

Cisco 350-018



CCIE Security Exam (4.0)

Version: 17.0

Topic 1, Volume A

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 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: 3

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: 4

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: 5

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: 6

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: 7

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: 8

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: 9

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: 10

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: 11

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: 12

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: 13

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: 14

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: 15

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: 16

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

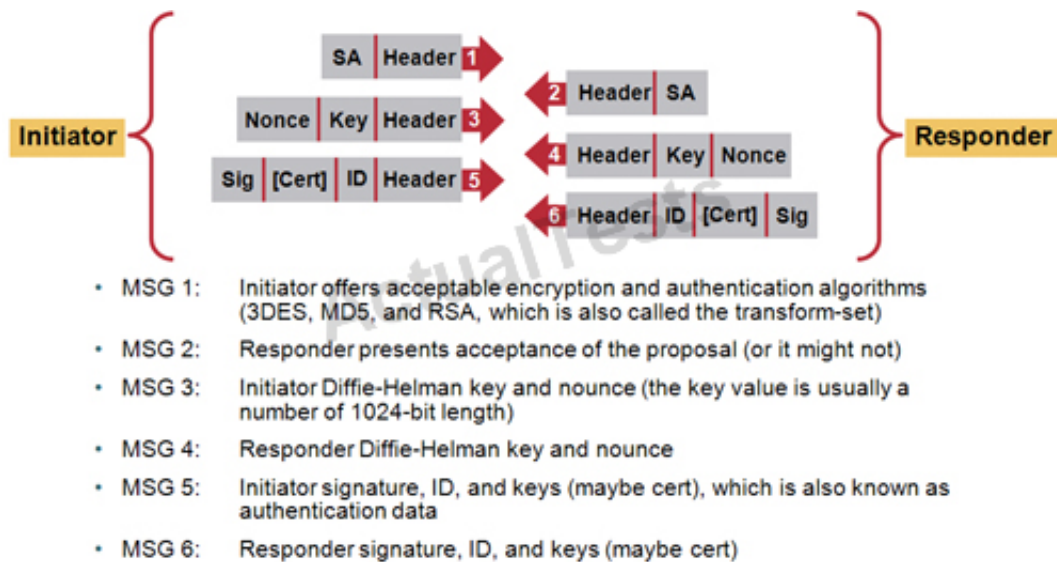
- A. Mobile IPv6 does not require a foreign agent, but Mobile IPv4 does.
- B. Mobile IPv6 supports route optimization as a fundamental part of the protocol; IPv4 requires extensions.
- C. Mobile IPv6 and Mobile IPv4 use a directed broadcast approach for home agent address discovery.
- D. Mobile IPv6 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: 17

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: 18

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: 19

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: 20

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: 21

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: 22

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: 23

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: 24

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: 25

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: 26

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: 27

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: 28

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: 29

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: 30

Refer to the exhibit.

```
Router2#show ntp associations detail
```

```
32.6.43.12 configured, authenticated, our_master, sane, valid, stratum 8
ref ID 127.127.7.1, time D2F543E6.A1C84F68 (10:51:02.631 EDT Mon Feb 27 2012)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 377, sync dist 0.381
delay -0.24 msec, offset 0.0055 msec, dispersion 0.23
precision 2**18, version 3
org time D2F54424.BA637C58 (10:52:04.728 EDT Mon Feb 27 2012)
rcv time D2F54424.BA5B2013 (10:52:04.727 EDT Mon Feb 27 2012)
xmt time D2F54424.BA632013 (10:52:04.728 EDT Mon Feb 27 2012)
filtdelay =   -0.24   0.00   0.00   0.00   4.00   4.00   4.00   0.00
filtoffset =    0.01   0.01   0.01   0.01  -1.99  -1.99  -1.99   0.01
filtererror =    0.02   0.99   1.97   1.98   2.00   2.01   2.03   2.04
```

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: 31

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: 32

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: 33

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: 34

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: 35

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: 36

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: 37

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: 38

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: 39

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: 40

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: 41

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: 42

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: 43

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: 44

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: 45

Refer to the exhibit.

```
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 ISAKMP 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: 46

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: 47

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: 48

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: 49

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: 50

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: 51

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: 52

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: 53

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: 54

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: 55

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: 56

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: 57

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: 58

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: 59

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: 60

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: 61

Refer to the exhibit.

```
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: 62

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: 63

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: 64

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: 65

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: 66

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: 67

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: 68

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: 69

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: 70

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: 71

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: 72

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: 73

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: 74

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: 75

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: 76

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: 77

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: 78

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: 79

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: 80

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

Explanation:

QUESTION NO: 81

Which of the following provides the features of route summarization, assignment of contiguous blocks of addresses, and combining routes for multiple classful networks into a single route?

- A. classless interdomain routing
- B. route summarization
- C. supernetting
- D. private IP addressing

Answer: A

Explanation:

QUESTION NO: 82

Aggregate global IPv6 addresses begin with which bit pattern in the first 16-bit group?

- A. 000/3
- B. 001/3
- C. 010/2
- D. 011/2

Answer: B

Explanation:

QUESTION NO: 83

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

Explanation:

QUESTION NO: 84

Which statement best describes a key difference in IPv6 fragmentation support compared to IPv4?

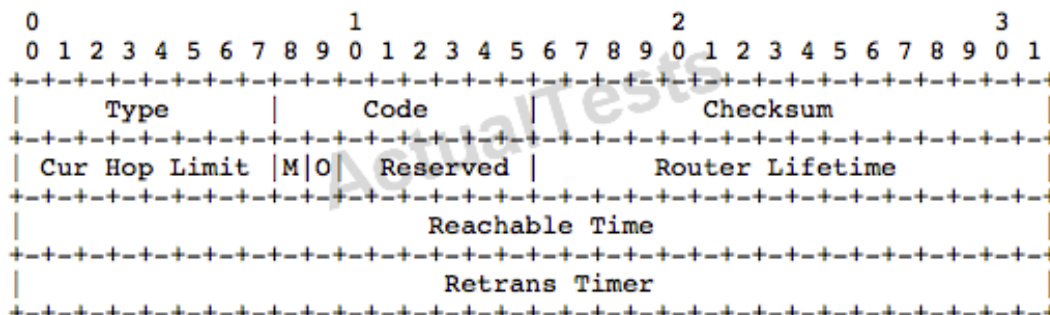
- A. In IPv6, IP fragmentation is no longer needed because all Internet links must have an IP MTU of 1280 bytes or greater.
- B. In IPv6, PMTUD is no longer performed by the source node of an IP packet.
- C. In IPv6, IP fragmentation is no longer needed since all nodes must perform PMTUD and send packets equal to or smaller than the minimum discovered path MTU.
- D. In IPv6, PMTUD is no longer performed by any node since the don't fragment flag is removed from the IPv6 header.
- E. In IPv6, IP fragmentation is performed only by the source node of a large packet, and not by any other devices in the data path.

Answer: E

Explanation:

QUESTION NO: 85

Refer to the exhibit.



It shows the format of an IPv6 Router Advertisement packet. If the Router Lifetime value is set to 0, what does that mean?

- A. The router that is sending the RA is not the default router.
- B. The router that is sending the RA is the default router.
- C. The router that is sending the RA will never power down.
- D. The router that is sending the RA is the NTP master.
- E. The router that is sending the RA is a certificate authority.
- F. The router that is sending the RA has its time synchronized to an NTP source.

Answer: A

Explanation:

QUESTION NO: 86

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

Explanation:

QUESTION NO: 87

A network administrator uses a LAN analyzer to troubleshoot OSPF router exchange messages sent to all OSPF routers. To which one of these MAC addresses 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

Explanation:

QUESTION NO: 88

Which option correctly describes the security enhancement added for OSPFv3?

- A. The AuType field in OSPFv3 now supports the more secure SHA-1 and SHA-2 algorithms in addition to MD5.
- B. The AuType field is removed from the OSPFv3 header since simple password authentication is no longer an option.
- C. The Authentication field in OSPFv3 is increased from 64 bits to 128 bits to accommodate more

secure authentication algorithms.

D. Both the AuType and Authentication fields are removed from the OSPF header in OSPFv3, since now it relies on the IPv6 Authentication Header (AH) and IPv6 Encapsulating Security Payload (ESP) to provide integrity, authentication, and/or confidentiality.?

E. The Authentication field is removed from the OSPF header in OSPFv3, because OSPFv3 must only run inside of an authenticated IPsec tunnel.

Answer: D

Explanation:

QUESTION NO: 89

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

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

Answer: A

Explanation:

QUESTION NO: 90

What IP protocol number is used in the protocol field of an IPv4 header, when IPv4 is used to tunnel IPv6 packets?

- A.** 6
- B.** 27
- C.** 41
- D.** 47
- E.** 51

Answer: C

Explanation:

QUESTION NO: 91

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

Explanation:

QUESTION NO: 92

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

Explanation:

QUESTION NO: 93

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

Explanation:

QUESTION NO: 94

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: 95

Which option explains the passive scan technique that is used by wireless clients to discover available wireless networks?

- A. listening for access point beacons that contain available wireless networks
- B. sending a null probe request
- C. sending a null association request
- D. listening for access point probe response frames that contain available wireless networks

Answer: A

Explanation:

QUESTION NO: 96

Which protocol can be used to encrypt traffic sent over a GRE tunnel?

- A. SSL
- B. SSH
- C. IPsec
- D. DH
- E. TLS

Answer: C

Explanation:

QUESTION NO: 97

Which three options are security measures that are defined for Mobile IPv6? (Choose three.)

- A. IPsec SAs are used for binding updates and acknowledgements.
- B. The use of IKEv1 or IKEv2 is mandatory for connections between the home agent and mobile node.
- C. Mobile nodes and the home agents must support ESP in transport mode with non-NULL payload authentication.
- D. Mobile IPv6 control messages are protected by SHA-2.
- E. IPsec SAs are used to protect dynamic home agent address discovery.
- F. IPsec SAs can be used to protect mobile prefix solicitations and advertisements.

Answer: A,C,F

Explanation:

QUESTION NO: 98

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

- A. A 56-bit key is used to encrypt 56-bit blocks of plaintext.
- B. A 56-bit key is used to encrypt 64-bit blocks of plaintext.
- C. Each block of plaintext is processed through 16 rounds of identical operations.
- D. Each block of plaintext is processed through 64 rounds of identical operations.
- E. ECB, CBC, and CFB are modes of DES.
- F. Each Block of plaintext is processed through 8 rounds of identical operations.
- G. CTR, CBC, and OFB are modes of DES.

Answer: B,C,E

Explanation:

QUESTION NO: 99

Comparing and contrasting IKEv1 and IKEv2, which three statements are true? (Choose three.)

- A. IKEv2 adds EAP as a method of authentication for clients; IKEv1 does not use EAP.
- B. IKEv1 and IKEv2 endpoints indicate support for NAT-T via the vendor_ID payload.
- C. IKEv2 and IKEv1 always ensure protection of the identities of the peers during the negotiation process.
- D. IKEv2 provides user authentication via the IKE_AUTH exchange; IKEv1 uses the XAUTH exchange.
- E. IKEv1 and IKEv2 both use INITIAL_CONTACT to synchronize SAs.
- F. IKEv1 supports config mode via the SET/ACK and REQUEST/RESPONSE methods; IKEv2 supports only REQUEST/RESPONSE.

Answer: A,D,E

Explanation:

QUESTION NO: 100

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

- A. GDOI uses TCP port 848.
- B. The GROUPKEY_PULL exchange is protected by an IKE phase 1 exchange.
- C. The KEK protects the GROUPKEY_PUSH message.
- D. The TEK is used to encrypt and decrypt data traffic.
- E. GDOI does not support PFS.

Answer: B,C,D

Explanation:

Topic 2, Volume B

QUESTION NO: 101

Which three nonproprietary EAP methods do not require the use of a client-side certificate for mutual authentication? (Choose three.)

- A. LEAP**
- B. EAP-TLS**
- C. PEAP**
- D. EAP-TTLS**
- E. EAP-FAST**

Answer: C,D,E

Explanation:

QUESTION NO: 102

When you compare WEP to WPA (not WPA2), which three protections are gained? (Choose three.)

- A. a message integrity check**
- B. AES-based encryption**
- C. avoidance of weak Initialization vectors**
- D. longer RC4 keys**
- E. a rekeying mechanism**

Answer: A,C,E

Explanation:

QUESTION NO: 103

Which option shows the correct sequence of the DHCP packets that are involved in IP address assignment between the DHCP client and the server?

- A. REQUEST, OFFER, ACK**

- B. DISCOVER, OFFER, REQUEST, ACK
- C. REQUEST, ASSIGN, ACK
- D. DISCOVER, ASSIGN, ACK
- E. REQUEST, DISCOVER, OFFER, ACK

Answer: B

Explanation:

QUESTION NO: 104

Which common FTP client command transmits a direct, byte-for-byte copy of a file?

- A. ascii
- B. binary
- C. hash
- D. quote
- E. glob

Answer: B

Explanation:

QUESTION NO: 105

Which option is a desktop sharing application, used across a variety of platforms, with default TCP ports 5800/5801 and 5900/5901?

- A. X Windows
- B. remote desktop protocol
- C. VNC
- D. desktop proxy

Answer: C

Explanation:

QUESTION NO: 106

Which two of the following provide protect against man-in-the-middle attacks? (Choose two.)

- A. TCP initial sequence number randomization?
- B. TCP sliding-window checking
- C. Network Address Translation
- D. IPsec VPNs
- E. Secure Sockets Layer

Answer: D,E

Explanation:

QUESTION NO: 107

An exploit that involves connecting to a specific TCP port and gaining access to an administrative command prompt is an example of which type of attack?

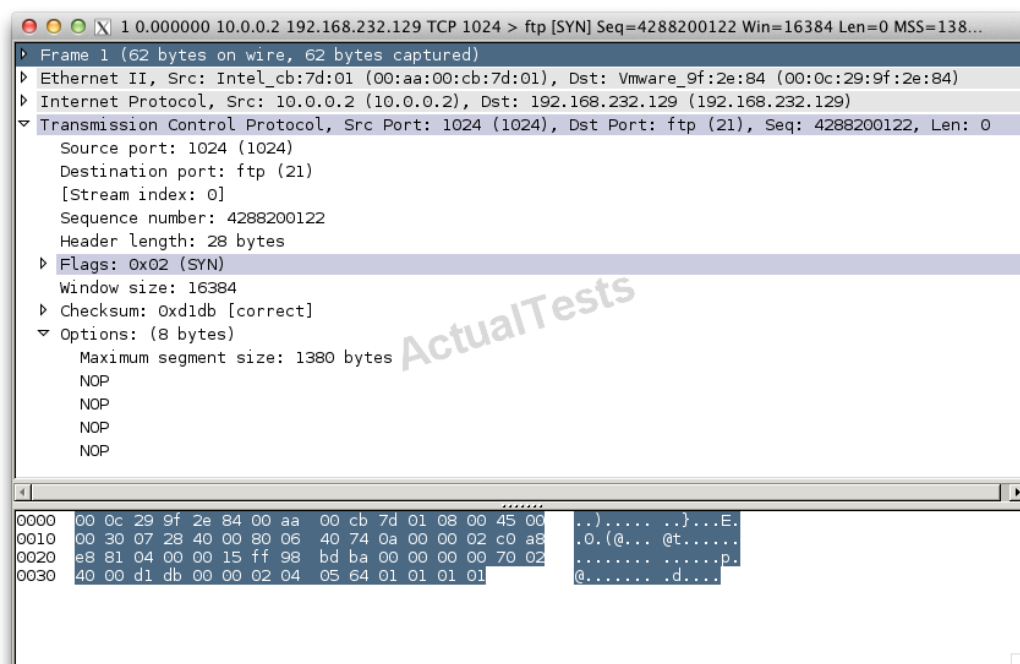
- A. botnet
- B. Trojan horse
- C. privilege escalation
- D. DoS

Answer: C

Explanation:

QUESTION NO: 108

Refer to the exhibit.



Which statement is true?

- A. This packet decoder is using relative TCP sequence numbering?.
- B. This TCP client is proposing the use of TCP window scaling?.
- C. This packet represents an active FTP data session?.
- D. This packet contains no TCP payload.

Answer: D

Explanation:

QUESTION NO: 109

When configuring an Infrastructure ACL (iACL) to protect the IPv6 infrastructure of an enterprise network, where should the iACL be applied??

- A. all infrastructure devices in both the inbound and outbound direction
- B. all infrastructure devices in the inbound direction
- C. all infrastructure devices in the outbound direction
- D. all parameter devices in both the inbound and outbound direction
- E. all parameter devices in the inbound direction
- F. all parameter devices in the outbound direction

Answer: E

Explanation:

QUESTION NO: 110

What feature on the Cisco ASA is used to check for the presence of an up-to-date antivirus vendor on an AnyConnect client?

- A. Dynamic Access Policies with no additional options
- B. Dynamic Access Policies with Host Scan enabled
- C. advanced endpoint assessment
- D. LDAP attribute maps obtained from Antivirus vendor

Answer: B

Explanation:

QUESTION NO: 111

What type of attack consists of injecting traffic that is marked with the DSCP value of EF into the network?

- A. brute-force attack
- B. QoS marking attack
- C. DHCP starvation attack
- D. SYN flood attack

Answer: B

Explanation:

QUESTION NO: 112

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: 113

Which three multicast features are supported on the Cisco ASA? (Choose three.)

- A. PIM sparse mode?
- B. IGMP forwarding?
- C. Auto-RP
- D. NAT of multicast traffic?

Answer: A,B,D

Explanation:

QUESTION NO: 114

Which three configuration tasks are required for VPN clustering of AnyConnect clients that are connecting to an FQDN on the Cisco ASA?? (Choose three.)

- A. The redirect-fqdn command must be entered under the vpn load-balancing sub-configuration.
- B. Each ASA in the VPN cluster must be able to resolve the IP of all DNS hostnames that are used in the cluster?.
- C. The identification and CA certificates for the master FQDN hostname must be imported into each VPN cluster-member device?.
- D. The remote-access IP pools must be configured the same on each VPN cluster-member interface.

Answer: A,B,C

Explanation:

QUESTION NO: 115

Which three statements are true about objects and object groups on a Cisco ASA appliance that is running Software Version 8.4 or later? (Choose three.)

- A. TCP, UDP, ICMP, and ICMPv6 are supported service object protocol types.
- B. IPv6 object nesting is supported.
- C. Network objects support IPv4 and IPv6 addresses.
- D. Objects are not supported in transparent mode.
- E. Objects are supported in single- and multiple-context firewall modes.

Answer: A,C,E

Explanation:

QUESTION NO: 116

Which command is used to replicate HTTP connections from the Active to the Standby Cisco ASA appliance in failover?

- A. monitor-interface http
- B. failover link fover replicate http
- C. failover replication http
- D. interface fover
replicate http standby
- E. No command is needed, as this is the default behavior.

Answer: C

Explanation:

QUESTION NO: 117

policy-map type inspect ipv6 IPv6-map

match header routing-type range 0 255

drop

class-map outside-class

match any

policy-map outside-policy

class outside-class

inspect ipv6 IPv6-map

service-policy outside-policy interface outside

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: xxxxxxxx

Confirm Password: xxxxxxxx

☐ Certificate Authentication

Name: [dropdown]

☐ Send CA Certificate Chain

Erase User Password Save Cancel

Given the Cisco ASA configuration above, which commands need to be added in order for the Cisco ASA appliance to deny all IPv6 packets with more than three extension headers?

- A.** policy-map type inspect ipv6 IPv6-map
match ipv6 header
count > 3
- B.** policy-map outside-policy
class outside-class
inspect ipv6 header count gt 3
- C.** class-map outside-class
match ipv6 header count greater 3
- D.** policy-map type inspect ipv6 IPv6-map
match header count gt 3
drop

Answer: D

Explanation:

QUESTION NO: 118

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: 119

Which three NAT types support bidirectional traffic initiation? (Choose three.)

- A. static NAT
- B. NAT exemption
- C. policy NAT with nat/global
- D. static PAT
- E. identity NAT

Answer: A,B,D

Explanation:

QUESTION NO: 120

Which IPS module can be installed on the Cisco ASA 5520 appliance?

- A. IPS-AIM
- B. AIP-SSM
- C. AIP-SSC
- D. NME-IPS-K9
- E. IDSM-2

Answer: B

Explanation:

QUESTION NO: 121

Which two options best describe the authorization process as it relates to network access? (Choose two.)

- A. the process of identifying the validity of a certificate, and validating specific fields in the certificate against an identity store
- B. the process of providing network access to the end user
- C. applying enforcement controls, such as downloadable ACLs and VLAN assignment, to the network access session of a user
- D. the process of validating the provided credentials

Answer: B,C

Explanation:

QUESTION NO: 122

If ISE is not Layer 2 adjacent to the Wireless LAN Controller, which two options should be configured on the Wireless LAN Controller to profile wireless endpoints accurately? (Choose two.)

- A. Configure the Call Station ID Type to be: "IP Address".
- B. Configure the Call Station ID Type to be: "System MAC Address".
- C. Configure the Call Station ID Type to be: "MAC and IP Address".
- D. Enable DHCP Proxy.
- E. Disable DHCP Proxy.

Answer: B,E

Explanation:

QUESTION NO: 123

Refer to the exhibit.

The screenshot shows the 'VPN Client | Properties for "Test ASA"' window. The 'Connection Entry' is 'Test ASA', 'Host' is '10.1.1.1', and 'Description' is empty. The 'Authentication' tab is selected, showing 'Group Authentication' as the chosen method. The 'Name' field contains 'test', and both 'Password' and 'Confirm Password' fields are masked with 'xxxxxxx'. The 'Certificate Authentication' option is unselected. At the bottom, there are buttons for 'Erase User Password', 'Save', and 'Cancel'. A Cisco logo is visible in the top right corner of the dialog.

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: 124

Refer to the exhibit.

R1#show crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	LastSeqN	IP-Address
1655	IPsec	SHA+AES	0	0	0	7.7.11.33
1656	IPsec	SHA+AES	9	0	0	7.7.11.33

R2#show crypto engine connections active

Crypto Engine Connections

ID	Type	Algorithm	Encrypt	Decrypt	LastSeqN	IP-Address
1655	IPsec	SHA+AES	0	0	0	7.7.11.35
1656	IPsec	SHA+AES	0	0	0	7.7.11.35

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: 125

Which two methods are used for forwarding traffic to the Cisco ScanSafe Web Security service? (Choose two.)

- A. Cisco AnyConnect VPN Client with Web Security and ScanSafe subscription
- B. Cisco ISR G2 Router with SECK9 and ScanSafe subscription
- C. Cisco ASA adaptive security appliance using DNAT policies to forward traffic to ScanSafe subscription servers
- D. Cisco Web Security Appliance with ScanSafe subscription

Answer: B,C

Explanation:

QUESTION NO: 126

Which four statements about SeND for IPv6 are correct? (Choose four.)

- A. It protects against rogue RAs.
- B. NDP exchanges are protected by IPsec SAs and provide for anti-replay.
- C. It defines secure extensions for NDP.
- D. It authorizes routers to advertise certain prefixes.
- E. It provides a method for secure default router election on hosts.
- F. Neighbor identity protection is provided by Cryptographically Generated Addresses that are derived from a Diffie-Hellman key exchange.
- G. It is facilitated by the Certification Path Request and Certification Path Response ND messages.

Answer: A,C,D,E

Explanation:

QUESTION NO: 127

What is the recommended network MACSec policy mode for high security deployments?

- A. should-secure
- B. must-not-secure
- C. must-secure
- D. monitor-only
- E. high-impact

Answer: A

Explanation:

QUESTION NO: 128

Which three statements about NetFlow version 9 are correct? (Choose three.)

- A. It is backward-compatible with versions 8 and 5.
- B. Version 9 is dependent on the underlying transport; only UDP is supported.
- C. A version 9 export packet consists of a packet header and flow sets.
- D. Generating and maintaining valid template flow sets requires additional processing.
- E. NetFlow version 9 does not access the NetFlow cache entry directly.

Answer: C,D,E

Explanation:

QUESTION NO: 129

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

- A. It requires that IP protocol 8472 be opened to allow traffic through a firewall.
- B. Layer 2 frames are encapsulated in IP, using a VXLAN ID to identify the source VM.
- C. A VXLAN gateway maps VXLAN IDs to VLAN IDs.
- D. IGMP join messages are sent by new VMs to determine the VXLAN multicast IP.
- E. A VXLAN ID is a 32-bit value.

Answer: B,C,D

Explanation:

QUESTION NO: 130

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: 131

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: 132

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: 133

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: 134

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: 135

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: 136

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

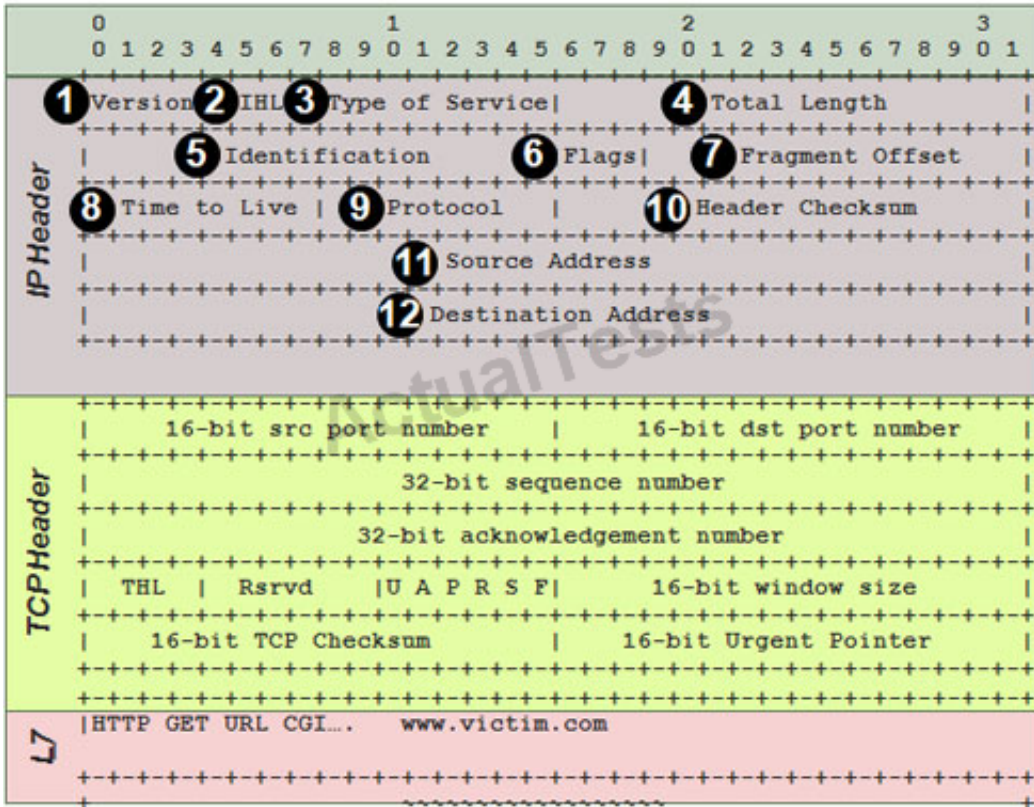
- A. 8 bytes, and protocol number 74
- B. 4 bytes, and protocol number 47
- C. 2 bytes, and protocol number 71
- D. 24 bytes, and protocol number 1
- E. 8 bytes, and protocol number 47

Answer: B

Explanation:

QUESTION NO: 137

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: 138

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: 139

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: 140

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: 141

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: 142

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: 143

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: 144

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: 145

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: 146

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: 147

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: 148

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: 149

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: 150

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: 151

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: 152

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: 153

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: 154

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: 155

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: A

Explanation:

QUESTION NO: 156

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: 157

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: 158

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: 159

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: 160

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: 161

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: 162

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: 163

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: 164

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: 165

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.)

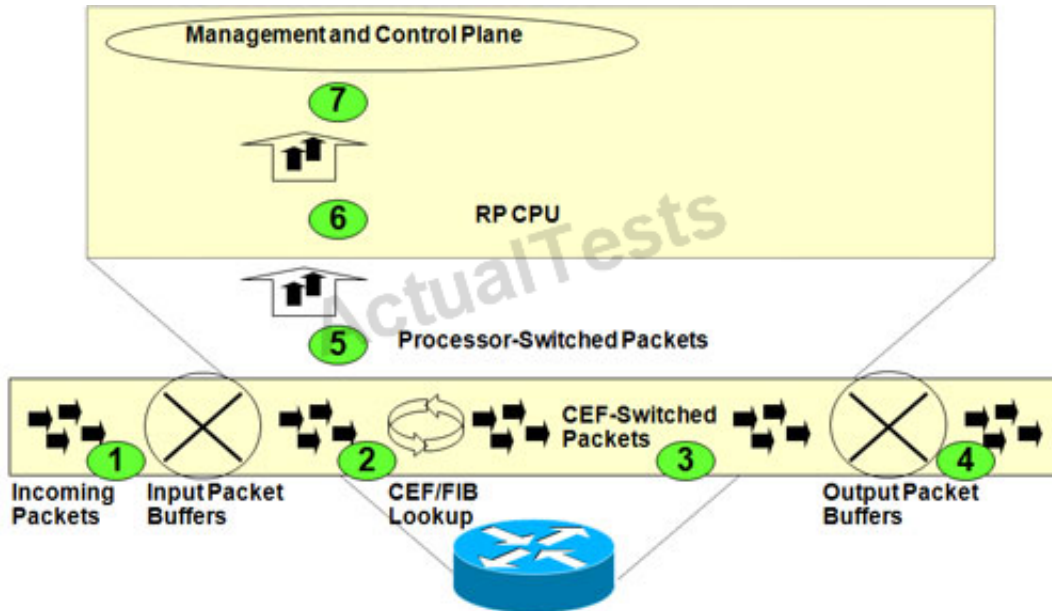
- A. interface Tunnel0
tunnel mode ipsec ipv6
- B. crypto isakmp-profile
match identity address ipv6 any
- C. interface Tunnel0
ipv6 enable
- D. ipv6 unicast-routing
- E. interface Tunnel0
ipv6 enable-ipsec

Answer: A,C,D

Explanation:

QUESTION NO: 166

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: 167

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: 168

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: 169

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: 170

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: 171

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: 172

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: 173

According to 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: 174

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: 175

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: 176

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: 177

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

- 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.

Answer: A,C,E

Explanation:

QUESTION NO: 178

Which two VLSM subnets, when taken as a pair, overlap? (Choose two.)

- A. 10.22.21.128/26
- B. 10.22.22.128/26
- C. 10.22.22.0/27
- D. 10.22.20.0/23
- E. 10.22.16.0/22

Answer: A,D

Explanation:

QUESTION NO: 179

The address of an inside client is translated from a private address to a public address by a NAT

router for access to an outside web server. What term describes the destination address (client) after the outside web server responds, and before it hits the NAT router?

- A. inside local
- B. inside global
- C. outside local
- D. outside global

Answer: B

Explanation:

QUESTION NO: 180

What is the ICMPv6 type and destination IPv6 address for a Neighbor Solicitation packet that is sent by a router that wants to learn about a newly introduced network device?

- A. ICMP type 136 and the Solicited-Node multicast address
- B. ICMP type 135 and the Broadcast address
- C. ICMP type 136 and the All-Routers multicast address
- D. ICMP type 135 and the All-Routers multicast address
- E. ICMP type 135 and the Solicited-Node multicast address
- F. ICMP type 136 and the Broadcast address

Answer: E

Explanation:

QUESTION NO: 181

Which three statements are true about Cryptographically Generated Addresses for IPv6? (Choose three.)

- A. They prevent spoofing and stealing of existing IPv6 addresses.
- B. They are derived by generating a random 128-bit IPv6 address based on the public key of the node.
- C. They are used for securing neighbor discovery using SeND.
- D. SHA or MD5 is used during their computation.
- E. The minimum RSA key length is 512 bits.
- F. The SHA-1 hash function is used during their computation.

Answer: A,C,F

Explanation:

QUESTION NO: 182

Which three options are extension headers that are implemented in IPv6? (Choose three.)

- A. Routing Header.
- B. Generic Tunnel Header.
- C. Quality of Service Header.
- D. Fragment Header.
- E. Encapsulating Security Payload Header.
- F. Path MTU Discovery Header.

Answer: A,D,E

Explanation:

QUESTION NO: 183

What is a key characteristic of MSTP?

- A. always uses a separate STP instance per VLAN to increase efficiency
- B. only supports a single STP instance for all VLANs
- C. is a Cisco proprietary standard
- D. several VLANs can be mapped to the same spanning-tree instance

Answer: D

Explanation:

QUESTION NO: 184

Which spanning-tree mode supports a separate spanning-tree instance for each VLAN and also supports the 802.1w standard that has a faster convergence than 802.1D?

- A. PVST+
- B. PVRST+
- C. PVST
- D. CST
- E. MST

F. RST

Answer: B

Explanation:

QUESTION NO: 185

Which three LSA types are used by OSPFv3? (Choose three.)

- A. Link LSA
- B. Intra-Area Prefix LSA
- C. Interarea-prefix LSA for ASBRs
- D. Autonomous system external LSA
- E. Internetwork LSA

Answer: A,B,D

Explanation:

QUESTION NO: 186

Which protocol provides the same functions in IPv6 that IGMP provides in IPv4 networks?

- A. ICMPv6
- B. ND
- C. MLD
- D. TLA

Answer: C

Explanation:

QUESTION NO: 187

After a client discovers a supportable wireless network, what is the correct sequence of operations that the client will take to join it?

- A. association, then authentication
- B. authentication, then association

- C. probe request, then association
- D. authentication, then authorization

Answer: B

Explanation:

QUESTION NO: 188

Which authentication scheme, that is supported on the Cisco ASA, generates a unique key that is used in a single password challenge?

- A. one-time passwords
- B. disposable certificates
- C. password management
- D. Capcha web text

Answer: A

Explanation:

QUESTION NO: 189

Which label is advertised by an LSR to inform neighboring LSRs to perform the penultimate hop popping operation?

- A. 0x00
- B. php
- C. swap
- D. push
- E. imp-null

Answer: E

Explanation:

QUESTION NO: 190

When the RSA algorithm is used for signing a message from Alice to Bob, which statement best describes that operation?

- A. Alice signs the message with her private key, and Bob verifies that signature with Alice's public key.
- B. Alice signs the message with her public key, and Bob verifies that signature with Alice's private key.
- C. Alice signs the message with Bob's private key, and Bob verifies that signature with his public key.
- D. Alice signs the message with Bob's public key, and Bob verifies that signature with his private key.
- E. Alice signs the message with her public key, and Bob verifies that signature with his private key.
- F. Alice signs the message with her private key, and Bob verifies that signature with his public key.

Answer: A

Explanation:

QUESTION NO: 191

Which three statements about triple DES are true? (Choose three.)

- A. For 3DES, ANSI X9.52 describes three options for the selection of the keys in a bundle, where all keys are independent.
- B. A 3DES key bundle is 192 bits long.
- C. A 3DES keyspace is 168 bits.
- D. CBC, 64-bit CFB, OFB, and CTR are modes of 3DES.
- E. 3DES involves encrypting a 64-bit block of plaintext with the 3 keys of the key bundle.

Answer: B,C,D

Explanation:

QUESTION NO: 192

Which three options correctly describe the AH protocol? (Choose three.)

- A. The AH protocol encrypts the entire IP and upper layer protocols for security.
- B. The AH protocol provides connectionless integrity and data origin authentication.
- C. The AH protocol provides protection against replay attacks.
- D. The AH protocol supports tunnel mode only.
- E. The AH protocol uses IP protocol 51.
- F. The AH protocol supports IPv4 only.

Answer: B,C,E

Explanation:

QUESTION NO: 193

Which three features are supported with ESP? (Choose three.)

- A. ESP uses IP protocol 50.
- B. ESP supports Layer 4 and above encryption only.
- C. ESP provides confidentiality, data origin authentication, connectionless integrity, and antireplay service.
- D. ESP supports tunnel or transport modes.
- E. ESP has less overhead and is faster than the AH protocol.
- F. ESP provides confidentiality, data origin authentication, connection-oriented integrity, and antireplay service.

Answer: A,C,D

Explanation:

QUESTION NO: 194

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

- A. TLS protocol uses a MAC to protect the message integrity.
- B. TLS data encryption is provided by the use of asymmetric cryptography.
- C. The identity of a TLS peer can be authenticated using public key or asymmetric cryptography.
- D. TLS protocol is originally based on the SSL 3.0 protocol specification.
- E. TLS provides support for confidentiality, authentication, and nonrepudiation.

Answer: A,C,D

Explanation:

QUESTION NO: 195

Which three RADIUS protocol statements are true? (Choose three.)

- A. RADIUS protocol runs over TCP 1645 and 1646.
- B. Network Access Server operates as a server for RADIUS.
- C. RADIUS packet types for authentication include Access-Request, Access-Challenge, Access-

Accept, and Access-Reject.

D. RADIUS protocol runs over UDP 1812 and 1813.

E. RADIUS packet types for authentication include Access-Request, Access-Challenge, Access-Permit, and Access-Denied.

F. RADIUS supports PPP, PAP, and CHAP as authentication methods.

Answer: C,D,F

Explanation:

QUESTION NO: 196

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

A. OCSP is defined in RFC2560.

B. OCSP uses only http as a transport.

C. OCSP responders can use RSA and DSA signatures to validate that responses are from trusted entities.

D. A response indicator may be good, revoked, or unknown.

E. OCSP is an updated version SCEP.

Answer: A,C,D

Explanation:

QUESTION NO: 197

Which three statements describe the security weaknesses of WEP? (Choose three.)

A. Key strength is weak and non-standardized.

B. The WEP ICV algorithm is not optimal for cryptographic integrity checking.

C. There is no key distribution mechanism.

D. Its key rotation mechanism is too predictable.

E. For integrity, it uses MD5, which has known weaknesses.

Answer: A,B,C

Explanation:

QUESTION NO: 198

In HTTPS session establishment, what does the server hello message inform the client?

- A. that the server will accept only HTTPS traffic
- B. which versions of SSL/TLS the server will accept
- C. which ciphersuites the client may choose from
- D. which ciphersuite the server has chosen to use
- E. the PreMaster secret to use in generating keys

Answer: D

Explanation:

QUESTION NO: 199

DHCPv6 is used in which IPv6 address autoconfiguration method?

- A. stateful autoconfiguration
- B. stateless autoconfiguration
- C. EUI-64 address generation
- D. cryptographically generated addresses

Answer: A

Explanation:

QUESTION NO: 200

Refer to the exhibit.

```
C:\Users> nslookup
> set type=soa
> cisco.com

Server: dns1.abcompany.com
Address: 2.3.4.5

cisco.com
    responsible mail addr = postmaster.cisco.com
    serial = 10973831
    refresh = 7200 (2 hours)
    retry = 1800 (30 mins)
    expire = 864000 (10 days)
    default TTL = 86400 (1 day)
cisco.com      nameserver = ns2.cisco.com
cisco.com      nameserver = ns1.cisco.com
ns1.cisco.com  internet address = 72.163.5.201
ns2.cisco.com  internet address = 64.102.255.44
```

Which statement regarding the output is true?

- A. Every 1800 seconds the secondary name server will query the SOA record of the primary name server for updates.
- B. If the secondary name server has an SOA record with the serial number of 10973815, it will initiate a zone transfer on the next cycle.
- C. Other DNS servers will cache records from this domain for 864000 seconds (10 days) before requesting them again.
- D. Email queries concerning this domain should be sent to "admin@postmaster.cisco.com".
- E. Both primary and secondary name servers will clear (refresh) their caches every 7200 seconds to ensure that up-to-date information is always in use.

Answer: B

Explanation:

Topic 3, Volume C

QUESTION NO: 201

Which two options represent definitions that are found in the syslog protocol (RFC 5426)?
(Choose two.)

- A. Syslog message transport is reliable.
- B. Each syslog datagram must contain only one message.
- C. IPv6 syslog receivers must be able to receive datagrams of up to 1180 bytes.
- D. Syslog messages must be prioritized with an IP precedence of 7.
- E. Syslog servers must use NTP for the accurate time stamping of message arrival.

Answer: B,C

Explanation:

QUESTION NO: 202

According to RFC-5426, syslog senders must support sending syslog message datagrams to which port?

- A. TCP port 514
- B. UDP port 514
- C. TCP port 69
- D. UDP port 69
- E. TCP port 161
- F. UDP port 161

Answer: B

Explanation:

QUESTION NO: 203

Refer to the exhibit.

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:12	
194 vty 0	admin	idle	00:00:02	internal.example.com

What service is enabled on the router for a remote attacker to obtain this information?

- A. TCP small services
- B. finger
- C. maintenance operation protocol
- D. chargen
- E. Telnet
- F. CEF

Answer: B

Explanation:

QUESTION NO: 204

In an 802.11 wireless network, what would an attacker have to spoof to initiate a deauthentication attack against connected clients?

- A. the BSSID of the AP where the clients are currently connected
- B. the SSID of the wireless network
- C. the MAC address of the target client machine
- D. the broadcast address of the wireless network

Answer: A

Explanation:

QUESTION NO: 205

What is the commonly known name for the process of generating and gathering initialization vectors, either passively or actively, for the purpose of determining the security key of a wireless network?

- A. WEP cracking
- B. session hijacking
- C. man-in-the-middle attacks
- D. disassociation flood frames

Answer: A

Explanation:

QUESTION NO: 206

According to RFC 4890, which four ICMPv6 types are recommended to be allowed to transit a firewall? (Choose four.)

- A. Type 1 - destination unreachable
- B. Type 2 - packet too big
- C. Type 3 - time exceeded
- D. Type 0 - echo reply
- E. Type 8 - echo request
- F. Type 4 - parameter problem

Answer: A,B,C,F

Explanation:

QUESTION NO: 207

Which action is performed first on the Cisco ASA appliance when it receives an incoming packet on its outside interface?

- A. check if the packet is permitted or denied by the inbound ACL applied to the outside interface
- B. check if the packet is permitted or denied by the global ACL
- C. check if the packet matches an existing connection in the connection table
- D. check if the packet matches an inspection policy
- E. check if the packet matches a NAT rule
- F. check if the packet needs to be passed to the Cisco ASA AIP-SSM for inspections

Answer: C

Explanation:

QUESTION NO: 208

Refer to the exhibit.

The screenshot shows the 'Edit Access Rule' dialog box in Cisco ASDM. The 'Interface' is set to '-- Any --'. The 'Action' is 'Permit'. The 'Source' is '1.1.1.1' and the 'Destination' is '2.2.2.1'. The 'Service' is 'ip'. The 'Description' field is empty. The 'Enable Logging' checkbox is checked, and the 'Logging Level' is set to 'Default'. A 'More Options' tag is visible at the bottom. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

Which three statements about the Cisco ASDM screen seen in the exhibit are true? (Choose three.)

- A.** This access rule is applied to all the ASA interfaces in the inbound direction.
- B.** The ASA administrator needs to expand the More Options tag to configure the inbound or outbound direction of the access rule.
- C.** The ASA administrator needs to expand the More Options tag to apply the access rule to an interface.
- D.** The resulting ASA CLI command from this ASDM configuration is `access-list global_access line 1 extended permit ip host 1.1.1.1 host 2.2.2.1`.
- E.** This access rule is valid only on the ASA appliance that is running software release 8.3 or later.
- F.** This is an outbound access rule.

Answer: A,D,E

Explanation:

QUESTION NO: 209

If an incoming packet from the outside interface does not match an existing connection in the connection table, which action will the Cisco ASA appliance perform next?

- A. drop the packet
- B. check the outside interface inbound ACL to determine if the packet is permitted or denied
- C. perform NAT operations on the packet if required
- D. check the MPF policy to determine if the packet should be passed to the SSM
- E. perform stateful packet inspection based on the MPF policy

Answer: B

Explanation:

QUESTION NO: 210

Refer to the exhibit.

```
ASA# show failover
Failover On
Failover unit Primary
Failover LAN Interface: fover GigabitEthernet0/4 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 114 maximum
Version: Ours 8.6(1), Mate 8.6(1)
Group 1 last failover at: 13:18:39 UTC Sep 5 2012
Group 2 last failover at: 13:18:39 UTC Sep 5 2012

This host:      Primary
Group 1        State:          Standby Ready
                Active time:   176 (sec)
Group 2        State:          Active
                Active time:   176 (sec)

slot 0: ASA5512 hw/sw rev (1.0/8.6(1)) status (Up Sys)
c1 Interface outside (10.10.55.11): Normal (Monitored)
c1 Interface inside (10.10.3.11): Normal (Monitored)
c2 Interface outside (10.10.5.10): Normal (Monitored)
c2 Interface inside (10.10.8.10): Normal (Monitored)

Other host:     Secondary
Group 1        State:          Active
                Active time:   0 (sec)
Group 2        State:          Standby Ready
                Active time:   0 (sec)

slot 0: ASA5512 hw/sw rev (1.0/8.6(1)) status (Up Sys)
c1 Interface outside (10.10.55.10): Normal (Monitored)
c1 Interface inside (10.10.3.10): Normal (Monitored)
c2 Interface outside (10.10.5.11): Normal (Monitored)
c2 Interface inside (10.10.8.11): Normal (Monitored)
```

Choose the correct description of the implementation that produced this output on the Cisco ASA appliance.

- A. stateful failover using active-active for multi-context
- B. stateful failover using active-standby for multi-context
- C. stateful failover using active-standby for single-context
- D. stateless failover using interface-level failover for multi-context

Answer: A

Explanation:

QUESTION NO: 211

When you are configuring QoS on the Cisco ASA appliance, which four are valid traffic selection criteria? (Choose four.)

- A. VPN group
- B. tunnel group
- C. IP precedence
- D. DSCP
- E. default-inspection-traffic
- F. qos-group

Answer: B,C,D,E

Explanation:

QUESTION NO: 212

Which command is required in order for the Botnet Traffic Filter on the Cisco ASA appliance to function properly?

- A. dynamic-filter inspect tcp/80
- B. dynamic-filter whitelist
- C. inspect botnet
- D. inspect dns dynamic-filter-snoop

Answer: D

Explanation:

QUESTION NO: 213

You have been asked to configure a Cisco ASA appliance in multiple mode with these settings:

- A) You need two customer contexts, named contextA and contextB.
- B) Allocate interfaces G0/0 and G0/1 to contextA.
- C) Allocate interfaces G0/0 and G0/2 to contextB.
- D) The physical interface name for G0/1 within contextA should be "inside".
- E) All other context interfaces must be viewable via their physical interface names.

If the admin context is already defined and all interfaces are enabled, which command set will complete this configuration?

A. context contextA

```
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/1 inside
context contextB
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/2 visible
```

B. context contexta

```
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/1 inside
context contextb
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/2 visible
```

C. context contextA

```
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0 invisible
allocate-interface GigabitEthernet0/1 inside
context contextB
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0 invisible
allocate-interface GigabitEthernet0/2 invisible
```

D. context contextA

```
config-url disk0:/contextA.cfg
```

```
allocate-interface GigabitEthernet0/0
allocate-interface GigabitEthernet0/1 inside
context contextB
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/0
allocate-interface GigabitEthernet0/2
E. context contextA
config-url disk0:/contextA.cfg
allocate-interface GigabitEthernet0/0 visible
allocate-interface GigabitEthernet0/1 inside
context contextB
config-url disk0:/contextB.cfg
allocate-interface GigabitEthernet0/1 visible
allocate-interface GigabitEthernet0/2 visible
```

Answer: A

Explanation:

QUESTION NO: 214

Which four configuration steps are required to implement a zone-based policy firewall configuration on a Cisco IOS router? (Choose four.)

- A. Create the security zones and security zone pairs.
- B. Create the self zone.
- C. Create the default global inspection policy.
- D. Create the type inspect class maps and policy maps.
- E. Assign a security level to each security zone.
- F. Assign each router interface to a security zone.
- G. Apply a type inspect policy map to each zone pair.

Answer: A,D,F,G

Explanation:

QUESTION NO: 215

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

ipv6 access-list extended ZBFW_ACL
  permit ipv6 any any sequence 10

class-map type inspect match-all HTTP_CMAP
  match protocol HTTP
class-map type inspect match-all SMTP_CMAP
  match protocol SMTP
  match access-group name ZBFW_ACL
class-map type inspect match-all TCP_CMAP

policy-map type inspect IN-OUT_PMAP
  class type inspect TCP_CMAP
    inspect
  class type inspect HTTP_CMAP
    pass
  class type inspect SMTP_CMAP
    inspect
  class class-default
    drop

zone-pair IN-OUT_ZP source inside destination outside
  service-policy type inspect IN-OUT_PMAP

```

The client is protected by a firewall. An IPv6 SMTP connection from the client to the server on TCP port 25 will be subject to which action?

- A. pass action by the HTTP_CMAP
- B. inspection action by the TCP_CMAP
- C. inspection action by the SMTP_CMAP
- D. drop action by the default class
- E. pass action by the HTTP_CMAP

Answer: B

Explanation:

QUESTION NO: 216

Which Cisco IPS appliance signature engine defines events that occur in a related manner, within a sliding time interval, as components of a combined signature?

- A. Service engine
- B. Sweep engine
- C. Multistring engine
- D. Meta engine

Answer: D

Explanation:

QUESTION NO: 217

Which three options are the types of zones that are defined for anomaly detection on the Cisco IPS Sensor? (Choose three.)

- A. inside
- B. outside
- C. internal
- D. external
- E. illegal
- F. baseline

Answer: C,D,E

Explanation:

QUESTION NO: 218

Which three statements are true regarding RFC 5176 (Change of Authorization)? (Choose three.)

- A. It defines a mechanism to allow a RADIUS server to initiate a communication inbound to a NAD.
- B. It defines a wide variety of authorization actions, including "reauthenticate."
- C. It defines the format for a Change of Authorization packet.
- D. It defines a DM.

E. It specifies that TCP port 3799 be used for transport of Change of Authorization packets.

Answer: A,C,D

Explanation:

QUESTION NO: 219

Which three statements are true regarding Security Group Tags? (Choose three.)

- A. When using the Cisco ISE solution, the Security Group Tag gets defined as a separate authorization result.
- B. When using the Cisco ISE solution, the Security Group Tag gets defined as part of a standard authorization profile.
- C. Security Group Tags are a supported network authorization result using Cisco ACS 5.x.
- D. Security Group Tags are a supported network authorization result for 802.1X, MAC Authentication Bypass, and WebAuth methods of authentication.
- E. A Security Group Tag is a variable length string that is returned as an authorization result.

Answer: A,C,D

Explanation:

QUESTION NO: 220

Refer to the exhibit.

```
w6d: IPSEC(validate_proposal_request): proposal part #1,  
  (key eng. msg.) INBOUND local= 172.16.1.20, remote= 172.16.1.10,  
    local_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),  
    remote_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),  
    protocol= ESP, transform= esp-3des esp-md5-hmac ,  
    lifedur= 0s and 0kb,  
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4  
w6d: IPSEC(validate_transform_proposal): proxy identities not supported  
w6d: ISAKMP (0:2): IPsec policy invalidated proposal  
w6d: ISAKMP (0:2): phase 2 SA not acceptable!
```

What is the cause of the issue that is reported in this debug output?

- A. The identity of the peer is not acceptable.
- B. There is an esp transform mismatch.

- C. There are mismatched ACLs on remote and local peers.
- D. The SA lifetimes are set to 0.

Answer: C

Explanation:

QUESTION NO: 221

Refer to the exhibit,

```
aaa authentication login vpn local
aaa authorization network vpn local
```

```
crypto isakmp client configuration group ezvpn_DVTI
key cisco123
domain cisco.com
pool dynpool
acl 101
save-password
```

```
crypto isakmp profile isakmp_profile_dvti
  client authentication list vpn
  client configuration address respond
```

which shows a partial configuration for the EzVPN server. Which three missing ISAKMP profile options are required to support EzVPN using DVTI? (Choose three.)

- A. match identity group
- B. trustpoint
- C. virtual-interface
- D. keyring
- E. enable udp-encapsulation
- F. isakmp authorization list
- G. virtual-template

Answer: A,F,G

Explanation:

QUESTION NO: 222

Which two certificate enrollment methods can be completed without an RA and require no direct connection to a CA by the end entity? (Choose two.)

- A. SCEP
- B. TFTP
- C. manual cut and paste
- D. enrollment profile with direct HTTP
- E. PKCS#12 import/export

Answer: C,E

Explanation:

QUESTION NO: 223

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

- A. Control Plane Policing
- B. interface ACLs
- C. uRPF
- D. MD5 authentication
- E. FPM
- F. QoS

Answer: B,C,E,F

Explanation:

QUESTION NO: 224

In order to implement CGA on a Cisco IOS router for SeND, which three configuration steps are required? (Choose three.)

- A. Generate an RSA key pair.
- B. Define a site-wide pre-shared key.
- C. Define a hash algorithm that is used to generate the CGA.
- D. Generate the CGA modifier.
- E. Assign a CGA link-local or globally unique address to the interface.
- F. Define an encryption algorithm that is used to generate the CGA.

Answer: A,D,E

Explanation:

QUESTION NO: 225

As defined by Cisco TrustSec, which EAP method is used for Network Device Admission Control authentication?

- A. EAP-FAST
- B. EAP-TLS
- C. PEAP
- D. LEAP

Answer: A

Explanation:

QUESTION NO: 226

Which three statements about the keying methods used by MACSec are true? (Choose three.)

- A. Key management for host-to-switch and switch-to-switch MACSec sessions is provided by MKA.
- B. A valid mode for SAP is NULL.
- C. MKA is implemented as an EAPoL packet exchange.
- D. SAP is enabled by default for Cisco TrustSec in manual configuration mode.
- E. SAP is not supported on switch SVIs.
- F. SAP is supported on SPAN destination ports.

Answer: B,C,E

Explanation:

QUESTION NO: 227

What is the function of this command?

switch(config-if)# switchport port-security mac-address sticky

- A.** It allows the switch to restrict the MAC addresses on the switch port, based on the static MAC addresses configured in the startup configuration.
- B.** It allows the administrator to manually configure the secured MAC addresses on the switch port.
- C.** It allows the switch to permanently store the secured MAC addresses in the MAC address table (CAM table).
- D.** It allows the switch to perform sticky learning, in which the dynamically learned MAC addresses are copied from the MAC address table (CAM table) to the startup configuration.
- E.** It allows the switch to dynamically learn the MAC addresses on the switch port, and the MAC addresses will be added to the running configuration

Answer: E

Explanation:

QUESTION NO: 228

When configuring a switchport for port security that will support multiple devices and that has already been configured for 802.1X support, which two commands need to be added? (Choose two.)

- A.** The 802.1X port configuration must be extended with the command `dot1x multiple-host`.
- B.** The 802.1X port configuration must be extended with the command `dot1x port-security`.
- C.** The switchport configuration needs to include the command `switchport port-security`.
- D.** The switchport configuration needs to include the `port-security aging` command.
- E.** The 802.1X port configuration needs to remain in `port-control force-authorized` rather than `port-control auto`.

Answer: A,C

Explanation:

QUESTION NO: 229

In Cisco IOS, what is the result of the `ip dns spoofing` command on DNS queries that are coming from the inside and are destined to DNS servers on the outside?

- A.** The router will prevent DNS packets without TSIG information from passing through the router.
- B.** The router will act as a proxy to the DNS request and reply to the DNS request with the IP address of the interface that received the DNS query if the outside interface is down.
- C.** The router will take the DNS query and forward it on to the DNS server with its information in place of the client IP.
- D.** The router will block unknown DNS requests on both the inside and outside interfaces.

Answer: B

Explanation:

QUESTION NO: 230

The Wi-Fi Alliance defined two certification programs, called WPA and WPA2, which are based on the IEEE 802.11i standard. Which three statements are true about these certifications? (Choose three.)

- A. WPA is based on the ratified IEEE 802.11i standard.
- B. WPA2 is based on the ratified IEEE 802.11i standard.
- C. WPA enhanced WEP with the introduction of TKIP.
- D. WPA2 requires the support of AES-CCMP.
- E. WPA2 supports only 802.1x/EAP authentication.

Answer: B,C,D

Explanation:

QUESTION NO: 231

When you are configuring the COOP feature for GETVPN redundancy, which two steps are required to ensure the proper COOP operations between the key servers? (Choose two.)

- A. Generate an exportable RSA key pair on the primary key server and export it to the secondary key server.
- B. Enable dead peer detection between the primary and secondary key servers.
- C. Configure HSRP between the primary and secondary key servers.
- D. Enable IPC between the primary and secondary key servers.
- E. Enable NTP on both the primary and secondary key servers to ensure that they are synchronized to the same clock source.

Answer: A,B

Explanation:

QUESTION NO: 232

A Cisco Easy VPN software client is unable to access its local LAN devices once the VPN tunnel is established. What is the best way to solve this issue?

- A. The IP address that is assigned by the Cisco Easy VPN Server to the client must be on the same network as the local LAN of the client.
- B. The Cisco Easy VPN Server should apply split-tunnel-policy excludespecified with a split-tunnel-list containing the local LAN addresses that are relevant to the client.
- C. The Cisco Easy VPN Server must push down an interface ACL that permits the traffic to the local LAN from the client.
- D. The Cisco Easy VPN Server should apply a split-tunnel-policy tunnelall policy to the client.
- E. The Cisco Easy VPN client machine needs to have multiple NICs to support this.

Answer: B

Explanation:

QUESTION NO: 233

During the establishment of an Easy VPN tunnel, when is XAUTH performed?

- A. at the end of IKEv1 Phase 2
- B. at the beginning of IKEv1 Phase 1
- C. at the end of Phase 1 and before Phase 2 starts in IKEv1 and IKEv2
- D. at the end of Phase 1 and before Phase 2 starts in IKEv1

Answer: D

Explanation:

QUESTION NO: 234

Which three traffic conditions can be matched when configuring single rate, dual token bucket traffic policing on Cisco routers? (Choose three.)

- A. conform
- B. normal
- C. violate
- D. peak
- E. exceed
- F. average

Answer: A,C,E

Explanation:

QUESTION NO: 235

A frame relay PVC at router HQ has a CIR of 768 kb/s and the frame relay PVC at router branch office has a CIR of 384 kb/s. Which QoS mechanism can best be used to ease the data congestion and data loss due to the CIR speed mismatch?

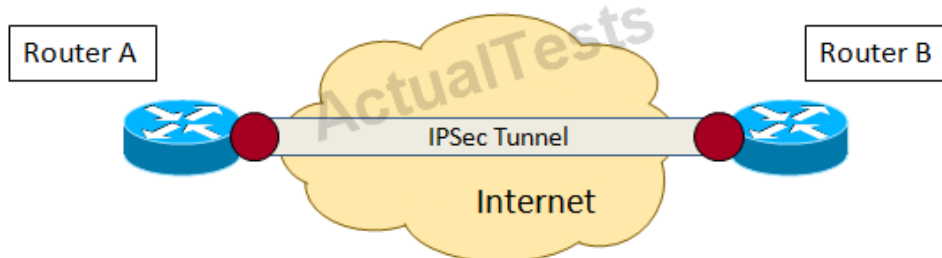
- A. traffic policing at the HQ
- B. traffic policing at the branch office
- C. traffic shaping at the HQ
- D. traffic shaping at the branch office
- E. LLQ at the HQ
- F. LLQ at the branch office

Answer: C

Explanation:

QUESTION NO: 236

Refer to the exhibit.



A customer has an IPsec tunnel that is configured between two remote offices. The customer is seeing these syslog messages on Router B:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=x, sequence number=y
```

What is the most likely cause of this error?

- A. The customer has an LLQ QoS policy that is configured on the WAN interface of Router A.
- B. A hacker on the Internet is launching a spoofing attack.
- C. Router B has an incorrectly configured IP MTU value on the WAN interface.
- D. There is packet corruption in the network between Router A and Router B.
- E. Router A and Router B are not synchronized to the same timer source.

Answer: A

Explanation:

QUESTION NO: 237

In ISO 27001 ISMS, which three of these certification process phases are required to collect information for ISO 27001? (Choose three.)

- A. discover
- B. certification audit
- C. post-audit
- D. observation
- E. pre-audit
- F. major compliance

Answer: B,C,E

Explanation:

QUESTION NO: 238

Which three statements regarding ISO 27002 and COBIT are correct? (Choose three.)

- A. COBIT and ISO 27002 both define a best practices framework for IT controls.
- B. COBIT focuses on information system processes, whereas ISO 27002 focuses on the security of the information systems.
- C. ISO 27002 addresses control objectives, whereas COBIT addresses information security management process requirements.
- D. Compared to COBIT, ISO 27002 covers a broader area in planning, operations, delivery, support, maintenance, and IT governance.
- E. Unlike COBIT, ISO 27002 is used mainly by the IT audit community to demonstrate risk mitigation and avoidance mechanisms.

Answer: A,B,C

Explanation:

QUESTION NO: 239

The IETF is a collaborative effort by the international community of Internet professionals to improve the design, use, and management of the Internet. Which international organization charters the activity of IETF?

- A. IANA**
- B. ISO**
- C. ISOC**
- D. RIR**
- E. IEC**

Answer: C

Explanation:

QUESTION NO: 240

Which RFC outlines BCP 84?

- A. RFC 3704**
- B. RFC 2827**
- C. RFC 3030**
- D. RFC 2267**
- E. RFC 1918**

Answer: A

Explanation:

QUESTION NO: 241

Which two current RFCs discuss special use IP addresses that may be used as a checklist of invalid routing prefixes for IPv4 and IPv6 addresses? (Choose two.)

- A. RFC 5156**
- B. RFC 5735**

- C. RFC 3330
- D. RFC 1918
- E. RFC 2827

Answer: A,B

Explanation:

QUESTION NO: 242

Which four options could be flagged as potential issues by a network security risk assessment?
(Choose four.)

- A. router hostname and IP addressing scheme
- B. router filtering rules
- C. route optimization
- D. database connectivity and RTT
- E. weak authentication mechanisms
- F. improperly configured email servers
- G. potential web server exploits

Answer: B,E,F,G

Explanation:

QUESTION NO: 243

Which three of these situations warrant engagement of a Security Incident Response team?
(Choose three.)

- A. loss of data confidentiality/integrity
- B. damage to computer/network resources
- C. denial of service (DoS)
- D. computer or network misuse/abuse
- E. pornographic blogs/websites

Answer: A,C,D

Explanation:

QUESTION NO: 244

Which MPLS label is the signaled value to activate PHP (penultimate hop popping)?

- A. 0x00
- B. php
- C. swap
- D. push
- E. imp-null

Answer: E

Explanation:

QUESTION NO: 245

What action will be taken by a Cisco IOS router if a TCP packet, with the DF bit set, is larger than the egress interface MTU?

- A. Split the packet into two packets, so that neither packet exceeds the egress interface MTU, and forward them out.
- B. Respond to the sender with an ICMP Type 3 , Code 4.
- C. Respond to the sender with an ICMP Type 12, Code 2.
- D. Transmit the packet unmodified.

Answer: B

Explanation:

QUESTION NO: 246

What will the receiving router do when it receives a packet that is too large to forward, and the DF bit is not set in the IP header?

- A. Drop the packet, and send the source an ICMP packet, indicating that the packet was too big to transmit.
- B. Fragment the packet into segments, with all segments having the MF bit set.
- C. Fragment the packet into segments, with all except the last segment having the MF bit set.
- D. Fragment the packet into segments, with all except the first segment having the MF bit set.

Answer: C

Explanation:

QUESTION NO: 247

Identify three IPv6 extension headers? (Choose three.)

- A. traffic class
- B. flow label
- C. routing
- D. fragment
- E. encapsulating security payload

Answer: C,D,E

Explanation:

QUESTION NO: 248

Which three statements correctly describe the purpose and operation of IPv6 RS and RA messages? (Choose three.)

- A. Both IPv6 RS and RA packets are ICMPv6 messages.
- B. IPv6 RA messages can help host devices perform stateful or stateless address autoconfiguration; RS messages are sent by hosts to determine the addresses of routers.
- C. RS and RA packets are always sent to an all-nodes multicast address.
- D. RS and RA packets are used by the duplicate address detection function of IPv6.
- E. IPv6 hosts learn connected router information from RA messages which may be sent in response to an RS message.
- F. RS and RA packets are used for IPv6 nodes to perform address resolution that is similar to ARP in IPv4.

Answer: A,B,E

Explanation:

QUESTION NO: 249

Which three statements are true regarding the EIGRP update message? (Choose three.)

- A. Updates require an acknowledgement with an ACK message.
- B. Updates can be sent to the multicast address 224.0.0.10.
- C. Updates are sent as unicasts when they are retransmitted.
- D. Updates always include all routes known by the router with partial updates sent in the Reply message.
- E. ACKs for updates are handled by TCP mechanisms.

Answer: A,B,C

Explanation:

QUESTION NO: 250

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: 251

Which two OSPF network types support the concept of a designated router? (Choose two.)

- A. broadcast
- B. NBMA
- C. point-to-multipoint
- D. point-to-multipoint nonbroadcast
- E. loopback

Answer: A,B

Explanation:

QUESTION NO: 252

Which IPv6 routing protocol can use IPv6 ESP and AH to provide integrity, authentication, and confidentiality services to protect the routing information exchange between the adjacent routing neighbors?

- A. RIPng
- B. EIGRPv6
- C. BGP-4

- D. IS-IS
- E. OSPFv6

Answer: E

Explanation:

QUESTION NO: 253

Which three IPv6 tunneling methods are point-to-multipoint in nature? (Choose three.)

- A. automatic 6to4
- B. manually configured
- C. IPv6 over IPv4 GRE
- D. ISATAP
- E. automatic IPv4-compatible

Answer: A,D,E

Explanation:

QUESTION NO: 254

Which additional capability was added in IGMPv3?

- A. leave group messages support
- B. source filtering support
- C. group-specific host membership queries support
- D. IPv6 support
- E. authentication support between the multicast receivers and the last hop router

Answer: B

Explanation:

QUESTION NO: 255

Beacons, probe request, and association request frames are associated with which category?

- A. management

- B. control
- C. data
- D. request

Answer: A

Explanation:

QUESTION NO: 256

Which feature can be implemented to avoid any MPLS packet loss?

- A. IP TTL propagation
- B. LDP IGP sync
- C. label advertisement sync
- D. conditional label advertisement
- E. PHP

Answer: B

Explanation:

QUESTION NO: 257

Which four types of VPN natively provide encryption of user traffic? (Choose four.)

- A. MPLS
- B. IPsec
- C. L2TPv3
- D. SSL
- E. VPLS
- F. AToM
- G. GETVPN
- H. Microsoft PPTP

Answer: B,D,G,H

Explanation:

QUESTION NO: 258

Which three options are components of Mobile IPv6? (Choose three.)

- A. home agent
- B. correspondent node
- C. mobile node
- D. binding node
- E. discovery probe

Answer: A,B,C

Explanation:

QUESTION NO: 259

What are two uses of an RSA algorithm? (Choose two.)

- A. data encryption
- B. digital signature verification
- C. shared key generation
- D. message hashing

Answer: A,B

Explanation:

QUESTION NO: 260

What is needed to verify a digital signature that was created using an RSA algorithm?

- A. public key
- B. private key
- C. both public and private key
- D. trusted third-party certificate

Answer: A

Explanation:

QUESTION NO: 261

Which algorithm is used to generate the IKEv2 session key?

- A. Diffie-Hellman

- B. Rivest, Shamir, and Adleman
- C. Secure Hash Algorithm
- D. Rivest Cipher 4

Answer: A

Explanation:

QUESTION NO: 262

Which statement is true about IKEv2 and IKEv1?

- A. IKEv2 can be configured to use EAP, but IKEv1 cannot.
- B. IKEv2 can be configured to use AES encryption, but IKEv1 cannot.
- C. IKEv2 can be configured to interoperate with IKEv1 on the other end.
- D. IKEv2 consumes more bandwidth than IKEv1.

Answer: A

Explanation:

QUESTION NO: 263

Which statement is true about IKEv2 preshared key authentication between two peers?

- A. IKEv2 allows usage of different preshared keys for local and remote authentication.
- B. IKEv2 allows usage of only one preshared key.
- C. IKEv2 allows usage of only one preshared key and only in hub-and-spoke topology.
- D. IKEv2 does not allow usage of preshared key authentication.

Answer: A

Explanation:

QUESTION NO: 264

How does 3DES use the DES algorithm to encrypt a message?

- A. encrypts a message with K1, decrypts the output with K2, then encrypts it with K3
- B. encrypts a message with K1, encrypts the output with K2, then encrypts it with K3
- C. encrypts K1 using K2, then encrypts it using K3, then encrypts a message using the output key

D. encrypts a message with K1, encrypts the output with the K2, then decrypts it with K3

Answer: A

Explanation:

QUESTION NO: 265

Which protocol is superseded by AES?

- A. DES
- B. RSA
- C. RC4
- D. MD5

Answer: A

Explanation:

QUESTION NO: 266

What is the purpose of the SPI field in an IPsec packet?

- A. identifies a transmission channel
- B. provides anti-replay protection
- C. ensures data integrity
- D. contains a shared session key

Answer: A

Explanation:

QUESTION NO: 267

Which IPsec protocol provides data integrity but no data encryption?

- A. AH
- B. ESP
- C. SPI
- D. DH

Answer: A

Explanation:

QUESTION NO: 268

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: 269

What entities decrypt a transmission sent by a GDOI group member?

- A. all group members
- B. the key server only
- C. the peer that is indicated by the key server
- D. the key server and the peer that is indicated by the key server

Answer: A

Explanation:

QUESTION NO: 270

What transport protocol and port are used by GDOI for its IKE sessions that are established between the group members and the key server?

- A. UDP port 848
- B. TCP port 848
- C. ESP port 51

- D. SSL port 443
- E. UDP port 4500

Answer: A

Explanation:

QUESTION NO: 271

What is the advantage of using the ESP protocol over the AH?

- A. data confidentiality
- B. data integrity verification
- C. nonrepudiation
- D. anti-replay protection

Answer: A

Explanation:

QUESTION NO: 272

What applications take advantage of a DTLS protocol?

- A. delay-sensitive applications, such as voice or video
- B. applications that require double encryption
- C. point-to-multipoint topology applications
- D. applications that are unable to use TLS

Answer: A

Explanation:

QUESTION NO: 273

What mechanism does SSL use to provide confidentiality of user data?

- A. symmetric encryption
- B. asymmetric encryption
- C. RSA public-key encryption
- D. Diffie-Hellman exchange

Answer: A

Explanation:

QUESTION NO: 274

What action does a RADIUS server take when it cannot authenticate the credentials of a user?

- A. An Access-Reject message is sent.
- B. An Access-Challenge message is sent, and the user is prompted to re-enter credentials.
- C. A Reject message is sent.
- D. A RADIUS start-stop message is sent via the accounting service to disconnect the session.

Answer: A

Explanation:

QUESTION NO: 275

Which transport mechanism is used between a RADIUS authenticator and a RADIUS authentication server?

- A. UDP, with only the password in the Access-Request packet encrypted
- B. UDP, with the whole packet body encrypted
- C. TCP, with only the password in the Access-Request packet encrypted
- D. EAPOL, with TLS encrypting the entire packet
- E. UDP RADIUS encapsulated in the EAP mode enforced by the authentication server.

Answer: A

Explanation:

QUESTION NO: 276

Which three statements about the TACACS protocol are correct? (Choose three.)

- A. TACACS+ is an IETF standard protocol.
- B. TACACS+ uses TCP port 47 by default.
- C. TACACS+ is considered to be more secure than the RADIUS protocol.
- D. TACACS+ can support authorization and accounting while having another separate authentication solution.

- E. TACACS+ only encrypts the password of the user for security.
- F. TACACS+ supports per-user or per-group for authorization of router commands.

Answer: C,D,F

Explanation:

QUESTION NO: 277

Which three EAP methods require a server-side certificate? (Choose three.)

- A. PEAP with MS-CHAPv2
- B. EAP-TLS
- C. EAP-FAST
- D. EAP-TTLS
- E. EAP-GTP

Answer: A,B,D

Explanation:

QUESTION NO: 278

Which statement is true about EAP-FAST?

- A. It supports Windows single sign-on.
- B. It is a proprietary protocol.
- C. It requires a certificate only on the server side.
- D. It does not support an LDAP database.

Answer: A

Explanation:

QUESTION NO: 279

Which four attributes are identified in an X.509v3 basic certificate field? (Choose four.)

- A. key usage
- B. certificate serial number
- C. issuer

- D. subject name
- E. signature algorithm identifier
- F. CRL distribution points
- G. subject alt name

Answer: B,C,D,E

Explanation:

QUESTION NO: 280

What is the purpose of the OCSP protocol?

- A. checks the revocation status of a digital certificate
- B. submits a certificate signing request
- C. verifies a signature of a digital certificate
- D. protects a digital certificate with its private key

Answer: A

Explanation:

QUESTION NO: 281

What are two reasons for a certificate to appear in a CRL? (Choose two.)

- A. CA key compromise
- B. cessation of operation
- C. validity expiration
- D. key length incompatibility
- E. certification path invalidity

Answer: A,B

Explanation:

QUESTION NO: 282

Which transport method is used by the IEEE 802.1X protocol?

- A. EAPOL frames

- B. 802.3 frames
- C. UDP RADIUS datagrams
- D. PPPoE frames

Answer: A

Explanation:

QUESTION NO: 283

Which encryption mechanism is used in WEP?

- A. RC4
- B. RC5
- C. DES
- D. AES

Answer: A

Explanation:

QUESTION NO: 284

Which three statements about Security Group Tag Exchange Protocol are true? (Choose three.)

- A. SXP runs on UDP port 64999.
- B. A connection is established between a "listener" and a "speaker."
- C. It propagates the IP-to-SGT binding table across network devices that do not have the ability to perform SGT tagging at Layer 2 to devices that support it.
- D. SXP is supported across multiple hops.
- E. SXPv2 introduces connection security via TLS.

Answer: B,C,D

Explanation:

QUESTION NO: 285

What does the SXP protocol exchange between peers?

- A. IP to SGT binding information

- B. MAC to SGT binding information
- C. ingress port to SGT binding information
- D. ingress switch to SGT binding information

Answer: A

Explanation:

QUESTION NO: 286

What is a primary function of the SXP protocol?

- A. to extend a TrustSec domain on switches that do not support packet tagging with SGTs
- B. to map the SGT tag to VLAN information
- C. to allow the SGT tagged packets to be transmitted on trunks
- D. to exchange the SGT information between different TrustSec domains

Answer: A

Explanation:

QUESTION NO: 287

In RFC 4034, DNSSEC introduced which four new resource record types? (Choose four.)

- A. DNS Public Key (DNSKEY)
- B. Next Secure (NSEC)
- C. Resource Record Signature (RRSIG)
- D. Delegation Signer (DS)
- E. Top Level Domain (TLD)
- F. Zone Signing Key (ZSK)

Answer: A,B,C,D

Explanation:

QUESTION NO: 288

What functionality is provided by DNSSEC?

- A. origin authentication of DNS data

- B. data confidentiality of DNS queries and answers
- C. access restriction of DNS zone transfers
- D. storage of the certificate records in a DNS zone file

Answer: A

Explanation:

QUESTION NO: 289

How are the username and password transmitted if a basic HTTP authentication is used?

- A. Base64 encoded username and password
- B. MD5 hash of the combined username and password
- C. username in cleartext and MD5 hash of the password
- D. cleartext username and password

Answer: A

Explanation:

QUESTION NO: 290

Which field in an HTTPS server certificate is compared to a server name in the URL?

- A. Common Name
- B. Issuer Name
- C. Organization
- D. Organizational Unit

Answer: A

Explanation:

QUESTION NO: 291

Which transport type is used by the DHCP protocol?

- A. UDP ports 67 and 69
- B. TCP ports 67 and 68
- C. UDP and TCP port 67

D. UDP ports 67 and 68

Answer: A

Explanation:

QUESTION NO: 292

Which domain is used for a reverse lookup of IPv4 addresses?

- A. in-addr.arpa
- B. ip4.arpa
- C. in-addr.net
- D. ip4.net

Answer: A

Explanation:

QUESTION NO: 293

Which port or ports are used for the FTP data channel in passive mode?

- A. random TCP ports
- B. TCP port 21 on the server side
- C. TCP port 21 on the client side
- D. TCP port 20 on the server side
- E. TCP port 20 on the client side

Answer: A

Explanation:

QUESTION NO: 294

Why do firewalls need to specially treat an active mode FTP session?

- A. The data channel is originating from a server side.
- B. The FTP client opens too many concurrent data connections.
- C. The FTP server sends chunks of data that are too big.
- D. The data channel is using a 7-bit transfer mode.

Answer: A

Explanation:

QUESTION NO: 295

Which statement is true about the TFTP protocol?

- A.** The client is unable to get a directory listing from the server.
- B.** The client is unable to create a new file on a server.
- C.** The client needs to log in with a username and password.
- D.** The client needs to log in using "anonymous" as a username and specifying an email address as a password.

Answer: A

Explanation:

QUESTION NO: 296

Which NTP stratum level means that the clock is unsynchronized?

- A.** 0
- B.** 1
- C.** 8
- D.** 16

Answer: D

Explanation:

QUESTION NO: 297

Which statement is true about an NTP server?

- A.** It answers using UTC time.
- B.** It uses the local time of the server with its time zone indication.
- C.** It uses the local time of the server and does not indicate its time zone.
- D.** It answers using the time zone of the client.

Answer: A

Explanation:

QUESTION NO: 298

Which statement is true about an SNMPv2 communication?

- A. The whole communication is not encrypted.
- B. Only the community field is encrypted.
- C. Only the query packets are encrypted.
- D. The whole communication is encrypted.

Answer: A

Explanation:

QUESTION NO: 299

Refer to the exhibit.

```
dns domain-lookup outside
dns server-group DefaultDNS
name-server 10.1.1.1
domain-name mydomain.cisco.com

dynamic-filter updater-client enable
dynamic-filter use-database

dynamic-filter enable interface outside

policy-map global_policy
class inspection_default
inspect dns dynamic-filter-snoop
```

What is this configuration designed to prevent?

- A. Man in the Middle Attacks

- B. DNS Inspection
- C. Backdoor control channels for infected hosts
- D. Dynamic payload inspection

Answer: C

Explanation:

QUESTION NO: 300

Refer to the exhibit.

```
regex TESTFILE ".*.bat"

class-map type regex match-any TESTFILECLASSMAP
  match regex TESTFILE

class-map type inspect ftp match-all TESTFILECLASSMAPFILTER
  match filename regex class TESTFILECLASSMAP

policy-map type inspect ftp FTPPOLICYMAP
  parameters
    class TESTFILECLASSMAPFILTER
  reset log

policy-map global_policy
  class inspection_default
    inspect ftp strict FTPPOLICYMAP
```

What does this configuration prevent?

- A. HTTP downloads of files with the ".bat" extension on all interfaces
- B. HTTP downloads of files with the ".batch" extension on the inside interface
- C. FTP commands of GET or PUT for files with the ".bat" extension on all interfaces
- D. FTP commands of GET or PUT for files with the ".batch" extension on the inside interface

Answer: C

Explanation:

Topic 4, Volume D

QUESTION NO: 301

Which four functionalities are built into the ISE? (Choose four.)

- A. Profiling Server
- B. Profiling Collector
- C. RADIUS AAA for Device Administration
- D. RADIUS AAA for Network Access
- E. TACACS+ for Device Administration
- F. TACACS+ for Network Access
- G. Guest Lifecycle Management

Answer: A,B,D,G

Explanation:

QUESTION NO: 302

Which statement is correct about the Cisco IOS Control Plane Protection feature?

- A. Control Plane Protection is restricted to the IPv4 or IPv6 input path.
- B. Traffic that is destined to the router with IP options will be redirected to the host control plane.
- C. Disabling CEF will remove all active control-plane protection policies. Aggregate control-plane policies will continue to operate.?
- D. The open-port option of a port-filtering policy allows access to all TCP/UDP based services that are configured on the router.

Answer: C

Explanation:

QUESTION NO: 303

Which Category to Protocol mapping for NBAR is correct?

- A. Category: Enterprise Applications
Protocol: Citrix ICA, PCAnywhere, SAP, IMAP
- B. Category: Internet
Protocol: FTP, HTTP, TFTP
- C. Category: Network Management
Protocol: ICMP, SNMP, SSH, Telnet
- D. Category: Network Mail Services
Protocol: MAPI, POP3, SMTP

Answer: B

Explanation:

Answer:

QUESTION NO: 304

Which two options correctly describe Remote Triggered Black Hole Filtering (RFC 5635)? (Choose two.)

- A.** RTBH destination based filtering can drop traffic destined to a host based on triggered entries in the FIB.
- B.** RTBH source based filtering will drop traffic from a source destined to a host based on triggered entries in the RIB
- C.** Loose uRPF must be used in conjunction with RTBH destination based filtering
- D.** Strict uRPF must be used in conjunction with RTBH source based filtering
- E.** RTBH uses a discard route on the edge devices of the network and a route server to send triggered route updates
- F.** When setting the BGP community attribute in a route-map for RTBH use the no-export community unless BGP confederations are used then use local-as to advertise to sub-as confederations

Answer: A,E

Explanation:

QUESTION NO: 305

A Cisco IOS router is configured as follows:

```
ip dns spoofing 192.168.20.1
```

What will the router respond with when it receives a DNS query for its own host name?

- A.** The router will respond with the IP address of the incoming interface.
- B.** The router will respond with 192.168.20.1 only if the outside interface is down.
- C.** The router will respond with 192.168.20.1.
- D.** The router will ignore the DNS query and forward it directly to the DNS server.

Answer: A

Explanation:

QUESTION NO: 306

Which configuration is the correct way to change a GET VPN Key Encryption Key lifetime to 10800 seconds on the key server?

- A.** crypto isakmp policy 1
lifetime 10800
- B.** crypto ipsec security-association lifetime? seconds 10800
- C.** crypto ipsec profile getvpn-profile
set security-association lifetime seconds 10800
!
crypto gdoi group GET-Group
identity number 1234
server local
sa ipsec 1
profile getvpn-profile
- D.** ?crypto gdoi group GET-Group
identity number 1234
server local
rekey lifetime seconds 10800
- E.** crypto gdoi group GET-Group
identity number 1234
server local
set security-association lifetime seconds 10800

Answer: D

Explanation:

QUESTION NO: 307

A Cisco Easy VPN software client is unable to access its local LAN devices once the VPN tunnel is established. How can this issue be resolved?

- A.** The IP address that is assigned by the Cisco Easy VPN Server to the client must be on the same network as the local LAN of the client.
- B.** The Cisco Easy VPN Server should apply split-tunnel-policy excludespecified with a split-tunnel-list containing the local LAN addresses that are relevant to the client.
- C.** The Cisco Easy VPN Server must push down an interface ACL that permits the traffic to the local LAN from the client.

- D. The Cisco Easy VPN Server should apply a split-tunnel-policy tunnelall policy to the client.
- E. The Cisco Easy VPN client machine needs to have multiple NICs to support this.

Answer: B

Explanation:

QUESTION NO: 308

Which three routing characteristics are relevant for DMVPN Phase 3? (Choose three.)

- A. Hubs must not preserve the original IP next-hop.
- B. Hubs must preserve the original IP next-hop.
- C. Split-horizon must be turned off for RIP and EIGRP.
- D. Spokes are only routing neighbors with hubs.
- E. Spokes are routing neighbors with hubs and other spokes.
- F. Hubs are routing neighbors with other hubs and must use the same routing protocol as that used on hub-spoke tunnels.

Answer: A,C,D

Explanation:

QUESTION NO: 309

Using Cisco IOS, which two object-group options will permit networks 10.1.1.0/24 and 10.1.2.0/24 to host 192.168.5.1 port 80 and 443? (Choose 2.)

A. object-group network SOURCE

range 10.1.1.0 10.1.2.255

object-group network DESTINATION

host 192.168.5.1

object-group service HTTP

tcp eq www

tcp eq 443

tcp source gt 1024

!

access-list 101 permit object-group HTTP object-group SOURCE object-group DESTINATION

B. object-group network SOURCE

10.1.1.0 0.0.0.255

10.1.2.0 0.0.0.255

object-group network DESTINATION

host 192.168.5.1

```
object-group service HTTP
tcp eq www
tcp eq 443
!
ip access-list extended ACL-NEW
permit object-group SOURCE object-group DESTINATION object-group HTTP
C. object-group network SOURCE
10.1.1.0 255.255.255.0
10.1.2.0 255.255.255.0
object-group network DESTINATION
host 192.168.5.1
object-group service HTTP
tcp eq www
tcp eq 443
!
ip access-list extended ACL-NEW
permit object-group SOURCE object-group DESTINATION object-group HTTP
D. object-group network SOURCE
10.1.1.0 255.255.255.0
10.1.2.0 255.255.255.0
object-group network DESTINATION
host 192.168.5.1
object-group service HTTP
tcp eq www
tcp eq 443
tcp source gt 1024
!
ip access-list extended ACL-NEW
permit object-group HTTP object-group SOURCE object-group DESTINATION
```

Answer: A,D

Explanation:

QUESTION NO: 310

Which two statements about the fragmentation of IPsec packets in routers are true? (Choose two.)

- A.** By default, the IP packets that need encryption are first encrypted with ESP. If the resulting encrypted packet exceeds the IP MTU on the egress physical interface, then the encrypted packet is fragmented and sent out.
- B.** By default, the router knows the IPsec overhead to add to the packet. The router performs a lookup if the packet will exceed the egress physical interface IP MTU after encryption, then fragments the packet and encrypts the resulting IP fragments separately.

- C. increases CPU utilization on the decrypting device.
- D. increases CPU utilization on the encrypting device.

Answer: B,C

Explanation:

QUESTION NO: 311

```
crypto gdoi group gdoi_group  
identity number 1234  
server local  
sa receive-only  
sa ipsec 1  
profile gdoi-p  
match address ipv4 120
```

Which statement about the above configuration is true?

- A. The key server instructs the DMVPN spoke to install SAs outbound only.
- B. The key server instructs the GDOI group to install SAs inbound only.
- C. The key server instructs the DMVPN hub to install SAs outbound only.
- D. The key server instructs the GDOI spoke to install SAs inbound only.

Answer: B

Explanation:

QUESTION NO: 312

```
class-map nbar_rtp  
match protocol rtp payload-type "0, 1, 4 - 0x10, 10001b - 10010b, 64"
```

The above NBAR configuration matches RTP traffic with which payload types?

- A. 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 64
- B. 0, 1, 4, 5, 6, 7, 8, 9, 10
- C. 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 64
- D. 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 64

Answer: A

Explanation:

QUESTION NO: 313

Which standard prescribes a risk assessment to identify whether each control is required to decrease risks and if so, to which extent it should be applied?

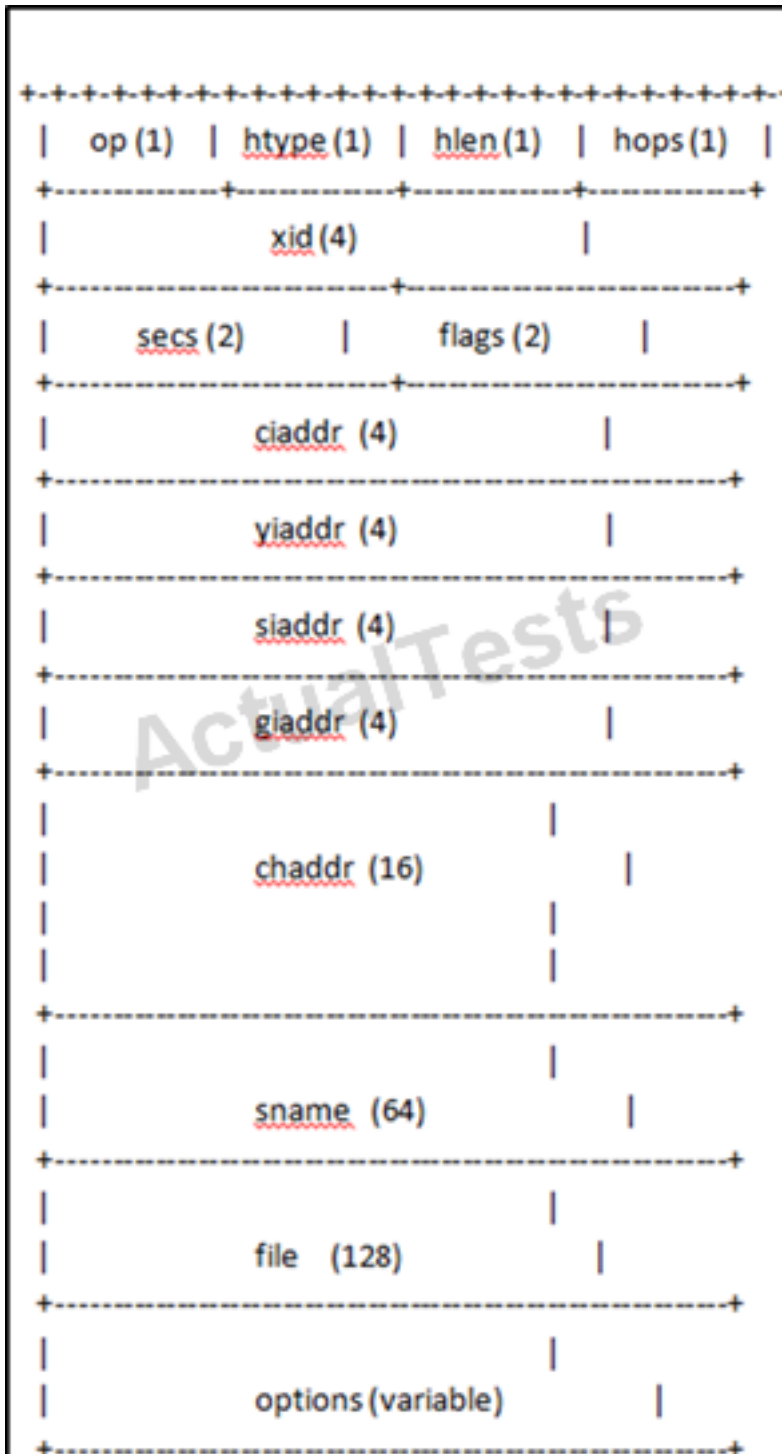
- A. ISO 27001
- B. ISO 27002
- C. ISO 17799
- D. HIPPA
- E. ISO 9000

Answer: A

Explanation:

QUESTION NO: 314

Refer to the exhibit.



According to this DHCP packet header, which field is populated by a DHCP relay agent with its own IP address before the DHCPDISCOVER message is forwarded to the DHCP server?

- A. ciaddr
- B. yiaddr
- C. siaddr
- D. giaddr

Answer: D

Explanation:

QUESTION NO: 315

Which two are valid SMTP commands, according to RFC 821? (Choose two.)

- A. EHLO
- B. HELO
- C. RCPT
- D. AUTH

Answer: B,C

Explanation:

QUESTION NO: 316

EAP-MD5 provides one-way client authentication. The server sends the client a random challenge. The client proves its identity by hashing the challenge and its password with MD5. What is the problem with EAP-MD5?

- A. EAP-MD5 is vulnerable to dictionary attack over an open medium and to spoofing because there is no server authentication.
- B. EAP-MD5 communication must happen over an encrypted medium, which makes it operationally expensive.
- C. EAP-MD5 is CPU-intensive on the devices.
- D. EAP-MD5 not used by RADIUS protocol.

Answer: A

Explanation:

QUESTION NO: 317

error: % Invalid input detected at '^' marker.

Above error is received when generating RSA keys for SSH access on a router using the crypto key generate rsa command. What are the reasons for this error? (Choose two.)

- A. The hostname must be configured before generating RSA keys.

- B.** The image that is used on the router does not support the crypto key generate rsa command.
- C.** The command has been used with incorrect syntax.
- D.** The crypto key generate rsa command is used to configure SSHv2, which is not supported on Cisco IOS devices.

Answer: B,C

Explanation:

QUESTION NO: 318

```
crypto isakmp profile vpn1  
  
vrf vpn1  
  
keyring vpn1  
  
match identity address 172.16.1.1 255.255.255.255  
  
crypto map crypmap 1 ipsec-isakmp  
  
set peer 172.16.1.1  
  
set transform-set vpn1  
  
set isakmp-profile vpn1  
  
match address 101  
  
!  
  
interface Ethernet1/2  
  
crypto map crypmap
```

Which statements apply to the above configuration? (Choose two.)

- A.** This configuration shows the VRF-Aware IPsec feature that is used to map the crypto ISAKMP profile to a specific VRF.
- B.** VRF and ISAKMP profiles are mutually exclusive, so the configuration is invalid.
- C.** An IPsec tunnel can be mapped to a VRF instance.
- D.** Peer command under the crypto map is redundant and not required.

Answer: A,C

Explanation:

QUESTION NO: 319

MACsec, which is defined in 802.1AE, provides MAC-layer encryption over wired networks. Which two statements about MACsec are true? (Choose two.)

- A.** Only links between network access devices and endpoint devices can be secured by using MACsec.
- B.** MACsec is designed to support communications between network devices only.
- C.** MACsec manages the encryption keys that the MKA protocol uses.
- D.** A switch that uses MACsec accepts either MACsec or non-MACsec frames, depending on the policy that is associated with the client.

Answer: A,D

Explanation:

QUESTION NO: 320

With ASM, sources can launch attacks by sending traffic to any groups that are supported by an active RP. Such traffic might not reach a receiver but will reach at least the first-hop router in the path, as well as the RP, allowing limited attacks. However, if the attacking source knows a group to which a target receiver is listening and there are no appropriate filters in place, then the attacking source can send traffic to that group. This traffic is received as long as the attacking source is listening to the group.

Based on the above description, which type of security threat is involved?

- A.** DoS
- B.** man-in-the-middle
- C.** compromised key
- D.** data modification

Answer: A

Explanation:

QUESTION NO: 321

Which two statements about VTP passwords are true? (Choose two)

- A. The VTP password can only be configured when the switch is in Server mode.
- B. The VTP password is sent in the summary advertisements..
- C. The VTP password is encrypted for confidentiality using 3DES.
- D. VTP is not required to be configured on all switches in the domain.
- E. The VTP password is hashed to preserve authenticity using the MD5 algorithm.
- F. The VTP password can only be configured when the switch is in Client mode.

Answer: B,E

Explanation:

QUESTION NO: 322

Which option represents IPv6 address ff02::1?

- A. PIM routers.
- B. RIP routers.
- C. all nodes on the local network.
- D. NTP.

Answer: C

Explanation:

QUESTION NO: 323

Which two statements about IPv6 are true? (Choose two.)

- A. Broadcast is available.
- B. Routing tables are less complicated.
- C. The address pool will eventually deplete.
- D. Data encryption is built into the packet frame.
- E. Increased NAT is required.
- F. Fewer bits makes IPv6 easier to configure.

Answer: B,D

Explanation:

QUESTION NO: 324

Which statement describes an IPv6 benefit?

- A. Broadcast is not available.
- B. Routing tables are more complicated.
- C. The address pool is limited.
- D. Data encryption is not built into the packet frame.
- E. Increased NAT is required.

Answer: A

Explanation:

QUESTION NO: 325

Which option is representative of automatic IP addressing in IPv4?

- A. 10.1.x.x
- B. 172.10.1.x
- C. 169.254.x.x
- D. 196.245.x.x
- E. 128.1.1.x
- F. 127.1.x.x

Answer: C

Explanation:

QUESTION NO: 326

Refer to the exhibit.

```
object network obj-10.10.0.0
subnet 10.10.0.0 255.255.0.0
object network obj-30.30.30.0
subnet 30.30.30.0 255.255.255.0
nat (inside,any) source static obj-10.10.0.0 obj-10.10.0.0 destination
static obj-30.30.30.0 obj-30.30.30.0
```

Which option describes the behavior of this configuration?

- A. Traffic from the 30.30.0.0/16 network to the 10.10.0.0/32 network will be translated.
- B. Traffic from the 30.30.0.0/32 network to the 10.10.0.0/16 network will not be translated.
- C. Traffic from the 10.10.0.0/16 network to the 30.30.30.0/24 network will not be translated.
- D. Traffic from the 10.10.0.0/32 network to the 30.30.30.0/16 network will be translated.

Answer: C

Explanation:

QUESTION NO: 327

Refer to the exhibit.

```
object network obj-10.10.10.1
host 10.10.10.1
nat (inside,outside) dynamic 20.20.20.1
```

Which option describes the behavior of this configuration?

- A. Host 10.10.10.1 will get translated as 20.20.20.1 from inside to outside.
- B. Host 20.20.20.1 will be translated as 10.10.10.1 from outside to inside.
- C. Host 20.20.20.1 will be translated as 10.10.10.1 from inside to outside.
- D. Host 10.10.10.1 will be translated as 20.20.20.1 from outside to inside.

Answer: A

Explanation:

QUESTION NO: 328

Which ICMP message type code indicates fragment reassembly time exceeded?

- A. Type 4, Code 0
- B. Type 11, Code 0
- C. Type 11, Code 1
- D. Type 12, Code 2

Answer: C

Explanation:

QUESTION NO: 329

Which IPv4 header field increments every time when packet is sent from a source to a destination?

- A. Flag
- B. Fragment Offset
- C. Identification
- D. Time To Live

Answer: C

Explanation:

QUESTION NO: 330

A device is sending a PDU of 5000 B on a link with an MTU of 1500 B. If the PDU includes 20 B of IP header, which statement is true?

- A. The first three packets will have a packet payload size of 1400.
- B. The last packet will have a payload size of 560.
- C. The first three packets will have a packet payload size of 1480.
- D. The last packet will have a payload size of 20.

Answer: C

Explanation:

QUESTION NO: 331

Which statement about VLAN is true?

- A. VLAN cannot be routed.
- B. VLANs 1006 through 4094 are not propagated by VTP.
- C. VLAN1 is a Cisco default VLAN that can be deleted.
- D. The extended-range VLANs cannot be configured in global configuration mode.

Answer: B

Explanation:

QUESTION NO: 332

Which two statements about OSPF authentication are true? (Choose two.)

- A. OSPF authentication is required in area 0.
- B. There are three types of OSPF authentication.
- C. In MD5 authentication, the password is encrypted when it is sent.
- D. Null authentication includes the password in clear-text.
- E. Type-3 authentication is a clear-text password authentication.
- F. In MD5 authentication, the password never goes across the network.

Answer: B,F

Explanation:

QUESTION NO: 333

Which option describes the main purpose of EIGRP authentication?

- A. to authenticate peers
- B. to allow faster convergence
- C. to provide redundancy
- D. to avoid routing table corruption

Answer: D

Explanation:

QUESTION NO: 334

What is the purpose of the BGP TTL security check?

- A. The BGP TTL security check is used for iBGP session.
- B. The BGP TTL security check protects against CPU utilization-based attacks.
- C. The BGP TTL security check checks for a TTL value in packet header of less than or equal to for successful peering.
- D. The BGP TTL security check authenticates a peer.
- E. The BGP TTL security check protects against routing table corruption.

Answer: B

Explanation:

QUESTION NO: 335

Refer to the exhibit.

```
neighbor 100.10.10.10 maximum-prefix 1000 80 warning-only
```

Which option describes the behavior of this configuration?

- A. The peer session is dropped when 80 prefixes are received.
- B. A warning message is displayed when 1000 prefixes are received.
- C. The peer session is dropped when 800 prefixes are received.
- D. An Initial warning message is displayed when 800 prefixes are received. A different message is displayed when 1000 prefixes received and the session will not be disconnected
- E. An Initial warning message is displayed when 80 prefixes received. The same warning message is displayed when 1000 prefixes are received and the session will be disconnected.

Answer: D

Explanation:

QUESTION NO: 336

Which two statements describe GRE? (Choose two.)

- A. GRE acts as passenger protocol for a Layer 3 transport protocol.
- B. GRE acts as a tunneling protocol and encapsulates other protocols.
- C. GRE provides data confidentiality.
- D. Packet MTU must be adjusted to accommodate GRE overhead.
- E. GRE does not allow multicast to be sent across the tunnel.
- F. The GRE tunnel interface remains down until it can see the remote tunnel end.

Answer: B,D

Explanation:

QUESTION NO: 337

Which two statements about NHRP are true? (Choose two.)

- A. NHRP is used for broadcast multi-access networks.
- B. NHRP allows NHC to dynamically learn the mapping of VPN IP to NBMA IP.
- C. NHRP allows NHS to dynamically learn the mapping of VPN IP to BMA IP.
- D. NHC registers with NHS.
- E. Traffic between two NHCs always flows through the NHS.
- F. NHRP provides Layer-2 to Layer-3 address mapping.

Answer: B,D

Explanation:

QUESTION NO: 338

Refer to the exhibit.

```
NHRP: Receive Registration Request via Tunnel0 vrf 0, packet : 92
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: 92 extoff: 52
(M) flags: "unique nat ", reqid: 65584
src NBMA: 69.1.1.2
src protocol: 192.168.10.2, dst protocol: 192.168.10.1
(C-1) code: no error(0)
prefix: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
%DUAL-5-NBRCHANGE: EIGRP-IPv4 101: Neighbor 192.168.10.2 (Tunnel0) is up: new adjacency
```

Which two statements correctly describe the debug output that is shown in the exhibit? (Choose two.)

- A. The request is from NHS to NNC.
- B. The request is from NHC to NHS.
- C. 69.1.1.2 is the local non-routable address.
- D. 192.168.10.2 is the remote NBMA address.
- E. 192.168.10.1 is the local VPN address.
- F. This debug output represents a failed NHRP request.

Answer: B,E

Explanation:

QUESTION NO: 339

Which two statements about the AES algorithm are true? (Choose two)

- A. The AES algorithm is an asymmetric block cipher.
- B. The AES algorithm operates on a 128-bits block.
- C. The AES algorithm uses a fixed length-key of 128 bits.
- D. The AES algorithm does not give any advantage over 3DES due to the same key length.
- E. The AES algorithm consist of four functions. Three functions provide confusion-diffusion and one provides encryption.

Answer: B,E

Explanation:

QUESTION NO: 340

Which two statements about the RC4 algorithm are true? (Choose two.)

- A. The RC4 algorithm is an asymmetric key algorithm.
- B. The RC4 algorithm is a symmetric key algorithm.
- C. The RC4 algorithm is slower in computation than DES.
- D. The RC4 algorithm is used with wireless encryption protocols.
- E. The RC4 algorithm uses fixed-length keys.

Answer: B,D

Explanation:

QUESTION NO: 341

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

- A. The RSA algorithm provides encryption but not authentication.
- B. The RSA algorithm provides authentication but not encryption.
- C. The RSA algorithm creates a pair of public-private keys that are shared by entities that perform encryption.
- D. The private key is never sent across after it is generated.
- E. The public key is used to decrypt the message that was encrypted by the private key.
- F. The private key is used to decrypt the message that was encrypted by the public key.

Answer: C,D,F

Explanation:

QUESTION NO: 342

Which two statements about the MD5 Hash are true? (Choose two.)

- A. Length of the hash value varies with the length of the message that is being hashed.
- B. Every unique message has a unique hash value.
- C. Its mathematically possible to find a pair of message that yield the same hash value.
- D. MD5 always yields a different value for the same message if repeatedly hashed.
- E. The hash value cannot be used to discover the message.

Answer: B,E

Explanation:

QUESTION NO: 343

Which two statements about the SHA-1 algorithm are true? (Choose two)

- A. The SHA-1 algorithm is considered secure because it always produces a unique hash for the same message.
- B. The SHA-1 algorithm takes input message of any length and produces 160-bit hash output.
- C. The SHA-1 algorithm is considered secure because it is possible to find a message from its hash.
- D. The purpose of the SHA-1 algorithm is to provide data confidentiality.
- E. The purpose of the SHA-1 algorithm is to provide data authenticity.

Answer: B,E

Explanation:

QUESTION NO: 344

Which two statements about the DES algorithm are true? (Chosse two)

- A. The DES algorithm is based on asymmetric cryptography.
- B. The DES algorithm is a stream cipher.
- C. The DES algorithm is based on symmetric cryptography.
- D. The DES algorithm encrypts a block of 128 bits.
- E. The DES algorithm uses a 56-bit key.

Answer: C,E

Explanation:

QUESTION NO: 345

Which statement about the 3DES algorithm is true?

- A. The 3DES algorithm uses the same key for encryption and decryption,
- B. The 3DES algorithm uses a public-private key pair with a public key for encryption and a private key for decryption.
- C. The 3DES algorithm is a block cipher.
- D. The 3DES algorithm uses a key length of 112 bits.
- E. The 3DES algorithm is faster than DES due to the shorter key length.

Answer: C

Explanation:

QUESTION NO: 346

Which two statements about the DH group are true? (Choose two.)

- A. The DH group is used to provide data authentication.
- B. The DH group is negotiated in IPsec phase-1.
- C. The DH group is used to provide data confidentiality.
- D. The DH group is used to establish a shared key over an unsecured medium.
- E. The DH group is negotiated in IPsec phase-2.

Answer: B,D

Explanation:

QUESTION NO: 347

Which statement describes the computed authentication data in the AH protocol?

- A. The computed authentication data is never sent across.
- B. The computed authentication data is part of a new IP header.
- C. The computed authentication data is part of the AH header.
- D. The computed authentication data is part of the original IP header.

Answer: C

Explanation:

QUESTION NO: 348

Which statement about the AH is true?

- A. AH authenticates only the data.
- B. AH authenticates only the IP header.
- C. AH authenticates only the TCP-UDP header.
- D. AH authenticates the entire packet and any mutable fields.
- E. AH authenticates the entire packet except for any mutable fields.

Answer: E

Explanation:

QUESTION NO: 349

Which three fields are part of the AH header? (Choose three.)

- A. Source Address
- B. Destination Address
- C. Packet ICV
- D. Protocol ID
- E. Application Port
- F. SPI identifying SA
- G. Payload Data Type Identifier

Answer: C,F,G

Explanation:

QUESTION NO: 350

Which statement about the HTTP protocol is true?

- A. The request method does not include the protocol version.
- B. The proxy acts as an intermediary receiving agent in the request-response chain.
- C. The tunnel acts as an intermediary relay agent in the request-response chain.

- D. The gateway acts as an intermediary forwarding agent in the request-response chain.
- E. The success and error codes are returned in the response message by the user-agent.

Answer: C

Explanation:

QUESTION NO: 351

Which statement about SMTP is true?

- A. SMTP uses UDP port 25.
- B. The POP protocol is used by the SMTP client to manage stored mail.
- C. The IMAP protocol is used by the SMTP client to retrieve and manage stored email.
- D. The mail delivery agent in the SMTP architecture is responsible for DNS lookup.
- E. SMTP uses TCP port 20.

Answer: C

Explanation:

QUESTION NO: 352

Which two statements about DHCP are true? (Choose two.)

- A. DHCP uses TCP port 67.
- B. DHCP uses UDP ports 67 and 68.
- C. The DHCPDiscover packet has a multicast address of 239.1.1.1.
- D. DHCPRequest is a broadcast message.
- E. The DHCPOffer packet is sent from the DHCP server.

Answer: B,E

Explanation:

QUESTION NO: 353

Which two statements about SNMP are true? (Choose two)

- A. SNMP operates at Layer-6 of the OSI model.
- B. NMS sends a request to the agent at TCP port 161.

- C. NMS sends request to the agent from any source port.
- D. NMS receives notifications from the agent on UDP 162.
- E. MIB is a hierarchical representation of management data on NMS.

Answer: C,D

Explanation:

QUESTION NO: 354

Which two statement about the DNS are true? (Choose two.)

- A. The client-server architecture is based on query and response messages.
- B. Query and response messages have different format.
- C. In the DNS message header, the QR flag set to 1 indicates a query.
- D. In the DNS header, an Opcode value of 2 represents a client status request.
- E. In the DNS header, the Rcode value is set to 0 in Query message.

Answer: A,E

Explanation:

QUESTION NO: 355

Which is an example of a network reconnaissance attack?

- A. botnets
- B. backdoor
- C. ICMP sweep
- D. firewalk
- E. inverse mapping

Answer: C

Explanation:

QUESTION NO: 356

Which ICMP message could be used with traceroute to map network topology?

- A. Echo Reply

- B. Redirect
- C. Time Exceeded
- D. Echo
- E. Router Selection
- F. Address Mask Request

Answer: C

Explanation:

QUESTION NO: 357

Which statement about the Firewalk attack is true?

- A. The firewall attack is used to discover hosts behind firewall device.
- B. The firewall attack uses ICMP sweep to find expected hosts behind the firewall.
- C. The firewall attack uses traceroute with a predetermined TTL value to discover hosts behind the firewall.
- D. The firewall attack is used to find the vulnerability in the Cisco IOS firewall code.
- E. The firewall attack uses an ICMP echo message to discover firewall misconfiguration.

Answer: C

Explanation:

QUESTION NO: 358

Which pair of ICMP messages is used in an inverse mapping attack?

- A. Echo-Echo Request
- B. Route Solicitation- Time Exceeded
- C. Echo-Time Exceeded
- D. Echo Reply-Host Unreachable
- E. Echo-Host Unreachable

Answer: D

Explanation:

QUESTION NO: 359

Which statement about a botnet attack is true?

- A. The botnet attack is an attack on a firewall to disable its filtering ability.
- B. The botnet attack is a network sweeping attack to find hosts that are alive behind the filtering device.
- C. The botnet attack is a collection of infected computers that launch automated attacks.
- D. The owner of the infected computer willingly participates in automated attacks.
- E. The botnet attack enhances the efficiency of the computer for effective automated attacks.

Answer: C

Explanation:

QUESTION NO: 360

Which two statements about IPS signatures are true? (Choose two.)

- A. All of the built-in signatures are enabled by default.
- B. Tuned signatures are built-in signatures whose parameters are adjusted.
- C. Once the signature is removed from the sensing engine it cannot be restored
- D. It is recommended not to retire a signature that is not being used because then it cannot be restored.
- E. It is possible to define custom signatures.

Answer: B,E

Explanation:

QUESTION NO: 361

Which two statements about Infrastructure ACLs on Cisco IOS software are true? (Choose two.)

- A. Infrastructure ACLs are used to block-permit the traffic in the router forwarding path.
- B. Infrastructure ACLs are used to block-permit the traffic handled by the route processor.
- C. Infrastructure ACLs are used to block-permit the transit traffic.
- D. Infrastructure ACLs only protect device physical management interface.

Answer: B,D

Explanation:

QUESTION NO: 362

Which statement about the SYN flood attack is true?

- A. The SYN flood attack is always directed from valid address.
- B. The SYN flood attack target is to deplete server memory so that legitimate request cannot be served.
- C. The SYN flood attack is meant to completely deplete the TCB SYN-Received state backlog.
- D. The SYN flood attack can be launched for both UDP and TCP open ports on the server.
- E. SYN-Received state backlog for TCBs is meant to protect server CPU cycles.

Answer: C

Explanation:

QUESTION NO: 363

The HTTP inspection engine has the ability to inspect traffic based on which three parameters? (Choose three.)

- A. Transfer Encoding
- B. Request Method
- C. Header
- D. Application Type
- E. Header Size
- F. Source Address

Answer: A,B,D

Explanation:

QUESTION NO: 364

For which two reasons BVI is required in the Transparent Cisco IOS Firewall? (Choose two)

- A. BVI is required for the inspection of IP traffic.
- B. The firewall can perform routing on bridged interfaces.
- C. BVI is required if routing is disabled on the firewall.
- D. BVI is required if more than two interfaces are in a bridge group.
- E. BVI is required for the inspection of non-IP traffic.
- F. BVI can manage the device without having an interface that is configured for routing.

Answer: D,F

Explanation:

QUESTION NO: 365

Event Store is a component of which IPS application?

- A. SensorApp
- B. InterfaceApp
- C. MainApp
- D. NotificationApp
- E. AuthenticationApp

Answer: C

Explanation:

QUESTION NO: 366

Which statement about the Cisco Secure ACS Solution Engine TACACS+ AV pair is true?

- A. AV pairs are only required to be enabled on Cisco Secure ACS for successful implementation.
- B. The Cisco Secure ACS Solution Engine does not support accounting AV pairs.
- C. AV pairs are only string values.
- D. AV pairs are of two types: string and integer.

Answer: C

Explanation:

QUESTION NO: 367

Refer to the exhibit.

```
(config-if)#authentication order mab dot1x
(config-if)#authentication priority mab dot1x
```

Which option describes the behavior of this configuration?

- A. Devices that perform IEEE 802.1X should be in the MAC address database for successful authentication.

- B. IEEE 802.1x devices must fail MAB to perform IEEE 802.1X authentication.
- C. If 802.1X fails, the device will be assigned to the default guest VLAN.
- D. The device will perform subsequent IEEE 802.1X authentication if it passed MAB authentication.
- E. If the device fails IEEE 802.1X, it will start MAB again.

Answer: B

Explanation:

QUESTION NO: 368

When is the supplicant considered to be clientless?

- A. when the authentication server does not have credentials to authenticate.
- B. when the authenticator is missing the dot1x guest VLAN under the port with which the supplicant is connected.
- C. when the supplicant fails EAP-MD5 challenge with the authentication server.
- D. when the supplicant fails to respond to EAPOL messages from the authenticator.
- E. when the authenticator is missing the reauthentication timeout configuration under the port with which the supplicant is connected.

Answer: D

Explanation:

QUESTION NO: 369

Which Cisco IOS IPS signature action denies an attacker session using the dynamic access list?

- A. produce-alert
- B. deny-attacker-inline
- C. deny-connection-inline
- D. reset-tcp-action
- E. deny-session-inline
- F. deny-packet-inline

Answer: C

Explanation:

QUESTION NO: 370

Which IPS appliance signature engine inspects IPv6 Layer 3 traffic?

- A. Atomic IP
- B. Meta
- C. Atomic IP Advanced
- D. Fixed
- E. Service

Answer: C

Explanation:

QUESTION NO: 371

When routing is configured on ASA, which statement is true?

- A. If the default route is not present, then the routing table is checked.
- B. If the routing table has two matching entries, the packet is dropped.
- C. If routing table has two matching entries with same prefix length, the first entry is used.
- D. If routing table has two matching entries with different prefix lengths, the entry with the longer prefix length is used.

Answer: D

Explanation:

QUESTION NO: 372

Which statement about the ASA redundant interface is true?

- A. It is a logical interface that combines two physical interfaces, both of which are active.
- B. It can only be used for failover links.
- C. By default, the first physical interface that is configured in the pair is the active interface.
- D. The redundant interface uses the MAC address of the second physical interface in the pair.

Answer: C

Explanation:

QUESTION NO: 373

Which two pieces of information are communicated by the ASA failover link? (Choose two.)

- A. unit state
- B. connections State
- C. routing tables
- D. power status
- E. MAC address exchange

Answer: A,E

Explanation:

QUESTION NO: 374

When is a connection entry created on ASA for a packet that is received on the ingress interface?

- A. When the packet is checked by the access-list.
- B. When the packet reaches the ingress interface internal buffer.
- C. When the packet is a SYN packet or UDP packet.
- D. When a translation rule exists for the packet.
- E. When the packet is subjected to inspection.

Answer: D

Explanation:

QUESTION NO: 375

Which two statements about the multiple context mode running Version 9.x are true? (Choose two.)

- A. RIP is not supported.
- B. An interface cannot be shared by multiple contexts.
- C. Remote access VPN is supported.
- D. Only the admin and context configuration files are supported.
- E. OSPFv3 is supported.
- F. Multicast feature is supported
- G. Site-To-Site VPN feature is supported

Answer: A,G

Explanation:

QUESTION NO: 376

Which two options describe how the traffic for the shared interface is classified in ASA multi context mode? (Choose two.)

- A. Traffic is classified at the source address in the packet.
- B. Traffic is classified at the destination address in the packet.
- C. Traffic is classified at the destination address in the context.
- D. Traffic is classified by copying and sending the packet to all the contexts.
- E. Traffic is classified by sending the MAC address for the shared interface.

Answer: C,E

Explanation:

QUESTION NO: 377

Which two statements correctly describes ASA resource management in multiple context mode? (Choose two.)

- A. The class sets the resource maximum limit for a context to which it belongs.
- B. A resource cannot be oversubscribed or set to be unlimited in the class.
- C. The resource limit can only be set as a percentage in the class and not as an absolute value.
- D. Context belongs to a default class if not assigned to any other class.
- E. The default class provides unlimited access for all the resources.

Answer: A,D

Explanation:

QUESTION NO: 378

Which two statements about ASA transparent mode are true? (Choose two.)

- A. Transparent mode acts as a Layer-3 firewall.
- B. The inside and outside interface must be in a different subnet.
- C. IP traffic will not pass unless it is permitted by an access-list.
- D. ARP traffic is dropped unless it is permitted.

- E. A configured route applies only to the traffic that is originated by the ASA.
- F. In multiple context mode, all contexts need to be in transparent mode.

Answer: C,E

Explanation:

QUESTION NO: 379

Which statement correctly describes a botnet filter category?

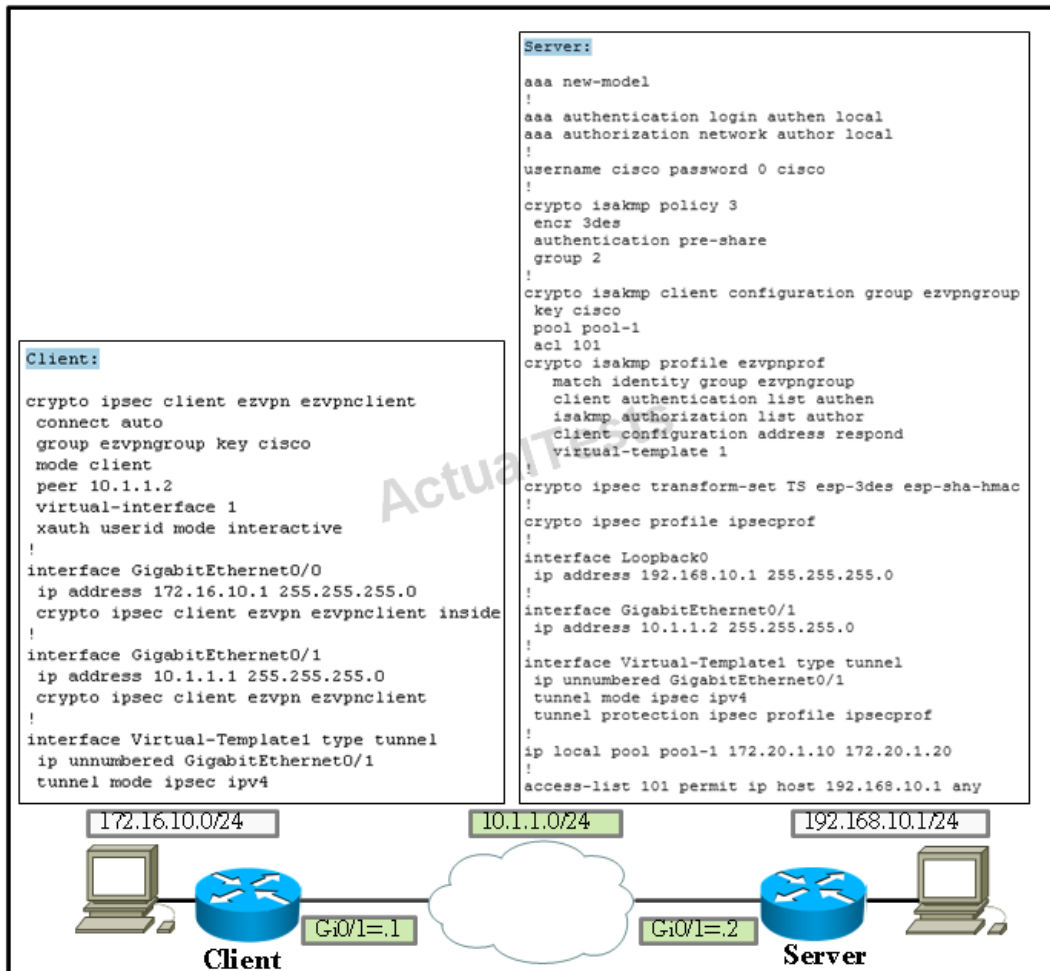
- A.** Unlisted addresses: The addresses are malware addresses that are not identified by the dynamic database and are hence defined statically.
- B.** Ambiguous addresses: In this case, the same domain name has multiple malware addresses but not all the addresses are in the dynamic database. These addresses are on the graylist.
- C.** Known malware addresses: These addresses are identified as blacklist addresses in the dynamic database and static list.
- D.** Known allowed addresses: These addresses are identified as whitelist addresses that are bad addresses but still allowed.

Answer: C

Explanation:

QUESTION NO: 380

Refer to the exhibit.



Why does the EasyVPN session fail to establish between the client and server?

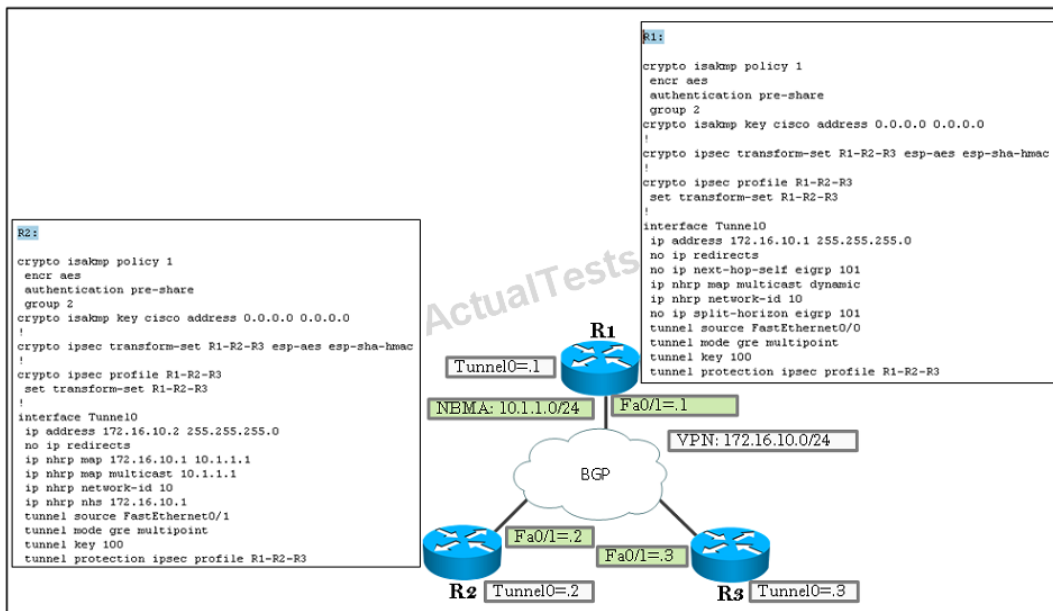
- A. incomplete ISAKMP profile configuration on the server
- B. incorrect IPsec phase-2 configuration on the server
- C. incorrect group configuration on the client
- D. ISAKMP key mismatch
- E. incorrect ACL in the ISAKMP client group configuration

Answer: B

Explanation:

QUESTION NO: 381

Refer to the exhibit.



What is the reason for the failure of the DMVPN session between R1 and R2?

- A. tunnel mode mismatch
- B. IPsec phase-1 configuration is missing peer address on R2
- C. IPsec phase-1 policy mismatch
- D. IPsec phase-2 policy mismatch
- E. incorrect tunnel source interface on R1

Answer: E

Explanation:

QUESTION NO: 382

Which three HTTP header fields can be classified by NBAR for request messages? (Choose three.)

- A. User-Agent
- B. Server
- C. Referrer
- D. Content-Encoding
- E. Location
- F. From

Answer: A,C,F

Explanation:

QUESTION NO: 383

Refer to the exhibit.

```
ip verify unicast source reachable-via rx
```

Which option describes the behavior of this configuration?

- A. The packet will be dropped if received on the same interface that the router would use to forward return packet.
- B. The packet will be forwarded as long as it is in the routing table.
- C. The packet will be forwarded if received on the same interface that the router would use to forward return packet.
- D. Packet will be forwarded only if exists a default route for the return path.

Answer: C

Explanation:

QUESTION NO: 384

Which three types of traffic are processed by CoPP configured on the device? (Choose three.)

- A. tansient traffic
- B. routing protocol traffic
- C. IPsec traffic
- D. traffic that is destined to the device interface
- E. any traffic filtered by the access list
- F. traffic from a management protocol such as Telnet or SNMP

Answer: B,D,F

Explanation:

QUESTION NO: 385

Which statement about PVLAN setup is true?

- A.** The host that is connected to the community port can communicate with a host that is connected to a different community port.
- B.** The host that is connected to the community port cannot communicate with hosts that are connected to the promiscuous port.
- C.** The host that is connected to the community port cannot communicate with hosts that are connected to the isolated port.
- D.** The host that is connected to the community port can only communicate with hosts that are connected to the same community port.

Answer: C

Explanation:

QUESTION NO: 386

Which statement applies to Flexible NetFlow?

- A.** Flexible NetFlow uses seven key fields in IP datagrams to identify the flow.
- B.** Flexible NetFlow uses key fields of IP datagram to identify fields from which data is captured.
- C.** User-defined flows can be defined in Flexible NetFlow.
- D.** Flexible NetFlow cannot be used for billing and accounting applications.
- E.** Flexible NetFlow does not have any predefined records.

Answer: C

Explanation:

QUESTION NO: 387

Which statement about Storm Control implementation on a switch is true?

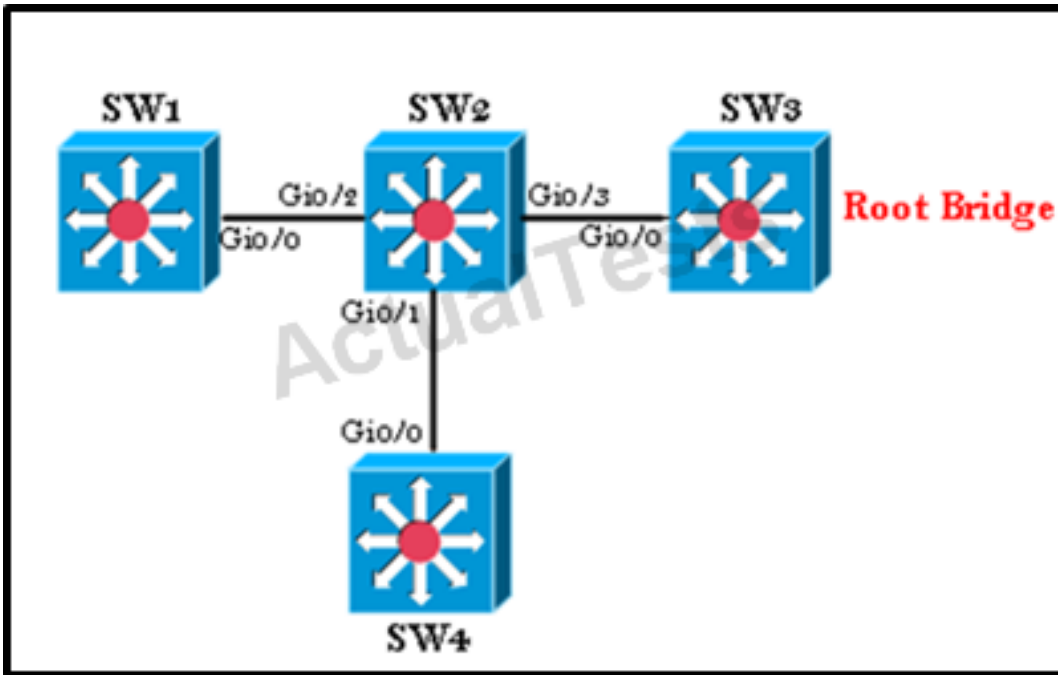
- A.** Storm Control does not prevent disruption due to unicast traffic.
- B.** Storm Control is implemented as a global configuration.
- C.** Storm Control uses the bandwidth and rate at which a packet is received to measure the activity.
- D.** Storm Control uses the bandwidth and rate at which a packet is dispatched to measure the activity.
- E.** Storm Control is enabled by default.

Answer: C

Explanation:

QUESTION NO: 388

Refer to the exhibit.



If SW4 is sending superior BPDUs, where should the root guard feature be configured to preserve SW3 as a root bridge?

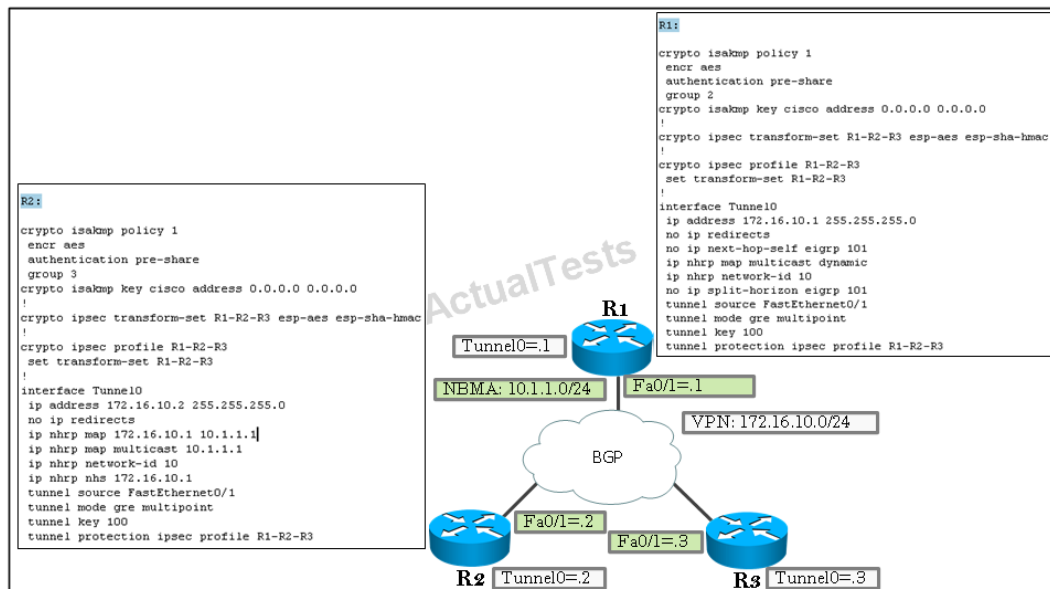
- A. SW4 Gi0/0 interface.
- B. Sw3 Gi0/0 interface.
- C. Sw2 Gi0/1 interface.
- D. SW2 Gi0/1 and SW3 Gi0/1

Answer: C

Explanation:

QUESTION NO: 389

Refer to the exhibit.



What is the reason for the failure of the DMVPN session between R1 and R2?

- A. tunnel mode mismatch
- B. IPsec phase-1 configuration missing peer address on R2
- C. IPsec phase-1 policy mismatch
- D. IPsec phase-2 policy mismatch
- E. incorrect tunnel source interface on R1

Answer: C

Explanation:

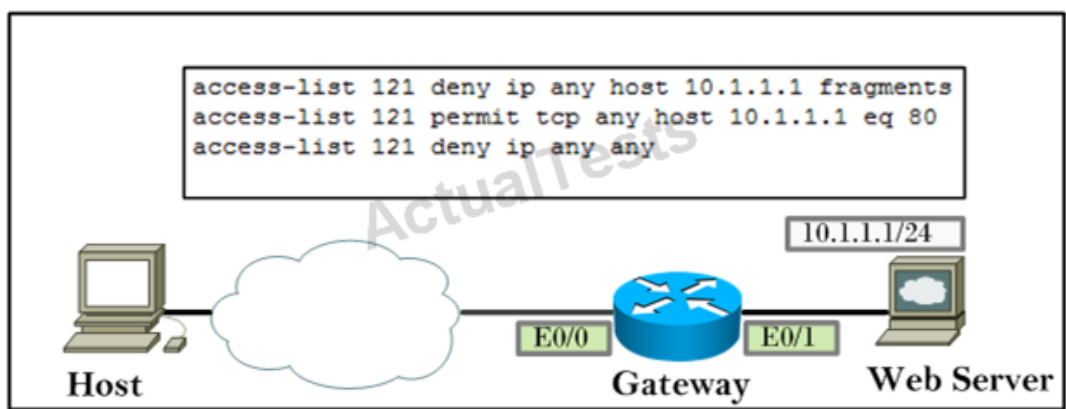
QUESTION NO: 390

Refer to the exhibit.

- A.** The tunnel configuration is incomplete and the DMVPN session will fail between R1 and R2.
- B.** IPsec phase-2 will fail to negotiate due to a mismatch in parameters.
- C.** A DMVPN session will establish between R1 and R2 provided that the BGP and EIGRP configurations are correct.
- D.** A DMVPN session will establish between R1 and R2 provided that the BGP configuration is correct.
- E.** A DMVPN session will fail to establish because R2 is missing the ISAKMP peer address.

Explanation:

Refer to the exhibit.



Identify the behavior of the ACL if it is applied inbound on E0/0.

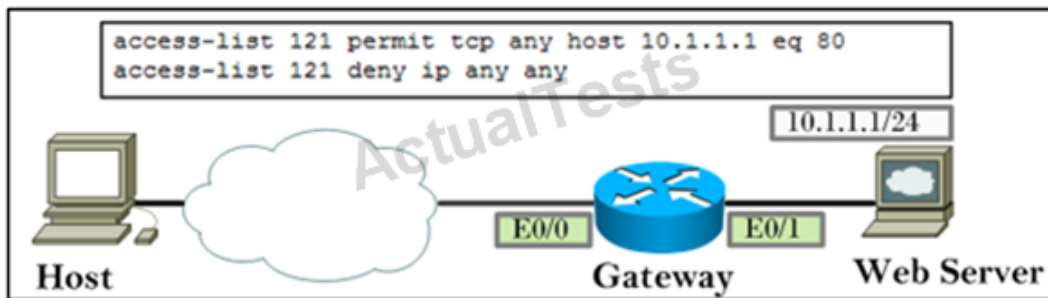
- A. The ACL will drop both initial and noninitial fragments for port 80 only.
- B. The ACL will pass both initial and noninitial fragments for port 80 only.
- C. The ACL will pass the initial fragment for port 80 but drop the noninitial fragment for any port.
- D. The ACL will drop the initial fragment for port 80 but pass the noninitial fragment for any port.

Answer: C

Explanation:

QUESTION NO: 392

Refer to the exhibit.



Identify the behavior of the ACL if it is applied inbound on E0/0.

- A. The ACL will drop both initial and noninitial fragments for port 80 only.
- B. The ACL will pass both initial and non-initial fragments for port 80 only.
- C. The ACL will pass the initial fragment for port 80 but drop the noninitial fragment for any port.
- D. The ACL will drop the initial fragment for port 80 but pass the noninitial fragment for any port.

Answer: B

Explanation:

QUESTION NO: 393

Which three are RFC 5735 addresses? (Choose three.)

- A. 171.10.0.0/24
- B. 0.0.0.0/8
- C. 203.0.113.0/24

- D. 192.80.90.0/24
- E. 172.16.0.0/12
- F. 198.50.100.0/24

Answer: B,C,E

Explanation:

QUESTION NO: 394

Which statement about ISO/IEC 27001 is true?

- A. ISO/IEC 27001 is only intended to report security breaches to the management authority.
- B. ISO/IEC 27001 was reviewed by the International Organization for Standardization.
- C. ISO/IEC 27001 is intend to bring information security under management control.
- D. ISO/IEC 27001 was reviewed by the International Electrotechnical Commission.
- E. ISO/IEC 27001 was published by ISO/IEC.

Answer: C

Explanation:

QUESTION NO: 395

Which two statements about the ISO are true? (Choose two.)

- A. The ISO is a government-based organization.
- B. The ISO has three membership categories: Member, Correspondent, and Subscribers.
- C. Subscriber members are individual organizations.
- D. Only member bodies have voting rights.
- E. Correspondent bodies are small countries with their own standards organization.

Answer: B,D

Explanation:

QUESTION NO: 396

Which three IP resources is the IANA responsible? (Choose three.)

- A. IP address allocation

- B. detection of spoofed address
- C. criminal prosecution of hackers
- D. autonomous system number allocation
- E. root zone management in DNS
- F. BGP protocol vulnerabilities

Answer: A,D,E

Explanation:

QUESTION NO: 397

Which two statements about RFC 2827 are true? (Choose two.)

- A. RFC 2827 defines egress packet filtering to safeguard against IP spoofing.
- B. A corresponding practice is documented by the IEFT in BCP 38.
- C. RFC 2827 defines ingress packet filtering for the multihomed network.
- D. RFC 2827 defines ingress packet filtering to defeat DoS using IP spoofing.
- E. A corresponding practice is documented by the IEFT in BCP 84.

Answer: B,D

Explanation:

QUESTION NO: 398

Which two statements about SOX are true? (Choose two.)

- A. SOX is an IEFT compliance procedure for computer systems security.
- B. SOX is a US law.
- C. SOX is an IEEE compliance procedure for IT management to produce audit reports.
- D. SOX is a private organization that provides best practices for financial institution computer systems.
- E. Section 404 of SOX is related to IT compliance.

Answer: B,E

Explanation:

QUESTION NO: 399

Refer to the exhibit.

```
interface Tunnel0
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip next-hop-self eigrp 101
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 no ip split-horizon eigrp 101
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 1000
 tunnel protection ipsec profile Hub-Spoke
```

Which three statements correctly describe the configuration? (Choose three).

- A. The tunnel is not providing peer authentication
- B. The tunnel encapsulates multicast traffic.
- C. This is a point-to-point GRE tunnel.
- D. The configuration is on the NHS.
- E. The configuration is on the NHC.
- F. The tunnel provides data confidentiality.
- G. The tunnel IP address represents the NBMA address.

Answer: B,D,F

Explanation:

QUESTION NO: 400

Refer to the exhibit.

```
aaa new-model
 parser view Test
 secret abcd1234

commands exec include configure terminal
commands exec include show run
```

Which statement correctly describes the configuration?

- A. The configuration is the super view configuration of role-based access control.
- B. The configuration would not work unless the AAA server is configured for authentication and authorization.
- C. The exec commands in the configuration will be excluded from the test view.
- D. The configuration is the CLI configuration of role-based access control.

Answer: D

Explanation:

QUESTION NO: 401

Which item is not encrypted by ESP?

- A. ESP header
- B. ESP trailer
- C. IP header
- D. Data
- E. TCP-UDP header

Answer: A

Explanation:

QUESTION NO: 402

Which item is not authenticated by ESP?

- A. ESP header
- B. ESP trailer
- C. New IP header
- D. Original IP header
- E. Data
- F. TCP-UDP header

Answer: C

Explanation:

QUESTION NO: 403

Which statement about the distributed SYN flood attack is true?

- A. A distributed SYN flood attack is carried out only by the valid address.
- B. A distributed SYN flood attack is carried out only by spoofed addresses.
- C. Botnet could be used to launch a distributed SYN flood attack.
- D. A distributed SYN flood attack does not completely deplete TCBS SYN-Received state backlog.
- E. A distributed SYN flood attack is the most effective SYN flood attack because it targets server memory.

Answer: C

Explanation:

QUESTION NO: 404

Which statement about the Cisco NAC CAS is true?

- A. The Cisco NAC CAS acts as a gateway between untrusted networks.
- B. The Cisco NAC CAS can only operate as an in-band real IP gateway.
- C. The Cisco NAC CAS can operate as an out-of-band virtual gateway.
- D. The Cisco NAC CAS is an administration and monitoring server.

Answer: C

Explanation:

QUESTION NO: 405

Which statement about the prelogin assessment module in Cisco Secure Desktop is true?

- A. It assigns an IP address to the remote device after successful authentication.
- B. It checks for any viruses on the remote device and reports back to the security appliance.
- C. It checks the presence or absence of specified files on the remote device.
- D. It clears the browser cache on the remote device after successful authentication.
- E. It quarantines the remote device for further assessment if specific registry keys are found.

Answer: C

Explanation:

QUESTION NO: 406

Which two statements about dynamic ARP inspection are true? (Choose two.)

- A. Dynamic ARP inspection checks ARP packets on both trusted and untrusted ports.
- B. Dynamic ARP inspection is only supported on access and trunk ports.
- C. Dynamic ARP inspection checks invalid ARP packets against the trusted database.
- D. The trusted database to check for an invalid ARP packet is manually configured.
- E. Dynamic ARP inspection does not perform ingress security checking.
- F. DHCP snooping must be enabled.

Answer: C,F

Explanation:

QUESTION NO: 407

Which statement about DHCP snooping is true?

- A. The dynamic ARP inspection feature must be enabled for DHCP snooping to work.
- B. DHCP snooping is enabled on a per-VLAN basis.
- C. DHCP snooping builds a binding database using information that is extracted from intercepted ARP requests.
- D. DHCP snooping is enabled on a per-port basis.
- E. DHCP snooping is does not rate-limit DHCP traffic from trusted ports.

Answer: B

Explanation:

QUESTION NO: 408

Which two statements about PCI DSS are true? (Choose two.)

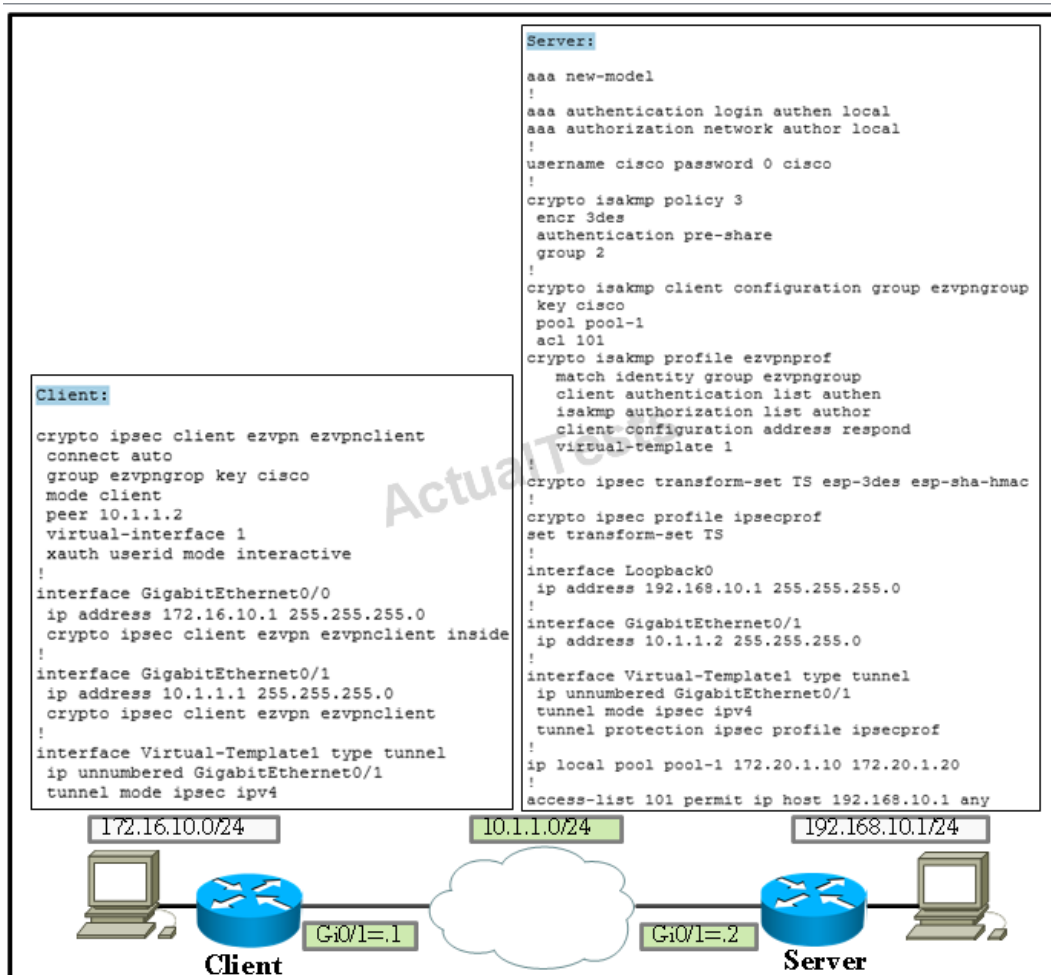
- A. PCI DSS is a US government standard that defines ISP security compliance.
- B. PCI DSS is a proprietary security standard that defines a framework for credit, debit, and ATM cardholder information.
- C. PCI DSS is a criminal act of cardholder information fraud.
- D. One of the PCI DSS objectives is to restrict physical access to credit, debit, and ATM cardholder information.
- E. PCI DSS is an IETF standard for companies to protect credit, debit, and ATM cardholder information.

Answer: B,D

Explanation:

QUESTION NO: 409

Refer to the exhibit.



Why does the EasyVPN session fail to establish between the client and server?

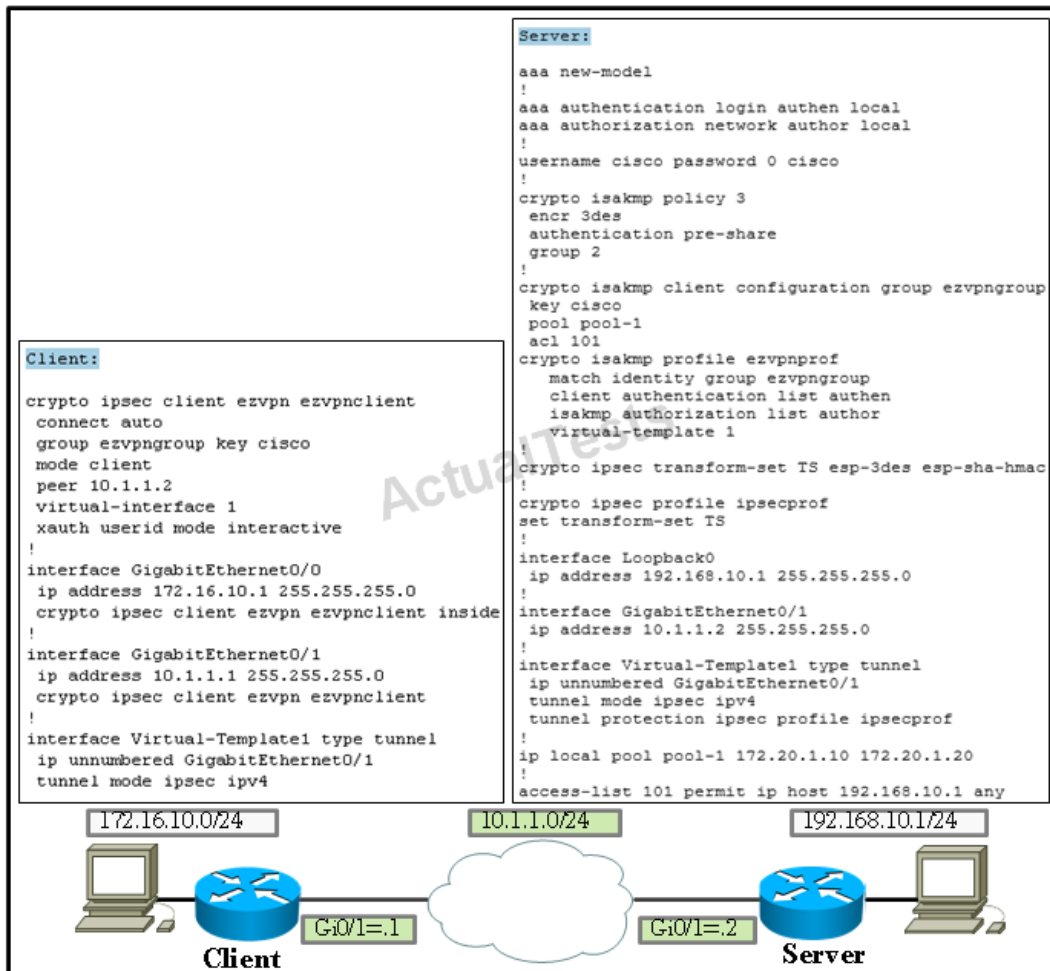
- A. incomplete IPsec phase-1 configuration on the server
- B. incorrect IPsec phase-2 configuration on the server
- C. incorrect group configuration on the client
- D. ISAKMP key mismatch
- E. incorrect ACL in the ISAKMP client group configuration

Answer: C

Explanation:

QUESTION NO: 410

Refer to the exhibit.



Why does the EasyVPN session fail to establish between the client and server?

- A. incomplete ISAKMP profile configuration on the server
- B. incorrect IPsec phase-2 configuration on the server
- C. incorrect group configuration on the client
- D. ISAKMP key mismatch
- E. incorrect virtual-template configuration on the sever

Answer: A

Explanation:

QUESTION NO: 411 DRAG DROP

Match the IKE phase-1 components on the left with their values on the right.

Key Establishment Method	Lifetime in seconds
Data Integrity	DES
Data Confidentiality	MD5
Key Sharing	Pre-shared
Security Association	DH Group 1

Answer:

Match the IKE phase-1 components on the left with their values on the right.

Key Establishment Method	Security Association
Data Integrity	Data Confidentiality
Data Confidentiality	Data Integrity
Key Sharing	Key Sharing
Security Association	Key Establishment Method

Explanation:

Security Association
Data Confidentiality
Data Integrity
Key Sharing
Key Establishment Method

QUESTION NO: 412 DRAG DROP

Match the IKE phase-2 components on the left with their values on the right.

Data Integrity	Lifetime in seconds
Data Confidentiality	ESP
Security Association	DH Keying material
Session Keys Extraction	AH

Answer:

Match the IKE phase-2 components on the left with their values on the right.

Data Integrity	Security Association
Data Confidentiality	Data Confidentiality
Security Association	Session Keys Extraction
Session Keys Extraction	Data Integrity

Explanation:

Security Association
Data Confidentiality
Session Keys Extraction
Data Integrity

QUESTION NO: 413 DRAG DROP

Match the HTTP-HTTPS components on left with their corresponding elements on the right.

HTTPS	URL
HTTP	443
Request	80
Response	Forwarding
Proxy	Relay
Tunnel	Error Codes

Answer:

Match the HTTP-HTTPS components on left with their corresponding elements on the right.

HTTPS	Request
HTTP	HTTPS
Request	HTTP
Response	Proxy
Proxy	Tunnel
Tunnel	Response

Explanation:

Request
HTTPS
HTTP
Proxy
Tunnel
Response

QUESTION NO: 414 DRAG DROP

Match each SMTP component on the left with its roles on the right.	
MTA	Use by MUA to retrieve mail
MUA	Mail Server
MSA	Mail Client
MDA	MTA component for accepting mails
IMAP	MTA component to deliver mails

Answer:

Match each SMTP component on the left with its roles on the right.	
MTA	IMAP
MUA	MTA
MSA	MUA
MDA	MSA
IMAP	MDA

Explanation:

IMAP
MTA
MUA
MSA
MDA

QUESTION NO: 415 DRAG DROP

Match the DNS header Opcode value on the left with the corresponding query type on the right.

0	NOTIFY
1	IXQUERY
2	QUERY
4	STATUS
5	UPDATE

Answer:

Match the DNS header Opcode value on the left with the corresponding query type on the right.

0	4
1	1
2	0
4	2
5	5

Explanation:

4
1
0
2
5

QUESTION NO: 416 DRAG DROP

Match the DNS header Rcode value on the left with the corresponding response code on the right.

0	Server Failure
2	No Error
3	Name Error
4	Refused
5	Not Implemented

Answer:

Match the DNS header Rcode value on the left with the corresponding response code on the right.

0	2
2	0
3	3
4	5
5	4

Explanation:

2
0
3
5
4

QUESTION NO: 417 DRAG DROP

Match the steps on the left with the corresponding description on the right of the URL filtering process on Cisco ASA.	
Step-1	ASA forwards URL to URL filtering server for lookup
Step-2	Lookup response from URL filtering server (Allow-Deny)
Step-3	If URL allowed, ASA forwards HTTP Response to client
Step-4	If URL blocked, ASA resets connection on both sides
Step-5	ASA receives HTTP Response
Step-6	ASA forwards request to Web server
Step-7	HTTP Request sent from client to ASA

Answer:

Match the steps on the left with the corresponding description on the right of the URL filtering process on Cisco ASA.	
Step-1	Step-3
Step-2	Step-5
Step-3	Step-6
Step-4	Step-7
Step-5	Step-4
Step-6	Step-2
Step-7	Step-1

Explanation:

Step-3
Step-5
Step-6
Step-7
Step-4
Step-2
Step-1

QUESTION NO: 418 DRAG DROP

Match the ISE profiler component on the right with its corresponding functionality description on the left.	
Sensor	allows probe configuration to start-stop attribute-value collection from endpoints
Probe Manager	stores endpoints along with their attribute-value in the Cisco ISE database
Forwarder	Classifies endpoints into specified group using their attribute-value
Analyzer	consists of probes capturing attribute-values from the endpoints

Answer:

Match the ISE profiler component on the right with its corresponding functionality description on the left.	
Sensor	Probe Manager
Probe Manager	Forwarder
Forwarder	Analyzer
Analyzer	Sensor

Explanation:

Probe Manager
Forwarder
Analyzer
Sensor

QUESTION NO: 419 DRAG DROP

Matchp the ISO/IEC 27001 domains on left with their corresponding match description on the right?	
Security Policy	defined by the management
Assets Management	information assets inventory and classification
Human Resource Security	access restrictions for Information resources
Physical Security	employees security aspects
Access control	facility security aspects

Answer:

Matchp the ISO/IEC 27001 domains on left with their corresponding match description on the right?	
Security Policy	Security Policy
Assets Management	Assets Management
Human Resource Security	Access control
Physical Security	Human Resource Security
Access control	Physical Security

Explanation:

Security Policy
Assets Management
Access control
Human Resource Security
Physical Security

QUESTION NO: 420 DRAG DROP

Match each SNMP PDUs on the left with the its corresponding functionality on the right.

GetRequest	unsolicited message acknowledgement
SetRequest	unsolicited message
GetNextRequest	to discover available variables value
Trap	to set variables value
InformRequest	to retrieve variables value

Answer:

Match each SNMP PDUs on the left with the its corresponding functionality on the right.

GetRequest	InformRequest
SetRequest	Trap
GetNextRequest	GetNextRequest
Trap	SetRequest
InformRequest	GetRequest

Explanation:

InformRequest
Trap
GetNextRequest
SetRequest
GetRequest