

IPsec LAN-to-LAN Tunnel on a VPN 3000 Concentrator with a Cisco IOS Router Configured for DHCP Configuration Example

Document ID: 5403

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- VPN 3000 Concentrator Configuration
- Remote Cisco IOS Router Configuration

Verify

Troubleshoot

- VPN Concentrator Debugs
- IOS Router Debugs

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how 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. Dynamic Host Configuration Protocol (DHCP) provides a mechanism in order to allocate IP addresses dynamically. This allows IP addresses to be reused when hosts no longer need them.

Refer to LAN-to-LAN Tunnels on a VPN 3000 Concentrator With a PIX Firewall Configured for DHCP to configure the Cisco VPN 3000 Concentrator Series to create IPsec tunnels dynamically with remote Cisco PIX Firewalls that use DHCP to get 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

This document assumes that you have already assigned the IP addresses on both the public and private interfaces and that you are able to ping the IP address of the remote VPN device.

Components Used

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

- Cisco IOS Software Release 12.4(8) (any Cisco IOS Software Release 12.1 or later works)
- Cisco VPN 3000 Concentrator software version 4.7.2.J (any version that starts from 3.1 or later works)
- Cisco 3600 Router

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.

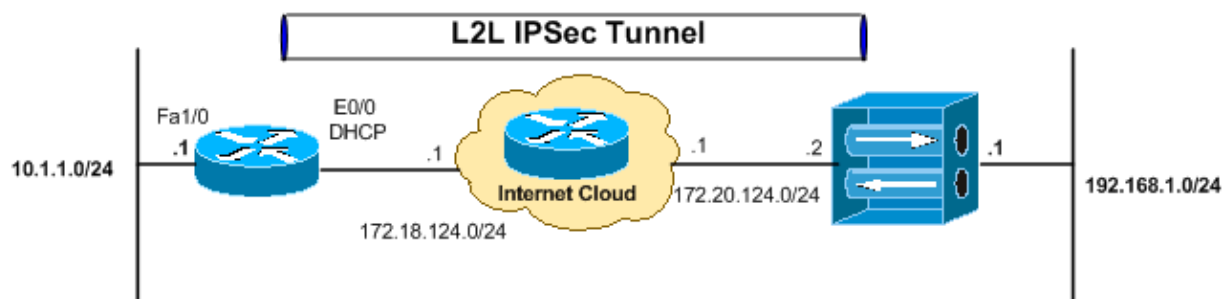
Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

This document uses these configurations.

- VPN 3000 Concentrator
- Remote Cisco IOS Router

Network Diagram

This document uses this network setup:



VPN 3000 Concentrator Configuration

Complete the procedure in this section in order to configure a Cisco VPN 3000 Concentrator for the parameters required for the IPsec connection.

In this lab setting, the VPN Concentrator is first accessed through the console port and a minimal configuration is added as this output shows:

```
Login: admin
```

```
!--- The password must be "admin".
```

Password:*****

 Welcome to
 Cisco Systems
 VPN 3000 Concentrator Series
 Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 1

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Tunneling and Security
- 6) Back

Config -> 1

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	DOWN	10.10.10.1/255.255.255.0	00.03.A0.89.BF.D0
Ether2-Pub	Not Configured	0.0.0.0/0.0.0.0	
Ether3-Ext	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies
- 5) Back

Interfaces -> 1

- 1) Interface Setting (Disable, DHCP or Static IP)
- 2) Set Public Interface
- 3) Select IP Filter
- 4) Select Ethernet Speed
- 5) Select Duplex
- 6) Set MTU
- 7) Set Port Routing Config
- 8) Set Bandwidth Management
- 9) Set Public Interface IPSec Fragmentation Policy
- 10) Set Interface WebVPN Parameters
- 11) Back

Ethernet Interface 1 -> 1

- 1) Disable
- 2) Enable using DHCP Client
- 3) Enable using Static IP Addressing

Ethernet Interface 1 -> [] 3

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	DOWN	10.10.10.1/255.255.255.0	00.03.A0.89.BF.D0
Ether2-Pub	Not Configured	0.0.0.0/0.0.0.0	
Ether3-Ext	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

> Enter IP Address

Ethernet Interface 1 -> [10.10.10.1] 192.168.1.1

20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3
IP Interface 1 status changed to Link Down.

21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3
IP Interface 1 status changed to Link Up.

22 02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4
IP Interface 1 status changed to Link Up.
>Enter Subnet Mask

23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4
IP Interface 1 status changed to Link Down.

Ethernet Interface 1 -> [255.255.255.0]

- 1) Interface Setting (Disable, DHCP or Static IP)
- 2) Set Public Interface
- 3) Select IP Filter
- 4) Select Ethernet Speed
- 5) Select Duplex
- 6) Set MTU
- 7) Set Port Routing Config
- 8) Set Bandwidth Management
- 9) Set Public Interface IPSec Fragmentation Policy
- 10) Set Interface WebVPN Parameters
- 11) Back

Ethernet Interface 1 -> 11

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	Up	192.168.1.1/255.255.255.0	00.03.A0.89.BF.D0
Ether2-Pub	Not Configured	0.0.0.0/0.0.0.0	
Ether3-Ext	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies
- 5) Back

Interfaces ->

You can complete the remainder of the configuration through the GUI. The VPN Concentrator appears in Quick Configuration, and these items are configured.

- Time/Date
- Interfaces/Masks in **Configuration > Interfaces** (public=172.20.124.2/24, private=192.168.1.1/24)
- Default Gateway in **Configuration > System > IP routing > Default_Gateway** (172.20.124.1)

At this point, the VPN Concentrator is accessible through HTML from the inside network.

Note: Because the VPN Concentrator is managed from outside, you also have to select:

- **Configuration > Interfaces > 2. Public > Select IP Filter > 1. Private (Default)**
- **Administration > Access Rights > Access Control List > Add Manager Workstation** in order to add the IP address of the external manager

This is not necessary unless you manage the VPN Concentrator from outside.

1. Select **Configuration > Interfaces** and make sure that the IP addresses are assigned.


Configuration | Interfaces Tuesday, 20 Feb
Save Net

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	192.168.1.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	172.20.124.2	255.255.255.0	00.03.A0.89.BF.D1	
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](#)



2. Choose **Configuration > System > IP Routing > Default Gateways** in order to configure the Default (Internet) Gateway.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

3. Choose **Configuration > User Management > Base Group**. On the General tab, make sure that **IPSec** is selected under the Tunneling Protocols section.

Configuration User Management Base Group		
General IPsec Client Config Client FW HW Client PPTP/L2TP WebVPN RAC		
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. When set to 0, WebVPN sessions use the Default Idle Timeout value specified in Configuration Tunneling and Security WebVPN HTTPS Proxy .
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 type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.

- On the IPsec tab, enter the preshared key. Your preshared key needs to match the preshared key on the remote VPN device. In this example, the preshared key is "cisco123", and the Phase 2 security association (SA) is ESP-DES-MD5. Select **Remote Access** for the Tunnel Type.

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 checked="" 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	Internal	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 checked="" 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 Altiga/Cisco client is being used by members of this group.

Apply Cancel

5. 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 Save Needed

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	

6. Select the IPSec SA and 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 Specify the name of this Security Association (SA).

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the ESP encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

Lifetime Measurement Select the lifetime measurement of the IPSec keys.

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

Time Lifetime Specify the time lifetime in seconds.

IKE Parameters

IKE Peer Specify the IKE Peer for a LAN-to-LAN IPSec connection.

Negotiation Mode Select the IKE Negotiation mode to use.

Digital Certificate Select the Digital Certificate to use.

Certificate Transmission Entire certificate chain
 Identity certificate only Choose how to send the digital certificate to the IKE peer.

IKE Proposal Select the IKE Proposal to use as IKE initiator.

Remote Cisco IOS Router Configuration

```

Router
Router#show running-config
Building configuration...

Current configuration : 1171 bytes
!
! Last configuration change at 16:03:26 UTC Tue Feb 20 2007
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!
!--- This defines the Phase 1 policy.

```

```

!--- This example uses encryption = DES, hashing = md5, and DH group = 1.

crypto isakmp policy 1
  hash md5
  authentication pre-share

!--- This is how you define the preshared key on the router.

crypto isakmp key cisco123 address 172.20.124.2
!
!

!--- This defines the Phase 2 policy.
!--- This example uses encryption = DES, hashing = md5, and mode = Tunnel.

crypto ipsec transform-set weak esp-des esp-md5-hmac
!

!--- Define a crypto map to be applied on the interface.

crypto map vpn 10 ipsec-isakmp
  set peer 172.20.124.2
  set transform-set weak
  match address 100
!
!
!
!
interface Ethernet0/0

!--- The interface dynamically learns its IP address.

ip address dhcp
  half-duplex

!--- Apply the crypto map on the interface.
!--- If the crypto map is not applied, then the crypto engine is not active.

crypto map vpn
!
interface FastEthernet1/0
  ip address 10.1.1.1 255.255.255.0
  duplex auto
  speed auto
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
!
!

!--- Access list used to define the interesting traffic for encryption.

access-list 100 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
control-plane
!
```

```
!--- Output is suppressed.
```

```
!  
!  
end
```

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.

Use these **show** commands in order to verify if the IPsec tunnel is successfully established from the router.

- **show crypto isakmp sa** Shows all current Internet Key Exchange (IKE) security associations (SAs) at a peer. The state QM_IDLE denotes that the SA remains authenticated with its peer and can be used for subsequent quick mode exchanges.

```
Router#show crypto isakmp sa  
dst          src          state          conn-id slot status  
172.20.124.2 172.18.124.3 QM_IDLE        2      0 ACTIVE
```

- **show crypto ipsec sa** Shows the Phase 2 SAs. It displays a detailed list of the active IPsec SA of the router.

```
Router#show crypto ipsec sa  
  
interface: Ethernet0/0  
  Crypto map tag: vpn, local addr 172.18.124.3  
  
protected vrf: (none)  
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)  
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)  
current_peer 172.20.124.2 port 500  
  PERMIT, flags={origin_is_acl,}  
  #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11  
  #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11  
  #pkts compressed: 0, #pkts decompressed: 0  
  #pkts not compressed: 0, #pkts compr. failed: 0  
  #pkts not decompressed: 0, #pkts decompress failed: 0  
  #send errors 29, #recv errors 0  
  
local crypto endpt.: 172.18.124.3, remote crypto endpt.: 172.20.124.2  
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0  
current outbound spi: 0x1B31309E(456208542)  
  
inbound esp sas:  
  spi: 0xD3DAF071(3554340977)  
  transform: esp-des esp-md5-hmac ,  
  in use settings ={Tunnel, }  
  conn id: 2002, flow_id: SW:2, crypto map: vpn  
  sa timing: remaining key lifetime (k/sec): (4547299/1960)  
  IV size: 8 bytes  
  replay detection support: Y  
  Status: ACTIVE  
  
inbound ah sas:  
  
inbound pcp sas:
```

```

outbound esp sas:
  spi: 0x1B31309E(456208542)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  conn id: 2001, flow_id: SW:1, crypto map: vpn
  sa timing: remaining key lifetime (k/sec): (4547299/1959)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

```
outbound ah sas:
```

```
outbound pcg sas:
```

- **show crypto map** Shows the crypto maps configured on the router along with the details such as crypto access lists, transform sets, peers, and so forth.

```

Router#show crypto map
Crypto Map "vpn" 10 ipsec-isakmp
  Peer = 172.20.124.2
  Extended IP access list 100
    access-list 100 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
  Current peer: 172.20.124.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    weak,
  }
  Interfaces using crypto map vpn:
    Ethernet0/0

```

- **show crypto engine connections active** Shows the current active encrypted session connections for all crypto engines. Each connection ID is unique. The number of packets that are encrypted and decrypted are displayed in the last two columns.

```

Router#show crypto engine connections active

ID Interface      IP-Address      State  Algorithm      Encrypt  Decrypt
  4 Ethernet0/0    172.18.124.3   set    HMAC_MD5+DES_56_CB  0        0
2001 Ethernet0/0    172.18.124.3   set    DES+MD5        4        0
2002 Ethernet0/0    172.18.124.3   set    DES+MD5        0        4

```

Choose **Monitoring > Sessions** and select the Base group to verify the IPsec tunnel on the VPN Concentrator.

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Weighted Active Load	Percent Session Load	Concurrent Sessions Limit	Total Cumulative Sessions
0	1	1	2	2	1	1.00%	100	11

NAC Session Summary

Accepted		Rejected		Exempted		Non-responsive		Hold-off		N/A	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	0	0

LAN-to-LAN Sessions

[[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions

[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
Base Group	10.1.1.0 172.18.124.3	Base Group	IPSec DES-56	Feb 20 15:32:21 0:17:41	N/A N/A	416 416	Unknown

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Sample **debug** output for this configuration is also shown.

- VPN Concentrator Debugs
- IOS Router Debugs

For additional information on troubleshooting IPsec debugs, refer to [IP Security Troubleshooting – Understanding and Using debug Commands](#).

Note: Refer to [Important Information on Debug Commands](#) before you issue **debug** commands.

VPN Concentrator Debugs

Choose **Monitoring > Filterable Event Log** in order to enable the debugs as shown.

- IKE Severity to log = 1–13
- IKEDBG Severity to log = 1–13
- IPSEC Severity to log = 1–13
- IPSECDBG Severity to log = 1–13

Choose **Monitoring > Live Event Log** in order to view the debugs on IKE/IPsec negotiations.



IOS Router Debugs

- **debug crypto isakmp** Displays the ISAKMP negotiations of IKE Phase 1.

```

Router#debug crypto isakmp
Crypto ISAKMP debugging is on
Router#
Feb 20 16:49:19.179: ISAKMP: received ke message (1/1)
Feb 20 16:49:19.183: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
Feb 20 16:49:19.183: ISAKMP: Created a peer struct for 172.20.124.2,
peer port 500
Feb 20 16:49:19.183: ISAKMP: New peer created peer = 0x64CF4F68
peer_handle = 0x80000010
Feb 20 16:49:19.183: ISAKMP: Locking peer struct 0x64CF4F68,
IKE refcount 1 for isakmp_initiator
Feb 20 16:49:19.183: ISAKMP: local port 500, remote port 500
Feb 20 16:49:19.183: ISAKMP: set new node 0 to QM_IDLE
Feb 20 16:49:19.183: ISAKMP: Find a dup sa in the avl tree
during calling isadb_insert sa = 6483D390
Feb 20 16:49:19.183: ISAKMP:(0:0:N/A:0):Can not start Aggressive mode,
trying Main mode.
Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0):found peer pre-shared key
matching 172.20.124.2
Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-07 ID
Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-03 ID
Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-02 ID
Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0):Input = IKE_MSG_FROM_IPSEC,
IKE_SA_REQ_MM
Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0):Old State = IKE_READY
New State = IKE_I_MM1

Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0): beginning Main Mode exchange
Feb 20 16:49:19.187: ISAKMP:(0:0:N/A:0): sending packet to 172.20.124.2
my_port 500 peer_port 500 (I
) MM_NO_STATE
Feb 20 16:49:19.239: ISAKMP (0:0): received packet from 172.20.124.2
dport 500 sport 500 Global (I)
MM_NO_STATE
Feb 20 16:49:19.239: ISAKMP:(0:0:N/A:0):Input = IKE_MSG_FROM_PEER,

```

```
IKE_MM_EXCH
Feb 20 16:49:19.239: ISAKMP:(0:0:N/A:0):Old State = IKE_I_MM1
New State = IKE_I_MM2

Feb 20 16:49:19.243: ISAKMP:(0:0:N/A:0): processing SA payload. message ID = 0
Feb 20 16:49:19.243: ISAKMP:(0:0:N/A:0): processing vendor id payload
Feb 20 16:49:19.243: ISAKMP:(0:0:N/A:0): vendor ID seems Unity/DPD
but major 194 mismatch
Feb 20 16:49:19.243: ISAKMP:(0:0:N/A:0):found peer pre-shared key
matching 172.20.124.2
Feb 20 16:49:19.243: ISAKMP:(0:0:N/A:0): local preshared key found
Feb 20 16:49:19.243: ISAKMP : Scanning profiles for xauth ...
Feb 20 16:49:19.247: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 1
against priority 1 policy
Feb 20 16:49:19.247: ISAKMP:          encryption DES-CBC
Feb 20 16:49:19.247: ISAKMP:          hash MD5
Feb 20 16:49:19.247: ISAKMP:          default group 1
Feb 20 16:49:19.247: ISAKMP:          auth pre-share
Feb 20 16:49:19.247: ISAKMP:          life type in seconds
Feb 20 16:49:19.247: ISAKMP:          life duration (VPI) of  0x0 0x1 0x51 0x80
Feb 20 16:49:19.247: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
Feb 20 16:49:19.335: ISAKMP:(0:3:SW:1): processing vendor id payload
Feb 20 16:49:19.335: ISAKMP:(0:3:SW:1): vendor ID seems Unity/DPD
but major 194 mismatch
Feb 20 16:49:19.335: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Feb 20 16:49:19.335: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM2
New State = IKE_I_MM2

Feb 20 16:49:19.339: ISAKMP:(0:3:SW:1): sending packet to
172.20.124.2 my_port 500 peer_port 500 (I)
MM_SA_SETUP
Feb 20 16:49:19.339: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Feb 20 16:49:19.343: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM2
New State = IKE_I_MM3

Feb 20 16:49:19.399: ISAKMP (0:134217731): received packet from
172.20.124.2 dport 500 sport 500 Glo
bal (I) MM_SA_SETUP
Feb 20 16:49:19.399: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
Feb 20 16:49:19.399: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM3
New State = IKE_I_MM4

Feb 20 16:49:19.403: ISAKMP:(0:3:SW:1): processing KE payload.
message ID = 0
Feb 20 16:49:19.507: ISAKMP:(0:3:SW:1): processing NONCE payload.
message ID = 0
Feb 20 16:49:19.511: ISAKMP:(0:3:SW:1):found peer pre-shared key
matching 172.20.124.2
Feb 20 16:49:19.511: ISAKMP:(0:3:SW:1):SKEYID state generated
Feb 20 16:49:19.511: ISAKMP:(0:3:SW:1): processing vendor id payload
Feb 20 16:49:19.511: ISAKMP:(0:3:SW:1): vendor ID is Unity
Feb 20 16:49:19.511: ISAKMP:(0:3:SW:1): processing vendor id payload
Feb 20 16:49:19.511: ISAKMP:(0:3:SW:1): vendor ID seems Unity/DPD
but major 240 mismatch
Feb 20 16:49:19.515: ISAKMP:(0:3:SW:1): vendor ID is XAUTH
Feb 20 16:49:19.515: ISAKMP:(0:3:SW:1): processing vendor id payload
Feb 20 16:49:19.515: ISAKMP:(0:3:SW:1): speaking to another IOS box!
Feb 20 16:49:19.515: ISAKMP:(0:3:SW:1): processing vendor id payload
Feb 20 16:49:19.515: ISAKMP:(0:3:SW:1): vendor ID seems Unity/DPD
but major 4 mismatch
Feb 20 16:49:19.515: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Feb 20 16:49:19.515: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM4
```

New State = IKE_I_MM4

Feb 20 16:49:19.519: ISAKMP:(0:3:SW:1):Send initial contact
Feb 20 16:49:19.519: ISAKMP:(0:3:SW:1):SA is doing pre-shared
key authentication using id type ID_IP
V4_ADDR

Feb 20 16:49:19.519: ISAKMP (0:134217731): ID payload
next-payload : 8
type : 1
address : 172.18.124.3
protocol : 17
port : 500
length : 12

Feb 20 16:49:19.519: ISAKMP:(0:3:SW:1):Total payload length: 12
Feb 20 16:49:19.523: ISAKMP:(0:3:SW:1): sending packet to 172.20.124.2
my_port 500 peer_port 500 (I)
MM_KEY_EXCH

Feb 20 16:49:19.523: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Feb 20 16:49:19.523: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM4
New State = IKE_I_MM5

Feb 20 16:49:19.627: ISAKMP (0:134217731): received packet from
172.20.124.2 dport 500 sport 500 Glo
bal (I) MM_KEY_EXCH

Feb 20 16:49:19.631: ISAKMP:(0:3:SW:1): processing ID payload. message ID = 0
Feb 20 16:49:19.631: ISAKMP (0:134217731): ID payload
next-payload : 8
type : 1
address : 172.20.124.2
protocol : 17
port : 500
length : 12

Feb 20 16:49:19.631: ISAKMP:(0:3:SW:1):: peer matches *none* of the profiles
Feb 20 16:49:19.631: ISAKMP:(0:3:SW:1): processing HASH payload. message ID = 0
Feb 20 16:49:19.631: ISAKMP:received payload type 17
Feb 20 16:49:19.631: ISAKMP:(0:3:SW:1): processing vendor id payload
Feb 20 16:49:19.631: ISAKMP:(0:3:SW:1): vendor ID is DPD
Feb 20 16:49:19.635: ISAKMP:(0:3:SW:1):SA authentication status:
authenticated

Feb 20 16:49:19.635: ISAKMP:(0:3:SW:1):SA has been authenticated
with 172.20.124.2

Feb 20 16:49:19.635: ISAKMP: Trying to insert a peer
172.18.124.3/172.20.124.2/500/, and inserted s
uccessfully 64CF4F68.

Feb 20 16:49:19.635: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH

Feb 20 16:49:19.635: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM5
New State = IKE_I_MM6

Feb 20 16:49:19.639: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE

Feb 20 16:49:19.639: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM6
New State = IKE_I_MM6

Feb 20 16:49:19.639: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE

Feb 20 16:49:19.643: ISAKMP:(0:3:SW:1):Old State = IKE_I_MM6
New State = IKE_P1_COMPLETE

Feb 20 16:49:19.643: ISAKMP:(0:3:SW:1):beginning Quick Mode
exchange, M-ID of -1014048696

Feb 20 16:49:19.647: ISAKMP:(0:3:SW:1): sending packet to 172.20.124.2
my_port 500 peer_port 500 (I)

QM_IDLE

Feb 20 16:49:19.647: ISAKMP:(0:3:SW:1):Node -1014048696, Input =

```

IKE_MESG_INTERNAL, IKE_INIT_QM
Feb 20 16:49:19.651: ISAKMP:(0:3:SW:1):Old State = IKE_QM_READY
New State = IKE_QM_I_QM1
Feb 20 16:49:19.651: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
Feb 20 16:49:19.651: ISAKMP:(0:3:SW:1):Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE

Feb 20 16:49:19.667: ISAKMP (0:134217731): received packet from
172.20.124.2 dport 500 sport 500 Glo
bal (I) QM_IDLE
Feb 20 16:49:19.671: ISAKMP:(0:3:SW:1): processing HASH payload.
message ID = -1014048696
Feb 20 16:49:19.671: ISAKMP:(0:3:SW:1): processing SA payload.
message ID = -1014048696
Feb 20 16:49:19.671: ISAKMP:(0:3:SW:1):Checking IPsec proposal 1
Feb 20 16:49:19.671: ISAKMP: transform 1, ESP_DES
Feb 20 16:49:19.671: ISAKMP: attributes in transform:
Feb 20 16:49:19.671: ISAKMP: SA life type in seconds
Feb 20 16:49:19.671: ISAKMP: SA life duration (basic) of 3600
Feb 20 16:49:19.671: ISAKMP: SA life type in kilobytes
Feb 20 16:49:19.671: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
Feb 20 16:49:19.671: ISAKMP: encaps is 1 (Tunnel)
Feb 20 16:49:19.671: ISAKMP: authenticator is HMAC-MD5
Feb 20 16:49:19.675: ISAKMP:(0:3:SW:1):atts are acceptable.
Feb 20 16:49:19.675: ISAKMP:(0:3:SW:1): processing NONCE payload.
message ID = -1014048696
Feb 20 16:49:19.675: ISAKMP:(0:3:SW:1): processing ID payload.
message ID = -1014048696
Feb 20 16:49:19.675: ISAKMP:(0:3:SW:1): processing ID payload.
message ID = -1014048696
Feb 20 16:49:19.679: ISAKMP: Locking peer struct 0x64CF4F68,
IPSEC refcount 1 for for stuff_ke
Feb 20 16:49:19.679: ISAKMP:(0:3:SW:1): Creating IPsec SAs
Feb 20 16:49:19.679: inbound SA from 172.20.124.2 to
172.18.124.3 (f/i) 0/ 0
(proxy 192.168.1.0 to 10.1.1.0)
Feb 20 16:49:19.679: has spi 0xE1F91A82 and conn_id 0 and flags 2
Feb 20 16:49:19.679: lifetime of 3600 seconds
Feb 20 16:49:19.683: lifetime of 4608000 kilobytes
Feb 20 16:49:19.683: has client flags 0x0
Feb 20 16:49:19.683: outbound SA from 172.18.124.3 to
172.20.124.2 (f/i) 0/0
(proxy 10.1.1.0 to 192.168.1.0)
Feb 20 16:49:19.683: has spi 726409612 and conn_id 0 and flags A
Feb 20 16:49:19.683: lifetime of 3600 seconds
Feb 20 16:49:19.683: lifetime of 4608000 kilobytes
Feb 20 16:49:19.683: has client flags 0x0
Feb 20 16:49:19.683: ISAKMP:(0:3:SW:1): sending packet to 172.20.124.2
my_port 500 peer_port 500 (I)
QM_IDLE
Feb 20 16:49:19.683: ISAKMP:(0:3:SW:1):deleting node -1014048696
error FALSE reason "No Error"
Feb 20 16:49:19.687: ISAKMP:(0:3:SW:1):Node -1014048696, Input =
IKE_MESG_FROM_PEER, IKE_QM_EXCH
Feb 20 16:49:19.687: ISAKMP:(0:3:SW:1):Old State = IKE_QM_I_QM1
New State = IKE_QM_PHASE2_COMPLETE
Feb 20 16:49:19.687: ISAKMP: Locking peer struct 0x64CF4F68,
IPSEC refcount 2 for from create_transf
orms
Feb 20 16:49:19.687: ISAKMP: Unlocking IPSEC struct 0x64CF4F68
from create_transforms, count 1
Feb 20 16:49:34.971: ISAKMP:(0:2:SW:1):purging SA., sa=64A7B994,
delme=64A7B994

```

- **debug crypto ipsec** Displays the IPsec negotiations of IKE Phase 2.

```

Router#debug crypto ipsec
Crypto IPSEC debugging is on
Router#
Feb 20 16:50:38.663: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.18.124.3, remote= 172.20.124.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x44C4DBA4(1153751972), conn_id= 0, keysize= 0, flags= 0x400A
Feb 20 16:50:39.111: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.18.124.3, remote= 172.20.124.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
Feb 20 16:50:39.111: Crypto mapdb : proxy_match
  src addr      : 10.1.1.0
  dst addr      : 192.168.1.0
  protocol      : 0
  src port      : 0
  dst port      : 0
Feb 20 16:50:39.119: IPSEC(key_engine): got a queue event with 2
kei messages
Feb 20 16:50:39.119: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 172.18.124.3, remote= 172.20.124.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x44C4DBA4(1153751972), conn_id= 0, keysize= 0, flags= 0x2
Feb 20 16:50:39.119: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 172.18.124.3, remote= 172.20.124.2,
  local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
  remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x8387219(137916953), conn_id= 0, keysize= 0, flags= 0xA
Feb 20 16:50:39.123: Crypto mapdb : proxy_match
  src addr      : 10.1.1.0
  dst addr      : 192.168.1.0
  protocol      : 0
  src port      : 0
  dst port      : 0
Feb 20 16:50:39.123: IPSEC(crypto_ipsec_sa_find_ident_head):
reconnecting with the same proxies and
172.20.124.2
Feb 20 16:50:39.123: IPsec: Flow_switching Allocated flow for
sibling 80000005
Feb 20 16:50:39.123: IPSEC(policy_db_add_ident): src 10.1.1.0,
dest 192.168.1.0, dest_port 0

Feb 20 16:50:39.123: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.3, sa_proto= 50,
  sa_spi= 0x44C4DBA4(1153751972),
  sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2002
Feb 20 16:50:39.123: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.20.124.2, sa_proto= 50,
  sa_spi= 0x8387219(137916953),
  sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001

```

- **debug crypto engine** Displays information about the crypto engine that performs the encryption and decryption process.

```

Router#debug crypto engine
Feb 20 19:55:04.890: CryptoEngine0: generating alg parameter for connid 1

```

```
Feb 20 19:55:04.978: CRYPTO_ENGINE: Dh phase 1 status: 0
Feb 20 19:55:04.978: CRYPTO_ENGINE: Dh phase 1 status: OK
Feb 20 19:55:05.042: CryptoEngine0: generating alg parameter for connid 0
Feb 20 19:55:05.150: CryptoEngine0: create ISAKMP SKEYID for conn id 1
Feb 20 19:55:05.154: CryptoEngine0: generate hmac context for conn id 1
Feb 20 19:55:05.262: CryptoEngine0: generate hmac context for conn id 1
Feb 20 19:55:05.266: CryptoEngine0: clear dh number for conn id 1
Feb 20 19:55:05.270: CryptoEngine0: generate hmac context for conn id 1
Feb 20 19:55:05.290: CryptoEngine0: generate hmac context for conn id 1
Feb 20 19:55:05.294: CryptoEngine0: validate proposal request
Feb 20 19:55:05.294: CryptoEngine0: generate hmac context for conn id 1
Feb 20 19:55:05.298: crypto_engine: ipsec_key_create_by_keys
Feb 20 19:55:05.298: crypto_engine: ipsec_key_create_by_keys
```

Refer to IPsec Troubleshooting for more detailed information on the outputs.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [IP Security Troubleshooting – Understanding and Using debug Commands](#)
- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 21, 2007

Document ID: 5403
