ISLEVER

642-521

Cisco Secure PIX Firewall Advanced

DEMO

QUESTION NO: 1

An administrator wants to add a comment about access-list aclin line 2. What command should they enter to accomplish this addition?

```
pix1(config)# show access-list
access-list aclin line 1 permit tcp any host
    192.168.0.8 eq www (hitcnt=0)
access-list aclin line 2 permit tcp any host      Insert
    192.168.0.11 eq www (hitcnt=0)                ActualTests
```

A. pix1(config)# access-list aclin line 1
comment partner server http access
B. pix1(config)# access-list aclin line 2
comment partner server http access
C. pix1(config)# access-list aclin line 2
remark partner server http access
D. pix1(config)# access-list aclin line 1
remark partner server http access

Answer: C

QUESTION NO: 2

What is the default polling period that the PIX Firewall uses to check for updates on the AUS?

A. 1440 seconds
B. 720 minutes
C. 1440 minutes
D. 2880 minutes

Answer: B

QUESTION NO: 3

The administrator would like to create an inactivity timeout value of 10 minutes on all console cable sessions. To do so, the administrator would enter which command?

A. Pix1 (config) # authentication console timeout 10
B. Pix1 (config) # enable timeout 10
C. Pix1 (config) # console timeout 10
D. Pix1 (config) # console-idle-timeout timeout10

Answer: C

QUESTION NO: 4

While entering a list of host addresses to an ACL, the administrator left out an ACE for host 192.168.0.9. The administrator wants to add an access control entry for 192.168.0.9 between line 3 and line 4 of the existing access-list. What command should be entered to accomplish this addition?

```
pix1(config)# show access-list
access-list aclin line 2 permit tcp any host
    192.168.0.7 eq www (hitcnt=0)
access-list aclin line 3 permit tcp any host
    192.168.0.8 eq www (hitcnt=0)
access-list aclin line 4 permit tcp any host    Insert
    192.168.0.10 eq www (hitcnt=0)
access-list aclin line 5 permit tcp any host
    192.168.0.11 eq www (hitcnt=0)        ActualTests
```

A. pix1(config)# access-list aclin add-line 4
permit tcp any host 192.168.0.9 eq www
B. pix1(config)# access-list aclin line 4
permit tcp any host 192.168.0.9 eq www
C. pix1(config)# access-list aclin line 3
permit tcp any host 192.168.0.9 eq www
D. pix1(config)# access-list aclin add-line 3
permit tcp any host 192.168.0.9 eq www

Answer: B

QUESTION NO: 5

Which must you do to enable hosts behind the PIX Firewall to receive multicast transmissions? Choose two.

A. Use theigmp join-group command to configure the PIX Firewall to join a multicast group.
B. Use the multicast interface command to enable multicast forwarding on each interface and place the interfaces in multicast safe mode.
C. Use theigmp forward command to enable IGMP forwarding on each PIX Firewall interface connected to hosts that will receive multicast transmissions.
D. Use the multicast interface command to enable multicast forwarding on each interface and place the interfaces in multicast promiscuous mode.

E. Use the permit option of the access-list command to configure an ACL that allows traffic to permissible Class D destination addresses.

Answer: C,D

QUESTION NO: 6

Which statement about license keys for PIX Firewalls is true?

A. License keys are specific to the PIX Firewall software versions.
B. License keys are not required for any of the PIX Firewall software versions.
C. License keys exist for the PIX Firewall 515E software version only.
D. License keys are not specific to a particular PIX Firewall software version.

Answer: D

QUESTION NO: 7

You have 100 users on your internal network; you want only six of these users to perform FTP, Telnet, or HTTP outside the network. Which PIX Firewall feature do you enable?

A. object grouping
B. AAA
C. access lists
D. VAC+

Answer: B

QUESTION NO: 8

Which statements about authenticating to the PIX Firewall are true? Choose two.

A. If you are authenticating for FTP and the username or password on the authentication database differs from the username or password on the remote host to which you are accessing via FTP, you need to enter the username and password in the following formats:aaa_username@remote_usernameaaa_password@remote_password
B. Although FTP is a widely-used service, there is no way to authenticate.
C. You cannot authenticate with HTTP.
D. You can authenticate with Telnet with which you have up to four chances to log in.
E. If you are authenticating for HTTP and enter an incorrect password, the connection is dropped immediately.