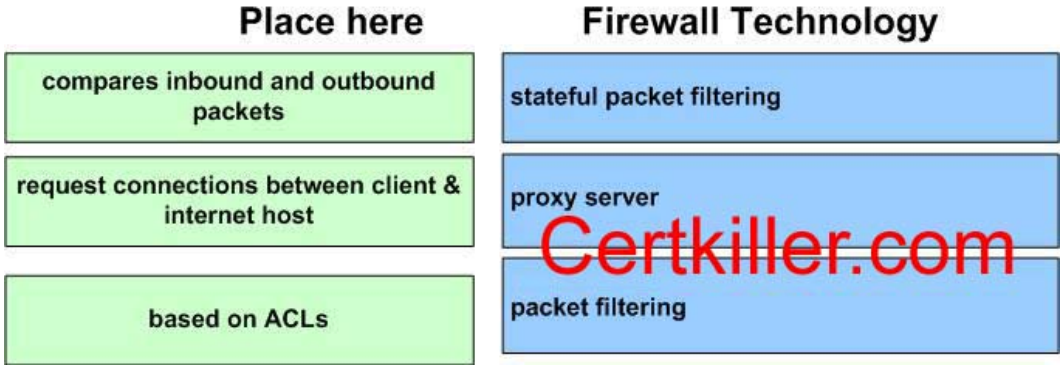
Exam : 642-521

Title : Cisco Secure PIX Firewall Exam (CSPFA)□□

Ver : 11.14.05

QUESTION 1
You are the security administrator at Certkiller Inc. and your assignment is to match the firewall technology with its description.

Answer:



Explanation:
Proxy server - hides valuable data by requiring users to communicate with secure system by means of a proxy. Users gain access to the network by going through a process that establishes session state, user authentication, and authorized policy.
Packet filters - A Cisco router configured with an ACL to filter traffic flowing through it is an example of a packet filter.
Stateful Packet filters - A stateful packet filter keeps complete session state information for each session built through the firewall. Each time an IP connection is established for an inbound or outbound connection, the information is logged in a stateful session flow table.
Reference: Cisco Secure PIX Firewall (Ciscopress) pages 16 - 18

QUESTION 2
Which of the following is a problem with packet-filtering firewalls?

A. It is simple to add new services to the firewall, and services can be easily exploited.
B. Packets are permitted to pass through the filter by being fragmented.
C. It is problematic to add new services to the firewall.
D. Packets are unable to pass through the filter by being fragmented.

Answer: B

Explanation:
Packet filtering

A firewall can use packet filtering to limit information entering a network or information moving from one segment of a network to another. Packet filtering uses access control lists (ACLs), which allow a firewall to accept or deny access based on packet types and other variables.
This method is effective when a protected network receives a packet from an unprotected network. Any packet that is sent to the protected network and does not fit the criteria defined by the ACLs is dropped.
However, there are problems with packet filtering:
1. Arbitrary but undesirable packets can be sent that fit the ACL criteria and, therefore, pass through the filter.
2. Packets can pass through the filter by being fragmented.
3. Complex ACLs are difficult to implement and maintain correctly.
4. Some services cannot be filtered.
PIX FW Advanced, Cisco Press, p. 18
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.3-5

QUESTION 3
At which of the following stages will the PIX Firewall log information about packets, such as source and destination IP addresses, in the stateful session table?

A. Each time it is reloaded.
B. Each time a TCP or UDP outbound connection attempt is made.
C. Each time a TCP or UDP inbound or outbound connection attempt is made.
D. Only when a TCP inbound or outbound connection attempts is made.
E. Never.

Answer: C

Explanation:
Stateful packet filterin is the method used by the Cisco PIX Firewall. This technology maintains complete session state. Each time a Transimission Control Protocol (TCP) or User Datagram Protocol (UDP) connection is established for inbound or outbound connections, the information is logged in a stateful session flow table.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.3-7
PIX FW Advanced, Cisco Press, p. 19

QUESTION 4
John the security administrator at Certkiller Inc. is working on configuring the PIX Firewall. John must choose two features on the PIX Firewall? (Choose two)

A. One feature is it uses Cisco Finesse operating system.
B. One feature is it uses Cisco IOS operating system.
C. One feature is it's based on Windows NT technology.
D. One feature is it snalyzes every packet at the application layer of the OSI model.
E. One feature is it can be configured to provide full routing functionality.
F. One feature is it uses a cut-through proxy to provide user-based authentication

connections.

Answer: A, F

Explanation:
The PIX Firewall features the following technologies and benefits
Non-Unix, secure, real-time, embedded system
ASA
Cut-through proxy - A user-based authentication method of both inbound and outbound connections, providing improved performance in comparison to that of a proxy server.
Statefull packet filtering
Finesse, a Cisco proprietary operating system, is a non-unix, non-windows nt, IOS-like operating system. Use of Finesse eliminates the risks associated with general-purpose operating system.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 3 pages 8-9

QUESTION 5
What is the operating system that a pix runs?

A. unix
B. solaris
C. windows
D. none of the above

Answer: D

Explanation:
The pix firewall runs code written by Cisco specifically to function as a hardened firewall, limiting its vulnerabilities.

QUESTION 6
What encryption protocols does the pix firewall support for vpn's? Choose all that apply.

A. MD5
B. 3DES
C. AES
D. DES

Answer: B,C,D

Explanation:
The pix firewall supports 56 bit DES, 168 bit 3DES, and 128, 192, and 256 bit AES encryption protocols for IPSEC VPN's.

QUESTION 7
What is the maximum number of interfaces the PIX Firewall 535 supports with an unrestricted license?

A. PIX Firewall 535 supports 20
B. PIX Firewall 535 supports 10
C. PIX Firewall 535 supports 6
D. PIX Firewall 535 supports 5

Answer: B

Explanation: A total of eight interface circuit boards are configurable with the restricted license and a total of ten are configurable with the unrestricted license.
- The Cisco PIX 535 Security Appliance support up to 10 Physical Ethernet interfaces.
- With version 6.3 the PIX supports a total of 24 combined physical and virtual interfaces.
- A total of 8 interfaces are configurable on the PIX 535 with the restricted license, and a total of 10 are configurable with the unrestricted license.
PIX model license Comparison

Model	515E	525	535
Restricted			
Maximum Physical	3	6	8
Maximum VLAN	3	4	6
Maximum	5	6	8
RAM	32	128	512
Unrestricted			
Maximum Physical	6	8	10
Maximum VLAN	8	10	22
Maximum	10	12	24
RAM	64	256	1,000

Reference:
http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2030/products_installation_guide_chapter09186a0

QUESTION 8
As of PIX Firewall release 6.3, Advanced Encryption Standard (AES) is supported on a PIX Firewall.
Which of the following statements regarding the capabilities of AES on the PIX Firewall is valid?

A. Supported in software only on all models.
B. Supported on software on all models and in hardware in a VAC card.
C. Not supported by the PIX 501 and 506.
D. Supported in software on all models and in hardware on a VAC+ card.
E. Supported in software on all models and in hardware on an AIM II card.
F. None of the above.

Answer: D

Explanation:
PIX FW Advanced, Cisco Press, p. 29

QUESTION 9
Which of the following are valid pix models? Choose all that apply.

A. 505
B. 515
C. 530
D. 535

Answer: B,D

Explanation:
The pix firewall comes in 6 different models. 501, 506, 515, 520, 525, 535. There is also the FWSM blade.

QUESTION 10
How much flash memory does a pix firewall need to run OS version 6.1?

A. 2mb
B. 4mb
C. 8mb
D. 16mb

Answer: C

Explanation:
You need at least 8mb of flash memory to run pix OS version 5.2 and later.

QUESTION 11
What is the maximum number of interfaces the pix 535 can support?

A. 6
B. 8
C. 9
D. 10

Answer: D

Explanation:
The 535 can support up to 10 different interfaces. The 525 can support 8 and the 515 and 520 can support up to 6.

QUESTION 12
Which of the following pix models are unable to provide failover? Choose all that apply.

A. 501
B. 506
C. 515
D. 520

Answer: A,B

Explanation:
All pix models including the FWSM can provide failover, except for the 501 and 506.

QUESTION 13
Which of the following is a hardware card that can be installed on a pix to increase vpn throughput?

A. pfs
B. ike
C. stp
D. vac

Answer: D

Explanation:
Pix firewall models 515, 525, and 535 support VPN Accelerator Cards (VAC's) that process encryption and decryption in hardware, relieving the pix cpu.

QUESTION 14
How many available PCI slots does a pix 515 have?

A. 0
B. 1
C. 2
D. 3
E. 4
F. 6

Answer: C

Explanation:
The pix 515 has two available pci slots for additional ethernet interfaces to be installed.

QUESTION 15
How much flash memory does a pix 525 come standard with?

A. 8mb
B. 16mb
C. 32mb
D. 64mb

Answer: B

Explanation:
The 515, 520, 525, and 535 all come standard with 16mb of flash.

QUESTION 16
What is the maximum amount of RAM the pix 535 supports?

A. 128mb
B. 512mb
C. 1gb
D. 2gb
E. 4gb

Answer: C

Explanation:
The pix 535 firewall can support up to 1024mb (1gb) of RAM memory.

QUESTION 17
Which of the following ports are not on a pix? Choose all that apply.

A. RJ-45
B. USB
C. Firewire
D. DB-15

Answer: C

Explanation:
No pix firewall has a firewire port, but they do have RJ-45 (ethernet), DB-15 (failover), and USB (reserved for future use) ports.

QUESTION 18
How many concurrent vpn peers can the pix 525 support?

A. 250
B. 750
C. 2000
D. 5500

Answer: C

Explanation:
The pix 535, 525, 520, and 515 support up to 2000 concurrent vpn peers.

QUESTION 19
John the security administrator at Certkiller Inc. is working with FWSM. Which statement about installing the FWSM in a Catalyst 6500 switch is true?

A. The true statement is it must be installed in slot 1.
B. The true statement is it must be installed in slot 5.
C. The true statement is it cannot be installed in slot 1 because slot 1 is reserved for the Supervisor Module.
D. The true statement is it is best to avoid installing it in slots 1, 2, 3 or 4 because they are used for Supervisor and Switch Fabric Modules.

Answer: C

Explanation:
The following is an example of the output of the show module command
Router#show module
Mod slot ports module type model sub status
1 1 2 1000basex supervisor ws-x6k-s2u-msfc2 yes ok
15 1 1 multilayer switch feature ws-f6k-msfc2 no ok
2 2 6 firewall service module ws-svc-fwm-1 no ok
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap19 page 14

QUESTION 20
Which of the following supports FWSM installation? Choose all that apply.

A. 1720 router
B. 5500 access server
C. 6500 switch
D. 7600 router

Answer: C,D

Explanation:
The pix os FWSM blade can be installed on 6500 series switches and 7600 series routers.

QUESTION 21
What is the maximum number of interfaces the PIX Firewall 535 supports with an unrestricted license?

A. 5

B. 6
C. 10
D. 20

Answer: C
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.13-7

QUESTION 22
Which of the following statements regarding license keys for PIX Firewalls is valid?

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

Answer: B
An activation key is "tied" to a specific PIX Firewall, such as PIX Firewall-serial number 12345678. An activation key is not specific to a particular PIX Firewall software version.
Reference: CSPFA Student Guide v3.2 -Cisco Secure PIX Advanced Page 4-30

QUESTION 23
How many interfaces can be configured on a pix 515 with a restricted license?

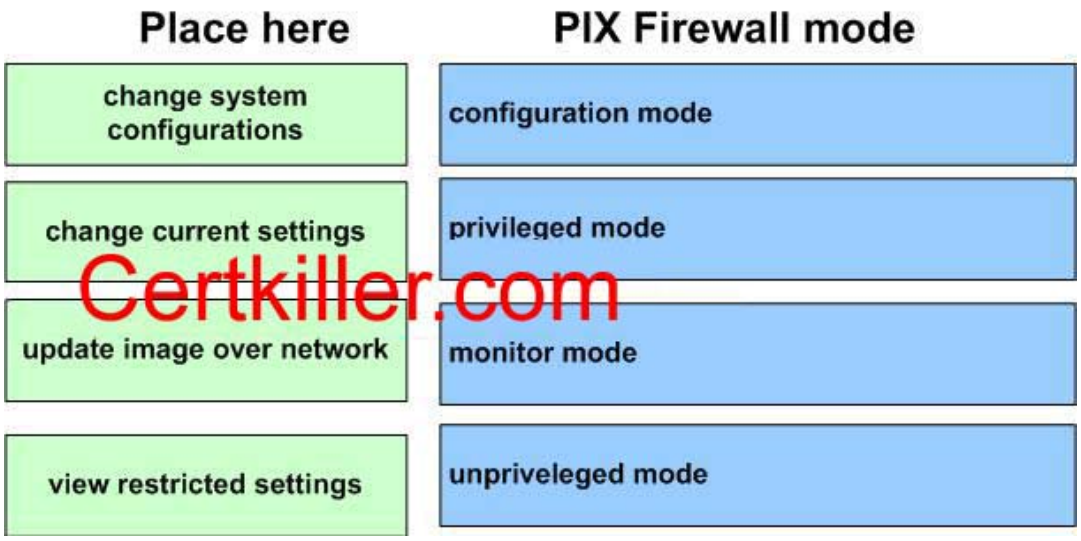
A. 2
B. 3
C. 4
D. 6

Answer: B

Explanation:
The pix 515 restricted license supports up to 3 interfaces. If you need to enable more you must upgrade to the unrestricted license.

QUESTION 24
Jason the security administrator at Certkiller Inc. has the assignment to match the PIX Firewall mode with its description.

Answer:



Explanation:
* Unprivileged mode displays the ">" prompt and lets you view current running settings.
* Privileged mode displays the "#" prompt and lets you change current settings and write to flash memory. Any unprivileged command also works in privileged mode.
* Configuration mode displays the "(config)#" prompt and lets you change system configurations. Only configuration mode commands work in this mode.
* Monitor mode permits you to perform special tasks that could otherwise not be performed. One of those tasks is updating an image over the network.
Reference: Cisco Secure PIX Firewall (Ciscopress) page 32

QUESTION 25
Which of the following pix commands is used to set the name of an interface?

A. interface
B. nameif
C. global
D. ip address
E. conduit

Answer: B

Explanation:
The nameif command sets the name of the interface (nameif ethernet3 webserver security40).

QUESTION 26
What priority does ethernet1 have by default on a pix?

A. 0
B. 50
C. 100
D. no default

Answer: C

Explanation:
Ethernet 1 is the Inside security interface on a pix and by default it has a security value of 100.

QUESTION 27
Which of the following is the correct way to enable a pix interface?

A. interface inside enable
B. interface ethernet1 enable
C. interface ethernet1 100basetx
D. interface ethernet1 no shut

Answer: C

Explanation:
To enable an interface, set the interface speed for the hardware ID: Interface (interface ID) (speed). Disable the interface with the shutdown argument: Interface (interface ID) (speed) shutdown.

QUESTION 28
How can you find the os version number running on your pix? Choose all that apply.

A. show system
B. show memory
C. show version
D. write terminal
E. write memory

Answer: C,D

Explanation:
Use the show version, write terminal, or show running-configuration commands to see the pix os currently running.

QUESTION 29
Which of the following commands shows the translation table entries on a pix?

A. show conn
B. show trans
C. show xlate
D. show tslot

Answer: C

Explanation:
Use the show xlate command to see all ip address translations currently on the pix.

QUESTION 30
How do you show the running configuration of your pix? Choose all that apply.

A. write start
B. write memory
C. write config
D. write terminal
E. show running-configuration

Answer: D,E

Explanation:
To display the current running configuration on your pix, use the show running-configuration command or the write terminal command.

QUESTION 31
How can you view the files listed in pix flash memory?

A. show pix flash
B. show flash memory
C. show flashfs
D. show flash mfs

Answer: C

Explanation:
The pix show flashfs command will display all of the files listed in flash memory such as the pix os image, PDM, etc.

QUESTION 32
What is the core of the pix firewall?

A. PFS
B. ASA
C. VAC
D. FWSM

Answer: B

Explanation:
The Adaptive Security Algorithm (ASA) is the brains of the pix, keeping track of stateful connection information.

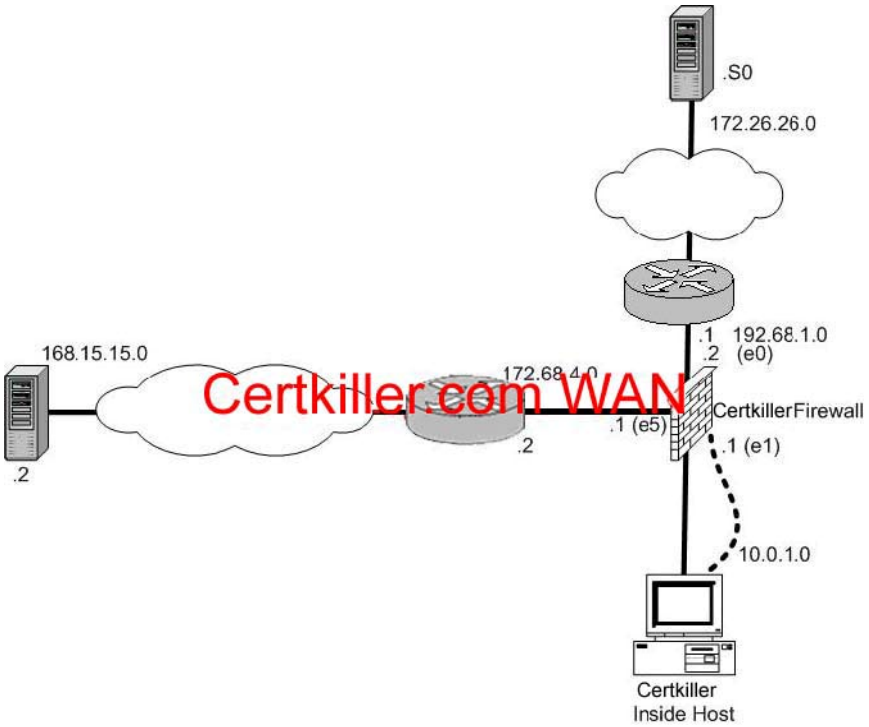
QUESTION 33
Up to how many connections can the ASA of the pix 535 track?

A. 100,000
B. 500,000
C. 1,000,000
D. 2,000,000

Answer: B

Explanation:
The pix 535 ASA can track up to 500,000 different connections in the connection table.

QUESTION 34
You are the network security administrator for Certkiller .com, a law firm. In an effort to evolve into total environmental design, Certkiller has recently acquired Acme International. Mr King, the CEO of Certkiller , has asked you to add an interface to the PIX Firewall 515E to support a dedicated network for the new employees. Your task is to enable the ethernet5 interface for 100 Mbps full duplex communication and configure it with the following parameters.
The configuration will be as follows:
Name: Certkiller 3
Security level: 40
IP address: 172.68.4.1
Network: 255.255.255.192
1. You will not be able to the Inside PIX Interface from an Interface connected to an inside host.
2. The Firewall is named Certkiller
3. The enable password is Certkiller
Click on picture of the host connected to the PIX Firewall by a serial console cable.



Answer:

Explanation:
Certkiller >enable
Password: Certkiller 123
Certkiller #config t
Certkiller (config)#nameif ethernet5 Certkiller 3 security40
Certkiller (config)#interface ethernet5 100full
Certkiller (config)#ip address Certkiller 3 172.68.4.1 255.255.255.192
Certkiller (config)#exit
Certkiller #write mem
show run(option, if you want see changes you have done)
When you configuring ip address to ethernet5 interface it should valid IP address not network address. So it should 172.68.4.1 255.255.255.192 NOT 172.68.4.0
Also correct command for ethernet5 interface settings is.
interface ethernet5 100full (100full should be one word)
When you saving configuration it should be in privilege mode and with write mem command,
There is no copy run start command to save configuration
Note:
- nameif command lets you assign a name to an interface. You can use this command to assign interface names if you have more than two network interface circuit boards in your PIXFirewall. The first two interfaces have the default names inside and outside. The inside interface has a default security level of 100, the outside interface has a default security level of 0.
- interface command sets the speed and duplex settings of the network interface boards,

and brings up the interfaces specified.
- ip address command lets you assign an IP address to each interface.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/cmdref/qref.htm
Alternative #1:
Name: Certkiller 3
Security level: 22
IP address: 172.20.1.1
Network: 255.255.255.0

QUESTION 35
You are the network administrator for Certkiller Inc. You have been instructed to create an inactivity timeout value of 10 minutes on all console cable sessions. Which of the following command will you use?

A. Certkiller 1 (config) # enable timeout 10
B. Certkiller 1 (config) # authentication console timeout 10
C. Certkiller 1 (config) # console timeout 10
D. Certkiller 1 (config) # console-idle-timeout timeout 10

Answer: C

Explanation:
The console timeout command sets the timeout value for any authenticated, privileged mode, or configuration mode user session when accessing the firewall console through a serial cable. The default value is zero, no timeout. This may present a security risk. By setting the number to a non-zero number, the user is logged out after the specified period of inactivity. This timeout does not alter the Telnet or SSH timeouts; these access methods maintain their own timeout values.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.5-11

QUESTION 36
Which of the following commands sets the security level of an interface?

A. conduit
B. ip address
C. nameif
D. nat
E. global

Answer: C

Explanation:
Use the nameif command to set the interface security level. (0-100)

QUESTION 37
Which of the following sets the dmz2 interface to a security level of 20?

A. interface (dmz2) security 20
B. ip address 192.168.10.10 (dmz2) security 20
C. nameif ethernet3 dmz2 security20
D. global dmz2 security20

Answer: C

Explanation:
Use the nameif command to set the security level of an interface. There is no space entered in the security level (security20 not security 20).

QUESTION 38
What is the command that saves your pix configuration to flash memory?

A. save flash
B. write memory
C. write flash
D. write run
E. write start

Answer: B

Explanation:
The write memory command saves the configuration running in ram to the startup configuration in flash.

QUESTION 39
What is the command to set the clock on a pix?

A. set clock
B. set time
C. clock set
D. time set

Answer: C

Explanation:
The clock set command configures local time on the pix. It is set with the following format: hh:mm:ss mmm dd yyyy (note that mmm is entered as a three letter month such as feb or nov, etc.).

QUESTION 40
How do you configure a pix firewall to use an ntp time server?

A. ntp server 192.168.10.10
B. ip ntp server 192.168.10.10
C. local ntp server 192.168.10.10
D. ntp local server 192.168.10.10

Answer: A

Explanation:
Synchronize your internal pix clock via an NTP timer server with the ntp server (ip address) command.

QUESTION 41
What is the maximum number of syslog messages the pix firewall can store with internal buffers?

A. 20
B. 100
C. 350
D. 600

Answer: B

Explanation:
The internal buffers can only store a maximum of 100 syslog messages. Once the buffers are full, the oldest syslog messages will start to be written over.

QUESTION 42
John the security administrator at Certkiller Inc. is downloading the Cisco IP phones configuration from a TFTP server. How does John enable the PIX Firewall to provide information about a TFTP server to the IP phone?

A. John has to use the tftp server command.
B. John has to enable the PIX Firewall's TFTP fixup.
C. John has to configure the PIX Firewall's TFTP server and enable TFTP option 150 or DHCP option 66.
D. John has to configure the PIX Firewall's DHCP server and enable DHCP option 150 or DHCP option 66.

Answer: D

Explanation:
These options are useful for IP phones, which may need to obtain configuration files from a tftp server. With dhcp option 66 command, the pix firewall distributes the ip address of a single tftp server. With the dhcp option 150 command, it distributes a list of tftp servers.

The tftp-server command lets you specify the IP address of the server that you use to propagate PIXFirewall configuration files to your firewalls.
Reference:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps2120/products_command_reference_chapter09186a
Note:
Commands:
dhcpd option 66 ascii {server_name| server_ip_str}
dhcpd option 150 ip server_ip1[server_ip2]

option 150	Specifies the TFTP server IP address(es) designated for Cisco IP phones in dotted decimal format. DHCP option 150 is site-specific; it gives the IP addresses of a list of TFTP servers.
option 66	Specifies the TFTP server IP address designated for Cisco IP phones and gives the IP address or the hostname of a single TFTP server.

Reference: CSPFA Student Guide v3.2 -Cisco Secure PIX Advanced Page 16-30
The dhcpd option commands enable the PIX Firewall's DHCP server to distribute the IP address of a TFTP server to serve DHCP clients. These options are useful for IP Phones, which
may need to obtain configuration files from a TFTP server. With the dhcpd option 66 command, the PIX Firewall distributes the IP address of a single TFTP server. With the dhcpd
option 150 command, it distributes a list of TFTP servers. You can remove the dhcpd option
commands by using their no forms.
The syntax for the dhcpd option commands is as follows:
dhcpd option 66 ascii {server_name | server_ip_str}
dhcpd option 150 ipserver_ip1 [server_ip2]

QUESTION 43
Which of the following statements regarding PIX Firewall's DHCP capabilities are valid? Choose two.

A. You have to remove a configured domain name.

B. It can be both DHCP server and client simultaneously.
C. It cannot pass configuration parameters it receives from another DHCP server to its own DHCP clients.
D. It can be a DHCP server.
E. It cannot be a DHCP client.
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: B, D

Explanation:
The PIX Firewall can be a DHCP server, a DHCP client, or a DHCP server and client simultaneously. DHCP server and client support enables you to automatically leverage the DNS, WINS, and domain name values obtained by the PIX Firewall DHCP client for use by the hosts served by the PIX Firewall's DHCP server.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.16-33

QUESTION 44
What is the amount of DNS servers that can be specified with the dhcp dns command?

A. With the 50-user license, 128 addresses are supported.
B. Up to two.
C. Up to four.
D. The DHCP address pool is limited to 32 addresses for a PIX Firewall 501 with a 10-user license.

Answer: B

Explanation:
The IP addresses of the DNS servers for the DHCP client. Specifies that DNS A (address) resource records that match the static translation are rewritten. A second server address is optional.

QUESTION 45
Which of the following commands configures the pix to act as a dhcp client on its outside interface?

A. interface outside dhcp
B. ip address outside dhcp
C. ip interface outside dhcp
D. ip route outside dhcp

Answer: B

Explanation:

IP address outside dhcp enables the pix outside interface to receive a dhcp assigned ip address. This is used in soho environments that need to receive a dhcp assigned address on the outside interface from a dsl or cable modem ISP.

QUESTION 46
How do you enable the pix to act as a dhcp server for clients on the inside interface?

A. ip address inside dhcp
B. dhcpd enable inside
C. interface inside dhcpd enable
D. interface inside dhcp server

Answer: B

Explanation:
Enable the dhcp server on the pix inside interface with the dhcpd enable inside command. Only the inside interface can have the dhcp server enabled.

QUESTION 47
Johnthe security administrator at Certkiller Inc. is working on PPPoE
Which statement about the PIX Firewall and PPPoE is true?

A. The true statement is when PPPoE is configured, the user enters his username and password to connect to a PPPoE server and set the MTU size to 1492 bytes.
B. The true statement is the PIX Firewall does not detect PPPoE session termination.
C. The true statement is when configured, the PIX Firewall's PPPoE client automatically connects to a service providers access concentrator without user intervention.
D. The true statement is when PPPoE is configured, you must se the MTU size to the correct value to allow PPPoE to be transmitted in an Ethernet frame.
E. The true statement is to clear and restart a PPPoE session, enter the clear ppp session command.

Answer: C

Explanation: After it is configured, the PIX Firewall's PPPOE client automatically connects to a service provider's AC without user intervention. The MTU size is automatically set to 1492 bytes, the correct value to allow PPPoE to be transmitted in an Ethernet frame.
Reference: Cisco Secure PIX Firewall Advanced 3.1 5-67

QUESTION 48
Jason the security administrator at Certkiller Inc. is working on configuring the PIX Firewall PPPoE client.
Which commands configure the PIX Firewall's PPPoE client?

A. The commands vpngroup and vpnusername

B. The commands vpdn group, vpdn username, and ip address pppoe
C. The commands vpdn group and interface pppoe
D. The commands vpngroup and ip address pppoe

Answer: B

Explanation: Five steps are needed to configure the PIX firewall PPPoE clients. The first four steps require the use of the VPDN command as follows
Step 1 use the vpdn group command to define a vpdn group to be used for pppoe.
Step 4 Use the vpdn username command to create a username and password pair for the PPoE connection.
Step 5 Use the Ip address PPPoE command to enable PPPoE on the Pix firewall. PPPoE client functionality is disabled by default.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 5 pages 69 and 71

QUESTION 49
Which of the following statements regarding PIX Firewall and PPPoE is valid?

A. The PIX Firewall PPPoE serve can operate in environments where URL and content filtering is being performed before transmission to or from the outside interface.
B. The PIX Firewall PPPoE client can operate in environments where URL and content filtering is being performed before transmission to or from the outside interface.
C. The PIX Firewall PPPoE client cannot operate in environments where NAT is being performed on traffic moving through a VPN.
D. The PIX Firewall PPPoE server can operate in environments where application of firewall rules is being performed on traffic before transmission to or from the outside interface.

Answer: B

Explanation:
The PIX Firewall PPPoE client can operate in environments where other PIX Firewall features are being used. For example, the following features function as usual:
1) NAT on traffic to or from the outside interface or over a VPN
2) URL and content filtering before transmission to or from the outside interface
3) Application of firewall rules on traffic before transmission to or from the outside interface or over a VPN.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.13-30
PIX FW Advanced, Cisco Press, p. 129

QUESTION 50
Starting in which pix os version is pppoe supported?

A. 6.0
B. 6.1
C. 6.2

D. 6.3

Answer: C

Explanation:
Pix os version 6.2 supports Point to Point Protocol over Ethernet (PPPoE). This allows an ethernet host to be authenticated using PPP.

QUESTION 51
The security team at Certkiller Inc. is working on the problems with UDP.
What are two of the problems with UDP? (Choose two)

A. The problem with UDP is Spoofing packets is very easy because there is not handshaking or sequencing.
B. The problem with UDP is its method of guaranteeing delivery makes it processor-intensive.
C. The problem with UDP is the congestion management and avoidance it uses makes it rather slow.
D. The problem with UDP is the UDP connection slow is never deleted from the connection table.
E. The problem with UDP is spoofing UDP packets is difficult.
F. The problem with UDP is the initiator of the transaction or the current state usually cannot be determined because there is no state machine.

Answer: A, F

Explanation: UDP characteristics
UDP is an unreliable (connectionless) but efficient transport protocol.
Spoofing UDp packets is very easy (no handshaking or sequencing). As there is no state machine, both the initiator of the transaction and the current state cannot be determined.
UDP has no delivery guarantees.
There is no connection setup and termination(application implements a state machine).
UDP has no congestion management or avoidance.
Reference: Cisco Secure PIX Firewalls (Ciscopress) Page 70

QUESTION 52
What protocol does IKE use? What port number does it use?

A. tcp, 123
B. tcp, 132
C. udp, 500
D. udp, 1651

Answer: C

Explanation:

Internet Key Exchange (IKE) uses the UDP protocol on port number 500 to set up security associations between two hosts trying to establish a VPN.

QUESTION 53
Transmission Control Protocol is considered what?

A. connection-oriented, reliable, layer 3
B. connection-oriented, reliable, layer 4
C. connection-oriented, unreliable, layer 3
D. connection-oriented, unreliable, layer 4
E. connectionless, reliable, layer 3
F. connectionless, reliable, layer 4
G. connectionless, unreliable, layer 3
H. connectionless, unreliable, layer 4

Answer: B

Explanation:
TCP is a layer 4 protocol that connects with a host before and during data transmission, and it is reliable because it can resend segments and packets lost during network transmission.

QUESTION 54
James the team leader for the security team at Certkiller Inc. is working on dynamic NAT. How can dynamic outside NAT simplify router configuration on your internal or perimeter networks?

A. It can simplify because you can configure your routing within the nat command.
B. It can simplify because you can configure your routing within the global command.
C. It can simplify by controlling the addresses that appear on these networks.
D. It can simplify because statics take precedence over nat and global command pairs.

Answer: C

Explanation:
Dynamic outside NAT -Translates host addresses on less secure interfaces to a range or pool of IP address on a more secure interface. This is most useful for controlling the address on a more secure interface. This is most useful for controlling the address that appear on inside of the pix firewall and for connecting networks with overlapping addresses.
Reference: Cisco Secure PIX Firewall Advanced 3.1 6-11
Inside dynamic NAT
Translates between host addresses on more secure interfaces and a range or pool of IP addresses on a less secure interface. This provides a one-to-one mapping between internal and external addresses that allows internal users to share registered IP addresses and hides internal addresses from view on the public Internet.

Reference: Establishing Connectivity
www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/bafwcfg.htm

---

QUESTION 55
You are the administrator at Certkiller Inc. and you want to have IP addresses of hosts on your DMZ and those of hosts on your inside network translated when they make connections to hosts on the outside interface of the PIX Firewall. What is the minimum NAT configuration you can enter?

A. The minimum is 1 NAT statement and 1 global statement.
B. The minimum is 1 NAT statement and 2 global statements.
C. The minimum is 2 NAT statements and 2 global statements.
D. The minimum is 2 NAT statements and 1 global statement.

Answer: D

Explanation:
Pix<config># nat (inside) 1 10.0.0.0 255.255.255.0
Pix<config># nat (dmz) 1 172.16.1.0 255.255.255.0
Pix<config># golbal (outside) 1 192.168.0.1 netmask 255.255.255.255
First nat command statement permits all host on the inside network 10.0.0.0 to start outbound connections using the IP address from Global ID 1.
Second nat command statement permits all host on the DMZ network 172.16.1.0 to start outbound connections using the IP address from Global ID 1.

QUESTION 56
You are the administrator at Certkiller Inc. and you are troubleshooting the PIX Firewall. You need to know what PIX Firewall feature simplifies the integration of two existing networks that use overlapping IP address spaces.

A. NAT 0
B. outside NAT
C. inside NAT
D. expanded NAT

Answer: B

Explanation:
Outside Nat- Translates address of hosts on lower security level (outside) interfaces - dynamic and static. ...(Dynamic nat) is most useful for controlling the addresses that appear on inside interfaces of the PIX firewall and for connecting private networks with overlapping addresses.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 6 page 11

QUESTION 57
Exhibit, Network topology

Exhibit, Router Configuration

```
Certkiller2(config)# ip address (inside) 10.0.0.1 255.255.255.0
Certkiller2(config)# ip address (outside) 192.168.0.2
      255.255.255.0
Certkiller2(config)# route outside 0.0.0.0 0.0.0.0 192.168.0.1
Certkiller2(config)# nat (inside) 1 10.0.0.0 255.255.255.0
Certkiller2(config)# global (outside) 1 192.168.0.9-192.168.0.100
      netmask 255.255.255.0
```

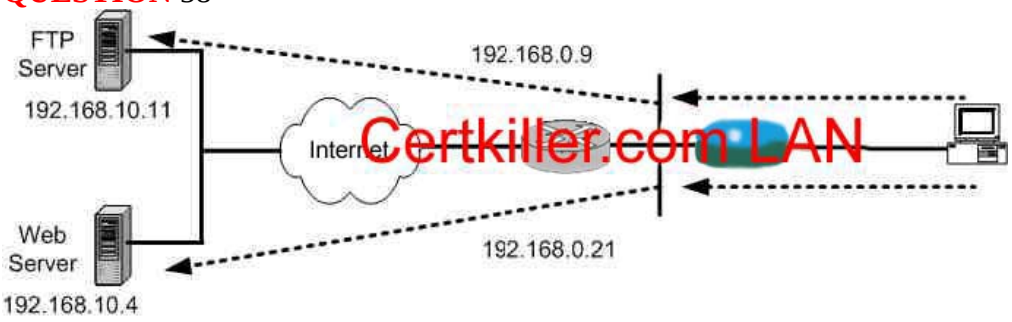
A host on the sales subnet is unable to initiate a web connection to an outside website. When troubleshooting the problem, it was determined that the sales router was not doing address translation and that it was configured correctly. After revealing the network diagram and the partial configuration, the network diagram and the partial configuration, the network administrator determined the following: (Select one)

A. The NAT command is not configured correctly.
B. The administrator needs to add an access-list and static command for the return web traffic.
C. The global command is not configured correctly.
D. The PIX Firewall is configured correctly; a problem exists in the sales PC browser or the destination website.

Answer: A

Explanation:
Since sales router was not doing address translation, sales host on the sales subnet 10.0.1.0 is unable to initiate a web connection to an outside website because NAT command configured in PIX firewall is for subnet 10.0.0.0 255.255.255.0. Since netmask is /24, sale subnet is not included in nat process to access the web server.
Correct Nat command should be
Certkiller 2 (config) # nat (inside) 1 10.0.0.0 255.255.0.0

QUESTION 58



An IT professional at Certkiller asked Certkiller 's PIX Firewall administrator if a user on the inside network could access two sites on the Internet and present two different source IP addresses. When accessing an FTP server, the source IP address is translated to 192.168.0.9. When accessing a web server, the source address is translated to 192.168.0.21. The PIX Firewall administrator could accomplish this application by completing which of the following tasks?

A. Configure NAT and global commands.
B. Configure NAT 0 access-list and global commands.
C. Configure outside NAT and global commands.
D. Configure NAT access-list and global commands.

Answer: D

QUESTION 59
Which of the following VPN protocols cannot be used with NAT?

A. ike
B. esp
C. aes
D. ah

Answer: D

Explanation:
You cannot use Authentication Header (AH) on a VPN network that translates the IP header of the VPN packets. AH uses the IP address as part of the authentication of the packet, so if NAT changes the address, authentication will always fail. Use ESP with SHA-1 or MD5 HMAC's for authentication on an NAT VPN network.

QUESTION 60
What commands need to be enabled to allow a user on a lower security interface initiate a connection to a host on a higher security interface? Choose all that apply.

A. nat
B. static
C. global

D. ip address
E. conduit

Answer: B,E

Explanation:
For the lower security interface user to initiate a connection through the pix to host on a higher security interface, the host would need to be permitted by a conduit statement. For the initiating host to correctly send traffic to the destination host, a static statement needs to be configured so the initiating host has a correct IP address to use.

QUESTION 61
What is the minimum pix os version needed to allow a host on a lower security interface (outside) to have its IP address NAT'ed to a higher security interface (inside)?

A. 5.5
B. 5.8
C. 6.2
D. 6.3

Answer: C

Explanation:
A host on a lower security interface such as the outside interface can be configured to have its IP address translated when initiating a connection to a host on a higher security interface such as the inside interface starting in pix os version 6.2.

QUESTION 62
Which of the following commands allows an administrator to disable IP address translation through a pix?

A. NAT 0
B. Global disable
C. access list
D. static

Answer: A

Explanation:
If you want to disable the ip address translation of a host as it goes through a pix, reference that host in an NAT 0 command. All hosts reference in nat 0 will not have their ip addresses translated and the destination host will see its real ip address.

QUESTION 63
A client on an inside network requests DNS resolution of an inside address from a

DNS server on an outside interface. How can the PIX Firewall be configured to translate the DNS A-record correctly? (Choose three)

A. By making use of the alias command.
B. By making use of the dns arecord command.
C. By specifying the dns option in the alias command.
D. By specifying the dns option in the nat command.
E. By specifying the dns option in the static command.
F. By specifying the dnsarec option in the nat command.

Answer: A, D, E

QUESTION 64
Jason the security administrator at Certkiller Inc. and he is working on the PAT feature. Which statements about the PIX Firewalls PAT feature are true? (Choose three)

A. The true statement is it maps TCP port numbers to a single IP address.
B. The true statement is it cannot be used with NAT.
C. The true statement is it provides security by hiding the outside source address, using a global IP address from the PIX Firewall.
D. The true statement is the IP address of a PIX Firewall interface cannot be used as the PAT address.
E. The true statement is the PAT address can be a virtual address, different from the outside address.
F. The true statement is it provides security by hiding the inside source address, using a single IP address from the PIX Firewall.

Answer: A E F

Explanation:
Pat maps TCP port numbers to a single IP address
Pat provides security by hiding the inside source address by using a single IP address from PIX
PAT can be used with NAT
A Pat address can be a virtual address, different from the outside address. Do not use PAT when running multimedia applications through the PIX firewall. Multimedia applications need access to specific ports and can conflict with port mappings provided by PAT.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 6 page 39

QUESTION 65
How many ip addresses can be translated to a single ip address with PAT?

A. 160
B. 2450
C. 12600

D. 64000

Answer: D

Explanation:
From just a single IP address using PAT, there are approximately 64,000 available ports that can be used to translate IP addresses to.

QUESTION 66
Jason the security administrator for Certkiller Inc. wants to know which command enables the PIX Firewall to permit hosts on different interfaces to ping each other.

A. The icmp command
B. The conduit command
C. The ping command
D. The ip audit command

Answer: A

Explanation: By default, the PIX Firewall denies all inbound traffic through the outside interface. Based on your network security policy, you should consider configuring the PIX Firewall to deny all ICMP traffic at the outside interface, or any other interface you deem necessary, by using the icmp command
The icmp deny command disables pinging to an interface, and the icmp permit command enables pinging to an interface. With pinging disabled, the PIXFirewall cannot be detected on the network. This is also referred to as configurable proxy pinging.
For traffic that is routed through the PIX Firewall only, you can use the access-list or access-group commands to control the ICMP traffic routed through the PIX Firewall.
Reference:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps2120/products_command_reference_chapter09186a

---

QUESTION 67
You are a network administrator at Certkiller .com. You already created an ACL named ACLIN to permit traffic from certain Internet hosts to the web server on Certkiller 's DMZ.
How do you make the ACL work? (Choose two)

A. Bind the ACL to the DMZ interface.
B. Bind the ACL to the outside interface.
C. Bind the ACL to the inside interface.
D. Create a static mapping for the DMZ interface.
E. Create a conduit mapping for the web server.
F. Create a static mapping for the web server.

Answer: B, F

Explanation:
Static address translation creates a permanent, one-to-one mapping between an address on an internal network (a higher security level interface) and a perimeter or external network (lower security level interface). For example, to share a web server on a perimeter interface with users on the public Internet, use static address translation to map the server's actual address to a registered IP address. Static address translation hides the actual address of the server from users on the less secure interface, making casual access by unauthorized users less likely. Unlike NAT or PAT, it requires a dedicated address on the outside network for each host, so it does not save registered IP addresses.
If you use a static command to allow inbound connections to a fixed IP address, use the access-list and access-group commands to create an access list and to bind it to the appropriate interface. For more information, refer to "Allowing Inbound Connections."
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_61/config/mngacl.pdf

---

QUESTION 68
You are the network security administrator at Certkiller for an enterprise network with a complex security policy.
Which PIX Firewall feature should you configure to minimize the average search time for access lists containing a large number of entries?

A. object grouping
B. turbo ACLs
C. nested object groups
D. ASA
E. IP helper
F. comments in ACLs

Answer: B

Explanation:
Turbo ACLs improve the average search time for ACLs containing a large number of entries by causing the PIX firewall to compile tables for ACLs.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 7 page 10

QUESTION 69
What is the rationale behind including a deny statement in an ACL; even though the implicit deny at the end of the ACL will block traffic as needed?

A. You can view the hit counters with the show access-list command.
B. You can enable the turbot ACL feature for individual ACLs.
C. As a back-up, in case the implicit deny does not work.
D. There is no reason to include the deny statement.

Answer: A

Explanation:
When you use the show access-list command you will get a counter for how many hit that specific line got. If you want to see the denied statements you will need to specify them in an access-list.

QUESTION 70
Which of the following statements regarding ACLs are valid? Choose two.

A. By default, all access in an ACL is permitted.
B. Using the access-group command creates ACL entries.
C. For traffic moving form a lower security level interface to a higher security level interface, the destination address argument of the ACL command is the global IP address assigned in the static command.
D. For traffic moving form a lower security level interface to a higher security level interface, the destination host must have a statically mapped address.
E. For traffic moving from a higher security level interface to a lower security level interface, the source address argument of the ACL command is the translated address of the host or network.
F. For traffic moving from a lower security level interface to a higher security level interface, the source address argument of the ACL command is the translated address of the host or network.

Answer: C, F

Explanation:
The access-list command is used to permit or deny traffic. The following are guidelines to use when designing and implementing ACLs:
1) Higher to lower security:
- The ACL is used to restrict outbound traffic.
- The source address argument of the ACL command is the actual address of the host or network.
2) Lower to higher:
- The ACL is used to restrict inbound traffic/
- The destination address argument of the ACL command is the translated global IP address.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.8-6

QUESTION 71
Why are turbo ACLs the most suitable to make use of for high-end PIX Firewall models such as the PIX Firewall 525 and 535?

A. Turbo ACLs are not supported in any of the low-end models, such as the 506.
B. Turbo ACLs are processor-intensive.
C. Turbo ACLs require significant amounts of memory.
D. Although turbo ACLs can improve ACL search time with any PIX Firewall model,

they are complicate and rather difficult to configure. It is unlikely that environments using low-end models have personnel property trained to configure turbo ACLs.

Answer: C

Explanation:
The Turbo ACL feature requires significant amounts of memory and is most appropriate for high-end PIX Firewall models, such as the PIX Firewall 525 or 535. The minimum memory required for Turbo ACL support is 2.1 MB, and approximately 1 MB of memory is required for every 2,000 ACL elements. The actual amount of memory required depends not only on the number of ACL elements but also on the complexity of the entries.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.7-22

QUESTION 72
The newly appointed Certkiller trainee technician wants to know which type of downloadable ACLs are best when there are frequent requests for downloading a large ACL. What will your reply be?

A. Unnamed ACLs
B. Dynamic ACLs
C. Named ACLs
D. Static ACLs

Answer: C

Explanation:
The actual ACL entries can be named or unnamed, depending on whether the ACL will be used by multiple users. A named ACL should be used when frequent request occur for downloading large list. Whit named ACL, after authentication the ACS server sends the ACL name to the firewall to see if the ACL already exists. If not the firewall request the ACL to be downloaded. A named ACL isn't downloaded again as log as it exists on the firewall.

QUESTION 73
Which of the following pix 535 slot ranges support gigabit ethernet interface cards?

A. 0-1
B. 0-2
C. 0-3
D. 5-6
E. 5-7

Answer: C

Explanation:

Gigabit line cards on the pix 535 can only be installed in slots 0-3. Slots 4-8 cannot support gigabit cards because they run at a slower bus speed.

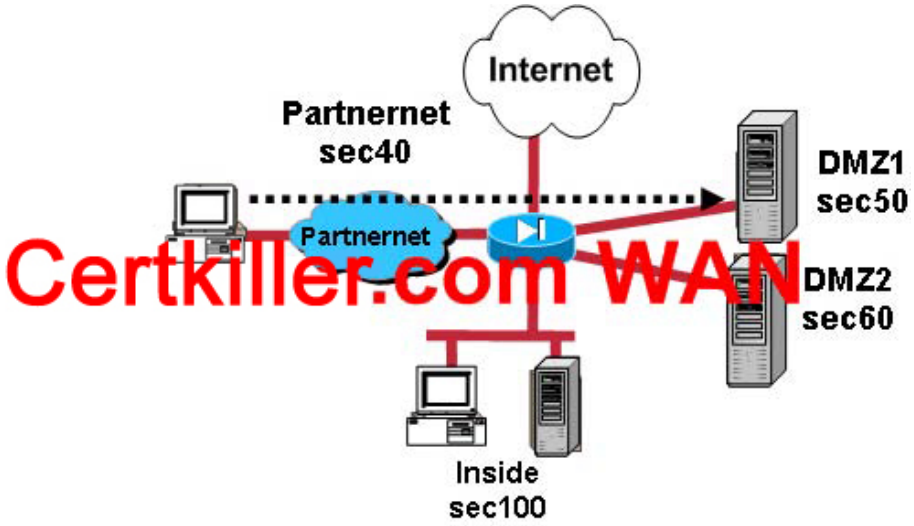
QUESTION 74
How many lines are needed in an access list before TurboACL will compile them?

A. 2
B. 13
C. 16
D. 19

Answer: D

Explanation:
When you enable TurboACL on your pix firewall, only access lists with 19 or more entries can be compiled by TurboACL.

QUESTION 75
Exhibit:



Certkiller.com WAN

In the network above, which two methods will enable a PC on the parinernet to connect to a server on DMZ1 and deny the Parinerent PC access to DMZ2 and the inside network? (Choose two.)

A. Apply a static command and ACL to the partnernet interface.
B. Raise the security level of the partnernet interface to 70.
C. Raise the security level of the partnernet interface to 55.
D. Apply a static command and ACL to the DMZ1 interface.
E. Apply a static command and ACL to the DMZ2 interface.

Answer: A, C

Explanation:

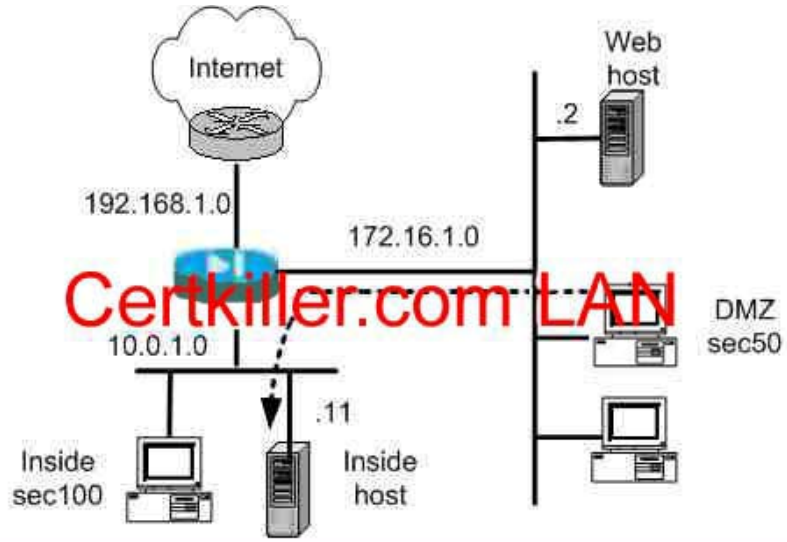
Sec for Partner=40, DMZ 1=50 and DMZ2= 60
By default, the PIX Security Appliance does not allow access to the higher security DMZ network from the lower security outside network. Therefore, in order to allow outside users access to a company Website, an ACL must be configured on the PIX.
Answer C is correct; Raising the security level of the partnernet interface to 55 will allows to connect to a server on DMZ1(Security 50), because it originates from a higher security interface.
The administrator would need to create an ACL and apply it to an interface on the PIX Security Appliance. Typically, it would be applied to the partnernet interface.

QUESTION 76
Which of the following commands can you use to accomplish the addition of an access control entry for 192.168.0.9. between line 3 and line 4 for the existing access-list while entering a slit of host addresses to an ACL, the administrator left out an ACE for host 192.168.0.9?

A. Certkiller 1 (config)#access-list aclin line 4
permit tcp any host 192.168.0.9 eq www
B. pix (config)#access-list aclin line 3
permit tcp any host 192.168.0.9 eq www
C. Certkiller 1 (config)# access-list aclin add-line 4
permit tcp any host 192.168.0.9 eq www
D. Certkiller 1 (config)# access-list aclin add-line 3
permit tcp any host 192.168.0.9 eq www

Answer: A

QUESTION 77




```
name 10.0.1.11 insidehost
name 172.16.1.2 webhost

global (outside) 1 192.168.1.20-192.168.1.254 netmask 255.255.255.0
global (dmz) 1 172.16.1.20-172.16.1.254 netmask 255.255.255.0
nat (inside) 1 10.0.1.0 255.255.255.0 0 0

static (dmz,outside) 192.168.1.18 webhost netmask 255.255.255.255 0 0
static (inside,dmz) 172.16.1.11 insidehost netmask 255.255.255.255 0 0
access-list dmzin permit tcp any host 10.0.1.11 eq www (hitcnt=0)
access-group dmzin in interface dmz
access-list aclin permit tcp any host 192.168.0.18 eq www (hitcnt=0)
access-group aclin in interface outside
```

A user on the dmz is complaining that they are unable to gain access to the inside host via HTTP. After reviewing the network diagram and partial configuration, the network administrator determined the following:

A. The global (dmz) command is not configured correctly.
B. The static (inside, dmz) command is not configured correctly.
C. The nat (dmz) command is missing.
D. The dmzin access list is not configured correctly.
E. The PIX is configured correctly, the issue is with the user's PC.

Answer: D

Explanation:
The DMZ can`t get access to inside host in www port 80 .
static (inside,DMZ) 172.16.1.11 insidehost (10.0.1.11) netmask 255.255.255.255
access-list DMZ-IN permit tcp 172.16.1.0 255.255.255.0 (or any) host 172.16.1.11 eq www
NB : access-list DMZ-IN permit tcp any host 10.0.1.11 eq www ==> the ip address 10.0.1.11 is an internal address must and can only be translated but not used to contact the external address

---

QUESTION 78
Which of the following commands enables TurboACL on a pix?

A. turboacl enable
B. turboacl global
C. turboacl setup
D. turboacl compiled

Answer: D

Explanation:
The turboacl compiled command on a pix firewall will globally enable the turboacl process and cause all access lists to be checked for turboacl eligibility. If any access lists have 19 or more entries, they are eligible and will be compiled into a table for more efficient access list checking.

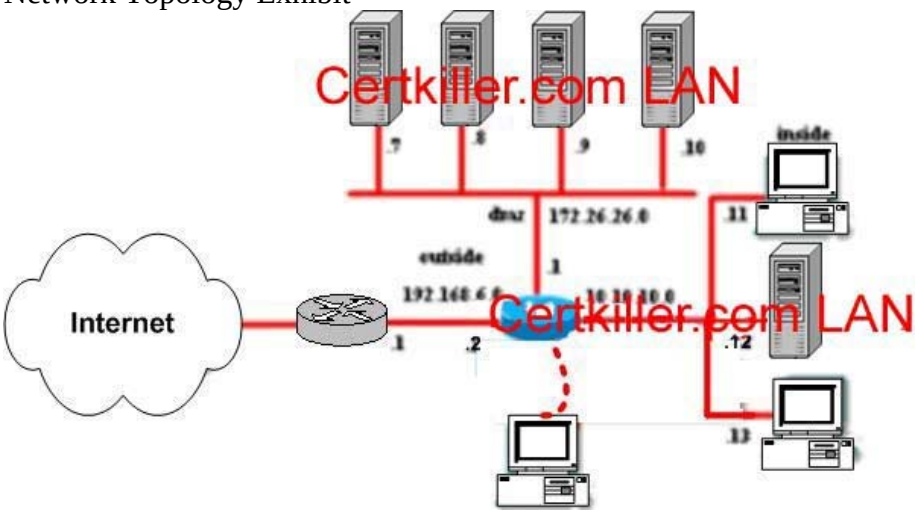
QUESTION 79
You have 100 users on your internal network at Certkiller Inc., you want only six of these users to perform FTP, Telnet, or HTTP outside the network.
Which PIX Firewall feature do you enable?

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

Answer: A

Explanation:
Not C: VAC+ is an acellerator card for IPSEC.

QUESTION 80
Network Topology Exhibit



Simulation Output Exhibit

```
PIX1#show ru
Building configuration...
: Saved
:
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
enable password [illegible]
passwd 2KFQnbNIdI [illegible]
hostname PIX1
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
name 10.10.10.11 insidehost
access-list aclin remark webserver 7
access-list aclin permit tcp any host 192.168.6.7 eq www
access-list aclin remark webserver 8
access-list aclin permit tcp any host 192.168.6.8 eq www
access-list aclin remark webserver 10
access-list aclin permit tcp any host 192.168.6.10 eq www
access-list aclin deny ip any any
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
```

Certkiller.com

Simulation Output Exhibit, continued

```
ip address outside 192.168.6.2 255.255.255.0
ip address inside 10.10.10.1 255.255.255.0
ip address dmz 172.26.26.1 255.255.255.0
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address dmz
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
global (outside) 1 192.168.6.17-192.168.6.254 netmask 255.255.255.0
global (dmz) 1 172.26.26.20-172.26.26.100 netmask 255.255.255.0
nat (inside) 1 0 0 0 0
static (dmz, outside) 192.168.6.7 172.26.26.7 netmask 255.255.255.255 0 0
nat (inside) 1 0 0 0 0
static (dmz, outside) 192.168.6.7 172.26.26.7 netmask 255.255.255.255 0 0
static (dmz, outside) 192.168.6.8 172.26.26.8 netmask 255.255.255.255 0 0
static (dmz, outside) 192.168.6.10 172.26.26.10 netmask 255.255.255.255 0 0
access-group aclin in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.6.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:65677976fdb81613092109e1f68af9d6
: end
PIX1#_
```

Certkiller.com

Scenario

You work as a Network administrator at the Moscow office of Certkiller .com. Certkiller recently added a new partnernet Server to the DMZ 182.26.26.9. To make it easier to manage the network, you are required to insert the new server ACE (access control element) to the existing access list in numerical order according to the server address. You also need to a remark defining the new server as the partnernet server. As the network administrator, perform the following tasks.

* Map the new partnernet server to the DMZ to a static address on the outside network, 192.168.6.9.

* Insert an access control element into the "aclin" ACL to allow anyone access to only port 80 of the new partnernet server. Make sure the new partnernet server ace is insterted

into the "aclin" ACL between the existing 192.168.6.8 server ace and the remark for webserver 10.
* Add a remark, "partnernet server, above the new parnernet server ace.
Note: You will not be able to ping the inside PIX interface from an interface connected to an inside host.

Answer:

Explanation:
1. Mapping the new partnernet server to DMZ:
pix(config)# static (dmz,outside) 192.168.6.9 192.26.26.9 netmask 255.255.255.255 0 0
2. Add remark and insert an access control elentment to "aclin" ACL
pix# show access-list
access-list aclin; 4 elements
access-list aclin line 1 remark webserver 7
access-list aclin line 2 permit tcp any host 192.168.6.7 eq www (hitcnt=0)
access-list aclin line 3 remark webserver 8
access-list aclin line 4 permit tcp any host 192.168.6.8 eq www (hitcnt=0)
access-list aclin line 5 remark webserver 10
access-list aclin line 6 permit tcp any host 192.168.6.10 eq www (hitcnt=0)
access-list aclin line 7 deny ip any any (hitcnt=0)
pix# conf t
pix(config)access-list aclin line 5 remark partnernet server
pix(config)# access-list aclin line 6 permit tcp any host 192.168.6.9 eq www
pix(config)# exit
pix# show access-list
access-list aclin; 5 elements
access-list aclin line 1 remark webserver 7
access-list aclin line 2 permit tcp any host 192.168.6.7 eq www (hitcnt=0)
access-list aclin line 3 remark webserver 8
access-list aclin line 4 permit tcp any host 192.168.6.8 eq www (hitcnt=0)
access-list aclin line 5 remark partnernet server
access-list aclin line 6 permit tcp any host 192.168.6.9 eq www (hitcnt=0)
access-list aclin line 7 remark webserver 10
access-list aclin line 8 permit tcp any host 192.168.6.10 eq www (hitcnt=0)

access-list aclin line 9 deny ip any any (hitcnt=0)
pix#

QUESTION 81
Kathy the security administrator at Certkiller Inc. and is working on ACLs. She needs to know which ACL parameters can be replaced by object-groups. (Choose three)

A. acl_ID
B. if_name
C. port
D. ICMP-type
E. source_addr
F. remote mask

Answer: C D E

Explanation:
Object grouping provides a way to group objects of a similar type so that a single ACL can apply to all the objects in the group. You can create the following types object groups
Network - Used to group client hosts, server hosts or subnets
Protocol - ip, tcp, or udp
Service - Used to group TCP or UDP port numbers assigned to a different service
Icmp - Used to group ICMP message types to which you permit or deny access.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 8 page 4

QUESTION 82
You are the network security administrator at Certkiller Inc., Certkiller has an enterprise network with a complex security policy.
Which PIX Firewall feature should you configure to minimize the number of ACLs needed to implement your policy?

A. You should configure the ASA
B. You should configure the packet capture
C. You should configure the object grouping
D. You should configure the turbo ACLs
E. You should configure the IP helper

Answer: C

Explanation:
To simplify the task of creating and applying ACLs, you can group network objects such as hosts and services such as FTP and HTTP. This reduces the number of ACLs required to implement complex security policies.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 8 page 3

QUESTION 83
Which of the following object group types can be created in the PIX Firewall? Choose three.

A. icmp-type
B. service
C. server host
D. ACL out
E. DHCP
F. protocol

Answer: A, B, F

Explanation:
Object grouping provides a way to group objects of a similar type so that a single ACL can apply to all the objects in the group. You can create the following types of object groups:
1) Network - Used to group client hosts, server hosts, or subnets.
2) Protocol - Used to group protocols. It can contain one of the keywords icmp, ip, tcp, or udp, or an integer in the range 1 to 254 representing an IP protocol number. Use the keyword to match any Internet protocol, including Internet Control Message Protocol (ICMP), TCP, and UDP.
3) Servcie - Used to group TCP or UDP port numbers assigned to a different service.
4) ICMP-type - Used to group ICMP message types to which you permit or deny access.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.8-6

QUESTION 84
What role does the object-group command fulfill? Choose two.

A. defines members of an object group
B. inserts an object group in an ACL
C. displays a list of the currently configured object groups of the specified type.
D. names an object group
E. enables sub-command mode
F. Describes the object group

Answer: D, E

Explanation:
Use the object-group command to enter the appropriate subcommand mode for the type of group you want to configure. When you enter the object-group command, the system enters the appropriate subcommand mode for the type of object you specify in the object-group command. All subcommands entered from the subcommand prompt apply to the object group identified by the object-group command.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.8-7

QUESTION 85
What pix command enables object-grouping for the network object-group type?

A. object-group network servers
B. object-grouping network servers
C. group-object network servers
D. group-object type network servers

Answer: A

Explanation:
Create pix object-groups with the object-group (type) (name) command.

QUESTION 86
Jason the security administrator at Certkiller Inc. is working on the object-group command on the PIX Firewall. Which are functions of the object-group command? (Choose two)

A. A function of the object-group command defines members of an object group.
B. A function of the object-group command inserts an object group in an ACL.
C. A function of the object-group command displays a list of the currently configured object groups of the specified type.
D. A function of the object-group command names an object group.
E. A function of the object-group command enables sub-command mode.
F. A function of the object-group command describes the object group.

Answer: D E

Explanation: Object-group network grp_id assigns a name to the group and enables the network sub-command mode.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 8 page10
To simplify your configuration, object grouping is supported in Cisco PIX Device Manager Version 2.0. Object grouping enables you to define groups of objects such as hosts, IP addresses, or network services. You can use these groups, for example, when you create and apply access rules. When you include a Cisco PIX Firewall object group in a PIX Firewall command, it is the equivalent of applying every element of the object group to the PIX Firewall command.
Reference: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixge_ds.pdf

---

QUESTION 87
How do you view all object-groups configured on a pix?

A. show object-group
B. show group-object
C. show object-types

D. show object-group types

Answer: A

Explanation:
All of the object-groups configured on a pix can be viewed with the show object-group command.

QUESTION 88
When are duplicate objects allowed in object groups?

A. When they are due to the inclusion of group objects.
B. When a group object is included, which causes the group hierarchy to become circular.
C. Never
D. Always, because there are not conditions of restrictions.

Answer: A

Explanation: Duplicated objects are allowed in an object group if it is due to the inclusion of group objects.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 8 page 15

QUESTION 89
If the FTP protocol fixup is not enabled for a given port, which statements are true? (Choose two)

A. The true statement is outbound standard FTP will not work properly on that port.
B. The true statement is outbound standard FTP will work properly on that port.
C. The true statement is outbound passive FTP will not work properly on that port.
D. The true statement is outbound passive FTP will work properly on that port as long as outbound traffic is not explicitly disallowed.
E. The true statement is outbound standard FTP will work properly on that port if outbound traffic is not explicitly disallowed.
F. The true statement is inbound standard FTP will not work properly on that port even if a conduit to the inside server exists.

Answer: A D

Explanation: If the Fixup protocol ftp command is not enabled for a given port, then:
Outbound standard FTP will NOT work properly on that port.
Outbound PFTP will work properly on that port as long as outbound traffic is not explicitly disallowed
Inbound standard FTP will work properly on that port if a conduit to the inside server exists

Inbound PFTP will NOT work properly on that port.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 10 page 7

QUESTION 90
Jason the security administrator at Certkiller Inc. is working on the SMTP fixup command on the PIX Fiewall. If the SMTP fixup is disabled, what happens?

A. What happens is all SMTP commands are allowed to mail servers, and they are no longer protected from known security problems with some mail server implementations.
B. What happens is a safe conduit exists for SMTP connections from the outside to an inside e-mail server.
C. What happens is only the SMTP commands specified in RFC 821 section 4.5.1 are allowed to a mail server: HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT.
D. What happens is all SMTP commands are allowed to a mail server, but mail servers are still protected from known security problems with some mail server implementations.

Answer: A

Explanation: If disabled, all SMTP commands are allowed through the firewall-potential mail server vulnerabilities are exposed.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 11 page 3
Mailguard allows only the seven SMTP minimum-required commands as described in Section 4.5.1 of
RFC 821. These seven minimum-required commands are: HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. Other commands, such as KILL, WIZ, and so forth, are intercepted by the PIX and they are never sent to the mail server on the inside of your network. The PIX responds with an "OK" to even denied commands, so attackers would not know that their attempts are being thwarted.
Reference:
http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2030/products_tech_note09186a00800b2ecb.shtml

---

QUESTION 91
What port does the PIX Firewall inspect for FTP traffic by default?

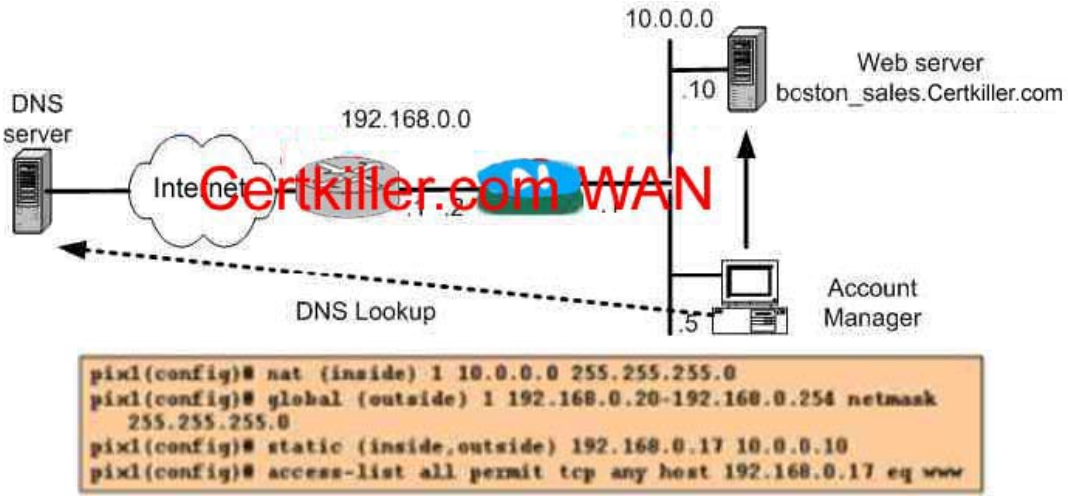
A. Port 20
B. Port 21
C. Port 23
D. It does not inspect any port for FTP traffic

Answer: B

Explanation:
Active mode FTP uses two channels for communications. When a clients start an FTP connection, it opens a TCP channel from one of its high-order ports to port 21 on the server. This is referred to as the command channel. When the client requests data from

the server, it thells the server to send the data to given high-order port. The server acknowledges the request and initiates a conncection from its own port 20 to the high-order port that the client requested. This is referred to as the data channel.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.9-10

QUESTION 92



The graphic shows a partial configuration. An account manager (AM) at a small site wants to access the boston_sales. Certkiller .com server. The account manager knows the name, but not the IP address of the server. The AM's PC requests DNS resolution of the inside web server address from a DNS server on an outside network. To enable the PIX Firewall to perform a DNS A record translation correctly for the above mention application, the DNS key word should be added to which of the above mention commands?

A. NAT command
B. Global command
C. Access-list command
D. Static command

Answer: D

Explanation:
Both the NAT and the STACTIC statement have a DNS option, the difference is that the static rewrites the local address in DNS replies to the global address, so since the DNS server is a server on the outside interface this is the right answer.

QUESTION 93
John the security administrator for Certkiller Inc. is working to multicast.
How does John get to the multicast subcommand mode where he can enter the igmp commands for further multicast support?

A. By using the clear IGMP group command.
B. By entering the igmp interface command in privileged mode.

C. By entering the multicast interface command in configuration mode.
D. By entering the multicast mode command in configuration mode.

Answer: C

Explanation: Use the multicast interface command to enable multicast forwarding on each interface and place the interfaces in multicast promiscuous mode. When you enter the command, the CLO enters multicast subcommand mode and the prompt changes to (Config-mulitacast)#.
Reference: Cisco Secure PIX Firewall Advanced 3.1 9-10

QUESTION 94
The security team at Certkiller Inc. is working on VoIP for the PIX Firewall.
Which statements about the PIX Firewall in VoIP environments are true? (Choose two)

A. The true statement is the PIX Firewall allows SCCP signaling and media packets to traverse the PIX Firewall and interoperate with H.323 terminals.
B. The true statement is the PIX Firewall does not support the popular call setup protocol SIP because TCP can be used for call setup.
C. The true statement is the PIX Firewall supports the Skinny Client Control Protocol, which allows you to place IP phones and Call Manager on separate sides of the PIX Firewall.
D. The true statement is users behind the PIX Firewall can place outbound calls with IP phones because they use HTTP tunneling to route packets through port 80, making them appear as web traffic.

Answer: A, C

Explanation: Fixup protocol skinny port [-port]
Enables the SCCP (skinny) protocol
Dynamically opens pinholes for media sessions and nat -embedded IP addresses
Supports Ip telephony
Can coexist in an H323 environment
Default port is 2000
Due to SCCP support, an IP phone and Cisco Call manager can now be placed on separate sides of the PIX Firewall.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 10 page 14

QUESTION 95
John the security administrator at Certkiller Inc. is configuring the PIX Firewall to forward multicast transmissions from an inside source. Which of these steps are necessary? (Choose two)

A. It is necessary for John to use the igmp join-group command to enable the PIX Firewall to forward IGMP reports.
B. It is necessary for John to use the multicast interface command to enable multicast

forwarding on each PIX Firewall interface.
C. It is necessary for John to use the igmp forward command to enable multicast forwarding on each PIX Firewall interface.
D. It is necessary for John to use the mroute command to create a static route from the transmission source to the next-hop router interface.
E. It is necessary for John to use the route command to create a static route from the transmission source to the next-hop router interface.

Answer: B, D

Explanation: Use the Mroute command to create a static route from the transmission source to the next-hop router interface.
Inside Multicast transmission source example
Pixfirewall (config)# multicast interface outside
Pixfirewall (config-multicast)# exit
Pixfirewall (config))# multicast interface inside
Pixfirewall (config-multicast)# mroute 10.0.0.11 255.255.255.255 inside 230.1.1.2 255.255.255.255 outside
In the figure, multicast traffic is enabled on the inside and outside interface. A static multicast route is configured to enable inside host 10.0.0.11 to transmit multicasts to members of group 230.1.1.2 on the outside interface
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 9 pages 13-14

QUESTION 96
Greg the security administrator at Certkiller Inc. is working allowing multicast transmissions to host on the PIX Firewall.
What must Greg do to enable hosts behind the PIX Firewall to receive multicast transmissions? (Choose two)

A. Greg must use the multicast interface command to enable multicast forwarding on each interface and place the interfaces in multicast promiscuous mode.
B. Greg must use the igmp forward command to enable IGMP forwarding on each PIX Firewall interface connected to hosts that will receive multicast transmissions.
C. Greg must use the igmp join-group command to configure the PIX Firewall to join a multicast group.
D. Greg must use the multicast interface command to enable multicast forwarding on each interface and place the interfaces in multicast safe mode.
E. v the permit option of the access-list command to configure an ACL that allows traffic to permissible Class D destination addresses.

Answer: A B

Explanation: Use the multicast interface command to enable multicast forwarding on each interface and place the interface in multicast promiscuous mode.
Use the igmp forward command to enable IGMP forwarding on each PIX interface connected to hosts that will receive multicast transmissions.

Pixfirewall (config)# multicast interface dmz
Pixfirewall (config-multicast)# exit
Pixfirewall (config)# multicast interface inside
Pixfirewall (Config-multicast)#igmp forward interface dmz
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 9 pages 10 and 12

QUESTION 97
Kathy is the security administrator at Certkiller Inc. and she needs to know which protocols does the PIX Firewall use to enable call handling sessions, particularly two-party audio conferences or calls?

A. Remote Function Call
B. Real-Time Transport Protocol
C. Session Initiation Protocol
D. Point-to-Point Protocol over Ethernet

Answer: C

Explanation:
Session Initiation Protocol (SIP) enables call handling sessions-particulary two party audio conference, or "calls."
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap10 page 13

QUESTION 98
What will you advice the Certkiller trainee to do to enable hosts behind the PIX Firewall to receive multicast transmissions? Choose all that apply.

A. Use the igmp 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 interface in multicast safe mode.
C. Use the multicast interface command to enable multicast forwarding on each interface and place the interfaces in multicast promiscuous mode.
D. Use the igmp forward command to enable IGMP forwarding on each PIX Firewall interface connected to hosts that will receive multicast transmissions.
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 99
Which of the following statements regarding PIX Firewall's multicasting capabilities are valid? Select three.

A. The PIX Firewall is incapable of supporting multicast.
B. The PIX Firewall is capable of supporting Stub Multicast Routing.

C. The only way you can currently enable the PIX Firewall to pass multicast traffic is by constructing GRE tunnels.
D. To enable the PIX Firewall for Stub Multicast Routing, you must configure GRE tunnels for passing multicast traffic.
E. The PIX Firewall can be configured to act as an IGMP proxy agent.
F. When the PIX Firewall is configured for Stub Multicast Routing, it is not necessary to construct GRE tunnels to allow multicast traffic to bypass the PIX Firewall.

Answer: B, E, F

Explanation: With SMR, the PIX Firewall acts as an IGMP proxy agent. It forwards IGMP messages from hosts to the upstream multicast router, which takes responsibility for forwarding multicast datagrams from one multicast group to all other network that have members in the group. When SMR is used, it is not necessary to construct Generic Route Encapsulation (GRE) tunnels to allow multicast traffic to bypass the PIX Firewall.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.13-30

QUESTION 100

pix1 (config) # multicast interface outside
pix1 (config-multicast) " igmp access-group 120
pix1 (config) # accesss-list 120 permit udp any
host 10.0.1.20
pix1 (config) # multicast interface inside
pix1 (config-multicast) # igmp forward
interface outside
Certkiller 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, 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

QUESTION 101
Your new network administrator at Certkiller has recently modified your PIX Firewall's configuration. You are suddenly experiencing security breaches involving Internet mail.
What change did the administrator make?

A. The administrator disabled the PIX Firewalls smtp fixup.
B. The administrator disabled the PIX Firewalls mailport fixup.
C. The administrator enabled the PIX Firewalls ils fixup on port 25.
D. The administrator defined the ports on which to activate Mail Guard.

Answer: A

Explanation: The fixup protocol smtp command enables the Mail Guard feature, which only lets mail servers receive the RFC 821, section 4.5.1, commands of HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/cmdref/qref.htm

---

QUESTION 102
What port does the PIX Firewall inspect for FTP traffic, by default?

A. It does not inspect any port for FTP traffic.
B. The default port is 23
C. The default port is 21
D. The default port is 20

Answer: C

Explanation: By default, the PIX Firewall inspects port 21 connections for FTP traffic. If you have FTP servers using ports other than ports 21, you need to use the fixup protocol ftp command to have the pix firewall inspect these other ports for FTP traffic.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 10 page 7

QUESTION 103
James the security administrator at Certkiller Inc. is working on the SYN Flood Guard command. Which two commands can James use to enable SYN Flood Guard? (Choose two)

A. The nat command

B. The static command
C. The alias command
D. The synflood command

Answer: A B

Explanation:
Use the static command to limit the number of embryonic connections allowed to the server to protect internal hosts against DoS attacks.
Use the nat command to protect external hosts against DoS attacks, and to limit the number of embryonic connections allowed to the server.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 5 pages 69 and 71

QUESTION 104
Certkiller 's web traffic has come to a halt because your PIX Firewall is dropping all new connection attempts.
Why?

A. The shun feature of the PIX Firewall has taken effect because the embryonic threshold you set in the nat command was reached.
B. You are running a software version older than 5.2, and the embryonic threshold you set in the static command was reached.
C. The TCP Intercept feature of the PIX Firewall has taken effect because the embryonic threshold you set in the static command was reached.
D. The intrusion detection feature of the PIX Firewall has taken effect because the embryonic threshold you set in the conduit command was reached.

Answer: B

Explanation:
Prior to version 5.2, PIX Firewall offered no mechanism to protect systems reachable via a static and TCP conduit from TCP SYN segment attacks. With the new TCP intercept feature, once the optional embryonic connection limit is reached, and until the embryonic connection count falls below this threshold, every SYN segment bound for the affected server is intercepted.
This feature requires no change to the PIX Firewall command set, only that the embryonic connection limit on the static command now has a new behavior.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/relnotes/pixrn521.pdf
also see: Cisco Secure PIX Firewall Advanced 3.1 chap 11 page 13

QUESTION 105
How will you go about configuring the PIX Firewall to protect against SYN floods?

A. Make use of the emb_conns argument to limit the number of fully opened connections.

B. Set the max_conns option in the nat command to less than the server can handle.
C. Set the emb_limit option in the name command to less than the server can handle.
D. Set the emb_limit option in the static command to less than the server can handle.

Answer: D

Explanation:
Specifies the maximum number of embryonic connections per host. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. Set a small value for slower systems, and a higher value for faster systems. The default is 0, which means unlimited embryonic connections.
The embryonic connection limit lets you prevent a type of attack where processes are started without being completed. When the embryonic limit is surpassed, the TCP intercept feature intercepts TCP synchronization (SYN) packets from clients to servers on a higher security level. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and combines the two half-connections together transparently. Thus, connection attempts from unreachable hosts never reach the server. The PIX firewall accomplishes TCP intercept functionality using SYN cookies.
Note
This option does not apply to outside NAT. The TCP intercept feature applies only to hosts or servers on a higher security level. If you set the embryonic limitfor outside NAT, the embryonic limit is ignored.

QUESTION 106
In which way does the DNS Guard feature help in the prevention of UDP session hijacking and DoS attacks?

A. It prevents all DNS responses from passing through the PIX Firewall.
B. It prevents any DNS name resolution requests to DNS servers behind the PIX Firewall.
C. If multiple DNS servers are queried, only the first answer from the first server to reply is allowed through the PIX Firewall.
The PIX does not wait for the default UDP timer to close the sessions but tears down connections to all DNS servers after receiving the first reply.
D. Only the first reply from any given DNS server is allowed through the PIX Firewall.
The PIX discards all other replies from the same server.

Answer: C
Excel nr b-49 föreslår D (Only the first...)

Explanation:
Generic UDP handling of DNS queries leaves connection opens longer than prudent. Instead, the PIX Firewall identifies each outbound DNS resolve request and then tears down the connection as soon at the reply is received.
PIX FW Advanced, Cisco Press, p. 365-366

QUESTION 107
What pix feature prevents DNS DOS attacks?

A. DNS MAX
B. Dynamic DNS
C. DNS SYN Reject
D. DNS Flood Guard

Answer: D

Explanation:
DNS Flood Guard prevents multiple responses to a DNS request. Only 1 DNS response is let through the pix to the requesting host, and all other DNS responses are dropped. This helps the requesting host from possibly experiencing a DNS DOS.

QUESTION 108
Johnthe security administrator for Certkiller Inc. is working on securing the Firewall with using a blocking function.
Which command applies a blocking function to an interface receiving an attack?

A. The shun command
B. The conduit command
C. The ip deny command
D. The interface command

Answer: A

Explanation:
Shun src_ip [dst_ip sport dport [protocol] Applies a blocking function to an interface -
Reference: Cisco Secure PIX Firewall Advanced 3.1 11-22

QUESTION 109
Kathy the security administrator at Certkiller Inc. is working on enabling IDS in the PIX Firewall. Which command enables intrusion detection in the PIX Firewall?

A. The shun command
B. The ip audit command
C. The enable ids command
D. The ids enable command

Answer: B

Explanation: Intrusion detection, or auditing, is enabled on the PIX Firewall with the ip audit commands.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 5 pages 69 and 71

QUESTION 110
Which of the following statements regarding intrusion detection in the PIX Firewall are valid? Choose two.

A. When a policy for a given signature class is crated and applied to an interface, all supported signatures of that class are monitored unless you disable them.
B. Only the signatures you enable will be monitored.
C. The PIX Firewall supports only inbound auditing.
D. IP audit policies must be applied to an interface with the ip audit interface command.
E. When a policy for a given signature class is created and applied to an interface, all supported signatures of that class are monitored and cannot be disabled until you remove the policy from the interface.
F. IP audit policies must be applied to an interface with the ip audit signature command

Answer: A, D

Explanation:
Each interface can have two policies: one for informational signatures and one for attack signatures. If you want them both to be active simultaneously, they shoud share the same policy name. When a policy for a given signature class is created and applied to an interface, all supported signatures of that class are monitored unless you disable them with the ip audit signature disable command.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.10-18

QUESTION 111
What is the rationale behind using the shun command?

A. PIX Firewall does not support shunning.
B. To enable the PIX Firewall to detect and block intrusion attempts.
C. You know the IP address of an attacking host and want the PIX Firewall to drop packets containing its source address.
D. You know the IP address of an attacking host and want the PIX Firewall to drop packets containing its destination address.

Answer: C

Explanation:
The shun command applies a blocking function to the interface receiving the attack. Packets containing the IP source address of the attacking host will be dropped and logged until the blocking function is removed manually or by the Cisco IDS master unit. No traffic from the IP source address will be allowed to traverse the PIXFirewall unit and any remaining connections will time out as part of the normal architecture. The blocking function of the shun command is applied whether or not a connection with the specified host address is currently active.
If the shun command is used only with the source IP address of the host, then the other

defaults will be 0. No further traffic from the offending host will be allowed.
Because the shun command is used to block attacks dynamically, it is not displayed in your PIXFirewall configuration.

QUESTION 112
Which of the following statements regarding intrusion detection in the PIX Firewall is valid?

A. The PIX Firewall supports a subset of the intrusion detection signatures supported by the Cisco IDS product family.
B. The PIX Firewall can detect three different types of signatures: information signatures, alarm signatures, and attack signatures.
C. The PIX Firewall supports the Cisco IDS PostOffice protocol that is used by the Cisco IDS appliances and the Catalyst 6000 IDSM.
D. The PIX Firewall recognizes the same signatures supported by the Cisco IDS product family.

Answer: A

Explanation:
The Cisco IDS family can detect over 700 signatures while the PIX IDS can detect 56 different signatures.

QUESTION 113
How many different intrusion detection signatures (IDS) can a pix firewall detect?

A. 5
B. 17
C. 53
D. 96

Answer: C

Explanation:
The pix firewall has modest IDS capabilities, including the scanning of up to 53 of the most common IDS signatures.

QUESTION 114
John the security administrator at Certkiller Inc. has configured the PIX Firewall and an AAA server for authentication. Telnet and FTP authentication work normally, but HTTP authentication does not.
Why?

A. The problem is John has not enabled HTTP, Telnet, and FTP authorization, which is required for HTTP authentication.
B. The problem is John has not enabled HTTP authorization, which is required for HTTP

authentication.
C. The problem is HTTP authentication is not supported.
D. The problem is re-authentication may be taking place with the web browser sending the cached username and password back to the PIX Firewall.

Answer: D

Explanation:
HTTP - A window is displayed in the browser requesting username and password. If authentication (and authorization) is successful, the user arrives at the destination web site beyond. Keep in mind that browsers cache usernames and passwords! If it appears that the PIX should be timing out an HTTP connection but is not doing so, it is likely that re-authentication actually is taking place with the browser "shooting" the cached username and password to the PIX, which then forwards this to the authentication server. PIX syslog and/or server debug will show this phenomenon. If Telnet and FTP seem to work "normally", but HTTP connections do not, this is why.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094ea9.shtml

---

QUESTION 115
James is the security administrator at Certkiller Inc. and he needs to know which statements about authenticating to the PIX Firewall are true? (Choose two)

A. You cannot authenticate with Telnet.
B. You can authenticate with Telnet with which you have up to four changes to log in.
C. You cannot authenticate with HTTP.
D. Although FTP is a widely-used service, there is not way to authenticate.
E. 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_username
aaa_password@remote_password
F. If you are authenticating for HTTP and enter an incorrect password, the connection is dropped immediately.

Answer: B, E

Explanation:
Telnet-you get a prompt generated by the pix firewall. You have up to four chances to log in. If the username or password fails after the fourth attempt, the pix firewall drops the connection.
If 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, enter the username and password in the following format.

Aaa_username@remote_username
Aaa_password@remote_password
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 12 page 4

QUESTION 116
Which of the following statements regarding authentication and the PIX Firewall is valid?

A. One network is capable of authenticating with both TACACS+and RADIUS.
B. If any network connected to your PIX Firewall authenticates with TACACS+, any other networks are compelled to use RADIUS for authentication.
C. One network is unable to authenticate with both TACACS+and RADIUS.
D. If any network connected to your PIX Firewall authenticates with TACACS+, any other networks that use authentication and connect to the PIX Firewall must also use TACAS+.

Answer: C

Explanation:
For each IP address, one aaa authentication command is permitted for inbound connections and one for outbound connections. The PIX firewall permits only one authentication type per network. For example, if one network connects through the PIX Firewall using TACACS+ for authentication, another network connecting through the PIX Firewall can authenticate with RADIUS, but a single network cannot authenticate with both TACACS+ and RADIUS. In the example in the figure, any inbound FTP, HTTP, HTTPS, and Telnet session is intercepted by the PIX Firewall and authenticated by the AAA server. An AAA server from the NYCSACS group verifies the authentication username and password. Once authenticated, the session is cut through the PIX Firewall.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.11-19

QUESTION 117
How many times will a pix attempt to contact an AAA server before trying to contact a new AAA server?

A. 0
B. 1
C. 2
D. 3
E. 4

Answer: E

Explanation:
By default, a pix firewall will try to contact an AAA server for user authentication 4

times before considering that server unresponsive and attempting to contact a different AAA server.

QUESTION 118
How long does a pix firewall wait by default for a response from an AAA server before trying to contact the server again?

A. 2 seconds
B. 4 seconds
C. 5 seconds
D. 8 seconds

Answer: C

Explanation:
When a pix firewall queries an AAA server to authenticate a user, the firewall will by default wait 5 seconds for a response. If one is not received within 5 seconds, it will then query the server again (up to 4 times). Change this timer with the timeout keyword with the aaa-server command (aaa-server radius (dmz1) host 192.168.10.1 (key) timeout (seconds)).

QUESTION 119
What external AAA servers can the pix firewall use to authenticate users? Choose all that apply.

A. tacacs
B. tacacs+
C. radius
D. radius+
E. kerberos
F. kerberos+

Answer: B,C

Explanation:
RADIUS and TACACS+ AAA servers are supported by the pix to authenticate remote users with. The pix can also authenticate with an internal database, but that is only recommended for small networks.

QUESTION 120
What are the three parts of AAA? Choose all that apply.

A. administration
B. authorization
C. accounting
D. authentication

E. auditing

Answer: B,C,D

Explanation:
An AAA server provides three different functions: Authorization, Authentication, and Accounting.

QUESTION 121
Jen the new Certkiller Inc. security administrator is working on the installation for Cisco Secure ACS.
During Cisco Secure ACS installation, Jen is prompted to enter the access server name and the access server IP address.
Which device name and IP address do Jen enter?

A. Server on which AAA services are running.
B. Windows NT server from which you will be accessing the PIX Firewall.
C. IOS router on which AAA services are running.
D. Network access server that will be using the Cisco Secure ACS services.

Answer: D

Explanation: Access Server Name - Name of the network access server (NAS) that will be using the CSACS services.
Access Server IP Address - Ip address of the NAS that will be using the CSACS services
Reference:-Cisco Secure PIX Firewall Advanced 3.1 chap 12 page 10

QUESTION 122
Which of the following operating systems can CSACS be installed on? Choose all that apply.

A. windows nt
B. unix
C. solaris
D. macintosh
E. windows 2000

Answer: A,E

Explanation:
The Cisco Secure Access Control Server (CSACS) application developed by Cisco is available for Windows NT and Windows 2000 only.

QUESTION 123
Jason the security administrator at Certkiller Inc. is working on configuring the PIX Firewall command.

Why is the group tag in the aaa-server command important?

A. It is important because the group tag identifies which users require authorization to use certain services.
B. It is important because the group tag identifies which user groups must authenticate.
C. It is important because the aaa command references the group tag to know where to direct authentication, authorization, or accounting traffic.
D. It is important because the group tag enables or disables user authentication services.

Answer: C

Explanation:
Use the aaa-server command to specify AAA server groups...The AAA command references the group tag to direct authentication, authorization, and accounting traffic to the appropriate AAA server.
Reference: Cisco Secure PIX Firewall Advanced 3.1 12-12

QUESTION 124
John the security administrator at Certkiller is trying to have users reauthenticate.
A user does not have to reauthenticate as you think he should.
What is the easiest way to force him to reauthenticate the next time he tries to establish a connection?

A. By rebooting the PIX Firewall.
B. By using the timeout uauth command.
C. By using the reauth command.
D. By using the clear auth command

Answer: D

Explanation:
Use the timeout uauth command to specify how long the cache should be kept after the user
connections become idle. The timeout command value must be at least two minutes. Use the
clear uauth command to delete all authorization caches for all users, which causes them to
reauthenticate the next time they create a connection.
The inactivity and absolute qualifiers cause users to reauthenticate after either a period of inactivity or an absolute duration. The inactivity timer starts after a connection becomes idle. If a user establishes a new connection before the duration of the inactivity timer, the user is not required to reauthenticate. If a user establishes a new connection after the inactivity timer
expires, the user must reauthenticate.
Reading the above, D is probably the correct answer. The timeout has to be at least 2 minutes, and it says: If a user establishes a new connection before the duration of the

inactivity timer, the user is not required to reauthenticate. But "clear auth" guarantees reauthorization.

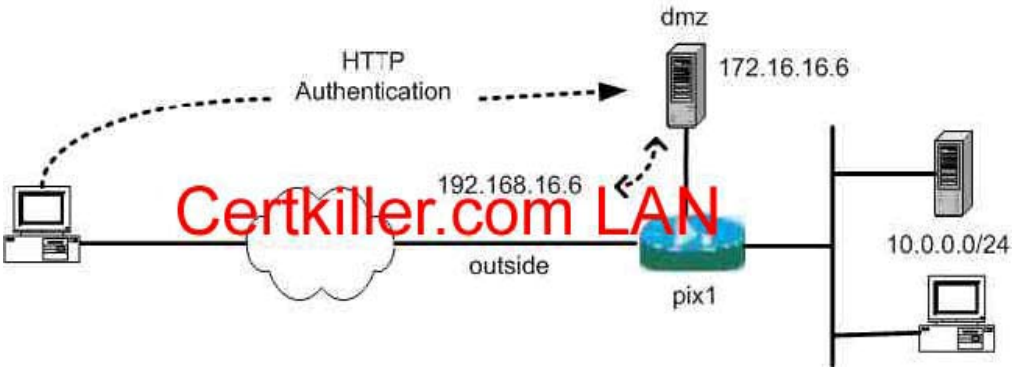
QUESTION 125
Which of the following statements regarding PIX Firewall and virtual HTTP is valid?

A. The PIX Firewall enables web browsers to work correctly with its HTTP authentication. The PIX Firewall redirects the web browser's initial connections to an IP address which resides within the PIX Firewall, authenticates the user, and then redirects the browser back to the URL the 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 use, 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
REFERENCE:
http://www.cisco.com/en/US/products/sw/cscowork/ps3993/products_user_guide09186a008019b149.html

---

QUESTION 126



At a small site in the above network diagram illustrated above, network administrator chose to authenticate WWW cut-through proxy traffic via a local database on the PIX Firewall.
What commands should the administrator enter to accomplish this task?

A. pix1(config)# static (dmz,outside) 192.168.16.6 172.16.16.6
pix1(config)# access-list 150 permit tcp any host 172.16.16.6 eq www
pix1(config)# aaa authentication match 150 outside LOCAL
B. pix1(config)# static (dmz,outside) 192.168.16.6 172.16.16.6
pix1(config)# access-list 150 permit tcp any host 192.168.16.6 eq www
pix(config)# aaa authentication match 150 outside pix1
C. pix1(config)# static (dmz,outside) 192.168.16.6 172.16.16.6
pix1(config)# access-list 150 permit tcp any host 172.16.16.6 eq www
pix1(config)# aaa authentication match 150 outside pix1

D. pix1(config)# static (dmz, outside) 192.168.16.6 172.16.16.6
pix1(config)# access-list 150 permit tcp any host 192.168.16.6 eq www
pix1(config)# aaa authentication match 150 outside LOCAL

Answer: D

QUESTION 127
What will you as the network security for a large network do if you want to compel users require authentication for connections through the PIX Firewall using services or protocols that do not support authentication.
What can you do?

A. Make use of Virtual HTTP.
B. Create a virtual Telnet address, and have users authenticate to this address before accessing other services.
C. There is currently no way to require authentication for services other than those that support it; FTP, HTTP, and Telnet.
D. Create a virtual FTP address, and have users authenticate to this address before accessing other services.

Answer: B

Explanation:
The virtual telnet command allows the Virtual Telnet server to provide a way to pre-authenticate users who require connections through the PIXFirewall using services or protocols that do not support authentication.
The virtual telnet command can be used both to log in and log out of the PIXFirewall. When an unauthenticated user Telnets to the virtual IP address, they are challenged for their username and password, and then authenticated with the TACACS+ or RADIUS server. Once authenticated, they see the message "Authentication Successful" and their authentication credentials are cached in the PIXFirewall for the duration of the uauth timeout.
If a user wishes to log out and clear their entry in the PIXFirewall uauth cache, the user can again Telnet to the virtual address. The user is prompted for their username and password, the PIXFirewall removes the associated credentials from the uauth cache, and the user will receive a "Logout Successful" message.
If inbound users on either the perimeter or outside interfaces need access to the Virtual Telnet server, a static and access-list command pair must accompany use of the virtual telnet command.
The Virtual Telnet server provides a way to pre-authenticate users who require connections through the PIXFirewall using services or protocols that do not support authentication. Users first connect to the Virtual Telnet server IP address, where the user is prompted for a username and password.
virtual telnet-After adding the virtual telnet command to the configuration and writing the configuration to Flash memory, users wanting to start PPTP sessions through PIXFirewall use Telnet to access the ip_address as shown in the following example:

On the PIXFirewall:
virtual telnet 209.165.201.25static (inside, outside) 209.165.201.25 209.165.201.25 netmask 255.255.255.255access-list acl_out permit tcp any host 209.165.201.25 eq telnetaccess-group acl_out in interface outsidewrite memory

---

QUESTION 128
How do you add a AAA server to your pix firewall configuration?

A. aaa-server farm tacacs+
B. aaa-server farm protocol tacacs+
C. aaa new-model farm radius
D. aaa new-model farm tacacs+

Answer: B

Explanation:
Add a AAA server to your pix configuration by using the aaa-server (server name) protocol (radius/tacacs+) command.

QUESTION 129
Johnthe security administrator at Certkiller Inc. is working on ACLs.
Which statement about downloadable ACLs is true?

A. The true statement is a downloadable ACL is not downloaded again as long as it exists on the PIX Firewall.
B. The true statement is a the PIX Firewall does not support versioning downloadable ACLs.
C. The true statement is a downloadable ACLs must have names assigned to them.
D. The true statement is a downloadable ACLs are downloaded from the PIX Firewall to the Cisco Secure ACS server during authentication

Answer: A

Explanation:
The PIX Firewall checks to see if it already has the named ACL. A downloadable ACL is not downloaded again as long as it exists on the PIX Firewall.
Student Guide CSPFA 3.2 page 11-48
There are two methods of configuring downloadable ACLs on the AAA server. The first method, downloading named ACLs, is to configure the Shared Profile Components (SPC) to include both the ACL name and the actual ACL and then configure a user, or group, authentication profile to include the SPC. . If you configure a downloadable ACL as a named SPC, you can apply that ACL to any number of Cisco Secure ACS user, or group, profiles. This method should be used when there are frequent requests for downloading a large ACL. The second method is to configure on an AAA server a user authentication profile that includes the actual PIX Firewall ACL.In this case, the ACL is not identified by a name. You must define each ACL entry in the user profile. This

method should be used when there are not frequent requests for the same ACL. For instructions on downloading ACLs without names, refer to the documentation on Cisco.com.
Student Guide CSPFA 3.2 page 11-50
The answer C appears wrnog. Page 11-48 co-insides with option A i.e. downloadable acl is not downloaded again
Page 11-50 provides procedures of names and unnamed downloadable ACL. Therefore, the statement that ACLs must have names assigned to them is FALSE.

QUESTION 130
In what way can downloading 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 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.
C. You can enter an ACL once, in Cisco Secure ACS, and then have it downloaded to any number of PIX Firewalls during user authentication.
D. You can enter an ACL once in Cisco Secure ACS, and then have it downloaded to no more than 10 PIX Firewalls during authentication.

Answer: C

Explanation:
Downloadbable ACLs enable you to enter an ACL once, in Cisco Secure ACS, and then load that ACL to any number of PIX Firewalls. Sownloadable ACLs work in conjunction with ACLs that are configured directly on the PIX Firewall and applied to its interfaces. Neither type of ACL takes precedence over the other. In order to pass through the PIX Firewall, traffic must be permitted by both the interface ACL and the dynamic ACL if both are applicable. If either ACL denies the traffic, the traffic is prohibited.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.11-48

QUESTION 131
You work as network administrator at Certkiller . Certkiller 's 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. The current IP addresses on the primary PIX Firewall remain the same, but the current IP addresses of the secondary become the virtual IP addresses you configured.
B. The current IP addresses will be deleted.
C. The ones on both the primary and secondary PIX Firewalls are deleted and both assume the failover IP addresses you configured.
D. The current IP addresses will become those of the standby PIX Firewall.

Answer: D
Explanation -
The failover feature allows you to use a standby PIX Firewall to take over the functionality of a failed PIX Firewall. When the active unit fails, it changes to the standby state, while the standby unit changes to the active state. The unit that becomes active takes over the active unit's IP addresses and MAC addresses, and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC addresses.
Reference: Cisco PIX Firewall Software - Using PIX Firewall Failover
www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278a.h

---

QUESTION 132
You are the security administrator at Certkiller Inc and you need which statement about failover is true?

A. The true statement is when configuring the PIX Firewall for failover, you must configure the primary and secondary PIX Firewalls exactly the same.
B. The true statement is the configuration replication is automatic from the active PIX Firewall to the standby PIX Firewall.
C. The true statement is the configuration can be modified on either the primary or secondary PIX Firewalls with the same results.
D. The true statement is the active PIX Firewall replicates only the failover configuration to the standby PIX Firewall.

Answer: B

Explanation:
Configuration replication occurs
When the standby firewall completes its initial bootup
As commands are entered on the active firewall
By entering the write standby command
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap13 page 6

QUESTION 133
What does it mean when the output invoked by the show failover command displays interface status waiting?

A. The active PIX Firewall is operational and the standby PIX Firewall is ready.
B. The active PIX Firewall is waiting for configuration replication to be completed.
C. Monitoring the other Pix Firewall's network interfaces has not yet stand.
D. The primary PIC Firewall has completed testing the standby PIX Firewall's interfaces and the standby PIX Firewall is waiting to take control.

Answer: C

Usage NotesThe following notes apply to the use of failover on the PIX Firewall:
1. Syslog messages indicate whether the Primary unit or Secondary unit failed. Refer to "Failover Syslog Messages" for more information.
2. If you are upgrading from a previous version, refer to "Upgrading from PIX Firewall Version 4.1 to Version 4.2" and "Upgrading from PIX Firewall Version 4.2(1) to the Current Version" before continuing.
3. The ACT indicator light on the front of the PIX 515 is on when the unit is the Active failover unit. If failover is not enabled, this light is on. If failover is present, the light is on when the unit is the Active unit and off when the unit is in standby mode.
4. The Cable Status that displays with the show failover command has these values:
(a) Normal-Indicates that the Active unit is working and that the Standby unit is ready.
(b) Waiting-Indicates that monitoring of the other unit's network interfaces has not yet started.
(c) Failed-Indicates that the PIX Firewall has failed.
5. Changes made on the Standby unit are not replicated on the Active unit.
6. Failover works by passing control to the Standby unit should the Active unit fail. For Ethernet, failover detection should occur within 30 seconds. Token Ring requires additional time for failover.
7. Failover works in a switched environment. If the unit is attached to a switch running spanning tree, this will take twice the forward delay time configured in the switch (typically 15 seconds) plus 30 seconds. This is because at bootup (and immediately following a failover event) the network switch will detect a temporary bridge loop.

QUESTION 134
With failover, how do you save the active pix running configuration to the startup configuration of the standby pix?

A. write standby
B. write standby run
C. write standby startup
D. write standby failover

Answer: A

Explanation:
The write standby command when issued from the active pix, will save the running configuration of the active pix to the startup configuration (flash memory) of the standby pix.

QUESTION 135
What is the default failover hello timer interval between two pix's?

A. 3 seconds
B. 5 seconds
C. 12 seconds
D. 15 seconds
E. 20 seconds

Answer: D

Explanation:
When two pix's are configured for failover, by default they will send out a hello protocol every 15 seconds on the failover link to maintain connectivity. If two successive hello packets are not responded to, the pix will attempt to determine if the other pix has failed.

QUESTION 136
The team at Certkiller Inc. is working on the Firewall redundancy.
Which is likely to prevent serial-cable failover from working? (Choose two)

A. The problem is the hardware models are the same.
B. The problem is the two PIX Firewalls are running different version of the software.
C. The problem is the secondary PIX Firewall has not been properly configured as a secondary PIX Firewall.
D. The problem is the secondary PIX Firewall has a 3DES license.
E. The problem is the standby PIX Firewall has not yet replicated its configuration to the primary PIX Firewall.
F. The problem is the hardware models are different.

Answer: B, F

Explanation: -
Failover System Requirements
Identical PIX Firewall hardware and software versions
Description
The failover feature requires two units that are identical in the following respects:
Model (a PIX 515E cannot be used with a PIX 515)
Same number and type of interfaces
Software version
Activation key type (DES or 3DES)
Flash memory
Amount of RAM
Reference: Cisco PIX Firewall Software - Using PIX Firewall Failover
www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278a.h

---

QUESTION 137
Kathy the security administrator at Certkiller Inc. is having problems with failover on the PIX Firewall. Which is likely to cause standard failover via the special serial cable not to work? (Choose two)

A. The problem is the hardware models are the same.
B. The problem is the two PIX Firewalls are running different versions of software.
C. The problem is the secondary PIX Firewall has not been properly configured as a secondary PIX Firewall.
D. The problem is the secondary PIX Firewall has a 3DES license.

E. The problem is the standby PIX Firewall has not yet replicated its configuration to the primary PIX Firewall.
F. The problem is the hardware models are different.

Answer: B, F

Explanation: Failover System Requirements
Identical PIX Firewall hardware and software versions
Description
The failover feature requires two units that are identical in the following respects:
Model (a PIX 515E cannot be used with a PIX 515)
Same number and type of interfaces
Software version
Activation key type (DES or 3DES)
Flash memory
Amount of RAM
Reference: Cisco PIX Firewall Software - Using PIX Firewall Failover
www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278a.h

---

QUESTION 138
How do you configure the hello timer interval used between two pix's that have failover enabled?

A. failover interval link
B. failover timer
C. failover hello
D. failover poll

Answer: D

Explanation:
The failover poll (seconds) command sets the interval at which the pix sends packets to its failover neighbor to determine if it is still up.

QUESTION 139
Which of the following commands enables failover on a pix?

A. failover enable
B. failover enabled
C. failover active
D. failover

Answer: D

Explanation:
Enter the failover command to turn the failover process on, on a pix.

QUESTION 140
What command displays the active or standby status of a pix configured for failover?

A. show failover
B. show failover poll
C. show failover status
D. show failover link

Answer: A

Explanation:
The show failover command will list failover parameters for the pix, such as whether it is the active pix or the standby pix.

QUESTION 141
Which of the following commands correctly configures a pix interface for Stateful failover?

A. failover ip address 192.168.10.1
B. failover interface (dmz1)
C. failover lan (dmz1)
D. failover link (dmz1)

Answer: D

Explanation:
The failover link (interface name) command enables that pix interface for Stateful failover.

QUESTION 142
The LAN-based failover Kathy configured does not work.
Kathy's boss Jack, at Certkiller Inc. demands an explanation regarding why the error occurred. What should you tell her. (Choose two reasons)

A. You tell her you did not set a failover IP address.
B. You tell her you used a crossover Ethernet cable between the two PIX Firewalls.
C. You tell her you used a hub for failover operation.
D. You tell her you used a switch for failover operation.
E. You tell her you used a dedicated VLAN for failover operation.
F. You tell her you did not use a crossover Ethernet cable between the two PIX Firewalls.

Answer: A, B

Explanation: You must set an Failover IP address for LAN-based failover.
Ethernet connection ("LAN-based failover")-You can use any unused Ethernet interface on the device. If the units are further than six feet apart, use this method. We recommend that you connect this link through a dedicated switch. You cannot use a crossover Ethernet cable to link the units directly.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/failover.pdf

---

QUESTION 143
You are the new administrator at Certkiller Inc. and you want to know how are LAN-based failover and serial failover alike?

A. They are alike because both require that all configuration is performed on the primary PIX Firewall.
B. They are alike because both require the use of a special serial cable.
C. They are alike because they are configured with the same command set.
D. They are alike because both provide stateful failover.
E. They are alike because both require two dedicated interfaces: one for configuration replication and another for stateful failover.

Answer: D

Explanation: The same LAN interface used for LAN-based failover can also be used for Stateful failover.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 13 page 21

QUESTION 144
With what pix os version is LAN Based Failover (LBF) available?

A. 6.0
B. 6.1
C. 6.2
D. 6.3

Answer: C

Explanation:
LAN Based Failover (LBF) is available on pix os version 6.2, and allows failover to be done through ethernet interfaces on the two pix instead of using the 115kbps serial interfaces.

QUESTION 145
Which of the following commands configures a pix interface for LAN Based Failover?

A. failover interface (dmz2)
B. failover lan interface (dmz2)
C. failover lan based (dmz2)
D. failover lan link (dmz2)

Answer: B

Explanation:
The pix command failover lan interface (interface name) enables an ethernet interface to be used for LAN Based Failover instead of using the serial failover interface.

QUESTION 146
Kathy is the security administrator at Certkiller Inc. and she is configuring VPN.
Why should Kathy use ESP security protocol rather than the AH security protocol when creating a VPN with IPSec?

A. Because ESP provides data confidentiality and AH does not.
B. Because ESP provides anti-replay and AH does not.
C. Because ESP provides data integrity and AH does not.
D. Because ESP provides data origin authentication and AH does not.

Answer: A

Explanation: Authentication Header (AH) - A security protocol that provides authentication and optional REPLAY-DETECTION services...AH does NOT provide data encryption and decryption services.
Encapsulating Security Payload (ESP) - Security protocol that provides DATA CONFIDENTIALITY and protection with optional authentication and replay-detection services. The PIX firewall uses ESP to encrypt the data payload of IP packets
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 14 pages 7 and 8

QUESTION 147
The newly appointed Certkiller trainee technician wants to know which of the following is a hybrid protocol that provides utility services for IPSec, including authentication of the IPSec peers, negotiation of IKE and IPSec SAs, and establishment of keys for encryption algorithms. What will your reply be?

A. 3DES
B. ESP
C. IKE
D. MD5

Answer: C

Explanation:
IKE is a hybrid protocol that provides utility services for IPSec: authentication of the

IPSec peers, negotiation of IKE and IPSec security associations (SAs), and establishment of keys for encryption algorithms used by IPSec. IKE is synonymous with Internet Security Association Key Management Protocol (ISAKMP) in PIX Firewall configuration.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.15-43

QUESTION 148
Which of the following statements regarding AH and ESP security protocols is valid?

A. Each can be used alone or in conjunction with other.
B. They must be used together for the desired effect.
C. You must choose one or the other.
They cannot be used together.
D. You need to use both when you need data encryption, data authentication, and replay-detection.

Answer: A

Explanation:
The ESP security protocol (Encapsulating Security Protocol) provides confidentiality via encryption, data origin authentication, data integrity and optional antireplay services. So D is clearly wrong since ESP provides all this services. AH and ESP can be used in conjunction with each other or alone so that leaves us with A.

QUESTION 149
What protocol does ESP use?

A. 35
B. 50
C. 65
D. 80

Answer: B

Explanation:
Encapsulating Security Payload (ESP) is used with IPSEC VPN's to encrypt and optionally authenticate data. It uses protocol number 50.

QUESTION 150
What encryption algorithm does a pix use by default for ipsec vpn's?

A. aes
B. md5
C. des
D. esp

E. 3des

Answer: C

Explanation:
The default policy suite encryption algorithm on a pix is Data Encryption Standard (DES).

QUESTION 151
What protocol does AH use

A. 17
B. 51
C. 79
D. 82

Answer: B

Explanation:
Authentication Header (AH) is an IPSEC protocol used to authenticate packets from a source. It does not provide encryption and cannot be used with NAT. It uses protocol number 51.

QUESTION 152
Which of the following establishes the first security association (SA) between two vpn peers?

A. esp
B. ike
C. ah
D. ipsec
E. rsa

Answer: B

Explanation:
IKE is the protocol that authenticates a peer and establishes the first security association with that peer.

QUESTION 153
What is the bit length of the SHA-1 HMAC?

A. 128 bit
B. 160 bit
C. 192 bit
D. 220 bit

Answer: B

Explanation:
SHA-1 HMAC produces 160-bit fixed length hash outputs. The other IPSEC HMAC, MD5, produces 128-bit fixed length hash outputs.

QUESTION 154
The security team at Certkiller Inc is working on the IKE Phase 1 policy parameters.
Which are IKE Phase 1 policy parameters? (Choose three)

A. IKE Phase 1 policy parameters are Key exchange
B. IKE Phase 1 policy parameters are Transform set
C. IKE Phase 1 policy parameters are Encryption algorithm
D. IKE Phase 1 policy parameters are IP addresses of IPSec peer
E. IKE Phase 1 policy parameters are Hash algorithm
F. IKE Phase 1 policy parameters are Hostname of IPSec peer

Answer: A, C, E

Explanation: Ike Phase One policy Parameters
Encryption Algorithm
Hash algorithm
Authentication methodR
Key exchange
Ike SA lifetime
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 14 page 14

QUESTION 155
Which of the following represents IKE Phase 1 policy parameters? Choose three.

A. transform set
B. key exchange
C. hostname of IPSec peer
D. hash algorithm
E. encryption algorithm
F. IP addresses of IPSec peer

Answer: B, D, E

Explanation:
The basic purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges. IKE phase 1 performs the following functions:
Authenticates and protects the identities of the IPSec peers
Negotiates a matching IKE SA policy between peers to protect the IKE exchange

Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
Sets up a secure tunnel to negotiate IKE phase 2 parameters
So encryption algorithm, hash algorithm and key exchange are the right answers

---

QUESTION 156
Which of the following can authenticate IPSEC VPN packets? Choose all that apply.

A. DES
B. ESP
C. AH
D. CA

Answer: B,C

Explanation:
ESP and AH can be used to authenticate IPSEC packets using MD5 and SHA-1 HMAC's.

QUESTION 157
Which command will you advice the newly appointed Certkiller trainee technician to use to enable IKE on the outside interface?

A. The ike enable outside command
B. The ipsec enable outside command
C. The isakmp enable outside command
D. The ikeenable (outbound) command

Answer: C
PIX FW Advanced, Cisco Press, p. 502

QUESTION 158
Which of the following is entered into a transform set?

A. rsa sig
B. preshared keys
C. esp
D. ike

Answer: C

Explanation:
Configure transforms sets using encryption algorithms and authentication protocols for ESP and AH.

QUESTION 159
Which of the following commands turns on the isakmp process for a pix interface?

A. crypto isakmp
B. isakmp enable
C. crypto isakmp enable
D. isakmp crypto enable

Answer: B

Explanation:
The pix firewall command to enable isakmp on an interface for vpn configuration is isakmp enable (interface name).

QUESTION 160
What is the default authentication method used on a pix firewall for IKE?

A. RSA Signatures
B. RSA encrypted nonces
C. Pre-shared keys
D. Message Digest 5

Answer: A

Explanation:
By default the pix firewall will use RSA Signatures during IKE phase 1 for peer authentication. RSA Signatures sign a digital certificate for authentication.

QUESTION 161
Jason the security administrator at Certkiller Inc. is working on transform set. Which command correctly specifies a transform set for a crypto map?

A. isakmp policy 10 hash sha
B. transform-set pix2 set crypto map MYMAP
C. crypto map peer2 10 set transform-set pix2
D. crypto-map policy 10 set 192.168.7.2
E. crypto map peer7 10 set peer 192.168.7.2
F. crypto transform peer2 10 set transform-set pix2

Answer: C

Explanation:
Specify which transform sets are allowed for this crypto map entry.
Pixfirewall(config)# crypto map map-name seg-num set tansform-set transform-set-name
Pixfirewall(config)# crypto map MYMAP 10 set transform-set pix6
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap14 page 28

QUESTION 162
Kathy the security administrator at Certkiller Inc. is configuring a crypto map, which command correctly specified the peer to which IPSec-protected traffic can be forwarded?

A. The answer is crypto map set peer 192.168.7.2
B. The answer is crypto map 20 set-peer insidehost
C. The answer is crypto map peer7 10 set peer 192.168.7.2
D. The answer is crypto-map policy 10 set 192.168.7.2

Answer: C

Explanation:
Specify the peer to which the IPSec protected traffic can be forwarded.
Pixfirewall(config)#crypto map map-name seq-num set peer hostname|ip address
Pixfirewall)config)#crypto map MYMAP 10 set peer 192.168.6.2
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 14 page 28

QUESTION 163
You are the network technician for Certkiller .com. You have been instructed to create a site-to-site VPN by making use of IPSec between two PIX Firewalls. Which of the following steps can be regarded as optional when configuring the crypto maps on the firewalls?

A. Create a crypto map entry identifying the crypto map with a unique crypto map name and sequence number.
B. Specify which transform sets are allowed for this crypto map entry.
C. Specify a dynamic crypto map to act as a policy template where the missing parameters are later dynamically configured to match a peer's requirements.
D. Assign an ACL to the crypto map entry.
E. Specify the peer to which IPSec-protected traffic can be forwarded.

Answer: C

Explanation:
A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a remote peer's requirements. This allows remote peers to exchange IPSec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all of the remote peer's requirements.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.15-43

QUESTION 164
What is the function of the deny option in a crypto ACL?

A. It is to instruct the PIX Firewall to deny certain outbound traffic.

B. It is to cause all IP traffic that matches the specified conditions to be protected by crypto.
C. It is to prevent traffic from being protected by IPSec in the context of that particular crypto map entry.
D. It is to specify which IP packet types to encrypt.

Answer: C

QUESTION 165
What do you apply a crypto map to?

A. esp
B. group-object
C. transform set
D. interface

Answer: D

Explanation:
A crypto map needs to be applied to an interface on the pix to allow all ipsec configured crypto map parameters to go into effect.

QUESTION 166
Which of the following is a valid pix transform set? Choose all that apply.

A. crypto isakmp transform-set tunnel esp-des
B. crypto isakmp transform-set tunnel ah-sha-hmac esp-des
C. crypto ipsec transform-set tunnel esp-3des ah-md5-hmac
D. crypto ipsec transform-set tunnel ah-sha-hmac

Answer: C,D

Explanation:
To configure a transform set on the pix, use the crypto ipsec transform-set (name) command, followed by the AH (md5, sha-1) and ESP(des, 3des, aes) transforms you wish to use.

QUESTION 167
Which of the following pix commands displays the default isakmp policy suite parameters?

A. show crypto isakmp
B. show crypto policy
C. show ipsec isakmp
D. show isakmp policy

Answer: D

Explanation:
Issuing a show isakmp policy command on a pix will display all configured policies, as well as the default policy the pix will use if none of the isakmp values are adjusted when a new policy is created.

QUESTION 168
John the security administrator at Certkiller Inc. is working on pre-shared keys. If John configures a VPN between a Cisco VPN Client and the PIX Firewall using pre-shared keys for authentication, which should John do? (Choose two)

A. John should use pre-shared keys for authentication.
B. John should use digital certificates for authentication instead of pre-shared keys.
C. John should ensure that the password on the VPN client matches the vpngroup password on the PIX Firewall.
D. John should not use digital certificates for authentication.
E. John should ensure that the group name on the VPN Client matches the vpngroup name on the PIX Firewall.
F. John should ensure that the group name differs from the VPN group name on the PIX Firewall.

Answer: C, E

Explanation: If you are use pre-share keys for authentication, make sure that the group name (training, in this case) matches the VPN group name on the PIX firewall, and that the password (the pre-share key) matches the VPN group password. You can use digital certificates for authentication instead of pre-share keys.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 14 page 44

QUESTION 169
What type of network infrastructure device issues digital certificates?

A. SCEP
B. ACS
C. SA
D. CA

Answer: D

Explanation:
A Certificate Authority (CA) takes requests for X.509 digital certificates, creates, signs, and sends the certificate to the requesting host. The host will then use it for authentication purposes during the IKE IPSEC SA.

QUESTION 170
Which of the following protocols can a pix firewall use to automatically install a digital certificate?

A. IKE
B. Diffie Hellman
C. ACS
D. SCEP

Answer: D

Explanation:
The Simplified Certificate Enrollment Protocol (SCEP) allows a device to automatically enroll with a Certificate Authority (CA) to request, receive, and install a digital certificate.

QUESTION 171
The security team at Certkiller Inc. is looking for the truth about the PIX firewall. Which statement about the PIX Firewall is true?

A. The true statement is the PIX Firewall passes RIP updates between interfaces.
B. The true statement is the PIX Firewall uses the dynamically learned routes to forward traffic to the appropriate destinations but does not propagate learned routes to other devices.
C. The true statement is you cannot configure the PIX Firewall to learn routes dynamically from RIP version 1 or RIP version 2 broadcasts.
D. The true statement is the PIX Firewall uses dynamically learned routes to forward traffic to the appropriate destinations, passes RIP updates between its interfaces, and propagates learned routes to other devices.

Answer: B

Explanation: You can configure the PIX Firewall to learn routes dynamically from RIP version 1 or RIP version 2 broadcasts. Although the PIX firewall uses the dynamically learned routes itself to forward traffic to the appropriate destinations, it does not propagate learned routes to other devices. The Pix firewall cannot pass RIP updates between interfaces. It can, however, advertise one of its interfaces as a default route.
Reference: Cisco Secure PIX Firewall Advanced 3.1 9-5

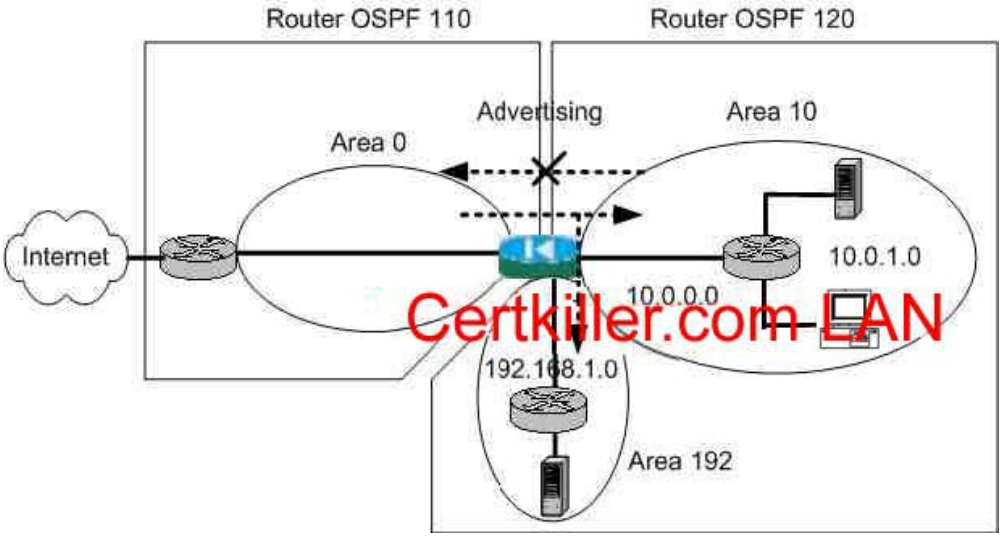
QUESTION 172
What is the default state for passing LSA 3 advertisements after configuring a PIX Firewall to run two OSPF processes?

A. LSA 3 advertisements can not pass between processes or areas.
B. LSA 3 advertisements can pass between processes, but not between areas within a

process.
C. LSA 3 advertisements can pas between processes and areas.
D. LSA 3 advertisements can pass between areas within a process, but not between processes.

Answer: D
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.13-23

QUESTION 173



In the above illustration of a network, a customer configured two OSPF processes: one for the public network and one for the private network. The customer wants to forward LSA3 advertisements from the public OSPF process to the private process, but not the reverse.
Which of the following commands should the administrator enter?

A. pix1(config)# router ospf 120
pix1(config-router)# redistribute ospf 110
B. pix1(config)# router ospf 120
pix1(config-router)# area 120 filter-list prefix ten out
pix1(config)# pre-fix-list ten deny 10.0.0.0/16
pix1(config)# pre-fix-list-ten deny 192.168.1.0/24
pix1(config)# pre-fix-list ten permit 172.16.6.0/24
C. pix1(config)# router ospf 110
px1(config-router)# redistribute ospf 120
D. pix1(config)# router ospf 110
pix1(config-router)# area 110 filter-list prefix ten in
pix1(conig)# pre-fix-list ten deny 10.0.0.0/16
pix1(config)# pre-fix list ten deny 192.168.1.0/24
pix1(config)# pre-fix-list ten permit 172.16.6.0/24

Answer: A
CSPFA Student Guide V3.2 P 13-25

QUESTION 174
How do you enter a default ip route on a pix?

A. ip route 0.0.0.0 0.0.0.0 192.168.10.1
B. route 0.0.0.0 0.0.0.0 192.168.10.1
C. set route 0.0.0.0 0.0.0.0 192.168.10.1
D. default route 0.0.0.0 0.0.0.0 192.168.10.1

Answer: B

Explanation:
Create a static route such as a default route on the pix with the route command.

QUESTION 175
Choose all of the interior gateway routing protocols the pix supports.

A. rip
B. rip2
C. isis
D. ospf
E. igrp
F. eigrp

Answer: A,B, D

Explanation:
A pix firewall only has support for rip and rip2 routing protocols.

QUESTION 176
James the security administrator for Certkiller Inc. is working on Telnet to PIX firewall.
Which statement about Telnet and the PIX Firewall is true?

A. The true statement is you can enable Telnet on all interfaces except the outside interface.
B. The true statement is you can enable Telnet on all interfaces, but the PIX Firewall requires that all Telnet traffic to the outside interface be IPSec protected.
C. The true statement is you can enable Telnet on all interfaces, but the PIX Firewall requires that all Telnet traffic to all interfaces be IPSec protected.
D. The true statement is Telnet connections to the PIX Firewall are not permitted.

Answer: B

Explanation: You can enable telnet to the PIX firewall on all interfaces. However, the PIX Firewall requires that all telnet traffic to the outside interface be IPSec

protected.
Reference: Cisco Secure PIX Firewall Advanced 3.1 15-3

QUESTION 177
Johnthe security administrator at Certkiller Inc. wants to know what the purpose is of the who command.

A. The purpose is to enable you to view which IP addresses are currently accessing the PIX Firewall console via SSH.
B. The purpose is to remove Telnet access from a previously authorized IP address.
C. The purpose is to enable you to view who is currently accessing the PIX Firewall Device Manager console from a browser.
D. The purpose is to enable you to view which IP addresses are currently accessing the PIX Firewall console via Telnet.

Answer: D

Explanation: Who - Enables you to view which IP address are currently accessing the PIX firewall console via telnet.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 15 page5

QUESTION 178
James the security administrator at Certkiller Inc. needs to know the purpose of the command ip local pool MYPOOL 10.0.0.20-10.0.0.29.

A. The purpose is to designate a pool of IP addresses for NAT.
B. The purpose is to designate a pool of IP addresses that will dynamically be assigned to PPPoE clients.
C. The purpose is to designate a pool of IP addresses that will be dynamically assigned to VPN clients via IKE mode.
D. The purpose is to designate a pool of IP addresses that will be dynamically assigned to DHCP clients.

Answer: C

Explanation: Creates a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients. The address range of this pool of local addresses must not overlap with any command statement that lets you specify an IP address.
Reference: http://www.cisco.com/en/US/partner/products/sw/secursw/ps2120/products_command_reference_chapter09186a

---

QUESTION 179
You have just purchased a PIX firewall and your PIX Firewall is displaying a dot (.) on the console before the SSH user authentication appears, as pixfirewall(config)#.
Why?

A. The dot means the PIX Firewall's CPU utilization is high.
B. The dot means the PIX Firewall is frozen and must be reloaded.
C. The dot means the generation of the server key is failing.
D. The dot means the dot is a progress indicator that verifies that the PIX Firewall is busy and has not frozen.

Answer: D

Explanation:
The display of the dot does not affect the functionality of SSH. The dot appears at the console when generating a server key or decrypting a message using private keys during ssh key exchange before user authentication occurs. These task can take up to two minutes or longer. The dot is a progress indicator that verifies that the PIX Firewall is busy and has not hung.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap15 page 10

QUESTION 180
Which of the following statements regarding SSH and the PIX Firewall are valid? Choose three.

A. You must generate an RSA key-pair for the PIX Firewall before SSH clients can connect to the PIX Firewall console.
B. You can use either an SSH version 1 or 2 client because the two versions are essentially the same and are entirely compatible.
C. The PIX Firewall supports the SSH remote functionality as provided in SSH version.1.
D. You must upgrade you DES activation key to 3DES.
E. The PIX Firewall allows up to 5 SSH clients to simultaneously access its console.
F. The PIX Firewall does not support SSH remote functionality as provided in SSH version 1.

Answer: A, C, E

Explanation:
The PIX Firewall supports the SSH remote functionality, as provided in SSH version 1, which provides strong authentication and encryption capabilities. SSH, an application running on top of reliable transport layer such as TCP, supports logging onto another computer over a network, executing command remotely, and moving files from one host to another.
Both ends of an SSH connection are authenticated, and passwords are protected by being encrypted. Since SSH uses RSA public key cryptography, an Internet encryption and authentication system, you must generate an RSA key pair for the PIX Firewall before clients can connect to the PIX Firewall console.
The PIX Firewall allows up to five SSH clients to simultaneously access its console.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.17-7

QUESTION 181
Which of the following combinations of username and password will establish an SSH connection to your PIX Firewall?

A. username pix, current enable password
B. username pixfirewall, password attack
C. username pixfirewal, password aaapass
D. username pix, current Telnet password

Answer: D

Explanation:
To establish an SSH connection to your PIX Firewall console, enter the username pix ans the Telnet password at the SSH client. When starting an SSH session, the PIX Firewall displays a dot (.) on the console before the SSH user authentication propt appears.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.17-10

QUESTION 182
What command reassigns a specific command to a different privilege level?

A. privilege
B. command auth
C. level-priv
D. ourpriv

Answer: A

Explanation:
To assign commands to privilege levels, use the privilege command. Replace the level argument with the privilege level, and replace the command argument with the command you want to assign to the specified level You can use the show, clear, or configure parameter to oprionally set the privilege level for the show, clear, or configure command modifiers of the specified command. The privilege command can be removed by using the no keyword.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.17-6

QUESTION 183
You made use of the privilege command to set privilege levels for PIX Firewall commands. How can an administrator be prevented from gaining access to a particular privilege level?

A. From the # prompt, enter the privilege command with a privilege-level designation; when prompted, enter the user name for that level.
B. From the > prompt, enter the login command with a privilege-level designation, when prompted enter the password.
C. From the # prompt, enter the privilege command with a privilege-level designation;

when prompted, enter the password for that level.
D. From the > prompt, enter the enable command with a privilege-level designation, when prompted, enter the password for that level.

Answer: D

Explanation:
The PIX Firewall has four administrative access modes:
1. Unprivileged mode à pix>
2. Privileged mode à pix#
3. Configuration mode à pix<config>#
4. Monitor mode à monitor>
Upon first accessing a PIX Firewall, the admin is presented with pix> prompt. This is the unprivileged mode.
To gain access to particular privileged level, enter enable [priv_level]
[priv_level] à The Privileged level, from 0 to 15
Privileged mode - This mode displays the # prompt and enable the user to change the current settings.

QUESTION 184
What command reassigns a specific command to a different privilege level?

A. privilege
B. command auth
C. level-priv
D. ourpriv

Answer: A

Explanation:
The privilege command sets user-defined privilege levels for PIXFirewall commands. This is especially useful for setting different privilege levels for related configuration, show, and clear commands. However, be sure to verify privilege level changes in your commands with your security policies before implementing the new privilege levels.
When commands have privilege levels set, and users have privilege levels set, then the two are compared to determine if a given user can execute a given command. If the user's privilege level is lower than the privilege level of the command, the user is prevented from executing the command. This is modeled after Cisco IOS software.
To change between privilege levels, use the login command to access

---

QUESTION 185
If you telnet into a pix, by default what period of idle time will pass before the pix will terminate the connection?

A. 5 minutes
B. 10 minutes

C. 15 minutes
D. 20 minutes

Answer: A

Explanation:
The pix will terminate telnet and ssh connections into the pix after 5 minutes of link idle time by default.

QUESTION 186
Which of the following are valid ways to connect to a pix firewall? Choose all that apply.

A. tftp
B. telnet
C. ssh
D. icmp

Answer: B,C

Explanation:
You can connect remotely to your pix in clear text with telnet, or connect with a secure encrypted tunnel with ssh.

QUESTION 187
When you connect remotely to a pix using ssh, what is the username you should enter when prompted?

A. cisco
B. user
C. pix
D. firewall
E. admin

Answer: C

Explanation:
For Secure Shell (SSH) connections to the pix, use the username pix and the ssh password.

QUESTION 188
Help Johnfrom the security department at Certkiller Inc find out which statement about authorization and the PIX Firewall is true.

A. The true statement is the PIX Firewall does not support per-user authorization.
B. The true statement is the PIX Firewall does not support TACACS+ authorization.

C. The true statement is the PIX Firewall supports downloadable ACLs using TACACS+.
D. The true statement is the PIX Firewall supports downloadable ACLs using RADIUS.

Answer: D

Explanation: Note- Downloadable ACLs are supported with Radius only. They are not supported with TACACS+. -
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 12 page 38

QUESTION 189
The administrator at Certkiller Inc. needs to know the command to enables command authorization. What is the command to enable command authorization.

A. aaa authorization command LOCAL
B. aaa authorization permit any LOCAL
C. level-priv
D. passwd

Answer: A

Explanation: Aaa authorization command local - enables command authorization (use it's own local database).
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 15 page 24

QUESTION 190
James the security administrator at Certkiller is working on PDM. He needs to know which operating systems the PDM runs on. (Choose the best answer?)

A. PDM runs on Windows, Linux, and Sun Solaris
B. PDM runs on Windows, Macintosh, and Linux
C. PDM runs on Windows and Sun Solaris
D. PDM runs on Windows and Linux

Answer: A

Explanation: PDM can operate in browsers running on Windows, SUN, Solaris, or Linux operating systems.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 16 page 9

QUESTION 191
Which of the following transform sets are pre-defined by PDM? Choose two.

A. AH-SHA-HMAC
B. ESP-DES-MD5
C. AH-MD5_HAMAC

D. AH-DES-MD5
E. nat 0 match acl
F. ESP-3DES-SHA

Answer: A, B
AH come with SHA OR MD5 only
Not D: There is nothing called AH-DES-MD5.

QUESTION 192
What minimum pix os version must be running to conduct pix configuration via PDM?

A. 5.9
B. 6.0
C. 6.1
D. 6.2

Answer: B

Explanation:
Starting in pix os 6.0 you can configure the pix through a web browser gui called the Pix Device Manager (PDM).

QUESTION 193
What is the maximum number of users that can be logged into a pix via PDM?

A. 1
B. 2
C. 4
D. 5
E. 12

Answer: D

Explanation:
A pix can have up to 5 different users logged into it via PDM.

QUESTION 194
What is the minimum amount of flash memory needed on a pix to run PDM?

A. 2mb
B. 4mb
C. 8mb
D. 16mb
E. 32mb

Answer: C

Explanation:
To install the PDM file into your pix flash memory, your pix must have at least 8 megs of flash.

QUESTION 195
What is the highest PDM version you can use with pix os version 6.0?

A. 1.0
B. 1.1
C. 2.0
D. 2.1

Answer: B

Explanation:
Pix os versions 6.1 and below can run PDM 1.1. To run PIX
PDM 2.0, you must have pix os 6.2 or higher.

QUESTION 196
You are the administrator at Certkiller Inc and you installed PDM on a PIX Firewall with an existing configuration. You notice that you have access only to the monitoring tab. What is the most likely cause of this problem?

A. The problem is you are running PDM on a software image earlier than 6.0.
B. The problem is you have not specified the host or network authorized to initiate an HTTP connection to the PIX Firewall.
C. The problem is you have a command in your configuration that PDM does not support.
D. The problem is you installed a corrupt pdmxx.bin file.

Answer: C

Explanation: PDM works with PIX firewall software versions 6.0 and higher and comes preloaded into flash memory on new PIX firewalls running software versions 6 and higher.
-Cisco Secure PIX Firewall Advanced 3.1 chap 16 page 5
There are certain commands that PDM does not support in a configuration. IF these commands are present in your configuration, you will only have access to the monitoring tab.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 16 page 12

QUESTION 197
When connecting to a pix firewall PDM, what username is used?

A. pix
B. admin
C. cisco
D. (none)

Answer: D

Explanation:
Pix PDM connections prompt for a username and password. The username field is left blank, and the enable password is used as the password.

QUESTION 198
Which of the following are PDM main tabs? Choose 3.

A. hosts/networks
B. administration
C. update server
D. vpn
E. monitoring

Answer: A,D,E

Explanation:
The Pix Device Manager (PDM) GUI has 6 tabs. Access rules, translation rules, vpn, hosts/networks, monitoring, and system properties.

QUESTION 199
Which of the following are some CA vendors the pix firewall supports? Choose all that apply.

A. Microsoft
B. Baltimore tech
C. Digital FXS
D. Secure E-systems

Answer: A,B

Explanation:
The pix supports the following Certificate Authority (CA) vendors: Microsoft, Verisign, Baltimore Tech, and Entrust.

QUESTION 200
When using PDM to configure a site-to-site vpn, what pix interface will the vpn terminate on, by default?

A. inside

B. outside
C. dmz1
D. dmz2

Answer: B

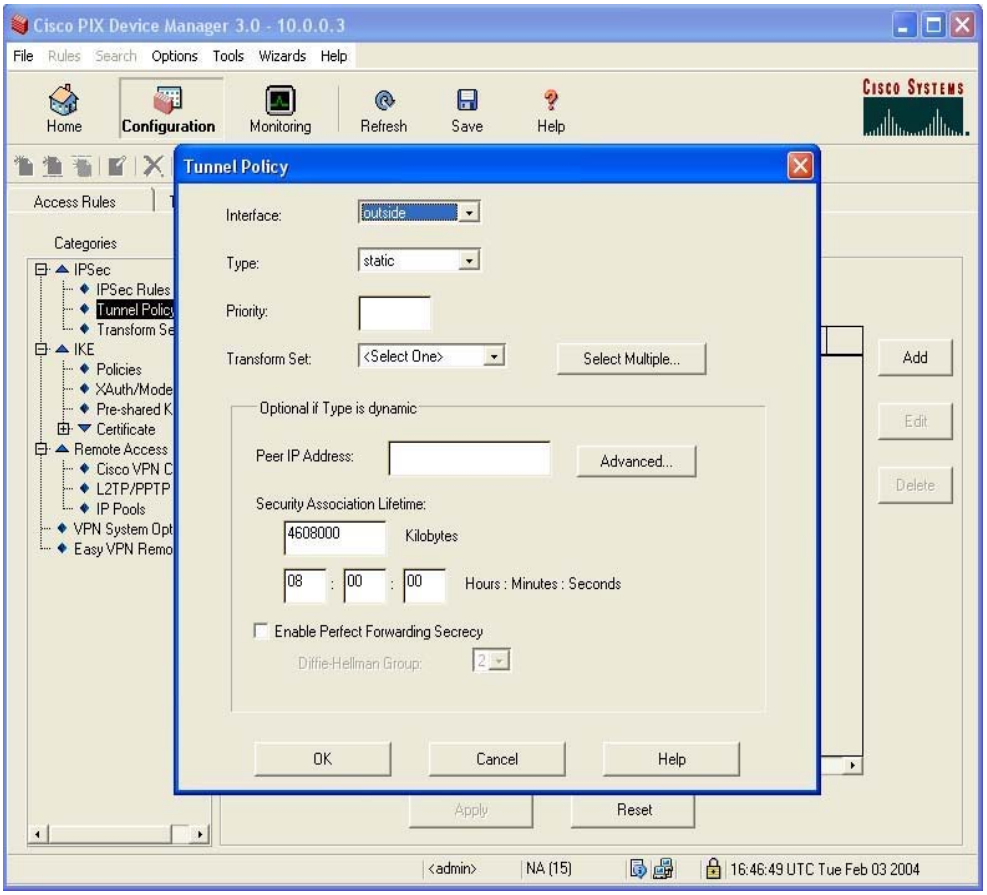
Explanation:
A PDM created vpn is terminated on the outside interface by default for both site-to-site and remote access vpn's.

QUESTION 201
Kathy the security administrator at Certkiller Inc. is working on creating VPN's. Which two of these statements about creating VPNs in PDM are true? (Choose two)

A. The true statement is when the inactivity timeout for all IPSec SAs have expired for a given VPN Client, the tunnel is established.
B. The true statement is PDM hides the concept of crypto map.
C. The true statement is PDM supports tunnel polices that are not bound to an interface.
D. The true statement is to create a crypto map, select crypto maps from the IPSec branch of the categories tree.
E. The true statement is PDM does not support tunnel polices that are not bound to an interface.You must select an interface for a tunnel policy when you create it.
F. The true statement is after you create a tunnel policy in the VPN tab's tunnel policy window, you must bind it to an interface from the Access Rules tab.

Answer: B, E

Explanation:
D: PDM hides the concept of the crypto map. IT does not support crypto maps that are not applied to any interface.
F: Open PDM
-VPN tab
--IPSec category
---tunnel policy
----select "Add" tunnel policy
As you can see the interfaces is chosen in the Tunnel Policy window...not from the Access Rules tab (Not E)...the access rules tab is all about access lists and the PDM creates needed access list for VPN connections on its own...Again



Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 16 pages 17 and 33

QUESTION 202

Kathy the security administrator at Certkiller Inc. is looking to configure the PIX Firewall with the static command. Which statements about the static command are true? (Choose two)

A. The true statement is static take precedence over nat and globalcommand pairs.
B. The true statement is it cannot be used alone for outbound connections.
C. The true statement is the nat and globalcommand pairs take precedence over statics.
D. The true statement is if a global IP address will be used for port address translation, you should use the same global IP address for a static translation.
E. The true statement is if a global IP address will be used for PAT, you should not use the same global IP address for a static translation.
F. The true statement is if a global IP address will be used in a global pool for use with NAT, you should use the same global IP address for a static translation.

Answer: A, E

Explanation:
Net statics take precedence over use of the nat 1 0 0 and global command pair. This means that nat 1 0 0only grants outbound access to hosts not specified in the net

staticstatement.
Reference:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps2120/prod_release_note09186a008008cfdd.html

---

QUESTION 203
When the pix adds an IP address translation entry into the translation table, how long by default will that entry exist?

A. 15 minutes
B. 3 hours
C. 12 hours
D. 24 hours

Answer: B

Explanation:
IP address translations entered into the translation table will remain there by default for 3 hours.

QUESTION 204
Which of the following commands defines a group of ip addresses a host will use when translating through the pix?

A. conduit
B. nat
C. global
D. static

Answer: C

Explanation:
The global command defines an ip address or group of ip addresses that defined hosts will have their ip addresses translated to when making a connection through the pix.

QUESTION 205
What are the two URL filtering vendors the pix firewall supports?

A. Microsoft
B. KGO
C. N2H2
D. Websense

Answer: C,D

Explanation:
N2H2 and Websense are the only URL filtering server vendors the pix supports.

QUESTION 206
How many different URL filtering servers can a pix support?

A. 8
B. 12
C. 16
D. 20

Answer: C

Explanation:
A pix can be configured with up to 16 different URL filtering servers. (all servers must be the same vendor I.E. all Websense or all N2H2 servers-the pix doesn't support a combination of both.).

QUESTION 207
How do you add a url filter server to your pix firewall configuration?

A. url-filter server
B. url-server
C. url-filter
D. url-access filter

Answer: B

Explanation:
To add a URL server you use URL-SERVER command to filter traffic you use URL-FILTER command.

QUESTION 208
What command is entered on a pix to view the ASA connections table?

A. show conn
B. show connections
C. show connections table
D. show asa table

Answer: A

Explanation:
The pix show conn command will display all connections the Adaptive Security Algorithm is tracking through pix.

QUESTION 209
How do you set the pix firewall translation table timeout?

A. xlate timer
B. translation timer
C. timeout xlate
D. xlate table timeout

Answer: C

Explanation:
Adjust the time an IP address translation stays in the pix translation table by using the timeout xlate (hh:mm:ss) command. Default is 03:00:00.

QUESTION 210
Which of the following pix commands will drop all current ip address translations?

A. clear xlate
B. drop xlate
C. xlate erase
D. xlate release

Answer: A

Explanation:
The pix clear xlate command will drop all current ip address translations the pix has made, and will force the hosts to have their ip addresses retranslated.

QUESTION 211
What protocol does the PIX MC use to communicate with the PIX Firewall?

A. The protocol SSH
B. The protocol HTTP
C. The protocol HTTPS
D. The protocol SNMP

Answer: C

Explanation: Taken from the Using Management Center for PIX:
The HTTPS (SSL) feature allows you to configure rules that permit only specific hosts or networks to connect to the PIX Firewall using HTTPS. A secure connection is needed to allow a PC or workstation client running a network browser and/or PIX MC to communicate with the PIX Firewall. The rules restrict HTTPS access through a PIX Firewall interface to a specific IP address and netmask. Any HTTPS connection attempts that comply with the rules must be authenticated using a preconfigured AAA server or the enable password. Once established, Secure Sockets Layer (SSL) protocol is used to encrypt the data.

QUESTION 212
Greg the security administrator at Certkiller Inc. needs to know what default group is installed with the PIX MC.

A. The default group is the Global group
B. The default group is the Local group
C. The default group is the Default group
D. The default group is the Management group

Answer: A

Explanation: Configuration Hierarchy - The PIX MC provides a way for you to group PIX firewalls that have similar attributes, such as common rules and settings. The global group contains all groups, subgroups, and devices.
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 17 page 4

QUESTION 213
John the security administrator at Certkiller Inc. is working on the PIX MC. 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 create a file that captures information about the PIX MC.
C. To show available support options for the PIX MC.
D. To place the PIX MC in safe mode so you can troubleshoot it.

Answer: B

Explanation:
The support feature allows you to produces a file that captures the state of your entire system, which can help you troubleshoot any problems that might occur. The snapshot is of all PIX firewall setting on the network. It includes configuration settings, defined policies and administrative accounts
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap17 page 94

QUESTION 214
The Certkiller trainee technician wants to know what default HTTP port number accesses the CiscoWorks Server desktop form client browser. What will your reply be?

A. 80
B. 1471
C. 110
D. 1741

Answer: D

Explanation:
Firewall MC service definitions can contain IP protocols, TCP and UDP source and destination ports, and Internet Control Message Protocol (ICMP) message types. With a service definition, the administrator can assign a name to a protocol and related port and message type information. In the figure in the example, a service definition is given the name of CiscoWorks. CiscoWorks uses TcP transport protocol. The destination port is 1741. The source port range is from 1 to 65535.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.13-30

QUESTION 215
The new Certkiller trainee technician wants to know which component of the PIX MX selects devices or groups for configuration through the configuration tab. What will your reply be?

A. devices tab
B. object bar
C. object selector
D. activity bar
E. all of the above

Answer: C

Explanation:
Configuration settings are those settings that control individual features of a firewall device.
Configuration settings define characteristics for the device, such as interface definitions and failover settings, that are required for the device to operate on the network. When defining settings under Configuration, you specify wheather to define them for a group or device. Selecting a group allows you to define settings for all the members of that group - inheritable attributes. Selecting a device allows the administrator a device specific attributes.
Reference: CSPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.19-28

QUESTION 216
What is the maximum amount of PIX Firewalls the AUS is capable of supporting?

A. 100
B. 500
C. 750
D. 1000
E. unlimited

Answer: D

Explanation:

AUS facilitates the managing of up to one thousand firewalls. Firewalls operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM, and to pass device information and status to AUS. Using AUS also facilitates the managing of devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP) or that sit behind Network Access Translation (NAT) boundaries.

QUESTION 217
Which of the following pix commands enables the auto update server?

A. auto-update enable
B. auto-update server
C. enable auto-update
D. enable auto-update server

Answer: B

Explanation:
The pix auto update server feature allows a remote management application to push configuration changes to the pix, thus easing the administration on networks with many pix firewalls.

QUESTION 218
Johnthe security administrator at Certkiller Inc. want to know what the default port number that the PIX Firewall uses to contact the AUS.

A. The default port number is 444
B. The default port number is 443
C. The default port number is 110
D. The default port number is 25

Answer: B

Explanation: AUS uses port 443 SSL
Reference: Page 18-12 of the course manual version 3.1

QUESTION 219
The Certkiller trainee wants to know which tab will permit one to view a device summary with Aus. What will your reply be?

A. reports
B. admin
C. devices
D. assignment

Answer: C

Explanation:
Clicking on the Device tab displays the Device Summary table. The table shows all managed devices, devices that have not yet contacted AUS, or devices whose image files are not up to date. The table contains information about the devices in AUS, such as the device ID, platform family, platform type, and the last time that a device contacted AUS.

QUESTION 220
What role does the admin tab of the AUS fulfill? Choose two.

A. support tools
B. AUS database password changes
C. PIX MC and AUS communication settings
D. AUS communication settings
E. NAT settings

Answer: B, E

Explanation:
Taken from the Using Management Center for PIX:
Click the Admin tab to display options that allow you to perform AUS administrative tasks. From this tab, you can specify NAT settings if AUS is behind a NAT boundary, and you can change your AUS database password.

QUESTION 221
Which tab allows you to view device summary with AUS?

A. devices
B. resorts
C. admin
D. assignment
E. images

Answer: A

Explanation:
Clicking on the Device tab displays the Device Summary table. The table shows all managed devices, devices that have not yet contacted AUS, or devices whose image files are not up to date. The table contains information about the devices in AUS, such as the device ID, platform family, platform type, and the last time that a device contacted AUS.

QUESTION 222
Which of the following are made possible by the images tab of the AUS? Choose three.

A. To add and delete PDM images

B. To add and delete PIX Firewall configuration files
C. To delete but not add PIX Firewall configuration files
D. To add but not delete PDM images
E. To add and delete PIX Firewall software images
F. To add but not delete PIX Firewall software images

Answer: A, C, E

Explanation: PIX FW Advanced, Cisco Press, p. 767

QUESTION 223
Which of the following correctly upgrades the pix image?

A. copy ftp tftp flash
B. tftp flash copy
C. copy flash tftp
D. copy tftp flash

Answer: D

Explanation:
Upgrade your pix operating system image file from a local TFTP server with the copy tftp flash command.

QUESTION 224
Type the command that reboots the PIX Firewall.

Answer: Reload

Explanation:
Reboot and reload the configuration.
Reference:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps2120/products_command_reference_chapter09186a

---

QUESTION 225
Kathy the security administrator for Certkiller Inc. has installed a FWSM in the Catalyst 6500 switch, initialized it in the switch, configured switch VLANs, and configured the module interface, however, Kathy is unable to establish outbound connections. Kathy has checked the configuration and find that she has correctly configured the six basic commands (nameif, interface, ip address, nat, global, and route. What could be the cause of the problem?

A. Kathy needs an ACL for the outside interface.
B. Kathy has not configured a switch VLAN for the inside interface.
C. The MSFC is configured as a connected router only on the outside interface.

D. Kathy needs an ACL for the inside interface.

Answer: D

QUESTION 226
Certkiller Inc. needs a firewall that delivers at least 15 Gbps of throughput. Cost is a factor. Which would best meet your needs?

A. The best choice would be two PIX 525 or 535 Firewalls configured for failover.
B. The best choice would be multiple FWSMs for your Catalyst 6500 switch.
C. The best choice would be a PIX Firewall 535.
D. The best choice would be a FWSM for your Catalyst 6500 switch.

Answer: B

Explanation:
The Cisco FWSM is a high-performance firewall solution, providing 5 GBPS of throughput per module and scaling to 20GB of bandwidth with multiple modules in one chassis.
Reference: Cisco Secure PIX Firewall Advanced 3.1 19-3

QUESTION 227
What is the maximum number of connections the FWSM can track with the ASA?

A. 300
B. 17,000
C. 500,000
D. 4,000,000

Answer: C

Explanation:
The Cisco pix os Firewall Service Module (FWSM) blade can track up to 500,000 connections with the Adaptive Security Algorithm (ASA).

QUESTION 228
What is the maximum amount of traffic per second the FWSM blade can process?

A. 300mb
B. 1.2gb
C. 5gb
D. 9gb
E. 45gb

Answer: C

Explanation:
The FWSM blade module can process up to 5gb traffic per second.

QUESTION 229
What is the amount of flash memory the FWSM has?

A. 16mb
B. 32mb
C. 64mb
D. 128mb

Answer: D

Explanation:
The FWSM blade module comes with 128 megs of flash, and 1 gig of ram, neither of which can be upgraded.

QUESTION 230
In which way does the PDM running on the FWSM differ from PDM running on the PIX Firewall?

A. When running on the FWSM, the PDM has a Startup Wizard.
B. When running on the FWSM, the PDM has a VPN Wizard.
C. When running on the FWSM, the PDM does not have a VPN tab.
D. When running on the FWSM, the PDM does not have a System Properties tab.

Answer: C

Explanation:
Reference:
http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/prod_release_note09186a00800e21a4.html

---

QUESTION 231
To enable multicast forwarding on the PIX outside interface, which of the following commands should the administrator enter?

A. Certkiller 1(config)# multicast on outside
B. Certkiller 1(config)# enable multicast outside
C. Certkiller 1(config)# multicast enable outside
D. Certkiller 1(config)# multicast interface outside

Answer: D
Explanation
IP multicasting is actually the transmission of an IP datagram to a host group, which is a set of hosts identified by a single IP destination address.
When hosts that need to receive a multicast transmission are separated from the multicast

router by a PIX Security Appliance, configure the PIX Security Appliance to forward IGMP reports from the downstream hosts and to forward multicast transmissions from the upstream router. To allow hosts to receive multicast transmissions through the PIX Security Appliance, Use the multicast interface command to enable multicast forwarding on each interface

---

QUESTION 232
Which is possible with the FWSM for the Catalyst 6500 switch?

A. Virtual Private Networks
B. 1000 firewall interfaces
C. IDS syslog messages
D. intra-chassis stateful failover

Answer: D
Explanation
Some of FWSM Key Features are,
1. Support up to 100 firewall VLANs NOT 1000
2. High availability via intra- or interchassis statefull failover
3. VPN functionality (IPSec, PPTP,and L2TP) for packet flowing across the firwall is not supported.
4. IDS Syslog messages are not generated

QUESTION 233
Exhibit
Certkiller 1(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 192.168.0.11 eq www (hitcnt=0)
You work as an administrator at Certkiller .com. You want to add a comment about access-list aclin line 2.
What command should you use to accomplish this addition?

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

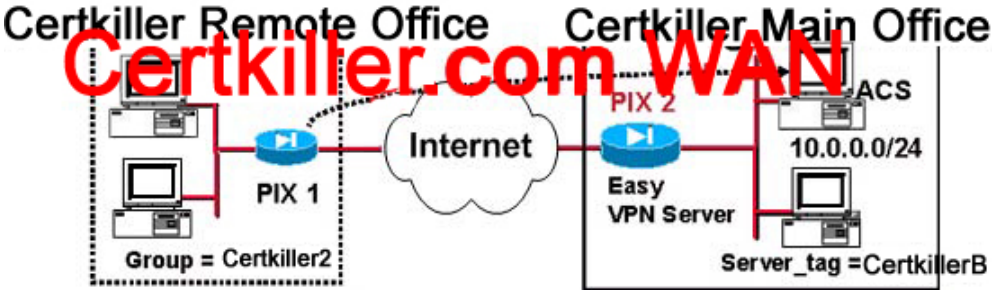
Answer: B

QUESTION 234
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
Explanation
The default polling period is 12 hours (720 Minutes).
The AUS is a web-based application that facilitates the maintenance of PIX firewalls Firewalls operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM, and to pass device information and status to AUS.

QUESTION 235
Exhibit, Network Topology



You work as a network administrator at Certkiller .com. For added security you want PCs on the inside network at the remote office to authenticate with an ACS Server, Certkiller A, at the central site before allowing these individuals PCs to access a VPN tunnel. At which location and what commands should you enter to force remote PC users to authenticate before allowing them access to a VPN tunnel? Select two.

A. vpngroup Certkiller 2 user-authentication
vpngroup Certkiller 2 authentication-server Certkiller B
B. configure at PIX1
C. configure at PIX2
D. vpngroup Certkiller 2 authentication-authentication Certkiller B
E. vpngroup Certkiller 2 mode network-extension-mode
vpngroup Certkiller 2 authentication-server Certkiller B

Answer: A, C

QUESTION 236
What does the PIX Firewall license determine? Select 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 of RAM supported by the platform
E. the software image that can be installed
F. failover support

Answer: C, D, F
Explanation
The PIX Firewall license determines the level of service it provides, its functions in a network, the maximum number of interfaces, and memory it can support.
The following three basic license types are available:
1. Unrestricted-PIX Security Appliance platforms in an Unrestricted (UR) license mode allow installation and use of the maximum number of interfaces and RAM supported by the platform. The UR license supports failover.
2. Restricted-PIX Security Appliance platforms in a Restricted (R) license mode limit the number of interfaces supported and the amount of RAM available within the system. A Restricted licensed firewall does not support a redundant system for failover configurations.
3. Failover- The failover (FO) software license places the PIX Security Appliance in a failover mode for use alongside another PIX Security Appliance with an unrestricted license.

QUESTION 237
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

QUESTION 238
What command applies a blocking function to an interface receiving an attack?

A. conduit
B. ip deny
C. interface

D. shun

Answer: D
Explanation
The PIX Firewall shun feature, when combined with a Cisco IDS Sensor, allows the PIX to dynamically respond to an attacking host.
The shun command is intended for use primarily by a Cisco IDS device. The shun command applies a blocking function to an interface receiving an attack.

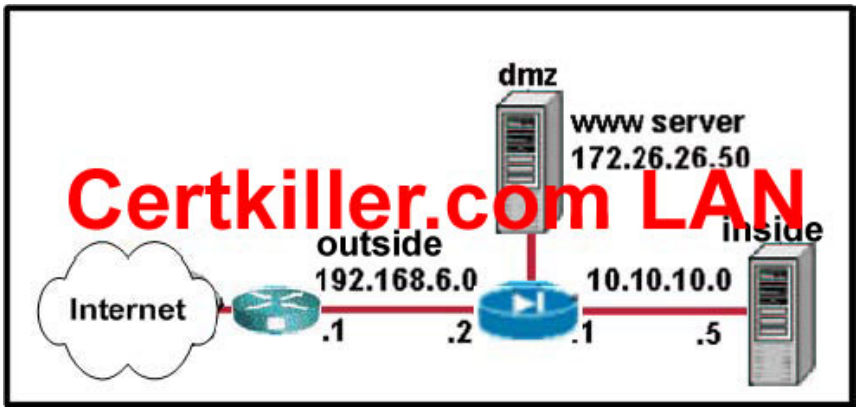
QUESTION 239
What is the maximum number of transforms in a transform set?

A. 3
B. 6
C. 9
D. 10

Answer: A
Explanation
Pix<config>#
Crypto ipsec transform-set transform-set-name transfrom1 [transfrom2 [transfrom3]]
1. Sets are limited to up to one AH and up to two ESP transforms
A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow. Each transform represents an IPSec security protocol such as ESP, AH, or both, and the algorithm used for encryption or authentication

---

QUESTION 240
Exhibit:



After reviewing the above network diagram, which command should an administrator use to map the www server on the DMZ to a static address on the outside network, 192.168.6.9?

A. Certkiller 1 (config)# static (dmz,outside) 172.26.26.50 192.168.6.9
B. Certkiller 1 (config)# static (outside,dmz) 192.168.6.9 172.26.26.50

C. Certkiller 1 (config)# static (dmz,outside) 192.168.6.9 172.26.26.50
D. Certkiller 1 (config)# static (outside,dmz) 172.26.26.50 192.168.6.9

Answer: C

QUESTION 241
Which tasks enable DHCP server support on the PIX Firewall? Choose two.

A. Specify a range of addresses for the DHCP server to distribute by using the dhcp ippool command.
B. Specify a range of addresses for the DHCP server to distribute by using the dhcpd address command.
C. Use the iphelper command to enable the PIX Firewall to pass broadcast messages between its DHCP client and DHCP server.
D. Enable the DHCP daemon within the PIX Firewall to listen for DHCP client requests on the enabled interface by using the dhcpd enable command
E. Enable the PIX Firewall to distribute IP addresses to its DHCP clients from a global pool by using the global command with the dhcp option. Specify the IP address of at least one DNS server.

Answer: B, D

QUESTION 242
You are attempting to create a protocol object group to contain a group of protocols frequently used by users on your network. You enter the command object-group protocol PROTO. What happens?

A. You get an error message
B. You get the proper syntax for the object-group command
C. You get a sub-command prompt: pixfirewall (config-protocol)#
D. You get the prompt pixfirewall(config)# access-list so that you can quickly insert the object group into an ACL

Answer: C

Explanation:
You get a sub-command prompt: pix<config-protocol>#
Explanation
object-group protocol grp_id à Assigns a name to a Service group and enables the Service sub-command mode
object-group protocol à Assigns a protocol to the protocol object group
sample:
pix<config># object-group protocol PROTO
pix<config-protocol>#object-group icmp
pix<config-protocol>#object-group tcp
Object group types

object grouping provides a way to group objects of a similar type so that a single ACL can apply to all the objects in the group. There are several types of configurable object groups available to the network administrator. They include the following:
1. Network - It is used to group client hosts, server hosts, or subnets.
2. Protocol - It is used to group protocols. It can contain one of the keywords icmp, ip, tcp, or udp, or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword ip.
3. Service - It is used to group TCP or UDP port numbers assigned to a different service.
4. ICMP type - It is used to group ICMP message types that permit or deny access.

QUESTION 243
You made use of the privilege command to set privilege levels for PIX Firewall commands. How can an administrator now gain access to a particular privilege level?
E. From the # prompt, enter the privilege command with a privilege-level designation; when prompted, enter the user name for that level.
F. From the > prompt, enter the login command with a privilege-level designation, when prompted enter the password.
G. From the # prompt, enter the privilege command with a privilege-level designation; when prompted, enter the password for that level.
H. From the > prompt, enter the enable command with a privilege-level designation, when prompted, enter the password for that level.

Answer: D

QUESTION 244
Which statement about the PIX Firewall and PPPoE is true?

A. The PIX Firewall PPPoE client cannot operate in environments where NAT is being performaed on traffic moving through a VPN.
B. The PIX Firewall PPPoE server can operate in environments where URL and content filtering is being performed before transmission to or from the outside interface.
C. The PIX Firewall PPPoE client can operate in environments where NAT is being performed on traffic to or from the outside interface
D. The PIX Firewall PPPoE server can operate in environments where application of firewall rules is being performed on traffic before transmission to or from the outside interface.

Answer: C

QUESTION 245
A user does not have to reauthenticate as you think he should. What is the easiest way to force him to reauthenticate the next time he tries to establish a connection?

A. reboot the PIX Firewall
B. use the clear uauth command

C. use the timeout uauth command
D. use the reauth command

Answer: D

QUESTION 246
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