



642-515

Securing Networks with ASA Advanced Exam

Q&A

DEMO Version

Copyright (c) 2012 Chinatag LLC. All rights reserved.

Important Note

Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have (average) more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

QUESTION 1

Refer to the exhibit. You are configuring a Cisco ASA security appliance to participate in a VPN cluster. Based on the exhibit, to which value would you set the priority to increase the chances of this Cisco ASA security appliance becoming the cluster master?

Configuration > Remote Access VPN > Load Balancing

Participate in Load Balancing Cluster

VPN Cluster Configuration

All servers in the cluster must get an identical cluster configuration.

Cluster IP address: UDP port:

Enable IPsec encryption

IPsec shared secret: Verify secret:

VPN Server Configuration

Public interface: Priority:

Private interface: NAT assigned IP address:

As a VPN cluster master, this device can send a fully qualified domain name (FQDN) using reverse DNS lookup of a cluster device, instead of its outside IP address, when redirecting VPN client connections to that cluster device.

Send FQDN to client instead of an IP address when redirecting

Note

All of the outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP

- A. 0
- B. 1
- C. 10
- D. 100

Answer: C

QUESTION 2

Refer to the exhibit. You are the administrator of multiple remote Cisco ASA security appliances, which are administered through Cisco ASDM. You recently configured one of these Cisco ASA security appliances for SSL VPNs and are requiring a client certificate, as shown. How would this configuration affect your next ASDM connection to this Cisco ASA security appliance?

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#).)

PassGuide.com

Access Interfaces

Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Access Port: DTLS Port:

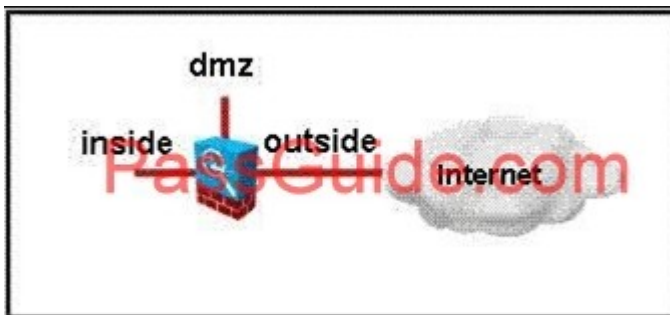
[Click here to Assign Certificate to Interface.](#)

- 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 download the identity certificate of the remote 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

QUESTION 3

Refer to the exhibit. You are the administrator of a corporate Cisco ASA security appliance with a Cisco ASA AIP-SSM. You have been tasked to deploy 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 that is 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.)

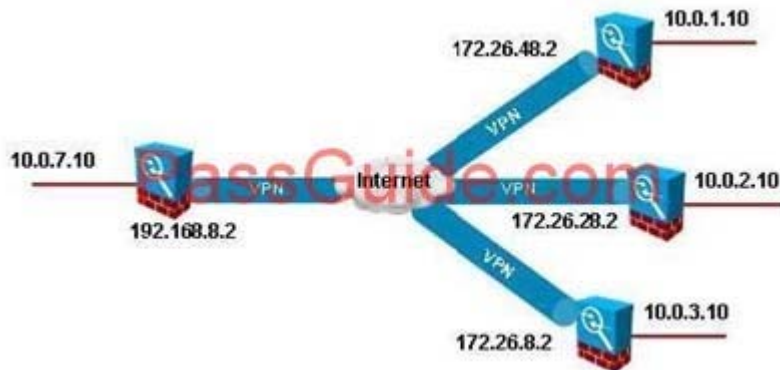


- A. Inside interface
- B. Dmz interface
- C. Internet interface
- D. Globally on all interfaces
- E. Outside interface

Answer: BE

QUESTION 4

Refer to the exhibit. You are configuring the Cisco ASA security appliance as the hub in a hub- and-spoke site-to-site VPN. Which of these configurations will enable traffic to flow between spokes?



A.

The screenshot shows the configuration for the 'outside' interface on a Cisco ASA security appliance. The configuration is as follows:

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Redundant	Member	H
GigabitEthernet0/0	outside	Yes	0	192.168.7.2	255.255.255.0	No	No	
GigabitEthernet0/1	inside	Yes	100	10.0.7.1	255.255.255.0	No	No	
GigabitEthernet0/2		No				No	No	
GigabitEthernet0/3	dmz	Yes	50	172.16.7.1	255.255.255.0	No	No	
Management0/0		No				No	No	

Below the table, there are two checkboxes:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface

B.

Add IPsec Site-to-Site Connection Profile

Peer IP Address: Static

Connection Name: Same as IP Address Sub

Interface:

IKE Authentication

Pre-shared Key:

Identity Certificate:

Protected Networks

Local Network:

Remote Network:

Encryption Algorithms

IKE Proposal:

C.

Add Internal Group Policy

Name:

Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec L2TP/IPsec

Filter: Inherit

Configuration 3

D

Configuration > Device Setup > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Redundant	Member	M	Add
GigabitEthernet0/0	outside	Yes	0	192.168.7.2	255.255.255.0	No	No		
GigabitEthernet0/1	inside	Yes	100	10.0.7.1	255.255.255.0	No	No		
GigabitEthernet0/2		No							
GigabitEthernet0/3	dmz	Yes	50	172.16.7.1	255.255.255.0	No	No		

Answer:

QUESTION 5

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

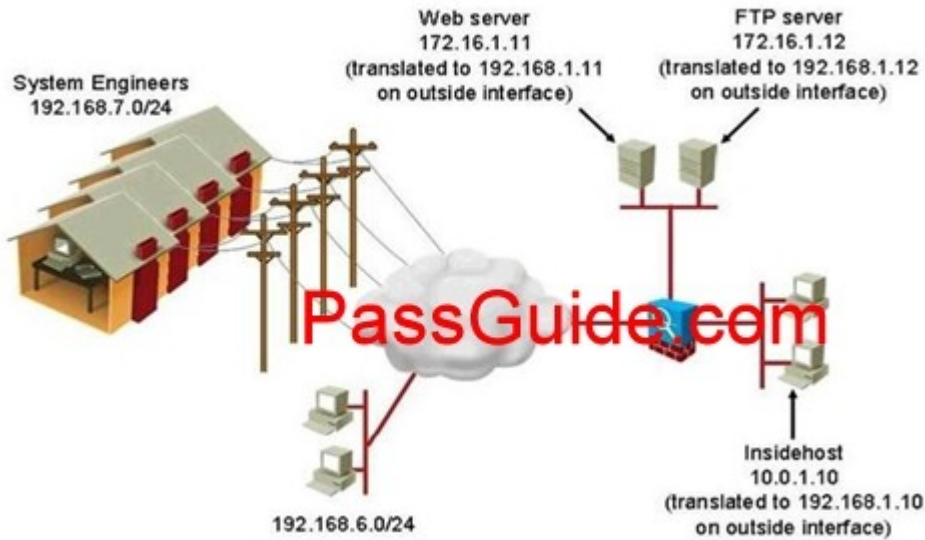
Answer: A

QUESTION 6

Refer to the exhibit. The network security administrator for XYZ Corporation wants to configure the corporate Cisco ASA security appliance to take the following actions 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 Which set of Modular Policy Framework components will be involved in accomplishing this goal?

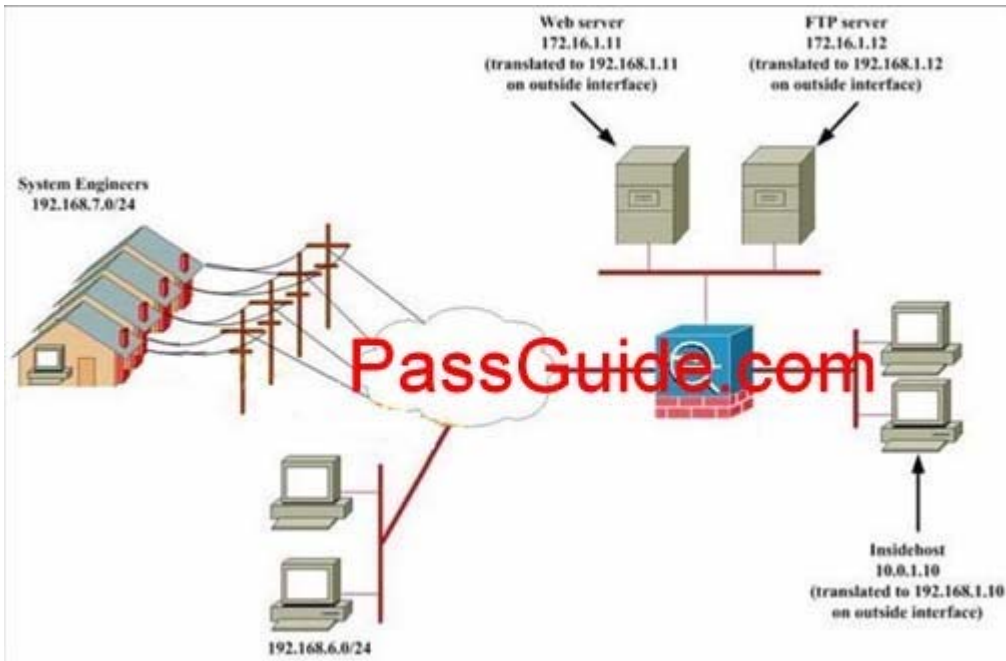


- A. One Layer 7 class map, two Layer 7 policy maps, three Layer 3/4 class maps, one Layer ?policy map
- B. One Layer 7 class map, one Layer 7 policy map, three Layer 3/4 class maps, one Layer ?policy map
- C. Two Layer 7 class maps, one Layer 7 policy map, three Layer 3/4 class maps, one Layer ?policy map
- D. Three Layer 7 policy maps, one Layer 3/4 class map, one Layer 3/4 policy map

Answer: A

QUESTION 7

Refer to the exhibit. You have configured a Cisco ASA 5505 Adaptive Security Appliance as an Easy VPN hardware client. During the configuration, you defined a list of backup servers for the security appliance to use. After a few 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?

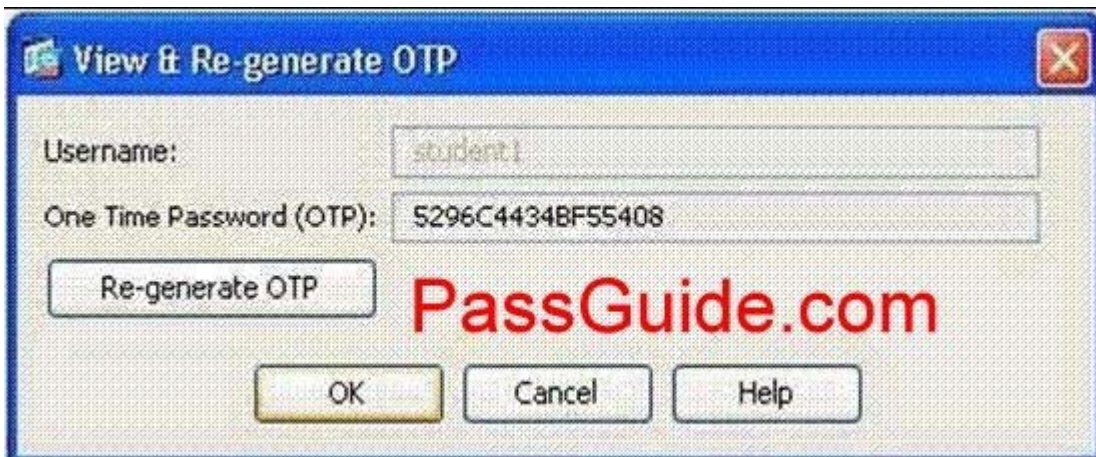


- A. The backup servers that you listed were no longer available, so the Easy VPN hardware client used the list of backup servers that it retrieved from the primary server.
- B. The group policy that was configured on the primary VPN server was pushed to your Easy VPN client and overwrote the list of backup servers that you had configured.
- C. The 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.
- D. 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.

Answer: B

QUESTION 8

Refer to the exhibit. You are the administrator of a Cisco ASA security appliance that is configured with a local CA. Based on the exhibit, for which purpose would the user student1 use this password?



- A. Authentication to the SSL VPN server
- B. Retrieval of the digital certificate from the local CA on the Cisco ASA security appliance
- C. Retrieval of the Cisco ASA security appliance identity certificate
- D. The initial authentication to the SSL VPN server

Answer: B

QUESTION 9

Refer to the exhibit. When TCP connections are tunneled over another TCP connection and latency exists between the two endpoints, each TCP session will trigger a retransmission, which can quickly spiral out of control when the latency issues persist. This issue is often referred to as TCP-over-TCP meltdown. Based on the Cisco ASDM configuration that is shown, which Cisco ASA security appliance configuration will help alleviate this problem?

Configuration > Remote Access VPN > Easy VPN Remote

Configure this feature to enable the ASA to act as an Easy VPN Remote device. The ASA can then establish a VPN tunnel to a Cisco VPN 3000 Concentrator, IOS-based router, or firewall acting as an Easy VPN Server.

Enable Easy VPN Remote

Mode

Client mode Network extension mode

Auto connect

Group Settings

Pre-shared Key

Group Name:

Group Password: Confirm Password:

X.509 Certificate

Select Certificate: Send certificate chain To configure certificates, go to [Identity Certificates](#).

User Settings

Username:

User Password: Confirm Password:

Easy VPN Server To Be Added

Name or IP Address:

192.168.8.2
192.168.28.2
192.168.48.2

- A. Keepalive Messages
- B. Compression
- C. MTU size of 500
- D. Datagram TLS

Answer: D