Release Notes for the Cisco VPN 5000 Manager Version 5.5.1

November 21, 2000

These release notes provide information about the VPN 5000 Manager Version 5.5.1. These release notes are updated as needed to describe caveats that were fixed from the previous releases, open caveats, and documentation updates.

Contents

Software Compatibility

- The Cisco VPN 5000 Manager is compatible with Cisco VPN 5000 concentrators running Version 5.x software only. Do not use VPN 5000 Manager Version 5.5.1 with a concentrator running Version 6.x software.

CISCO SYSTEMS

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

78-11133-02

New Features

The following sections list new features since the previous major release.

Table 1 VPN 5000 Software New Features

Feature	Description
Server-side certificates and certificate generation to support hybrid XAUTH authentication	Allows AXENT Defender, SecurID, and RADIUS to use hybrid XAUTH to authenticate clients.
No differentiation between supported numbers of client tunnels and LAN-to-LAN tunnels	Allows you to combine tunnels of any type to reach to the maximum number of tunnels supported.
LAN-to-LAN tunnel rekeying and perfect forward secrecy (PFS)	Increases the security of the tunnel through rekeying and PFS. PFS specifies that every time the concentrator computes encryption or authentication keys, it includes a new Diffie-Hellman Key Exchange. Rekeying forces the tunnel to periodically be reestablished with a new key. Both techniques greatly increase the difficulty of finding the session keys used to encrypt a VPN session.
LAN-to-LAN tunnel default responder	Allows you to configure a concentrator as a default responder to allow tunnels with any remote peer, without having to configure the concentrator for communication with each individual peer.
New or improved VPN management commands	• **show vpn** command provides extensive displays to help troubleshoot and maintain VPN tunnels. • **reset vpn** command terminates VPN tunnels. • **vpn cutoff** command stops new connections.

Hardware Supported

The following platforms are supported for VPN 5000 Manager version 5.5.1. The IntraPort servers are Compatible Systems legacy platforms.

- IntraPort 2
- IntraPort 2+
- IntraPort Carrier and Enterprise
- VPN 5001
- VPN 5002
- VPN 5008

Upgrading the IntraPort 2 and 2+ Servers

The IntraPort 2 and 2+ servers have the same functionality as the VPN 5001 concentrator except for the number of tunnels supported. Table 2 lists the tunnels supported for each platform.

Table 2 Tunnels Supported for the VPN 5001 and IntraPort 2 and 2+

Model	Tunnels
VPN 5001 concentrator	1500
IntraPort 2+	500
IntraPort 2	64

For information about configuring and upgrading the IntraPort 2 and 2+, use the information about the VPN 5001 concentrator in the *Cisco VPN 5000 Manager Software Reference Guide*.

Upgrading the IntraPort Carrier and Enterprise Servers

The IntraPort Carrier and Enterprise servers have the same functionality as the VPN 5002 or 5008 concentrators. For information about configuring the IntraPort Carrier and Enterprise servers, see the VPN 5002 and VPN 5008 information in the *Cisco VPN 5002 and 5008 Software Configuration Guide*. The Carrier and Enterprise servers use the same software build as the VPN 5002 and VPN 5008 concentrators.

You can upgrade the Carrier server according to the *Cisco VPN 5002 and 5008 Software Configuration Guide*. To upgrade the Enterprise server to the new version, follow these steps:

Note You only need to use this procedure the first time you upgrade an Enterprise server to Version 5.2.x or later. After you perform the upgrade, you can use the normal procedure to load software.

Step 1 As a precaution, save the configuration by using TFTP according to the *Cisco VPN 5002 and 5008 Software Configuration Guide.*

This procedure preserves and uses the configuration already in the concentrator. To copy the configuration back to the concentrator at the end of this procedure, copy it using the following file name:

vpn5002_8.cfg

Step 2 On the module in slot 0, attach a console to the console port.

Step 3 On the module in slot 0, set the test switch to position 3.

Step 4 Restart the concentrator.

Step 5 At the console prompt, enter:

setip *address mask* [*gateway*]

Where:

- *address* is the IP address of the port in slot 0.
- *mask* is the subnet mask.
- *gateway* is the default gateway.

Step 6 Set the test switch back to 0.

Step 7 Download the new vpn-5002-5008-*x.x.x*-[3]des.dld software using TFTP or the VPN 5000 Manager.

After you perform the download, the concentrator reboots using the new software. The software then propagates to the other cards in the chassis.

Cisco VPN 5000 Manager Caveats Fixed from Last Release

The following caveats were fixed from the last release, Compatible Systems CompatiView Version 5.4.x. CompatiView is now called the Cisco VPN 5000 Manager.

- CSCco909

  The manager no longer allows you to download a text file to the device using the **Download Software** command without checking to see if the file is a DLD file. Text files caused the device to boot from ROM. The manager now checks the file to see if it is a valid DLD file. If it is not valid, the manager prompts you to be sure before you download the file.

- CSCdr36708

  You are no longer required to restart the device when you use the **Write** command to write a modified configuration file. Restarting the device is now an option.

- CSCdr47718

  When you edit a VPN group on a VPN 5002 concentrator, the manager no longer puts in the line KeepAliveInterval = 60. The range for this device is 120 to 65535. The default has been changed to 120, and the range has been corrected.

- CSCdr48186

  If you change the IP Protocol Precedence section and save it to the device, the manager no longer adds a new IP Protocol Precedence section instead of changing the existing one.

- CSCdr53286

  The VPN 5000 Manager no longer freezes if you continuously enter the incorrect password for a device then click Cancel. The VPN 5000 Manager now allows you to abort if your device password fails multiple times.

Cisco VPN 5000 Manager Open Caveats

This section lists known issues with the VPN 5000 Manager software Version 5.5.x.

- CSCco675

  When you configure TCP/IP routing for a WAN port, you can exit the configuration window without entering subnet mask information, resulting in a partially-configured WAN.

  Workaround: Make sure you enter all the necessary configuration information, including subnet mask information.

- CSCdr47705

  The Cisco VPN 5000 manager puts some section headers into the configuration by default that are no longer correct.

  These errors appear in the boot sequence:

```
Flash Cfg: 238: Invalid section name: 'IP Bridge 0'
Flash Cfg: 250: Invalid section name: 'Bridging VPN 0:2'
Flash Cfg: 256: Invalid section name: 'AppleTalk VPN 2'
Flash Cfg: 265: Invalid section name: 'IPX Bridge 0:0'
Flash Cfg: 275: Invalid section name: 'Bridging VPN 0:2'
```

  Workaround: Manually correct the section names using the command line interface.

- CSCdr47732

  Multiple identical transforms are listed in the same VPN Group section. The Cisco VPN 5000 Manager allows you to add the same transform multiple times.

  Workaround: Edit the transforms out manually using the command line interface.

- CSCdr56193

  If you manage the concentrator from both the command line interface and the manager simultaneously, reloading the concentrator using the manager displays an exception error.

  Workaround: When you modify the concentrator configuration using the command line interface, delete the device from the manager database before reloading it using the manager.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com

Language	E-mail Address
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.