Cisco VPN 3000 Concentrator - Häufig gestellte Fragen

Inhalt

Einführung

Dieses Dokument beantwortet häufig gestellte Fragen (FAQs) zum Cisco VPN Concentrator der Serie 3000.

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Allgemeines

F. Was bedeutet die Fehlermeldung "`Lost Service`"?

Antwort: Wenn für einen bestimmten Zeitraum kein Datenverkehr zwischen dem VPN-Concentrator und dem VPN-Client gesendet wird, wird vom VPN-Concentrator ein Dead Peer Detection (DPD)-Paket an den VPN-Client gesendet, um sicherzustellen, dass der Peer weiterhin vorhanden ist. Bei Verbindungsproblemen zwischen den beiden Peers, bei denen der VPN-Client nicht auf den VPN-Concentrator reagiert, sendet der VPN-Concentrator weiterhin DPD-Pakete über einen bestimmten Zeitraum. Dadurch wird der Tunnel beendet, und es wird ein Fehler ausgegeben, wenn während dieser Zeit keine Antwort eingeht. Weitere Informationen finden Sie unter Cisco Bug ID CSCdz45586 (Support-Vertrag erforderlich).

Der Fehler sollte wie folgt aussehen:

```
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)
```

Ursache: Der Remote-IKE-Peer reagierte nicht auf Keepalives innerhalb des erwarteten Zeitfensters, sodass die Verbindung zum IKE-Peer gelöscht wurde. Die Nachricht enthält den verwendeten Keepalive-Mechanismus. Dieses Problem ist nur reproduzierbar, wenn die öffentliche Schnittstelle während einer aktiven Tunnelsitzung getrennt wird. Der Kunde muss die Netzwerkverbindung überwachen, wenn diese Ereignisse generiert werden, um die Ursache potenzieller Netzwerkverbindungsprobleme zu ermitteln.

Deaktivieren Sie IKE-Keepalive, indem Sie **%System Root%\Programme\Cisco Systems\VPN Client\Profiles** auf dem Client-PC aufrufen, auf dem das Problem auftritt, und bearbeiten Sie die **PCF-Datei** (falls zutreffend) für die Verbindung.

Ändern Sie 'ForceKeepAlives=0' (Standard) in '**ForceKeepAlives=1**'.

Wenn das Problem weiterhin besteht, öffnen Sie eine Serviceanfrage beim technischen Support von Cisco und stellen Sie dem Client "Log Viewer" zur Verfügung, und der VPN Concentrator protokolliert das Problem.

F. Was bedeutet die Fehlermeldung "`q_send`" Fehler, die für die EMQ1-Warteschlange erkannt wurden?

Antwort: Diese Fehlermeldung tritt auf, wenn zu viele Debugereignisse/Informationen im Puffer vorhanden sind. Es hat keine negativen Auswirkungen, außer möglicherweise einige Ereignismeldungen zu verlieren. Versuchen Sie, die Ereignisse auf die Mindestanzahl zu reduzieren, die erforderlich ist, um die Nachricht zu verhindern.

F. Meine gelöschte Gruppe wird immer noch in der Konfiguration des VPN-Konzentrators angezeigt. Wie lösche ich diese?

Antwort: Kopieren Sie die Konfiguration in einen Texteditor (z. B. Notepad), und bearbeiten oder löschen Sie die betroffenen Gruppeninformationen, die mit **[ipaddrgrouppool #.0]** gekennzeichnet sind. Speichern Sie die Konfiguration, und laden Sie sie in den VPN Concentrator hoch. Hier ist ein Beispiel dargestellt.

```
!--- 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
```

F. Können mehrere primäre SDI-Server verwendet werden?

Antwort: Die VPN 300 Concentrators können jeweils nur eine geheime Knotendatei herunterladen. In der SDI-Version vor 5.0 können Sie mehrere SDI-Server hinzufügen, aber alle müssen dieselbe geheime Knotendatei gemeinsam nutzen (denken Sie daran, dass es sich um die primären und Backup-Server handelt). In SDI Version 5.0 können Sie nur den einen primären SDI-Server (die Backup-Server sind in der Node-geheimen Datei aufgelistet) und Replikationsserver eingeben.

F. Ich erhalte die Fehlermeldung "`SSL-Zertifikat läuft in 28 Tagen ab`". Was soll ich tun?

Antwort: Die Meldung weist darauf hin, dass Ihr SSL-Zertifikat (Secure Socket Layer) in 28 Tagen abläuft. Dieses Zertifikat wird zum Surfen in die Webverwaltung über HTTPS verwendet. Sie können das Zertifikat mit den Standardeinstellungen belassen oder verschiedene Optionen konfigurieren, bevor Sie das neue Zertifikat generieren. Wählen Sie **dazu Configuration > System > Management Protocols > SSL** aus. Wählen Sie **Administration > Certificate Management** aus, und klicken Sie auf **Generate**, um das Zertifikat zu erneuern.

Wenn Sie Bedenken hinsichtlich der Sicherheit Ihres VPN Concentrator haben und nicht autorisierten Zugriff verhindern möchten, deaktivieren Sie HTTP und/oder HTTPS auf der öffentlichen Schnittstelle, indem Sie **Configuration > Policy Management > Traffic Management > Filters** aufrufen. Wenn Sie über HTTP oder HTTPS auf den VPN Concentrator zugreifen möchten,

können Sie den Zugriff basierend auf der Quelladresse unter **Administration > Access Rights > Access Control List (Verwaltung > Zugriffsrechte > Zugriffskontrollliste)** festlegen. Weitere Informationen erhalten Sie im Hilfemenü in der rechten oberen Ecke des Fensters.

F. Wie kann ich die Benutzerinformationen in der internen Benutzerdatenbank anzeigen? Sie wird nicht angezeigt, wenn ich die Konfigurationsdatei sehe.

Antwort: Wählen Sie **Administration > Access Rights > Access Settings aus**, wählen Sie **Config File Encryption=None**, und speichern Sie die Konfiguration, um Benutzer und Kennwörter anzuzeigen. Sie sollten nach dem jeweiligen Benutzer suchen können.

F. Wie viele Benutzer können im internen Datenbankspeicher gespeichert werden?

Antwort: Die Anzahl der Benutzer ist versionsabhängig und wird im Abschnitt **Konfiguration > Benutzerverwaltung** im Benutzerhandbuch für Ihre VPN 3000 Concentrator-Version angegeben. In den VPN 300-Versionen 2.2 bis 2.5.2 sind insgesamt 100 Benutzer oder Gruppen möglich (die Summe der Benutzer und Gruppen muss 100 oder weniger ergeben). In den VPN 300-Versionen 3.0 und höher beträgt die Anzahl der Concentrators 3005 und 3015 weiterhin 100. Für den VPN 3030- und 3020-Konzentrator ist die Zahl 500, für die VPN 3060- oder 3080-Konzentratoren die Zahl 1000. Darüber hinaus verbessert die Verwendung eines externen Authentifizierungsservers die Skalierbarkeit und Verwaltbarkeit.

F. Worin besteht der Unterschied zwischen dem Standard-Tunnel-Gateway und dem Standard-Gateway?

Antwort: Der VPN 3000 Concentrator verwendet das Tunnel-Standardgateway, um die getunnelten Benutzer innerhalb des privaten Netzwerks (in der Regel der interne Router) weiterzuleiten. Der VPN Concentrator verwendet das Standard-Gateway, um Pakete an das Internet weiterzuleiten (in der Regel an den externen Router).

F. Welche Ports und Protokolle muss ich zulassen, wenn ich meinen VPN 300-Konzentrator hinter einer Firewall oder einem Router mit Zugriffskontrolllisten platziere?

Antwort: Dieses Diagramm enthält Ports und Protokolle.

Service	Protokollnummer	Quell-Port	Zielport
PPTP-Steuerverbindung	6 (TCP)	1023	1723
PPTP Tunnel Encapsulation	47 (GRE)	–	–
ISAKMP/IPSec-Schlüsselverwaltung	17 (UDP)	500	500
IPSec-Tunnelkapselung	50 (ESP)	–	–
IPSec NAT-Transparenz	17 (UDP)	10000 (Standard)	10000 (Standard)

Hinweis: Der Network Address Translation (NAT) Transparency-Port kann auf einen beliebigen

Wert im Bereich von 4001 bis 49151 konfiguriert werden. In Version 3.5 oder höher können Sie IPsec über TCP konfigurieren, indem Sie **Configuration > System > Tunneling Protocols > IPSec > IPSec über TCP wählen**. Sie können bis zu 10 kommagetrennte TCP-Ports (1 - 65535) eingeben. Wenn diese Option konfiguriert ist, stellen Sie sicher, dass diese Ports in Ihrer Firewall oder Ihrem Router Zugriffskontrolllisten ausführen dürfen.

F. Wie kann ich den VPN Concentrator auf die Werkseinstellungen zurücksetzen?

Antwort: Löschen Sie im Bildschirm "File Management" die Konfigurationsdatei, und starten Sie neu. Wenn diese Datei versehentlich gelöscht wird, wird eine Sicherungskopie "config.bak" gespeichert.

F. Kann ich TACACS+ für die administrative Authentifizierung verwenden? Was sollte ich beachten, wenn ich es tue?

Antwort: Ja, ab VPN 3000 Concentrator Version 3.0 können Sie TACACS+ für die administrative Authentifizierung verwenden. Nachdem Sie TACACS+ konfiguriert haben, sollten Sie die Authentifizierung testen, bevor Sie sich abmelden. Eine falsche Konfiguration von TACACS+ kann Sie blockieren. Dies erfordert eine Konsolenport-Anmeldung, um TACACS+ zu deaktivieren und das Problem zu beheben.

F. Was mache ich, wenn das Administratorkennwort vergessen wurde?

Antwort: Schließen Sie in Version 2.5.1 und höher einen PC mithilfe eines seriellen Durchgangskabels RS-232 mit dem PC-Set an den Konsolenport des VPN Concentrator an:

- 9600 Bit pro Sekunde
- 8 Datenbits
- Keine Parität
- 1 Stoppbit
- Hardware Flow Control auf
- VT100-Emulation

Starten Sie den VPN Concentrator neu. Nach Abschluss der Diagnoseüberprüfung wird in der Konsole eine Zeile mit drei Punkten (...) angezeigt. Drücken Sie **STRG-C** innerhalb von drei Sekunden, nachdem diese Punkte angezeigt werden. Es wird ein Menü angezeigt, in dem Sie die Systemkennwörter auf die Standardeinstellungen zurücksetzen können.

F. Wozu dient der Gruppenname und das Gruppenkennwort?

Antwort: Der Gruppenname und das Gruppenkennwort werden zum Erstellen eines Hashs verwendet, der dann zum Erstellen einer Sicherheitszuordnung verwendet wird.

F. Proxy-ARP des VPN Concentrator für getunnelte Benutzer?

Antwort: Ja.

F. Wo stelle ich den VPN 300-Konzentrator in Bezug auf meine Netzwerk-Firewall?

Antwort: Der VPN 3000-Konzentrator kann vor, hinter, parallel oder in der DMZ einer Firewall

platziert werden. Es ist nicht ratsam, die öffentlichen und privaten Schnittstellen im gleichen virtuellen LAN (VLAN) zu haben.

F. Gibt es eine Möglichkeit, die Proxy-ARP im Cisco VPN 300 Concentrator zu deaktivieren?

Antwort: Das Proxy Address Resolution Protocol (ARP) kann auf dem Cisco VPN 300 Concentrator nicht deaktiviert werden.

F. Wo finde ich Fehler, die gegen den VPN 3000 Concentrator gemeldet wurden?

Antwort: Benutzer können das Bug Search Tool verwenden (Support-Vertrag erforderlich), um detaillierte Informationen zu Bugs zu finden.

F. Wo finde ich Konfigurationsbeispiele für den VPN 3000-Konzentrator?

Antwort: Zusätzlich zur Dokumentation des VPN 300 Concentrator finden Sie weitere Konfigurationsbeispiele auf der Seite zur Unterstützung von Cisco VPN Concentrator der Serie 300.

F. Wie kann ich die Protokollierung erhöhen, um bessere Debugging-Informationen für bestimmte Ereignisse zu erhalten?

Antwort: Sie können unter **Configuration > System > Events > Classes (Konfiguration > System > Ereignisse > Klassen)** die spezifischen Ereignisse (z. B. IPsec oder PPTP) konfigurieren, um bessere Debugging-Vorgänge zu erhalten. Das Debuggen sollte nur während der Fehlerbehebungsübung aktiviert werden, da es zu Leistungseinbußen führen kann. Aktivieren Sie für das IPsec-Debuggen IKE, IKEDBG, IPSEC, IPSECDBG, AUTH und AUTHDBG. Wenn Sie Zertifikate verwenden, fügen Sie der Liste die CERT-Klasse hinzu.

F. Wie kann ich den Datenverkehr zum VPN 3000 Concentrator überwachen?

Antwort: Die HTML-Schnittstelle des VPN 300 Concentrator bietet eine grundlegende Überwachungsfunktion, wenn Sie unter **Überwachung > Sitzungen** suchen. Der VPN 3000 Concentrator kann auch über das Simple Network Management Protocol (SNMP) mithilfe eines von Ihnen gewählten SNMP-Managers überwacht werden. Alternativ können Sie die Cisco VPN/Security Management Solution (VMS) erwerben. Das Cisco VMS stellt wichtige Funktionen bereit, die Sie bei der Bereitstellung der VPN 300 Concentrator-Serie unterstützen und eine detaillierte Überwachung des Remote-Zugriffs und der Site-to-Site-VPNs auf der Basis von IPsec, L2TP und PPTP erfordern. Weitere Informationen zu VMS finden Sie in der VPN Security Management Solution.

F. Verfügt die Cisco VPN Concentrator Serie 3000 über eine integrierte Firewall? Wenn ja, welche Funktionen werden unterstützt?

Antwort: Während die Serie über integrierte Funktionen für Stateless-Port/Filterung und NAT verfügt, empfiehlt Cisco die Verwendung eines Geräts wie der Cisco Secure PIX Firewall für die Unternehmens-Firewall.

F. Welche Routing-Optionen und VPN-Protokolle werden von der Cisco VPN Concentrator Serie 3000 unterstützt?

Antwort: Die Serie unterstützt die folgenden Routing-Optionen:

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

Zu den unterstützten VPN-Protokollen gehören Point-to-Point Tunneling Protocol (PPTP), L2TP, L2TP/IPsec und IPsec mit oder ohne NAT-Gerät zwischen dem VPN 3000 und dem Endclient. IPsec durch NAT wird als NAT-Transparenz bezeichnet.

F. Welche Authentifizierungsmechanismen/-systeme unterstützt die Cisco VPN Concentrator Serie 300 für Client-PCs?

Antwort: NT Domain, RADIUS oder RADIUS-Proxy, RSA Security SecurID (SDI), Digital Certificates und interne Authentifizierung werden unterstützt.

F. Kann ich statische Network Address Translation (NAT) für Benutzer erstellen, die den VPN 3000 Concentrator nutzen?

Antwort: Sie können nur die Port Address Translation (PAT) für die ausgehenden Benutzer durchführen. Auf dem VPN 300-Konzentrator kann keine statische NAT durchgeführt werden.

F. Wie kann ich einem bestimmten PPTP- (Point-to-Point Tunneling Protocol) oder IPsec-Benutzer über den VPN 3000 Concentrator eine statische IP-Adresse zuweisen?

Antwort: In dieser Liste wird erläutert, wie statische IP-Adressen zugewiesen werden:

- **PPTP-Benutzer**Aktivieren Sie im Abschnitt IP-Adressenverwaltung zusätzlich zur Auswahl der Optionen für Ihren Pool oder das Dynamic Host Configuration Protocol (DHCP) die Option **Use Client Address** (Client-Adresse verwenden). Definieren Sie dann den Benutzer und die IP-Adresse im VPN 3000-Konzentrator. Dieser Benutzer erhält bei der Verbindung immer die im VPN-Concentrator konfigurierte IP-Adresse.
- **IPsec-Benutzer**Aktivieren Sie im Abschnitt IP-Adressenverwaltung zusätzlich zur Auswahl der Optionen für Ihren Pool oder DHCP die Option **Adresse von Authentifizierungsserver verwenden**. Definieren Sie dann den Benutzer und die IP-Adresse im VPN 3000-Konzentrator. Dieser Benutzer erhält bei der Verbindung immer die im VPN-Concentrator konfigurierte IP-Adresse. Alle anderen, die derselben Gruppe oder anderen Gruppen angehören, erhalten eine IP-Adresse aus dem globalen Pool oder DHCP.Mit der Cisco VPN 3000 Concentrator-Software ab Version 3.0 haben Sie die Möglichkeit, einen Adresspool auf Gruppenbasis zu konfigurieren. Mit dieser Funktion können Sie auch einem bestimmten Benutzer eine statische IP-Adresse zuweisen. Wenn Sie einen Pool für eine Gruppe konfigurieren, erhält der Benutzer mit statischer IP die ihnen zugewiesene IP-Adresse, und andere Mitglieder derselben Gruppe erhalten IP-Adressen aus dem Gruppenpool. Dies gilt

nur, wenn Sie den VPN Concentrator als Authentifizierungsserver verwenden.

Hinweis: Wenn Sie einen externen Authentifizierungsserver verwenden, müssen Sie den externen Server verwenden, um die Adressen korrekt zuzuweisen.

F. Welche Kompatibilitätsprobleme sind mit den PPTP-Produkten von Microsoft und dem VPN 3000 Concentrator bekannt?

Antwort: Diese Informationen basieren auf der VPN Concentrator Software 3.5 und höher der Serie 3000. VPN Concentrators der Serie 3000, Modelle 3005, 3015, 3020, 3030, 3060, 3080; und Microsoft-Betriebssysteme Windows 95 und höher.

- **Windows 95-DFÜ-Netzwerk (DUN) 1.2**Microsoft Point-to-Point Encryption (MPPE) wird unter DUN 1.2 nicht unterstützt. Um eine Verbindung über MPPE herzustellen, installieren Sie Windows 95 DUN 1.3. Sie können das Microsoft DUN 1.3-Upgrade von der Microsoft-Website herunterladen.
- **Windows NT 4.0**Windows NT wird vollständig für PPTP-Verbindungen (Point-to-Point Tunneling Protocol) zum VPN Concentrator unterstützt. Service Pack 3 (SP3) oder höher ist erforderlich. Wenn Sie SP3 ausführen, sollten Sie die PPTP-Leistungs- und Sicherheits-Patches installieren. Weitere Informationen zur Microsoft PPTP Performance and Security Upgrade for WinNT 4.0 finden Sie auf der Microsoft-Website.Beachten Sie, dass das 128-Bit Service Pack 5 die MPPE-Schlüssel nicht korrekt behandelt und PPTP möglicherweise keine Daten übergibt. In diesem Fall zeigt das Ereignisprotokoll folgende Meldung an:

  ```
  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.
  ```

  Um dieses Problem zu beheben, laden Sie das Upgrade für How to obtain the latest Windows NT Service Pack 6a and Windows NT 4.0 Service Pack 6a Available herunter. Weitere Informationen finden Sie im Microsoft-Artikel MPPE-Schlüssel nicht korrekt behandelt für eine 128-Bit-MS-CHAP-Anforderung .

F. Wie viele Filter sind maximal für einen VPN 3000-Konzentrator zulässig?

Antwort: Die maximale Anzahl der Filter, die Sie auf einer VPN 30xx-Einheit hinzufügen können (selbst auf einer 3030- oder 3060-Einheit), ist auf 100 festgelegt. Benutzer können weitere Informationen zu diesem Problem finden, indem Sie die Cisco Bug-ID CSCdw86558 anzeigen (Support-Vertrag erforderlich).

F. Wie viele Routen sind maximal in der 30xx-Serie von VPN Concentrators verfügbar?

Antwort: Die maximale Anzahl von Routen ist wie folgt:

- Der VPN 3005-Konzentrator hatte zuvor maximal 200 Routen. Diese Zahl wurde jetzt auf 350 Routen erhöht. Weitere Informationen finden Sie unter Cisco Bug ID CSCeb35779 (Support-Vertrag erforderlich).
- Der VPN 3030 Concentrator wurde für bis zu 10.000 Routen getestet.
- Der Grenzwert für die Routing-Tabelle auf den VPN-Konzentratoren 3030, 3060 und 3080 ist proportional zu den verfügbaren Ressourcen/dem verfügbaren Speicher in jedem Gerät.
- Der VPN 3015 Concentrator hat keine vordefinierte Obergrenze. Dies gilt für das Routing

Information Protocol (RIP) und das Open Shortest Path First (OSPF)-Protokoll.
- VPN 3020 Concentrator - Aufgrund der Microsoft-Einschränkung können Windows XP-PCs keine große Anzahl von CSR (Classless Static Routes) empfangen. Der VPN 3000 Concentrator begrenzt die Anzahl der CSRs, die in eine DHCP-INFORM-Nachrichtenantwort eingefügt werden, wenn dies konfiguriert wurde. Der VPN 3000-Konzentrator beschränkt die Anzahl der Routen je nach Klasse auf 28 bis 42.

F. Wie lösche ich die Schnittstellenstatistiken für den VPN 3000 Concentrator vollständig?

Antwort: Wählen Sie **Monitoring > Statistics > MIB-II > Ethernet aus**, und setzen Sie die Statistiken zurück, um die Statistiken für die aktuelle Sitzung zu löschen. Denken Sie daran, dass die Statistiken dadurch nicht vollständig gelöscht werden. Sie müssen neu starten, um die Statistiken zurücksetzen zu können (anstatt sie zu Überwachungszwecken zurückzusetzen).

F. Welche Ports sollte ich für die VPN Concentrator for Network Time Protocol (NTP)-Kommunikation zulassen?

Antwort: TCP- und UDP-Port 123 zulassen.

F. Welche Funktionen haben die UDP-Ports 625xx?

Antwort: Die Ports werden für die VPN-Client-Kommunikation zwischen dem tatsächlichen shim/Deterministic NDIS Extender (DNE) und dem TCP/IP-Stack des PCs verwendet und sind nur für die interne Entwicklung bestimmt. Beispielsweise wird Port 62515 vom VPN-Client zum Senden von Informationen an das VPN-Client-Protokoll verwendet. Weitere Portfunktionen sind hier aufgeführt.

- 62514 - Cisco Systems, Inc. VPN Service to Cisco Systems IPsec Driver
- 62515 - Cisco Systems IPsec-Treiber für Cisco Systems, Inc. VPN-Service
- 62516 - Cisco Systems, Inc. VPN-Service bis XAUTH
- 62517 - XAUTH to Cisco Systems, Inc. VPN-Service
- 62518 - Cisco Systems, Inc. VPN-Service für CLI
- 62519 - CLI zu Cisco Systems, Inc VPN Service
- 62520 - Cisco Systems, Inc. VPN-Service für die Benutzeroberfläche
- 62521 - Benutzeroberfläche für Cisco Systems, Inc. VPN-Service
- 62522 - Protokollmeldungen
- 62523 - Connection Manager für Cisco Systems, Inc. VPN-Service
- 62524 - PPPTool zu Cisco Systems, Inc. VPN-Service

F. Kann ich die unverankerte WebVPN-Leiste entfernen?

Antwort: Sie können weder die unverankerte Symbolleiste entfernen noch verhindern, dass die unverankerte Symbolleiste geladen wird, während Sie die WebVPN-Sitzung einrichten. Das liegt daran, dass beim Schließen dieses Fensters die Sitzung sofort beendet wird und das Fenster erneut geladen wird, wenn Sie erneut versuchen, sich anzumelden. So wurden die WebVPN-Sitzungen ursprünglich konzipiert. Sie können das Hauptfenster schließen, aber das unverankerte Fenster kann nicht geschlossen werden.

Software

F. Unterstützt WebVPN Outlook Web Access (OWA) 2003?

Antwort: Die OWA 2003-Unterstützung für WebVPN auf dem VPN 3000 Concentrator ist jetzt auch für Downloads der Version 4.1.7 verfügbar (Support-Vertrag erforderlich).

F. Wo erhalte ich die neuesten Software-Updates für den VPN 3000 Concentrator?

Antwort: Alle Cisco VPN 300 Concentrators werden mit dem aktuellsten Code ausgeliefert. Benutzer können jedoch die Downloads überprüfen (Support-Vertrag erforderlich), um festzustellen, ob weitere aktuelle Software verfügbar ist.

Die aktuelle Dokumentation zum VPN 3000 Concentrator finden Sie auf der Seite zur Dokumentation des Cisco VPN Concentrator der Serie 300.

F. Benötige ich einen TFTP-Server, um den VPN 3000 Concentrator zu aktualisieren? Gibt es eine alternative Möglichkeit, das Paket zu aktualisieren?

Antwort: Neben der Verwendung von TFTP können Sie den VPN Concentrator aktualisieren, indem Sie die neueste Software auf Ihre Festplatte herunterladen. Navigieren Sie dann von einem Browser auf dem System, auf dem sich die Software befindet, zu **Administration > Software Update** und suchen Sie die heruntergeladene Software auf Ihrer Festplatte (wie zum Öffnen einer Datei). Wenn Sie sie finden, wählen Sie die Registerkarte **Hochladen** aus.

F. Was bedeutet "k9" in den neuesten Codenamen (z. B. in "vpn3000-3.0.4.Rel-k9.bin")?

Antwort: Die Bezeichnung "k9" für den Bildnamen hat die ursprünglich verwendete 3DES-Bezeichnung ersetzt (z. B. vpn3000-2.5.2.F-3des.bin). Somit bedeutet "k9" nun, dass es sich um ein 3DES-Bild handelt.

F. Soll ich die Datenkomprimierungsoption unter der IPsec-Gruppe für alle meine Benutzer verwenden?

Antwort: Die Datenkomprimierung erhöht die Speicheranforderungen und die CPU-Auslastung für jede Benutzersitzung und reduziert somit den Gesamtdurchsatz des VPN Concentrator. Aus diesem Grund empfiehlt Cisco, die Datenkomprimierung nur zu aktivieren, wenn jedes Mitglied der Gruppe ein Remote-Benutzer ist, der eine Verbindung mit einem Modem herstellt. Wenn ein Mitglied der Gruppe über Breitband eine Verbindung herstellt, aktivieren Sie keine Datenkomprimierung für die Gruppe. Teilen Sie die Gruppe stattdessen in zwei Gruppen auf: eine für Modembenutzer und eine für Breitbandbenutzer. Aktivieren Sie die Datenkomprimierung nur für die Gruppe der Modembenutzer.

Weitere erweiterte Funktionen

F. Funktioniert der Lastenausgleich mit LAN-zu-LAN-Verbindungen?

Antwort: Der Lastenausgleich ist nur bei Remote-Sitzungen wirksam, die mit dem Cisco VPN Software Client (Version 3.0 und höher) initiiert wurden. Alle anderen Clients (PPTP, L2TP) und LAN-zu-LAN-Verbindungen können eine Verbindung zu einem VPN-Konzentrator herstellen, für den der Lastenausgleich aktiviert ist. Sie können jedoch nicht am Lastenausgleich teilnehmen.

F. Wie entschlüssle ich die Passwörter aus der Konfigurationsdatei?

Antwort: Gehen Sie zu **Configuration > System > Management Protocols > XML** und dann zu **Administration. | XML-Format für die Dateiverwaltung**. Verwenden Sie den gleichen oder einen anderen Namen, und öffnen Sie die Datei, um die Kennwörter anzuzeigen.

F. Kann ich Virtual Router Redundancy Protocol (VRRP) und Load Balancing zusammen verwenden?

Antwort: Sie können den Lastenausgleich nicht mit VRRP verwenden. In einer VRRP-Konfiguration bleibt das Backup-Gerät inaktiv, es sei denn, der aktive VPN-Concentrator schlägt fehl. In einer Lastenausgleichskonfiguration gibt es keine freien Geräte.

F. Muss der gesamte VPN-Datenverkehr des Remote-Zugriffs-Clients über einen verschlüsselten Tunnel zum VPN Concentrator im Unternehmen oder Service Provider geleitet werden? Kann beispielsweise ein einfacher Internetzugriff auf andere Websites direkt über die Internetverbindung des ISP möglich sein?

Antwort: Ja. Dieses Konzept wird als "Split-Tunneling" bezeichnet. Split-Tunneling ermöglicht den sicheren Zugriff auf Unternehmensressourcen über einen verschlüsselten Tunnel, während der Internetzugriff direkt über die Ressourcen des ISP ermöglicht wird (dadurch wird das Unternehmensnetzwerk vom Pfad für den Webzugriff ausgeschlossen). Die Cisco VPN 300 Concentrator-Serie für den Cisco VPN-Client und den VPN 3002 Hardware-Client unterstützt Split-Tunneling. Für zusätzliche Sicherheit ist diese Funktion vom Administrator des VPN Concentrator und nicht vom Benutzer steuerbar.

F. Ist es sicher, Split-Tunneling zu verwenden?

Antwort: Durch Split-Tunneling können Sie während der Verbindung über den VPN-Tunnel bequem im Internet surfen. Es besteht jedoch ein gewisses Risiko, wenn der mit dem Unternehmensnetzwerk verbundene VPN-Benutzer anfällig für Angriffe ist. Es wird empfohlen, dass die Benutzer in diesem Fall eine persönliche Firewall verwenden. Die Versionshinweise für eine beliebige VPN-Client-Version behandeln die Interoperabilität mit persönlichen Firewalls.

F. Wie funktioniert der Lastenausgleich mit dem Cisco VPN 3000 Concentrator?

Antwort: Die Last wird als Prozentsatz berechnet, der von den aktiven Verbindungen abgeleitet ist, geteilt durch die maximal konfigurierten Verbindungen. Der Director Switch versucht immer, die geringste Last zu haben, da er durch die zusätzliche (inhärente) Last belastet wird, die bei der Wartung aller administrativen LAN-zu-LAN-Sitzungen, der Berechnung aller anderen Cluster-Elemente-Ladevorgänge anfällt, und er für alle Client-Umleitungen verantwortlich ist.

Bei einem neu konfigurierten funktionalen Cluster wird der Director-Switch etwa 1 Prozent geladen, bevor Verbindungen hergestellt wurden. Aus diesem Grund leitet der Director Verbindungen zum Backup-Konzentrator um, bis der Lastanteil für die Sicherung größer ist als der

Lastanteil für den Director. Beispiel: Bei zwei VPN 3030-Concentrators im Leerlauf ist der Director-Switch mit einer Last von 1 Prozent ausgestattet. Dem sekundären Gerät werden 30 Verbindungen (2 % Last) zugewiesen, bevor der Director Verbindungen akzeptiert.

Um zu überprüfen, ob der Director-Manager Verbindungen akzeptiert, gehen Sie zu **Configuration > System > General > Sessions** und senken Sie die maximale Anzahl von Verbindungen zu einer künstlich niedrigen Zahl, um die Auslastung des Backup-VPN-Concentrators schnell zu erhöhen.

F. Wie viele Headend-Geräte kann der VPN Monitor verfolgen?

Antwort: Der VPN Monitor kann 20 Headend-Geräte verfolgen. In einem Hub-and-Spoke-Szenario werden Verbindungen von Remote-Standorten am Headend überwacht. Es ist nicht erforderlich, alle Remote-Standorte und Benutzer zu überwachen, da diese Informationen auf dem Hub-Router nachverfolgt werden können. Diese Headend-Geräte können bis zu 20.000 Remote-Benutzer oder 2.500 Remote-Standorte unterstützen. Ein Dual-Homed VPN-Gerät, das an die Spoke-Standorte ausgeht, zählt als zwei der maximal 20 Geräte, die überwacht werden können.

Zugehörige Informationen

- Support-Seite für Cisco VPN 3000 Concentrator
- Cisco VPN 3000 Client Support-Seite
- Technischer Support und Dokumentation für Cisco Systeme