

ASA/New PIX

Cisco PIX Challenge 97

Outline

This challenge involves configuring external access to an email server on the DMZ.

Objectives

The objectives of this challenge are to:

- Define fixup for SMTP.
- Define access-list to allow access to the email server.
- Define a static mapping between the email server and an outside address.
- Apply the access-list.
- Define MAC addresses for the ports (just in case they are used on other devices).

Example

In the following example, the addresses of the ports are:

E0 (outside) – 10.0.0.1

E1 (inside) – 192.168.0.1

E2 (dmz) – 172.16.10.1

The email server is at 172.16.10.2 and will be mapped to 10.0.0.3 for external access.

The default gateway is at 10.0.0.2

```
(config)# fixup protocol smtp 25
(config)# int e0
(config-if)# ip address 10.0.0.1 255.255.255.0
(config-if)# nameif outside
(config-if)# mac-address 1111.2222.3333
(config-if)# no shutdown
(config-if)# exit
(config)# int e1
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif inside
(config-if)# mac-address 2222.3333.4444
(config-if)# no shutdown
(config-if)# exit
(config)# int e2
(config-if)# ip address 172.16.10.1 255.255.255.0
```

```
(config-if)# nameif dmz
(config-if)# mac-address 3333.4444.5555
(config-if)# no shutdown
(config-if)# exit
```

Next permit access from the outside interface to the Email server:

```
(config)#access-list outside_int permit tcp any host 10.0.0.3 eq smtp
```

Allow all outgoing connections from the Email server to external nodes:

```
(config)# access-list dmz_interface permit tcp host 172.16.10.2 any eq smtp
```

Map the Email server on the DMZ, which is at 172.16.0.2, and let its accessible address be 10.0.0.3:

```
(config)# static (dmz,outside) 10.0.0.3 172.16.0.2
```

Apply the access-lists:

```
(config)# access-group outside_interface in interface outside
(config)# access-group dmz_interface in interface dmz
```

Cisco PIX Challenge 98

Outline

This challenge involves configuring **WebVPN**, which supports a secure, remote-access VPN tunnel to the security device using a web browser. There is thus no need for any special software or hardware clients. It can be used in a number of applications such as for internal websites, Web-enabled applications, secure directory shares, secure email, and so on. It also uses **SLA** (Service Level Agreement) which monitors a remote IP address. In this case a static IP address is used.

Objectives

The objectives of this challenge are to:

- Define the E0 name, IP address and subnet mask.
- Define WebVPN port.
- Define WebVPN on the outside interface.
- Define an SLA for a remote host on a certain interface.

Commands

```
(config)# int e0
(config-if)# nameif newjersey
(config-if)# ip address 1.2.3.5 255.255.0.0
```

```

(config-if)# no shutdown
(config-if)# exit
(config)# webvpn
(config-webvpn)# port 444
(config-webvpn)# enable newjersey
(config-webvpn)# exit
(config)# sla mon 1
(config-sla-monitor)# t e p i 1.2.3.4 i newjersey
(config-sla-monitor-echo)# ?

```

Example

```

(config)# int e0
(config-if)# nameif newjersey
(config-if)# exit

```

```

(config)# webvpn
(config-webvpn)# ?

```

WebVPN commands:

apcf	Load Application Profile Customization Framework (APCF) profile
authorization-dn-attributes	The DN of the peer certificate used as username for authorization
authorization-required	Require users to authorize successfully in order to connect
auto-signon	Auto signon
cache	Configure WebVPN cache
character-encoding	Configures the character encoding for WebVPN portal pages
csd	This specifies whether Cisco Secure Desktop is enabled and the package file name to be used.
customization	Configure WebVPN GUI Customization object
default-idle-timeout	This is the default idle timeout in seconds
enable	Enable WebVPN on the specified interface
exit	Exit from WebVPN configuration mode
file-encoding	Configures the file encoding for a file sharing server
help	Help for WebVPN commands
http-proxy	This is the proxy server to use for HTTP requests
https-proxy	This is the proxy server to use for HTTPS requests
java-trustpoint	Configure WebVPN java trustpoint
memory-size	Configure WebVPN memory size
no	Remove a WebVPN command or set to its default
port	WebVPN should listen for connections on the specified port
port-forward	Configure the port-forward list for WebVPN
proxy-bypass	Configure proxy bypass
rewrite	Configure content rewriting rule
sso-server	Configure an SSO Server
svc	This specifies whether the SSL VPN Client is enabled and the package file name to be used.
tunnel-group-list	Configure WebVPN group list dropdown in login page
url-list	Configure a list of URLs for use with WebVPN

```

(config-webvpn)# port ?

```

webvpn mode commands/options:

```

<1-65535> The WebVPN server's SSL listening port. TCP port 443 is the

```

default.

(config-webvpn)# port 444

(config-webvpn)# enable ?

webvpn mode commands/options:
 inf2 Name of interface Ethernet2
 inside Name of interface Ethernet1
 newjersey Name of interface Ethernet0

(config-webvpn)# enable newjersey

(config-webvpn)# exit

(config)# sla ?

configure mode commands/options:
 monitor IP Service Level Agreement Monitor

(config)# sla mon ?

configure mode commands/options:
 <1-2147483647> Entry Number
 schedule IP SLA Monitor Entry Scheduling

(config)# sla mon 1

(config-sla-monitor)# ?

IP SLA Monitor entry configuration commands:
 exit Exit operation configuration
 type Type of entry

(config-sla-monitor)# type ?

sla-monitor mode commands/options:
 echo Echo Operation

(config-sla-monitor)# type echo ?

sla-monitor mode commands/options:
 protocol Protocol to Use for Operations

(config-sla-monitor)# type echo ipicmpecho ?

sla-monitor mode commands/options:
 ipIcmpEcho Use IP/ICMP

(config-sla-monitor)# t e p i ?

sla-monitor mode commands/options:
 Hostname or A.B.C.D IP address or hostname

(config-sla-monitor)# t e p i 1.2.3.4 ?

sla-monitor mode commands/options:
 interface Interface keyword

(config-sla-monitor)# t e p i 1.2.3.4 i ?

sla-monitor mode commands/options:
Current available interface(s):
 inf2 Name of interface Ethernet2

```
inside      Name of interface Ethernet1
newjersey   Name of interface Ethernet0
(config-sla-monitor)# type echo protocol ipicmp 1.2.3.4 interface newjersey
(config-sla-monitor-echo)# ?
```

```
IP SLA Monitor Echo Configuration Commands:
default      Set a command to its defaults
exit         Exit probe configuration
frequency    Frequency of an operation
no           Negate a command or set its defaults
num-packets  Number of Packets
request-data-size Request data size
threshold    Operation threshold in milliseconds
timeout      Timeout of an operation
tos          Type Of Service
<cr>
```

Cisco ASA/PIX Challenge 99

Outline

The ASA device supports a time-range for ACLs, such as defining an access-list for a weekend, or for specific day. It also includes two configuration elements for AAA settings (not linked to time-ranges).

Note: ASA/PIX 7.x only

Objectives

The objectives of this challenge are to:

- Define a time-range.
- Implement a time-ranged ACL.
- Define an AAA group tag.
- Define an AAA host.
- Define AAA host details.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit

(config)# time-range workingday
(config-time-range)# periodic weekday 5:00 to 9:00
(config-time-range)# periodic saturday 3:00 to 15:00
(config-time-range)# exit
(config)# access-list Columbia permit ip any any time-range workingday
(config)# aaa-server test protocol radius
(config-aaa-server-group)# exit
```

```
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# key testkey
(config-aaa-server-host)# authentication-port 1645
(config-aaa-server-host)# accounting-port 1646
(config-aaa-server-host)# retry-interval 10
(config-aaa-server-host)# exit
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
```

```
(config)# time-range workingday
(config-time-range)# ?
```

Time range configuration commands:

absolute	absolute time and date
exit	Exit from time-range configuration mode
help	Help for time-range configuration commands
no	Negate a command or set its defaults
periodic	periodic time and date

```
(config-time-range)# ab ?
```

trange mode commands/options:

end	ending time and date
start	starting time and date

```
(config-time-range)# periodic ?
```

trange mode commands/options:

Friday	Friday
Monday	Monday
Saturday	Saturday
Sunday	Sunday
Thursday	Thursday
Tuesday	Tuesday
Wednesday	Wednesday
daily	Every day of the week
weekdays	Monday thru Friday
weekend	Saturday and Sunday

exec mode commands/options:

interval	Performance monitoring interval in seconds
quiet	Turn on quiet mode for performance monitoring
settings	View performance monitoring settings
verbose	Turn on verbose mode for performance monitoring

```
(config-time-range)# periodic weekday ?
```

trange mode commands/options:

hh:mm	Starting time
-------	---------------

```
(config-time-range)# periodic weekday 5:00 ?
```

trange mode commands/options:

to	ending day and time
----	---------------------

```
(config-time-range)# periodic weekday 5:00 to ?
```

```
trange mode commands/options:
  hh:mm Ending time - stays valid until beginning of next minute
(config-time-range)# periodic weekday 5:00 to 9:00
(config-time-range)# exit
(config)# access-list Columbia permit ip any any time-range workingday
```

Next the AAA server is defined:

```
pixfirewall(config)# aaa-server ?
```

```
configure mode commands/options:
  WORD < 17 char Enter a AAA server group tag
```

```
pixfirewall(config)# aaa-server test ?
```

```
configure mode commands/options:
  ( Open parenthesis for the name of the network interface
    where the designated AAA server is accessed
  deadtime Specify the amount of time that will elapse between the
    disabling of the last server in the group and the
    subsequent re-enabling of all servers
  host Enter this keyword to specify the IP address for the
    server
  max-failed-attempts Specify the maximum number of failures that will be
    allowed for any server in the group before that server
    is deactivated
  protocol Enter the protocol for a AAA server group
```

```
pixfirewall(config)# aaa-s test protocol ?
```

```
configure mode commands/options:
  kerberos Protocol Kerberos
  ldap Protocol LDAP
  nt Protocol NT
  radius Protocol RADIUS
  sdi Protocol SDI
  tacacs+ Protocol TACACS+
```

```
(config)# aaa-server test protocol radius
```

```
(config-aaa-server-group)# ?
```

```
AAA server configuration commands:
  accounting-mode Enter this keyword to specify accounting mode
  exit Exit from aaa-server group configuration mode
  help Help for AAA server configuration commands
  max-failed-attempts Specify the maximum number of failures that will be
    allowed for any server in the group before that server
    is deactivated
  no Remove an item from aaa-server group configuration
  reactivation-mode Specify the method by which failed servers are
    reactivated
```

```
(config-aaa-server-group)# accounting-mode ?
```

```
aaa-server-group mode commands/options:
  simultaneous Enter this keyword to specify simultaneous accounting
  single Enter this keyword to specify single accounting
```

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

```
(config-aaa-server-group)# max-failed-attempts ?
```

```

aaa-server-group mode commands/options:
  <1-5> Maximum number of failures (1-5)

(config-aaa-server-group)# reactivation-mode ?

aaa-server-group mode commands/options:
  depletion Failed servers will remain inactive until all other servers in
             this group are inactive
  timed     Failed servers will be reactivated after 30 seconds of down time

(config-aaa-server-group)# exit
(config)# aaa-server test ?

configure mode commands/options:
  (                               Open parenthesis for the name of the network interface
                               where the designated AAA server is accessed
  deadtime                       Specify the amount of time that will elapse between the
                               disabling of the last server in the group and the
                               subsequent re-enabling of all servers
  host                           Enter this keyword to specify the IP address for the
                               server
  max-failed-attempts            Specify the maximum number of failures that will be
                               allowed for any server in the group before that server
                               is deactivated
  protocol                       Enter the protocol for a AAA server group
(config)# aaa-server test (newyork) ?

configure mode commands/options:
  host Enter this keyword to specify the IP address for the server
(config)# aaa-server test (newyork) h ?

configure mode commands/options:
  Hostname or A.B.C.D Enter an IP address or a name
  WORD < 129 char     Enter a DNS name
(config)# aaa-server test (newyork) h 1.2.3.4 ?

configure mode commands/options:
  WORD Alphanumeric keyword up to 128 characters used as the encryption key
       for communicating with the AAA server.
  timeout Specify the maximum time to wait for response from configured server
  <cr>
(config)# aaa-server test (inside) host 1.2.3.4
(config-aaa-server-host)# ?

AAA server configuration commands:
  accounting-port Specify the port number to be used for accounting
  acl-netmask-convert Specify the ACL Downloadable Netmask Operation
  authentication-port Specify the port number to be used for authentication
  exit Exit from aaa-server host configuration mode
  help Help for AAA server configuration commands
  key Specify the secret used to authenticate the NAS to the
      AAA server
  no Remove an item from aaa-server host configuration
  radius-common-pw Specify a common password for all RADIUS authorization
                  transactions
  retry-interval Specify the amount of time between retry attempts
  timeout Specify the maximum time to wait for response from
          configured server
(config-aaa-server-host)# acc ?

aaa-server-host mode commands/options:
  <0-65535> Enter port number (0 - 65535)

```

```

configure mode commands/options:
ERROR: % Ambiguous command: "acc "
(config-aaa-server-host)# acl- ?

aaa-server-host mode commands/options:
  auto-detect  Enter this keyword to specify auto-detect netmask
  standard     Enter this keyword to specify standard netmask
  wildcard     Enter this keyword to specify wildcard netmask

                               configured server
(config-aaa-server-host)# key ?

aaa-server-host mode commands/options:
  WORD < 129 char  Enter an alphanumeric string up to 128 characters
(config-aaa-server-host)# key testkey

(config-aaa-server-host)# radius ?

aaa-server-host mode commands/options:
  WORD < 128 char  Enter an alphanumeric string up to 127 characters
(config-aaa-server-host)# ret ?

aaa-server-host mode commands/options:
  <1-10>  Number of seconds (1 - 10)
(config-aaa-server-host)# tim ?

aaa-server-host mode commands/options:
  <1-300>  Number of seconds (1 - 300)
(config-aaa-server-host)# authentication-port 1645
(config-aaa-server-host)# accounting-port 1646
(config-aaa-server-host)# retry-interval 10

```

Cisco ASA/PIX Challenge 100

Title: Interface-level Redundancy

Outline

The ASA device supports **interface redundancy**, where interfaces can be defined with the same firewall functionality (inside, outside, and so on), and thus connect to the same network. One of the interfaces can thus be active while the other goes into a standby mode. If the active interface goes down, then the standby interface will take its place.

The redundant interface is a logical interface with pairs for an active and a standby physical interface, and the ASA supports up to **eight** redundant interface pairs.

Note: PIX/ASA 8.x only

Objectives

The objectives of this challenge are to:

- Enable Ethernet interfaces.
- Define the redundancy interface.
- Define name and IP details for the redundant interface.
- Define the interfaces for membership of the redundant interface.
- Show the active device, and standby (using the show redundant command)

Commands

```
# show version
(config)# int e0
(config-if)# no nameif
(config-if)# no shutdown
(config-if)# no ip address
(config-if)# no ip security-level
(config-if)# exit
(config)# int e1
(config-if)# no nameif
(config-if)# no shutdown
(config-if)# no ip address
(config-if)# no ip security-level
(config-if)# exit
(config)# int redundant 1
(config-if)# nameif inside
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# member-interface e0
(config-if)# member-interface e1
(config-if)# no shutdown
(config-if)# exit
(config)# exit
# show interface redundant 1
```

Example

```
# show version
Cisco PIX Security Appliance Software Version 7.0(1)
Device Manager Version 5.0(1)

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

pixfirewall up 10 mins 40 secs

Hardware:   PIX-515E, 96 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xffff0000, 16MB
BIOS Flash AM29F400B @ 0xffffd8000, 32KB

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

Licensed features for this platform:
Maximum Physical Interfaces : 3
Maximum VLANs              : 10
Inside Hosts               : Unlimited
Failover                   : Disabled
```

```
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Cut-through Proxy : Enabled
Guards : Enabled
URL Filtering : Enabled
Security Contexts : 0
GTP/GPRS : Disabled
VPN Peers : Unlimited
```

This platform has a Restricted (R) license.

```
Serial Number: 807290112
Running Activation Key: 0x3f43a2b7 0xf5909081 0x5fd21d2b 0x16cbcc59
Configuration last modified by enable_15 at 15:42:06.949 UTC Thu Dec 28 2006
```

```
(config)# int e0
(config-if)# no nameif
(config-if)# no shutdown
(config-if)# no ip address
(config-if)# no ip security-level
(config-if)# exit
(config)# int e1
(config-if)# no nameif
(config-if)# no shutdown
(config-if)# no ip address
(config-if)# no ip security-level
(config-if)# exit
(config)# int redundant 1
(config-if)# nameif inside
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# member-interface e0
(config-if)# member-interface e1
(config-if)# no shutdown
(config-if)# exit
(config)# exit
# show interface redundant 1
Interface Redundant1 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 192.168.0.1, 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
Redundancy Information:
  Member e0 (active), e1
  Last switchover at 00:00:00 GMT Jun 1 2008
```

After the redundant interface is define, there should be no changes to the interfaces involved, apart from setting the duplex and speed settings, which are inherited by the

redundant interface. A great strength of interface redundancy is that it responds within 0.5s, which is faster than for failover.

To change the active interface to e1, the following command is used:

```
# redundant-interface redundant1 active-member e1
```

Cisco ASA/PIX Challenge 101

Title: Routing Information to Prevent IP Address Spoofing

Outline

With Reverse Path Forwarding (RPF), the firewall detects spoofed source addresses, as it examines the source of every data packet which arrives at a specific interface. It then tried to find a reverse path back to the source. If it cannot find this, it will reject the packet (and a logging message stored).

Objectives

The objectives of this challenge are to:

- Enable Ethernet interfaces.
- Define RPF on an interface.
- Display RPF statistics.

Commands

```
# show version
# config t
(config)# int e0
(config-if)# nameif outside
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# int e1
(config-if)# nameif inside
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 100
(config-if)# exit
(config)# ip verify reverse-path interface inside
(config)# ip verify reverse-path interface outside
(config)# exit
# show ip verify statistics
```

Example

```

# show version
# config t
(config)# int e0
(config-if)# nameif outside
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# int e1
(config-if)# nameif inside
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 100
(config-if)# exit
(config)# ip verify ?

configure mode commands/options:
  reverse-path Keyword to indicate Reverse-Path Filtering

(config)# ip verify reverse-path ?

configure mode commands/options:
  interface Keyword to apply RPF on an interface

(config)# ip verify reverse-path interface ?

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

(config)# ip verify reverse-path interface inside
(config)# ip verify reverse-path interface outside

# sh ip ?
address Show IP addresses, DHCP leases
audit   Show ip audit statistics
local   Show ip local pool information
verify  Show Reverse Path Verify (RPF) statistics
|       Output modifiers
<cr>

# sh ip verify ?
statistics Show Reverse Path Verify (RPF) statistics

# sh ip verify statistics
interface outside: 100 unicast rpf drops
interface inside: 300 unicast rpf drops
interface inf: 43 unicast rpf drops

```

Cisco ASA/PIX Challenge 102

Title: Default route for tunneled traffic

Outline

The PIX/ASA devices can have multiple default routes, each with a different cost. It can also have a default route for tunneled traffic, thus non-encrypted traffic, without a static route, would go via the normal default gateway, and encrypted traffic, without a static route, would go via the tunneled gateway.

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 interface details.
- Define a default gateway for non-encrypted traffic. A default metric (1) is used for the distance metric.
- Define a default gateway for encrypted traffic.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# route Glasgow 0 0 192.168.0.1
(config)# route Glasgow 0 0 192.168.0.2
(config)# route Glasgow 0 0 192.168.0.3 tunneled
```

Example

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# route ?

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

(config)# route Glasgow ?
configure mode commands/options:
  Hostname or A.B.C.D  The foreign network for this route, 0 means default

(config)# route Glasgow 0 ?
configure mode commands/options:
  A.B.C.D  The netmask for the destined foreign network

(config)# route Glasgow 0 0 ?
```

```
configure mode commands/options:
  Hostname or A.B.C.D The address of the gateway by which the foreign network
  is reached.
```

```
(config)# route Glasgow 0 0 192.168.0.1
(config)# route Glasgow 0 0 192.168.0.2
(config)# route Glasgow 0 0 192.168.0.3 ?
```

```
configure mode commands/options:
  <1-255> Distance metric for this route, default is 1
  tunneled Enable the default tunnel gateway option, metric is set
  to 255
  <cr>
```

```
(config)# route Glasgow 0 0 192.168.0.3 tunneled
```

Cisco ASA/PIX Challenge 103

Title: Favouring Static Routes with better Reachability

Outline

Normally a static route will stay active, but problems can occur if the route goes down. Thus the PIX/ASA device can base the static route on the best performance, thus if one route goes down, the other will take over. The SLA (Service Level Agreement) monitor process is used to monitor an arbitrary target address.

Objectives

The objectives of this challenge are to:

- Enable the SLA monitor process (with **sla monitor ID**).
- Define the reachability test (with **type echo protocol ipicmpecho IPDEST interface IFNAME**), which sends an ICMP packet require to a target IP address (IPDEST) on a given interface (IFNAME).
- Define optional test parameters, such as frequency of test, number of packets, request data size, Type-of-service (TOS), timeout and threshold.
- Run tests forever (with **sla monitor ID life forever now**).
- Enable reachability tracking (using **track TRACKID rtr ID reachability**).
- Define tracking on a static route (**route INTERFACENAME 0 0 IPGATEWAY track TRACKID**).

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
```

```

(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# sla monitor 3
(config-sla-monitor)# type echo protocol ipicmpecho 192.168.0.2 interface glasgow
(config-sla-monitor-echo)# frequency 10
(config-sla-monitor-echo)# num-packets 100
(config-sla-monitor-echo)# request-data-size 100
(config-sla-monitor-echo)# tos 10
(config-sla-monitor-echo)# timeout 100
(config-sla-monitor-echo)# threshold 100
(config-sla-monitor-echo)# exit
(config-sla-monitor)# exit
(config)# sla monitor 3 schedule life forever now
(config)# track 1 rtr 3 reachability
(config)# route Glasgow 0 0 192.168.0.2 track 1
(config)# exit
# show track
# show route

```

Example

```

# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# sla ?

```

configure mode commands/options:
 monitor IP Service Level Agreement Monitor

```
(config)# sla mon ?
```

```

configure mode commands/options:
 <1-2147483647> Entry Number
  schedule IP SLA Monitor Entry Scheduling
(config)# sla monitor 3
(config-sla-monitor)# type echo protocol ipicmpecho 192.168.0.2 interface glasgow
(config-sla-monitor-echo)# ?

```

IP SLA Monitor Echo Configuration Commands:

default	Set a command to its defaults
exit	Exit probe configuration
frequency	Frequency of an operation
no	Negate a command or set its defaults
num-packets	Number of Packets
request-data-size	Request data size
threshold	Operation threshold in milliseconds
timeout	Timeout of an operation
tos	Type Of Service
<cr>	

```
(config-sla-monitor-echo)# freq ?
```

sla-monitor-echo mode commands/options:
 <1-604800> Frequency in seconds

```
(config-sla-monitor-echo)# num ?
```

```

sla-monitor-echo mode commands/options:
  <1-100> Number of Packets to be transmitted

(config-sla-monitor-echo)# req ?

sla-monitor-echo mode commands/options:
  <0-16384> Number of bytes in payload

(config-sla-monitor-echo)# thre ?

sla-monitor-echo mode commands/options:
  <0-2147483647> Millisecond threshold value

(config-sla-monitor-echo)# timeout ?

sla-monitor-echo mode commands/options:
  <0-604800000> Timeout in milliseconds

(config-sla-monitor-echo)# tos ?

sla-monitor-echo mode commands/options:
  <0-255> Type of Service Value
(config-sla-monitor-echo)# frequency 10
(config-sla-monitor-echo)# num-packets 100
(config-sla-monitor-echo)# request-data-size 100
(config-sla-monitor-echo)# tos 10
(config-sla-monitor-echo)# timeout 100
(config-sla-monitor-echo)# threshold 100
(config-sla-monitor-echo)# exit
(config-sla-monitor)# exit
(config)# sla monitor schedule 3 life forever now
(config)# track 1 rtr 3 reachability
(config)# route Glasgow 0 0 192.168.0.2 track 1
(config)# exit
# show track
Track 1
  Response Time Reporter 142 reachability
  Reachability is UP
  3 changes, last change 02:31:36
  Latest operation return code: OK
  Latest RTT (millisecs) 0
  Tracked by:
    STATIC-IP-ROUTING 0
# show route
S   0.0.0.0 0.0.0.0 [1/0] via 192.168.0.2, glasgow
C   192.168.0.1 255.255.255.0 is directly connected, glasgow
C   192.168.1.1 255.255.255.0 is directly connected, inside
C   192.168.2.1 255.255.255.0 is directly connected, dmz

```

In this case the default gateway is at 192.168.0.2, and will be tracked for SLA 3.

Cisco ASA/PIX Challenge 104

Title: Favouring Static Routes with better Reachability, and using DHCP to track the default gateway.

Outline

This challenge uses DHCP to track the default route. The device will poll the DHCP server to determine the default route.

Objectives

The objectives of this challenge are to:

- Enable the SLA monitor process (with **sla monitor ID**).
- Define the reachability test (with **type echo protocol ipicmpecho IPDEST interface IFNAME**), which sends an ICMP packet require to a target IP address (IPDEST) on a given interface (IFNAME).
- Define optional test parameters, such as frequency of test, number of packets, request data size, Type-of-service (TOS), timeout and threshold.
- Run tests forever (with **sla monitor ID life forever now**).
- Enable reachability tracking (using **track TRACKID rtr ID reachability**).
- Define tracking on a static route (**route INTERFACENAME 0 0 IPGATEWAY track TRACKID**).
- Enable DHCP tracking.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# dhcp client route track 1
(config-if)# ip address dhcp setroute
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# sla monitor 3
(config-sla-monitor)# type echo protocol ipicmpecho 192.168.0.2 interface glasgow
(config-sla-monitor-echo)# frequency 10
(config-sla-monitor-echo)# num-packets 100
(config-sla-monitor-echo)# request-data-size 100
(config-sla-monitor-echo)# tos 10
(config-sla-monitor-echo)# timeout 100
(config-sla-monitor-echo)# threshold 100
(config-sla-monitor-echo)# exit
(config-sla-monitor)# exit
(config)# sla monitor 3 schedule life forever now
(config)# track 1 rtr 3 reachability
(config)# route Glasgow 0 0 192.168.0.2 track 1
(config)# exit
# show track
# show route
```

Example

```
# config t
(config)# int e0
(config-if)# nameif Glasgow
(config-if)# dhcp ?
```

```

interface mode commands/options:
  client DHCP client configuration

(config-if)# dhcp client ?

interface mode commands/options:
  route Options for routes installed by dhcp
  update Dynamically update information

(config-if)# dhcp client route ?

interface mode commands/options:
  distance Administrative distance for dhcp routes
  track Track dhcp routes

(config-if)# dhcp client route track ?

interface mode commands/options:
  <1-500> Tracked object number

(config-if)# dhcp client route track 1 ?

interface mode commands/options:
  <cr>

(config-if)# dhcp client route track 1

(config-if)# ip ?

interface mode commands/options:
  address Configure the ip address and mask for an interface

configure mode commands/options:
  audit Configure the Intrusion Detection System
  local Define a local pool of IP addresses
  verify Configure Unicast Reverse Path Filtering on an interface

(config-if)# ip address ?

interface mode commands/options:
  Hostname or A.B.C.D Firewall's network interface address
  dhcp Keyword to use DHCP to poll for information. Enables the
  DHCP client feature on the specified interface
  pppoe Keyword to use PPPoE to poll for information. Enables
  the PPPoE client feature on the specified interface

(config-if)# ip address dhcp ?

interface mode commands/options:
  setroute Keyword to set the default route using the default gateway
  parameter the DHCP server returns

  <cr>

(config-if)# ip address dhcp setroute
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# sla monitor 3
(config-sla-monitor)# type echo protocol ipicmp echo 192.168.0.2 interface glasgow
(config-sla-monitor-echo)# frequency 10
(config-sla-monitor-echo)# num-packets 100
(config-sla-monitor-echo)# request-data-size 100

```

```
(config-sla-monitor-echo)# tos 10
(config-sla-monitor-echo)# timeout 100
(config-sla-monitor-echo)# threshold 100
(config-sla-monitor-echo)# exit
(config-sla-monitor)# exit
(config)# sla monitor 3 schedule life forever now
(config)# track 1 rtr 3 reachability
(config)# route Glasgow 0 0 192.168.0.2 track 1
(config)# exit
# show track
# show route
```

Cisco ASA/PIX Challenge 105

Title: Favouring Static Routes with better Reachability, and using PPP over Ethernet (PPPoE) to track the default gateway.

Outline

This challenge uses PPPoE to track the default route. The device will use PPPoE to determine the default route.

Objectives

The objectives of this challenge are to:

- Enable the SLA monitor process (with **sla monitor ID**).
- Define the reachability test (with **type echo protocol ipicmpecho IPDEST interface IFNAME**), which sends an ICMP packet require to a target IP address (IPDEST) on a given interface (IFNAME).
- Define optional test parameters, such as frequency of test, number of packets, request data size, Type-of-service (TOS), timeout and threshold.
- Run tests forever (with **sla monitor ID life forever now**).
- Enable reachability tracking (using **track TRACKID rtr ID reachability**).
- Define tracking on a static route (**route INTERFACENAME 0 0 IPGATEWAY track TRACKID**).
- Enable PPPoE tracking.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# pppoe client route track 1
(config-if)# ip address pppoe setroute
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
```

```

(config)# sla monitor 3
(config-sla-monitor)# type echo protocol ipicmpecho 192.168.0.2 interface glasgow
(config-sla-monitor-echo)# frequency 10
(config-sla-monitor-echo)# num-packets 100
(config-sla-monitor-echo)# request-data-size 100
(config-sla-monitor-echo)# tos 10
(config-sla-monitor-echo)# timeout 100
(config-sla-monitor-echo)# threshold 100
(config-sla-monitor-echo)# exit
(config-sla-monitor)# exit
(config)# sla monitor 3 schedule life forever now
(config)# track 1 rtr 3 reachability
(config)# route Glasgow 0 0 192.168.0.2 track 1
(config)# exit
# show track

```

```
# show route
```

Example

```

# config t
(config)# int e0
(config-if)# nameif Glasgow
(config-if)# pppoe ?

interface mode commands/options:
  client  PPPoE client configuration

(config-if)# pppoe client ?

interface mode commands/options:
  route      Options for routes installed by pppoe
  secondary  Options for backup pppoe interfaces
  vpdn       Configure VPDN parameters

(config-if)# pppoe client route ?

interface mode commands/options:
  distance  Administrative distance for pppoe routes
  track     Track pppoe routes

(config-if)# pppoe client route track ?

interface mode commands/options:
  <1-500>   Tracked object number

(config-if)# pppoe client route track 1 ?

interface mode commands/options:
  <cr>

(config-if)# pppoe client route track 1

(config-if)# ip ?

interface mode commands/options:
  address   Configure the ip address and mask for an interface

configure mode commands/options:
  audit     Configure the Intrusion Detection System
  local     Define a local pool of IP addresses
  verify    Configure Unicast Reverse Path Filtering on an interface

```

```

(config-if)# ip address ?

interface mode commands/options:
  Hostname or A.B.C.D Firewall's network interface address
  dhcp                 Keyword to use DHCP to poll for information. Enables the
                       DHCP client feature on the specified interface
  pppoe                Keyword to use PPPoE to poll for information. Enables
                       the PPPoE client feature on the specified interface

(config-if)# ip address pppoe ?

interface mode commands/options:
  setroute             Keyword to set the default route using the default gateway
                       parameter the PPPoE server returns
  <cr>
(config-if)# ip address pppoe setroute ?

interface mode commands/options:
  <cr>

(config-if)# ip address pppoe setroute
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# sla monitor 3
(config-sla-monitor)# type echo protocol ipicmpecho 192.168.0.2 interface glasgow
(config-sla-monitor-echo)# frequency 10
(config-sla-monitor-echo)# num-packets 100
(config-sla-monitor-echo)# request-data-size 100
(config-sla-monitor-echo)# tos 10
(config-sla-monitor-echo)# timeout 100
(config-sla-monitor-echo)# threshold 100
(config-sla-monitor-echo)# exit
(config-sla-monitor)# exit
(config)# sla monitor 3 schedule life forever now
(config)# track 1 rtr 3 reachability
(config)# route Glasgow 0 0 192.168.0.2 track 1
(config)# exit
# show track
# show route

```

Cisco ASA/PIX Challenge 106

Title: Redistributing Routes in OSPF

Outline

The PIX/ASA can redistribute routers in OSPF using a route-map. OSPF is an excellent routing method, and uses a link-state algorithm to find the shortest path to every route. Each routing device maintains the same link-state routing database, for each interface and all the reachable interfaces. All routing decisions are based on a cost based on bandwidth or for route preference, rather than on simple methods, such as hop count (as used in RIP). Unfortunately OSPF is fairly heavy on CPU utilization. In this example two OSPF processes are run, and there is a redistribution of the subnets of the routes, before the processes.

Objectives

The objectives of this challenge are to:

- Define a route-map.
- Define OSPF routing details.
- Redistribute routes using the route-map.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# route-map testing permit
(config-route-map)# match metric 1
(config-route-map)# set metric 5
(config-route-map)# set metric-type type-1
(config-route-map)# set tag 1
(config-route-map)# exit
(config)# router ospf 111
(config-router)# network 192.168.0.0 255.255.255.0 area 0
(config-router)# redistribute ospf 1 route-map testing
(config-router)# exit
```

Example

```
(config)# route-map ?
```

```
configure mode commands/options:
  WORD < 58 char  Route map tag
```

```
(config)# route-map rtest ?
```

```
configure mode commands/options:
  <0-65535> Sequence to insert to/delete from existing route-map entry
  deny      Route map denies set operations
  permit    Route map permits set operations
  <cr>
```

```
(config)# route-map testing permit
```

```
(config-route-map)# ?
```

```
Route Map configuration commands:
```

```
  exit      Exit from route-map configuration mode
  help      Interactive help for route-map subcommands
  match     Match values from routing table
  no        Negate a command
  set       Set values in destination routing protocol
```

```
pixfirewall(config-route-map)# match ?
```

```
route-map mode commands/options:
```

```
  interface Match first hop interface of route
  ip         Match IP address or next-hop or route-source
```

```

metric      Match metric of route
route-type  Match route-type of route

(config-route-map)# match metric ?

route-map mode commands/options:
  <0-4294967295> Metric value

(config-route-map)# match metric 1

(config-route-map)# set ?

route-map mode commands/options:
  metric      Set metric value for destination routing protocol
  metric-type Set type of metric for destination routing protocol

(config-route-map)# set metric- ?

route-map mode commands/options:
  type-1  OSPF external type 1 metric
  type-2  OSPF external type 2 metric

(config-route-map)# set metric- type-1

(config-route-map)# set metric ?

route-map mode commands/options:
  <0-4294967295> Metric value
(config-route-map)# set metric 5

(config)# router ospf 111
(config-router)# redistribute ?

router mode commands/options:
  connected  Connected
  ospf       Open Shortest Path First (OSPF)
  static     Static routes
(config-router)# redistribute ospf 1 ?

router mode commands/options:
  match      Redistribution of OSPF routes
  metric     Metric for redistributed routes
  metric-type Set OSPF exterior metric type for redistributed routes
  route-map  Route map reference
  subnets   Consider subnets for redistribution into OSPF
  tag        Set tag for routes redistributed into OSPF
  <cr>

(config-router)# redistribute ospf 1 route-map ?

router mode commands/options:
  WORD Pointer to route-map entries

(config-router)# redistribute ospf 1 route-map rtest ?

router mode commands/options:
  match      Redistribution of OSPF routes
  metric     Metric for redistributed routes
  metric-type Set OSPF exterior metric type for redistributed routes
  subnets   Consider subnets for redistribution into OSPF
  tag        Set tag for routes redistributed into OSPF
  <cr>
(config-router)# redistribute ospf 1 route-map rtest

```

In this case:

```
(config)# route-map testing permit
(config-route-map)# match metric 1
(config-route-map)# set metric 5
(config-route-map)# set metric-type type-1
(config-route-map)# set tag 1
(config-route-map)# exit
(config)# router ospf 111
(config-router)# network 192.168.0.0 255.255.255.0 area 0
(config-router)# redistribute ospf 1 route-map testing
(config-router)# exit
```

will redistribute the routes from **OSPF process 1** into **OSPF process 111**, using a match metric of 1. The PIX/ASA will then redistribute these with a metric of 5, with a Type-1 metric tag, and a tag value of 1.

Cisco ASA/PIX Challenge 107

Title: Defining OSPF Interface Costs

Outline

With OSPF, each routing device maintains the same link-state routing database, for each interface and all the reachable interfaces. All routing decisions are based on a cost based on bandwidth or for route preference, rather than on simple methods, such as hop count (as used in RIP). In this challenge the OSPF costs are defined for an interface. For the interface, the **dead-interval** is the time that the device must wait before it declares that a neighboring device is down. Normally hello packets are passed, and if no hello packets are received with the dead-interval, it is declared as down. The length of time between transmitted hello packets is defined by the **hello-interval**. If OSPF MD5 authentication is used, the key is defined with a key ID and a key, using the ospf **message-digest-key** command. Also the priority of the OSPF device is defined so that the OSPF designated router can be found for the network. This uses the **priority** option of the ospf command in an interface. For simple pass phase authentication (OSPF password), the **authentication-key** option is used.

Objectives

The objectives of this challenge are to:

- Define a route-map.
- Define OSPF routing details.
- Redistribute routes using the route-map.

Commands

```

(config)# router ospf 111
(config-router)# network 10.0.0.0 255.0.0.0 area 0
(config-router)# exit
(config)# int e1
(config-if)# ospf cost 20
(config-if)# ospf retransmit-interval 20
(config-if)# ospf transmit-delay 20
(config-if)# ospf priority 20
(config-if)# ospf hello-interval 20
(config-if)# ospf dead-interval 20
(config-if)# ospf authentication-key test
(config-if)# ospf message-digest-key 1 md5 test
(config-if)# ospf authentication message-digest

```

Example

```

(config)# router ospf 111
(config-router)# network 10.0.0.0 255.0.0.0 area 0
(config-router)# exit
(config)# int e1
(config-if)# ospf ?

```

interface mode commands/options:

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

```

(config-if)# ospf cost ?

```

interface mode commands/options:

```
<1-65535> Cost
```

```

(config-if)# ospf cost 20

```

```

pixfirewall(config-if)# ospf retransmit-interval ?

```

interface mode commands/options:

```
<1-65535> Seconds
```

```

(config-if)# ospf retransmit-interval 20

```

```

(config-if)# ospf transmit-delay ?

```

interface mode commands/options:

```
<1-65535> Seconds
```

```

(config-if)# ospf transmit-delay 20

```

```

(config-if)# ospf priority ?

```

```

interface mode commands/options:
  <0-255> Priority

(config-if)# ospf priority 20

(config-if)# os he ?

interface mode commands/options:
  <1-65535> Seconds

(config-if)# ospf hello-interval 20

(config-if)# os de ?

interface mode commands/options:
  <1-65535> Seconds

(config-if)# ospf dead-interval 20

(config-if)# ospf authentication-key ?

interface mode commands/options:
  LINE < 9 char The OSPF password (key)

(config-if)# ospf authentication-key test

(config-if)# ospf message-digest-key ?

interface mode commands/options:
  <1-255> Key ID

(config-if)# ospf message-digest-key 1 ?

interface mode commands/options:
  md5 Use MD5 algorithm

(config-if)# ospf message-digest-key 1 md5 ?

interface mode commands/options:
  LINE < 17 char The OSPF password (key)

(config-if)# ospf message-digest-key 1 md5 test

(config-if)# ospf authentication ?

interface mode commands/options:
  message-digest Use message-digest authentication
  null          Use no authentication
  <cr>

(config-if)# ospf authentication message-digest
(config-if)# exit
(config)# exit
# sh ospf

Routing Process "ospf 1" with ID 1.2.3.4 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Does not support opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x 0
Number of opaque AS LSA 0. Checksum Sum 0x 0
Number of DCbitless external and opaque AS LSA 0

```

```
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area 1
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 1 times
    Area ranges are
    Number of LSA 1. Checksum Sum 0x ff12
    Number of opaque link LSA 0. Checksum Sum 0x 0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Cisco ASA/PIX Challenge 108

Title: Defining OSPF Area Details

Outline

With OSPF, the main area details include defining:

- **Authenication.** This provides protection against intruders with an OSPF authentication password.
- **Stub areas.** These are areas in which any information gained on external networks is not sent.
- **Default costs.**

Other features included in this challenge are:

Route Summarization. It is possible to summarize routes between OSPF areas, such as with:

```
(config-router)# area 10 range 2.3.4.0 255.255.0.0
```

command which cause a single route summarization to be sent for the network address of 2.3.4.0, which should cover all the networks within this area (10).

Default Route. In this case a boundary router generates a default route for the whole of the OSPF domain. For example:

```
(config-router)# default-information originate always
```

forces the boundary device to generate a default route for the OSPF routing domain.

Route Calculation Timers. This relates to the delays used with OSPF for topology changes, and for SPF (Shortest Path First) calculations. For example:

```
(config-router)# timers spf 10 20
```

defines a delay between receiving a change is the SPF calculation as 10 seconds, and a hold time between consecutive SPF calculations of 20 seconds.

Logging Neighbor state. This is used to log the state of neighboring devices. For example:

```
(config-router)# log-adj-changes detail
```

logs the neighbor state in detail.

Objectives

The objectives of this challenge are to:

- Define OSPF.
- Define OSPF routing area details.
- Define OSPF stub details.
- Define route timers.
- Define default route.
- Define logging of neighbors.

Outline

```
(config)# router ospf 111
(config-router)# area 1 authentication
(config-router)# area 1 authentication message-digest
(config-router)# area 10 stub
(config-router)# area 10 default-cost 15
(config-router)# summary-address 1.2.3.0 255.255.0.0
(config-router)# area 10 range 2.3.4.0 255.255.0.0
(config-router)# default-information originate always
(config-router)# log-adj-changes detail
(config-router)# timers spf 10 10
```

Example

```
(config)# router ospf 111
(config-router)# ?
```

Router configuration commands:

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

redistribute	Redistribute information from another routing process
router-id	router-id for this OSPF process
summary-address	Configure IP address summaries
timers	Adjust routing timers

(config-router)# area ?

router mode commands/options:

<0-4294967295>	OSPF area ID as a decimal value
A.B.C.D	OSPF area ID in IP address format

(config-router)# area 1 ?

router mode commands/options:

authentication	Enable authentication
default-cost	Set the summary default-cost of a NSSA/stub area
filter-list	Filter networks between OSPF areas
nssa	Specify a NSSA area
range	Summarize routes matching address/mask (border routers only)
stub	Specify a stub area
virtual-link	Define a virtual link and its parameters

<cr>

(config-router)# area 1 authentication

(config-router)# area 1 authentication ?

router mode commands/options:

message-digest	Use message-digest authentication
----------------	-----------------------------------

<cr>

(config-router)# area 1 authentication message-digest

(config-router)# area 10 stub

(config-router)# area 10 default-cost ?

router mode commands/options:

<0-65535>	Stub's advertised external route metric
-----------	---

(config-router)# area 10 default-cost 15

Route summarization allows for various routes to be summarized into a single address, and help to reduce the size of the routing tables:

(config-router)# summary-address ?

router mode commands/options:

A.B.C.D	IP summary address
---------	--------------------

(config-router)# summary-address 1.2.3.0 ?

router mode commands/options:

A.B.C.D	Summary mask
---------	--------------

(config-router)# summary-address 1.2.3.0 255.255.0.0

To summarize between OSPF areas:

(config-router)# area 10 range ?

router mode commands/options:

A.B.C.D	IP address to match
---------	---------------------

(config-router)# area 10 range 2.3.4.0 ?

router mode commands/options:

```
A.B.C.D IP mask for address  
(config-router)# area 10 range 2.3.4.0 255.255.0.0
```

To generate a default route:

```
(config-router)# default-information ?  
router mode commands/options:  
  originate  Distribute a default route  
  
(config-router)# default-information originate ?  
router mode commands/options:  
  always      Always advertise default route  
  metric      OSPF default metric  
  metric-type OSPF metric type for default routes  
  route-map   Route-map reference  
  <cr>  
  
(config-router)# default-information originate always  
  
(config-router)# log-adj-changes ?  
router mode commands/options:  
  detail  Log all state changes  
  <cr>  
(config-router)# log-adj-changes detail
```

For OSPF timers:

```
(config-router)# timers ?  
router mode commands/options:  
  lsa-group-pacing  OSPF LSA group pacing timer  
  spf                OSPF SPF timers  
  
(config-router)# timers spf ?  
router mode commands/options:  
  <1-65535>  Delay between receiving a change to SPF calculation  
  
(config-router)# timers spf 10 ?  
router mode commands/options:  
  <1-65535>  Hold time between consecutive SPF calculations  
  
(config-router)# timers spf 10 10
```

Cisco ASA/PIX Challenge 109

Title: Listening to RIP for Routing Information (Version 1)

Outline

The PIX/ASA devices can passively listen to RIP updates, using RIP Version 1 or RIP Version 2. RIP Version 1 only supports classful addressing, with unencrypted broadcasts, while RIP Version 2 supports classless addressing, and authentication. This challenge defines RIP Version 1.

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 interface details.
- Define RIP Version 1 on each of the interfaces.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# rip Glasgow passive version 1
```

Example

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# rip ?

configure mode commands/options:
Current available interface(s):
  Inf2      Name of interface Ethernet2
  Inside   Name of interface Ethernet1
  Glasgow  Name of interface Ethernet0
(config)# rip Glasgow ?

configure mode commands/options:
  default  Configure the system to advertise default route
  passive  Enable the system to passively listen to RIP updates

(config)# rip Glasgow passive ?

configure mode commands/options:
  version  RIP version, default is RIPv1
  <cr>
(config)# rip Glasgow passive version ?

configure mode commands/options:
  1  RIP Version 1 (RIPv1)
  2  RIP Version 2 (RIPv2)
```

```
(config)# rip Glasgow passive version 1 ?
```

configure mode commands/options:

```
<cr>
```

```
(config)# rip Glasgow passive version 1
```

Cisco ASA/PIX Challenge 110

Title: Listening to RIP for Routing Information (Version 2)

Outline

The PIX/ASA devices can passively listen to RIP updates, using RIP Version 1 or RIP Version 2. RIP Version 1 only supports classful addressing, with unencrypted broadcasts, while RIP Version 2 supports classless addressing, and authentication. This challenge defines RIP Version 2.

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 interface details.
- Define RIP Version 2 on each of the interfaces.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# rip Glasgow passive version 2 authentication text popup
```

Example

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# rip ?
```

configure mode commands/options:

Current available interface(s):

```

    Inf2      Name of interface Ethernet2
    Inside    Name of interface Ethernet1
    Glasgow   Name of interface Ethernet0
(config)# rip Glasgow ?

configure mode commands/options:
  default   Configure the system to advertise default route
  passive   Enable the system to passively listen to RIP updates

(config)# rip Glasgow passive ?

configure mode commands/options:
  version   RIP version, default is RIPv1
  <cr>
(config)# rip Glasgow passive version ?

configure mode commands/options:
  1         RIP Version 1 (RIPv1)
  2         RIP Version 2 (RIPv2)

(config)# rip Glasgow passive version 2 ?

configure mode commands/options:
  authentication  Authenticate using the specified mode
  <cr>

(config)# rip Glasgow version 2 authentication ?

configure mode commands/options:
  md5   Authenticate using md5 mode
  text  Authenticate using text mode

(config)# rip Glasgow passive version 2 authentication text ?

configure mode commands/options:
  WORD < 17 char  The shared key to be used for authentication
(config)# rip Glasgow passive version 2 authentication text popup

```

Cisco ASA/PIX Challenge 111

Title: RIP on a PIX/ASA device.

Outline

In the past, an PIX/ASA device could only **passively** listen to RIP updates, using RIP Version 1 or RIP Version 2, where RIP Version 1 supports classful addressing, with unencrypted broadcasts, and RIP Version 2 supports classless addressing, and authentication. Many PIX/ASA devices now fully support RIP.

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 interface details.
- Define RIP Version 2.
- Define RIP broadcast networks.
- Define a **passive interface**. In this mode the interface accepts RIP updates, but does not send them out.
- Generate a default route with the **default-information** command.
- Define RIP authentication details on an interface.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# rip authentication mode text
(config-if)# rip send version 2
(config-if)# rip receive version 2
(config-if)# rip authentication key test key-id 1
(config-if)# exit
(config)# router rip
(config-router)# network 192.168.0.0
(config-router)# network 192.168.1.0
(config-router)# version 2
(config-router)# passive-interface Glasgow
(config-router)# exit
```

Example

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# rip ?

interface mode commands/options:
 authentication Authentication control
 receive advertisement reception
 send advertisement transmission
(config-if)# rip a ?

interface mode commands/options:
 key Authentication key
 mode Authentication mode

(config-if)# rip a m ?

interface mode commands/options:
 md5 Keyed message digest
 text Clear text authentication

(config-if)# rip a m t ?
```

```

interface mode commands/options:
  <cr>

(config-if)# rip authentication mode text

(config-if)# rip r ?

interface mode commands/options:
  version version control

(config-if)# rip s ?

interface mode commands/options:
  version version control
(config-if)# rip s v ?

interface mode commands/options:
  1 RIP version 1
  2 RIP version 2

(config-if)# rip send version 2
(config-if)# rip receive version 2

(config-if)# rip a key ?

interface mode commands/options:
  WORD < 17 char The shared key to be used for authentication key string

(config-if)# rip a k test ?

interface mode commands/options:
  key_id Authentication key

(config-if)# rip a k test k ?

interface mode commands/options:
  <0-255> The shared key id that matches the key

(config-if)# rip a k test k 1 ?

interface mode commands/options:
  <cr>
(config-if)# rip authentication key test key-id 1
(config-if)# exit
(config)# router ?

configure mode commands/options:
  ospf Open Shortest Path First (OSPF)
  rip Routing Information Protocol (RIP)
(config)# router rip
(config-router)# ?

Router configuration commands:
  auto-summary Enable automatic network number summarization
  default-information Control distribution of default information
  distribute-list Filter networks in routing updates
  exit Exit from router configuration mode
  help Interactive help for router subcommands
  network Add/remove interfaces to/from routing process
  no Negate a command
  passive-interface Suppress routing updates on an interface
  redistribute Redistribute information from another routing process
  version Set routing protocol version

```

```
(config-router)# network ?

router mode commands/options:
  Hostname or A.B.C.D Network address
(config-router)# network 192.168.0.0
(config-router)# network 192.168.1.0
(config-router)# version ?

router mode commands/options:
  <1-2> version

exec mode commands/options:
  /md5    Compute an MD5 signature for a file
  disk0:  File to be verified
  flash:  File to be verified
(config-router)# version 2
(config-router)# default-information ?

router mode commands/options:
  originate Distribute a default route
(config-router)# default-information o ?

router mode commands/options:
  route-map Route-map reference
  <cr>
(config-router)# default-information originate
(config-router)# passive-interface ?

router mode commands/options:
Current available interface(s):
  default Suppress routing updates on all interfaces
  Glasgow Name of interface ETHERNET0
  Inside Name of interface ETHERNET1
  Inf2 Name of interface ETHERNET2
  <cr>

(config-router)# passive-interface Glasgow
(config-router)# exit
```

Cisco ASA/PIX Challenge 112

Title: Enabling and configuring EIGRP

Outline

ASA 8.x brought many new features to the range, including:

- EIGRP routing.
- High-availability functionality.
- SSL VPN enhancements.
- SSL VPN support for Windows Vista and Mac OS X clients is now available.
- AnyConnect VPN client.
- Local certificate authority.

- VPN load balancing.
- Additional browser-based SSL VPN features.
- Transparent NAT.

The PIX/ASA devices can thus enable EIGRP routing, which is an enhancement of IGRP. The main advantage of this protocol is that it only sends out routing information when there is a change in the topology. EIPGRP is one of the new features of the PIX/ASA device.

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 interface details.
- Define EIGRP routing and the networks in which to broadcast into (that is, the networks which participate in the EIGRP routing process).
- Define EIGRP authentication on E0.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# authentication mode eigrp 111 md5
(config-if)# authentication key eigrp 111 testing key-id 1
(config-if)# exit
(config)# router eigrp 111
(config-router)# network 192.168.0.0
(config-router)# network 192.168.1.0
```

Example

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# authentication mode eigrp 111 md5
(config-if)# authentication key eigrp 111 testing key-id 1
(config-if)# exit
(config)# router eigrp 111
(config-router)# network 192.168.0.0
(config-router)# network 192.168.1.0
```

Cisco PIX Test (Challenge 113)

Outline

This challenge involves taking a PIX test on routing protocols. The main facts are:

- PIX/ASA have used RIP and OSPF, and have now added EIGRP.
- RIP uses hop count to determine the best route.
- OSPF uses a link-state algorithm to determine the best route.
- OSPF uses the DUAL algorithm to determine the best route.

Cisco ASA/PIX Challenge 114

Title: DHCP Server on a PIX/ASA.

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.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# dhcpd enable glasgow
(config)# dhcpd dns 197.174.60.1
(config)# dhcpd address 197.174.60.2-197.174.60.22 glasgow
(config)# dhcpd wins 195.94.110.3
(config)# dhcpd lease 6
(config)# dhcpd domain athome.com
(config)# show dhcpd
```

Example

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
```

```

(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# dhcpd ?

configure mode commands/options:
  address      Configure the IP pool address range after this keyword
  auto_config  Enable auto configuration from client
  dns          Configure the IP addresses of the DNS servers after this
              keyword
  domain       Configure DNS domain name after this keyword
  enable       Enable the DHCP server
  lease        Configure the DHCPD lease length after this keyword
  option       Configure options to pass to DHCP clients after this keyword
  ping_timeout Configure ping timeout value after this keyword
  wins         Configure the IP addresses of the NETBIOS servers after this
              keyword
pixfirewall(config)# dhcpd enable ?

configure mode commands/options:
Available interfaces on which to enable the DHCP server:
  Glasgow      Name of interface ETHERNET0
  Inside       Name of interface ETHERNET1
  Inf2         Name of interface ETHERNET2
  <cr>

(config)# dhcpd enable glasgow
(config)# dhcpd dn ?

configure mode commands/options:
  Hostname or A.B.C.D  IP address of server 1
(config)# dhcpd dns 197.174.60.1
(config)# dhcpd add ?

configure mode commands/options:
  WORD  IP address[es], <ip1>[-<ip2>]
(config)# dhcpd address 197.174.60.2-197.174.60.22 glasgow
(config)# dhcpd wins ?

configure mode commands/options:
  Hostname or A.B.C.D  IP address of server 1

(config)# dhcpd wins 195.94.110.3
(config)# dhcpd lease ?

configure mode commands/options:
  <300-1048575>  The length of lease, in seconds, granted to DHCP client
                 from the DHCP server, default is 3600
(config)# dhcpd lease 6
(config)# dhcpd domain ?

configure mode commands/options:
  WORD  DNS domain name
(config)# dhcpd domain athome.com
(config)# show dhcpd

```

Cisco ASA/PIX Challenge 115

Title: Configuring DHCP server options for Cisco IP phones

Outline

Cisco IP phones download their configuration from TFTP servers, which are not preconfigured on them. Thus they send a DHCP request with an option field set to **150** (for a list of TFTP servers) or **66** (for a single TFTP server) to discover the address for their configuration. Also they may request the default gateway with an option of **3**.

Objectives

The objectives of this challenge are to:

- Enable the DHCP server.
- Define DHCP parameters.
- Define default TFTP server for DHCP option 150.
- Define default TFTP server for DHCP option 66.
- Define default gateway server for DHCP option 3.
- Show DHCP parameters.

Commands

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# dhcpd enable glasgow
(config)# dhcpd dns 197.174.60.1
(config)# dhcpd address 197.174.60.2-197.174.60.22 glasgow
(config)# dhcpd wins 195.94.110.3
(config)# dhcpd lease 6
(config)# dhcpd domain athome.com
(config)# dhcpd option 150 ip 192.168.0.1
(config)# dhcpd option 66 ascii 192.168.0.1
(config)# dhcpd option 3 ip 192.168.0.2
(config)# show dhcpd
```

Example

```
# config t
(config)# int e0
(config-if)# nameif glasgow
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# security-level 0
(config-if)# exit
(config)# dhcpd ?
```

configure mode commands/options:

address Configure the IP pool address range after this keyword

```

auto_config  Enable auto configuration from client
dns          Configure the IP addresses of the DNS servers after this
            keyword
domain       Configure DNS domain name after this keyword
enable       Enable the DHCP server
lease        Configure the DHCPD lease length after this keyword
option       Configure options to pass to DHCP clients after this keyword
ping_timeout Configure ping timeout value after this keyword
wins         Configure the IP addresses of the NETBIOS servers after this
            keyword
pixfirewall(config)# dhcpd enable ?

configure mode commands/options:
Available interfaces on which to enable the DHCP server:
  Glasgow  Name of interface ETHERNET0
  Inside   Name of interface ETHERNET1
  Inf2     Name of interface ETHERNET2
  <cr>

(config)# dhcpd enable glasgow
(config)# dhcpd dn ?

configure mode commands/options:
  Hostname or A.B.C.D  IP address of server 1
(config)# dhcpd dns 197.174.60.1
(config)# dhcpd add ?

configure mode commands/options:
  WORD  IP address[es], <ip1>[-<ip2>]
(config)# dhcpd address 197.174.60.2-197.174.60.22 glasgow
(config)# dhcpd wins ?

configure mode commands/options:
  Hostname or A.B.C.D  IP address of server 1

(config)# dhcpd wins 195.94.110.3
(config)# dhcpd lease ?

configure mode commands/options:
  <300-1048575>  The length of lease, in seconds, granted to DHCP client
                from the DHCP server, default is 3600
(config)# dhcpd lease 6
(config)# dhcpd domain ?

configure mode commands/options:
  WORD  DNS domain name
(config)# dhcpd domain athome.com
(config)# dhcpd option ?

configure mode commands/options:
  <0-255>  DHCP option code

ciscoasa(config)# dhcpd option 150 ?

configure mode commands/options:
  ascii  Configure the option information in ascii after this keyword
  hex    Configure the option information as a hexadecimal value after this
        keyword
  ip     Configure the option information as IP address(es) after this keyword
  <cr>
ciscoasa(config)# dhcpd option 150 ip ?

configure mode commands/options:

```

```
Hostname or A.B.C.D IP address of server 1

(config)# dhcpd option 150 ip 192.168.0.1
(config)# dhcpd option 66 ascii ?

configure mode commands/options:
WORD ASCII string without whitespace

(config)# dhcpd option 66 ascii 192.168.0.1
(config)# dhcpd option 3 ip 192.168.0.2
(config)# show dhcpd
```

Cisco PIX/ASA Challenge 116

Title: Configuring DHCP Relay Services

Outline

This challenge involves defining DHCP relay, where DHCP requests can be forwarded to a certain interface. DHCP relay is used to send DHCP requests from clients to a destination DHCP device. Thus DHCP servers to be placed outside local networks, and the PIX/ASA device is then used to point to the required server. For DHCP relay, there must be no DHCP server on the same interface. Also, for security purposes, clients cannot send their DHCP requests through the PIX/ASA, and all requests must come through it.

Objectives

The objectives of this challenge are to:

- Define interface details.
- Enable the DHCP relay service on an interface (**dhcprelay enable** interfaceName).
- Define a timeout for the address negotiation (**dhcprelay timeout** seconds).
- Define the router gateway address, instead of the DHCP gateway reply to a PIX/ASA interface (**dhcprelay setroute** interfaceName). Thus the PIX/ASA device can be made to be the default gateway, even though the DHCP server has defined another gateway.

Commands

```
# config t
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# nameif Edinburgh
(config-if)# exit
(config)# dhcprelay server 192.168.1.2
(config)# dhcprelay enable Edinburgh
(config)# dhcprelay timeout 10
```

```
(config)# exit
# show dhcprelay statistics
# show dhcprelay state
```

Example

```
# config t
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# nameif Edinburgh
(config-if)# exit
(config)# dhcprelay ?

configure mode commands/options:
  enable      Start a DHCP server task on an interface, but at least one
              dhcpdrelay server must be configured before enable is issued
  server      Configure dhcprelay server information
  setroute    Configure the DHCP Relay Agent to change the first default
              router address (in the packet sent from the DHCP server) to
              the address of the client interface
  timeout     Configure timeout, the number of seconds for relay address
              negotiation after this keyword

configure mode commands/options:
  infinity    Always stay on shared-tree
(config)# dhcprelay server ?

configure mode commands/options:
  Hostname or A.B.C.D  IP address of dhcprelay server to which
                      requests are forwarded
(config)# dhcprelay server 192.168.1.2
(config)# dhcprelay setroute ?

configure mode commands/options:
Available client interface names:
  Inf2        Name of interface Ethernet2
  Inside      Name of interface Ethernet1
  Edinburgh   Name of interface Ethernet0
(config)# dhcprelay enable ?

configure mode commands/options:
Available interfaces on which relay agent will accept client requests:
  Inf2        Name of interface Ethernet2
  Inside      Name of interface Ethernet1
  Edinburgh   Name of interface Ethernet0
(config)# dhcprelay enable Edinburgh
(config)# dhcprelay timeout ?

configure mode commands/options:
  <1-3600>    Enter number of seconds for relay address negotiation, default
              is 60 seconds
  <cr>
(config)# dhcprelay timeout 10
(config)# exit

# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
Packets Relayed
BOOTREQUEST          0
DHCPCDISCOVER        7
```

```
DHCPREQUEST      3
DHCPDECLINE      0
DHCPRELEASE      0
DHCPINFORM       0
BOOTREPLY        0
DHCPOFFER        7
DHCPACK          3
```

```
# show dhcprelay state
```

```
Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface inf, Configured for DHCP RELAY SERVER
Interface Edinburgh, Configured for DHCP RELAY
```

Cisco PIX/ASA Challenge 117

Title: Configuring Dynamic DNS (DDNS)

Outline

DDNS is a service which integrates DNS and DHCP, where the DHCP service allocates IP addresses based on physical addresses, while DNS resolves hostnames to IP addresses, or vice-versa. A DDNS name and address mapping are held within the DHCP server using the following records:

- **A RR** (Resource Record), which is the name to IP address mapping.
- **PTR RR** record, which maps addresses to names.

The main application of DDNS is where hosts are continually changing their IP address (such as in mobile applications), and hosts can still find each other. The mapping is thus held on a DHCP server. The main advantage of DDNS is that a host can notify a DHCP server of a change of the active DNS configuration of its configured parameters, such as, typically, for hostnames and addresses. The most common DDNS setups are where the DHCP client updates the A RR, and the DHCP server updates PTR RR, and where the DHCP server updates both.

In this example the client updates both A RR and PTR RR for a defined static IP address.

Objectives

The objectives of this challenge are to:

- Define interface details.
- Define a static IP address on E0 (the static IP address).

- Define a DDNS update method for the client to update both the A RR and the PTR RR using the **ddns both** command.
- Associate the DDNS update method with an interface.

Commands

In this example the hostname is defined as myddns.com, which will associate with an IP address of 192.168.1.1:

```
# config t
(config)# ddns update method myddns
(DDNS-update-method)# ddns both
(DDNS-update-method)# exit
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# nameif Edinburgh
(config-if)# ddns update myddns
(config-if)# ddns update hostname myddns.com
(config-if)# exit
(config)# exit
```

Example

```
# config t
(config)# ddns ?

configure mode commands/options:
  update  Configure dynamic DNS update

(config)# ddns update ?

configure mode commands/options:
  method  Configure dynamic DNS update method

(config)# ddns update method ?

configure mode commands/options:
  WORD    Dynamic DNS update method name
(config)# ddns update method myddns
(DDNS-update-method)# ?

Dynamic DNS update method configuration commands:
  ddns    IETF standardized Dynamic DNS update
  exit    Exit from DNS dynamic update method configuration mode
  help    Help for Dynamic DNS update method configuration commands
  interval Specify interval between DNS updates
  no      Negate a command or set its defaults
(DDNS-update-method)# ddns ?

dynupd-method mode commands/options:
  both    Update both DNS A and PTR records
  <cr>

configure mode commands/options:
  update  Configure dynamic DNS update

(DDNS-update-method)# ddns both ?
```

```

dynupd-method mode commands/options:
  <cr>
(DDNS-update-method)# ddns both
(DDNS-update-method)# inter ?

dynupd-method mode commands/options:
  maximum Specify maximum interval between DNS updates

configure mode commands/options:
  Ethernet IEEE 802.3
  Vlan Catalyst Vlans
  <cr>
(DDNS-update-method)# inter max ?

dynupd-method mode commands/options:
  <0-364> Days

(DDNS-update-method)# help ddns

USAGE:
  [no] ddns [both]

DESCRIPTION:
  ddns IETF standardized Dynamic DNS update

SYNTAX:
  both Update both DNS A and PTR records

(DDNS-update-method)# exit
(config)# int e0
(config-if)# ddns ?

interface mode commands/options:
  update Configure dynamic DNS update

configure mode commands/options:
  update Configure dynamic DNS update

(config-if)# ddns update ?

interface mode commands/options:
  WORD Method name
  hostname Dynamic DNS update hostname

configure mode commands/options:
  method Configure dynamic DNS update method

(config-if)# ddns update host ?

interface mode commands/options:
  WORD Update DNS address records for this hostname

(config-if)# ddns u myddns?

interface mode commands/options:
  <cr>

(config-if)# nameif Edinburgh
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# ddns update myddns
(config-if)# ddns update hostname myddns.com
(config-if)# exit

```

```
(config)# exit
```

Cisco PIX/ASA Challenge 118

Title: Configuring Dynamic DNS (DDNS) – for Client Updates on A RR and PTR RR, where the DHCP server implements the update request.

Outline

In this example of DDNS, the client updates both A RR and PTR RR and the DHCP server honors the client update request.

The objectives of this challenge are to:

- Define interface details.
- Define a DHCP entry on the interface.
- Define a DDNS update method for the client to update both the A RR and the PTR RR using the **ddns both** command.
- Associate the DDNS update method with an interface.
- Define that the DHCP client requests that the DHCP does not make any updates (using **dhcp-client update dns server none**).

Commands

```
# config t
(config)# dhcp-client update dns server none
(config)# ddns update method myddns
(DDNS-update-method)# ddns both
(DDNS-update-method)# exit
(config)# int e0
(config-if)# ip address dhcp
(config-if)# nameif Edinburgh
(config-if)# ddns update myddns
(config-if)# ddns update hostname myddns.com
(config-if)# exit
(config)# exit
```

Example

```
# config t
(config)# dhcp-client ?
configure mode commands/options:
  update  Configure automatic updates
(config)# dhcp-client update ?
configure mode commands/options:
```

```

    dns    Configure DNS dynamic update information

(config)# dhcp-client update dns ?

configure mode commands/options:
  server  Configure requested server dynamic DNS updates
  <cr>
(config)# dhcp-client update dns server ?

configure mode commands/options:
  both   Server updates both (A and PTR) records
  none   Ask server to perform no updates

(config)# dhcp-client update dns server none

(config)# ddns ?

configure mode commands/options:
  update  Configure dynamic DNS update

(config)# ddns update ?

configure mode commands/options:
  method  Configure dynamic DNS update method

(config)# ddns update method ?

configure mode commands/options:
  WORD    Dynamic DNS update method name
(config)# ddns update method myddns
(DDNS-update-method)# ?

Dynamic DNS update method configuration commands:
  ddns    IETF standardized Dynamic DNS update
  exit    Exit from DNS dynamic update method configuration mode
  help    Help for Dynamic DNS update method configuration commands
  interval Specify interval between DNS updates
  no      Negate a command or set its defaults
(DDNS-update-method)# ddns ?

dynupd-method mode commands/options:
  both   Update both DNS A and PTR records
  <cr>

configure mode commands/options:
  update  Configure dynamic DNS update

(DDNS-update-method)# ddns both
(DDNS-update-method)# exit
(config)# int e0
(config-if)# ddns ?

interface mode commands/options:
  update  Configure dynamic DNS update

configure mode commands/options:
  update  Configure dynamic DNS update

(config-if)# ddns update ?

interface mode commands/options:
  WORD    Method name
  hostname Dynamic DNS update hostname

```

```

configure mode commands/options:
  method Configure dynamic DNS update method

(config-if)# ddns update host ?

interface mode commands/options:
  WORD Update DNS address records for this hostname

(config-if)# ddns u myddns?

interface mode commands/options:
  <cr>

(config-if)# nameif Edinburgh
(config-if)# ip address ?

interface mode commands/options:
  Hostname or A.B.C.D Firewall's network interface address
  dhcp Keyword to use DHCP to poll for information. Enables the
  DHCP client feature on the specified interface
  pppoe Keyword to use PPPoE to poll for information. Enables
  the PPPoE client feature on the specified interface

(config-if)# ip address dhcp
(config-if)# ddns update myddns
(config-if)# ddns update hostname myddns.com
(config-if)# exit
(config)# exit

```

Cisco PIX/ASA Challenge 119

Title: Configuring Dynamic DNS (DDNS) – for Client instructs the server not to update on A RR and PTR RR.

Outline

In this example of DDNS, the client instructs the server not to update on A RR and PTR RR.

The objectives of this challenge are to:

- Define interface details.
- Define a DHCP entry on the interface (using **ip address dhcp** and **dhcp client update dns server none**).
- Enable the DHCP server to override client update requests (using **dhcpd update dns both override**).
- Define a DDNS update method for the client to update both the A RR and the PTR RR using the **ddns both** command.
- Associate the DDNS update method with an interface.

Commands

```

# config t
(config)# dhcpd update dns both override
(config)# ddns update method myddns
(DDNS-update-method)# ddns both
(DDNS-update-method)# exit
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ddns update myddns
(config-if)# ddns update hostname myddns.com
(config-if)# dhcp client update dns server none
(config-if)# ip address dhcp
(config-if)# exit
(config)# exit

```

Example

```

# config t
pixfirewall(config)# dhcpd ?

configure mode commands/options:
  address      Configure the IP pool address range after this keyword
  auto_config  Enable auto configuration from client
  dns          Configure the IP addresses of the DNS servers after this
              keyword
  domain       Configure DNS domain name after this keyword
  enable       Enable the DHCP server
  lease        Configure the DHCPD lease length after this keyword
  option       Configure options to pass to DHCP clients after this keyword
  ping_timeout Configure ping timeout value after this keyword
  wins         Configure the IP addresses of the NETBIOS servers after this
              keyword

(config)# dhcpd u ?

configure mode commands/options:
  dns  Configure DNS dynamic updates

(config)# dhcpd u d ?

configure mode commands/options:
  both      Update both A and PTR DNS records
  interface Specify interface to which action will apply to
  override  Server overrides client request
  <cr>

(config)# dhcpd u d b ?

configure mode commands/options:
  interface Specify interface to which action will apply to
  override  Server overrides client request
  <cr>
(config)# dhcpd update dns both override
(config)# ddns update method myddns
(DDNS-update-method)# ddns both
(DDNS-update-method)# exit
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address dhcp
(config-if)# ddns update myddns
(config-if)# ddns update hostname myddns.com

```

```
(config-if)# dhcp c ?  
  
interface mode commands/options:  
  route  Options for routes installed by dhcp  
  update Dynamically update information  
  
(config-if)# dhcp c u ?  
  
interface mode commands/options:  
  dns    Dynamic DNS update configuration  
  
(config-if)# dhcp c u d ?  
  
interface mode commands/options:  
  server Dynamic DNS updates requested of server  
  <cr>  
  
(config-if)# dhcp c u d s ?  
  
interface mode commands/options:  
  both  Server updates both (A and PTR) records  
  none  Ask server to perform no updates  
  
(config-if)# exit  
(config)# exit
```

Cisco PIX/ASA Challenge 120

Title: WCCP (Web Cache Communications Protocol)

Outline

WCCP is a Cisco-derived protocol which stores previously access Web pages in a Web-cache, which can then be accessed, rather than the remote page, when users re-request the page.

The objectives of this challenge are to:

- Define interface details.
- Enable WCCP (wccp web-cache).
- Define that Web traffic (on port 80) that enters from the outside interface is redirected to a web cache.

Commands

```
# config t
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# exit
(config)# wccp web-cache
(config)# wccp interface Edinburgh web-cache redirect in
(config)# exit
```

Example

```
# config t
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address dhcp
(config-if)# exit
(config)# wccp ?
```

configure mode commands/options:
<0-254> Dynamically defined service identifier number
interface Keyword to specify an interface
web-cache Standard web caching service

```
(config)# wccp web ?
```

configure mode commands/options:
group-list Set the access-list used to permit group membership
password Authentication password (key)
redirect-list Set the access-list used to permit redirection
<cr>

```
(config)# wccp web-cache
```

```
(config)# wccp interface ?
```

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

```
(config)# wccp in Edinburgh ?
```

configure mode commands/options:
<0-254> Dynamically defined service identifier number
web-cache Standard web caching service

```
(config)# wccp in Edinburgh web-cache ?
```

configure mode commands/options:
redirect Set packet redirection options for the service

```
(config)# wccp in Edinburgh web-cache redirect ?
```

configure mode commands/options:
in Redirect to a Cache Engine appropriate ingress packets

```
(config)# wccp in Edinburgh web-cache redirect in ?
```

configure mode commands/options:
<cr>

```
(config)# wccp interface Edinburgh web-cache redirect in
(config)# exit
```

Cisco PIX/ASA Test (Challenge 121)

Outline

This challenge involves taking a PIX test on DHCP, DDNS and WCCP. The main facts are:

- DHCP allocates IP addresses based on client MAC addresses.
- DDNS supports the updating of IP information.
- WCCP allows Web requests to be forwarded to a web cache, if the page already exists in the cache.

Cisco PIX/ASA Challenge 122

Title: Multicast Routing

Outline

Multicast allows a sender to send packets to multiple recipients, which is useful in reducing bandwidth. These use special multicast addresses of 224.0.0.0/4 (Class D), which spans from 224.0.0.0 to 239.255.255.255. Subscribers then join groups using the **Internet Group Management Protocol** (IGMP) protocol to alert local multicast routers. IGMP is a fairly simple protocol and consists of:

- A version number.
- A type.
- A checksum.
- Group. This is the multicast address to be joined.

Thus when a multicast packet is sent, the multicast router will then know that at least one of the host that are interested in receiving packets for a specific multicast address. The router then requires to implement multicast routing between the routers in order to get the data packet to the host(s).

Multicast routing protocols typically work on two main methods:

- **Dense mode.** This works by flooding data into the network and then pruning back parts of the tree. This tree represent a set of routers, and the more pruning that is done, the smaller the tree, and the less bandwidth will be wasted in sending multicast packets. Thus if there are no branches of interested within an AS, the border router sends a prune message to the upstream router.
- **Sparse mode.** This uses a Rendezvous Point (RP), where join messages are sent to the RP's unicast address. It cuts down bandwidth, and is efficient, but requires careful configuration on devices.

The main multicast routing mechanisms are:

- **DVMRP** (Distance Vector Multicast Routing Protocol). DVMRP uses IGMP sub-code 13, and implements **Dense Flooding**, which is effective, but not inefficient in its usage of bandwidth. With this the router floods the whole network at the start, and then prune back subnets that are not of interest.
- **PIM** (Protocol Independent Multicast). PIM uses IP protocol 103. In dense mode operation it operates like DVMRP. It implements joins, prunes, and grafts, where a graft is the opposite of a prune, and adds a branch back onto the tree.

The objectives of this challenge are to:

- Enable multicast routing. When this is enabled on the device, IGMP Version 2 is automatically enabled on the interfaces.
- Disable IGMP on E1. This is useful in cutting down on excess traffic, if an interface is not used for multicast traffic.

Commands

```
# config t
(config)# multicast-routing
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int e1
(config-if)# nameif Glasgow
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# no igmp
(config-if)# exit
```

Example

```
# config t
(config)# multicast-routing
```

```
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int e1
(config-if)# nameif Glasgow
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# no igmp
(config-if)# exit
```

Cisco PIX/ASA Challenge 123

Title: Multicast Group Membership

Outline

The PIX/ASA can become part of a multicast group using the IGMP protocol on an interface, and defining the group-group (**igmp join-group** address). Also multicast traffic can be sent to a network segment using a statically joined group (**igmp static-group** address). The objectives of this challenge are to:

- Enable multicast routing.
- Configure the Ethernet ports.
- Configure **join-group** membership on E0. With join-group memberships, the PIX/ASA accepts and forwards all multicast packets to the defined interface.
- Configure **static-group** membership on E1. With the static-group membership, the PIX/ASA does not accept multicast packet, but forwards them to the defined interface.
- Show IGMP traffic.

Commands

```
# config t
(config)# multicast-routing
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# igmp join-group 224.0.0.1
(config-if)# exit
(config)# int e1
(config-if)# nameif Glasgow
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# igmp static-group 224.0.0.1
(config-if)# exit
```

Example

```

# config t
(config)# multicast-routing
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# igmp ?

```

interface mode commands/options:

```

access-group          group membership access
forward              forward
join-group           join multicast group
limit                host join limit
query-interval       host query interval
query-max-response-time max query response value
query-timeout        previous querier timeout
static-group         static multicast group
version              version
<cr>

```

```
(config-if)# igmp join-group ?
```

interface mode commands/options:

```
A.B.C.D IP group address
```

```

(config-if)# igmp join-group 224.0.0.1
(config-if)# exit
(config)# int e1
(config-if)# nameif Glasgow
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# igmp static-group ?

```

interface mode commands/options:

```
A.B.C.D IP group address
```

```

(config-if)# igmp static-group 224.0.0.1
(config-if)# exit
(config)# exit

```

```
# show igmp traffic
```

IGMP Traffic Counters

Elapsed time since counters cleared: 00:00:35

	Received	Sent
Valid IGMP Packets	10	4
Queries	5	0
Reports	2	0
Leaves	0	0
Mtrace packets	0	0
DVMRP packets	0	0
PIM packets	30	0

Errors:

Malformed Packets	0
Martian source	0
Bad Checksums	0

Cisco PIX/ASA Challenge 124

Title: Controlling Access to Multicast Group Membership using Access-lists

Outline

The PIX/ASA can use access-lists to define the groups that hosts will join (using the **igmp access-list** listno command on the defined interface).

- Enable multicast routing.
- Configure the Ethernet ports.
- Configure an extended access-list which define the hosts that can join multicast groups.
- Define the limit of the number of IGMP host that can join on a per interface basis.
- Define the Query Interval, which is the time that the PIX/ASA waits between sending out messages to discover multicast groups (**igmp query-interval** time).
- Define the Query Timeout, which is the time that the PIX/ASA will wait before it will assume that it is the designated router and will start sending query messages (**igmp query-timeout** time).

Commands

```
# config t
(config)# multicast-routing
(config)# access-list 100 permit igmp host 20.10.10.1 host 224.0.0.1
(config)# int e0
(config-if)# nameif Edinburgh
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
(config-if)# igmp access-group 100
(config-if)# igmp join-group 224.0.0.1
(config-if)# igmp limit 20
(config-if)# igmp query-interval 100
(config-if)# igmp query-timeout 100
(config-if)# exit
(config)# int e1
(config-if)# nameif Glasgow
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# igmp static-group 224.0.0.1
(config-if)# exit
```

Example

```
# config t
(config)# multicast-routing
(config)# access-list ?
```

configure mode commands/options:

```
WORD < 241 char Access list identifier
alert-interval Specify the alert interval for generating syslog message
106001 which alerts that the system has reached a deny
flow maximum. If not specified, the default value is 300 sec
```

deny-flow-max Specify the maximum number of concurrent deny flows that can be created. If not specified, the default value is 4096

(config)# access-list 100 ?

configure mode commands/options:

deny Specify packets to reject
ethertype Configure access policy for non IP traffic through the system when configured in transparent mode
extended Configure access policy for IP traffic through the system
line Use this to specify line number at which ACE should be entered
permit Specify packets to forward
remark Specify a comment (remark) for the access-list after this keyword
standard Use this to configure policy having destination host or network only
webtype Use this to configure WebVPN related policy

(config)# access-1 100 permit ?

configure mode commands/options:

<0-255> Enter protocol number (0 - 255)
Hostname or A.B.C.D Match based on destination network address
ah
any Abbreviation for an address and mask of 0.0.0.0 0.0.0.0
eigrp
esp
gre
host Use this keyword to configure destination host
icmp
icmp6
igmp
igrp
ip
ipinip
ipsec
nos
object-group Specify a protocol object-group after this keyword
ospf
pcp
pim
pptp
snp
tcp
udp

(config)# access-1 100 permit igmp ?

configure mode commands/options:

Hostname or A.B.C.D Source IP address
any Abbreviation for source address and mask of 0.0.0.0 0.0.0.0
host Use this keyword to configure source host
interface Use interface address as source address
object-group Network object-group for source address

(config)# access-list 100 permit igmp host 20.10.10.1 host 224.0.0.1

(config)# int e0

(config-if)# nameif Edinburgh

(config-if)# ip address 192.168.0.1 255.255.255.0

(config-if)# no shutdown

```

(config-if)# igmp access-group ?

interface mode commands/options:
  WORD Named access list specifying access group range

(config-if)# igmp access-group 100
(config-if)# igmp join-group 224.0.0.1
(config-if)# igmp limit ?

interface mode commands/options:
  <0-500> Number of IGMP hosts that can join

(config-if)# igmp limit 20
(config-if)# igmp query-interval ?

interface mode commands/options:
  <1-3600> Query interval in seconds

(config-if)# igmp query-interval 100
(config-if)# igmp query-t ?

interface mode commands/options:
  <60-300> timeout value in seconds
(config-if)# igmp query-timeout 100
(config-if)# exit
(config)# int e1
(config-if)# nameif Glasgow
(config-if)# ip address 192.168.0.2 255.255.255.0
(config-if)# no shutdown
(config-if)# igmp static-group 224.0.0.1
(config-if)# exit

```

Cisco PIX/ASA Challenge 125

Title: Enabling and configuring PIM (Protocol Independent Multicast) for Sparse Mode

Outline

With multicast, PIM is used to construct a multicast distribution tree of an IP multicast group. For this it uses these multicast distribution trees so that data packets from senders to a multicast group are then forwarded to the receivers which have joined the group. It uses the following elements:

- **Rendezvous Point (RP).** This is a router is the root of a distribution tree for a multicast group. Receivers then send join messages for a group, and senders send their data to the RP so that receivers can thus discover senders, and thus receive data from them.
- **Designated Router (DR).** There can be several PIM-SM routers on a local network. One of these, the DR, then acts on behalf of directly connected hosts. An election process determines the winning interface.

The main methods used in PIM are:

- **Sparse Mode (SM)**. PIM-SM is the most popular deployment, and is efficient for routing to multicast groups that may span many subnets. It constructs a tree from each sender to the receivers in the multicast group. All routers in a common PIM-SM require to know the RP (Rendezvous Point). The command used for this is **pim rp-address IP**. PIM-SM is used when there are very few nodes subscribing to multicast sessions.
- **Dense Mode (DM)**. PIM-DM flooded packets throughout the networks and then prunes-off the branches where there were receivers exist.
- **Source Specific Mode (SSM)**.
- **Bidirectional Mode (Bidir)**.

For a multicast group (G), the host joins using IGMP. The router then forwards multicast packets only to the interfaces where host have joined the group. Designated Routers (DRs) are then used to send out join/prune messages to a group-specific Rendezvous Point (RP), for every group in which it has active members. The main objectives of this challenge are to:

- Configure the Ethernet ports.
- Enable PIM on E0.
- Define PIM parameters.
- Define a static rendezvous point (RP). The command used is **pim rp-address IP**.
- Define the designated router (DR) priority. The DR must send-out register, join, and prune messages to the RP. If there is more than one multicast router within a given network segment, there is an election process, where the higher the value, the higher the priority. The command used is **pim dr-priority value**.
- Define PIM hello message interval. The DR sends out router query message every 30 seconds. If this is to be changed the command used is **pim hello-interval value**.
- Define PIM join-prune interval. The DR sends out PIM join/prune messages every 60 seconds. If this is to be changed the command used is **pim join-prune-interval value**.

Commands

```
# config t
(config)# int e0
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# nameif Edinburgh
(config-if)# pim
(config-if)# pim dr-priority 50
(config-if)# pim hello-interval 50
(config-if)# pim join-prune-interval 50
(config-if)# exit
(config)# pim rp-address 192.168.0.1
```

Example

```

# config t
(config)# int e0
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# nameif ?

interface mode commands/options:
  WORD < 49 char  A name by which this interface will be referred in all other
                  Commands
(config-if)# nameif Edinburgh
(config-if)# pim ?

interface mode commands/options:
  dr-priority      PIM Hello DR priority
  hello-interval  PIM neighbor Hello announcement interval
  join-prune-interval PIM periodic Join-Prune announcement interval
  <cr>

configure mode commands/options:
  accept-register      Register accept filter
  old-register-checksum Generate registers compatible with older IOS versions
  rp-address           Configure Sparse-Mode Rendezvous Point
  spt-threshold       Configure threshold for SPT switchover on last-hop

(config-if)# pim

(config-if)# pim dr-priority ?

interface mode commands/options:
  <0-4294967295> Hello DR priority, preference given to larger value
(config-if)# pim dr-priority 50

(config-if)# pim hello-interval ?

interface mode commands/options:
  <1-3600> Hello interval in seconds
(config-if)# pim hello-interval 50

(config-if)# pi join-prune-interval ?

interface mode commands/options:
  <10-600> Join-Prune interval in seconds
(config-if)# pi join-prune-interval 50

(config-if)# exit
(config)# pim ?

configure mode commands/options:
  accept-register      Register accept filter
  old-register-checksum Generate registers compatible with older IOS versions
  rp-address           Configure Sparse-Mode Rendezvous Point
  spt-threshold       Configure threshold for SPT switchover on last-hop

(config)# pim accept-register ?
configure mode commands/options:
  list      Access list
  route-map Route-map

(config)# pim old-register-checksum ?

configure mode commands/options:
  <cr>

```

```
exec mode commands/options:
  Hostname or A.B.C.D      Ping destination IPv4 address or hostname
  Hostname or X:X:X:X::X  Ping destination IPv6 address or hostname
  <cr>
```

```
(config)# pim rp-address ?
```

```
configure mode commands/options:
  Hostname or A.B.C.D  IP name or address of Rendezvous Point
```

```
(config)# pim rp-address 192.168.0.1
```

```
(config)# pim spt-threshold ?
```

```
configure mode commands/options:
  infinity  Always stay on shared-tree
```

Cisco PIX/ASA Challenge 126

Title: Defining a multicast boundary

Outline

A standard ACL can be used to define the limits of a multicast boundary. The main objectives of this challenge are to:

- Configure the Ethernet ports.
- Enable PIM on E0.
- Define a standard ACL.
- Apply the ACL to a multicast boundary.

Commands

```
# config t
(config)# access-list 10 standard permit 10.0.0.1 0.0.0.255
(config)# int e0
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# nameif Edinburgh
(config-if)# multicast boundary 10
(config-if)# exit
```

Example

```
# config t
(config)# access-list 10 standard permit 10.0.0.1 0.0.0.255
(config)# int e0
(config-if)# ip address outside 192.168.1.1 255.255.255.0
(config-if)# nameif Edinburgh
(config-if)# multicast boundary 10
(config-if)# exit
```

Cisco PIX/ASA Test (Challenge 127)

Outline

This challenge involves taking a PIX test on multicast routing. The main facts are:

- Multicast routing uses Class D addresses, ranging from 224.0.0.0 239.255.255.255.
- 224.0.0.0 is never assigned to a group.
- 224.0.0.1 is assigned to all the systems within a given subnet.
- IGMP Version is automatically enabled on all the interfaces when multicast routing is enabled.
- The `no igmp` command is used on an interface to disable multicast routing on an interface.

Cisco PIX/ASA Challenge 128

Title: IPv6 - Explained

Outline

The RFC2460 specification outlines IPv6, which defines the main changes over IPv4 as:

- **Expanded addressing capabilities.** The size of the IP address will be increased to 128 bits, rather than 32 bits. This will allow for more levels of addressing hierarchy, an increased number of addressable nodes and a simpler auto-configuration of addresses. With multicast routing, the scalability is improved by adding a scope field to the multicast addresses. As well as this, an anycast address has been added so that packets can be sent to any one of a group of nodes.
- **Improved IP header format.** This tidies the IPv4 header fields by dropping the least used options, or making them optional.
- **Improved support for extensions and options.** These allow for different encodings of the IP header options, and thus allow for variable lengths and increased flexibility for new options.
- **Flow labeling capability.** A new capability is added to enable the labeling of packet belonging to particular traffic *flows* for which the sender requests special handling, such as non-default quality of service or *real-time* service.
- **Authentication and privacy capabilities.** Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.

Autoconfiguration and multiple IP addresses

IPv4 requires a significant amount of human intervention to set up the address of each of the nodes. IPv6 improves this by supplying autoconfiguration and renumbering facilities, which allows hosts to renumber without significant human intervention.

IPv4 has a stateful address structure, which either requires the user to manually set up the IP address of the computer or to use DHCP servers to provide IP addresses for a given MAC address. If a node moves from one subnet to another, the user must reconfigure the IP address, or request a new IP address from the DHCP. IPv6 supports a stateless autoconfiguration, where a host constructs its own IPv6. This occurs by adding its MAC address to a subnet prefix. The host automatically learns which subnet it is on by communicating from the router which is connected to the network that the host is connected to.

IPv6 supports multiple IP addresses for each host. These addresses can be either *valid*, *deprecated* or *invalid*. A valid address would be used for new and existing communications. A deprecated address could be used only for the existing communications (as they perhaps migrated to the new address). An invalid address would not be used for any communications. When renumbering, a host would deprecate the existing IP address, and set the new IP address as valid. All new communications would use the new IP address, but connections to the previous address would still operate. This allows a node to gradually migrate from one IP address to another.

IPv6 header format

Figure 1 shows the basic format of the IPv6 header. The main fields are:

- **Version number** (4 bits) – contains the version number, such as 6 for IP Ver6. It is used to differentiate between IPv4 and IPv6.
- **Priority** (4 bits) – indicates the priority of the datagram, and gives 16 levels of priority (0 to 15). The first eight values (0 to 7) are used where the source is providing congestion control (which is traffic that backs-off when congestion occurs). Examples are 0 defines no priority, 1 defines background traffic (such as netnews) and 2 defines unattended transfer (such as e-mail), 3 (reserved). The other values are used for traffic that will not back off in response to congestion (such as real-time traffic). The lowest priority for this is 8 (traffic which is the most willing to be discarded) and the highest is 15 (traffic which is the least willing to be discarded).
- **Flow label** (24 bits) – still experimental, but will be used to identify different data flow characteristics. It is assigned by the source and can be used to label data packets which require special handling by IPv6 routers, such as defined QoS (Quality of Service) or real-time services.

- **Payload length** (16 bits) – defines the total size of the IP datagram (and includes the IP header attached data).
- **Next header** – this field indicates which header follows the IP header (it uses the same IPv4). For example: 0 defines IP information; 1 defines ICMP information; 6 defines TCP information and 80 defines ISO-IP.
- **Hop limit** – defines the maximum number of hops that the datagram takes as it traverses the network. Each router decrements the hop limit by 1; when it reaches 0 it is deleted. This has been renamed from IPv4, where it was called time-to-live, as it better describes the parameter.
- **IP addresses** (128 bits) – defines IP address. There will be three main groups of IP addresses: unicast, multicast and anycast. A unicast address identifies a particular host, a multicast address enables the hosts within a particular group to receive the same packet, and the anycast address will be addressed to a number of interfaces on a single multicast address.

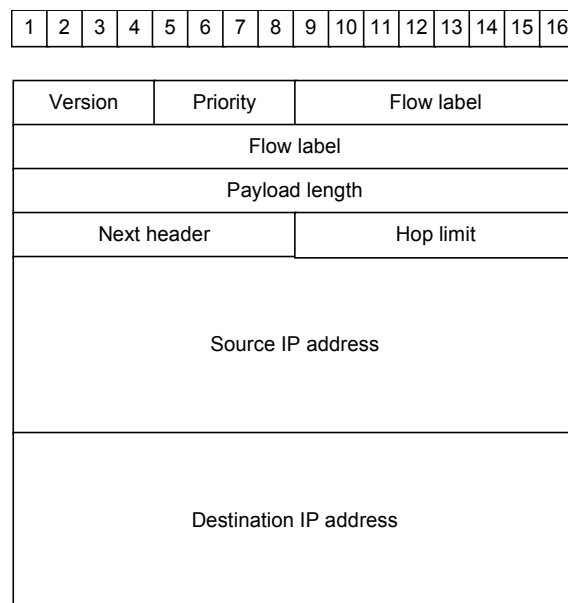


Figure 1 **IP Ver6 header format**

IPv6 addresses do not use the dotted notion and are written in a hexadecimal format, such as:

114F:0000:0000:0000:0006:0600:4411:CB1D

Often the leading zero's are omitted to give:

114F:0:0:0:6:600:4411:CB1D

This address can be shorted further by converting all zero values to a double colon, to give:

114F::6:600:4411:CB1D

These addresses can have certain scopes:

- Link-local. These have a scope on the local link (which are the nodes on the same subnet).
- Site-local. These have a scope within the organization (private site addressing).
- Global. These have global scope and are IPv6 Internet addresses.

Of the 128 bit global unicast addresses, the format can be viewed as:

- Public Topology (48 bits).
- Site Topology (16 bits).
- Interface ID (64 bits).

Objectives

The objectives of this challenge are to:

- Define IPv6 on E0 using the autoconfig option for the address (**ipv6 address autoconfig**) which enables stateless autoconfiguration, where the interface itself configures its own address based on the prefixes it receives from Router Advertisements (using the Modified EUI-64 Interface ID).
- Define IPv6 neighbor discovery to learn about neighboring devices.
- Define a static IPv6 mapping (if the automated discovery does not work).
- Define the default route.

Commands

```
(config)# int e0
(config-if)# ipv6 address autoconfig
(config-if)# ipv6 enable
(config-if)# exit
(config)# int e1
(config-if)# ipv6 address 2001:400:3:1::1/64
(config-if)# ipv6 enable
(config-if)# ipv6 nd ns-interval 1000
(config-if)# ipv6 nd ra-interval 1000
(config-if)# ipv6 nd reachable-time 100
(config-if)# ipv6 nd prefix 0800::/64
(config-if)# exit
(config)# ipv6 route outside ::/0 2001:400:3:1::1
(config)# ipv6 neighbor fe80:0000 inside 0000.1111.22222
# sh ipv interface
# sh ipv6 route
```

Step-by-step

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

! The next command defines that the interface builds its own IPv6 address
! based on Router Advertisements:

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

! The next command enables IPv6 on the interface:

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

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

! The next command assigns a global address on the interface, which automatically creates a
! link-local address (using the Interface ID):

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

! The next command enables IPv6 on the interface:

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

! IPv6 contains a duplicate address detection system. To determine the interval for neighbor
! solicitation message with the following (in this case 1000 milliseconds):

```
(config-if)# ipv6 nd ns-interval 1000
```

! The interval between IPv6 router advertisement retransmissions on an interface can be defined
! with:

```
(config-if)# ipv6 nd ra-interval 1000
```

! The time that a remote IPv6 node is considered reachable after a reachability confirmation event
! has occurred, is defined with:

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

! The IPv6 prefix which is included in IPv6 router advertisements is defined with:

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

! To define a default route:

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

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

```
(config)# ipv6 neighbor fe80:0000 inside 0000.1111.2222  
(config)# exit  
# sh ipv interface  
# sh ipv6 route
```

Example

```
(config)# int e0
(config-if)# ipv6 ?
```

```
interface mode commands/options:
IPv6 interface subcommands:
  address  Configure IPv6 address on interface
  enable   Enable IPv6 on interface
  nd       IPv6 interface Neighbor Discovery subcommands
```

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

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

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

```
configure mode commands/options:
  WORD  Access list identifier
```

```
(config-if)# ipv6 address autoconfig
(config-if)# ipv6 enable
(config-if)# exit
(config)# int e1
(config-if)# ipv6 address 2001:400:3:1::1/64
(config-if)# ipv6 enable
(config-if)# ipv6 nd ?
```

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

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

```
interface mode commands/options:
  <1000-3600000> Retransmission interval in milliseconds
```

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

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

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

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

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

```
interface mode commands/options:
  <3-1800> RA Interval (sec)
```

```

    msec          Interval in milliseconds

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

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

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

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

(config-if)# exit

(config)# ipv6 ?

configure mode commands/options:
  access-list      Configure access policy for IPv6 traffic through the system
  enforce-eui64    Enforce correct EUI-64 source address
  icmp             Configure access rules for ICMPv6 traffic terminating at an
                  interface
  neighbor         Neighbor
  route            Configure IPv6 routes

(config)# ipv6 route ?

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

(config)# ipv r outside ?

configure mode commands/options:
  X:X:X:X::X/<0-128> IPv6 prefix
(config)# ipv r outside ::/0 ?

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

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

(config)# ipv6 ?

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

(config)# ipv6 neighbor ?

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

(config)# ipv6 neighbor fe80:0000 ?

```

```
configure mode commands/options:
Current available interface(s):
  Inf2Name of interface Ethernet2
  Outside Name of interface Ethernet1
  Inside Name of interface Ethernet0
```

```
(config)# ipv6 neighbor fe80:0000 inside 0000.1111.2222
(config)# exit
```

```
# sh ipv6 ?
```

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

```
# sh ipv6 interface
```

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

```
# sh ipv6 route
```

```
IPv6 Routing Table - 2 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
```

```

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L fe80::/10 [0/0]
  via ::, outside
  via ::, inside
  via ::, inf2
L ff00::/8 [0/0]
  via ::, outside
  via ::, inside
  via ::, inf2

```

Cisco PIX/ASA Challenge 129

Title: Enforcing Modified EUI64 for Interface IDs for IPv6 interfaces

Outline

IPv6 addresses do not use the dotted notion and are written in a hexadecimal format, such as:

```
114F:0000:0000:0000:0006:0600:4411:CB1D
```

Often the leading zero's are omitted to give:

```
114F:0:0:0:6:600:4411:CB1D
```

This address can be shorted further by converting all zero values to a double colon, to give:

```
114F::6:600:4411:CB1D
```

The unicast address contains 128 bits, and has the following fields:

- **Field Prefix (FP) field (3 bits).** This identifies when the address is unicast, multicast, and so on). A value of 001 identifies aggregatable global unicasts.
- **Top-Level Aggregation Identifier (TLA ID field) (13 bits).** This is used to identify the authority responsible for the address at the highest level of the routing hierarchy.
- **Res field (8 bits).** This is reserved so that the TLA or NLA IDs can be expanded for future use.
- **NLA ID field (24 bits).** This is used to identify ISPs, and can be organized to reflect a hierarchy, or multitiered relationship, among providers.
- **SLA ID field (16 bits).** This is used by individual organizations in order to defined a local addressing hierarchy and to identify subnets.
- **Interface ID field (64 bits)** – This uses an **IEEE EUI-64** format and is a unique ID for the network interface. In Ethernet-type networks, it uses the 16 bits from the MAC address of the network port.

The RFC 3513 defines the IPv6 addressing architecture, and defines that all IPv6 addresses, apart from those beginning with 000, are constructed of a 64-bit Modified EUI-64 format. In this challenge the PIX/ASA is setup to check the received source IPv6 address against the source MAC address, so that the sending interface has used the Modified EUI-64 format. If it has not, the packet is dropped, and an error message shown.

Objectives

The objectives of this challenge are to:

- Define IPv6 on E0.
- Enforce Modified EUI-64 Interface IDs on E0.

Commands

```
(config)# int e0
(config-if)# ipv6 address autoconfig
(config-if)# ipv6 enable
(config-if)# exit
(config)# ipv6 enforce-eui64 inside
(config)# ipv6 enforce-eui64 outside
```

Example

```
(config)# int e0
(config-if)# ipv6 address autoconfig
(config-if)# ipv6 enable
(config-if)# exit
(config)# ipv6 ?
```

configure mode commands/options:

```
access-list      Configure access policy for IPv6 traffic through the system
enforce-eui64    Enforce correct EUI-64 source address
icmp             Configure access rules for ICMPv6 traffic terminating at an
                interface
neighbor        Neighbor
route           Configure IPv6 routes
```

```
(config)# ipv6 enforce-eui-64 ?
```

configure mode commands/options:

```
Current available interface(s):
Inf2Name of interface Ethernet2
Inside Name of interface Ethernet1
Outside  Name of interface Ethernet0
```

```
(config)# ipv6 enforce-eui64 inside
(config)# ipv6 enforce-eui64 outside
```

Cisco PIX/ASA Challenge 130

Title: Define an IPv6 ACL

Outline

IPv6 ACLs operate in a same way as normal ACLs, but operate on IPv6 addresses.

Objectives

The objectives of this challenge are to:

- Define an IPv6 ACL.
- Define IPv6 on E0.
- Enforce Modified EUI-64 Interface IDs on E0.
- Apply an IPv6 ACL onto E0 and E1.

Commands

```
(config)# ipv6 access-list testing deny ip 3EFE:3031:5::/48 any
(config)# ipv6 access-list testing deny ip 3EFE:3031:8::/48 any
(config)# ipv6 access-list testing permit ip any any
(config)# int e0
(config-if)# ipv6 address autoconfig
(config-if)# ipv6 enable
(config-if)# exit
(config)# ipv6 enforce-eui64 inside
(config)# ipv6 enforce-eui64 outside
(config)# access-group testing interface inside
(config)# access-group testing interface outside
```

Example

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

```
configure mode commands/options:
  access-list      Configure access policy for IPv6 traffic through the system
  enforce-eui64    Enforce correct EUI-64 source address
  icmp             Configure access rules for ICMPv6 traffic terminating at an
                  interface
  neighbor         Neighbor
  route            Configure IPv6 routes
```

```
(config)# ipv6 access-list ?
```

```
configure mode commands/options:
  WORD            Access list identifier
```

```
(config)# ipv6 access-list testing ?
```

```
configure mode commands/options:
  deny            Specify packets to reject
```

line Use this to specify line number at which ACE should be entered
permit Specify packets to forward
remark Specify a comment (remark) for the access-list after this keyword

(config)# ipv6 a testing deny ?

configure mode commands/options:
<0-255> Enter protocol number (0 - 255)
ah
eigrp
esp
gre
icmp
icmp6
igmp
igrp
ip
ipinip
ipsec
nos
object-group Specify a protocol object-group after this keyword
ospf
pcp
pim
pptp
snp
tcp
udp

(config)# ipv6 access-list testing deny ip ?

configure mode commands/options:
X:X:X:X:X/<0-128> Source IPv6 address/prefix
any Abbreviation for source prefix ::/0
host Use this keyword to configure source host
interface Use interface address as source address
object-group Network object-group for source address

(config)# ipv6 access-list testing deny ip 3EFE:3031:3::/48

(config)# ipv6 access-list testing deny ip 3EFE:3031:3::/48 ?

configure mode commands/options:
Hostname or A.B.C.D Destination IP address
X:X:X:X:X/<0-128> Destination IPv6 address/prefix
any Abbreviation for destination prefix ::/0
host Use this keyword to configure destination host
interface Use interface address as destination address
object-group Network object-group for destination address

(config)# ipv6 access-list testing deny ip 3EFE:3031:5::/48 any

(config)# ipv6 access-list testing permit ip any any

(config)# int e0

(config-if)# ipv6 address autoconfig

(config-if)# ipv6 enable

(config-if)# exit

(config)# ipv6 enforce-eui64 inside

(config)# ipv6 enforce-eui64 outside

(config)# access-group testing interface inside

(config)# access-group testing interface outside

Cisco PIX/ASA Test (Challenge 131)

Outline

This challenge involves taking a PIX test on IPv6. The main facts are:

- An IPv6 address has 128 bits.
- The Interface ID is based on 64 bits from the MAC address (which has 48 bits).
- The format is in two digit hexadecimal separated by colons.
- A double colon represent a run of zeros.

Cisco PIX/ASA Challenge 132

Title: Defining users and passwords

Outline

The PIX/ASA has a local database for users which defines user details for:

- CLI access login. This involves the user authentication for login to the device.
- Privilege mode authentication. This defines the privileged level for the access. With a Cisco device the highest privileged level is 15.
- Command authentication. This defines the commands that can be executed for given levels of user authentication.
- Network access authentication.
- VPN authentication/authorization.

The local user database is also useful as a fallback system, when the back-end user authentication system, such as for a RADIUS user authentication system fails, the local database should still work.

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 names.
- Define username and password. The user name can be between 4 and 64 characters, while the password by be between 3 and 16 characters.

- Define username attributes. This supports the username mode (config-username), and includes user specific information, such as for VPN settings.
- Define a privileged level. By default the privilege level is 2. The lowest is 0, and the highest is 16.

Commands

```
> enable
# config t
(config)# hostname amsterdam
amsterdam (config)# domain-name shetland.gov
amsterdam (config)# int e0
amsterdam (config-if)# nameif california
amsterdam (config-if)# exit
amsterdam (config)# int e1
amsterdam (config-if)# nameif texas
amsterdam (config-if)# exit
amsterdam (config)# int e2
amsterdam (config-if)# nameif newyork
amsterdam (config-if)# exit
amsterdam (config)# username bert password test privilege 15
amsterdam (config)# username anne password test
amsterdam (config)# username anne attrib
amsterdam (config-username)# service-type nas-prompt
```

Example

```
> enable
# config t
(config)# hostname amsterdam
amsterdam (config)# domain-name shetland.gov
amsterdam (config)# int e0
amsterdam (config-if)# nameif california
amsterdam (config-if)# exit
amsterdam (config)# int e1
amsterdam (config-if)# nameif texas
amsterdam (config-if)# exit
amsterdam (config)# int e2
amsterdam (config-if)# nameif newyork
amsterdam (config-if)# exit
amsterdam (config)# username ?
```

configure mode commands/options:

WORD < 65 char Enter the name of the user. A minimum of 4 characters is required. A maximum of 64 characters is allowed.

```
amsterdam (config)# username anne ?
```

configure mode commands/options:

attributes Enter the attributes sub-command mode for the specified user
 nopassword Indicates that this user has no password
 password The password for this user

```
amsterdam (config)# username anne password ?
```

configure mode commands/options:

WORD Enter the password for this user

```
amsterdam (config)# username anne password test
```

```
amsterdam (config)# username bert password test ?
```

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

```
encrypted      Indicates the <password> entered is encrypted
mschap         The password will be converted to unicode and hashed using MD4.
               User entries must be created this way if they are to be
               authenticated using MSCHAPv1 or MSCHAPv2
nt-encrypted   Indicates the <password> entered has been converted to unicode
               and hashed using MD4, and can be used for MS-CHAP.
privilege      Enter the privilege level for this user
<cr>
```

```
amsterdam (config)# username bert password privilege ?
```

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

```
<0-15> The privilege level for this user
```

```
amsterdam (config)# username bert password test privilege 15
```

```
amsterdam (config)# username anne attrib
```

```
amsterdam (config-username)# ?
```

```
username configuration commands:
```

```
exit           Exit from username attribute configuration mode
group-lock     Enter name of an existing tunnel-group that the user
               is required to connect with
help          Help for username configuration commands
no            Remove an attribute value pair
password-storage Enable/disable storage of the login password on the
               client system
service-type   Define service-type
vpn-access-hours Enter name of a configured time-range policy
vpn-filter     Enter name of user specific ACL
vpn-framed-ip-address Enter the IP address and the net mask to be assigned
               to the client
vpn-group-policy Enter name of a group-policy to inherit attributes
               from
vpn-idle-timeout Enter idle timeout period in minutes, enter none to
               disable
vpn-session-timeout Enter maximum user connection time in minutes, enter
               none for unlimited time
vpn-simultaneous-logins Enter maximum number of simultaneous logins allowed
vpn-tunnel-protocol Enter permitted tunneling protocols
webvpn        Configure user policy for WebVPN
```

```
amsterdam (config-username)# service-type ?
```

```
username mode commands/options:
```

```
admin         User is allowed access to the configuration prompt.
nas-prompt    User is allowed access to the exec prompt.
remote-access User is allowed network access.
```

```
amsterdam (config-username)# service-type nas-prompt
```

Cisco PIX/ASA Challenge 133

Title: Defining local authentication

Outline

The PIX/ASA has a local database for users, and can use AAA for local authentication. This is enabled with the following for checking users against the local database for serial (console connection), telnet (Telnet connection), ssh (SSH connection) and http (Web connection) login:

```
(config)# aaa authentication serial console MYLOCAL
(config)# aaa authentication telnet console MYLOCAL
(config)# aaa authentication ssh console MYLOCAL
(config)# aaa authentication http console MYLOCAL
```

The **console** keyword is important as it defines that management sessions are authenticated, whereas **local** defines that the local database is used.

Also users can be authenticated for the enable mode with:

```
(config)# aaa authentication enable console MYLOCAL
```

Where level 15 is the level required for the enable password command. Also the aaa-server command can be used to intercept any outgoing AAA requests to the local database:

```
(config)# aaa-server MYLOCAL protocol local
```

Objectives

The objectives of this challenge are to:

- Define E0, E1 and E2 names.
- Define username and password. The user name can be between 4 and 64 characters, while the password by be between 3 and 16 characters.
- Define authorization for Console, SSH, Telnet and HTTP login (**aaa authentication http console MYLOCAL**).
- Define local authentication (**aaa-server MYLOCAL protocol local**).

Commands

```
> enable
# config t
(config)# int e0
(config-if)# nameif california
(config-if)# exit
(config)# int e1
(config-if)# nameif texas
(config-if)# exit
(config)# int e2
(config-if)# nameif newyork
(config-if)# exit
(config)# username bert password test privilege 15
(config)# username anne password test
(config)# aaa-server MYLOCAL protocol local
(config-aaa-server-group)# exit
(config)# aaa authentication serial console MYLOCAL
```

```
(config)# aaa authentication telnet console MYLOCAL
(config)# aaa authentication ssh console MYLOCAL
(config)# aaa authentication http console MYLOCAL
(config)# aaa authentication enable console MYLOCAL
```

Example

```
> enable
# config t
(config)# int e0
(config-if)# nameif california
(config-if)# exit
(config)# int e1
(config-if)# nameif texas
(config-if)# exit
(config)# int e2
(config-if)# nameif newyork
(config-if)# exit
(config)# username bert password test privilege 15
(config)# username anne password test
pixfirewall(config)# aaa-s ?
```

configure mode commands/options:
WORD < 17 char Enter a AAA server group tag

```
pixfirewall(config)# aaa-s MYLOCAL ?
```

configure mode commands/options:

(Open parenthesis for the name of the network interface where the designated AAA server is accessed
deadtime	Specify the amount of time that will elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers
host	Enter this keyword to specify the IP address for the server
max-failed-attempts	Specify the maximum number of failures that will be allowed for any server in the group before that server is deactivated
protocol	Enter the protocol for a AAA server group

```
(config)# aaa-server MYLOCAL protocol ?
```

configure mode commands/options:

http-form	Protocol HTTP form-based
kerberos	Protocol Kerberos
ldap	Protocol LDAP
local	Protocol Local
nt	Protocol NT
radius	Protocol RADIUS
sdi	Protocol SDI
tacacs+	Protocol TACACS+

```
(config)# aaa-server MYLOCAL protocol local
(config-aaa-server-group)# exit
(config)# aaa ?
```

configure mode commands/options:

accounting	Configure user accounting parameters
authentication	Configure user authentication parameters
authorization	Configure user authorization parameters
local	AAA Local method options

```

mac-exempt      Configure MAC Exempt parameters
proxy-limit     Configure number of concurrent proxy connections allowed per
                user

(config)# aaa authentication ?

configure mode commands/options:
  enable        Enable
  exclude       Exclude the service, local and foreign network which
                needs to be authenticated, authorized, and accounted
  http          HTTP
  include       Include the service, local and foreign network which
                needs to be authenticated, authorized, and accounted
  match         Specify this keyword to configure an ACL to match
  secure-http-client Specify this keyword to ensure HTTP client authentication
                is secured (over SSL)
  serial        Serial
  ssh           SSH
  telnet        Telnet

(config)# aaa auth serial ?

configure mode commands/options:
  console       Specify this keyword to identify a server group for administrative
                authentication

(config)# aaa auth serial console ?

configure mode commands/options:
  LOCAL         Predefined server tag for AAA protocol 'local'
  WORD          Name of RADIUS or TACACS+ aaa-server group for administrative
                Authentication

(config)# aaa authentication serial console MYLOCAL
(config)# aaa authentication telnet console MYLOCAL
(config)# aaa authentication ssh console MYLOCAL
(config)# aaa authentication http console MYLOCAL
(config)# aaa authentication enable console MYLOCAL

```

Cisco PIX/ASA Challenge 134

Title: RADIUS Authentication

Outline

The ASA/PIX device supports a wide range of AAA backbones, including RADIUS (Remote Authentication Dial In User Service), Tacacs+, NT, LDAP, SDI and Kerberos. RADIUS is a useful system for authentication, as it is well supported in many systems, and is common in wireless systems. Microsoft RADIUS servers default to 1812 (accounting) and 1813 (authentication), but Cisco and Juniper RADIUS servers use default ports of 1645 (for accounting) and 1646 (for authentication). RADIUS uses UDP over IP, and combines authentication and authorization.

For the configuration, a group AAA server is defined initially:

```
(config)# aaa-server TEST protocol radius
(config-aaa-server-group)# max-failed-attempts 5
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit
```

This defines a group name of **TEST**. Next the details of each of the servers in the group are defined, such as for a single server host of:

```
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# key testkey
(config-aaa-server-host)# authentication-port 1645
(config-aaa-server-host)# accounting-port 1646
(config-aaa-server-host)# retry-interval 10
(config-aaa-server-host)# exit
```

Which defines that the server is on the (newyork) interface, and has an address of 1.2.3.4. With RADIUS a shared key is used, which is defined by the **key** command. This must be the same as the key defined on the server. In this case the authentication and accounting ports are defined as 1645 and 1646, respectively.

The main settings for RADIUS are:

- **Accounting-port.** This is the port which the RADIUS server listens to account communications on. Default = 1646.
- **Authorization-port.** This is the port which the RADIUS server listens to authorization communications on. Default = 1645.
- **Retry-interval.** This is the time that the device will wait for the RADIUS server to communicate before it tries again. Default = 10 seconds.
- **Timeout.** This is the timeout that the device will wait before it times-out the communications. Default = 10 seconds.
- **Key.** This is the key that the device and the server will use.

Objectives

The objectives of this challenge are to:

- Define an AAA group tag.
- Define an AAA host.
- Define AAA host details.

Commands

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

```

(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit

(config)# aaa-server test protocol radius
(config-aaa-server-group)# max-failed-attempts 5
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# key testkey
(config-aaa-server-host)# authentication-port 1645
(config-aaa-server-host)# accounting-port 1646
(config-aaa-server-host)# retry-interval 10
(config-aaa-server-host)# exit

```

Example

```

(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit

```

pixfirewall(config)# aaa-server ?

configure mode commands/options:
WORD < 17 char Enter a AAA server group tag

pixfirewall(config)# aaa-server test ?

configure mode commands/options:

(Open parenthesis for the name of the network interface where the designated AAA server is accessed
deadtime	Specify the amount of time that will elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers
host	Enter this keyword to specify the IP address for the server
max-failed-attempts	Specify the maximum number of failures that will be allowed for any server in the group before that server is deactivated
protocol	Enter the protocol for a AAA server group

pixfirewall(config)# aaa-server test protocol ?

configure mode commands/options:

kerberos	Protocol Kerberos
ldap	Protocol LDAP
nt	Protocol NT
radius	Protocol RADIUS
sdi	Protocol SDI
tacacs+	Protocol TACACS+

(config)# aaa-server test protocol radius

(config-aaa-server-group)# ?

AAA server configuration commands:

accounting-mode	Enter this keyword to specify accounting mode
exit	Exit from aaa-server group configuration mode
help	Help for AAA server configuration commands
max-failed-attempts	Specify the maximum number of failures that will be allowed for any server in the group before that server

```

no          is deactivated
reactivation-mode Remove an item from aaa-server group configuration
              Specify the method by which failed servers are
              reactivated

(config-aaa-server-group)# max-failed-attempts ?

aaa-server-group mode commands/options:
<1-5> Maximum number of failures (1-5)

(config-aaa-server-group)# reactivation-mode ?

aaa-server-group mode commands/options:
depletion Failed servers will remain inactive until all other servers in
           this group are inactive
timed     Failed servers will be reactivated after 30 seconds of down time

(config-aaa-server-group)# max-failed-attempts 5
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit

(config)# aaa-server test ?

configure mode commands/options:
(          Open parenthesis for the name of the network interface
           where the designated AAA server is accessed
deadtime  Specify the amount of time that will elapse between the
           disabling of the last server in the group and the
           subsequent re-enabling of all servers
host      Enter this keyword to specify the IP address for the
           server
max-failed-attempts Specify the maximum number of failures that will be
           allowed for any server in the group before that server
           is deactivated
protocol  Enter the protocol for a AAA server group

(config)# aaa-server test (newyork) ?

configure mode commands/options:
host      Enter this keyword to specify the IP address for the server

(config)# aaa-server test (newyork) host ?

configure mode commands/options:
Hostname or A.B.C.D Enter an IP address or a name
WORD < 129 char     Enter a DNS name

(config)# aaa-server test (newyork) host 1.2.3.4 ?

configure mode commands/options:
WORD      Alphanumeric keyword up to 128 characters used as the encryption key
           for communicating with the AAA server.
timeout   Specify the maximum time to wait for response from configured server
<cr>

(config)# aaa-server test (inside) host 1.2.3.4
(config-aaa-server-host)# ?

AAA server configuration commands:
accounting-port Specify the port number to be used for accounting
acl-netmask-convert Specify the ACL Downloadable Netmask Operation
authentication-port Specify the port number to be used for authentication

```

```

exit          Exit from aaa-server host configuration mode
help         Help for AAA server configuration commands
key          Specify the secret used to authenticate the NAS to the
            AAA server
no           Remove an item from aaa-server host configuration
radius-common-pw Specify a common password for all RADIUS authorization
            transactions
retry-interval Specify the amount of time between retry attempts
timeout      Specify the maximum time to wait for response from
            configured server

```

```
(config-aaa-server-host)# key ?
```

```
aaa-server-host mode commands/options:
```

```
WORD < 129 char Enter an alphanumeric string up to 128 characters
```

```
(config-aaa-server-host)# key testkey
```

```
(config-aaa-server-host)# accounting-port ?
```

```
aaa-server-host mode commands/options:
```

```
<0-65535> Enter port number (0 - 65535)
```

```
(config-aaa-server-host)# accounting-port 1646
```

```
(config-aaa-server-host)# authentication-port 1645
```

```
(config-aaa-server-host)# retry-interval ?
```

```
aaa-server-host mode commands/options:
```

```
<1-10> Number of seconds (1 - 10)
```

```
(config-aaa-server-host)# retry-interval 10
```

Cisco PIX/ASA Challenge 135

Title: Tacacs+ Authentication

Outline

The ASA/PIX device supports a wide range of AAA backbones, including RADIUS (Remote Authentication Dial In User Service), Tacacs+, NT, LDAP, SDI and Kerberos. Tacacs+ uses TCP over IP, and has separate elements for Authentication, Authorization and Accounting.

For the configuration, a group AAA server is defined initially:

```

(config)# aaa-server TEST protocol tacacs+
(config-aaa-server-group)# max-failed-attempts 5
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit

```

This defines a group name of **TEST**. Next the details of each of the servers in the group are defined, such as for a single server host of:

```

(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# key testkey

```

```
(config-aaa-server-host)# exit
```

Which defines that the server is on the (newyork) interface, and has an address of 1.2.3.4. With RADIUS a shared key is used, which is defined by the **key** command. This must be the same as the key defined on the server.

Objectives

The objectives of this challenge are to:

- Define an AAA group tag.
- Define an AAA host.
- Define AAA host details.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit

(config)# aaa-server TEST protocol tacacs+
(config-aaa-server-group)# max-failed-attempts 5
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# key testkey
(config-aaa-server-host)# exit
```

Cisco PIX/ASA Challenge 136

Title: LDAP Authentication

Outline

The ASA/PIX device supports a wide range of AAA backbones, including Tacacs+, NT, LDAP (Lightweight Directory Access Protocol), SDI and Kerberos. LDAP is a useful method in authentication. LDAP is an application protocol that builds on TCP and IP and is used to query and modify directory services. It can also be used for authentication.

For the configuration, a group AAA server is defined initially:

```
(config)# aaa-server TEST protocol ldap
(config-aaa-server-group)# max-failed-attempts 5
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit
```

This defines a group name of **TEST**. Next the details of each of the servers in the group are defined, such as for a single server host of:

```
(config)# aaa-server TEST (newyork) host 1.2.3.4
(config-aaa-server-host)# timeout 10
(config-aaa-server-host)# ldap-over-ssl enable
(config-aaa-server-host)# server-type Microsoft
(config-aaa-server-host)# sasl-mechanism digest-md5
(config-aaa-server-host)# exit
```

Which defines that the server is on the (newyork) interface, and has an address of 1.2.3.4. With LDAP the main parameters which can be set are:

- ldap-base-dn
- ldap-defaults
- ldap-dn
- ldap-login-dn
- ldap-login-password
- ldap-naming-attribute
- ldap-scope
- timeout
- server-port

For LDAP the PIX/ASA passes the user details to the LDAP server, by default, in a plaintext format for the username and password. If this is seen as a security problem, the username and password can be sent over an SSL connection using the **ldap-over-ssl** command. Also the LDAP server type can be Sun, Microsoft or Auto-detect. This is defined with the **server-type** command.

Objectives

The objectives of this challenge are to:

- Define an AAA group tag for LDAP.
- Define an AAA host.
- Define AAA host details.
- Define LDAP over SSL for secure username and password transmission.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit

(config)# aaa-server TEST protocol ldap
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
```

```
(config-aaa-server-host)# timeout 10
(config-aaa-server-host)# ldap-over-ssl enable
(config-aaa-server-host)# server-type Microsoft
(config-aaa-server-host)# sasl-mechanism digest-md5
(config-aaa-server-host)# exit
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
```

```
(config)# aaa-server TEST protocol ldap
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# ?
```

AAA server configuration commands:

exit	Exit from aaa-server host configuration mode
help	Help for AAA server configuration commands
ldap-attribute-map	Specify the name of the LDAP attribute mapping table
ldap-base-dn	Specify the location to begin searching in the LDAP hierarchy
ldap-login-dn	Specify the DN to be used to bind to the LDAP server
ldap-login-password	Specify password to be used to bind to the LDAP server
ldap-naming-attribute	Specify the Relative Distinguished Name attribute that uniquely identifies an entry on the LDAP server
ldap-over-ssl	Specify if an SSL connection is needed to the LDAP server
ldap-scope	Specify the extent of the search in the LDAP hierarchy
no	Remove an item from aaa-server host configuration
sasl-mechanism	Specify which authentication mechanism(s) to use with the LDAP server
server-port	Specify the port number to be used for AAA operations
server-type	Specify the vendor of the LDAP server
timeout	Specify the maximum time to wait for response from configured server

```
(config-aaa-server-host)# ldap-over-ssl ?
```

aaa-server-host mode commands/options:

enable	Require an SSL connection to the LDAP server
--------	--

```
(config-aaa-server-host)# ldap-over-ssl enable
(config-aaa-server-host)# server-type ?
```

aaa-server-host mode commands/options:

auto-detect	Specify the vendor of the LDAP server is auto-detected
microsoft	Specify the vendor of the LDAP server is Microsoft
sun	Specify the vendor of the LDAP server is Sun

<external_if_name> is the External or postnat interface

```
(config-aaa-server-host)# server-type Microsoft
```

```
(config-aaa-server-host)# sasl-mechanism ?
```

aaa-server-host mode commands/options:

digest-md5	select Digest-MD5
kerberos	select Kerberos

configure mode commands/options:

permit	Keyword for enabling this functionality
--------	---

```
(config-aaa-server-host)# sasl-mechanism digest-md5
(config-aaa-server-host)# timeout 10
(config-aaa-server-host)# exit
```

Cisco PIX/ASA Challenge 137

Title: VPN Access with LDAP Authentication

Outline

LDAP can be used to authenticate users for VPN access. When this happens the PIX/ASA then queries the LDAP server for its attributes. To setup LDAP authorization, a tunnel group is setup, along with an AAA server group. For the tunnel group:

```
(config)# tunnel-group TEST type ipsec-ra
(config)# tunnel-group TEST general-attributes
(config-general)# authorization-server-group LDAP1
(config-general)# exit
```

Where:

- **tunnel-group TEST type ipsec-ra** defines an IPSec tunnel named TEST.
- **authorization-server-group LDAP1** which defines that LDAP1 is the authorization server group name.

Next the server group is defined:

```
(config)# aaa-server LDAP1 protocol ldap
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# ldap-login-dn testing123
(config-aaa-server-host)# ldap-base-dn location123
(config-aaa-server-host)# ldap-scope subtree
```

Where:

- **ldap-scope subtree** searches all the levels beneath the base DN (Distinguished Name).
- **ldap-base-dn location123** defines that location123 is the location to begin searching in the LDAP hierarchy
- **ldap-login-dn testing123** defines that testing123 is the DN used to bind to the LDAP server.

Objectives

The objectives of this challenge are to:

- Define a tunnel group with attributes.
- Define an AAA group tag for LDAP.
- Define AAA host details.
- Define LDAP details for VPN access.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# tunnel-group TEST type ipsec-ra
(config)# tunnel-group TEST general-attributes
(config-general)# authorization-server-group LDAP1
(config-general)# exit
(config)# aaa-server LDAP1 protocol ldap
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# ldap-login-dn testing123
(config-aaa-server-host)# ldap-base-dn location123
(config-aaa-server-host)# ldap-scope subtree
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# tunnel-group ?
```

```
configure mode commands/options:
  WORD < 65 char  Enter the name of the tunnel group
```

```
(config)# tunnel-group TEST ?
```

```
configure mode commands/options:
  general-attributes  Enter the general-attributes sub command mode
  ipsec-attributes    Enter the ipsec-attributes sub command mode
  type                Enter the type of this group-policy
```

```
(config)# tunnel-group TEST type ?
```

```
configure mode commands/options:
  ipsec-l2l  IPSec Site to Site group
  ipsec-ra   IPSec Remote Access group
```

```
(config)# tunnel-group TEST type ipsec-ra
(config)# tunnel-group TEST general-attributes
(config-general)# ?
```

```
group_policy configuration commands:
  accounting-server-group  Enter name of the accounting server group
  address-pool             Enter a list of address pools to assign
                           addresses from
  authentication-server-group  Enter name of the authentication server group
  authorization-server-group  Enter name of the authorization server group
  default-group-policy      Enter name of the default group policy
```

```

dhcp-server          Enter IP address or name of the DHCP server
exit                Exit from tunnel-group general attribute
                   configuration mode
help               Help for tunnel group configuration commands
no                 Remove an attribute value pair
strip-group        Enable strip-group processing
strip-realm        Enable strip-realm processing

(config-general)# authorization-server-group ?

tunnel-group-general mode commands/options:
  WORD < 17 char  Name of authorization server group

(config-general)# authorization-server-group LDAP1
(config-general)# exit
(config)# aaa-server LDAP1 protocol ldap
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# ldap-login-dn ?

aaa-server-host mode commands/options:
  LINE < 129 char  The DN used to bind to the LDAP server

(config-aaa-server-host)# ldap-login-dn testing123

(config-aaa-server-host)# ldap-base-dn ?

aaa-server-host mode commands/options:
  LINE < 129 char  The location to begin searching in the LDAP hierarchy

(config-aaa-server-host)# ldap-base-dn location123

(config-aaa-server-host)# ldap-scope ?

aaa-server-host mode commands/options:
  onelevel  Search only one level beneath the Base DN
  subtree   Search all levels beneath the Base DN

(config-aaa-server-host)# ldap-scope subtree

```

Cisco PIX/ASA Challenge 138

Title: LDAP Attribute Mapping

Outline

Typically the LDAP attribute names and values are different between the PIX/ASA and the LDAP server. This challenge involves remapping these. The commands used are:

```

(config)# ldap attribute-map testing
(config-ldap-attribute-map)# map-name testing CiscoAttr1
(config-ldap-attribute-map)# map-value testing CiscoAttr2

```

Objectives

The objectives of this challenge are to:

- Define an AAA group tag for LDAP.
- Define AAA host details.
- Define LDAP attributes

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server TEST protocol ldap
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# timeout 10
(config-aaa-server-host)# ldap-over-ssl enable
(config-aaa-server-host)# server-type Microsoft
(config-aaa-server-host)# sasl-mechanism digest-md5
(config-aaa-server-host)# exit
(config)# ldap attribute-map testing
(config-ldap-attribute-map)# map-name testing Cisco1
(config-ldap-attribute-map)# map-value testing Cisco2
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server TEST protocol ldap
(config-aaa-server-group)# exit
(config)# aaa-server test (newyork) host 1.2.3.4
(config-aaa-server-host)# timeout 10
(config-aaa-server-host)# ldap-over-ssl enable
(config-aaa-server-host)# server-type Microsoft
(config-aaa-server-host)# sasl-mechanism digest-md5
(config-aaa-server-host)# exit
(config)# ldap ?
```

```
configure mode commands/options:
  attribute-map keyword
```

```
(config)# ldap attribute-map ?
```

```
configure mode commands/options:
  LINE < 64 char  Enter LDAP Mapping Name
```

```
(config)# ldap attribute-map testing
(config-ldap-attribute-map)# ?
```

```
LDAP commands:
  exit          Exit from LDAP Attribute configuration mode
  map-name      map-name configuration
  map-value     map-value configuration
  no           Remove a LDAP configuration
```

```
(config-ldap-attribute-map)# map-name ?
```

```
ldap mode commands/options:  
WORD Enter Customer Attribute Name.
```

```
(config-ldap-attribute-map)# map-name testing ?
```

```
ldap mode commands/options:  
cisco-attribute-names:  
cVPN3000-Access-Hours  
cVPN3000-Allow-Network-Extension-Mode  
cVPN3000-Auth-Service-Type  
cVPN3000-Authenticated-User-Idle-Timeout  
cVPN3000-Authorization-Required  
cVPN3000-Authorization-Type  
cVPN3000-Cisco-AV-Pair  
cVPN3000-Cisco-IP-Phone-Bypass  
cVPN3000-Cisco-LEAP-Bypass  
cVPN3000-Client-Intercept-DHCP-Configure-Msg  
cVPN3000-Client-Type-Version-Limiting  
cVPN3000-Confidence-Interval  
cVPN3000-DHCP-Network-Scope  
cVPN3000-DN-Field  
cVPN3000-Firewall-ACL-In  
cVPN3000-Firewall-ACL-Out  
cVPN3000-IE-Proxy-Bypass-Local  
cVPN3000-IE-Proxy-Exception-List  
cVPN3000-IE-Proxy-Method  
cVPN3000-IE-Proxy-Server  
cVPN3000-IETF-Radius-Class  
cVPN3000-IETF-Radius-Filter-Id  
cVPN3000-IETF-Radius-Framed-IP-Address  
cVPN3000-IETF-Radius-Framed-IP-Netmask  
cVPN3000-IETF-Radius-Idle-Timeout  
cVPN3000-IETF-Radius-Session-Timeout  
cVPN3000-IKE-DPD-Retry-Interval  
cVPN3000-IKE-Keep-Alives  
cVPN3000-IPSec-Allow-Passwd-Store  
cVPN3000-IPSec-Auth-On-Rekey  
cVPN3000-IPSec-Authentication  
cVPN3000-IPSec-Backup-Server-List  
cVPN3000-IPSec-Backup-Servers  
cVPN3000-IPSec-Banner1  
cVPN3000-IPSec-Banner2  
cVPN3000-IPSec-Client-Firewall-Filter-Name  
cVPN3000-IPSec-Client-Firewall-Filter-Optional  
cVPN3000-IPSec-Default-Domain  
cVPN3000-IPSec-IKE-Peer-ID-Check  
cVPN3000-IPSec-IP-Compression  
cVPN3000-IPSec-Mode-Config  
cVPN3000-IPSec-Over-UDP  
cVPN3000-IPSec-Over-UDP-Port  
cVPN3000-IPSec-Required-Client-Firewall-Capability  
cVPN3000-IPSec-Sec-Association  
cVPN3000-IPSec-Split-DNS-Names  
cVPN3000-IPSec-Split-Tunnel-List  
cVPN3000-IPSec-Split-Tunneling-Policy  
cVPN3000-IPSec-Tunnel-Type  
cVPN3000-IPSec-User-Group-Lock  
cVPN3000-L2TP-Encryption  
cVPN3000-L2TP-MPPC-Compression  
cVPN3000-LDAP-Base-DN  
cVPN3000-LDAP-CRL-Data  
cVPN3000-LDAP-Filter
```

```
cVPN3000-LDAP-Host-Name
cVPN3000-LDAP-Host-Port
cVPN3000-LDAP-Login
cVPN3000-LDAP-Password
cVPN3000-LDAP-Request-Type
cVPN3000-LDAP-Scope
cVPN3000-LDAP-Version
cVPN3000-MS-Client-Subnet-Mask
cVPN3000-PFS-Required
cVPN3000-PPTP-Encryption
cVPN3000-PPTP-MPPC-Compression
cVPN3000-Primary-DNS
cVPN3000-Primary-WINS
cVPN3000-Require-HW-Client-Auth
cVPN3000-Require-Individual-User-Auth
cVPN3000-Required-Client-Firewall-Description
cVPN3000-Required-Client-Firewall-Product-Code
cVPN3000-Required-Client-Firewall-Vendor-Code
cVPN3000-SEP-Card-Assignment
cVPN3000-Secondary-DNS
cVPN3000-Secondary-WINS
cVPN3000-Simultaneous-Logins
cVPN3000-Strip-Realm
cVPN3000-TACACS-Authtype
cVPN3000-TACACS-Privilege-Level
cVPN3000-Tunnel-Group-Lock
cVPN3000-Tunneling-Protocols
cVPN3000-Use-Client-Address
cVPN3000-User-Auth-Server-Name
cVPN3000-User-Auth-Server-Port
cVPN3000-User-Auth-Server-Secret
cVPN3000-WebVPN-ACL-Filters
cVPN3000-WebVPN-Apply-ACL-Enable
cVPN3000-WebVPN-Citrix-Support-Enable
cVPN3000-WebVPN-Content-Filter-Parameters
cVPN3000-WebVPN-Enable-Functions
cVPN3000-WebVPN-Exchange-NETBIOS-Name
cVPN3000-WebVPN-Exchange-Server-Address
cVPN3000-WebVPN-File-Access-Enable
cVPN3000-WebVPN-File-Server-Browsing-Enable
cVPN3000-WebVPN-File-Server-Entry-Enable
cVPN3000-WebVPN-Forwarded-Ports
cVPN3000-WebVPN-Homepage
cVPN3000-WebVPN-Port-Forwarding-Auto-Download-Enable
cVPN3000-WebVPN-Port-Forwarding-Enable
cVPN3000-WebVPN-Port-Forwarding-Exchange-Proxy-Enable
cVPN3000-WebVPN-Port-Forwarding-HTTP-Proxy-Enable
cVPN3000-WebVPN-Port-Forwarding-Name
cVPN3000-WebVPN-SVC-Client-DPD
cVPN3000-WebVPN-SVC-Compression
cVPN3000-WebVPN-SVC-Enable
cVPN3000-WebVPN-SVC-Gateway-DPD
cVPN3000-WebVPN-SVC-Keep-Enable
cVPN3000-WebVPN-SVC-Keepalive
cVPN3000-WebVPN-SVC-Rekey-Method
cVPN3000-WebVPN-SVC-Rekey-Period
cVPN3000-WebVPN-SVC-Required-Enable
cVPN3000-WebVPN-Single-Sign-On-Server-Name
cVPN3000-WebVPN-URL-Entry-Enable
cVPN3000-WebVPN-URL-List
cVPN3000-X509-Cert-Data
(config-ldap-attribute-map)# map-name testing cVPN3000-WebVPN-URL-List
```

```
(config-ldap-attribute-map)# map-value ?
```

```
ldap mode commands/options:  
customer-attribute-names:
```

```
(config-ldap-attribute-map)# map-value testing cVPN3000-WebVPN-URL-List
```

Cisco PIX/ASA Challenge 139

Title: Using AAA for End-user Cut-through Proxy Applications

Outline

The PIX/ASA can authenticate users before they make connections. Once authenticated it is then possible to cache the authentication for the user, so that there does not need to be a re-authentication with the authentication server. The PIX/ASA thus acts as an authentication proxy, and the command which triggers the authentication is in the form of:

```
(config)# aaa authentication include telnet outside 0 0 0 0 SERVERTAG  
(config)# aaa authentication include ssh outside 0 0 0 0 SERVERTAG  
(config)# aaa authentication include ftp outside 0 0 0 0 SERVERTAG  
(config)# aaa authentication include http outside 0 0 0 0 SERVERTAG  
(config)# aaa authentication include https outside 0 0 0 0 SERVERTAG
```

which will authenticates all Telnet, SSH, Ftp, Http and Https accesses on the inside interface, for all source and destination addresses (where 0 is the same as 0.0.0.0). In this case SERVERTAG is the tag that defines the authentication, such as:

```
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
```

Objectives

The objectives of this challenge are to:

- Define an end-user cut-through proxy for various protocols..
- Define AAA host details.

Commands

```
(config)# int e0  
(config-if)# ip address 192.168.0.1 255.255.255.0  
(config-if)# nameif newyork  
(config-if)# exit  
(config)# aaa-server SERVERTAG protocol radius  
(config-aaa-server-group)# exit  
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4  
(config)# aaa authentication include telnet outside 0 0 0 0 SERVERTAG  
(config)# aaa authentication include ssh outside 0 0 0 0 SERVERTAG  
(config)# aaa authentication include ftp outside 0 0 0 0 SERVERTAG  
(config)# aaa authentication include http outside 0 0 0 0 SERVERTAG
```

```
(config)# aaa authentication include https outside 0 0 0 0 SERVERTAG
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# aaa authentication ?
```

```
configure mode commands/options:
  command  Specify this keyword to allow command authorization to be configured
           for all administrators on all consoles
  exclude  Exclude the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  include  Include the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  match    Specify this keyword to configure an ACL to match
```

```
(config)# aaa authentication include ?
```

```
configure mode commands/options:
  WORD    Specify <protocol[/<port>] as the service to be authorized or
           accounted
  any     Specify all TCP as the service to be authenticated, authorized or
           accounted
  ftp     Specify FTP as the service to be authenticated, authorized or
           accounted
  http    Specify HTTP as the service to be authenticated, authorized or
           accounted
  https   Specify HTTPS as the service to be authenticated, authorized or
           accounted
  icmp/   Specify icmp/<port> as the service to be authorized or accounted
  ssh     Specify SSH as the service to be authenticated, authorized or
           accounted
  tcp/    Specify tcp/<port> as the service to be authenticated, authorized or
           accounted
  tcp/0   Specify all TCP as the service to be authenticated, authorized or
           accounted
  telnet  Specify telnet as the service to be authenticated, authorized or
           accounted
  udp/    Specify udp/<port> as the service to be authorized or accounted
```

```
(config)# aaa authentication include telnet ?
```

```
configure mode commands/options:
Current available interface(s):
  newyork Name of interface Ethernet0
```

```
(config)# aaa authentication include te newyork ?
```

```
configure mode commands/options:
  Hostname or A.B.C.D  The address and mask of the local/internal host which is
                       source or destination for connections requiring
                       authentication
```

```
(config)# aaa authentication include telnet newyork 0 ?
```

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

```

A.B.C.D Network mask to apply to <local ip address>

(config)# aaa authentication include te newyork 0 0 ?

configure mode commands/options:
  Hostname or A.B.C.D The address and mask of the foreign host which is either
                      source or destination for connections requiring
                      authentication
  WORD                Specify name of server group defined by the aaa-server
                      command.

(config)# aaa authentication include te newyork 0 0 0 ?

configure mode commands/options:
  A.B.C.D Network mask to apply to <foreign ip address>

(config)# aaa authentication include te newyork 0 0 0 0 ?

configure mode commands/options:
  WORD Specify name of server group defined by the aaa-server command.

(config)# aaa authentication include te newyork 0 0 0 0 ANY ?

configure mode commands/options:
  <cr>

(config)# aaa authentication include telnet outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ssh outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ftp outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include http outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include https outside 0 0 0 0 SERVERTAG

```

Cisco PIX/ASA Challenge 140

Title: AAA for End-user Cut-through Proxy Applications using an ACL

Outline

The PIX/ASA can authenticate users before they make connections. In the previous challenge the protocol match was defined, such as:

```
(config)# aaa authentication include telnet outside 0 0 0 0 SERVERTAG
```

which defines that all Telnet accesses will be authenticated against user credentials. If a more complex method of filtering is required, ACLs can be used to determine the traffic to be authenticated. For example:

```
(config)# access-list TEST permit 192.168.0.0 255.255.255.0
(config)# access-list TEST permit tcp any any eq ftp
(config)# access-list TEST permit tcp any any eq http
(config)# aaa authentication match TEST inside SERVERTAG
```

which will authenticates all incoming traffic from 192.168.0.0/24, and also all FTP and HTTP accesses on the inside interface. In this case SERVERTAG is the tag that defines the authentication, such as:

```
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
```

Objectives

The objectives of this challenge are to:

- Define an end-user cut-through proxy for various protocols.
- Define ACLs for interesting traffic to be authenticated.
- Define AAA host details.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# access-list TEST permit 192.168.0.0 255.255.255.0
(config)# access-list TEST permit tcp any any eq ftp
(config)# access-list TEST permit tcp any any eq http
(config)# aaa authentication match TEST newyork SERVERTAG
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# access-list TEST permit 192.168.0.0 255.255.255.0
(config)# access-list TEST permit tcp any any eq ftp
(config)# access-list TEST permit tcp any any eq http
(config)# aaa ?
```

configure mode commands/options:

```
accounting      Configure user accounting parameters
authentication  Configure user authentication parameters
authorization   Configure user authorization parameters
local          AAA Local method options
mac-exempt     Configure MAC Exempt parameters
proxy-limit    Configure number of concurrent proxy connections allowed per
               user
```

```
(config)# aaa authentication ?
```

configure mode commands/options:

```
command Specify this keyword to allow command authorization to be configured
         for all administrators on all consoles
```

```

exclude  Exclude the service, local and foreign network which needs to be
         authenticated, authorized, and accounted
include  Include the service, local and foreign network which needs to be
         authenticated, authorized, and accounted
match    Specify this keyword to configure an ACL to match

(config)# aaa authentication match ?

configure mode commands/options:
  WORD  Name of configured access-list to match

(config)# aaa authentication TEST ?

configure mode commands/options:
Current available interface(s):
  newyork  Name of interface Ethernet0

(config)# aaa authentication TEST newyork ?

configure mode commands/options:
  LOCAL  Predefined server tag for AAA protocol 'local'
  WORD   Specify name of server group defined by the aaa-server command.

(config)# aaa authentication match TEST newyork  SERVERTAG

```

Cisco PIX/ASA Challenge 141

Title: AAA for End-user Cut-through Proxy Applications using an ACL, with a MAC-list for exemptions

Outline

In the previous challenge an ACL was used to define the traffic to be authenticated, such as:

```

(config)# access-list TEST permit 192.168.0.0 255.255.255.0
(config)# access-list TEST permit tcp any any eq ftp
(config)# access-list TEST permit tcp any any eq http
(config)# aaa authentication match TEST inside SERVERTAG

```

It is possible to use SSL for all web-related authentication with:

```

(config)# aaa authentication secure-http-client

```

Along with this devices can be exempted from authentication with a MAC-list, such as:

```

(config)# mac-list MACLIST permit 00c0.0000.0001 ffff.ffff.ffff
(config)# mac-list MACLIST permit 00c0.0000.0002 ffff.ffff.ffff

```

which will allow the devices with the MAC addresses of 00c0.0000.0001 and 00c0.0000.0002 to pass through without authentication. This is then applied with:

```

(config)# aaa mac-exempt match MACLIST

```

Objectives

The objectives of this challenge are to:

- Define an end-user cut-through proxy for various protocols.
- Define ACLs for interesting traffic to be authenticated.
- Define AAA host details.
- Define a MAC-list for exempted devices.
- Applied the MAC-list.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# aaa authentication secure-http-client
(config)# access-list TEST permit 192.168.0.0 255.255.255.0
(config)# access-list TEST permit tcp any any eq ftp
(config)# access-list TEST permit tcp any any eq http
(config)# aaa authentication match TEST newyork SERVERTAG
(config)# mac-list MACLIST permit 00c0.0000.0001 ffff.ffff.ffff
(config)# mac-list MACLIST permit 00c0.0000.0002 ffff.ffff.ffff
(config)# aaa mac-exempt match MACLIST
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# aaa authentication secure-http-client
(config)# access-list TEST permit 192.168.0.0 255.255.255.0
(config)# access-list TEST permit tcp any any eq ftp
(config)# access-list TEST permit tcp any any eq http
(config)# aaa authentication match TEST newyork SERVERTAG
(config)# mac-list ?
```

```
configure mode commands/options:
  WORD  Mac list identifier
```

```
(config)# mac-list MACLIST ?
```

```
configure mode commands/options:
  deny  Specify packets to reject
  permit Specify packets to forward
```

```
(config)# mac-list MACLIST permit ?
```

```

configure mode commands/options:
  H.H.H Match based on source MAC address

(config)# mac-list MACLIST permit 00c0.0000.0001 ?

configure mode commands/options:
  H.H.H Mac mask

(config)# mac-list MACLIST permit 00c0.0000.0001 ffff.ffff.ffff
(config)# mac-list MACLIST permit 00c0.0000.0002 ffff.ffff.ffff
(config)# aaa mac-list ?

configure mode commands/options:
  match Specify this keyword to configure a mac-list to match

(config)# aaa mac-list mac match ?

configure mode commands/options:
  WORD Name of configured mac-list to match

(config)# aaa mac-list mac match MACLIST ?

configure mode commands/options:
  <cr>

(config)# aaa mac-exempt match MACLIST

```

Cisco PIX/ASA Challenge 142

Title: Using AAA for End-user Cut-through Proxy Applications with a limit on **per-user proxy connections**, and a **timeout for inactivity**.

Outline

The maximum number of per-user proxy connections is defined with:

```
(config)# aaa proxy-limit 50
```

which defines a limit for 50 active connections for each user. The maximum number that can be set is 128, and the default is 16. Also the timeout for inactivity after a successful authentication is defined with:

```
(config)# timeout uauth 00:30:00 inactivity
```

which defines an inactivity time of 30 minutes.

Objectives

The objectives of this challenge are to:

- Define an end-user cut-through proxy for various protocols.
- Define AAA host details.

- Define a limit on per-user proxy connections.
- Define a timeout for inactivity.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# aaa authentication include telnet outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ssh outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ftp outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include http outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include https outside 0 0 0 0 SERVERTAG
(config)# aaa proxy-limit 50
(config)# timeout uauth 00:30:00 inactivity
(config)# exit
# show uauth
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# aaa authentication include telnet outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ssh outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ftp outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include http outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include https outside 0 0 0 0 SERVERTAG
(config)# aaa proxy-limit ?
```

```
configure mode commands/options:
  <1-128> Number of concurrent proxy connections allowed per user (1 - 128),
           default is 16
  disable Disable concurrent proxy connections
```

```
(config)# aaa proxy-limit 50
(config)# timeout ?
```

```
configure mode commands/options:
  conn          Configure idle time after which a TCP connection state
                will be closed, default is 1:00:00
  h225          Configure idle time after which an H.225 signaling conn
                will be closed, default is 1:00:00
  h323          Configure idle time after which an H.323 control connection
                will be closed, default is 0:05:00
  half-closed  Configure idle time after which a TCP half-closed connection
                will be freed, default is 0:10:00
  icmp          Configure idle timeout for ICMP, default is 0:00:02
  mgcp          Configure idle time after which an MGCP media connection
                will be closed, default is 0:05:00
  mgcp-pat     Configure the time after which an MGCP PAT Xlate
```

sip will be removed, default is 0:05:00
 Configure idle time after which a SIP control connection will be closed, default is 0:30:00
 sip_media Configure idle time after which a SIP Media connection will be closed, default is 0:02:00
 sunrpc Configure idle time after which a SUNRPC slot will be closed, default is 0:10:00
 uauth Configure idle time after which an authentication will no longer be cached and the user will need to re-authenticate on their connection, default is 0:05:00. The default uauth timer is absolute.
 udp Configure idle time after which general UDP states will be closed, default is 0:02:00, This timer does not apply to DNS or SUNRPC
 xlate Configure idle time after which a dynamic address will be returned to the free pool, default is 3:00:00

(config)# timeout uauth ?

configure mode commands/options:

<0:0:0> - <1193:0:0> Idle time after which an authentication will no longer be cached and the user will need to re-authenticate on their connection, default is 0:05:00. The default uauth timer is absolute.

(config)# timeout uauth 00:30:00 ?

configure mode commands/options:

absolute Run uauth timer continuously, the default uauth timer is absolute
 conn Configure idle time after which a TCP connection state will be closed, default is 1:00:00
 h225 Configure idle time after which an H.225 signaling conn will be closed, default is 1:00:00
 h323 Configure idle time after which an H.323 control connection will be closed, default is 0:05:00
 half-closed Configure idle time after which a TCP half-closed connection will be freed, default is 0:10:00
 icmp Configure idle timeout for ICMP, default is 0:00:02
 inactivity Start uauth timer after a connection becomes idle
 mgcp Configure idle time after which an MGCP media connection will be closed, default is 0:05:00
 mgcp-pat Configure the time after which an MGCP PAT Xlate will be removed, default is 0:05:00
 sip Configure idle time after which a SIP control connection will be closed, default is 0:30:00
 sip-disconnect Configure idle timeout after which SIP session is deleted if 200 OK is not received for a CANCEL or BYE message, default is 0:02:00
 sip-invite Configure idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, default is 0:03:00
 sip_media Configure idle time after which a SIP Media connection will be closed, default is 0:02:00
 sunrpc Configure idle time after which a SUNRPC slot will be closed, default is 0:10:00
 udp Configure idle time after which general UDP states will be closed, default is 0:02:00, This timer does not apply to DNS or SUNRPC
 xlate Configure idle time after which a dynamic address will be returned to the free pool, default is 3:00:00
 <cr>

(config)# timeout uauth 00:30:00 inactivity

```
(config)# exit

(config)# show uauth
Current      Most Seen
Authenticated Users      1          1
Authen In Progress      0          1
user 'fred' at 192.168.0.1, authorized to:
  port 192.168.0.1/telnet
  absolute timeout: 0:05:00
  inactivity timeout: 0:30:00

# sh ua ?

WORD  User name
|     Output modifiers
<cr>
```

```
# sh uauth fred
Current      Most Seen
Authenticated Users      0          0
Authen In Progress      0          0
```

Cisco PIX/ASA Challenge 143

Title: Using AAA Accounting

Outline

The PIX/ASA can setup accounting on connections. To define the traffic for the accounting:

```
(config)# aaa accounting include telnet outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include ssh outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include ftp outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include http outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include https outside 0 0 0 0 SERVERTAG
```

which will accounts for all Telnet, SSH, Ftp, Http and Https accesses on the inside interface, for all source and destination addresses (where 0 is the same as 0.0.0.0). In this case SERVERTAG is the tag that defines the accounting, such as:

```
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
```

Objectives

The objectives of this challenge are to:

- Define accounting traffic.
- Define AAA host details.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
```

```
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# aaa accounting include telnet outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include ssh outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include ftp outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include http outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include https outside 0 0 0 0 SERVERTAG
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# nameif newyork
(config-if)# exit
(config)# aaa-server SERVERTAG protocol radius
(config-aaa-server-group)# exit
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
(config)# aaa accounting include telnet outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include ssh outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include ftp outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include http outside 0 0 0 0 SERVERTAG
(config)# aaa accounting include https outside 0 0 0 0 SERVERTAG
```

Cisco PIX/ASA Test (Challenge 144)

Outline

This challenge involves taking a PIX/ASA test on local users and AAA. The main facts are:

- Cisco IOS has 16 different privilege levels, 0 to 15.
- Level 15 is the highest privilege and 0 is the lowest.
- show privilege is used to display the current privilege level.
- Privileged EXEC mode is Level 15.
- EXEC mode mode is Level 1.

Key commands

Local authentication:

```
(config)# aaa-server MYLOCAL protocol local
(config-aaa-server-group)# exit
(config)# aaa authentication serial console MYLOCAL
(config)# aaa authentication telnet console MYLOCAL
(config)# aaa authentication ssh console MYLOCAL
(config)# aaa authentication http console MYLOCAL
(config)# aaa authentication enable console MYLOCAL
```

RADIUS authentication:

```
(config)# aaa-server TEST protocol radius
(config-aaa-server-group)# max-failed-attempts 5
```

```
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit
(config)# aaa-server TEST (inside) host 1.2.3.4
(config-aaa-server-host)# key testkey
(config-aaa-server-host)# authentication-port 1645
(config-aaa-server-host)# accounting-port 1646
(config-aaa-server-host)# retry-interval 10
(config-aaa-server-host)# exit
```

Tacacs+ authentication:

```
(config)# aaa-server TEST protocol tacacs+
(config-aaa-server-group)# max-failed-attempts 5
(config-aaa-server-group)# reactivation-mode depletion deadtime 10
(config-aaa-server-group)# exit
(config)# aaa-server TEST (inside) host 1.2.3.4
(config-aaa-server-host)# key testkey
(config-aaa-server-host)# exit
```

End-User Cut-Through Proxy:

```
(config)# aaa authentication include telnet outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ssh outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include ftp outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include http outside 0 0 0 0 SERVERTAG
(config)# aaa authentication include https outside 0 0 0 0 SERVERTAG
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
```

Where 0 identifies 0.0.0.0.

End-User Cut-Through Proxy with ACL:

```
(config)# access-list TEST permit 192.168.0.0 255.255.255.0
(config)# access-list TEST permit tcp any any eq ftp
(config)# access-list TEST permit tcp any any eq http
(config)# aaa authentication match TEST inside SERVERTAG
(config)# aaa-server SERVERTAG (inside) host 1.2.3.4
```

End-User Cut-Through Proxy with ACL and exempting some devices:

```
(config)# mac-list MACLIST permit 00c0.0000.0001 ffff.ffff.ffff
(config)# mac-list MACLIST permit 00c0.0000.0002 ffff.ffff.ffff
(config)# aaa mac-exempt match MACLIST
```

Define a limit to per-user proxy connections

```
(config)# aaa proxy-limit 50
```

Define an inactivity time

```
(config)# timeout uauth 00:30:00 inactivity
```

Cisco PIX/ASA Challenge 145

Title: Stateful Failover (Cable-based Active/Standby Failover)

Outline

The PIX 500 supports cable-based failover (stateful failover). With stateful failover the secondary device keeps a track of all the states of the primary firewall, and thus the secondary can seamlessly takes over from the primary.

Initially the failover cable connects between the PIX devices (primary and secondary). The cable end marked "Primary" is connected to the primary unit, and the other end to the secondary unit.

The IP address of an interface and its standby address can be defined with:

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0 standby 192.168.0.2
(config-if)# no shutdown
(config)# int e1
(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
(config-if)# no shutdown
```

Next the stateful failover is configured on the Stateful Failover link, such as:

```
(config)# failover link inf2 e2
```

in this case **inf2** is the name of the physical interface (e2). This will be used for the failover link. Next an IP address and failover address for the Stateful Failover link can be assigned:

```
(config)# int e2
(config-if)# no shutdown
(config)# failover interface ip inf2 192.168.2.1 255.255.255.0 standby 192.168.2.2
```

And then to enable failover:

```
(config)# failover
```

Objectives

The objectives of this challenge are to:

- Enable failover.
- Define failover addresses.

Commands

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0 standby 192.168.0.2
(config-if)# no shutdown
(config-if)# exit
(config)# int e1
(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
(config-if)# no shutdown
(config-if)# exit
```

```
(config)# int e2
(config-if)# no shutdown
(config-if)# exit
(config)# failover link inf2 e2
(config)# failover interface ip inf2 192.168.2.1 255.255.255.0 standby 192.168.2.2
(config)# failover
```

Example

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0 standby 192.168.0.2
(config-if)# no shutdown
(config-if)# exit
(config)# int e1
(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
(config-if)# no shutdown
(config-if)# exit
(config)# int e2
(config-if)# no shutdown
(config-if)# exit
(config)# failover link inf2 e2
(config)# failover interface ip inf2 192.168.2.1 255.255.255.0 standby 192.168.2.2
(config)# failover
```

Cisco PIX/ASA Test (Challenge 146)

Outline

This challenge involves taking a PIX/ASA test on failover.

Key commands

Stateful Failover (Cable-based Active/Standby Failover)

```
(config)# int e0
(config-if)# ip address 192.168.0.1 255.255.255.0 standby 192.168.0.2
(config-if)# no shutdown
(config-if)# exit
(config)# int e1
(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
(config-if)# no shutdown
(config-if)# exit
(config)# int e2
(config-if)# no shutdown
(config-if)# exit
(config)# failover link inf2 e2
(config)# failover interface ip inf2 192.168.2.1 255.255.255.0 standby 192.168.2.2
(config)# failover
```

Where E2 is used as the failover link, and the standby addresses for E0 and E1 are 192.168.0.2 and 192.168.1.2, respectively.

