Häufig gestellte Fragen zum VPN-Client

Inhalt

Einführung

Dieses Dokument beantwortet häufig gestellte Fragen zum Cisco VPN Client.

Hinweis: Die Namenskonventionen für die verschiedenen VPN-Clients sind wie folgt:

- Nur Cisco Secure VPN Client Version 1.0 bis 1.1a
- Nur Cisco VPN 3000 Client Version 2.x
- Cisco VPN Client 3.x oder höher

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

VPN-Client-Software herunterladen

F. Wo kann ich die Cisco VPN Client-Software herunterladen?

Antwort: Sie müssen sich anmelden und über einen gültigen Servicevertrag verfügen, um auf die Cisco VPN Client-Software zugreifen zu können. Die Cisco VPN Client-Software kann von der Cisco Download Software-Seite heruntergeladen werden (nur registrierte Kunden). **Wenn Sie keinen gültigen Servicevertrag mit Ihrem Cisco.com-Profil haben, können Sie sich nicht anmelden und die VPN-Client-Software herunterladen.**

Um einen gültigen Servicevertrag zu erhalten, können Sie:

- Wenden Sie sich an Ihr Cisco Account Team, wenn Sie einen direkten Kaufvertrag abgeschlossen haben.
- Wenden Sie sich an einen Cisco Partner oder Reseller, um einen Servicevertrag zu erwerben.

- Verwenden Sie den Profile Manager (nur registrierte Kunden), um Ihr Cisco.com-Profil zu aktualisieren und eine Zuordnung zu einem Servicevertrag anzufordern.

F. Der Download-Bereich des Cisco VPN-Clients scheint leer zu sein. Warum?

Antwort: Wenn Sie den VPN-Clientbereich des Software Center erreichen (nur registrierte Kunden), sollten Sie in der Mitte der Seite den Download-Bereich für das gewünschte Betriebssystem auswählen.

F. Wie kann ich die Stateful Firewall-Funktion während der Installation des Cisco VPN-Clients deaktivieren?

Antwort: Für VPN-Client-Versionen vor 5.0:

Im Abschnitt Dokumentationsänderungen der Versionshinweise zum VPN-Client Version 4.7 finden Sie Informationen zu den beiden Themen "Verwenden von MSI zum Installieren des Windows-VPN-Clients ohne Stateful Firewall" und "Verwenden von InstallShield zum Installieren des Windows-VPN-Clients ohne Stateful Firewall".

Für VPN-Clientversionen nach 5.0:

Ab Cisco VPN Client Release 5.0.3.0560 wurde ein MSI-Installations-Flag hinzugefügt, um die Installation der Gilde in Firewall-Dateien zu vermeiden:

```
msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1
```

Weitere Informationen hierzu finden Sie im Abschnitt "Installation von Firewall-Dateien umgehen, wenn keine Stateful Firewall erforderlich ist".

F. Wie kann ich den Cisco VPN Client deinstallieren oder aktualisieren?

Antwort: Weitere Informationen zur manuellen Deinstallation (InstallShield) und zum anschließenden Upgrade des Cisco VPN Client Version 3.5 und höher für Windows 2000 und Windows XP finden Sie unter Entfernen einer mit dem MSI Installer installierten VPN Client-Version.

Der Cisco VPN Client für Windows 2000 und die Windows XP-Software können Updates und neue Versionen automatisch über einen Tunnel von einem VPN 3000 Concentrator oder einem anderen VPN-Server herunterladen, der Benachrichtigungen bereitstellen kann. Voraussetzung hierfür ist, dass Remote-Benutzer den VPN-Client für Windows 4.6 oder höher auf ihren PCs installieren müssen, um die automatische Aktualisierungsfunktion verwenden zu können.

Mit dieser Funktion, dem so genannten automatischen Update, müssen Benutzer keine alte Version der Software deinstallieren, einen Neustart durchführen, die neue Version installieren und dann erneut neu starten. Stattdessen stellt ein Administrator Aktualisierungen und Profile auf einem Webserver zur Verfügung. Wenn ein Remote-Benutzer den VPN-Client startet, erkennt die Software, dass ein Download verfügbar ist, und erhält diesen automatisch. Weitere Informationen finden Sie unter Verwalten von AutoUpdates und Funktionsweise von automatischen Aktualisierungen.

Informationen zum Konfigurieren von Client-Updates auf einer Cisco Adaptive Security Appliance

der Serie ASA 5500 mit ASDM finden Sie unter Konfigurieren von Client-Software-Updates mithilfe von ASDM.

F. Ich möchte die VPN-Clients für Vista anpassen. Mir ist klar, dass es mit der neuen VPN Client-Version für Vista keine Datei wie oem.mst gibt. Wie können wir die neuen VPN Client-Versionen (5.x) anpassen, oder wo kann ich diese Datei finden?

Antwort: Die MST-Datei wird nicht mehr mit dem VPN-Client bereitgestellt, Sie können sie jedoch von der Download-Software-Seite herunterladen (nur registrierte Kunden):

Dateiname: Readme und MST für die Installation auf der internationalen Windows-Version.

Betriebssystem

F. Bietet Cisco einen VPN-Client für Windows Vista?

Antwort: Die neue Version Cisco VPN Client 5.0.07 unterstützt Windows Vista auf x86 (32-Bit) und x64. Weitere Informationen finden Sie in den Versionshinweisen 5.0.07.0240.

Hinweis: Cisco VPN Client wird nur bei der Installation von Windows Vista Clean unterstützt. Dies bedeutet, dass ein Upgrade eines Windows-Betriebssystems auf Windows Vista von der VPN-Clientsoftware nicht unterstützt wird. Sie müssen Windows Vista neu installieren und anschließend die Vista VPN Client-Software installieren.

Hinweis: Wenn Sie keinen gültigen Servicevertrag mit Ihrem Cisco.com-Profil haben, können Sie sich nicht anmelden und die VPN Client-Software herunterladen. Weitere Informationen finden Sie unter VPN-Client-Software herunterladen.

Tipp: Der Cisco AnyConnect VPN Client ist jetzt auch für Windows-Betriebssysteme verfügbar, darunter Vista 32 und 64-Bit. Der AnyConnect-Client unterstützt SSL und DTLS. IPsec wird derzeit nicht unterstützt. Darüber hinaus ist AnyConnect nur für die Verwendung mit einer Cisco Adaptive Security Appliance verfügbar, die Version 8.0(2) oder höher ausführt. Der Client kann auch im Weblaunch-Modus verwendet werden, wenn IOS-Appliances die Version 12.4(15)T ausführen. VPN 3000 wird nicht unterstützt.

Der Cisco AnyConnect VPN Client und die ASA 8.0 können über das Software Center bezogen werden (nur registrierte Kunden). Weitere Informationen zum AnyConnect Client finden Sie in den Versionshinweisen zum Cisco AnyConnect VPN Client. Weitere Informationen zur ASA 8.0 finden Sie in den Versionshinweisen zu Adaptive Security Appliances der Serie ASA 5500 von Cisco.

Hinweis: Wenn Sie keinen gültigen Servicevertrag mit Ihrem Cisco.com-Profil haben, können Sie sich nicht anmelden und die AnyConnect VPN Client- oder ASA-Software herunterladen. Weitere Informationen finden Sie unter VPN-Client-Software herunterladen.

F. Wie richte ich eine PPTP-Verbindung von einem Microsoft Windows-PC aus ein?

Antwort: Das Setup hängt von der Microsoft Windows-Version ab, die Sie ausführen. Wenden Sie sich für spezifische Informationen an Microsoft. Hier finden Sie Setup-Anweisungen für einige der gängigen Windows-Versionen:

Windows 95

1. Installieren Sie Msdun13.exe.
2. Wählen Sie **Programme > Zubehör > DFÜ-Netzwerk aus**.
3. Erstellen Sie eine neue Verbindung mit dem Namen "PPTP".
4. Wählen Sie den **VPN-Adapter** als Gerät für die Verbindung aus.
5. Geben Sie die IP-Adresse der öffentlichen Schnittstelle des Switches ein, und klicken Sie auf **Fertig stellen**.
6. Kehren Sie zur gerade erstellten Verbindung zurück, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften** aus.
7. Deaktivieren Sie unter Zulässige Netzwerkprotokolle mindestens die Option **netbeui**.
8. Konfigurieren Sie die Einstellung **Erweiterte Optionen**: Lassen Sie die Standardeinstellungen unverändert, damit der Switch und der Client die Authentifizierungsmethode automatisch aushandeln können.Aktivieren Sie **Require Encrypted Password**, um die CHAP-Authentifizierung (Challenge Handshake Authentication Protocol) zu erzwingen.Aktivieren Sie **Erforderliches verschlüsseltes Kennwort** und **Datenverschlüsselung erforderlich**, um die MS-CHAP-Authentifizierung zu erzwingen.

Windows 98

1. Gehen Sie wie folgt vor, um die PPTP-Funktion zu installieren: Wählen Sie **Start > Einstellungen > Systemsteuerung > Neue Hardware hinzufügen aus**, und klicken Sie auf **Weiter**.Klicken Sie auf **Aus Liste auswählen**, wählen Sie **Netzwerkadapter aus**, und klicken Sie auf **Weiter**.Wählen Sie **Microsoft** im linken Bereich und **Microsoft VPN Adapter** im rechten Bereich aus.
2. Gehen Sie wie folgt vor, um die PPTP-Funktion zu konfigurieren: Wählen Sie **Start > Programme > Zubehör > Kommunikation > DFÜ-Netzwerk aus**.Klicken Sie auf **Neue Verbindung herstellen**, und wählen Sie **Microsoft VPN Adapter** für Geräte auswählen aus. Die IP-Adresse des VPN-Servers= 3000 Tunnel-Endpunkt.
3. Führen Sie die folgenden Schritte aus, um den PC so zu ändern, dass auch Kennwort Authentication Protocol (PAP) zugelassen wird: **Hinweis:** Die Windows 98-Standardauthentifizierung besteht in der Verwendung von Kennwortverschlüsselung (CHAP oder MS-CHAP).Wählen Sie **Eigenschaften > Servertypen aus**.Deaktivieren Sie **Verschlüsseltes Kennwort erforderlich**. In diesem Bereich können Sie die Datenverschlüsselung (Microsoft Point-to-Point Encryption [MPPE] oder kein MPPE) konfigurieren.

Windows 2000

1. Wählen Sie **Start > Programme > Zubehör > Kommunikation > Netzwerk- und DFÜ-Verbindungen aus**.
2. Klicken Sie auf **Neue Verbindung herstellen** und dann auf **Weiter**.
3. Wählen Sie **Verbinden mit einem privaten Netzwerk über das Internet, und wählen Sie vorher eine Verbindung** (wählen Sie diese nicht aus, wenn Sie ein LAN haben), und klicken Sie auf **Weiter**.
4. Geben Sie den Hostnamen oder die IP-Adresse des Tunnelendpunkts (3000) ein.
5. Wenn Sie den Kennworttyp ändern müssen, wählen Sie **Eigenschaften > Sicherheit für die Verbindung > Erweitert aus**. Der Standardwert ist MS-CHAP und MS-CHAP v2 (nicht CHAP oder PAP). In diesem Bereich können Sie die Datenverschlüsselung (MPPE oder kein MPPE) konfigurieren.

Windows NT

Weitere Informationen finden Sie unter Installieren, Konfigurieren und Verwenden von PPTP mit Microsoft-Clients und -Servern .

F. Welche Betriebssystemversionen unterstützen den Cisco VPN Client?

Antwort: Für den VPN-Client wird ständig die Unterstützung weiterer Betriebssysteme hinzugefügt. Informationen hierzu finden Sie in den Systemanforderungen in den Versionshinweisen für den VPN-Client 5.0.07 oder unter Cisco Hardware- und VPN-Clients, die IPsec/PPTP/L2TP unterstützen.

Hinweise:

- Der VPN-Client unterstützt Dualprozessor- und Dualcore-Workstations für Windows XP und Windows Vista.
- Windows VPN Client Release 4.8.00.440 war die endgültige Version, die das Betriebssystem Windows 98 offiziell unterstützte.
- Windows VPN Client Release 4.6.04.0043 war die endgültige Version, die das Windows NT-Betriebssystem offiziell unterstützte.
- Cisco VPN Client 5.0.07 unterstützt Windows Vista und Windows 7 sowohl in der x86- (32-Bit) als auch in der x64-Version (64-Bit).
- Der Cisco VPN Client unterstützt nur Windows XP 32-Bit, Windows XP 64-Bit wird jedoch nicht unterstützt.**Hinweis:** Windows Vista 32-Bit-Unterstützung war in allen 5.x-Versionen verfügbar. Die 64-Bit-Unterstützung wurde durch den Cisco VPN Client Version 5.0.07 hinzugefügt.

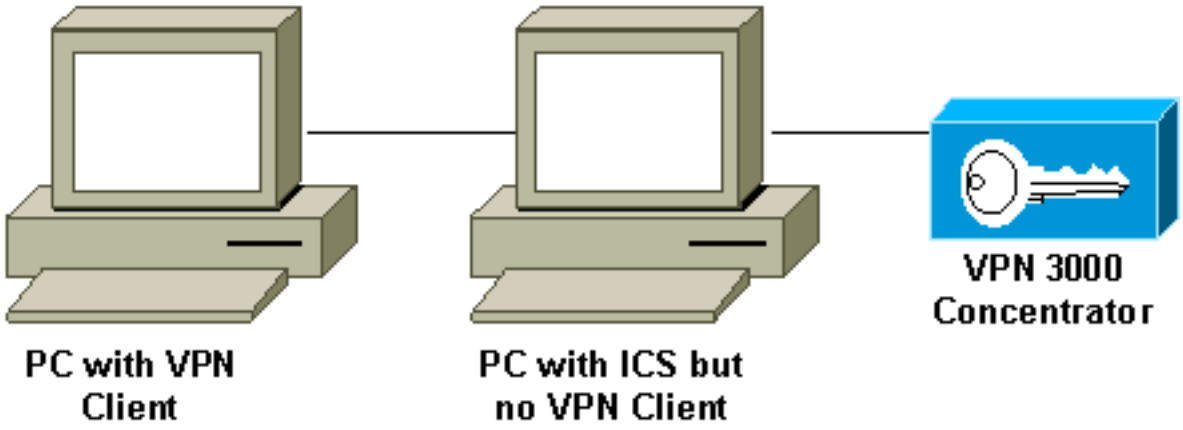
F. Muss ich ein Administrator auf Windows NT/2000-Computern sein, um den VPN-Client zu laden?

Antwort: Ja, Sie müssen über Administratorrechte verfügen, um den VPN-Client unter Windows NT und Windows 2000 zu installieren, da diese Betriebssysteme Administratorrechte benötigen, um eine Bindung an die vorhandenen Netzwerktreiber herzustellen oder neue Netzwerktreiber zu installieren. Die VPN-Client-Software ist Netzwerksoftware. Sie müssen über Administratorrechte verfügen, um sie zu installieren.

F. Kann der Cisco VPN Client mit Microsoft Internet Connection Sharing (ICS) verwendet werden, die auf demselben Computer installiert ist?

Antwort: Nein, der Cisco VPN 300 Client ist nicht mit Microsoft ICS auf demselben System kompatibel. Sie müssen ICS deinstallieren, bevor Sie den VPN-Client installieren können. Weitere Informationen finden Sie unter Deaktivieren von ICS bei der Vorbereitung auf die Installation oder das Upgrade auf Cisco VPN Client 3.5.x unter Microsoft Windows XP.

Obwohl der VPN-Client und der ICS auf demselben PC nicht funktionieren, funktioniert diese Anordnung nicht.



F. Mein VPN-Client scheint sich nur mit bestimmten Adressen zu verbinden. Ich verwende Windows XP. Was soll ich tun?

Antwort: Überprüfen Sie, ob die integrierte Firewall in Windows XP deaktiviert ist.

F. Ist der Cisco VPN Client mit der Windows XP Stateful Firewall kompatibel?

Antwort: Dieses Problem wurde behoben. Weitere Informationen finden Sie unter CSCdx15865 (nur registrierte Kunden) im Bug Toolkit.

F. Ist bei der Installation des VPN-Clients unter Windows XP und Windows 2000 die Benutzeroberfläche für mehrere Benutzer deaktiviert?

Antwort: Die Installation deaktiviert den Begrüßungsbildschirm und das schnelle Umschalten der Benutzer. Weitere Informationen finden Sie im Bug Toolkit unter Cisco Bug ID CSCdu24073 (nur registrierte Kunden).

F. Wie kann ich den VPN-Client für Linux nach der Ausführung in den Hintergrund verschieben? Wenn ich eine Verbindung wie vpnclient connect foo initiiere, komme ich rein, aber die Shell wird zurückgegeben.

Antwort: Geben Sie nach der Anmeldung Folgendes ein:

- ^Z
- BG

F. Wenn ich den Cisco VPN Client unter Windows XP Home Edition installiere, wird die Taskleiste nicht angezeigt. Wie kann ich das rückgängig machen?

Antwort: Wählen Sie **Systemsteuerung > Netzwerkverbindungen > Netzwerkbrücke entfernen**, um diese Einstellung anzupassen.

F. Wenn ich versuche, Linux VPN Client auf RedHat 8.0 zu installieren, bekomme ich einen Fehler, der besagt, dass das Modul nicht geladen werden kann, weil das Modul mit GCC 2 kompiliert wurde und der Kernel mit GCC 3.2 kompiliert wurde. Was soll ich tun?

Antwort: Dies liegt daran, dass die neue Version von RedHat eine neuere Version des GCC-Compilers (3.2+) hat, was dazu führt, dass der aktuelle Cisco VPN-Client fehlschlägt. Dieses Problem wurde behoben und ist in Cisco VPN 3.6.2a verfügbar. Weitere Informationen finden Sie unter Cisco Bug ID CSCdy49082 (nur registrierte Kunden) im Bug Toolkit oder laden Sie die Software vom VPN Software Center herunter (nur registrierte Kunden).

F. Warum deaktiviert die Software Fast User Switching, wenn ich VPN Client 3.1 unter Windows XP installiere?

Antwort: Microsoft deaktiviert Fast User Switching in Windows XP automatisch, wenn eine GINA.dll in der Registrierung angegeben ist. Der Cisco VPN Client installiert CSgina.dll, um die Funktion "Start Before Login" (Vor Anmeldung starten) zu implementieren. Wenn Sie Fast User Switching benötigen, deaktivieren Sie die Funktion "Start Before Login" (Vor Anmeldung starten). Registrierte Benutzer erhalten weitere Informationen in der Cisco Bug ID CSCdu24073 (nur registrierte Kunden) im Bug Toolkit.

F. Unterstützt der IPsec-VPN-Client die SBL-Funktion (Start Before Logon) in Windows 7?

Antwort: Die SBL-Funktion wird von IPsec-VPN-Clients unter Windows7 nicht unterstützt. Diese wird vom AnyConnect VPN-Client unterstützt.

Fehlermeldungen

F. Bei der Installation von Cisco VPN Client 4.x wird folgende Fehlermeldung angezeigt: `Warnung 201: Das erforderliche VPN-Subsystem ist nicht verfügbar. Sie können keine Verbindung zum Remote-VPN-Server herstellen`

Antwort: Dieses Problem kann durch auf Ihrem VPN-Client-Computer installierte Firewall-Pakete verursacht werden. Um diese Fehlermeldung zu vermeiden, stellen Sie sicher, dass zum Zeitpunkt der Installation keine Firewall oder Virenschutzprogramme auf Ihrem Computer installiert oder ausgeführt werden.

F. Ich habe ein Upgrade auf Mac OS X 10.3 durchgeführt (bekannt als "Panther"), jetzt zeigt mein Cisco VPN Client 4.x jedoch folgende Fehlermeldungen an: `Sichere VPN-Verbindung wird lokal durch Client-Grund beendet: Das Sicherheits-Gateway konnte nicht kontaktiert werden.`

Antwort: Sie müssen UseLegacyIKEPort=0 dem Profil (.pcf-Datei) hinzufügen, das im Verzeichnis /etc/CiscoSystemsVPNClient/Profiles/Profile für den Cisco VPN Client 4.x gefunden wurde, um mit Mac OS X 10.3 ("Panther") arbeiten zu können.

F. Beim Versuch, den VPN-Client zu deinstallieren, wird die folgende Fehlermeldung angezeigt: `Fehlermeldung: Die Deinstallationsdatei konnte nicht gefunden werden.`. Was bedeutet diese Fehlermeldung und wie kann ich die Deinstallation erfolgreich abschließen?

Antwort: Überprüfen Sie die Systemsteuerung des Netzwerks, um sicherzustellen, dass der deterministische NDIS Extender (DNE) nicht installiert wurde. Wählen Sie außerdem **Microsoft >**

Current Version > Uninstall, um die Deinstallationsdatei zu suchen. Entfernen Sie die **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5}**-Datei, und versuchen Sie die Deinstallation erneut.

F. Ich kann den VPN-Client nicht auf Windows 2000 Professional installieren. Ich erhalte diesen Fehler: `Eine Installationssupportdatei konnte nicht installiert werden.` Katastrophenversagen. Was soll ich tun?

Antwort: Entfernen Sie den **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall**-Schlüssel. Starten Sie anschließend den Computer neu, und installieren Sie den VPN-Client neu.

Hinweis: Um den richtigen Schlüssel für die Cisco VPN Client-Software unter dem Pfad HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<*Schlüssel zu bestimmen*> zu finden, gehen Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\, und klicken Sie auf **VPN Client**. Zeigen Sie im rechten Fenster den Deinstallationspfad (unter der Spalte Name) an. Die entsprechende Spalte Daten zeigt den Wert des VPN-Client-Schlüssels an. Notieren Sie sich diesen Schlüssel, gehen Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\, wählen Sie den bestimmten Schlüssel aus, und löschen Sie ihn.

Weitere Informationen finden Sie unter Initialisierungsfehler-Fehlerbehebung und unter Cisco Bug ID CSCdv15391 (nur registrierte Kunden) im Bug Toolkit.

F. Wenn ich versuche, Linux VPN Client auf RedHat 8.0 zu installieren, erhalte ich einen Fehler, der besagt, dass das Modul nicht geladen werden kann, weil das Modul mit GCC 2 kompiliert wurde und der Kernel mit GCC 3.2 kompiliert wurde. Was soll ich tun?

Antwort: Dieses Problem tritt auf, weil die neue Version von RedHat eine neuere Version des GCC-Compilers (3.2+) hat, wodurch der aktuelle Cisco VPN-Client fehlschlägt. Dieses Problem wurde behoben und ist in Cisco VPN 3.6.2a verfügbar. Weitere Informationen finden Sie unter Cisco Bug ID CSCdy49082 (nur registrierte Kunden) im Bug Toolkit oder zum Download der Software aus dem VPN Software Center (nur registrierte Kunden) .

F. Ich erhalte die Fehlermeldung "Peer reagiert nicht mehr", wenn mein Linux Client 3.5 versucht, eine IPsec-Verbindung zu einem PIX oder einem VPN 3000-Konzentrator herzustellen. Was soll ich tun?

Antwort: Das Symptom dieses Problems ist, dass der Linux-Client scheinbar versucht, eine Verbindung herzustellen, aber er erhält nie eine Antwort vom Gateway-Gerät.

Das Linux-Betriebssystem verfügt über eine integrierte Firewall (ipketten), die UDP-Port 500, UDP-Port 1000 und ESP-Pakete (Encapsulating Security Payload) blockiert. Da die Firewall standardmäßig aktiviert ist, müssen Sie entweder die Firewall deaktivieren oder die Ports für die IPsec-Kommunikation für eingehende und ausgehende Verbindungen öffnen, um das Problem zu beheben.

F. Ich erhalte einen Kernel-Erweiterungsfehler, wenn ich versuche, Cisco VPN 500 5.2.2 Client unter Mac OS X 10.3 auszuführen. Was soll ich tun?

Antwort: Wie in den Versionshinweisen zum Produkt angegeben, wird der Cisco VPN 5000 Client bis Version 10.1.x unterstützt und wird daher von Version 10.3 nicht unterstützt. Es ist möglich, den VPN-Client so zu konfigurieren, dass er funktioniert, wenn Sie die Berechtigungen für zwei der installierten Dateien zurücksetzen, nachdem Sie das Installationsskript ausgeführt haben. Hier ein Beispiel:

Hinweis: Diese Konfiguration wird *nicht* von Cisco unterstützt.

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

F. Ich kann die neue Version des Cisco VPN Client nicht installieren. Bei der Installation erhalte ich eine der folgenden Fehlermeldungen: "**Fehler DNEinst Ausführungsfehler bei der Installation von DNE, Rückgabecode -2146500093**" oder "**InstallDNE-Fehler: DNEinst Ausführungsfehler bei der Installation von DNE, return -2147024891.**" Dieses Problem tritt auf, wenn ich den Deterministischen Network Enhancer installiert habe.

Antwort: Installieren Sie das neueste DNE-Upgrade von Deterministic Networks .

F. Ich erhalte diese Protokolle für den Cisco VPN Client, wenn ich eine Verbindung herstelle:

```
208    15:09:08.619  01/17/08  Sev=Debug/7CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209    15:09:08.619  01/17/08  Sev=Warning/2CVPND/0xE3400003
Function RegOpenKey failed with an error code of 0x00000002(WindowsVirtualAdapter:558)

210    15:09:08.619  01/17/08  Sev=Warning/3CVPND/0xE340000C
The Client was unable to enable the Virtual Adapter because it could not open the device.
```

Antwort: Es handelt sich um eine recht allgemeine Fehlermeldung, die normalerweise eine manuelle Deinstallation des Clients erfordert. Folgen Sie den Anweisungen in diesem Link. Entfernen einer mit dem MSI Installer installierten VPN Client-Version.

Wenn Sie die Deinstallation abgeschlossen haben, stellen Sie sicher, dass Sie neu starten. Installieren Sie dann den Client neu. Stellen Sie sicher, dass Sie als Benutzer angemeldet sind, der Administratorrechte auf dem lokalen Computer hat.

F. Wenn ich versuche, den Cisco VPN Client unter Mac OS zu verbinden, erhalte ich die folgende Fehlermeldung: **Fehler 51 - Kommunikation mit dem VPN-Subsystem nicht möglich.** Wie kann ich dieses Problem beheben?

Antwort: Das Problem kann behoben werden, wenn Sie den Dienst neu starten, nachdem Sie den VPN-Client auf diese Weise geschlossen haben:

So stoppen Sie:

```
sudo kextunload -b com.cisco.nke.ipsec
```

So starten Sie:

`sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN`
Überprüfen Sie außerdem die folgenden Vorgänge auf demselben Computer, auf dem der VPN-Client installiert ist, und deaktivieren Sie sie.

- Alle virtuellen Software (z. B. VMWare Fusions, Parallels, Crossover).
- Alle Antivirus-/Firewall-Software.
- Kompatibilität des VPN-Clients mit dem 64-Bit-Betriebssystem; Weitere Informationen finden Sie in den Versionshinweisen zum Cisco VPN-Client.

F. Ich erhalte die Meldung "Grund 442: Fehler "Virtual Adapter" konnte nicht aktiviert werden. Wie kann ich diesen Fehler beheben?

Antwort: Der `Grund 442: Der` Fehler `für die Aktivierung des virtuellen Adapters` wird angezeigt, nachdem Vista meldet, dass eine doppelte IP-Adresse erkannt wurde. Die nachfolgenden Verbindungen schlagen mit derselben Meldung fehl, Vista meldet jedoch nicht, dass eine doppelte IP-Adresse erkannt wurde. Weitere Informationen zur Behebung dieses Problems finden Sie unter Fehler 442 für doppelte IP-Adressenauslöser unter Windows Vista.

F. Bei der Installation des Cisco VPN Client wird der Fehler **`Deterministic Network Enhancer Add Plugin Failed (deterministisches Hinzufügen eines Plugins fehlgeschlagen)`** ausgegeben. Wie wird dieser Fehler behoben?

Antwort: Durch die Installation des DNE-Adapters kann das Problem behoben werden. Es ist besser, die Installshield-Version anstelle von MSI für die Installation zu verwenden.

F. Ich habe diesen Fehler erhalten: **`Grund 442: Fehler bei der Aktivierung des virtuellen Adapters`**. Wie kann ich dieses Problem beheben?

Antwort: Dieser Fehler wird angezeigt, nachdem Windows 7 und Windows Vista eine doppelte IP-Adresse erkannt haben. Die nachfolgenden Verbindungen schlagen mit derselben Meldung fehl, aber das Betriebssystem meldet nicht, dass die doppelte IP-Adresse erkannt wurde. Weitere Informationen zur Behebung dieses Problems finden Sie unter Fehler 442 für doppelte IP-Adressenauslöser unter Windows 7 und Vista.

F. Wenn ich versuche, den VPN Client 4.9 für MAC OS 10.6 zu starten, wird folgender Fehler angezeigt: **`Fehler 51: Kommunikation mit dem VPN-Subsystem nicht möglich.`** Wie kann dieses Problem behoben werden?

Antwort: Dieses Problem tritt auf, weil 64-Bit-Unterstützung bei Cisco VPN Client für MAC OS Version 4.9 nicht verfügbar ist. Als Problemumgehung können Sie im 32-Bit-Kernelmodus booten. Weitere Informationen finden Sie in den Versionshinweisen für MAC OSX unter Cisco Bug ID CSCth11092 (nur registrierte Kunden) und Cisco VPN Client.

Kompatibilität mit Drittanbietern

F. Ist der Nortel Client mit den Cisco VPN 3000 Concentrators kompatibel?

Antwort: Nein. Der Nortel Client kann keine Verbindung zum Cisco VPN 3000 Concentrator

herstellen.

F. Kann ich VPN-Clients von anderen Anbietern, wie z. B. dem Nortel Contivity VPN Client, gleichzeitig mit dem Cisco VPN Client installieren lassen?

Antwort: Nein. Es sind Probleme bekannt, wenn mehrere VPN-Clients auf demselben PC installiert sind.

F. Werden Cisco VPN-Clients mit VPN-Konzentratoren von Drittanbietern unterstützt?

Antwort: Cisco VPN-Clients werden nicht von VPN-Konzentratoren von Drittanbietern unterstützt.

Authentifizierung

F. Wie speichern Cisco VPN-Clients Version 1.1 und 3.x intern digitale Zertifikate (X.509v3)?

Antwort: Der Cisco VPN Client 1.1 verfügt über einen eigenen Zertifikatsspeicher. Der Cisco VPN Client 3.x kann Zertifikate entweder über die Common Application Programming Interface (CAPI) im Microsoft-Store speichern oder sie im eigenen Speicher (RSA Data Security) von Cisco speichern.

F. Kann ich denselben Gruppennamen und denselben Benutzernamen im VPN-Konzentrator haben?

Antwort: Nein, Gruppenname und Benutzername dürfen nicht identisch sein. Dies ist ein bekanntes Problem, das in den Softwareversionen 2.5.2 und 3.0 vorkommt und in 3.1.2 integriert ist. Weitere Informationen finden Sie im Bug Toolkit unter Cisco Bug ID CSCdw29034 (nur registrierte Kunden).

F. Werden auf dem Cisco VPN Client zu PIX Challenge-Karten wie Defender unterstützt?

Antwort: Nein, Karten dieses Typs werden nicht unterstützt.

VPN-Client-Softwareversion

F. Was ist mit der Option "Set MTU Utility" (MTU-Dienstprogramm festlegen) in Cisco VPN Client Version 2.5.2 und früher passiert?

Antwort: Der Cisco VPN Client passt jetzt die MTU-Größe (Maximum Transmission Unit) an. Die Option MTU Utility festlegen ist nicht mehr ein erforderlicher Installationsschritt. Die Option Set MTU (MTU festlegen) wird hauptsächlich zur Behebung von Verbindungsproblemen verwendet. Die Option SetMTU für einen Windows-Computer kann über **Start > Programme > Cisco Systems VPN Client > SetMTU** ausgewählt werden. Weitere Informationen zur SetMTU-Option und zum Festlegen dieser Option in anderen Betriebssystemen finden Sie unter Ändern der MTU-Größe

durch die SetMTU-Option.

F. Welche Sprachen werden von der Benutzeroberfläche des Cisco VPN Client nach Version 4.0 unterstützt?

Antwort: Die in der Benutzeroberfläche von Cisco VPN Client ab Version 4.0 unterstützten Sprachen sind Kanada, Französisch und Japanisch.

F. Welche persönlichen Firewalls werden vom Cisco VPN Client unterstützt?

Antwort: Um ein höheres Maß an Sicherheit zu gewährleisten, kann der VPN Client entweder den Betrieb einer unterstützten Firewall durchsetzen oder eine ausgedrückte Stateful Firewall-Richtlinie für Internetdatenverkehr erhalten.

Derzeit unterstützt der VPN Client 5.0 die folgenden persönlichen Firewalls:

- BlackIce Defender
- Cisco Security Agent
- Sygate Personal Firewall
- Sygate Personal Firewall Pro
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

Ab Version 3.1 wird dem VPN 300 Concentrator eine neue Funktion hinzugefügt, die erkennt, welche persönliche Firewall-Software von Remote-Benutzern installiert wurde, und die Benutzer daran hindert, sich ohne die entsprechende Software anzuschließen. Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen > Client FW**, und klicken Sie auf die Registerkarte für die Gruppe, um diese Funktion zu konfigurieren.

Weitere Informationen zur Durchsetzung von Firewall-Richtlinien auf einem Cisco VPN Client-Computer finden Sie unter Firewall-Konfigurationsszenarien.

F. Gibt es Verbindungsprobleme bei der Verwendung des Cisco VPN Client 3.x mit AOL 7.0?

Antwort: Der Cisco VPN Client kann ohne Split-Tunneling nicht mit AOL 7.0 verwendet werden. Weitere Informationen finden Sie unter CSCdx04842 (nur registrierte Kunden) im Bug Toolkit.

Konfiguration der VPN-Client-Software

F. Warum trennt der Cisco VPN-Client die Verbindung nach 30 Minuten? Kann ich diesen Zeitraum verlängern?

Antwort: Wenn während dieses Zeitraums von 30 Minuten keine Kommunikationsaktivität auf einer Benutzerverbindung besteht, beendet das System die Verbindung. Die Standardeinstellung für die Leerlaufzeitüberschreitung beträgt 30 Minuten mit einem zulässigen Mindestwert von 1 Minute und einem zulässigen Maximalwert von 2.147.483.647 Minuten (mehr als 4.000 Jahre).

Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen**, und wählen Sie den entsprechenden

Gruppennamen aus, um die Einstellung für Leerlaufzeitüberschreitung zu ändern. Wählen Sie **Gruppe ändern**, klicken Sie auf die Registerkarte **HW Client**, und geben Sie den gewünschten Wert in das Feld User Idle Timeout (Benutzer-Leerlaufzeit-Timeout) ein. Geben Sie **0 ein**, um die Zeitüberschreitung zu deaktivieren und eine unbegrenzte Leerlaufzeit zuzulassen.

F. Kann der Cisco VPN Client mit allen vorkonfigurierten Parametern bereitgestellt werden?

Antwort: Wenn die Datei vpnclient.ini bei der ersten Installation mit der VPN Client-Software gebündelt wird, wird der VPN Client während der Installation automatisch konfiguriert. Sie können auch die Profildateien (eine .pcf-Datei für jeden Verbindungseintrag) als vorkonfigurierte Verbindungsprofile für die automatische Konfiguration verteilen. Gehen Sie wie folgt vor, um vorkonfigurierte Kopien der VPN Client-Software zur Installation an Benutzer zu verteilen:

1. Kopieren Sie die VPN Client-Softwaredateien von der Distributions-CD-ROM in jedes Verzeichnis, in dem Sie eine vpnclient.ini (globale) Datei und separate Verbindungsprofile für eine Reihe von Benutzern erstellt haben.**Hinweis:** Für die Mac OS X-Plattform werden vorkonfigurierte Dateien in den Ordner Profile und Ressourcen abgelegt, bevor der VPN Client installiert wird. Die Datei vpnclient.ini wird im Installationsverzeichnis abgelegt. Sie müssen benutzerdefinierte vpnclient.ini-Dateien im Verzeichnis des VPN-Client-Installers auf derselben Ebene wie die Ordner Profile und Ressourcen ablegen. Weitere Informationen finden Sie in Kapitel 2 des VPN-Client-Benutzerhandbuchs für Mac OS X.
2. Vorbereiten und Verteilen der Software. CD-ROM oder Netzwerkverteilung. Stellen Sie sicher, dass sich die Datei "vpnclient.ini" und die Profildateien im gleichen Verzeichnis befinden, in dem sich alle CD-ROM-Bilddateien befinden. Sie können Benutzer über eine Netzwerkverbindung von diesem Verzeichnis installieren lassen. oder Sie können alle Dateien auf eine neue CD-ROM zur Verteilung kopieren. Sie können auch eine selbstextrahierende ZIP-Datei erstellen, die alle Dateien aus diesem Verzeichnis enthält, und die Benutzer dazu veranlassen, diese herunterzuladen und dann die Software zu installieren.
3. Geben Sie den Benutzern alle weiteren erforderlichen Konfigurationsinformationen und -anweisungen. Siehe Kapitel 2 des VPN-Client-Benutzerhandbuchs für Ihre Plattform.

F. Der Cisco VPN Client scheint einen Konflikt mit meiner NIC-Karte zu haben. Wie kann ich eine Fehlerbehebung durchführen?

Antwort: Stellen Sie sicher, dass Sie die neuesten Treiber auf der Netzwerkkarte ausführen. Dies wird immer empfohlen. Wenn möglich sollten Sie testen, ob das Problem speziell auf das Betriebssystem, die PC-Hardware und andere NIC-Karten zurückzuführen ist.

F. Wie kann ich die Verbindung des Cisco VPN-Clients über das DFÜ-Netzwerk automatisieren?

Antwort: Wählen Sie **Optionen > Eigenschaften > Verbindungen**, und lassen Sie den Cisco VPN-Client einen Eintrag für ein DFÜ-Netzwerk abziehen, um die Einwahl in die VPN-Verbindung vollständig zu automatisieren.

F. Wie konfiguriere ich den Cisco VPN 300 Concentrator, um Remote-Benutzer über das VPN-Client-Update zu benachrichtigen?

Antwort: Sie können VPN-Client-Benutzer benachrichtigen, wenn es an der Zeit ist, die VPN-Client-Software auf ihren Remote-Systemen zu aktualisieren. Eine schrittweise Anleitung finden Sie unter Benachrichtigen von Remote-Benutzern über ein Client-Update. Stellen Sie sicher, dass Sie die Versionsinformationen wie in Schritt 7 des Prozesses beschrieben als "(Rel)" eingeben.

F. Was kann eine Verzögerung verursachen, bevor der Cisco VPN Client angezeigt wird, insbesondere wenn die Option "Start Before Logon" (Vor Anmeldung starten) aktiviert ist?

Antwort: Der Cisco VPN Client befindet sich im *Ausfallmodus*. Dies trägt zur Verzögerung bei. Im Fallback-Modus führt der VPN-Client beim Start vor der Verwendung der Anmeldung eine andere Funktion aus. Beim Betrieb im Fallback-Modus überprüft der VPN-Client nicht, ob die erforderlichen Windows-Dienste gestartet wurden. Daher kann die VPN-Verbindung fehlschlagen, wenn sie zu schnell initiiert wird.Deinstallieren Sie den Cisco VPN Client, und entfernen Sie die fehlerhaften Anwendungen, um das Hochfahren zu ermöglichen, ohne sich im Ausfallmodus zu befinden. Installieren Sie anschließend den Cisco VPN Client neu. Weitere Informationen zum Fallback-Modus finden Sie unter Start before Logon (Vor Anmeldung starten).

Weitere Informationen finden Sie in den Cisco Bug IDs CSCdt88922 (nur registrierte Kunden) und CSCdt55739 (nur registrierte Kunden) im Bug Toolkit.

F. Ich muss den Unterschied zwischen ipsecdialer.exe und vpngui.exe verstehen. Warum ist vpngui.exe in STARTUP in meinem Windows XP installiert, aber ich muss noch manuell starten ipsecdialer, um meine Unternehmen Ressourcen zu erreichen? Abgesehen von der Größe scheinen diese Programme das gleiche auszulösen: eine VPN-Anmeldung bei meinem Unternehmensnetzwerk.

Antwort: ipsecdialer.exe war der ursprüngliche Startmechanismus für den Cisco VPN Client Version 3.x. Wenn die GUI in den Versionen 4.x geändert wurde, wurde eine neue ausführbare Datei mit dem Namen vpngui.exe erstellt. Die Datei ipsecdialer.exe wurde nur aus Gründen der Abwärtskompatibilität mit dem Namen fortgeführt und startet lediglich die Datei vpngui.exe. Dies ist der Grund, warum Sie den Unterschied in der Dateigröße sehen können.

Wenn Sie also ein Downgrade von Version 4.x auf Version 3.x des Cisco VPN Client durchführen, müssen Sie die Datei ipsecdialer.exe ausführen.

F. Kann ich das VPN-Startsymbol sicher entfernen? Wozu wird sie benötigt?

Antwort: Der Cisco VPN Client im Startordner unterstützt die Funktion "Start Before Logon" (Vor Anmeldung starten). Wenn Sie die Funktion nicht verwenden, benötigen Sie sie nicht im Startordner.

F. Warum wird "user_logon" hinzugefügt und nicht auf der Verknüpfung ipsecdialer.exe? Wozu dient "Benutzeranmeldung"?

Antwort: Für die Funktion "Start Before Logon" (Vor Anmeldung starten) ist "user_logon" erforderlich. Bei einem normalen Start des Cisco VPN Clients durch den Benutzer ist dies jedoch nicht erforderlich.

NAT-/PAT-Probleme

F. Ich habe Probleme damit, dass nur ein VPN-Client (für Versionen 3.3 und älter) über ein PAT-Gerät (Port Address Translation) eine Verbindung herstellen kann. Was kann ich tun, um dieses Problem zu beheben?

Antwort: Bei mehreren Network Address Translation (NAT)/PAT-Implementierungen ist ein Fehler aufgetreten, der dazu führt, dass Ports mit weniger als 1024 nicht übersetzt werden. Auf dem Cisco VPN Client 3.1 verwendet die ISAKMP-Sitzung (Internet Security Association and Key Management Protocol) UDP 512, selbst wenn die NAT-Transparenz aktiviert ist. Der erste VPN-Client durchläuft das PAT-Gerät und behält den Quellport 512 außen bei. Wenn der zweite VPN-Client eine Verbindung herstellt, wird Port 512 bereits verwendet. Der Versuch schlägt fehl.

Es gibt drei mögliche Problemumgehungen.

- PAT-Gerät reparieren.
- Aktualisieren Sie die VPN-Clients auf 3.4, und verwenden Sie TCP-Kapselung.
- Installieren Sie ein VPN 3002, das alle VPN-Clients ersetzt.

F. Können zwei Laptops am gleichen Standort mit dem Cisco VPN Client verbunden werden?

Antwort: Zwei Clients können vom gleichen Standort aus eine Verbindung mit demselben Headend herstellen, sofern sich die Clients nicht beide hinter einem Gerät befinden, das eine PAT ausführt, z. B. ein SOHO-Router oder eine SOHO-Firewall. Viele PAT-Geräte können einer VPN-Verbindung einen Client dahinter zuweisen, nicht jedoch zwei. Damit zwei VPN-Clients von demselben Standort hinter einem PAT-Gerät eine Verbindung herstellen können, aktivieren Sie eine Kapselung wie NAT-T, IPSec über UDP oder IPsec über TCP am Headend. Im Allgemeinen sollte NAT-T oder eine andere Kapselung aktiviert werden, wenn sich EIN NAT-Gerät zwischen dem Client und dem Headend befindet.

Verschiedenes

F. Wenn ich mit meinem Laptop eine Verbindung zum Netzwerk im Büro herstellen und dann den Laptop zu Hause mitnehmen möchte, kann ich von zu Hause aus keine Verbindung mit dem VPN 3000 Concentrator herstellen. Was ist das Problem?

Antwort: Der Laptop behält möglicherweise die Routing-Informationen aus der LAN-Verbindung bei. Informationen zur Behebung dieses Problems finden Sie unter VPN-Clients mit Microsoft Routing-Problemen.

F. Wie kann ich feststellen, ob ein VPN-Client mit dem VPN-Konzentrator verbunden ist?

Antwort: Überprüfen Sie den Registrierungsschlüssel HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. Wenn ein Tunnel aktiv ist, ist der Wert 1. Wenn kein Tunnel vorhanden ist, ist der Wert 0.

F. Ich habe Probleme mit der NetMeeting-Verbindung von einem PC hinter einem VPN-Konzentrator zu einem VPN-Client, aber die Verbindung funktioniert, wenn ich vom PC zu einem VPN-Client hinter einem VPN-Konzentrator führe. Wie kann ich dieses Problem beheben?

Antwort: Befolgen Sie die hier aufgeführten Schritte, um die Verbindungseinstellungen zu steuern:

- Wählen Sie auf dem Hauptlaufwerk des PCs **Programme > Cisco Systems > VPN Client > Profile aus**. Klicken Sie mit der rechten Maustaste auf das Profil, das Sie verwenden, und wählen Sie **Öffnen mit aus**, um das Profil in einem Texteditor (z. B. Notepad) zu öffnen. (Wenn Sie das zu verwendende Programm auswählen, deaktivieren Sie das Kontrollkästchen **Verwenden Sie dieses Programm immer, um diese Dateien zu öffnen**.) Suchen Sie den Profilparameter für ForcekeepAlives, ändern Sie den Wert von 0 auf **1**, und speichern Sie dann das Profil.oder
- Wählen Sie für den VPN-Client **Optionen > Eigenschaften > Allgemein**, und geben Sie einen Wert für das Peer-Response-Timeout ein, wie in diesem Beispielfenster gezeigt. Sie können eine Timeout-Empfindlichkeit von 30 bis 480 Sekunden angeben.oder
- Wählen Sie für den VPN-Konzentrator **Konfiguration > Benutzerverwaltung > Gruppen > *Gruppe ändern aus***. Wählen Sie auf der Registerkarte IPsec die Option für IKE-Keepalives aus, wie in diesem Beispielfenster gezeigt.

Das DPD-Intervall (Dead Peer Detection) hängt von der Empfindlichkeitseinstellung ab. Wenn eine Antwort nicht empfangen wird, wechselt sie in einen aggressiveren Modus und sendet alle fünf Sekunden Pakete, bis der Peer-Response-Schwellenwert erreicht ist. Zu diesem Zeitpunkt wird die Verbindung abgebrochen. Sie können die Keepalives deaktivieren, aber wenn die Verbindung tatsächlich getrennt wird, müssen Sie auf die Zeitüberschreitung warten. Cisco empfiehlt, den Empfindlichkeitswert zunächst sehr niedrig einzustellen.

F. Unterstützt der Cisco VPN Client die doppelte Authentifizierung?

Antwort: Nein. Doppelte Authentifizierung wird vom Cisco VPN-Client nicht unterstützt.

F. Wie konfiguriere ich den Cisco VPN Client für die Verbindung im Hauptmodus anstelle des aggressiven Modus?

Antwort: Sie müssen digitale Signaturen (Zertifikate) verwenden, damit der Cisco VPN Client im Hauptmodus eine Verbindung herstellen kann. Dafür gibt es zwei Methoden:

1. Sie erhalten Zertifizierungsstellenzertifikate des Drittanbieters (z. B. Verisign oder Entrust) auf dem Router und allen Cisco VPN-Clients. Registrieren Sie die Identitätszertifikate desselben CA-Servers, und verwenden Sie digitale Signaturen, um sich zwischen dem Cisco VPN-Client und dem Router zu authentifizieren. Weitere Informationen zu dieser Konfiguration finden Sie unter Konfigurieren von IPSec zwischen Cisco IOS-Routern und Cisco VPN-Client mithilfe von Vertrauenzertifikaten.
2. Die zweite Option besteht in der Konfiguration des Routers als CA-Server zusammen mit dem Headend für das Remote-Access-VPN. Die Installation der Zertifikate (und alles andere) bleibt wie in der vorherigen Verbindung beschrieben, mit der Ausnahme, dass sich der Router als CA-Server verhält. Weitere Informationen finden Sie unter Dynamic LAN-to-LAN VPN zwischen Cisco IOS-Routern mit IOS-CA im Konfigurationsbeispiel für den Hub.

F. Wie stelle ich sicher, dass die erforderlichen Parameter in der VPN-Client-Zugriffsdatei schreibgeschützt sind?

Antwort: Fügen Sie an der Vorderseite jedes Parameters in der .pcf-Datei für jeden Benutzer ein Ausrufezeichen (!) hinzu, damit der Parameter schreibgeschützt ist.

Die Werte für Parameter, die mit einem Ausrufezeichen (!) beginnen, können vom Benutzer im VPN-Client nicht geändert werden. Die Felder für diese Werte in der GUI werden grau ausgegraut (schreibgeschützt).

Nachfolgend finden Sie eine Beispielkonfiguration:

Originaldatei .pcf

```
[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1

GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C85
              1ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice
```

PDF-Datei geändert

```
[main]

!Description=connection to TechPubs server

!Host=10.10.99.30

AuthType=1

!GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C
          851ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0
```

```
ISPConnectType=0

ISPConnect=

ISPCommand=

!Username=alice
```

In diesem Beispiel kann der Benutzer die Werte *Description*, *Host*, *GroupName* und *Username* nicht ändern.

F. Ist es möglich, den Zugriff für VPN-Clients basierend auf MAC-Adressen zu beschränken bzw. einzuschränken?

Antwort: Nein. Es ist nicht möglich, den Zugriff für VPN-Clients basierend auf MAC-Adressen zu beschränken bzw. einzuschränken.

Zugehörige Informationen

- Cisco VPN 3000 Client Support-Seite
- Support-Seite für Cisco VPN-Clients
- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- Technischer Support und Dokumentation - Cisco Systems