Troubleshooting the Implementation of IPSec VPNs

Session SEC-310

Virtual Private Network (VPN) Defined

“A Virtual Private Network carries private traffic over public network.”
What Is IPSec?

- IPSec stands for IP Security
- “A security protocol in the network layer will be developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality” (IETF)
Why IPSec? (Cont.)

- Standard for privacy, integrity and authenticity for networked commerce
- Implemented transparently in the network infrastructure
- End-to-end security solution including routers, firewalls, PCs, and servers

Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity to IPSec Peers
- Interoperability Troubleshooting
Router#  
!  
crypto isakmp policy 10  
    authentication pre-share  
crypto isakmp key gwock address 172.21.114.68  
!  
crypto IPSec transform-set t1 esp-des esp-md5-hmac  
!  
crypto map multi-peer 10 IPSec-isakmp  
    set peer 172.21.114.68  
    set transform-set t1  
    match address 151
Normal Router Configurations

interface Ethernet0
  ip address 172.21.114.123 255.255.255.224
  no ip directed-broadcast
  no ip mroute-cache
  crypto map multi-peer

access list 151 permit ip host 172.21.114.123 host 172.21.114.68

Router#sh crypto IPSec transform-set
Transform set t1: { esp-des esp-md5-hmac } will negotiate = { Tunnel, }
Normal Router Configurations

Router#sh crypto map
Crypto Map "multi-peer" 10 IPSec-isakmp
Peer = 172.21.114.68
Extended IP access list 151
access list 151 permit ip
source: addr = 172.21.114.123/0.0.0.0
dest: addr = 172.21.114.68/0.0.0.0
Current peer: 172.21.114.68
Security association lifetime: 4608000
kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ t1, }

The Two Main Debugs

- debug crypto isakmp
- debug crypto ipsec
Other Useful Debugs

- debug crypto engine
- debug ip packet <acl> detail
- debug ip error detail

Debuds Functionality Flow Chart
Tunnel Establishment

Interesting Traffic Received

- The ping source and destination addresses matched the match address access list for the crypto map multi-peer
  05:59:42: IPSec(sa_request): ,
  (key eng. msg.) src= 172.21.114.123,
  dest= 172.21.114.68,
- The 'src' is the local tunnel end-point, the 'dest' is the remote crypto end point as configured in the map
  src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
  dest_proxy= 172.21.114.68/255.255.255.255/0/0 (type=1),
- The src proxy is the src interesting traffic as defined by the match address access list; The dst proxy is the destination interesting traffic as defined by the match address access list

Tunnel Establishment

protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
- The protocol and the transforms are specified by the crypto map which has been hit, as are the lifetimes
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
  05:59:42: ISAKMP (1): beginning Main Mode exchange.....
- Note that the SPI is still 0; the main mode of negotiation is being started
ISAKMP Main Mode Negotiation

05:59:51: ISAKMP (1): processing SA payload. message ID = 0
05:59:51: ISAKMP (1): Checking ISAKMP transform 1 against priority 10 policy

- Policy 10 is the only isakmp policy configured on the router
  05:59:51: ISAKMP: encryption DES-CBC
  05:59:51: ISAKMP: hash SHA
  05:59:51: ISAKMP: default group 1
  05:59:51: ISAKMP: auth pre-share

- These are the isakmp attributes being offered by the other side

05:59:51: ISAKMP (1): atts are acceptable. Next payload is 0

- The policy 10 on this router and the atts offered by the other side matched
  05:59:53: ISAKMP (1): SA is doing preshared key authentication

- Preshared key authentication will start now
ISAKMP Authentication

05:59:53: ISAKMP (1): processing KE payload. message ID = 0
05:59:55: ISAKMP (1): processing NONCE payload. message ID = 0
• Nonce from the far end is being processed
05:59:55: ISAKMP (1): SKEYID state generated
05:59:55: ISAKMP (1): processing ID payload. message ID = 0
05:59:55: ISAKMP (1): processing HASH payload. message ID = 0
05:59:55: ISAKMP (1): SA has been authenticated
• Preshared authentication has succeeded at this point; the ISAKMP SA has been successfully negotiated

ISAKMP Quick Mode

• The quick mode is starting here, the IPSec SA will be negotiated here; ISAKMP will do the negotiating for IPSec as well
ISAKMP (1): beginning Quick Mode
exchange, M-ID of 132876399
IPSec(key_engine): got a queue event...
IPSec(spi_response): getting spi 6008371161d for SA
    from 172.21.114.68 to 172.21.114.123 for prot 3
ISAKMP gets the SPI from the IPSec routine to offer to the far side
ISAKMP (1): processing SA payload. message ID = 132876399
ISAKMP (1): Checking IPSec proposal 1
ISAKMP Quick Mode

- Here ISAKMP will process the IPSec attributes offered by the remote end
  ISAKMP: transform 1, ESP_DES
- This is the protocol offered by the remote end in accordance with its transform set
  ISAKMP: attributes in transform:
  ISAKMP: encaps is 1
  ISAKMP: SA life type in seconds
  ISAKMP: SA life duration (basic) of 3600

ISAKMP Quick Mode

  ISAKMP: SA life type in kilobytes
  ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
  ISAKMP: authenticator is HMAC-MD5
- This is the payload authentication hash offered by the remote end in accordance with its transform set
  ISAKMP (1): atts are acceptable.
- The IPSec SA has now been successfully negotiated; ISAKMP will now go into a state known as QM-IDLE
05:59:55: IPSec(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.21.114.68,
src= 172.21.114.123,
|dest_proxy|= 172.21.114.68/255.255.255.255/0/0 (type=1),
|src_proxy|= 172.21.114.123/255.255.255.255/0/0 (type=1),
|protocol|= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

Here ISAMKP has asked the IPSec routine to validate the IPSec proposal that it has negotiated with the remote side.

05:59:55: ISAKMP (1): Creating IPSec SAs
(proxy 172.21.114.68 to 172.21.114.123)
05:59:55: has spi 600837116 and conn_id 2 and flags 4
05:59:55: lifetime of 3600 seconds
05:59:55: lifetime of 4608000 kilobytes
IPSec SA Establishment

(proxy 172.21.114.123 to 172.21.114.68)
05:59:55: has spi 130883577 and conn_id 3 and flags 4
05:59:55: lifetime of 3600 seconds
05:59:55: lifetime of 4608000 kilobytes

- Two IPSec SAs have been negotiated, an incoming SA with the SPI generated by the local machine and an outbound SA with the SPIs proposed by the remote end; Crypto engine entries have been created

IPSec SA Establishment

- Here the ISAKMP routine will inform the IPSec routine of the IPSec SA so that the SADB can be populated
05:59:55: IPSec(initialize_sas): ,
(key eng. msg.) dest= 172.21.114.123, src= 172.21.114.68,
dest_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
src_proxy= 172.21.114.68/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac,
lifedur= 3600s and 4608000kb,
spi= 0x23D00BFC (600837116), conn_id= 2, keysize= 0,
flags= 0x4
IPSec SA Establishment

05:59:56: IPSec(initialize_sas):,
(key eng. msg.) src= 172.21.114.123, dest= 172.21.114.68,
src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
dest_proxy= 172.21.114.68/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x7CD1FF9(130883577), conn_id= 3, keysize= 0, flags= 0x4

• The IPSec routine is populating the SADB with the IPSec entries

05:59:56: IPSec(create_sa): sa created,
(sa) sa_dest= 172.21.114.123, sa_prot= 50,
sa_spi= 0x23D00BFC(600837116),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2

05:59:56: IPSec(create_sa): sa created,
(sa) sa_dest= 172.21.114.68, sa_prot= 50,
sa_spi= 0x7CD1FF9(130883577),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3

• The SADB has been updated and the IPSec SAs have been initialized.
• The tunnel is now fully functional
Show Commands

- Sh crypto engine conn active
- Sh crypto isakmp sa
- Sh crypto ipsec sa
- Sh crypto engine configuration

Router#sh cry engine connection active

<table>
<thead>
<tr>
<th>ID</th>
<th>Interface</th>
<th>IP-Address</th>
<th>State</th>
<th>Algorithm</th>
<th>Encrypt</th>
<th>Decrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>no idb</td>
<td>no address</td>
<td>set</td>
<td>DES_56_CBC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>This is the ISAKMP SA</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Ethernet0</td>
<td>172.21.114.123</td>
<td>set</td>
<td>HMAC_MD5+DES_56_CBC</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Ethernet0</td>
<td>172.21.114.123</td>
<td>set</td>
<td>HMAC_MD5+DES_56_CBC</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>These two are the IPSec SAs</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Router#sh crypto isakmp sa

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.21.114.68</td>
<td>172.21.114.123</td>
<td>QM_IDLE</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Show Commands

Router#sh crypto IPSec sa
interface: Ethernet0
  Crypto map tag: multi-peer, local addr. 172.21.114.123
  local ident (addr/mask/prot/port):
    (172.21.114.123/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port):
    (172.21.114.68/255.255.255.255/0/0)
  current_peer: 172.21.114.68
  PERMIT, flags={origin_is_acl},
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
  #send errors 0, #recv errors 0

local crypto endpt.: 172.21.114.123, remote crypto endpt.:
  172.21.114.68
  path mtu 1500, media mtu 1500
  current outbound spi: 7CD1FF9

  inbound esp sas:
    spi: 0x23D00BFC(600837116)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2, crypto map: multi-peer
    sa timing: remaining key lifetime (k/sec): (4607999/3400)
  IV size: 8 bytes
  replay detection support: Y
Show Commands

inbound ah sas:

outbound esp sas:

spi: 0x7CD1FF9(130883577)
transform: esp-des esp-md5-hmac,
in use settings = (Tunnel, )
slot: 0, conn id: 3, crypto map: multi-peer
sa timing: remaining key lifetime (k/sec): (4607999/3400)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

Show Commands

router#sh crypto engine configuration

crypto engine name: unknown
crypto engine type: ISA/ISM
CryptIC Version: FF41
CGX Version: 0111
DSP firmware version: 0061
MIPS firmware version: 0003030F
ISA/ISM serial number: 
B82CA6C09E080DF0E0A1029EF8E7112F3FF5F67B
     PCBd info: 3-DES [07F000260000]
Compression: No
3 DES: Yes
Show Commands

Privileged Mode: 0x0000

- Maximum buffer length: 4096
- Maximum DH index: 1014
- Maximum SA index: 2029
- Maximum Flow index: 4059
- Maximum RSA key size: 0000
- crypto engine in slot: 5
  - platform: predator crypto_engine

Crypto Adjacency Counts:
- Lock Count: 0
- Unlock Count: 0

Common Issues

- Incompatible ISAKMP policy or preshared secrets
- Incompatible or incorrect access lists
- Crypto map on the wrong interface
- Incorrect SA selection by the router
- Routing issues
- Caveats: switching paths
Incompatible ISAKMP Policy or Preshared Secrets

- If no ISAKMP policies configured match, or if no preshared key for the negotiating peer is configured, the router tries the default policy, 65535, and if that too does not match it fails ISAKMP negotiation.

- A `sh crypto isakmp sa` shows the ISAKMP SA to be in `MM_NO_STATE`, meaning the main-mode failed.

%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode Failed with Peer at 155.0.0.1

Private

Encrypted

Public

Private

Router

Internet
Incompatible ISAKMP Policy or Preshared Secrets

- If the preshared secrets are not the same on both sides, the negotiation will fail again, with the router complaining about sanity check failed

- A `sh crypto isakmp sa` shows the ISAKMP SA to be in `MM_NO_STATE`, meaning the main mode failed
Incompatible ISAKMP Policy or Preshared Secrets

ISAKMP (62): processing SA payload. message ID = 0
ISAKMP (62): Checking ISAKMP transform 1 against priority 10 policy
  encryption DES-CBC
  hash SHA
  default group 1
  auth pre-share
ISAKMP (62): attrs are acceptable. Next payload is 0
ISAKMP (62): SA is doing preshared key authentication
ISAKMP (62): processing KE payload. message ID = 0
ISAKMP (62): processing NONCE payload. message ID = 0
ISAKMP (62): SKEYID state generated
ISAKMP (62): processing vendor id payload
ISAKMP (62): speaking to another IOS box!
ISAKMP: reserved no zero on payload 5!
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 155.0.0.1 failed its
sanity check or is malformed

Incompatible or Incorrect Access Lists

- If the access lists on the two routers don’t match or at least overlap, INVALID PROXY IDS or PROXY IDS NOT SUPPORTED will result
- It is recommended that access lists on the two routers be ‘reflections’ of each other
- It is also highly recommended that the key words any not be used in match address access lists
Incompatible or Incorrect Access Lists

3d00h: IPSec(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.16.171.5, src= 172.16.171.27,
    dest_proxy= 172.16.171.5/255.255.255.255/0/0 (type=1),
    src_proxy= 172.16.171.27/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spie= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
3d00h: validate proposal request 0
3d00h: IPSec(validate_transform_proposal): proxy identities not supported
3d00h: ISAKMP (0:3): IPSec policy invalidated proposal
3d00h: ISAKMP (0:3): phase 2 SA not acceptable!

Access List:
access list 110 permit ip host 172.16.171.5 host 172.16.171.30
Crypto Map on the Wrong Interface

• The crypto map needs to be applied to the outgoing interface of the router; if you don’t want to use the outside interface’s IP as the local ID, use the command `crypto map <name> local address <interface>`, to specify the correct interface.

• If there are physical as well as logical interfaces involved in carrying outgoing traffic, the crypto map needs to be applied to both.

Incorrect SA Selection by the Router

• If there are multiple peers to a router, make sure that the match address access lists for each of the peers are mutually exclusive from the match address access list for the other peers.

• If this is not done, the router will chose the wrong crypto map to try and establish a tunnel with one of the peers.
Incorrect SA Selection by the Router

Identity Doesn’t Match Negotiated Identity

Router

Private

Internet

Encrypted

Public

Router

Private

Identity doesn’t match negotiated identity

(ip) dest_addr= 1.2.3.4, src_addr= 2.3.4.5, prot= 1
(ident) local=5.5.5.5, remote=6.6.6.6
local_proxy=1.2.3.5/255.255.255.255/0/0,
remote_proxy=2.3.4.5/255.255.255.255/0/0

Access list for 5.6.7.8:
Access-list 100 permit ip host 1.2.3.5 host 5.6.7.9
Access-list 100 permit ip host 1.2.3.5 host 2.3.4.5

Access list for 1.2.3.4:
Access-list 110 permit ip host 1.2.3.5 host 2.3.4.5
Routing Issues

- A packet needs to be routed to the interface which has the crypto map configured on it before IPSec will kick in
- Routes need to be there not only for the router to reach its peers address but also for the IP subnets in the packets once they have been decrypted
- Use the `debug ip packet <acl> detailed` to see if the routing is occurring correctly (be careful on busy networks!)

Caveats: Switching Paths

- Different switching methods use completely different code paths; it is very much possible to have one switching method break IPSec (due to a bug maybe) and another one to function correctly
- Try a different switching path (cef, fast switching, process switching (possible performance impact) etc.) in case you are running into an obscure problem
Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting

Layout

![Diagram of network layout with VPN client, routers, and encrypted communication between private and public networks.]
Standard Configuration

access list bypassingnat permit ip 172.16.0.0 255.255.0.0 10.1.100.0 255.255.255.0
access list bypassingnat permit ip host 20.1.1.1 host 10.1.1.1
access list 101 permit ip host 20.1.1.1 host 10.1.1.1

ip address outside 192.168.10.1 255.255.255.0
nat (inside) 0 access list bypassingnat
route inside 20.0.0.0 255.0.0.0 172.16.171.13 1

aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server myserver protocol tacacs+
aaa-server myserver (inside) host 171.68.178.124 cisco timeout 5

Standard Configuration

sysopt connection permit-IPSec
crypto IPSec transform-set mysetdes esp-des esp-md5-hmac
crypto dynamic-map mydynmap 10 set transform-set mysetdes
crypto map newmap 20 IPSec-isakmp
crypto map newmap 20 match address 101
crypto map newmap 20 set peer 192.168.10.2
crypto map newmap 20 set transform-set mysetdes
crypto map newmap 30 IPSec-isakmp dynamic mydynmap
crypto map newmap client configuration address initiate
crypto map newmap client authentication myserver
Standard Configuration

crypto map newmap interface outside
isakmp enable outside

isakmp key mysecretkey address 0.0.0.0 netmask 0.0.0.0
isakmp key myotherkey address 192.168.10.2 netmask 255.255.255.255
no-xauth no-config-mode

isakmp identity address
isakmp client configuration address-pool local vpnpool outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000

Common Issues

- Bypassing NAT
- Enabling ISAKMP
- Missing sysopt commands
- Combining PIX-PIX and PIX-VPN issues
Bypassing NAT

• Nat needs to be bypassed on the PIX in order for the remote side to access the private network behind the PIX seamlessly

• Use the sysopt IPSec pl-compatible command to bypass NAT till 5.1; from 5.1 onwards use the NAT 0 command with an access list

Enabling ISAKMP

• Unlike the router, ISAKMP is not enabled by default on the PIX

• Use the command enable isakmp <interface> to enable it on an interface
Missing Sysopt Commands

- At least one and before 5.1, two sysopt commands are needed for the PIX to work correctly
- Sysopt connection permit-IPSec
- Sysopt IPSec pl-compatible (not needed after 5.1)

Combining PIX-PIX and PIX-VPN Issues

- If you are doing mode config or x-auth for the VPN clients you would need to disable that for the PIX to PIX connection
- Use the no mode-config and no x-auth tags at the end of the preshared key definitions to disable mode config and x-auth
Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting

Layout

VPN Client

Internet

192.168.10.1

VPN 3000

Private

192.168.10.2

VPN 3000

Private

Encrypted

Public
### Cisco VPN 3000 Standard Configuration (Remote Access IPSec VPN)

#### General Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Hours</td>
<td></td>
<td>Select the access hours assigned to the group.</td>
</tr>
<tr>
<td>Simultaneous Logins</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Alphabetic Only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle Timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Connects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary DNS</td>
<td></td>
<td>Enter the IP address of the primary DNS server.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary WINS</td>
<td></td>
<td>Enter the IP address of the primary WINS server.</td>
</tr>
<tr>
<td>Secondary WINS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEP Card Assignment</td>
<td></td>
<td>Select the SEP card assignment.</td>
</tr>
<tr>
<td>Tunneling Protocols</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strip Domain</td>
<td></td>
<td>Check to remove the domain qualifier from names.</td>
</tr>
</tbody>
</table>

#### IPSec Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec SA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE Peer Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE Keepalive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reauthentication Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnel Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Remote Access Parameters

- **Internal, RADIUS, NT, SD**

...continued...
### Cisco VPN 3000 Standard Configuration (Remote Access IPSec VPN)

#### Mode Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Password Storage on Client</td>
<td>Check to allow the IPSec client to store the password locally.</td>
</tr>
<tr>
<td>Split Horizon</td>
<td>Select the network list to be used for split tunneling.</td>
</tr>
<tr>
<td>Default Domain Name</td>
<td>Enter the default domain name given to users of this group.</td>
</tr>
</tbody>
</table>

#### IPSec through NAT

- Check to allow the IPSec client to operate through a traversal using NAT via UDP.
- Enter the UDP port to be used for IPSec through NAT (4001 - 49151).

### Configuration | User Management | Users | Add

#### Identity Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>&lt;user&gt;</td>
<td>Enter a unique user name.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>Enter the user’s password. The password must satisfy the group password requirements.</td>
</tr>
<tr>
<td>Verify</td>
<td></td>
<td>Verify the user’s password.</td>
</tr>
<tr>
<td>Group</td>
<td>&lt;group&gt;</td>
<td>Enter the group to which the user belongs.</td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td>Enter the IP address assigned to this user.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
<td>Enter the subnet mask assigned to this user.</td>
</tr>
</tbody>
</table>

Add | Cancel
**Cisco VPN 3000 Debug Tool (Event Log)**

### Configure Event Log on VPN 3000 Concentrator:

This screen lets you add and configure an event class for special handling.

- **Class Name**: IKE
- **Enable**: Yes
- **Severity to Log**: 1-13

### Most commonly used classes for IPSec VPN:

**IKE** | **IKEDBG** | **IPSEC** | **IPSECDBG** | **AUTH** | **AUTHDBG**
--- | --- | --- | --- | --- | ---

**Raise Severity to Level 13 During Troubleshooting and set it back to default When it is done**

---

**Cisco VPN 3000 Debug Tool (Event Log)**

- **Use FILTER and FILTERDBG for packet level debugging**
  - Define specific rules and assign them to the top of the filter
  - Apply the filter to the interface
  - Enable FILTER and FILTERDBG Classes to Severity Level 13
  - Monitoring the Event Log
Cisco VPN 3000
Debug Tool (Event Log)

Monitoring Event Log

Select Filter Options
Event Class
- All Classes
- AUTH
- AUTHNOP
- AUTHDECODE

Client IP Address
Group
- All-

Direction
- Oldest to Newest

Events/Page
100

6458 04/18/2001 04:24:52.990 SEP-9 IKE/0 RPT=365 172.16.172.19
Generating keys for Initiator...

Common Issues

- Common configuration errors in remote access IPSec VPNs
- No access to Internet after the VPN tunnel is established
- Routing issues
Common Configuration Errors in Remote Access IPSec VPNs

- **Filter missing on public interface**
  
  8 04/28/2001 11:08:47.630 SEV=4 IKE/2 RPT=2 171.68.9.125
  Filter missing on interface 2, IKE data from Peer 171.68.9.125 dropped

- **IPSec feature is not enabled under VPN group setup**
  
  46 04/28/2001 11:51:22.980 SEV=4 IKE/51 RPT=1 171.68.9.125
  Group [ciscotac]
  Terminating connection attempt: IPSEC not permitted for group (ciscotac)

- **Wrong group name configured on VPN client**
  
  469 04/28/2001 12:08:59.770 SEV=4 IKE/22 RPT=22 171.68.9.125
  No Group found matching ciscotech for Pre-shared key peer 171.68.9.125

- **Wrong group password configured on VPN client**
  
  305 04/28/2001 11:58:39.020 SEV=5 IKE/68 RPT=2 171.68.9.125
  Group [ciscotac]
  Received non-routine Notify message: Invalid hash info (23)

- **Wrong user password inputted by user**
  
  333 04/28/2001 12:08:25.320 SEV=3 AUTH/5 RPT=1 171.68.9.125
  Authentication rejected: Reason = Invalid password
  handle = 23, server = Internal, user = vpnuser, domain = <not specified>

- **IP address assignment scheme not specified on concentrator**
  
  420 04/28/2001 12:03:23.780 SEV=5 IKE/132 RPT=1 171.68.9.125
  Group [ciscotac] User [vpnuser]
  Cannot obtain an IP address for remote peer
No Access to Internet after VPN Tunnel Is Established

- After remote users establish the IPSec tunnel, they can no longer access the internet since all traffic is tunneled through the VPN to the private network;
- Use the split Tunneling feature to encrypt specific traffic

Routing Issues

Cisco VPN 3000 In Parallel Position with PIX Firewall

- PIX doesn’t redirect packets, use the router as host’s default gateway
- Router has a specific route for VPN traffic and the gateway of last resort is the PIX
- Router is Configured as tunnel default gateway on VPN 3000 Concentrator
Routing Issues

**Cisco VPN 3000 behind PIX Firewall**

Private

Public

Internet

- Better design. VPN 3000 concentrator protected by stateful firewall.
- Make sure that the PIX has holes for VPN traffic

Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting
Cisco VPN 5000 Standard Configuration

[ General ]

IPSecGateway = 200.1.1.1

[ IP Ethernet 0:0 ]

IPBroadcast = 20.1.1.255
SubnetMask = 255.255.255.0
IPAddress = 20.1.1.1
Mode = Routed

[ IP Ethernet 1:0 ]

Mode = Routed
IPBroadcast = 200.1.1.255
SubnetMask = 255.255.255.0
IPAddress = 200.1.1.2
Cisco VPN 5000 Standard Configuration

[ IKE Policy ]
  Protection = MD5_DES_G1

[ Tunnel Partner VPN 1 ]
  SharedKey = "cisco"
  BindTo = "ethernet 1:0"
  Transform = esp(md5,des)
  Mode = Aggressive
  KeyManage = Auto
  Partner = 200.1.1.1

[ IP VPN 1 ]
  Mode = Routed
  Numbered = Off

Cisco VPN 5000 Standard Configuration

[ IP Static ]
  50.1.1.0 255.255.255.0 VPN 1 1

[ VPN Group "testgroup" ]
  IPNet = 20.1.1.0/24
  Transform = esp(sha,3des)
  Transform = esp(md5,des)
  StartIPAddress = 20.1.1.10
  MaxConnections = 5
  BindTo = "ethernet 0:0"

[ VPN Users ]
cisco1 config="testgroup" sharedkey="ciscocisco"
Cisco VPN 5000 Standard Configuration

[ Radius ]

ChallengeType = Off
VPNPassword = 78
VPNGroupInfo = 79
BindTo = "ethernet0:0"
Secret = "cisco123"
Authentication = On
AcctPort = 1646
AuthPort = 1645
PrimAddress = "20.1.1.2"

Cisco VPN 5000 Debug Commands

• Configure logging on VPN 5000 Concentrator

[ Logging ]

LogToAuxPort = On
Enabled = On
LogToSysLog = Off
Level = 7

• Display the log in buffer:

Show system log buffer
Cisco VPN 5000 Show Commands

- **Show commands:**
  - Show vpn partner [verbose]
  - Show vpn stat [verbose]
  - Show vpn user [verbose]
  - Show vpn runtime

- **VPN trace dump**
  - Vpn trace dump all
  - Vpn trace dump user <username|ip addr>

---

5002# sh vpn partner ver

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Partner Address</th>
<th>Partner Port</th>
<th>Default</th>
<th>Bindto Port</th>
<th>Connect Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN 0:1</td>
<td>200.1.1.1</td>
<td>500</td>
<td>No</td>
<td>200.1.1.2</td>
<td>00:00:00:12</td>
</tr>
</tbody>
</table>

- Auth/Encrypt: MD5e/DES
- User Auth: Shared Key
- Access: Dynamic
- Start: 904 seconds
- Managed: 904 seconds
- State: imnt_maintenance
Cisco VPN 5000 Show Commands

```
sh vpn stat ver
```

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>In</th>
<th>Water</th>
<th>Total</th>
<th>Running</th>
<th>Tunnel Starts</th>
<th>Tunnel OK</th>
<th>Tunnel Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Partners</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stats</th>
<th>VPN1</th>
<th>VPN0</th>
<th>Stats</th>
<th>VPN1</th>
<th>VPN0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrapped</td>
<td>6</td>
<td>4</td>
<td>rx IP</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Unwrapped</td>
<td>0</td>
<td>4</td>
<td>rx IPX</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BadEncap</td>
<td>0</td>
<td>0</td>
<td>rx Apple</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BadAuth</td>
<td>0</td>
<td>0</td>
<td>rx Other</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BadEncrypt</td>
<td>0</td>
<td>0</td>
<td>tx IP</td>
<td>7</td>
<td>4</td>
</tr>
</tbody>
</table>

Cisco VPN 5000 Common Problems

- Common configuration errors
- Extended authentication using Radius
- Interoperability with other VPN products
- Routing issues
Common Configuration Errors (LAN-to-LAN IPSec)

- **Shared key doesn't match**
  Error 48.24 seconds IKE ERROR: Authentication Failed
  Notice 48.26 seconds VPN 0:2 reset: connection script finished.
  Notice 48.29 seconds reason: _S_HASH_MISMATCH_ (24381982)

- **IKE policy doesn't match**
  Notice 6988.42 seconds <No ifp> reset: no matching proposals in [ IKE Policy ] section.

- **Remote peer doesn't have “bindto” under VPN tunnel partner**
  Error 2576.16 seconds step_do_isakmp_pkt: no conn/mgr for, src IP [30.1.1.1]
  Error 2576.19 seconds . . . dropping ISAKMP admin packet
  Warnin 2616.12 seconds LAN-LAN connection attempt from 30.1.1.1 dropped, no policy found

Common Configuration Errors (Remote Access IPSec)

- **Bad shared secret input by users**
  New IKE connection: [200.1.1.5]:1050:cisco
  Bad IKE authentication request from cisco at 200.1.1.5
  VPN 0:0 (cisco) reset due to connection failure.

- **Invalid Username inputted by users**
  New IKE connection: [200.1.1.5]:1052:cisco123
  Invalid user configuration for cisco123
  <No ifp> (cisco123) reset -- user is unknown / invalid.

- **The group name configured under VPN users section does not exist**
  New IKE connection: [200.1.1.5]:1061:vpnuser
  User, "vpnuser", has an invalid VPN Group config, "vpngroup"
  <No ifp> (vpnuser) reset: connection script finished.
  -- reason: _S_NO_POLICY_ (220@772)
Extended Authentication Using Radius

- Other than the Radius username and password, two more attributes need to be defined on the Radius server: **VPNPassword** (shared secret) and **VPNGroupInfo** (corresponding to VPN group defined on concentrator)

- Radius server informs the concentrator which VPN group the user belongs to, by replying with the **VPNGroupInfo** attribute

- Make sure the attribute number defined on concentrator matches the Radius attribute number used in the Radius server

Extended Authentication Using Radius

**Typical Logs with different Radius Authentication Errors:**

**Radius Server is Unreachable**
New IKE connection: [200.1.1.5]:1040:vpnuser
Sending RADIUS CHAP challenge to vpnuser at 200.1.1.5
Received RADIUS challenge resp. from vpnuser at 200.1.1.5, contacting server
(vpnuser) reset: RADIUS server never responded.

**Radius Username or Password invalid:**
New IKE connection: [200.1.1.5]:1041:vpnuser
Sending RADIUS CHAP challenge to vpnuser at 200.1.1.5
Received RADIUS challenge resp. from vpnuser at 200.1.1.5, contacting server
Auth request for vpnuser rejected by RADIUS server
(vpnuser) reset due to RADIUS authentication failure
Extended Authentication Using Radius

VPN Group Name Returned From Radius Server does not match VPN Group Name on Concentrator

New IKE connection: [200.1.1.5]:1042:vpnuser
Sending RADIUS CHAP challenge to vpnuser at 200.1.1.5
Received RADIUS challenge resp. From vpnuser at 200.1.1.5, contacting server
User, “vpnuser”, has an invalid VPN Group config, “fakegroup”
(vpnuser) reset: connection script finished.
reason: S_NO_POLICY (220@772)

• Also check radius authentication logs which might indicate where the problem is

Interoperability with Other VPN Products

• Use main mode instead of aggressive mode
• Use Default Responder if remote peer doesn’t have static IP address
• Different from IOS, PIX and VPN 3000, VPN 5000 establishes VPN tunnel during boot time (instead of being triggered by interesting traffic)
• Caveat in current version: only supports phase II IKE rekey
Interoperability with Other VPN Products

- **KeyManage** modes decide who initiates VPN tunnel:
  - **Initiate**—IKE initiator, never responds (including IKE rekey)
  - **Respond**—IKE responder, never initiates
  - **Auto**—Partner lower IP address is IKE initiator (only used for proprietary tunnel)
  - **Manual**—No IKE; used for GRE tunnel

Interoperability with Other VPN Products

- **Default VPN Tunnel Configuration**
  
  [ Tunnel Partner VPN Default ]
  - **SharedKey** = "cisco123"
  - **Transform** = esp(md5,des)
  - **BindTo** = "ethernet 1:0"

  [ IP VPN Default ]
  - **Numbered** = Off
  - **Mode** = Routed
Interoperability with Other VPN Products

- **Main Mode VPN Tunnel Configuration**
  
  [ Tunnel Partner VPN 2 ]
  
  LocalAccess = "20.1.1.0/24"
  Peer = "60.1.1.0/24"
  Partner = 200.1.1.10
  Mode = Main
  KeyManage = respond
  BindTo = "ethernet1:0"
  Transform = esp(md5,des)
  SharedKey = "cisco123"

  [ IP VPN 2 ]
  Numbered = Off
  Mode = Routed

Routing Issue

- Use **IPSecGateway** (VPNGateway in v6.0) to define the next hop after packets are encrypted
- Default route under [ IP Static ] section can be saved for internal network routing
- For aggressive mode LAN-to-LAN VPN, static routes are still needed to forward packets to corresponding VPN tunnels even if IPSecGateway has been configured
**Agenda**

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting

**Common Problems**

- Incorrect time settings
- Unable to query the servers
- Incorrect CA identity
- Cert request rejections by CA
- CRL download issues
Debugging Tools

- debug crypto pki m
- debug crypto pki t

Incorrect Time Settings

- Incorrect time setting can result in the machine considering the validity date of a certificate to be in the future or the past, resulting in main mode failure
- Use `sh clock` and `set clock`
- Configure network time protocol (NTP)
Unable to Query the Servers

- The CA and/or the RA server should be accessible from the router

- Error messages:
  
  CRYPTO_PKI: socket connect error.
  CRYPTO_PKI: 0, failed to open http connection
  CRYPTO_PKI: 65535, failed to send out the pki message

  or

  a Failed to query CA certificate message

Incorrect CA Identity

- Sample CA IDs for three major Certificate Authority servers are:

- Entrust:

  crypto ca identity sisu.cisco.com
  
  hq_sanJose(cfg-ca-id)# enrollment mode ra
  hq_sanJose(cfg-ca-id)# enrollment url http://entrust-ca
  hq_sanJose(cfg-ca-id)# query url http://entrust-ca
  hq_sanJose(cfg-ca-id)# crl optional
Incorrect CA Identity

- Microsoft:
  - crypto ca identity cisco.com
  - enrollment retry count 100
  - enrollment mode ra
  - enrollment url http://ciscob0tpyy88:80/certsrv/mscep/mscep.dll
  - crl optional
- Verisign:
  - cry ca identity smalik.cisco.com
  - enrollment url http://testdriveIPSec.verisign.com
  - crl option

Cert Request Rejections by CA

‘Certificate enrollment request was rejected by Certificate Authority’

- Most common cause for this is that the CA has already issued certificates for the device; revoke the previously issued certificates and try again
CRL Download Issues

- CRL optional can avoid main mode failure with the 'invalid certificate' error
- A work around could also be to download the CRL manually using the 'Crypto ca crl download' command

Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting
Common Problems

- Bypassing static NAT entries
- NAT in the middle of an IPSec tunnel

Bypassing Static NAT Entries

- Static NAT entries can be bypassed using a loopback interface and policy routing
- Tools to debug this setup are:
  - Debug ip nat
  - Debug ip policy
  - Debug ip packet
Bypassing Static NAT Entries

crypto map test 10 IPSec-isakmp
  set peer 1.1.1.1
  set transform-set transform
  match address 100

interface Loopback1
  ip address 10.2.2.2 255.255.255.252

interface Ethernet0/0
  ip address 1.1.1.2 255.255.255.0
  ip nat outside
  crypto map test

Bypassing Static NAT Entries

interface Ethernet0/1
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
  ip route-cache policy
  ip policy route-map nonat

  ip nat inside source access list 1 interface Ethernet0/0 overload
  ip nat inside source static 10.1.1.2 100.1.1.3
  access list 1 permit 10.0.0.0 0.255.255.255
  access list 100 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
  access list 120 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
  route-map nonat permit 10
    match ip address 120
    set ip next-hop 10.2.2.1


NAT in the Middle of an IPSec Tunnel

- **Problem 1:** IPSec end point behind a PATing device; no solution; you can't do PAT if you can't see the ports
- **Hint:** Use IPSec/UDP with VPN 3000 or IPSec in HTTP (fTCP) with VPN 5000 for Problem 1
- **Problem 2:** IPSec end point device behind a static Nat translating device

---

NAT in the Middle of an IPSec Tunnel

- For PIX-to-PIX or PIX-to-router scenarios use normal IPSec configs
- For PIX-to-Cisco Secure VPN client or router-to-Cisco Secure VPN client with the PIX or the router behind the NATing device, use the following config on the router (and the corresponding config on the PIX)
NAT in the Middle of an IPSec Tunnel

- **On the router:**
  - Hostname router
  - Ip domain-name me.com
  - Crypto isakmp identity hostname

- **On the Cisco Secure VPN client:**
  - Secure gateway tunnel:
  - Domain name: router.me.com
  - IP address: <routers statically translated IP address>

---

Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting
Common Problems

- Not allowing everything through

Firewall in the Middle

Router

Private

Encrypted

Public

Private

Internet
Firewalling and IPSec

- Things to allow in for IPSec to work through a firewall:
  - **Firewall in the middle of the tunnel:**
    - ESP or/and AH
    - UDP port 500 (ISAKMP)
    - For IPSec through NAT in VPN 3000, open UDP ports configured on concentrator
    - For NAT transparency mode in VPN 5000, open TCP with source port 500 and destination port 80

Firewall on IPSec Endpoint

[Diagram showing a router connected to an internet cloud, with private networks on both sides and an encrypted public network.]
Firewalling and IPSec

- Firewall on the IPSec endpoint router:
  - Esp or/and
  - AH
  - UDP port 500
  - Decrypted packet IP addresses (incoming access group is applied twice)

- Firewall on the IPSec endpoint PIX:
  - Sysopt connection permit-IPSec
  - (Note: No conduits needed)

Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewallsing and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting
Common Problems

- IPSec adds on a further ~60 bytes to each packet; since it does not have logical interface defined for it, it is possible that it receives packets on a physical interface, which after adding on the IPSec header become too large to transmit on that interface unfragmented.

- Do ICMP packet dumps to see if the ICMP type 3 Code 4 packet too large and DF bit set messages are being sent, try with small and large file sizes.

  e.g. **debug ip icmp output on IOS**

  ![Example output](image)

Work Arounnds

- Make sure that there is no MTU black hole device on the network and let normal path MTU discovery work for you.

- If there is some unknown device blocking the ICMP packet too large messages, reduce the MTU on the end machines until the IPSec device does not have to fragment the packet after adding the IPSec header.
Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting

GRE over IPSec

a. Original Packet
b. GRE Encapsulation
c. GRE over IPSec Transport Mode
d. GRE over IPSec Tunnel Mode

<table>
<thead>
<tr>
<th></th>
<th>IP Hdr 1</th>
<th>TCP hdr</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GRE Over IPSec
(Common Configuration Issues)

- Apply crypto map on both the tunnel interfaces and the physical interfaces
- Specify GRE traffic as IPSec interesting traffic.
  
  access-list 101 permit gre host 200.1.1.1 host 150.1.1.1
- Static or dynamic routing is needed to send VPN traffic to the GRE tunnel before it gets encrypted.

GRE over IPSec
(Avoid Recursive Routing)

- To avoid GRE tunnel interface damping due to recursive routing, keep transport and passenger routing info. separate:
  
  Use different routing protocols or separate routing protocol identifiers
  
  Keep tunnel IP address and actual IP network addresses ranges distinct
  
  For tunnel interface IP address, don’t use unnumbered to loopback interface when the loopback’s IP address resides in the ISP address space
GRE over IPsec (MTU Issues)

- Overhead calculation of GRE over IPsec (assume ESP-DES & ESP-MD5-HMAC):
  - ESP overhead (with authentication): 31 ~ 38 bytes
  - GRE header: 24 bytes
  - IP header: 20 bytes
- GRE over IPsec with tunnel mode introduces ~75 bytes overhead, GRE over IPsec with transport mode introduces ~55 bytes overhead

GRE over IPsec (MTU Issues)

- After GRE tunnel encapsulation, the packets will be sent to physical interface with DF bit set to 0
- The GRE packets will then be encrypted at physical interface; if IPsec overhead causes final IPsec packets to be bigger than the interface MTU, the router will fragment the packets
- The remote router will need to reassemble the fragmented IPsec packets (process switched) which causes performance degradation
GRE over IPSec (MTU issue)

- To avoid fragmentation and reassembly of IPSec packets:
  - Set `ip mtu 1420` (GRE/IPSec tunnel mode), `ip mtu 1440` (GRE/IPSec transport mode) under tunnel interface.
  - Enable “tunnel path-mtu-discovery” (DF bit copied after GRE encapsulation) under tunnel interface.
- Use “show ip int switching” to verify switching path.

GRE over IPSec with NAT in Middle

**Standard Configuration Won't Work:**

R1:
- GRE: `tunnel_src 10.1.1.1` `tunnel_dest 200.1.1.3`
- IPSec: `peer 200.1.1.3`
  `gre host 10.1.1.1 host 200.1.1.3`

R2:
- GRE: `tunnel_src 200.1.1.3` `tunnel_dest 200.1.1.1`
- IPSec: `peer 200.1.1.1`
  `gre host 200.1.1.3 host 200.1.1.1`

`IPSEC(validate_transform_proposal):proxy identities not supported`
GRE over IPSec with NAT in Middle

**R1:**
- **GRE:**
  - `tunnel_src 10.1.1.1`
  - `tunnel_dest 200.1.1.3`
- **IPsec (tunnel mode):**
  - `peer 200.1.1.3`
  - `gre host 10.1.1.1 host 200.1.1.3`

**R2:**
- **GRE:**
  - `tunnel_src 200.1.1.3`
  - `tunnel_dest 10.1.1.1`
- **IPSec (tunnel mode):**
  - `Peer 200.1.1.1`
  - `gre host 200.1.1.3 host 10.1.1.1`

**GRE over IPSec with NAT in Middle**

```
hostname R1
crypto isakmp policy 10
    hash md5
    authentication pre-share
crypto isakmp key cisco123 address 200.1.1.3
crypto ipsec transform-set test esp-des esp-md5-hmac
    mode transport
    !
crypto map mymap local-addr e1
gre host 20.1.1.1 host 200.1.1.3

interface Tunnel0
    ip address 172.16.1.1 255.255.255.252
tunnel source Ethernet0
tunnel destination 200.1.1.3
crypto map test
    !
interface Ethernet0
    ip address 20.1.1.1 255.255.255.0
    !
interface Ethernet1
    ip address 10.1.1.1 255.255.255.0
crypto map test
```
GRE over IPSec with NAT in Middle

hostname R2

crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
crypto ipsec transform-set test esp-des esp-md5-hmac
mode transport
crypto map test 10 ipsec-isakmp
set peer 200.1.1.1
set transform-set test
match address 101

access list 101 permit gre host 200.1.1.3 host 20.1.1.1

interface Tunnel0
ip address 172.16.1.2 255.255.255.252
tunnel source Ethernet4/1
tunnel destination 20.1.1.1
crypto map test

! interface Ethernet4/1
ip address 200.1.1.3 255.255.255.0
duplex half
crypto map test

Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting
Loss of Connectivity of IPSec Peers

- Use ISAKMP keepalives to detect loss of connectivity of IOS IPSec peers
  
crypto isakmp keepalive <# of sec. between keepalive> 
  <number of sec. between retries if keepalive fails>

- ISAKMP keepalives might cause performance degradation for large deployments, choose keepalive parameters carefully
Agenda

- Router IPSec VPNs
- PIX IPSec VPNs
- Cisco VPN 3000 IPSec VPNs
- Cisco VPN 5000 IPSec VPNs
- CA Server Issues
- NAT with IPSec
- Firewalling and IPSec
- MTU Issues
- GRE over IPSec
- Loss of Connectivity of IPSec Peers
- Interoperability Troubleshooting

Interoperability Tips

- **Keep things simple** like mode config and xauth; use preshare; work your way up the feature list

- **Start from one host** behind Cisco to one host behind the other device

- **Try to establish the connection from both sides**; there might be issues starting it in a particular direction

- **Configure the two ends side by side**
Interoperability Tips

- Make sure life time entries are matching both ends
- Try transport mode if tunnel mode does not work
- Remember that Cisco does not initiate aggressive mode but does accept it

Troubleshooting the Implementation of IPSec VPNs
Session SEC-310
Please Complete Your Evaluation Form
Session SEC-310