Cisco

Exam 300-207

Implementing Cisco Threat Control Solutions

Version: 11.0

[Total Questions: 242]

Question No : 1

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

Question No : 2

Which three administrator actions are used to configure IP logging in Cisco IME? (Choose three.)

A. Select a virtual sensor.
B. Enable IP logging.
C. Specify the host IP address.
D. Set the logging duration.
E. Set the number of packets to capture.
F. Set the number of bytes to capture.

Answer: A,C,D

Question No : 3

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

Question No : 4

Which option is a benefit of Cisco Email Security virtual appliance over the Cisco ESA appliance?

A. reduced space and power requirements
B. outbound message protection
C. automated administration
D. global threat intelligence updates from Talos

Answer: A

Question No : 5

Refer to the exhibit.

Option	Redirect Method	Assignment Method	Ingress/Egress Redirection	Switching Result
1	L2	Hash	Ingress	Software Processing
2	L2 (Recommended)	Mask	Ingress	Full Hardware Processing with ACL TCAM
3	L2	Hash	Egress	Software Processing
4	L2	Mask	Egress	Software Processing of initial packet
5	GRE (PFC3 or newer)	Hash	Ingress	Software Processing of Initial packet with Netflow Partial-Flow
6	GRE (PFC3 or newer)	Mask	Ingress	Full Hardware Processing with Netflow Full-Flow
7	GRE	Hash	Egress	Software Processing
8	GRE (PFC3 or newer)	Mask	Egress	Software Processing of initial packet

When designing the network to redirect web traffic utilizing the Catalyst 6500 to the Cisco Web Security Appliance, impact on the switch platform needs consideration. Which four rows identify the switch behavior in correlation to the redirect method? (Choose four.)

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5
F. Row 6

G. Row 7
H. Row 8

Answer: B,C,F,G

Question No : 6

Which solution must a customer deploy to prioritize traffic to a cloud-based contact management application while still allowing employees access to the Internet for business and personal use?

A. Cisco Application Visibility and Control
B. Cisco Intrusion Prevention Services
C. Cisco NetFlow
D. policy-based routing

Answer: A

Question No : 7

An IPS is configured to fail-closed and you observe that all packets are dropped. What is a possible reason for this behavior?

A. Mainapp is unresponsive.
B. The global correlation update failed.
C. The IPS span session failed.
D. The attack drop file is misconfigured.

Answer: A

Question No : 8

Which Cisco technology provides spam filtering and email protection?

A. IPS
B. ESA
C. WSA

D. CX

Answer: B

Question No : 9

When centralized message tracking is enabled on the Cisco ESA, over which port does the communication to the SMA occur by default?

A. port 2222/TCP
B. port 443/TCP
C. port 25/TCP
D. port 22/TCP

Answer: D

Question No : 10

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

Question No : 11

Within Cisco IPS anomaly detection, 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

Question No : 12

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

Question No : 13

Which command sets the number of packets to log on a Cisco IPS sensor?

A. ip-log-count number
B. ip-log-packets number
C. ip-log-bytes number
D. ip-log number

Answer: B

Question No : 14

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

Question No : 15

Which Cisco IPS CLI command shows the most fired signature?

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

Answer: A

Question No : 16

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

Question No : 17

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

Question No : 18

r01(config)#ip wccp web-cache redirect-list 80 password local

Refer to the above. What can be determined from this router configuration command for Cisco

WSA?

A. Traffic using TCP port 80 is redirected to the Cisco WSA.
B. The default “cisco” password is configured on the Cisco WSA.
C. Traffic denied in prefix-list 80 is redirected to the Cisco WSA.
D. Traffic permitted in access-list 80 is redirected to the Cisco WSA.

Answer: D

Question No : 19

What are the two policy types that can use a web reputation profile to perform reputation-based processing? (Choose two.)

A. profile policies
B. encryption policies
C. decryption policies
D. access policies

Answer: C,D

Question No : 20

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

Question No : 21

Which signature engine is responsible for ICMP inspection on Cisco IPS?

A. AIC Engine
B. Fixed Engine
C. Service Engine
D. Atomic IP Engine

Answer: D

Question No : 22

What is a difference between a Cisco Content Security Management virtual appliance and a physical appliance?

A. The virtual appliance requires an additional license to run on a host.
B. The physical appliance requires an additional license to activate its adapters.
C. Migration between virtual appliances of varying sizes is possible, but physical appliances must be of equal size.
D. The physical appliance is configured with a DHCP-enabled management port to receive an IP address automatically, but you must assign the virtual appliance an IP address manually in your management subnet.

Answer: A

Question No : 23

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

Question No : 24

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

Question No : 25

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

A. It supports custom signatures
B. It supports virtual sensors.
C. It supports multiple VRFs.
D. It uses configurable anomaly detection.
E. Signature definition files have been deprecated.

Answer: C,E

Question No : 26

What is the correct deployment for an IPS appliance in a network where traffic identified as