IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

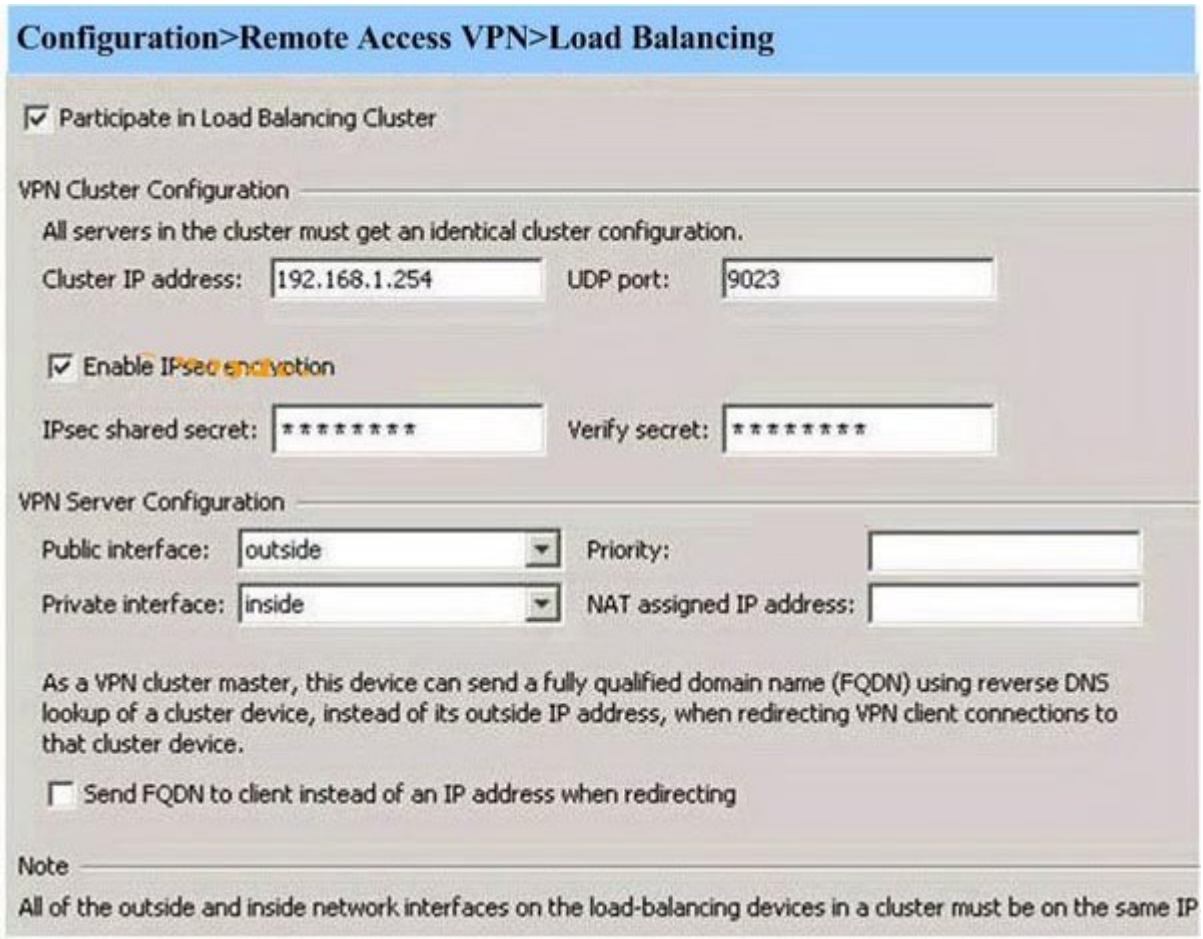
http://www.itrenzheng.com

Exam : **642-515**

Title : Securing Networks with ASA Advanced

Version : Demo

1. The following exhibit shows a Cisco ASA security appliance configured to participate in a VPN cluster. According to the exhibit, to which value will you set the priority to increase the chances of this Cisco ASA security appliance becoming the cluster master?



A. 100

B. 0

C. 10

D. 1

Answer: C

2. Tom works as a network administrator for the CISCO company. The primary adaptive security appliance in an active/standby failover configuration failed, so the secondary adaptive security appliance was automatically activated. Tom then fixed the problem. Now he would like to restore the primary to active status. Which one of the following commands can reactivate the primary adaptive security appliance and restore it to active status while issued on the primary adaptive security appliance?

A. failover reset

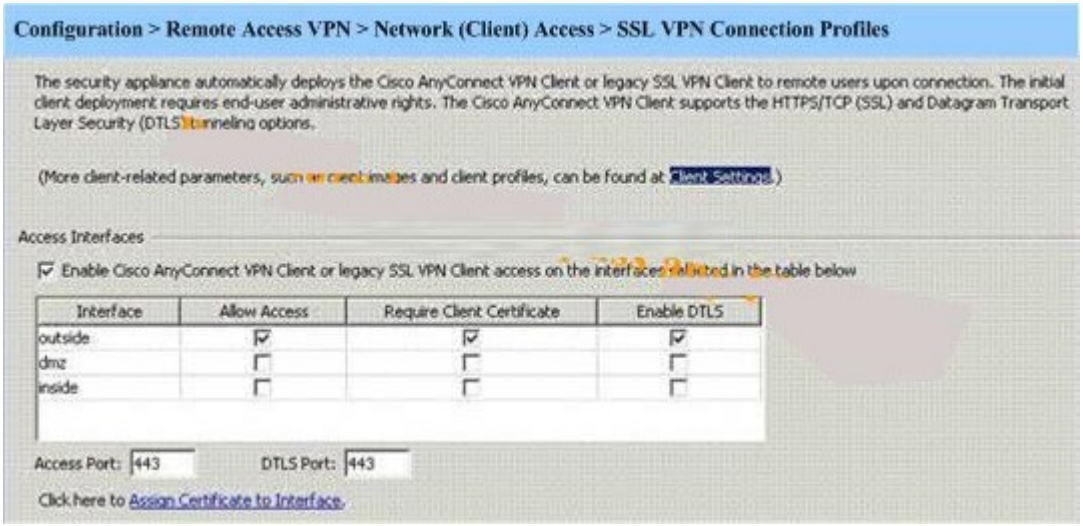
B. failover primary active

C. failover active

D. failover exec standby

Answer: C

3. You work as a network administrator for your company. Study the exhibit carefully. ASDM is short for Adaptive Security Device Manager. You are responsible for multiple remote Cisco ASA security appliances administered through Cisco ASDM. Recently, you have been tasked to configure one of these Cisco ASA security appliances for SSL VPNs and are requiring a client certificate, as shown. How will this configuration affect your next ASDM connection to this Cisco ASA security appliance?



A. You would be required to download the identity certificate of the remote Cisco ASA security appliance.

B. You would be asked to present an identity certificate. If you did not have one, the Cisco ASA security appliance would prompt you for authentication credentials, consisting of a username and password.

C. Your connection would be handled the way it is always handled by this Cisco ASA security appliance.

D. You would be required to have an identity certificate that the Cisco ASA security appliance can use for authentication.

Answer: D

4. Which three statements correctly describe protocol inspection on the Cisco ASA adaptive security appliance? (Choose three.)

A. For the security appliance to inspect packets for signs of malicious application misuse, you must enable advanced (application layer) protocol inspection.

B. If you want to enable inspection globally for a protocol that is not inspected by default or if you want to globally disable inspection for a protocol, you can edit the default global policy.

C. The protocol inspection feature of the security appliance securely opens and closes negotiated ports

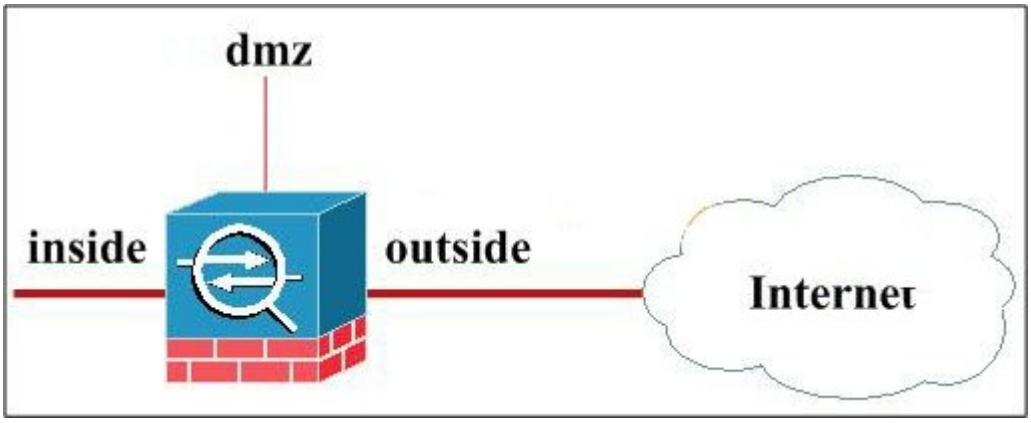
and IP addresses for legitimate client-server connections through the security appliance.

D. If inspection for a protocol is not enabled, traffic for that protocol may be blocked.

Answer: BCD

5. Study the following exhibit carefully. You work as the network administrator of a corporate Cisco ASA security appliance with a Cisco ASA AIP-SSM. You are asked to use the AIP-SSM to protect corporate DMZ web servers. The AIP-SSM has been configured, and a service policy has been configured to identify the traffic to be passed to the AIP-SSM.

On which two interfaces would application of the service policy for the AIP-SSM be most effective while causing the least amount of impact to Cisco ASA security appliance performance? (Choose two.)



A. Internet interface

B. dmz interface

C. globally on all interfaces

D. outside interface

Answer: BD

6. Multimedia applications transmit requests on TCP, get responses on UDP or TCP, use dynamic ports, and use the same port for source and destination, so they can pose challenges to a firewall. Which three items are true about how the Cisco ASA adaptive security appliance handles multimedia applications? (Choose three.)

A. It dynamically opens and closes UDP ports for secure multimedia connections, so you do not need to open a large range of ports.

B. It supports SIP with NAT but not with PAT.

C. It supports multimedia with or without NAT.

D. It supports RTSP, H.323, Skinny, and CTIQBE.

Answer: ACD

7. Which two options are correct about the impacts of this configuration? (Choose two.)

class-map INBOUND_HTTP_TRAFFIC

match access-list TOINSIDEHOST

class-map OUTBOUND_HTTP_TRAFFIC

match access-list TOOUTSIDEHOST

policy-map MYPOLICY

class INBOUND_HTTP_TRAFFIC

inspect http

set connection conn-max 100

policy-map MYOTHERPOLICY

class OUTBOUND_HTTP_TRAFFIC

inspect http

service-policy MYOTHERPOLICY interface inside

service-policy MYPOLICY interface outside

A. Traffic that matches access control list TOINSIDEHOST is subject to HTTP inspection and maximum connection limits.

B. Traffic that enters the security appliance through the inside interface is subject to HTTP inspection.

C. Traffic that enters the security appliance through the outside interface and matches access control list TOINSIDEHOST is subject to HTTP inspection and maximum connection limits.

D. Traffic that enters the security appliance through the inside interface and matches access control list TOOUTSIDEHOST is subject to HTTP inspection.

Answer: CD

8. Refer to the exhibit. You have configured a Layer 7 policy map to match the size of HTTP header fields that are traversing the network. Based on this configuration, will HTTP headers that are greater than 200 bytes be logged?

```
policy-map type inspect http TEST
  parameters
  match request header length gt 100
    reset
  match request header length gt 200
    log
```

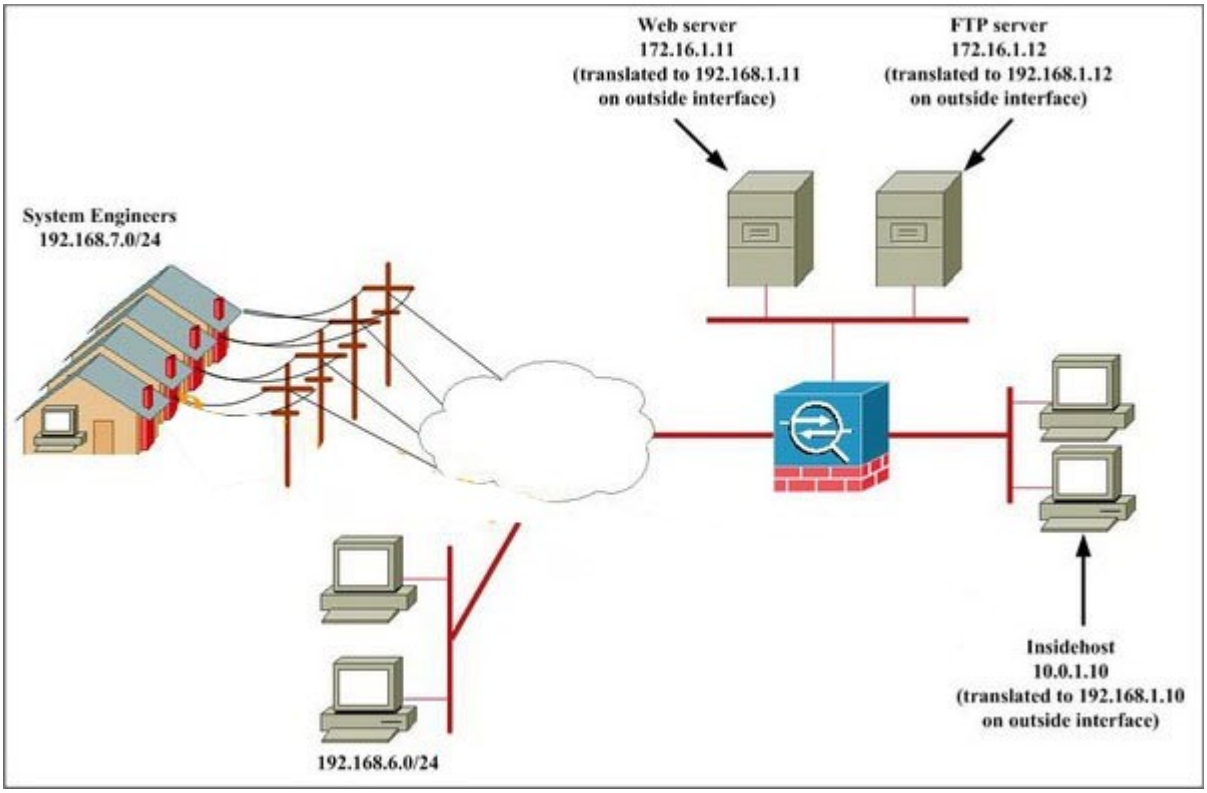
A. No, because the reset action for headers greater than 100 bytes would be the first match.

B. Yes, because the log action for headers greater than 200 bytes would be the last match.

C. Yes, because the reset action for headers greater than 100 bytes and the log action for headers greater than 200 bytes would both be applied.
D. No, because reset or log actions are a part of the service policy and the Layer 7 policy map.
Answer: A

9. What is the reason that you want to configure VLANs on a security appliance interface?
A. for use in conjunction with device-level failover to increase the reliability of your security appliance
B. for use in transparent firewall mode, where only VLAN interfaces are used
C. to increase the number of interfaces available to the network without adding additional physical interfaces or security appliances
D. for use in multiple context mode, where you can map only VLAN interfaces to contexts
Answer: C

10. You work as a network security administrator for your company. Now, you are asked to configure the corporate Cisco ASA security appliance to take the following steps on its outside interface:
--rate limit all IP traffic from telecommuting system engineers to the insidehost
--drop all HTTP requests from the Internet to the web server that have a body length greater than 1000 bytes
--prevent users on network 192.168.6.0/24 from using the FTP PUT command to store .exe files on the FTP server
In order to achieve this objective, which set of Modular Policy Framework components will be included?



A. one Layer 7 class map, two Layer 7 policy maps, three Layer 3/4 class maps, one Layer 3/4 policy map

B. three Layer 7 policy maps, one Layer 3/4 class map, one Layer 3/4 policy map

C. one Layer 7 class map, one Layer 7 policy map, three Layer 3/4 class maps, one Layer 3/4 policy map

D. two Layer 7 class maps, one Layer 7 policy map, three Layer 3/4 class maps, one Layer 3/4 policy map

Answer: A

11. Which one of the following commands can provide detailed information about the crypto map configurations of a Cisco ASA adaptive security appliance?

A. show ipsec sa

B. show crypto map

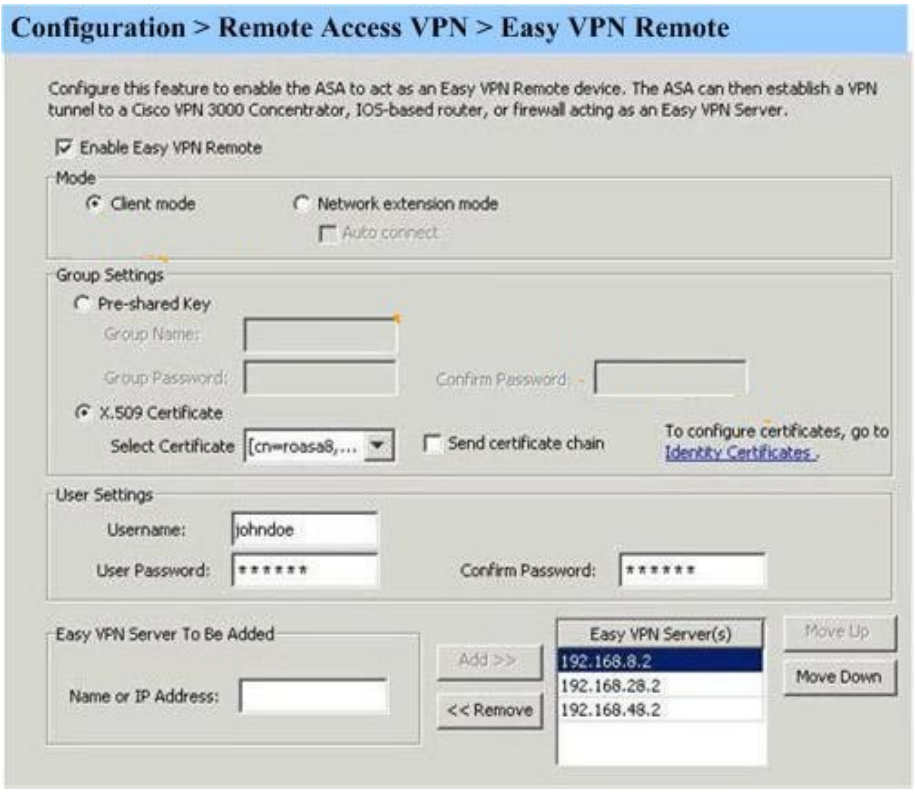
C. show run ipsec sa

D. show run crypto map

Answer: D

12. Cisco ASA 5500 Series Adaptive Security Appliances are easy-to-deploy solutions that integrate world-class firewall, Unified Communications (voice/video) security, SSL and IPsec VPN, intrusion prevention (IPS), and content security services in a flexible, modular product family. You are asked to configure a Cisco ASA 5505 Adaptive Security Appliance as an Easy VPN hardware client. In the process of configuration, you defined a list of backup servers for the security appliance to use. After several hours of being connected to the primary VPN server, the security appliance fails. You notice that your Easy VPN

hardware client has now connected to a backup server that is not defined within the configuration of the client. Where did your Easy VPN hardware client get this backup server?



A. The connection profile that was configured on the primary VPN server was pushed to your Easy VPN hardware client and overwrote the list of backup servers that you had configured.

B. The group policy that was configured on the primary VPN server was pushed to your Easy VPN client and overwrote the list of backup servers that you had configured.

C. The backup servers that you listed were not configured as VPN servers, so the Easy VPN hardware client used the list of backup servers retrieved from the primary server.

D. The backup servers that you listed were no longer available, so the Easy VPN hardware client used the list of backup servers that it retrieved from the primary server.

Answer: B

13. Which three features can the Cisco ASA adaptive security appliance support? (Choose three.)

A. BGP dynamic routing

B. 802.1Q VLANs

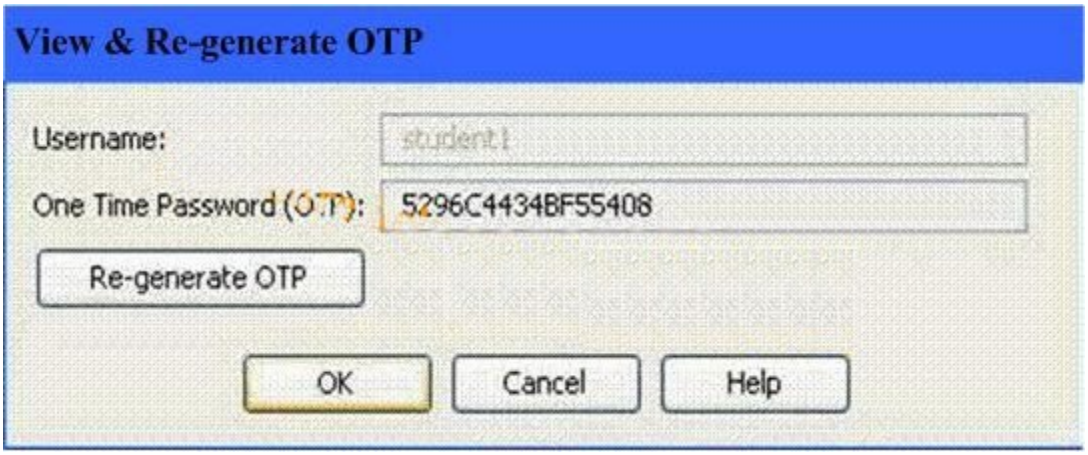
C. OSPF dynamic routing

D. static routes

Answer: BCD

14. You are the network administrator for your company. Study the exhibit carefully. You are responsible

for a Cisco ASA security appliance configured with a local CA. According to the exhibit below, what is the reason that the user student1 will use this password?



A. retrieval of the Cisco ASA security appliance identity certificate

B. retrieval of the digital certificate from the local CA on the Cisco ASA security appliance

C. the initial authentication to the SSL VPN server

D. authentication to the SSL VPN server

Answer: B

15. Which two statements are true about multiple context mode? (Choose two.)

A. Multiple context mode does not support IPS, IPsec, and SSL VPNs, or dynamic routing protocols.

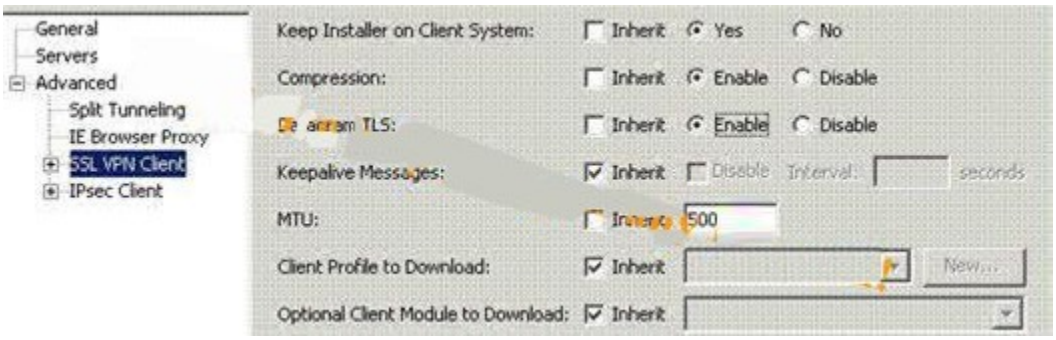
B. Multiple context mode enables you to create multiple independent virtual firewalls with their own security policies and interfaces.

C. Multiple context mode enables you to add to the security appliance a hardware module that supports up to four independent virtual firewalls.

D. When you convert from single mode to multiple mode, the security appliance automatically adds an entry for the admin context to the system configuration with the name "admin."

Answer: BD

16. Observe the following exhibit carefully. When TCP connections are tunneled over another TCP connection and latency exists between the two endpoints, each TCP session would trigger a retransmission, which can quickly spiral out of control when the latency issues persist. This issue is often called TCP-over-TCP meltdown. According to the presented Cisco ASDM configuration, which Cisco ASA security appliance configuration will most likely solve this problem?



A. Compression

B. MTU size of 500

C. Keepalive Messages

D. Datagram TLS

Answer: D

17. For creating and configuring a security context, which three tasks are mandatory? (Choose three.)

A. allocating interfaces to the context

B. assigning MAC addresses to context interfaces

C. creating a context name

D. specifying the location of the context startup configuration

Answer: ACD

18. Which two statements about the downloadable ACL feature of the security appliance are correct? (Choose two.)

A. Downloadable ACLs are supported using TACACS+ or RADIUS.

B. Downloadable ACLs enable you to store full ACLs on a AAA server and download them to the security appliance.

C. The security appliance supports only per-user ACL authorization.

D. The downloadable ACL must be attached to a user or group profile on a AAA server.

Answer: BD

19. While implementing QoS, which two types of queues are available on the Cisco ASA security appliance? (Choose two.)

A. weighted fair

B. round robin queue

C. low latency queue

D. best effort queue

Answer: CD

20. Which three commands can display the contents of flash memory on the Cisco ASA adaptive security appliance? (Choose three.)

A. show disk0:

B. show memory

C. dir

D. show flash:

Answer: ACD