

Configuring IDS Blocking Using IDM and IEV

Document ID: 44905

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Start the Sensor Configuration

Add the Sensor into the IEV

Configure Blocking for the Cisco IOS Router

Verify

- Launch the Attack and Blocking

Troubleshoot

- IEV Problem
- Tips

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document discusses the configuration of the Intrusion Detection System (IDS) blocking using the IDS Device Manager (IDM) and IDS Event Viewer (IEV). IDM and IDS 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 IDS Event Viewer 4.1.1S(50)
- Cisco IDS Sensor 4.1.1S(50)
- Cisco IOS® router with Cisco IOS Software Release 12.2(15)T5

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.

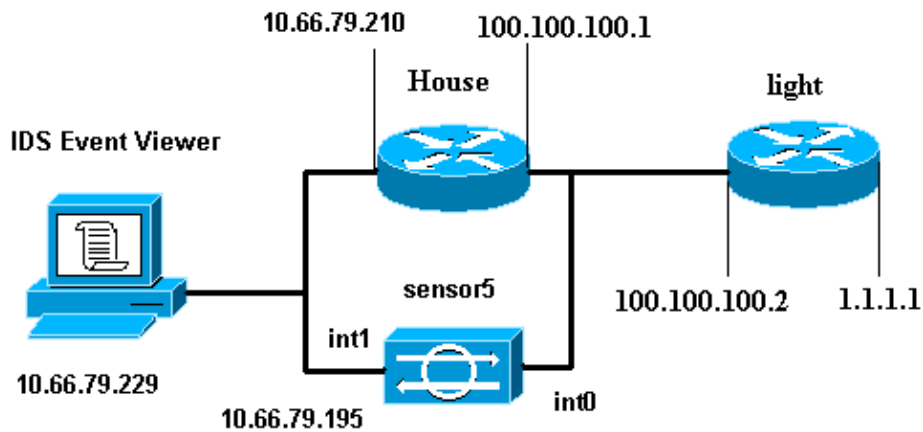
Conventions

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
<pre>Current configuration : 906 bytes ! version 12.2 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 ! ! !</pre>

```

fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
!
!
!
interface FastEthernet0/0
  ip address 100.100.100.2 255.255.255.0
  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 0.0.0.0 100.100.100.1
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 12.2
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 100.100.100.1 255.255.255.0  
  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 1.1.1.0 255.255.255.0 100.100.100.2  
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  
!  
!
```

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 Configuration:

```
networkParams
ipAddress 10.66.79.195
netmask 255.255.255.224
defaultGateway 10.66.79.193
hostname sensor5
telnetOption enabled
accessList ipAddress 10.66.79.0 netmask 255.255.255.0
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
```

5. Save the configuration.

It might take a few minutes for the Sensor saving 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.
```

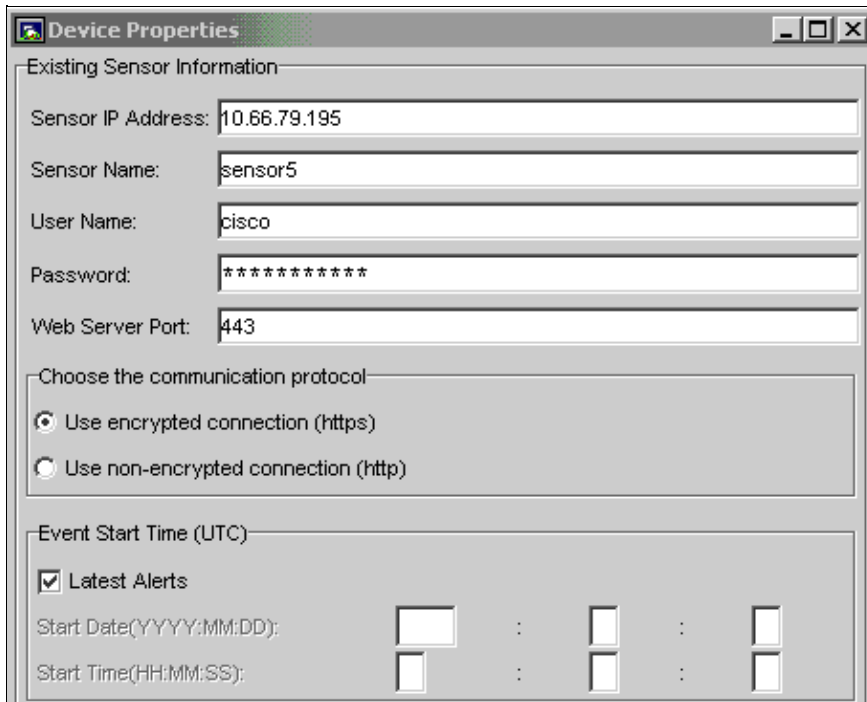
```
Enter your selection[2]: 2
```

Add the Sensor into the IEV

Complete these steps to add the Sensor into the IEV.

1. Go to the Windows 2000 PC which installed the IEV and open the IEV.

2. Select **File > New > Device**.
3. Type in this information and click **OK** to finish the configuration.



Device Properties

Existing Sensor Information

Sensor IP Address: 10.66.79.195

Sensor Name: sensor5

User Name: cisco

Password: *****

Web Server Port: 443

Choose the communication protocol

Use encrypted connection (https)

Use non-encrypted connection (http)

Event Start Time (UTC)

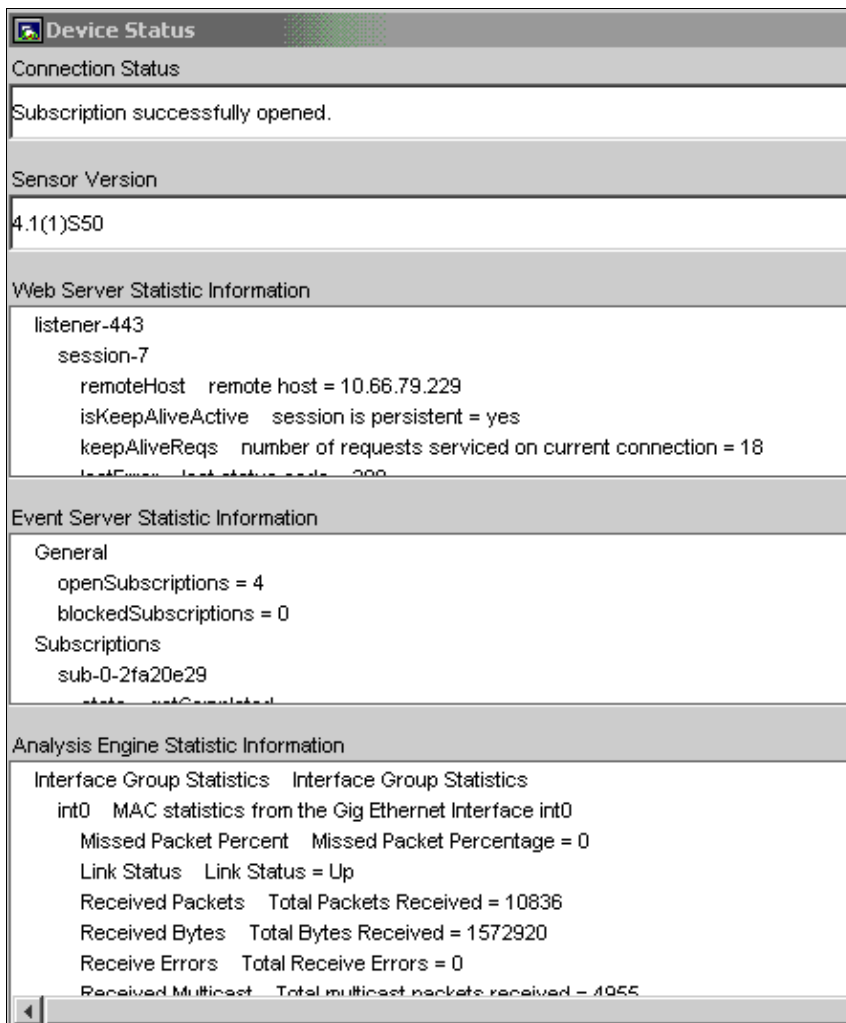
Latest Alerts

Start Date(YYYY:MM:DD): : :

Start Time(HH:MM:SS): : :

4. Verify the Sensor status by selecting **Devices > sensor5** and then right-click to select **Device Status**.

Make sure that you can see "Subscription successfully opened."

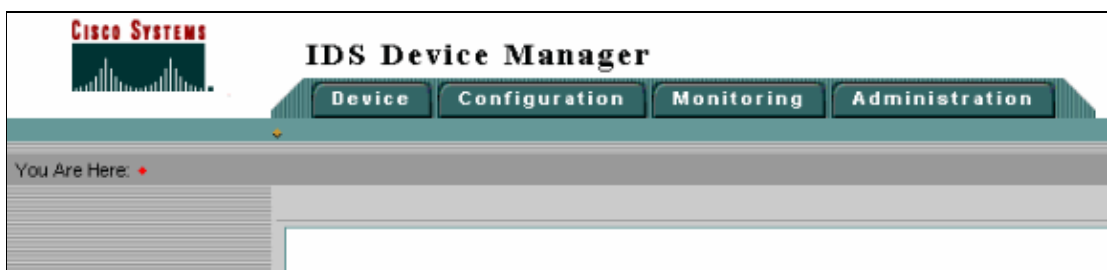


Configure Blocking for the Cisco IOS Router

Complete these steps to configure the blocking for the Cisco IOS router.

1. From the IEV PC, open your web browser and go to <https://10.66.79.195>.
2. Click **OK** 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 IDM management interface appears:



4. From the Configuration tab, click **Sensing Engine**.
5. On the left pane, click **Signature Wizard**.
6. Under Virtual Sensor Configuration, click the **Start the Wizard** button.
7. Select **Signature Type** from Wizard Tasks then choose **TCP Stream Signature**.
8. Click **Next** to continue.

Wizard Tasks	
<input checked="" type="checkbox"/> Signature Type	
<input type="checkbox"/> Signature Identification	
<input type="checkbox"/> Engine-Specific Parameters	
<input type="checkbox"/> Alert Response	
<input type="checkbox"/> Alert Behavior	
<input type="checkbox"/> Finish	

Web Server Signatures	
Web Server Signature:	<input type="radio"/>
Packet Signatures	
TCP Packet Signature:	<input type="radio"/>
UDP Packet Signature:	<input type="radio"/>
IP Packet Signature:	<input type="radio"/>
Stream Signatures	
TCP Stream Signature:	<input checked="" type="radio"/>
UDP Stream Signature:	<input type="radio"/>
ICMP Stream Signature:	<input type="radio"/>

Note: * - Required Field

9. You can leave this information as Default or enter your own Signature ID and User Notes. Click **Next** to continue.

Wizard Tasks	
<input checked="" type="checkbox"/> Signature Type	
<input checked="" type="checkbox"/> Signature Identification	
<input type="checkbox"/> Engine-Specific Parameters	
<input type="checkbox"/> Alert Response	
<input type="checkbox"/> Alert Behavior	
<input type="checkbox"/> Finish	

Signature Identification	
Signature ID *:	<input type="text" value="20002"/>
SubSignature ID *:	<input type="text" value="0"/>
Signature Name:	<input type="text" value="STRING.TCP"/>
Alert Notes:	<input type="text"/>
User Notes:	<input type="text"/>

Note: * - Required Field

10. Enter a Regular Expression ("testattack" is used in this example), enter **23** for Service Ports, select **To Port** for the Direction, and click **Next** to continue.

TCP Stream Signature	
Regular Expression *	testattack
Service Ports *	23
Direction *	To Port
Offset in Packet to Examine(bytes):	
Minimum Matching String Length:	
<input type="button" value="Back"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Next"/>	
Note: * - Required Field	

11. Set the Severity of the Alert to **high** and highlight **Shun Host** in the Action to Take in Response list.

Shun Host blocks attacking IP hosts or IP subnets.

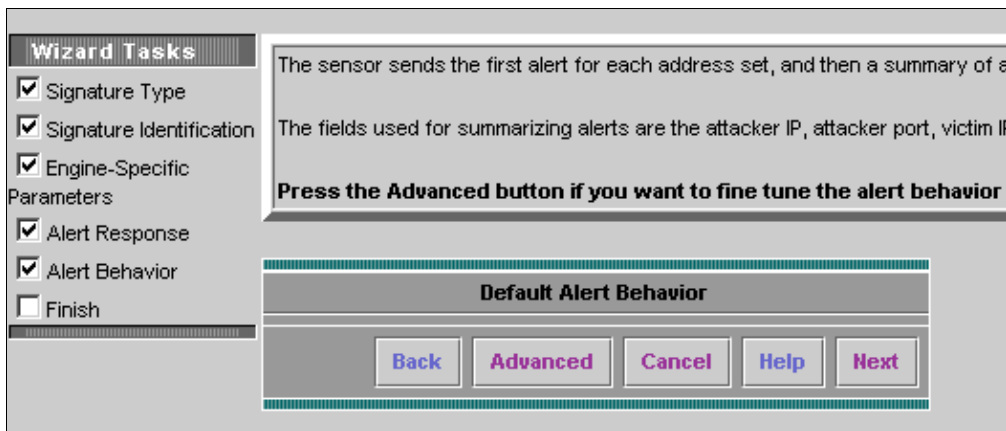
Shun Connection blocks TCP or UDP ports (based on attacking TCP or UDP connections).

12. Click **Next** to continue.

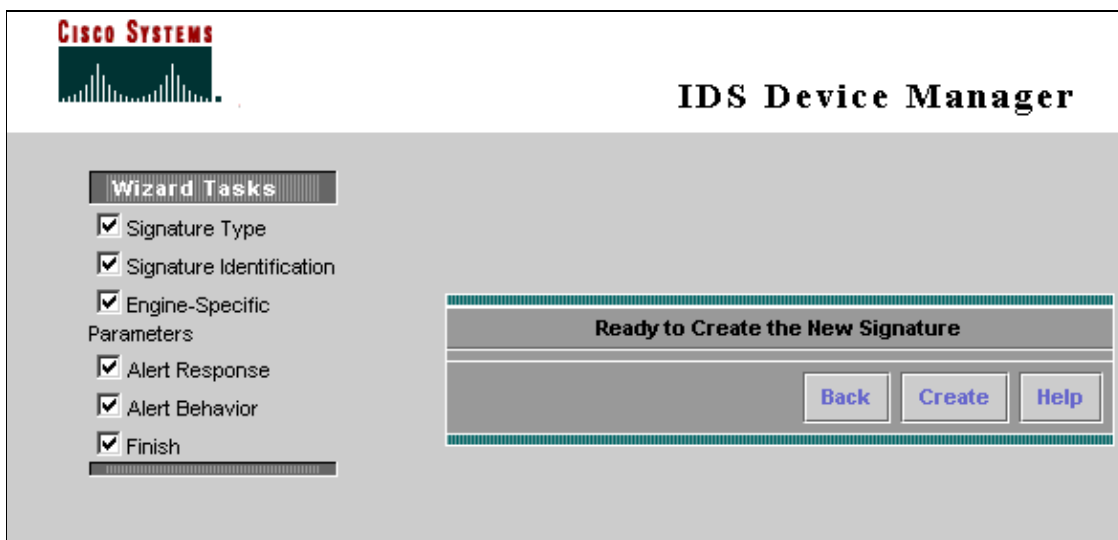
Wizard Tasks	Alert Response Actions
<input checked="" type="checkbox"/> Signature Type	Severity of the Alert: high
<input checked="" type="checkbox"/> Signature Identification	Action to Take in Response: Log Reset Shun Host Shun Connection
<input checked="" type="checkbox"/> Engine-Specific Parameters	
<input checked="" type="checkbox"/> Alert Response	Swap Address Report Ordering:
<input type="checkbox"/> Alert Behavior	Include Packet in Alert: False
<input type="checkbox"/> Finish	<input type="button" value="Back"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Next"/>
Note: * - Required Field	

13. Use the Default settings in the Alert Behavior screen and click **Next** to continue.

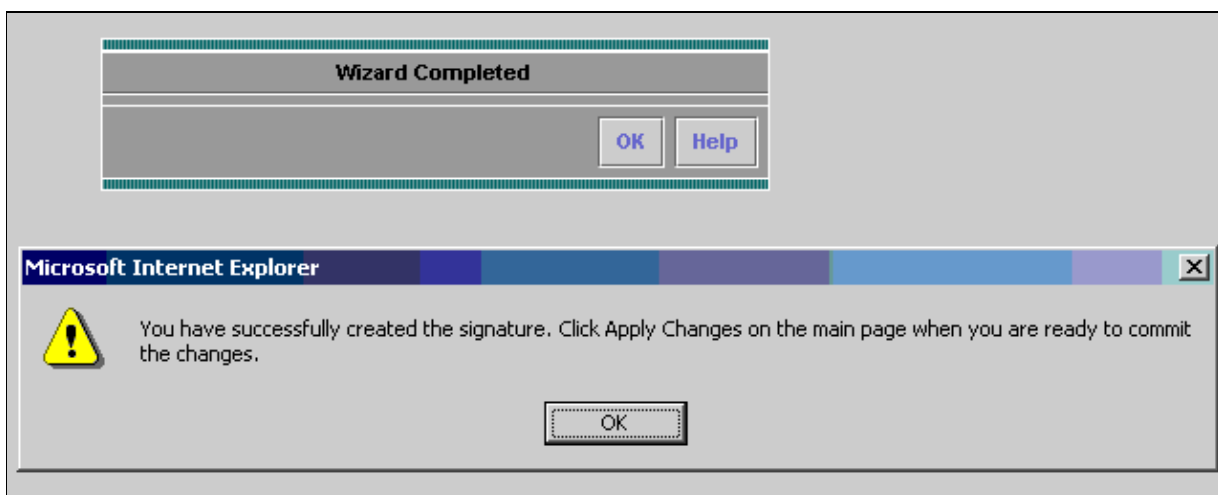
Click **Advanced** if you want to fine tune the alert behavior.



14. Click **Create** to create the new signature.



15. Click **OK** twice to confirm it.



16. From the main menu, click the **Save Changes** icon to apply the signature to the Sensor.

17. This step is optional, and is used if you want to verify or perform further modification to the signature.

- a. Click the Configuration tab and choose **Sensing Engine**.
- b. From the left pane, select **Signature Configuration Mode** under Virtual Sensor Configuration.
- c. Click **All Signatures**.
- d. From the Page drop-down menu, select **20002**.

e. For the Signature ID, check **20002** and click **Edit**.

You can modify everything about this signature from this page.

f. Click **OK** to confirm your change or click **Cancel** if you are not applying any changes.

Direction * :	ToService
Enabled * :	True
EndMatchOffset :	
EventAction :	log reset shunHost shunConnection
FlipAddr :	
MaxInspectLength :	
MaxTTL :	
MinHits :	1
MinMatchLength :	
Protocol * :	FRAG IP TCP UDP
RegexString * :	testattack
ResetAfterIdle :	15
ServicePorts * :	23
SigComment :	
SigName :	STRING.TCP

18. From the Configuration tab, click **Blocking**.

19. From the left pane, select **Blocking Properties** and check **Enable Blocking**.

20. Set the timer (for example, 15 minutes).

21. Click **Apply to Sensor** to continue.

Blocking Properties	
Enable Blocking:	<input checked="" type="checkbox"/>
Allow the Sensor IP to be Blocked:	<input type="checkbox"/>
Maximum Block Entries *:	100
Block Time *:	15
Apply to Sensor Reset	
Note: * - Required Field	

22. From the left pane, select **Logical Devices** and click **Add** to add this information and then click **Apply to Sensor** to continue.

Adding	
Name *	<input type="text" value="house"/>
Enable Password:	<input type="password" value="*****"/>
Password:	<input type="password" value="*****"/>
Username:	<input type="text"/>
<input type="button" value="Apply to Sensor"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/>	

Note: * - Required Field

23. From the left pane, select **Blocking Devices**, click **Add** to add this information, and then click **Apply to Sensor** to continue.

Adding	
IP Address *	<input type="text" value="10.66.79.210"/>
NAT Address:	<input type="text"/>
Apply Logical Device:	<input type="text" value="house"/>
Device Type:	<input type="text" value="Cisco Router"/>
Communication:	<input type="text" value="Telnet"/>
<input type="button" value="Apply to Sensor"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/>	

Note: * - Required Field

24. Under Blocking Devices, select **Router Blocking Device Interfaces**, click **Add** to add this information, and click **Apply to Sensor** to continue.

Editing	
IP Address *	<input type="text" value="10.66.79.210"/>
Blocking Interface:	<input type="text" value="FastEthernet0/1"/>
Blocking Direction:	<input type="text" value="In"/>
Pre-Block ACL Name:	<input type="text" value="198"/>
Post-Block ACL Name:	<input type="text" value="199"/>
<input type="button" value="Apply to Sensor"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/>	

Note: * - Required Field

Verify

Launch the Attack and Blocking

Complete these steps to launch the attack and blocking.

1. Before you launch the attack, go to the IEV, select **Tools > Realtime Dashboard** and click **Launch Dashboard**.
2. Telnet to Router House and verify the communication from the server using the commands shown here.

```
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>** to reset your Telnet session.

```
light#telnet 100.100.100.1
```

```
Trying 100.100.100.1 ... Open
```

```
User Access Verification
```

```
Password:
```

```
house>en
```

```
Password:
```

```
house#testattack
```

```
[Connection to 100.100.100.1 lost]
```

```
!--- Host 100.100.100.2 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 100.100.100.2 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.

Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time
STRING.TCP	20002	High	sensor5	2003-08-22 06:48:05
STRING.TCP	20002	High	sensor5	2003-08-22 06:47:22
STRING.TCP	20002	High	sensor5	2003-08-22 06:46:52
STRING.TCP	20002	High	sensor5	2003-08-22 03:52:18

6. In the Dashboard, highlight one of the alarms, then right-click and choose **show context** or **NSDB link** to view more detail information with the alarm.

You can check the online version of NSDB in the Cisco Secure Encyclopedia (registered customers only)

Troubleshoot

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

IEV Problem

The `IOException` when try to get certificate: Connection times out: connect error message displays if you are not able to connect the IDS Sensor from IEV. The problem might be due to obstacles like the Firewall or any Cisco device with an access list configuration that blocks the traffic between the IEV and IDS Sensor. In general, the path between the IEV and IDS device should be clear communication.

Tips

Use these troubleshooting tips:

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

```
sensor5#show statistics networkaccess
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 = 100.100.100.2
      ShunMinutes = 15
      MinutesRemaining = 12
sensor5#
```

- Make sure the communication parameter shows that the correct protocol is being used such as Telnet or SSH with 3DES. You can try a manual SSH or Telnet from an SSH/Telnet client on a PC 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.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security

Security: Intrusion Detection [Systems]

Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco Secure Intrusion Detection Support Page](#)
- [Documentation for Cisco Secure Intrusion Detection System](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 21, 2007

Document ID: 44905
