Pass
WRITTEN

# CCNA Security Written

## 210-260

1.You are configuring an IPS that must be able to react to a potential attack.
Which deployment method do you use?
A. passive deployment that uses tap mode
B. transparent inline mode
C. inline deployment that uses a SPAN
D. passive deployment that uses failsafe
**Answer:** B

2.What is the best definition of hairpinning?
A. traffic that enters and exits a device through the same interface
B. traffic that tunnels through a device interface
C. traffic that enters one interface on a device and that exits through another interface
D. ingress traffic that traverses the outbound interface on a device
**Answer:** A

3.Which command do you enter to verify the phase 1 status of a VPN connection?
A. sh crypto ipsec sa
B. sh crypto isakmp sa
C. sh crypto session
D. debug crypto isakmp
**Answer:** B

4.Which two statements about hardware-based encryption are true? (Choose two)
A. It is potentially easier to compromise than software-based encryption
B. It can be implemented without impacting performance
C. It is highly cost-effective
D. It requires minimal configuration
E. It is widely accessible
**Answer:** BC

5.Which mitigation technology for web-based threats prevents the removal of confidential data from the network?
A. CTA
B. AMP
C. DLP
D. DCA
**Answer:** C

6.Which two types of malware can self-replicate and spread? (Choose two)
A. bots
B. backdoors
C. Trojans
D. worms

E. viruses
**Answer:** CD

7.How is management traffic isolated on a Cisco ASR 1002?
A. Traffic is isolated based upon how you configure routing on the device
B. The management interface is configured in a special VRF that provides traffic isolation from the default routing table
C. Traffic isolation is done on the VLAN level
D. There is no management traffic isolation on a Cisco ASR 1002.
**Answer:** B

8.Which option is the logical container used to maintain information about the connections going through a Cisco ASA firewall?
A. estate table
B. NAI table
C. Cisco Express Forwarding table
D. routing table
**Answer:** A

9.In which two modes can the Cisco Web Security Appliance be deployed? (Choose two)
A. as a transparent proxy using the Secure Sockets Layer protocol
B. as a transparent proxy using the Hyper Text Transfer Protocol
C. explicit proxy mode
D. as a transparent proxy using the Web Cache Communication Protocol
E. explicit active mode
**Answer:** CD

10.Which SNMPv3 security level provides authentication using HMAC with MD5, but does not use encryption?
A. authNoPriv
B. NoauthPriv
C. authPriv
D. noAuthNoPriv
**Answer:** A

11.What are two default behaviors of the traffic on a zone-based firewall? (Choose two)
A. Traffic within the self zone uses an implicit deny all
B. All traffic between zones is implicitly blocked:
C. Communication is allowed between interfaces that are members of the same zone
D. The CBAC rules that are configured on router interfaces apply to zone interfaces
E. Communication is blocked between interfaces that are members of the same zone
**Answer:** BC

12.Which three descriptions of RADIUS are true? (Choose three)

A. It combines authentication and authorization
B. It separates authentication, authorization, and accounting.
C. It uses UDP as its transport protocol.
D. Only the password is encrypted
E. It uses TCP as its transport protocol
F. It supports multiple transport protocols
**Answer:** ACD

13.Which four tunneling protocols are enabled in the DfitGrpPolicy group policy? (Choose four)
A. Clientless SSL VPN
B. SSL VPN Client
C. PPPTP
D. L2TP/IPsec
E. IPsec IKEv1
F. IPsec IKEv2
**Answer:** ADEF

14.WhenuserslogintotheClientlessSslvpnusinghttps://209.165.201.2/est, which group policy will be applied?
A. test
B. clientless
C. Sales
D. DfitGrpPolicy
E. DefaultRAGroup
F. DefaultwEBVPNGroup
**Answer:** C

15.Which user authentication method is used when users login to the Clientless SSLVPN portal usinghttps:1/209.165.201.2/test?
A. AAA with LOCAL database
B. AAA with RADIUS server
C. Certificate
D. Both Certificate and AAA with LOCAL database
E. Both Certificate and AAA with RADIUS server
**Answer:** A

16.Which two statements regarding the ASA VPN configurations are correct? (Choose two)
A. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_TrustPoint1
B. The DefaultwEBVPNGroup Connection Profile is using the AAA with RADIUS server method
C. MtheInsidesrvbookmarkreferenceshttps://10.2.1.1 URL
D. Only Clientless SSL VPN access is allowed with the Sales group policy
E. AnyConnect, IPSec IKEv1, and IPSec IKEV2 VPN access is enabled on the outside interface
F. The Inside-SRV bookmark has not been applied to the Sales group policy

**Answer:** BC

17.What is the maximum number of methods that a single method list can contain?
A. 4
B. 3
C. 2
D. 5
**Answer:** D

18.Which attack involves large numbers of ICMP packets with a spoofed source IP address?
A. Teardrop attack
B. SYN Flood attack
C. Nuke attack
D. smurf attack
**Answer:** D

19.Which two models of ASA tend to be used in a data center? (Choose two)
A. 5555X
B. ASA service module
C. 5520
D. 5585X
E. 5540
F. 5512X
**Answer:** BD

20.What are two major considerations when choosing between a SPAN and a TAP when implementing IPS? (Choose two)
A. the type of analysis the IPS will perform
B. the amount of bandwidth available
C. Whether RX and TX signals will use separate ports
D. the way in which media errors will be handled
E. the which dropped packets will be handled
**Answer:** C

21.When connecting to an external resource, you must change a source IP address to use one IP address from a range of 207.165.201.1 to 207.165.201.30.
Which option do you implement?
A. static destination NAT that uses a subnet as a real source
B. static destination NAT that uses a subnet as a real destination
C. dynamic source NAT that uses a range as a mapped source
D. dynamic source NAT that uses an IP address as a mapped source
**Answer:** C

22.What is the minimum Cisco los version that supports zone-based firewalls?

A. 12.1
B. 12.4(6)T
C. 15.1
D. 15.0
**Answer:** B

23.Of all the parameters that are negotiated for the IKE Phase 1 tunnel, which parameter is the only one that does not have to exactly match between VPN pees to be accepted?
A. Digital signature
B. Lifetime
C. Hashing algorithm
D. DH group
E. Encryption algorithm
F. Authentication method
**Answer:** C

24.What is the range of levels provided by the Privilege command?
A. 0-14
B. 1-14
C. 1-16
D. 0-15
E. 0-16
F. 1-15
**Answer:** D

25.Which term is most closely aligned with the basic purpose of a SIEM solution?
A. Repudiation
B. Non-Repudiation
C. Accountability
D. Causality
**Answer:** C

26.Which 802.1x component enforces the network access policy?
A. authentication server
B. RADIUS server
C. Authenticator
D. supplicant
**Answer:** C

27.How can you mitigate DCE/RPC evasion techniques while allowing access to the DCE/RPC service?
A. Configure the DCE/RPC preprocessor
B. Update the IPS signature for HT TPS to validate DCE/RPC connections
C. Block suspicious hosts from DCE/RPC port 593
D. Tunnel DCE/RPC traffic through GRE

**Answer:** C

28.What does the policy map do in CoPP?
A. defines service parameters
B. defines packet selection parameters
C. defines the packet filter
D. defines the action to be performed
**Answer:** D

29.Which two advantages does the on-premise model for MDM deployment have over the cloud-based model? (Choose two)
A. The on premise model generally has less latency than the cloud-based model
B. The on premise model provides more control of the MDM solution than the cloud based model
C. The on-premise model is generally less expensive than the cloud based model
D. The on- premise model is more scalable than the cloud based model
E. The on-premise model is easier and faster to deploy than the cloud based model.
**Answer:** AB

30.Which action does standard antivirus software perform as part of the file-analysis process?
A. flag the unexamined file as a potential threat
B. examine the execution instructions in the file
C. create a backup copy of the file
D. execute the file in a simulated environment to examine its behavior
**Answer:** B

31.Which information can you display by executing the show crypto IPSec sa command?
A. recent changes to the IP address of a peer router
B. proxy information for the connection between two peers
C. IPsec SAs established between two peers
D. ISAKMP SAs that are established between two peers
**Answer:** C

32.Which type of firewall can perform deep packet inspection?
A. application firewall
B. personal firewall
C. packet-filtering firewall
D. stateless firewall
**Answer:** A

33.You have implemented a dynamic blacklist, using security intelligence to block illicit network activity. However, the blacklist contains several approved connections that users must access for business purposes.
Which action can you take to retain the blacklist while allowing users to a approved sites?
A. Disable the dynamic blacklist and create a static backlist in its place.

B. Edit the dynamic blacklist to remove the approved addresses.
C. Create a whitelist and manually add the approved addresses
D. Disable the dynamic blacklist and deny the specific address on a whitelist while permitting the others
**Answer:** C

34.Which type of social engineering attack targets top executives?
A. vishing
B. baiting
C. whaling
D. spear phishing
**Answer:** C

35.Which two configurations can prevent VLAN hopping attack from attackers at VLAN 10? (Choose two)
A. using switchport nonegotiate command on dynamic desirable ports
B. using switchport mode access command on all host ports
C. applying ACL between VLANS
D. creating VLAN 99 and using switchport trunk native vlan 99 command on trunk ports
E. using switchport trunk native vlan 10 command on trunk ports
F. enabling BPDU guard on all access ports
**Answer:** BD

36.Which IPS detection method examines network traffic for preconfigured patterns?
A. honey- pot detection
B. anomaly based detection
C. signature based detection
D. policy-based detection
**Answer:** C

37.Which two statements about STP attacks are true? (Choose two)
A. The attacker sends BPDU messages to become the root bridge
B. The attacker sets up a rogue DHCP server to intercept requests
C. They can be performed only when Cisco Discovery Protocol is running
D. They can be mitigated by disabling STP
E. They can be executed only from a hub.
F. They can create the opportunity for subsequent man-in-the-middle attacks
**Answer:** AF

38.Which statement about TACACS+ is true?
A. TACACS+ is used for user access to network resources more than administrative access to network devices
B. All data that is transmitted between the client and TACACS+ server is cleartext
C. TACACS+ is more flexible than RADIUS because it separates all AAA into individual processes
D. Passwords are transmitted between the client and server using MD5 hashing
E. TACACS+ server listens UDP port 1813 for accounting.

**Answer:** C

39.Which type of mechanism does Cisco FirePOWER deploy to protect against email threats that are detected moving across other networks?
A. signature-based
B. antivirus scanning
C. policy-based
D. reputation based
**Answer:** D

40.In a Cisco Cloud Web Security environment, when can network traffic bypass the scanning proxies?
A. when the client is connected to a WPA2 Enterprise network
B. when the client is connected to a VPN service that bypasses proxies
C. when the client is on a trusted corporate network
D. when the client is connected to a wired network
**Answer:** C

41.What action must you take on the ISE to blacklist a wired device?
A. Revoke the device's certificate so it is unable to authenticate to the network
B. Add the device's MAC address to a list of blacklisted devices.
C. Issue a CoA request for the device's MAC address to each access switch in the network
D. Locate the switch through which the device is connected and push an ACL restricting all access by the device.
**Answer:** B

42.What is the main purpose of Control Plane Policing?
A. to prevent exhaustion of route -processor resources
B. to organize the egress packet queues
C. to define traffic classes
D. to maintain the policy map
**Answer:** A

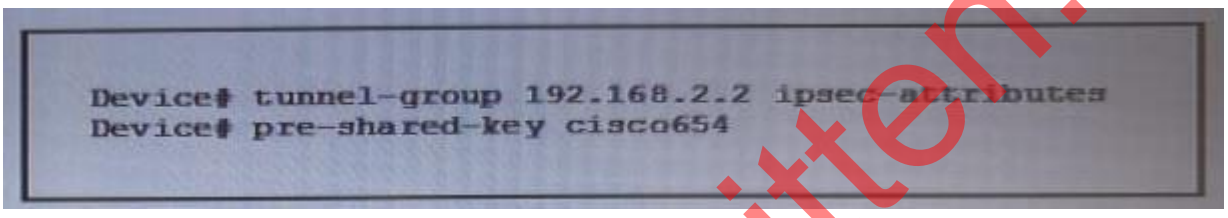
43.How does the 802.1x supplicant communicate with the authentication server?
A. The supplicant creates RADIUS packets and sends them to the authenticator, which encapsulates them into EAP and forwards them to the authentication server
B. The supplicant creates EAP packets and sends them to the authenticator, which translates them into RADIUS and forwards them to the authentication server
C. The supplicant creates EAP packets and sends them to the authenticator, which encapsulates them into RADIUS and forwards them to the
D. The supplicant creates RADIUS packets and sends them to the authenticator, which translates them into EAP and forwards them to the
**Answer:** B

44.Which statement about the native VLAN is true?

A. It is most secure when it is assigned to VLAN 1.
B. It is the Cisco recommended VLAN for switch-management traffic
C. It is susceptible to VLAN hopping attacks
D. It is the Cisco-recommended VLAN for user traffic
**Answer:** C

45.Which term refers to the electromagnetic interference that can radiate from network cables?
A. multimode distortion
B. Gaussian distributions
C. Doppler waves
D. emanations
**Answer:** D

46.Refer to the exhibit.




What is the effect of the given configuration?
A. It establishes the preshared key for the firewall
B. It establishes the preshared key for the router.
C. It establishes the preshared key for the switch.
D. It establishes the preshared key for the Cisco ISE appliance
**Answer:** A

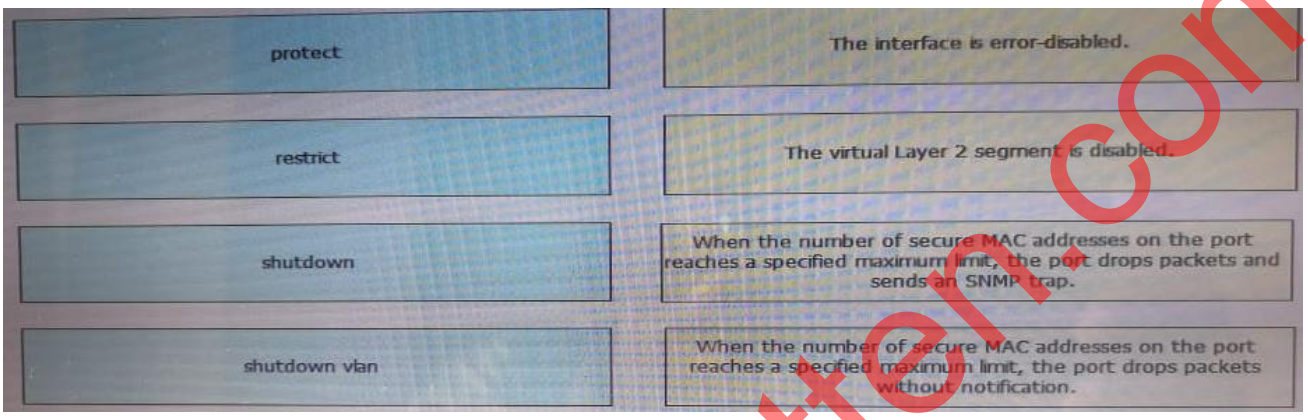
47.Which path do you follow to enable AAA through the SDM?
A. Configure Additional Authentication> AAA
B. Configure AAA
C. Configure-Additional Tasks >AAA
D. Configure =Tasks=AAA
E. Configure Authentication >AAA
**Answer:** C

48.You have just deployed SNMPv3 in your environment. Your manager asks you to make sure that your SNMP agents can only talk to the SNMP Manager.
What would you configure on your SNMP agents to satisfy this request?
A. A SNMP Group containing the SNMP managers
B. Routing Filter with the SNMP managers in it applied outbound
C. A SNMP View containing the SNMP managers
D. A standard ACL containing the SNMP managers applied to the SNMP configuration
**Answer:** A

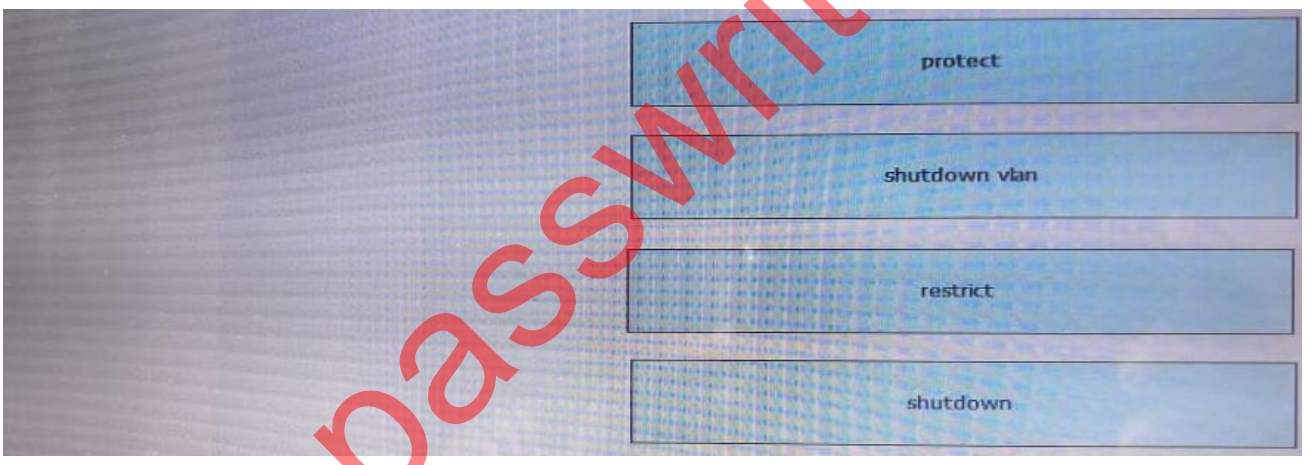
49.Which next generation encryption algorithm supports four variants?

A. SHA-2
B. MD5
C. HMAC
D. SHA-1
**Answer:** A

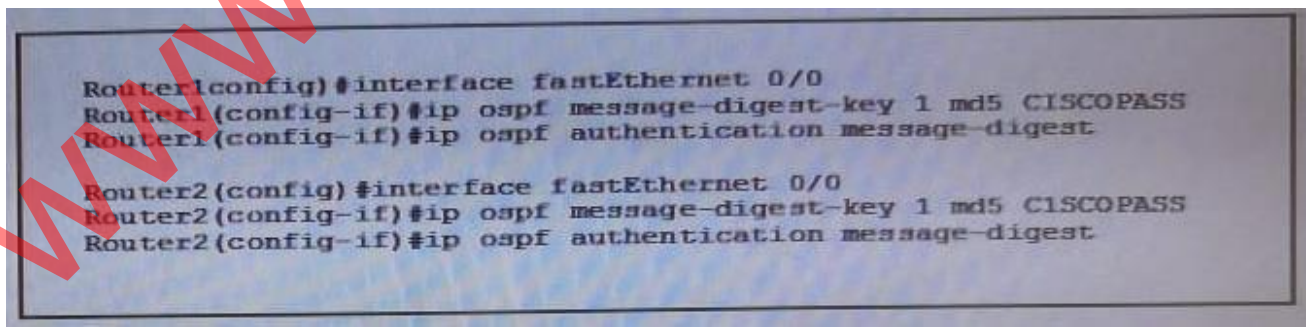
50.Drag and drop each port security violation mode from the left onto the corresponding action on the right




**Answer:**




51.Refer to the exhibit.




What is the effect of the given configuration?
A. It prevents keychain authentication
B. It enables authentication
C. The two devices are able to pass the message digest to one another

D. The two routers receive normal updates from one another
**Answer:** B

52.What does the DH group refer to?
A. length of key for hashing
B. length of key for authentication
C. length of key for encryption
D. tunnel lifetime key
E. Length of key for key exchange
**Answer:** E

53.In which type of attack does an attacker overwrite an entry in the CAM table to divert traffic destined to a legitimate host?
A. ARP spoofing
B. DHCP spoofing
C. MAC spoofing
D. CAM table overflow
**Answer:** C

54.What are two features of transparent firewall mode? (Choose two)
A. It allows some traffic that is blocked in routed mode
B. It enables the ASA to perform as a router
C. It conceals the presence of the firewall from attackers
D. It is configured by default
E. It acts as a routed hop in the network
**Answer:** AC

55.You are configuring a site to- site tunnel between two Cisco routers by using IPsec.
Which option do you set to specify the peer to which you want to connect?
A. IP address of a tunnel destination
B. tunnel group that has a peer IP address
C. IP address as part of the ISAKMP configuration
D. IP address by using a crypto map
**Answer:** D

56.Which statement about interface and global access rules is true?
A. Interface access rules are processed before global access rules
B. The implicit allow is processed after both the global and interface access rules
C. Global access rules apply only to outbound traffic, but interface access rules can be applied in either direction
D. If an interface access rule is applied, the global access rule is ignored.
**Answer:** A

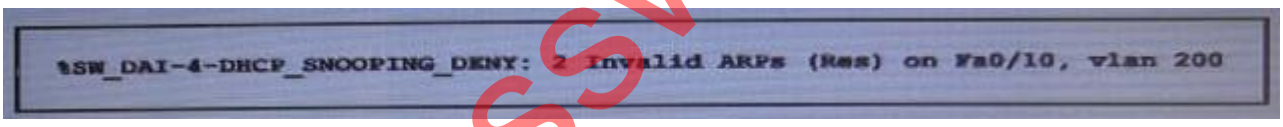
57.What aims to remove the ability to deny an action?

A. Non-Repudiation
B. Integrity
C. Deniability
D. Accountability
**Answer:** A

58.On which operating system does the Cisco mail Security Appliance run?
A. Crisco IOS XE
B. Crisco NX-OS
C. Cisco ESA-OS
D. Cisco AsyncOS
E. Cisco IOS XR
**Answer:** D

59.What are two advanced features of the Cisco AMP solution for endpoints? (Choose two)
A. reputation
B. foresight
C. reflection
D. contemplation
E. sandboxing
**Answer:** AE

60.Refer to the exhibit.




You notice this error message in the syslog.
Which command do you enter on the switch to gather more information?
A. show ip dhcp snooping binding
B. show ip source binding
C. show ip arp
D. show mac address-table
**Answer:** A

61.Which security term refers to the likelihood that a weakness will be exploited to cause damage to an asset?
A. threat
B. countermeasure
C. risk
D. vulnerability
**Answer:** C

62.There are two versions of IKE: IKEv1 and IKEv2 Both IKEv1 and IKEv2 protocols operate in phases. IKEv1 operates in two phases. IKEv2 operates in how many phases?

A. 2
B. 3
C. 4
D. 5
**Answer:** A

63.How can you prevent NAT rules from sending traffic to incorrect interfaces?
A. Assign the output interface in the NAT statement.
B. Use packet-tracer rules to reroute misrouted NAT entries.
C. Add the no-proxy-arp command to the nat line
D. Configure twice NAT instead of object NAT
**Answer:** C

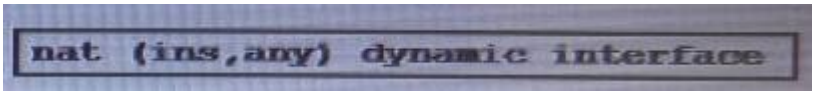
64.Which attack can be prevented by OSPF authentication?
A. IP spoofing attack
B. denial of service attack
C. smurf attack
D. buffer overflow attack
**Answer:** A

65.Which component of a security zone firewall policy defines how traffic is handled?
A. service policy
B. ACL
C. class map
D. policy map
**Answer:** D

66.Which two statements about an IPS in tap mode are true? (Choose two)
A. It can analyze intrusion events without impacting network efficiency
B. It directly analyzes the actual packets as they pass through the system
C. It requires an asynchronous routing configuration for full traffic analysis
D. The device forwards all traffic regardless of its source or destination
E. It is unable to drop packets in the main flow
**Answer:** AE

67.When you edit an IPS subsignature, what is the effect on the parent signature and the family of subsignatures?
A. Other signatures are unaffected, the change applies only to the subsignature that you edit
B. The change applies only to subsignatures that are numbered sequentially after the subsignature that you edit
C. The change applies to the parent signature and the entire family of subsignatures
D. The change applies to the parent signature and the subsignature that you edit
**Answer:** A

68.Refer to the exhibit.

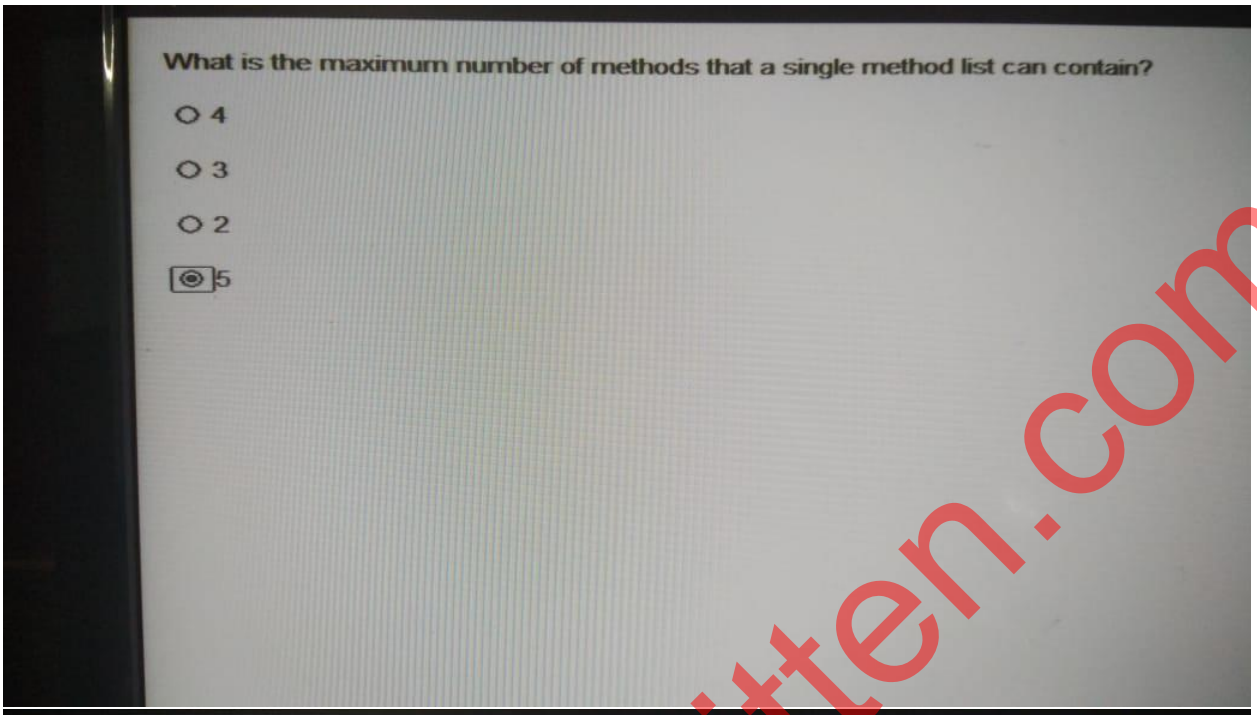


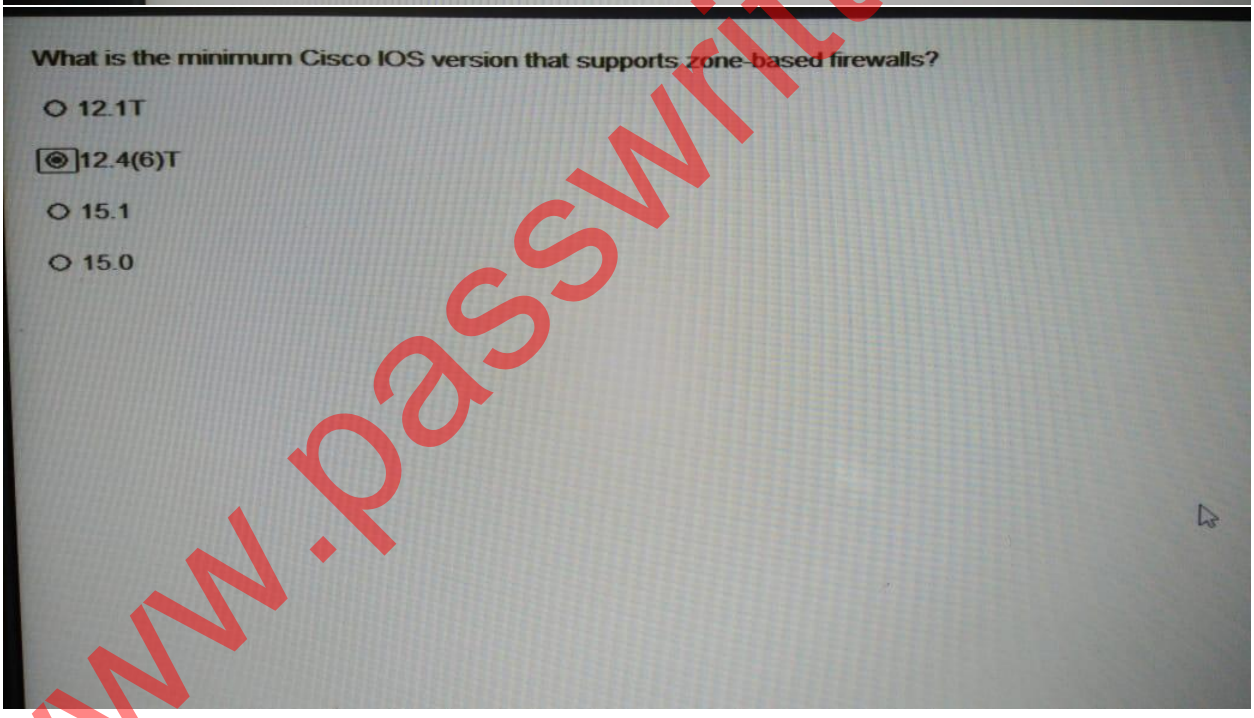

Which type of NAT is configured on a Cisco ASA?
A. source identity NAT
B. identity twice NAT
C. dynamic PAT
D. dynamic NAT
**Answer:** C

69.Which effect of the secure boot-image command is true?
A. It displays the status of the bootset.
B. It archives a secure copy of the IOS image
C. It configures the device to boot to the secure IOS image.
D. It archives a secure copy of the device configuration.
**Answer:** B

70.How will a stateful firewall handle an inbound packet that it receives and cannot match in its state table?
A. Drops the traffic
B. looks for an ACL, and acts based upon the ACL
C. passes the traffic
D. broadcasts the traffic
**Answer:** A

your preparation for the exam is done just read and go through questions below
If you found any question repeated then skip that question ok
mostly questions are repeated , some are new in it prepare those new questions simple



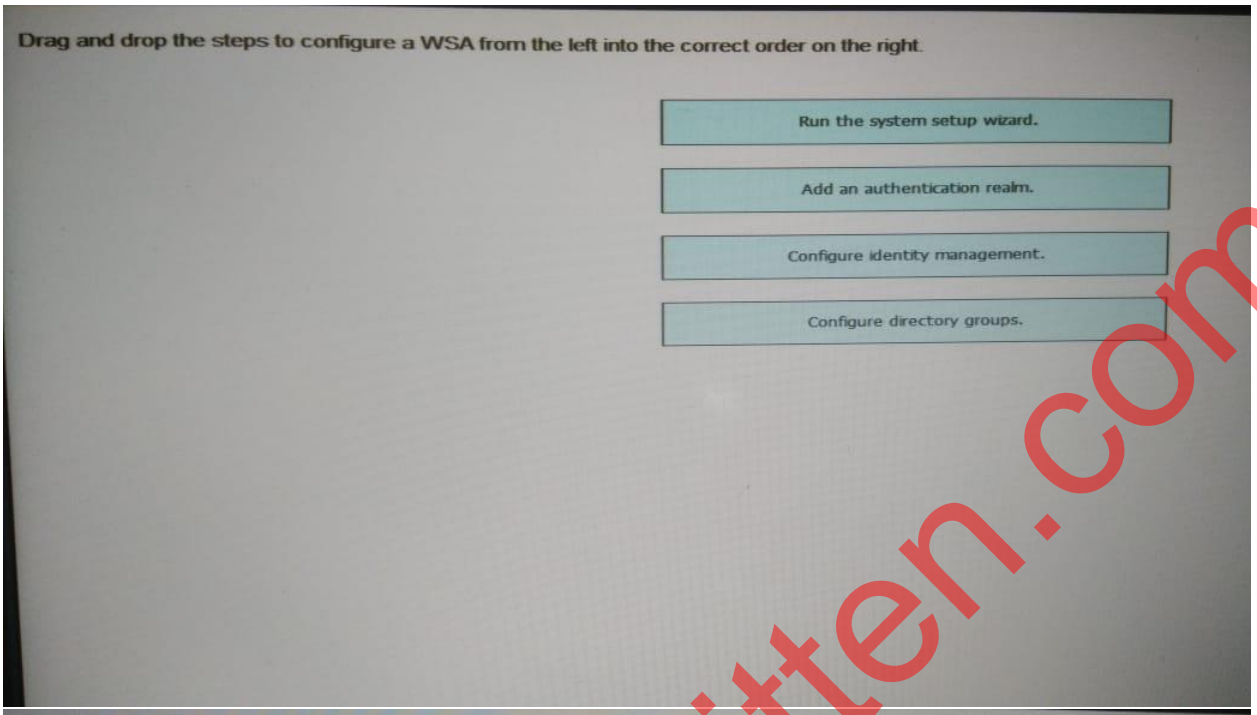



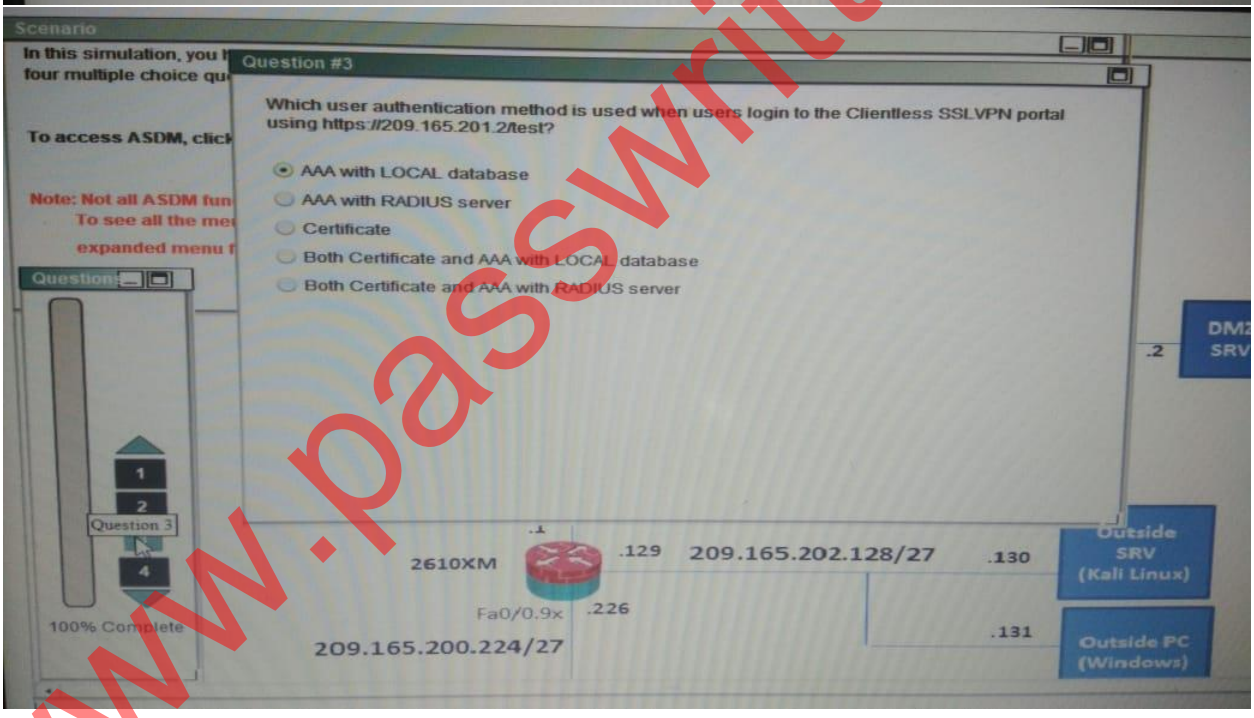
What is a limitation of network-based IPS?

- It must be individually configured to support every operating system on the network.
- It is most effective at the individual host level.
- [x] Large installations require numerous sensors to fully protect the network.
- It is unable to monitor attacks across the entire network.

What is the best definition of hairpinning?

- traffic that enters one interface on a device and that exits through another interface
- [x] traffic that enters and exits a device through the same interface
- ingress traffic that traverses the outbound interface on a device
- traffic that tunnels through a device interface



In which type of attack does an attacker overwrite an entry in the CAM table to divert traffic destined to a legitimate host?

- ARP spoofing
- MAC spoofing
- CAM table overflow
- DHCP spoofing

Which path do you follow to enable AAA through the SDM?

- Configure > Additional Authentication > AAA
- Configure > Additional Tasks > AAA
- Configure > Tasks > AAA
- Configure > AAA
- Configure > Authentication > AAA

What is the main purpose of Control Plane Policing?

- [x] to prevent exhaustion of route-processor resources
- [ ] to organize the egress packet queues
- [ ] to define traffic classes
- [ ] to maintain the policy map

What does the policy map do in CoPP?

- [ ] defines service parameters
- [ ] defines packet selection parameters
- [x] defines the action to be performed
- [ ] defines the packet filter

When would you configure the **ip dhcp snooping trust** command on a switch?

- when the switch is working in an edge capacity
- when the switch is connected to a client system
- [x] when the switch is connected to a DHCP server
- when the switch is serving as an aggregator

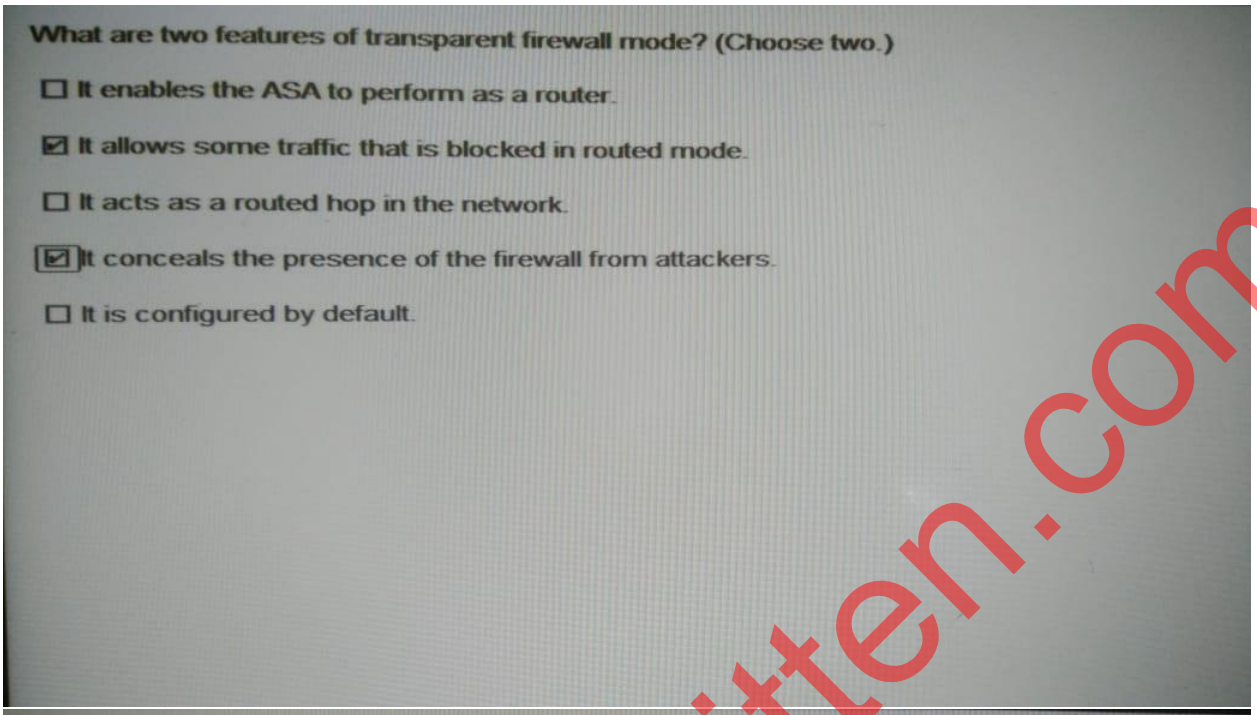
Drag and drop each feature that can protect against DHCP attacks from the left onto the correct description on the right.

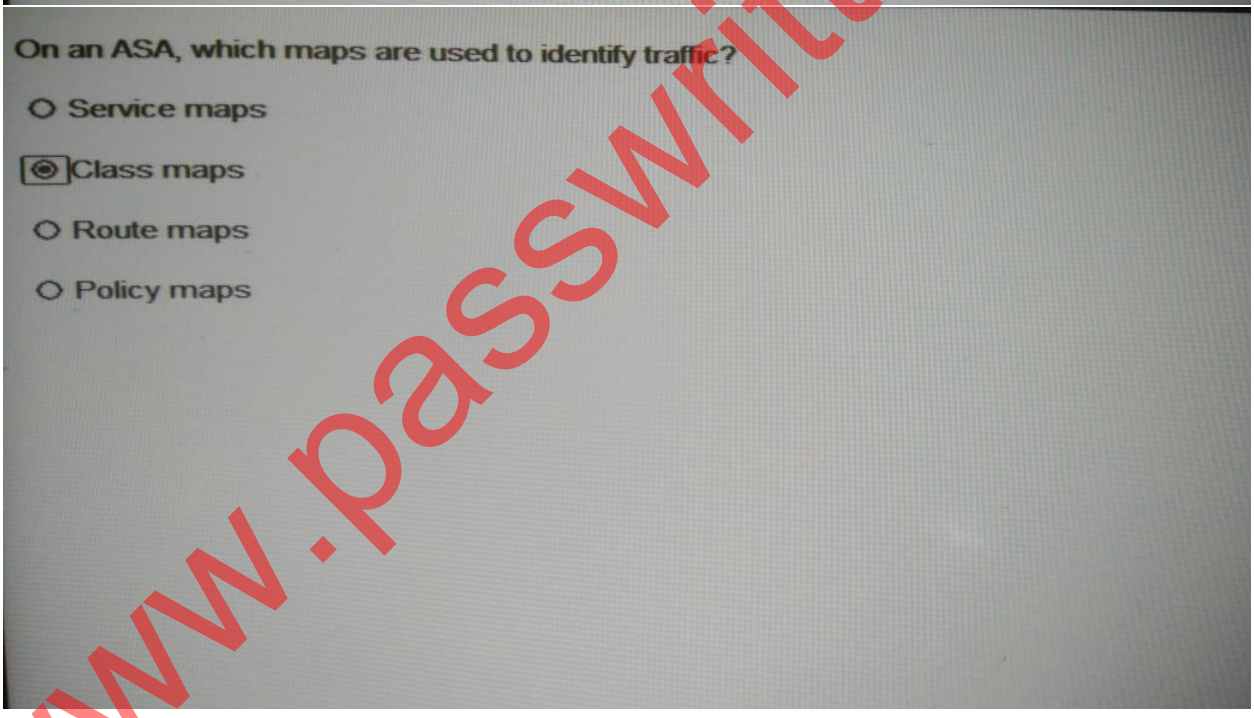
DHCP snooping

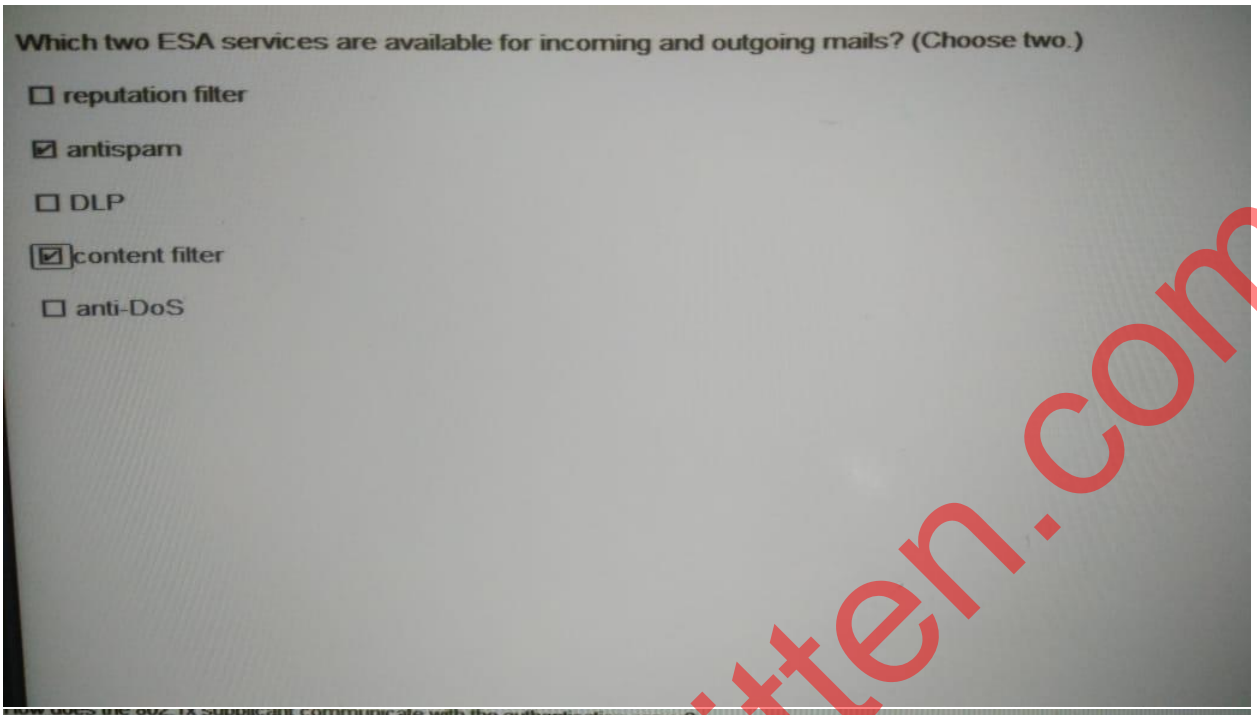
dynamic ARP inspection

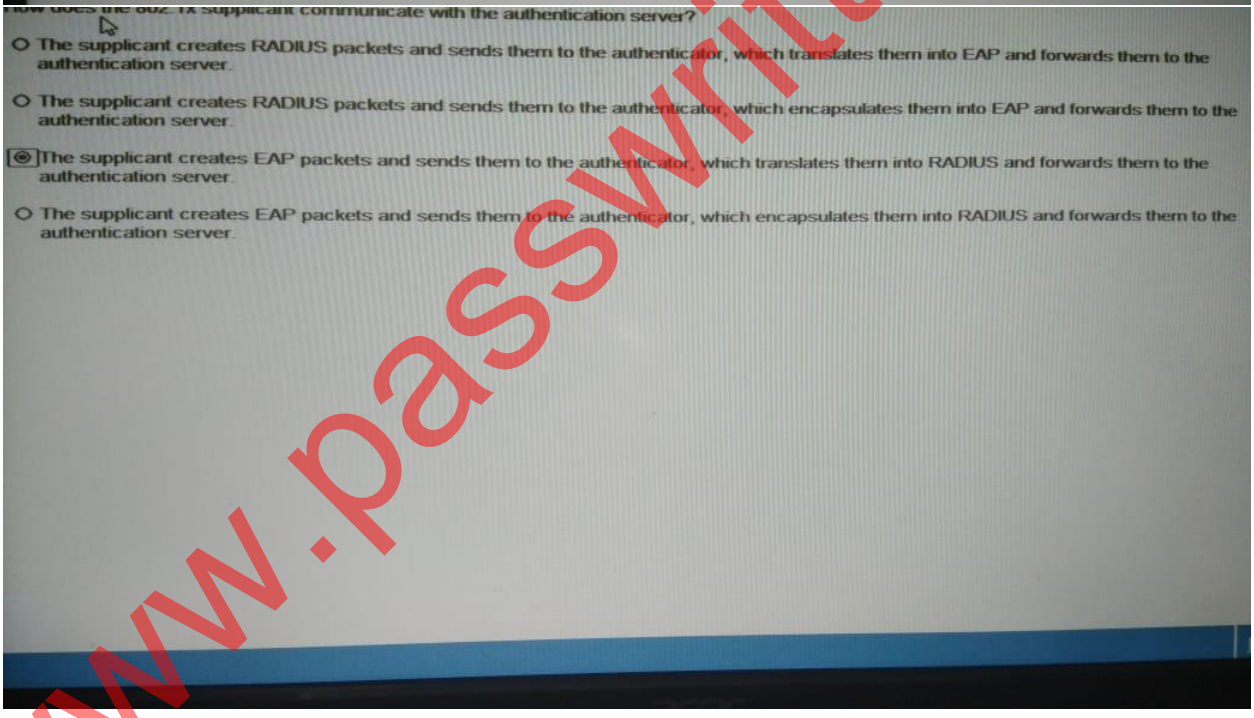
port security

IP source guard





Which statement about interface and global access rules is true?

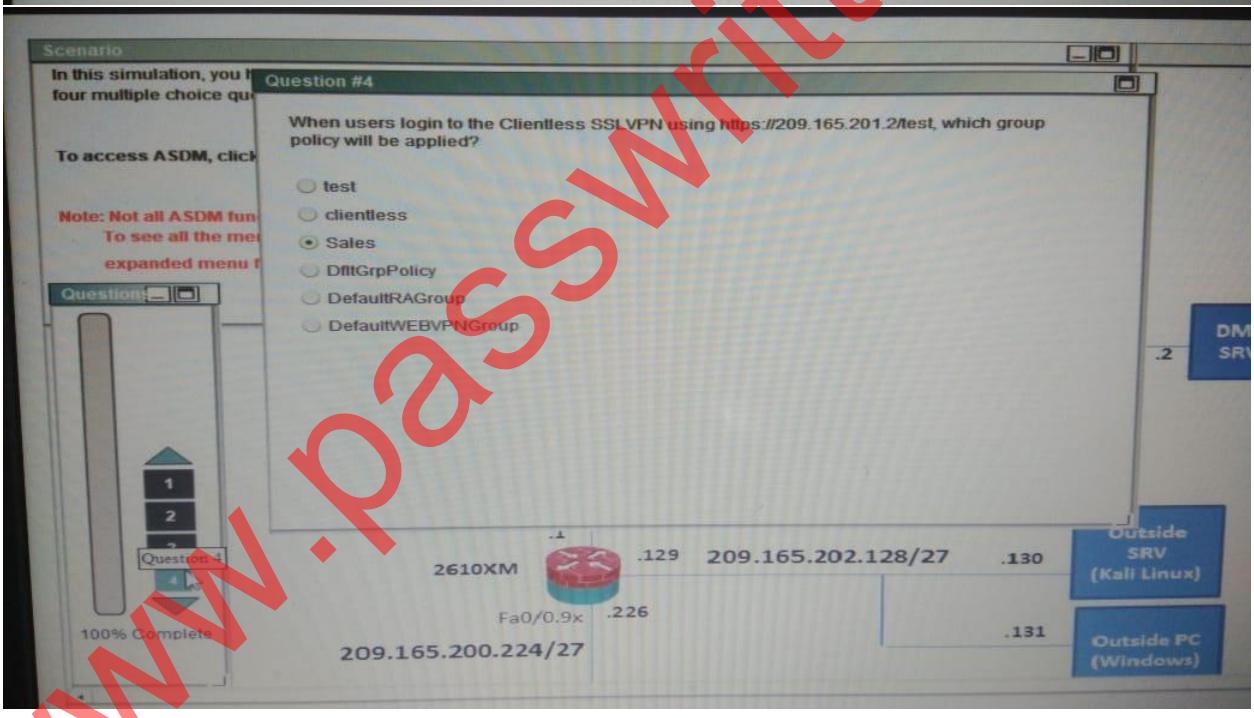
- (●) Interface access rules are processed before global access rules.
- ( ) If an interface access rule is applied, the global access rule is ignored.
- ( ) The implicit allow is processed after both the global and interface access rules.
- ( ) Global access rules apply only to outbound traffic, but interface access rules can be applied in either direction.

Which two models of ASA tend to be used in a data center? (Choose two.)

- [ ] 5520
- [x] ASA service module
- [ ] 5555X
- [ ] 5540
- [x] 5585X
- [ ] 5512X

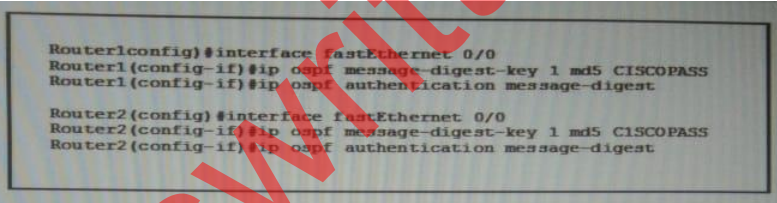
Which three descriptions of RADIUS are true? (Choose three.)

- ☐ It supports multiple transport protocols.
- ☑ It combines authentication and authorization.
- ☐ It separates authentication, authorization, and accounting.
- ☐ It uses TCP as its transport protocol.
- ☑ Only the password is encrypted.
- ☑ It uses UDP as its transport protocol.



Which term refers to the electromagnetic interference that can radiate from network cables?

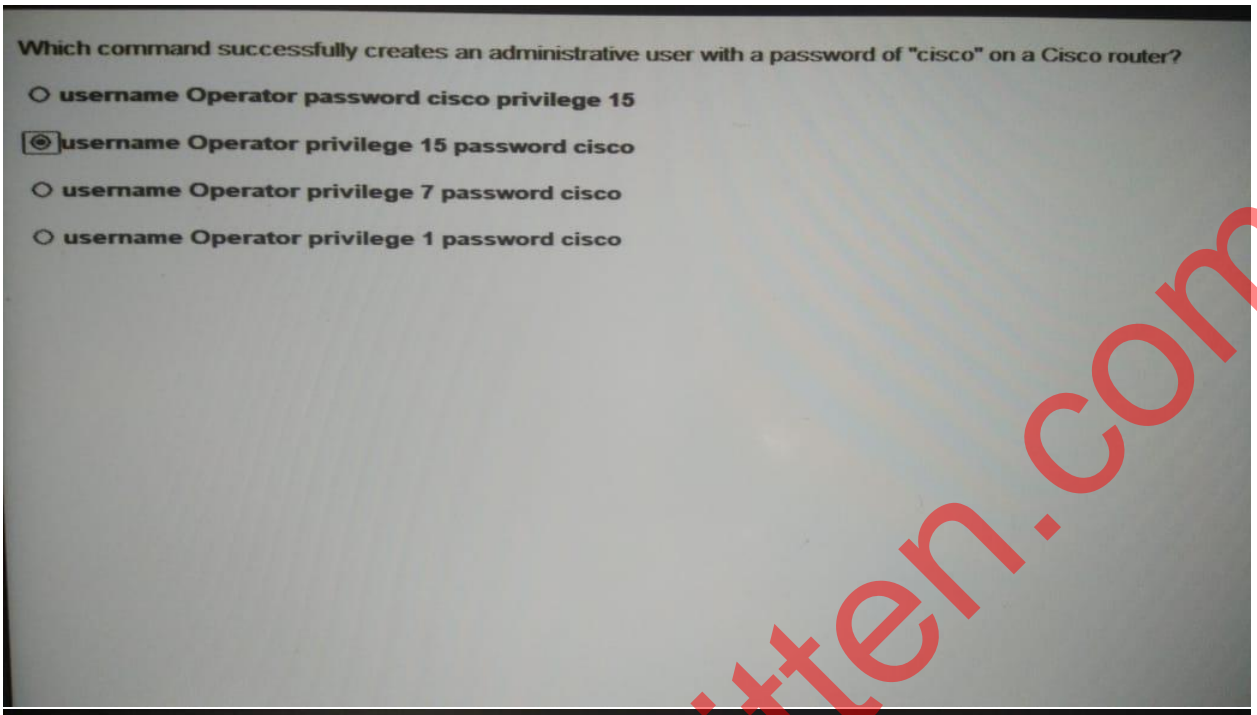
- multimode distortion
- [x] emanations
- Doppler waves
- Gaussian distributions

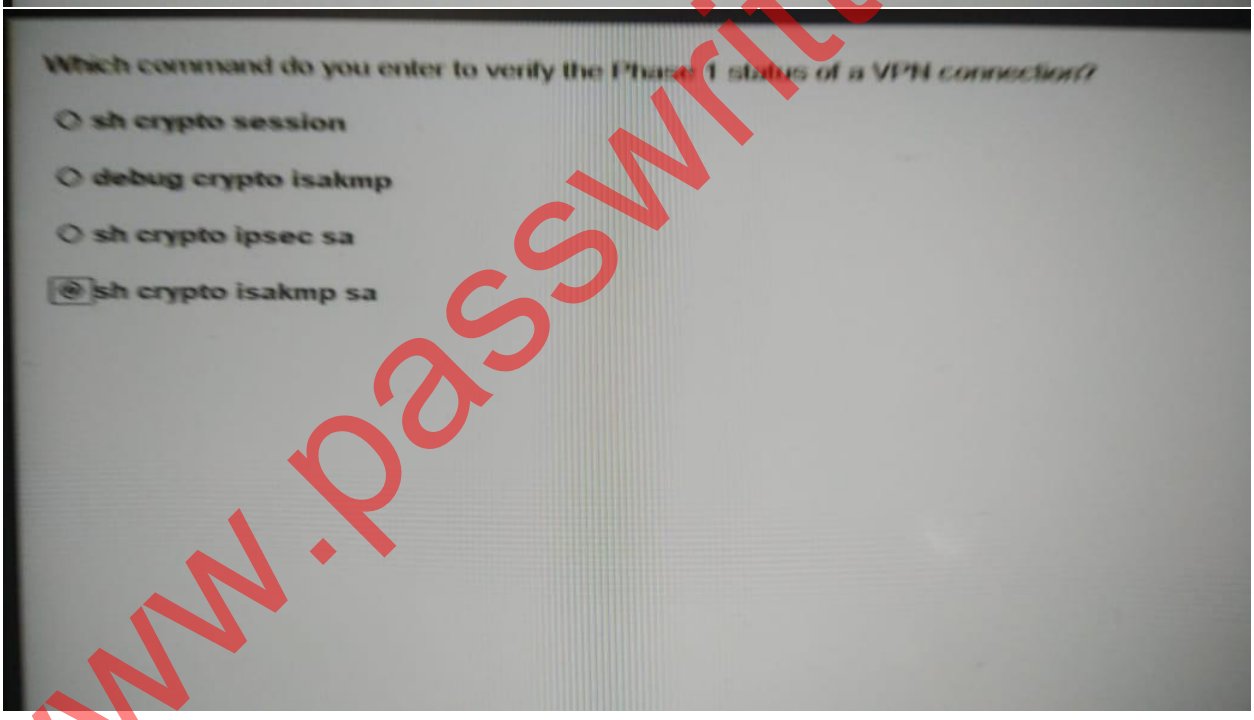


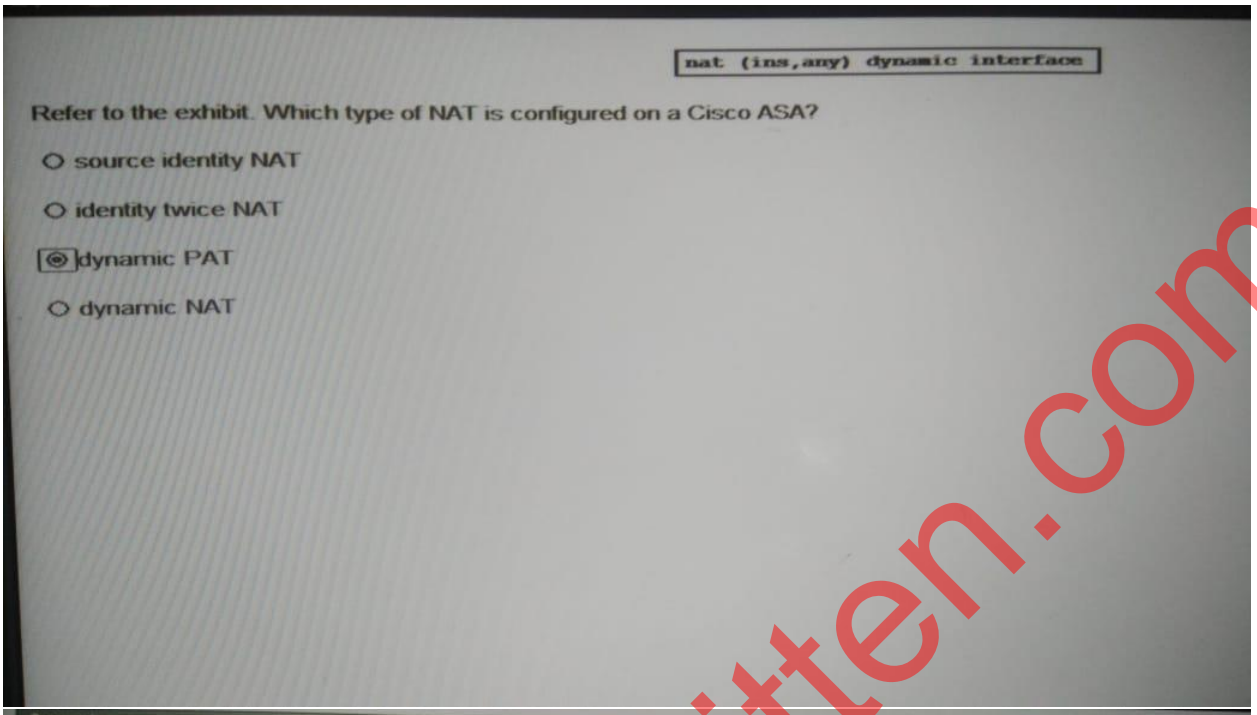
```
Router1config)#interface fastEthernet 0/0
Router1(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
Router1(config-if)#ip ospf authentication message-digest

Router2(config)#interface fastEthernet 0/0
Router2(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
Router2(config-if)#ip ospf authentication message-digest
```

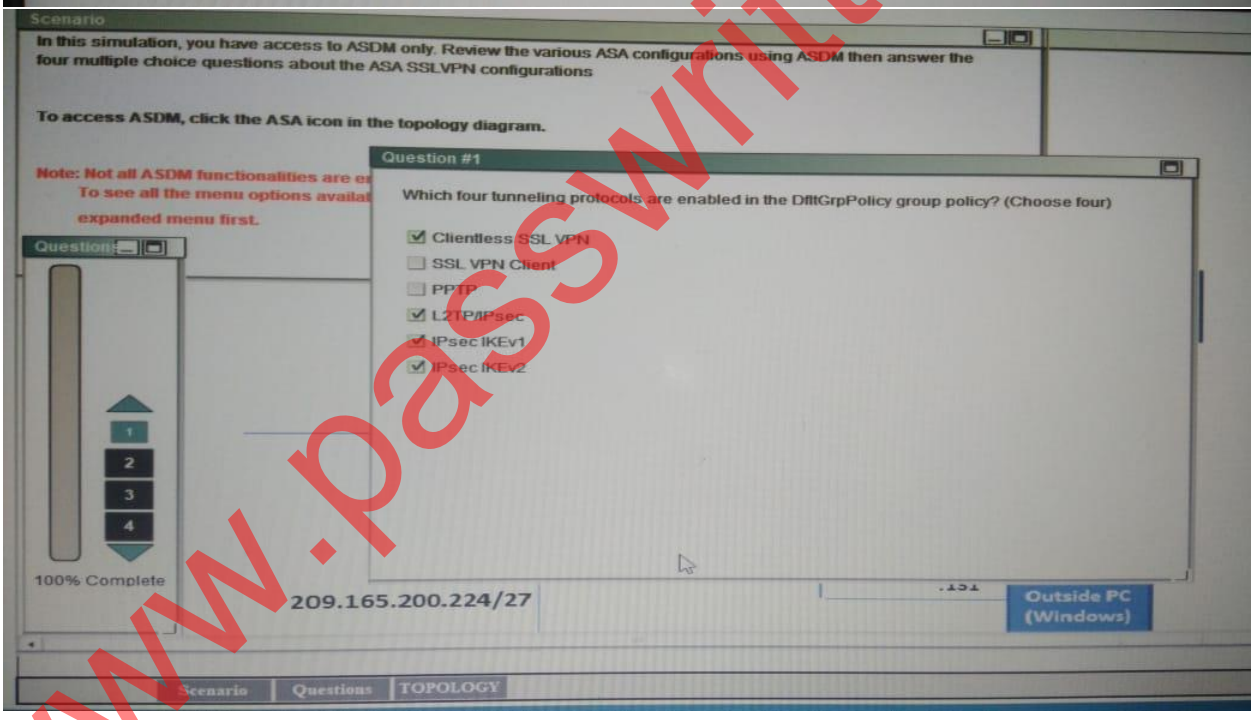
Refer to the exhibit. What is the effect of the given configuration?

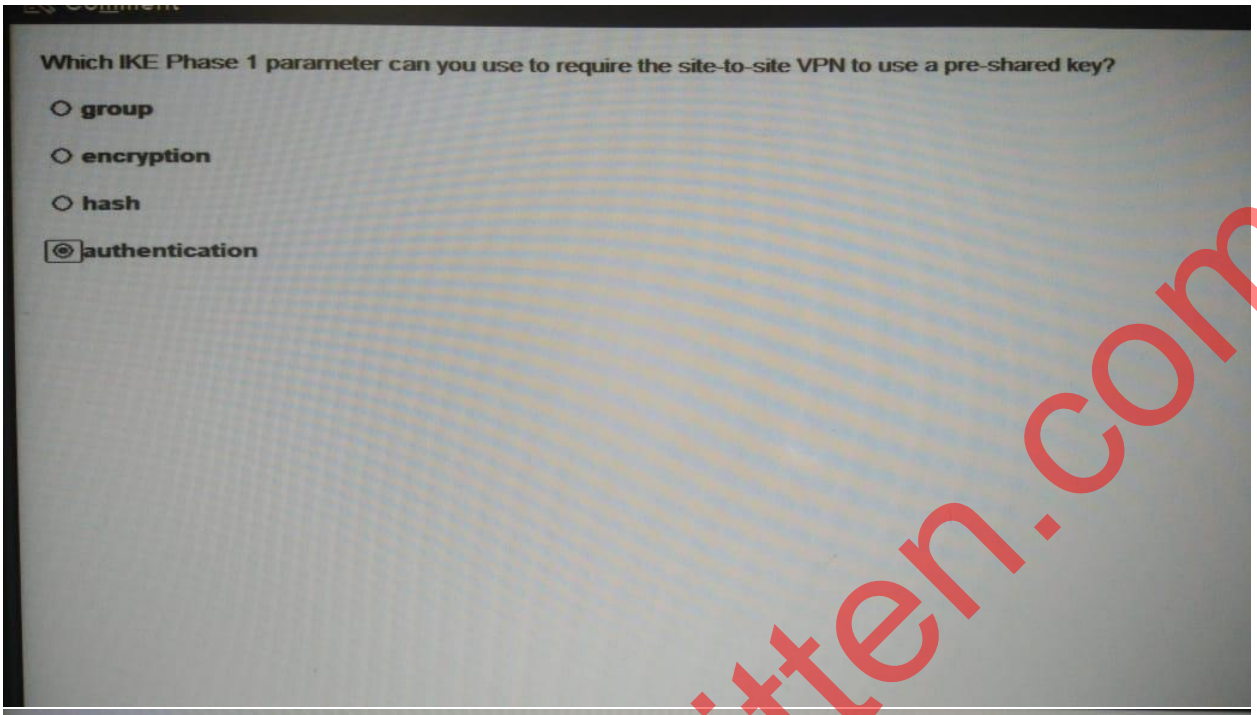
- It prevents keychain authentication.
- The two devices are able to pass the message digest to one another.
- The two routers receive normal updates from one another.
- [x] It enables authentication.

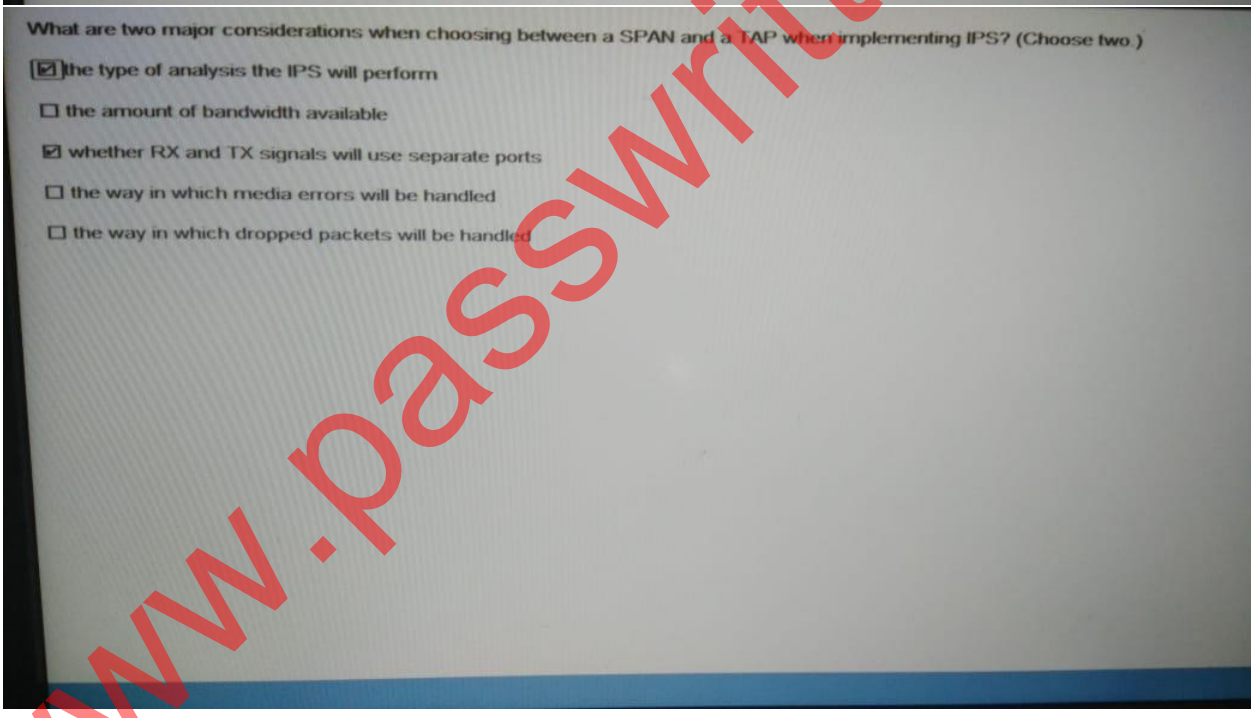






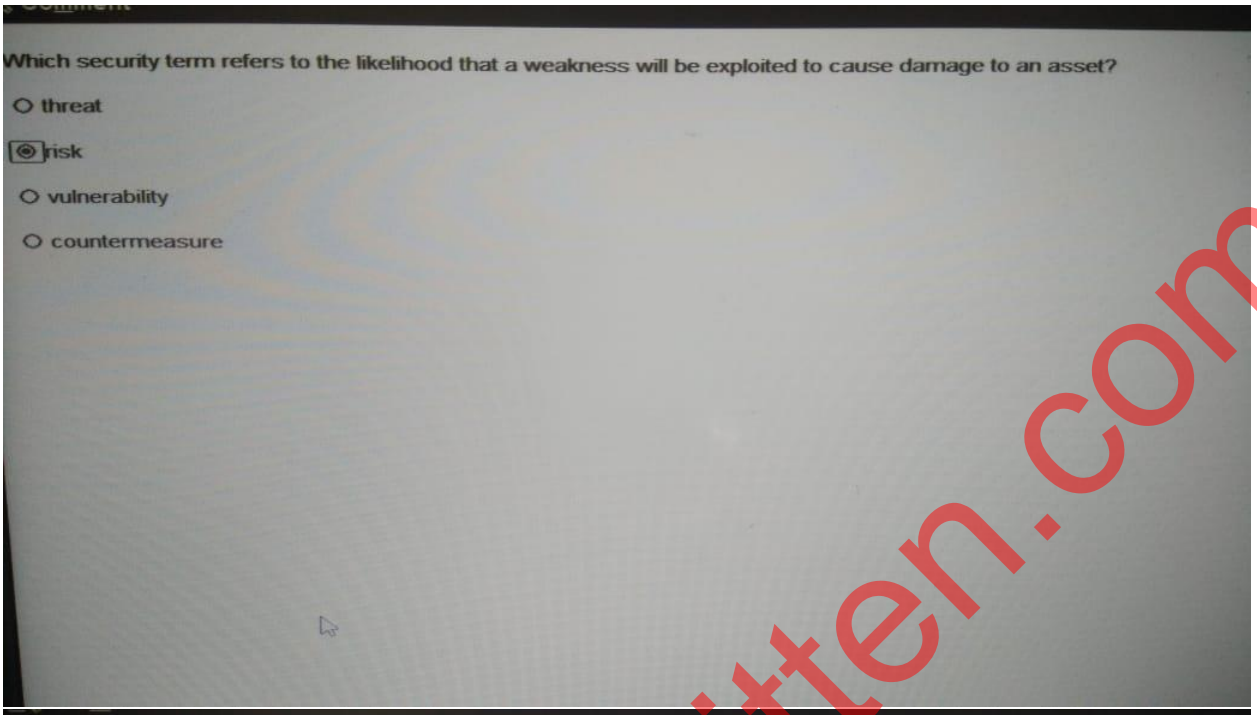



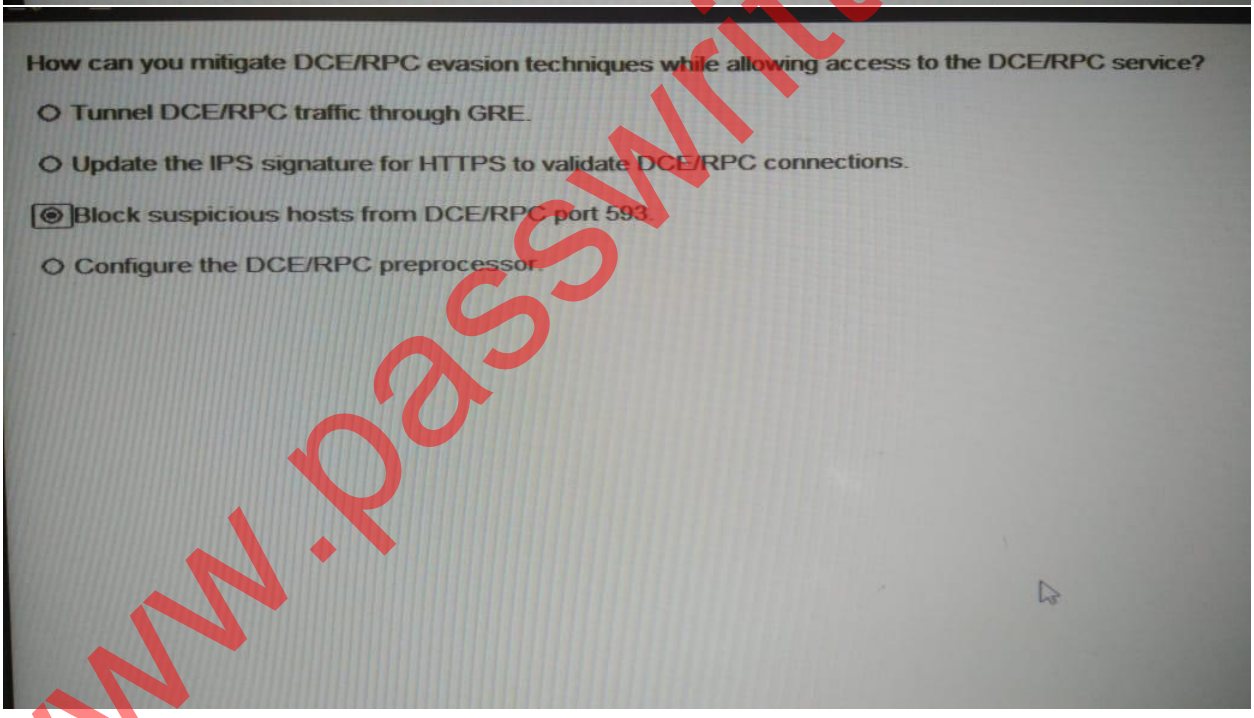
Which type of malicious software can create a back-door into a device or network?

- (●) Trojan
- ( ) bot
- ( ) worm
- ( ) virus

Drag and drop the steps to configure a WSA from the left into the correct order on the right.

| | |
|---|---|
| Configure directory groups. | step 1 |
| Configure identity management. | step 2 |
| Run the system setup wizard. | step 3 |
| Add an authentication realm. | step 4 |



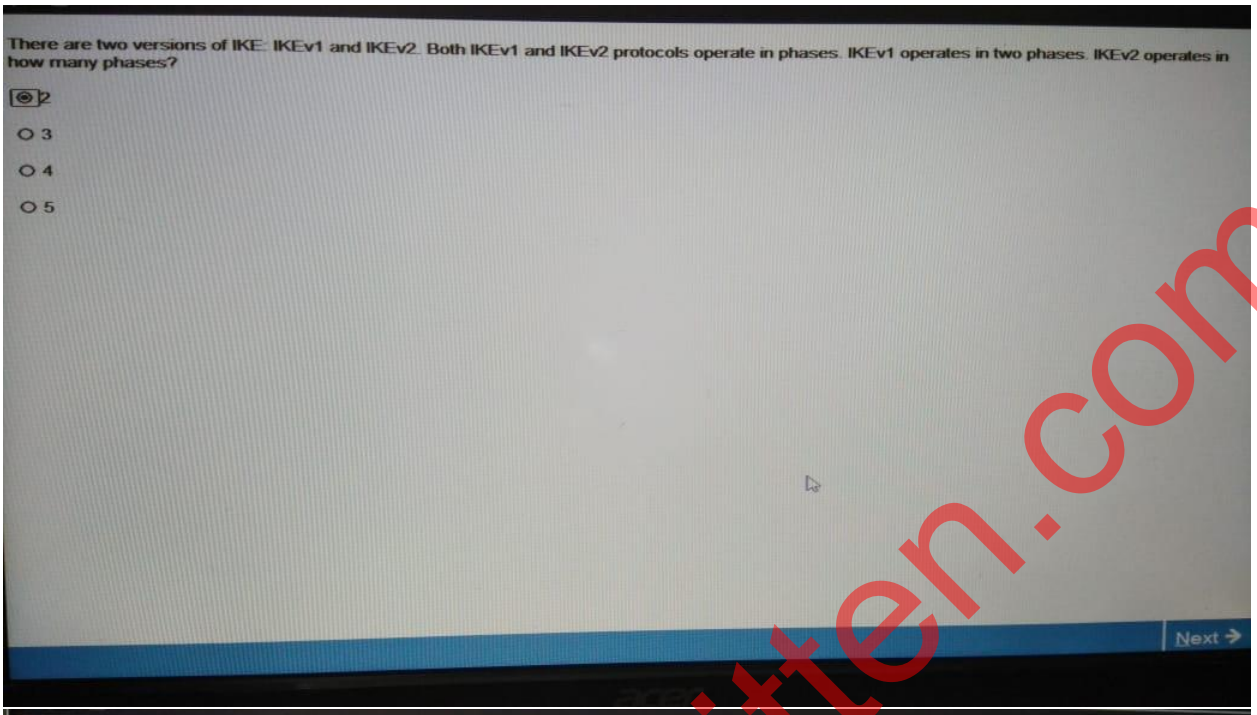



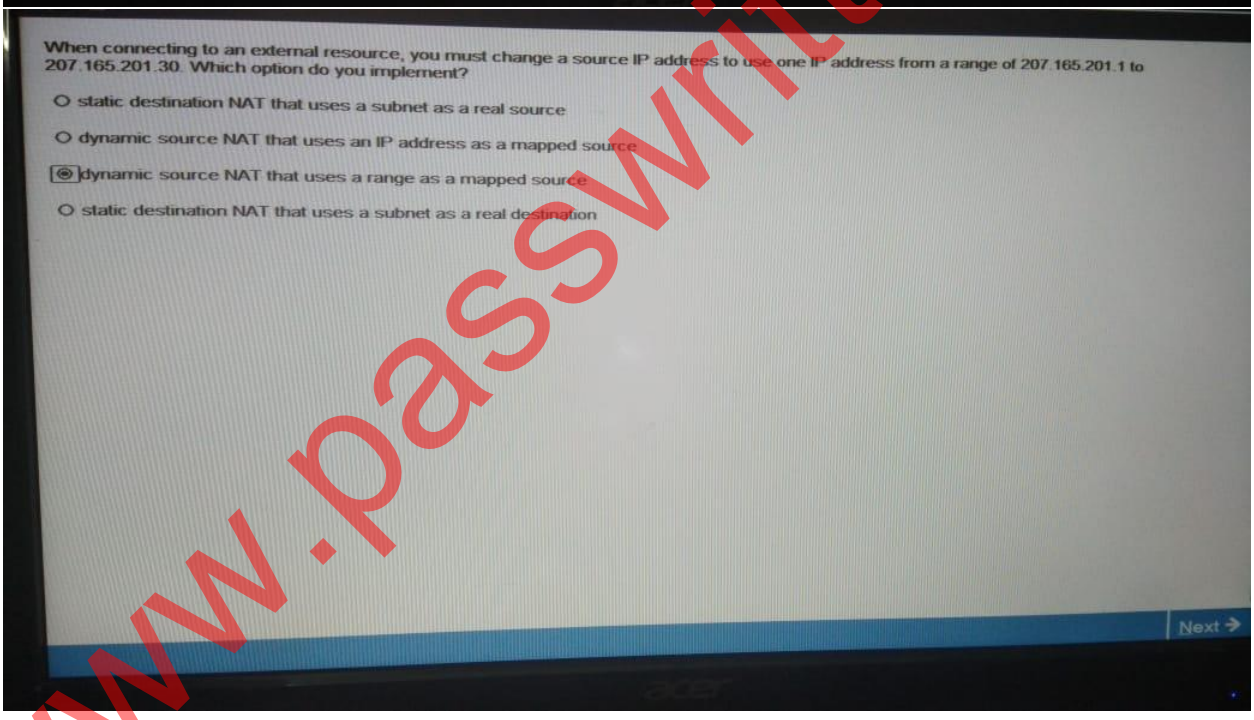
What are two default behaviors of the traffic on a zone-based firewall? (Choose two.)

- [x] All traffic between zones is implicitly blocked.
- [x] Communication is allowed between interfaces that are members of the same zone.
- [ ] The CBAC rules that are configured on router interfaces apply to zone interfaces.
- [ ] Traffic within the self zone uses an implicit **deny all**.
- [ ] Communication is blocked between interfaces that are members of the same zone.

Drag and drop each feature that can protect against DHCP attacks from the left onto the correct description on the right.

| | |
|---|---|
| DHCP snooping | blocks DHCP messages from untrusted sources |
| dynamic ARP inspection | mitigates MAC-address spoofing at the access interface |
| IP source guard | provides Layer 2 interface security with port ACLs |
| port security | verifies IP-to-MAC traffic on untrusted ports |



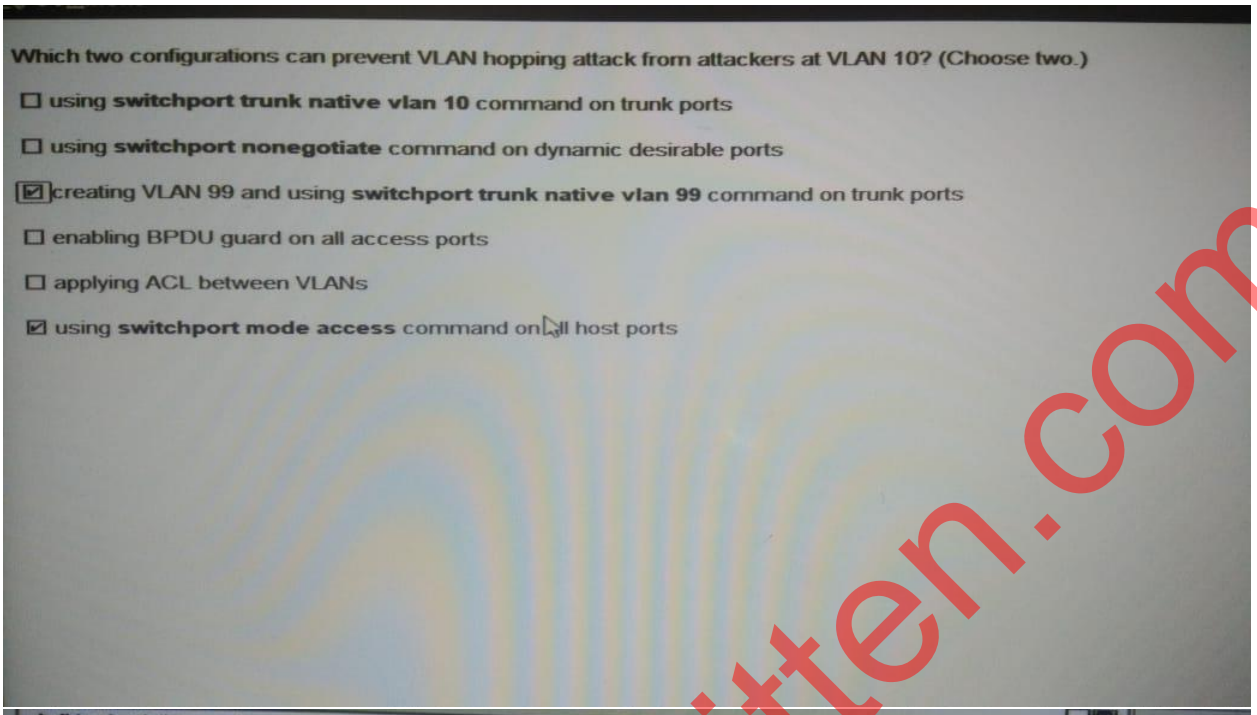



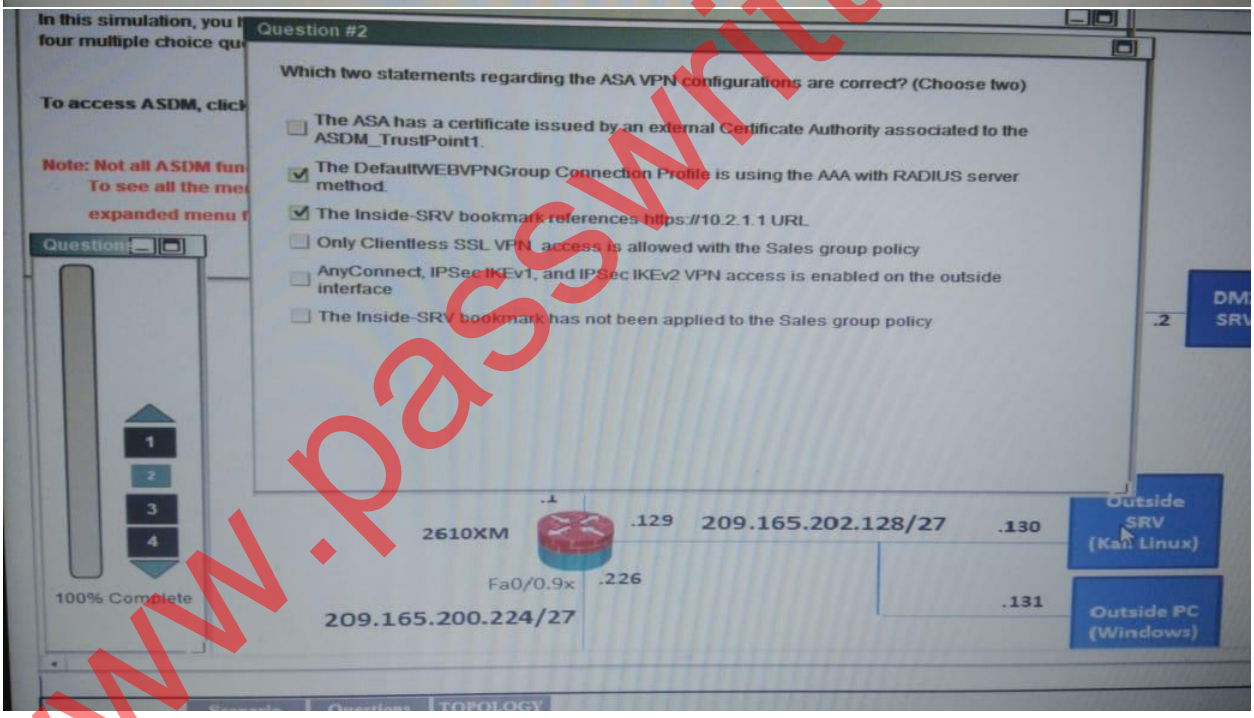
When you edit an IPS subsignature, what is the effect on the parent signature and the family of subsignatures?

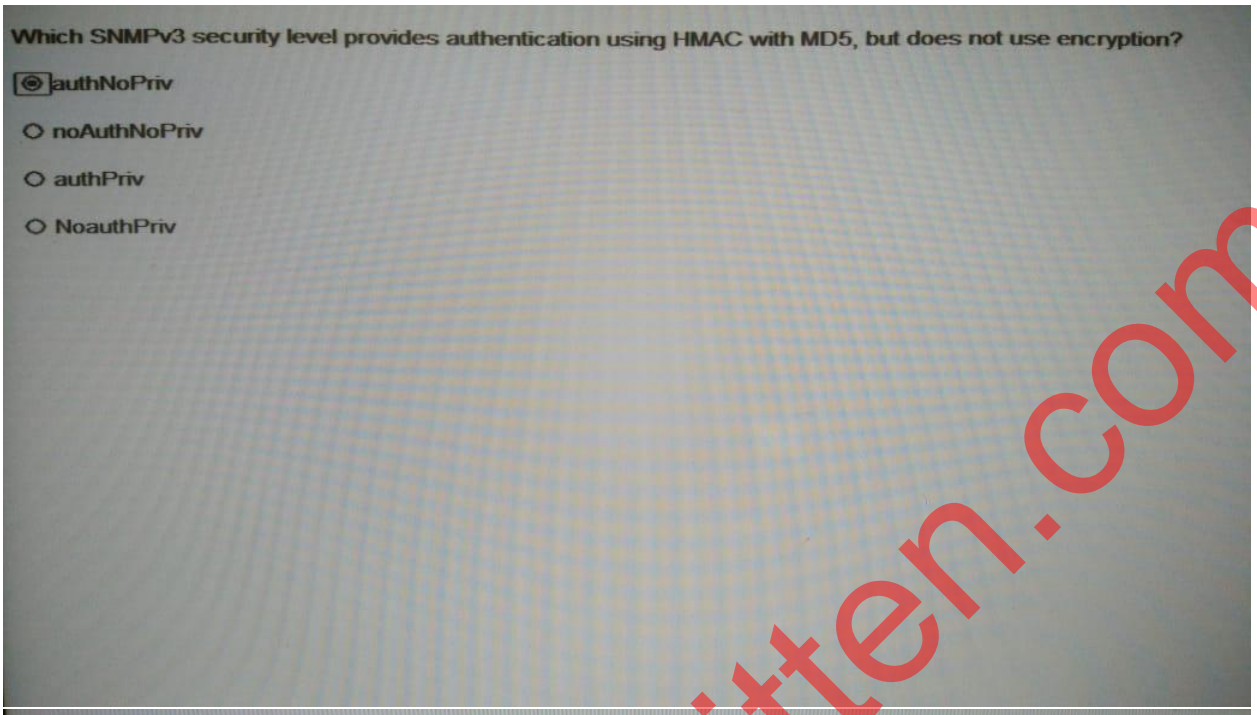
- ○ The change applies only to subsignatures that are numbered sequentially after the subsignature that you edit.
- ○ The change applies to the parent signature and the subsignature that you edit.
- ◉ Other signatures are unaffected; the change applies only to the subsignature that you edit.
- ○ The change applies to the parent signature and the entire family of subsignatures.

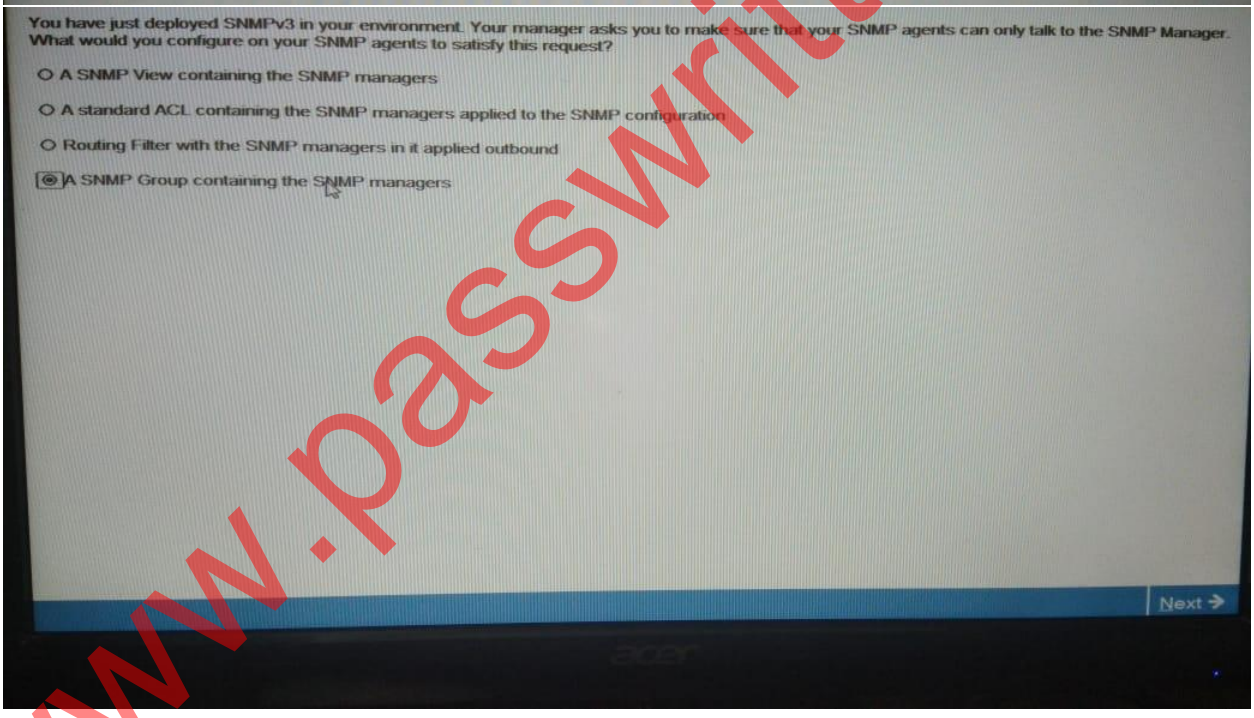
Which command can you enter to verify the status of Cisco IOS Resilient Configuration on a Cisco router?

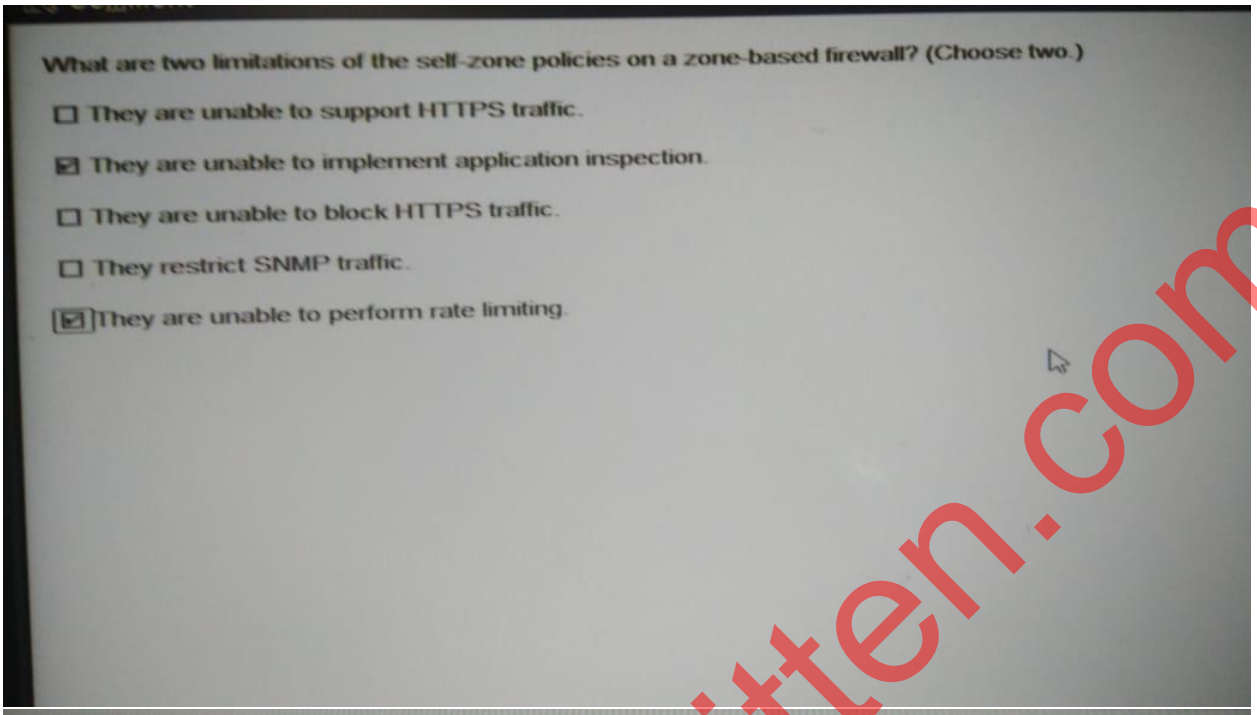
- ◉ **show secure bootset**
- ○ **secure boot-image**
- ○ **show binary file**
- ○ **secure boot-config**

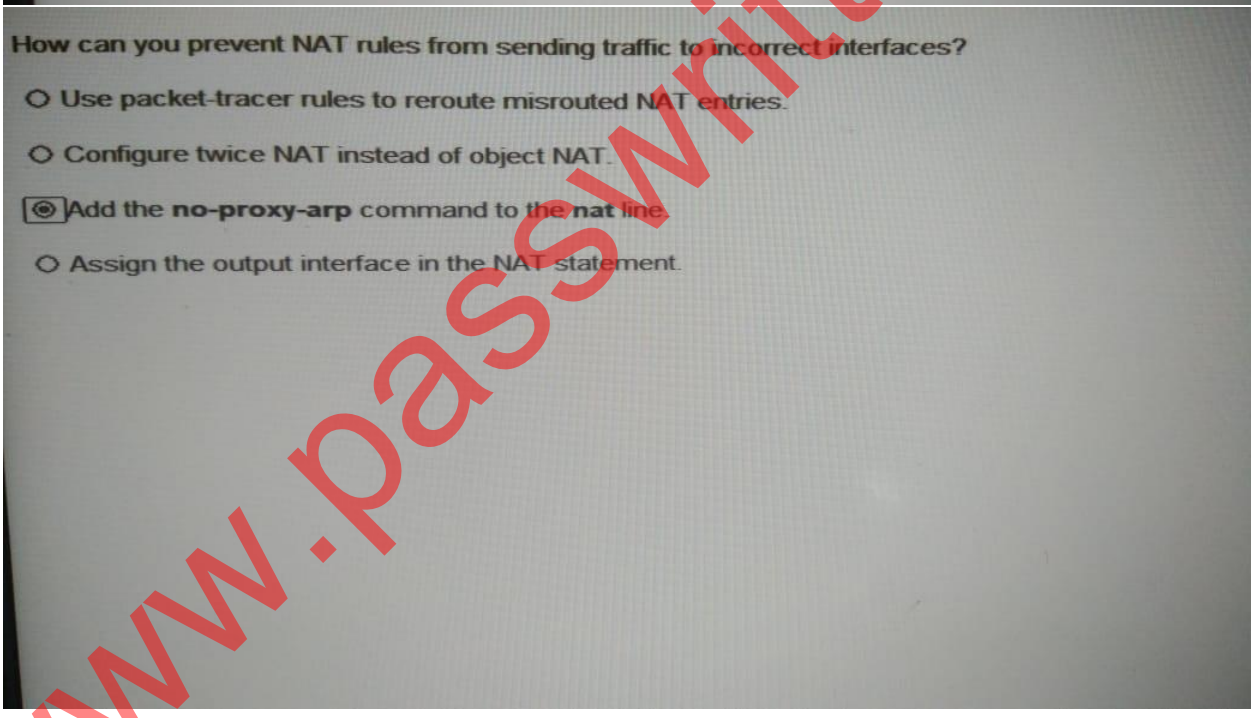


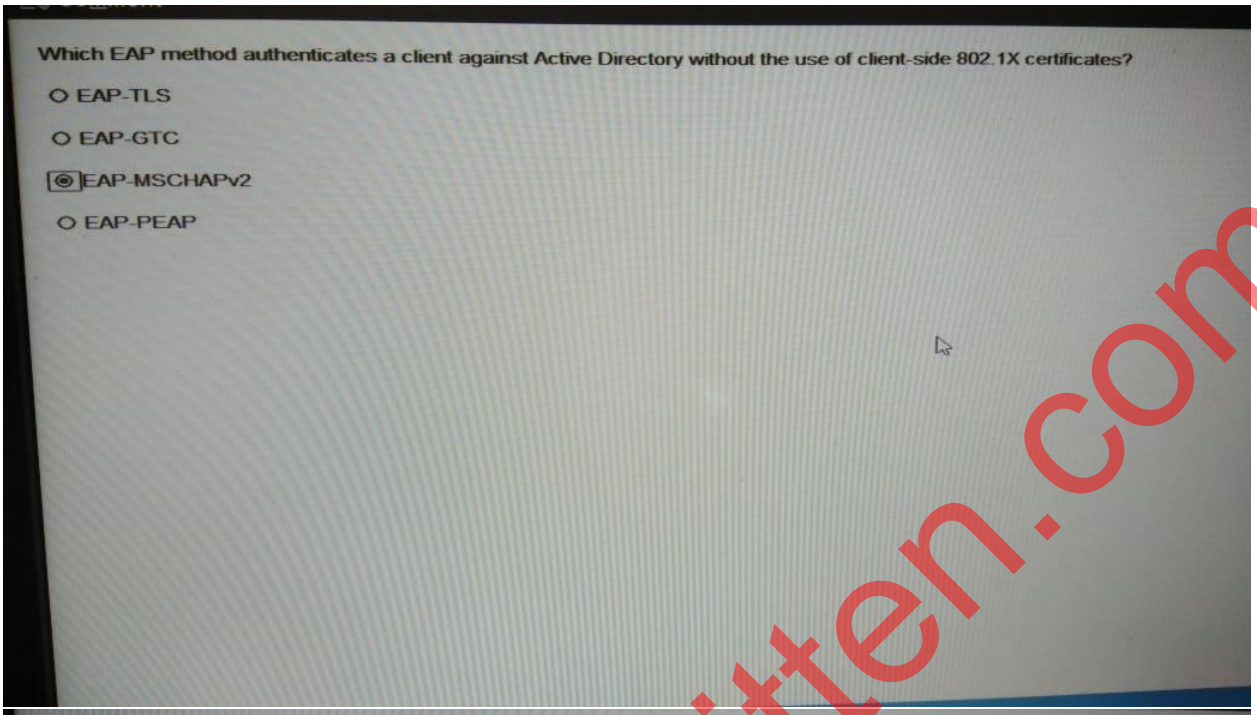



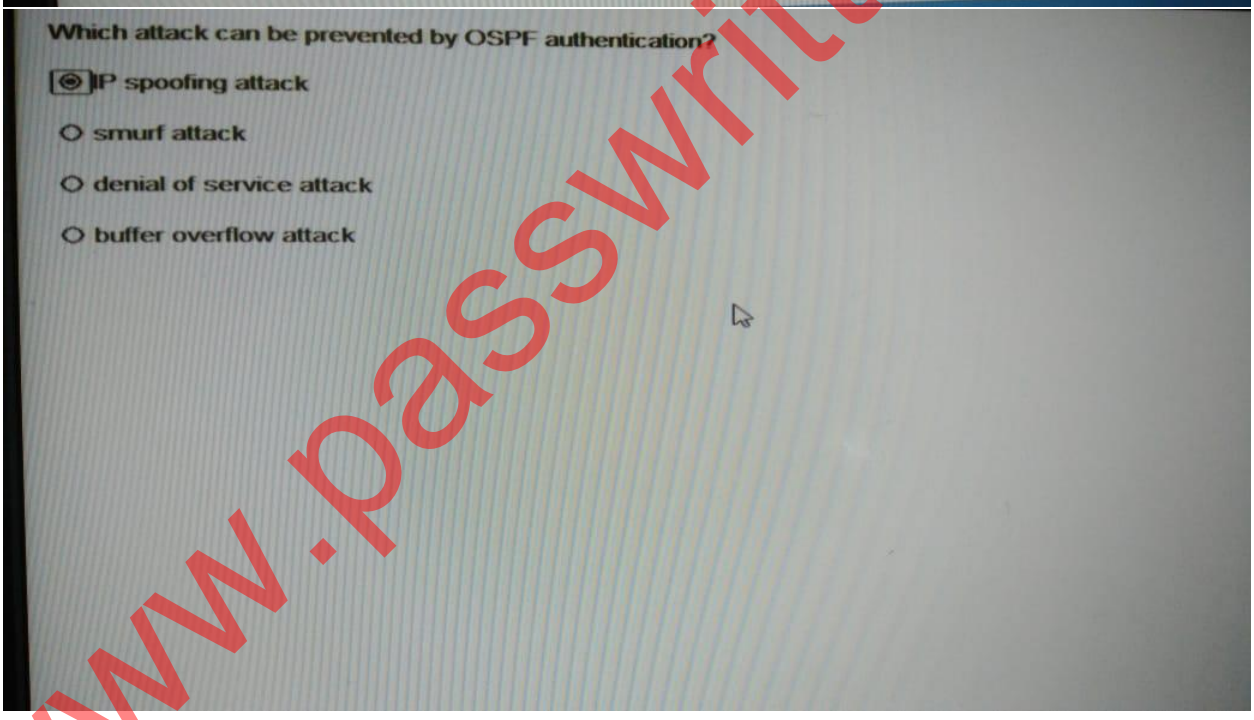






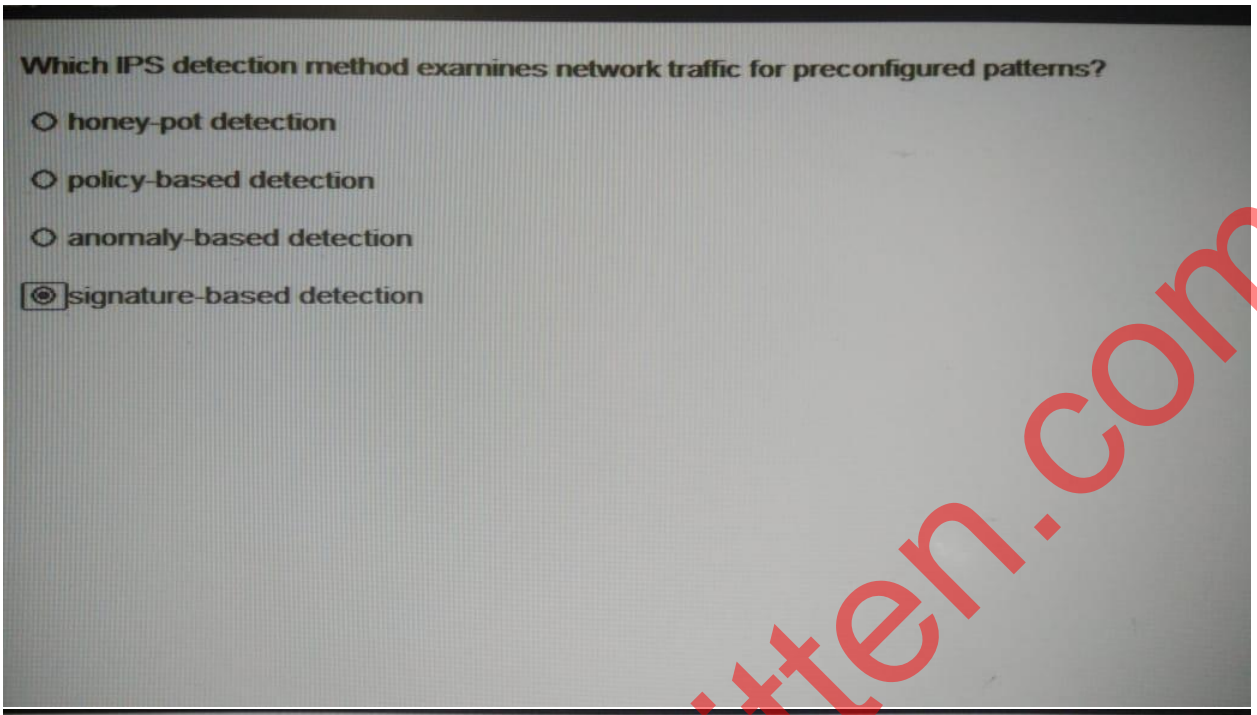



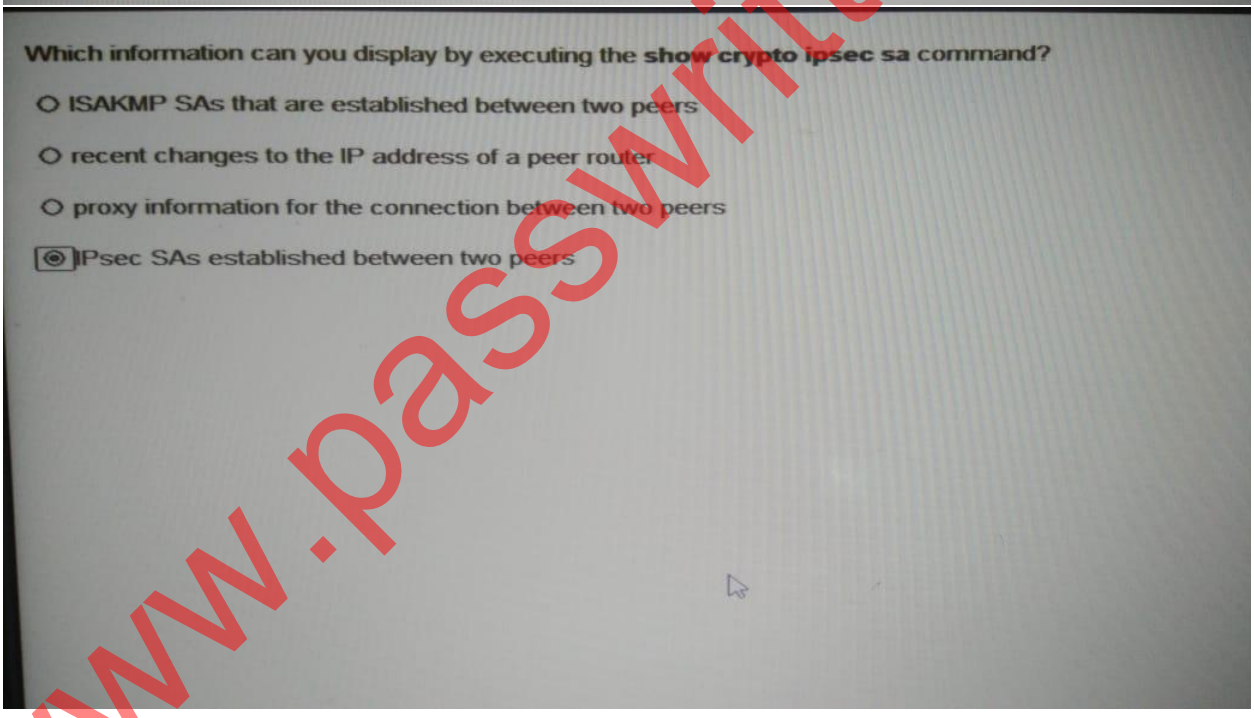
Which two descriptions of TACACS+ are true? (Choose two.)

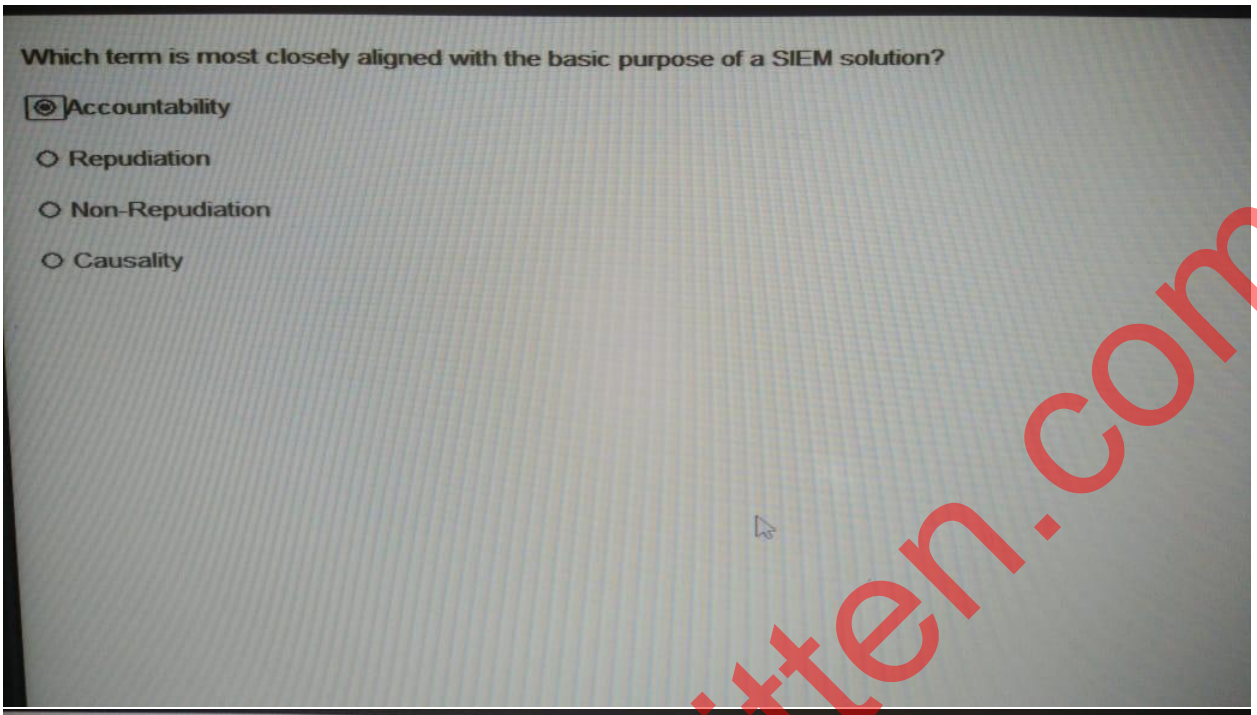
- ☐ It combines authentication and authorization.
- ☐ Only the password is encrypted.
- ☐ It uses UDP as its transport protocol.
- ☑ The TACACS+ header is unencrypted.
- ☑ It uses TCP as its transport protocol.

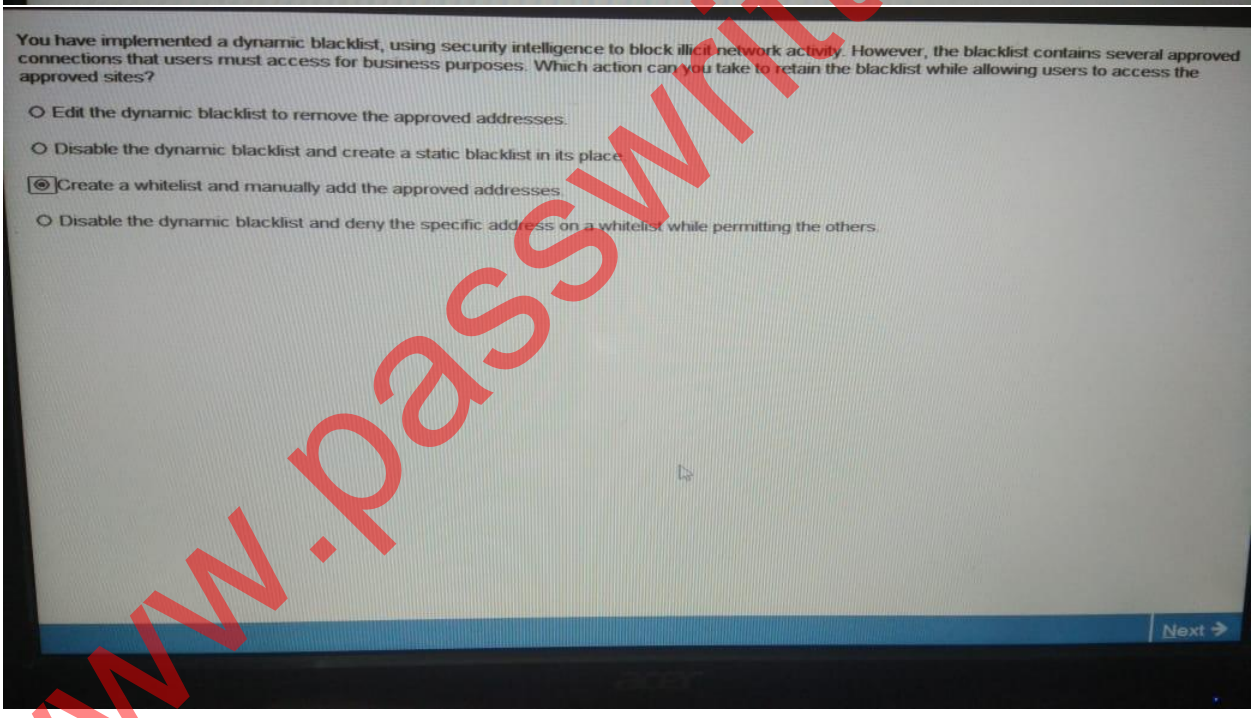
Which two statements about hardware-based encryption are true? (Choose two.)

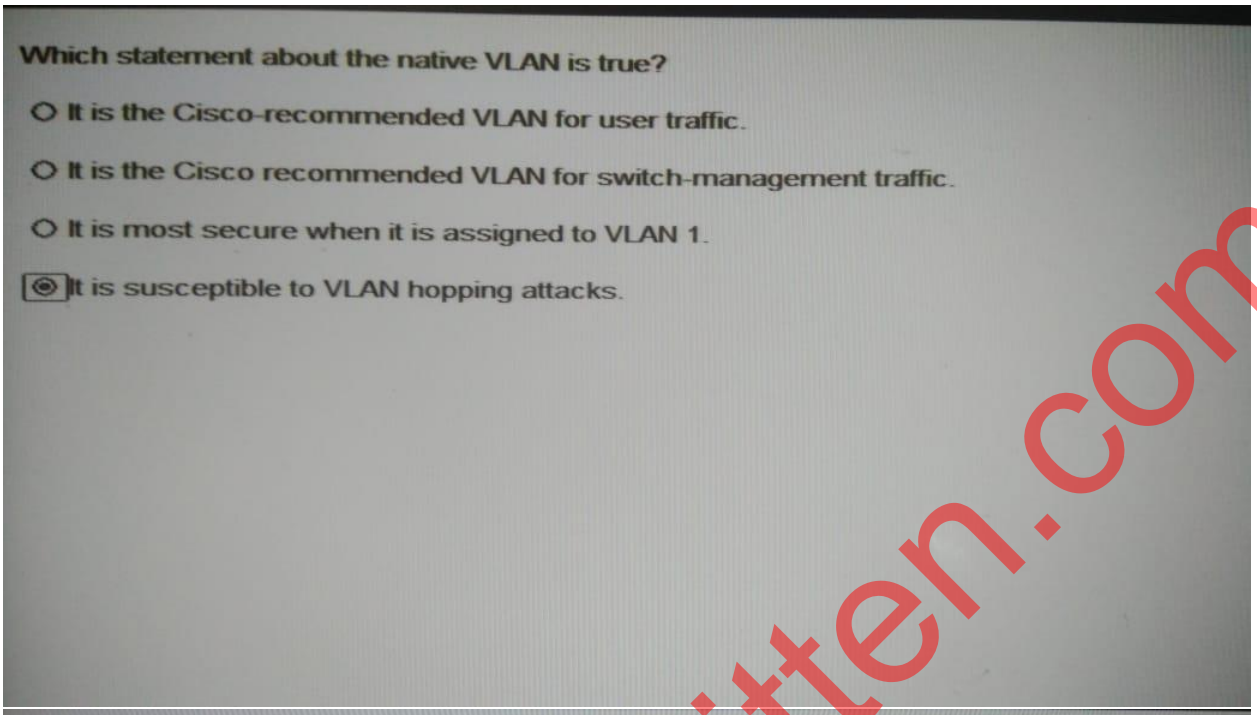
- ☐ It is widely accessible.
- ☐ It requires minimal configuration.
- ☑ It can be implemented without impacting performance.
- ☐ It is potentially easier to compromise than software-based encryption.
- ☑ It is highly cost-effective.

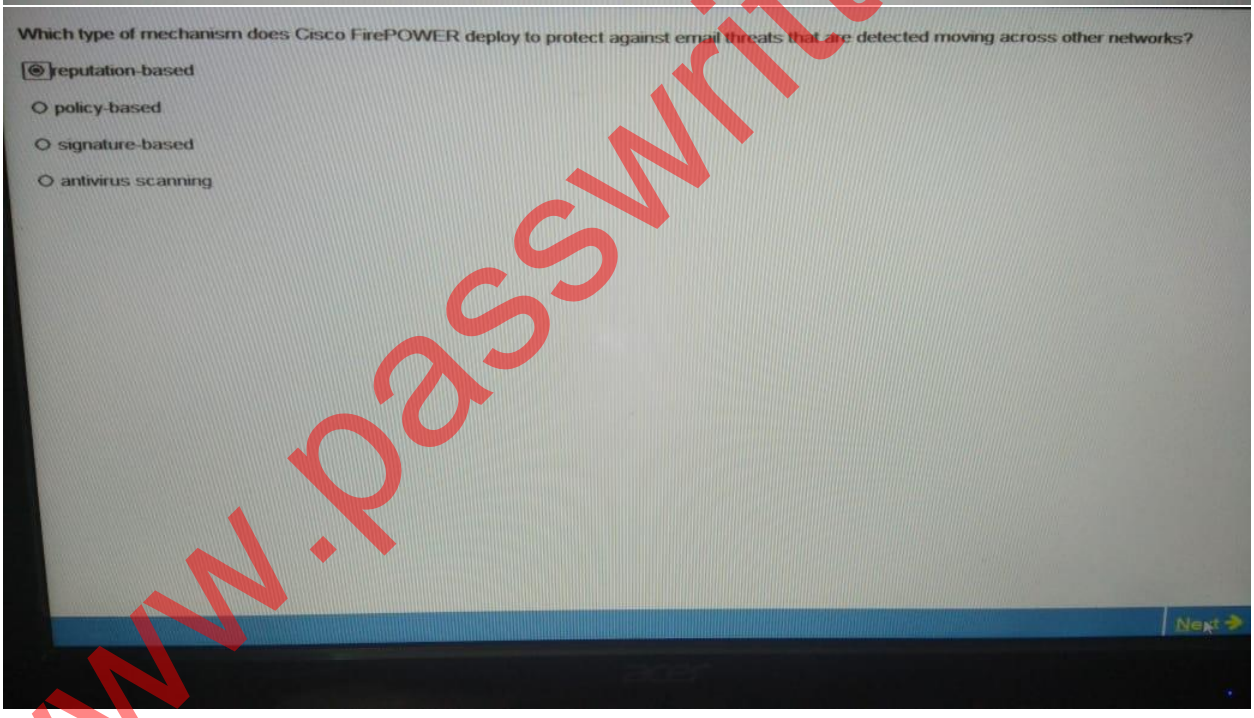


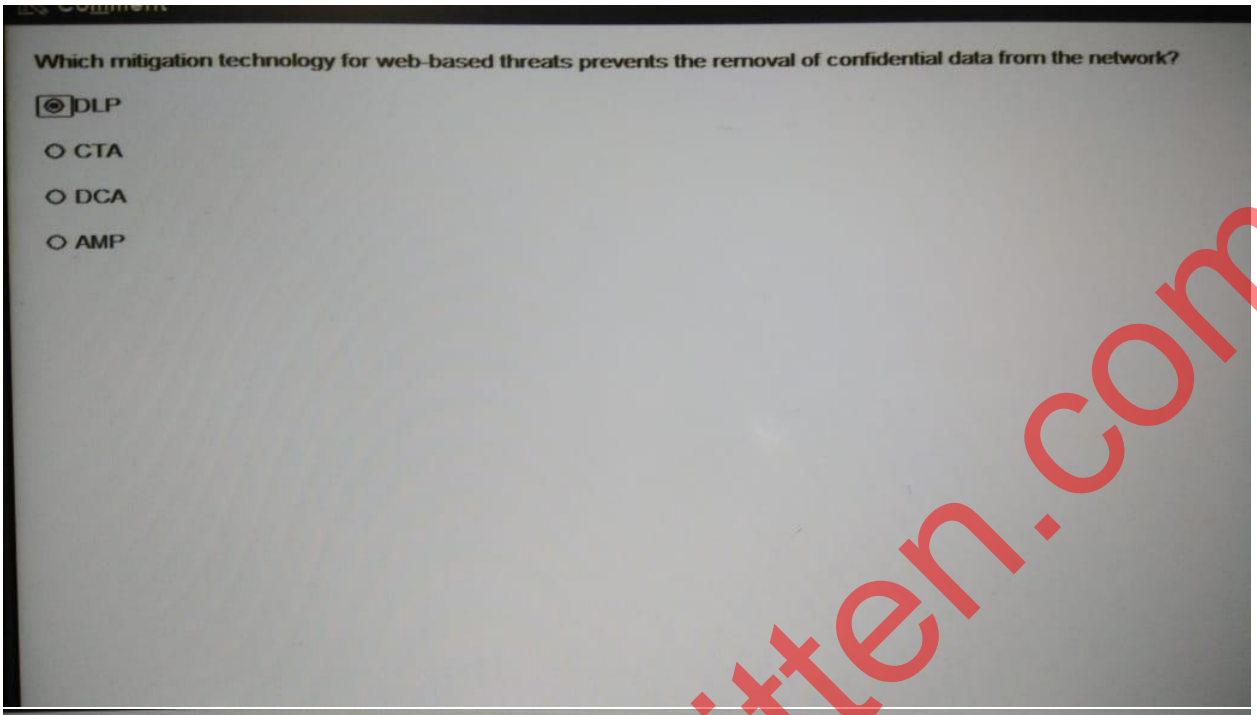



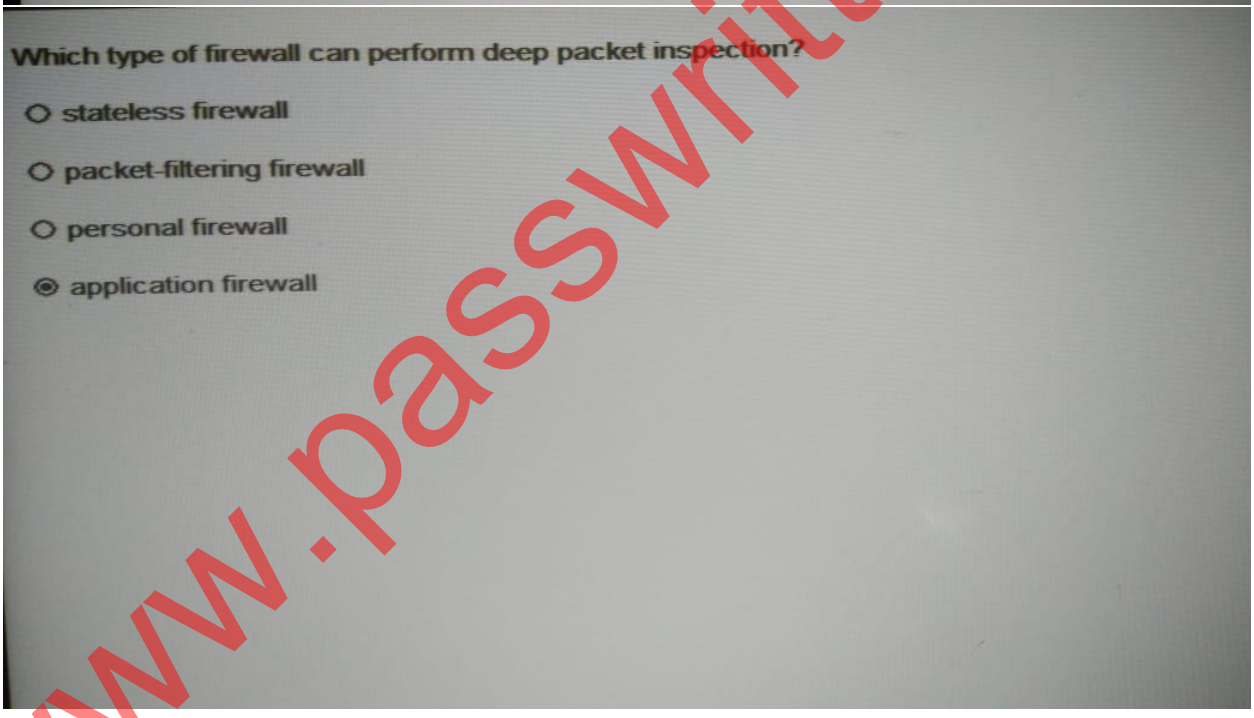


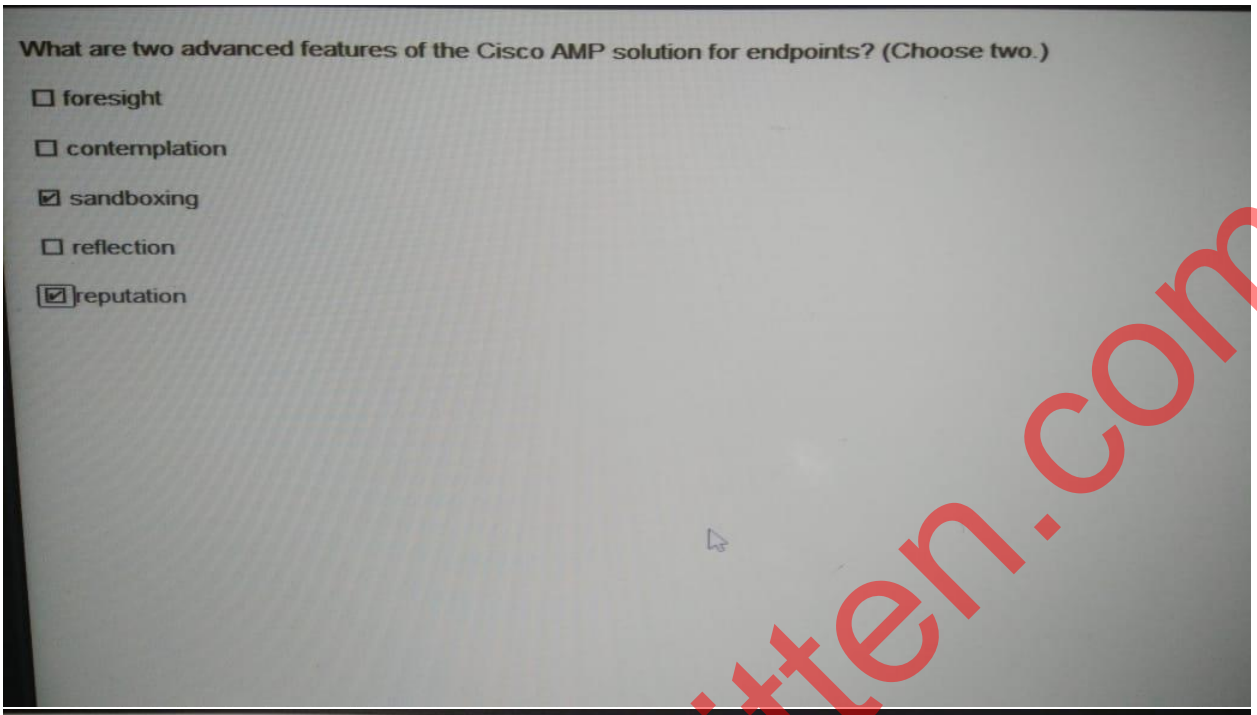



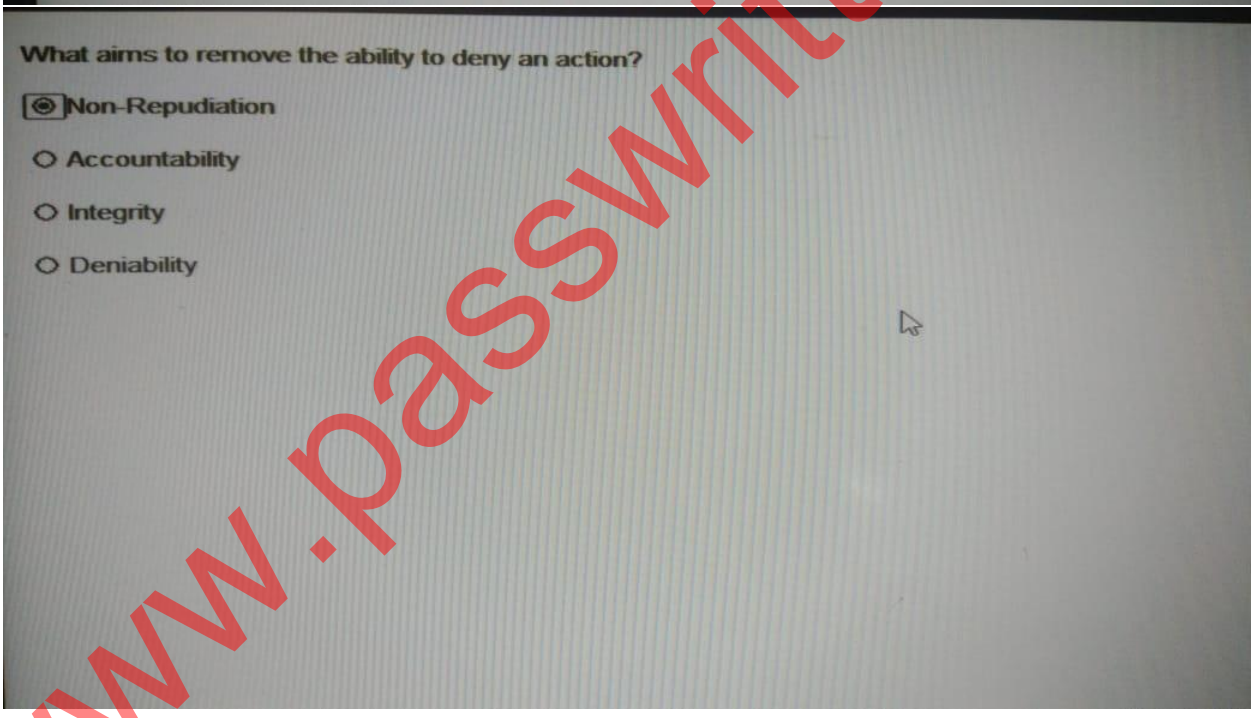


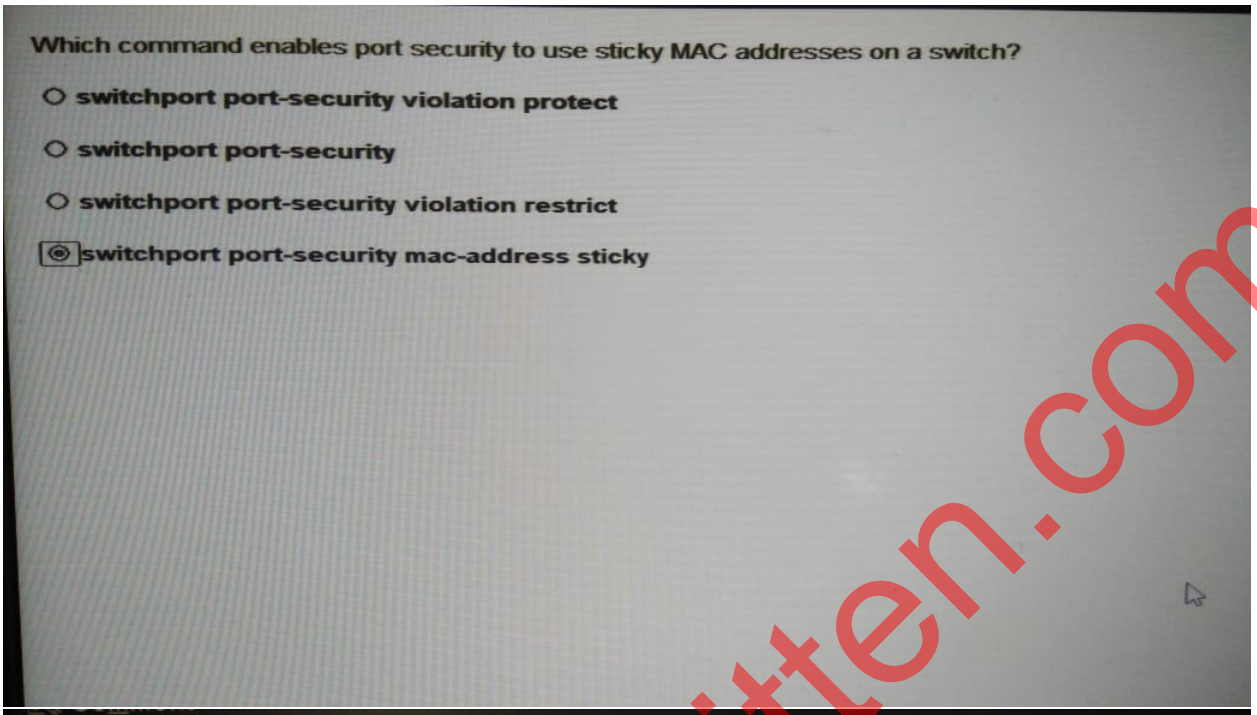



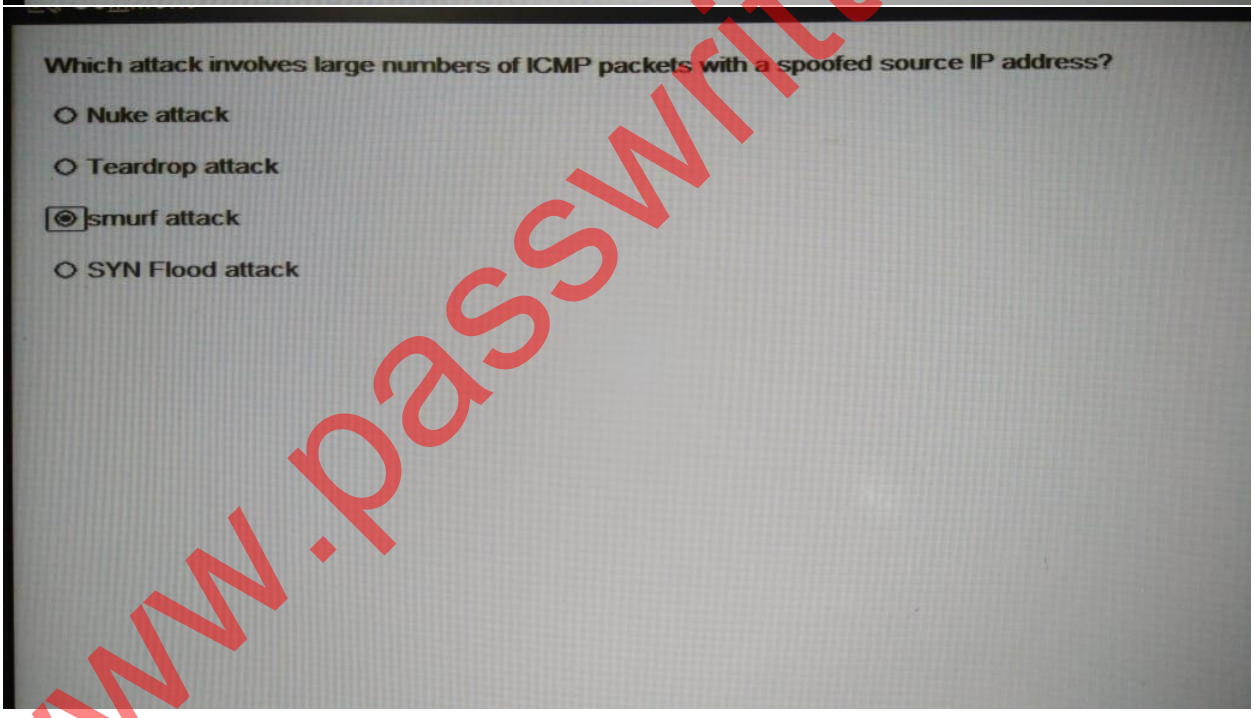


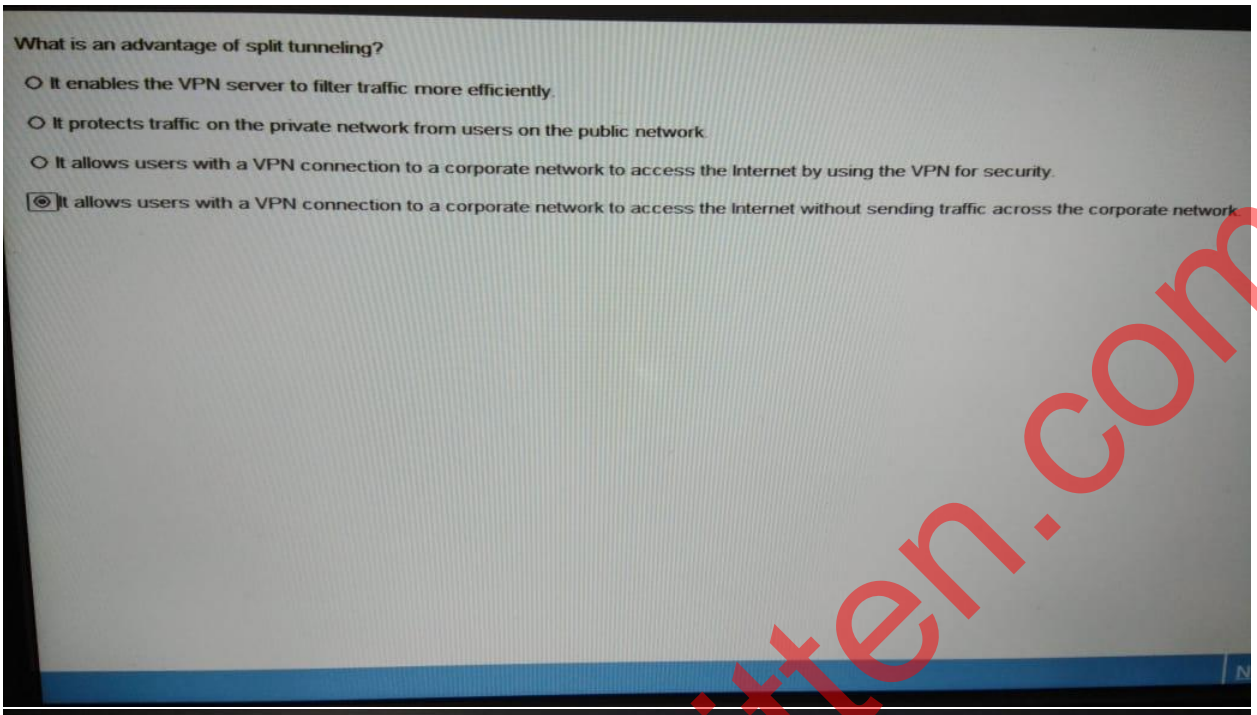



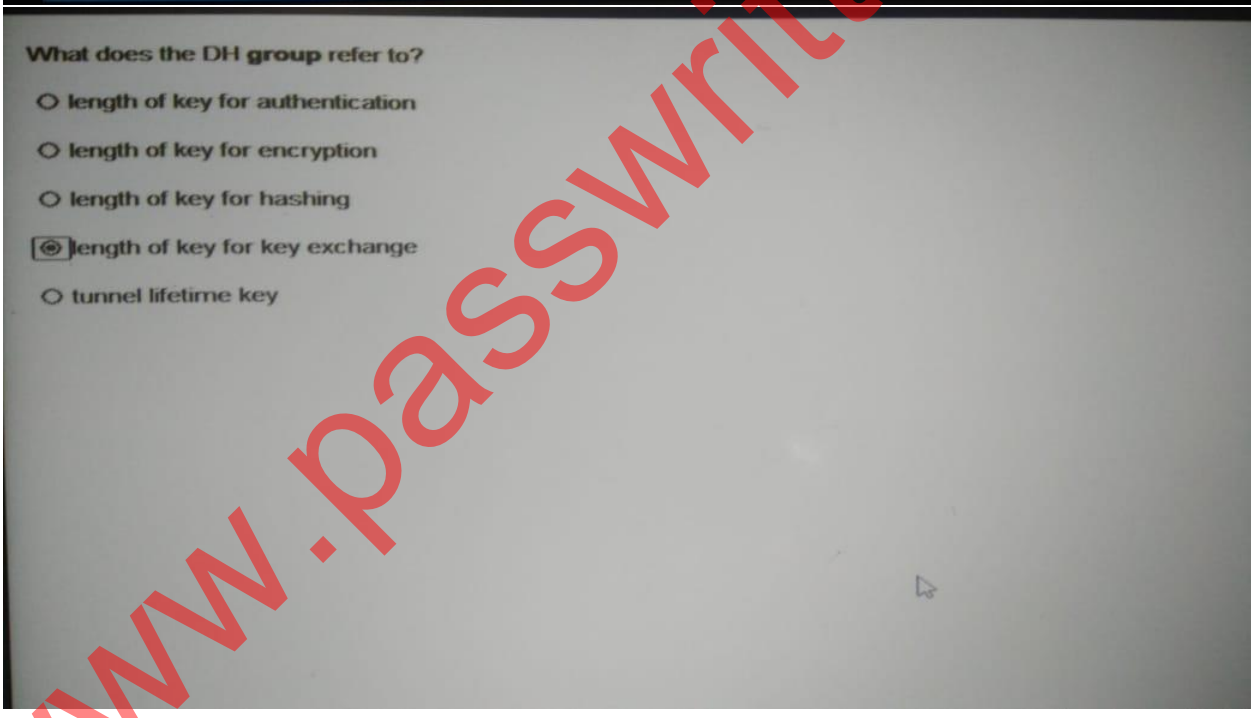


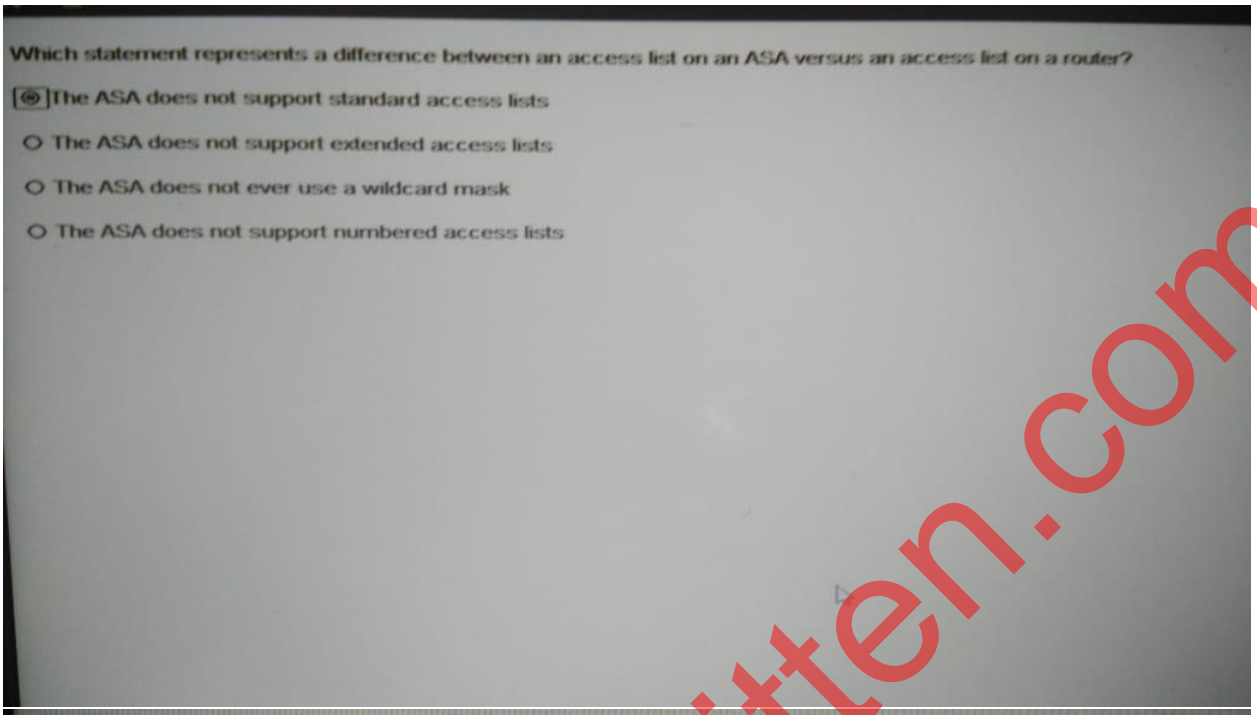



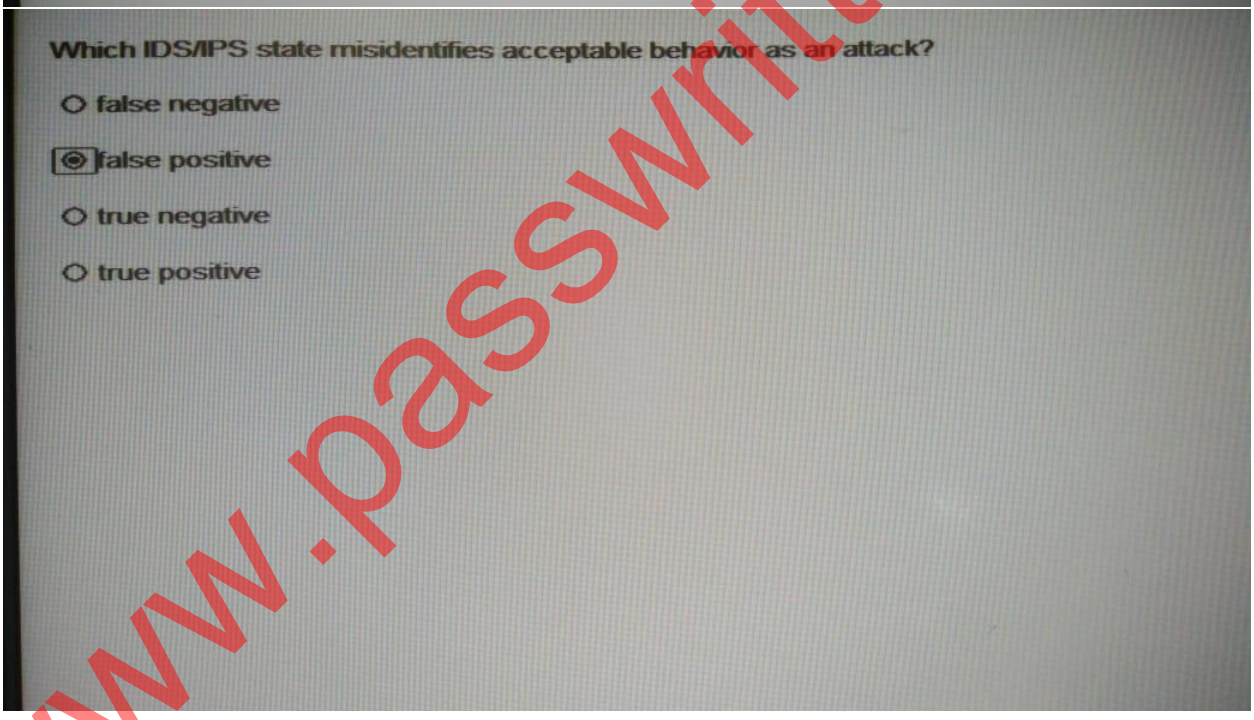


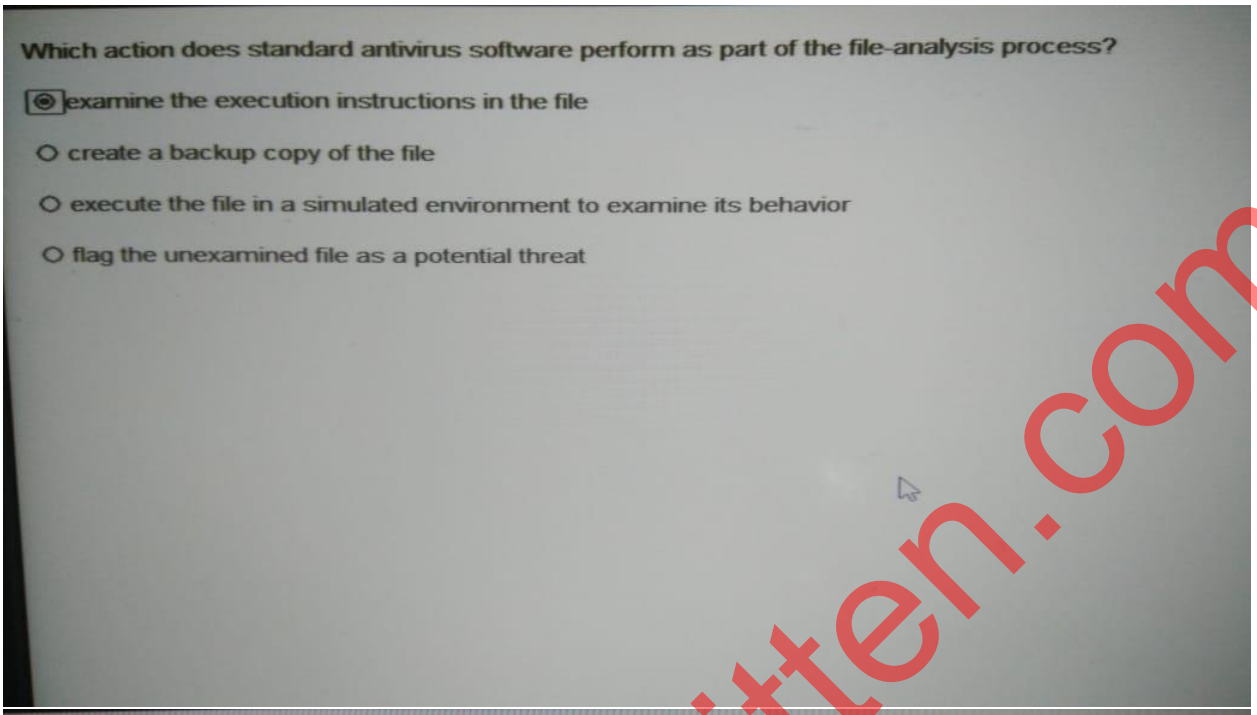



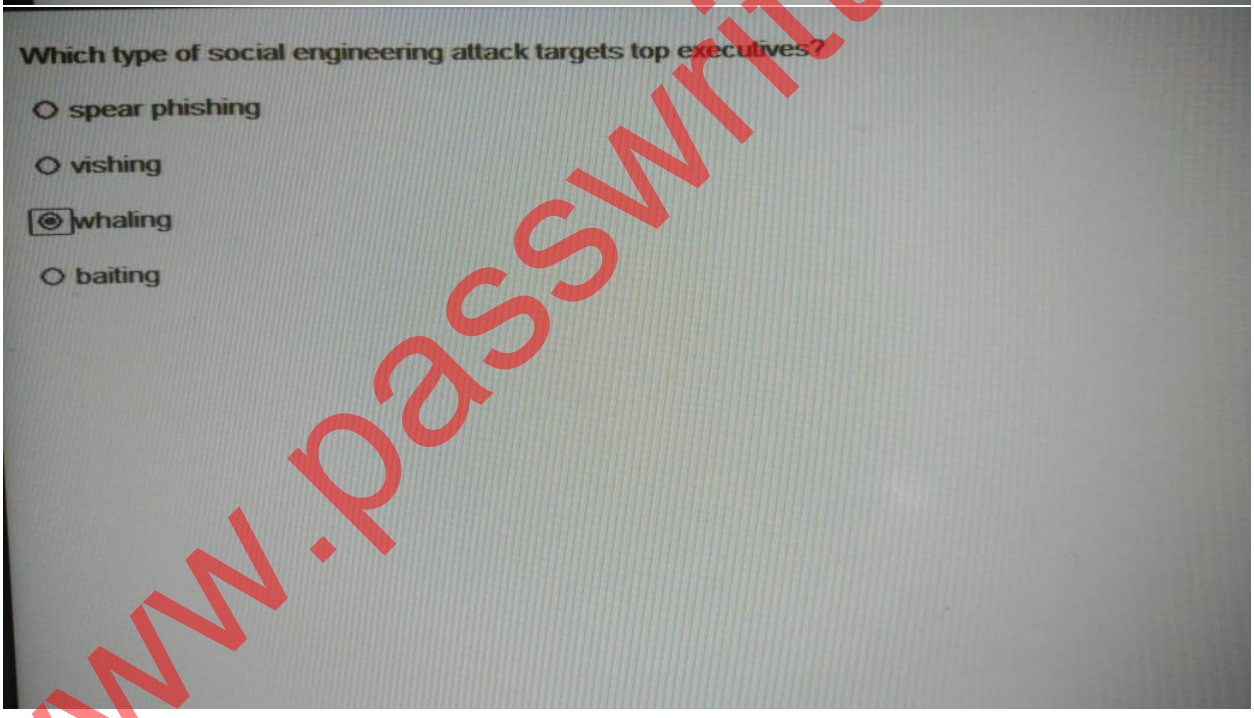






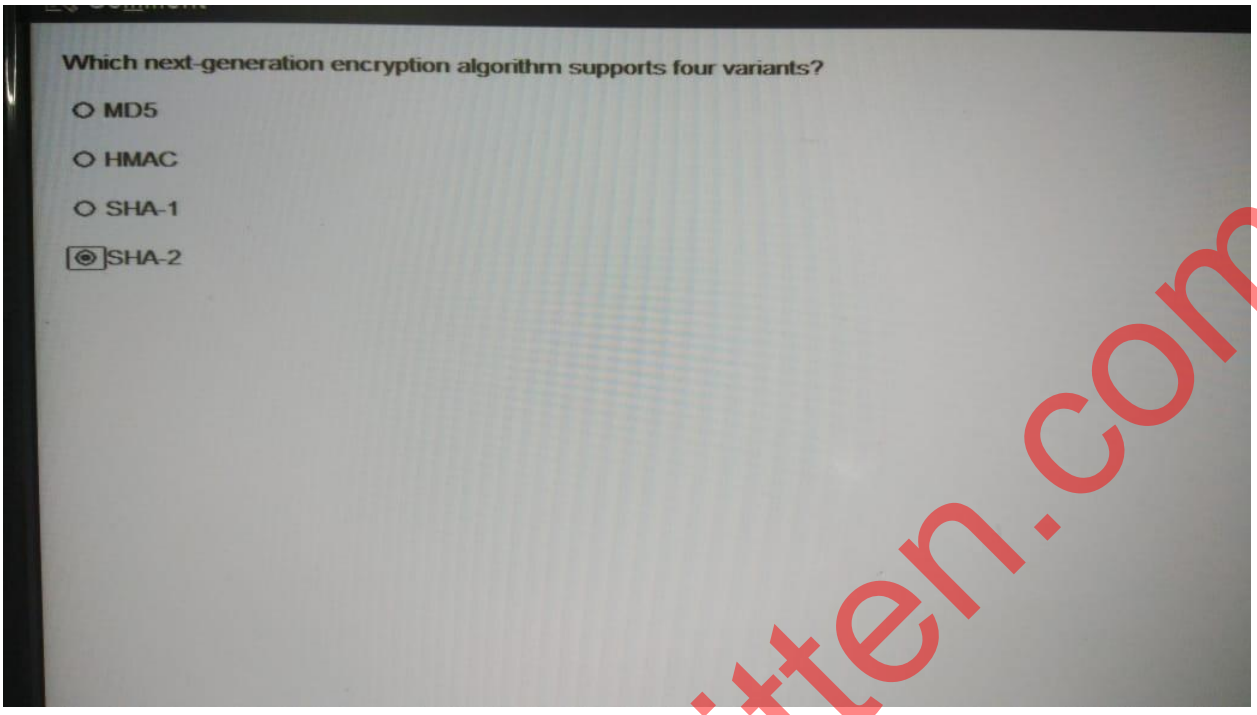
How is management traffic isolated on a Cisco ASR 1002?

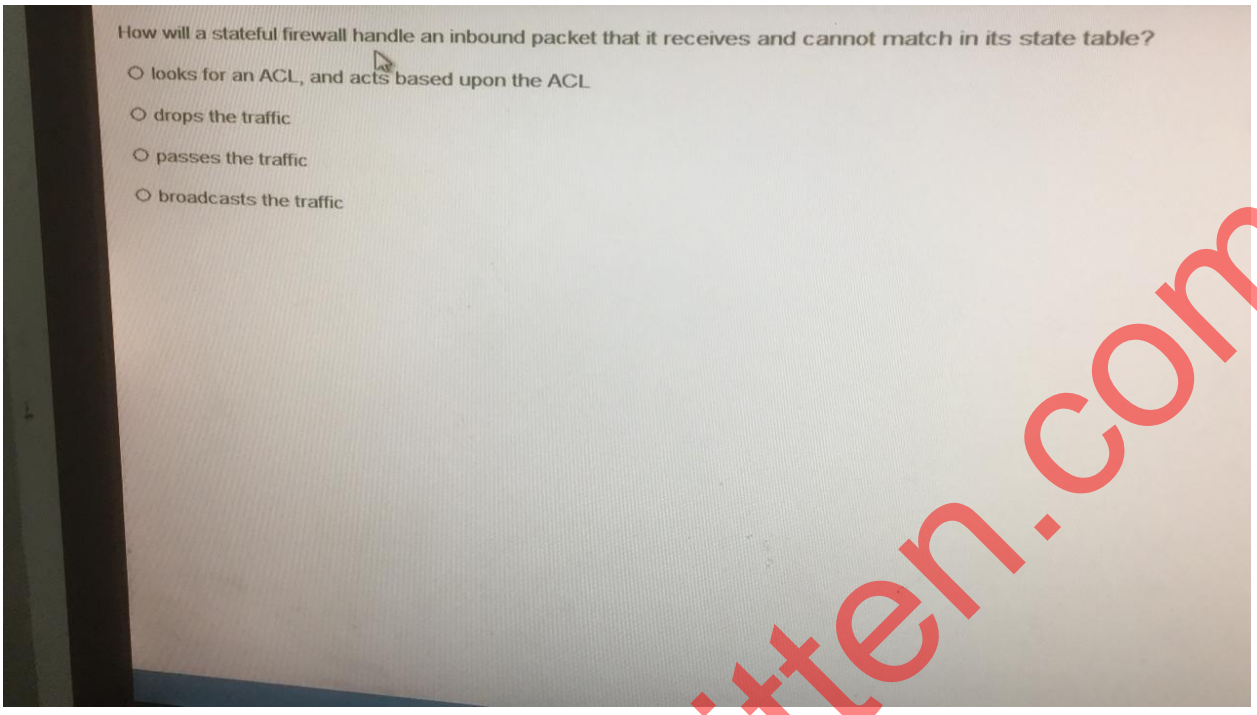
- [x] The management interface is configured in a special VRF that provides traffic isolation from the default routing table.
- [ ] Traffic isolation is done on the VLAN level.
- [ ] There is no management traffic isolation on a Cisco ASR 1002.
- [ ] Traffic is isolated based upon how you configure routing on the device.

Comment

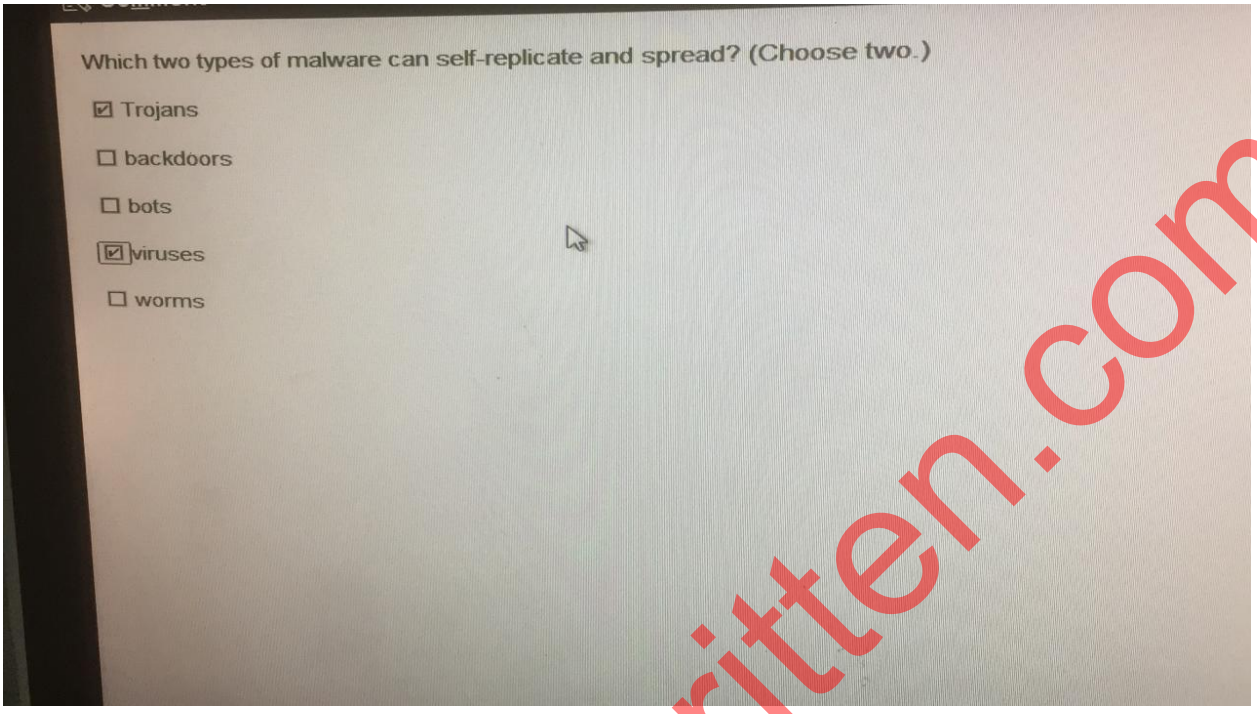
What action must you take on the ISE to blacklist a wired device?

- [ ] Locate the switch through which the device is connected and push an ACL restricting all access by the device.
- [x] Add the device's MAC address to a list of blacklisted devices.
- [ ] Revoke the device's certificate so it is unable to authenticate to the network.
- [ ] Issue a CoA request for the device's MAC address to each access switch in the network.

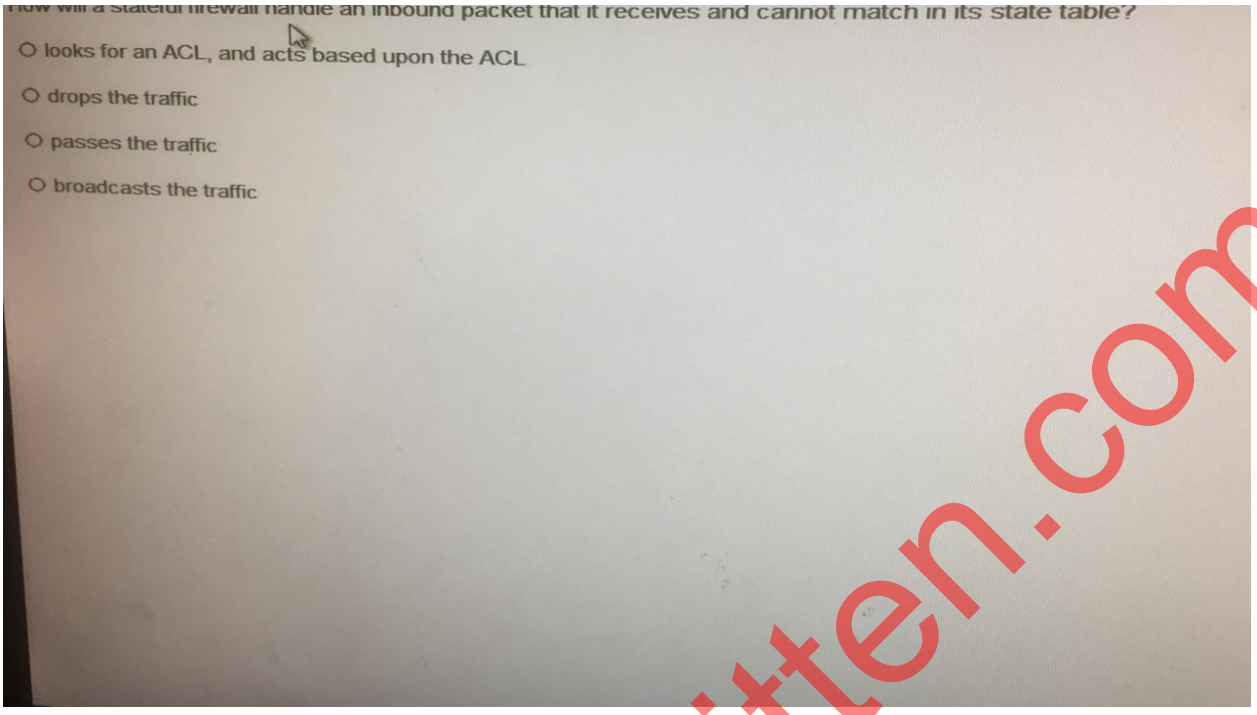




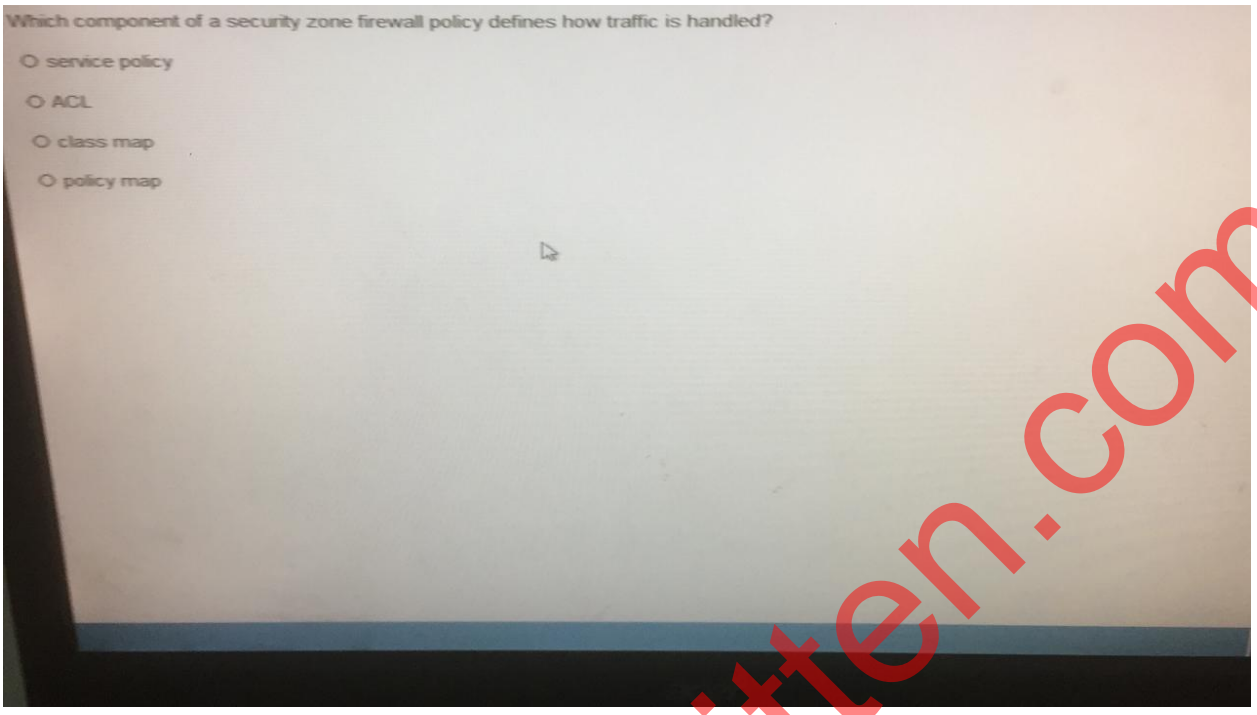

Answer is B



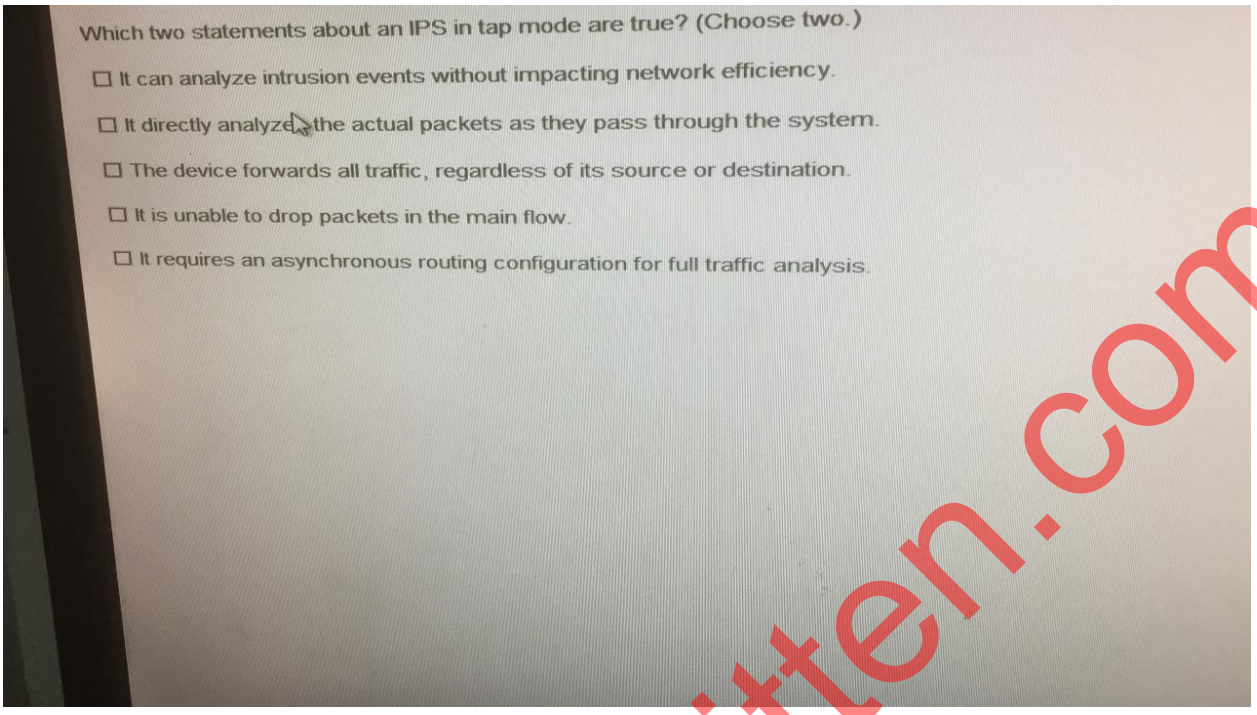

Answer are D and E



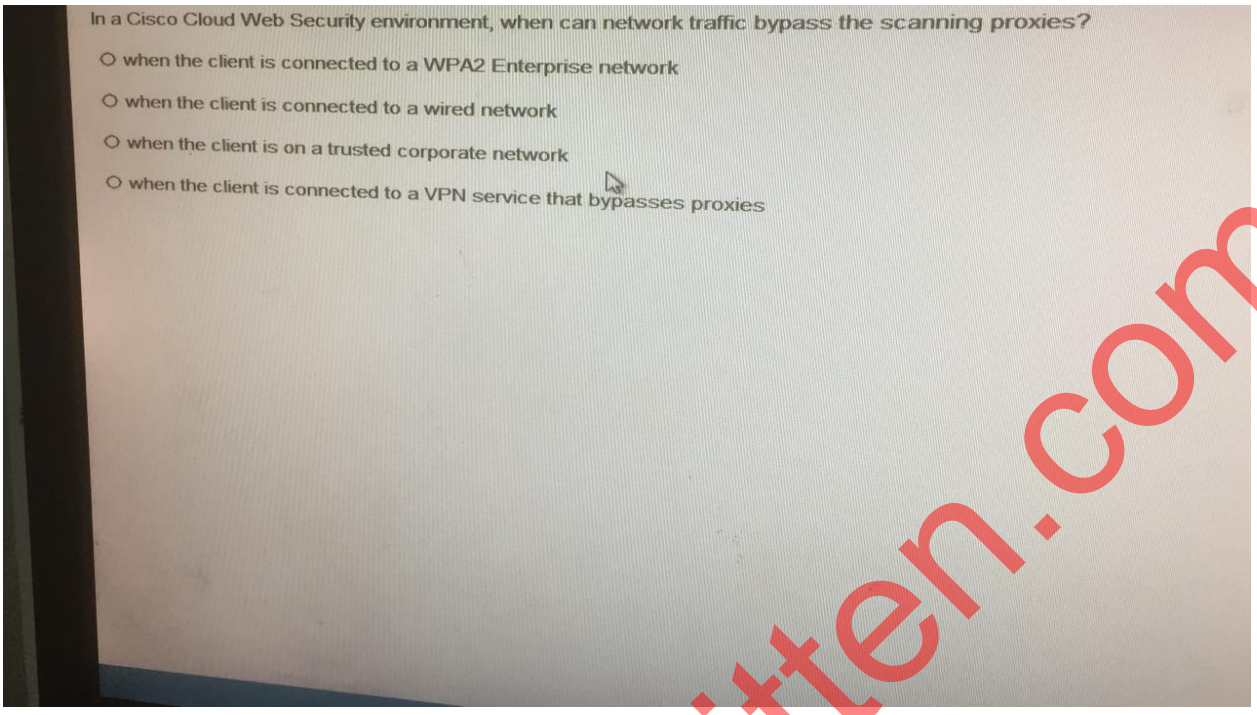

Answer is B



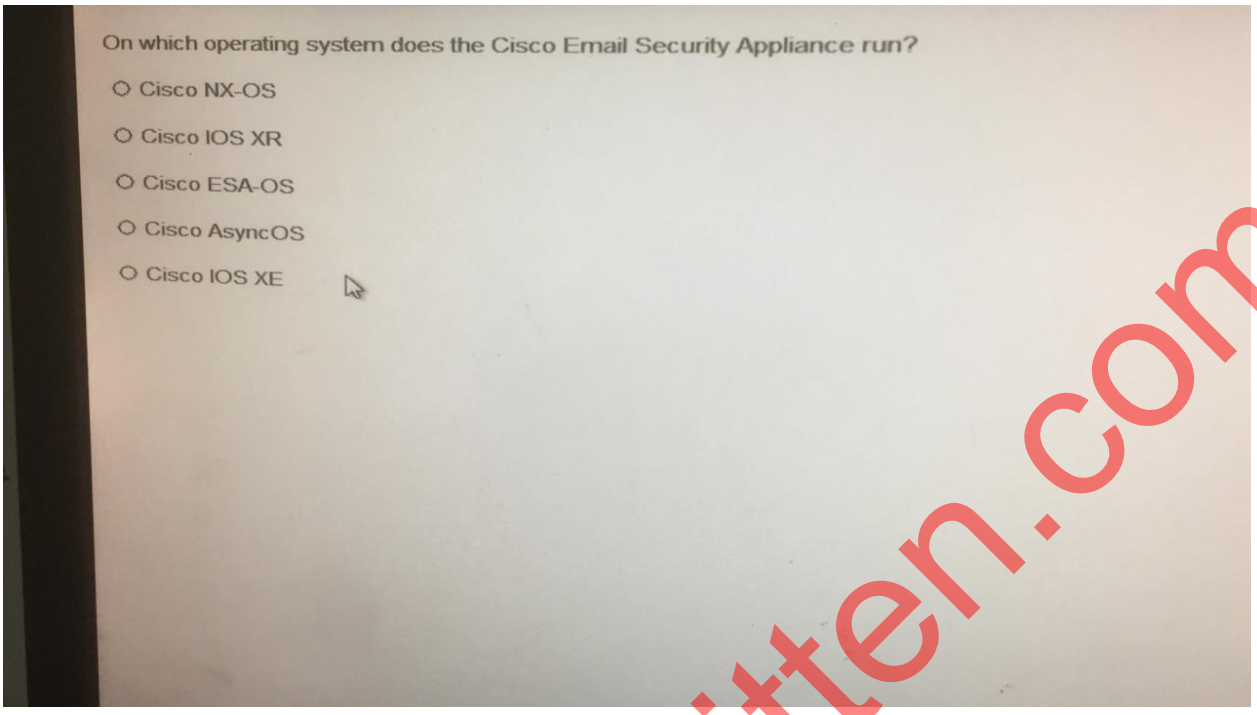

Answer is A



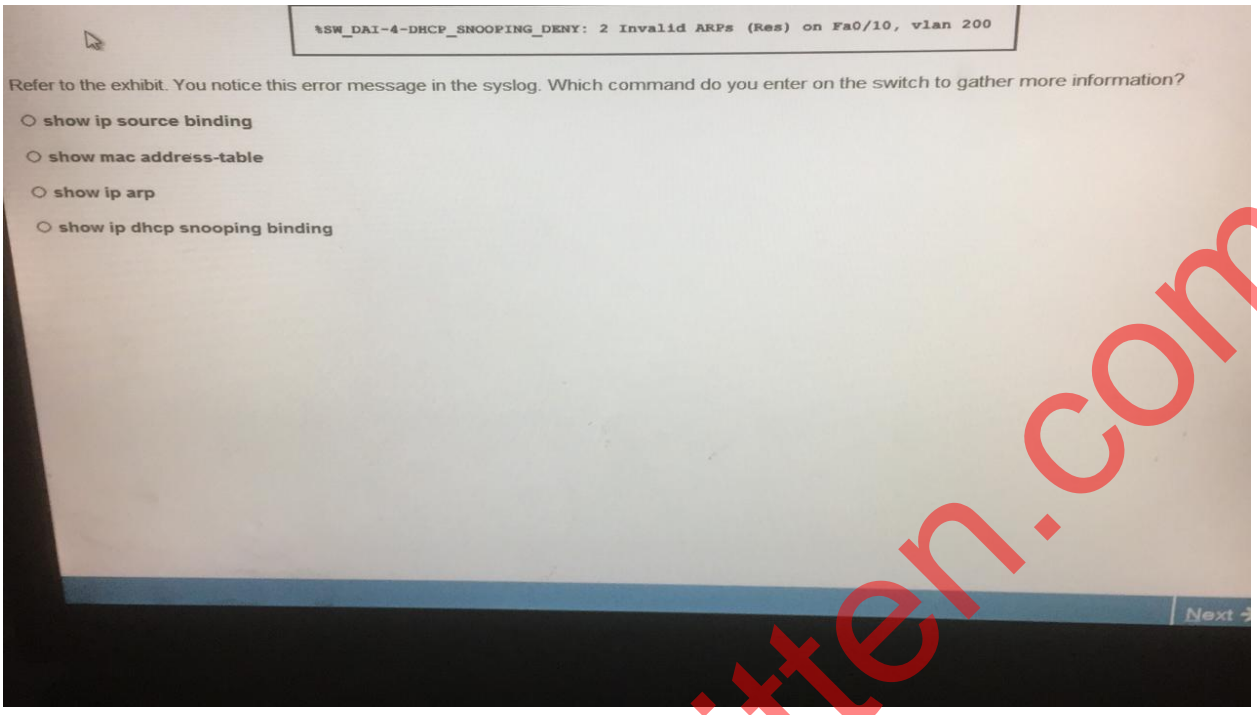

Answers are A and D



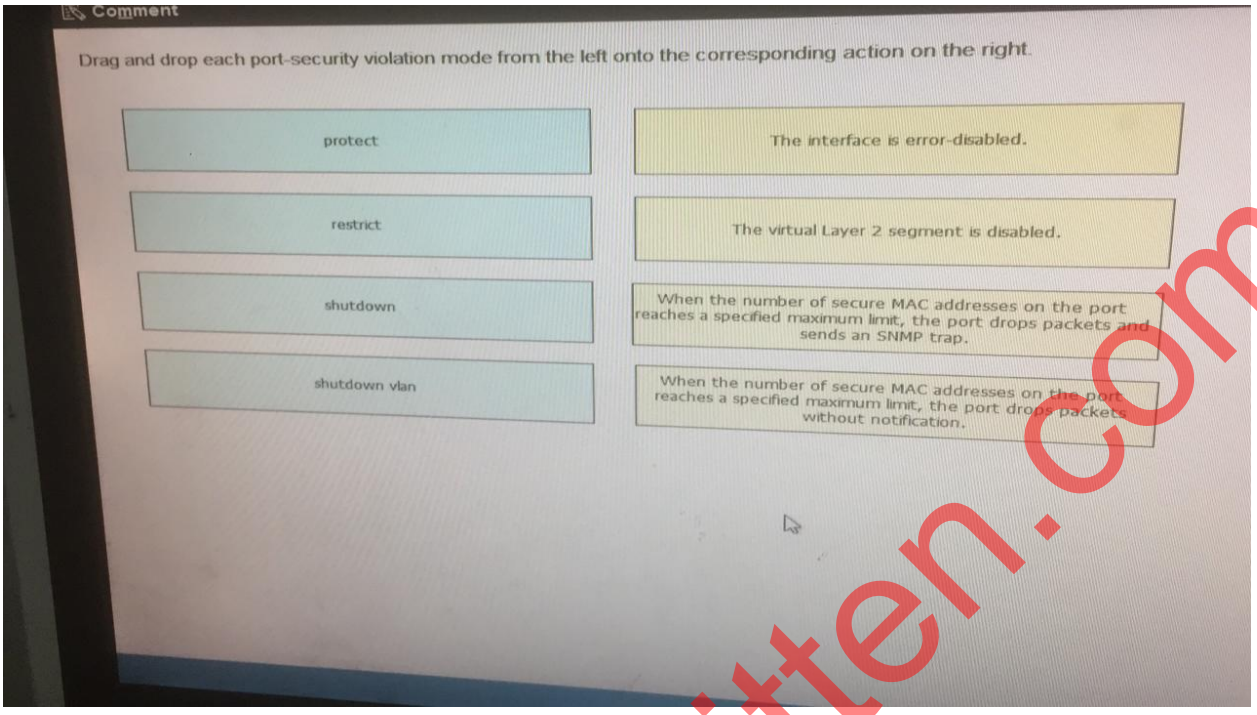

Answer is C




Answer is D




Answer is C



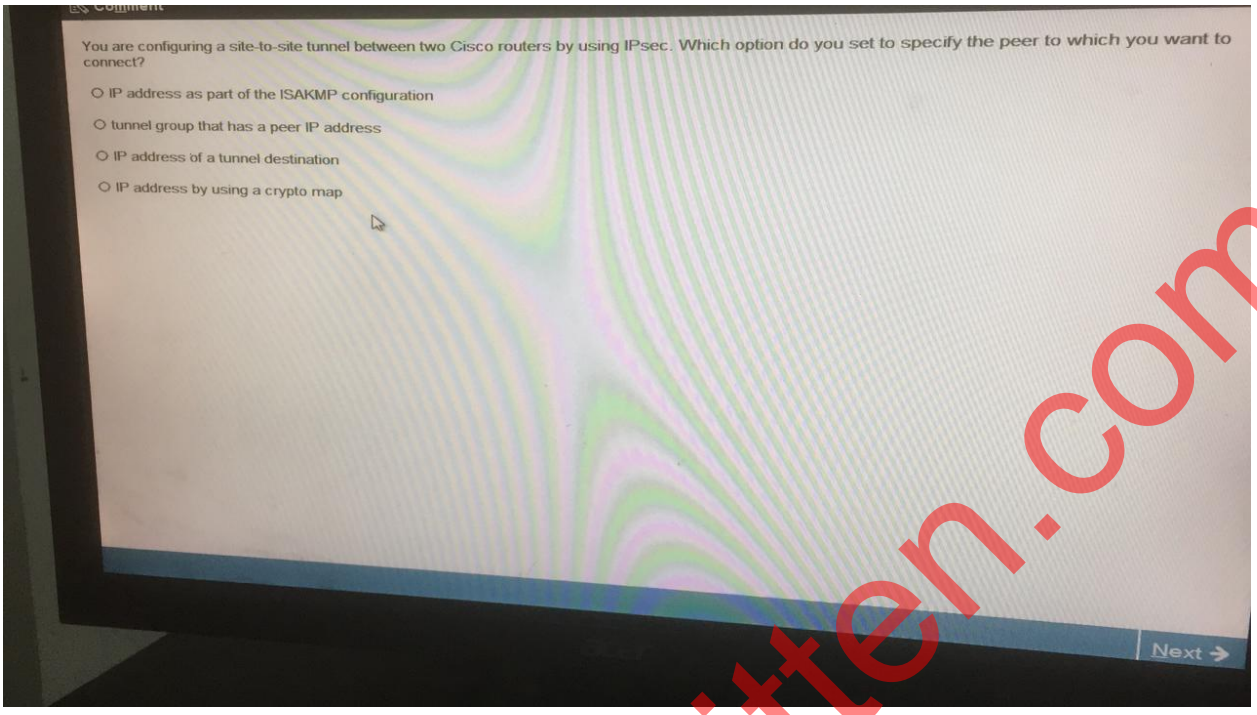

Correct sequence is given below which you have to memorize

Protect

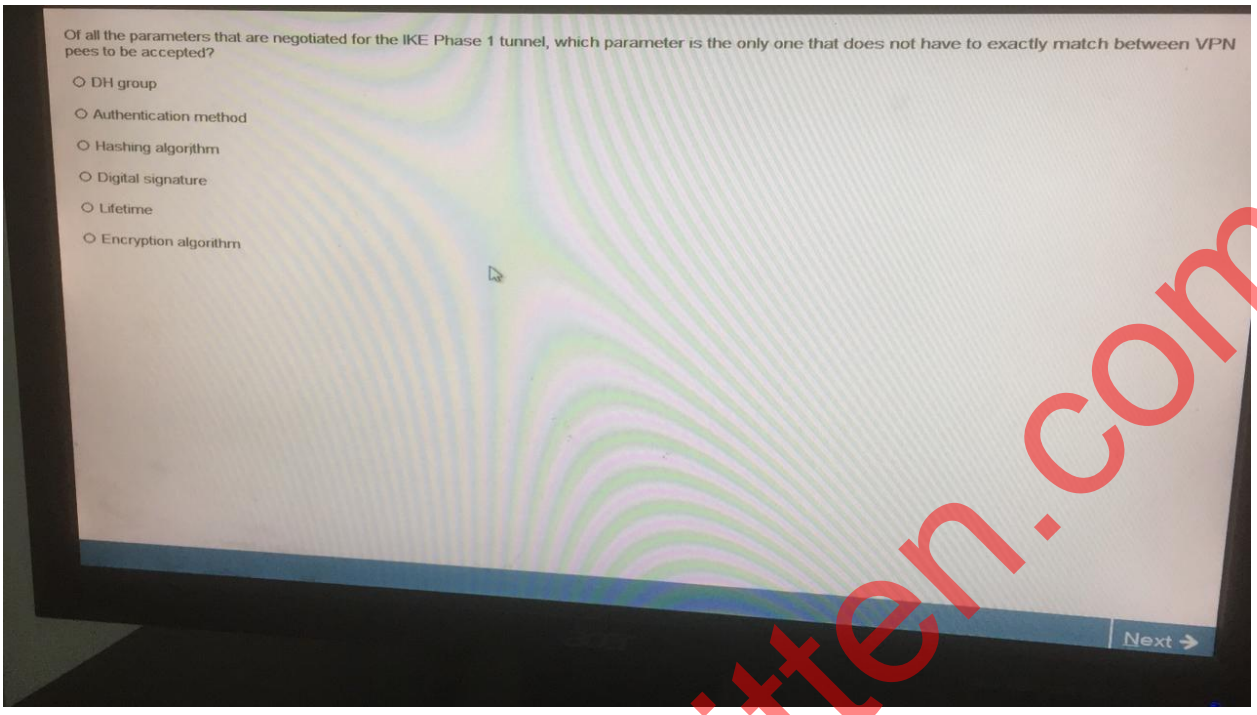
Shutdown Vlan

Restrict

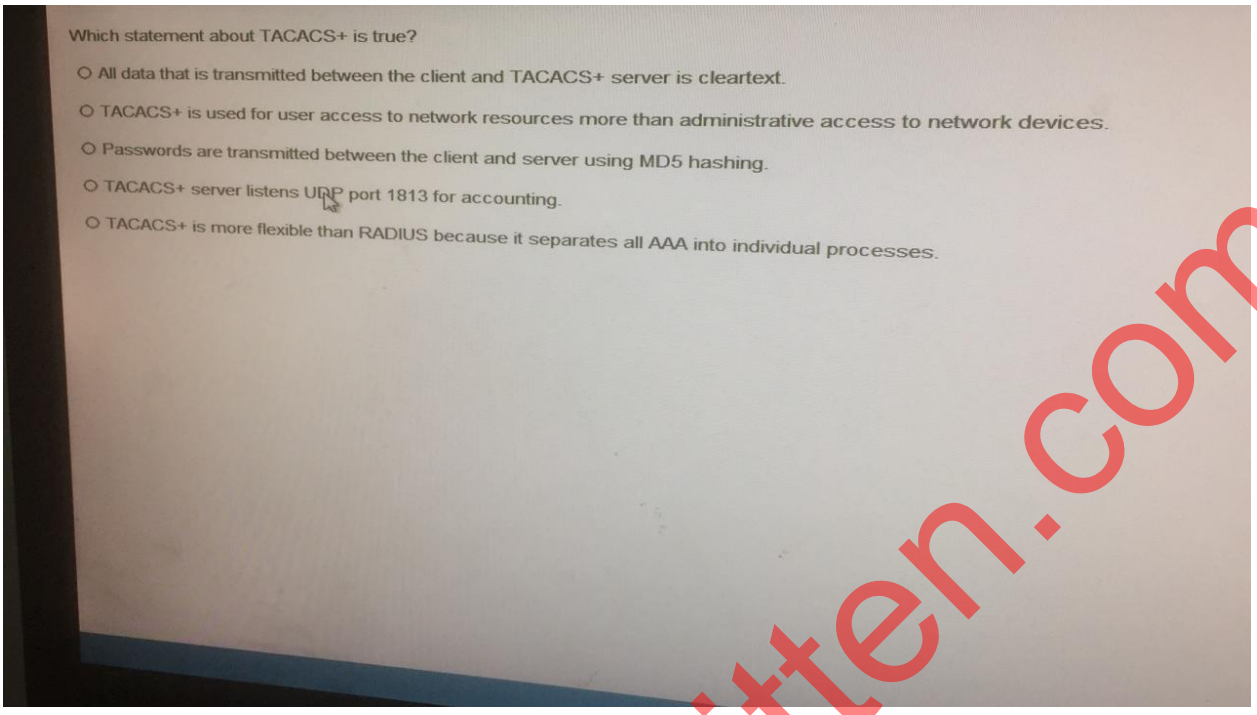
Protect



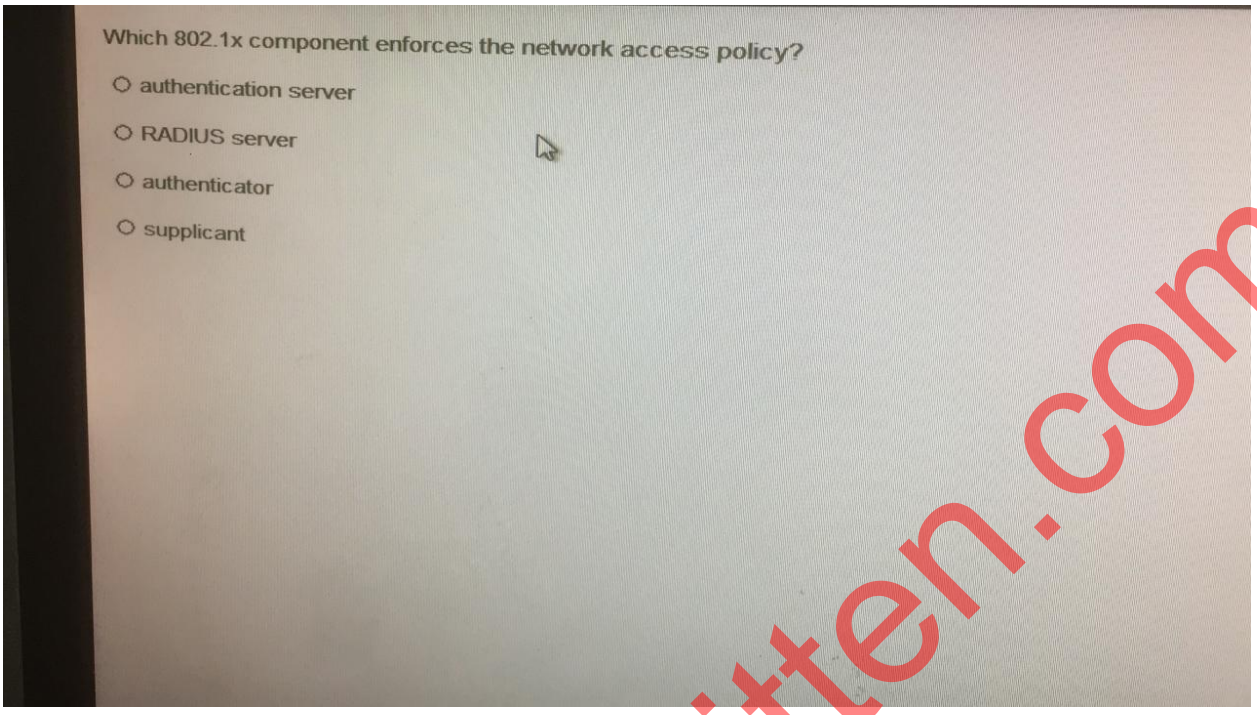

Answer is C



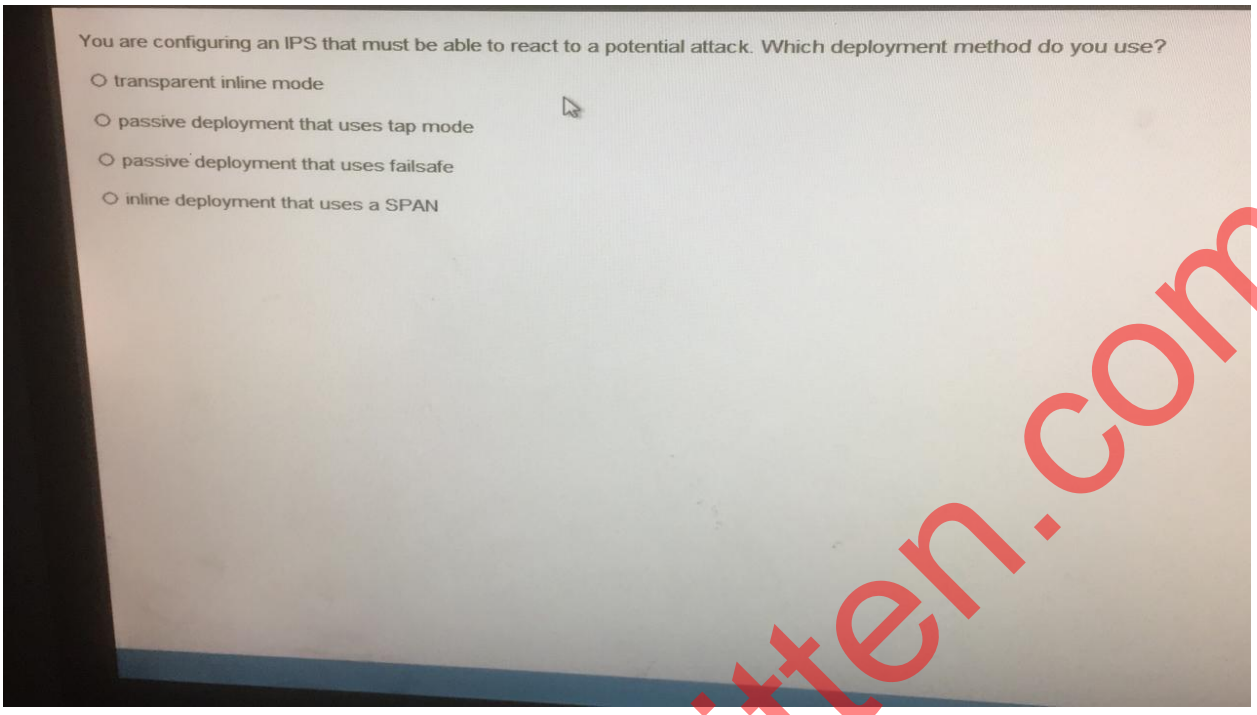

Answer is C



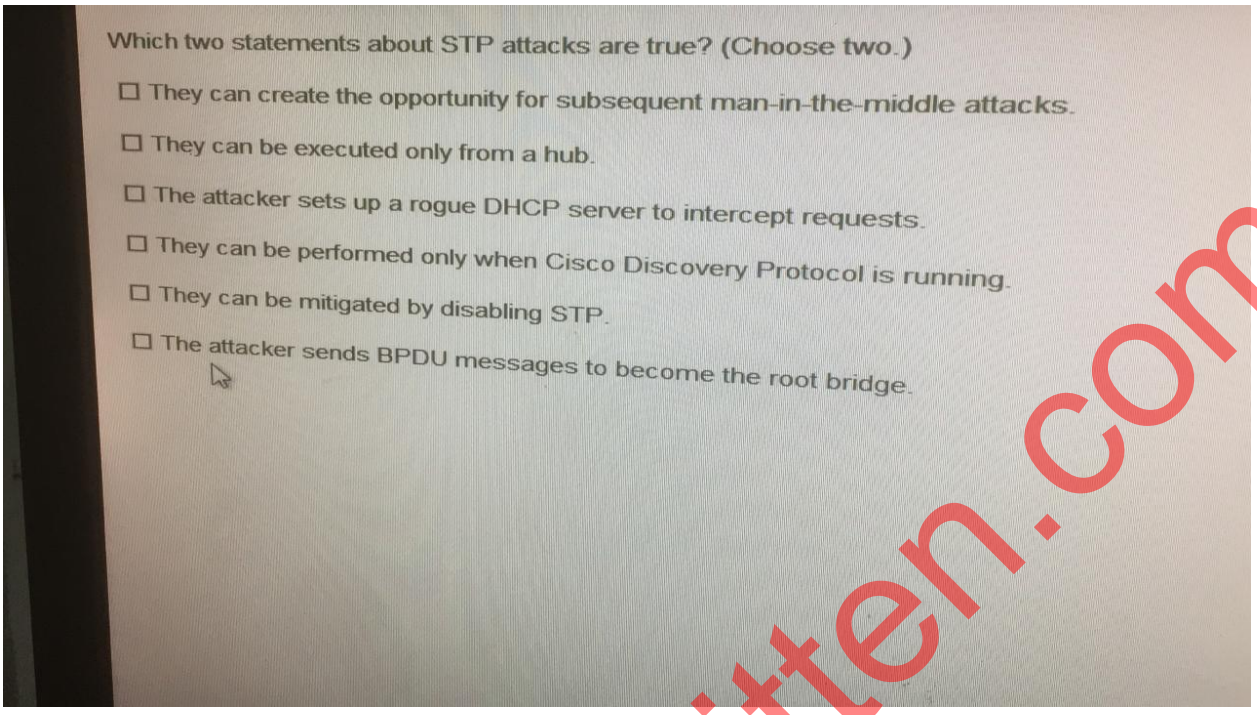

Answer is E




Answer is B




Answer is A




Answers are E and F

**1. how does the Cisco ASA use Active Directory to authorize VPN users?**

A. It queries the Active Directory server for a Specfic attribute for the specific user
B. It sends the username and password to retire an ACCEPT or Reject message from the Active Directory server
C. It downloads and stores the Active Directory databas to query for future authorization
D. It redirects requests to the Active Directory server defined for the VPN group

ANSWER:A

**2. Which three statements about host-based IPS are true? (Choose three)**

A. It can view encrypted files —> IPS cannot see encr packets, right?
B. It can be deployed at the perimeter
C. It uses signature-based policies
D. It can have more restrictive policies than network-based IPS
E. It works with deployed firewalls
F. It can generate alerts based on behavior at the desktop level.

ANSWER:ADF

**3. If a router configuration includes the lineaaa authentication login default group tacacs+ enable, which events will occur when the TACACS+ server returns an error? (Choose two.)**

A. The user will be prompted to authenticate using the enable password
B. Authentication attempts to the router will be denied
C. Authentication will use the router`s local database
D. Authentication attempts will be sent to the TACACS+ server

ANSWER:AB

**4.Which of encryption technology has the broadcast(broadest) platform support to protect operating systems?**

A. Middleware
B. Hardware
C. software
D. file-level

ANSWER:C

**5. Which technology can be used to rate data fidelity and to provide an authenticated hash for data**

A. Network blocking
B. signature updates
C. file analysis
D. file reputation

ANSWER: D

**6. Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What type of attack did your team discover**?

A. social activism
B. drive-by spyware
C. targeted malware
D. advance persistent threat
E. Polymorphic virus……

ANSWER:DE

**7. SIf the native VLAN on a trunk is different on each end of the link, what is a potential consequence?**

A. The interface on both switches may shut down
B. STP loops meway occur
C. The switch with the higher native VLAN may shut down
D. The interface with the lower native VLAN may shut down

ANSWER: B

**8. Which type of firewall can perform deep packet inspection?**

A. application firewall
B. stateless firewall
C. packet-filtering firewall
D. personal firewall

ANSWER: A

**9. When using Cisco cloud web protection, in what case proxy scanning is skipped.**

a)When connected by wired connection,
b) when connected using wpa2 connection,
c) when connected to trusted corporate network,
d) when connected via vpn with proxy scanning skipped service.

CORRECT ANSWER: C

**10. Which effect of the secure boot-image command is true?**

a. It configures the device to bot to secure IOS image
b. It displays the status of the bootset
c. It archives a secure copy of the IOS image
d. It archives a secure copy of the device configuration

ANSWER: C

**11. On which operating system does the Cisco Email Security Appliance run?**

a. Cisco IOS XR
b. Cisco IOS XE
c. Cisco AsyncOS
d. Cisco NX-OS
e. Cisco ESA-OS

ANSWER: C

**12. You are configuring an IPS that must be able to react to potential attack. Which deployment method do you use?**

a. Passive deployment that uses failsafe
b. Passive deployment that uses tap mode
c. Inline deployment that uses a SPAN
d. Transparent Inline Mode

ANSWER: D

**13. Drag and Drop**

• Shutdown – The interface is error-disabled
• Shutdown Vlan – The virtual layer 2 segment is disabled
• Restrict – When the number of secure MAC address on the port reaches a specified maximum limit, the port drops packet and sends an SNMP trap
• Protect – When the number of secure MAC addresses on the port reaches a special maximum, the port drops packets without notification.

**14. Refer to the exhibit. Your notice the error message in the syslog. Which command do you enter on the switch to gather more information?**

**%SW_DAI-4-DHCP_SNOOPING _DENY: 2 invalid ARPs (Res) on Fa0/10, Vlan 200.**

a. Show ip dhcp snooping binding
b. Show mac address-table
c. Show ip arp
d. Show ip source binding

ANSWER: A

**15. Which two statement about STP attacks are true?(choose two)**

a. The attacker sets up a rogue DHCP server to intercept requests
b. They can be performed only when Cisco Discovery protocol Is running
c. Then can mitigate by disabling STP
d. They can create the opportunity for subsequent man-in-the middle attacks
e. The attacker sends BPDU messages to become the root bridge
f. They can be executed only from a hub

ANSWER: DE

**16.Which statement about TACACS+ is true**

a. TACACS+ is used for user access to network resources more than administrative access to network devices
b.All data that is transmitted between the client and TACACS+ Server Is cleartext
c. TACACS+ server listens UDP port 1813 for accounting
d. TACACS+ is more flexible than RADIUS because it separates all AAA into individual process
e. Password are transmitted between the client and server using MD5 hashing

ANSWER: D

**17.You are configuring a site-to-site tunnel between two cisco routers by using IPsec. Which option do you set to specify the peer to which you want to connect?**

a. IP address by using a crypto map
b. IP address of tunnel destination
c. Tunnel group that has a peer P address
d. IP address as part of the ISAKMP configuration

ANSWER: A

**18. What type of malware spread and infects:(choose two)**

a) bot
b) torjan
c) virus
d) worm
e) backdoor

ANSWER: D, A?

**19. How can you mitigate DCE/RPC evasion techniques while allowing access to the DCE/RPC service?**

A. Update the IPS signature for HTTPS to validate DCE/RPC connections.
B. Block suspicious hosts from DCE/RPC port 593.
C. Tunnel DCE/RPC traffic through GRE.
D. Configure the DCE/RPC preprocessor.

Answer: B , D?

**20. Which 802.1x component enforces the network access policy?**

a. RADIUS Server
b. Authentication server
c. Supplicant
d. Authenticator

ANSWER: D