

**Exam 642-524 study material**

**Made available by CertsKing.com**



**Free 642-524 Exam Preparation Questions**

**Exam 642-524: Securing Networks with ASA Foundation**

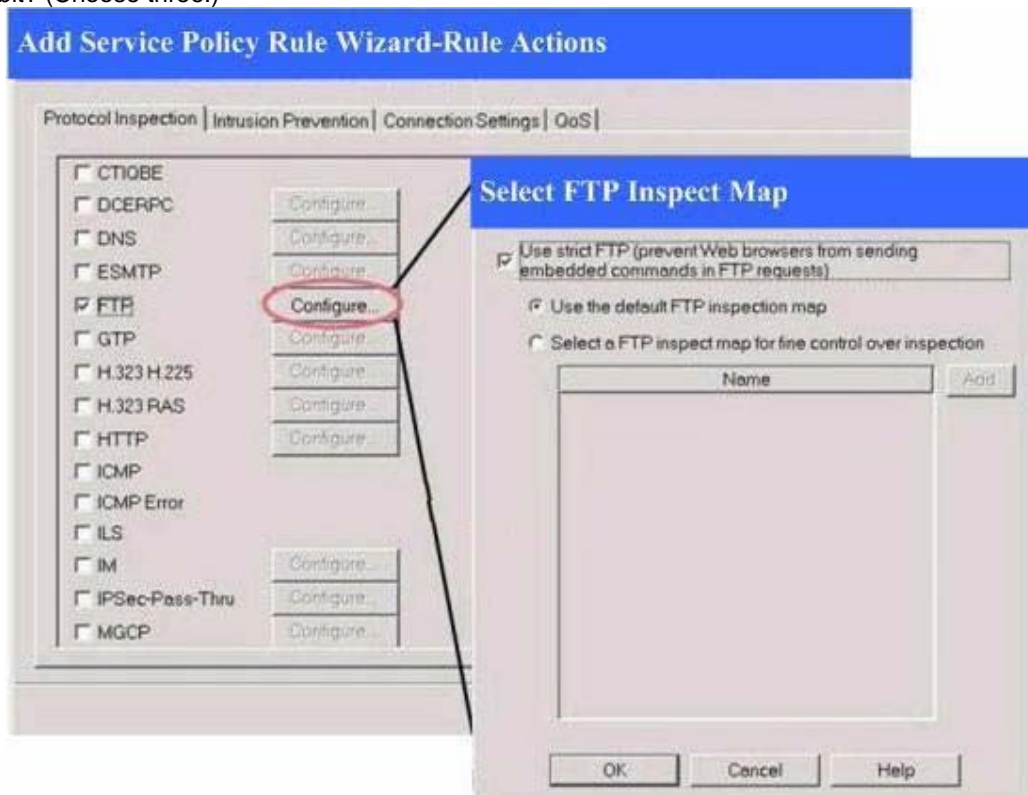
**Question:1**

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. An internet customer is sending HTTP traffic to a DMZ server with the external address of 192.168.1.4. Which command would redirect HTTP traffic bound for the DMZ web server to its real IP address of 10.10.11.4?

- A. static (dmz,inside) udp 192.168.1.4 www 10.10.11.4 www
- B. static (outside,dmz) tcp 192.168.1.4 www 10.10.11.4 www
- C. static (dmz,outside) tcp 192.168.1.4 www 10.10.11.4 www
- D. static (dmz,outside) tcp 10.10.11.4 www 192.168.1.4 www

**Answer: C****Question:2**

When applied to the default global inspection policy, which three effects are of this configuration according to the following exhibit? (Choose three.)



- A. filter FTP commands that are considered unsafe
- B. prevent web browsers from sending embedded commands in FTP requests
- C. require an FTP command to be acknowledged before allowing a new command
- D. track each FTP command and response sequence for the certain anomalous activity

**Answer: B, C, D****Question:3**

Which three items will be necessary for setting up a CSC SSM on the Cisco ASA? (Choose three.)

- A. activation codes
- B. the IP address of the CSC interface
- C. an SSL certificate to use for HTTPS connections
- D. an e-mail address for notifications

**Answer: A, B, D****Question:4**

The P4S network security department wants to adjust the default DoS drop rate thresholds for basic threat detection to trigger logs properly for its network environment. This can give more accurate information about the possibility of a DoS

attack. How to set the following values?

--Rate interval: 600 sec --Average rate: 50 drops per sec -

-Burst rate: 100 drops per sec

- A. Enter this command at the security appliance CLI: threat-detection rate dos-drop rate-interval 600 average-rate 50 burst-rate 100.
- B. Enter this command at the security appliance CLI: threat-detection rate inspect-drop rate-interval 600 average-rate 50 burst-rate 100.
- C. Enable basic threat detection, and enter the values in the activated fields in the Cisco ASDM Threat Detection panel.
- D. Enter the values in the fields provided in the Cisco ASDM Threat Detection panel.

**Answer: A**

**Question:5**

The ASDM client is supported on which PC operating systems? Choose the best answer.

- A. Windows and Sun Solaris
- B. Windows and Linux
- C. Windows, Linux, and Sun Solaris
- D. Windows, Macintosh, and Linux

**Answer: C**

**Question:6**

While using an adaptive security appliance code of version 7.0 or later, which two requirements should be satisfied for active/standby failover to work? (Choose two.)

- A. The number and types of interfaces on the failover peers must be identical.
- B. Both failover peers must be in multicontext mode.
- C. The failover peers must have the same amount of flash memory.
- D. The same interface cannot be used as both the LAN-based failover link and the stateful failover link.

**Answer: A, C**

**Question:7**

What is the inspect http HTTP\_TRAFFIC command used for in this policy map presented as follows?

```
P4S-hostname(config)# class-map inspection_default P4S-hostname(config-cmap)# match
default_inspection_traffic P4S-hostname(config)# class-map HTTP_TRAFFIC P4S-
hostname(config-cmap)# match port tcp eq 80 P4S-hostname(config)# class-map
HTTP_PROXY_TRAFFIC_8080 P4S-hostname(config-cmap)# match port tcp eq 8080 P4S-
hostname(config)# policy-map OUTSIDE_POLICY P4S-hostname(config-pmap)# class
inspection_default P4S-hostname(config-pmap-c)# inspect http HTTP_TRAFFIC P4S-
hostname(config-pmap-c)# inspect http HTTP_PROXY_TRAFFIC_8080 P4S-
hostname(config-pmap)# class HTTP_TRAFFIC P4S-hostname(config-pmap-c)# set
connection timeout tcp 0:10:0 P4S-hostname(config-pmap)# class HTTP_PROXY_TRAFFIC
P4S-hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

- A. It adds HTTP traffic inspection to the OUTSIDE\_POLICY policy map.
- B. It adds HTTP traffic inspection to the inspection-default global class map.
- C. It adds HTTP traffic limits to the OUTSIDE\_POLICY policy map.
- D. It adds HTTP traffic inspection on TCP port 8080 to the OUTSIDE\_POLICY policy map.

**Answer: A**

**Question:8**

What is the objective of the nat 0 command?

- A. The nat 0 command, followed by a range of IP addresses, specifies the addresses that are to be translated using network address translation.
- B. The nat 0 command, followed by an access list, specifies the addresses that are to be used in translations only once.
- C. The nat 0 command, followed by a range of IP addresses, specifies the addresses that are to be translated when used for IPsec.
- D. The nat 0 command, followed by an access list, specifies the addresses that are not to be translated.

**Answer: D**

**Question:9**

What is displayed as a result of entering the command syntax show aaa-server group1 host 192.168.30.60 in the security appliance?

- A. aaa-server configuration for server group group1
- B. aaa-server statistics for a particular host in server group group1
- C. aaa-server statistics for the host group1 at IP address 192.168.30.60
- D. aaa-server configuration for a particular host in server group group1

**Answer: B**

**Question:10**

Which three protocols are able to configure the Content Security and Control module for the Cisco ASA to scan?  
(Choose three.)

- A. POP3
- B. SMTP
- C. Telnet
- D. FTP

**Answer: A, B, D**

**Question:11**

According to the exhibit. Chose the appropriate command that will apply this policy map to an interface and the proper command that will apply it globally on the Cisco ASA. (Choose two.)

```
P4S-hostname(config)# class-map inspection_default P4S-hostname(config-cmap)# match default_inspection_traffic
P4S-hostname(config)# class-map HTTP_TRAFFIC P4S-hostname(config-cmap)# match port tcp eq 80 P4S-
hostname(config)# class-map HTTP_PROXY_TRAFFIC_8080 P4S-hostname(config-cmap)# match port tcp eq 8080
P4S-hostname(config)# policy-map OUTSIDE_POLICY P4S-hostname(config-pmap)# class inspection_default P4S-
hostname(config-pmap-c)# inspect http HTTP_TRAFFIC P4S-hostname(config-pmap-c)# inspect http
HTTP_PROXY_TRAFFIC_8080 P4S-hostname(config-pmap)# class HTTP_TRAFFIC P4S-hostname(config-pmap-c)#
set connection timeout tcp 0:10:0 P4S-hostname(config-pmap)# class HTTP_PROXY_TRAFFIC P4S-hostname(config-
pmap-c)# set connection timeout tcp 0:10:0
```

- A. policy-map OUTSIDE\_POLICY interface outside
- B. service-policy OUTSIDE\_POLICY interface outside
- C. policy-map OUTSIDE\_POLICY global
- D. service-policy OUTSIDE\_POLICY global

**Answer: B, D**

**Question:12**

In order to add a port for DNS inspection, which command will be used?

- A. class-map, match, policy-map, class, inspect
- B. class-map, fixup, policy-map
- C. class-map, match, fixup, policy-map, inspect
- D. fixup

**Answer: A**

**Question:13**

You work as a security appliance administrator. You have defined a regular expression to match an unauthorized website. Which pair of commands would be used to configure a regular expression class map?

- A. class-map regex match-any URL match  
UNAUTHORIZED\_SITE
- B. class-map type regex match-any URL match regex  
UNAUTHORIZED\_SITE
- C. class-map type regex match-any match regex  
UNAUTHORIZED\_SITE
- D. class-map match-any type regex match  
UNAUTHORIZED\_SITE

**Answer: B**

**Question: 14**

What is one purpose of a tunnel group?

- A. to group similar IPSec protocols
- B. to group similar IPSec users
- C. to group similar IPSec networks
- D. to identify AAA servers

**Answer: D**

**Question: 15**

What would the adaptive security appliance do when it is configured as displayed?

```
regex NEWCLIENT1 NewP2P1 regex NEWCLIENT2 NewP2P2 class-map type regex match-any NEW_P2P match regex NEWCLIENT1 match regex NEWCLIENT2 class-map type inspect http match-all BLOCK_NEW_P2P match request header user-agent regex class NEW_P2P match request method post policy-map type inspect http MY_HTTP_MAP parameters class BLOCK_NEW_P2P drop-connection policy-map WEB_POLICY class inspection_default inspect http MY_HTTP_MAP service-policy WEB_POLICY interface inside
```

- A. drop any HTTP connection request that either contains the NewP2P1 and the NewP2P2 strings, or uses the POST request method
- B. drop any HTTP connection request that contains the NewP2P1 and NewP2P2 strings and also uses the POST request method
- C. drop any HTTP connection request that contains either the NewP2P1 or the NewP2P2 string, or that uses the POST request method
- D. drop any HTTP connection request that contains either the NewP2P1 or the NewP2P2 string, and also uses the POST request method

**Answer: D**

**Question: 16**

Tom works as a network administrator for P4S Ltd. He receives a new Cisco ASA. Which command, when entered from the console, directs the Cisco ASA to provide interactive prompts that aid in the building of a first-use, minimal configuration?

- A. setup
- B. configure factory default
- C. configure terminal
- D. configure startup

**Answer: A**

**Question: 17**

For the following regular expressions, which one would best match the website address

"www.cisco.com/go/ccsp"?

- A. "www+cisco+com\go\ccsp"
- B. "www.cisco.com/go/ccsp \r"
- C. (w){3,}.cisco.com\go\c){2}sp
- D. (w){3}\.cisco\.com\go\c){2}sp

**Answer: D**

For complete [Exam 642-524 Training kits and Self-Paced Study Material](http://www.certsking.com/642-524)

Visit:

<http://www.certsking.com/642-524.html>

