KillTest

높은 품질, 더 나은 서비스



연습 문제

https://www.killtest.kr

1년간 무료 업데이트 제공

Exam : **642-521**

Title : Cisco Secure PIX Firewall Advanced

Version : DEMO

1. Your primary PIX Firewall is currently the active unit in your failover topology. What will happen to the current IP addresses on the primary PIX Firewall if it fails?

A. They become those of the standby PIX Firewall.

B. The ones on the primary PIX Firewall remain the same, but the current IP addresses of the secondary become the virtual IP addresses you configured.

C. They are deleted.

D. The ones on both the primary and secondary PIX Firewalls are deleted and both assume the failover IP addresses you configured.

Answer: A

2. What is the default port number that the PIX Firewall uses to contact the AUS?

A. 25

B. 110

C. 443

D. 444

Answer: C

3. Which statements about the PIX Firewall's DHCP capabilities are true? Choose two.

A. It can be a DHCP server.

B. It cannot be a DHCP client.

C. You must remove a configured domain name.

D. It can be a DHCP server and client simultaneously.

E. It cannot pass configuration parameters it receives from another DHCP server to its own DHCP clients.

F. The PIX Firewall's DHCP server can be configured to distribute the IP addresses of up to four DNS servers to its clients.

Answer: AD

4. You already created an ACL named ACLIN to permit traffic from certain Internet hosts to the web server on your DMZ. How do you make the ACL work? Choose two.

A. bind the ACL to the DMZ interface

B. bind the ACL to the inside interface

C. bind the ACL to the outside interface

D. create a static mapping for the DMZ interface

E. create a static mapping for the web server

F. create a conduit mapping for the web server

Answer: CE

5. If the FTP protocol fixup is not enabled for a given port, which statements are true? Choose two.

A. Outbound standard FTP will work properly on that port.

B. Outbound passive FTP will not work properly on that port.

C. Outbound standard FTP will not work properly on that port.

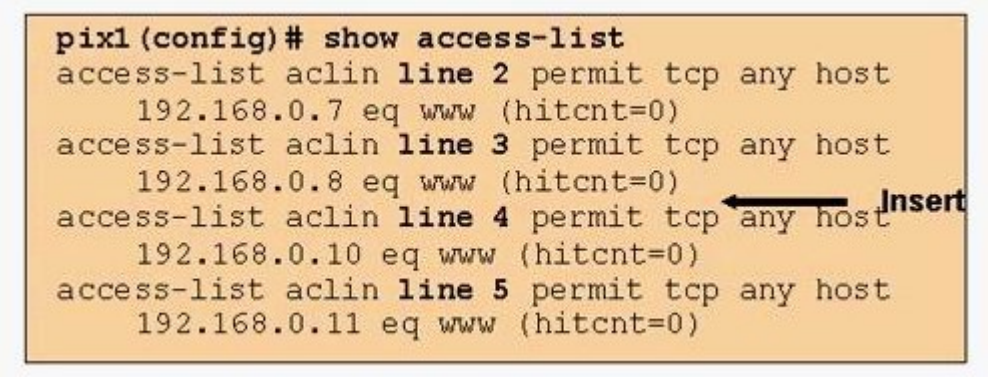
D. Outbound standard FTP will work properly on that port if outbound traffic is not explicitly disallowed.

E. Inbound standard FTP will not work properly on that port even if a conduit to the inside server exists.

F. Outbound passive FTP will work properly on that port as long as outbound traffic is not explicitly disallowed.

Answer: CF

6. 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?



A. pix1(config)# access-list aclin line 4

permit tcp any host 192.168.0.9 eq www

B. pix1(config)# access-list aclin line 3

permit tcp any host 192.168.0.9 eq www

C. pix1(config)# access-list aclin add-line 4

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: A

7. If you configure a VPN between a Cisco VPN Client and the PIX Firewall using pre-shared keys for authentication, which should you do? Choose two.

A. Use pre-shared keys for authentication.

B. Use digital certificates for authentication instead of pre-shared keys.

C. Do not use digital certificates for authentication.

D. Ensure that the password on the VPN client matches the vpngroup password on the PIX Firewall.

E. Ensure that the group name differs from the VPN group name on the PIX Firewall.

F. Ensure that the group name on the VPN Client matches the vpngroup name on the PIX Firewall.

Answer: DF

8. What is the function of the support tool in the PIX MC?

A. to allow technical support to remotely administer the PIX MC

B. to show available support options for the PIX MC

C. to create a file that captures information about the PIX MC

D. to place the PIX MC in safe mode so you can troubleshoot it

Answer: C

9. Which command enables IKE on the outside interface?

A. ike enable outside

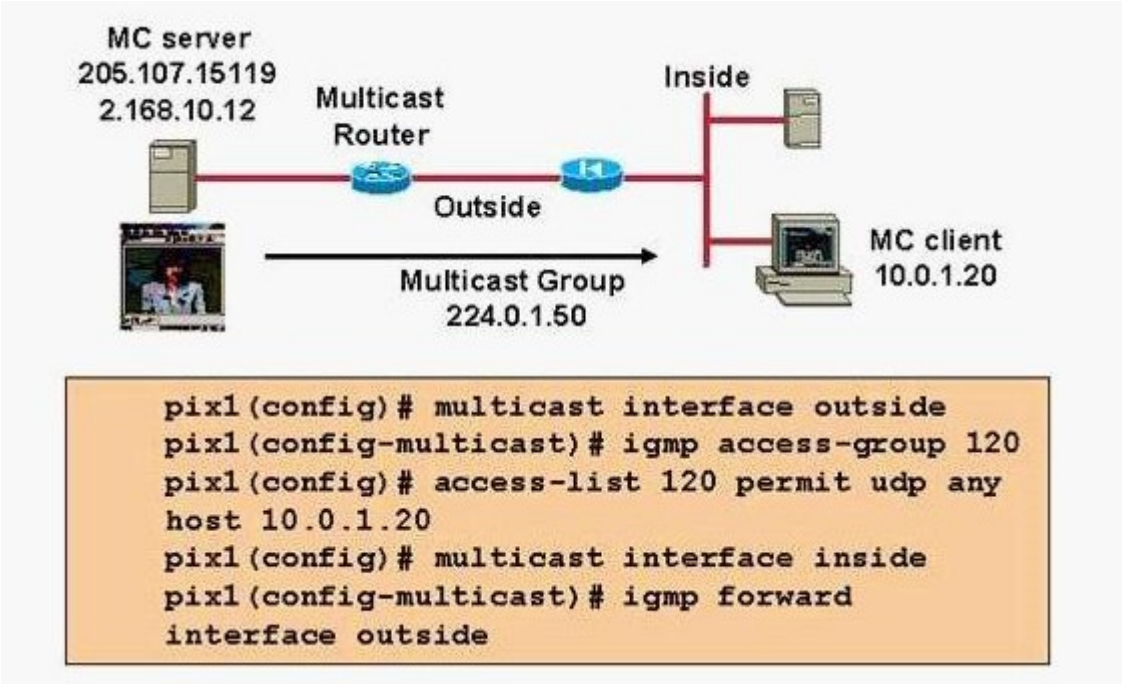
B. ipsec enable outside

C. isakmp enable outside

D. ike enable (outbound)

Answer: C

10. A company just completed the rollout of IP/TV. The first inside network MC client to use the new feature claims they can not access the service. After viewing the above PIX Firewall configuration and network diagram again, the administrator was able to determine the following:



A. The PIX multicast configuration is correct, the configuration problem exists in the MC client's PC.

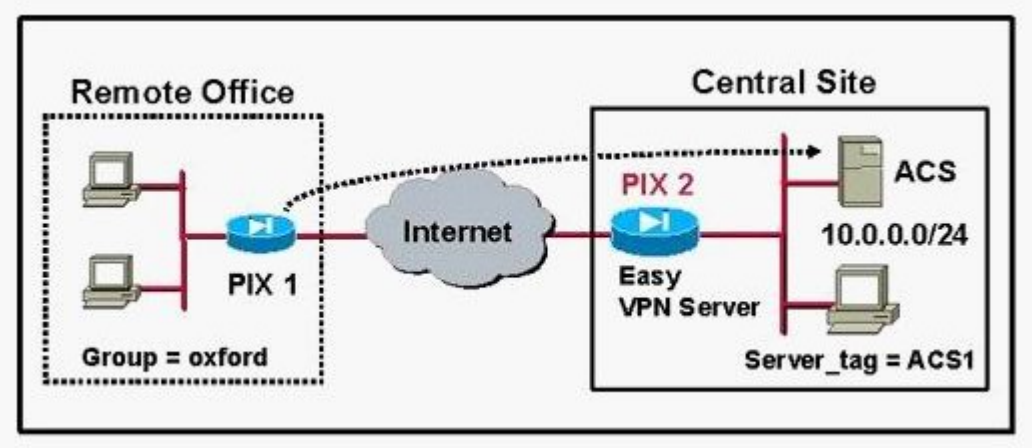
B. The igmp forward command was not correct, it should be changed to the following: pix1(config-multicast)# igmp forward interface inside

C. The igmp access-group command was not correct, it should be changed to the following: pix1(config-multicast)# igmp object-group 120.

D. The access-list command was not correct, it should be changed to the following: pix1(config)# access-list 120 permit udp any host 224.0.1.50

Answer: D

11. For added security, the network manager wants PCs on the inside network at the remote office to authenticate with an ACS server, ACS1, at the central site before allowing these individuals PCs to access a VPN tunnel. As the network administrator, at which location and what commands should they enter to force remote PC users to authenticate before allowing them access to a VPN tunnel? (Choose two.)



A. vpngroup oxford user-authenticationvpngroup oxford authentication-server ACS1

B. Configured at PIX1

C. Configured at PIX2

D. vpngroup oxford individual-user-authentication ACS1

E. vpngroup oxford mode network-extension-modevpngroup oxford authentication-server ACS1

Answer: AC

12. Which statement about the PIX Firewall and virtual HTTP is true?

A. The PIX Firewall enables web browsers to work correctly with its HTTP authentication. The PIX Firewall redirects the web browser's initial connection to an IP address which resides within the PIX Firewall, authenticates the user, and then redirects the browser back to the URL the user originally requested.

B. The PIX Firewall supports virtual Telnet, but not virtual HTTP.

C. The PIX Firewall enables RADIUS authorization by redirecting the web browser's initial connection to an IP address which resides on a web server you specify, authorizing the user, and then redirecting the browser back to the URL the user originally requested.

D. The PIX Firewall enables you to access URLs from its console.

Answer: A

13. What does the PIX Firewall license determine? Choose three.

A. its ability to provide cut-through proxy services

B. whether it can be managed by PDM

C. number of interfaces supported by the platform

D. amount fo RAM supported by the platform

E. the software image that can be installed

F. failover support

Answer: CDF

14. You have installed a FWSM in your Catalyst 6500 switch, initialized it in the switch, configured switch VLANs, and configured the module interfaces; however, you are unable to establish outbound connections. You check your configuration and find that you have correctly configured the six basic commands (nameif, interface, ip address, nat, global, and route). What could be the cause of the problem?

A. You have not configured a switch VLAN for the inside interface.

B. You need an ACL for the outside interface.

C. The MSFC is configured as a connected router only on the outside interface.

D. You need an ACL for the inside interface.

Answer: D

15. 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

16. 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) # enable timeout 10

B. Pix1 (config) # console timeout 10

C. Pix1 (config) # authentication console timeout 10

D. Pix1 (config) # console-idle-timeout timeout10

Answer: B

17. Which statement about Telnet and the PIX Firewall is true?

A. You can enable Telnet on all interfaces except the outside interface.

B. You can enable Telnet on all interfaces, but the PIX Firewall requires that all Telnet traffic to all interfaces be IPSec protected.

C. You can enable Telnet on all interfaces, but the PIX Firewall requires that all Telnet traffic to the outside interface be IPSec protected.

D. Telnet connections to the PIX Firewall are not permitted.

Answer: C

18. How can downloadable ACLs increase your efficiency when you find yourself creating massive amounts of ACLs on several different PIX Firewalls?

A. They enable you to configure your PIX Firewall to download pre-written ACLs from Cisco Connection Online.

B. You can enter an ACL once, in Cisco Secure ACS, and then have it downloaded to any number of PIX Firewalls during user authentication.

C. You can create all ACLs on one PIX Firewall and distribute them to other PIX Firewalls by using the download command on the receiving PIX Firewall or the upload command on the sending PIX Firewall.

D. You can enter an ACL once in Cisco Secure ACS, and then have it downloaded to no more than 100 PIX Firewalls during authorization.

Answer: B

19. What is the difference between inside and outside NAT?

A. Inside NAT's main purpose is to control the IP addresses that appear on inner networks, while outside NAT's main purpose is to hide IP addresses of hosts on outer networks.

B. Outside NAT translates addresses of hosts residing on the less secure interfaces of the PIX Firewall while inside NAT translates addresses of hosts residing on the more secure interfaces.

C. Outside NAT translates addresses of hosts residing on the more secure interfaces of the PIX Firewall while inside NAT translates addresses of hosts residing on the less secure interfaces.

D. Outside NAT translates addresses of hosts residing on the more secure interfaces of the PIX Firewall to addresses on the least secure interface. Inside NAT translates addresses of hosts residing on the more secure interfaces of the PIX Firewall to addresses on any more secure interface except the actual most secure interface.

Answer: B

20. What is the purpose of the command ip local pool MYPOOL 10.0.0.20-10.0.0.29?

A. to designate a pool of IP addresses for NAT

B. to designate a pool of IP addresses that will dynamically be assigned to PPPoE clients

C. to designate a pool of IP addresses that will be dynamically assigned to DHCP clients

D. to designate a pool of IP addresses that will be dynamically assigned to VPN clients via IKE mode configuration

Answer: D