

# OpenVPN op een RV160 en RV260 router

## Doel

Het doel van dit artikel is om u door het instellen van OpenVPN op uw RV160- of RV260-router en de VPN-clientinstellingen van OpenVPN op uw computer te begeleiden.

## Toepasselijke apparaten

- RV160
- RV260

## Softwareversie

- 1.0.00.15

## Inhoud

[Een demo OpenVPN-applicatie instellen op een RV160/RV260-router](#)

[Instellen van OpenVPN op een RV160/RV260 router](#)

[Inloggen met een zelfondertekend certificaat na installatie van Demo OpenVPN](#)

[OpenVPN-clientinstelling op computer](#)

## Inleiding

OpenVPN is een gratis, open-source toepassing die kan worden ingesteld en gebruikt voor een Virtual Private Network (VPN). Het maakt gebruik van een client-server verbinding om beveiligde communicatie tussen een server en een externe clientlocatie via het internet mogelijk te maken.

OpenVPN gebruikt OpenSSL voor encryptie van UDP en TCP voor verkeerstransmissie. Een VPN biedt een beveiligde tunnel van bescherming, die minder kwetsbaar is voor hackers omdat het gegevens versleutelt die van uw computer worden verzonden via de VPN-verbinding. Als u bijvoorbeeld WiFi gebruikt op een openbare plaats, zoals op een luchthaven, houdt het uw gegevens, transacties en vragen bij om door andere gebruikers gezien te worden. Net als HTTPS, versleutelt het gegevens die tussen twee eindpunten worden verzonden.

Een van de belangrijkste stappen in het opzetten van OpenVPN is het verkrijgen van een Certificaat van een certificaatinstantie (CA). Dit wordt gebruikt voor authenticatie. Certificaten worden van elk aantal locaties van derden aangekocht. Het is een officiële manier om te bewijzen dat je site veilig is. De CA is in wezen een vertrouwde bron die verifieert dat u een legitiem bedrijf bent en kan worden vertrouwd. Voor OpenVPN hebt u alleen een lagere certificering nodig tegen minimale kosten. U wordt uitgecheckt door de CA en zodra ze uw informatie hebben geverifieerd, geven ze het certificaat aan u af. Dit certificaat kan als bestand op uw computer worden gedownload. U kunt dan naar uw router (of VPN-server) gaan en het daar uploaden. Houd er rekening mee dat klanten geen Certificaat nodig hebben om OpenVPN te gebruiken; het is alleen voor verificatie door de router.

## Voorwaarden

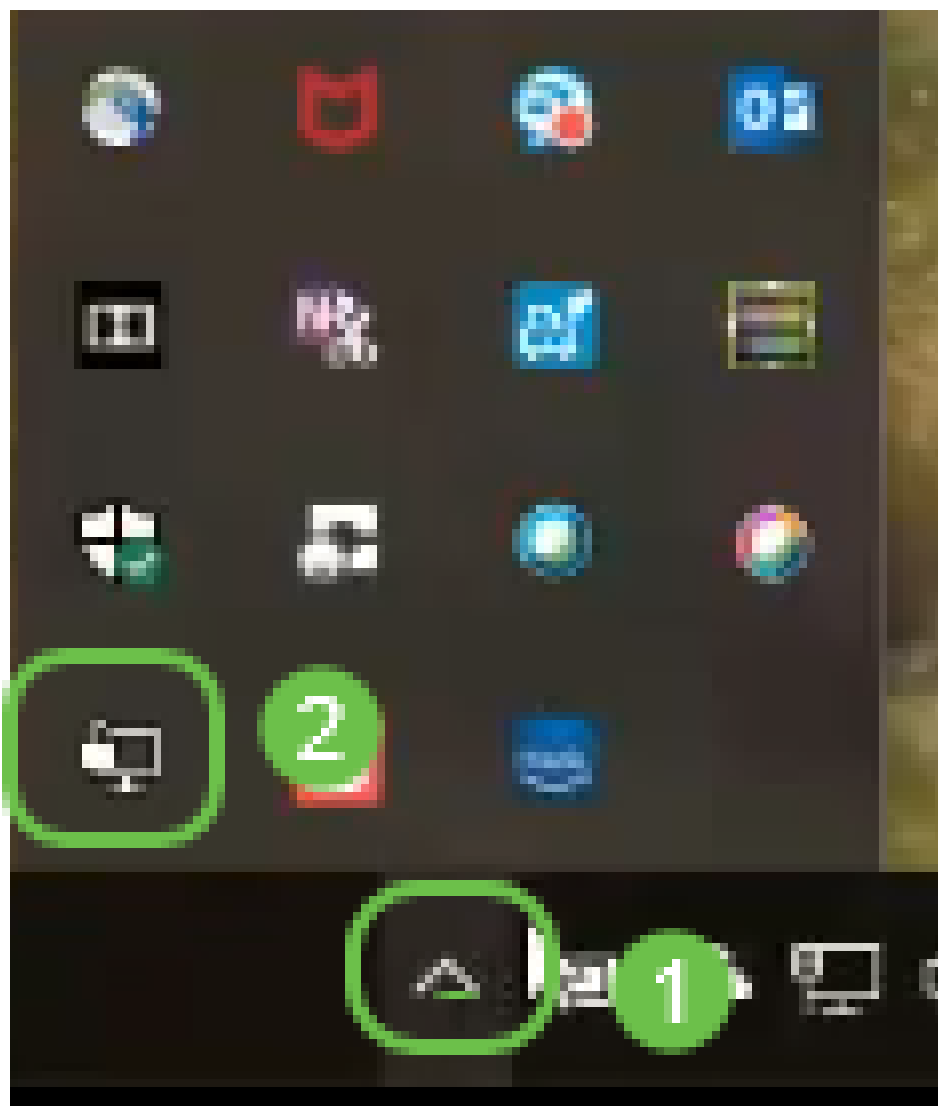
Installeer de OpenVPN-toepassing op uw systeem. Klik [hier](#) om naar de OpenVPN-website te gaan.

Voor meer informatie over OpenVPN en antwoorden op veel vragen die u kunt hebben, klik [hier](#).

Opmerking: Deze instelling is specifiek voor Windows 10.



Zodra u OpenVPN hebt geïnstalleerd, moet de toepassing op uw desktop of als een klein pictogram aan de rechterkant van de taakbalk verschijnen. OpenVPN-clients hebben deze geïnstalleerde software nodig.



Zorg ervoor dat u de juiste systeemtijd op alle apparaten hebt ingesteld. De juiste systeemtijd

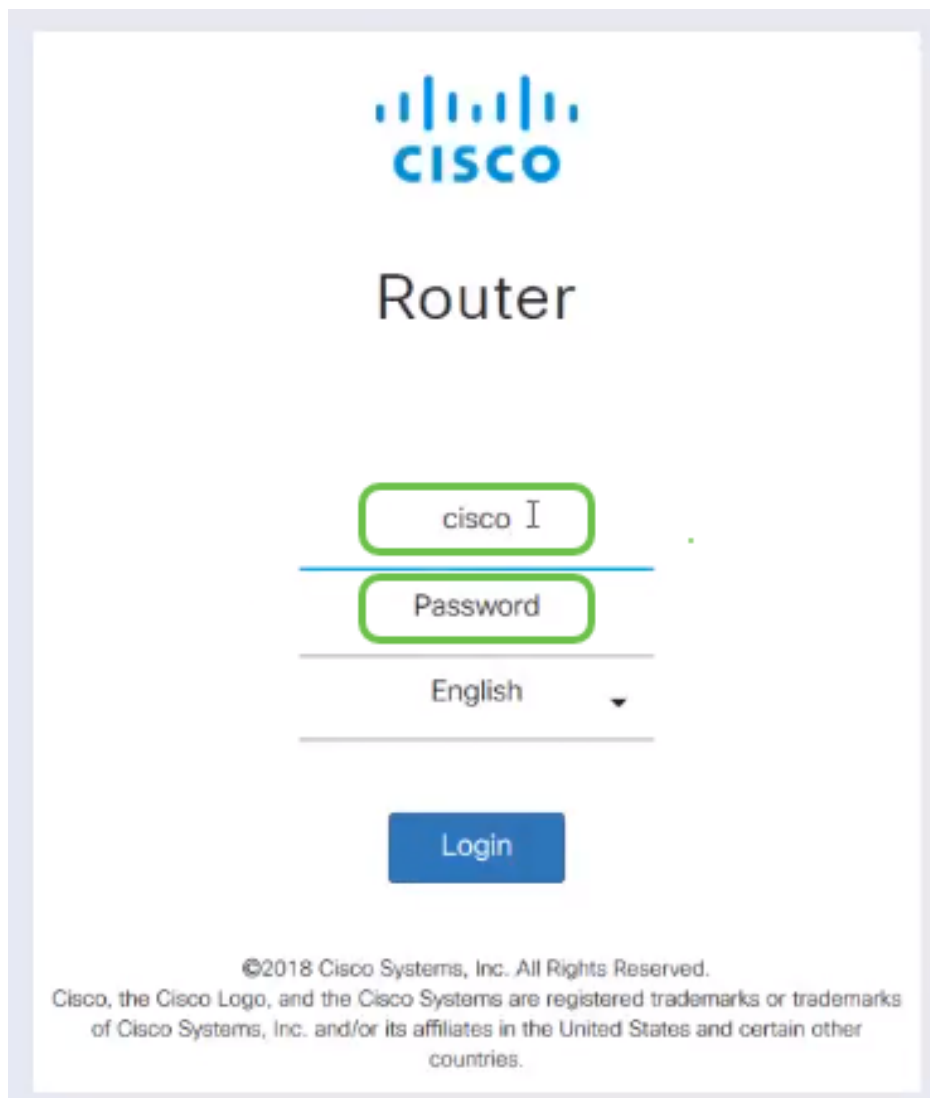
moet volledig op de router worden gesynchroniseerd voordat er een certificaat wordt gemaakt. Dit gebeurt vaak automatisch, maar als je problemen hebt, is dit een goede plek om te controleren.

## Een demo OpenVPN-applicatie instellen op een RV160/RV260-router

Als u OpenVPN wilt uitproberen voordat u geld voor een CA betaalt, kunt u een zelfgetekend certificaat maken. Dit is een kosteloze manier om te zien of OpenVPN iets is dat u voor uw bedrijf wilt inzetten. Als u al weet dat u een CA wilt aanschaffen, kunt u deze sectie van het artikel overslaan en rechtstreeks naar [OpenVPN-instelling gaan op een RV160/RV260-router](#).

Stap 1. Meld u aan bij de router met uw aanmeldingsgegevens. De standaardnaam en het wachtwoord zijn *Cisco*.

Opmerking: Het is sterk aanbevolen, alle wachtwoorden te wijzigen in iets complexers. Anders is het alsof u de toets aan de vergrendelde deur op de deur laat.



The image shows the login interface of a Cisco RV160/RV260 router. At the top is the Cisco logo. Below it, the word "Router" is displayed. The login form consists of a username field containing "cisco I", a password field labeled "Password", and a language selection dropdown menu currently set to "English". A blue "Login" button is positioned below the form. At the bottom of the page, there is a copyright notice: "©2018 Cisco Systems, Inc. All Rights Reserved. Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries."

Stap 2. Het is een vereiste dat u een certificaat op de router verkrijgen. Navigeer naar **Administratie > Certificaat > Genereert CSR/Certificaat...** Dit is hoe u het verzoek om een certificaat kunt maken.

RV260-PnP Demo

Alert cisco(admin) English

### Certificate

Certificate Table

| Index | Certificate        | Used by                    | Type              | Signed By        | Duration  | Details | Action |
|-------|--------------------|----------------------------|-------------------|------------------|---|---------|--------|
| 1     | Default            | -                          | Local Certificate | -                | From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00 |         |        |
| 2     | CertTr             | -                          | CA Certificate    | Self-Signed      | From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00 |         |        |
| 3     | CertImport         | NETCONF WebServer RESTCONF | Local Certificate | CiscoTest-DC1-CA | From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00 |         |        |
| 4     | AnthonyRouterIm... | -                          | Local Certificate | CiscoTest-DC1-CA | From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00 |         |        |

Import Certificate... Generate CSR/Certificate... Show built-in 3rd party CA Certificates... Select as Primary Certificate...

Stap 3. Voer een verzoek om een *CA-certificaat* in.

### Generate CSR/Certificate

Generate Cancel

Type: CA Certificate

Certificate Name: Cert\_Test\_CA

Subject Alternative Name: 192.168.1.50  
 IP Address  FQDN  Email

Country Name (C): United States

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU): Training

Common Name (CN): Cert Test CA

Email Address (E): @cisco.com

Key Encryption Length: 2048

- Selecteer *CA-certificaat* in het uitrolmenu
- Voer een certificaatnaam in
- Voer het IP-adres in, Full Qualified Domain Name (FQDN) of E-mail. Het invoeren van het IP-adres is de meest gebruikelijke keuze.
- Voer uw land in
- Voer uw status in
- Voer uw plaatselijke naam in (meestal uw plaats)
- Voer uw naam van de organisatie in
- Voer uw naam van de organisatie-eenheid in
- Voer uw e-mailadres in
- Lengte encryptie-toets invoeren, wordt 2048 aanbevolen

Klik op de rechter bovenknop **Generate**.

Stap 4. U hebt ook een servercertificaat nodig. Dit *certificaat* dat *is ondertekend door een CA-certificaat*, wordt ondertekend door het CA-certificaat dat u zojuist hebt gemaakt.

RV260-PnP Demo

Alert cisco(admin) English

### Certificate

| Index | Certificate        | Used by                    | Type              | Signed By        | Duration  | Details | Action |
|-------|--------------------|----------------------------|-------------------|------------------|---|---------|--------|
| 1     | Default            | -                          | Local Certificate | -                | From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00 |         |        |
| 2     | CertT              |                            | CA Certificate    | Self-Signed      | From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00 |         |        |
| 3     | CertImport         | NETCONF WebServer RESTCONF | Local Certificate | CiscoTest-DC1-CA | From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00 |         |        |
| 4     | AnthonyRouterIm... | -                          | Local Certificate | CiscoTest-DC1-CA | From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00 |         |        |

Buttons: Import Certificate..., **Generate CSR/Certificate...**, Show built-in 3rd party CA Certificates..., Select as Primary Certificate...

Stap 5. Voer een verzoek om een *certificaat* in *dat is ondertekend door een CA-certificaat*.

### Generate CSR/Certificate

Buttons: Generate, Cancel

Type: Certificate Signed by CA Certificate

Authorize External CSR:

Certificate Name: CertTest\_CA

Subject Alternative Name: 192.168.1.50

Country Name (C): United States

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU):

Common Name (CN): Cert Test CA

Email Address (E): .com

Key Encryption Length: 2048

Valid Duration: 360 days (Range: 1-10950, Default 360)

Certificate Authority:

- Selecteer *certificaataanvraag* in het uitrolmenu
- Voer een certificaatnaam in
- Voer het IP-adres in, Full Qualified Domain Name (FQDN) of E-mail. Het invoeren van het IP-adres is de meest gebruikelijke keuze.
- Voer uw land in
- Voer uw status in
- Voer uw plaatselijke naam in (meestal uw plaats)
- Voer uw naam van de organisatie in
- Voer uw naam van de organisatie-eenheid in
- Voer uw e-mailadres in
- Lengte encryptie-toets invoeren, wordt 2048 aanbevolen
- Kies de juiste certificaatinstantie in het uitrolmenu

Klik op de rechter bovenknop **Generate**.

Stap 6. Navigeer naar **stelselconfiguratie > gebruikersgroepen**. Selecteer het pictogram **plus** om de nieuwe groep toe te voegen.

Getting Started  
 Status and Statistics  
 Administration 1  
 System Configuration 1  
 Initial Router Setup  
 System  
 Time  
 Log  
 Email  
 User Accounts  
 User Groups 2

### User Groups

Apply Cancel

3 + [edit] [delete]

| <input type="checkbox"/> Group      | Web Login /NETCONF /RESTCONF | Lobby Ambassa... | 802.1x  | S2S IPSec VPN | C2S IPSec VPN | OpenVPN | PPTP    | Captive Portal |
|-------------------------------------|------------------------------|------------------|---------|---------------|---------------|---------|---------|----------------|
| <input type="checkbox"/> Ambassa... | Disable                      | Enable           | Disable | Disable       | Disable       | Disable | Disable | Enable         |
| <input type="checkbox"/> admin      | Admin                        | Enable           | Enable  | Enable        | Enable        | Enable  | Enable  | Enable         |
| <input type="checkbox"/> guest      | Disable                      | Disable          | Disable | Disable       | Disable       | Disable | Disable | Disable        |

Stap 7. Voer de naam van de groep in en klik op *Aan* voor de radioknop om OpenVPN aan te zetten. Klik op *Toepassen*.

### User Groups

3 Apply Cancel

Group Name: OpenVPN 1

#### Local User Membership List

+ [delete]

| <input type="checkbox"/> # | User |
|----------------------------|------|
| _____                      |      |

\* Should have at least one account in the 'admin' group.

#### Services

Web Login/NETCONF/RESTCONF:  Disable  Readonly  Admin

Site to Site VPN:

+ [delete]

| <input type="checkbox"/> # | Connection Name |
|----------------------------|-----------------|
| _____                      |                 |

Client to Site VPN:

+ [delete]

| <input type="checkbox"/> # | Group Name |
|----------------------------|------------|
| _____                      |            |

OpenVPN: 2  On  Off  
 PPTP VPN:  On  Off  
 802.1x:  On  Off  
 Lobby Ambassador:  On  Off

Stap 8. Navigeer in het menu *Systeemconfiguratie* en klik op **Gebruikersrekeningen**. Klik onder *Local Gebruikers* op het pictogram **plus**.

Getting Started  
Status and Statistics  
Administration  
System Configuration  
Initial Router Setup  
System  
Time  
Log  
Email  
User Accounts  
User Groups  
IP Address Groups  
SNMP  
Discovery-Bonjour  
LLDP  
Automatic Updates  
Schedules

### User Accounts

Minimal Password Length:  (Range: 0-64, Default: 8)  
Minimal Number of Character Classes:  (Range: 0-4, Default: 3)  
The four classes are: uppercase (A,B,C...), lowercase (a,b,c...), numbers (1,2,3...) and special characters (!@#\$....).  
The new password must be different from the current one.:  Enabled  
Password Aging Time:  days (Range: 0-365, 0 means never expires)

Local Users

| Username                            | Group      |
|-------------------------------------|------------|
| <input type="checkbox"/> Test_Admin | Ambassador |
| <input type="checkbox"/> cisco      | admin      |
| <input type="checkbox"/> guest      | guest      |

\* Should have at least one account in the 'admin' group.

Stap 9. Vul de onderstaande informatie in. Zorg ervoor dat u OpenVPN in het uitrolmenu selecteert. Klik op **Toepassen**.

## Add user account

The current minimum requirements are as follows

- \* Minimal Password Length: 8
- \* Minimal Number of Character Classes: 3

Username:  **1**

New Password:

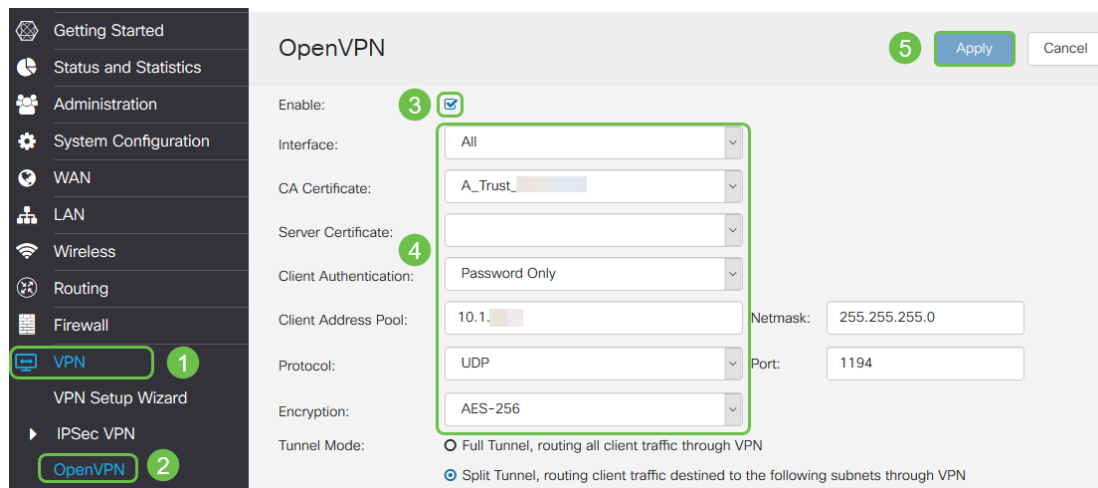
Confirm Password:

Password Strength meter:

Group:  **2**

Alle afhankelijkheden zijn voltooid en de router kan nu voor OpenVPN worden geconfigureerd.

Stap 10. Navigeer naar **VPN > OpenVPN**. De pagina OpenVPN wordt geopend. Vul elk vakje op de pagina in, zodat u de eerder gemaakte certificaten in het uitrolmenu kunt selecteren.



- Controleer het vakje *Enable*. Selecteer de interface die in verkeer zal toestaan. In dit geval een WAN-interfacekaart (Wide Area Network) en selecteer een CA-certificaat (certificaatautoriteit).
- Selecteer het *CA-certificaat* in het uitrolmenu
- Selecteer het servercertificaat dat u in het uitrolmenu hebt gedownload
- Selecteer *Clientverificatie*. Als u het wachtwoord selecteert, moeten ze voor authentiek zijn met een wachtwoord. Als u Wachtwoord + Certificaat selecteert, moet de cliënt ook een certificaat hebben. Dit is veiliger maar voegt aan de kosten van VPN toe aangezien zij een afzonderlijk CA moeten kopen.
- Voer de *clientadresgroep in*. Kies een IP adres op netwerksubtype dat niet elders in het bedrijf wordt gebruikt. U selecteert uit de gereserveerde bereiken en kiest een bereik dat nergens anders wordt gebruikt.
- Kies het formulier voor *encryptie*. Zorg ervoor dat de encryptie dezelfde is als de client. DES en 3DES worden niet aanbevolen en dienen alleen te worden gebruikt voor compatibiliteit met de achterzijde.
- Kies Split-tunnel als u alleen wilt specificeren welk verkeer door VPN gaat. Voor een VPN is een gesplitste tunnel nodig. *De volledige Tunnelmodus* wordt in andere situaties geselecteerd wanneer u al het clientverkeer door VPN wilt laten gaan.

Stap 1. Scrollt de pagina en vul de *domeinnaam* en *DNS1* in.

|              |  |
|--------------|--|
| Domain Name: | <input type="text" value="Openvpn.net"/> |
| DNS1:        | <input type="text" value="192.168.1.1"/> |

**Opmerking:** het DNS1 IP-adres kan een speciale interne DNS-server zijn, hetzelfde IP-adres van uw standaardgateway die door uw Internet Service Provider (ISP) wordt geleverd, op een virtuele machine of een vertrouwde DNS-server op het internet.

Stap 12. Klik op **Toepassen** om de configuratie op de router op te slaan.

Stap 13. Blijf op dezelfde pagina en ga verder met scrollen. Generate de configuratiesjabloon die op de OpenVPN client moet worden geïnstalleerd. Dit bestand heeft een *.ovpn*-extensie en wordt gebruikt door de OpenVPN-client. Controleer het vakje om de *configuratiejabloon van de client uit te voeren (.ovpn)* en klik op **Generate**. Dit downloads van het bestand naar uw computer.



Export setting:

Include client certificate:

Please choose the method you want to export:

1  Export client configuration template (.ovpn)

Send Email [Click here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma):

Email Subject:

2

Stap 14. Navigeer naar **Status en Statistieken > VPN-status**. U hebt de mogelijkheid om naar beneden te scrollen voor gedetailleerdere informatie.

**System Summary**

IPv4 | IPv6

WAN (Copper) | USB

IP Address: 210.1.100.20/24 | --

Default Gateway: 210.1.100.1 | --

DNS: 210.1.100.1 | --

Dynamic DNS: Disabled | Disabled

(No Attached)

**VPN Status**

| Type    | Active   | Configured | Max Supported | Connected |
|---------|----------|------------|---------------|-----------|
| IPSec   | Disabled | 0          | 20            | 0         |
| PPTP    | Disabled | 1          | 20            | 0         |
| OpenVPN | Enabled  | 1          | 20            | 0         |

**Firewall Setting Status**

SPI (Stateful Packet Inspection): On

DoS (Denial of Service): On

Block WAN Request: Off

Remote Management: On

**Log Setting Status**

Syslog Server: Off

Email Log: Off

Het volgende gedeelte van dit artikel is belangrijk om te bekijken, omdat het uitlegt hoe je kunt inloggen met een zelfondertekend certificaat.

## Inloggen met een zelfondertekend certificaat na het instellen van Demo OpenVPN

Wanneer u inlogt met een zichzelf ondertekend certificaat, verschijnt er mogelijk een waarschuwing wanneer u probeert in te loggen. U moet op Geavanceerd, Verwerken, Vertrouwen of een andere optie klikken, afhankelijk van uw webbrowser, om verder te kunnen gaan.

Op dit punt kunt u een waarschuwing ontvangen dat het niet veilig is. U kunt kiezen om te gaan, een uitzondering of een geavanceerd pad toe te voegen. Dit zal per webbrowser verschillen.

In dit voorbeeld werd Chrome gebruikt voor een webbrowser. Klik op **Geavanceerd** in dit bericht.



## Your connection is not private

Attackers might be trying to steal your information from ██████████.net (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Help improve Safe Browsing by sending some [system information and page content](#) to Google. [Privacy policy](#)

ADVANCED

BACK TO SAFETY

Er wordt een nieuw scherm geopend en u moet op **Ga naar uw website.net (onveilig)** klikken

This server could not prove that it is ██████████.net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to ██████████.net (unsafe)

Hier is een voorbeeld van toegang tot de apparaatwaarschuwing wanneer Firefox als webbrowser wordt gebruikt. Klik op **Geavanceerd**.



## Your connection is not secure

The owner of ██████████.net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

Go Back

Advanced

Klik op **Uitzondering toevoegen...**

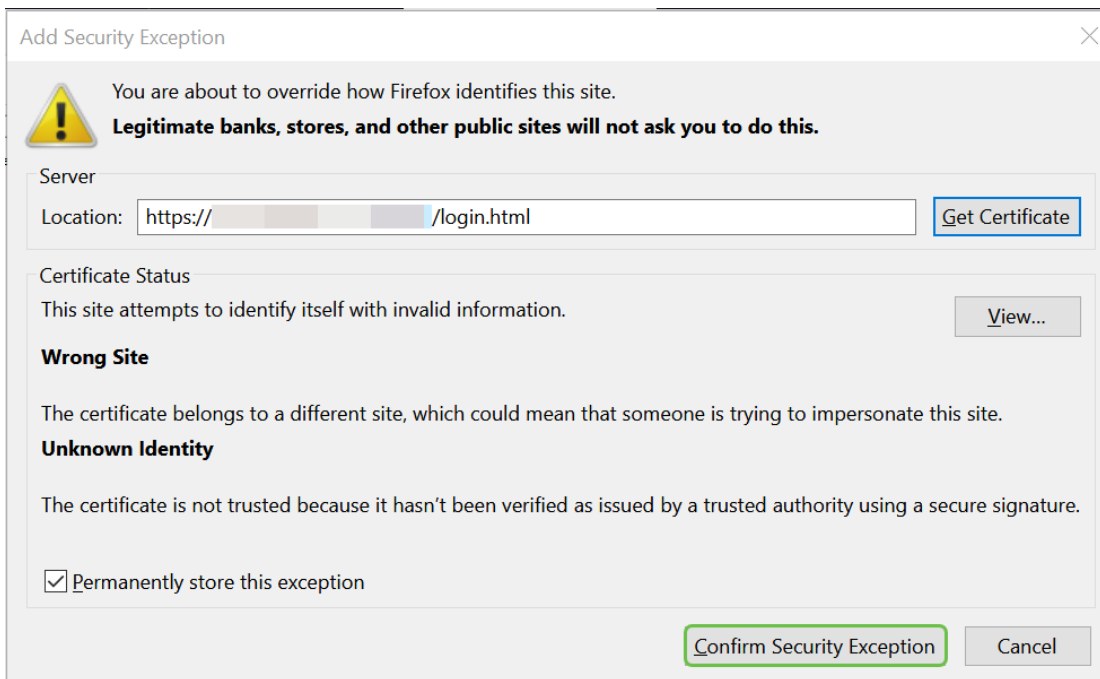
██████████.net:50 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.  
The certificate is only valid for .

Error code: [MOZILLA\\_PKIX\\_ERROR\\_SELF\\_SIGNED\\_CERT](#)

Add Exception...

Tot slot moet u op **Beveiligingsuitzondering bevestigen** klikken.



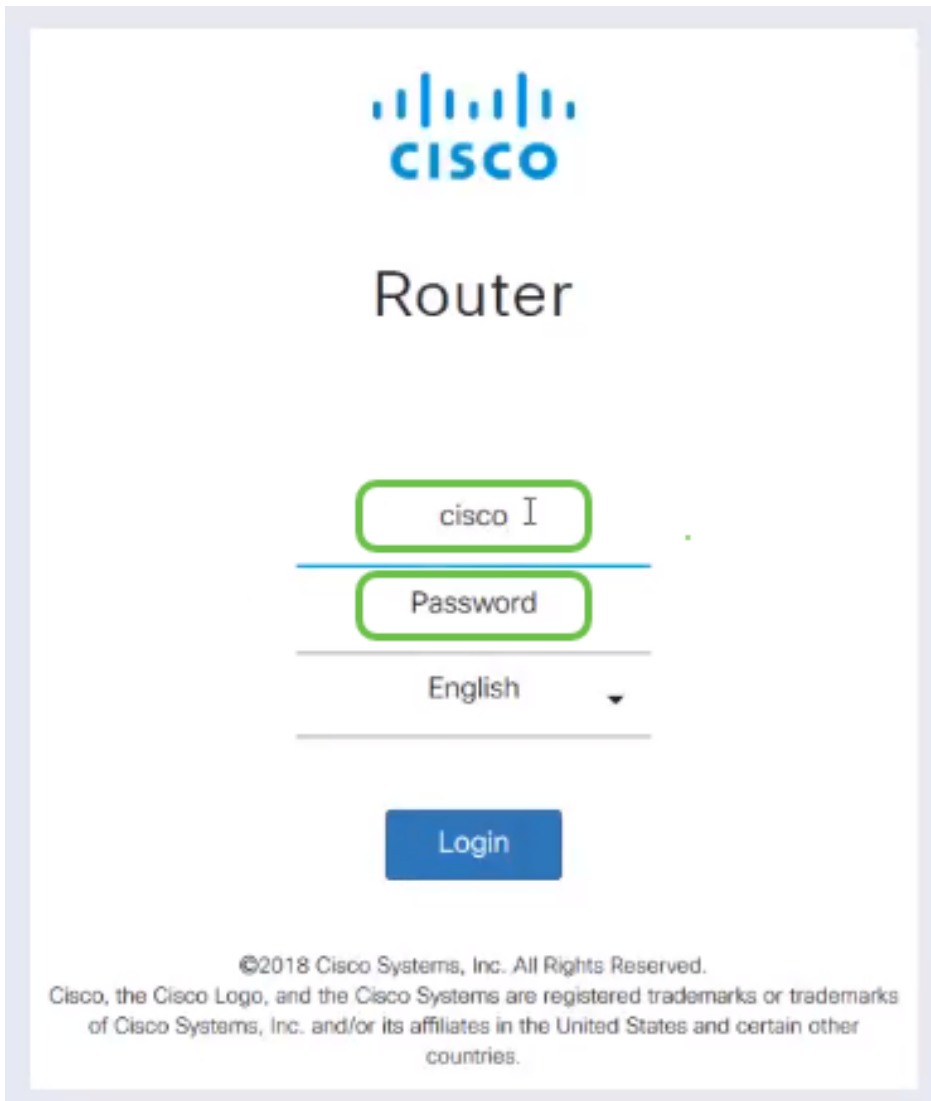
De router is nu geconfigureerd met alle parameters die nodig zijn om een OpenVPN-clientverbinding te ondersteunen. Aangezien u de configuratiesjabloon voor de client al naar uw apparaat hebt gedownload, de sjabloon die eindigt in `.ovpn`, kunt u naar de sectie [OpenVPN Client Setup op Computer](#) bewegen. Als u OpenVPN voor uw bedrijf wilt implementeren, kunt u de stappen in deze volgende sectie volgen.

## Instellen van OpenVPN op een RV160/RV260 router

Dit is een ingewikkelder proces, omdat het gaat om het verkrijgen van een CA van een derde partij, die geld kost. U moet ook de VPN client configuratie sjabloon sturen, eindigend in `.ovpn`, naar alle clients zodat ze op hun apparaat kunnen instellen. Clients moeten verschillende instellingen hebben die gelijk zijn aan de router om te kunnen communiceren. Het beste is dat u en uw medewerkers tegen minimale kosten het internet kunnen gebruiken en beter zaken kunnen doen.

Stap 1. Meld u aan bij de router met uw aanmeldingsgegevens. De standaardnaam en het wachtwoord zijn *Cisco*.

Opmerking: Het is sterk aanbevolen, alle wachtwoorden te wijzigen in iets complexers. Anders is het alsof u de toets aan de vergrendelde deur op de deur laat.



Stap 2. U eist een certificaat op. Navigeer naar **Administratie > Certificaat > Genereert CSR/Certificaat...** Dit is hoe u het verzoek om een certificaat kunt maken.

| Index | Certificate        | Used by                    | Type              | Signed By        | Duration  | Details | Action |
|-------|--------------------|----------------------------|-------------------|------------------|---|---------|--------|
| 1     | Default            | -                          | Local Certificate | -                | From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00 |         |        |
| 2     | CertT              |                            | CA Certificate    | Self-Signed      | From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00 |         |        |
| 3     | CertImport         | NETCONF WebServer RESTCONF | Local Certificate | CiscoTest-DC1-CA | From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00 |         |        |
| 4     | AnthonyRouterIm... | -                          | Local Certificate | CiscoTest-DC1-CA | From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00 |         |        |

Stap 3. Voer een verzoek om een *certificaat* in dat *is ondertekend door een CA-certificaat*. Dit kan worden gevonden door te navigeren naar **Administratie > Certificaat**.

- Selecteer *certificaataanvraag* in het uitrolmenu
- Voer een certificaatnaam in
- Voer het IP-adres in, Full Qualified Domain Name (FQDN) of E-mail. Het invoeren van het IP-adres is de meest gebruikelijke keuze.
- Voer uw land in
- Voer uw status in
- Voer uw plaatselijke naam in (meestal uw plaats)
- Voer uw naam van de organisatie in
- Voer uw naam van de organisatie-eenheid in
- Voer uw e-mailadres in
- Lengte encryptie-toets invoeren, wordt 2048 aanbevolen

Klik op de **knop** rechtsboven **Generate**.

Stap 4. Selecteer deze optie om de afbeelding te exporteren door op de pijl-omhoog onder Actie te klikken.

Stap 5. Dit scherm verschijnt. Klik op **Exporteren**.

Stap 6. Selecteer *Met en Kladblok* (standaard) openen in het uitrolmenu. Klik op **OK**.

You have chosen to open:

 **AnthonyRouter.pem**

which is: PEM file (1.2 KB)

from: blob:

What should Firefox do with this file?

**Open with:** Notepad (default)

Save File

Do this automatically for files like this from now on.

OK

Cancel

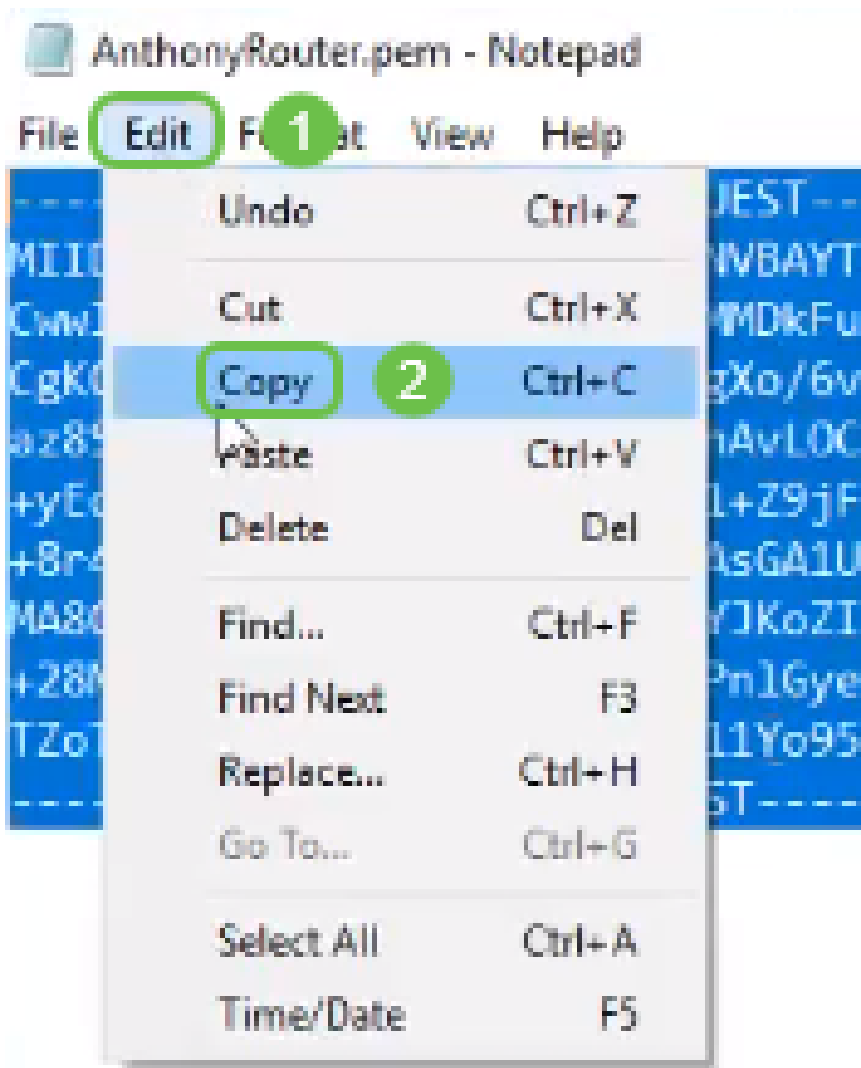
Stap 7. Een XML-bestand wordt geopend.



```
AnthonyRouter.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIIDYTCBAAkCAQAwZ2x0czA3BglhbnVAYTA1VTMRUWUWYyYVQ1IDAxTb3V0aCBYwtdGExFDASBglhbnVAcMC1Npb3V4IEZhbGxzMQ4wDAYDVQQKDAVDMHJibzERMhA0GA1UE
CwVhbnVAcwEwDQYJKoZIhvcNAQkBFhbnVAcwEwDQYJKoZIhvcNAQkBFhbnVAcwEwDQYJKoZIhvcNAQkBFhbnVAcwEwDQYJKoZIhvcNAQkBFhbnVAcwEwDQYJKoZIhvcNAQkBFhbnVAcwEw
CgKCAQEAQzLPhuMov2Iq5vM7b1gXo/6vnp18Yn1HKMDkjNlz#CroCdqRcEjEe17XYGLsR9LXt61F1JGkaQOrRopLyz7n11jRoLOBsZaeV30/bFDwOFF6X1DxOpaAyNS
az85o3RgkIoCYrgjWUj1yEF91ThAvLOCepd+BPjFpyE5j] [ ]akrBDL47n9rv4M9dNL/IKPD5tVxLw23+vFntDh821t2gyJ921hVb3dfZ42yZfEw+xjWln/N
+yEd51bVH1P6TyqK2bD0eEs1xs1+Z9jF1ac3Gw6CFDYXg09C0ja8x1qgBasGcrwnJaycF+WBOL5s41URwIDAQABoIGDMIGAAGbqkqkI69w0BCQ4xczBxMakGA1UdEwQCAAwHQDVROB0BEBFFPI
+8r4zePCPIInbV54HYdDPQCvz8MAsGA1UdDwQEAwIF4DAnBgNVH4SUEI0AeBggrBGFEBQCDAQYIKwYBBQUHwIICCSsGAQFCAIC
MA8GA1UdEQQIMAAhBMCoASgwDQYJKoZIhvcNAQELBQADggEBAF2+aVr
44sZy0N0hntamj49GnKChXMI3vFuxYVvsgo0wN1XY5nUzmDQg15jE1
+28MB1J0YuthSLMPAtb1c6zUzPn1GyemQz+JRjN/RRnq5NH5L70sd8jwadO2XXp6Xo2+mK5pm6vA1e0ef3mdJ/R+rP2AHb+1iRVWrqqQhSfJswRS2HEon4
TZoTKfXBCMTWpCh1jPFyALeH811Yo95aB02WX2e+9vIOT5XgVae2wFomPHBbsUvcUNT4jUzYHysV7XkREz7oY1PF5TZn9KzZAIoZN8aQbNUqNTxJqfBm41F01cMUys73qOGM2M=
-----END CERTIFICATE REQUEST-----
```

Opmerking: Zorg ervoor dat het BEGIN-CERTIFICAATVERZOEK EN DE EINDCERTIFICAATVERZOEK elk op hun eigen regels staan, zoals hierboven wordt aangegeven.

Stap 8. Klik boven op het scherm op **Bewerken** en selecteer **Kopie** uit het vervolgkeuzemenu.



Stap 9. Kies een gerenommeerde website van derden om het certificaat aan te vragen. U moet het gekopieerde XML bestand als deel van het verzoek toevoegen.

Opmerking: Als u een interne certificatieserver op uw netwerk hebt, kunt u dat gebruiken, maar dit komt niet veel voor.

## Submit a Certificate Request or Renewal Request

---

To submit a saved request to the CA, paste a base-64-encoded CMC Saved Request box.

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
TZoTKHXBcMTWpCh1jPFyALeNH811Yo95aBO2WX2e  
cUNT4jUzYNYaV7XkREz7oY1PF5TZW9KzzAIoZW8a  
3qO6K2H=  
  
-----END CERTIFICATE REQUEST-----
```

### Certificate Template:

---

Web Server

### Additional Attributes:

---

Attributes:

Submit >

Stap 10. Zodra u bent geverifieerd, kunt u het *Downloadcertificaat* kiezen.

## Certificate Issued

---

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

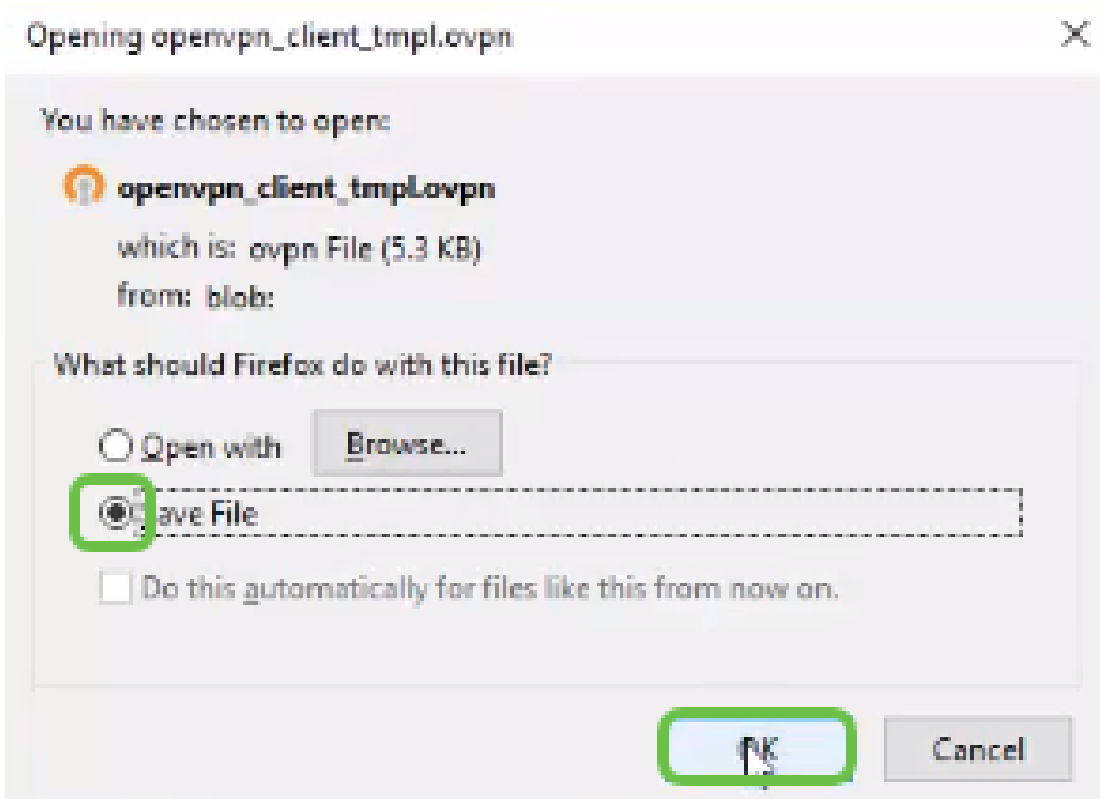


[Download certificate](#)

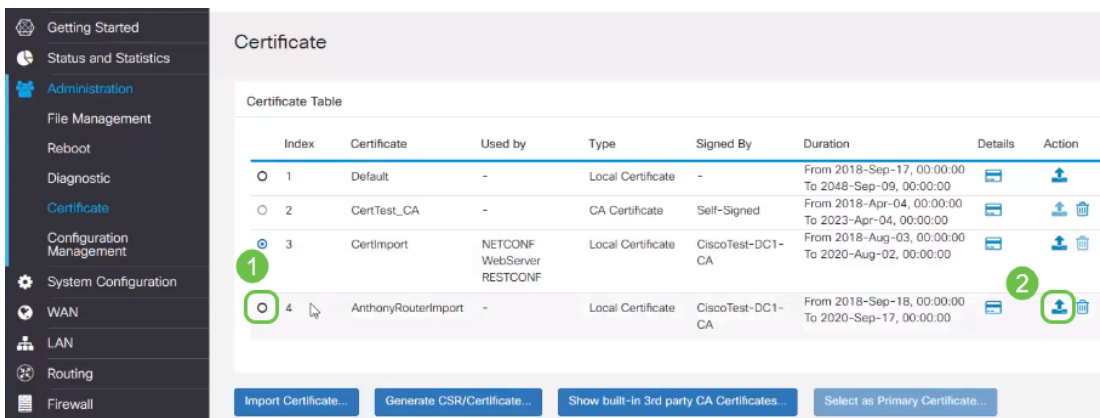
[Download certificate chain](#)

Stap 1. Klik op het keuzerondje om *Bestand* op te slaan en klik op OK.





Stap 12. Zodra het is opgeslagen, selecteert u de radioknop voor dat certificaat en klikt u op het pictogram **pijl-omlaag**.



Stap 13. Dit scherm wordt geopend. **Bladeren** selecteren....

## Import Signed-Certificate


Type: Local Certificate

Certificate Name:

### Upload Certificate file

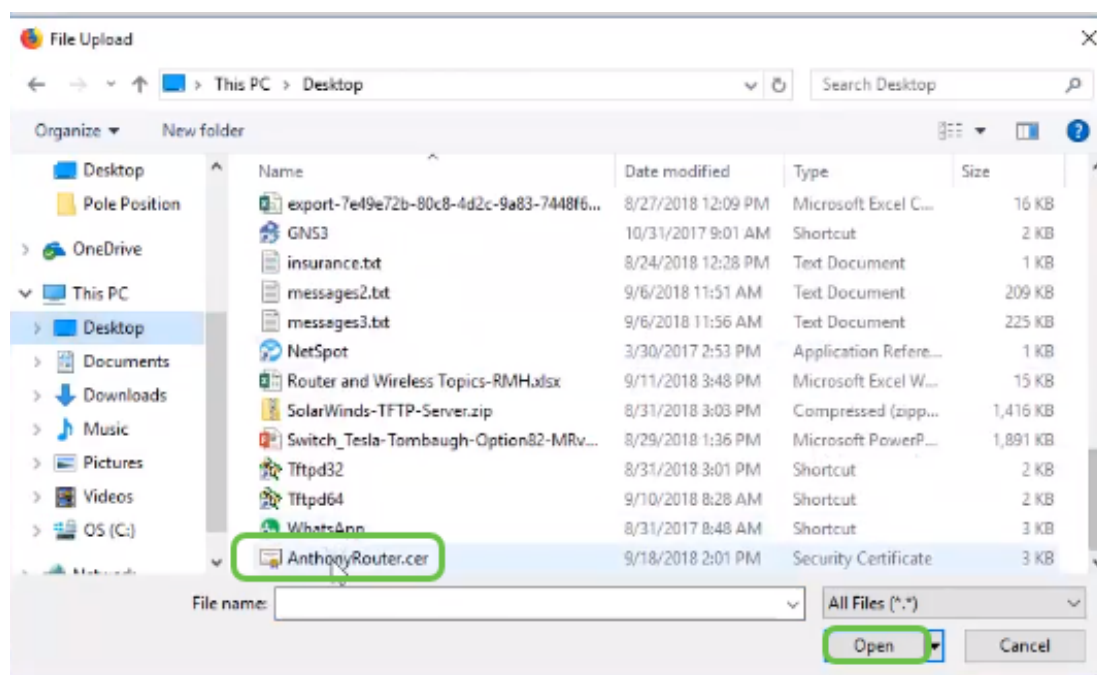
Import from PC

No file is selected

Import from USB 

No file is selected

Stap 14. Kies het bestand van het certificaat en klik op **Openen**.



Stap 15. Voer de *certificaatnaam* in om te importeren en klik op **Upload**.

## Import Signed-Certificate



Type: Local Certificate

Certificate Name: AnthonyRouterImport

### Upload Certificate file

Import from PC

Browse...

AnthonyRouter.cer

Import from USB



Browse...

No file is selected

Upload

Cancel

Stap 16. U ontvangt een melding dat het certificaat is geïmporteerd. Klik op OK.

## Information



Import certificate successfully!

OK

Stap 17. Navigeer naar **Administratie** > **Certificaat**. Het certificaat is geladen.

Opmerking: In dit voorbeeld werd een lokale certificeringsserver gebruikt.

The screenshot shows the Cisco configuration interface for a device (RV260-PrPDemo). The left sidebar has 'Administration' selected, and 'Certificate' is highlighted in the sub-menu. The main area displays the 'Certificate Table' with the following data:

| Index | Certificate         | Used by                      | Type              | Signed By        | Duration   | Details | Action |
|-------|---------------------|------------------------------|-------------------|------------------|--|---------|--------|
| 1     | Default             | -                            | Local Certificate | -                | From 2018-Sep-17, 00:00:00<br>To 2048-Sep-09, 00:00:00 |         |        |
| 2     | CertTest_CA         | -                            | CA Certificate    | Self-Signed      | From 2018-Apr-04, 00:00:00<br>To 2023-Apr-04, 00:00:00 |         |        |
| 3     | Certimport          | NETCOM WebServer<br>#3230048 | Local Certificate | CiscoTest-OC1-CA | From 2018-Aug-03, 00:00:00<br>To 2020-Aug-02, 00:00:00 |         |        |
| 4     | AnthonyRouterImport | -                            | Local Certificate | CiscoTest-OC1-CA | From 2018-Sep-18, 00:00:00<br>To 2020-Sep-17, 00:00:00 |         |        |

At the bottom of the table, there are four buttons: 'Import Certificate...', 'Generate CSR/Certificate', 'Show built-in 3rd party CA Certificates', and 'Select as Primary Certificate'.

Stap 18. Navigeer naar **VPN** > **OpenVPN**. De pagina OpenVPN wordt geopend. Volg uw informatie op het volgende.

- Controleer het vakje *Enable*. Selecteer de interface die in verkeer zal toestaan. In dit geval een WAN-interfacekaart (Wide Area Network) en selecteer een CA-certificaat (certificaatautoriteit)
- Selecteer het *CA-certificaat* in het uitrolmenu
- Selecteer het *servercertificaat* dat u in het uitrolmenu hebt gedownload
- Selecteer *Clientverificatie*. Als u het wachtwoord selecteert, moeten ze voor authentiek zijn met een wachtwoord. Als u Wachtwoord + Certificaat selecteert, moet de cliënt ook een certificaat hebben. Dit is veiliger maar voegt aan de kosten van VPN toe aangezien zij een afzonderlijk CA moeten kopen.
- Voer de *clientadresgroep* in. Kies een IP adres op netwerksubtype dat niet elders in het bedrijf wordt gebruikt. U selecteert uit de gereserveerde bereiken en kiest een bereik dat nergens anders wordt gebruikt.
- Kies het formulier voor *encryptie*. Zorg ervoor dat de encryptie dezelfde is als de client. DES en 3DES worden niet aanbevolen en dienen alleen te worden gebruikt voor compatibiliteit met de achterzijde.
- Kies *Full Tunnel Modus* als u al clientverkeer door VPN wilt laten gaan of tunnels wilt splitsen als u alleen wilt specificeren welk verkeer door VPN gaat
- Het *DNS1* IP-adres kan een speciale interne DNS-server zijn, hetzelfde IP-adres van uw standaardgateway die wordt geleverd door uw Internet Service Provider (ISP), op een virtuele machine of een vertrouwde DNS-server op het internet.

Klik op **Toepassen** om de configuratie op te slaan.

Stap 19 (Optie 1). Je kunt deze configuratie naar de klant e-mailen. Controleer het vakje *Verzend e-mail*. Voer een e-mailadres in. Voeg een Onderwerp titel voor de e-mail toe. Klik op **Generate**.

Export setting:

Include client certificate: AnthonyRouterImport

Please choose the method you want to export:

1  Export client configuration template (.ovpn)

Send Email Click [here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): nick@cisco.com

Email Subject: OpenVPN Client Config

4

Stap 20. (Optie 2). Selecteer de optie *Clientconfiguratiejabloon exporteren (.ovpn)* en klik op **Generate**.

Export setting:

Include client certificate:

Please choose the method you want to export:

1  Export client configuration template (.ovpn)

Send Email Click [here](#) to configure Email settings.


Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): input email address

Email Subject: OpenVPN Client Configurat

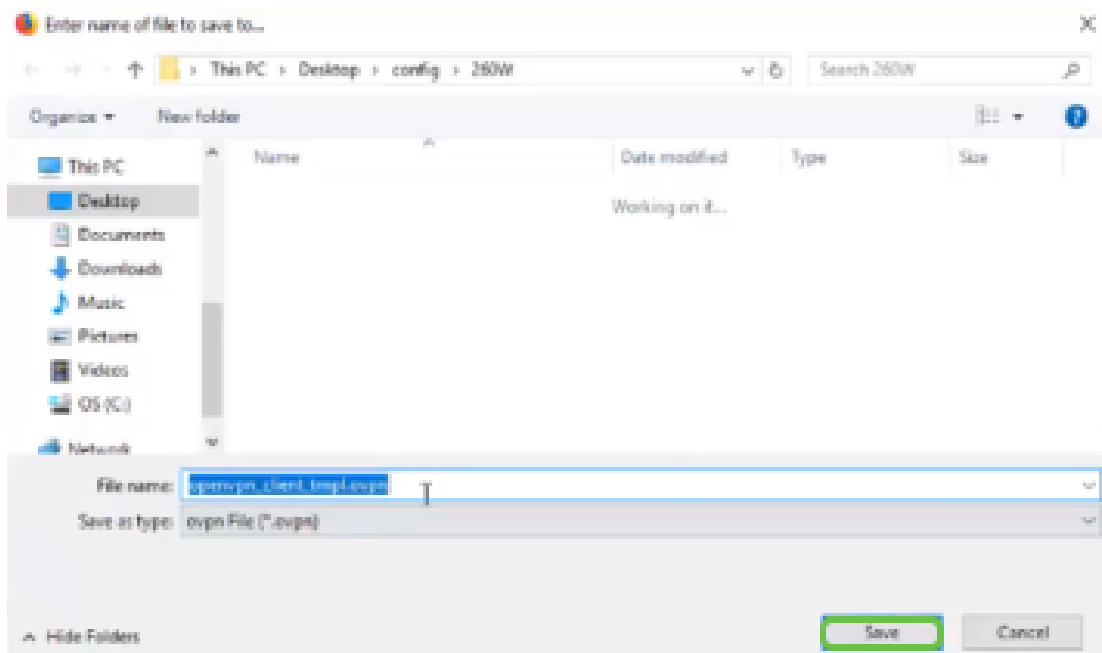
2

Stap 21. U ontvangt een bevestiging die succesvol is. Klik op **OK**.

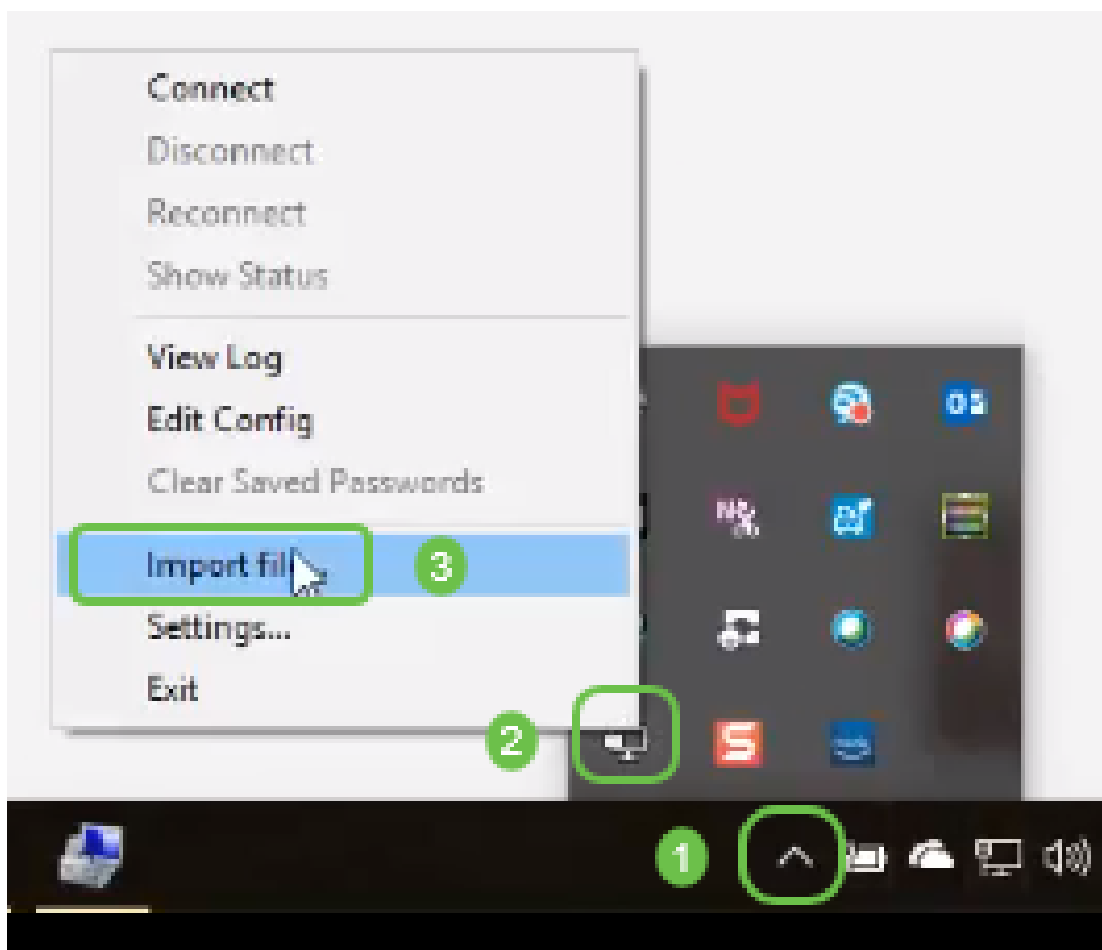
## Information

 Export client configuration template downloaded successfully!

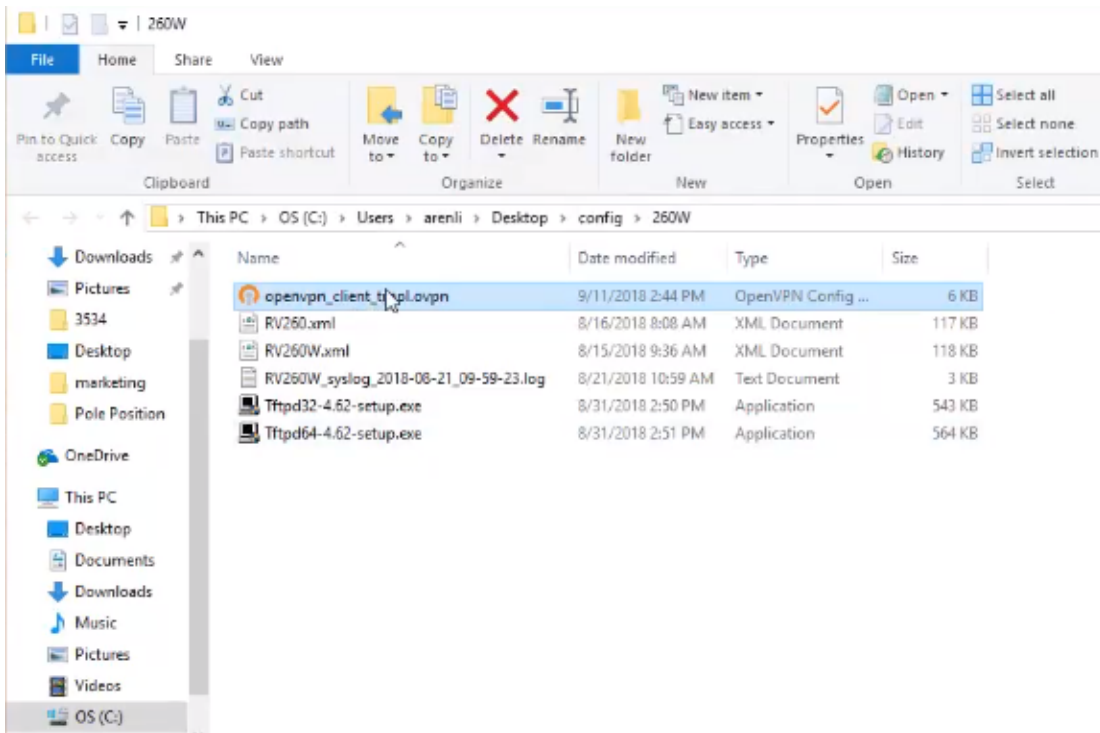
Stap 2. Klik op **Opslaan**.



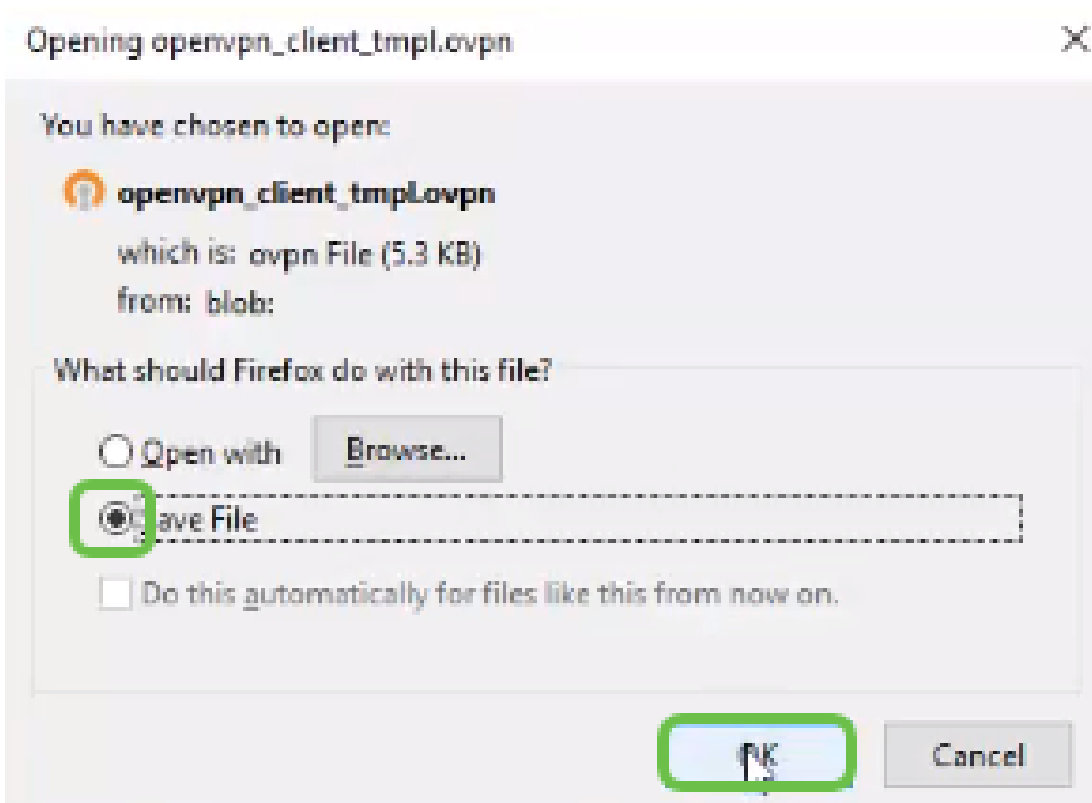
Stap 23. Onder in uw bureaublad en klik om OpenVPN te openen. Rechtsklik om het uitrolmenu te openen. Klik op *Bestand importeren*.



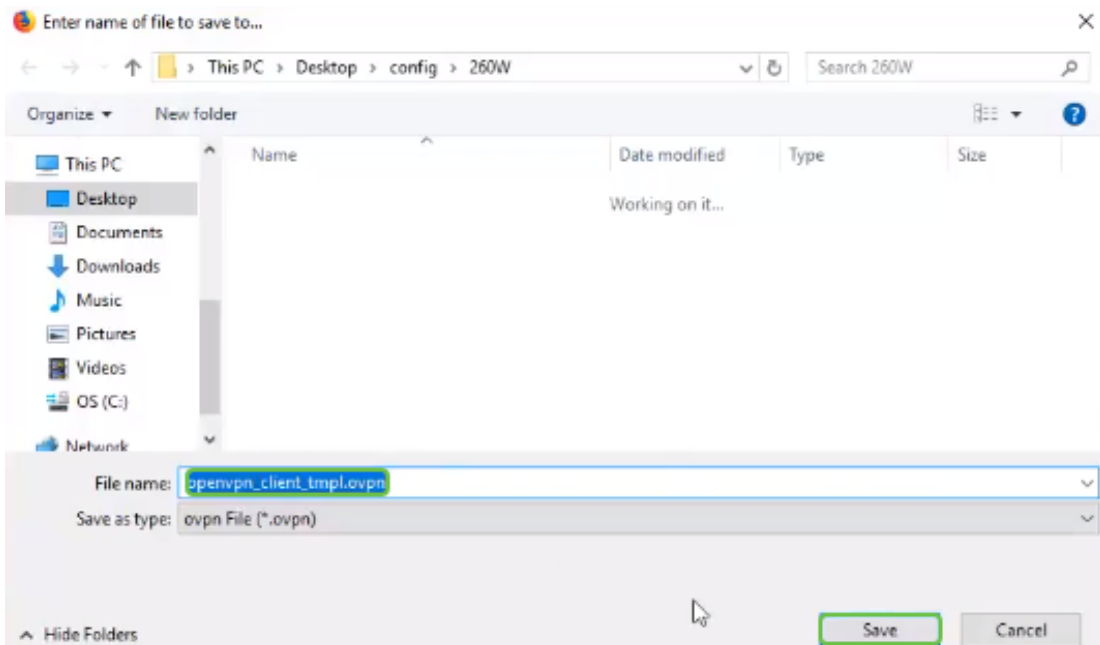
Stap 24. Selecteer het OpenVPN-bestand dat in *.ovpn* eindigt.



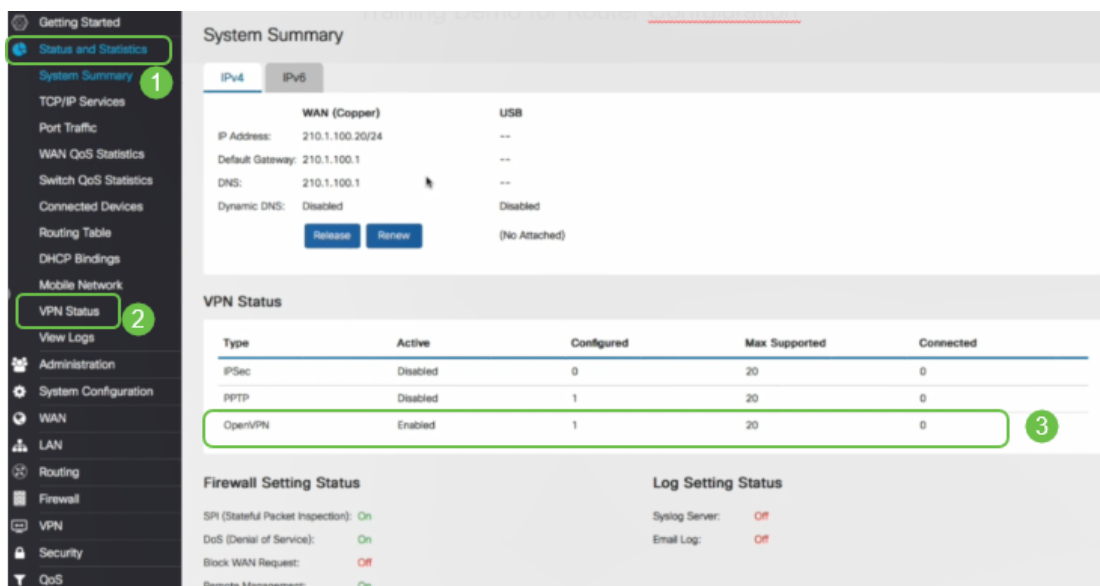
Stap 25. Klik op de knop *Opslaan bestand* en klik op **OK**.



Stap 26. Wijzig de naam van het bestand indien u dit kiest, maar laat *.ovpn* aan het einde van de bestandsnaam achter. Klik op **Opslaan**.



Stap 27. Navigeer naar **Status en Statistieken > VPN-status**. U hebt de mogelijkheid om naar beneden te scrollen voor gedetailleerdere informatie.



De router is nu geconfigureerd met alle parameters die nodig zijn om een OpenVPN-clientverbinding te ondersteunen voor uw persoonlijk proces.

## OpenVPN-clientinstelling op computer

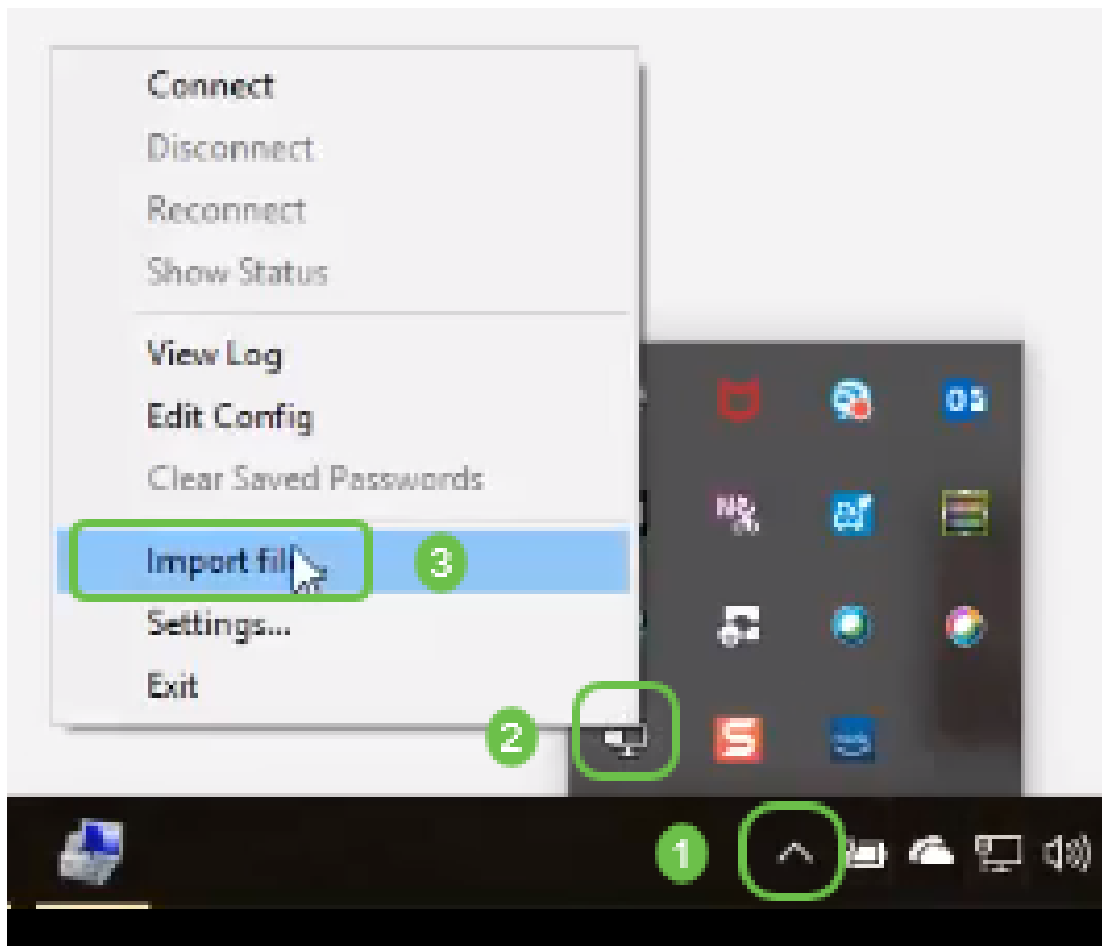
Elke OpenVPN-client moet de volgende taken als vereiste uitvoeren:

- Download de OpenVPN-toepassing op uw apparaat.
- Open het configuratiebestand dat in de voorgaande sectie in stappen 19-22 is verzonden en bewaar het configuratiebestand. Het configuratiebestand eindigt in *.ovpn*.

Opmerking: Deze instelling is specifiek voor Windows 10.

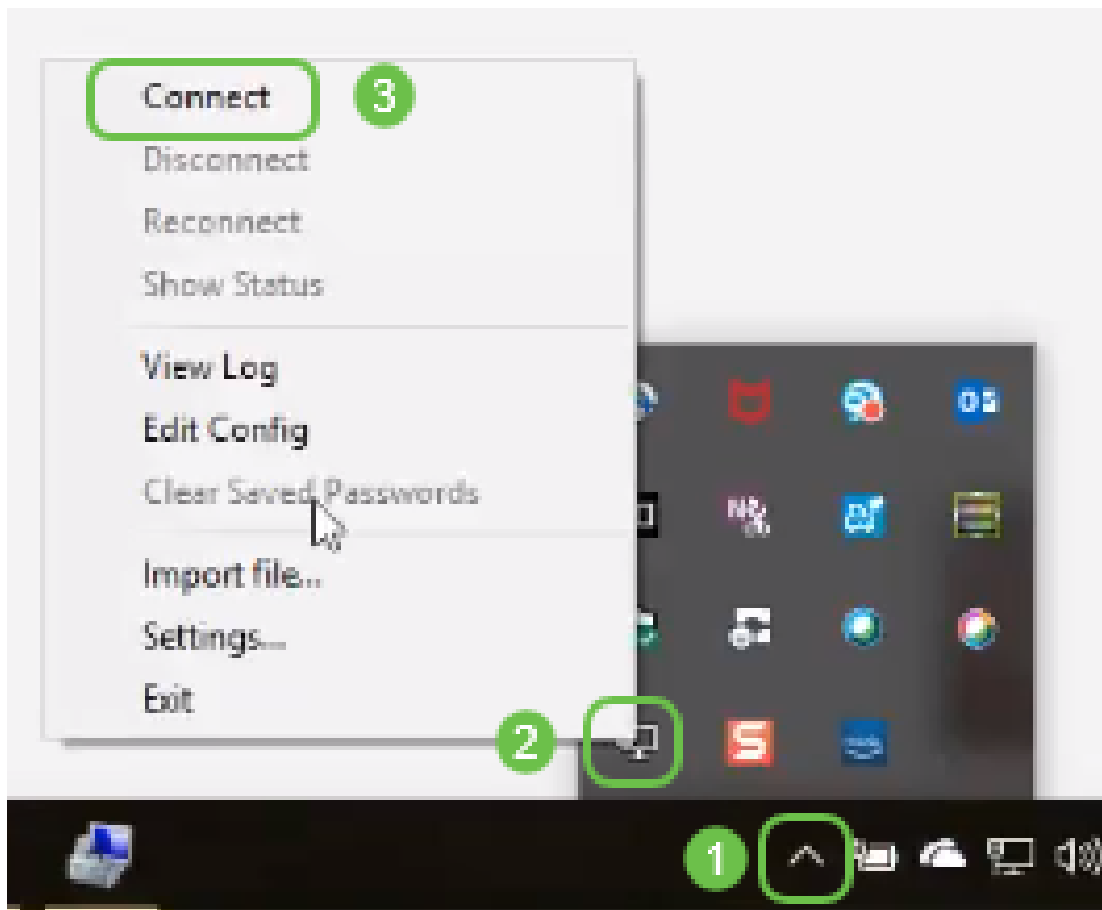
Stap 1. Navigeer naar het pijlpictogram rechts onder op het bureaublad en klik om het pictogram OpenVPN te openen. Klik met de rechtermuisknop en selecteer *Bestand importeren*.



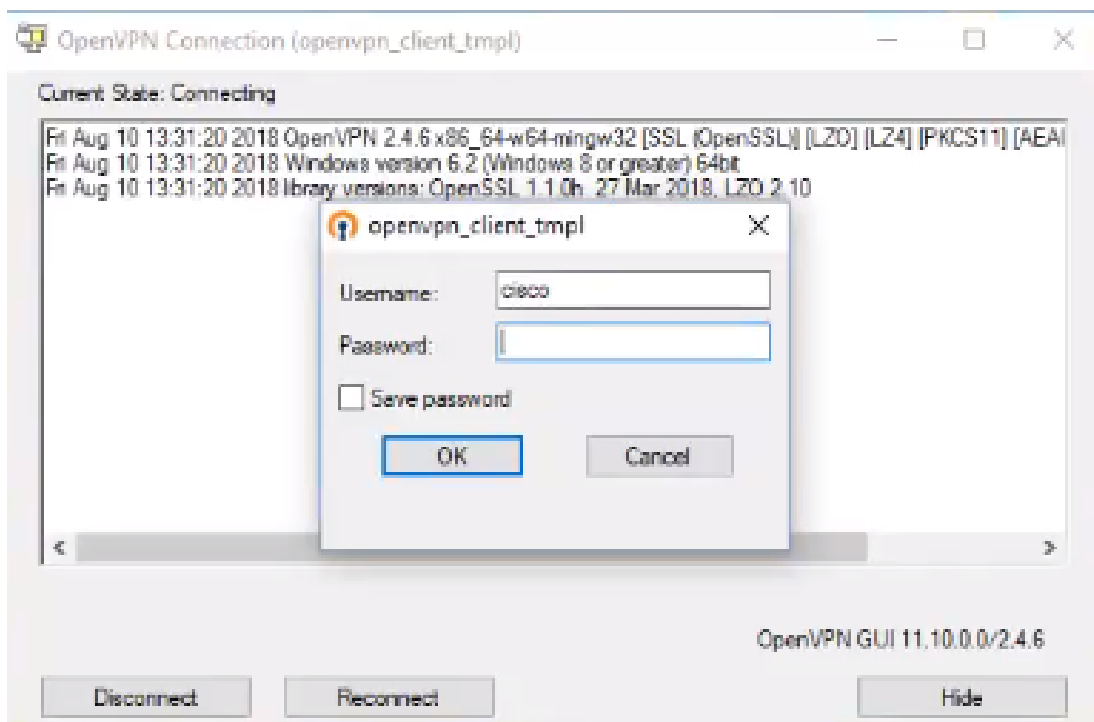


Opmerking: Het pictogram is zwart-wit, wat aangeeft dat het momenteel niet actief is. Zodra het pictogram actief is, verschijnt het in kleur.

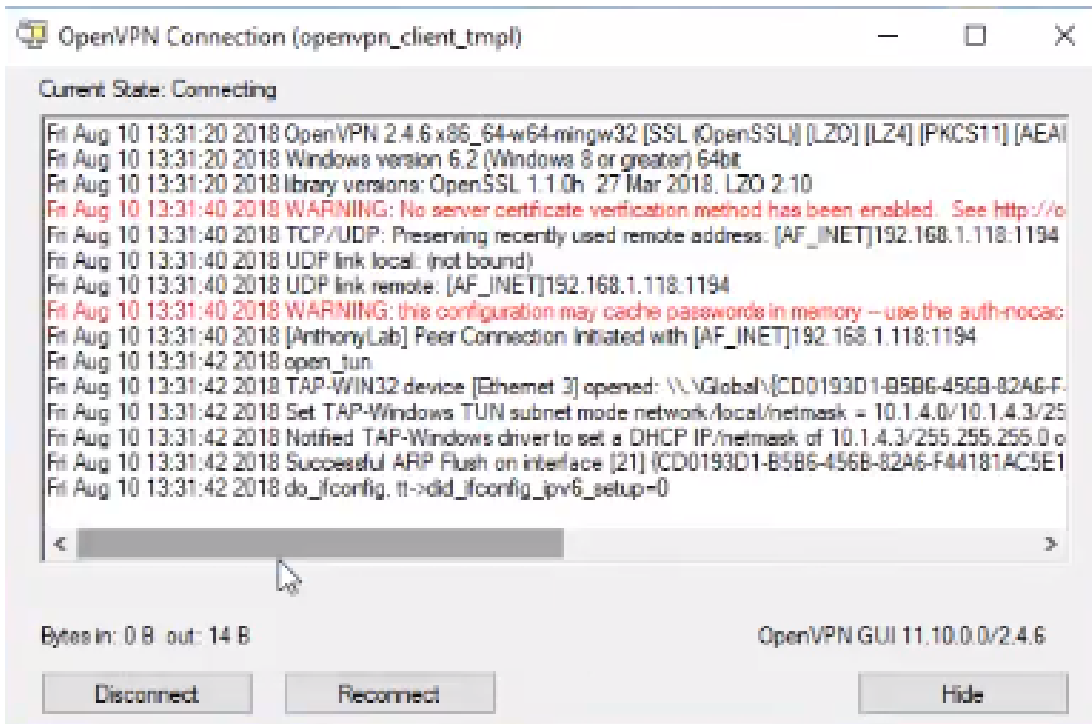
Stap 2. Klik op de *pijl-omhoog*. Klik op het pictogram OpenVPN. Klik met de rechtermuisknop en selecteer *Connect* in het uitrolmenu.



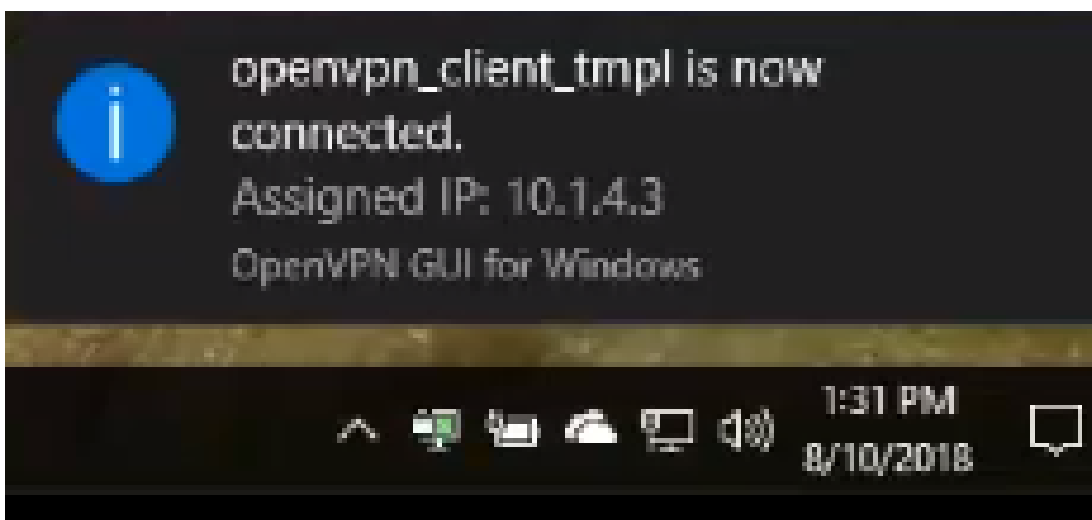
Stap 3. Voer de gebruikersnaam en het wachtwoord in.



Stap 4. Het venster toont het OpenVPN-venster dat met een aantal loggegevens is verbonden.

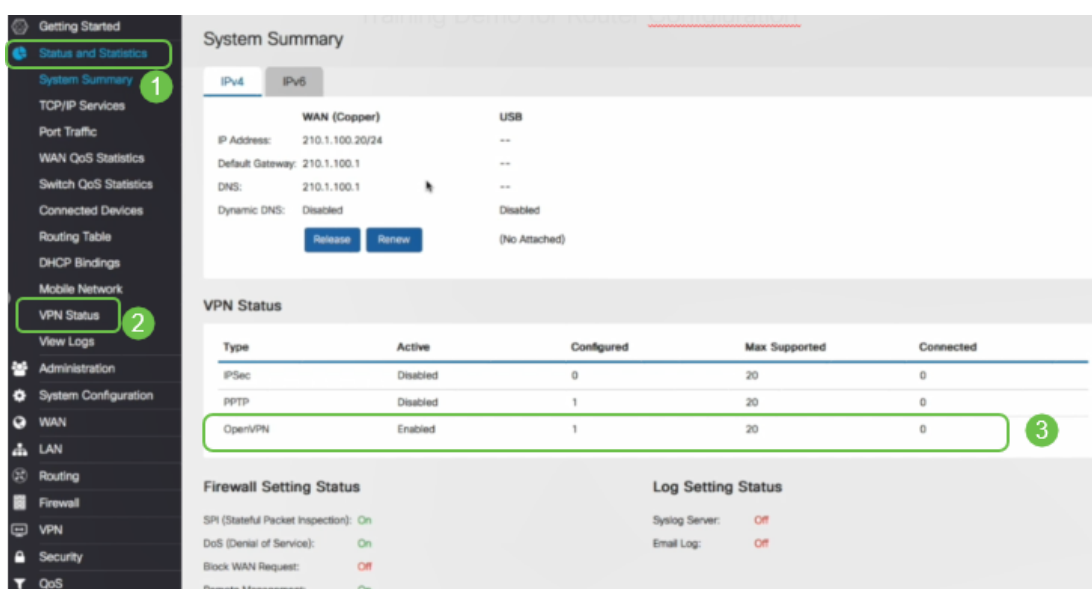


Stap 5. Een systeemlogboek moet waarschuwen dat er een verbinding is.



Stap 6. De VPN-client moet veilig in staat zijn inkomende en uitgaande informatie via OpenVPN te tunnen. Dit kan worden ingesteld om automatisch verbinding te maken met de instellingen OpenVPN.

Stap 7. De beheerder kan de VPN-status bevestigen door naar **Status en Statistieken > VPN-status** op de router te navigeren.



## Conclusie

U moet nu met succes OpenVPN op uw RV160- of RV260-router en op de VPN-clientwebsite hebben geïnstalleerd.

Voor community-discussies op OpenVPN klikt u [hier](#) en zoekt u OpenVPN.

**Bekijk een video gerelateerd aan dit artikel...**

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)