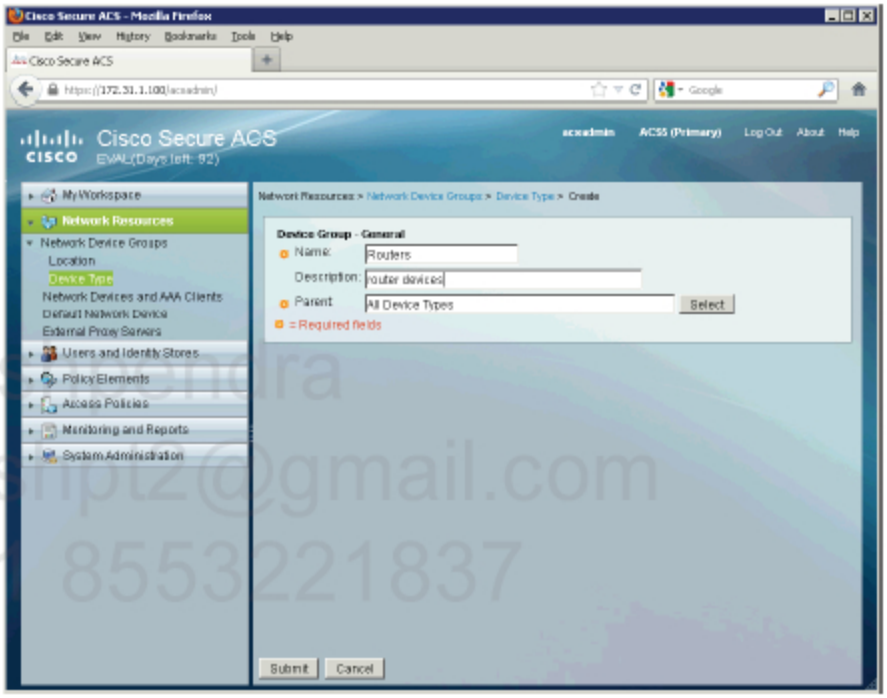
- Go to **Network Resources > Network Device Groups > Location** and click **Create**. Add name **HQ** under **All Locations** and click **Submit**.





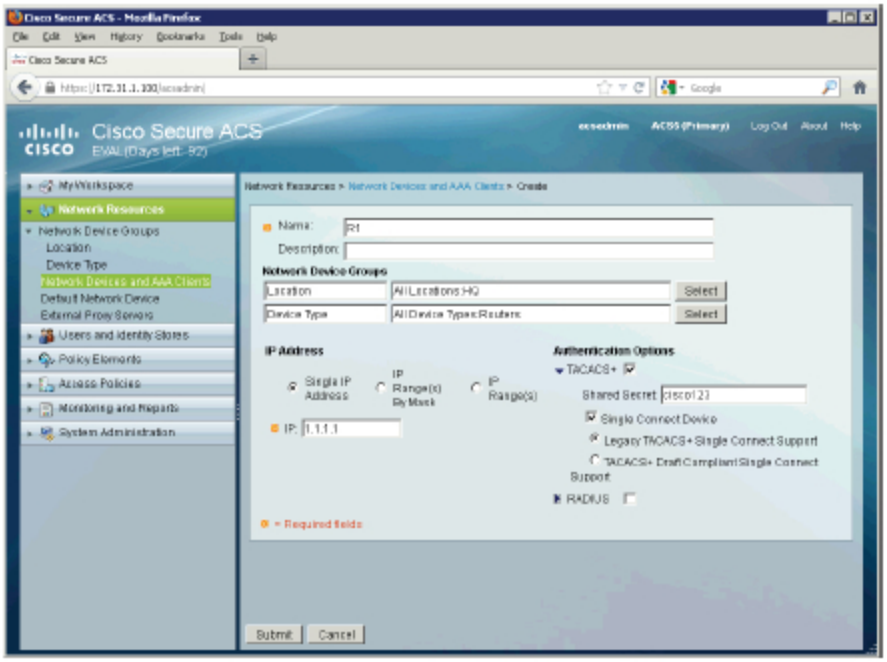
Devices can be differentiated based on their type and/or location. There are two pre-defined containers in ACS: one for location and second for type. This information can be further used in authorization policies and it is recommended to add new devices to correct categories.

- Go to **Network Resources > Network Device Groups > Device Type** and click **Create**. Add name **Routers** under **All Device Types** and click **Submit**.




**Step 2** Add new AAA client to the ACS.

- Go to **Network Resources > Network Device and AAA Clients** and click **Create**. Add new client with name of **R1**, select Location = **HQ** and Device Type = **Routers**, configure IP address of **1.1.1.1**, select TACACS+ as a protocol and configure **Shared Secret** of **cisco123**. Select **Single Connect Device** option and click **Submit**.




**Step 3** Router configuration.

```
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
aaa new-model
!
tacacs server ACS
 address ipv4 172.31.1.100
 key cisco123
 single-connection
!
```



Notice that we do not need to configure 'aaa authentication…' command here. It is enough to specify TACACS server in the configuration and then we can use it in 'test aaa' command.
Also note that you can specify AAA server in three ways:

1. using old command structure like 'tacacs-server host…'
2. using new command structure as configured above
3. using AAA groups with commands like 'aaa group server…'

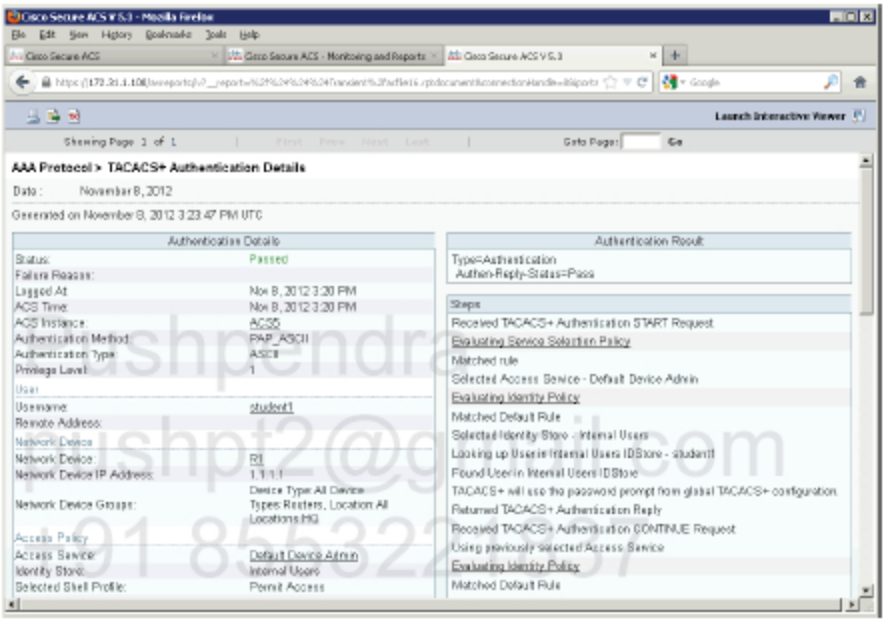
The first option is deprecated and is not recommanded to be used in IOS 15.0 and above.

## Verification

Use **test aaa** command to check user authentication.

```
R1#test aaa group tacacs+ student1 student123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

Check logs on ACS. Go to **Monitoring and Reports** and launch **Authentications – TACACS – Today** report.



## Task 3 – Adding the switch as AAA client in ACS

Configure SW1 switch as AAA client in ACS using RADIUS with secret key of **cisco123.** Make sure the device is sourcing RADIUS traffic from vlan10 interface with IP address of 10.1.10.7/24.

The new AAA client should be added as Device Type = Switches in Location = HQ. Configure AAA on the switch and use **test aaa** command to verify your solution.

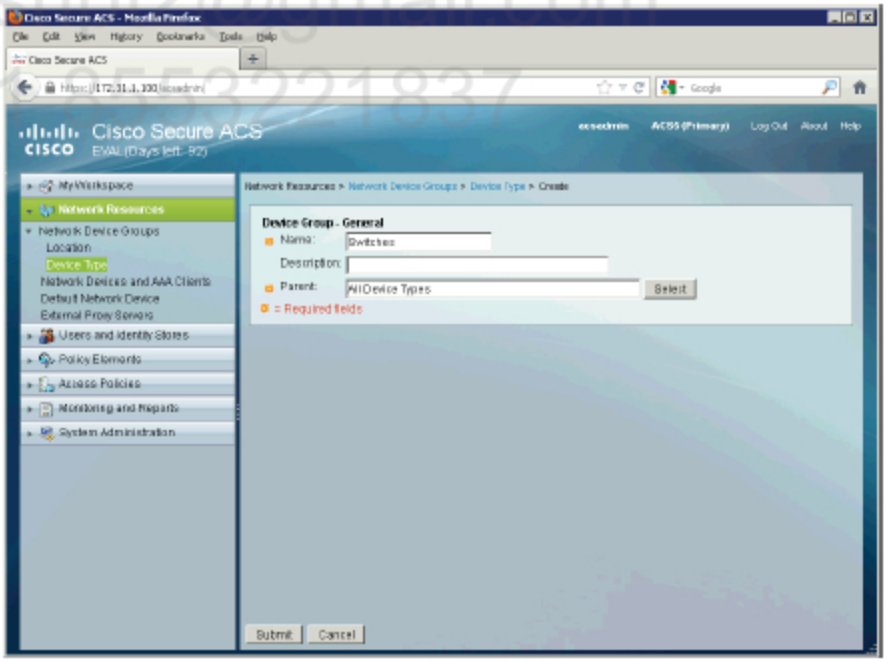
### Configuration

Complete these steps:

**Step 1** Connect to ACS from WinXP PC and authenticate using **acsadmin**.

- Go to **Network Resources > Network Device Groups > Device Type** and click **Create**. Add name **Switches** under **All Device Types** and click **Submit**.

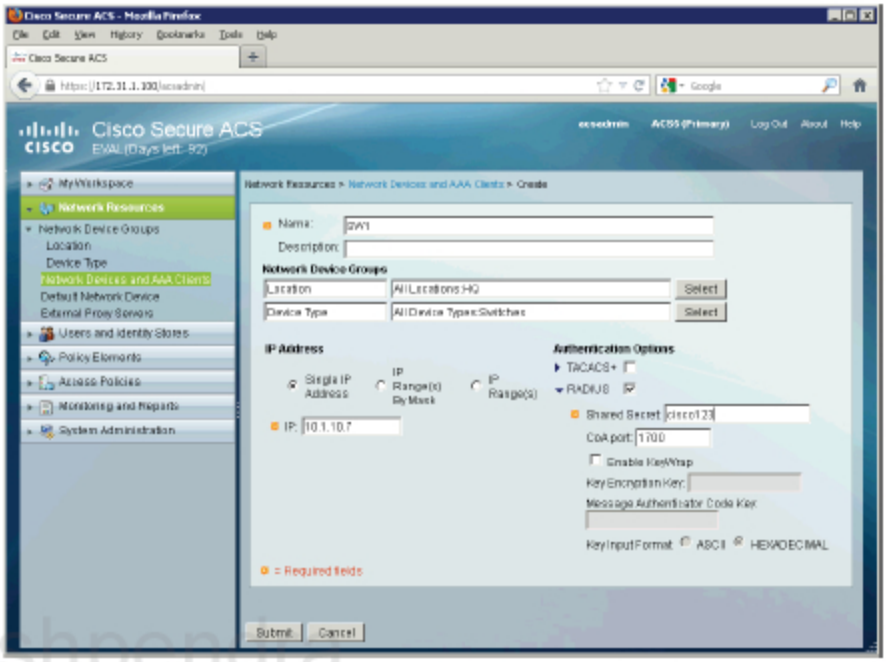





**Step 2** Add new AAA client to the ACS.

- Go to **Network Resources > Network Device and AAA Clients** and click **Create**. Add new client with name of **SW1**, select Location = **HQ** and Device Type = **Switches**, configure IP address of **10.1.10.7**,

select RADIUS as a protocol and configure **Shared Secret** of **cisco123** and click **Submit**.






**Step 3** Switch configuration.

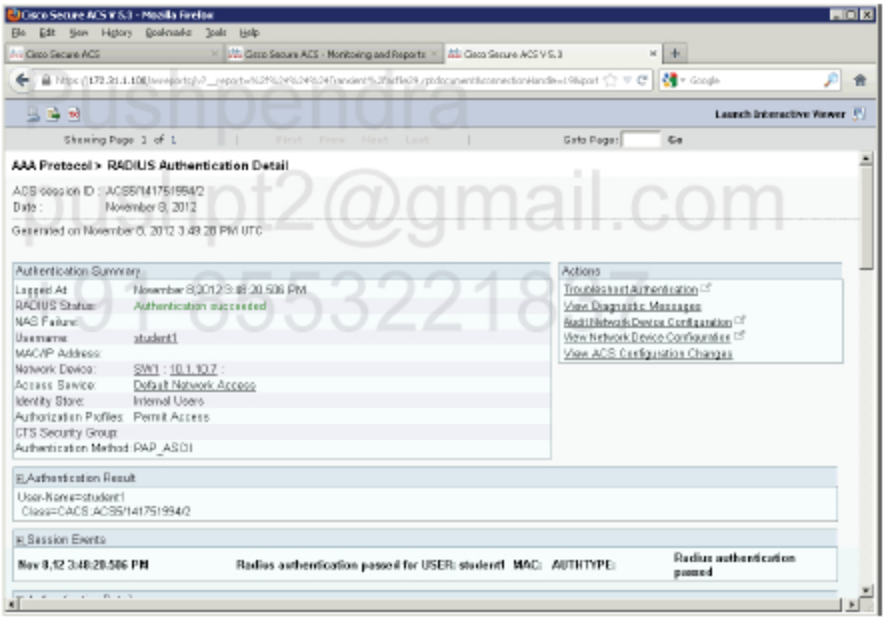
```
!
interface Vlan10
 ip address 10.1.10.7 255.255.255.0
!
aaa new-model
!
ip default-gateway 10.1.10.1
ip radius source-interface Vlan10
radius-server host 172.31.1.100 key cisco123
!

Note that when you enable 'aaa new-model' the router will start asking
for Username/Password on VTY lines. You must either configure 'login
authentication' command on VTYs or create some backup/fallback username
in the local router's database.
It is always recommended to have such local user account.

!
username backup password backup
!
```

## Verification

Use **test aaa** command to check user authentication.

```
SW1#ping 172.31.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/205/1015 ms

SW1#test aaa group radius student1 student123 legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

Check logs on ACS. Go to **Monitoring and Reports** and launch **Authentications – RADIUS – Today** report.



# LAB 2.29. User authentication and authorization (IOS)

## Objectives

This lab shows how to configure routers to perform basic authentication and authorization.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |



*The router may authenticate remote users using its local user database. Every user connecting to the router must be authenticated and authorized to perform specific tasks. There are 16 privilege levels on the router. The levels are defined with a number of 0 through 15. By default only three levels are configured:*

- *Level 0 – basic level which is accessible by every user with only access to basic commands like "exit" and "logout"*
- *Level 1 – user without administrative permissions has this level assigned. Usually every user in non-privileged router mode (non-enable mode) is on this level*
- *Level 15 – user with administrative privileges is on this level. All commands are available on this level by default. When a user enters "enable" command and authenticates successfully, he/she is by default authorized on level 15.*

*Rest of the levels (2-14) is user configurable so that we can assign commands to a specific level. The term "assign" is unfortunate here as we are able to only "move" a command between levels. For example, if a command is by default on level 15 (remember that most of the configuration commands are available only on level 15) we can move it down to level 10. However, this command will be now available on level 10 and on all levels above up to level 15.*
*The router can have different passwords for every privilege level, so that we can authenticate to a specified level by entering command "enable <lvl>".*
*Note that because most configuration commands are available on level 15, entering level 5 for example will not give us any access to other commands. We need to "move" specific commands first to that level to be able to use them.*

## Task 1 – Local user authentication on router

On R2 configure local user "luser1" with a password of "luser1" and allow him to issue only "show" commands when accessing the router using TELNET session. Use strong encryption for enable password if possible. You are not allowed to use any AAA commands or views to accomplish this task.

### Configuration

Complete these steps:

**Step 1** Configure R2 as follows:

```
!
privilege exec all level 3 show
!
enable secret level 3 enable3
!
username luser1 password luser1
!
line vty 0 4
 login local
!
```



### Verification

```
R1#telnet 100.2.2.2
Trying 100.2.2.2 ... Open


User Access Verification

Username: luser1
Password:
R2>show priv
    ^              ← "show" command is not accessible for level 1 user - it is now on
level 3
% Invalid input detected at '^' marker.

R2>enable
% No password set ← there's no enalble password for level 15 configured

R2>enable 3
Password:         ← "enable3" password works for privilege level 3 only

R2#sh priv
Current privilege level is 3
```

```
R2#show ?
  aaa                       Show AAA values
  aal2                      Show commands for AAL2
  access-expression         List access expression
  access-lists              List access lists
  accounting                Accounting data for active sessions
  adjacency                 Adjacent nodes
  alarm-interface           Display information about a specific Alarm
                            Interface Card
  aliases                   Display alias commands
  alignment                 Show alignment information
  alps                      Alps information
  appfw                     Application Firewall information
  appletalk                 AppleTalk information
  arap                      Show Appletalk Remote Access statistics
  archive                   Archive of the running configuration information
  arp                       ARP table
  ase                       Display ASE specific information
  async                     Information on terminal lines used as router
                            interfaces
  auto                      Show Automation Template
  autoupgrade               Show autoupgrade related information
  backhaul-session-manager  Backhaul Session Manager information

<...snip...>

R2#conf t
      ^ ← higher level commands are not accessible for level 3 user
% Invalid input detected at '^' marker.

R2#exit

[Connection to 100.2.2.2 closed by foreign host]
R1#
```

## Task 2 – Local user authentication and authorization on router

On R2 configure user “admin15” with password of ”admin15” and allow him to access all commands when accessing the router via TELNET session as well as via CONSOLE connection.

*A user can have a privilege level assigned. This can be done when creating a user in the router's local database. Once the user has privilege assigned the router will try to authorize the user to that level while user is connecting.*

### Configuration

Complete these steps:

**Step 1** Configure R2 as follows:

```
!
username admin15 privilege 15 password admin15
!
line con 0
 login local
!
```



### Verification

```
R2 con0 is now available

Press RETURN to get started.


User Access Verification

Username: admin15
Password:
R2#sh priv
Current privilege level is 15
```

This was for Console access. Note that we have landed on level 15 automatically.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#exi
R2#
```

```
R1#telnet 100.2.2.2
Trying 100.2.2.2 ... Open


User Access Verification

Username: admin15
Password:
R2#sh priv
Current privilege level is 15
R2#
```

This was for TELNET access. Note that we have landed on level 15 automatically.

# LAB 2.30. Local user authentication and authorization using AAA (IOS)

## Objectives

This lab shows how to configure routers to perform basic authentication and authorization using AAA.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |

## Task 1 – Local user authentication and authorization using AAA

Configure R2 so that it authenticates CONSOLE connections using AAA services and its local user database. Create a new user "admin" with a password of "admin123". Local password policy should enforce password length for local users (min. 6 characters). To be compliant with company's security policy you need to configure login banner with the following information:

```
Access to this router is restricted!
Disconnect now if you are NOT legitimate user!
```

Set enable password for administrative level (15) to "enable321" with strong encryption. You are allowed to alter previous configuration to accomplish this task.



*Another option is to use AAA (Authentication, Authorization and Accounting) services. Although, it is commonly used in conjunction with external user databases, we can use it for local user database as well. We should use "named" method when configuring AAA. The name assigned to the AAA method is used on specific line (console, VTY, AUX). There is also "default" method that by default enforces AAA service on every line on the router.*
*Be careful here, because when we use "aaa authentication login default local" command without first creating a username in the local database, we'd be effectively blocked out of the router.*
*The router can also enforce some basic password policy to be compliant with best practices and security standards.*

### Configuration

Complete these steps:

**Step 1** Configure R2 as follows:

```
!
aaa new-model
aaa authentication login CON local
aaa authentication banner &
Enter TEXT message.  End with the character '&'
```

```
Access to this router is restricted!
Disconnect now if you are NOT legitimate user!
&
!
security passwords min-length 6
username admin password admin123
enable secret enable321
!
line con 0
 login authentication CON
!
```

## Verification

```
R2 con0 is now available

Press RETURN to get started.



Access to this router is restricted!
Disconnect now if you are NOT legitimate user!

Username: admin
Password:

R2>en
Password:
R2#

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#
R2(config)#username test password test
% Invalid Password length - must contain 6 to 25 characters. Password configuration
failed
```



Note that the password is not compliant with our policy.

### Verification (detailed)

```
R2#deb aaa authentication
AAA Authentication debugging is on
R2#deb aaa authorization
AAA Authorization debugging is on


AAA/BIND(00000008): Bind i/f
AAA/AUTHEN/LOGIN (00000008): Pick method list 'CON'
AAA: parse name=tty0 idb type=-1 tty=-1
AAA: name=tty0 flags=0x11 type=4 shelf=0 slot=0 adapter=0 port=0 channel=0
```

```
AAA/MEMORY: create_user (0x49C383EC) user='admin' ruser='NULL' ds0=0 port='tty0'
rem_addr='async' authen_type=ASCII service=ENABLE priv=15 initial_task_id='0', vrf=
(id=0)
AAA/AUTHEN/START (2451440368): port='tty0' list='' action=LOGIN service=ENABLE
AAA/AUTHEN/START (2451440368): console enable - default to enable password (if any)
AAA/AUTHEN/START (2451440368): Method=ENABLE
AAA/AUTHEN(2451440368): Status=GETPASS
AAA/AUTHEN/CONT (2451440368): continue_login (user='(undef)')
AAA/AUTHEN(2451440368): Status=GETPASS
AAA/AUTHEN/CONT (2451440368): Method=ENABLE
AAA/AUTHEN(2451440368): Status=PASS
AAA/MEMORY: free_user (0x49C383EC) user='NULL' ruser='NULL' port='tty0'
rem_addr='async' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
```

## Task 2 – Local user authentication and authorization using AAA

On R2 create a new user "student1" with password of "student1" and assign a privilege level of 6 to that user. User should be authenticated when connecting remotely and authorized to issue the following commands only:

- show startup
- show privilege
- ip route

  all commands starting with "ip" under interface configuration mode

*Assigning a privilege level to the user is an easy task. It will enable the user to access only commands specified on the user's level and below. Commands from higher level must be "moved" down to the user's level to make them available to that user. We do that using "privilege' command where we specify at which configuration mode and privilege level a command can be accessed. When we need to move a command with its all arguments we should use keyword "all".*



### Configuration

Complete these steps:

**Step 1** Configure R2 as follows:

```
!
username student1 privilege 6 password student1
aaa authentication login VTY local
aaa authorization exec VTY local
!
privilege exec level 6 conf t
privilege exec level 6 show startup
privilege exec level 6 show privilege
privilege configure level 6 interface
privilege interface all level 6 ip
privilege configure level 6 ip route
!
line vty 0 4
 login authentication VTY
 authorization exec VTY
!
```

## Verification

```
R1#telnet 100.2.2.2
Trying 100.2.2.2 ... Open

Access to this router is restricted!
Disconnect now if you are NOT logitimate user!

Username: student1
Password:

R2#sh privilege
Current privilege level is 6
```

The user has landed on level 6. As we can see below the user sees the required commands.

```
R2#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  configure        Enter configuration mode
  connect          Open a terminal connection
  credential       load the credential info from file system
  crypto           Encryption related commands.
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  dot11            IEEE 802.11 commands
  emm              Run a configured Menu System
  enable           Turn on privileged commands
  ethernet         Ethernet parameters
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lat              Open a lat connection
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  modemui          Start a modem-like user interface
  mrinfo           Request neighbor and version information from a multicast router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  radius           radius exec commands
  release          Release a resource
  renew            Renew a resource
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
```

```
  set              Set system parameter (not config)
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  ssh              Open a secure shell client connection
  systat           Display information about terminal lines
  tclquit          Quit Tool Command Language shell
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  tn3270           Open a tn3270 connection
  traceroute       Trace route to destination

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#?
Configure commands:
  beep       Configure BEEP (Blocks Extensible Exchange Protocol)
  call       Configure Call parameters
  default    Set a command to its defaults
  end        Exit from configure mode
  exit       Exit from configure mode
  help       Description of the interactive help system
  interface  Select an interface to configure
  ip         Global IP configuration subcommands
  license    Configure license features
  netconf    Configure NETCONF
  no         Negate a command or set its defaults
  oer        Optimized Exit Routing configuration submodes
  sasl       Configure SASL
  wsma       Configure Web Services Management Agents

R2(config)#ip ?
Global IP configuration subcommands:
  route  Establish static routes

R2(config)#interface g0/0
R2(config-if)#?
Interface configuration commands:
  default  Set a command to its defaults
  exit     Exit from interface configuration mode
  help     Description of the interactive help system
  ip       Interface Internet Protocol config commands
  no       Negate a command or set its defaults

R2(config-if)#ip ?
Interface IP configuration subcommands:
  access-group        Specify access control for packets
  accounting          Enable IP accounting on this interface
  address             Set the IP address of an interface
  admission           Apply Network Admission Control
  auth-proxy          Apply authentication proxy
  authentication      authentication subcommands
```

```
bandwidth-percent   Set EIGRP bandwidth limit
bgp                 BGP interface commands
broadcast-address   Set the broadcast address of an interface
cef                 Cisco Express Forwarding interface commands
cgmp                Enable/disable CGMP
ddns                Configure dynamic DNS
dhcp                Configure DHCP parameters for this interface
directed-broadcast  Enable forwarding of directed broadcasts
dns                 Configure DNS server
dvmrp               DVMRP interface commands
flow                NetFlow related commands
hello-interval      Configures IP-EIGRP hello interval
helper-address      Specify a destination address for UDP broadcasts
hold-time           Configures IP-EIGRP hold time
idle-group          Specify interesting packets for idle-timer
igmp                IGMP interface commands
information-reply   Enable sending ICMP Information Reply messages
inspect             Apply inspect name
ips                 Create IPS rule
irdp                ICMP Router Discovery Protocol
load-sharing        Style of load sharing
local-proxy-arp     Enable local-proxy ARP
mask-reply          Enable sending ICMP Mask Reply messages
mobile              Mobile IP support
mrm                 Configure IP Multicast Routing Monitor tester
mroute-cache        Enable switching cache for incoming multicast packets
mtu                 Set IP Maximum Transmission Unit
multicast           IP multicast interface commands
nat                 NAT interface commands
nbar                Network-Based Application Recognition
next-hop-self       Configures IP-EIGRP next-hop-self
ospf                OSPF interface commands
pgm                 PGM Reliable Transport Protocol
pim                 PIM interface commands
policy              Enable policy routing
proxy-arp           Enable proxy ARP
proxy-mobile        Enable Proxy Mobile IP services
rarp-server         Enable RARP server for static arp entries
rbscp               RBSCP subfeatures for this interface
redirects           Enable sending ICMP Redirect messages
rgmp                Enable/disable RGMP
rip                 Router Information Protocol
route-cache         Enable fast-switching cache for outgoing packets
router              IP router interface commands
rsvp                RSVP Interface Commands
sap                 Session Announcement Protocol interface commands
security            DDN IP Security Option
service             IP service
split-horizon       Perform split horizon
summary-address     Perform address summarization
tcp                 TCP header compression and other parameters
```

```
  traffic-export      Configure this interface for exporting ip traffic
  unnumbered          Enable IP processing without an explicit address
  unreachables        Enable sending ICMP Unreachable messages
  urd                 Configure URL Rendezvousing
  verify              Enable per packet validation
  virtual-reassembly  Enable Virtual Fragment Reassembly
  vrf                 VPN Routing/Forwarding parameters on the interface
  wccp                WCCP interface commands

R2#show startup
startup-config is not present
R2#exi

[Connection to 100.2.2.2 closed by foreign host]
R1#
```

Note that only commands from that level and below are visible to the user.

## Verification (detailed)



```
AAA/BIND(0000000C): Bind i/f
AAA/AUTHEN/LOGIN (0000000C): Pick method list 'VTY'
AAA/AUTHOR (0xC): Pick method list 'VTY'
AAA/AUTHOR/EXEC(0000000C): processing AV cmd=
AAA/AUTHOR/EXEC(0000000C): processing AV priv-lvl=6
AAA/AUTHOR/EXEC(0000000C): Authorization successful
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 6 list=
'' AUTHOR-TYPE= 'command'
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 6 list=
'' AUTHOR-TYPE= 'command'
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 6 list=
'' AUTHOR-TYPE= 'command'
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 0 list=
'' AUTHOR-TYPE= 'command'
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 0 list=
'' AUTHOR-TYPE= 'command'
%SYS-5-CONFIG_I: Configured from console by student1 on vty0 (10.1.10.1)
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 6 list=
'' AUTHOR-TYPE= 'command'
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 0 list=
'' AUTHOR-TYPE= 'command'
```

## Task 3 – Local command authorization

On R2 configure local commands authorization for all privilege level 6 commands.

*Having a command on specific level is one thing but having access to that command is another thing. We can configure command authorization to authorize a user to run specific command so that before running a command the router will consult its database for permission to run that command.*
*By default configuration commands (those entered in configuration mode) are not authorized and must be explicitly configured to do so. Also, command authorization for a specific level must be enabled on a line.*

### Configuration

Complete these steps:

**Step 1** Configure R2 as follows:

```
!
aaa authorization commands 6 VTY local
aaa authorization config-commands
!
line vty 0 4
 authorization commands 6 VTY
!
```



### Verification

```
R1#telnet 100.2.2.2
Trying 100.2.2.2 ... Open

Access to this router is restricted!
Disconnect now if you are NOT logitimate user!

Username: student1
Password:

R2#show priv
Current privilege level is 6
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 1.1.1.1 255.255.255.255 100.2.2.10
R2(config)#exit
R2#exit
```

```
[Connection to 100.2.2.2 closed by foreign host]
R1#
```

The user has landed on level 6 and is able to run "ip route" command. See below what has happened in the background.

## Verification (detailed)

```
AAA/BIND(0000000F): Bind i/f
AAA/ACCT/EVENT/(0000000F): CALL START
Getting session id for NET(0000000F) : db=49DAC694
AAA/ACCT(00000000): add node, session 12
AAA/ACCT/NET(0000000F): add, count 1
Getting session id for NONE(0000000F) : db=49DAC694
AAA/AUTHEN/LOGIN (0000000F): Pick method list 'VTY'
AAA/AUTHOR (0xF): Pick method list 'VTY'
AAA/AUTHOR/EXEC(0000000F): processing AV cmd=
AAA/AUTHOR/EXEC(0000000F): processing AV priv-lvl=6
AAA/AUTHOR/EXEC(0000000F): Authorization successful
```

The user has been authorized to use level 6. Note that the AAA authorization-exec process has done that (AAA/AUTHOR/EXEC).



```
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 6 list=
'VTY' AUTHOR-TYPE= 'command'
AAA: parse name=tty514 idb type=-1 tty=-1
AAA: name=tty514 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=514 channel=0
AAA/MEMORY: create_user (0x49FA48B0) user='student1' ruser='R2' ds0=0 port='tty514'
rem_addr='10.1.10.1' authen_type=ASCII service=NONE priv=6 initial_task_id='0', vrf=
(id=0)
tty514 AAA/AUTHOR/CMD(1980387562): Port='tty514' list='VTY' service=CMD
AAA/AUTHOR/CMD: tty514(1980387562) user='student1'
tty514 AAA/AUTHOR/CMD(1980387562): send AV service=shell
tty514 AAA/AUTHOR/CMD(1980387562): send AV cmd=show
tty514 AAA/AUTHOR/CMD(1980387562): send AV cmd-arg=privilege
tty514 AAA/AUTHOR/CMD(1980387562): send AV cmd-arg=<cr>
```

After connecting the user has issued "sh priv' command so that the AAA authorization-command process has been consulted. This process was repeated for every command the user issued.

```
tty514 AAA/AUTHOR/CMD(1980387562): found list "VTY"
tty514 AAA/AUTHOR/CMD(1980387562): Method=LOCAL
AAA/AUTHOR (1980387562): Post authorization status = PASS_ADD
AAA/MEMORY: free_user (0x49FA48B0) user='student1' ruser='R2' port='tty514'
rem_addr='10.1.10.1' authen_type=ASCII service=NONE priv=6 vrf= (id=0)
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 6 list=
'VTY' AUTHOR-TYPE= 'command'
AAA: parse name=tty514 idb type=-1 tty=-1
AAA: name=tty514 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=514 channel=0
```

```
AAA/MEMORY: create_user (0x48F7C388) user='student1' ruser='R2' ds0=0 port='tty514'
rem_addr='10.1.10.1' authen_type=ASCII service=NONE priv=6 initial_task_id='0', vrf=
(id=0)
tty514 AAA/AUTHOR/CMD(4198853883): Port='tty514' list='VTY' service=CMD
AAA/AUTHOR/CMD: tty514(4198853883) user='student1'
tty514 AAA/AUTHOR/CMD(4198853883): send AV service=shell
tty514 AAA/AUTHOR/CMD(4198853883): send AV cmd=configure
tty514 AAA/AUTHOR/CMD(4198853883): send AV cmd-arg=terminal
tty514 AAA/AUTHOR/CMD(4198853883): send AV cmd-arg=<cr>
tty514 AAA/AUTHOR/CMD(4198853883): found list "VTY"
tty514 AAA/AUTHOR/CMD(4198853883): Method=LOCAL
AAA/AUTHOR (4198853883): Post authorization status = PASS_ADD
AAA/MEMORY: free_user (0x48F7C388) user='student1' ruser='R2' port='tty514'
rem_addr='10.1.10.1' authen_type=ASCII service=NONE priv=6 vrf= (id=0)
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 6 list=
'VTY' AUTHOR-TYPE= 'command'
AAA: parse name=tty514 idb type=-1 tty=-1
AAA: name=tty514 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=514 channel=0
AAA/MEMORY: create_user (0x496E9768) user='student1' ruser='R2' ds0=0 port='tty514'
rem_addr='10.1.10.1' authen_type=ASCII service=NONE priv=6 initial_task_id='0', vrf=
(id=0)
tty514 AAA/AUTHOR/CMD(3915173581): Port='tty514' list='VTY' service=CMD
AAA/AUTHOR/CMD: tty514(3915173581) user='student1'
tty514 AAA/AUTHOR/CMD(3915173581): send AV service=shell
tty514 AAA/AUTHOR/CMD(3915173581): send AV cmd=ip
tty514 AAA/AUTHOR/CMD(3915173581): send AV cmd-arg=route
tty514 AAA/AUTHOR/CMD(3915173581): send AV cmd-arg=1.1.1.1
tty514 AAA/AUTHOR/CMD(3915173581): send AV cmd-arg=255.255.255.255
tty514 AAA/AUTHOR/CMD(3915173581): send AV cmd-arg=100.2.2.10
tty514 AAA/AUTHOR/CMD(3915173581): send AV cmd-arg=<cr>
tty514 AAA/AUTHOR/CMD(3915173581): found list "VTY"
tty514 AAA/AUTHOR/CMD(3915173581): Method=LOCAL
AAA/AUTHOR (3915173581): Post authorization status = PASS_ADD
AAA/MEMORY: free_user (0x496E9768) user='student1' ruser='R2' port='tty514'
rem_addr='10.1.10.1' authen_type=ASCII service=NONE priv=6 vrf= (id=0)
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 0 list=
'' AUTHOR-TYPE= 'command'
%SYS-5-CONFIG_I: Configured from console by student1 on vty0 (10.1.10.1)
AAA/AUTHOR: auth_need : user= 'student1' ruser= 'R2'rem_addr= '10.1.10.1' priv= 0 list=
'' AUTHOR-TYPE= 'command'
unknown AAA/DISC: 1/"User Request"
unknown AAA/DISC/EXT: 1020/"User Request"
AAA/ACCT/EVENT/(0000000F): CALL STOP
AAA/ACCT/CALL STOP(0000000F): Sending stop requests
AAA/ACCT(0000000F): Send all stops
AAA/ACCT/NET(0000000F): STOP
AAA/ACCT/NET(0000000F): Method list not found
AAA/ACCT(0000000F): del node, session 12
AAA/ACCT/NET(0000000F): free_rec, count 0
AAA/ACCT/NET(0000000F) reccnt 0, csr TRUE, osr 0
AAA/ACCT/NET(0000000F): Last rec in db, intf not enqueued
```

# LAB 2.31. TACACS+ user authentication (IOS)

## Objectives

This lab shows how to configure routers to perform user authentication and authorization using TACACS+ protocol and AAA server.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| ACS | NIC | 172.31.1.100 |
| WinXP | NIC | 10.1.10.50 |

## Task 1 – Basic TACACS+ user authentication

Configure R1 router to use TACACS+ protocol for remote users TELNET session authentication. On the ACS create a new user "r1admin" with a password of "r1admin" which is a member of user group "ADMINS".
You must successfully authenticate when telnetting from WinXP and have evidence in the ACS's log file for that event.

*The most common scenario for authentication is to use external user database. This can be done by configuring TACACS+ server where user's profile is stored and configuring the router to consult that server in order to authenticate the user. The server must be aware of the router as well to be able to serve it with requested data. So that the router and the TACACS+ server must have the same Secret Key. This key is used for encryption of TACACS+ messages.*

*The router R1 has already been added as AAA clent to the ACS.*



### Configuration

Complete these steps:

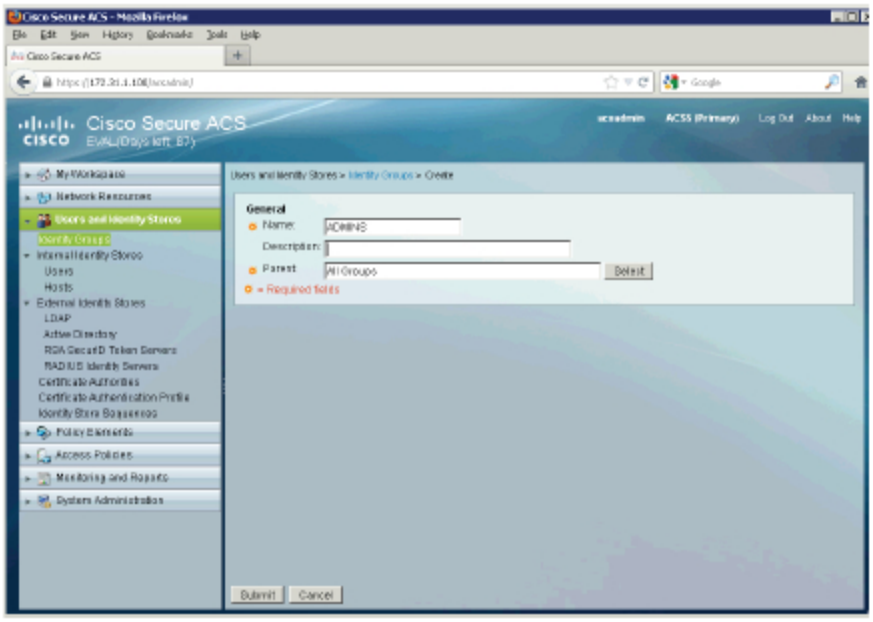
**Step 1** Configure R1 as follows:

```
!
aaa new-model
!
tacacs server ACS
 address ipv4 172.31.1.100
 key cisco123
 single-connection!
!
aaa authentication login VTY-AAA group tacacs+ local
!
line vty 0 4
 login authentication VTY-AAA
!
```

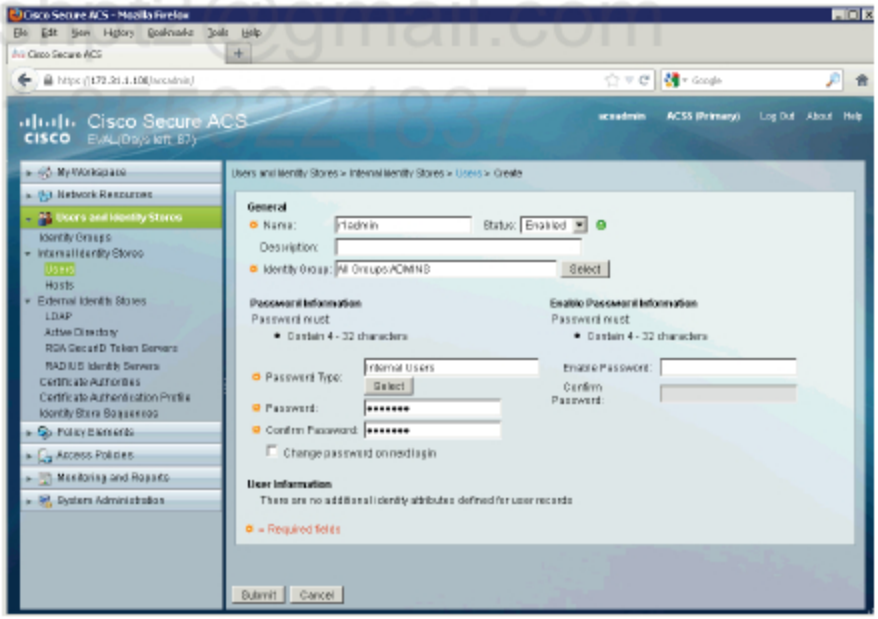
**Step 2** Add user to the ACS.

Connect to ACS from WinXP PC and authenticate using **acsadmin**.

- Go to **Users and Identity Stores > Identity Groups** and click **Create**. Add name **ADMINS** under **All Groups** and click **Submit**.




- Go to **Users and Identity Stores > Users** and click **Create**. Add new user with a name of **r1admin** and password of **r1admin**, select **ADMINS** under **Identity Groups** and click **Submit**.

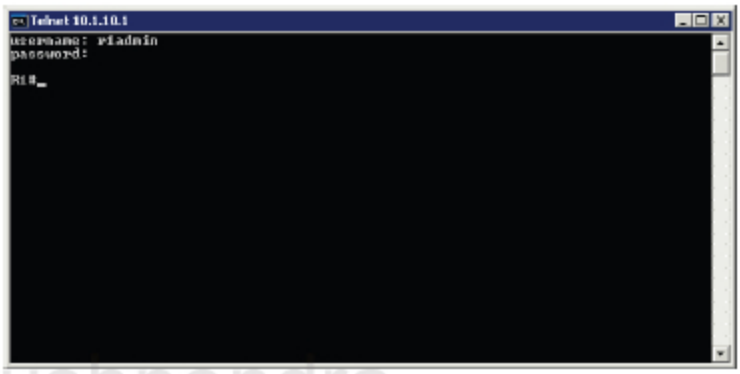


## Verification

```
R1#test aaa group tacacs+ r1admin r1admin legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

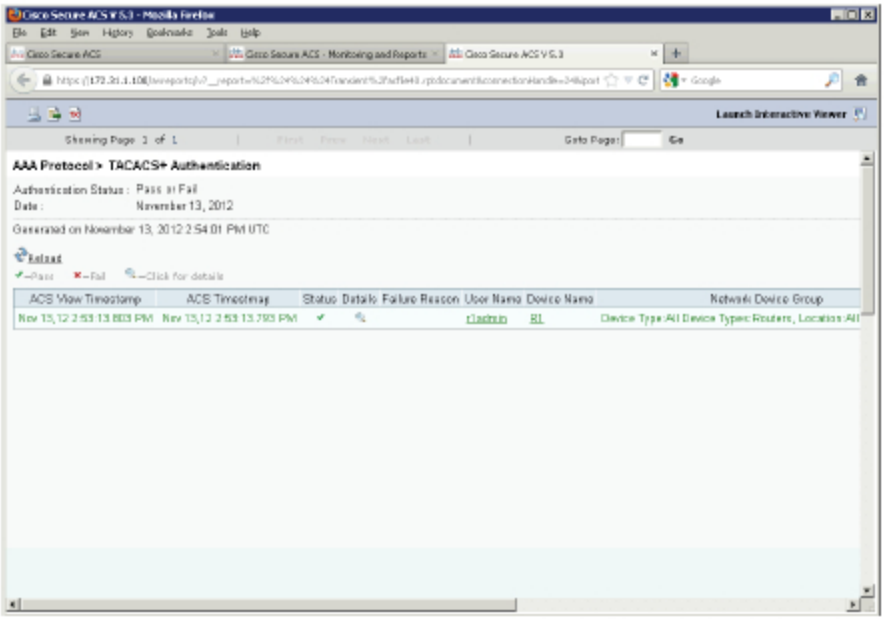
The "test" command is very useful in order to verify communication between the router and the ACS. From above command we see that the user r1admin has been successfully authenticated.

Telnet from WinXP machine to R1 and authenticate.






Go to **Monitoring and Reports** and click on **Launch Monitoring and Report Viewer**. Click on **Authentications – TACACS – Today** report on the **Dashboard** to see the log.



## Verification (detailed)

```
R1#deb aaa authentication
AAA Authentication debugging is on
R1#
R1#deb aaa authorization
AAA Authorization debugging is on
R1#
R1#
R1#
R1#
Nov 13 15:48:19.659: AAA/BIND(00000010): Bind i/f
Nov 13 15:48:19.659: AAA/AUTHEN/LOGIN (00000010): Pick method list 'VTY-AAA'
R1#
Nov 13 15:48:25.664: AAA/AUTHOR (00000010): Method list id=0 not configured. Skip
author
```

There is no AAA Authorization list configured so the authorization is skipped.

## Task 2 – Basic AAA with TACACS+

On ACS configure a new user "contractor1" with a password of "contractor1" and make him a member of **Contractors** group. This group should have access to network devices only during workdays (Mon-Fri) between 9am and 6pm and be allowed to only one session at time.

*This must be done using ACS Authorization Rules. The ACS v5 is rule-based. This means that Authentication and/or Authorization decisions are independed and based on configured rules.*

### Configuration



Complete these steps:

**Step 1** Configure Authorization and Accounting on R1. Whole AAA configuration should look like this:

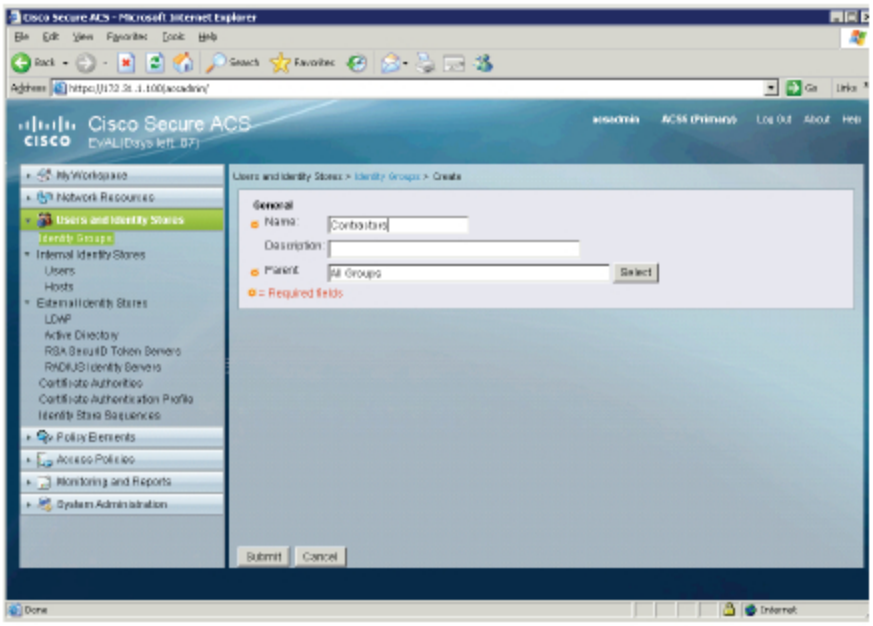
```
!
aaa authentication login VTY-AAA group tacacs+ local
aaa authorization exec VTY-AUTHZ group tacacs+ local
aaa accounting exec VTY-ACC start-stop group tacacs+
!
line vty 0 4
 authorization exec VTY-AUTHZ
 accounting exec VTY-ACC
 login authentication VTY-AAA
!
```

To make Session Count restrictions on the ACS work, TACAS authorization and accounting must also be enabled. This is important to let ACS know about new user session in a particular group and to differentiate between new session and re-authenticated session.

**Step 2** Add user group and new user to the ACS.

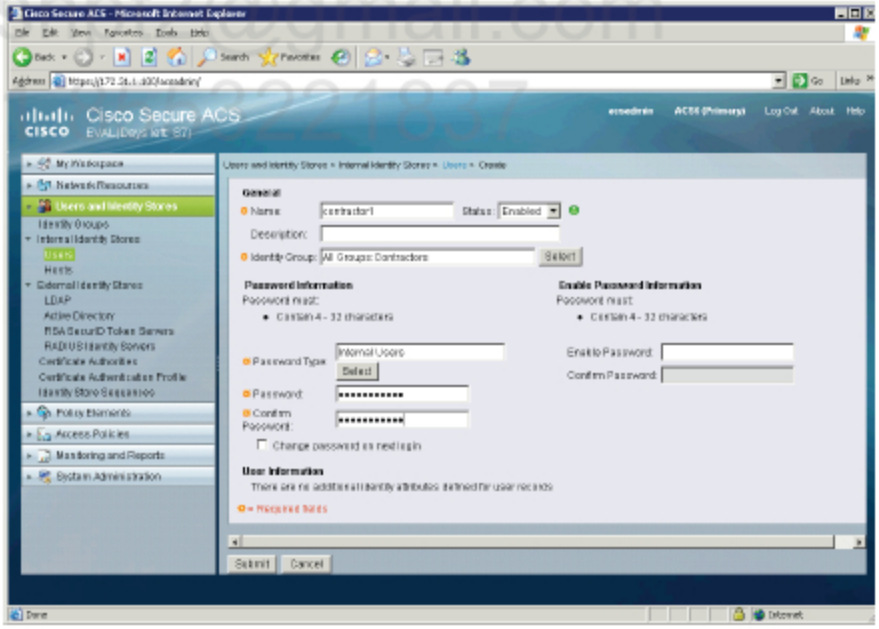
Connect to ACS from WinXP PC and authenticate using **acsadmin**.

- Go to **Users and Identity Stores > Identity Groups** and click **Create**. Add name **Contractors** under **All Groups** and click **Submit**.



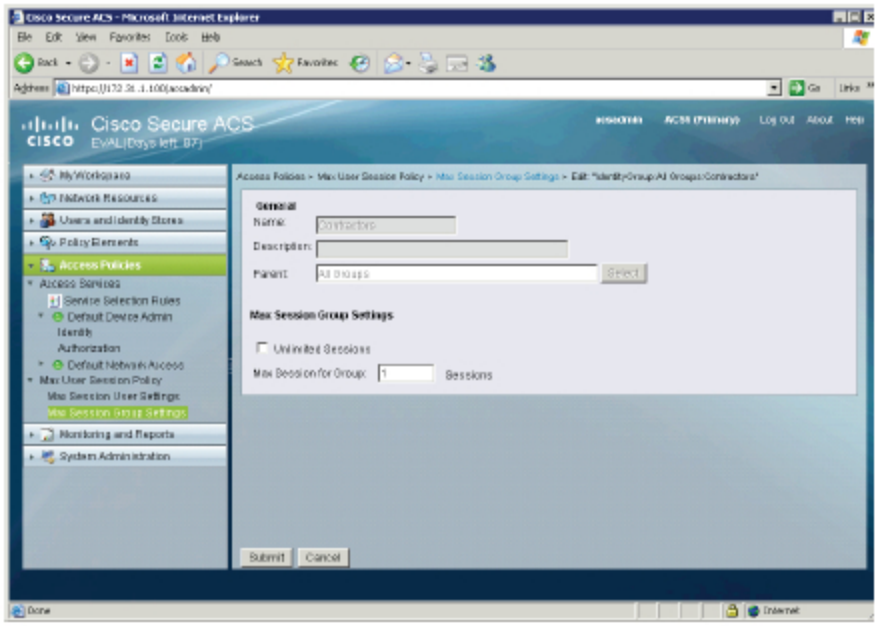

- Go to **Users and Identity Stores > Users** and click **Create**. Add new user with a name of **contractor1** and password of **contractor1**, select **Contractors** under **Identity Groups** and click **Submit**.





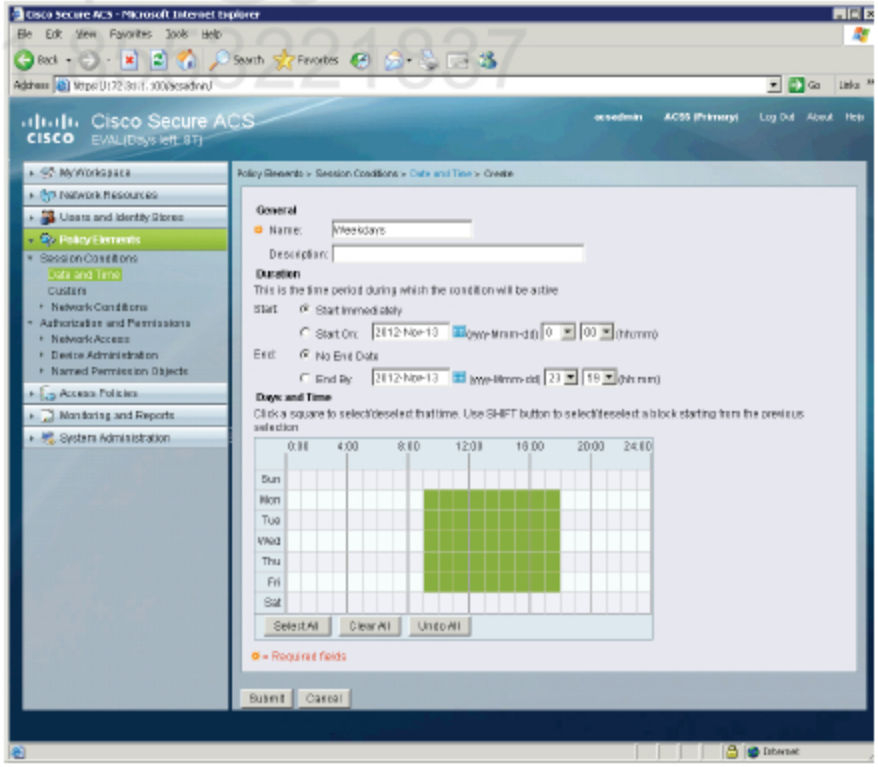

**Step 3** Set max sessions per group.

- Go to **Access Policies > Max User Session Policy > Max Session Group Settings** and click on **Contractors** group. Uncheck **Unlimited Sessions** checkbox and set **Max Session for Group** to **1**, then click **Submit**.



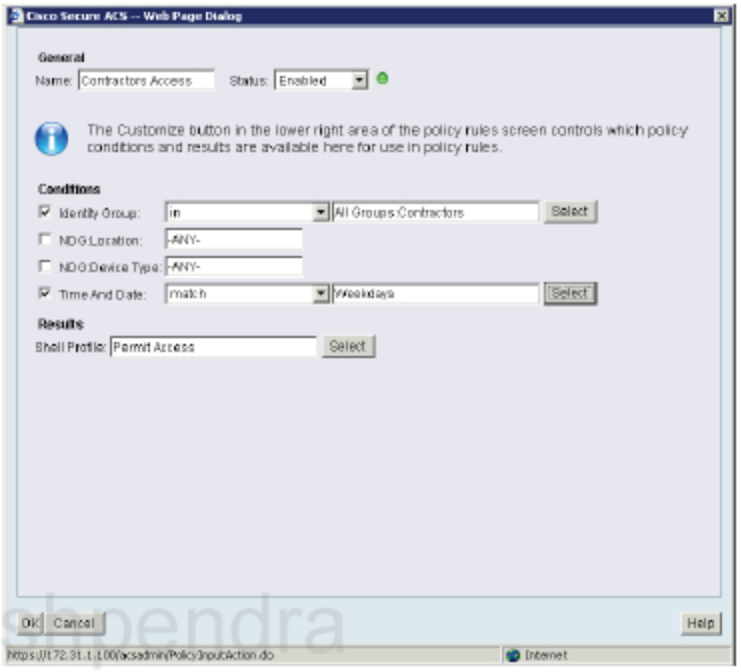

**Step 4** Set time restriction policy.

- Go to **Policy Elements > Session Conditions > Date and Time** and click **Create**. Provide a name for the condition and select only **Mon-Fri 9am-6pm** boxes on the chart, and then click **Submit**.



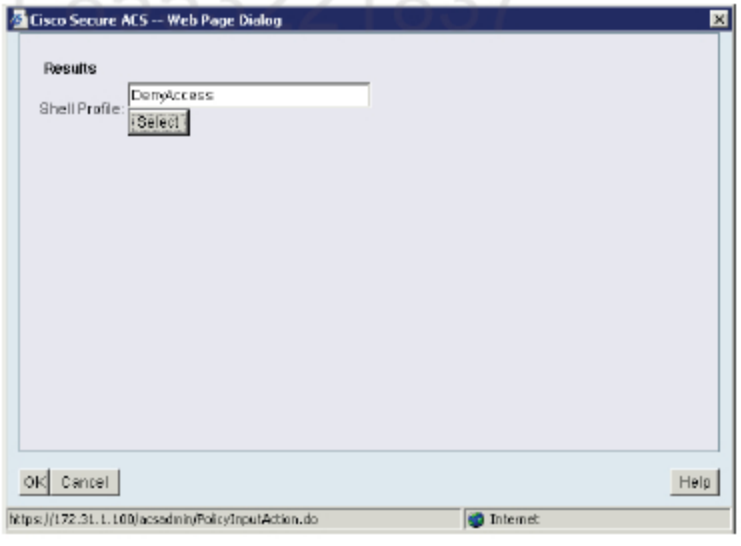

- Go to **Access Policies > Access Services > Default Device**

**Admin > Authorization** and click **Create**. Name it **Contractors Access** and select **Contractors** group for **Identity Group** and **Weekdays** for **Time And Date** then click **OK**.

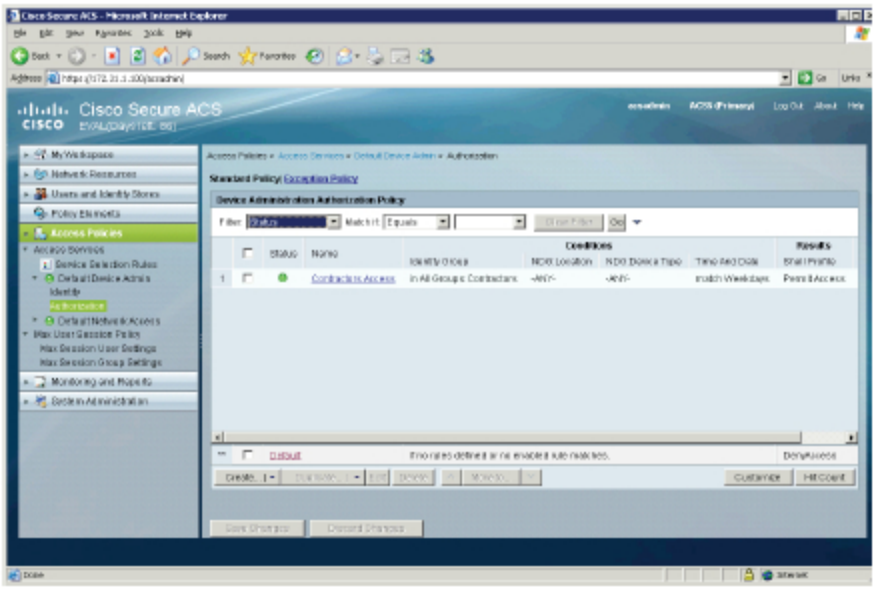





- Change the default policy to **DenyAcess** by clicking on **Default** hyperlink at the bottom of the page. Click on **OK** button.



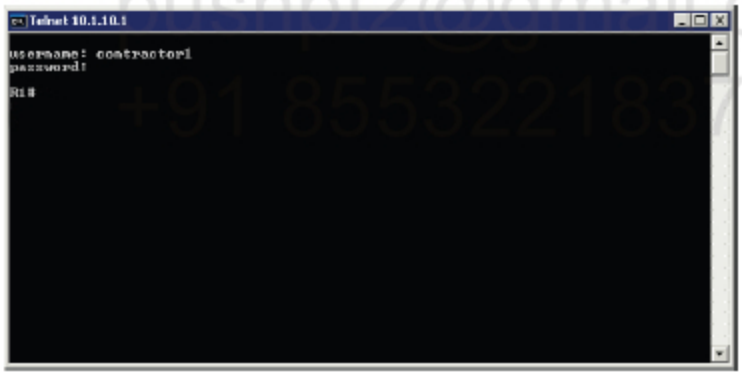

- Click on **Save Changes** button.




## Verification

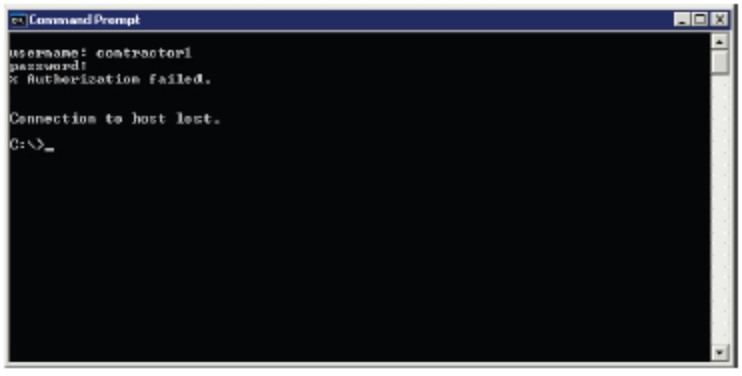
TELNET to R1 and authenticate.

**The success of this operation depends of the time as we have restrictions and should only be allowed to authenticate during the business hours Mon-Fri.**




Do not close this session and TELNET again to R1.

**You should NOT be allowed to authenticate.**

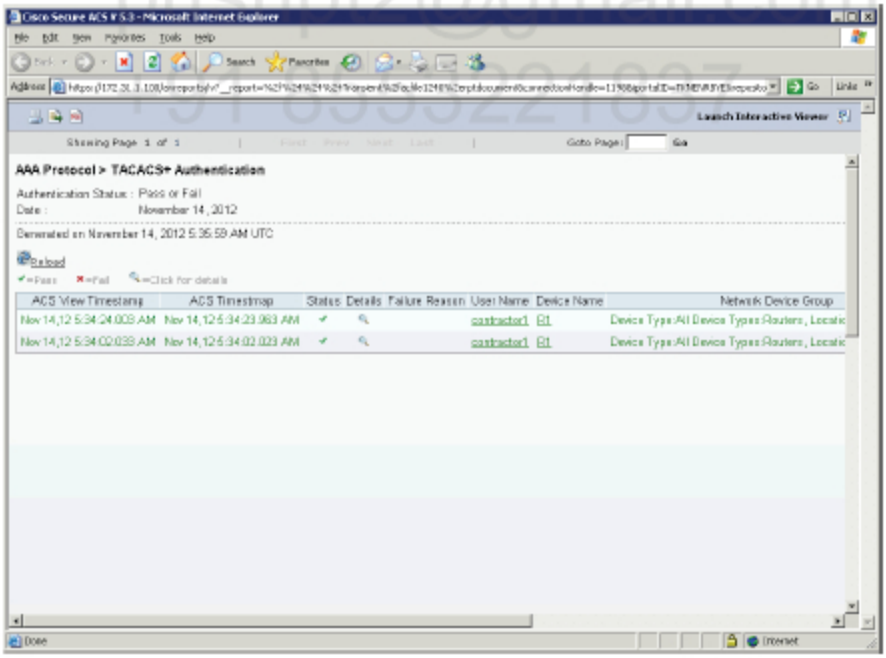


Enable 'debug aaa authentication' and 'debug aaa authorization' on the router and see what happened.

```
Nov 14 05:33:54.824: AAA/BIND(00000027): Bind i/f
Nov 14 05:33:54.824: AAA/AUTHEN/LOGIN (00000027): Pick method list 'VTY-AAA'
R1#
Nov 14 05:34:02.021: AAA/AUTHOR (0x27): Pick method list 'VTY-AUTHZ'
Nov 14 05:34:02.033: AAA/AUTHOR/EXEC(00000027): processing AV cmd=
Nov 14 05:34:02.033: AAA/AUTHOR/EXEC(00000027): Authorization successful
R1#
Nov 14 05:34:05.273: AAA/AUTHOR: auth_need : user= 'contractor1' ruser= 'R1'rem_addr=
'10.1.10.50' priv= 1 list= '' AUTHOR-TYPE= 'command'
R1#
Nov 14 05:34:16.896: AAA/BIND(00000028): Bind i/f
Nov 14 05:34:16.896: AAA/AUTHEN/LOGIN (00000028): Pick method list 'VTY-AAA'
R1#
Nov 14 05:34:23.961: AAA/AUTHOR (0x28): Pick method list 'VTY-AUTHZ'
Nov 14 05:34:23.969: AAA/AUTHOR/EXEC(00000028): Authorization FAILED
R1#
```

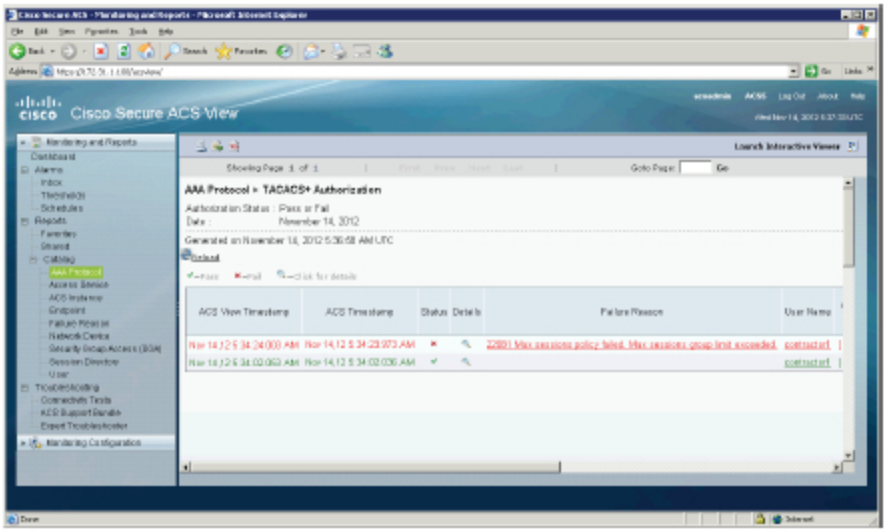


Check TACACS+ Authentication log.



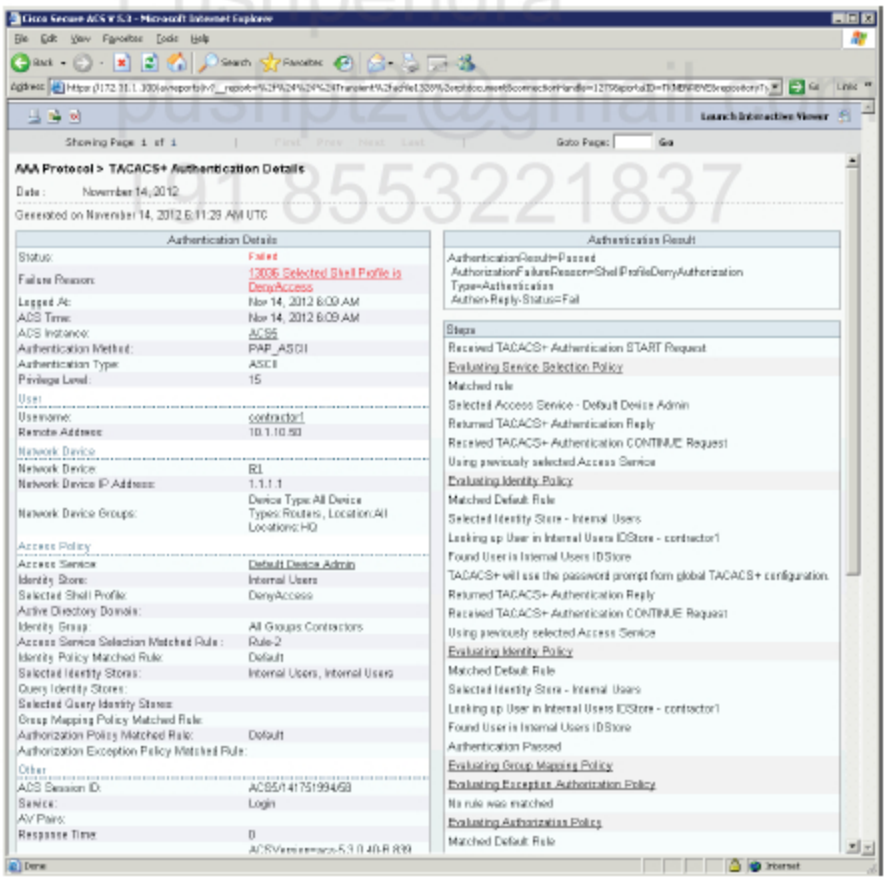

**Note that both sessions have been successfully authenticated. To really see what happened you must check TACACS Authorization log (note that this log is not showed on the Dashboard).**

You must go to **Reports > Catalog > AAA Protocol** and click on **TACACS Authorization** log.




**There is a Failure Reason of '22081 Max sessions policy failed. Max sessions group limit exceeded."**

Temporarily change the time on ACS or Time and Date restrictions to enforce that policy. See the TACACS Authentication log to verify that.




**Note that the Failure Reason is '13036 Selected Shell Profile is DenyAccess'. This means our session has not matched by our Contractors Access rule. Check out 'Access Service Selection Matched Rule : Rule-2'.**

## Task 3 – Basic AAA with TACACS+

On ACS configure a user **restricted1** with a password of **restricted1** and make him a member of **Restricted** group. This user should be able to telnet to R1 from R2's loopback0 interface only.

*The first thing you should note here is that TELNET traffic will be traversing the ASA firewall. This implies special configuration on the ASA. There is no need for any NAT configuration.*
*Also note that only that user must be affected by this configuration. Hence, you must add new Authorization policy.*

### Configuration

Complete these steps:

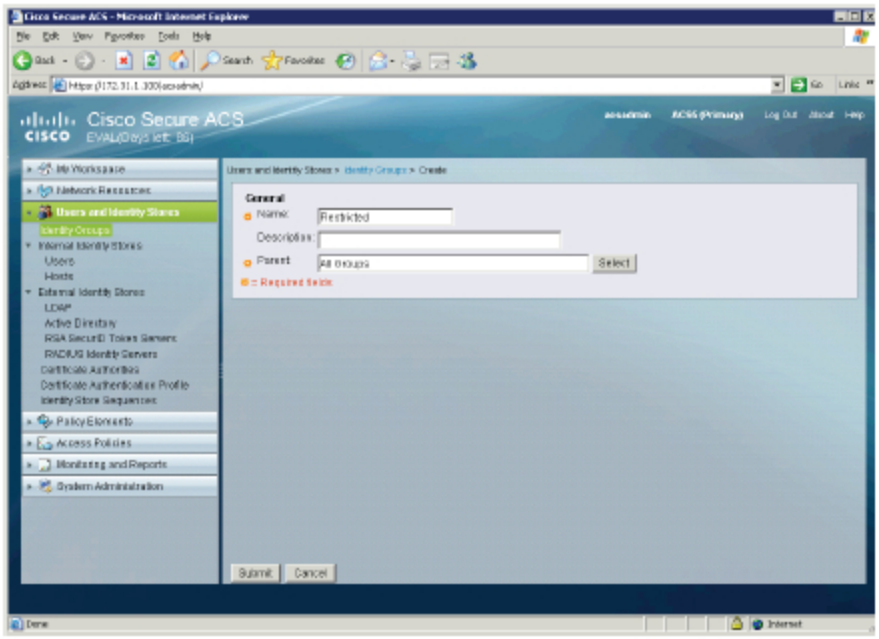
**Step 1** Make changes on ASA to allow TELNET traffic from R2.

```
!
access-list OUTSIDE_IN extended permit tcp host 2.2.2.2 host
10.1.10.1 eq telnet
!
access-group OUTSIDE_IN in interface outside
!
```

**Step 2** Create user group and new user.

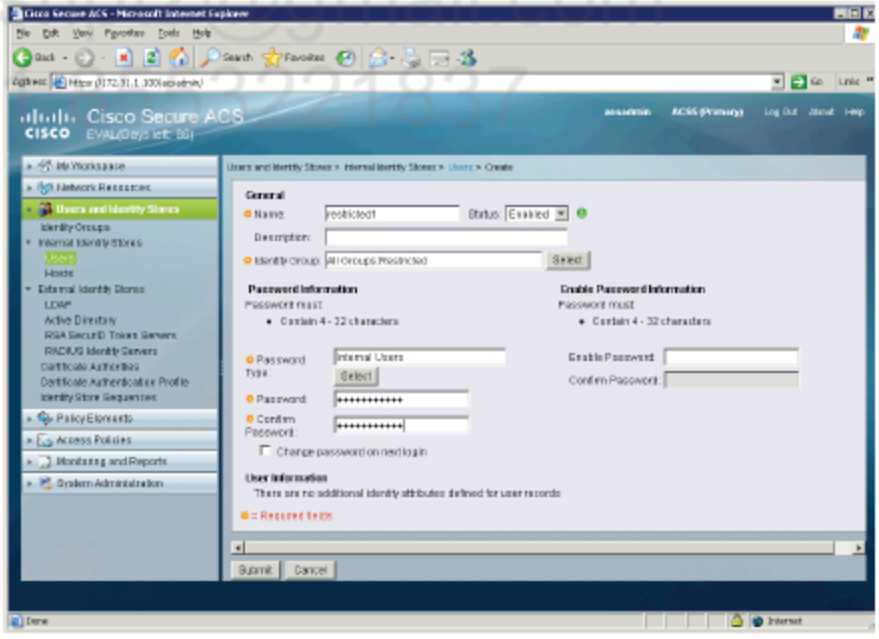
Connect to ACS from WinXP PC and authenticate using **acsadmin**.

- Go to **Users and Identity Stores > Identity Groups** and click **Create**. Add name **Restricted** under **All Groups** and click **Submit**.



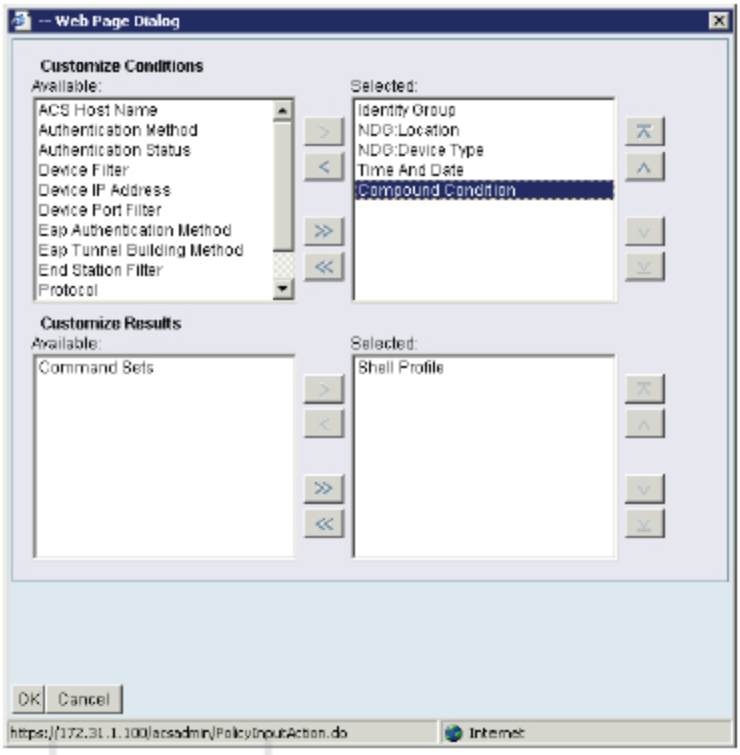

- Go to **Users and Identity Stores > Users** and click **Create**. Add new user with a name of **restricted1** and password of **restricted1**, select **Restricted** under **Identity Groups** and click **Submit**.





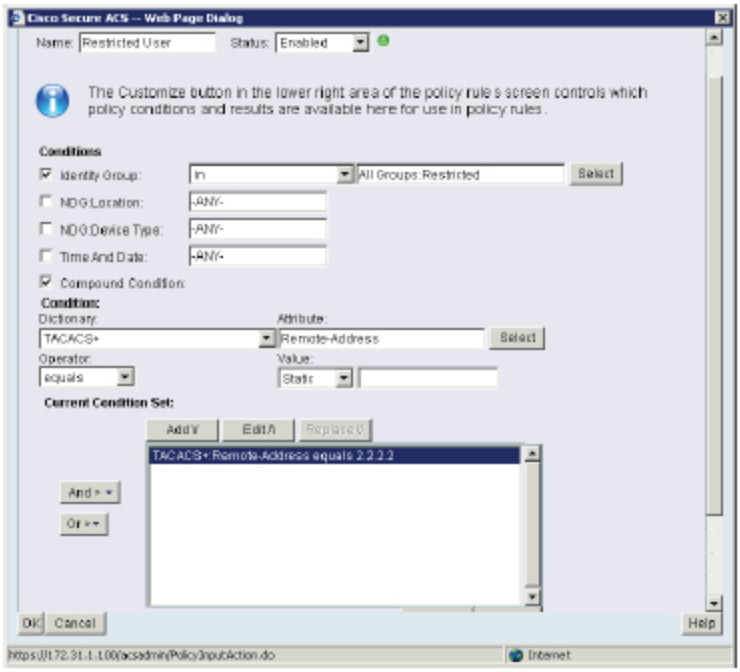

**Step 3** Create new Authorization rule.

- Go to **Access Policies > Access Services > Default Device Admin > Authorization** and click **Customize**. Select **Compound Condition** from the left pane and move it to **Selected** pane. Click **OK**.

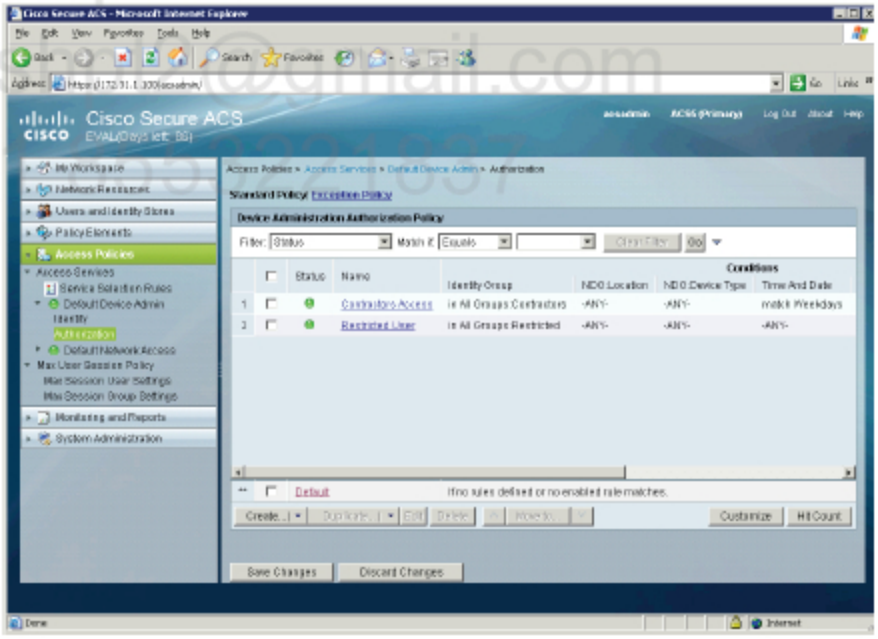





- Click **Create** to create new Authorization rule. Name it **Restricted User** and select **Restricted** group for **Identity Group** and select **Compound Condition** checkbox. Pick **TACACS+** from **Dictionary** drop-down list, click **Select** button and chose **Remote-Address** attribute. Value set to **Static 2.2.2.2** and click **Add V** button. Click **OK**.




- Click on **Save Changes** button.



## Verification

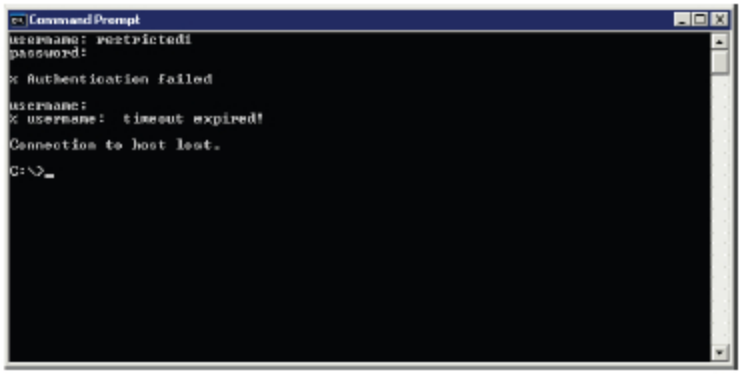
### TELNET from R2 loopback0

```
R2#tel 10.1.10.1 /so lo0
Trying 10.1.10.1 ... Open

username: restricted1
password:

R1#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:23:06
*  2 vty 0     restricted idle                 00:00:00 2.2.2.2

  Interface    User               Mode         Idle     Peer Address

R1#exit

[Connection to 10.1.10.1 closed by foreign host]
R2#
R2#tel 10.1.10.1
Trying 10.1.10.1 ...
% Connection timed out; remote host not responding
```

**You can connect and authenticate when sourcing from R2 loopback0 interface only. You cannot even connect using different source address because the ASA firewall blocks the traffic.**



### TELNET from WinXP




**You can connect but cannot authenticate to R1 when sourcing traffic from WinXP. This is because ACS denies the user based on our configuration. To check that see ACS logs.**

| ACS View Timestamp | ACS Timestmap | Status | Details | Failure Reason | User Name | Device |
|---|---|---|---|---|---|---|
| Nov 14,12 9:45:01.933 AM | Nov 14,12 9:45:01.913 AM | ✖ | 🔍 | 13036 Selected Shell Profile is DenyAccess | restricted1 | R1 |
| Nov 14,12 9:44:07.583 AM | Nov 14,12 9:44:07.566 AM | ✔ | 🔍 | | restricted1 | R1 |

**The green connection is for successful authentication and authorization. The AAA session was hit Restricted User authorizationrule.**

The red connection has missed all authorization rules and finally hit Default rule that says DenyAccess.

# LAB 2.32. TACACS+ authentication and authorization (IOS)

## Objectives

This lab shows how to configure routers to perform user authentication and authorization using TACACS+ protocol and AAA server.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| ACS | NIC | 172.31.1.100 |
| WinXP | NIC | 10.1.10.50 |

## Task 1 – TACACS+ authorization (IOS)

Configure R1 and ACS so that all users from ADMINS group (already created in previous lab) get authorized to use CLI at privilege level of 15 and their session idle timout is set to 2 minutes when connecting using TELNET. The user must not use “enable” command to switch to the appropriate privilege level.

*AAA EXEC authorization is a method of authorization to use router's shell. The most common usage is to configure privilege level for a user on the ACS and then this user is automatically raised to that level during connection.*



### Configuration

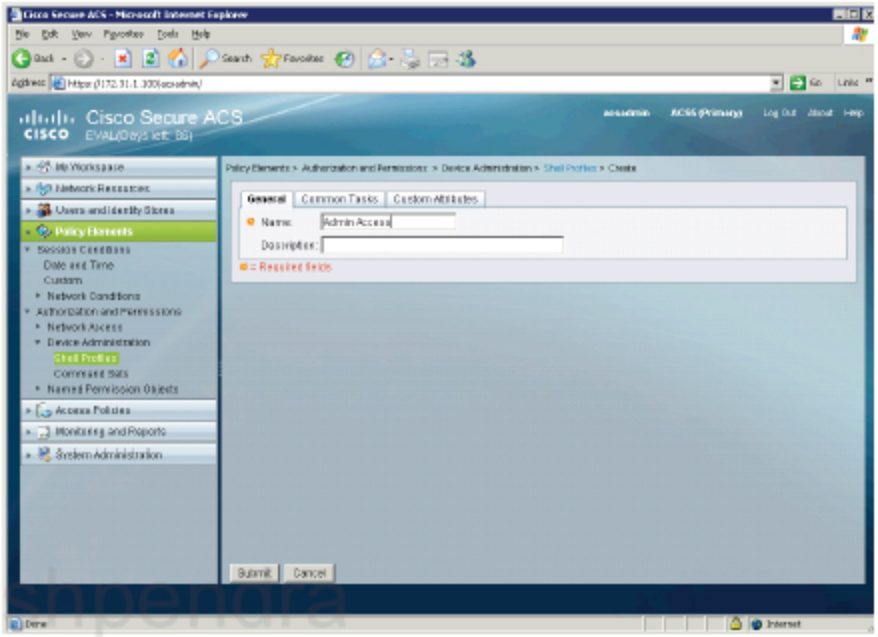
Complete these steps:

**Step 1** Configure R1 (the router should be configured already in the previous tasks). The following configuration is just for reference.

```
!
aaa new-model
!
tacacs server ACS
 address ipv4 172.31.1.100
 key cisco123
 single-connection
ip tacacs source-interface Loopback0
!
aaa authentication login VTY-AAA group tacacs+ local
aaa authorization exec VTY-AUTHZ group tacacs+ local
aaa accounting exec VTY-ACC start-stop group tacacs+
!
line vty 0 4
 authorization exec VTY-AUTHZ
 accounting exec VTY-ACC
 login authentication VTY-AAA
!
```

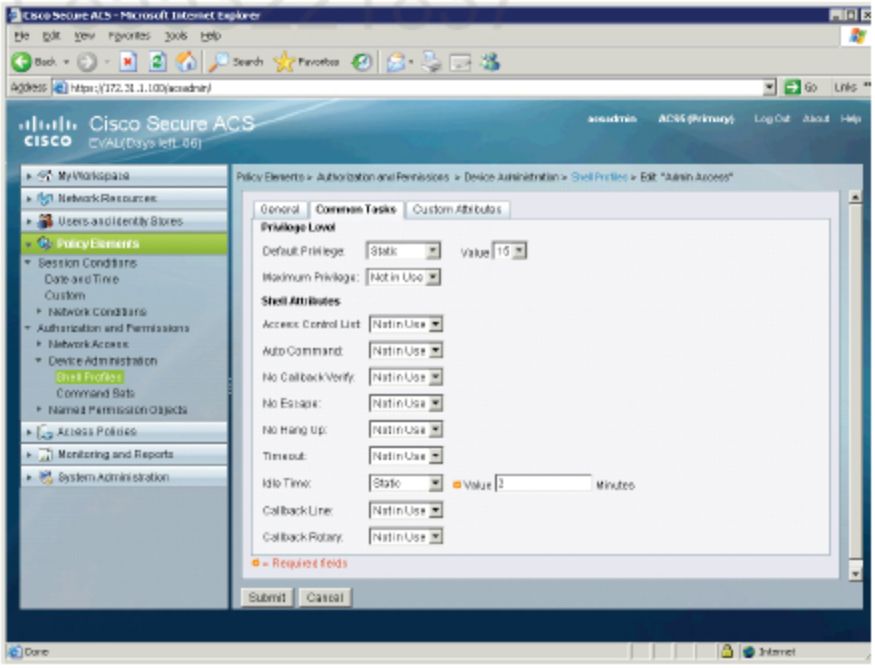
**Step 2** Configure ACS to assign privilege level 15 to all users in ADMINS group. First create Shell Profile wich will be applied to Authorization Policy.

- Go to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** and click **Create**. On the **General** tab provide a name for the profile (e.g. Admin Access).



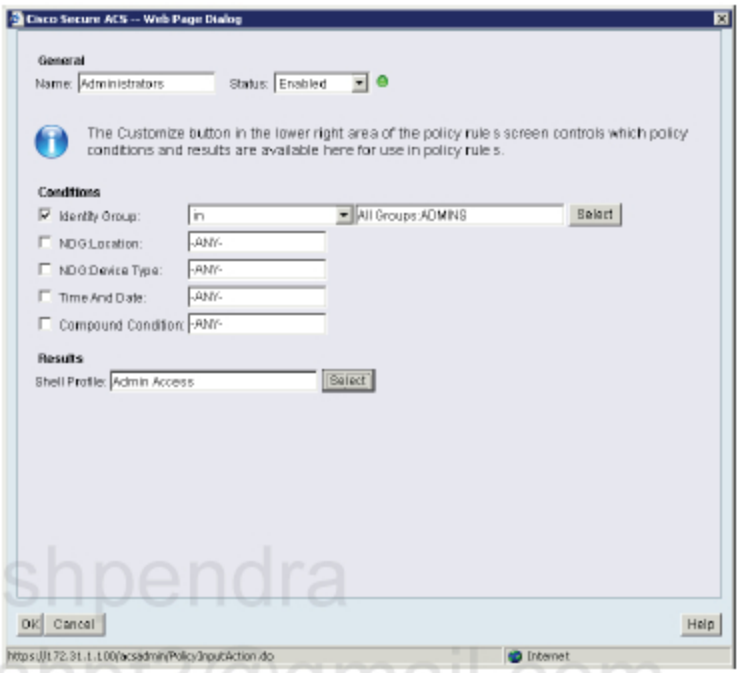



- Click on **Common Tasks** tab and set **Default Priviledge** to **15** and **Idle Time** to **2**. Click on **Submit**.



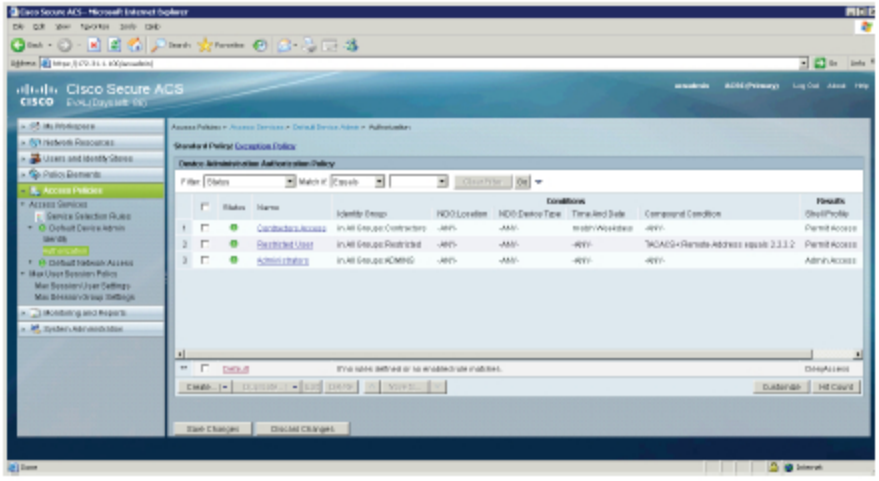

**Step 3** Create Authorization rule.

- Go to **Access Policies > Access Services > Default Device Admin > Authorization** and click **Create**. Enter name for the rule (e.g. Administrators), select **ADMINS** for **Identity Group** and assign **Shell Profile** of **Admin Access**. Click **OK**.






- Click **Save Changes**.



## Verification

TELNET to R1 from WinXP PC and authenticate using r1admin. You should get the following debug information on R1 console (if debug aaa is enabled).

```
Nov 14 10:53:56.413: AAA/AUTHEN/LOGIN (00000030): Pick method list 'VTY-AAA'
R1#
Nov 14 10:54:02.222: AAA/AUTHOR (0x30): Pick method list 'VTY-AUTHZ'
Nov 14 10:54:02.231: AAA/AUTHOR/EXEC(00000030): processing AV cmd=
Nov 14 10:54:02.231: AAA/AUTHOR/EXEC(00000030): processing AV idletime=120
Nov 14 10:54:02.231: AAA/AUTHOR/EXEC(00000030): processing AV priv-lvl=15
Nov 14 10:54:02.231: AAA/AUTHOR/EXEC(00000030): Authorization successful
```

User's attribute "priv-lvl" is sent down to the router from the ACS. This attribute contains user's privilege level assigned. Another attribute is for Idle Timeout.

## Task 2 – Local privilege and TACACS+ authorization (IOS)

On ACS create a new user “student4” with a password of “student4” (a member of Students group) and assign privilege level 4 to his account. This user must have access to run the following commands at privilege level 4 on R2:

- configure terminal
- interface
- ip address
- ip route

The user cannot escalate his privileges to the higher level.

Also, create local user ‘local4’ with a password of ‘local4’ on R2 that will have access to privilege level 4 and be used only when ACS is inaccessible.



*There is a difference between local and remote authorization. There are sixteen privilege levels available on the router where only three of them are preconfigured. Level 0,1 are basic levels for unprivileged users (their command prompt looks like ‘>’), and level 15 is for privileged user (command prompt is ‘#’). We can configure other levels and assign/move commands to those levels locally on the router. The user will get access to those commands on a specific level and all levels below while being authenticated and authorized to that level. For example, if we create level 7 and assign some commands with that level, the user authorized to that level would get access to all commands from level 7 as well as for lower levels 0-6.*

*The goil in this task is to create a new level 4, assign some commands to that level and authorize ACS-based user (student4) as well as local user (local4) to that level.*

### Configuration

Complete these steps:

**Step 1** Configure R2 to authenticate and authorize the users.

```
!
aaa new-model
!
aaa authentication login VTY-AAA group tacacs+ local
```

```
aaa authorization exec VTY-AUTHZ group tacacs+ local
!
tacacs server ACS
 address ipv4 172.31.1.100
 key cisco123
 single-connection
!
ip tacacs source-interface loopback0
!
line vty 0 4
 authorization exec VTY-AUTHZ
 login authentication VTY-AAA
!
username local4 privilege 4 password local4
!
priv exec level 4 configure terminal
priv configure level 4 interface
priv configure level 4 ip route
priv interface level 4 ip address
!
```

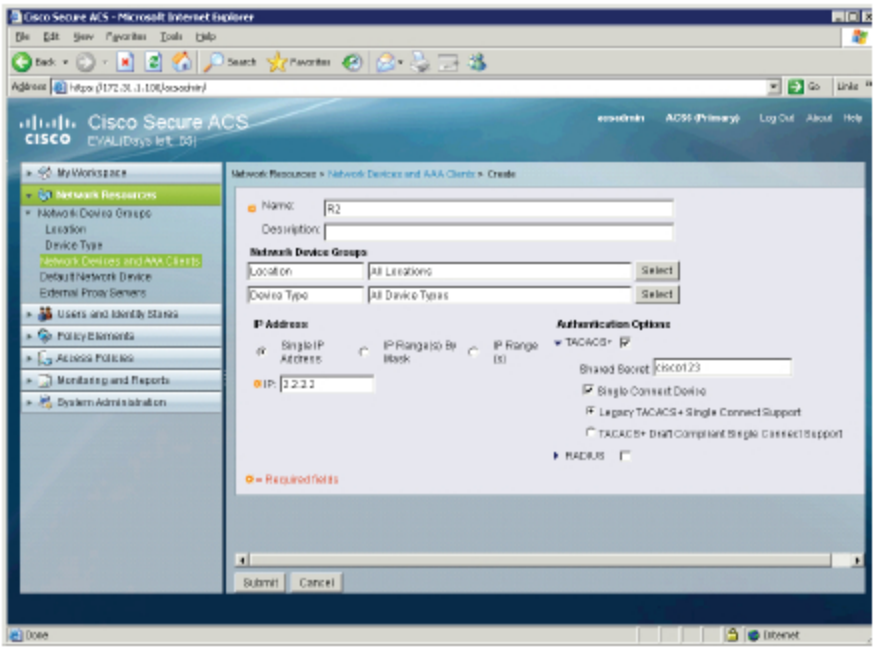
**Step 2** Configure ASA firewall to pass TACACS traffic.



```
!
route inside 172.31.1.0 255.255.255.0 10.1.10.1
!
access-list OUTSIDE_IN permit tcp host 2.2.2.2 host 172.31.1.100 eq
49
!
```

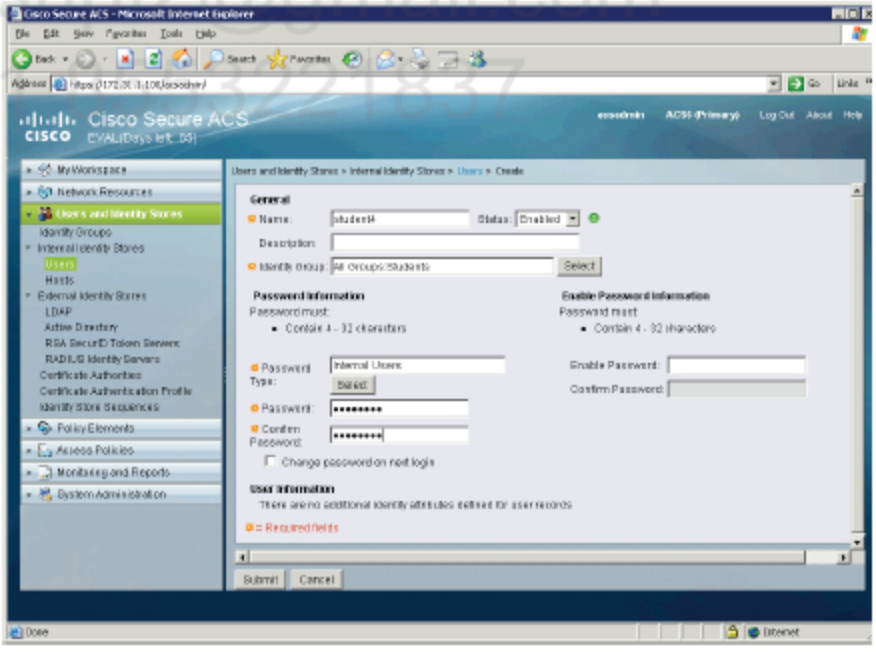
**Step 3** Configure R2 as AAA client on the ACS.

- Go to **Network Resources > Network Device and AAA Clients** and click **Create**. Add new client with name of **R2**, configure IP address of **2.2.2.2**, select TACACS+ as a protocol and configure **Shared Secret** of **cisco123**. Select **Single Connect Device** option and click **Submit**.



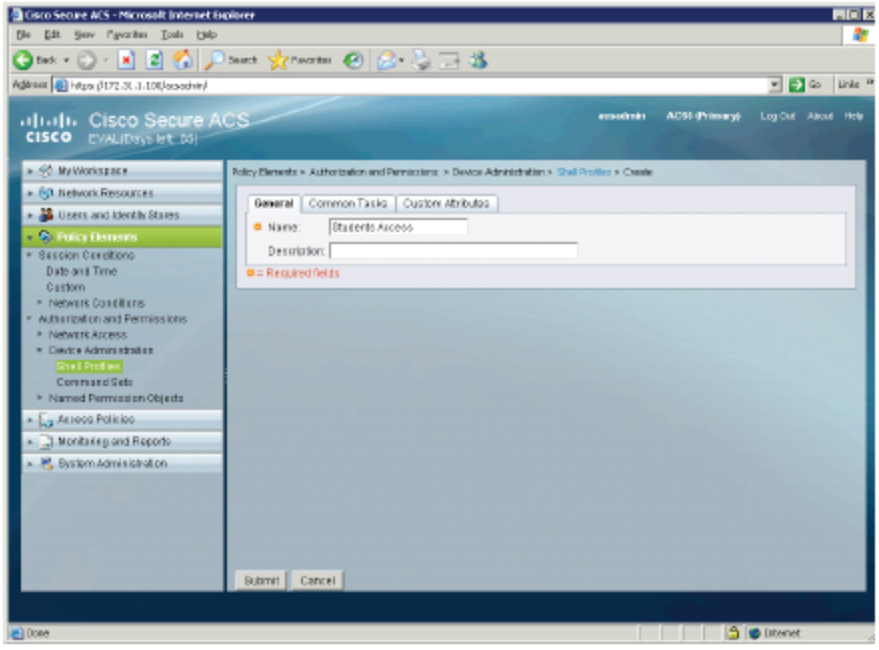

**Step 4** Create a new user on the ACS.

- Go to **Users and Identity Stores > Users** and click **Create**. Add new user with a name of **student4** and password of **student4**, select **Students** under **Identity Groups** and click **Submit**.

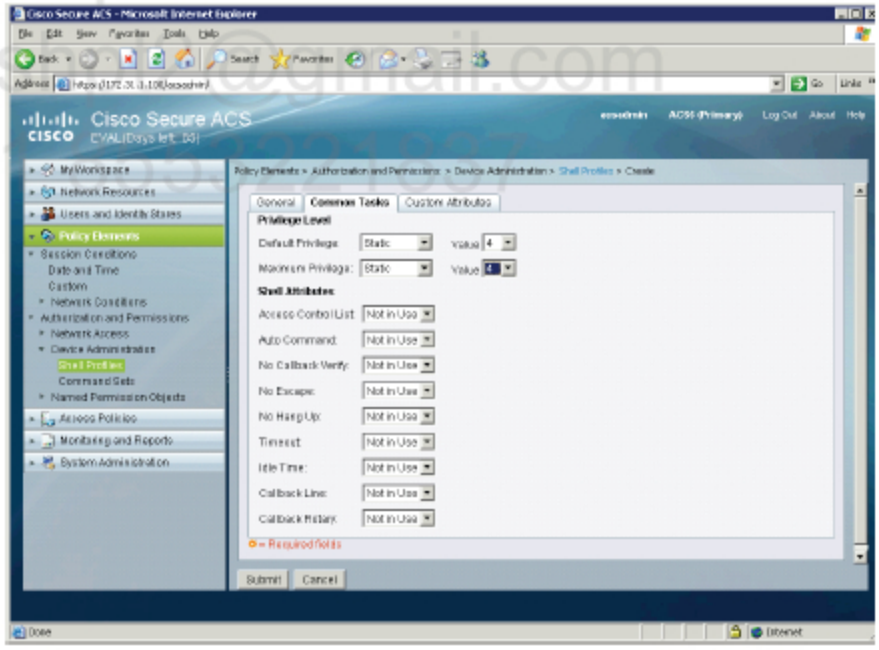



**Step 5** Create Shell Profile with provilge level 4 assigned.

- Go to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** and click **Create**. On the **General** tab provide a name for the profile (e.g. Students Access).

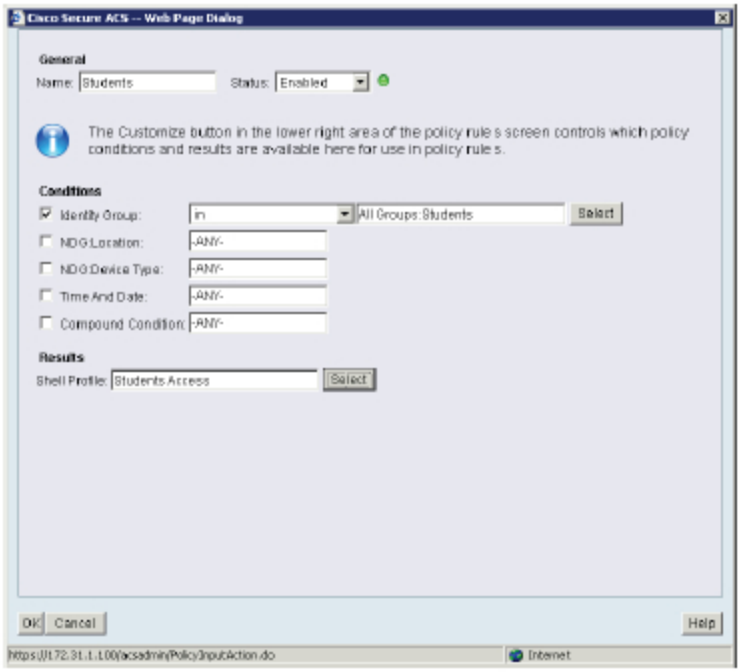



- Click on **Common Tasks** tab and set **Default Priviledge** to **4** and **Max Privilege** to **4**. Click on **Submit**.



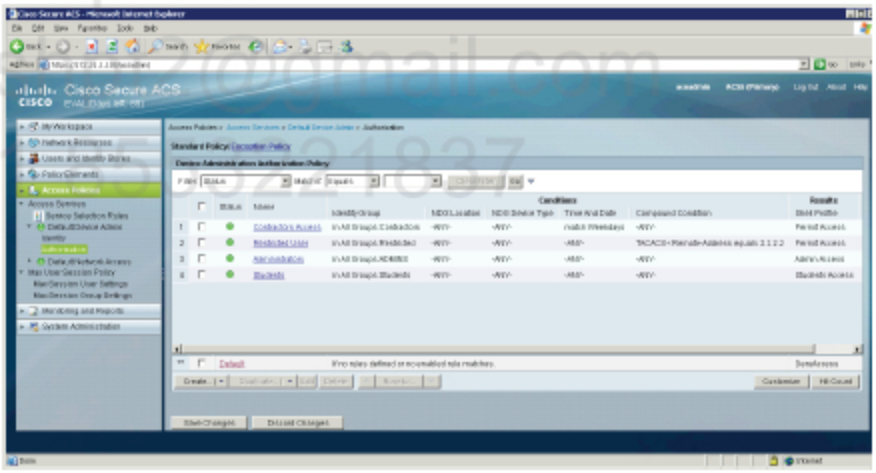

**Step 6** Configure new authorization rule for the user.

- Go to **Access Policies > Access Services > Default Device Admin > Authorization** and click **Create**. Enter name for the rule (e.g. Students), select **Students** for **Identity Group** and assign **Shell Profile** of **Students Access**. Click **OK**.






- Click **Save Changes**.



## Verification

### TELNET to R2 from R1 and authenticate as student4.

```
R1#tel 100.2.2.2
Trying 100.2.2.2 ... Open
username: student4
password:

R2#sh privilege
Current privilege level is 4
R2#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  configure        Enter configuration mode
  connect          Open a terminal connection
  credential       load the credential info from file system
  crypto           Encryption related commands.
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  do-exec          Mode-independent "do-exec" prefix support
  enable           Turn on privileged commands
  ethernet         Ethernet parameters
  exit             Exit from the EXEC
  help             Description of the interactive help system
  ips              Intrusion Prevention System
  lat              Open a lat connection
  lig              LISP Internet Groper
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#?
Configure commands:
  beep       Configure BEEP (Blocks Extensible Exchange Protocol)
  call       Configure Call parameters
  cts        Cisco Trusted Security commands
  default    Set a command to its defaults
  end        Exit from configure mode
  exit       Exit from configure mode
  help       Description of the interactive help system
  interface  Select an interface to configure
  ip         Global IP configuration subcommands
  netconf    Configure NETCONF
  no         Negate a command or set its defaults
  pfr        Performance Routing configuration submodes
  sasl       Configure SASL
```

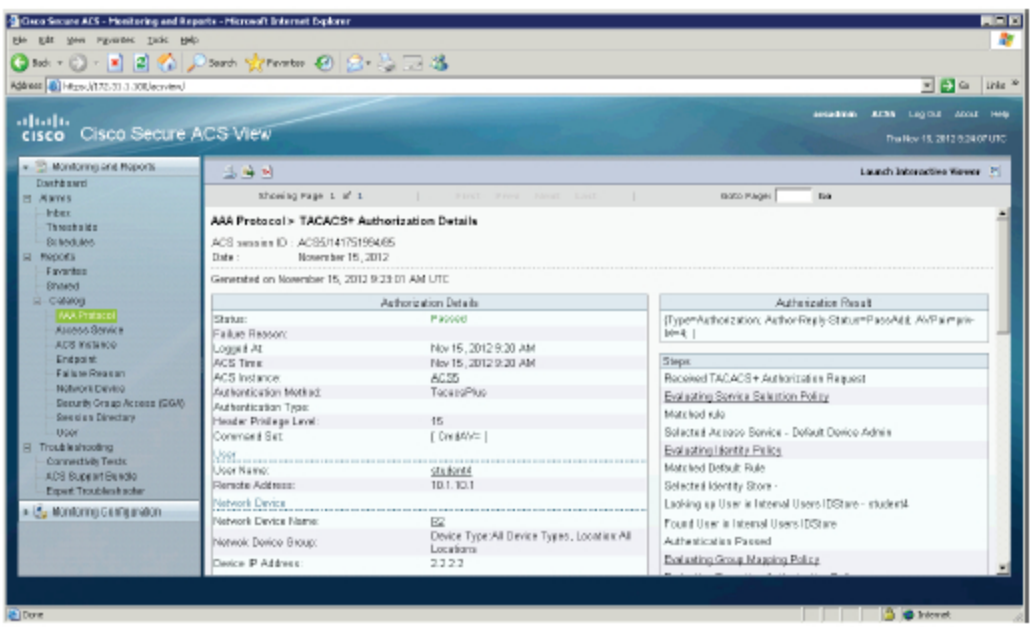
```
  waas        IOS Wide Area Application Services
  wsma        Configure Web Services Management Agents

R2(config)#
```

## Debug on R2 shows:

```
R2#deb aaa authentication
AAA Authentication debugging is on
R2#deb aaa authorization
AAA Authorization debugging is on
R2#
R2#
R2#
*Nov 15 09:20:02.908: AAA/BIND(00000012): Bind i/f
*Nov 15 09:20:02.908: AAA/AUTHEN/LOGIN (00000012): Pick method list 'VTY-AAA'
R2#
*Nov 15 09:20:10.545: AAA/AUTHOR (0x12): Pick method list 'VTY-AUTHZ'
*Nov 15 09:20:10.595: AAA/AUTHOR/EXEC(00000012): processing AV cmd=
*Nov 15 09:20:10.595: AAA/AUTHOR/EXEC(00000012): processing AV priv-lvl=4
*Nov 15 09:20:10.595: AAA/AUTHOR/EXEC(00000012): Authorization successful
R2#
*Nov 15 09:20:16.582: AAA/AUTHOR: auth_need : user= 'student4' ruser= 'R2'rem_addr=
'10.1.10.1' priv= 3 list= '' AUTHOR-TYPE= 'command'
R2#
*Nov 15 09:20:27.243: AAA/AUTHOR: auth_need : user= 'student4' ruser= 'R2'rem_addr=
'10.1.10.1' priv= 4 list= '' AUTHOR-TYPE= 'command'
```



## You should see in TACACS Authorization log on the ACS:



Verify if fallback user works by temporarly block out TACACS traffic on the ASA firewall. Then try to authenticate.

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


User Access Verification

Username: student4
Password:

% Authentication failed
```

Note that student4 cannot authenticate. We must use local username to authenticate.

```
Username: local4
Password:

R2#sh priv
Current privilege level is 4
```

## Task 3 – TACACS+ command authorization (IOS)

User "r1admin" has privilege level 15 (as configured in previous task). Configure ACS to authorize this user to issue "show run" command only and be able to disconnect from Telnet session using "logout" command.

*Command authorization can be configured on the ACS. This is very flexible solution so that every user in a specified group on the ACS has access to a list of commands.*
*Remember that the user must see the command on an appropriate level to access it. So that we first need to "move" a command to a lower level and then configure command authorization on the ACS. The ACS will confirm that the user may have (or may not) access to a specified command.*
*The most common scenario is when the user has privilege level 15 but is limited/authorized to run specific commands only. The disadvantage of this is that the user sees all commands but can run only some of them (or all if specified on ACS for that user/group).*
*Keep in mind that configuration commands (commands issued in configuration mode) and console commands (commands issued while connected through the console) are not authorized by default. You must configure this explicitly.*



*Command authorization only works for level for which it was configured. So that we can have a scenario when a user has access to privilege level 15 and sees all commands accessible on the router but cannot use some of them (is not authorized to use them) as those commands may be from different level. This is very common mistake because we often forget that there are default levels of 0 and 1 with some useful commands on those levels. For example, the command "exit" is on level 0 so that we cannot close the session or change the configuration mode without allowing this simple command.*

### Configuration

Complete these steps:

**Step 1** Configure R1 to authorize commands.

```
!
aaa authorization commands 0 VTY-AAA-CMD group tacacs+
aaa authorization commands 1 VTY-AAA-CMD group tacacs+
aaa authorization commands 15 VTY-AAA-CMD group tacacs+
```

```
!
line vty 0 4
 authorization commands 0 VTY-AAA-CMD
 authorization commands 1 VTY-AAA-CMD
 authorization commands 15 VTY-AAA-CMD
!
```

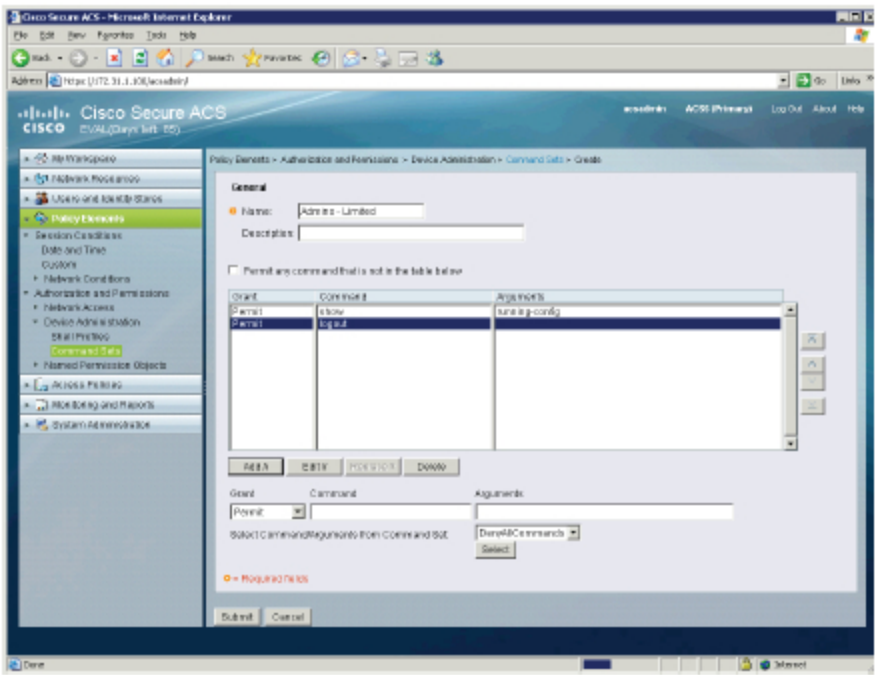
```
Why do we need to configure command authorization for all 3 levels?
Command 'logout' is from level 0
Command 'show runn' is from level 15
 Other commands MUST NOT be allowed, so the router MUST send them to
 ACS in order to get authorization. If we not enable command
 authorization on level 1, other commands (e.g. 'show priv') will be
 allowed without even consulting ACS.
```

**Step 2** Configure Command Set on ACS.

- Go to **Policy Elements > Authorization and Permissions > Device Administration > Command Sets** and click **Create**. Name the new object **Admins – Limited** and add to allowed commands list the following commands:

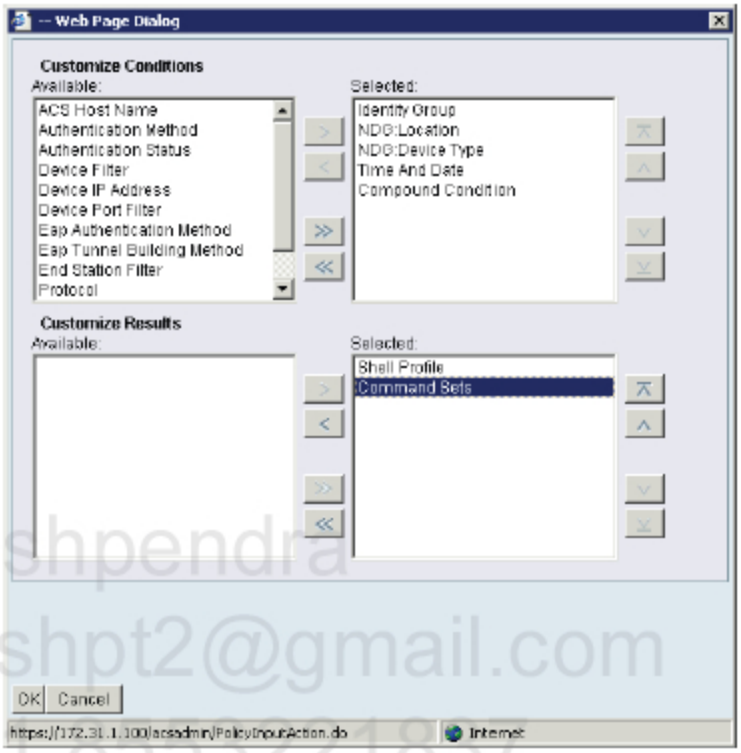


| Grant | Command | Arguments |
|---|---|---|
| **Permit** | Show | Running-config |
| **Permit** | logout | |



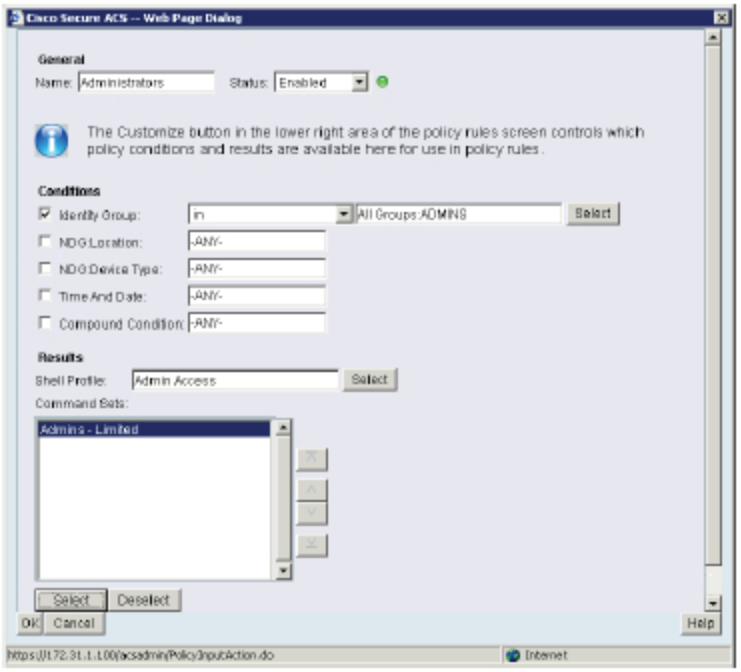
**Step 3** Reconfigure Authorization profile for ADMINS group.

- Go to **Access Policies > Access Services > Default Device Admin > Authorization** and click **Customize**. Select **Command Sets** from the left pane and move it to **Selected** pane. Click **OK**.



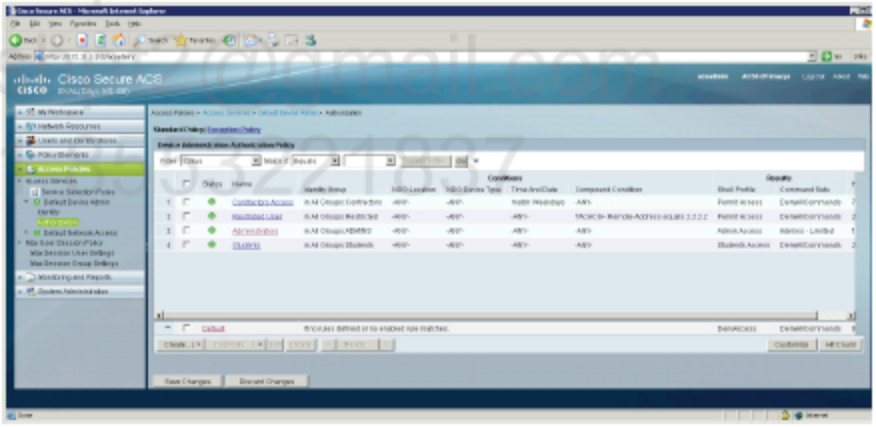



- Click on **Administrators** rule to edit it. Click Select button under **Command Sets** list and chose **Admins – Limited** command set. Click **OK**.



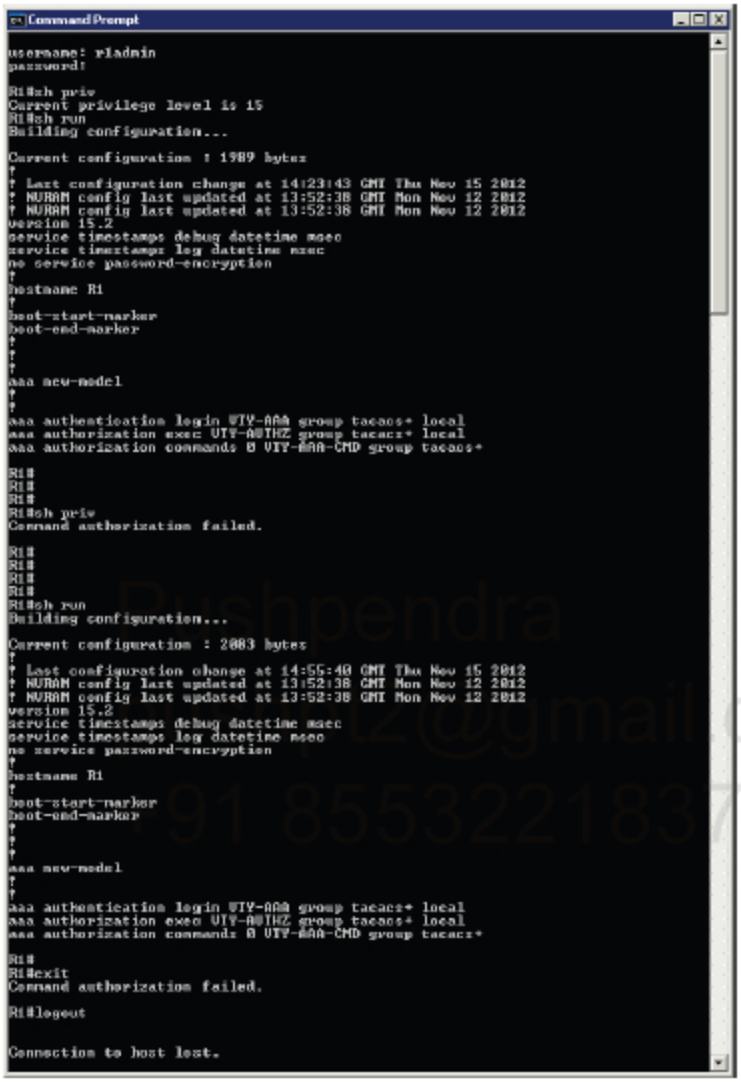



- Click on **Save Changes** button.



## Verification

TELNET to R1 from WinXP and authenticate as r1admin. Check if you can run commands.




**As you can see you can run 'show run' and 'logout' commands but you cannot run 'exit' and 'sh priv' commands. This is because those commands are not authorized. You can check ACS log to see that.**

| ACS View Timestamp | ACS Timestamp | Status | Details | Failure Reason | User Name | Command Set | Shell Profile | Network Device |
|---|---|---|---|---|---|---|---|---|
| Nov 15,12 2:56:09.453 PM | Nov 15,12 2:56:08.426 PM | ✔ | | | r1admin | [ CmdAV=logout ] | | R1 |
| Nov 15,12 2:56:05.403 PM | Nov 15,12 2:56:06.376 PM | ✖ | | 13025 Command failed to match a Permit rule | r1admin | [ CmdAV=exit ] | | R1 |
| Nov 15,12 2:55:56.033 PM | Nov 15,12 2:55:58.016 PM | ✔ | | | r1admin | [ CmdAV=show running-config ] | | R1 |
| Nov 15,12 2:55:44.423 PM | Nov 15,12 2:55:44.376 PM | ✖ | | 13025 Command failed to match a Permit rule | r1admin | [ CmdAV=show privilege ] | | R1 |
| Nov 15,12 2:54:54.153 PM | Nov 15,12 2:54:54.136 PM | ✔ | | | r1admin | [ CmdAV=show running-config ] | | R1 |
| Nov 15,12 2:53:52.316 PM | Nov 15,12 2:53:52.293 PM | ✔ | | | r1admin | [ CmdAV= ] | Admin Access | R1 |

It is also recommended to run 'deb aaa authentication', 'deb aaa authorization', and 'deb tacacs' commands to see what exactly is happening behind the scene.

```
Nov 15 14:55:44.270: AAA/AUTHOR: auth_need : user= 'r1admin' ruser= 'R1'rem_addr=
'10.1.10.50' priv= 1 list= 'VTY-AAA-CMD' AUTHOR-TYPE= 'command'
Nov 15 14:55:44.270: AAA: parse name=tty2 idb type=-1 tty=-1
Nov 15 14:55:44.270: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=2
channel=0
Nov 15 14:55:44.270: AAA/MEMORY: create_user (0xB3091DF0) user='r1admin' ruser='R1'
ds0=0 port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=1
initial_task_id='0', vrf= (id=0)
Nov 15 14:55:44.270: tty2 AAA/AUTHOR/CMD (2279862949): Port='tty2' list='VTY-AAA-CMD'
service=CMD
Nov 15 14:55:44.270: AAA/AUTHOR/CMD: tty2 (2279862949) user='r1admin'
Nov 15 14:55:44.270: tty2 AAA/AUTHOR/CMD (2279862949): send AV service=shell
Nov 15 14:55:44.270: tty2 AAA/AUTHOR/CMD (2279862949): send AV cmd=show
Nov 15 14:55:44.270: tty2 AAA/AUTHOR/CMD (2279862949): send AV cmd-arg=privilege
Nov 15 14:55:44.270: tty2 AAA/AUTHOR/CMD (2279862949): send AV cmd-arg=<cr>
```

Note that using those recommended debugs you can check what level a particular command is at (priv=1), what user is trying to run the command (user='r1admin') and the command itself.



```
Nov 15 14:55:44.270: tty2 AAA/AUTHOR/CMD(2279862949): found list "VTY-AAA-CMD"
Nov 15 14:55:44.270: tty2 AAA/AUTHOR/CMD (2279862949): Method=tacacs+ (tacacs+)
Nov 15 14:55:44.270: AAA/AUTHOR/TAC+: (2279862949): user=r1admin
Nov 15 14:55:44.270: AAA/AUTHOR/TAC+: (2279862949): send AV service=shell
Nov 15 14:55:44.270: AAA/AUTHOR/TAC+: (2279862949): send AV cmd=show
Nov 15 14:55:44.270: AAA/AUTHOR/TAC+: (2279862949): send AV cmd-arg=privilege
Nov 15 14:55:44.270: AAA/AUTHOR/TAC+: (2279862949): send AV cmd-arg=<cr>
Nov 15 14:55:44.270: TAC+: using previously set server 172.31.1.100 from group tacacs+
Nov 15 14:55:44.270: TAC+: 172.31.1.100 (2279862949) AUTHOR/START queued
Nov 15 14:55:44.474: TAC+: (2279862949) AUTHOR/START processed
Nov 15 14:55:44.474: TAC+: (-2015104347): received author response status = FAIL
Nov 15 14:55:44.474: AAA/AUTHOR (2279862949): Post authorization status = FAIL
Nov 15 14:55:44.474: AAA/MEMORY: free_user (0xB3091DF0) user='r1admin' ruser='R1'
port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=1 vrf= (id=0)
Nov 15 14:55:55.910: AAA/AUTHOR: auth_need : user= 'r1admin' ruser= 'R1'rem_addr=
'10.1.10.50' priv= 15 list= 'VTY-AAA-CMD' AUTHOR-TYPE= 'command'
Nov 15 14:55:55.910: AAA: parse name=tty2 idb type=-1 tty=-1
Nov 15 14:55:55.910: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=2
channel=0
Nov 15 14:55:55.910: AAA/MEMORY: create_user (0xB31254A0) user='r1admin' ruser='R1'
ds0=0 port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=15
initial_task_id='0', vrf= (id=0)
Nov 15 14:55:55.910: tty2 AAA/AUTHOR/CMD (1808451892): Port='tty2' list='VTY-AAA-CMD'
service=CMD
Nov 15 14:55:55.910: AAA/AUTHOR/CMD: tty2 (1808451892) user='r1admin'
Nov 15 14:55:55.910: tty2 AAA/AUTHOR/CMD (1808451892): send AV service=shell
Nov 15 14:55:55.910: tty2 AAA/AUTHOR/CMD (1808451892): send AV cmd=show
```

```
Nov 15 14:55:55.910: tty2 AAA/AUTHOR/CMD (1808451892): send AV cmd-arg=running-config
Nov 15 14:55:55.910: tty2 AAA/AUTHOR/CMD (1808451892): send AV cmd-arg=<cr>
```

Note that every command has its name and arguments. Even though you specify the command without the argument, there is always <cr> arguments sent to the ACS. CR means Carrier Return and this is nothing more than ENTER key.
Notice that even if you specify a short form of the command like 'sho runn' this will be expanded to the full command. You must always profide full commands in the ACS configuration.

```
Nov 15 14:55:55.910: tty2 AAA/AUTHOR/CMD(1808451892): found list "VTY-AAA-CMD"
Nov 15 14:55:55.910: tty2 AAA/AUTHOR/CMD (1808451892): Method=tacacs+ (tacacs+)
Nov 15 14:55:55.910: AAA/AUTHOR/TAC+: (1808451892): user=r1admin
Nov 15 14:55:55.910: AAA/AUTHOR/TAC+: (1808451892): send AV service=shell
Nov 15 14:55:55.910: AAA/AUTHOR/TAC+: (1808451892): send AV cmd=show
Nov 15 14:55:55.910: AAA/AUTHOR/TAC+: (1808451892): send AV cmd-arg=running-config
Nov 15 14:55:55.910: AAA/AUTHOR/TAC+: (1808451892): send AV cmd-arg=<cr>
Nov 15 14:55:55.910: TAC+: using previously set server 172.31.1.100 from group tacacs+
Nov 15 14:55:55.910: TAC+: 172.31.1.100 (1808451892) AUTHOR/START queued
Nov 15 14:55:56.117: TAC+: (1808451892) AUTHOR/START processed
Nov 15 14:55:56.117: TAC+: (1808451892): received author response status = PASS_ADD
Nov 15 14:55:56.117: AAA/AUTHOR (1808451892): Post authorization status = PASS_ADD
Nov 15 14:55:56.117: AAA/MEMORY: free_user (0xB31254A0) user='r1admin' ruser='R1'
port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=15 vrf= (id=0)
Nov 15 14:56:05.270: AAA/AUTHOR: auth_need : user= 'r1admin' ruser= 'R1'rem_addr=
'10.1.10.50' priv= 0 list= 'VTY-AAA-CMD' AUTHOR-TYPE= 'command'
Nov 15 14:56:05.270: AAA: parse name=tty2 idb type=-1 tty=-1
Nov 15 14:56:05.270: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=2
channel=0
Nov 15 14:56:05.270: AAA/MEMORY: create_user (0xB31254A0) user='r1admin' ruser='R1'
ds0=0 port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=0
initial_task_id='0', vrf= (id=0)
Nov 15 14:56:05.270: tty2 AAA/AUTHOR/CMD (1446193452): Port='tty2' list='VTY-AAA-CMD'
service=CMD
Nov 15 14:56:05.270: AAA/AUTHOR/CMD: tty2 (1446193452) user='r1admin'
Nov 15 14:56:05.270: tty2 AAA/AUTHOR/CMD (1446193452): send AV service=shell
Nov 15 14:56:05.270: tty2 AAA/AUTHOR/CMD (1446193452): send AV cmd=exit
Nov 15 14:56:05.270: tty2 AAA/AUTHOR/CMD (1446193452): send AV cmd-arg=<cr>
Nov 15 14:56:05.270: tty2 AAA/AUTHOR/CMD(1446193452): found list "VTY-AAA-CMD"
Nov 15 14:56:05.270: tty2 AAA/AUTHOR/CMD (1446193452): Method=tacacs+ (tacacs+)
Nov 15 14:56:05.270: AAA/AUTHOR/TAC+: (1446193452): user=r1admin
Nov 15 14:56:05.270: AAA/AUTHOR/TAC+: (1446193452): send AV service=shell
Nov 15 14:56:05.270: AAA/AUTHOR/TAC+: (1446193452): send AV cmd=exit
Nov 15 14:56:05.270: AAA/AUTHOR/TAC+: (1446193452): send AV cmd-arg=<cr>
R1#
Nov 15 14:56:05.270: TAC+: using previously set server 172.31.1.100 from group tacacs+
Nov 15 14:56:05.270: TAC+: 172.31.1.100 (1446193452) AUTHOR/START queued
Nov 15 14:56:05.474: TAC+: (1446193452) AUTHOR/START processed
Nov 15 14:56:05.474: TAC+: (1446193452): received author response status = FAIL
Nov 15 14:56:05.474: AAA/AUTHOR (1446193452): Post authorization status = FAIL
```

```
Nov 15 14:56:05.474: AAA/MEMORY: free_user (0xB31254A0) user='r1admin' ruser='R1'
port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=0 vrf= (id=0)
Nov 15 14:56:08.317: AAA/AUTHOR: auth_need : user= 'r1admin' ruser= 'R1'rem_addr=
'10.1.10.50' priv= 0 list= 'VTY-AAA-CMD' AUTHOR-TYPE= 'command'
Nov 15 14:56:08.318: AAA: parse name=tty2 idb type=-1 tty=-1
Nov 15 14:56:08.318: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=2
channel=0
Nov 15 14:56:08.318: AAA/MEMORY: create_user (0xB3091DF0) user='r1admin' ruser='R1'
ds0=0 port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=0
initial_task_id='0', vrf= (id=0)
Nov 15 14:56:08.318: tty2 AAA/AUTHOR/CMD (3058483521): Port='tty2' list='VTY-AAA-CMD'
service=CMD
Nov 15 14:56:08.318: AAA/AUTHOR/CMD: tty2 (3058483521) user='r1admin'
Nov 15 14:56:08.318: tty2 AAA/AUTHOR/CMD (3058483521): send AV service=shell
Nov 15 14:56:08.318: tty2 AAA/AUTHOR/CMD (3058483521): send AV cmd=logout
Nov 15 14:56:08.318: tty2 AAA/AUTHOR/CMD (3058483521): send AV cmd-arg=<cr>
Nov 15 14:56:08.318: tty2 AAA/AUTHOR/CMD(3058483521): found list "VTY-AAA-CMD"
Nov 15 14:56:08.318: tty2 AAA/AUTHOR/CMD (3058483521): Method=tacacs+ (tacacs+)
Nov 15 14:56:08.318: AAA/AUTHOR/TAC+: (3058483521): user=r1admin
Nov 15 14:56:08.318: AAA/AUTHOR/TAC+: (3058483521): send AV service=shell
Nov 15 14:56:08.318: AAA/AUTHOR/TAC+: (3058483521): send AV cmd=logout
Nov 15 14:56:08.318: AAA/AUTHOR/TAC+: (3058483521): send AV cmd-arg=<cr>
Nov 15 14:56:08.318: TAC+: using previously set server 172.31.1.100 from group tacacs+
Nov 15 14:56:08.318: TAC+: 172.31.1.100 (3058483521) AUTHOR/START queued
Nov 15 14:56:08.520: TAC+: (3058483521) AUTHOR/START processed
Nov 15 14:56:08.520: TAC+: (-1236483775): received author response status = PASS_ADD
Nov 15 14:56:08.520: AAA/AUTHOR (3058483521): Post authorization status = PASS_ADD
Nov 15 14:56:08.520: AAA/MEMORY: free_user (0xB3091DF0) user='r1admin' ruser='R1'
port='tty2' rem_addr='10.1.10.50' authen_type=ASCII service=NONE priv=0 vrf= (id=0)
```

# LAB 2.33. Accounting using TACACS+ and RADIUS (IOS)

## Objectives

This lab shows how to configure routers to perform accounting using TACACS+ and RADIUS protocols.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| ACS | NIC | 172.31.1.100 |
| WinXP | NIC | 10.1.10.50 |

## Task 1 – TACACS+ accounting (IOS)

Configure R2 to send accounting information for all users connecting to the router via TELNET/SSH. There must be session start and stop events in the log. In addition to that, enable privilege level 4 commands accounting.

*Using AAA services we can perform accounting that is nothing more than information logging about user's session. This information may be useful for billing purposes or for security reasons so that we know who and when has connected to the device and what commands he/she used.*

*There are two basic accounting services:*

- *EXEC accounting – for user's access to the shell*
- *COMMAND accounting – for information about commands entered by the user*



### Configuration

Complete these steps:

**Step 1** Configure R2 for TACACS+ accounting.

```
!
aaa accounting exec VTY-AAA-ACC start-stop group tacacs+
aaa accounting commands 4 VTY-AAA-ACC start-stop group tacacs+
!
line vty 0 4
 accounting exec VTY-AAA-ACC
 accounting commands 4 VTY-AAA-ACC
!
```

## Verification

TELNET to R2 from R1 and authenticate as student4. Check debug command output on R2 and ACS logs.

```
R1#telnet 100.2.2.2
Trying 100.2.2.2 ... Open

username: student4
password:

R2#
R2#sho priv
Current privilege level is 4
R2#
R2#exit

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

### Debug on R2



```
R2#deb aaa accounting
AAA Accounting debugging is on
R2#deb tacacs
TACACS access control debugging is on
R2#
```

```
        // TACACS START message

*Nov 15 16:19:52.288: AAA/ACCT/EVENT/(00000014): CALL START
*Nov 15 16:19:52.288: Getting session id for NET(00000014) : db=B3157518
*Nov 15 16:19:52.288: AAA/ACCT(00000000): add node, session 3
*Nov 15 16:19:52.288: AAA/ACCT/NET(00000014): add, count 1
*Nov 15 16:19:52.288: Getting session id for NONE(00000014) : db=B3157518
*Nov 15 16:19:52.291: TPLUS: Queuing AAA Authentication request 20 for processing
*Nov 15 16:19:52.291: TPLUS: processing authentication start request id 20
*Nov 15 16:19:52.291: TPLUS: Authentication start packet created for 20()
*Nov 15 16:19:52.291: TPLUS: Using server 172.31.1.100
*Nov 15 16:19:52.291: TPLUS(00000014)/0/NB_WAIT/B3161030: Started 5 sec timeout
*Nov 15 16:19:52.301: TPLUS(00000014)/0/NB_WAIT: wrote entire 33 bytes request
*Nov 15 16:19:52.301: TPLUS: Would block while reading pak header
*Nov 15 16:19:52.304: TPLUS(00000014)/0/READ: read entire 12 header bytes (expect 16
bytes)
*Nov 15 16:19:52.305: TPLUS(00000014)/0/READ: read entire 28 bytes response
*Nov 15 16:19:52.305: TPLUS(00000014)/0/B3161030: Processing the reply packet
*Nov 15 16:19:52.305: TPLUS: Received authen response status GET_USER (7)
*Nov 15 16:19:55.178: TPLUS: Queuing AAA Authentication request 20 for processing
*Nov 15 16:19:55.178: TPLUS: processing authentication continue request id 20
*Nov 15 16:19:55.178: TPLUS: Authentication continue packet generated for 20
```

```
*Nov 15 16:19:55.178: TPLUS(00000014)/0/WRITE/B28438C8: Started 5 sec timeout
*Nov 15 16:19:55.178: TPLUS(00000014)/0/WRITE: wrote entire 25 bytes request
*Nov 15 16:19:55.187: TPLUS(00000014)/0/READ: read entire 12 header bytes (expect 16
bytes)
*Nov 15 16:19:55.187: TPLUS(00000014)/0/READ: read entire 28 bytes response
*Nov 15 16:19:55.187: TPLUS(00000014)/0/B28438C8: Processing the reply packet
R2#
*Nov 15 16:19:55.187: TPLUS: Received authen response status GET_PASSWORD (8)
R2#
*Nov 15 16:19:57.797: TPLUS: Queuing AAA Authentication request 20 for processing
*Nov 15 16:19:57.797: TPLUS: processing authentication continue request id 20
*Nov 15 16:19:57.797: TPLUS: Authentication continue packet generated for 20
*Nov 15 16:19:57.797: TPLUS(00000014)/0/WRITE/B28438C8: Started 5 sec timeout
*Nov 15 16:19:57.797: TPLUS(00000014)/0/WRITE: wrote entire 25 bytes request
*Nov 15 16:19:57.805: TPLUS(00000014)/0/READ: read entire 12 header bytes (expect 6
bytes)
*Nov 15 16:19:57.805: TPLUS(00000014)/0/READ: read entire 18 bytes response
*Nov 15 16:19:57.805: TPLUS(00000014)/0/B28438C8: Processing the reply packet
*Nov 15 16:19:57.805: TPLUS: Received authen response status PASS (2)
*Nov 15 16:19:57.809: TPLUS: Queuing AAA Authorization request 20 for processing
*Nov 15 16:19:57.809: TPLUS: processing authorization request id 20
*Nov 15 16:19:57.809: TPLUS: Protocol set to None .....Skipping
*Nov 15 16:19:57.809: TPLUS: Sending AV service=shell
*Nov 15 16:19:57.809: TPLUS: Sending AV cmd*
*Nov 15 16:19:57.809: TPLUS: Authorization request created for 20(student4)
*Nov 15 16:19:57.809: TPLUS: using previously set server 172.31.1.100 from group
tacacs+
*Nov 15 16:19:57.809: TPLUS(00000014)/0/IDLE/B28438C8: got immediate connect on new 0
*Nov 15 16:19:57.809: TPLUS(00000014)/0/WRITE/B28438C8: Started 5 sec timeout
*Nov 15 16:19:57.809: TPLUS(00000014)/0/WRITE: wrote entire 60 bytes request
*Nov 15 16:19:57.818: TPLUS(00000014)/0/READ: read entire 12 header bytes (expect 17
bytes)
*Nov 15 16:19:57.818: TPLUS(00000014)/0/READ: read entire 29 bytes response
*Nov 15 16:19:57.818: TPLUS(00000014)/0/B28438C8: Processing the reply packet
*Nov 15 16:19:57.818: TPLUS: Processed AV priv-lvl=4
*Nov 15 16:19:57.818: TPLUS: received authorization response for 20: PASS
*Nov 15 16:19:57.818: AAA/ACCT/EXEC(00000014): Pick method list 'VTY-AAA-ACC'
*Nov 15 16:19:57.818: AAA/ACCT/SETMLIST(00000014): Handle 4C000005, mlist B31611D0,
Name VTY-AAA-ACC
*Nov 15 16:19:57.818: Getting session id for EXEC(00000014) : db=B3157518
*Nov 15 16:19:57.818: AAA/ACCT/EXEC(00000014): add, count 2
*Nov 15 16:19:57.818: AAA/ACCT/EVENT/(00000014): EXEC UP
*Nov 15 16:19:57.818: AAA/ACCT/EXEC(00000014): Queueing record is START

        // TACACS Accounting message for shell access.

*Nov 15 16:19:57.822: AAA/ACCT(00000014): Accounting method=tacacs+ (TACACS+)
*Nov 15 16:19:57.822: TPLUS: Queuing AAA Accounting request 20 for processing
*Nov 15 16:19:57.822: TPLUS: processing accounting request id 20
*Nov 15 16:19:57.822: TPLUS: Sending AV task_id=3
*Nov 15 16:19:57.822: TPLUS: Sending AV timezone=GMT
```

```
*Nov 15 16:19:57.822: TPLUS: Sending AV service=shell
*Nov 15 16:19:57.822: TPLUS: Accounting request created for 20(student4)
*Nov 15 16:19:57.822: TPLUS: using previously set server 172.31.1.100 from group
tacacs+
*Nov 15 16:19:57.823: TPLUS(00000014)/0/IDLE/B31644E8: got immediate connect on new 0
*Nov 15 16:19:57.823: TPLUS(00000014)/0/WRITE/B31644E8: Started 5 sec timeout
*Nov 15 16:19:57.823: TPLUS(00000014)/0/WRITE: wrote entire 79 bytes request
*Nov 15 16:19:57.827: TPLUS(00000014)/0/READ: read entire 12 header bytes (expect 5
bytes)
*Nov 15 16:19:57.827: TPLUS(00000014)/0/READ: read entire 17 bytes response
*Nov 15 16:19:57.827: TPLUS(00000014)/0/B31644E8: Processing the reply packet
*Nov 15 16:19:57.827: TPLUS: Received accounting response with status PASS
*Nov 15 16:19:57.827: AAA/ACCT/EXEC(00000014): START protocol reply PASS
*Nov 15 16:19:57.827: AAA/ACCT(00000014): Accounting response status = SUCCESS
*Nov 15 16:19:57.827: AAA/ACCT(00000014): Send START accounting notification to EM
successfully
*Nov 15 16:19:57.827: AAA/ACCT(00000014): mlist_periodic is not set, interval 0
*Nov 15 16:20:12.458: unknown AAA/DISC: 1/"User Request"
*Nov 15 16:20:12.458: unknown AAA/DISC/EXT: 1020/"User Request"
*Nov 15 16:20:12.458: AAA/ACCT/EXEC(00000014): Pick method list 'VTY-AAA-ACC'
*Nov 15 16:20:12.458: AAA/ACCT/SETMLIST(00000014): Handle 4C000005, mlist B31611D0,
Name VTY-AAA-ACC
```



// TACACS STOP message, see what information is sent while session's over.

```
*Nov 15 16:20:12.462: AAA/ACCT/EVENT/(00000014): CALL STOP
*Nov 15 16:20:12.462: AAA/ACCT/CALL STOP(00000014): Sending stop requests
*Nov 15 16:20:12.462: AAA/ACCT(00000014): Send all stops
*Nov 15 16:20:12.462: AAA/ACCT/EXEC(00000014): STOP
*Nov 15 16:20:12.462: AAA/ACCT/EXEC(00000014): Queueing record is STOP osr 1
*Nov 15 16:20:12.462: AAA/ACCT/NET(00000014): STOP
*Nov 15 16:20:12.462: AAA/ACCT/NET(00000014): Method list not found
*Nov 15 16:20:12.462: AAA/ACCT/NET(00000014): free_rec, count 1
*Nov 15 16:20:12.462: /AAA/ACCTNET(00000014) reccnt 1, csr TRUE, osr 1
*Nov 15 16:20:12.462: AAA/ACCT(00000014): Accounting method=tacacs+ (TACACS+)
*Nov 15 16:20:12.462: TPLUS: Queuing AAA Accounting request 20 for processing
*Nov 15 16:20:12.462: TPLUS: processing accounting request id 20
*Nov 15 16:20:12.462: TPLUS: Sending AV task_id=3
*Nov 15 16:20:12.462: TPLUS: Sending AV timezone=GMT
*Nov 15 16:20:12.462: TPLUS: Sending AV service=shell
*Nov 15 16:20:12.462: TPLUS: Sending AV disc-cause=1
*Nov 15 16:20:12.462: TPLUS: Sending AV disc-cause-ext=9
*Nov 15 16:20:12.462: TPLUS: Sending AV pre-session-time=6
*Nov 15 16:20:12.462: TPLUS: Sending AV elapsed_time=15
*Nov 15 16:20:12.463: TPLUS: Sending AV stop_time=1352996412
*Nov 15 16:20:12.463: TPLUS: Accounting request created for 20(student4)
*Nov 15 16:20:12.463: TPLUS: using previously set server 172.31.1.100 from group
tacacs+
*Nov 15 16:20:12.463: TPLUS(00000014)/0/IDLE/B3161030: got immediate connect on new 0
*Nov 15 16:20:12.463: TPLUS(00000014)/0/WRITE/B3161030: Started 5 sec timeout
*Nov 15 16:20:12.463: TPLUS(00000014)/0/WRITE: wrote entire 165 bytes request
```

```
*Nov 15 16:20:12.467: TPLUS(00000014)/0/READ: read entire 12 header bytes (expect 5
bytes)
*Nov 15 16:20:12.467: TPLUS(00000014)/0/READ: read entire 17 bytes response
*Nov 15 16:20:12.467: TPLUS(00000014)/0/B3161030: Processing the reply packet
*Nov 15 16:20:12.467: TPLUS: Received accounting response with status PASS
*Nov 15 16:20:12.467: AAA/ACCT/EXEC(00000014): STOP protocol reply PASS
*Nov 15 16:20:12.467: AAA/ACCT(00000014): Accounting response status = SUCCESS
*Nov 15 16:20:12.467: AAA/ACCT(00000014): Send STOP accounting notification to EM
successfully
*Nov 15 16:20:12.467: AAA/ACCT/EXEC(00000014): Cleaning up from Callback osr 0
*Nov 15 16:20:12.467: AAA/ACCT(00000014): del node, session 3
*Nov 15 16:20:12.467: AAA/ACCT/EXEC(00000014): free_rec, count 0
*Nov 15 16:20:12.467: /AAA/ACCTEXEC(00000014) reccnt 0, csr TRUE, osr 0
*Nov 15 16:20:12.467: AAA/ACCT/EXEC(00000014): Last rec in db, intf not enqueued
```

## TACACS Accounting log on ACS shows two events.

| ACS View Timestamp | ACS Timestamp | Details | ACS | User Name |
|---|---|---|---|---|
| Nov 15,12 4:20:12.520 PM | Nov 15,12 4:20:12.466 PM | | ACS5 | student4 |
| Nov 15,12 4:19:57.840 PM | Nov 15,12 4:19:57.826 PM | | ACS5 | student4 |

## Task 2 – RADIUS accounting (IOS)

Configure R2 to send EXEC accounting information (for all possible lines) using RADIUS protocol. Set RADIUS secret key to cisco123 and source RADIUS packets from R2's loopback0 interface. Periodically verify RADIUS server reachability using 'radtest' user and use newer ports for accounting.

*RADIUS usues ports UDP/1813 or UDP/1646 for accounting purposes. You must open a path to the ACS server if there is a firewall in between the client and AAA server.*
*RADIUS messages are usually more informative than TACACS+. Hence, RADIUS is often used for billing purposes.*

### Configuration

Complete these steps:

**Step 1** Configure R2 for RADIUS accounting.

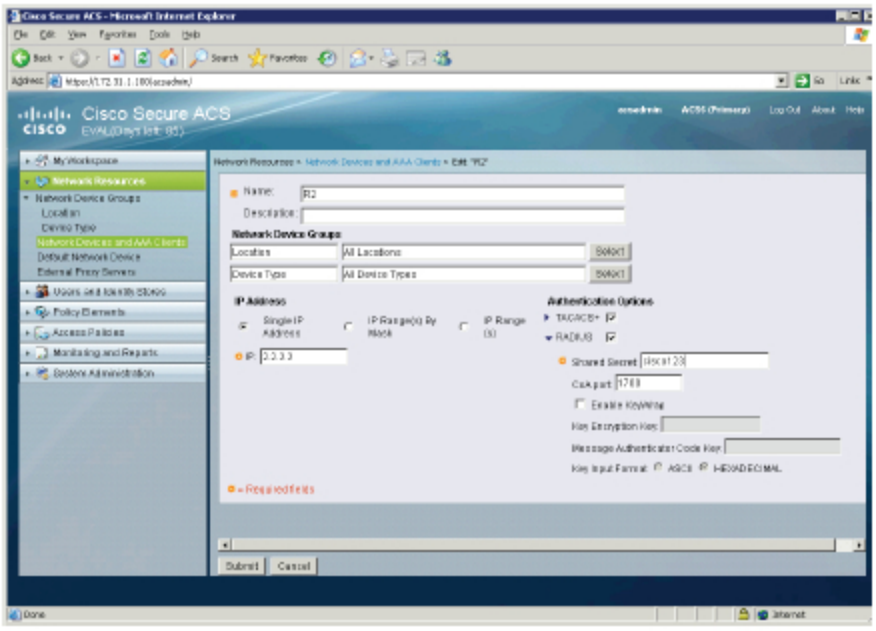
```
!
aaa accounting exec default start-stop group radius
!
ip radius source-interface Loopback0
radius server ACS
 address ipv4 172.31.1.100 auth-port 1812 acct-port 1813
 automate-tester username radtest
 key cisco123
!
```

**Step 2** Reconfigure ASA firewall.

```
!
access-list OUTSIDE_IN permit udp host 2.2.2.2 host 172.31.1.100 eq
1813
!
```

**Step 3** Reconfigure R2 AAA client on ACS.

- Go to **Network Resources > Network Devices and AAA Clients** and edit **R2** device. Check **RADIUS** protocol and set **Shared Secret**. Click **Submit**.






## Verification

TELNET to R2 from R1 and authenticate as student4. Check debug command output on R2 and ACS logs.

**There is no log messages on R2. Why?**
**This is because RADIUS accounting is enabled using 'default' AAA list. The 'default' method means it is automatically applied to all 'lines' including CONSOLE and VTY. Unfortunately, we have 'named' list applied already to the VTY. The list is for TACACS+ accounting and is takes precendence before 'default' list for RADIUS.**
**There is no way to enable accounting of the same service (EXEC in this case) to two different protocols.**

Connect to R2 CONSOLE and see debugs.

```
*Nov 15 16:55:16.571: RADIUS/ENCODE(00000017):Orig. component type = Exec
*Nov 15 16:55:16.571: RADIUS(00000017): Config NAS IP: 2.2.2.2
*Nov 15 16:55:16.571: RADIUS(00000017): Config NAS IPv6: ::
*Nov 15 16:55:16.571: RADIUS(00000017): sending
*Nov 15 16:55:16.571: RADIUS(00000017): Sending a IPv4 Radius Packet
*Nov 15 16:55:16.571: RADIUS(00000017): Send Accounting-Request to 172.31.1.100:1813 id
1646/1, len 78
*Nov 15 16:55:16.571: RADIUS:  authenticator 47 91 6C BF 50 C6 84 9F - A4 7D 6D 77 E1
6D 03 73
*Nov 15 16:55:16.571: RADIUS:  Acct-Session-Id     [44]  10  "00000006"
*Nov 15 16:55:16.571: RADIUS:  Acct-Authentic      [45]  6   Local
[2]
```

```
*Nov 15 16:55:16.571: RADIUS:  Acct-Status-Type    [40]  6   Start
[1]
*Nov 15 16:55:16.571: RADIUS:  NAS-Port            [5]   6   0
*Nov 15 16:55:16.571: RADIUS:  NAS-Port-Id         [87]  6   "tty0"
*Nov 15 16:55:16.571: RADIUS:  NAS-Port-Type       [61]  6   Async
[0]
*Nov 15 16:55:16.571: RADIUS:  Service-Type        [6]   6   NAS Prompt
[7]
*Nov 15 16:55:16.571: RADIUS:  NAS-IP-Address      [4]   6   2.2.2.2
*Nov 15 16:55:16.571: RADIUS:  Acct-Delay-Time     [41]  6   0
*Nov 15 16:55:16.571: RADIUS(00000017): Started 5 sec timeout
*Nov 15 16:55:16.627: RADIUS: Received from id 1646/1 172.31.1.100:1813, Accounting-
response, len 20
*Nov 15 16:55:16.627: RADIUS:  authenticator 9A 60 DA 88 64 AB 2C DA - 2E AD E1 77 FD
06 5C 62
R2#
R2#exit


*Nov 15 16:55:25.271: RADIUS/ENCODE(00000017):Orig. component type = Exec
*Nov 15 16:55:25.271: RADIUS(00000017): Config NAS IP: 2.2.2.2
*Nov 15 16:55:25.271: RADIUS(00000017): Config NAS IPv6: ::
*Nov 15 16:55:25.271: RADIUS(00000017): sending
*Nov 15 16:55:25.271: RADIUS(00000017): Sending a IPv4 Radius Packet
*Nov 15 16:55:25.271: RADIUS(00000017): Send Accounting-Request to 172.31.1.100:1813 id
1646/2, len 90
*Nov 15 16:55:25.271: RADIUS:  authenticator 16 32 6B 1C C6 04 5E 31 - EA 8A 4D 71 14
7A FE 4D
*Nov 15 16:55:25.271: RADIUS:  Acct-Session-Id     [44]  10  "00000006"
*Nov 15 16:55:25.271: RADIUS:  Acct-Authentic      [45]  6   Local
[2]
*Nov 15 16:55:25.271: RADIUS:  Acct-Terminate-Cause[49]  6   user-request
[1]
*Nov 15 16:55:25.271: RADIUS:  Acct-Session-Time   [46]  6   9
*Nov 15 16:55:25.271: RADIUS:  Acct-Status-Type    [40]  6   Stop
[2]
*Nov 15 16:55:25.271: RADIUS:  NAS-Port            [5]   6   0
*Nov 15 16:55:25.271: RADIUS:  NAS-Port-Id         [87]  6   "tty0"
*Nov 15 16:55:25.271: RADIUS:  NAS-Port-Type       [61]  6   Async
[0]
*Nov 15 16:55:25.271: RADIUS:  Service-Type        [6]   6   NAS Prompt
[7]
*Nov 15 16:55:25.271: RADIUS:  NAS-IP-Address      [4]   6   2.2.2.2
*Nov 15 16:55:25.271: RADIUS:  Acct-Delay-Time     [41]  6   0
*Nov 15 16:55:25.271: RADIUS(00000017): Started 5 sec timeout
*Nov 15 16:55:25.373: RADIUS: Received from id 1646/2 172.31.1.100:1813, Accounting-
response, len 20
*Nov 15 16:55:25.373: RADIUS:  authenticator 18 43 23 D9 C6 E4 FA 19 - 07 D8 96 E8 BF
71 2E F8
R2>
```

```
*Nov 15 16:55:28.617: RADIUS/ENCODE(00000018):Orig. component type = Exec
*Nov 15 16:55:28.617: RADIUS(00000018): Config NAS IP: 2.2.2.2
*Nov 15 16:55:28.617: RADIUS(00000018): Config NAS IPv6: ::
*Nov 15 16:55:28.617: RADIUS(00000018): sending
*Nov 15 16:55:28.617: RADIUS(00000018): Sending a IPv4 Radius Packet
*Nov 15 16:55:28.617: RADIUS(00000018): Send Accounting-Request to 172.31.1.100:1813 id
1646/3, len 78
*Nov 15 16:55:28.617: RADIUS:  authenticator 29 9E DB 30 C3 EC A3 32 - FF 58 EB F8 4F
CF 59 12
*Nov 15 16:55:28.617: RADIUS:  Acct-Session-Id     [44]  10  "00000007"
*Nov 15 16:55:28.617: RADIUS:  Acct-Authentic      [45]  6   Local
[2]
*Nov 15 16:55:28.617: RADIUS:  Acct-Status-Type    [40]  6   Start
[1]
*Nov 15 16:55:28.617: RADIUS:  NAS-Port            [5]   6   0
*Nov 15 16:55:28.617: RADIUS:  NAS-Port-Id         [87]  6   "tty0"
*Nov 15 16:55:28.617: RADIUS:  NAS-Port-Type       [61]  6   Async
[0]
*Nov 15 16:55:28.617: RADIUS:  Service-Type        [6]   6   NAS Prompt
[7]
*Nov 15 16:55:28.617: RADIUS:  NAS-IP-Address      [4]   6   2.2.2.2
*Nov 15 16:55:28.617: RADIUS:  Acct-Delay-Time     [41]  6   0
*Nov 15 16:55:28.617: RADIUS(00000018): Started 5 sec timeout
R2>
*Nov 15 16:55:28.622: RADIUS: Received from id 1646/3 172.31.1.100:1813, Accounting-
response, len 20
*Nov 15 16:55:28.622: RADIUS:  authenticator 23 F9 07 0F 3E 51 B9 B9 - 55 AB E6 EF 91
F6 87 75
R2>
```



See RADIUS accounting log on ACS.

AAA Protocol > RADIUS Accounting

Date : November 15, 2012

Generated on November 15, 2012 4:56:06 PM UTC

Reload

Click for details

| ACS View Timestamp | ACS Timestamp | Details | Account StatusType | User Name | Calling Station ID | Endpoint IP Address | Account Authentic | Account Terminate |
|---|---|---|---|---|---|---|---|---|
| Nov 15, 12 4:55:28.646 PM | Nov 15, 12 4:55:28.616 PM | | Start | | | | Local | |
| Nov 15, 12 4:55:25.306 PM | Nov 15, 12 4:55:25.276 PM | | Stop | | | | Local | User Request |
| Nov 15, 12 4:55:16.636 PM | Nov 15, 12 4:55:16.630 PM | | Start | | | | Local | |

# LAB 2.34. IOS Authentication Proxy

## Objectives

This lab shows how to configure routers to perform Cut-Through Proxy authentication.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| ACS | NIC | 172.31.1.100 |
| WinXP | NIC | 10.1.10.50 |

## Task 1 – TACACS+ CTP (IOS)

Configure R1 so that it first authenticate and authorize users via TELNET and HTTP behind its 0/0 interface to be able to connect to **inside.micronics.local** website. User "proxy1" with a password of "proxy1", a member of CTP group on ACS, must be able to use the following services after successful authentication:

| Protocol | DST IP | DST Port |
|---|---|---|
| TCP | 172.31.1.200 | 80 |
| ICMP | ANY | - |

You must allow the following traffic to pass without authentication:

| Protocol | DST IP | DST Ports |
|---|---|---|
| TCP | 10.1.10.1 | 22-23 |
| UDP | 10.1.10.1 | 123 |
| TCP | 172.31.1.100 | 49, 443 |
| UDP | 172.31.1.100 | 1645-1646, 1812-1813 |
| UDP | 172.31.1.200 | 53 |



In order to be compliant with the regulations, all users connecting through the router must see the following message:

```
You must first be authenticated to connect to the network!
Please provide username and password!

Have a nice day!
```

You must use ACS server to authenticate, authorize and log user's (dis)connect time using TACACS+ protocol.

## Configuration

Complete these steps:

**Step 1** Configure R1 for TACACS+ Cut-Through Proxy (CTP). Note that some AAA commands are already on the router.

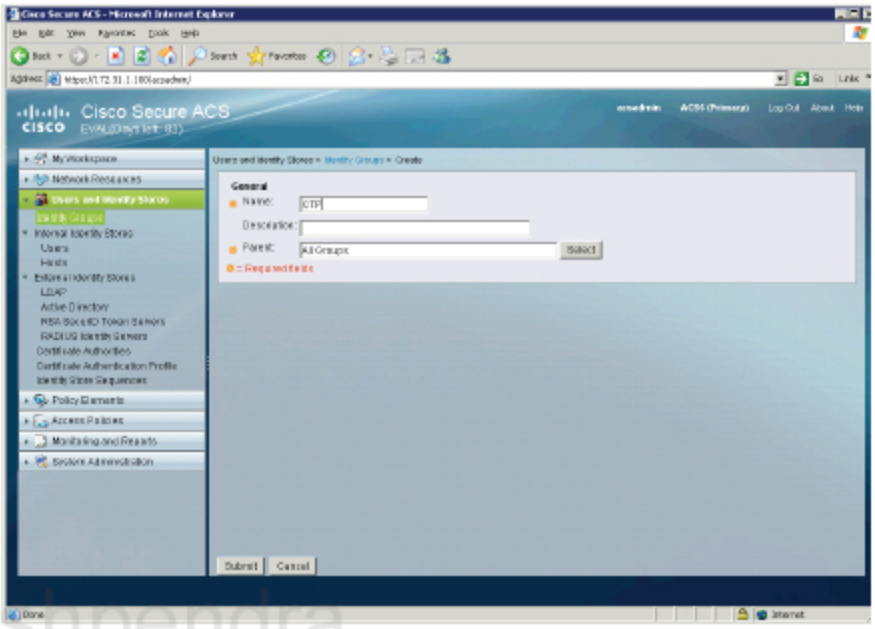
```
!
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
!
ip auth-proxy name PROXY telnet
ip auth-proxy auth-proxy-banner telnet &
Enter TEXT message.  End with the character '&'
You must first be authenticated to connect to the network!
Please provide username and password!

Have a nice day!

&
!
ip auth-proxy name PROXY http
ip auth-proxy auth-proxy-banner http &
Enter TEXT message.  End with the character '&'
You must first be authenticated to connect to the network!
Please provide username and password!

Have a nice day!

&

!
access-list 100 permit tcp any host 172.31.1.100 eq 443
access-list 100 permit udp any host 172.31.1.100 range 1645 1646
access-list 100 permit udp any host 172.31.1.100 range 1812 1813
access-list 100 permit tcp any host 172.31.1.100 eq 49
access-list 100 permit tcp any host 10.1.10.1 eq 22
access-list 100 permit tcp any host 10.1.10.1 eq 23
access-list 100 permit udp any host 10.1.10.1 eq 123
access-list 100 permit udp any host 172.31.1.200 eq 53
!
ip http server
!
int e0/0
 ip access-group 100 in
 ip auth-proxy PROXY
!
```



**Step 2** Create CTP group and proxy1 user. Connect to ACS from WinXP PC

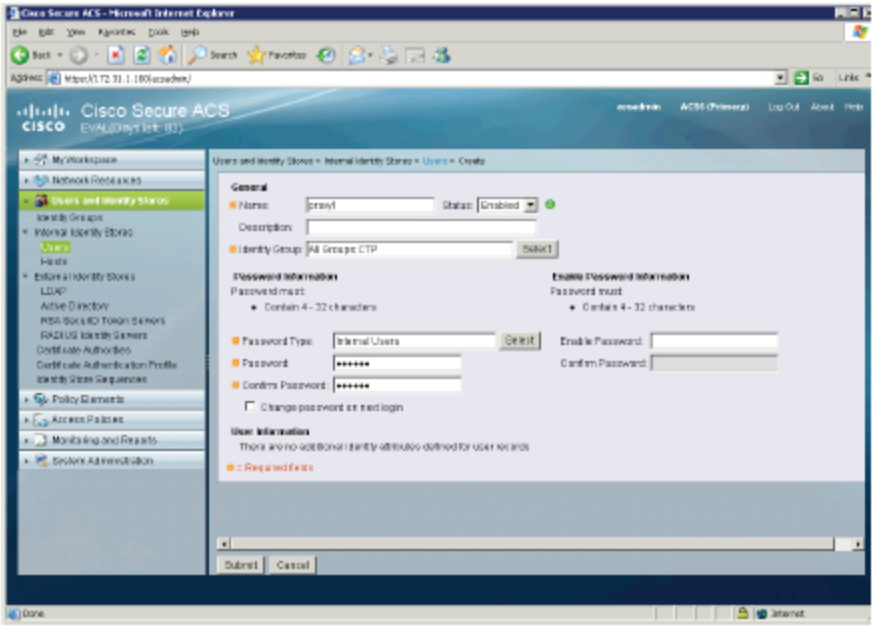
and authenticate using **acsadmin**.

- Go to **Users and Identity Stores > Identity Groups** and click **Create**. Add name **CTP** under **All Groups** and click **Submit**.



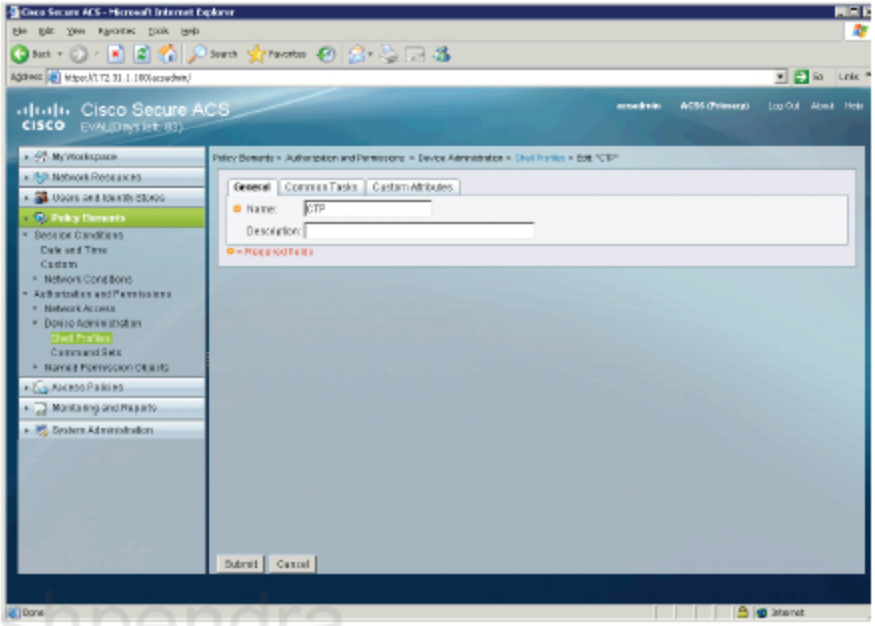



- Go to **Users and Identity Stores > Users** and click **Create**. Add new user with a name of **proxy1** and password of **proxy1**, select **CTP** under **Identity Groups** and click **Submit**.




**Step 3** Create new Shell Profile for CTP.

- Go to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** and click **Create**. On the **General** tab provide a name for the profile (e.g. CTP).

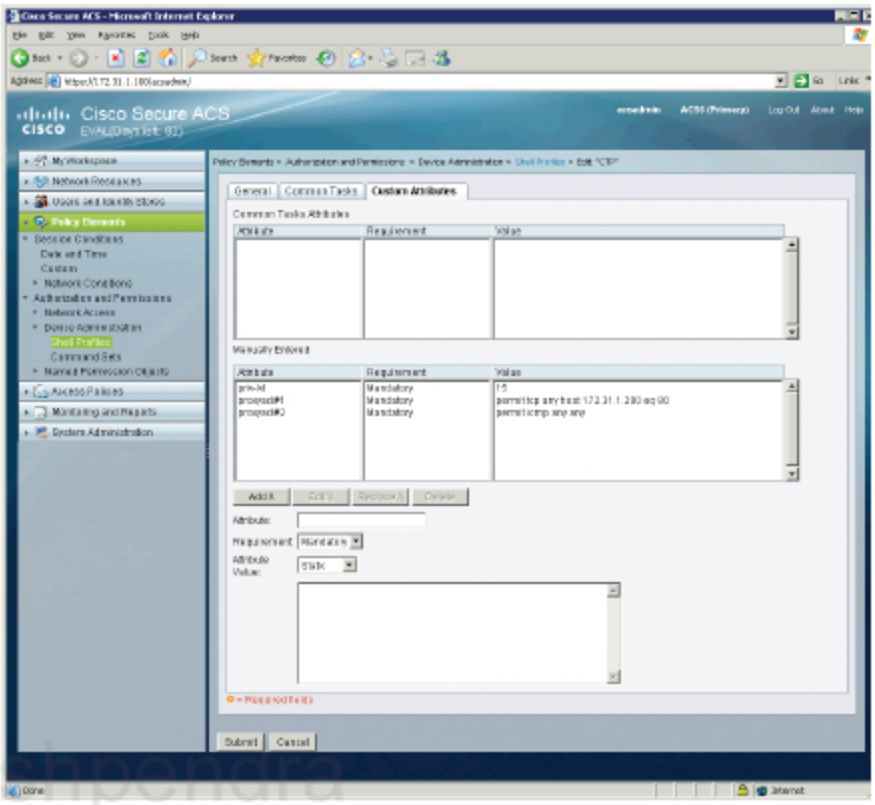





- Click on **Custom Attributes** tab and add the following attributes to the list:

| Attribute | Requirement | Value |
|---|---|---|
| **priv-lvl** | Mandatory | 15 |
| **proxyacl#1** | Mandatory | permit tcp any host 172.31.1.200 eq 80 |
| **proxyacl#2** | Mandatory | permit icmp any any |

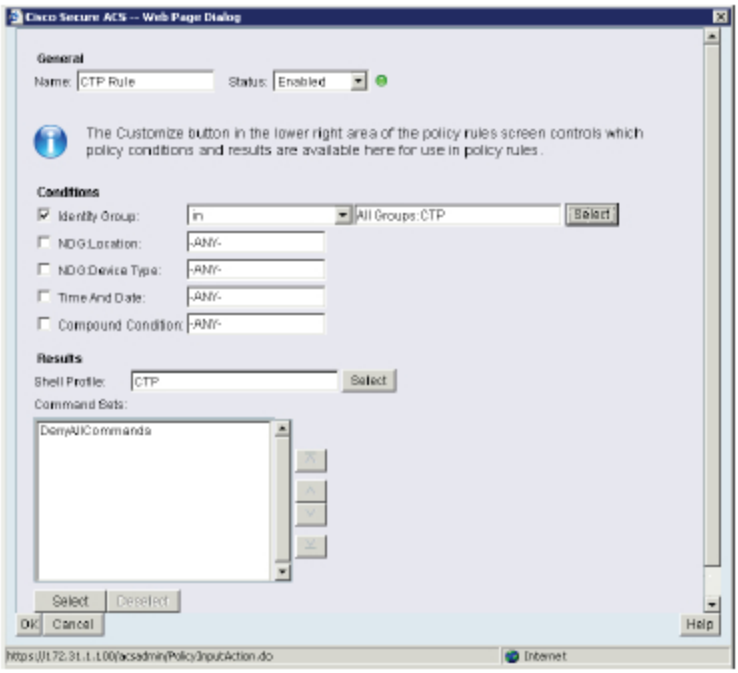
You must enter above vlues in respective fields and click on **Add^** button to add them to the list. Click on **Submit**.



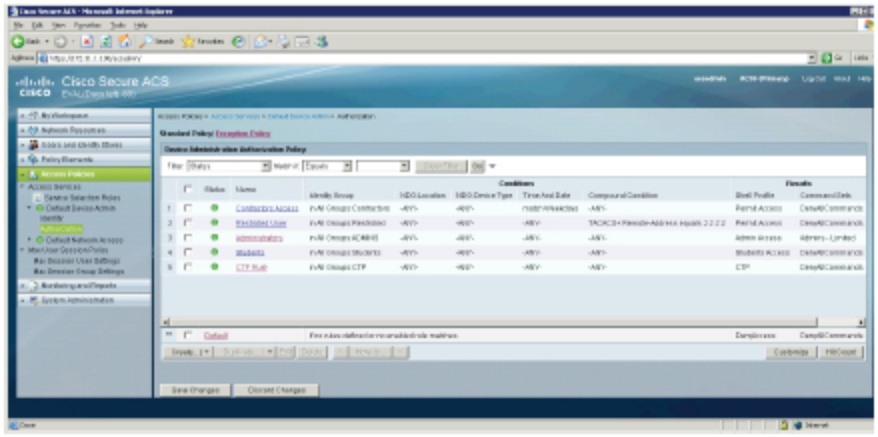



**Step 4** Create new authorization rule.

- Go to **Access Policies > Access Services > Default Device Admin > Authorization** and click **Create**. Name it **CTP Rule** and select **CTP** group for **Identity** then click **OK**.



- Click on **Save Changes** button.



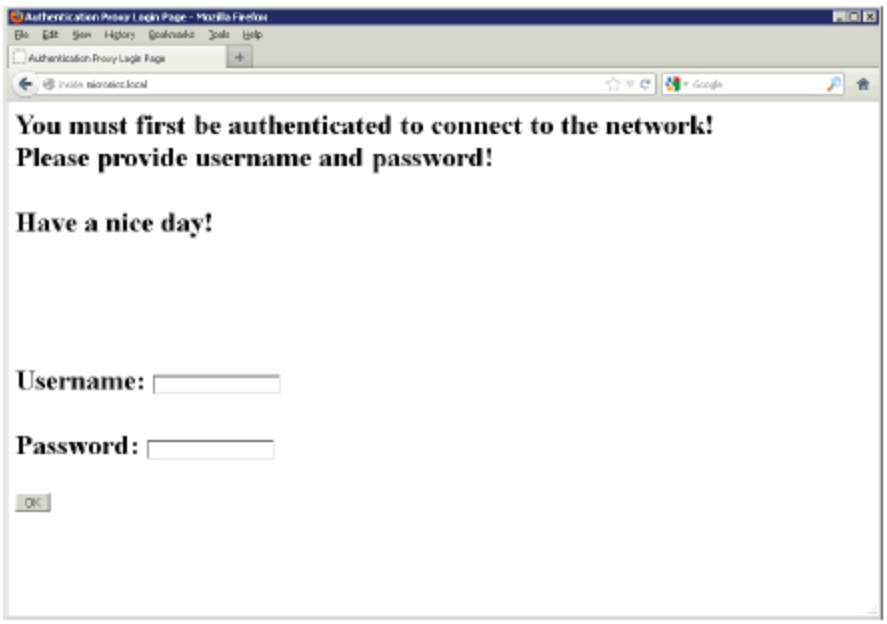

## Verification

Enable the following debugs on R1:

```
R1#deb aaa authentication
AAA Authentication debugging is on
R1#deb aaa authorization
AAA Authorization debugging is on
R1#deb tacacs packet
TACACS+ packets debugging is on
```



Open up the web browser (FF) and enter **inside.micronics.local** in the URL bar. Hit **Enter**. Router should present website for authentication:



Provide username and password and click **OK**. You should get a new window with **Successful Authentication** message.
Shortly after that you should be redirected to **inside.micronics.local** webpage.

Check R1 ACL:

```
R1#sh ip access-lists
Extended IP access list 100
```

Those two entries at the beginning of the list have been added during the authorization.

```
    permit tcp host 10.1.10.50 host 172.31.1.200 eq www (7 matches)
    permit icmp host 10.1.10.50 any
   10 permit tcp any host 172.31.1.100 eq 443 (9020 matches)
   20 permit tcp any host 10.1.10.1 eq 22
   30 permit tcp any host 10.1.10.1 eq telnet (139 matches)
   40 permit udp any host 172.31.1.200 eq domain (1075 matches)

R1#sh ip auth-proxy cache
Authentication Proxy Cache
 Client Name proxy1, Client IP 10.1.10.50, Port 2371, timeout 54, Time Remaining 54,
state ESTAB
```



Here's the debug output:

```
Nov 17 14:29:14.654: AAA/BIND(00000044): Bind i/f
Nov 17 14:29:14.654: AAA/AUTHEN/LOGIN (00000044): Pick method list 'default'
Nov 17 14:29:14.667: T+: Version 192 (0xC0), type 1, seq 1, encryption 1
Nov 17 14:29:14.667: T+: session_id 2298529072 (0x8900C530), dlen 14 (0xE)
Nov 17 14:29:14.667: T+: type:AUTHEN/START, priv_lvl:15 action:LOGIN ascii
Nov 17 14:29:14.667: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raddr_len:0 (0x0)
data_len:0
```

The first packet is TACACS Authentication. The router asks for username and password.

```
Nov 17 14:29:14.667: T+: user:  proxy1
Nov 17 14:29:14.667: T+: port:
Nov 17 14:29:14.667: T+: rem_addr:
Nov 17 14:29:14.667: T+: data:
Nov 17 14:29:14.667: T+: End Packet
Nov 17 14:29:14.676: T+: Version 192 (0xC0), type 1, seq 2, encryption 1
Nov 17 14:29:14.676: T+: session_id 2298529072 (0x8900C530), dlen 16 (0x10)
Nov 17 14:29:14.676: T+: AUTHEN/REPLY status:5 flags:0x1 msg_len:10, data_len:0
Nov 17 14:29:14.676: T+: msg:  password:
Nov 17 14:29:14.676: T+: data:
```

```
Nov 17 14:29:14.676: T+: End Packet
Nov 17 14:29:14.680: T+: Version 192 (0xC0), type 1, seq 3, encryption 1
Nov 17 14:29:14.680: T+: session_id 2298529072 (0x8900C530), dlen 11 (0xB)
Nov 17 14:29:14.680: T+: AUTHEN/CONT msg_len:6 (0x6), data_len:0 (0x0) flags:0x0
Nov 17 14:29:14.680: T+: User msg: <elided>
Nov 17 14:29:14.680: T+: User data:
Nov 17 14:29:14.680: T+: End Packet
Nov 17 14:29:14.687: T+: Version 192 (0xC0), type 1, seq 4, encryption 1
Nov 17 14:29:14.687: T+: session_id 2298529072 (0x8900C530), dlen 6 (0x6)
Nov 17 14:29:14.687: T+: AUTHEN/REPLY status:1 flags:0x0 msg_len:0, data_len:0
Nov 17 14:29:14.687: T+: msg:
Nov 17 14:29:14.687: T+: data:
Nov 17 14:29:14.687: T+: End Packet
Nov 17 14:29:14.687: AAA/AUTHOR (0x44): Pick method list 'default'
Nov 17 14:29:14.691: T+: Version 192 (0xC0), type 2, seq 1, encryption 1
Nov 17 14:29:14.691: T+: session_id 3714287399 (0xDD638727), dlen 45 (0x2D)
Nov 17 14:29:14.691: T+: AUTHOR, priv_lvl:15, authen:1 method:tacacs+
Nov 17 14:29:14.691: T+: svc:1 user_len:6 port_len:0 rem_addr_len:0 arg_cnt:2
```

The next packet is TACACS Authorization. Note that the service field specifies 'auth-proxy'. This is different than authorization to the exec where the service is 'shell'.



```
Nov 17 14:29:14.691: T+: user:  proxy1
Nov 17 14:29:14.691: T+: port:
Nov 17 14:29:14.691: T+: rem_addr:
Nov 17 14:29:14.691: T+: arg[0]: size:18 service=auth-proxy
Nov 17 14:29:14.691: T+: arg[1]: size:11 protocol=ip
Nov 17 14:29:14.691: T+: End Packet
Nov 17 14:29:14.697: T+: Version 192 (0xC0), type 2, seq 2, encryption 1
Nov 17 14:29:14.697: T+: session_id 3714287399 (0xDD638727), dlen 99 (0x63)
Nov 17 14:29:14.697: T+: AUTHOR/REPLY status:1 msg_len:0, data_len:0 arg_cnt:3
Nov 17 14:29:14.697: T+: msg:
Nov 17 14:29:14.697: T+: data:
```

Here are arguments the router got from ACS upon successful authorization.

```
Nov 17 14:29:14.697: T+: arg[0] size:11
Nov 17 14:29:14.697: T+:  priv-lvl=15
Nov 17 14:29:14.697: T+: arg[1] size:49
Nov 17 14:29:14.697: T+:  proxyacl#1=permit tcp any host 172.31.1.200 eq 80
Nov 17 14:29:14.697: T+: arg[2] size:30
Nov 17 14:29:14.697: T+:  proxyacl#2=permit icmp any any
Nov 17 14:29:14.697: T+: End Packet
Nov 17 14:29:14.701: T+: Version 192 (0xC0), type 3, seq 1, encryption 1
Nov 17 14:29:14.701: T+: session_id 2367776413 (0x8D21669D), dlen 132 (0x84)
Nov 17 14:29:14.701: T+: ACCT, flags:0x2 method:6 priv_lvl:15
Nov 17 14:29:14.701: T+: type:1 svc:1 user_len:6 port_len:0 rem_addr_len:10
Nov 17 14:29:14.701: T+: arg_cnt:5
```

This is TACACS Accounting packet.

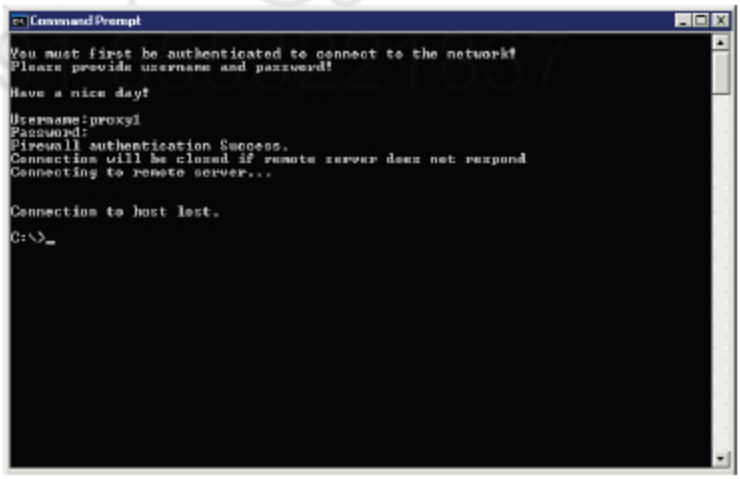
```
Nov 17 14:29:14.701: T+: user:  proxy1
Nov 17 14:29:14.701: T+: port:
Nov 17 14:29:14.701: T+: rem_addr:  10.1.10.50
Nov 17 14:29:14.701: T+: arg[0]: size:10 task_id=55
Nov 17 14:29:14.701: T+: arg[1]: size:12 timezone=GMT
Nov 17 14:29:14.701: T+: arg[2]: size:18 service=auth-proxy
Nov 17 14:29:14.701: T+: arg[3]: size:21 start_time=1353162554
Nov 17 14:29:14.701: T+: arg[4]: size:41 audit-session-id=0A010A010000000A33E725F7
Nov 17 14:29:14.701: T+: End Packet
Nov 17 14:29:14.703: T+: Version 192 (0xC0), type 3, seq 2, encryption 1
Nov 17 14:29:14.703: T+: session_id 2367776413 (0x8D21669D), dlen 5 (0x5)
Nov 17 14:29:14.703: T+: ACCT/REPLY status:1 msg_len:0 data_len:0
Nov 17 14:29:14.703: T+: msg:
R1#
Nov 17 14:29:14.703: T+: data:
Nov 17 14:29:14.703: T+: End Packet
R1#
```

## Clear Auth-Proxy cache and check CTP with TELNET.



```
R1#clear ip auth-proxy cache *
```

## TELNET to **inside.micronics.local** and authenticate.




**Note that you're not allowed to telnet to inside.micronics.local after authentication because the ACL downloaded from ACS does not contain TELNET.**

## Task 1 – RADIUS CTP (IOS)

Configure R2 so that it first authenticate and authorize users (via HTTP) behind its 0/0 interface to be able to connect to **www.micronics.com** website. Members of CTP group on ACS, must be able to use the following services after successful authentication:

| Protocol | DST IP | DST Port |
|---|---|---|
| TCP | 200.1.1.1 | 80 |
| TCP | ANY | 23 |

You must allow the following traffic to pass without authentication:

| Protocol | DST IP | DST Ports |
|---|---|---|
| IP | 2.2.2.2 | - |
| ICMP | ANY | - |
| TCP | ANY | 3389 |



In order to be compliant with the regulations, all users connecting through the router must see the following message:

```
You must first be authenticated to connect to the network!
Please provide username and password!
```

You must use ACS server to authenticate and authorize the user using Downloadable ACLs and limit Proxy-Auth login reties to 2.

*You can configure Cut-Through Proxy on IOS router with RADIUS AAA. Depending on the software version this can be done either using dACL or Cisco AVP (proxyacl) or both. Note that since you're using RADIUS for AAA, the authorization policy on the ACS must be configured under 'Default Network Access'.*

## Configuration

Complete these steps:

**Step 1** Configure R2 for RADIUS Cut-Through Proxy (CTP). Note that some AAA commands are already on the router.

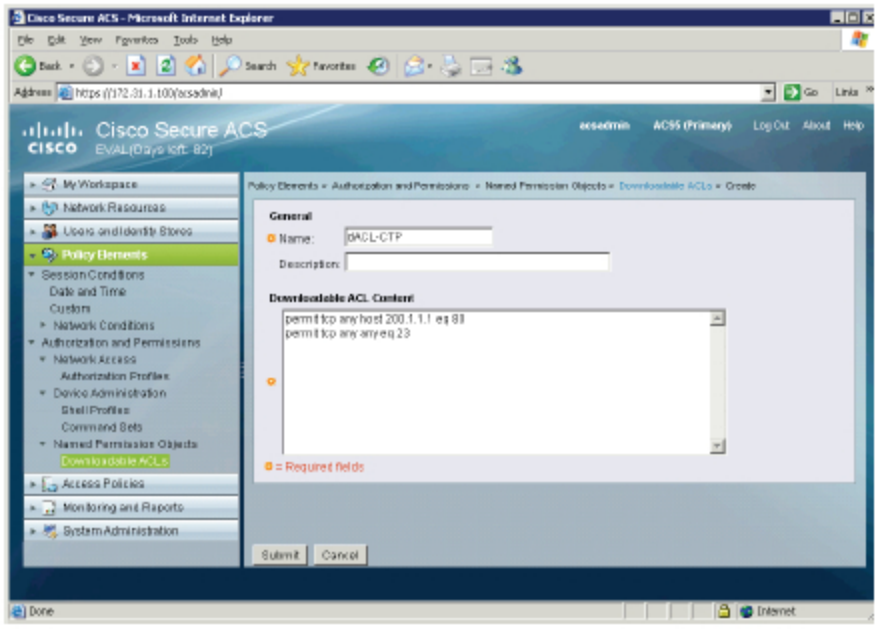
```
!
aaa new-model
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
!
ip auth-proxy auth-proxy-banner http &
You must first be authenticated to connect to the network!
Please provide username and password!
&
!
ip auth-proxy max-login-attempts 2
ip auth-proxy name PROXY http
!
interface Ethernet0/0
 ip access-group 100 in
 ip auth-proxy PROXY
!
access-list 100 permit icmp any any
access-list 100 permit tcp any any eq 3389
access-list 100 permit ip any host 2.2.2.2
!
radius-server attribute 6 on-for-login-auth
radius-server vsa send
!
```



```
Notice that you MUST enable 'authorization network' in order to allow
the router to download the dACL entries.
Also, there must be RADIUS AVP #6 and VSA (Vendor Specific Attributes)
enabled.
```

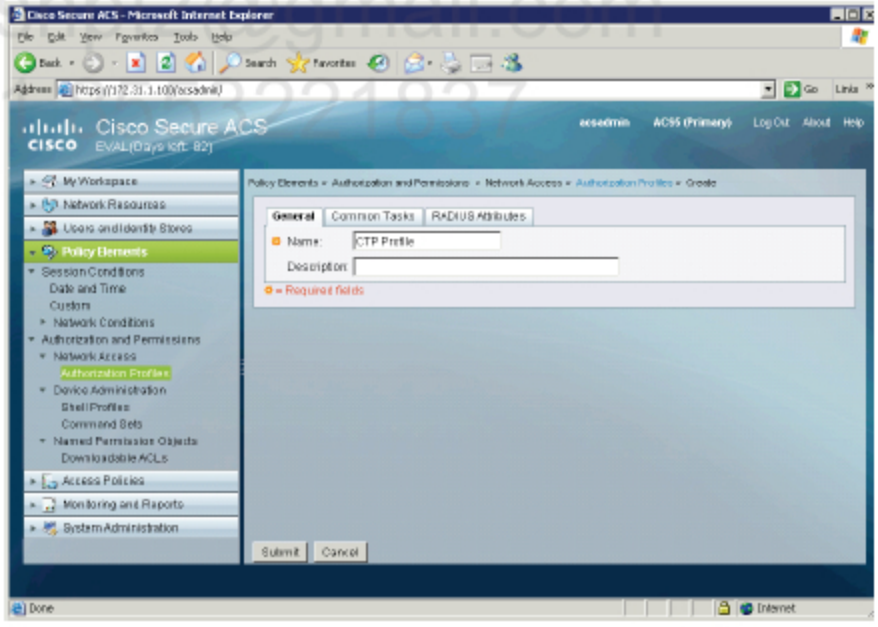
**Step 2** Create Downloadable ACL.

- Go to **Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs** and click **Create**. Enter name e.g. **dACL-CTP** and the following entries. Note that ACS does NOT check those entries.

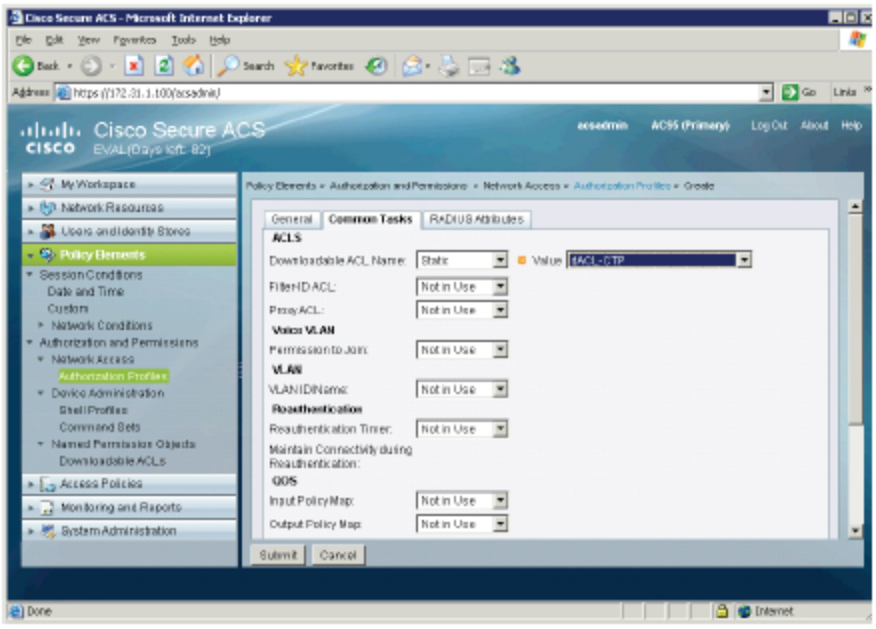



**Step 3** Create new Authorization Profile for CTP.

- Go to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** and click **Create**. On the **General** tab provide a name for the profile (e.g. CTP Profile).

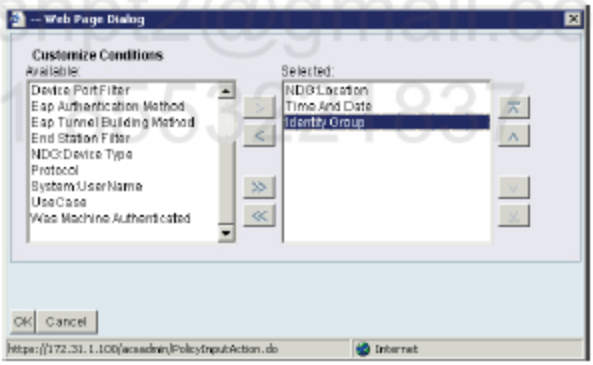



- Click on **Common Tasks** tab and select **Static** option for **Downloadable ACL Name** and pick newly created dACL from the drop-down list. Click on **Submit**.

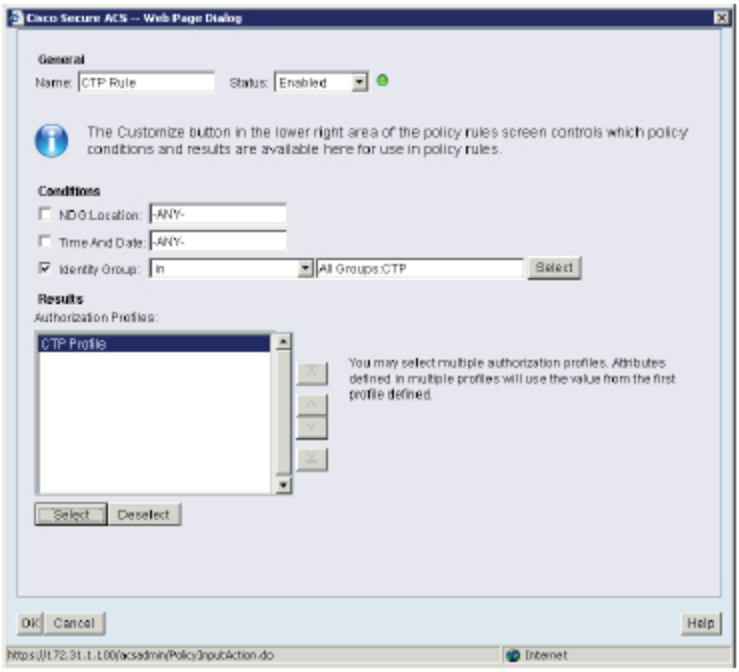



**Step 4** Create new authorization rule.

- Go to **Access Policies > Access Services > Default Network Access > Authorization** and click **Customize**. Select **Identity Group** from **Avaialable** list and move it to the right pane. Click **OK**.

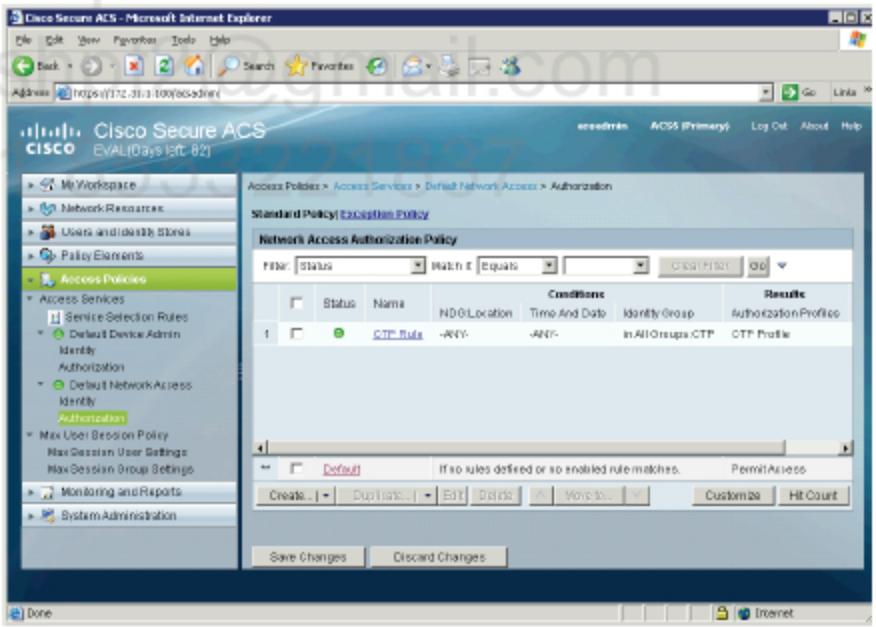



- Click on **Create** to create new authorization rule. Name it **CTP Rule** and select **CTP** group for **Identity**. Click **Select** button and chose **CTP Profile** then click **OK**.






- Click on **Save Changes** button.



## Verification

Enable the following debugs on R2:

```
R2#deb radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging debugging is off
```

First try to ping www.micronics.com to see if DNS default ACL on R2 work.

```
C:\>ping www.micronics.com

Pinging www.micronics.com [200.1.1.1] with 32 bytes of data:

Reply from 200.1.1.1: bytes=32 time=28ms TTL=127
Reply from 200.1.1.1: bytes=32 time=56ms TTL=127
Reply from 200.1.1.1: bytes=32 time=2ms TTL=127
Reply from 200.1.1.1: bytes=32 time=25ms TTL=127

Ping statistics for 200.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 56ms, Average = 27ms
```



Using web browser connect to www.micronics.com website. You should be asked for authentication.

You should get new window with **Authentication Successful!** message.


See debug output on R2

```
*Nov 18 11:34:39.825: RADIUS/ENCODE(00000024):Orig. component type = Auth Proxy
*Nov 18 11:34:39.825: RADIUS(00000024): Config NAS IP: 2.2.2.2
*Nov 18 11:34:39.825: RADIUS(00000024): Config NAS IPv6: ::
*Nov 18 11:34:39.825: RADIUS/ENCODE(00000024): acct_session_id: 19
*Nov 18 11:34:39.825: RADIUS(00000024): sending
*Nov 18 11:34:39.825: RADIUS(00000024): Sending a IPv4 Radius Packet
*Nov 18 11:34:39.825: RADIUS(00000024): Send Access-Request to
172.31.1.100:1812 id 1645/116, len 160
*Nov 18 11:34:39.825: RADIUS:  authenticator FB C9 38 A0 31 DA 68 76 - B6 CE 63
24 D7 9A 52 FD
```



```
        This is RADIUS Access-Request message with 'proxy1' user.

*Nov 18 11:34:39.825: RADIUS:  User-Name           [1]   8   "proxy1"
*Nov 18 11:34:39.825: RADIUS:  User-Password       [2]   18  *
*Nov 18 11:34:39.825: RADIUS:  Service-Type        [6]   6   Outbound
[5]
*Nov 18 11:34:39.825: RADIUS:  Vendor, Cisco       [26]  29
*Nov 18 11:34:39.825: RADIUS:   Cisco AVpair       [1]   23  "service-
type=Outbound"
*Nov 18 11:34:39.825: RADIUS:  Message-Authenticato[80]  18
*Nov 18 11:34:39.825: RADIUS:   AF B2 87 20 B8 90 39 98 FB B1 20 89 51 F3 E8 68
[  9 Qh]
*Nov 18 11:34:39.826: RADIUS:  Vendor, Cisco       [26]  49
*Nov 18 11:34:39.826: RADIUS:   Cisco AVpair       [1]   43  "audit-session-
id=640202020000000D386DB8B0"
*Nov 18 11:34:39.826: RADIUS:  NAS-Port-Type       [61]  6   Async
[0]
*Nov 18 11:34:39.826: RADIUS:  NAS-IP-Address      [4]   6   2.2.2.2
*Nov 18 11:34:39.826: RADIUS(00000024): Started 5 sec timeout
*Nov 18 11:34:39.922: RADIUS: Received from id 1645/116 172.31.1.100:1812,
Access-Accept, len 136

        This is RADIUS Access-Accept message with dACL name.
```

```
*Nov 18 11:34:39.922: RADIUS:  authenticator A3 49 ED 1C EE AC 7A 0E - 2C 2C 7B
9A 7F 18 75 11
*Nov 18 11:34:39.922: RADIUS:  User-Name           [1]   8   "proxy1"
*Nov 18 11:34:39.922: RADIUS:  Class               [25]  25
*Nov 18 11:34:39.922: RADIUS:   43 41 43 53 3A 41 43 53 35 2F 31 34 31 37 35 31
[CACS:ACS5/141751]
*Nov 18 11:34:39.922: RADIUS:   39 39 34 2F 38 34 38          [ 994/848]
*Nov 18 11:34:39.922: RADIUS:  Message-Authenticato[80]  18
*Nov 18 11:34:39.922: RADIUS:   31 2C 4D CB CF 44 9B 8E D8 DA 25 EB 16 DC 57 D2
[ 1,MD?W]
*Nov 18 11:34:39.923: RADIUS:  Vendor, Cisco       [26]  65
*Nov 18 11:34:39.923: RADIUS:   Cisco AVpair       [1]   59  "ACS:CiscoSecure-
Defined-ACL=#ACSACL#-IP-dACL-CTP-50a8c275"
*Nov 18 11:34:39.927: RADIUS(00000024): Received from id 1645/116
*Nov 18 11:34:39.927: RADIUS/ENCODE(00000000):Orig. component type = Invalid
*Nov 18 11:34:39.927: RADIUS(00000000): Config NAS IP: 2.2.2.2
*Nov 18 11:34:39.927: RADIUS(00000000): sending
*Nov 18 11:34:39.928: RADIUS(00000000): Sending a IPv4 Radius Packet
*Nov 18 11:34:39.928: RADIUS(00000000): Send Access-Request to
172.31.1.100:1812 id 1645/117, len 137
```

This is RADIUS Access-Request message with dACL as a username. This is a second step to download the ACL entries from ACS.



```
*Nov 18 11:34:39.928: RADIUS:  authenticator A3 B7 CC 96 9E 20 E3 8C - 80 E8 BF
10 5A 17 57 46
*Nov 18 11:34:39.928: RADIUS:  NAS-IP-Address      [4]   6   2.2.2.2
*Nov 18 11:34:39.928: RADIUS:  User-Name           [1]   31  "#ACSACL#-IP-dACL-
CTP-50a8c275"
*Nov 18 11:34:39.928: RADIUS:  Vendor, Cisco       [26]  32
*Nov 18 11:34:39.928: RADIUS:   Cisco AVpair       [1]   26
"aaa:service=ip_admission"
*Nov 18 11:34:39.928: RADIUS:  Vendor, Cisco       [26]  30
*Nov 18 11:34:39.928: RADIUS:   Cisco AVpair       [1]   24  "aaa:event=acl-
download"
*Nov 18 11:34:39.928: RADIUS:  Message-Authenticato[80]  18
*Nov 18 11:34:39.928: RADIUS:   F3 D5 C1 48 E1 A0 2C 7A 68 F7 D6 F4 DB B6 CB D0
[ H,zh]
*Nov 18 11:34:39.928: RADIUS(00000000): Started 5 sec timeout
*Nov 18 11:34:39.931: RADIUS: Received from id 1645/117 172.31.1.100:1812,
Access-Accept, len 191
*Nov 18 11:34:39.931: RADIUS:  authenticator 7F 30 43 1B A4 46 F6 B2 - 36 49 F5
9F 6B B6 76 85
*Nov 18 11:34:39.931: RADIUS:  User-Name           [1]   31  "#ACSACL#-IP-dACL-
CTP-50a8c275"
*Nov 18 11:34:39.931: RADIUS:  Class               [25]  25
*Nov 18 11:34:39.931: RADIUS:   43 41 43 53 3A 41 43 53 35 2F 31 34 31 37 35 31
[CACS:ACS5/141751]
*Nov 18 11:34:39.931: RADIUS:   39 39 34 2F 38 34 39          [ 994/849]
*Nov 18 11:34:39.931: RADIUS:  Message-Authenticato[80]  18
```

```
*Nov 18 11:34:39.931: RADIUS:    B9 16 11 33 DF 7E 70 45 0D DD B6 7F 20 D6 DD CA
[ 3~pE ]
*Nov 18 11:34:39.931: RADIUS:  Vendor, Cisco       [26]  54
```

Those are ACL entries in RADIUS Access-Accept message.

```
*Nov 18 11:34:39.931: RADIUS:    Cisco AVpair      [1]   48  "ip:inacl#1=permit
tcp any host 200.1.1.1 eq 80"
*Nov 18 11:34:39.931: RADIUS:  Vendor, Cisco       [26]  43
*Nov 18 11:34:39.931: RADIUS:    Cisco AVpair      [1]   37  "ip:inacl#2=permit
tcp any any eq 23"
R2#
*Nov 18 11:34:39.936: RADIUS(00000000): Received from id 1645/117
R2#
```

## A bunch of useful commands R2

```
// to see who has authenticated
R2#sh ip auth-proxy cache
Authentication Proxy Cache
 Client Name proxy1, Client IP 100.2.2.10, Port 16717, timeout 52, Time
Remaining 52, state ESTAB
```



```
// to see authentication sessions per interface
R2#sh epm session summary
EPM Session Information
-----------------------
Total sessions seen so far : 10
Total active sessions      : 1

 Interface               IP Address        MAC Address       Audit Session Id:
 ------------------------------------------------------------------------------
Ethernet0/0             100.2.2.10        0000.0000.0000    64020202000000D386DB8B0

// to see per-user dACL on the router (can't see where ACL is applied though)
R2#sh ip access-lists
Extended IP access list 100
    10 permit icmp any any (8 matches)
    20 permit ip any host 2.2.2.2 (14 matches)
    30 permit tcp any any eq 8888
Extended IP access list xACSACLx-IP-dACL-CTP-50a8c275 (per-user)
    10 permit tcp any host 200.1.1.1 eq www
    20 permit tcp any any eq telnet


// to see dACL applied to the interface
R2#sh ip access-lists interface e0/0
Extended IP access list 100 in
    10 permit icmp any any (8 matches)
    20 permit ip any host 2.2.2.2 (14 matches)
    30 permit tcp any any eq 8888
     permit tcp host 100.2.2.10 host 200.1.1.1 eq www (10 matches)
     permit tcp host 100.2.2.10 any eq telnet
```

# LAB 2.35. Authentication Proxy on ASA

## Objectives

This lab shows how to configure ASA to perform Cut-Through Proxy.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| ASA | 0/1 (inside) | 10.1.10.10/24 |
| | 0/0 (outside) | 100.2.2.10/24 |
| ACS | NIC | 172.31.1.100 |
| WinXP | NIC | 10.1.10.50 |

## Task 1 – RADIUS CTP

Configure ASA1 to authenticate users on the Inside network (10.1.10.0) who want to connect through the firewall to outside hosts using port 3389. The users from group CTP on the ACS must use HTTP website of **http://<asa-inside>:8888/netaccess/connstatus.html** to authenticate. Make sure the user's session can last for up to 2 hours and be disconnected after 15 minutes of inactivity.

Use 'cisco123' as RADIUS secret key and assign the ASA to Firewall NDG (Network Device Group).

### Configuration

Complete these steps:

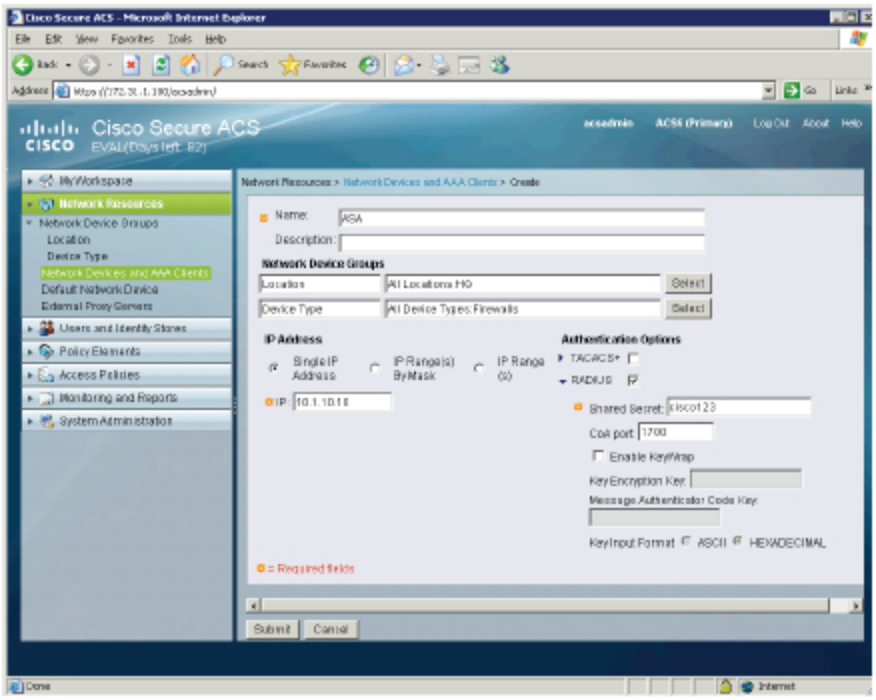
**Step 1** Configure ASA for RADIUS AAA.



```
!
aaa-server ACS protocol radius
aaa-server ACS (inside) host 172.31.1.100 cisco123
!
access-list CTP extended permit tcp 10.1.10.0 255.255.255.0 any eq
3389
access-list CTP extended permit tcp 10.1.10.0 255.255.255.0 host
10.1.10.10 eq 8888
!
aaa authentication match CTP inside ACS
aaa authentication listener http inside port 8888 redirect
!
timeout uauth 2:00:00
timeout uauth 0:15:00 inactivity
!
```

**Step 2** Add ASA to the ACS AAA client list.

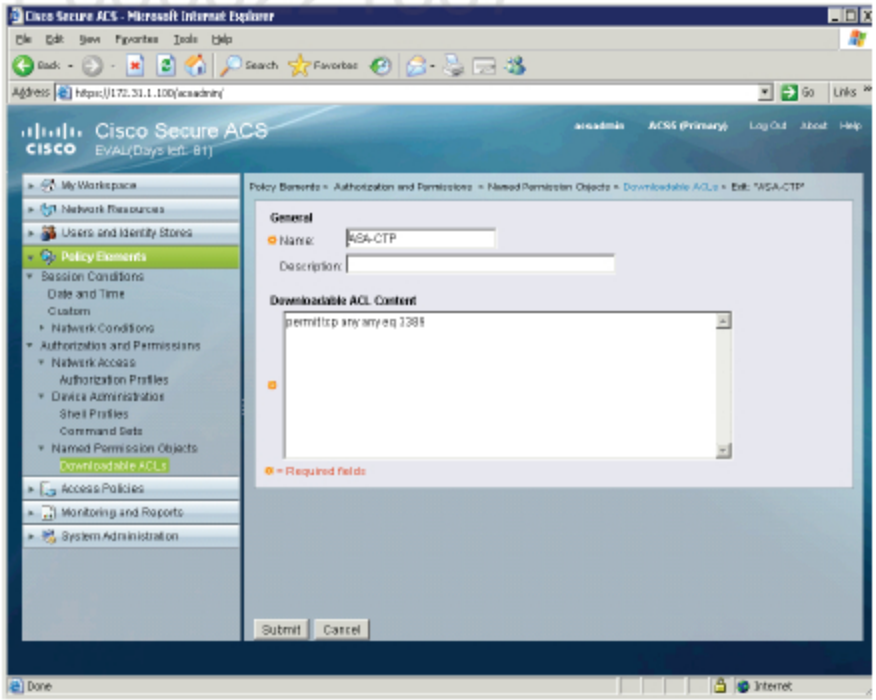
- Go to **Network Resources > Network Device and AAA Clients** and click **Create**. Add new client with name of **ASA**, select Location = **HQ** and Device Type = **Firewalls** (create it if there is no such NDG), configure IP address of **10.1.10.10**, select RADIUS as a protocol and configure **Shared Secret** of **cisco123** and click **Submit**.





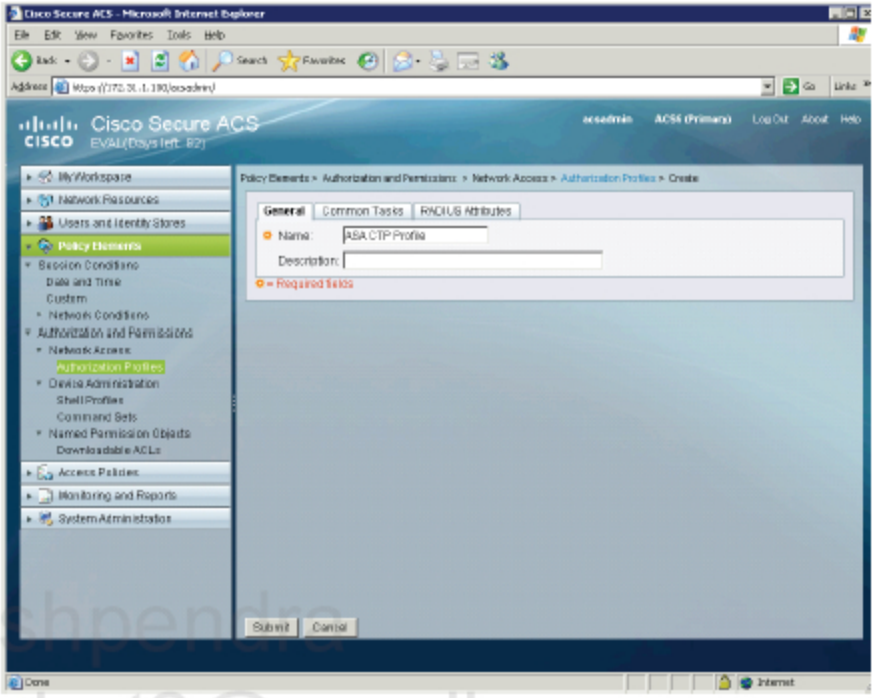

**Step 3** Create Downloadable ACL.

- Go to **Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs** and click **Create**. Enter name e.g. **ASA-CTP** and add the following entries:



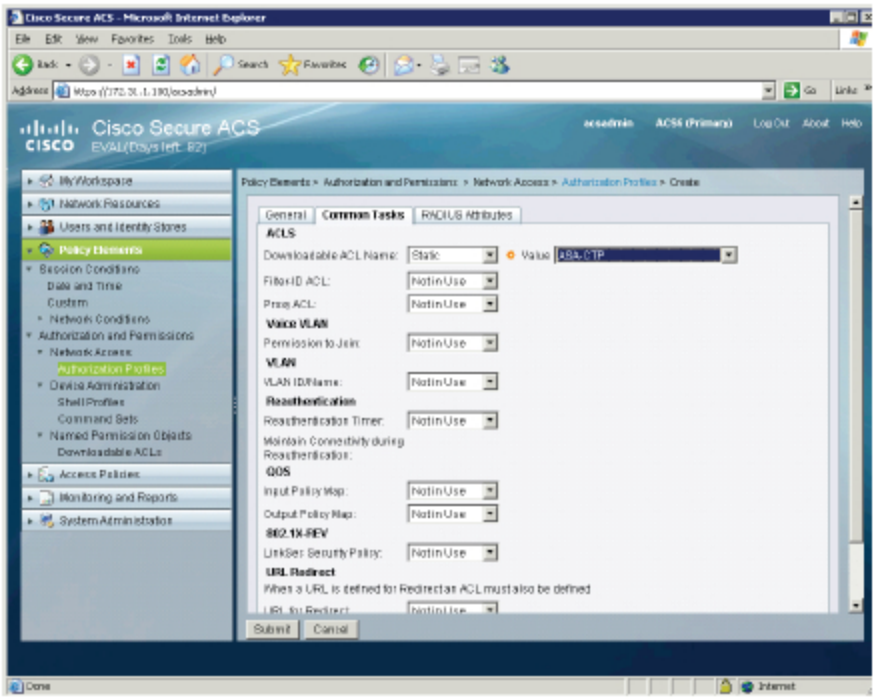

**Step 5** Create new Authorization Profile for CTP.

- Go to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** and click **Create**. On the **General** tab provide a name for the profile (e.g. ASA CTP Profile).



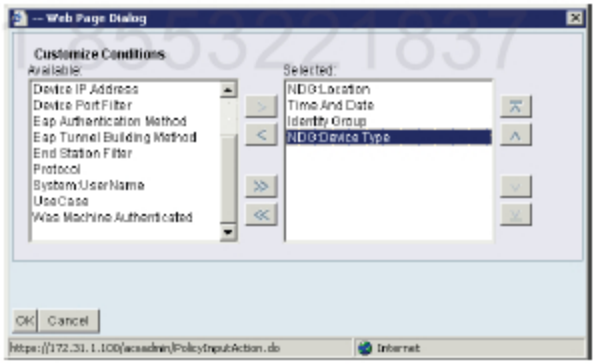



- Click on **Common Tasks** tab and select **Static** option for **Downloadable ACL Name** and pick newly created dACL from the drop-down list. Click on **Submit**.

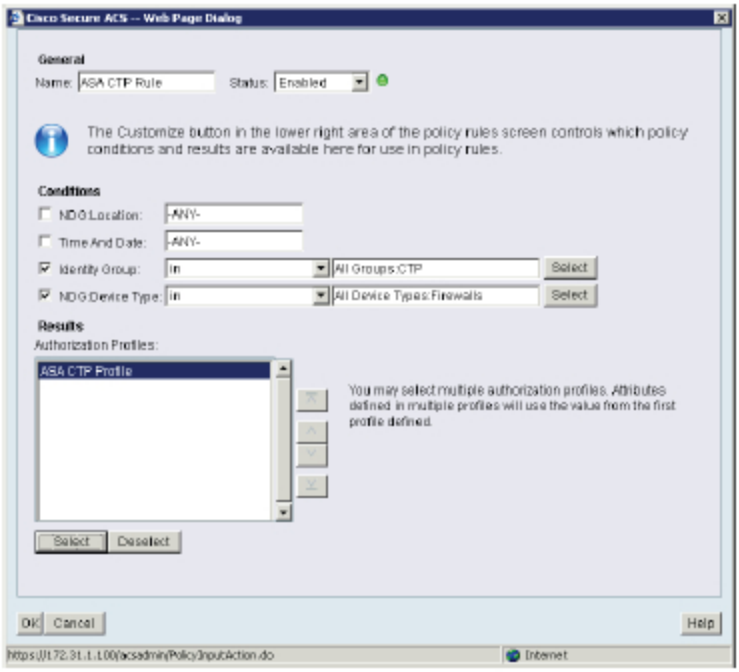



**Step 6** Create new authorization rule.

- Go to **Access Policies > Access Services > Default Network Access > Authorization** and click **Customize**. Select **NDG:Device Type** from **Avaialable** list and move it to the right pane. Click **OK**.

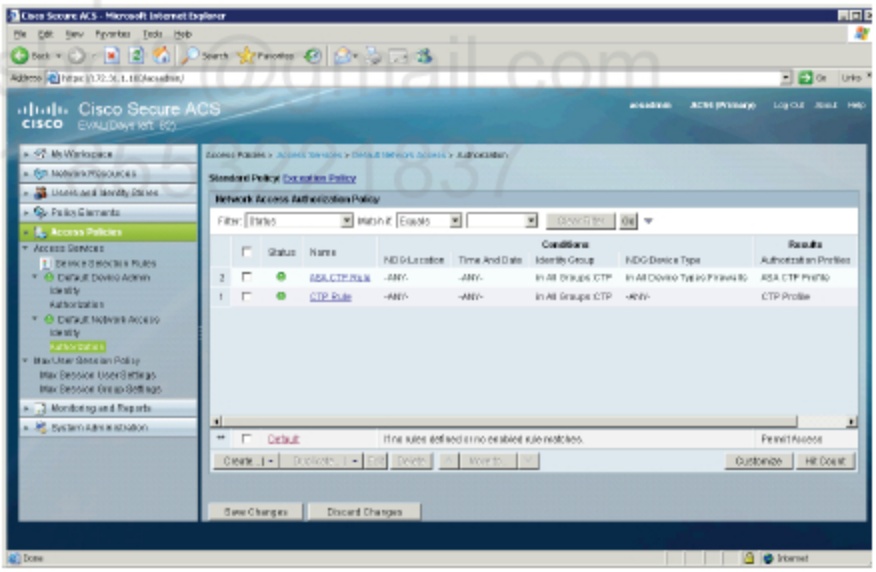



- Check **CTP Rule** on the authorization rules list and click on arrow next to the **Create** button and chose **Create** Above option to create new rule. Name it **ASA CTP Rule**, select **CTP** group for **Identity** and **All Device Types:Firewalls** for NDG:Device Type. Click **Select** button and chose **ASA CTP Profile** then click **OK**.






- Click on **Save Changes** button.

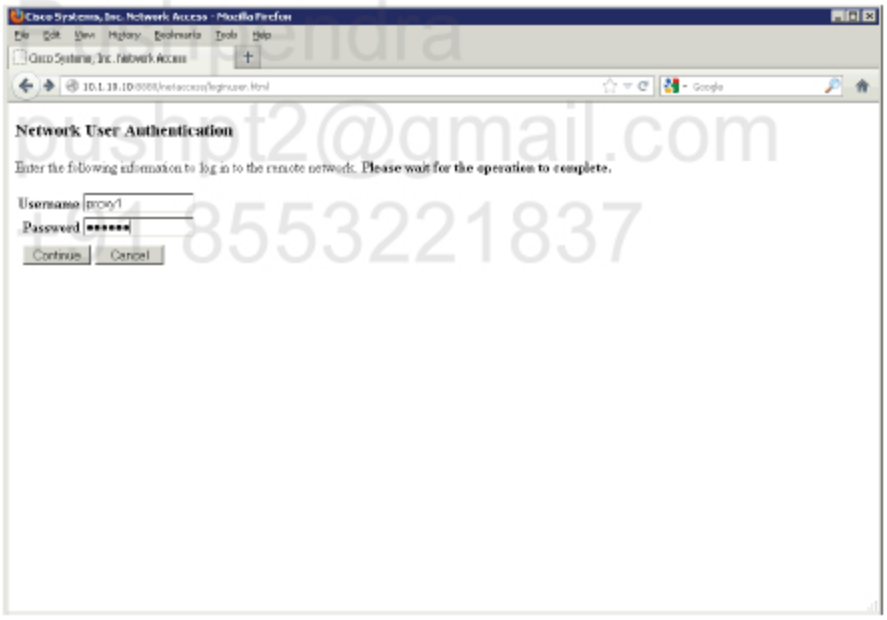


## Verification

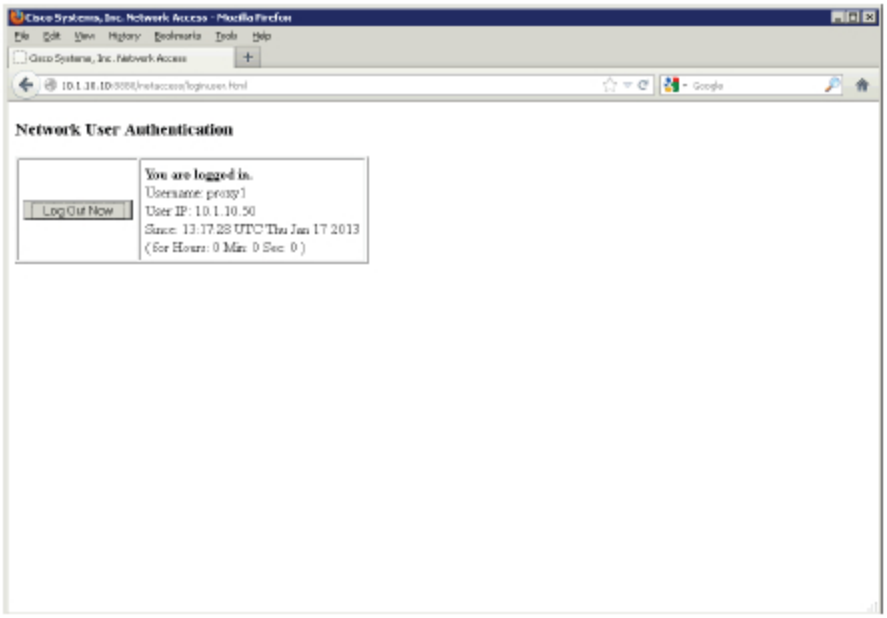
Using Windows CMD start TELNET session to www.micronics.com on port 3389. The session should fail.

```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> open www.micronics.com 3389
Connecting To www.micronics.com...

Error:  Must authenticate before using this service.

Connection to host lost.
Press any key to continue...
```

Open up the web browser and go to http://10.1.10.10:8888/netaccess/loginuser.html. Provide username and password for authentication and click Continue button.




You should get the following information after successful authentication.



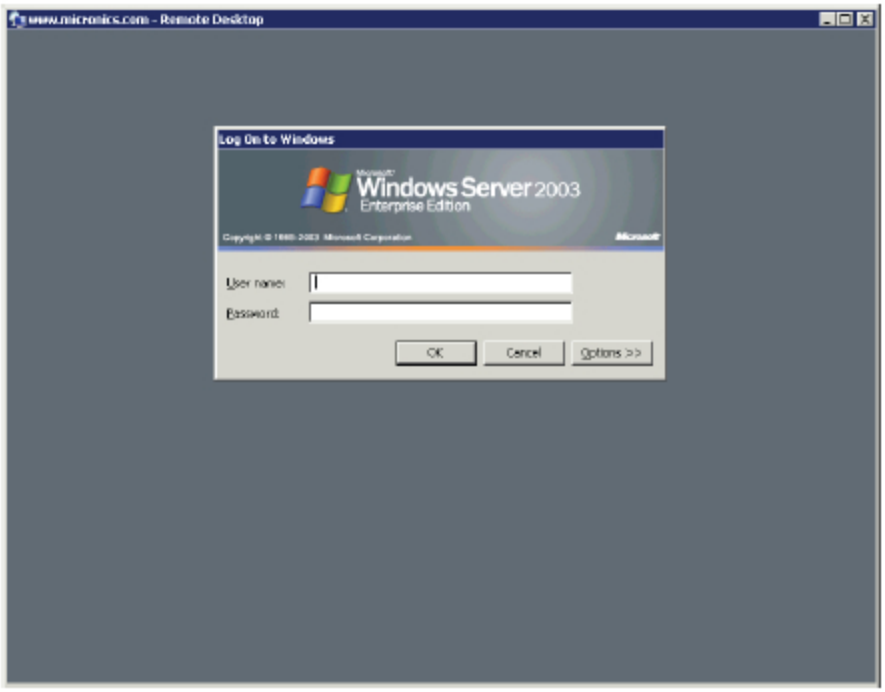

## Verify commands on the ASA

```
ASA1(config)# sh uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          2
user 'proxy1' at 10.1.10.50, authenticated
   access-list #ACSACL#-IP-ASA-CTP-50aa0baf (*)
   absolute   timeout: 2:00:00
   inactivity timeout: 0:15:00
```

Note the username and DACL name. Also timeout values are important.
Check the ACL. It is applied 'per user'.

```
ASA1(config)# sh access-list #ACSACL#-IP-ASA-CTP-50aa0baf
access-list #ACSACL#-IP-ASA-CTP-50aa0baf; 1 elements; name hash: 0x7fda124f (dynamic)
access-list #ACSACL#-IP-ASA-CTP-50aa0baf line 1 extended permit tcp any any eq 3389
(hitcnt=0) 0x30224544
```

Try to TELNET to www.micronics.com port 3389. It should now be successful. Alternatively you can try to use RDP client for that connection.



# LAB 2.36. ACS External Identity Store

## Objectives

This lab shows how to configure ACS to perform use External Identity Stores and enable Identity Seqences.

## IP Addressing and devices

| Device | Interface | IP address |
|---|---|---|
| R1 | Lo0 | 1.1.1.1/32 |
| | E0/0 | 10.1.10.1/24 |
| | E0/1 | 172.31.1.1/24 |
| R2 | Lo0 | 2.2.2.2/32 |
| | E0/0 | 100.2.2.2/24 |
| ASA | 0/1 (inside) | 10.1.10.10/24 |
| | 0/0 (outside) | 100.2.2.10/24 |
| ACS | NIC | 172.31.1.100 |
| WinXP | NIC | 10.1.10.50 |

# Task 1 – AD Integration

Configure ACS to join Active Directory domain of **micronics.local**. Use AD user credentials of employee1/Micronics1 to join the domain. Import the following groups from AD to the ACS:

- micronics.local/Users/contractors
- micronics.local/Users/employees
- micronics.local/Users/students

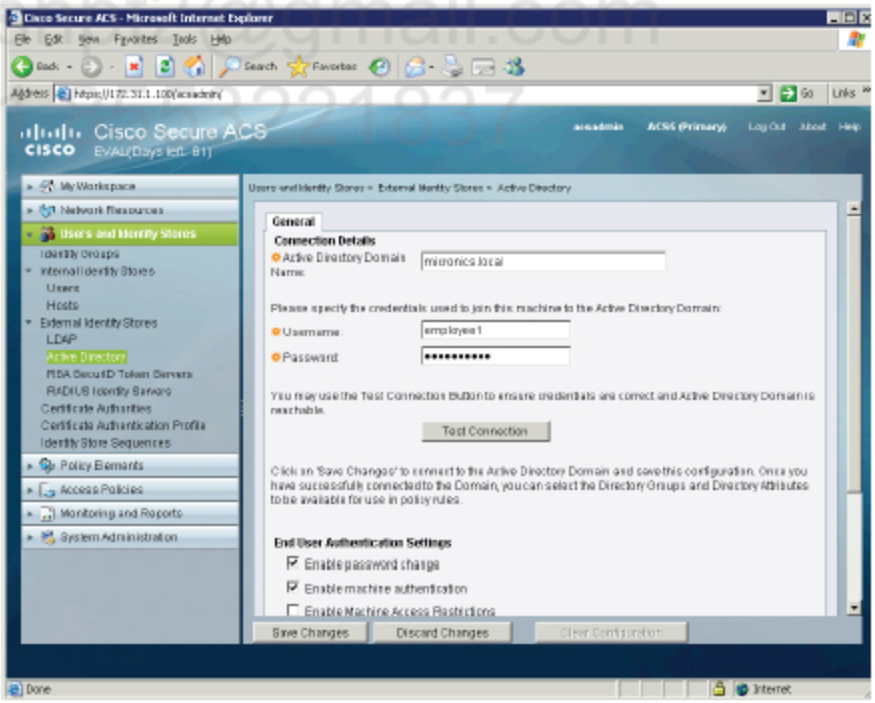
## Configuration

Complete these steps:

**Step 1** Join the Active Directory domain.

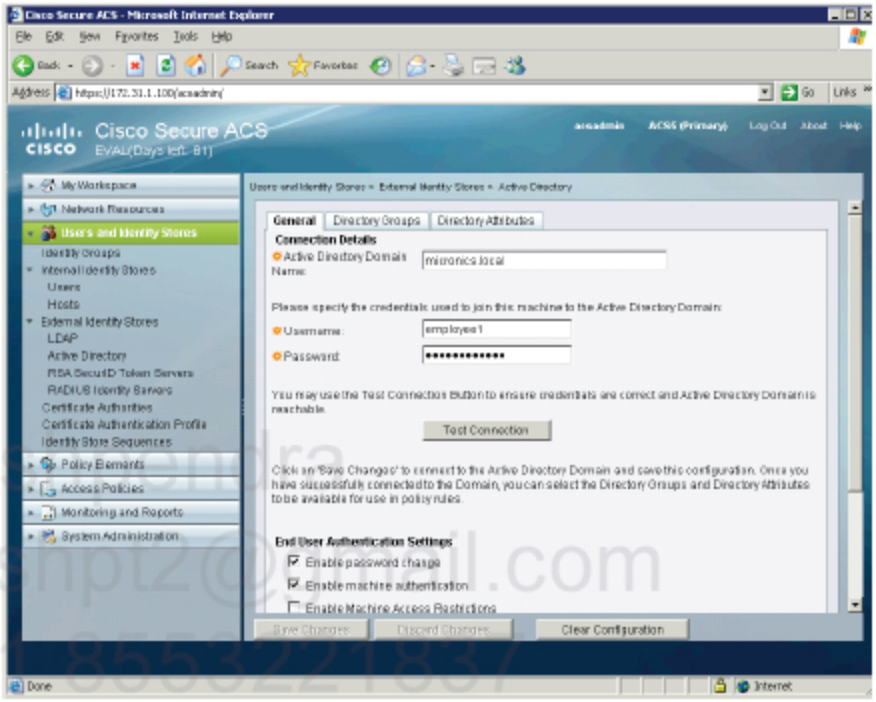
- Go to **Users and Identity Stores > External Identity Stores > Active Directory** and provide **micronics.local** as Active Directory Domain Name. Provide user credentials and click **Test Connection**.





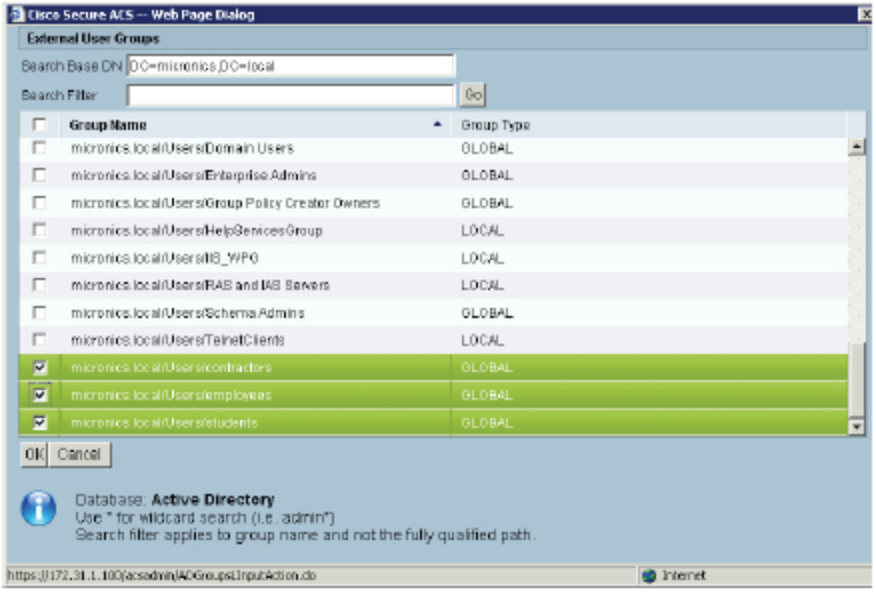

- You should get the following message when connection is successful.


- Click on **Save Changes** to join the domain.

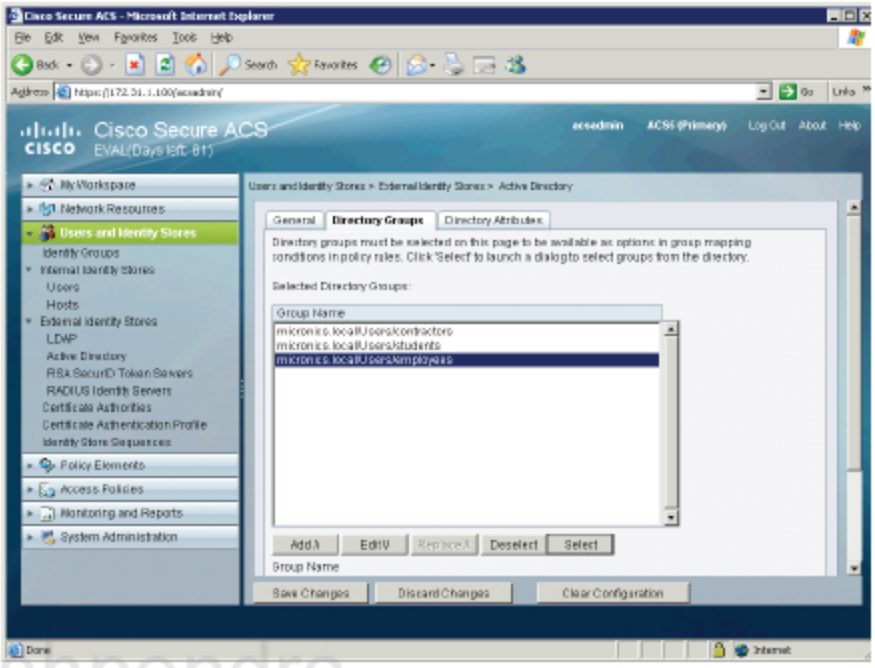



**Step 2** Import AD groups into ACS.

- Go to **Directory Groups** tab and click **Select**. All groups from AD should be displayed. Select those three to import them and click **OK**.



- Click **Save Changes**.






## Verification

There is no verification for that task.

## Task 2 – Identity Seqences

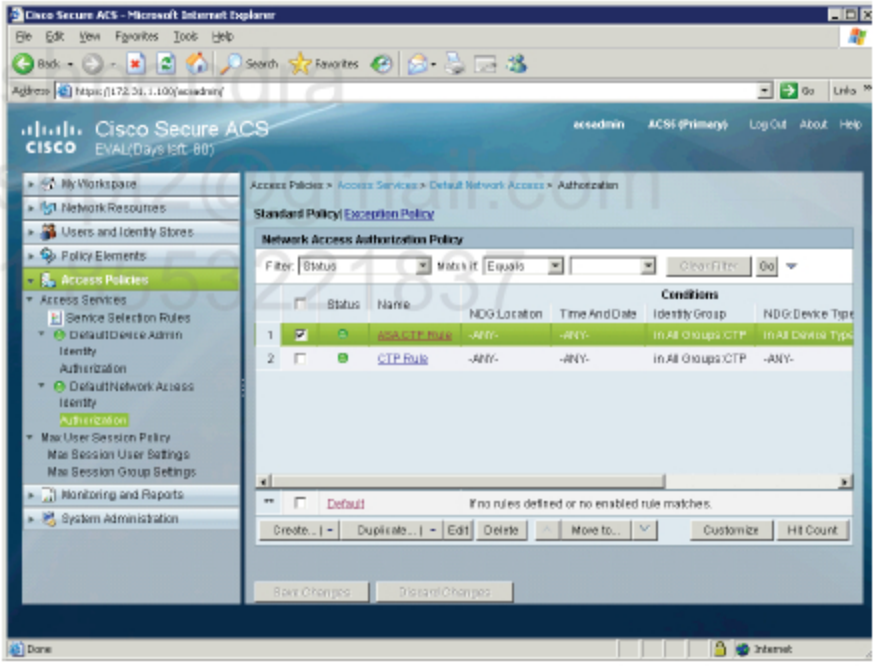
The ASA is currently configured to authenticate users before allowing connection to port 3389. Reconfigure ACS so that it first considers users from Active Directory **employees** group and then ACS Internal Users Store. This must be done only for ASA Cut-Through Proxy using new service on the ACS. You may alter previous ACS configuration.

## Configuration

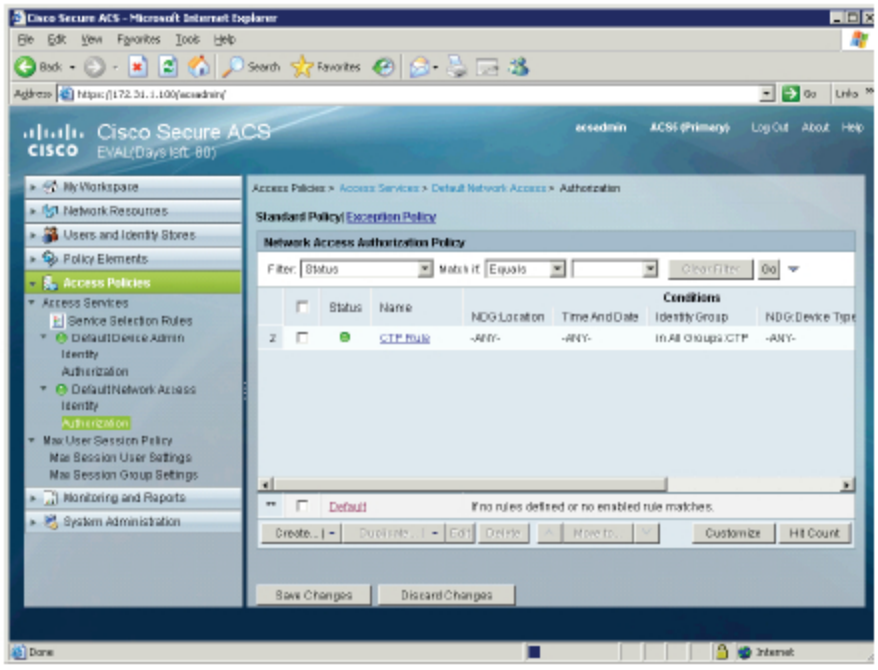
Complete these steps:

**Step 1** Delete previous **ASA CTP Rule** from authorization rules.

- Go to **Access Policies > Access Services > Default Network Access > Authorization**, check **ASA CTP Rule** on the listand click Delete.



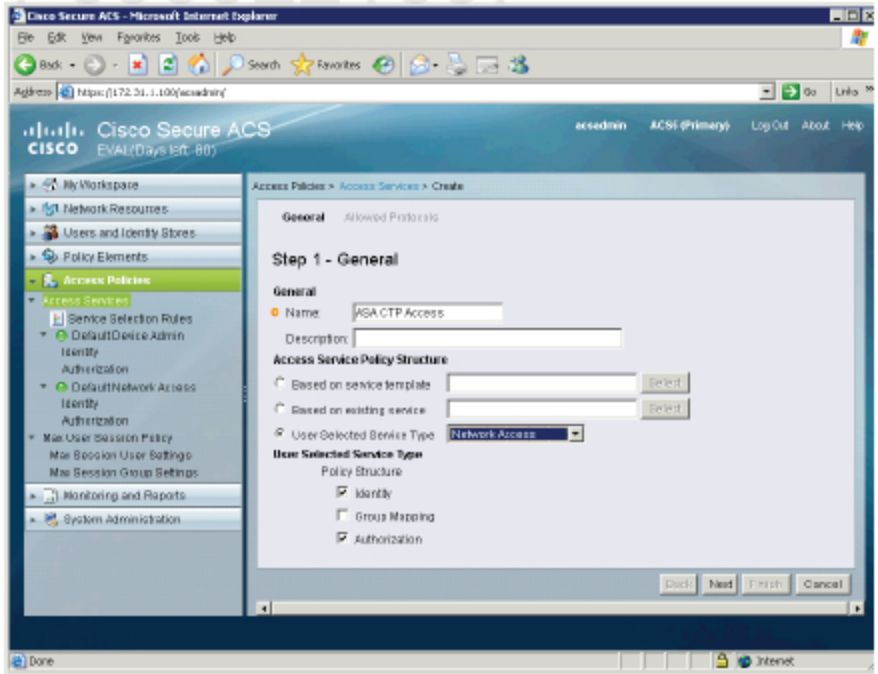

- Click on **Save Changes**.




**Step 2** Create new **Access Service.**

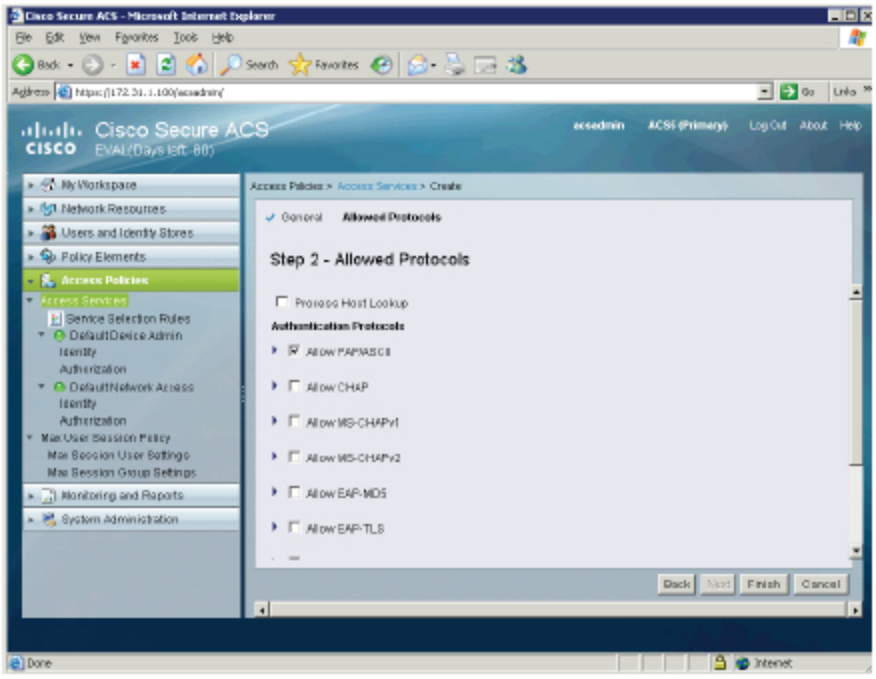
- Go to **Access Policies > Access Services** and click **Create**. Enter a name for new service e.g. **ASA CTP** Access, select **User Selected Service** Type and chose **Network** Access from the drop-down list and click **Next**.





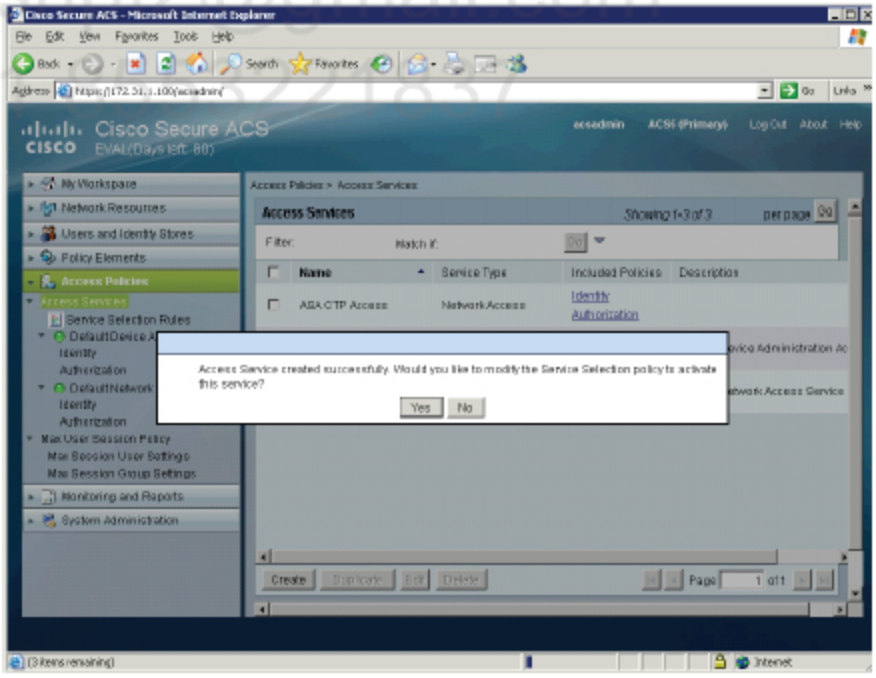

- On **Step 2 – Allowed Protocols** select **Allow PAP/ASCII** and

uncheck **Process Host Lookup**. Click **Finish**.

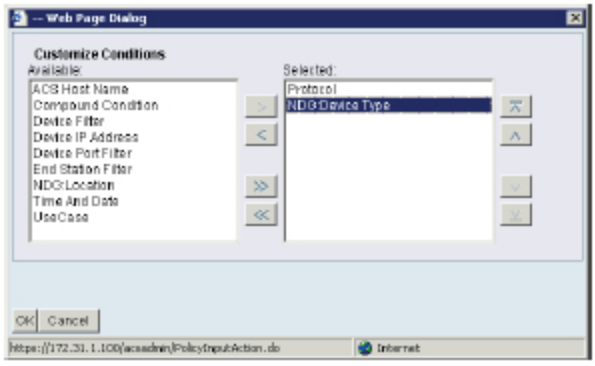




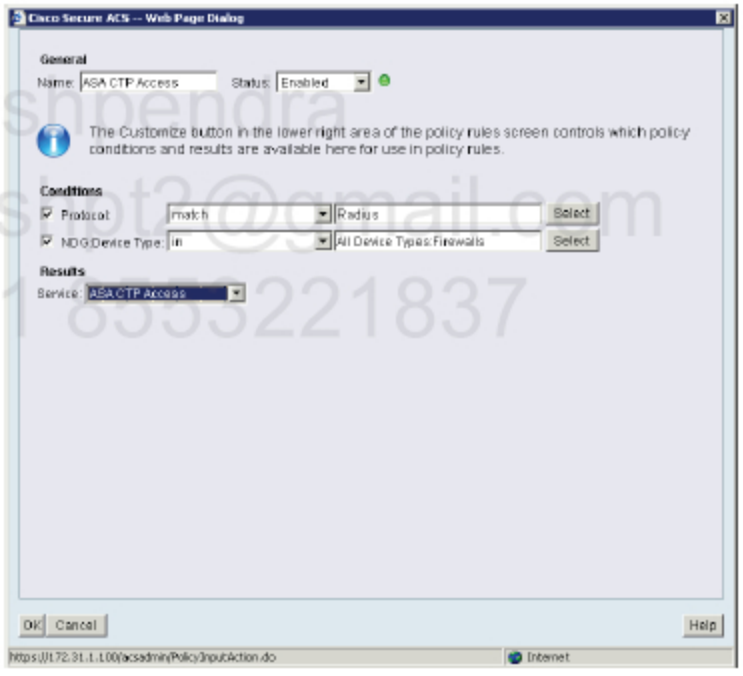

- Answer **Yes** to the following question. You should be transferred to **Service Selection Rules** configuration.




- On **Service Selection Rules** click **Customize** and move **NDG:Device Type** to the right pane. Click **OK**.

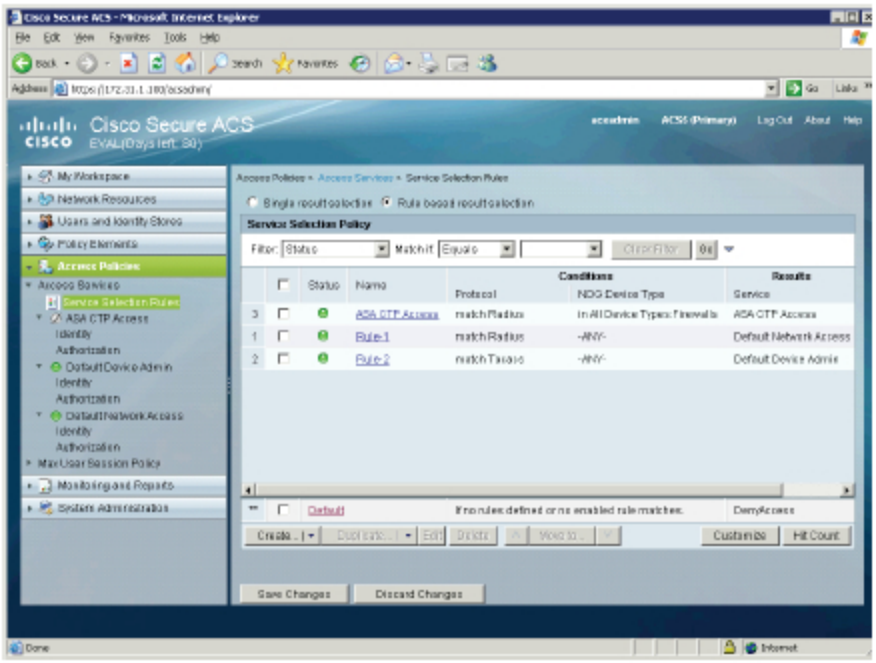



On **Service Selection Rules** pick **Rule-1** on the list, click an arrow next to the **Create** button and chose **Create Above**. Enter a name for new policy rule e.g. **ASA CTP Access**, select **Radius** for **Protocol**, select **All Devices Types: Firewalls** for **NDG:Device Type,** select **ASA CTP Access** for **Service** and click **OK**.



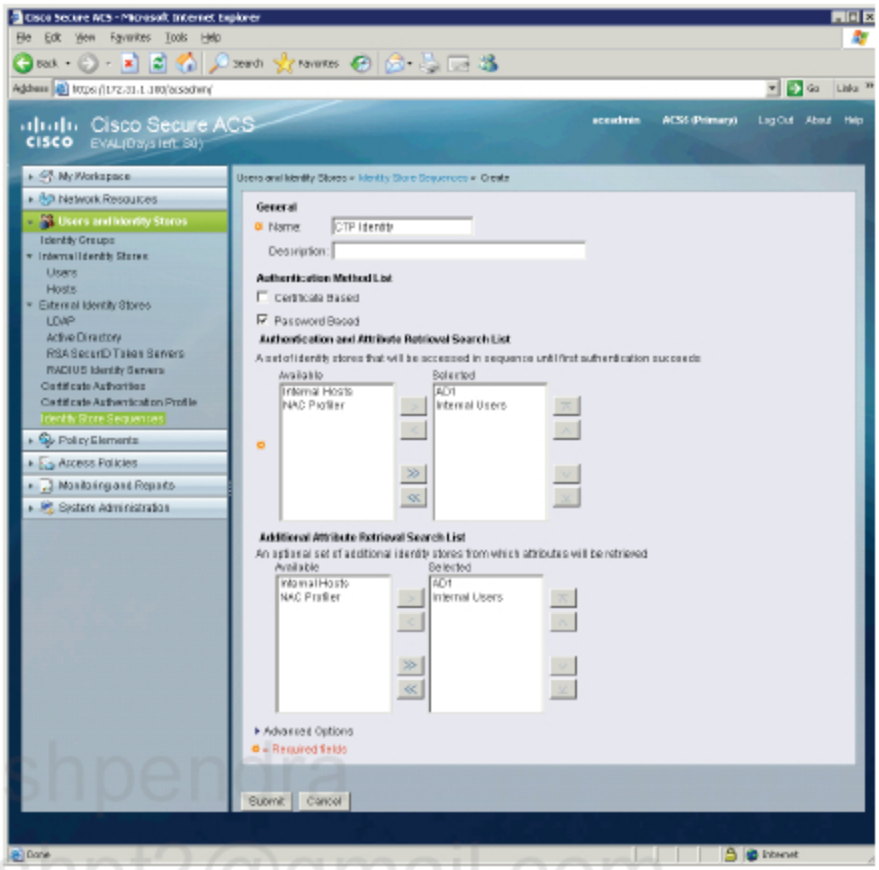



Click on **Default** rule and change its **Results** to **DenyAccess**. Click **Save Changes**.




**Step 3** Create new Identity Sequence.

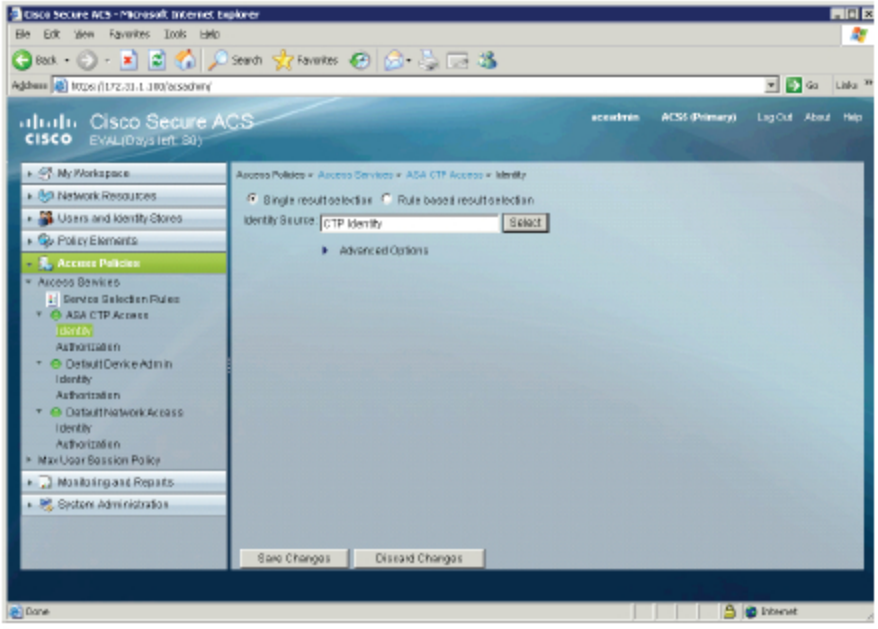
- Go to **Users and Identity Stores > identity Store Sequences** and click **Create**. Enter a name e.g **CTP Identity**, pick **Password Based** checkbox and move **AD1** and **Internal Users** to the right pane on both lists. The **AD1** must appear first on the list.






**Step 4** Change the identity for **ASA CTP Access** service.

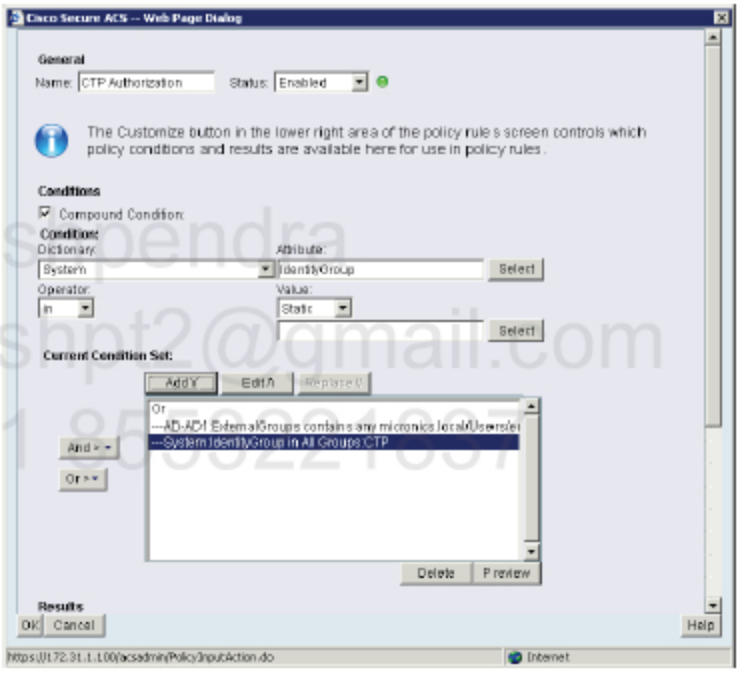
- Go to **Access Policies > ASA CTP Access > Identity** and change default **Identity Source** to **CTP Identity** (identity sequence). Click on **Save Changes**.



**Step 5** Add new authorization rule for **ASA CTP Access** service.

- Go to **Access Policies > Acess Services > ASA CTP Access > Authorization** and click **Create**. Enter a name for a new rule e.g. **CTP Authorization** and create new **Compound Condition** built upon two rules (with OR in between):

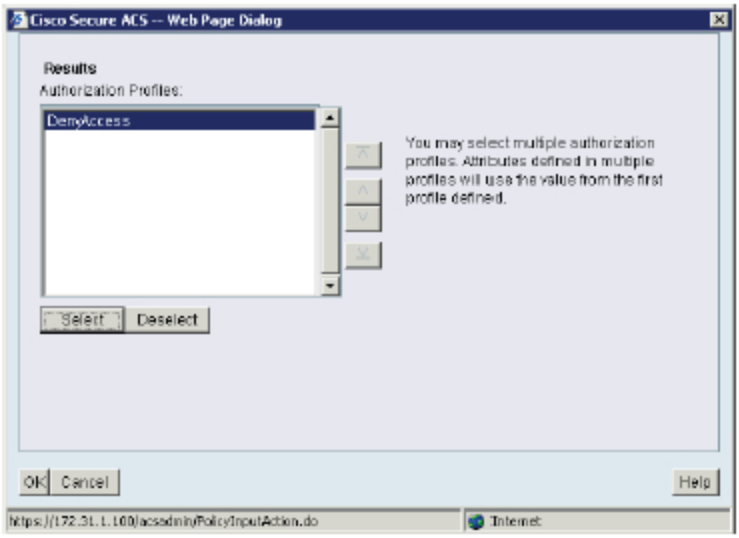
| Dictionary | Attribute | Operator | Value |
|---|---|---|---|
| **AD-AD1** | **ExternalGroups** | **contains any** | **Micronics.local/Users/employees** |
| **System** | **IdentityGroup** | **in** | **All Groups:CTP** |



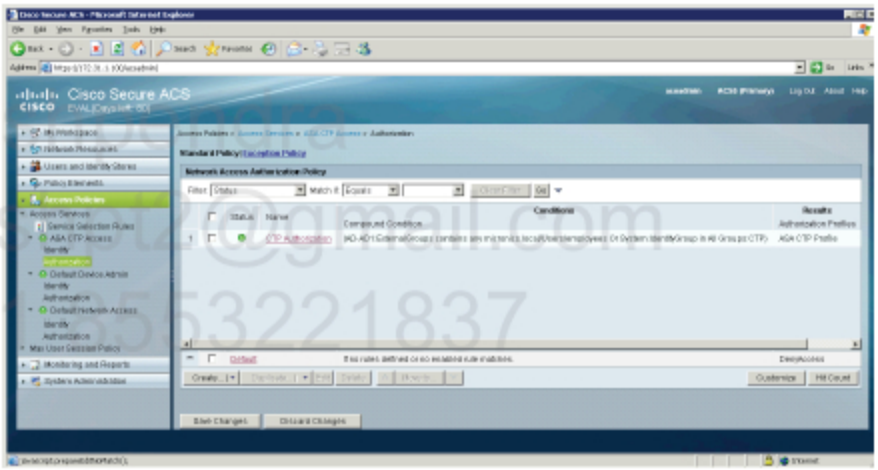



- If you're unsure if this is correct rule, you can always click **Preview** button to see the whole ruleset.


- Click on **Default** rule to edit it and change **Results** to **DenyAccess**.




Click on **Save Changes**.



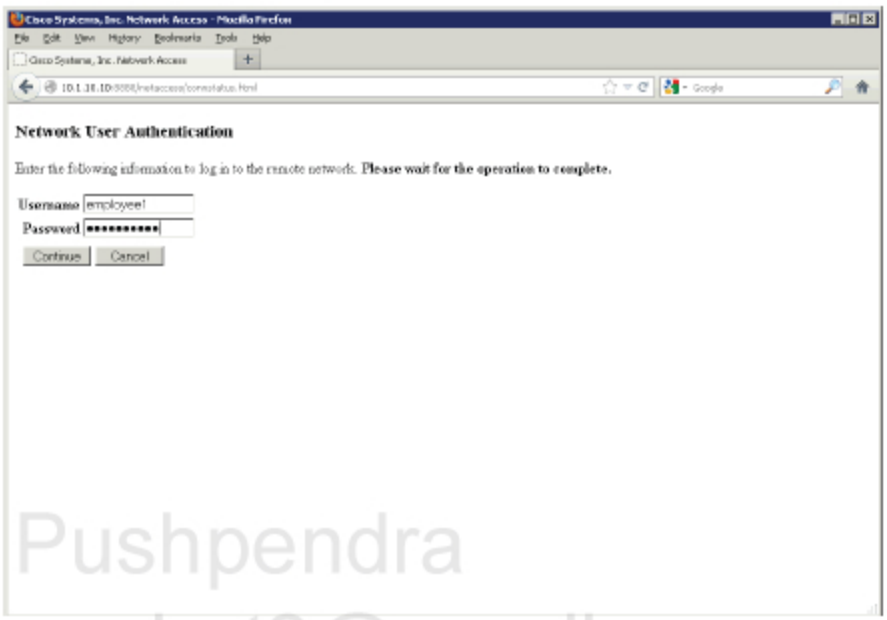

## Verification

Using Windows CMD start TELNET session to www.micronics.com on port 3389. The session should fail.

```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> open www.micronics.com 3389
Connecting To www.micronics.com...

Error:  Must authenticate before using this service.

Connection to host lost.
```

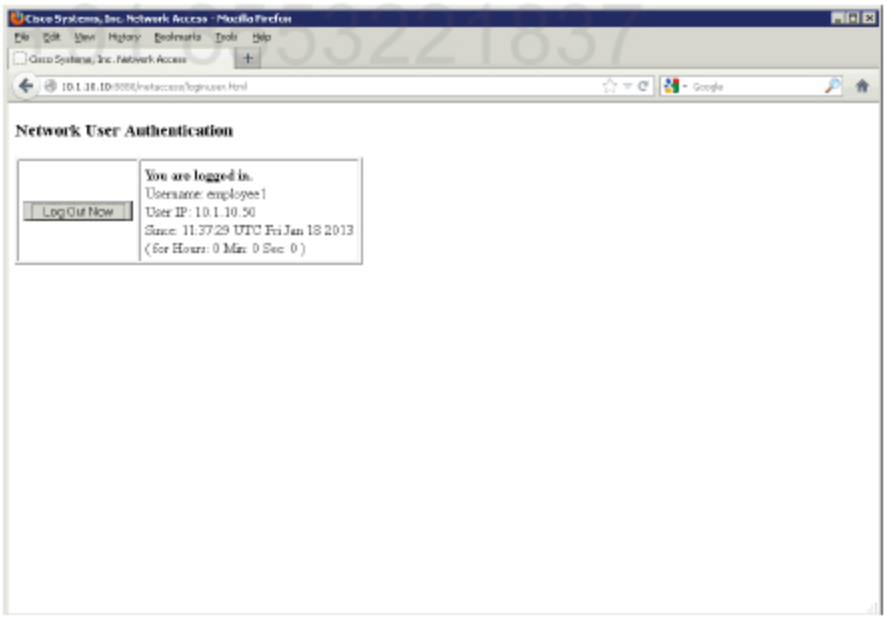
```
Press any key to continue...
```

Open up the web browser and go to http://10.1.10.10:8888/netaccess/loginuser.html. Provide username and password from Active Directory and click Continue button.






You should get the following information after successful authentication.




Verify commands on the ASA

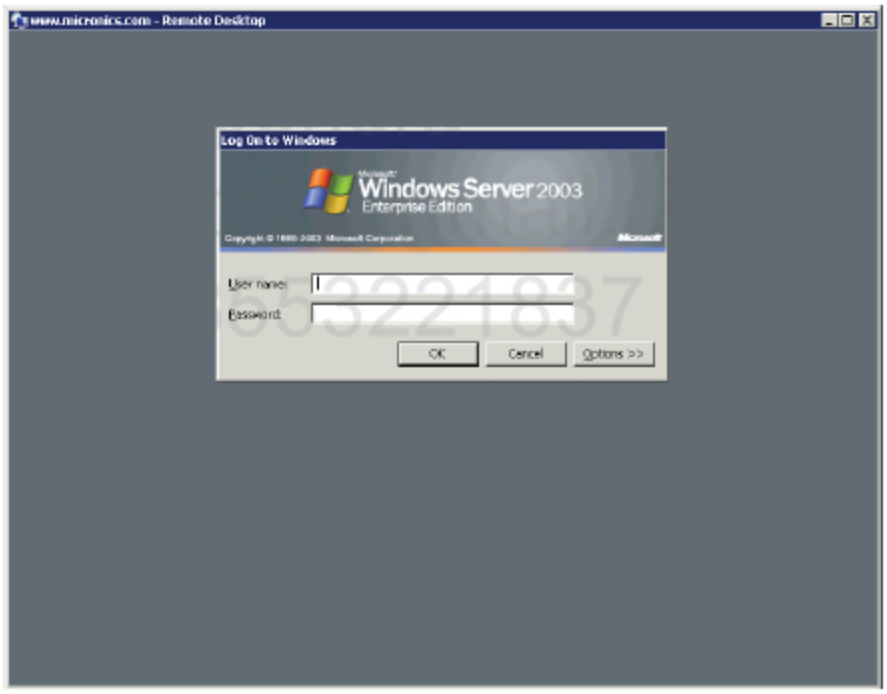
```
ASA1(config)# sh uauth
                        Current    Most Seen
```

```
Authenticated Users       1          1
Authen In Progress        0          2
user 'employee1' at 10.1.10.50, authenticated
   access-list #ACSACL#-IP-ASA-CTP-50aa0baf (*)
   absolute   timeout: 2:00:00
   inactivity timeout: 0:15:00
```

**Note the username and DACL name. Also timeout values are important. Check the ACL. It is applied 'per user'.**

```
ASA1(config)# sh access-list #ACSACL#-IP-ASA-CTP-50aa0baf
access-list #ACSACL#-IP-ASA-CTP-50aa0baf; 1 elements; name hash: 0x7fda124f (dynamic)
access-list #ACSACL#-IP-ASA-CTP-50aa0baf line 1 extended permit tcp any any eq 3389
(hitcnt=0) 0x30224544
```

Try to TELNET to www.micronics.com port 3389. It should now be successful. Alternatively you can try to use RDP client for that connection.




Check ACS RADIUS Authentication logs. You should see the employee1 user was authenticated and authorized by ASA CTP Access service.

| ACS View Timestamp | ACS Timestamp | RADIUS Status | NAS Failure | Details | Username | MAC/IP Address | Access Service | Authentication Method | Network Device | NAS IP Address |
|---|---|---|---|---|---|---|---|---|---|---|
| Nov 20,12 9:38:37.310 AM | Nov 20,12 9:38:37.280 AM | ✔ | | | #ACSACL#-IP-ASA-CTP-50aa0baf | ip:source-ip=10.1.10.50 | | | ASA | 10.1.10.10 |
| Nov 20,12 9:38:37.190 AM | Nov 20,12 9:38:37.176 AM | ✔ | | | employee1 | ip:source-ip=10.1.10.50 | ASA CTP Access | PAP_ASCII | ASA | 10.1.10.10 |