

IPsec zwischen einem VPN 300-Concentrator und einem VPN-Client 4.x für Windows mit RADIUS für die Konfiguration der Benutzerauthentifizierung und -abrechnung (Beispiel)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Benutzergruppen im VPN 300-Konzentrator](#)

[Verwendung von Gruppen- und Benutzerattributen im VPN 3000-Concentrator](#)

[Konfiguration des VPN Concentrators der Serie 3000](#)

[RADIUS-Serverkonfiguration](#)

[Zuweisen einer statischen IP-Adresse zum VPN-Client-Benutzer](#)

[VPN-Client-Konfiguration](#)

[Accounting hinzufügen](#)

[Überprüfen](#)

[Überprüfen des VPN-Konzentrators](#)

[Überprüfen des VPN-Clients](#)

[Fehlerbehebung](#)

[Fehlerbehebung beim VPN Client 4.8 für Windows](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie ein IPsec-Tunnel zwischen einem Cisco VPN 3000-Konzentrator und einem Cisco VPN Client 4.x für Microsoft Windows erstellt wird, der RADIUS für die Benutzerauthentifizierung und -abrechnung verwendet. In diesem Dokument wird der Cisco Secure Access Control Server (ACS) für Windows empfohlen, um die RADIUS-Konfiguration zu vereinfachen und Benutzer zu authentifizieren, die eine Verbindung zu einem VPN 3000-Konzentrator herstellen. Eine Gruppe auf einem VPN 300-Konzentrator ist eine Gruppe von Benutzern, die als eine Einheit behandelt werden. Die Konfiguration von Gruppen kann im Gegensatz zu einzelnen Benutzern die Systemverwaltung vereinfachen und Konfigurationsaufgaben optimieren.

Weitere Informationen finden Sie unter [PIX/ASA 7.x und Cisco VPN Client 4.x für Windows mit Microsoft Windows 2003 IAS RADIUS Authentication Configuration Example](#) zum Einrichten der Remotezugriff-VPN-Verbindung zwischen einem Cisco VPN Client (4.x für Windows) und der PIX 500 Security Appliance 7.x, die einen Microsoft Windows 2003 Internet Authentication Service (RADIUS) verwendet. US-Server.

Unter [Konfigurieren von IPsec zwischen einem Cisco IOS-Router und einem Cisco VPN-Client 4.x für Windows mithilfe von RADIUS für die Benutzerauthentifizierung](#) finden Sie Informationen zum Konfigurieren einer Verbindung zwischen einem Router und dem Cisco VPN Client 4.x, der RADIUS für die Benutzerauthentifizierung verwendet.

[Voraussetzungen](#)

[Anforderungen](#)

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Secure ACS für Windows RADIUS ist installiert und funktioniert ordnungsgemäß mit anderen Geräten.
- Der Cisco VPN 3000 Concentrator wird konfiguriert und kann über die HTML-Schnittstelle verwaltet werden.

[Verwendete Komponenten](#)

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

- Cisco Secure ACS für Windows mit Version 4.0
- Cisco VPN Concentrator der Serie 3000 mit Bilddatei 4.7.2.B
- Cisco VPN-Client 4.x

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.

[Konventionen](#)

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

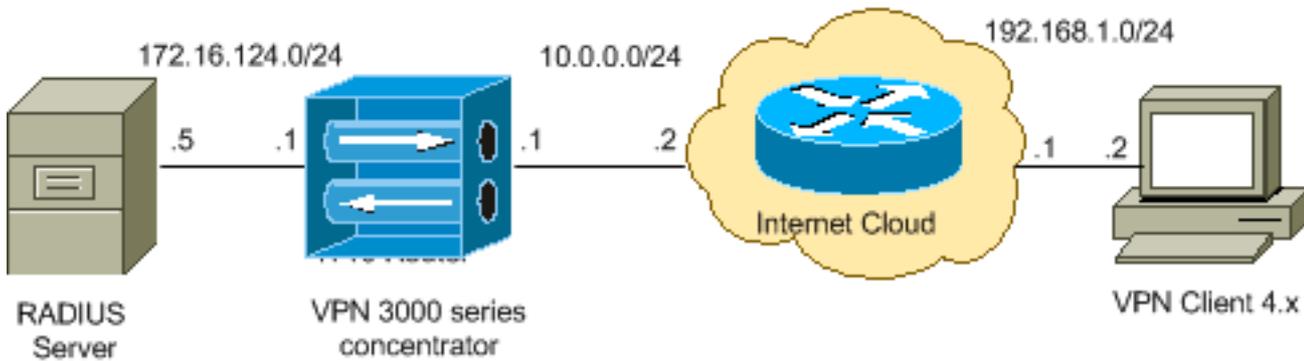
[Konfigurieren](#)

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdigramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind [RFC 1918](#) -Adressen, die in einer Laborumgebung verwendet werden.

Benutzergruppen im VPN 300-Konzentrator

Gruppen können sowohl für Cisco Secure ACS für Windows als auch für den VPN 3000-Konzentrator definiert werden, verwenden jedoch Gruppen auf etwas andere Weise. Führen Sie diese Aufgaben aus, um die Dinge zu vereinfachen:

- **Konfigurieren Sie eine Gruppe im VPN 300-Konzentrator** für den ersten Tunnel. Dies wird häufig als "Tunnel Group" (Tunnelgruppe) bezeichnet und dient zum Einrichten einer verschlüsselten Internet Key Exchange (IKE)-Sitzung mit dem VPN 3000 Concentrator mithilfe eines vorinstallierten Schlüssels (dem Gruppenkennwort). Dabei handelt es sich um denselben Gruppennamen und dasselbe Kennwort, die für alle Cisco VPN-Clients konfiguriert werden sollten, die eine Verbindung zum VPN Concentrator herstellen möchten.
- **Konfigurieren Sie Gruppen auf dem Cisco Secure ACS für Windows-Server**, die standardmäßige RADIUS-Attribute und VSAs (Vendor Specific Attributes) für die Richtlinienverwaltung verwenden. Bei den VSAs, die mit dem VPN 3000 Concentrator verwendet werden sollen, handelt es sich um die RADIUS-Attribute (VPN 3000).
- **Konfigurieren Sie Benutzer auf dem Cisco Secure ACS für Windows RADIUS-Server, und weisen Sie sie einer auf demselben Server konfigurierten Gruppe zu.** Die Benutzer erben die für ihre Gruppe definierten Attribute, und Cisco Secure ACS für Windows sendet diese Attribute an den VPN Concentrator, wenn der Benutzer authentifiziert wird.

Verwendung von Gruppen- und Benutzerattributen im VPN 3000-Konzentrator

Nachdem der VPN 300 Concentrator die Tunnelgruppe mit dem VPN Concentrator und der Benutzer mit RADIUS authentifiziert hat, muss er die erhaltenen Attribute organisieren. Der VPN Concentrator verwendet die Attribute in der angegebenen Reihenfolge, unabhängig davon, ob die Authentifizierung im VPN Concentrator oder mit RADIUS erfolgt:

1. **Benutzerattribute** - Diese Attribute haben immer Vorrang vor anderen Attributen.
2. **Tunnelgruppenattribute** - Alle Attribute, die bei der Benutzerauthentifizierung nicht zurückgegeben wurden, werden durch die Tunnelgruppenattribute ausgefüllt.
3. **Basisattribute** - Alle Attribute, die in den Attributen Benutzer oder Tunnelgruppe fehlen,

werden durch die Attribute der VPN Concentrator Base Group ausgefüllt.

Konfiguration des VPN Concentrators der Serie 3000

Führen Sie die Schritte in diesem Abschnitt aus, um einen Cisco VPN 3000-Konzentrator für die Parameter zu konfigurieren, die für die IPsec-Verbindung erforderlich sind, sowie den AAA-Client, der dem VPN-Benutzer die Authentifizierung beim RADIUS-Server ermöglicht.

In dieser Übung wird zuerst auf den VPN Concentrator über den Konsolenport zugegriffen, und es wird eine minimale Konfiguration hinzugefügt, wie die folgende Ausgabe zeigt:

Login: admin

```
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address -----
----- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
----- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address -----
----- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>
```

Der VPN-Konzentrator wird in der Schnellkonfiguration angezeigt, und diese Artikel sind konfiguriert.

- Uhrzeit/Datum
- Schnittstellen/Masken in **Konfiguration > Schnittstellen** (public=10.0.0.1/24, private=172.16.124.1/24)
- Standard-Gateway in **Konfiguration > System > IP-Routing > Default_Gateway** (10.0.0.2)

Der Zugriff auf den VPN Concentrator erfolgt über HTML aus dem internen Netzwerk.

Hinweis: Wenn der VPN Concentrator von außen verwaltet wird, führen Sie auch die folgenden Schritte aus:

1. Wählen Sie **Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1 aus. Private (Standard)**.
2. Wählen Sie **Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager Workstation**, um die IP-Adresse des externen Managers hinzuzufügen.

Diese Schritte sind nur erforderlich, wenn Sie den VPN Concentrator von außen verwalten.

Wenn Sie diese beiden Schritte abgeschlossen haben, können Sie die restliche Konfiguration über die Benutzeroberfläche vornehmen, indem Sie einen Webbrowser verwenden und eine Verbindung mit der IP-Adresse der soeben konfigurierten Schnittstelle herstellen. In diesem Beispiel und zu diesem Zeitpunkt ist der Zugriff auf den VPN Concentrator über HTML vom internen Netzwerk aus möglich:

1. Wählen Sie **Configuration > Interfaces (Konfiguration > Schnittstellen)** aus, um die Schnittstellen nach dem Aufrufen der Benutzeroberfläche erneut zu überprüfen.

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

2. Führen Sie diese Schritte aus, um den Cisco Secure ACS für Windows RADIUS-Server zur Konfiguration des VPN 3000 Concentrator hinzuzufügen. Wählen Sie **Configuration > System > Servers > Authentication** aus, und klicken Sie im linken Menü auf **Add**.

Configure and add a user authentication server.

Server Type	<input type="text" value="RADIUS"/>	Selecting <i>Internal Server</i> will let you add users to database. If you are using RADIUS authenticator additional authorization check, do not configure at
Authentication Server	<input type="text" value="172.16.124.5"/>	Enter IP address or hostname.
Used For	<input type="text" value="User Authentication"/>	Select the operation(s) for which this RADIUS se
Server Port	<input type="text" value="0"/>	Enter 0 for default port (1645).
Timeout	<input type="text" value="4"/>	Enter the timeout for this server (seconds).
Retries	<input type="text" value="2"/>	Enter the number of retries for this server.
Server Secret	<input type="text" value="aAaAaAaAaA"/>	Enter the RADIUS server secret.
Verify	<input type="text" value="aAaAaAaAaA"/>	Re-enter the secret.

Wählen Sie den Servertyp **RADIUS** aus, und fügen Sie diese Parameter für Ihren Cisco Secure ACS für Windows RADIUS-Server hinzu. Behalten Sie alle anderen Parameter im Standardzustand bei. **Authentication Server** (Authentifizierungsserver): Geben Sie die IP-Adresse des Cisco Secure ACS für Windows RADIUS-Server ein. **Server Secret** (Servergeheimnis): Geben Sie den geheimen RADIUS-Server ein. Dies muss der gleiche geheime Schlüssel sein, den Sie bei der Konfiguration des VPN 3000-Konzentrators in der Cisco Secure ACS for Windows-Konfiguration verwenden. **Verifizieren** - Geben Sie das Kennwort zur Überprüfung erneut ein. Damit wird der Authentifizierungsserver in die globale Konfiguration des VPN 3000 Concentrator aufgenommen. Dieser Server wird von allen Gruppen verwendet, außer wenn ein Authentifizierungsserver speziell definiert wurde. Wenn ein Authentifizierungsserver nicht für eine Gruppe konfiguriert ist, wird er auf den globalen Authentifizierungsserver zurückgesetzt.

- Führen Sie diese Schritte aus, um die Tunnelgruppe auf dem VPN 3000-Konzentrator zu konfigurieren. Wählen Sie im linken Menü **Konfiguration > Benutzerverwaltung > Gruppen** aus, und klicken Sie auf **Hinzufügen**. Ändern oder fügen Sie diese Parameter auf den Registerkarten "Konfiguration" hinzu. Klicken Sie erst auf Apply, wenn Sie alle folgenden Parameter geändert haben: **Hinweis:** Diese Parameter sind das Minimum, das für VPN-Verbindungen mit Remote-Zugriff erforderlich ist. Bei diesen Parametern wird außerdem davon ausgegangen, dass die Standardeinstellungen in der Basisgruppe des VPN 3000-Konzentrators nicht geändert wurden. **Identität**

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	<input type="text" value="ipsecgroup"/>	Enter a unique name for the group.
Password	<input type="password" value=""/>	Enter the password for the group.
Verify	<input type="password" value=""/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

Gruppenname: Geben Sie einen Gruppennamen ein. Beispielsweise IPsecUsers.
Password (Kennwort): Geben Sie ein Kennwort für die Gruppe ein. Dies ist der vorinstallierte Schlüssel für die IKE-Sitzung.
Verifizieren - Geben Sie das Kennwort zur Überprüfung erneut ein.
Type (Typ): Lassen Sie dies als Standard:
 Intern.**IPsec**

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	<input type="text" value="ESP-3DES-MD5"/>	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	<input type="text" value="If supported by certificate"/>	<input checked="" type="checkbox"/>	Select whether or not to validate the identity.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives.
Confidence Interval	<input type="text" value="300"/>	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to remain idle before the concentrator checks to see if it is still connected.
Tunnel Type	<input type="text" value="Remote Access"/>	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Upgrades may be needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	<input type="text" value="RADIUS"/>	<input type="checkbox"/>	Select the authentication method for members of this group. This method only applies to Individual User Authentication .
Authorization Type	<input type="text" value="None"/>	<input checked="" type="checkbox"/>	If members of this group need authorization, select the authorization method. If you configure this method, you must also configure an Authorization Server.

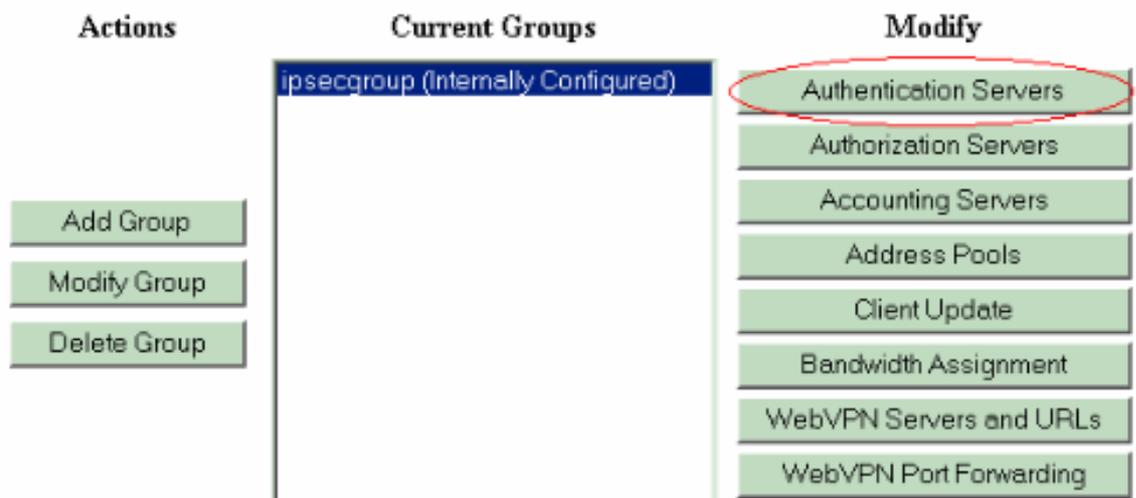
Tunnel Type (Tunnel-Typ): Wählen Sie **Remote Access (Remote-Zugriff)**.
Authentication (Authentifizierung) - RADIUS Dadurch wird dem VPN Concentrator mitgeteilt, welche Methode zur Benutzerauthentifizierung verwendet wird.
Mode Config (Moduskonfiguration): Konfig. Klicken Sie auf **Übernehmen**.

- Führen Sie diese Schritte aus, um mehrere Authentifizierungsserver im VPN 3000 Concentrator zu konfigurieren. Wenn die Gruppe definiert ist, markieren Sie diese Gruppe, und klicken Sie in der Spalte Ändern auf **Authentifizierungsserver**. Für jede Gruppe können individuelle Authentifizierungsserver definiert werden, auch wenn diese Server nicht auf den globalen Servern vorhanden

sind.

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To group parameters, select a group and click the appropriate button.



Wählen Sie den Servertyp **RADIUS aus**, und fügen Sie diese Parameter für Ihren Cisco Secure ACS für Windows RADIUS-Server hinzu. Behalten Sie alle anderen Parameter im Standardzustand bei.**Authentication Server** (Authentifizierungsserver): Geben Sie die IP-Adresse des Cisco Secure ACS für Windows RADIUS-Server ein.**Server Secret** (Servergeheimnis): Geben Sie den geheimen RADIUS-Server ein. Dies muss der gleiche geheime Schlüssel sein, den Sie bei der Konfiguration des VPN 3000-Konzentrators in der Cisco Secure ACS for Windows-Konfiguration verwenden.**Verifizieren** - Geben Sie das Kennwort zur Überprüfung erneut ein.

5. Wählen Sie **Configuration > System > Address Management > Assignment (Konfiguration > System > Adressenverwaltung > Zuweisung)** aus, und aktivieren Sie **Use Address from Authentication Server (Adresse aus Authentifizierungsserver verwenden)**, um den VPN-Clients die IP-Adresse aus dem im RADIUS-Server erstellten IP-Pool zuzuweisen, sobald der Client authentifiziert wurde.

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

- Use Client Address** Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
 - Use Address from Authentication Server** Check to use an IP address retrieved from an authentication server for the client.
 - Use DHCP** Check to use DHCP to obtain an IP address for the client.
 - Use Address Pools** Check to use internal address pool configuration to obtain an IP address for the client.
- IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply

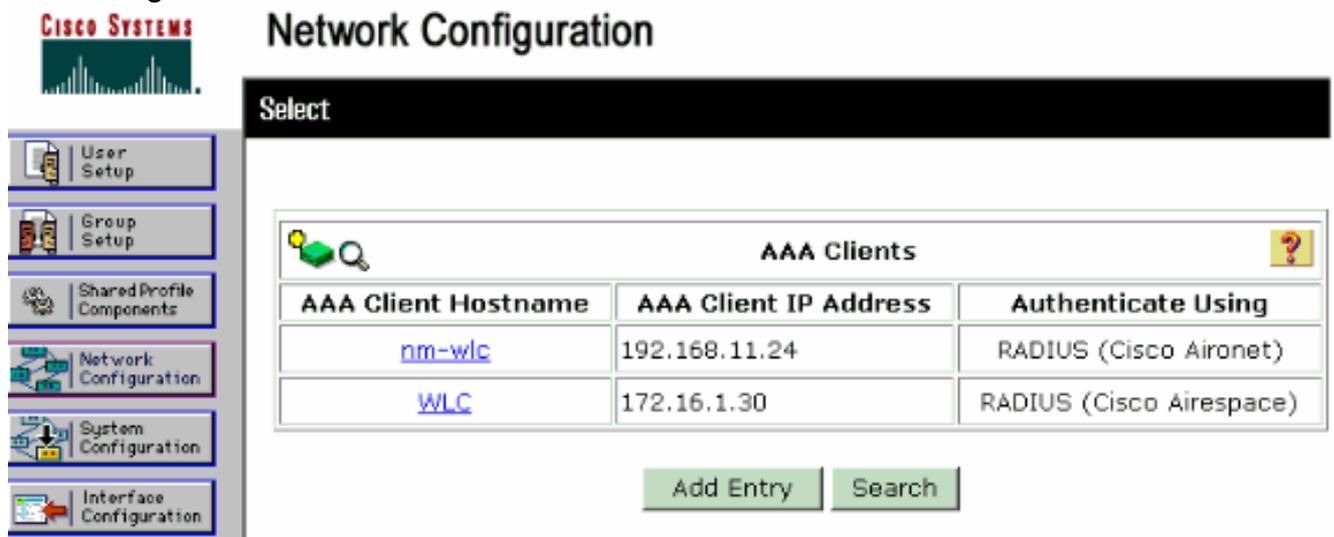
Cancel

RADIUS-Serverkonfiguration

In diesem Abschnitt des Dokuments wird das erforderliche Verfahren zur Konfiguration des Cisco Secure ACS als RADIUS-Server für die vom Cisco VPN Concentrator der Serie 3000 - AAA-Client weitergeleitete VPN-Client-Benutzerauthentifizierung beschrieben.

Doppelklicken Sie auf das Symbol **ACS Admin**, um die Admin-Sitzung auf dem PC zu starten, auf dem der Cisco Secure ACS für Windows RADIUS-Server ausgeführt wird. Melden Sie sich ggf. mit dem richtigen Benutzernamen und Kennwort an.

1. Gehen Sie wie folgt vor, um den VPN 300-Konzentrator der Cisco Secure ACS für Windows-Serverkonfiguration hinzuzufügen. Wählen Sie **Network Configuration** (Netzwerkkonfiguration) aus, und klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um dem RADIUS-Server einen AAA-Client hinzuzufügen.



The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation pane with icons for User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, and Interface Configuration. The main area is titled 'Network Configuration' and contains a 'Select' header. Below this is a table titled 'AAA Clients' with a search icon and a help icon. The table has three columns: 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. It lists two entries: 'nm-wlc' with IP 192.168.11.24 and 'WLC' with IP 172.16.1.30. Below the table are 'Add Entry' and 'Search' buttons.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
nm-wlc	192.168.11.24	RADIUS (Cisco Aironet)
WLC	172.16.1.30	RADIUS (Cisco Airespace)

Fügen Sie die folgenden Parameter für den VPN 300-Konzentrator hinzu:

Network Configuration

Edit

Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="172.16.124.1"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

Submit

Submit + Apply

Cancel

AAA-Client-Hostname - Geben Sie den Hostnamen des VPN 3000-Konzentrators (für die DNS-Auflösung) ein.**AAA-Client-IP-Adresse** - Geben Sie die IP-Adresse Ihres VPN 3000-Konzentrators ein.**Key** (Schlüssel) - Geben Sie den geheimen RADIUS-Server ein. Dies muss der gleiche geheime Schlüssel sein, den Sie beim Hinzufügen des Authentifizierungsservers im VPN Concentrator konfiguriert haben.**Authentication Using (Authentifizierung über RADIUS)** - Wählen Sie **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** aus. Dadurch können die VPN 3000 VSAs im Fenster "Gruppenkonfiguration" angezeigt werden.Klicken Sie auf **Senden**.Wählen Sie **Schnittstellenkonfiguration aus**, klicken Sie auf **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**, und aktivieren Sie **Group [26] Vendor-Specific (anbieterspezifische Gruppe [26])**.

Interface Configuration

Edit

RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

User Group

- [026/3076/001] Access-Hours
- [026/3076/002] Simultaneous-Logins
- [026/3076/005] Primary-DNS
- [026/3076/006] Secondary-DNS
- [026/3076/007] Primary-WINS
- [026/3076/008] Secondary-WINS
- [026/3076/009] SEP-Card-Assignment
- [026/3076/011] Tunneling-Protocols
- [026/3076/012] IPSec-Sec-Association
- [026/3076/013] IPSec-Authentication
- [026/3076/015] IPSec-Banner1
- [026/3076/016] IPSec-Allow-Passwd-Store

Submit

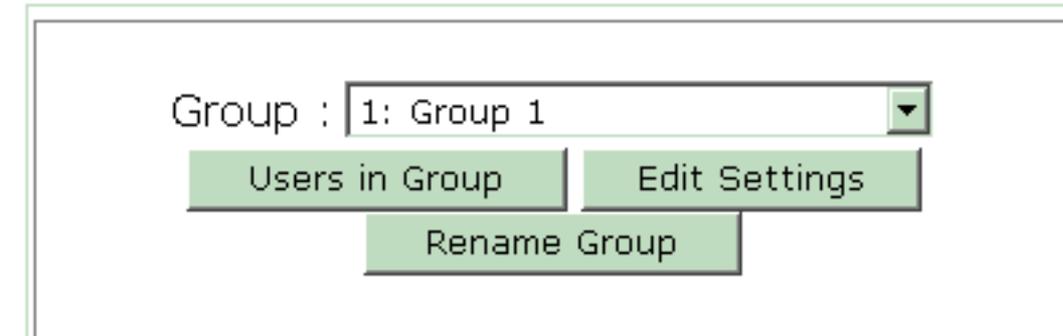
Cancel

Hinweis: "RADIUS-Attribut 26" bezieht sich auf alle anbieterspezifischen Attribute. Wählen Sie beispielsweise **Interface Configuration > RADIUS (Cisco VPN 3000)** und stellen Sie sicher, dass alle verfügbaren Attribute mit 026 beginnen. Dies zeigt, dass alle diese anbieterspezifischen Attribute unter den IETF RADIUS 26-Standard fallen. Diese Attribute werden standardmäßig nicht in der Benutzer- oder Gruppeneinrichtung angezeigt. Erstellen Sie zum Aufrufen in der Gruppe-Konfiguration einen AAA-Client (in diesem Fall VPN 3000-Konzentrator), der sich in der Netzwerkkonfiguration mit RADIUS authentifiziert. Überprüfen Sie dann die Attribute, die in User Setup (Benutzereinrichtung), Group Setup (Gruppeneinrichtung) oder in beiden Optionen in der Schnittstellenkonfiguration angezeigt werden müssen. Unter [RADIUS-Attribute](#) finden Sie weitere Informationen zu den verfügbaren Attributen und deren Verwendung. Klicken Sie auf **Senden**.

2. Führen Sie diese Schritte aus, um der Cisco Secure ACS für Windows-Konfiguration Gruppen hinzuzufügen. Wählen Sie **Group Setup (Gruppeneinrichtung)** aus, wählen Sie eine der Vorlagengruppen aus, z. B. Gruppe 1, und klicken Sie auf **Gruppe**

Group Setup

Select



Group : 1: Group 1

Users in Group Edit Settings

Rename Group

umbenennen.

Ändern Sie den Namen in eine für Ihre Organisation geeignete Form, z. B. ipsecgroup. Da diesen Gruppen Benutzer hinzugefügt werden, sollte der Gruppenname den tatsächlichen Zweck dieser Gruppe widerspiegeln. Wenn alle Benutzer derselben Gruppe angehören, können Sie diese VPN-Benutzergruppe nennen. Klicken Sie auf **Einstellungen bearbeiten**, um die Parameter in der neu umbenannten Gruppe zu

Group Setup

Jump To

Group Settings : ipsecgroup

Access Restrictions

Group Disabled 

Members of this group will be denied access to the network.

Callback 

No callback allowed
 Dialup client specifies callback number
 Use Windows Database callback settings (where possible)

bearbeiten.

Klicken Sie auf **Cisco VPN 3000 RADIUS**, und konfigurieren Sie diese empfohlenen Attribute. Auf diese Weise können Benutzer, die dieser Gruppe zugewiesen sind, die Cisco VPN 3000 RADIUS-Attribute erben, sodass Sie Richtlinien für alle Benutzer in Cisco Secure ACS für Windows zentralisieren

Group Setup

Jump To

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

können.

Hin

weis: Technisch gesehen müssen VPN 3000 RADIUS-Attribute nicht konfiguriert werden, solange die Tunnelgruppe in Schritt 3 der [Konfiguration](#) des [VPN-Konzentrators der Serie 300](#) eingerichtet ist und die Basisgruppe im VPN-Konzentrator nicht von den ursprünglichen Standardeinstellungen abweicht. **Empfohlene VPN 3000-Attribute:** **Primary-DNS** (Primärer DNS): Geben Sie die IP-Adresse Ihres primären DNS-Servers ein. **Secondary-DNS** - Geben Sie die IP-Adresse Ihres sekundären DNS-Servers ein. **Primary-WINS** - Geben Sie die IP-Adresse Ihres primären WINS-Servers ein. **Secondary-WINS** - Geben Sie die IP-Adresse Ihres sekundären WINS-Servers ein. **Tunneling-Protokolle** - Wählen Sie **IPsec** aus. Dies ermöglicht *nur* IPsec-Clientverbindungen. PPTP oder L2TP sind nicht zulässig. **IPsec-Sec-Association** - Geben Sie **ESP-3DES-MD5 ein**. Dadurch wird sichergestellt, dass alle IPsec-Clients die höchstmögliche Verschlüsselung verwenden. **IPsec-Allow-Password-Store** - Wählen Sie **Disallow (Unterbrechen)** aus, damit Benutzer ihr Kennwort nicht im VPN-Client speichern können. **IPsec-Banner** - Geben Sie ein Begrüßungs-Banner ein, das dem Benutzer bei der Verbindung angezeigt wird. Beispiel: "Willkommen beim VPN-Zugriff für Mitarbeiter von MyCompany!" **IPsec-Default Domain** - Geben Sie den Domännennamen Ihres

Unternehmens ein. Beispiel: "mycompany.com". Dieser Satz von Attributen ist nicht erforderlich. Wenn Sie sich jedoch nicht sicher sind, ob sich die Attribute der Basisgruppe des VPN 3000-Konzentrators geändert haben, empfiehlt Cisco, die folgenden Attribute zu konfigurieren:

- Simultaneous-Logins:** Geben Sie die Anzahl der Anmeldeversuche eines Benutzers mit demselben Benutzernamen ein. Die Empfehlung lautet 1 oder 2.
- SEP-Card-Assignment** - Wählen Sie **Any-SEP aus**.
- IPsec-Mode-Config** - Wählen Sie **ON (EIN)**.
- IPsec over UDP** (IPsec über UDP): Wählen Sie **AUS**, es sei denn, Sie möchten, dass Benutzer in dieser Gruppe IPsec über das UDP-Protokoll verbinden. Wenn Sie **ON** auswählen, kann der VPN-Client IPsec über UDP lokal deaktivieren und eine normale Verbindung herstellen.
- IPsec über UDP-Port** - Wählen Sie eine UDP-Portnummer zwischen 4001 und 49151 aus. Dies wird nur verwendet, wenn IPsec über UDP **ON** ist. Für den nächsten Satz von Attributen müssen Sie zunächst im VPN-Concentrator etwas einrichten, bevor Sie diese verwenden können. Dies wird nur für fortgeschrittene Benutzer empfohlen.
- Zugriffszeiten:** Sie müssen für den VPN 3000-Konzentrator unter **Konfiguration > Richtlinienmanagement** eine Reihe von Zugriffszeiten einrichten. Verwenden Sie stattdessen die in Cisco Secure ACS für Windows verfügbaren Zugriffszeiten, um dieses Attribut zu verwalten.
- IPsec-Split-Tunnel-List:** Hierfür müssen Sie im VPN-Konzentrator unter **Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement** eine Netzwerkliste einrichten. Dies ist eine Liste von Netzwerken, die an den Client gesendet werden, um den Client anzuweisen, Daten nur an die Netzwerke in der Liste zu verschlüsseln. Wählen Sie **IP-Zuweisung in der Gruppeneinrichtung aus**, und aktivieren Sie **Assigned from AAA server Pool (Aus AAA-Serverpool zugewiesen)**, um die IP-Adressen nach der Authentifizierung VPN Client-Benutzern

Group Setup

Jump To IP Address Assignment

IP Assignment

No IP address assignment

Assigned by dialup client

Assigned from AAA Client pool

Assigned from AAA server pool

Available Pools

Selected Pools

pool1

->

<-

Up Down

zuzuweisen.

W

ählen Sie **Systemkonfiguration > IP-Pools**, um einen IP-Pool für VPN-Client-Benutzer zu erstellen, und klicken Sie auf

System Configuration

Edit

New Pool

Name

Start Address

End Address

Submit

Cancel

Senden.

System Configuration

Select

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
pool1	10.1.1.1	10.1.1.10	0%

Wählen Sie

Senden > Neu starten, um die Konfiguration zu speichern und die neue Gruppe zu aktivieren. Wiederholen Sie diese Schritte, um weitere Gruppen hinzuzufügen.

3. Konfigurieren von Benutzern auf Cisco Secure ACS für Windows Wählen Sie **User Setup**, geben Sie einen Benutzernamen ein, und klicken Sie auf **Hinzufügen/Bearbeiten**.

User Setup

Select

User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

Konfigurieren Sie

diese Parameter im Abschnitt
"Benutzereinrichtung":

User Setup

User: ipsecuser1 (New User)

Account Disabled

Supplementary User Info 

Real Name

Description

User Setup 

Password Authentication:



CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:



Kennwortauthentifizierung - Wählen Sie **ACS Internal Database (Interne ACS-Datenbank)** aus. **Cisco Secure PAP - Kennwort** - Geben Sie ein Kennwort für den Benutzer ein. **Cisco Secure PAP - Passwort bestätigen** - Geben Sie das Kennwort für den neuen Benutzer erneut ein. **Gruppe, der der Benutzer zugewiesen ist** - Wählen Sie den Namen der Gruppe aus, die Sie im vorherigen Schritt erstellt haben. Klicken Sie auf **Senden**, um die Benutzereinstellungen zu speichern und zu aktivieren. Wiederholen Sie diese Schritte, um weitere Benutzer hinzuzufügen.

[Zuweisen einer statischen IP-Adresse zum VPN-Client-Benutzer](#)

Gehen Sie wie folgt vor:

1. Erstellen Sie eine neue VPN-Gruppe IPSECGRP.
2. Erstellen Sie einen Benutzer, der die statische IP empfangen möchte, und wählen Sie **IPSECGRP** aus. Wählen Sie **Statische IP-Adresse** mit der statischen IP-Adresse **zuweisen**, die unter der Client-IP-Adressenzuweisung zugewiesen

User Setup

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm
Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IPSECGRP

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

Submit

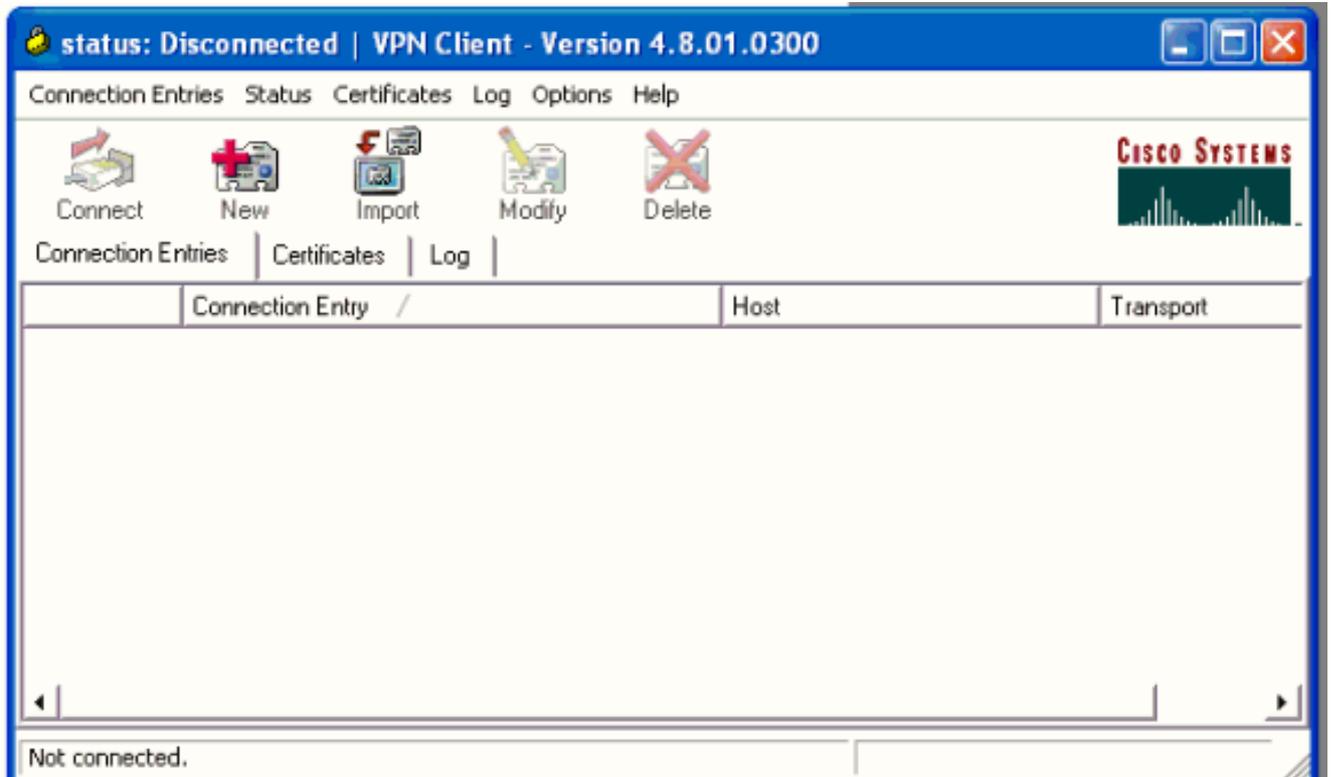
Delete

Cancel

wird.

In diesem Abschnitt wird die Konfiguration der VPN-Client-Seite beschrieben.

1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > VPN Client** aus.
2. Klicken Sie auf **Neu**, um das Fenster Create New VPN Connection Entry (Neue VPN-Verbindung erstellen) zu öffnen.



3. Weisen Sie Ihrem Eintrag bei Aufforderung einen Namen zu. Sie können auch eine Beschreibung eingeben, wenn Sie möchten. Geben Sie die IP-Adresse der öffentlichen Schnittstelle des VPN 3000 Concentrator in der Spalte Host an, und wählen Sie **Gruppenauthentifizierung** aus. Geben Sie dann den Gruppennamen und das Kennwort ein. Klicken Sie auf **Speichern**, um den neuen VPN-Verbindungseintrag abzuschließen.

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name:

Password:

Confirm Password:

Certificate Authentication

Name:

Send CA Certificate Chain

Erase User Password | Save | Cancel

Hinweis:

Stellen Sie sicher, dass der VPN-Client so konfiguriert ist, dass er denselben Gruppennamen und dasselbe Kennwort verwendet, der im Cisco VPN-Konzentrator der Serie 3000 konfiguriert wurde.

Accounting hinzufügen

Nach der Authentifizierung können Sie Accounting hinzufügen.

1. Wählen Sie auf dem VPN 300 **Configuration > System > Servers > Accounting Servers** aus, und fügen Sie den **Cisco Secure ACS für Windows-Server** hinzu.
2. Sie können jeder Gruppe individuelle Accounting-Server hinzufügen, wenn Sie **Konfiguration > Benutzerverwaltung > Gruppen** auswählen, eine Gruppe markieren und auf **Konto ändern** klicken. **Server**. Geben Sie dann die IP-Adresse des Accounting-Servers mit dem Servergeheimnis ein.

Remote Access Sessions

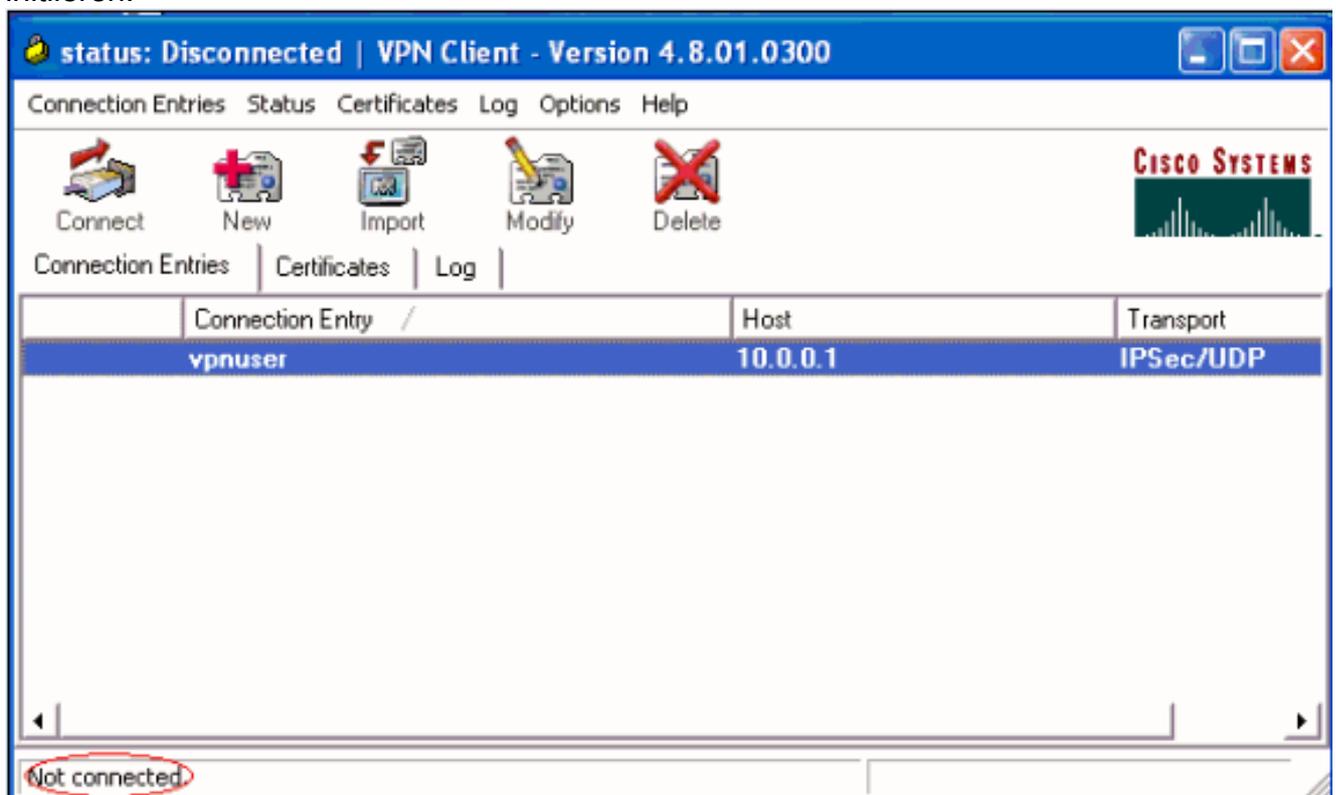
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

<u>Username</u>	<u>Assigned IP Address</u> <u>Public IP Address</u>	<u>Group</u>	<u>Protocol Encryption</u>	<u>Login Time Duration</u>	<u>Client Type Version</u>	<u>Bytes Tx</u> <u>Bytes Rx</u>	<u>NAC Result Posture Token</u>	<u>Actions</u>
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout Ping]

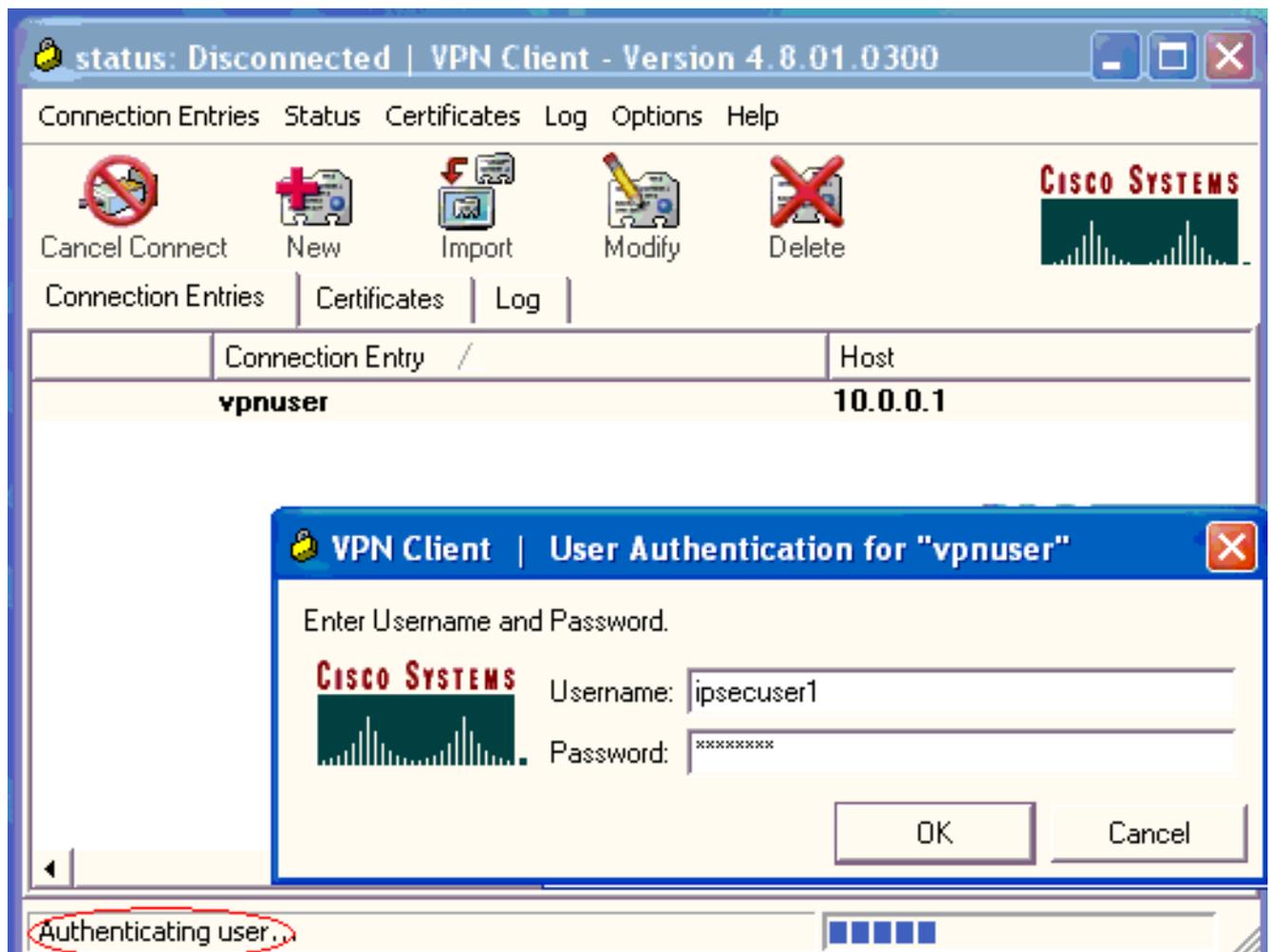
Überprüfen des VPN-Clients

Führen Sie diese Schritte aus, um den VPN-Client zu überprüfen.

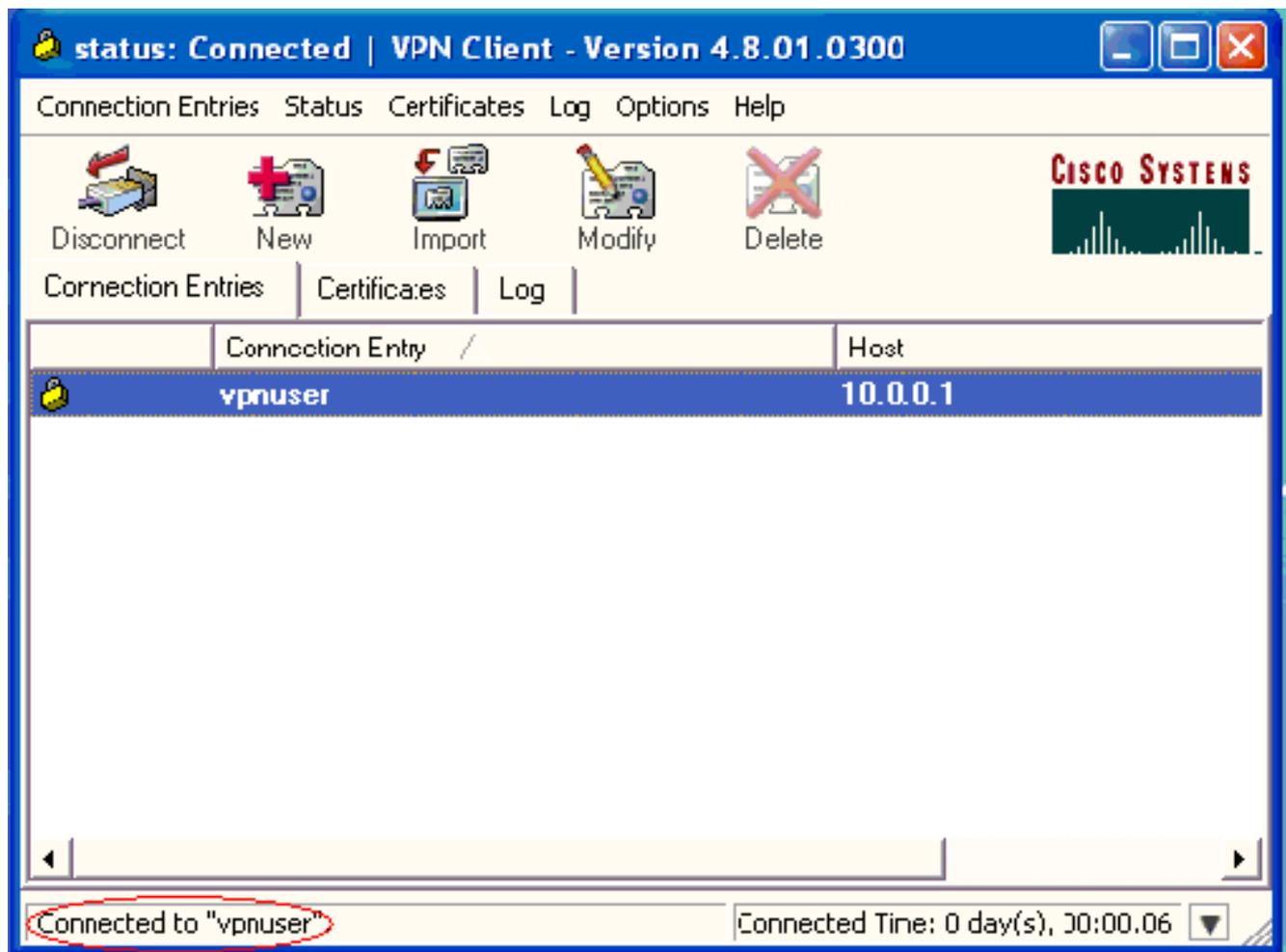
1. Klicken Sie auf **Verbinden**, um eine VPN-Verbindung zu initiieren.



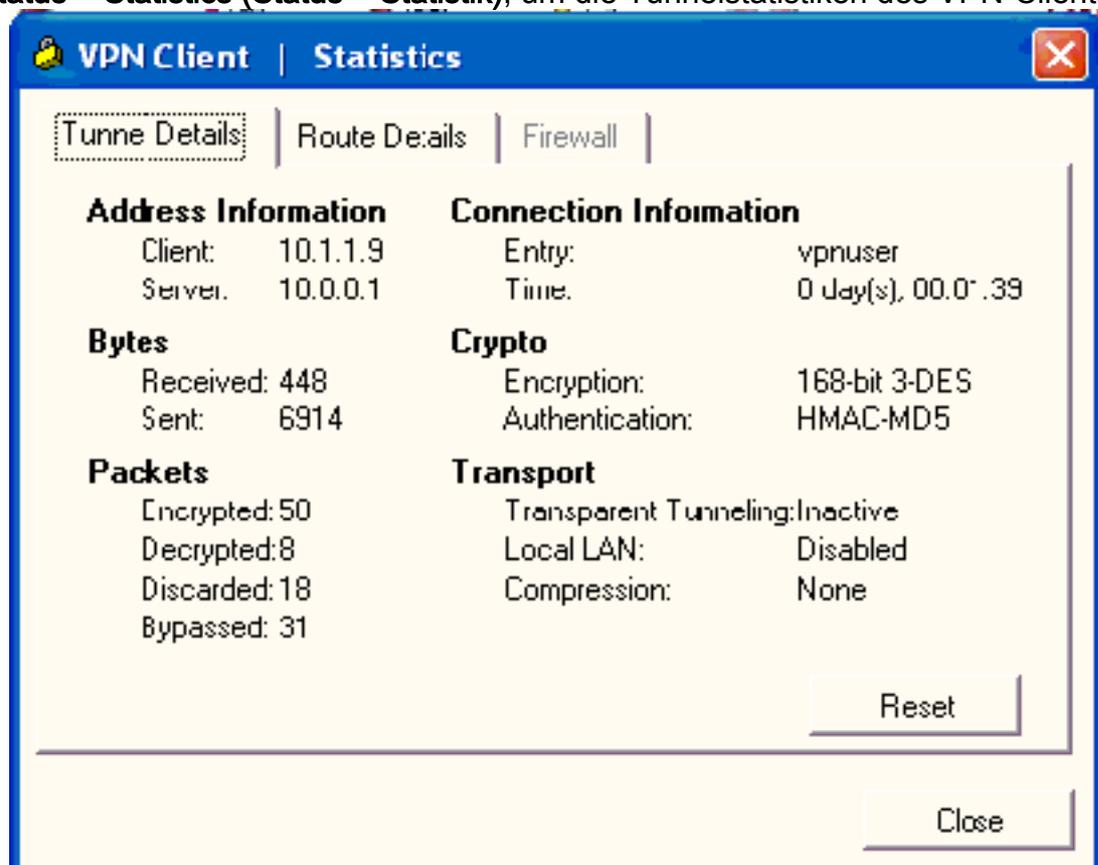
2. Dieses Fenster wird für die Benutzerauthentifizierung angezeigt. Geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort ein, um die VPN-Verbindung herzustellen.



3. Der VPN-Client wird in der Zentrale mit dem VPN 3000-Konzentrator verbunden.



4. Wählen Sie **Status > Statistics (Status > Statistik)**, um die Tunnelstatistiken des VPN-Clients



zu überprüfen.

Fehlerbehebung

Führen Sie diese Schritte aus, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen.

1. Wählen Sie **Configuration > System > Servers > Authentication (Konfiguration > System > Server > Authentifizierung)** aus, und führen Sie diese Schritte aus, um die Verbindung zwischen dem RADIUS-Server und dem VPN 3000-Konzentrator zu testen. Wählen Sie den Server aus, und klicken Sie dann auf **Test**.

Configuration | System | Servers | Authentication

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or

Authentication Servers	Actions
172.16.124.5 (Radius/User Authentication) Internal (Internal)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test"/>

Geben Sie den RADIUS-Benutzernamen und das RADIUS-Kennwort ein, und klicken Sie auf **OK**.

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation**

Username

Password

Success

 Authentication Successful

Continue

Eine erfolgreiche Authentifizierung wird angezeigt.

2. Wenn es fehlschlägt, liegt entweder ein Konfigurationsproblem oder ein IP-Verbindungsproblem vor. Überprüfen Sie, ob im ACS-Server bei fehlgeschlagenen Versuchen Meldungen zu dem Fehler eingehen. Wenn in diesem Protokoll keine Meldungen angezeigt werden, liegt wahrscheinlich ein Problem mit der IP-Verbindung vor. Die RADIUS-Anforderung erreicht den RADIUS-Server nicht. Überprüfen Sie, ob die auf die entsprechende VPN 300 Concentrator-Schnittstelle angewendeten Filter RADIUS (1645)-Pakete ein- und auslassen. Wenn die Testauthentifizierung erfolgreich ist, die Anmeldung beim VPN 3000-Konzentrator jedoch weiterhin fehlschlägt, überprüfen Sie das filterbare Ereignisprotokoll über den Konsolenport. Wenn Verbindungen nicht funktionieren, können Sie dem VPN-Konzentrator AUTH-, IKE- und IPsec-Ereignisklassen hinzufügen, wenn Sie **Configuration > System > Events > Classes > Modify (Severity to Log=1-9, Severity to Console=1-3)** auswählen. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG und IPSECDECODE sind ebenfalls verfügbar, können aber zu viele Informationen bereitstellen. Wenn detaillierte Informationen zu den Attributen benötigt werden, die vom RADIUS-Server, AUTHDECODE, IKEDECODE und IPSECDECODE weitergeleitet werden, stellen Sie diese auf der Ebene Severity to Log=1-13 bereit.
3. Rufen Sie das Ereignisprotokoll von **Überwachung > Ereignisprotokoll** ab.

Monitoring | Live Event Log

```
1513 10/27/2006 18:37:25.330 SEV=8 IKEDBG/81 RPT=47 192.168.1.2
SENDING Message (msgid=6679165e) with payloads :
HDR + HASH (8) + NOTIFY (11)
total length : 80

1515 10/27/2006 18:37:35.830 SEV=8 IKEDBG/81 RPT=48 192.168.1.2
RECEIVED Message (msgid=8575be96) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0)
total length : 80

1517 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=120 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
processing hash

1518 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=121 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Processing Notify payload

1519 10/27/2006 18:37:35.830 SEV=9 IKEDBG/36 RPT=10 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x653e486d)

1521 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=122 192.168.1.2
```

Pause Display

Clear Display

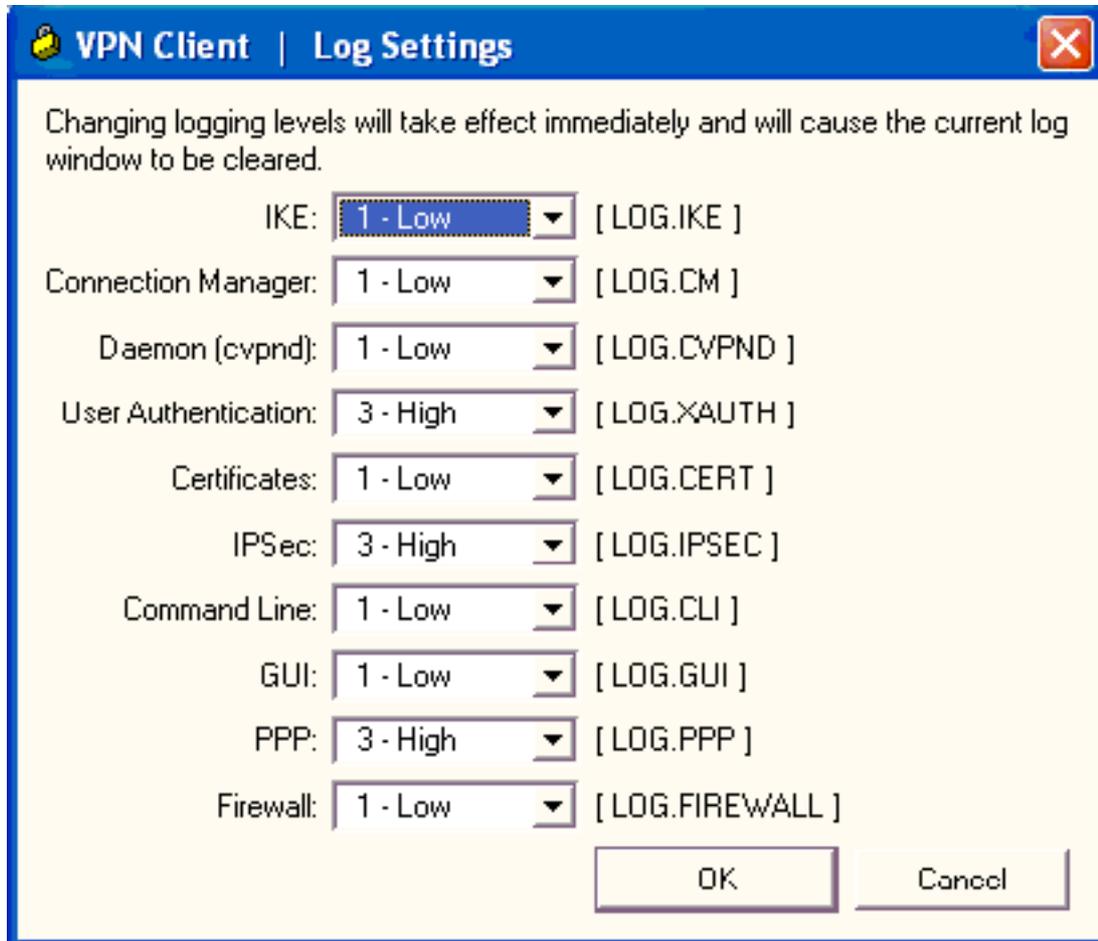
Restart

Receiving.....

Fehlerbehebung beim VPN Client 4.8 für Windows

Führen Sie diese Schritte aus, um eine Fehlerbehebung für VPN Client 4.8 für Windows durchzuführen.

1. Wählen Sie **Log > Log settings** (Protokoll > Protokolleinstellungen), um die Protokollstufen im VPN-Client zu



aktivieren.

2. Wählen Sie **Log > Log Window** (Protokoll > Protokollfenster), um die Protokolleinträge im VPN-Client anzuzeigen.

```
Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1  13:26:29.234 10/31/06 Sev=Warning/2  IKE/0xA3000067
Received an IPC message during invalid state (IKE_MAIN:507)

2  13:26:36.109 10/31/06 Sev=Warning/2  CVPND/0xE3400013
AddRoute failed to add a route: code 87
    Destination      192.168.1.255
    Netmask           255.255.255.255
    Gateway           10.1.1.9
    Interface         10.1.1.9

3  13:26:36.109 10/31/06 Sev=Warning/2  CM/0xA3100024
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1  13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2  13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0xc9c1b7d5

3  13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0xc9c1b7d5

4  13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2c9afd45

5  13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2c9afd45
```

[Zugehörige Informationen](#)

- [Support-Seite für Cisco VPN Concentrator der Serie 3000](#)
- [Support-Seite für Cisco VPN-Clients](#)
- [IPsec-Aushandlung/IKE-Protokolle](#)
- [Support-Seite für Cisco Secure ACS für Windows](#)
- [Konfigurieren dynamischer Filter auf einem RADIUS-Server](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)