Exam : 642-523

Title : Securing Networks with PIX and ASA

Ver : 10-16-2008

QUESTION 1:

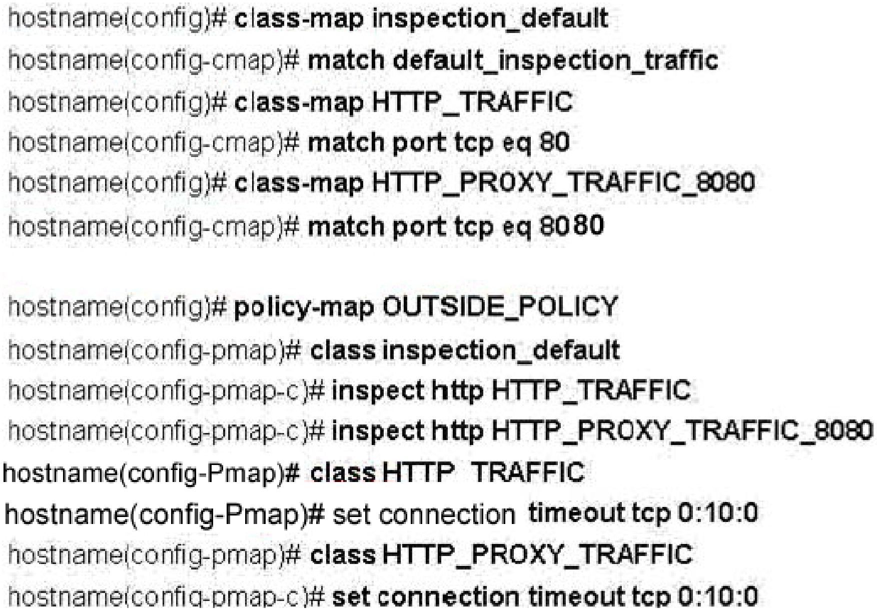
Which three of these are Cisco ASA syslog message fields? (Choose three.)

A. syslog community string
B. message.text
C. triggering packet copy
D. logging device ip
E. default ASA gateway
F. logging level

Answer: B,D,F

QUESTION 2:

Exhibit:



```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default_inspection_traffic
hostname(config)# class-map HTTP_TRAFFIC
hostname(config-cmap)# match port tcp eq 80
hostname(config)# class-map HTTP_PROXY_TRAFFIC_8080
hostname(config-cmap)# match port tcp eq 8080

hostname(config)# policy-map OUTSIDE_POLICY
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http HTTP_TRAFFIC
hostname(config-pmap-c)# inspect http HTTP_PROXY_TRAFFIC_8080
hostname(config-Pmap)# class HTTP  TRAFFIC
hostname(config-Pmap)# set connection  timeout tcp 0:10:0
hostname(config-pmap)# class HTTP_PROXY_TRAFFIC
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

You work as a network technician at Certkiller .com. Please study the exhibit carefully.
What does the inspect http HTTP_TRAFFIC command do in this policy map?

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

Answer: A

QUESTION 3:

An Administrator wants to protect a DMZ web server from SYN Flood attacks. Which three of these commands, used individually would allow the administrator to place limits on the number of embryonic connections? (choose three.)

A. http redirect
B. nat
C. http-proxy
D. static
E. set connection
F. access-list

Answer: B,D,E

QUESTION 4:

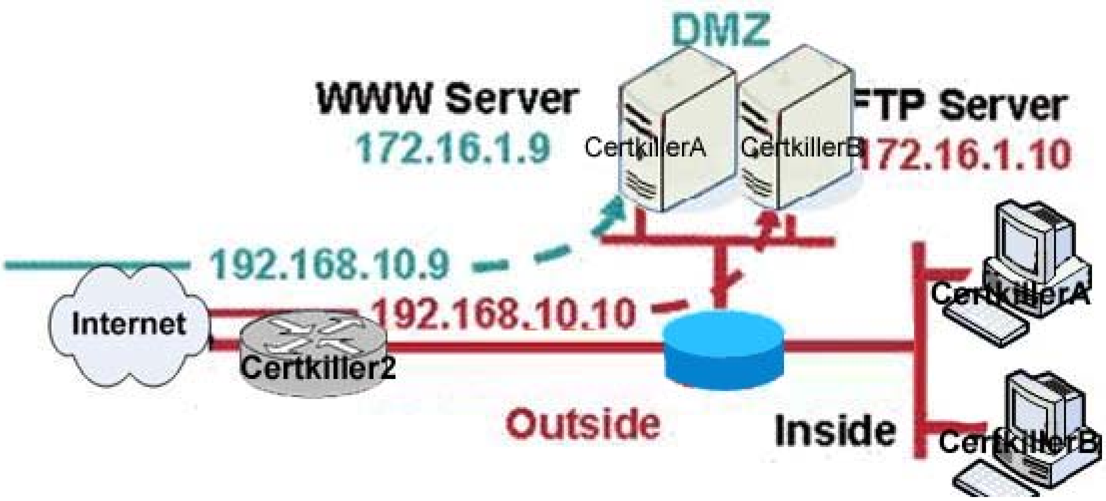
Which three of these are Cisco ASA syslog message fields? (Choose three.)

A. triggering packet copy
B. message.text
C. syslog community string
D. logging level
E. default ASA gateway
F. logging device ip

Answer: B,D,F

QUESTION 5:

Exhibit:



You work as a network technician at Certkiller .com. Please study the exhibit carefully. An administrator wants to permanently map host addresses on the DMZ subnet to the same host addresses, but a different subnet on the outside interface. Which command or commands should the administrator use to accomplish this?

A. access-list server_map permit tcp any 192.168.1.0.0 255.255.255.0
nat(outside) 10 access-list server_map
global (dmz) 10 172.16.1.9-10 netmask 255.255.255.0
B. static (dmz,outside) 192.168.10.0 172.16.1.0 netmask 255.255.255.0
C. nat (dmz) 1 172.16.1.0 netmask 255.255.255.0
global (outside) 1 192.168.10.9-10 netmask 255.255.255.0
D. NAT (dmz) 0 172.16.1.0 netmask 255.255.255.0

Answer: B

Explanation:
To configure regular static NAT, use the "static" command. This command is normally done to create static 1-1 mappings, but can be done to create static mappings for an entire subnet as required in this example.
For example, the following command maps the outside address (209.165.201.15) to an inside address (10.1.1.6):

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask
255.255.255.255
```

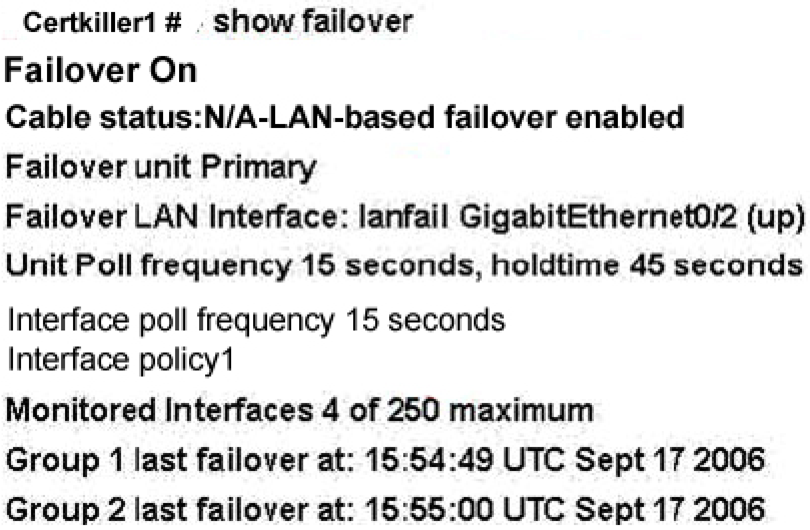
The following command statically maps an entire subnet:

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

Note: If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the security appliance translates the .0 and .255 addresses.
Reference: Cisco Security Appliance Command Line Configuration Guide Forthe Cisco ASA 5500 Series and Cisco PIX 500 Series, page 14-45.

QUESTION 6:

Exhibit:



```
Certkiller1 # . show failover
Failover On
Cable status:N/A-LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: lanfail GigabitEthernet0/2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface poll frequency 15 seconds
Interface policy1
Monitored Interfaces 4 of 250 maximum
Group 1 last failover at: 15:54:49 UTC Sept 17 2006
Group 2 last failover at: 15:55:00 UTC Sept 17 2006
```

You work as a network technician at Certkiller .com. Please study the exhibit carefully. This adaptive security appliance is configured for which two types of failover? (Choose two.)

A. Stateful Failover
B. LAN-Based Failover
C. Active/Standby Failover
D. Active/Active failover
E. Context/Group failover
F. Cable-based failover

Answer: B,D
It is a LAN-Based Failover as indicated in the show failover output:
"Cable status: N/A - LAN-based failover enabled"
The Active/Active failover is indicated by the 2 Groups in the output, an excerpt from the "Cisco Security Appliance Command Line Configuration Guide, Version 7.2" follows:
.."
In Active/Active failover, you divide the security contexts on the security appliance into failover groups. A failover group is simply a logical group of one or more security contexts. You can create a maximum of two failover groups on the security appliance. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.

QUESTION 7:

Which these commands displays the status of the CSC SSM on the Cisco ASA?

A. show module 1 CSC details

B. show hw 1 details
C. show module 1 details
D. show interface GigabitEthernet 1/0

Answer: C

Explanation:
To check the status of an SSM, use the show module command.
The argument 1, at the end of the command, is the slot number occupied by the SSM. If you do not know the slot number, you can omit it and see information about all modules, including the adaptive security appliance, which is considered to occupy slot 0 (zero).
Use the details keyword to view additional information for the SSM.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 8:

Which command both verifies that NAT is working properly and displays active NAT translations?

A. show nat translation
B. show running-confugration nat
C. show ip nat all
D. show xlate

Answer: D

Explanation:
xlate An xlate, also referred to as a translation entry, represents the mapping of one IP address to another, or the mapping of one IP address/port pair to another.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 9:

The Cisco VPN Client supports which three of these tunneling protocols and methods? (Choose three.)

A. AH
B. LZS
C. IPSec over TCP
D. IPSec over UDP
E. SCEP
F. ESP

Answer: C,D,F

Explanation:
By default, the Easy VPN hardware client and server encapsulate IPSec in User Datagram Protocol (UDP) packets. Some environments, such as those with certain firewall rules, or NAT and PAT devices, prohibit UDP. To use standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) in such environments, you must configure the client and the server to encapsulate IPSec within TCP packets to enable secure tunneling. If your environment allows UDP, however, configuring IPSec over TCP adds unnecessary overhead. To configure the Easy VPN hardware client to use TCP-encapsulated IPSec, enter the following command in global configuration mode: vpnclient ipsec-over-tcp [port tcp_port] Reference: Cisco Security Appliance Command Line Configuration Guide, Version 7.2
The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).
Reference: RFC 4303 - IP Encapsulating Security Payload (ESP) (http://tools.ietf.org/html/rfc4303)

QUESTION 10:

What does the nat 0 command do?

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

Answer: A

Explanation:
You can configure traffic to bypass NAT using one of three methods. All methods achieve compatibility with inspection engines. However, each method offers slightly different capabilities, as follows:
Identity NAT (nat command)-When you configure identity NAT (which is similar to dynamic NAT), you do not limit translation for a host on specific interfaces; you must use identity NAT for connections through all interfaces. Therefore, you cannot choose to perform normal translation on real addresses when you access interface A, but use identity NAT when accessing interface B. Regular dynamic NAT, on the other hand, lets you specify a particular interface on which to translate the addresses. Make sure that the real addresses for which you use identity NAT are routable on all networks that are

available according to your access lists. For identity NAT, even though the mapped address is the same as the real address, you cannot initiate a connection from the outside to the inside (even if the interface access list allows it). Use static identity NAT or NAT exemption for this functionality.
Static identity NAT (static command)-Static Identity NAT lets you specify the interface on which you want to allow the real addresses to appear, so you can use identity NAT when you access interface A, and use regular translation when you access interface B. Static identity NAT also lets you use policy NAT, which identifies the real and destination addresses when determining the real addresses to translate (see the "Policy NAT" section on page 17-9 for more information about policy NAT). For example, you can use static identity NAT for an inside address when it accesses the outside interface and the destination is server A, but use a normal translation when accessing the outside server B.
NAT exemption (nat 0 access-list command)-NAT exemption allows both translated and remote hosts to initiate connections. Like identity NAT, you do not limit translation for a host on specific interfaces; you must use NAT exemption for connections through all interfaces. However, NAT exemption does let you specify the real and destination addresses when determining the real addresses to translate (similar to policy NAT), so you have greater control using NAT exemption. However unlike policy NAT, NAT exemption does not consider the ports in the access list.
Reference: Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 11:

What does the activation-key command in the Cisco ASA do?

A. Applies the activation key to the Cisco ASDM so the Cisco ASA can be managed using a web interface
B. Applies the activation key to the Cisco ASA operating system, so that the Cisco ASA is licensed and all features are available
C. Activates the SSM module in the Cisco ASA, providing intrusion protection and content filtering
D. Automatically activates the Cisco ASA, allowing it to be configured right out of the box

Answer: B

QUESTION 12:

Which three of these are required in order to set up a CSC SSM on the Cisco ASA? (Choose three.)

A. The IP Address of the CSC interface

B. An SSL Certificate to user for HTTPS connections
C. An E-mail address for notifications
D. Activation codes
E. DNS names of critical hosts
F. IP Addresses of external routers

Answer: A,C,D

Explanation:
This is an excerpt of the steps to configure the CSC SSM:
..."
The management port of the CSC SSM must be connected to your network to allow management of and automatic updates to the CSC SSM software. Additionally, the CSC SSM uses the management port for email notifications and syslogging.
Step 2 With the CSC SSM, you should have received a Product Authorization Key (PAK). Use the PAK to register the CSC SSM at the following URL.
http://www.cisco.com/go/license After you register, you will receive activation keys by email. The activation keys are required before you can complete Step 6
Step 3 Gather the following information, for use in Step 6.
Activation Keys, received after completing Step2.
SSM management port IP address, netmask, and gateway IP address
"...
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 13:

Which of these commands enables IKE on the outside interface?

A. isakmp enable outside
B. ike enable outside
C. nameif outside isakmp enable
D. int g0/0 ike enable (outbound)

Answer: A

Explanation:
Enabling ISAKMP on the Outside Interface
You must enable ISAKMP on the interface that terminates the VPN tunnel. Typically this is the outside, or public interface.
To enable ISAKMP, enter the following command:

```
crypto isakmp enable interface-name
```

For example:

```
hostname(config)# crypto isakmp enable outside
```

Reference :Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 14:

The Cisco VPN Client supports which three of these tunneling protocols and methods? (Choose three.)

A. ESP
B. IPSec over UDP
C. LZS
D. SCEP
E. IPSec over TCP
F. AH

Answer: A,B,E

QUESTION 15:

Which three of these are potential groups of users for WebVPN? (Choose three.)

A. Remote Employees that need daily access to the internet corporate network
B. Employees that only need occasional corporate access to a few applications
C. Employees accessing specific internal applications from desktops and laptops not managed by IT
D. Administrators who need to manage servers and networking equipment
E. Users of a customer service kiosk placed in a retail store
F. Employees that need access to a wide range of corporate applications

Answer: B,C,E

QUESTION 16:

Which of the following statements about the Configuration of WebVPN on the Cisco ASA is true for Cisco ASA version 7.2?

A. WebVPN and Cisco ASDM can't be enabled at the same time on the Cisco ASA
B. WebVPN and Cisco ASDM can only be enabled at the same time using the command line interface
C. WebVPN and Cisco ASDM can't run on the same interface
D. WebVPN and Cisco ASDM can both be enabled on the same interface but must run on different TCP ports

Answer: D

Explanation:
Configuring WebVPN and ASDM on the Same Interface
The security appliance can support both WebVPN connections and HTTPS connections for ASDM administrative sessions simultaneously on the same interface. Both HTTPS and WebVPN use port 443 by default. Therefore, to enable both HTTPS and WebVPN on the same interface, you must specify a different port number for either HTTPS or WebVPN. An alternative is to configure WebVPN and HTTPS on different interfaces.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

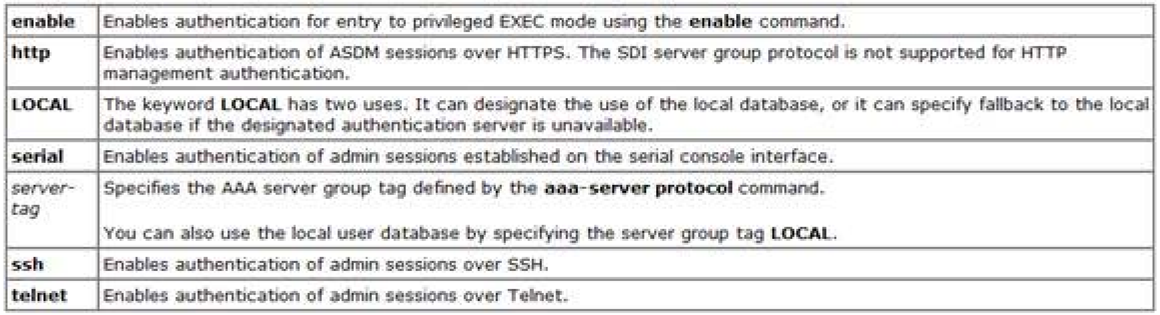
QUESTION 17:

Which command configures the Cisco ASA console for SSH access by a local user?

A. ssh username sysadmin password cisco123
B. aaa authentication ssh console LOCAL
C. aaa authentication ssh LOCAL
D. ssh console username sysadmin password cisco123

Answer: B

Explanation:
aaa authentication console
To enable authentication service for access to the security appliance console over an SSH, HTTP, or Telnet connection or from the Console connector on the security appliance, use the aaa authentication console command in global configuration mode. This command also lets you enable access to privileged EXEC mode. To disable this authentication service, use the no form of this command.
aaa authentication {serial | enable | telnet | ssh | http} console {server-tag [LOCAL] | LOCAL}
no aaa authentication {serial | enable | telnet | ssh | http} console {server-tag [LOCAL] | LOCAL}
Syntax Description

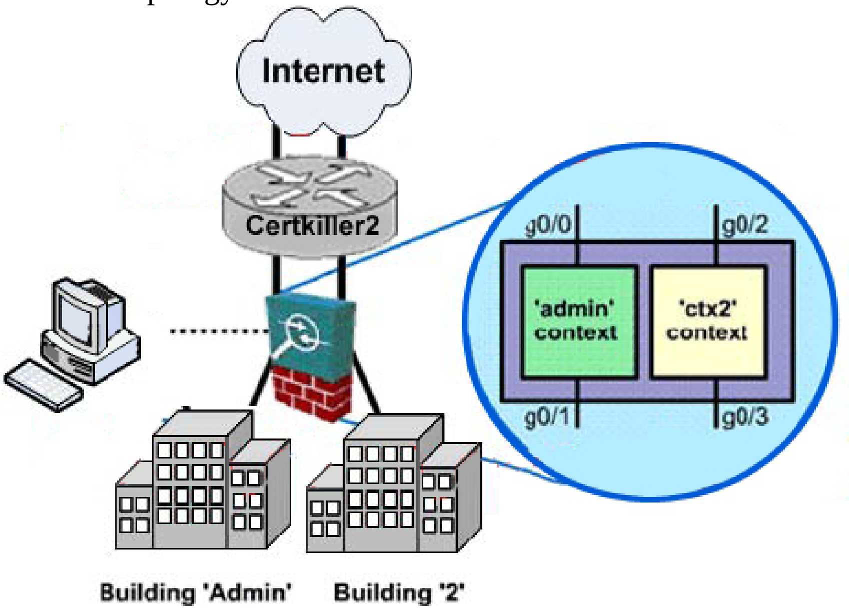


enable	Enables authentication for entry to privileged EXEC mode using the **enable** command.
http	Enables authentication of ASDM sessions over HTTPS. The SDI server group protocol is not supported for HTTP management authentication.
LOCAL	The keyword **LOCAL** has two uses. It can designate the use of the local database, or it can specify fallback to the local database if the designated authentication server is unavailable.
serial	Enables authentication of admin sessions established on the serial console interface.
server-tag	Specifies the AAA server group tag defined by the **aaa-server protocol** command. You can also use the local user database by specifying the server group tag **LOCAL**.
ssh	Enables authentication of admin sessions over SSH.
telnet	Enables authentication of admin sessions over Telnet.

Reference : Cisco Security Appliance Command Reference, Version 7.2

QUESTION 18:

SIMULATION
Network topology exhibit:



You work as a network engineer at Certkiller .com. You have installed a brand new ASA.
You have configured it with factory-default, single mode.
Your boss, Ms. Certkiller, has asked you to make further configurations.
More specifically, use host Certkiller A to:
* add two security appliance contexts and tx2.
* allocate appropriate interface to each context
* identify location from which the system downloads the context configuration
* the context named dminand will support interfaces GigabetEthernet0/0 and GigabitEthernet0/1
* the context named dminand must be stored in the ASA flash file admin.cfg
* the context named tx2 will support interfaces GigabetEthernet0/2 and GigabitEthernet0/3
* the context named tx2 must be stored in the ASA flash file ctx2.cfg
You are finished with the task after the contexts are created, interfaces allocated and context configuration file locations are configured in the ASA system context.

Answer:

Explanation:

```
ASA(config)#admin-context admin
ASA(config)#context admin
ASA(config-ctx)#allocate-interface gigabitethernet0/0
ASA(config-ctx)#allocate-interface gigabitethernet0/1
ASA(config-ctx)#config-url flash:/admin.cfg
ASA(config-ctx)#exit
ASA(config)#context tx2
ASA(config-ctx)#allocate-interface gigabitethernet0/2
ASA(config-ctx)#allocate-interface gigabitethernet0/3
ASA(config-ctx)#config-url flash:/ctx2.cfg
```

QUESTION 19:

Which of these commands would block all SIP INVITE packets, such as calling-party and request-method from specific SIP EndPoints?

A. Use the match calling-party command in a class map. Apply the class map to a policy map that contains the match request-methods command.
B. Group match commands in the global_polocy policy map
C. Group the match commands in a SIP inspection policy map
D. Group the match commands in a SIP inspection class map

Answer: D

QUESTION 20:

Which three of these protocols can the content security and control module for the Cisco ASA be configured to scan? (Choose three.)

A. Telnet
B. SMTP
C. FTP
D. POP3
E. HTTPS
F. SSH

Answer: B,C,D
Sending Traffic to the Content Security and Control Security Services Module
If your model supports it, the CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that you configure the adaptive security appliance to send to it.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 21:

Which username and password can you use to establish an SSH connection to you adaptive security appliance when no local or remote user database has been configured?

A. The username "pix" and the password "cisco123"

B. The username "ssh" and the password "cisco123"
C. The username "ssh" and the password "pix"
D. The username "pix" and the password "cisco"

Answer: D

Explanation:
SSH Access to the Security Appliance
Complete these steps in order to configure SSH access to the security appliance:
SSH sessions always require a username and password for authentication. There are two ways to meet this requirement.
Configure a username and password and use AAA:
Syntax :

```
pix(config)#username username password password
pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL |
server_group [LOCAL]}
```

Note: If you use a TACACS+ or RADIUS server group for authentication, you can configure the security appliance to use the local database as a fallback method if the AAA server is unavailable. Specify the server group name and then LOCAL (LOCAL is case sensitive). We recommend that you use the same username and password in the local database as the AAA server, because the security appliance prompt does not give any indication which method is used.
Note: Example :

```
pix(config)#aaa authentication ssh console TACACS+ LOCAL
```

Note: You can alternatively use the local database as your main method of authentication with no fallback. In order to do this, enter LOCAL alone.
Example :

```
pix(config)#aaa authentication ssh console LOCAL
```

OR
Use the default username of pix and the default Telnet password of cisco. You can change the Telnet password with this command:

```
pix(config)#passwd password
```

Note: The password command can also be used in this situation. Both commands do the same thing.

QUESTION 22:

Which mode of operation must you enter in order to recover the Cisco ASA password?

A. configure
B. unprivileged
C. privileged
D. Monitor

Answer: D

Explanation:
Performing Password Recovery for the ASA 5500 Series Adaptive Security Appliance
To recover from the loss of passwords, perform the following steps:
Step 1 Connect to the security appliance console port according to the "Accessing the Command-Line Interface" section on page 2-1.
Step 2 Power off the security appliance, and then power it on.
Step 3 During the startup messages, press the Escape key when prompted to enter ROMMON.
Step 4 To set the security appliance to ignore the startup configuration at reload, enter the following command:
rommon #1> confreg
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.1

QUESTION 23:

The primary adaptive security appliance failed, so the secondary adaptive security appliance was automatically activated. The network administrator then fixed the problem. Now the administrator wants to return the primary to "active" status.
Which of these commands, when issued on the primary adaptive security appliance, will reactivate the primary security appliance and restore it to "active" status?

A. Failover primary active
B. Failover secondary group 1
C. Failover active group 1
D. Failover secondary standby group 1

Answer: C

Explanation:
If the failover groups are configured with the preempt command, they will automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with the preempt command, you can return them to active status on their designated units using the failover active group command.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 24:

What does the csd enable command enable on the Cisco ASA?

A. It enables the Cisco Secure Desktop for IPSec VPN Clients when they connect to the Cisco ASA
B. It enables the Cisco Secure Desktop on the host connecting to the Cisco ASDM
C. It enables the Cisco Secure Desktop on SSL VPN clients without a host-based firewall
D. It enables the Cisco Secure Desktop for SSL VPN clients when they connect

Answer: D

QUESTION 25:

Which of these commands will configure the adaptive security appliance to use an ACS server fro console access authentication?

A. aaa authentication serial console SRVGRP1 LOCAL
B. aaa authentication serial console LOCAL
C. aaa authentication console SRVGRP1
D. aaa authentication console LOCAL

Answer: A
To authenticate users who access the CLI, enter the following command:

```
hostname(config)# aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group
[LOCAL]}
```

The http keyword authenticates the ASDM client that accesses the security appliance using HTTPS. You only need to configure HTTP authentication if you want to use a AAA server. By default, ASDM uses the local database for authentication even if you do not configure this command. HTTP management authentication does not support the SDI protocol for a AAA server group.
If you use a AAA server group for authentication, you can configure the security appliance to use the local database as a fallback method if the AAA server is unavailable. Specify the server group name followed by LOCAL (LOCAL is case sensitive). We recommend that you use the same username and password in the local database as the AAA server because the security appliance prompt does not give any indication which method is being used. You can alternatively use the local database as your main method of authentication (with no fallback) by entering LOCAL alone.
Reference :Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 26:

Which command will set the default route for an adaptive security appliance to the IP Address 10.10.10.1?

A. route outside 0 0 10.10.10.1.1
B. route add default 0 10.10.10.1
C. route management 10.10.10.0 0.0.0.255 10.10.10.1.1
D. route 0 0 10.10.10.1.1

Answer: A
To define the default route, enter the following command:

```
hostname(config)# route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance | tunneled]
```

Tip You can enter 0 0 instead of 0.0.0.0 0.0.0.0 for the destination network address and mask, for example:

```
hostname(config)# route outside 0 0 192.168.1 1
```

Reference: Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 27:

Which of the following statements about adaptive security appliance failover is true?

A. The PIX adaptive security appliance only supports LAN-based failover
B. The PIX adaptive security appliance supports LAN-based and cable-based failover
C. The Cisco ASA security appliance only supports cable-based failover
D. The Cisco ASA and PIX security appliance support LAN-based and cable-based failover

Answer: B

Explanation:
On the PIX 500 series security appliance, the failover link can be either a LAN-based connection or a dedicated serial Failover cable. On the ASA 5500 series adaptive security appliance, the failover link can only be a LAN-based connection.
Reference: Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 28:

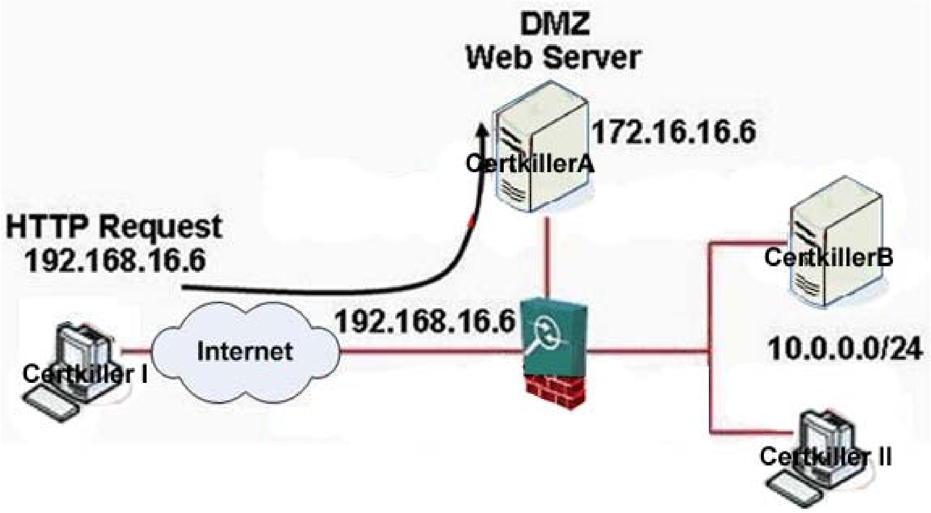
Which three of these are encryption algorithms used by Cisco ASA security appliances? (Choose three.)

A. RC4
B. DES
C. Diffie-Hellman Group 5
D. AES
E. Blowfish
F. 3DES

Answer: B,D,F

QUESTION 29:

Exhibit:



You work as a network technician at Certkiller .com. Please study the exhibit carefully.
The network administrator for this small site has chosen to authenticate HTTP
cut-through proxy traffic via a local database on the Cisco AS
A. Which set of command
strings should the administrator enter to accomplish this?

A. Certkiller 1(config)#static (dmz,outside) 192.168.16.6 172.16.16.6
Certkiller 1(config)#access-list 150 permit tcp any host 172.16.16.6 eq www
Certkiller 1(config)#aaa authentication match 150 outside LOCAL
B. Certkiller 1(config)#static (dmz,outside) 192.168.16.6 172.16.16.6
Certkiller 1(config)#access-list 150 permit tcp any host 192.168.16.6 eq www
Certkiller 1(config)#aaa authentication match 150 outside LOCAL
C. Certkiller 1(config)#static (dmz,outside) 192.168.16.6 172.16.16.6
Certkiller 1(config)#access-list 150 permit tcp any host 172.16.16.6 eq www
Certkiller 1(config)#aaa authentication match 150 outside Certkiller 1
D. Certkiller 1(config)#static (dmz,outside) 192.168.16.6 172.16.16.6
Certkiller 1(config)#access-list 150 permit tcp any host 172.16.16.6 eq www
Certkiller 1(config)#aaa authentication match 150 outside asa2

Answer: B

Explanation:
The first option could seem like the correct choice but In fact it is the Outside interface
that is the Destination IP/host and not the "Real IP" (the IP of the server in the DMZ).
The following excerpts are from "Cisco Security Appliance Command Line
Configuration Guide, Version 7.2"
* Take note of the static and access-list commands below
Redirect Telnet requests for 209.165.201.5 to 10.1.1.6 by entering the following
command:

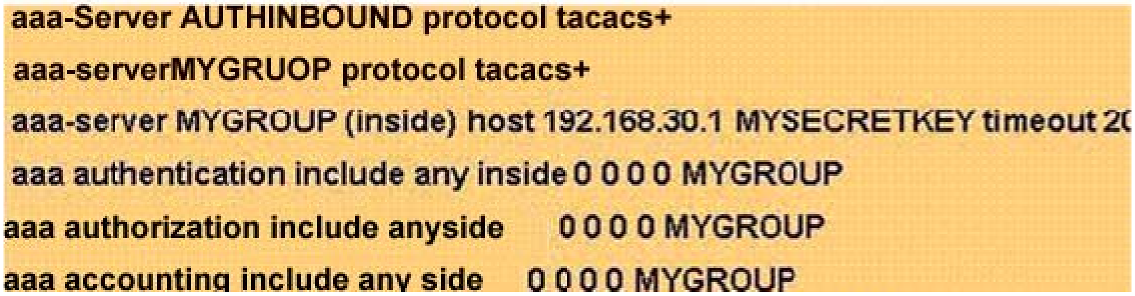
```
hostname(config)# static (inside,outside) tcp 209.165.201.5 telnet 10.1.1.6 telnet netmask
255.255.255.255
```

The following commands authenticate Telnet traffic from the outside interface to a
particular server (209.165.201.5):

```
hostname(config)# aaa-server AuthInbound protocol tacacs+
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# access-list TELNET_AUTH extended permit tcp any host
209.165.201.5 eq telnet
hostname(config)# aaa authentication match TELNET_AUTH outside AuthInbound
```

QUESTION 30:

Exhibit:



```
aaa-Server AUTHINBOUND protocol tacacs+
aaa-serverMYGRUOP protocol tacacs+
aaa-server MYGROUP (inside) host 192.168.30.1 MYSECRETKEY timeout 2
aaa authentication include any inside 0 0 0 0 MYGROUP
aaa authorization include anyside     0 0 0 0 MYGROUP
aaa accounting include any side     0 0 0 0 MYGROUP
```

You work as a network technician at Certkiller .com. Please study the exhibit carefully. Given the configuration commands shown, what traffic will be logged to the AAA Server?

A. Only the authenticated console connection information will be logged int eh accounting database
B. All connection information will be logged in the accounting database
C. No information will be logged. This is not a valid configuration because TACACS+ connection information can't be captured and logged
D. All outbound connection information will be logged in the accounting database

Answer: D

QUESTION 31:

Which of these commands causes the CSC SSM to load a new software image from a remote TFTP server via the CLI?

A. Module 1 recover config
B. Copy tftp:tftphost/image.bin hardware:module1/image.bin
C. Hw module 1 recover config
D. Hw module recover config

Answer: C

Transferring an Image onto an SSM

For an intelligent SSM, such as AIP SSM or CSC SSM, you can transfer application images from a TFTP server to the SSM. This process supports upgrade images and maintenance images.

Note If you are upgrading the application on the SSM, the SSM application may support backup of its configuration. If you do not back up the configuration of the SSM application, it is lost when you transfer an image onto the SSM. For more information about how your SSM supports backups, see the documentation for your SSM.

To transfer an image onto an intelligent SSM, perform the following steps:

Step 1 Create or modify a recovery configuration for the SSM. To do so, perform the following steps:

a. Determine if there is a recovery configuration for the SSM. To do so, use the show module command with the recover keyword, as follows.

hostname# show module slot recover where slot is the slot number occupied by the SSM.

If the recover keyword is not valid, a recovery configuration does not exist. The recover keyword of the show module command is available only when a recovery configuration exists for the SSM.

Note When the adaptive security appliance operates in multiple context mode, the configure keyword is available only in the system context. If there is a recovery configuration for the SSM, the adaptive security appliance displays it. Examine the recovery configuration closely to ensure that it is correct, especially the Image URL field. The following example show a recovery configuration for an SSM in slot 1.

```
hostname# show module 1 recover
Module 1 recoverparameters. . .
Boot Recovery Image: Yes
Image URL: tftp://10.21.18.1/ids-oldimg
Port IP Address: 10.1.2.10
Port Mask : 255.255.255.0
Gateway IP Address: 10.1.2.254
```

b. If you need to create or modify the recovery configuration, use the hw-module module recover command with the configure keyword, as follows:

```
hostname# hw-module module slot recover configure
```

whereslot is the slot number occupied by the SSM.

Complete the prompts as applicable. If you are modifying a configuration, you can keep the previously configured value by pressing Enter. The following example shows the prompts. For more information about them, see the entry for the hw-module module recover command in the Cisco Security Appliance Command Reference.

```
Image URL [tftp://0.0.0.0/]:
Port IP Address [0.0.0.0]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
```

Note Be sure the TFTP server you specify can transfer files up to 60 MB in size. Also, be sure the TFTP server can connect to the management port IP address that you specify for the SSM. After you complete the prompts, the adaptive security appliance is ready to transfer to the SSM the image that it finds at the URL you specified.

Step 2 Transfer the image from the TFTP server to the SSM and restart the SSM. To do so, use the hw-module module recover command with the boot keyword, as follows.

```
hostname# hw-module module slot recover boot
```

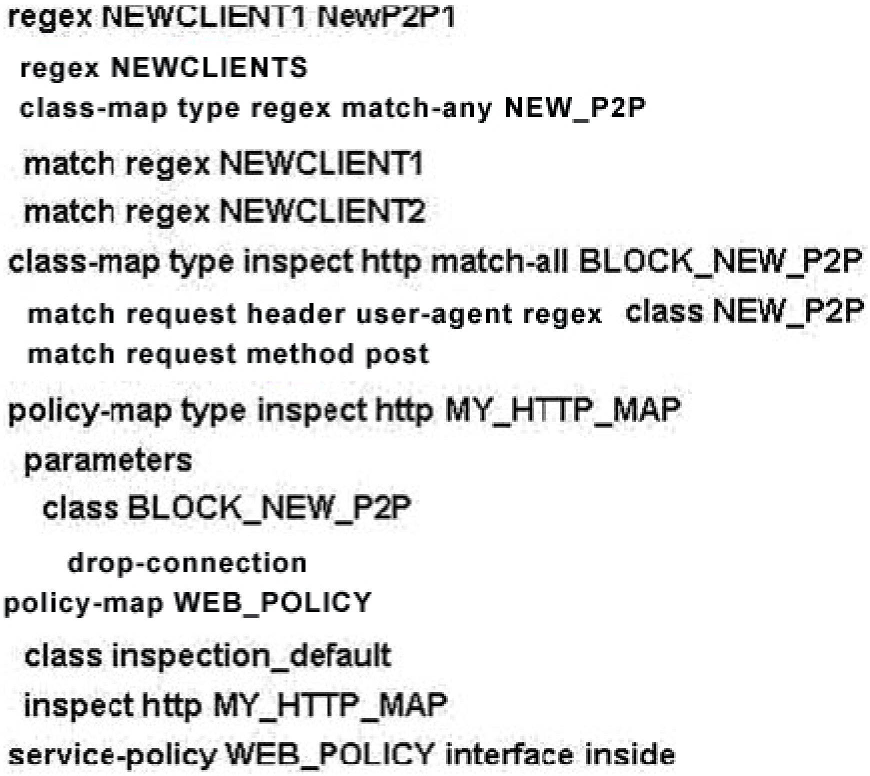
whereslot is the slot number occupied by the SSM.

Step 3 Check the progress of the image transfer and SSM restart process. To do so, use the

show module command. For details, see the "Checking SSM Status" section on page 22-13. When the adaptive security appliance completes the image transfer and restart of the SSM, the SSM is running the newly transferred image.
Note If your SSM supports configuration backups and you want to restore the configuration of the application running on the SSM, see the documentation for your SSM for details.
Reference :Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 32:

Exhibit:



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

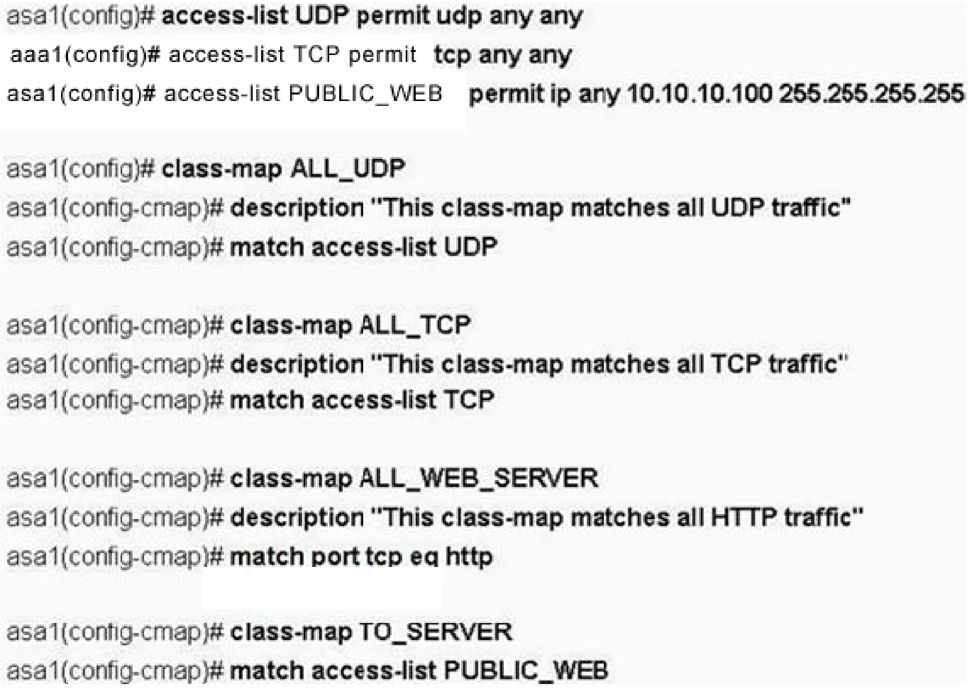
You work as a network technician at Certkiller .com. Please study the exhibit carefully.
What will the adaptive security appliance do if it is configured as shown?

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

Answer: A

QUESTION 33:

Exhibit:



```
asa1(config)# access-list UDP permit udp any any
aaa1(config)# access-list TCP permit  tcp any any
asa1(config)# access-list PUBLIC_WEB  permit ip any 10.10.10.100 255.255.255.255

asa1(config)# class-map ALL_UDP
asa1(config-cmap)# description "This class-map matches all UDP traffic"
asa1(config-cmap)# match access-list UDP

asa1(config-cmap)# class-map ALL_TCP
asa1(config-cmap)# description "This class-map matches all TCP traffic"
asa1(config-cmap)# match access-list TCP

asa1(config-cmap)# class-map ALL_WEB_SERVER
asa1(config-cmap)# description "This class-map matches all HTTP traffic"
asa1(config-cmap)# match port tcp eq http

asa1(config-cmap)# class-map TO_SERVER
asa1(config-cmap)# match access-list PUBLIC_WEB
```

You work as a network technician at Certkiller .com. Please study the exhibit carefully. An administrator is adding descriptions to class maps for each port of the modular policy framework. What text would the administrator add to the description command to describe the TO_SERVER class map?

A. Description "This class-map matches all TCP traffic for public web server"
B. Description "This class-map matches all HTTP traffic for the public web server"
C. Description "This class-map matches all HTTPS traffic for public web server"
D. "This class-map matches all IP traffic for public web server"

Answer: D

QUESTION 34:

When configuring a crypto ipsec transform-set command, how many unique transforms can a single transform set contain?

A. Three
B. One
C. Four
D. Two

Answer: A

Explanation:
Sets are limited to up to one AH and up to two ESP transforms
When configuring IPSec, configure a transform set to define how to protect the traffic. You can configure multiple transform sets (up to three), and then specify one or more of these transform sets in a crypto map
cryptoipsec transform-set transform-set-name transform1 [tcansform2, transform3]
For example:
cryptoipsec transform-set myset1 esp-des esp-sha-hmac
cryptoipsec transform-set myset2 esp-3des esp-sha-hmac
cryptoipsec transform-set aes_set esp-md5-hmac esp-aes-256
In this example, "myset1" and "myset2" and "aes_set" are the names of the transform sets.
Reference:Cisco Security Appliance Command Line Configuration Guide 7.0, Page 23-23

QUESTION 35:

Which command configures the adaptive security appliance interface as a DHCP client and sets the default route to be the default gateway parameter returned from the DHCP server?

A. ip address dhcp
B. ip address dhcp default route
C. ip address dhcp setroute
D. dhcp setroute

Answer: C
Excerpts from Cisco Security Appliance Command Line Configuration Guide, Version 7.2
hostname(config-if)# ip address dhcp [setroute]
Reenter this command to reset the DHCP lease and request a new lease. If you do not enable the interface using the no shutdown command before you enter the ip address dhcp command, some DHCP requests might not be sent. "..
.." You must use the setroute argument with the ip address dhcp command to obtain the default route using DHCP. "..

QUESTION 36:

Which three types of information can be found in the syslog output for an adaptive security appliance? (Choose three.)

A. default router
B. interface packet received
C. hostname of the packet sender
D. time stamp and date
E. logging level
F. message text

Answer: D,E,F

QUESTION 37:

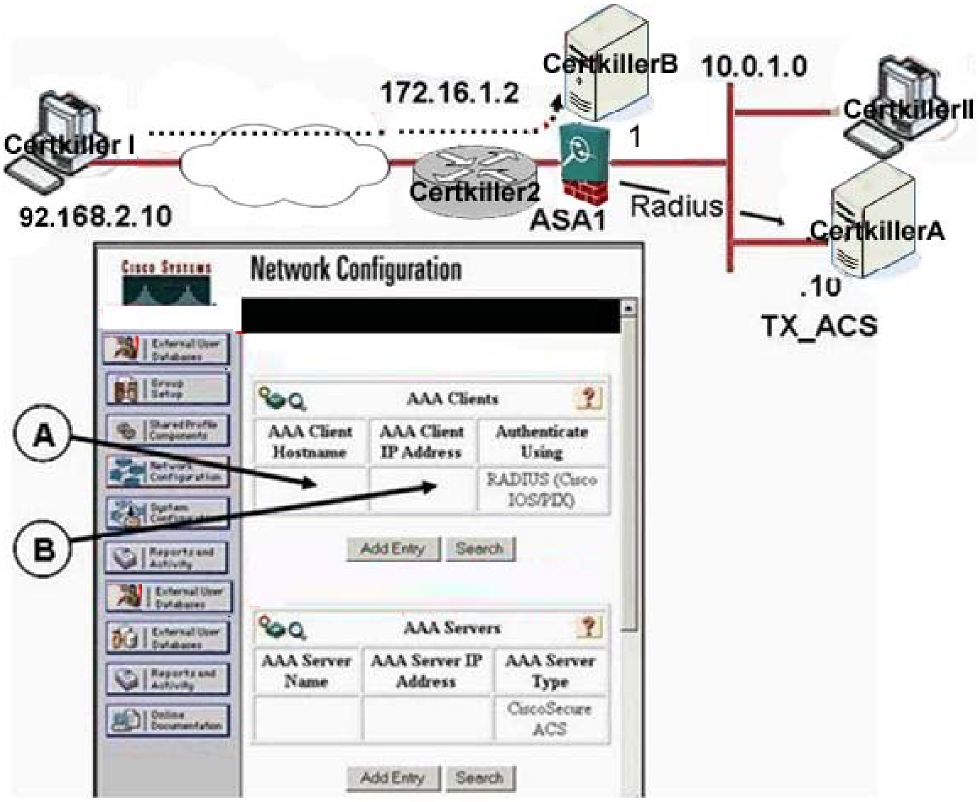
Which three of these commands will show you the contents of flash memory on the Cisco ASA? (Choose three.)

A. dir
B. info flash
C. directory
D. show disk
E. flash
F. show flash

Answer: A,D,F

QUESTION 38:

Exhibit:



AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
		RADIUS (Cisco IOS/PIX)

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
		CiscoSecure ACS

Refer to the exhibit: A network administrator wants to authenticate remote users who are accessing the Certkiller B server from the internet. When a remote user initiates a session to the Certkiller B server, the ASA1 security appliance will verify the user's credentials with the TX_ACS AAA server via RADIUS. To accomplish this the administrator must load and configure Cisco ACS software on the TX_ACS AAA server. During the process, the administrator must correctly configure the AAA client information in the Cisco ACS network configuration window.
What must the administrator place in filed A (AAA client hostname) and filed B (AAA client IP Address)?

A. AX_ACS
B?0.0.1.10
B. Aave
B?92.168.2.10
C. ASA1
B?0.0.1.1
D. AEB1
B?72.168.1.2

Answer: C

Explanation:
To add a device to the ACS network configuration and to use RADIUS as the protocol,follow these steps:
Step 1. Select Network Configuration.

Step 2. Select Add Entry under the AAA client table.
Step 3. Enter the hostname of the AAA client.
Step 4. Enter the IP addresses of the security appliance.
Step 5. Use the drop-down list to select RADIUS.
Step 6. Enter a secret key to be used for encryption.
Step 7. Select Submit + Apply.
Reference: CCSP SNPA Quick Reference

QUESTION 39:

Which commands are necessary in order to add a port for DNS inspection?

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

Answer: A

Explanation:
Configuring Application Inspection
Step 1 To identify the traffic to which you want to apply inspections, add either a Layer 3/4 class map for through traffic or a Layer 3/4 class map for management traffic.
For example, to limit inspection to traffic from 10.1.1.0 to 192.168.1.0 using the default class map, enter the following commands:

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

Step 2 (Optional) Some inspection engines let you control additional parameters when you apply the inspection to the traffic.........
Step 3 To add or edit a Layer 3/4 policy map that sets the actions to take with the class map traffic, enter the following command:

```
hostname(config)# policy-map name
```

Step 4 To identify the class map from Step 1 to which you want to assign an action, enter the following command:

```
hostname(config-pmap)# class class_map_name
```

Step 5 Enable application inspection by entering the following command:

```
hostname(config-pmap-c)# inspect protocol
```

Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 40:

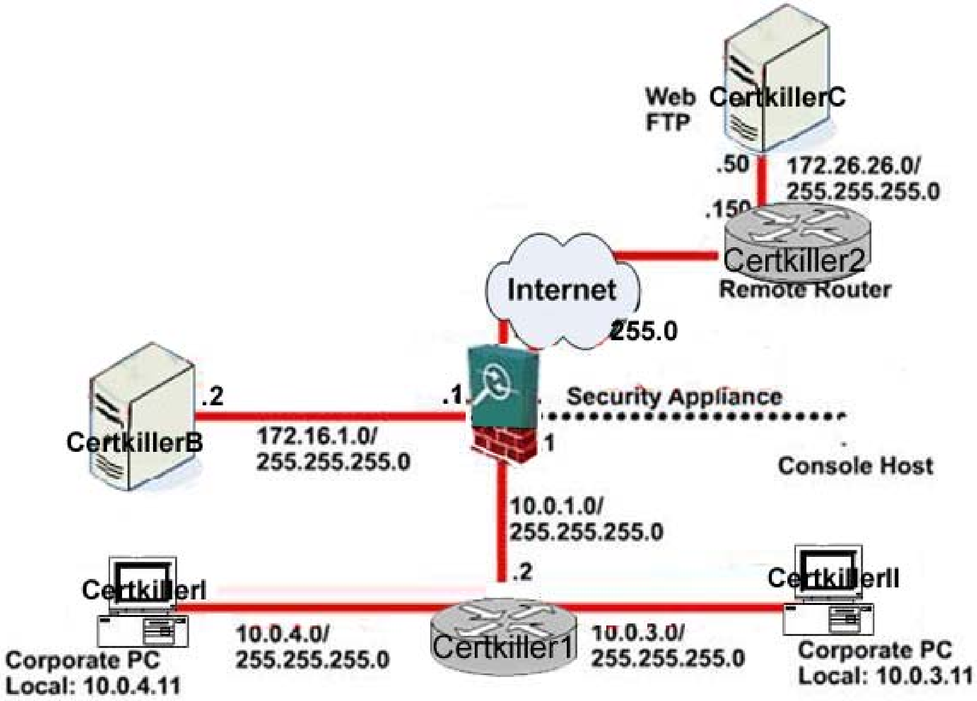
On a Cisco ASA adaptive security appliance, the administrator enters the boot config disk0:/startup.txt command. What will this command do when the system is rebooted?

A. It will copy the current config file to the startup.txt file on disk 0.
B. It will configure the Cisco ASA to boot using the startup.txt config file stored in flash memory.
C. It will do nothing until the file extension is changed to .cfg, at which time it will boot the startup.cfg config file
D. It will configure the ASA to skip the hardware diagnostics and perform a warm boot of the startup.txt config file

Answer: B
Configuring the File to Boot as the Startup Configuration
By default, the security appliance boots from a startup configuration that is a hidden file. You can alternatively set any configuration to be the startup configuration by entering the following command:
hostname(config)# boot config {flash:/ | disk0:/ | disk1:/}[path/]filename
The flash:/ keyword represents the internal Flash memory on the PIX 500 series security appliance. You can enter flash:/ or disk0:/ for the internal Flash memory on the ASA 5500 series adaptive security appliance. The disk1:/ keyword represents the external Flash memory on the ASA.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 41:

SIMULATION
Network topology exhibit:



You work as a network engineer at Certkiller .com. You study the network topology very

carefully and then you install a Cisco ASA (Adaptive Securit Appliance). Your boss, Ms. Certkiller, has asked you to make further configurations.
In particular:
* basic outbound configured on the outside interface for all hosts on the inside network 10.0.3.0/255.255.255.0.
* the real IP addresses of the inside hosts should be hidden from the outside network
* packet traversing from a higher security interface to a lower security interface for all other inside network must match a NAT rule, or else processing for the packet must stop
* after the configuration has been completed you should be able to open a Web session from the corporate PC at 10.0.3.11 to the Certkiller C server located at 172.26.26.50. 172.26.26.50.
* you should not be able to open a Web session from the session from the corporate PC at 10.0.4.11 to the Web server located at 172.26.26.50.

Answer:

QUESTION 42:

A security appliance administrator has defined a regular expression to match an authorized website. Which pair of commands would the administrator need to enter to configure a regular expression class map?

A. class-map type regex match-any URL
match regex UNATHORIZED_SITE
B. class-map type regex match-any
Match regex UNAUTHORIZED_SITE
C. class-map regex match-any URL
Match UNAUTHORIZED_SITE
D. class-map match-any type regex
Match UNAUTHORIZED_SITE

Answer: A
Creating a Regular Expression Class Map
A regular expression class map identifies one or more regular expressions. You can use a regular expression class map to match the content of certain traffic; for example, you can match URL strings inside HTTP packets. To create a regular expression class map, perform the following steps:
Step 1 Create one or more regular expressions according to the "Creating a Regular Expression" section.
Step 2 Create a class map by entering the following command:

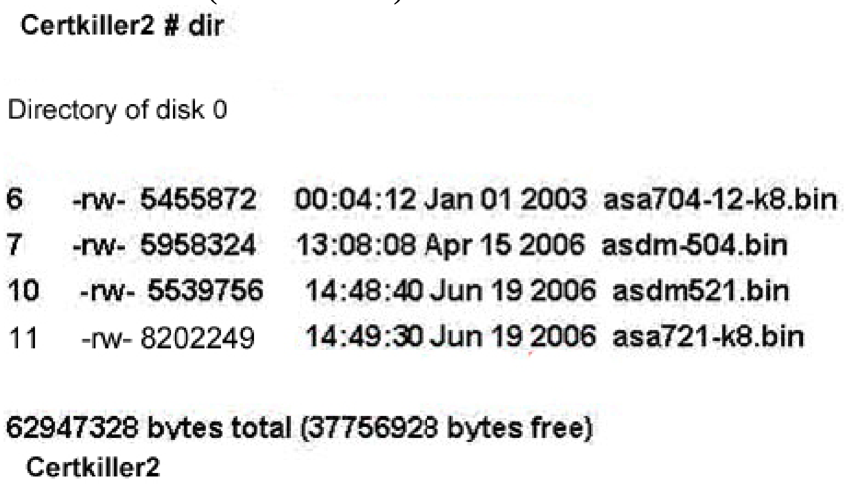
```
hostname(config)# class-map type regex match-any class_map_name
hostname(config-cmap)#
```

Where class_map_name is a string up to 40 characters in length. The name "class-default" is reserved. All types of class maps use the same name space, so you cannot reuse a name already used by another type of class map. The match-any keyword specifies that the traffic matches the class map if it matches only one of the regular

expressions. The CLI enters class-map configuration mode.
Step 3 (Optional) Add a description to the class map by entering the following command:
hostname(config-cmap)# description string
Step 4 Identify the regular expressions you want to include by entering the following command for each regular expression:
hostname(config-cmap)# match regex regex_name
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 43:

Refer to exhibit: Which three show commands would verify that the boot image is asa721-k8.bin? (Choose three.)



```
 Certkiller2 # dir

Directory of disk 0

6    -rw-  5455872    00:04:12 Jan 01 2003  asa704-12-k8.bin
7    -rw-  5958324    13:08:08 Apr 15 2006  asdm-504.bin
10    -rw-  5539756    14:48:40 Jun 19 2006  asdm521.bin
11    -rw- 8202249     14:49:30 Jun 19 2006  asa721-k8.bin

62947328 bytes total (37756928 bytes free)
  Certkiller2
```

A. show startup-config
B. show processes
C. show version
D. show disk0:
E. show bootvar
F. show cpu profile

Answer: A,C,E

QUESTION 44:

By default, adaptive security appliances configured for LAN-based failover will fail over after approximately 15 seconds. Which two commands should an administrator configure on the security appliance to detect a failure faster? (Choose two.)

A. Failover polltime interface

B. Failover polltime unit
C. Failover interface-police polltime
D. Failover unit-policy polltime

Answer: A,B

QUESTION 45:

You want to block a new instant messaging application. Which three of these are mandatory for accomplishing this goal with your Cisco ASA? (Choose three.)

A. A regular expression
B. A Layer 3/4 Policy map
C. A regex class map
D. An HTTP inspection class map
E. An IM inspection policy map
F. An HTTP inspection Policy map

Answer: A,C,E

Explanation:
Configuring Special Actions for Application Inspections (Inspection Policy Map)
Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the Layer 3/4 policy map, you can also optionally enable actions as defined in an inspection policy map. When the inspection policy map matches traffic within the Layer 3/4 class map for which you have defined an inspection action, then that subset of traffic will be acted upon as specified (for example, dropped or rate-limited). This section includes the following topics:
Inspection Policy Map Overview, Page 21-8
Defining Actions in an Inspection policy Map , page 21-8
Identifying Traffic in an Inspection Class Map , page 21-11
Creating a Regular Expression , page 21-12
Creating a Regular Expression Class Map, page 21-14
"...
..."
Configuring an Instant Messaging Inspection Policy Map for Additional Inspection Control
To specify actions when a message violates a parameter, create an IM inspection policy map. You can then apply the inspection policy map when you enable IM inspection according to the "Configuring Application Inspection" section.
To create an IM inspection policy map, perform the following steps:

Step 1 (Optional) Add one or more regular expressions for use in traffic matching commands according to the "Creating a Regular Expression" section on page 21-12. See the types of text you can match in the match commands described in Step 3.
Step 2 (Optional) Create one or more regular expression class maps to group regular

expressions according to the "Creating a Regular Expression Class Map" section on page 21-14.s

Step 3 (Optional) Create an IM inspection class map by performing the following steps.

A class map groups multiple traffic matches. Traffic must match all of the match commands to match the class map. You can alternatively identify match commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the match not command. For example, if the match not command specifies the string "example.com," then any traffic that includes "example.com" does not match the class map.

For the traffic that you identify in this class map, you can specify actions such as drop-connection, reset, and/or log the connection in the inspection policy map.

If you want to perform different actions for each match command, you should identify the traffic directly in the policy map.

a. Create the class map by entering the following command:

```
hostname(config)# class-map type inspect im [match-all] class_map_name
hostname(config-cmap)#
```

Where the class_map_name is the name of the class map.The match-all keyword specifies that traffic must match all criteria to match the class map. match-all is the default and only option. The CLI enters class-map configuration mode, where you can enter one or more match commands.

b. (Optional) To add a description to the class map, enter the following command:

```
hostname(config-cmap)# description string
```

Where the string is the description of the class map (up to 200 characters).

c. (Optional) To match traffic of a specific IM protocol, such as Yahoo or MSN, enter the following command:

```
hostname(config-cmap)# match [not] protocol {im-yahoo | im-msn}
```

d. (Optional) To match a specific IM service, such as chat, file-transfer, webcam, voice-chat, conference, or games, enter the following command:

```
hostname(config-cmap)# match [not] service {chat | file-transfer | webcam | voice-chat
| conference | games}
```

e. (Optional) To match the source login name of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] login-name regex {class class_name | regex_name}
```

Where the regex regex_name argument is the regular expression you created in Step 1. The class regex_class_name is the regular expression class map you created in Step 2.

f. (Optional) To match the destination login name of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] peer-login-name regex {class class_name |
regex_name}
```

Where the regex regex_name argument is the regular expression you created in Step 1. The class regex_class_name is the regular expression class map you created in Step 2.

g. (Optional) To match the source IP address of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] ip-address ip_address ip_address_mask
```

Where the ip_address and the ip_address_mask is the IP address and netmask of the message source.
h. (Optional) To match the destination IP address of the IM message, enter the following command:
hostname(config-cmap)# match [not] peer-ip-address ip_address ip_address_mask
Where the ip_address and the ip_address_mask is the IP address and netmask of the message destination.
i. (Optional) To match the version of the IM message, enter the following command:
hostname(config-cmap)# match [not] version regex {class class_name | regex_name}
Where the regex regex_name argument is the regular expression you created in Step 1.
The class regex_class_name is the regular expression class map you created in Step 2.
j. (Optional) To match the filename of the IM message, enter the following command:
hostname(config-cmap)# match [not] filename regex {class class_name | regex_name}
Where the regex regex_name argument is the regular expression you created in Step 1.
The class regex_class_name is the regular expression class map you created in Step 2.

Note Not supported using MSN IM protocol.

Step 4 Create an IM inspection policy map, enter the following command:
hostname(config)# policy-map type inspect im policy_map_name
hostname(config-pmap)#
Where the policy_map_name is the name of the policy map. The CLI enters policy-map configuration mode.
Step 5 (Optional) To add a description to the policy map, enter the following command:
hostname(config-pmap)# description string
Step 6 Specify the traffic on which you want to perform actions using one of the following methods:
Specify the IM class map that you created in Step 3 by entering the following command:
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
Specify traffic Directly in the policy map using one of the match commands described in Step 3. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.
You can specify multiple class or match commands in the policy map. For information about the order of class and match commands.
Step 7 Specify the action you want to perform on the matching traffic by entering the following command:
hostname(config-pmap-c)# {drop-connection | reset | log}
Where the drop-connection action closes the connection. The reset action closes the connection and sends a TCP reset to the client. The log action sends a system log message when this policy map matches traffic.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 46:

What does the activation-key command in the Cisco ASA do?

A. Automatically activates the Cisco ASA, allowing it to be configured right out of the box
B. Applies the activation key to the Cisco ASDM so the Cisco ASA can be managed using a web interface
C. Activates the SSM module in the Cisco ASA, providing intrusion protection and content filtering
D. Applies the activation key to the Cisco ASA operating system, so that the Cisco ASA is licensed and all features are available

Answer: D

QUESTION 47:

An administrator receives a new Cisco ASA. Which command when entered form the console, directs the Cisco ASA to provide interactive prompts that aid in the building of a first-use, minimal configuration?

A. Configure factory default
B. Configure terminal
C. setup
D. Configure startup

Answer: C

QUESTION 48:

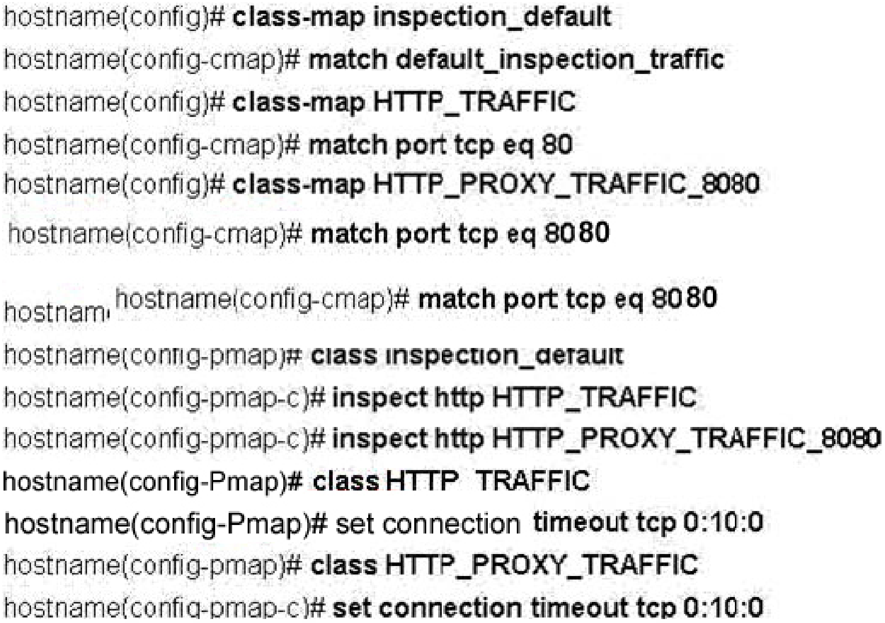
When configuring a crypto ipsec transform-set command, how many unique transforms can a single transform set contain?

A. Four
B. Two
C. One
D. Three

Answer: B

QUESTION 49:

Exhibit:



```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default_inspection_traffic
hostname(config)# class-map HTTP_TRAFFIC
hostname(config-cmap)# match port tcp eq 80
hostname(config)# class-map HTTP_PROXY_TRAFFIC_8080
 hostname(config-cmap)# match port tcp eq 8080

hostnam hostname(config-cmap)# match port tcp eq 8080
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http HTTP_TRAFFIC
hostname(config-pmap-c)# inspect http HTTP_PROXY_TRAFFIC_8080
hostname(config-Pmap)# class HTTP  TRAFFIC
hostname(config-Pmap)# set connection timeout tcp 0:10:0
hostname(config-pmap)# class HTTP_PROXY_TRAFFIC
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

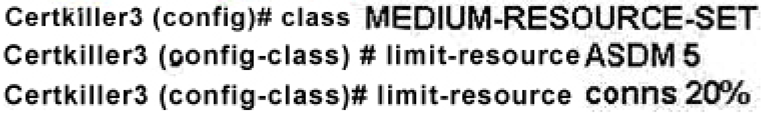
You work as a network technician at Certkiller .com. Please study the exhibit carefully.
What does the inspect http HTTP_TRAFFIC command do in this policy map?

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

Answer: C

QUESTION 50:

Exhibit:



```
Certkiller3 (config)# class MEDIUM-RESOURCE-SET
Certkiller3 (config-class) # limit-resource ASDM 5
Certkiller3 (config-class)# limit-resource conns 20%
```

You work as a network technician at Certkiller .com. Please study the exhibit carefully.
What do these commands accomplish?

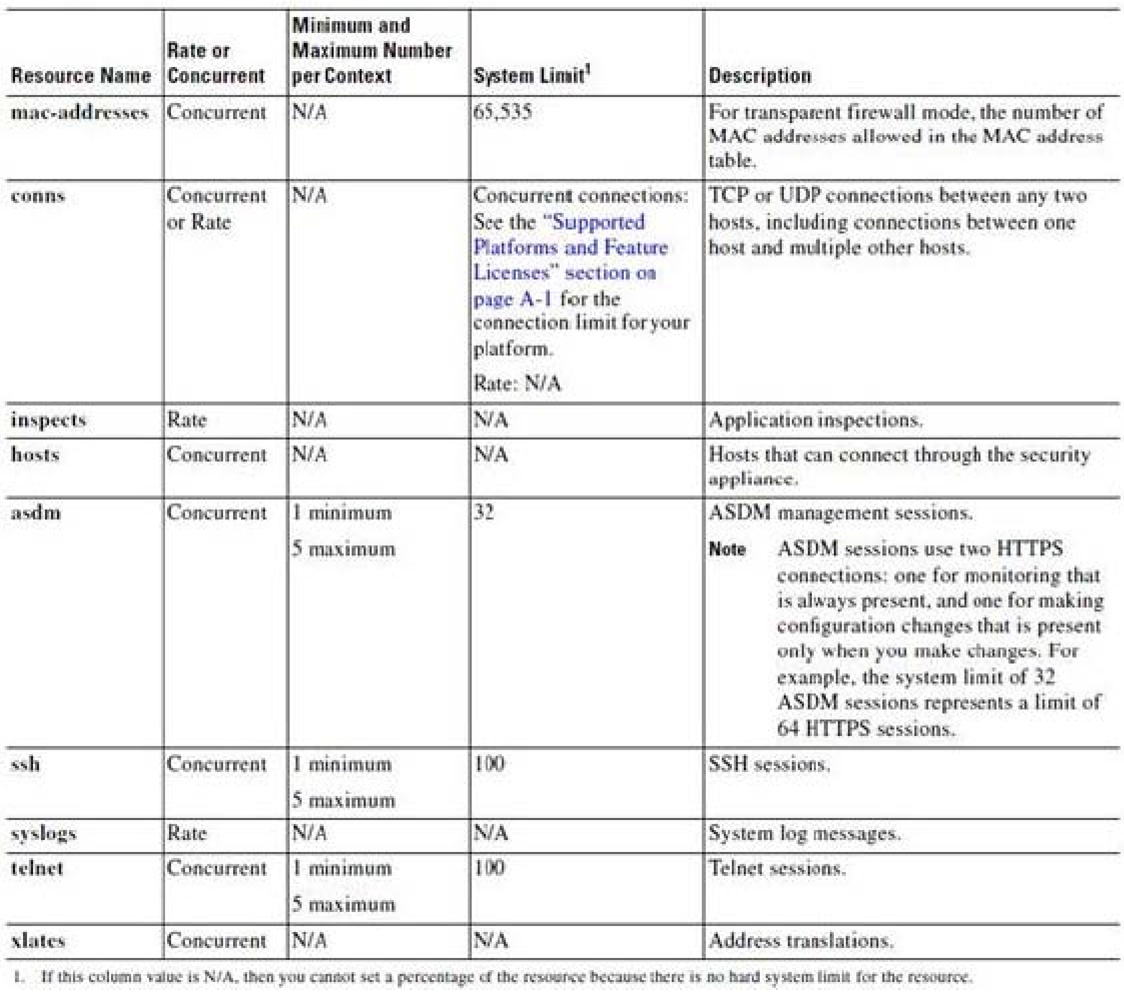
A. They limit the MEDIUM-RESOURCE-SET class to five failed Cisco ASDM connection attempts and 20% of system resources
B. They guarantee five Cisco ASDM sessions and a system connection of 20% for resources belonging to the MEDIUM-RESOURCE-SET class
C. They increase the default Cisco ASDM session limit by five for the

MEDIUM-RESOURCE-SET class and increase the system connection limit by 20%
D. They limit the MEDIUM-RESOURCE-SET class to five Cisco ASDM sessions and 20% of the system connection limit

Answer: D

Explanation:
To set a particular resource limit, enter the following command:
hostname(config-resmgmt)# limit-resource [rate] resource_name number[%]
For this particular resource, the limit overrides the limit set for all. Enter the rate argument to set the rate per second for certain resources. For resources that do not have a system limit, you cannot set the percentage (%) between 1 and 100; you can only set an absolute value. See Table below for resources for which you can set the rate per second and which to not have a system limit.
The table lists the resource types and the limits. See also the show resource types command.

Resource Names and Limits

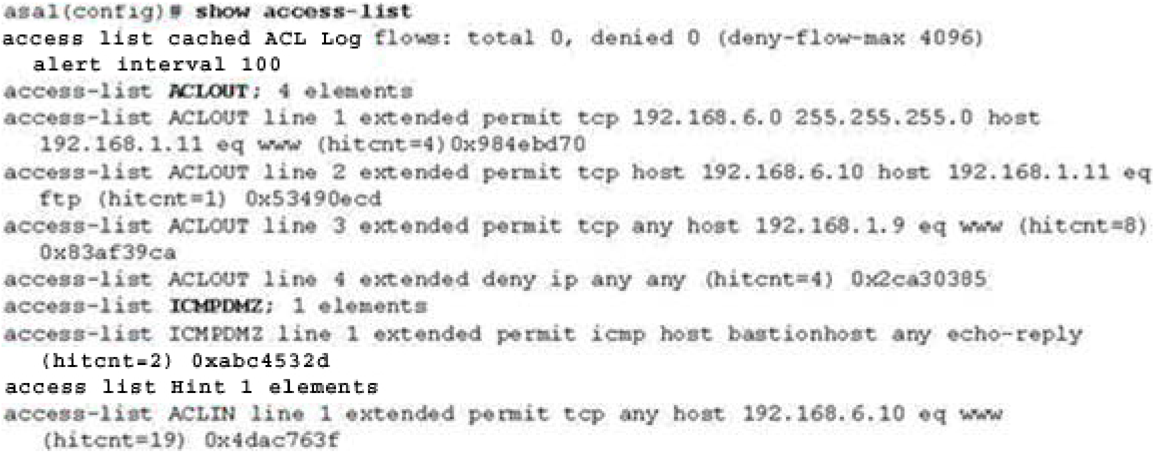


Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
mac-addresses	Concurrent	N/A	65,535	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
conns	Concurrent or Rate	N/A	Concurrent connections: See the "Supported Platforms and Feature Licenses" section on page A-1 for the connection limit for your platform. Rate: N/A	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.
inspects	Rate	N/A	N/A	Application inspections.
hosts	Concurrent	N/A	N/A	Hosts that can connect through the security appliance.
asdm	Concurrent	1 minimum 5 maximum	32	ASDM management sessions. **Note** ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 32 ASDM sessions represents a limit of 64 HTTPS sessions.
ssh	Concurrent	1 minimum 5 maximum	100	SSH sessions.
syslogs	Rate	N/A	N/A	System log messages.
telnet	Concurrent	1 minimum 5 maximum	100	Telnet sessions.
xlates	Concurrent	N/A	N/A	Address translations.

[1] If this column value is N/A, then you cannot set a percentage of the resource because there is no hard system limit for the resource.

QUESTION 51:

Exhibit:



```
asa1(config)# show access-list
access list cached ACL Log flows: total 0, denied 0 (deny-flow-max 4096)
  alert interval 100
access-list ACLOUT; 4 elements
access-list ACLOUT line 1 extended permit tcp 192.168.6.0 255.255.255.0 host
   192.168.1.11 eq www (hitcnt=4)0x984ebd70
access-list ACLOUT line 2 extended permit tcp host 192.168.6.10 host 192.168.1.11 eq
   ftp (hitcnt=1) 0x53490ecd
access-list ACLOUT line 3 extended permit tcp any host 192.168.1.9 eq www (hitcnt=8)
   0x83af39ca
access-list ACLOUT line 4 extended deny ip any any (hitcnt=4) 0x2ca30385
access-list ICMPDMZ; 1 elements
access-list ICMPDMZ line 1 extended permit icmp host bastionhost any echo-reply
   (hitcnt=2) 0xabc4532d
access list Hint 1 elements
access-list ACLIN line 1 extended permit tcp any host 192.168.6.10 eq www
   (hitcnt=19) 0x4dac763f
```

You work as a network technician at Certkiller .com. Please study the exhibit carefully. Based on this output, which of the following statements is true?

A. The ACLOUT access list has been designed to allow the IP address with the network address of 192.168.6.0 to have unrestricted access to the web server at IP address 192.168.1.11
B. The ACLIN access list permits web access from host 192.168.6.10 to all hosts behind the Cisco ASA
C. The IPCMPDMZ access list denies all ICMP traffic bound for the bastion host except echo replies
D. The ACLOUT access list has been designed to deny the IP Address 192.168.1.11 web access to the host with a network address of 192.168.6.0

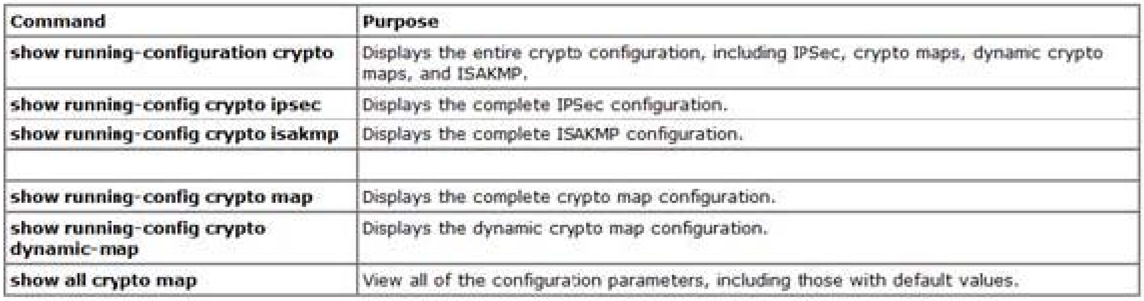
Answer: A

QUESTION 52:

Which of these commands will provide detailed information about the crypto man configurations of a Cisco ASA?

A. show crypto map
B. show ipsec sa
C. show run ipsec sa
D. show run crypto map

Answer: D
Commands to View IPSec Configuration Information



Command	Purpose
show running-configuration crypto	Displays the entire crypto configuration, including IPSec, crypto maps, dynamic crypto maps, and ISAKMP.
show running-config crypto ipsec	Displays the complete IPSec configuration.
show running-config crypto isakmp	Displays the complete ISAKMP configuration.
show running-config crypto map	Displays the complete crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show all crypto map	View all of the configuration parameters, including those with default values.

Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 53:

.Which of these statements regarding Active/Active Failover configurations is correct?

A. Configure two failover groups group1 and group 2
B. Allocate interfaces to failover group using the failover group sub-command mode
C. Configure failover interface parameters in the "ADMIN" Context
D. Use the failover active command to enable Active/Active failover on the Cisco ASA security appliance

Answer: A

QUESTION 54:

Which of these regular expressions would best match the website address www. Certkiller .com/go/ccsp?

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

Answer: D

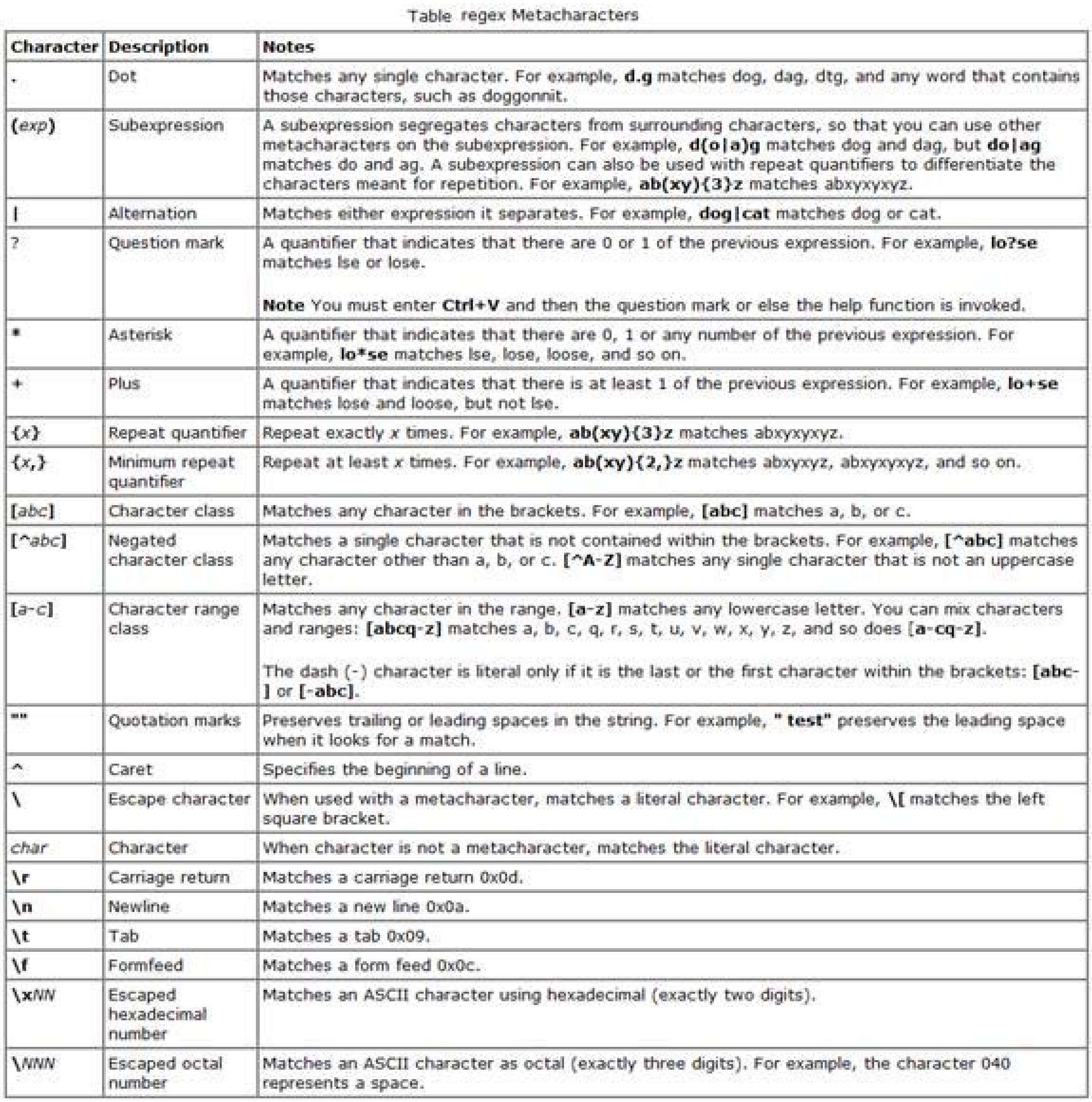


Table regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp*)	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x*}	Repeat quantifier	Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.
{*x*,}	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc*]	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc*]	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a*-*c*]	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does **[a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, **" test"** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, **\[** matches the left square bracket.
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

Reference :Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 55:

With adaptive security appliance code of version 7.0 or later, which three hardware and software requirements must be met before failover can be configured? (Choose three.)

A. Major and minor software releases must match, but software versions do not need to be identical
B. The adaptive security appliances must be the same type of platform
C. RAM, Flash, Modules and interfaces must be identical on each unit
D. Only RAM and interface must be identical on each unit

E. The failover pair must meet hardware and software requirements but can be a PIX and a Cisco ASA

Answer: A,B,C

QUESTION 56:

Which command will provide interface IP information, the interface operational status and the interface configuration method for an adaptive security appliance?

A. Show interface ip brief
B. Show interface stats
C. Show ip interface
D. Show interface detail

Answer: A

QUESTION 57:

An internet user is sending HTTP traffic to a DMZ server with the external address of 192.168.1.4. Which command will redirect HTTP traffic bound for the DMZ web server to its real IP Address of 10.10.11.4?

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

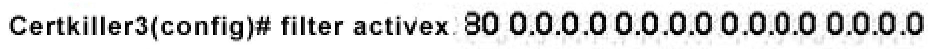
Answer: A

Explanation:
Static NAT creates a fixed translation of real address(es) to mapped address(es).With dynamic NAT and PAT, each host uses a different address or port for each subsequent translation. Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host (if there is an access list that allows it). The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host (if there is an access list that allows it), while dynamic NAT does not. You also need an equal number of mapped addresses as real addresses with static NAT.
To configure static NAT, enter one of the following commands.
For policy static NAT ,enter the following command
hostname(config)# static (real_interface,mapped_interface) {mapped_ip | interface} access-list acl_name [dns] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp

udp_max_conns]
Reference: Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 58:

Exhibit:



```
Certkiller3(config)# filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

You work as a network technician at Certkiller .com. Please study the exhibit carefully.
What is the purpose of this command?

A. To filter ActiveX traffic from the default route
B. To filter Java traffic on HTTP from any host and to any host
C. To filter ActiveX traffic on HTTP from any host and to any host
D. To filter ActiveX traffic once it has been applied to an interface

Answer: C
Enabling ActiveX Filtering
This section describes how to remove ActiveX objects in HTTP traffic passing through the security appliance. To remove ActiveX objects, enter the following command in global configuration mode:
hostname(config)# filter activex port[-port] local_ip local_mask foreign_ip foreign_mask
To use this command, replace port with the TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The http or url literal can be used for port 80. You can specify a range of ports by using a hyphen between the starting port number and the ending port number. The local IP address and mask identify one or more internal hosts that are the source of the traffic to be filtered. The foreign address and mask specify the external destination of the traffic to be filtered. You can set either address to 0.0.0.0 (or in shortened form, 0) to specify all hosts. You can use 0.0.0.0 for either mask (or in shortened form, 0) to specify all hosts. The following example specifies that ActiveX objects are blocked on all outbound connections:
hostname(config)# filter activex 80 0 0 0 0
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2

QUESTION 59:

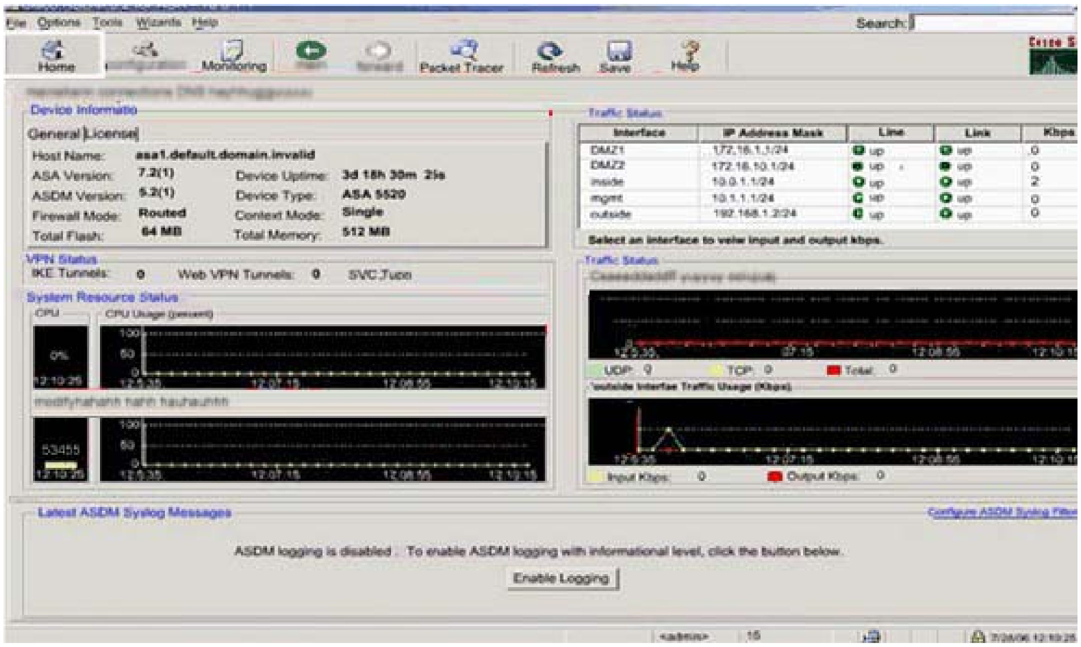
Which commands are necessary in order to add a port for DNS inspection?

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

Answer: D

Certkiller .com Scenario

Cisco ASDM Exhibit:



Host Name: asa1.default.domain.invalid

ASA Version: 7.2(1)   Device Uptime: 3d 18h 30m 2ls

ASDM Version: 5.2(1)   Device Type: ASA 5520

Firewall Mode: Routed   Context Mode: Single

Total Flash: 64 MB   Total Memory: 512 MB

IKE Tunnels: 0   Web VPN Tunnels: 0   SVC Tunn

Interface	IP Address Mask	Line	Link	Kbps
DMZ1	172.16.1.1/24	up	up	0
DMZ2	172.16.10.1/24	up	up	0
inside	10.0.1.1/24	up	up	2
mgmt	10.1.1.1/24	up	up	0
outside	192.168.1.2/24	up	up	0

Select an interface to veiw input and output kbps.

UDP: 0   TCP: 0   Total: 0

'outside' Interfae Traffic Usage (Kbps)

Input Kbps: 0   Output Kbps: 0

ASDM logging is disabled . To enable ASDM logging with informational level, click the button below.

You work as a network administrator at Certkiller c.om. In particular you re handling ASDM administrator. Using the information in the exhibit(s) you must answer the questions of this scenario.
Note: some scenario information might be missing.

Certkiller .com (6 Questions)

QUESTION 60:

Please refer to the Certkiller .com scenario
Which of the following traffic is permitted based on the current access-list configuration?

A. Any IP traffic from any host on the DMZ1 network to any host on the inside.
B. Any IP traffic from any outside host to the 172.16.10.2 host on the DMZ2 network.
C. Any IP traffic from any outside host to the 172.16.1.2 host on the DMZ1 network.
D. FTP traffic from any outside host to the 172.16.1.12 host on the DMZ1 network.
E. HTTP and HTTPS traffic from the 172.16.10.2 DMZ2 host to any host on the outside.

Answer: D

QUESTION 61:

Please refer to the Certkiller .com scenario
How is the address translation feature of the security appliance used in the current configuration? Select two.

A. Static NAT is used to translate the 172.16.1.2 DMZ1 host address to a global address of 192.168.1.10.
B. Static NAT is used to translate the 172.16.10.2 DMZ1 host address to a global address of 192.168.1.12.
C. Port Address Translation (PAT) is used to translate any host on the inside to the 192.168.1.10 global address.
D. Dynamic NAT is used to translate any host on the DMZ1 network and the DMZ2 network to a mapped address from the address pool of 192.168.1.20 to 192.168.1.254.
E. Dynamic NAT is used to translate any host on the inside to a mapped address from the address pool of 192.168.1.20 to 192.168.1.254.

Answer: B, E

QUESTION 62:

Please refer to the Certkiller .com scenario
What is the currently configured default gateway IP address on the security appliance?

A. 10.0.11
B. 172.16.10.1
C. 192.168.1.1
D. 172.16.1.1

Answer: C

QUESTION 63:

Please refer to the Certkiller .com scenario
Which hosts are allowed to mange this security appliance using ASDM or HTTPS?

A. Any host on the 172.16.1.0/24 subnet
B. The 10.0.1.11 host only
C. Any host on the 10.0.0.1/24 subnet

D. Any host on the 172.16.10.0/24 subnet
E. The 172.16.10.2 host only.
F. The 172.16.1.2 host only.

Answer: B

QUESTION 64:

Please refer to the Certkiller .com scenario
Which interface on this security appliance is enabled for DHCP server functionality?

A. All
B. None
C. The inside and DMZ1 interfaces
D. GigabitEthernet 0/0
E. GigabitEthernet 0/1
F. GigabitEthernet 0/2

Answer: E

QUESTION 65:

Please refer to the Certkiller .com scenario
What is the maximum number of VLANs and physical interfaces supported based on the current security appliance software license?

A. 100 VLANs and unlimited interafaces
B. 25 VLANs and 6 interfaces
C. 150 VLANs and 14 interfaces
D. 10 VLANs and 3 interfaces
E. 50 VLANs and 8 interfaces

Answer: A

MIXED QUESTION .

QUESTION 66:

Digital Certificates are used in the Certkiller IPSec connections. What type of network infrastructure device issues digital certificates?

A. SCEP
B. ACS
C. SA
D. CA
E. None of the above.

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 67:

Digital Certificates are used in many of the Certkiller IPSec connections. 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
E. All of the above

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 68:

IPSec is being used to create VPN's in the Certkiller network. 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?

A. 3DES
B. ESP
C. IKE
D. MD5
E. PFS
F. None of the above

Answer: C

Explanation:
According to the "Cisco Secure Virtual Private Networks Study Guide" (ISBN: 1587050331:
Internet Key Exchange (IKE) is a hybrid protocol that provides utility services for IPSec: authentication of the IPSec peers, negotiation of IKE and IPSec security associations, and establishment of keys for encryption algorithms used by IPSec.
NOTE: IKE is synonymous with Internet Security Association Key Management Protocol (ISAKMP) in Cisco router or PIX Firewall configurations.
Reference: http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=3&rl=1

QUESTION 69:

Kathy is the security administrator at Certkiller Inc. and she is configuring a VPN connection. 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 70:

IKE is an integral part of any IPSec based connection. 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 correct answers.

QUESTION 71:

Which of the following choices correctly describe the correct protocol and port number used by the Internet Key Exchange (IKE)?

A. TCP, 123
B. TCP, 132
C. UDP, 500
D. UDP, 1651
E. None of the above

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 72:

You need to configure IKE on a new Certkiller PIX firewall. Which command enables IKE on the outside interface?

A. ike enable outside
B. ipsec enable outside
C. isakmp enable outside
D. ike enable (outbound)
E. None of the above

Answer: C

Explanation:
To configure ISAKMP policies, in global configuration mode, enter the isakmp policy command with its various arguments. The syntax for ISAKMP policy commands is isakmp policy priority attribute_name [attribute_value | integer].
Perform the following steps and use the command syntax in the following examples as a guide. The last step in this sequence defines the answer given in choice C above.
Step1
Set the authentication method. The following example configures preshared key. The priority is 1 in this and all following steps.

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)#
```

Step2
Set the encryption method. The following example configures 3DES.

```
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)#
```

Step3
Set the HMAC method. The following example configures SHA-1.

```
hostname(config)# isakmp policy 1 hash sha
hostname(config)#
```

Step4
Set the Diffie-Hellman group. The following example configures Group 2.

```
hostname(config)# isakmp policy 1 group 2
hostname(config)#
```

Step5
Set the encryption key lifetime. The following example configures 43,200 seconds (12 hours).

```
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)#
```

Step6
Finally, Enable ISAKMP on the interface named outside.

```
hostname(config)# isakmp enable outside
hostname(config)#
```

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008045

QUESTION 73:

NAT is being used within a VPN in the Certkiller network. Which of the following VPN protocols are not recommended to be used with NAT?

A. IKE
B. ESP
C. AES
D. AH
E. 3DES

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 74:

A Certkiller VPN is being created using default IPSEC values. 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 Cisco PIX is Data Encryption Standard (DES).

QUESTION 75:

When configuring transform sets for an IPSec tunnel, how many unique transforms can a single transform set contain?

A. One
B. Two
C. Three
D. Four
E. Five

Answer: C

Explanation:
Sets are limited to up to one AH and up to two ESP transforms
When configuring IPSec, configure a transform set to define how to protect the traffic.
You can configure multiple transform sets (up to three), and then specify one or more of these transform sets in a crypto map
cryptoipsec transform-set transform-set-name transform1 [tcansform2, transform3]
For example:
cryptoipsec transform-set myset1 esp-des esp-sha-hmac
cryptoipsec transform-set myset2 esp-3des esp-sha-hmac
cryptoipsec transform-set aes_set esp-md5-hmac esp-aes-256
In this example, "myset1" and "myset2" and "aes_set" are the names of the transform sets.
Reference: Cisco Security Appliance Command Line Configuration Guide 7.0, Page 23-23

QUESTION 76:

A new Certkiller security appliance is being configured to use tunnel groups. What is one of the purposes of a tunnel group?

A. To group similar IPSec users.
B. To group similar IPSec networks.
C. To group similar IPSec protocols.
D. To identify AAA servers.
E. None of the above

Answer: D

Explanation:
A tunnel group consists of a set of records that contain tunnel connection policies. Tunnel groups contain a small number of attributes that pertain to creating the tunnel itself. Tunnel groups include a pointer to a group policy that defines user-oriented attributes.

The security appliance provides two default tunnel groups, one for LAN-to-LAN connections, and one for remote access connections. You can modify these default tunnel groups, but you cannot delete them. You can also create one or more tunnel groups specific to your environment. Tunnel groups are local to the security appliance and are not configurable on external servers.
Tunnel groups specify the following attributes:
General parameters
IPSec connection parameters
The general parameters include the following:
Tunnel group name-Both remote access and LAN-to-LAN clients select a tunnel group by its name, as follows:
For IPSec clients that use preshared keys to authenticate, the tunnel group name is the same as the group name that the IPSec client passes to the security appliance.
IPSec clients that use certificates to authenticate pass this name as part of the certificate, and the security appliance extracts the name from the certificate.
Tunnel group records contain tunnel connection policy information. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters.
Connection type-Connection types include remote access IPSec, and LAN-to-LAN IPSec. A tunnel group can have only one connection type.
Authentication, Authorization, and Accounting servers-These parameters identify the server groups or lists that the security appliance uses for the following purposes:
Authenticating users
Obtaining information about services users are authorized to access
Storing accounting records
A server group can consist of one or more servers.
Default group policy for the connection-A group policy is a set of user-oriented attributes. The default group policy is the group policy whose attributes the security appliance uses as defaults when authenticating or authorizing a tunnel user.
Client address assignment method-This method includes values for one or more DHCP servers or address pools that the security appliance assigns to clients.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080452488.html

---

QUESTION 77:

You need to configure an IPSec tunnel between two Certkiller locations. When configuring a crypto map, which command correctly specifies the peer to which IPSec-protected traffic can be forwarded?

A. crypto map set peer 192.168.7.2
B. crypto map 20 set-peer insidehost
C. crypto-map policy 10 set 192.168.7.2

D. crypto map peer7 10 set peer 192.168.7.2
E. None of the above

Answer: D

Explanation:
The following steps cover basic IPSec configuration with static crypto maps:
Step 1: Create an access list to define the traffic to protect:
Step 2: Configure a transform set that defines how to protect the traffic. You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map.
Step 3 Create a crypto map by performing the following steps:
a. Assign an access list to a crypto map:
crypto map map-name seq-num match address access-list-name
b. Specify the peer to which the IPSec protected traffic can be forwarded:
crypto map map-name seq-num set peer ip-address
For example: crypto map mymap 10 set peer 192.168.1.100
The security appliance sets ups an SA with the peer assigned the IP address 192.168.1.100.
Specify multiple peers by repeating this command.
Reference: Cisco Security Appliance Command Line Configuration Guide For the Cisco ASA 5500 Series and Cisco PIX 500 Series, page 23-23.

QUESTION 78:

IPSec Dead Peer Detection is being used in the Certkiller network to ensure that dead peers are detected immediately. On which device can Dead Peer Detection be configured when it is used for IPSec remote access?

A. The remote device only.
B. The head-end device only.
C. Both the head-end and remote device.
D. Dead Peer Detection should not be used in IPSec remote access applications.

Answer: C

Explanation:
The IPSec Dead Peer Detection Periodic Message Option feature allows you to configure your router to query the liveliness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.
DPD and Cisco IOS keepalives function on the basis of the timer. If the timer is set for 10 seconds, the router will send a "hello" message every 10 seconds (unless, of course, the router receives a "hello" message from the peer, which means that either end of the

connection can be configured for DPD). The benefit of IOS keepalives and periodic DPD is earlier detection of dead peers. However, IOS keepalives and periodic DPD rely on periodic messages that have to be sent with considerable frequency. The result of sending frequent messages is that the communicating peers must encrypt and decrypt more packets.
Reference:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455afd.html

---

QUESTION 79:

Remote Certkiller users need to connect via a VPN to the Certkiller network through a firewall. What type of tunneling should be used on the VPN Client to allow IPSec traffic through a stateful firewall that may be performing NAT or PAT?

A. GRE/IPSec
B. IPSec over TCP
C. IPSec over UDP
D. Split tunneling
E. L2TP
F. All of the above are acceptable

Answer: C

Explanation:
Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translations (PAT). Transparent tunneling encapsulates Protocol 50 (ESP) traffic within UDP packets and can allow for both IKE (UDP 500) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices and/or firewalls. The most common application for transparent tunneling is behind a home router performing PAT.
Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Be sure to check with your device's vendor to verify whether this limitation exists. Some vendors support Protocol-50 (ESP) Port Address Translation (IPSec passthrough), which might let you operate without enabling transparent tunneling.
To use transparent tunneling, the central-site group in the Cisco VPN device must be configured to support it. For an example, refer to the VPN 3000 Concentrator Manager, Configuration | User Management | Groups | IPSec tab (refer to VPN 3000 Series Concentrator Reference Volume 1: Configuration or Help in the VPN 3000 Concentrator Manager browser).
This parameter is enabled by default. To disable this parameter, uncheck the check box. We recommend that you always keep this parameter checked.
Then choose a mode of transparent tunneling, over UDP or over TCP. The mode you use

must match that used by the secure gateway to which you are connecting. Either mode operates properly through a PAT device. Multiple simultaneous connections might work better with TCP, and if you are in an extranet environment, then in general, TCP mode is preferable. UDP does not operate with stateful firewalls, so in this case, you should use TCP. Therefore, choice B is correct.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide_chapter09186a008015e271.htm

QUESTION 80:

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 81:

Certkiller remote access users connect to the network via a web based VPN. Which type of access list supports filtering for WebVPN?

A. Extended
B. Standard
C. Ethertype
D. Webtype
E. One way

F. None of the above

Answer: D

Explanation:
WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTP(S) Internet sites. WebVPN uses Secure Socket Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.
The following table describes the different types of access lists and some common uses for them, including the webtype shown at the bottom.

Access List Types and Common Uses		
Access List Use	Access List Type	Description
Control network access for IPtraffic (routed and transparent mode)	Extended	The security appliance does not allow any traffic unless it is explicitly permitted by an extendedaccess list.
Identify traffic for AAA rules	Extended	AAA rules use access lists to identify traffic.
Control network access for IP traffic for a given user	Extended, downloaded from a AAA server per user	You can configure the RADIUS server to download a dynamic access list to be applied to the user, or the server can send the name of an access list that you already configured on the security appliance.
Identify addresses for NAT (policy NAT and NATexemption)	Extended	Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses in an extended access list.

Establish VPN access	Extended	You can use an extended access list in VPN commands.
Identify traffic in a traffic class map for Modular Policy	Extended EtherType	Access lists can be used to identify traffic in a class map, which is used for features that support Modular Policy Framework. Features that support Modular Policy Framework include TCP and general connection settings, and inspection.
For transparent firewall mode, control network access for non-IP traffic	EtherType	You can configure an access list that controls traffic based on its EtherType.
WebVPN	Webtype	You can configure a Webtype access list to filter URLs.

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008045

QUESTION 82:

While in global configuration mode, the Certkiller administrator issued the "url-list" command on a Cisco security appliance. What is the purpose of the url-list command in global configuration mode?

A. Allow end users access to URLs.
B. Allow end users access to CIFS shares and URLs.
C. Stop the end user from accessing pre-defined URLs.
D. Configure a set of URLs for Web VPN users to access.
E. List URLs that the end user cannot access.

Answer: D

Explanation:

Use the port forward, url-list, and access-list commands in global configuration mode to configure lists of ports to forward and URLs to present to WebVPN users, and their level of access.
Before you can enter the url-list command in webvpn mode to identify a URL list that you want to display on the WebVPN home page for a group policy, you must create the list. Enter the url-list command in global configuration mode to create one or more lists.
Reference: Cisco Security Appliance Command Line Configuration Guide 7.0, Page 508

QUESTION 83:

A new Certkiller security appliance is being configured for Web VPN. What is the result if the WebVPN url-entry parameter is disabled?

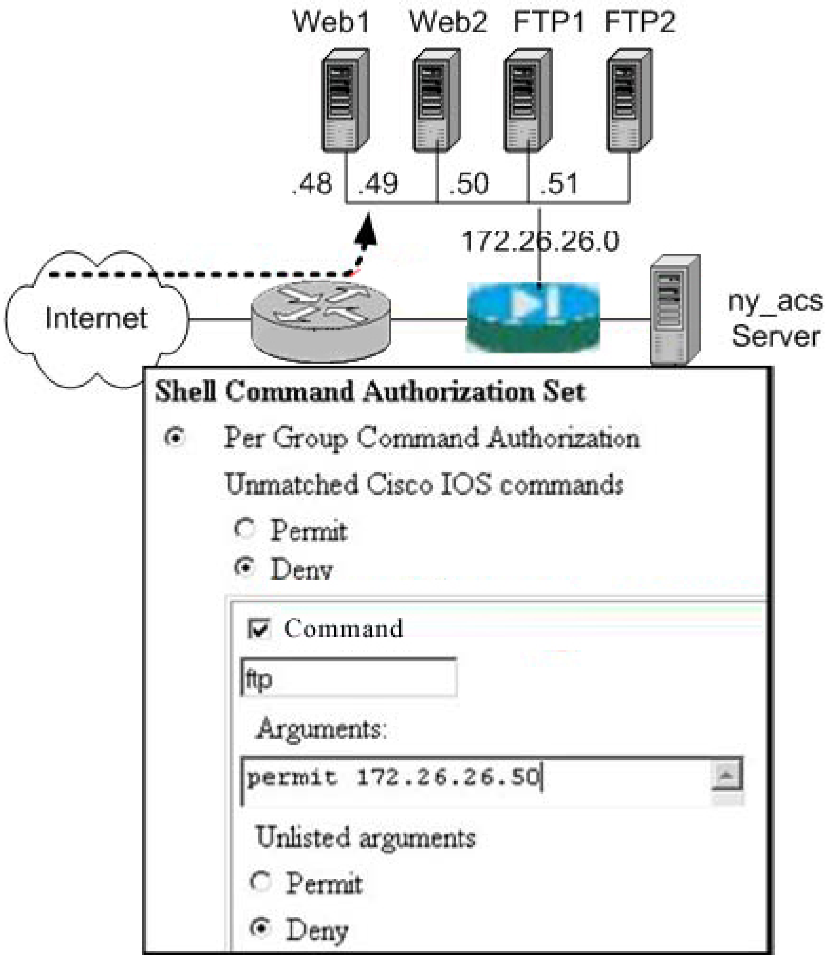
A. The end user is unable to access any CIFS shares or URLs.
B. The end user is able to access CIFS shares but not URLs.
C. The end user is unable to access pre-defined URLs.
D. The end user is able to access pre-defined URLs.

Answer: D

Explanation:
The "url-entry" command enables or disables user entry of URLs. When enabled, the security appliance still restricts URLs with any configured URL or network ACLs. When URL entry is disabled, the security appliance restricts WebVPN users to the URLs on the home page.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008045

QUESTION 84:

The Certkiller network is shown in the following diagram:



Shell Command Authorization Set

● Per Group Command Authorization

Unmatched Cisco IOS commands

○ Permit
● Deny

☑ Command

ftp

Arguments:

permit 172.26.26.50

Unlisted arguments

○ Permit
● Deny

Refer to the exhibit. In the network diagram there are four servers on the DMZ; two web servers and two FTP servers. According to the group configuration in the ny_acs server, when a remote user accesses the security appliance and is authenticated, the user is authorized to perform which two actions? (Choose two)

A. Access any server on the DMZ.
B. Access any FTP server.
C. Access FTP1 server only.
D. Utilize FTP and HTTP protocol to attach to the server.
E. Utilize HTTP protocol only to attach to the server.
F. Utilize FTP protocol only to attach to the server.

Answer: C, F

Explanation:
According to the authorization set shown in this example, everything is being denied by default, except for the single rule allowing access to the server with IP address 172.26.26.50 (which is shown as server FTP1), and only the FTP protocol is allowed as shown by the protocol value within the checked box.

QUESTION 85:

The Certkiller administrator needs to verify the IPSec parameters on a security appliance. Which of the following commands displays the default isakmp policy suite parameters?

A. show crypto isakmp
B. show crypto policy
C. show ipsec isakmp
D. show isakmp policy
E. None of the above

Answer: D

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

QUESTION 86:

A new Certkiller firewall is being configured for transparent mode. How is NAT configured in transparent firewall mode?

A. NAT must be configured on all interfaces.
B. NAT must be configured on all outbound traffic flows.
C. NAT must be configured on all inbound traffic flows.
D. NAT is not configured in transparent firewall mode.

Answer: D

Explanation:
The security appliance can run in two firewall modes:
Routed mode
Transparent mode
In routed mode, the security appliance is considered to be a router hop in the network. It can perform NAT between connected networks, and can use OSPF or passive RIP (in single context mode). Routed mode supports many interfaces. Each interface is on a different subnet. You can share interfaces between contexts.
In transparent mode, the security appliance acts like a "bump in the wire," or a "stealth firewall," and is not a router hop. The security appliance connects the same network on its inside and outside interfaces. No dynamic routing protocols or NAT are used.

However, like routed mode, transparent mode also requires access lists to allow any traffic through the security appliance, except for ARP packets, which are allowed automatically. Transparent mode can allow certain types of traffic in an access list that are blocked by routed mode, including unsupported routing protocols. Transparent mode can also optionally use EtherType access lists to allow non-IP traffic. Transparent mode only supports two interfaces, an inside interface and an outside interface, in addition to a dedicated management interface, if available for your platform.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450b68.html

QUESTION 87:

What can the Certkiller security administrator do to ensure users require authentication for connections through the PIX Firewall using services or protocols that do not support authentication?

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.

QUESTION 88:

Two Certkiller firewalls have been configured for failover to provide network redundancy. During failover, which security appliance attribute does NOT change?

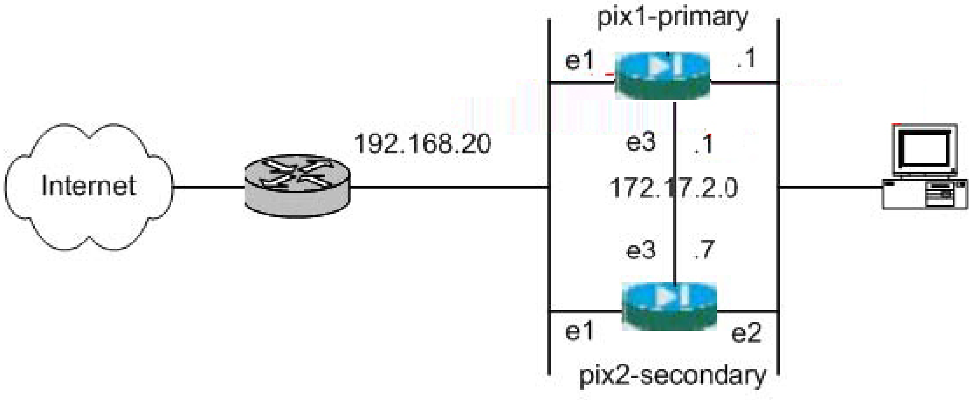
A. Failover unit status-active and standby.
B. Active and standby interfaces-IP address.
C. Failover unit type-primary and secondary.
D. Active and standby interfaces-MAC address.
E. None of the above

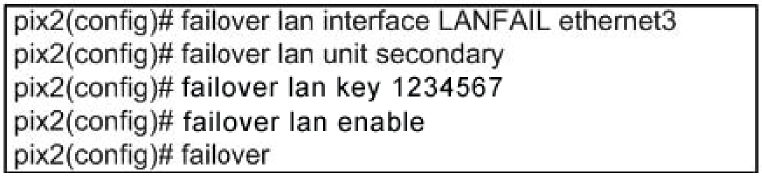
Answer: C

Explanation:
Active/Standby failover lets you use a standby security appliance to take over the functionality of a failed unit. 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 assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network. With failover, the active/standby status of each firewall is unrelated to the primary/secondary unit type status, meaning that it is possible for a secondary unit to become the active firewall.
Primary/Secondary Status and Active/Standby Status
The main differences between the two units in a failover pair are related to which unit is active and which unit is standby, namely which IP addresses to use and which unit actively passes traffic.
However, a few differences exist between the units based on which unit is primary (as specified in the configuration) and which unit is secondary:
The primary unit always becomes the active unit if both units start up at the same time (and are of equal operational health).
The primary unit MAC address is always coupled with the active IP addresses. The exception to this rule occurs when the secondary unit is active, and cannot obtain the primary MAC address over the failover link. In this case, the secondary MAC address is used.
Reference: Cisco Security Appliance Command Line Configuration Guide For the Cisco ASA 5500 Series and Cisco PIX 500 Series, page 11-6.

QUESTION 89:

The Certkiller network perimeter is shown below:





```
pix2(config)# failover lan interface LANFAIL ethernet3
pix2(config)# failover lan unit secondary
pix2(config)# failover lan key 1234567
pix2(config)# failover lan enable
pix2(config)# failover
```

Refer to the exhibit. The Certkiller administrator is configuring the failover link on the secondary unit, pix2, and needs to configure the IP addresses of the failover link. At pix2, which of these additional commands should be entered?

A. pix2(config)# failover lan nip 172.17.2.1 255.255.255.0 standby 172.17.2.7
B. pix2(config)# failover link 172.17.2.7 255.255.255.0 standby 172.17.2.1
C. pix2(config)# failover interface ip LANFAIL 172.17.2.1 255.255.255.0 standby 172.17.2.7
D. pix2(config)# interface ethernet3
pix2(config-if)# failover ip address 172.17.2.7 255.255.255.0 standby 172.17.2.1

Answer: C

Explanation:
To configure the active and failover IP addresses of the PIX for LAN failover, perform the following task:
Assign the active and standby IP address to the failover link:
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
The standby IPaddress must be in the same subnet as the active IPaddress. You do not need to identify the standby address subnetmask.
The failoverlink IP address and MAC address do not change at failover. The active IP address for the failover link always stays with the primary unit, while the standby IP address stays with the secondary unit.
The following is a complete configuration example using LAN failoever:

```
failover
failover lan unit primary
failover lan interface failover Ethernet2
failover lan enable
failover key ******
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
```

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008045

QUESTION 90:

You have configured two Certkiller PIX Firewalls for failover but it is not working. What could you have done that would cause failover to not work correctly? (Choose two)

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

Answer: A, B

Explanation:
You must set a 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 91:

The team at Certkiller Inc. is troubleshooting a non-working failover configuration between two firewalls. Which of the following are the most likely reasons to prevent a 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:
1. Identical PIX Firewall hardware and software versions
2. The failover feature requires two units that are identical in the following respects:
For example, a PIX 515E cannot be used with a PIX 515.
3. Same number and type of interfaces
4. Identical software version
5. Same activation key type (DES or 3DES)
6. Same amount of flash memory
7 Same 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 92:

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.
E. None of the above.

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 93:

Two Certkiller firewalls are configured in an Active/Active fashion. Which of these statements regarding Active/Active failover configurations is correct?

A. Use the failover active command to enable Active/Active failover on the Cisco ASA Security Appliance.
B. Allocate interfaces to a failover group using the failover group sub-command mode.
C. Configure two failover groups: group 1 and group 2.
D. Configure failover interface parameters in the "admin" context.

Answer: C, D

Explanation:
Active/Active failover is only available to security appliances in multiple context mode.
In an
Active/Active failover configuration, both security appliances can pass network traffic.
In Active/Active failover, you divide the security contexts on the security appliance into failover groups.
A failover group is simply a logical group of one or more security contexts. You can create a maximum of two failover groups on the security appliance. The admin context is always a member of failover group 1, and any unassigned security contexts are also members of failover group 1 by default.
The failover group forms the base unit for failover in Active/Active failover. Interface failure monitoring, failover, and active/standby status are all attributes of a failover group, rather than the unit. When an active failover group fails, it changes to the standby state while the standby failover group becomes active. The interfaces in the failover group that becomes active assume the MAC and IP addresses of the interfaces in the failover group that failed. The interfaces in the failover group that is now in the standby state take over the standby MAC and IP addresses.
As in Active/Standby failover, one unit in an Active/Active failover pair is designated the primary unit, and the other unit the secondary unit. Unlike Active/Standby failover, this designation does not indicate which unit becomes active when both units start simultaneously. Instead, the primary/secondary designation determines which unit provides the running configuration to the pair and on which unit each failover group appears in the active state when both start simultaneously.
Each failover group in the configuration is given a primary or secondary unit preference. This preference determines on which unit in the failover pair the contexts in the failover

group appear in the active state when both units start simultaneously. You can have both failover groups be in the active state on a single unit in the pair, with the other unit containing the failover groups in the standby state. However, a more typical configuration is to assign each failover group a different role preference to make each one active on a different unit, balancing the traffic across the devices.
Incorrect Answers:
A: This command is used to failover the active PIX, forcing the secondary PIX to take over as the active one.
B: A sub-command configuration is not used.

QUESTION 94:

The following was issues on a Certkiller security appliance:

```
CKSA-2# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: lanfail Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Group 1 last failover at: 15.54.49 UTC Jun 14 2005
Group 2 last failover at: 15.55.00 UTC Jun 14 2005
```

Refer to the "show failover" output shown above. This security appliance is configured for what two types of failover? (Choose two)

A. Unit-based failover
B. LAN based failover
C. Stateful failover
D. Active/Standby failover
E. Active/Active failover
F. Context/Group failover

Answer: B, E

Explanation:
Active/Active failover is only available to security appliances in multiple context mode. In an Active/Active failover configuration, both security appliances can pass network traffic.
In Active/Active failover, you divide the security contexts on the security appliance into failover groups. A failover group is simply a logical group of one or more security contexts. You can create a maximum of two failover groups on the security appliance. The admin context is always a member of failover group1, and any unassigned security

contexts are also members of failover group 1 by default.
The failover group forms the base unit for failover in Active/Active failover. Interface failure monitoring, failover, and active/standby status are all attributes of a failover group, rather than the unit.
In this example, it can be seen that LAN based failover is being used as opposed to using a failover cable. This can be seen by the "Cable status: N/A - LAN-based failover enabled" output, making choice B correct. E is also correct due to the fact that there are two failover groups shown here, meaning that an active/active configuration is used.

QUESTION 95:

The Certkiller security admin has issued the "show failover" command and the status shows a "waiting" state. What does this state mean?

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 started.
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

Explanation:
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.

QUESTION 96:

A Certkiller security appliance is being configured to support the use of external AAA servers. 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. KERBOROS+

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 due to scalability issues.

QUESTION 97:

AAA is being implemented within the Certkiller network. What are the three parts of AAA? (Choose all that apply)

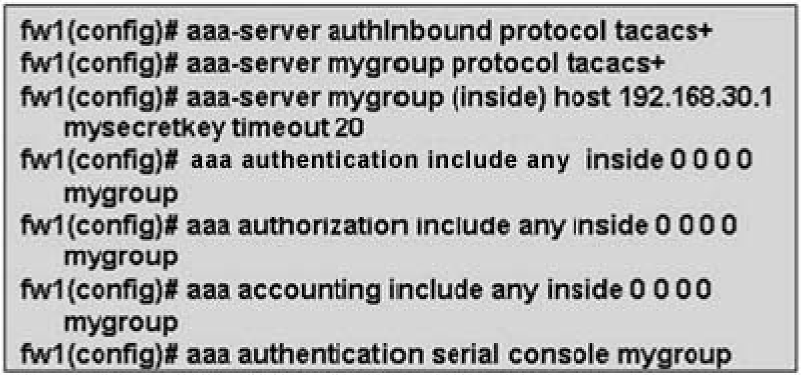
A. Administration
B. Authorization
C. Accounting
D. Authentication
E. Auditing

Answer: B, C, D

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

QUESTION 98:

Part of the configuration file of a Certkiller firewall is shown below:



```
fw1(config)# aaa-server authInbound protocol tacacs+
fw1(config)# aaa-server mygroup protocol tacacs+
fw1(config)# aaa-server mygroup (inside) host 192.168.30.1
     mysecretkey timeout 20
fw1(config)#  aaa authentication include any  inside 0 0 0 0
     mygroup
fw1(config)# aaa authorization include any inside 0 0 0 0
     mygroup
fw1(config)# aaa accounting include any inside 0 0 0 0
     mygroup
fw1(config)# aaa authentication serial console mygroup
```

Refer to the exhibit shown above. Given this configuration, what traffic will be logged to the AAA server?

A. All connection information will be logged in the accounting database.
B. All outbound connection information will be logged in the accounting database.

C. Only the authenticated console connection information will be logged in the accounting database.
D. This is not a valid configuration because TACAS+ connection information cannot be captured and logged.
E. No traffic will be logged

Answer: B

Explanation:
The "include" option is used to enable, disable, or view TACACS+ or RADIUS user authentication, authorization, and accounting for the server previously designated with the aaa-server command. In the configuration shown above, all traffic sourced from the inside network to anywhere (all outbound traffic). An example outbound AAA configuration using RADIUS instead of TACACS is found in the link shown below.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_configuration_guide_chapter09186a00801fd

QUESTION 99:

The security administrator at Certkiller is working on configuring a PIX Firewallfor AAA. 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, page 12-12

QUESTION 100:

You are having problems with HTTP authentication on a new Certkiller security appliance. You have configured the security appliance and an AAA server for authentication. Why does Telnet and FTP authentication work normally but HTTP authentication does not?

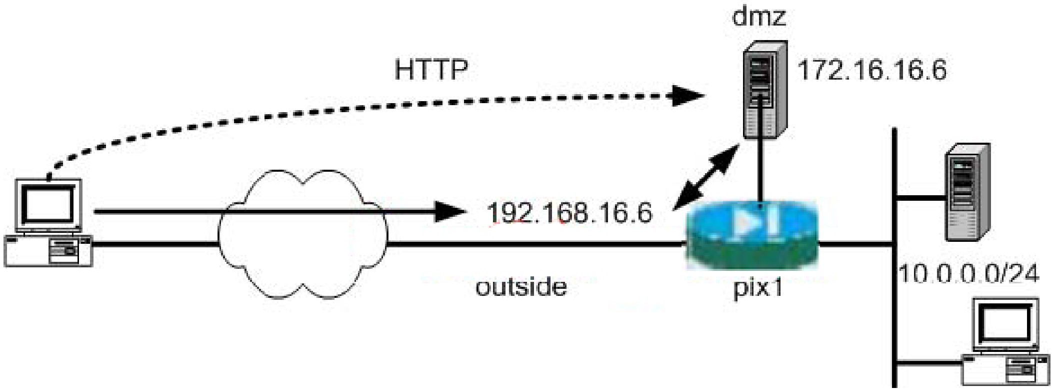
A. The AAA server is not properly configured to accept HTTP authentication requests.
B. You have not enabled HTTP authorization, which is required for HTTP authentication.
C. You must specify HTTPS authentication in your configuration.
D. HTTP re-authentication may be taking place with the web browser sending the cached username and password back to the security appliance.

Answer: D

Explanation:
HTTP Authentication
When using HTTP authentication to a site running Microsoft IIS that has "Basic text authentication" or "NT Challenge" enabled, users might be denied access from the Microsoft IIS server. This occurs because the browser appends the string: "Authorization: Basic=Uuhjksdkfhk==" to the HTTP GET commands. This string contains the security appliance authentication credentials.
Windows NT Microsoft IIS servers respond to the credentials and assume that a Windows NT user is trying to access privileged pages on the server. Unless the security appliance username-password combination is exactly the same as a valid Windows NT username and password combination on the
Microsoft IIS server, the HTTP GET command is denied.
To solve this problem, the security appliance provides the virtual http command, which redirects the browser's initial connection to another IP address, authenticates the user, then redirects the browser back to the URL that the user originally requested.
Once authenticated, a user never has to reauthenticate, no matter how low the security appliance uauth timeout is set, because the browser caches the "Authorization: Basic=Uuhjksdkfhk==" string in every subsequent connection to that particular site. This can be cleared only when the user exits all instances of Netscape Navigator or Internet Explorer and restarts. Flushing the cache is of no use.
As long as the user repeatedly browses the Internet, the browser resends the "Authorization:
Basic=Uuhjksdkfhk==" string to transparently reauthenticate the user.
Multimedia applications such as CU-SeeMe, Intel Internet Phone, MeetingPoint, and MS NetMeeting silently start the HTTP service before an H.323 session is established from the inside to the outside.
Network browsers such as Netscape Navigator do not present a challenge value during authentication; therefore, only password authentication can be used from a network browser.
Reference: Cisco Security Appliance Command Reference for the Cisco ASA 5500 Series and Cisco PIX 500 Series, page 2-20.

QUESTION 101:

The Certkiller network is shown in the display below:



The Certkiller network administrator for this small site shown above has chosen to authenticate HTTP cut-through proxy traffic via a local database on the Cisco PIX Security Appliance. Which command strings should the administrator enter to accomplish this?

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) 192.168.16.6 172.16.16.16
pix1(config)# access-list 150 permit tcp any host 192.168.16.6 eq www
pix1(config)# aaa authentication match 150 outside pix 1
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

Explanation:
Choice D is correct as the source traffic that needs to be authenticated is 192.168.16.6, and the PIX needs to be configured to authenticate traffic as shown in the access list in choice D. In this access list, only web traffic sourced from 192.168.16.6 should be authenticated using the local user database configured on the PIX.
Incorrect Answers:
A: Since the initial traffic is coming from 192.168.16.6 (before NAT) the access list should use this IP address, and not 172.16.16.6
B: To configure authentication using the local user database configured on the PIX, use the "local" keyword, not the "pix 1" keyword. Using the "pix 1" phrase is invalid.
C: In this choice, both the IP address used in the access list is incorrect, as well as the use of the invalid "pix 1" keyword instead of the local keyword.

QUESTION 102:

Authorization services have been applied on a new Certkiller appliance. Which is a method of identifying the traffic requiring authorization on the security appliance?

A. Implicitly enabling TACAS+ authorization rules in the response packet.
B. Specifying ACLs that authorization rules must match.
C. Independently interpreting authorized rules before authentication has occurred to decrease overall AAA processing time.
D. Checking the authentication rules for a match thus allowing the traffic to be authorized.
E. None of the above

Answer: B

Explanation:
Access lists are made up of one or more Access Control Entries. An ACE is a single entry in an access list that specifies a permit or deny rule, and is applied to a protocol, a source and destination IPaddress or network, and optionally the source and destination ports.
Access lists are used in a variety of feature, as shown by the table below:

Access List Types and Common Uses

Access List Use	**Access List Type**	**Description**
Control network access for IPtraffic (routed and transparent mode)	Extended	The security appliance does not allow any traffic unless it is explicitly permitted by an extendedaccess list.
Identify traffic for AAA rules	**Extended**	**AAA rules use access lists to identify traffic.**
Control network access for IP traffic for a given user	Extended, downloaded from a AAA server per user	You can configure the RADIUS server to download a dynamic access list to be applied to the user, or the server can send the name of an access list that you already configured on the security appliance.

Identify addresses for NAT (policy NAT and NATexemption)	Extended	Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses in an extended access list.
Establish VPN access	Extended	You can use an extended access list in VPN commands.
Identify traffic in a traffic class map for Modular Policy	Extended EtherType	Access lists can be used to identify traffic in a class map, which is used for features that support Modular Policy Framework. Features that support Modular Policy Framework include TCP and general connection settings, and inspection.
For transparent firewall mode, control network access for non-IP traffic	EtherType	You can configure an access list that controls traffic based on its EtherType.
Filtering for WebVPN	Webtype	You can configure a Webtype access list to filter URLs.

Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450bf0.html

QUESTION 103:

On a new Certkiller PIX, an access group was created using the "per-user-override" keyword. What is the effect of the per-user override option when applied to the access-group command syntax?

A. It increases security by building upon the existing access list applied to the interface. All subsequent users are also subject to the additional access list entries.
B. The log option in the per-user access list overrides existing interface log options.

C. It allows downloadable user access lists to override the access list applied to the interface.
D. It allows for extended authentication on a per-user basis.
E. None of the above.

Answer: C

Explanation:
To apply an extended access list to the inbound or outbound direction of an interface, enter the following command:
hostname(config)# access-groupaccess_list_name {in | out} interface interface_name [per-user-override]
You can apply one access list of each type (extended and EtherType) to both directions of the interface.
The per-user-override keyword allows dynamic access lists that are downloaded for user authorization to override the access list assigned to the interface. For example, if the interface access list denies all traffic from 10.0.0.0, but the dynamic access list permits all traffic from 10.0.0.0, then the dynamic access list overrides the interface access list for that user. The per-user-override keyword is only available for inbound access lists.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450b93.html

QUESTION 104:

A Certkiller security appliance needs to have a large number of ACL configuration lines applied to it. 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:
Downloadable ACLs enable you to enter an ACL once, in Cisco Secure ACS, and then load that ACL to any number of PIX Firewalls. Downloadable 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 105:

A Certkiller security appliance is being configured to use multiple AAA servers for redundancy. By default, 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
F. 5

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 106:

A Certkiller security appliance is being configured to support the use of AAA servers. 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 107:

What is displayed as a result of entering the command syntax "show aaa-server group1 host 192.168.30.166" in the security appliance?

A. aaa-server configuration for a particular host in server group group1
B. aaa-server statistics for a particular host in server group group1
C. aaa-server configuration for server group group1
D. aaa-server statistics for the host group1 at IP address 192.168.30.166

Answer: B

Explanation:
To display AAA server statistics for AAA servers, use the show aaa-server command in privileged
EXEC mode: The optional "host hostname" keywords how statistics for a particular server in the group.

```
showaaa-server [LOCAL | groupname [host hostname] | protocol protocol]
```

Example:
This example shows the use of the show aaa-server command to display statistics for a particular host in server group group1:

```
hostname(config)# show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: ACTIVE/FAILED. Last transaction (success) at 11:10:08 UTC Fri Aug 22
Number of pending requests 20
Average round trip time4ms
Number of authentication requests20
```

Reference: Cisco Security Appliance Command Reference For the Cisco ASA 5500 Series and Cisco PIX 500 Series Software Version 7.0.4 Page 1480.

QUESTION 108:

DHCP needs to be set up on a new Certkiller location. 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 109:

A new Certkiller firewall needs to act as a DHCP server for a small office. How do you enable this PIX to act as a DHCP server for clients in this network?

A. ip address inside dhcp
B. dhcpd enable inside
C. interface inside dhcpd enable
D. interface inside dhcp server
E. None of the above

Answer: B

Explanation:
Enable the DHCP server function on the PIX inside interface with the "dhcpd enable inside" command. Only the inside interface can have the dhcp server enabled.

QUESTION 110:

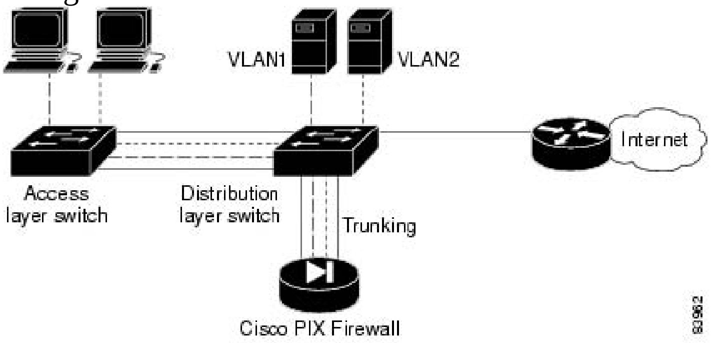
A new Certkiller PIX is installed on the network, and VLAN support needs to be configured on it. What is the minimum number of physical interfaces that is required for all security appliance platforms to support VLANs?

A. One

B. Two
C. Three
D. Four
E. Five

Answer: A

Explanation:
Only a single physical interface is needed to firewall logical VLAN interfaces as shown in the diagram below:
Using a PIX Firewall to Interconnect VLANs



In the diagram shown above, two VLANs are configured on two switches. Workstations are connected to the access layer switch, while servers are connected to the distribution layer switch. Links using the 802.1q protocol interconnect the two switches and the PIXFirewall. The 802.1q protocol allows trunking VLAN traffic between devices, which means that traffic to and from multiple VLANs can be transmitted over a single physical link. Each packet contains a VLAN tag that identifies the source and destination VLAN. The PIXFirewall supports 802.1q, allowing it to send and receive traffic for multiple VLANs on a single interface.
In this example the PIXFirewall is configured with only one physical and one logical interface assigned to VLAN 2 and VLAN 3. The PIXFirewall interconnects the two VLANs, while providing firewall services, such as access lists, to improve network security.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017

QUESTION 111:

A new Certkiller firewall was configured for subinterfaces on one of the links. How do you ensure that the main interface does not pass untagged traffic when using subinterfaces?

A. Use the shutdown command on the main interface.

B. Omit the nameif command on the subinterface.
C. Use the vlan command on the main interface.
D. Omit the nameif command on the main interface.
E. Use the shutdown and then use the nameif command on the main interface.

Answer: D

Explanation:
You can only assign a single VLAN to a subinterface, and not to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the no option; you can enter the vlan command with a different VLAN ID, and the security appliance changes the old ID. You need to enable the physical interface with the no shutdown command tolet subinterfaces be enabled. If you enable subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Therefore, you cannot prevent traffic from passing through the physical interface by bringing down the interface. Instead, ensure that the physical interface does not pass traffic by leaving out the nameif command. If you want to let the physical interface pass untagged packets, you can configure the nameif command as usual.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_command_reference_chapter09186a0080452780.html

QUESTION 112:

Dynamic Routing is being configured on one of the Certkiller security appliances. What are the two purposes of the network area subcommand? (Choose two)

A. It defines the interfaces on which OSPF runs.
B. It defines the interfaces on which RIP runs.
C. It defines the OSPF area the interface belongs to.
D. It separates the public area from the private area.
E. It defines the OSPF area type.

Answer: A, C

Explanation:
To define the IP addresses on which OSPF runs and to define the area ID for that interface, enter the following command:

```
hostname(config-router)# network ip_address mask area area_id
```

The following example shows how to enable OSPF:

```
hostname(config)# router ospf 2
hostname(config-router)# network 10.0.0.0 255.0.0.0 area 0
```

In this example, all interfaces that are configured on the PIX with an IP address in the 10.X.X.X range will be configured to belong to OSPF area 0.

QUESTION 113:

The Certkiller network is using PIM sparse mode in their IP multicast implementation. What are two instances when sparse-mode PIM is most useful? (Choose two)

A. When there are few receivers in a group.
B. When there are many receivers in a group.
C. When the type of traffic is intermittent.
D. When the type of traffic is constant.
E. When the traffic is not ethertype.
F. When the traffic is ethertype.

Answer: A, C

Explanation:
Sparse multicast is most useful when:
1. There are few receivers in a group.
2. Senders and receivers are separated by WAN links.
3. The type of traffic is intermittent.
Sparse-mode PIM is optimized for environments where there are many multipoint data streams. Each data stream goes to a relatively small number of the LANs in the internetwork. For these types of groups, Reverse Path Forwarding techniques waste bandwidth. Sparse-mode PIM works by defining a Rendezvous Point. When a sender wants to send data, it first sends to the Rendezvous Point. When a receiver wants to receive data, it registers with the Rendezvous Point. Once the data stream begins to flow from sender to Rendezvous Point to receiver, the routers in the path will optimize the path automatically to remove any unnecessary hops. Sparse-mode PIM assumes that no hosts want the multicast traffic unless they specifically ask for it.
Reference: http://www.cisco.com/warp/public/614/17.html

QUESTION 114:

IP multicast needs to be configured on a new Certkiller PIX firewall. Which statements about the security appliance's multicasting capabilities are true? (Choose two)

A. When the PIX security appliance is configured for Stub Multicast Routing, it is necessary to construct GRE tunnels to allow multicast traffic to bypass the PIX security

appliance.
B. The security appliance supports Stub Multicast Routing.
C. The PIX supports PIM and DVRMP and MOSPF.
D. The PIX security appliance can be configured to act as an IGMP proxy agent.

Answer: B, D

Explanation:
The security appliance supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single security appliance.
Stub multicast routing provides dynamic host registration and facilitates multicast routing. When configured for stub multicast routing, the security appliance acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the security appliance forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for stub multicast routing, the security appliance cannot be configured for PIM.
The security appliance supports both PIM-SM and bi-directional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a single Rendezvous Point per multicast group and optionally creates shortest-path trees per multicast source.
Reference: Cisco Security Appliance Command Line Configuration Guide 7.0, p. 8-17

QUESTION 115:

To enable multicast forwarding on a PIX outside interface, which of the following commands should the Certkiller security 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
E. None of the above

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 116:

The security administrator at Certkiller 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 to use the igmp join-group command to enable the PIX Firewall to forward IGMP reports.
B. It is necessary to use the multicast interface command to enable multicast forwarding on each PIX Firewall interface.
C. It is necessary to use the igmp forward command to enable multicast forwarding on each PIX Firewall interface.
D. It is necessary to use the mroute command to create a static route from the transmission source to the next-hop router interface.
E. It is necessary 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 example, 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, Chapter 9, pages 13-14.

QUESTION 117:

The security administrator at Certkiller wants to enable the PIX Firewall to permit hosts on different interfaces to ping each other. What command should be used to accomplish this?

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 118:

An administrator is defining a modular policy. As part of the policy, the administrator wants to define a traffic flow between Internet hosts and a specific web server on the DMZ. Which command should the administrator use?

A. class-map http_traffic
match port tcp eq www
B. class-map http_traffic
match flow ip destination address 192.168.1.11
C. class-map http_traffic
match set 192.168.1.11
D. access-list 150 permit tcp any host 192.168.1.11 eq www
class-map http_traffic
match access-list 150

Answer: D

Explanation:
Modular Policy Framework provides a consistent and flexible way to configure security appliance features in a manner similar to Cisco IOS software QoS CLI. For example, you can use Modular Policy
Framework to create a timeout configuration that is specific to a particular TCP

application, as opposed to one that applies to all TCP applications.
The following is an example for the class-map command:

```
CK1 (config)# access-list 101 permit tcp any any eq www
CK1 (config)# class-map all_www
CK1 (config-cmap)# match access-list 101
CK1 (config-cmap)# exit
```

Reference: Cisco Security Appliance Command Line Configuration Guide 7.0, p. 18-4

QUESTION 119:

After a new Cisco PIX was installed, some Certkiller users are experiencing problems using FTP. If the FTP protocol inspection is not enabled for a given port, which two statements are true? (Choose two)

A. Outbound standard FTP will work properly on that port.
B. Outbound passive FTP will not work properly on that port.
C. Outbound standard FTP will not work properly on that port.
D.
Inbound standard FTP will not work properly on that port even if the traffic to the inside server is permitted by an access element.
E. Outbound passive FTP will work properly on that port as long as outbound traffic is not explicitly disallowed.

Answer: C, E

Explanation:
The FTP application inspection inspects FTP sessions and performs four tasks:
Prepares a dynamic secondary data connection
Tracks the ftp command-response sequence
Generates an audit trail
NATs the embedded IP address
FTP application inspection prepares secondary channels for FTP data transfer. The channels are allocated in response to a file upload, a file download, or a directory listing event, and they must be prenegotiated. The port is negotiated through the PORT or PASV (227) commands.
You can use the fixup command to change the default port assignment for FTP. The command syntax is as follows:

```
[no] fixup protocol ftp [strict] [port]
```

The port option lets you configure the port at which the PIX listens for FTP traffic.
The strict option prevents web browsers from sending embedded commands in FTP requests. Each ftp command must be acknowledged before a new command is allowed. Connections sending embedded commands are dropped. The strict option only lets the server generate the PASV reply command (227) and only lets the client generate the PORT command. The PASV reply and PORT commands are checked to ensure that they do not appear in an error string.
If you disable FTP fixups with the no fixup protocol ftp command, outbound users can

start connections only in passive mode, and all inbound FTP is disabled.
Note: The Cisco PIX protocol inspection configuration is new to PIX 7.0, and replaces the "fixup" protocol configuration statements. An FTP map will be used instead.
Reference: CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide, Cisco Press, page 123.

QUESTION 120:

When an outside FTP client accesses a corporation's dmz FTP server through a security appliance, the Certkiller administrator wants the security appliance to restrict ftp commands that can be performed by the client. Which security appliance commands enable the administrator to restrict the ftp client to performing a specific set of ftp commands.

A. ftp-map inbound_ftp
request-command deny appe dele rm
B. ftp-map inbound_ftp
request-command permit get put cdup
C. policy-map inbound
class inbound_ftp_traffic
inspect ftp strict get put cdup
D. policy-map inbound
class inbound_ftp_traffic
inspect ftp strict appe dele rmd

Answer: A

Explanation:
Configuring FTP Inspection:
FTP application inspection is enabled default, so you only need to perform the procedures in this section if you want to change the default FTP configuration, in any of the following ways:
Enable the strict option.
Identify specific FTP commands that are not permitted to pass through the security appliance.
Change the default port number.
To change the default configuration for FTP inspection, perform the following steps:
Step1
Name the traffic class by entering the following command in global configuration mode:
hostname(config)# class-map class_map_name
Replace class_map_name with the name of the traffic class, as in the following example:
hostname(config)# class-map ftp_port
When you enter the class-map command, the CLI enters the class map configuration mode, and the prompt changes, as in the following example:
hostname(config-cmap)#
Step2

In the class map configuration mode, define the match command, as in the following example:

```
hostname(config-cmap)# match port tcp eq 23
hostname(config-cmap)# exit
hostname(config)#
```

To assign a range of continuous ports, enter the range keyword, as in the following example:

```
hostname(config-cmap)# match port tcp range 1023-1025
```

To assign more than one non-contiguous port for FTP inspection, enter the access-list command and define an access control entry to match each port. Then enter the match command to associate the access lists with the FTP traffic class.

Step3

Create an FTP map by entering the following command:

```
hostname(config)# ftp-map ftp_map_name
```

Replace ftp_map_name with the name of the FTP map, for example:

```
hostname(config)# ftp-map inbound_ftp
```

The system enters FTP map configuration mode and the CLI prompt changes as in the following example:

```
hostname(config-ftp-map)#
```

Step4

Define the configuration of the FTP map by entering the following command:

```
hostname(config-ftp-map)# request-command deny ftp_command
hostname(config-ftp-map)# exit
hostname(config)#
```

Replace ftp_command with one or more FTP commands that you want to restrict. See the table below for a list of the FTP commands that you can restrict. For example, the following command prevents storing or appending files:

```
hostname(config-inbound_ftp)# request-command deny put stou appe
```

Table of FTP Map request-command deny Options	
request-command deny Option	**Purpose**
appe	Disallows the command that appends
	to a file.
cdup	Disallows the command that changes
	to the parent directory of the current
	working directory.
dele	Disallows the command that deletes a

	file on the server.
get	Disallows the client command for retrieving a file from the server.
help	Disallows the command that provides
	help information.
mkd	Disallows the command that makes a
	directory on the server.
put	Disallows the client command for sending a file to the server.
rmd	Disallows the command that deletes a
	directory on the server.
rnfr	Disallows the command that specifies
	rename-from filename.
rnto	Disallows the command that specifies
	rename-to filename.
site	Disallows the command that are
	specific to the server system. Usually
	used for remote administration.
stou	Disallows the command that stores a
	file using a unique file name.

Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450d38.html#w

QUESTION 121:

The Certkiller administrator wants to protect against spoofing attacks on the LAN.
Which feature prevents ARP spoofing?

A. ARP fixup
B. ARP inspection
C. MAC fixup
D. MAC inspection
E. All of the above

Answer: B

Explanation:
By default, all ARP packets are allowed through the security appliance. You can control the flow of ARP packets by enabling ARP inspection.
When you enable ARP inspection, the security appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:
If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet.
If the ARP packet does not match any entries in the static ARP table, then you can set the security appliance to either forward the packet out all interfaces (flood), or to drop the packet.
ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.
ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.
Reference: Cisco Security Appliance Command Line Configuration Guide for the Cisco ASA 5500 Series and Cisco PIX 500 Series, chapter 22.

QUESTION 122:

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

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

QUESTION 123:

The Certkiller network is installing an IPS device to mitigate the threat of outside attacks. The inline IPS software feature set is available in which security appliances?

A. Any Cisco PIX and ASA Security Appliance running v.7 software and an AIP-SSM module.
B. Only Cisco PIX 515, 525, and 535 Security Appliances with an AIP-SSM module.
C. Only Cisco ASA 5520 and 5540 Security Appliances with an AIP-SSM module.
D. Any Cisco ASA 5510, 5520, or 5540 Security Appliances with an AIP-SSM module.

Answer: D

Explanation:
Cisco IPS Sensor software Version 5 delivers inline IPS capabilities to Cisco IPS 4200 Series sensors; Cisco Catalyst(r) 6500 Series IPSM-2 modulesand the AIP SSM Module for the Cisco Adaptive Security Appliance, which offers full IPS features within a converged appliance, allallowing effective worm and virus mitigation at strategic points across the network.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_data_sheet0900aecd801e6a45.html

QUESTION 124:

The Certkiller network administrator needs to upgrade the IOS on a security appliance. Which of the following choices can be used to upgrade the image?

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

Answer: D

Explanation:
Upgrade your PIX operating system image file from a local TFTP server with the copy tftp flash command. This will allow the PIX to download an image from a TFTP server and save it to flash memory.

QUESTION 125:

A Certkiller PIX needs to have its license upgraded. 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 126:

You need to access a Certkiller PIX remotely via SSH. What username and password will establish an SSH connection to your PIX security appliance?

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

Answer: D

Explanation:
To gain access to the security appliance console using SSH, at the SSH client enter the username pix and enter the login password set by the password command.
The login password is used for Telnet and SSH connections. By default, the login password is "cisco."
Incorrect Answers:
A, C: The username used is "pix" by default, not "pixfirewall.
B: The login (telnet) password is used initially to access the PIX firewall via SSH, not the enable password.
Reference:
Cisco Security Appliance Command Line Configuration Guide For the Cisco ASA 5500 Series and Cisco PIX 500 Series version 7.0, Page 31-3

QUESTION 127:

Which statement about Telnet and the security appliance is true?

A. You can enable Telnet on all interfaces except the outside interface.
B. You can enable Telnet on all interfaces, but the PIX security appliance requires that all Telnet traffic to all interfaces be IPSec protected.
C. You can enable Telnet on all interfaces, but the PIX security appliance requires that all Telnet traffic to the outside interface be IPSec protected.
D. You can enable Telnet on all interfaces, but it most be protected with SSH.

Answer: C

Explanation:

The security appliance allows Telnet connections to the security appliance for management purposes. You cannot use Telnet to the lowest security interface unless you use Telnet inside an encrypted IPSec tunnel. Normally, if outside access to the appliance is required, SSH or web access via ASDM over HTTPS is used.
Reference: Cisco Security Appliance Command Line Configuration Guide 7.0, p. 31-1

QUESTION 128:

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 tasks 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 129:

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: SPFA Student Guide v3.2 - Cisco Secure PIX Advanced p.17-7

QUESTION 130:

You want to configure a Certkiller user with the highest privilege level available on a new Cisco PIX firewall. What privilege level is the highest on this security appliance?

A. 1
B. 5
C. 10
D. 15
E. 16
F. 20

Answer: D

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. The privilege level can be a value from 0 to 15. (Lower numbers are lower privilege levels while 15 is the highest.)
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a008042

QUESTION 131:

You want to apply a set of commands to a specific privileged level on a Certkiller security appliance. What command reassigns a specific command to a different privilege level?

A. privilege
B. command auth
C. level-priv
D. ourpriv
E. None of the above

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.

QUESTION 132:

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 133:

The administrator at Certkiller Inc. needs to know the command to enable command authorization. What is this command?

A. aaa authorization command LOCAL
B. aaa authorization permit any LOCAL
C. level-priv
D. passwd
E. None of the above

Answer: A

Explanation:
The "aaa authorization command local" enables command authorization (using it's own local database).
Reference: Cisco Secure PIX Firewall Advanced 3.1 chap 15 page 24

QUESTION 134:

The Certkiller PIX firewall administrator issued the "who" command. What is the purpose of this command?

A. To enable you to view which IP addresses are currently accessing the security appliance console via Telnet.
B. To enable you to view which IP addresses are currently accessing the security appliance console via SSH.
C. To enable you to view the hostname of devices accessing the security appliance.
D. To enable you to view who is currently accessing the security appliance Device Manager console from a browser.
E. None of the above.

Answer: A

Explanation:
The "who" command shows the PIXFirewall TTY_ID and IP address of each Telnet client currently logged into the PIXFirewall. This command is the same as the "show who" command.
The following example shows how to display the current Telnet sessions:

```
pixCKfirewall# who
0: From 192.168.1.3
1: From 192.168.2.2
```

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a008042

QUESTION 135:

ASDM is being used in the Certkiller network for managing the security appliances. The ASDM client is supported on which PC operating systems (Choose the best answer)

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

Answer: C

Explanation:
Cisco Adaptive Security Device Manager (ASDM) can be accessed directly with a Web browser from any Java plug-in enabled computer on the network, providing security administrators with rapid, secure access to their Cisco ASA 5500 Series Adaptive Security Appliances or Cisco PIX Security Appliances.
The table below lists the operating systems and Web browsers supported by Cisco ASDM Version 5.0.
Supported Operating Systems and Web Browsers:

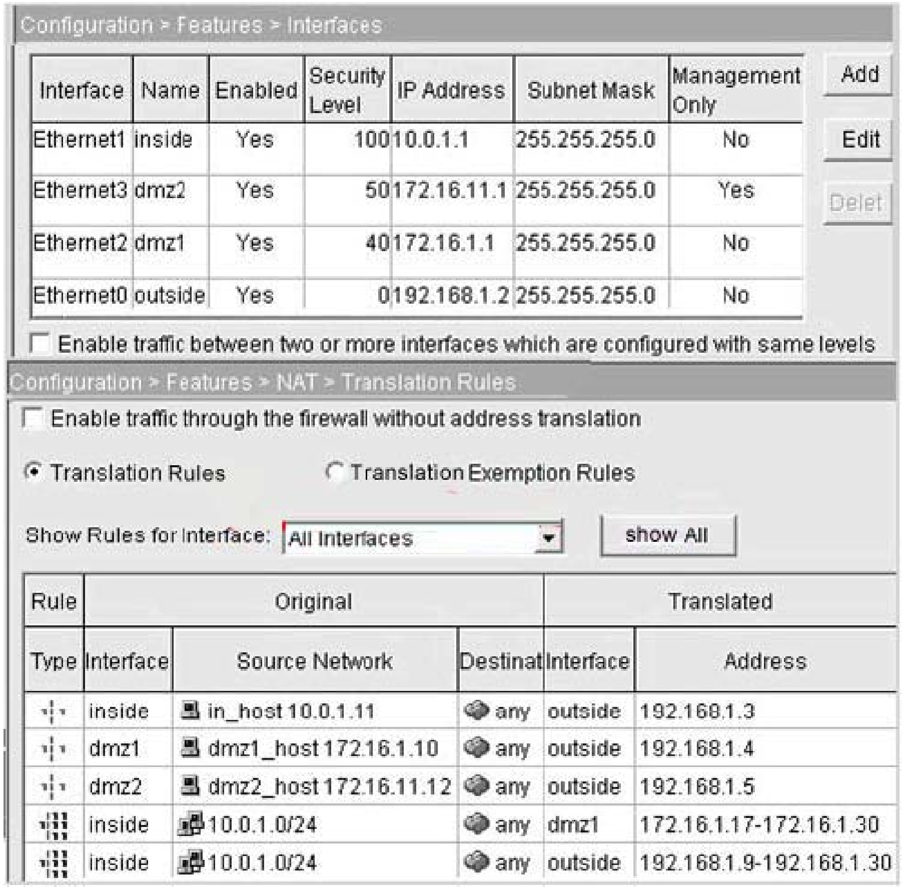
Operating Systems	**Browsers (JavaScript- and Java-Enabled)**
Windows 2000 with Service Pack 4 (English/Japanese)	Microsoft Internet Explorer 6.0 with Java Plug-In v1.4.2 or 1.5.0
Windows XP (English/Japanese)	Netscape Communicator 7.2 with Java Plug-In v1.4.2 or 1.5.0
Sun Solaris 2.8 or Higher Running	Mozilla 1.7.3 with Java Plug-In v1.4.2

CDE	or 1.5.0
Red Hat Linux 9.0 Running GNOME or KDE Red Hat Enterprise Linux WS Version 3	Mozilla 1.7.3 with Java Plug-In v1.4.2

Note: Cisco ASDM Version 5.0 does not support Windows 95, Windows 98, Windows ME, Windows NT, or Sun Solaris OpenWindows.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a008014871d.html

QUESTION 136:

A Certkiller firewall is configured for address translation as shown in the figure below:



Configuration > Features > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only
Ethernet1	inside	Yes	100	10.0.1.1	255.255.255.0	No
Ethernet3	dmz2	Yes	50	172.16.11.1	255.255.255.0	Yes
Ethernet2	dmz1	Yes	40	172.16.1.1	255.255.255.0	No
Ethernet0	outside	Yes	0	192.168.1.2	255.255.255.0	No

□ Enable traffic between two or more interfaces which are configured with same levels

Configuration > Features > NAT > Translation Rules

□ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

Rule	Original			Translated	
Type	Interface	Source Network	Destinat	Interface	Address
	inside	in_host 10.0.1.11	any	outside	192.168.1.3
	dmz1	dmz1_host 172.16.1.10	any	outside	192.168.1.4
	dmz2	dmz2_host 172.16.11.12	any	outside	192.168.1.5
	inside	10.0.1.0/24	any	dmz1	172.16.1.17-172.16.1.30
	inside	10.0.1.0/24	any	outside	192.168.1.9-192.168.1.30

Refer to the exhibit above. The Certkiller administrator is troubleshooting a security appliance connectivity issue using ASDM. The problem is that a new partner is trying to access the order entry server on dmz1_host from a PC on the outside network. The administrator is able to access the host successfully from the outside.

After successfully troubleshooting the problem, the administrator determines that the partner is trying to access the server on the wrong IP address.
From the information present on the ASDM screen, what address should the partner use to connect to dmz1_host?

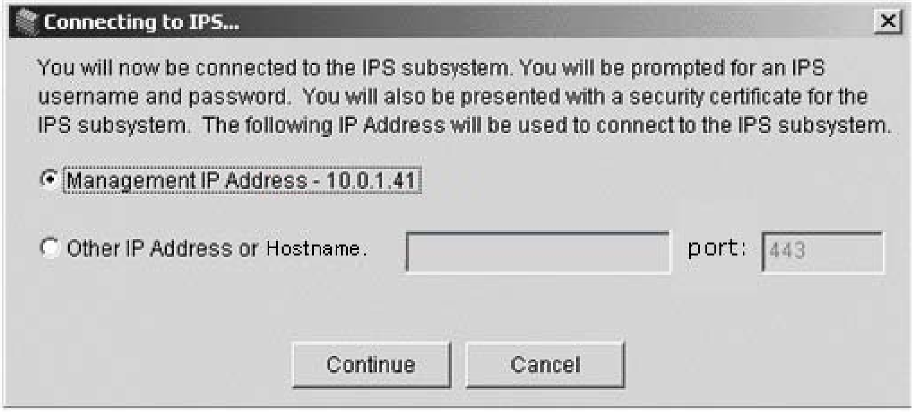
A. 172.16.1.17
B. 172.16.1.10
C. 192.168.1.9
D. 192.168.1.4
E. 10.0.1.0

Answer: D

Explanation:
When users from the outside connect to a server on the DMZ, they will need to use the translated IP address of the server, not the real IP address. According to the firewall ASDM information shown above, the DMZ server's real IP address is 172.16.1.10, and the translated IP address is 192.168.1.4. To users on the outside, the server appears as if it is using the 192.168.1.4 IP address.

QUESTION 137:

The following was seen by the Certkiller security administrator:



Connecting to IPS...

You will now be connected to the IPS subsystem. You will be prompted for an IPS username and password. You will also be presented with a security certificate for the IPS subsystem. The following IP Address will be used to connect to the IPS subsystem.

● Management IP Address - 10.0.1.41

○ Other IP Address or Hostname. port: 443

Refer to the exhibit shown above. When accessing the IPS icon in ASDM, the administrator is presented with a "Connecting to IPS" popup window. In the window, the management IP address A.B.C.D is displayed where A.B.C.D is an actual IP address.
What is IPS management 'connecting to" which has an IP address of A.B.C.D?

A. The AIP-SSM IPS control channel IP address.
B. The AIP-SSM IPS data channel IP address.
C. The AIP-SSM external interface IP address.
D. The AIP-SSM HTTP server virtual address.

E. None of the above

Answer: C

Explanation:
The AIP-SSM is configured with an IP address on it's interface, allowing for management of the AIP-SSM on a security appliance, such as the ASA 5500. When the AIP-SSM module is installed, the status of it can be seen as shown in the example below:

```
Certkiller 1# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA-SSM-20
Hardware version: 0.2
Serial Number: P2B000005D0
Firmware version: 1.0(10)0
Software version: 5.0(0.27)S129.0
Status: Up
Mgmt IP addr: 10.8.147.210
Mgmt web ports: 881
Mgmt TLS enabled: false
Certkiller 1#
```

In this example, the outside interface/management IP address is 10.8.147.210.

QUESTION 138:

An activation license key is being applied to a new Certkiller firewall. 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

Explanation:
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 Guide, page 4-30.

QUESTION 139:

A new Cisco PIX 515 is being installed in a Certkiller location. How many interfaces can be configured on a Cisco PIX 515 with a restricted license?

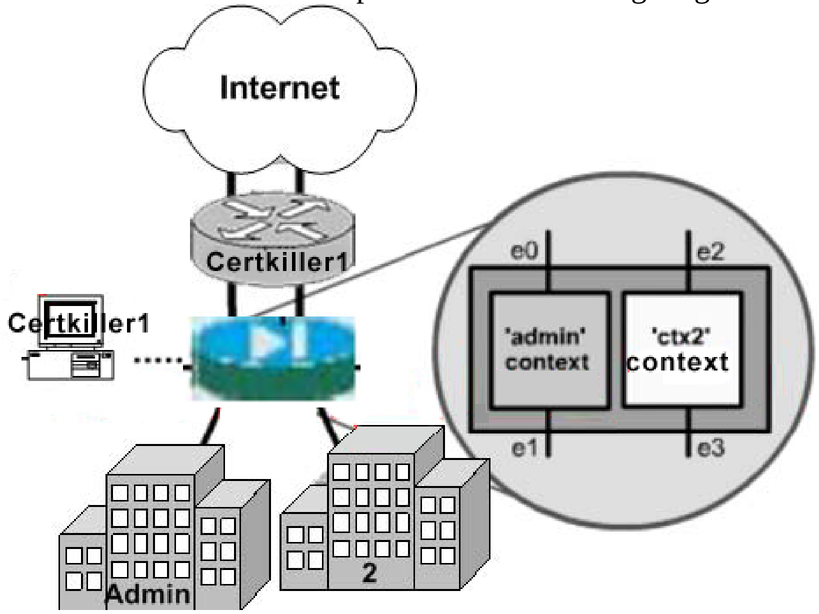
A. 2
B. 3
C. 4
D. 6

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.

Certkiller .com, Scenario

The Certkiller network is depicted in the following diagram:

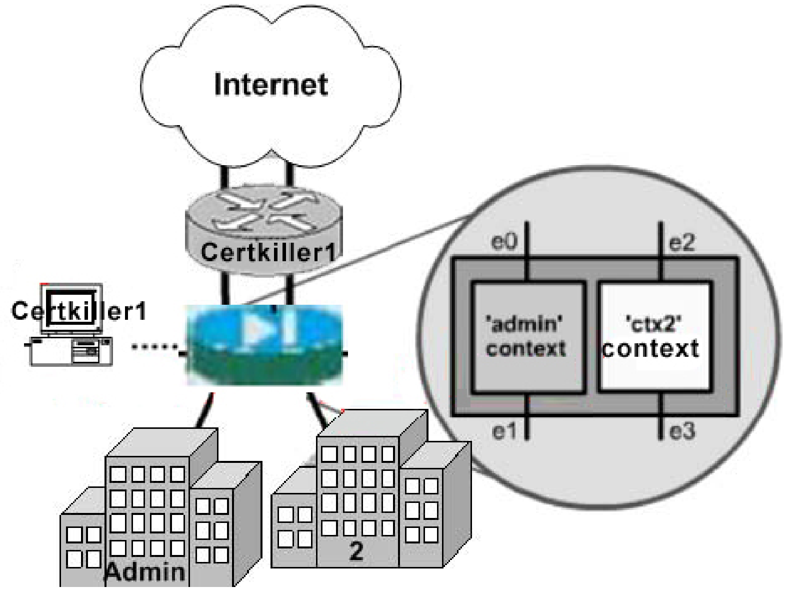


Note: Scenario is incomplete.

Certkiller .com (7 Questions)

QUESTION 140:

SIMULATION
The Certkiller network is depicted in the following diagram:



Certkiller .com installed a brand new PIX security appliance. The PIX configuration is currently at factory-default, single mode. From Host Certkiller 1, your task is to add two security contexts, allocate the appropriate interfaces to each context, and identify the location from which the system download the context configuration. The security appliance contexts are named dminand tx2. The dmincontext will support interaces ethernet0 and ethernet1. The dmincontext configuration should be stored in the PIX flash file admin.cfg. The tx2context will support interfaces ethernet2 and ethernet3. The tx2context configuration should be stored in the PIX flash file ctx2.cfg. You are finished with the task after the contexts are created, interfaces allocated and context configuration file locations are configured in the PIX system context.

Enable secret password is: Certkiller

Click on Host Certkiller 1 to start the simulation.

Answer:

Explanation:

```
pix> enable
password: pix
pix# configure terminal
pix(config)# mode multiple
Hit enter
Hit enter
pix# configure terminal
pix(config)# context ctx2
pix(config-ctx)# config-url flash:/ctx2.cfg
pix(config-ctx)# allocate-interface e2
pix(config-ctx)# allocate-interface e3
pix(config-ctx)# end
pix# configure terminal
pix(config)# context admin
pix(config-ctx)# config-url flash:/admin.cfg
pix(config-ctx)# allocate-interface e0
pix(config-ctx)# allocate-interface e1
pix(config-ctx)# end
pix# copy running-config startup-config
pix# show running-config
```

Note: the "changeto" command is not allowed in this scenario, and had to be removed
Note: the "disk0" was not allowed in the this scenario, but flash is a synonym for disk0, so this was OK

QUESTION 141:

Note: Please refer to the Certkiller .com scenario.
Which of the following traffic is permitted based on the current access-list configuration? (Choose two)

A. FTP traffic from outside the host to the 172.16.1.2 host on the dmz1.
B. HTTP and HTTPS traffic from the 172.16.10.2 dmz2 host to any host on the outside.
C. Any IP traffic from any outside host to the 172.16.10.2 host on the dmz2.
D. Any IP traffic from any outside host to the 172.16.1.2 host on the dmze1.
E. Any IP traffic from any host on the dmz1 to any host on the inside.

Answer: A, B

QUESTION 142:

Note: Please refer to the Certkiller .com scenario.
What is the current address translation configuration on the security appliance? (Choose two)

A. Using Dynamic NAT to translate any host on the inside to a mapped address from the address pool of 192.168.1.20 to 192.158.1.254.
B. Using Port Address Translation (PAT) to translate any host on the inside to the 192.168.1.10 global address.
C. Using Static NAT to translate the 172.16.10.2 DMZ host to a global address of 192.168.1.12.
D. Using Dynamic NAT to translate any host on dmz1 and dmz2 to a mapped address from the address pool of 192.168.1.20 to 192.168.1.254.
E. Using Static NAT to translate the 172.16.1.2 DMZ host to a global address of 192.168.1.10.

Answer: A, C

QUESTION 143:

Note: Please refer to the Certkiller .com scenario.
What is the current configured default gateway IP address on the security appliance?

A. 172.16.10.1
B. 172.16.1.1
C. 192.168.1.1
D. 10.0.1.1

Answer: C

QUESTION 144:

Note: Please refer to the Certkiller .com scenario.
Which hosts are allowed to manage this security appliance using ASDM or HTTPS?

A. The 10.0.1.11 host only.
B. The 172.16.1.2 host only.
C. The 172.16.10.2 host only.
D. Any host on the 10.0.1.0/24 subnet.
E. Any host on the 172.16.1.0/24 subnet.
F. Any host on the 172.16.10.0/24 subnet.

Answer: A

QUESTION 145:

Note: Please refer to the Certkiller .com scenario.
Which interface on this security appliance is enabled for DHCP server functionality?

A. None
B. Ethernet2
C. Ethernet1
D. Ethernet0
E. The inside and DMZ interfaces.

Answer: C

QUESTION 146:

Note: Please refer to the Certkiller .com scenario.
What is the maximum number of VLANs and physical interfaces supported based on the current security appliance software license?

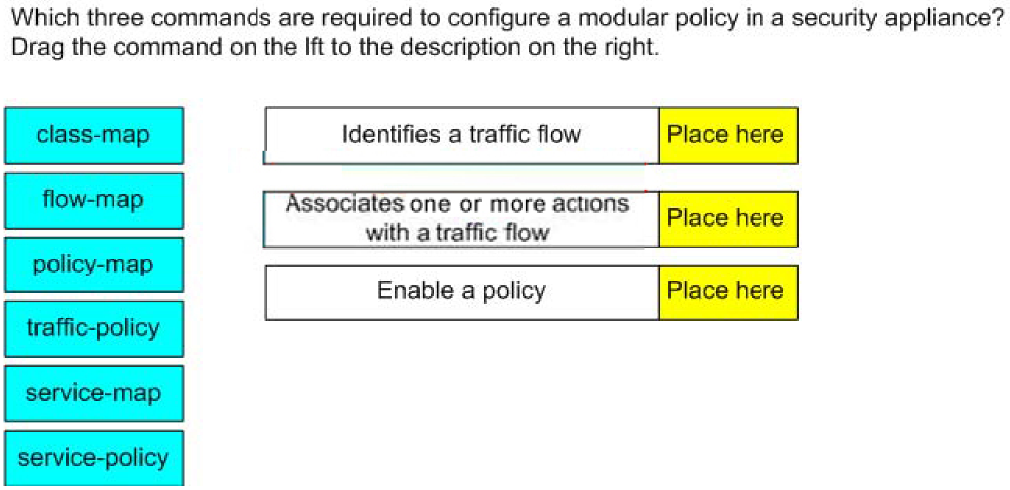
A. 25 VLANs and 6 interfaces
B. 10 VLANs and 3 interfaces
C. 50 VLANs and 8 interfaces
D. 150 VLANs and 14 interfaces
E. 100 VLANs and 10 interfaces

Answer: A

MIXED QUESTIONS.

QUESTION 147:

DRAG DROP

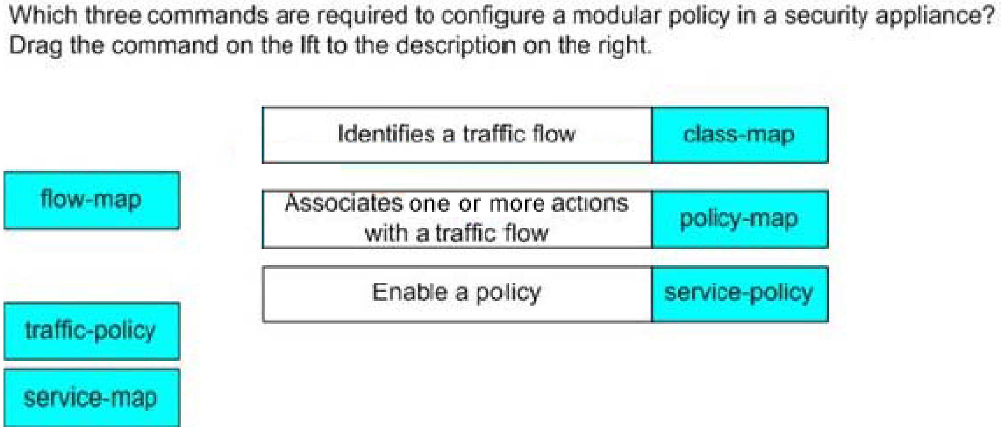


Which three commands are required to configure a modular policy in a security appliance?
Drag the command on the lft to the description on the right.

class-map
flow-map
policy-map
traffic-policy
service-map
service-policy

Identifies a traffic flow	Place here
Associates one or more actions with a traffic flow	Place here
Enable a policy	Place here

Answer:



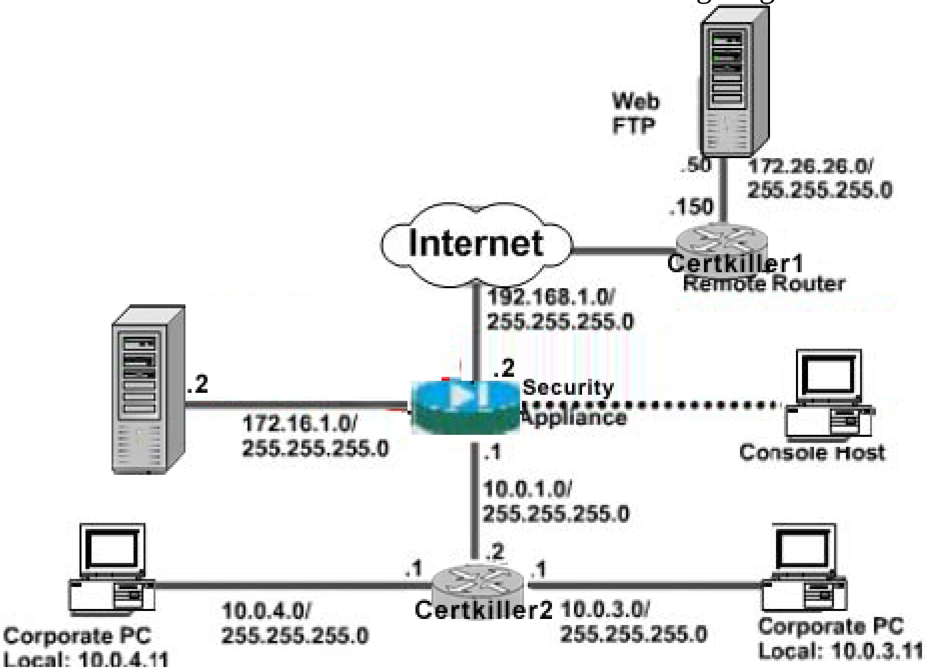
Which three commands are required to configure a modular policy in a security appliance?
Drag the command on the lft to the description on the right.

Identifies a traffic flow	class-map
Associates one or more actions with a traffic flow	policy-map
Enable a policy	service-policy

QUESTION 148:

SIMULATION

Part of the Certkiller network is shown in the following diagram:



Certkiller .com has installed a PIX security appliance and wants basic outbound access configured on the outside interface for all hosts on the inside network of 10.0.3.0/255.255.255.0. The real IP addresses of the inside hosts should be hidden from the outside network. Certkiller .com policy requires that packets traversing from a higher security interface to a lower security interface for all other inside networks must match a NAT rule, or else processing for the packet must stop. use the topology provided and the parameters below to complete this configuration. When you complete the exercise you should be able to open a Web session from the Corporate PC at 10.0.3.11 to the Web server located at 172.26.26.50. You should not

be able to open a Web Session from the Corporate PC at 10.0.4.11 to the Web server located at 172.26.26.50.
Ethernet1 Name inside
Ethernet2 Name outside
Nat ID 1
Global IP Addresses 192.168.1.20-192.168.1.254
Global Network 255.255.255.0
Inside Network A 10.0.1.0/255.255.255.0
Inside Network B 10.0.3.0/255.255.255.0
Inside Network C 10.0.4.0/255.255.255.0
DMZ Network 172.168.1.1
Hostname pix1
Hostname 172.16.1.2 bastionhost
Hostname 10.0.3.11 Insidehost
Enable Password blank
Start the simulation by clicking on the host icon connected to the PIX Firewall

Answer:

Explanation:

```
Certkiller # conf t
Certkiller (conf)# nat (inside) 1 10.0.4.0 255.255.255.0
Certkiller (conf)# nat (inside) 1 10.0.3.0 255.255.255.0
Certkiller (conf)# nat (dmz) 1 172.16.1.0 255.255.255.0
//We allow NAT'ting for all of the networks except
10.0.3.0
Certkiller (conf)# global (outside) 1
192.168.1.20-192.168.1.254 netmask 255.255.255.0
Certkiller (conf)# nat-control
//Have NAT control over all internal hosts.
Certkiller (conf)#end
Certkiller # copy run start
//Note: We could have used nat (inside) 1 0.0.0.0
0.0.0.0 unless the question doesnt specify the
requirement for host 10.0.4.11 to be denied access.
```

QUESTION 149:

A new PIX firewall was installed in the Certkiller network to guard against outside attacks. Why does this PIX security appliance record information about a packet in its stateful session flow table?

A. To build the reverse path forwarding (RFP) table to prevent spoofed source IP address.

B. To establish a proxy session by relaying the application layer requests and response between two endpoints.
C. To compare against return packets for determining whether the packet should be allowed through the firewall.
D. To track outbound UDP connections.

Answer: C

Explanation:
The Adaptive Security Algorithm (ASA), used by the PIXFirewall for stateful application inspection, ensures the secure use of applications and services. Some applications require special handling by the PIXFirewall application inspection function. Applications that require special application inspection functions are those that embed IP addressing information in the user data packet or open secondary channels on dynamically assigned ports.
The application inspection function monitors sessions to determine the port numbers for secondary channels. Many protocols open secondary TCP or UDP ports to improve performance. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application inspection function monitors these sessions, identifies the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.
Packets going through PIX are checked using these steps:
Access control lists (ACLs)-Used for authentication and authorization of connections based on specific networks, hosts, and services (TCP/UDP port numbers).
Inspections-Contains a static, pre-defined set of application-level inspection functions.
Connections (XLATE and CONN tables)-Maintains state and other information about each established connection. This information is used by ASA and cut-through proxy to efficiently forward traffic within established sessions.
1. A TCP SYN packet arrives at the PIXFirewall to establish a new connection.
2. The PIXFirewall checks the access control list (ACL) database to determine if the connection is permitted.
3. The PIXFirewall creates a new entry in the connection database (XLATE and CONN tables).
4. The PIXFirewall checks the Inspections database to determine if the connection requires application-level inspection.
5. After the application inspection function completes any required operations for the packet, the PIXFirewall forwards the packet to the destination system.
6. The destination system responds to the initial request.
7. The PIXFirewall receives the reply packet, looks up the connection in the connection database, and forwards the packet because it belongs to an established session.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800e

QUESTION 150:

A new Certkiller ASA 5500 was installed in the Certkiller network. In the Cisco ASA 5500 series, what is the flash keyword aliased to?

A. Disk0
B. Disk1
C. Both Disk0 and Disk1
D. Flash0
E. Flash1

Answer: A

Explanation:
See the following URL syntax:
disk0:/[path/]filename
For the ASA 5500 series adaptive security appliance, this URL indicates the internal Flash memory. You can also use flash instead of disk0; they are aliased.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450b90.html

QUESTION 151:

Cisco firewalls maintain state awareness of all traffic going through it. What is the core component of the PIX firewall that accommodates for this?

A. PFS
B. ASA
C. VAC
D. FWSM
E. None of the above

Answer: B

Explanation:
The Adaptive Security Algorithm (ASA) is the brains of the pix, keeping track of stateful connection information. This allows the firewall to maintain stateful packet awareness to allow for the return traffic to traverse through the firewall.

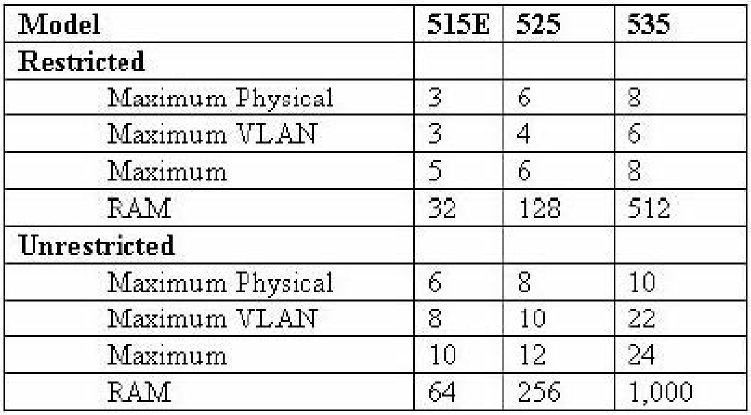
QUESTION 152:

A new Cisco PIX 535 is being installed in the Certkiller network. What is the maximum number of physical interfaces the PIX Firewall 535 supports with an unrestricted license?

A. 20
B. 10
C. 6
D. 5
E. 3

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.
- 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

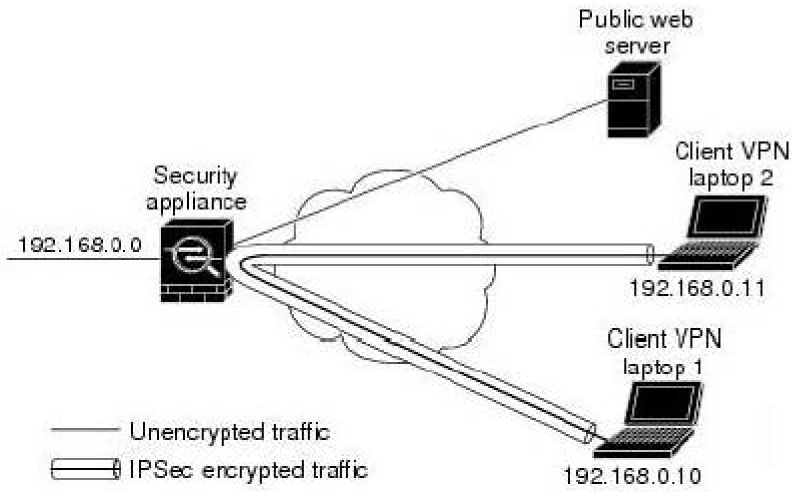
QUESTION 153:

On a new Certkiller PIX the "same-security-traffic permit intra-interface" configuration command was issued. What are two purposes of this command? (Choose all that apply)

A. It allows all of the VPN spokes in a hub-and-spoke configuration to be terminated on a single interface.
B. It allows communication between different interfaces that have the same security level.
C. It permits communication in and out of the same interface when the traffic is IPSec protected.
D. It enabled Dynamic Multipoint VPN.

Answer: D

Explanation:
If B was a correct answer then the "inter-interface" option would have been used... and it wasnt so it does not allow for comms between different interfaces... the "intra-interface" option was used... so B is incorrect
Here are the options as stated on an ASA:
inter-interface Permit communication between different interfaces with the same security level
intra-interface Permit communication between peers connected to the same interface
Permitting Intra-Interface Traffic
The security appliance includes a feature that lets a VPN client send IPSec-protected traffic to another VPN user by allowing such traffic in and out of the same interface. Also called "hairpinning", this feature can be thought of as VPN spokes (clients) connecting through a VPN hub (security appliance).
In another application, this feature can redirect incoming VPN traffic back out through the same interface as unencrypted traffic. This would be useful, for example, to a VPN client that does not have split tunneling but needs to both access a VPN and browse the Web.
Figure 29-1 shows VPN Client 1 sending secure IPSec traffic to VPN Client 2 while also sending unencrypted traffic to a public Web server.
Figure 29-1 VPN Client Using Intra-Interface Feature for Hairpinning

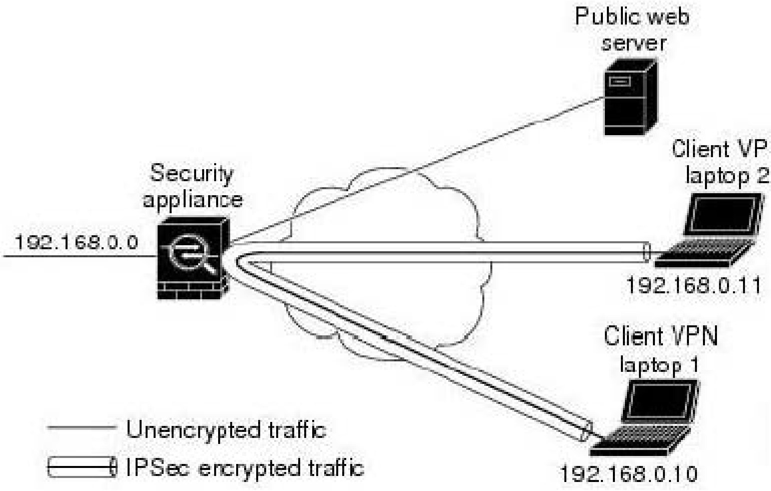


To configure this feature, use the same-security-traffic command in global configuration mode with its intra-interface argument.
The command syntax is same-security-traffic permit {inter-interface | intra-interface}.
The following example shows how to enable intra-interface traffic:

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```

Note You use the same-security-traffic command, but with the inter-interface argument, to permit communication between interfaces that have the same security level. This

feature is not specific to IPSec connections. For more information, see the "Configuring Interface Parameters" chapter of this guide.
Reference : Cisco Security Appliance Command Line Configuration Guide, Version 7.2



QUESTION 154:

A new Certkiller security appliance is being installed for the first time. By default, the AIP-SSM IPS software is accessible from the management port at IP address 10.1.9.201/24. Which CLI command should and administrator use to change the default AIP-SSM management port IP address?

A. hw module 1 setup
B. interface
C. setup
D. hw module 1 recover
E. None of the above

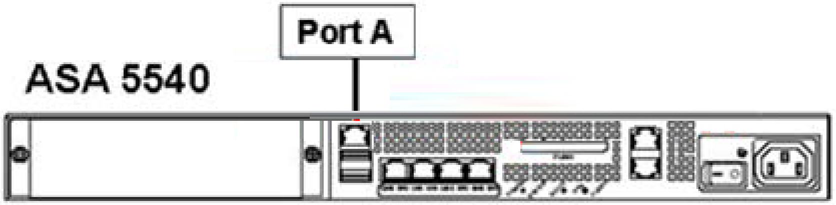
Answer: C

Explanation:
After you have completed configuration of the ASA 5500 series adaptive security appliance to divert traffic to the AIP SSM, session to the AIP SSM and run the setup utility for initial configuration.
To session to the AIP SSM from the adaptive security appliance, perform the following steps:
Step 1 Enter the session 1 command to session from the ASA 5500 series adaptive security appliance to the AIP SSM.
hostname# session 1

Step 2 Enter the username and password. The default username and password are both cisco.
Note: The first time you log in to the AIP SSM you are prompted to change the default password.
Step 3 Enter the setup command to run the setup utility for initial configuration of the AIP SSM.
AIP SSM# setup
You are now ready to configure the AIP SSM for intrusion prevention, including the ability to change the AIP-SSM management IP address..
Reference: Cisco Security Appliance Command Line Configuration Guide for the Cisco ASA 5500 Series and Cisco PIX 500 Series Software Version 7.0(4) page 19-3

QUESTION 155:

A Certkiller ASA appliance is shown below:



Refer to the exhibit above. The Certkiller administrator has configured the first four ports on a Cisco ASA 5540 Security Appliance. The technician attached the next data cable to Port A.
When configuring this interface, what physical type, slot, and port number should the administrator add to the configuration?

A. GigabitEthernet0/0
B. GigabitEthernet0/5
C. GigabitEthernet0/4
D. Management0/0

Answer: D

Explanation:
If you want to use ASDM to configure the security appliance instead of the command-line interface, you can connect to the default management address of 192.168.1.1 (if your security appliance includes a factory default configuration). On the ASA 5500 series adaptive security appliance, the interface to which you connect with ASDM is Management 0/0. For the PIX 500 series security appliance, the interface to which you connect with ASDM is Ethernet 1. If you do not have a factory default configuration, follow the steps in this section to access the command-line interface. You can then configure the minimum parameters to access ASDM by entering the setup command.

Reference: Cisco Security Appliance Command Line Configuration Guide for the Cisco ASA 5500 Series and Cisco PIX 500 Series, page 2-84

QUESTION 156:

The files on a Certkiller security appliance need to be verified. How can you view the files listed in a PIX flash memory?

A. show pix flash
B. show flash memory
C. show flashfs
D. show flash mfs
E. None of the above

Answer: C

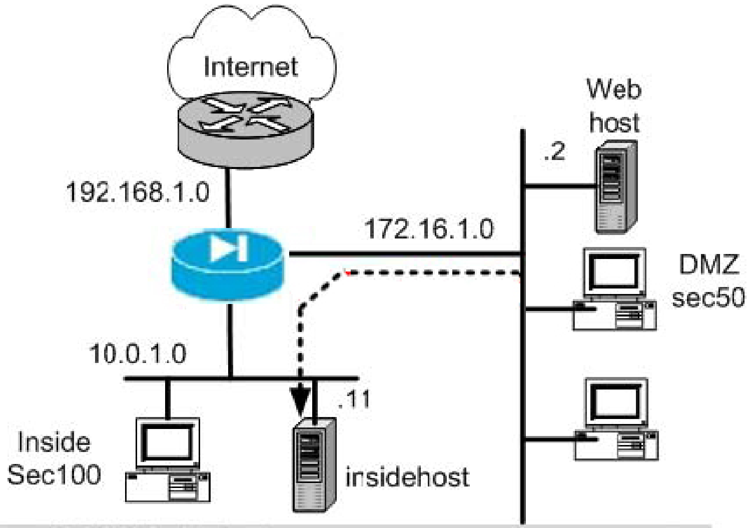
Explanation:
You can view the size of your configuration from the PIX Firewall console. Either connect a computer to the PIX Firewall unit or use Telnet to access the console. After entering the enable mode password, use the show flashfs command to view the configuration size, as shown in the following example:

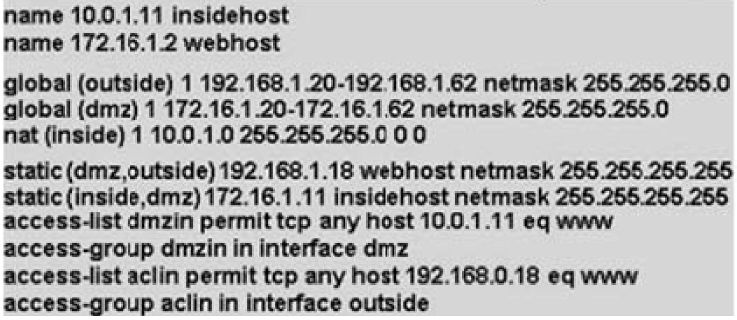
```
CK1 #show flashfs
flash file system: version:2 magic:0x12345679
file 0: origin: 0 length:2502712
file 1: origin: 2621440 length:2324
file 2: origin: 0 length:0
file 3: origin: 2752512 length:2608708
file 4: origin: 8257536 length:280
```

The "file 1" line lists the number of characters in your configuration after the "length" parameter. In this example, the configuration consists of 2,324 characters. Divide this number by 1,024 to view the number of kilobytes. The configuration in this example is slightly more than 2 KB.
The optimal configuration file size to use with PDM is less than 100KB, which is approximately 1500 lines. PIXFirewall configuration files over 100KB may interfere with the performance of PDM on your workstation.
Reference:
http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/products_installation_guide_chapter09186a008007d

QUESTION 157:

The Certkiller network is displayed in the following diagram:





```
name 10.0.1.11 insidehost
name 172.16.1.2 webhost

global (outside) 1 192.168.1.20-192.168.1.62 netmask 255.255.255.0
global (dmz) 1 172.16.1.20-172.16.1.62 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
static (inside,dmz) 172.16.1.11 insidehost netmask 255.255.255.255
access-list dmzin permit tcp any host 10.0.1.11 eq www
access-group dmzin in interface dmz
access-list aclin permit tcp any host 192.168.0.18 eq www
access-group aclin in interface outside
```

Refer to the exhibit above. Users on the DMZ are complaining that they cannot gain access to the inside host via HTTP. What did the network administrator determine after reviewing the network diagram and partial configuration?

A. The static (inside,dmz) command is not configured correctly.
B. The global (dmz) command is not configured correctly.
C. The nat (dmz) command is missing.
D. The dmzin access list is not configured correctly.
E. None of the above

Answer: D

Explanation:
Based on the configuration above, the real IP address of the WWW server (insidehost) is 10.0.1.11, but there is a static NAT entry that translates this address to 192.168.1.18. Users from the outside will attempt to connect to the server "insidehost" using the 192.168.1.18 IP address. The access list must therefore permit WWW traffic to this host, not the 10.0.1.11 host. The DMZ access list should read "access-list dmzin permit tcp any host 192.168.1.18 eq www"

QUESTION 158:

The security team at Certkiller 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 159:

A new Certkiller security appliance is being used on a small office with a DSL connection. 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
E. None of the above

Answer: B

Explanation:
The "IP address outside dhcp" command 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 160:

You need to configure a default route on a new Certkiller security appliance. Which of the following correctly describe how to configure this?

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
E. None of the above.

Answer: B

Explanation:
Create a static route such as a default route on the pix with the route command.
Incorrect Answers:
A: The "ip route command is used for IOS routers, not PIX firewalls.
C: The "set route" is used for CAT OS devices such as Catalyst switches.
D: This is an invalid command.

QUESTION 161:

The Certkiller security administrator is viewing the syslog messages stored on an installed security appliance. What is the maximum number of syslog messages the PIX firewall can store with internal buffers?

A. 20
B. 100
C. 350
D. 600
E. 1500

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 162:

You need to manage the security contexts of a Certkiller security appliance. Which of these identifies basic settings for the security appliance, including a list of contexts?

A. Primary configuration
B. Network configuration
C. System configuration
D. Admin configuration
E. None of the above

Answer: C

Explanation:
The security context definition in the system configuration identifies the context name, configuration file URL, and interfaces that a context can use. You can only remove a context by editing the system configuration. You cannot remove the current admin context, unless you remove all contexts using the clear context command.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450b90.html#w

---

QUESTION 163:

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?

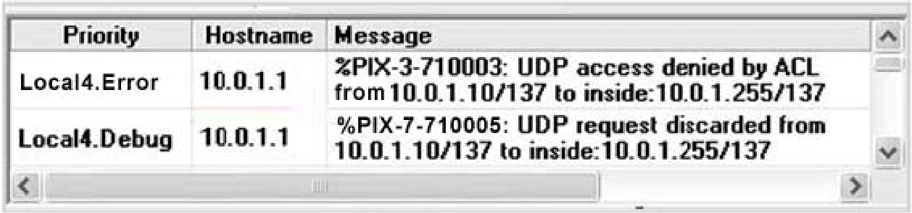
A. Each time it is reloaded.
B. Each time a TCP or UDP outbound connection attempt is made.
C. Each time a TCP or UDP inbound or outbound connection attempt is made.
D. Only when a TCP inbound or outbound connection attempts is made.
E. Never.

Answer: C

Explanation:
Stateful packet filtering is the method used by the Cisco PIX Firewall. This technology maintains complete session state. Each time a Transmission 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 Guide, pages 3-7

QUESTION 164:

The following was displayed in a Certkiller syslog server:



Priority	Hostname	Message
Local4.Error	10.0.1.1	%PIX-3-710003: UDP access denied by ACL from 10.0.1.10/137 to inside:10.0.1.255/137
Local4.Debug	10.0.1.1	%PIX-7-710005: UDP request discarded from 10.0.1.10/137 to inside:10.0.1.255/137

Refer to the exhibit shown above. You are the Certkiller administrator who is inundated with unwanted syslog messages. You want to stay at your current syslog message level but block selected unwanted syslog messages from filling your syslog. What command should you use to block specific unwanted message number 710005?

A. logging message deny 710005
B. no logging debug 710005
C. logging trap deny 71005
D. no logging message 710005

Answer: D

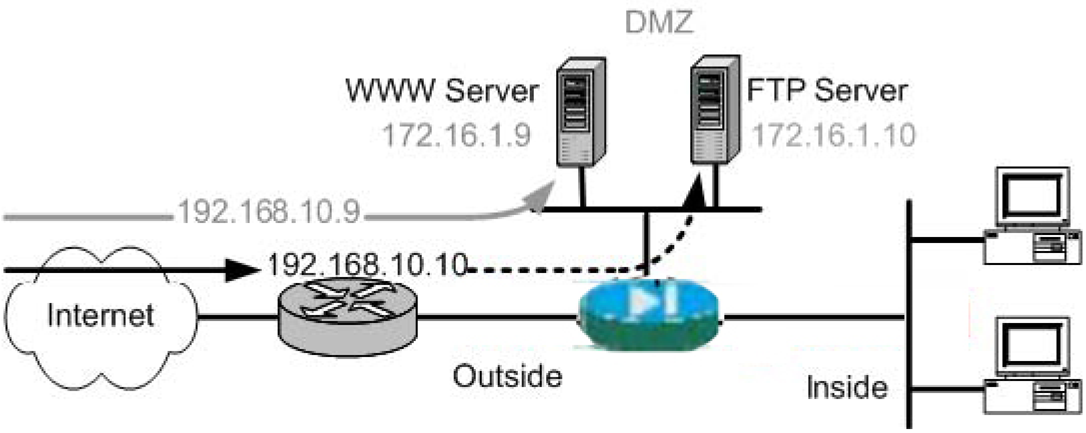
Explanation:
The following table displays the relevant Cisco PIX syslog configuration commands:

Command	Description
logging on	Enables transmission of syslog messages to all output locations. You can disable sending syslog messages with the no logging on command.
no logging message message_number	Allows you to disable specific syslog messages. Use the logging message message_number command to resume logging of specific disabled messages.

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guide_chapter09186a0080

QUESTION 165:

The Certkiller WAN is displayed in the following diagram:



Refer to the exhibit shown above. The Certkiller administrator wants to permanently map host addresses on the DMZ subnet to the same host addresses, but using a different subnet on the outside interface. Which command (or set of commands) should the administrator use to accomplish this?

A. NAT (dmz) 0 172.16.1.0 netmask 255.255.255.0
B. access-list server_map permit tcp any 192.168.10.0 255.255.255.0
Nat (outside) 10 access-list server_map
Global (dmz) 10 172.16.1.9-10 netmask 255.255.255.0
C. static (dmz,outside) 192.168.10.0 172.16.1.0 netmask 255.255.255.0
D. NAT (dmz) 1 172.16.1.0 netmask 255.255.255.0
Global (outside) 1 192.168.10.9-10 netmask 255.255.255.0

Answer: C

Explanation:
To configure regular static NAT, use the "static" command. This command is normally done to create static 1-1 mappings, but can be done to create static mappings for an entire subnet as required in this example.
For example, the following command maps the outside address (209.165.201.15) to an inside address (10.1.1.6):
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask 255.255.255.255
The following command statically maps an entire subnet:
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
Note: If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the security appliance translates the .0 and .255 addresses.
Reference: Cisco Security Appliance Command Line Configuration Guide For the Cisco ASA 5500 Series and Cisco PIX 500 Series, page 14-45.

QUESTION 166:

If you want IP addresses of hosts on the Certkiller DMZ and inside network translated when they make connections to hosts on the outside interface of the security appliance, what is the minimum NAT configuration you can enter?

A. 1 NAT statement and 1 global statement
B. 1 NAT statement and 2 global statements
C. 2 NAT statements and 1 global statement
D. 2 NAT statements and 2 global statements
E. None of the above.

Answer: C

Explanation:
A single global NAT statement can be used to translate both the inside hosts and the DMZ hosts to the same external IP address. Typically, the IP address of the outside interface is used. In addition to this, two NAT statements will be required so the firewall knows which IP subnets are to be translated. In this case, one that specifies the hosts on the inside network, and one to specify the hosts on the DMZ; giving us a total of 2 NAT statements and 1 global statement.
Example:

```
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 167:

Which of the following commands allows the Certkiller security administrator to disable IP address translation through a PIX firewall?

A. NAT 0
B. Global disable
C. access list
D. static
E. None of the above

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 IOS 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 168:

The Certkiller administrator wants to protect the DMZ web server from SYN flood attacks. Which command does NOT allow this administrator to place limits on the number of embryonic connections?

A. nat
B. static
C. set connection
D. HTTP-map
E. All of the above

Answer: D

Explanation:
You can limit TCP and UDP connections and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. The security appliance uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination, and can be configured using NAT and static commands, as well as through the use of the "set connection" command. HTTP maps are not used to set embryonic connection limits.
Incorrect Answers:
A, B: You can also configure maximum connections, maximum embryonic connections, and TCP sequence randomization in the NAT configuration. If you configure these settings for the same traffic using both methods, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence rand
C: To set embryonic connection limits, perform the following steps:
Step 1: To identify the traffic, add a class map using the class-map command.
Step 2: To add or edit a policy map that sets the actions to take with the class map traffic, enter the following command:

```
CK1 (config)# policy-map name
```

Step 3: To identify the class map from Step 1 to which you want to assign an action, enter the following command:

```
CK1 (config-pmap)# class class_map_name
```

Step 4: To set the maximum connections (both TCP and UDP), maximum embryonic connections, or whether to disable TCP sequence randomization, enter the following command:

```
CK1 (config-pmap-c)# set connection {[conn-max number] [embryonic-conn-max number] [random-sequence-number {enable | disable}}
```

Where number is an integer between 0 and 65535. The default is 0, which means no limit on connections.

You can enter this command all on one line (in any order), or you can enter each attribute as a separate command. The command is combined onto one line in the running configuration.

Step 5: To set the timeout for connections, embryonic connections (half-opened), and half-closed connections, enter the following command:

```
CK1 (config-pmap-c)# set connection {[embryonic hh[:mm[:ss]]]
[half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
```

Where embryonic hh[:mm[:ss] is a time between 0:0:5 and 1192:59:59. The default is 0:0:30. You can also set this value to 0, which means the connection never times out.

Reference: Cisco Security Appliance Command Line Configuration Guide for the Cisco ASA 5500 Series and Cisco PIX 500 Series, page 19-9

QUESTION 169:

You want to verify the NAT/PAT configuration on a new Certkiller security appliance. Which of the following commands shows the translation table entries?

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

Answer: C

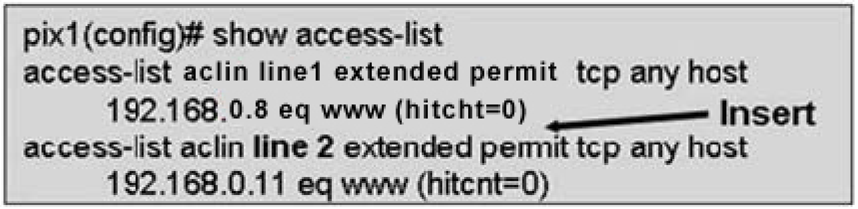
Explanation:
Use the show xlate command to see all ip address translations currently on the pix.
Example:
The following is sample output from the show xlate command with three active Port Address Translations (PATs):

```
CKPIX1(config)# show xlate
3 in use, 3 most used
PAT Global 192.150.49.1(0) Local 10.1.1.15 ICMP id 340
PAT Global 192.150.49.1(1024) Local 10.1.1.15(1028)
PAT Global 192.150.49.1(1024) Local 10.1.1.15(516)
```

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801c

QUESTION 170:

Observe the following diagram regarding a Certkiller PIX access list.



```
pix1(config)# show access-list
access-list aclin line1 extended permit  tcp any host
       192.168.0.8 eq www (hitcht=0)
access-list aclin line 2 extended permit tcp any host
       192.168.0.11 eq www (hitcnt=0)
```

The Certkiller administrator wants to add a comment about access-list aclin before line 2 as shown above. What command should the administrator enter to accomplish this addition?

A. pix1(config)# access-list aclin line 1 remark partner server http access
B. pix1(config)# access-list aclin line 2 remark partner server http access
C. pix1(config)# access-list aclin line 1 comment partner server http access
D. pix1(config)# access-list aclin line 2 comment partner server http access
E. None of the above

Answer: B

Explanation:
You can include remarks about entries in any access list, including extended, EtherType, and standard access lists. The remarks make the access list easier to understand.
To add a remark after the last access-list command you entered, enter the following command:
hostname(config)# access-list access_list_name remark text
If you enter the remark before any access-list command, then the remark is the first line in the access list.
If you delete an access list using the no access-list access_list_name command, then all the remarks are also removed.
The text can be up to 100 characters in length. You can enter leading spaces at the beginning of the text. Trailing spaces are ignored.
For example, you can add remarks before each ACE, and the remark appears in the access list in this location. Entering a dash (-) at the beginning of the remark helps set it apart from ACEs.
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
If you wish to add the remark to an already existing access list, use the "line" keyword to specify which line to add the remark to, as specified in answer choice B. In this case, because we want to insert the remark before line 2, we need to specify line 2, not line 1.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450bf0.html#w

QUESTION 171:

At the end of an access list configured on a Certkiller router, an explicit deny statement was configured. Why include a deny statement at the end of 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. There is no reason to include the deny statement.
C. You can enable the turbo ACL feature for individual ACLs.
D. As back-up, in case the implicit deny does not work.
E. All of the above

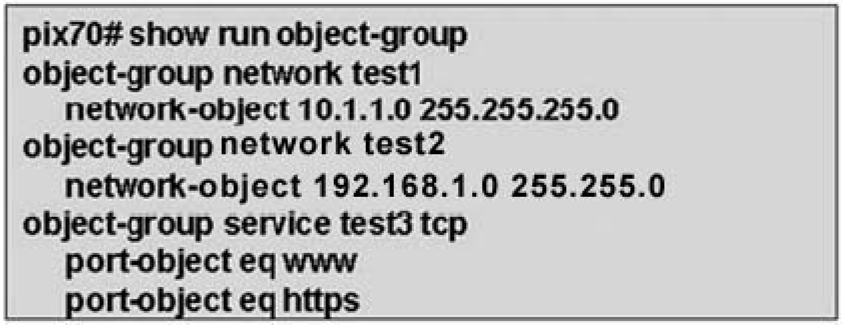
Answer: A

Explanation:
You can use the show access-list command to monitor specific deny entries that can be monitored for hit count. This provides information about prohibited network access attempts without having to enable logging on ACL entries. The last line of the ACL should be a
deny ip any any. Once again, the hit count against this last entry can provide information about prohibited access attempts and this can only be seen with explicit access list entries.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3 61/technologies_white_paper09186a00801afc76.shtml

---

QUESTION 172:

The following output was seen on a Certkiller PIX firewall:



```
pix70# show run object-group
object-group network test1
   network-object 10.1.1.0 255.255.255.0
object-group network test2
   network-object 192.168.1.0 255.255.0
object-group service test3 tcp
   port-object eq www
   port-object eq https
```

Refer to the show run output in the exhibit shown above. Which access-list configuration using the object-groups shown will only permit HTTP and HTTPS traffic from any host on 10.1.1.0/24 to any host on 192.168.1.0/24?

A. access-list aclin extended permit tcp object-group test2 object-group test1 object-group test3
B. access-list aclin extended permit tcp object-group test1 object-group test2 object-group test3

C. access-list aclin extended permit tcp object-group test1 object-group test3
object-group test2
D. access-list aclin extended permit ip object-group test1 object-group test2

Answer: B

Explanation:
To use object groups in an access list, replace the normal protocol (protocol), network (source_addressmask, etc.), service (operator port), or ICMP type (icmp_type) parameter with object-group grp_id parameter.
For example, to use object groups for all available parameters in theaccess-list {tcp | udp} command, enter the following command:
hostname(config)# access-listaccess_list_name [line line_number] [extended] {deny| permit} {tcp | udp} object-group nw_grp_id [object-group svc_grp_id] object-group nw_grp_id [object-group svc_grp_id] [log[[level] [interval secs] | disable | default]] [inactive | time-range time_range_name]
Fundamentally, the same access rules apply whether of not object groups are used. First, the source network or networks is looked at, then the destination network, and finally the protocols used. Therefore, choice B is correct.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450bf0.html#w

---

QUESTION 173:

A new Certkiller security appliance is being configured for object groups. Which two of these are valid types of object groups? (Choose two)

A. Ping
B. Service
C. Protocol
D. Port
E. TCP
F. UDP

Answer: B, C

Explanation:
The following lists the various object groups that can be configured:
- ICMP-Type Object Group
The ICMP-type object group is used in order to specify specific ICMP types for use only with ICMP access control lists (ACLs) and conduits.
- Network Object Group
Use the network object group in order to specify host IP addresses or subnet ranges that

you want to define in an ACL or conduit.
- Protocol Object Group
Use the protocol object group in order to specify a protocol(s) that you want to define in an ACL or conduit.
- Service Configuration
Use the service object group in order to specify specific or ranges of TCP and/or UDP ports that you want to define in an ACL or conduit.
Reference:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a00800d641d.shtml#using

QUESTION 174:

Object groups are being configured on a Certkiller security appliance. When are duplicate objects allowed in object groups?

A. Never
B. Always, because there are no conditions or restrictions.
C. When a group object is included and causes the group hierarchy to become circular.
D. When they are due to the inclusion of group objects.

Answer: D

Explanation:
The following example shows how to use the group-object mode to create a new object group that consists of previously defined objects:

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)#access-list all permit tcp object-group all_hosts any eq www
```

Without the group-object command, you need to define the all_hosts group to include all the IP addresses that have already been defined in host_grp_1 and host_grp_2. With the group-object command, the duplicated definitions of the hosts are eliminated.

Reference: Cisco Security Appliance Command Reference for the Cisco ASA 5500 Series and Cisco PIX 500 Series, page 6-116.

QUESTION 175:

The Certkiller network has a complex security policy configured on their firewalls. 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, Chapter 8, Page 3.

QUESTION 176:

A Certkiller PIX used for a VPN has been configured with the "nat 0" command. What is the purpose of the "nat 0" command when used in conjunction with IPSec?

A. It instructs the security appliance not to use Network Address Translation for any traffic deemed interesting traffic for IPSec.
B. It instructs the security appliance to use Network Address Translation for any traffic deemed interesting traffic for IPSec.
C. It disables Network Address Translation control on the security appliance.
D. It enables Network Address Translation Traversal for any traffic deemed interesting for IPSec.
E. None of the above

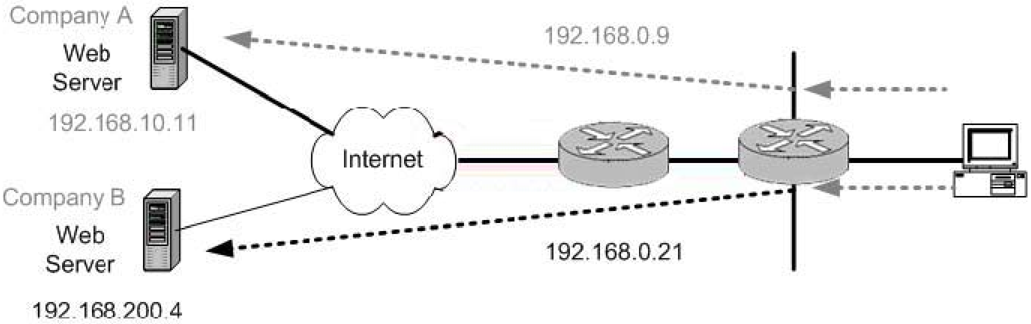
Answer: A

Explanation:
The nat 0 command bypasses NAT for the packets destined over the IPsec tunnel in a PIX firewall. In the following example, access list 140 is used to specify the networks

that are not to be translated over the IPSec tunnel.
Example:
CKPIX# Nat (inside) 0 access-list 140

QUESTION 177:

The Certkiller network is shown in the following diagram:



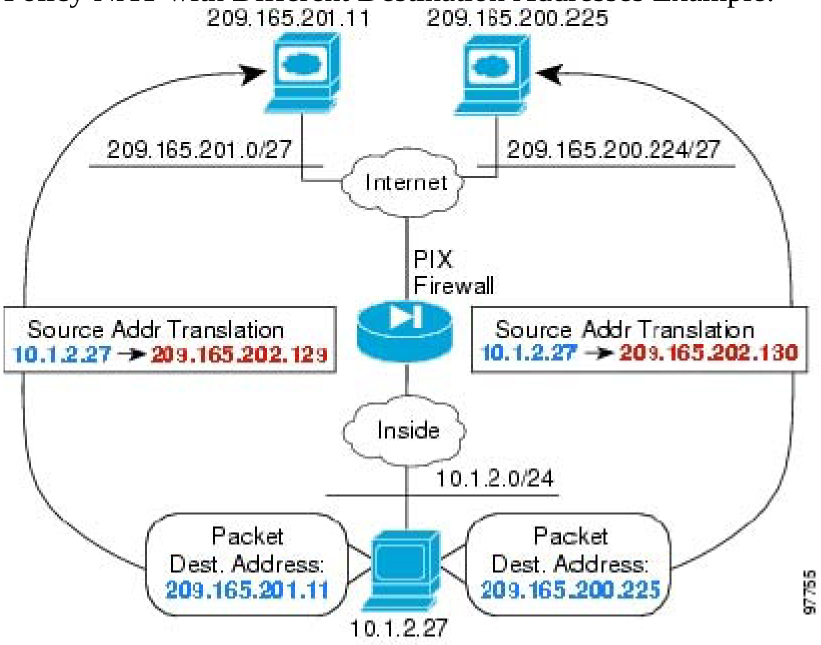
Refer to the exhibit above. The Certkiller administrator wants a user on the inside network to access two sites on the Internet and present two different source IP addresses. When the user is accessing Company A's web servers, the source IP address is translated to 192.168.0.9. When the user is accessing Company B's web servers, the source address is translated to 192.168.0.21.
Which of these can the security appliance administrator configure to accomplish this application?

A. Inside NAT
B. Identity NAT
C. Static
D. Policy NAT
E. None of the above

Answer: D

Explanation:
Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses (or ports) in an access list. Regular NAT uses source addresses/ports only, whereas policy NAT uses both source and destination addresses/ports.
With policy NAT, you can create multiple NAT or static statements that identify the same local address as long as the source/port and destination/port combination is unique for each statement. You can then match different global addresses to each source/port and destination/port pair.
The example below shows a host on the 10.1.2.0/24 network accessing two different servers. When the host accesses the server at 209.165.201.11, the local address is translated to 209.165.202.129. When the host accesses the server at 209.165.200.225, the local address is translated to 209.165.202.130.

Policy NAT with Different Destination Addresses Example:



Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017

QUESTION 178:

URL filtering is being implemented in the Certkiller network. How many different URL filtering servers can a pix support?

A. 8
B. 12
C. 16
D. 20
E. 1

Answer: C

Explanation:
The url-server command designates the server running the N2H2 or Websense URL filtering application. The limit is 16 URL servers; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the PIXFirewall does not update the configuration on the application server; this must be done separately, according to the individual vendor's instructions.
Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a008042

QUESTION 179:

The Certkiller network administrator wants to implement a URL filtering system at a remote branch. What are the two URL filtering vendors the firewall IOS supports?

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

Answer: C, D

Explanation:
Cisco offers URL filtering to support the Cisco IOS Firewall, allowing customers to use either Websense or N2H2 URL filtering products with Ciscosecurity routers. The Websense URL filtering feature helps enable a company's Cisco IOS Firewall to interact with the Websense or N2H2 URL filtering software to prevent users from accessing specified Websites on the basis of their security policy. The Cisco IOS Firewall works with the Websense and N2H2 server to determine whether to allow or deny (block) a particular URL.
Reference:
http://www.cisco.com/en/US/products/ps5854/products_white_paper0900aecd80173e40.shtml

QUESTION 180:

Internet browsing filters need to be implemented in the Certkiller network. 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

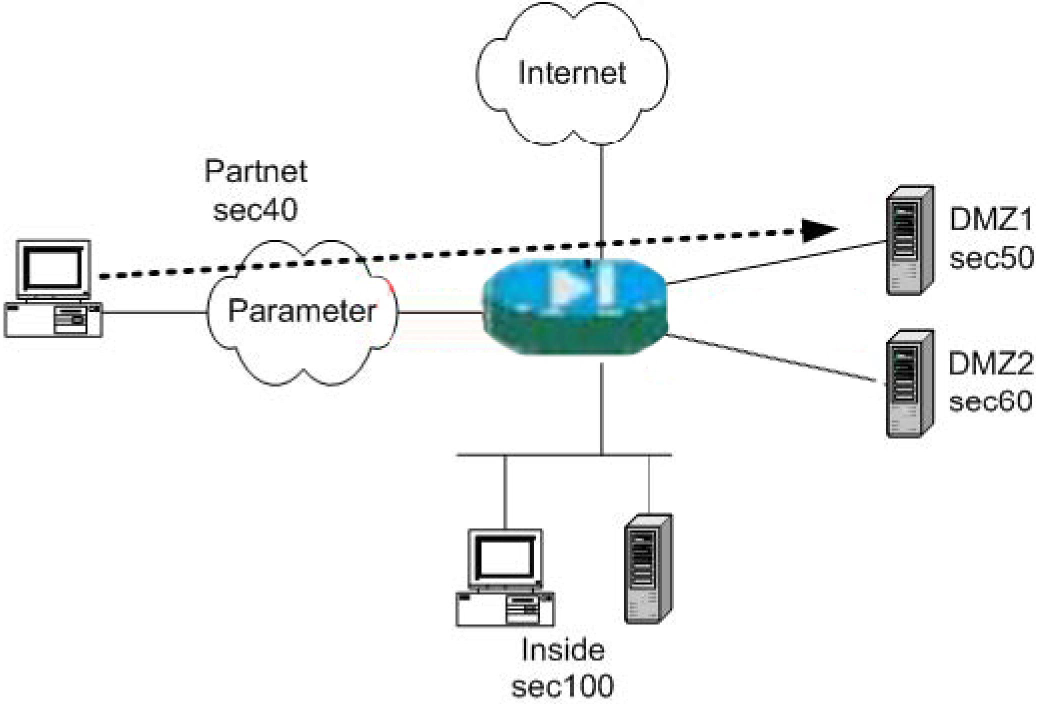
Answer: B

Explanation:
The url-server command designates the server running the N2H2 or Websense URL

filtering application. The limit is 16 URL servers; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the PIXFirewall does not update the configuration on the application server; this must be done separately, according to the individual vendor's instructions. Once you designate the server, enable the URL filtering service with the "filter" command.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a008042

QUESTION 181:

The Certkiller network is shown in the following diagram:



In the network diagram which two methods will enable a PC on the Partnernet to connect to a server on DMZ1 and deny the Partnernet PC access to DMZ2 and the inside network? (Choose two)

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

Answer: A, E

Explanation:
By default, the PIXFirewall denies access to an internal or perimeter (more secure) network from an external (less secure) network. You specifically allow inbound connections by using access lists. Access lists work on a first-match basis, so for inbound access, you must deny first and then permit after. In this example, traffic from an interface with security level 40 will not be allowed to devices behind a security level of 50. By giving the Partnernet a security value of 51-59, access to DMZ1 will be allowed but not to DMZ2.
An alternative to this would be to assign a static command and ACL to the Partnernet interface, which will automatically create rules to allow the specified access to all of the security level interfaces higher than its own value of 40.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017