

CCIE Security Written Exam (350-018)

www.wallslab.net

100 Questions
2015.10

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

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

Answer: BC

2. Which statement about DNS is true?

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

Answer: D

3.

Neighbor 100.10.10.10 maximum-prefix 1000 80 warning-only

Refer to the exhibit. Which option describes the behavior of this configuration?

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

Answer: A

4. What is the default duration of IPS anomaly detection's learning accept mode?

- A. 24 hours
- B. 48 hours
- C. 12 hours
- D. 8 hours

Answer: A

5. Which three statements about SSHv1 and SSHv2 are true? (Choose three)

- A. Both SSHv1 and SSHv2 require a server key to protect the session key.
- B. SSHv2 supports a wider variety of user-authentication methods than SSHv1.

- C. Unlike SSHv1, SSHv2 uses separate protocols for authentication, connection, and transport.
- D. Unlike SSHv1, SSHv2 supports multiple forms of user authentication in a single session.
- E. Both SSHv1 and SSHv2 negotiate the bulk cipher.
- F. Both SSHv1 and SSHv2 support multiple session channels on a single connection.

Answer: ACD

6. Which two statements about the BGP backdoor feature are true?(Choose two)

- A. It changes the eBGP administrative distance from 20 to 200.
- B. It makes iBGP learned routes preferred over IGP learned routes.
- C. It makes IGP learned routes preferred over eBGP learned routes.
- D. It changes the iBGP administrative distance from 200 to 20.
- E. It makes eBGP learned routes preferred over IGP learned routes.
- F. It changes the eBGP administrative distance from 200 to 20.

Answer: AC

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

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

Answer: C

8. Which of these is an invalid syslog facility?

- A. 0
- B. 31
- C. 1
- D. 12

Answer: B

9. What is the range of valid stratum numbers for NTP when configuring a Cisco IOS device as an authoritative NTP server?

- A. 1 to 16
- B. 1 to 15
- C. 0 to 16
- D. 0 to 4

Answer: B

10. Which set of encryption algorithms is used by WPA and WPA2?

- A. TKIP and AES
- B. Blowfish and AES
- C. CAST and RC6
- D. TKIP and RC6

Answer: A

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

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

Answer: CE

12. Which of the following statement is true about the ARP Spoofing attack?

- A. Attacker sends the ARP request with the MAC address and IP address of a legitimate resource in the network.
- B. Attacker sends the ARP request with it's own MAC address and IP address of a legitimate resource in the network.
- C. Attacker sends the ARP request with the MAC address and IP address of it's own.
- D. ARP spoofing does not facilitate man-in-the middle attack for the attacker.

Answer: B

13. For which reason would an RSA key pair need to be removed?

- A. The CA has suffered a power outage
- B. PKI architecture would never allow the RSA key pair removal
- C. The existing CA is replaced, and the new CA requires newly generated keys
- D. The CA is under DoS attack

Answer: C

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

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

Answer: A

15. Which statement is true regarding Transparent mode configuration on Cisco ASA firewall running version 9?

- A. Networks connected with the ASA data interfaces must be in different subnets for the traffic to flow.
- B. You need to make management interface of the ASA as the next-hop for the connected devices to establish.
- C. Default route defined on the ASA is only for the management traffic return path.
- D. Management interface does not update the MAC address table.
- E. Bridge Groups are not supported in Transparent mode.

Answer: C

16. What are two enhancements in WCCP V2.0 over WCCP V1.0? (Choose two)

- A. authentication support
- B. multicast support
- C. encryption support
- D. IPv6 support
- E. support for HTTP redirection

Answer: AB

17. Which three items does TLS rely on to prove identity? (Choose three)

- A. password
- B. Trustpoint
- C. private keys
- D. certificates
- E. public keys
- F. username

Answer: CDE

18.

```
ASA5540(config)#class-map snoop-DNS
ASA5540(config-cmap)#match port udp eq domain
ASA5540(config)#policy-map snoop-policy
ASA5540(config-pmap)#class snoop-DNS
ASA5540(config-pmap-c)#inspect dns dynamic-filter-snoop
ASA5540(config)#service-policy snoop-policy interface outside
```

Refer to the exhibit. Against which type of attack does the given configuration protect?

- A. a botnet attack
- B. pharming
- C. phishing
- D. DNS hijacking

E. DNS cache poisoning

Answer: A

19. Which two statements about IPv6 path MTU discovery are true? (Choose two)

- A. If the source host receives an ICMPv6 Packet Too Big message from a router, it reduces its path MTU.
- B. During the discovery process, the DF bit is set to 1.
- C. If the destination host receives an ICMPv6 Packet Too Big message from a router, it reduces its path MTU.
- D. It can allow fragmentation when the minimum MTU is below a configured value.
- E. The initial path MTU is the same as the MTU of the original node's link layer interface.
- F. The discovery packets are dropped if there is congestion on the link.

Answer: AE

20. Which MAC address control command enables usage monitoring for a CAM table on a switch?

- A. mac-address-table learning
- B. mac-address-table synchronize
- C. mac-address-table limit
- D. mac-address-table secure
- E. mac-address-table notification threshold

Answer: E

21.

```
crypto ipsec transform-set Hub-Spoke esp-aes esp-sha-hmac
!
crypto ipsec profile Hub-Spoke
 set transform-set Hub-Spoke
!
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
```

Refer to the exhibit. Which three descriptions of the configuration are true? (Choose three)

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

Answer: ABD

22.

```
ipv6 nat v6v4 pool v4pool 10.1.10.1 10.1.10.10 prefix-length 24
```

Refer to the exhibit. What is the purpose of the command in the NAT-PT for IPv6 implementation on a Cisco IOS device?

- A. It defines the IPv4 address pool used by the NAT-PT for dynamic address mapping.
- B. It defines the IPv6 address pool used by the NAT-PT for dynamic address mapping.
- C. It defines the IPv4 address pool used by the NAT-PT for static address mapping.
- D. It defines address pool used by the IPv6 access-list.
- E. It defines address pool used by the IPv4 access-list.

Answer: A

23. What technology can secure DNS information in IP networks?

- A. DNSSEC
- B. a combination of DNS and SSL/TLS
- C. a combination of DNS and IPSec
- D. DNS encryption

Answer: A

24.

```
Client:
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/1
!
crypto ipsec client ezvpn client
 connect auto
 group vpngroup key cisco
 mode client
 peer 101.1.1.2
 virtual-interface 1
 username ccie password ccie
 xauth userid mode local
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.0
 crypto ipsec client ezvpn ezvpncient
 inside
!
interface GigabitEthernet0/1
 ip address 101.1.1.1 255.255.255.0
```

www.wallslab.net

Server:

```
username ccie password 0 ccie
!
interface Loopback0
 ip address 20.20.20.1 255.255.255.0
!
ip local pool client 169.10.10.10 169.10.10.20
!
access-list 101 permit ip host 20.20.20.1 any
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group vpngroup
 key cisco
 pool client
 acl 101
 save-password
!
crypto ipsec transform-set ts esp-3des
 esp-sha-hmac
!
crypto ipsec profile ipsecprofile
 set transform-set ts
!
interface Virtual-Template type tunnel
 ip unnumbered GigabitEthernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsecprofile
!
crypto isakmp profile isakmpprofile
 match identity group vpngroup
 client authentication list authen
 isakmp authorization list author
 client configuration address respond
 virtual-template 1
!
interface GigabitEthernet0/1
 ip address 101.1.1.2 255.255.255.0
```

Refer to the exhibit. Why is there no encrypted session between host 10.10.10.1 and 20.20.20.1?

A. incorrect or missing Virtual-Template configuration on the server

- B. incorrect or missing Virtual-Template configuration on the client
- C. incorrect or missing phase 1 configuration on server
- D. incorrect or missing group configuration on the server
- E. incorrect or missing phase 2 configuration on the server
- F. incorrect or missing group configuration on the client

Answer: B

注：错点在 client:

```
Client:
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/1
! 缺 tunnel mode ipsec ipv4
```

25. An RSA key pair consists of a public key and a private key and is used to set up PKI. Which statement applies to RSA and PKI?

- A. It is possible to determine the RSA key-pair private key from its corresponding public key
- B. The RSA key-pair is a symmetric cryptography
- C. When a router that does not have an RSA key pair requests a certificate, the certificate request is sent, but a warning is shown to generate the RSA key pair before a CA signed certificate is received.
- D. The public key must be included in the certificate enrollment request

Answer: D

26. Which three parameters does the HTTP inspection engine use to inspect the traffic on Cisco IOS firewall? (Choose three)

- A. source address
- B. application
- C. transfer encoding type
- D. request method
- E. minimum header length
- F. destination address

Answer: BCD

27. 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 faster in computation than DES.
- C. The RC4 algorithm cannot be used with wireless encryption protocols.
- D. The RC4 algorithm uses variable-length keys.
- E. in the RC4 algorithm, the 40-bit key represents four characters of ASCII code.

Answer: BD

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

- A. The VTP password is hashed to preserve authenticity using the MD5 algorithm.
- B. The VTP password is encrypted for confidentiality using 3DES.
- C. The VTP password can be configured only when the switch is in Server mode.
- D. The VTP password is sent in the summary advertisements.
- E. The VTP password can only be configured when the switch is in Client mode.

Answer: AD

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

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

Answer: AE

30. To transport VXLAN traffic, which minimum MTU change, from a default MTU of 1500 bytes on the port, is required to avoid fragmentation and performance degradation?

- A. 1650 bytes
- B. 1550 bytes
- C. 9100 bytes
- D. 9114 bytes

Answer: B 31.

```
Client:
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/1
 tunnel mode ipsec ipv4
!
crypto ipsec client ezvpn client
 connect auto
 group vpngroup key cisco
 mode client
 peer 101.1.1.2
 virtual-interface 1
 username ccie password ccie
 xauth userid mode local
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.0
 crypto ipsec client ezvpn ezvpncient
 inside
!
interface GigabitEthernet0/1
 ip address 101.1.1.1 255.255.255.0
```

www.wallslab.net

Server:

```
username ccie password 0 ccie
!
interface Loopback0
 ip address 20.20.20.1 255.255.255.0
!
ip local pool client 169.10.10.10 169.10.10.20
!
access-list 101 permit ip host 20.20.20.1 any
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group vpngroup
 key Cisco
 pool client
 acl 101
 save-password
!
crypto ipsec transform-set ts esp-3des esp-sha-
hmac
!
crypto ipsec profile ipsecprofile
 set transform-set ts
!
interface Virtual-Template type tunnel
 ip unnumbered GigabitEthernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsecprofile
!
crypto isakmp profile isakmpprofile
 match identity group vpngroup
 client authentication list authen
 isakmp authorization list author
 client configuration address respond
 virtual-template 1
!
interface GigabitEthernet0/1
 ip address 101.1.1.2 255.255.255.0
```

Refer to the exhibit. Why is there no encrypted session between host 10.10.10.1 and 20.20.20.1?

A. incorrect or missing group configuration on the server

- B. incorrect or missing phase 2 configuration on the server
- C. incorrect or missing Virtual-Template configuration on the server
- D. incorrect or missing phase 1 configuration on server
- E. incorrect or missing Virtual-Template configuration on the client

Answer: A

注：错点在 Server:

```
crypto isakmp client configuration group vpngrpou
key Cisco
pool client
acl 101
save-password
```

32. Which statement is valid regarding SGACL?

- A. Dynamically downloaded SGACL does not override manually configured conflicting policies.
- B. SGACL is access-list bound with a range of SGTs and DGTs.
- C. SGACL mapping and policies can only be manually configured.
- D. SGACL is not a role-based access list.

Answer: B

33. Which statement about the fragmentation of IPsec packets in routers is true?

- A. By default, the router knows the IPsec overhead to add to the packet, performs a lookup if the packet will exceed egress physical interface IP MTU after encryption, then fragments the packet before encrypting and separately encrypts the resulting IP fragments.
- B. By default if the packet size exceeds MTU of the egress physical interface, it will be dropped.
- C. By default if the packet size exceeds MTU of ingress physical interface, it will be fragmented and sent without encryption.
- D. 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, the the encrypted packet is fragmented before being sent.

Answer: A

34. Which two statements about ISO 27001 are true? (Choose two)

- A. It was formerly known as BS7799-2.
- B. It is an Information Security Management Systems specification.
- C. It is an ISO 17799 code of practice.
- D. It is a code of practice for Informational Social Management.
- E. It is closely aligned to ISO 22000 standards.

Answer: AB

35. Depending on configuration, which two behaviors can the ASA classifier exhibit when it receives unicast traffic on an interface that is shared by multiple contexts? (Choose two)

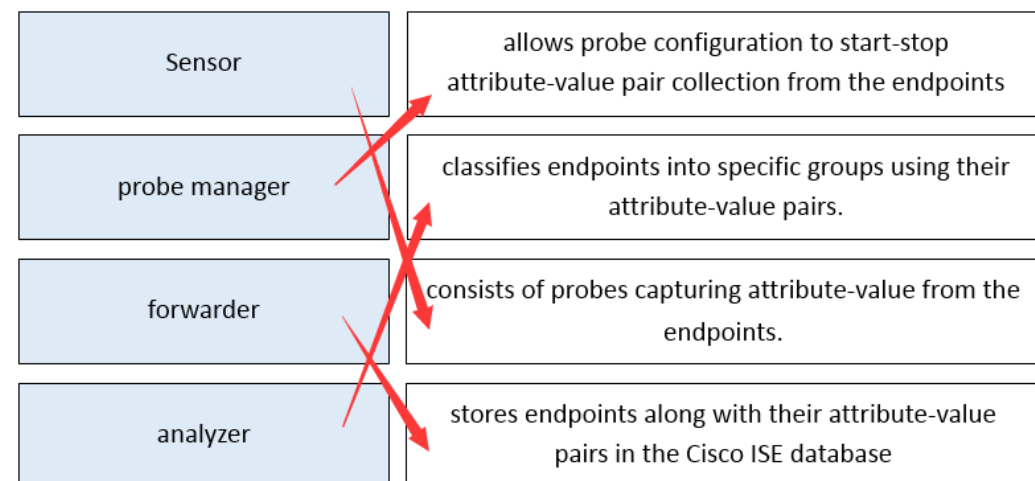
- A. It is classified using the destination address of the packet using the routing table.
- B. It is classified using the destination address of the packet using the NAT table.
- C. It is classified by copying and sending the packet to all the contexts.
- D. It is classified using the destination MAC address of the packet.
- E. It is classified using the destination address of the packet using the connection table.

Answer: BD

36. Drag and drop the ISE profiler components on the left onto their corresponding functionalities description on the right.

Sensor	allows probe configuration to start-stop attribute-value pair collection from the endpoints
probe manager	classifies endpoints into specific groups using their attribute-value pairs.
forwarder	consists of probes capturing attribute-value from the endpoints.
analyzer	stores endpoints along with their attribute-value pairs in the Cisco ISE database

Answer:



Sensor	allows probe configuration to start-stop attribute-value pair collection from the endpoints
probe manager	classifies endpoints into specific groups using their attribute-value pairs.
forwarder	consists of probes capturing attribute-value from the endpoints.
analyzer	stores endpoints along with their attribute-value pairs in the Cisco ISE database

37. Drag and drop the ISO/IEC 27001 domains on the left onto their corresponding description on the right.

Assets Management	defined by the management
-------------------	---------------------------

Security Policy	information assets inventory and classification
Human Resource Security	access restriction for the information resources
Physical Security	employees security aspect
Access Control	facility security aspect

Answer:

Assets Management	defined by the management
Security Policy	information assets inventory and classification
Human Resource Security	access restriction for the information resources
Physical Security	employees security aspect
Access Control	facility security aspect

38. Which encapsulation technique does VXLAN use?

- A. MAC in GRE
- B. MAC in UDP
- C. MAC in TCP
- D. MAC in MAC

Answer: B

39. Drag the elements on the left to their corresponding functionality on right.

Cisco TrustSec SGT Exchange Protocol	facility security aspect
SGACL	control protocol for propagating IP-to-SGT binding information across network device.
Cisco TrustSec	build secure networks by establishing domains of trusted network devices.

Answer:

Cisco TrustSec SGT Exchange Protocol	facility security aspect
SGACL	control protocol for propagating IP-to-SGT binding information across network device.
Cisco TrustSec	build secure networks by establishing domains of trusted network devices.

注：考试时“facility security aspect”可能会变成“associates SGT with a policy”，记住另外两条即可

40. Which statement is true about the Cisco ASA interface monitoring?

- A. It is possible to configure a context to monitor a shared interface
- B. If the monitored interface has both IPv4 and IPv6 addresses then it cannot be monitored.
- C. ASA does not clear the received packets count on the monitored interface before running the tests.
- D. Interfaces of the same context cannot be monitored.

Answer: C

41. Which option describes the main purpose of EIGRP authentication?

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

Answer: D

42. Which two values you must configure on the Cisco ASA firewall to support FQDN ACL?(Choose two)

- A. a DNS server
- B. a service object
- C. a service policy
- D. a class map
- E. an FQDN object
- F. a policy map

Answer: AE

43.

```
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
```

Refer to the exhibit. Which two statements about this **debug** output are true? (Choose two)

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

Answer: AD

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

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

Answer: CD

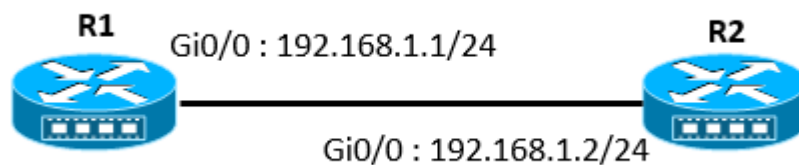
45. Attacks can originate from multicast receivers. Any receivers that sends an IGMP or MLD report typically creates state on which router?

- A. source

- B. RP
- C. first-hop
- D. customer

Answer: C

46.



Refer to the exhibit. Which configuration prevents R2 from becoming a PIM neighbor with R1?

- A. access-list 10 deny 192.168.1.2 0.0.0.0

!

Interface gi0/0

ip pim neighbor-filter 10

- B. access-list 10 deny 192.168.1.2 0.0.0.0

!

Interface gi0/0

ip pim neighbor-filter 1

- C. access-list 10 deny 192.168.1.2 0.0.0.0

!

Interface gi0/0

ip igmp access-group 10

- D. access-list 10 permit 192.168.1.2 0.0.0.0

!

Interface gi0/0

ip pim neighbor-filter 10

Answer: A

47. Which statement is true about the PKI deployment using Cisco IOS devices?

- A. During the enrollment, CA or RA signs the client certificate request with its public key.
- B. RA is capable to publish the CRLs.
- C. Certificate Revocation is not supported by SCEP protocol.
- D. RA is used for accepting the enrollment requests.
- E. Peers use private keys in their certificates to negotiate IPsec SAs to establish the secure channel.

Answer: D

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

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

Answer: C

49. Of which IPS application is Event Store a component?

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

Answer: A

50. For what reason has the IPv6 Type 0 Routing Header been recommended for deprecation?

- A. Attackers can exploit its functionality to generate DoS attacks.
- B. It can create a black hold when used in combination with other routing headers.
- C. When Type 0 traffic is blocked by a firewall policy, all other traffic with routing headers is dropped automatically.
- D. It can conflict with ingress filtering.

Answer: A

51. In the IPv6 address 2001:DB8:130F::870:0:140B/64, which portion is the IPv6 interface identifier?

- A. 2001:DB8:130F:0:
- B. 0:870:0:140B
- C. 870:0:140B
- D. 2001:DB8:130F

Answer: B

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

- A. A corresponding practice is documented by the IETF in BCP 84.
- B. it defines ingress packet filtering to defeat DoS that uses IP spoofing.
- C. it defines ingress packet filtering for the multihomed network.
- D. it is endorsed by the IETF in BCP 38.
- E. it defines egress packet filtering to safeguard against IP spoofing.

Answer: BD

53.

```
NHRP: Attempting to send packet via DEST 180.10.10.1
NHRP: NHRP successfully resolved 180.10.10.1 to NBMA 20.10.10.3
NHRP: Encapsulation succeeded. Tunnel IP addr 20.10.10.3
NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 92
src: 180.10.10.2, dst: 180.10.10.1
(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: 66461
src NBMA: 91.91.91.1
src protocol: 180.10.10.2, dst protocol: 180.10.10.1 (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
NHRP: 120 bytes out Tunnel0
```

Refer to the exhibit. Which two statements correctly describe the debug output? (Choose two)

- A. The message is observed on the NHS
- B. The NHRP hold time is 3 hours
- C. The local non-routable address is 20.10.10.3
- D. The message is observed on the NHC
- E. The remote routable address 91.91.91.1
- F. The remote VPN address is 180.10.10.1

Answer: DF

54. When attempting to use basic HTTP authentication a client, which type of HTTP message should the server use?

- A. HTTP 302 with an Authenticate header
- B. HTTP 200 with a WWW-Authenticate header
- C. HTTP 401 with a WWW-Authenticate header
- D. HTTP 407

Answer: C

55. In traceroute, which ICMP message indicates that the packet is dropped by a router in the path?

- A. Type 3, Code 1
- B. Type 11, Code 0
- C. Type 5, Code 1
- D. Type 3, Code 3
- E. Type 11, Code 1


Answer: B

56. Drag and drop the description on the left onto the associated items on the right

collection of similar programs that work together to execute specific tasks	Trojan horse
independent malicious program copies itself from one host to another over a network and carries other programs	worm
programs that appear to have one function but actually perform a different function	virus
programs that modify other programs and that attach themselves to other programs on execution	botnet

Answer:

collection of similar programs that work together to execute specific tasks	Trojan horse
independent malicious program copies itself from one host to another over a network and carries other programs	worm
programs that appear to have one function but actually perform a different function	virus
programs that modify other programs and that attach themselves to other programs on execution	botnet



57. Which statement about the Cisco ASA operation running version 8.3 is true?

- A. The interface access list is matched first before the global access lists.
- B. The interface and global access lists both can be applied in the input or output direction.
- C. The **static** CLI command is used to configure static NAT translation rules.
- D. NAT control is enabled by default.

Answer: A

58. What are two advantages of SNMPv3 over SNMPv2c? (Choose two)

- A. integrity, to ensure that data has not been tampered with in transit
- B. GetBulkRequest capability, to retrieve large amounts of data in a single request
- C. confidentiality via encryption of packets, to prevent man-in-the-middle attacks
- D. Packet replay protection mechanism removed for efficiency
- E. no source authentication mechanism for faster response time

Answer: AC

59. Which two of the following pieces of information are communicated by the ASA in version 8.4 or later when the Stateful Failover is enabled? (Choose two)

- A. user authentication
- B. NAT translation table
- C. DHCP server address leases.
- D. dynamic routing tables
- E. power status

Answer: BD

60. Which two statements about the storm control implementation on the switch are true? (Choose two)

- A. Traffic storm level is the rate at which Layer 3 traffic is received on the port.
- B. A lower storm control level means more traffic is allowed to pass through.
- C. Traffic storm level is the percentage of total available bandwidth of the port.
- D. Traffic storm control monitors the broadcast, multicast, and unicast traffic.
- E. Traffic storm level is the rate at which Layer 2 traffic is received on the port.
- F. Traffic storm control monitors only the broadcast traffic.

Answer: CD

61. Which statement about VLAN is true?

- A. VLAN cannot be routed.
- B. VLAN1 is a Cisco default VLAN that can be deleted.
- C. The extended-range VLANs cannot be configured in global configuration mode.
- D. VLANs 1006 through 4094 are not propagated by VTP version 3

Answer: A

62. Which statement about the DH group is true?

- A. It establishes a shared key over a secured medium.
- B. It is negotiated in IPsec phase 2.
- C. It does not provide data authentication.
- D. It provides data confidentiality.

Answer: C

63. Drag and drop the SMTP components on the left onto their corresponding roles on the right.

MUA	Is the component that interacts with the end user.
-----	--

MTA	Is the component responsible to move email from sending mail server to the recipient mail server.
MDA	Is the component responsible to move email from MTA to the user mailbox in the recipient mail server.
POP/IMAP	Is the component responsible to fetch email from recipient mail server mailbox to recipient MUA.

Answer:

MUA	Is the component that interacts with the end user.
MTA	Is the component responsible to move email from sending mail server to the recipient mail server.
MDA	Is the component responsible to move email from MTA to the user mailbox in the recipient mail server.
POP/IMAP	Is the component responsible to fetch email from recipient mail server mailbox to recipient MUA.

注：别记顺序，记对应关系

64. Which statement about ISO/IEC 27001 is true?

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

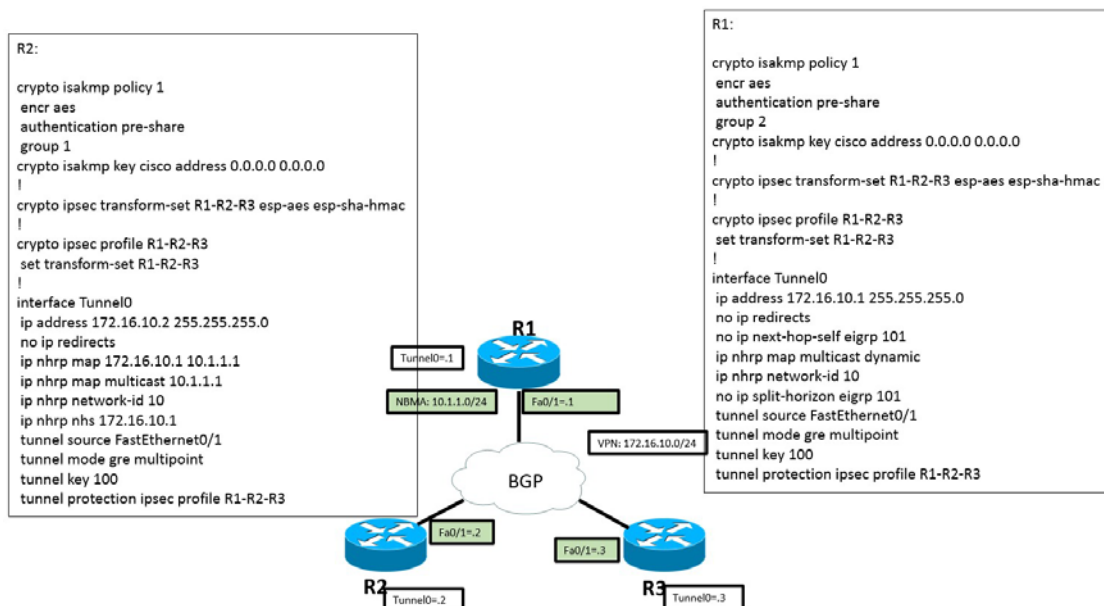
Answer: C

65. Which two statements about SSL VPN smart tunnels on a Cisco IOS device are true? (Choose two)

- A. They can be started in more than one Web browser at the same time.
- B. They support private socket libraries
- C. They do not support FTP.
- D. They are incompatible with MAPI proxy.
- E. They are incompatible with split tunneling.

Answer: DE

66.



Refer to the exhibit. Which option is the reason for the failure of the DMVPN session between R1 and R2?

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

Answer: B

注：错点在



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

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

Answer: ADF

68. Of which IPS application is Event Action Rule a component?

- A. AuthenticationApp
- B. InterfaceApp

- C. SensorApp
- D. MainApp
- E. SensorDefinition
- F. NotificationApp

Answer: C

69. Which statement describes RA?

- A. The RA is part of private key infrastructure.
- B. The RA has the power to accept registration requests and to issue certificates.
- C. The RA is not responsible to verify users request for digital certificates.
- D. The RA only forwards the requests to the CA to issue certificates.

Answer: D

70. Which statement about Infrastructure ACLs on Cisco IOS software is true?

- A. They are used to protect the device forwarding path.
- B. They are used to protect device management and internal link addresses.
- C. They only protect device physical management interface.
- D. They are used to authorize the transit traffic.

Answer: B

71.

Client:

```

crypto ipsec client ezvpn ezvpncient
connect auto
group ezvpngroup key cisco
mode client
peer 10.1.1.2
virtual-interface 1
xauth userid mode interactive
!
interface GigabitEthernet0/0
ip address 172.16.10.1 255.255.255.0
crypto ipsec client ezvpn ezvpncient inside
!
interface GigabitEthernet0/1
ip address 10.1.1.1 255.255.255.0
crypto ipsec client ezvpn ezvpncient
!
interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/1
tunnel mode ipsec ipv4

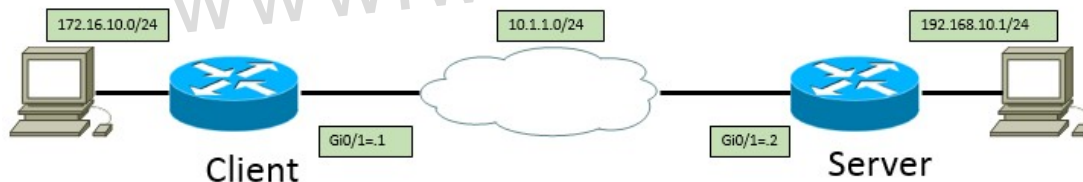
```

Server:

```

aaa new-model
!
aaa authentication login authen local
aaa authorization network author local
!
username cisco password 0 cisco
!
crypto isakmp policy 3
encr 3des
authentication pre-share
group 2
!
crypto isakmp client configuration group ezvpngroup
key cisco
pool pool-1
acl 101
crypto isakmp profile ezvpnpf
match identity group ezvpngroup
client authentication list authen
isakmp authorization list author
client configuration address respond
virtual-template 1
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile ipsecprof
set transform-set TS
!
interface Loopback0
ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
ip address 10.1.1.2 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/1
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsecprof
!
ip local pool pool-1 172.20.1.10 172.20.1.20
!
access-list 101 permit ip host 192.168.10.1 any

```



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

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

Answer: C

注：错点在

Client:

```

crypto ipsec client ezvpn ezvpncient
connect auto
group ezvpngroup key cisco
mode client
peer 10.1.1.2
virtual-interface 1
xauth userid mode interactive
! 缺username cisco password cisco

```

72.

```
authentication order mab dot1x
authentication priority dot1x mab
```

Refer to the exhibit. Which statement about the configuration commands is true?

- A. These commands return an error because of a mismatch between the Dot1x order and priority.
- B. By default, the switch attempts MAB and then Dot1x.
- C. Changing the default order of authentication does not introduce additional authentication traffic in the network.
- D. These are valid configuration commands and the switch accepts them.

Answer: D

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

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

Answer: D

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

- A. It drops ARP traffic unless it is permitted.
- B. It cannot pass multicast traffic.
- C. It supports ARP inspection.
- D. It requires the inside and outside interface to be in different subnets.
- E. It does not support NAT.
- F. It can pass IPv6 traffic.

Answer: CF

75. Which two ESMTTP commands are supported by the ASA inspection engine? (Choose two)

- A. ATRN
- B. ETRN
- C. VERB
- D. VERB
- E. ONEX
- F. SOML
- G. LINK

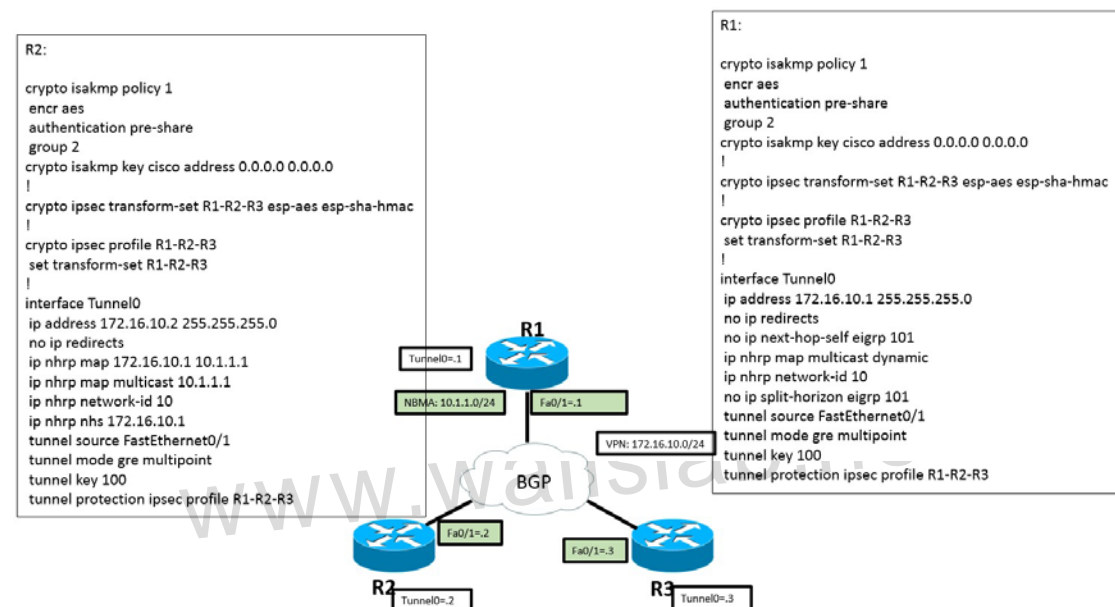
Answer: BF

76. What is the purpose of the BGP TTL security check?

- A. to use for iBGP session
- B. to check for a TTL value in packet header of less than or equal to for successful peering
- C. to protect against routing table corruption
- D. to authenticate a peer
- E. to protect against CPU utilization-based attacks

Answer: E

77.



Refer to the exhibit. Which statement about the exhibit is true?

- A. IPsec phase-2 will fail to negotiate due to a mismatch in parameters.
- B. A DMVPN session will fail to establish because R2 is missing the ISAKMP peer address.
- C. A DMVPN session will establish between R1 and R2
- D. IPsec phase-1 will fail to negotiate due to a mismatch in parameters
- E. The tunnel configuration is incomplete and the DMVPN session will fail between R1 and R2

Answer: C

注：没有错误，可以正常建立

78. Which two options describe the main purpose of EIGRP authentication? (Choose two)

- A. to identify authorized peers
- B. to prevent injection of incorrect routing information
- C. to provide routing updates confidentiality
- D. to provide redundancy
- E. to allow faster convergence

Answer: AB

79. Which ICMP message type code indicates that fragment reassembly time has been exceeded?
- A. Type 12, Code 2
 - B. Type 11, Code 1
 - C. Type 4, Code 0
 - D. Type 11, Code 0

Answer: B

80. Which two statements about PCI DSS are true? (Choose two)
- A. it is an IETF standard for companies to protect credit, debit, and ATM cardholder information.
 - B. it is a proprietary security that defines a framework for credit, debit, and ATM cardholder information.
 - C. it is a criminal act of cardholder information fraud.
 - D. it has as one of its objectives to restrict physical access to credit, debit, and ATM cardholder information.
 - E. it is a US government standard that defines ISP security compliance.

Answer: BD

81. When a client attempts to authenticate to an access point with the RADIUS server, the server returns the error message "Invalid message authenticator in EAP request". Which action can you take to correct the problem?
- A. Enable the external database account.
 - B. Add the user profile to ACS.
 - C. Configure the required privileges for the authentication service.
 - D. Synchronize the shared password between AP and ACS.

Answer: D

82.

%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=1

Refer to the exhibit, After setting the replay window size on your Cisco router, you received the given system message. What is the reason for the message?

- A. The replay window size is set too low for the number of packets received.
- B. The IPSec anti-replay feature is enabled, but the window size feature is disabled.
- C. The IPSec anti-reply feature is disabled.
- D. The replay window size is set too high for the number of packets received.

Answer: A

83. Which signature engine would you choose to filter for the regex `[aA][tT][tT][aA][cC][kK]` in the

URI field of the HTTP header?

- A. AIC HTTP
- B. ATOMIC IP
- C. service HTTP
- D. string TCP

Answer: C

84. What is Cisco CKM (Centralized Key Management) used for?

- A. to provide switch port security
- B. to allow an access point to act as a TACACS server to authenticate the client
- C. to avoid configuring PSKs (Pre-Shared Key) locally on network access devices and to configure a PSK once on a RADIUS server
- D. to allow authenticated client devices to roam from one access point to another without any perceptible delay during re-association

Answer: D

85. What are two limitations of the Atomic IP Advanced Engine? (Choose two)

- A. It is unable to fire high-severity alerts for known vulnerabilities.
- B. It is usable to detect IP address anomalies, including IP spoofing.
- C. It has limited ability to check the fragmentation header.
- D. It is unable to inspect a packet's length fields for bad information.
- E. It is unable to detect Layer 4 attacks if the packets were fragmented by IPv6.

Answer: CE

86. Which statement is true regarding the packet flow on Cisco ASA firewall version 8.2?

- A. For the packet that has been received on the ingress interface. ACL is only checked if the connection entry exists for the packet flow.
- B. For the packet that has been received on the ingress interface. ACL is only checked if the connection entry does not exist for the packet flow.
- C. For the packet that has been received on the ingress interface. translation rule is checked before the ACL if the connection entry for the packet flow does not exist.
- D. For the packet that has been received on the egress interface. translation rule is checked before the ACL if the connection entry does not exist for the packet flow.

Answer: B

87. your coworker is working on a project to prevent DDoS and ingress filtering and needs advice on the standard and associated process for a single-homed network. Which two options do you suggest? (Choose two)

- A. RFC 3704
- B. RFC 5735

- C. RFC 2827
- D. BCP 38
- E. BCP 84

Answer: CD

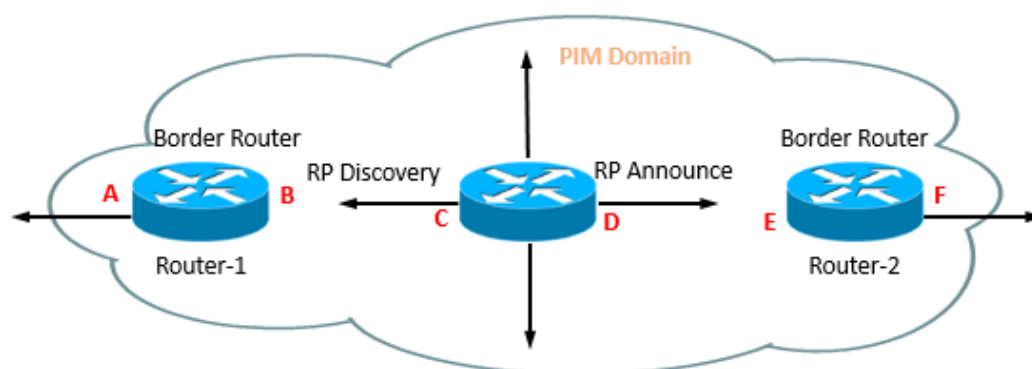
88. Which three fields are part of the AH header? (Choose three)

- A. Packet ICV
- B. Destination Address
- C. Source Address
- D. Protocol ID
- E. Next Header
- F. SPI identifying SA
- G. Application Port

Answer: AEF

www.wallslab.net

89.



Refer to the exhibit, In which two parts should the multicast boundary command be applied? (Choose two)

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

- E. E
- F. F

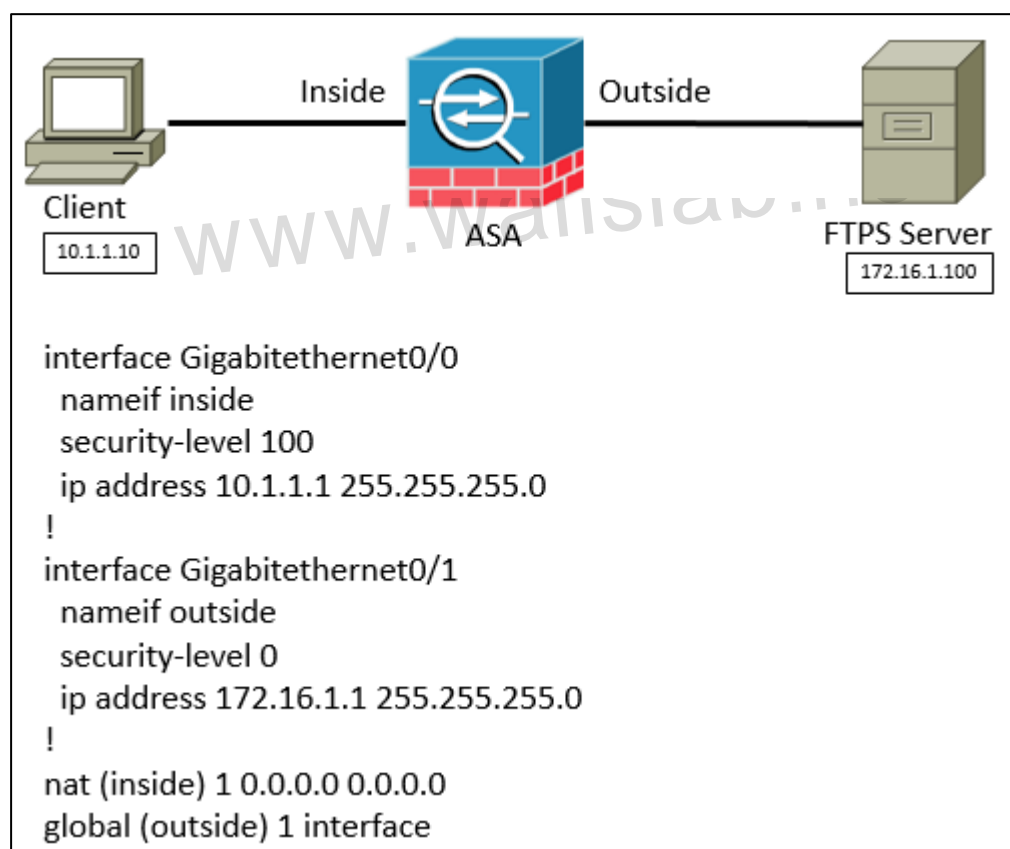
Answer: AF

90. Which three statements about Dynamic ARP Inspection on Cisco switches are true? (Choose three)

- A. Dynamic ARP inspection checks ARP packets on trusted and untrusted ports
- B. Dynamic ARP inspection checks ARP packets against the trusted database
- C. Dynamic ARP inspection is supported only on access ports
- D. Dynamic ARP inspection does not perform ingress security checking
- E. DHCP snooping is used to dynamically build the trusted database
- F. The trusted database can be manually configured using the CLI

Answer: BEF

91.



Refer to the exhibit. With the client attempting an implicit SFTP connection to the SFTP server, which mode works by default?

- A. passive
- B. active
- C. both passive and active
- D. neither passive nor active

Answer: A

92. For which router configuration is the attack-drop sdf file recommended?

- A. Routers with less than 128 MB of memory
- B. Routers with at least 256 MB of memory
- C. Routers with at least 128 MB of memory
- D. Routers with at least 192 MB of memory
- E. Routers with less than 64 MB of memory

Answer: A

93. Which statement about the Firewalk attack is true?

- A. It uses ICMP sweep to find expected hosts behind a firewall.
- B. It uses ICMP sweep with a predetermined TTL value to discover hosts behind a firewall.
- C. It is used to discover hosts behind a firewall device.
- D. It is used to find the vulnerability in the Cisco IOS firewall code.
- E. It uses TTL handling to determine whether packets can pass through a packet-filtering device.

Answer: B

94.

```
switchport mode access
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator spanning-
tree portfast
```

Refer to the exhibit. Which option describes the behavior of this configuration?

- A. IEEE 802.1x devices must first authenticate via MAB to perform subsequent IEEE 802.1X authentication. If 802.1X fails, the device is assigned to the default guest VLAN.
- B. The switch initiates the authentication.
- C. The device performs subsequent IEEE 802.1X authentication if it passed MAB authentication. If the device fails IEEE 802.1X, it will start MAB again.
- D. Devices that perform IEEE 802.1X should be in the MAC address database for successful authentication.

Answer: C

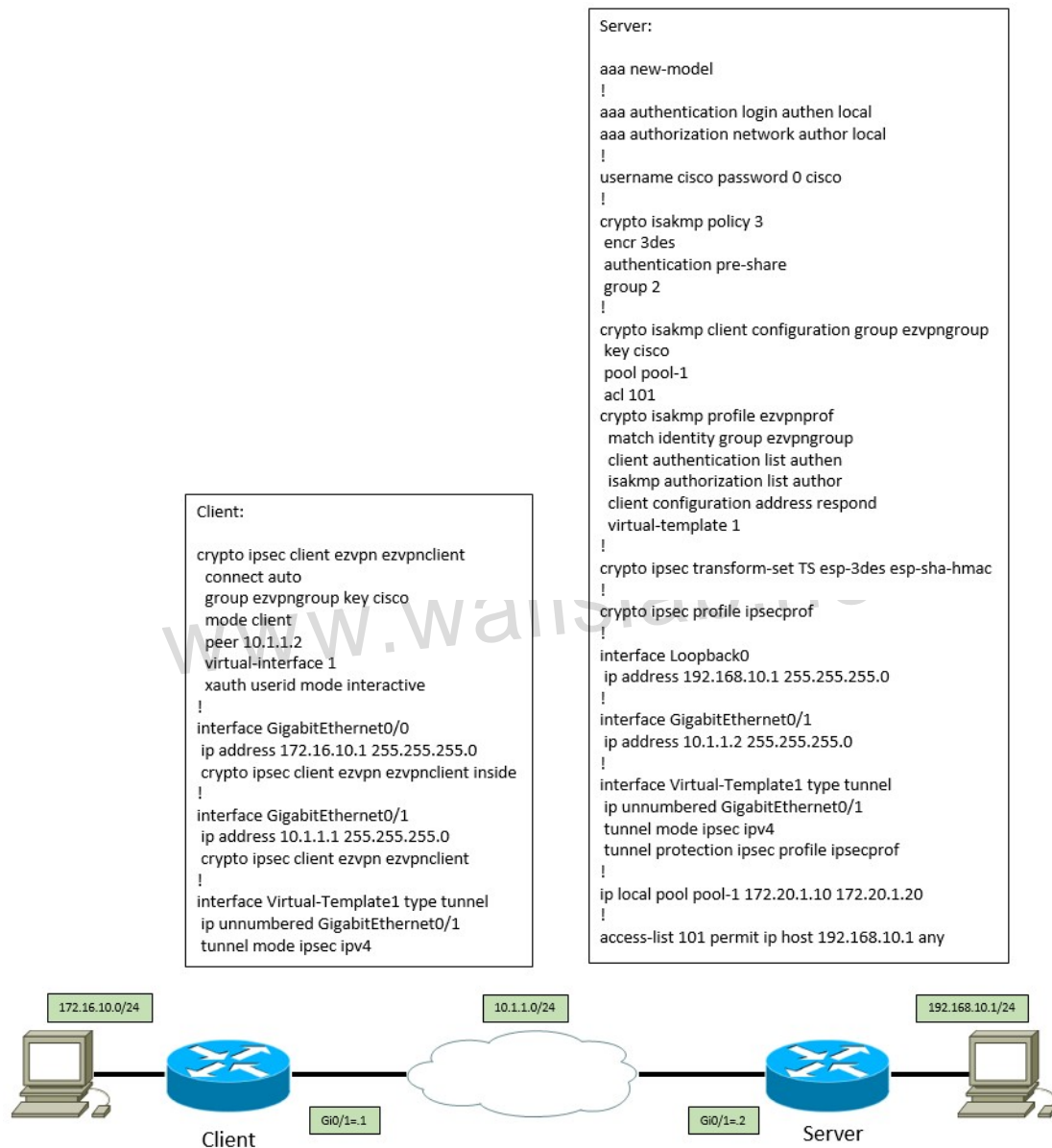
95. Which two statements about NEAT are true? (Choose two)

- A. NEAT is not supported on an EtherChannel port.
- B. NEAT should be deployed only with autoconfiguration.

- C. NEAT is supported on an EtherChannel port.
- D. NEAT supports standard ACLs on the switch port.
- E. NEAT uses CISP (Client Information Signalling Protocol) to propagate client IP address.

Answer: AB

96.



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

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

Answer: A

注：错点在

```
Server:
aaa new-model
!
aaa authentication login authen local
aaa authorization network author local
!
username cisco password 0 cisco
!
crypto isakmp policy 3
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp client configuration group ezvpngroup
  key cisco
  pool pool-1
  acl 101
crypto isakmp profile ezvpnprof
  match identity group ezvpngroup
  client authentication list authen
  isakmp authorization list author
  client configuration address respond
  virtual-template 1
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile ipsecprof
! 缺set transform-set TS
```

97. What are two authentication algorithms supported with SNMPv3 on an ASA? (Choose two)

- A. RC5
- B. DES
- C. RC4
- D. MD5
- E. 3DES
- F. SHA

Answer: DF

98. Which statement about SOX is true?

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

Answer: C

99.

```
%BGP-4-MAXPFX: No. of prefix received from 101.0.0.1 (afi 0) reaches 351, max 500
%BGP-3-MAXPFXEXCEED: No. of prefix received from 101.0.0.1 (afi 0): 501 exceed limit 500
%BGP-5-ADJCHANGE: neighbor 101.0.0.1 Down BGP Notification sent
```

Refer to the exhibit. Which command caused the above messages?

- A. neighbor 101.0.0.1 maximum-prefix 500 90
- B. neighbor 101.0.0.1 maximum-prefix 500 80 warning-only
- C. neighbor 101.0.0.1 maximum-prefix 500 70 warning-only
- D. neighbor 101.0.0.1 maximum-prefix 500 70

Answer: D

100. What is the unit of measurement of the average rate of a token bucket?

- A. kilobits per second
- B. bytes per second
- C. bits per second
- D. kilobytes per second

Answer: C

www.wallslab.net