Exam : **642-825**

Title : Implementing Secure Converged Wide Area Networks

Version : Demo

1.What are three methods of network reconnaissance? (Choose three.)
A.IP spoofing
B.one-time password
C.dictionary attack
D.packet sniffer
E.ping sweep
F.port scan
Answer:D E F

2.Which three statements are correct about MPLS-based VPNs? (Choose three.)
A.Route Targets (RTs) are attributes attached to a VPNv4 BGP route to indicate its VPN membership.
B.Scalability becomes challenging for a very large, fully meshed deployment.
C.Authentication is done using a digital certificate or pre-shared key.
D.A VPN client is required for client-initiated deployments.
E.A VPN client is not required for users to interact with the network.
F.An MPLS-based VPN is highly scalable because no site-to-site peering is required.
Answer:A E F

3.What are two steps that must be taken when mitigating a worm attack? (Choose two.)
A.Inoculate systems by applying update patches.
B.Limit traffic rate.
C.Apply authentication.
D.Quarantine infected machines.
E.Enable anti-spoof measures
Answer:A D

4.Refer to the exhibit. What information can be derived from the SDM firewall configuration that is shown?

```
Router# show running-config | include access-list
access-list 100 remark Autogenerated by SDM firewall configuration
access-list 100 remark SDM_ACL Category=1
access-list 100 deny   ip 200.0.0.0 0.0.0.3 any
access-list 100 deny   ip host 255.255.255.255 any
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
access-list 101 remark Autogenerated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 deny   ip 10.1.1.0 0.0.0.255 any
access-list 101 permit icmp any host 200.0.0.1 echo-reply
access-list 101 permit icmp any host 200.0.0.1 time-exceeded
access-list 101 permit icmp any host 200.0.0.1 unreachable
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip host 0.0.0.0 any
access-list 101 deny   ip any any log
```

A.Access-list 100 was configured for the trusted interface, and access-list 101 was configured for the untrusted interface.
B.Access-list 101 was configured for the trusted interface, and access-list 100 was configured for the untrusted interface.
C.Access-list 100 was configured for the inbound direction, and access-list 101 was configured for the outbound direction on the trusted interface.
D.Access-list 100 was configured for the inbound direction, and access-list 101 was configured for the outbound direction on the untrusted interface.
Answer:A

5.Which three statements about IOS Firewall configurations are true? (Choose three.)
A.The IP inspection rule can be applied in the inbound direction on the secured interface.
B.The IP inspection rule can be applied in the outbound direction on the unsecured interface.
C.The ACL applied in the outbound direction on the unsecured interface should be an extended ACL.
D.The ACL applied in the inbound direction on the unsecured interface should be an extended ACL.
E.For temporary openings to be created dynamically by Cisco IOS Firewall, the access-list for the returning traffic must be a standard ACL.
F.For temporary openings to be created dynamically by Cisco IOS Firewall, the IP inspection rule must be applied to the secured interface.
Answer:A B D

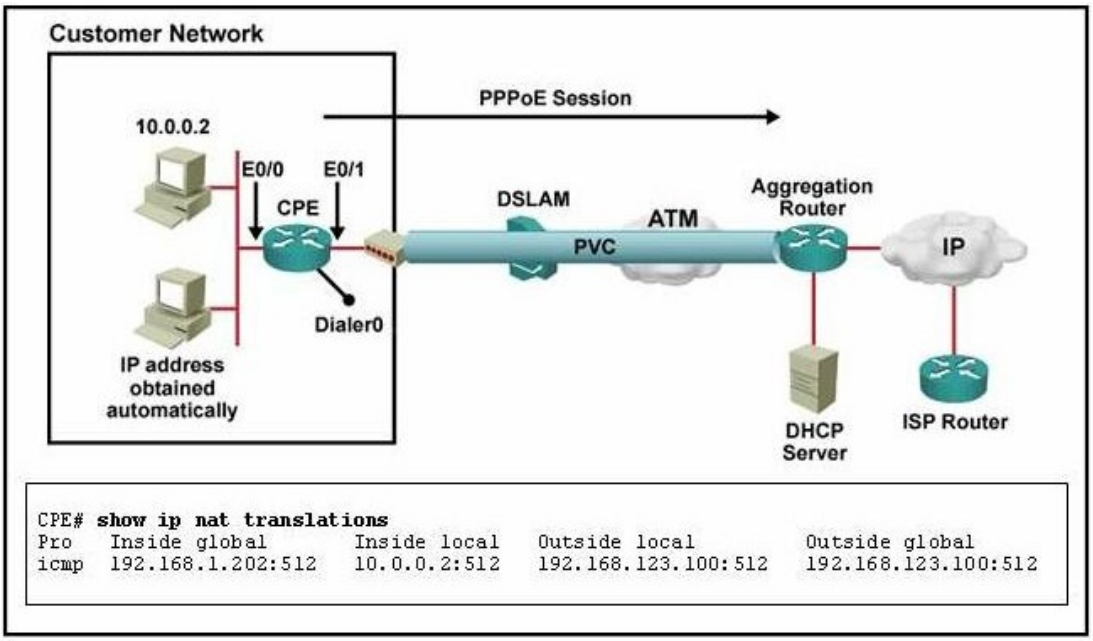
6.Which statement describes the Authentication Proxy feature?
A.All traffic is permitted from the inbound to the outbound interface upon successful authentication of the user.
B.A specific access profile is retrieved from a TACACS+ or RADIUS server and applied to an IOS Firewall based on user provided credentials.
C.Prior to responding to a proxy ARP, the router will prompt the user for a login and password which are authenticated based on the configured AAA policy.
D.The proxy server capabilities of the IOS Firewall are enabled upon successful authentication of the user.
Answer:B

7.Refer to the exhibit. Which two statements are true about the authentication method used to authenticate users who want privileged access into Router1? (Choose two.)

```
hostname Router1
!
username Router1 password cisco
!
aaa new-model
aaa authentication login default group radius local
!
<output omitted>
!
line con 0
exec-timeout 0 0
password cisco
!
<output omitted>
```

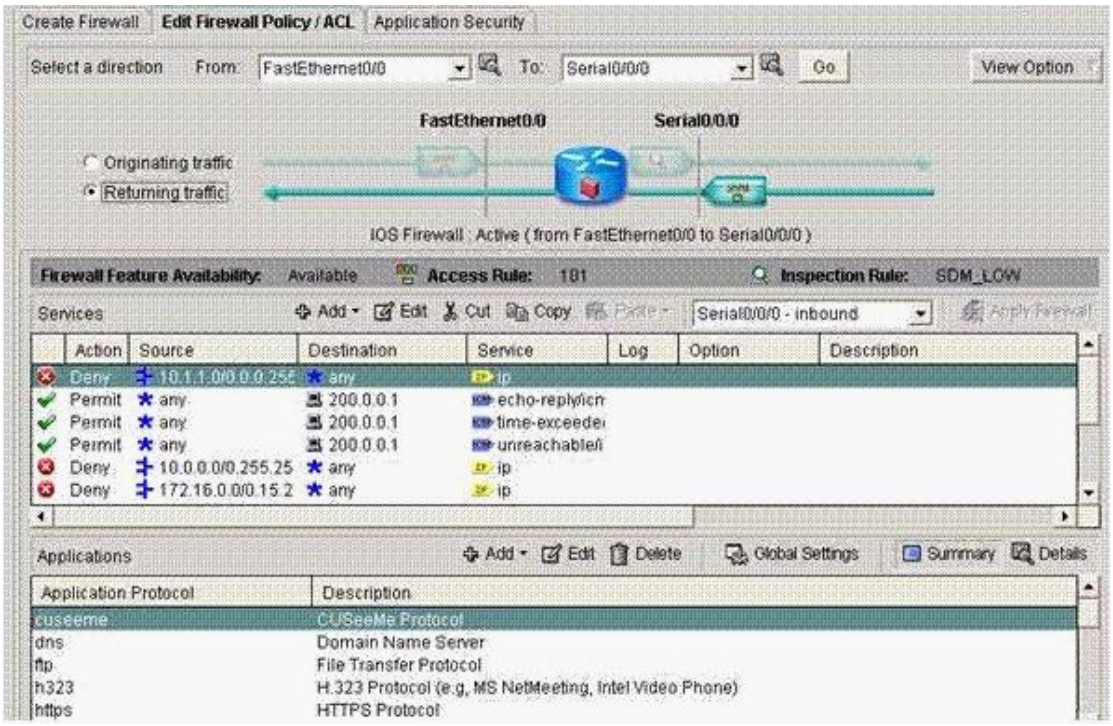
A.All users will be authenticated using the RADIUS server. If the RADIUS server is unavailable, the router will attempt to authenticate the user using its local database.
B.All users will be authenticated using the RADIUS server. If the RADIUS server is unavailable, the authentication process stops and no other authentication method is attempted.
C.All users will be authenticated using the RADIUS server. If the user authentication fails, the router will attempt to authenticate the user using its local database.
D.All users will be authenticated using the RADIUS server. If the user authentication fails, the authentication process stops and no other authentication method is attempted.
E.The default login authentication method is applied automatically to all lines including console, auxiliary, TTY, and VTY lines.
Answer:A D

8.Refer to the exhibit. On the basis of the presented information, which configuration was completed on the router CPE?



A.CPE(config)# ip nat inside source list 101 interface Dialer0
CPE(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255 any
B.CPE(config)# ip nat inside source list 101 interface Dialer0 overload
CPE(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255 any
C.CPE(config)# ip nat inside source list 101 interface Ethernet 0/0
CPE(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255 any
D.CPE(config)# ip nat inside source list 101 interface Ethernet 0/0 overload
CPE(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255 any
E.CPE(config)# ip nat inside source list 101 interface Ethernet 0/1
CPE(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255 any
F.CPE(config)# ip nat inside source list 101 interface Ethernet 0/1 overload
CPE(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255 any
Answer:B

9.Refer to the exhibit. FastEthernet0/0 has been assigned a network address of 200.0.1.2/24 and no ACL has been applied to that interface. Serial0/0/0 has been assigned a network address of 200.0.0.1/30. Assuming that there are no network-related problems, which ping will be successful?



A.from 200.0.0.1 to 200.0.0.2
B.from 200.0.0.2 to 200.0.0.1
C.from 200.0.0.2 to 200.0.1.1
D.from 200.0.0.2 to 200.0.1.2
E.from 200.0.1.1 to 200.0.0.2
F.from 200.0.1.2 to 200.0.0.2
Answer:A

10.If an edge Label Switch Router (LSR) is properly configured, which three combinations are possible? (Choose three.)
A.A received IP packet is forwarded based on the IP destination address and the packet is sent as an IP packet.
B.An IP destination exists in the IP forwarding table. A received labeled packet is dropped because the label is not found in the LFIB table.
C.There is an MPLS label-switched path toward the destination. A received IP packet is dropped because the destination is not found in the IP forwarding table.
D.A received IP packet is forwarded based on the IP destination address and the packet is sent as a labeled packet.
E.A received labeled IP packet is forwarded based upon both the label and the IP address.
F.A received labeled packet is forwarded based on the label. After the label is swapped, the newly labeled packet is sent.
Answer:A D F

11.Which approach for identifying malicious traffic involves looking for a fixed sequence of bytes in a single packet or in predefined content?
A.policy-based

B.anomaly-based
C.honeypot-based
D.signature-based
E.regular-expression-based
Answer:D

12.Which three DSL technologies support an analog POTS channel and utilize the entire bandwidth of the copper to carry data? (Choose three.)
A.ADSL
B.IDSL
C.SDSL
D.RADSL
E.VDSL
Answer:A D E

13.Refer to the exhibit. On the basis of the information that is provided, which statement is true?

```
FWRouter# show ip inspect session detail

Established Sessions
 Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
   Created 00:00:08, Last heard 00:00:04
   Bytes sent (initiator:responder) [140:298] acl created 2
   Outgoing access-list 102 applied to interface FastEthernet0/0
   Inbound access-list 101 applied to interface FastEthernet0/1

FWRouter# show access-lists

Extended IP access list 101
    permit tcp host 192.168.101.115 eq telnet host 192.168.1.116 eq 32956 (27  matches)
    deny udp any any
    deny tcp any any
    permit ip any any

Extended IP access list 102
    permit tcp host 192.168.101.115 eq telnet host 192.168.1.116 eq 32956 (27 matches)
    deny udp any any
    deny tcp any any
    permit ip any any
```

A.The IOS firewall has allowed an HTTP session between two devices.
B.A TCP session that started between 192.168.1.116 and 192.168.101.115 caused dynamic ACL entries to be created.
C.A UDP session that started between 192.168.1.116 and 192.168.101.115 caused dynamic ACL entries to be created.
D.Telnet is the only protocol allowed through this IOS firewall configuration.
Answer:B

14.Refer to the exhibit. What Cisco feature generated the configuration?

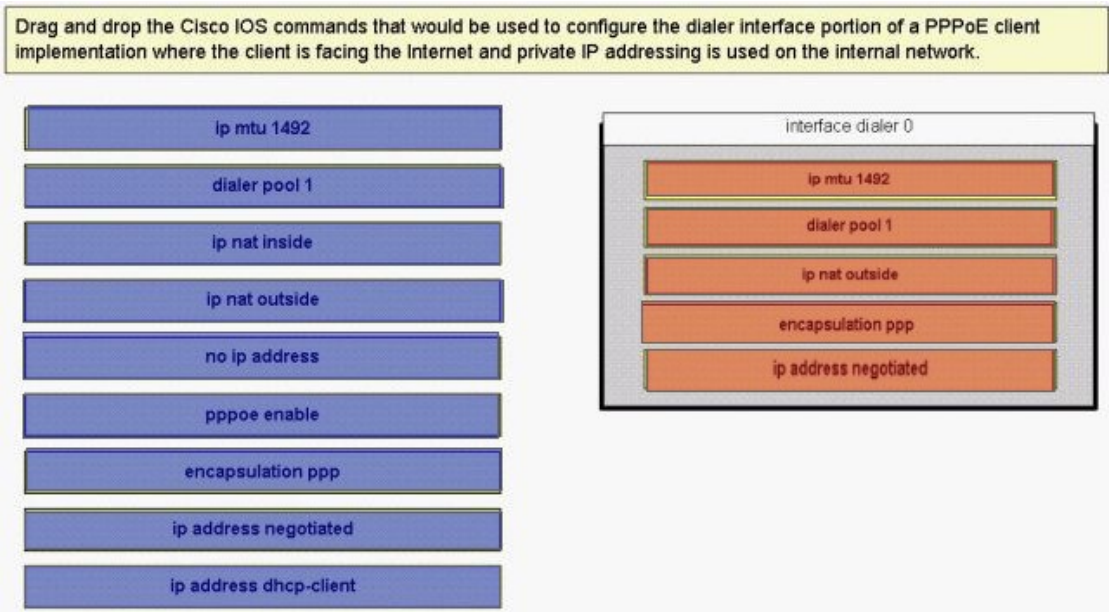
```
enable secret 5 $1$270i$BF/ftKAvuEzue3kfdikyP.
enable password 7 1414110209082722
username ccie password 7 08224F470C1A061E17
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
login block-for 60 attempts 3 within 5
hostname amos_eaton
ip domain-name amos_eaton.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
```

A.EZ VPN
B.IOS Firewall
C.AutoSecure
D.IOS IPS
E.AAA
F.TACACS+
Answer:C

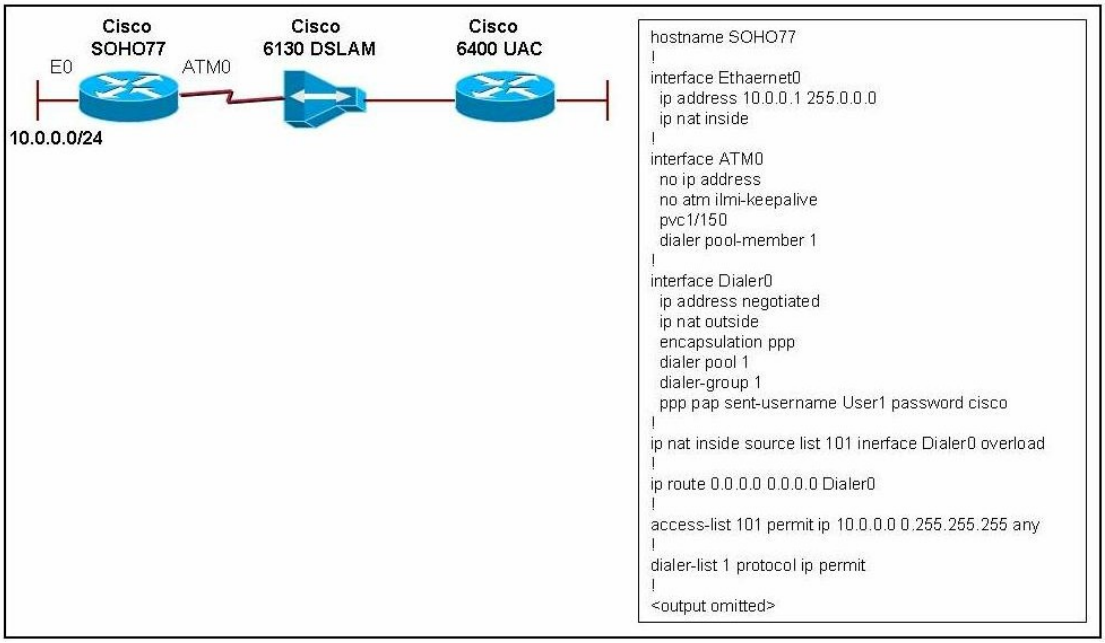
15.What are three features of the Cisco IOS Firewall feature set? (Choose three.)
A.network-based application recognition (NBAR)
B.authentication proxy
C.stateful packet filtering
D.AAA services
E.proxy server
F.IPS

Answer:B C F

16.Drop



17.Refer to the exhibit, which shows a PPPoA diagram and partial SOHO77 configuration. Which command needs to be applied to the SOHO77 to complete the configuration?



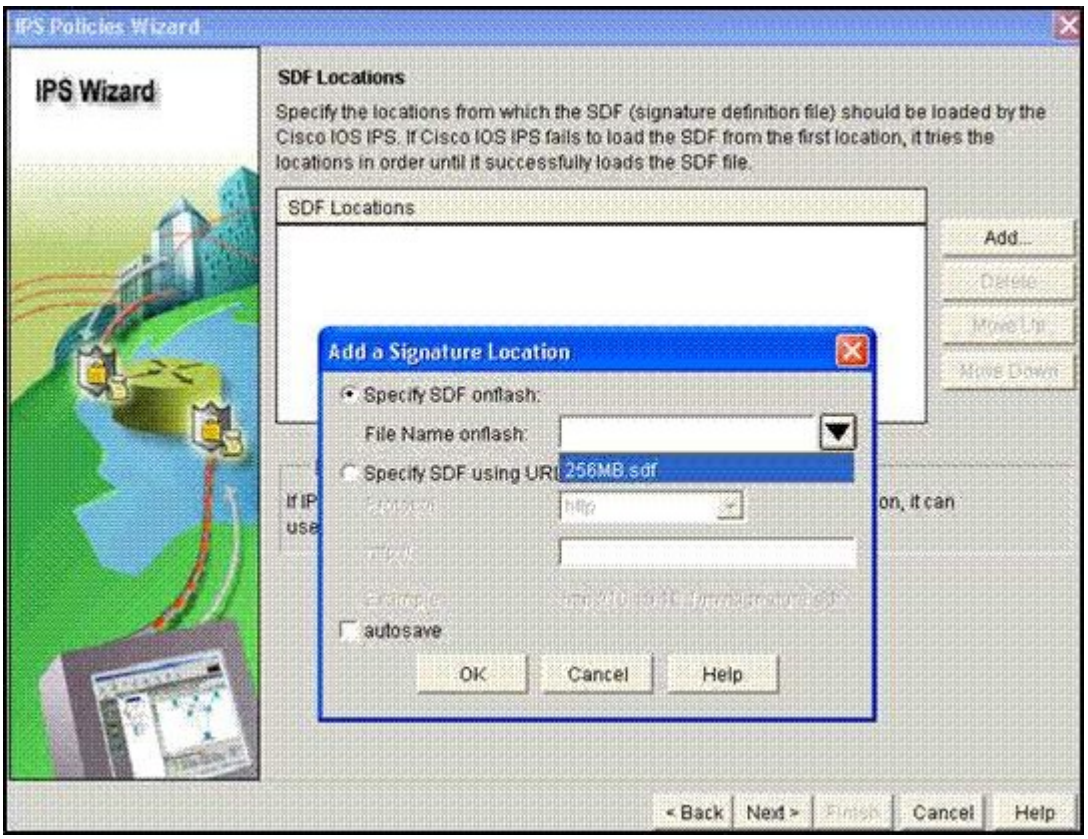
A.encapsulation aal5snap applied to the PVC.
B.encapsulation aal5ciscoppp applied to the PVC
C.encapsulation aal5ciscoppp applied to the ATM0 interface
D.encapsulation aal5mux ppp dialer applied to the ATM0 interface
E.encapsulation aal5mux ppp dialer applied to the PVC
Answer:E

18.Which three techniques should be used to secure management protocols? (Choose three.)
A.Configure SNMP with only read-only community strings.
B.Encrypt TFTP and syslog traffic in an IPSec tunnel.
C.Implement RFC 2827 filtering at the perimeter router when allowing syslog access from devices on the outside of a firewall.
D.Synchronize the NTP master clock with an Internet atomic clock.
E.Use SNMP version 2.
F.Use TFTP version 3 or above because these versions support a cryptographic authentication mechanism between peers.
Answer:A B C

19.Which two active response capabilities can be configured on an intrusion detection system (IDS) in response to malicious traffic detection? (Choose two.)
A.the initiation of dynamic access lists on the IDS to prevent further malicious traffic
B.the configuration of network devices to prevent malicious traffic from passing through
C.the shutdown of ports on intermediary devices
D.the transmission of a TCP reset to the offending end host
E.the invoking of SNMP-sourced controls
Answer:B D

20.What are three objectives that the no ip inspect command achieves? (Choose three.)
A.removes the entire CBAC configuration
B.removes all associated static ACLs
C.turns off the automatic audit feature in SDM
D.denies HTTP and Java applets to the inside interface but permits this traffic to the DMZ
E.resets all global timeouts and thresholds to the defaults
F.deletes all existing sessions
Answer:A E F

21.Refer to the exhibit. Which statement describes the results of clicking the OK button in the Security Device Manager (SDM) Add a Signature Location window?



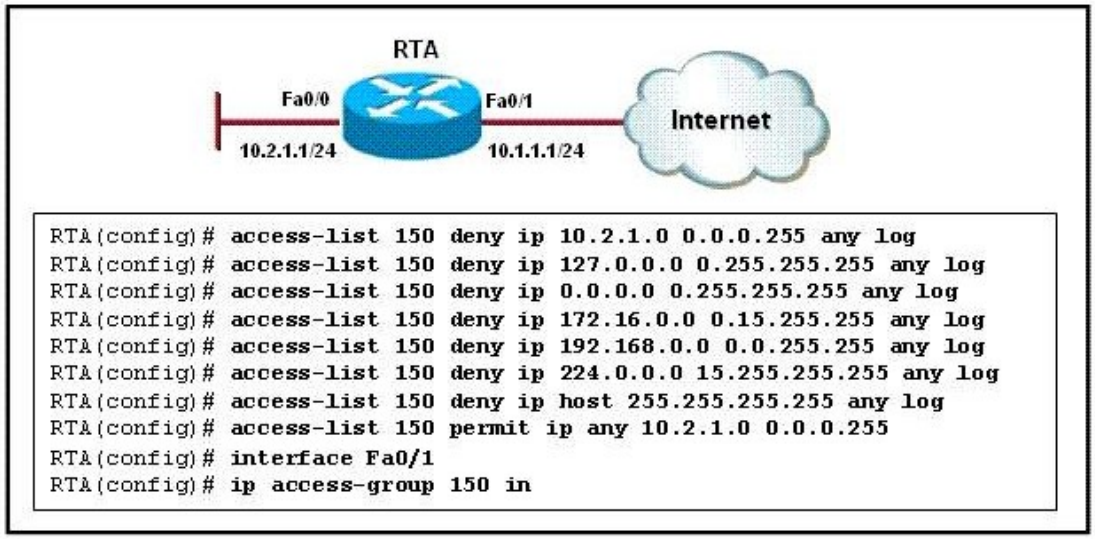
A.SDM will respond with a message asking for the URL that points to the 256MB.sdf file.
B.Cisco IOS IPS will choose to load the 256MB.sdf only if the Built-in Signatures (as backup) check box is unchecked.
C.If Cisco IOS IPS fails to load the 256MB.sdf, it will load the built-in signatures provided the Built-in Signatures (as backup) check box is checked.
D.Cisco IOS IPS will choose to load the 256MB.sdf and then also add the Cisco IOS built-in signatures.
E.SDM will respond with an error that indicates that no such file exists.
Answer:C

22.Which statement is true about a worm attack?
A.Human interaction is required to facilitate the spread.
B.The worm executes arbitrary code and installs copies of itself in the memory of the infected computer.
C.Extremely large volumes of requests are sent over a network or over the Internet.
D.Data or commands are injected into an existing stream of data. That stream is passed between a client and server application.
Answer:B

23.Which three categories of signatures can a Cisco IPS microengine identify? (Choose three.)
A.DDoS signatures
B.strong signatures
C.exploit signatures
D.numeric signatures
E.spoofing signatures
F.connection signatures

Answer:A C F

24.Refer to the exhibit. ACL 150 was configured on Router RTA to mitigate against a range of common threats. On the basis of the information in the exhibit, which statement is true?



A.ACL 150 will mitigate common threats.
B.Interface Fa0/0 and interface Fa0/1 should have been configured with the IP addresses 10.1.1.1 and 10.2.1.1, respectively.
C.The ip access-group 150 command should have been applied to interface FastEthernet 0/0 in an inbound direction.
D.The ip access-group 150 command should have been applied to interface FastEthernet 0/0 in an outbound direction.
E.The ip access-group 150 command should have been applied to interface FastEthernet 0/1 in an outbound direction.
F.The last statement in ACL 150 should have been access-list 150 permit tcp 10.2.1.0 0.0.0.255 any established.
Answer:A

25.Which form of DSL technology is typically used as a replacement for T1 lines?
A.VDSL
B.HDSL
C.ADSL
D.SDSL
E.G.SHDSL
F.IDSL
Answer:B

26.Which two statements are true about broadband cable (HFC) systems? (Choose two.)
A.Cable modems only operate at Layer 1 of the OSI model.
B.Cable modems operate at Layers 1 and 2 of the OSI model.
C.Cable modems operate at Layers 1, 2, and 3 of the OSI model.

D.A function of the cable modem termination system (CMTS) is to convert the modulated signal from the cable modem into a digital signal.
E.A function of the cable modem termination system is to convert the digital data stream from the end user host into a modulated RF signal for transmission onto the cable system.
Answer:B D

27.Refer to the exhibit. On the basis of the information presented, which configuration change would correct the Secure Shell (SSH) problem?

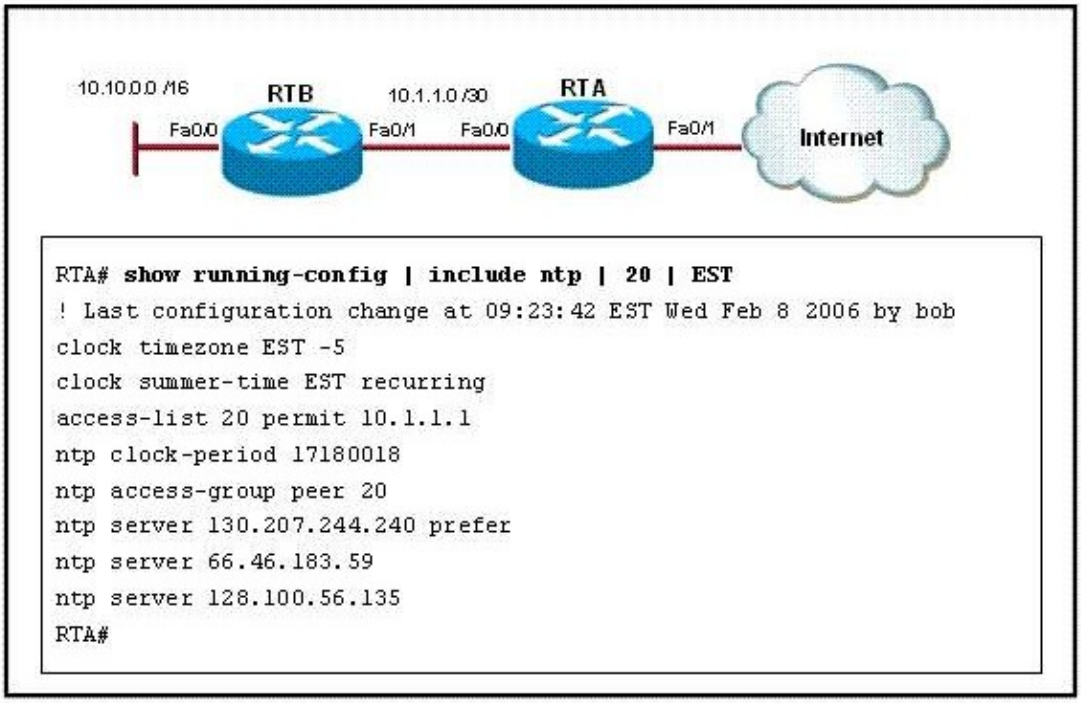
```
RTA# debug ip ssh
Incoming SSH debugging is on
RTA#
*Mar  1 00:18:39.277: SSH: Could not get a vty line for incoming session
```

A.Configure router RTA with the ip domain name domain-name global configuration command.
B.Configure router RTA with the crypto key generate rsa general-keys modulus modulus-number global configuration command.
C.Configure router RTA with the crypto key generate rsa usage-keys modulus modulus-number global configuration command.
D.Configure router RTA with the transport input ssh vty line configuration command.
E.Configure router RTA with the no transport input telnet vty line configuration command.
Answer:D

28.Which statement is true about the management protocols?
A.TFTP data is sent encrypted.
B.Syslog data is sent encrypted between the server and device.
C.SNMP v1/v2 can be compromised because the community string information for authentication is sent in clear text.
D.NTP v.3 does not support a cryptographic authentication mechanism between peers.
Answer:C

29.Which PPPoA configuration statement is true?
A.The dsl operating-mode auto command is required if the default mode has been changed.
B.The encapsulation ppp command is required.
C.The ip mtu 1492 command must be applied on the dialer interface.
D.The ip mtu 1496 command must be applied on the dialer interface.
E.The ip mtu 1492 command must be applied on the Ethernet interface.
F.The ip mtu 1496 command must be applied on the Ethernet interface.
Answer:A

30.Refer to the exhibit. Which two statements about the Network Time Protocol (NTP) are true? (Choose two.)



A.Router RTA will adjust for eastern daylight savings time.
B.To enable authentication, the ntp authenticate command is required on routers RTA and RTB.
C.To enable NTP, the ntp master command must be configured on routers RTA and RTB.
D.Only NTP time requests are allowed from the host with IP address 10.1.1.1.
E.The preferred time source located at 130.207.244.240 will be used for synchronization regardless of the other time sources.
Answer:A B