

# Cisco Academy Network Security 2

## Cisco Router Challenge 192

### Outline

This challenge involves the downloading an IPS signature file, and using it.

### Objectives

The objectives of this challenge are to:

- Download IPS signature file.
- Apply it.
- Define logging.

### Example

```
> en
# config t
# copy tftp://10.0.0.1/new.sdf flash:new.sdf
(config)# config t

(config)# ip ips ?
deny-action Specify Deny action
fail        Specify what to do during any failures
name        Specify an IPS rule
notify      Specify the notification mechanisms (SDEE, nr-director or log)
            for the alarms
sdf         Specify the location of the signature definition file
signature   Add a policy to a signature

(config)# ip ips na ?
WORD       Name of IPS rule

(config)# ip ips na TEST ?
list       Specify an access list to match
<cr>

(config)# ip ips name TEST

(config)# ip ips sd ?
builtin    Use the built in signature definition file
location   Location of the signature definition file

(config)# ip ips sdf location ?
WORD       URL of the signature definition file

(config)# ip ips sdf location flash:attack-drop.sdf
```

```

(config)# int e0
(config-if)# ip ips ?
WORD Name of defined IPS rule

(config-if)# ip ips TEST ?
in Inbound IPS
out Outbound IPS

(config-if)# ip ips TEST in
(config-if)# exit

(config)# logging ?
Hostname or A.B.C.D IP address of the logging host
buffered Set buffered logging parameters
cns-events Set CNS Event logging level
console Set console logging parameters
count Count every log message and timestamp last occurrence
exception Limit size of exception flush output
facility Facility parameter for syslog messages
history Configure syslog history table
host Set syslog server IP address and parameters
monitor Set terminal line (monitor) logging parameters
on Enable logging to all enabled destinations
origin-id Add origin ID to syslog messages
rate-limit Set messages per second limit
reload Set reload logging level
server-arp Enable sending ARP requests for syslog servers when
first configured
source-interface Specify interface for source address in logging
transactions
trap Set syslog server logging level

(config)# logging on
(config)# logging 212.72.52.7
(config)# logging buffer ?
<0-7> Logging severity level
<4096-2147483647> Logging buffer size
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
xml Enable logging in XML to XML logging buffer
<cr>

(config)# logging buffer 440240
(config)# logging host 138.24.170.8
(config)# logging trap emergency
(config)# logging monitor emergency
(config)# logging console emergency
(config)# logging buffer emergency

```

In this case the logging of traps will be sent to the Syslog server.

## Cisco PIX Challenge 34

### Outline

This challenge involves the configuration of IDS signatures.

## Objectives

The objectives of this challenge are to:

- Define IP audit rules.
- Remove IDS signatures.

## Example

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

USAGE:

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

DESCRIPTION:

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

SYNTAX:

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

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

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

```
myPIX (config)# ip audit signature 3041 disable
myPIX (config)# ip audit signature 6100 disable
myPIX (config)# ip audit signature 6152 disable
```

```
myPIX (config)# logging ?
```

```
Usage:  [no] logging on
        [no] logging timestamp
        [no] logging standby
        [no] logging host [<in_if>] <l_ip> [tcp|udp/port#] [format {emblem}]
        [no] logging console <level>
        [no] logging buffered <level>
        [no] logging monitor <level>
        [no] logging history <level>
        [no] logging trap <level>
        [no] logging message <syslog_id> level <level>
        [no] logging facility <fac>
        [no] logging device-id hostname | ipaddress <if_name>
            | string <text>
        logging queue <queue_size>
        show logging [{message [<syslog_id>|all]} | level | disabled]
```

```
myPIX (config)# logging on
myPIX (config)# logging host 197.38.34.10
myPIX (config)# logging trap informational
myPIX (config)# logging monitor informational
myPIX (config)# logging console informational
myPIX (config)# logging buffer informational
```

# Cisco Router Challenge 56

## Outline

This challenge involves setting up IKE for a VPN connection.

## Objectives

The objectives of this challenge are to:

- Define the IKE policy.
- Define encryption.
- Define hash function.
- Define authentication type.
- Define identity type.
- Define authentication key and address (for pre-share authentication).
- Define the transform set.

## Example

```
> en
# config t
(config)# crypto isakmp enable
```

```
(config)# crypto isakmp policy 111
(config-isakmp)# encryption des
(config-isakmp)# hash sha
(config-isakmp)# authentication pre-share
(config-isakmp)# group 1
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
(config)# crypto isakmp key test address 192.168.1.1
(config)# crypto ipsec transform-set test esp-des
```

# Cisco Router Challenge 57

## Outline

This challenge involves setting up a crypto map and applying it to an interface.

## Objectives

The objectives of this challenge are to:

- Define a Crypto access-list, to identify the traffic to encrypt.
- Define IKE.
- Define a crypto map.
- Bind the ACL with the crypto map.
- Apply crypto map to E0.
- Show the tunnel details.

## Example

```
> en
# config t
(config)# hostname newhampshire
(config)# access-list 109 permit ip 50.93.142.0 0.0.255.255
      136.163.130.0 0.0.255.255
(config)# crypto isakmp enable
(config)# crypto isakmp policy 111
(config-isakmp)# ?
ISAKMP commands:
 authentication  Set authentication method for protection suite
 default         Set a command to its defaults
 encryption      Set encryption algorithm for protection suite
 exit            Exit from ISAKMP protection suite configuration mode
 group           Set the Diffie-Hellman group
 hash            Set hash algorithm for protection suite
 lifetime        Set lifetime for ISAKMP security association
```

```

no          Negate a command or set its defaults
(config-isakmp)# en ?
 3des      Three key triple DES
 aes       AES - Advanced Encryption Standard.
 des       DES - Data Encryption Standard (56 bit keys).
(config-isakmp)# encryption des
(config-isakmp)# hash ?
 md5       Message Digest 5
 sha       Secure Hash Standard
(config-isakmp)# hash sha
(config-isakmp)# authentication ?
 pre-share Pre-Shared Key
 rsa-encr  Rivest-Shamir-Adleman Encryption
 rsa-sig   Rivest-Shamir-Adleman Signature
(config-isakmp)# authentication pre-share
(config-isakmp)# g ?
 1         Diffie-Hellman group 1
 2         Diffie-Hellman group 2
 5         Diffie-Hellman group 5
(config-isakmp)# group 1
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
(config)# crypto isakmp key test address 192.168.1.1
(config)# crypto ipsec transform-set finland esp-des
(config)# crypto map manchester 10 ipsec-isakmp
(config-crypto-map)# ?
Crypto Map configuration commands:
 default      Set a command to its defaults
 description  Description of the crypto map statement policy
 dialer       Dialer related commands
 exit         Exit from crypto map configuration mode
 match        Match values.
 no           Negate a command or set its defaults
 qos          Quality of Service related commands
 reverse-route Reverse Route Injection.
 set          Set values for encryption/decryption
Router(config-crypto-map)# match ?
 address      Match address of packets to encrypt.

Router(config-crypto-map)# match address ?
 <100-199>    IP access-list number
 <2000-2699>  IP access-list number (expanded range)
 WORD         Access-list name
(config-crypto-map)# match address 109
(config-crypto-map)# set ?
 identity     Identity restriction.
 isakmp-profile Specify isakmp Profile
 peer         Allowed Encryption/Decryption peer.
 pfs          Specify pfs settings
 security-association Security association parameters
 transform-set Specify list of transform sets in priority order
(config-crypto-map)# set peer 144.55.62.1
(config-crypto-map)# s t ?
 WORD         Proposal tag
(config-crypto-map)# set transform-set finland
(config-crypto-map)# exit
(config)# int e0

```

```

(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shut
(config-if)# crypto map Manchester
(config-if)# exit
(config)# exit
# show crypto ipsec sa

```

```

interface: E0
  Crypto map tag: Manchester, local addr 192.168.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (50.93.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (136.163.0.0/255.255.0.0/0/0)
current_peer 192.168.1.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 43, #pkts encrypt: 43, #pkts digest: 43
  #pkts decaps: 43, #pkts decrypt: 43, #pkts verify: 43
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 4, #recv errors 0

local crypto endpt.: 192.168.1.1, remote crypto endpt.: 144.55.62.1
path mtu 1500, ip mtu 1500, ip mtu idb E0
current outbound spi: 0x267BC43(40352835)

```

```

inbound esp sas:
  spi: 0xD9F4BC76(3656694902)
  transform: esp-des
  in use settings = {Tunnel, }
  conn id: 2001, flow_id: SW:1, crypto map: Manchester
  sa timing: remaining key lifetime (k/sec): (4558868/3550)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

```

inbound ah sas:

```

```

inbound pcp sas:

```

```

outbound esp sas:
  spi: 0x267BC43(40352835)
  transform: esp-des
  in use settings = {Tunnel, }
  conn id: 2002, flow_id: SW:2, crypto map: Manchester
  sa timing: remaining key lifetime (k/sec): (4558868/3548)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

```

outbound ah sas:

```

```

outbound pcp sas:

```

```

# show crypto isakmp sa
dst          src          state          conn-id slot          status
144.55.62.1  192.168.1.1  QM_IDLE       1      0      ACTIVE

```

# Cisco Router Challenge 58

## Outline

This challenge involves setting an access-list to allow IPSec.

## Objectives

The objectives of this challenge are to:

- Create an access-list which allows AHP, ESP and ISAKMP.
- Applies the access-list.

## Example

```
> en
# config t
(config)# hostname london

london (config)# access-list 101 permit ahp host 117.84.81.2 host
61.222.47.2

london (config)# access-list 101 permit esp host 117.84.81.2 host
61.222.47.2

london (config)# access-list 101 permit udp host 117.84.81.2 host
61.222.47.2 eq isakmp

london (config)# int e0
london (config-if)# ip address 136.22.25.1 255.252.0.0
london (config-if)# no shut
london (config-if)# ip access-group 101 in
```

# Cisco PIX Challenge 22

## Outline

This challenge involves the configuration of ISAKMP.

## Objectives

The objectives of this challenge are to:

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

### Example

#### **pixfirewall(config)# isakmp**

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

#### **pixfirewall(config)# help isakmp**

USAGE:

```
isakmp am-disable
isakmp ipsec-over-tcp [port <port1>..<port10>]
isakmp disconnect-notify
(DEPRECATED) isakmp key <keystring> address <peer-address> [netmask <mask>]
[no-xauth] [no-config-mode]
isakmp enable <if_name>
isakmp identity {auto|address|hostname|key_id <key_id_str>}
(DEPRECATED) isakmp keepalive <threshold> [<retry-interval>]
isakmp nat-traversal [<natkeepalive>]
(DEPRECATED) isakmp client configuration address-pool local <pool-name>
[<if_name>]
(DEPRECATED) isakmp peer fqdn | ip <fqdn | ip> {no-xauth | no-mode-cfg}
isakmp policy <priority> authen {<pre-share|rsa-sig|dsa-sig>}
isakmp policy <priority> encrypt {<des|3des|aes|aes-192|aes-256>}
isakmp policy <priority> group {<1|2|5|7>}
isakmp policy <priority> hash {<md5|sha>}
isakmp policy <priority> lifetime <seconds>
isakmp reload-wait
```

DESCRIPTION:

isakmp            Configure ISAKMP key, peer, policy and other options

SYNTAX:

am-disable	Disable inbound aggressive mode connections
ipsec-over-tcp	Enable and configure IPSec over TCP
port	Set IPSec over TCP ports
<port1..port10>	Specify up to 10 IPSec over TCP ports
disconnect-notify	Enable disconnect notification to peers
key	Configure a pre-shared key associated with a peer

	This command is deprecated. Refer to 'tunnel-group ipsec-attributes' instead
<keystring>	String (ASCII) to be used for authentication pre-share
<peer-address>	IP address of peer associated with pre-shared key
<mask>	Netmask specified in dotted-decimal notation
no-xauth	Specifies an xauth policy exception
no-mode-config	Specifies a config mode policy exception
enable	Enable ISAKMP on specified interface
<if_name>	Interface name on which to enable ISAKMP
identity	Set identity type (address,hostname or key-id)
<address>	Use IP address of the interface for the identity
<auto>	Identity auto(IP address for preshared key and Cert DN for Cert based connections)
<hostname>	Use hostname of the device for the identity
<key-id>	Use specified key-id string for the identity
<key-id-str>	The string to be used as key-id
keepalive	Set keepalive interval. This command is deprecated. Refer to 'tunnel-group ipsec-attributes' instead
<threshold>	Time, in seconds, peer can remain idle before keep-alive monitoring commences
<retry-interval>	Time, in seconds, between keep-alive messages
nat-traversal	Enable and configure nat traversal
<natkeepalive>	Set nat traversal keepalive interval
<priority>	Policy suite priority (1 highest, 65535 lowest)
authentication	Authentication method (pre-share,rsa-sig or dsa-sig)
encryption	Encryption algorithm (des,3des,aes,aes-192 or aes256)
hash	Hash algorithm (md5 or sha)
group	Diffie-Hellman group (1,2,5 or 7)
lifetime	ISAKMP SA lifetime (seconds)
client configuration address-pool local	Configure client IP address pool attribute
	This command is deprecated. Refer to 'ip local-pool', 'tunnel-group general-attributes address-pool' instead
<pool-name>	Name of ip local pool to allocate dynamic client ip
<if_name>	Interface name the ip local pool is associated with
	Defaults to 'outside' if not specified
peer	Identify a peer security gateway to exempt from Xauth and/or Mode Configuration. This command is deprecated. Refer to 'isakmp identity' instead
<fqdn   ip>	Fully qualified domain name or IP address of a remote peer to be exempted from xauth or config mode policy
reload-wait	Wait for voluntary termination of sessions before reboot

see also: ca, dynamic-map, ipsec, map

```
(config)# isakmp enable outside
(config)# isakmp key ABC&FDD address 176.16.0.2 netmask 255.255.255.255
(config)# isakmp identity address
(config)# isakmp policy 5 authen pre-share
(config)# isakmp policy 5 encrypt des
(config)# isakmp policy 5 hash sha
(config)# isakmp policy 5 group 1
(config)# isakmp policy 5 lifetime 86400
```

```
(config)# show isakmp
```

## Cisco PIX Challenge 23

### Outline

This challenge involves the configuration of crypto details.

## Objectives

The objectives of this challenge are to:

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

## Example

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

USAGE:

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

DESCRIPTION:

sysopt                    Set system functional option

SYNTAX:

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

```
(config)# sysopt connection permit-ipsec
```

```
(config)# help cry
```

USAGE:

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

DESCRIPTION:

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

SYNTAX:

```

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

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

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

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

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

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

```

```

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

```

## Cisco PIX Challenge 24

### Outline

This challenge involves the configuration of VPDN.

### Objectives

The objectives of this challenge are to:

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

### Example

```

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

```

USAGE:

```

ip local pool <poolname> <ip1>[-<ip2>] [mask <netmask>]
ip verify reverse-path interface <if_name>

```

```

ip audit {info|attack} action [alarm] [drop] [reset]
ip audit name <audit_name> {info|attack} [action [alarm] [drop] [reset]]
ip audit interface <if_name> <audit_name>
ip audit signature <sig_number> disable
show|clear ip audit count [global] [interface <interface>]
clear configure ip audit [configuration]

```

DESCRIPTION:

```

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

```

SYNTAX:

```

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

```

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

```

(config)# ip local pool pptp-pool 10.0.0.1-10.0.0.100
(config)# help vpd

```

USAGE:

```

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

```

DESCRIPTION:

vpdn                    Configure VPDN (L2TP, PPPoE) Policy

SYNTAX:

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

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

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

## Cisco Router Challenge 194

### Outline

This challenge involves the configuration of a digital certificate server.

### Objectives

The objectives of this challenge are to:

- Enable domain name.
- Generate RSA keys.
- Define trustpoints.

### Example

```
# config t
(config)# hostname test
test(config)# ip host FRED 1.2.3.4

test(config)# ip domain-name test.com
test(config)# crypto ?
  ca                    Certification authority
  dynamic-map          Specify a dynamic crypto map template
  identity             Enter a crypto identity list
  ipsec                Configure IPSEC policy
  isakmp               Configure ISAKMP policy
```

```

key          Long term key operations
keyring     Key ring commands
map         Enter a crypto map
mib         Configure Crypto-related MIB Parameters
pki         Public Key components
wui         Crypto HTTP configuration interfaces
xauth       X-Auth parameters
test(config)# crypto ca ?
authenticate  Get the CA certificate
certificate   Actions on certificates
crl           Actions on certificate revocation lists
enroll        Request a certificate from a CA
export        Export certificate or PKCS12 file
import        Import certificate or PKCS12 file
profile       Define a certificate profile
trustpoint   Define a CA trustpoint
test(config)# cry ca t ?
WORD         CA Server Name

test(config)# cry ca t ANY ?
<cr>
test (config)# crypto ca trustpoint testing
test(ca-trustpoint)# ?
CA Trust Point configuration commands:
authorization  Authorization parameters.
auto-enroll    Automatically enroll this router identity
crl            CRL options
default        Set a command to its defaults
enrollment    Enrollment parameters
exit           Exit from certificate authority trustpoint entry mode
fqdn           include fully-qualified domain name
ip-address     include ip address
match          Match a certificate map
no             Negate a command or set its defaults
ocsp           OCSP parameters
password       revocation password
primary        Specify trustpoint as primary
query          Query parameters
regenerate     Regenerate keys on re-enrollment
revocation-check  Revocation checking options
root           Protocol to get CA certificate
rsakeypair    Specify rsakeypair for this identity
serial-number  include serial number
show           Show this router trustpoint
source         Specify source
subject-name   Subject Name
usage          Certificate Usage
vrf            vrf to use for enrollment and obtaining CRLs
test(ca-trustpoint)# enrollment ?
http-proxy    HTTP proxy server for enrollment
mode          Mode supported by the Certificate Authority
profile       Specify an profile for enrollment
retry         Polling parameters
terminal      Enroll via the terminal (cut-and-paste)
url           CA server enrollment URL
test(ca-trustpoint)# enrollment url ?
WORD          HTTP URL
flash:        Enroll via flash: file system
ftp:          Enroll via ftp: file system
http:         Enroll via http: file system
https:        Enroll via https: file system
null:         Enroll via null: file system
nvram:        Enroll via nvram: file system

```

```

pem      Include PEM encapsulation boundaries
rcp:     Enroll via rcp: file system
scp:     Enroll via scp: file system
system:  Enroll via system: file system
tftp:    Enroll via tftp: file system
<cr>
test(ca-trustpoint)# enrollment url http://testing/1.dll
test(ca-trustpoint)# crl ?
    optional Optional crl
    query      Query crl
test(ca-trustpoint)# crl optional
test(ca-trustpoint)# exit

test(config)# crypto ca authenticate ?
    WORD      CA Server Name
test(config)# crypto ca authenticate fred
test(config)# crypto ca enroll ?
    WORD      CA Server Name
<cr>
test(config)# crypto ca enroll fred

```

# Cisco Router Challenge 193

## Outline

This challenge involves the configuration of SNMP settings

## Objectives

The objectives of this challenge are to:

- Define SNMP parameters.

## Example

```

# config t

(config)# snmp-server ?
chassis-id      String to uniquely identify this chassis
community       Enable SNMP; set community string and access privs
contact         Text for mib object sysContact
context         Create/Delete a context apart from default
drop            Silently drop SNMP packets
enable          Enable SNMP Traps or Informs
engineID        Configure a local or remote SNMPv3 engineID
group           Define a User Security Model group
host            Specify hosts to receive SNMP notifications
ifindex         Enable ifindex persistence
location        Text for mib object sysLocation

```

```

packetsize      Largest SNMP packet size
queue-length    Message queue length for each TRAP host
system-shutdown Enable use of the SNMP reload command
tftp-server-list Limit TFTP servers used via SNMP
trap            SNMP trap options
trap-source     Assign an interface for the source address of all traps
trap-timeout    Set timeout for TRAP message retransmissions
user            Define a user who can access the SNMP engine
view            Define an SNMPv2 MIB view
(config)# snmp-server community popup ro
(config)# snmp-server contact june
(config)# snmp-server location glasgow
(config)# snmp-server enable ?
  informs      Enable SNMP Informs
  traps        Enable SNMP Traps
(config)# snmp-server enable traps
(config)# snmp-server chassis-id brighton

(config)# access-list 10 permit 10.0.0.0 0.0.0.255
(config)# access-list 10 deny any

(config)# snmp-server com popup ?
<1-99>          Std IP accesslist allowing access with this community string
<1300-1999>     Expanded IP accesslist allowing access with this community
                string
WORD            Access-list name
ro              Read-only access with this community string
rw             Read-write access with this community string
view           Restrict this community to a named MIB view
<cr>

(config)# snmp-server community popup ro ?
<1-99>          Std IP accesslist allowing access with this community string
<1300-1999>     Expanded IP accesslist allowing access with this community
                string
WORD            Access-list name
<cr>
(config)# snmp-server community popup ro 10

```

Which limits access to SNMP to only the 10.0.0.0 network.

## Cisco Router Challenge 194

### Outline

This challenge involves setting up the Easy VPN server on the IOS Firewall. In this challenge the details for the Cisco VPN Client will be defined.

### Objectives

The objectives of this challenge are to:

- Define AAA details.
- Define Cisco VPN group details.

- Define VPN details.

### Example

```

# config t
(config)# aaa new-model
(config)# aaa authentication login DEFAULT1 ?
    enable      Use enable password for authentication.
    group       Use Server-group
    krb5        Use Kerberos 5 authentication.
    krb5-telnet Allow logins only if already authenticated via Kerberos V
                Telnet.
    line        Use line password for authentication.
    local       Use local username authentication.
    local-case  Use case-sensitive local username authentication.
    none        NO authentication.
(config)# aaa authentication login DEFAULT1 local
(config)# aaa authorization network DEFAULT2 ?
    group       Use server-group.
    if-authenticated Succeed if user has authenticated.
    local       Use local database.
    none        No authorization (always succeeds).
(config)# aaa authorization network DEFAULT2 local

(config)# username fred password bert

(config)# ip local pool POOL1 10.0.0.1 10.0.0.254

(config)# crypto isakmp policy 5
(config-isakmp)# encryption des
(config-isakmp)# hash md5
(config-isakmp)# authentication pre-share
(config-isakmp)# group 2
(config-isakmp)# exit

```

The following details will be used by users for their VPN connection:

```

(config)# crypto isakmp client configuration group MYCONNECTION
(config-isakmp-group)# ?
ISAKMP group policy config commands:
    access-restrict  Restrict clients in this group to an interface
    acl              Specify split tunneling inclusion access-list number
    backup-gateway   Specify backup gateway
    dns              Specify DNS Addresses
    domain           Set default domain name to send to client
    firewall         Enforce group firewall feature
    group-lock       Enforce group lock feature
    include-local-lan Enable Local LAN Access with no split tunnel
    key              pre-shared key/IKE password
    max-logins       Set maximum simultaneous logins for users in this group
    max-users        Set maximum number of users for this group
    netmask          netmask used by the client for local connectivity
    no               Negate a command or set its defaults
    pfs              The client should propose PFS
    pool             Set name of address pool
    save-password    Allows remote client to save XAUTH password
    split-dns        DNS name to append for resolution
    wins             Specify WINS Addresses
    <cr>
(config-isakmp-group)# domain ?

```

```

WORD default domain name

(config-isakmp-group)# domain test.com

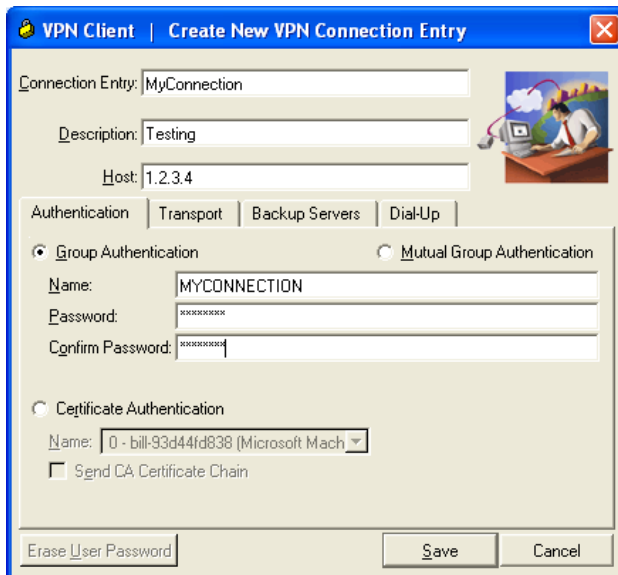
(config-isakmp-group)# key ?
0 Specifies an UNENCRYPTED password will follow
6 Specifies an ENCRYPTED password will follow
WORD The UNENCRYPTED (cleartext) user password
(config-isakmp-group)# key testing

(config-isakmp-group)# pool ?
WORD address pool name
(config-isakmp-group)# pool POOL1
(config-isakmp-group)# exit

```

On the VPN client the following details would be defined:

Group name: **MYCONNECTION**  
Group password: **testing**



The user, if successful, will then be allocated an address from the IP pool (POOL1).

Now we must define the IPSec transform to be used:

```

(config)# crypto ipsec transform-set MYSET esp-des

(cfg-crypto-trans)# ?
Crypto transform configuration commands:
 default Set a command to its defaults
 exit Exit from crypto transform configuration mode
 mode encapsulation mode (transport/tunnel)
 no Negate a command or set its defaults
(cfg-crypto-trans)# exit

```

To define the authorization and authentication for local users:

```
(config)# crypto map MYMAP client authentication list DEFAULT1
(config)# crypto map MYMAP isakmp authorization list DEFAULT2

(config)# crypto map MYMAP 10
(config-config-map)# set transform-set MYSET
(config-config-map)# exit
(config)# int e0
(config-if)# crypto map MYMAP
```