

Cisco VPN 500 Concentrator und Client - Häufig gestellte Fragen

Inhalt

[Einführung](#)

[Warum erhalte ich den "FEHLER: InitSTEP wurde zurückgegeben. Fehler "STEP VxD" kann im VPN 5000-Client für Windows XP nicht gefunden werden, und wie kann ich dies beheben?](#)

[Unterstützt der VPN 500 Concentrator den in Macintosh OS 10.3 \(auch Panther genannt\) enthaltenen nativen VPN-Client?](#)

[Ich erhalte einen Kernel-Erweiterungsfehler, wenn ich versuche, den Cisco VPN 5000 5.2.2 Client auf Macintosh OS X 10.3 auszuführen. Was soll ich tun?](#)

[Wenn ich die Funktion "Auto-Connect to Default Before Logon" \(Automatische Verbindung zur Standardanmeldung\) mit einer DFÜ-Verbindung verwende, warum ist die Option für das Telefonbuch des Benutzers deaktiviert?](#)

[Was bedeutet "Fehler-ID = -1"?](#)

[Was bedeuten Fehler 0, Fehler 4, Fehler 6, Fehler 7 und Fehler 14?](#)

[Welche Probleme hat der Linksys® Router mit IPSec-Clients?](#)

[Welche Zeichen sind zulässig, wenn Sie einen Benutzernamen für den VPN 5000-Client angeben?](#)

[Wie viele interne Benutzer können im VPN 500 Concentrator definiert werden?](#)

[Wie viele Tunnel können auf dem VPN 5001, dem VPN 5002 und den VPN 5008 Concentrators konfiguriert werden?](#)

[Welche Befehle werden mit **modinfo** und **dmesg** angezeigt?](#)

[Wie kann ich den Linux® Client vollständig entfernen?](#)

[Kann die VPN 5000 Client-Software zusammen mit dem Nortel® Extranet Access Client oder einem anderen Client im selben Gerät vorhanden sein? Wird dies unterstützt?](#)

[Gibt es eine verfügbare DES-Version von Macintosh OS X?](#)

[Was sind die Anzeichen dafür, dass der VPN 5002 Concentrator heiß läuft?](#)

[Können H.323-Sitzungen mit dem VPN 5001 Concentrator und der VPN 5000 Client-Software Version 5.1.7 unterstützt werden?](#)

[In einer LAN-to-LAN-Situation mit einem VPN 500-Konzentrator und einem Cisco IOS®-Router stelle ich fest, dass die erneute Eingabe nach einer Stunde zwischen den beiden Geräten nicht synchronisiert wird. Wie kann ich dieses Problem beheben?](#)

[Was tut der "<local7.warn>macvpn ftCP ERR? Unknown next proto, 69 from 172.21.139.5" Fehlermeldung bedeuten?](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument behandelt häufig gestellte Fragen zum Cisco VPN Concentrator der Serie 5000 und zum Cisco VPN 5000 Client.

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

F. Warum erhalte ich den "FEHLER: InitSTEP wurde zurückgegeben. Fehler "STEP VxD" kann im VPN 5000-Client für Windows XP nicht gefunden werden, und wie kann ich dies beheben?

Antwort: Dieser Fehler tritt auf, wenn der VPN-Client nicht gebunden werden kann oder die erforderlichen VPN-Services nicht verfügbar sind. Der VPN 5000-Client für Windows XP enthält ein Installationsprogramm, das automatisch ein Programm zur Installation des Netzwerktreibers startet. Wenn das Programm aus irgendeinem Grund fehlschlägt, installieren Sie den Netzwerktreiber mit diesem Verfahren manuell.

1. Installieren Sie die VPN-Client-Software im Abschnitt [Installation des VPN-Clients für Windows XP](#).
2. Melden Sie sich als Administrator oder als Benutzer mit Administratorrechten beim System an.
3. Wählen Sie **Start > Einstellungen > Netzwerk- und Internetverbindungen > Netzwerkverbindungen aus**.
4. Doppelklicken Sie auf die entsprechende LAN-Verbindung.
5. Klicken Sie auf **Eigenschaften**.
6. Klicken Sie auf **Installieren**.
7. Wählen Sie **Service aus**.
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf **Datenträger haben**.
10. Geben Sie den Pfad zu dem Ordner ein, in dem sich die Dateien netcs.inf, netcs_m.inf und step.sys befinden. In den meisten Fällen handelt es sich um denselben Ordner wie die Installationsdatei des VPN-Clients.
11. Klicken Sie auf **OK**, um den Treiber zu installieren.
12. Schließen Sie nach der Installation des Treibers das Fenster Netzwerk- und DFÜ-Verbindungen.
13. Starten Sie den Computer neu.

F. Unterstützt der VPN 500 Concentrator den in Macintosh OS 10.3 (auch Panther genannt) enthaltenen nativen VPN-Client?

Antwort: Der VPN 500 Concentrator wurde nicht mit anderen als dem Macintosh-Betriebssystem (OS) 10.1.5 getestet. Für die Panther-Version kann kein Support angefordert werden. Es wurde noch nie im Kontext des VPN 500 Concentrator, sondern nur für den Cisco VPN Client, betrachtet. Falls eine spätere Betriebssystemunterstützung erforderlich ist, sollte eine Umstellung auf den Cisco VPN-Client in Betracht gezogen werden. Darüber hinaus ist der Native VPN Client in 10.3 IPsec over Layer 2 Tunneling Protocol (L2TP), das im VPN 500 Concentrator nicht unterstützt wird.

F. Ich erhalte einen Kernel-Erweiterungsfehler, wenn ich versuche, den Cisco VPN 5000 5.2.2 Client auf Macintosh OS X 10.3 auszuführen. Was soll ich tun?

Antwort: Wie in den [Versionshinweisen für den Cisco VPN 500 Client Version 5.2.3 für Macintosh Operating System \(OS\) X](#) angegeben, wird der Cisco VPN 5000 Client bis Version 10.1.x

unterstützt. Es wird von Version 10.3 nicht unterstützt. Es ist jedoch möglich, den VPN-Client funktionsfähig zu machen. Setzen Sie die Berechtigungen für zwei der installierten Dateien zurück, nachdem Sie das Installationsskript ausgeführt haben. Diese Ausgabe ist ein Beispiel.

Hinweis: Diese Konfiguration wird von Cisco nicht unterstützt.

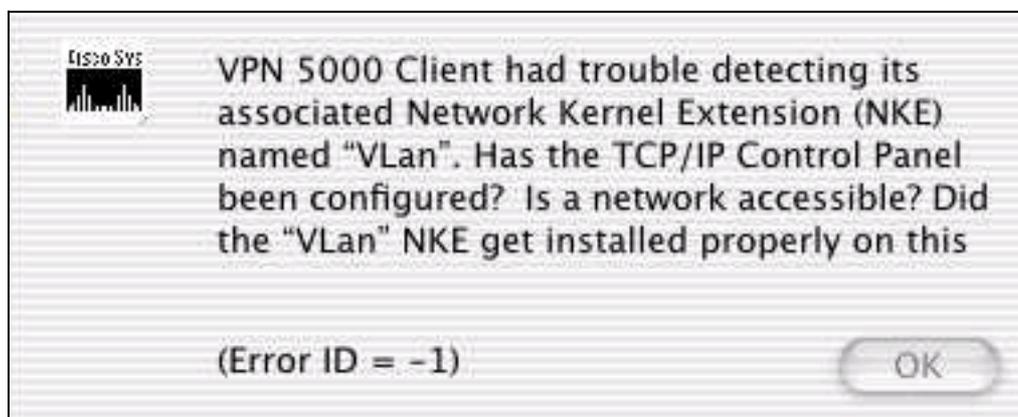
```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

F. Wenn ich die Funktion "Auto-Connect to Default Before Logon" (Automatische Verbindung zur Standardanmeldung) mit einer DFÜ-Verbindung verwende, warum ist die Option für das Telefonbuch des Benutzers deaktiviert?

Antwort: Der Grund hierfür ist in der Regel eine teilweise, falsche oder fehlende Installation des RAS (Registration, Admission and Status Protocol) im System. Versuchen Sie, Windows RAS zu deinstallieren und neu zu installieren, anstatt eine Neuinstallation auf dem VPN-Client durchzuführen.

F. Was bedeutet "Fehler-ID = -1"?

Antwort: Dies ist eine Fehlermeldung des Macintosh-Betriebssystems (OS), die auftritt, wenn die VPN 5000 Client-Version 10.0 auf dem Macintosh OS 10.1 installiert ist, der noch nicht unterstützt wird. Der Fehler weist auf eine Kernel-Diskrepanz hin. Im [Bug Toolkit](#) (nur [registrierte](#) Kunden) finden Sie weitere Informationen zur Cisco Bug-ID CSCdv57716. Dies ist ein Beispiel für den Fehler:



F. Was bedeuten Fehler 0, Fehler 4, Fehler 6, Fehler 7 und Fehler 14?

Antwort: In dieser Liste werden ihre Bedeutungen erläutert:

- **Fehler 0** - Dieser Fehler tritt auf, wenn kein IKE-Richtlinienabschnitt (Internet Key Exchange) für den VPN 500-Konzentrator konfiguriert wurde oder wenn für diese VPN-Gruppenkonfiguration keine IKE-Konfiguration konfiguriert wurde.
- **Fehler 4:** Für den VPN 500-Konzentrator sind keine VPN-Ressourcen verfügbar. Das bedeutet, dass der VPN 500-Konzentrator die maximale Anzahl an Verbindungen für diese Gruppe erreicht hat. Dies kann auch bedeuten, dass die Konfiguration ein LocalIPNet mit einer ungeeigneten Syntax wie "LocalIPNet=204.144.171.64" enthält (es sollte eine /26-Maske oder eine andere Maske definiert sein).
- **Fehler 6:** Wenn der VPN 500-Konzentrator für den Benutzernamen "Bob" konfiguriert wurde

und der Benutzer "bob" (mit dem richtigen Kennwort) eingibt, gibt der VPN 5000-Konzentrator den VPN-Serverfehler 6 zurück. Wenn der Benutzer "Bob" und das falsche Kennwort eingibt, gibt der VPN 500 Concentrator ebenfalls den Fehler 6 zurück. Wenn der VPN 500 Concentrator DES-Code ausführt und versucht, eine 3DES-Transform wie ESP (MD5, 3DES) zu verwenden, wird Fehler 6 an den VPN 5000-Client zurückgegeben. Der Non-Export-Code (3DES) hat einen "US" (z. B. Version 5.0US) und kann 3DES-Verschlüsselungsmethoden verwenden. Alle Cisco VPN 500 Concentrators werden mit DES-Code ausgeliefert. Löschen Sie die 3DES-Transform, und verwenden Sie eine andere Transform, wenn Sie nur DES-Code verwenden.

- **Fehler 7** - Dieser Fehler bedeutet, dass der VPN 500-Konzentrator mit einer IKE-Richtlinie konfiguriert ist, die für die Codeversion derzeit inaktiv ist. Derzeit sind für den Code der Version 5.x alle 3DES- und G2-Richtlinien inaktiv. Entfernen Sie diese, und legen Sie für die IKE-Richtlinie entweder MD5_DES_G1 oder SHA_DES_G1 fest.
- **Fehler 14** - Dies ist ein RADIUS-Fehler, bei dem der VPN 500 Concentrator nicht die richtigen Informationen vom RADIUS-Server erhält, um die Anmeldung des VPN 500-Clients zu ermöglichen.
- **Betroffene Produkte:**Windows 95-98 VPN-Client für die Cisco VPN 500 Concentrator-Serie
Windows NT 4.0 VPN-Client für die Cisco VPN 500 Concentrator-Serie
Macintosh Operating System (OS) VPN-Client für die Cisco VPN 500 Concentrator-Serie
Linux-Kernel 2.2.5 VPN-Client für die Cisco VPN 500 Concentrator-Serie
SPARC Solaris VPN Client für die Cisco VPN 500 Concentrator-Serie
Cisco VPN 5001 Concentrator
Cisco VPN 5002 Concentrator
Cisco VPN 5008 Concentrator
- **Betroffene Versionen:**Alle 5.x-Versionen

F. Welche Probleme hat der Linksys® Router mit IPSec-Clients?

Antwort: Linksys®-Router unterstützen IPSec-Verbindungen nur mit Firmware-Versionen 1.34 oder höher (neueste Version 1.39). Der IPSec-Passthrough sollte auf dem Linksys®-Router aktiviert sein.

F. Welche Zeichen sind zulässig, wenn Sie einen Benutzernamen für den VPN 5000-Client angeben?

Antwort: Beim Benutzernamen und der Domäne wird die Groß- und Kleinschreibung beachtet. Sie können 1 bis 60 alphanumerische Zeichen kombinieren. Dazu gehört das Zeichen "at" (@). Weitere Informationen finden Sie unter [VPN-Benutzer](#).

Dieser Benutzername ist illegal (das "-" Zeichen ist ungültig):

```
[ VPN Users ]  
user-2 Config="test" SharedKey="cisco"
```

F. Wie viele interne Benutzer können im VPN 500 Concentrator definiert werden?

Antwort: Es wird immer empfohlen, für große Implementierungen RADIUS- oder SDI-Authentifizierung (Secure ID) zu verwenden. Die Anzahl der internen Benutzer hängt von der Größe Ihrer Konfiguration ab. Die maximale Konfigurationsgröße beträgt 65.500 Byte. Um dies anzuzeigen, überprüfen Sie die letzte Zeile der Befehlsausgabe **show configuration**. Beispiel:

Configuration size is 6732 out of 65500 bytes.

F. Wie viele Tunnel können auf dem VPN 5001, dem VPN 5002 und den VPN 5008 Concentrators konfiguriert werden?

Antwort: Der VPN 5001 Concentrator kann bis zu 1.500 Tunnel unterstützen, der VPN 5002 Concentrator kann bis zu 10.000 Tunnel unterstützen und der VPN 5008 Concentrator kann bis zu 40.000 Tunnel pro Linecard unterstützen.

F. Welche Befehle werden mit modinfo und dmesg angezeigt?

Antwort: Der Befehl `modinfo` zeigt an, welche und wie viele Module geladen werden. Der Befehl `dmesg` zeigt Systemstart-Syslog-Meldungen an.

F. Wie kann ich den Linux® Client vollständig entfernen?

Antwort: Bei der Installation werden diese Dateien erstellt oder auf Ihrem System abgelegt:

- `/etc/vpn_config`: Es wird empfohlen, diese Konfiguration beizubehalten, da es sich um die VPN 5000-Client-Konfiguration handelt.
- `/etc/rc.d/init.d/vpn`: Dies ist das Boot-Time-Skript, das das "vpnmod"-Kernelmodul lädt.
- `/etc/rc.d/rc3.d/s85.vpn`: Dies ist ein Link zu `/etc/rc.d/init.d/vpn`.
- `/etc/rc.d/rc5.d/s85.vpn`: Dies ist ein Link zu `/etc/rc.d/init.d/vpn`.
- `/usr/local/bin/open_tunnel`: Damit wird die Tunnelverbindung geöffnet.
- `/usr/local/bin/close_tunnel`: Dieser Vorgang schließt den Tunnel.
- `/usr/local/bin/vpn_control` - Dies ist ein Tool zur Fehlerbehebung, mit dem Debug-Flags aktiviert werden können. Es wird hauptsächlich in der Entwicklung verwendet.
- `/lib/modules/<kernelversion>/COMPvpn/vpnmod` - Dies ist das Kernelmodul. Führen Sie den Befehl `uname -r` aus, um den <Kernelversion> zu bestimmen.

Wenn Sie diese Dateien löschen und dann neu starten, deinstallieren Sie den Client effektiv. Alternativ können Sie `/usr/local/bin/close_tunnel` und `/etc/rc.d/init.d/vpnstop` ausführen und anschließend die oben genannten Dateien löschen.

Die Datei `/etc/vpn_config` ist die Clientkonfiguration. Sie enthält Informationen zu Server, Benutzername und Kennwort. Wenn Sie eine Neuinstallation des VPN-Clients planen, sollten Sie eine Kopie dieser Datei aufbewahren.

F. Kann die VPN 5000 Client-Software zusammen mit dem Nortel® Extranet Access Client oder einem anderen Client im selben Gerät vorhanden sein? Wird dies unterstützt?

Antwort: Cisco VPN Client Version 4.0 und höher kann gleichzeitig vorhanden sein. Weitere Informationen finden Sie im Abschnitt [Koexistenz mit VPN-Anbietern](#) in den [Versionshinweisen für VPN-Client, Version 4.0](#).

F. Gibt es eine verfügbare DES-Version von Macintosh OS X?

Antwort: Nein, aber es gibt eine 3DES-Version.

F. Was sind die Anzeichen dafür, dass der VPN 5002 Concentrator heiß läuft?

Antwort: Wenn die Over Temp-LED einer ESP-Karte (Extended Services Processor) im VPN 5002 Concentrator leuchtet oder andere Temperaturprobleme mit der Einheit auftreten, kann es sein, dass der integrierte Luftfilter mit Schmutz verstopft ist und den Luftstrom beeinträchtigt. Weitere Informationen zum Ersetzen des Luftfilters finden Sie unter [Ersetzen des Luftfilters](#).

F. Können H.323-Sitzungen mit dem VPN 5001 Concentrator und der VPN 5000 Client-Software Version 5.1.7 unterstützt werden?

Antwort: Nein, sie können nicht unterstützt werden, da die IP-Adresse in den Datenabschnitt des Pakets eingebettet ist. Der VPN 5000-Client kann nicht auf diese Adresse zugreifen oder diese ändern.

F. In einer LAN-to-LAN-Situation mit einem VPN 500-Konzentrator und einem Cisco IOS®-Router stelle ich fest, dass die erneute Eingabe nach einer Stunde zwischen den beiden Geräten nicht synchronisiert wird. Wie kann ich dieses Problem beheben?

Antwort: Dieses Problem kann in der Regel durch die Einstellung "keymanager=zuverlässiges" in der Konfiguration des VPN 5000 Concentrator gelöst werden. Sie funktioniert jedoch nicht, wenn das Cisco IOS-Gerät über eine dynamische IP-Adresse verfügt.

F. Was tut der "<local7.warn>macvpn fTCP ERR? Unknown next_proto, 69 from 172.21.139.5" Fehlermeldung bedeuten?

Antwort: Die gefälschte TCP (fTCP)-Nachricht wird angezeigt, wenn der VPN Concentrator ein Paket mit Port 80 empfängt und nach dem Entfernen der Header kein ESP-Paket gefunden hat. Der VPN Concentrator akzeptiert nur IPSec (ESP)-Pakete, und alle anderen Komponenten werden verworfen. Als der Code Red Wurm im Internet veröffentlicht wurde, füllte diese Warnung den Syslog-Puffer auf vielen Kundencomputern aus. Diese Fehlermeldung kann darauf hinweisen, dass Ihr Computer infiziert ist und versucht, über Port fTCP auf den VPN 5000-Konzentrator zuzugreifen.

Zugehörige Informationen

- [Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes](#)
- [Support-Seite für Cisco VPN Concentrators der Serie 5000](#)
- [Support-Seite für Cisco VPN 5000-Client](#)
- [Support-Seite für IPSec \(IP Security Protocol\)](#)
- [Technischer Support - Cisco Systems](#)