



Virtual Private Network (VPN) Defined

A Virtual Private Network Carries Private Traffic Over a Public Network

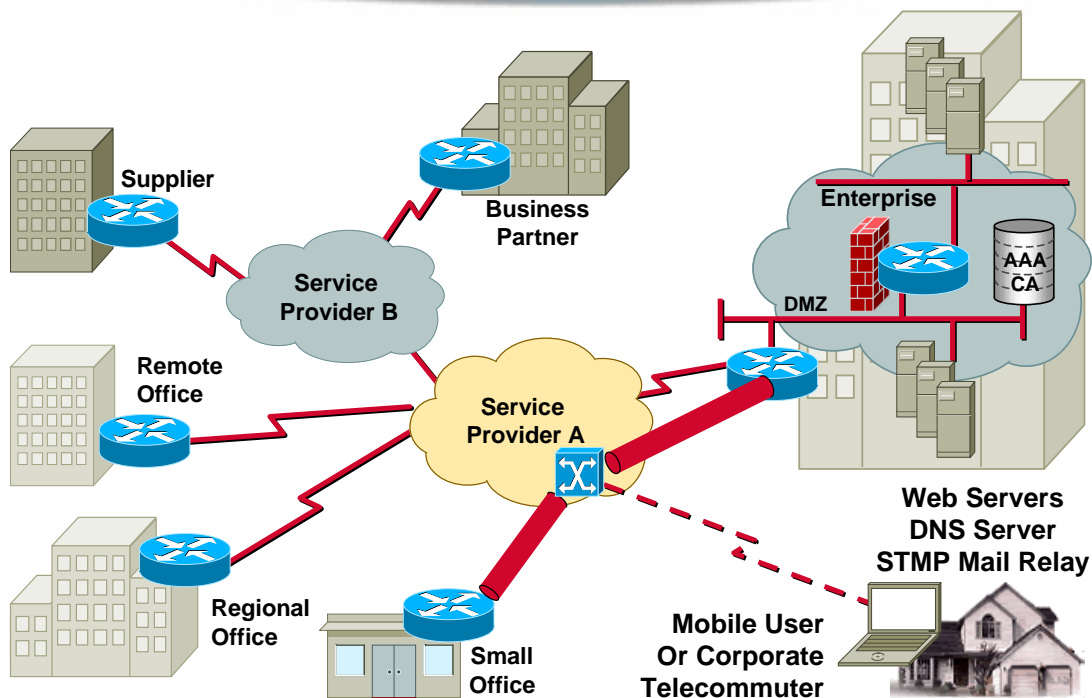
2405
1352_06_2000_c2

© 2000, Cisco Systems, Inc.

cisco.com

3

The Complete VPN



2405
1352_06_2000_c2

© 2000, Cisco Systems, Inc.

cisco.com

4

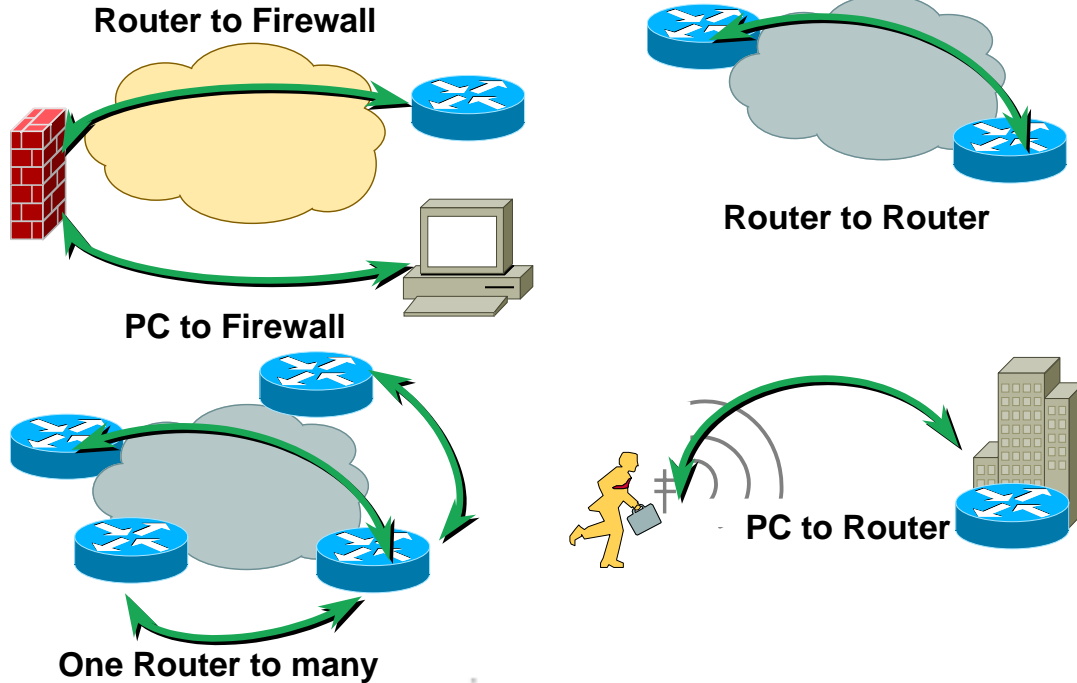
What Is IPSec?

- **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**

Design Scenarios



2405
1352_06_2000_c2

© 2000, Cisco Systems, Inc.

cisco.com

7

Agenda

- **Router VPNs**
- **PIX VPNs**
- **CA server problems**
- **NAT with IPSec**
- **Firewalling and IPSec**
- **MTU issues**
- **Interoperability troubleshooting**

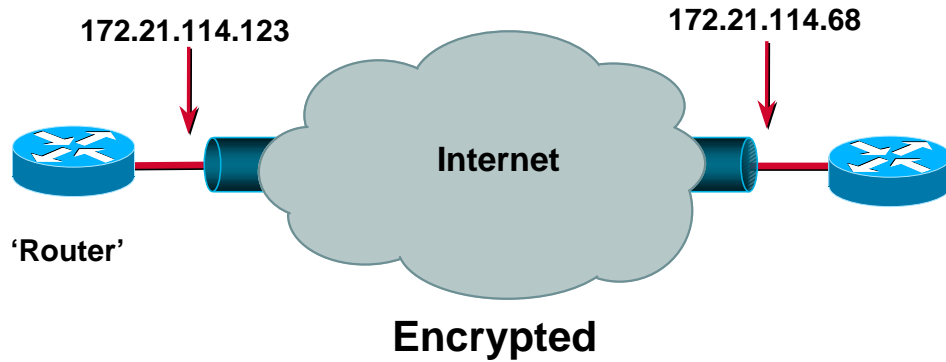
2405
1352_06_2000_c2

© 2000, Cisco Systems, Inc.

cisco.com

8

Layout



Normal Router Configurations

```
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
```

Normal Router Configurations

```
Router#sh cry IPsec transform
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, }
```

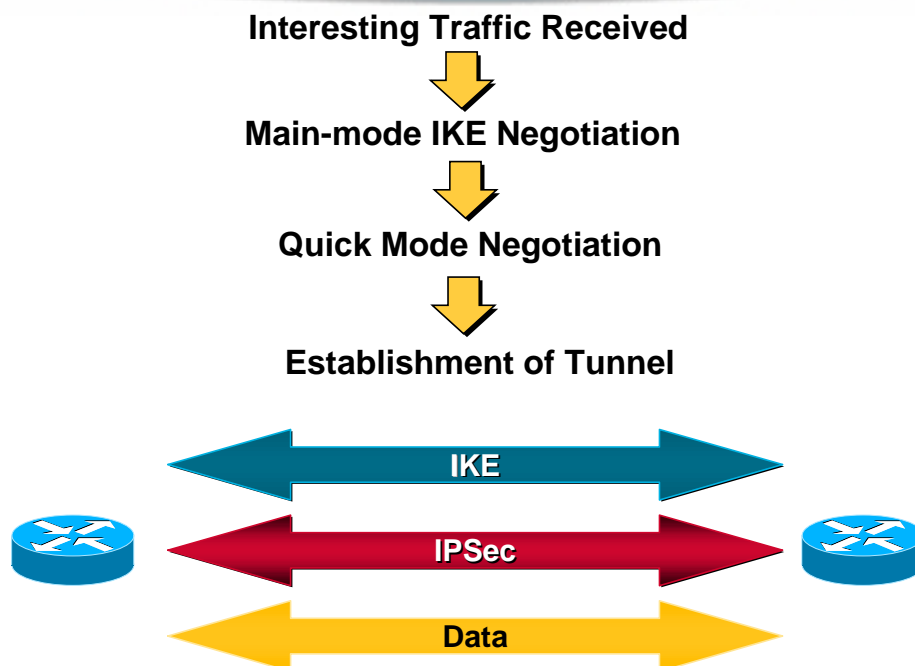
The Two Main Debugs

- **debug crypto isakmp**
- **debug crypto IPSec**

Other Useful Debugs

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

Debugs 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 configed 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

Interesting Traffic Received
Main-Mode IKE



- 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

ISAKMP Main-Mode Negotiation

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

Interesting Traffic Received

↓
Main-Mode IKE

↓
Quick Mode



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.

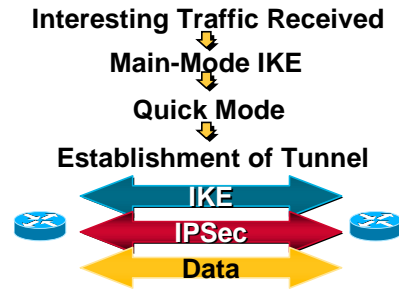
```
ISAKMP (1): atts are acceptable.
```

- The IPsec SA has now been successfully negotiated. ISAKMP will now go into a state known as QM-IDLE.

IPSec SA Establishment

```
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 ISAKMP has asked the IPsec routine to validate the IPsec proposal that it has negotiated with the remote side



IPSec SA Establishment

```
05:59:55: ISAKMP (1): Creating IPsec SAs
05:59:55: inbound SA from 172.21.114.68 to
172.21.114.123
(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

```
05:59:55:      outbound SA from 172.21.114.123  to
172.21.114.68
```

```
(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.**

IPSec SA Establishment

```
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

Show Commands

```
Router#sh cry engine connection active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	no idb	no address	set	DES_56_CBC	0	0

- This is the ISAKMP SA

2	Ethernet0	172.21.114.123	set	HMAC_MD5+DES_56_CB	0	5
---	-----------	----------------	-----	--------------------	---	---

3	Ethernet0	172.21.114.123	set	HMAC_MD5+DES_56_CB	5	0
---	-----------	----------------	-----	--------------------	---	---

- These two are the IPsec SAs

```
Router#sh crypto isakmp sa
```

dst	src	state	conn-id	slot
172.21.114.68	172.21.114.123	QM_IDLE	1	0

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
```

Show Commands

```
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:`

Common Problems

- **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

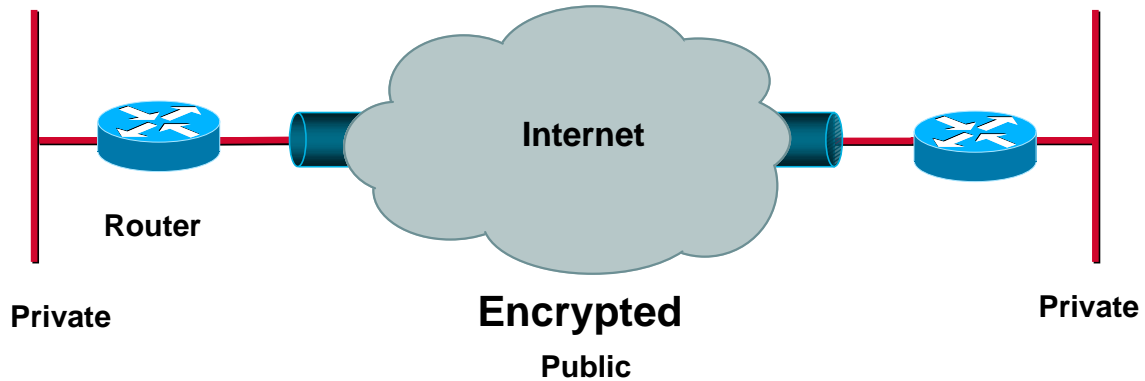
- If no ISAKMP policies configured match, or if no preshared key for the negotiating peer is configured, the router tries the default policy, 65535, and if that too does not match it fails ISAKMP negotiation
- A **sh crypto isakmp sa** shows the ISAKMP SA to be in **MM_NO_STATE**, meaning the main-mode failed

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.

Incompatible ISAKMP Policy or Preshared Secrets

%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer at 155.0.0.1



Incompatible ISAKMP Policy or Preshared Secrets

ISAKMP (17): processing SA payload. Message ID = 0

ISAKMP (17): Checking ISAKMP transform 1 against priority 10 policy
encryption DES-CBC
hash SHA
default group 1
auth pre-share

ISAKMP (17): Checking ISAKMP transform 1 against priority 65535 policy
encryption DES-CBC
hash SHA
default group 1
auth pre-share

ISAKMP (17): atts are not acceptable. Next payload is 0

ISAKMP (17); no offers accepted!

ISAKMP (17): SA not acceptable!

%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer at 155.0.0.1

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

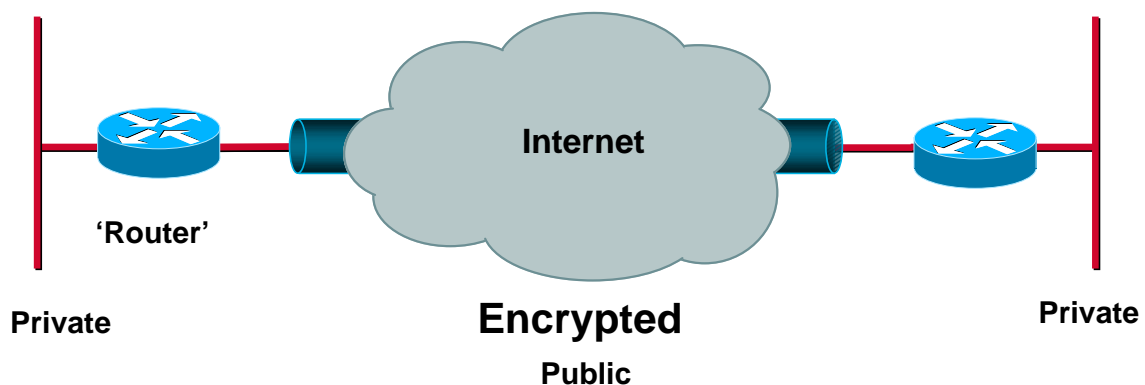
```
ISAKMP (62): processing SA payload. message ID = 0
ISAKMP (62): Checking ISAKMP transform 1 against priority 10 policy
                encryption DES-CBC
                hash SHA
                default group 1
                auth pre-share
ISAKMP (62): atts are acceptable. Next payload is 0
ISAKMP (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_transform_proposal): proxy identities not supported



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,

spi= 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

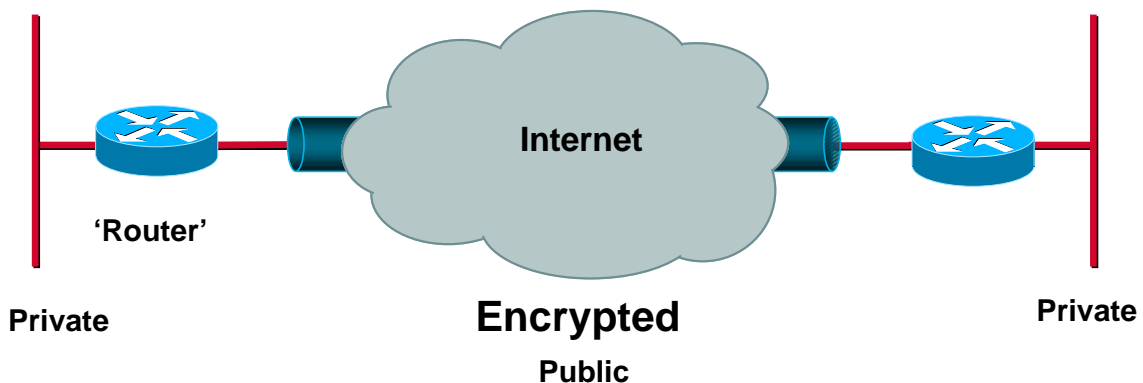
- The crypto map needs to be applied to the outgoing interface of the router. If you don't want to use the outside interface's IP as the local ID, use the command '**crypto map <name> local address <interface>**', to specify the correct interface
- If there are physical as well as logical interfaces 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



Incorrect SA Selection by the Router

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
```

A ccess list for 5.6.7.8:

```
A ccess-list 100 perm it ip host 1.2.3.5 host 5.6.7.9
```

```
A ccess-list 100 perm it ip host 1.2.3.5 host 2.3.4.5
```

A ccess list for 1.2.3.4:

```
A ccess-list 110 perm it 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!)

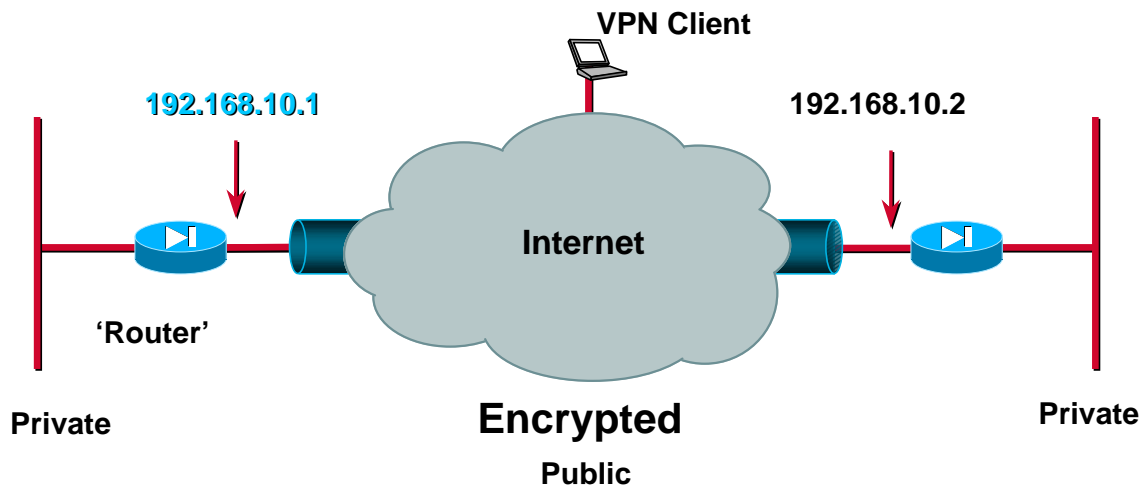
Caveats: Switching Paths

- 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 etc.) in case you are running into an **obscure** problem

Agenda

- Router VPNs
- **PIX VPNs**
- CA server problems
- NAT with IPsec
- Firewalling and IPsec
- MTU issues
- Interoperability troubleshooting

Layout



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 Problems

- 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 VPNs
- PIX VPNs
- **CA server problems**
- NAT with IPSec
- Firewalling and IPSec
- MTU issues
- 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**

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://ciscob0tpppy88:80/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 VPNs
- PIX VPNs
- CA server problems
- **NAT with IPSec**
- Firewalling and IPSec
- MTU issues
- Interoperability troubleshooting

Common Problems

- Bypassing static NAT entries
- NAT in the middle of an IPSec tunnel
- NAT and embedded IP addresses

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 Altiga or IPsec in HTTP with Compatible for Problem 1
- **Problem 2:** IPsec end point device behind a static Nat translating device 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 VPN client or router to 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 VPN client:

```
Secure gateway tunnel:  
Domain name: router.me.com  
IP address: <routers statically translated IP address>
```

NAT and Embedded IP Addresses

- **Keep in mind that IPSec encrypts all embedded addresses. So even if the NATing device is intelligent enough to **fix** these addresses during a translation, it won't be able to do so for an encrypted packet**
- **Example of such a situation is GRE in IPSec**

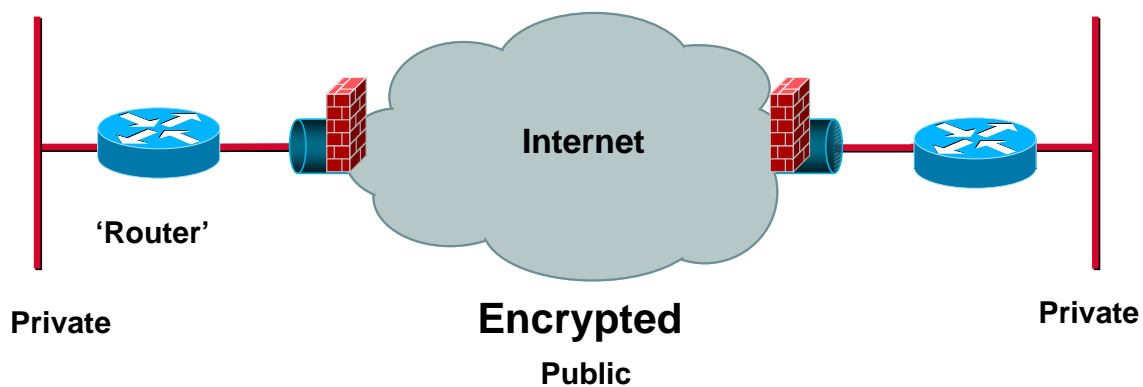
Agenda

- Router VPNs
- PIX VPNs
- CA server problems
- NAT with IPSec
- **Firewalling and IPSec**
- MTU issues
- Interoperability troubleshooting

Common Problems

- Not allowing everything through

Firewall in the Middle



Firewalling and IPSec

- Things to allow in for IPSec to work through a firewall:

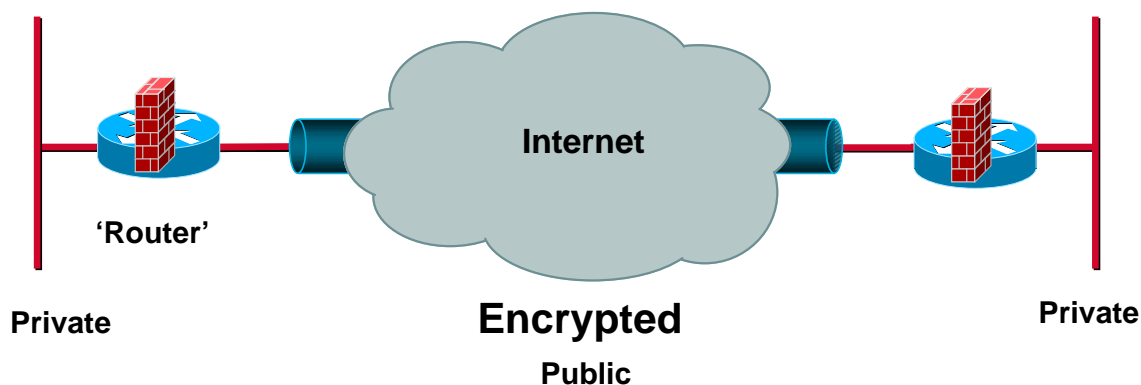
- **Firewall in the middle of the tunnel:**

Esp or/and

AH

UDP port 500

Firewall on IPSec Endpoint



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 VPNs
- PIX VPNs
- CA server problems
- NAT with IPSec
- Firewalling and IPSec
- **MTU issues**
- 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**

Work Arounds

- **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 VPNs
- PIX VPNs
- CA server problems
- NAT with IPSec
- Firewalling and IPSec
- MTU issues
- **Interoperability troubleshooting**

Inter Operability Tips

- **Keep things simple.**
like mode config and xauth. Use preshared. 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**

Inter Operability 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 IPSec Design and Implementation

Session 2405



Please Complete Your Evaluation Form

Session 2405

2405
1352_06_2000_c2

© 2000, Cisco Systems, Inc.

cisco.com

93

CISCO SYSTEMS



EMPOWERING THE INTERNET GENERATIONSM

2405
1352_06_2000_c2

© 2000, Cisco Systems, Inc.

cisco.com

94