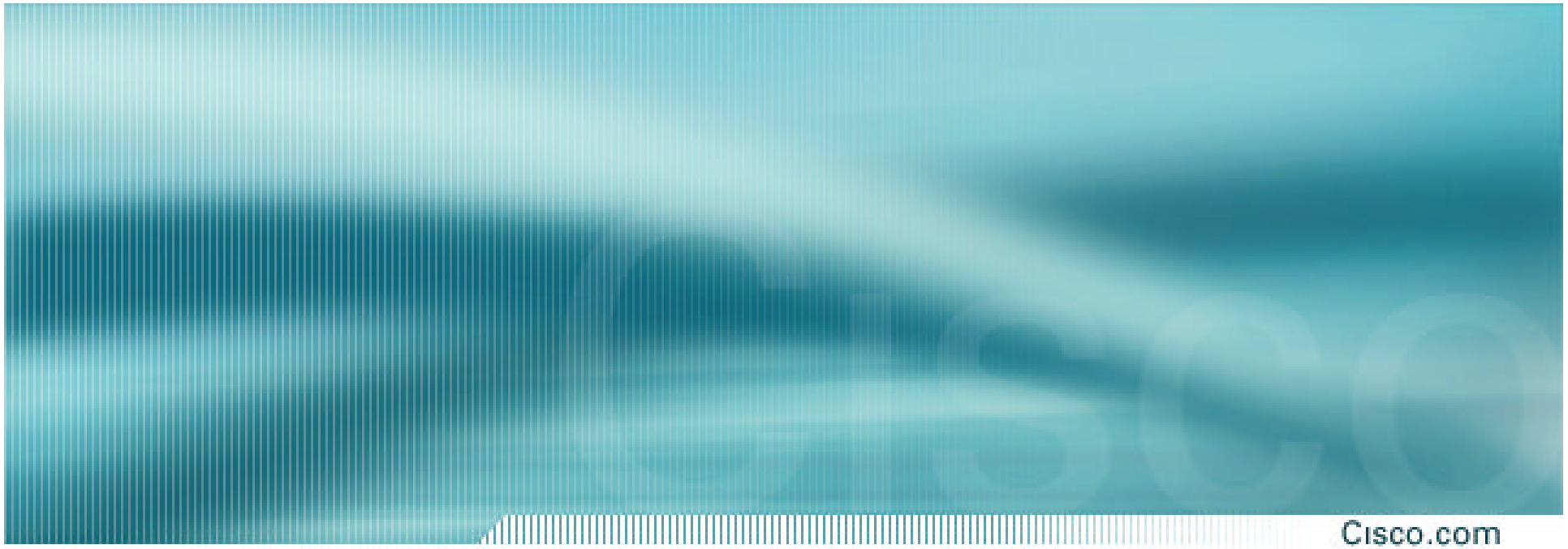

Cisco Systems



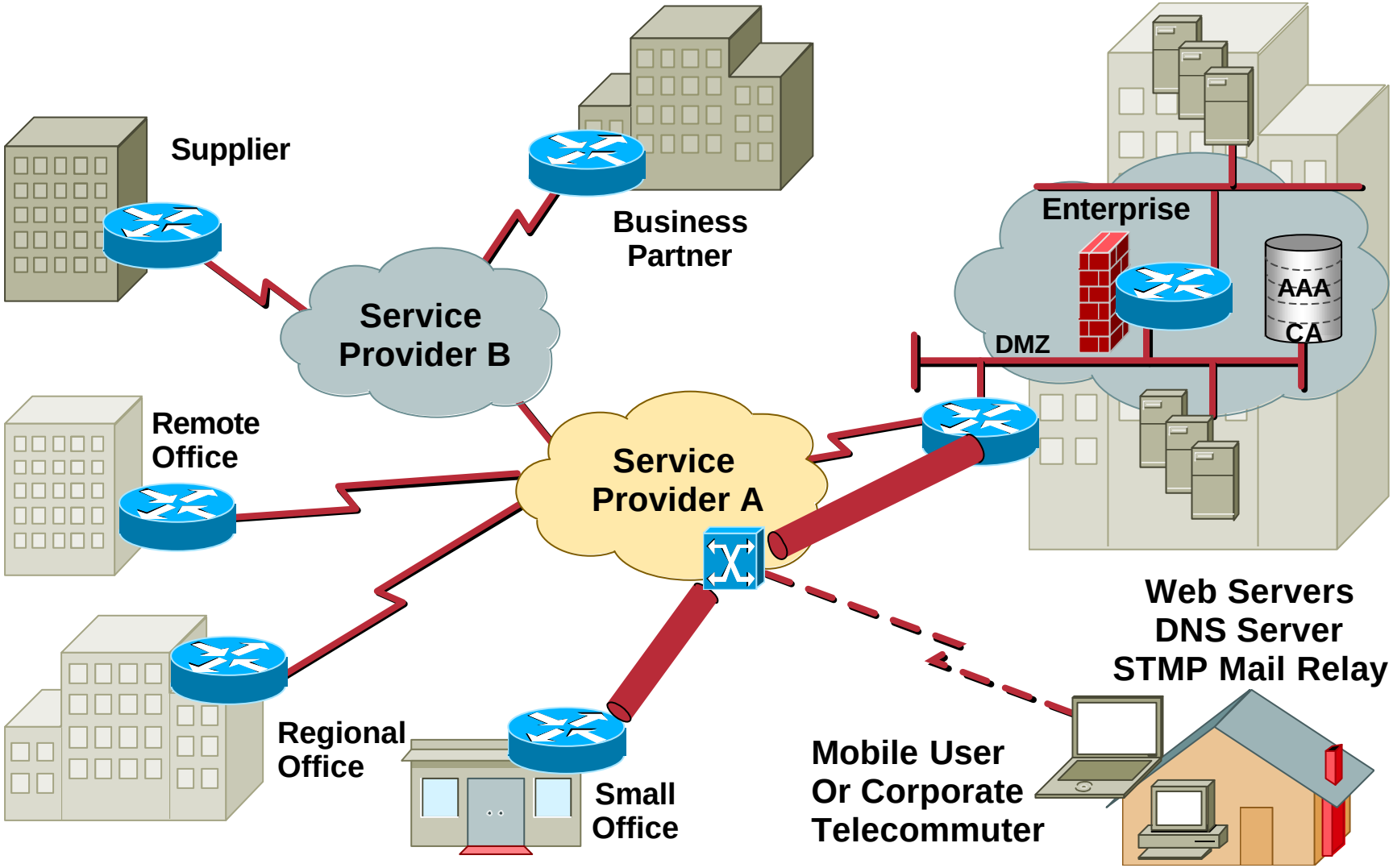
Troubleshooting the Implementation of IPSec VPNs

Session SEC-310

Virtual Private Network (VPN) Defined

"A Virtual Private Network carries private traffic over public network."

The Complete VPN



What Is IPSec?

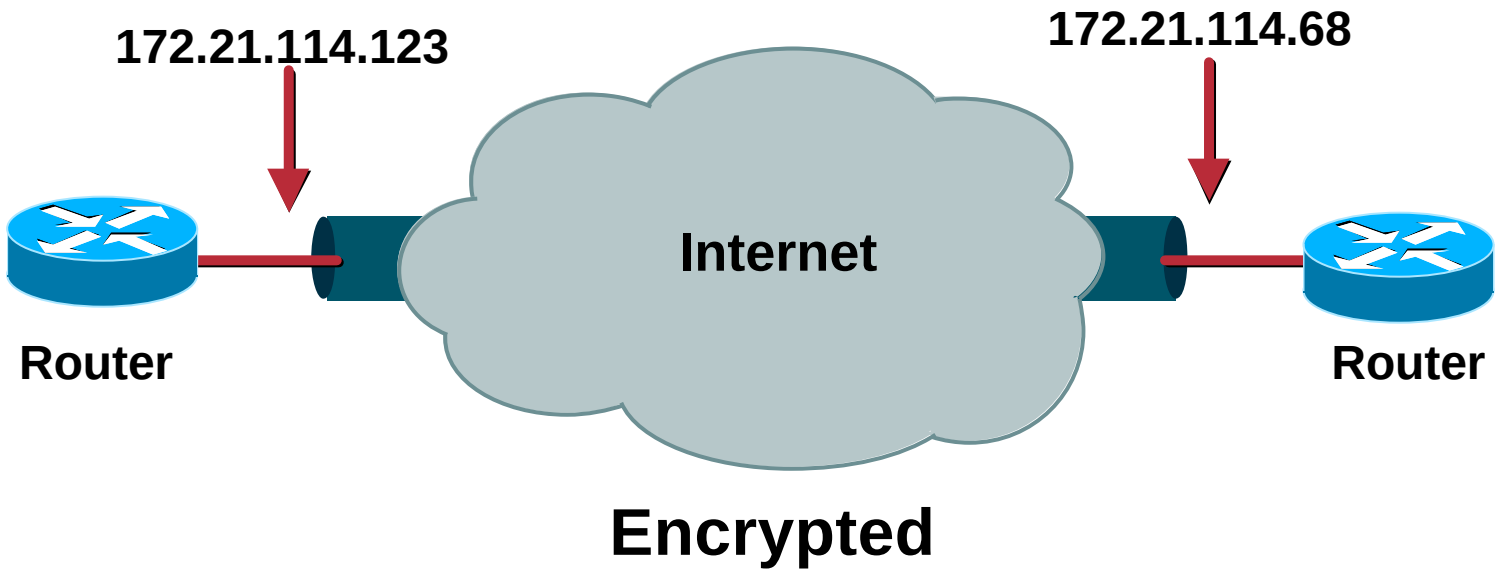
- IPSec stands for IP Security
- Standard for privacy, integrity and authenticity for networked commerce
- Implemented transparently in the network infrastructure
- End-to-end security solution including routers, firewalls, PCs, and servers

Agenda

Cisco.com

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

Layout



Normal Router Configurations

Cisco.com

```
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

Cisco.com

```
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

Cisco.com

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

Normal Router Configurations

Cisco.com

```
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

Interesting Traffic Received

↓

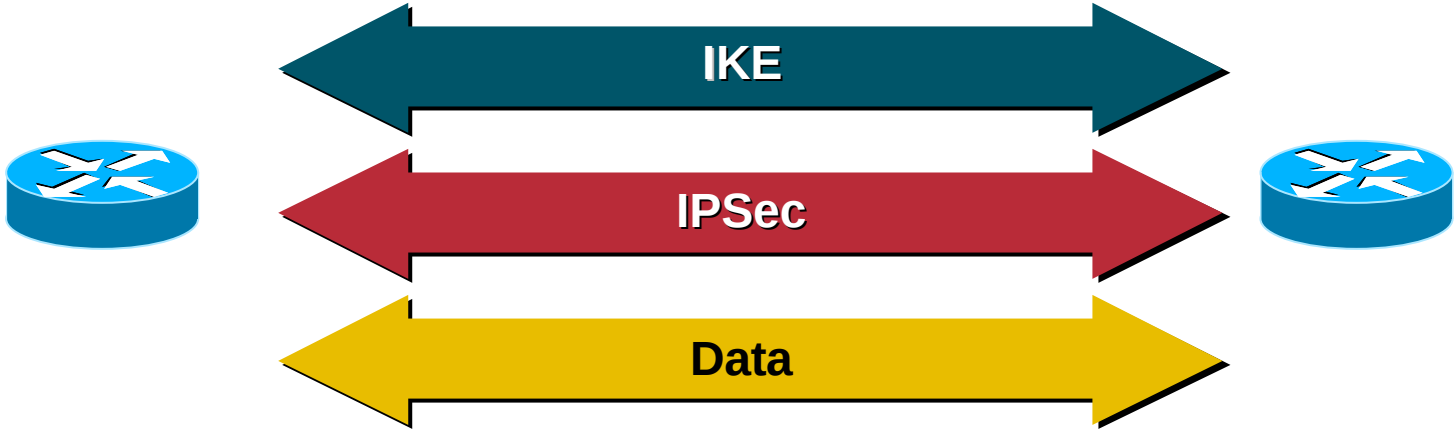
Main Mode IKE Negotiation

↓

Quick Mode Negotiation

↓

Establishment of Tunnel



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 liftimes

```
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

Interesting Traffic Received

Main-Mode IKE

```
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 (apart from 65535)

```
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

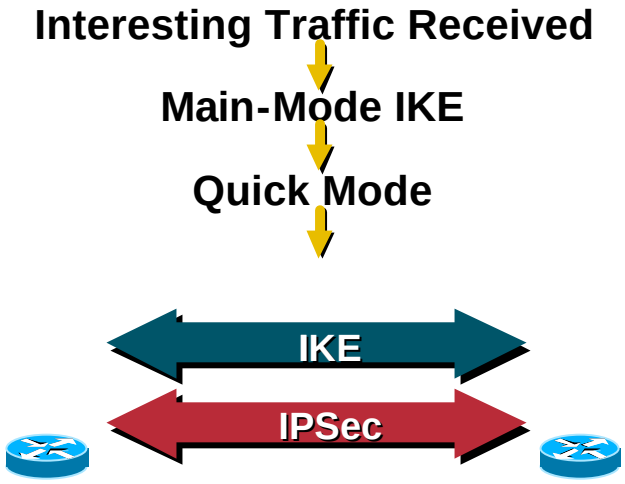

```
05:59:53: ISAKMP (1): processing KE payload. message ID = 0
05:59:55: ISAKMP (1): processing NONCE payload. message ID =0
```

- 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, state is QM_IDLE, or IKE_P1_COMPLETE.
- ISADB entry added.

ISAKMP Quick Mode



- Quick mode is started. 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 600837116ld 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 it s 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

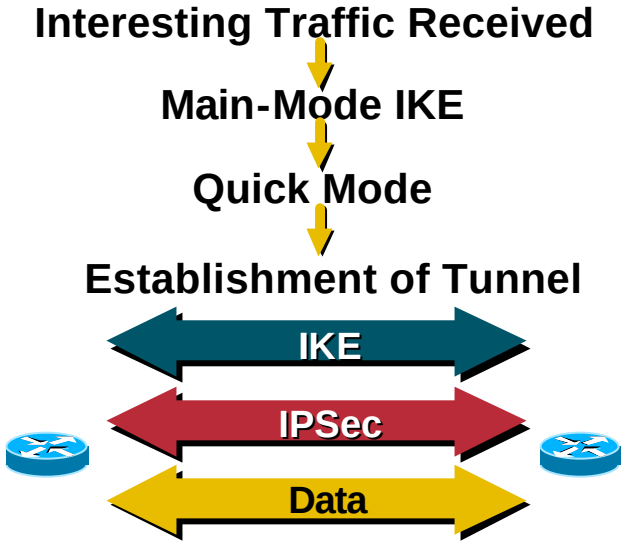

```
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of
0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
```

- This is the payload authentication hash offered by the remote end in accordance with it's transform set

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

- The IPSec SA has now been successfully negotiated.

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

IPSec SA Establishment

Cisco.com

```
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 initialised.
- The tunnel is now fully functional

Show Commands

Cisco.com

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

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

Cisco.com

```
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:
```

Show Commands

Cisco.com

```
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

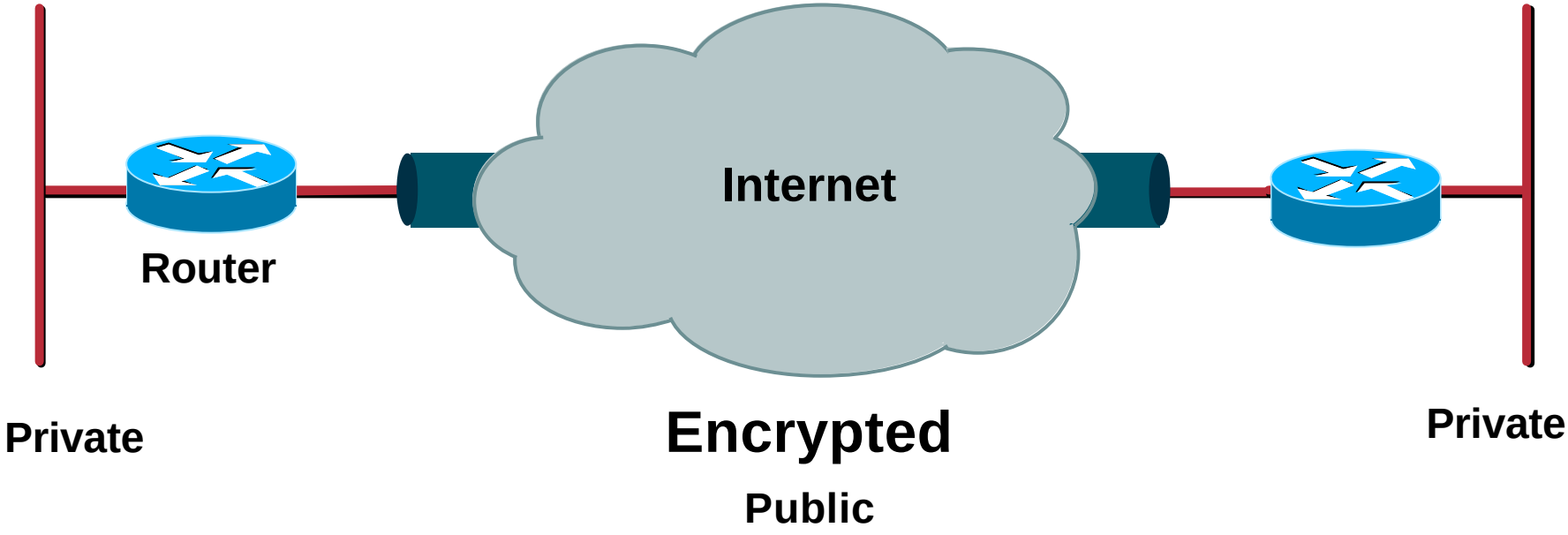
- Incompatible ISAKMP policy or preshared secrets
- Incompatible or incorrect access lists
- Crypto map on the wrong interface
- Routing issues

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

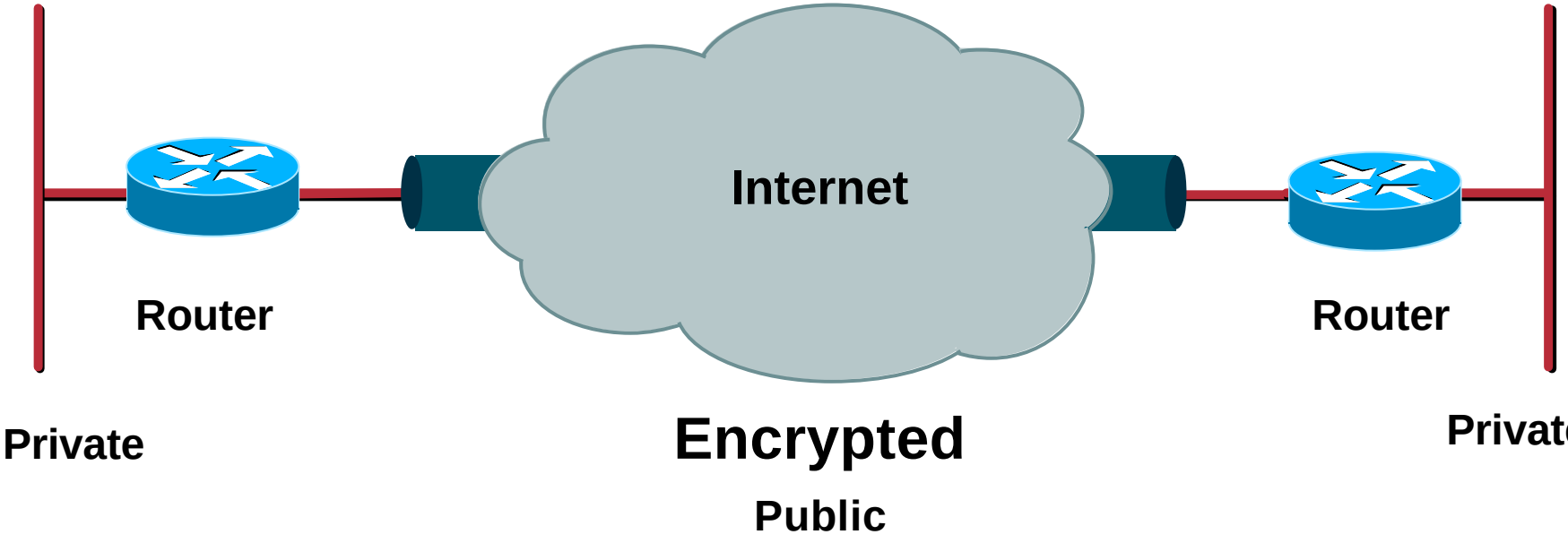

```
ISAKMP (62): processing SA payload. message ID = 0
ISAKMP (62): Checking ISAKMP transform 1 against priority 10 policy
              encryption DES-CBC
              hash SHA
              default group 1
              auth pre-share
ISAKMP (62): atts are acceptable. Next payload is 0
ISAKMP (62): 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 keyword 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

Routing Issues

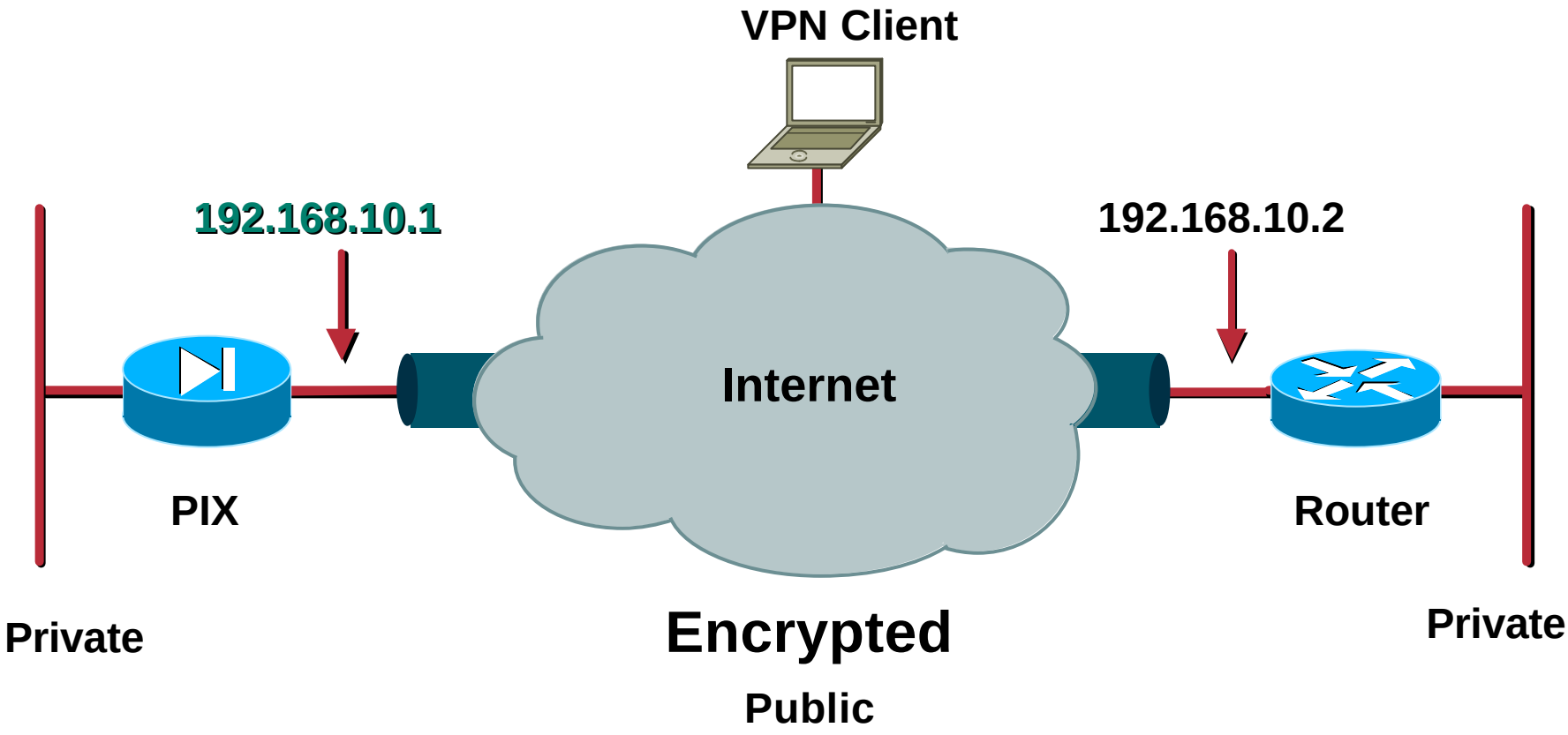
- A packet needs to be routed to the interface which has the crypto map configured on it before IPSec will kick in
- Routes need to be there not only for the router to reach its peers address but also for the IP subnets in the packets once they have been decrypted
- Use the debug ip packet <acl> detailed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

Agenda

Cisco.com

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

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

Cisco.com

```
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

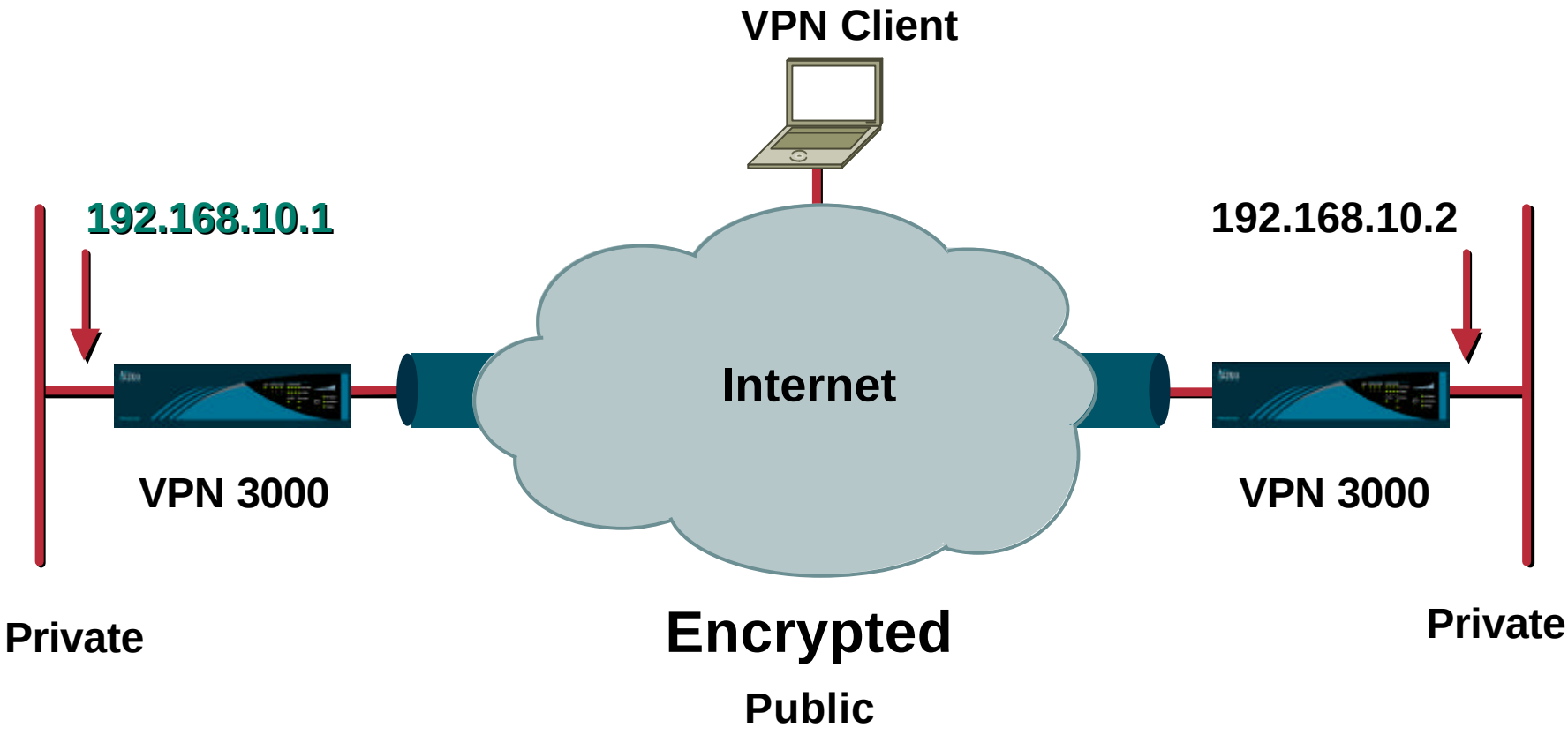
- If you are doing mode config or x-auth for the VPN clients you would need to disable that for the PIX to PIX connection
- Use the no mode-config and no x-auth tags at the end of the preshared key definitions to disable mode config and x-auth

Agenda

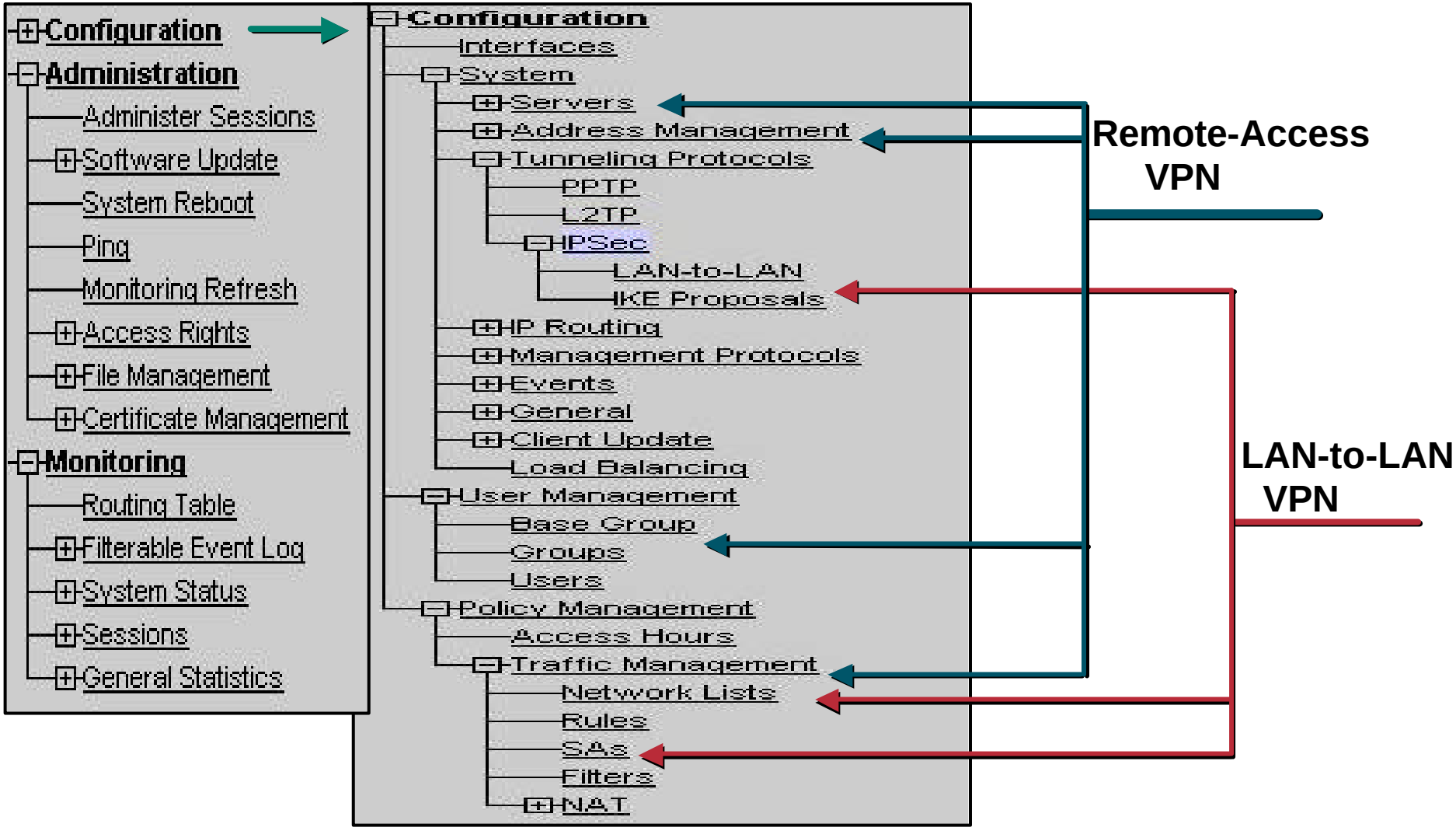
Cisco.com

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

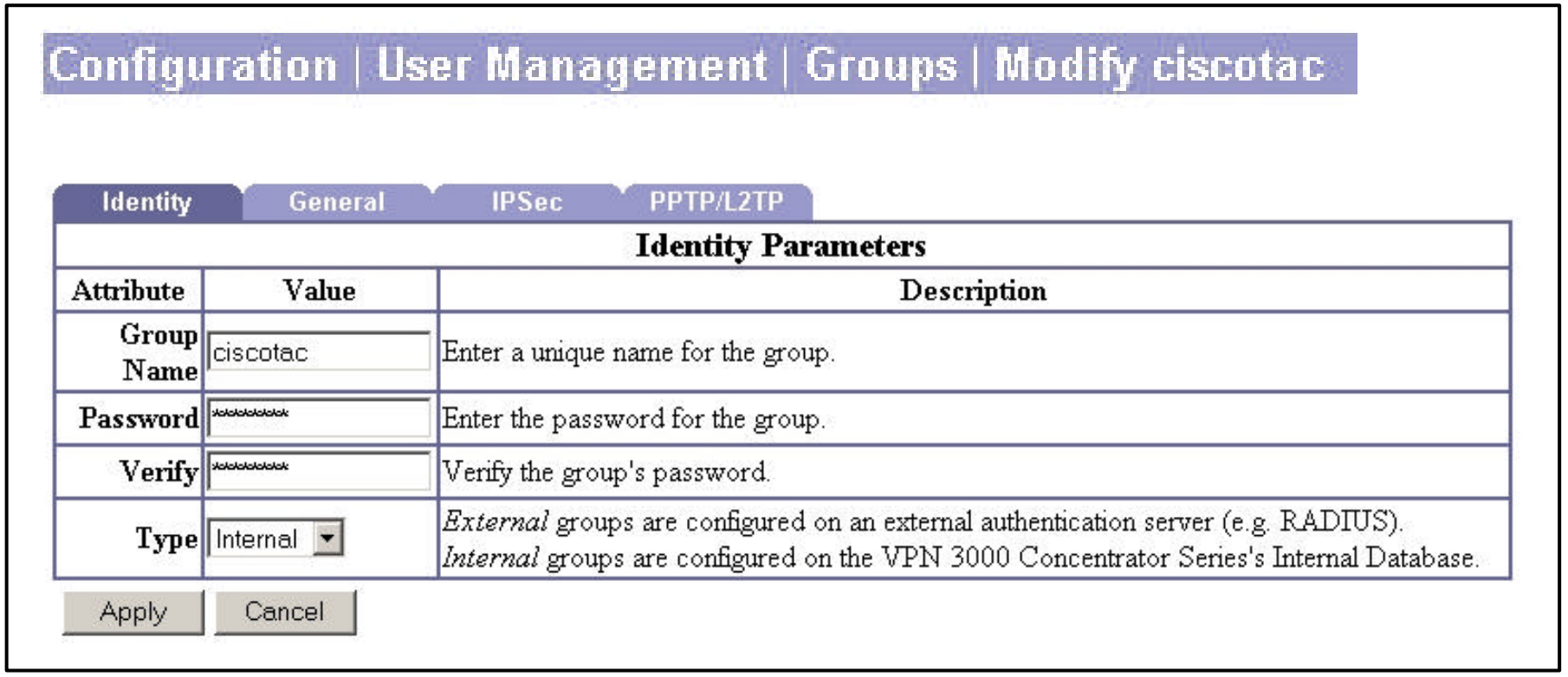
Layout



Cisco VPN 3000 WebGUI Panel



Cisco VPN 3000 Standard Configuration (Remote Access IPSec VPN)



Cisco VPN 3000 Standard Configuration (Remote Access IPSec VPN)

Identity | General | IPSec | PPTP/L2TP

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	MyGroupFilter	☐	Enter the filter assigned to this group.
Primary DNS	10.1.1.1	☐	Enter the IP address of the primary DNS server.
Secondary DNS	10.1.1.5	☐	Enter the IP address of the secondary DNS server.
Primary WINS	10.1.1.10	☐	Enter the IP address of the primary WINS server.
Secondary WINS	10.1.1.15	☐	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	☐	Select the tunneling protocols this group can connect with.
Strip Realm	☐	☑	Check to remove the realm qualifier of the user name during authentication.

Apply | Cancel

Cisco VPN 3000 Standard Configuration (Remote Access IPSec VPN)

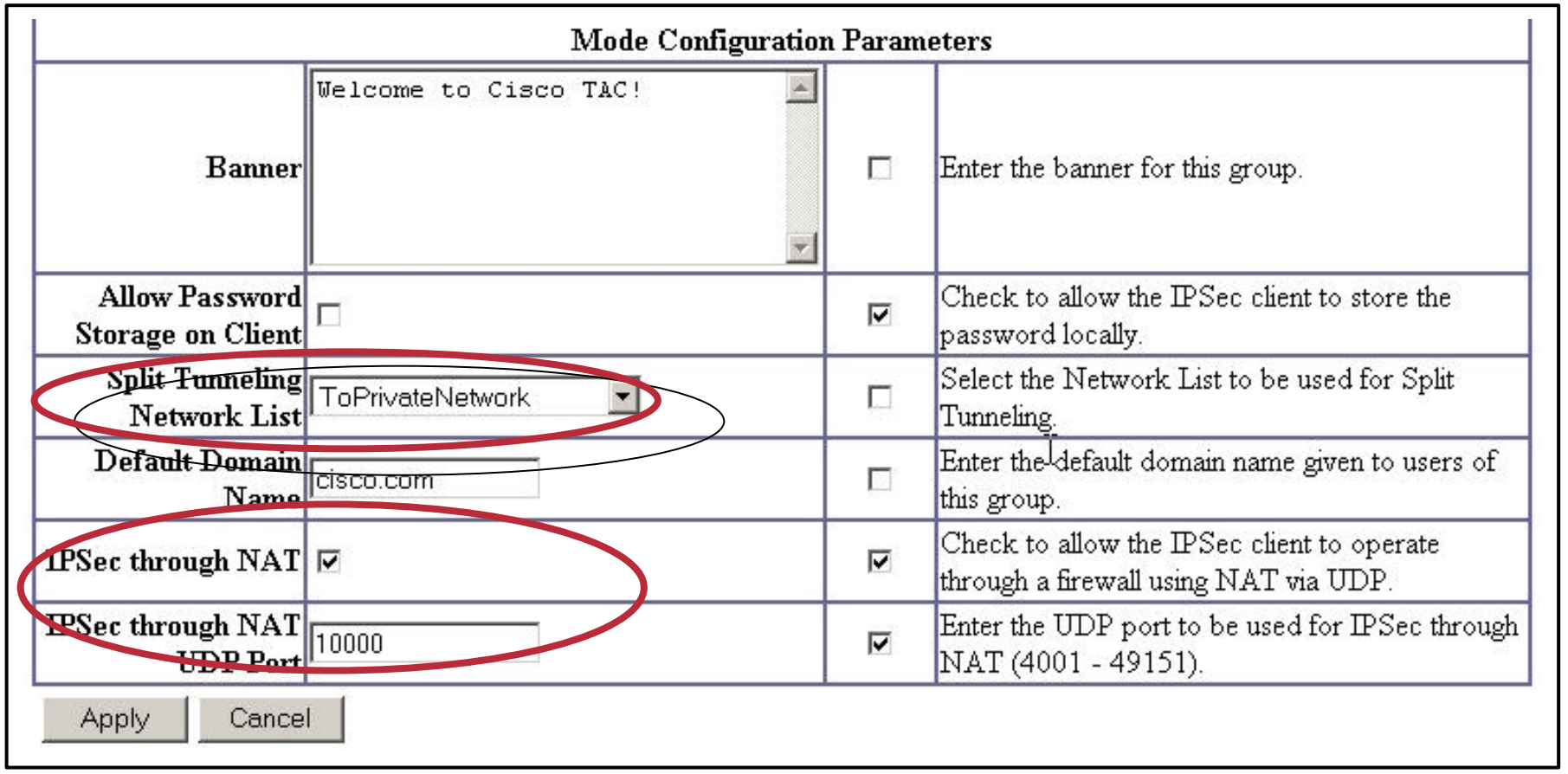
Identity | General | IPSec | PPTP/L2TP

IPSec Parameters

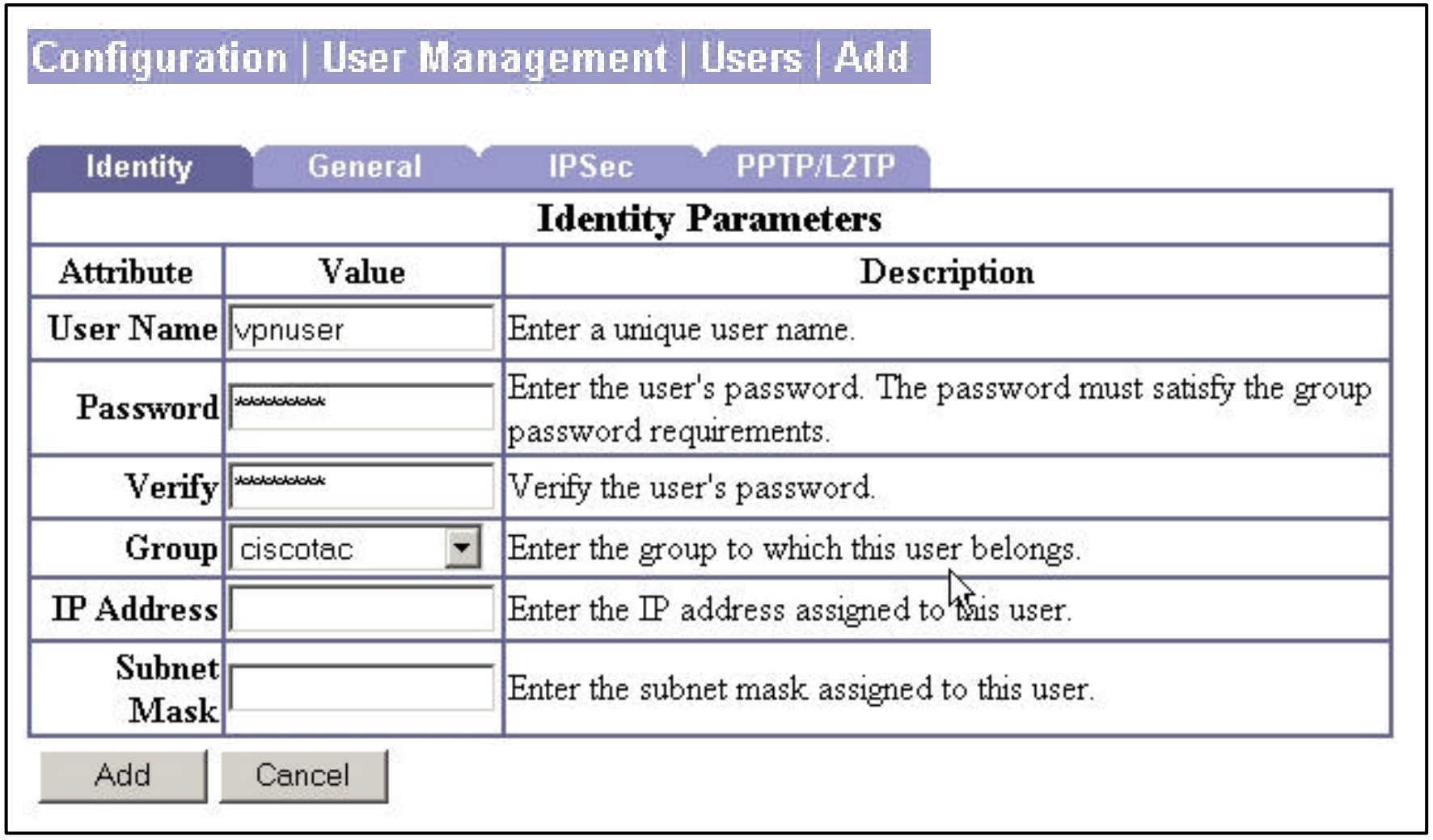
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for users of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed
Remote Access Parameters			
Group Lock	☐	☑	Lock users into this group.
Authentication	Internal	☑	for users in this
IPComp	None	☑	Select the method of IP Compression for members of this group.
Mode Configuration	☑	☑	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Altiga/Cisco client are being used by members of this group.

Internal, RADIUS, NT, SDI

Cisco VPN 3000 Standard Configuration (Remote Access IPSec VPN)

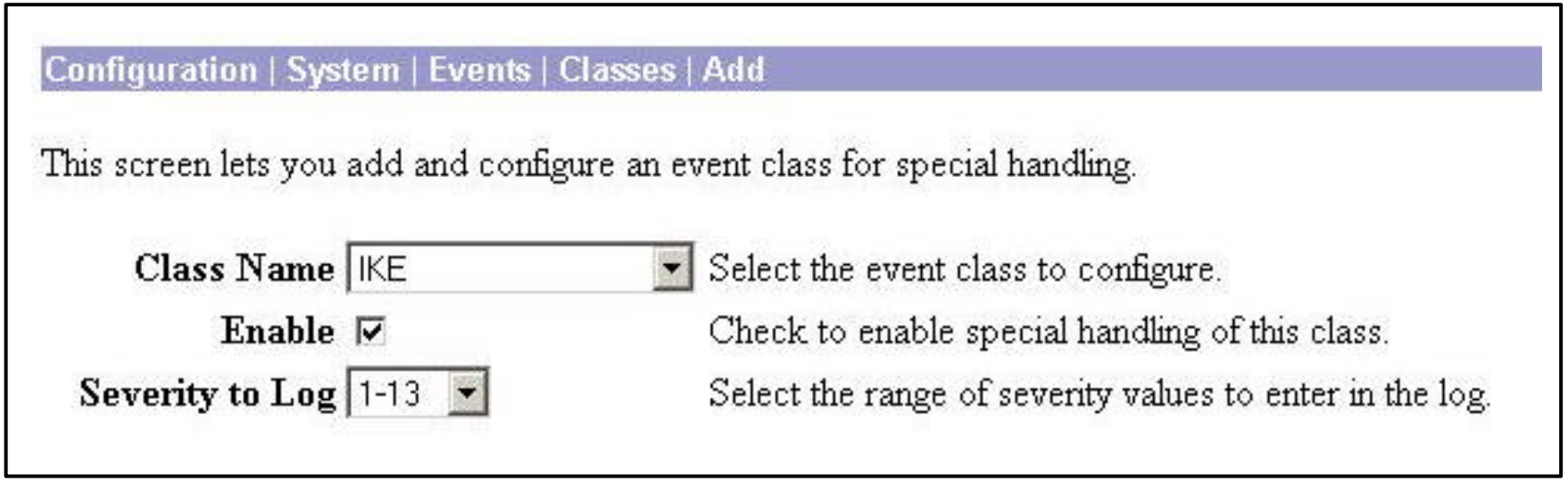


Cisco VPN 3000 Standard Configuration (Remote Access IPSec VPN)



Cisco VPN 3000
Debug Tool (Event Log)

Configure Event Log on VPN 3000 Concentrator:



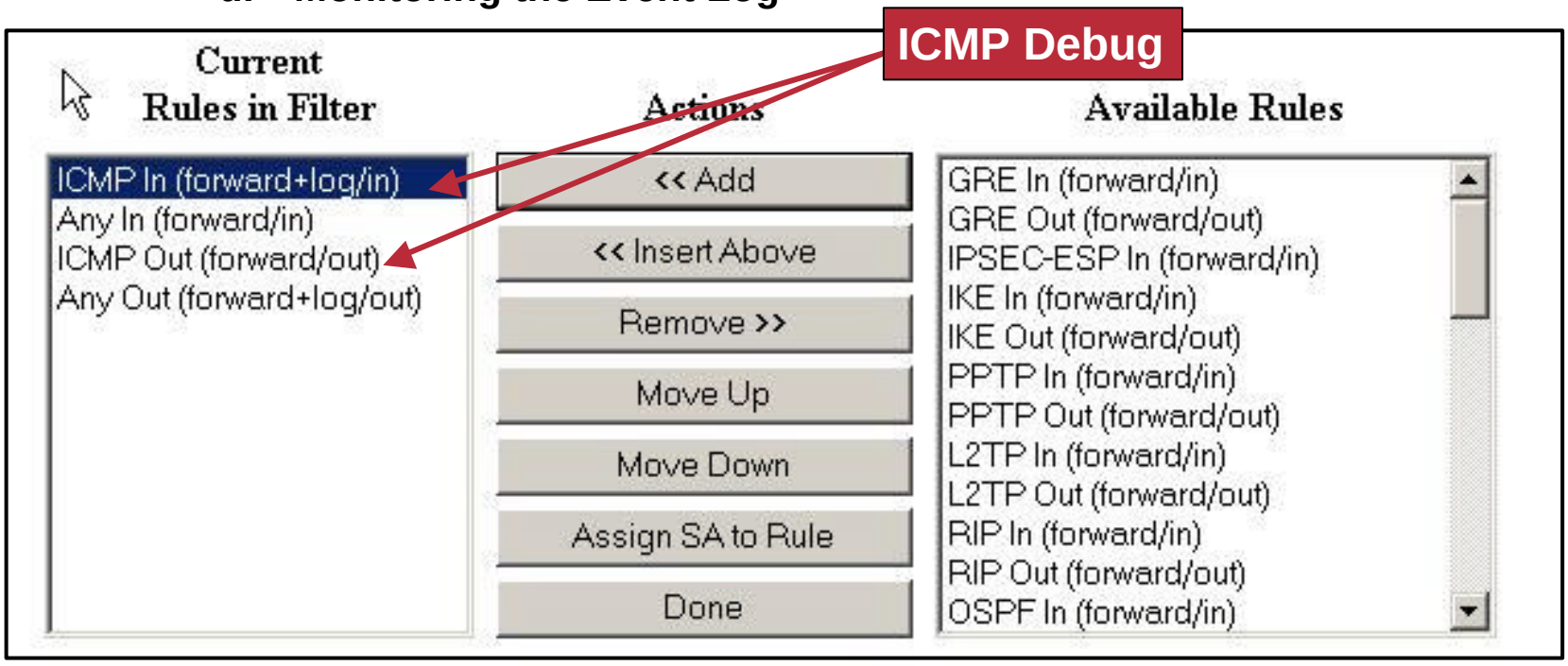
Most commonly used classes for IPSec VPN:

IKE IKEDBG IPSEC IPSECDBG AUTH AUTHDBG

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

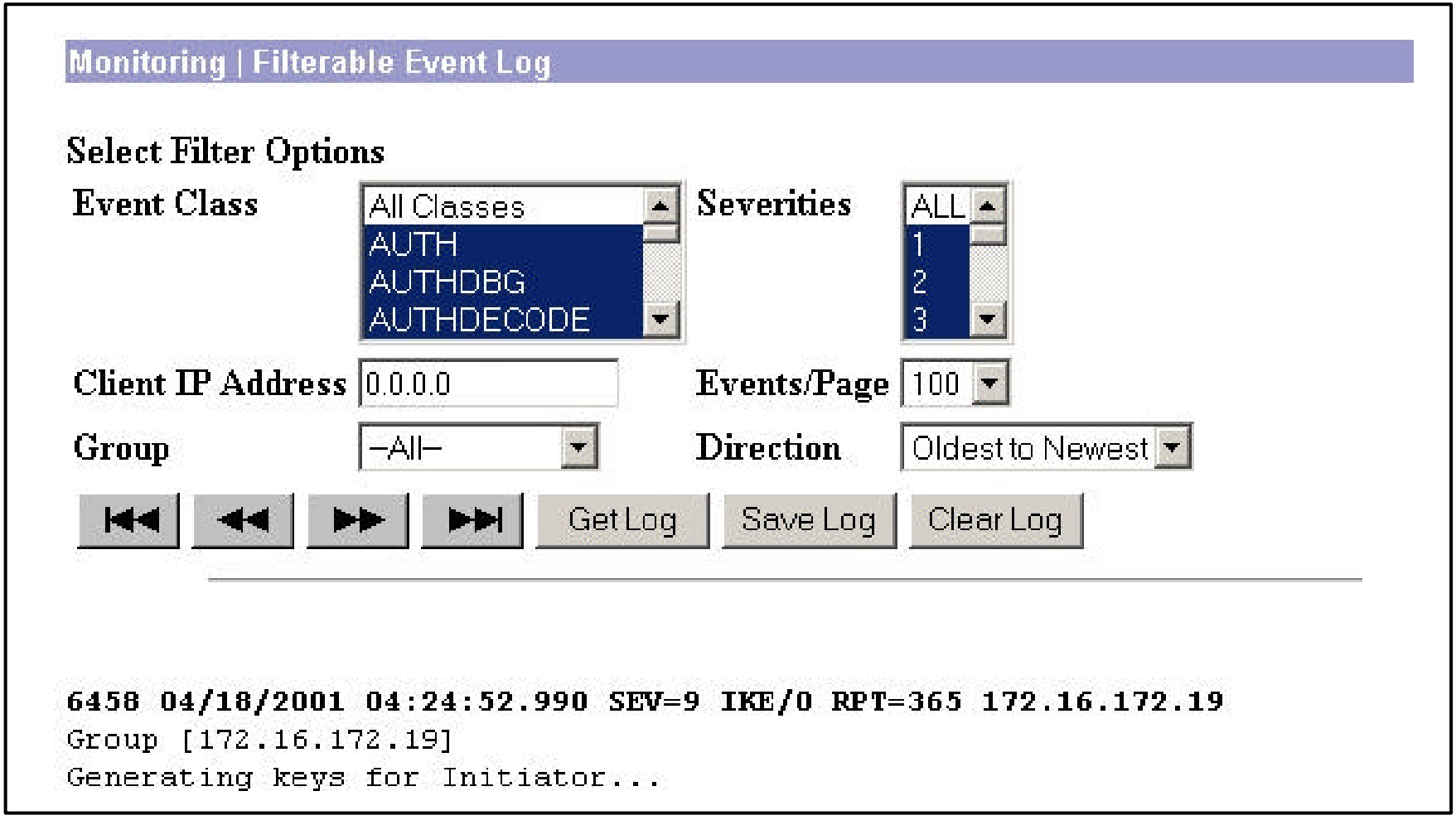
Cisco VPN 3000
Debug Tool (Event Log)

- **Use FILTER and FILTERDBG for packet level debugging**
  - a. **Define specific rules and assign them to the top of the filter**
  - b. **Apply the filter to the interface**
  - c. **Enable FILTER and FILTERDBG Classes to Severity Level 13**
  - d. **Monitoring the Event Log**



Cisco VPN 3000
Debug Tool (Event Log)

Monitoring Event Log



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
```

Common Configuration Errors in Remote Access IPSec VPNs

- **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**

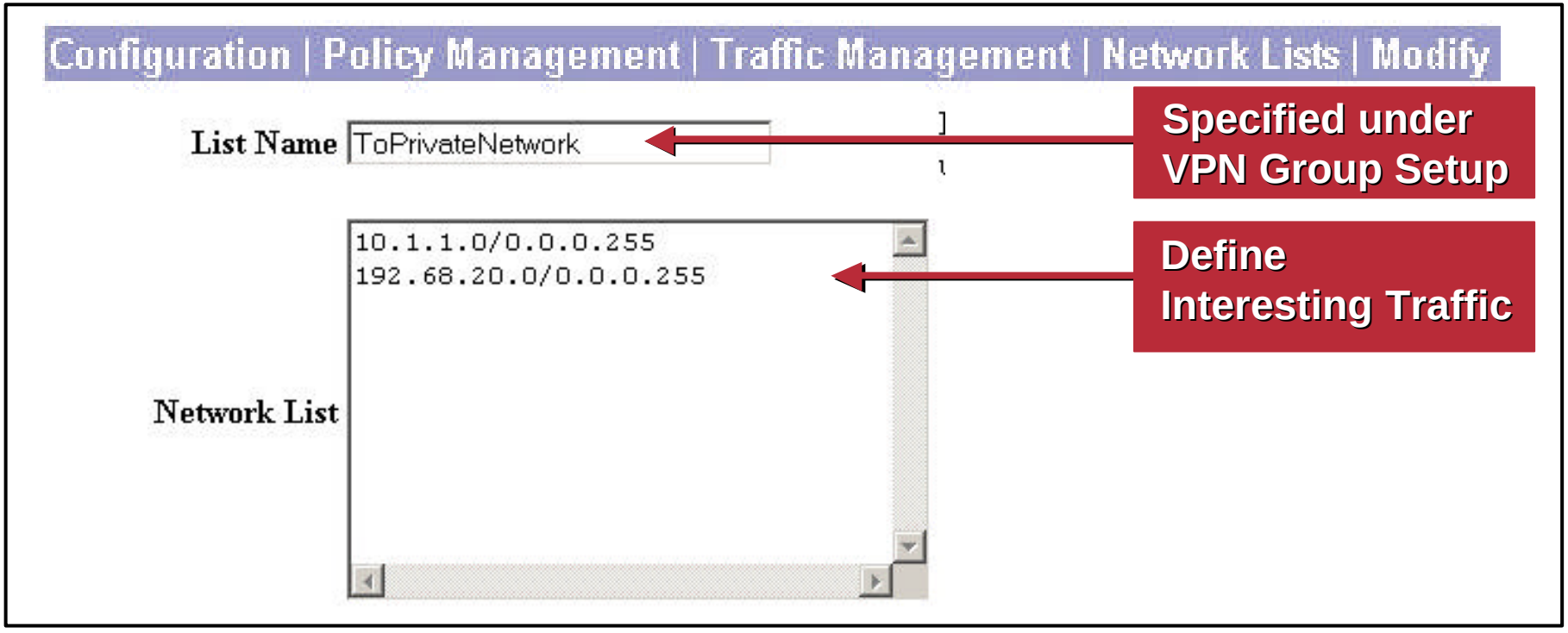
```
333 04/28/2001 12:08:25.320 SEV=3 AUTH/5 RPT=1 171.68.9.125
Authentication rejected: Reason = Invalid password
handle = 23, server = Internal, user = vpnuser, domain = <not specified>
```

- **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
```

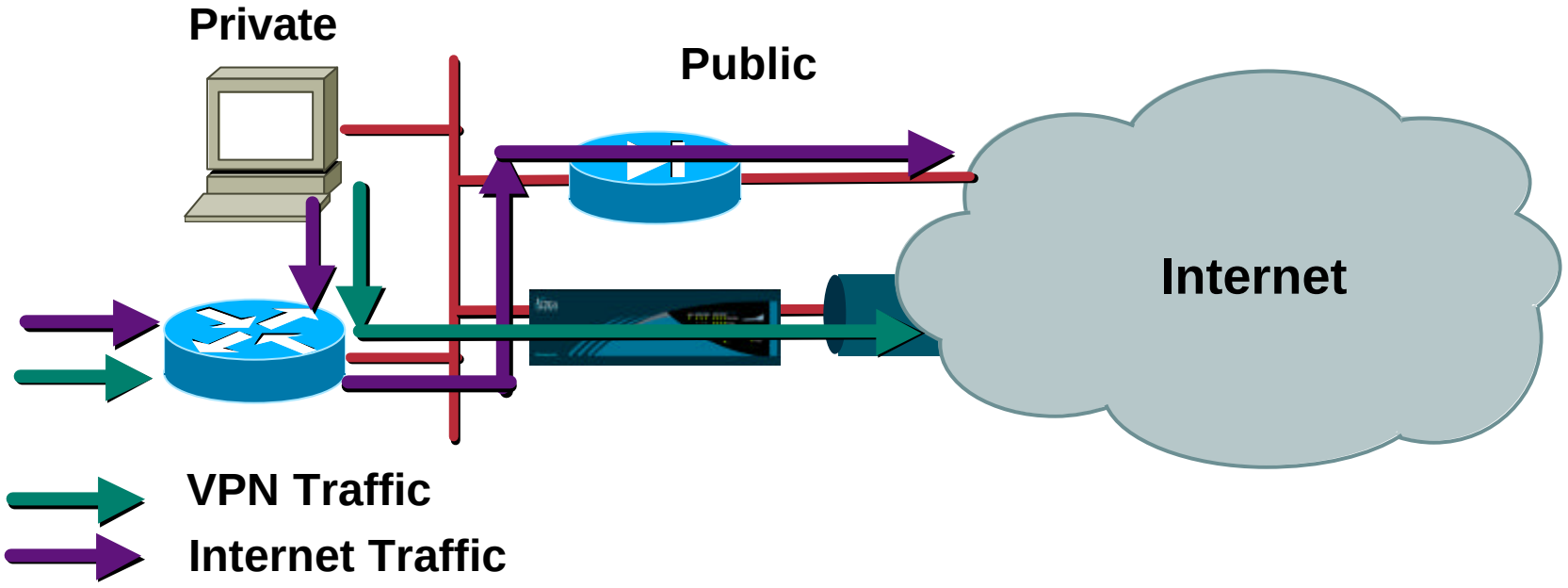
No Access to Internet after VPN Tunnel Is Established

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



Routing Issues

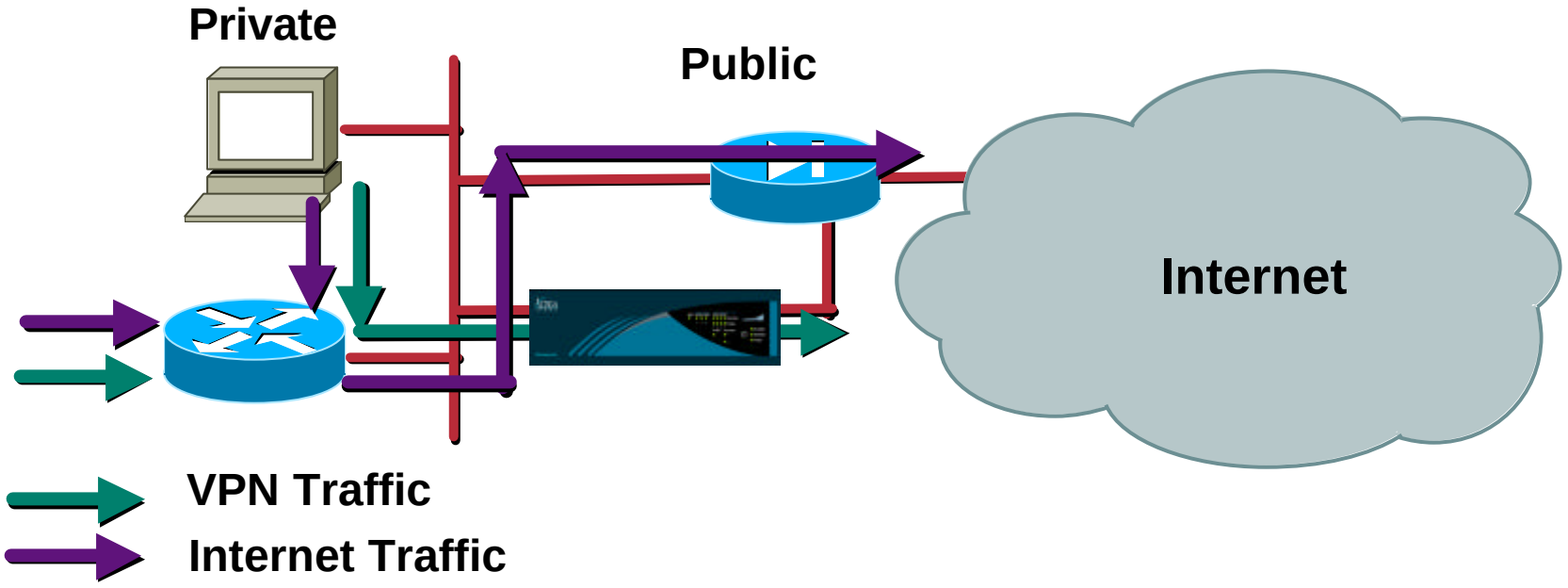
Cisco VPN 3000 In Parallel Position with PIX Firewall



- 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



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

Agenda

Cisco.com

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

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://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

Cisco.com

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

Common Problems

- **Split Tunnel on a gateway**
- **NAT in the middle of an IPSec tunnel**

Split Tunnel on a Gateway

- **Use PAT/NAT to the Internet, but bypass for IPSec tunnel traversal**
- **Tools to debug this setup are:**
  - **Debug ip nat**
  - **Debug ip policy**
  - **Debug ip packet**

Split Tunnel Config


```
crypto map pat 1 ipsec-isakmp
 set peer 10.0.0.100
 set transform-set ahmd5
 match address 150

interface Serial0
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
 crypto map pat
```

Split Tunnel Config


```
interface Ethernet0
 ip address 192.168.0.1 255.255.255.0
 ip nat inside

ip nat inside source route-map internet interface Serial0 overload
access-list 150 permit ip 192.168.0.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 151 deny   ip 192.168.0.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 151 permit ip 192.168.0.0 0.0.0.255 any

route-map internet permit 10
 match ip address 151
```

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. Cisco IOS and PIX to support UDP encaps via new IETF draft by mid year..12.2(9)T and PIX 6.3.**
- **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

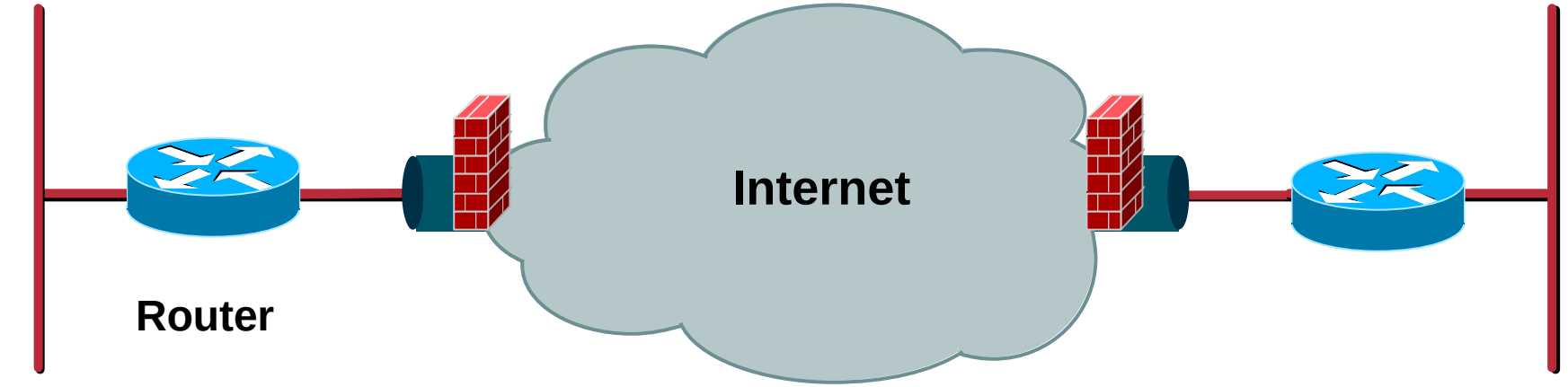
  IP address: <routers statically translated IP address>

Agenda

Cisco.com

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

Firewall in the Middle



Firewalling and IPSec

- **Things to allow in for IPSec to work though a firewall:**
- **Firewall in the middle of the tunnel:**

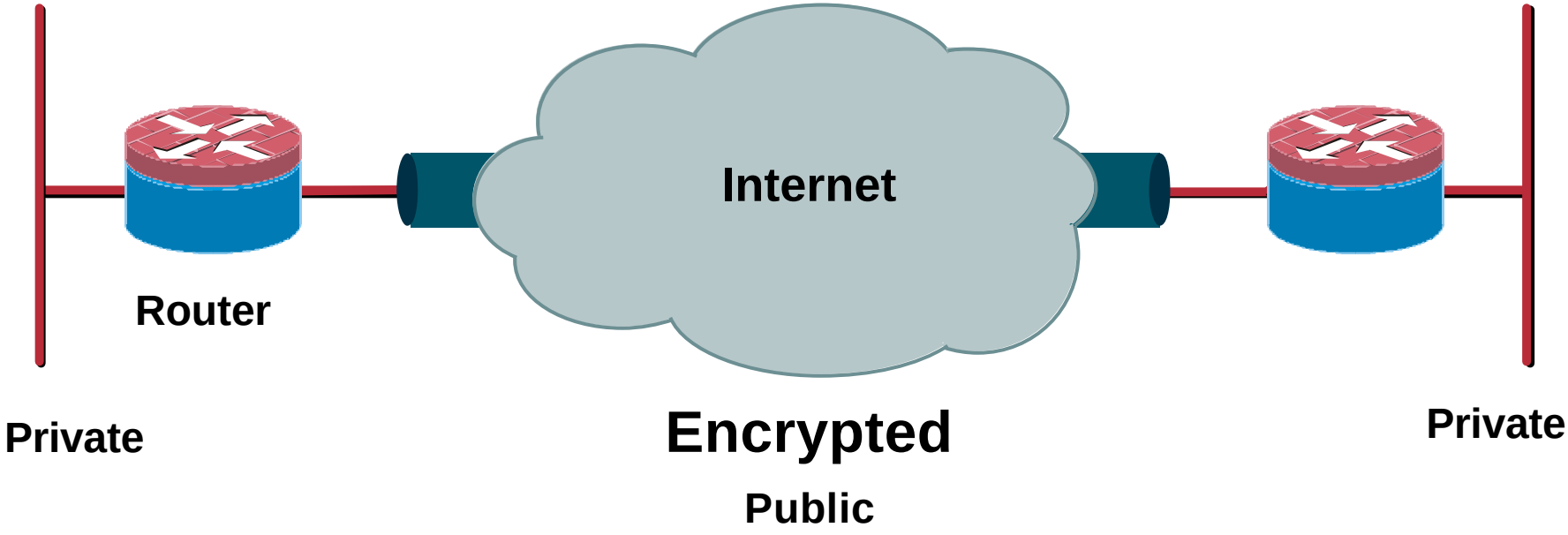
  ESP or/and AH

  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



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

Cisco.com

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

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

```
ICMP: dst (10.1.1.1) frag. needed and DF set unreachable sent to
   192.168.1.1
```

Work Arounds

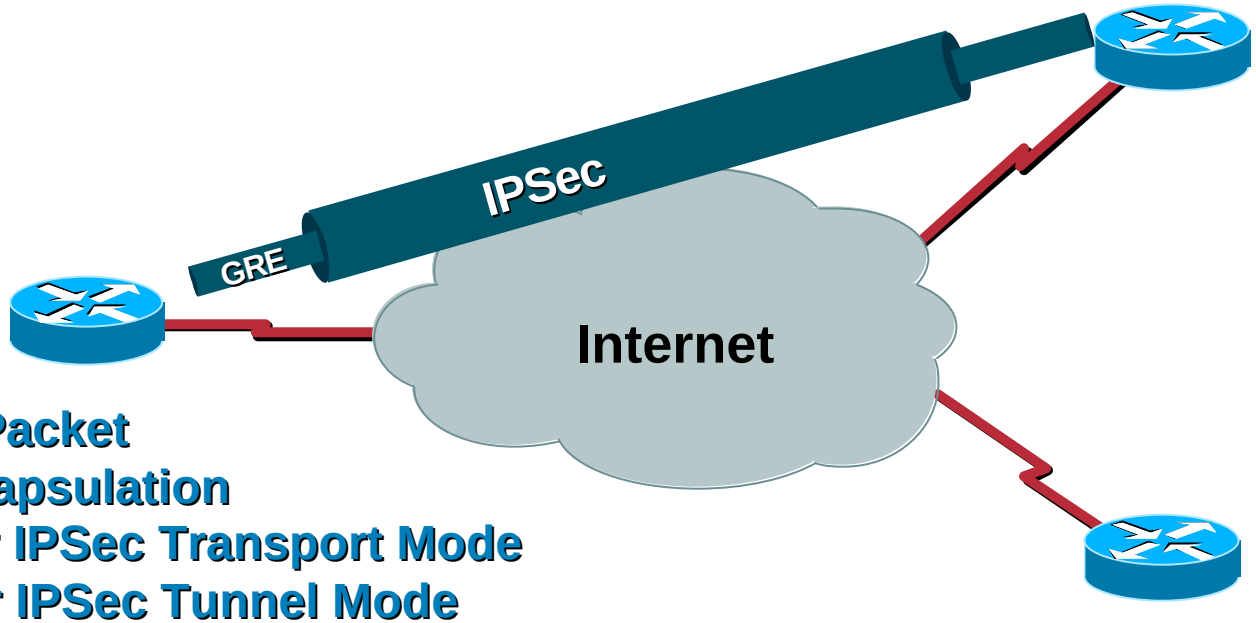
- Make sure that there is no MTU black hole device on the network and let normal path MTU discovery work for you
- If there is some unknown device blocking the ICMP packet too large messages, reduce the MTU on the end machines until the IPSec device does not have to fragment the packet after adding the IPSec header
- 12.1(10)E, 12.2(9)T, 12.2(S)….Pre-frag for Cisco IOS, will look-ahead at packet size after adding max. header size and if > MTU, fragmentation will occur before crypto.

Agenda

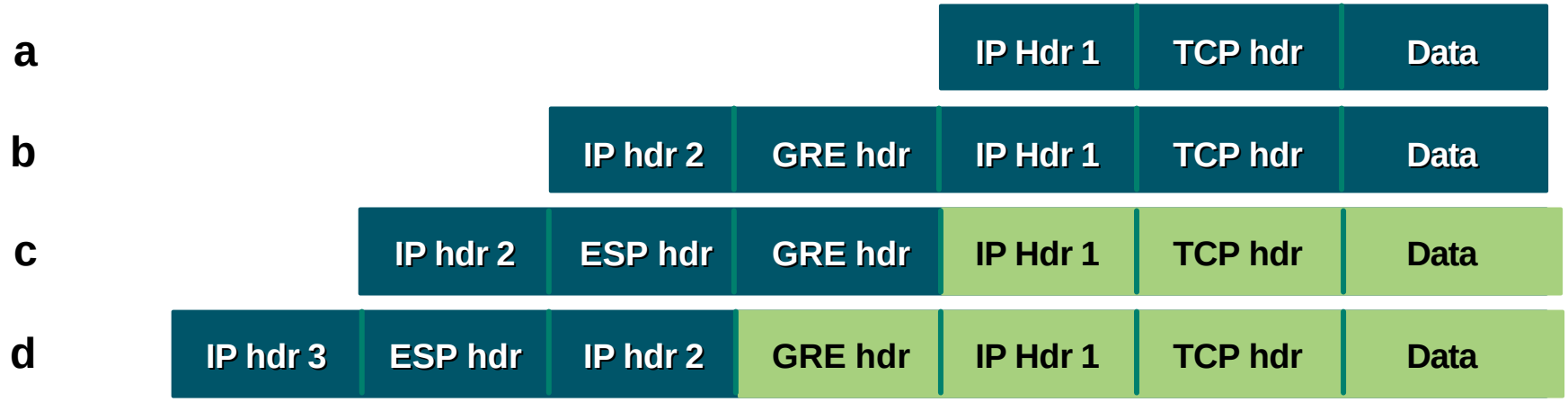
Cisco.com

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

GRE over IPSec



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



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 byes**
- **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…fixed in 12.2(9)T, 12.1(10)E, 12.2(S) via “pre-frag”.

GRE over IPSec (MTU issue)

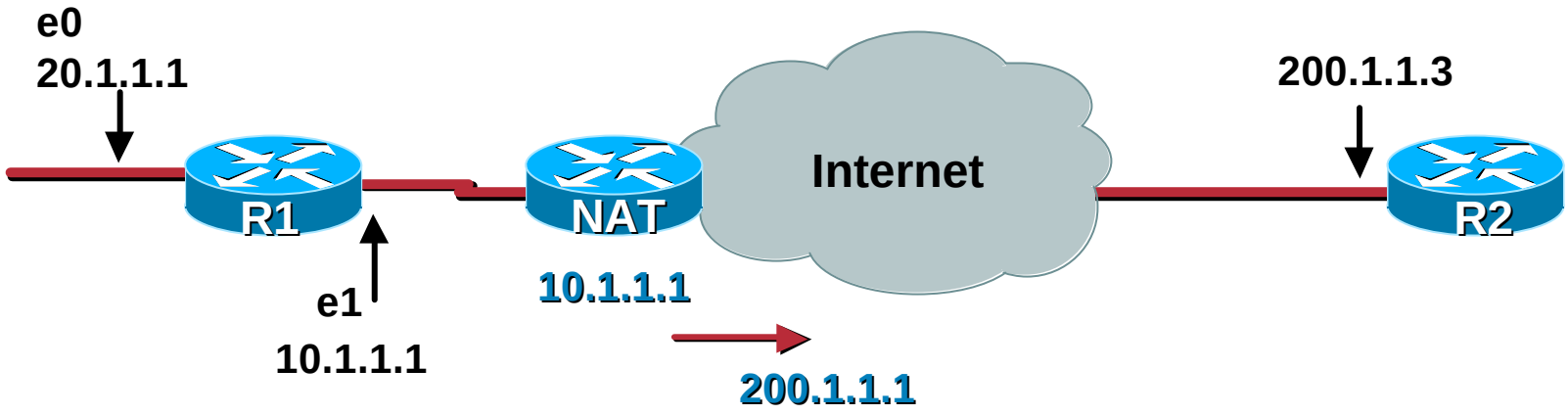
- **To avoid fragementation and reassembly of IPSec packets:**

  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



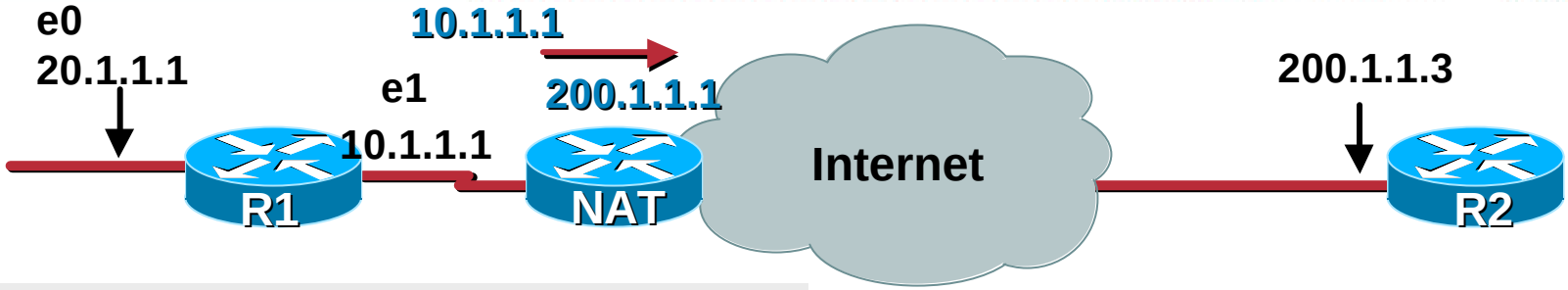
Standard Configuration Won't Work:

```
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_prososal):proxy identities not
supported
```

GRE over IPSec with NAT in Middle



1

```
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
```

2

```
GRE : tunnel_src 20.1.1.1
      tunnel_dest 200.1.1.3
 IPsec (transport mode):
     Peer 200.1.1.3
crypto map mymap local-addr e1
gre host 20.1.1.1 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 :tunnel_src 200.1.1.3
     tunnel_dest 20.1.1.1
IPSec (transport mode):
       Peer 200.1.1.1
gre host 200.1.1.3 host 20.1.1.1
```

GRE over IPSec with NAT in Middle

Cisco.com

2

```
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 test local-address Ethernet1
crypto map test 10 ipsec-isakmp
 set peer 200.1.1.3
 set transform-set test
 match address 101
access list 101 permit 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

Cisco.com

2

```
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
```

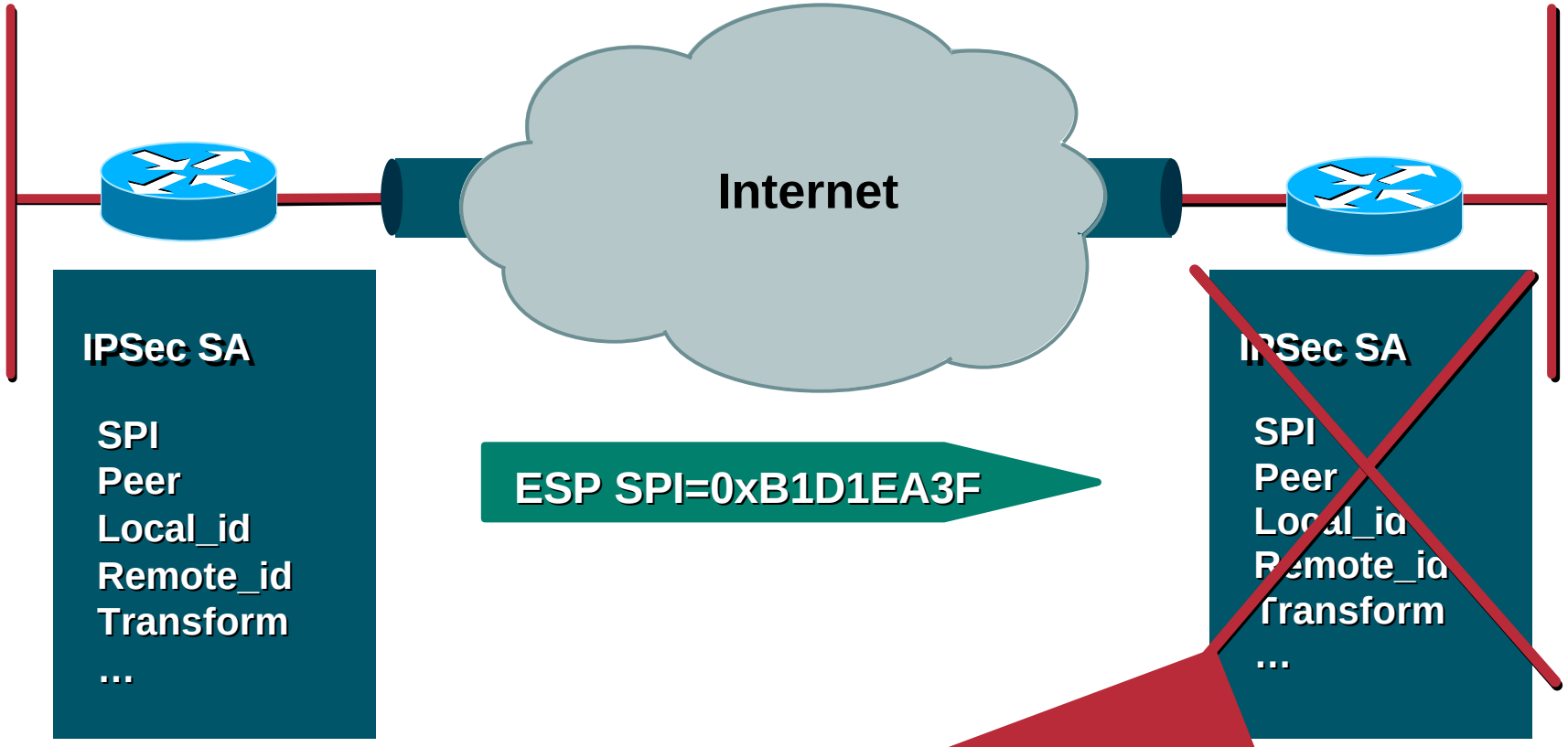
```
interface Tunnel0
 ip address 172.16.1.2
255.255.255.252
 tunnel source Ethernet4/1
 tunnel destination 20.1.1.1
 crypto map test
!
interface Ethernet4/1
 ip address 200.1.1.3 255.255.255.0
 duplex half
 crypto map test
```

Agenda

Cisco.com

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

Loss of Connectivity of IPSec Peers



00:01:33: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=172.16.172.28, prot=50, spi=0xB1D1EA3F(-1311643073)

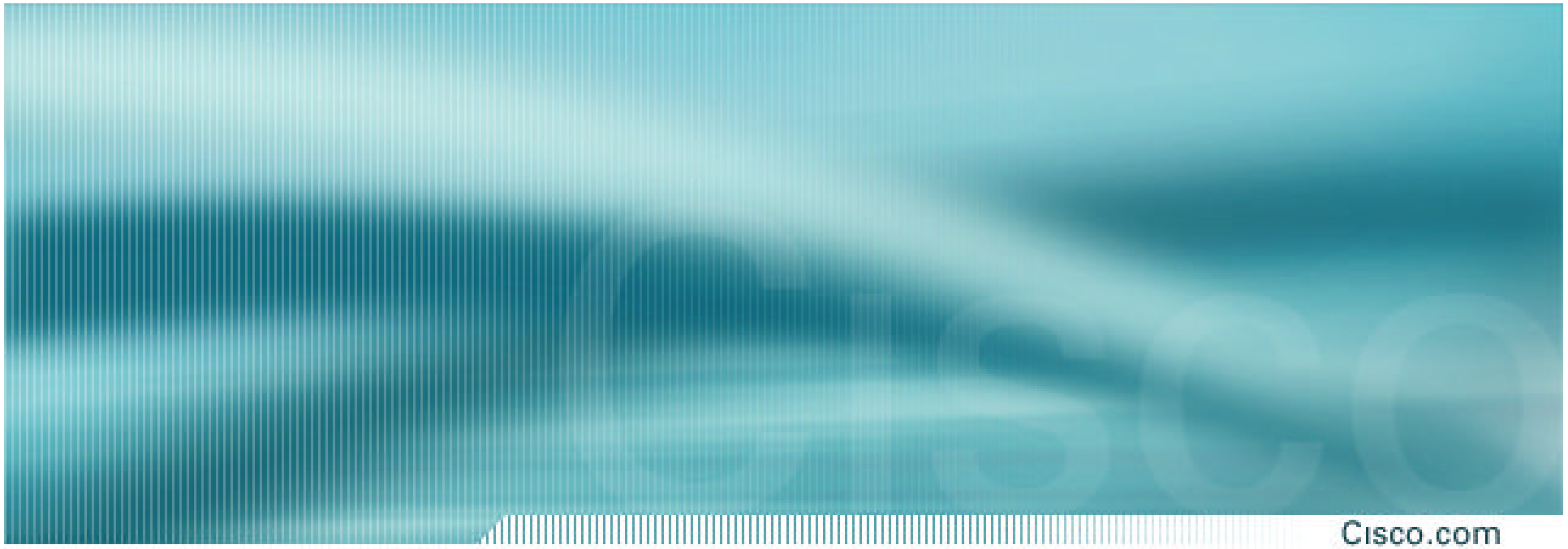
Loss of Connectivity of IPSec Peers

- **Use DPD (Dead Peer Detection) to detect loss of connectivity of IOS IPSec peers**

  crypto isakmp keepalive <# of sec. between keepalive> <number of sec. between retries if keepalive fails>

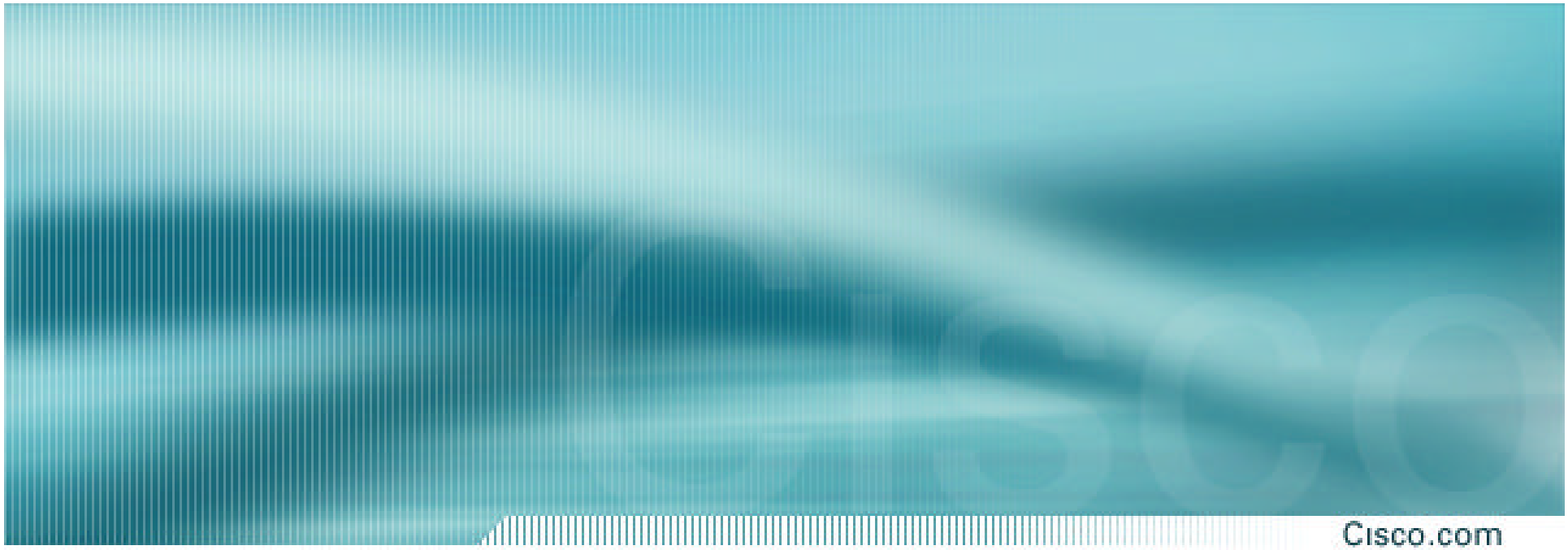
  DPD is new keepalive mechanism.

- **INITIAL_CONTACT will help eliminate INVALID_SPI out of sync errors. See 12.2(8)T, PIX 6.1, VPN3000 3.2, Cisco VPN Client 3.0.**



Troubleshooting the Implementation of IPSec VPNs

Session SEC-310



Please Complete Your Evaluation Form

Session SEC-310