

Cisco 300-207



Implementing Cisco Threat Control Solutions

Version: 4.0

QUESTION NO: 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

Answer: B

Explanation:

QUESTION NO: 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

Answer: B,D,F

Explanation:

QUESTION NO: 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

Answer: C,E

Explanation:

QUESTION NO: 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

Answer: C,D

Explanation:

QUESTION NO: 5

Which Cisco Web Security Appliance design requires minimal change to endpoint devices?

- A. Transparent Mode
- B. Explicit Forward Mode
- C. Promiscuous Mode
- D. Inline Mode

Answer: A

Explanation:

QUESTION NO: 6

What step is required to enable HTTPS Proxy on the Cisco Web Security Appliance?

- A. Web Security Manager HTTPS Proxy click Enable
- B. Security Services HTTPS Proxy click Enable
- C. HTTPS Proxy is enabled by default
- D. System Administration HTTPS Proxy click Enable

Answer: B

Explanation:

QUESTION NO: 7

Which two statements about Cisco Cloud Web Security functionality are true? (Choose two.)

- A. It integrates with Cisco Integrated Service Routers.
- B. It supports threat avoidance and threat remediation.
- C. It extends web security to the desktop, laptop, and PDA.
- D. It integrates with Cisco ASA Firewalls.

Answer: A,D

Explanation:

QUESTION NO: 8

Which Cisco Cloud Web Security tool provides URL categorization?

- A. Cisco Dynamic Content Analysis Engine
- B. Cisco ScanSafe
- C. ASA Firewall Proxy
- D. Cisco Web Usage Control

Answer: D

Explanation:

QUESTION NO: 9

Which three functions can Cisco Application Visibility and Control perform? (Choose three.)

- A. Validation of malicious traffic
- B. Traffic control
- C. Extending Web Security to all computing devices
- D. Application-level classification
- E. Monitoring
- F. Signature tuning

Answer: B,D,E

Explanation:

QUESTION NO: 10

Which two options are features of the Cisco Email Security Appliance? (Choose two.)

- A. Cisco Anti-Replay Services
- B. Cisco Destination Routing
- C. Cisco Registered Envelope Service
- D. Cisco IronPort SenderBase Network

Answer: C,D

Explanation:

QUESTION NO: 11

What is the authentication method for an encryption envelope that is set to medium security?

- A. The recipient must always enter a password, even if credentials are cached.
- B. A password is required, but cached credentials are permitted.
- C. The recipient must acknowledge the sensitivity of the message before it opens.
- D. The recipient can open the message without authentication.

Answer: B

Explanation:

QUESTION NO: 12

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

Answer: C

Explanation:

QUESTION NO: 13

Which command establishes a virtual console session to a CX module within a Cisco Adaptive Security Appliance?

- A. session 1 ip address
- B. session 2 ip address
- C. session 1
- D. session ips console
- E. session cxsc console

Answer: E

Explanation:

QUESTION NO: 14

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

Answer: F

Explanation:

QUESTION NO: 15

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

Answer: B

Explanation:

QUESTION NO: 16

A new Cisco IPS device has been placed on the network without prior analysis. Which CLI command shows the most fired signature?

- A. Show statistics virtual-sensor
- B. Show event alert
- C. Show alert
- D. Show version

Answer: A

Explanation:

QUESTION NO: 17

What CLI command configures IP-based access to restrict GUI and CLI access to a Cisco Email Security appliance's administrative interface?

- A. adminaccessconfig
- B. sshconfig
- C. sslconfig
- D. ipaccessconfig

Answer: A

Explanation:

QUESTION NO: 18

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

Answer: B

Explanation:

QUESTION NO: 19

A new Cisco IPS device has been placed on the network without prior analysis. Which CLI command shows the most fired signature?

- A. Show statistics virtual-sensor
- B. Show event alert
- C. Show alert
- D. Show version

Answer: A

Explanation:

QUESTION NO: 20

Which three options are characteristics of router-based IPS? (Choose three.)

- A. It is used for large networks.
- B. It is used for small networks.
- C. It supports virtual sensors.
- D. It supports multiple VRFs.
- E. It uses configurable anomaly detection.
- F. Signature definition files have been deprecated.

Answer: B,D,F

Explanation:

QUESTION NO: 21

What are three best practices for a Cisco Intrusion Prevention System? (Choose three.)

- A. Checking for new signatures every 4 hours
- B. Checking for new signatures on a staggered schedule
- C. Automatically updating signature packs
- D. Manually updating signature packs

- E. Group tuning of signatures
- F. Single tuning of signatures

Answer: B,C,E

Explanation:

QUESTION NO: 22

Who or what calculates the signature fidelity rating?

- A. the signature author
- B. Cisco Professional Services
- C. the administrator
- D. the security policy

Answer: A

Explanation:

QUESTION NO: 23

Which three zones are used for anomaly detection? (Choose three.)

- A. Internal zone
- B. External zone
- C. Illegal zone
- D. Inside zone
- E. Outside zone
- F. DMZ zone

Answer: A,B,C

Explanation:

QUESTION NO: 24

What is the default IP range of the external zone?

- A. 0.0.0.0 0.0.0.0
- B. 0.0.0.0 - 255.255.255.255

- C. 0.0.0.0/8
- D. The network of the management interface

Answer: B

Explanation:

QUESTION NO: 25

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.

Answer: A

Explanation:

QUESTION NO: 26

What is the CLI command to create a new Message Filter in a Cisco Email Security Appliance?

- A. filterconfig
- B. filters new
- C. messagefilters
- D. policyconfig-- inbound or outbound-- filters

Answer: B

Explanation:

QUESTION NO: 27

A Cisco Email Security Appliance uses which message filter to drop all executable attachments entering and leaving the Cisco Email Security Appliance?

- A. drop-exe: if (attachment-filename == "\\.\exe\$") OR (attachment-filetype == "exe") { drop(); }
- B. drop-exe: if (recv-listener == "InboundMail") AND ((attachment-filename == "\\.\exe\$") OR

(attachment-filetype == "exe")) { drop(); }

C. drop-exe! if (attachment-filename == "\\.\exe\$") OR (attachment-filetype == "exe") { drop(); }

D. drop-exe! if (recv-listener == "InboundMail") AND ((attachment-filename == "\\.\exe\$") OR (attachment-filetype == "exe")) { drop(); }

Answer: A

Explanation:

QUESTION NO: 28

What can Cisco Prime Security Manager (PRSM) be used to achieve?

A. Configure and Monitor Cisco CX Application Visibility and Control, web filtering, access and decryption policies

B. Configure Cisco ASA connection limits

C. Configure TCP state bypass in Cisco ASA and IOS

D. Configure Cisco IPS signature and monitor signature alerts

E. Cisco Cloud Security on Cisco ASA

Answer: A

Explanation:

QUESTION NO: 29

Which is the default IP address and admin port setting for https in the Cisco Web Security Appliance?

A. http://192.168.42.42:8080

B. http://192.168.42.42:80

C. https://192.168.42.42:443

D. https://192.168.42.42:8443

Answer: D

Explanation:

QUESTION NO: 30

Which port is used for CLI Secure shell access?

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

Answer: C

Explanation:

QUESTION NO: 31

Which Cisco technology prevents targeted malware attacks, provides data loss prevention and spam protection, and encrypts email?

- A. SBA
- B. secure mobile access
- C. IPv6 DMZ web service
- D. ESA

Answer: D

Explanation:

QUESTION NO: 32

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

Answer: D

Explanation:

QUESTION NO: 33

Which Cisco WSA is intended for deployment in organizations of up to 1500 users?

- A. WSA S370
- B. WSA S670
- C. WSA S370-2RU
- D. WSA S170

Answer: D

Explanation:

QUESTION NO: 34

Which Cisco WSA is intended for deployment in organizations of more than 6000 users?

- A. WSA S370
- B. WSA S670
- C. WSA S370-2RU
- D. WSA S170

Answer: B

Explanation:

QUESTION NO: 35

Which command verifies that the correct CWS license key information was entered on the Cisco ASA?

- A. sh run scansafe server
- B. sh run scansafe
- C. sh run server
- D. sh run server scansafe

Answer: B

Explanation:

QUESTION NO: 36

Which five system management protocols are supported by the Cisco Intrusion Prevention System? (Choose five.)

- A. SNMPv2c
- B. SNMPv1
- C. SNMPv2
- D. SNMPv3
- E. Syslog
- F. SDEE
- G. SMTP

Answer: A,B,C,F,G

Explanation:

QUESTION NO: 37

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

Answer: B,D,E,G

Explanation:

QUESTION NO: 38

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

Answer: C,D

Explanation:

QUESTION NO: 39

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

Answer: A,E,F

Explanation:

QUESTION NO: 40

What three alert notification options are available in Cisco IntelliShield Alert Manager? (Choose three.)

- A. Alert Summary as Text
- B. Complete Alert as an HTML Attachment
- C. Complete Alert as HTML
- D. Complete Alert as RSS
- E. Alert Summary as Plain Text
- F. Alert Summary as MMS

Answer: A,B,C

Explanation:

QUESTION NO: 41

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

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

Answer: B

Explanation:

QUESTION NO: 42

Which two benefits are provided by the dynamic dashboard in Cisco ASDM Version 5.2? (Choose two.)

- A. It configures system polices for NAC devices.
- B. It forwards traffic to destination devices.
- C. It provides statistics for device health.
- D. It replaces syslog, RADIUS, and TACACS+ servers.
- E. It automatically detects Cisco security appliances to configure.

Answer: C,E

Explanation:

QUESTION NO: 43

Which Cisco monitoring solution displays information and important statistics for the security devices in a network?

- A. Cisco Prime LAN Management
- B. Cisco ASDM Version 5.2
- C. Cisco Threat Defense Solution
- D. Syslog Server
- E. TACACS+

Answer: B

Explanation:

QUESTION NO: 44

Which three search parameters are supported by the Email Security Monitor? (Choose three.)

- A. Destination domain
- B. Network owner
- C. MAC address
- D. Policy requirements

- E. Internal sender IP address
- F. Originating domain

Answer: A,B,E

Explanation:

QUESTION NO: 45

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

Answer: A

Explanation:

QUESTION NO: 46

A network engineer can assign IPS event action overrides to virtual sensors and configure which three modes? (Choose three.)

- A. Anomaly detection operational mode
- B. Inline TCP session tracking mode
- C. Normalizer mode
- D. Load-balancing mode
- E. Inline and Promiscuous mixed mode
- F. Fail-open and fail-close mode

Answer: A,B,C

Explanation:

QUESTION NO: 47

What is the correct deployment for an IPS appliance in a network where traffic identified as threat traffic should be blocked and all traffic is blocked if the IPS fails?

- A. Inline; fail open
- B. Inline; fail closed
- C. Promiscuous; fail open
- D. Promiscuous; fail closed

Answer: B

Explanation:

QUESTION NO: 48

Which two practices are recommended for implementing NIPS at enterprise Internet edges?
(Choose two.)

- A. Integrate sensors primarily on the more trusted side of the firewall (inside or DMZ interfaces).
- B. Integrate sensors primarily on the less trusted side of the firewall (outside interfaces).
- C. Implement redundant IPS and make data paths symmetrical.
- D. Implement redundant IPS and make data paths asymmetrical.
- E. Use NIPS only for small implementations.

Answer: A,C

Explanation:

QUESTION NO: 49

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
```

Answer: C

Explanation:

QUESTION NO: 50

What are two benefits of using SPAN with promiscuous mode deployment? (Choose two.)

- A. SPAN does not introduce latency to network traffic.
- B. SPAN can perform granular scanning on captures of per-IP-address or per-port monitoring.
- C. Promiscuous Mode can silently block traffic flows on the IDS.
- D. SPAN can analyze network traffic from multiple points.

Answer: A,D

Explanation:

QUESTION NO: 51

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

Answer: A

Explanation:

QUESTION NO: 52

Refer to the exhibit.

```

Status as of:           Wed May 22 16:05:13 2013 GMT
Hosts marked with '*' were down as of the last delivery attempt.

```

#	Recipient Host	Active Recip.	Conn. Out	Deliv. Recip.	Soft Bounced	Hard Bounced
1	example.com	1	11	10078	0	1
2	acme.com	0	3	34021	0	0
3	biology.acme.com	0	9	64026	0	0
4	*chemistry.acme.com	0	2	94091	0	0
5	pluto.acme.com	0	6	75021	0	0
5	*venus.acme.com	100	0	0	0	0
7	the.encryption.queue	0	0	90649	0	0
8	the.euq.queue	0	0	1	0	0
9	the.euq.release.queue	0	0	4531	0	0

email.example.com>

What CLI command generated the output?

- A. smtproutes
- B. tophosts
- C. hoststatus
- D. workqueuestatus

Answer: B

Explanation:

QUESTION NO: 53

Which version of AsyncOS for web is required to deploy the Web Security Appliance as a CWS connector?

- A. AsyncOS version 7.7.x
- B. AsyncOS version 7.5.x
- C. AsyncOS version 7.5.7
- D. AsyncOS version 7.5.0

Answer: C

Explanation:

QUESTION NO: 54

What are three benefits of the Cisco AnyConnect Secure Mobility Solution? (Choose three.)

- A. It can protect against command-injection and directory-traversal attacks.
- B. It provides Internet transport while maintaining corporate security policies.
- C. It provides secure remote access to managed computers.
- D. It provides clientless remote access to multiple network-based systems.
- E. It enforces security policies, regardless of the user location.
- F. It uses ACLs to determine best-route connections for clients in a secure environment.

Answer: B,C,E

Explanation:

QUESTION NO: 55

Which Cisco technology secures the network through malware filtering, category-based control, and reputation-based control?

- A. Cisco ASA 5500 Series appliances
- B. Cisco remote-access VPNs
- C. Cisco IronPort WSA
- D. Cisco IPS

Answer: C

Explanation:

QUESTION NO: 56

Which antispam technology assumes that email from server A, which has a history of distributing spam, is more likely to be spam than email from server B, which does not have a history of distributing spam?

- A. Reputation-based filtering
- B. Context-based filtering
- C. Cisco ESA multilayer approach
- D. Policy-based filtering

Answer: A

Explanation:

QUESTION NO: 57

Which Cisco technology is a modular security service that combines a stateful inspection firewall with next-generation application awareness, providing near real-time threat protection?

- A. Cisco ASA 5500 series appliances
- B. Cisco ASA CX Context-Aware Security
- C. WSA
- D. Internet Edge Firewall / IPS

Answer: B

Explanation:

QUESTION NO: 58

Which three statements about Cisco ASA CX are true? (Choose three.)

- A. It groups multiple ASAs as a single logical device.
- B. It can perform context-aware inspection.
- C. It provides high-density security services with high availability.
- D. It uses policy-based interface controls to inspect and forward TCP- and UDP-based packets.
- E. It can make context-aware decisions.
- F. It uses four cooperative architectural constructs to build the firewall.

Answer: B,E,F

Explanation:

QUESTION NO: 59

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

Answer: B

Explanation:

QUESTION NO: 60

Cisco AVC allows control of which three of the following? (Choose three.)

- A. Facebook
- B. LWAPP
- C. IPv6
- D. MySpace
- E. Twitter
- F. WCCP

Answer: A,D,E

Explanation:

QUESTION NO: 61

The Web Security Appliance has identities defined for faculty and staff, students, and default access. The faculty and staff identity identifies users based on the source network and authenticated credentials. The identity for students identifies users based on the source network along with successful authentication credentials. The global identity is for guest users not authenticated against the domain.

Recently, a change was made to the organization's security policy to allow faculty and staff access to a social network website, and the security group changed the access policy for faculty and staff to allow the social networking category.

Which are the two most likely reasons that the category is still being blocked for a faculty and staff user? (Choose two.)

- A. The user is being matched against the student policy because the user did not enter credentials.
- B. The user is using an unsupported browser so the credentials are not working.
- C. The social networking URL was entered into a custom URL category that is blocked in the access policy.
- D. The user is connected to the wrong network and is being blocked by the student policy.
- E. The social networking category is being allowed but the AVC policy is still blocking the website.

Answer: C,E

Explanation:

QUESTION NO: 62

Which five system management protocols are supported by the Intrusion Prevention System?
(Choose five.)

- A. SNMPv2c
- B. SNMPv1
- C. SNMPv2
- D. SNMPv3
- E. syslog
- F. SDEE
- G. SMTP

Answer: A,B,C,F,G

Explanation:

QUESTION NO: 63

Which IPS signature regular expression CLI command matches a host issuing a domain lookup for www.theblock.com?

- A. regex-string (\x03[Tt][Hh][Ee]\x05[Bb][Ll][Oo][Cc][Kk])
- B. regex-string (\x0b[theblock.com])
- C. regex-string (\x03[the]\x05[block]0x3[com])
- D. regex-string (\x03[T][H][E]\x05[B][L][O][C][K]\x03[.][C][O][M])

Answer: A

Explanation:

QUESTION NO: 64

Which three user roles are partially defined by default in Prime Security Manager? (Choose three.)

- A. networkoperator
- B. admin
- C. helpdesk
- D. securityoperator
- E. monitoringadmin
- F. systemadmin

Answer: B,C,F

Explanation:

QUESTION NO: 65

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

Answer: A,C,D

Explanation:

QUESTION NO: 66

At which value do custom signatures begin?

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

Answer: D

Explanation:

QUESTION NO: 67

Which two commands are valid URL filtering commands? (Choose two.)

- A. url-server (DMZ) vendor smartfilter host 10.0.1.1
- B. url-server (DMZ) vendor url-filter host 10.0.1.1
- C. url-server (DMZ) vendor n2h2 host 10.0.1.1
- D. url-server (DMZ) vendor CISCO host 10.0.1.1
- E. url-server (DMZ) vendor web host 10.0.1.1

Answer: A,C

Explanation:

QUESTION NO: 68

Which Cisco technology is a customizable web-based alerting service designed to report threats and vulnerabilities?

- A. Cisco Security Intelligence Operations
- B. Cisco Security IntelliShield Alert Manager Service
- C. Cisco Security Optimization Service
- D. Cisco Software Application Support Service

Answer: B

Explanation:

QUESTION NO: 69

Instructions

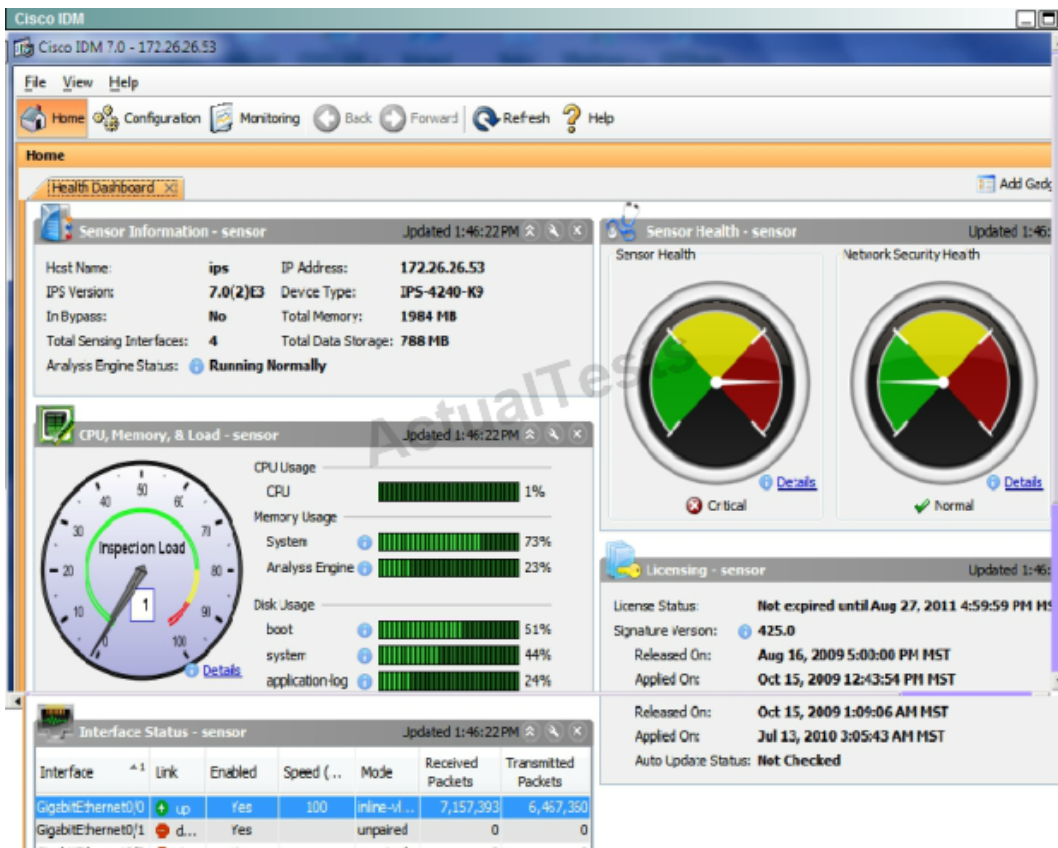
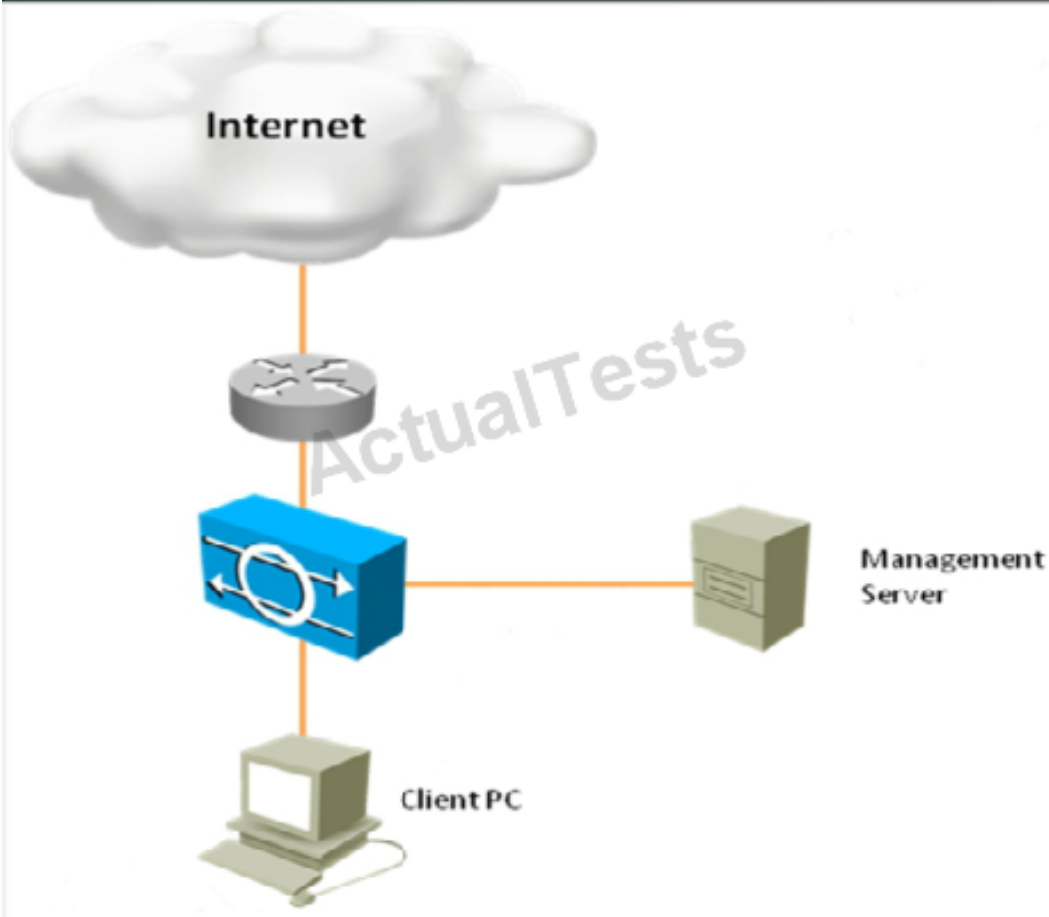
You can click the grey buttons at the bottom of this frame to view the different windows.

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



Which signature definition is virtual sensor 0 assigned to use?

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

Answer: C

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 NO: 70

Instructions

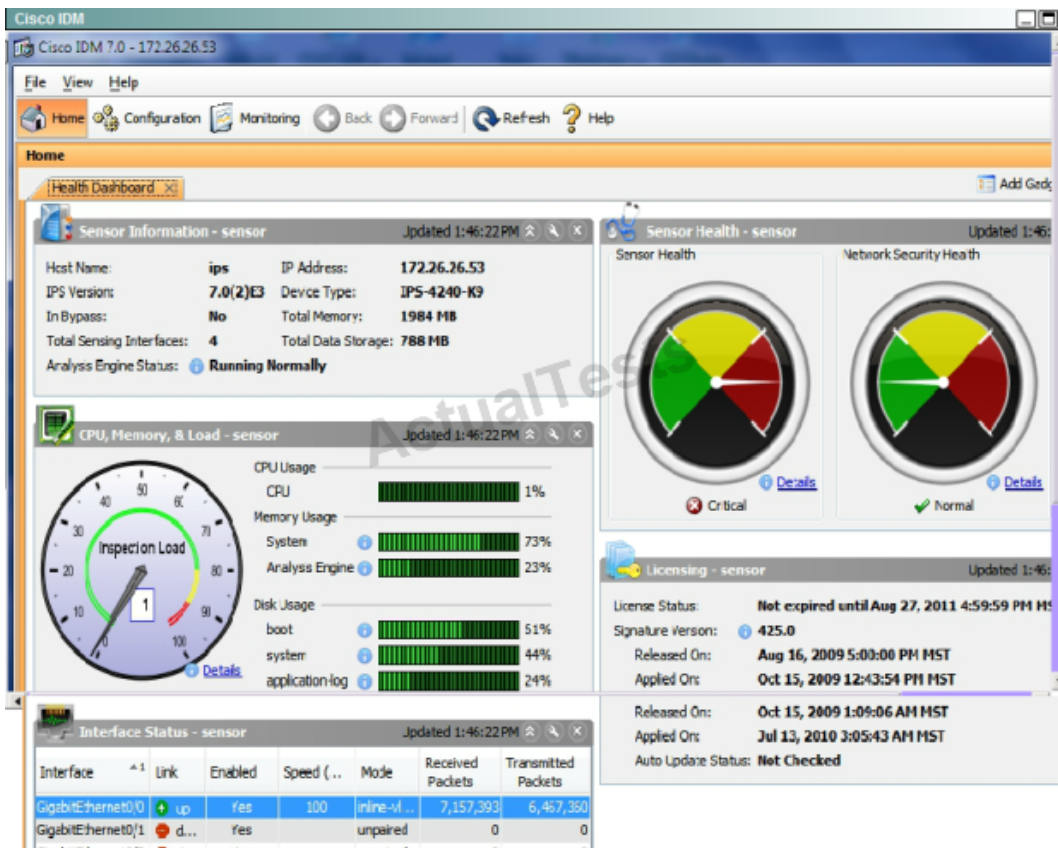
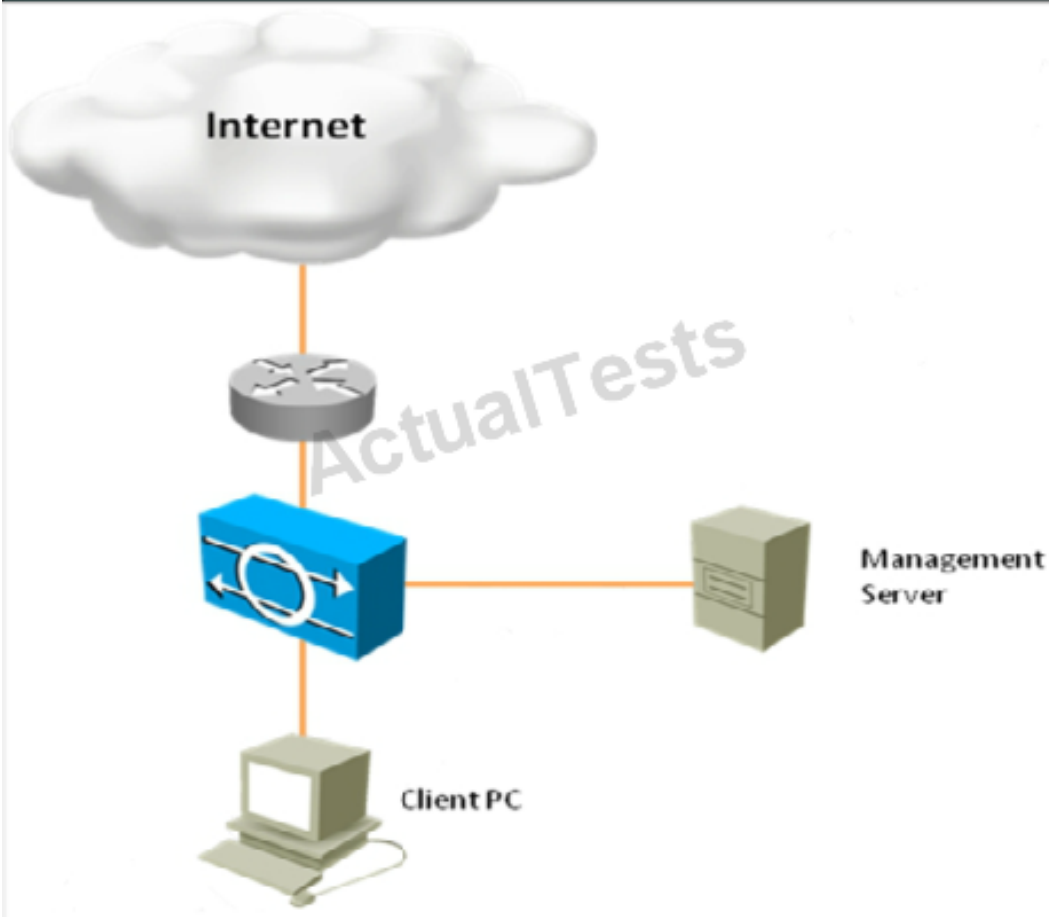
You can click the grey buttons at the bottom of this frame to view the different windows.

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



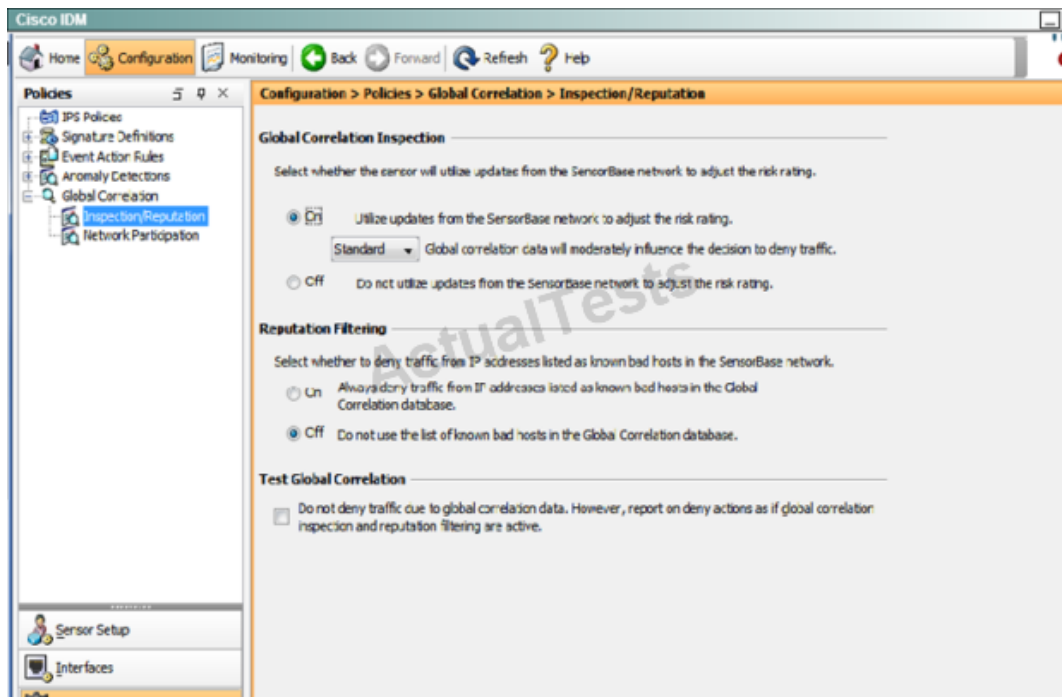
What action will the sensor take regarding IP addresses listed as known bad hosts in the Cisco SensorBase network?

- A. Global correlation is configured in Audit mode for testing the feature without actually denying any hosts.
- B. Global correlation is configured in Aggressive mode, which has a very aggressive effect on deny actions.
- C. It will not adjust risk rating values based on the known bad hosts list.
- D. Reputation filtering is disabled.

Answer: D

Explanation:

This can be seen on the Global Correlation – Inspection/Reputation tab shown below:



QUESTION NO: 71

Instructions

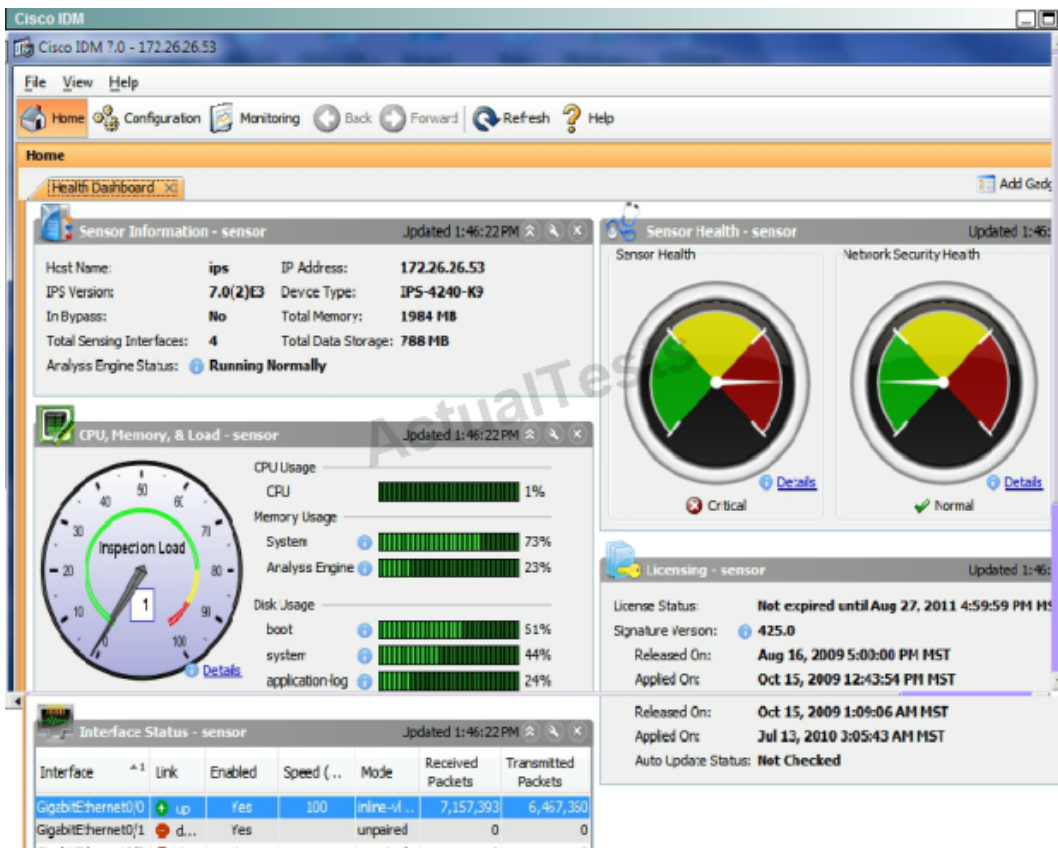
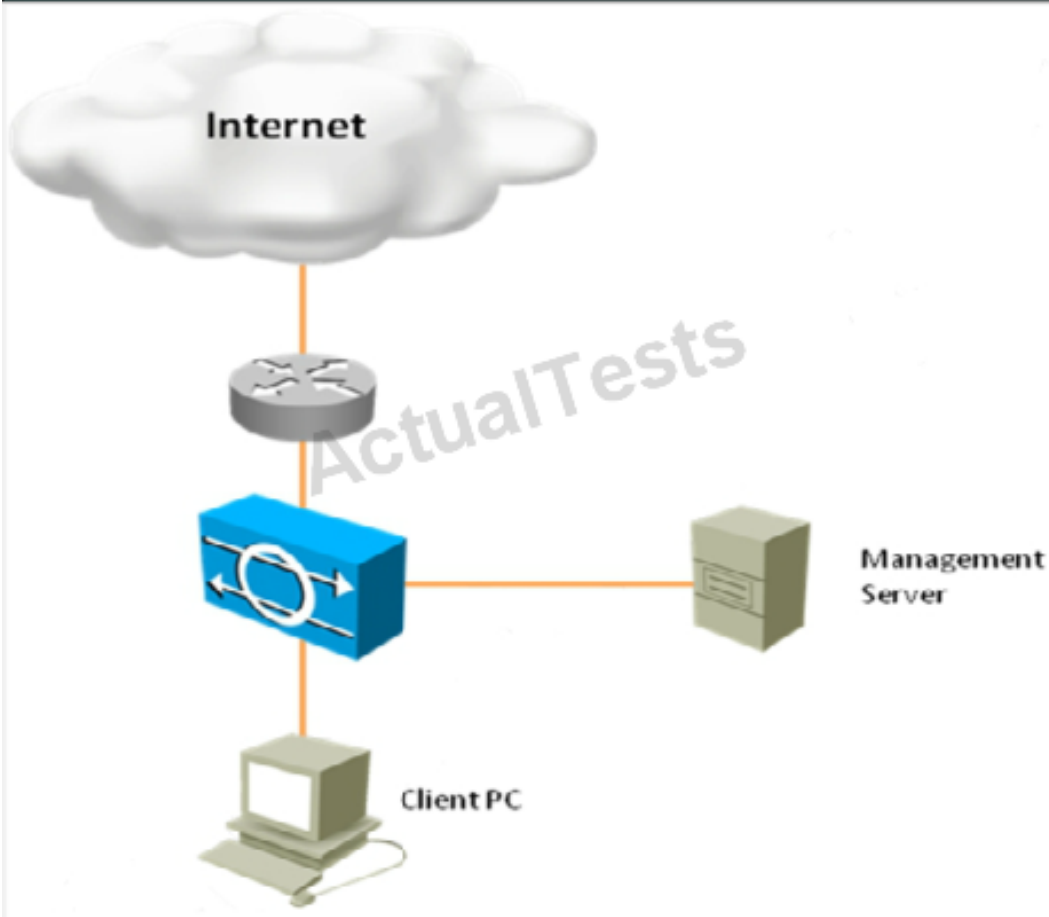
You can click the grey buttons at the bottom of this frame to view the different windows.

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



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

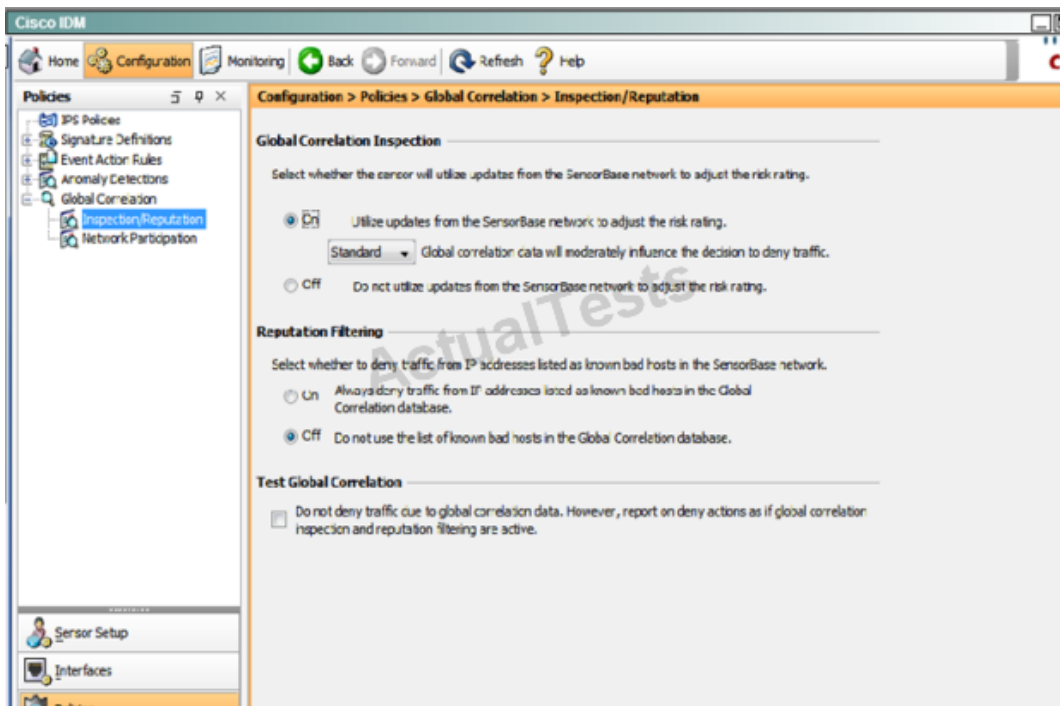
- A. It will not contribute to the SensorBase network.
- B. It will contribute to the SensorBase network, but will withhold some sensitive information
- C. It will contribute the victim IP address and port to the SensorBase network.
- D. It will not contribute to Risk Rating adjustments that use information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

Answer: B

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:



QUESTION NO: 72

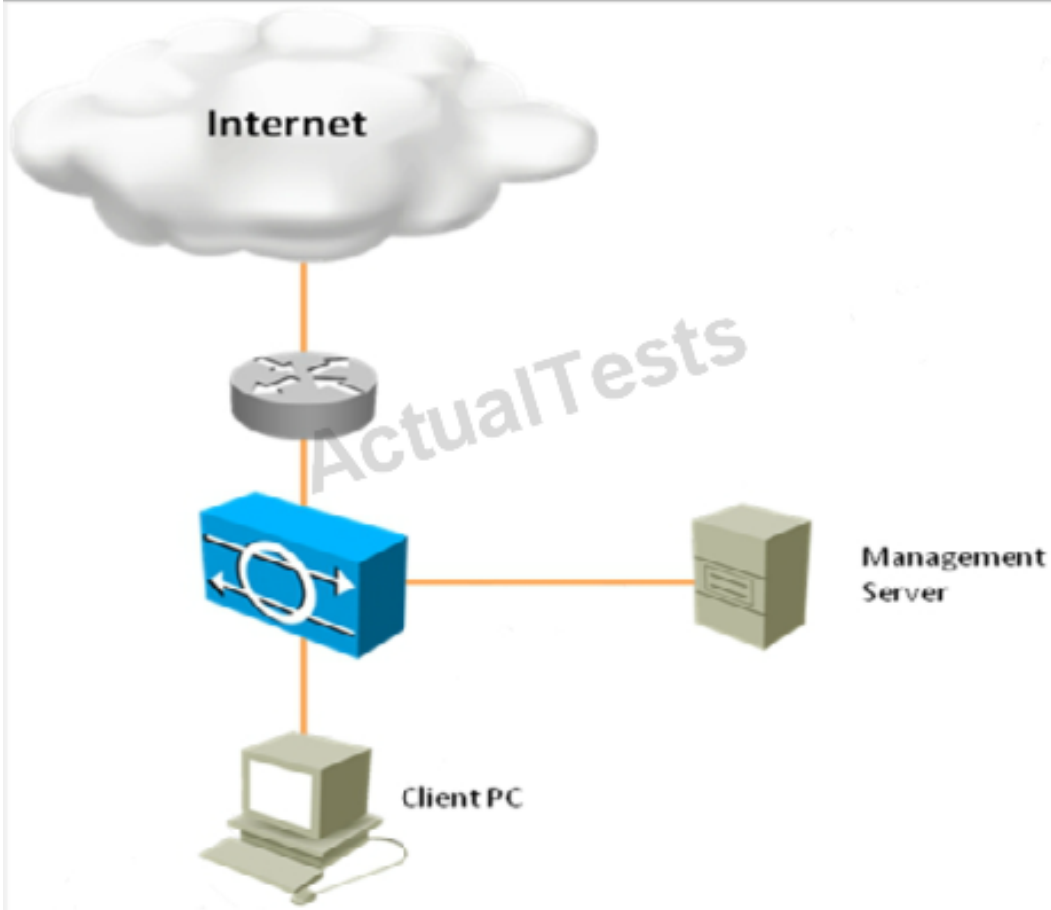
Instructions

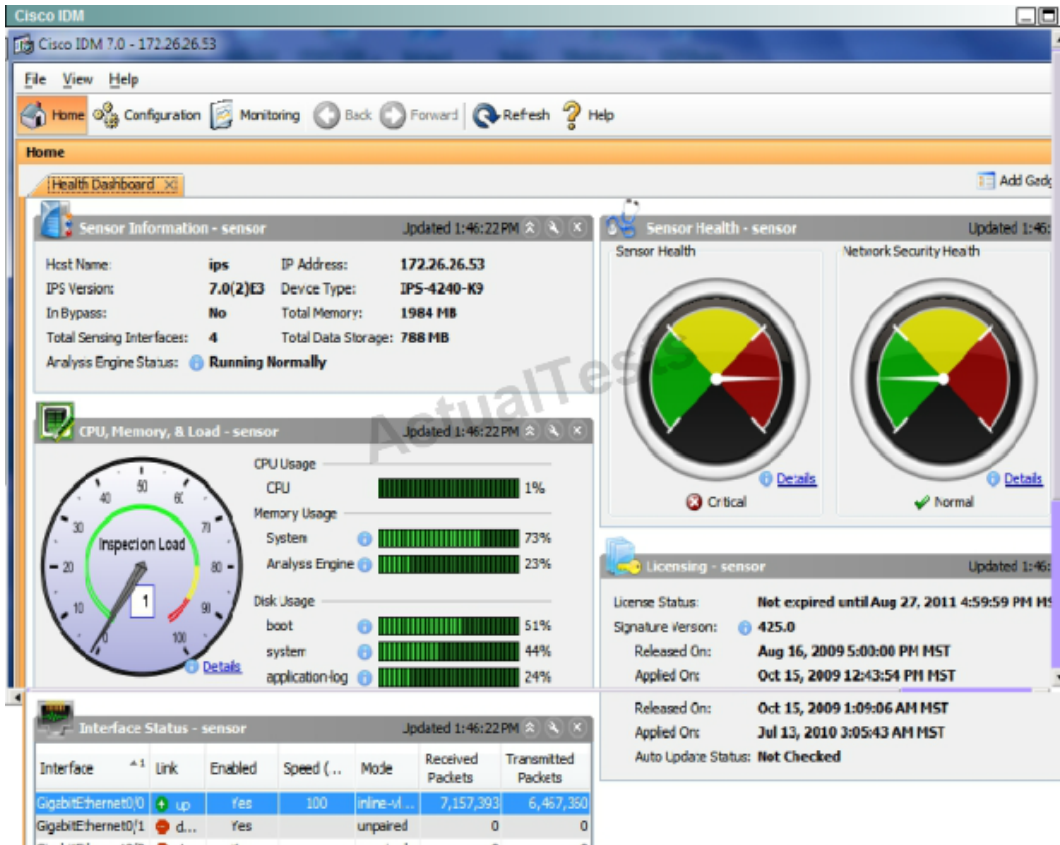
You can click the grey buttons at the bottom of this frame to view the different windows.

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



Which two statements about Signature 1104 are true? (Choose two.)

- A. This is a custom signature.
- B. The severity level is High.
- C. This signature has triggered as indicated by the red severity icon.
- D. Produce Alert is the only action defined.
- E. This signature is enabled, but inactive, as indicated by the 0 to that follows the signature number.

Answer: B,D

Explanation:

This can be seen here where signature 1004 is the 5th one down:

Configuration > Policies > Signature Definitions > sig0 > All Signatures

Filter: Sig ID

ID	Name	Enabled	Severity	Fidelity Rating	Case Rtr	Signature Actions	Alert and Log	Deny	Other	Type	Engine
1000/0	IP options-Bad Option ...	☒	Inform	75	18	Alert				Default	Atc
1001/0	IP options-Record Pac...	☒	Inform	100	25	Alert				Default	Atc
1002/0	IP options-Timestamp	☒	Inform	100	25	Alert				Default	Atc
1003/0	IP options-Provide s...	☒	Inform	100	25	Alert				Default	Atc
1004/0	IP options-Loose Sour...	☒	High	100	100	Alert				Default	Atc
1005/0	IP options-SATNET ID	☒	Inform	100	25	Alert				Default	Atc
1006/0	IP options-Strict Sourc...	☒	High	100	100	Alert				Default	Atc
1007/0	IPv6 over IPv4 or IPv6	☒	Inform	100	25	Alert				Default	Atc
1101/0	Unknown IP Protocol	☒	Inform	75	18	Alert				Default	Atc
1102/0	Impossible IP Packet	☒	High	100	100	Alert				Default	Atc
1104/0	IP Localhost Source S...	☒	High	100	100	Alert				Default	Atc
1107/0	RFC 1913 Addresses ...	☒	Inform	100	25	Alert				Default	Atc
1108/0	IP Packet with Proto 11	☒	High	100	100	Alert				Default	Atc
1109/0	Cisco IOS Interface DoS	☒	Medium	75	56	Alert				Default	Atc
1109/1	Cisco IOS Interface DoS	☒	Medium	75	56	Alert				Default	Atc
1109/2	Cisco IOS Interface DoS	☒	Medium	75	56	Alert				Default	Atc
1109/3	Cisco IOS Interface DoS	☒	Medium	75	56	Alert				Default	Atc
1200/0	IP Fragmentation Buff...	☒	Inform	100	25	Alert		Packet		Default	Nor

QUESTION NO: 73

Instructions

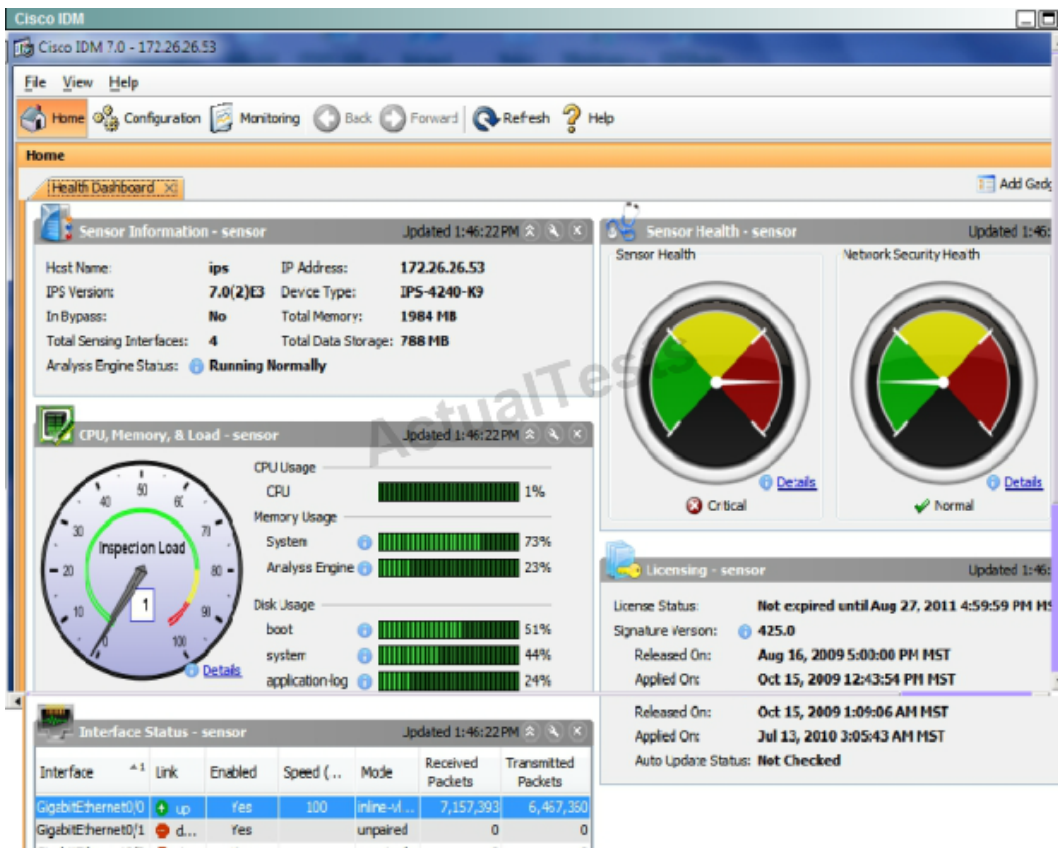
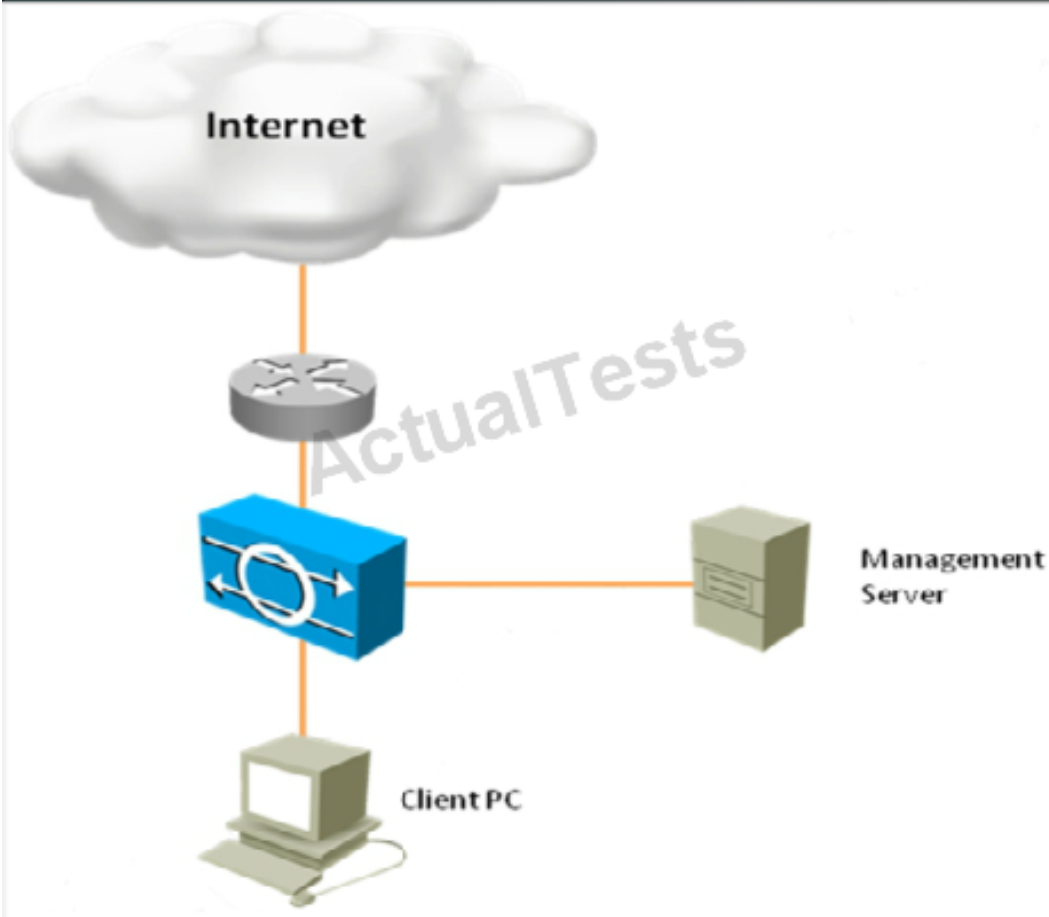
You can click the grey buttons at the bottom of this frame to view the different windows.

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



Which three statements about the Cisco IPS appliance configurations are true? (Choose three.)

- A. The maximum number of denied attackers is set to 10000.
- B. The block action duration is set to 3600 seconds.
- C. The Meta Event Generator is globally enabled.
- D. Events Summarization is globally disabled.
- E. Threat Rating Adjustment is globally disabled.

Answer: A,B,C

Explanation:

QUESTION NO: 74

Instructions

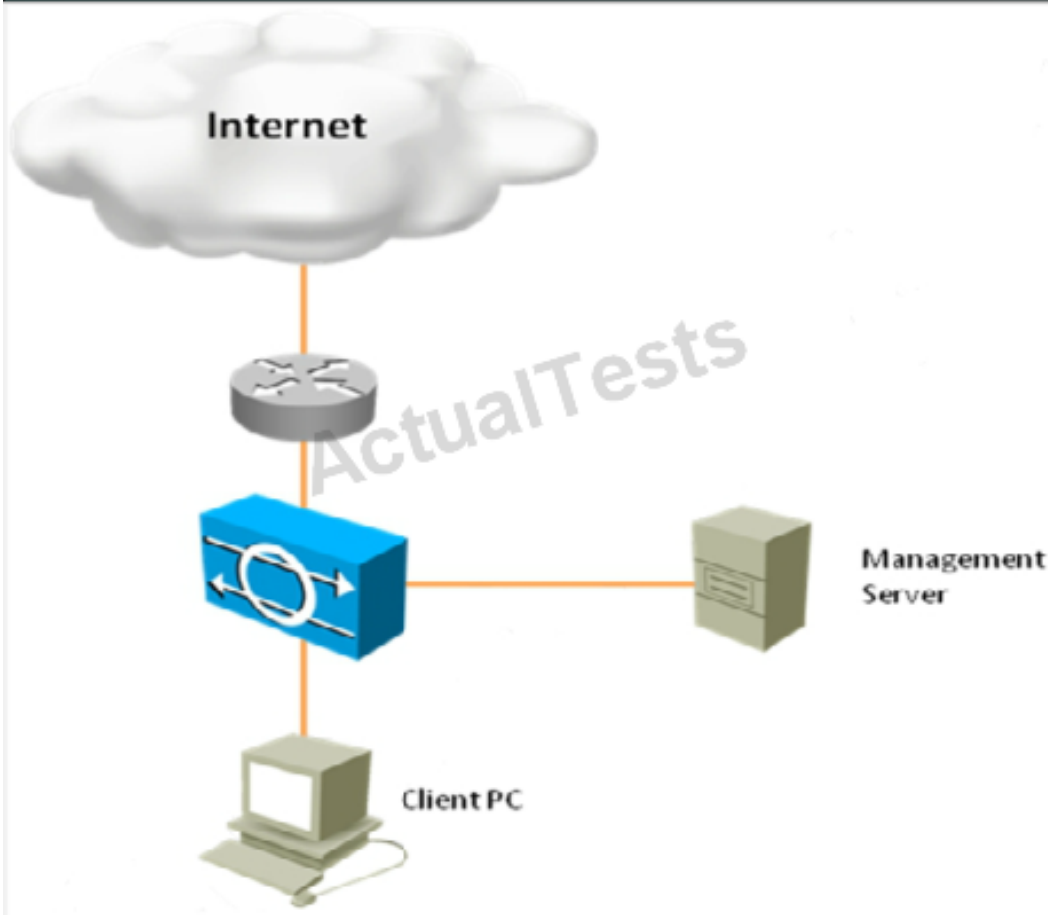
You can click the grey buttons at the bottom of this frame to view the different windows.

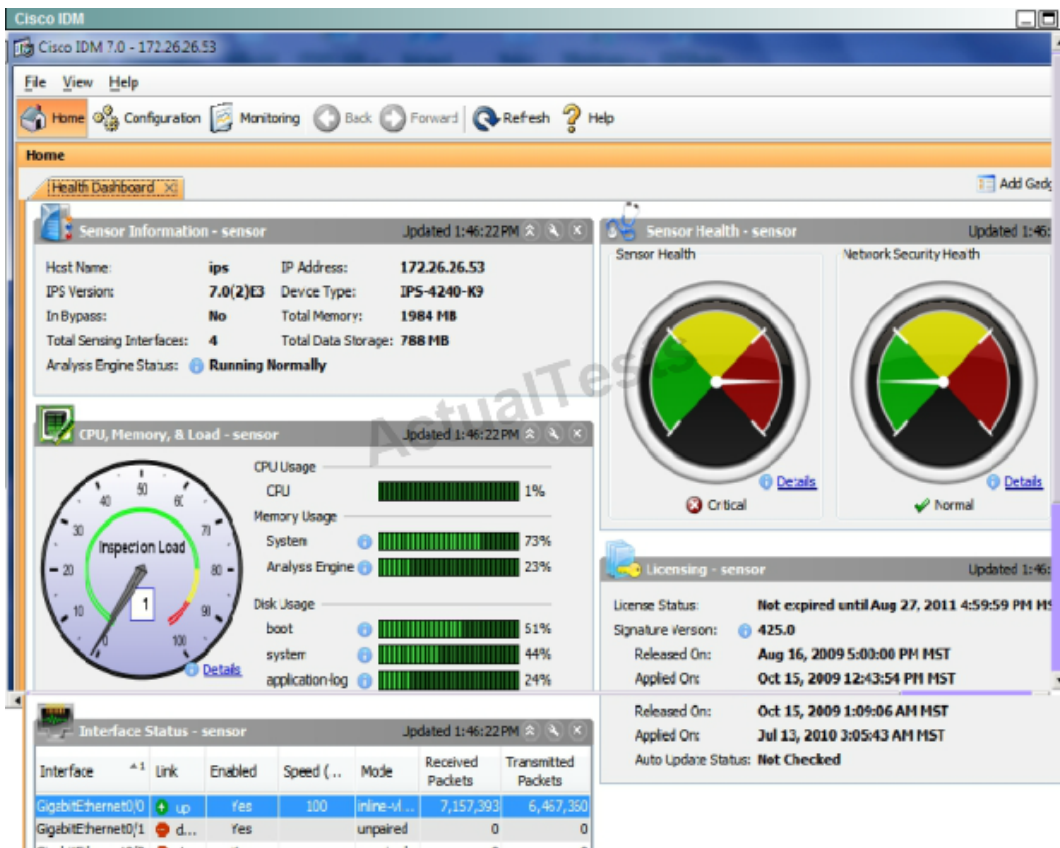
To minimize the window, click the [-]. To move the window, click the title bar and drag the window.

Scenario

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

Topology





What is the status of OS Identification?

- A. It is only enabled to identify "Cisco IOS" OS using statically mapped OS fingerprinting
- B. OS mapping information will not be used for Risk Rating calculations.
- C. It is configured to enable OS mapping and ARR only for the 10.0.0.0/24 network.
- D. It is enabled for passive OS fingerprinting for all networks.

Answer: D

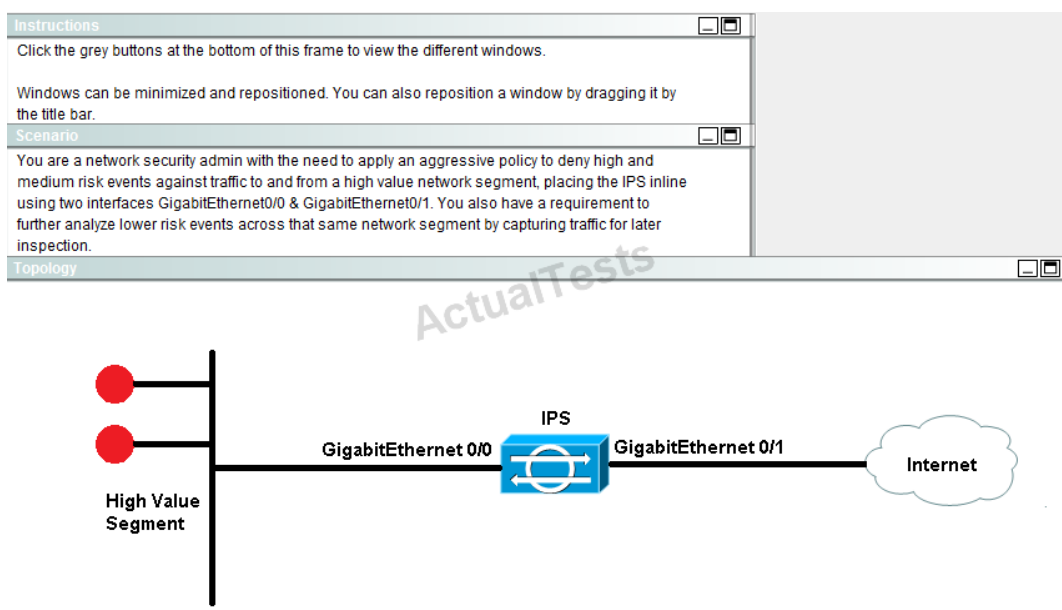
Explanation:

Understanding Passive OS Fingerprinting Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type. The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack and/or the sensor may filter the alert for the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert. Passive OS fingerprinting consists of three components:

- Passive OS learning Passive OS learning occurs as the sensor observes traffic on the network.

Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address. •User-configurable OS identification You can configure OS host mappings, which take precedence over learned OS mappings. •Computation of attack relevance rating and risk rating

QUESTION NO: 75 CORRECT TEXT



ASDM

File View Help

Home Configuration Monitoring Back Forward Refresh Help

Interfaces

- Summary
- Interfaces
- Interface Pairs
- VLAN Pairs
- VLAN Groups
- Bypass
- Traffic Flow Notifications
- CDP Mode

Configuration > Interfaces > Summary

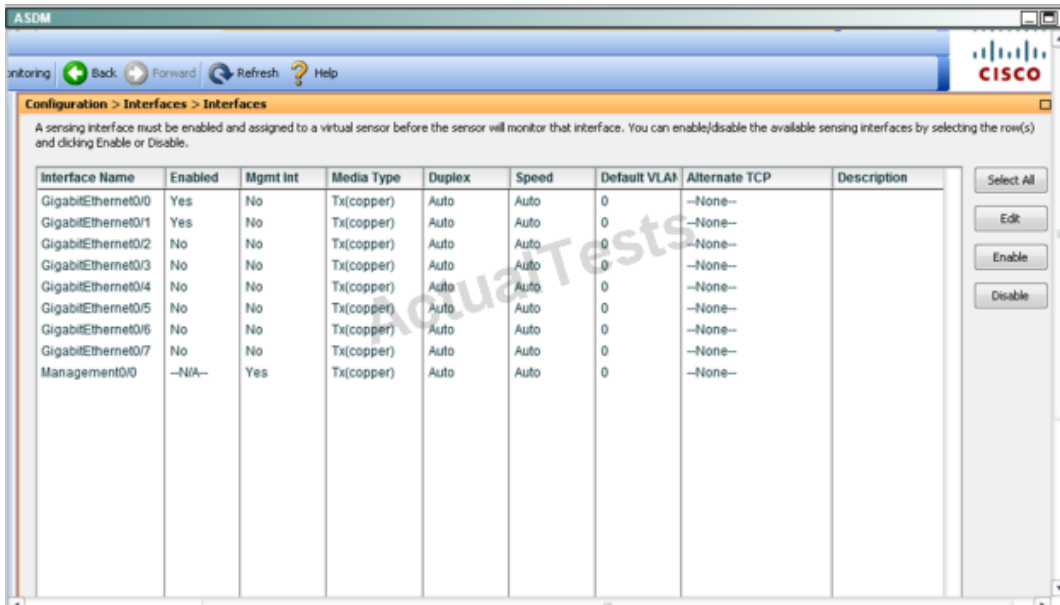
The following is the configuration summary of the sensing interfaces. You can configure any single physical interface for promiscuous, inline interface pair combination of these modes is allowed.

Name	Details	Assigned Virtual Sensor
GigabitEthernet0/0	TX (copper)	--None--
GigabitEthernet0/1	TX (copper)	--None--
GigabitEthernet0/2	TX (copper)	--None--
GigabitEthernet0/3	TX (copper)	--None--
GigabitEthernet0/4	TX (copper)	--None--
GigabitEthernet0/5	TX (copper)	--None--
GigabitEthernet0/6	TX (copper)	--None--
GigabitEthernet0/7	TX (copper)	--None--
Management0/0	TX (copper)	--None--

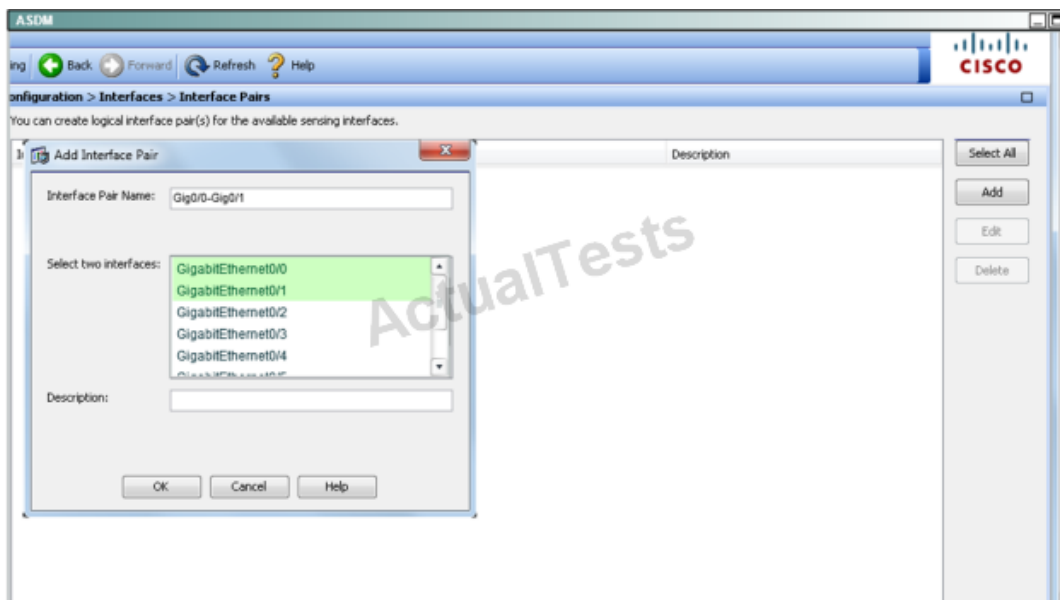
Answer: Steps are in Explanation below:

Explanation:

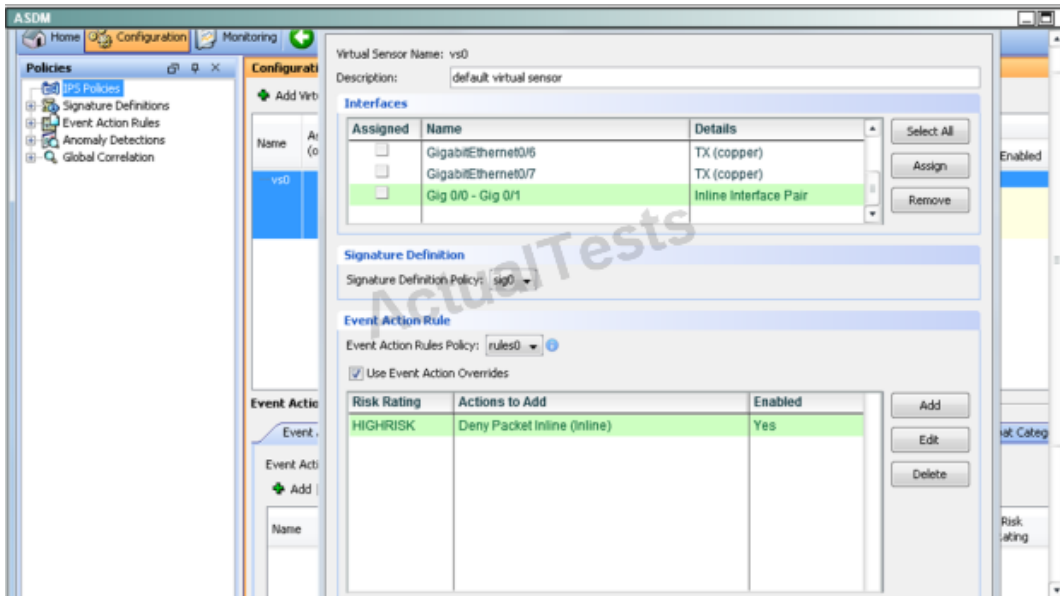
First, enable the Gig 0/0 and Gig 0/1 interfaces:



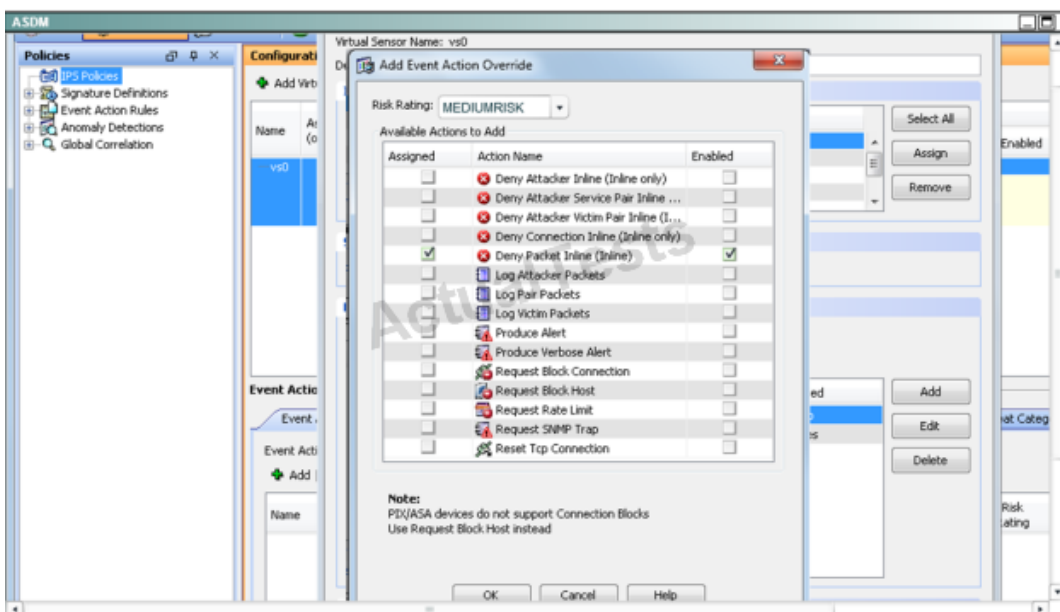
Second, create the pair under the "interface pairs" tab:



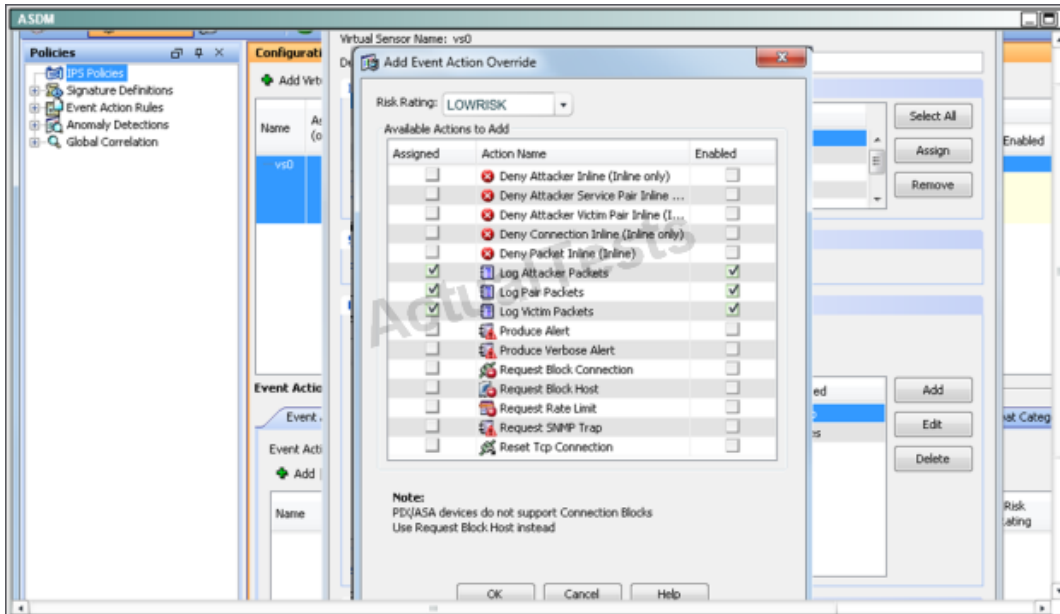
Then, apply the HIGHRISK action rule to the newly created interface pair:



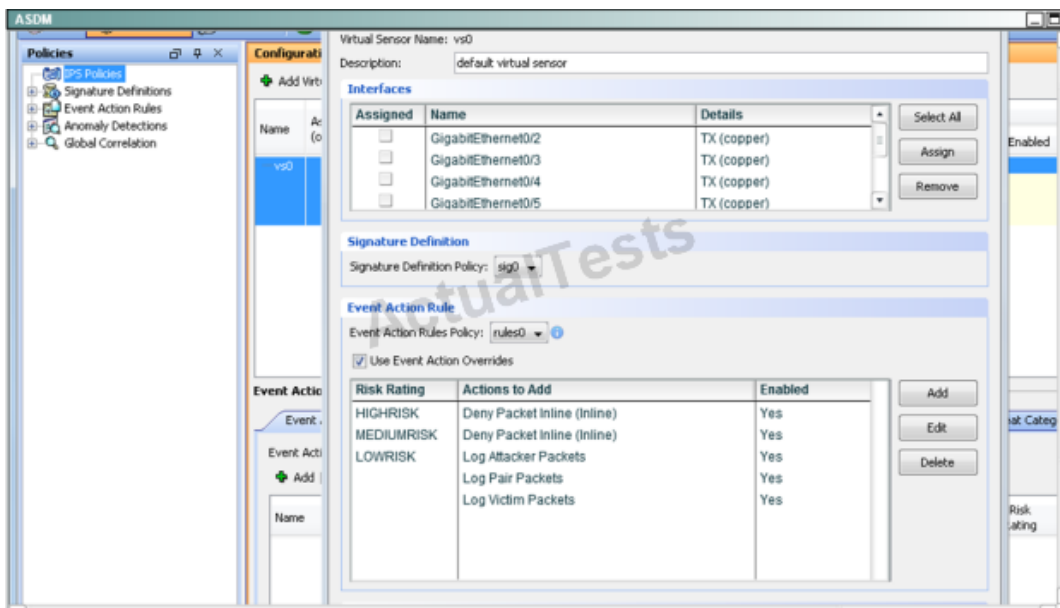
Then apply the same for the MEDIUM RISK traffic (deny attacker inline)



Finally. Log the packets for the LOW RISK event:



When done it should look like this:



ASDM

ing Back Forward Refresh Help

Configuration > Policies > IPS Policies

Add Virtual Sensor Edit Delete

Name	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 Packet Yes		

Event 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 Help

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

Add Edit Delete

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