Cisco VPN 3000集中器常见问题

目录

简介

本文档旨在回答有关 Cisco VPN 3000 系列集中器的一些常见问题 (FAQ)。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

一般问题

Q. 错误消息“Lost Service”是什么意思？

A. 如果在一段时间内 VPN 集中器与 VPN 客户端之间没有数据流发送，则会从 VPN 集中器向 VPN 客户端发送一个失效对等体检测 (DPD) 数据包以确保其对等体仍然存在。如果两个对等体之间出现连接问题，使得 VPN 客户端未能响应 VPN 集中器，VPN 集中器会继续在一段时间内发送 DPD 数据包。如果在该时间内未收到响应，这将终止隧道并生成错误。请参阅 Cisco Bug ID CSCdz45586（仅限注册用户）。

该错误类似如下所示：

```
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)
```

原因：远程 IKE 对等体未能在预期时间段内响应 Keepalives，因此与 IKE 对等体的连接被删除。消息中包含使用的保活机制。仅当在活动隧道会话期间断开公共接口的连接时，才会重现此问题。用户需要监控其网络连接，因为所生成的这些事件可用于查明其潜在网络连接问题的根本原因。

在发生问题的客户端 PC 上，转到 **%System Root%\Program Files\Cisco Systems\VPN Client\Profiles** 以禁用 IKE Keepalive，并编辑连接的 **PCF** 文件（如果适用）。

将 **ForceKeepAlives=0**（默认值）更改为 ForceKeepAlives=1。

如果问题仍然存在，请通过 Cisco 技术支持提出服务请求并提供问题发生时的客户端“日志查看器”日志和 VPN 集中器日志。

Q. 为 EMQ1 队列检测到的错误消息“q_send”失败是什么意思？

A. 当缓冲区中的调试事件/信息过多时就会出现此错误消息。除了可能丢失一些事件消息外，它没有什么负面影响。请尝试将事件减少为所需的最小数量以防止出现该消息。

Q. 删除后的组仍显示在 VPN 集中器配置中。如何将其删除？

A. 复制配置到文本编辑器(例如Notepad)，手工编辑或者删除受影响的组信息，表示为[ipaddrgrouppool-.0]。保存配置并将其上载至 VPN 集中器。此处给出了一个示例。

```
!--- 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. 能否具有多个主 SDI 服务器？

A. VPN 3000 集中器每次只能下载一个节点密钥文件。在 5.0 之前的 SDI 版本中，您可以添加多个 SDI 服务器，但它们必须共享相同的节点密钥文件（可将其视为主服务器和备份服务器）。在 SDI 版本 5.0 中，您只能输入一个主 SDI 服务器（备份服务器列在节点密钥文件中）和多个复本服务器。

Q. 我收到“SSL certificate will expire in 28 days”颁发者错误消息。我该怎么办？

A. 该消息表明您的安全套接字层 (SSL) 证书将在 28 天后过期。该证书用于通过 HTTPS 浏览 Web 管理。您可以保留证书的默认设置，也可以在生成新证书之前配置不同的选项。为此，请选择 **Configuration > System > Management Protocols > SSL**。要更新证书，请选择 **Administration > Certificate Management** 并单击 **Generate**。

如果您关注 VPN 集中器的安全并希望防止未经授权的访问，请转到 **Configuration > Policy Management > Traffic Management > Filters** 以禁用公共接口上的 HTTP 和/或 HTTPS。如果需要使用 HTTP 或 HTTPS 通过 Internet 访问您的 VPN 集中器，可转到 **Administration > Access Rights > Access Control List** 并基于源地址指定访问权限。您可以使用窗口右上角的帮助菜单以获取更多信息。

Q. 如何能够查看内部用户数据库中的用户信息？我在配置文件中看不到它。

A. 选择 Administration > Access Rights > Access Settings，选择 Config File Encryption=None 并保存配置文件即可查看用户和口令。您应当能够搜索特定用户。

Q. 内部数据库能存储多少用户？

A. 用户数取决于版本，您的 VPN 3000 集中器版本的用户指南的**配置 > 用户管理**部分指定了具体数字。在 VPN 3000 版本 2.2 到 2.5.2 中，总共可以有 100 个用户或组（用户与组的合计必须小于等于 100）。在 VPN 3000 版本 3.0 及更高版本中，3005 和 3015 集中器的数字仍为 100。对于 VPN 3030 和 3020 集中器，该数字为 500，对于 VPN 3060 或 3080 集中器，该数字为 1000。此外，使用外部认证服务器可以改进可扩展性和可管理性。

Q. 隧道默认网关和默认网关有何区别？

A. VPN 3000 集中器在专用网络中使用隧道默认网关路由隧道用户（通常是内部路由器）。VPN 集中器使用默认网关将数据包路由到 Internet（通常是外部路由器）。

Q. 如果我在运行访问控制列表的防火墙或路由器后面放置我的 VPN 3000 集中器，我需要允许通过哪些端口和协议？

A. 下表列出了端口和协议。

服务	协议编号	源端口	目的端口
PPTP 控制连接	6 (TCP)	1023	1723
PPTP 隧道封装	47 (GRE)	不适用	不适用
ISAKMP/IPSec 密钥管理	17 (UDP)	500	500
IPSec 隧道封装	50 (ESP)	不适用	不适用
IPSec NAT 透明模式	17 (UDP)	10000（默认值）	10000（默认值）

注意： 网络地址转换 (NAT) 透明模式端口可配置为 4001 到 49151 范围内的任何值。在版本 3.5 或更高版本中，您可以转到 **Configuration > System > Tunneling Protocols > IPSec > IPSec over TCP** 并配置 IPsec over TCP。您最多可以输入 10 个逗号分隔的 TCP 端口 (1 - 65535)。如果配置此选项，请确保运行访问控制列表的防火墙或路由器中允许使用这些端口。

Q. 如何将 VPN 集中器恢复为出厂默认设置？

A. 在 File Management 屏幕中，删除“config”文件并重新启动。如果意外删除了此文件，还有一个备份副本“config.bak”。

Q. 能否为管理型认证使用 TACACS+？这样做时有哪些注意事项？

A. 可以，从 VPN 3000 集中器版本 3.0 开始，您可以为管理型认证使用 TACACS+。在配置 TACACS+ 后，请确保在注销之前测试认证。不适当的 TACACS+ 配置会将您锁定。这时需要进行控制台端口登录以禁用 TACACS+ 并纠正问题。

Q. 当忘记管理口令时该怎么办？

A. 在版本 2.5.1 及更高版本中，请使用一条直通式 RS-232 串行电缆将一台 PC 连接到 VPN 集中器的控制台端口，并将 PC 设置为：

- 9600 bps
- 8 个数据位
- 无奇偶校验
- 1 个停止位
- 启用硬件流控制
- VT100 仿真

重新启动 VPN 集中器。诊断检查完成后，控制台将显示三个小点 (...)。在这些小点出现后的三秒钟内按 **CTRL-C**。这将显示一个菜单，从中可以将系统口令重置为其默认值。

Q. 组名称和组口令的用途是什么？

A. 组名称和组口令用于创建 Hash，后者随后用于创建安全关联。

Q. VPN 集中器代理 ARP 是代表隧道用户吗？

A. 可以。

Q. VPN 3000 集中器相对于网络防火墙应当怎样放置？

A. VPN 3000 集中器可以放在防火墙的前面、后边、并行位置或隔离区 (DMZ) 中。不宜将公共和专用接口放在相同的虚拟 LAN (VLAN) 中。

Q. 能否禁用 Cisco VPN 3000 集中器上的代理 ARP？

A. 无法在 Cisco VPN 3000 集中器上禁用代理地址解析服务 (ARP)。

Q. 在哪里能找到 VPN 3000 集中器的 Bug 文件？

A. 用户可以使用 Bug 工具包（仅限注册用户）查找有关 Bug 的详细信息。

Q. 在哪里能找到 VPN 3000 集中器的配置示例？

A. 除了 VPN 3000 集中器文档之外，在 Cisco VPN 3000 系列集中器支持页上还可以找到更多配置示例。

Q. 如何能增加日志记录以便能够更好地调试特定事件？

A. 您可以转到 **Configuration > System > Events > Classes** 并配置特定事件（如 IPsec 或 PPTP）以便能够进行更好的调试。调试会导致性能降低，因此应只在进行故障排除的过程中进行调试。对于 IPSec 调试，请打开 IKE、IKEDBG、IPSEC、IPSECDBG、AUTH 和 AUTHDBG。如果使用证书，还应再将 CERT 类添加到此列表中。

Q. 如何监控指向 VPN 3000 集中器的数据流？

A. VPN 3000 集中器附带的 HTML 界面在 **Monitoring > Sessions** 下为您提供了基本监控功能。您也可以选择使用某个 SNMP 管理器并通过简单网络管理协议 (SNMP) 监控 VPN 3000 集中器。或者，您还可以购买 Cisco VPN/Security Management Solution (VMS)。如果您部署了 VPN 3000 集中器系列并需要基于 IPsec、L2TP 和 PPTP 深入监控远程访问和站间 VPN，则可以借助 Cisco VMS 提供的主要功能。有关 VMS 的详细信息，请参阅 VPN Security Management Solution。

Q. Cisco VPN 3000 集中器系列有没有集成式防火墙？如果有，都支持哪些功能？

A. 虽然该系列具有集成式无状态端口/过滤功能和 NAT，但 Cisco 建议您使用诸如 Cisco Secure PIX 防火墙那样的设备作为公司防火墙。

Q. Cisco VPN 3000 集中器系列支持哪些路由选项和 VPN 协议？

A. 该系列支持以下路由选项：

- 路由信息协议 (RIP)
- RIP2
- 开放最短路径优先 (OSPF)
- 静态路由
- 虚拟路由器冗余协议 (VRRP)

支持的 VPN 协议包括点对点隧道协议 (PPTP)、L2TP、L2TP/IPsec 以及在 VPN 3000 与终端客户端之间配有或没有 NAT 设备的 IPsec。通过 NAT 的 IPSec 称为 NAT 透明模式。

Q. Cisco VPN 3000 集中器系列支持客户端 PC 采用哪种认证机制/系统？

A. 支持 NT 域、RADIUS 或 RADIUS 代理、RSA Security SecurID (SDI)、数字证书和内部认证。

Q. 能否为通过 VPN 3000 集中器连出去的用户执行静态网络地址转换 (NAT)？

A. 只能为连出去的用户执行端口地址转换 (PAT)。不能在 VPN 3000 集中器上执行静态 NAT。

Q. 如何通过 VPN 3000 集中器为特定点对点隧道协议 (PPTP) 或 IPSec 用户分配静态 IP 地址？

A. 以下列表解释了如何分配静态 IP 地址：

- **PPTP 用户**在 IP Address Management 部分中，除了选择您的池或动态主机配置协议 (DHCP) 选项外，还要选中 **Use Client Address** 选项。然后，在 VPN 3000 集中器中定义用户和 IP 地址。连接时，该用户将始终获取在 VPN 集中器中配置的 IP 地址。
- **IPSec 用户**在 IP Address Management 部分，除了选择您的池或 DHCP 选项外，还要选中 **Use Address from Authentication Server** 选项。然后，在 VPN 3000 集中器中定义用户和 IP 地址。连接时，该用户将始终获取在 VPN 集中器中配置的 IP 地址。属于相同组或其他组的所有其他用户将从全局池或 DHCP 获取 IP 地址。在 Cisco VPN 3000 集中器软件版本 3.0 及更高版本中，您可以选择以组为基础配置地址池。此功能可以帮助您将静态IP地址分配到特定用户。如果为一个组配置一个池，具有静态 IP 的用户将获得分配给他们的 IP 地址，同组中的其他成员将从组池中获取 IP 地址。仅当您使用 VPN 集中器作为认证服务器时才适用这种情况。

注意： 如果使用外部认证服务器，则需要使用外部服务器以正确分配地址。

Q. Microsoft 的 PPTP 产品和 VPN 3000 集中器有哪些已知的兼容性问题？

A. 以下信息基于：VPN 3000 系列集中器软件版本 3.5 和更高版本；VPN 3000 系列集中器（型号 3005、3015、3020、3030、3060、3080）；以及 Microsoft 操作系统 Windows 95 和更高版本。

- **Windows 95 Dial-Up Networking (DUN) 1.2**DUN 1.2 不支持 Microsoft 点对点加密 (MPPE)。要使用 MPPE 进行连接，请安装 Windows 95 DUN 1.3。可以从 Microsoft 网站下载Microsoft DUN 1.3 升级文件。
- **Windows NT 4.0**Windows NT 完全支持与 VPN 集中器的点对点隧道协议 (PPTP) 连接。需要 Service Pack 3 (SP3) 或更高版本。如果您运行的是 SP3，则应安装 PPTP 性能和安全补丁程序。有关 WinNT 4.0 的 Microsoft PPTP 性能和安全升级 的信息，请访问 Microsoft 网站。注意，128 位 Service Pack 5 不能正确处理 MPPE 键，并且 PPTP 无法传递数据。发生这种情况时，事件日志会显示以下消息：`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.
```
要解决此问题，请下载如何的升级能获取最新的WINDOWS NT服务软件包6a和Windows NT 4.0服务包6a联机。有关详细信息，请参阅以下 Microsoft 文章：未针对 128 位 MS-CHAP 请求正确处理 MPPE 密钥 。

Q. VPN 3000 集中器最多允许有多少过滤器？

A. 您可以在 VPN 30xx 设备（甚至 3030 或 3060）上添加的过滤器的最大数量固定为 100 个。用户可以查看 Cisco Bug ID CSCdw86558（仅限注册用户）以找到有关此问题的更多信息。

Q. 30xx 系列 VPN 集中器中的最大路由数是多少？

A. 最大路由数为：

- VPN 3005 集中器以前最多可以有 200 个路由，现在增加到 350 个路由。有关详细信息，请参阅 Cisco Bug ID CSCeb35779（仅限注册用户）。
- VPN 3030 集中器最多测试过 10,000 个路由。
- VPN 3030、3060 和 3080 集中器上的路由表限值与每台设备中的可用资源/内存成正比。
- VPN 3015 集中器没有预定义的最大限制。路由信息协议 (RIP) 和开放最短路径优先 (OSPF) 协议也是如此。
- VPN 3020 集中器 — 由于 Microsoft 的限制，Windows XP PC 不能接收大量的无类静态路由 (CSR)。进行相应配置后，VPN 3000 集中器可限制插入到 DHCP INFORM 消息响应中的 CSR 数。VPN 3000 集中器可将路由数量限制为 28-42，具体取决于类。

Q. 如何在 VPN 3000 集中器上完全清除接口统计数据？

A. 选择 Monitoring > Statistics > MIB-II > Ethernet 并重置统计以清除当前会话的统计数据。注意，这不会清除全部统计数据。要切实重置统计数据（相对于出于监控目的的重置），您需要重新启动。

Q. 要进行网络时间协议 (NTP) 通信，需要在 VPN 集中器上启用哪个端口？

A. 启用 TCP 和 UDP 端口 123。

Q. UDP 端口 625xx 的功能是什么？

A. 这些端口用于实际 shim/Deterministic NDIS Extender (DNE) 和 PC 的 TCP/IP 协议栈之间的 VPN 客户端通信，且仅供内部开发使用。例如，VPN 客户端使用端口 62515 将信息发送到 VPN 客户端日志。其他端口功能如下所示。

- 62514 - Cisco Systems, Inc. VPN 服务到 Cisco Systems IPsec 驱动程序
- 62515 - Cisco Systems IPsec 驱动程序到 Cisco Systems, Inc. VPN 服务
- 62516 - Cisco Systems, Inc. VPN 服务到 XAUTH
- 62517 - XAUTH 到 Cisco Systems, Inc. VPN 服务
- 62518 - Cisco Systems, Inc. VPN 服务到 CLI
- 62519 - CLI 到 Cisco Systems, Inc VPN 服务
- 62520 - Cisco Systems, Inc. VPN 服务到 UI
- 62521 - UI 到 Cisco Systems, Inc. VPN 服务

- 62522 - 日志消息
- 62523 - Connection Manager 到 Cisco Systems, Inc. VPN 服务
- 62524 - PPPTool 到 Cisco Systems, Inc. VPN 服务

Q. 能否删除 WebVPN 浮动工具栏？

A. 在建立 WebVPN 会话时，您不能删除浮动工具栏，也无法避免加载浮动工具栏。这是因为，当您关闭此窗口时会话将立即终止，而当您尝试再次登录时该窗口将重新载入。这是 WebVPN 会话的原始设计方式。您可以关闭主窗口，但无法关闭浮动窗口。

软件

Q. WebVPN 是否支持 Outlook Web Access (OWA) 2003？

A. 现在版本 4.1.7 为 VPN 3000 集中器上的 WebVPN 提供了 OWA 2003 支持（下载（仅限注册用户））。

Q. 在哪里可以获得 VPN 3000 集中器的最新软件版本？

A. 所有 Cisco VPN 3000 集中器在出厂时都采用了最新的代码，但用户可以检查下载（仅限注册用户）以查看是否有更新的软件可用。

有关 VPN 3000 集中器的最新文档，请参阅 Cisco VPN 3000 系列集中器文档页面。

Q. 是否需要 TFTP 服务器以升级 VPN 3000 集中器？有没有其他升级方式？

A. 除了使用 TFTP 外，您还可以通过将最新软件下载到您的硬盘驱动器上来升级 VPN 集中器。然后，通过软件所在系统中的浏览器转到 **Administration > Software Update**，并找出下载到您的硬盘驱动器的软件（就像打开一个文件一样）。找到后，选择 **Upload** 选项卡。

Q. 最新代码名称中的“k9”（例如在“vpn3000-3.0.4.Rel-k9.bin”中）表示什么意思？

A. “k9”表示镜像名称，它取代了最初使用的 3DES 指示方式（例如，vpn3000-2.5.2.F-3des.bin）。因此，“k9”现在表示这是 3DES 镜像。

Q. 我是否应当为我的所有用户使用 IPsec 组下的数据压缩选项？

A. 数据压缩会增加内存需求和每个用户会话的 CPU 利用率，从而减少 VPN 集中器的整体吞吐量。为此，Cisco 建议您只有在每名组成员都是与调制解调器连接的远程用户时，才启用数据压缩。如有任何组成员通过宽带连接，请勿为组启用数据压缩，而应把组分成两组，一组用于调制解调器用户，另一组用于宽带用户，并只为调制解调器用户组启用数据压缩。

其他高级功能

Q. 负载均衡是否适用于 LAN 间的连接？

A. 负载均衡仅对由 Cisco VPN 软件客户端（版本 3.0 及更高版本）启动的远程会话有效。所有其

他客户端（PPTP、L2TP）和 LAN 间连接可以连接到启用了负载均衡的 VPN 集中器，但它们不能参与负载均衡。

Q. 如何通过配置文件解密口令？

A. 转到 Configuration > System > Management Protocols > XML，然后转到 administration|file management select XML format。使用相同或不同的名称打开文件以查看口令。

Q. 我能否配合使用虚拟路由器冗余协议 (VRRP) 和负载均衡？

A. 您不能将负载均衡与 VRRP 配合使用。在 VRRP 配置中，除非活动 VPN 集中器出现故障，否则备份设备将保持空闲状态。而在负载均衡配置中，没有空闲设备。

Q. 所有远程访问客户端 VPN 数据流是否都必须通过加密隧道才能到达企业或服务提供商的 VPN 集中器？例如，明文 Web 访问能否直接通过 ISP 的 Internet 连接以不加密的方式访问其他站点？

A. 可以。这一概念称为“Split Tunneling”。Split Tunneling 允许通过加密隧道安全访问公司资源，同时允许直接通过 ISP 的资源接入 Internet（Web 访问路径中不包含公司网络）。针对 Cisco VPN 客户端和 VPN 3002 硬件客户端的 Cisco VPN 3000 集中器系列都支持 Split Tunneling。出于其他安全考虑，此功能由 VPN 集中器的管理员而不是由用户控制。

Q. 使用 Split Tunneling 是否安全？

A. Split Tunneling 允许您在通过 VPN 隧道进行连接的同时能够方便地浏览 Internet。然而，如果连接到公司网络的 VPN 用户容易受到攻击，则会带来某种风险。在这种情况下，我们建议用户使用个人防火墙。所有特定 VPN 客户端版本的发行版本注释都论述了与个人防火墙之间的互操作性。

Q. 负载均衡在 Cisco VPN 3000 集中器上如何工作？

A. 负载计算为活动连接数除以最大配置连接数所得的百分比。主设备总是设法承担最少负载，因为主设备还承担着其他（固有）负载，以维护所有管理型 LAN 间会话，计算所有其他集群成员负载，并负责重定向所有客户端。

对于新配置的功能集群，在建立任何连接之前，主设备已有 1% 左右的负载。因此，主设备会将连接重定向到备份集中器上，直到备份设备的负载百分比高于主设备的负载百分比。例如，假设有两台处于“空闲”状态的 VPN 3030 集中器，主设备有 1% 的负载。在主设备接受连接之前，备份设备将承担 30 个连接（2% 的负载）。

要验证主设备是否接受了连接，请转到 Configuration > System > General > Sessions 并将最大连接数减少到一个非常低的数值，以快速增加放到备份 VPN 集中器上的负载。

Q. VPN Monitor 可以跟踪多少数据转发设备？

A. VPN Monitor 可以跟踪 20 个数据转发设备。在一个星型网络方案中，来自远程站点的连接将在转发设备上予以监控。这时不需要对所有远程站点和用户进行监控，因为可以在集线路由器上跟踪这些信息。这些数据转发设备可支持多达 20,000 个远程用户或 2,500 个远程站点。一个指向分支站点的双宿主 VPN 设备将视为最多可监控 20 台设备中的两台。

相关信息

- Cisco VPN 3000 集中器支持页
- Cisco VPN 3000 Client 支持页
- 技术支持和文档 - Cisco Systems