Cisco VPN 3000 Concentrator FAQ

Contents

Introduction

This document answers frequently asked questions (FAQs) about the Cisco VPN 3000 Series Concentrator.

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

General

Q. What does the error message "`Lost Service`" mean?

A. If there is no traffic sent between the VPN Concentrator and the VPN Client for a period of time, a Dead Peer Detection (DPD) packet is sent from the VPN Concentrator to the VPN Client to ensure its peer is still there. If there is a connectivity issue between the two peers where the VPN Client does not respond to the VPN Concentrator, the VPN Concentrator continues to send DPD packets over a period of time. This terminates the tunnel and generates the error if it does not receive a response during that time. Refer to Cisco bug ID CSCdz45586 (Support contract required).

The error should look like this:

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

Cause: The remote IKE peer did not respond to keepalives within the expected window of time, so the connection to the IKE peer was deleted. The message includes the keep-alive mechanism used. This issue is only reproducible if the public interface is disconnected during an active tunnel session. The customer needs to monitor their network connectivity as these events are generated to pinpoint the root cause of their potential network connectivity issue(s).

Disable IKE keepalive by going to **%System Root%\Program Files\Cisco Systems\VPN Client\Profiles** on the Client PC that experiences the issue, and edit the **PCF file** (where applicable) for the connection.

Change the 'ForceKeepAlives=0' (default) to '**ForceKeepAlives=1**'.

If the problem persists, open a Service Request with Cisco Technical Support and provide the Client "Log Viewer" and the VPN Concentrator logs as the problem occurs.

Q. What does the error message "q_send" failures detected for EMQ1 queue mean?

A. This error message occurs when there are too many debug events / information in the buffer. It has no negative impact other than possibly losing a few event messages. Try to reduce the events to the minimum number needed to prevent the message.

Q. My deleted group still shows in the VPN Concentrator configuration. How do I delete this?

A. Copy the configuration into a text editor (such as Notepad) and manually edit or delete the affected group information denoted by **[ipaddrgrouppool #.0]**. Save the configuration and upload it to the VPN Concentrator. An example is shown here.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than
0). [ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1
endaddr=172.18.124.2
```

Q. Is it possible to have multiple primary SDI servers?

A. The VPN 3000 Concentrators are only able to download one node secret file at a time. In SDI Version pre-5.0, you can add multiple SDI servers, but they must all share the same node secret file (think of it as the primary and backup servers). In SDI Version 5.0, you are only able to enter the one primary SDI server (the backup servers are listed in the node secret file) and replica servers.

Q. I am getting an "SSL certificate will expire in 28 days" Issuer error message. What should I do?

A. The message indicates that your Secure Socket Layer (SSL) certificate will expire in 28 days. This certificate is used to browse into the web management via HTTPS. You can leave the certificate with the default settings, or you can configure different options before you generate the new certificate. Select **Configuration > System > Management Protocols > SSL** to do this. Select **Administration > Certificate Management** and click **Generate** to renew the certificate.

If you are concerned about security on your VPN Concentrator and would like to prevent unauthorized access, disable HTTP and / or HTTPS on the public interface by going to **Configuration > Policy Management > Traffic Management > Filters**. If you need to get to your VPN Concentrator over the Internet via HTTP or HTTPS, then you can specify access based on source address by going to **Administration > Access Rights > Access Control List**. You can use the help menu on the top right corner of the window to get more information.

Q. How can I view the user information in the internal user database? It is not visible when I look in the config file.

A. Select **Administration > Access Rights > Access Settings**, choose **Config File Encryption=None**, and save the config to view users and passwords. You should be able to search for the specific user.

Q. How many users can the internal database store?

A. The number of users is version-dependent and specified in the **Configuration > User Management** section of the User Guide for your VPN 3000 Concentrator release. A total of 100 users or groups (the sum of users and groups must equal 100 or less) is possible in VPN 3000 Releases 2.2 through 2.5.2. In VPN 3000 Releases 3.0 and later, the number for the 3005 and 3015 Concentrators remains at 100. For the VPN 3030 and 3020 Concentrator, the number is 500, for the VPN 3060 or 3080 Concentrators, the number is 1000. Also, using an external authentication server improves scalability and manageability.

Q. What is the difference between the tunnel default gateway and the default gateway?

A. The VPN 3000 Concentrator uses the tunnel default gateway to route the tunneled users within the private network (usually the inside router). The VPN Concentrator uses the default gateway to route packets to the Internet (usually the outside router).

Q. If I place my VPN 3000 Concentrator behind a firewall or router running access control lists, which ports and protocols do I need to allow through?

A. This chart lists ports and protocols.

Service	Protocol Number	Source Port	Destination Port
PPTP Control Connection	6 (TCP)	1023	1723
PPTP Tunnel Encapsulation	47 (GRE)	N/A	N/A
ISAKMP/IPSec Key Management	17 (UDP)	500	500
IPSec Tunnel Encapsulation	50 (ESP)	N/A	N/A
IPSec NAT Transparency	17 (UDP)	10000 (default)	10000 (default)

Note: The Network Address Translation (NAT) Transparency port is configurable to any value in the 4001 through 49151 range. In versions 3.5 or later, you can configure IPsec over TCP by going to **Configuration > System > Tunneling Protocols > IPSec > IPSec over TCP**. You can enter up to 10 comma-separated TCP ports (1 - 65535). If this option is configured, make sure that these ports are allowed in your firewall or router running access-control lists.

Q. How can I set the VPN Concentrator back to factory defaults?

A. From the File Management screen, delete the "config" file and reboot. If this file is deleted accidentally, a backup copy, "config.bak" is kept.

Q. Can I use TACACS+ for Administrative authentication? What should I keep in mind while I do it?

A. Yes, starting in VPN 3000 Concentrator Release 3.0, you can use a TACACS+ for Administrative authentication. After you configure TACACS+, make sure you test authentication before you log out. Improper configuration of TACACS+ can lock you out. This requires a console port login in order to disable TACACS+ and rectify the problem.

Q. What do I do when the administrative password is forgotten?

A. In versions 2.5.1 and later, connect a PC to the console port of the VPN Concentrator using a straight-through RS-232 serial cable with the PC set for:

- 9600 bits per second
- 8 data bits
- no parity
- 1 stop bit
- hardware flow control on
- VT100 emulation

Reboot the VPN Concentrator. After the diagnostic check is complete, a line of three dots (...) appears on the console. Press **CTRL-C** within three seconds after these dots appear. A menu displays that lets you reset the system passwords to their defaults.

Q. What is the purpose of the group name and group password?

A. The group name and group password are used to create a hash which is then used to create a security association.

Q. Does the VPN Concentrator proxy ARP on behalf of tunneled users?

A. Yes.

Q. Where do I place the VPN 3000 Concentrator in regard to my network firewall?

A. The VPN 3000 Concentrator can be placed in front of, behind, parallel to, or in the demilitarized zone (DMZ) of a firewall. It is not advisable to have the public and private interfaces in the same virtual LAN (VLAN).

Q. Is there any way to disable proxy ARP on the Cisco VPN 3000 Concentrator?

A. Proxy Address Resolution Protocol (ARP) cannot be disabled on the Cisco VPN 3000 Concentrator.

Q. Where can I find bugs filed against the VPN 3000 Concentrator?

A. Users can use the Bug Search Tool (Support contract required) to find detailed information

about bugs.

Q. Where can I find configuration examples for the VPN 3000 Concentrator?

A. In addition to the VPN 3000 Concentrator documentation, more configuration examples can be found on the Cisco VPN 3000 Series Concentrator Support Page.

Q. How can I increase the logging to get better debugs for specific events?

A. You can go to **Configuration > System > Events > Classes** and configure the specific events (such as IPsec or PPTP) to get better debugs. Debugging should only be turned on for the duration of the troubleshooting exercise because it can cause performance degradation. For IPsec debug, turn on IKE, IKEDBG, IPSEC, IPSECDBG, AUTH, and AUTHDBG. If using certificates, then add the CERT class to the list.

Q. How can I monitor the traffic to the VPN 3000 Concentrator?

A. The HTML interface that comes with the VPN 3000 Concentrator allows you to have basic monitoring functionality if you look under **Monitoring > Sessions**. The VPN 3000 Concentrator can also be monitored through Simple Network Management Protocol (SNMP) using an SNMP manager of your choice. Alternatively, you can purchase the Cisco VPN / Security Management Solution (VMS). The Cisco VMS provides key functionality to assist you if you deploy the VPN 3000 Concentrator Series and require in-depth monitoring of remote access and site-to-site VPNs, based upon IPsec, L2TP, and PPTP. Refer to the VPN Security Management Solution for more details about VMS.

Q. Does the Cisco VPN 3000 Concentrator Series have an integrated firewall? If so, what features are supported?

A. While the series has integrated stateless port / filtering capabilities and NAT, Cisco suggests you use a device like the Cisco Secure PIX Firewall for the corporate firewall.

Q. What routing options and VPN protocols are supported by the Cisco VPN 3000 Concentrator Series?

A. The series supports these routing options:

- Routing Information Protocol (RIP)
- RIP2
- Open Shortest Path First (OSPF)
- static routes
- Virtual Router Redundancy Protocol (VRRP)

Supported VPN protocols include Point-to-Point Tunneling Protocol (PPTP), L2TP, L2TP / IPsec, and IPsec with or without a NAT device between the VPN 3000 and the end client. IPsec through NAT is known as NAT Transparency.

Q. What authentication mechanisms / systems does the Cisco VPN 3000 Concentrator Series support for client PCs?

A. NT Domain, RADIUS or RADIUS proxy, RSA Security SecurID (SDI), Digital Certificates, and internal authentication are supported.

Q. Can I do static Network Address Translation (NAT) for users going out through the VPN 3000 Concentrator?

A. You can only do Port Address Translation (PAT) for the users going out. You cannot do static NAT on the VPN 3000 Concentrator.

Q. How can I assign a static IP address to a specific Point-to-Point Tunneling Protocol (PPTP) or IPsec user through the VPN 3000 Concentrator?

A. This list explains how to assign static IP addresses:

- **PPTP users**In the IP Address Management section, in addition to choosing your pool or Dynamic Host Configuration Protocol (DHCP) options, check the **Use Client Address** option. Then, define the user and the IP address in the VPN 3000 Concentrator. This user always get the IP address configured in the VPN Concentrator when connecting.
- **IPsec users**In the IP Address Management section, in addition to choosing to your pool or DHCP options, check the **Use Address from Authentication Server** option. Then, define the user and the IP address in the VPN 3000 Concentrator. This user always gets the IP address configured in the VPN Concentrator when connecting. All others that belong to the same group or to other groups gets an IP address from the global pool or DHCP.With the Cisco VPN 3000 Concentrator software version 3.0 and later, you have the option to configure an address pool on a group basis. This feature can help you to assign a static IP address to a specific user as well. If you configure a pool for a group, the user with static IP gets the IP address assigned to them, and other members of the same group get IP addresses from the group pool. This only applies when you use the VPN Concentrator as an authentication server.

Note: If you use an external authentication server, then you need to use the external server to assign the addresses correctly.

Q. What are some known compatibility issues with Microsoft's PPTP products and the VPN 3000 Concentrator?

A. This information is based on VPN 3000 Series Concentrator Software Release 3.5 and later; VPN 3000 Series Concentrators, Models 3005, 3015, 3020, 3030, 3060, 3080; and Microsoft Operating Systems Windows 95 and later.

- **Windows 95 Dial-Up Networking (DUN) 1.2**Microsoft Point-to-Point Encryption (MPPE) is not supported under DUN 1.2. To connect using MPPE, install Windows 95 DUN 1.3. You can download the Microsoft DUN 1.3 upgrade from the Microsoft web site.
- **Windows NT 4.0**Windows NT is fully supported for Point-to-Point Tunneling Protocol (PPTP) connections to the VPN Concentrator. Service Pack 3 (SP3) or later is required. If you are running SP3, you should install the PPTP Performance and Security patches. Refer to the Microsoft web site for information about the Microsoft PPTP Performance and Security Upgrade for WinNT 4.0 .Note that the 128-bit Service Pack 5 does not handle MPPE keys correctly, and PPTP can fail to pass data. When this occurs, the event log shows this

message:

```
103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4
User [ testuser ]
disconnected. Experiencing excessive packet decrypt failure.
```

To solve this problem, download the upgrade for How to obtain the latest Windows NT Service Pack 6a and Windows NT 4.0 Service Pack 6a Available. Refer to the Microsoft article MPPE Keys Not Handled Correctly for a 128-Bit MS-CHAP Request for more information.

Q. What is the maximum number of filters allowed on a VPN 3000 Concentrator?

A. The maximum number of filters that you can add on a VPN 30xx unit (even a 3030 or 3060) is fixed at 100. Users can find additional information about this issue by viewing Cisco bug ID CSCdw86558 (Support contract required).

Q. What is the maximum number of routes in the 30xx line of VPN Concentrators?

A. The maximum number of routes are:

- The VPN 3005 Concentrator previously held a maximum of 200 routes. This number has now increased to 350 routes. Refer to Cisco bug ID CSCeb35779 (Support contract required) for more details.
- The VPN 3030 Concentrator has been tested up to 10,000 routes.
- The routing table limit on the VPN 3030, 3060, and 3080 Concentrators is proportional to the available resources / memory in each device.
- The VPN 3015 Concentrator has no predefined maximum limit. This holds true for Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) protocol.
- The VPN 3020 Concentrator - 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.

Q. How do I completely clear the interface statistics on the VPN 3000 Concentrator?

A. Select **Monitoring > Statistics > MIB-II > Ethernet** and reset the statistics to clear statistics for the current session. Remember that this does not totally clear the statistics. You need to reboot to actually reset the statistics (versus resetting for monitoring purposes).

Q. What ports should I allow on the VPN Concentrator for Network Time Protocol (NTP) communication?

A. Allow TCP and UDP port 123.

Q. What are the functions of UDP ports 625xx?

A. The ports are used for the VPN Client communication between the actual shim / Deterministic

NDIS Extender (DNE) and the TCP / IP stack of the PC, and are for internal developmental use only. For example, port 62515 is used by the VPN Client for sending information to the VPN Client log. Other port functions are shown here.

- 62514 - Cisco Systems, Inc. VPN Service to Cisco Systems IPsec Driver
- 62515 - Cisco Systems IPsec Driver to Cisco Systems, Inc. VPN Service
- 62516 - Cisco Systems, Inc. VPN Service to XAUTH
- 62517 - XAUTH to Cisco Systems, Inc. VPN Service
- 62518 - Cisco Systems, Inc. VPN Service to CLI
- 62519 - CLI to Cisco Systems, Inc VPN Service
- 62520 - Cisco Systems, Inc. VPN Service to UI
- 62521 - UI to Cisco Systems, Inc. VPN Service
- 62522 - Log Messages
- 62523 - Connection Manager to Cisco Systems, Inc. VPN Service
- 62524 - PPPTool to Cisco Systems, Inc. VPN Service

Q. Can I remove the WebVPN floating bar?

A. You cannot remove the floating tool bar nor avoid loading the floating toolbar while you establish the WebVPN session. This is because when you close this window the session is terminated immediately and when you try to login again the window is loaded again. This is the way the WebVPN sessions were designed originally. You can close the main window but it is not possible to close the floating window.

Software

Q. Does WebVPN support Outlook Web Access (OWA) 2003?

A. OWA 2003 support for WebVPN on the VPN 3000 Concentrator is now available with version 4.1.7 downloads (Support contract required).

Q. Where can I get the latest software revisions for the VPN 3000 Concentrator?

A. All Cisco VPN 3000 Concentrators ship with the most current code, but users can check the downloads (Support contract required) to see if more current software is available.

Refer to the Cisco VPN 3000 Series Concentrator documentation page for the latest documentation on the VPN 3000 Concentrator.

Q. Do I need a TFTP server to upgrade the VPN 3000 Concentrator? Is there an alternative way to upgrade the box?

A. In addition to using TFTP, you can upgrade the VPN Concentrator by downloading the latest software onto your hard drive. Then, from a browser on the system where the software is located, go to **Administration > Software Update** and find the downloaded software on your hard drive (just like opening a file). When you find it, select the **Upload** tab.

Q. What does the "k9" signify in the latest code names (such as in "vpn3000-3.0.4.Rel-k9.bin")?

A. The "k9" designation for the image name has replaced the originally used 3DES designation (for example, vpn3000-2.5.2.F-3des.bin). Thus, the "k9" now signifies that this is a 3DES image.

Q. Should I use the Data Compression option under the IPsec group for all my users?

A. Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the VPN Concentrator. For this reason, Cisco recommends that you enable data compression only if every member of the group is a remote user that connects with a modem. If any member of the group connects through broadband, do not enable data compression for the group. Instead, divide the group into two groups, one for modem users and the other for broadband users. Enable data compression only for the group of modem users.

Other Advanced Features

Q. Does load balancing work with LAN-to-LAN connections?

A. Load balancing is effective only on remote sessions initiated with the Cisco VPN Software Client (Release 3.0 and later). All other clients (PPTP, L2TP) and LAN-to-LAN connections can connect to a VPN Concentrator on which load balancing is enabled, but they cannot participate in load balancing.

Q. How do I decrypt the passwords from the config file?

A. Go to **Configuration > System > Management Protocols > XML** and then to **administration | file management select XML format**. Use the same name, or different, and open the file in order to view the passwords.

Q. Can I use Virtual Router Redundancy Protocol (VRRP) and load balancing together?

A. You cannot use load balancing with VRRP. In a VRRP configuration, the backup device remains idle unless the active VPN Concentrator fails. In a load balancing configuration, there are no idle devices.

Q. Does all remote access client VPN traffic have to go through an encrypted tunnel to the VPN Concentrator at the enterprise or service provider? For example, can plain web access to other sites go in the open, directly through the ISP's Internet connection?

A. Yes. This concept is known as "split tunneling." Split tunneling allows for secure access to corporate resources through an encrypted tunnel while it allows Internet access directly through the ISP's resources (this eliminates the corporate network from the path for web access). The Cisco VPN 3000 Concentrator Series to both the Cisco VPN Client and the VPN 3002 Hardware

Client can support split tunneling. For additional security, this feature is controllable by the administrator of the VPN Concentrator and not the user.

Q. Is it safe to use split tunneling?

A. Split tunneling allows you to have the convenience of browsing the Internet while connected through the VPN tunnel. However, it does pose us some risk if the VPN user connected to the corporate network is vulnerable to attacks. It is recommended that the users use a personal firewall in that case. The release notes for any given VPN Client version discuss interoperability with personal firewalls.

Q. How does load balancing work on the Cisco VPN 3000 Concentrator?

A. Load is calculated as a percentage derived from the active connections divided by the maximum configured connections. The director always tries to have the least load because it is burdened with the additional (inherent) load of maintaining all of the administrative LAN-to-LAN sessions, calculating all other cluster member loading, and it is responsible for all client redirects.

For a newly configured functional cluster, the director has about a 1 percent load before any connections have been established. Therefore, the director redirects connections to the backup concentrator until the percentage of load on the backup is higher than the percentage of load on the director. For example, given two VPN 3030 Concentrators in "idle" states, the director has a 1 percent load. The secondary is given 30 connections (2 percent load) before the director accepts connections.

In order to verify that the director accepts connections, go to **Configuration > System > General > Sessions** and lower the maximum number of connections to an artificially low number to quickly increase the load placed on the backup VPN Concentrator.

Q. How many headend devices can the VPN Monitor track?

A. The VPN Monitor can track 20 headend devices. In a hub-and-spoke scenario, connections from remote sites are monitored at the headend. There is no need to monitor all the remote sites and users since that information can be traced on the hub router. These headend devices can support up to 20,000 remote users or 2,500 remote sites. A dual-homed VPN device that goes out to the spoke sites counts as two of the 20 maximum devices that can be monitored.

Related Information

- **Cisco VPN 3000 Concentrator Support Page**
- **Cisco VPN 3000 Client Support Page**
- **Technical Support & Documentation - Cisco Systems**