Vendor: Cisco

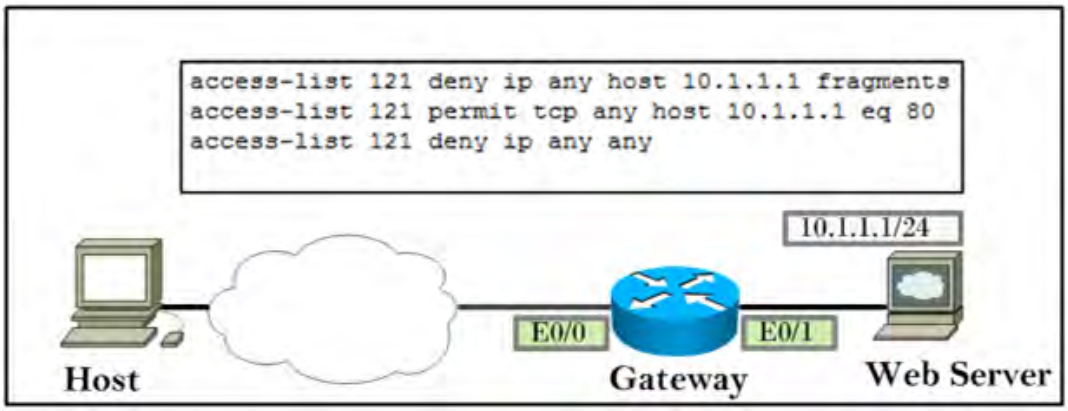
Exam Code: 350-018

Exam Name: CCIE Security written(V4.0)

Version: Demo

Question No : 1

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

Question No : 2

Which two statements about the IPv6 OSPFv3 authentication Trailer are true (choose two)

A. The AT-bit resides in the OSPFv3 Header field
B. The IPv6 Payload length includes the length of the authentication Trailer
C. It Provide an alternative option to OSPFv3 IPsec authentication
D. The AT-bit must be set only in OSPFv3 Hello packets that include an Authentication Trailer
E. The AT-bit must be set only in OSPFv3 Database Description packets that include an Authentication Trailer
F. The OSPFv3 packet length includes the length of the Authentication Trailer

Answer: D,E

Question No : 3

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

Question No : 4

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

Question No : 5

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

Question No : 6

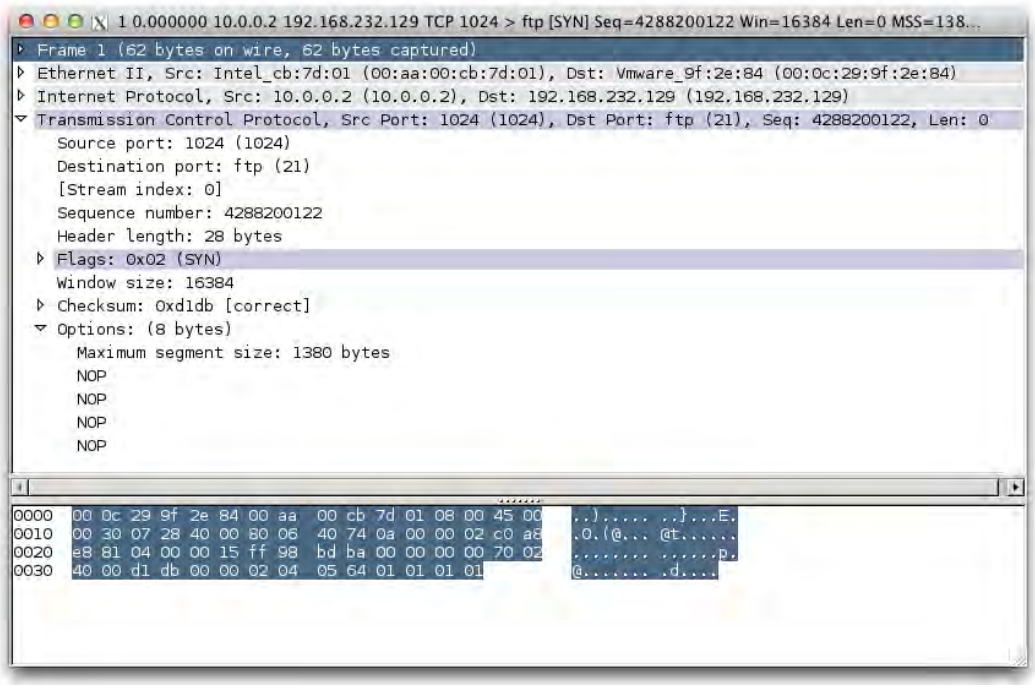
Which statement is true about an SNMPv2 communication?

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

Question No : 7

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

Question No : 8

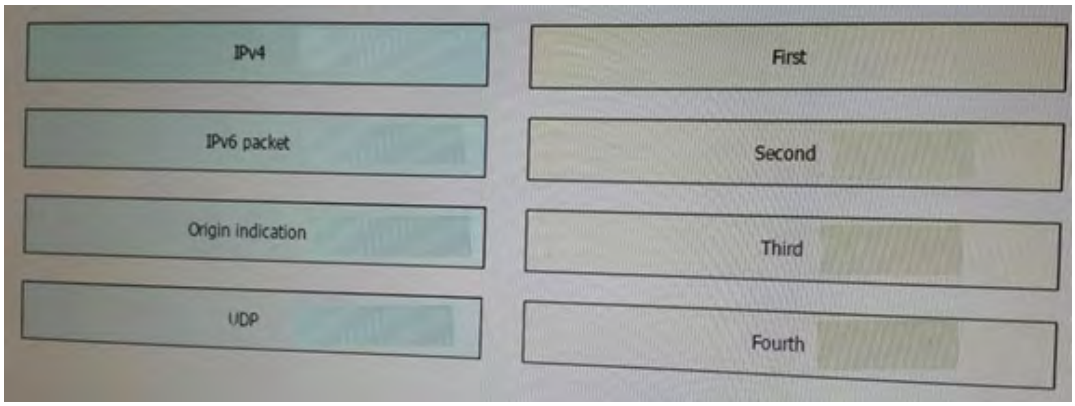
What is the purpose of the BGP TTL security check?

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.

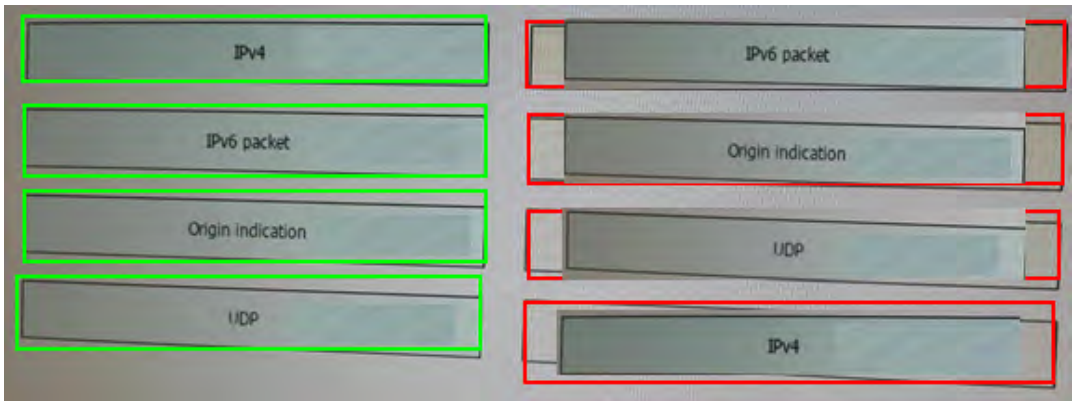
Answer: B

Question No : 9 DRAG DROP

Drag and drop the components of a Teredo IPv6 packet from the left to the correct position in the packet on the right



Answer:



Question No : 10

Which two statements about Network Edge Authentication Technology (NEAT) are true? (Choose two.)

A. It can be configured on both access ports and trunk ports.
B. It allows you to configure redundant links between authenticator and supplicant switches
C. It can be configured on both access ports and EtherChannel ports.
D. It supports port-based authentication on the authenticator switch.
E. It conflicts with auto-configuration
F. It requires a standard ACL on the switch port.

Answer: A,D

Question No : 11

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

Question No : 12

In Cisco Wireless LAN Controller (WLC) , which web policy enables failed Layer 2 authentication to fall back to WebAuth authentication with a user name and password ?

A. Splash Page Web Redirect
B. B. Passthough
C. C.On MAC Filter Failure
D. D. Authentcaiton
E. E.Conditional Web Redirect

Answer: C

Question No : 13

Which three IP resources is IANA responsible for? (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

Question No : 14

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

Question No : 15

Which command sets the key-length for the IPv6 SeND protocol?

A. ipv6 nd inspection
B. ipv6 nd ra-interval
C. ipv6 nd prefix
D. ipv6 nd secured
E. ipv6 nd ns-interval

Answer: D

Explanation:

ipv6 nd secured key-length [[**minimum** | **maximum**] *v alue* **Example:**
Router(config)# ipv6 nd secured key-length minimum 512
Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-first-hop-security.html

Question No : 16

What is the purpose of aaa server radius dynamic-author command?

A. Enables the device to dynamically receive updates from a policy server
B. Enables the switch to automatically authorize the connecting device if all the configured RADIUS servers are unavailable
C. Impairs the ability to configure RADIUS local AAA
D. This command disables dynamic authorization local server configuration mode.

Answer: A

Question No : 17

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 specifiy 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.

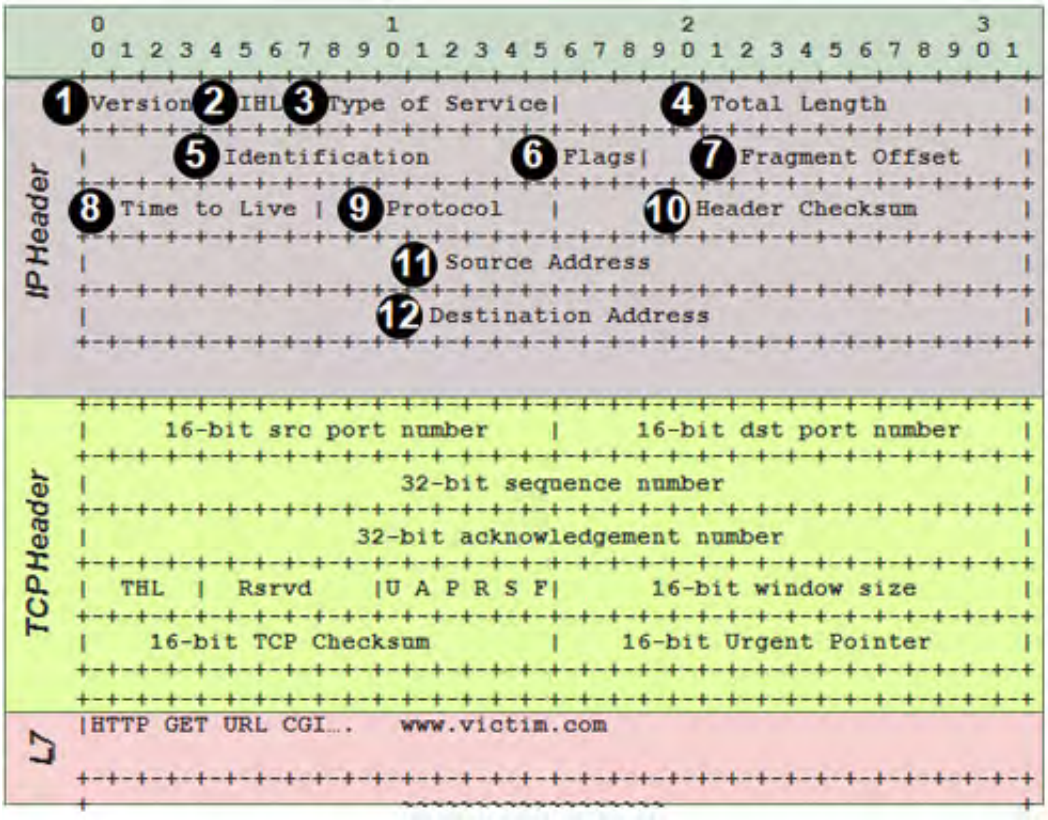
Which three statements about the Cisco IPS sensor are true? (Choose three.)

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

Answer: A,C,E

Question No : 18

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

Question No : 19

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

Question No : 20

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

Question No : 21

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

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

Answer: A

Question No : 22

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

Question No : 23

What security element must an organization have in place before it can implement a security audit and validate the audit results?

A. an Incident Response Team
B. firewalls
C. network access control
D. a security policy
E. a Security Operations Center

Answer: D

Question No : 24

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

Question No : 25

Many guidelines can be used to identify the areas that security policies should cover. In which four areas is coverage most important? (Choose four.)

A. Physical
B. Host
C. User
D. Document
E. Incident handling and response
F. Security awareness training

Answer: A,B,C,D

Question No : 26

Which two statements about Cisco MQC are true? (Choose two)

A. It can classify Layer 2 Packets from legacy protocols
B. By default, its uses match-any matching
C. A packet can match only one traffic class within an individual traffic policy
D. It allows you to link multiple traffic policies to a single traffic class.
E. Unclassified traffic is queued in a FIFO queue to be managed by the match not command configuration
F. It can handle Layer2 packets from legacy protocol without classifying them.

Answer: E,F

Question No : 27

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

Question No : 28

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

Question No : 29

Refer to the exhibit.

```
Router(config)# ipv6 access-list infra-cal
Router(config-ipv6-acl)#deny ipv6 any any routing-type 0
Router(config-ipv6-acl)#

Router(config-ipv6-acl)# interface gi0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 traffic-filter infra-acl in
```

What is the effect of the given ACL Policy?

A. The policy will deny all ipv6 eBGP session
B. The policy will deny all ipv6 routed packets
C. The policy will disable ipv6 source routing
D. The policy will deny all ipv6 routing packet

Answer: C

Question No : 30

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

Question No : 31

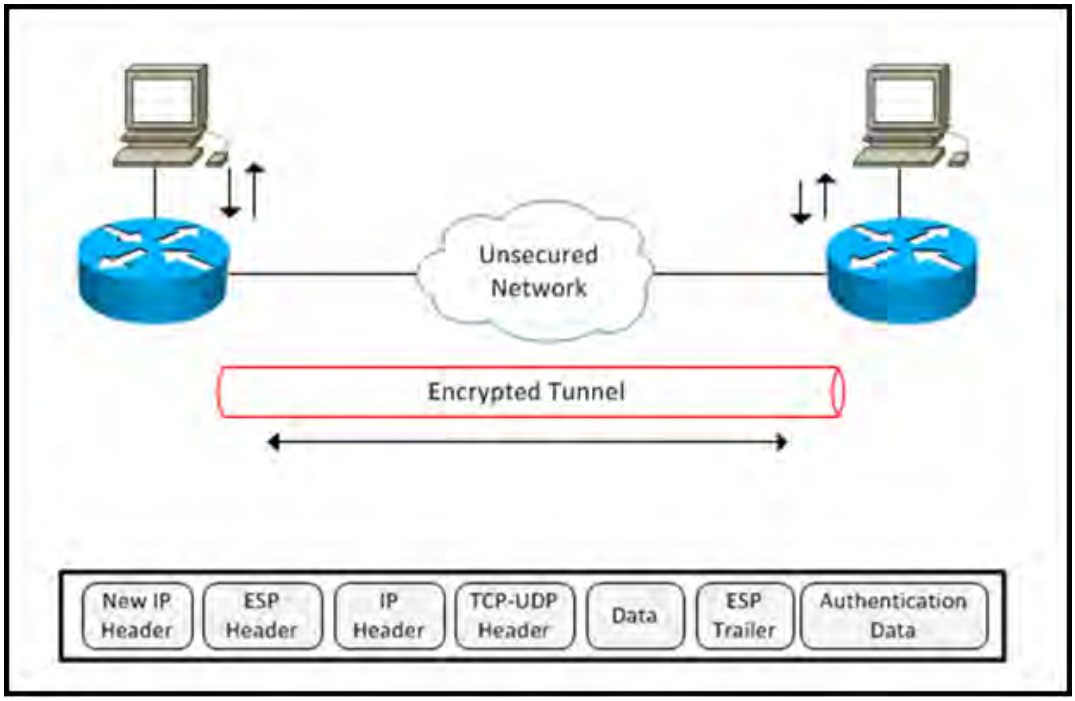
Which three options are the types of zones that are defined for anomaly detection on the Cisco IPS Sensor? (Choose three.)

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

Answer: C,D,E

Question No : 32

Refer to the exhibit.



Which two items are not encrypted by ESP in tunnel mode? (Choose two)

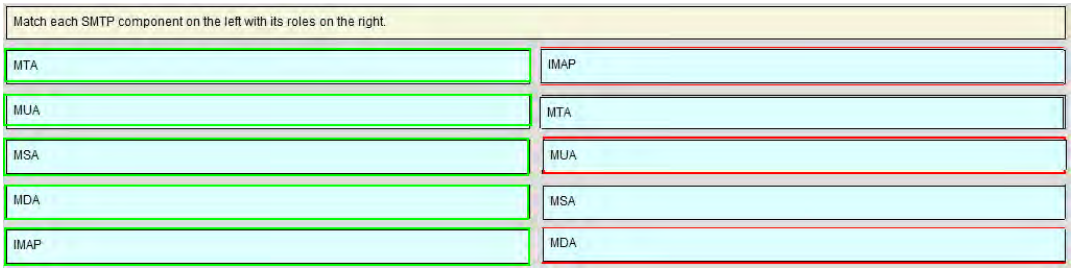
A. ESP header
B. ESP trailer
C. Original IP header
D. Data
E. TCP-UDP header
F. Authentication Data

Answer: A,F

Question No : 33 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:



Question No : 34

Which two are characteristics of WPA? (Choose two.)

A. implements a key mixing function before passing the initialization vector to the RC4 algorithm
B. uses a 40-bit key with 24-bit initialization vector
C. introduces a 64-bit MIC mechanism
D. WPA does not allow Pre-Shared key mode
E. makes the use of AES mandatory

Answer: A,C

Explanation:
On October 31, 2002, the Wi-Fi Alliance endorsed TKIP under the name Wi-Fi Protected Access (WPA).
TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC).
Reference: https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

Question No : 35

Which statement about a botnet attack is true?

A. The botnet attack is an attack on a firewall to disable it's filtering ability.
B. The botnet attack is a network sweeping attack to find hosts that are alive 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

Question No : 36

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

A. rogue
B. unclassified
C. interferer
D. malicious

Answer: A

Question No : 37

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

A. It is part of the original IP header.
B. It is sent to the peer.
C. It is part of a new IP header.
D. It provides integrity only for the new IP header.

Answer: B

Question No : 38

What are the two most common methods that security auditors use to assess an organization's security processes? (Choose two)

A. social engineering attempts
B. B. interviews
C. C. policy assessment
D. D. penetration testing
E. E. document review
F. F. physical observation

Answer: B,E

Question No : 39

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

Question No : 40

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

Question No : 41

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

Question No : 42

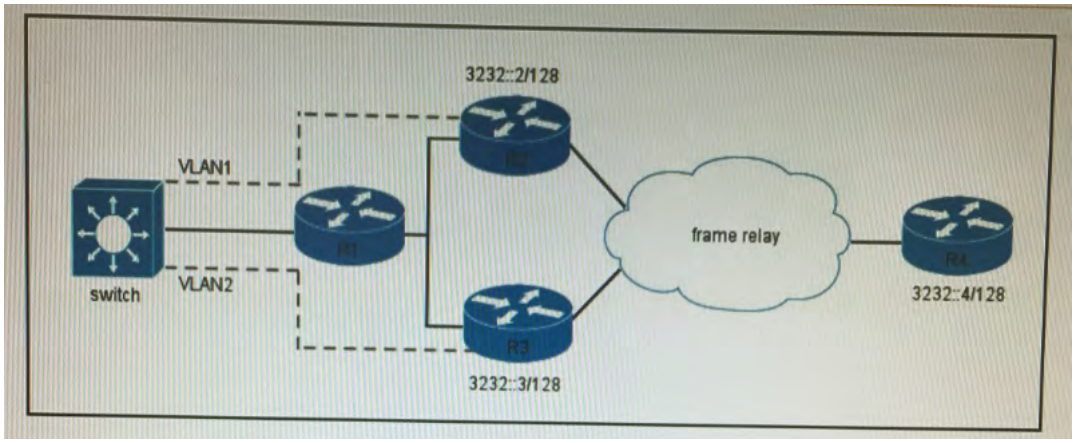
Which IPv6 routing protocol can use IPv6 ESP and AH to provide integrity, authentication, and confidentiality services to protect the routing information exchange between the adjacent routing neighbors?

A. RIPng
B. EIGRPv6
C. BGP-4
D. IS-IS
E. OSPFv3

Answer: E

Question No : 43

Refer to the exhibit.



You have configured two route-map instances on R1. which passes traffic from switch 1 on both VLAN 1 and VLAN 2 You wish to ensure that * The first route-map instance matches packets from VLAN 1 and sets the next hop to 3232:2/128. * The second route-map instance matches packets from VLAN 2 and sets the next hop to 3232:3/128. What feature can you implement on R1 to make this configuration possible?

A. BGP next-hop
B. BGP local-preference
C. PBR
D. VSSP
E. GLBP

Answer: C

Question No : 44

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

Question No : 45

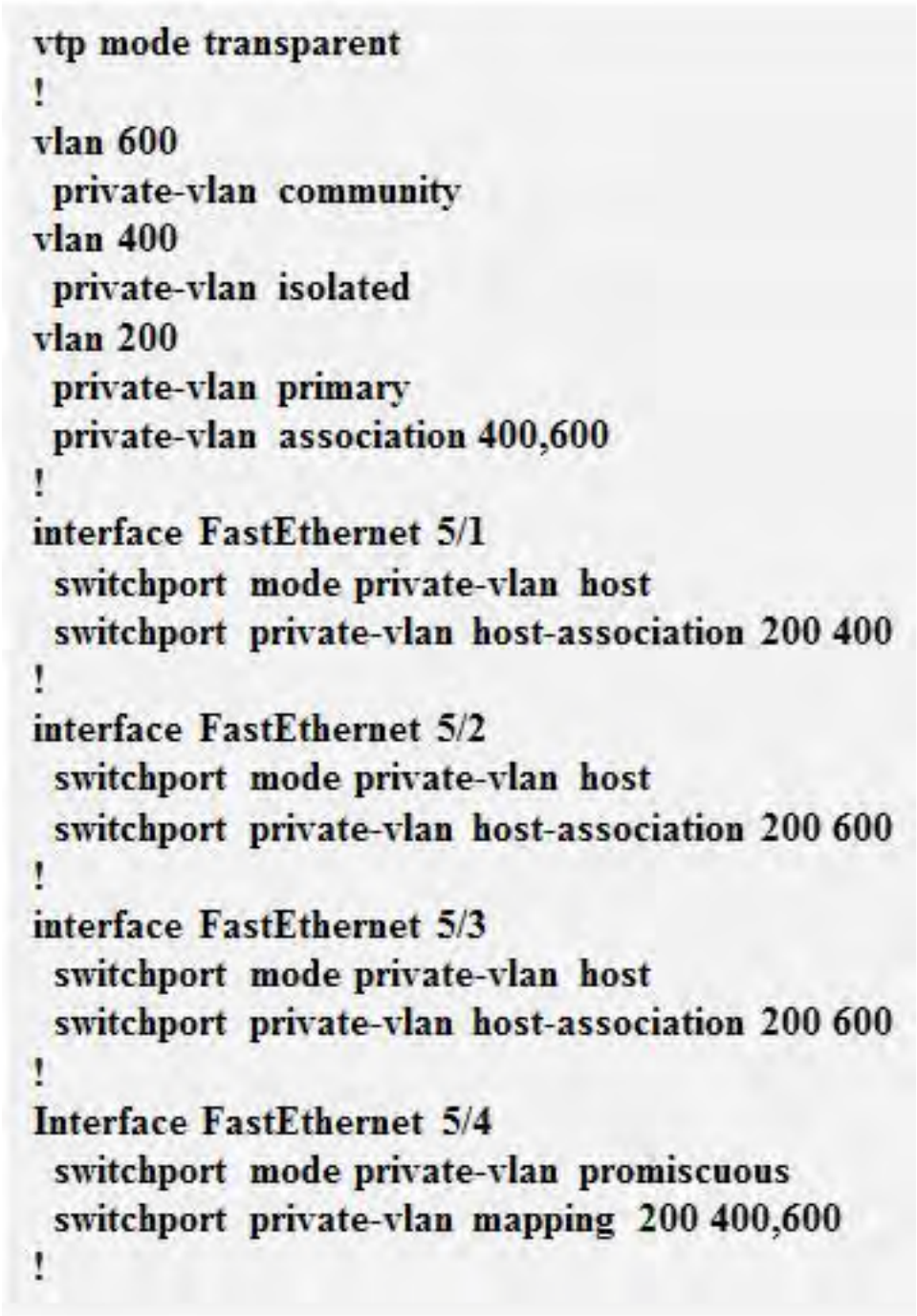
Which pair of ICMP messages is used in an inverse mapping attack?

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

Answer: D

Question No : 46

Refer to the exhibit.



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

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

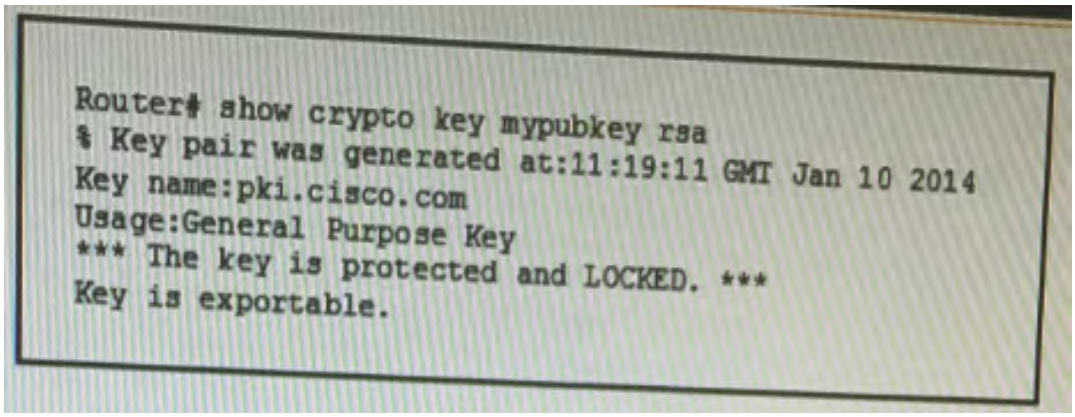
A. The default gateway for VLAN 200 should be attached to the FastEthernet 5/1 interface.
B. Hosts attached to the FastEthernet 5/1 interface can communicate only with hosts attached to the FastEthernet 5/4 interface.

C. Hosts attached to the FastEthernet 5/2 interface can communicate with hosts attached to the FastEthernet 5/3 interface.
D. Hosts attached to the FastEthernet 5/4 interface can communicate only with hosts attached to the FastEthernet 5/2 and FastEthernet 5/3 interfaces.
E. Interface FastEthernet 5/1 is the community port.
F. Interface FastEthernet 5/4 is the isolated port.

Answer: B,C

Question No : 47

Refer to the exhibit.



You executed the show crypto key mypubkey rsa command to verify that the RSA key is protected and it generated the given output. What command must you have entered to protect the key?

A. crypto key decrypt rsa name pki.cisco.com passphrase CiscoPKI
B. crypto key zeroize rsa CiscoPKI
C. crypto key export rsa pki.cisco.com pem url flash: 3des CiscoPKI
D. crypto key lock rsa name pki.cisco.com passphrase CiscoPKI
E. crypto key import rsa pki.cisco.com pem url nvram: CiscoPKI

Answer: D

Question No : 48

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

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

Answer: A,B,C,F

Question No : 49

Which three statements about Cisco Secure Desktop are true? (Choose three)

A. It is interpretable with Clientless SSL VPN, AnyConnect, and the IPSec VPN client.
B. Its supports shared network folder
C. It validate PKI certificates
D. It supports multiple prelogin checks, including IP address, certificate and OS
E. It supports unlimited CSD locations.
F. It can be pre-installed to reduce download time.

Answer: B,C,E

Question No : 50

What Context-Based Access Control (CBAC) command sets the maximum time that a muter running Cisco IOS will wait for a new TCP session to reach the established state?

A. ip inspect max-incomplete
B. ip inspect tcp idle-time
C. ip inspect tcp finwait-time
D. ip inspect udp idle-time
E. ip inspect tcp synwait-time

Answer: E

Explanation: ip inspect tcp synwait-time
To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the ip inspect tcp synwait-timecommand in global configuration mode. To reset the timeout to the default of 30 seconds, use the no form of this command.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

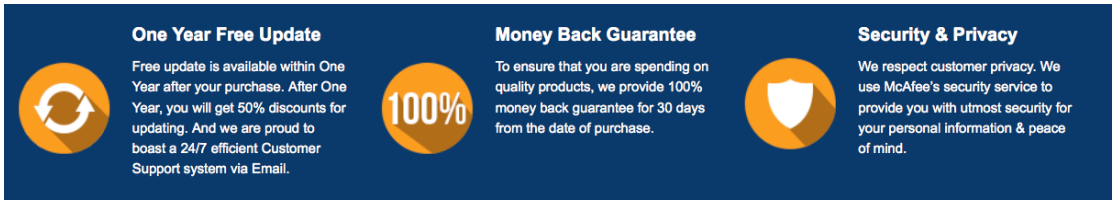
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions