Vendor: Cisco

Exam Code:351-018

Exam Name:CCIE Security written

Version: Demo

QUESTION 1

Which would be the best method to deploy on a Cisco ASA to detect and prevent viruses and worms?

A. deep packet inspection

B. content security via the Control Security Services Module

C. Unicast Reverse Path Forwarding

D. IP audit signatures

Correct Answer: B

QUESTION 2

Which three options are the types of zones that are defined for anomaly detection on the Cisco IPS Sensor? (Choose three.)

A. inside

B. outside

C. internal

D. external

E. illegal

F. baseline

Correct Answer: CDE

QUESTION 3

A device is sending a PDU of 5000 B on a link with an MTU of 1500 B. If the PDU includes 20 B of IP header, which statement is true?

A. The first three packets will have a packet payload size of 1400.

B. The last packet will have a payload size of 560.

C. The first three packets will have a packet payload size of 1480.

D. The last packet will have a payload size of 20.

Correct Answer: C

QUESTION 4

Which field in an HTTPS server certificate is compared to a server name in the URL?

A. Common Name

B. Issuer Name

C. Organization

D. Organizational Unit

Correct Answer: A

QUESTION 5

Which three object tracking options are supported by Cisco IOS policy-based routing? (Choose three.)

A. absence of an entry in the routing table

B. existence of a CDP neighbor relationship

C. existence of an entry in the routing table

D. results of an SAA operation

E. state of the line protocol of an interface

Correct Answer: CDE

QUESTION 6

Which statement about SMTP is true?

A. SMTP uses UDP port 25.

B. The POP protocol is used by the SMTP client to manage stored mail.

C. The IMAP protocol is used by the SMTP client to retrieve and manage stored email.

D. The mail delivery agent in the SMTP architecture is responsible for DNS lookup.

E. SMTP uses TCP port 20.

Correct Answer: C

QUESTION 7

Which common FTP client command transmits a direct, byte-for-byte copy of a file?

A. ascii

B. binary

C. hash

D. quote

E. glob

Correct Answer: B

QUESTION 8

A Cisco Easy VPN software client is unable to access its local LAN devices once the VPN tunnel is established. What is the best way to solve this issue?

A. The IP address that is assigned by the Cisco Easy VPN Server to the client must be on the same network as the local LAN of the client.

B. The Cisco Easy VPN Server should apply split-tunnel-policy excludespecified with a split- tunnel-list containing the local LAN addresses that are relevant to the client.

C. The Cisco Easy VPN Server must push down an interface ACL that permits the traffic to the local LAN from the client.

D. The Cisco Easy VPN Server should apply a split-tunnel-policy tunnelall policy to the client.

E. The Cisco Easy VPN client machine needs to have multiple NICs to support this.
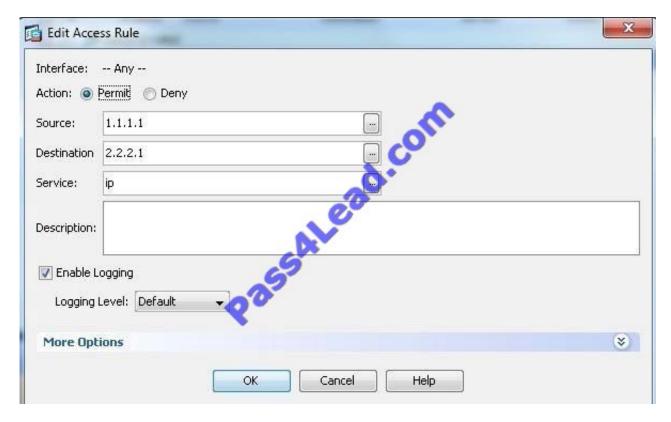
Correct Answer: B

QUESTION 9

According to RFC 4890, which four ICMPv6 types are recommended to be allowed to transit a firewall? (Choose four.)

A. Type 1 - destination unreachable

B. Type 2 - packet too big

C. Type 3 - time exceeded

D. Type 0 - echo reply

E. Type 8 - echo request

F. Type 4 - parameter problem

Correct Answer: ABCF

QUESTION 10

Refer to the exhibit.

Which three statements about the Cisco ASDM screen seen in the exhibit are true? (Choose three.)

A. This access rule is applied to all the ASA interfaces in the inbound direction.

B. The ASA administrator needs to expand the More Options tag to configure the inbound or outbound direction of the access rule.

C. The ASA administrator needs to expand the More Options tag to apply the access rule to an interface.

D. The resulting ASA CLI command from this ASDM configuration is access-list global_access line 1 extended permit ip host 1.1.1.1 host 2.2.2.1.

E. This access rule is valid only on the ASA appliance that is running software release 8.3 or later.

F. This is an outbound access rule.

Correct Answer: ADE

QUESTION 11

Which statement is true about EAP-FAST?

A. It supports Windows single sign-on.

B. It is a proprietary protocol.

C. It requires a certificate only on the server side.

D. It does not support an LDAP database.

Correct Answer: A

QUESTION 12

Which statement about the distributed SYN flood attack is true?

A. A distributed SYN flood attack is carried out only by the valid address.

B. A distributed SYN flood attack is carried out only by spoofed addresses.

C. Botnet could be used to launch a distributed SYN flood attack.

D. A distributed SYN flood attack does not completely deplete TCBs SYN-Received state backlog.

E. A distributed SYN flood attack is the most effective SYN flood attack because it targets server memory.

Correct Answer: C

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

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

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.