# Setting Up the Cisco VPN 5000 Concentrator Initially and for Remote Client Access

## Contents



## Introduction

This guide explains the initial configuration of the Cisco VPN 5000 Concentrator, specifically how to configure it to connect to the network using IP, and offer remote-client connectivity.

You can install the concentrator in either of two configurations, depending on where you connect it to the network in relation to a firewall. The 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 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 requirements for this document.

## Components Used

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

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

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 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 concentrator to complete the configuration. You can also generate a configuration file in an appropriate text editor, and send it to the 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 this:

```
*[ 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.

### 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 concentrator. Avoid using an address in the same TCP/IP network as Ethernet 0, as this will disable TCP/IP in the VPN Concentrator.

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

```
*[ 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 default route.

## Default Route

You need to configure a default route that the 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. Later, you'll configure 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 this:

```
*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#
```

Now you need to configure the IPSec Gateway.

## IPSec Gateway

The IPSec Gateway controls where the concentrator sends all the IPSec, or tunneled, traffic. This is independent of the default route you just configured. Start by entering the **configure general** command, responding to prompts with your system information. The sequence of prompts should look like this:

```
* 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#
```

Next, configure the IKE policy.

# IKE Policy

Set the Internet Security Association Key Management Protocol/Internet Key Exchange (ISAKMP/IKE) parameters for the concentrator. These settings control how the concentrator and the client identify and authenticate each other in order to establish tunnel sessions. This initial negotiation is referred to as Phase 1. Phase 1 parameters are global to the device and are not 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 client handle individual tunnel sessions. Phase 2 IKE negotiation parameters for the VPN Concentrator and 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 client. This keyword may appear multiple times within this section, in which case the concentrator proposes all of the specified protection suites. The client accepts one of the options for the negotiation. The first piece of each option, MD-5 (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.

```
* 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 the basics are configured, enter group parameters.

# VPN Group Configuration

When entering group parameters, remember that the VPN Group name should not contain spaces, even though the command-line parser allows you to enter spaces in the VPN Group name. The VPN Group name can contain letters, numbers, dashes, and underscores.

There are four basic parameters that are required in each VPN Group for IP operation:

- Maxconnections
- StartIPaddress or LocalIPNet
- Transform
- IPNet

The Maxconnections parameter is the maximum number of concurrent client sessions allowed in this particular VPN Group configuration. Keep this number in mind, as it works in conjunction with the StartIPAddress or LocalIPNet parameter.

The VPN Concentrator assigns IP addresses to remote clients by two different schemes, StartIPAddress and LocalIPNet. StartIPAddress assigns IP numbers from the subnet connected to Ethernet 0 and proxy-arps for the connected clients. LocalIPNet assigns IP numbers to remote clients from a subnet unique to the VPN clients, and requires that the rest of the network is made aware of the existence of the VPN subnet through static or dynamic routing. StartIPAddress offers easier configuration, but may limit the size of the address space. LocalIPNet offers greater flexibility of addressing for remote users, but requires slightly more work to configure the necessary routing.

For StartIPAddress, use the first IP address assigned to an incoming client tunnel session. In a basic configuration setup, this should be an IP address on the internal TCP/IP network (the same network as the Ethernet 0 port). In our example below, the first client session is assigned the 192.168.233.50 address, the next concurrent client session is assigned 192.168.233.51, and so on. We have assigned a Maxconnections value of 30, which means we need to have a block of 30 unused IP addresses (including DHCP servers if you have any) starting with 192.168.233.50 and ending with 192.168.233.79. Avoid overlapping the IP addresses used in different VPN Group configurations.

LocalIPNet assigns IP addresses to remote clients from a subnet that must be unused elsewhere on the LAN. For instance, if you specify the parameter "LocalIPNet=182.168.1.0/24" in the VPN group configuration, the concentrator assigns IP addresses to clients starting with 192.168.1.1. Therefore, you need to assign "Maxconnections=254", as the concentrator won't heed subnet boundaries when assigning IP numbers using LocalIPNet.

The Transform keyword specifies the protection types and algorithms which the concentrator uses for IKE client sessions. The options are as follows:

```
Transform = [ 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) ]
```

Each option is a protection piece that specifies authentication and encryption parameters. This keyword may appear multiple times within this section, in which case the concentrator proposes the specified protection pieces in the order they are parsed, until one is accepted by the client for use during the session. In most cases, only one Transform keyword is needed.

ESP(SHA,DES), ESP(SHA,3DES), ESP(MD5,DES), and ESP(MD5,3DES) denote the Encapsulating Security Payload (ESP) header 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, and 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 installations. ESP(MD5) and ESP(SHA) use the ESP header to authenticate packets with no encryption. AH(MD5) and AH(SHA) use the Authentication Header (AH) to authenticate packets. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), and AH(SHA)+ESP(3DES) use the Authentication Header to authenticate packets and the ESP header to encrypt packets.

**Note:** The Mac OS Client software doesn't support the AH option. You should specify at least one ESP option if you use the Mac OS Client software.

The IPNet field is important, since it controls where the concentrator clients can go. The values you enter in this field determine what TCP/IP traffic is tunneled, or more commonly, where a client who belongs to this VPN Group can go on your network.

Cisco recommends configuring the internal network (in this example 192.168.233.0/24), so all traffic from a client going to the internal network is sent through the tunnel, and therefore authenticated and encrypted (if you enable encryption). In this scenario, no other traffic is tunneled; instead, it's routed normally. You can have multiple entries, including single or host addresses. The format is the address (in our example, the network address 192.168.233.0) and then the mask associated with that address in bits (/24, which is a Class C mask).

Start this part of the configuration by entering the **configure VPN group basic-user** command, and then respond to the prompts with your system information. Here's an example of the entire configuration sequence:

```
*IntraPort2+_A56CB700# configure VPN group basic-user
      Section 'VPN Group basic-user' 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 "?"
      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
                                   or
      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24
      *[ VPN Group "basic-user" ]# maxconnections=30
      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)
      *[ VPN Group "basic-user" ]# ipnet=192.168.233.0/24
      *[ VPN Group "basic-user" ]# exit
      Leaving section editor.
      *IntraPort2_A51EB700#
```

The next step is to define the user's database.

# VPN User Configuration

In this section of the configuration, you define the VPN users database. Each line defines a VPN user along with that user's VPN Group configuration and password. Multi-line entries must have line breaks ending with a backslash. However, line breaks enclosed in a double quotation marks are preserved.

When a VPN client begins a tunnel session, the client's username is transmitted to the device. If the device finds the user in this section, it uses the information in the entry to set up the tunnel. (You can also use a RADIUS server for authentication of VPN users). If the device doesn't find the username, and you haven't configured a RADIUS server to perform the authentication, the tunnel

session isn't opened and an error is returned to the client.

Start the configuration by entering the **edit config VPN users** command. Let's look at an example that adds a user named "User1" to the VPN Group "basic-user".

```
*IntraPort2+_A56CB700# edit config VPN users
      Section 'VPN users' not found in the config.
      Do you want to add it to the config? y
      <Name> <Config> <SharedKey>
      Editing "[ VPN Users ]"...
      1: [ VPN Users ]
      End of buffer
      Edit [ VPN Users ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> User1 Config="basic-user" SharedKey="Burnt"
      Append> .
      Edit [ VPN Users ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

This user's SharedKey is "Burnt". All of these configuration values are case sensitive; if you configure "User1", the user must enter "User1" in the client software. Entering "user1" results in an invalid or unauthorized user error message. You can continue to enter users instead of exiting the editor, but remember, you must enter a period to exit the editor. Failure to do so can cause invalid entries in the configuration.

# Finishing Up

Your last step is saving the configuration. When asked if you are sure that you want to download the configuration and restart the device, type y and press the Enter key. Don't turn off the concentrator during the boot process. After the concentrator has rebooted, users can connect using the concentrator 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 are connected to the concentrator using Telnet, the output above is all you will see. If you are connected through a console, you will see output similar to the following, only much longer. At the end of this output, the 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....
```

## 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 & Documentation - Cisco Systems**