

IPsec tussen een VPN 3000 Concentrator en een VPN-client 4.x voor Windows met RADIUS voor gebruikersverificatie en -accounting

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Gebruik groepen in de VPN-Concentrator 3000](#)

[Hoe de VPN 3000 Concentrator groep en gebruikerskenmerken gebruikt](#)

[VPN 3000 Series Concentrator-configuratie](#)

[Configuratie van RADIUS-servers](#)

[Een statisch IP-adres aan de VPN-clientgebruiker toewijzen](#)

[VPN-clientconfiguratie](#)

[Voeg accounting toe](#)

[Verifiëren](#)

[Controleer de VPN-concentratie](#)

[Controleer de VPN-client](#)

[Problemen oplossen](#)

[Probleemoplossing VPN-client 4.8 voor Windows](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u een IPsec-tunnel kunt creëren tussen een Cisco VPN 3000 Concentrator en een Cisco VPN-client 4.x voor Microsoft Windows die RADIUS gebruikt voor gebruikersverificatie en -accounting. Dit document raadt Cisco Secure Access Control Server (ACS) aan voor Windows voor een makkelijke RADIUS-configuratie om gebruikers te authentifieren die verbinding maken met een VPN 3000 Concentrator. Een groep op een VPN 3000 Concentrator is een verzameling gebruikers die als één entiteit worden behandeld. De configuratie van groepen in tegenstelling tot individuele gebruikers kan het systeembeheer vereenvoudigen en de configuratie van taken stroomlijnen.

Raadpleeg [PIX/ASA 7.x en Cisco VPN-client 4.x voor Windows met Microsoft Windows 2003 IAS RADIUS-verificatievoorbeeld](#) voor het instellen van de VPN-verbinding voor externe toegang tussen een Cisco VPN-client (4.x voor Windows) en de PIX 500 Series security applicatie 7.x die gebruik maakt van een Microsoft Windows 2003 Internet Accounting Service (IAS) RADIUS-server

Raadpleeg [IPsec configureren tussen een Cisco IOS-router en een Cisco VPN-client 4.x voor Windows Gebruik van RADIUS voor gebruikersverificatie](#) om een verbinding te configureren tussen een router en Cisco VPN-client 4.x die RADIUS gebruikt voor gebruikersverificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure ACS voor Windows RADIUS is geïnstalleerd en werkt correct met andere apparaten.
- De Cisco VPN 3000 Concentrator wordt geconfigureerd en kan worden beheerd met de HTML-interface.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure ACS voor Windows met versie 4.0
- Cisco VPN 3000 Series Concentrator met beeldbestand 4.7.2.B
- Cisco VPN-client 4.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

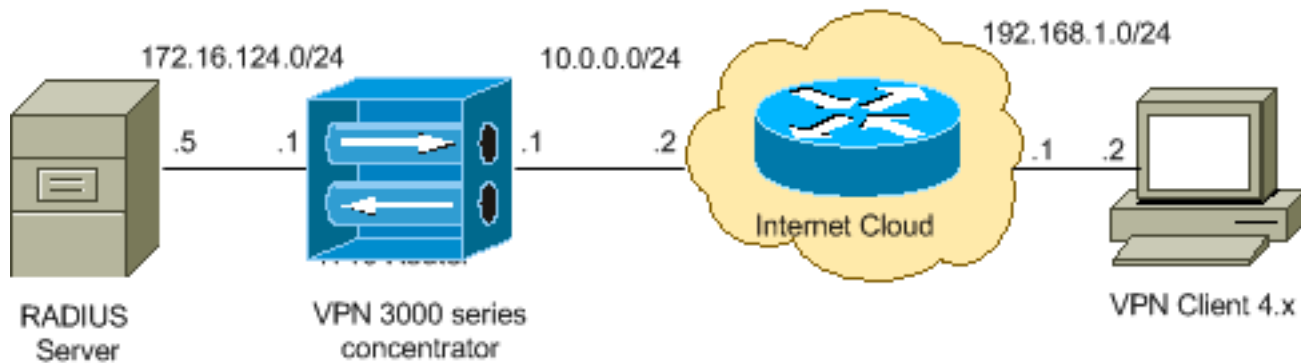
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het [Opname Gereedschap](#) ([alleen geregistreerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Gebruik groepen in de VPN-Concentrator 3000

Groepen kunnen worden gedefinieerd voor Cisco Secure ACS voor Windows en de VPN 3000 Concentrator, maar ze gebruiken groepen op een verschillende manier. Voer deze taken uit om de zaken te vereenvoudigen:

- **Configuratie één enkele groep op de VPN 3000 Concentrator** voor wanneer u de aanvankelijke tunnel opstelt. Dit wordt vaak de Tunnel Groep genoemd en wordt gebruikt om een gecodeerde Toets Exchange (IKE)-sessie aan de VPN 3000 Concentrator op te zetten met behulp van een vooraf gedeelde toets (het groepswachtwoord). Dit is dezelfde groepsnaam en hetzelfde wachtwoord dat op alle Cisco VPN-clients moet worden ingesteld die met de VPN-centrator willen verbinden.
- **Configureer groepen op de Cisco Secure ACS voor Windows-server** die de standaard RADIUS-kenmerken en leveranciersspecifieke kenmerken (VSA's) gebruiken voor beleidsbeheer. De VSA's die met de VPN 3000 Concentrator zouden moeten worden gebruikt zijn de RADIUS (VPN 3000) eigenschappen.
- **Configureer gebruikers op de Cisco Secure ACS voor Windows RADIUS-server en wijs ze toe aan een van de groepen** die op dezelfde server zijn geconfigureerd. De gebruikers erven eigenschappen die voor hun groep worden gedefinieerd en Cisco Secure ACS voor Windows versturen die eigenschappen naar VPN Concentrator wanneer de gebruiker voor authentiek is verklaard.

Hoe de VPN 3000 Concentrator groep en gebruikerskenmerken gebruikt

Nadat de VPN 3000 Concentrator de Tunnel Group met de VPN Concentrator en de gebruiker met RADIUS voor authentiek heeft verklaard, moet deze de eigenschappen organiseren die hij heeft ontvangen. De VPN Concentrator gebruikt de eigenschappen in deze volgorde van voorkeur, of de authenticatie plaatsvindt in de VPN-centrator of met RADIUS:

1. **Eigenschappen**—Deze eigenschappen hebben altijd voorrang op enige andere eigenschappen.
2. **Eigenschappen van de Tunnelgroep**—Om het even welke eigenschappen die niet werden teruggegeven toen de gebruiker echt werd bevonden worden ingevuld door de eigenschappen van de Tunnelgroep.
3. **Eigenschappen van de Base Group**—Alle eigenschappen die ontbreken van de

eigenschappen van de gebruiker of de Tunnelgroep worden ingevuld door de eigenschappen van de Base Group van VPN Concentrator.

VPN 3000 Series Concentrator-configuratie

Voltooi de procedure in dit gedeelte om een Cisco VPN 3000 Concentrator te configureren voor de parameters die vereist zijn voor de IPsec-verbinding en de AAA-client voor de VPN-gebruiker om te authenticeren met de RADIUS-server.

In deze lab-instelling wordt eerst VPN Concentrator benaderd via de console poort en wordt een minimale configuratie toegevoegd zoals deze uitvoer toont:

```
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 -
>
```

De VPN Concentrator verschijnt in Quick Configuration en deze items worden ingesteld.

- Tijd/datum
- Interfaces/maskers in **configuratie > Interfaces** (publiek=10.0.0.1/24, privé=172.16.124.1/24)
- Standaard gateway in **configuratie > Systeem > IP-routing > Default_Gateway** (10.0.0.2)

Op dit punt is de VPN Concentrator toegankelijk via HTML van het binnennetwerk.

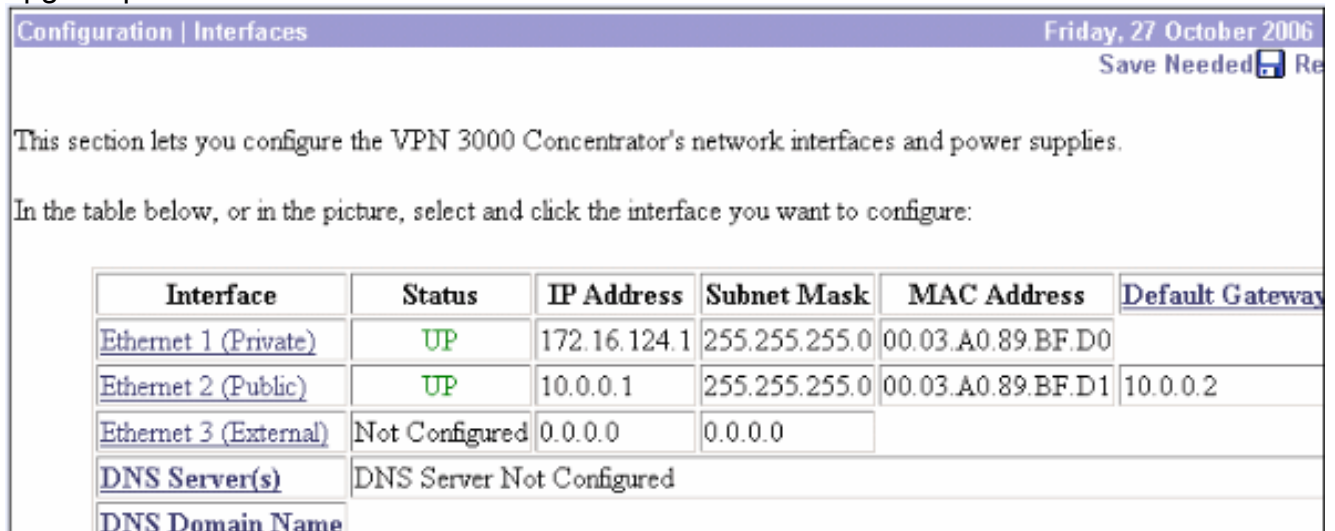
N.B.: Als de VPN Concentrator van buiten wordt beheerd, voert u ook deze stappen uit:

1. Kies **Configuratie > 1-interfaces > 2-openbare > 4-Selecteer IP-filter > 1. Private (standaard)**.
2. Kies **Beheer > 7-toegangsrechten > 2-toegangscontrolelijst > 1-Add Manager Workstation** om het IP-adres van de externe manager toe te voegen.

Deze stappen zijn alleen vereist als u de VPN-centrator van buiten beheert.

Nadat u deze twee stappen hebt voltooid, kan de rest van de configuratie door de GUI worden uitgevoerd door gebruik te maken van een webbrowser en een verbinding te maken met de IP van de interface die u zojuist hebt ingesteld. In dit voorbeeld en op dit punt, is de VPN Concentrator toegankelijk door HTML van het binnennetwerk:

1. Kies **Configuration > Interfaces** om de interfaces opnieuw te controleren nadat u de GUI hebt opgeroepen.



The screenshot shows a web browser window with the title "Configuration | Interfaces" and the date "Friday, 27 October 2006". A "Save Needed" button is visible in the top right corner. The main content area contains the following text:

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

| 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. Voltooi deze stappen om Cisco Secure ACS voor Windows RADIUS-server toe te voegen aan de VPN 3000 Concentrator-configuratie. Kies **Configuratie > Systeem > Server > Verificatie** en klik op **Toevoegen** in het linkermenu.

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="*****"/> | Enter the RADIUS server secret. |
| Verify | <input type="text" value="*****"/> | Re-enter the secret. |
| <input type="button" value="Add"/> <input type="button" value="Cancel"/> | | |

Kies het servertype **RADIUS** en voeg deze parameters toe voor uw Cisco Secure ACS voor Windows RADIUS-server. Laat alle andere parameters in hun standaard toestand staan.**Verificatieserver**-Voer het IP-adres in van uw Cisco Secure ACS voor Windows RADIUS-server.**Beveiliging van de server**: Voer het RADIUS-servergeheim in. Dit moet het zelfde geheim zijn dat u gebruikt wanneer u de VPN 3000 Concentrator in Cisco Secure ACS voor de configuratie van Windows vormt.**Controleer** - voer het wachtwoord opnieuw in ter verificatie.Dit voegt de authenticatieserver toe in de mondiale configuratie van de VPN 3000 Concentrator. Deze server wordt gebruikt door alle groepen behalve wanneer een authenticatieserver specifiek is gedefinieerd. Als een authenticatieserver niet voor een groep is ingesteld, keert deze terug naar de globale authenticatieserver.

- Voltooi deze stappen om de tunnelgroep op de VPN 3000-centrator te configureren.Kies **Configuratie > Gebruikersbeheer > Groepen** in het linkermenu en klik op **Toevoegen**.Wijzig deze parameters in de tabbladen Configuration of voeg deze toe. Klik niet op Toepassen totdat u al deze parameters wijzigt:**Opmerking**: deze parameters zijn minimaal nodig voor VPN-verbindingen met externe toegang. Deze parameters veronderstellen ook de standaardinstellingen in de Base Group op de VPN 3000 Concentrator zijn niet gewijzigd.**Identiteit**

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. |

groepsnaam - Typ een groepsnaam. IPsec-gebruikers bijvoorbeeld. **Wachtwoord** - Voer een wachtwoord in voor de groep. Dit is de vooraf gedeelde sleutel voor de IKE-sessie. **Controleer** - voer het wachtwoord opnieuw in ter verificatie. **Type** - Laat dit standaard als volgt achter: 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 Associat |
| IKE Peer Identity Validation | <input type="text" value="If supported by certificate"/> | <input checked="" type="checkbox"/> | Select whether or not to validate the identit |
| 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 permitte 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. Up 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 membe apply to Individual User Authentication . |
| Authorization Type | <input type="text" value="None"/> | <input checked="" type="checkbox"/> | If members of this group need authorizatio authorization method. If you configure this f Server. |

Tunneltype - Kies **afstandsbediening**. **Verificatie**-RADIUS. Dit vertelt de VPN Concentrator welke methode je moet gebruiken om gebruikers voor authentiek te verklaren. **Modus configuratie**—Controleer **mode configuratie**. Klik op **Apply** (Toepassen).

- Voltooi deze stappen om meerdere verificatieservers te configureren op de VPN 3000-centrator. Zodra de groep is gedefinieerd, markeer deze groep en klik op **Verificatieservers** onder de kolom Wijzigen. Individuele verificatieservers kunnen voor elke groep worden gedefinieerd, zelfs indien deze servers niet in de mondiale servers bestaan.

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.

| Actions | Current Groups | Modify |
|--|------------------------------------|--|
| <input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/> | ipsecgroup (Internally Configured) | <input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/> |

Kies het servertype **RADIUS** en voeg deze parameters toe voor uw Cisco Secure ACS voor Windows RADIUS-server. Laat alle andere parameters in hun standaard toestand staan. **Verificatieserver**-Voer het IP-adres in van uw Cisco Secure ACS voor Windows RADIUS-server. **Beveiliging van de server**: Voer het RADIUS-servergeheim in. Dit moet het zelfde geheim zijn dat u gebruikt wanneer u de VPN 3000 Concentrator in Cisco Secure ACS voor de configuratie van Windows vormt. **Controleer** - voer het wachtwoord opnieuw in ter verificatie.

5. Kies **Configuratie > Systeem > Adres Management > Toewijzing** en controleer **het Adres van de Verificatieserver** om het IP-adres aan de VPN-clients toe te wijzen vanuit de IP-pool die in de RADIUS-server is gemaakt, zodra de client geauthentificeerd is.

Configuration | System | Address Management | Assignment

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.

[Configuratie van RADIUS-servers](#)

Dit deel van het document beschrijft de procedure die vereist is om Cisco Secure ACS als een RADIUS-server voor VPN-clientverificatie te configureren die door Cisco VPN 3000 Series

Concentrator - AAA-client wordt doorgestuurd.

Dubbelklik op het pictogram **ACS Admin** om de beheersessie op de PC te starten die de Cisco Secure ACS voor Windows RADIUS-server draait. Meld u indien nodig aan met de juiste gebruikersnaam en het juiste wachtwoord.

1. Voltooi deze stappen om de VPN 3000 Concentrator aan Cisco Secure ACS voor Windows serverconfiguratie toe te voegen. Kies **Network Configuration** en klik op **Add Entry** om een AAA-client aan de RADIUS-server toe te voegen.



The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, and Interface Configuration. The main area is titled 'Network Configuration' and has a 'Select' header. Below this is a table titled 'AAA Clients' with three columns: AAA Client Hostname, AAA Client IP Address, and Authenticate Using. The table contains 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) |

Voeg deze parameters toe voor uw VPN 3000 Concentrator:

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 | |

AAA-clientnaam - Voer de hostnaam van uw VPN 3000-centrator in (voor DNS-resolutie). **AAA client-IP-adres** Voer het IP-adres van uw VPN-Concentrator 3000 in. **Belangrijk** - Voer het RADIUS-servergeheim in. Dit moet hetzelfde geheim zijn dat u hebt ingesteld wanneer u de verificatieserver in de VPN-centrator hebt toegevoegd. **Verifieer het gebruik**-Kies **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**. Hiermee kunnen VPN 3000 VSA's in het venster voor groepsconfiguratie worden weergegeven. Klik op **Inzenden**. Kies **interfaceconfiguratie**, klik op **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** en controleer **groep [26] leverancierspecifieke**.

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

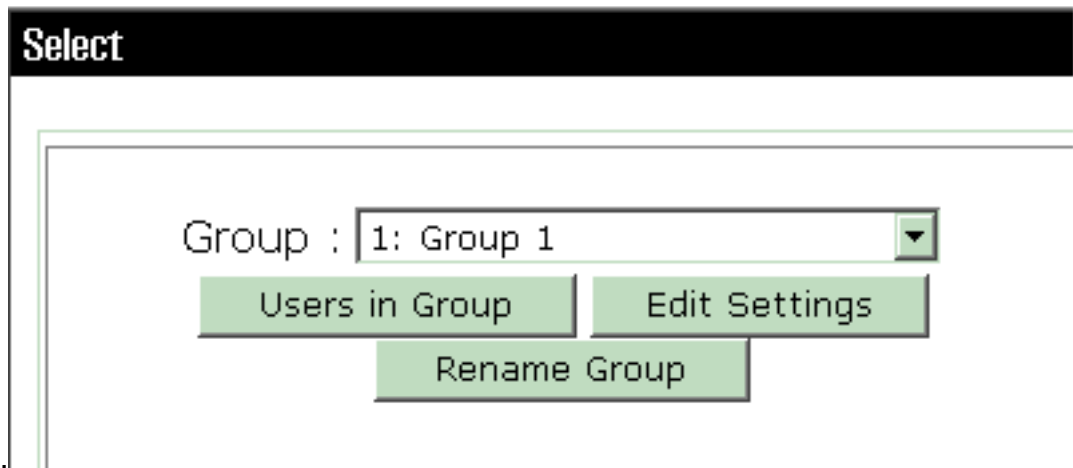
Submit

Cancel

Opmerking: 'RADIUS-kenmerk 26' heeft betrekking op alle specifieke eigenschappen van de verkoper. Kies bijvoorbeeld **Interface Configuration > RADIUS (Cisco VPN 3000)** en zie dat alle beschikbare eigenschappen beginnen met 206. Dit toont aan dat al deze verkoper-specifieke eigenschappen vallen onder de IETF RADIUS 26-standaard. Deze eigenschappen worden standaard niet weergegeven in door gebruiker of groep ingestelde instellingen. Om in de instelling van de Groep te verschijnen, kunt u een AAA-client maken (in dit geval VPN 3000 Concentrator) die voor authentiek is met RADIUS in de netwerkconfiguratie. Controleer vervolgens de eigenschappen die in de Instellingen gebruiker, Groepsinstelling of beide bij de interfaceconfiguratie moeten worden weergegeven. Raadpleeg [RADIUS-kenmerken](#) voor meer informatie over de beschikbare kenmerken en de manier waarop ze worden gebruikt. Klik op **Inzenden**.

2. Voltooi deze stappen om groepen aan de Cisco Secure ACS voor Windows-configuratie toe te voegen. Kies **Groepsinstelling**, selecteer vervolgens een van de sjabloon groepen, bijvoorbeeld groep 1, en klik op

Group Setup



Hernoemen.

V


erander de naam naar iets dat geschikt is voor uw organisatie. Bijvoorbeeld een deelgroep. Aangezien gebruikers aan deze groepen worden toegevoegd, maak de groepsnaam een weerspiegeling van het eigenlijke doel van die groep. Als alle gebruikers in dezelfde groep worden geplaatst, kunt u de VPN-gebruikersgroep bellen. Klik op **Instellingen bewerken** om de parameters te bewerken in de nieuwe

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)

groep.

Klik

op **Cisco VPN 3000 RADIUS** en stel deze aanbevolen eigenschappen in. Dit staat gebruikers toe die aan deze groep worden toegewezen om de eigenschappen van Cisco VPN 3000 RADIUS te erven, die u staat om beleid voor alle gebruikers in Cisco Secure ACS voor Windows te centraliseren.

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

Opmerking:

Technisch gezien hoeven VPN 3000 RADIUS-kenmerken niet te worden geconfigureerd zolang de Tunnelgroep is ingesteld in stap 3 van de [VPN 3000 Series Concentrator-configuratie](#) en de Base Group in VPN Concentrator verandert niet van de oorspronkelijke standaardinstellingen. **Aanbevolen VPN 3000-kenmerken:** **Primair-DNS**-Voer het IP-adres van uw primaire DNS-server in. **Secundair-DNS**-Voer het IP-adres van uw secundaire DNS-server in. **Primair WINS**-Voer het IP-adres in van de primaire WINS-server. **Secundaire WINS** - Voer het IP-adres van de Secundaire WINS-server in. **Tunneling-protocollen**—Kies **IPsec**. Dit staat *alleen* IPsec client verbindingen toe. PPTP of L2TP zijn niet toegestaan. **IPsec-Sec-Association**—Voer **ESP-3DES-MD5** in. Dit garandeert dat al uw IPsec-clients worden aangesloten op de hoogste beschikbare encryptie. **IPsec-toestaan-Wachtwoord-opslaan**-kiezen **Onthouden** zodat gebruikers *hun wachtwoord niet* in de VPN-client mogen opslaan. **IPsec-banner**-Voer een welkome berichtbanner in die bij verbinding aan de gebruiker moet worden aangeboden. Bijvoorbeeld, "Welkom bij MyCompany werknemer VPN toegang!" **IPsec-standaard-domein** - Voer de domeinnaam van uw bedrijf in. Bijvoorbeeld "mycompany.com". Deze reeks eigenschappen is niet nodig. Maar als u niet

zeker bent of de eigenschappen van de Base Group van de VPN 3000 Concentrator zijn gewijzigd, raadt Cisco u aan deze eigenschappen te configureren: **Gelijktijdig registreren** - Voer het aantal keer in dat u een gebruiker toestaat om tegelijkertijd in te loggen met dezelfde gebruikersnaam. De aanbeveling is 1 of 2. **SEP-kaart-toewijzing** - Kies **Any-SEP**. **IPsec-mode-configuratie**—Kies **ON**. **IPsec over UDP**-Kies **OFF**, tenzij u wilt dat gebruikers in deze groep een verbinding maken met IPsec via het UDP-protocol. Als u **ON** selecteert, heeft de VPN-client nog de mogelijkheid om IPsec lokaal uit te schakelen via UDP en normaal te verbinden. **IPsec over UDP Port**-Selecteer een UDP-poortnummer in het bereik van 4001 tot en met 4915. Dit wordt alleen gebruikt als IPsec over UDP is ingeschakeld. De volgende reeks eigenschappen vereist dat u eerst iets op de VPN Concentrator instelt voordat u ze kunt gebruiken. Dit wordt alleen aanbevolen voor geavanceerde gebruikers. **Access-uren** - Dit vereist dat u een verscheidenheid aan toegangsuren op de VPN 3000 Concentrator instelt onder **Configuratie > Beleidsbeheer**. Gebruik in plaats daarvan de uren van de Toegang die in Cisco Secure ACS voor Windows beschikbaar zijn om deze eigenschap te beheren. **IPsec-splitter-tunnellijst** - Dit vereist dat u een netwerklijst op de VPN-Concentrator instelt onder **Configuration > Policy Management > Traffic Management**. Dit is een lijst van netwerken die naar de client worden verstuurd die de client vertellen om gegevens te versleutelen naar alleen die netwerken in de lijst. Kies **IP-toewijzing in groepsinstellingen** en controleer **Toegewezen op AAA server Pool** om de IP-adressen aan VPN-clientgebruikers toe te wijzen wanneer ze echt zijn

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

bevonden.


Kie

s de **systemconfiguratie > IP-pools** om een IP-pool voor VPN-clientgebruikers te maken en

klik op

System Configuration

Edit

| New Pool | |  |
|---------------|--|---|
| Name | <input type="text" value="pool1"/> | |
| Start Address | <input type="text" value="10.1.1.1"/> | |
| End Address | <input type="text" value="10.1.1.10"/> | |


Submit

Cancel

Indienen.

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% | |

Kies Indienen

- > **Opnieuw beginnen** om de configuratie op te slaan en de nieuwe groep te activeren. Herhaal deze stappen om meer groepen toe te voegen.
3. **Configureer gebruikers op Cisco Secure ACS voor Windows.** Klik op **Gebruikersinstelling**, voer een gebruikersnaam in en klik op **Toevoegen/Bewerken**.

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


Configureer deze

parameters in het vak
gebruikersinstelling:

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:



Wachtwoordverificatie - Kies ACS interne database. **Cisco Secure PP - Wachtwoord** - Voer een wachtwoord in voor de gebruiker. **Cisco Secure PP - Wachtwoord bevestigen** - voer het wachtwoord voor de nieuwe gebruiker opnieuw in. **Groep waaraan de gebruiker is toegewezen** - Selecteer de naam van de groep die u in de vorige stap hebt gemaakt. Klik op **Inzenden** om de gebruikersinstellingen op te slaan en te activeren. Herhaal deze stappen om extra gebruikers toe te voegen.

[Een statisch IP-adres aan de VPN-clientgebruiker toewijzen](#)

Voer de volgende stappen uit:

1. Maak een nieuwe VPN-groep IPSECGRP.
2. Maak een gebruiker die het statische IP wil ontvangen en kies **IPSECTOR**. Kies een **statisch IP-adres** aan het statische IP-adres toewijzen dat onder de Clientfunctie voor IP-adres wordt toegewezen.

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

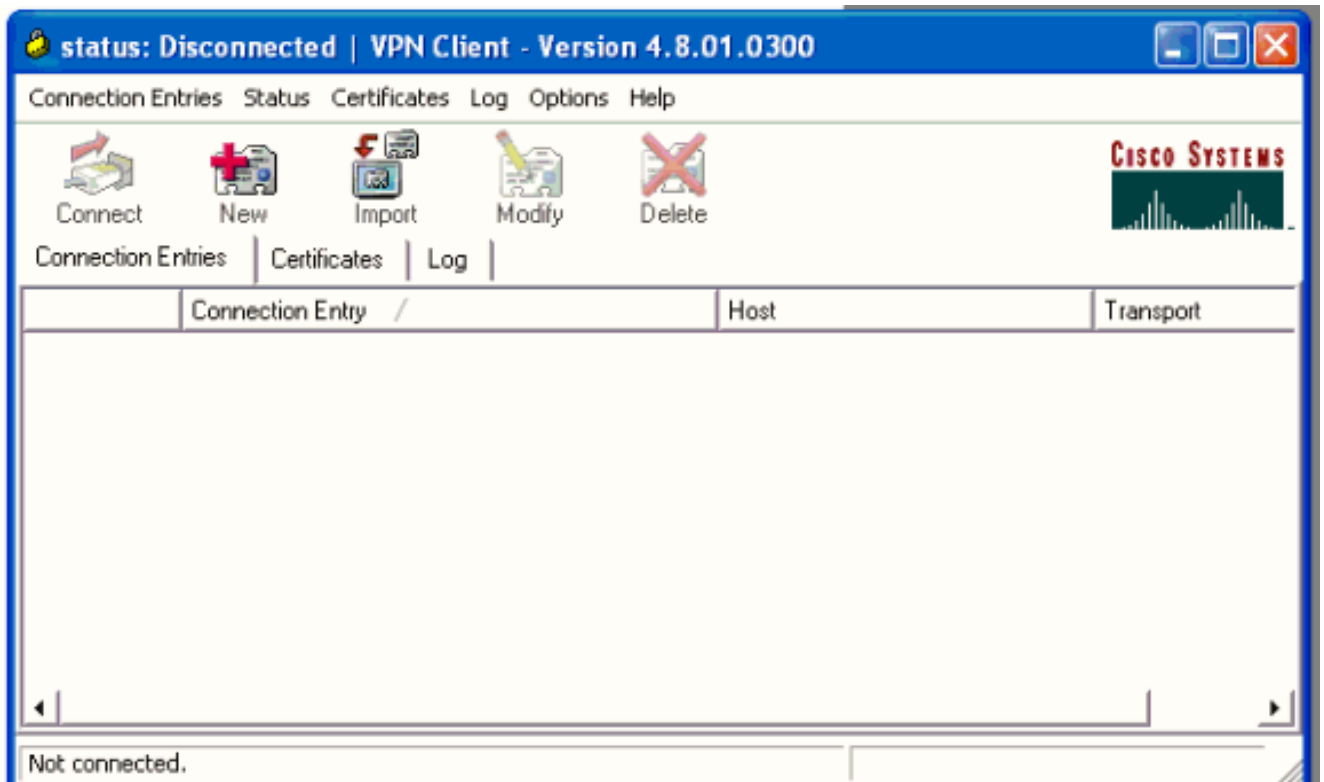
Submit

Delete

Cancel

In deze sectie worden de VPN-clientsconfiguratie beschreven.

1. Kies **Start > Programma's > Cisco Systems VPN-client > VPN-client**.
2. Klik op **Nieuw** om het venster Nieuwe VPN-verbinding maken te starten.



3. Wanneer gevraagd wordt, voer een naam voor uw ingang toe. U kunt desgewenst ook een beschrijving invoeren. Specificeer het VPN 3000 Concentrator openbare IP-adres in de kolom Host en kies **Group Verificatie**. Typ vervolgens de groepsnaam en het wachtwoord. Klik op **Opslaan** om de nieuwe VPN-verbinding te

VPN Client | Create New VPN Connection Entry

Connection Entry: vpnuser

Description: Headoffice

Host: 10.0.0.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name: ipsecgroup

Password: *****

Confirm Password: *****

Certificate Authentication

Name: [dropdown]

Send CA Certificate Chain

Erase User Password | Save | Cancel

voltooien.

.B.: Zorg ervoor dat de VPN-client is geconfigureerd voor gebruik van dezelfde groepsnaam en wachtwoord in Cisco VPN 3000 Series Concentrator.

[Voeg accounting toe](#)

Nadat de authenticatie werkt, kunt u accounting toevoegen.

1. Kies in VPN 3000 **Configuration > System > Server > Accounting Server** en voeg **Cisco Secure ACS toe voor Windows-server**.
2. U kunt afzonderlijke accounting servers aan elke groep toevoegen als u **Configuratie > Gebruikersbeheer > Groepen** kiest, een groep markeert en op **Wijzigen** klikt. **servers**. Voer vervolgens het IP-adres van de boekhoudserver in met het servergeheim.

Configure and add a RADIUS user accounting server.

| | | |
|--------------------------|---|---------------------------------------|
| Accounting Server | <input type="text" value="172.16.124.5"/> | Enter IP address or hostname. |
| Server Port | <input type="text" value="1646"/> | Enter the server UDP port number. |
| Timeout | <input type="text" value="1"/> | Enter the timeout for this server (se |
| Retries | <input type="text" value="3"/> | Enter the number of retries for this |
| Server Secret | <input type="password" value="*****"/> | Enter the RADIUS server secret. |
| Verify | <input type="password" value="*****"/> | Re-enter the server secret. |

In Cisco Secure ACS voor Windows verschijnen de accounting records zoals deze uitvoer toont:

Select

RADIUS Accounting active.csv

Regular Expression: Start Date & Time: End Date & Time: Rows per Page:

Filtering is not applied.

| Date | Time | User-Name | Group-Name | Calling-Station-Id | Acct-Status-Type | Acct-Session-Id | Acct-Session-Time | Service-Type | Framed-Protocol | Acct-Input-Octets | Acct-Output-Octets | Acct-Input-Packets | Acct-Output-Packets |
|------------|----------|-----------------------|---------------|--------------------|------------------|-----------------|-------------------|--------------|-----------------|-------------------|--------------------|--------------------|---------------------|
| 10/27/2006 | 18:38:20 | ipseuser1 | ipsecgroup | 192.168.1.2 | Start | E8700001 | .. | Framed | PPP | .. | .. | .. | .. |
| 10/27/2006 | 18:38:20 | VPN 3000 Concentrator | Default Group | .. | Accounting On | .. | .. | .. | .. | .. | .. | .. | .. |
| 10/27/2006 | 13:17:10 | VPN 3000 Concentrator | Default Group | .. | Accounting Off | .. | .. | .. | .. | .. | .. | .. | .. |

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het [Uitvoer Tolk](#) (uitsluitend geregistreeerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Controleer de VPN-concentratie

Kies aan de kant VPN 3000 Concentrator **Administratie > Sessies beheren** om de externe VPN-tunnelvestiging te controleren.

Remote Access Sessions

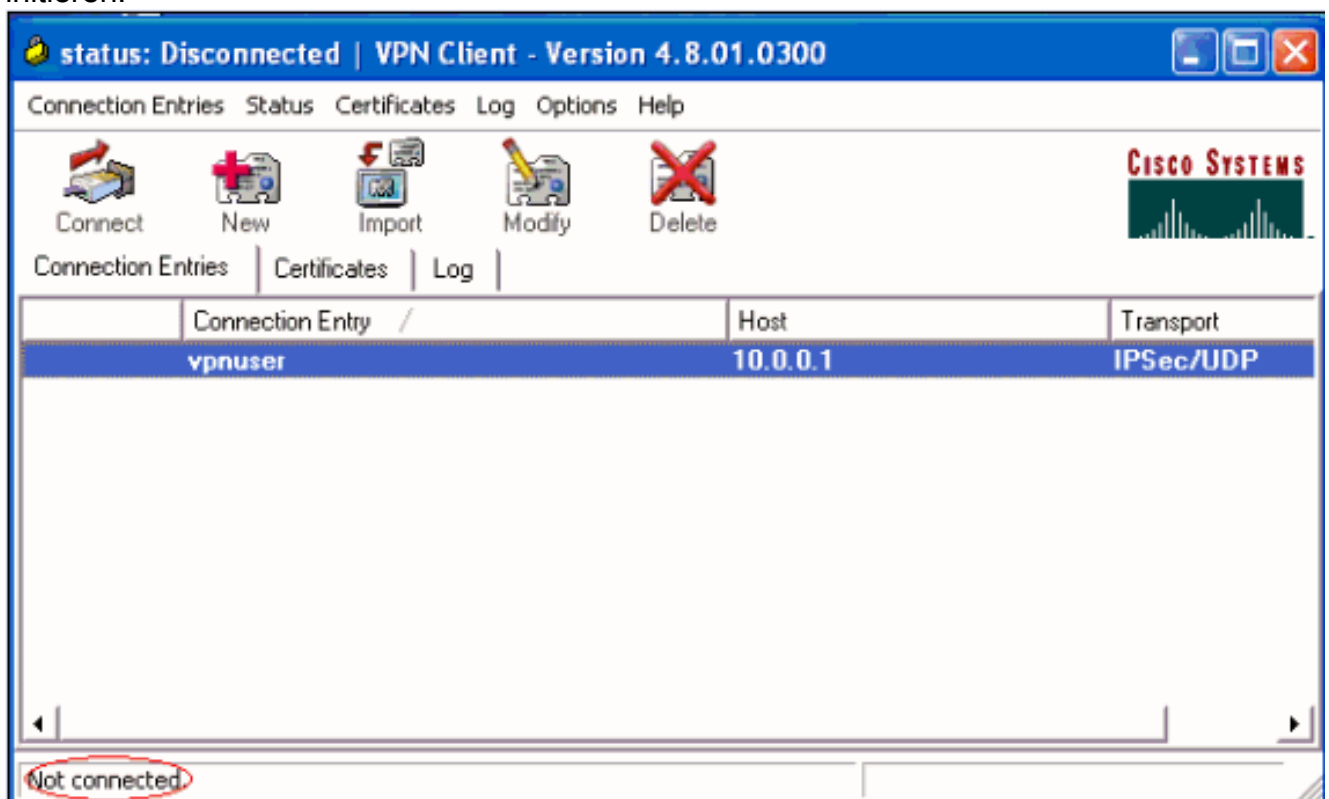
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

| Username | Assigned IP Address Public IP Address | Group | Protocol Encryption | Login Time Duration | Client Type Version | Bytes Tx Bytes Rx | NAC Result Posture Token | Actions |
|----------------------------|--|-----------------------|-------------------------------------|-------------------------------------|-------------------------------------|--|--|---|
| 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] |

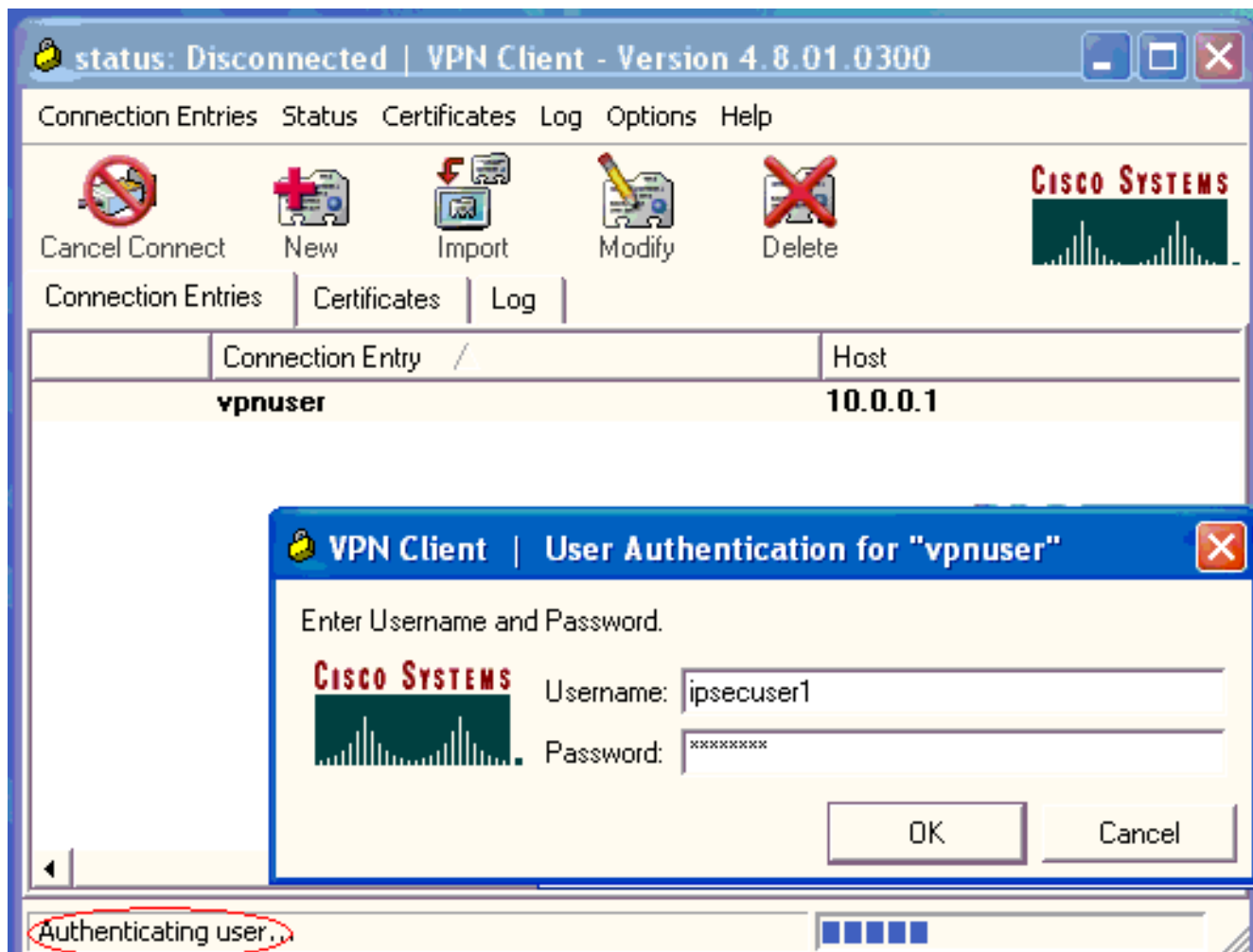
[Controleer de VPN-client](#)

Voltooi deze stappen om de VPN-client te controleren.

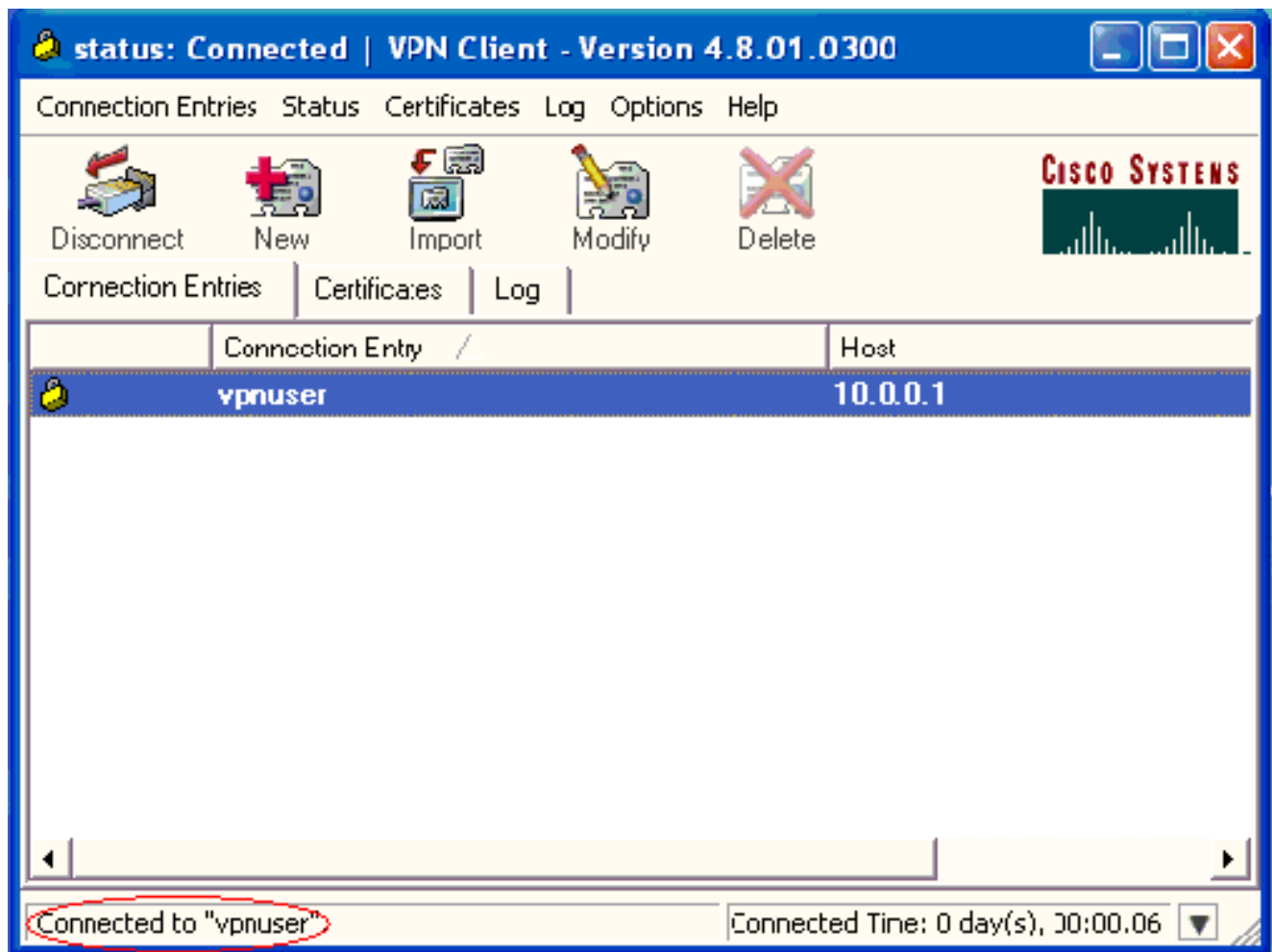
1. Klik op **Connect** om een VPN-verbinding te initiëren.



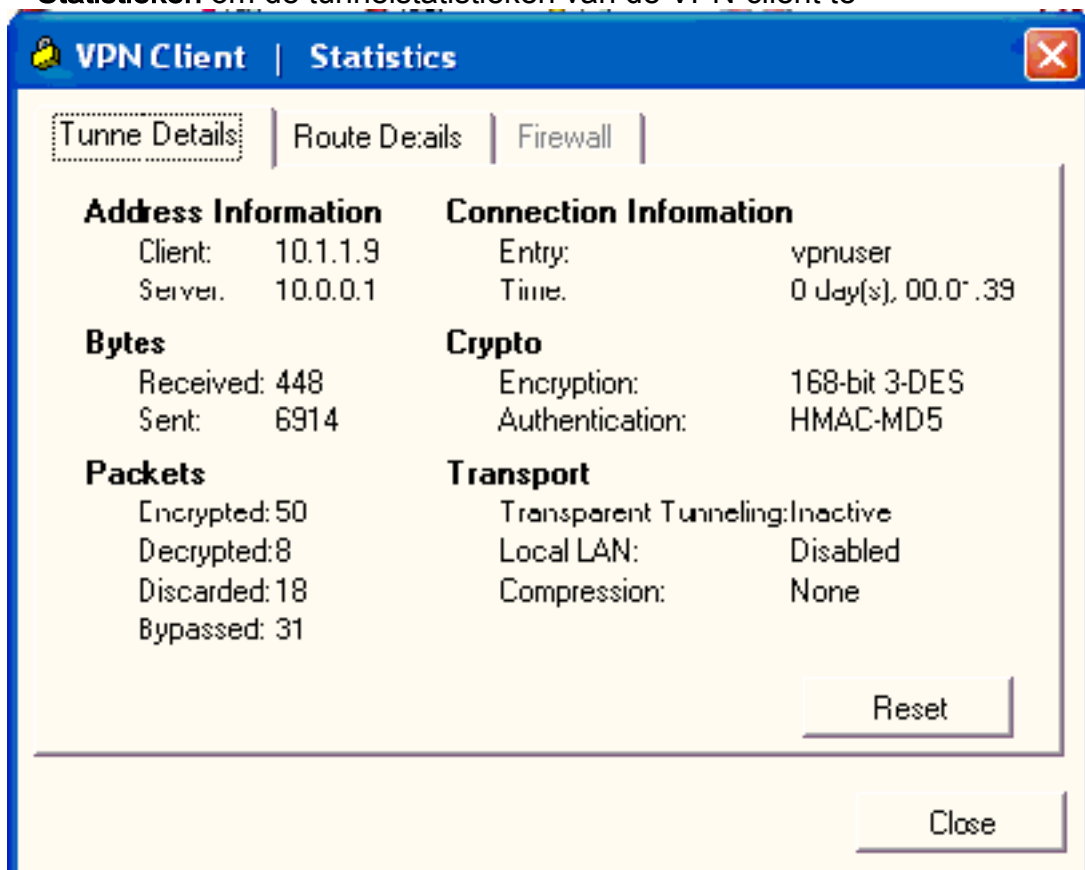
2. Dit venster verschijnt voor gebruikersverificatie. Voer een geldige naam en wachtwoord in om de VPN-verbinding op te zetten.



3. De VPN-client wordt aangesloten op de VPN 3000 Concentrator op de centrale site.



4. Kies **Status > Statistieken** om de tunnelstatistieken van de VPN-client te



controleren.

[Problemen oplossen](#)

Voltooi deze stappen om problemen met de configuratie op te lossen.

1. Kies **Configuratie > Systeem > Server > Verificatie** en voltooi deze stappen om de connectiviteit tussen de RADIUS-server en de VPN 3000 Concentrator te testen. Selecteer uw server en klik vervolgens op **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"/> |

Voer de gebruikersnaam en het wachtwoord van de RADIUS in en klik op **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

Een succesvolle authenticatie lijkt te bestaan.

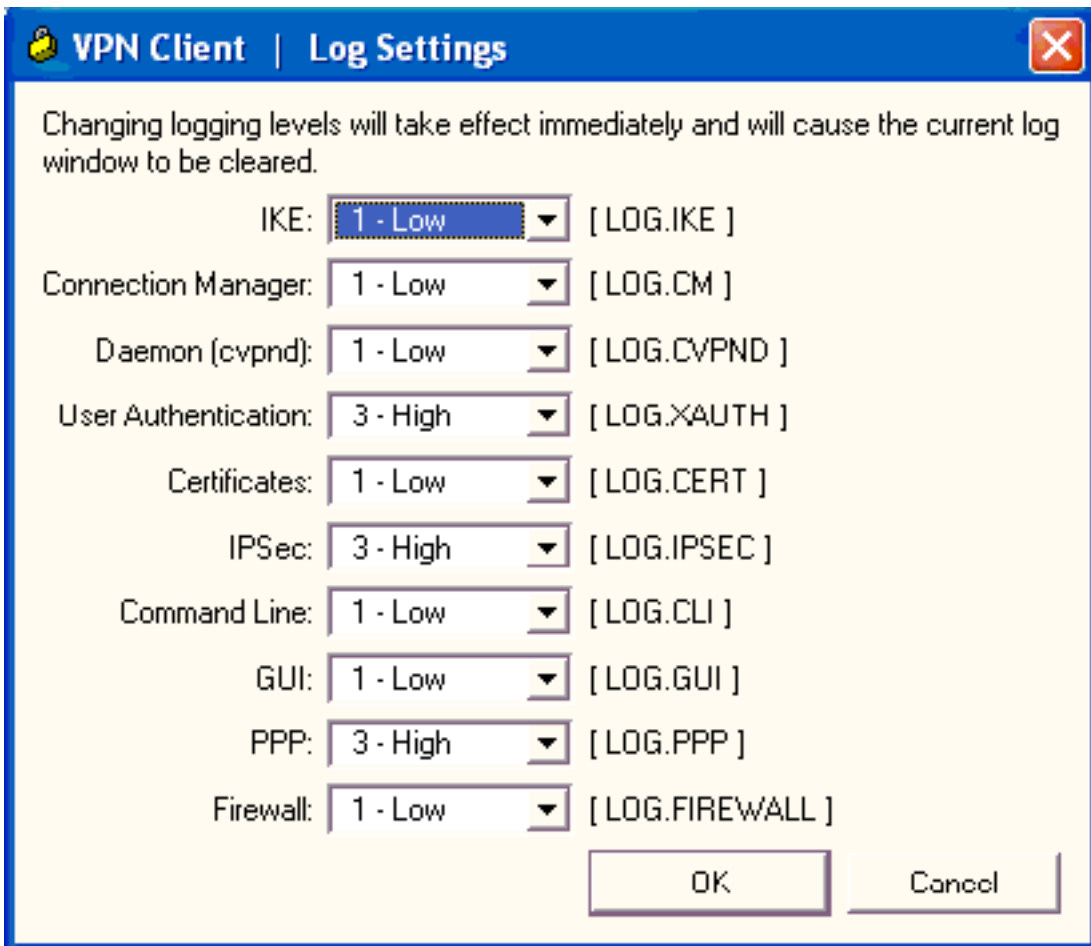
- Als het mislukt, is er een configuratieprobleem of een IP-connectiviteit-probleem. Controleer de mislukte pogingen om op de ACS-server in te loggen op berichten met betrekking tot de fout. Als er geen berichten in dit logbestand verschijnen is er waarschijnlijk een probleem met IP-connectiviteit. Het RADIUS-verzoek bereikt de RADIUS-server niet. Controleer de filters die worden toegepast op de juiste VPN 3000 Concentrator-interface om RADIUS (1645)-pakketten in en uit toe te staan. Als de testverificatie geslaagd is, maar de logins bij de VPN 3000 Concentrator blijven mislukken, controleert u het logbestand van gebeurtenis voor filtering via de console-poort. Als de verbindingen niet werken, kunt u AUTH-, IKE- en IPsec-eventklassen toevoegen aan VPN Concentrator wanneer u **Configuration > System > Events > Classes > Change (Severity to Log=1-9, Severity to Console=1-3)** selecteert. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG en IPSECDECODE zijn ook beschikbaar, maar kunnen te veel informatie verstrekken. Indien gedetailleerde informatie nodig is over de kenmerken die worden doorgegeven van de RADIUS-server, geven AUTHDECODE, IKEDECODE en IPSECDECODE dit aan op het niveau Severity to Log=1-13.
- Het logbestand van de gebeurtenis terughalen uit **Monitoring > Event Log**.



[Probleemoplossing VPN-client 4.8 voor Windows](#)

Voltooi deze stappen om een oplossing te vinden voor VPN-client 4.8 voor Windows.

- Kies de instellingen voor **Log > Log** om de logniveaus in de VPN-client in te



schakelen.

2. Kies **Log > venster in** om de logitems in de VPN-client te bekijken.

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

[Gerelateerde informatie](#)

- [Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina](#)
- [Cisco VPN-clientondersteuningspagina](#)
- [IPsec-onderhandeling/IKE-protocollen](#)
- [Cisco Secure ACS voor Windows-ondersteuningspagina](#)
- [Dynamische filters op een RADIUS-server configureren](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)