

Cisco VPN 5000 Concentrator and Client Frequently Asked Questions

Document ID: 6322

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, refer to the End-of-Sales Announcement.

Contents

Introduction

Why do I receive the "ERROR: InitSTEP returned. Cannot find STEP VxD" error in the VPN 5000 Client for Windows XP and how do I fix this?

Does the VPN 5000 Concentrator support the Native VPN Client found in Macintosh OS 10.3 (also known as Panther)?

I receive a kernel extension error when I try to run Cisco VPN 5000 5.2.2 Client on Macintosh OS X 10.3. What should I do?

When I use the Auto-Connect to Default Before Logon feature with a dialup connection, why is the user's phone book option grayed out?

What does "Error ID = -1" mean?

What do Error 0, Error 4, Error 6, Error 7, and Error 14 mean?

What are the Linksys® router issues with IPsec clients?

What are the allowed characters when you specify a user name for the VPN 5000 Client?

How many internal users can be defined on the VPN 5000 Concentrator?

How many tunnels can be configured on the VPN 5001, the VPN 5002, and the VPN 5008 Concentrators?

What do the **modinfo** and **dmesg** commands display?

How can I completely remove the Linux® client?

Can the VPN 5000 Client software exist on the same box with Nortel® Extranet Access Client or any other client? Is this supported?

Is there an available DES version of Macintosh OS X?

What are the indications that the VPN 5002 Concentrator runs hot?

Can H.323 sessions be supported using the VPN 5001 Concentrator and VPN 5000 Client software version 5.1.7?

In a LAN-to-LAN situation with a VPN 5000 Concentrator to a Cisco IOS® router, I notice that after one hour the rekeying is not synchronized between them. How can I fix this problem?

What does the "<local7.warn>macypn fTCP ERR: Unknown next_proto, 69 from 172.21.139.5" error message mean?

Related Information

Introduction

This document addresses frequently asked questions about the Cisco VPN 5000 Series Concentrator and the Cisco VPN 5000 Client.

For more information on document conventions, see the Cisco Technical Tips Conventions.

Q. Why do I receive the "ERROR: InitSTEP returned. Cannot find STEP VxD" error in the VPN 5000 Client for Windows XP and how do I fix this?

A. This error occurs anytime the VPN Client cannot be binded, or the necessary VPN services are not accessible. The VPN 5000 Client for Windows XP includes a setup program that automatically launches a program to install the network driver. If the program fails for any reason, use this procedure to manually install the network driver.

1. Install the VPN Client software using the Installing the VPN Client for Windows XP section.
2. Log into the system as the administrator, or as a user with administrator privileges.
3. Select **Start > Settings > Network and Internet Connections > Network Connections**.
4. Double-click the appropriate Local Area Connection.
5. Click **Properties**.
6. Click **Install**.
7. Select **Service**.
8. Click **Add**.
9. Click **Have Disk**.
10. Enter the path to the folder in which the netcs.inf, netcs_m.inf, and step.sys files reside. In most cases, this is the same folder as the VPN Client install file.
11. Click **OK** to install the driver.
12. After the driver is installed, close the Network and Dial-up Connections window.
13. Reboot your computer.

Q. Does the VPN 5000 Concentrator support the Native VPN Client found in Macintosh OS 10.3 (also known as Panther)?

A. The VPN 5000 Concentrator has not been tested with anything beyond Macintosh Operating System (OS) 10.1.5. No support can be claimed for the Panther release. It has never been looked at in the context of the VPN 5000 Concentrator, only for that of the Cisco VPN Client. If later OS support is needed, consider moving to the Cisco VPN Client. Additionally, the Native VPN Client in 10.3 is IPSec over Layer 2 Tunneling Protocol (L2TP), which is not supported in the VPN 5000 Concentrator.

Q. I receive a kernel extension error when I try to run Cisco VPN 5000 5.2.2 Client on Macintosh OS X 10.3. What should I do?

A. As stated in the Release Notes for the Cisco VPN 5000 Client Version 5.2.3 for Macintosh Operating System (OS) X, the Cisco VPN 5000 Client is supported up to version 10.1.x. It is not supported on version 10.3. It is possible, however, to make the VPN Client work. Reset the permissions on two of the installed files after you run the install script. This output is an example.

Note: This configuration is not supported by Cisco.

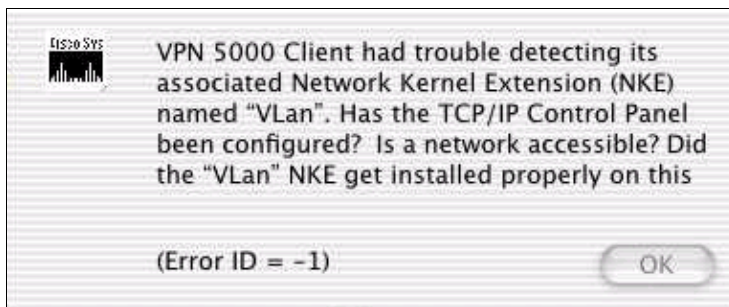
```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. When I use the Auto-Connect to Default Before Logon feature with a dialup connection, why is the user's phone book option grayed out?

A. The typical reason this happens is because of a partial, incorrect, or missing installation of the Registration, Admission, and Status Protocol (RAS) on the system. Instead of performing a reinstall on the VPN Client, try to uninstall and reinstall Windows RAS.

Q. What does "Error ID = -1" mean?

A. This is a Macintosh Operating System (OS) error message that occurs when the VPN 5000 Client version 10.0 is installed on the Macintosh OS 10.1, which is not yet supported. The error is indicative of a kernel mismatch. Refer to the Bug Toolkit (registered customers only) to look up more information on Cisco bug ID CSCdv57716. This is a sample of the error:



Q. What do Error 0, Error 4, Error 6, Error 7, and Error 14 mean?

A. This list explains their meanings:

- ◆ **Error 0** This error occurs when no Internet Key Exchange (IKE) Policy section has been configured for the VPN 5000 Concentrator, or if an IKE configuration has not been configured for that VPN Group configuration.
- ◆ **Error 4** No VPN resources are available on the VPN 5000 Concentrator. This means that the VPN 5000 Concentrator has reached the maximum connections for this group. It can also mean that the configuration contains a LocalIPNet with an improper syntax such as "LocalIPNet=204.144.171.64" (there should be a /26 or another mask defined).
- ◆ **Error 6** If the VPN 5000 Concentrator was configured for a user name "Bob" and the user puts in "bob" (with the correct password), then the VPN 5000 Concentrator returns a VPN Server Error 6. If the user puts in "Bob" and the wrong password, then the VPN 5000 Concentrator also returns an Error 6. If the VPN 5000 Concentrator runs DES code and tries to use a 3DES Transform, such as ESP (MD5, 3DES), then Error 6 is returned to the VPN 5000 Client. Non-export code (3DES) has a "US" after it (for example, version 5.0US), and it is able to use 3DES encryption methods. All Cisco VPN 5000 Concentrators are shipped with DES code. Delete the 3DES Transform and use another if you only use DES code.
- ◆ **Error 7** This error means that your VPN 5000 Concentrator is configured with an IKE Policy that is currently inactive for the code version. Currently, for version 5.x code, all 3DES and G2 policies are inactive. Remove those and set the IKE Policy to either MD5_DES_G1 or SHA_DES_G1.
- ◆ **Error 14** This is a RADIUS error where the VPN 5000 Concentrator does not receive the correct information from the RADIUS server to allow the VPN 5000 Client to log in.
- ◆ **Affected Products:**

- ◇ Windows 95–98 VPN Client for the Cisco VPN 5000 Concentrator Series
- ◇ Windows NT 4.0 VPN Client for the Cisco VPN 5000 Concentrator Series

- ◇ Macintosh Operating System (OS) VPN Client for the Cisco VPN 5000 Concentrator Series
- ◇ Linux Kernel 2.2.5 VPN Client for the Cisco VPN 5000 Concentrator Series
- ◇ SPARC Solaris VPN Client for the Cisco VPN 5000 Concentrator Series
- ◇ Cisco VPN 5001 Concentrator
- ◇ Cisco VPN 5002 Concentrator
- ◇ Cisco VPN 5008 Concentrator

◆ **Affected Versions:**

- ◇ All 5.x versions

Q. What are the Linksys® router issues with IPSec clients?

A. Linksys® routers support IPSec connections only on firmware versions 1.34 or later (1.39 is the latest version). The IPSec pass through should be enabled on the Linksys® router.

Q. What are the allowed characters when you specify a user name for the VPN 5000 Client?

A. The user name and domain are case sensitive and can be between 1 and 60 alphanumeric characters combined. This includes the "at" sign (@). Refer to VPN Users for more details.

This user name is illegal (the "-" character is invalid):

```
[ VPN Users ]
user-2 Config="test" SharedKey="cisco"
```

Q. How many internal users can be defined on the VPN 5000 Concentrator?

A. It is always recommended that you use RADIUS or Secure ID (SDI) authentication for large implementations. The number of internal users are subject to the size of your configuration. The maximum configuration size is 65,500 bytes. In order to see this, review the last line of the **show configuration** command output. For example:

```
Configuration size is 6732 out of 65500 bytes.
```

Q. How many tunnels can be configured on the VPN 5001, the VPN 5002, and the VPN 5008 Concentrators?

A. The VPN 5001 Concentrator can support up to 1,500 tunnels, the VPN 5002 Concentrator can support up to 10,000 tunnels, and the VPN 5008 Concentrator can support up to 40,000 tunnels per line card.

Q. What do the modinfo and dmesg commands display?

A. The **modinfo** command displays what and how many modules are loaded. The **dmesg** command displays bootup syslog messages.

Q. How can I completely remove the Linux® client?

A. At installation, these files are created, or placed on your system:

- ◆ **/etc/vpn_config** It is recommended that you keep this one because it is the VPN 5000 Client configuration.
- ◆ **/etc/rc.d/init.d/vpn** This is the boot-time script that loads the "vpnmod" kernel module.
- ◆ **/etc/rc.d/rc3.d/s85.vpn** This is a link to /etc/rc.d/init.d/vpn.
- ◆ **/etc/rc.d/rc5.d/s85.vpn** This is a link to /etc/rc.d/init.d/vpn.
- ◆ **/usr/local/bin/open_tunnel** This opens the tunnel connection.
- ◆ **/usr/local/bin/close_tunnel** This closes the tunnel.
- ◆ **/usr/local/bin/vpn_control** This is a troubleshooting tool used to turn on debug flags. It is mostly used in development.
- ◆ **/lib/modules/<kernelversion>/COMPvpn/vpnmod** This is the kernel module. Execute the **uname -r** command to determine the <kernelversion>.

If you delete these files, then reboot, you effectively uninstall your client. Alternatively, you can run **/usr/local/bin/close_tunnel** and **/etc/rc.d/init.d/vpnstop**, and then delete the above files.

The **/etc/vpn_config** file is the client configuration. It contains the server, user name, and password information. If you plan to reinstall the VPN Client, it is recommended that you keep a copy of this file.

Q. Can the VPN 5000 Client software exist on the same box with Nortel® Extranet Access Client or any other client? Is this supported?

A. Cisco VPN Client version 4.0 and later can coexist. Refer to the Coexistence with Third-Party VPN Vendors section of the Release Notes for VPN Client, Release 4.0.

Q. Is there an available DES version of Macintosh OS X?

A. No, but there is a 3DES version available.

Q. What are the indications that the VPN 5002 Concentrator runs hot?

A. If the Over Temp LED on an Extended Services Processor (ESP) card in the VPN 5002 Concentrator is lit, or if there are other temperature problems with the unit, it can be that the built-in air filter is clogged with dirt and impeding air flow. In order to replace the air filter, consult Replacing the Air Filter for further instructions.

Q. Can H.323 sessions be supported using the VPN 5001 Concentrator and VPN 5000 Client software version 5.1.7?

A. No, they cannot be supported because the IP address is embedded in the data portion of the packet. The VPN 5000 Client cannot access or modify this address.

Q. In a LAN-to-LAN situation with a VPN 5000 Concentrator to a Cisco IOS® router, I notice that after one hour the rekeying is not synchronized between them. How can I fix this problem?

A. This problem is usually solved by setting "keymanage=reliable" on the VPN 5000 Concentrator configuration. However, it does not work when the Cisco IOS device has a dynamic IP address.

Q. What does the "<local7.warn>macvpn fTCP ERR: Unknown next_proto, 69 from 172.21.139.5" error message mean?

A. The fake TCP (fTCP) message appears when the VPN Concentrator receives a packet with port 80, and after removing the headers, has not found an ESP packet. The VPN Concentrator only takes IPSec (ESP) packets and anything else is dropped. When the Code Red worm was released on the Internet, this warning filled up the syslog buffer on many customer machines. This error message can indicate that your machine is infected and is trying to access the VPN 5000 Concentrator, via port fTCP.

Related Information

- [Cisco VPN 5000 Series Concentrators End-of-Sales Announcement](#)
- [Cisco VPN 5000 Series Concentrators Support Page](#)
- [Cisco VPN 5000 Client Support Page](#)
- [IPSec \(IP Security Protocol\) Support Page](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 02, 2008

Document ID: 6322
