Configuring IPS Blocking Using IME

Document ID: 44905

Contents

Introduction

This document discusses the configuration of the Intrusion Prevention System (IPS) blocking with the use of the IPS Manager Express (IME). IME and IPS Sensors are used to manage a Cisco router for blocking. Remember these items when you consider this configuration:

- Install the Sensor and make sure the Sensor works properly.
- Make the sniffing interface span to the router outside the interface.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IPS Manager Express 7.0
- Cisco IPS Sensor 7.0(0.88)E3
- Cisco IOS® router with Cisco IOS Software Release 12.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

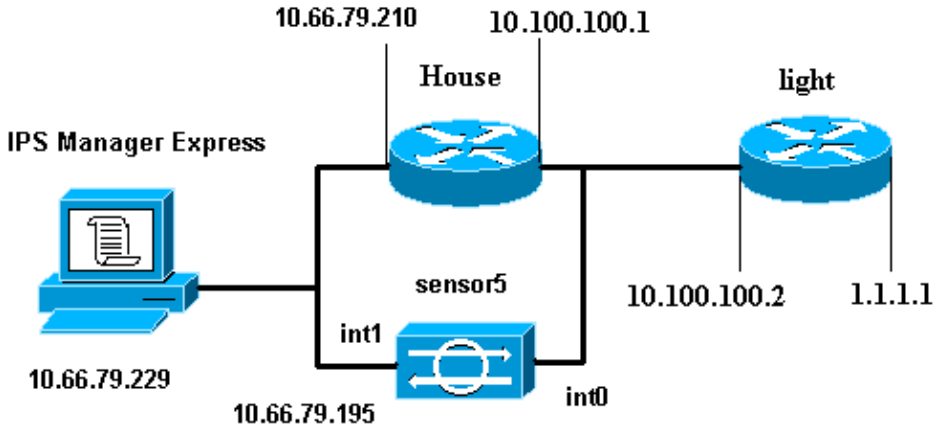
Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

Network Diagram

This document uses this network setup.



Configurations

This document uses these configurations.

- Router Light
- Router House

Router Light
Current configuration : 906 bytes ! version 12.4 service timestamps debug uptime service timestamps log uptime no service password-encryption ! **hostname light** ! enable password cisco ! username cisco password 0 cisco ip subnet-zero ! ! ! ip ssh time-out 120 ip ssh authentication-retries 3 ! call rsvp-sync ! ! !

```
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
!
!
!
interface FastEthernet0/0
 ip address 10.100.100.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface BRI4/0
 no ip address
 shutdown
interface BRI4/1
 no ip address
 shutdown
!
interface BRI4/2
 no ip address
 shutdown
!
interface BRI4/3
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.100.1
ip http server
ip pim bidir-enable
!
!
dial-peer cor custom
!
!
line con 0
line 97 108
line aux 0
line vty 0 4
 login
!
end
```

Router House

```
Current configuration : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
logging queue-limit 100
enable password cisco
!
ip subnet-zero
!
```

```
!
no ip cef
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
!
interface FastEthernet0/0
 ip address 10.66.79.210 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.100.100.1 255.255.255.0
 ip access-group IDS_FastEthernet0/1_in_0 in

!--- After you configure blocking,
!--- IDS Sensor inserts this line.

 duplex auto
 speed auto
!
interface ATM1/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.193
ip route 1.1.1.0 255.255.255.0 10.100.100.2
no ip http server
no ip http secure-server
!
!
ip access-list extended IDS_FastEthernet0/1_in_0
 permit ip host 10.66.79.195 any
 permit ip any any

!--- After you configure blocking,
!--- IDS Sensor inserts this line.

!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
line vty 5 15
 login
!
!
```

```
end
```

Start the Sensor Configuration

Complete these steps to start the configuration of the Sensor.

1. If this is your first time logging into the Sensor, you must enter **cisco** as the user name and **cisco** as the password.
2. When the system prompts you, change your password.

   Note: Cisco123 is a dictionary word and is not allowed in the system.
3. Type **setup** and follow the system prompt to setup the basic parameters for the Sensors.
4. Enter this information:

```
sensor5#setup

    --- System Configuration Dialog ---


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

Current time: Thu Oct  22 21:19:51 2009

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[10.66.79.195/24,10.66.79.193]:

Modify current access list?[no]:
Current access list entries:

!--- permit the ip address of workstation or network with IME

Permit:10.66.79.0/24
Permit:
Modify system clock settings?[no]:
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
```

5. Save the configuration.

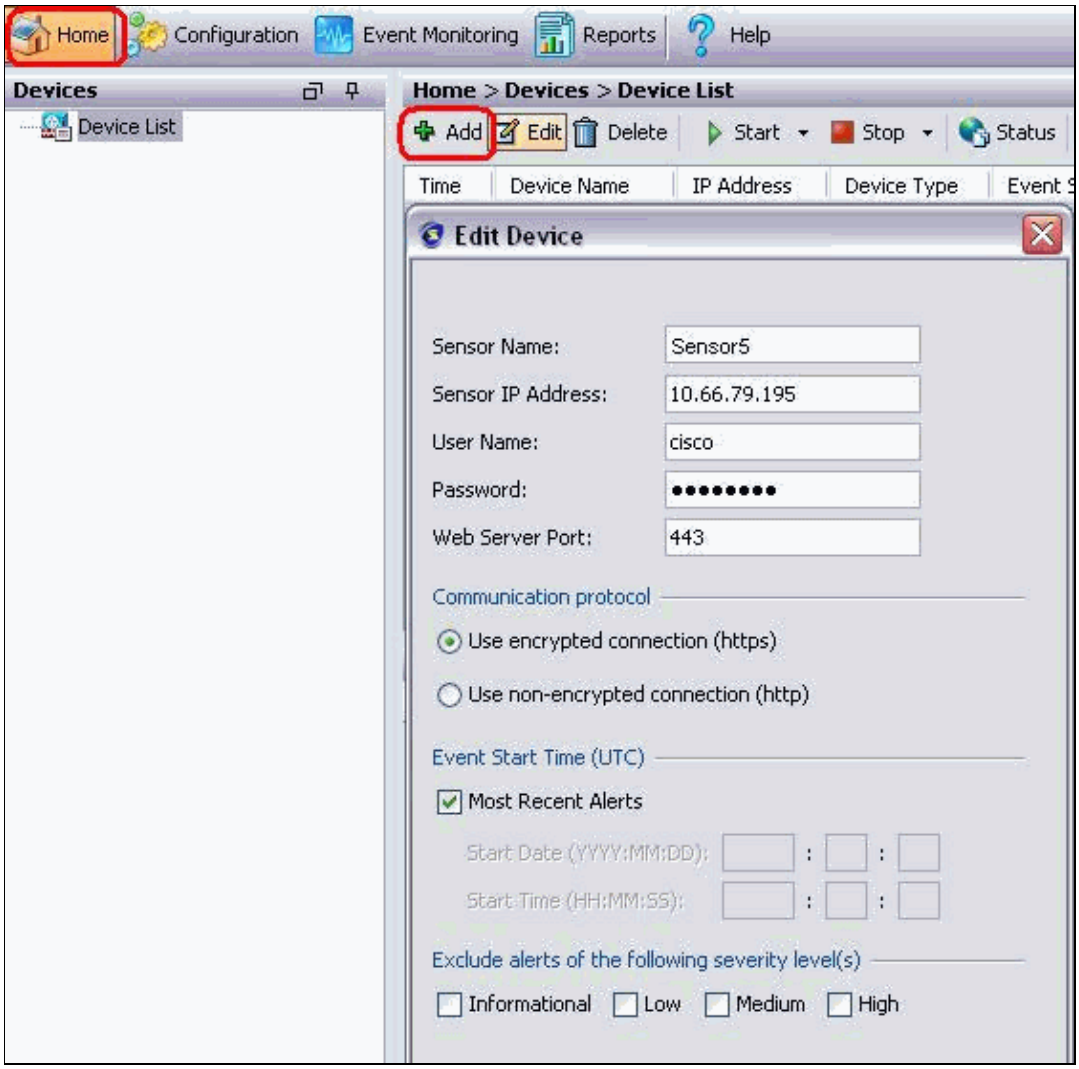
It can take a few minutes for the Sensor to save the configuration.

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

Enter your selection[2]: 2
```

Add the Sensor into the IME

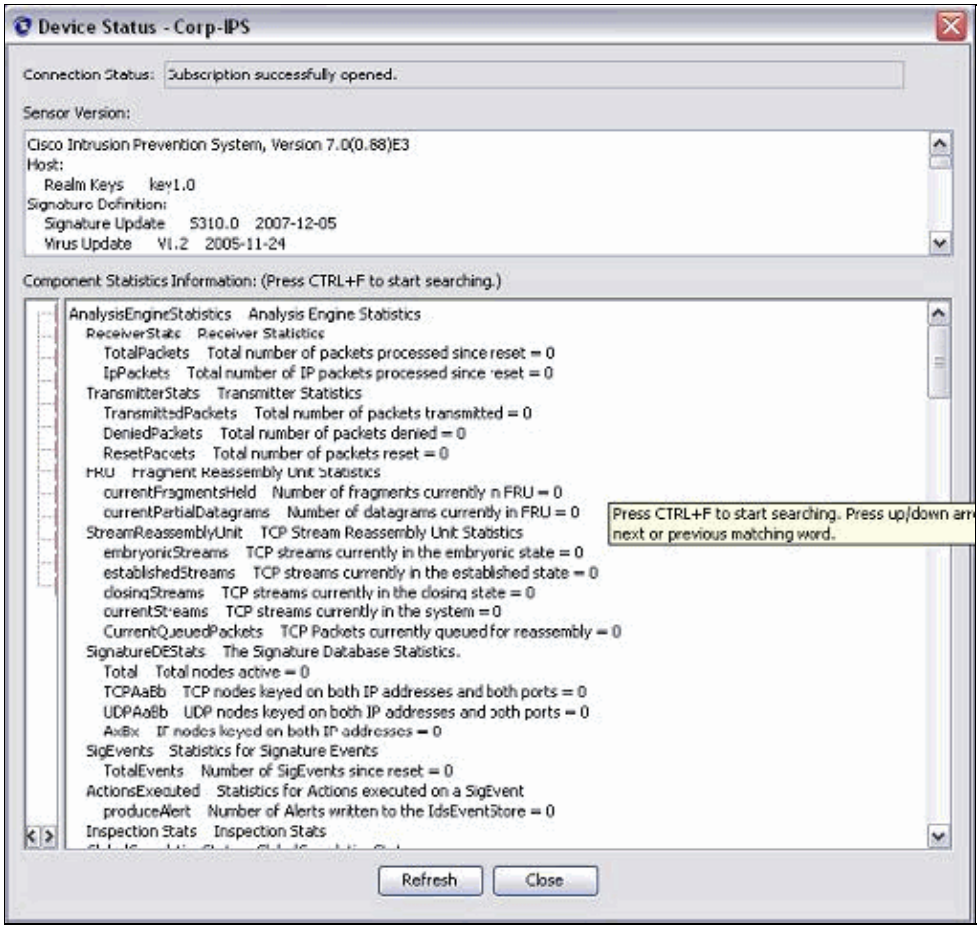
Complete these steps in order to add the Sensor into the IME.

1. Go to the Windows PC, which installed the IPS Manager Express and open the **IPS Manager Express**.
2. Choose **Home** > **Add**.
3. Type in this information and click **OK** in order to finish the configuration.



4. Choose **Devices** > **sensor5** in order to verify the Sensor status and then right−click to choose **Status**.

   Make sure that you can see the *Subscription successfully opened.* message.

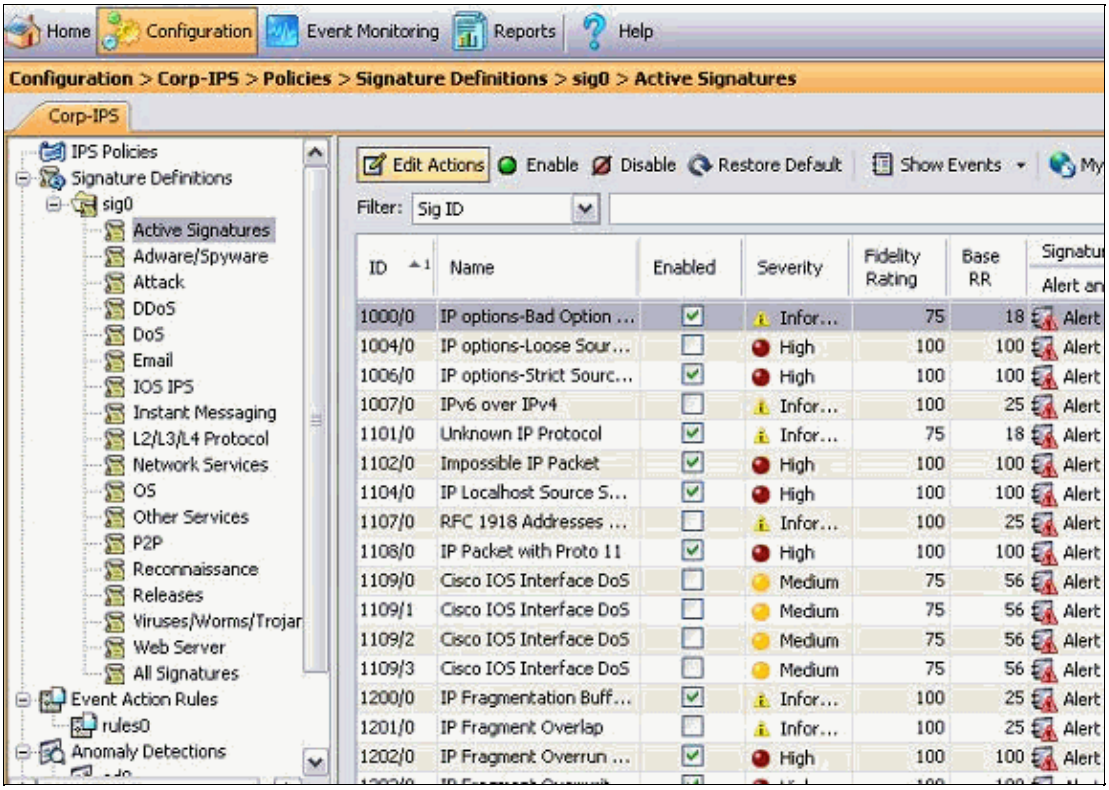


Configure Blocking for the Cisco IOS Router

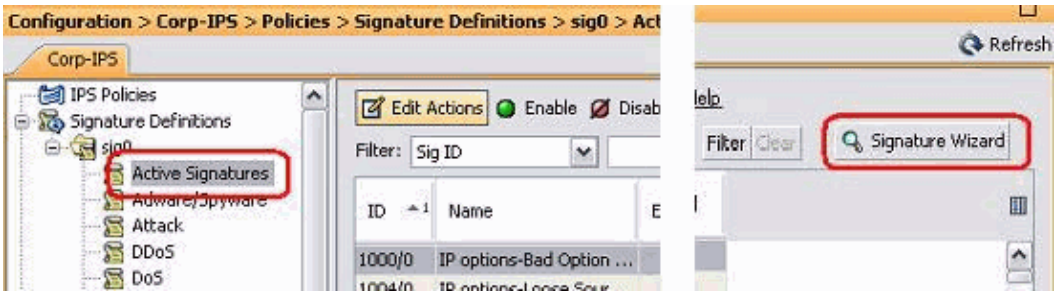
Complete these steps in order to configure the blocking for the Cisco IOS route:.

1. From the IME PC, open your web browser and go to **https://10.66.79.195**.
2. Click **OK** in order to accept the HTTPS certificate downloaded from the Sensor.
3. In the Login window, enter **cisco** for the user name and **123cisco123** for the password.

   This IME management interface appears:

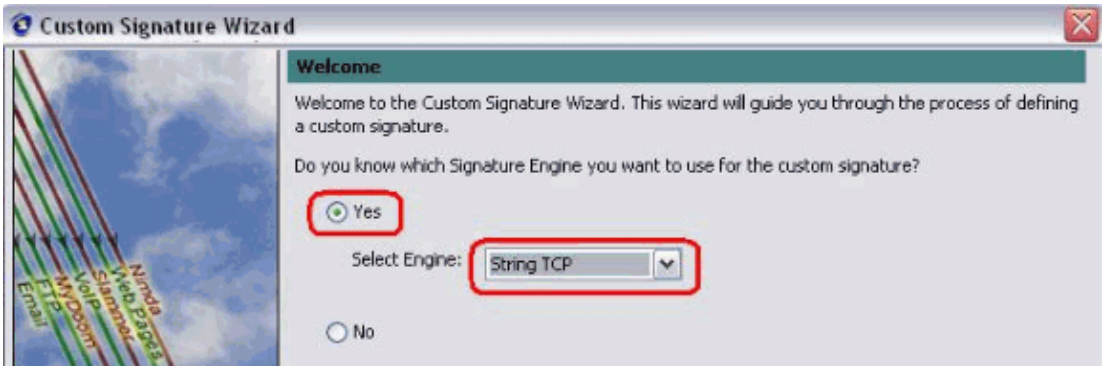


4. From the Configuration tab, click **Active Signatures**.
5. Then, click **Signature Wizard**.

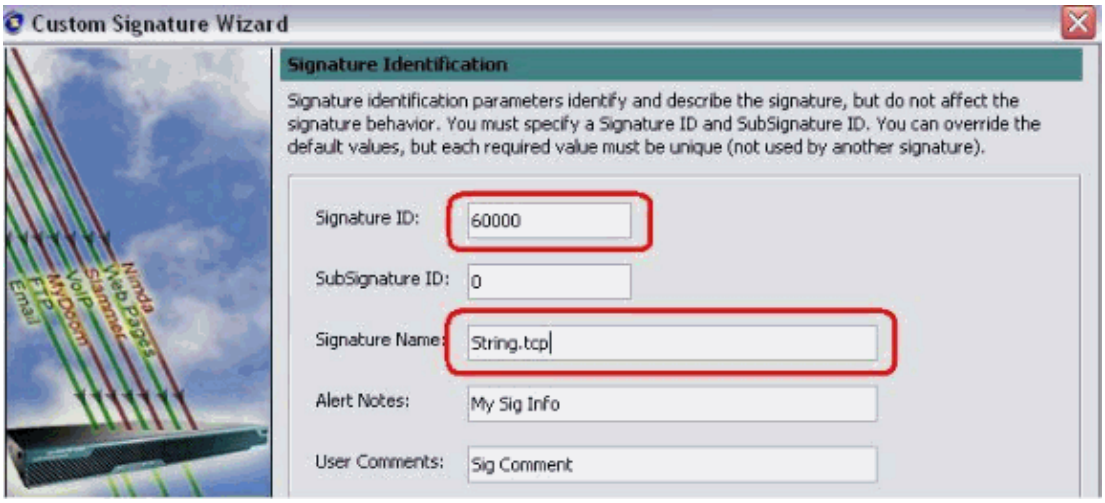


Note: The previous screenshot has been cut into two parts because of space limitation.

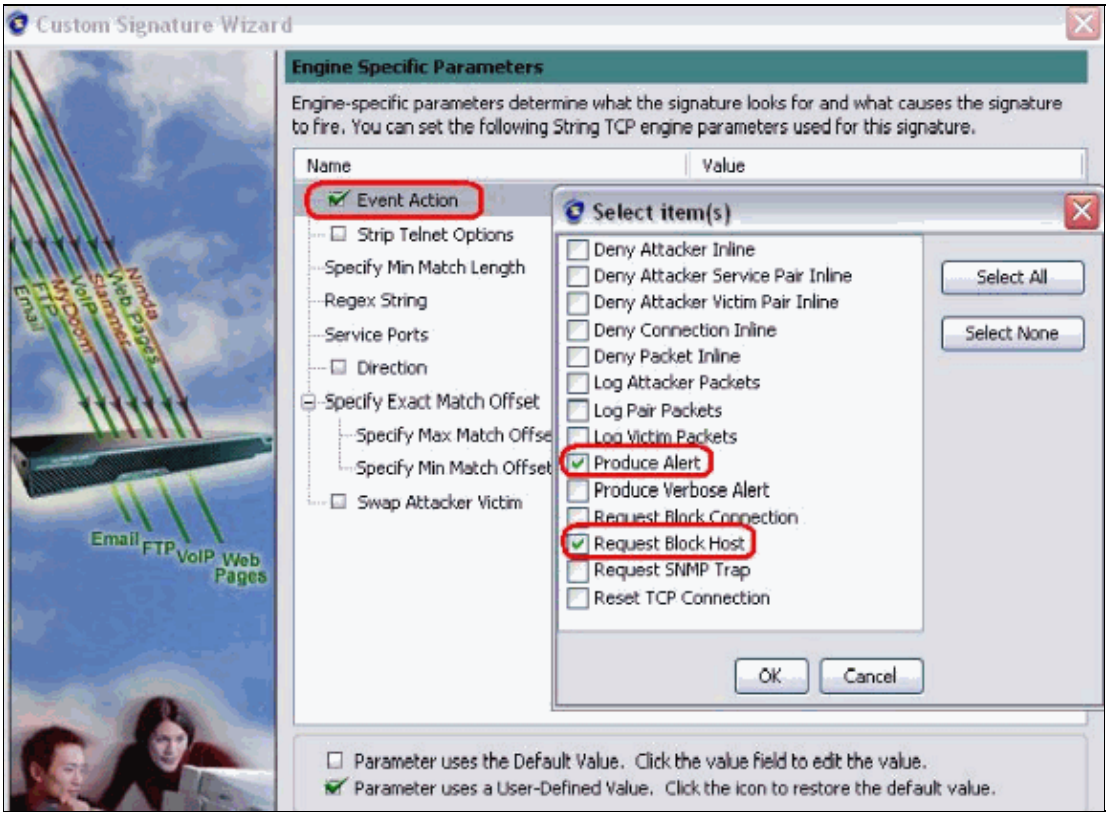
6. Choose **Yes** and **String TCP** as Signature engine. Click **Next**.



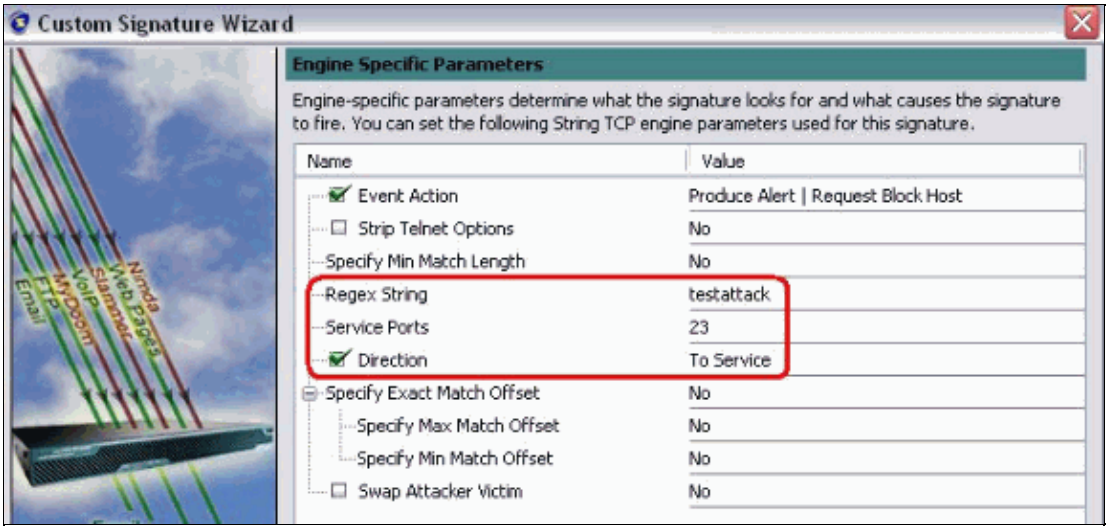
7. You can leave this information as Default or enter your own Signature ID, Signature Name and User Notes. Click **Next**.



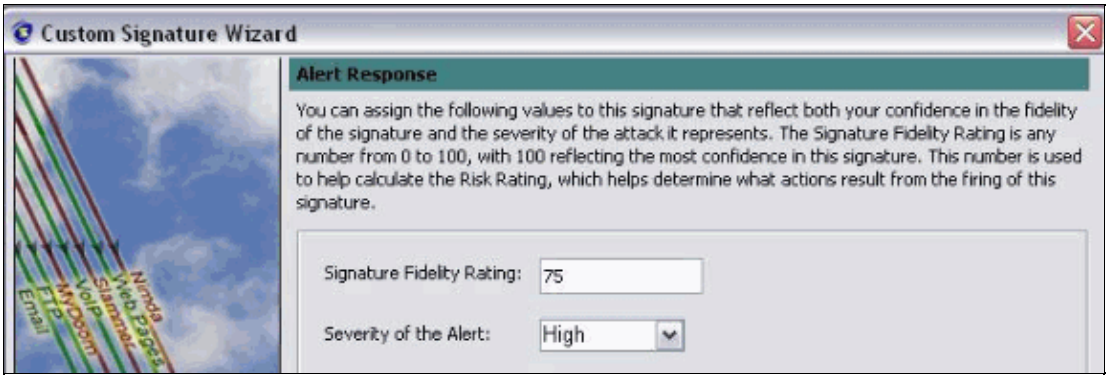
8. Choose **Event Action** and choose **Produce Alert** and **Request Block Host**. Click **Next** in order to continue.



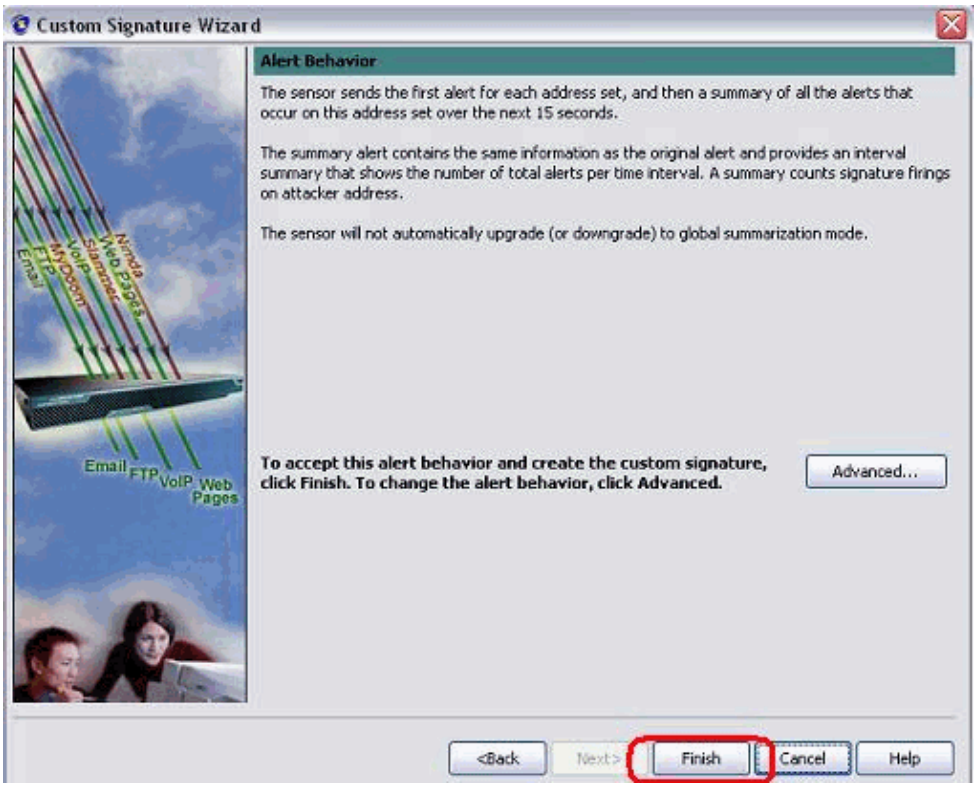
9. Enter a Regular Expression , which in this example is *testattack*, enter **23** for Service Ports, choose **To Service** for the Direction, and click **Next** in order to continue.



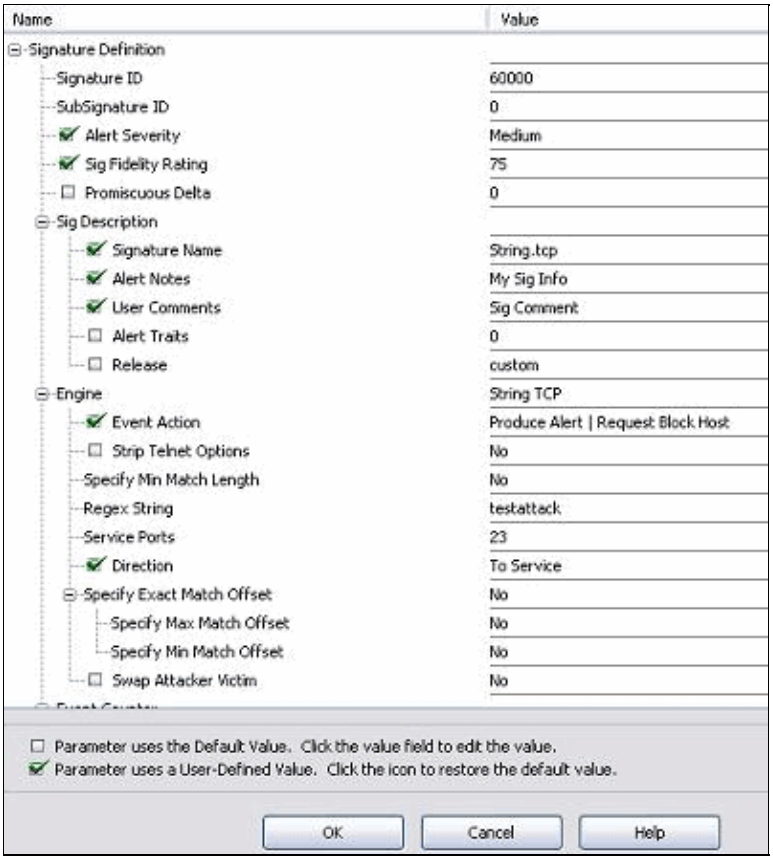
10. You can leave this information as Default. Click **Next**.



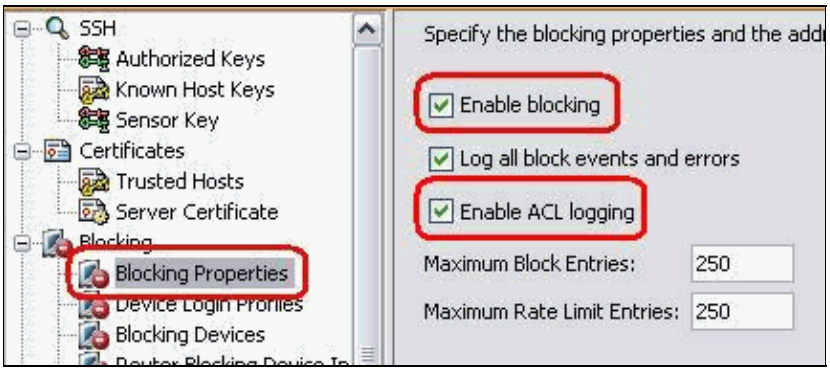
11. Click **Finish** in order to finish the Wizard.



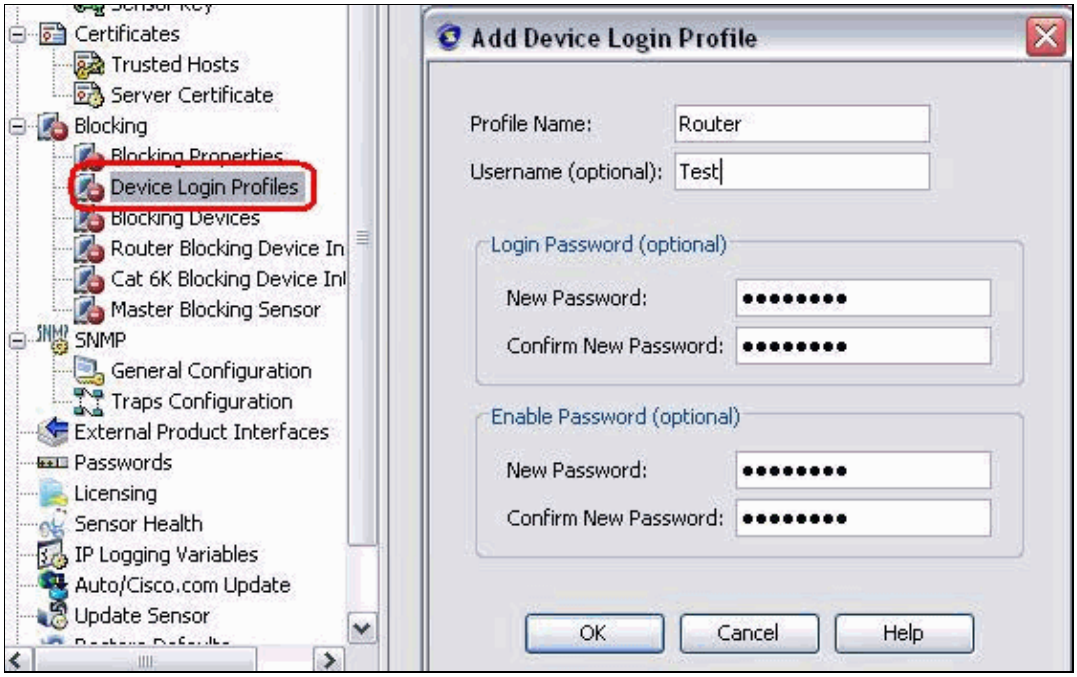
12. Choose **Configuration > sig0 > Active Signatures** in order locate the newly created signature by **Sig ID** or **Sig Name**. Click **Edit** in order to view the signature.



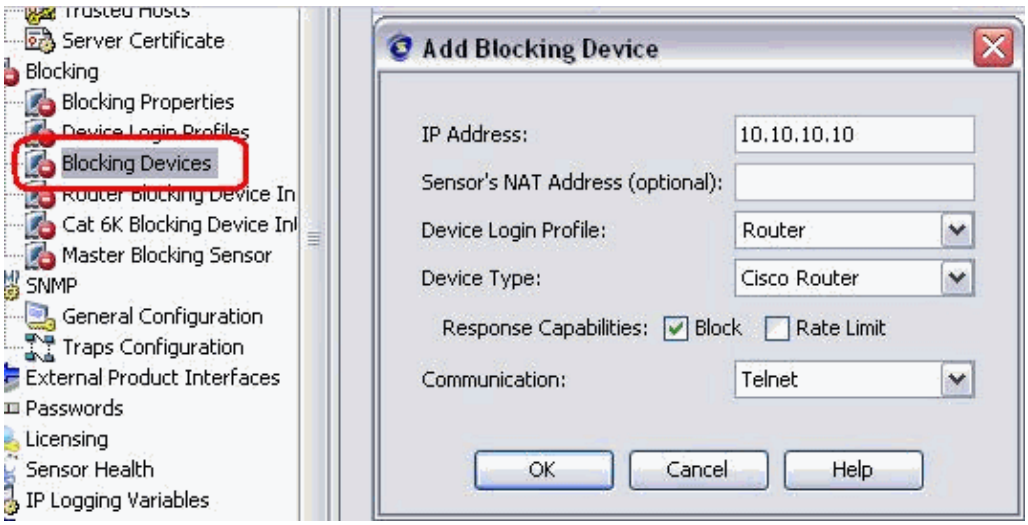
13. Click **OK** after you confirm and click the **Apply** button in order to apply the signature to the Sensor.
14. From the Configuration tab, under Sensor Management click **Blocking**. From the left pane, choose **Blocking Properties** and check **Enable Blocking**.



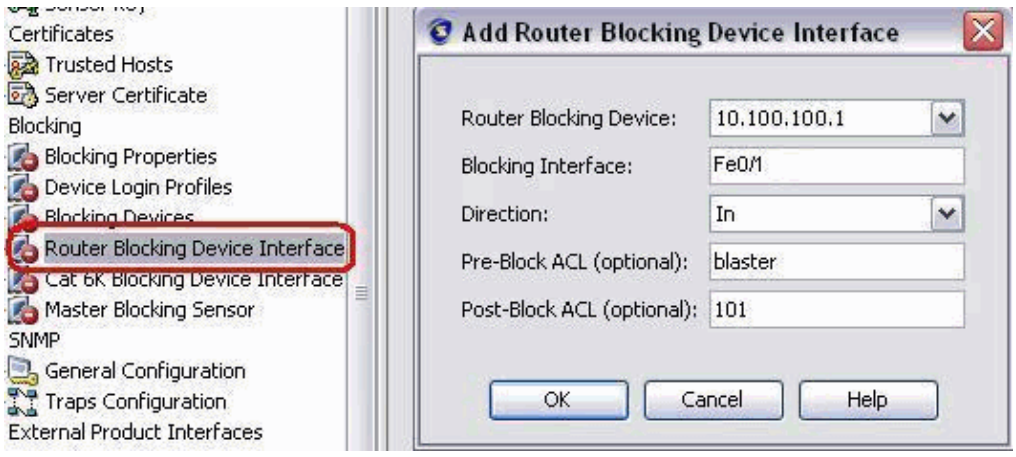
15. Now from the left pane, go to **Device Login Profile**. In order to create a new profile, click **Add**. Once created click **OK** and **Apply** in order to sensor and continue.



16. The next step is to configure Router as Blocking device. From the left pane, choose **Blocking Device**, click **Add** in order to add this information. Then click **OK** and **Apply**.



17. Now from the left pane configure the Blocking device interfaces. Add the information, click **OK** and **Apply**..



Verify

Launch the Attack and Blocking

Complete these steps to launch the attack and blocking:

1. Before you launch the attack, go to the IME, choose **Event Monitoring > Dropped Attacks View** and choose the sensor on the right.
2. Telnet to Router House and verify the communication from the server with these commands.

```
house#show user

  Line      User       Host(s)          Idle        Location
* 0 con 0                idle          00:00:00
226 vty 0               idle          00:00:17     10.66.79.195


house#show access-list
Extended IP access list IDS_FastEthernet0/1_in_0
  permit ip host 10.66.79.195 any
  permit ip any any (12 matches)
house#
```

3. From Router Light, Telnet to Router House and type **testattack**.

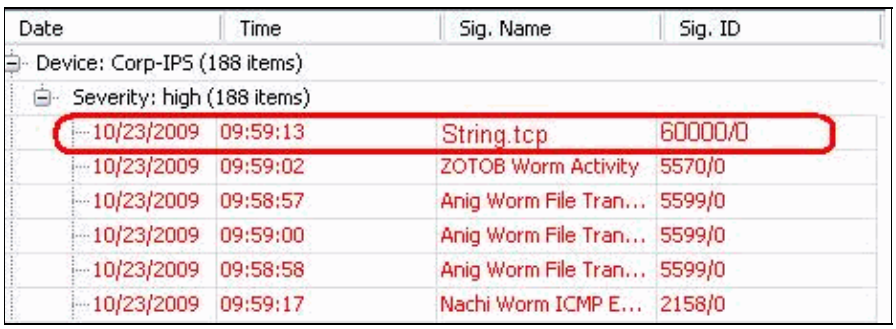
   Hit either **<space>** or **<enter>** in order to reset your Telnet session.

```
light#telnet 10.100.100.1
    Trying 10.100.100.1 ... Open

    User Access Verification
    Password:
    house>en
    Password:
    house#testattack
    [Connection to 10.100.100.1 lost]

!--- Host 10.100.100.2 has been blocked due to the
   !--- signature "testattack" triggered.
```

4. Telnet to Router House and use the **show access-list** command as shown here.

```
house#show access-list
Extended IP access list IDS_FastEthernet0/1_in_0
10 permit ip host 10.66.79.195 any
20 deny ip host 10.100.100.2 any (71 matches)
30 permit ip any any
```

5. From the Dashboard of the IDS Event Viewer, the Red Alarm appears once the attack is launched.



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Tips

Use these troubleshooting tips:

- From the Sensor look at the **show statistics network−access** output and make sure that the `state`"is active. From the console or SSH to the Sensor, this information is viewed:

```
sensor5#show statistics network-access
Current Configuration
  AllowSensorShun = false
  ShunMaxEntries = 100
  NetDevice
    Type = Cisco
    IP = 10.66.79.210
    NATAddr = 0.0.0.0
    Communications = telnet
    ShunInterface
      InterfaceName = FastEthernet0/1
      InterfaceDirection = in
State
  ShunEnable = true
  NetDevice
    IP = 10.66.79.210
    AclSupport = uses Named ACLs
    State = Active
  ShunnedAddr
    Host
      IP = 10.100.100.2
      ShunMinutes = 15
      MinutesRemaining = 12
sensor5#
```

- Make sure the communication parameter shows that the correct protocol is used such as Telnet or SSH with 3DES. You can try a manual SSH or Telnet from an SSH/Telnet client on a PC in order to check the username and password credentials are correct. Then try to Telnet or SSH from the Sensor itself to the router and see if you can login successfully to the router.

Related Information

- **Cisco Secure Intrusion Prevention Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Dec 17, 2009 Document ID: 44905