

# Cisco Academy Network Security 1

## Router Challenge 195

**Outline:** This challenge involves an analysis of SSH.

**Objectives:** The objectives of this challenge are to explain SSH.

The TELNET protocol is insecure as the text is passed as plain text. An improved method is to use SSH, which encrypts data. It requires that the domain-name and an RSA key pair:

```
# config t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# hostname ap
ap(config)# username fred password bert

ap(config)# ip domain-name test.com
ap(config)# crypto key generate rsa
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

ap # show crypto key mypubkey rsa
% Key pair was generated at: 00:39:47 UTC Mar 1 2002
Key name: ap.test.com
Usage: General Purpose Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CE28A6 6697D889
 D28C19FD 3587872D ED4834F0 707B1D8F 944F665E 084DA46B 9D9C0BF4 E992059A
 521A750B B9C09A7F E14275B9 AA29B962 BB0CCCAA 9FA30168 7B020301 0001
% Key pair was generated at: 00:39:56 UTC Mar 1 2002
Key name: ap.test.com.server
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D56417 15E52D1C
 26C2CE81 B264D2C0 9C52AD73 90731CF7 34D122BC 59CD560F 9600714C E8DB3AA8
 1D80B1E7 74E194B2 3F6C6EA8 8D1505DB 485AD29F A982AB04 950DD4CA ED113E5F
 78D60CFF 2B568C97 0CF21335 0DE55420 BD7929AE 763EDDB9 A1020301 0001

ap (config)# ip ssh ?
 authentication-retries Specify number of authentication retries
 break-string           break-string
 port                   Starting (or only) Port number to listen on
 rsa                    Configure RSA keypair name for SSH
 source-interface       Specify interface for source address in SSH
                        connections
 time-out               Specify SSH time-out interval
 version                Specify protocol version to be supported
ap (config)# ip ssh time-out ?
 <1-120> SSH time-out interval (secs)
ap (config)# ip ssh time-out 60
```

```

ap (config)# ip ssh authentication-retries ?
<0-5> Number of authentication retries
ap (config)# ip ssh authentication-retries 2
ap (config)# ip ssh version ?
<1-2> Protocol version
ap (config)# ip ssh version 2

ap (config)# line vty 0 4
ap (config-line)# transport ?
input      Define which protocols to use when connecting to the terminal
           server
output     Define which protocols to use for outgoing connections
preferred  Specify the preferred protocol to use
(config-line)# transport input ?
all        All protocols
mop        DEC MOP Remote Console Protocol
none       No protocols
pad        X.3 PAD
rlogin     Unix rlogin protocol
ssh        TCP/IP SSH protocol
telnet     TCP/IP Telnet protocol
udptn      UDPTN async via UDP protocol
v120       Async over ISDN
ap (config-line)# transport input ssh
ap (config-line)# login ?
local      Local password checking
tacacs     Use tacacs server for password checking
<cr>
ap (config-line)# login local

```

# Cisco Router Challenge 196

## Outline

This challenge involves the configuration of services on the router.

## Objectives

The objectives of this challenge are to:

- Define encrypted passwords.
- Define timestamps.
- Disable TCP small services.
- Disable UDP small services.
- Disable CDP on an interface.
- Disable ICMP on an interface.
- Disable SNMP.
- Restrict Web access.

## Example

```

> en
# config t
(config)# service ?
compress-config      Compress the configuration file
config               TFTP load config files
dhcp                 Enable DHCP server and relay agent
disable-ip-fast-frag Disable IP particle-based fast fragmentation
exec-callback        Enable exec callback
exec-wait            Delay EXEC startup on noisy lines
finger               Allow responses to finger requests
hide-telnet-addresses Hide destination addresses in telnet command
linenumber           enable line number banner for each exec
nagle                Enable Nagle's congestion control algorithm
old-slip-prompts     Allow old scripts to operate with slip/ppp
pad                  Enable PAD commands
password-encryption Encrypt system passwords
prompt              Enable mode specific prompt
pt-vty-logging       Log significant VTY-Async events
sequence-numbers     Stamp logger messages with a sequence number
slave-log            Enable log capability of slave IPs
tcp-keepalives-in    Generate keepalives on idle incoming network
                    connections
tcp-keepalives-out   Generate keepalives on idle outgoing network
                    connections
tcp-small-servers    Enable small TCP servers (e.g., ECHO)
telnet-zeroidle      Set TCP window 0 when connection is idle
timestamps           Timestamp debug/log messages
udp-small-servers    Enable small UDP servers (e.g., ECHO)
(config)# service timestamps ?
debug                Timestamp debug messages
log                  Timestamp log messages
<cr>
(config)# service timestamps log ?
datetime             Timestamp with date and time
uptime               Timestamp with system uptime
<cr>
(config)# service timestamps log datetime
(config)# sequence-numbers ?
compress-config      Compress the configuration file
config               TFTP load config files
dhcp                 Enable DHCP server and relay agent
disable-ip-fast-frag Disable IP particle-based fast fragmentation
exec-callback        Enable exec callback
exec-wait            Delay EXEC startup on noisy lines
finger               Allow responses to finger requests
hide-telnet-addresses Hide destination addresses in telnet command
linenumber           enable line number banner for each exec
nagle                Enable Nagle's congestion control algorithm
old-slip-prompts     Allow old scripts to operate with slip/ppp
pad                  Enable PAD commands
password-encryption Encrypt system passwords
prompt              Enable mode specific prompt
pt-vty-logging       Log significant VTY-Async events
sequence-numbers     Stamp logger messages with a sequence number
slave-log            Enable log capability of slave IPs
tcp-keepalives-in    Generate keepalives on idle incoming network
                    connections
tcp-keepalives-out   Generate keepalives on idle outgoing network
                    connections
tcp-small-servers    Enable small TCP servers (e.g., ECHO)
telnet-zeroidle      Set TCP window 0 when connection is idle
timestamps           Timestamp debug/log messages
udp-small-servers    Enable small UDP servers (e.g., ECHO)

```

```

(config)# service sequence-numbers
(config)# service dhcp
(config)# service finger

(config)# no service tcp-small-servers
(config)# no service udp-small-servers
(config)# service password-encryption

```

To disable ping on the interface:

```

(config)# int e0
(config-if)# no ip ?

```

Interface IP configuration subcommands:

access-group	Specify access control for packets
accounting	Enable IP accounting on this interface
address	Set the IP address of an interface
audit	Apply IDS audit name
auth-proxy	Apply authentication proxy
authentication	authentication subcommands
bandwidth-percent	Set EIGRP bandwidth limit
broadcast-address	Set the broadcast address of an interface
cef	Cisco Express Forwarding interface commands
cgmp	Enable/disable CGMP
dhcp	Configure DHCP parameters for this interface
directed-broadcast	Enable forwarding of directed broadcasts
dvmrp	DVMRP interface commands
flow	NetFlow related commands
header-compression	IPHC options
hello-interval	Configures IP-EIGRP hello interval
helper-address	Specify a destination address for UDP broadcasts
hold-time	Configures IP-EIGRP hold time
idle-group	Specify interesting packets for idle-timer
igmp	IGMP interface commands
information-reply	Enable sending ICMP Information Reply messages
inspect	Apply inspect name
irdp	ICMP Router Discovery Protocol
load-sharing	Style of load sharing
local-proxy-arp	Enable local-proxy ARP
mask-reply	Enable sending ICMP Mask Reply messages
mobile	Mobile IP support
mrm	Configure IP Multicast Routing Monitor tester
mroute-cache	Enable switching cache for incoming multicast packets
mtu	Set IP Maximum Transmission Unit
multicast	IP multicast interface commands
nat	NAT interface commands
nbar	Network-Based Application Recognition
next-hop-self	Configures IP-EIGRP next-hop-self
nhrp	NHRP interface subcommands
ospf	OSPF interface commands
pgm	PGM Reliable Transport Protocol
pim	PIM interface commands
policy	Enable policy routing
proxy-arp	Enable proxy ARP
rarp-server	Enable RARP server for static arp entries
redirects	Enable sending ICMP Redirect messages
rgmp	Enable/disable RGMP
rip	Router Information Protocol
route-cache	Enable fast-switching cache for outgoing packets
router	IP router interface commands
rsvp	RSVP Interface Commands
rtp	RTP parameters
sap	Session Announcement Protocol interface commands

```

security          DDN IP Security Option
split-horizon     Perform split horizon
summary-address  Perform address summarization
tcp              TCP header compression and other parameters
unnumbered       Enable IP processing without an explicit address
unreachables     Enable sending ICMP Unreachable messages
urd              Configure URL Rendezvousing
verify           Enable per packet validation
vrf              VPN Routing/Forwarding parameters on the interface
wccp             WCCP interface commands
(config-if)# no ip redirects
(config-if)# no ip unreachable
(config-if)# no ip mask-reply

```

To disable multiroute-cache:

```

(config-if)# no ip mroute-cache
(config-if)# exit

```

To setup Web access from only a single host:

```

(config)# access-list 5 permit host 192.168.1.1
(config)# ip http server access-class 5

```

And to disable SNMP:

```

(config)# no snmp-server

```

# Cisco Router Challenge 197

## Outline

This challenge involves the configuration of RIP Version 2 with authenticated routing tables.

## Objectives

The objectives of this challenge are to:

- Setup a RIP Version 2.
- Define authentication for RIP.

## Example

```

> en
# config t
(config)# router rip
(config-router)# version 2
(config-router)# network 194.205.128.0
(config-router)# ?
Router configuration commands:
  address-family      Enter Address Family command mode
  auto-summary        Enable automatic network number summarization

```

```

default          Set a command to its defaults
default-information  Control distribution of default information
default-metric   Set metric of redistributed routes
distance        Define an administrative distance
distribute-list  Filter networks in routing updates
exit            Exit from routing protocol configuration mode
flash-update-threshold  Specify flash update threshold in second
help           Description of the interactive help system
input-queue     Specify input queue depth
maximum-paths   Forward packets over multiple paths
neighbor       Specify a neighbor router
network        Enable routing on an IP network
no             Negate a command or set its defaults
offset-list     Add or subtract offset from IGRP or RIP metrics
output-delay   Interpacket delay for RIP updates
passive-interface  Suppress routing updates on an interface
redistribute    Redistribute information from another routing
               protocol
timers         Adjust routing timers
traffic-share   How to compute traffic share over alternate paths
validate-update-source  Perform sanity checks against source address of
               routing updates
version        Set routing protocol version

(config-router)# exit
(config)# key ?
  chain        Key-chain management
  config-key   Set a private configuration key
(config)# key chain ?
  WORD        Key-chain name
(config)# key chain martin
(config-keychain)# ?
Key-chain configuration commands:
  default     Set a command to its defaults
  exit       Exit from key-chain configuration mode
  key        Configure a key
  no         Negate a command or set its defaults
(config-keychain)# key ?
  <0-2147483647>  Key identifier
(config-keychain)# key 1
(config-keychain-key)# ?
Key-chain key configuration commands:
  accept-lifetime  Set accept lifetime of key
  default         Set a command to its defaults
  exit           Exit from key-chain key configuration mode
  key-string      Set key string
  no             Negate a command or set its defaults
  send-lifetime   Set send lifetime of key
(config-keychain-key)# key-string officer
(config-keychain-key)# exit
(config-keychain)# exit
(config)# int e0
(config-if)# ip rip ?
  advertise      Specify update interval
  authentication  Authentication control
  receive        advertisement reception
  send           advertisement transmission
  v2-broadcast   send ip broadcast v2 update
(config-if)# ip rip authentication ?
  key-chain      Authentication key-chain
  mode           Authentication mode
(config-if)# ip rip authentication key-chain ?
  LINE          name of key-chain
(config-if)# ip rip authentication key-chain martin

```

```
(config-if)# ip rip authentication mode ?
  md5   Keyed message digest
  text  Clear text authentication
(config-if)# ip rip authentication mode md5
```

# Cisco Router Challenge 197

## Outline

This challenge involves the configuration of RIP Version 2 with authenticated routing tables, and using a distribution-list with passive interfaces.

## Objectives

The objectives of this challenge are to:

- Setup a RIP Version 2.
- Define authentication for RIP.
- Define a routing filter to limit the transmission of routing information.
- Define a passive-interface for routing updates.

## Example

```
> en
# config t
(config)# access-list 10 permit 10.0.0.0 0.0.0.255

(config)# router rip
(config-router)# distribution-list 10 in fa0/1
(config-router)# passive-interface fa0/2

(config-router)# version 2
(config-router)# network 194.205.128.0
(config-router)# exit
(config)# key chain martin
(config-keychain)# key 1
(config-keychain-key)# key-string officer
(config-keychain-key)# exit
(config-keychain)# exit
(config)# int fa0/1
(config-if)# ip rip authentication key-chain martin
(config-if)# ip rip authentication mode md5
```

The passive-interface command stops the transmission of the routing tables on the specified interface.

# 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 fred
```

```
(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 (E1 and E2).

### 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 (names of interfaces, security levels, and so on).

## 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
```



```
# show running user
```

# Cisco PIX Challenge 4

## Outline

This challenge involves the configuration of basic PIX details (HTTP, Passwords, MOTD, and so on).

## 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

```
mypix(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

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

configure mode commands/options:

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

```
pixfirewall(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.

```
pixfirewall(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

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

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

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

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

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

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

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

## 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 for various settings, such as duplex, speed, and so on.

## 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:

speed 10|100|1000|auto  
no speed [10|100|1000|auto]

DESCRIPTION:

speed                    Configure speed operation

SYNTAX:

Possible Ethernet values are:  
10                    Force 10 Mbps operation  
100                   Force 100 Mbps operation  
auto                   Enable AUTO speed configuration

```
Possible GigabitEthernet values are:
10          Force 10 Mbps operation
100         Force 100 Mbps operation
1000        Force 1000 Mbps operation
auto        Enable AUTO speed configuration
```

```
see also:      duplex
(config-if)# speed 100
(config-if)# exit
(config)# int e1
(config-if)# nameif alabama
(config-if)# security-level 100
(config-if)# duplex full
(config-if)# speed 100
  (config-if)# exit
(config)# int e2
(config-if)# nameif uranus
(config-if)# security-level 50
(config-if)# duplex full
(config-if)# speed 100
(config-if)# exit
(config)# exit
# show running
```

# Cisco PIX Challenge 10

## Outline

This challenge involves the configuration of the DHCP server.

## Objectives

The objectives of this challenge are to:

- Enable the DHCP server.
- Define DHCP parameters.
- Show DHCP parameters.

## 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>]}
```

```
dhcpcd enable <srv_ifc_name>
dhcpcd auto_config <clnt_if_name>
show dhcpcd [binding|statistics]
clear dhcpcd
clear dhcpcd [binding|statistics]
```

DESCRIPTION:

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

# 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.



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 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  
**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)# 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)# 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 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)# username fred password bert
```

```
pixfirewall(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
```

## 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 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 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 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

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

# Cisco Switch Challenge 67

## Outline

This challenge involves enabling 802.1x authentication.

## Objectives

The objectives of this challenge are to:

- Define AAA
- Enable 802.1x.
- Define re-authentication.

## Example

```
> en
# config t
(config)# int fa0/1
(config-if)# no switchport
(config-if)# dot1x ?
  default          Configure Dot1x with default values for this port
  host-mode        Set the Host mode for 802.1x on this interface
  max-req          Max No.of Retries
  port-control     set the port-control value
  reauthentication Enable or Disable Reauthentication for this port
  timeout          Various Timeouts

(config-if)# dot1x port-control ?
  auto             PortState will be set to AUTO
  force-authorized PortState set to Authorized
  force-unauthorized PortState will be set to Unauthorized
(config-if)# dot1x port-control auto
(config-if)# dot1x reauthentication ?
  <cr>
(config-if)# dot1x re-authentication

(config-if)# dot1x timeout ?
  quiet-period    QuietPeriod in Seconds
  reauth-period   Time after which an automatic re-authentication should be
                  initiated
  server-timeout  Timeout for Radius Retries
  supp-timeout    Timeout for Supplicant retries
  tx-period       Timeout for Supplicant Re-transmissions

(config-if)# dot1x timeout reauth-period ?
  <1-65535>       Enter a value between 1 and 65535
```

```
(config-if)# dot1x timeout reauth-period 180
```

# Cisco Switch Challenge 68

## Outline

This challenge involves enabling 802.1x authentication with authentication from an AAA server.

## Objectives

The objectives of this challenge are to:

- Enable AAA.
- Define the Radius server.
- radius server.
- Enable 802.1x.
- Define re-authentication.
- Define Dot1x timeouts.

The commands used are:

```
(config)# aaa new-model
(config)# aaa accounting connection default start-stop group radius
(config)# aaa accounting network default start-stop group radius
(config)# aaa authentication dot1x default group radius local
(config)# dot1x system-auth-control
(config)# radius-server host 10.0.0.1 auth-port 1812 key test
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# dot1x port-control auto
(config-if)# dot1x re-authentication
(config-if)# dot1x timeout reauth-period 180
(config-if)# dot1x timeout tx-period 40
(config-if)# dot1x timeout quiet-period 10
(config-if)# dot1x max-req 3
```

## Example

```
> en
# config t
(config)# aaa new-model
(config)# aaa authen dot1x ?
  WORD      Named authentication list.
  default   The default authentication list.

(config)# aaa authentication dot1x default ?
  enable    Use enable password for authentication.
  group     Use Server-group
  line     Use line password for authentication.
```

```

local          Use local username authentication.
local-case    Use case-sensitive local username authentication.
none          NO authentication.

(config)# aaa authentication dot1x default ?
enable        Use enable password for authentication.
group         Use Server-group
line          Use line password for authentication.
local         Use local username authentication.
local-case    Use case-sensitive local username authentication.
none          NO authentication.
(config)# aaa authentication dot1x default group ?
WORD          Server-group name
radius        Use list of all Radius hosts.
tacacs+       Use list of all Tacacs+ hosts.
(config)# aaa authentication dot1x default group radius local
(config)# aaa accounting network ?
WORD          Named Accounting list.
default       The default accounting list.

(config)# aaa accounting network default ?
none          No accounting.
start-stop    Record start and stop without waiting
stop-only     Record stop when service terminates.
wait-start    Same as start-stop but wait for start-record commit.

(config)# aaa accounting network d star ?
group         Use Server-group

(config)# aaa accounting net d star g ?
WORD          Server-group name
radius        Use list of all Radius hosts.
tacacs+       Use list of all Tacacs+ hosts.
(config)# aaa accounting network default start-stop group radius
(config)# aaa accounting connection ?
WORD          Named Accounting list.
default       The default accounting list.

(config)# aaa accounting connection default ?
none          No accounting.
start-stop    Record start and stop without waiting
stop-only     Record stop when service terminates.
wait-start    Same as start-stop but wait for start-record commit.

(config)# aaa accounting connection default start-stop ?
group         Use Server-group

(config)# aaa accounting connection default start-stop group ?
WORD          Server-group name
radius        Use list of all Radius hosts.
tacacs+       Use list of all Tacacs+ hosts.

(config)# aaa accounting connection default start-stop group radius ?
group         Use Server-group
<cr>
(config)# aaa accounting connection default start-stop group radius
(config)# dot1x ?
system-auth-control  Enable or Disable SysAuthControl
(config)# dot1x system-auth-control

(config)# radius-server host ?
Hostname or A.B.C.D  IP address of RADIUS server

```

```

(config)# radius-server host 10.0.0.1 ?
acct-port      UDP port for RADIUS accounting server (default is 1646)
alias          1-8 aliases for this server (max. 8)
auth-port     UDP port for RADIUS authentication server (default is 1645)
backoff       Retry backoff pattern (Default is retransmits with constant
              delay)
key           per-server encryption key (overrides default)
non-standard  Parse attributes that violate the RADIUS standard
retransmit    Specify the number of retries to active server (overrides
              default)
timeout       Time to wait for this RADIUS server to reply (overrides
              default)
<cr>

(config)# radius-server host 10.0.0.1 au ?
<0-65536> Port number

(config)# radius-server host 10.0.0.1 au 1812 ?
acct-port      UDP port for RADIUS accounting server (default is 1813)
auth-port     UDP port for RADIUS authentication server (default is 1812)
key           per-server encryption key (overrides default)
non-standard  Parse attributes that violate the RADIUS standard
retransmit    Specify the number of retries to active server (overrides
              default)
timeout       Time to wait for this RADIUS server to reply (overrides
              default)
<cr>

(config)# radius-server host 10.0.0.1 auth-port 1812 key ?
LINE Text for this server's key

(config)# radius-server host 10.0.0.1 auth-port 1812 key test

(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# dot1x ?
default       Configure Dot1x with default values for this port
host-mode     Set the Host mode for 802.1x on this interface
max-req       Max No.of Retries
port-control  set the port-control value
reauthentication Enable or Disable Reauthentication for this port
timeout       Various Timeouts
(config-if)# dot1x port-control auto
(config-if)# dot1x re-authentication
(config-if)# dot1x timeout ?
quiet-period  QuietPeriod in Seconds
reauth-period Time after which an automatic re-authentication should be
              initiated
server-timeout Timeout for Radius Retries
supp-timeout  Timeout for Supplicant retries
tx-period     Timeout for Supplicant Re-transmissions
(config-if)# dot1x timeout reauth-period 180
(config-if)# dot1x timeout tx-period 40
(config-if)# dot1x timeout quiet-period 10
(config-if)# dot1 max-req ?
<1-10> Enter a value between 1 and 10
(config-if)# dot1x max-req 3

```

## Cisco Router Challenge 197

## Outline

This challenge involves enabling an authentication proxy using Tacacs+.

## Objectives

The objectives of this challenge are to:

- Enable AAA.
- Define the Tacacs+ server.
- Define authentication proxy settings for the HTTP server.

The commands used are:

```
> en
# config t
(config)# aaa new-model
(config)# aaa authentication login default group tacacs+
(config)# aaa authorization auth-proxy default group tacacs+
(config)# tacacs=server host 1.2.3.4
(config)# ip http server
(config)# ip http authentication tacacs
(config)# ip auth-proxy name AR http
(config)# int e0
(config-if)# ip auth-proxy AR
```

## Example

```
> en
# config t
(config)# aaa new-model
(config)# aaa authentication login default group tacacs+
(config)# aaa authorization ?
  auth-proxy      For Authentication Proxy Services
  cache           For AAA cache configuration
  commands        For exec (shell) commands.
  config-commands For configuration mode commands.
  configuration    For downloading configurations from AAA server
  exec            For starting an exec (shell).
  ipmobile        For Mobile IP services.
  network         For network services. (PPP, SLIP, ARAP)
  reverse-access  For reverse access connections
  template        Enable template authorization
(config)# aaa authorization auth-proxy ?
  default The default authorization list.

(config)# aaa authorization auth-proxy default ?
  group Use server-group.
  local Use local database.

(config)# aaa authorization auth-proxy default group ?
  WORD      Server-group name
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
```

```

(config)# aaa authorization auth-proxy default group tacacs+
(config)# tacacs-server host 1.2.3.4
(config)# ip http server
(config)# ip http ?
  access-class      Restrict http server access by access-class
  authentication    Set http server authentication method
  client            Set http client parameters
  max-connections  Set maximum number of concurrent http server connections
  path              Set base path for HTML
  port              Set http server port
  secure-ciphersuite Set http secure server ciphersuite
  secure-client-auth Set http secure server with client authentication
  secure-port       Set http secure server port number for listening
  secure-server     Enable HTTP secure server
  secure-trustpoint Set http secure server certificate trustpoint
  server            Enable http server
  timeout-policy    Set http server time-out policy parameters
(config)# ip http authentication ?
  enable Use enable passwords
  local  Use local username and passwords
  tacacs Use tacacs to authorize user
(config)# ip http authentication tacacs
(config)# ip auth-proxy ?
  absolute-timer      Absolute Timeout in min
  auth-cache-time     Alias of inactivity-timer
  auth-proxy-audit    Authentication Proxy Auditing
  auth-proxy-banner   Authentication Proxy Banner
  inactivity-timer    Inactivity Timeout in min
  max-login-attempts  Max Login attempts per user
  name                Specify an Authentication Proxy Rule
  watch-list          Watch-list
  <cr>

(config)# ip auth-proxy name ?
  WORD Name of Authentication Rule

(config)# ip auth-proxy name AR ?
  ftp      FTP Protocol
  http     HTTP Protocol
  telnet   Telnet Protocol
  <cr>
(config)# ip auth-proxy name AR http

(config)# int e0
(config-if)# ip auth-proxy ?
  WORD Name of authenticaion proxy rule

(config-if)# ip auth-proxy AR ?
  <cr>
(config-if)# ip auth-proxy AR

```

## Cisco Router Challenge 44

### Outline

This challenge involves the configuration of IP Inspect.

## Objectives

The objectives of this challenge are to:

- Setup limits for the number of connections over one-minute.
- Setup limits for the number of open connections.
- Define SYN waits.

## Example

```
> en
# config t
(config)# ip inspect ?
  alert-off          Disable alert
  audit-trail        Enable the logging of session information (addresses and
                    bytes)
  dns-timeout        Specify timeout for DNS
  max-incomplete     Specify maximum number of incomplete connections before
                    clamping
  name               Specify an inspection rule
  one-minute         Specify one-minute-sample watermarks for clamping
  tcp                Config timeout values for tcp connections
  udp                Config timeout values for udp flows
  <cr>
(config)# ip inspect one-minute ?
  high              Specify high-watermark for clamping
  low               Specify low-watermark for clamping
(config)# ip inspect one-minute low 360
(config)# ip inspect one-minute high 410
(config)# ip inspect max-incomplete low 720
(config)# ip inspect max-incomplete high 770
(config)# ip inspect dns-timeout 1
(config)# ip inspect tcp ?
  finwait-time      Specify timeout for TCP connections after a FIN
  idle-time         Specify idle timeout for tcp connections
  max-incomplete    Specify max half-open connection per host
  synwait-time      Specify timeout for TCP connections after a SYN and no
                    further data
(config)# ip inspect tcp synwait-time ?
  <1-2147483>       Timeout in seconds
(config)# ip inspect tcp synwait-time 35
(config)# ip inspect tcp finwait-time 5

(config)# ip inspect tcp max-incomplete ?
  host              Specify max half-open connection per host
(config)# ip inspect tcp max-incomplete host 800
(config)# ip inspect tcp ?
  finwait-time      Specify timeout for TCP connections after a FIN
  idle-time         Specify idle timeout for tcp connections
  max-incomplete    Specify max half-open connection per host
  synwait-time      Specify timeout for TCP connections after a SYN and no
                    further data
(config)# ip inspect tcp idle-time 70
(config)# ip inspect udp idle-time 57
```

# Cisco Router Challenge 45

## Outline

This challenge involves the configuration of a context based access-list (CBAC).

## Objectives

The objectives of this challenge are to:

- Setup a CBAC.
- Define the protocols which the CBAC applies to.

## Example

```
> en
# config t
(config)# access-list 105 permit ip any any
(config)# int fa0/0
(config-if)# ip access-group 105 in
(config-if)# exit
(config)# ip inspect name cisco ?
cuseeme      CUSeeMe Protocol
fragment     IP fragment inspection
ftp          File Transfer Protocol
h323         H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http         HTTP Protocol
netshow      Microsoft NetShow Protocol
rcmd         R commands (r-exec, r-login, r-sh)
realaudio    Real Audio Protocol
rpc          Remote Procedure Call Protocol
rtsp         Real Time Streaming Protocol
smtp         Simple Mail Transfer Protocol
sqlnet       SQL Net Protocol
streamworks  StreamWorks Protocol
tcp          Transmission Control Protocol
tftp         TFTP Protocol
udp          User Datagram Protocol
vdolive      VDOLive Protocol
(config)# ip inspect name cisco tcp
(config)# ip inspect name cisco udp
(config)# ip inspect name cisco ftp
(config)# ip inspect name cisco sqlnet
(config)# int e0
(config-if)#ip inspect ?
WORD Name of inspection defined
(config-if)#ip inspect cisco
(config-if)#ip inspect cisco in
(config-if)# exit
(config)# access-list 106 deny ip any any
(config)# int s0
(config-if)# ip access-group 106 in
```

## Explanation

ACLs are fairly static in their operation, and they do not take into account the context of a data packet. Thus they cannot detect the actual state of a connection. A typical type of attack

in a system is DoS (Denial-of-Service), which is caused when multiple remote clients make access to the same server. Knowing the context of a data packet, or its associated connection thus allows finer control of the security of the system. For example in a DoS the firewall could detect that the number of connections in a given time limit had exceeded a given number, and block any other ones, within a given time. Context-based Access Control (CBAC) are thus stateful, and dynamic, and can look further into packets than normal ACLs. In client-server communications the key states in most connections are:

- Client sends a **SYN** flag to the server.
- The server responds with a **SYN, ACK** to the client.
- The client responds with an **ACK**, and the connection is made.
- The client and server then communicate.
- The client sends a **FIN, ACK** flag.
- The server sends an **ACK** flag, and the connection is finished.

Context-based Access Control is used to implement firewall options, such as limiting the number of open connections. A typical attack is the DoS (Denial of Service) attack, where the external party opens up multiple connections. To overcome this, the router can be setup to detect a minimum threshold for half-open sessions. The half-open session is where either the client or server quits the session without the other side knowing about it. In a DoS, the client opens a connection, and does not complete it. The server does not know that the client has disconnected, thus the connection still takes some resources on the server, which can become overburdened if there are many open sessions. On the Napier pods, use Pod C (Router 1) for an example of router which implements these CBACs.

### Global timeouts and thresholds

The main limits that are defined are:

- **ip inspect tcp synwait-time**. This defines the time to wait before a connection drops. Default: 30 seconds.
- **ip inspect tcp finwait-time**. This defined the time after a FIN flag for a connection to be dropped. Default: 5 seconds.
- **ip inspect tcp idle-time**. This defines the length of time that a connection can be idle. Default: 1 hour.
- **ip inspect dns-time**. This defines the amount of time of a time-out for a DNS query. Default: 5 seconds.
- **ip inspect max-incomplete high**. This defines the maximum number of half-open connections, before it starts to delete them one-by-one. Default: 500.
- **ip inspect max-incomplete low**. This defines the lower limit for the half-open connections. Default: 400.
- **ip inspect one-minute high**. This defines the maximum number of half-open connections in a minute, before it starts to delete them one-by-one. Default: 500 per minute.

- **ip inspect one-minute low.** This defines the lower limit for the half-open connections over a minute. Default: 400.

For example to limit the maximum open sessions at any time to between 900 and 1100:

```
(config)# ip inspect ?
  alert-off      Disable alert
  audit-trail    Enable the logging of session information (addresses and
                bytes)
  dns-timeout    Specify timeout for DNS
  max-incomplete Specify maximum number of incomplete connections before
                clamping
  name           Specify an inspection rule
  one-minute     Specify one-minute-sample watermarks for clamping
  tcp           Config timeout values for tcp connections
  udp           Config timeout values for udp flows
  <cr>
(config)# ip inspect tcp ?
  finwait-time  Specify timeout for TCP connections after a FIN
  idle-time     Specify idle timeout for tcp connections
  max-incomplete Specify max half-open connection per host
  synwait-time  Specify timeout for TCP connections after a SYN and no
                further data
(config)# ip inspect max-incomplete low 900
(config)# ip inspect max-incomplete high 1100
```

and for the maximum open sessions for one-minute:

```
(config)# ip inspect one-minute low 900
(config)# ip inspect one-minute high 1100
```

get rid of IP inspect, use:

```
(config)# no ip inspect one-minute low
```

To limit the DNS-timeout to 10 seconds:

```
(config)# ip inspect dns-timeout 10
```

# Cisco Router Challenge 191

## Outline

This challenge involves the configuration of a context based access-list (CBAC) for inspect rules for timeouts, alerts and audit-trails.

## Objectives

The objectives of this challenge are to:

- Setup a CBAC.

- Define the protocols which the CBAC applies to.

### Example

```

> en
# config t
(config)# ip inspect name cisco ?
cuseeme      CUSeeMe Protocol
fragment     IP fragment inspection
ftp          File Transfer Protocol
h323         H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http         HTTP Protocol
netshow      Microsoft NetShow Protocol
rcmd         R commands (r-exec, r-login, r-sh)
realaudio    Real Audio Protocol
rpc          Remote Procedure Call Protocol
rtsp         Real Time Streaming Protocol
smtp         Simple Mail Transfer Protocol
sqlnet       SQL Net Protocol
streamworks  StreamWorks Protocol
tcp          Transmission Control Protocol
tftp         TFTP Protocol
udp          User Datagram Protocol
vdolive      VDOLive Protocol

(config)# ip inspect name cisco icmp ?
alert        Turn on/off alert
audit-trail  Turn on/off audit trail
timeout      Specify the inactivity timeout time
<cr>

(config)# ip inspect name cisco icmp timeout ?
<5-43200>   Timeout in seconds

(config)# ip inspect name cisco icmp timeout 10

(config)# ip inspect name cisco http ?
alert        Turn on/off alert
audit-trail  Turn on/off audit trail
java-list    Specify a standard access-list to apply the Java blocking. If
              specified, MUST appear directly after option "http"
timeout      Specify the inactivity timeout time
urlfilter    Specify URL filtering for HTTP traffic
<cr>

(config)# ip inspect nam cisco http alert ?
off          Turn off alert
on           Turn on alert

(config)# ip inspect nam cisco http alert off

(config)# ip inspect name cisco ftp ?
alert        Turn on/off alert

audit-trail  Turn on/off audit trail
timeout      Specify the inactivity timeout time
<cr>

(config)# ip inspect name cisco ftp audit-trail ?
off          Turn off audit trail
on           Turn on audit trail

```

```

(config)# ip inspect name cisco ftp audit-trail on

(config)# ip inspect udp idle-time 50
(config)# ip inspect tcp idle-time 500

(config)# int s0
(config-if)# ip inspect ?
WORD Name of inspection defined
(config-if)# ip inspect cisco ?
in Inbound inspection
out Outbound inspection
(config-if)# ip inspect cisco in
(config-if)# exit

```

## Cisco Switch Challenge 49

### Outline

This challenge involves enabling port security and the BPDU guard (to be defined against spanning-tree attacks).

### Objectives

The objectives of this challenge are to:

- Enable BPDU guard.
- Enable port-security.
- Define a maximum number of MAC addresses on a port.
- Define a MAC address on a port.

### Example

```

> en
# config t
Switch(config)# spanning-tree ?
backbonefast Enable BackboneFast Feature
etherchannel Spanning tree etherchannel specific configuration
extend Spanning Tree 802.1t extensions
loopguard Spanning tree loopguard options
mode Spanning tree operating mode
mst Multiple spanning tree configuration
pathcost Spanning tree pathcost options
portfast Spanning tree portfast options
uplinkfast Enable UplinkFast Feature
vlan VLAN Switch Spanning Tree

Switch(config)# spanning-tree portfast ?
bpdufilter Enable portfast bpdu filter on this switch
bpduguard Enable portfast bpdu guard on this switch
default Enable portfast by default on all access ports

```

```

Switch(config)# spanning-tree portfast bpduguard ?
    default  Enable bdpu guard by default on all portfast ports

Switch(config)# spanning-tree portfast bpduguard def ?
    <cr>

Switch(config)# spanning-tree portfast bpduguard def
Switch(config)# int fa0/1
Switch(config-if)# sw po ?
    aging          Port-security aging commands
    mac-address    Secure mac address
    maximum        Max secure addr
    violation      Security Violation Mode
    <cr>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security max ?
    <1-5120>  Maximum addresses

Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security mac-address ?
    H.H.H      48 bit mac address
    sticky    Configure dynamic secure addresses as sticky
Switch(config-if)# switchport port-security mac-address 0000.1111.2222

```

# Cisco Switch Challenge 50

## Outline

This challenge involves defending against an attacker depleting the DHCP pool using DHCP snooping.

## Objectives

The objectives of this challenge are to:

- Enable DHCP snooping.
- Apply DHCP snooping on an interface.

## Example

```

> en
# config t
Switch(config)# ip dhcp ?
    conflict          DHCP address conflict parameters
    database          Configure DHCP database agents
    excluded-address  Prevent DHCP from assigning certain addresses

```

```

limited-broadcast-address  Use all 1's broadcast address
ping                      Specify ping parameters used by DHCP
pool                      Configure DHCP address pools
relay                     DHCP relay agent parameters
smart-relay               Enable Smart Relay feature
snooding                  DHCP Snooping
Switch(config)# ip dhcp snooping ?
  information             DHCP Snooping information
  vlan                    DHCP Snooping vlan
  <cr>
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan ?
  <1-4094>                DHCP Snooping vlan first number
Switch(config)# ip dhcp snooping vlan 4
Switch(config)# int fa0/1
Switch(config-if)# switchport mode access

Switch(config-if)# ip dhcp ?
  snooping                DHCP Snooping
Switch(config-if)# ip dhcp snooping ?
  limit                   DHCP Snooping limit
  trust                   DHCP Snooping trust config
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit ?
  rate                    DHCP Snooping limit

Switch(config-if)# ip dhcp snooping limit rate ?
  <1-4294967294>          DHCP snooping rate limit
Switch(config-if)# ip dhcp snooping limit rate 30

```

## 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

```

## PIX/ASA Test

### End of unit test

Take the on-line test, go to:

[http://networksims.com/e\\_ns.html](http://networksims.com/e_ns.html)

### Key facts

Not available in this version.

## Network Security 1

### **End of unit test**

Take the on-line test, go to:

**[http://networksims.com/e\\_ns2.htm](http://networksims.com/e_ns2.htm)**

### **Key facts**

Not available in this version.