

**Exam Code:** 642-381

**Exam Name:** Foundation Express for Field  
Engineers(FOUND FE)

**Vendor:** CISCO

**Version:** DEMO

## Part: A

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

**Correct Answers: B**

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.

**Correct Answers: A**

3: Refer to the exhibit. 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?

```
%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
```

- 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.

**Correct Answers: D**

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.

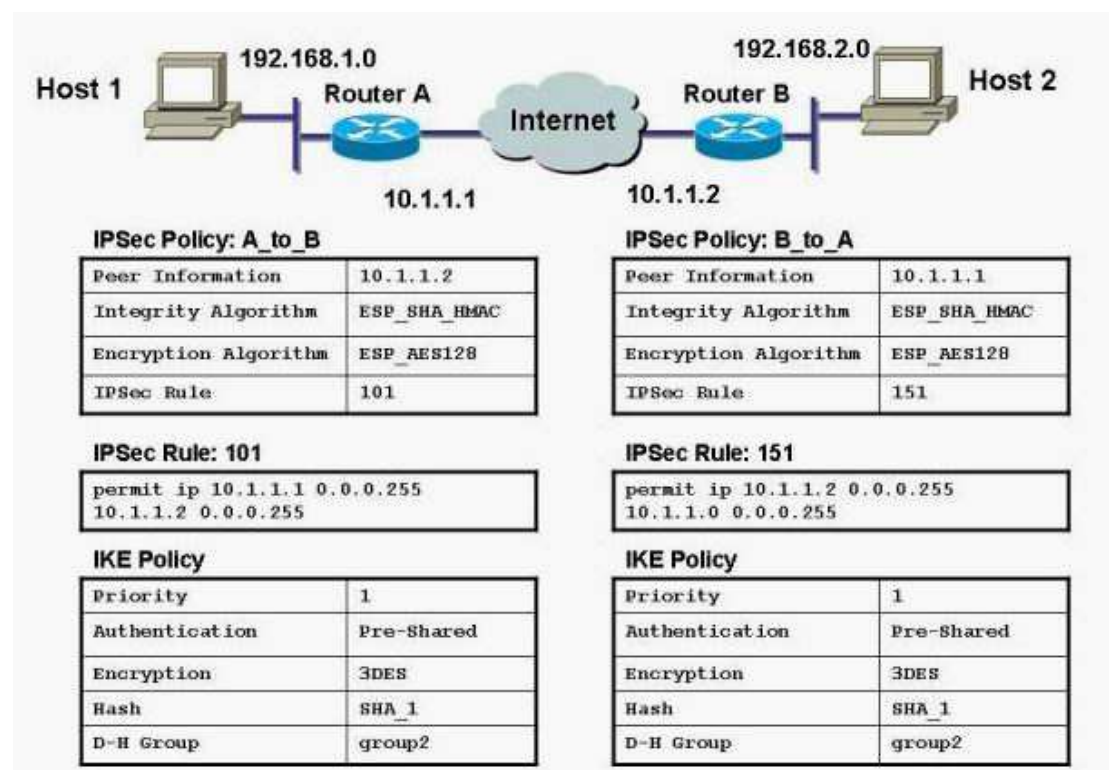
**Correct Answers: B D**

5: The customer 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

**Correct Answers: B**

6: Refer to the exhibit. The tables contain information from the Cisco Router and Security Device Manager configuration of Router A and Router B. Traffic between Host 1 and Host 2 is not successfully establishing the site-to-site VPN between Router A and Router B. 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.Router A is using a standard IP ACL (100-149) while Router B 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.

**Correct Answers: E**

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

**Correct Answers: C E**

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

**Correct Answers: D**

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.

**Correct Answers: C**

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

**Correct Answers: B C D F**