Split Tunneling für VPN-Clients im VPN 3000 Concentrator - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält schrittweise Anweisungen, wie VPN-Clients Zugriff auf das Internet gewähren, während sie in einen VPN-Konzentrator der Serie 300 getunnelt werden. Diese Konfiguration ermöglicht VPN-Clients den sicheren Zugriff auf Unternehmensressourcen über IPsec und bietet gleichzeitig einen ungesicherten Zugriff auf das Internet.

Hinweis: Split-Tunneling kann bei der Konfiguration ein Sicherheitsrisiko darstellen. Da VPN-Clients über ungesicherten Zugriff auf das Internet verfügen, können sie von einem Angreifer kompromittiert werden. Dieser Angreifer kann dann über den IPsec-Tunnel auf das Firmen-LAN zugreifen. Ein Kompromiss zwischen Full-Tunneling und Split-Tunneling kann darin bestehen, nur den lokalen LAN-Zugriff von VPN-Clients zuzulassen. Weitere Informationen finden Sie im Konfigurationsbeispiel für den VPN-Concentrator für VPN-Clients den lokalen LAN-Zugriff zulassen.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass auf dem VPN Concentrator bereits eine funktionierende VPN-Konfiguration für den Remote-Zugriff vorhanden ist. Weitere Informationen finden Sie im Konfigurationsbeispiel IPsec mit VPN Client to VPN 3000 Concentrator (IPsec mit VPN-Client für VPN 3000-Konzentrator), falls dieses noch nicht konfiguriert ist.

Verwendete Komponenten

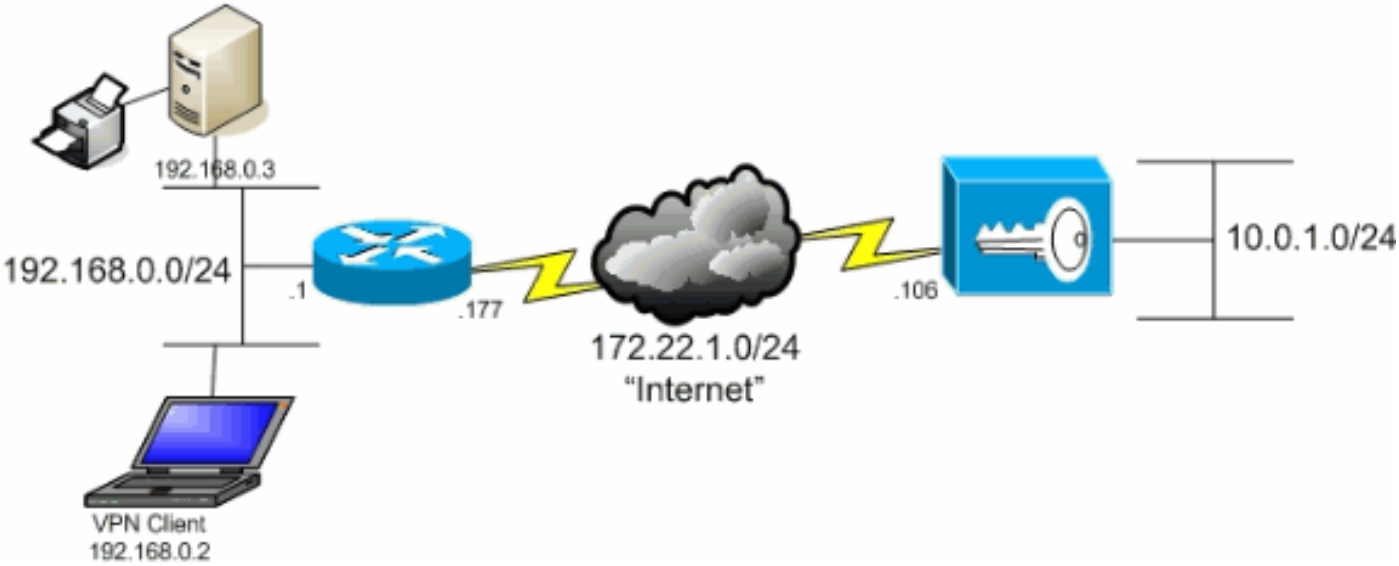
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco VPN Concentrator der Serie 300 - Softwareversion 4.7.2.H
- Cisco VPN Client Version 4.0.5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

Der VPN-Client befindet sich in einem typischen SOHO-Netzwerk und ist über das Internet mit der Hauptniederlassung verbunden.



Konventionen

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

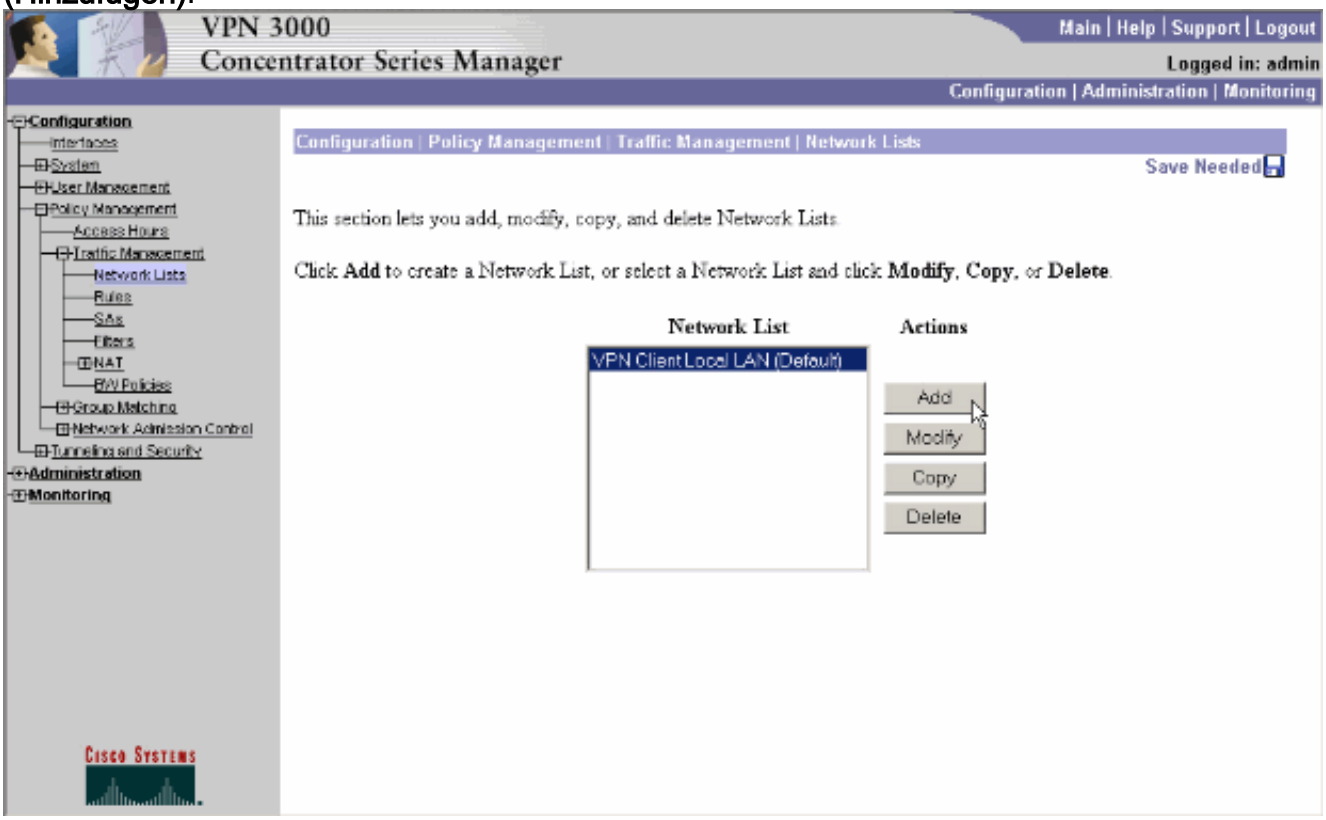
Hintergrundinformationen

In einem grundlegenden VPN-Client-zu-VPN-Concentrator-Szenario wird der gesamte Datenverkehr vom VPN-Client verschlüsselt und an den VPN-Concentrator gesendet, unabhängig vom Ziel. Basierend auf Ihrer Konfiguration und der Anzahl der unterstützten Benutzer kann eine solche Konfiguration eine hohe Bandbreite beanspruchen. Split-Tunneling kann zur Behebung dieses Problems beitragen, indem Benutzern ermöglicht wird, nur den für das Unternehmensnetzwerk bestimmten Datenverkehr über den Tunnel zu senden. Sämtlicher anderer Datenverkehr wie IM, E-Mail oder Surfen im Internet wird über das lokale LAN des VPN-Clients übertragen.

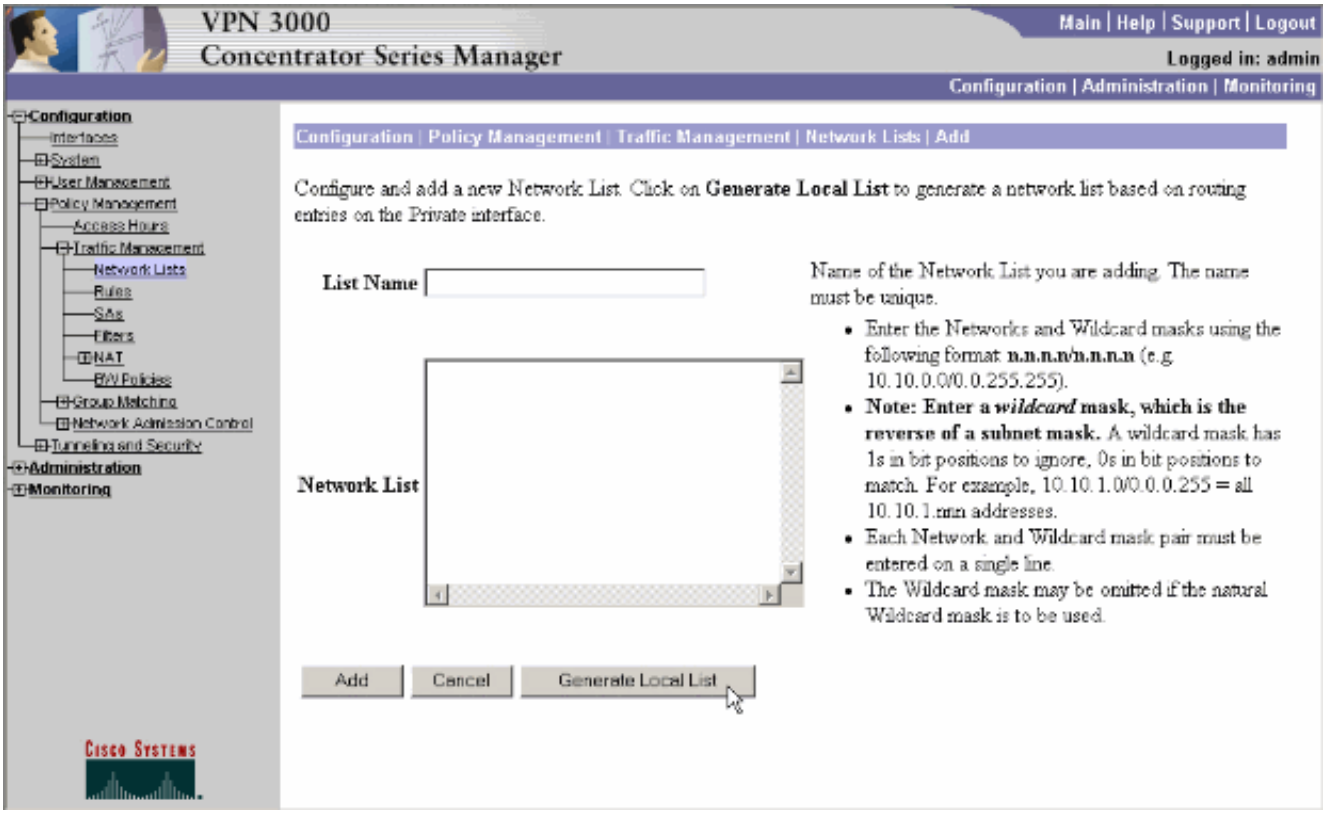
Konfigurieren von Split Tunneling auf dem VPN Concentrator

Führen Sie diese Schritte aus, um Ihre Tunnelgruppe so zu konfigurieren, dass Split-Tunneling für Benutzer in der Gruppe möglich ist. Erstellen Sie zunächst eine Netzwerkliste. Diese Liste definiert die Zielnetzwerke, an die der VPN-Client verschlüsselten Datenverkehr sendet. Nachdem die Liste erstellt wurde, fügen Sie sie der Split-Tunneling-Richtlinie der Client-Tunnelgruppe hinzu.

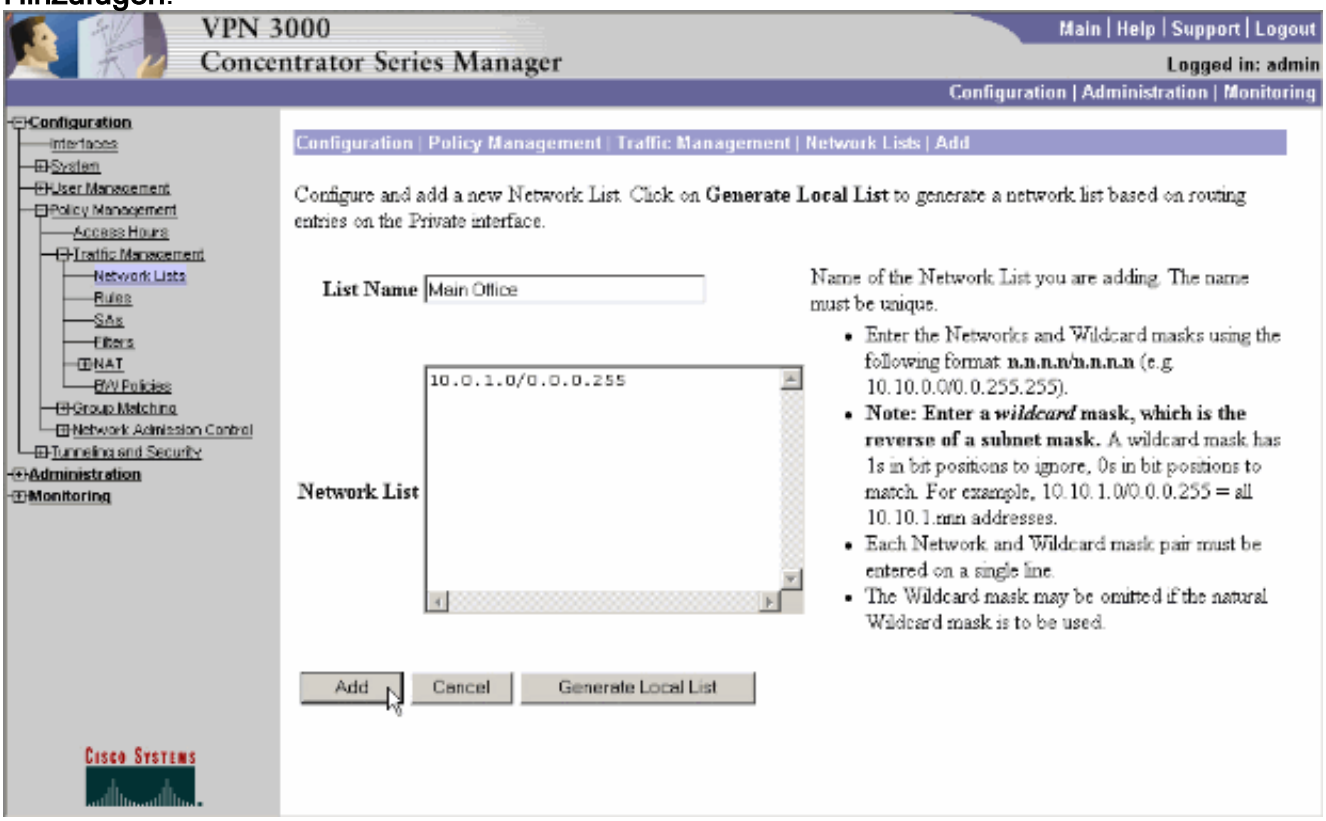
1. Wählen Sie **Configuration > Policy Management > Traffic Management > Network Lists (Konfiguration > Richtlinienverwaltung > Datenverkehrsmanagement > Netzwerklisten) aus,** und klicken Sie auf **Add (Hinzufügen)**.



2. Diese Liste definiert die Zielnetzwerke, an die der VPN-Client verschlüsselten Datenverkehr sendet. Geben Sie diese Netzwerke entweder manuell ein, oder klicken Sie auf **Lokale Liste generieren**, um eine Liste auf der Grundlage von Routing-Einträgen auf der privaten Schnittstelle des VPN Concentrator zu erstellen.In diesem Beispiel wurde die Liste automatisch
erstellt.

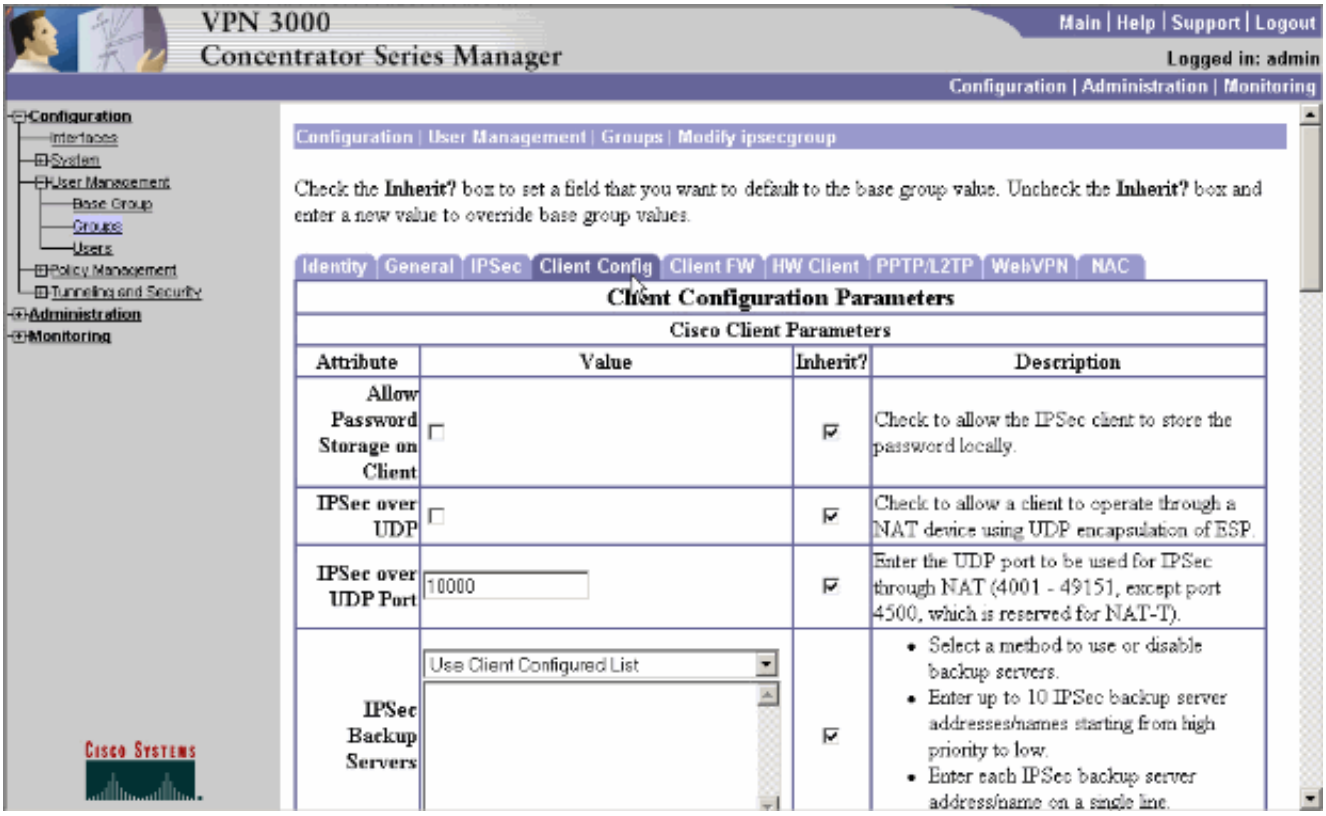


3. Geben Sie nach dem Erstellen oder Ausfüllen einen Namen für die Liste an, und klicken Sie auf **Hinzufügen**.

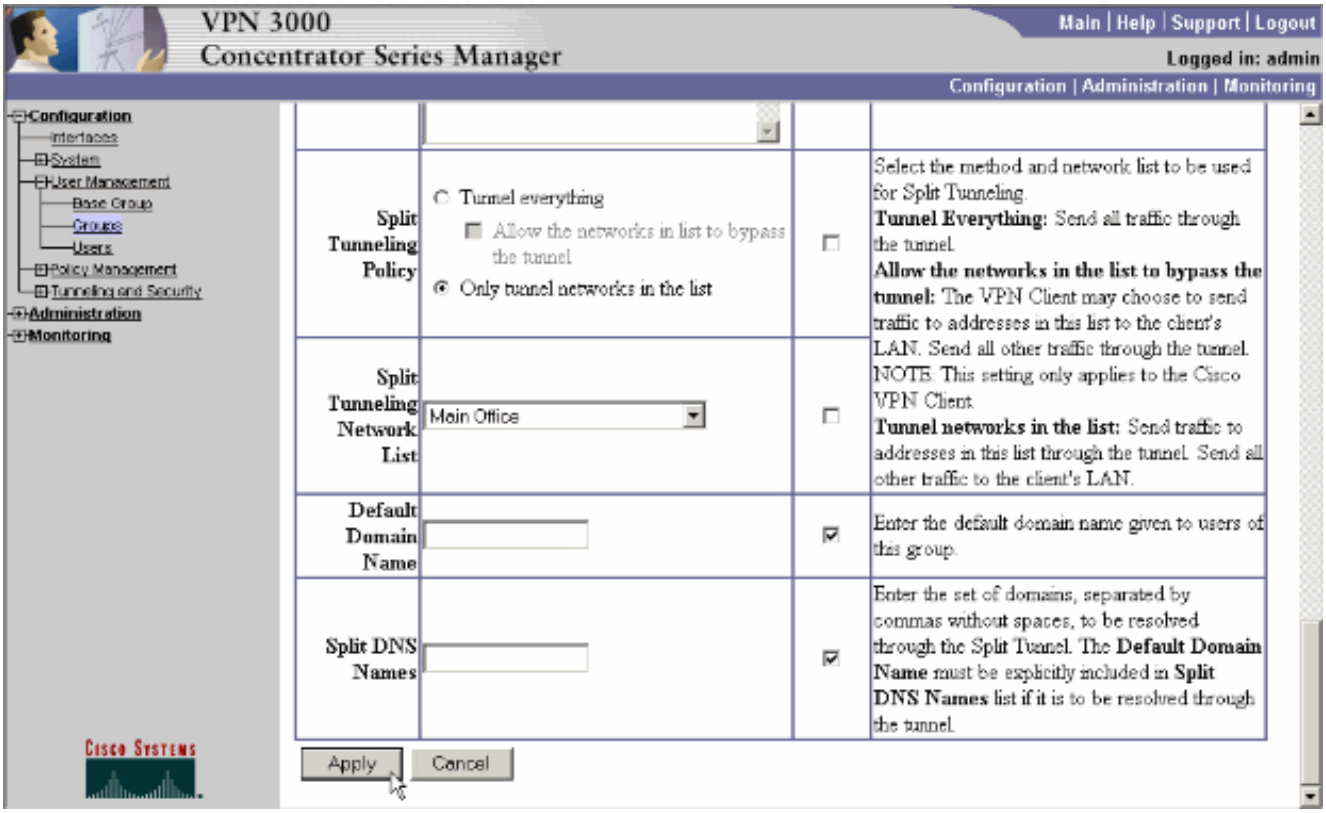


4. Nachdem Sie die Netzwerkliste erstellt haben, weisen Sie sie einer Tunnelgruppe zu. Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen aus**, wählen Sie die Gruppe aus, die geändert werden soll, und klicken Sie auf **Gruppe ändern**.

5. Öffnen Sie die Registerkarte Client Config (Client-Konfiguration) der Gruppe, die Sie ändern möchten.



6. Blättern Sie nach unten zu den Abschnitten "Split Tunneling Policy" und "Split Tunneling Network List", und klicken Sie **in der Liste** auf **Only Tunnel Networks**.
7. Wählen Sie die zuvor erstellte Liste aus dem Dropdown-Menü aus. In diesem Fall ist es die **Hauptniederlassung**. Die Erben? in beiden Fällen werden die Kontrollkästchen automatisch geleert.



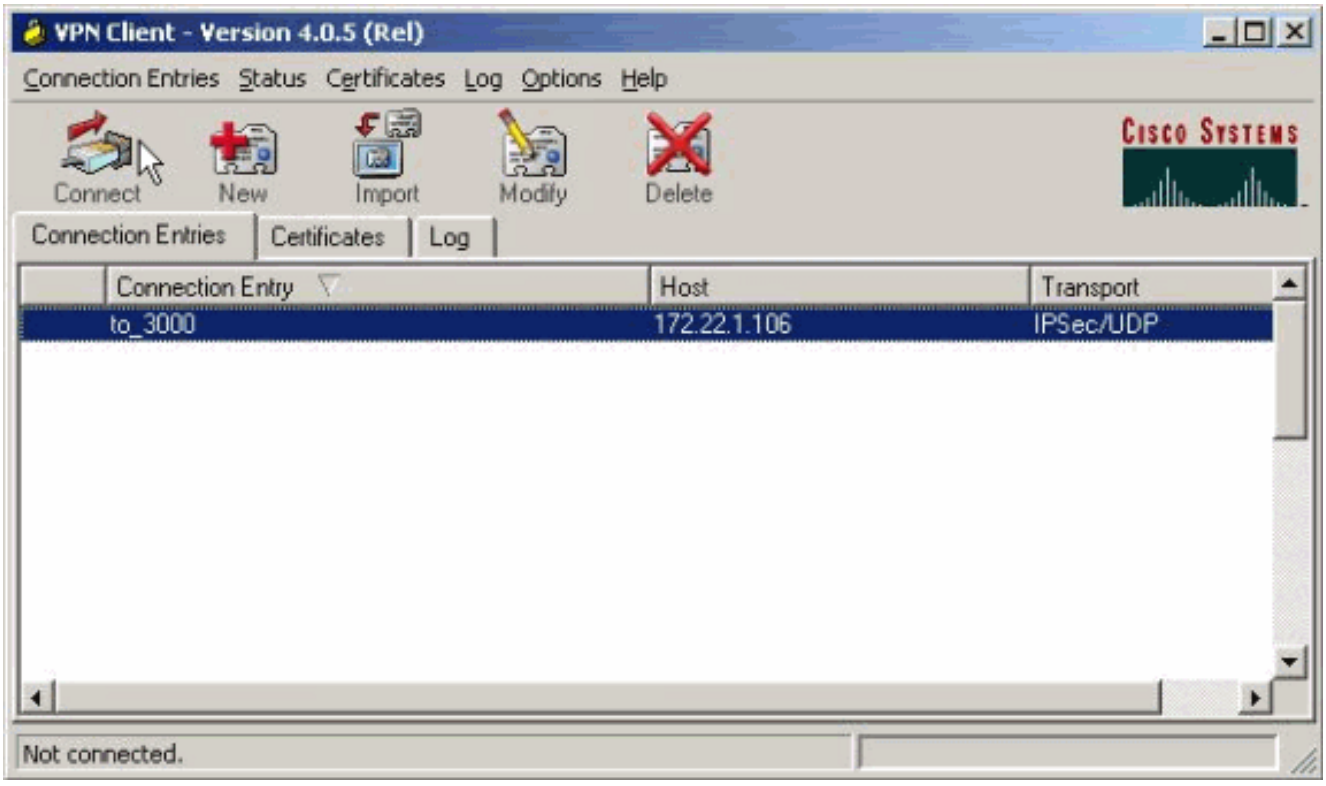
8. Klicken Sie abschließend auf **Übernehmen**.

Überprüfen

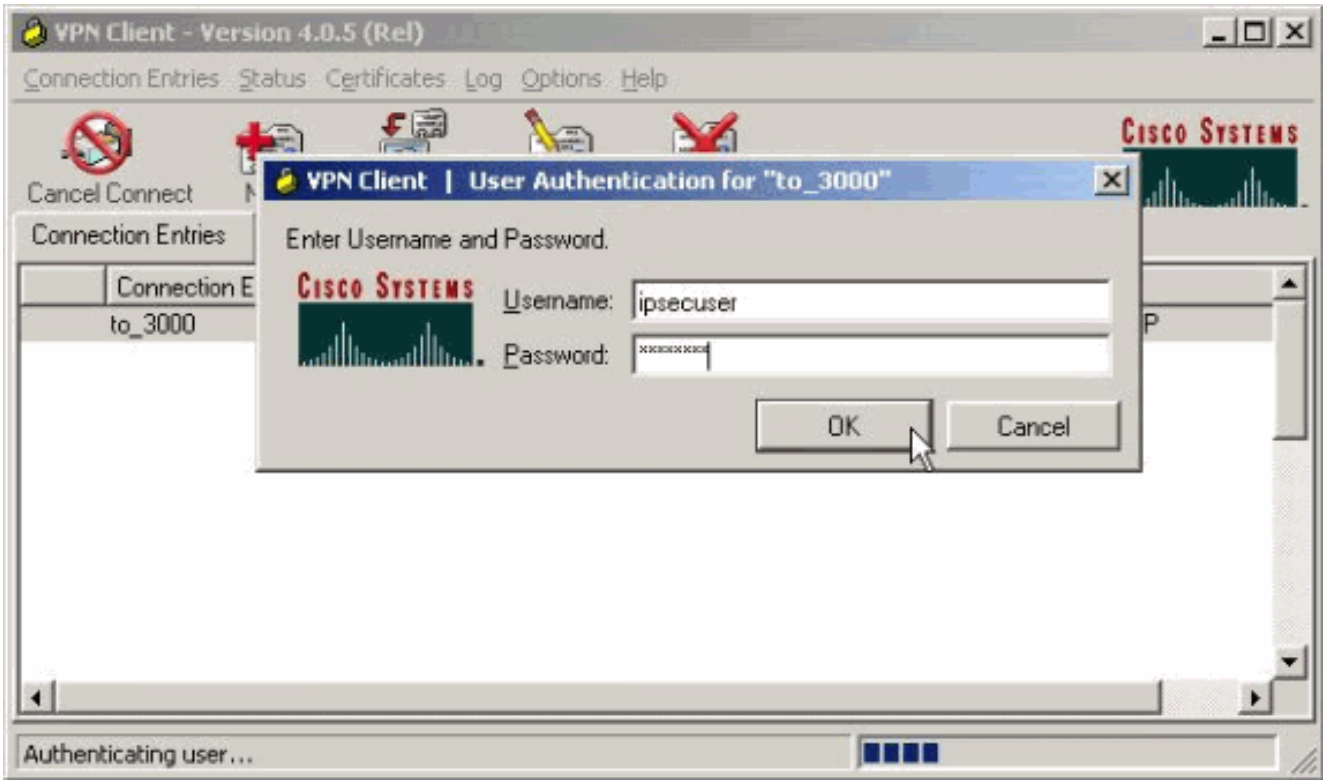
Herstellen einer Verbindung mit dem VPN-Client

Verbinden Sie den VPN-Client mit dem VPN-Konzentrator, um Ihre Konfiguration zu überprüfen.

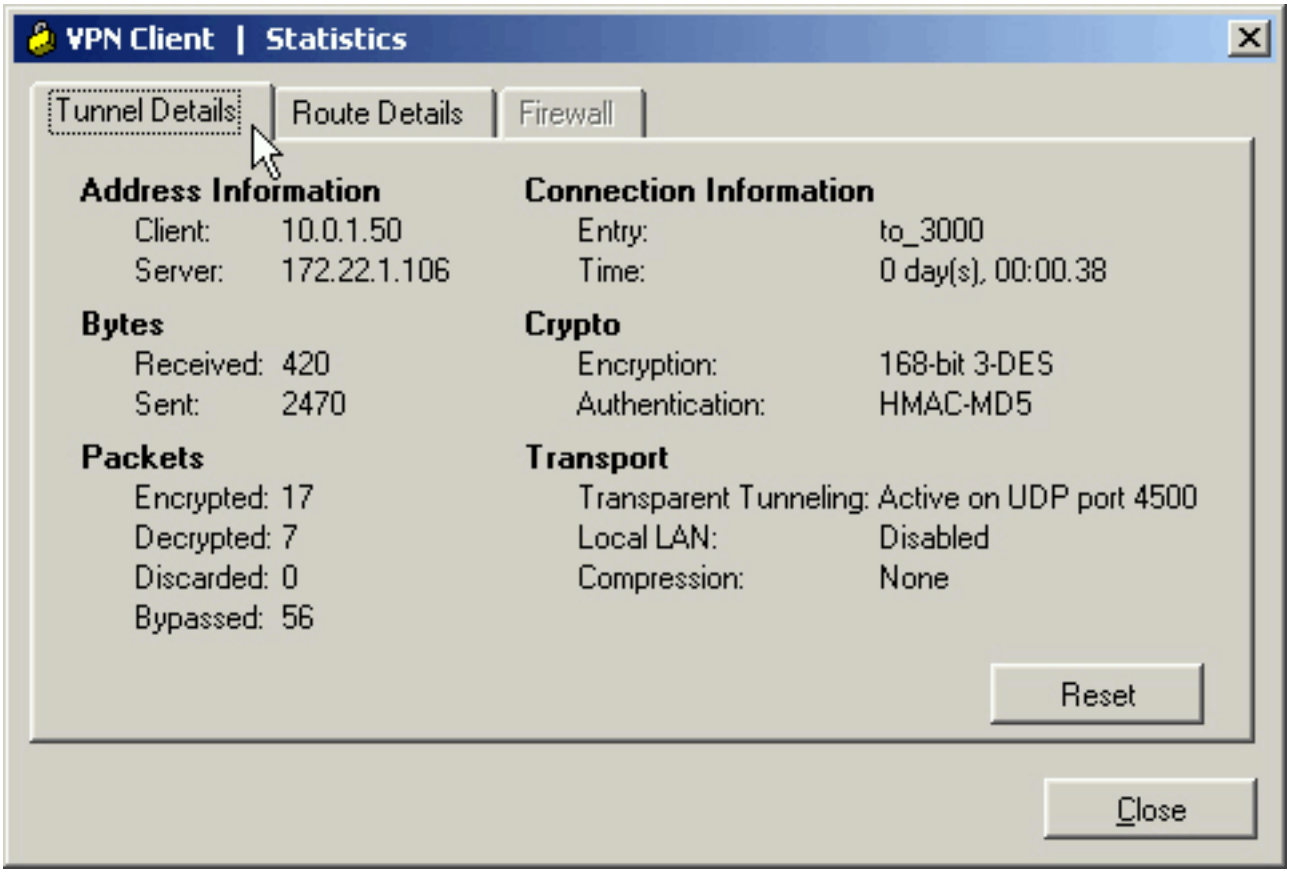
1. Wählen Sie den Eintrag für die Verbindung aus der Liste aus, und klicken Sie auf **Verbinden**.



2. Geben Sie Ihre Anmeldeinformationen ein.

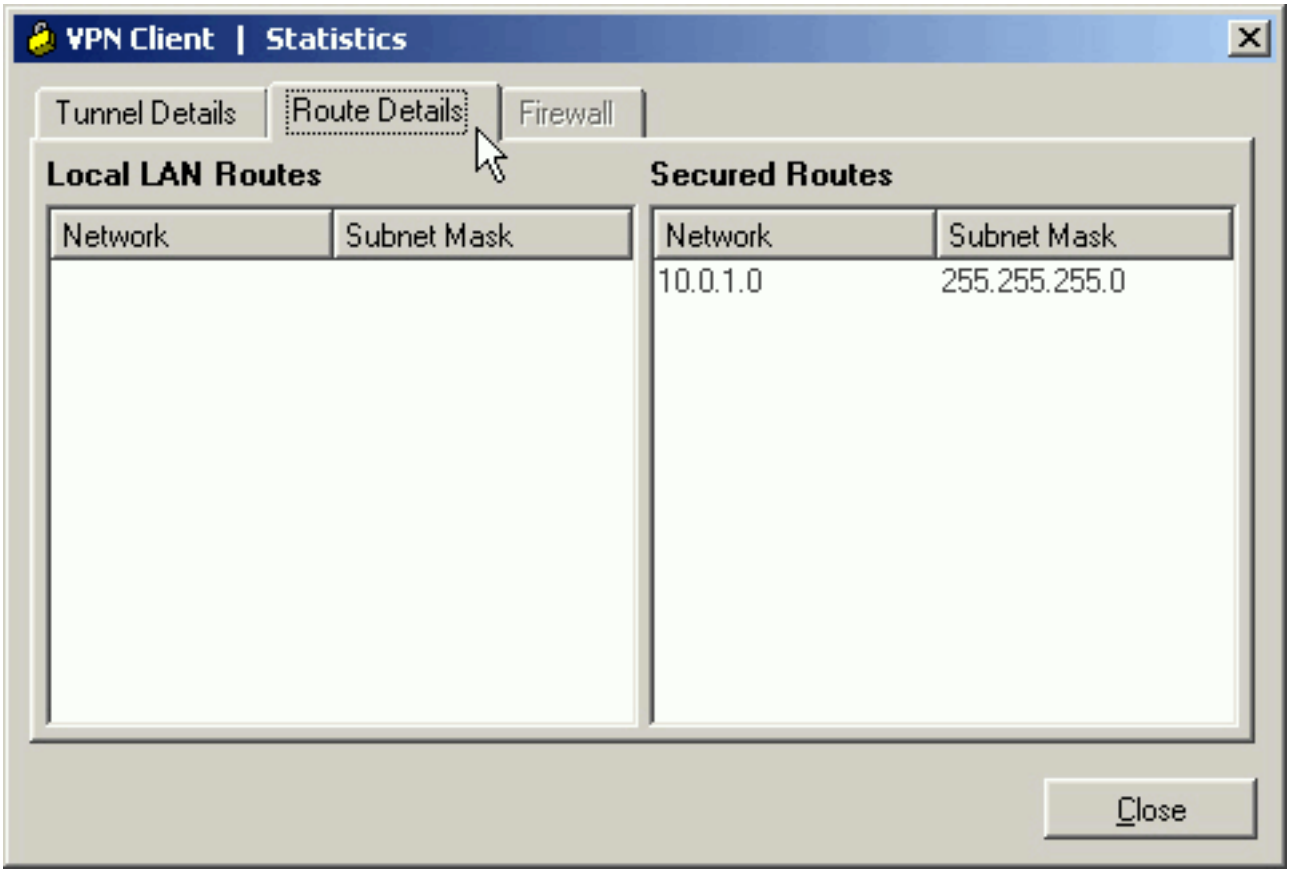


3. Wählen Sie **Status > Statistics.. (Status > Statistik) aus.** um das Fenster Tunneldetails anzuzeigen, in dem Sie die Einzelheiten des Tunnels überprüfen und den Verkehrsfluss sehen können.



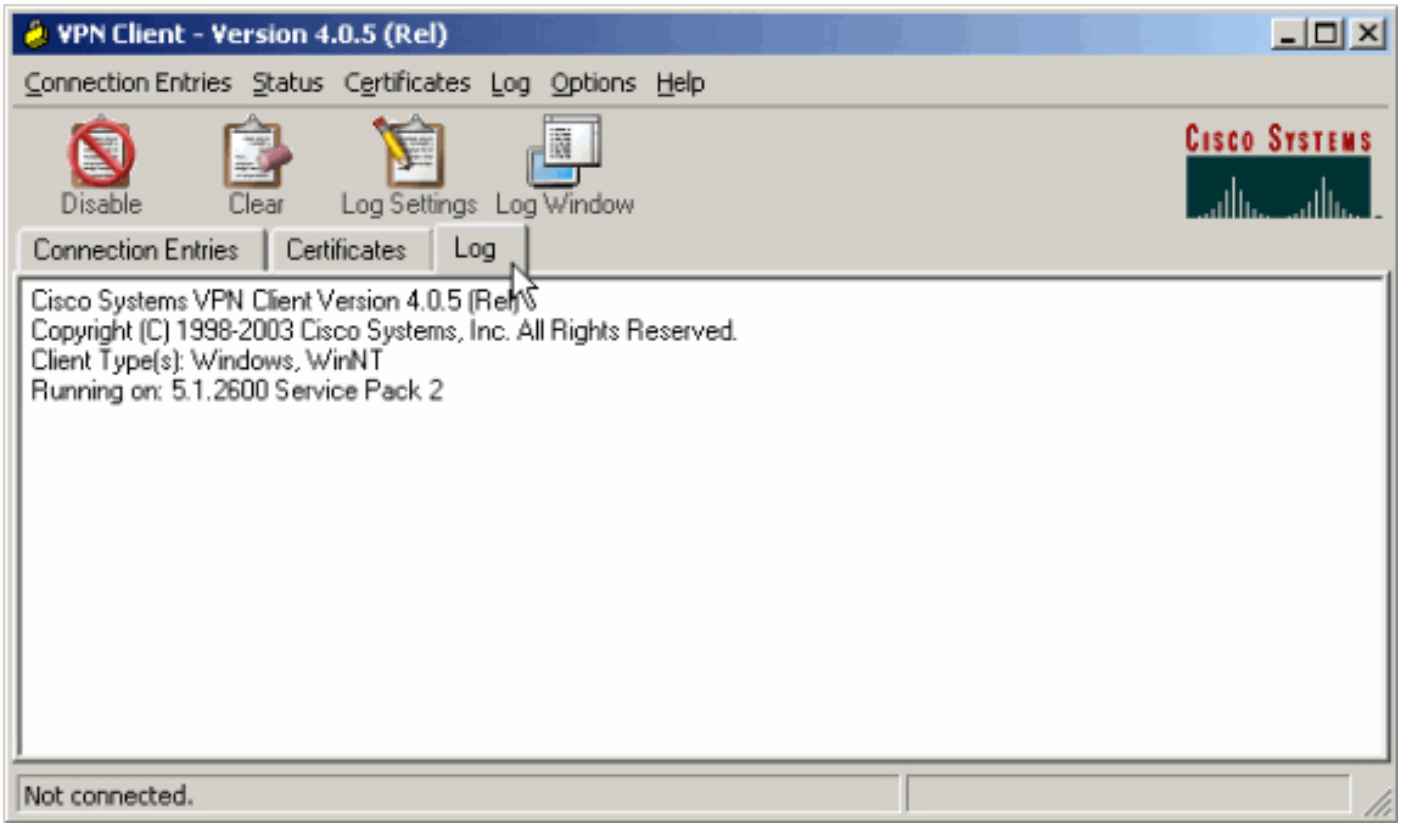
4. Wechseln Sie zur Registerkarte Routendetails, um zu sehen, an welche Netzwerke der VPN-Client verschlüsselten Datenverkehr sendet. In diesem Beispiel kommuniziert der VPN-Client sicher mit 10.0.1.0/24, während der gesamte andere Datenverkehr unverschlüsselt in das

Internet gesendet wird.



VPN-Clientprotokoll anzeigen

Wenn Sie das VPN-Clientprotokoll überprüfen, können Sie bestimmen, ob der Parameter für Split-Tunneling festgelegt ist. Öffnen Sie im VPN-Client die Registerkarte Log (Protokoll), um das Protokoll anzuzeigen. Klicken Sie auf **Protokolleinstellungen**, um die protokollierten Einstellungen anzupassen. In diesem Beispiel sind IKE und IPsec auf **3-High** festgelegt**,** während alle anderen Protokollelemente auf **1-Low** festgelegt sind.




```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      14:21:43.106  07/21/06  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.

!--- Output is supressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30
14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114
07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value
= 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0
mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40
14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29
2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed.
```

Fehlerbehebung

Weitere allgemeine Informationen zur Fehlerbehebung finden Sie unter Konfigurationsbeispiel für IPsec mit VPN-Client für VPN 3000 Concentrator - Fehlerbehebung.

Zugehörige Informationen

- Konfigurationsbeispiel: IPsec mit VPN-Client für VPN 3000-Concentrator
- Cisco VPN Concentrators der Serie 3000
- Cisco VPN-Client
- Technischer Support und Dokumentation - Cisco Systems