

Cisco 351-018



CCIE Security Exam v4.0

Version: 5.0

QUESTION NO: 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

Explanation:

QUESTION NO: 2

Which multicast routing mechanism is optimal to support many-to-many multicast applications?

- A. PIM-SM
- B. MOSPF
- C. DVMRP
- D. BIDIR-PIM
- E. MSDP

Answer: D

Explanation:

QUESTION NO: 3

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

Explanation:

QUESTION NO: 4

Which three statements regarding VLANs are true? (Choose three.)

- A.** To create a new VLAN on a Cisco Catalyst switch, the VLAN name, VLAN ID and VLAN type must all be specifically configured by the administrator.
- B.** A VLAN is a broadcast domain.
- C.** Each VLAN must have an SVI configured on the Cisco Catalyst switch for it to be operational.
- D.** The native VLAN is used for untagged traffic on an 802.1Q trunk.
- E.** VLANs can be connected across wide-area networks.

Answer: B,D,E

Explanation:

QUESTION NO: 5

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

Explanation:

QUESTION NO: 6

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

Explanation:

QUESTION NO: 7

Which technology, configured on the Cisco ASA, allows Active Directory authentication credentials to be applied automatically to web forms that require authentication for clientless SSL connections?

- A. one-time passwords
- B. certificate authentication
- C. user credentials obtained during authentication
- D. Kerberos authentication

Answer: C

Explanation:

QUESTION NO: 8

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

Explanation:

QUESTION NO: 9

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

Explanation:

QUESTION NO: 10

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

Explanation:

QUESTION NO: 11

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

Explanation:

QUESTION NO: 12

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

Explanation:

QUESTION NO: 13

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

Explanation:

QUESTION NO: 14

In what subnet does address 192.168.23.197/27 reside?

- A. 192.168.23.0
- B. 192.168.23.128
- C. 192.168.23.160
- D. 192.168.23.192
- E. 192.168.23.196

Answer: D

Explanation:

QUESTION NO: 15

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

Explanation:

QUESTION NO: 16

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

Explanation:

QUESTION NO: 17

Given the IPv4 address 10.10.100.16, which two addresses are valid IPv4-compatible IPv6 addresses? (Choose two.)

- A. ::A:A:64:10
- B. ::10:10:100:16
- C. 0:0:0:0:0:10:10:100:16
- D. 0:0:10:10:100:16:0:0:0

Answer: B,C

Explanation:

QUESTION NO: 18

Which authentication mechanism is available to OSPFv3?

- A. simple passwords
- B. MD5
- C. null
- D. IKEv2
- E. IPsec AH/ESP

Answer: E

Explanation:

QUESTION NO: 19

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

Explanation:

QUESTION NO: 20

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

Explanation:

QUESTION NO: 21

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

Explanation:

QUESTION NO: 22

What is the size of a point-to-point GRE header, and what is the protocol number at the IP layer?

- A. 8 bytes, and protocol number 74
- B. 4 bytes, and protocol number 47
- C. 2 bytes, and protocol number 71
- D. 24 bytes, and protocol number 1
- E. 8 bytes, and protocol number 47

Answer: B

Explanation:

QUESTION NO: 23

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

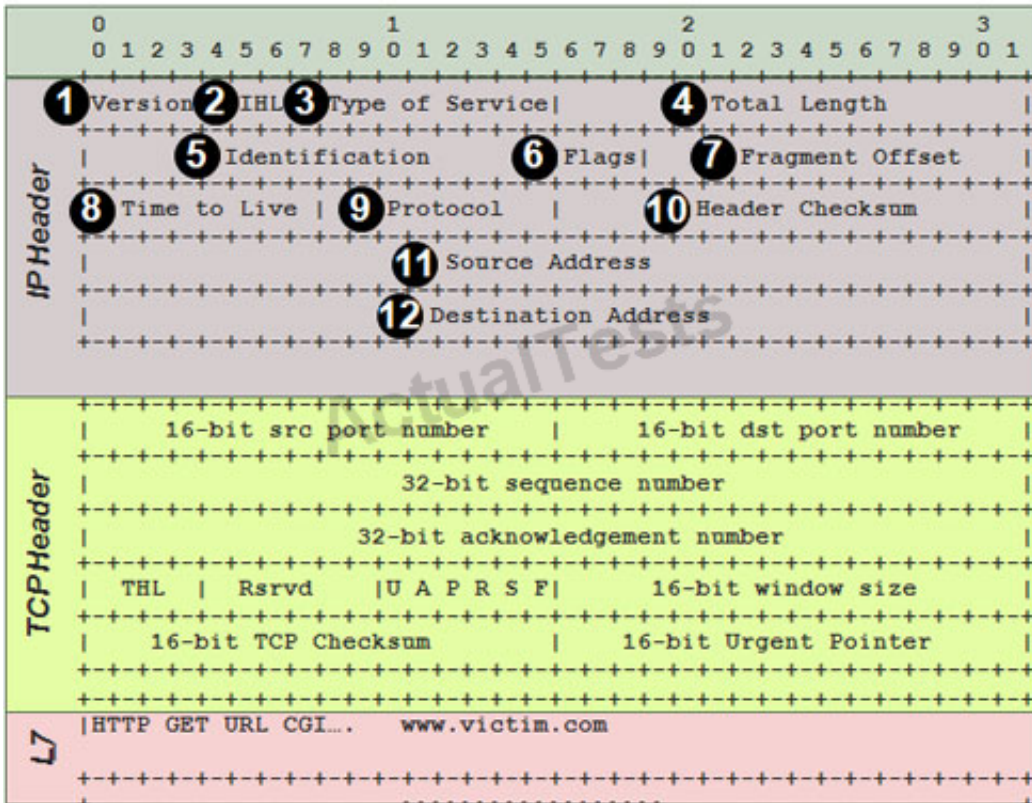
- A. Mobile IPv6 does not require a foreign agent, but Mobile IPv4 does.
- B. Mobile IPv6 supports route optimization as a fundamental part of the protocol; IPv4 requires extensions.
- C. Mobile IPv6 and Mobile IPv4 use a directed broadcast approach for home agent address discovery.
- D. Mobile IPv6 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

Explanation:

QUESTION NO: 24

Refer to the exhibit.



Which three fields of the IP header labeled can be used in a spoofing attack? (Choose one.)

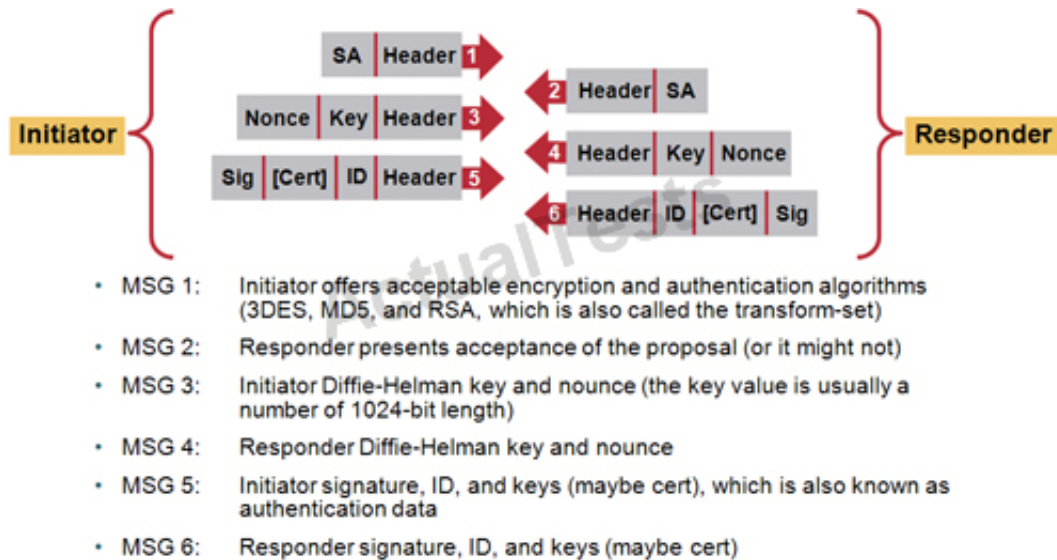
- A. 6,7,11
- B. 6,11,12
- C. 3,11,12
- D. 4,7,11

Answer: A

Explanation:

QUESTION NO: 25

Refer to the exhibit.



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

Explanation:

QUESTION NO: 26

When implementing WLAN security, what are three benefits of using the TKIP instead of WEP? (Choose three.)

- A. TKIP uses an advanced encryption scheme based on AES.
- B. TKIP provides authentication and integrity checking using CBC-MAC.
- C. TKIP provides per-packet keying and a rekeying mechanism.
- D. TKIP provides message integrity check.
- E. TKIP reduces WEP vulnerabilities by using a different hardware encryption chipset.
- F. TKIP uses a 48-bit initialization vector.

Answer: C,D,F

Explanation:

QUESTION NO: 27

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

Explanation:

QUESTION NO: 28

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

Explanation:

QUESTION NO: 29

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

Explanation:

QUESTION NO: 30

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

Explanation:

QUESTION NO: 31

Which two statements about SHA are correct? (Choose two.)

- A. Five 32-bit variables are applied to the message to produce the 160-bit hash.
- B. The message is split into 64-bit blocks for processing.
- C. The message is split into 512-bit blocks for processing.
- D. SHA-2 and MD5 both consist of four rounds of processing.

Answer: A,C

Explanation:

QUESTION NO: 32

Which three statements about IKEv2 are correct? (Choose three.)

- A. INITIAL_CONTACT is used to synchronize state between peers.
- B. The IKEv2 standard defines a method for fragmenting large messages.
- C. The initial exchanges of IKEv2 consist of IKE_SA_INIT and IKE_AUTH.
- D. Rekeying IKE and child SAs is facilitated by the IKEv2 CREATE_CHILD_SA exchange.
- E. NAT-T is not supported.
- F. Attribute policy push (via the configuration payload) is only supported in REQUEST/REPLY

mode.

Answer: A,C,D

Explanation:

QUESTION NO: 33

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

- A. LDAP uses UDP port 389 by default.
- B. LDAP is defined in terms of ASN.1 and transmitted using BER.
- C. LDAP is used for accessing X.500 directory services.
- D. An LDAP directory entry is uniquely identified by its DN.
- E. A secure connection via TLS is established via the UseTLS operation.

Answer: B,C,D

Explanation:

QUESTION NO: 34

Which two EAP methods may be susceptible to offline dictionary attacks? (Choose two.)

- A. EAP-MD5
- B. LEAP
- C. PEAP with MS-CHAPv2
- D. EAP-FAST

Answer: A,B

Explanation:

QUESTION NO: 35

Which PKCS is invoked during IKE MM5 and MM6 when digital certificates are used as the authentication method?

- A. PKCS#7
- B. PKCS#10

- C. PKCS#13
- D. PKCS#11
- E. PKCS#3

Answer: A

Explanation:

QUESTION NO: 36

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

Explanation:

QUESTION NO: 37

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

Explanation:

QUESTION NO: 38

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

Explanation:

QUESTION NO: 39

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

Answer: A,B,C,D

Explanation:

QUESTION NO: 40

Which three features describe DTLS protocol? (Choose three.)

- A. DTLS handshake does not support reordering or manage loss packets.
- B. DTLS provides enhanced security, as compared to TLS.
- C. DTLS provides block cipher encryption and decryption services.
- D. DTLS is designed to prevent man-in-the-middle attacks, message tampering, and message forgery.
- E. DTLS is used by application layer protocols that use UDP as a transport mechanism.
- F. DTLS does not support replay detection.

Answer: C,D,E

Explanation:

QUESTION NO: 41

Which three statements are true about the SSH protocol? (Choose three.)

- A. SSH protocol runs over TCP port 23.
- B. SSH protocol provides for secure remote login and other secure network services over an insecure network.
- C. Telnet is more secure than SSH for remote terminal access.
- D. SSH protocol runs over UDP port 22.
- E. SSH transport protocol provides for authentication, key exchange, confidentiality, and integrity.
- F. SSH authentication protocol supports public key, password, host based, or none as authentication methods.

Answer: B,E,F

Explanation:

QUESTION NO: 42

Which statement regarding TFTP is not true?

- A. Communication is initiated over UDP port 69.
- B. Files are transferred using a secondary data channel.
- C. Data is transferred using fixed-size blocks.
- D. TFTP authentication information is sent in clear text.
- E. TFTP is often utilized by operating system boot loader procedures.
- F. The TFTP protocol is implemented by a wide variety of operating systems and network devices.

Answer: D

Explanation:

QUESTION NO: 43

Which two statements are true when comparing ESMTP and SMTP? (Choose two.)

- A. Only SMTP inspection is provided on the Cisco ASA firewall.
- B. A mail sender identifies itself as only able to support SMTP by issuing an EHLO command to the mail server.
- C. ESMTP mail servers will respond to an EHLO with a list of the additional extensions they

support.

D. SMTP commands must be in upper case, whereas ESMTP can be either lower or upper case.

E. ESMTP servers can identify the maximum email size they can receive by using the SIZE command.

Answer: C,E

Explanation:

QUESTION NO: 44

How does a DHCP client request its previously used IP address in a DHCP DISCOVER packet?

A. It is included in the CIADDR field.

B. It is included as DHCP Option 50 in the OPTIONS field.

C. It is included in the YIADDR field.

D. It is the source IP address of the UDP/53 wrapper packet.

E. The client cannot request its last IP address; it is assigned automatically by the server.

Answer: B

Explanation:

QUESTION NO: 45

Which two statements about an authoritative server in a DNS system are true? (Choose two.)

A. It indicates that it is authoritative for a name by setting the AA bit in responses.

B. It has a direct connection to one of the root name servers.

C. It has a ratio of exactly one authoritative name server per domain.

D. It cannot cache or respond to queries from domains outside its authority.

E. It has a ratio of at least one authoritative name server per domain.

Answer: A,E

Explanation:

QUESTION NO: 46

User A at Company A is trying to transfer files to Company B, using FTP. User A can connect to the FTP server at Company B correctly, but User A cannot get a directory listing or upload files. The session hangs.

What are two possible causes for this problem? (Choose two.)

- A.** Active FTP is being used, and the firewall at Company A is not allowing the returning data connection to be initiated from the FTP server at Company B.
- B.** Passive FTP is being used, and the firewall at Company A is not allowing the returning data connection to be initiated from the FTP server at Company B.
- C.** At Company A, active FTP is being used with a non-application aware firewall applying NAT to the source address of User A only.
- D.** The FTP server administrator at Company B has disallowed User A from accessing files on that server.
- E.** Passive FTP is being used, and the firewall at Company B is not allowing connections through to port 20 on the FTP server.

Answer: A,C

Explanation:

QUESTION NO: 47

Refer to the exhibit. Which three statements are true? (Choose three.)

- A.** Because of a "root delay" of 0ms, this router is probably receiving its time directly from a Stratum 0 or 1 GPS reference clock.
- B.** This router has correctly synchronized its clock to its NTP master.
- C.** The NTP server is running authentication and should be trusted as a valid time source.
- D.** Specific local time zones have not been configured on this router.
- E.** This router will not act as an NTP server for requests from other devices.

Answer: B,C,E

Explanation:

QUESTION NO: 48

Which three security features were introduced with the SNMPv3 protocol? (Choose three.)

- A.** Message integrity, which ensures that a packet has not been tampered with in-transit
- B.** DoS prevention, which ensures that the device cannot be impacted by SNMP buffer overflow
- C.** Authentication, which ensures that the message is from a valid source
- D.** Authorization, which allows access to certain data sections for certain authorized users
- E.** Digital certificates, which ensure nonrepudiation of authentications

F. Encryption of the packet to prevent it from being seen by an unauthorized source

Answer: A,C,F

Explanation:

QUESTION NO: 49

Which common Microsoft protocol allows Microsoft machine administration and operates over TCP port 3389?

- A. remote desktop protocol
- B. desktop mirroring
- C. desktop shadowing
- D. Tarantella remote desktop

Answer: A

Explanation:

QUESTION NO: 50

To prevent a potential attack on a Cisco IOS router with the echo service enabled, what action should you take?

- A. Disable the service with the no ip echo command.
- B. Disable the service with the no echo command.
- C. Disable tcp-small-servers.
- D. Disable this service with a global access-list.

Answer: C

Explanation:

QUESTION NO: 51

Which three new capabilities were added to HTTP v1.1 over HTTP v1.0? (Choose three.)

- A. chunked transfer encoding
- B. HTTP pipelining
- C. POST method

- D. HTTP cookies
- E. keepalive mechanism

Answer: A,B,E

Explanation:

QUESTION NO: 52

Which query type is required for an nslookup on an IPv6 addressed host?

- A. type=AAAA
- B. type=ANY
- C. type=PTR
- D. type=NAME-IPV6

Answer: A

Explanation:

QUESTION NO: 53

According to OWASP guidelines, what is the recommended method to prevent cross-site request forgery?

- A. Allow only POST requests.
- B. Mark all cookies as HTTP only.
- C. Use per-session challenge tokens in links within your web application.
- D. Always use the "secure" attribute for cookies.
- E. Require strong passwords.

Answer: C

Explanation:

QUESTION NO: 54

Which option is used to collect wireless traffic passively, for the purposes of eavesdropping or information gathering?

- A. network taps

- B. repeater Access Points
- C. wireless sniffers
- D. intrusion prevention systems

Answer: C

Explanation:

QUESTION NO: 55

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

Explanation:

QUESTION NO: 56

In the context of a botnet, what is true regarding a command and control server?

- A. It can launch an attack using IRC or Twitter.
- B. It is another name for a zombie.
- C. It is used to generate a worm.
- D. It sends the command to the botnets via adware.

Answer: A

Explanation:

QUESTION NO: 57

Which option is used for anti-replay prevention in a Cisco IOS IPsec implementation?

- A. session token
- B. one-time password

- C. time stamps
- D. sequence number
- E. nonce

Answer: D

Explanation:

QUESTION NO: 58

Which three Cisco security product features assist in preventing TCP-based man-in-the-middle attacks? (Choose three.)

- A. Cisco ASA TCP initial sequence number randomization?
- B. Cisco ASA TCP sliding-window conformance validation?
- C. Cisco IPS TCP stream reassembly?
- D. Cisco IOS TCP maximum segment size adjustment?

Answer: A,B,C

Explanation:

QUESTION NO: 59

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

Answer: B

Explanation:

QUESTION NO: 60

Refer to the exhibit.

```
regex domainlist1 "\.facebook\.com"
regex domainlist2 "\.youtube\.com"
regex domainlist3 "\.twitter\.com"

class-map type regex match-any DomainBlockList
  match regex domainlist1
  match regex domainlist3

class-map type inspect http match-all BlockDomainsClass
  match request header host regex class DomainBlockList

policy-map type inspect http http_inspection_policy
  parameters
    protocol-violation action drop-connection
  class BlockDomainsClass
    reset log

policy-map inside-policy
  class httptraffic
    inspect http http_inspection_policy

service-policy inside-policy interface inside
```

What will be the default action?

- A. HTTP traffic to the Facebook, Youtube, and Twitter websites will be dropped.
- B. HTTP traffic to the Facebook and Youtube websites will be dropped.
- C. HTTP traffic to the Youtube and Twitter websites will be dropped.
- D. HTTP traffic to the Facebook and Twitter websites will be dropped.

Answer: D

Explanation:

QUESTION NO: 61

Which Cisco ASA feature can be used to update non-compliant antivirus/antispyware definition files on an AnyConnect client?

- A. dynamic access policies
- B. dynamic access policies with Host Scan and advanced endpoint assessment
- C. Cisco Secure Desktop

D. advanced endpoint assessment

Answer: B

Explanation:

QUESTION NO: 62

Refer to the exhibit.

Below is a sample HTTP GET request made by the iTunes application to access a podcast.

```
<CRLF>  
Accept: */*  
User-Agent: iTunes/4.9 (Windows; N)  
Host: 10.1.5.20  
<CRLF>  
<CRLF>
```

When configuring a Cisco IPS custom signature, what type of signature engine must you use to block podcast clients from accessing the network?

- A. service HTTP
- B. service TCP
- C. string TCP
- D. fixed TCP
- E. service GENERIC

Answer: A

Explanation:

QUESTION NO: 63

An attacker configures an access point to broadcast the same SSID that is used at a public hot-spot, and launches a deauthentication attack against the clients that are connected to the hot-spot, with the hope that the clients will then associate to the AP of the attacker.

In addition to the deauthentication attack, what attack has been launched?

- A. man-in-the-middle
- B. MAC spoofing
- C. Layer 1 DoS
- D. disassociation attack

Answer: A

Explanation:

QUESTION NO: 64

Which four IPv6 messages should be allowed to transit a transparent firewall? (Choose four.)

- A. router solicitation with hop limit = 1
- B. router advertisement with hop limit = 1
- C. neighbor solicitation with hop limit = 255
- D. neighbor advertisement with hop limit = 255
- E. listener query with link-local source address
- F. listener report with link-local source address

Answer: C,D,E,F

Explanation:

QUESTION NO: 65

Which statement best describes the concepts of rootkits and privilege escalation?

- A. Rootkits propagate themselves.
- B. Privilege escalation is the result of a rootkit.
- C. Rootkits are a result of a privilege escalation.
- D. Both of these require a TCP port to gain access.

Answer: B

Explanation:

QUESTION NO: 66

Refer to the exhibit of an ISAKMP debug.

```
ISAKMP (62): processing SA payload. message ID = 0
ISAKMP (62): Checking ISAKMP transform 1 against priority 10 policy
                encryption DES-CBC
                hash SHA
                default group 1
                auth pre-share
ISAKMP (62): atts are acceptable. Next payload is 0
ISAKMP (62): SA is doing pre-shared key authentication
ISAKMP (62): processing KE payload. message ID = 0
ISAKMP (62): processing NONCE payload. message ID = 0
ISAKMP (62): SKEYID state generated
ISAKMP (62): processing vendor id payload
ISAKMP (62): speaking to another Cisco IOS box!
ISAKMP: reserved not zero on ID payload!
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 172.16.100.201
failed its sanity check or is malformed
```

Which message of the exchange is failing?

- A. main mode 1
- B. main mode 3
- C. aggressive mode 1
- D. main mode 5
- E. aggressive mode 2

Answer: B

Explanation:

QUESTION NO: 67

Which multicast capability is not supported by the Cisco ASA appliance?

- A. ASA configured as a rendezvous point
- B. sending multicast traffic across a VPN tunnel
- C. NAT of multicast traffic
- D. IGMP forwarding (stub) mode

Answer: B

Explanation:

QUESTION NO: 68

Refer to the exhibit.

```
regex App_regex_1
"[uU][nN][iI][oO][nN]([%2[0bB]]+)([aA][lL][lL]([%2[0bB]]+))?[
[sS][eE][lL][eE][cC][tT]"
regex App_regex_2 "[Ss][Ee][Ll][Ee][Cc][Tt](%2[0bB]+)[^\\r\\x00-
\\x19\\x7f-\\xff]+(%2[0bB]+)[Ff][Rr][Oo][Mm](%2[0bB]+)"
!
class-map WebServers
match port tcp eq www
class-map type inspect http match-any App-map
match request body regex App_regex_1
match request body regex App_regex_2
!
policy-map type inspect http drop-Protocol
parameters
body-match-maximum 3000
class App-map
drop-connection log
policy-map protocol-traffic
class WebServers
inspect http drop-Protocol
!
service-policy protocol-traffic interface outside
```

What type of attack is being mitigated on the Cisco ASA appliance?

- A. HTTPS certificate man-in-the-middle attack
- B. HTTP distributed denial of service attack
- C. HTTP Shockwave Flash exploit
- D. HTTP SQL injection attack

Answer: D

Explanation:

QUESTION NO: 69

Which method of output queuing is supported on the Cisco ASA appliance?

- A. CBWFQ
- B. priority queuing
- C. MDRR
- D. WFQ
- E. custom queuing

Answer: B

Explanation:

QUESTION NO: 70

Which statement is true regarding Cisco ASA operations using software versions 8.3 and later?

- A. The global access list is matched first before the interface access lists.
- B. Both the interface and global access lists can be applied in the input or output direction.
- C. When creating an access list entry using the Cisco ASDM Add Access Rule window, choosing "global" as the interface will apply the access list entry globally.
- D. NAT control is enabled by default.
- E. The static CLI command is used to configure static NAT translation rules.

Answer: A

Explanation:

QUESTION NO: 71

Which four values can be used by the Cisco IPS appliance in the risk rating calculation? (Choose four.)

- A. attack severity rating
- B. target value rating
- C. signature fidelity rating
- D. promiscuous delta
- E. threat rating
- F. alert rating

Answer: A,B,C,D

Explanation:

QUESTION NO: 72

Which three authentication methods does the Cisco IBNS Flexible Authentication feature support? (Choose three.)

- A. cut-through proxy
- B. dot1x
- C. MAB
- D. SSO
- E. web authentication

Answer: B,C,E

Explanation:

QUESTION NO: 73

Troubleshooting the web authentication fallback feature on a Cisco Catalyst switch shows that clients with the 802.1X supplicant are able to authenticate, but clients without the supplicant are not able to use web authentication. Which configuration option will correct this issue?

- A. switch(config)# aaa accounting auth-proxy default start-stop group radius
- B. switch(config-if)# authentication host-mode multi-auth
- C. switch(config-if)# webauth
- D. switch(config)# ip http server
- E. switch(config-if)# authentication priority webauth dot1x

Answer: D

Explanation:

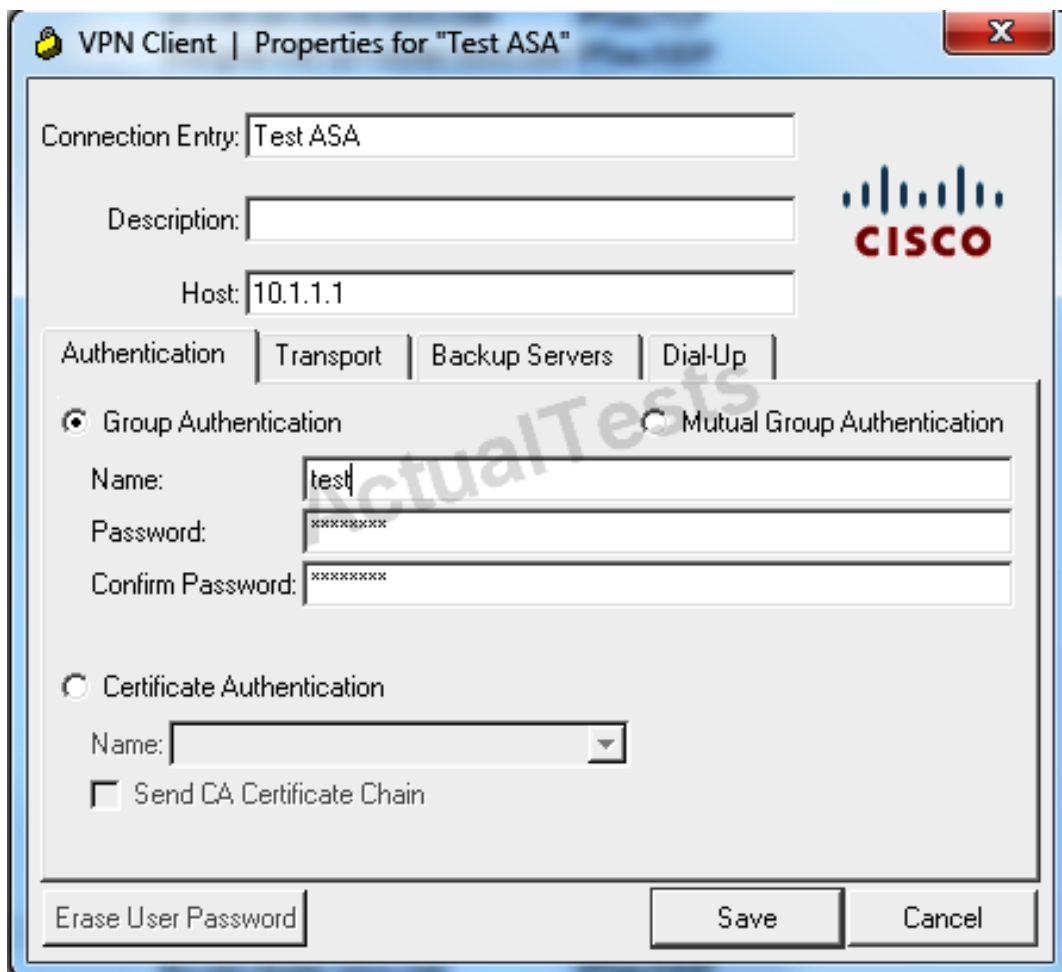
QUESTION NO: 74

Which option on the Cisco ASA appliance must be enabled when implementing botnet traffic filtering?

- A. HTTP inspection
- B. static entries in the botnet blacklist and whitelist
- C. global ACL
- D. NetFlow

E. DNS inspection and DNS snooping**Answer: E****Explanation:****QUESTION NO: 75**

Refer to the exhibit.



VPN Client | Properties for "Test ASA"

Connection Entry: Test ASA

Description:

Host: 10.1.1.1

Authentication | Transport | Backup Servers | Dial-Up

☒ Group Authentication ☐ Mutual Group Authentication

Name: test

Password:

Confirm Password:

☐ Certificate Authentication

Name:

☐ Send CA Certificate Chain

Erase User Password Save Cancel

To configure the Cisco ASA, what should you enter in the Name field, under the Group Authentication option for the IPSec VPN client?

- A. group policy name
- B. crypto map name
- C. isakmp policy name
- D. crypto ipsec transform-set name
- E. tunnel group name

Answer: E

Explanation:

QUESTION NO: 76

Refer to the exhibit.

```
!other commands omitted
switch(config-if)# switchport access vlan 10
switch(config-if)# switchport mode access
switch(config-if)# switchport voice vlan 20
switch(config-if)# dot1x pae authenticator
switch(config-if)#authentication port-control auto
switch(config-if)#authentication host-mode multi-domain
switch(config-if)#authentication order mab dot1x
switch(config-if)#authentication priority dot1x mab
switch(config-if)#mab
!other commands omitted
```

Which statement about this Cisco Catalyst switch 802.1X configuration is true?

- A.** If an IP phone behind the switch port has an 802.1X supplicant, MAC address bypass will still be used to authenticate the IP Phone.
- B.** If an IP phone behind the switch port has an 802.1X supplicant, 802.1X authentication will be used to authenticate the IP phone.
- C.** The authentication host-mode multi-domain command enables the PC connected behind the IP phone to bypass 802.1X authentication.
- D.** Using the authentication host-mode multi-domain command will allow up to eight PCs connected behind the IP phone via a hub to be individually authentication using 802.1X.

Answer: B

Explanation:

QUESTION NO: 77

Which C3PL configuration component is used to tune the inspection timers such as setting the tcp idle-time and tcp synwait-time on the Cisco ZBFW?

- A. class-map type inspect
- B. parameter-map type inspect
- C. service-policy type inspect
- D. policy-map type inspect tcp
- E. inspect-map type tcp

Answer: B

Explanation:

QUESTION NO: 78

Which signature engine is used to create a custom IPS signature on a Cisco IPS appliance that triggers when a vulnerable web application identified by the "/runscript.php" URI is run?

- A. AIC HTTP
- B. Service HTTP
- C. String TCP
- D. Atomic IP
- E. META
- F. Multi-String

Answer: B

Explanation:

QUESTION NO: 79

Which Cisco IPS appliance feature can automatically adjust the risk rating of IPS events based on the reputation of the attacker?

- A. botnet traffic filter
- B. event action rules
- C. anomaly detection
- D. reputation filtering
- E. global correlation inspection

Answer: E

Explanation:

QUESTION NO: 80

The ASA can be configured to drop IPv6 headers with routing-type 0 using the MPF. Choose the correct configuration.

- A.** policy-map type inspect ipv6 IPv6_PMAP
match header routing-type eq 0
drop log
- B.** policy-map type inspect icmpv6 ICMPv6_PMAP
match header routing-type eq 0
drop log
- C.** policy-map type inspect ipv6-header HEADER_PMAP
match header routing-type eq 0
drop log
- D.** policy-map type inspect http HEADER_PMAP
match routing-header 0
drop log
- E.** policy-map type inspect ipv6 IPv6_PMAP
match header type 0
drop log
- F.** policy-map type inspect ipv6-header HEADER_PMAP
match header type 0
drop log

Answer: A

Explanation:

QUESTION NO: 81

Refer to the exhibit.

Client

|
|

(inside)

ZBFW

(outside)

|
|

Server

zone security inside

zone security outside

interface inside

zone-member security inside

interface outside

zone-member security outside

class-map type inspect match-all HTTP_CMAP
match protocol HTTP

class-map type inspect match-all TCP_CMAP
match protocol TCP

policy-map type inspect IN-OUT_PMAP

class type inspect TCP_CMAP

inspect

class type inspect HTTP_CMAP

pass

class class-default

drop

zone-pair IN-OUT_ZP source inside destination outside

service-policy type inspect IN-OUT_PMAP

With the client protected by the firewall, an HTTP connection from the client to the server on TCP port 80 will be subject to which action?

- A. inspection action by the HTTP_CMAP
- B. inspection action by the TCP_CMAP
- C. drop action by the default class
- D. inspection action by both the HTTP_CMAP and TCP_CMAP
- E. pass action by the HTTP_CMAP
- F. drop action due to class-map misclassification

Answer: B

Explanation:

QUESTION NO: 82

Which mode of operation must be enabled on CSM to support roles such as Network Administrator, Approver, Network Operator, and Help Desk?

- A. Deployment Mode
- B. Activity Mode
- C. Workflow Mode
- D. User Roles Mode
- E. Administration Mode
- F. Network Mode

Answer: C

Explanation:

QUESTION NO: 83

Which two ISE Probes would be required to distinguish accurately the difference between an iPad and a MacBook Pro? (Choose two.)

- A. DHCP or DHCPSPAN
- B. SNMPTRAP
- C. SNMPQUERY
- D. NESSUS
- E. HTTP
- F. DHCP TRAP

Answer: A,E

Explanation:

QUESTION NO: 84

Which configuration option will correctly process network authentication and authorization using both 802.1X and MAB on a single port?

A)

```
interface FastEthernet1/0/9
switchport access vlan 200
switchport mode access
switchport voice vlan 40
ip access-group ACL-DEFAULT in
authentication event fail action next-method
authentication event server dead action authorize vlan 200
authentication event server alive action reinitialize
authentication host-mode multi-domain
authentication open
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
ip dhcp snooping information option allow-untrusted
end
```

B)

```
interface FastEthernet1/0/9
switchport access vlan 200
switchport mode access
switchport voice vlan 40
ip access-group ACL-DEFAULT in
authentication event fail action next-method
authentication event server dead action authorize vlan 200
authentication event server alive action reinitialize
authentication host-mode multi-domain
authentication open
authentication order mab dot1x
authentication priority dot1x mab
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
ip dhcp snooping information option allow-untrusted
end
```

C)

```
interface FastEthernet1/0/9
  switchport access vlan 200
  switchport mode access
  switchport voice vlan 40
  ip access-group ACL-DEFAULT in
  authentication event fail action next-method
  authentication event server dead action authorize vlan 200
  authentication event server alive action reinitialize
  authentication host-mode multi-domain
  authentication open
  authentication order mab dot1x
  authentication priority dot1x mab
  authentication violation restrict
  mab
  dot1x pae authenticator
  dot1x timeout tx-period 10
  spanning-tree portfast
  ip dhcp snooping information option allow-untrusted
end
```

D)

```
interface FastEthernet1/0/9
  switchport access vlan 200
  switchport mode access
  switchport voice vlan 40
  ip access-group ACL-DEFAULT in
  authentication event fail action next-method
  authentication event server dead action authorize vlan 200
  authentication event server alive action reinitialize
  authentication host-mode multi-domain
  authentication open
  authentication order mab dot1x
  authentication priority dot1x mab
  authentication port-control force-unauthorized
  authentication violation restrict
  mab
  dot1x pae authenticator
  dot1x timeout tx-period 10
  spanning-tree portfast
  ip dhcp snooping information option allow-untrusted
end
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

QUESTION NO: 85

Which statement regarding the routing functions of the Cisco ASA is true?

- A. The translation table can override the routing table for new connections.
- B. The ASA supports policy-based routing with route maps?.
- C. In a failover pair of ASAs, the standby firewall establishes a peer relationship with OSPF neighbors.
- D. Routes to the Null0 interface can be configured to black-hole traffic.

Answer: A

Explanation:

QUESTION NO: 86

Refer to the exhibit.

```
!  
access-list routemapacl standard deny host 10.66.42.215  
access-list routemapacl standard deny 10.40.29.0 255.255.255.0  
access-list routemapacl standard deny 10.39.24.0 255.255.255.0  
access-list routemapacl standard permit any  
!  
route outside 10.39.23.0 255.255.255.0 192.168.1.1 1  
route outside 10.39.24.0 255.255.255.0 192.168.1.1 1  
route outside 10.39.27.0 255.255.255.0 192.168.1.1 1  
route outside 10.40.29.0 255.255.255.0 192.168.1.1 1  
route outside 10.40.30.0 255.255.255.0 192.168.1.1 1  
route outside 10.66.42.215 255.255.255.255 192.168.1.1 1  
!  
route-map static_route_map permit 10  
match ip address routemapacl  
!  
router ospf90  
network 192.168.1.0 255.255.255.0 area 0  
log-adj-changes  
redistribute static subnets route-map static_route_map
```

Which route will be advertised by the Cisco ASA to its OSPF neighbors?

- A. 10.39.23.0/24
- B. 10.40.29.0/24
- C. 10.66.42.215/32
- D. 10.40.29.0/24

Answer: A

Explanation:

QUESTION NO: 87

Which three statements are true about the Cisco ASA object configuration below? (Choose three.)

```
object network vpnclients
```

```
range 10.1.100.4 10.1.100.10
```

```
object network vpnclients
```

```
nat (outside,outside) dynamic interface
```

- A. The NAT configuration in the object specifies a PAT rule?.
- B. This configuration requires the command same-security-traffic inter-interface for traffic that matches this NAT rule to pass through the Cisco ASA appliance.
- C. The NAT rule of this object will be placed in Section 1 (Auto-NAT) of the Cisco ASA NAT table?.
- D. This configuration is most likely used to provide Internet access to connected VPN clients.
- E. Addresses in the range will be assigned during config-mode.

Answer: A,C,D

Explanation:

QUESTION NO: 88

Which three options can be configured within the definition of a network object, as introduced in Cisco ASA version 8.3(1)? (Choose three.)

- A. range of IP addresses
- B. subnet of IP addresses
- C. destination IP NAT translation
- D. source IP NAT translation
- E. source and destination FQDNs
- F. port and protocol ranges

Answer: A,B,D

Explanation:

QUESTION NO: 89

Which three attributes may be configured as part of the Common Tasks panel of an authorization profile in the Cisco ISE solution? (Choose three.)

- A. VLAN
- B. voice VLAN
- C. dACL name
- D. voice domain permission
- E. SGT

Answer: A,C,D

Explanation:

QUESTION NO: 90

Which two statements describe the Cisco TrustSec system correctly? (Choose two.)

- A. The Cisco TrustSec system is a partner program, where Cisco certifies third-party security products as extensions to the secure infrastructure.
- B. The Cisco TrustSec system is an approach to certifying multimedia and collaboration applications as secure.
- C. The Cisco TrustSec system is an Advanced Network Access Control System that leverages enforcement intelligence in the network infrastructure.
- D. The Cisco TrustSec system tests and certifies all products and product versions that make up the system as working together in a validated manner.

Answer: C,D

Explanation:

QUESTION NO: 91

Which option is the correct definition for MAB?

- A.** MAB is the process of checking the mac-address-table on the local switch for the sticky address. If the mac-address of the device attempting to access the network matches the configured sticky address, it will be permitted to bypass 802.1X authentication.
- B.** MAB is a process where the switch will send an authentication request on behalf of the endpoint that is attempting to access the network, using the mac-address of the device as the credentials. The authentication server evaluates that MAC address against a list of devices permitted to access the network without a stronger authentication.
- C.** MAB is a process where the switch will check a local list of MAC addresses to identify systems that are permitted network access without using 802.1X.
- D.** MAB is a process where the supplicant on the endpoint is configured to send the MAC address of the endpoint as its credentials.

Answer: B

Explanation:

QUESTION NO: 92

Regarding VSAs, which statement is true?

- A.** VSAs may be implemented on any RADIUS server.
- B.** VSAs are proprietary, and therefore may only be used on the RADIUS server of that vendor. For example, a Cisco VSA may only be used on a Cisco RADIUS server, such as ACS or ISE.
- C.** VSAs do not apply to RADIUS; they are a TACACS attribute.
- D.** Each VSA is defined in an RFC and is considered to be a standard.

Answer: A

Explanation:

QUESTION NO: 93

Which four items may be checked via a Cisco NAC Agent posture assessment? (Choose four.)

- A.** Microsoft Windows registry keys
- B.** the existence of specific processes in memory
- C.** the UUID of an Apple iPad or iPhone
- D.** if a service is started on a Windows host
- E.** the HTTP User-Agent string of a device

- F. if an Apple iPad or iPhone has been "jail-broken"
 G. if an antivirus application is installed on an Apple MacBook

Answer: A,B,D,G

Explanation:

QUESTION NO: 94

Which three statements are true about the Cisco NAC Appliance solution? (Choose three.)

- A. In a Layer 3 OOB ACL deployment of the Cisco NAC Appliance, the discovery host must be configured as the untrusted IP address of the Cisco NAC Appliance Server.
 B. In a Cisco NAC Appliance deployment, the discovery host must be configured on a Cisco router using the "NAC discovery-host" global configuration command.
 C. In a VRF-style OOB deployment of the Cisco NAC Appliance, the discovery host may be the IP address that is on the trusted side of the Cisco NAC Appliance Server.
 D. In a Layer 3 IB deployment of the Cisco NAC Appliance, the discovery host may be configured as the IP address of the Cisco NAC Appliance Manager.

Answer: A,C,D

Explanation:

QUESTION NO: 95

Refer to the exhibit.

R1# show crypto engine connection active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	<none>	<none>	set	HMAC_SHA+3DES_56_C	0	0
2000	FastEthernet0/1	172.16.1.10	set	HMAC_MD5+3DES_56_C	0	0
2001	FastEthernet0/1	172.16.1.10	set	HMAC_MD5+3DES_56_C	9	0

R2# show crypto engine connection active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0/0	172.16.1.20	set	HMAC_SHA+3DES_56_C	0	0
2000	FastEthernet0/0	172.16.1.20	set	HMAC_MD5+3DES_56_C	0	9
2001	FastEthernet0/0	172.16.1.20	set	HMAC_MD5+3DES_56_C	0	0

On R1, encrypt counters are incrementing. On R2, packets are decrypted, but the encrypt counter

is not being incremented. What is the most likely cause of this issue?

- A. a routing problem on R1
- B. a routing problem on R2
- C. incomplete IPsec SA establishment
- D. crypto engine failure on R2
- E. IPsec rekeying is occurring

Answer: B

Explanation:

QUESTION NO: 96

Refer to the exhibit, which shows a partial output of the show command.

```
sslvpn1#show webvpn context
Codes: AS - Admin Status, OS - Operation Status
      VHost - Virtual Host
Context Name      AS   OS
-----
vpn1              down down
```

Which statement best describes the problem?

- A. Context vpn1 is not inservice.
- B. There is no gateway that is configured under context vpn1.
- C. The config has not been properly updated for context vpn1.
- D. The gateway that is configured under context vpn1 is not inservice.

Answer: A

Explanation:

QUESTION NO: 97

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

Explanation:

QUESTION NO: 98

Which three statements about Cisco IOS RRI are correct? (Choose three.)

- A. RRI is not supported with ipsec-profiles.
- B. Routes are created from ACL entries when they are applied to a static crypto map.
- C. Routes are created from source proxy IDs by the receiver with dynamic crypto maps.
- D. VRF-based routes are supported.
- E. RRI must be configured with DMVPN.

Answer: B,C,D

Explanation:

QUESTION NO: 99

Review the exhibit.

With inline VLAN pairs on a sensor:

- A. You cannot pair a VLAN with itself.
- B. For a given sensing interface, an interface used in a VLAN pair can be a member of another inline interface pair.
- C. For a given sensing interface, a VLAN can be a member of only one inline VLAN pair; however, a given VLAN can be a member of an inline VLAN pair on more than one sensing interface.
- D. The order in which you specify the VLANs in a inline pair is significant.
- E. A sensing interface in inline VLAN pair mode can have from 1 to 255 inline VLAN pairs.

Which three statements about the Cisco IPS sensor are true? (Choose three.)

- A. A
- B. B
- C. C
- D. D
- E. E

Answer: A,C,E

Explanation:

QUESTION NO: 100

An internal DNS server requires a NAT on a Cisco IOS router that is dual-homed to separate ISPs using distinct CIDR blocks. Which NAT capability is required to allow hosts in each CIDR block to contact the DNS server via one translated address?

- A. NAT overload
- B. NAT extendable
- C. NAT TCP load balancing
- D. NAT service-type DNS
- E. NAT port-to-application mapping

Answer: B

Explanation:

QUESTION NO: 101

Refer to the exhibit.

```
ip routing

crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp key myPreShareKey0 address ipv6
3FFE:2002::A8BB:CCFF:FE01:2C02/128
!
crypto ipsec transform-set 3des ah-sha-hmac esp-3des
!
crypto ipsec profile profile0
 set transform-set 3des
!
ipv6 cef
!
interface Tunnel0
 ipv6 address 3FFE:1001::/64 eui-64
 ipv6 cef
 tunnel source Ethernet2/0
 tunnel destination 3FFE:2002::A8BB:CCFF:FE01:2C02
 tunnel protection ipsec profile profile0
```

Which three command sets are required to complete this IPv6 IPsec site-to-site VTI? (Choose three.)

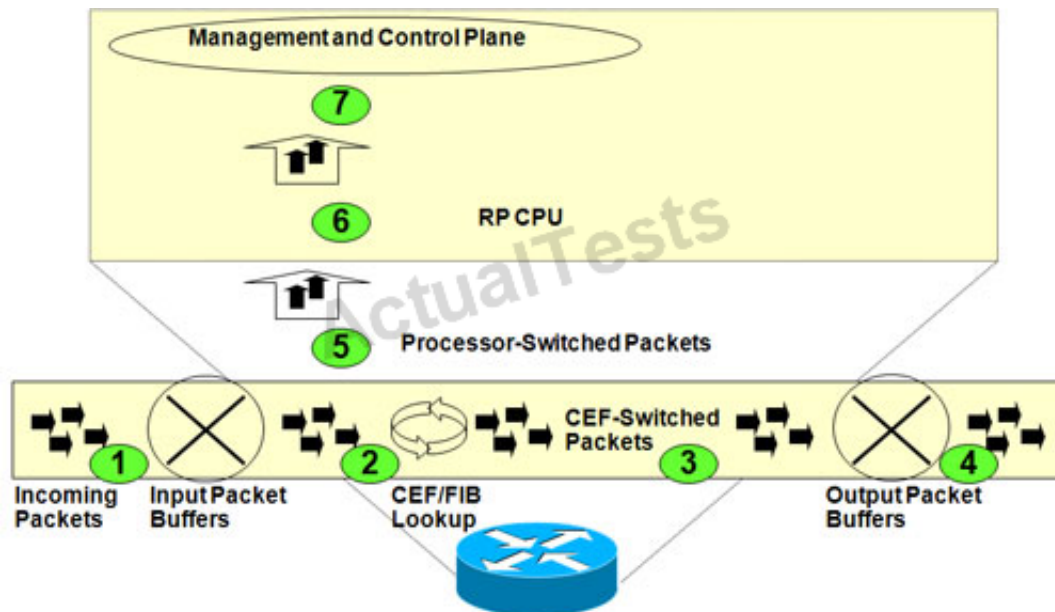
- A. interface Tunnel0
tunnel mode ipsec ipv6
- B. crypto isakmp-profile
match identity address ipv6 any
- C. interface Tunnel0
ipv6 enable
- D. ipv6 unicast-routing
- E. interface Tunnel0
ipv6 enable-ipsec

Answer: A,C,D

Explanation:

QUESTION NO: 102

Refer to the exhibit.



Which option correctly identifies the point on the exhibit where Control Plane Policing (input) is applied to incoming packets?

- A. point 6
- B. point 7
- C. point 4
- D. point 1
- E. points 5 and 6

Answer: A

Explanation:

QUESTION NO: 103

Which of the following describes the DHCP "starvation" attack?

- A. Exhaust the address space available on the DHCP servers so that an attacker can inject their own DHCP server for malicious reasons.
- B. Saturate the network with DHCP requests to prevent other network services from working.
- C. Inject a DHCP server on the network for the purpose of overflowing DNS servers with bogus learned host names.
- D. Send DHCP response packets for the purpose of overloading CAM tables.

Answer: A

Explanation:

QUESTION NO: 104

Which Cisco technology protects against Spanning Tree Protocol manipulation?

- A. spanning-tree protection
- B. root guard and BPDU guard
- C. Unicast Reverse Path Forwarding
- D. MAC spoof guard
- E. port security

Answer: B

Explanation:

QUESTION NO: 105

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

Explanation:

QUESTION NO: 106

Which three configuration components are required to implement QoS policies on Cisco routers using MQC? (Choose three.)

- A. class-map
- B. global-policy
- C. policy-map
- D. service-policy
- E. inspect-map

Answer: A,C,D

Explanation:

QUESTION NO: 107

Which QoS marking is only locally significant on a Cisco router?

- A. MPLS EXP
- B. DSCP
- C. QoS group
- D. IP precedence
- E. traffic class

F. flow label

Answer: C

Explanation:

QUESTION NO: 108

Which three control plane subinterfaces are available when implementing Cisco IOS Control Plane Protection? (Choose three.)

- A. CPU
- B. host
- C. fast-cache
- D. transit
- E. CEF-exception
- F. management

Answer: B,D,E

Explanation:

QUESTION NO: 109

Which type of PVLAN ports can communicate among themselves and with the promiscuous port?

- A. isolated
- B. community
- C. primary
- D. secondary
- E. protected

Answer: B

Explanation:

QUESTION NO: 110

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

Explanation:

QUESTION NO: 111

Which additional configuration component is required to implement a MACSec Key Agreement policy on user-facing Cisco Catalyst switch ports?

- A. PKI
- B. TACACS+
- C. multi-auth host mode
- D. port security
- E. 802.1x

Answer: E

Explanation:

QUESTION NO: 112

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

Explanation:

QUESTION NO: 113

Which four techniques can you use for IP management plane security? (Choose four.)

- A. Management Plane Protection
- B. uRPF
- C. strong passwords
- D. RBAC
- E. SNMP security measures
- F. MD5 authentication

Answer: A,C,D,E

Explanation:

QUESTION NO: 114

Which three statements about remotely triggered black hole filtering are true? (Choose three.)

- A. It filters undesirable traffic.
- B. It uses BGP or OSPF to trigger a network-wide remotely controlled response to attacks.
- C. It provides a rapid-response technique that can be used in handling security-related events and incidents.
- D. It requires uRPF.

Answer: A,C,D

Explanation:

QUESTION NO: 115

Which three statements about Cisco Flexible NetFlow are true? (Choose three.)

- A. The packet information used to create flows is not configurable by the user.
- B. It supports IPv4 and IPv6 packet fields.
- C. It tracks all fields of an IPv4 header as well as sections of the data payload.
- D. It uses two types of flow cache, normal and permanent.
- E. It can be a useful tool in monitoring the network for attacks.

Answer: B,C,E

Explanation:

QUESTION NO: 116

Management Frame Protection is available in two deployment modes, Infrastructure and Client. Which three statements describe the differences between these modes? (Choose three.)

- A. Infrastructure mode appends a MIC to management frames.
- B. Client mode encrypts management frames.
- C. Infrastructure mode can detect and prevent common DoS attacks.
- D. Client mode can detect and prevent common DoS attacks.
- E. Infrastructure mode requires Cisco Compatible Extensions version 5 support on clients.

Answer: A,B,D

Explanation:

QUESTION NO: 117

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

Answer: C,D,E

Explanation:

QUESTION NO: 118

Which four protocols are supported by Cisco IOS Management Plane Protection? (Choose four.)

- A. Blocks Extensible Exchange Protocol (BEEP)
- B. Hypertext Transfer Protocol Secure (HTTPS)
- C. Secure Copy Protocol (SCP)
- D. Secure File Transfer Protocol (SFTP)
- E. Secure Shell (SSH)

F. Simple Network Management Protocol (SNMP)

Answer: A,B,E,F

Explanation:

QUESTION NO: 119

Which four Cisco IOS features are used to implement First Hop Security in IPv6? (Choose four.)

- A. IPv6 First-Hop Security Binding Table**
- B. IPv6 Device Tracking**
- C. IPv6 RA Guard**
- D. SeND**
- E. IPv6 Selective Packet Discard**
- F. IPv6 Source Guard**

Answer: A,B,C,D

Explanation:

QUESTION NO: 120

Which two identifiers are used by a Cisco Easy VPN Server to reference the correct group policy information for connecting a Cisco Easy VPN Client? (Choose two.)

- A. IKE ID_KEY_ID**
- B. OU field in a certificate that is presented by a client**
- C. XAUTH username**
- D. hash of the OTP that is sent during XAUTH challenge/response**
- E. IKE ID_IPV4_ADDR**

Answer: A,B

Explanation:

QUESTION NO: 121

According ISO27001 ISMS, which of the following are mandatory documents? (Choose 4)

- A. ISMS Policy**

- B. Corrective Action Procedure
- C. IS Procedures
- D. Risk Assessment Reports
- E. Complete Inventory of all information assets

Answer: A,B,C,D

Explanation:

QUESTION NO: 122

Which current RFC made RFCs 2409, 2407, and 2408 obsolete?

- A. RFC 4306
- B. RFC 2401
- C. RFC 5996
- D. RFC 4301
- E. RFC 1825

Answer: C

Explanation:

QUESTION NO: 123

During a computer security forensic investigation, a laptop computer is retrieved that requires content analysis and information retrieval. Which file system is on it, assuming it has the default installation of Microsoft Windows Vista operating system?

- A. HSFS
- B. WinFS
- C. NTFS
- D. FAT
- E. FAT32

Answer: C

Explanation:

QUESTION NO: 124

Which of these is a core function of the risk assessment process? (Choose one.)

- A. performing regular network upgrades
- B. performing network optimization
- C. performing network posture validation
- D. establishing network baselines
- E. prioritizing network roll-outs

Answer: C

Explanation:

QUESTION NO: 125

Which two answers describe provisions of the SOX Act and its international counterpart Acts? (Choose two.)

- A. confidentiality and integrity of customer records and credit card information
- B. accountability in the event of corporate fraud
- C. financial information handled by entities such as banks, and mortgage and insurance brokers
- D. assurance of the accuracy of financial records
- E. US Federal government information
- F. security standards that protect healthcare patient data

Answer: B,D

Explanation:

QUESTION NO: 126

Which three statements about the IANA are true? (Choose three.)

- A. IANA is a department that is operated by the IETF.
- B. IANA oversees global IP address allocation.
- C. IANA managed the root zone in the DNS.
- D. IANA is administered by the ICANN.
- E. IANA defines URI schemes for use on the Internet.

Answer: B,C,D

Explanation:

QUESTION NO: 127

What does the Common Criteria (CC) standard define?

- A. The current list of Common Vulnerabilities and Exposures (CVEs)
- B. The U.S standards for encryption export regulations
- C. Tools to support the development of pivotal, forward-looking information system technologies
- D. The international standards for evaluating trust in information systems and products
- E. The international standards for privacy laws
- F. The standards for establishing a security incident response system

Answer: D

Explanation:

QUESTION NO: 128

Which three types of information could be used during the incident response investigation phase? (Choose three.)

- A. netflow data
- B. SNMP alerts
- C. encryption policy
- D. syslog output
- E. IT compliance reports

Answer: A,B,D

Explanation:

QUESTION NO: 129

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

Explanation:

QUESTION NO: 130

Which option 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. defeats DoS attacks which employ IP source address spoofing
- D. restricts directed broadcasts at the ingress router
- E. allows DHCP or BOOTP packets to reach the relay agents as appropriate

Answer: C