

PIX/SPNA

Cisco PIX Challenge 1

Outline

This challenge involves the configuration of basic PIX details.

Objectives

The objectives of this challenge are to:

- Setup the hostname.
- Define the domain name.
- Setup IP address of E0.
- Enable E0.

Example (Version 6.x)

```
# sh ip add
System IP Addresses:
  IP address outside 0.0.0.0
  IP address inside 0.0.0.0
  IP address inf2 0.0.0.0
Current IP Addresses:
  IP address outside 0.0.0.0
  IP address inside 0.0.0.0
  IP address inf2 0.0.0.0
# sh nameif
# config t
(config)# help hos

USAGE:

      hostname <name>
      show hostname [fqdn]

DESCRIPTION:

hostname          Change host name

(config)# hostname freds
(config)# domain-name fred.com
(config)# help domain-

USAGE:

      [no] domain-name <name>
      clear configure domain-name
```

DESCRIPTION:

```
domain-name      Change domain name
(config)# ip address outside 192.168.1.1 255.255.255.0
(config)# interface e0 auto
(config)# exit
# show ip add
# show running
# sh int e0
Interface Ethernet0 outside, is up, line protocol is up
  Hardware is i82559, BW 100 Mbps
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000d.6585.77d9, MTU 1500
    IP address 192.168.1.1, subnet mask 255.255.255.0
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software (0/0)
    output queue (curr/max blocks): hardware (0/1) software (0/1)
    Received 0 VLAN untagged packets, 0 bytes
    Transmitted 1 VLAN untagged packets, 28 bytes
    Dropped 0 VLAN untagged packets
```

Example (Version 7.x)

```
# sh nameif
# config t
(config)# help hostname
```

USAGE:

```
hostname <name>
show hostname [fqdn]
```

DESCRIPTION:

hostname Change host name

```
(config)# help domain-
```

USAGE:

```
[no] domain-name <name>
clear configure domain-name
```

DESCRIPTION:

domain-name Change domain name

```
(config)# hostname ?
```

configure mode commands/options:

```
WORD < 64 char Host name for this system. A hostname must start and end with
a letter or digit and have as interior characters only
letters, digits, or a hyphen.
```

```
(config)# hostname freds
(config)# domain-name?
```

configure mode commands/options:

WORD Domain names must begin and end with a digit/letter, only letters, digits, and hyphen are allowed as internal characters, labels are separated by a dot. A maximum of 63 characters is allowed.

```
(config)# domain-name fred.com
(config)# int e0
(config-if)# help ip
```

USAGE:

```
[no] ip address <ip_address> [<mask>] [standby <sby_ip_addr>]
[no] ip address dhcp [setroute] [retry <4-16>]
show ip address [<interface> | <if_name>]
clear ip
```

DESCRIPTION:

ip Set the ip address and mask for an interface

SYNTAX:

```
<ip_address> Device's network interface address
<mask> Netmask of ip_address
<sby_ip_addr> Device failover peer's network interface address
<4-16> Number of retries performed by dhcp client, default is 4
<interface>: Interface hardware name as used by 'interface' command.
Composed of <type> <port>[/<subif_number>] or
<type> <slot>/<port>[/<subif_number>]
<if_name>: Interface name assigned by 'nameif' command
```

see also: nameif, security-level

```
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# help shut
```

USAGE:

```
[no] shutdown
```

DESCRIPTION:

shutdown Shutdown the selected interface

```
(config-if)# no shutdown
(config-if)# exit
(config)# exit
# show ip add
# sh ip add
```

System IP Addresses:

```
IP address outside 192.168.1.1
IP address inside 0.0.0.0
IP address inf2 0.0.0.0
```

Current IP Addresses:

```
IP address outside 0.0.0.0
IP address inside 0.0.0.0
IP address inf2 0.0.0.0
```

```
# show running
```

```
myPIX # sh int e0
```

```
Interface Ethernet0 outside, is up, line protocol is up
Hardware is i82559, BW 100 Mbps
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 000d.6585.77d9, MTU 1500
IP address 192.168.1.1, subnet mask 255.255.255.0
0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1 packets output, 64 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (128/128) software (0/0)
output queue (curr/max blocks): hardware (0/1) software (0/1)
Received 0 VLAN untagged packets, 0 bytes
Transmitted 1 VLAN untagged packets, 28 bytes
Dropped 0 VLAN untagged packets
```

```
myPIX # sh int e1
```

```
Interface Ethernet1 inside, is down, line protocol is down
  Hardware is i82559, BW 100 Mbps
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000d.6585.77d9, MTU 1500
    IP address 0.0.0.0, subnet mask 255.255.255.0
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software (0/0)
    output queue (curr/max blocks): hardware (0/1) software (0/1)
    Received 0 VLAN untagged packets, 0 bytes
    Transmitted 1 VLAN untagged packets, 28 bytes
    Dropped 0 VLAN untagged packets
```

Cisco PIX Challenge 2

Outline

This challenge involves the configuration of basic PIX details.

Objectives

The objectives of this challenge are to:

- Define the IP address and subnet mask of E1.
- Define the IP address and subnet mask of E2.

Example (Ver 6.x)

```
> enable
# nameif
# config t
(config)# ip address inf2 192.168.1.1 255.255.255.0
(config)# ip address inside 10.0.1.1 255.255.0.0
(config)# interface e1 auto
(config)# interface e2 auto
(config)# exit
# show ip
```

```

# show running
# sh int e1
Interface Ethernet1 inside, is up, line protocol is up
  Hardware is i82559, BW 100 Mbps
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000d.6585.77d9, MTU 1500
    IP address 192.168.1.1, subnet mask 255.255.255.0
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software (0/0)
    output queue (curr/max blocks): hardware (0/1) software (0/1)
    Received 0 VLAN untagged packets, 0 bytes
    Transmitted 1 VLAN untagged packets, 28 bytes
    Dropped 0 VLAN untagged packets

```

Example (Ver 7.x)

```

> enable
# sh nameif
# config t
(config)# int e1
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int e2
(config-if)# ip address outside 192.168.2.1 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# exit
# show ip add
# show running
# sh int e1
Interface Ethernet1 inside, is up, line protocol is up
  Hardware is i82559, BW 100 Mbps
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000d.6585.77d9, MTU 1500
    IP address 192.168.1.1, subnet mask 255.255.255.0
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software (0/0)
    output queue (curr/max blocks): hardware (0/1) software (0/1)
    Received 0 VLAN untagged packets, 0 bytes
    Transmitted 1 VLAN untagged packets, 28 bytes
    Dropped 0 VLAN untagged packets

```

Cisco PIX Challenge 3

Outline

This challenge involves the configuration of basic PIX details.

Objectives

The objectives of this challenge are to:

- Define the name of each of the interfaces.

Example (Ver 6.x)

```
> enable
# nameif
# config t
(config)# nameif e0 mars security0
(config)# nameif e1 pluto security100
(config)# nameif e2 jupiter security50
(config)# help username
```

USAGE:

```
username <username> {nopassword|password <password>
                    [encrypted]} [privilege <level>]
no username <name>
[no] username <name> attributes
clear configure username [<name>]
show running-config [all] username [<name> [attributes]]
```

DESCRIPTION:

username Configure user authentication local database

SYNTAX:

```
<username>            The name of the user. A minimum of 4 characters is required.
                      A maximum of 64 characters is allowed.
<nopassword>         Indicates that this user has no password
<password>            The password for this user
encrypted             Indicate the <password> entered is encrypted
<level>                The privilege level for this user
attributes            Enter the attributes sub-command mode
(config)# username fred password bert
(config)# exit
# show running
```

Example (Ver 7.x)

```
> enable
# nameif
# config t
(config)# int e0
(config-if)# nameif mars
(config-if)# security-level 0
(config-if)# exit
(config)# int e1
(config-if)# nameif pluto
(config-if)# security-level 100
```

```
(config-if)# exit
(config)# int e2
(config-if)# help nameif
```

USAGE:

```
nameif <if_name>
no nameif [<if_name>]
show running-config [all] nameif [<interface>]
show nameif [<interface>]
clear nameif
```

DESCRIPTION:

nameif Assign name to interface

SYNTAX:

<if_name> A name by which this interface will be referred in all other commands
<interface>: Interface identifier as used in the 'interface' command.

see also: security-level, interface, static, global, nat

```
(config-if)# nameif jupiter
(config-if)# help security-level
```

USAGE:

```
security-level <0-100>
no security-level [<0-100>]
```

DESCRIPTION:

security-level Specify security level of interface

SYNTAX:

<0-100> The security level of this interface from 0 to 100. The relative security level between two interfaces determines the way the Adaptive Security Algorithm is applied. A lower security_level interface is outside relative to a higher level interface and equivalent interfaces are outside to each other.

see also: nameif

```
(config-if)# security-level 50
(config-if)# exit
(config)# help username
```

USAGE:

```
username <username> {nopassword|password <password>
                    [encrypted]} [privilege <level>]
no username <name>
[no] username <name> attributes
clear configure username [<name>]
show running-config [all] username [<name> [attributes]]
```

DESCRIPTION:

username Configure user authentication local database

SYNTAX:

```
<username>      The name of the user. A minimum of 4 characters is required.
                 A maximum of 64 characters is allowed.
<nopassword>    Indicates that this user has no password
<password>      The password for this user
encrypted        Indicate the <password> entered is encrypted
<level>         The privilege level for this user
attributes       Enter the attributes sub-command mode
(config)# username fred password bert
(config)# exit
# show running
# show running user
```

Cisco PIX Challenge 4

Outline

This challenge involves the configuration of basic PIX details.

Objectives

The objectives of this challenge are to:

- Defines a hostname and passwords
- Enables the HTTP server.
- Defines a MOTD banner.

Example (Ver 6.x)

```
> enable
# nameif
# config t
(config)# hostname mars
(config)# help enable
```

USAGE:

```
enable password [<pw>] [level <level>] [encrypted]
no enable password level <level>
show running-config enable
```

DESCRIPTION:

enable Configure enable passwords

SYNTAX:

```
<pw>            The password for this privilege level
<level>         The privilege level
<encrypted>     Indicates that this password is encrypted
(config)# enable ?
```

configure mode commands/options:
password Configure password for the enable command
(config)# enable password ?

configure mode commands/options:
WORD Enter a password for the privilege level
<cr>
(config)# enable password kirk
(config)# password ?

configure mode commands/options:
WORD A password of up to 16 alphanumeric characters
(config)# passwd kent
(config)# help password

USAGE:

[no] password|passwd <password> encrypted
clear configure passwd

DESCRIPTION:

passwd Change Telnet console access password

SYNTAX:

<password> A password of up to 16 alphanumeric characters
Factory-default password is cisco

encrypted Indicate the <password> entered is encrypted

see also: telnet

(config)# help http

USAGE:

[no] http <local_ip> <mask> <if_name>
[no] http server enable

DESCRIPTION:

http Configure HTTP server

SYNTAX:

<local_ip> The ip address of the host and/or network authorized to
access the device HTTP server.

<mask> The IP netmask to apply to <local_ip>.
Default is 255.255.255.255.

<if_name> Network interface name.

see also: password, aaa

(config)# http server enable

(config)# help banner

USAGE:

banner {exec | login | motd} <text>
no banner {exec | login | motd} [<text>]
show banner [{exec | login | motd}]

```
clear banner
```

DESCRIPTION:

banner Configure login/session banners

SYNTAX:

exec Configures the system to display a banner before the enable prompt is displayed.

login Configures the system to display a banner before the password login prompt when accessing the device using telnet.

motd Configures the system to display a message-of-the-day banner.

<text> A line of the message to be displayed. It will be added to the end of an existing banner. The tokens \$(domain) and \$(hostname) will be replaced with the host name and domain name.

```
(config)# banner motd hello
(config)# show banner
# show banner
```

Example (Ver 7.x)

As V6.0, but use **show running banner** instead of **show banner**.

Cisco PIX Challenge 5

Outline

This challenge involves the configuration of a static route, and some banners.

Objectives

The objectives of this challenge are to:

- Define a static route.
- Define banners.

Example

```
(config)# help route
```

USAGE:

```
[no] route <if_name> <foreign_ip> <mask> <gateway>
      [<metric>|tunneled]
clear configure route [<if_name>]
clear route [<if_name>]
show running-config route
show route [<if_name>]
```

DESCRIPTION:

route Enter a static route for an interface

SYNTAX:

<if_name> The interface name, as specified by the 'nameif' command, for which the route will apply

<foreign_ip> The foreign network for this route, 0 means default

<mask> The netmask for the destined foreign network <foreign_ip>

<gateway> The address of the gateway by which <foreign_ip> is reached

<metric> Distance metric for this route, default is 1

tunneled Specifies route as the default tunnel gateway for VPN traffic.

see also: rip, ping

```
(config)# route inside 10.0.0.0 ?
```

configure mode commands/options:

A.B.C.D The netmask for the destined foreign network

```
(config)# route inside 10.0.0.0 255.255.0.0 ?
```

configure mode commands/options:

Hostname or A.B.C.D The address of the gateway by which the foreign network is reached.

```
(config)# route inside 10.0.0.0 255.255.0.0 206.59.124.10 ?
```

configure mode commands/options:

<1-255> Distance metric for this route, default is 1
tunneled Enable the default tunnel gateway option, metric is set to 255

```
(config)# route outside 10.0.0.0 255.255.0.0 206.59.124.10
```

```
(config)# show route
```

```
(config)# banner motd admin device
```

```
(config)# banner login personal device
```

```
(config)# banner exec main device
```

```
(config)# show domain-name
```

```
(config)# domain-name dumfries.eu
```

```
(config)# exit
```

```
# show route
```

```
S 10.0.0.0 255.255.0.0 [1/0] via 206.59.124.10, inside
C 192.168.0.1 255.255.255.0 is directly connected, glasgow
C 192.168.1.1 255.255.255.0 is directly connected, inside
C 192.168.2.1 255.255.255.0 is directly connected, dmz
```

Cisco PIX Challenge 6

Outline

This challenge involves the configuration of Telnet, SSH and Console timeouts.

Objectives

The objectives of this challenge are to:

- Setup the hostname.
- Define the domain name.
- Define the Telnet timeout.
- Define the SSH timeout.
- Define the Console timeout.

Example

```
myPIX (config)# hostname arizona
```

```
arizona (config)# domain-name fife.nu
```

```
arizona (config)# show domain-name
```

```
myPIX (config)# help telnet
```

USAGE:

```
[no] telnet <local_ip> <mask> <if_name>
telnet timeout <number>
no telnet timeout [<number>]
```

DESCRIPTION:

telnet Add telnet access to device console and set idle timeout

SYNTAX:

<local_ip> The ip address of the host and/or network authorized to login to the device

<mask> The IP netmask to apply to <local_ip>.

<if_name> Network interface name.

<number> Idle time in minutes after which a telnet session will be closed. Default is 5 minutes.

see also: ssh, password, aaa

```
arizona (config)# telnet timeout 8
```

```
arizona (config)# help ssh
```

USAGE:

```
[no] ssh <local_ip> <mask> <if_name>
[no] ssh timeout <number>
[no] ssh version 1|2
[no] ssh scopy enable
show ssh sessions [<client_ip>]
ssh disconnect <session_id>
```

DESCRIPTION:

ssh Add SSH access to the Device console, set idle timeout, set version supported, enable Secure Copy as an SSH application, display a list of active SSH sessions, and terminate an SSH session.

SYNTAX:

<local_ip> The IP address of the host and/or network authorized to login to the Device.

<mask> The IP netmask to apply to <local_ip>.

<if_name> Network interface name.

<number> Idle time in minutes after which a SSH session will be closed.

<client_ip> The IP address of the SSH client.

<session_id> Session ID as displayed by the 'show ssh sessions' command.

see also: telnet, password, enable, aaa
arizona (config)# ssh timeout 9
pixfirewall(config)# help console

USAGE:

[no] console timeout <number>

DESCRIPTION:

console Set idle timeout for the serial console of the PIX

SYNTAX:

<number> Valid range <0-60>. For <1..60>, console session will be closed after idle time of <1..60> minutes. console will never close for timeout <0>

see also: telnet, ssh, passwd, aaa
arizona (config)# console timeout 9

arizona (config)# show telnet
arizona (config)# show ssh
arizona (config)# show console

Cisco PIX Challenge 7

Outline

This challenge involves the configuration of the security levels on the interfaces.

Objectives

The objectives of this challenge are to:

- Rename the interfaces, and define the security level on each interface.

Note: A port with the name of outside always has a security level of 0, while a port with the name of inside always has a security level of 100.

Example (Ver 6.x)

```
myPIX (config)# nameif e0 strathclyde security24
myPIX (config)# nameif e1 orkney security61
myPIX (config)# nameif e2 rhodeisland security44
```

Example (Ver 7.x)

```
> enable
# nameif
# config t
(config)# int e0
(config-if)# nameif strathclyde
(config-if)# security-level 24
(config-if)# exit
(config)# int e1
(config-if)# nameif orkney
(config-if)# security-level 61
(config-if)# exit
(config)# int e2
(config-if)# nameif rhodeisland
(config-if)# security-level 44
(config-if)# exit
(config)# exit
# show running
```

Cisco PIX Challenge 8

Outline

This challenge involves the configuration of a shutdown on the interfaces.

Objectives

The objectives of this challenge are to:

- Define the names of the interfaces.
- Shutdown each of the interfaces.

Example (6.x)

```
myPIX (config)# nameif e0 gretna security0
myPIX (config)# nameif e1 alabama security100
myPIX (config)# nameif e2 uranus security50
myPIX (config)# show nameif

myPIX (config)# interface e0 auto shut
myPIX (config)# interface e1 auto shut
myPIX (config)# interface e2 auto shut
myPIX (config)# show int
myPIX (config)# show int e0
```

```
myPIX (config)# show int e1
myPIX (config)# show int e2
```

Example (Ver 7.x)

```
> enable
# nameif
# config t
(config)# int e0
(config-if)# nameif gretna
(config-if)# security-level 0
(config-if)# shutdown
(config-if)# exit
(config)# int e1
(config-if)# nameif alabama
(config-if)# security-level 100
(config-if)# shutdown
(config-if)# exit
(config)# int e2
(config-if)# nameif uranus
(config-if)# security-level 50
(config-if)# shutdown
(config-if)# exit
(config)# exit
# show running
```

Cisco PIX Challenge 9

Outline

This challenge involves the configuration of interfaces.

Objectives

The objectives of this challenge are to:

- Define the names of the interfaces.
- Define the basic operation of the interfaces.

Example (Ver 6.x)

```
myPIX (config)# nameif e0 hawaii security0
myPIX (config)# nameif e1 alberta security100
myPIX (config)# nameif e2 orkney security50

myPIX (config)# interface e0 100full
myPIX (config)# interface e1 100full
myPIX (config)# interface e2 100full
```

Example (Ver 7.x)

```
> enable
```

```
# nameif
# config t
(config)# help interface
```

USAGE:

```
interface <type> <port>
interface <type> <port>.<subif_number>
no interface <type> <port>.<subif_number>
show running-config [default] interface {<type> <port>[.<subif_number>]}
show interface {<type> <port>[.<subif_number>] | <if_name>}
    [detail|stats|ip brief]
clear config interface {<type> <port>[.<subif_number>]}
clear interface {<type> <port>[.<subif_number>]}
```

DESCRIPTION:

```
interface      Set network interface parameters
                show/clear interface counters
                show brief summary of IP status and configuration
```

SYNTAX:

```
<type>          Type of interface to be configured
                Possible values: Ethernet, GigabitEthernet
<port>          Port number. Refer to the appropriate hardware manual for
                port information
<subif_number>  Subinterface number in the range 1 to 4,294,967,293
<if_name>       Interface name assigned by 'nameif' command
```

WARNING! Using 'no' on a Subinterface will remove the interface from the system. Removing a Subinterface will delete all configuration rules applied to the interface. Exercise caution when using the 'no interface' command.

see also: allocate-interface

```
(config)# int e0
(config-if)# nameif gretna
(config-if)# security-level 0
(config-if)# help du
```

USAGE:

```
duplex auto|full|half
no duplex [auto|full|half]
```

DESCRIPTION:

```
duplex          Configure duplex operation
```

SYNTAX:

```
auto           Enable AUTO duplex configuration
full           Force full duplex operation
half           Force half-duplex operation
```

see also: speed

```
(config-if)# duplex full
(config-if)# help speed
```

USAGE:


```

myPIX (config)# dhcpd enable inside
myPIX (config)# dhcpd dns 197.174.60.1
myPIX (config)# dhcpd address 197.174.60.2-197.174.60.22 inside
myPIX (config)# dhcpd wins 195.94.110.3
myPIX (config)# dhcpd lease 6
myPIX (config)# dhcpd domain athome.com
myPIX (config)# show dhcpd

```

Example

```
myPIX (config)# help dhcpd
```

USAGE:

```

dhcpd address <ip1>[-<ip2>] <srv_ifc_name>
dhcpd dns <dnsip1> [<dnsip2>]
dhcpd wins <winsip1> [<winsip2>]
dhcpd lease <lease_length>
dhcpd ping_timeout <timeout>
dhcpd domain <domain_name>
dhcpd option <code> {ascii <string> | hex <hex_string> |
    ip <address_1> [<address_2>]}
dhcpd enable <srv_ifc_name>
dhcpd auto_config <clnt_if_name>
show dhcpd [binding|statistics]
clear dhcpd
clear dhcpd [binding|statistics]

```

DESCRIPTION:

```
dhcpd          Configure DHCP Server
```

SYNTAX:

```

<ip1>          Start address of the DHCP address pool
<ip2>          End address of the DHCP address pool
<dnsip>        DNS server IP address
<winsip>       NetBios name server IP address
<lease_length> DHCP lease length in seconds
<timeout>      Ping timeout in milliseconds
<domain_name>  DNS domain name
<code>         positive number representing the DHCP option code
<string>       ASCII string without whitespace
<hex_string>   hexadecimal string without whitespace
<address_1>    IP address
<address_2>    IP address
<srv_ifc_name> Interface to enable DHCP server

```

```
<clnt_if_name> Interface to retrieve DHCP client info
```

```

myPIX (config)# dhcpd enable inside
myPIX (config)# dhcpd address 197.174.60.2-197.174.60.22 inside
myPIX (config)# dhcpd wins 195.94.110.3
myPIX (config)# dhcpd lease 6
myPIX (config)# dhcpd domain athome.com
myPIX (config)# show dhcpd

```

Cisco PIX Challenge 11

Outline

This challenge involves the configuration of fixups.

Objectives

The objectives of this challenge are to:

- Define fixup protocols.
- Show fixup protocols.

Example (V6.x)

```
myPIX (config)# help fixup
```

```
USAGE:
```

```
    [no] fixup protocol <prot> [<option>] <port>[-<port>]
```

```
DESCRIPTION:
```

```
fixup          Add or delete inspection service and feature defaults
```

```
SYNTAX:
```

```
<prot> Protocol fixup to be enabled or disabled:
```

```
ctiqbe, dns [maximum-length <length>], ftp [strict], h323,  
http, icmp [error], ils, mgcp, netbios, pptp, rsh, rtsp, sip,  
skinny, smtp, snmp, sqlnet, sunrpc, sunrpc_udp, tftp, xdmcp
```

```
The fixup can be disabled via the no form of the command, e.g.,
```

```
no fixup protocol ftp strict 21
```

```
<option>
```

```
option to the inspection function
```

```
<port1>[-<port2>]
```

```
A range of ports to enable the fixup
```

```
myPIX (config)# fixup protocol ?
```

```
configure mode commands/options:
```

```
ctiqbe  
dns  
ftp  
h323  
http  
icmp  
ils  
mgcp  
netbios  
pptp  
rsh
```

```
rtsp
sip
skinny
smtp
snmp
sqlnet
sunrpc
sunrpc_udp
tftp
xdmcp
```

myPIX (config)# fix pro http ?

configure mode commands/options:

```
WORD Specify port(s) to enable fixup, <port1>[-<port2>]; default port(s):
ctiqbe-----2748 ftp-----21
gtp-----2123,3386 h323-h225-----1720
h323-ras-----1718-1719 http-----80
ils-----389 mgcp-----2427,2727
netbios-----137-138 pptp-----1723
rsh-----514 rtsp-----554
sip-----5060 skinny-----2000
smtp-----25 snmp-----161
sqlnet-----1521 sunrpc-----111
sunrpc_udp-----111 tftp-----69
xdmcp-----177
highs Ports 1024-65535
lows Ports 1-1023
udp Enable SIP over UDP application inspection
```

myPIX (config)# fixup protocol http 161

myPIX (config)# fixup protocol ftp 60

myPIX (config)# fixup protocol smtp 84

myPIX (config)# show fixup

Example (V7.x)

As V6.x but replace show fixup with:

myPIX # sh run fix

```
INFO: All 'fixup' commands have been converted to 'inspect' commands.
Please use 'show running-config service-policy' in conjunction
with 'show running-config policy-map' to view the new configuration.
```

myPIX # sh run service-p

```
service-policy global_policy global
```

myPIX # sh run policy-m

```
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
```

```
inspect sip
inspect netbios
inspect tftp
inspect http
!
```

Cisco PIX Challenge 12

Outline

This challenge involves the configuration of an encryption key.

Objectives

The objectives of this challenge are to:

- Define the domain name.
- Define a user and a password.
- Create an RSA key.
- Show the RSA key.

Example

```
myPIX (config)# domain-name fife.nu
myPIX (config)# username fred password bert
myPIX (config)# help ca
```

USAGE:

```
crypto ca trustpoint <name>
no crypto ca trustpoint <name> [noconfirm]
crypto ca authenticate <name> [fingerprint <hex value>] [nointeractive]
crypto ca enroll <name> [noconfirm]
crypto ca import <name> certificate [nointeractive]
crypto ca import <name> pkcs12 <passphrase> [nointeractive]
crypto ca export <name> pkcs12 <passphrase>
crypto ca crl request <name>
crypto ca certificate map <sequence #>
crypto ca certificate chain <name>
clear configure crypto ca trustpoint
clear configure ca certificate map [<sequence #>]
clear crypto ca crls [<name>]
show crypto ca crls [<name>]
show crypto ca certificates [<name>]
show running-config [all] crypto ca
```

DESCRIPTION:

ca Configure the Certification Authority.

SYNTAX:

trustpoint	Define a CA trustpoint
authenticate	Get the CA certificate
enroll	Request a certificate from a CA

```

import          Import certificate or pkcs-12 data
export         Export a trustpoint configuration with all associated
              keys and certificates in PKCS12 format
crl            For manual CRL polling, displaying, and erasing.
certificate map Define certificate attributes map
certificate chain Enter certificate chain configuration mode for the
              indicated trustpoint
noconfirm      Suppress all interactive prompting
nointeractive   Execute the command in non-interactive mode
fingerprint    A key consisting of alphanumeric characters that is
              used to authenticate the CA's certificate.
<name>        A nickname for the CA server.
<passphrase>  A required password that gives the CA administrator
              some authentication when a user calls to ask for a
              certificate to be revoked.
              It can be up to 80 characters in length.
<sequence #> Sequence to insert into certificate map entry
see also: key, crypto, ipsec, isakmp, tunnel-group
myPIX (config)# ca generate rsa key 256
myPIX (config)# show ca mypubkey rsa

```

Cisco PIX Challenge 13

Outline

This challenge involves the configuration of NAT.

Objectives

The objectives of this challenge are to:

- Define inside address range.
- Define outside address range.
- Show NAT parameters.
- Show Global parameters.

Example (Ver 6.x)

```
myPIX (config)# help nat
```

USAGE:

```

[no] nat (<if_name>) <nat_id> <local_ip> [<mask>]
      [dns] [outside]
      [[tcp] <max_conns> [<emb_limit> [<norandomseq>]]]
      [udp <udp_max_conns>]
[no] nat (if_name) <nat_id> access-list <acl-name>
      [dns] [outside]
      [[tcp] <max_conns> [<emb_limit> [<norandomseq>]]]
      [udp <udp_max_conns>]

```

DESCRIPTION:

nat Associate a network with a pool of global IP addresses

SYNTAX:

<if_name> The name of the network interface, as specified by 'nameif', where the hosts/network designated by <local_ip> are accessed.

<nat_id> The id of this group of hosts or networks. This id will be referenced by the 'global' command to associate a global pool with this command. The id '0' is reserved to indicate (i) no address translation with the access-list option or (ii) identity translation for the <real_ip> option. The maximum nat_id with access-list is 65535. The maximum nat_id without access-list is 2147483647.

<local_ip> The hosts/networks in this <nat_id> group. '0' indicates all networks or the default <nat_id> group. An IP address not found in a more explicit <nat_id> group will default to a less explicit or '0', the least explicit

<mask> The IP netmask to apply to <local_ip>.

dns Use the created xlate to rewrite DNS address record.

tcp TCP connections.

udp UDP connections.

<max_conns> The maximum number of simultaneous connections. the <local_ip> hosts will each be allowed to use. Idle connections are closed after the time specified by the timeout conn command.

<emb_limit> The maximum number of embryonic connections per host. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

norandomseq Disable TCP sequence number randomization.

<acl-name> access-list name.

see also: access-list, apply, global

myPIX (config)# nat ?

configure mode commands/options:

(Open parenthesis for the name of the network interface where the hosts/network designated by the local IP address are accessed

myPIX (config)# nat (inside) ?

configure mode commands/options:

<0-2147483647> The <nat_id> of this group of hosts/networks. This <nat_id> will be referenced by the global command to associate a global pool with the local IP address. <nat_id> '0' is used to indicate no address translation for local IP. The limit is 65535 with access-lists

myPIX (config)# nat (inside) 1 ?

configure mode commands/options:

Hostname or A.B.C.D The hosts/networks in this <nat_id> group, '0' indicates all networks or the default <nat_id> group
 access-list Specify access-list name after this keyword

myPIX (config)# nat (inside) 1 143.163.128.0 ?

configure mode commands/options:

A.B.C.D IP netmask to apply to the local IP address
<cr>

myPIX (config)# nat (inside) 1 143.163.128.0 255.255.192.0

myPIX (config)# help global

USAGE:

[no] global (<ext_if_name>) <nat_id> {<global_ip>[-<global_ip>] [netmask
<global_mask>]} | interface

DESCRIPTION:

global Specify, delete or view global address pools,
or designate a PAT(Port Address Translated) address

SYNTAX:

<(ext_if_name)> The external network interface name

<nat_id> The id of the nat group(from the nat command) that
will draw from these global addresses

<global_ip> The IP address, network or range of addresses that will
dynamically be translated on an as needed basis to hosts
in the nat group <nat_id>.
If this <ext_if_name> is connected to the Internet, the
<global_ip> should be registered with the Network Information
Center(NIC).
These addresses should also be reverse resolvable(in-addr.arpa)
on the outside DNS servers.
An address specified singly will be used as a PAT address.
When all of the non-PAT addresses of a global pool are in use
and there is a PAT address, subsequent hosts from the nat
group <nat_id> will share the single PAT address for up to
the number of licensed connections.
[netmask <global_mask>] The netmask of the global_ip.

interface IP address of <ext_if_name> overloaded for PAT.

see also: nat, alias, static

myPIX (config)# global ?

configure mode commands/options:

(Open parenthesis for the external network interface name

myPIX (config)# global (outside) 3 ?

configure mode commands/options:

WORD Enter IP address or a range of IP addresses <start_ip>[-<end_ip>]

interface Specifies PAT using the IP address at the interface

myPIX (config)# global (outside) 3 137.68.10.3-137.68.10.23 ?

configure mode commands/options:

netmask Specify netmask for the IP address(es) after this keyword

<cr>

myPIX (config)# global (outside) 3 1.2.3.4 net ?

configure mode commands/options:

A.B.C.D Netmask for the IP address(es)

myPIX (config)# global (outside) 3 137.68.10.3-137.68.10.23 netmask 255.255.255.0

myPIX (config)# show nat

```
myPIX (config)# show global
```

Example (Ver 7.x)

As Ver 6.0, but replace **show nat** and **show global** with:

```
myPIX (config)# show running nat
myPIX (config)# show running global
```

Cisco PIX Challenge 14

Outline

This challenge involves the configuration of a static route.

Objectives

The objectives of this challenge are to:

- Define the IP address and subnet mask of the interfaces.
- Define a static mapping.

Example (Ver 6.x)

```
myPIX (config)# ip address outside 84.120.11.5 255.128.0.0
myPIX (config)# ip address inside 10.10.0.1 255.128.0.0
myPIX (config)# ip address inf 172.16.0.1 255.128.0.0
myPIX (config)# show ip address
myPIX (config)# static (inside, outside) 84.120.11.15 211.204.152.13
myPIX (config)# show static
```

Example (Ver 7.x)

```
myPIX (config)# int e0
myPIX (config-if)# ip address 84.120.11.5 255.128.0.0
myPIX (config-if)# nameif outside
```

```
myPIX (config-if)# int e1
myPIX (config-if)# ip address 10.10.0.1 255.128.0.0
myPIX (config-if)# nameif inside
```

```
myPIX (config-if)# int e2
myPIX (config-if)# ip address 172.16.0.1 255.128.0.0
myPIX (config-if)# nameif inf2
myPIX (config-if)# exit
```

```
myPIX (config)# show ip address
```

```
myPIX (config)# help static
```

USAGE:

```

[no] static [(real_ifc, mapped_ifc)]
    {<mapped_ip>|interface}
    {<real_ip> [netmask <mask>]} | {access-list <acl_name>}
    [dns]
    [[tcp] <max_conns> [<emb_lim> [<norandomseq> [nailed]]]]
    [udp <max_conns>]
[no] static [(real_ifc, mapped_ifc)] {tcp|udp}
    {<mapped_ip>|interface} <mapped_port>
    {<real_ip> <real_port> [netmask <mask>]} |
    {access-list <acl_name>}
    [dns]
    [[tcp] <max_conns> [<emb_lim> [<norandomseq> [nailed]]]]
    [udp <max_conns>]

```

DESCRIPTION:

static Configure one-to-one address translation rule

SYNTAX:

<real_ifc> Name of the network interface, as specified by 'nameif', where the hosts or networks designated by <real_ip> or sources in access-list are accessed.

<mapped_ifc> Name of the network interface, as specified by 'nameif', where the <real_ip> or by the source in access-list are translated into <mapped_ip>.

tcp TCP static PAT.

udp UDP static PAT.

<real_ip> Address as configured at the actual host.

<real_port> Port as viewed from the actual host.

<mapped_ip> Masquerade address of the <real_ip> or of the source address in access-list.

<mask> The IP netmask to apply to <real_ip>.

<mapped_port> Masquerade port of the <real_port> or of the source port in access-list.

interface Address taken from <mapped_ifc>.

<mapped_port> Masquerade port of the <real_port> or of the source port in access-list.

<acl_name> The access-list name with the source fields defining the real address and real port, if applicable, before translation.

dns Rewrite DNS address record.

norandomseq Disable TCP sequence number randomization.

nailed Allow TCP sessions for asymmetrically routed traffic

<max_conn> The maximum number of simultaneous TCP connections that each <real_ip> hosts will each be allowed to use. Idle

connections are closed after the time specified by the timeout conn command.

<emb_limit> Maximum number of embryonic connections per host. An embryonic connection is a connection request that has not completed TCP 3-way handshake between source and destination.

see also: nat, global
myPIX (config)# static ?

configure mode commands/options:

(Open parenthesis for (<internal_if_name>,<external_if_name>) pair
where <internal_if_name> is the Internal or prenat interface and
<external_if_name> is the External or postnat interface

myPIX (config)# static (inside, outside) 84.120.11.15 211.204.152.13
myPIX (config)# show running static

Cisco PIX Challenge 15

Outline

This challenge involves the configuration of the activation key.

Objectives

The objectives of this challenge are to:

- Configure the activation key.
- Show the activation key.

Example

myPIX # help activation-key

USAGE:

activation-key <activation-key-four-or-five-tuple>
show activation-key

DESCRIPTION:

activation-key Modify activation-key.

SYNTAX:

<activation-key-four-or-five-tuple> a four or five element hexadecimal string.
myPIX (config)# activation-key 1aa3aaab abfbcef1 133445ee ee56f6b0
myPIX (config)# show activation-key

Cisco PIX Challenge 16

Outline

This challenge involves the configuration of an access-list.

Objectives

The objectives of this challenge are to:

- Define a named access-list.
- Apply the access-list onto an interface.

Example

myPIX (config)# help access-l

USAGE:

Extended access list:

Use this to configure policy for IP traffic through the firewall

```
[no] access-list <id> [line <line_num>] [extended] {deny | permit}
      {<protocol> | object-group <protocol_obj_grp_id>}
      {host <sip> | <sip> <smask> |
      object-group <network_obj_grp_id>}
      [<operator> <port> [<port>] |
      object-group <service_obj_grp_id>]
      {<dip> <dmask> | object-group <network_obj_grp_id>}
      [<operator> <port> [<port>] |
      object-group <service_obj_grp_id>]
      [log [disable] | [<level>] | [default] [interval <secs>]]
[no] access-list <id> [line <line_num>] {deny | permit} icmp
      {host <sip> | <sip> <smask> |
      object-group <network_obj_grp_id>}
      {<dip> <dmask> | object-group <network_obj_grp_id>}
      [<icmp_type> | object-group <icmp_type_obj_grp_id>}
      [log [disable] | [<level>] | [default] [interval <secs>]]
[no] access-list <id> weftype {deny|permit}
      url {<url-string>|any} [log {disable | default | level}
      [interval <seconds>]] [time-range <name>] [inactive]
[no] access-list <id> weftype {deny | permit}
      tcp {host <host-addr> | <dest-addr> <dest-mask> | any}
      [{{EQ | NEQ | LT | GT} <port> | RANGE <port> <port>}}]
      [log {disable | default | <level>} [interval <seconds>]]
      [time-range <name> ] [ inactive ]
[no] access-list <id> [line <line_num>] remark <text>
access-list deny-flow-max <n>
access-list alert-interval <secs>
```

Standard access list:

Use this to configure policy having destination host or network only

```
[no] access-list <id> standard {deny|permit} {any | <ip> <mask> | host <ip>}
[no] access-list <id> remark <text>
```

Generic Commands:

```

show access-list [<id>]
show running-config access-list
      [alert-interval | deny-flow-max | <id>]
clear configure access-list [<id>]
clear access-list [<id> [counters]]

```

DESCRIPTION:

access-list Add an access list

SYNTAX:

<id> Access list number

<line_num> Specify line number at which ACE should be entered

<weftype> Use this to configure Web related policy

deny Denies access if the conditions are matched.

permit Permits access if the conditions are matched.

object-group Keyword for specifying an object group.

obj_grp_id Identifier of an existing object group.

remark Specify a comment (remark)

<protocol> The IP protocol name or number that will be open
udp is 17, tcp is 6, egp is 47, etc.

<sip> Source IP address

<smask> Mask to be applied to <sip>

<dip> Destination IP address

<dmask> Mask to be applied to <dip>

<operator> Compares <sip> or <dip> ports. Possible operands
include lt (less than), gt (greater than), eq (equal), neq
(not equal), and range (inclusive range).

<port> The decimal number or name of a TCP or UDP port

<text> comment (remark)

log Keyword for enabling log option on this ACL element.

disable Keyword for disabling log option on this ACL element.

default Keyword for set log option on this ACL element to
default values.

<level> Optional syslog level (0-7); default level is 6.

interval Keyword for specifying log interval.

<secs> Optional log interval value (1-600); default is 300.

<icmp_type> 0 echo-reply,

```
3 unreachable,
4 source-quench,
5 redirect,
6 alternate-address,
8 echo,
9 router-advertisement,
10 router-solicitation,
11 time-exceeded,
12 parameter-problem,
13 timestamp-request,
14 timestamp-reply,
15 information-request,
16 information-reply,
17 address-mask-request,
18 address-mask-reply,
31 conversion-error or
32 mobile-redirect
```

see also: access-group, object-group

```
myPIX (config)# access-list uranus permit ip host 26.32.188.8 host 129.67.195.1
```

```
myPIX (config)# access-list uranus deny ip host 201.122.28.7 host 209.215.90.6
```

```
myPIX (config)# help access-g
```

USAGE:

```
[no] access-group <access-list> <in|out> interface <if_name> [per-user-override]
```

DESCRIPTION:

access-group Bind an extended access-list to an interface to filter inbound traffic

SYNTAX:

```
<access-list> Extended access list number
<in|out> Inbound or Outbound access list
<if_name> Name of the interface
per-user-override Allow AAA downloaded per-user ACL to override
```

see also: access-list, object-group

```
myPIX (config)# access-group uranus in interface outside
```

Cisco PIX Challenge 17

Outline

This challenge involves the configuration of object groups.

Objectives

The objectives of this challenge are to:

- Define a network object-group.
- Define a protocol object-group.
- Define an ICMP object-group.

Example

```
myPIX (config)# help object-group
```

USAGE:

```
[no] object-group protocol | network | icmp-type <obj_grp_id>
[no] object-group service <obj_grp_id> tcp|udp|tcp-udp
show running-config [all] object-group
      [protocol | service | icmp-type | network]
show running-config [all] object-group id <obj_grp_id>
clear configure object-group [protocol | service | icmp-type | network]
```

DESCRIPTION:

object-group Create an object group for use in 'access-list'

SYNTAX:

```
protocol                Specifies a group of protocols, such as TCP, etc
network                Specifies a group of host or subnet IP addresses
service                Specifies a group of TCP/UDP ports/services
icmp-type              Specifies a group of ICMP types, such as echo
```

```
<obj_grp_id>            The identifier for the object group:
                       Must be 1 - 64 characters long, consisting of
                       letters, digits, '-', '_', or '.'.
```

```
tcp|udp|tcp-udp        Specifies the protocol type for a service group;
                       tcp - services provided via TCP only, such as ftp
                       udp - services provided via UDP only, such as snmp
                       tcp-udp - services provided via both TCP and UDP
```

```
show                    Show object group(s) running config
```

```
clear                   Remove existing object group(s) config
```

```
see also:              protocol-object, network-object,
                       port-object, icmp-object, group-object
```

```
myPIX (config)# object-group network montana
```

```
myPIX(config-network)# exit
```

```
myPIX (config)# object-group protocol newyork
```

```
myPIX(config-protocol)# exit
```

```
myPIX (config)# object-group icmp-type birmingham
```

```
myPIX(config-icmp-type)# exit
```

Cisco PIX Challenge 18

Outline

This challenge involves the configuration of NTP.

Objectives

The objectives of this challenge are to:

- Define the names of the interfaces.
- Define the details of the NTP servers.

Example (Ver 6.x)

```
> enable
myPIX # config t
myPIX (config)# nameif e0 columbia security0
myPIX (config)# nameif e1 orkney security100
myPIX (config)# nameif e2 florida security50

myPIX (config)# ntp server 73.35.212.5 source columbia
myPIX (config)# ntp server 70.51.127.73 source orkney
myPIX (config)# ntp server 69.49.18.8 source florida
myPIX (config)# show ntp
```

Example (Ver 7.x)

```
> enable
myPIX # config t
myPIX (config)# int e0
myPIX (config-if)# nameif columbia
myPIX (config-if)# security-level 0
myPIX (config-if)# exit
myPIX (config)# int e1
myPIX (config-if)# nameif orkney
myPIX (config-if)# speed 100
myPIX (config-if)# exit
myPIX (config)# int e2
myPIX (config-if)# nameif florida
myPIX (config-if)# security-level 50
myPIX (config-if)# exit
myPIX (config)# help ntp
```

USAGE:

```
ntp authenticate
no ntp authenticate
ntp authentication-key <number> md5 <value>
no ntp authentication-key <number> [md5 <value>]
ntp server <ip_address> [key <number>] [source <if_name>] [prefer]
no ntp server <ip_address> [key <number>] [source <if_name>] [prefer]
ntp trusted-key <number>
```

```
no ntp trusted-key <number>
show ntp [associations [detail] | status]
```

DESCRIPTION:

ntp Configure Network Time Protocol

SYNTAX:

```
<if_name>            The interface name of the time server.
<ip_address>        The ip address of the time server.
<number>            The key number, range <1-4294967295>.
<value>             The key value. Key length range is <1-32>.
```

see also: clock

myPIX (config)# ntp server ?

configure mode commands/options:
 Hostname or A.B.C.D IP address of peer

myPIX (config)# ntp server 73.35.212.5 ?

configure mode commands/options:
 key Configure peer authentication key
 prefer Prefer this peer when possible
 source Interface for source address
 <cr>

pixfirewall(config)# ntp server 73.35.212.5 source ?

configure mode commands/options:
Current available interface(s):
 florida Name of interface Ethernet2
 orkney Name of interface Ethernet1
 columbia Name of interface Ethernet0
myPIX (config)# ntp server 73.35.212.5 source columbia
myPIX (config)# ntp server 70.51.127.73 source orkney
myPIX (config)# ntp server 69.49.18.8 source florida
myPIX (config)# exit
myPIX # show ntp status

Cisco PIX Challenge 19

Outline

This challenge involves the configuration of cable-based failover.

Objectives

The objectives of this challenge are to:

- Enable failover.
- Define failover addresses.
- Define failover poll time.

Example (V6.x)

myPIX (config)# help fail

USAGE:

```
[no] failover
[no] failover polltime [unit] [msec] <time> [holdtime <seconds>]
[no] failover polltime interface <seconds>
[no] failover replication http
[no] failover lan unit primary|secondary
[no] failover interface ip <ifc_name> <ip_address> <mask> standby
    <ip_address>
[no] failover interface-policy <n>[%]
[no] failover key <shared_key>
[no] failover lan interface <ifc_name> <phyifc>[.<subifc_id>]
[no] failover link <ifc_name> [<phyifc>[.<subifc_id>]]
[no] failover mac address <phyifc> <act_mac> <stn_mac>
[no] failover timeout <hh:mm:ss>
[no] failover lan enable
[no] failover active
failover reset
failover reload-standby
show failover [history|interface|state|statistics]
```

DESCRIPTION:

failover Configure failover feature

SYNTAX:

active	Make this the active unit of a failover pair
reset	Force both units back to an unfailed state
<ifc_name>	Interface name
<ip_address>	IP Address
<mask>	IP Netmask
<n>[%]	Number/percent of monitored interfaces causing failover
[unit] [msec] <time>	Unit poll interval (500msec-999msec, 1-15 seconds)
holdtime <seconds>	Unit holdtime (3-45 seconds)
polltime interface <seconds>	Interface poll interval (3-15 seconds)
replication http	Enable HTTP (port 80) connection replication
lan unit {primary secondary}	Specify the unit as primary or secondary
lan interface	Specify the failover interface parameters
link	Specify the stateful interface parameters
interface ip	Specify IP and mask for failover/stateful interface
interface-policy	Specify interface monitoring failure policy
key <shared_key>	Specify failover encryption shared key
show failover	Display failover runtime info
mac address	Specify virtual mac address for a physical interface
<phyifc>	Physical interface name
<subifc_id>	Sub-interface id
<act_mac> <stn_mac>	Active and standby mac address
timeout	Specify failover reconnect timeout value for ASR sessions
lan enable	Enable LAN-Based failover on PIX platform

myPIX (config)# failover active

myPIX (config)# failover ip address outside 157.202.212.2

myPIX (config)# failover ip address inside 73.105.56.11

myPIX (config)# failover ip address inf2 166.209.230.11

myPIX (config)# failover poll 2

```
myPIX (config)# show failover
```

Example (V7.x)

```
myPIX (config)# help fail
```

USAGE:

```
[no] failover
[no] failover polltime [unit] [msec] <time> [holdtime <seconds>]
[no] failover polltime interface <seconds>
[no] failover replication http
[no] failover lan unit primary|secondary
[no] failover interface ip <ifc_name> <ip_address> <mask> standby
    <ip_address>
[no] failover interface-policy <n>[%]
[no] failover key <shared_key>
[no] failover lan interface <ifc_name> <phyifc>[.<subifc_id>]
[no] failover link <ifc_name> [<phyifc>[.<subifc_id>]]
[no] failover mac address <phyifc> <act_mac> <stn_mac>
[no] failover timeout <hh:mm:ss>
[no] failover lan enable
[no] failover active
failover reset
failover reload-standby
show failover [history|interface|state|statistics]
```

DESCRIPTION:

```
failover          Configure failover feature
```

SYNTAX:

```
active            Make this the active unit of a failover pair
reset            Force both units back to an unfailed state
<ifc_name>       Interface name
<ip_address>     IP Address
<mask>          IP Netmask
<n>[%]          Number/percent of monitored interfaces causing failover
[unit] [msec] <time> Unit poll interval (500msec-999msec, 1-15 seconds)
holdtime <seconds> Unit holdtime (3-45 seconds)
polltime interface <seconds> Interface poll interval (3-15 seconds)
replication http Enable HTTP (port 80) connection replication
lan unit {primary|secondary} Specify the unit as primary or secondary
lan interface    Specify the failover interface parameters
link            Specify the stateful interface parameters
interface ip     Specify IP and mask for failover/stateful interface
interface-policy Specify interface monitoring failure policy
key <shared_key> Specify failover encryption shared key
show failover   Display failover runtime info
mac address     Specify virtual mac address for a physical interface
<phyifc>       Physical interface name
<subifc_id>    Sub-interface id
<act_mac> <stn_mac> Active and standby mac address
timeout        Specify failover reconnect timeout value for ASR sessions
lan enable      Enable LAN-Based failover on PIX platform
myPIX (config)# failover active
myPIX (config)# failover int ?
```

```

configure mode commands/options:
  ip Configure the IP address and mask after this keyword
myPIX (config)# fai int ip ?

configure mode commands/options:
  WORD Interface name
myPIX (config)# fai int ip ANY ?

configure mode commands/options:
  Hostname or A.B.C.D Specify the IP address
myPIX (config)# fai int ip ANY 157.202.212.2 ?

configure mode commands/options:
  A.B.C.D Specify the mask for the IP address
myPIX (config)# fai int ip ANY 157.202.212.2 255.255.255.0 ?

configure mode commands/options:
  standby Configure the standby IP address after this keyword
myPIX (config)# fai int ip ANY 157.202.212.2 255.255.255.0 stan ?

configure mode commands/options:
  Hostname or A.B.C.D Specify the IP address
myPIX (config)# fai int ip ANY 157.202.212.2 255.255.255.0 stan 157.202.212.3
?

configure mode commands/options:
  <cr>

myPIX (config)# failover interface ip address outside 157.202.212.2
myPIX (config)# failover interface ip address inside 73.105.56.11
myPIX (config)# failover interface ip address inf2 166.209.230.11

myPIX (config)# failover poll 2
myPIX (config)# show running failover

```

Cisco PIX Challenge 20

Outline

This challenge involves the configuration of failover for a primary device over a LAN.

Objectives

The objectives of this challenge are to:

- Enable failover.
- Define failover addresses.
- Define failover parameters.

Example (V6.x)

```

myPIX (config)# failover active

myPIX (config)# failover ip address outside 157.202.212.2
myPIX (config)# failover ip address inside 73.105.56.11
myPIX (config)# failover ip address inf2 166.209.230.11

myPIX (config)# failover poll 2
myPIX (config)# failover lan key mypix
myPIX (config)# failover lan unit primary
myPIX (config)# failover lan interface inf2
myPIX (config)# show failover

```

Example (V6

7.x)

```
myPIX (config)# failover ?
```

configure mode commands/options:

```

interface          Configure the IP address and mask to be used for failover
                   and/or stateful update information
interface-policy   Set the policy for failover due to interface failures
key                Configure the failover shared secret
lan                Specify the unit as primary or secondary or configure the
                   interface and vlan to be used for failover communication
link               Configure the interface and vlan to be used as a link for
                   stateful update information
mac                Specify the virtual mac address for a physical interface
polltime           Configure failover poll interval
replication        Enable HTTP (port 80) connection replication
timeout            Specify the failover reconnect timeout value for
                   asymmetrically routed sessions

<cr>

```

exec mode commands/options:

```

active             Make this system to be the active unit of the failover pair
reload-standby    Force standby unit to reboot
reset              Force an unit or failover group to an unfailed state

```

```
myPIX (config)# failover active
```

```
myPIX (config)# failover int ?
```

configure mode commands/options:

```
ip                 Configure the IP address and mask after this keyword
```

```
myPIX (config)# fai int ip ?
```

configure mode commands/options:

```
WORD              Interface name
```

```
myPIX (config)# fai int ip ANY ?
```

configure mode commands/options:

```
Hostname or A.B.C.D Specify the IP address
```

```
myPIX (config)# fai int ip ANY 157.202.212.2 ?
```

configure mode commands/options:

```
A.B.C.D           Specify the mask for the IP address
```

```
myPIX (config)# fai int ip ANY 157.202.212.2 255.255.255.0 ?
```

configure mode commands/options:

```
standby           Configure the standby IP address after this keyword
```

```
myPIX (config)# fai int ip ANY 157.202.212.2 255.255.255.0 stan ?
```

configure mode commands/options:

```
Hostname or A.B.C.D Specify the IP address
myPIX (config)# failover interface ip address outside 157.202.212.2 255.255.255.0
myPIX (config)# failover interface ip address inside 73.105.56.11
myPIX (config)# failover interface ip address inf2 166.209.230.11
?
```

configure mode commands/options:

```
<cr>
myPIX (config)# failover interface ip address outside 157.202.212.2
myPIX (config)# failover interface ip address inside 73.105.56.11
myPIX (config)# failover interface ip address inf2 166.209.230.11
```

```
myPIX (config)# failover poll 2
myPIX (config)# failover lan ?
```

configure mode commands/options:

```
enable      Enable LAN-Based failover
interface   Configure the interface and vlan to be used for failover
            communication
unit        Configure the unit as primary or secondary
myPIX (config)# failover lan key mypix
myPIX (config)# failover lan unit primary
myPIX (config)# failover lan interface inf2
myPIX (config)# show running failover
```

Cisco PIX Challenge 21

Outline

This challenge involves the configuration of failover for a secondary device over a LAN.

Objectives

The objectives of this challenge are to:

- Enable failover.
- Define failover addresses.
- Define failover parameters.

Example (V6.x)

```
myPIX (config)# failover active

myPIX (config)# failover ip address outside 157.202.212.2
myPIX (config)# failover ip address inside 73.105.56.11
myPIX (config)# failover ip address inf2 166.209.230.11

myPIX (config)# failover poll 2
myPIX (config)# failover lan key mypix
myPIX (config)# failover lan unit secondary
myPIX (config)# failover lan interface inf2
myPIX (config)# show failover
```

Example (V7.x)

```
myPIX (config)# failover active

myPIX (config)# failover interface ip outside 157.202.212.2 standby 157.202.212.3
myPIX (config)# failover interface ip inside 73.105.56.11 standby 73.105.56.12
myPIX (config)# failover interface ip inf2 166.209.230.11 standby 166.209.230.12

myPIX (config)# failover poll 2
myPIX (config)# failover lan key mypix
myPIX (config)# failover lan unit secondary
myPIX (config)# failover lan interface inf2
myPIX (config)# show failover
```

Cisco PIX Challenge 22

Outline

This challenge involves the configuration of ISAKMP.

Objectives

The objectives of this challenge are to:

- Define ISAKMP.
- Define ISAKMP policy.
- Enable ISAKMP on an interface.

Example

```
pixfirewall(config)# isakmp
Usage:  isakmp policy <priority> authen <pre-share|rsa-sig>
        isakmp policy <priority> encrypt <aes|aes-192|aes-256|des|3des>
        isakmp policy <priority> hash <md5|sha>
        isakmp policy <priority> group <1|2|5>
        isakmp policy <priority> lifetime <seconds>
        isakmp key <key-string> address <ip> [netmask <mask>] [no-xauth] [no-
        config-mode]
        isakmp enable <if_name>
        isakmp identity <address|hostname|key-id> [<key-id-string>]
        isakmp keepalive <seconds> [<retry seconds>]
        isakmp nat-traversal [<natkeepalive>]
        isakmp client configuration address-pool local <poolname> [<pif_name>]
        isakmp peer fqdn|ip <fqdn|ip> [no-xauth] [no-config-mode]
pixfirewall(config)# help isakmp

USAGE:

        isakmp am-disable
        isakmp ipsec-over-tcp [port <port1>..<port10>]
        isakmp disconnect-notify
        (DEPRECATED) isakmp key <keystring> address <peer-address> [netmask <mask>]
[no-xauth] [no-config-mode]
```

```

isakmp enable <if_name>
isakmp identity {auto|address|hostname|key_id <key_id_str>}
(DEPRECATED) isakmp keepalive <threshold> [<retry-interval>]
isakmp nat-traversal [<natkeepalive>]
(DEPRECATED) isakmp client configuration address-pool local <pool-name>
[<if_name>]
(DEPRECATED) isakmp peer fqdn | ip <fqdn | ip> {no-xauth | no-mode-cfg}
isakmp policy <priority> authen {<pre-share|rsa-sig|dsa-sig>}
isakmp policy <priority> encrypt {<des|3des|aes|aes-192|aes-256>}
isakmp policy <priority> group {<1|2|5|7>}
isakmp policy <priority> hash {<md5|sha>}
isakmp policy <priority> lifetime <seconds>
isakmp reload-wait

```

DESCRIPTION:

isakmp Configure ISAKMP key, peer, policy and other options

SYNTAX:

am-disable	Disable inbound aggressive mode connections
ipsec-over-tcp	Enable and configure IPsec over TCP
port	Set IPsec over TCP ports
<port1..port10>	Specify up to 10 IPsec over TCP ports
disconnect-notify	Enable disconnect notification to peers
key	Configure a pre-shared key associated with a peer This command is deprecated. Refer to 'tunnel-group ipsec-attributes' instead
<keystring>	String (ASCII) to be used for authentication pre-share
<peer-address>	IP address of peer associated with pre-shared key
<mask>	Netmask specified in dotted-decimal notation
no-xauth	Specifies an xauth policy exception
no-mode-config	Specifies a config mode policy exception
enable	Enable ISAKMP on specified interface
<if_name>	Interface name on which to enable ISAKMP
identity	Set identity type (address,hostname or key-id)
<address>	Use IP address of the interface for the identity
<auto>	Identity auto(IP address for preshared key and Cert DN for Cert based connections)
<hostname>	Use hostname of the device for the identity
<key-id>	Use specified key-id string for the identity
<key-id-str>	The string to be used as key-id
keepalive	Set keepalive interval. This command is deprecated. Refer to 'tunnel-group ipsec-attributes' instead
<threshold>	Time, in seconds, peer can remain idle before keep-alive monitoring commences
<retry-interval>	Time, in seconds, between keep-alive messages
nat-traversal	Enable and configure nat traversal
<natkeepalive>	Set nat traversal keepalive interval
<priority>	Policy suite priority (1 highest, 65535 lowest)
authentication	Authentication method (pre-share,rsa-sig or dsa-sig)
encryption	Encryption algorithm (des,3des,aes,aes-192 or aes256)
hash	Hash algorithm (md5 or sha)
group	Diffie-Hellman group (1,2,5 or 7)
lifetime	ISAKMP SA lifetime (seconds)
client configuration address-pool local	Configure client IP address pool attribute This command is deprecated. Refer to 'ip local-pool', 'tunnel-group general-attributes address-pool' instead
<pool-name>	Name of ip local pool to allocate dynamic client ip
<if_name>	Interface name the ip local pool is associated with Defaults to 'outside' if not specified

```
peer                Identify a peer security gateway to exempt from Xauth
                    and/or Mode Configuration. This command is deprecated.
                    Refer to 'isakmp identity' instead
<fqdn | ip>        Fully qualified domain name or IP address of a remote
                    peer to be exempted from xauth or config mode policy
reload-wait        Wait for voluntary termination of sessions before reboot
```

```
see also:          ca, dynamic-map, ipsec, map
(config)# isakmp enable outside
(config)# isakmp key ABC&FDD address 176.16.0.2 netmask 255.255.255.255
(config)# isakmp identity address
(config)# isakmp policy 5 authen pre-share
(config)# isakmp policy 5 encrypt des
(config)# isakmp policy 5 hash sha
(config)# isakmp policy 5 group 1
(config)# isakmp policy 5 lifetime 86400

(config)# show isakmp
```

Cisco PIX Challenge 23

Outline

This challenge involves the configuration of crypto details.

Objectives

The objectives of this challenge are to:

- Enable IPSEC.
- Define a crypto map.
- Apply a crypto map.

Example

```
(config)# help sysopt
```

USAGE:

```
[no] sysopt connection { permit-ipsec |
                        timewait | {tcpmss [minimum] <bytes>}
[no] sysopt noproxyarp <if-name>
[no] sysopt nodnsalias { inbound | outbound }
[no] sysopt radius ignore-secret
[no] sysopt uauth allow-http-cache
show running-config [all] sysopt
clear configure sysopt
```

DESCRIPTION:

```
sysopt          Set system functional option
```

SYNTAX:

```

connection permit-ipsec - Exempt IPSec traffic from access check.
connection timewait      - TCP conn undergoes TIMEWAIT state.
connection tcpmss        - Set maximum limit of TCP MSS to <bytes>.
connection tcpmss minimum - Set minimum limit of TCP MSS to <bytes>.
noproxyarp <if-name>     - Disable proxy arp on interface <if-name>.
nodnsalias inbound       - Disable alias inbound DNS A record translation.
nodnsalias outbound      - Disable alias outbound DNS A record translation.
radius ignore-secret     - Ignore secret in RADIUS accounting responses.
uauth allow-http-cache   - Allow browser to use cached user credentials.
see also: alias, ca, ipsec, isakmp, map, dynamic-map

```

```

(config)# sysopt connection permit-ipsec
(config)# help cry

```

USAGE:

```

crypto { ca | dynamic-map | ipsec | isakmp | key | map }
For more detailed help, please refer directly to the subcommands

```

DESCRIPTION:

```

crypto          Configure IPsec, IKE, Certificate Authority and Long Term
                Key Operations

```

SYNTAX:

```

ca              Configure the Certification Authority
                See "crypto ca ?" or "help ca"

dynamic-map     IPsec crypto dynamic-map policy
                See "crypto dynamic-map ?" or "dynamic-map ?" or
                "help dynamic-map"

ipsec           Configure transform-set and IPsec SA lifetime
                See "crypto ipsec ?" or "ipsec ?" or "help ipsec"

isakmp          IKE policy and configuration
                See "crypto isakmp ?" or "isakmp ?" or "help isakmp"

key            Long term key operations
                See "crypto key ?" or "help key"

map            IPsec crypto map policy
                See "crypto map ?" or "map ?" or "help map"

```

```

(config)# crypto ipsec transform-set MYIPSECFORMAT esp-des esp-sha-hmac
(config)# crypto map MYIPSEC 10 ipsec-isakmp
(config)# access-list 111 permit ip 10.0.0.0 255.255.255.0 176.16.0.0
        255.255.255.0
(config)# crypto map MYIPSEC 10 match address 111
(config)# crypto map MYIPSEC 10 set peer 176.16.0.2
(config)# crypto map MYIPSEC 10 set transform-set MYIPSECFORMAT
(config)# crypto map MYIPSEC interface outside

```

Cisco PIX Challenge 24

Outline

This challenge involves the configuration of VPDN.

Objectives

The objectives of this challenge are to:

- Enable PPTP.
- Define local pool.
- Create VPDN group.
- Enable VPDN on an interface.

Example

```
(config)# sysopt connection permit-pptp
(config)# help ip
```

USAGE:

```
ip local pool <poolname> <ip1>[-<ip2>] [mask <netmask>]
ip verify reverse-path interface <if_name>
ip audit {info|attack} action [alarm] [drop] [reset]
ip audit name <audit_name> {info|attack} [action [alarm] [drop] [reset]]
ip audit interface <if_name> <audit_name>
ip audit signature <sig_number> disable
show|clear ip audit count [global] [interface <interface>]
clear configure ip audit [configuration]
```

DESCRIPTION:

```
ip          Define a local address pool
            Configure Unicast RPF on an interface
            Configure the Intrusion Detection System
```

SYNTAX:

```
<poolname>    name of the local address pool
<ip1>[-<ip2>] address range of the local address pool
<netmask>     network mask of the local address pool
<if_name>     The name designated for the interface by the nameif command
info          IDS informational signatures.
attack        IDS attack signatures.
alarm         When a signature match is detected, report the event
              to syslog servers.
drop          When a signature match is detected, drop the offending
              packet.
reset         When a signature match is detected, drop the offending
              packet and close the connection if it is part of an
              active connection.
<audit_name> Audit policy name.
<sig_number>  IDS signature number.
```

```
see also:     interface, ip address (interface sub-mode command),
              show interface, isakmp
```

```
(config)# ip local pool pptp-pool 10.0.0.1-10.0.0.100
```

```
(config)# help vpd
```

USAGE:

```
vpdn group <name>
  accept dialin l2tp
  ppp authentication pap|chap|mschap|eap
  This command has been deprecated. New syntax:
  tunnel-group <name> ppp-attributes
  authentication pap
  authentication chap
  authentication mschap
  authentication eap |
  client configuration address local <address_pool_name> |
  client configuration dns <dns_ip1> [<dns_ip2>]|
  client configuration wins <wins_ip1> [<wins_ip2>]|
  client authentication local|aaa <auth_aaa_group>|
  client accounting <acct_aaa_group>|
  l2tp tunnel hello <hello_time>
show vpdn tunnel [l2tp|pppoe] [id <tnl_id>|packets|state|summary|transport]
show vpdn session [l2tp|pppoe] [id <sess_id>|packets|state|window]
show vpdn pppinterface [id <dev_id>]
show vpdn group [<group_name>]
show vpdn username [user_name]
clear vpdn [group|interface|tunnel|username]
```

DESCRIPTION:

vpdn Configure VPDN (L2TP, PPPoE) Policy

SYNTAX:

<address_pool_name>	local address pool name
<dns_ip>	DNS server ip address
<wins_ip>	WINS server ip address
<auth_aaa_group>	Authentication AAA server group name
<acct_aaa_group>	Accounting AAA server group name
<hello_time>	l2tp tunnel keep-alive hello timeout value (seconds)
<if_name>	Interface to accept L2TP request
<name>	user name
<passwd>	user password
<tnl_id>	tunnel id
<sess_id>	session id
<store-local>	Store in local flash instead of using external config

see also: crypto, aaa-server, ip local pool

```
(config)# vpdn group 1 accept dialin pptp
(config)# vpdn group 1 ppp authentication mschap
(config)# vpdn group 1 ppp encryption mppe 40
(config)# vpdn group 1 client configuration address local pptp-pool
(config)# vpdn group 1 client configuration dns 172.64.10.1
(config)# vpdn group 1 client authentication local
(config)# vpdn enable outside
```

Cisco PIX Challenge 25

Outline

This challenge involves the configuration of URL filtering.

Objectives

The objectives of this challenge are to:

- Setup Websense.
- Define URL filtering.
- Define URL cache distance.

Example

```
(config)# help url-server
```

USAGE:

```
[no] url-server <(if_name)> [vendor websense] host <local_ip> [timeout
<seconds>] [protocol TCP|UDP [version 1|4] [connections <num_conns>]]
[no] url-server <(if_name)> vendor n2h2 host <local_ip> [port <number>]
[timeout <seconds>] [protocol TCP|UDP [connections <num_conns>]]
show url-server stat
clear url-server stat
```

DESCRIPTION:

url-server Specify a URL filter server

SYNTAX:

<if_name> The network interface where the URL filtering server resides.

<vendor_name> The url-server vendor.
The default is Websense. All configured url-servers must have the same vendor. To change vendors first clear out the existing url-server configuration.

<local_ip> The IP address of the URL filtering server

[port <N>] Optional N2H2 port value
Defines which port on the N2H2 server to connect to (for both UDP and TCP).
All configured url-servers must have the same port. To change first clear out the existing url-server configuration.

[timeout <N>] Optional timeout value
Timeout value in seconds for down URL filter server

[protocol TCP|UDP [version 1|4]] Optional definition on protocol communicating to Websense in TCP or UDP (only applicable in 4) and definition to talk to Websense in protocol version 1 or protocol version 4. The optional version number defaults to 1. The N2H2 url-server doesn't have a version number.

<num_conns> The number of TCP connections created from the PIX to the url-server.

stat To print out url server usage statistics

```
see also:      filter, url-cache
myPIX (config)# url-server (inside) vendor websense host 192.168.1.1 timeout 47
myPIX (config)# help filter
```

USAGE:

```
[no] filter url <port>[-<port>]|except <lcl_ip> <mask> <frgn_ip> <mask>
[allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]
      [no] filter ftp <port>[-<port>]|except <lcl_ip> <mask> <frgn_ip> <mask>
[allow] [interact-block]
      [no] filter https <port>[-<port>]|except <lcl_ip> <mask> <frgn_ip> <mask>
[allow]
      [no] filter activex|java <port>[-<port>]|except <lcl_ip> <mask> <frgn_ip>
<mask>
```

DESCRIPTION:

filter Enable, disable, or view URL, FTP, and HTTPS filtering

SYNTAX:

```
url|ftp|https|java|activex      Keyword to turn on URL, FTP, HTTPS, Java,
                                or ActiveX filtering
<port>[-<port>] TCP port number range
except Create an exception to previously specified set of IP
<lcl_ip> The address of local/internal host which is source
          for connections requiring filtering.
<frgn_ip> The address of foreign/external host which is
           destination for connections requiring filtering.
<mask> Network mask to apply to lcl_ip or frgn_ip
[allow] When url-server is down, allow outbound <service> traffic
[proxy-block] Prevent users from connecting to an HTTP proxy server
[longurl-truncate] When a long URL has exceeded the buffer limit,
                   truncate the URL sent to the url-server by only sending the
                   destination hostname or IP address
[longurl-deny] When the long URL buffer is not available, deny
               outbound URL traffic
[cgi-truncate] When a URL has a parameter list prefixed by '?' (e.g. a
               CGI script) truncate the URL sent to the url-server by
               removing all text after and including '?'
[interact-block] Prevent users from connecting FTP server
                 by interactive FTP program
```

```
see also:      url-server (Only apply on URL-filtering)
myPIX (config)# filter url http 0 0 0 0
myPIX (config)# filter url except 204.76.192.7 255.255.252.0 0 0 allow
myPIX (config)# url-cache dst 2
```

Cisco PIX Challenge 26

Outline

This challenge involves the configuration of local AAA.

Objectives

The objectives of this challenge are to:

- Define local AAA.
- Define authentication.

Example

```
myPIX (config)# help aaa-server
```

USAGE:

```
[no] aaa-server <tag> <(if_name)> host <ip_address>
[no] aaa-server <tag> protocol <protocol>
clear configure aaa-server [<tag>]
show running-config [all] aaa-server [<tag> [<(if_name)>
    host <ip_address>]]
show aaa-server [<tag> [host <hostname>]]
show aaa-server protocol <protocol>
clear aaa-server statistics [<tag> [host <hostname>]]
clear aaa-server statistics protocol <protocol>
test aaa-server authentication <group tag> [host <ip_address>]
    [username <user>] [password <password>]
test aaa-server authorization <group tag> [host <ip_address>]
    [username <user>]
```

DESCRIPTION:

aaa-server Define AAA Server group

SYNTAX:

```
<tag>                         Symbolic name of the server group.
<if_name>                     The network interface where the authentication server
                             resides.
<local_ip>                    The IP address of the AAA server.
<protocol>                    The AAA protocol supported by servers in the group.
                             Supported protocol types are radius, tacacs+, sdi,
                             nt, kerberos and ldap
<acct mode>                   Specify either 'simultaneous' or 'single' mode
                             accounting
<reactivation mode>         Specify the method by which failed servers are
                             reactivated. Either timed or depletion.
```

see also: aaa,nameif

```
myPIX (config)# aaa-server orange protocol local
```

```
myPIX (config-aaa-server-group)# exit
```

```
myPIX (config)# username fred password bert
```

```
myPIX (config)# help aaa
```

USAGE:

```

[no] aaa mac-exempt match <mac-list-id>
[no] aaa authentication secure-http-client
[no] aaa authentication|authorization|accounting include|exclude <svc>
    <if_name> <l_ip> <l_mask> [<f_ip> <f_mask>] <server_tag>
[no] aaa authentication serial|telnet|ssh|http|enable console
    <server_tag> [LOCAL]
[no] aaa accounting telnet|ssh|http|serial|enable console <server_tag>
[no] aaa authentication|authorization|accounting match
    <access_list_name> <if_name> <server_tag>
[no] aaa authorization command {LOCAL | <tacacs_server_tag> [LOCAL]}
[no] aaa accounting command {privilege <level>} <tacacs_server_tag>
[no] aaa proxy-limit <proxy limit> | disable
[no] aaa local authentication attempts max-fail <fail-attempts>
clear configure aaa
clear aaa local user {fail-attempts|lockout} {all | username <uname>}}
show running-config [all] aaa [authentication|authorization|accounting
    |max-exempt|proxy-limit]
show aaa local user [lockout]

```

DESCRIPTION:

aaa Enable, disable, or view TACACS+, RADIUS or LOCAL user authentication, authorization and accounting

SYNTAX:

secure-http-client HTTP client authentication is secured (over SSL)

include|exclude Include or exclude the service, local and foreign network which needs to be authenticated, authorized, and accounted

<svc> For Authentication, use the following values: telnet, ftp, http, https, tcp/<port> and tcp/0. For Authorization, use the following values: telnet, ftp, http, https, tcp/0, tcp/<port>, udp/<port>, icmp/<port> or <protocol>[</port>] For Accounting, use the following values: telnet, ftp, http, https, tcp/0, tcp/<port>, udp/<port>, icmp/<port> or <protocol>[</port>] For authentication of console access, telnet access, SSH access and enable mode access, specify telnet|ssh|enable respectively.

<if_name> Authenticate, authorize or account connections originated at an interface.

<l_ip> The address of the local/internal host which is source or destination for connections requiring authentication

<l_mask> Network mask to apply to <l_ip>

<f_ip> The address of the foreign host which is either source or destination for connections requiring authentication

<f_mask> Network mask to apply to <f_ip>

<server_tag> For Authentication and Accounting, use values defined by aaa-server command. For cut-through and 'to the box' Authentication and Command Authorization, the server tag LOCAL, can also be used. Only tacacs+ is supported for 'through the box' Authorization.

LOCAL Predefined server tag for aaa protocol 'local'

The server tag LOCAL can also be used as a fallback method in case of the AAA server tag being unreachable. The AAA Fallback is available only for 'to the box' authentication and command authorization. The fallback method can only be LOCAL and it can be used only if a AAA server is specified for the server_tag

<proxy limit> Number of concurrent proxy connections allowed per user.

<fail-attempts> Number of failed authentication attempts after which user is locked out

<uname> Locally configured username

```
see also:      aaa-server      username
myPIX (config)# aaa authentication http console orange
myPIX (config)# aaa authentication serial console orange
myPIX (config)# aaa authentication telnet console orange
myPIX (config)# aaa authentication enable console orange
```

Cisco PIX Challenge 27

Outline

This challenge involves the configuration of remote AAA.

Objectives

The objectives of this challenge are to:

- Enable AAA.
- Define authentication.

Example

```
myPIX (config)# aaa-server orange protocol radius
myPIX (config)# aaa-server orange (inside) host 155.109.40.4 beetroot
myPIX (config)# aaa authentication http console orange
myPIX (config)# aaa authentication serial console orange
myPIX (config)# aaa authentication telnet console orange
```

Cisco PIX Challenge 28

Outline

This challenge involves the configuration of Telnet, SSH, and HTTP access.

Objectives

The objectives of this challenge are to:

- Define Telnet access on interfaces.
- Define SSH access on interfaces.
- Enable HTTP server.
- Define HTTP access on interfaces.
- Define timeouts for servers.

Example

```
myPIX (config)# telnet 204.134.17.7 255.255.192.0 inside
myPIX (config)# telnet 201.13.14.2 255.255.240.0 outside
myPIX (config)# telnet 210.1.170.5 255.255.224.0 inf2
myPIX (config)# telnet timeout 10
myPIX (config)# show telnet
myPIX (config)# show telnet timeout
myPIX (config)# ssh 204.134.17.7 255.255.192.0 inside
myPIX (config)# ssh timeout 10
myPIX (config)# http server enable
myPIX (config)# http 204.134.17.7 255.255.192.0 inside
myPIX (config)# http 201.13.14.2 255.255.240.0 outside
```

Cisco PIX Challenge 29

Outline

This challenge involves the configuration of SNMP.

Objectives

The objectives of this challenge are to:

- Define SNMP community.
- Define SNMP location.
- Define SNMP host.
- Define SNMP contact.
- Enable SNMP traps.

Example

```
> en
```

```
myPIX # config t
myPIX (config)# help snmp-server
```

USAGE:

```
[no] snmp-server community|contact|location <text>
[no] snmp-server host <if_name> <local_ip> [trap|poll]
      [community <text>] [version {1|2c}] [udp-port <port>]
[no] snmp-server enable [traps [all | <feature> [<trap1> ... <trapn>]]]
show snmp-server statistics
show running-config [all] snmp-server
clear configure snmp-server
```

DESCRIPTION:

snmp-server Provide SNMP and event information

SYNTAX:

```
community Configure the community string.
contact Text for mib object sysContact.
location Text for mib object sysLocation.
<text> The contact person name, location, or community string.
host Specify hosts to receive SNMP traps and send SNMP polls.
<if_name> The network interface where the SNMP management station resides.
<local_ip> The address of the SNMP management station.
[trap|poll] specify whether the host can poll or receive traps.
Default is both.
udp-port Override the default SNMP trap port.
Only valid when host may receive traps.
<port> The port to which traps will be sent.
version SNMP version to use for notification message.
[1|2c] Use SNMPv1 or SNMPv2c.
enable Enable/Disable snmp-server or particular traps.
traps Enable/disable particular traps to SNMP management station(s).
all Enable/disable traps for all features.
<feature> The feature for which traps are enabled.
<trapn> A specific trap to enable.
listen-port Configure the SNMP engine's listening port.
statistics Show snmp-server statistics.
```

see also: logging

myPIX (config)# snmp-server

Not enough arguments.

Usage: [no] snmp-server community|contact|location <text>

```

        [no] snmp-server host [<if_name>] <local_ip> [trap|poll]
        [no] snmp-server enable traps
myPIX (config)# snmp-server community oldest ro
myPIX (config)# snmp-server location edinburgh
myPIX (config)# snmp-server host inside 160.61.110.11
myPIX (config)# snmp-server contact june
myPIX (config)# snmp-server enable traps

```

Cisco PIX Challenge 30

Outline

This challenge involves the configuration of logging.

Objectives

The objectives of this challenge are to:

- Enable logging.
- Define logging levels.

Example

```

> en
myPIX # config t

```

```

myPIX (config)# help logg

```

USAGE:

```

        [no] logging enable
        [no] logging timestamp
        [no] logging standby
        [no] logging debug-trace
        [no] logging emblem
        [no] logging flash-bufferwrap
        [no] logging flash-minimum-free <kbytes>
        [no] logging flash-maximum-allocation <kbytes>
        [no] logging ftp-bufferwrap
        [no] logging ftp-server <ftp-server> <path> <username> <password>
        [no] logging buffer-size <bytes>
        [no] logging permit-hostdown
        [no] logging from-address <mail-address>
        [no] logging recipient-address <mail-address> [level <level>]
        [no] logging host <in_if> <l_ip> [{tcp|6}|{udp|17}[/<port#>]] [format
emblem]
        [no] logging console <level>|<list>
        [no] logging buffered <level>|<list>
        [no] logging mail <level>|<list>
        [no] logging monitor <level>|<list>
        [no] logging history <level>|<list>
        [no] logging trap <level>|<list>
        [no] logging message <syslog_id> level <level>
        [no] logging asdm <level>|<list>

```

```

[no] logging asdm-buffer-size <num_of_msgs>
[no] logging facility <fac>
[no] logging device-id {hostname | ipaddress <if_name>
    | string <text> | context-name}
[no] logging queue <queue_size>
[no] logging rate-limit <unlimited | <num> [interval]> message
    <syslog_id> (FWSM only)
[no] logging rate-limit <unlimited | <num> [interval]> level
    <syslog_level> (FWSM only)
[no] logging class <class> <dest1> <level> [<dest2> <level>..]
[no] logging list <list> level <level> [class <class>]
[no] logging list <list> message <syslog_id1>[-<syslog_id2>]
clear logging buffer
clear config logging [disable | level | rate-limit | asdm]
show logging [{message [<syslog_id>|all]} | setting | asdm]
show running-config [all] logging [level | disabled | rate-limit]

```

DESCRIPTION:

logging Enable logging facility

SYNTAX:

```

enable            Enable logging to all supported destinations
timestamp        Enable logging time-stamp on syslog file
standby          Enable logging on standby unit with failover enabled
debug-trace      redirect debug trace output to syslog
ftp-server       Set external ftp server info
<ftp-server>    FTP server name or IP address
<path>           Directory PATH on ftp server for saved log file
<username>       User login on ftp server
<password>       Password for username
buffer-size      Specify the logging buffer size
<bytes>          Logging buffer in bytes. Default/min. is 4096, and
                 max. is 1048576 bytes
permit-hostdown Allow new connection even if TCP syslog server
                 is down
class            Specify logging event class
<class>          Logging event class name
<destN>          Logging output destination, ie: console, buffer...
list             Specify logging event list
<list>           Logging event list name
host             Send messages to a host
console          Set console logging level
buffered         Copy logging messages to an internal buffer
history          Set SNMP Syslog traps logging level
trap             Set Syslog messages logging level
asdm             Set ASDM logging syslog level
asdm-buffer-size        Set ASDM logging buffer size
message          Disable reporting of this syslog message
device-id        Include the specified device ID in all non-EMBLEM
                 syslog messages
context-name     Sets the device ID to be the name of the current context
rate-limit       Limit the rate at which syslog is generated
unlimited         Keyword to denote rate limit is disabled
<in_if>          The internal interface name, as specified
                 by the 'nameif' command
<l_ip>           The IP address of the host receiving the syslog messages
<emblem>        Log messages in Cisco EMBLEM format (available only for UDP)
<fac>           Eight facilities, 16(LOCAL0) - 23(LOCAL7)
                 The default is 20(LOCAL4), syslog hosts organize messages
                 based on the facility number. The facility may also be set to
                 0 - 15, but is only recommended for system use.

```

```

<level>          Sets the level above which the device suppresses
                  messages to the syslog host
                  0 - System Unusable
                  1 - Take Immediate Action
                  2 - Critical Condition
                  3 - Error Message
                  4 - Warning Message
                  5 - Normal but significant condition
                  6 - Informational
                  7 - Debug Message
<syslog_id>      The ID of the syslog to suppress reporting
<num>            Number at which the syslog(s) is to be rate limited
<interval>       Time interval (in seconds) over which the syslogs should
                  be limited to 'num'. This parameter is optional and if not
                  specified the default is 1 sec
<syslog_level>   The level for which all the syslogs should be rate limited
<queue_size>     The length limit of log queue, 0 - unlimited
<if_name>        interface name
<text>           user-defined device ID
all              This displays all the syslog_ids and their corresponding levels
from-address     Specify from address of mail logging message
recipient-address Specify recipient address of mail logging message.
                 A maximum of 5 recipient addresses can be specified
flash-bufferwrap Save logging buffer to flash when buffer wraps
ftp-bufferwrap   Save logging buffer to external ftp server when
                 buffer wraps
flash-minimum-free      Minimum free flash space logging must maintain
flash-maximum-allocation Maximum flash space logging can consume
<kbytes>               Size in Kilo Bytes
myPIX (config)# logging ?
Usage:  [no] logging on
        [no] logging timestamp
        [no] logging standby
        [no] logging host [<in_if>] <l_ip> [tcp|udp/port#] [format {emblem}]
        [no] logging console <level>
        [no] logging buffered <level>
        [no] logging monitor <level>
        [no] logging history <level>
        [no] logging trap <level>
        [no] logging message <syslog_id> level <level>
        [no] logging facility <fac>
        [no] logging device-id hostname | ipaddress <if_name>
                | string <text>
        logging queue <queue_size>
        show logging [{message [<syslog_id>|all]} | level | disabled]
myPIX (config)# logging on
myPIX (config)# logging host 197.38.34.10
myPIX (config)# logging trap informational
myPIX (config)# logging monitor informational
myPIX (config)# logging console informational
myPIX (config)# logging buffer informational

```

Cisco PIX Challenge 31

Outline

This challenge involves the configuration of PPPoE.

Objectives

The objectives of this challenge are to:

- Define IP addresses of interfaces.
- Define a VPDN group.
- Apply PPPoE.

Example (Ver 6.x)

```
myPIX # config t
myPIX (config)# ip address outside 212.246.206.7 255.255.255.0
myPIX (config)# ip address inside 22.229.82.10 255.255.255.0
myPIX (config)# ip address inf2 165.31.47.6 255.255.255.0
myPIX (config)# vpdn group 7 request dialout pppoe
myPIX (config)# vpdn group 7 localname newmexico
myPIX (config)# vpdn group 7 ppp authen pap
myPIX (config)# vpdn username daniel password dates
myPIX (config)# ip address outside pppoe setroute
```

Example (Ver 7.x)

```
myPIX (config)# int e0
myPIX (config-if)# nameif outside
myPIX (config-if)# ip address 192.168.1.1 255.255.255.0
myPIX (config-if)# no shutdown
myPIX (config-if)# exit
myPIX (config)# int e1
myPIX (config-if)# nameif inside
myPIX (config-if)# ip address 192.168.2.1 255.255.255.0
myPIX (config-if)# no shutdown
myPIX (config-if)# exit
myPIX (config)# int e2
myPIX (config-if)# nameif inf2
myPIX (config-if)# ip address 192.168.3.1 255.255.255.0
myPIX (config-if)# no shutdown
myPIX (config-if)# exit
myPIX (config)# vpdn group 7 request dialout pppoe
myPIX (config)# vpdn group 7 localname newmexico
myPIX (config)# vpdn group 7 ppp authen pap
myPIX (config)# vpdn username daniel password dates
myPIX (config)# ip address outside pppoe setroute
```

Cisco PIX Challenge 32

Outline

This challenge involves the configuration of RIP on interfaces.

Objectives

The objectives of this challenge are to:

- Define RIP listening version on interfaces.

Example

```
myPIX (config)# help rip
```

USAGE:

```
[no] rip <if_name> default|passive [version <1|2>]
      [authentication <text|md5> <key> <key id>]
```

DESCRIPTION:

rip Broadcast default route or passive RIP

SYNTAX:

<if_name> The interface name, as specified by the 'nameif' command, to set the RIP parameters for

default Cause the Firewall to broadcast a default route

passive Enable the Firewall to passively listen to RIP updates

[version <1|2>] Send/receive RIPv1 or RIPv2 packets (no authentication) Default is RIPv1.

[authentication <text|md5> <key> <key id>] Specify authentication.

<text|md5> Authenticate using the specified mode

<key> The shared key to be used for authentication (16 chars. MAX)

<key id> The shared key id that matches the <key> (0 - 255)

see also: route, ping

```
myPIX (config)# rip outside passive version 1
```

```
myPIX (config)# rip inside passive version 1
```

```
myPIX (config)# rip inf2 passive version 1
```

Cisco PIX Challenge 33

Outline

This challenge involves the configuration of multicast protocol.

Objectives

The objectives of this challenge are to:

- Define multicast interface.

- Define multicast parameters.

Example

```
myPIX # config t
myPIX (config)# multicast interface outside
myPIX(config-multicast)# igmp max 39
myPIX(config-multicast)# igmp version 2
myPIX(config-multicast)# igmp query-interval 33
myPIX(config-multicast)# igmp query-max 17
myPIX(config-multicast)# igmp forward interface inside
myPIX(config-multicast)# exit
myPIX (config)# multicast interface inside
myPIX(config-multicast)# exit
myPIX (config)# multicast interface inf2
```

Cisco PIX Challenge 34

Outline

This challenge involves the configuration of IDS signatures.

Objectives

The objectives of this challenge are to:

- Define IP audit rules.
- Remove IDS signatures.

Example

```
myPIX # config t
myPIX (config)# help ip
```

USAGE:

```
ip local pool <poolname> <ip1>[-<ip2>] [mask <netmask>]
ip verify reverse-path interface <if_name>
ip audit {info|attack} action [alarm] [drop] [reset]
ip audit name <audit_name> {info|attack} [action [alarm] [drop] [reset]]
ip audit interface <if_name> <audit_name>
ip audit signature <sig_number> disable
show|clear ip audit count [global] [interface <interface>]
clear configure ip audit [configuration]
```

DESCRIPTION:

```
ip          Define a local address pool
            Configure Unicast RPF on an interface
            Configure the Intrusion Detection System
```

SYNTAX:

```
<poolname>      name of the local address pool
<ip1>-[<ip2>]  address range of the local address pool
<netmask>      network mask of the local address pool
<if_name>      The name designated for the interface by the nameif command
info           IDS informational signatures.
attack         IDS attack signatures.
alarm          When a signature match is detected, report the event
              to syslog servers.
drop           When a signature match is detected, drop the offending
              packet.
reset          When a signature match is detected, drop the offending
              packet and close the connection if it is part of an
              active connection.
<audit_name>   Audit policy name.
<sig_number>   IDS signature number.
```

see also: interface, ip address (interface sub-mode command),
show interface, isakmp

```
myPIX (config)# ip audit info action alarm
myPIX (config)# ip audit attack action alarm
myPIX (config)# ip audit signature 1001 disable
myPIX (config)# ip audit signature 2001 disable
myPIX (config)# ip audit signature 3041 disable
myPIX (config)# ip audit signature 6100 disable
myPIX (config)# ip audit signature 6152 disable
```

Cisco PIX Challenge 35

Outline

This challenge involves the configuration of fragment guards.

Objectives

The objectives of this challenge are to:

- Define fragment size.
- Define fragment timeout.
- Define ARP timeout.
- Define names.

Example

```
myPIX # config t
myPIX (config)# sysopt security fragguard
myPIX (config)# help fragment
```

USAGE:

```
fragment {size|chain|timeout} <limit> [<interface>]
no fragment {size|chain|timeout} <limit> <interface>
show fragment [<interface>]
show running-config [all] fragment [<interface>]
clear configure fragment [<interface>]
clear fragment {queue|statistics} [<interface>]
```

DESCRIPTION:

fragment Configure and display statistics of the IP fragment database

SYNTAX:

```
size     <limit> - maximum number of blocks in database, range <1-30000>
chain    <limit> - maximum number of element in a fragment set, range <1-8200>
timeout <limit> - number of seconds to assemble a fragment set, range <1-30>
queue    - IP reassembly queue
statistics - IP reassembly statistics
<interface> - name of interface
```

```
myPIX (config)# fragment size 900
myPIX (config)# fragment chain 25
myPIX (config)# fragment timeout 5
myPIX (config)# help arp
```

USAGE:

```
[no] arp <if_name> <ip> <mac> [alias]
[no] arp timeout <seconds>
show arp [statistics]
clear arp [statistics]
show running-config [all] arp [timeout]
clear configure arp
```

DESCRIPTION:

arp Change or view the ARP table, add or delete static ARP entries, set or clear the ARP timeout value and clear ARP statistics

SYNTAX:

<if_name> The interface name whose arp table will be changed or viewed

<ip> IP address for an arp table entry

<mac> Hardware 6 byte MAC address specified as XX:XX:XX:XX:XX:XX or XXXX.XXXX.XXXX

alias Proxy ARP for this static entry

<seconds> Duration for which the dynamic ARP entries will remain in the table

statistics Statistics of the arp module

```
myPIX (config)# arp timeout 12718
myPIX (config)# name 210.139.173.7 newhampshire
myPIX (config)# name 155.146.19.10 fife
myPIX (config)# name illinois 212.176.154.6
```

Cisco PIX Challenge 36

Outline

This challenge involves the configuration of MTU for each interface.

Objectives

The objectives of this challenge are to:

- Define the name and security level of each interface.
- Define the IP address and subnet mask of each interface.
- Define the MTU for each interface.

Example

```
myPIX # config t
myPIX (config)# nameif e0 delaware security_0
myPIX (config)# ip address delaware 134.100.122.5 255.255.252.0
myPIX (config)# interface e0 auto
myPIX (config)# help mtu
```

USAGE:

```
mtu <if_name> <bytes> | (300-65535)
```

DESCRIPTION:

```
mtu Specify MTU(Maximum Transmission Unit) for an interface
```

SYNTAX:

```
<if_name> The interface name specified in the nameif command
```

```
<bytes> The number of bytes from 300-65535 for the MTU
```

```
pixfirewall(config)# help multicast-r
```

USAGE:

```
[no] multicast-routing
clear configure multicast-routing
```

DESCRIPTION:

```
multicast-routing
Configure multicast routing
```

```
myPIX (config)# mtu delaware 1268
```

```
myPIX (config)# nameif e1 falkirk security_100
myPIX (config)# ip address falkirk 192.130.14.15 255.255.252.0
myPIX (config)# interface e1 auto
myPIX (config)# mtu falkirk 1500
```

```
myPIX (config)# nameif e2 dmz security_50
myPIX (config)# ip address dmz 121.110.12.6 255.255.252.0
myPIX (config)# interface e2 auto
```

```
myPIX (config)# mtu dmz 1300
```

Example (V 7.x)

```
myPIX # config t
myPIX # int e0
myPIX (config-if)# nameif delaware
myPIX (config-if)# security 0
myPIX (config-if)# ip address 134.100.122.5 255.255.252.0
myPIX (config-if)# no shutdown
myPIX (config-if)# exit
myPIX (config)# help mtu
```

USAGE:

```
mtu <if_name> <bytes> | (300-65535)
```

DESCRIPTION:

mtu Specify MTU(Maximum Transmission Unit) for an interface

SYNTAX:

<if_name> The interface name specified in the nameif command

<bytes> The number of bytes from 300-65535 for the MTU

```
pixfirewall(config)# help multicast-r
```

USAGE:

```
[no] multicast-routing
clear configure multicast-routing
```

DESCRIPTION:

multicast-routing Configure multicast routing

```
myPIX (config)# mtu delaware 1500
```

etc...

Cisco PIX Challenge 37

Outline

This challenge involves the configuration of network and service objects.

Objectives

The objectives of this challenge are to:

- Define the name of the network object-group.
- Define the description of the network object-group.
- Define hosts for the network object-group.

- Define a network for the network object-group.
- Define the name of the service object-group.
- Define the description of the service object-group.
- Define protocols of the TCP protocols.
- Define a range of protocols for the service object-group.

Example

myPIX # config t

myPIX (config)# help object-group

USAGE:

```
[no] object-group protocol | network | icmp-type <obj_grp_id>
[no] object-group service <obj_grp_id> tcp|udp|tcp-udp
show running-config [all] object-group
      [protocol | service | icmp-type | network]
show running-config [all] object-group id <obj_grp_id>
clear configure object-group [protocol | service | icmp-type | network]
```

DESCRIPTION:

object-group Create an object group for use in 'access-list'

SYNTAX:

protocol	Specifies a group of protocols, such as TCP, etc
network	Specifies a group of host or subnet IP addresses
service	Specifies a group of TCP/UDP ports/services
icmp-type	Specifies a group of ICMP types, such as echo
<obj_grp_id>	The identifier for the object group: Must be 1 - 64 characters long, consisting of letters, digits, '-', '_', or '.'.
tcp udp tcp-udp	Specifies the protocol type for a service group; tcp - services provided via TCP only, such as ftp udp - services provided via UDP only, such as snmp tcp-udp - services provided via both TCP and UDP
show	Show object group(s) running config
clear	Remove existing object group(s) config

see also: protocol-object, network-object,
 port-object, icmp-object, group-object

myPIX (config)# object-group ?

configure mode commands/options:

```
icmp-type  Specifies a group of ICMP types, such as echo
network    Specifies a group of host or subnet IP addresses
protocol   Specifies a group of protocols, such as TCP, etc
service    Specifies a group of TCP/UDP ports/services
```

pixfirewall(config)# object-group network ?

configure mode commands/options:

WORD < 65 char Specifies object-group ID (1-64 characters)

```
myPIX (config)# object-group network mississippi
myPIX(config-network)# description sales connection
myPIX(config-network)# net ?
```

network-object-group mode commands/options:

Hostname or A.B.C.D Enter an IPv4 network address
X:X:X:X::X/<0-128> Enter an IPv6 prefix
host Enter this keyword to specify a single host object

```
myPIX(config-network)# net host ?
```

network-object-group mode commands/options:

Hostname or A.B.C.D Enter a host IP address or name
Hostname or X:X:X:X::X Enter a host IPv6 address or name
myPIX(config-network)# network-object host 110.162.152.2 ?
myPIX(config-network)# network-object host 110.162.152.2
myPIX(config-network)# network-object host 192.167.1.1
myPIX(config-network)# network-object host 194.10.1.10
myPIX(config-network)# network-object 110.162.152.0 ?

network-object-group mode commands/options:

A.B.C.D Enter an IPv4 network mask
myPIX(config-network)# network-object 110.162.152.0 255.255.0.0
myPIX(config-network)# exit
myPIX (config)# object-group service ?

configure mode commands/options:

WORD < 65 char Specifies object-group ID (1-64 characters)
myPIX (config)# object-group service texas ?

configure mode commands/options:

tcp Specifies this object-group is for TCP protocol only
tcp-udp Specifies this object-group is for both TCP & UDP
udp Specifies this object-group is for UDP protocol only

```
myPIX (config)# object-group service texas tcp
myPIX(config-network)# description test connection
myPIX (config-service)# port- ?
```

service-object-group mode commands/options:

eq Enter this keyword to specify a port
range Enter this keyword to specify a range of ports
myPIX (config-service)# port-object eq ?

service-object-group mode commands/options:

<0-65535> Enter port number (0 - 65535)
aol
bgp
chargen
cifs
citrix-ica
cmd
ctiqbe
daytime
discard
domain
echo
exec
finger
ftp
ftp-data

```
gopher
h323
hostname
http
https
ident
imap4
irc
kerberos
klogin
kshell
ldap
ldaps
login
lotusnotes
lpd
netbios-ssn
nntp
pcanywhere-data
pim-auto-rp
pop2
pop3
pptp
rsh
rtsp
sip
smtp
sqlnet
ssh
sunrpc
tacacs
talk
telnet
uucp
whois
www
myPIX(config-network)# port-object eq telnet
myPIX(config-network)# port-object eq ftp
myPIX(config-network)# port-object eq www
myPIX(config-network)# port-object range 1411 1422
```

Cisco PIX Challenge 38

Outline

This challenge involves enabling ICMP on interfaces, and the setup of virtual Telnet and virtual HTTP.

Objectives

The objectives of this challenge are to:

- Enable ICMP on the inside interface.
- Enable ICMP on the outside interface.
- Enable ICMP on the DMZ interface.

Example

```
myPIX # config t
myPIX (config)# help icmp
```

USAGE:

```
[no] icmp permit|deny <ip-address> <net-mask> [<icmp-type>] <if-name>
clear configure icmp
show running-config [all] icmp
```

DESCRIPTION:

icmp Configure access for ICMP traffic that terminates at an interface

SYNTAX:

deny Denies access if the conditions are matched.

permit Permits access if the conditions are matched.

<ip-address> IP address

<net-mask> Mask to be applied to <ip-address>

<icmp-type> echo-reply, unreachable, source-quench,
 redirect, alternate-address, echo,
 router-advertisement, router-solicitation, time-exceeded,
 parameter-problem, timestamp-reply, timestamp-request,
 information-request, information-reply, mask-request,
 mask-reply, conversion-error or mobile-redirect

<if-name> Name of the interface

see also: access-list, access-group

```
myPIX(config)# icmp permit 10.0.0.0 255.255.0.0 ?
```

configure mode commands/options:

<0-255> Enter ICMP type number (0 - 255)

alternate-address

conversion-error

echo

echo-reply

information-reply

information-request

mask-reply

mask-request

mobile-redirect

parameter-problem

redirect

router-advertisement

router-solicitation

source-quench

time-exceeded

timestamp-reply

timestamp-request

traceroute

Current available interface(s):

inf Name of interface Ethernet2

inside Name of interface Ethernet1

outside Name of interface Ethernet0

```
myPIX (config)# icmp enable 10.0.0.0 255.255.0.0 inside
myPIX (config)# icmp enable 10.0.0.0 255.255.0.0 outside
myPIX (config)# icmp enable 10.0.0.0 255.255.0.0 inf2
```

```
myPIX (config)# help virtual
```

USAGE:

```
[no] virtual http <ip> [warn]
[no] virtual telnet <ip>
```

DESCRIPTION:

```
virtual          Set address for authentication virtual servers
```

SYNTAX:

```
<ip>             A public or private IP address that is not the address
                  of a real web server on the interface you are accessing.
                  Cisco recommends using an RFC 1918 address.
<warn>          Let users know that the command was redirected.
                  The options is only applicable for text-based browsers
                  where the redirect cannot happen automatically.
```

```
myPIX (config)# virtual telnet 10.1.2.3
```

```
myPIX (config)# vir http ?
```

configure mode commands/options:

```
  Hostname or A.B.C.D  A public or private IP address that is not the address
                        of a real web server on the interface accessed.
                        Cisco recommends using an RFC 1918 address.
```

```
myPIX (config)# virtual http 176.1.2.3
```

Cisco PIX Challenge 39

Outline

This challenge involves denying certain MAC addresses.

Objectives

The objectives of this challenge are to:

- Define a list of denied MAC addresses.

Example

```
myPIX # config t
myPIX (config)# help mac-
```

USAGE:

```
[no] mac-list <id> deny|permit <mac> <macmask>
show mac-list [id]
```

```
clear mac-list [id]
```

DESCRIPTION:

mac-list Add a list of mac addresses using first match search

SYNTAX:

<id> Mac Access list number

deny Traffic matching deny is not included in list

permit Traffic matching permit is included in list

<mac> Source mac address

<macmask> Mask to be applied to <mac>

```
myPIX (config)# mac-list 1 deny 0000.1111.ffff
```

```
myPIX (config)# mac-list 1 deny 0000.2222.ffff
```

```
myPIX (config)# mac-list 1 deny 0000.3333.ffff
```

Cisco PIX Challenge 40

Outline

PIX Version 7.x

The new PIX image supports interface configuration mode. This challenge shows how to set the interface parameters.

Objectives

The objectives of this challenge are to:

- Define the IP address and subnet mask for E0.
- Define the name of the E0 interface.
- Define the description of the E0 interface.
- Define the IP address and subnet mask for E1.
- Define the name of the E1 interface.
- Define the description of the E1 interface.
- Define the IP address and subnet mask for E2.
- Define the name of the E2 interface.
- Define the description of the E2 interface.

Example

```
# config t
myPIX (config)# hostname myPIX
myPIX (config)# int e0
myPIX (config-if)# nameif fred
```

```
myPIX (config-if)# ip address 192.168.1.1 255.255.255.0
myPIX (config-if)# no shutdown
myPIX (config-if)# description my port
myPIX (config-if)# exit
myPIX (config)# int e1
myPIX (config-if)# nameif test
myPIX (config-if)# ip address 192.168.2.1 255.255.255.0
myPIX (config-if)# no shutdown
myPIX (config-if)# description your port
myPIX (config-if)# exit
myPIX (config)# int e2
myPIX (config-if)# nameif market
myPIX (config-if)# ip address 192.168.3.1 255.255.255.0
myPIX (config-if)# no shutdown
myPIX (config-if)# description any port
myPIX (config-if)# exit
```

Cisco PIX Challenge 41

Outline

PIX Version 7.x only

The new PIX image supports a modular policy framework.

Objectives

The objectives of this challenge are to:

- **Define class maps.** Remember the class map defines the traffic which is interesting. In this case the class-map relates to defining TCP ports and an access-list.
- **Apply the class maps.**
- **Define a policy map and apply it to an interface.**

Example

```
myPIX# config t
myPIX(config)# access-list 100 permit tcp host 165.246.68.4 host 200.194.252.5 eq
echo
myPIX(config)# class-map ?
myPIX(config)# class-map delaware
myPIX(config-cmap)# ?
myPIX(config-cmap)# description ?
myPIX(config-cmap)# description testing
myPIX(config-cmap)# match ?
myPIX(config-cmap)# match port ?
myPIX(config-cmap)# match port tcp ?
myPIX(config-cmap)# match port tcp eq ?
```

```

myPIX(config-cmap)# match port tcp eq 80
myPIX(config-cmap)# match port tcp eq 21
myPIX(config-cmap)# match port tcp eq 23
myPIX(config-cmap)# match port udp eq 23
myPIX(config-cmap)# match access-list ?
myPIX(config-cmap)# match access-list 100
myPIX(config-cmap)# match dscp ?
myPIX(config-cmap)# exit
myPIX(config)# class-map VOICE
myPIX(config-cmap)# exit
myPIX(config)# class-map EXECTEST
myPIX(config-cmap)# exit
myPIX(config)# policy-map ?
myPIX(config)# policy-map NEW
myPIX(config-pmap)# ?
myPIX(config-pmap)# description ?
myPIX(config-pmap)# description test
myPIX(config-pmap)# class ?
myPIX(config-pmap)# class delaware
myPIX(config-pmap-c)# ?
myPIX(config-pmap-c)# inspect ?
myPIX(config-pmap-c)# ips ?
myPIX(config-pmap-c)# police ?
myPIX(config-pmap-c)# police 1000 ?
myPIX(config-pmap-c)# police 1000 500
myPIX(config-pmap-c)# set ?
myPIX(config-pmap-c)# set conn ?
myPIX(config-pmap-c)# exit
myPIX(config-pmap)# exit
myPIX(config)# service-policy ?
myPIX(config)# service-policy NEW ?
myPIX(config)# service-policy NEW interface ?
myPIX(config)# service-policy NEW interface outside

```

Example

An example, which has not yet been implemented in the challenge, is:

```

pix1(config)# class-map TEST
pix1(config-cmap)# match port tcp eq 25
pix1(config-cmap)# match tunnel-group S2S
pix1(config-cmap)# exit
pix1(config)# class-map VOICE
pix1(config-cmap)# match dscp ef
pix1(config-cmap)# exit
pix1(config)# class-map EXECTEST
pix1(config-cmap)# match access-list 112
pix1(config-cmap)# exit
pix1(config)# policy-map NEW
pix1(config-cmap)# class TEST

```

Cisco PIX Challenge 42

Outline

PIX Version 7.x only

The new PIX image supports multiple contexts.

Objectives

The objectives of this challenge are to:

- Define context mode.
- Save context mode to a configuration file.
- Define that interfaces on the same security level can communicate with each other.

Example (Ver 7.x)

```
pix1(config)# mode multiple
pix1(config)# context test1
pix1(config-ctx)# allocate-interface e0
pix1(config-ctx)# allocate-interface e1
pix1(config-ctx)# config-url flash:/test1.cfg
pix1(config-ctx)# exit
pix1(config)# context test2
pix1(config-ctx)# allocate-interface e2
pix1(config-ctx)# config-url flash:/test2.cfg
pix1(config-ctx)# exit
pix1(config)# same-security-traffic permit inter-interface
```

Cisco PIX Challenge 43

Outline

This is a test for some basic PIX configuration parameters ... no help is given.

Cisco PIX Challenge 44

Outline

This is a test for some basic PIX configuration parameters ... no help is given.

Cisco PIX Challenge 45

Outline

This is a test for some basic PIX configuration parameters ... no help is given.

Cisco PIX Challenge 46

Outline

This challenge uses DHCP allocation.

Objectives

The objectives of this challenge are to:

- Define E0 details.
- Define E1 details.

Example (Ver 6.x)

```
> enable
# config t
(config)# hostname myPIX
myPIX (config)# domain-name strathclyde.int
myPIX (config)# nameif e0 moon security9
myPIX (config)# ip address moon dhcp
myPIX (config)# interface e0 auto

myPIX (config)# nameif e1 mars security100
myPIX (config)# ip address mars dhcp
myPIX (config)# interface e1 auto

myPIX (config)# nameif e2 pluto security100
myPIX (config)# ip address pluto dhcp
myPIX (config)# interface e1 auto
```

Example (Ver 7.x)

```
> enable
# config t
(config)# hostname myPIX
myPIX (config)# domain-name strathclyde.int
myPIX (config)# int e0
myPIX (config-if)# nameif moon
myPIX (config-if)# help ip
```

USAGE:

```
[no] ip address <ip_address> [<mask>] [standby <sby_ip_addr>]
[no] ip address dhcp [setroute] [retry <4-16>]
show ip address [<interface> | <if_name>]
clear ip
```

DESCRIPTION:

ip Set the ip address and mask for an interface

SYNTAX:

```
<ip_address>       Device's network interface address
<mask>             Netmask of ip_address
<sby_ip_addr>       Device failover peer's network interface address
<4-16>             Number of retries performed by dhcp client, default is 4
<interface>:       Interface hardware name as used by 'interface' command.
                    Composed of <type> <port>[/<subif_number>] or
                    <type> <slot>/<port>[/<subif_number>]
<if_name>:          Interface name assigned by 'nameif' command
```

see also: nameif, security-level

```
myPIX (config-if)# ip address dhcp
myPIX (config-if)# no shutdown
myPIX (config-if)# int e1
myPIX (config-if)# nameif mars
myPIX (config-if)# ip address dhcp
myPIX (config-if)# no shutdown
myPIX (config-if)# int e2
myPIX (config-if)# nameif pluto
```

```
myPIX (config-if)# ip address dhcp
myPIX (config-if)# no shutdown
```

Cisco PIX Challenge 47

Outline

This challenge uses a static mapping with non-default names of the interfaces.

Objectives

The objectives of this challenge are to:

- Define E0 details.
- Define E1 details.
- Define a static mapping (with non-default names).

Example (Ver 7.x)

```
> enable
myPIX # config t
myPIX (config)# hostname amsterdam
amsterdam (config)# domain-name shetland.gov
amsterdam (config)# int e0
amsterdam (config-if)# nameif california
amsterdam (config-if)# ip address 144.128.32.1 255.255.255.0
amsterdam (config-if)# no shut
amsterdam (config-if)# security-level 1
amsterdam (config-if)# exit
amsterdam (config)# int e1
amsterdam (config-if)# nameif vermont
amsterdam (config-if)# ip address 81.213.27.8 255.255.255.0
amsterdam (config-if)# no shut
amsterdam (config-if)# security-level 12
amsterdam (config-if)# exit
amsterdam (config)# int e2
amsterdam (config-if)# nameif northdakota
amsterdam (config-if)# ip address 145.7.193.1 255.255.0.0
amsterdam (config-if)# no shut
amsterdam (config-if)# security-level 10
amsterdam (config-if)# exit
amsterdam (config)# static (vermont,california) 144.128.32.4 81.213.27.18
amsterdam (config)# static (vermont,california) 144.128.32.5 81.213.27.19
amsterdam (config)# static (vermont,california) 144.128.32.6 81.213.27.20
```

Cisco PIX Challenge 48

Outline

This challenge applies an ACL to the E0 interface.

Objectives

The objectives of this challenge are to:

- Define E0 details.
- Define an access-list
- Apply the access-list to E0.

Example (Ver 7.x)

```
> enable
myPIX # config t
myPIX (config)# hostname amsterdam
amsterdam (config)# domain-name shetland.gov
amsterdam (config)# int e0
amsterdam (config-if)# nameif california
amsterdam (config-if)# ip address 144.128.32.1 255.255.255.0
amsterdam (config-if)# no shut
amsterdam (config-if)# security-level 1
amsterdam (config-if)# exit
amsterdam (config)# access-list 101 permit tcp host 132.178.215.10 host
197.161.244.7 eq ftp
amsterdam (config)# access-list 101 deny tcp 120.205.173.0 255.255.0.0
154.213.112.0 255.255.0.0 eq ftp
amsterdam (config)# access-list 101 permit tcp any any
amsterdam (config)# help access-group
```

USAGE:

```
[no] access-group <access-list> <in|out> interface <if_name> [per-user-override]
```

DESCRIPTION:

```
access-group      Bind an extended access-list to an interface to filter inbound traffic
```

SYNTAX:

```
<access-list>      Extended access list number
<in|out>           Inbound or Outbund access list
<if_name>         Name of the interface
per-user-override  Allow AAA downloaded per-user ACL to override
```

see also: access-list, object-group

```
amsterdam (config)# access-group 101 in interface california
```

Cisco PIX Challenge 49

Outline

This challenge manually generates a public and private RSA key.

Objectives

The objectives of this challenge are to:

- Define E0 details.
- Generate RSA keys.
- Display public key.

Example (Ver 7.x)

```
> enable
myPIX # config t
myPIX (config)# hostname amsterdam
amsterdam (config)# domain-name shetland.gov
amsterdam (config)# int e0
amsterdam (config-if)# nameif california
amsterdam (config-if)# ip address 144.128.32.1 255.255.255.0
amsterdam (config-if)# no shut
amsterdam (config-if)# exit
amsterdam (config)# crypto key generate rsa
amsterdam (config)# show crypto key mypubkey rsa
amsterdam (config)# sh crypto key mypub rsa
Key pair was generated at: 13:28:00 UTC Jun 25 2006
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00eff641
 77632bdc 93f8872a 1631c8ca 24f5e102 826acdb7 346dfaf2 64770144 0dc8625e
 20f8c42f 9650eb7f leddd836 090a6b94 2ec34e2c cbca8ebe a3f4490a 3daee2aa
 40ea6964 eaecc909 46d6lace ffd6aa62 250c21d6 4356610e 7d2e6d61 86591d35
 513d3100 7a25f98c 31bb660d 4e47587b ace9bee9 4e6ea81c 78b6e7cd 67020301 0001
amsterdam (config)# crypto ca ?

configure mode commands/options:
 authenticate Get the CA certificate
 certificate Actions on certificates
  crl Actions on certificate revocation lists
  enroll Request a certificate from a CA
  export Export a trustpoint configuration with all associated keys and
 certificates in PKCS12 format.
  import Import certificate or pkcs-12 data
  trustpoint Define a CA trustpoint
amsterdam (config)# crypto ca trustpoint ?

configure mode commands/options:
 WORD < 129 char Trustpoint Name
amsterdam (config)# crypto ca trustpoint jupiter
amsterdam (config-ca-trustpoint)# ?
crypto ca trustpoint configuration commands:
```

accept-subordinates	Accept subordinate CA certificates
crl	CRL options
default	Return all enrollment parameters to their default values
email	Email Address
enrollment	Enrollment parameters
exit	Exit from certificate authority trustpoint entry mode
fqdn	include fully-qualified domain name
help	Help for crypto ca trustpoint configuration commands
id-cert-issuer	Accept ID certificates
ip-address	include ip address
keypair	Specify the key pair whose public key is to be certified
no	Negate a command or set its defaults
password	revocation password
serial-number	include serial number
subject-name	Subject Name
support-user-cert-validation	Validate remote user certificates using the configuration from this trust point provided that this trust point is authenticated to the CA that issued the remote certificate

amsterdam(config-ca-trustpoint)# enrollment url http://yourcert

Cisco PIX Challenge 50

Outline

This challenge defines parameters within username mode.

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 names.
- Define username and password.
- Define username attributes.

Example (Ver 7.x)

```
> enable
myPIX # config t
myPIX (config)# hostname amsterdam
amsterdam (config)# domain-name shetland.gov
amsterdam (config)# int e0
amsterdam (config-if)# nameif california
amsterdam (config-if)# exit
amsterdam (config)# int e1
amsterdam (config-if)# nameif texas
amsterdam (config-if)# exit
```

```

amsterdam (config)# int e2
amsterdam (config-if)# nameif newyork
amsterdam (config-if)# exit
amsterdam (config)# username anne password test
amsterdam (config)# username anne attrib
amsterdam (config-username)# vpn-tunnel-protocol ipsec
amsterdam (config-username)# vpn-simultaneous ?

username mode commands/options:
  <0-2147483647> Maximum number of simultaneous logins allowed
amsterdam (config-username)# vpn-simultaneous 2

```

Cisco PIX Challenge 51

Outline

This challenge involves investigating the initial commands and on showing help.

Objectives

The objectives of this challenge are to:

- Investigate initial mode.
- Showing help on commands.

Example

```

> ?

clear      Reset functions
enable     Turn on privileged commands
exit       Exit from the EXEC
help       Interactive help for commands
login      Log in as a particular user
logout     Exit from the EXEC
ping       Send echo messages
quit       Exit from the EXEC
show       Show running system information

> clear ?

igmp       Clear multicast membership related information
> enable ?

<0-15>     Enter optional privilege level (0-15)
<cr>
> exit ?

<cr>
> help ?

enable     Turn on privileged commands
exit       Exit the current command mode
login      Log in as a particular user

```

```

logout      Exit from current user profile to unprivileged mode
perfmon     Change or view performance monitoring options
ping        Test connectivity from specified interface to an IP address
quit        Exit the current command mode
> login ?

<cr>
> logout ?

<cr>
> ping ?

Hostname or A.B.C.D      Ping destination IPv4 address or hostname
Hostname or X:X:X:X::X   Ping destination IPv6 address or hostname
<cr>
> quit ?

<cr>

> show ?

checksum    Display configuration information cryptochecksum
curpriv     Display current privilege level
flash:      Display information about flash: file system
history     Display the session command history
version     Display system software version

> show checksum
Cryptochecksum: a0b3ec1d 272c2e58 183687ff b14a65a8
> show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
> show flash

Directory of flash:/

5      -rw-  5103672      14:05:27 Jun 06 2006  image.bin
9      -rw-  5919340      14:10:49 Jun 06 2006  asdm-501.bin

16128000 bytes total (5099008 bytes free)

> show history

?
clear ?
enable ?
exit ?
help ?
login ?
logout ?
ping ?
?
quit ?
show ?
show checksum
show curpriv
show flash
show history

> show version

Cisco PIX Security Appliance Software Version 7.0(1)

```

Device Manager Version 5.0(1)

Compiled on Thu 31-Mar-05 14:37 by builders
System image file is 'flash:/image.bin'
Config file at boot was 'startup-config'

pixfirewall up 17 mins 34 secs

Hardware: PIX-515E, 96 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xffff00000, 16MB
BIOS Flash AM29F400B @ 0xffffd8000, 32KB

0: Ext: Ethernet0 : media index 0: irq 10
1: Ext: Ethernet1 : media index 1: irq 11
2: Ext: Ethernet2 : media index 2: irq 11

Licensed features for this platform:

Maximum Physical Interfaces : 3
Maximum VLANs : 10
Inside Hosts : Unlimited
Failover : Disabled
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Cut-through Proxy : Enabled
--More----- press any key ---
Guards : Enabled
URL Filtering : Enabled
Security Contexts : 0
GTP/GPRS : Disabled
VPN Peers : Unlimited

This platform has a Restricted (R) license.

Serial Number: 807290112
Running Activation Key: 0x3f43a2b7 0xf5909081 0x5fd21d2b 0x16cbcc59
Configuration has not been modified since last system restart.

> enable
help bl

USAGE:

```
show blocks [address <hex-address>|all|assigned|free|old|
            pool <block-size> [dump|header|packet]]
[no] blocks queue history enable [buffer-size]
[clear|show] blocks queue history [detail]
```

DESCRIPTION:

blocks System packet buffer (block) utilization and diagnostic tools. By default, the maximum, lowest, and current available counts are displayed for each block size.

SYNTAX:

address Shows a block corresponding to <hex-address>
all Shows all blocks
assigned Shows assigned (not free) blocks
free Shows free blocks
old Shows old (retained for more than 1 minute) blocks
pool Shows blocks of a specific <block-size>
header Shows only the block header
packet Shows the block header and the packet data

dump Shows the block header and entire block contents

queue history Diagnose packet buffer exhaustion
enable A small amount of memory is always allocated to this diagnostic. This keyword allocates additional memory for more extensive diagnostics when needed. By default, the amount of memory is determined by the system. Use 'no' to return this memory back to the system.
buffer-size Number of memory bytes to allocate for diagnostics
detail Display a portion of packet buffer contents

help bo

USAGE:

```
[no] boot system | config <url>  
clear configure boot [system | config]
```

DESCRIPTION:

boot Configure the system image and startup-config file used to boot the system

SYNTAX:

system <url> Configure a url pointing to the system image file that will be run on reload. Multiple system urls can be configured, the first one found will be loaded.
config <url> Configure a url pointing to the startup-config that will be used to configure the system on reload. Only one url can be set, multiple invocations of this command will overwrite the previous setting.

When you use these commands, you affect only the running configuration. You must save the environment variable setting to your startup configuration to place the information under ROM monitor control and to have the environment variable function as expected. Use the write mem or copy running-config startup-config commands to save the environment variable from your running configuration to your startup configuration and place them under ROM monitor control.

sh process

PC	SP	STATE	Runtime	SBASE	Stack	Process
Lwe	00105689	00ffb9e0	00db4a10	0	00ff9f08	8072/8192 block_diag
Mrd	001dba60	011c63d0	00db4a78	593450	011c2478	16044/16384 Dispatch Unit
Mwe	00112cf5	0120bec0	00db49c8	0	01209f48	7772/8192 Reload Control Thread
Mwe	00116edf	0120e410	00db5ff8	0	0120c4c8	8008/8192 aaa
Lwe	001db106	012168c0	00db5e540	0	01214948	7308/8192 dbgtrace
Msi	003cda1f	0121ab00	00db49c8	0	01218b88	7840/8192 557mcfix
Mrd	003cd97a	0121cc20	00db4a78	1270490	0121aca8	7660/8192 557poll
Msi	003cd9cb	0121ed40	00db49c8	0	0121cdc8	7776/8192 557statspoll
Mwe	00b6e13d	0122f5e0	00db49c8	0	0122d658	7788/8192 Chunk Manager
Msi	006f6c3e	01238cb8	00db49c8	0	01236d50	7684/8192 PIX Garbage Collector
Lsi	00a4d60d	0123adf8	00db49c8	0	01238e70	7428/8192 route_process
Mwe	006e73bd	012481b8	00d3a280	0	01246240	8056/8192 IP Address Assign
Mwe	008ce47d	0124dd80	00d441f0	0	0124be08	8056/8192 QoS Support Module
Mwe	0074ff85	0124fed8	00d3af64	0	0124df60	8056/8192 Client Update Task
Lwe	00b89581	012527b0	00db49c8	7780	01250838	7740/8192 Checkheaps
Mwe	00908601	01258b00	00db49c8	0	01256b98	7276/8192 Session Manager
Mwe	009eba89	012636b8	016dda58	0	0125f7d0	15636/16384 uauth
Mwe	009e7911	01267910	00d5ad60	0	012659c8	7660/8192 SMTP
Mwe	009d8925	01269a40	00d5a730	0	01267ae8	7276/8192 Logger

```

Mwe 009d9d31 0126bb80 00db49c8      0 01269c08 7292/8192 Thread Logger
Mwe 00ac127b 01278230 00d85390      0 012762c8 6956/8192 vpnlb_thread
Msi 00487913 0131e2a8 00db49c8      0 0131c330 7324/8192 arp_timer
Mwe 004907b1 013231d8 00dcca70      0 01321270 7964/8192 arp_forward_thread
Mwe 009edfa9 0133e988 00d5b770      0 0133ca20 7824/8192 tcp_fast
Mwe 009ededd 013409a0 00d5b770      0 0133ea48 7808/8192 tcp_slow
Mwe 009f893b 01350d90 00d5b8f0      0 0134ee28 8040/8192 udp_timer
Mrd 005e39c6 0122b330 00db4a78      813010 01229418 7788/8192 snp_timer_thread
Mwe 00166f31 01225ea8 00db49c8      0 01223f20 7976/8192 CTCP Timer process
Mwe 0017c064 01631c38 01228490      0 0162fcd0 7700/8192 IPsec message handler
Msi 00189b71 01633c60 00db49c8      0 01631cf8 7720/8192 CTM message handler
Mwe 00a78685 01635c78 00db49c8      0 01633d20 7928/8192 L2TP data daemon
Mwe 00a78475 01637cb0 00db49c8      0 01635d48 7944/8192 L2TP mgmt daemon
Mwe 00a637df 0166fdb8 00d80128      0 0166be50 16184/16384 ppp_timer_thread
Msi 00ac1b7a 01671dc0 00db49c8      0 0166fe78 7792/8192 vpnlb_timer_thread
Mwe 00691e95 016864c8 00db49c8      0 01682560 16048/16384 IP Background
Mwe 001d48dd 016cf518 00d11ef0      10 016af5c0 126852/131072 tmatch compile
thread
Mwe 0081bbd9 0170df38 00db49c8      0 01709fb0 15980/16384 Crypto PKI RECV
Mwe 008212d4 01710038 00db49c8      0 0170e0d0 7772/8192 Crypto CA
Lsi 0070b0a9 01212690 00db49c8      0 01210708 7856/8192 uauth_urlb clean
Lsi 006f1020 01771498 00db49c8      0 0176f520 7840/8192 perfmon
Mwe 0041eb69 01773808 00db49c8      0 01771890 7960/8192 IKE Timekeeper
Mwe 004117a9 01778ba8 00d2c9c0      0 01774f50 15404/16384 IKE Daemon
Mwe 009add91 0177bb80 00d5a0f8      0 01779c08 8056/8192 RADIUS Proxy Event
Daemon
Mwe 009838b4 0177db30 017b5b68      0 0177bd28 7260/8192 RADIUS Proxy Listener
Mwe 009af891 0177fdd0 00db49c8      0 0177de48 7976/8192 RADIUS Proxy Time
Keeper
M* 001e41e7 0009feec 00db4a78      1730 017a49d8 4844/16384 ci/console
Csi 007260e9 017aaa60 00db49c8      0 017a8af8 7340/8192 update_cpu_usage
Msi 007268bd 017b0c48 00db49c8      0 017aed70 7364/8192 NIC status poll
Mwe 00a9ead8 017bd5e0 00d8457c      0 017bb688 8024/8192 vpnfo_thread_msg
Msi 00aaa63b 017bf608 00db49c8      0 017bd6b0 7808/8192 vpnfo_thread_timer
Mwe 00aa70f7 017c1630 00d84688      0 017bf6d8 8024/8192 vpnfo_thread_sync
Msi 00aa9f28 017c3760 00db49c8      0 017c17f8 7824/8192 vpnfo_thread_unsent

```

sh startup

```

: Saved
: Written by enable_15 at 15:48:15.415 UTC Thu Dec 28 2006

```

```

PIX Version 7.0(1)
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted

```

```

passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
pager lines 2
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
!
service-policy global_policy global
Cryptochecksum:a0b3ec1d272c2e58183687ffb14a65a8

# a?
# b?
# c?

```

Cisco PIX Challenge 52

Outline

This challenge involves investigating the initial commands and on showing help.

Objectives

The objectives of this challenge are to:

- Investigate initial mode.

- Showing help on commands.

Example

```
pixfirewall# help ?
```

```

activation-key  Modify activation-key
arp             Show ARP cache or clear ARP cache or statistics
blocks         System packet buffer utilization
boot           Configure the system image and startup-config file to boot
               the system
capture        Capture inbound and outbound packets on one or more
               interfaces
cd             Change the working directory
configure      Configure from terminal
copy           Copy files from and to, disk or flash or TFTP server or HTTP
               server
crashinfo      Configure, test and view crash information collection
debug          Debug packets or ICMP tracings through the system
delete         Delete a file
dir            Display the directory contents
disable        Exit from privileged mode
downgrade      Downgrade the file system and reboot
erase          Erase and format filesystem
exit           Exit the current command mode
format         Format filesystem
fsck           File system check
kill           Terminate a telnet session
logging        Configure, show, clear logging command options or operational
               data
logout         Exit from current user profile to unprivileged mode
memory         System memory utilization
mkdir          Create new directory
more           Display a file's contents
ospf           Display or clear OSPF information
perfmon        Change or view performance monitoring options
ping           Test connectivity from specified interface to an IP address
pwd            Display the current directory
quit           Exit the current command mode
reload         Halt and reload system
rename         Rename a file
resource       Display or clear resource usage
rmdir          Remove existing directory
shun           Manages the filtering of packets from undesired hosts
terminal       Turn on/off syslogging or set pagers for the terminal
traffic        Counters for traffic statistics
undebg         Undebug packets or ICMP tracings through the system
who            Show active administration sessions
write          Write config to net, flash, or terminal, or erase flash

```

```
pixfirewall# help act
```

```
USAGE:
```

```

activation-key <activation-key-four-or-five-tuple>
show activation-key

```

```
DESCRIPTION:
```

```
activation-key Modify activation-key.
```

```
SYNTAX:
```

<activation-key-four-or-five-tuple> a four or five element hexadecimal string.
pixfirewall# help arp
Unrecognized command: arp

At the end of show <command>, use the pipe character '|' followed by:
begin|include|exclude|grep [-v] <regular_exp>, to filter show output.

activation-key	Modify activation-key.
boot	Configure the system image and startup-config file used to boot the system
blocks	System packet buffer (block) utilization and diagnostic tools. By default, the maximum, lowest, and current available counts are displayed for each block size.
capture	Capture inbound and outbound packets on one or more interfaces
configure	Configure from terminal
copy	Copy files from and to, disk or flash or TFTP server or HTTP server
Crashinfo	Read, write and configure crash write to flash. Force a crash.
debug	Enable debugging functions
disable	Exit from privileged mode
firewall	Switch to router/transparent mode.
kill	Terminate a telnet session
logout	Exit from current user profile to unprivileged mode
logging	Configure, show or clear logging command options or operational data
memory	System memory utilization and diagnostic tools
mode	Toggle between single and multiple security context mode
more	Display a file's contents
ospf	Show or clear OSPF information
perfmon	Display perfmon stats or change options
ping	Test connectivity from specified interface to an IP address
priority-queue	Configure a priority queue object
quit	Disable, end configuration or logout
reload	Halt and reload system
resource	Display system resource allocation and usage
session	Open a command session to another module
hw-module	Perform operations on an installed hardware module
shun	Manages the filtering of packets from undesired hosts
terminal	Set and reset terminal monitor or pagination
downgrade	Downgrade the system image. Unit will reboot with execution of this command.
traffic	Counters for traffic statistics
who	Show active administration sessions on the device
write	Write config to net, flash, or terminal, or erase flash. Write without argument defaults to write memory
cd	Change the working directory
delete	Delete a file
dir	Display the directory contents
erase	Erase and format filesystem
format	Format filesystem
more	Display a file's contents
pwd	Display the current directory
mkdir	Create new directory
rename	Rename a file
rmdir	Remove existing directory
fsck	Perform file system check

pixfirewall# help bl

USAGE:

```
show blocks [address <hex-address>|all|assigned|free|old|
pool <block-size> [dump|header|packet]]
```

```
[no] blocks queue history enable [buffer-size]
[clear|show] blocks queue history [detail]
```

DESCRIPTION:

blocks System packet buffer (block) utilization and diagnostic tools. By default, the maximum, lowest, and current available counts are displayed for each block size.

SYNTAX:

```
address    Shows a block corresponding to <hex-address>
all        Shows all blocks
assigned   Shows assigned (not free) blocks
free       Shows free blocks
old        Shows old (retained for more than 1 minute) blocks
pool       Shows blocks of a specific <block-size>
header     Shows only the block header
packet     Shows the block header and the packet data
dump       Shows the block header and entire block contents

queue history    Diagnose packet buffer exhaustion
  enable        A small amount of memory is always allocated to this diagnostic. This keyword allocates additional memory for more extensive diagnostics when needed. By default, the amount of memory is determined by the system. Use 'no' to return this memory back to the system.
  buffer-size   Number of memory bytes to allocate for diagnostics
  detail        Display a portion of packet buffer contents
```

pixfirewall# help bo

USAGE:

```
[no] boot system | config <url>
clear configure boot [system | config]
```

DESCRIPTION:

boot Configure the system image and startup-config file used to boot the system

SYNTAX:

```
system <url>     Configure a url pointing to the system image file that will be run on reload. Multiple system urls can be configured, the first one found will be loaded.
config <url>     Configure a url pointing to the startup-config that will be used to configure the system on reload. Only one url can be set, multiple invocations of this command will overwrite the previous setting.
```

When you use these commands, you affect only the running configuration. You must save the environment variable setting to your startup configuration to place the information under ROM monitor control and to have the environment variable function as expected. Use the write mem or copy running-config startup-config commands to save the environment variable from your running configuration to your startup configuration and place them under ROM monitor control.

pixfirewall# help cap

USAGE:

```
capture <capture-name> [type raw-data] [type asp-drop <drop-code>]
[type isakmp]
[access-list <acl-name>] [buffer <buf-size>]
[ethernet-type <type>] [interface <if-name>]
[packet-length <bytes>]
[circular-buffer]
clear capture <capture-name>
no capture <capture-name> [type raw-data][type asp-drop <drop-code>]
[type isakmp]
[access-list <acl_name>] [circular-buffer] [interface <if-name>]
show capture [[context-name/]<capture-name> [access-list <acl-name>]
[count <number>] [detail] [dump][decode][packet-number <number>]]
```

DESCRIPTION:

capture Capture inbound and outbound packets on one or more interfaces

SYNTAX:

```
<capture-name> - name of capture
<context-name> - name of the context
<acl-name> - capture IP packets that match access-list <acl-name>
<buf-size> - size of capture buffer in bytes, range <84-33554432>
<type> - capture Ethernet packets of <type>, valid types are
ip, arp, rarp, ipx, ip6, ppoed, pppoes and <0-65535>
<if-name> - the physical interface to listen
<bytes> - maximum length to save from each packet
circular-buffer - overwrite buffer from beginning when full
count - display <number> of packets in capture
detail - display more information for each packet
dump - display the hex dump for each packet
```

see also: copy

pixfirewall# help cd

USAGE:

```
cd [{disk0:|disk1:|flash:}][<path>]
```

DESCRIPTION:

cd Change the working directory

SYNTAX:

```
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<path> Directory name
```

pixfirewall# help conf

USAGE:

```
configure terminal
```

DESCRIPTION:

configure Configure from terminal

SYNTAX:

see also: the configure options in configure mode

pixfirewall# help copy

USAGE:

```
copy [/<options>] capture:[<context-name>/]<buffer name> <URL>
copy [/<options>] [<local>:]<file spec> [<local>:]<file spec>
copy [/<options>] [<local>:]<file spec> <URL>
copy [/<options>] <URL>                [<local>:]<file spec>
```

DESCRIPTION:

copy Copy files from and to local and remote file systems

SYNTAX:

```
<options>      noconfirm - Do not prompt for confirmation
                pcap      - Use raw dump of the capture buffer
<local>       Local file system prefix, default assumed if omitted
<file spec>   Name of the file or one of startup-config, running-config
startup-config Configuration file stored in flash
running-config Configuration file stored in memory
<URL>        <scheme>://[<user>:<password>@]<location>[:<port>]/<pathname>[
                ;<options>]
<scheme>      Remote file system type - TFTP, FTP,
                HTTP (not available as target), HTTPS (not available as target)
<user>       User name for logging into server
<location>   The IP address (or name) of the server. Place IPv6 address
                within square brackets
<password>   Password for logging into server
<pathname>   The path and filename
<port>       Port of the remote server
<options>    One or more options of the form <option>=<value>, delimited by
                ';' character. Valid options are:
                type=<xx>
                int=<interface>
type          Valid only if FTP is used, specifies FTP mode and transfer type
<xx>        Used with type to specify the FTP type. This can be any of
                the four combinations ap, an, ip and in, where
                a- Ascii transmission mode,
                i- Image (binary) transmission mode,
                p- Passive mode,
                n- Normal or non passive mode
int          Valid only if TFTP is used, specifies the interface used to
                perform the remote access
<interface> Name of the interface, specified using the nameif interface
                subcommand
```

pixfirewall# help cr

USAGE:

```
[show|clear] crashinfo
crashinfo test
crashinfo force [page-fault|watchdog]
[no] crashinfo save disable
show crashinfo save
```

DESCRIPTION:

Crashinfo Read, write and configure crash write to flash. Force a crash.

pixfirewall# help deb

USAGE:

```
no debug all | undebug all
[no] debug aaa [<1-255>]
[no] debug appfw chunk|event|eventverb|regex [<1-255>]
[no] debug arp
[no] debug arp-inspection [<1-255>]
[no] debug cmgr [<1-255>]
[no] debug context [<1-255>]
[no] debug cplane [<1-255>]
[no] debug crypto isakmp [timers [<1-255>]] |
    [capture <cap_name> [options]] |
    [<1-255>]
[no] debug ctiqbe [<1-255>]
[no] debug ctm [<1-255>]
[no] debug dhcpc detail|error|packet [<1-255>]
[no] debug dhcpcd packet|event [<1-255>]
[no] debug dhcprelay error|packet|event [<1-255>]
[no] debug disk file|filesystem|file-verbose [<1-255>]
[no] debug dns [resolver|all [<1-255>]]
[no] debug entity [<1-255>]
[no] debug fixup tcp|udp|onat [<1-255>]
[no] debug fover cable|fail|fmsg|ifc|open|rx|rxdump|rxip|
    switch|sync|tx|txdump|txip|verify|off
[no] debug fsm [<1-255>]
[no] debug ftp client [<1-255>]
[no] debug generic [<1-255>]
[no] debug h323 h225|h245|ras [asn|event]
[no] debug http [<1-255>]
[no] debug http-map
[no] debug icmp trace [<1-255>]
[no] debug igmp [group [A.B.C.D]|interface [<if_name>]]
[no] debug ils [<1-255>]
[no] debug imagemgr [<1-255>]
[no] debug ipsec-over-tcp [<1-255>]
[no] debug ipv6 icmp|interface|nd|packet|routing
[no] debug iua-proxy [<1-255>]
[no] debug kerberos [<1-255>]
[no] debug ldap [<1-255>]
[no] debug mac-address-table [<1-255>]
[no] debug menu aaa|ipsec-over-tcp|ctm|vpnlb|ike|ipaddrutl|
    qos|pki|vpnfo [LINE]
[no] debug mfib db|init|mrib|pak|ps|signal [<group_addr>]
[no] debug mgcp messages|parser|sessions
[no] debug module-boot [<1-255>]
[no] debug mrib client|io|route[<host_name>]|table
[no] debug np drops[breaks acl|all|bad-crypto|bad-ipsec-natt|
    bad-ipsec-prot|bad-ipsec-udp|bad-tcp-cksum|bad-tcp-flags|
    clear|ctm-error|dst-l2-lookup-fail|flow-expired|fo-standby|
    ids-fail-close|ids-request|ifc-classify|inspect-dns|
    inspect-icmp|intercept-unexpected|interface-down|
    invalid-app-length|invalid-encap|invalid-ethertype|
    invalid-ip-addr|invalid-ip-length|invalid-ip-option|
    invalid-tcp|invalid-tcp-hlength|invalid-udp-length|
    ip-fragment|ipsec-clearpkt-notun|ipsec-ipv6|ipsec-need-sa|
    ipsec-spoof|ipsec-tun-down|ipsecudp-keepalive|l2-acl|
    l2-same-lan-port|large-buf-alloc-fail|lu-invalid-pkt|
    natt-keepalive|no-adjacency|no-mcast-entry|no-mcast-intrf|
    no-punt-cb|no-route|np-sp-invalid-spi|queue-removed|
    rate-exceeded|rpf-violated|security-failed|send-ctm-error|
    show|tcp-acked|tcp-bad-option-len|tcp-bad-option-list|
    tcp-bad-sack-allow|tcp-bad-winscale|tcp-buffer-full|
    tcp-conn-limit|tcp-data-past-fin|tcp-discarded-ooo|
```

```

tcp-dual-open|tcp-mss-exceeded|tcp-mss-no-syn|
tcp-not-syn|tcp-paws-fail|tcp-reserved-set|
tcp-rst-syn-in-win|tcp-syn-data|tcp-synack-data|
tcp-tsopt-notallowed|tcp-winscale-no-syn|
unable-to-add-flow|unable-to-create-flow|
unimplemented|unsupport-ipv6-hdr|
unsupported-ip-version break]
[no] debug ntdomain [<1-255>]
[no] debug ntp adjust|authentication|events|loopfilter|
packets|params|select|sync|validity
[no] debug ospf [adj|database-timer|events|flood|lsa-generation|
packet|retransmission|tree|spf[external|inter|intra]]
[no] debug parser cache [<1-255>]
[no] debug asdm history <1-255>
[no] debug pim [df-election [interface <ifname>] [rp <addr>] |
group <group_addr> | interface <ifname> | neighbor]
[no] debug [pix process|uauth|cls|pkt2pc|acl[<1-4294967295>]]
[no] debug pppoe error|packet|event [<1-255>]
[no] debug pptp [<1-255>]
[no] debug radius [all|decode|session|user user_name]
[no] debug rip [<1-255>]
[no] debug rtsp [<1-255>]
[no] debug sdi [<1-255>]
[no] debug sequence [<1-255>]
[no] debug session-command [<1-255>]
[no] debug sip [<1-255>]
[no] debug skinny [<1-255>]
[no] debug smtp [<1-255>]
[no] debug sqlnet [<1-255>]
[no] debug ssh [<1-255>]
[no] debug ssl cipher|device [<1-255>]
[no] debug sunrpc [<1-255>]
[no] debug tacacs [session|user user_name]
[no] debug tcp-map
[no] debug timestamps [<1-255>]
[no] debug vpn-sessiondb [<1-255>]
[no] debug xdmcp [<1-255>]

```

```

<if_name>      Interface name.
<host_name>    Hostname or A.B.C.D IP group address.
<user_name>    User name.

```

DESCRIPTION:

```
debug          Enable debugging functions
```

```
pixfirewall# help del
```

USAGE:

```
delete [/recursive] [/noconfirm] [{disk0:|disk1:|flash:}] <path>
```

DESCRIPTION:

```
delete        Delete a file
```

SYNTAX:

```

/recursive          Recursive delete
/noconfirm          No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem

```

<path> File to be deleted

pixfirewall# help dir

USAGE:

```
dir [/all] [/recursive]
    [{all-fileSYSTEMS | [(disk0:|disk1:|flash:)]<path>}]
```

DESCRIPTION:

dir Display the directory contents

SYNTAX:

```
/all List all files
/recursive List files recursively
all-fileSYSTEMS List files on all fileSYSTEMS
{disk0:|disk1:|flash:} Optional parameter that specifies the fileSYSTEM
<path> Directory or file name
pixfirewall# help dis
```

USAGE:

```
disable
```

DESCRIPTION:

disable Exit from privileged mode

pixfirewall# help do

USAGE:

```
downgrade [/noconfirm] <image_url>
    [activation-key (flash|file|<actkey>)]
    [config <config_url>]
```

DESCRIPTION:

downgrade Downgrade the system image. Unit will reboot with execution of this command.

SYNTAX:

```
noconfirm Do not prompt for confirmation
<image_url> File name or URL of the image to be downgraded with
activation-key Specify the 4-tuple activation key to be used after downgrade
flash Use the 4-tuple activation key last used in this unit
file Use the activation key saved with the image file (<image_url>)
during upgrade
<actkey> Specify the 4-tuple activation key in the command line
config Specify the startup configuration file to be used after
downgrade
<config_url> File name or URL of the configuration
```

Notes: The default for activation-key is to use the 4-tuple key in flash.
The default for config is to use the file downgrade.cfg in flash.

pixfirewall# help er

USAGE:

```

        erase {disk0:|disk1:|flash:}

DESCRIPTION:
erase          Erase and format filesystem

SYNTAX:
{disk0:|disk1:|flash:}  Filesystem to be formatted
pixfirewall# help ex

USAGE:
        quit|exit

DESCRIPTION:
quit          Disable, end configuration or logout
pixfirewall# help f?

        format  fsck
pixfirewall# help fo

USAGE:
        format {disk0:|disk1:|flash:}

DESCRIPTION:
format        Format filesystem

SYNTAX:
{disk0:|disk1:|flash:}  Filesystem to be formatted
pixfirewall# help fs

USAGE:
        fsck [/nocrc] flash:

DESCRIPTION:
fsck          Perform file system check

SYNTAX:
nocrc        Skip the CRC checks during FSCK
pixfirewall# help kill

USAGE:
        kill <telnet_id>

DESCRIPTION:
kill          Terminate a telnet session

SYNTAX:

```

<telnet_id> Session ID as displayed by the who command

see also: who
pixfirewall# help logging

USAGE:

```
logging savelog [<logfile>]
clear logging [asdm | buffer]
show logging [{message [<syslog_id>|all]} | asdm | queue | setting]
show running-config [all] logging [level | disabled | rate-limit]
```

DESCRIPTION:

logging Configure, show or clear logging command options or operational data

SYNTAX:

```
savelog            save logging buffer to flash
<logfile>        optional log file name on flash
disable            disabled syslog message
level             syslog message with modified level
message            display which messages are suppressed
queue             show syslog queue
rate-limit        show rate-limit info (FWSM only)
see also:         logging buffered <level>, logging queue <queue_size>
```

pixfirewall# help logout

USAGE:

```
logout
```

DESCRIPTION:

logout Exit from current user profile to unprivileged mode
pixfirewall# help mem

USAGE:

```
show memory [detail]

                  [no] memory delayed-free-poisoner enable
                          memory delayed-free-poisoner validate
[clear|show] memory delayed-free-poisoner
```

DESCRIPTION:

memory System memory utilization and diagnostic tools

SYNTAX:

detail Indicate the amount of total, free, used, reserved, least free, most used, fragmented and allocated memory statistics. By default, only the total, free, and used memory is emitted.

```
delayed-free-poisoner    diagnose illegal memory use
enable                    enable the tool
validate                  ensure the cached memory is still valid
```

The delayed-free-poisoner is a tool for finding illegal reuse

of system memory. This tool, which is not enabled by default, helps find memory corruptions by a combination of steps including: setting memory returned to the system by the apps to poisoned values, deferring reuse of such poisoned memory for as long as possible by storing this memory within the tool, and finally ensuring the poisoned values, while they are stored in the tool, have not been unexpectedly modified.

The use of the delayed-free-poisoner has significant impact upon the observed system memory use, processor cycles, internal memory bus bandwidth, and if issues are found, uptime. The tool's primary audience is development or testing environments having suitable expectation and tolerance for the types of behaviors the previous concerns imply; use in live or production networks is not recommended.

```
pixfirewall# help mk
```

USAGE:

```
mkdir /noconfirm [{disk0:|disk1:|flash:}] <path>
```

DESCRIPTION:

```
mkdir          Create new directory
```

SYNTAX:

```
/noconfirm          No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<path>              Directory name
```

```
pixfirewall# help more
```

USAGE:

```
more [/ascii] || [/binary] || [/ebcdic] [filesystem] <path>
```

DESCRIPTION:

```
more          Display a file's contents
```

SYNTAX:

```
/ascii          Display binary files in ascii
/binary         Force display to hex/text format
/ebcdic        Force display to ebcdic format
[filesystem]   Optional parameter that can be disk0: or disk1: or
               flash: or ftp: or http: or https: or system: or tftp:
<path>        File to display
```

```
pixfirewall# help os
```

USAGE:

```
show ospf [<pid> [<ip_addr>]]...
...interface [<interface>]
...neighbor [detail] [<interface>] [<nbr-router-id>]
...[summary-address]
...database [router | network | summary |
            asbr-summary | external | nssa-external]
            [<ip_addr>] [internal]
            [self-originate | adv-router <ip_addr>]
```

```
...database database-summary
...request-list <nbr-router-id> <interface>
...flood-list <interface>
...retransmission-list <nbr-router-id> <interface>
...border-routers
...virtual-links
clear ospf [<pid>]
...process
...counters [neighbor [<nbr-interface>] [<nbr-id>]]
```

DESCRIPTION:

ospf Show or clear OSPF information

SYNTAX:

<pid> OSPF process ID
<nbr-router-id> Neighbor router address
<interface> Interface name as specified by nameif

pixfirewall# help per

USAGE:

```
perfmon interval <seconds>
perfmon quiet | verbose
perfmon settings
```

DESCRIPTION:

perfmon Display perfmon stats or change options

SYNTAX:

show perfmon Shows current and running average of a set of rates, xlate/sec, conn/sec, websense query/sec, url/sec, etc.

<seconds> Sets the interval used to calculate the current rate (the default is 120 seconds).

verbose Rather than have to type "show perfmon" over and over, you can use perfmon verbose to automatically print the stats to the console every interval seconds.

quiet Turn verbose mode OFF.

settings Show current interval and verbose/quiet settings.

pixfirewall# help ping

USAGE:

```
ping [if_name] <host> [data <pattern>] [repeat <count>] [size <bytes>]
[timeout <seconds>] [validate]
```

DESCRIPTION:

ping Test connectivity from specified interface to an IP address

SYNTAX:

[if_name] The interface name, as specified by the 'nameif' command,

by which <host> is accessible. If not supplied, then <host> is resolved to an IP address and then the routing table is consulted to determine the destination interface.

<host> IPv4 address, IPv6 address or name of host to ping.

<pattern> 16 bit data pattern in hex.

<count> Repeat count.

<bytes> Datagram size in bytes.

<seconds> Timeout in seconds.

validate Validate reply data.

pixfirewall# help pwd

USAGE:

pwd

DESCRIPTION:

pwd Display the current directory

pixfirewall# help rel

USAGE:

reload [quick] [noconfirm] [save-config] [max-hold-time [hhh:]mm]
[[in [hhh:]mm | at hh:mm [{Mon dd | dd Mon}]]] [reason <text>]
reload cancel

DESCRIPTION:

reload Halt and reload system

SYNTAX:

quick Reload without properly shutting down each subsystem
noconfirm Reload immediately without asking for confirmation
save-config Save configuration before reload
max-hold-time Maximum hold time for orderly reload
at Reload at a specific time/date
in Reload after a time interval
reason Reason for reload

pixfirewall# help rena

USAGE:

rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:|
flash:}] <destination path>

DESCRIPTION:

rename Rename a file

SYNTAX:

/noconfirm No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path> Source file path

```
pixfirewall# help res
```

USAGE:

```
show resource usage
    [resource {<resource_name>|all}]
    [counter <counter_name> [<count_threshold>]]
clear resource usage
    [resource {<resource_name>|all}]
show resource types
```

DESCRIPTION:

resource Display/clear system resource usage

SYNTAX:

Where:

```
<resource_name>        See 'show resource types' for resource names
<counter_name>         One of: current, peak, all
<count_threshold>      Only view counters at or above this threshold
```

Default command: 'show resource usage resource all counter all 1'

```
pixfirewall# help rm
```

USAGE:

```
rmdir /noconfirm [{disk0:|disk1:|flash:}] <path>
```

DESCRIPTION:

rmdir Remove existing directory

SYNTAX:

```
/noconfirm                    No confirmation
{disk0:|disk1:|flash:}        Optional parameter that specifies the filesystem
<path>                        Directory name
```

```
pixfirewall# help sh
```

USAGE:

```
shun <src_ip> [<dst_ip> <sport> <dport> [<prot>]] [vlan <vlan_number>]
no shun <src_ip> [vlan <vlan_number>]
show shun [<src_ip>|statistics]
clear shun [statistics]
```

DESCRIPTION:

shun Manages the filtering of packets from undesired hosts

SYNTAX:

```
src_ip    the IP src address of a mischievous host.
dst_ip    the IP dest. address used for connection lookup and termination.
sport     the source port for connection lookup and termination.
dport     the dest. port for connection lookup and termination.
prot      the protocol for connection lookup and termination.
vlan_number    the vlan on which the mischievous host resides.
```

```
pixfirewall# help ter
```

USAGE:

```
terminal monitor
terminal no monitor
[no] terminal pager [lines <lines>]
```

DESCRIPTION:

```
terminal          Set and reset terminal monitor or pagination
```

SYNTAX:

```
lines             number of lines per page
pixfirewall# help tra
```

USAGE:

```
show traffic
clear traffic
```

DESCRIPTION:

```
traffic          Counters for traffic statistics
pixfirewall# help u?
```

```
undebg
pixfirewall# help unde
```

USAGE:

```
no debug all | undebg all
[no] debug aaa [<1-255>]
[no] debug appfw chunk|event|eventverb|regex [<1-255>]
[no] debug arp
[no] debug arp-inspection [<1-255>]
[no] debug cmgr [<1-255>]
[no] debug context [<1-255>]
[no] debug cplane [<1-255>]
[no] debug crypto isakmp [timers [<1-255>]] |
    [capture <cap_name> [options]] |
    [<1-255>]
[no] debug ctiqbe [<1-255>]
[no] debug ctm [<1-255>]
[no] debug dhcpc detail|error|packet [<1-255>]
[no] debug dhcpd packet|event [<1-255>]
[no] debug dhcprelay error|packet|event [<1-255>]
[no] debug disk file|filesystem|file-verbose [<1-255>]
[no] debug dns [resolver|all [<1-255>]]
[no] debug entity [<1-255>]
[no] debug fixup tcp|udp|onat [<1-255>]
[no] debug fover cable|fail|fmsg|ifc|open|rx|rxcmp|rxip|
    switch|sync|tx|txcmp|txip|verify|off
[no] debug fsm [<1-255>]
[no] debug ftp client [<1-255>]
[no] debug generic [<1-255>]
[no] debug h323 h225|h245|ras [asn|event]
[no] debug http [<1-255>]
[no] debug http-map
[no] debug icmp trace [<1-255>]
[no] debug igmp [group [A.B.C.D]|interface [<if_name>]]
[no] debug ils [<1-255>]
[no] debug imagemgr [<1-255>]
```

```

[no] debug ipsec-over-tcp [<1-255>]
[no] debug ipv6 icmp|interface|nd|packet|routing
[no] debug iua-proxy [<1-255>]
[no] debug kerberos [<1-255>]
[no] debug ldap [<1-255>]
[no] debug mac-address-table [<1-255>]
[no] debug menu aaa|ipsec-over-tcp|ctm|vpnlb|ike|ipaddrutl|
    qos|pki|vpnfo [LINE]
[no] debug mfib db|init|mrib|pak|ps|signal [<group_addr>]
[no] debug mgcp messages|parser|sessions
[no] debug module-boot [<1-255>]
[no] debug mrib client|io|route[<host_name>]|table
[no] debug np drops[breaks acl|all|bad-crypto|bad-ipsec-natt|
    bad-ipsec-prot|bad-ipsec-udp|bad-tcp-cksum|bad-tcp-flags|
    clear|ctm-error|dst-l2-lookup-fail|flow-expired|fo-standby|
    ids-fail-close|ids-request|ifc-classify|inspect-dns|
    inspect-icmp|intercept-unexpected|interface-down|
    invalid-app-length|invalid-encap|invalid-ethertype|
    invalid-ip-addr|invalid-ip-length|invalid-ip-option|
    invalid-tcp|invalid-tcp-hlength|invalid-udp-length|
    ip-fragment|ipsec-clearpkt-notun|ipsec-ipv6|ipsec-need-sa|
    ipsec-spoof|ipsec-tun-down|ipsecudp-keepalive|l2-acl|
    l2-same-lan-port|large-buf-alloc-fail|lu-invalid-pkt|
    natt-keepalive|no-adjacency|no-mcast-entry|no-mcast-intrf|
    no-punt-cb|no-route|np-sp-invalid-spi|queue-removed|
    rate-exceeded|rpf-violated|security-failed|send-ctm-error|
    show|tcp-acked|tcp-bad-option-len|tcp-bad-option-list|
    tcp-bad-sack-allow|tcp-bad-winscale|tcp-buffer-full|
    tcp-conn-limit|tcp-data-past-fin|tcp-discarded-ooo|
    tcp-dual-open|tcp-mss-exceeded|tcp-mss-no-syn|
    tcp-not-syn|tcp-paws-fail|tcp-reserved-set|
    tcp-rst-syn-in-win|tcp-syn-data|tcp-synack-data|
    tcp-tsopt-notallowed|tcp-winscale-no-syn|
    unable-to-add-flow|unable-to-create-flow|
    unimplemented|unsupport-ipv6-hdr|
    unsupported-ip-version break]
[no] debug ntdomain [<1-255>]
[no] debug ntp adjust|authentication|events|loopfilter|
    packets|params|select|sync|validity
[no] debug ospf [adj|database-timer|events|flood|lsa-generation|
    packet|retransmission|tree|spf[external|inter|intra]]
[no] debug parser cache [<1-255>]
[no] debug asdm history <1-255>
[no] debug pim [df-election [interface <ifname>] [rp <addr>] |
    group <group_addr> | interface <ifname> | neighbor]
[no] debug [pix process|uauth|cls|pkt2pc|acl[<1-4294967295>]]
[no] debug pppoe error|packet|event [<1-255>]
[no] debug pptp [<1-255>]
[no] debug radius [all|decode|session|user user_name]
[no] debug rip [<1-255>]
[no] debug rtsp [<1-255>]
[no] debug sdi [<1-255>]
[no] debug sequence [<1-255>]
[no] debug session-command [<1-255>]
[no] debug sip [<1-255>]
[no] debug skinny [<1-255>]
[no] debug smtp [<1-255>]
[no] debug sqlnet [<1-255>]
[no] debug ssh [<1-255>]
[no] debug ssl cipher|device [<1-255>]
[no] debug sunrpc [<1-255>]
[no] debug tacacs [session|user user_name]
[no] debug tcp-map

```

```
[no] debug timestamps [<1-255>]
[no] debug vpn-sessiondb [<1-255>]
[no] debug xdmcp [<1-255>]
```

<if_name> Interface name.
<host_name> Hostname or A.B.C.D IP group address.
<user_name> User name.

DESCRIPTION:

debug Enable debugging functions

pixfirewall# help who

USAGE:

who [ip]

DESCRIPTION:

who Show active administration sessions on the device

pixfirewall# help wr

USAGE:

write erase|terminal|standby
write net [<tftp_ip>]:<filename>
write [memory]

DESCRIPTION:

write Write config to net, flash, or terminal, or erase flash.
Write without argument defaults to write memory

SYNTAX:

erase Clears the flash memory configuration

terminal Display the current active configuration, not necessarily
the saved configuration

mem Save the active configuration to the flash, so that it will
be the active configuration after a reload

standby Save the active configuration on the active unit to the
flash on the standby unit

net Save the active configuration to the tftp server

see also: configure

<tftp_ip> IP address of the tftp server. Place IPv6 address
within square brackets.

<filename> Name of the configuration file.

Cisco PIX Challenge 53

Outline

This challenge involves configuring ARP entries.

Objectives

The objectives of this challenge are to:

- Define a static ARP entry

Example

```
pixfirewall# sh nameif
Interface          Name          Security
Ethernet0          outside       0
Ethernet1          inside        100
Ethernet2          inf2          50
pixfirewall# config t
pixfirewall(config)# help arp
```

USAGE:

```
[no] arp <if_name> <ip> <mac> [alias]
[no] arp timeout <seconds>
show arp [statistics]
clear arp [statistics]
show running-config [all] arp [timeout]
clear configure arp
```

DESCRIPTION:

```
arp          Change or view the ARP table, add or delete static ARP entries,
              set or clear the ARP timeout value and clear ARP statistics
```

SYNTAX:

```
<if_name>    The interface name whose arp table will be changed or viewed
<ip>        IP address for an arp table entry
<mac>       Hardware 6 byte MAC address specified as XX:XX:XX:XX:XX:XX
              or XXXX.XXXX.XXXX
alias        Proxy ARP for this static entry
<seconds>   Duration for which the dynamic ARP entries will remain
              in the table
statistics   Statistics of the arp module
```

```
pixfirewall(config)# arp outside ?
```

configure mode commands/options:

Hostname or A.B.C.D IP address for an ARP table entry

```
pixfirewall(config)# arp outside 10.0.0.1 ?
```

configure mode commands/options:

H.H.H Hardware MAC address

```
pixfirewall(config)# arp outside 10.0.0.1 1.2.3 ?
```

```
configure mode commands/options:
  alias Don't expire this ARP entry after timeout
  <cr>
pixfirewall(config)# arp outside 10.0.0.1 1.2.3
pixfirewall(config)# arp inside 11.0.0.1 f.2.4
pixfirewall(config)# arp inf2 13.0.0.1 1.2.5
```

Cisco PIX Challenge 54

Outline

This challenge involves configuring FTP and MGCP inspection.

Objectives

The objectives of this challenge are to:

- Define FTP and MGCP inspection.

Example

```
pixfirewall(config)# ftp-map ftpm
pixfirewall(config-ftp-map)# ?
```

```
Ftp-map configuration commands:
  mask-syst-reply Mask reply to syst command
  no              Negate a command or set its defaults
  request-command FTP request command inspection
```

```
pixfirewall(config-ftp-map)# mask- ?
```

```
ftp-map mode commands/options:
  <cr>
```

```
pixfirewall(config-ftp-map)# re ?
```

```
ftp-map mode commands/options:
  deny Specify FTP request commands to block
```

```
pixfirewall(config-ftp-map)# re den ?
```

```
ftp-map mode commands/options:
  appe Append to a file
  cdup Change to parent of current directory
  dele Delete a file at server site
  get  FTP client command for the retr command - retrieve a file
  help Help information from server
  mkd  Create a directory
  put  FTP client command for the stor command - store a file
  rmd  Remove a directory
  rnfr Rename from
  rnto Rename to
  site Specify server specific command
  stou Store a file with a unique name
```

```
pixfirewall(config-ftp-map)# exit
pixfirewall(config)# mgcp-map mmap
pixfirewall(config-mgcp-map)# ?
```

```
mgcp-map configuration commands:
  call-agent      Add a Call-Agent
  command-queue  Configure Command Queue
  gateway         Add a Gateway
  help           Help for mgcp-map configuration commands
  no             Negate or set default values of a command
```

```
pixfirewall(config-mgcp-map)# call ?
```

```
mgcp-map mode commands/options:
  A.B.C.D  IP address
```

```
pixfirewall(config-mgcp-map)# gat ?
```

```
mgcp-map mode commands/options:
  A.B.C.D  IP address
```

Cisco PIX Challenge 55

Outline

This challenge involves configuring IPv6.

Objectives

The objectives of this challenge are to:

- Define IPv6 on E0.
- Define IPv6 neighbor discovery to learn about neighboring devices.
- Define a static IPv6 mapping (if the automated discovery does not work).
- Define the default route.

Commands

```
pixfirewall(config)# int e0
pixfirewall(config-if)# ipv6 address autoconfig
pixfirewall(config-if)# ipv6 enable
pixfirewall(config-if)# exit
pixfirewall(config)# int e1
pixfirewall(config-if)# ipv6 address 2001:400:3:1::1/64
pixfirewall(config-if)# ipv6 enable
pixfirewall(config-if)# ipv6 nd ns-interval 100
pixfirewall(config-if)# ipv6 nd ra-interval 100
pixfirewall(config-if)# ipv6 nd reachable-time 100
pixfirewall(config-if)# ipv6 nd prefix 0800::/64
pixfirewall(config-if)# exit
pixfirewall(config)# ipv6 route outside ::/0 2001:400:3:1::1
pixfirewall(config)# ipv6 neighbor fe80:0000 inside 0000.1111.22222
pixfirewall# sh ipv interface
pixfirewall# sh ipv6 route
```

Example

```
pixfirewall(config)# int e0
```

```
pixfirewall(config-if)# ipv6 ?
```

```
interface mode commands/options:
```

```
IPv6 interface subcommands:
```

```
  address  Configure IPv6 address on interface
  enable   Enable IPv6 on interface
  nd       IPv6 interface Neighbor Discovery subcommands
```

```
configure mode commands/options:
```

```
  access-list  Configure access policy for IPv6 traffic through the system
  icmp        Configure access rules for ICMPv6 traffic terminating at an
              interface
  neighbor     Neighbor
  route       Configure IPv6 routes
```

```
pixfirewall(config-if)# ipv6 address ?
```

```
interface mode commands/options:
```

```
  Hostname or X:X:X:X::X  IPv6 link-local address
  X:X:X:X::X/<0-128>      IPv6 prefix
  autoconfig             Obtain address using autoconfiguration
```

```
configure mode commands/options:
```

```
  WORD  Access list identifier
```

```
pixfirewall(config-if)# ipv6 address autoconfig
```

```
pixfirewall(config-if)# ipv6 enable
```

```
pixfirewall(config-if)# exit
```

```
pixfirewall(config)# int e1
```

```
pixfirewall(config-if)# ipv6 address 2001:400:3:1::1/64
```

```
pixfirewall(config-if)# ipv6 enable
```

```
pixfirewall(config-if)# ipv6 nd ?
```

```
interface mode commands/options:
```

```
  dad          Duplicate Address Detection
  ns-interval  Set advertised NS retransmission interval
  prefix       Configure IPv6 Routing Prefix Advertisement
  ra-interval  Set IPv6 Router Advertisement Interval
  ra-lifetime  Set IPv6 Router Advertisement Lifetime
  reachable-time Set advertised reachability time
  suppress-ra  Suppress IPv6 Router Advertisements
```

```
pixfirewall(config-if)# ipv6 nd ns-interval ?
```

```
interface mode commands/options:
```

```
<1000-3600000> Retransmission interval in milliseconds
```

```
pixfirewall(config-if)# ipv6 nd ns-interval 100
```

```
pixfirewall(config-if)# ipv6 nd p ?
```

```
interface mode commands/options:
```

```
  X:X:X:X::X/<0-128>  IPv6 prefix x:x::y/<z>
  default            Specify prefix default parameters
```

```
pixfirewall(config-if)# ipv6 nd prefix 0800::/64
```

```
pixfirewall(config-if)# ipv6 nd ra-interval ?
```

```
interface mode commands/options:
```

```
<3-1800> RA Interval (sec)
msec     Interval in milliseconds
```

```
pixfirewall(config-if)# ipv6 nd ra-interval 100
```

```
pixfirewall(config-if)# ipv6 nd reachable-time ?
```

```
interface mode commands/options:  
  <0-3600000> Reachability time in milliseconds
```

```
pixfirewall(config-if)# ipv6 nd reachable-time 100
```

```
pixfirewall(config-if)# exit
```

```
pixfirewall(config)# ipv ?
```

```
configure mode commands/options:  
  access-list  Configure access policy for IPv6 traffic through the system  
  icmp        Configure access rules for ICMPv6 traffic terminating at an  
              interface  
  neighbor    Neighbor  
  route       Configure IPv6 routes
```

```
pixfirewall(config)# ipv route ?
```

```
configure mode commands/options:  
Current available interface(s):  
  Inf2      Name of interface Ethernet2  
  Inside    Name of interface Ethernet1  
  Outside   Name of interface Ethernet0
```

```
pixfirewall(config)# ipv r outside ?
```

```
configure mode commands/options:  
  X:X:X:X::X/<0-128> IPv6 prefix
```

```
pixfirewall(config)# ipv r outside ::/0 ?
```

```
configure mode commands/options:  
  Hostname or X:X:X:X::X IPv6 name or address
```

```
pixfirewall(config)# ipv6 route outside ::/0 2001:400:3:1::1
```

To define a static entry, if discovery does not work:

```
pixfirewall(config)# ipv6 ?
```

```
configure mode commands/options:  
  access-list  Configure access policy for IPv6 traffic through the system  
  icmp        Configure access rules for ICMPv6 traffic terminating at an  
              interface  
  neighbor    Neighbor  
  route       Configure IPv6 routes
```

```
pixfirewall(config)# ipv6 neighbor ?
```

```
configure mode commands/options:  
  X:X:X:X::X IPv6 address
```

```
pixfirewall(config)# ipv6 neighbor fe80:0000 ?
```

```
configure mode commands/options:  
Current available interface(s):  
  Inf2Name of interface Ethernet2
```

Outside Name of interface Ethernet1
Inside Name of interface Ethernet0

```
pixfirewall(config)# ipv6 neighbor fe80:0000 inside 0000.1111.22222  
pixfirewall(config)# exit
```

```
pixfirewall# sh ipv6 ?
```

```
access-list Show hit counters for access policies  
icmp Show ICMPv6 access rules configured on all interfaces  
interface IPv6 interface status and configuration  
neighbor Show IPv6 neighbor cache entries  
route Show IPv6 routes  
routers Show local IPv6 routers  
traffic IPv6 traffic statistics
```

```
pixfirewall# sh ipv interface
```

```
outside is administratively down, line protocol is down  
IPv6 is enabled, link-local address is fe80::20d:65ff:fe85:77d9 [TENTATIVE]  
No global unicast address is configured  
Joined group address(es):  
ff02::1  
ff02::2  
ff02::1:ff85:77d9  
ICMP error messages limited to one every 100 milliseconds  
ICMP redirects are enabled  
ND DAD is enabled, number of DAD attempts: 1  
ND reachable time is 30000 milliseconds  
ND advertised reachable time is 0 milliseconds  
ND advertised retransmit interval is 1000 milliseconds  
ND router advertisements are sent every 200 seconds  
ND router advertisements live for 1800 seconds  
Hosts use stateless autoconfig for addresses.  
inside is administratively down, line protocol is down  
IPv6 is enabled, link-local address is fe80::20d:65ff:fe85:77da [TENTATIVE]  
Global unicast address(es):  
2001:400:3:1::1, subnet is 2001:400:3:1::/64 [TENTATIVE]  
Joined group address(es):  
ff02::1  
ff02::2  
ff02::1:ff85:77da  
ICMP error messages limited to one every 100 milliseconds  
ICMP redirects are enabled  
ND DAD is enabled, number of DAD attempts: 1  
ND reachable time is 30000 milliseconds  
ND advertised reachable time is 0 milliseconds  
ND advertised retransmit interval is 1000 milliseconds  
ND router advertisements are sent every 200 seconds  
ND router advertisements live for 1800 seconds  
Hosts use stateless autoconfig for addresses.
```

```
pixfirewall# sh ipv6 route
```

```
IPv6 Routing Table - 2 entries  
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP  
U - Per-user Static route  
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea  
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2  
L fe80::/10 [0/0]  
via ::, outside
```

```
    via ::, inside
    via ::, inf2
L   ff00::/8 [0/0]
    via ::, outside
    via ::, inside
    via ::, inf2
```

Cisco PIX Challenge 56

Outline

This challenge involves configuring OSPF routing

Objectives

The objectives of this challenge are to:

- Define OSPF.

Example

```
pixfirewall(config)# router ?
```

```
configure mode commands/options:
  ospf  Open Shortest Path First (OSPF)
```

```
pixfirewall(config)# router ospf ?
```

```
pixfirewall(config)# router os ?
```

```
configure mode commands/options:
  <1-65535> Process ID
```

```
pixfirewall(config)# router ospf 111
```

```
pixfirewall(config-router)# ?
```

```
Router configuration commands:
```

```
area          OSPF area parameters
compatible    OSPF compatibility list
default-information  Control distribution of default information
distance      Define an administrative distance
exit          Exit from router configuration mode
help          Interactive help for router subcommands
ignore        Do not complain about specific event
log-adj-changes  Log changes in adjacency state
neighbor      Specify a neighbor router
network       Add/remove interfaces to/from OSPF routing process
no            Negate a command
redistribute  Redistribute information from another routing process
router-id     router-id for this OSPF process
summary-address  Configure IP address summaries
timers        Adjust routing timers
```

```
pixfirewall(config-router)# net ?
```

```
router mode commands/options:
  A.B.C.D Network address
```

```
pixfirewall(config-router)# net 10.0.0.0 ?
```

```

router mode commands/options:
  A.B.C.D Mask for network address
pixfirewall(config-router)# net 10.0.0.0 0.0.0.255 ?

router mode commands/options:
  area Set the OSPF area ID
pixfirewall(config-router)# net 10.0.0.0 0.0.0.255 area ?

router mode commands/options:
  <0-4294967295> OSPF area ID as a decimal value
  A.B.C.D OSPF area ID in IP address format
pixfirewall(config-router)# network 10.0.0.0 0.0.0.255 area 1
pixfirewall(config-router)# area ?

router mode commands/options:
  <0-4294967295> OSPF area ID as a decimal value
  A.B.C.D OSPF area ID in IP address format

pixfirewall(config-router)# area 1 ?

router mode commands/options:
  authentication Enable authentication
  default-cost Set the summary default-cost of a NSSA/stub area
  filter-list Filter networks between OSPF areas
  nssa Specify a NSSA area
  range Summarize routes matching address/mask (border routers only)
  stub Specify a stub area
  virtual-link Define a virtual link and its parameters
  <cr>
pixfirewall(config-router)# area 1 authentication
pixfirewall(config-router)# exit
pixfirewall(config)# int e0
pixfirewall(config-if)# ospf ?

interface mode commands/options:
  authentication Enable authentication
  authentication-key Authentication password (key)
  cost Interface cost
  database-filter Filter OSPF LSA during synchronization and flooding
  dead-interval Interval after which a neighbor is declared dead
  hello-interval Time between HELLO packets
  message-digest-key Message digest authentication password (key)
  mtu-ignore Ignores the MTU in DBD packets
  network Network type
  priority Router priority
  retransmit-interval Time between retransmitting lost link state
  advertisements
  transmit-delay Link state transmit delay
pixfirewall(config-if)# ospf authentication ?

interface mode commands/options:
  message-digest Use message-digest authentication
  null Use no authentication
  <cr>
pixfirewall(config-if)# ospf authentication message-digest
pixfirewall(config-if)# exit
pixfirewall(config)# exit
pixfirewall# sh ospf

Routing Process "ospf 1" with ID 10.0.0.0 and Domain ID 0.0.0.255
Supports only single TOS(TOS0) routes
Does not support opaque LSA

```

```

SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x      0
Number of opaque AS LSA 0. Checksum Sum 0x      0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area 1
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 1 times
    Area ranges are
    Number of LSA 1. Checksum Sum 0x ff12
    Number of opaque link LSA 0. Checksum Sum 0x      0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

```

Cisco PIX Challenge 57

Outline

This challenge involves diverting all the traffic to the AIP SSM in promiscuous mode. If the AIP SSM cards then fails, all the traffic will be blocked.

Objectives

The objectives of this challenge are to:

- Define the class-map.
- Define the policy-map.
- Apply the policy-map.

Example

```

pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# class-map ctest

```

```

pixfirewall(config-cmap)# ?

```

MPF class-map configuration commands:

```

description Specify class-map description
exit         Exit from MPF class-map configuration mode
help        Help for MPF class-map configuration commands
match       Configure classification criteria
no          Negate or set default values of a command
rename      Rename this class-map

```

```

pixfirewall(config-cmap)# match ?

```

mpf-class-map mode commands/options:

```

access-list Match an Access List
any         Match any packet
default-inspection-traffic Match default inspection traffic:
            ctiqbe----tcp--2748      dns-----udp--53

```

```

ftp-----tcp--21          gtp-----udp--2123,3386
h323-h225-tcp--1720      h323-ras--udp--1718-1719
http-----tcp--80       icmp-----icmp
ils-----tcp--389       mgcp-----udp--2427,2727
netbios---udp--137-138  rpc-----udp--111
rsh-----tcp--514      rtsp-----tcp--554
sip-----tcp--5060     sip-----udp--5060
skinny----tcp--2000    smtp-----tcp--25
sqlnet----tcp--1521    tftp-----udp--69
xdmcp-----udp--177

dscp          Match IP DSCP (DiffServ CodePoints)
flow         Flow based Policy
port         Match TCP/UDP port(s)
precedence   Match IP precedence
rtp         Match RTP port numbers
tunnel-group Match a Tunnel Group
pixfirewall(config-cmap)# match access-list ?

mpf-class-map mode commands/options:
WORD Access List name
pixfirewall(config-cmap)# match access-list Columbia
pixfirewall(config-cmap)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# ?

MPF policy-map class configuration commands:
exit          Exit from MPF class action configuration mode
help         Help for MPF policy-map configuration commands
inspect      Protocol inspection services
ips          Intrusion prevention services
no           Negate or set default values of a command
police       Rate limit traffic for this class
priority     Strict scheduling priority for this class
set          Set QoS values or connection values
<cr>
pixfirewall(config-pmap-c)# ips ?

mpf-policy-map-class mode commands/options:
inline       Inline mode IPS
promiscuous  Promiscuous mode IPS

configure mode commands/options:
df-bit       Set IPsec DF policy
fragmentation Set IPsec fragmentation policy
security-association Set security association lifetime
transform-set Define transform and settings
pixfirewall(config-pmap-c)# ips promiscuous ?

mpf-policy-map-class mode commands/options:
fail-close  Block traffic if IPS card fails
fail-open   Permit traffic if IPS card fails
pixfirewall(config-pmap-c)# ips promiscuous fail-close
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ?

configure mode commands/options:
WORD Specify policy-map name

pixfirewall(config)# service-policy ANY ?

```

```
configure mode commands/options:
  global      Enter this keyword to specify a global policy
  interface   Enter this keyword to specify an interface policy
pixfirewall(config)# service-policy ptest global
```

In this case global is used to define all the interfaces in the PIX. Other alternatives are:

```
pixfirewall(config)# service-policy ptest interface inside
pixfirewall(config)# service-policy ptest interface outside
pixfirewall(config)# service-policy ptest interface inf2
```

Cisco PIX Challenge 58

Outline

This challenge involves defines a TCP-map.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.

Example

```
pixfirewall(config)# tcp-map test
```

```
pixfirewall(config-tcp-map)# ?
```

TCP-map configuration commands:

check-retransmission	Check retransmit data, disabled by default
checksum-verification	Verify TCP checksum, disabled by default
default	Set a command to its defaults
exceed-mss	Packet that exceed the Maximum Segment Size set by peer, default is to drop packet
no	Negate a command or set its defaults
reserved-bits	Reserved bits in TCP header are set, default is to allow packet
syn-data	TCP SYN packets that contain data, default is to allow packet
tcp-options	Options in TCP header
ttl-evasion-protection	Protection against time to live (TTL) attacks, enabled by default
urgent-flag	Urgent flag and urgent offset set, default is to clear flag and offset
window-variation	Unexpected window size variation, default is to allow connection

```
pixfirewall(config-tcp-map)# urgent-flag ?
```

tcp-map mode commands/options:

```
  allow Allow packet with urgent flag and urgent offset
  clear Clear urgent flag and urgent offset and allow packet
pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map ctest
```

pixfirewall(config-cmap)# ?

MPF class-map configuration commands:

description Specify class-map description
exit Exit from MPF class-map configuration mode
help Help for MPF class-map configuration commands
match Configure classification criteria
no Negate or set default values of a command
rename Rename this class-map

pixfirewall(config-cmap)# match ?

mpf-class-map mode commands/options:

access-list Match an Access List
any Match any packet
default-inspection-traffic Match default inspection traffic:
ctiqbe----tcp--2748 dns-----udp--53
ftp-----tcp--21 gtp-----udp--2123,3386
h323-h225-tcp--1720 h323-ras--udp--1718-1719
http-----tcp--80 icmp-----icmp
ils-----tcp--389 mgcp-----udp--2427,2727
netbios---udp--137-138 rpc-----udp--111
rsh-----tcp--514 rtsp-----tcp--554
sip-----tcp--5060 sip-----udp--5060
skinny----tcp--2000 smtp-----tcp--25
sqlnet----tcp--1521 tftp-----udp--69
xdmcp-----udp--177

dscp Match IP DSCP (DiffServ CodePoints)
flow Flow based Policy
port Match TCP/UDP port(s)
precedence Match IP precedence
rtp Match RTP port numbers
tunnel-group Match a Tunnel Group

pixfirewall(config-cmap)# match port ?

mpf-class-map mode commands/options:

tcp This keyword specifies TCP port(s)
udp This keyword specifies UDP port(s)

pixfirewall(config-cmap)# match port tcp ?

mpf-class-map mode commands/options:

eq Port equal to operator
range Port range operator

pixfirewall(config-cmap)# match port tcp range ?

mpf-class-map mode commands/options:

<0-65535> Enter port number (0 - 65535)
aol
bgp
chargen
cifs
citrix-ica
cmd
ctiqbe
daytime
discard
domain
echo
exec

```
finger
ftp
ftp-data
gopher
h323
hostname
http
https
ident
imap4
irc
kerberos
klogin
kshell
ldap
ldaps
login
lotusnotes
lpd
netbios-ssn
nntp
pcanywhere-data
pim-auto-rp
pop2
pop3
pptp
rsh
rtsp
sip
smtp
sqlnet
ssh
sunrpc
tacacs
talk
telnet
uucp
whois
www
```

```
pixfirewall(config-cmap)# match port tcp range ftp-data ?
```

```
mpf-class-map mode commands/options:
<0-65535>      Enter port number (0 - 65535)
aol
bgp
chargen
cifs
citrix-ica
cmd
ctiqbe
daytime
discard
domain
echo
exec
finger
ftp
ftp-data
gopher
h323
hostname
http
```

```

https
ident
imap4
irc
kerberos
klogin
kshell
ldap
ldaps
login
lotusnotes
lpd
netbios-ssn
nntp
pcanywhere-data
pim-auto-rp
pop2
pop3
pptp
rsh
rtsp
sip
smtp
sqlnet
ssh
sunrpc
tacacs
talk
telnet
uucp
whois
www
pixfirewall(config-cmap)# match port tcp range ftp-data www
pixfirewall(config-cmap)# exit
pixfirewall(config-cmap)# policy-map testing
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set ?

mpf-policy-map-class mode commands/options:
  connection  Configure connection parameters

configure mode commands/options:
  password-recovery  Password recovery configuration
  resetinbound      Send reset to a denied inbound TCP packet
  resetoutside      Send reset to a denied TCP packet to outside interface
pixfirewall(config-pmap-c)# set connection ?

mpf-policy-map-class mode commands/options:
  advanced-options  Configure advanced connection parameters
  conn-max          Keyword to set the maximum number of all simultaneous
                   connections that are allowed.  Default is 0 which
                   means unlimited connections.
  embryonic-conn-max  Keyword to set the maximum number of TCP embryonic
                     connections that are allowed.  Default is 0 which
                     means unlimited connections.
  random-sequence-number  Enable/disable TCP sequence number randomization.
                          Default is to enable TCP sequence number
                          randomization
  timeout           Configure connection timeout parameters
pixfirewall(config-pmap-c)# set connection advanced-options ?

mpf-policy-map-class mode commands/options:
  WORD  Enter TCP map name

```

```
pixfirewall(config-pmap-c)# set connection advanced-options test
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ?
```

```
configure mode commands/options:
  WORD Specify policy-map name
```

```
pixfirewall(config)# service-policy testing ?
```

```
configure mode commands/options:
  global      Enter this keyword to specify a global policy
  interface   Enter this keyword to specify an interface policy
pixfirewall(config)# service-policy testing global
```

Cisco PIX Challenge 59

Outline

This challenge involves defines an embryonic TCP connection timeout.

Objectives

The objectives of this challenge are to:

- Define an embryonic TCP connection timeout.

Example

```
pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# class-map ctest
```

```
pixfirewall(config-cmap)# ?
```

```
MPF class-map configuration commands:
  description Specify class-map description
  exit         Exit from MPF class-map configuration mode
  help        Help for MPF class-map configuration commands
  match       Configure classification criteria
  no          Negate or set default values of a command
  rename      Rename this class-map
```

```
pixfirewall(config-cmap)# match ?
```

```
mpf-class-map mode commands/options:
  access-list      Match an Access List
  any              Match any packet
  default-inspection-traffic Match default inspection traffic:
  ctigbe----tcp--2748      dns-----udp--53
  ftp-----tcp--21       gtp-----udp--2123,3386
  h323-h225-tcp--1720     h323-ras--udp--1718-1719
  http-----tcp--80      icmp-----icmp
  ils-----tcp--389      mgcp-----udp--2427,2727
  netbios---udp--137-138  rpc-----udp--111
  rsh-----tcp--514      rtsp-----tcp--554
  sip-----tcp--5060     sip-----udp--5060
  skinny----tcp--2000    smtp-----tcp--25
```

```

                                sqlnet----tcp--1521      tftp-----udp--69
                                xdmcp-----udp--177

dscp                            Match IP DSCP (DiffServ CodePoints)
flow                            Flow based Policy
port                            Match TCP/UDP port(s)
precedence                      Match IP precedence
rtp                             Match RTP port numbers
tunnel-group                    Match a Tunnel Group
pixfirewall(config-cmap)# match access-list ?

mpf-class-map mode commands/options:
  WORD Access List name
pixfirewall(config-cmap)# match access-list Columbia
pixfirewall(config-cmap)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# ?

MPF policy-map class configuration commands:
  exit      Exit from MPF class action configuration mode
  help      Help for MPF policy-map configuration commands
  inspect   Protocol inspection services
  ips       Intrusion prevention services
  no        Negate or set default values of a command
  police    Rate limit traffic for this class
  priority  Strict scheduling priority for this class
  set       Set QoS values or connection values
  <cr>
pixfirewall(config-pmap-c)# set ?

mpf-policy-map-class mode commands/options:
  connection  Configure connection parameters

configure mode commands/options:
  password-recovery Password recovery configuration
  resetinbound  Send reset to a denied inbound TCP packet
  resetoutside  Send reset to a denied TCP packet to outside interface
pixfirewall(config-pmap-c)# set connection ?

mpf-policy-map-class mode commands/options:
  advanced-options  Configure advanced connection parameters
  conn-max          Keyword to set the maximum number of all simultaneous
                  connections that are allowed. Default is 0 which
                  means unlimited connections.
  embryonic-conn-max  Keyword to set the maximum number of TCP embryonic
                  connections that are allowed. Default is 0 which
                  means unlimited connections.
  random-sequence-number  Enable/disable TCP sequence number randomization.
                  Default is to enable TCP sequence number
                  randomization
  timeout          Configure connection timeout parameters
pixfirewall(config-pmap-c)# set connection timeout ?

mpf-policy-map-class mode commands/options:
  embryonic  Configure absolute time after which an embryonic TCP connection
            will be closed, default is 0:00:30.
  half-closed  Configure idle time after which a TCP half-closed connection
            will be freed, default is 0:10:00
  tcp         Configure idle time after which a TCP connection state will be
            closed, default is 1:00:00
pixfirewall(config-pmap-c)# set connection timeout embryonic ?

```

```
mpf-policy-map-class mode commands/options:
  0:0:0 | <0:5:0> - <1192:59:59> Idle time after which a TCP connection state
                                will be closed, default is 1:00:00. Specify
                                0:0:0 to never time out
  <0-0>                            Specify this value to never time out
pixfirewall(config-pmap-c)# set connection timeout embryonic 0:00:10
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ?
```

```
configure mode commands/options:
  WORD Specify policy-map name
```

```
pixfirewall(config)# service-policy ptest?
```

```
configure mode commands/options:
  global      Enter this keyword to specify a global policy
  interface   Enter this keyword to specify an interface policy
pixfirewall(config)# service-policy ptest global
```

In this case global is used to define all the interfaces in the PIX. Other alternatives are:

```
pixfirewall(config)# service-policy ptest interface inside
pixfirewall(config)# service-policy ptest interface outside
pixfirewall(config)# service-policy ptest interface inf2
```

Cisco PIX Challenge 60

Outline

This challenge involves defines the maximum number of embryonic TCP connections.

Objectives

The objectives of this challenge are to:

- Define maximum number of embryonic TCP connections.

Example

```
pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list Columbia
pixfirewall(config-cmap)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set ?
```

```
mpf-policy-map-class mode commands/options:
  connection Configure connection parameters
```

```
configure mode commands/options:
```

```

password-recovery Password recovery configuration
resetinbound      Send reset to a denied inbound TCP packet
resetoutside      Send reset to a denied TCP packet to outside interface
pixfirewall(config-pmap-c)# set connection ?

mpf-policy-map-class mode commands/options:
  advanced-options  Configure advanced connection parameters
  conn-max          Keyword to set the maximum number of all simultaneous
                   connections that are allowed. Default is 0 which
                   means unlimited connections.
  embryonic-conn-max Keyword to set the maximum number of TCP embryonic
                   connections that are allowed. Default is 0 which
                   means unlimited connections.
  random-sequence-number Enable/disable TCP sequence number randomization.
                   Default is to enable TCP sequence number
                   randomization
  timeout           Configure connection timeout parameters
pixfirewall(config-pmap-c)# set connection embryonic-conn-max ?

mpf-policy-map-class mode commands/options:
  <0-65535> Enter the maximum number for all simultaneous connections
pixfirewall(config-pmap-c)# set connection embryonic-conn-max 2
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest global

```

In this case the TCP Intercept is used to proxy connections after the second one, thus the PIX firewall will send the SYN, ACK reply to a SYN request.

Cisco PIX Challenge 61

Outline

This challenge involves the PIX check TCP checksums.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Define that checksums must be verified.

Example

```

pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# tcp-map TEST
pixfirewall(config-tcp-map)# ?

```

```

TCP-map configuration commands:
  check-retransmission  Check retransmit data, disabled by default
  checksum-verification Verify TCP checksum, disabled by default
  default               Set a command to its defaults

```

```

exceed-mss          Packet that exceed the Maximum Segment Size set by
                    peer, default is to drop packet
no                  Negate a command or set its defaults
reserved-bits       Reserved bits in TCP header are set, default is to
                    allow packet
syn-data            TCP SYN packets that contain data, default is to
                    allow packet
tcp-options         Options in TCP header
ttl-evasion-protection Protection against time to live (TTL) attacks,
                    enabled by default
urgent-flag         Urgent flag and urgent offset set, default is to
                    clear flag and offset
window-variation    Unexpected window size variation, default is to allow
                    connection
pixfirewall(config-tcp-map)# checksum-verification

pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list test
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map testing
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set connection advanced-options TEST
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy testing global

```

In this case the checksum of all TCP segments will be checked. If they are incorrect, as in the case of spoofed data packets, they will be dropped. This, though, will have a performance impact on the firewall, and should be checked for its performance. The access-list:

```

pixfirewall(config)# access-list Columbia permit ip any any

```

allow for all the traffic to be checked.

Cisco PIX Challenge 62

Outline

This challenge involves the PIX checks the maximum segment size for TCP details.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Define that Exceeded-MSS is allowed or not.

Example

```

pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# tcp-map TEST

```

```
pixfirewall(config-tcp-map)# ?
```

```
TCP-map configuration commands:
```

```
check-retransmission    Check retransmit data, disabled by default
checksum-verification  Verify TCP checksum, disabled by default
default                 Set a command to its defaults
exceed-mss              Packet that exceed the Maximum Segment Size set by
                        peer, default is to drop packet
no                       Negate a command or set its defaults
reserved-bits           Reserved bits in TCP header are set, default is to
                        allow packet
syn-data                TCP SYN packets that contain data, default is to
                        allow packet
tcp-options             Options in TCP header
ttl-evasion-protection  Protection against time to live (TTL) attacks,
                        enabled by default
urgent-flag             Urgent flag and urgent offset set, default is to
                        clear flag and offset
window-variation        Unexpected window size variation, default is to allow
                        connection
```

```
pixfirewall(config-tcp-map)# exceed-mss ?
```

```
tcp-map mode commands/options:
```

```
allow Allow packet that exceed the Maximum Segment Size
drop Drop packet that exceed the Maximum Segment Size
```

```
pixfirewall(config-tcp-map)# exceed-mss allow
```

```
pixfirewall(config-tcp-map)# exit
```

```
pixfirewall(config)# class-map ctest
```

```
pixfirewall(config-cmap)# match access-list test
```

```
pixfirewall(config-cmap)# exit
```

```
pixfirewall(config)# policy-map testing
```

```
pixfirewall(config-pmap)# class ctest
```

```
pixfirewall(config-pmap-c)# set connection advanced-options TEST
```

```
pixfirewall(config-pmap-c)# exit
```

```
pixfirewall(config-pmap)# exit
```

```
pixfirewall(config)# service-policy testing global
```

Cisco PIX Challenge 63

Outline

This challenge involves the preventing inconsistent TCP re-transmissions.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Check for TCP re-transmissions.

Example

```
pixfirewall(config)# access-list Columbia permit ip any any
```

```
pixfirewall(config)# tcp-map TEST  
pixfirewall(config-tcp-map)# ?
```

TCP-map configuration commands:

```
check-retransmission    Check retransmit data, disabled by default  
checksum-verification  Verify TCP checksum, disabled by default  
default                 Set a command to its defaults  
exceed-mss              Packet that exceed the Maximum Segment Size set by  
                        peer, default is to drop packet  
no                       Negate a command or set its defaults  
reserved-bits           Reserved bits in TCP header are set, default is to  
                        allow packet  
syn-data                TCP SYN packets that contain data, default is to  
                        allow packet  
tcp-options             Options in TCP header  
ttl-evasion-protection  Protection against time to live (TTL) attacks,  
                        enabled by default  
urgent-flag             Urgent flag and urgent offset set, default is to  
                        clear flag and offset  
window-variation        Unexpected window size variation, default is to allow  
                        connection
```

```
pixfirewall(config-tcp-map)# check-retransmission
```

```
pixfirewall(config-tcp-map)# exit  
pixfirewall(config)# class-map ctest  
pixfirewall(config-cmap)# match access-list test  
pixfirewall(config-cmap)# exit  
pixfirewall(config)# policy-map testing  
pixfirewall(config-pmap)# class ctest  
pixfirewall(config-pmap-c)# set connection advanced-options TEST  
pixfirewall(config-pmap-c)# exit  
pixfirewall(config-pmap)# exit  
pixfirewall(config)# service-policy testing global
```

Cisco PIX Challenge 64

Outline

This challenge involves the setting the limit for out-of-sequence TCP segments.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Define the limit for the TCP queue.

Example

```
pixfirewall(config)# access-list Columbia permit ip any any  
pixfirewall(config)# tcp-map TEST  
pixfirewall(config-tcp-map)# ?
```

TCP-map configuration commands:

```
check-retransmission    Check retransmit data, disabled by default
```

```

checksum-verification  Verify TCP checksum, disabled by default
default                Set a command to its defaults
exceed-mss             Packet that exceed the Maximum Segment Size set by
                        peer, default is to drop packet
no                     Negate a command or set its defaults
reserved-bits          Reserved bits in TCP header are set, default is to
                        allow packet
syn-data               TCP SYN packets that contain data, default is to
                        allow packet
tcp-options            Options in TCP header
ttl-evasion-protection Protection against time to live (TTL) attacks,
                        enabled by default
urgent-flag            Urgent flag and urgent offset set, default is to
                        clear flag and offset
window-variation       Unexpected window size variation, default is to allow
                        connection
pixfirewall(config-tcp-map)# queue-limit 64

pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list test
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map testing
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set connection advanced-options TEST
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy testing global

```

Cisco PIX Challenge 64

Outline

This challenge involves checking the TCP reserved bits.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Define the action of reserved bits.

Example

```

pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# tcp-map TEST
pixfirewall(config-tcp-map)# ?

```

TCP-map configuration commands:

```

check-retransmission  Check retransmit data, disabled by default
checksum-verification Verify TCP checksum, disabled by default
default                Set a command to its defaults
exceed-mss             Packet that exceed the Maximum Segment Size set by
                        peer, default is to drop packet
no                     Negate a command or set its defaults

```

```

reserved-bits      Reserved bits in TCP header are set, default is to
                   allow packet
syn-data           TCP SYN packets that contain data, default is to
                   allow packet
tcp-options        Options in TCP header
ttl-evasion-protection Protection against time to live (TTL) attacks,
                   enabled by default
urgent-flag        Urgent flag and urgent offset set, default is to
                   clear flag and offset
window-variation   Unexpected window size variation, default is to allow
                   connection
pixfirewall(config-tcp-map)# reserved-bit ?

tcp-map mode commands/options:
  allow Allow packets with reserved bits in TCP header
  clear Clear reserved bits in TCP header and allow packet
  drop Drop packet with reserved bits set

configure mode commands/options:
  threshold Configure remote-access thresholds
pixfirewall(config-tcp-map)# reserved-bit allow

pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list test
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map testing
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set connection advanced-options TEST
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy testing global

```

Cisco PIX Challenge 66

Outline

This challenge involves checking if the SYN flag appears with Data.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Define the action of SYN-Data.

Example

```

pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# tcp-map TEST
pixfirewall(config-tcp-map)# ?

```

```

TCP-map configuration commands:
  check-retransmission Check retransmit data, disabled by default
  checksum-verification Verify TCP checksum, disabled by default

```

```

default          Set a command to its defaults
exceed-mss       Packet that exceed the Maximum Segment Size set by
                 peer, default is to drop packet
no               Negate a command or set its defaults
reserved-bits    Reserved bits in TCP header are set, default is to
                 allow packet
syn-data         TCP SYN packets that contain data, default is to
                 allow packet
tcp-options      Options in TCP header
ttl-evasion-protection Protection against time to live (TTL) attacks,
                 enabled by default
urgent-flag      Urgent flag and urgent offset set, default is to
                 clear flag and offset
window-variation Unexpected window size variation, default is to allow
                 connection
pixfirewall(config-tcp-map)# syn-data ?
tcp-map mode commands/options:
  allow  Allow SYN packets that contain data
  drop   Drop SYN packets that contain data

configure mode commands/options:
  connection  Configure sysopt connection settings
  nodnsalias  Disable DNS A record translation
  noproxyarp  Disable proxy ARP
  radius      Ignore secret in RADIUS accounting responses
  uauth       Allow web browsers to supply a cached username and password for
              AAA authentication
pixfirewall(config-tcp-map)# syn-data drop

pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list test
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map testing
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set connection advanced-options TEST
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy testing global

```

Cisco PIX Challenge 67

Outline

This challenge involves disabling TTL evasion protection.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Disable TTL evasion protection.

Example

```
pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# tcp-map TEST
pixfirewall(config-tcp-map)# ?
```

TCP-map configuration commands:

check-retransmission	Check retransmit data, disabled by default
checksum-verification	Verify TCP checksum, disabled by default
default	Set a command to its defaults
exceed-mss	Packet that exceed the Maximum Segment Size set by peer, default is to drop packet
no	Negate a command or set its defaults
reserved-bits	Reserved bits in TCP header are set, default is to allow packet
syn-data	TCP SYN packets that contain data, default is to allow packet
tcp-options	Options in TCP header
ttl-evasion-protection	Protection against time to live (TTL) attacks, enabled by default
urgent-flag	Urgent flag and urgent offset set, default is to clear flag and offset
window-variation	Unexpected window size variation, default is to allow connection

```
pixfirewall(config-tcp-map)# ttl-evasion-protection
```

```
pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list test
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map testing
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set connection advanced-options TEST
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy testing global
```

With TTL evasion, an attacker can send a packet to the firewall with a small TTL (Time-to-Live). Once it goes to zero, somewhere between the firewall and the host, the packet is dropped. The attacker can then send more packets with high TTLs which will get through. The rebuilt segments could then contain malicious information, which would not be detected by IDSs or the firewalls.

Cisco PIX Challenge 68

Outline

This challenge involves allowing or denying TCP Window variations in TCP connections.

Objectives

The objectives of this challenge are to:

- Define a TCP-map.
- Disable/enable TCP Window variations.

Example

```
pixfirewall(config)# access-list Columbia permit ip any any
pixfirewall(config)# tcp-map TEST
pixfirewall(config-tcp-map)# ?
```

TCP-map configuration commands:

check-retransmission	Check retransmit data, disabled by default
checksum-verification	Verify TCP checksum, disabled by default
default	Set a command to its defaults
exceed-mss	Packet that exceed the Maximum Segment Size set by peer, default is to drop packet
no	Negate a command or set its defaults
reserved-bits	Reserved bits in TCP header are set, default is to allow packet
syn-data	TCP SYN packets that contain data, default is to allow packet
tcp-options	Options in TCP header
ttl-evasion-protection	Protection against time to live (TTL) attacks, enabled by default
urgent-flag	Urgent flag and urgent offset set, default is to clear flag and offset
window-variation	Unexpected window size variation, default is to allow connection

```
pixfirewall(config-tcp-map)# window-variation ?
```

tcp-map mode commands/options:

allow-connection	Allow connection with unexpected window size variation
drop-connection	Drop connection with unexpected window size variation

```
pixfirewall(config-tcp-map)# window-variation drop
```

```
pixfirewall(config-tcp-map)# exit
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list test
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map testing
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# set connection advanced-options TEST
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy testing global
```

With TTL evasion, an attacker can send a packet to the firewall with a small TTL (Time-to-Live). Once it goes to zero, somewhere between the firewall and the host, the packet is dropped. The attacker can then send more packets with high TTLs which will get through. The rebuilt segments could then contain malicious information, which would not be detected by IDSs or the firewalls.

Cisco PIX Challenge 69

Outline

This challenge involves preventing IP spoofing by enabling Unicast Reverse Path Forwarding (Unicast RPF) which ensures that all of the packets have a source IP address which matches the correct source interface according to the routing table.

Objectives

The objectives of this challenge are to:

- Enable Unicast RPF.

Example

```
pixfirewall(config)# int e0
pixfirewall(config-if)# ip address 192.168.0.1 255.255.255.0
pixfirewall(config-if)# nameif test1
pixfirewall(config-if)# exit
pixfirewall(config)# int e1
pixfirewall(config-if)# ip address 192.168.0.1 255.255.255.0
pixfirewall(config-if)# nameif test2
pixfirewall(config-if)# exit
pixfirewall(config)# int e2
pixfirewall(config-if)# ip address 192.168.0.1 255.255.255.0
pixfirewall(config-if)# nameif test3
pixfirewall(config-if)# exit

pixfirewall(config)# ip ?

configure mode commands/options:
  audit    Configure the Intrusion Detection System
  local    Define a local pool of IP addresses
  verify   Configure Unicast Reverse Path Filtering on an interface
pixfirewall(config)# ip verify ?

configure mode commands/options:
  reverse-path Keyword to indicate Reverse-Path Filtering
pixfirewall(config)# ip verify reverse-path ?

configure mode commands/options:
  interface Keyword to apply RPF on an interface
pixfirewall(config)# ip verify reverse-path interface ?

configure mode commands/options:
Current available interface(s):
  test3    Name of interface Ethernet2
  test2    Name of interface Ethernet1
  test1    Name of interface Ethernet0
pixfirewall(config)# ip verify reverse-path interface test1
pixfirewall(config)# ip verify reverse-path interface test2
pixfirewall(config)# ip verify reverse-path interface test3
```

Cisco PIX Challenge 70

Outline

This challenge involves defining the fragments per IP packet. Normally this is set at a maximum of 24 fragments per IP packet, with, up to, 200 fragments awaiting reassembly.

Fragmented packets can be used in a DoS attack. This challenge restricts the number of fragments.

Objectives

The objectives of this challenge are to:

- Define maximum fragments per packet (using the **fragment chain** command)
- Define the maximum number of awaiting fragments (using the **fragment size** command).
- Define the timeout for all the parts of a packet to arrive (using the **fragment timeout** command).

Example

```
pixfirewall(config)# int e0
pixfirewall(config-if)# ip address 192.168.0.1 255.255.255.0
pixfirewall(config-if)# nameif test1
pixfirewall(config-if)# exit
pixfirewall(config)# int e1
pixfirewall(config-if)# ip address 192.168.0.1 255.255.255.0
pixfirewall(config-if)# nameif test2
pixfirewall(config-if)# exit
pixfirewall(config)# int e2
pixfirewall(config-if)# ip address 192.168.0.1 255.255.255.0
pixfirewall(config-if)# nameif test3
pixfirewall(config-if)# exit
```

```
pixfirewall(config)# fragment ?
```

```
configure mode commands/options:
```

```
chain    Configure maximum number of elements in a fragment set
size     Configure maximum number of blocks in database
timeout  Configure number of seconds to assemble a fragment set
```

```
pixfirewall(config)# fragment chain ?
```

```
configure mode commands/options:
```

```
<1-8200> Maximum number of elements in a fragment set, default is 24
```

```
pixfirewall(config)# fragment chain 1 ?
```

```
configure mode commands/options:
```

```
Current available interface(s):
```

```
Test3    Name of interface Ethernet2
Test2    Name of interface Ethernet1
Test1    Name of interface Ethernet0
<cr>
```

```
pixfirewall(config)# fragment chain 1 test3
```

```
pixfirewall(config)# fragment size ?
```

```
configure mode commands/options:
```

```
<1-30000> Maximum number of blocks in database, default is 200
```

```
pixfirewall(config)# fragment size 10 test1
```

```
pixfirewall(config)# fragment timeout ?
```

configure mode commands/options:

<1-30> Number of seconds to assemble a fragment set, default is 5

```
pixfirewall(config)# fragment timeout 10 test1
```

The **fragment chain** command is used to define the fragments per packet, while the **fragment size** command defines the maximum number of fragments that await assembly. Also the fragment timeout command is used to limit the time for all parts of a packet to arrive.

The command:

```
(config)# fragment chain 500
```

Would define the fragments per packet on all interfaces, while:

```
(config)# fragment chain 500 outside
```

would define it for the outside interface.

Cisco PIX Challenge 71

Outline

This challenge involves defining a VLAN on a subinterface. It is not possible to assign a VLAN to a subinterface and not to a physical interface.

Objectives

The objectives of this challenge are to:

- Define a VLAN on a sub-interface.
- Enable the sub-interface

Example

```
pixfirewall(config)# int e0.1
```

```
pixfirewall(config-subif)# ?
```

Interface configuration commands:

default Set a command to its defaults

description Interface specific description

```

exit                Exit from interface configuration mode
help                Interactive help for interface subcommands
igmp                IGMP interface commands
ip                  Configure ip addresses.
ipv6                IPv6 interface subcommands
management-only    Dedicate an interface to management. Block thru traffic
nameif              Assign name to interface
no                  Negate a command or set its defaults
ospf                Configure interface specific OSPF parameters
pim                 PIM interface commands
security-level      Specify the security level of this interface after this
                    keyword, Eg: 0, 100 etc. The relative security level between
                    two interfaces determines the way the Adaptive Security
                    Algorithm is applied. A lower security_level interface is
                    outside relative to a higher level interface and equivalent
                    interfaces are outside to each other
shutdown            Shutdown the selected interface
vlan                Configure VLAN identifier
pixfirewall(config-subif)# vl ?

subinterface mode commands/options:
<1-4094> IEEE 802.1Q VLAN Identifier
pixfirewall(config-subif)# vlan 2
pixfirewall(config-subif)# no shutdown
pixfirewall(config-subif)# exit
pixfirewall(config)# int e1.1
pixfirewall(config-subif)# vlan 2
pixfirewall(config-subif)# no shutdown
pixfirewall(config-subif)# exit
pixfirewall(config)# int e2.1
pixfirewall(config-subif)# vlan 2
pixfirewall(config-subif)# no shutdown
pixfirewall(config-subif)# exit

```

Cisco PIX Challenge 72

Outline

This challenge involves defining the attributes for the group-policy.

Objectives

The objectives of this challenge are to:

- Define a group-policy attribute.
- Define attributes.
- Define a tunnel-group.
- Define IPSec attributes.

Example

```
pixfirewall(config)# group-policy ?
```

```
configure mode commands/options:
```

WORD < 65 char Enter the name of the group policy

pixfirewall(config)# group-policy test ?

configure mode commands/options:

attributes Enter the attributes sub-command mode
external Enter this keyword to specify an external group policy
internal Enter this keyword to specify an internal group policy

pixfirewall(config)# group-policy test attributes

pixfirewall(config-group-policy)# ?

group_policy configuration commands:

backup-servers	Configure list of backup servers to be used by the remote client
banner	Configure a banner, or welcome text to be displayed on the VPN remote client
client-access-rule	Specify rules permitting/denying access to specific client types and versions.
client-firewall	Configure the firewall requirements for users in this group-policy
default-domain	Configure default domain name given to users of this group
dhcp-network-scope	Specify the range of IP addresses to indicate to the DHCP server for address assignment
dns-server	Configure the primary and secondary DNS servers
exit	Exit from group-policy configuration mode
group-lock	Enter name of an existing tunnel-group that users are required to connect with
help	Help for group_policy configuration commands
ip-comp	Enter this command to enable IP compression(LZS)
ip-phone-bypass	Configure to allow Cisco IP phones behind Hardware clients to bypass the Individual User Authentication process.
ipsec-udp	Enter this command to allow a client to operate through a NAT device using UDP encapsulation
ipsec-udp-port	Enter the UDP port to be used by the client for IPSec through NAT
leap-bypass	Enable/disable LEAP packets from Cisco wireless devices to bypass the individual user authentication process. This setting applies only to HW clients.
nem	Configure hardware clients to use network extension mode. This setting applies only to HW clients.
no	Remove an attribute value pair
password-storage	Enable/disable storage of the login password on the client system
pfs	Enter this command to indicate that the remote client needs to perform PFS
re-xauth	Enter this command to enable reauthentication of the user on IKE rekey
secure-unit-authentication	Configure interactive authentication. This setting applies only to HW clients.
split-dns	Configure list of domains to be resolved through the Split Tunnel
split-tunnel-network-list	Configure name of access-list for split tunnel configuration
split-tunnel-policy	Select the split tunneling method to be

user-authentication	used by the remote client Configure individual user authentication. This setting applies only to HW clients.
user-authentication-idle-timeout	Configure the idle timeout period in minutes. If there is no communication in this period, the system terminates the connection. This setting applies only to HW clients.
vpn-access-hours	Enter name of a configured time-range policy
vpn-filter	Enter name of a configured ACL to apply to users
vpn-idle-timeout	Enter idle timeout period in minutes, enter none to disable
vpn-session-timeout	Enter maximum user connection time in minutes, enter none for unlimited time
vpn-simultaneous-logins	Enter maximum number of simultaneous logins allowed
vpn-tunnel-protocol	Enter permitted tunneling protocols
wins-server	Configure the primary and secondary WINS servers

pixfirewall(config-group-policy)# banner none

group-policy mode commands/options:

none Specify that no banner text will be displayed on the VPN remote client
value Specify the banner or welcome text to be displayed on the VPN remote client

pixfirewall(config-group-policy)# banner none

pixfirewall(config-group-policy)# vpn-simultaneous-logins ?

group-policy mode commands/options:

<0-2147483647> Maximum number of simultaneous logins allowed, enter 0 to disable login and prevent user access

pixfirewall(config-group-policy)# vpn-simultaneous-logins 10

pixfirewall(config-group-policy)# vpn-idle ?

group-policy mode commands/options:

<1-35791394> Number of minutes
none Disable timeout and allow an unlimited idle period

pixfirewall(config-group-policy)# vpn-idle 10

pixfirewall(config-group-policy)# vpn-tunnel ?

group-policy mode commands/options:

IPSec IP Security Protocol

pixfirewall(config-group-policy)# vpn-tunnel ipsec

pixfirewall(config-group-policy)# wins-server ?

group-policy mode commands/options:

none No wins-server will be specified and disable inheritance
value Specify the primary and secondary WINS servers

pixfirewall(config-group-policy)# wins-server 10

pixfirewall(config-group-policy)# dhcp-server ?

group-policy mode commands/options:

A.B.C.D The IP sub-network that the DHCP server should assign to users in this group

```

    none      No range of IP addresses will be specified and disable inheritance
pixfirewall(config-group-policy)# dhcp-server 10
pixfirewall(config-group-policy)# exit
pixfirewall(config)# exit
pixfirewall# sh running
pixfirewall# config t

```

```
pixfirewall(config)# tunnel-group test type ?
```

```

configure mode commands/options:
    ipsec-l2l  IPsec Site to Site group
    ipsec-ra   IPsec Remote Access group
pixfirewall(config)# tunnel-group test type ipsec-ra

```

```
pixfirewall(config)# tunnel-group test ?
```

```

configure mode commands/options:
    general-attributes  Enter the general-attributes sub command mode
    ipsec-attributes    Enter the ipsec-attributes sub command mode
    type                Enter the type of this group-policy
pixfirewall(config)# tunnel-group test general-attributes

```

```
pixfirewall(config-general)# ?
```

```

group_policy configuration commands:
    accounting-server-group  Enter name of the accounting server group
    address-pool             Enter a list of address pools to assign
                             addresses from
    authentication-server-group  Enter name of the authentication server group
    authorization-server-group  Enter name of the authorization server group
    default-group-policy      Enter name of the default group policy
    dhcp-server               Enter IP address or name of the DHCP server
    exit                      Exit from tunnel-group general attribute
                             configuration mode
    help                      Help for tunnel group configuration commands
    no                        Remove an attribute value pair
    strip-group               Enable strip-group processing
    strip-realm               Enable strip-realm processing

```

```
pixfirewall(config-general)# exit
```

```
pixfirewall(config)# tunnel-g test ?
```

```

configure mode commands/options:
    general-attributes  Enter the general-attributes sub command mode
    ipsec-attributes    Enter the ipsec-attributes sub command mode
    type                Enter the type of this group-policy

```

```
pixfirewall(config)# tunnel-group test ipsec-attributes
```

```
pixfirewall(config-ipsec)# ?
```

```

group_policy configuration commands:
    authorization-dn-attributes  The DN of the peer certificate used as username
                                for authorization
    authorization-required       Require users to authorize successfully in order
                                to connect
    chain                        Enable sending certificate chain
    client-update                Configure and change client update parameters
    exit                         Exit from tunnel-group IPsec attribute
                                configuration mode
    help                         Help for tunnel group configuration commands
    isakmp                       Configure ISAKMP policy
    no                           Remove an attribute value pair
    peer-id-validate             Validate identity of the peer using the peer's
                                certificate

```

pre-shared-key	Associate a pre-shared key with the connection policy
radius-with-expiry	Enable negotiation of password update during RADIUS authentication
trust-point	Enter name of the trustpoint that identifies the certificate to be sent to the IKE peer

Cisco PIX Challenge 73

Outline

This challenge involves defining that each of the ports has the same security level, so that all the ports can communicate with each other. Also the test recaps TELNET, SSH and HTTP details.

Objectives

The objectives of this challenge are to:

- Define the details of the ports
- Apply the same security level.
- Generate RSA keys.
- Define TELNET, SSH and HTTP details.

Example

```
# config t
(config)# int e0
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# nameif ?

interface mode commands/options:
  WORD < 49 char  A name by which this interface will be referred in all other
                  Commands
(config-if)# nameif out
(config-if)# security ?

interface mode commands/options:
  <0-100> Security level for the interface

(config-if)# security 0
(config-if)# no shutdown
(config-if)# exit
(config)# int e1
(config-if)# ip address outside 192.168.2.1 255.255.255.0
(config-if)# nameif in
(config-if)# no shutdown
(config-if)# exit

(config)# same-security-traffic ?

configure mode commands/options:
  permit Keyword for enabling this functionality
```

```

(config)# same-security-traffic permit ?

configure mode commands/options:
  inter-interface  Permit communication between different interfaces with the
                   same security level
  intra-interface Permit communication between VPN peers connected to the same
                   interface
(config)# same-security-traffic permit inter-interface

(config)# cry key ?

configure mode commands/options:
  generate  Generate new keys
  zeroize   Remove keys
(config)# crypto key generate ?

configure mode commands/options:
  dsa  Generate DSA keys
  rsa  Generate RSA keys
(config)# crypto key generate rsa ?

configure mode commands/options:
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  label         Provide a label
  modulus       Provide number of modulus bits on the command line
  noconfirm     Specify this keyword to suppress all interactive prompting.
  usage-keys    Generate separate RSA key pairs for signing and encryption
  <cr>

(config)# crypto key generate rsa modulus ?

configure mode commands/options:
  1024  1024 bits
  2048  2048 bits
  512   512 bits
  768   768 bits
(config)# crypto key generate rsa modulus 1024
(config)# telnet 204.134.17.7 255.255.192.0 inside
(config)# telnet 201.13.14.2 255.255.240.0 outside
(config)# telnet 210.1.170.5 255.255.224.0 inf2
(config)# telnet timeout 10
(config)# show telnet
(config)# show telnet timeout
(config)# ssh 204.134.17.7 255.255.192.0 inside
(config)# ssh timeout 10
(config)# http server enable
(config)# http 204.134.17.7 255.255.192.0 inside
(config)# http 201.13.14.2 255.255.240.0 outside

```

Cisco PIX Challenge 74

Outline

This challenge involves defining the default route for traffic for both tunneled and non-tunneled traffic.

Objectives

The objectives of this challenge are to:

- Define interface details.
- Define default routes.

Example

```
# config t
(config)# int e0
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# nameif ?

interface mode commands/options:
  WORD < 49 char  A name by which this interface will be referred in all other
                  Commands
(config-if)# nameif edinburgh
(config-if)# exit
(config)# exit
(config)# route ?

configure mode commands/options:
Current available interface(s):
  Inf2 Name of interface Ethernet2
  Inside      Name of interface Ethernet1
  Edinburgh   Name of interface Ethernet0
(config)# route Edinburgh ?

configure mode commands/options:
  Hostname or A.B.C.D  The foreign network for this route, 0 means default

(config)# route Edinburgh 0 ?

configure mode commands/options:
  A.B.C.D  The netmask for the destined foreign network

(config)# route Edinburgh 0 0 ?

configure mode commands/options:
  Hostname or A.B.C.D  The address of the gateway by which the foreign network
                      is reached.
(config)# route Edinburgh 0 0 192.168.0.2

(config)# route Edinburgh 0 0 192.168.0.3 ?

configure mode commands/options:
  <1-255>  Distance metric for this route, default is 1
  tunneled Enable the default tunnel gateway option, metric is set
          to 255
  <cr>
(config)# route Edinburgh 0 0 192.168.0.3 tunneled
```

Cisco PIX Challenge 75

Outline

This challenge involves defining PIM to maintain forwarding tables for forwarding multicast diagrams.

Objectives

The objectives of this challenge are to:

- Define interface details.
- Define PIM details.

Example

```
# config t
(config)# int e0
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# nameif ?

interface mode commands/options:
  WORD < 49 char  A name by which this interface will be referred in all other
                  Commands
(config-if)# nameif Edinburgh
(config-if)# pim ?

interface mode commands/options:
  dr-priority          PIM Hello DR priority
  hello-interval      PIM neighbor Hello announcement interval
  join-prune-interval PIM periodic Join-Prune announcement interval
  <cr>

configure mode commands/options:
  accept-register      Register accept filter
  old-register-checksum Generate registers compatible with older IOS versions
  rp-address           Configure Sparse-Mode Rendezvous Point
  spt-threshold        Configure threshold for SPT switchover on last-hop

(config-if)# pim

(config-if)# pim dr-priority ?

interface mode commands/options:
  <0-4294967295> Hello DR priority, preference given to larger value
(config-if)# pim dr-priority 50

(config-if)# pim hello-interval ?

interface mode commands/options:
  <1-3600> Hello interval in seconds
(config-if)# pim hello-interval 50

(config-if)# pi join-prune-interval ?

interface mode commands/options:
  <10-600> Join-Prune interval in seconds
(config-if)# pi join-prune-interval 50

(config-if)# exit
(config)# pim ?
```

```
configure mode commands/options:
  accept-register      Register accept filter
  old-register-checksum  Generate registers compatible with older IOS versions
  rp-address           Configure Sparse-Mode Rendezvous Point
  spt-threshold        Configure threshold for SPT switchover on last-hop
```

```
(config)# pim accept-register ?
```

```
configure mode commands/options:
  list      Access list
  route-map Route-map
```

```
(config)# pim old-register-checksum ?
```

```
configure mode commands/options:
  <cr>
```

```
exec mode commands/options:
```

```
  Hostname or A.B.C.D      Ping destination IPv4 address or hostname
  Hostname or X:X:X:X::X   Ping destination IPv6 address or hostname
  <cr>
```

```
(config)# pim rp-address ?
```

```
configure mode commands/options:
  Hostname or A.B.C.D  IP name or address of Rendezvous Point
```

```
(config)# pim rp-address 192.168.0.1
```

```
(config)# pim spt-threshold ?
```

```
configure mode commands/options:
  infinity  Always stay on shared-tree
```

Cisco PIX Challenge 76

Outline

This challenge involves defining DHCP relay, where DHCP requests can be forwarded to a certain interface.

Objectives

The objectives of this challenge are to:

- Define interface details.
- Define DHCP relay details.

Example

```
# config t
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# nameif Edinburgh
(config-if)# exit
```

```

(config)# dhcprelay ?

configure mode commands/options:
  enable      Start a DHCP server task on an interface, but at least one
              dhcpdrelay server must be configured before enable is issued
  server      Configure dhcprelay server information
  setroute    Configure the DHCP Relay Agent to change the first default
              router address (in the packet sent from the DHCP server) to
              the address of the client interface
  timeout     Configure timeout, the number of seconds for relay address
              negotiation after this keyword
configure mode commands/options:
  infinity    Always stay on shared-tree
(config)# dhcprelay server ?

configure mode commands/options:
  Hostname or A.B.C.D  IP address of dhcprelay server to which
                      requests are forwarded
(config)# dhcprelay server 192.168.1.2
(config)# dhcprelay setroute ?

configure mode commands/options:
Available client interface names:
  Inf2        Name of interface Ethernet2
  Inside      Name of interface Ethernet1
  Edinburgh   Name of interface Ethernet0
(config)# dhcprelay enable ?

configure mode commands/options:
Available interfaces on which relay agent will accept client requests:
  Inf2        Name of interface Ethernet2
  Inside      Name of interface Ethernet1
  Edinburgh   Name of interface Ethernet0
(config)# dhcprelay enable Edinburgh
(config)# dhcprelay timeout ?

configure mode commands/options:
  <1-3600>    Enter number of seconds for relay address negotiation, default
              is 60 seconds
  <cr>
(config)# dhcprelay timeout 10

```

Cisco PIX Challenge 77

Outline

This challenge involves defining the transparent firewall mode, and to enable EtherType access filtering.

Objectives

The objectives of this challenge are to:

- Define a transparent firewall.
- Define EtherType filtering.

Example

```
# config t
pixfirewall(config)# firewall ?

configure mode commands/options:
  transparent  Switch to transparent mode
(config)# firewall transparent
Switched to transparent mode
(config)# access-list ?

configure mode commands/options:
  WORD < 241 char  Access list identifier
  alert-interval  Specify the alert interval for generating syslog message
                  106001 which alerts that the system has reached a deny
                  flow maximum. If not specified, the default value is 300 sec
  deny-flow-max   Specify the maximum number of concurrent deny flows that can
                  be created. If not specified, the default value is 4096
(config)# access-list TEST ?

configure mode commands/options:
  deny          Specify packets to reject
  ethertype    Configure access policy for non IP traffic through the
               system when configured in transparent mode
  extended     Configure access policy for IP traffic through the system
  line        Use this to specify line number at which ACE should be entered
  permit      Specify packets to forward
  remark      Specify a comment (remark) for the access-list after this
               keyword
  standard    Use this to configure policy having destination host or network
               only
(config)# access-list TEST ethertype ?

configure mode commands/options:
  deny  Specify packets to reject
  permit Specify packets to forward
(config)# access-list TEST ethertype deny ?

configure mode commands/options:
  bpd
  ipx
  mpls-unicast
  mpls-multicast
  any
  <0x600-0xffff> Specify ethertype value
(config)# access-list TEST ethertype deny ipx
(config)# access-list TEST ethertype deny bpd

pixfirewall(config)# access-group TEST ?

configure mode commands/options:
  in  For input traffic
  out For output traffic
pixfirewall(config)# access-group TEST in ?

configure mode commands/options:
  interface Keyword to specify an interface
pixfirewall(config)# access-group TEST in interface ?

configure mode commands/options:
Current available interface(s):
```

```
Current available interface(s):
  Inf2      Name of interface Ethernet2
  inside   Name of interface Ethernet1
  outside  Name of interface Ethernet0
```

```
(config)# access-group TEST in interface outside
(config)# access-group TEST in interface inside
```

Cisco PIX Challenge 78

Outline

This challenge involves automated updates for the firewall, and enabling ARP inspection. ARP inspect helps to overcome the ARP spoofing, where an intruder can respond to a request for a gateway address with their own address, and thus route packets through the intruders system. This is known as a man-in-the-middle attack, where the intruder would route the data out of the main gateway. For this to work the firewall must contain an ARP entry for each host on the network.

NOTE: A transport firewall does not route data, and does thus not have IP addresses on its ports. It can have one IP address, but this is used only for management purposes.

Objectives

The objectives of this challenge are to:

- Define auto-update parameters.
- Define an static ARP entry.
- Enable ARP inspection.

Example

```
# config t
pixfirewall(config)# auto-update ?

configure mode commands/options:
  device-id      Specify the device ID reported to the Auto Update Server
  poll-period    Specify how often to poll the Auto Update Server
  server         Specify the URL of the Auto Update Server
  timeout        Specify maximum wait to contact the Auto Update Server
pixfirewall(config)# auto-update device-id ?

configure mode commands/options:
  hardware-serial Hardware serial number
  hostname        Host name
  ipaddress       IP address of the specified interface
  mac-address     MAC address of the specified interface
  string          Text string
pixfirewall(config)# auto-update device-id hostname
pixfirewall(config)# auto-update poll-period ?
```

```

configure mode commands/options:
  <1-35791> Period in minutes between poll updates
pixfirewall(config)# auto-update poll-period 10
pixfirewall(config)# auto-update server ?

configure mode commands/options:
  WORD < 450 char URL of the auto update server
pixfirewall(config)# auto-update server http://user:password@1.2.3.4:8080/update ?

configure mode commands/options:
  verify-certificate Verify the Auto Update Server certificate
  <cr>
pixfirewall(config)# auto-update server http://user:password@1.2.3.4:8080/update
pixfirewall(config)# auto-update timeout ?

configure mode commands/options:
  <1-35791> Timeout in minutes to contact server
pixfirewall(config)# auto-update timeout 10

pixfirewall(config)# firewall transparent

pixfirewall(config)# ip address 1.2.3.4 255.255.255.0

pixfirewall(config)# arp-inspection ?

configure mode commands/options:
Current available interface(s):
  Inf2      Name of interface Ethernet2
  Inside    Name of interface Ethernet1
  Outside   Name of interface Ethernet0

pixfirewall(config)# arp-inspection outside ?

configure mode commands/options:
  enable Enable arp inspection

pixfirewall(config)# arp-inspection outside enable ?

configure mode commands/options:
  flood      Flood arp requests
  no-flood   Do not flood arp requests
  <cr>
pixfirewall(config)# arp-inspection outside enable no-flood

pixfirewall(config)# arp ?

configure mode commands/options:
  timeout Configure ARP timeout value
Current available interface(s):
  inside Name of interface Ethernet1
  outside Name of interface Ethernet0

pixfirewall(config)# arp inside ?

configure mode commands/options:
  Hostname or A.B.C.D IP address for an ARP table entry
pixfirewall(config)# arp inside 1.2.3.4 ?

configure mode commands/options:
  H.H.H Hardware MAC address
pixfirewall(config)# arp inside 1.2.3.4 1.1.1 ?

```

```
configure mode commands/options:
  alias Don't expire this ARP entry after timeout
  <cr>
```

```
pixfirewall(config)# mac-address-table ?
```

```
configure mode commands/options:
  aging-time Configure duration that a bridge entry will remain in the table,
              default is 5 minutes
  static      Add static entries to the table
```

```
pixfirewall(config)# mac-address-table aging-time ?
```

```
configure mode commands/options:
  <5-720> Aging interval in minutes
```

```
pixfirewall(config)# mac-address-table aging-time 10
```

```
pixfirewall(config)# mac-address-table static ?
```

```
configure mode commands/options:
Current available interface(s):
  $E2.NAME$\tName of interface Ethernet2
  $E1.NAME$\tName of interface Ethernet1
  $E0.NAME$\tName of interface Ethernet0
```

```
pixfirewall(config)# mac-address-table static 1.1.1 ?
```

```
configure mode commands/options:
  H.H.H MAC address
```

```
pixfirewall(config)# mac-address-table static 1.1.1 0.0.0 ?
```

```
configure mode commands/options:
  <cr>
```

Cisco PIX Challenge 79

Outline

In most applications, the firewall keeps a table of the known MAC addresses on each of its interfaces. It uses this to route packets to the correct node on the network. In order to guard against MAC address spoofing, automatically learning of MAC addresses can be switched off, and MAC addresses can be statically added, for all valid nodes.

NOTE: A transport firewall does not route data, and does thus not have IP addresses on its ports. It can have one IP address, but this is used only for management purposes.

Objectives

The objectives of this challenge are to:

- Define MAC addresses of the MAC address table.

- Disable MAC address learning.

Example

```

# config t
pixfirewall(config)# firewall transparent

pixfirewall(config)# ip address 1.2.3.4 255.255.255.0

pixfirewall(config)# mac-address-table ?

configure mode commands/options:
  aging-time  Configure duration that a bridge entry will remain in the table,
               default is 5 minutes
  static      Add static entries to the table

pixfirewall(config)# mac-address-table a ?

configure mode commands/options:
  <5-720>     Aging interval in minutes

pixfirewall(config)# mac-address-table static ?

configure mode commands/options:
Current available interface(s):
  Inf2        Name of interface Ethernet2
  Inside      Name of interface Ethernet1
  Outside     Name of interface Ethernet0

pixfirewall(config)# mac-address-table static outside ?

configure mode commands/options:
  H.H.H       MAC address

pixfirewall(config)# mac-address-table static outside 1.1.1

pixfirewall(config)# mac-learn ?

configure mode commands/options:
Current available interface(s):
  Inf2        Name of interface Ethernet2
  Inside      Name of interface Ethernet1
  Outside     Name of interface Ethernet0

pixfirewall(config)# mac-learn outside ?

configure mode commands/options:
  disable     Disable mac learning on the interface

pixfirewall(config)# mac-learn outside disable

```

Cisco PIX Challenge 80

Outline

Some application protocols require the firewall to inspect the operation, as new ports may be open in their usage. The firewall must thus open these to make the protocol work.

CTIQBE inspection supports the Cisco IP SoftwarePhone and other Cisco TAPI applications with Cisco CallManager. These are used in many Voice-over-IP applications.

Objectives

The objectives of this challenge are to:

- Define interesting CTIQBE traffic.
- Define a policy map.
- Define CTIQBE inspection.
- Apply the policy map.

Example

```
# config t
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match port tcp eq ?
```

```
mpf-class-map mode commands/options:
<0-65535>      Enter port number (0 - 65535)
aol
bgp
chargen
cifs
citrix-ica
cmd
ctiqbe
daytime
discard
domain
echo
exec
finger
ftp
ftp-data
gopher
h323
hostname
http
https
ident
imap4
irc
kerberos
klogin
kshell
ldap
ldaps
login
lotusnotes
lpd
netbios-ssn
nntp
pcanywhere-data
pim-auto-rp
pop2
pop3
```

```
pptp
rsh
rtsp
sip
smtp
sqlnet
ssh
sunrpc
tacacs
talk
telnet
uucp
whois
www
```

```
pixfirewall(config-cmap)# match port tcp eq 2748
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect ?
```

mpf-policy-map-class mode commands/options:

```
ctiqbe
dns
esmtpt
ftp
gtp
h323
http
icmp
ils
mgcp
netbios
pptp
rsh
rtsp
sip
skinny
snmp
sqlnet
sunrpc
tftp
xdmcp
pixfirewall(config-pmap-c)# inspect ctiqbe
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest interface outside
```

Cisco PIX Challenge 81

Outline

DNS inspection guards against an incorrect return address used for a DNS query. This prevents a proxy DNS attack, where an attacker sends multiple requests to a DNS server with the return address of the machine that the attacker wishes to attack. The attacked machine then receives multiple DNS replies, which it must service, and is likely to reduce the performance of the machine.

Objectives

The objectives of this challenge are to:

- Define interesting DNS traffic (UDP port 53).
- Define a policy map.
- Define DNS inspection.
- Apply the policy map.

Example

```
# config t
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match port udp eq 53
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect dns ?

mpf-policy-map-class mode commands/options:
  maximum-length Maximum DNS packet length
  <cr>
pixfirewall(config-pmap-c)# inspect dns max-length ?

mpf-policy-map-class mode commands/options:
  <512-65535> Enter maximum DNS packet length
pixfirewall(config-pmap-c)# inspect dns max 1500
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest interface outside
```

Cisco PIX Challenge 82

Outline

FTP inspection allows the firewall to setup the data connection, and tracks the FTP command responses for possibly invalid commands. It can also create an audit trail and embedded NAT information in the IP address. The **strict** part of the inspection command applies FTP restrictions from an FTP map.

Objectives

The objectives of this challenge are to:

- Define interesting FTP traffic (TCP port 21).
- Define an FTP map.
- Define a policy map.
- Define FTP inspection.

- Apply the policy map.

Example

```

# config t
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match port tcp eq 21
pixfirewall(config-cmap)# exit
pixfirewall(config)# ftp-map ftest
pixfirewall(config-ftp-map)# ?

Ftp-map configuration commands:
  mask-syst-reply  Mask reply to syst command
  no               Negate a command or set its defaults
  request-command FTP request command inspection
pixfirewall(config-ftp-map)# request-command ?

ftp-map mode commands/options:
  deny Specify FTP request commands to block

pixfirewall(config-ftp-map)# request-command deny ?

ftp-map mode commands/options:
  appe Append to a file
  cdup Change to parent of current directory
  dele Delete a file at server site
  get  FTP client command for the retr command - retrieve a file
  help Help information from server
  mkd  Create a directory
  put  FTP client command for the stor command - store a file
  rmd  Remove a directory
  rnfr Rename from
  rnto Rename to
  site Specify server specific command
  stou Store a file with a unique name

pixfirewall(config-ftp-map)# request-command deny cdup

pixfirewall(config-ftp-map)# exit
pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect ftp ?

mpf-policy-map-class mode commands/options:
  strict Prevent web browsers from sending embedded commands
        in FTP requests
  <cr>
pixfirewall(config-pmap-c)# inspect ftp strict ?

mpf-policy-map-class mode commands/options:
  WORD < 64 char Optional ftp-map name
  <cr>
pixfirewall(config-pmap-c)# inspect ftp strict ftest
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest interface outside

```

Cisco PIX Challenge 83

Outline

GTP allows data to be tunneled through a GSM network (UMTS/GPRS). GTP inspection allows the firewall to check the details of these connections.

Objectives

The objectives of this challenge are to:

- Define interesting GTP traffic (UDP ports 3386 and 2123).
- Define a GTP map.
- Define a policy map.
- Define GTP inspection.
- Apply the policy map.

Note: An access-list is required in this case, instead of a match command in the class-map, as there are more than one protocol. Only the tunnel-group allows to match more than one protocol. Thus we need an access-list to identify ports 2123 and 3386.

Example

```
# config t
pixfirewall(config)# access-list atest permit udp any any eq 2123
pixfirewall(config)# access-list atest permit udp any any eq 3386

pixfirewall(config)# class-map ctest

pixfirewall(config-cmap)# match ?

mpf-class-map mode commands/options:
access-list          Match an Access List
any                  Match any packet
default-inspection-traffic Match default inspection traffic:
ctiqbe----tcp--2748   dns-----udp--53
ftp-----tcp--21      gtp-----udp--2123,3386
h323-h225-tcp--1720   h323-ras--udp--1718-1719
http-----tcp--80    icmp-----icmp
ils-----tcp--389    mgcp-----udp--2427,2727
netbios---udp--137-138  rpc-----udp--111
rsh-----tcp--514    rtsp-----tcp--554
sip-----tcp--5060    sip-----udp--5060
skinny---tcp--2000    smtp-----tcp--25
sqlnet---tcp--1521    tftp-----udp--69
xdmcp-----udp--177

dscp                 Match IP DSCP (DiffServ CodePoints)
flow                 Flow based Policy
port                 Match TCP/UDP port(s)
precedence           Match IP precedence
rtp                  Match RTP port numbers
tunnel-group         Match a Tunnel Group
pixfirewall(config-cmap)# match access-list ?
```

```

mpf-class-map mode commands/options:
  WORD Access List name
pixfirewall(config-cmap)# match access-list atest
pixfirewall(config-cmap)# exit
pixfirewall(config)# gtp-map gtest
pixfirewall(config-gtp-map)# ?

description      GRP configuration map description
drop             Message ID, APN or GTP version to drop
help            Displays help
mcc             Three-digit mobile code (000-999)
message-length  Message length max and min values
permit errors   Permits packets with errors
permit response Permit GSN loading balance
request-queue   Maximum requests for the queue
timeout         Idle timeout
tunnel-limit    Maximum number of tunnels
pixfirewall(config-gtp-map)# request-queue 100
pixfirewall(config-gtp-map)# mcc 044
pixfirewall(config-gtp-map)# message-length min 10 max 1000
pixfirewall(config-gtp-map)# tunnel-limit 10000
pixfirewall(config-gtp-map)# exit
pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect gtp gtest
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest interface outside

```

Cisco PIX Challenge 84

Outline

H.323 is a wide ranging protocol suite which supports many types of video and voice communications.

Objectives

The objectives of this challenge are to:

- Define interesting H.323 traffic (UDP ports 1720 and 1720).
- Define a policy map.
- Define H.323 inspection.
- Apply the policy map.

Note: An access-list is required in this case, instead of a match command in the class-map, as there are more than one protocol. Only the tunnel-group allows to match more than one protocol. Thus we need an access-list to identify ports 2123 and 3386.

Example

```
# config t
```

```

pixfirewall(config)# access-list atest permit udp any any eq 1720
pixfirewall(config)# access-list atest permit udp any any eq 1721

pixfirewall(config)# class-map ctest

pixfirewall(config-cmap)# match ?

mpf-class-map mode commands/options:
  access-list          Match an Access List
  any                  Match any packet
  default-inspection-traffic Match default inspection traffic:
    ctigbe----tcp--2748      dns-----udp--53
    ftp-----tcp--21        gtp-----udp--2123,3386
    h323-h225-tcp--1720      h323-ras--udp--1718-1719
    http-----tcp--80       icmp-----icmp
    ils-----tcp--389       mgcp-----udp--2427,2727
    netbios---udp--137-138   rpc-----udp--111
    rsh-----tcp--514       rtsp-----tcp--554
    sip-----tcp--5060      sip-----udp--5060
    skinny---tcp--2000       smtp-----tcp--25
    sqlnet----tcp--1521     tftp-----udp--69
    xdmcp-----udp--177

  dscp                 Match IP DSCP (DiffServ CodePoints)
  flow                 Flow based Policy
  port                 Match TCP/UDP port(s)
  precedence           Match IP precedence
  rtp                  Match RTP port numbers
  tunnel-group         Match a Tunnel Group
pixfirewall(config-cmap)# match access-list ?

mpf-class-map mode commands/options:
  WORD Access List name
pixfirewall(config-cmap)# match access-list atest
pixfirewall(config-cmap)# exit
pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect h323 ?

mpf-policy-map-class mode commands/options:
  h225 Enable H.225 signalling inspection
  ras Enable RAS inspection
pixfirewall(config-pmap-c)# inspect h323 ras
pixfirewall(config-pmap-c)# inspect h323 h225
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest interface outside

```

Cisco PIX Challenge 85

Outline

HTTP inspection allows the firewall to detect possible malisousness in the HTTP protocol.

Objectives

The objectives of this challenge are to:

- Define a policy map.
- Define HTTP inspection.
- Apply the policy map.

Example

```
# config t

pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match tcp port eq 80
pixfirewall(config-cmap)# exit
pixfirewall(config)# http-map htest

pixfirewall(config-http-map)# ?

Http-map configuration commands:
  content-length           Content length range inspection
  content-type-verification Content type inspection
  max-header-length       Maximum header size inspection
  max-uri-length          Maximum URI size inspection
  no                       Negate a command or set its defaults
  port-misuse             Application inspection
  request-method          Request method inspection
  strict-http             Strict HTTP inspection
  transfer-encoding       Transfer encoding inspection

pixfirewall(config-http-map)# content-l ?

http-map mode commands/options:
  max Maximum content length allowed
  min Minimum content length allowed
pixfirewall(config-http-map)# content-l min ?

http-map mode commands/options:
<1-65535> Number of bytes
pixfirewall(config-http-map)# content-l min 1 ?

http-map mode commands/options:
  action Action taken when a violation occurs
  max     Maximum content length allowed
pixfirewall(config-http-map)# content-l min 1 max ?

http-map mode commands/options:
<1-50000000> Number of bytes
pixfirewall(config-http-map)# content-l min 1 max 1000 ?

http-map mode commands/options:
  action Action taken when a violation occurs
pixfirewall(config-http-map)# content-l min 1 max 1000 action ?

http-map mode commands/options:
  allow Allow the message
  drop  Close the connection
  reset Close the connection with a TCP reset message
pixfirewall(config-http-map)# content-l min 10 max 1000 action reset

pixfirewall(config-http-map)# content-type-verification ?

http-map mode commands/options:
```

```

    action          Action taken when a violation occurs
    match-req-rsp   Check response matches ACCEPT value in request message
pixfirewall(config-http-map)# content-type-verification match ?

http-map mode commands/options:
    action          Action taken when a violation occurs
pixfirewall(config-http-map)# content-type-verification match action ?

http-map mode commands/options:
    allow          Allow the message
    drop           Close the connection
    reset          Close the connection with a TCP reset message

pixfirewall(config-http-map)# content-type-verification match action reset ?

http-map mode commands/options:
    log            Generate a log message
    <cr>
pixfirewall(config-http-map)# content-type-verification match action reset log ?

http-map mode commands/options:
    <cr>
pixfirewall(config-http-map)# content-type-verification match action reset log

pixfirewall(config-http-map)# max-header-length request 100 action reset log
pixfirewall(config-http-map)# max-uri 100 action reset log

pixfirewall(config-http-map)# exit
pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect http htest
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest interface outside

```

1 TCP/IP services reference

<i>Port</i>	<i>Service</i>	<i>Comment</i>	<i>Port</i>	<i>Service</i>	<i>Comment</i>
1	TCPmux		7	echo	
9	discard	Null	11	systat	Users
13	daytime		15	netstat	
17	qotd	Quote	18	mtp	Message send protocol
19	chargen	ttytst source	21	ftp	
23	telnet		25	smtp	Mail
37	time	Timserver	39	rlp	Resource location
42	nameserver	IEN 116	43	whois	Nickname
53	domain	DNS	57	mtp	Deprecated
67	bootps	BOOTP server	67	bootps	
68	bootpc	BOOTP client	69	tftp	
70	gopher	Internet Gopher	77	rje	Netrjs
79	finger		80	www	WWW HTTP
87	link	Ttylink	88	kerberos	Kerberos v5
95	supdup		101	hostnames	
102	iso-tsap	ISODE	105	csnet-ns	CSO name server
107	rtelnet	Remote Telnet	109	pop2	POP version 2
110	pop3	POP version 3	111	sunrpc	
113	auth	Rap ID	115	sftp	
117	uucp-path		119	nntp	USENET
123	ntp	Network Time	137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS	139	netbios-ssn	NETBIOS session
143	imap2		161	snmp	SNMP
162	snmp-trap	SNMP trap	163	cmip-man	ISO management over IP
164	cmip-agent		177	xdmcp	X Display Manager
178	nextstep	NeXTStep	179	bgp	BGP
191	prospero		194	irc	Internet Relay Chat
199	smux	SNMP Multiplexer	201	at-rtmp	AppleTalk routing
202	at-nbp	AppleTalk name binding	204	at-echo	AppleTalk echo
206	at-zis	AppleTalk zone information	210	z3950	NISO Z39.50 database
213	ipx	IPX	220	imap3	Interactive Mail Access
372	ulistserv	UNIX Listserv	512	exec	Comsat 513 login
513	who	Whod	514	shell	No passwords used
514	syslog		515	printer	Line printer spooler
517	talk		518	ntalk	
520	route	RIP	525	timed	Timeserver
526	tempo	Newdate	530	courier	Rpc
531	conference	Chat	532	netnews	Readnews

Cisco PIX Challenge 86

Outline

MGCP is a protocol which uses media gateways to provide trunks for the transmission of audio from telephone exchanges over the Internet. This challenge involves defining MGCP inspection.

Objectives

The objectives of this challenge are to:

- Define interesting traffic (normally UDP ports 2427 and 2727).
- Define a policy map.
- Define MGCP inspection.
- Apply the policy map.

Example

```
# config t

# config t
pixfirewall(config)# access-list atest permit udp any any eq 2427
pixfirewall(config)# access-list atest permit udp any any eq 2727
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list atest
pixfirewall(config-cmap)# exit
pixfirewall(config)# mgcp-map mtest
pixfirewall(config-mgcp-map) # ?
mgcp-map configuration commands:
  call-agent      Add a Call-Agent
  command-queue  Configure Command Queue
  gateway         Add a Gateway
  help           Help for mgcp-map configuration commands
  no             Negate or set default values of a command

pixfirewall(config-mgcp-map)# call-agent ?

mgcp-map mode commands/options:
  A.B.C.D IP address
pixfirewall(config-mgcp-map)# call-agent 1.2.3.4 ?

mgcp-map mode commands/options:
  <0-2147483647> ID of the group
pixfirewall(config-mgcp-map)# call-agent 1.2.3.4 111

pixfirewall(config-mgcp-map)# command-limit ?

mgcp-map mode commands/options:
  <1-2147483647> Command limit

pixfirewall(config-mgcp-map)# command-limit 100

pixfirewall(config-mgcp-map)# gateway ?

mgcp-map mode commands/options:
  A.B.C.D IP address
pixfirewall(config-mgcp-map)# gateway 1.2.3.5 111

pixfirewall(config-mgcp-map)# exit
pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect mgcp mtest
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest global
```

Cisco PIX Challenge 87

Outline

RTSP is used in streaming audio and video applications, such as for RealPlayer.

Objectives

The objectives of this challenge are to:

- Define interesting traffic (normally UDP ports 554 and 8554).
- Define a policy map.
- Define RTSP inspection.
- Apply the policy map.

Example

```
# config t
pixfirewall(config)# access-list atest permit tcp any any eq 554
pixfirewall(config)# access-list atest permit tcp any any eq 8554
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list atest
pixfirewall(config-cmap)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect rtsp
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest global
```

Cisco PIX Challenge 88

Outline

SIP is used for voice-over-IP applications. This challenge involves SIP inspections.

Objectives

The objectives of this challenge are to:

- Define interesting traffic (normally TCP port 5060).
- Define a policy map.
- Define SIP inspection.

- Apply the policy map.
- Define SIP timeout.

Example

```

# config t
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match port tcp eq 5060
pixfirewall(config-cmap)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect sip
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest global

pixfirewall(config)# timeout ?

configure mode commands/options:
  conn          Configure idle time after which a TCP connection state
                will be closed, default is 1:00:00
  h225          Configure idle time after which an H.225 signaling conn
                will be closed, default is 1:00:00
  h323          Configure idle time after which an H.323 control connection
                will be closed, default is 0:05:00
  half-closed  Configure idle time after which a TCP half-closed connection
                will be freed, default is 0:10:00
  icmp         Configure idle timeout for ICMP, default is 0:00:02
  mgcp         Configure idle time after which an MGCP media connection
                will be closed, default is 0:05:00
  mgcp-pat     Configure the time after which an MGCP PAT Xlate
                will be removed, default is 0:05:00
  sip          Configure idle time after which a SIP control connection
                will be closed, default is 0:30:00
  sip_media    Configure idle time after which a SIP Media connection
                will be closed, default is 0:02:00
  sunrpc       Configure idle time after which a SUNRPC slot
                will be closed, default is 0:10:00
  uauth        Configure idle time after which an authentication will no
                longer be cached and the user will need to re-authenticate on
                their connection, default is 0:05:00. The default uauth timer
                is absolute.
  udp          Configure idle time after which general UDP states
                will be closed, default is 0:02:00, This timer does not
                apply to DNS or SUNRPC
  xlate        Configure idle time after which a dynamic address
                will be returned to the free pool, default is 3:00:00

pixfirewall(config)# timeout sip ?

configure mode commands/options:
  0:0:0 | <0:5:0> - <1192:59:59> Idle time after which a SIP control
                                connection will be closed, default is 0:30:00
  <0-0>                               Specify this value to never time out

pixfirewall(config)# timeout sip 0:15:00

```

Also:

```
pixfirewall(config)# timeo sip_media ?
```

```
configure mode commands/options:
```

```
0:0:0 | <0:1:0> - <1192:59:59> Idle time after which a SIP Media connection  
will be closed, default is 0:02:00  
<0-0> Specify this value to never time out
```

Cisco PIX Challenge 89

Outline

SCCP (Skinny) is a simple protocol using in voice-over-IP applications. This challenge involves SCCP inspections.

Objectives

The objectives of this challenge are to:

- Define interesting traffic (normally TCP port 2000).
- Define a policy map.
- Define SCCP inspection.
- Apply the policy map.

Example

```
# config t  
pixfirewall(config)# class-map ctest  
pixfirewall(config-cmap)# match port tcp eq 2000  
pixfirewall(config-cmap)# exit  
  
pixfirewall(config)# policy-map ptest  
pixfirewall(config-pmap)# class ctest  
pixfirewall(config-pmap-c)# inspect skinny  
pixfirewall(config-pmap-c)# exit  
pixfirewall(config-pmap)# exit  
pixfirewall(config)# service-policy ptest global
```

Cisco PIX Challenge 90

Outline

SMTP is used to send email from a client to an SMTP server. It can be the source of attack, such as sending incorrectly formatted SMTP commands. Example commands are DATA, HELO, MAIL, SEND, and so on. SMTP inspection allows the firewall to check for incorrectly formatted SMTP messages. This includes:

- Limiting to seven basic SMTP commands, plus the eight extended ones.
- Monitoring the command-response phase, so that messages are not sent out-of-sequence.
- Catches truncated commands.
- Catches commands without a carriage-return/line-feed sequence.
- And so on.

Objectives

The objectives of this challenge are to:

- Define interesting traffic (normally TCP port 25).
- Define a policy map.
- Define SMTP inspection.
- Apply the policy map.

Example

```
# config t
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match port tcp eq 25
pixfirewall(config-cmap)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect esmtp
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest global
```

2 TCP/IP services reference

<i>Port</i>	<i>Service</i>	<i>Comment</i>	<i>Port</i>	<i>Service</i>	<i>Comment</i>
1	TCPmux		7	echo	
9	discard	Null	11	systat	Users
13	daytime		15	netstat	
17	qotd	Quote	18	misp	Message send protocol
19	chargen	ttytst source	21	ftp	
23	telnet		25 smtp	Mail	
37	time	Timserver	39	rlp	Resource location
42	nameserver	IEN 116	43	whois	Nickname
53	domain	DNS	57	mtp	Deprecated
67	bootps	BOOTP server	67	bootps	
68	bootpc	BOOTP client	69	tftp	
70	gopher	Internet Gopher	77	rje	Netrjs
79	finger		80	www	WWW HTTP
87	link	Ttylink	88	kerberos	Kerberos v5
95	supdup		101	hostnames	
102	iso-tsap	ISODE	105	csnet-ns	CSO name server
107	rtelnet	Remote Telnet	109	pop2	POP version 2
110	pop3	POP version 3	111	sunrpc	
113	auth	Rap ID	115	sftp	
117	uucp-path		119	nntp	USENET
123	ntp	Network Time	137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS	139	netbios-ssn	NETBIOS session
143	imap2		161	snmp	SNMP
162	snmp-trap	SNMP trap	163	cmip-man	ISO management over IP
164	cmip-agent		177	xdmcp	X Display Manager
178	nextstep	NeXTStep	179	bgp	BGP
191	prospero		194	irc	Internet Relay Chat
199	smux	SNMP Multiplexer	201	at-rtmp	AppleTalk routing
202	at-nbp	AppleTalk name binding	204	at-echo	AppleTalk echo
206	at-zis	AppleTalk zone information	210	z3950	NISO Z39.50 database
213	ipx	IPX	220	imap3	Interactive Mail Access
372	ulistserv	UNIX Listserv	512	exec	Comsat 513 login
513	who	Whod	514	shell	No passwords used
514	syslog		515	printer	Line printer spooler
517	talk		518	ntalk	
520	route	RIP	525	timed	Timeserver
526	tempo	Newdate	530	courier	Rpc
531	conference	Chat	532	netnews	Readnews

Cisco PIX Challenge 91

Outline

SNMP is used to gain information from networked devices. Unfortunately there are security problems with early versions of it, where plain text values for the access parameters are sent over the network. In this example SNMP Version 1 is blocked by the firewall.

Objectives

The objectives of this challenge are to:

- Define interesting traffic (normally TCP port 161 and 162).
- Define an SNMP map.
- Define a policy map.
- Define SNMP inspection.
- Apply the policy map.

Example

```
# config t
pixfirewall(config)# access-list atest permit tcp any any eq 161
pixfirewall(config)# access-list atest permit tcp any any eq 162
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match access-list atest
pixfirewall(config-cmap)# exit

pixfirewall(config)# snmp-map stest
pixfirewall(config-snmp-map)# ?

snmp-map configuration commands:
 deny Deny SNMP traffic
 help Help for snmp-map configuration commands
 no Negate or set default values of a command

pixfirewall(config-snmp-map)# deny ?

snmp-map mode commands/options:
 version Specify the version to deny

pixfirewall(config-snmp-map)# deny version ?

snmp-map mode commands/options:
 1 SNMP version 1
 2 SNMP version 2 (party based)
 2c SNMP version 2c (community based)
 3 SNMP version 3
pixfirewall(config-snmp-map)# deny version ?
pixfirewall(config-snmp-map)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect snmp stest
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest global
```

3 TCP/IP services reference

<i>Port</i>	<i>Service</i>	<i>Comment</i>	<i>Port</i>	<i>Service</i>	<i>Comment</i>
1	TCPmux		7	echo	
9	discard	Null	11	systat	Users
13	daytime		15	netstat	
17	qotd	Quote	18	mtp	Message send protocol
19	chargen	ttytst source	21	ftp	
23	telnet		25	smtp	Mail
37	time	Timserver	39	rlp	Resource location
42	nameserver	IEN 116	43	whois	Nickname
53	domain	DNS	57	mtp	Deprecated
67	bootps	BOOTP server	67	bootps	
68	bootpc	BOOTP client	69	tftp	
70	gopher	Internet Gopher	77	rje	Netrjs
79	finger		80	www	WWW HTTP
87	link	Ttylink	88	kerberos	Kerberos v5
95	supdup		101	hostnames	
102	iso-tsap	ISODE	105	csnet-ns	CSO name server
107	rtelnet	Remote Telnet	109	pop2	POP version 2
110	pop3	POP version 3	111	sunrpc	
113	auth	Rap ID	115	sftp	
117	uucp-path		119	nntp	USENET
123	ntp	Network Time	137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS	139	netbios-ssn	NETBIOS session
143	imap2		161	snmp	SNMP
162	snmp-trap	SNMP trap	163	cmip-man	ISO management over IP
164	cmip-agent		177	xdmcp	X Display Manager
178	nextstep	NeXTStep	179	bgp	BGP
191	prospero		194	irc	Internet Relay Chat
199	smux	SNMP Multiplexer	201	at-rtmp	AppleTalk routing
202	at-nbp	AppleTalk name binding	204	at-echo	AppleTalk echo
206	at-zis	AppleTalk zone information	210	z3950	NISO Z39.50 database
213	ipx	IPX	220	imap3	Interactive Mail Access
372	ulistserv	UNIX Listserv	512	exec	Comsat 513 login
513	who	Whod	514	shell	No passwords used
514	syslog		515	printer	Line printer spooler
517	talk		518	ntalk	
520	route	RIP	525	timed	Timeserver
526	tempo	Newdate	530	courier	Rpc
531	conference	Chat	532	netnews	Readnews

Cisco PIX Challenge 92

Outline

RPC is used mainly in UNIX-based systems to remotely invoke services on servers, such as for file access, and so on. It uses NFS (for file services) and NIS (for domain control). When a client requires a service it sends an RPC program number over TCP port 111. On RPC interception, the firewall intercepts the connection, and checks the details.

Objectives

The objectives of this challenge are to:

- Define interesting traffic (normally TCP port 111).
- Define a policy map.
- Define RPC inspection.
- Apply the policy map.
- Define an Sun RPC table.

Example

```
# config t
pixfirewall(config)# class-map ctest
pixfirewall(config-cmap)# match port tcp eq 111
pixfirewall(config-cmap)# exit

pixfirewall(config)# policy-map ptest
pixfirewall(config-pmap)# class ctest
pixfirewall(config-pmap-c)# inspect rpc
pixfirewall(config-pmap-c)# exit
pixfirewall(config-pmap)# exit
pixfirewall(config)# service-policy ptest global
```

The firewall can create an RPC services table to control Sun RPC traffic through the security appliance with:

```
pixfirewall(config)# sunrpc ?

configure mode commands/options:
Current available interface(s):
  Inf2      Name of interface Ethernet2
  Inside   Name of interface Ethernet1
  Outside  Name of interface Ethernet0

pixfirewall(config)# sunrpc inside ?

configure mode commands/options:
  Hostname or A.B.C.D  IP address of SUNRPC server

pixfirewall(config)# sunrpc inside 1.2.3.4 ?

configure mode commands/options:
  A.B.C.D  The network mask to be applied to IP address

pixfirewall(config)# sunrpc inside 1.2.3.4 255.255.255.0 ?

configure mode commands/options:
  service  Specify the SUNRPC service program number after this keyword

pixfirewall(config)# sunrpc inside 1.2.3.4 255.255.255.0 service ?

configure mode commands/options:
  <0-2147483647>  SUNRPC service program number
```

```

pixfirewall(config)# sunrpc inside 1.2.3.4 255.255.255.0 service 100004 ?

configure mode commands/options:
  protocol  SUNRPC transport protocol to be used

pixfirewall(config)# sunrpc inside 1.2.3.4 255.255.255.0 service 100004 p ?

configure mode commands/options:
  tcp  TCP to be used as transport protocol
  udp  UDP to be used as transport protocol

pixfirewall(config)# sunrpc inside 1.2.3.4 255.255.255.0 service 100004 p t ?

configure mode commands/options:
  port  Configure SUNRPC port range after this keyword

pixfirewall(config)# sunrpc inside 1.2.3.4 255.255.255.0 service 100004 p t p ?

configure mode commands/options:
  highs      Keyword indicating port range 1024-65535
  lows       Keyword indicating port range 1-1023
Enter the port or port range <start>[-<end>]
aol
bgp
chargen
cifs
citrix-ica
cmd
ctiqbe
daytime
discard
domain
echo
exec
finger
ftp
ftp-data
gopher
h323
hostname
http
https
ident
imap4
irc
kerberos
klogin
kshell
ldap
ldaps
login
lotusnotes
lpd
netbios-ssn
nntp
pcanywhere-data
pim-auto-rp
pop2
pop3
pftp
rsh
rtsp
sip

```

```
smtp
sqlnet
ssh
sunrpc
tacacs
talk
telnet
uucp
whois
www
<start>[-<end>]    Enter a specific port (0-65535) or a range of ports

pixfirewall(config)# sunrpc inside 1.2.3.4 255.255.255.0 service 100004 protocol
tcp port 111
```

4 TCP/IP services reference

<i>Port</i>	<i>Service</i>	<i>Comment</i>	<i>Port</i>	<i>Service</i>	<i>Comment</i>
1	TCPmux		7	echo	
9	discard	Null	11	systat	Users
13	daytime		15	netstat	
17	qotd	Quote	18	mtp	Message send protocol
19	chargen	ttytst source	21	ftp	
23	telnet		25	smtp	Mail
37	time	Timserver	39	rlp	Resource location
42	nameserver	IEN 116	43	whois	Nickname
53	domain	DNS	57	mtp	Deprecated
67	bootps	BOOTP server	67	bootps	
68	bootpc	BOOTP client	69	tftp	
70	gopher	Internet Gopher	77	rje	Netrjs
79	finger		80	www	WWW HTTP
87	link	Ttylink	88	kerberos	Kerberos v5
95	supdup		101	hostnames	
102	iso-tsap	ISODE	105	csnet-ns	CSO name server
107	rtelnet	Remote Telnet	109	pop2	POP version 2
110	pop3	POP version 3	111	sunrpc	
113	auth	Rap ID	115	sftp	
117	uucp-path		119	nntp	USENET
123	ntp	Network Time	137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS	139	netbios-ssn	NETBIOS session
143	imap2		161	snmp	SNMP
162	snmp-trap	SNMP trap	163	cmip-man	ISO management over IP
164	cmip-agent		177	xdmcp	X Display Manager
178	nextstep	NeXTStep	179	bgp	BGP
191	prospero		194	irc	Internet Relay Chat
199	smux	SNMP Multiplexer	201	at-rtmp	AppleTalk routing
202	at-nbp	AppleTalk name binding	204	at-echo	AppleTalk echo
206	at-zis	AppleTalk zone information	210	z3950	NISO Z39.50 database
213	ipx	IPX	220	imap3	Interactive Mail Access
372	ulistserv	UNIX Listserv	512	exec	Comsat 513 login
513	who	Whod	514	shell	No passwords used
514	syslog		515	printer	Line printer spooler
517	talk		518	ntalk	
520	route	RIP	525	timed	Timeserver
526	tempo	Newdate	530	courier	Rpc
531	conference	Chat	532	netnews	Readnews

Cisco PIX Challenge 93

Outline

This challenge involves redistributed OSPF processes from one to another.

Objectives

The objectives of this challenge are to:

- Define a route-map.
- Define redistribution.

Example

```

# config t
(config)# route-map ?

configure mode commands/options:
  WORD < 58 char  Route map tag

(config)# route-map rtest ?

configure mode commands/options:
  <0-65535> Sequence to insert to/delete from existing route-map entry
  deny      Route map denies set operations
  permit    Route map permits set operations
  <cr>

(config)# route-map rtest permit
(config-route-map)# ?

Route Map configuration commands:
  exit      Exit from route-map configuration mode
  help      Interactive help for route-map subcommands
  match     Match values from routing table
  no        Negate a command
  set       Set values in destination routing protocol

(config-route-map)# match ?

route-map mode commands/options:
  interface Match first hop interface of route
  ip         Match IP address or next-hop or route-source
  metric     Match metric of route
  route-type Match route-type of route

(config-route-map)# match metric ?

route-map mode commands/options:
  <0-4294967295> Metric value

(config-route-map)# match metric 1

(config-route-map)# set ?

route-map mode commands/options:
  metric     Set metric value for destination routing protocol
  metric-type Set type of metric for destination routing protocol

(config-route-map)# set metric- ?

route-map mode commands/options:
  type-1    OSPF external type 1 metric
  type-2    OSPF external type 2 metric

(config-route-map)# set metric- type-1

(config-route-map)# set metric ?

```

```

route-map mode commands/options:
  <0-4294967295> Metric value
(config-route-map)# set metric 5

(config)# router ospf 111
(config-router)# redistribute ?

router mode commands/options:
  connected Connected
  ospf       Open Shortest Path First (OSPF)
  static     Static routes
(config-router)# redistribute ospf 1 ?

router mode commands/options:
  match      Redistribution of OSPF routes
  metric     Metric for redistributed routes
  metric-type Set OSPF exterior metric type for redistributed routes
  route-map  Route map reference
  subnets   Consider subnets for redistribution into OSPF
  tag        Set tag for routes redistributed into OSPF
  <cr>

(config-router)# redistribute ospf 1 route-map ?

router mode commands/options:
  WORD Pointer to route-map entries

(config-router)# redistribute ospf 1 route-map rtest ?

router mode commands/options:
  match      Redistribution of OSPF routes
  metric     Metric for redistributed routes
  metric-type Set OSPF exterior metric type for redistributed routes
  subnets   Consider subnets for redistribution into OSPF
  tag        Set tag for routes redistributed into OSPF
  <cr>
(config-router)# redistribute ospf 1 route-map rtest

```

Cisco PIX Challenge 94

Outline

This challenge involves configuring OSPF routing

Objectives

The objectives of this challenge are to:

- Define OSPF.
- Define E1 OSPF parameters.

Example

```

(config)# router ospf 111
(config-router)# network 10.0.0.0 255.0.0.0 area 0

```

```
(config-router)# exit
(config)# int e1
(config-if)# ospf cost 20
(config-if)# ospf retransmit-interval 20
(config-if)# ospf transmit-delay 20
(config-if)# ospf priority 20
(config-if)# ospf hello-interval 20
(config-if)# ospf dead-interval 20
(config-if)# ospf authentication-key test
(config-if)# ospf message-digest-key 1 md5 test
(config-if)# ospf authentication message-digest
```

Cisco PIX Challenge 95

Outline

This challenge involves configuring OSPF routing area details.

Objectives

The objectives of this challenge are to:

- Define OSPF.
- Define OSPF routing area details.
- Define OSPF stub details.
- Define route timers.
- Define default route.
- Define logging of neighbors.

Outline

```
(config)# router ospf 111
(config-router)# area 1 authentication
(config-router)# area 1 authentication message-digest
(config-router)# area 10 stub
(config-router)# area 10 default-cost 15
(config-router)# summary-address 1.2.3.0 255.255.0.0
(config-router)# area 10 range 2.3.4.0 255.255.0.0
(config-router)# default-information originate always
(config-router)# log-adj-changes detail
(config-router)# timers spf 10 10
```

Example

```
pixfirewall(config)# router ospf 111
pixfirewall(config-router)# ?
```

Router configuration commands:
area OSPF area parameters

compatible	OSPF compatibility list
default-information	Control distribution of default information
distance	Define an administrative distance
exit	Exit from router configuration mode
help	Interactive help for router subcommands
ignore	Do not complain about specific event
log-adj-changes	Log changes in adjacency state
neighbor	Specify a neighbor router
network	Add/remove interfaces to/from OSPF routing process
no	Negate a command
redistribute	Redistribute information from another routing process
router-id	router-id for this OSPF process
summary-address	Configure IP address summaries
timers	Adjust routing timers

pixfirewall(config-router)# area ?

router mode commands/options:

<0-4294967295> OSPF area ID as a decimal value
A.B.C.D OSPF area ID in IP address format

pixfirewall(config-router)# area 1 ?

router mode commands/options:

authentication Enable authentication
default-cost Set the summary default-cost of a NSSA/stub area
filter-list Filter networks between OSPF areas
nssa Specify a NSSA area
range Summarize routes matching address/mask (border routers only)
stub Specify a stub area
virtual-link Define a virtual link and its parameters
<cr>

pixfirewall(config-router)# area 1 authentication

pixfirewall(config-router)# area 1 authentication ?

router mode commands/options:

message-digest Use message-digest authentication
<cr>

pixfirewall(config-router)# area 1 authentication message-digest

pixfirewall(config-router)# area 10 stub

pixfirewall(config-router)# area 10 default-cost ?

router mode commands/options:

<0-65535> Stub's advertised external route metric

pixfirewall(config-router)# area 10 default-cost 15

Route summarization allows for various routes to be summarized into a single address, and help to reduce the size of the routing tables:

pixfirewall(config-router)# summary-address ?

router mode commands/options:

A.B.C.D IP summary address

pixfirewall(config-router)# summary-address 1.2.3.0 ?

router mode commands/options:

A.B.C.D Summary mask

pixfirewall(config-router)# summary-address 1.2.3.0 255.255.0.0

To summarize between OSPF areas:

```
pixfirewall(config-router)# area 10 range ?
```

```
router mode commands/options:  
  A.B.C.D IP address to match
```

```
pixfirewall(config-router)# area 10 range 2.3.4.0 ?
```

```
router mode commands/options:  
  A.B.C.D IP mask for address
```

```
pixfirewall(config-router)# area 10 range 2.3.4.0 255.255.0.0
```

To generate a default route:

```
pixfirewall(config-router)# default-information ?
```

```
router mode commands/options:  
  originate Distribute a default route
```

```
pixfirewall(config-router)# default-information originate ?
```

```
router mode commands/options:  
  always      Always advertise default route  
  metric      OSPF default metric  
  metric-type OSPF metric type for default routes  
  route-map   Route-map reference  
  <cr>
```

```
pixfirewall(config-router)# default-information originate always
```

```
pixfirewall(config-router)# log-adj-changes ?
```

```
router mode commands/options:  
  detail Log all state changes  
  <cr>
```

```
pixfirewall(config-router)# log-adj-changes detail
```

For OSPF timers:

```
pixfirewall(config-router)# timers ?
```

```
router mode commands/options:  
  lsa-group-pacing OSPF LSA group pacing timer  
  spf              OSPF SPF timers
```

```
pixfirewall(config-router)# timers spf ?
```

```
router mode commands/options:  
  <1-65535> Delay between receiving a change to SPF calculation
```

```
pixfirewall(config-router)# timers spf 10 ?
```

```
router mode commands/options:  
  <1-65535> Hold time between consecutive SPF calculations
```

```
pixfirewall(config-router)# timers spf 10 10
```

Cisco PIX Test

Outline

This challenge involves taking a PIX test.

Cisco PIX Challenge 97

Outline

This challenge involves configuring external access to an email server on the DMZ.

Objectives

The objectives of this challenge are to:

- Define fixup for SMTP.
- Define access-list to allow access to the email server.
- Define a static mapping between the email server and an outside address.
- Apply the access-list.
- Define MAC addresses for the ports (just in case they are used on other devices).

Example

In the following example, the addresses of the ports are:

E0 (outside) – 10.0.0.1

E1 (inside) – 192.168.0.1

E2 (dmz) – 172.16.10.1

The email server is at 172.16.10.2 and will be mapped to 10.0.0.3 for external access.

The default gateway is at 10.0.0.2

```
(config)# fixup protocol smtp 25
(config)# int e0
(config-if)# ip address 10.0.0.1 255.255.255.0
(config-if)# nameif outside
(config-if)# mac-address 1111.2222.3333
(config-if)# no shutdown
(config-if)# exit
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif inside
(config-if)# mac-address 2222.3333.4444
(config-if)# no shutdown
(config-if)# exit
```

```
(config)# int e2
(config-if)# ip address 172.16.10.1 255.255.255.0
(config-if)# nameif dmz
(config-if)# mac-address 3333.4444.5555
(config-if)# no shutdown
(config-if)# exit
```

Next permit access from the outside interface to the Email server:

```
(config)#access-list outside_int permit tcp any host 10.0.0.3 eq smtp
```

Allow all outgoing connections from the Email server to external nodes:

```
(config)# access-list dmz_interface permit tcp host 172.16.10.2 any eq smtp
```

Map the Email server on the DMZ, which is at 172.16.0.2, and let its accessible address be 10.0.0.3:

```
(config)# static (dmz,outside) 10.0.0.3 172.16.0.2
```

Apply the access-lists:

```
(config)# access-group outside_interface in interface outside
(config)# access-group dmz_interface in interface dmz
```