Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.0.4.B

CCO Date: January 16, 2004

Part Number 78-15719-03

Introduction

Note You can find the most current documentation for released Cisco VPN 3000 products at http://www.cisco.com or http://cco.cisco.com. 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 Release 4.0 through Release 4.0.4.B software. These release notes describe new features, limitations and restrictions, and related documentation. They also list issues you should be aware of and the procedures you should follow before loading this release. The section, “Usage Notes,” describes interoperability considerations and

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

other issues you should be aware of when installing and using the VPN 3000 Series Concentrator. Read these release notes carefully prior to installing this release.

Contents

These release notes describe the following topics:

System Requirements

This section describes the system requirements for Release 4.0.

Hardware Supported

Cisco VPN 3000 Series Concentrator software Release 4.0 supports the following hardware platforms:

- Cisco VPN 3000 Series Concentrators, Models 3005 through 3080
- Altiga Networks VPN Concentrators, Models C10 through C60

Platform Files

Release 4.0 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.

Caution Be sure you install the correct file for the platform you are upgrading.

Upgrading to Release 4.0

This section contains information about upgrading from earlier releases to Release 4.0.

When upgrading VPN 3000 Concentrator releases, you must clear the cache in your browser to ensure that all new screens display correctly when you are managing the VPN Concentrator.

Note You must also log in and click "Save Needed" to add new Release 4.0 parameters to the configuration file. These new Release 4.0 parameters are added to the running configuration immediately, but they are not added to the saved configuration until you click the "Save Needed" or "Save" icon in the VPN Concentrator Manager.

Upgrading to a new version of the VPN 3000 Concentrator software does not automatically overwrite the existing configuration file. Configuration options for new features (for example, IKE proposals) are not automatically saved to the configuration file on an upgrade. The HTML Manager displays "Save Needed" (rather than "Save") to indicate that the configuration needs to be saved. If the configuration is not saved, then on the next reboot, the new configuration options are added again. If you need to send the configuration file to the TAC, save the running configuration to the configuration file first.

Before You Begin

Before you upgrade to this release, *back up your existing configuration to the flash and to an external server.* This ensures that you can return to the previous configuration and software if you need to.

Be aware of the following considerations before you upgrade. These are known product behaviors, and your knowing about them at the beginning of the process should expedite your product upgrade experience. Where appropriate, the number of the caveat documenting the issue appears at the end of the item. See Open Caveats for VPN 3000 Series Concentrator, page 19 for a description of using this number to locate a particular caveat.

Release 4.0 of the VPN 3000 Concentrator software contains several features that interact with corresponding features in the Release 3.6.x and 4.0.x versions of the VPN Client and VPN 3002 Hardware Client software. To get the full benefit of this release you should upgrade your client software to one of these versions.

Note No VPN Client software upgrade is being released at the same time as the VPN 3000 Concentrator Release 4.0.4.

The VPN 3000 Concentrator software, Release 4.0, does operate with VPN Client and VPN 3002 Hardware Client versions 3.0 and higher, but you should upgrade these, too, to take full advantage of the new features.

- To use the VPN Client, Release 3.0 or higher, you *must* upgrade the VPN Concentrator to Release 3.0 or higher. The VPN Client, Release 3.0 or higher, does *not* operate with the VPN 3000 Concentrator version 2.5 or earlier versions.
- Do not update the VPN 3000 Concentrator when the system is under heavy use, as the update might fail (CSCdr61206).
- If you are upgrading from Release 3.0 to Release 3.1 or higher and you are using the "Group Lookup" feature, you must manually set Group Lookup after the upgrade. To enable this feature, go to Configuration | System | General | Authentication and select the Enable check box (CSCdu63961).

Use the following backup procedure to ensure that you have a ready backup configuration.

Backing Up the Existing Configuration to the Flash

1. Go to Administration | File Management | Files.
2. Select the configuration file and click Copy.
3. Enter a name for the backup file (in 8.3 format; for example, name it CON367BK.TST)

You have now backed up the existing configuration to the flash.

Backing Up the Existing Configuration to an External Server

You should also back up the configuration to a server. You can do this in many ways, one of which is to download the file using your Web Browser from the HTML interface (VPN Manager).

You can now upgrade the software with assurance that you can return to your previous firmware using your previous configuration.

Note After upgrading, be sure to clear the cache on your browser. Release 4.0 adds features and enhances HTML page layouts. Clearing your browser cache ensures that everything displays correctly and uses the new features and layout.

Downgrading from Release 4.0

If you need to return to a release prior to Release 4.0, do the following:

Step 1 Reload the firmware for the desired release. (Do not reboot yet.)

Step 2 Rename the existing configuration (for example, rename it as CON367BK.TST).

Step 3 Delete "CONFIG".

Step 4 Copy the previously saved backup file (for example, CON36BKP.TST) to CONFIG. Do not click Save (otherwise, your original CONFIG file will be overwritten with the running configuration).

Step 5 Perform a software reset.

Your prior firmware and image are restored.

New Features in Release 4.0.4

Release 4.0.4 introduces the following features.

VPN 3020 Concentrator

The VPN 3000 Concentrator Series now includes the VPN 3020, which has these specifications:

- Support for 750 simultaneous remote access IPSec sessions *or* 100 simultaneous WebVPN sessions
- 256 MB memory

- One SEP module for hardware-based encryption
- Single power supply
- Expansion capabilities:
  - One additional SEP module for hardware-based encryption
  - Up to two additional SEP modules for redundancy
  - Optional redundant power supply

The VPN3020 is not upgradable to a VPN 3030, 3060, or 3080.

VPN 3005 Concentrator Enhancement

Beginning with Release 4.04, the VPN 3005 Concentrator with 64 MB memory supports up to 200 simultaneous remote access IPSec sessions.

To achieve this number, VPN Client must either:

- Run 4.0 or later software, or
- Refrain from split tunneling if they are running pre-4.0 software.

VPN 3002 Hardware Client must refrain from split tunneling.

Note A VPN 3005 Concentrator with 32 MB of memory supports up to 100 IPSec or PPTP sessions.

New Features in Release 4.0

This section describes the new features in Release 4.0 of the VPN 3000 Series Concentrator. For detailed instructions about how to configure and use these features, see *VPN 3000 Series Concentrator Reference Volume I: Configuration* and *VPN 3000 Series Concentrator Reference Volume II: Administration and Management.*

Hardware Acceleration for Advanced Encryption Standard (AES)

VPN 3000 Concentrator models 3015 and higher now offer an enhanced, scalable encryption processor (SEP-E), that provides hardware support for AES (software support was added in Release 3.6). This feature has no configuration implications. For installation information about the new SEP-E modules, see *Installing SEP or SEP-E Modules in the VPN 3000 Series Concentrator.*

Note The VPN 3000 Concentrator uses *either* SEP or SEP-E modules, not both. Do not install both on the same device. If you install a SEP-E module on a VPN Concentrator that already contains a SEP module, the VPN Concentrator disables the SEP module and uses only the SEP-E module.

512 MB On-Board Memory

You can now upgrade your VPN 3060 or 3080 Concentrator memory to 512 MB.

Note To take advantage of this additional memory, you must also update the VPN Concentrator Manager to Version 4.0 and update the VPN Concentrator Bootcode to Version 4.0.

If your VPN 3000 Concentrator is running low on memory resources, upgrading to 512 MB will help. Symptoms that indicate low memory include the following:

- VPN Concentrator cannot support the necessary number of tunnels.
- VPN Concentrator cannot accept additional connections.
- VPN Concentrator failures.

To determine the amount of memory currently installed in your VPN Concentrator, use the Monitoring | Status screen. For information about installing memory upgrades and about updating the VPN Concentrator Manager and the VPN Concentrator Bootcode, see *Upgrading Memory to 512 MB in the VPN 3000 Series Concentrator,* included with your memory upgrade kit.

Note Increasing memory to 512 MB on any VPN Concentrator model does *not* increase the number of sessions supported.

RADIUS User Filters

With Release 4.0, administrators can define remote access user filters in Cisco Secure ACS as download PIX ACLs or as a Cisco vendor-specific RADIUS attribute AV-PAIR (26/9/1), rather than having to define them on each VPN Concentrator. This feature provides limited support for to download inbound access control lists or filters and apply them to a user or group, rather than defining the filters on the VPN Concentrator.

A network administrator can configure the filters on a RADIUS server, rather than on the VPN Concentrator. To provide information about the filter and filter rules, the VPN Concentrator's management system includes a new screen in the monitoring and administration sessions.

Backup LAN-to-LAN

The Backup LAN-to-LAN feature lets you establish redundancy for your LAN-to-LAN connection. Unlike VRRP, which provides a failover for the VPN Concentrator, Backup LAN-to-LAN provides a failover for the connection itself. Although VRRP and Backup LAN-to-LAN are both ways of establishing continuity of service should a VPN Concentrator fail, Backup LAN-to-LAN provides certain advantages that VRRP does not.

- You *can* configure Backup LAN-to-LAN and load balancing on the same device, but you cannot configure VRRP and load balancing on the same VPN Concentrator.
- Redundant Backup LAN-to-LAN peers do not have to be located at the same site. VRRP backup peers cannot be geographically dispersed,

Note This feature does not work in conjunction with VRRP. If you set up a Backup LAN-to-LAN configuration, disable VRRP.

Native Kerberos Authentication

Release 4.0 supports authentication to Kerberos/Active directory, which is the default authentication mechanism in Windows 2000 and Windows XP. Kerberos is an authentication protocol for use on untrusted networks. The protocol comprises two stages of authentication--the first level is to a key distribution center (KDC), and the second level is between each client and server.

To configure this feature, an administrator must add a Kerberos authentication server on a group basis or add the server to the global authentication servers list and configure such parameters as server IP address, server port, number of retries, and so on. The IPSec group tab includes Kerberos as an authentication type, and statistical displays also include Kerberos authentication statistics.

See the Open Caveats section for information about configuration issues with Active Directory (CSCdz62206) and Linux/UNIX (CSCea20236).

LDAP/RADIUS Authorization

This feature separates user authorization (permissions) from user authentication. It lets certificate users receive permissions by means of LDAP or RADIUS without secondary authentication via XAUTH. It also lets non-certificate users using any type of authentication scheme (Kerberos, NT Domain, SDI, Radius, and Internal) to retrieve these permissions/attributes.

The feature provides a way to configure RADIUS and LDAP authorization servers and event information. The network administrator configures authorization servers on a global system or group basis.

Alerts (Delete with Reason Notifications)

The VPN 3000 Concentrator and the VPN 3002 Hardware Client can send alerts with reasons for disconnects and reboots they initiate to either the VPN Client or Concentrator to which they connect. When a disconnect occurs, the VPN Client displays the disconnect notice and the reason (if available) in the Event log.

The VPN Client can also send alerts regarding disconnects that it initiates, but it does not send a reason.

SNMP Enhancements

With Release 4.0, you can configure a list of particular event identifiers to track, as well as tracking events by class and severity. For more information, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*, Chapter 10, "Events."

Disable LAN-to-LAN Tunnels

With Release 4.0, an administrator can disable a LAN-to-LAN VPN connection without deleting its configuration. This feature can be useful for troubleshooting a connection.

Configurable giaddr for Group-Based DHCP

This feature lets an administrator define a network address on a group basis to be used in DHCP proxy address assignments. To use this feature, DHCP proxy must be enabled on the VPN 3000 Series Concentrator. The administrator enters a network address without a subnet mask under group and user configuration. This address indicates to the DHCP server the scope (that is, the range of available IP addresses on the DHCP server) within which to assign the address.

Memory Conservation Enhancements

Release 4.0 includes modifications to memory structures and allocation algorithms to limit unnecessary memory use.

Memory Statistics Display Enhancements

The VPN 3000 Concentrator and the VPN 3002 Hardware Client now monitor and display memory usage in terms of block size and free and used blocks. The display also includes a new page with detailed statistics.

Enhanced Sygate Firewall AYT Support

Release 4.0 includes support for Sygate Personal Firewall, Sygate Personal Firewall Pro, and Sygate Security Agent.

Enhanced PING Command Features

Admin users who have only read access can now do PING commands, using either the Monitor tab on the GUI or the command-line interface. The PING command also appears, as before, on the Admin tab, accessible to users who have full access privileges. The PING command now shows the reply time in milliseconds and not just “device is available.”

Adjustable DPD Timeout

For dead-peer detection (DPD), this feature lets an administrator configure the interval that the Concentrator waits before beginning Keepalive monitoring. This feature applies only to Easy VPN Clients that are using IKE Keepalives.

LDAP Authorization Authenticated Bind (Login DN) Support

Release 4.0.1 adds support for LDAP Authorization Authenticated Binds by allowing you to configure the Login DN and Password fields. The field names and the order of fields on the LDAP Authentication Server configuration page have changed, as follows (CSCea73064):

- The Server Secret field and description are now called Password (as it relates to the Login DN field), and the description changed to say “Enter the Login DN password”.
- The LDAP Base DN field is now Base DN.

The LDAP config fields are now in the following order:

- Server Type
- Authorization Server
- Server Port

- Timeout
- Retries
- Login DN
- Password
- Verify
- Base DN
- Search Scope
- Naming Attributes

The Login DN represents a user on the LDAP server with administrative privileges. For example, on the Microsoft Active Directory LDAP Server, the Login DN could be:

cn=Administrator,cn=Users,dc=mycompany,dc=com(CSCea69156)

Usage Notes

This section lists interoperability considerations and other issues to consider before installing and using Release 4.0 of the VPN 3000 Series Concentrator software.

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 or higher. The latest version of Adobe Acrobat is available at the Adobe web site: http://www.adobe.com.

Disable Group Lock When Using SDI or NT Domain Authentication

This feature is supported only when using Internal or RADIUS authentication. To ensure that you are using this feature properly please refer to the following URL: http://www.cisco.com/warp/customer/471/altigagroup.html

Password Expiry Does Not Change User Profile for LAN

You must enable Start Before Logon on the VPN Client and possibly may need to make sure that DNS and WINS servers are properly configured (CSCdv73252).

Browser Interoperability Issues

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

VPN 3000 Concentrator Fully Supports Only Netscape and Internet Explorer

Currently, the VPN 3000 Concentrator fully supports only Netscape and Internet Explorer. Using other browsers might cause unacceptable behavior; for example, if you attempt to use an unsupported Web Browser to manage the VPN 3000 Concentrator, clicking any of the links might return you to the login screen. (CSCdx87630).

Internet Explorer 4.x Browser Issues

The following are known issues with Internet Explorer 4.X and the VPN Concentrator Manager (the HTML management interface). To avoid these problems, use the latest version of Internet Explorer.

- 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.
- When connecting to the VPN Concentrator 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.

VPN Client Used with Zone Labs Integrity Agent Uses Port 5054

VPN Clients, when used with the Zone Labs Integrity Agent, are put into a "restricted state" upon connection to the Integrity Server if a port other than 5054 is used. The restricted state simply means the VPN Client is able to communicate only with the Integrity Server; all other traffic is blocked (CSCdw50994).

Workaround:

Do *one* of the following:

- Configure the VPN Concentrator and the Integrity Server to use port 5054 when communicating with each other.
- Edit the WEB.XML file in the Integrity directory and search for 5054 (the port that Integrity uses/looks for). Change it to 5000, save, and restart the Integrity Server.

Administer Sessions Screen Shows Data for Wrong Group

When an L2TP/IPSec connection is established, authentication should behave as follows:

1. The Tunnel Group is authenticated (using the OU field in the Certificate or using the Base Group).
2. The User should be authenticated (using the authentication method of the tunnel group.
3. The User's Group (as defined by the group delimiter option) should be authenticated.

This all works properly, but in the Administration | Administer Sessions screen, the Tunnel Group displays instead of the User's Group (CSCdy00360).

Long Initialization for SNMP Traps in Releases 3.0, 3.5, and 3.5.1

In Releases 3.0, 3.5, and 3.5.1 of the VPN 3000/3002 products, the SNMP task takes 3-5 minutes to complete initialization after a device reboot. Traps being processed during this interval are queued and sent to the SNMP Management station after SNMP task initialization completes.

However, the cold start trap, normally sent as a result of a device rebooting, is never sent.

In Release 2.5.X, the cold start trap is properly sent to the SNMP Manager after a device reboots (CSCdt01583).

Windows NT Authentication Servers Can't Follow Other Server Types in the a Prioritized Authentication Server List

If an Windows NT server follows a non-NT server in the prioritized authentication server list, and the non-NT server becomes unavailable for some reason, the VPN 3000 Concentrator detects this and falls back to the Windows NT server. If the tunnel being established is PPTP or L2TP, the authentication attempt to the Windows NT server also fails.

Therefore, when configuring PPTP or L2TP connections, do not place Windows NT authentication servers behind other types of servers in the applicable authentication server list (CSCdy07226).

Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact univercd at www.cisco.com (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

"The page cannot be displayed."

To access the Glossary, you must be connected to www.cisco.com (CSCdy14238).

SNMP Traps VRRP Notifications and cipSecMIBNotifications Are Not Supported

The VPN 3000 Concentrator does not support the VRRPNotifications and cipSecMIBNotifications SNMP traps. You can configure VRRP for these SNMP traps without getting an error message, but the traps themselves are not supported, so no action occurs. The same is true of Cisco IPSec-flow MIB notifications (CSCdx44580).

RSA Allows a CA to Issue Only One Certificate with any DN

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 1 certificate with any particular DN (CSCdv27743).

Reauthentication on Rekey Interval

If you have enabled the Reauthentication on Rekey feature, the VPN Concentrator prompts users to enter an ID and password during Phase 1 IKE negotiations and also prompts for user authentication whenever a rekey occurs. Reauthentication provides additional security.

If the configured rekey interval is very short, users might find repeated authorization requests inconvenient. In this case, disable reauthentication. To check your VPN Concentrator's configured rekey interval, see the Lifetime Measurement, Data Lifetime, and Time Lifetime fields on the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add or Modify screen.

Note At 85% of the rekey interval, the software client prompts the user to reauthenticate. If the user does not respond within approximately 90 seconds, the VPN Concentrator drops the connection.

VPN 3000 Concentrator Ignores RADIUS Packets Longer Than 4096 Bytes

Some RADIUS Servers exceed the Maximum RADIUS packet size of 4096 bytes. The VPN 3000 Series Concentrator ignores RADIUS packets that exceed this length (CSCdz90027).

Downgrading to Release 3.6 with a Release 4.0 Configuration Deletes Information from LAN-to-LAN Groups

A VPN Concentrator with more than 125 users and groups combined fails to terminate tunnels if the SEPs are not active. This is because a VPN Concentrator with no active SEPs is considered to be a model 3015, and model 3015 supports only 125 users and groups combined.

This condition could unexpectedly arise if a VPN Concentrator with a SEP-E, running Release 4.0, is downgraded to Release 3.6. This would result in the problem, because the Release 3.6 does not support the SEP-E module. The SEP-Es are detected as unknown cards if present when running Release 3.6 code.

If you encounter a situation, for whatever reason, where you are trying to load a configuration with more users than are supported by the model, the following event appears on the console after a reboot:

****

3 03/20/2003 14:03:16.260 SEV=3 CONFIG/32 RPT=1

SERVE Too Many Entries Error. Delete an entry before adding a new one.

****

(CSCea51435)

VPN Client Supports Elevated Privileges Using the MSI Installer

Windows Installer 2.0 must be installed on a Windows NT or Windows 2000 PC prior to configuring the PC for a Restricted User with Elevated Privileges When using elevated privileges, the VPN Client program files are created under the specific user, not “ALL” users. (CSCea37900).

Change to Network List Creation for LAN-to-LAN Configuration

The functionality that allows the administrator to create a network list from within a LAN-to-LAN configuration page has changed.

In previous releases, the administrator could create a network list from within the LAN-to-LAN configuration page. The new method for creating a network list uses a link on the LAN-to-LAN index page to the network list configuration page.

This change was resolves a problem with Reverse Route Injection when the network lists are added from within the LAN-to-LAN page. With the previous method, the routes, corresponding to the network lists that were added via the LAN-to-LAN page, were not present in the routing table (CSCea13002, CSCdz87573).

Open Caveats for VPN 3000 Series Concentrator

Caveats describe unexpected behavior or defects in Cisco software releases. The following list is sorted by identifier number.

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/cgi-bin/Support/Bugtool/launch_bugtool.pl.

The following problems exist with the VPN 3000 Series Concentrator, Release 4.0.

- CSCds44095

  L2TP over IPSec connections fail if going through a NAT device. During the connection establishment, the VPN Client and the VPN 3000 Concentrator exchange IP addresses. When the client sends what it believes to be the VPN 3000 Concentrator's address (really the NATed address), the VPN 3000 Concentrator releases the connection.

This is because the address assigned to the interface does not match the address coming in from the client. The same issue exists on the client side. This will not be resolved until the Windows 2000 MS client supports UDP encapsulation.

- CSCdt08303

  When configuring a LAN-to-LAN connection with IOS or PIX, it is important to match the keepalive configuration (both "ON" or both "OFF"). If the keepalive configuration is OFF for the VPN 3000 Concentrator and ON for the IOS device, the tunnel will be established with data.

  IOS tears down the tunnel because the VPN 3000 Concentrator does not respond to IOS style keepalives if keepalives are configured to be OFF for the VPN 3000 Concentrator.

- CSCdw36613

  In some cases, the Zone Labs Integrity Agent may not properly update on the Windows NT version 4.0 operating system while the VPN Client is connected, policy is changed and re-deployed, and the connection is up. Specifically, if you "Block Internet Servers" under the Firewall Security Rules in the Policy and then Deploy that new policy, a PC running Windows NT version 4.0 receives the updated policy, but it might not put the "Block Internet Servers" setting of that policy into effect.

  Workaround:

  Reboot the operating system.

- CSCdx47596

  Due to a Microsoft limitation, Windows XP PCs are not capable of receiving a large number of Classless Static Routes (CSR). The VPN 3000 Concentrator limits the number of CSRs that are inserted into a DHCP INFORM message response when configured to do so.

  The VPN 3000 Concentrator limits the number of routes to 28-42, depending on the class.

- CSCdx89348

  The Concentrator may display the following events during a VPN Client connection. These events were found to be due to the client being behind a Linksys Cable/DSL router that was incorrectly modifying the Client's packets, causing them to fail authentication when received by the VPN Concentrator. The problem is more prominent if LZS compression is used.

Events:

131500 06/20/2002 17:08:34.300 SEV=4 IPSEC/4 RPT=4632

IPSec ESP Tunnel Inb: Packet authentication failed, username: gray, SPI:

4e01db67, Seq Num: 0000850f. Dump of failed hash follows.

Linksys has been notified about the problem.

Workaround:

Although no workaround currently exists, disabling LZS compression on the Concentrator helps reduce the number of events. To disable LZS compression on the Concentrator set the “IPComp” setting on the IPSec tab of the group configuration to “none”.

- CSCdy26161

  The Microsoft L2TP/IPSec client for Windows 98, Windows ME, and Windows NT does not connect to the VPN 3000 Concentrator using digital certificates.

  Workaround:

  Use Preshared keys.

- CSCdy27564

  The Assigned IP address for a PIX-501 in Network Extension Mode appears on the VPN 3000 Concentrator as 0.0.0.0 until the first IPSec/Phase 2 rekey takes place. After the Phase 2 rekey completes, the Assigned IP address is correctly set to the PIX-501's private interface network address.

- CSCdz24882

  Using Microsoft Internet Explorer version 5.0, you cannot create a detailed memory report from the Monitoring | System Status | Memory Status | Detailed Memory Report button. The file memory.txt is *not* created. The report does work if the file already exists. You *can* create the file initially if you run a detailed report from the CLI interface. Internet Explorer version 5.5 and Netscape work fine.

- CSCdz83332

  When switching between tabs under the interfaces section of the html-management page, the action may eventually fail.

  If this happens simply go back to the interface summary page and drill back down into the desired interface. Everything will resume working again.

- CSCdz87108

  The LDAP Authorization failure reasons depend on how the LDAP server implements these error codes. RFC 1777-LDAP states that the LDAP server might not return an error code, therefore in those situations the VPN 3000 failure reason is “Invalid response received from server”.

  For the case in which the LDAP server *does* return a specific error diagnostic (for example, noSuchAttribute) the VPN 3000 failure reason displays the appropriate string.

- CSCea20236

  Before you use the VPN Concentrator to authenticate a user to a Linux or Unix server running a Kerberos server, follow these steps:

  a. Check the keys available for the user you want to authenticate. Run:

     kadmin.local -q “getprinc *username*”

  b. Make sure that “DES cbc mode with RSA-MD5, Version 5” is one of the available keys. If you do not see “DES cbc mode with RSA-MD5, Version 5”, edit the kdc.conf file and add or move des-cbc-md5 selections to the beginning of the supported_enctypes = line. For example:

     [realms]

     MYCOMPANY.COM = {

     master_key_type = des-cbc-crc

     supported_enctypes = des-cbc-md5:normal des-cbc-md5:norealm des-cbc-md5:onlyrealm

     Save the file. Then, restart the krb5kdc, kadmin, and krb524 services.

  c. To create the “DES cbc mode with RSA-MD5” keys, change the users password:

     kadmin.local -q “cpw -pw newpassword *username*”

  Now you should be able to authenticate that user to your Linux/Unix Kerberos 5 server.

- CSCea29828

  HTTP Software Updates sometimes fail with “Software Update Error”. Retrying the operation does not update the image.

- CSCea52820

  The text from the Help page for the Monitoring | System Status | Memory Details page in HTML incorrectly refers to “Memory Detail Report”. The page is labelled and called: “Detailed Memory Report”.

- CSCea52936

  The Help for the SEP-E in the Monitoring | System Status | SEP in-line SEP page is incomplete. In other sections, we make reference to the SEP-E. We should add:

  “AES (SEP-E only)” to the Encryption and Decryption bullet.

  This screen displays status and statistics for a VPN Concentrator SEP (Scalable Encryption Processing) or a SEP-E (Enhanced SEP) module, which performs hardware-based cryptographic functions:

  – Random-number generation.

  – Hash transforms (MD5 and SHA-1) for authentication.

  – Encryption and decryption (DES and Triple-DES).

  The screen shows cumulative data since the system was last booted or reset.

Caveats Resolved in Release 4.0.4.B

Release 4.0.4.B resolves the following issues:

- CSCec02285

  The VPN 3002 CLI, Administration | Access Rights | Administrators menu displays the ISP user instead of the monitor user. But the GUI displays the monitor user. Logon to the GUI using a monitor account fails. Logon to the GUI using an ISP account succeeds, but you can still change the config through the quick configuration. If the VPN 3002 has this problem, it's always there; if the VPN 3002 does not have this problem, it never happens, no matter which version of the code is in use.

- CSCec16876

  The VPN 3000 Concentrator does not automatically add routes for more than one remote LAN. You must enter static routes for each additional remote LAN on the VPN 3000 Concentrator.

- CSCec77145

  Cisco VPN 3000 Concentrator implementation using RSA/Ace 5.0.3 Agent API does not work for cross realm authentications. The ACE/Server sends a downgrade request to the agent. This is meant to be interpreted by the agent to generate a v2 authentication request with a v5 header. The VPN Concentrator actually downgrades and sends a full v2 request. The ACE/Server then fails the request because it appears that this is a v2 agent, which needs acting primary/secondary.

- CSCed14234

  Using Release 3.6.8 or 4.0.3, when we clear the check box for “Enable Telnet/SSL” at Configuration | System | Management Protocols | Telnet, the check box is filled after reloading the VPN 3000 configuration.

- CSCed34928

  The Filter Rule Copy from the HTML does not copy the network list from the old rule to the new rule.

- CSCed40267

  The VPN 3000 Concentrator slowly runs out of memory when processing a DCHP Inform message from an L2TP or PPTP client with Network Lists and DHCP Intercept enabled. The size of the memory block that is not released varies, based on Network List size.

- CSCed42494

  Two PIX501 (EZ VPN Clients) behind Linksys devices (with same DHCP pool) disconnect during IKE rekey. In this case, the PIXes keep trying to bring up public-to-public IPSec SA's (tearing down the others). The PIX establishes a new IPSec SA on the new IKE SA. The up and down causes the deletion of the IKE.

Note NOTE: The old IKE SA does not transfer the tunnels to the new IKE SA until it activates the new SA when it receives a delete message or the SA expires.

Caveats Resolved in Release 4.0.4.A

Release 4.0.4.A resolves the following issues:

- CSCed18995

  Each IKE rekey for main mode (that is, using digital certificates) fails to release a 64-byte memory block, eventually causing the device to fail.

- CSCed22626

  With Release 4.0.4 only, the VPN 3000 Concentrator removes RRI routes from NEM connections after a re-key.

Caveats Resolved in Release 4.0.4

Release 4.0.4 resolves the following issues:

- CSCeb27069

  In Release 4.0.1, denying certain PINs with RSA SecurID is not functioning (for example, denying alphanumeric PINs or those based on PIN length).

- CSCeb48289

  VPN 3000 Concentrator failed due to a malformed PPP IP Control Protocol message.

- CSCeb65325

  The VPN 3000 Concentrator passes a blank username/password to an authentication server.

- CSCec51632

  The VPN 3000 Concentrator does not support ReadOnly community strings. All community strings are considered Read/Write.

  For security reasons, the VPN 3000 should not support remote SNMP sets. If you rely on this feature, contact Cisco TAC.

- CSCec61306

  Kerberos support for 3DES/SHA not functioning.

- CSCec66975

  The ifType (1.3.6.1.2.1.2.2.1.3) for the VPN 3000 Concentrator FastEthernet interfaces is reported as 7 (iso88023Csmacd). Per IANA, ifType 7 was deprecated via RFC-draft-ietf-hubmib-etherif-mib-v3. IfType 6 (ethernetCsmacd) should be used instead.

(See ianaiftype-mib and RFC 2665):

http://www.iana.org/assignments/ianaiftype-mib

http://www.ietf.org/rfc/rfc2665.txt?number=2665

The wrong ifType might confuse some NMS systems, as they are expecting ifType=6 for Ethernet interfaces.

- CSCec67748

  Master VPN 3000 Concentrator's interfaces are "Master" after a reboot, even though one of the interfaces is Down. This occurs on VPN 3030/VPN 3080 Concentrators using software revisions 3.6.8 and 4.0.1.C

- CSCec69061

  The command snmpget to certain OIDs might cause the VPN 3000 Concentrator to fail. This happens only if the snmpget is sent to the private interface and the community string is correct.It has occurred for software versions 4.0.1 and 4.0.2.

- CSCec72004

  The AUTH login message for SNMP says user "Unknown". This should be user "SNMP".

- CSCec73218

  Some cable modems, if they loose their broadband signal, issue the IP address 192.168.1.11 address via DHCP. When this happens and the VPN 3002 accepts this address, the VPN 3002 uses the 192 address in its IKE negotiations.

  The result is a tunnel that cannot pass traffic. You see from the central site Concentrator what looks like a functional tunnel with no RX bytes and no private-to-private SA.

- CSCed03366

  New pin mode for user authentication to SDI server via RADIUS not working.This issue was introduced in Release 4.0.3.REL.

- CSCed09411

  The VPN3000 might fail while displaying Memory Statistics.

- CSCed09496

  A VPN 3000 Concentrator accepts NEM PIX 501 connections with split tunneling enabled. After a period of time, the VPN Concentrator shows high cpu usage, eventually dropping connections due to dead-peer-detection (dpd) loss.

  PIX NEM connections are more frequently affected than others due to their low default dpd interval. All others, however, are occasionally affected.

  Workaround:

  Disable split tunneling or increase the dpd interval.

Caveat Resolved in Release 4.0.3

Release 4.0.3 resolves the following issue:

- CSCec62519

  L2TP and PPTP connections to VPN 3000 Concentrator Release 4.0.2 causes the VPN 3000 Concentrator to fail.

Caveats Resolved in Release 4.0.2

Release 4.0.2 resolves the following issues:

- CSCdy76967

  Attempting to delete a file from an ftp session into the VPN 3000 Concentrator fails and terminates the ftp session.

- CSCdz09899

  When editing a LAN-to-LAN orig-only record by adding more peers to the list the following event appears in the event log:

  23 10/23/2002 13:44:20.410 SEV=4 BMGT/29 RPT=1

  Attempting to specify an Aggregate Group reservation [961150977 bps] on Group [group-name] Interface [2], which is outside the range of a minimum of [8000 bps] to a maximum of [100000000 bps]. (Note: The true maximum depends on the interface link rate to which the group is applied.)

Bandwidth management was not enabled at all on the interface or group.

- CSCdz17373

  A customer connects from a VPN 3002 Hardware Client configured as a PPPoE client to a VPN 3000 Concentrator using a service provider. According to the customer, this configuration was working fine until recently, when the provider changed on their side to use PAP instead of MS-CHAP v1 for PPPoE authentication. Debugs from the VPN 3002 show the following authentication error:

  Conn Id 1 : PPP_AuthLogErr() illegal fsm event received.

  The customer sees same behavior whether they use Release 3.6.3, 3.6.1, or 3.5.5.

- CSCdz21620

  In IP packets that have the TOS field set, such as in VoIP and QOS applications, the TOS field is not copied into the IPSec packet header when it is tunneled. The packet is then treated like other IP traffic while encapsulated.

- CSCdz29105

  The Ping command under “Actions” on the LAN-to-LAN sessions screen refreshes the screen instead of stating whether the tunnel is active.

- CSCdz58797

  On the Ethernet 2 (Public) interface, if the checkbox “Public Interface” is not selected, then all IPSec over TCP connections cannot be initiated to the VPN 3000 Concentrator, although all IPSec over UDP initiations work fine.

- CSCea44603

  When using VPN 3000 Concentrator software Release 3.6.2, the CRL check bind request does not send the login ID/password combination. Anonymous login is successful, however.

- CSCea46018

  When a backup SEP-E fails over to Software, the Activity LED and Status LED stay green, even though the SEP-E is no longer operational.

- CSCea50428

  A VPN 3000 Concentrator, using the external interfaces on parallel VPN Concentrators with DHCP relay enabled, might fail to free message buffers. This could prevent new connections and possibly cause the device to fail.

- CSCdz54963

  VPN 3000 Concentrator SDI AUTH/64 events appear in the log when a backup server is not defined. This is a cosmetic message.

- CSCea64917

  A VPN 3000 Concentrator running Release 3.6.7.C has a problem generating the XML file from the XML export if the VPN Concentrator has more than 15 LAN-to-LAN tunnels configured.

- CSCea66439

  A third-party VPN client connects to a VPN 3000 Concentrator and proposes a shorter Ipsec SA lifetime than what is configured on the VPN Concentrator (proposed 1 hour; but the VPN Concentrator is configured for a lifetime of 8 hours). The display indicates that the VPN Concentrator uses the configured 8 hours instead of the proposed 1 hour. This is a display problem only. The rekey still occurs at 1 hour.

- CSCea70449

  The User [user], Group [group] event log message for a client disconnect is separated by comma in Release 3.6.7 and later code. In the code before Release 3.6.7, this comma was not present and the User [user] Group [group] event log message was separated with a space tab format.

- CSCea77918

  Under the Group IPSec tab, the Confidence Interval option shouldn't say Easy VPN Client only, because that option also exists for the Site-to-Site tunnels. The current text is confusing and seems to be a valid option only for Remote Access clients.

- CSCea79618

  Configuration errors might occur when downgrading from Release 4.0 to 3.x. Be sure to backup your current configuration before upgrading to Release 4.0. Failure to do so might prevent you from being able to seamlessly revert back to Release 3.x.

- CSCea81010

  When using multiple static CRL servers, if the first server fails without being taken off-line, the subsequent searches also fail.

- CSCea91878

  A VPN 3000 Concentrator sends VRRP messages on the Public interface after system shutdown. This occurs with software Releases 3.6.7C, 3.6.7D, and 4.0.

- CSCea91950

  NAT-T or UDP keepalive packets are sent out the Private interface if the Public interface checkbox is not checked on the Public interface.

- CSCea93008

  On a VPN 3000 Series Concentrator running Release 3.x or 4.x, when you click on a LAN-to-LAN session to get more detailed information under Monitoring | Sessions (HTTP management console), there is a hyperlink on the top called “Back to Sessions”. This link redirects you incorrectly to Administration | Administer Sessions and not back to the Monitoring | Sessions section.

- CSCeb00271

  With the VPN 3000 Concentrator running Release 3.6.7.C or 4.0, the VPN 3002 Hardware Client deletes the existing tunnel upon receiving a malformed IKE packet from an unknown source.

- CSCeb00629

  Clicking Cancel in the bandwidth policy and returning to the same screen from the same frame gives confusing output.

  If the administrator goes into the group’s bandwidth policy via the right frame after clicking Cancel while editing the same policy, the indicator None is displayed, although the running config contains some policy.

- CSCeb07283

  A VPN 3000 Concentrator running Release 3.6.7 and using L2TP over IPSec with EAP-TLS AND L2TP compression stops encrypting traffic after 2-3 hours, but the connection stays up.

- CSCeb18649

  VPN client can't connect using cTCP to the virtual address in the VPN 3000 Series Concentrator using load balancing following a reboot. This issue occurs only in Releases 3.6.7.F, 3.6.7.G, 4.0.1 and 4.0.1.A.

- CSCeb19687

  During the TFTP upgrade of a VPN 3000 Concentrator from Release 3.6.7 to Release 4.0, reboot occurs when the word “no” is typed instead of N for the question “Reboot now? (Y/N) [Y]”.

- CSCeb21307

  The VPN 3000 Concentrator supports IPSec rekeys by time, volume, both, or none. The VPN 3000 Concentrator does not send a rekey attribute when it is not involved. This introduces the possibility of one side being configured for time and the other for data. In this case, the responder rekeys on both, but it does not inform its peer of its rekey requirements.

  This is not a issue when interoperating with PIX or IOS, because they support only rekey on both. The VPN 3000 Concentrator should send its rekey requirement even if its peer does not have that requirement.The VPN Client software does not support rekey by data and ignores this requirement.

- CSCeb22460

  VRRP and IPSec over TCP might not work in 3.6.7F and 4.0.1. They work in Release 3.6.3.

- CSCeb22797

  With a VPN3002 using PPPoE, the TCP packets from behind the VPN3002 must have their MSS adjusted for split-tunneling. If the TCP MSS is not adjusted to the MTU, the MSS negotiated in the TCP session exceed the MTU for the PPPoE session. The problem occurs when the IP packets DF bit is set. This could prevent the packet from reaching the PC behind the VPN3002.

  If the MSS is adjusted, the packet fixes in the PPPoE tunnel and does not require fragmentation.

- CSCeb23697

  VPN 3000 Concentrator software does not have a Time Zone for Adelaide and Darwin (GMT+9:30).

- CSCeb23856

  RRI support does not work properly for hardware clients in network extension mode that do not support sending an application version to the VPN 3000 Concentrator.

- CSCeb29180

  Using Release 4.0.1, the VPN 3000 Concentrator appends, as expected, the configured REALM when it sends the authentication request to the Windows 2000 Kerberos server when a user uses “joe” as a username.

  However, when, for example, a username like “joe.blocks@domain.com” is used, the VPN 3000 Concentrator does not append the configured REALM. The VPN 3000 Concentrator assumes the string after the @ in the user name is a user specified Realm.

  Depending on how you configure the username and on how the end user enters his or her username with a domain (for example, “joe.blocks@domain.com”), you might need to turn on “Strip Realm” within the group. If the user is defined in the Active Directory as username “Joe.Block” and principal name suffix as “@domain.com”, then you should enable “Strip Realm”. If the user is defined in the Active Directory as username “Joe.Block@blahblah.com” and the principal name suffix as “@domain.com”, then you should disable “Strip Realm”.

  When testing the authentication server, the Strip Realm function works only if the server is defined under the group (that is, not globally).

- CSCeb30226

  Using a VPN 3060, running either Release 3.5.5 or 3.6.7.F, when we set VRRP and Master VPN's private interface fails, switchover delay happens at Backup VPN, so we cannot communicate end-to-end.

- CSCeb31543

  In Release 4.0.1.A, when configuring long static CRL Distribution Points, some of the text would truncate into the Login DN field. This could affect the LDAP Distribution Point authentication process.

- CSCeb35779

  Customer requests more than 200 routes to be supported with a 3005 w/ 64MB.

- CSCeb37368

  Issues related to freeing buffers in memory cause the VPN 3000 Concentrator to fail.

- CSCeb38654

VPN Hardware Client 3002-8E models continuously reboot if the public interface's link is down when the unit boots.

- CSCeb53534

  When using Kerberos/Active directory authentication to a Windows 2000 Active Directory, If the user is defined in the Active Directory as username “user” and has the principal name suffix “@domain.com”, then you should enable “Strip Realm” and make sure the authentication server is defined in a group.

- CSCeb59176

  Using release 4.0.1A or 4.0.1B, pinging from the VPN 3000 Concentrator under the Administration page of the management GUI to the peer’s network does not initiate any IPSec tunnel negotiation. Using the same configuration, a ping from the VPN Concentrator builds the tunnel with the peer if we downgrade to Release 4.0.1 or 3.X. (the VPN Concentrator’s private address is in the list of traffic to be encrypted, as defined in the IPSec LAN-to-LAN configuration).

- CSCeb65899

  A VPN 3000 Concentrator running Release 3.6.7 cannot decode the objects in the CA certificate or in the client certificate.

  The VPN 3000 Concentrator accepts the CA certificate and the certificate for the Concentrator, but it shows the Subject and Issuer as Unknown. When the client connects, it always ends in the Base group, not in the group matching the OU or the group matching the configuration.

- CSCeb67245

  When you change a VPN3005 from Master to Slave, you get the following javascript error.

  A Runtime Error has occurred.

  Do you wish to Debug?

  Line: 87

  Error: 'public_ipadddr' is null or not an object

  This occurs when the Public interface has the same value as the Public Group Shared Address. There is an extra 'd'.

- CSCeb77328

When using VRRP on a VPN 3000 Concentrator, L2TP/IPSec clients can not connect to the backup Concentrator when this one is active. Other IPSec clients (LAN-to-LAN, VPN Client) work fine.

- CSCeb78557

  A VPN 3000 Concentrator might report that the configuration is locked if an administrator goes to Administration | Administer Sessions and sorts by group. The concentrator shows 'configuration locked by console'.

  No other configuration can be done while the configuration is locked.

- CSCeb78773

  CiscoSecureACS does not display Caller ID for VPN 3000 Concentrator connections

- CSCec01487

  Using IMAP4S E-Mail Proxy issue on VPN 3000 Concentrators equipped with SEP-E module(s), the following problem occurs: while checking e-mail using an IMAP4S E-Mail Proxy, the process fails and the Mail Client returns the following errors:

  Your 'Inbox' folder was not polled for its unread count. Your server has unexpectedly terminated the connection. Possible causes for this include server problems, network problems, or a long period of inactivity. Account: 'pcuser IMAPS', Server: '100.160.100.14', Protocol: IMAP, Server Response: '', Port: 993, Secure(SSL): Yes, Error Number: 0x800CCC0F

  Header download for the 'Inbox' folder did not complete. Could not select 'Inbox' on the IMAP server. You might try refreshing your folder list to synchronize with the IMAP server. Account: 'pcuser IMAPS', Server: '100.160.100.14', Protocol: IMAP, Server Response: 'This IMAP command could not be sent to the server before the connection was terminated.', Port: 993, Secure(SSL): Yes, Error Number: 0x800CCC0F

- CSCec01582

  An exception in BMGT might occur immediately after loading Release 4.1 if a specific configuration combination, related to bandwidth management, exists.

  All of the following must be true in order to encounter this problem:

  Within the Group / Bandwidth settings:

  – A bandwidth management aggregate is set to any value.

– No policy is selected.

Within the interface settings:

– Bandwidth management is disabled.

– No policy is set at the interface.

There is a simple work around that prevents the exception without affecting the operation of the VPN 3000 Concentrator.

- CSCec04245

  If RIP listen is enabled and the number of learned routes exceeds the capacity of the routing table, an interface link down/link up causes some statically configured routes to show up as RIP routes. Other statically configured routes do not show up in the routing table at all.

  This can cause a failure in tunnel negotiation and data transmission, depending on the specific configuration of the network.

- CSCec10678

  LAN-to-LAN tunnels using 0.0.0.0 as the local or remote end can have issues routing traffic to connected clients, where traffic meant for the client gets routed over the LAN-to-LAN link.

- CSCec11767

  A small amount of memory leaks each time you perform an authentication server test from the web (or XML) interface.

- CSCec22680

  Username and password cannot be changed properly via XML.

- CSCec25392

  Users who have ACLs assigned to their profile might not be able to pass traffic after some time.

- CSCec28365

  Certificate group matching based on matching fields within the client's subject field fails.

  The indicating log message is:

  49795 07/31/2003 17:54:12.410 SEV=5 IKE/79 RPT=1026 10.229.61.227

  Group [PKI2-Test]

Validation of certificate successful

(CN=<unavailable>, SN=3D768903)

- CSCec43986

  After upgrading to 4.0.1.D or E, the VPN 3000 Concentrator tries to authenticate users to the Base Group instead of to the defined group. Errors on the logs add extra characters to the Group

- CSCec52144

  The way that Symantec's Raptor VPN deletes rekeyed IKE SAs is might cause traffic to the VPN 3000 Concentrator to stop flowing.

Caveats Resolved in Release 4.0.1

Release 4.0.1 resolves the following issues:

- CSCdu83085

  Autoupdate continues to retry even when tunnel fails.

- CSCdv51097

  The IPSec terminating interface is the External Interface, and the Inside Interface is the Private Interface. The Ethernet 2 (Public) interface has the Public Interface check box checked. but the Interface is set to “NOT CONFIGURED”. When this happens, all the IPSec/NAT connections fail by giving the error:

  Could not register UDP port for NAT enabled IPSec!

  Unchecking the public Interface check box when its not configured or giving it any bogus IP Address resolves the issue, and IPSec/NAT starts working fine.

- CSCdv87793

  If the DHCP Server address pool on the VPN 3002 is modified, it still renews IP Address from the previous address pool.

- CSCea21796

  The VPN3000 Concentrator will transmit data to exceed the negotiated Max Window Size. If going through a PIX edge firewall, the PIX shuts down the session when the window size is exceeded.

This occurs only when the ACKs coming back are delayed in transit.

The default window size for cTCP is 64K. The VPN Client and VPN3002 Hardware Client both generate ACKs at 8K intervals to avoid window issues. In this case the delays in ACK transport are significant enough that the window size is exceeded.

- CSCea45131

  VPN 3002 Ethernet ports might hang intermittently when connected to a Centercom hub.

- CSCea58142

  A VPN 3000 Concentrator running 3.6.7 cannot decode the objects in the CA certificate or in the Client certificate.

  The VPN 3000 Concentrator accepts the CA cert and the certificate for the Concentrator, but in Subject and Issuer, it shows Unknown. When the Client connects, it always ends up in the base group, not in the group matching the OU or the group matching config.

- CSCea69156

  LDAP Authorization to a Microsoft Active Directory LDAP server using authenticated Bind requests is not supported in this release. Only anonymous Binds are currently supported.

- CSCea72265

  When an SDI server is defined using its DNS hostname instead of its IP address, SDI authentications no longer function after the VPN Concentrator has been rebooted. A workaround is to use the IP address instead of the hostname of the SDI server.

- CSCea73064

  The fields on the LDAP Authorization configuration page have changed due to changes required to fix CSCea69156.

- CSCea74732

  Changing from DHCP to STATIC on an interface does not stop IP event logs 29 and 34 from showing in the filterable event log.

- CSCea83433

  With authentication set to Radius with Expiry, the user is prompted for username, password and domain name when connecting. The ACS authentication report shows “domain\username”, but the ACS accounting report page shows only the “username”.

Caveat Resolved in Release 4.0

Release 4.0 resolves the following issues:

- CSCdy09630

  The description of the IPSec Backup Servers feature in the VPN 3000 Concentrator Series Reference documentation indicates that it applies only to the VPN3002 Hardware Client. The feature now applies to the Software Client as well. For information about this feature and how to configure it, on the VPN Concentrator, see *VPN Client Administrator Guide*, Chapter 1. For information about how to configure Backup Servers in the VPN Client, see *VPN Client User Guide*.

- CSCdy12056

  If a LAN-to-LAN tunnel between a VPN 3000 Concentrator and an IOS device is misconfigured and repeatedly fails to establish, then the VPN 3000 Concentrator could enter a state where a reboot is required.

  One way to encounter this problem is to try to setup IOS to handle both LAN-to-LAN tunnels and Remote Access tunnels on the same interface, without breaking the IOS interface into V-LANs. This is a misconfiguration and is not supported by IOS, but it can lead to problems with the VPN 3000 Concentrator.

  This configuration is not supported because IOS does not allow the same crypto map to be used to terminate both LAN-to-LAN tunnels and Remote Access tunnels. In addition, IOS only allows one crypto map to be applied per interface.

  Consequently, if both types of tunnels must be terminated on a single physical interface, that interface must be broken out into V-LANs. Dividing the physical interface in this way enables a different crypto map to be applied to

each virtual interface. This in turn enables both types of tunnels to be terminated on the same physical interface while maintaining a valid configuration.

- CSCdy26296

  When viewing bandwidth management statistics via the CLI, with Bandwidth Management enabled and multiple users connected, all user sessions scroll through on the screen without the user being prompted to press space to continue or Q to quit.

- CSCdy28464

  Documentation for the Bandwidth Management feature in Release 3.6.1 refers to a configuration option in which bandwidth aggregation is automatically applied to a LAN-to-LAN connection when a bandwidth reservation policy is applied to a LAN-to-LAN connection. This feature is not available in Release 3.6.1.

  To ensure that bandwidth is always available for a LAN-to-LAN connection via the HTML interface, navigate to Configuration | User Management | Groups. Highlight the LAN-to-LAN group, and select the Assign Bandwidth Policies button. Select the public interface, and next to the Bandwidth Aggregation parameter, enter the amount of bandwidth to reserve from the total available bandwidth for this connection.

  If bandwidth aggregation is not set for a LAN-to-LAN connection, a situation might occur where there is not enough bandwidth available for the tunnel to be established.

- CSCdz48220

  The VPN 3000 Concentrator continually requests the node secret from the RSA server. The RSA server considers these requests as failed login attempts by the RSA server; therefore, the user's account is disabled.

  This problem occurs under the following conditions:

  – The VPN 3000 Concentrator does not have the node secret stored locally.

  – The VPN Client provides an incorrect passcode.

- CSCdz48332

  If you add and delete filters through the GUI interface (Configuration |System |Policy Management | Traffic Management | Filters), there is a very small memory leak for each filter created and deleted.

- CSCdz48402

  The VPN 3000 Concentrator does not consistently send Delete with Reason messages to all the connected clients when you do Reboot *NOW*. The VPN Clients believe they are still connected, but they will eventually disconnect due to the Client's Dead-Peer-Detection mechanism.

- CSCdz53656

  Authorization server statistics are not available in this release.

- CSCdz62206

  If you use Active Directory/Kerberos authentication on the VPN 3000 Concentrator and would like to authenticate to a Windows 2000 or .NET Active Directory server, you *must* change *all* the users' Account options to “Use DES encryption types for this account”. This is *required* because the Release 4.0 VPN 3000 Concentrator uses DES encryption, but Windows Active Directory uses RC4.

- CSCdz71450

  When using Active Directory/Kerberos for authentication, if the user types in the username or password incorrectly, the VPN 3000 Concentrator simply ends the connection after the first failure. The user should be prompted three times before failing as it does when using Internal, Radius, or NT Domain authentication methods.

- CSCdz77794

  On the Monitoring | Statistics | Authentication and Monitoring | Statistics | Accounting screens, if you click Reset, then all group-based statistics show up with the Group column=Base Group. In order to show group-based statistics again, click Restore.

- CSCdz78109

  SEP-E to SEP-E failover and SEP-E to software failover are *not* supported in Beta releases.

  New connections are not accepted after SEP-E failover with several calls previously connected and passing data.

- CSCdz79541

  Duplicate of CSCdz85139.

- CSCdz83301

  If a simple password is configured under the OSPF tab, in any of the interface configuration pages, the deleted entry will re-appear even after deleting the password, selecting none for OSPF authentication and clicking apply.

- CSCdz84481

  When a user fails authentication due to a restriction placed on the account at the Active Directory server, the VPN 3000 Concentrator Events do not display the reason for the failure. Some restrictions on the account could be Account Expired, Account Disabled, Account Locked-Out, Not within Logon Hours and Password Change required. For most of these restrictions you will see the following Events:

  124 01/20/2003 11:12:55.590 SEV=10 AUTHDECODE/43 RPT=4

  Kerberos: Error type: Client's creds have been revoked

  130 01/20/2003 11:12:55.590 SEV=4 AUTH/9 RPT=9 70.139.1.5

  Authentication failed: Reason = Invalid response received from server handle = 196, server = 198.133.219.25, user = myuser

- CSCdz85139

  When you add an LDAP Authorization server, the events refer to the server with "type=TACACS+."

- CSCdz87048

  The VPN 3000 Concentrator may leak memory when a VPN Client connects and downloads and ACL User Filter from the RADIUS Server. The amount of memory leaked is closely associated with the size of the actual filter.

- CSCdz87381

  If you externally authenticate Groups and Users to a RADIUS Server, the User filters assigned by the RADIUS Server get corrupted. It is recommended that you authenticate the Groups locally on the Concentrator and the Users externally on a RADIUS Server when utilizing the RADIUS User Filter feature.

- CSCea02122

  RADIUS based user filters are not cleared from the Concentrator when PPTP or L2TP connections are terminated.

- CSCea03407

  Using Netscape version 4.7, under Admin | Admin Sessions, the RADIUS User ACL filters get displayed in a narrow 1 inch wide column with no scroll capabilities. The filters are displayed correctly under Monitoring | Dynamic filters.

- CSCea12148

  If your VPN Concentrator has a SEP-E installed, you might see the following event message when you boot:

  CAPI-RSA PKCS1 payload to be decrypted is not in PKCS1 format, bad block type=[0x7][0xb8].

  If you receive this event, you will be unable to use HTTPS to manage the VPN Concentrator. To workaround this problem, delete the SSL certificate (from the Administration | Certificate Management screen), then generate a new SSL certificate.

- CSCea16255

  When Strip Realm is disabled, accounting requests should be sent as user name=user. But instead, accounting requests are incorrectly sent with user name=user@realm (Duplicate of CSCea44988).

- CSCea20412

  Using Authentication=RADIUS with Expiry, the VPN Concentrator establishes the tunnel but skips either RADIUS or LDAP authorization.

- CSCea24328

  When using Kerberos/Active Directory authentication, if a user types a username with the "@" symbol and Realm using all lowercase for the realm (that is, usernam@mycompany.com instead of username@MYCOMPANY.COM), the following error occurs on the VPN Concentrator, and the Kerberos server status changes to "Not-in-service".

  ```
  78 02/19/2003 16:59:49.250 SEV=7 AUTHDBG/76 RPT=8
  Unable to correlate received message with authentication session

  83 02/19/2003 16:59:53.150 SEV=4 AUTH/15 RPT=76
  Server name = 100.136.50.2, type = KERBEROS,
  group = KerberosGroup, status = Not-in-service
  ```

When using Kerberos/Active directory for authenticating, users should enter only their username, username@REALM.COM with Realm all in UPPERCASE letters, or use the Strip Realm setting for the Group on the Concentrator.

- CSCea25668

  Statically assigned filters take precedence over dynamically assigned filters. It should be the other way around.

- CSCea41973

  After upgrading from Release 3.6.7 to Release 3.6.7A (through Release 3.6.7.C), a VPN 3000 Concentrator does not redirect any traffic coming in from a vpn client to across Lan-to-LAN tunnel.

- CSCea46018

  When a backup SEP-E fails over to Software, the Activity LED and Status LED stay green, even though the SEP-E is no longer operational.

- CSCea48892

  PIX-to-PIX spoke connectivity when each PIX is connected LAN-to-LAN to a VPN 3015 Concentrator running Release 3.6.7.A is broken.

- CSCea69156

  LDAP Authorization to a Microsoft Active Directory LDAP server using authenticated Bind requests is not supported in this release. Only anonymous Binds are currently supported.

Documentation Updates

The Cisco VPN 3000 Series Concentrator documentation set has been revised for this release and is available online through Cisco Connection Online (CCO). This section contains any changes and corrections to the documentation that occurred after the documentation was published.

Documentation Changes

The following document requires modifications, reflecting product changes, as noted in the following sections:

- *VPN 3000 Series Concentrator Reference Volume I: Configuration*

Changes to *VPN 3000 Series Concentrator Reference Volume I: Configuration*

Please note the following changes to the Configuration manual.

Syslog Servers Now Supported on Both Windows and UNIX Operating Systems

The VPN 3000 Concentrator now supports syslog servers on both Windows and UNIX (Linux and Solaris) operating system platforms. In *VPN 3000 Series Concentrator Reference Volume I: Configuration*, Chapter 10, "Events," and in the corresponding online Help, the text and the screen captures refer to UNIX syslog servers. This restriction on the type of syslog server operating environment no longer exists.

Inbound Firewall Rules Must Not Limit Traffic to UDP Source Port 4500

In *VPN 3000 Series Concentrator Reference Volume I: Configuration*, Chapter 7, "Tunneling Protocols," make the following change to the note on page 7-35, under Tunneling Protocols | Configuration | System | Tunneling Protocol | IPsec | NAT Transparency area, regarding IPsec over NAT-T:

Note The source port of the client may vary from UDP 4500 especially when traversing a PAT device, so any inbound firewall rules must not specifically limit traffic to a source port of 4500.

VPN 3000 Concentrator Documentation Updates

These Release Notes are the only new documentation for Release 4.0.4.A. In addition to these Release Notes, the following documents were updated for Release 4.0:

- *VPN 3000 Series Concentrator Reference Volume I: Configuration*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management*
- *VPN 3000 Series Concentrator Getting Started*

- Online Help

Related Documentation

- *VPN Client User Guide for Windows*
- *VPN Client Administrator Guide*
- *VPN 3002 Hardware Client Getting Started*
- *VPN 3002 Hardware Client Reference*
- *VPN 3002 Hardware Client Quick Start Card*

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 Cisco Technical Support Website

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

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

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Support website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the

Cisco Technical support website. Cisco.com registered users have complete access to the technical support resources on the Cisco technical support website, including tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Support

Cisco Technical Support is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco Technical Support website and the Cisco Technical Support Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco Technical support inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.

- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco Technical Support Website

The Cisco Technical Support website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco Technical Support website, go to this URL:

http://www.cisco.com/techsupport

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco Technical Support website. Some services on the Cisco Technical Support website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco Technical Support website, you can open a case online at this URL:

http://www.cisco.com/techsupport and select "Open a case (service request)" and follow the instructions from there.

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco Technical Support Escalation Center

The Cisco Technical Support Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the Technical Support Escalation Center with a P1 or P2 problem, a Cisco Technical Support engineer automatically opens a case.

To obtain a directory of toll-free Cisco Technical Support telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips,

configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.