# Testpassport考試指南

品　　質　　更　　高　　服　　務　　更　　好

一年免費更新服務

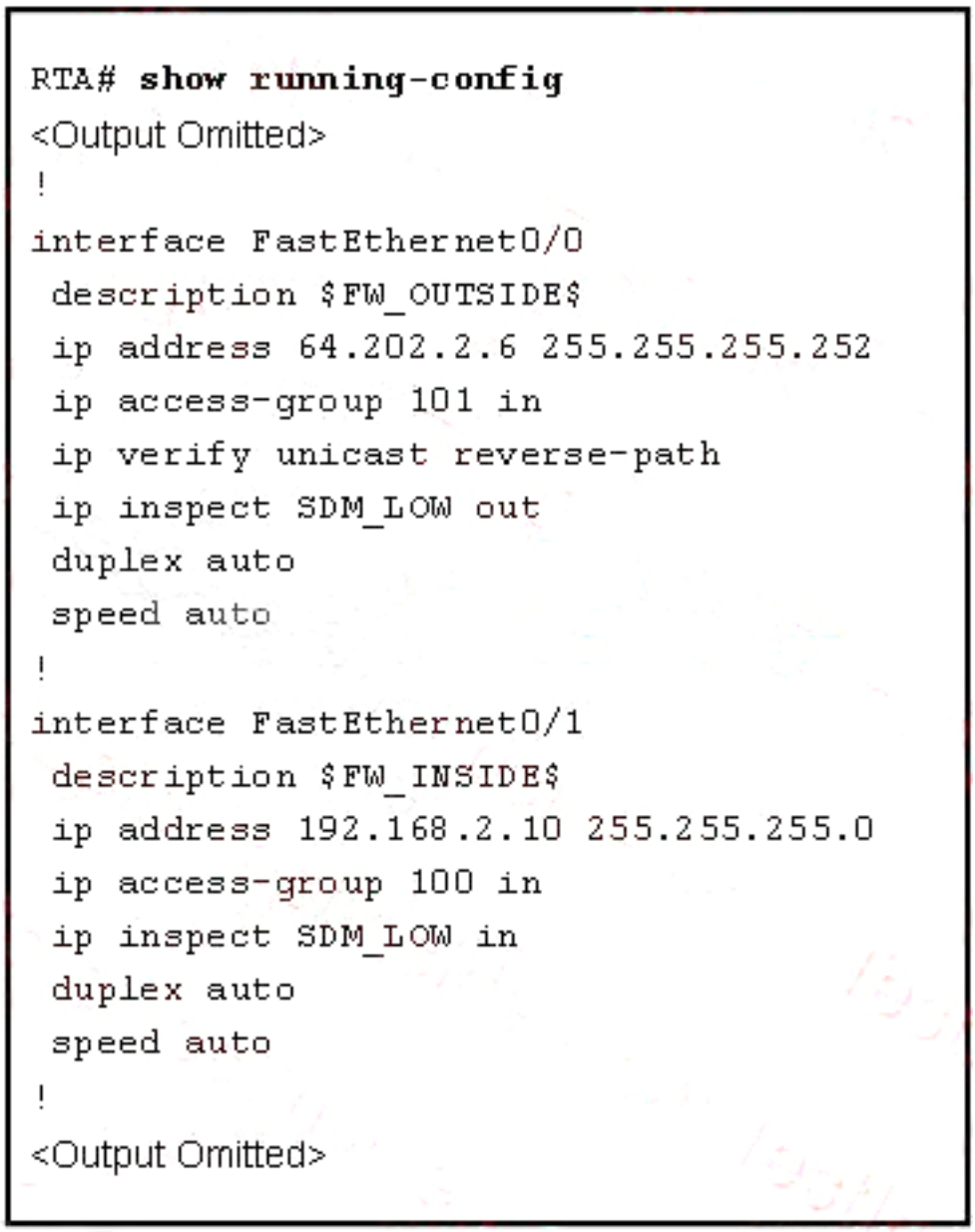
http://www.testpassport.net

**Exam** : **642-825**

**Title** : Implementing Secure Converged Wide Area Networks

**Version** : Demo

1. Refer to the exhibit. On the basis of the partial configuration, which two statements are true? (Choose two.)



```
RTA# show running-config
<Output Omitted>
!
interface FastEthernet0/0
 description $FW_OUTSIDE$
 ip address 64.202.2.6 255.255.255.252
 ip access-group 101 in
 ip verify unicast reverse-path
 ip inspect SDM_LOW out
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description $FW_INSIDE$
 ip address 192.168.2.10 255.255.255.0
 ip access-group 100 in
 ip inspect SDM_LOW in
 duplex auto
 speed auto
!
<Output Omitted>
```

A. A CBAC inspection rule is configured on router RTA.

B. A named ACL called SDM_LOW is configured on router RTA.

C. A QoS policy has been applied on interfaces Serial 0/0 and FastEthernet 0/1.

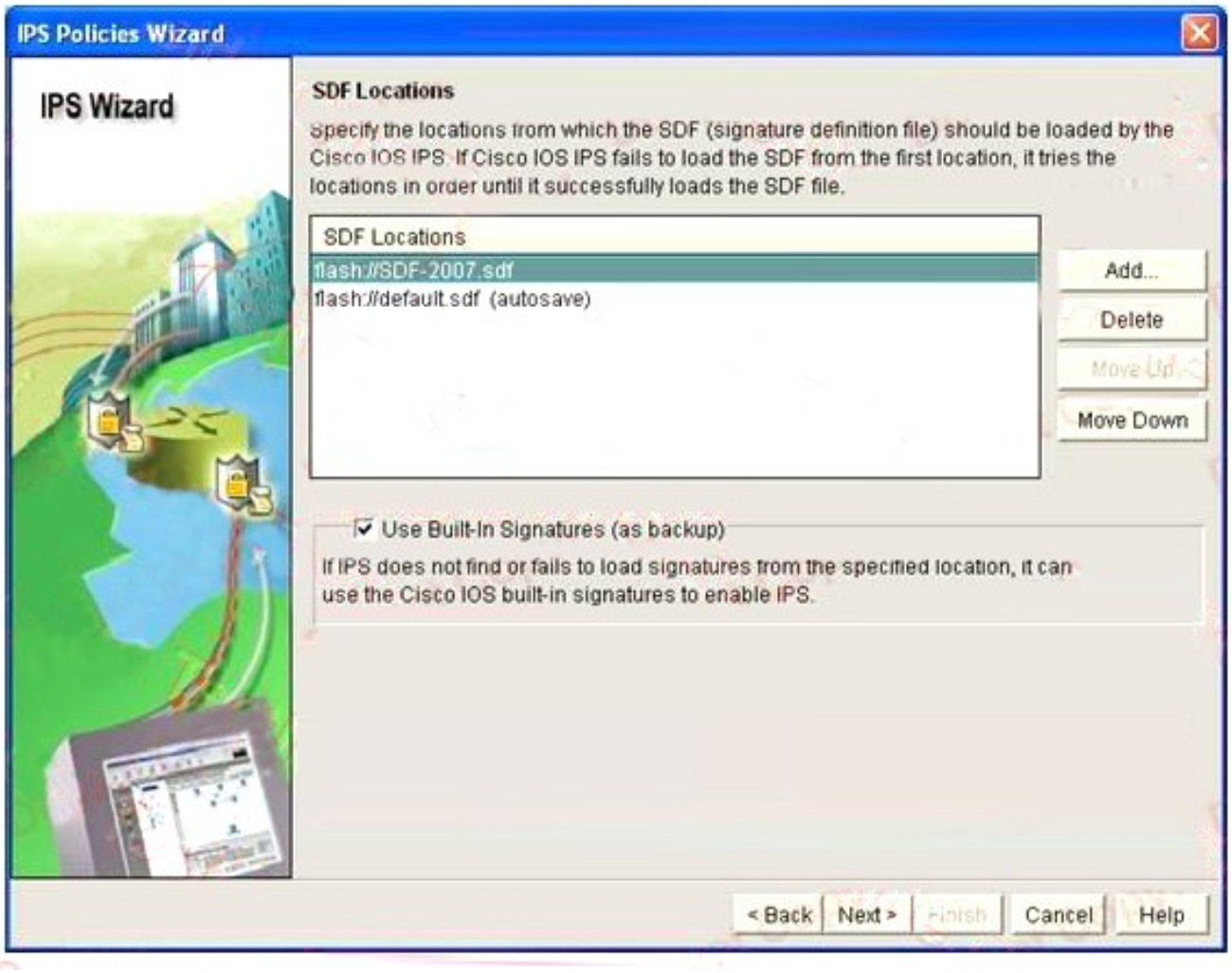
D. Interface Fa0/0 should be the inside interface and interface Fa0/1 should be the outside interface.

E. On interface Fa0/0, the ip inspect statement should be incoming.

F. The interface commands ip inspect SDM_LOW in allow CBAC to monitor multiple protocols.

**Answer:** AF

2. Refer to the exhibit. Which two statements about the SDF Locations window of the IPS Rule wizard are true? (Choose two.)




A. An HTTP SDF file location can be specified by clicking the Add button.

B. If all specified SDF locations fail to load, the signature file that is named default.sdf will be loaded.

C. The Autosave feature automatically saves the SDF alarms if the router crashes.

D. The Autosave feature is automatically enabled for the default built-in signature file.

E. The name of the built-in signature file is default.sdf.

F. The Use Built-In Signatures (as backup) check box is selected by default.

**Answer:** AF

3. Refer to the exhibit. Which two statements about the AAA configuration are true? (Choose two.)

```
aaa new-model
username Bob password itsasecret
aaa authentication enable default group tacacs+ none
```

A. A good security practice is to have the none parameter configured as the final method used to ensure that no other authentication method will be used.

B. If a TACACS+ server is not available, then a user connecting via the console port would not be able to gain access since no other authentication method has been defined.

C. If a TACACS+ server is not available, then the user Bob could be able to enter privileged mode as long as the proper enable password is entered.

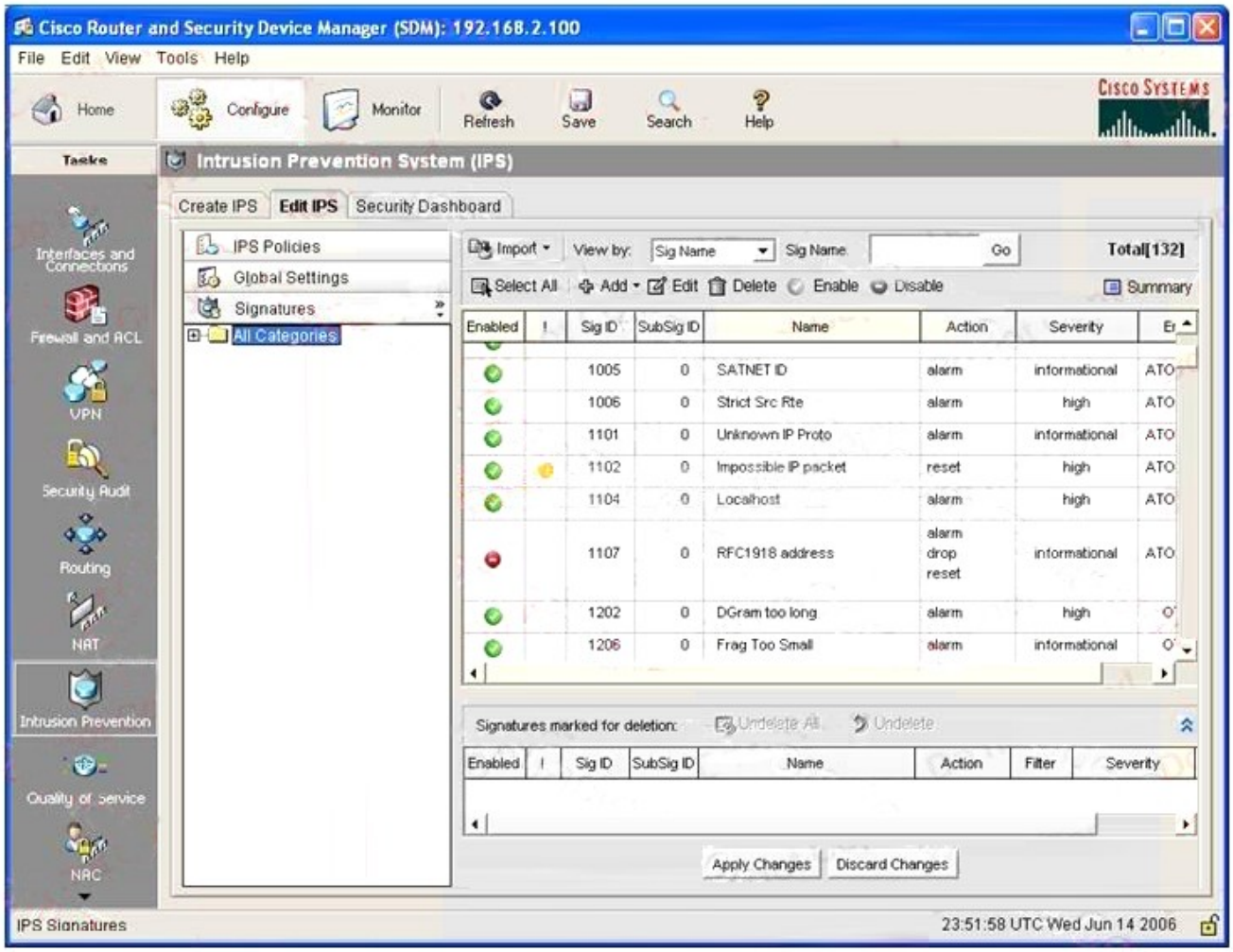
D. The aaa new-model command forces the router to override every other authentication method previously configured for the router lines.

E. To increase security, group radius should be used instead of group tacacs+.

F. Two authentication options are prescribed by the displayed aaa authentication command.

**Answer:** DF

4. Refer to the exhibit. On the basis of the information in the exhibit, which two statements are true? (Choose two.)




A. Any traffic matching signature 1107 will generate an alarm, reset the connection, and be dropped.

B. Signature 1102 has been modified, but the changes have not been applied to the router.

C. Signature 1102 has been triggered because of matching traffic.

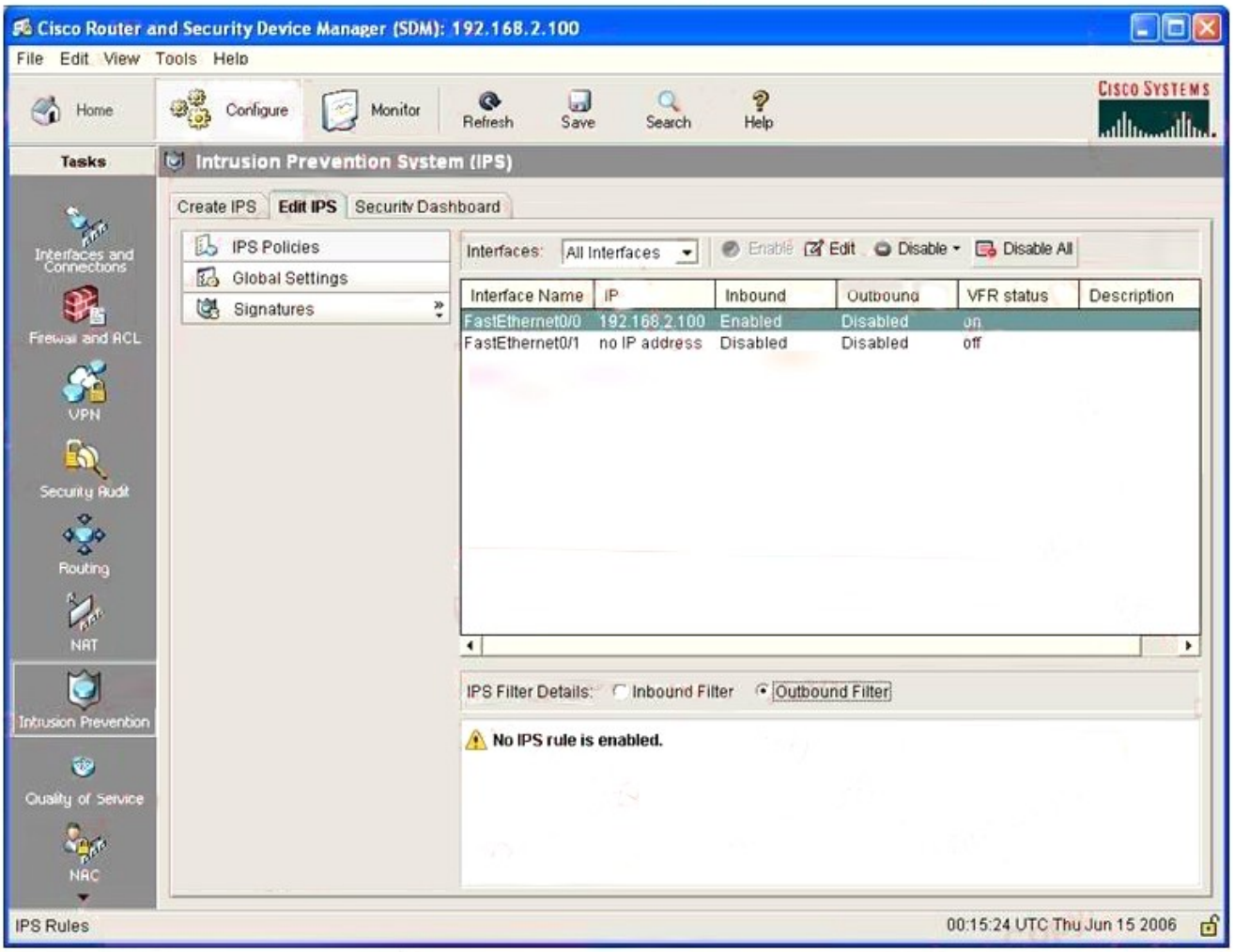
D. The Edit IPS window is currently displaying the Global Settings information.

E. The Edit IPS window is currently displaying the signatures in Details view.

F. The Edit IPS window is currently displaying the signatures in Summary view.

**Answer:** BE

5. Refer to the exhibit. On the basis of the information that is provided, which two statements are true? (Choose two.)




A. An IPS policy can be edited by choosing the Edit button.

B. Right-clicking on an interface will display a shortcut menu with options to edit an action or to set severity levels.

C. The Edit IPS window is currently in Global Settings view.

D. The Edit IPS window is currently in IPS Policies view.

E. The Edit IPS window is currently in Signatures view.

F. To enable an IPS policy on an interface, click on the interface and deselect Disable.

**Answer:** AD

6. 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:** AEF

7. Which three features are benefits of using GRE tunnels in conjunction with IPsec for building site-to-site VPNs? (Choose three.)

A. allows dynamic routing over the tunnel

B. supports multi-protocol (non-IP) traffic over the tunnel

C. reduces IPsec headers overhead since tunnel mode is used

D. simplifies the ACL used in the crypto map

E. uses Virtual Tunnel Interface (VTI) to simplify the IPsec VPN configuration

**Answer:** ABD

8. Which three IPsec VPN statements are true? (Choose three.)

A. IKE keepalives are unidirectional and sent every ten seconds.

B. IKE uses the Diffie-Hellman algorithm to generate symmetrical keys to be used by IPsec peers.

C. IPsec uses the Encapsulating Security Protocol (ESP) or the Authentication Header (AH) protocol for exchanging keys.

D. Main mode is the method used for the IKE phase two security association negotiations.

E. Quick mode is the method used for the IKE phase one security association negotiations.

F. To establish IKE SA, main mode utilizes six packets while aggressive mode utilizes only three packets.

**Answer:** ABF

9. Which three statements are true about Cisco IOS Firewall? (Choose three.)

A. It can be configured to block Java traffic.

B. It can be configured to detect and prevent SYN-flooding denial-of-service (DoS) network attacks.

C. It can only examine network layer and transport layer information.

D. It can only examine transport layer and application layer information.

E. The inspection rules can be used to set timeout values for specified protocols.

F. The ip inspect cbac-name command must be configured in global configuration mode.

**Answer:** ABE

10. Which two statements about common network attacks are true? (Choose two.)

A. Access attacks can consist of password attacks, trust exploitation, port redirection, and man-in-the-middle attacks.

B. Access attacks can consist of password attacks, ping sweeps, port scans, and man-in-the-middle attacks.

C. Access attacks can consist of packet sniffers, ping sweeps, port scans, and man-in-the-middle attacks.

D. Reconnaissance attacks can consist of password attacks, trust exploitation, port redirection and Internet information queries.

E. Reconnaissance attacks can consist of packet sniffers, port scans, ping sweeps, and Internet information queries.

F. Reconnaissance attacks can consist of ping sweeps, port scans, man-in-middle attacks and Internet information queries.

**Answer:** AE

11. Which two statements describe the functions and operations of IDS and IPS systems? (Choose two.)

A. A network administrator entering a wrong password would generate a true-negative alarm.

B. A false positive alarm is generated when an IDS/IPS signature is correctly identified.

C. An IDS is significantly more advanced over IPS because of its ability to prevent network attacks.

D. Cisco IDS works inline and stops attacks before they enter the network.

E. Cisco IPS taps the network traffic and responds after an attack.

F. Profile-based intrusion detection is also known as "anomaly detection".

**Answer:** BF

12. Refer to the exhibit. What statement is true about the interface S1/0 on router R1?

```
R1#sh mpls interfaces detail
Interface Serial1/0:
        IP tagging enabled
        TSP Tunnel tagging not enabled
        Tag Frame Relay Transport tagging not enabled
        BGP tagging not enabled
        Tagging not operational
        Fast Switching Vectors:
          IP to Tag Fast Switching Vector
          Tag Switching Turbo Vector
        MTU = 1500
```

A. Labeled packets can be sent over an interface.

B. MPLS Layer 2 negotiations have occurred.

C. IP label switching has been disabled on this interface.

D. None of the MPLS protocols have been configured on the interface.

**Answer:** D

13. Which two network attack statements are true? (Choose two.)

A. Access attacks can consist of password attacks, trust exploitation, port redirection, and man-in-the-middle attacks.

B. Access attacks can consist of UDP and TCP SYN flooding, ICMP echo-request floods, and ICMP directed broadcasts.

C. DoS attacks can be reduced through the use of access control configuration, encryption, and RFC 2827 filtering.

D. DoS attacks can consist of IP spoofing and DDoS attacks.

E. IP spoofing can be reduced through the use of policy-based routing.

F. IP spoofing exploits known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

**Answer:** AD

14. What are the four steps, in their correct order, to mitigate a worm attack?

A. contain, inoculate, quarantine, and treat

B. inoculate, contain, quarantine, and treat

C. quarantine, contain, inoculate, and treat

D. preparation, identification, traceback, and postmortem

E. preparation, classification, reaction, and treat

F. identification, inoculation, postmortem, and reaction

**Answer:** A

15. 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:** ADF

16. 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 3704 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:** ABC

17. Which statement describes Reverse Route Injection (RRI)?

A. A static route that points towards the Cisco Easy VPN server is created on the remote client.

B. A static route is created on the Cisco Easy VPN server for the internal IP address of each VPN client.

C. A default route is injected into the route table of the remote client.

D. A default route is injected into the route table of the Cisco Easy VPN server.

**Answer:** B

18. What are two possible actions an IOS IPS can take if a packet in a session matches a signature? (Choose two.)

A. reset the connection

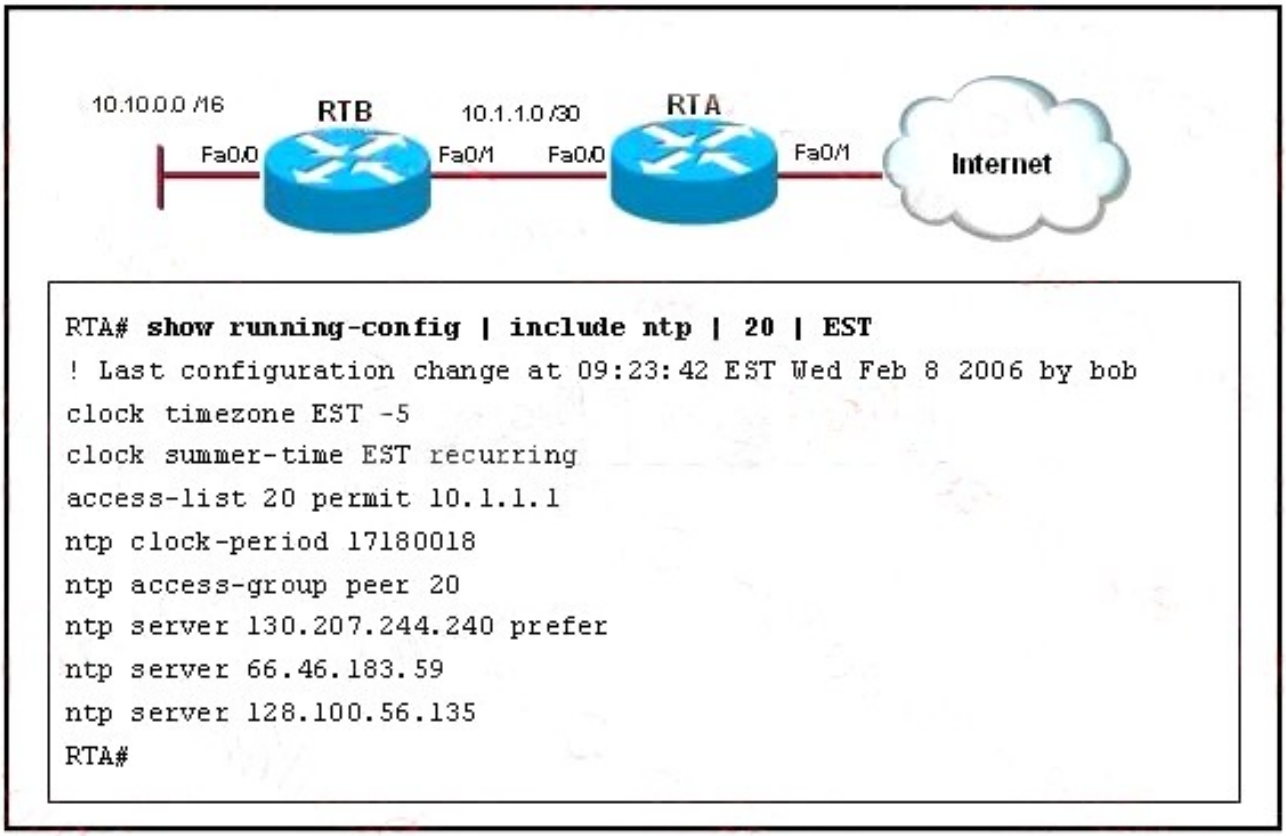
B. forward the packet

C. check the packet against an ACL

D. drop the packet

**Answer:** AD

19. 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:** AB

20. What is a reason for implementing MPLS in a network?

A. MPLS eliminates the need of an IGP in the core.

B. MPLS reduces the required number of BGP-enabled devices in the core.

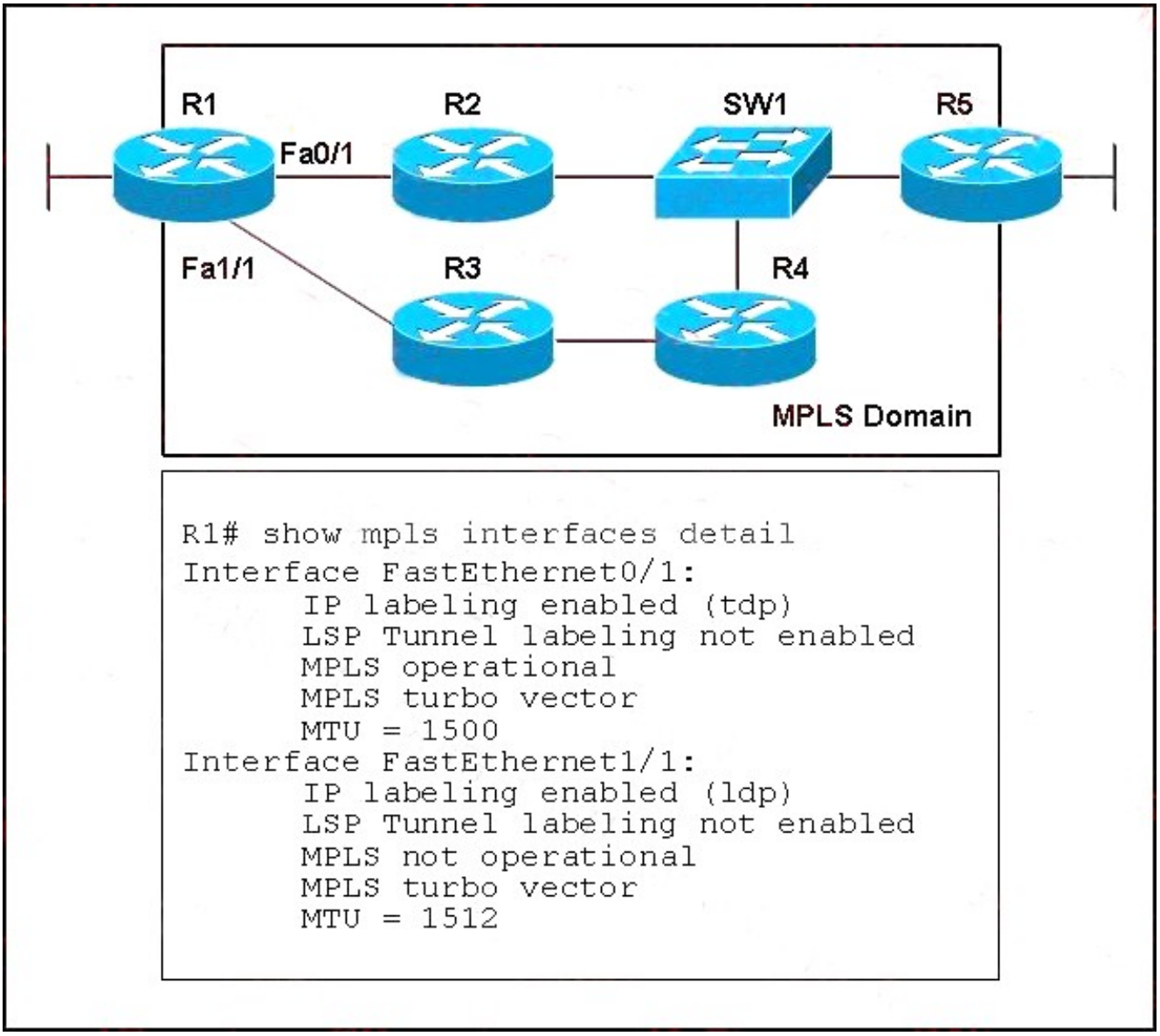
C. Reduces routing table lookup since only the MPLS core routers perform routing table lookups.

D. MPLS eliminates the need for fully meshed connections between BGP enabled devices.

**Answer:** B

21. Refer to the exhibit. The show mpls interfaces detail command has been used to display information

about the interfaces on router R1 that have been configured for label switching. Which statement is true about the MPLS edge router R1?




A. Packets can be labeled and forwarded out interface Fa0/1 because of the MPLS operational status of the interface.

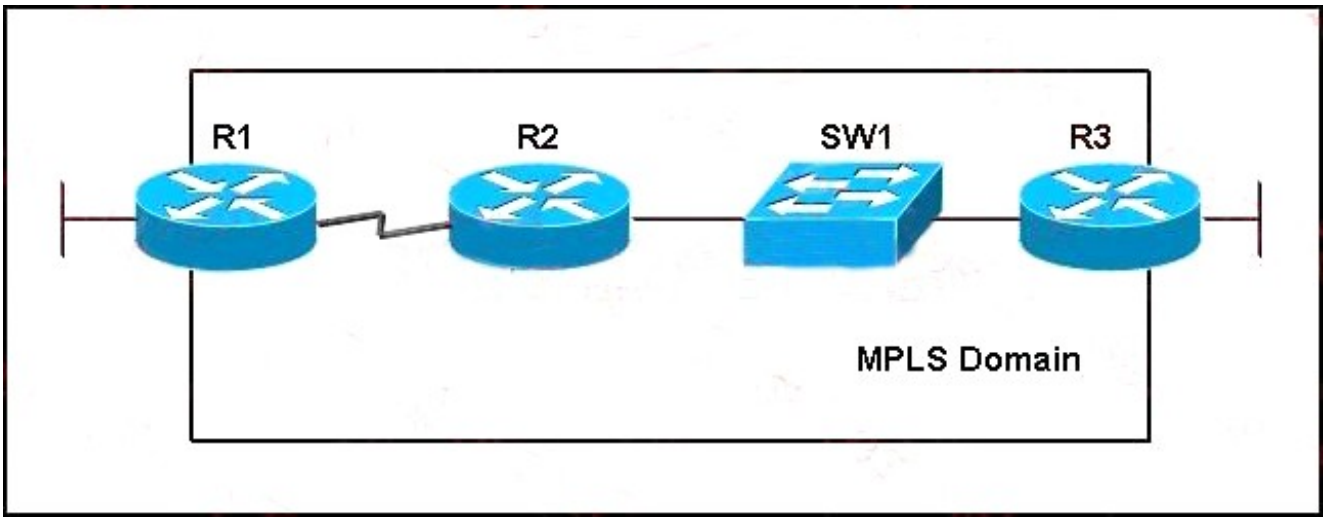
B. Because LSP tunnel labeling has not been enabled on interface Fa0/1, packets cannot be labeled and forwarded out interface Fa0/1.

C. Packets can be labeled and forwarded out interface Fa1/1 because MPLS has been enabled on this interface.

D. Because the MTU size is increased above the size limit, packets cannot be labeled and forwarded out interface Fa1/1.

**Answer:** A

22. Refer to the exhibit. MPLS has been configured on all routers in the domain. In order for R2 and R3 to forward frames between them with label headers, what additional configuration will be required on devices that are attached to the LAN segment?




A. Decrease the maximum MTU requirements on all router interfaces that are attached to the LAN segment.

B. Increase the maximum MTU requirements on all router interfaces that are attached to the LAN segment.

C. No additional configuration is required. Interface MTU size will be automatically adjusted to accommodate the larger size frames.

D. No additional configuration is required. Frames with larger MTU size will be automatically fragmented and forwarded on all LAN segments.

**Answer:** B

23. 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:** ABD

24. 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:** BCF

25. 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

26. Which two statements about an IDS are true? (Choose two.)

A. The IDS is in the traffic path.

B. The IDS can send TCP resets to the source device.

C. The IDS can send TCP resets to the destination device.

D. The IDS listens promiscuously to all traffic on the network.

E. Default operation is for the IDS to discard malicious traffic.

**Answer:** BD

27. Which statement about an IPS is true?

A. The IPS is in the traffic path.

B. Only one active interface is required.

C. Full benefit of an IPS will not be realized unless deployed in conjunction with an IDS.

D. When malicious traffic is detected, the IPS will only send an alert to a management station.

**Answer:** A

28. 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:** ACF

29. During the Easy VPN Remote connection process, which phase involves pushing the IP address, Domain Name System (DNS), and split tunnel attributes to the client?

A. mode configuration

B. the VPN client establishment of an ISAKMP SA

C. IPsec quick mode completion of the connection

D. VPN client initiation of the IKE phase 1 process

**Answer:** A

30. When configuring the Cisco VPN Client, what action is required prior to installing Mutual Group Authentication?

A. Transparent tunneling must be enabled.

B. A valid root certificate must be installed.

C. A group pre-shared secret must be properly configured.

D. The option to "Allow Local LAN Access" must be selected.

**Answer:** B