Cisco VPN 3000 Concentrator常見問題

目錄

簡介

本文檔回答有關Cisco VPN 3000系列集中器的常見問題(FAQ)。

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

一般

問：錯誤資訊「服務中斷麼意思？

A.如果VPN集中器和VPN客戶端之間在一段時間內沒有傳送任何流量，則會從VPN集中器向VPN客戶端傳送一個失效對等項檢測(DPD)資料包，以確保其對等項仍然存在。如果VPN客戶端不響應VPN集中器的兩個對等體之間存在連線問題，則VPN集中器會繼續在一段時間內傳送DPD資料包。這將終止隧道並生成錯誤（如果它在該時間內未收到響應）。請參閱Cisco錯誤ID CSCdz45586（需要支援合約）。

錯誤應該如下所示：

```
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：遠端IKE對等體未在預期的時間視窗內響應keepalive，因此與IKE對等體的連線被刪除。該消息包括使用的保活機制。只有在活動隧道會話期間斷開公共介面時，此問題才可能重現。客戶需要監控其網路連線，因為生成這些事件是為了查明其潛在網路連線問題的根本原因。

在遇到問題的客戶端PC上，通過轉至**%System Root%\Program Files\Cisco Systems\VPN Client\Profiles**來禁用IKE keepalive，並編輯連線的**PCF檔案**（如果適用）。

將「ForceKeepAlives=0」（預設值）更改為「**ForceKeepAlives=1**」。

如果問題仍然存在，請通過Cisco技術支援開啟服務請求，並在出現問題時提供客戶端「日誌檢視器」和VPN集中器日誌。

問：檢測到EMQ1隊列的錯誤消息「`q_send`」表示什麼？

A.當緩衝區中有太多調試事件/資訊時，會出現此錯誤消息。除了可能會丟失一些事件消息外，它沒有其他負面影響。嘗試將事件減少到防止消息所需的最小數目。

問：我的已刪除組仍顯示在VPN集中器配置中。如何刪除此內容？

A.將配置複製到文本編輯器（如記事本）中，並手動編輯或刪除由[ipaddrgrouppool #.**0]表示的影響組資訊**。儲存配置並將其上傳到VPN集中器。此處顯示範例。

```
!--- 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
```

問：是否可以有多個主SDI伺服器？

A. VPN 3000集中器一次只能下載一個節點機密檔案。在SDI 5.0之前的版本中，您可以新增多個SDI伺服器，但它們必須共用同一個節點機密檔案（可以將其視為主伺服器和備份伺服器）。 在SDI版本5.0中，您只能輸入一個主SDI伺服器（備份伺服器列在節點機密檔案中）和副本伺服器。

問：我收到「SSL certificate will expire in 28 days(SSL28)頒發者錯誤消息。我該怎麼辦？

A.此消息表示您的安全通訊端層(SSL)憑證將於28天後過期。此證書用於通過HTTPS瀏覽到Web管理。您可以將證書保留為預設設定，也可以在生成新證書之前配置不同的選項。選擇**Configuration > System > Management Protocols > SSL**執行此操作。選擇**Administration > Certificate Management**，然後按一下**Generate**以續訂證書。

如果您擔心VPN集中器的安全性並想要防止未經授權的訪問，請通過轉至**Configuration > Policy Management > Traffic Management > Filters**在公共介面上禁用HTTP和/或HTTPS。如果您需要通過HTTP或HTTPS通過Internet訪問VPN集中器，則可以通過轉至**管理>訪問許可權>訪問控制清單**來根據源地址指定訪問許可權。您可以使用視窗右上角的幫助選單獲取詳細資訊。

問：如何檢視內部使用者資料庫中的使用者資訊？我在配置檔案中查詢時看不到此項。

A.選擇**Administration > Access Rights > Access Settings，選擇Config File Encryption=None，然後儲存配置以檢視使用者和密碼。**您應該能夠搜尋特定的使用者。

問：內部資料庫可以儲存多少使用者？

A.用戶數量取決於版本，在VPN 3000 Concentrator發行版的使用手冊的**Configuration > User Management**部分中指定了使用者數。VPN 3000版本2.2至2.5.2中總共可以有100個使用者或組（使用者和組的總數必須等於100或更少）。在VPN 3000版本3.0及更高版本中，3005和3015集中器的數量仍為100。對於VPN 3030和3020集中器，VPN 3060或3080的編號為500集中商，數字是1000。此外，使用外部身份驗證伺服器可提高可擴充性和可管理性。

問：通道預設網關和預設網關有何區別？

A. VPN 3000集中器使用隧道預設網關路由專用網路（通常是內部路由器）中的隧道使用者。VPN集中器使用預設網關將資料包路由到Internet（通常是外部路由器）。

問：如果我將VPN 3000集中器放在運行訪問控制清單的防火牆或路由器後面，我需要允許通過哪些埠和協定？

A.此圖表列出埠和協定。

服務	通訊協定編號	來源連線埠	目的地連線埠
PPTP控制連線	6(TCP)	1023	1723
PPTP通道封裝	47(GRE)	不適用	不適用
ISAKMP/IPSec金鑰管理	17(UDP)	500	500
IPSec通道封裝	50（西班牙比塞塔）	不適用	不適用
IPSec NAT透明度	17(UDP)	10000（預設）	10000（預設）

注意：網路地址轉換(NAT)透明埠可配置為4001到4000範圍內的任49151值。在3.5版或更高版本中，可以通過轉至**Configuration > System > Tunneling Protocols > IPSec > IPSec over TCP**來配置IPsec over TCP。最多可輸入10個逗號分隔的TCP埠(1 - 65535)。 如果配置了此選項，請確保在運行訪問控制清單的防火牆或路由器中允許這些埠。

問：如何將VPN集中器重新設定為出廠預設設定？

A.在「檔案管理」螢幕中，刪除「config」檔案並重新啟動。如果意外刪除此檔案，則會保留備份副本「config.bak」。

問：我是否可以使用TACACS+進行管理身份驗證？做的時候應該牢記什麼？

答：是，從VPN 3000集中器版本3.0開始，您可以使用TACACS+進行管理身份驗證。設定TACACS+後，請確保在註銷前測試驗證。TACACS+設定不當可能會將您鎖定在網路之外。此功能需要登入主控台連線埠，才能停用TACACS+並修正問題。

如果忘記了管理密碼，該怎麼做？

A.在2.5.1及更高版本中，使用直通RS-232串列電纜將PC連線到VPN集中器的控制檯埠，並將PC設定為：

- 9600位元/秒
- 8個資料位
- 無奇偶校驗
- 1停止位
- 硬體流量控制開啟
- VT100模擬

重新啟動VPN集中器。診斷檢查完成後，控制檯上會顯示一行三點(...)。在這些點出現後的三秒內按**CTRL-C**。此時將顯示一個選單，用於將系統密碼重置為預設值。

問：組名和組密碼的作用是什麼？

A.組名和組密碼用於建立雜湊，然後用於建立安全關聯。

問：VPN集中器是否代表隧道使用者代理ARP?

A.是。

問：應該將VPN 3000集中器放在與網路防火牆相關的哪個位置？

A. VPN 3000集中器可以放置在防火牆的非軍事區(DMZ)之前、之後、平行或之內。不建議在同一虛擬LAN(VLAN)中使用公共介面和專用介面。

問：在Cisco VPN 3000集中器上是否有禁用代理ARP的方法？

答：無法在Cisco VPN 3000集中器上禁用代理地址解析協定(ARP)。

問：在哪裡可以找到針對VPN 3000集中器歸檔的錯誤？

A.使用者可以使用Bug Search工具（需要支援合約）尋找錯誤詳細資訊。

問：在哪裡可以找到VPN 3000集中器的配置示例？

答：除了VPN 3000集中器文檔外，還可以在Cisco VPN 3000系列集中器支援頁面上找到更多配置示例。

問：如何增加日誌記錄以更好地調試特定事件？

A.您可以轉至Configuration > System > Events > Classes，並配置特定事件（如IPsec或PPTP）以獲得更好的調試。只有在故障排除練習期間才應開啟調試，因為它可能會導致效能下降。對於IPsec調試，請開啟IKE、IKEDBG、IPSEC、IPSECDBG、AUTH和AUTHDBG。如果使用證書，請將CERT類新增到清單中。

問：如何監控到VPN 3000集中器的流量？

答：VPN 3000 Concentrator附帶的HTML介面允許您在Monitoring > Sessions下檢視基本監控功能。也可使用您選擇的SNMP管理器通過簡單網路管理協定(SNMP)監控VPN 3000集中器。或者，您可以購買Cisco VPN/安全管理解決方案(VMS)。 如果您部署VPN 3000集中器系列並需要基於IPsec、L2TP和PPTP對遠端訪問和站點到站點VPN進行深入監控，思科VMS可提供關鍵功能來協助您。有關VMS的詳細資訊，請參閱VPN安全管理解決方案。

問：Cisco VPN 3000 Concentrator系列是否具有整合防火牆？如果是，支援哪些功能？

答：雖然該系列整合了無狀態埠/過濾功能和NAT，但思科建議您使用類似於公司防火牆的Cisco Secure PIX防火牆的裝置。

問：Cisco VPN 3000集中器系列支援哪些路由選項和VPN協定？

A.該系列支援以下路由選項：

- 路由資訊通訊協定(RIP)
- RIP2
- 開放最短路徑優先(OSPF)
- 靜態路由
- 虛擬路由器備援通訊協定(VRRP)

支援的VPN協定包括點對點隧道協定(PPTP)、L2TP、L2TP/IPsec和IPsec，在VPN 3000與終端客戶端之間使用或不使用NAT裝置。通過NAT的IPsec稱為NAT透明。

問： Cisco VPN 3000集中器系列支援客戶端PC的哪些身份驗證機制/系統？

A.支持NT域、RADIUS或RADIUS代理、RSA安全SecureID(SDI)、數位證書和內部身份驗證。

問：我能為通過VPN 3000集中器外出的使用者執行靜態網路地址轉換(NAT)嗎？

A.您只能為外出使用者執行埠地址轉換(PAT)。您不能在VPN 3000集中器上執行靜態NAT。

問：如何通過VPN 3000集中器將靜態IP地址分配給特定的點對點隧道協定(PPTP)或IPsec使用者？

A.此清單說明如何分配靜態IP地址：

- **PPTP使用者**在「IP地址管理」部分中，除了選擇地址池或動態主機配置協定(DHCP)選項外，還選中**使用客戶端地址**選項。然後，在VPN 3000集中器中定義使用者和IP地址。此使用者在連線時始終獲得VPN集中器中的IP地址。
- **IPsec使用者**在IP Address Management部分中，除了選擇地址池或DHCP選項外，還選中**Use Address from Authentication Server**選項。然後，在VPN 3000集中器中定義使用者和IP地址。此使用者在連線時始終獲得VPN集中器中的IP地址。屬於同一組或其他組的所有其他組都從全域性池或DHCP獲取IP地址。在Cisco VPN 3000 Concentrator軟體3.0版及更高版本中，您可以選擇以組為基礎配置地址池。此功能還可以幫助您將靜態IP地址分配給特定使用者。如果為組配置池，則具有靜態IP的使用者將獲取分配給它們的IP地址，同一組的其他成員將從組池獲取IP地址。這僅在將VPN集中器用作身份驗證伺服器時才適用。

注意：如果使用外部身份驗證伺服器，則需要使用外部伺服器來正確分配地址。

問：微軟的PPTP產品和VPN 3000集中器有哪些已知的相容性問題？

A.此資訊基於VPN 3000系列集中器軟體版本3.5及更高版本；VPN 3000系列集中器，型號3005、3015、3020、3030、3060、3080;和Microsoft作業系統Windows 95及更高版本。

- **Windows 95撥號網路(DUN)1.2**DUN 1.2不支援Microsoft點對點加密(MPPE)。要使用MPPE連線，請安裝Windows 95 DUN 1.3。您可以從Microsoft網站下載Microsoft DUN 1.3升級 。
- **Windows NT 4.0**與VPN集中器的點對點隧道協定(PPTP)連線完全支援Windows NT。需要Service Pack 3(SP3)或更高版本。如果您正在運行SP3，則應安裝PPTP效能和安全修補程式。有關Microsoft PPTP Performance and Security Upgrade for WinNT 4.0的資訊，請參閱Microsoft網站 。請注意，128位Service Pack 5不能正確處理MPPE金鑰，並且PPTP可能無法傳遞資料。如果發生這種情況，事件日誌將顯示以下消息：

```
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.
```

要解決此問題，請下載如何獲取可用的最新Windows NT Service Pack 6a和Windows NT 4.0 Service Pack 6a的升級。有關詳細資訊，請參閱Microsoft文章MPPE Keys Not Handled Corrected For a 128-Bit MS-CHAP Request 。

問：VPN 3000集中器上允許的最大過濾器數是多少？

答：VPN 30xx裝置（甚至是3030或3060）上可以新增的最大過濾器數固定為100。使用者可以通過檢視思科錯誤ID CSCdw86558（需要支援合約）找到有關此問題的其他資訊。

問：VPN集中器的30xx行中的最大路由數是多少？

A.最大路由數為：

- VPN 3005集中器以前最多擁有200條路由。現在這一數字已增加到350條路由。如需更多詳細資訊，請參閱Cisco錯誤ID CSCeb35779（需要支援合約）。
- VPN 3030集中器已經測試了多達10,000條路由。
- VPN 3030、3060和3080集中器的路由表限制與每台裝置中的可用資源/記憶體成正比。
- VPN 3015集中器沒有預定義的最大限制。此情況適用於路由資訊通訊協定(RIP)和開放最短路徑優先(OSPF)通訊協定。
- VPN 3020集中器 — 由於Microsoft限制，Windows XP PC無法接收大量無類靜態路由(CSR)。VPN 3000集中器限制在配置為DHCP INFORM消息響應時插入CSR的數量。VPN 3000集中器將路由數量限製為28-42，具體取決於類別。

問：如何完全清除VPN 3000集中器上的介面統計資訊？

A.選擇Monitoring > Statistics > MIB-II > Ethernet，重置統計資訊以清除當前會話的統計資訊。請記住，這並不完全清除統計資料。您需要重新啟動以實際重置統計資訊（而不是出於監控目的重置）。

問：在VPN集中器上應該允許哪些埠用於網路時間協定(NTP)通訊？

A.允許TCP和UDP埠123。

問： UDP埠625xx有哪些功能？

A.這些埠用於實際填充物/確定性NDIS擴展器(DNE)與PC的TCP/IP堆疊之間的VPN客戶端通訊，僅供內部開發使用。例如，VPN客戶端62515用埠12將資訊傳送到VPN客戶端日誌。此處顯示其他連線埠功能。

- 62514 - Cisco Systems， Inc. VPN服務至Cisco Systems IPsec驅動程式
- 62515 - Cisco Systems， Inc. VPN服務的Cisco Systems IPsec驅動程式
- 62516 - Cisco Systems， Inc. VPN服務至XAUTH
- 62517 - XAUTH至Cisco Systems， Inc. VPN服務
- 62518 - Cisco Systems， Inc. CLI的VPN服務
- 62519 - CLI至Cisco Systems， Inc VPN服務
- 62520 - Cisco Systems， Inc. VPN服務至UI
- 62521 - Cisco Systems， Inc. VPN服務的UI
- 62522 — 日誌消息

- 62523 - Connection Manager to Cisco Systems， Inc. VPN Service
- 62524 - PPPTool至Cisco Systems， Inc. VPN服務

問：是否可以刪除WebVPN浮動欄？

A.在建立WebVPN會話時，不能刪除浮動工具欄，也不能避免載入浮動工具欄。這是因為當您關閉此視窗時，會話會立即終止，當您嘗試再次登入時，該視窗會再次載入。這就是最初設計WebVPN會話的方式。您可以關閉主視窗，但無法關閉浮動視窗。

軟體

問： WebVPN是否支援Outlook Web Access(OWA)2003?

答：VPN 3000集中器上的WebVPN的OWA 2003支援現已提供，可下載4.1.7版(需要支援合約)。

問：在哪裡可以獲得VPN 3000集中器的最新軟體版本？

答：所有Cisco VPN 3000集中器都帶有最新代碼，但使用者可以檢查下載項（需要支援合約）以檢視是否有更多最新軟體可用。

有關VPN 3000集中器的最新文檔，請參閱Cisco VPN 3000系列集中器文檔頁面。

問：我是否需要TFTP伺服器來升級VPN 3000 Concentrator?是否有其他方法來升級該盒？

答：除了使用TFTP外，您還可以將最新軟體下載到硬碟驅動器中來升級VPN集中器。接下來，從軟體所在系統上的瀏覽器中，前往**管理>軟體更新**，在硬體磁碟上尋找下載的軟體（與開啟檔案類似）。 找到後，選擇**Upload**頁籤。

問：「k9」在最新代碼名稱（如「vpn3000-3.0.4.Rel-k9.bin」）中表示什麼意思？

A.映像名稱的「k9」名稱已取代了最初使用的3DES名稱（例如，vpn3000-2.5.2.F-3des.bin）。 因此，「k9」現在表示這是3DES影象。

問：我是否應該為所有使用者使用IPsec組下的Data Compression選項？

A.資料壓縮會增加每個使用者會話的記憶體需求和CPU利用率，從而降低VPN集中器的整體吞吐量。因此，思科建議您僅在組中的每個成員都是與數據機連線的遠端使用者時，才啟用資料壓縮。如果組的任何成員通過寬頻連線，請不要為組啟用資料壓縮。相反，將組分為兩組，一組用於數據機使用者，另一組用於寬頻使用者。僅對數據機使用者組啟用資料壓縮。

其他進階功能

問：負載均衡是否適用於LAN到LAN連線？

A.負載均衡僅對通過Cisco VPN軟體客戶端（3.0版及更高版本）啟動的遠端會話有效。 所有其他客戶端(PPTP、L2TP)和LAN到LAN連線可以連線到啟用了負載平衡的VPN集中器，但是它們不能參

與負載平衡。

問：如何從配置檔案中解密密碼？

A.轉至Configuration > System > Management Protocols > XML，**然**後轉至administration |**檔案管理選擇XML格式**。使用相同或不同的名稱，然後開啟檔案以檢視密碼。

問：我是否可以同時使用虛擬路由器冗餘協定(VRRP)和負載平衡？

A.不能對VRRP使用負載均衡。在VRRP配置中，除非活動VPN集中器發生故障，否則備份裝置將保持空閒。在負載平衡配置中，沒有空閒裝置。

問：所有遠端訪問客戶端VPN流量是否必須通過加密隧道才能到達企業或服務提供商的VPN集中器？例如，對其它網站的普通Web訪問是否可以直接通過ISP的Internet連線公開進行？

A.是。此概念稱為「分割通道」。 分割隧道允許通過加密隧道安全訪問公司資源，同時允許直接通過ISP的資源訪問Internet（這樣可以消除公司網路訪問Web的路徑）。 連線到Cisco VPN客戶端和VPN 3002硬體客戶端的Cisco VPN 3000 Concentrator系列可支援分割隧道。為了獲得更高的安全性，此功能由VPN集中器的管理員而不是使用者控制。

使用分割隧道是否安全？

A.分割隧道允許您在通過VPN隧道連線時方便地瀏覽網際網路。但是，如果連線到公司網路的VPN使用者易受攻擊，這確實會給我們帶來一些風險。在這種情況下，建議使用者使用個人防火牆。任何特定VPN客戶端版本的發行說明均討論與個人防火牆的互操作性。

問：負載均衡在Cisco VPN 3000集中器上如何工作？

A.負載的計算方法是將活動連線數除以配置的最大連線數所得的百分比。指揮交換機總是嘗試負載最小，因為它承擔了維護所有管理性LAN到LAN會話、計算所有其他集群成員負載的附加（固有）負載，並且它負責所有客戶端重定向。

對於新配置的功能集群，在尚未建立任何連線之前，導向器有大約1%的負載。因此，控制器會將連線重定向到備份集中器，直到備份上的負載百分比高於控制器上的負載百分比為止。例如，假設兩個VPN 3030集中器處於「空閒」狀態，則控制器負載為1%。在控制器接受連線之前，為輔助控制器提供30個連線（2%負載）。

若要驗證控制器是否接受連線，請轉到Configuration > System > General > Sessions，將最大連線數降低到人為的低值，以快速增加備份VPN集中器上的負載。

問： VPN監控器可以跟蹤多少個頭端裝置？

A. VPN監控器可跟蹤20台頭端裝置。在集中星型場景中，來自遠端站點的連線會在前端受到監控。不需要監控所有遠端站點和使用者，因為可以在集線器路由器上跟蹤該資訊。這些頭端裝置最多可支援20,000個遠端使用者或2,500個遠端站點。通向分支站點的雙宿主VPN裝置被視為可監控的最大20個裝置中的兩個。

相關資訊

- Cisco VPN 3000 Concentrator支援頁面
- Cisco VPN 3000使用者端支援頁面
- 技術支援與文件 - Cisco Systems