



**Exam : 642-381**

**Title : Foundation Express for Field Engineers  
(FOUNDFE)**

**Ver : 10.24.07**

---

**QUESTION 1:**

When using the Site to Site VPN wizard in Cisco Router and Security Device Manager, why would you need to create an access list using the Add a Rule screen?

- A. to open holes on the firewall to permit ISAKMP, ESP, and AH traffic
- B. to define the traffic that will be protected by IPSec
- C. to specify a range of IP addresses on the inside interface
- D. to specify the remote-peer IP address range
- E. to enable split tunneling

Answer: B

---

**QUESTION 2:**

Under normal operation, which light sequence on the Cisco Aironet 1300 Wireless Bridge indicates that a device is associated to the bridge?

- A. The center LED (Status) is solid green.
- B. The center LED (Status) flashes green once every second.
- C. The center LED (Status) flashes green once every 3 seconds.
- D. The center LED (Status) blinks amber when an association occurs.

Answer: A

---

**QUESTION 3:**

Exhibit:

```
%SPANTREE-2-RECV_1Q_NON_TRUNK: Received IEEE 802.1Q BPDU on non trunkFastEthernet0/1 on vlan 1.  
%SPANTREE-2-BLOCK_PORT_TYPE: Blocking FastEthernet0/1 on vlan 1. Inconsistent port type.  
%SPANTREE-2-RX_1QPVIDERR: Rcvd pvid_inc BPDU on 1Q port 3/25 vlan 1  
%SPANTREE-2-RX_BLKPORTPVID: Block 3/25 on rcving vlan 1 for inc peer vlan 10  
%SPANTREE-2-TX_BLKPORTPVID: Block 3/25 on xmtting vlan 10 for inc peer vlan
```

According to the error log, VLAN 1 is where the BPDU was received, and VLAN 2 is where the BPDU originated. When inconsistency is detected, what happens?

- A. VLAN 1 is blocked, while VLAN 2 is forwarding.
- B. VLAN 1 is blocked, while VLAN 2 is listening.
- C. Both VLANs are listening on the port from which this BPDU is sent.
- D. Both VLANs are blocked on the port from which this BPDU is received.

Answer: D

---

**QUESTION 4:**

A user is not able to access the Cisco Router and Security Device Manager (SDM) via HTTPS. Which two situations could be causing the problem? (Choose two.)

- A. The ip https server command is not in the running-config.
- B. The ip http secure-server command is not in the running-config.
- C. The user is trying to launch Cisco SDM from the inside (secured) interface with firewall enabled.
- D. The user does not have a privilege level of 15.

Answer: B,D

---

**QUESTION 5:**

Certkiller .com wants to implement wireless security through implementation of WPAv2. Which component of WPAv2 would limit the rollout because of the continued use of old access points?

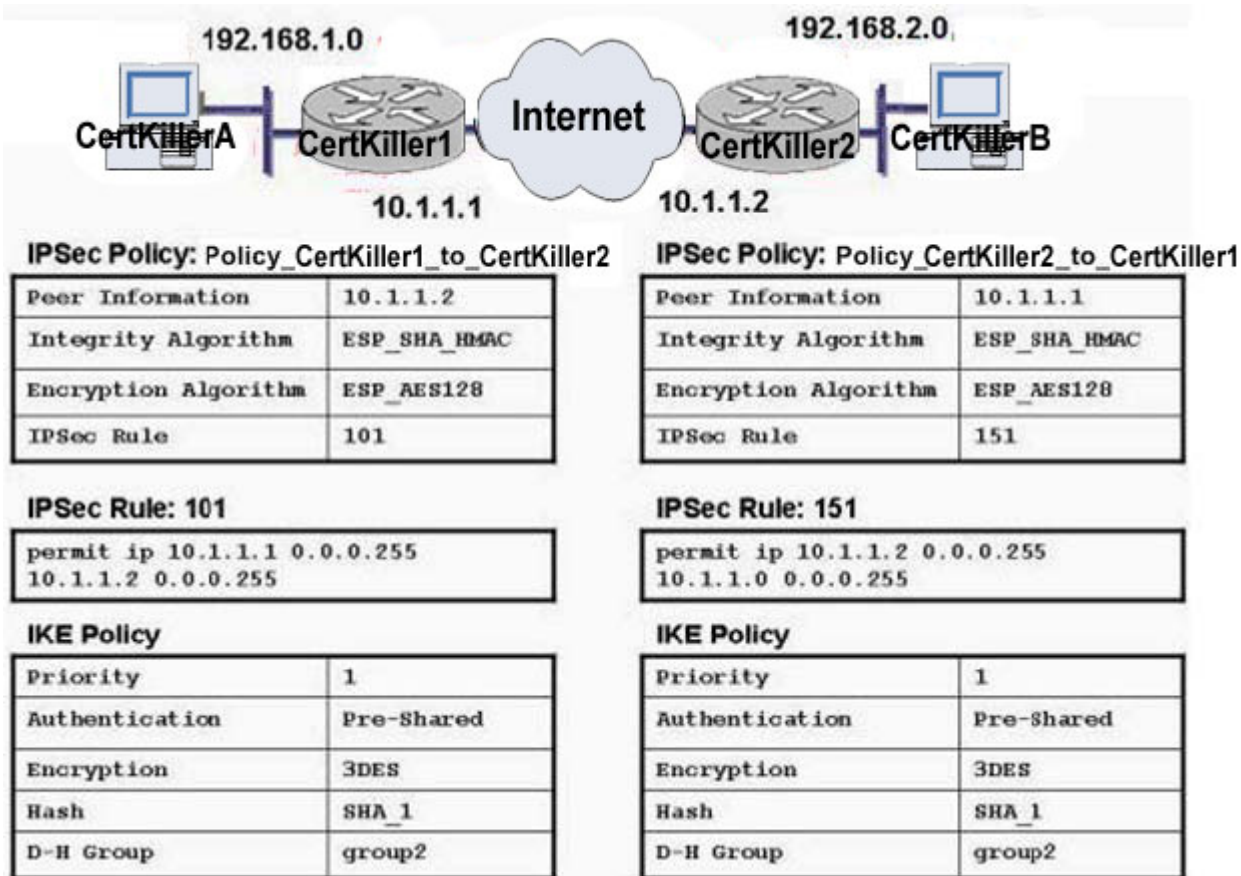
- A. 48-bit IV
- B. AES
- C. TKIP
- D. MIC

Answer: B

---

**QUESTION 6:**

Exhibit:



The tables contain information from the Cisco Router and Security Device Manager configuration of Router Certkiller 1 and Router Certkiller 1. Traffic between Host Certkiller A and Host Certkiller B is not successfully establishing the site-to-site VPN between Router Certkiller 1 and Router Certkiller 2. What is the mostly likely cause of this fault?

- A. The IPsec and IKE encryption methods do not match. They all have to be either 3DES or AES.
- B. Certkiller 1 is using a standard IP ACL (100-149) while Certkiller 2 is using a turbo ACL (150-199).
- C. The D-H Group settings on the two routers are set to group 2. They must be set to group 1 for SHA-1.
- D. The IPsec policy map names on the two routers do not match. They must be the same on both routers.
- E. The IPsec rules on the two routers are not permitting the correct interesting traffic.

Answer: E

### QUESTION 7:

An administrator at host address 10.0.1.11 is trying to gain access to Cisco Adaptive Security Device Manager via a Cisco ASA Security Appliance inside interface at IP address 10.0.1.1. Which two commands are required on a security appliance to enable

Cisco ASDM access? (Choose two.)

- A. http (inside) host 10.0.1.11
- B. Access-list asdm\_access permit tcp host 10.0.1.11 host 10.0.1.1 eq http ! http (inside)  
match asdm\_access !
- C. http server enable
- D. asdm-management enable
- E. http 10.0.1.1 255.255.255.255 inside
- F. Access-list asdm\_access permit tcp host 10.0.1.11 host 10.0.1.1 eq http asdm-map  
ASDM match asdm\_access

Answer: C,E

---

**QUESTION 8:**

What is the default authentication method when using HTTP to access the Cisco Router and Security Device Manager (SDM), assuming that you are not using the default configuration file (sdmconfig-xxxx.cfg) that comes with Cisco SDM?

- A. none
- B. local database
- C. aaa
- D. enable password
- E. line console password
- F. line vty password

Answer: D

---

**QUESTION 9:**

The network administrator has configured the SSID value in a wireless Cisco Aironet client card. What is the result of the client-to-access-point association if the client SSID1 is left blank, and the SSID2 is assigned a value of my\_ssid?

- A. The client will consider SSID1 a null value, causing the client to request the SSID from the access point.
- B. The client software will not allow this configuration and will create an error message until the configuration is corrected.
- C. The client software will replace SSID1 with SSID2, and use my\_ssid to attempt association with the access point.
- D. The client software will attempt association with the access point using a null value of SSID1, and if not successful it will rotate to use the SSID2 value of my\_ssid.

Answer: C

**QUESTION 10:**

Which four features can be configured using Cisco Router and Security Device Manager version 2.1.1? (Choose four.)

- A. IP multicast routing (PIM)
- B. IPS
- C. Easy VPN Remote and Easy VPN Server
- D. static routes and IGP routing protocols (OSPF, RIP, EIGRP)
- E. SSL VPN (WebVPN)
- F. AAA

Answer: B,C,D,F

---

**QUESTION 11:**

Which three are different types of STP inconsistencies in a Layer 2 network? (Choose three.)

- A. MAC inconsistency
- B. root inconsistency
- C. EtherChannel inconsistency
- D. type inconsistency
- E. PVID inconsistency
- F. vendor inconsistency

Answer: B,C,D

---

**QUESTION 12:**

Exhibit:



According to the Cisco VPN Client software outputs shown, which two statements are correct about the connection entry named isr? (Choose two.)

- A. HMAC-SHA1 is used to authenticate the remote users.
- B. Preshared key is used to authenticate the remote peer.
- C. AES is used to provide data confidentiality.
- D. The Cisco VPN Client software is assigned an internal IP address of 192.168.1.1.
- E. The PC that is running the Cisco VPN Client software will not have access to the local LAN once the PC is connected into the VPN.

Answer: B,E

### QUESTION 13:

Which two statements are correct about using Cisco Router and Security Device Manager (SDM) to configure the OSPF routing protocol? (Choose two.)

- A. Cisco SDM enforces the creation of area 0 when configuring OSPF.
- B. Cisco SDM will use the supplied wildcard mask to exclude the host bits from the configured network address.
- C. Cisco SDM allows the configuration of an area range to allow route summarization between OSPF areas.
- D. Cisco SDM allows the selection of OSPFv1 or OSPFv2.
- E. Cisco SDM allows the configuration of passive interfaces.

Answer: B,E

---

**QUESTION 14:**

The Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter has two LEDs. Which two situations indicate that the card is associated to an access point and is working properly? (Choose two.)

- A. green LED off; amber LED solid
- B. green LED off; amber LED blinking sporadically
- C. green LED blinking fast; amber LED blinking fast
- D. green LED blinking slowly; amber LED blinking slowly
- E. green LED blinking slowly; amber LED blinking fast

Answer: C,D

---

**QUESTION 15:**

Which two statements best describe the wireless core feature set using autonomous access points when implementing Wireless Domain Services? (Choose two.)

- A. The primary Layer 2 WDS server address is configured via the infrastructure access point GUI.
- B. The primary Layer 2 WDS server address is automatically discovered by the infrastructure access points through multicast.
- C. The primary Layer 2 WDS is selected by the highest MAC address, followed by priority number.
- D. The primary Layer 2 WDS is selected by the highest priority number, followed by MAC address.
- E. The primary Layer 2 WDS is selected by the highest IP address, followed by MAC address.

Answer: B,D

---

**QUESTION 16:**

When will you need to enable the transparent tunneling feature on the Cisco VPN Client



software?

- A. to enable DMVPN
- B. to enable dynamic routing over the IPsec tunnel using GRE
- C. to enable V3PN
- D. if the IPsec-protected traffic is going through a router that is performing NAT or PAT
- E. if IPsec is using tunnel mode instead of transport mode

Answer: D

---

**QUESTION 17:**

Several users have reported problems accessing the new company web server. How can the administrator test to ensure that all layers of the OSI model are working?

- A. Ping the web server by name.
- B. Ping the IP address of the web server.
- C. Telnet to port 80 of the web server.
- D. Use the debug ip http server command.
- E. Use the show ip http server command.
- F. Use the netstat -r command.

Answer: C

---

**QUESTION 18:**

You work as a network technician at Certkiller .com. Your boss, Miss Certkiller, asks to give a lecture to the new Certkiller trainees. During the lecture you explanation for the Certkiller trainees that the FCAPS model is an ISO model for network management that is designed to logically separate management tasks.

In this context, you are also required to match the definitions with the appropriate terms.

**Terms, select from these**

Fault monitoring	Configuration
Accounting	Performance
Security	

**Definitions**

AAA services are provided by asynchronous communication server and comitted access rate
A large amount of data must be gathered from many sources and processed into usable form
There is a larger number of data sources, and it is necessary to gather meaningful data
Changing just one parameter on multiple access points can be challenging
You need to ensure that there is adequate throughput and utilization from many access points.

**Terms, place here**

Place here
Place here
Place here
Place here
Place here

Answer:

**Definitions**

AAA services are provided by asynchronous communication server and comitted access rate
A large amount of data must be gathered from many sources and processed into usable form
There is a larger number of data sources, and it is necessary to gather meaningful data
Changing just one parameter on multiple access points can be challenging
You need to ensure that there is adequate throughput and utilization from many access points.

**Terms, place here**

Configuration
Accounting
Fault monitoring
Security
Performance

---

**QUESTION 19:**

Which two statements are correct about OSPF in a multiarea environment? (Choose two.)

- A. OSPF will by default summarize routing updates between areas.
- B. OSPF requires the use of the area range configuration command only when nondefault summarization is required.
- C. OSPF ABR routers are needed only at the boundary of another OSPF area.

- D. OSPF uses wildcard masks in the network statements but subnet masks in the area range statements.
- E. OSPF requires that all areas have a least one ASBR.

Answer: C,D

---

**QUESTION 20:**

When implementing an integrated network-security management design, which critical issue should you account for?

- A. that management stations intercommunicate and can correlate events
- B. that full syslogging of all events is enabled
- C. that all network devices are time synchronized
- D. that SNMP community read-write strings are configured to allow for total management access

Answer: B

---

**QUESTION 21:**

Users logging into Cisco Router and Security Device Manager (SDM) should be authenticated using the Cisco ISR local user database. Currently, none of the users can access the Cisco SDM via HTTP. Which command or commands should be verified as properly configured on the ISR to resolve this problem?

- A. ip http secure-server
- B. ip http authentication local
- C. line vty 0 5 login local
- D. line con 0 login local
- E. aaa new-model aaa authentication login default local
- F. aaa new-model aaa authorization exec default local

Answer: B

---

**QUESTION 22:**

Which two items have the most influence on an outdoor wireless antenna bridge-path installation? (Choose two.)

- A. snow
- B. Earth's curvature
- C. lightning
- D. Fresnel zone
- E. rain

Answer: B,D

---

**QUESTION 23:**

Which two statements best describe the wireless implementation of Cisco Aironet root and non-root bridging? (Choose two.)

- A. Point-to-point access points can be used if one is root and the other is non-root.
- B. WGB can be used with an access point if the distance is less than one mile.
- C. Root mode must be enabled only on one side in a point-to-point link to interoperate with other vendors and comply with 802.11.
- D. Up to 17 non-root bridges can associate to a root bridge.
- E. Point-to-point WGB can be used if total number of PCs is fewer than eight.

Answer: B,D

---

**QUESTION 24:**

Which two statements are correct about using Cisco Router and Security Device Manager (SDM) to configure RIP routing protocol? (Choose two.)

- A. Cisco SDM allows the configuration of RIPv2 network masks.
- B. Cisco SDM allows the configuration only of RIPv2.
- C. Cisco SDM allows the configuration of RIPv1 and RIPv2.
- D. Cisco SDM allows leaving the selection of the RIP protocol version to the default of the installed Cisco IOS software.

Answer: C,D

---

**QUESTION 25:**

What is not a correct statement about PoE ports that are implemented on Cisco Catalyst 4500 Series switches?

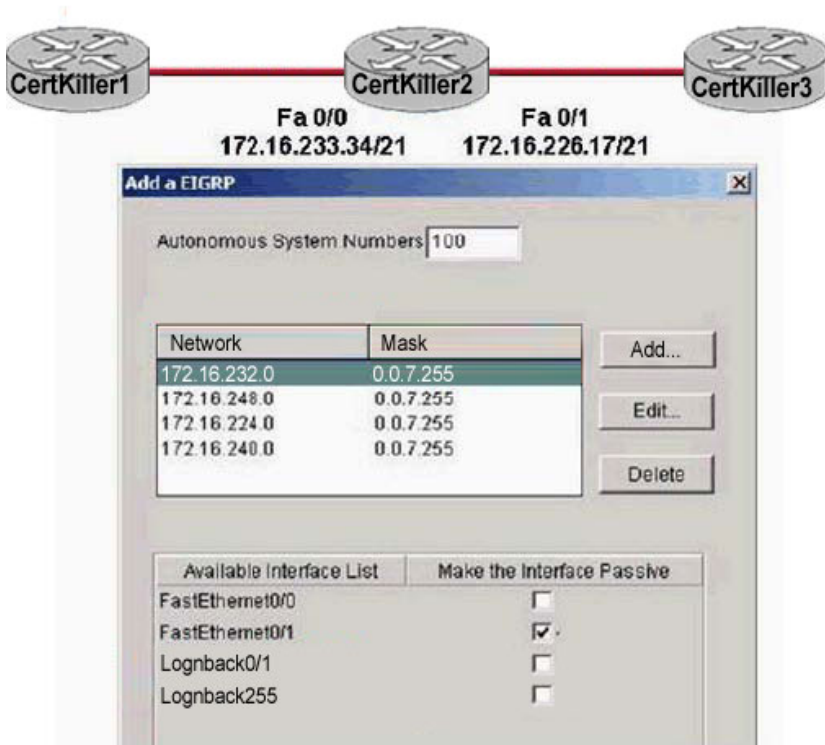
- A. They can distinguish a Cisco prestandard device.
- B. They can distinguish an IEEE 802.1af powered device.
- C. They can distinguish an unpowered NIC.
- D. They provide -48 VDC power over standard Category 5 UTP cable.
- E. They deliver power for a distance up to 100 meters over standard Category 5 UTP cable.

Answer: B

---

**QUESTION 26:**

Exhibit:



Cisco Router and Security Device Manager (SDM) is being used to configure EIGRP for the first time. Which three statements are correct about the Add a EIGRP display window? (Choose three.)

- A. Certkiller 1 will not receive any EIGRP updates from Certkiller 2.
- B. Certkiller 3 will not receive any EIGRP updates from Certkiller 2.
- C. It is possible to configure the auto summary behavior of EIGRP 100 on Certkiller 2 using Cisco SDM.
- D. It is possible to configure multiple instances of EIGRP on Certkiller 2 using Cisco SDM, providing the autonomous systems numbers do not conflict.
- E. The IP address masks of interfaces FastEthernet 0/0 and FastEthernet 0/1 must match their corresponding network statements in the EIGRP routing protocol for routing updates to be exchanged.
- F. The various network and mask configurations under EIGRP 100 can be reduced to a single line of 172.16.224.0 0.0.31.255.

Answer: B,D,F

### QUESTION 27:

After performing a security audit in Cisco Router and Security Device Manager (SDM), you receive this as one of the results: Enable Unicast RPF on all outside interfaces - Not Passed Which Cisco SDM configuration wizard can be used to resolve this?

- A. Easy VPN Server

- B. Basic Firewall
- C. Edit Interface/Connection
- D. Site to Site VPN
- E. Routing
- F. NAT

Answer: B

---

**QUESTION 28:**

Certkiller .com in Europe needs to establish an 11-Mbps wireless bridge link between two office buildings that are approximately 1.3 km apart. The wireless link will pass through a public park, which contains a lake that is surrounded by trees. You run the range calculation and determine that the Cisco Aironet 1300 Series Outdoor Access Point/Bridge should work. You install the link using 10.5-dB yagis with 75 feet of standard Cisco cabling and both radios set at 20 mW. The wireless bridges are not able to establish or maintain a link. What is needed to successfully complete this link?

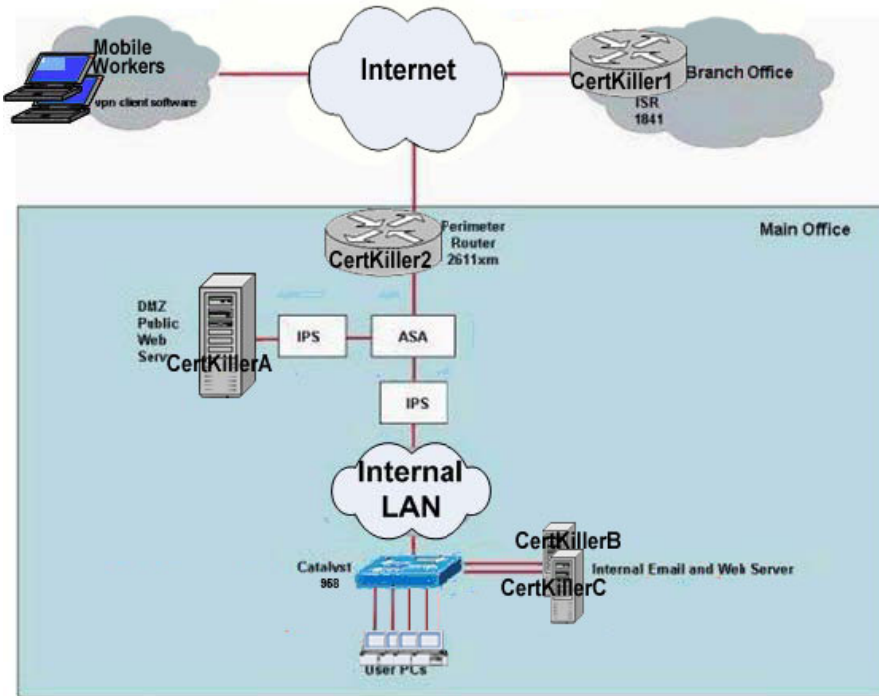
- A. An amplifier needs to be installed at one of the sites.
- B. The antenna must be raised high enough to clear the trees.
- C. Lower loss cabling needs to be used to bring the EIRP into legal limits.
- D. Due to the trees, a 21-dBi dish needs to be used for its narrower beamwidth.

Answer: B

---

**QUESTION 29:**

Exhibit:



You are asked to implement a network design that consists of two sites, the main office and one branch office connected via the Internet. Communications between these sites must be secure. The main office site also supports 30 local users and 15 remote mobile workers. Before gaining access to the internal network, both the local users and the mobile workers should be authenticated using a scalable solution. Before you begin the implementation, you need to identify which security component is missing in the design.

- A. Cisco VPN 3000 Series Concentrator
- B. ACS
- C. network-based IDS
- D. Cisco PIX Security Appliance
- E. 802.1x authenticator
- F. CBAC on the perimeter router

Answer: B

### QUESTION 30:

A North American customer is using 2.4-GHz radios in a point-to-point configuration. The radio power level is 17 dBm and is transmitting at 11 Mbps. Certkiller .com is using 21.5-dBi dish antennas and 50 feet of cabling, with a loss of 8.4 dB per 100 feet. Certkiller .com increased the distance between the transmitter stations and began experiencing link problems. Without using a professional installer, which step should Certkiller .com take to fix the situation?

- A. Use a cable with lower loss.
- B. Upgrade to an 802.11a radio.

- C. Install a higher gain antenna.
- D. Increase the transmitter power.

Answer: A

---

**QUESTION 31:**

You have configured and applied a Cisco IOS Firewall access rule to the inbound, untrusted interface. You suspect that the rule may be blocking necessary traffic onto the network. What must you do to delete that rule when using Cisco Router and Security Device Manager?

- A. Select ACL Editor > Access Rules to delete the rule.
- B. You must remove the association between the rule and the interface before deleting the rule.
- C. You must delete the associated access list on the interface, then reconfigure the access list as required, and then reapply the access group to the proper interface.
- D. Go to the Edit Firewall Policy tab to delete the rule.

Answer: B

---

**QUESTION 32:**

A concern has been expressed that the switched infrastructure in an integrated network is vulnerable to VLAN hopping attacks. Which two configuration statements can be used to mitigate VLAN hopping? (Choose two.)

- A. switchport port-security
- B. switchport port-security tagging
- C. switchport access vlan
- D. switchport double-tag snooping
- E. switchport mode access

Answer: C,E

---

**QUESTION 33:**

You are migrating the network design from using point security products (perimeter router, firewall, VPN router, IPS) to an integrated security solution using the Cisco ISR. During the migration process, you determine that you need to improve the VPN performance. What can you do?

- A. Upgrade the Cisco IOS image on the ISR to the V3PN bundle.
- B. Increase the RAM on the ISR.
- C. Install the AIM-VPN/EPII-PLUS on the ISR.
- D. Use AES encryption instead of 3DES.

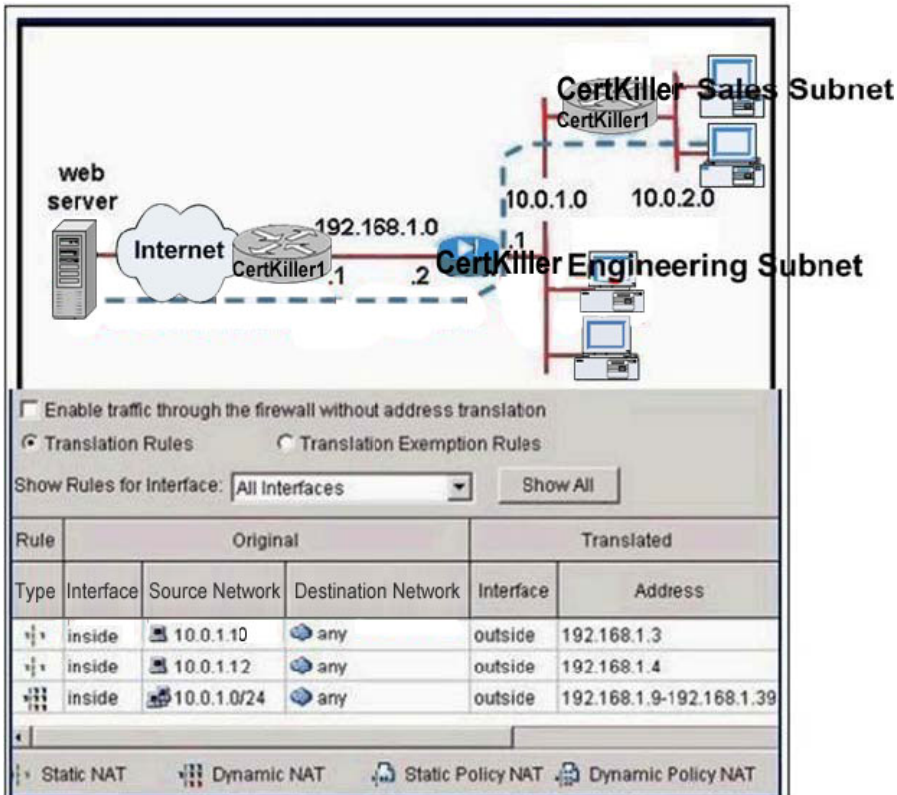


- E. Enable transparent tunneling using IPsec over TCP.
- F. Enable transparent tunneling using IPsec over UDP.

Answer: C

### QUESTION 34:

Exhibit:



You work as a network technician at Certkiller .com. Host Certkiller A on the CertK in Sales subnet (10.0.2.0/24) is not able to initiate a web connection to an outside website. According to the network diagram and the partial Cisco Adaptive Security Device Manager configuration shown in the exhibit, what is the cause of the problem?

- A. The dynamic NAT global pool is not configured correctly.
- B. The source networks for static NAT are not configured correctly.
- C. The administrator needs to add an access list and static command for the return web traffic.
- D. The source network for dynamic NAT is not configured correctly.

Answer: D

### QUESTION 35:

Which two statements best describe the wireless core feature set using autonomous access points when implementing repeater topology? (Choose two.)

- A. RF overlap between access points should be 10 to 15 percent with unique channels configured.
- B. RF overlap between primary and repeater access points should be 10 to 15 percent with the same channel configured.
- C. RF overlap between primary and repeater access points should be 50 percent with the same channel configured.
- D. RF overlap between primary and repeater access points should be 50 percent with unique channels configured.
- E. Clients that are associated with the repeater access point will have 10 to 15 percent less data throughput than clients that are associated with the primary root access point.
- F. Clients that are associated with the repeater access point will have 50 percent less data throughput than clients that are associated with the primary root access point.

Answer: C,F

---

**QUESTION 36:**

You have enabled SDEE to report Cisco IOS IPS events. However, when you attempt to view IPS events, none are available for viewing. Which two should you verify to ensure that your configuration is correct? (Choose two.)

- A. that ip ips notify sdee is enabled
- B. that you have a valid number of subscriptions enabled
- C. that the receiving host IP address and secret key are correctly configured
- D. that ip http server is enabled
- E. that ip ips deny-action parameters are enabled
- F. that you are connecting to the proper SDEE engine port number

Answer: A,D

---

**QUESTION 37:**

Exhibit:

Interface Name	IP	Inbound IPS	Outbound IPS	VFR status	Description
FastEthernet0/0	128.107.245.99	Enabled	Disabled	on	
FastEthernet0/1	172.16.1.1	Disabled	Disabled	on	

Action	Source	Destination	Stryce	log	Attributes	Description
Deny	10.1.1.0/0.0.255	any	www/tcp			
Permit	any	any	ip			

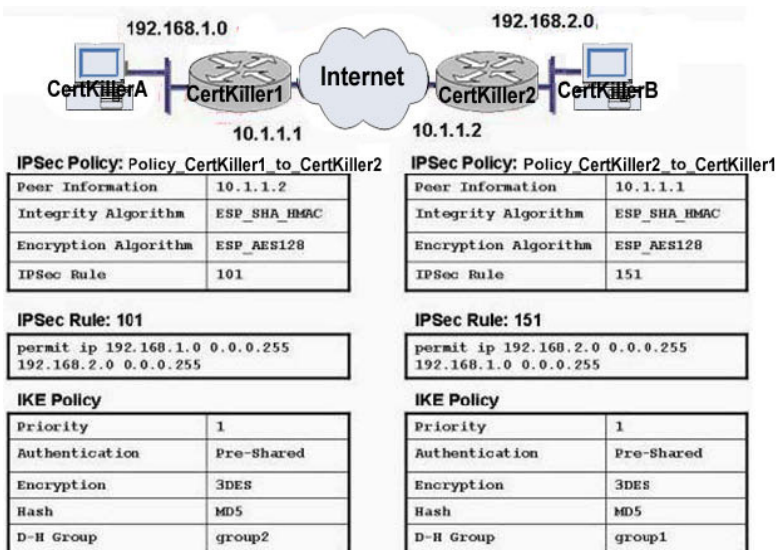
Based on the IPS configuration, which two types of traffic will be scanned by Cisco IOS IPS? (Choose two.)

- A. inbound HTTP traffic from host 10.1.1.1 to FastEthernet 0/0 interface
- B. inbound HTTP traffic from host 10.2.2.2 to the FastEthernet 0/0 interface
- C. all inbound traffic to the FastEthernet 0/0 interface
- D. all inbound and outbound traffic to the FastEthernet 0/0 interface
- E. inbound Telnet traffic from host 192.168.1.1 to the FastEthernet 0/0 interface
- F. all inbound traffic to the FastEthernet 0/0 interface or the FastEthernet 0/1 interface

Answer: B,E

### QUESTION 38:

Exhibit:



The tables contain information from the Cisco Router and Security Device Manager configuration of Router Certkiller 1 and Router Certkiller 2. Traffic between Host 1 and

Host 2 is not successfully establishing the site-to-site VPN between Router Certkiller 1 and Router Certkiller 2. What is the mostly likely cause of this fault?

- A. The D-H Group settings on the two routers are different. They must be the same.
- B. The IPSec and IKE encryption methods do not match. They all have to be either 3DES or AES.
- C. Router Certkiller 1 is using a standard IP ACL (100-149) while Router Certkiller 2 is using a turbo ACL (150-199).
- D. The IPSec policy map names on the two routers do not match. They must be the same on both routers.
- E. IPSec is using ESP for integrity while IKE is using MD5. They must use the same hashing algorithm.
- F. The IPSec rules on the two routers are not permitting the correct interesting traffic. They should permit router-to-router communications.

Answer: A

---

**QUESTION 39:**

Which two statements best describe the installation of Cisco Aironet LAN Client Adapters? (Choose two.)

- A. Cisco ACAU automates the deployment of Cisco ADU.
- B. Cisco ACAU automates the deployment of Cisco ACU.
- C. Cisco ADU is for the 802.11a/b/g radio client card.
- D. Cisco ACU is for the 802.11a/b/g radio client card.

Answer: A,C

---

**QUESTION 40:**

Which two statements best describe the wireless core feature set using autonomous access points when implementing Wireless Domain Services? (Choose two.)

- A. Layer 2 and Layer 3 services can be configured in a Cisco Aironet autonomous AP or a Cisco Integrated Services Router.
- B. Layer 2 services can be configured in a Cisco Aironet autonomous AP or a Cisco Integrated Services Router.
- C. Layer 2 and Layer 3 services can be configured in a Cisco Aironet autonomous AP or controllers.
- D. Layer 3 services can be configured in WLSM.
- E. Layer 3 services can be configured in WLSE.

Answer: B,D

---

**QUESTION 41:**

You have applied a firewall configuration to your router using the Cisco Router and Security Device Manager (SDM) Firewall wizard. You find that you are now locked out and access via Cisco SDM is denied. After accessing the router via the console port, what must you do to regain access via Cisco SDM?

- A. Generate an RSA key pair between the host and device to allow secure access.
- B. Specify the Cisco SDM management port number to gain access.
- C. Create a loopback interface and connect to that IP address for management purposes when the configuration has been applied to the router.
- D. Modify the access list that denies Cisco SDM access.

Answer: D

**QUESTION 42:**

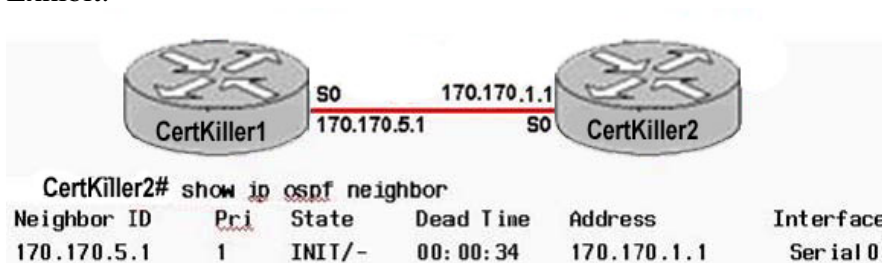
Which two features are only supported when using the Cisco Router and Security Device Manager (SDM) Advanced Firewall wizard and not supported when using the Cisco SDM Basic Firewall wizard? (Choose two.)

- A. deep-packet inspections
- B. IP unicast Reverse Path Forwarding on the outside (untrusted) interface
- C. DMZ services
- D. custom inspection rules
- E. proxy authentication

Answer: C,D

**QUESTION 43:**

Exhibit:



Certkiller 2 is always in the init state. Which two statements are correct? (Choose two.)

- A. Certkiller 2 is seeing hello packets from R1.
- B. Certkiller 2 is not seeing hello packets from R1.
- C. The exchanging of data between R1 and Certkiller 2 is occurring because each is sending hello packets.
- D. Two-way communication has not been established between R1 and Certkiller 2

because Certkiller 2 is not seeing its router ID in the hello packets that it is receiving from R1.

E. Certkiller 2 has an access list defined for S0 that is blocking an OSPF multicast IP address of 224.0.0.5.

Answer: A,D

---

**QUESTION 44:**

When using Cisco Router and Security Device Manager to configure AAA login authentication policies, which four methods are available? (Choose four.)

- A. group RADIUS: use a list of RADIUS hosts
- B. group TACACS+: use a list of TACACS+ hosts
- C. enable: use enable password
- D. otp: use one-time password
- E. local: use local database
- F. default: use line password

Answer: A,B,C,E

---

**QUESTION 45:**

An 802.11b telephone is receiving an audio signal from an access point, but cannot send audio. What is a possible cause?

- A. The RSSI value on the telephone is greater than 35.
- B. The access point is set to receive only at 802.11g data rates.
- C. The security settings in the telephone do not match the settings in the access point.
- D. The transmit power in the telephone is significantly lower than the transmit power in the access point.

Answer: D

---

**QUESTION 46:**

Exhibit:

```
CertKillerA# debug eigrp packets
...
01:39:13: EIGRP:Received HELLO on Serial0/0 nbr 10.1.2.2
01:39:13: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
01:39:13:      K-value mismatch
```

A network administrator is troubleshooting an EIGRP connection between Router Certkiller 1 and Router Certkiller 2. Given the debug output on Router Certkiller 1, which two statements are true? (Choose two.)

- A. Router Certkiller 1 received a hello packet with mismatched autonomous system

numbers.

- B. Router Certkiller 1 received a hello packet with mismatched hello timers.
- C. Router Certkiller 1 received a hello packet with mismatched authentication parameters.
- D. Router Certkiller 1 received a hello packet with mismatched metric-calculation mechanisms.
- E. Router Certkiller 1 will form an adjacency with Router Certkiller 2.
- F. Router Certkiller 1 will not form an adjacency with Router Certkiller 2.

Answer: D,F

---

**QUESTION 47:**

A wireless autonomous 1200 access point running core feature set in root mode has its SSID set to `Factory_floor` and provides connection to a repeater access point with its SSID set to `Factory_floor`. If the root-mode access point is using channel 11, which channel will the repeater access point use?

- A. channel 11
- B. channel 1 or 6
- C. any nonoverlapping channel
- D. The root access point and the repeater will negotiate this setting.

Answer: A

---

**QUESTION 48:**

Exhibit:

```
CertKillerA #show interfaces ethernet 0/0
Ethernet0/0 is up, line protocol is up
....
21 input errors, 0 CRC, 0 frame, 0 overrun, 21 ignored
```

This display has been truncated to remove information that is not relevant to the question. What would be a reason that there have been 21 ignored packets?

- A. Ethernet0 has no CDP neighbors.
- B. There are no free input buffers to accept new packets.
- C. There are no free output buffers for packets, which are traversing the router, to go into for transmission.
- D. Ethernet0 and the neighbor that it is connected to are not running the same routing protocol.
- E. This is not a valid error display. The display has been modified to show that there have been ignored packets.

Answer: B

---

**QUESTION 49:**

Exhibit:

Rule	Original		Translated		
Type	Interface	Source Network	Destination	Interface	Address
Static NAT	dmz1	ftp_host 172.16.1.2	any	outside	192.168.1.11
Dynamic NAT	inside	insidehost 10.0.1.11	any	outside	192.168.1.10
Static NAT	dmz2	www_server 172.16.10.2	any	outside	192.168.1.12
Static NAT	dmz2	www_server 172.16.10.2	any	dmz1	172.16.1.22
Dynamic NAT	inside	inside any/0	any	outside	192.168.1.20-192.168.1.94
Dynamic NAT	dmz1	172.16.1.0/24	any	outside	192.168.1.20-192.168.1.94

According to the Cisco Adaptive Security Device Manager window, which statement about address translation is correct?

- A. Using Network Address Translation, any host on the DMZ1 subnet (172.16.1.0) will be translated to a mapped address on the outside interface of 192.168.1.11.
- B. Using port address translation, DMZ2 host 172.16.10.2 will be translated on DMZ1 to IP address 172.16.1.22 with a dynamically assigned port address.
- C. Using Network Address Translation, host 10.0.1.10 on the inside network will be dynamically translated to a mapped address from the address pool of 192.168.1.20 to 192.168.1.94.
- D. Using port address translation, outside host 192.168.1.10 with a dynamically assigned port address will be translated to 10.0.1.11 on the inside interface.

Answer: C

**QUESTION 50:**

When troubleshooting poor network performance, which two symptoms would typically be associated with a network layer problem? (Choose two.)

- A. Packet loss is more than 30 percent.
- B. There is excessive broadcast traffic.
- C. There are excessive CRC errors.
- D. Pings succeed only part of the time.
- E. Slips are detected on WAN interfaces.
- F. ARP requests are timing out.

Answer: A,D

**QUESTION 51:**



Which three statements are correct about the IEEE 802.3af Power over Ethernet standard? (Choose three.)

- A. It defines a port that acts as a power source to be a PSE.
- B. It defines a powered device to be a PDE.
- C. It defines how a powered device is detected.
- D. It defines three methods of delivering Power over Ethernet to the discovered powered device.
- E. It describes five power classes to which a device may belong.
- F. It defines power class 0 as being reserved for future use.

Answer: A,C,E

---

**QUESTION 52:**

You have just configured and enabled the Cisco IOS Firewall feature set from a remote location using the Cisco Router and Security Device Manager (SDM) Firewall wizard. You later want to double-check your configuration using Cisco SDM. However, you find that you can no longer connect to the Cisco IOS Firewall using Cisco SDM. What is the probable cause of this failure?

- A. You must additionally specify the Cisco SDM management port number to gain access when the configuration has been applied.
- B. You have not generated an RSA key pair between the host and device to allow secure access via Cisco SDM.
- C. You have been locked out via access lists that have been applied to the router as a result of your Cisco SDM configuration.
- D. You must specify the host IP address of Cisco SDM in the Configuration panel for allowed management connections.

Answer: C

---

**QUESTION 53:**

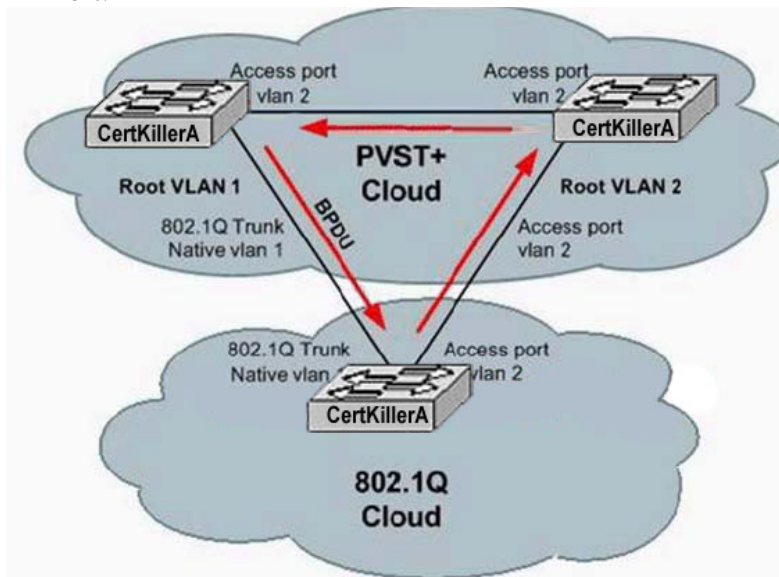
When using Cisco Router and Security Device Manager (SDM) to configure IPS, what must you do first before you can select Configure > Signature to edit any signatures?

- A. Select Configure > Global Settings to enable IPS globally on the router.
- B. Select Configure > Global Settings to disable the Failed Closed option.
- C. Select Configure > Global Settings to point Cisco SDM to the ips.tar file in the router Flash memory.
- D. Select Configure > Rules to create the inbound and/or outbound filter to determine which traffic will be scanned by IPS.
- E. Select Configure > Rules to enable an interface for inbound and/or outbound IPS.

Answer: E

**QUESTION 54:**

Exhibit:



Switches A and C are running PVST+ STP, and Switch B is running 802.1Q STP. If the BPDU of the root in VLAN 1 is better than the BPDU of the root in VLAN 2, then there is no blocking port in the VLAN 2 topology. The BPDU of VLAN 2 never makes a "full circle" around the topology; it is replaced by the VLAN 1 BPDU on the B-C link, because B runs only one STP merged with VLAN 1 STP of PVST+. Thus, there is a forwarding loop. What does PVST+ do to correct this?

- A. Switch A sends PVST+ BPDUs of VLAN 2 (to the SSTP address that is flooded by Switch B) towards Switch C. Switch C will put port C-B into a type-inconsistent state, which prevents the loop.
- B. Switch B sends PVST+ BPDUs of VLAN 1 (to the SSTP address that is flooded by Switch A) towards Switch C. Switch C will put port C-B into a type-inconsistent state, which prevents the loop.
- C. Switch C sends PVST+ BPDUs of VLAN 2 (to the SSTP address that is flooded by Switch B) towards Switch C. Switch A will put port C-B into a type-inconsistent state, which prevents the loop.
- D. Switch A sends PVST+ BPDUs of VLAN 1 (to the SSTP address that is flooded by Switch B) towards Switch B. Switch A will put port C-B into a type-inconsistent state, which prevents the loop.

Answer: A

**QUESTION 55:**

In an infrastructure based on a wireless advanced feature set using lightweight access points, by which method is a rogue contained?

- A. The WCS sends excessive traffic to the rogue, thus overloading the access point.
- B. The rogue MAC address is used to spoof broadcast deassociation packets.
- C. The rogue MAC address is used to spoof broadcast deauthentication packets.
- D. The WCS sends out excessive signals on the same channel when the rogue is detected.

Answer: C

---

**QUESTION 56:**

OSPF routes are being redistributed into EIGRP but they are not showing up in the routing table. What are two possible causes? (Choose two.)

- A. CEF has not been enabled.
- B. Synchronization has been turned off.
- C. Incorrect distribute lists have been configured.
- D. No default metric has been configured for EIGRP.
- E. The ip classless command is missing.
- F. There are mismatched autonomous system numbers.

Answer: C,D

---

**QUESTION 57:**

Exhibit:



Which two statements are correct about what is displayed? (Choose two.)

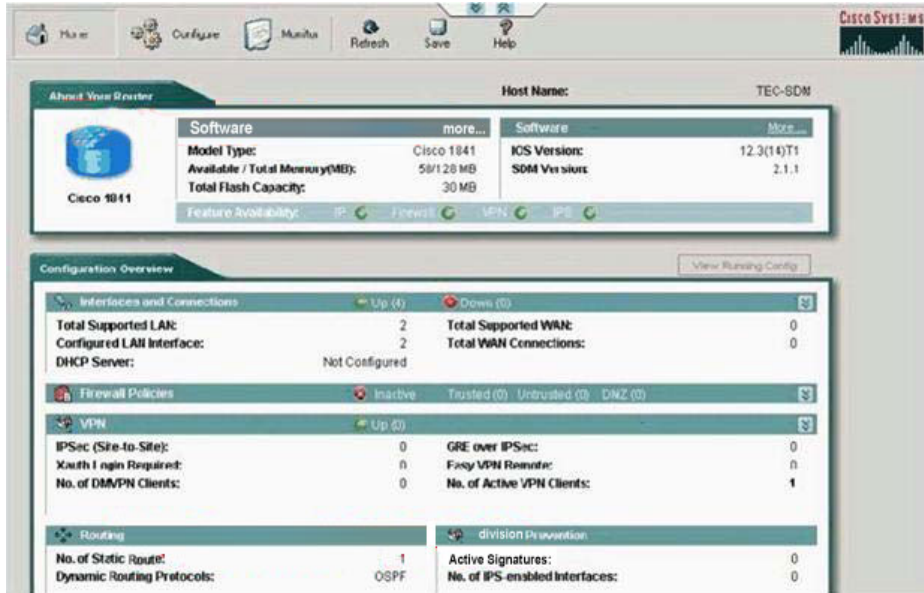
- A. The IP address that is used for the router ID must be reachable.
- B. Router 1 is the designated router because it has the lowest configured IP address.
- C. Router 1 is the designated router because it has the highest configured loopback address.
- D. If Router 1 had a PRI of 0, it could not be a designated router or a backup designated router.
- E. Router 1 has had its ID manually configured by using the router-ID command.

Answer: C,D

**Topic 1, Certkiller .com, Scenario**

You work as a network technician at Certkiller .com. You are required to troubleshoot a VPN environment.

Scenario exhibit:



**Topic 1, Questions (4 Questions)**

**QUESTION 58:**

How many active VPN clients are currently to the 1841 ISR router?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4
- F. 5
- G. 6
- H. 7
- I. 8

Answer: B

**QUESTION 59:**

Which IP address or address range will be used when allocating an internal IP address to the VPN clients for the "test" VPN group?

- A. 10.1.1.100 to 10.1.1.1200
- B. 10.1.1.2 to 10.1.1.254
- C. 192.168.1.1 to 192.168.1.100

- D. 192.168.1.2 to 192.168.1.254
- E. 10.1.1.1
- F. 192.168.1.1
- G. 192.168.1.2

Answer: A

---

**QUESTION 60:**

Which authentication method is used by the " Certkiller " VPN group?

- A. RSA Encrypted Noou7cne
- B. RSA Digital Signature
- C. Pre-Shared Key
- D. Digital Certificate
- E. DHZ

Answer: C

---

**QUESTION 61:**

Which method list and issued to authenticate the remove access VPN users? Select two.

- A. sdm\_vpn\_xauth\_ml\_1
- B. sdm\_vpn\_group\_ml\_1
- C. SDM\_CMAP\_1
- D. Local database on the ISR
- E. Remote TACACS+ server
- F. Remote Radius Server
- G. Enable password

Answer: A, D

**Topic 2, Certkiller Japan, Scenario**

You work as a network technician at the Osaka Certkiller .com branch office. You are required to troubleshoot the Certkiller network.

Scenario exhibit:



## Topic 2, Certkiller Japan (5 Questions)

### QUESTION 62:

Which two statements describe traffic that would be permitted based on the current access list configurations? Select two.

- A. Telnet traffic from any outside host to the 172.16.10.2 host on the dmz2
- B. HTTP and HTTPS traffic from any outside host to the 172.16.1.2 host on the dmz1
- C. Any IP traffic from any outside host to the 172.16.10.2 host on the dmz2
- D. Any IP traffic from any outside host to the 172.16.1.2 host on the dmz1
- E. Any IP traffic from any host on the dmaz1 to any host on the inside.
- F. Any IP traffic from any host on the dmaz2 to any host on the inside.

Answer: A, B

### QUESTION 63:

Which statement is correct about the current address translation configurations on the security appliance?

- A. Dynamic NAT is used to translate the 10.0.1.100 host on the inside interface to a global address of 192.168.1.1
- B. Port Address Translation (PAT) is used to translate any host on the inside interface to the 192.168.1.00 global address.
- C. Static NAT is used to translate the 172.16.1.2 host on the dmz1 interface to a global address of 192.168.1.102.
- D. Dynamic NAT is used to translate any host on dmaz1 and dmz2 interfaces to a mapped address from the address pool of 192.168.1.110 to 192.168.1.250
- E. Static NAT is used to translate the 172.168.1.100.

Answer: C

---

**QUESTION 64:**

What is the current configuration default gateway IP address on the security appliance?

- A. 172.16.10.1
- B. 172.16.1.1
- C. 192.168.1.2
- D. 10.0.1.1
- E. 172.16.1.2
- F. 172.16.10.2

Answer: C

---

**QUESTION 65:**

Which hosts are allowed to manage this security appliance using the ASDM?

- A. the 10.0.1.100 host only
- B. the 172.16.1.2 host only
- C. the 172.16.10.2 host only
- D. any host on the 10.0.1.0/24 subnet
- E. any host on the 172.16.1.0/24 subnet
- F. any host on the 172.16.10.0/24 subnet

Answer: A

---

**QUESTION 66:**

What is the maximum number of VLANs and physical interfaces are supported based on the current security appliance software license?

- A. 25 VLANs and 6 interfaces
- B. 10 VLANs and 6 interfaces
- C. 50 VLANs and 6 interfaces
- D. 150 VLANs and 6 interfaces
- E. 100 VLANs and 6 interfaces

Answer: A