

Configuring the Cisco VPN 3000 Concentrator to a Cisco Router

Document ID: 14102

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations
- VPN Concentrator Configuration

Verify

- On the Router
- On the VPN Concentrator

Troubleshoot

- On the Router
- Problem – Unable to Initiate the Tunnel
- PFS

Related Information

Introduction

This sample configuration shows how to connect a private network behind a router that runs Cisco IOS[®] software to a private network behind the Cisco VPN 3000 Concentrator. The devices on the networks know each other by their private addresses.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco 2611 router with Cisco IOS Software Release 12.3.(1)a

Note: Make sure that Cisco 2600 Series routers are installed with a crypto IPsec VPN IOS image that supports the VPN feature.

- Cisco VPN 3000 Concentrator with 4.0.1 B

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 Cisco Technical Tips Conventions for more information on document conventions.

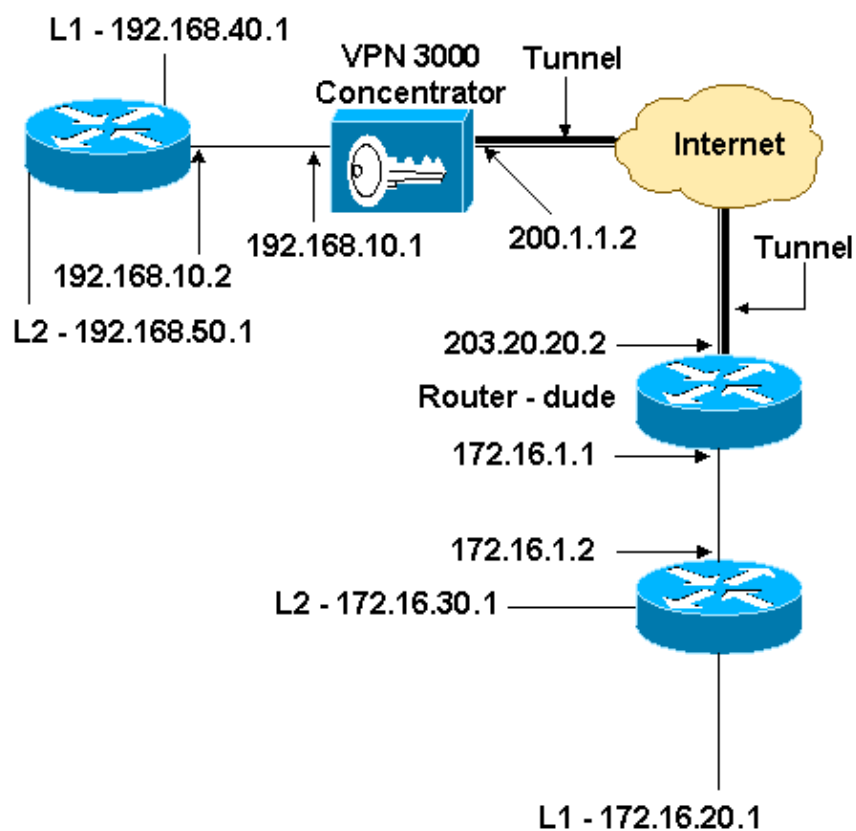
Configure

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 find more information on the commands used in this document.

Network Diagram

This document uses this network setup.



Configurations

This document uses this configuration.

Router Configuration
<pre>version 12.3 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname dude ! memory-size iomem 15 ip subnet-zero</pre>

```

!
ip audit notify log
ip audit po max-events 100
!
!--- IKE policies.

crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 200.1.1.2
!
!--- IPsec policies.

crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
  set peer 200.1.1.2
  set transform-set to_vpn

!--- Traffic to encrypt.

match address 101
!
interface Ethernet0/0
  ip address 203.20.20.2 255.255.255.0
  ip nat outside
  half-duplex
  crypto map to_vpn
!
interface Ethernet0/1
  ip address 172.16.1.1 255.255.255.0
  ip nat inside
  half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask 255.255.255.0
ip nat inside source route-map nonat pool mypool overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!
!--- Traffic to encrypt.

access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255

!--- Traffic to except from the NAT process.

access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255

```

```

access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end

```

VPN Concentrator Configuration

In this lab setting, the VPN Concentrator is first accessed through the console port and a minimal configuration is added so that the further configuration can be done through the graphical user interface (GUI).

Choose **Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration** to ensure that there is no existing configuration in the VPN Concentrator.

The VPN Concentrator appears in Quick Configuration, and these items are configured after the reboot:

- Time/Date
- Interfaces/Masks in **Configuration > Interfaces** (public=200.1.1.2/24, private=192.168.10.1/24)
- Default Gateway in **Configuration > System > IP routing > Default_Gateway** (200.1.1.1)

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** to add the IP address of the *external* manager.

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

1. Choose **Configuration > Interfaces** to recheck the interfaces after you bring up the GUI.

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
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** to configure the **Default (Internet) Gateway** and the **Tunnel Default (inside) Gateway** for IPsec to reach the other subnets in

the private network.

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 > Policy Management > Network Lists** to create the network lists that define the traffic to be encrypted.

These are the local networks:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

These are the remote networks:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

4. When completed, these are the two network lists:

Note: If the IPsec tunnel does not come up, check to see if the interesting traffic matches on both sides. The interesting traffic is defined by the access list on the router and PIX boxes. They are defined by network lists in the VPN Concentrators.

Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default) vpn_local_subnet router_subnet	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

5. Choose **Configuration > System > Tunneling Protocols > IPsec LAN-to-LAN** and define the LAN-to-LAN tunnel.

Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN | Add

Add a new IPsec LAN-to-LAN connection.

Enable Check to enable this LAN-to-LAN connection.

Name Enter the name for this LAN-to-LAN connection.

Interface Select the interface for this LAN-to-LAN connection.

Connection Type Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.

Peers Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.

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.

Preshared Key Enter the preshared key for this LAN-to-LAN connection.

Authentication Specify the packet authentication mechanism to use.

Encryption Specify the encryption mechanism to use.

IKE Proposal Select the IKE Proposal to use for this LAN-to-LAN connection.

Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.	
Network List <input type="text" value="vpn_local_subnet"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.	
Network List <input type="text" value="router_subnet"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	
<input type="button" value="Add"/>	<input type="button" value="Cancel"/>

6. After you click **Apply**, this window is displayed with the other configuration that is automatically created as a result of the LAN-to-LAN tunnel configuration.

Save Needed

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

Authentication Server Internal

Group 203.20.20.2

Security Association L2L: to_router

Filter Rules L2L: to_router Out
L2L: to_router In

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "L2L:" to indicate that they form a LAN-to-LAN configuration.

The previously created LAN-to-LAN IPsec parameters can be viewed or modified in **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN**.

Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN Save Needed

This section lets you configure IPsec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPsec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to [User Management](#) and configure a Group and User. To configure NAT over LAN-to-LAN, go to [LAN-to-LAN NAT Rules](#).

If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary [Network Lists](#) prior to creating the connection.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

(D) indicates a disabled LAN-to-LAN connection.

LAN-to-LAN Connection	Actions
to_router (203.20.20.2) on Ethernet 2 (Public)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

7. Choose **Configuration > System > Tunneling Protocols > IPsec > IKE Proposals** to confirm the active IKE Proposal.

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals Save Needed

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

8. Choose **Configuration > Policy Management > Traffic Management > Security Associations** to view the list of Security Associations.

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	
L2L: to_router	

9. Click the Security Association name, and then click **Modify** to verify the Security Associations.

SA Name	<input type="text" value="L2L: to_router"/>	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="3DES-168"/>	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		
Connection Type	Bidirectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	203.20.20.2	
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-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

Verify

This section lists the **show** commands used in this configuration.

On the Router

This section provides information you can use to confirm 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 ipsec sa** Shows the settings used by current Security Associations.

- **show crypto isakmp sa** Shows all current Internet Key Exchange Security Associations at a peer.
- **show crypto engine connection active** Shows the current active encrypted session connections for all crypto engines.

You can use the IOS Command Lookup Tool (registered customers only) to see more information about particular commands.

On the VPN Concentrator

Choose **Configuration > System > Events > Classes > Modify** to turn on logging. These options are available:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Severity to Log = 1–13

Severity to Console = 1–3

Select **Monitoring > Event Log** to retrieve the event log.

Troubleshoot

On the Router

Refer to Important Information on Debug Commands before you attempt any debug commands.

- **debug crypto engine** Displays the traffic that is encrypted.
- **debug crypto ipsec** Displays the IPsec negotiations of phase 2.
- **debug crypto isakmp** Displays the ISAKMP negotiations of phase 1.

Problem – Unable to Initiate the Tunnel

Error Message

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Solution

Complete this action in order to configure the desired number of simultaneous logins or set the simultaneous logins to 5 for this SA:

Go to **Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins** and change the number of logins to 5.

PFS

In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key. Either enable or disable PFS on both the tunnel peers. Otherwise, the LAN-to-LAN (L2L) IPsec tunnel is not established in routers.

In order to specify that IPsec should ask for PFS when new Security Associations are requested for this crypto map entry, or that IPsec requires PFS when it receives requests for new Security Associations, use the **set pfs** command in crypto map configuration mode. In order to specify that IPsec should not request PFS, use the **no** form of this command.

```
set pfs [group1 | group2]
no set pfs
```

For the **set pfs** command:

- *group1* Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when the new Diffie-Hellman exchange is performed.
- *group2* Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when the new Diffie-Hellman exchange is performed.

By default, PFS is not requested. If no group is specified with this command, *group1* is used as the default.

Example:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Refer to the Cisco IOS Security Command Reference for more information on the **set pfs** command.

Related Information

- [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)
 - [Cisco VPN 3000 Series Concentrators](#)
 - [Cisco VPN 3002 Hardware Clients](#)
 - [IPsec Negotiation/IKE Protocols](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[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: Mar 24, 2008

Document ID: 14102
