

• NETWORKERS

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

1


CISCO SYSTEMS



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

2



Cisco.com

Troubleshooting IOS and PIX Firewall-Based IPsec Implementations

Session SEC-310

SEC-310
5247_05_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 3

Agenda

Cisco.com

- **Introduction**
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x Client
- PKI Related Issues
- NAT With IPsec
- Firewalling and IPsec
- MTU Issues
- GRE Over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

SEC-310
5247_05_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 4

Why Troubleshooting Is Important in Today's VPN Deployment

Cisco.com

- **Complex security association and key management protocols and a rich set of cryptographic algorithms from which VPN peers can choose**
- **VPNs are often implemented on top of existing networks**
- **VPNs could be used between different vendors**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

5

A Key Point to Remember

Cisco.com

“Debug and Show commands are your friends in troubleshooting any IPsec related issues.”

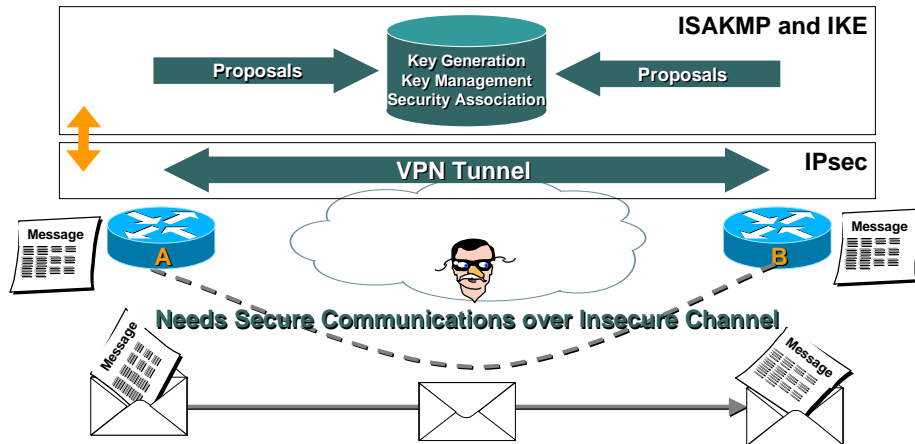
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

6

Secure Communications Using IPsec VPN

Cisco.com



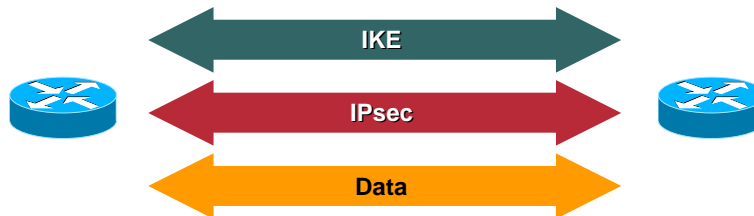
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

7

IKE (Two-Phase Protocol)

Cisco.com



- **Two-phase protocol:**

Phase I exchange: two peers establish a secure, authenticated channel with which to communicate; **Main mode** or **aggressive mode** accomplishes a phase I exchange

Phase II exchange: security associations are negotiated on behalf of IPsec services; **Quick mode** accomplishes a phase II exchange

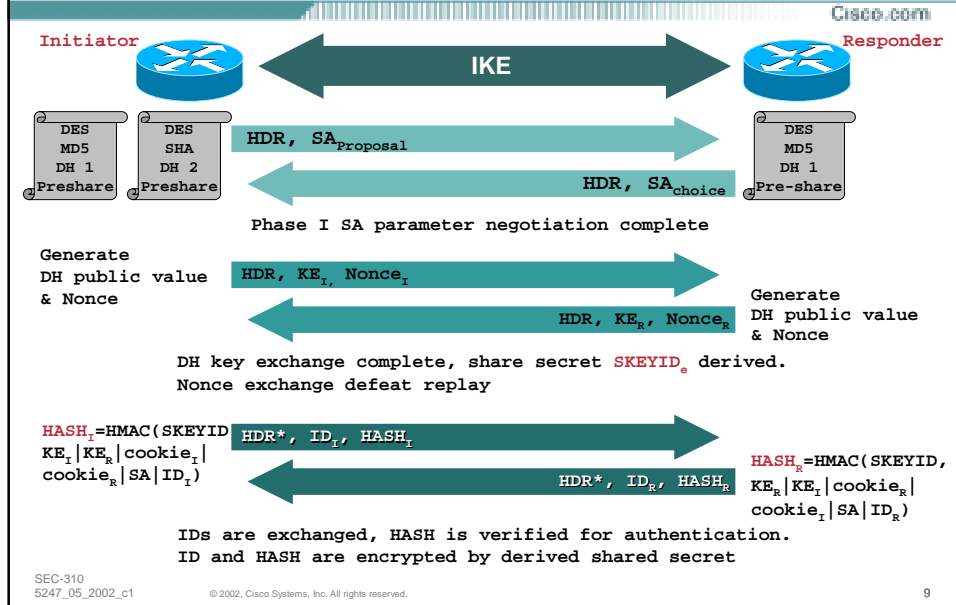
- **Each phase has its SAs: ISAKMP SA (phase I) and IPsec SA (phase II)**

SEC-310
5247_05_2002_c1

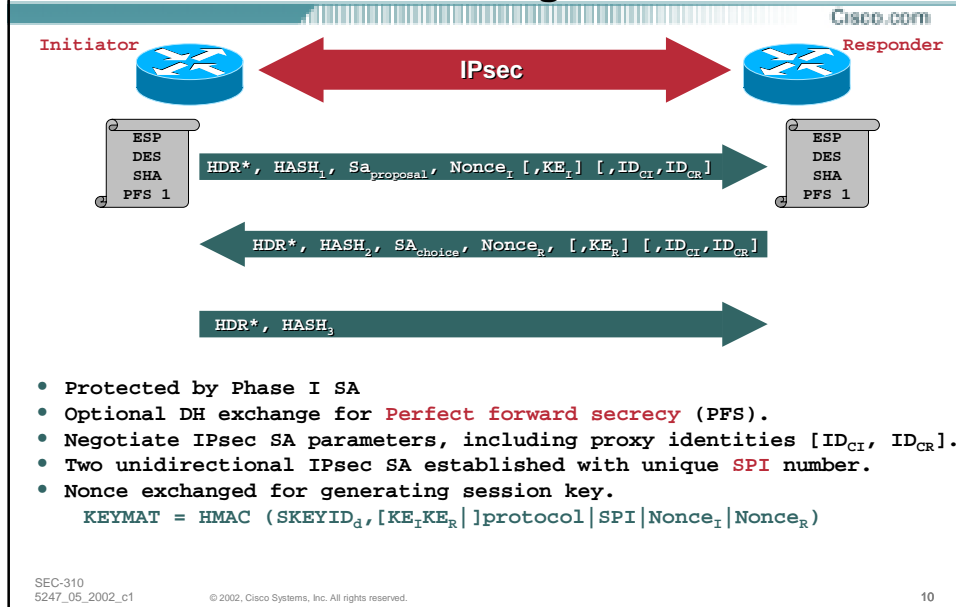
© 2002, Cisco Systems, Inc. All rights reserved.

8

Main Mode With Pre-Shared Key



Phase II Quick Mode Negotiation



Agenda

Cisco.com

- Introduction
- **Router IPsec VPNs**
- PIX IPsec VPNs
- Cisco VPN 3.x Client
- PKI Related Issues
- NAT With IPsec
- Firewalling and IPsec
- MTU Issues
- GRE Over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

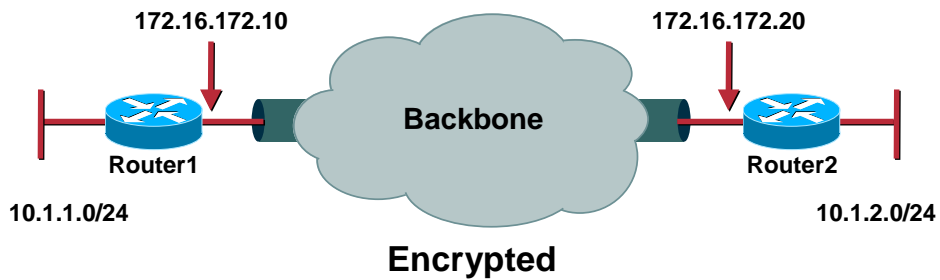
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

11

Layout

Cisco.com



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

12

Normal Router Configurations

Cisco.com

```
crypto isakmp policy 1
  encr 3des
  authentication pre-share
crypto isakmp key jw4ep9846804ijl address 172.16.172.20
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
  set peer 172.16.172.20
  set transform-set myset
  match address 101
```

“crypto isakmp policy” defines the Phase 1 SA parameters

“crypto ipsec transform-set..” command defines IPsec encryption and authn algo

“crypto map..” commands defines the IPsec SA (phase II SA) parameters

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

13

Normal Router Configurations

Cisco.com

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
ip address 172.16.172.10 255.255.255.240
crypto map vpn
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0
0.0.0.255
```

Interface that is connected to the private side of the network

crypto map is then applied to an outbound interface

Access-list defines interesting VPN traffic

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

14

Normal Router Configurations

Cisco.com

```
R1#show crypto map
Crypto Map "vpn" 10 IPsec-isakmp
  Peer = 172.16.172.20
  Extended IP access list 101
    access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0
    0.0.0.255
  Current peer: 172.16.172.20
  Security association lifetime: 4608000 kilobytes/3600
  seconds
  PFS (Y/N): N
  Transform sets={ myset, }
  Interfaces using crypto map vpn:
    Ethernet1/0
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

15

Important Debugs Commands

Cisco.com

- debug crypto isakmp
- debug crypto ipsec
- debug crypto engine
- debug ip packet **<acl>** detail

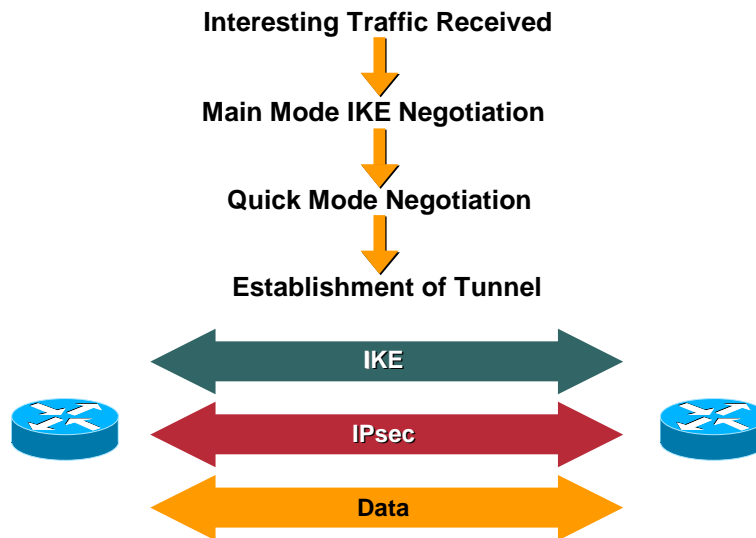
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

16

Debugs Functionality Flow Chart

Cisco.com



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

17

Tunnel Establishment

Cisco.com

- The ping source and destination addresses matched the match address access list for the crypto map vpn

```
00:04:10: IPsec(sa_request): ,  
(key eng. msg.) OUTBOUND local= 172.16.172.10, remote= 172.16.172.20,  
local_proxy = 10.1.1.0/255.255.255.0/0/0 (type=4),  
remote_proxy = 10.1.2.0/255.255.255.0/0/0 (type=4),
```

- The 'local' is the local tunnel end-point, the 'remote' is the remote crypto end point as configured in the map. 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

```
protocol= ESP, transform= esp-3des esp-md5-hmac ,  
lifedur= 3600s and 4608000kb,  
spi= 0x4A10F22E(1242624558), conn_id= 0, keysize= 0, flags= 0x400C
```

- The protocol and the transforms are specified by the crypto map which has been hit, as are the lifetimes

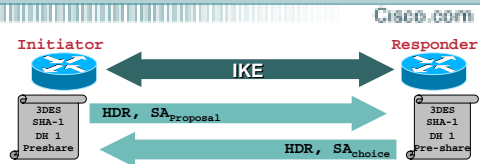
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

18

IKE Main Mode Negotiation— Phase I SA Negotiation

- **Begins Main Mode exchange;
The first two packets negotiate
phase I SA parameters**



```
ISAKMP: received ke message (1/1)
ISAKMP: local port 500, remote port 500
ISAKMP (0:1): Input = IKE_MSG_FROM_IPsec, IKE_SA_REQ_MM Old State =
    IKE_READY New State = IKE_I_MM1
```

```
ISAKMP (0:1): beginning Main Mode exchange
00:04:10: ISAKMP (0:1): sending packet to 172.16.172.20 (I) MM_NO_STATE
00:04:10: ISAKMP (0:1): received packet from 172.16.172.20 (I)
MM_NO_STATE
00:04:10: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM1 New State = IKE_I_MM2
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

19

IKE Main Mode Negotiation— Phase I SA Negotiation

```
00:04:10: ISAKMP (0:1): processing SA payload. message ID = 0
00:04:10: ISAKMP (0:1): found peer pre-shared key matching 172.16.172.20
00:04:10: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
00:04:10: ISAKMP: encryption 3DES-CBC
00:04:10: ISAKMP: hash SHA
00:04:10: ISAKMP: default group 1
00:04:10: ISAKMP: auth pre-share
00:04:10: ISAKMP: life type in seconds
00:04:10: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:04:10: ISAKMP (0:1): atts are acceptable. Next payload is 0
00:04:10: ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_I_MM2 New State = IKE_I_MM2
```

- **The policy 1 on this router and the atts offered by the other side matched**

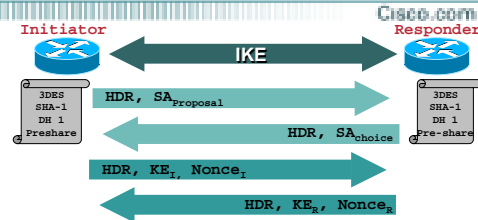
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

20

IKE Main Mode Negotiation— DH Exchange

- The third and fourth packets complete Diffie-Hellman exchange



```
ISAKMP (0:1): sending packet to
172.16.172.20 (I) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE Old State = IKE_I_MM2 New State = IKE_I_MM3
ISAKMP (0:1): received packet from 172.16.172.20 (I) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM3 New State = IKE_I_MM4

ISAKMP (0:1): processing KE payload. message ID = 0
ISAKMP (0:1): processing NONCE payload. message ID = 0
ISAKMP (0:1): found peer pre-shared key matching 172.16.172.20
ISAKMP (0:1): SKEYID state generated
ISAKMP (0:1): processing vendor id payload
```

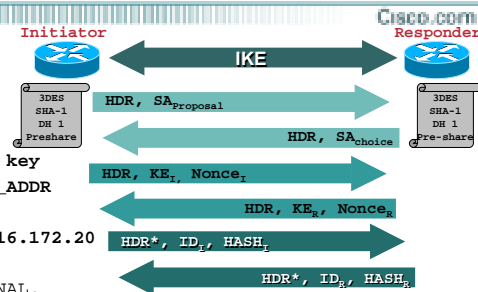
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

21

IKE Main Mode Negotiation— Authentication

- The fifth and sixth packets complete IKE authentication; Phase 1 SA established



```
ISAKMP (0:1): SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
.....
ISAKMP (0:1): sending packet to 172.16.172.20
(I) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE Old State = IKE_I_MM4 New State = IKE_I_MM5

ISAKMP (0:1): received packet from 172.16.172.20 (I) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM5 New State = IKE_I_MM6
ISAKMP (0:1): processing ID payload. message ID = 0
ISAKMP (0:1): processing HASH payload. message ID = 0
ISAKMP (0:1): SA has been authenticated with 172.16.172.20
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

22

IKE Quick Mode



- **Begin Quick Mode exchange; IPsec SA will be negotiated in QM**

```
ISAKMP (0:1): beginning Quick Mode exchange,
M-ID of 965273472
ISAKMP (0:1): sending packet to 172.16.172.20 (I) QM_IDLE
ISAKMP (0:1): Node 965273472, Input = IKE_MSG_INTERNAL, IKE_INIT_QM Old
State = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP (0:1): received packet from 172.16.172.20 (I) QM_IDLE
```

- **The IPsec SA proposal offered by far end will be checked against local crypto map configuration**

```
ISAKMP (0:1): processing HASH payload. message ID = 965273472
ISAKMP (0:1): processing SA payload. message ID = 965273472
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

23

IKE Quick Mode

Cisco.com

```
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 3600
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-MD5
ISAKMP (0:1): atts are acceptable.
IPsec(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.172.10, remote= 172.16.172.20,
local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

24

IKE Quick Mode

Cisco.com

- **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**

ISAKMP (0:1): **Creating IPsec SAs**

inbound SA from 172.16.172.20 to 172.16.172.10(proxy 10.1.2.0 to 10.1.1.0)

has spi 0x8EAB0B22 and conn_id 2029 and flags 4

lifetime of 3600 seconds lifetime of 4608000 kilobytes

outbound SA from 172.16.172.10 to 172.16.172.20 (proxy 10.1.1.0 to 10.1.2.0)

has spi -343614331 and conn_id 2030 and flags C

lifetime of 3600 seconds lifetime of 4608000 kilobytes

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

25

IKE Quick Mode

Cisco.com

- **The IPsec SA info negotiated by IKE will be populated into router's SADB**

00:04:10: IPsec(key_engine): got a queue event...

00:04:10: IPsec(initialize_sas): ,

(key eng. msg.) **INBOUND local=** 172.16.172.10, **remote=** 172.16.172.20,

local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),

remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),

protocol= ESP, **transform=** esp-3des esp-md5-hmac ,

lifedur= 3600s and 4608000kb,

spi= 0x8EAB0B22(2393574178), **conn_id=** 2029, **keysize=** 0, **flags=** 0x4

00:04:10: IPsec(initialize_sas): ,

(key eng. msg.) **OUTBOUND local=** 172.16.172.10, **remote=** 172.16.172.20,

local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),

remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),

protocol= ESP, **transform=** esp-3des esp-md5-hmac ,

lifedur= 3600s and 4608000kb,

spi= 0xEB84DC85(3951352965), **conn_id=** 2030, **keysize=** 0, **flags=** 0xC

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

26

IKE Quick Mode

- IPsec SA created in SADB, sent out last packet with commit bit set; IPsec tunnel established

```
IPsec(create_sa): sa created,
(sa) sa_dest= 172.16.172.10,
sa_prot= 50,
sa_spi= 0x8EAB0B22(2393574178),
sa_trans= esp-3des esp-md5-hmac ,
sa_conn_id= 2029
```

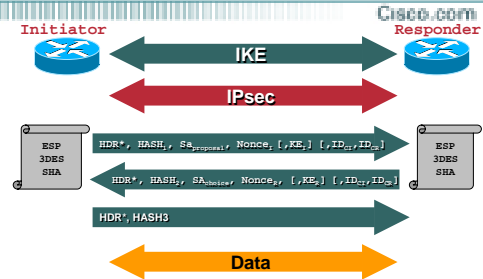
```
IPsec(create_sa): sa created,
```

```
(sa) sa_dest= 172.16.172.20, sa_prot= 50, sa_spi= 0xEB84DC85(3951352965),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2030
```

```
ISAKMP (0:1): sending packet to 172.16.172.20 (I) QM_IDLE
```

```
ISAKMP (0:1): Node 965273472, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
```

```
Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
```



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

27

Show Commands

Cisco.com

- Show crypto engine connection active
- Show crypto isakmp sa
- Show crypto ipsec sa

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

28

Show Commands

Cisco.com

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

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	<none>	<none>	set	HMAC_SHA+3DES_56_C	0	0
This is ISAKMP SA						
2029	Ethernet1/0	172.16.172.10	set	HMAC_MD5+3DES_56_C	0	4
2030	Ethernet1/0	172.16.172.10	set	HMAC_MD5+3DES_56_C	4	0
These two are IPsec SAs						

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

dst	src	state	conn-id	slot
172.16.172.20	172.16.172.10	QM_IDLE	1	0

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

29

Show Commands

Cisco.com

```
Router#sh crypto ipsec sa
```

```
interface: Ethernet1/0
  Crypto map tag: vpn, local addr. 172.16.172.10

  local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
  current_peer: 172.16.172.20
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 6, #recv errors 0

  local crypto endpt.: 172.16.172.10, remote crypto endpt.: 172.16.172.20
  path mtu 1500, media mtu 1500
  current outbound spi: EB84DC85
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

30

Show Commands

Cisco.com

inbound esp sas:

```
spi: 0x8EAB0B22(2393574178)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2029, flow_id: 1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607998/3347)
IV size: 8 bytes
replay detection support: Y
```

outbound esp sas:

```
spi: 0xEB84DC85(3951352965)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2030, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4607999/3347)
IV size: 8 bytes
replay detection support: Y
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

31

Hardware Crypto Engine

Cisco.com

- In latest IOS versions, show commands for different types of hardware crypto cards have been unified

Verify hardware/software
crypto engine

Show crypto engine configuration

Hardware info

Show diag

Turn on/off the hardware
crypto engine

[no] crypto engine accelerator [slot_no.]

Display statistics

Show crypto engine accelerator stat

Debug crypto engine

Debug crypto engine accelerator packet

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

32

Verify Crypto Engine

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:
B82CA6C09E080DF0E0A1029EF8E7112F3FF5F
67B
PCBD info: 3-DES [07F000260000]
Compression: No
3 DES: Yes
```

```
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
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

33

Common Issues

Cisco.com

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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

34

Incompatible ISAKMP Policy or Preshared Secrets

Cisco.com

- If the configured ISAKMP policies don't match the proposed policy by the remote peer, the router tries the default policy of 65535, and if that does not match either, it fails ISAKMP negotiation

Default protection suite

```
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group:  #1 (768 bit)
lifetime:              86400 seconds, no volume limit
```

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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

35

Incompatible ISAKMP Policy or Preshared Secrets

Cisco.com

```
3d01h: ISAKMP (0:1): processing SA
payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-
shared key matching 172.16.172.10
ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of
0x0 0x1 0x51 0x80
ISAKMP (0:1): Hash algorithm offered
does not match policy!
ISAKMP (0:1): atts are not acceptable.
Next payload is 0
```

```
ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 65535
policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of
0x0 0x1 0x51 0x80
ISAKMP (0:1): Encryption algorithm
offered does not match policy!
ISAKMP (0:1): atts are not acceptable.
Next payload is 0
ISAKMP (0:1): no offers accepted!
ISAKMP (0:1): phase 1 SA not
acceptable!
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

36

Incompatible ISAKMP Policy or Preshared Secrets

Cisco.com

- 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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

37

Incompatible ISAKMP Policy or Preshared Secrets

Cisco.com

```
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 not zero on ID payload!
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 172.16.172.10
failed its sanity check or is malformed
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

38

Incompatible IPsec Transform Set

Cisco.com

- If the ipsec transform-set is not compatible or mismatched on the two IPsec devices, the IPsec negotiation will fail, with the router complaining about "atts not acceptable" for the IPsec proposal

ISAKMP (0:2): Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES

ISAKMP: attributes in transform:

ISAKMP: encaps is 1

ISAKMP: SA life type in seconds

ISAKMP: SA life duration (basic) of 3600

ISAKMP: SA life type in kilobytes

ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0

IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 0) not supported

ISAKMP (0:2): atts not acceptable. Next payload is 0

ISAKMP (0:2): SA not acceptable!

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

39

Incompatible or Incorrect Access Lists

Cisco.com

- If the access lists on the two routers don't match **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 word **any** not be used in match address access lists

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

40

Incompatible or Incorrect Access Lists

Cisco.com

```
1w6d: IPSEC(validate_proposal_request): proposal part #1,  
(key eng. msg.) INBOUND local= 172.16.172.20, remote= 172.16.172.10,  
local_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),  
remote_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-3des esp-md5-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

```
1w6d: IPSEC(validate_transform_proposal): proxy identities not supported
```

```
1w6d: ISAKMP (0:2): IPsec policy invalidated proposal
```

```
1w6d: ISAKMP (0:2): phase 2 SA not acceptable!
```

```
Access List at 172.16.172.10:
```

```
access list 110 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
```

```
Access List at 172.16.172.20:
```

```
access list 110 permit ip 10.1.2.0 0.0.0.255 10.1.3.0 0.0.0.255
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

41

Crypto Map on the Wrong Interface

Cisco.com

- The crypto map needs to be applied to the outgoing interface of the router.
IPSEC(validate_proposal): invalid local address 172.16.172.20
ISAKMP (0:4): atts not acceptable. Next payload is 0
ISAKMP (0:4): phase 2 SA not acceptable!
- 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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

42

Incorrect SA Selection by the Router

Cisco.com

- 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 choose the wrong crypto map to try and establish a tunnel with one of the other peers

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

43

Incorrect SA Selection by the Router

Cisco.com

```
IPSEC(validate_proposal_request): proposal part #1,  
(key eng. msg.) INBOUND local= 172.16.172.10, remote= 172.16.172.30,  
local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),  
remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-3des esp-md5-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4  
IPSEC(validate_transform_proposal): peer address 172.16.172.30 not found  
ISAKMP (0:2): IPsec policy invalidated proposal  
ISAKMP (0:2): phase 2 SA not acceptable!  
  
Access list for 172.16.172.20:  
Access-list 100 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255  
Access-list 100 permit ip 10.1.1.0 0.0.0.255 10.1.5.0 0.0.0.255  
  
Access list for 172.16.172.30:  
Access-list 110 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

44

Routing Issues

Cisco.com

- 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 for:
 - the router to reach its peers address
 - the IP subnets of the destination host before the packets are encrypted
 - the IP subnets of the destination host once the packets are decrypted
- Use the **debug ip packet <acl> detailed** to see if the routing is occurring correctly
(be careful on the busy networks!!!)

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

45

Possible Caveats in Switching Paths

Cisco.com

- **Symptom:** Only see encryption or decryption counter incrementing from “show crypto eng conn active”

Caveats in the switching paths might cause IPsec encryption/decryption failures
- **Workaround:** Try different switch paths (CEF, Fast switching, Process switching)
- **Process switching can cause Performance issues!**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

46

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- **PIX IPsec VPNs**
- Cisco VPN 3.x client
- PKI related Issues
- NAT with IPsec
- Firewalling and IPsec
- MTU Issues
- GRE over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

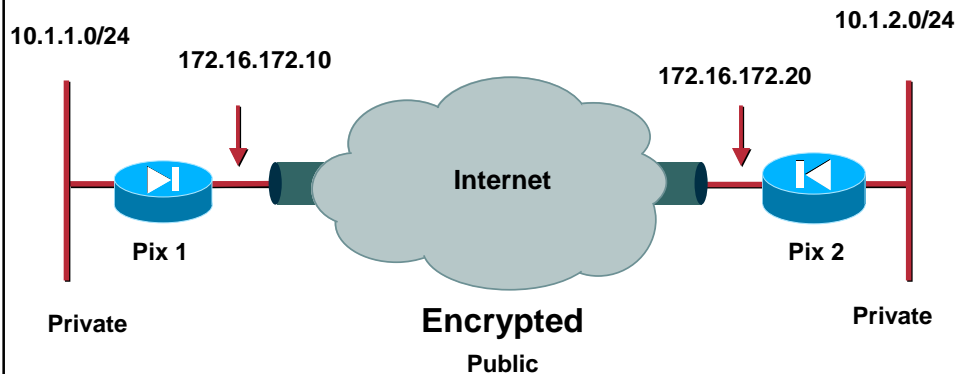
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

47

Layout

Cisco.com



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

48

Standard Site-to-Site VPN Configuration Highlight

Cisco.com

```
access-list bypassnat permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
```

Access-list "bypassnat" defines interesting traffic to bypass NAT for VPN

```
nat (inside) 0 access-list bypassnat
```

NAT 0 command bypasses NAT for the pkts destined over the IPsec tunnel

```
access-list encrypt permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
```

Access-list "encrypt" defines VPN interesting traffic

```
ip address outside 172.16.172.10 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
route outside 0.0.0.0 0.0.0.0 172.16.172.20 1
```

IP Addresses on the outside and inside interfaces

```
sysopt connection permit-ipsec
```

Sysopt command bypasses conduits or ACLs checking to be applied on the inbound VPN packets after decryption

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

49

Standard Site-to-Site VPN Configuration Highlight

Cisco.com

```
crypto ipsec transform-set mysetdes esp-des
esp-md5-hmac
```

"crypto IPsec.." command defines IPsec encryption and authn algo

```
crypto map encryptmap 20 ipsec-isakmp
crypto map encryptmap 20 match address encrypt
crypto map encryptmap 20 set peer 172.16.172.20
crypto map encryptmap 20 set transform-set
mysetdes
crypto map encryptmap interface outside
```

"crypto map.." commands define the IPsec SA (phase II SA) parameters

```
isakmp enable outside
isakmp key cisco123 address 172.16.172.20
netmask 255.255.255.255 no-xauth no-config-mode
```

"isakmp key.." command defines the Preshared key for the Peer Address

```
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 86400
```

"isakmp policy.." defines the Phase 1 SA parameters

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

50

Common Issues

Cisco.com

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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

51

Bypassing NAT

Cisco.com

- 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 **NAT 0** command with an access list to achieve that

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

52

Enabling ISAKMP

Cisco.com

- Unlike the router, ISAKMP is not enabled by default on the PIX
- Use the command **isakmp enable** **<interface>** to enable it on an interface

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

53

Missing Sysopt Commands

Cisco.com

- After decryption, PIX will check the access-lists or conduits against the decrypted IP packets
- Access-lists or conduits need to be configured to permit decrypted IP traffic
- Enable **sysopt connection permit-ipsec** to bypass the access-list/conduit checking against VPN traffic after decryption

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

54

Combining PIX-PIX and PIX-Client Issues

Cisco.com

- If you are doing mode config or x-auth for the VPN clients you would need to disable them for the site-to-site VPN connections
- Use the **no-config-mode** and **no x-auth** tags at the end of the preshared key definitions to disable mode config and x-auth
- **isakmp peer fqdn fqdn no-xauth no-config-mode** in case rsa-sig is used as IKE authentication method

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

55

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- **Cisco VPN 3.x Client**
- PKI Related Issues
- NAT With IPsec
- Firewalling and IPsec
- MTU Issues
- GRE Over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

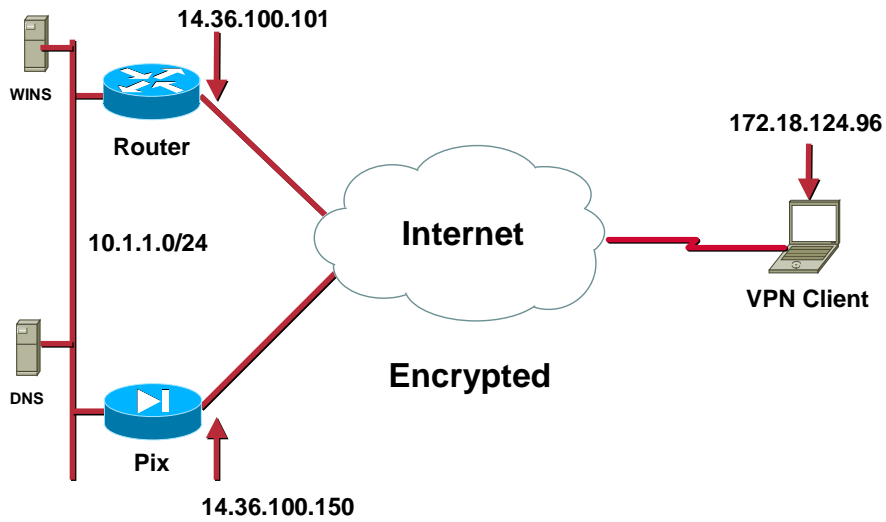
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

56

Layout

Cisco.com



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

57

VPN 3.x Client to a Router

Cisco.com

```
aaa new-model
aaa authentication login userauthen local
aaa authorization network groupauthen local
username cisco password 0 cisco123
!
crypto isakmp policy 3
encr 3des
authentication pre-share
group 2
!
crypto isakmp client configuration group vpnclient
key cisco123
dns 10.1.1.10
wins 10.1.1.20
domain cisco.com
pool ippool
acl 100
```

aaa commands enable user Authentication and Group Authorization

ISAKMP policy defines Phase 1 parameters

"Crypto isakmp client configuration .." commands define mode-configuration parameters that will be passed to the VPN clients

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

58

VPN 3.x client to a Router (Contd.)

Cisco.com

```
crypto IPsec transform-set myset esp-3des esp-sha-hmac
!
```

“crypto IPsec..” command defines IPsec encryption and authn algo

```
crypto dynamic-map dynmap 10
set transform-set myset
!
```

“crypto dynamic-map...” defines a dynamic map which would be included in the actual map

```
crypto map clientmap client authentication list userauthn
crypto map clientmap isakmp authorization list groupauthn
crypto map clientmap client configuration address respond
crypto map clientmap 10 IPsec-isakmp dynamic dynmap
```

“crypto map...” commands define the actual map which would be applied to the outbound interface for the data encryption

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

59

VPN 3.x client to a Router (Contd.)

Cisco.com

```
ip local pool ippool 14.1.1.1 14.1.1.254
!
```

“ip local pool...” command defines a pool of addresses to be assigned back to the VPN client

```
access-list 100 permit ip 10.1.1.0 0.0.0.255 14.1.1.0 0.0.0.255
!
```

access-list defines Split-Tunneling

```
interface FastEthernet2/0
ip address 14.36.100.101 255.255.0.0
crypto map clientmap
```

crypto map is then applied to an outbound interface

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

60

VPN 3.x client to a PIX

Cisco.com

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 10.1.2.0
255.255.255.0
nat (inside) 0 access-list 101

ip address outside 14.36.100.150 255.255.0.0
ip address inside 10.1.1.1 255.255.255.0

ip local pool ippool 10.1.2.1-10.1.2.254

isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

Define an Access-List, that would be used to by-pass NAT for the IPsec Traffic

Define IP Address on the Interfaces

Define a Pool of Addresses to be assigned back to the VPN client

ISAKMP policy defines Phase 1 parameters

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

61

VPN 3.x client to a PIX (Contd.)

Cisco.com

```
sysopt connection permit-IPsec

vpngroup vpnclient address-pool ippool
vpngroup vpnclient dns-server 10.1.1.2
vpngroup vpnclient wins-server 10.1.1.2
vpngroup vpnclient default-domain cisco.com
vpngroup vpnclient split-tunnel 101
vpngroup vpnclient idle-time 1800
vpngroup vpnclient password *****

crypto IPsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset

crypto map mymap 10 IPsec-isakmp dynamic dynmap
crypto map mymap interface outside
```

Sysopt command bypasses conduits or ACLs checking to be applied on the inbound VPN packets after decryption

vpngroup commands enable group authorization. You can pass down mode-configuration parameters within this section back to the VPN client
Note that Access-list 101 can be used again for Split-Tunneling

"crypto IPsec transform-set..." command defines Phase 2 negotiation parameters

"crypto map..." commands defines the actual map which would be applied to an interface for the data encryption

SEC-310
5247_05_2002_c1

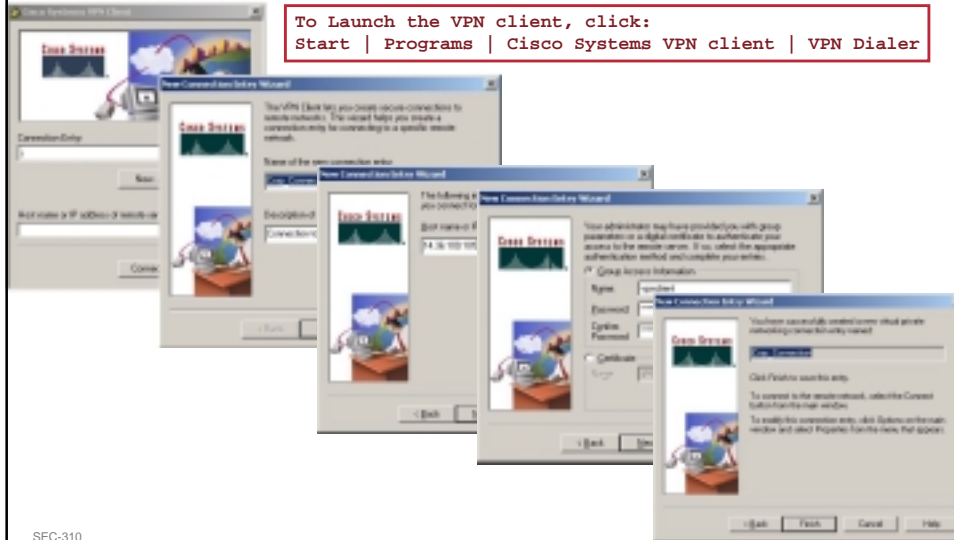
© 2002, Cisco Systems, Inc. All rights reserved.

62

VPN Client Configuration

Cisco.com

To Launch the VPN client, click:
Start | Programs | Cisco Systems VPN client | VPN Dialer



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

63

IOS Debugs: Phase I Negotiation

Cisco.com

Debug crypto isakmp
 Debug crypto ipsec

```

ISAKMP (0:0): received packet from 172.18.124.96 (N) NEW SA,
ISAKMP: local port 500, remote port 500
...
ISAKMP (0:10): Checking ISAKMP transform 1 against priority 3
policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:10): atts are acceptable. Next payload is 3
...
Old State = IKE_READY New State = IKE_R_AM_AWAIT
    
```

This message indicates that this Router received an ISAKMP message from the 3.x client on src port 500, dst port=500

Router is trying to match the received proposal # 1 with the configured proposal # 3

Received Proposal is acceptable

Since the 3.x client does Aggressive Mode, the new state is IKE_R_AM_AWAIT

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

64

IOS Debugs: Xauth

Cisco.com

```
...
ISAKMP (0:10): Need XAUTH
...
ISAKMP/xauth: request attribute XAUTH_TYPE_V2
ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute
  XAUTH_USER_PASSWORD_V2
...
ISAKMP: Config payload REPLY
ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected
ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
```

Router is requesting the VPN client for User Authentication

Router is receiving the X-Auth Attributes from the VPN Client

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

65

IOS Debugs: Mode Configuration

Cisco.com

```
ISAKMP (0:10): checking request:
ISAKMP: IP4_ADDRESS
ISAKMP: IP4_NETMASK
ISAKMP: IP4_DNS
ISAKMP: IP4_NBNS
ISAKMP: ADDRESS_EXPIRY
ISAKMP: APPLICATION_VERSION
ISAKMP: UNKNOWN Unknown Attr: 0x7000
...
ISAKMP: Sending private address: 14.1.1.3
ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
ISAKMP: Sending IP4_DNS server address: 14.36.1.10
ISAKMP: Sending IP4_NBNS server address: 14.36.1.20
ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the
  address: 86395
ISAKMP: Sending APPLICATION_VERSION string: Cisco
  Internetwork OperatingSystem Software
IOS (tm) 7200 Software (C7200-IK9S-M), Version 12.2(8)T,
  RELEASE SOFTWARE (fc1)
ISAKMP: Unknown Attr: UNKNOWN (0x7000)
```

Received mode configuration request from the VPN client

Unknown Attr: is not an Error. It just means that pix does not support this mode-config attribute requested by the VPN client

Router is sending the Mode-Configuration back to the VPN client

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

66

IOS Debugs : Phase II Negotiation

Cisco.com

```
ISAKMP (0:11): Checking IPsec proposal 4
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP:   authenticator is HMAC-SHA
ISAKMP:   encaps is 1
ISAKMP:   SA life type in seconds
ISAKMP:   SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP (0:11): atts are acceptable.
...
ISAKMP (0:11): Creating IPsec SAs
  inbound SA from 172.18.124.96 to 14.36.100.101
  (proxy 14.1.1.4 to 14.36.100.101)
  has spi 0x962A493B and conn_id 2000 and flags 4
  lifetime of 2147483 seconds
  outbound SA from 14.36.100.101 to 172.18.124.96 (proxy
  14.36.100.101 to 14.1.1.4)
  has spi -2145675534 and conn_id 2001 and flags C
  lifetime of 2147483 seconds
```

Router is checking and validating the IPsec proposals

After validating the phase II, the IPsec SAs are created; One SA for inbound traffic and the other SA for the outbound traffic

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

67

Common Issues

Cisco.com

- VPN clients only propose DH group 2 and 5. Configure **DH group 2** on IOS or PIX
- Configure “isakmp identity hostname” if rsa-sig is used as an IKE authentication method.
- aaa authorization needs to be enabled on the router, so that router can accept/send mode-configuration attributes

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

68

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x client
- **PKI related Issues**
- NAT with IPsec
- Firewalling and IPsec
- MTU Issues
- GRE over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

69

Common Issues

Cisco.com

- **Issues in Certificates enrollment process**
 - Unable to query the servers
 - Incorrect CA identity
- **Issues in IKE authentication using rsa-sig**
 - Incorrect time settings
 - Choices of ISAKMP identity
 - CRL issues
- **Issues related to Certificates lifetime**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

70

Debugging Tools

Cisco.com

IOS

- debug crypto pki message
- debug crypto pki transaction

PIX

- debug crypto ca

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

71

Unable to Query the Servers

Cisco.com

- The CA and/or the RA server should be accessible (TCP/80) 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**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

72

Incorrect CA Identity

Cisco.com

- Find out correct enrollment URL from CA admin.
- Find out from CA admin if RA (registration authority) is used
- How many certificates should you get ?
 - **CA mode** (CA root cert, router identity cert)
 - **RA mode** (CA root cert, RA signature cert, RA encryption cert, router identity cert)

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

73

Commonly Used CA Identities

Cisco.com

```
crypto ca trustpoint SJKPI
  enrollment mode ra
  enrollment url http://171.69.89.126
  crl query ldap://171.69.89.126
```

Entrust CA

```
crypto ca trustpoint SJKPI
  enrollment mode ra
  enrollment url http://171.68.89.127/certsrv/mscep/mscep.dll
  crl query ldap://171.69.89.126
```

Microsoft CA

```
cry ca trustpoint SJKPI
  enrollment url http://testdriveIPsec.verisign.com
  crl option
```

Verisign testdrive

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

74

IKE authentication using RSA-sig

Cisco.com

- **Certificate verification during IKE negotiation**
 - The responder receives the ID payload, cert payload and signature payload from initiator.
 - The responder verifies if the initiator's ISAKMP identity in the ID payload matches the identity in the certificate.
 - CRL checking
 - Lifetime checking
 - Verify the integrity of the certificate using the public key
- **IKE Authentication**
 - Integrity check by recalculating hash in signature payload

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

75

Debug Highlight of IKE Authentication Using RSA-sig

Cisco.com

```
ISAKMP (0:1): processing ID payload. message ID = 0
ISAKMP (0:1): processing CERT payload. message ID = 0
ISAKMP (0:1): processing a CT_X509_SIGNATURE cert
CRYPTO_PKI: status = 0: poll CRL ldap search: server=171.69.89.126, base=CN
CRL1, OU = sjvpn, O = cisco, C = us, attribute=: scope=2, filter=cn=CRL1
CRYPTO_PKI: ldap_bind() succeeded.
CRYPTO_PKI: set CRL update timer with delay: 66494
CRYPTO_PKI: the current router time: 10:00:28 UTC Apr 18 2002
CRYPTO_PKI: the last CRL update time: 03:28:42 UTC Apr 18 2002
CRYPTO_PKI: the next CRL update time: 04:28:42 UTC Apr 19 2002
CRYPTO_PKI: transaction GetCRL completed
CRYPTO_PKI: Certificate verified, chain status= 1
ISAKMP (0:1): OU = sjvpn
ISAKMP (0:1): processing SIG payload. message ID = 0
ISAKMP (1): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn = 7204-2.sjvpn.com
ISAKMP (0:1): SA has been authenticated with 172.16.172.10
```

Certificate Validation

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

76

Issues in IKE Authentication Using RSA-sig—Incorrect Time Setting

Cisco.com

- Make sure that the clock on the local and remote routers falls in the validity lifetime of the certificates
- Compares “show clock” and the validity date in “show crypto ca cert”

```
..
00:05:47: ISAKMP (0:2): SA is doing RSA signature authentication using id
type ID_FQDN
00:05:47: ISAKMP (2): ID payload
      next-payload : 6
      type          : 2
      protocol      : 17
      port          : 500
      length        : 20
00:05:47: ISAKMP (2): Total payload length: 24
00:05:47: ISAKMP (0:2): Self certificate is invalid, aborting negotiation
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

77

Display Router's Certificates

```
7204-2#sh cry ca cert
```

Certificate

Status: Available

Certificate Serial Number: 3C9CC580

Certificate Usage: General Purpose

Issuer:

OU = sjvpn

O = cisco

C = us

Subject:

Name: 7204-2.sjvpn.com

OID.1.2.840.113549.1.9.2 =<16>
7204-2.sjvpn.com

OU = sjvpn

O = cisco

C = us

SubAltName
FQDN

Distinguished
Name (DN)

CRL Distribution Point:

CN = CRL1, OU = sjvpn, O = cisco, C = us

Validity Date:

start date: 19:29:42 UTC Mar 24 2002

end date: 19:59:42 UTC Mar 24 2003

Associated Trustpoint: SJPKI

CA Certificate

...

RA KeyEncipher Certificate

...

RA Signature Certificate

...

CDP

Cert
Lifetime

CA and RA
certificates

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

78

Choices of ISAKMP identities

Cisco.com

- Identification of the VPN devices in IKE negotiation Contained in ID payload
- Use **crypto isakmp identity <address | hostname | dn>** command to choose the identity of the router:
 - Address: IP address
 - hostname
 - DN: X.500 distinguished name

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

79

Issues in IKE Authentication Using RSA-sig—CRL Issues

Cisco.com

- Connectivity to CA/RA server is require all the time
- Use “crl query...” to complete CRL search info

CRL Distribution Point:

CN = CRL1, OU = sjvpn, O = cisco,
C = us

+

crl query ldap://171.69.89.126



CRYPTO_PKI: status = 0: poll CRL ldap search: server=171.69.89.126,
base=CN = CRL1, OU = sjvpn, O = cisco, C = us, attribute= :
scope=2, filter=cn=CRL1

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

80

Issues Related to Certificate Lifetime

Cisco.com

- Re-enrollment is required after router or PIX certificate expires
- In latest IOS release, use **auto reenrollment** feature to avoid human intervention

```
3640(config)#crypto ca trustpoint SJKPI
3640(ca-trustpoint)# enrollment url http://171.69.89.126
3640(ca-trustpoint)#enrollment mode ra
3640(ca-trustpoint)#crl query ldap://171.69.89.126
3640(ca-trustpoint)#serial-number none
3640(ca-trustpoint)#ip-address none
3640(ca-trustpoint)#password revokeme
3640(ca-trustpoint)#auto-enroll
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

81

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x Client
- PKI Related Issues
- **NAT With IPsec**
- Firewalling and IPsec
- MTU Issues
- GRE Over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

82

Common Problems

Cisco.com

- Bypassing NAT entries
- NAT in the middle of an IPsec tunnel

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

83

Bypassing NAT Entries

Cisco.com

- Bypassing dynamic NAT entries

```
ip nat inside source route-map nonat interface Ethernet1/0 overload
access list 150 deny ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access list 150 permit ip 10.1.2.0 0.0.0.255 any
route-map nonat permit 10
match address 150
```

- Static NAT entries can be bypassed using a loopback interface and policy routing
- Tools to debug this setup are:
 - show ip nat translation
 - debug ip nat
 - debug ip policy

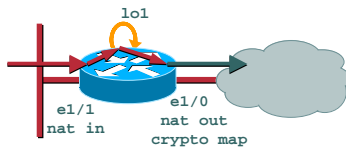
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

84

Bypassing Static NAT Entries

Cisco.com



```
crypto map test 10 IPsec-isakmp
set peer 172.16.172.10
set transform-set transform
match address 100
```

```
interface Loopback1
ip address 10.2.2.2 255.255.255.252
```

```
interface Ethernet1/0
ip address 172.16.172.20 255.255.255.0
ip nat outside
crypto map test
```

```
interface Ethernet1/1
ip address 10.1.2.1 255.255.255.0
ip nat inside
ip route-cache policy
ip policy route-map nonat
```

```
ip nat inside source list 1 interface Ethernet1/0 overload
ip nat inside source static 10.1.2.2 172.16.172.21
access list 1 permit 10.0.0.0 0.255.255.255
access list 100 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access list 120 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255
```

```
route-map nonat permit 10
match ip address 120
set ip next-hop 10.2.2.1
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

85

NAT in the Middle of an IPsec Tunnel

Cisco.com

- In many cases, VPN clients are behind NAT/PAT devices
- Currently, IOS and PIX have no solution
 - IPsec Over NAT will be supported in near future:
[draft-ietf-IPsec-udp-encaps-justification-00.txt](#)
 - IPsec pass-thru feature is supported on certain NAT/PAT devices. ISAKMP cookie and ESP SPI are used to build translation table.
- Turn on **IPsec Over UDP** or **IPsec Over TCP** feature in case of VPN 3000 concentrator

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

86

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x Client
- PKI Related Issues
- NAT With IPsec
- **Firewalling and IPsec**
- MTU Issues
- GRE Over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

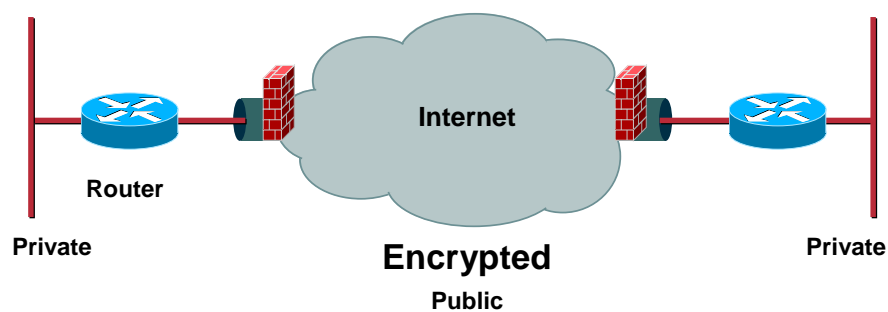
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

87

Firewall in the Middle

Cisco.com



- **ESP (IP protocol type 50) or/and AH (IP/51)**
- **UDP port 500 (ISAKMP)**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

88

Firewalling and IPsec

Cisco.com

- **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** (No conduit or access-list is needed)
 - **Use of conduits or access-list** (no sysopt connection permit-ipsec is needed – gives you more security for the decrypted pkts.)

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

89

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x Client
- PKI Related Issues
- NAT With IPsec
- Firewalling and IPsec
- **MTU Issues**
- GRE Over IPsec
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

90

IPsec MTU Issues

Cisco.com

- Overhead introduced by IPsec encapsulation (~60 bytes)
- Possible fragmentation after encryption leads to reassembly on the VPN peer router (process-switched, performance degradation)
- IPsec and Path MTU discovery (PMTU)
 - IPsec copies Don't Fragment (DF) bit from original data packets' IP header.
 - IPsec dynamically update Path MTU in the SADB if router receives PMTU ICMP message.
 - The MTU hint in the PMTU ICMP message is physical **MTU-ipsec_overhead** (calculated based on transform-set).

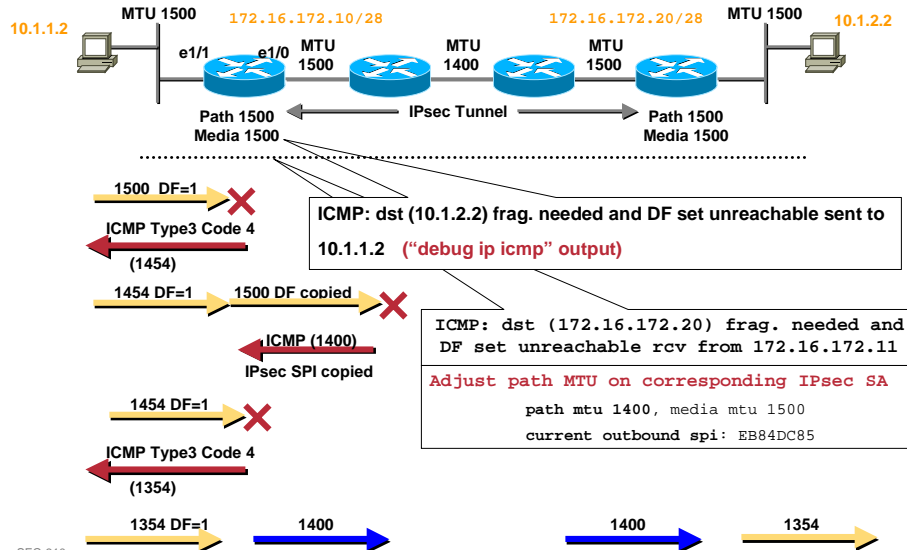
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

91

IPsec and PMTU

Cisco.com



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

92

Common Problem

Cisco.com

- **PMTU ICMP packets lost or blocked**
 - **Debug ip icmp** on router to verify if ICMP packets are sent or received
 - Use sniffer to verify if ICMP packets are lost
- **Workarounds**
 - Reduce MTU or disable PMTU on end host
 - configure router to clear DF bit of data packets
 - Adjust TCP MSS on router to fine tune TCP windows
 - Look-Ahead Fragmentation

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

93

MTU Issues Work Around: Policy Routing

Cisco.com

```
crypto map vpn 10 IPsec-isakmp
 set peer 172.16.172.10
 set transform-set myset
 match address 101
!
interface Ethernet1/0
 ip address 172.16.172.20 255.255.255.240
 no ip redirects
 duplex half
 crypto map vpn
!
interface Ethernet1/1
 ip address 10.1.2.1 255.255.255.0
 ip policy route-map ClearDF
 no ip redirects
 duplex half
```

```
route-map ClearDF permit 10
 match ip address 101
 set ip df 0
!
access-list 101 permit ip 10.1.2.0
0.0.0.255 10.1.1.0 0.0.0.255
```

Use policy routing to set DF bit of the interesting traffic to 0

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

94

MTU Issues Work Around: DF Bit Override Feature

Cisco.com

- DF bit Override feature with IPsec allows router to set, copy or clear the DF bit from the IPsec encapsulated header

Router(config)#**crypto ipsec df-bit clear**

- First introduced in 12.2(2)T
- Only works for IPsec tunnel mode
- With “**df-bit clear**” option, large packets will be fragmented after encryption

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

95

MTU Issues Work Around: Look Ahead Fragmentation

Cisco.com

- Fragment large packets **before** IPsec encryption to avoid performance issues
- Works for IPsec tunnel mode only
- Depends on **crypto ipsec df-bit** config
- First introduced in 12.1(11)E

```
Crypto ipsec df-bit clear  
Crypto ipsec fragmentation before-encryption
```

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

96

MTU Issues Work Around: Adjusting TCP MSS

Cisco.com

- Adjust TCP MSS (maximum send segment) under ingress interface:
`ip tcp adjust-mss <number>`
- Router will sniff on the incoming TCP SYN packets and tweak the TCP MSS field to configured number
- **Remote host** will use adjusted MSS value correspondingly
- Choose MSS to avoid fragmentation
 $MSS \leq \text{interface MTU} - \text{IPsec Overhead} - 40$
(IP header and TCP header)

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

97

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x client
- PKI related Issues
- NAT with IPsec
- Firewalling and IPsec
- MTU Issues
- GRE over IPsec*
- Loss of Connectivity of IPsec Peers
- Interoperability Troubleshooting

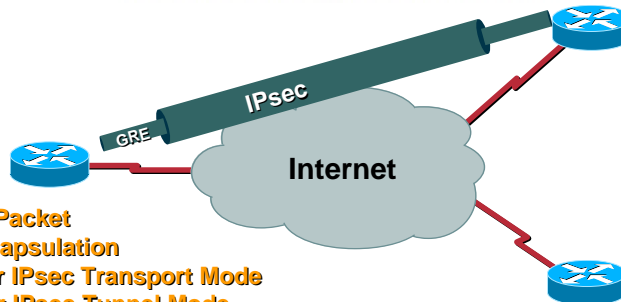
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

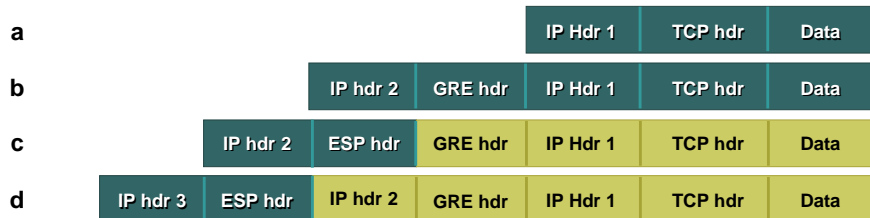
98

GRE Over IPsec

Cisco.com



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



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

99

GRE Over IPsec (Common Configuration Issues)

Cisco.com

- 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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

100

GRE Over IPsec (Avoid Recursive Routing)

Cisco.com

- **To avoid GRE tunnel interface flapping due to recursive routing, keep transport and passenger routing information 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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

101

GRE Over IPsec (MTU Issues)

Cisco.com

- **Overhead calculation of GRE over IPsec (assume ESP-DES and 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**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

102

GRE Over IPsec (MTU Issues)

Cisco.com

- 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

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

103

GRE Over IPsec (MTU Issues)

Cisco.com

- To avoid fragmentation and reassembly of IPsec packets:
 1. Set **ip mtu 1420** (GRE/IPsec tunnel mode), **ip mtu 1440** (GRE/IPsec transport mode) under tunnel interface
 2. Enable **“tunnel path-mtu-discovery”** (DF bit copied after GRE encapsulation) under tunnel interface
 3. Turn on **“Look-Ahead Fragmentation”** feature
- Use **“show ip int switching”** to verify switching path

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

104

GRE Over IPsec (MTU Issues)

Cisco.com

- Workarounds in case PMTU ICMP packets are lost or blocked

```
int tunnel 0
ip mtu 1500
```

- Incoming big size packets with DF=1 will not be dropped by GRE tunnel due to larger MTU setting
- The IPsec packets after GRE encapsulation (DF=0) will be fragmented before they leave the router
- Performance affects due to fragmentation

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

105

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x Client
- PKI Related Issues
- NAT With IPsec
- Firewalling and IPsec
- MTU Issues
- GRE Over IPsec
- **Loss of Connectivity of IPsec Peers**
- Interoperability Troubleshooting

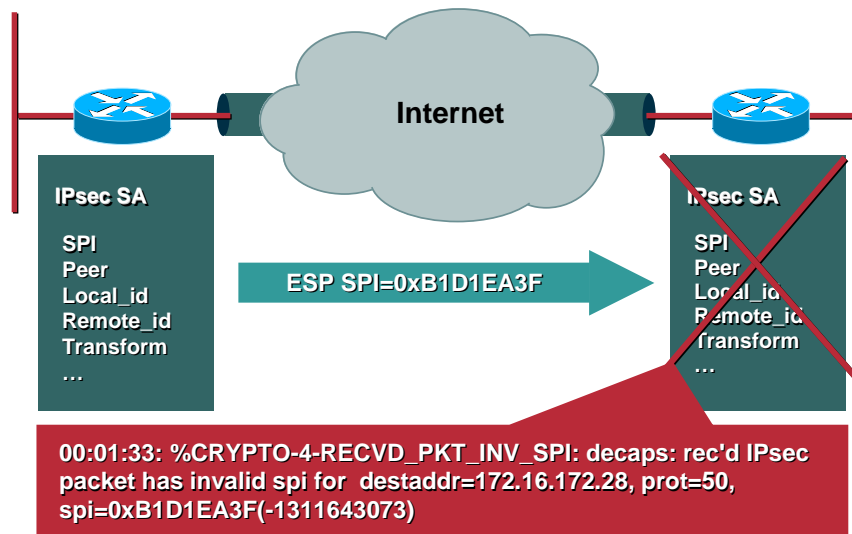
SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

106

Loss of Connectivity of IPsec Peers

Cisco.com



SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

107

Loss of Connectivity of IPsec Peers

Cisco.com

- 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
- In latest IOS and PIX versions, ISAKMP keepalives are replaced by **DPD (Dead peer detection)** for lower CPU overhead

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

108

Agenda

Cisco.com

- Introduction
- Router IPsec VPNs
- PIX IPsec VPNs
- Cisco VPN 3.x Client
- PKI Related Issues
- NAT With IPsec
- Firewalling and IPsec
- MTU Issues
- GRE Over IPsec
- Loss of Connectivity of IPsec Peers
- **Interoperability Troubleshooting**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

109

Interoperability Tips

Cisco.com

- **Start with configuring the two ends side by side with exact matching policies**

Phase I Parameters	Phase II Parameters
IKE authentication method	IPsec mode (tunnel or transport)
Hash algorithm	Encryption algorithm
DH group	Authentication algorithm
ISAKMP SA lifetime	PFS group
Encryption algorithm	IPsec SA Lifetime
Matching pre-shared secret	Interesting traffic definition

- **Turn off vendor specific features:
Mode config, Xauth, IKE keepalive**

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

110

Troubleshooting Resource—TAC Web

- **Field Notices**—alerts to critical issues
- **Security Advisories**—internet security issues and response procedures
- **TAC Technical Tips**—tips for troubleshooting; sample configurations

www.cisco.com/tac

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

111

Troubleshooting Resource—TAC Web

- **Task-based organization**
- **Overview**
- **Network design**
- **Implementation and configuration**
- **Verification and troubleshooting**
- **Operating and maintaining**
- **Documentation**

www.cisco.com/tac

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

112

Troubleshooting Resource—TAC Web

- Sample configurations
- Software upgrade procedures
- Links to additional resources
- ...and more

www.cisco.com/tac

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

113

Solutions | Products | Ordering | Support | Partners | Training | Corporate

Technical Assistance Center

Top Issues

Cisco Secure PIX Firewall

Home | What's New | How to Buy | Login | Profile | Feedback | Search | Map/Help

Technical Assistance Center > Top Issues > Cisco Secure PIX Firewall

Other PIX Firewall Resources

1. [Using nat, global, static, conduit and access-list Commands and Port Redirection on PIX](#)
2. [Upgrading Software for the Cisco Secure PIX Firewall](#)
3. [Password Recovery Procedure for PIX](#)
4. [Understanding the alias Command for the Cisco Secure PIX Firewall](#)
5. [Configuring Cisco Secure PIX Firewall 6.0 and Cisco VPN 3000 Clients Using IPSec](#)
6. [VPN Clients with Microsoft Routing Problems](#)
7. [Configuring the PIX Firewall and VPN Clients Using PPTP, MPPE and IPSec](#)
8. [Configuring and Troubleshooting the Cisco Secure PIX Firewall with a Single Internal Network](#)
9. [Configuring IPSec - Router to PIX Using the nat 0 access-list Command](#)
10. [Cisco Hardware and VPN Clients Supporting IPSec/PPTP/L2TP](#)
11. [Setting Up PIX Syslog](#)
12. [Unable to Display PIX Device Manager Page](#)
13. [Configuring a Simple PIX-to-PIX VPN Tunnel Using IPSec](#)

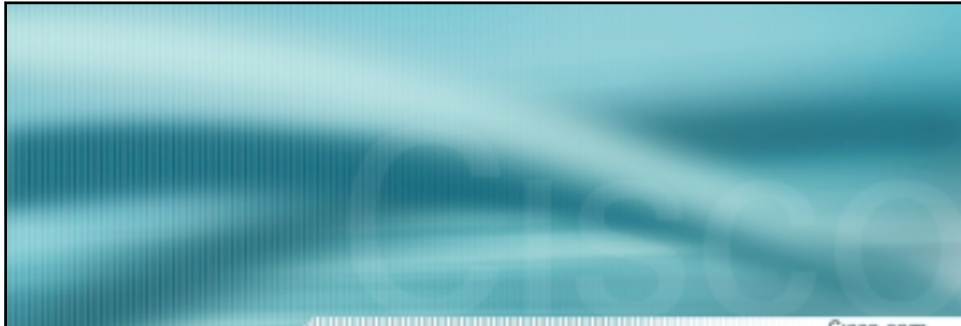
Troubleshooting the Implementation of IPsec VPNs

Session SEC-310

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

114



Cisco.com

Please Complete Your Evaluation Form

Session SEC-310

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

115

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION

SEC-310
5247_05_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

116