

LAN-to-LAN Tunnels on a VPN 3000 Concentrator With a PIX Firewall Configured for DHCP

Document ID: 46002

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Sample Debug Output

Related Information

Introduction

This document describes how to configure the Cisco VPN 3000 Concentrator Series to create IPsec tunnels dynamically with remote Cisco PIX Firewalls that use Dynamic Host Configuration Protocol (DHCP) to get IP addresses on their public interfaces. DHCP provides a mechanism for the allocation of IP addresses dynamically so that addresses can be reused when hosts no longer need them.

Refer to IPsec LAN-to-LAN Tunnel on a VPN 3000 Concentrator with a Cisco IOS® Router Configured for DHCP Configuration Example to configure the VPN 3000 Concentrator Series in order to create IPsec tunnels dynamically with remote VPN devices that receive dynamic IP addresses on their public interfaces.

Refer to Configuring an IPsec Router Dynamic LAN-to-LAN Peer and VPN Clients for more information on a LAN-to-LAN configuration between two routers in a hub-spoke environment.

Refer to IPsec Between a Static IOS Router and a Dynamic PIX/ASA 7.x with NAT Configuration Example for information on how to enable the PIX/ASA Security Appliance to accept dynamic IPsec connections from the IOS router.

Prerequisites

Requirements

The configuration in this document requires these conditions.

- The IP addresses on both the public and private interfaces of the VPN Concentrator are already assigned.
- You can ping the IP address of the VPN Concentrator from the Internet.

Components Used

The information in this document is based on these software and hardware versions.

- Cisco PIX Firewall version 6.1(1)
- Cisco VPN 3000 Concentrator Software version 4.0.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses these configurations.

- VPN 3000 Concentrator
- PIX Firewall

VPN 3000 Concentrator Configuration

This configuration sets the base group of the VPN Concentrator to accept a pre-shared key. In this instance, the PIX acts as the client. You cannot configure the VPN Concentrator for a LAN-to-LAN tunnel to this PIX because the address is assigned dynamically and is not always the same (and might not be known). For this reason, you can only use this configuration with the base group. Use Easy VPN in order to allow different client PIX Appliances to use different groups.

Note: As with all IPsec configurations, you must ensure that the policies match on both sides for Internet Security Association and Key Management Protocol (ISAKMP) and IPsec. The example in this document shows DES-MD5 for ISAKMP and IPsec. If you need to change these settings, ensure that you make the changes on both sides.

1. Choose **Configuration > Interfaces** and ensure that IP addresses are assigned.

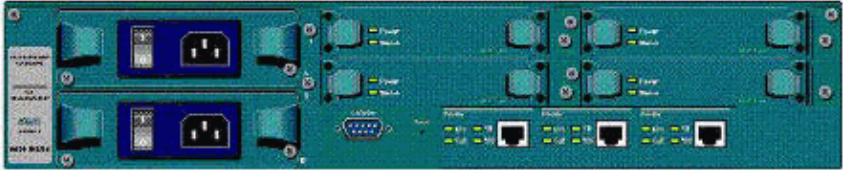
Configuration | Interfaces Thursday, 23 October 2003 13:47:45
Save Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	10.2.2.1	255.255.255.0	00.90.A4.00.1E.DC	
Ethernet 2 (Public)	UP	209.165.201.3	255.255.255.224	00.90.A4.00.1E.DD	209.165.201.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- Power Supplies



- Choose **Configuration > User Management > Base Group**. Go to the General tab and make sure that **IPSec** is selected as one of the tunneling protocols.

Configuration | User Management | Base Group

General | **IPSec** | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters		
Attribute	Value	Description
Access Hours	-No Restrictions-	Select the access hours for this group.
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	8	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
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	-None-	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply Cancel

- Select the IPSec tab and set these values.

- ◆ In the Default Preshared Key field, type in the pre-shared key that matches the key on the remote VPN device.
- ◆ Select the corresponding IPsec Security Association (SA) from the drop-down menu.
- ◆ Set the Authentication value to **None**.

Click **Apply** when you are finished.

This example shows a pre-shared key of "cisco123" and an IPsec SA value of ESP-DES-MD5.

Configuration User Management Base Group		
General IPsec Client Config Client FW HW Client PPTP/L2TP		
IPsec Parameters		
Attribute	Value	Description
IPsec SA	ESP-DES-MD5	Select the IPsec Security Association assigned to this group.
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	<input type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
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	<input type="checkbox"/>	Lock the users into this group.
Authentication	None	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
Authorization Type	None	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	Select the method of IP Compression for members of this group.
Default Preshared Key	cisco123	Enter the preshared key to be used with clients that do not support groups.
Reauthentication on Rekey	<input type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	<input type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Alliga/Cisco client is being used by members of this group.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

4. Choose **Configuration > System > Tunneling Protocols > IPsec > IKE Proposals** in order to confirm that the Internet Key Exchange (IKE) proposal you use appears in the list of active proposals.

This example shows an active proposal named IKE-DES-MD5.

Configuration System Tunneling Protocols IPsec IKE Proposals		
Add, delete, prioritize, and configure IKE Proposals.		
Select an Inactive Proposal and click Activate to make it Active , or click Modify , Copy or Delete as appropriate. Select an Active Proposal and click Deactivate to make it Inactive , or click Move Up or Move Down to change its priority. Click Add or Copy to add a new Inactive Proposal . IKE Proposals are used by Security Associations to specify IKE parameters.		
Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA	<input type="button" value="« Activate"/> <input type="button" value="Deactivate »"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA

5. Choose **Modify** in order to confirm that the ISAKMP policy matches that of the peer device, and then click **Apply**.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify

Modify a configured IKE Proposal.

Proposal Name Specify the name of this IKE Proposal.

Authentication Mode Select the authentication mode to use.

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the encryption algorithm to use.

Diffie-Hellman Group Select the Diffie Hellman Group to use.

Lifetime Measurement Select the lifetime measurement of the IKE keys.

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

6. Choose **Configuration > Policy Management > Traffic Management > Security Associations** in order to confirm that the selected IPsec SA is available and correct.

Configuration | Policy Management | Traffic Management | Security Associations

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs	Actions
ESP-3DES-MD5	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
ESP-3DES-MD5-DH5	
ESP-3DES-MD5-DH7	
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	

7. Select the IPsec SA, and then click **Modify** in order to confirm that the policy matches that of the peer.

Configuration Policy Management Traffic Management Security Associations Modify	
Modify a configured Security Association.	
SA Name <input type="text" value="ESP-DES-MD5"/>	Specify the name of this Security Association (SA).
Inheritance <input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters	
Authentication Algorithm <input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm <input type="text" value="DES-56"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode <input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy <input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement <input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime <input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime <input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters	
IKE Peer <input type="text" value="0.0.0.0"/>	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Negotiation Mode <input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate <input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal <input type="text" value="IKE-DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

PIX Firewall Configuration

Since the VPN Concentrator is configured for remote client access, the PIX is configured for LAN-to-LAN tunnels, as shown here.

PIX Firewall
<pre>sv2-11(config)#write terminal Building configuration... : Saved : PIX Version 6.3(3) interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto shutdown interface ethernet3 auto shutdown interface ethernet4 auto shutdown interface ethernet5 auto shutdown nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 intf2 security4 nameif ethernet3 intf3 security6 nameif ethernet4 intf4 security8 nameif ethernet5 intf5 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname sv2-11 domain-name cisco.com fixup protocol dns maximum-length 512 fixup protocol ftp 21 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719</pre>

```
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names

!--- Access list that defines what traffic is to be encrypted

access-list encrypt-acl permit ip 10.1.1.0 255.255.255.0
    10.2.2.0 255.255.255.0

!--- Access list that defines traffic that bypasses
!--- Network Address Translation (NAT)

access-list nonat-acl permit ip 10.1.1.0 255.255.255.0
    10.2.2.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500

!--- Outside address configured to receive the DHCP IP address

ip address outside dhcp
ip address inside 10.1.1.10 255.255.255.0
no ip address intf2
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
global (outside) 1 interface

!--- NAT bypass

nat (inside) 0 access-list nonat-acl
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 209.165.201.15 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
    rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
```

```

aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec

!--- Phase 2 IPsec policy

crypto ipsec transform-set aptset esp-des esp-md5-hmac
crypto map ozmap 10 ipsec-isakmp
crypto map ozmap 10 match address encrypt-acl
crypto map ozmap 10 set peer 209.165.201.3
crypto map ozmap 10 set transform-set aptset

!--- Enable IPsec on the outside interface.

crypto map ozmap interface outside
isakmp enable outside

!--- Phase 1 IPsec policy.

isakmp key ***** address 209.165.201.3 netmask 255.255.255.255
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
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:63353fba7fcfdf4127f7a933e6d55f0d
: end
[OK]

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto engine** Displays information related to encrypted and decrypted packets.
- **show crypto isakmp sa** Displays all current IKE SAs at a peer.
- **show crypto ipsec sa** Displays the settings used by current SAs.

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Refer to Troubleshooting the PIX to Pass Data Traffic on an Established IPsec Tunnel for additional information.

Sample Debug Output

This section provides sample debug output.

- PIX Debugs
- VPN 3000 Concentrator Debugs

Note: Before you issue **debug** commands, refer to Important Information on Debug Commands and IP Security Troubleshooting – Understanding and Using debug Commands.

PIX Debugs

```
lion(config)#
VPN Peer: ISAKMP: Added new peer: ip:203.1.1.1 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:203.1.1.1 Ref cnt incremented to:1
  Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (basic) of 1000
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using
  id type ID_FQDN
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a VPN3000 concentrator

ISAKMP (0): ID payload
  next-payload : 8
  type         : 2
  protocol     : 17
  port         : 500
  length      : 9
ISAKMP (0): Total payload length: 13
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange,
  M-ID of -67606134:fbf8698aIPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf382992d(4085422381) for SA
```

```
from      203.1.1.1 to      204.1.1.1 for prot 3

return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 203.1.1.1, dest 204.1.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 4227361162

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      encaps is 1
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
  proposal part #1,
  (key eng. msg.) dest= 203.1.1.1, src= 204.1.1.1,
  dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 4227361162

ISAKMP (0): processing ID payload. message ID = 4227361162
ISAKMP (0): processing ID payload. message ID = 4227361162
ISAKMP (0): Creating IPsec SAs
  inbound SA from 203.1.1.1 to 204.1.1.1
    (proxy 10.2.2.0 to 10.1.1.0)
  has spi 4085422381 and conn_id 1 and flags 4
  lifetime of 28800 seconds
  lifetime of 4608000 kilobytes
  outbound SA from 204.1.1.1 to 203.1.1.1
    (proxy 10.1.1.0 to 10.2.2.0)
  has spi 761912171 and conn_id 2 and flags 4
  lifetime of 28800 seconds
  lifetime of 4608000 kilobytesIPSEC(key_engine):
    got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 204.1.1.1, src= 203.1.1.1,
  dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 28800s and 4608000kb,
  spi= 0xf382992d(4085422381), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 204.1.1.1, dest= 203.1.1.1,
  src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 28800s and 4608000kb,
  spi= 0x2d69db6b(761912171), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:203.1.1.1 Ref cnt incremented to:2
  Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:203.1.1.1 Ref cnt incremented to:3
  Total VPN Peers:1
return status is IKMP_NO_ERROR
lion(config)#show crypto engine
```

```

Crypto Engine Connection Map:
  size = 8, free = 6, used = 2, active = 2
lion(config)#show crypto isakmp sa
Total      : 1
Embryonic  : 0
      dst      src      state      pending      created
      203.1.1.1  204.1.1.1  QM_IDLE    0             1
lion(config)#show crypto ipsec sa

interface: outside
  Crypto map tag: newmap, local addr. 204.1.1.1

local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
current_peer: 203.1.1.1
  PERMIT, flags={origin_is_acl,}
  #pkts encrypt: 8, #pkts decrypt: 8, #pkts digest 8
  #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 32, #recv errors 0

local crypto endpt.: 204.1.1.1, remote crypto endpt.: 203.1.1.1
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 2d69db6b

inbound esp sas:
  spi: 0xf382992d(4085422381)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 1, crypto map: newmap
  sa timing: remaining key lifetime (k/sec): (4607998/27548)
  IV size: 8 bytes
  replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x2d69db6b(761912171)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2, crypto map: newmap
  sa timing: remaining key lifetime (k/sec): (4607999/27548)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:

outbound pcp sas:

```

VPN 3000 Concentrator Debugs

```

1 02/12/2002 14:56:39.170 SEV=8 IKEDBG/0 RPT=199 204.1.1.1
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

3 02/12/2002 14:56:39.170 SEV=9 IKEDBG/0 RPT=200 204.1.1.1
processing SA payload

```

4 02/12/2002 14:56:39.170 SEV=7 IKEDBG/0 RPT=201 204.1.1.1
Oakley proposal is acceptable

5 02/12/2002 14:56:39.170 SEV=9 IKEDBG/0 RPT=202 204.1.1.1
processing IKE SA

6 02/12/2002 14:56:39.170 SEV=7 IKEDBG/28 RPT=9 204.1.1.1
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 1

7 02/12/2002 14:56:39.170 SEV=9 IKEDBG/0 RPT=203 204.1.1.1
constructing ISA_SA for isakmp

8 02/12/2002 14:56:39.170 SEV=8 IKEDBG/0 RPT=204 204.1.1.1
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

10 02/12/2002 14:56:39.390 SEV=8 IKEDBG/0 RPT=205 204.1.1.1
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) .
.. total length : 244

13 02/12/2002 14:56:39.390 SEV=8 IKEDBG/0 RPT=206 204.1.1.1
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) .
.. total length : 244

16 02/12/2002 14:56:39.390 SEV=9 IKEDBG/0 RPT=207 204.1.1.1
processing ke payload

17 02/12/2002 14:56:39.390 SEV=9 IKEDBG/0 RPT=208 204.1.1.1
processing ISA_KE

18 02/12/2002 14:56:39.390 SEV=9 IKEDBG/1 RPT=25 204.1.1.1
processing nonce payload

19 02/12/2002 14:56:39.390 SEV=9 IKEDBG/47 RPT=25 204.1.1.1
processing VID payload

20 02/12/2002 14:56:39.390 SEV=9 IKEDBG/49 RPT=17 204.1.1.1
Received Cisco Unity client VID

21 02/12/2002 14:56:39.390 SEV=9 IKEDBG/47 RPT=26 204.1.1.1
processing VID payload

22 02/12/2002 14:56:39.390 SEV=9 IKEDBG/49 RPT=18 204.1.1.1
Received DPD VID

23 02/12/2002 14:56:39.390 SEV=9 IKEDBG/47 RPT=27 204.1.1.1
processing VID payload

24 02/12/2002 14:56:39.390 SEV=9 IKEDBG/38 RPT=17 204.1.1.1
Processing IOS/PIX Vendor ID payload
(version: 1.0.0, capabilities: 00000025)

25 02/12/2002 14:56:39.420 SEV=9 IKEDBG/0 RPT=209 204.1.1.1
constructing ke payload

26 02/12/2002 14:56:39.420 SEV=9 IKEDBG/1 RPT=26 204.1.1.1
constructing nonce payload

27 02/12/2002 14:56:39.420 SEV=9 IKEDBG/46 RPT=25 204.1.1.1
constructing Cisco Unity VID payload

28 02/12/2002 14:56:39.420 SEV=9 IKEDBG/46 RPT=26 204.1.1.1
constructing xauth V6 VID payload

29 02/12/2002 14:56:39.420 SEV=9 IKEDBG/48 RPT=17 204.1.1.1
Send IOS VID

30 02/12/2002 14:56:39.420 SEV=9 IKEDBG/38 RPT=18 204.1.1.1
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

32 02/12/2002 14:56:39.420 SEV=9 IKEDBG/46 RPT=27 204.1.1.1
constructing VID payload

33 02/12/2002 14:56:39.420 SEV=9 IKEDBG/48 RPT=18 204.1.1.1
Send Altiga GW VID

34 02/12/2002 14:56:39.420 SEV=9 IKEDBG/0 RPT=210 204.1.1.1
Generating keys for Responder...

35 02/12/2002 14:56:39.420 SEV=6 IKE/139 RPT=9 204.1.1.1
Group 204.1.1.1 not found, using BASE GROUP default preshared key

36 02/12/2002 14:56:39.430 SEV=8 IKEDBG/0 RPT=211 204.1.1.1
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0)
... total length : 256

39 02/12/2002 14:56:40.000 SEV=8 IKEDBG/0 RPT=212 204.1.1.1
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 61

41 02/12/2002 14:56:40.000 SEV=9 IKEDBG/1 RPT=27 204.1.1.1
Group [VPNC_Base_Group]
Processing ID

42 02/12/2002 14:56:40.000 SEV=9 IKEDBG/0 RPT=213 204.1.1.1
Group [VPNC_Base_Group]
processing hash

43 02/12/2002 14:56:40.000 SEV=9 IKEDBG/0 RPT=214 204.1.1.1
Group [VPNC_Base_Group]
computing hash

44 02/12/2002 14:56:40.000 SEV=9 IKEDBG/23 RPT=9 204.1.1.1
Group [VPNC_Base_Group]
Starting group lookup for peer 204.1.1.1

45 02/12/2002 14:56:40.000 SEV=9 IKE/21 RPT=9 204.1.1.1
No Group found by matching IP Address of Cert peer 204.1.1.1

46 02/12/2002 14:56:40.000 SEV=9 IKE/0 RPT=9 204.1.1.1
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

48 02/12/2002 14:56:40.100 SEV=7 IKEDBG/0 RPT=215 204.1.1.1
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

49 02/12/2002 14:56:40.100 SEV=7 IKEDBG/14 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
Authentication configured for Internal

50 02/12/2002 14:56:40.100 SEV=9 IKEDBG/1 RPT=28 204.1.1.1
Group [VPNC_Base_Group]

constructing ID

51 02/12/2002 14:56:40.100 SEV=9 IKEDBG/0 RPT=216
Group [VPNC_Base_Group]
construct hash payload

52 02/12/2002 14:56:40.100 SEV=9 IKEDBG/0 RPT=217 204.1.1.1
Group [VPNC_Base_Group]
computing hash

53 02/12/2002 14:56:40.100 SEV=9 IKEDBG/34 RPT=1 204.1.1.1
Constructing IOS keep alive payload: proposal=32767/32767 sec.

54 02/12/2002 14:56:40.100 SEV=9 IKEDBG/46 RPT=28 204.1.1.1
Group [VPNC_Base_Group]
constructing dpd vid payload

55 02/12/2002 14:56:40.100 SEV=8 IKEDBG/0 RPT=218 204.1.1.1
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14)
+ VENDOR (13) + NONE (0)
... total length : 92

58 02/12/2002 14:56:40.100 SEV=4 IKE/119 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
PHASE 1 COMPLETED

59 02/12/2002 14:56:40.100 SEV=6 IKE/121 RPT=1 204.1.1.1
Keep-alive type for this connection: DPD

60 02/12/2002 14:56:40.100 SEV=7 IKEDBG/0 RPT=219 204.1.1.1
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 950000 (ms)

61 02/12/2002 14:56:40.100 SEV=4 AUTH/22 RPT=22
User Base Group connected

62 02/12/2002 14:56:40.670 SEV=8 IKEDBG/0 RPT=220 204.1.1.1
RECEIVED Message (msgid=fbf8698a) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5)
+ NOTIFY (11) + NONE (0)
... total length : 176

65 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=221 204.1.1.1
Group [VPNC_Base_Group]
processing hash

66 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=222 204.1.1.1
Group [VPNC_Base_Group]
processing SA payload

67 02/12/2002 14:56:40.670 SEV=9 IKEDBG/1 RPT=29 204.1.1.1
Group [VPNC_Base_Group]
processing nonce payload

68 02/12/2002 14:56:40.670 SEV=9 IKEDBG/1 RPT=30 204.1.1.1
Group [VPNC_Base_Group]
Processing ID

69 02/12/2002 14:56:40.670 SEV=5 IKE/35 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
Received remote IP Proxy Subnet data in ID Payload:
Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0

72 02/12/2002 14:56:40.670 SEV=9 IKEDBG/1 RPT=31 204.1.1.1
Group [VPNC_Base_Group]

Processing ID

73 02/12/2002 14:56:40.670 SEV=5 IKE/34 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
Received local IP Proxy Subnet data in ID Payload:
Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0

76 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=223 204.1.1.1
Group [VPNC_Base_Group]
Processing Notify payload

77 02/12/2002 14:56:40.670 SEV=8 IKEDBG/0 RPT=224
QM IsRekeyed old sa not found by addr

78 02/12/2002 14:56:40.670 SEV=5 IKE/66 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-DES-MD5

79 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=225 204.1.1.1
Group [VPNC_Base_Group]
processing IPSEC SA

80 02/12/2002 14:56:40.670 SEV=7 IKEDBG/27 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

81 02/12/2002 14:56:40.670 SEV=7 IKEDBG/0 RPT=226 204.1.1.1
Group [VPNC_Base_Group]
IKE: requesting SPI!

82 02/12/2002 14:56:40.670 SEV=6 IKE/0 RPT=10
MM received unexpected event EV_ACTIVATE_NEW_SA in state MM_ACTIVE

83 02/12/2002 14:56:40.670 SEV=9 IPSECDBG/6 RPT=1
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,
seq 1, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000,
encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetime 0,
lifetime1 708648, lifetime2 0, dsId 300

87 02/12/2002 14:56:40.670 SEV=9 IPSECDBG/1 RPT=1
Processing KEY_GETSPI msg!

88 02/12/2002 14:56:40.670 SEV=7 IPSECDBG/13 RPT=1
Reserved SPI 761912171

89 02/12/2002 14:56:40.670 SEV=8 IKEDBG/6 RPT=1
IKE got SPI from key engine: SPI = 0x2d69db6b

90 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=227 204.1.1.1
Group [VPNC_Base_Group]
oakley constructing quick mode

91 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=228 204.1.1.1
Group [VPNC_Base_Group]
constructing blank hash

92 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=229 204.1.1.1
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

93 02/12/2002 14:56:40.670 SEV=9 IKEDBG/1 RPT=32 204.1.1.1
Group [VPNC_Base_Group]
constructing ipsec nonce payload

94 02/12/2002 14:56:40.670 SEV=9 IKEDBG/1 RPT=33 204.1.1.1
Group [VPNC_Base_Group]

```
constructing proxy ID

95 02/12/2002 14:56:40.670 SEV=7 IKEDBG/0 RPT=230 204.1.1.1
Group [VPNC_Base_Group]
Transmitting Proxy Id:
  Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
  Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0

99 02/12/2002 14:56:40.670 SEV=9 IKEDBG/0 RPT=231 204.1.1.1
Group [VPNC_Base_Group]
constructing qm hash

100 02/12/2002 14:56:40.680 SEV=8 IKEDBG/0 RPT=232 204.1.1.1
SENDING Message (msgid=fbf8698a) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
+ ID (5) + NONE (0)
... total length : 164

103 02/12/2002 14:56:41.330 SEV=8 IKEDBG/0 RPT=233 204.1.1.1
RECEIVED Message (msgid=fbf8698a) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

105 02/12/2002 14:56:41.330 SEV=9 IKEDBG/0 RPT=234 204.1.1.1
Group [VPNC_Base_Group]
processing hash

106 02/12/2002 14:56:41.330 SEV=9 IKEDBG/0 RPT=235 204.1.1.1
Group [VPNC_Base_Group]
loading all IPSEC SAs

107 02/12/2002 14:56:41.330 SEV=9 IKEDBG/1 RPT=34 204.1.1.1
Group [VPNC_Base_Group]
Generating Quick Mode Key!

108 02/12/2002 14:56:41.330 SEV=9 IKEDBG/1 RPT=35 204.1.1.1
Group [VPNC_Base_Group]
Generating Quick Mode Key!

109 02/12/2002 14:56:41.330 SEV=7 IKEDBG/0 RPT=236 204.1.1.1
Group [VPNC_Base_Group]
Loading subnet:
  Dst: 10.2.2.0 mask: 255.255.255.0
  Src: 10.1.1.0 mask: 255.255.255.0

112 02/12/2002 14:56:41.330 SEV=4 IKE/49 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x2d69db6b, Outbound SPI = 0xf382992d

115 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 1, len 592, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi f382992d,
encrKeyLen 8, hashKeyLen 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0,
lifetime1 708648, lifetime2 0, dsId -378167296

119 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_ADD msg!

120 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/1 RPT=3
key_msghdr2secassoc(): Enter

121 02/12/2002 14:56:41.330 SEV=7 IPSECDBG/1 RPT=4
No USER filter configured

122 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/1 RPT=5
KeyProcessAdd: Enter
```

123 02/12/2002 14:56:41.330 SEV=8 IPSECDBG/1 RPT=6
KeyProcessAdd: Adding outbound SA

124 02/12/2002 14:56:41.330 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: src 10.2.2.0 mask 0.0.0.255, dst 10.1.1.0 mask 0.0.0.255

125 02/12/2002 14:56:41.330 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: FilterIpsecAddIkeSa success

126 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 3, len 312, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 2d69db6b,
encrKeyLen 8, hashKeyLen 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0,
lifetime1 708648, lifetime2 0, dsId -378167296

130 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/1 RPT=9
Processing KEY_UPDATE msg!

131 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/1 RPT=10
Update inbound SA addresses

132 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/1 RPT=11
key_msghdr2secassoc(): Enter

133 02/12/2002 14:56:41.330 SEV=7 IPSECDBG/1 RPT=12
No USER filter configured

134 02/12/2002 14:56:41.330 SEV=9 IPSECDBG/1 RPT=13
KeyProcessUpdate: Enter

135 02/12/2002 14:56:41.330 SEV=8 IPSECDBG/1 RPT=14
KeyProcessUpdate: success

136 02/12/2002 14:56:41.330 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD msg for SA: SPI = 0xf382992d

137 02/12/2002 14:56:41.330 SEV=8 IKEDBG/0 RPT=237
pitcher: rcv KEY_UPDATE, spi 0x2d69db6b

138 02/12/2002 14:56:41.330 SEV=4 IKE/120 RPT=1 204.1.1.1
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=fbf8698a)

139 02/12/2002 14:56:43.970 SEV=7 IPSECDBG/1 RPT=15
IPSec Inbound SA has received data!

140 02/12/2002 14:56:43.970 SEV=8 IKEDBG/0 RPT=238
pitcher: recv KEY_SA_ACTIVE spi 0x2d69db6b

141 02/12/2002 14:56:43.970 SEV=8 IKEDBG/0 RPT=239
KEY_SA_ACTIVE no old rekey centry found with new spi 0x2d69db6b,
mess_id 0x0

Related Information

- [Cisco VPN 3000 Series Concentrators Support Page](#)
- [Cisco VPN 3000 Client Support Page](#)
- [IPsec Negotiation/IKE Protocols Support Page](#)
- [PIX 500 Series Firewalls Support Page](#)
- [Documentation for PIX Firewall](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Requests for Comments \(RFCs\)](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 16, 2008

Document ID: 46002
