Cisco

Exam 350-018v4

CCIE Security Exam (4.0)

Version: 22.0

[Total Questions: 490]

Topic 1, Volume A

Question No : 1 - (Topic 1)

In order to reassemble IP fragments into a complete IP datagram, which three IP header fields are referenced by the receiver? (Choose three.)

A. don't fragment flag
B. packet is fragmented flag
C. IP identification field
D. more fragment flag
E. number of fragments field
F. fragment offset field

Answer: C,D,F

Question No : 2 - (Topic 1)

Which VTP mode allows the Cisco Catalyst switch administrator to make changes to the VLAN configuration that only affect the local switch and are not propagated to other switches in the VTP domain?

A. transparent
B. server
C. client
D. local
E. pass-through

Answer: A

Question No : 3 - (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 : 4 - (Topic 1)

Based on RFC 4890, what is the ICMP type and code that should never be dropped by the firewall to allow PMTUD?

A. ICMPv6 Type 1 – Code 0 – no route to host
B. ICMPv6 Type 1 – Code 1 – communication with destination administratively prohibited
C. ICMPv6 Type 2 – Code 0 – packet too big
D. ICMPv6 Type 3 – Code 1 – fragment reassembly time exceeded
E. ICMPv6 Type 128 – Code 0 – echo request
F. ICMPv6 Type 129 – Code 0 – echo reply

Answer: C

Question No : 5 - (Topic 1)

A firewall rule that filters on the protocol field of an IP packet is acting on which layer of the OSI reference model?

A. network layer
B. application layer
C. transport layer
D. session layer

Answer: A

Question No : 6 - (Topic 1)

Which layer of the OSI model is referenced when utilizing http inspection on the Cisco ASA to filter Instant Messaging or Peer to Peer networks with the Modular Policy Framework?

A. application layer
B. presentation layer
C. network layer
D. transport layer

Answer: A

Question No : 7 - (Topic 1)

When a Cisco IOS Router receives a TCP packet with a TTL value less than or equal to 1, what will it do?

A. Route the packet normally
B. Drop the packet and reply with an ICMP Type 3, Code 1 (Destination Unreachable, Host Unreachable)
C. Drop the packet and reply with an ICMP Type 11, Code 0 (Time Exceeded, Hop Count Exceeded)
D. Drop the packet and reply with an ICMP Type 14, Code 0 (Timestamp Reply)

Answer: C

Question No : 8 - (Topic 1)

In an 802.11 WLAN, which option is the Layer 2 identifier of a basic service set, and also is typically the MAC address of the radio of the access point?

A. BSSID
B. SSID
C. VBSSID
D. MBSSID

Answer: A

Question No : 9 - (Topic 1)

What term describes an access point which is detected by your wireless network, but is not a trusted or managed access point?

A. rogue

B. unclassified

C. interferer

D. malicious

Answer: A

Question No : 10 - (Topic 1)

A router has four interfaces addressed as 10.1.1.1/24, 10.1.2.1/24, 10.1.3.1/24, and 10.1.4.1/24. What is the smallest summary route that can be advertised covering these four subnets?

A. 10.1.2.0/22

B. 10.1.0.0/22

C. 10.1.0.0/21

D. 10.1.0.0/16

Answer: C

Question No : 11 - (Topic 1)

Which two address translation types can map a group of private addresses to a smaller group of public addresses? (Choose two.)

A. static NAT

B. dynamic NAT

C. dynamic NAT with overloading

D. PAT

E. VAT

Answer: C,D

Question No : 12 - (Topic 1)

Which authentication mechanism is available to OSPFv3?

A. simple passwords

B. MD5

C. null

D. IKEv2

E. IPsec AH/ESP

Answer: E

Question No : 13 - (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 : 14 - (Topic 1)

Which two EIGRP packet types are considered to be unreliable packets? (Choose two.)

A. update

B. query

C. reply

D. hello

E. acknowledgement

Answer: D,E

Question No : 15 - (Topic 1)

Before BGP update messages may be sent, a neighbor must stabilize into which neighbor state?

A. Active

B. Idle
C. Connected
D. Established

Answer: D

**Question No : 16 - (Topic 1)**

Which three statements are correct when comparing Mobile IPv6 and Mobile IPv4 support? (Choose three.)

A. Mobile IPv6 does not require a foreign agent, but Mobile IPv4 does.
B. Mobile IPv6 supports route optimization as a fundamental part of the protocol; IPv4 requires extensions.
C. Mobile IPv6 and Mobile IPv4 use a directed broadcast approach for home agent address discovery.
D. Mobile IPv6 makes use of its own routing header; Mobile IPv4 uses only IP encapsulation.
E. Mobile IPv6 and Mobile IPv4 use ARP for neighbor discovery.
F. Mobile IPv4 has adopted the use of IPv6 ND.

Answer: A,B,D

Question No : 17 - (Topic 1)

Refer to the exhibit.
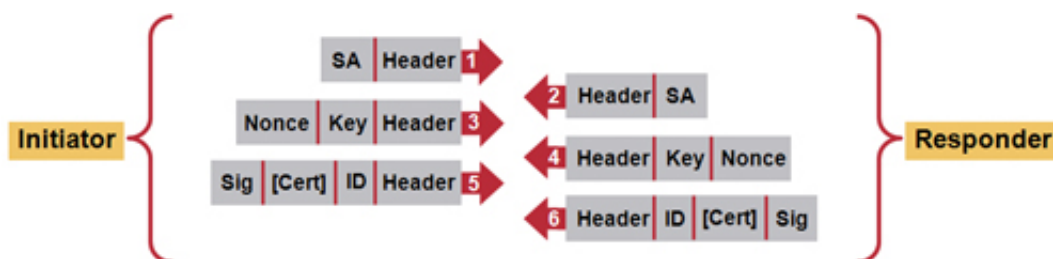
- MSG 1:   Initiator offers acceptable encryption and authentication algorithms (3DES, MD5, and RSA, which is also called the transform-set)
- MSG 2:   Responder presents acceptance of the proposal (or it might not)
- MSG 3:   Initiator Diffie-Helman key and nounce (the key value is usually a number of 1024-bit length)
- MSG 4:   Responder Diffie-Helman key and nounce
- MSG 5:   Initiator signature, ID, and keys (maybe cert), which is also known as authentication data
- MSG 6:   Responder signature, ID, and keys (maybe cert)

Which message could contain an authenticated initial_contact notify during IKE main mode negotiation?

A. message 3

B. message 5

C. message 1

D. none, initial_contact is sent only during quick mode

E. none, notify messages are sent only as independent message types

Answer: B

Question No : 18 - (Topic 1)

Which protocol does 802.1X use between the supplicant and the authenticator to authenticate users who wish to access the network?

A. SNMP

B. TACACS+

C. RADIUS

D. EAP over LAN

E. PPPoE

Answer: D

Question No : 19 - (Topic 1)

Which two statements are correct regarding the AES encryption algorithm? (Choose two.)

A. It is a FIPS-approved symmetric block cipher.

B. It supports a block size of 128, 192, or 256 bits.

C. It supports a variable length block size from 16 to 448 bits.

D. It supports a cipher key size of 128, 192, or 256 bits.

E. The AES encryption algorithm is based on the presumed difficulty of factoring large integers.

Answer: A,D

Question No : 20 - (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 : 21 - (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 : 22 - (Topic 1)

Which three statements are true about MACsec? (Choose three.)

A. It supports GCM modes of AES and 3DES.
B. It is defined under IEEE 802.1AE.
C. It provides hop-by-hop encryption at Layer 2.
D. MACsec expects a strict order of frames to prevent anti-replay.
E. MKA is used for session and encryption key management.
F. It uses EAP PACs to distribute encryption keys.

Answer: B,C,E

Question No : 23 - (Topic 1)

Which SSL protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment?

A. SSL Handshake Protocol
B. SSL Alert Protocol
C. SSL Record Protocol
D. SSL Change CipherSpec Protocol

Answer: C

Question No : 24 - (Topic 1)

IPsec SAs can be applied as a security mechanism for which three options? (Choose three.)

A. Send
B. Mobile IPv6
C. site-to-site virtual interfaces
D. OSPFv3
E. CAPWAP
F. LWAPP

Answer: B,C,D

Question No : 25 - (Topic 1)

Which four options are valid EAP mechanisms to be used with WPA2? (Choose four.)

A. PEAP
B. EAP-TLS
C. EAP-FAST
D. EAP-TTLS
E. EAPOL
F. EAP-RADIUS
G. EAP-MD5