Cisco 642-515

CISCO 642-515 Securing Networks with ASA Advanced

Practice Test

Version 3.1

QUESTION NO: 1

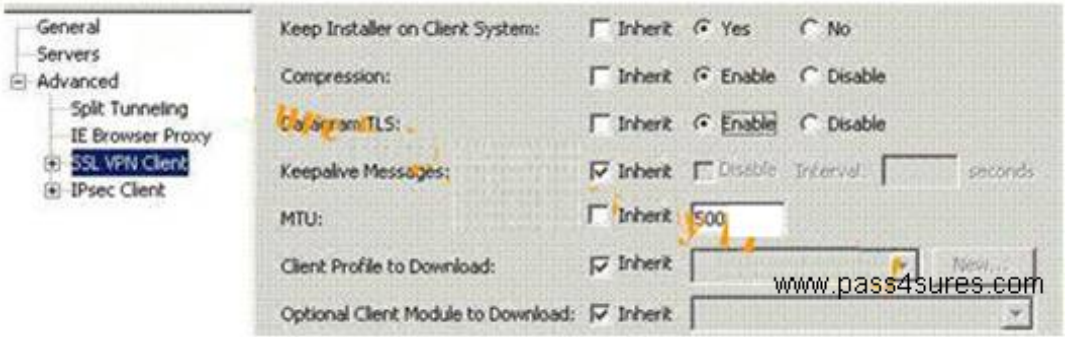
Which two statements correctly describe configuring active/active failover? (Choose two.)

A. You must assign contexts to failover groups from the admin context.
B. Both units must be in multiple mode.
C. You must configure two failover groups: group 1 and group 2.
D. You must use a crossover cable to connect the failover links on the two failover peers.

Answer: B,C

QUESTION NO: 2

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

QUESTION NO: 3

The IT department of your company must perform a custom-built TCP application within the clientless SSL VPN portal configured on your Cisco ASA security appliance. The application should be run by users who have either guest or normal user mode privileges. In order to allow this application to run, how to configure the clientless SSL VPN portal?

A. configure a smart tunnel for the application

B. configure a bookmark for the application
C. configure the plug-in that best fits the application
D. configure port forwarding for the application

Answer: A

QUESTION NO: 4

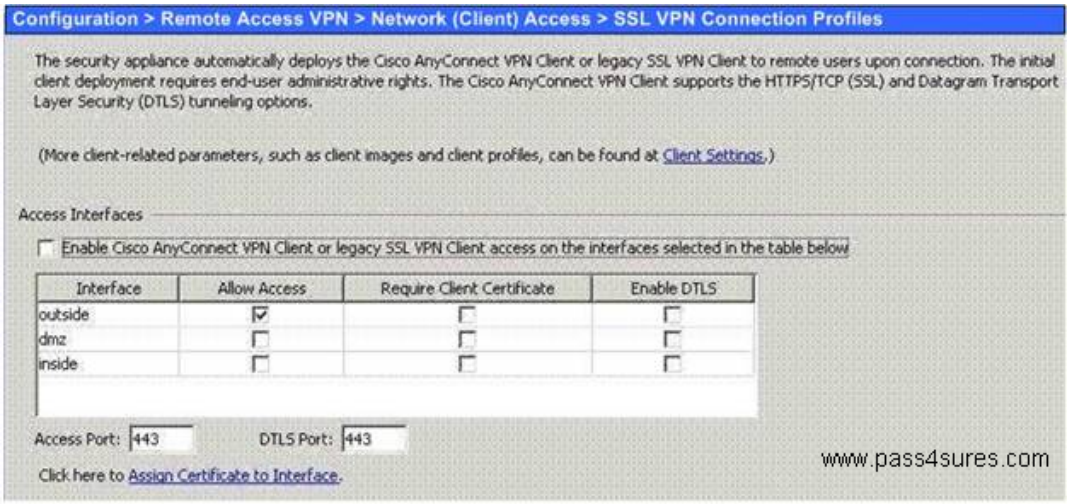
According to the following exhibit. When a host on the inside network attempted an HTTP connection to a host at IP address 172.26.10.100, which address pool will be used by the Cisco ASA security appliance for the NAT?

A. 192.168.8.101 - 192.168.8.105
B. 192.168.8.20 - 192.168.8.100
C. 192.168.8.106 - 192.168.8.110
D. 192.168.8.20 - 192.168.8.110

Answer: B

QUESTION NO: 5

Study the following exhibit carefully. You are asked to configure the Cisco ASA security appliance with a connection profile and group policy for full network access SSL VPNs. During a test of the configuration using the Cisco AnyConnect VPN Client, the connection times out. In the process of troubleshooting, you determine to make configuration changes. According to the provided Cisco ASDM configuration, which configuration change will you begin with?



A. Require a client certificate on the interface.
B. Enable an SSL VPN client type on the interface.
C. Enable DTLS on the interface.
D. Enable a different access port that doesn't conflict with Cisco ASDM.

Answer: B

QUESTION NO: 6

You are the network security administrator for the P4S company. You create an FTP inspection policy including the strict option, and it is applied to the outside interface of the corporate adaptive security appliance. How to handle FTP on the security appliance after this policy is applied? (Choose three.)

A. FTP inspection is applied to traffic entering the inside interface.
B. Strict FTP inspection is applied to traffic entering the outside interface.
C. FTP inspection is applied to traffic exiting the inside interface.
D. Strict FTP inspection is applied to traffic exiting the outside interface.

Answer: A,B,D

QUESTION NO: 7

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

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

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

Answer: A,C,D

QUESTION NO: 8

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. After configuring port forwarding for a clientless SSL VPN connection, if port forwarding is to work, which end user privilege level is required at the endpoint?

A. system level
B. guest level
C. user level
D. administrator level

Answer: D

QUESTION NO: 9

Which two methods can be used to decrease the amount of time it takes for an active Cisco ASA adaptive security appliance to fail over to its standby failover peer in an active/active failover configuration? (Choose two.)

A. decrease the interface failover poll time
B. decrease the unit failover poll time
C. use the special serial failover cable to connect the security appliances
D. use single mode

Answer: A,B

QUESTION NO: 10

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: A,C,D

QUESTION NO: 11

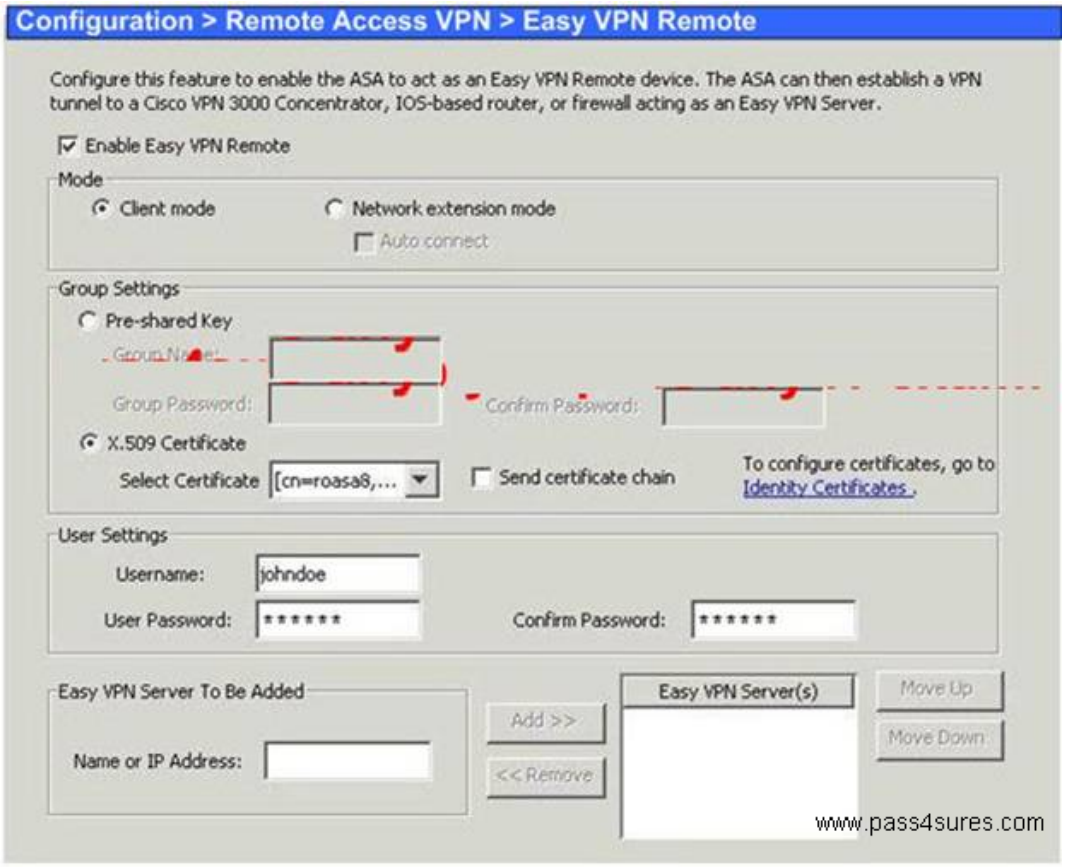
Which options can a clientless SSL VPN user access from a web browser without port forwarding, smart tunnels, or browser plug-ins?

A. web-enabled applications
B. Microsoft Outlook Web Access
C. files on the network, via FTP or the CIFS protocol
D. internal websites

Answer: A,B,C,D

QUESTION NO: 12

Cisco ASA 5505 Adaptive Security Appliance is designed for providing high-performance security services. Study the following exhibit carefully. You are asked to configure a Cisco ASA 5505 Adaptive Security Appliance as an Easy VPN hardware client. When the telecommuter using the ASA 5505 Adaptive Security Appliance for remote access first tries to connect to resources on the corporate network, he is prompted for authentication. Which two group policy features will require authentication, even if a username and password are configured on the Easy VPN hardware client? (Select two.)



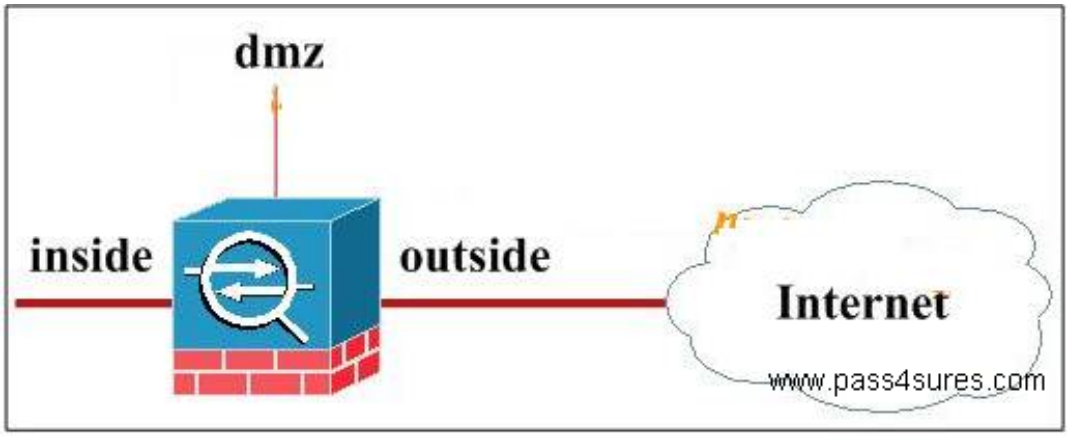
A. Individual User Authentication
B. Certificate Authentication
C. Secure Unit Authentication
D. Extended Authentication

Answer: A,C

QUESTION NO: 13

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. dmz interface
B. outside interface
C. globally on all interfaces
D. Internet interface

Answer: A,B

QUESTION NO: 14

You work as the network administrator for your company. Now, you are asked to configure the Cisco ASA security appliance, using Modular Policy Framework to prevent executables with the .exe file extension from being downloaded. Which regular expression should be created to match the .exe file extension?

A. *.exe
B. .+\.[Ee][Xx][Ee]
C. .+.[Ee][Xx][Ee]
D. .*\.[Ee][Xx][Ee.

Answer: B

QUESTION NO: 15

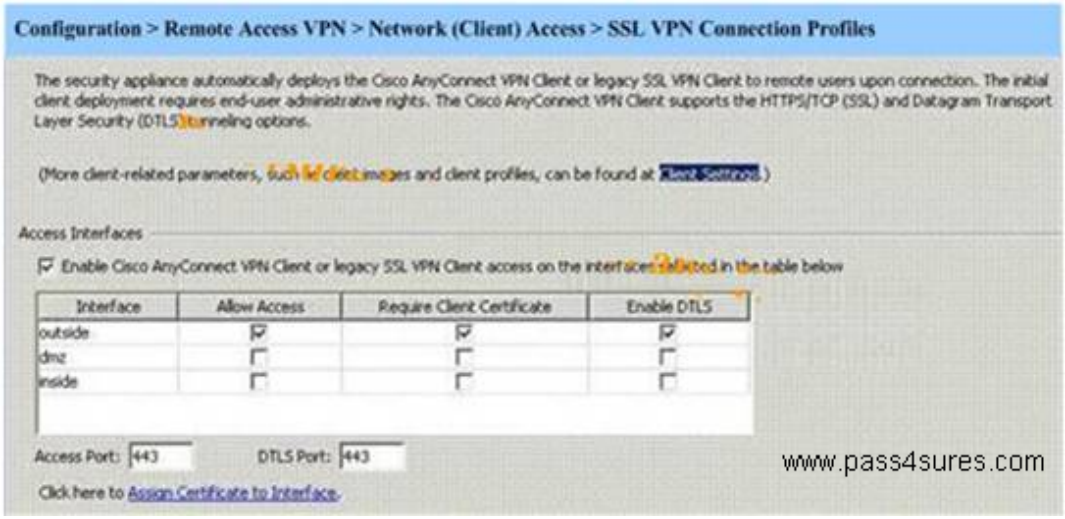
For the following commands, which one causes the Cisco CSC-SSM to load a new software image from a remote TFTP server, via the CLI?

A. hw module 1 recover reload
B. copy tftp hardware:module1
C. hw module 1 recover config
D. hw module 1 recover boot

Answer: D

QUESTION NO: 16

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 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.
B. Your connection would be handled the way it is always handled by this Cisco ASA security appliance.
C. You would be required to have an identity certificate that the Cisco ASA security appliance can use for authentication.
D. You would be required to download the identity certificate of the remote Cisco ASA security appliance.

Answer: C

QUESTION NO: 17

You are a new employee of your company. Recently, you have been tasked to configure Cisco ASA security appliance for multiple VLANs that use one physical interface. The switch to which the physical Cisco ASA security appliance interface is connected should be configured for the appropriate VLAN tagging protocol. In order to achieve this goal, which VLAN tagging protocol will the Cisco ASA security appliance use to communicate with this switch?

A. ISL
B. IEEE 802.1Q
C. IEEE 802.1AE
D. IEEE 802.3

Answer: B

QUESTION NO: 18

In an active/active failover configuration, which event triggers failover at the failover group level?

A. The no failover active group group_id command is entered in the system configuration.
B. The no failover active command is entered in the system configuration.
C. The unit has a software failure.
D. Two monitored interfaces in the group fail.

Answer: A

QUESTION NO: 19

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?