Release Notes for Cisco *VPN 3000 Series Concentrator, FIPS Release 3.1.3*

CCO March 19, 2002

Introduction

Note You can find the most current documentation for Cisco VPN 3000 products on CCO. These electronic documents might contain updates and changes made after the hard copy documents were printed.

These release notes are for Cisco VPN 3000 Series Concentrator FIPS Release, which is based on Release 3.1.3 software. These release notes describe limitations and restrictions, caveats, and related documentation. Read these release notes carefully prior to installation.

CISCO SYSTEMS

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

Contents

These release notes supplement the Security Policy document and describe the following topics:

System Requirements

This section describes the system requirements for FIPS release.

Hardware Supported

Cisco VPN 3000 Series Concentrator FIPS software release supports the following hardware platforms:

- Cisco VPN 3000 Series Concentrators, Models 3005 through 3080

Platform Files

FIPS Release contains two binary files, one for each of two platforms:

- Files beginning with `vpn3000`- support the VPN Concentrator 3015 through 3080 platforms.
- Files beginning with `vpn3005`- support the VPN Concentrator 3005 platform only.

Limitations and Restrictions

This section lists the issues you should know before installing this release of the VPN 3000 series products.

Online Documentation

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, which is available at the Adobe web site: http://www.adobe.com.

Browser Versions Required

The following versions of Netscape and Internet Explorer are the required versions for FIPS:

- Netscape version 6.1 or greater
- Internet Explorer 5.0 or greater with 128-bit cipher-strength

Certificates

This section describes known issues associated with specific PKI vendors and browsers. We list them to assist you in setting up the VPN Concentrator. For a complete list of supported certificate authorities (CAs), see the *VPN 3000 Series Concentrator Getting Started* manual.

Entrust Technologies PKI

To use the Entrust PKI, you must use the Entrust VPN Connector to enroll the VPN Concentrator and the Entrust Web connector to enroll the web browsers. If you are setting up the Entrust directory server and you want to implement CRL checking, use the binary option not the ASCII option. Cisco Systems does not support ASCII format for CRLs. If you have already set up the Entrust PKI to use ASCII, contact Entrust Technologies for help in converting to binary. Entrust can provide a step-by-step procedure to help you make this change easily.

Baltimore Technologies (UniCERT)

If using Baltimore Technologies for remote access, we recommend using UniCERT PKI Version 3.0.5 or later.

Verisign

The VPN Concentrator supports Verisign certificates. By default, Versign posts its CRL in HTTP format. For the VPN Concentrator to retrieve the CRL, it must be posted on an LDAP server.

OSPF Authentication

Cisco Systems supports an 8-character maximum in specifying a password for OSPF authentication (Configuration | Interfaces | Ethernet 1 2 3 OSPF tab).

VRRP

When a Cisco Catalyst switch uses Spanning-Tree Protocol (STP), the inherent delays with STP cause a delay in recognizing that a backup VPN Concentrator has taken over as the master in a VRRP scenario.

To reduce this delay to 15 seconds, you can enable Portfast on switches that use STP. To configure Portfast on Cisco switches, refer to the document: http://www.cisco.com/warp/customer/473/12.htm.

Password Maintenance

Be aware that there is no way to recover your system if you forget the Administrator password. Take appropriate measures to safeguard your password and remember it. If you forget the Administrator password, you cannot log in to your system and you will have to return the VPN Concentrator to be recovered.

Caveats for VPN 3000 Series Concentrator, FIPS Release 3.1.3

Caveats describe unexpected behavior or defects in Cisco software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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 Innovator II on CCO, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/support/bugtools.

Open Caveats

The following problems exist with the VPN 3000 Series Concentrator, FIPS Release 3.1.3.

- CSCal02854

  A VPN Concentrator running OSPF in which an OSPF area is assigned to the wrong interface might spontaneously reboot if another VPN Concentrator on the same area is rebooted following a configuration change. We have not yet identified the cause of this behavior.

- CSCdt08520

  IKE Diffie-Hellman Groups 1 and 7 are supported between the VPN 3000 Concentrator and the VPN 3002 Hardware Client only when digital certificates are in use. Specifically, unless the VPN 3002 Hardware Client uses a digital certificate, only Diffie-Hellman Group 2 is supported.

- CSCdt41281

  Packets coming through a tunnel from a client to a host on the public interface network exit through the Public Interface.

  Two workarounds exist:

  – Set up host routes for the External Boxes pointing at the Inside interface of the PIX.

  - Fake the subnet on the public interface to /30 with the outside router being the only host in the /30.

- CSCdu57263

  Multiple simultaneous connections from users behind a PAT (Port Address Translation) device can work, but only if the PAT device uses a unique source port for each simultaneous user (IKE and IPSec/UDP port for IPSec/UDP).

  Some PAT devices use UDP source = 500 for all IKE sessions even if there are multiple simultaneous. This will only allow 1 simultaneous session to work, the second connection brought up from behind this PAT device will cause the first session to be torn down.

  This is unrelated to whether or not a PAT device supports "ESP" PAT or if you are using the IPSec/UDP (NAT) functionality.

  Workaround:

  Use a PAT device that maps each additional simultaneous session to use unique UDP source ports. Connect to different destination Concentrators from behind the PAT device for additional users.

Documentation Updates

The Cisco VPN 3000 Series Concentrator documentation set has not been revised for this release. However, the standard documentation is available online through Cisco Connection Online (CCO).

On-line Context Sensitive Help Differences

Many differences exist between the FIPS-compliant Release and the online help. This section lists the most important differences.

- Throughout the VPN Concentrator Manager's browser interface, parameters that are not FIPS compliant have been labeled **(Non FIPS)**.
- Throughout the VPN Concentrator Manager, the toolbar on the third line of the screen now contains a new tab: **Check FIPS Compliance**. Clicking on this tab takes you to the new **Configuration | FIPS Compliance** page, which has a new help page that explains how to configure the VPN Concentrator to be FIPS compliant.

- The list of events contains two new event classes, FIPS and FIPSDIAG. These classes appear in the list on the **Configuration | System | Events | Classes | Add/Modify** screen.
- When configuring an IPSec Security Association (IPSec SA) on the **Configuration | Policy Management | Traffic Management | Security Association | Add/ Modify** page, the **Null** value is not available for **Encryption Algorithm**.
- The Reboot option on the **Administration | System Reboot** page is **Reboot/Zeroize (Deletes all keys and security parameters)**.

Some of the online help pages do not accurately reflect the default values for FIPS operation. The following list provides the correct default values.

- IKE proposals defaults
  - Active: IKE-3DES-SHA-DSA, CiscoVPNClient-3DES-SHA-DSA
  - Authentication Algorithm: SHA/HMAC-160
  - Encryption Algorithm: 3DES-168
- SA Configuration defaults
  - SA: ESP-3DES-SHA
  - Authentication Algorithm: ESP/SHA/HMAC-160
  - Encryption Algorithm: 3DES-168
  - IKE Proposal: IKE-3DES-SHA-DSA
- FTP: The FTP Server is disabled.
- HTTP/HTTPS: HTTP is disabled, and HTTPS is enabled.
- Telnet: Both Telnet and Telnet/SSL are disabled.
- SSL
  - Encryption Protocols: 3DES-168/SHA, DES-56/SHA,DES-40/SHA Export
  - SSL Version: TLS V1 with SSL V2 Hello
- SSH Encryption Protocols: 3DES-168, DES-56
- PPTP: PPTP is disabled
- L2TP: L2TP is disabled
- General Events severity to console is None

- Event Classes severity to console is None
- Access Settings: Configure File Encryption is DES.

Command-Line Interface Limitations

This section lists some limitations and differences in the way the command-line interface operates on the VPN Concentrator.

- You cannot access the file system from the command-line interface; however, you can access the file system through the browser interface using HTTPS.
- The Event log viewer is not accessible through the command-line interface.
- The software update feature is not accessible through the command-line interface; however you can access the software update feature through the browser interface using HTTPS.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” in *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco TAC Home Page

The Cisco TAC home page includes technical tips and configuration information for the VPN 3000 Concentrator and client. Find this information at:

http://www.cisco.com/warp/public/707/#vpn3000

Obtaining Documentation

This section describes how to obtain the documentation on the Web or how to access the documentation on CD-ROM.

Note Except for these Release Notes, no printed documentation ships automatically with this product. Please see the following sections for information about obtaining documentation for this product and for other Cisco products.

World Wide Web

Documentation for this product and for all Cisco products is available on the World Wide Web. You can access the most current Cisco documentation at: http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Ordering documentation

Cisco documentation and additional literature are available in a CD-ROM package, which is available as a single unit or as an annual subscription. 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 can 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.