

Cisco

Exam 351-018

CCIE Security Exam (4.0)

Version: 25.0

[Total Questions: 507]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	107

Topic 1, Volume A**Question No : 1 - (Topic 1)**

Which two security measures are provided when you configure 802.1X on switchports that connect to corporate-controlled wireless access points? (Choose two.)

- A. It prevents rogue APs from being wired into the network.
- B. It provides encryption capability of data traffic between APs and controllers.
- C. It prevents rogue clients from accessing the wired network.
- D. It ensures that 802.1x requirements for wired PCs can no longer be bypassed by disconnecting the AP and connecting a PC in its place.

Answer: A,D

Question No : 2 - (Topic 1)

An IPv6 multicast receiver joins an IPv6 multicast group using which mechanism?

- A. IGMPv3 report
- B. IGMPv3 join
- C. MLD report
- D. general query
- E. PIM join

Answer: C

Question No : 3 - (Topic 1)

DNSSEC was designed to overcome which security limitation of DNS?

- A. DNS man-in-the-middle attacks
- B. DNS flood attacks
- C. DNS fragmentation attacks
- D. DNS hash attacks
- E. DNS replay attacks
- F. DNS violation attacks

Answer: A

Question No : 4 - (Topic 1)

Which three statements are true about the transparent firewall mode in Cisco ASA?
(Choose three.)

- A. The firewall is not a routed hop.
- B. The firewall can connect to the same Layer 3 network on its inside and outside interfaces.
- C. Static routes are supported.
- D. PAT and NAT are not supported.
- E. Only one global address per device is supported for management.
- F. SSL VPN is supported for management.

Answer: A,B,C

Question No : 5 - (Topic 1)

With the Cisco FlexVPN solution, which four VPN deployments are supported? (Choose four.)

- A. site-to-site IPsec tunnels?
- B. dynamic spoke-to-spoke IPsec tunnels? (partial mesh)
- C. remote access from software or hardware IPsec clients?
- D. distributed full mesh IPsec tunnels?
- E. IPsec group encryption using GDOI?
- F. hub-and-spoke IPsec tunnels?

Answer: A,B,C,F

Question No : 6 - (Topic 1)

Which statement is true about the Cisco NEAT 802.1X feature?

- A. The multidomain authentication feature is not supported on the authenticator switch interface.

- B.** It allows a Cisco Catalyst switch to act as a supplicant to another Cisco Catalyst authenticator switch.
- C.** The supplicant switch uses CDP to send MAC address information of the connected host to the authenticator switch.
- D.** It supports redundant links between the supplicant switch and the authenticator switch.

Answer: B

Question No : 7 - (Topic 1)

Which type of VPN is based on the concept of trusted group members using the GDOI key management protocol?

- A.** DMVPN
- B.** SSLVPN
- C.** GETVPN
- D.** EzVPN
- E.** MPLS VPN
- F.** FlexVPN

Answer: C

Question No : 8 - (Topic 1)

Refer to the exhibit.

```
vtp mode transparent
!
vlan 600
  private-vlan community
vlan 400
  private-vlan isolated
vlan 200
  private-vlan primary
  private-vlan association 400,600
!
interface FastEthernet 5/1
  switchport mode private-vlan host
  switchport private-vlan host-association 200 400
!
interface FastEthernet 5/2
  switchport mode private-vlan host
  switchport private-vlan host-association 200 600
!
interface FastEthernet 5/3
  switchport mode private-vlan host
  switchport private-vlan host-association 200 600
!
Interface FastEthernet 5/4
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 200 400,600
!
```

Which two statements about this Cisco Catalyst switch configuration are correct? (Choose two.)

- A. The default gateway for VLAN 200 should be attached to the FastEthernet 5/1 interface.
- B. Hosts attached to the FastEthernet 5/1 interface can communicate only with hosts attached to the FastEthernet 5/4 interface.
- C. Hosts attached to the FastEthernet 5/2 interface can communicate with hosts attached to the FastEthernet 5/3 interface.
- D. Hosts attached to the FastEthernet 5/4 interface can communicate only with hosts attached to the FastEthernet 5/2 and FastEthernet 5/3 interfaces.
- E. Interface FastEthernet 5/1 is the community port.

F. Interface FastEthernet 5/4 is the isolated port.

Answer: B,C

Question No : 9 - (Topic 1)

Which IPv6 tunnel type is a standard that is defined in RFC 4214?

- A. ISATAP
- B. 6to4
- C. GREv6
- D. manually configured

Answer: A

Question No : 10 - (Topic 1)

Which configuration implements an ingress traffic filter on a dual-stack ISR border router to prevent attacks from the outside to services such as DNSv6 and DHCPv6?

A. !

```
ipv6 access-list test
deny ipv6 FF05::/16 any
deny ipv6 any FF05::/16
! output omitted
permit ipv6 any any
!
```

B. !

```
ipv6 access-list test
permit ipv6 any FF05::/16
! output omitted
deny ipv6 any any
!
```

C. !

```
ipv6 access-list test
deny ipv6 any any eq dns
deny ipv6 any any eq dhcp
! output omitted
permit ipv6 any any
!
```

D. !

```
ipv6 access-list test
deny ipv6 any 2000::/3
! output omitted
permit ipv6 any any
!
```

E. !

```
ipv6 access-list test
deny ipv6 any FE80::/10
! output omitted
permit ipv6 any any
!
```

Answer: A

Question No : 11 - (Topic 1)

Which layer of the OSI reference model typically deals with the physical addressing of interface cards?

- A. physical layer
- B. data-link layer
- C. network layer
- D. host layer

Answer: B

Question No : 12 - (Topic 1)

If a host receives a TCP packet with an SEQ number of 1234, an ACK number of 5678, and a length of 1000 bytes, what will it send in reply?

- A. a TCP packet with SEQ number: 6678, and ACK number: 1234
- B. a TCP packet with SEQ number: 2234, and ACK number: 5678
- C. a TCP packet with SEQ number: 1234, and ACK number: 2234
- D. a TCP packet with SEQ number: 5678, and ACK number 2234

Answer: D

Question No : 13 - (Topic 1)

Which traffic class is defined for non-business-relevant applications and receives any bandwidth that remains after QoS policies have been applied?

- A. scavenger class
- B. best effort
- C. discard eligible
- D. priority queued

Answer: A

Question No : 14 - (Topic 1)

Which three statements are true about PIM-SM operations? (Choose three.)

- A. PIM-SM supports RP configuration using static RP, Auto-RP, or BSR.
- B. PIM-SM uses a shared tree that is rooted at the multicast source.
- C. Different RPs can be configured for different multicast groups to increase RP scalability.
- D. Candidate RPs and RP mapping agents are configured to enable Auto-RP.
- E. PIM-SM uses the implicit join model.

Answer: A,C,D

Question No : 15 - (Topic 1)

What are two benefits of using IKEv2 instead of IKEv1 when deploying remote-access IPsec VPNs? (Choose two.)

- A. IKEv2 supports EAP authentication methods as part of the protocol.
- B. IKEv2 inherently supports NAT traversal.
- C. IKEv2 messages use random message IDs.
- D. The IKEv2 SA plus the IPsec SA can be established in six messages instead of nine messages.
- E. All IKEv2 messages are encryption-protected.

Answer: A,B

Question No : 16 - (Topic 1)

Which of the following best describes Chain of Evidence in the context of security forensics?

- A. Evidence is locked down, but not necessarily authenticated.
- B. Evidence is controlled and accounted for to maintain its authenticity and integrity.
- C. The general whereabouts of evidence is known.
- D. Someone knows where the evidence is and can say who had it if it is not logged.

Answer: B

Question No : 17 - (Topic 1)

Which two IPv6 tunnel types support only point-to-point communication? (Choose two.)

- A. manually configured
- B. automatic 6to4
- C. ISATAP
- D. GRE

Answer: A,D

Question No : 18 - (Topic 1)

Refer to the exhibit.