Release Notes for Cisco VPN 3002 Hardware Client Release 3.6.1

CCO Date: September 3, 2002

Note You can find the most current documentation for the Cisco VPN 3002 on CCO.

These release notes are for Cisco VPN 300Hardware Client Release 3.6.1 and Release 3.6 software. These release notes describe new features, limitations and restrictions, interoperability notes, and related documentation. They also list the caveats you should be aware of and the procedures you should follow before loading this release. Read these release notes carefully prior to installation.

Contents

These release notes include the following topics:

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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco VPN 3002 Hardware Client (referred to in these Release Notes as the VPN 3002) communicates with a VPN 3000 Series Concentrator to create a virtual private network across a TCP/IP network (such as the Internet). It can also establish IPSec connections to other IPSec security gateways, including the Cisco PIX firewall, and Cisco IOS routers. IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol.

The VPN 3002:

- Provides an alternative to deploying the VPN Client at remote locations.
- Is located at a remote site (like the VPN Client).
- Requires minimal configuration.

The secure connection between the VPN 3002 and the headend is called a *tunnel*. The VPN 3002 uses the IPSec protocol to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. It can support a single IP network.

The VPN 3002 Hardware Client provides an alternative to deploying the VPN Client software to PCs at remote locations. Like the software client, the VPN 3002 is located at a remote site, and provides a secure connection to an IPSec device at a central site. It is important to understand that the VPN 3002 is a hardware *client*, and that you configure it as a client, not as a site-to-site connection.

Installation Notes

For complete installation information, refer to the *VPN 3002 Hardware Client Getting Started* guide. To install and configure the VPN 3002 using default values, see the *VPN 3002 Quick Start* card, which ships with the VPN 3002.

Initial Configuration

You must meet the following requirements to configure the VPN 3002.

Central-site VPN Concentrator Requirements

To interoperate with a VPN 3002, the VPN 3000 Series Concentrator to which it connects must:

- Be running software version 3.0 or later. For most features new in software version 3.6.1, you must be running version 3.6.1 software on both the VPN 3002 and on the VPN Concentrator to which it connects.
- Configure IPSec group and user names and passwords for this VPN 3002.
- For a VPN 3002 running in PAT mode, enable a method of address assignment: DHCP, address pools, per user, or authentication server address.
- For a VPN 3002 running in Network Extension mode:
  - Use Reverse Route Injection, or configure on your central-site router a static route to the private network of the VPN 3002.
  - Check the box in the Allow Network Extension Mode parameter for the group (IPSec tab).

See Chapter 3, “Quick Configuration using the VPN 3002 Hardware Client Manager,” in the *VPN 3002 Hardware Client Getting Started* manual for step-by-step Quick Configuration instructions.

New Features

The following section describes software features new in Release 3.6.1 and 3.6.

H.323 in Client/PAT Mode

H.323 is the packet-based multimedia communications standard written by the ITU. A variety of applications use this standard to run real-time audio, video and data communications. This feature lets the Microsoft NetMeeting application operate behind the VPN 3002 hardware client in Client/PAT mode to communicate with a NetMeeting application at the central site or another VPN 3002 remote site. NetMeeting endpoints may register to Cisco H.323 Gatekeepers or Internet Listing Directory Services (ILS) through LDAP, which must be on the corporate or central site.

H.323 requires no configuration on either the VPN Concentrator or the VPN 3002.

Network Extension Mode per Group

A network administrator can now restrict the use of network extension mode. VPN 3002 hardware clients can use network extension mode only if, on the VPN Concentrator, you enable network extension mode on a group basis for VPN 3002 hardware clients.

Note If you disallow network extension mode, which is the default setting on the VPN Concentrator, the VPN 3002 can connect to that VPN Concentrator in PAT mode only. In this case, be careful that all VPN 3002s in the group are configured for PAT mode. If a VPN 3002 is configured to use network extension mode and the VPN Concentrator to which it connects disallows network extension mode, the VPN 3002 attempts to connect every 4 seconds, and every attempt is rejected; this is the equivalent of a denial of service attack.

IPSec over NAT-T

NAT Traversal (NAT-T) lets IPSec peers establish a connection through a NAT device. It does this by encapsulating IPSec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and encapsulates IPSec traffic only when necessary.

The VPN 3002 hardware client now supports NAT-T. It uses NAT-T by default, and requires no configuration. The VPN 3002 first attempts NAT-T, and then IPSec/UDP (if enabled) if a NAT device is not auto-detected, allowing IPSec traffic to pass through firewalls that disallow IPSec.

To use NAT-T you must:

- Open port 4500 on any firewall you have configured in front of a VPN 3002.
- Reconfigure any previous IPSec/UDP configuration using port 4500 to a different port.
- Select the second or third options for the Fragmentation Policy parameter in the Configuration | Interfaces | Public screen. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.

IPSec Fragmentation

The IPSec fragmentation policy specifies how to treat packets that exceed the MTU setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the VPN Concentrator and the VPN Client rejects or drops IP fragments. There are three options:

- Do not fragment prior to IP encapsulation; fragment prior to interface transmission
- Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)
- Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)

The fragmentation parameter is on the Configuration | Interfaces | Public screen.

MTU Interface Configuration

You can now configure the Maximum Transmission Unit (MTU) to be a value in the range from 68 through 1500 bytes. To configure the MTU, go to Configuration | Interfaces | Private/Public screens.

Online Technical Snapshot Explains PAT and Network Extension Modes

A new interactive multimedia piece explains the differences between Client (PAT) mode and Network Extension mode. To view it, go to this url:

http://www.cisco.com/mm/techsnap/VPN3002_techsnap.html

Your web browser must be equipped with a current version of the Macromedia Flash Player to view the content. If you are unsure whether your browser has the most recent version, you may want to download and install a free copy from:

http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash

Usage Notes

This section lists the issues to consider before installing Release 3.6.1 of the VPN 3002 Hardware Client software.

VPN 3002 Software

The following sections describe known behaviors and issues with VPN 3002 software.

Online Documentation and Adobe Acrobat 3.0.1

The online documentation might not be accessible when using Internet Explorer with Adobe Acrobat, Version 3.0.1. To resolve this issue, upgrade to Acrobat 4.0 or higher. The latest version of Adobe Acrobat is available at the Adobe web site: http://www.adobe.com.

Out of Sequence IP Addresses

The VPN 3002 DHCP server sometimes assigns addresses that are not in sequence, skipping addresses that are free for use (CSCdt38841).

Duplex Mode May Display Incorrectly

When the VPN 3002 is configured for 10 Mbps and the duplex mode is configured for auto, the duplex mode may be incorrectly displayed as half duplex even though it is running at full duplex (CSCdu57255).

SSL Certificate Requests Rejected Using ReKey Option

Using the rekey option to renew an SSL certificate from the RSA CA results in a rejection of the request.

The resubmit/renew feature does work with RSA as long as the certificate being rekeyed or renewed is first deleted from the CA database. RSA does not allow a CA to issue more than one certificate with any particular DN (CSCdv27743).

Network List Limits with Split Tunneling

If there are more than 150 networks in a network list used for split tunneling on the central site VPN Concentrator, when a VPN 3002 using this group connects to the VPN Concentrator and attempts to establish an SA to all of the networks within that network list, it may cause a reboot. We recommend that a network list that applies to a VPN 3002 contain 150 or fewer networks (CSCdv50669).

Inconsequential IPSec Event Display

With an active tunnel between a VPN 3002 and VPN Concentrator, occasionally the event `IPSec input - discarding packet with no NAT rule` displays. No negative operational issues have been observed (CSCdv69320).

Proxy Servers Incompatible with Individual User Authentication

When Netscape Navigator or Internet Explorer is configured for auto proxy configuration and you use the browser to try to log in as a user to the VPN 3002, the web redirect tries to set up the proxy settings for the browser. Proxy servers and Individual User Authentication are not compatible (CSCdw69363).

Configuration Error May Cause Denial of Service for Other VPN Clients

If a VPN 3002 cannot establish a tunnel to the central-site Concentrator, it keeps trying to connect. This can cause sufficient traffic to result in denial of service for other VPN clients during peak traffic hours. The probable cause is a configuration error. The workaround is to disconnect the VPN 3002 and correct the configuration (CSCdw77824).

DHCP Options Are Sent to the VPN 3002 Only if Requested

Configured VPN 3002 DHCP server options are sent to a DHCP client only if those options are specified in the Parameters Request List of the DHCPDISCOVER and DHCPREQUEST messages (CSCdy29626).

Some Data Is Not Tracked With Interactive Hardware Client Authentication and Individual User Authentication Enabled

If you are using an Accounting Server with Interactive Hardware Client Authentication and Individual User Authentication enabled, some session information specific to the level of data activity (number of octets and packets sent and received) back to the Accounting Server is not tracked (CSCdv82830).

Note This information *is* tracked if Interactive Hardware Client Authentication is not enabled.

VPN 3002 Using Digital Certificates Can Connect to PIX Devices Running Certain Versions of Code

When the VPN 3002 uses digital certificates to authenticate, it is unable to establish a connection to a PIX device unless the PIX device is running a version of code that corrects this problem. See PIX CSCdy05141 to determine which PIX releases include this correction (CSCdy05498).

Browser Issues

The following sections describe known behaviors and issues with Web browsers.

Internet Explorer 4.x Browser

The following are known issues with Internet Explorer 4.X and the VPN 3002 Hardware Client Manager (the HTML management interface). To avoid these problems, use the version of Internet Explorer on the Cisco VPN 3002 software distribution media.

- If you encounter a script error when you try to save your configuration file using Internet Explorer 4.0, reinstall Internet Explorer 4.0, or upgrade to a later version of Internet Explorer. Reinstalling Internet Explorer fixes the problem.
- If you plan to upgrade the firmware on multiple VPN Concentrators at the same time from the same PC, use the version of Internet Explorer on the Cisco VPN 3000 software distribution media or newer. Using an earlier version could cause a failure in one or more of the upgrades.

Secure Management Using SSL

When connecting to the VPN 3002 using SSL with Internet Explorer 4.0 (v4.72.2106.8), you might receive a message box saying, “This page contains both secure and non-secure items. Do you want to download the non-secure items?” Select Yes. There really are no *non-secure* items on the page and the problem is with Internet Explorer 4.0. If you upgrade to Internet Explorer 4.0 Service Pack 1 or Service Pack 2, you should not see this error message again.

After adding a new SSL certificate, you might have to restart the browser to use the new certificate.

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, select **Software & Support: Online Technical Support: Software Bug Toolkit** or navigate to http://www.cisco.com/support/bugtools.

Caveats Resolved in Release 3.6.1

Release 3.6.1 addresses multiple vulnerabilities for the VPN 3000 Series Concentrators and VPN 3002 Hardware Client. Please refer to the following URL for the details on the vulnerabilities addressed.

http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml

Open Caveats

The following problems exist with VPN 3002 Hardware Client, Release 3.6.1.

- CSCdw47278

  If the public interface uses PPPoE and the peer address is entered as a name rather than an IP address, DNS resolution fails; therefore the tunnel does not establish.

- CSCdy09539

  When the VPN 3002 obtains an IP address and DNS server attributes via PPPoE the VPN 3002 may fail to resolve DNS host names, causing the VPN 3002 PING utility to fail as well as IPSec VPN tunnels to fail to negotiate.

- CSCdv78999

  With split tunneling enabled, if a PC on the private interface of the VPN 3002 sends an ICMP Echo Request (PING) packet to the VPN 3002's IKE peer, that Echo Request packet travels unencrypted. The IKE peer sends the Echo Reply packet back to the VPN 3002 encrypted; therefore, the PING fails.

- CSCdv87793

  If the DHCP Server address pool on the VPN 3002 is modified, it still renews IP addresses from the previous address pool. To resolve this issue, reboot the VPN 3002 after modifying the IP address pool.

- CSCdx06212

  Users behind a VPN 3002 may have trouble accessing Active Directory shares or servers, especially if the VPN 3002 is behind a PAT device that does not handle fragmentation assembly properly. The workaround is to set up Kerberos to use TCP instead of UDP.

- CSCdx09099

  The VPN 3002 does not connect to the PIX when Perfect Forward Secrecy (Group 2) is set in the IPSec SA configuration on the PIX.

  The VPN 3002 does not clean up the peer SA after the failed attempt. It keeps trying to bring up the connection: IKE completes, the IPSec SA between the peers is attempted, but then fails. When the tunnel fails, the VPN 3002 does not delete it.

- CSCdx73959

  Packet authentication errors occur when the VPN 3002 is in network extension mode. Traffic passes normally.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

VPN 3002 Documentation

VPN 3002 documentation includes the following:

- The *VPN 3002 Hardware Client Getting Started* manual provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). This manual is online only.
- The *VPN 3002 Hardware Client Reference* provides details on all the functions available in the VPN 3002 Hardware Client Manager. This manual is online only.
- The HTML interface, called the VPN 3002 Hardware Client Manager, includes extensive context-sensitive online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.
- The *VPN 3002 Hardware Client Quick Start* card summarizes information for Quick Configuration. This quick reference card is provided with the VPN 3002, and is also available online. For easiest use, print it on 8 1/2” x 11” paper, in duplex mode. Current customers who obtain version 3.6 software from CCO can also order the 3.6 version of the card from CCO.
- The *VPN 3002 Hardware Client Basic Information* sticky label summarizes information for installing the VPN 3002 and beginning configuration. We suggest that you can affix the label to the VPN 3002 as a ready reference. You can also print a copy of the label from the online version. Current customers who obtain version 3.6 software from CCO can also order the 3.6 version of the label from CCO. When ordering the label, use product number CVPN3002-LABEL-31=.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- 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 and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

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, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com 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.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, 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 Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.