

# Connectiviteit van AnyConnect VPN (virtueel particulier netwerk) op de RV34x Series router configureren

## Doel

In dit document wordt beschreven hoe u AnyConnect VPN-connectiviteit configureert op de RV34x Series router.

## Voordelen van het gebruik van AnyConnect Secure Mobility Client:

1. Beveiligde en permanente connectiviteit
2. Blijvende veiligheid en beleidshandhaving
3. Uitbreidbaar vanaf de adaptieve security applicatie (ASA) of vanaf Enterprise Software Implementation Systems
4. Aanpasbaar en vertaalbaar
5. Eenvoudig geconfigureerd
6. Ondersteunt zowel Internet Protocol Security (IPSec) als Secure Sockets Layer (SSL)
7. Ondersteuning van Internet Key Exchange versie 2.0 (IKEv2.0) protocol

## Inleiding

Een Virtual Private Network (VPN)-verbinding stelt gebruikers in staat om toegang te krijgen tot, gegevens te verzenden en te ontvangen van en naar een privaat netwerk door middel van het doorlopen van een openbaar of gedeeld netwerk zoals het internet, maar nog steeds veilige verbindingen te verzekeren met een onderliggende netwerkinfrastructuur om het privaat netwerk en zijn bronnen te beschermen.

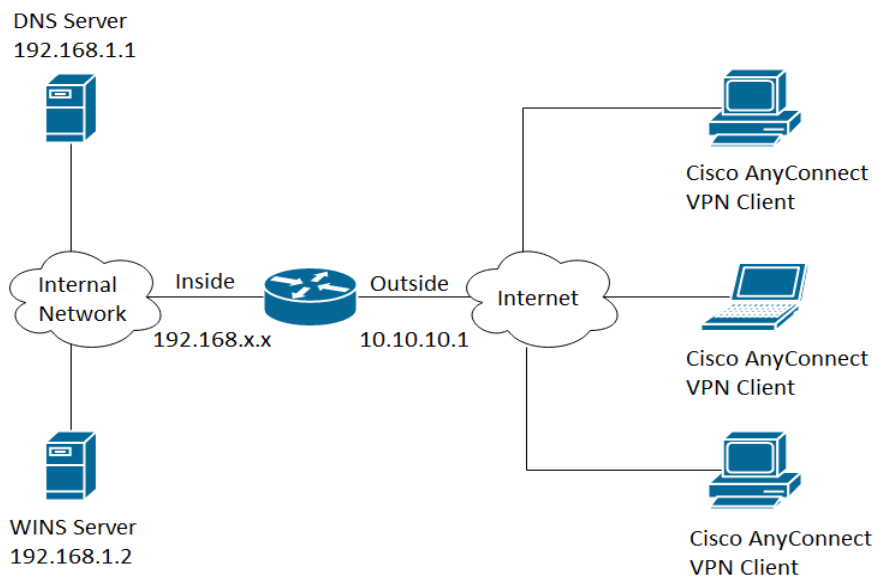
Een VPN-client is software die is geïnstalleerd en wordt uitgevoerd op een computer die verbinding wil maken met het externe netwerk. Deze clientsoftware moet worden ingesteld met dezelfde configuratie als de VPN-server, zoals het IP-adres en de verificatie-informatie. Deze verificatieinformatie bevat de gebruikersnaam en de vooraf gedeelde sleutel die worden gebruikt om de gegevens te versleutelen. Afhankelijk van de fysieke locatie van de netwerken die moeten worden aangesloten, kan een VPN-client ook een hardwareapparaat zijn. Dit gebeurt meestal als de VPN-verbinding wordt gebruikt om twee netwerken aan te sluiten die zich op verschillende locaties bevinden.

De Cisco AnyConnect Secure Mobility Client is een softwaretoepassing voor de aansluiting op een VPN-router die op verschillende besturingssystemen en hardwareconfiguraties werkt. Deze softwaretoepassing maakt het mogelijk dat externe bronnen van een ander netwerk toegankelijk worden alsof de gebruiker direct op zijn netwerk is aangesloten, maar op een veilige manier. Cisco AnyConnect Secure Mobility Client biedt een innovatieve nieuwe manier om mobiele gebruikers te beschermen op computergebaseerde of smartphoneplatforms, en biedt een naadloze, altijd beschermde ervaring voor eindgebruikers en uitgebreide beleidshandhaving voor IT-beheerders.

Op de RV34x router, te beginnen met firmware versie 1.0.3.15 en vooruit te gaan, is AnyConnect-licentie niet nodig. Er worden alleen kosten in rekening gebracht voor clientlicenties.

Raadpleeg het artikel over [AnyConnect-licenties voor de RV340 Series routers voor](#) meer

informatie over AnyConnect-[licenties voor de RV340 Series routers](#).



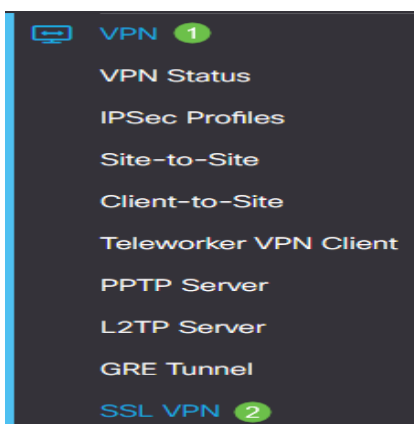
## Toepasselijke apparaten | Firmwareversie

- Cisco AnyConnect Secure Mobility Client | 4.4 ([meest recente versie downloaden](#))
- RV340x Series | 1.0.03.15 ([Download nieuwste release](#))

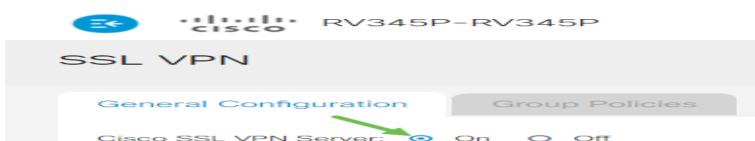
## AnyConnect VPN-connectiviteit configureren op de RV34x

### SSL VPN op de RV34x configureren

Stap 1. Open het router webgebaseerde hulpprogramma en kies **VPN > SSL VPN**.



Stap 2. Klik op de knop **Aan** om Cisco SSL VPN Server in te schakelen.



### Verplichte gateway-instellingen

De volgende configuratie-instellingen zijn verplicht:

Stap 3. Kies de Gateway-interface in de vervolgkeuzelijst. Dit is de poort die wordt gebruikt voor

het doorgeven van verkeer via de SSL VPN-tunnels. De opties zijn:

- WAN1
- WAN2
- USB 1
- USB 2

## Mandatory Gateway Settings

Gateway Interface:

**Opmerking:** in dit voorbeeld is WAN1 geselecteerd.

Stap 4. Voer het poortnummer in dat wordt gebruikt voor de SSL VPN-gateway in het veld *Gateway Port (Gateway Port)* van 1 tot 65535.

Gateway Interface:

Gateway Port:  (Range: 1-65535)

**Opmerking:** in dit voorbeeld wordt 8443 gebruikt als poortnummer.

Stap 5. Kies het certificaatbestand in de vervolgkeuzelijst. Dit certificaat verifieert gebruikers die proberen toegang te krijgen tot de netwerkbron via de SSL VPN-tunnels. De vervolgkeuzelijst bevat een standaardcertificaat en de certificaten die worden geïmporteerd.

Certificate File:

**Opmerking:** in dit voorbeeld is Default geselecteerd.

Stap 6. Voer in het veld *Clientadresgroep* het IP-adres van de clientadresgroep in. Deze pool is de reeks IP-adressen die worden toegewezen aan externe VPN-clients.

**N.B.:** Zorg ervoor dat het IP-adresbereik niet overlapt met IP-adressen in het lokale netwerk.

Client Address Pool: 192.168.0.0

**Opmerking:** in dit voorbeeld wordt 192.168.0.0 gebruikt.

Stap 7. Kies het Client Netmasker in de vervolgkeuzelijst.

Client Netmask: 255.255.255.0

**Opmerking:** in dit voorbeeld is 255.255.255.128 geselecteerd.

Stap 8. Voer in het veld *Clientdomein* de domeinnaam client in. Dit zal de domeinnaam zijn die naar SSL VPN-clients moet worden gedrukt.

Client Domain: WideDomain.com

**Opmerking:** in dit voorbeeld wordt WideDomain.com gebruikt als de client domeinnaam.

Stap 9. Voer de tekst in die als inlogbanner wordt weergegeven in het veld *Login Banner*. Dit wordt de banner die wordt weergegeven telkens wanneer een client zich aanmeldt.

## Mandatory Gateway Settings

Gateway Interface:	<input type="text" value="WAN1"/>
Gateway Port:	<input type="text" value="8443"/>
Certificate File:	<input type="text" value="Default"/>
Client Address Pool:	<input type="text" value="192.168.0.0"/>
Client Netmask:	<input type="text" value="255.255.255.0"/>
Client Domain:	<input type="text" value="yourdomain.com"/>
Login Banner:	<input type="text" value="Welcome to WideDomain!"/>

**Opmerking:** In dit voorbeeld wordt Welkom bij Widedomain! gebruikt als de Login Banner.

## Optionele gateway-instellingen

De volgende configuratie-instellingen zijn optioneel:

Stap 1. Voer een waarde in seconden in voor de tijdelijke versie van de inactiviteitstimer, gaande van 60 tot 86400. Dit is de tijdsduur gedurende welke de SSL VPN sessie inactief kan blijven.

### Optional Gateway Settings

Idle Timeout:  sec. (Range: 60-86400)

**Opmerking:** in dit voorbeeld wordt 3000 gebruikt.

Stap 2. Voer in het veld *Time-out sessie* een waarde in in seconden. Dit is de tijd die nodig is voor de TCP- (Transmission Control Protocol) of UDP-sessie (User Datagram Protocol) voor een time-out na de opgegeven inactiviteitstijd. Het bereik loopt van 60 tot 1209600.

### Optional Gateway Settings

Idle Timeout:  sec. (Range: 60-86400)  
Session Timeout:  sec. (Range: 0,60-1209600)

**Opmerking:** in dit voorbeeld wordt 60 gebruikt.

Stap 3. Voer in het veld *ClientDPD Time-out* een waarde in in seconden gaande van 0 tot 3600. Deze waarde specificeert het periodieke verzenden van HELLO/ACK-berichten om de status van de VPN-tunnel te controleren.

**Opmerking:** deze optie moet op beide uiteinden van de VPN-tunnel zijn ingeschakeld.

### Optional Gateway Settings

Idle Timeout:  sec. (Range: 60-86400)  
Session Timeout:  sec. (Range: 0,60-1209600)  
Client DPD Timeout:  sec. (Range: 0-3600)

**Opmerking:** in dit voorbeeld wordt 350 gebruikt.

Stap 4. Voer in het veld *GatewayDPD Time-out* een waarde in in seconden gaande van 0 tot 3600. Deze waarde specificeert het periodieke verzenden van HELLO/ACK-berichten om de status van de VPN-tunnel te controleren.

**Opmerking:** deze optie moet op beide uiteinden van de VPN-tunnel zijn ingeschakeld.

### Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)

**Opmerking:** in dit voorbeeld wordt 360 gebruikt.

Stap 5. Voer in het veld *Levend behouden* een waarde in in van 0 tot 600 seconden. Deze eigenschap zorgt ervoor dat uw router altijd met Internet wordt verbonden. Het zal proberen om de VPN verbinding te herstellen als deze wordt verbroken.

### Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)

**Opmerking:** in dit voorbeeld wordt 40 gebruikt.

Stap 6. Voer een waarde in in seconden voor de duur van de tunnel die moet worden aangesloten in het veld *Looptijd*. Het bereik loopt van 600 tot 1209600.

### Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)
Lease Duration:	<input type="text" value="43500"/>	sec. (Range: 600-1209600)

**Opmerking:** in dit voorbeeld wordt 43500 gebruikt.

Stap 7. Geef de pakketgrootte op in bytes die over het netwerk kunnen worden verzonden. Het bereik loopt van 576 tot 1406.

## Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)
Lease Duration:	<input type="text" value="43500"/>	sec. (Range: 600-1209600)
Max MTU:	<input type="text" value="1406"/>	bytes (Range: 576-1406)

**Opmerking:** in dit voorbeeld is 1406 gebruikt.

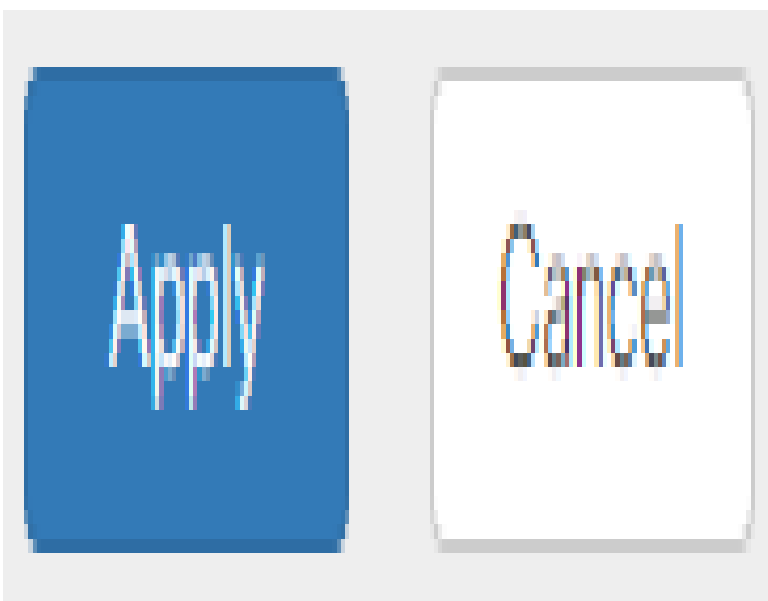
Stap 8. Voer in het veld *Rekey Interval* de Relay-intervaltijd in. Met de functie Rekey kunnen de SSL-toetsen opnieuw onderhandelen nadat de sessie is ingesteld. Het bereik loopt van 0 tot 43200.

## Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)
Lease Duration:	<input type="text" value="43500"/>	sec. (Range: 600-1209600)
Max MTU:	<input type="text" value="1406"/>	bytes (Range: 576-1406)
Rekey Interval:	<input type="text" value="3600"/>	sec. (Range: 0-43200)

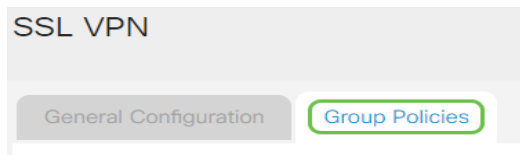
**Opmerking:** in dit voorbeeld wordt 3600 gebruikt.

Stap 9. Klik op **Apply** (Toepassen).

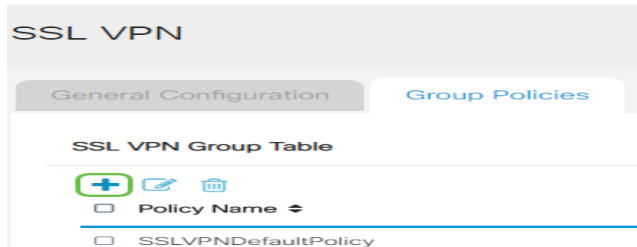


## Groepsbeleid configureren

Stap 1. Klik op het tabblad **Groepsbeleid**.



Stap 2. Klik op de knop **Add** onder de SSL VPN Group Table om een groepsbeleid toe te voegen.



**Opmerking:** de SSL VPN Group tabel toont de lijst met groepsbeleid op het apparaat. U kunt ook het eerste groepsbeleid bewerken in de lijst, die SLVPNDefaultPolicy wordt genoemd. Dit is het standaardbeleid dat door het apparaat wordt geleverd.

Stap 3. Voer in het veld *Beleidsnaam* uw voorkeursnaam in.

### SSLVPN Group Policy - Add/Edit

#### Basic Settings

Policy Name:

Primary DNS:

**Opmerking:** in dit voorbeeld wordt het beleid van groep 1 gebruikt.

Stap 4. Voer in het daarvoor bestemde veld het IP-adres van de primaire DNS in. Standaard is dit IP-adres al meegeleverd.



## SSLVPN Group Policy - Add/Edit

### Basic Settings

Policy Name:

Primary DNS:

**Opmerking:** in dit voorbeeld wordt 192.168.1.1 gebruikt.

Stap 5. (Optioneel) Voer in het daarvoor bestemde veld het IP-adres van de secundaire DNS in. Dit zal dienen als een back-up voor het geval dat de primaire DNS mislukt.

## SSLVPN Group Policy - Add/Edit

### Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

**Opmerking:** in dit voorbeeld wordt 192.168.1.2 gebruikt.

Stap 6. (Optioneel) Voer in het daarvoor bestemde veld het IP-adres in van de primaire WINS.

## SSLVPN Group Policy - Add/Edit

### Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

**Opmerking:** in dit voorbeeld wordt 192.168.1.1 gebruikt.

Stap 7. (Optioneel) Voer in het daarvoor bestemde veld het IP-adres in van de secundaire WINS.

## SSLVPN Group Policy - Add/Edit

### Basic Settings

Policy Name:	<input type="text" value="Group1Policy"/>
Primary DNS:	<input type="text" value="192.168.1.1"/>
Secondary DNS:	<input type="text" value="192.168.1.2"/>
Primary WINS:	<input type="text" value="192.168.1.1"/>
Secondary WINS:	<input type="text" value="192.168.1.2"/>

**Opmerking:** in dit voorbeeld wordt 192.168.1.2 gebruikt.

Stap 8. (Optioneel) Voer een beschrijving van het beleid in het veld *Description* in.

## SSLVPN Group Policy - Add/Edit

### Basic Settings

Policy Name:	<input type="text" value="Group 1 Policy"/>
Primary DNS:	<input type="text" value="192.168.1.1"/>
Secondary DNS:	<input type="text" value="192.168.1.2"/>
Primary WINS:	<input type="text" value="192.168.1.1"/>
Secondary WINS:	<input type="text" value="192.168.1.2"/>
Description:	<input type="text" value="Group policy with split tunnel"/>

**Opmerking:** in dit voorbeeld wordt groepsbeleid met gesplitste tunnel gebruikt.

Stap 9. (Optioneel) Klik op een radioknop om het IE Proxy-beleid te kiezen om Microsoft Internet Explorer (MSIE) proxy-instellingen in te schakelen om een VPN-tunnel tot stand te brengen. De opties zijn:

- Geen - staat de browser toe om geen proxyinstellingen te gebruiken.
- Auto - hiermee kan de browser automatisch de proxyinstellingen detecteren.
- Bypass-Local - Hiermee kan de browser de proxyinstellingen omzeilen die op de externe gebruiker zijn ingesteld.
- Uitgeschakeld - Schakelt de MSIE-proxyinstellingen uit.

### IE Proxy Settings

IE Proxy Policy:  None  Auto  Bypass-local  Disabled

**Opmerking:** in dit voorbeeld is de optie Uitgeschakeld geselecteerd. Dit is de standaardinstelling.

Stap 10. (Optioneel) In het gebied Split-tunnelinstellingen vinkt u het aanvinkvakje **Enable Split Tunneling** in om toe te staan dat voor internet bestemd verkeer zonder encryptie rechtstreeks naar internet wordt verzonden. Full Tunneling verstuurt al het verkeer naar het eindapparaat waar het vervolgens wordt verstuurd naar doelbronnen, waardoor het bedrijfsnetwerk van het pad voor

webtoegang wordt geëlimineerd.

# Split Tunneling Settings

Enable Split Tunneling

Stap 1. (Optioneel) Klik op een radioknop om te kiezen of u verkeer wilt opnemen of uitsluiten bij het toepassen van de gesplitste tunneling.

## Split Tunneling Settings

1  Enable Split Tunneling

2  Include Traffic  Exclude Traffic

Split Selection

**Opmerking:** in dit voorbeeld Omvat Traffic is geselecteerd.

Stap 12. Klik in de tabel Splitsen op de knop **Toevoegen** om een uitzondering voor gesplitste netwerken toe te voegen.

## Split Network Table



Stap 13. Voer in het daarvoor bestemde veld het IP-adres van het netwerk in.

## Split Tunneling Settings

Enable Split Tunneling

Split Selection  Include Traffic  Exclude Traffic

Split Network Table

+ ✎ 🗑️

IP ↕

<input checked="" type="checkbox"/> 192.168.1.0
---

**Opmerking:** in dit voorbeeld wordt 192.168.1.0 gebruikt.

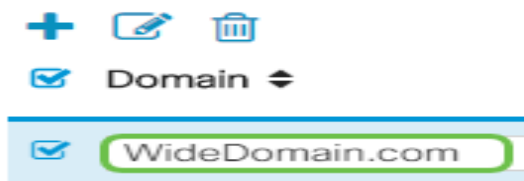
Stap 14. In de Split DNS Table, klik op de knop **Add** om gesplitste DNS uitzondering toe te voegen.

## Split DNS Table



Stap 15. Voer in het daarvoor bestemde veld de domeinnaam in en klik vervolgens op **Toepassen**.

## Split DNS Table

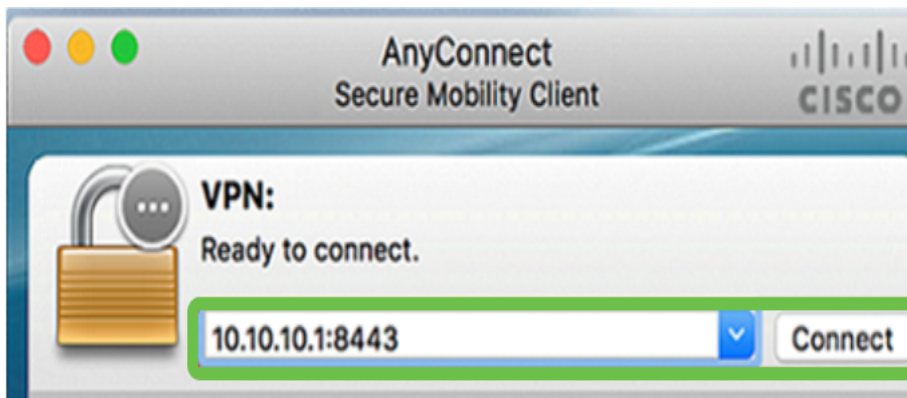


## Controleer de AnyConnect VPN-connectiviteit

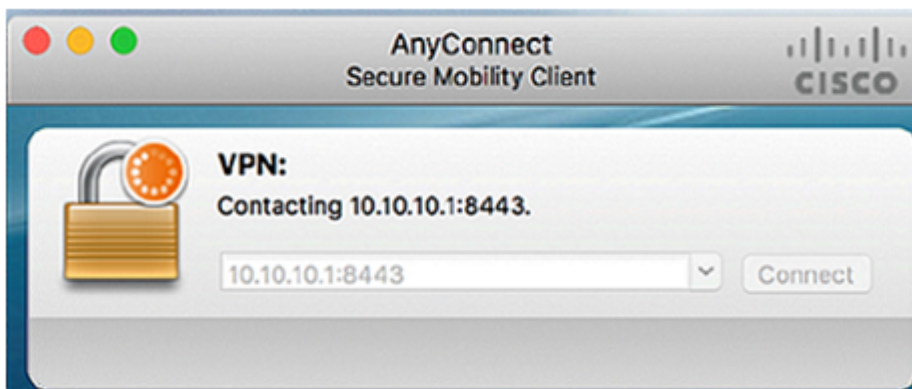
Stap 1. Klik op het pictogram van de **client voor AnyConnect Secure Mobility**.



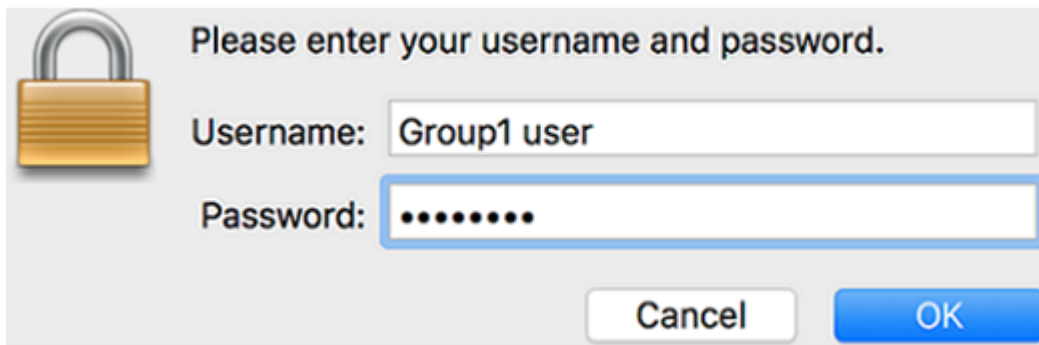
Stap 2. Voer in het venster AnyConnect Secure Mobility Client het IP-adres van de gateway en het poortnummer van de gateway in, gescheiden door een dubbele punt (:), en klik vervolgens op **Connect**.



**Opmerking:** in dit voorbeeld wordt 10.10.10.1:8443 gebruikt. De software zal nu laten zien dat hij contact opneemt met het externe netwerk.



Stap 3. Voer in de betreffende velden uw servergebruikersnaam en wachtwoord in en klik vervolgens op **OK**.



Please enter your username and password.

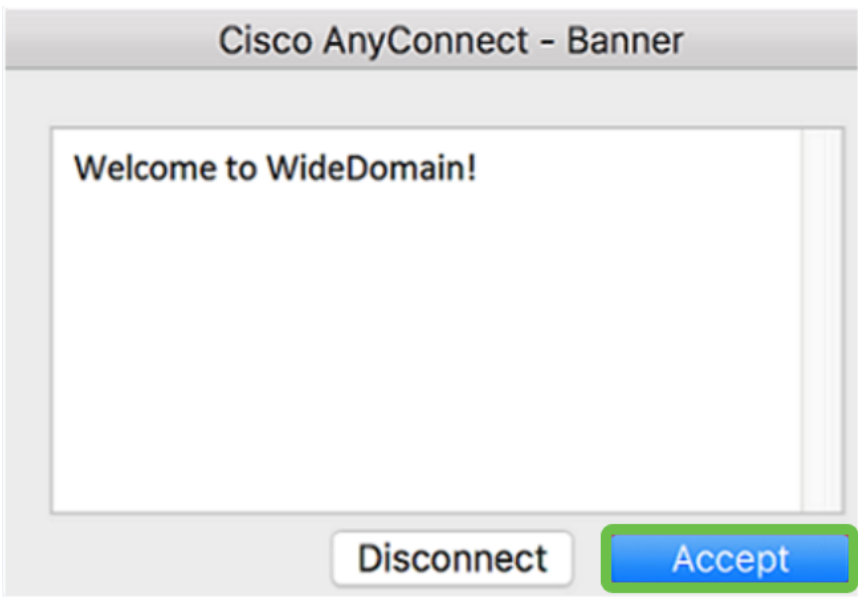
Username: Group1 user

Password: .....

Cancel OK

**Opmerking:** in dit voorbeeld wordt de gebruiker Group1 gebruikt als de gebruikersnaam.

Stap 4. Zodra de verbinding tot stand is gebracht, verschijnt de Login Banner. Klik op **Akkoord**.

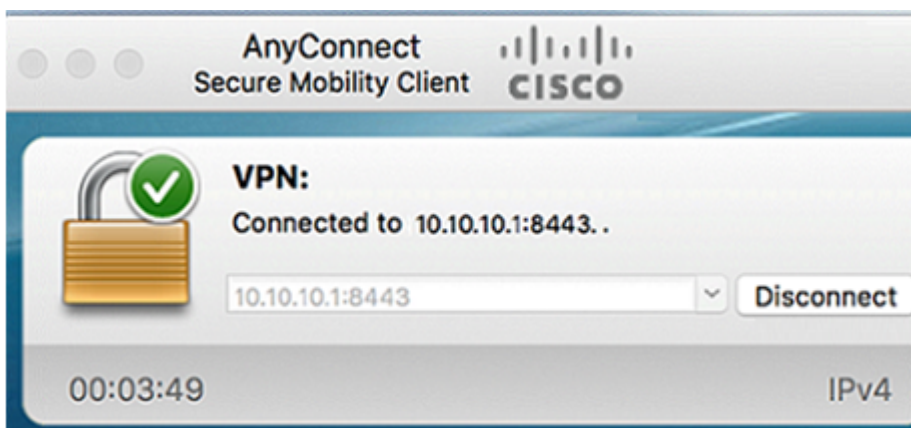


Cisco AnyConnect - Banner


Welcome to WideDomain!

Disconnect Accept

Het AnyConnect-venster moet nu de succesvolle VPN-verbinding met het netwerk aangeven.



AnyConnect Secure Mobility Client CISCO

VPN:  Connected to 10.10.10.1:8443..

10.10.10.1:8443 Disconnect

00:03:49 IPv4

Stap 5. (Optioneel) Klik op **Verbinding verbreken** om de verbinding met het netwerk te verbreken.

U moet nu met succes AnyConnect VPN-connectiviteit hebben geconfigureerd met een RV34x Series-router.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.