



Exam : **350-018**

Title : CCIE Pre-Qualification Test
for Security

Version : Demo

1. In an L2TP voluntary tunneling scenario, the VPDN tunnel is terminated between:

- A. The client and the NAS.
- B. The NAS and the LNS.
- C. The NAS and the LAC.
- D. The client and the LNS.

Answer: D

2. Which IOS QoS mechanism is used strictly to rate limit traffic destined to the router itself?

- A. Class-Based Policing
- B. Control Plane Policing
- C. Dual-Rate Policing
- D. Single-Rate Policing.

Answer: B

3. What are two key characteristics of VTP? (Choose 2)

- A. VTP messages are sent out all switch-switch connections.
- B. VTP L2 messages are communicated to neighbors using CDP.
- C. VTP manages addition, deletion, and renaming of VLANs 1 to 4094.
- D. VTP pruning restricts flooded traffic, increasing available bandwidth.
- E. VTP V2 can only be used in a domain consisting of V2 capable switches.
- F. VTP V2 performs consistency checks on all sources of VLAN information.

Answer: DE

4. 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?

- A. 00-00-1C-EF-00-00
- B. 01-00-5E-00-00-05
- C. 01-00-5E-EF-00-00
- D. EF-FF-FF-00-00-05
- E. EF-00-00-FF-FF-FF

F. FF-FF-FF-FF-FF-FF

Answer: B

5. What is Chain of Evidence in the context of security forensics?

- A. The concept that evidence is controlled in locked down, but not necessarily authenticated.
- B. The concept that evidence is controlled and accounted for as to not disrupt its authenticity and integrity.
- C. The concept that the general whereabouts of evidence is known.
- D. The concept that if a person has possession of evidence someone knows where the evidence is and can say who had it if it is not logged

Answer: B

6. In most buffer overflow attacks, which of the following behavior should be expected?

- A. A vulnerability used to overflow the buffer and an exploit used to run malicious software off of the stack.
- B. An exploit used to overflow the buffer and a vulnerability used to run malicious software off of the stack.
- C. A single crafted packet to overflow the buffer and run malicious software.
- D. Shell code to exploit the buffer.

Answer: A

7. Which of the following is the most effective technique to prevent source IP Address spoofing?

- A. policy based routing (PBR)
- B. unicast reverse path forwarding (uRPF)
- C. lock and key ACL
- D. RFC 1918 filtering
- E. IP source routing

Answer: B

8. Whenever a failover takes place on the ASA (configured for failover), all active connections are dropped and clients must re-establish their connections unless:(Choose 2)

- A. The ASA is configured for Active-Standby failover.
- B. The ASA is configured for Active-Active failover.
- C. The ASA is configured for Active-Active failover and a state failover link has been configured.

- D. The ASA is configured for Active-Standby failover and a state failover link has been configured.
- E. The ASA is configured to use a serial cable as failover link.
- F. The ASA is configured for LAN-Based failover.

Answer: CD

9. CSA protects your host by:

- A. Preventing browsers from opening network sockets in listening state.
- B. Preventing buffer overflows.
- C. Preventing users from entering unencrypted passwords.
- D. Preventing browsers from acting as client to web servers.

Answer: A

10. Which three statements regarding Cisco ASA multicast routing support are correct? (Choose three.)

- A. ASA supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single security appliance.
- B. When configured for stub multicast routing, the ASA can act as the Rendezvous Point (RP)
- C. If the ASA detects IGMP version 1 routers, the ASA will automatically switch to IGMP version 1 operations.
- D. The ASA supports both PIM-SM and bi-directional PIM.
- E. Enabling multicast routing globally on the ASA automatically enables PIM and IGMP on all interfaces.
- F. The ASA can be configured for IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring the multicast traffic to be forwarded only those interfaces associated with hosts requesting the multicast group.

Answer: ADE

11. Which of the following is true for RFC 4301 - Security Architecture for the Internet Protocol (obsoletes RFC 2401) - (Select two).

- A. Specifies the Security Architecture for the Internet.
- B. Specifies the base architecture for Key Management, the Internet Key Exchange (IKE)
- C. Specifies the base architecture for IPsec-compliant systems.
- D. Designed to provide security services for traffic at the IP layer, in the IPv4 environment only.

E. Designed to provide security services for traffic at the IP layer, in both the IPv4 and IPv6 environments

Answer: CE

12. Which access control model provides access to system resources based on the job function of the user or the tasks that the user has been assigned?

- A. Discretionary Access Control
- B. Mandatory Access Control
- C. Role Based Access Control
- D. Context Based Access Control
- E. Rule Based Access Control

Answer: C

13. What does qos pre-classify provides in regard to implementing QoS over GRE/IPSec VPN tunnels?

- A. enables IOS to copy the ToS field from the inner (original) IP header to the outer tunel IP header.
- B. enables IOS to make a copy of the inner (original) IP header and to run a QoS classification before encryption, based on fields in the inner IP header.
- C. enables IOS to classify packets based on the ToS field in the inner (original) IP header.
- D. enables IOS to classify packets based on the ToS field in the outer tunnel IP header.
- E. enables the IOS classification engine to only see a single encrypted and tunneled flow to reduce classification complexity.

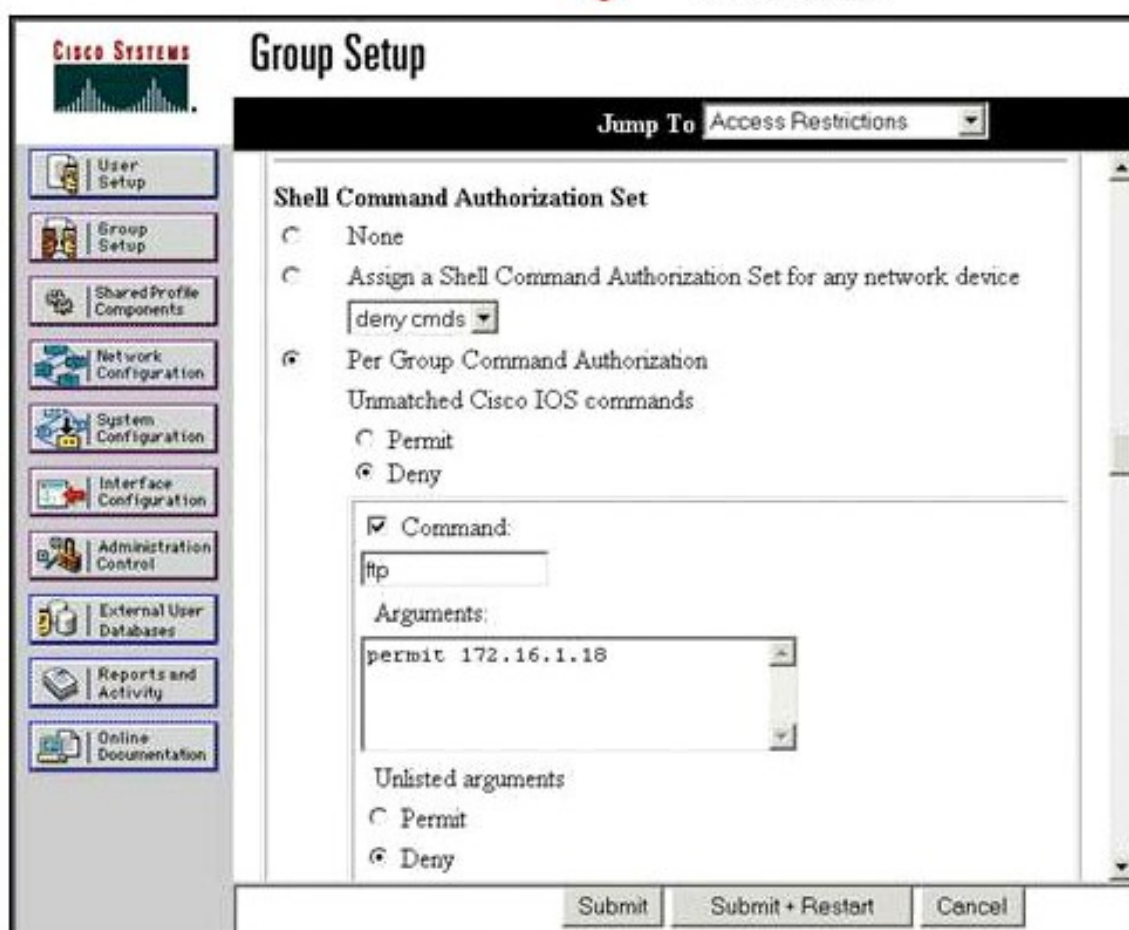
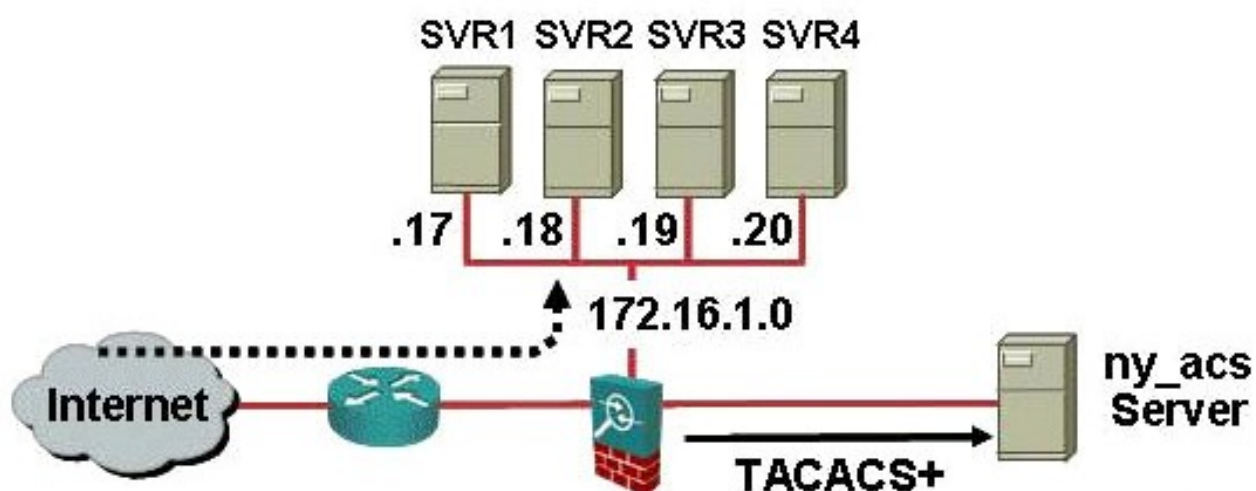
Answer: B

14. Which two steps does a receiver perform to validate a message using HMAC? (Choose two.)

- A. decrypts the received MAC using a secret key.
- B. compares the computed MAC vs. the MAC received.
- C. authenticate the received message using the sender's public key.
- D. look up the sender's public key.
- E. extracts the MAC from the received message then encrypts the received message with a secret key to produce the MAC
- F. Computes the MAC using the received message and a secret key as inputs to the hash function.

Answer: BF

15. Refer to network diagram in the exhibit. There are four servers on the DMZ. All servers are capable of supporting both FTP and HTTP applications. When a remote user accesses the security appliance and is authenticated, according to the group configuration in the ny_acs server, a remote user from this group is authorized to perform what two actions? (Choose 2)



- A. Access any server on the DMZ.
- B. Access any FTP server on the DMZ.
- C. Access "SVR 2" only
- D. Utilize FTP and HTTP protocols
- E. Utilize HTTP only

F. Utilize FTP only

Answer: CF

16. Referring to the debug output shown below, what is causing the IKE Main Mode failure?

1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0

1d00h: ISAKMP (0:1): no offers accepted!

1d00h: ISAKMP (0:1): SA not acceptable!

1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer at 150.150.150.1

- A. The IPsec transform set on the peers do not match.
- B. The Crypto ACL is not a mirror image of the peer.
- C. The pre-shared keys on the peers do not match.
- D. The IKE Phase I policy does not match on both sides.
- E. The received IPsec packet specifies a Security Parameters Index (SPI) that does not exist in the security associations database (SADB).

Answer: D

17. 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. 20 bytes
- B. 24 bytes
- C. 28 bytes
- D. 32 bytes

Answer: C

18. With NetFlow configured and several IPS, switches, routers and firewall devices imported into its

database, CS-MARS will provide which of the following security features? (Choose 4)

- A. Event correlation to help identify attacks
- B. Identification of hosts that generate abnormal amounts of traffic.
- C. Identify which hosts have CSA installed.
- D. Make mitigation recommendations to stop attacks.
- E. Draw a topology of your network.
- F. Pull SNMP traps from different devices.

Answer: ABDE

19. When implementing best practices for IP Source Address Spoofing and Defeating Denial of Service Attacks with IP Source Address Spoofing, what RFC is commonly used to protect your network?

- A. RFC 1149
- B. RFC 3704
- C. RFC 1918
- D. RFC 2827

Answer: D

20. What is the net effect of using ICMP Type 4 messages to attack RFC 1122 compliant hosts?

- A. Hosts will perform a "soft" TCP reset and restart the connection.
- B. Hosts will perform a "hard" TCP reset and tear down the connection.
- C. Hosts will reduce the rate at which they inject traffic into the network.
- D. Hosts will redirect packets to the IP address indicated in the ICMP type 4 message.
- E. Hosts will retransmit the last frame sent prior to receiving the ICMP type 4 message.

Answer: C