

Configuring IDS Blocking Using VMS IDS MC

Document ID: 46743

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations
- Initial Sensor Configuration
- Import the Sensor into IDS MC
- Import the Sensor into Security Monitor
- Use IDS MC for Signature Updates
- Configure Blocking for the IOS Router

Verify

- Launch the Attack and Blocking

Troubleshoot

- Troubleshooting Procedure

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a sample for the configuration of the Cisco Intrusion Detection System (IDS) via the VPN/Security Management Solution (VMS), IDS Management Console (IDS MC). In this case, Blocking from the IDS Sensor to a Cisco router is configured.

Prerequisites

Requirements

Before you configure Blocking, ensure you have met these conditions.

- The Sensor is installed and configured for sensing necessary traffic.
- The sniffing interface is spanned to the router outside interface.

Components Used

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

- VMS 2.2 with IDS MC and Security Monitor 1.2.3
- Cisco IDS Sensor 4.1.3S(63)
- Cisco Router running Cisco IOS® Software Release 12.3.5

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

For more information on document conventions, see the Cisco Technical Tips Conventions.

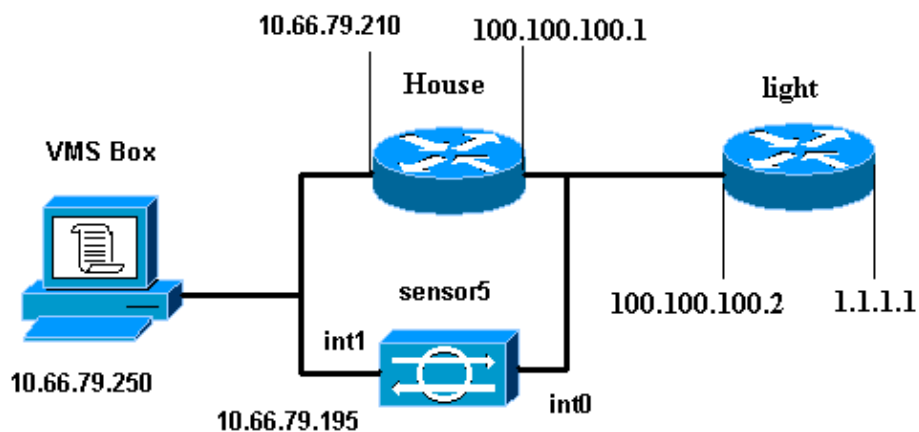
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses the configurations shown here.

- Router Light
- Router House

Router Light

```
Current configuration : 906 bytes
!
version 12.3
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 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

Building configuration...

Current configuration : 797 bytes

```
!
version 12.3
no service pad
service timestamps debug datetime msec
```

```

service timestamps log datetime msec
no service password-encryption
!
hostname House
!
logging queue-limit 100
enable password cisco
!
ip subnet-zero
no ip domain lookup
!
!
interface Ethernet0
  ip address 10.66.79.210 255.255.255.224
  hold-queue 100 out
!
interface Ethernet1
  ip address 100.100.100.1 255.255.255.0

!--- After Blocking is configured, the IDS Sensor
!--- adds this access-group ip access-group.

IDS_Ethernet1_in_0 in
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
ip http server
no ip http secure-server
!

!--- After Blocking is configured, the IDS Sensor
!--- adds this access list.

ip access-list extended IDS_Ethernet1_in_0.
  permit ip host 10.66.79.195 any
  permit ip any any
!
line con 0
  stopbits 1
line vty 0 4
  password cisco
  login
!
scheduler max-task-time 5000
end

```

Initial Sensor Configuration

Complete these steps to initially configure the Sensor.

Note: If you have performed the initial setup of your Sensor, proceed to the section Importing the Sensor into IDS MC.

1. Console into the Sensor.

You are prompted for a username and password. If this is the first time you are consoling into the Sensor, you must login with the username **cisco** and password **cisco**.

2. You are prompted to change the password and then re-type the new password to confirm.
3. Type **setup** and enter the appropriate information at each prompt to set up basic parameters for your Sensor, as per this example:

```
sensor5#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 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
```

4. Press **2** in order to save your configuration.

Import the Sensor into IDS MC

Complete these steps to import the Sensor into the IDS MC.

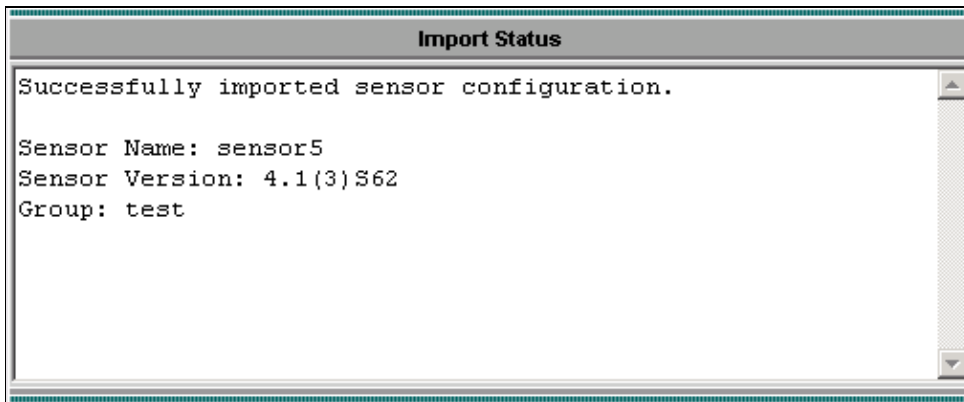
1. Browse to your Sensor.

In this case, browse to either **http://10.66.79.250:1741** or **https://10.66.79.250:1742**.

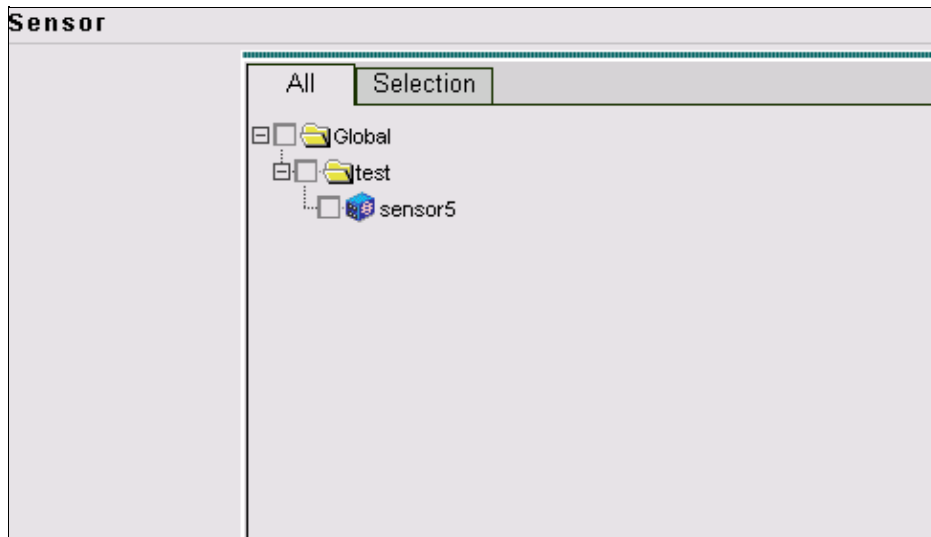
2. Login with the appropriate username and password.

In this example, the username **admin** and password **cisco** were used.

3. Select **VPN/Security Management Solution > Management Center** and choose **IDS Sensors**.
4. Click the **Devices** tab, select **Sensor Group**, highlight **Global**, and click **Create Subgroup**.
5. Enter the Group Name and ensure the **Default** radio button is selected, then click **OK** to add the subgroup into the IDS MC.



10. Your Sensor is imported into the IDS MC. In this case, sensor5 is imported.



Import the Sensor into Security Monitor

Complete this procedure to import the Sensor into the security monitor.

1. At the VMS Server menu, select **VPN/Security Management Solution > Monitoring Center > Security Monitor**.
2. Select the Devices tab, then click **Import** and enter the IDS MC Server Information, as per this example.

Enter IDS MC server contact information:	
IP Address/Host Name: *	<input type="text" value="10.66.79.250"/>
Web Server Port: *	<input type="text" value="443"/>
Username: *	<input type="text" value="admin"/>
Password: *	<input type="password" value="j@bb@ck"/>
Note: * - Required Field	

3. Select your Sensor (in this case, **sensor5**) and click **Next** to continue.

Showing 1 records

	<input type="checkbox"/>	Name	IP Address	NAT Address	Type	Comment
1.	<input checked="" type="checkbox"/>	sensor5	10.66.79.195		RDEP IDS	Comment

4. If need be, update the Network Address Translation (NAT) address for your Sensor, then click **Finish** to continue.

Showing 1 records

	Name	IP Address	NAT Address
1.	sensor5	10.66.79.195	

-- Editable columns

5. Click **OK** to finish importing the Sensor from IDS MC into Security Monitor.

Import Summary:

```
1 device(s) were imported.

Following 1 device(s) were imported successfully:
[sensor5]
```

OK

6. Your Sensor is successfully imported.

Showing 1-1 of 1 records

	Device Name	IP Address	NAT Address	Device Type	Description
1.	<input type="radio"/> sensor5	10.66.79.195		RDEP IDS	Comment

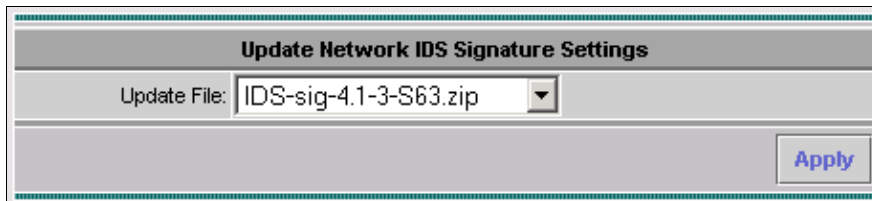
Rows per page: 10 << Page 1 >>

Add Edit Import View Delete

Use IDS MC for Signature Updates

Complete this procedure to use the IDS MC for signature updates.

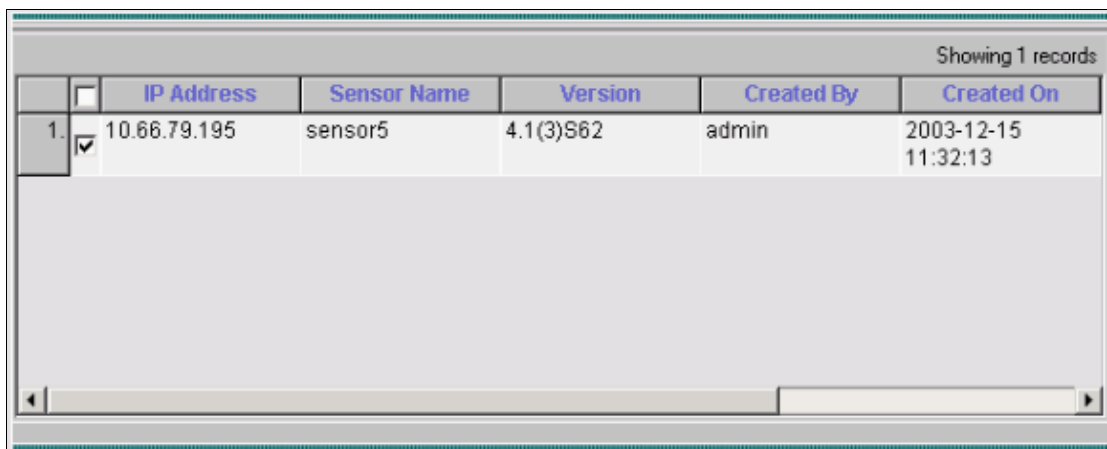
1. Download the Network IDS Signature updates (registered customers only) from the Downloads and save them in the C:\PROGRA~1\CSCOPx\MDC\etc\ids\updates\ directory on your VMS server.
2. At the VMS server console, select **VPN/Security Management Solution > Management Center > Sensors**.
3. Click the Configuration tab, select **Updates**, and click **Update Network IDS Signatures**.
4. Select the signature you want to upgrade from the drop-down menu and click **Apply** to continue.



Update Network IDS Signature Settings

Update File:

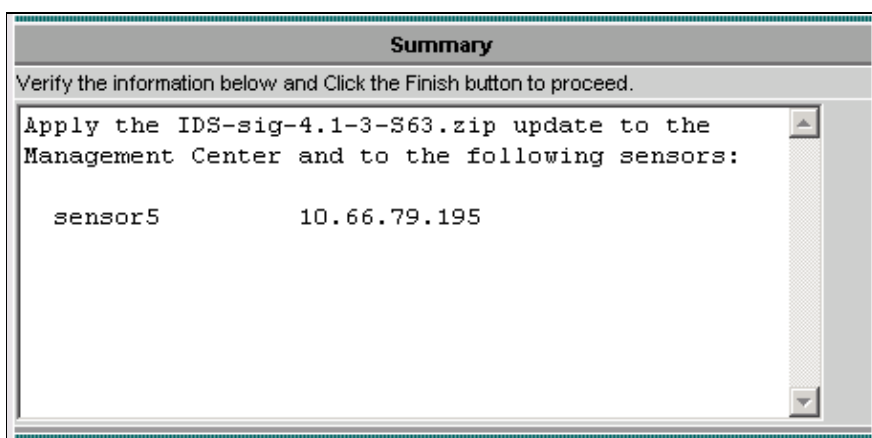
5. Select the Sensor(s) to update, and click **Next** to continue.



Showing 1 records

	<input type="checkbox"/>	IP Address	Sensor Name	Version	Created By	Created On
1.	<input checked="" type="checkbox"/>	10.66.79.195	sensor5	4.1(3)S62	admin	2003-12-15 11:32:13

6. After you are prompted to apply the update to the Management Center, as well as the Sensor, click **Finish** to continue.



Summary

Verify the information below and Click the Finish button to proceed.

Apply the IDS-sig-4.1-3-S63.zip update to the Management Center and to the following sensors:

sensor5 10.66.79.195

7. Telnet or console into the Sensor command line interface. Information similar to this appears:

```
sensor5#  
Broadcast message from root (Mon Dec 15 11:42:05 2003):  
Applying update IDS-sig-4.1-3-S63.  
This may take several minutes.  
Please do not reboot the sensor during this update.  
Broadcast message from root (Mon Dec 15 11:42:34 2003):
```

```
Update complete.
sensorApp is restarting
This may take several minutes.
```

8. Wait for a few minutes to allow the upgrade to complete, then enter **show version** to verify.

```
sensor5#show version
Application Partition:
Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63

Upgrade History:
* IDS-sig-4.1-3-S62          07:03:04 UTC Thu Dec 04 2003
  IDS-sig-4.1-3-S63.rpm.pkg 11:42:01 UTC Mon Dec 15 2003
```

Configure Blocking for the IOS Router

Complete this procedure to configure Blocking for the IOS router.

1. At the VMS server console, select **VPN/Security Management Solution > Management Center > IDS Sensors**.
2. Select the Configuration tab, select your Sensor from Object Selector, and click **Settings**.
3. Select **Signatures**, click **Custom**, then click **Add** to add a new signature.

Signature Group: Custom Filter Source: Signature Filter

Showing 0-0 of 0 records

<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
No records.							

Rows per page: 10 << Page 1 >>

Add Edit Delete

4. Enter the new Signature Name, then select the Engine (in this case, **STRING.TCP**).
5. You can customize the available parameters by checking the appropriate radio button and clicking **Edit**.

In this example, the ServicePorts parameter is edited to change its value to 23 (for port 23). The RegexpString parameter is also edited to add the value **testattack**. When this is complete, click **OK** to continue.

Tune Signature Parameters

Signature Name:

Engine:

Engine Description:

Showing 25 records				
	Parameter Name	Value	Default	Required
1.	<input type="radio"/> ServicePorts	23		Yes
2.	<input type="radio"/> StorageKey	STREAM	STREAM	Yes
3.	<input type="radio"/> RegexString	testattack		Yes
4.	<input type="radio"/> SummaryKey	AaBb	AaBb	Yes
5.	<input type="radio"/> Direction	ToService	ToService	Yes
6.	<input type="radio"/> Protocol	TCP	TCP	Yes
7.	<input type="radio"/> AlarmDelayTimer			No
8.	<input type="radio"/> AlarmInterval			No
9.	<input type="radio"/> AlarmThrottle	Summarize	Summarize	Nn

6. To edit the Signature Severity and Actions or to Enable/Disable the signature, click the name of the signature.

Signature Group: Filter Source:

Showing 1-1 of 1 records

<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
1. <input type="checkbox"/>	20001	mytest	0	STRING.TCP	Yes	Medium	None

Rows per page: << Page 1 >>

7. In this case, the severity is changed to **High** and the **Block Host** action is selected. Click **OK** to continue.

- ◆ The Block Host blocks attacking IP hosts or IP subnets.
- ◆ The Block Connection blocks TCP or UDP ports (based on attacking TCP or UDP connections).

Edit Signature(s)

Signature:

Enable

Severity:

Actions: Log Reset Block Host Block Connection

8. The complete signature looks similar to this:

Signature Group: Custom Filter Source: Signature <input type="text"/> <input type="button" value="Filter"/>							
Showing 1-1 of 1 records							
<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
1. <input type="checkbox"/>	20001	mytest	0	STRING.TCP	Yes	High	Block
Rows per page: 10							<< Page 1 >>
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

9. In order to configure the Blocking Device, select **Blocking > Blocking Devices** from the Object Selector (the menu on the left hand side of the screen), and click **Add** to enter the following information:

Blocking Device	
Device Type: *	Cisco Router
IP Address: *	10.66.79.210
NAT Address:	
Comment:	<input type="text"/>
Username:	<input type="text"/>
Password: *	*****
Enable Password:	*****
Secure Communications:	none
Interfaces: *	Edit Interfaces
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	
Note: * - Required Field	

10. Click **Edit Interfaces** (see previous screen capture), click **Add**, enter this information, then click **OK** to continue.

Blocking Device Interface	
Blocking Interface Name	Ethernet1
Blocking Direction	inbound
Pre-block ACL Name	198
Post-block ACL Name	199
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

11. Click **OK** twice to complete the configuration of the Blocking device.

Showing 1-1 of 1 records				
	IP Address	Device Type	Comment	Source
1.	10.66.79.210	Cisco Router		sensor5

Rows per page: 10 << Page 1 >>

[Add](#) [Edit](#) [Delete](#)

12. To configure Blocking Properties, select **Blocking** > **Blocking Properties**.

The Length of Automatic Block can be modified. In this case, it is changed to **15 minutes**. Click **Apply** to continue.

Blocking Properties	
Length of Automatic Block	15 minutes
Maximum ACL Entries	100
Enable ACL Logging	<input type="checkbox"/>
Allow blocking devices to block the sensor's IP address	<input type="checkbox"/>
<input checked="" type="checkbox"/> Override	Apply Reset

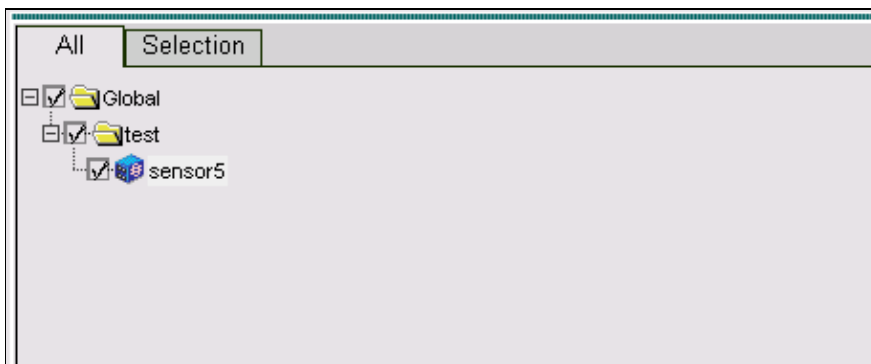
13. Select **Configuration** from the main menu, then select **Pending**, check the pending configuration to ensure it is correct, and click **Save**.

Showing 1-1 of 1 records				
<input type="checkbox"/>	Pending Configuration	Type	Last Modified On	Last Modified By
1.	<input checked="" type="checkbox"/> Global.test.sensor5	Sensor	2003-12-15 14:07:39	admin

Rows per page: 10 << Page 1 >>

[Save](#) [Delete](#)

14. To push the configuration changes to the Sensor, generate and then deploy the changes by selecting **Deployment** > **Generate** and click **Apply**.



15. Select **Deployment** > **Deploy**, then click **Submit**.
 16. Check the checkbox next to your Sensor, then click **Deploy**.
 17. Check the checkbox for the job in the queue, then click **Next** to continue.

Showing 1-1 of 1 records				
<input type="checkbox"/>	Configuration File Name	Sensor Name	Generated On	Generated By
1. <input checked="" type="checkbox"/>	sensor5_2003-12-15_17:00:14	Global.test.sensor5	2003-12-15 17:00:14	admin

Rows per page: 10 << Page 1 >>

18. Enter the Job Name and schedule the job as Immediate, then click **Finish**.

Schedule Type	
Job Name:	<input type="text" value="myjob1"/>
<input checked="" type="radio"/> Immediate	
<input type="radio"/> Scheduled	
Start Time:	December 15, 2003 18:54:03
Retry Options	
Maximum Number Of Attempts	<input type="text" value="0"/>
Time Between Attempts	<input type="text" value="15"/> minutes
Failure Options	
Overwrite conflicting sensor(s) configuration?	<input checked="" type="checkbox"/>
Require correct sensor versions?	<input checked="" type="checkbox"/>
Notification Options	
<input type="checkbox"/> Email report to:	<input type="text"/>
(When specifying more than one recipient, comma separate the addresses.)	

19. Select **Deployment > Deploy > Pending**.

Wait a few minutes until all the pending jobs have been completed. The queue is then empty.

20. To confirm the deployment, select **Configuration > History**.

Ensure the status of the configuration is displayed as **Deployed**. This means that the Sensor configuration has been updated successfully.

Showing 1-1 of 1 records				
<input type="checkbox"/>	Configuration File Name	Status	Generated	Deployed
1. <input type="checkbox"/>	sensor5_2003-12-15_23:04:36	Deployed	2003-12-15 23:04:36	2003-12-15 23:09:55

Rows per page: 10 << Page 1 >>

[View](#) [Delete](#)

Verify

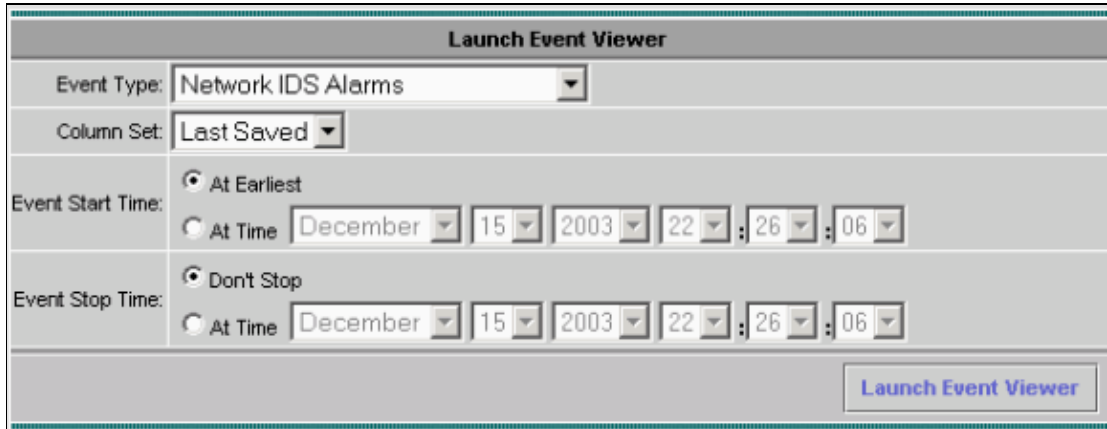
This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

Launch the Attack and Blocking

To verify that the Blocking process is working correctly, launch a test attack and check the results.

1. Before launching the attack, select **VPN/Security Management Solution > Monitoring Center > Security Monitor**.
2. Choose **Monitor** from the main menu, click **Events** and then click **Launch Event Viewer**.



The screenshot shows a 'Launch Event Viewer' dialog box with the following settings:

- Event Type: Network IDS Alarms
- Column Set: Last Saved
- Event Start Time: At Time (December 15, 2003, 22:26:06)
- Event Stop Time: Don't Stop

A 'Launch Event Viewer' button is located at the bottom right of the dialog.

3. Telnet to the router (in this case, Telnet to the House router), to verify the communication from the Sensor.

```
house#show user
      Line      User      Host(s)      Idle      Location
*  0 con 0
226 vty 0
      idle      idle      00:00:00
      idle      10.66.79.195
house#show access-list
Extended IP access list IDS_Ethernet1_in_0
 10 permit ip host 10.66.79.195 any
 20 permit ip any any (20 matches)
House#
```

4. To launch the attack, Telnet from one router to the other and type **testattack**.

In this case, we used Telnet to connect from the Light router to the House router. As soon as you press **<space>** or **<enter>**, after typing **testattack**, your Telnet session should be reset.

```
light#telnet 100.100.100.1
Trying 100.100.100.1 ... Open
User Access Verification
Password:
house>en
Password:
house#testattack
```

```
!--- Host 100.100.100.2 has been blocked due to the
!--- signature "testattack" being triggered.
```

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

5. Telnet to the router (House) and enter the command **show access-list**.

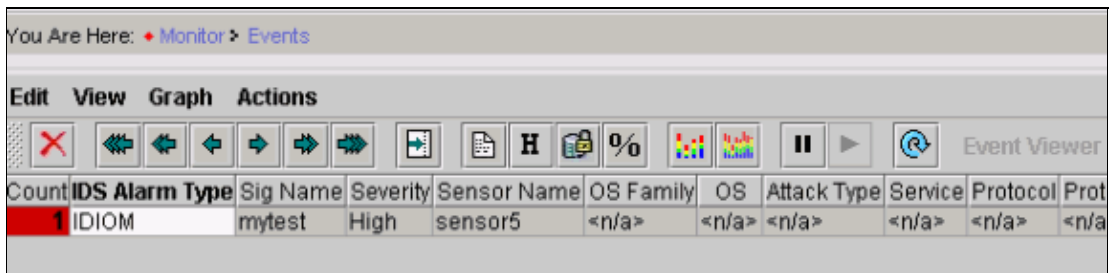
```
house#show access-list
Extended IP access list IDS_Ethernet1_in_1
10 permit ip host 10.66.79.195 any
```

```
!--- You will see a temporary entry has been added to
!--- the access list to block the router from which you connected via Telnet previous
```

```
20 deny ip host 100.100.100.2 any (37 matches)
```

30 permit ip any any

6. From the Event Viewer, click **Query Database** for new events now to view the alert for the previously launched attack.

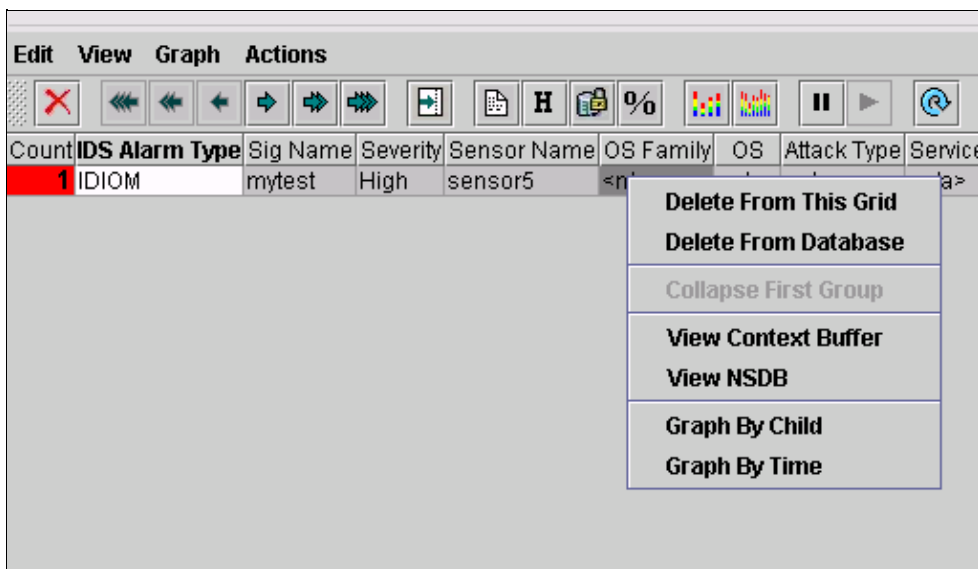


The screenshot shows the 'Event Viewer' window with a toolbar and a table of events. The toolbar includes icons for edit, view, graph, and actions. The table has columns for Count, IDS Alarm Type, Sig Name, Severity, Sensor Name, OS Family, OS, Attack Type, Service, Protocol, and Prot. The first row is highlighted in red and contains the following data:

Count	IDS Alarm Type	Sig Name	Severity	Sensor Name	OS Family	OS	Attack Type	Service	Protocol	Prot
1	IDIOM	mytest	High	sensor5	<n/a>	<n/a>	<n/a>	<n/a>	<n/a>	<n/a>

7. In the Event Viewer, highlight and right-click the alarm, then select **View Context Buffer** or **View NSDB** to view more detailed information about the alarm.

Note: The NSDB is also available online at the Cisco Secure Encyclopedia (registered customers only).



The screenshot shows the same Event Viewer window as above, but with a context menu open over the first row of the table. The menu options are:

- Delete From This Grid
- Delete From Database
- Collapse First Group
- View Context Buffer
- View NSDB
- Graph By Child
- Graph By Time

Troubleshoot

Troubleshooting Procedure

Use the following procedure for troubleshooting purposes.

1. In the IDS MC, select **Reports > Generate**.

Depending on the problem type, further detail should be found in one of the seven available reports.

Report Group: Audit Log		
Showing 1-7 of 7 records		
Available Reports ▾		
1.	<input type="radio"/>	Subsystem Report
2.	<input type="radio"/>	Sensor Version Import Report
3.	<input type="radio"/>	Sensor Configuration Import Report
4.	<input checked="" type="radio"/>	Sensor Configuration Deployment Report
5.	<input type="radio"/>	IDS Sensor Versions
6.	<input type="radio"/>	Console Notification Report
7.	<input type="radio"/>	Audit Log Report

Rows per page: << Page 1 >>

- At the Sensor console, enter the command **show statistics networkaccess** and check the output to ensure the "state" is active.

```

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#

```

- Ensure the communication parameter shows that the correct protocol is being used, such as Telnet or Secure Shell (SSH) with 3DES.

You can try a manual SSH or Telnet from an SSH/Telnet client on a PC to check username and password credentials are correct. You can then try Telnet or SSH from the Sensor itself, to the router, to ensure you are able to login successfully.

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.

Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco Secure Intrusion Detection Support Page](#)
 - [CiscoWorks VPN/Security Management Solution Support](#)
 - [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: Jan 19, 2006

Document ID: 46743
