Vendor: CISCO

Exam Code: 350-018

Exam Name: CCIE Pre-Qualification Test for Security
QUESTION 1
Which two of these commands are required to implement a Cisco Catalyst 6500 Series Firewall Services Module (FWSM) in a Catalyst 6500 running Cisco IOS? (Choose two.)

A. firewall multiple-vlan-interfaces
B. firewall module vlan-group
C. module secure-traffic
D. firewall vlan-group <vlan-x>
E. firewall module secure-traffic

Answer: BD

QUESTION 2
A DNS Client sends DNS messages to obtain information about the requested domain name space. The information is known as which of these?

A. Resource Record
B. Resolver
C. Branch
D. Authoritative Client
E. Recursive Client

Answer: A

QUESTION 3
Which three of these are performed by both RADIUS and TACACS+ servers? (Choose three.)

A. login authentication
B. EXEC authorization
C. command authorization
D. EXEC accounting
E. command accounting

Answer: ABD

QUESTION 4
You are trying to set up a site-to-site IPsec tunnel between two Cisco ASA adaptive security appliances, but you are not able to pass traffic. You try to troubleshoot the issue by enabling debug crypto isakmp and see the following messages:

CiscoASA# debug crypto isakmp

[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy

[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, QM FSM error (P2 struct &0xb0cf31e8, mess id 0x97d965e5)!

[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Removing peer from correlator table failed, no match!

What could be the potential problem?

A. The policy group mapped to the site-to-site tunnel group is configured to use both IPsec and SSL VPN tunnels.
B. The policy group mapped to the site-to-site tunnel group is configured to use both IPsec and L2TP over IPsec tunnels.
C. The policy group mapped to the site-to-site tunnel group is configured to just use the SSL VPN tunnel.
D. The site-to-site tunnel group is configured to use both IPsec and L2TP over IPsec tunnels.
E. The site-to-site tunnel group is configured to just use the SSL VPN tunnel.

Answer: C

QUESTION 5
What does the "authoritative" flag in the show ip nhrp command output indicate?

A. It indicates that the information was learned from the source mapping information of an NHRP resolution request received by the local router, or from an NHRP resolution packet being forwarded through the local router.
B. It indicates an NHRP mapping entry for networks local to this router for which this
router has answered an NHRP resolution request.

C. It indicates that the NHRP information was obtained from the next-hop server or router that maintains the NBMA-to-IP address mapping for a particular destination.

D. It indicates that this NHRP mapping entry must be unique; it cannot be overwritten with a mapping entry that has the same IP address but a different NBMA address.

**Answer:** C

**QUESTION 6**
You configured two routers for EBGP, but you see your BGP neighbor’s state is Active after issuing the show ip bgp neighbor command. Which three of these could be reasons? (Choose three.)

A. The EBGP neighbor is two hops away, but the neighbor ttl-security command was not configured.

B. The EBGP neighbor is two hops away, but the neighbor ebgp-multihop command was not configured.

C. The EBGP neighbor is two hops away, but the neighbor disable connected-check command was not configured.

D. One router is configured for version 4, but the other router is configured for version 6.

E. The EBGP neighbor password is incorrect.

**Answer:** ABE

**QUESTION 7**
Which of these authentication combinations would provide the highest level of security for an IPsec remote-access VPN client?

A. pre-shared key and xauth (RADIUS server)

B. certificate and xauth (local server)

C. certificate and xauth (RSA SecurID token)

D. pre-shared key and xauth (RSA SecurID token)

E. pre-shared key and xauth (local server)

F. certificate and xauth (RADIUS server)
QUESTION 8
What is the default username and password set for Cisco Security Device Manager (SDM)?

A. sdm/sdm
B. sdm/cisco
C. cisco/sdm
D. cisco/cisco
E. cisco/cisco123

Answer: D

QUESTION 9
Refer to the Exhibit. Switch SW2 has just been added to FastEthernet 0/23 on SW1. After a few seconds, interface Fa0/23 on SW1 is placed in the error-disabled state. SW2 is removed from port 0/23 and inserted into SW1 port Fa0/22 with the same result. What is the most likely cause of this problem?

A. PAgP is unable to correctly negotiate VLAN trunk characteristics on the link between SW1 and SW2.
B. BPDU filtering has been enabled either globally or on the interfaces of SW1.
C. The spanning-tree portfast feature has been configured on SW1.

A. PAgP is unable to correctly negotiate VLAN trunk characteristics on the link between SW1 and SW2.
D. The BPDU guard feature has been enabled on the FastEthernet interfaces of SW1.
E. The FastEthernet interfaces of SW1 are unable to auto-negotiate speed and duplex with SW2.

Answer: D

QUESTION 10
Which is a benefit of implementing RFC 2827?

A. Prevents Dos from legitimate, non-hostile end systems
B. Prevents disruption of “special services”, such as Mobile IP
C. Allows DHCP or BOOTP packets to reach the relay agents as appropriate
D. Restricts directed broadcasts at the ingress router
E. Defeats Dos attacks which employ IP Source Address Spoofing

Answer: E

QUESTION 11
Which of the following is the correct diagram for an IPsec Authentication Header?
Answer: C

QUESTION 12
Which two of followings are correct regarding the Cisco Trust Agent (CTA)? (Choose two.)

A. Includes both a Layer 3 communication component using EAP over UDP, as well as an 802.1x supplicant, allowing layer 2 EAP over LAN communications.
B. Can communicate the Cisco Security Agent (CSA) version, OS and patch version, as well as the presence, version, and other posture information of third-party applications that are part of the NAC initiative to the Authentication Server.
C. Provides the capability at the endpoint to apply QoS markings to application network traffic as specified by Cisco Trust Agent policy rules.
D. Resides between the applications and the Operating System Kernel to prevent day zero attacks.
E. Available on Windows operating systems only.

Answer: AB

QUESTION 13
With the Cisco's IOS Authentication Proxy feature, users can initiate network access via which three protocols? (Choose three)

A. HTTP/HTTPS
B. L2TP
C. TELNET
D. IPSec
E. SSH
F. FTP

Answer: ACF

QUESTION 14
With the following GRE tunnel configuration, how many bytes of GRE overhead does encapsulation add to the original data packet?

interface Tunnel0

ip address 1.1.1.1 255.255.255.252

tunnel source Ethernet0/0
tunnel destination 2.2.2.2

tunnel key 1234

A. 32 bytes
B. 24 bytes
C. 28 bytes
D. 20 bytes

**Answer:** C

**QUESTION 15**
Which of the following is an example of a security technology that could be enabled by Netflow?

A. SYN Cookies
B. Content filtering
C. Anti-X Protection
D. Anomaly Detection
E. Anti Virus
F. Application Inspection

**Answer:** D

**QUESTION 16**
Referring to the DMVPN topology diagram shown in the exhibit, which two statements are
A. At the Spoke A router, the next-hop to reach the 192.168.0.0/24 network should be 172.17.0.1
B. Before a spoke-to-spoke tunnel can be built, the spoke router needs to send NHRP query to the hub to resolve the remote spoke router physical interface ip address
C. The spoke routers act as the NHRP servers for resolving the remote spoke physical interface ip address
D. At the Spoke A router, the next-hop to reach the 192.168.2.0/24 network should be 10.0.0.1
E. The hub router tunnel interface must have EIGRP next-hop-self enabled
F. The hub router needs to have EIGRP split horizon disabled

Answer: BF

**QUESTION 17**
A network administrator is using a LAN analyzer to troubleshoot OSPF router exchange messages sent to ALL OSPF ROUTERS. To what MAC address are these messages sent?
QUESTION 18
To increase security, MD5 authentication is added to an OSPF virtual link. Company security policies dictate that all passwords must be changed after 90 days. What will be the effect on the OSPF network of changing the MD5 key?

A. A second MD5-authenticated virtual link should be created. Once that is operational, the old virtual link can be removed.
B. Once a MD5 key is configured a hash is created. For security purposes, this hash can only be removed by clearing the MD5 configuration and resetting the OSPF adjacency.
C. A new MD5 key can be configured after removing the old one. This will momentarily disable MD5 authentication until the new key is learned in updated LSAs.
D. If a second MD5 key is configured OSPF will authenticated both keys allowing the first key to be removed with no effect on OSPF
E. If a new MD5 key is configured using the same key-id, it automatically replaces the existing one with no effect on OSPF

Answer: D

QUESTION 19
Which three steps are required to enable SSH Server on an IOS router? (Choose three)

A. Configure a domain name
B. Configure a host name
C. Specifies a fingerprint that can be matched against the fingerprint of a CA certificate
during authentication.
D. Generate an RSA key pair.
E. Configure the Crypto PKI trustpoint (CA)
F. Import the SSH client fingerprint.

**Answer:** ABD

**QUESTION 20**

access-list 111 permit udp any any eq 1434

class-map match-all bad_worm

match access-group 111

match packet length min 404 max 404

policy-map drop-bad-worm

class bad-worm

police 1000000 22250 22250 conform-action drop exceed-action drop violate-action drop

Taking into consideration the shown configuration, what kind of attack are we attempting to mitigate?

A. Smurf Attack
B. Code Red Worm
C. This is not valid configuration.
D. MSQL and JavaScript attack
E. SQL Slammer Worm

**Answer:** E