300-207Q&As

Implementing Cisco Threat Control Solutions

Pass Cisco 300-207 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/300-207.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which Cisco ESA component receives connections from external mail servers?

A. MTA

B. public listener

C. private listener

D. recipient access table

E. SMTP incoming relay agent

Correct Answer: B

QUESTION 2

Which option is a benefit of Cisco hybrid email security?

A. on-premises control of outbound data

B. advanced malware protection

C. email encryption

D. message tracking

Correct Answer: A

QUESTION 3

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

Correct Answer: AC

QUESTION 4

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

Correct Answer: A

QUESTION 5

Which three zones are used for anomaly detection in a Cisco IPS? (Choose three.)

A. internal zone

B. external zone

C. illegal zone

D. inside zone

E. outside zone

F. DMZ zone

Correct Answer: ABC

QUESTION 6

Instructions

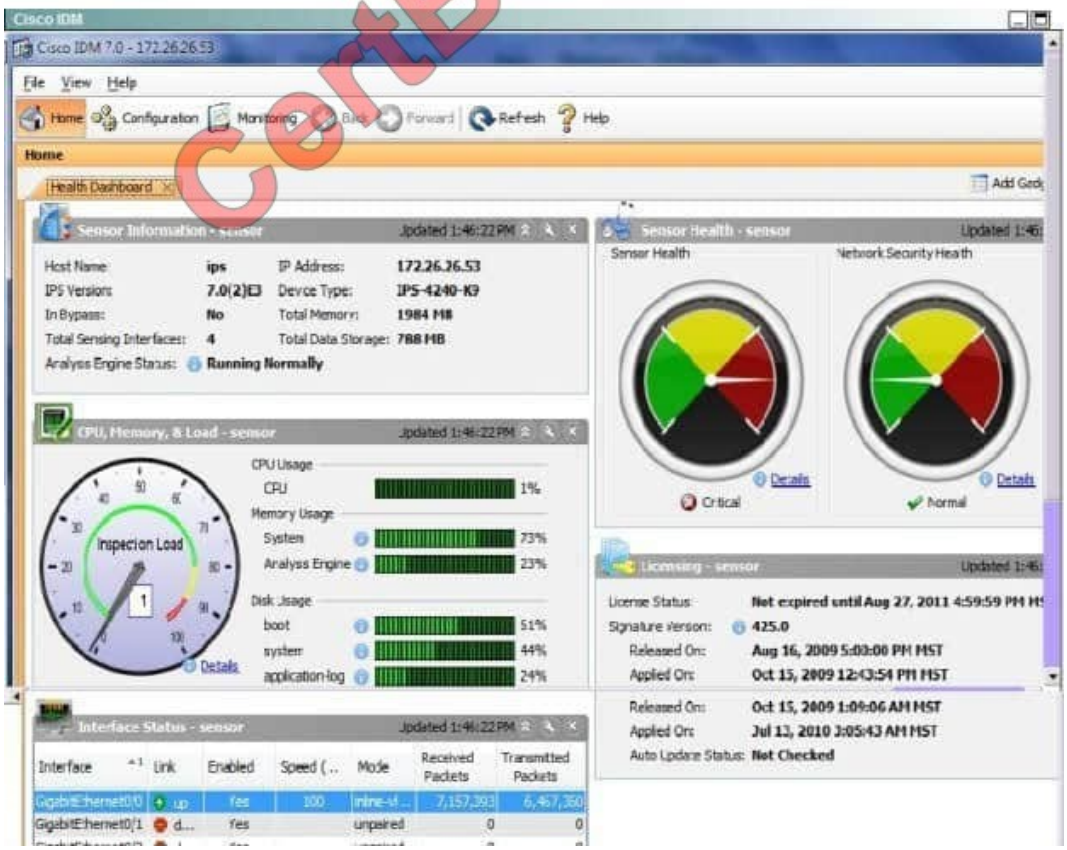
You can click the grey buttons at the bottom of this frame to view the different windows.

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

Correct Answer: C

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 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

QUESTION 8

Which two conditions must you configure in an event action override to implement a risk rating of 70 or higher and terminate the connection on the IPS? (Choose two.)

A. Configure the event action override to send a TCP reset.

B. Set the risk rating range to 70 to 100.

C. Configure the event action override to send a block-connection request.

D. Set the risk rating range to 0 to 100.

E. Configure the event action override to send a block-host request.

Correct Answer: AB

QUESTION 9

What are two features of the Cisco ASA NGFW? (Choose two.)

A. It can restrict access based on qualitative analysis.

B. It can restrict access based on reputation.

C. It can reactively protect against Internet threats.

D. It can proactively protect against Internet threats.

Correct Answer: BD

QUESTION 10

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.

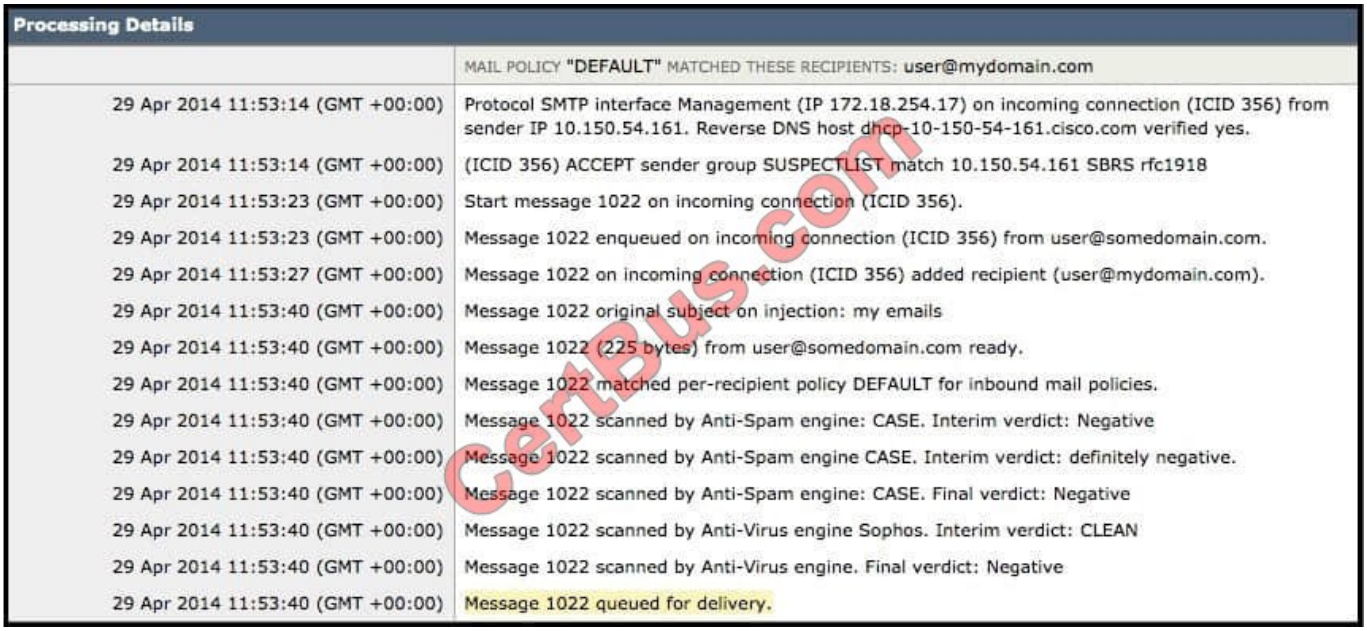
E. It enforces security policies, regardless of the user location.

F. It uses ACLs to determine best-route connections for clients in a secure environment.

Correct Answer: BCE

QUESTION 11

Refer to the exhibit.



Processing Details	
	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: user@mydomain.com
29 Apr 2014 11:53:14 (GMT +00:00)	Protocol SMTP interface Management (IP 172.18.254.17) on incoming connection (ICID 356) from sender IP 10.150.54.161. Reverse DNS host dhcp-10-150-54-161.cisco.com verified yes.
29 Apr 2014 11:53:14 (GMT +00:00)	(ICID 356) ACCEPT sender group SUSPECTLIST match 10.150.54.161 SBRS rfc1918
29 Apr 2014 11:53:23 (GMT +00:00)	Start message 1022 on incoming connection (ICID 356).
29 Apr 2014 11:53:23 (GMT +00:00)	Message 1022 enqueued on incoming connection (ICID 356) from user@somedomain.com.
29 Apr 2014 11:53:27 (GMT +00:00)	Message 1022 on incoming connection (ICID 356) added recipient (user@mydomain.com).
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 original subject on injection: my emails
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 (225 bytes) from user@somedomain.com ready.
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 matched per-recipient policy DEFAULT for inbound mail policies.
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Spam engine: CASE. Final verdict: Negative
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 scanned by Anti-Virus engine. Final verdict: Negative
29 Apr 2014 11:53:40 (GMT +00:00)	Message 1022 queued for delivery.

The system administrator of mydomain.com received complaints that some messages that were sent from sender user@somedomain.com were delayed. Message tracking data on the sender shows that an email sample that was received was clean and properly delivered. What is the likely cause of the intermittent delays?

A. The remote MTA has a SenderBase Reputation Score of -1.0.

B. The remote MTA is sending emails from RFC 1918 IP addresses.

C. The remote MTA has activated the SUSPECTLIST sender group.

D. The remote MTA has activated the default inbound mail policy.

Correct Answer: C

QUESTION 12

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

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: