

# Configuring the Cisco VPN 5000 Concentrator and Implementing IPSec Main-Mode LAN-to-LAN VPN Connectivity

Document ID: 9352

---

**Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, please see the End-of-Sales Announcement.**

---

## **Introduction**

### **Prerequisites**

- Requirements
- Components Used
- Conventions

### **Basic Connectivity Configuration**

- Configuring Ethernet 1 Port
- Configuring the IPSec Gateway
- Configuring the IKE Policy

### **Main-Mode Site-to-Site Configuration**

- Configuring the Tunnel Partner Section
- Configuring the IP Section
- Configuring the Default Route (TCP/IP Route Table)

### **Finishing Up**

### **NetPro Discussion Forums – Featured Conversations**

### **Related Information**

---

## **Introduction**

This document explains the initial configuration of the Cisco VPN 5000 Concentrator and demonstrates how to connect to the network using IP and how to offer IPSec Main-Mode LAN-to-LAN VPN connectivity.

You can install the VPN Concentrator in either of two configurations, depending on where you connect it to the network in relation to a firewall. The VPN Concentrator has two Ethernet ports, one of which (Ethernet 1) only passes IPSec traffic. The other port (Ethernet 0) routes all IP traffic. If you plan to install the VPN Concentrator in parallel with the firewall, you must use both ports so that Ethernet 0 faces the protected LAN, and Ethernet 1 faces the Internet through the network's Internet gateway router. You can also install the VPN Concentrator behind the firewall on the protected LAN and connect it through the Ethernet 0 port, so that the IPSec traffic passing between the Internet and the concentrator is passed through the firewall.

## **Prerequisites**

### **Requirements**

There are no specific prerequisites for this document.

## Components Used

The information in this document is based on the Cisco VPN 5000 Concentrator.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Basic Connectivity Configuration

The easiest way to establish basic network connectivity is to connect a serial cable to the console port on the VPN Concentrator and use terminal software to configure the IP address on the Ethernet 0 port. After configuring the IP address on Ethernet 0 port, you can use Telnet to connect to the VPN Concentrator to complete the configuration. You can also generate a configuration file in an appropriate text editor, and send it to the VPN Concentrator using TFTP.

Using terminal software through the console port, you are initially prompted for a password. Use the password "letmein." After responding with the password, issue the **configure ip ethernet 0** command, responding to prompts with your system information. The sequence of prompts should look like the following example.

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
Section 'ip ethernet 0' not found in the config.
Do you want to add it to the config? y
Configure parameters in this section by entering:
<Keyword> = <Value>
To find a list of valid keywords and additional help enter "?"
*[ IP Ethernet 0 ]# ipaddress=192.168.233.1
*[ IP Ethernet 0 ]# subnetmask=255.255.255.0
*[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
*[ IP Ethernet 0 ]# mode=routed
*[ IP Ethernet 0 ]#
```

Now you are ready to configure the Ethernet 1 port.

## Configuring Ethernet 1 Port

The TCP/IP addressing information on the Ethernet 1 port is the external, Internet–routable TCP/IP address you assigned for the VPN Concentrator. Avoid using an address in the same TCP/IP network as Ethernet 0, as this will disable TCP/IP in the concentrator.

Enter the **configure ip ethernet 1** commands, responding to prompts with your system information. The sequence of prompts should look like the following example.

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
Section 'ip ethernet 1' not found in the config.
Do you want to add it to the config? y
Configure parameters in this section by entering:
<Keyword> = <Value>
To find a list of valid keywords and additional help enter "?"
*[ IP Ethernet 1 ]# ipaddress=206.45.55.1
*[ IP Ethernet 1 ]# subnetmask=255.255.255.0
*[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
*[ IP Ethernet 1 ]# mode=routed
```

```
*[ IP Ethernet 1 ]#
```

Now you need to configure the IPsec gateway.

## Configuring the IPsec Gateway

The IPsec gateway controls where the VPN Concentrator sends all the IPsec, or tunneled, traffic. This is independent of the default route you configure later. Start by entering the **configure general** command, responding to prompts with your system information. The sequence of prompts should look like the example shown below.

```
* IntraPort2+_A56CB700# configure general
  Section 'general' not found in the config.
  Do you want to add it to the config? y
  Configure parameters in this section by entering:
  =
  To find a list of valid keywords and additional help enter "?"
  *[ General ]# ipsecgateway=206.45.55.2
  *[ General ]# exit
  Leaving section editor.
* IntraPort2+_A56CB700#
```

**Note:** In releases 6.x and later, the **ipsecgateway** command has been changed to the **vpngateway** command.

Now let's configure the Internet Key Exchange (IKE) policy.

## Configuring the IKE Policy

The Internet Security Association Key Management Protocol (ISAKMP)/IKE parameters control how the VPN Concentrator and the client identify and authenticate each other to establish tunnel sessions. This initial negotiation is referred to as Phase 1. Phase 1 parameters are global to the device and aren't associated with a particular interface. Keywords recognized in this section are described below. Phase 1 negotiation parameters for LAN-to-LAN tunnels may be set in the [Tunnel Partner <Section ID>] section. Phase 2 IKE negotiation controls how the VPN Concentrator and the VPN Client handle individual tunnel sessions. Phase 2 IKE negotiation parameters for the VPN Concentrator and the VPN Client are set in the [VPN Group <Name>] device.

The syntax for IKE policy is as follows.

```
Protection = [ MD5_DES_G1 | MD5_DES_G2 | SHA_DES_G1 | SHA_DES_G2 ]
```

The protection keyword specifies a protection suite for the ISAKMP/IKE negotiation between the VPN Concentrator and VPN Client. This keyword may appear multiple times within this section, in which case the VPN Concentrator proposes all of the specified protection suites. The VPN Client accepts one of the options for the negotiation. The first piece of each option, MD5 (Message Digest 5), is the authentication algorithm used for the negotiation. SHA stands for Secure Hash Algorithm, which is considered to be more secure than MD5. The second piece of each option is the encryption algorithm. DES (Data Encryption Standard) uses a 56-bit key to scramble the data. The third piece of each option is the Diffie-Hellman group, used for key exchange. Because larger numbers are used by the Group 2 (G2) algorithm, it is more secure than Group 1 (G1).

To start the configuration, enter the **configure IKE policy** command, responding to the prompts with your system information. An example is shown below.

```
* IntraPort2+_A56CB700# configure IKE Policy
  Section 'IKE Policy' was not found in the config.
```

```

Do you want to add it to the config? y
Configure parameters in this section by entering:
<Keyword> = <Value>
To find a list of valid keywords and additional help enter "?"
*[ IKE Policy ] Protection = MD5_DES_G1
*[ IKE Policy ] exit
Leaving section editor.
* IntraPort2+_A56CB700#

```

Now that you have configured the basics, it is time to define the tunnel and IP communication parameters.

## Main-Mode Site-to-Site Configuration

To configure the VPN Concentrator to support LAN-to-LAN connections, you need to define the tunnel configuration, as well as the IP communication parameters to be used in the tunnel. You'll do this in two sections, the [Tunnel Partner VPN x] section, and the [IP VPN x] section. For any given site-to-site configuration, the x defined in these two sections must match, so that the tunnel configuration is properly associated with the protocol configuration.

Let's look at each of these sections in detail.

### Configuring the Tunnel Partner Section

In the tunnel partner section, you must define at least the following eight parameters.

- Transform
- Partner
- KeyManage
- SharedKey
- Mode
- LocalAccess
- Peer
- BindTo

#### Transform

The Transform keyword specifies the protection types and algorithms used for IKE client sessions. Each option associated with this parameter is a protection piece that specifies authentication and encryption parameters. The Transform parameter may appear multiple times within this section, in which case the VPN Concentrator proposes the specified protection pieces in the order they're parsed, until one is accepted by the client for use during the session. In most cases, only one Transform keyword is needed.

The options for the Transform keyword are as follows.

```

[ ESP(SHA,DES) | ESP(SHA,3DES) | ESP(MD5,DES) | ESP(MD5,3DES) | ESP(MD5) |
ESP(SHA) | AH(MD5) | AH(SHA) |AH(MD5)+ESP(DES) | AH(MD5)+ESP(3DES) |
AH(SHA)+ESP(DES) | AH(SHA)+ESP(3DES) ]

```

ESP stands for Encapsulating Security Payload and AH stands for Authentication Header. Both these headers are used to encrypt and authenticate packets. DES (Data Encryption Standard) uses a 56-bit key to scramble the data. 3DES uses three different keys and three applications of the DES algorithm to scramble the data. MD5 is the message-digest 5 hash algorithm. SHA is the Secure Hash Algorithm, which is considered to be somewhat more secure than MD5.

ESP(MD5,DES) is the default setting, and is recommended for most setups. ESP(MD5) and ESP(SHA) use

ESP to authenticate packets (with no encryption). AH(MD5) and AH(SHA) use AH to authenticate packets. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), and AH(SHA)+ESP(3DES) use AH to authenticate packets and ESP to encrypt packets.

## **Partner**

The Partner keyword defines the IP address of the other tunnel terminator in the tunnel partnership. This number must be a public, routable IP address with which the local VPN Concentrator can create an IPSec connection.

## **KeyManage**

The KeyManage keyword defines how the two VPN Concentrators in a tunnel partnership determine which device initiates the tunnel and what type of tunnel establishment procedure to follow. The options are Auto, Initiate, Respond, and Manual. You can use the first three options to configure IKE tunnels, and the Manual keyword to configure fixed-encryption tunnels. This document doesn't cover how to configure fixed-encryption tunnels. Auto specifies that the tunnel partner can both initiate and respond to tunnel setup requests. Initiate specifies that the tunnel partner only sends tunnel setup requests, it doesn't respond to them. Respond specifies that tunnel partner to responds to tunnel-setup requests, but never initiates them.

## **SharedKey**

The SharedKey keyword is used as the IKE shared secret. You must set the same SharedKey value on both tunnel partners.

## **Mode**

The Mode keyword defines the IKE negotiation protocol. The default setting is Aggressive, so to set the VPN Concentrator for interoperability mode, you must set the Mode keyword to Main.

## **LocalAccess**

LocalAccess defines IP numbers that can be accessed through the tunnel, from a host mask to a default route. The LocalProto keyword defines which IP protocol numbers can be accessed through the tunnel, such as ICMP(1), TCP(6), UDP(17), and so on. If you want to pass all IP numbers, then you should set LocalProto=0. LocalPort determines which port numbers can be reached through the tunnel. Both LocalProto and LocalPort default to 0, or all-access.

## **Peer**

The Peer keyword specifies which subnets are found through a tunnel. PeerProto specifies which protocols are allowed through the remote tunnel endpoint, and PeerPort sets which port numbers can be accessed at the other end of the tunnel.

## **BindTo**

BindTo specifies which Ethernet port terminates site-to-site connections. You should always set this parameter to Ethernet 1, except when the VPN Concentrator is running in single-port mode.

## **Configuring the Parameters**

To configure these parameters, enter the **configure Tunnel Partner VPN 1** command, responding to prompts with your system information.

The sequence of prompts should look like the example below.

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1
Section ?config Tunnel Partner VPN 1? not found in the config.
Do you want to add it to the config? y
Configure parameters in this section by entering:
=
To find a list of valid keywords and additional help enter "?"
*[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)
*[ Tunnel Partner VPN 1 ]# sharedkey=letmein
*[ Tunnel Partner VPN 1 ]# partner=208.203.136.10
*[ Tunnel Partner VPN 1 ]# mode=main
*[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8
*[ Tunnel Partner VPN 1 ]# localaccess=192.168.233.0/24
*[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1
*[ Tunnel Partner VPN 1 ]# exit
Leaving section editor.
```

Now it is time to configure the IP section.

## Configuring the IP Section

You can use numbered or unnumbered connections (as in IP configuration on WAN connections) in the IP configuration section of each tunnel partnership. Here, we used unnumbered.

The minimum configuration for an unnumbered site-to-site connection requires two statements: `numbered=false` and `mode=routed`. Start by entering the **configure ip vpn 1** commands, and respond to system prompts as follows.

```
*[ IP Ethernet 0 ]# configure ip vpn 1
Section ?IP VPN 1? not found in the config.
Do you want to add it to the config? y
Configure parameters in this section by entering:
<Keyword> = <Value>
To find a list of valid keywords and additional help enter "?"
*[ IP VPN 1 ]# mode=routed
*[ IP VPN 1 ]# numbered=false
```

Now it is time to set up a default route.

## Configuring the Default Route (TCP/IP Route Table)

You need to configure a default route that the VPN Concentrator can use to send all TCP/IP traffic destined for networks other than the network(s) to which it is directly connected, or for which it has dynamic routes. The default route points back to all networks found on the internal port. You already configured the Intraport to send IPSec traffic to and from the Internet using the IPSec Gateway parameter. To start the default route configuration, enter the edit config ip static command, responding to prompts with your system information. The sequence of prompts should look like the example below.

```
*IntraPort2+_A56CB700# edit config ip static
Section 'ip static' not found in the config.
Do you want to add it to the config? y
Configuration lines in this section have the following format:
<Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
Editing "[ IP Static ]"...
1: [ IP Static ]
End of buffer
Edit [ IP Static ]> append 1
Enter lines at the prompt. To terminate input, enter
a . on a line all by itself.
```

```

Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
Append> .
Edit [ IP Static ]> exit
Saving section...
Checking syntax...
Section checked successfully.
*IntraPort2+_A56CB700#

```

## Finishing Up

The last step is to save the configuration. When asked if you are sure that you want to download the configuration and restart the device, type **y** and press **Enter**. Don't turn off the VPN Concentrator during the boot process. After the concentrator has rebooted, users can connect using the concentrator's VPN Client software.

To save the configuration, enter the **save** command, as follows.

```

*IntraPort2+_A56CB700# save
Save configuration to flash and restart device? y

```

If you're connected to the VPN Concentrator using Telnet, the output above is all you'll see. If you're connected through a console, you'll see output similar to the following, only much longer. At the end of this output, the VPN Concentrator returns "Hello Console..." and asks for a password. This is how you know you are finished.

```

Codesize => 0 pfree => 462
Updating Config variables...
Adding section '[ General ]' to config
Adding -- ConfiguredFrom = Command Line, from Console
Adding -- ConfiguredOn = Timeserver not configured
Adding -- DeviceType = IntraPort2
Adding -- SoftwareVersion = IntraPort2 V4.5
Adding -- EthernetAddress = 00:00:a5:6c:b7:00
Not starting command loop: restart in progress.
Rewriting Flash....

```

## 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 Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

## Related Information

- [Cisco VPN 5000 Series Concentrators End-of-Sales Announcement](#)
- [Cisco VPN 5000 Concentrator Support Page](#)
- [Cisco VPN 5000 Client Support Page](#)
- [IPSec Support Page](#)

• **Technical Support – 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: Apr 04, 2008

Document ID: 9352

---