Cisco 300-207 Exam Questions & Answers

Number: 300-207
Passing Score: 800
Time Limit: 120 min
File Version: 32.8

Exam Code: 300-207

Exam Name: Implementing Cisco Threat Control Solutions

Certkey

QUESTION 1
During initial configuration, the Cisco ASA can be configured to drop all traffic if the ASA CX SSP fails by using which command in a policy-map?

A. cxsc fail
B. cxsc fail-close
C. cxsc fail-open
D. cxssp fail-close

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A network engineer may use which three types of certificates when implementing HTTPS decryption services on the ASA CX? (Choose three.)

A. Self Signed Server Certificate
B. Self Signed Root Certificate
C. Microsoft CA Server Certificate
D. Microsoft CA Subordinate Root Certificate
E. LDAP CA Server Certificate
F. LDAP CA Root Certificate
G. Public Certificate Authority Server Certificate
H. Public Certificate Authority Root Certificate

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Cisco's ASA CX includes which two URL categories? (Choose two.)

A. Proxy Avoidance
B. Dropbox
C. Hate Speech
D. Facebook
E. Social Networking
F. Instant Messaging and Video Messaging

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A Cisco Web Security Appliance's policy can provide visibility and control of which two elements? (Choose two.)

A. Voice and Video Applications
B. Websites with a reputation between -100 and -60
C. Secure websites with certificates signed under an unknown CA
D. High bandwidth websites during business hours

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
What is the default antispam policy for positively identified messages?

A. Drop
B. Deliver and Append with [SPAM]
C. Deliver and Prepend with [SPAM]
D. Deliver and Alternate Mailbox

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What is the default CX Management 0/0 IP address on a Cisco ASA 5512-X appliance?

A. 192.168.1.1
B. 192.168.1.2
C. 192.168.1.3
D. 192.168.1.4
E. 192.168.1.5
F. 192.168.8.8

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
An ASA with an IPS module must be configured to drop traffic matching IPS signatures and block all traffic if the module fails. Which describes the correct configuration?

A. Inline Mode, Permit Traffic
B. Inline Mode, Close Traffic

C. Promiscuous Mode, Permit Traffic
D. Promiscuous Mode, Close Traffic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
When learning accept mode is set to auto, and the action is set to rotate, when is the KB created and used?

A. It is created every 24 hours and used for 24 hours.
B. It is created every 24 hours, but the current KB is used.
C. It is created every 1 hour and used for 24 hours.
D. A KB is created only in manual mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which port is used for CLI Secure shell access?

A. Port 23
B. Port 25
C. Port 22
D. Port 443

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which Cisco technology combats viruses and malware with virus outbreak filters that are downloaded from Cisco SenderBase?

A. ASA
B. WSA
C. Secure mobile access
D. IronPort ESA
E. SBA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which four statements are correct regarding management access to a Cisco Intrusion Prevention System? (Choose four.)

A. The Telnet protocol is enabled by default
B. The Telnet protocol is disabled by default
C. HTTP is enabled by default
D. HTTP is disabled by default
E. SSH is enabled by default
F. SSH is disabled by default
G. HTTPS is enabled by default
H. HTTPS is disabled by default

Correct Answer: BDEG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which two GUI options display users' activity in Cisco Web Security Appliance? (Choose two.)

A. Web Security Manager Identity Identity Name
B. Security Services Reporting
C. Reporting Users
D. Reporting Reports by User Location

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
The security team needs to limit the number of e-mails they receive from the Intellishield Alert Service. Which three parameters can they adjust to restrict alerts to specific product sets? (Choose three.)

A. Vendor
B. Chassis/Module
C. Device ID
D. Service Contract
E. Version/Release
F. Service Pack/Platform

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
With Cisco IDM, which rate limit option specifies the maximum bandwidth for rate-limited traffic?

A. protocol
B. rate
C. bandwidth
D. limit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which Cisco Security IntelliShield Alert Manager Service component mitigates new botnet, phishing, and web-based threats?

A. the IntelliShield Threat Outbreak Alert
B. IntelliShield Alert Manager vulnerability alerts
C. the IntelliShield Alert Manager historical database
D. the IntelliShield Alert Manager web portal
E. the IntelliShield Alert Manager back-end intelligence engine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which set of commands changes the FTP client timeout when the sensor is communicating with an FTP server?

A.
```
sensor# configure terminal
sensor(config)# service sensor
sensor(config-hos)# network-settings
sensor(config-hos-net)# ftp-timeout 500
```

B.
```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings parameter ftp sensor(config-hos-net)# ftp-timeout 500
```

C.
```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# ftp-timeout 500
```

D.
```
sensor# configure terminal
sensor(config)# service network
sensor(config-hos)# network-settings
sensor(config-hos-net)# ftp-timeout 500
```

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
What are the initial actions that can be performed on an incoming SMTP session by the workqueue of a Cisco Email Security Appliance?

A. Accept, Reject, Relay, TCPRefuse
B. LDAP Verification, Envelope Sender Verification, Bounce Verification, Alias Table Verification
C. Recipient Access Table Verification, Host DNS Verification, Masquerading, Spam Payload Check
D. SMTP Authentication, SBRS Verification, Sendergroup matching, DNS host verification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
During initial configuration, the Cisco ASA can be configured to drop all traffic if the ASA CX SSP fails by using which command in a policy-map?

A. cxsc fail
B. cxsc fail-close
C. cxsc fail-open
D. cxssp fail-close

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which three options are IPS signature classifications? (Choose three.)

A. tuned signatures
B. response signatures
C. default signatures
D. custom signatures
E. preloaded signatures
F. designated signatures

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

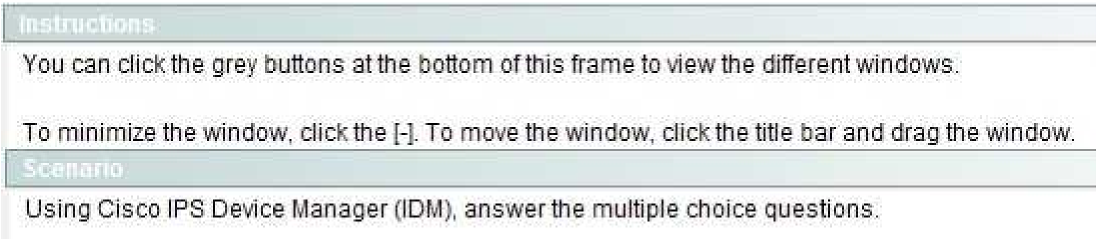
QUESTION 20
At which value do custom signatures begin?

A. 1024
B. 10000
C. 1
D. 60000

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21



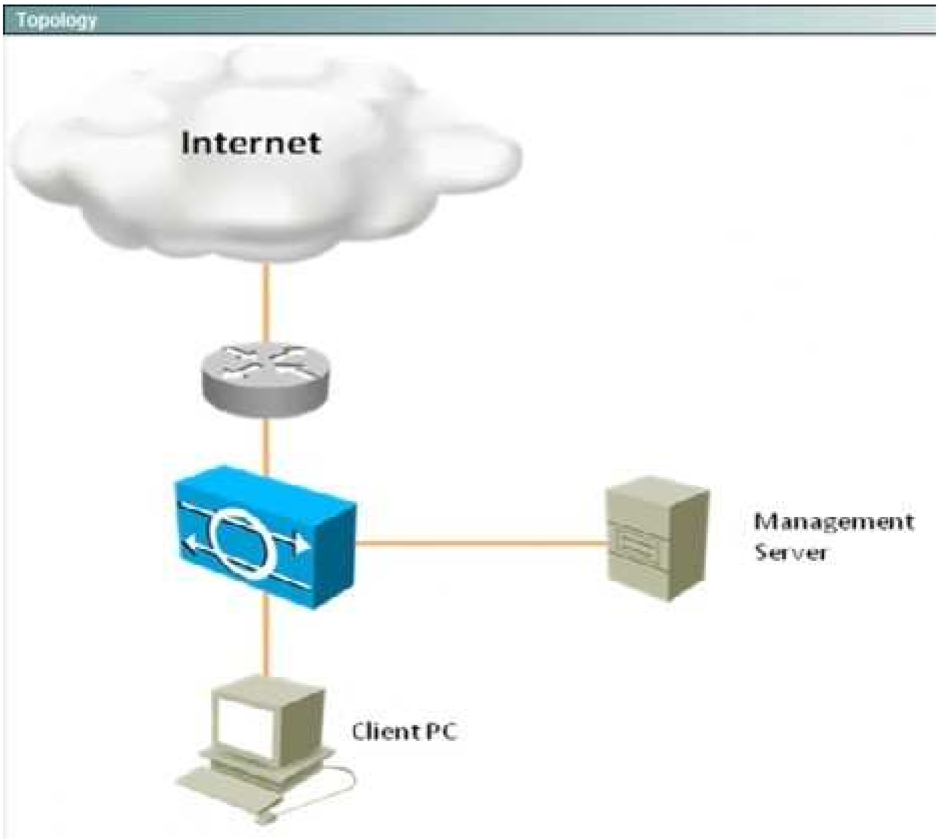
Instructions

You can click the grey buttons at the bottom of this frame to view the different windows.

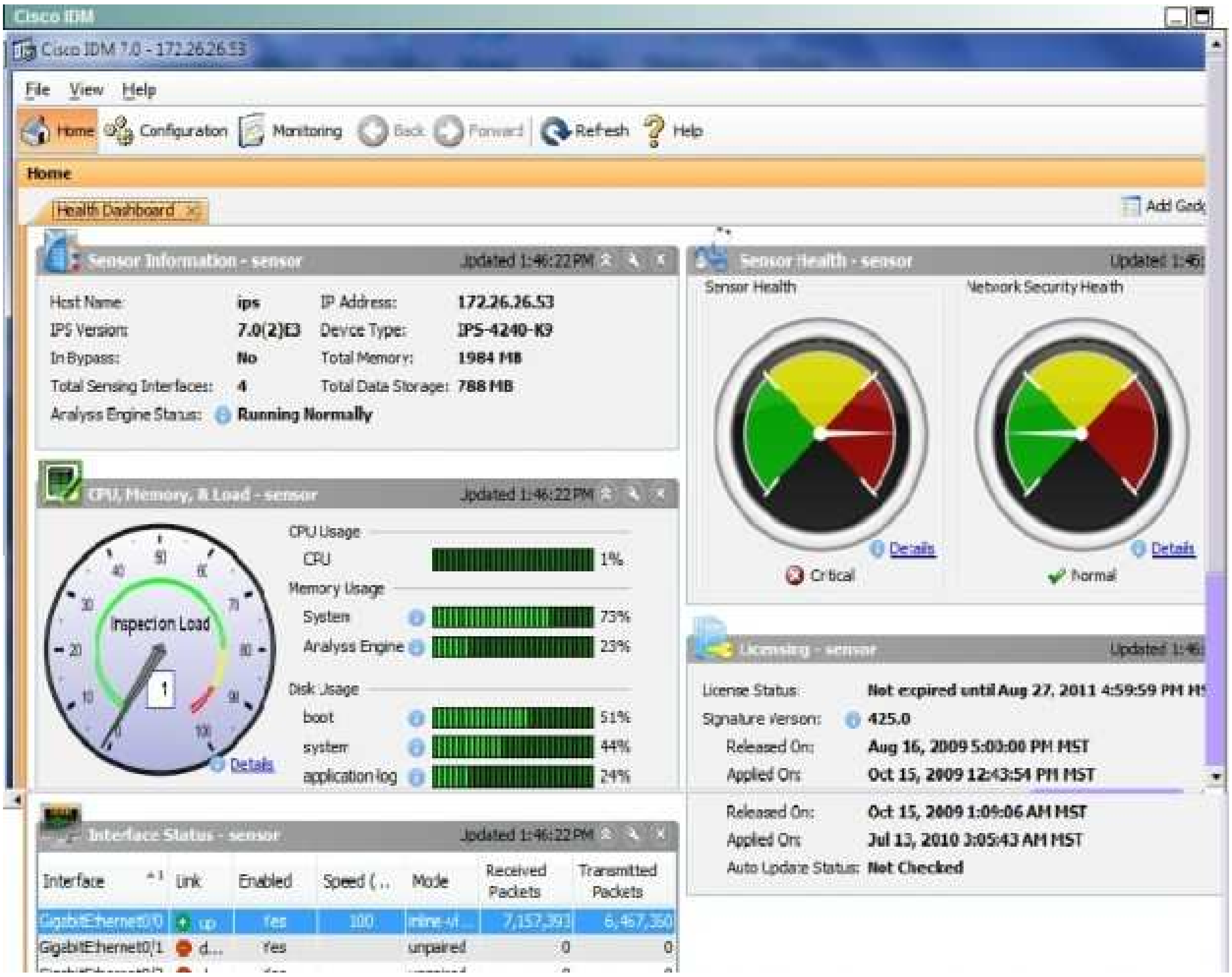
To minimize the window, click the [-]. To move the window, click the title bar and drag the window.

Scenario

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.



Topology



Sensor Information - sensor Updated 1:46:22 PM

Host Name:	ips	IP Address:	172.26.26.53
IPS Version:	7.0(2)E3	Device Type:	IPS-4240-K9
In Bypass:	No	Total Memory:	1984 MB
Total Sensing Interfaces:	4	Total Data Storage:	788 MB
Analysis Engine Status:	Running Normally		

Sensor Health - sensor Updated 1:46:

CPU, Memory, & Load - sensor Updated 1:46:22 PM

CPU Usage	
CPU	1%
Memory Usage	
System	73%
Analysis Engine	23%
Disk Usage	
boot	51%
system	44%
application log	24%

Licensing - sensor Updated 1:46:

License Status:	Not expired until Aug 27, 2011 4:59:59 PM M
Signature Version:	425.0
Released On:	Aug 16, 2009 5:00:00 PM MST
Applied On:	Oct 15, 2009 12:43:54 PM MST
Released On:	Oct 15, 2009 1:09:06 AM MST
Applied On:	Jul 13, 2010 3:05:43 AM MST
Auto Update Status:	Not Checked

Interface Status - sensor Updated 1:46:22 PM

Interface	Link	Enabled	Speed (...	Mode	Received Packets	Transmitted Packets
GigabitEthernet0/0	up	Yes	100	inline-vl...	7,157,393	6,467,360
GigabitEthernet0/1	d...	Yes		unpaired	0	0

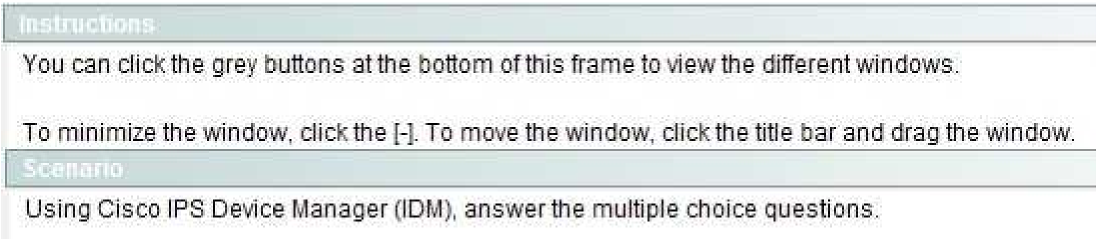
Which signature definition is virtual sensor 0 assigned to use?

A. rules0
B. vs0
C. sig0
D. ad0
E. ad1
F. sigl

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is the default signature.
You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies.

QUESTION 22



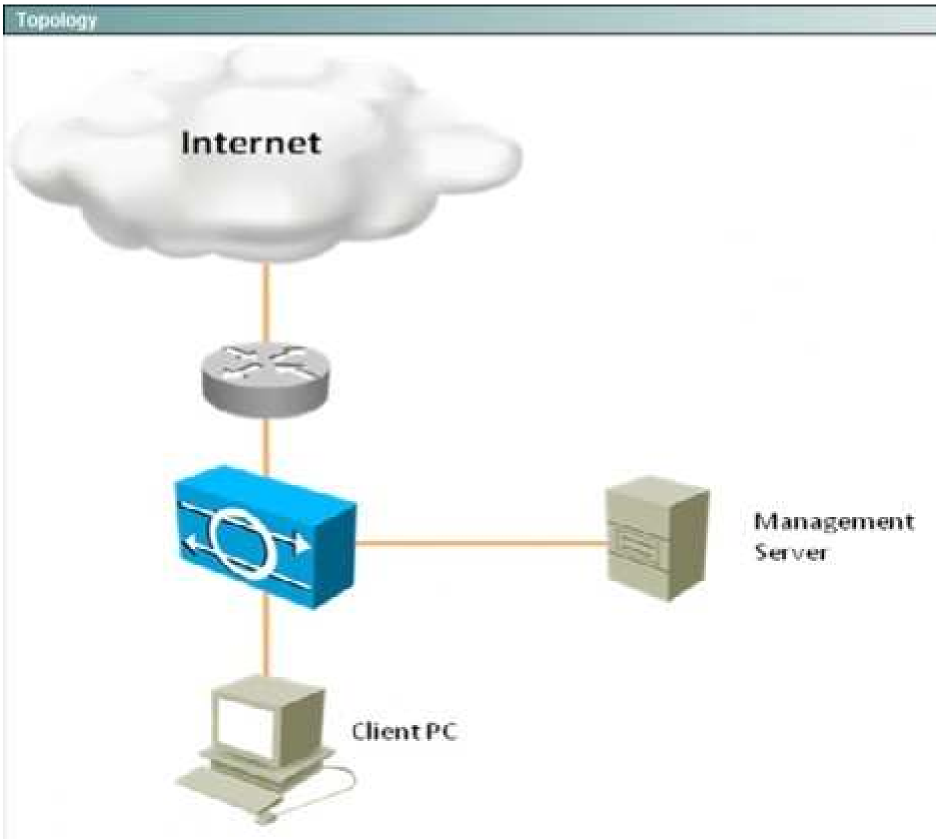
Instructions

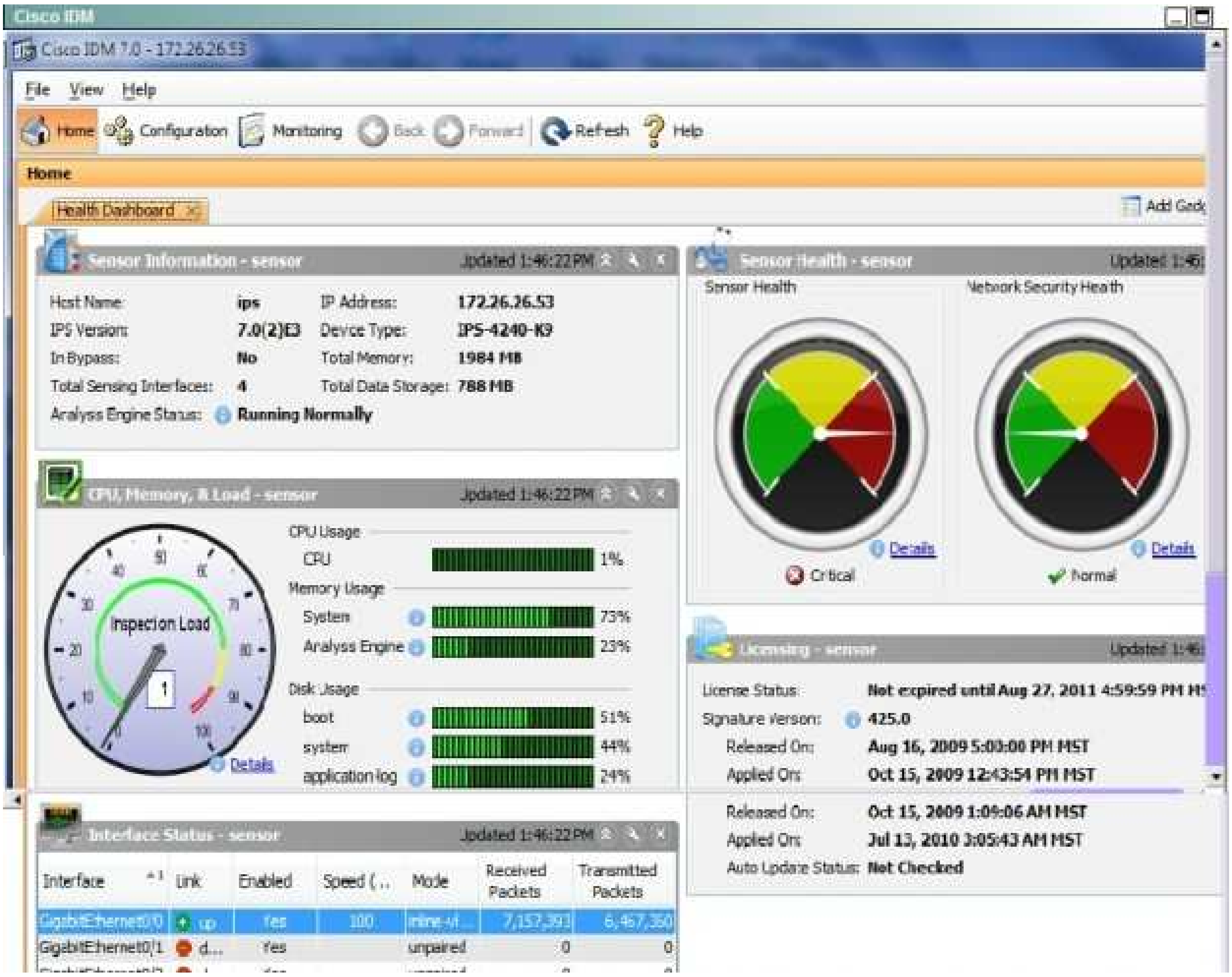
You can click the grey buttons at the bottom of this frame to view the different windows.

To minimize the window, click the [-]. To move the window, click the title bar and drag the window.

Scenario

Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.





Sensor Information - sensor Updated 1:46:22 PM

Host Name: ips
IP Address: 172.26.26.53
IPS Version: 7.0(2)E3
Device Type: IPS-4240-K9
In Bypass: No
Total Memory: 1984 MB
Total Sensing Interfaces: 4
Total Data Storage: 788 MB
Analysis Engine Status: Running Normally

Sensor Health - sensor Updated 1:46

Sensor Health: Critical
Network Security Health: Normal

CPU, Memory, & Load - sensor Updated 1:46:22 PM

Inspection Load: 1

CPU Usage
CPU 1%

Memory Usage
System 73%
Analysis Engine 23%

Disk Usage
boot 51%
system 44%
application-log 24%

Licensing - sensor Updated 1:46

License Status: Not expired until Aug 27, 2011 4:59:59 PM MS
Signature Version: 425.0
Released On: Aug 16, 2009 5:00:00 PM MST
Applied On: Oct 15, 2009 12:43:54 PM MST
Released On: Oct 15, 2009 1:09:06 AM MST
Applied On: Jul 13, 2010 3:05:43 AM MST
Auto Update Status: Not Checked

Interface Status - sensor Updated 1:46:22 PM

Interface	Link	Enabled	Speed (...	Mode	Received Packets	Transmitted Packets
GigabitEthernet0/0	up	Yes	100	inline-vl...	7,157,393	6,467,350
GigabitEthernet0/1	d...	Yes		unpaired	0	0

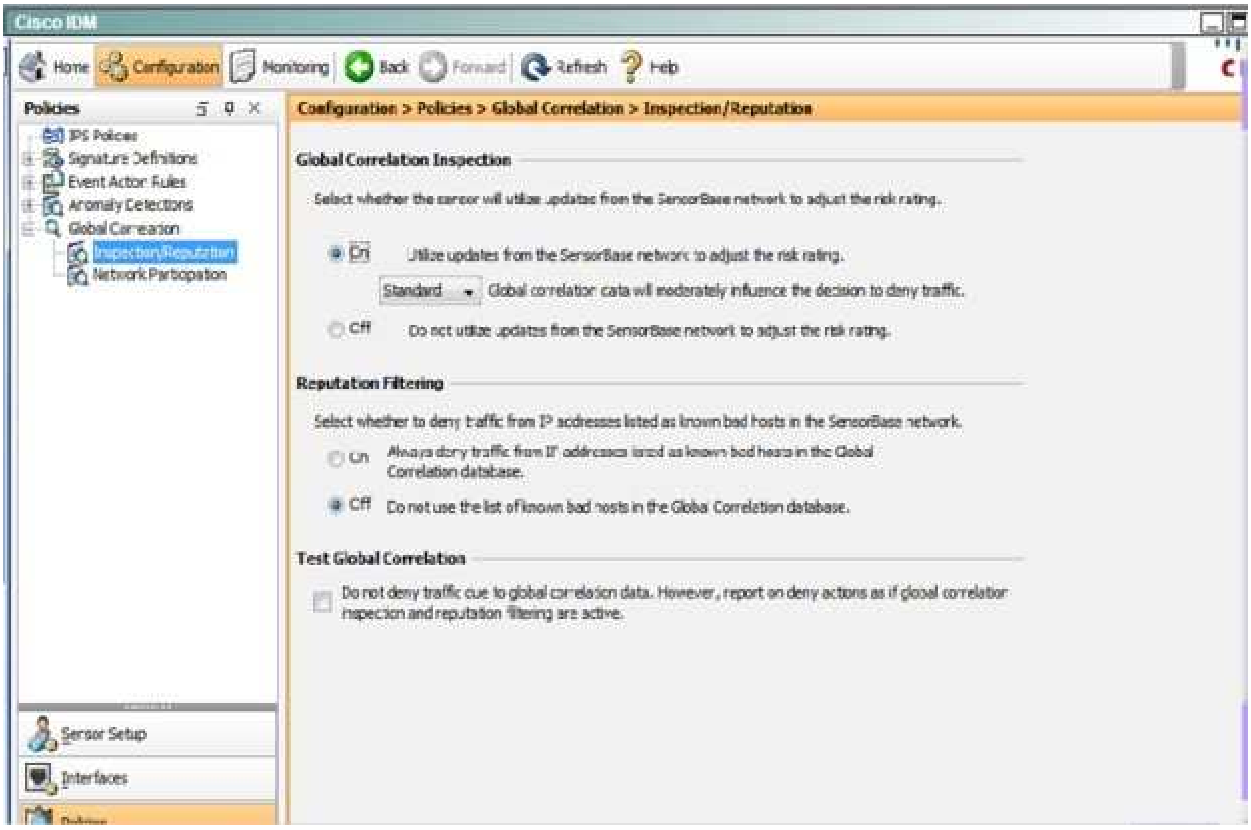
To what extent will the Cisco IPS sensor contribute data to the Cisco SensorBase network?

A. It will not contribute to the SensorBase network.
B. It will contribute to the SensorBase network, but will withhold some sensitive information
C. It will contribute the victim IP address and port to the SensorBase network.
D. It will not contribute to Risk Rating adjustments that use information from the SensorBase network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To configure network participation, follow these steps:
Step 1 Log in to IDM using an account with administrator privileges. Step 2 Choose Configuration > Policies > Global Correlation > Network Participation. Step 3 To turn on network participation, click the Partial or Full radio button:
·Partial--Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
·Full--All data is contributed to the SensorBase Network

In this case, we can see that this has been turned off as shown below:



Configuration > Policies > Global Correlation > Inspection/Reputation

Global Correlation Inspection

Select whether the sensor will utilize updates from the SensorBase network to adjust the risk rating.

● On Utilize updates from the SensorBase network to adjust the risk rating.

Standard ▾ Global correlation data will moderately influence the decision to deny traffic.

○ Off Do not utilize updates from the SensorBase network to adjust the risk rating.

Reputation Filtering

Select whether to deny traffic from IP addresses listed as known bad hosts in the SensorBase network.

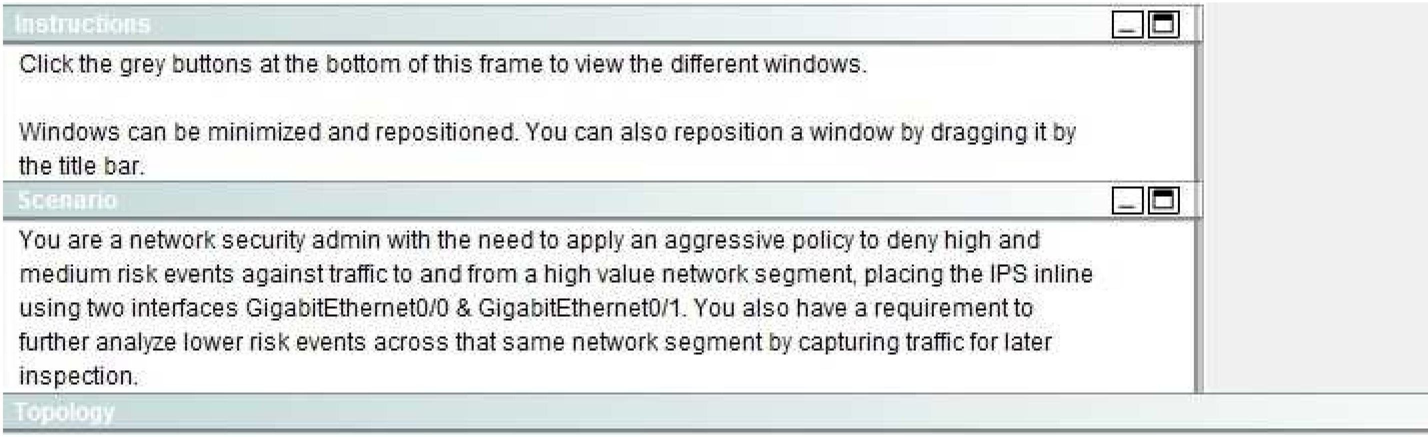
○ On Always deny traffic from IP addresses listed as known bad hosts in the Global Correlation database.

● Off Do not use the list of known bad hosts in the Global Correlation database.

Test Global Correlation

□ Do not deny traffic due to global correlation data. However, report on deny actions as if global correlation inspection and reputation filtering are active.

QUESTION 23



Instructions

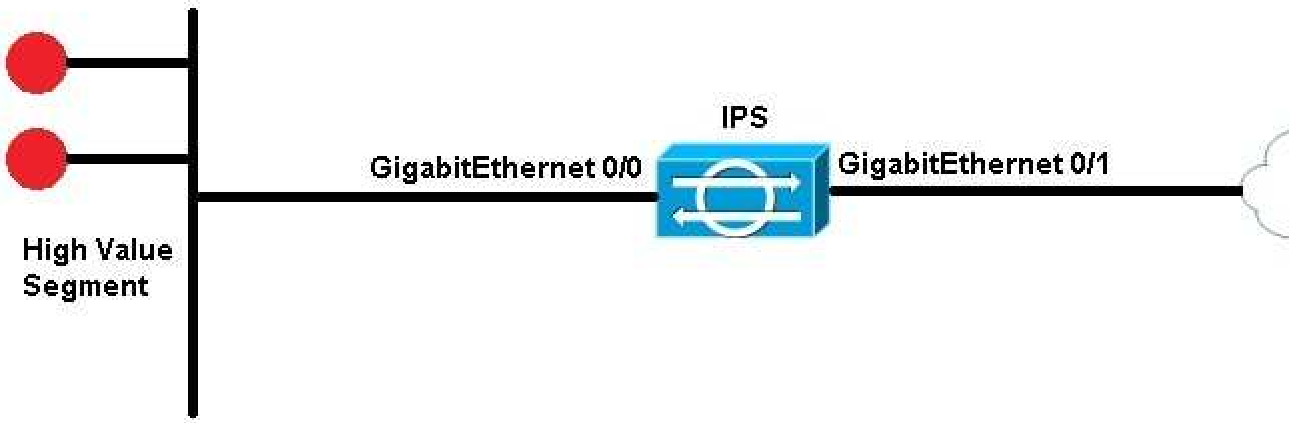
Click the grey buttons at the bottom of this frame to view the different windows.

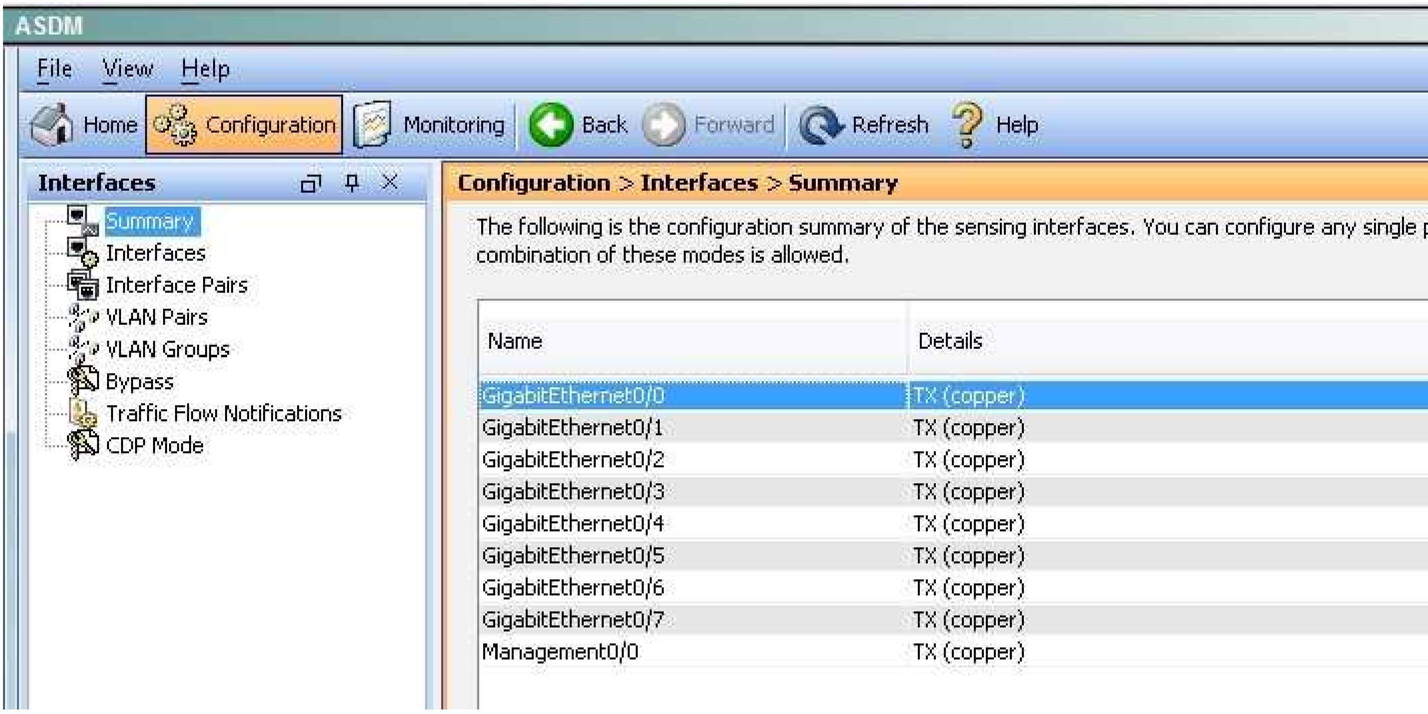
Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

Scenario

You are a network security admin with the need to apply an aggressive policy to deny high and medium risk events against traffic to and from a high value network segment, placing the IPS inline using two interfaces GigabitEthernet0/0 & GigabitEthernet0/1. You also have a requirement to further analyze lower risk events across that same network segment by capturing traffic for later inspection.

Topology





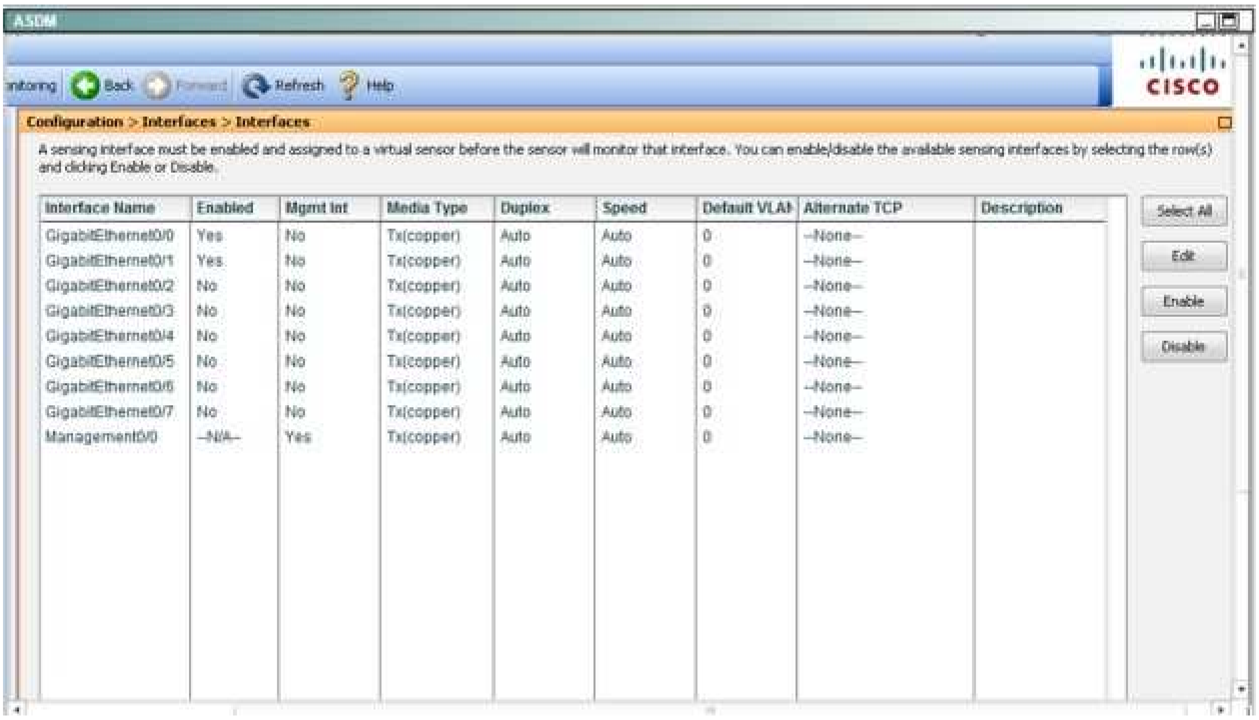
Configuration > Interfaces > Summary

The following is the configuration summary of the sensing interfaces. You can configure any single p
combination of these modes is allowed.

Name	Details
GigabitEthernet0/0	TX (copper)
GigabitEthernet0/1	TX (copper)
GigabitEthernet0/2	TX (copper)
GigabitEthernet0/3	TX (copper)
GigabitEthernet0/4	TX (copper)
GigabitEthernet0/5	TX (copper)
GigabitEthernet0/6	TX (copper)
GigabitEthernet0/7	TX (copper)
Management0/0	TX (copper)

Correct Answer: Steps are in Explanation below:
Section: (none)
Explanation

Explanation/Reference:
Explanation:
First, enable the Gig 0/0 and Gig 0/1 interfaces:

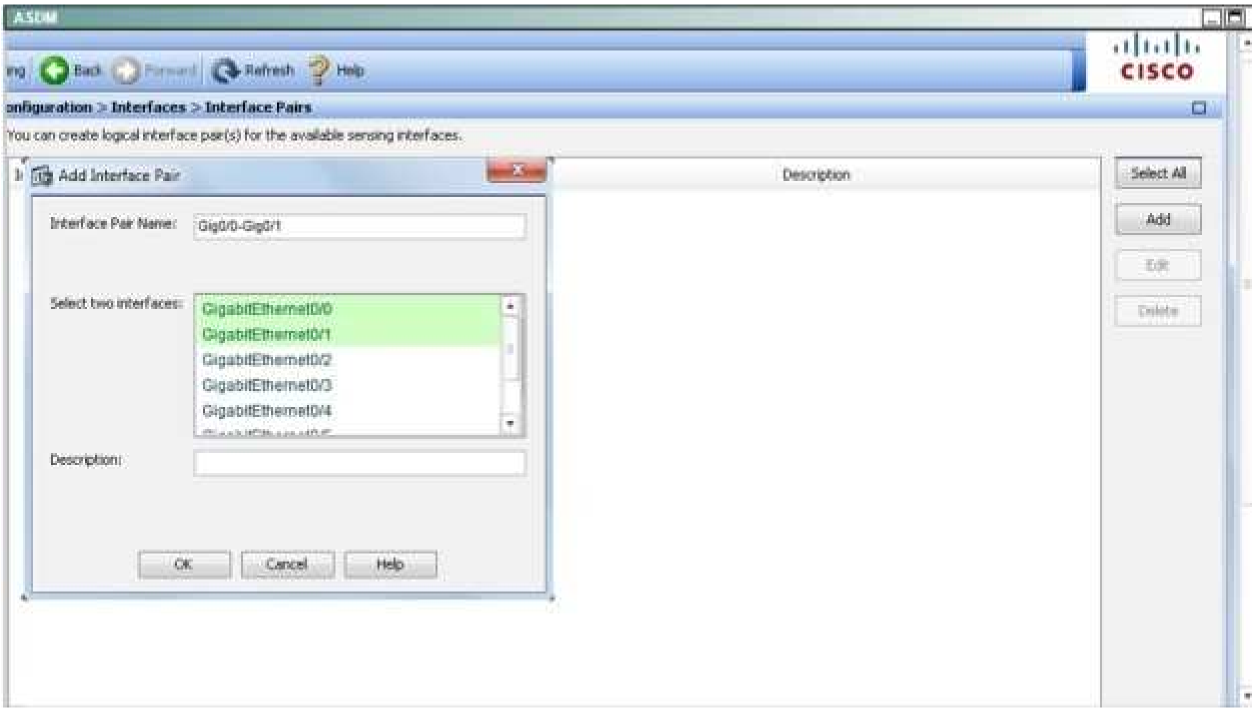


Configuration > Interfaces > Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Mgmt Int	Media Type	Duplex	Speed	Default VLAI	Alternate TCP	Description
GigabitEthernet0/0	Yes	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/1	Yes	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/2	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/3	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/4	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/5	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/6	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/7	No	No	Tx(copper)	Auto	Auto	0	--None--	
Management0/0	--N/A--	Yes	Tx(copper)	Auto	Auto	0	--None--	

Second, create the pair under the "interface pairs" tab:



Configuration > Interfaces > Interface Pairs

You can create logical interface pair(s) for the available sensing interfaces.

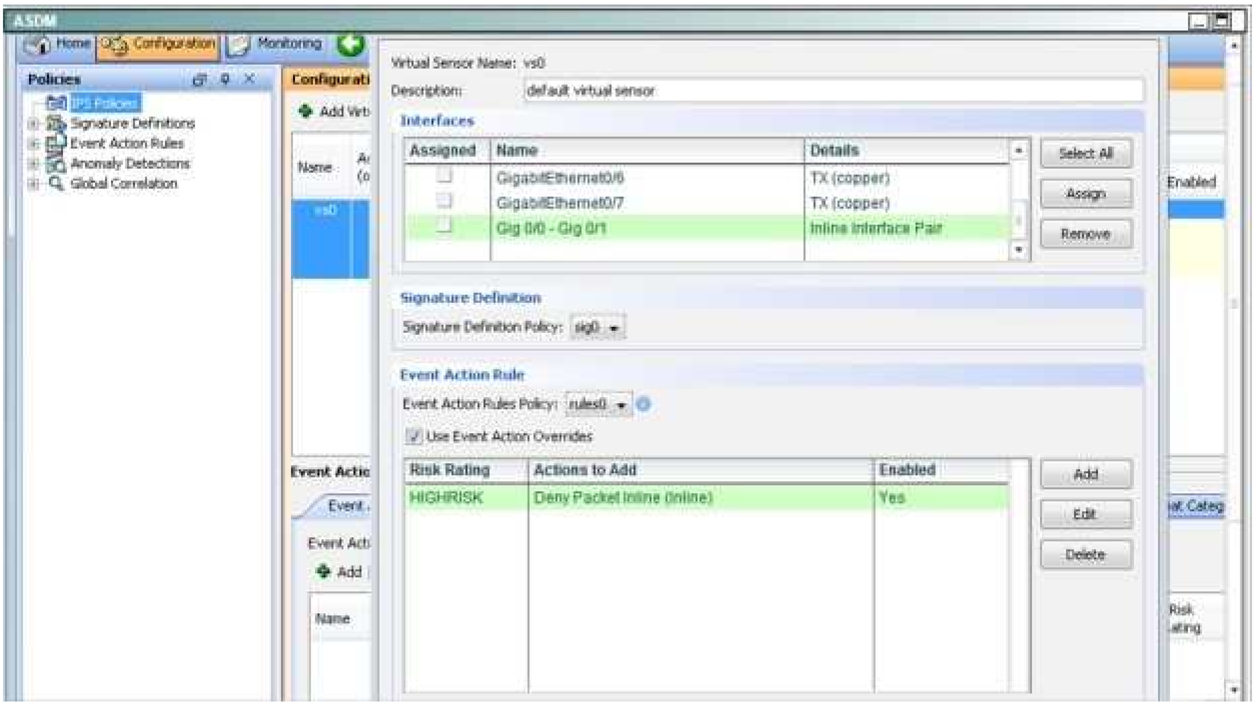
Add Interface Pair

Interface Pair Name: Gig0/0-Gig0/1

Select two interfaces:
- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2
- GigabitEthernet0/3
- GigabitEthernet0/4

Description:

Then, apply the HIGHRISK action rule to the newly created interface pair:



Virtual Sensor Name: vs0

Description: default virtual sensor

Interfaces

Assigned	Name	Details
□	GigabitEthernet0/6	TX (copper)
□	GigabitEthernet0/7	TX (copper)
□	Gig 0/0 - Gig 0/1	Inline Interface Pair

Signature Definition

Signature Definition Policy: sig0

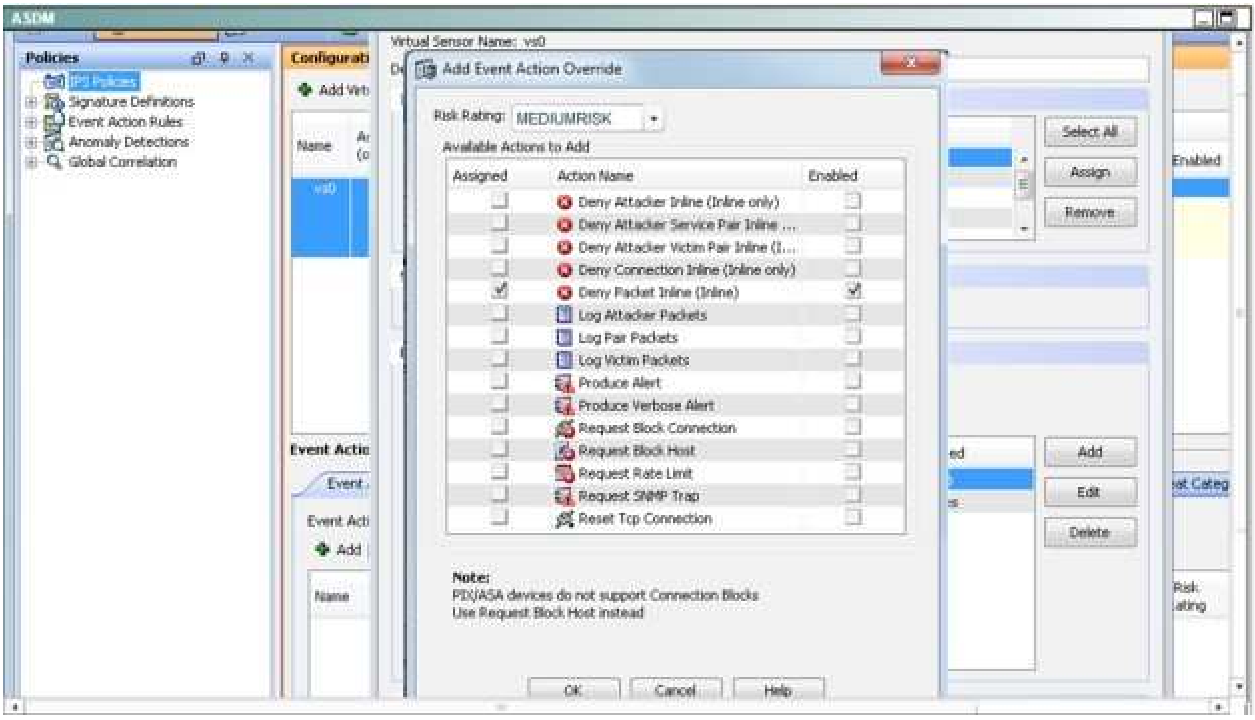
Event Action Rule

Event Action Rules Policy: rules0

☑ Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	Yes

Then apply the same for the MEDIUMRISK traffic (deny attacker inline)



Add Event Action Override

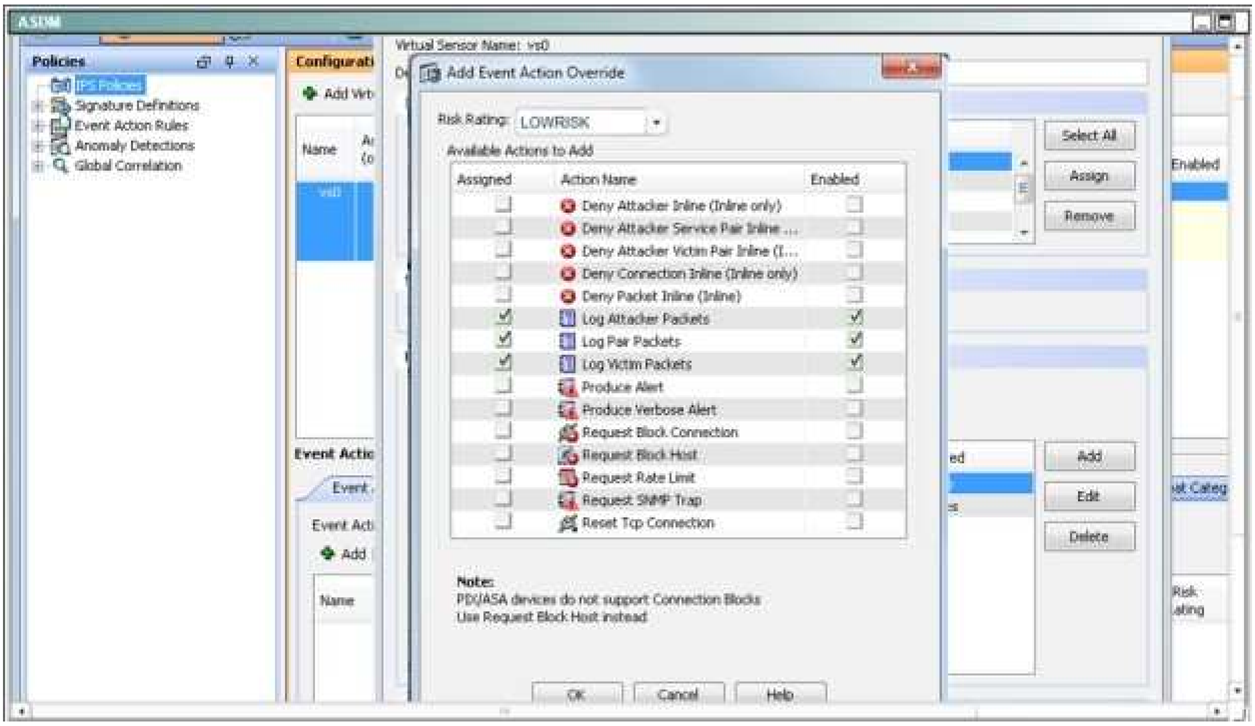
Risk Rating: MEDIUMRISK

Available Actions to Add

Assigned	Action Name	Enabled
☐	Deny Attacker Inline (Inline only)	☐
☐	Deny Attacker Service Pair Inline ...	☐
☐	Deny Attacker Victim Pair Inline (I...	☐
☐	Deny Connection Inline (Inline only)	☐
☑	Deny Packet Inline (Inline)	☑
☐	Log Attacker Packets	☐
☐	Log Pair Packets	☐
☐	Log Victim Packets	☐
☐	Produce Alert	☐
☐	Produce Verbose Alert	☐
☐	Request Block Connection	☐
☐	Request Block Host	☐
☐	Request Rate Limit	☐
☐	Request SNMP Trap	☐
☐	Reset Tcp Connection	☐

Note:
PIX/ASA devices do not support Connection Blocks
Use Request Block Host instead

Finally. Log the packets for the LOWRICK event:



Add Event Action Override

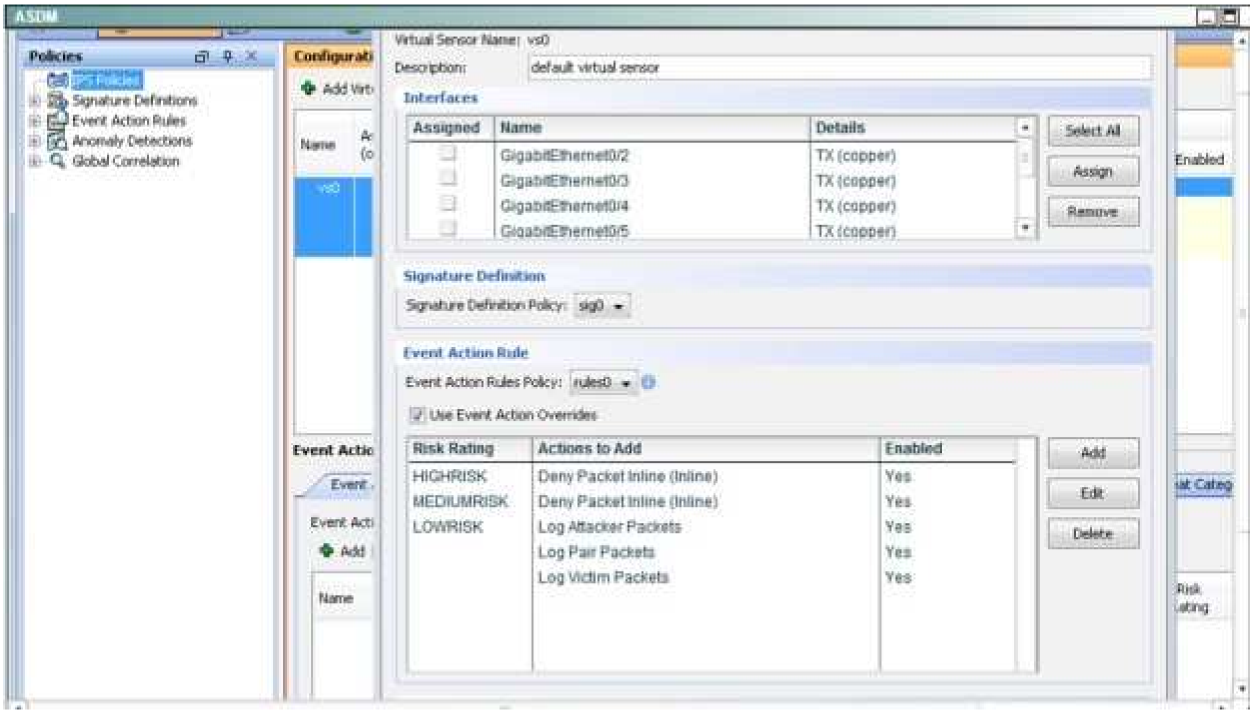
Risk Rating: LOWRISK

Available Actions to Add

Assigned	Action Name	Enabled
☐	Deny Attacker Inline (Inline only)	☐
☐	Deny Attacker Service Pair Inline ...	☐
☐	Deny Attacker Victim Pair Inline (I...	☐
☐	Deny Connection Inline (Inline only)	☐
☐	Deny Packet Inline (Inline)	☐
☑	Log Attacker Packets	☑
☑	Log Pair Packets	☑
☑	Log Victim Packets	☑
☐	Produce Alert	☐
☐	Produce Verbose Alert	☐
☐	Request Block Connection	☐
☐	Request Block Host	☐
☐	Request Rate Limit	☐
☐	Request SNMP Trap	☐
☐	Reset Tcp Connection	☐

Note:
PIX/ASA devices do not support Connection Blocks
Use Request Block Host instead

When done it should look like this:



Virtual Sensor Name: vs0

Description: default virtual sensor

Interfaces

Assigned	Name	Details
□	GigabitEthernet0/2	TX (copper)
□	GigabitEthernet0/3	TX (copper)
□	GigabitEthernet0/4	TX (copper)
□	GigabitEthernet0/5	TX (copper)

Signature Definition

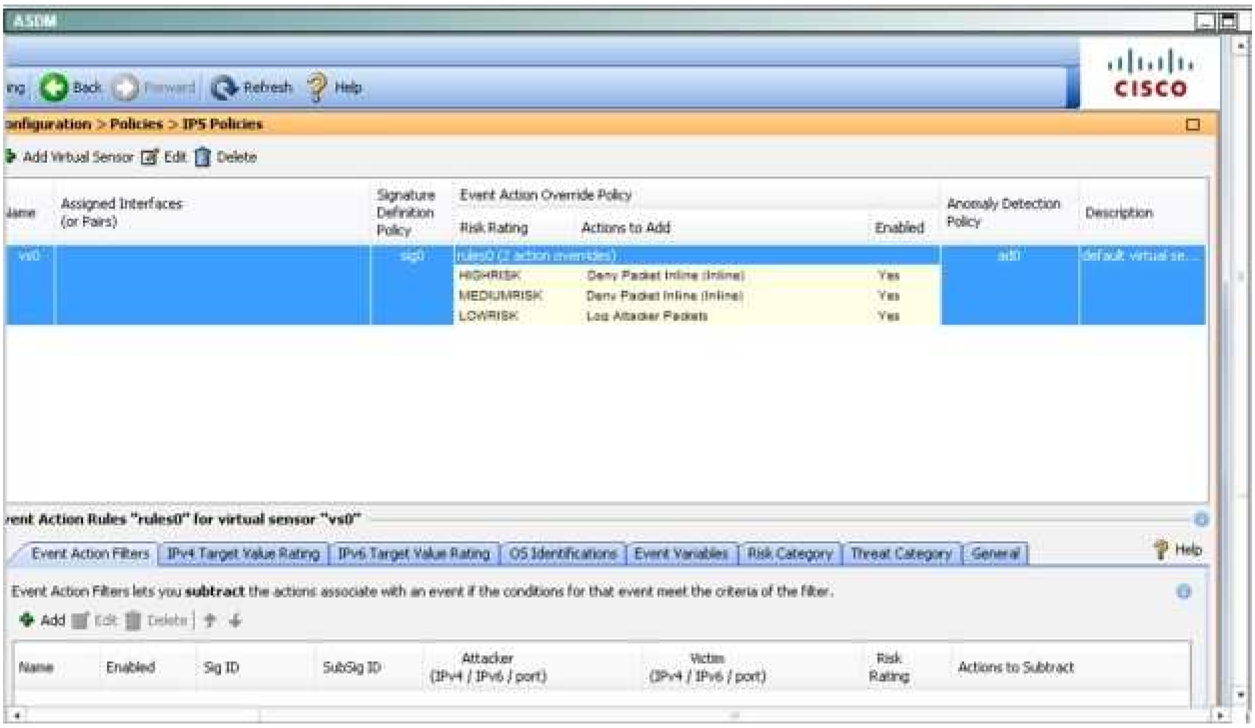
Signature Definition Policy: sig0

Event Action Rule

Event Action Rules Policy: rules0

☑ Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	Yes
MEDIUMRISK	Deny Packet Inline (Inline)	Yes
LOWRISK	Log Attacker Packets	Yes
	Log Pair Packets	Yes
	Log Victim Packets	Yes



onfiguration > Policies > IPS Policies

lame	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Description
			Risk Rating	Actions to Add	Enabled		
vs0		sig0	rules0 (2 action overrides)			ad0	default virtual se...
			HIGHRISK	Deny Packet Inline (Inline)	Yes		
			MEDIUMRISK	Deny Packet Inline (Inline)	Yes		
			LOWRISK	Log Attacker Packets	Yes		

vent Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters | IPv4 Target Value Rating | IPv6 Target Value Rating | OS Identifications | Event Variables | Risk Category | Threat Category | General

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)	Victim (IPv4 / IPv6 / port)	Risk Rating	Actions to Subtract