

OpenVPN sur un routeur RV160 et RV260

Objectif

L'objectif de cet article est de vous guider dans la configuration d'OpenVPN sur votre routeur RV160 ou RV260, ainsi que dans la configuration du client VPN d'OpenVPN sur votre ordinateur.

Périphériques pertinents

- RV160
- RV260

Version du logiciel

- 1.0.00.15

Table des matières

[Configuration d'un OpenVPN de démonstration sur un routeur RV160/RV260](#)

[Configuration d'OpenVPN sur un routeur RV160/RV260](#)

[Connexion à l'aide d'un certificat auto-signé après la configuration de la démonstration OpenVPN](#)

[Configuration du client OpenVPN sur l'ordinateur](#)

Introduction

OpenVPN est une application libre et open source qui peut être configurée et utilisée pour un réseau privé virtuel (VPN). Il utilise une connexion client-serveur pour fournir des communications sécurisées entre un serveur et un site client distant sur Internet.

OpenVPN utilise OpenSSL pour le chiffrement des protocoles UDP et TCP pour la transmission du trafic. Un VPN fournit un tunnel de protection sécurisé, qui est moins vulnérable aux pirates car il chiffre les données envoyées depuis votre ordinateur via la connexion VPN. Par exemple, si vous utilisez le Wi-Fi dans un lieu public, par exemple dans un aéroport, il empêche les autres utilisateurs de voir vos données, vos transactions et vos requêtes. Tout comme HTTPS, il chiffre les données envoyées entre deux points d'extrémité.

L'une des étapes les plus importantes de la configuration d'OpenVPN est l'obtention d'un certificat auprès d'une autorité de certification (CA). Ceci est utilisé pour l'authentification. Les certificats sont achetés sur un certain nombre de sites tiers. C'est un moyen officiel de prouver que votre site est sécurisé. Essentiellement, l'AC est une source fiable qui vérifie que vous êtes une entreprise légitime et qu'elle peut être approuvée. Pour OpenVPN, vous n'avez besoin que d'un certificat de niveau inférieur à un coût minime. Vous êtes extrait par l'autorité de certification, et une fois qu'ils vérifient vos informations, ils vous délivrent le certificat. Ce certificat peut être téléchargé sous forme de fichier sur votre ordinateur. Vous pouvez ensuite accéder à votre routeur (ou à votre serveur VPN) et le télécharger ici. Notez que les clients n'ont pas besoin d'un certificat pour utiliser OpenVPN, il s'agit uniquement d'une vérification via le routeur.

Conditions préalables

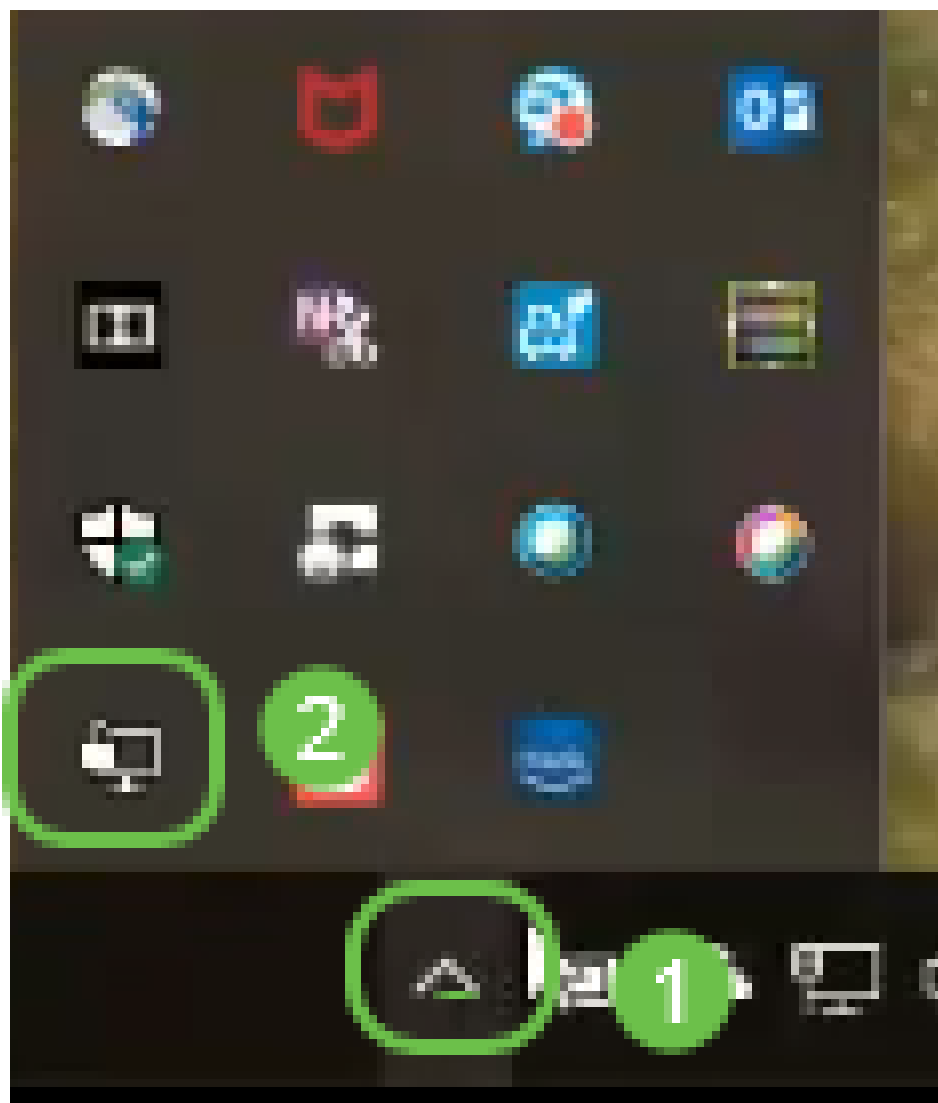
Installez l'application OpenVPN sur votre système. Cliquez [ici](#) pour accéder au site Web OpenVPN.

Pour plus d'informations sur OpenVPN et des réponses à de nombreuses questions, cliquez [ici](#).

Note: Cette configuration est spécifique à Windows 10.



Une fois OpenVPN installé, l'application doit apparaître sur votre bureau ou sous forme d'une petite icône à droite de la barre des tâches. Les clients OpenVPN auront également besoin de cette installation.



Assurez-vous que l'heure système est configurée correctement sur tous les périphériques. L'heure

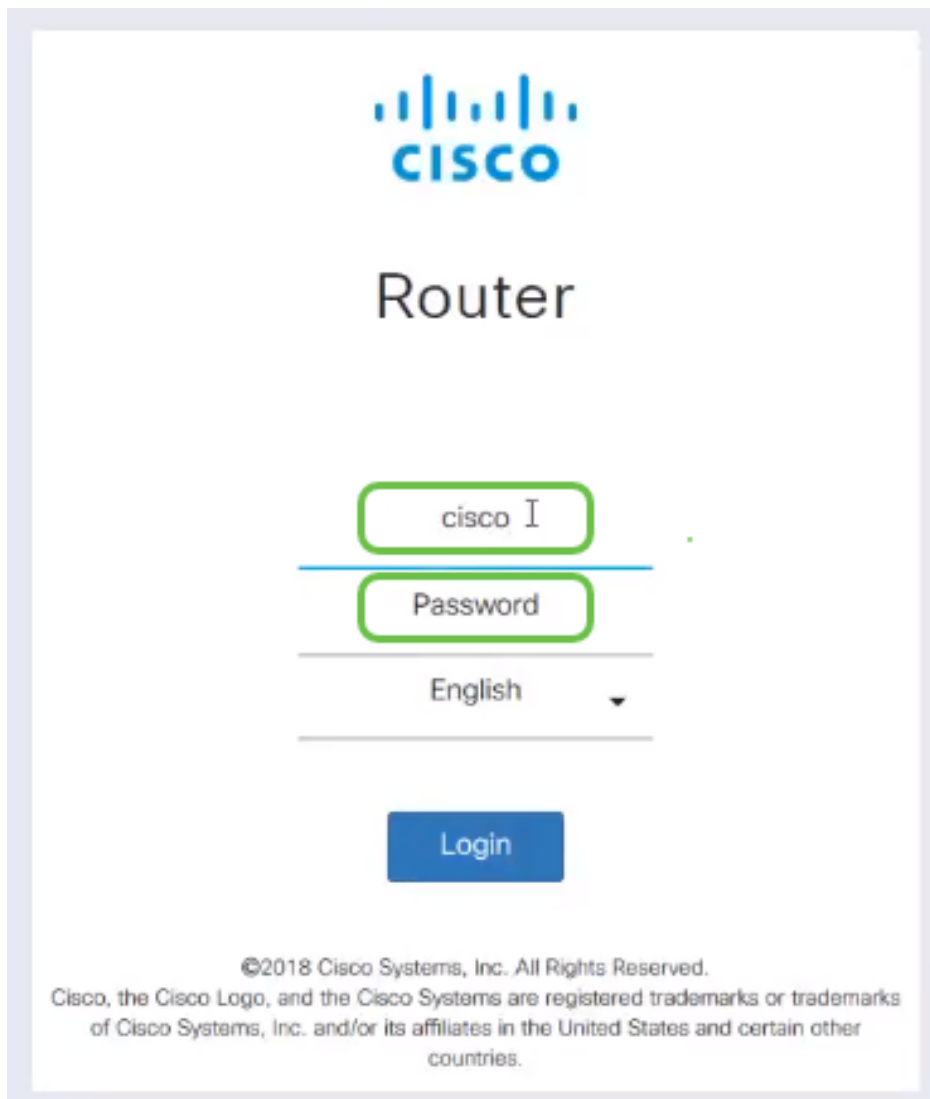
système appropriée doit être entièrement synchronisée au niveau du routeur avant la création d'un certificat. Ceci est souvent fait automatiquement, mais si vous rencontrez des problèmes, c'est un bon endroit pour vérifier.

Configuration d'un OpenVPN de démonstration sur un routeur RV160/RV260

Si vous voulez essayer OpenVPN avant de payer une CA, vous pouvez créer un certificat auto-signé. Il s'agit d'une façon gratuite de voir si OpenVPN est un élément que vous souhaitez déployer pour votre entreprise. Si vous savez déjà que vous souhaitez acheter une CA, vous pouvez ignorer cette section de l'article et accéder directement à [Configuration d'OpenVPN sur un routeur RV160/RV260](#).

Étape 1. Connectez-vous au routeur à l'aide de vos informations d'identification. Le nom d'utilisateur et le mot de passe par défaut sont *cisco*.

Note: Il est fortement recommandé de remplacer tous les mots de passe par quelque chose de plus complexe. Sinon, c'est comme laisser la clé à votre porte verrouillée sur le pas de la porte.



The image shows the Cisco Router login interface. At the top is the Cisco logo. Below it, the word "Router" is displayed. There are three input fields: the first contains "cisco I", the second is labeled "Password", and the third is labeled "English" with a dropdown arrow. A blue "Login" button is centered below these fields. At the bottom, 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."

Étape 2. Vous devez obtenir un certificat sur le routeur. Accédez à **Administration > Certificate > Generate CSR/Certificate...** Voici comment créer la demande de certificat.

RV260-PnP Demo

Alert cisco(admin) English ? i

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 | | |

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

Étape 3. Faites une demande de *certificat CA*.

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

- Sélectionnez *Certificat CA* dans le menu déroulant
- Entrez un nom de certificat
- Saisissez l'adresse IP, le nom de domaine complet (FQDN) ou l'adresse e-mail. La saisie de l'adresse IP est le choix le plus courant.
- Saisissez votre pays
- Entrez votre État
- Saisissez votre nom de localité, généralement votre ville
- Saisissez votre nom d'organisation
- Saisissez le nom de votre unité d'organisation
- Saisissez votre adresse e-mail
- Entrer la longueur de cryptage de clé, 2048 est recommandé

Cliquez sur le bouton **Générer** en haut à droite.

Étape 4. Vous avez également besoin d'un certificat de serveur. Ce *certificat signé par le certificat d'autorité de certification* sera signé par le certificat d'autorité de certification que vous venez de créer.

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...

Étape 5. Demandez un *certificat signé par un certificat CA*.

Generate CSR/Certificate

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:

Buttons: Generate, Cancel

- Sélectionnez *Demande de signature de certificat* dans le menu déroulant
- Entrez un nom de certificat
- Saisissez l'adresse IP, le nom de domaine complet (FQDN) ou l'adresse e-mail. La saisie de l'adresse IP est le choix le plus courant.
- Saisissez votre pays
- Entrez votre État
- Saisissez votre nom de localité, généralement votre ville
- Saisissez votre nom d'organisation
- Saisissez le nom de votre unité d'organisation
- Saisissez votre adresse e-mail
- Entrez la longueur de cryptage de clé, 2048 est recommandé
- Choisissez l'autorité de certification appropriée dans le menu déroulant

Cliquez sur le bouton **Générer** en haut à droite.

Étape 6. Accédez à **Configuration système > Groupes d'utilisateurs**. Sélectionnez l'icône **plus** pour ajouter le nouveau groupe.

User Groups [Apply] [Cancel]

| <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 |

Étape 7. Entrez le nom du groupe, cliquez sur *On* pour activer OpenVPN. Cliquez sur Apply.

User Groups [Apply] [Cancel]

Group Name: (1)

Local User Membership List

+ [trash icon]

User

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

Services

Web Login/NETCONF/RESTCONF: Disable Readonly Admin

Site to Site VPN:

+ [trash icon]

Connection Name

Client to Site VPN:

+ [trash icon]

Group Name

OpenVPN: (2) On Off

PPTP VPN: On Off

802.1x: On Off

Lobby Ambassador: On Off

Étape 8. Naviguez dans le menu Configuration du système et cliquez sur **Comptes d'utilisateurs**. Sous Utilisateurs locaux, cliquez sur l'icône **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)

| 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.

Apply Cancel

Étape 9. Complétez les informations ci-dessous. Veillez à sélectionner OpenVPN dans le menu déroulant. Cliquez sur Apply.

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**

2

Toutes les dépendances sont complètes et le routeur peut maintenant être configuré pour OpenVPN.

Étape 10. Accédez à **VPN > OpenVPN**. La page OpenVPN s'ouvre. Remplissez chaque case de la page, en vous assurant de sélectionner les certificats précédemment créés dans le menu déroulant.

- Cochez la case *Activer*. Sélectionnez l'interface qui va autoriser le trafic. Dans ce cas, sélectionnez un WAN (Wide Area Network) et un certificat d'autorité de certification (CA).
- Sélectionnez le *certificat CA* dans le menu déroulant
- Sélectionnez le certificat de serveur que vous avez téléchargé dans le menu déroulant
- Sélectionnez *Authentification du client*. Si vous sélectionnez Mot de passe, ils doivent s'authentifier avec un mot de passe. Si vous sélectionnez Mot de passe + Certificat, le client doit également posséder un certificat. Ceci est plus sécurisé, mais ajoute au coût du VPN, car il doit acheter une CA distincte.
- Entrez le *pool d'adresses du client*. Choisissez une adresse IP sur un sous-réseau réseau qui n'est utilisé nulle part ailleurs dans l'entreprise. Vous pouvez sélectionner une plage réservée et choisir une plage non utilisée ailleurs.
- Sélectionnez la forme de *chiffrement*. Assurez-vous que le chiffrement est identique au client. DES et 3DES ne sont pas recommandés et ne doivent être utilisés que pour la rétrocompatibilité.
- Sélectionnez Fractionner le tunnel si vous voulez seulement spécifier quel trafic passe par le VPN. Pour un VPN, un tunnel partagé est nécessaire. *Full Tunnel Mode* est sélectionné dans d'autres situations lorsque vous voulez que tout le trafic client passe par le VPN.

Étape 11. Faites défiler la page vers le bas et remplissez le *nom de domaine* et *DNS1*.

Remarque : l'adresse IP DNS1 peut être un serveur DNS interne dédié, la même adresse IP de votre passerelle par défaut fournie par votre fournisseur d'accès Internet (FAI), sur une machine virtuelle ou un serveur DNS de confiance sur Internet.

Étape 12. Cliquez sur **Apply** pour enregistrer la configuration au niveau du routeur.

Étape 13. Restez sur la même page et faites défiler la page. Générez le modèle de configuration à installer sur le client OpenVPN. Ce fichier a une extension *.ovpn* et sera utilisé par le client OpenVPN. Cochez la case pour *Exporter le modèle de configuration du client (.ovpn)* et cliquez sur **Générer**. Le fichier est alors téléchargé sur votre ordinateur.

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

Étape 14. Accédez à **Status and Statistics > VPN Status**. Vous pouvez faire défiler la liste vers le bas pour obtenir des informations plus détaillées.

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

La section suivante de cet article est importante à revoir, car elle explique comment se connecter avec un certificat auto-signé.

Connexion avec un certificat auto-signé après la configuration de Demo OpenVPN

Lorsque vous vous connectez avec un certificat auto-signé, un message d'avertissement s'affiche lorsque vous essayez de vous connecter. Pour continuer, vous devez cliquer sur **Avancé**, **Continuer**, **Approuver** ou une autre option selon votre navigateur Web.

À ce stade, vous pouvez recevoir un avertissement indiquant qu'il n'est pas sûr. Vous pouvez choisir de continuer, d'ajouter une exception ou avancé. Cela varie selon le navigateur Web.

Dans cet exemple, Chrome a été utilisé pour un navigateur Web. Ce message s'affiche, cliquez sur **Avancé**.



Your connection is not private

Attackers might be trying to steal your information from [redacted].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

Un nouvel écran s'ouvre et vous devez cliquer sur **Passer à votre site Web.net (non sécurisé)**

This server could not prove that it is [redacted].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 [redacted].net (unsafe)

Voici un exemple d'accès à l'avertissement de périphérique lors de l'utilisation de Firefox comme navigateur Web. Cliquez sur **Avancé**.


The screenshot shows a Firefox security warning dialog box. At the top left is a red padlock icon with a diagonal slash. To its right is the heading "Your connection is not secure". Below this, a paragraph explains that the website owner has configured the site improperly and that Firefox has not connected to protect information. There is a "Learn more..." link. Below that is a checkbox for reporting errors to Mozilla. At the bottom right are two buttons: "Go Back" (blue) and "Advanced" (green with a white border).

Cliquez sur **Ajouter une exception...**

The screenshot shows a Firefox security exception dialog box. It contains the text: "[redacted].net:50 uses an invalid security certificate. The certificate is not trusted because it is self-signed. The certificate is only valid for .". Below this is the error code: "Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT". At the bottom right is a green button with a white border labeled "Add Exception...".

Enfin, vous devrez cliquer sur **Confirmer l'exception de sécurité**.

Add Security Exception ✕

 You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location:

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

Permanently store this exception

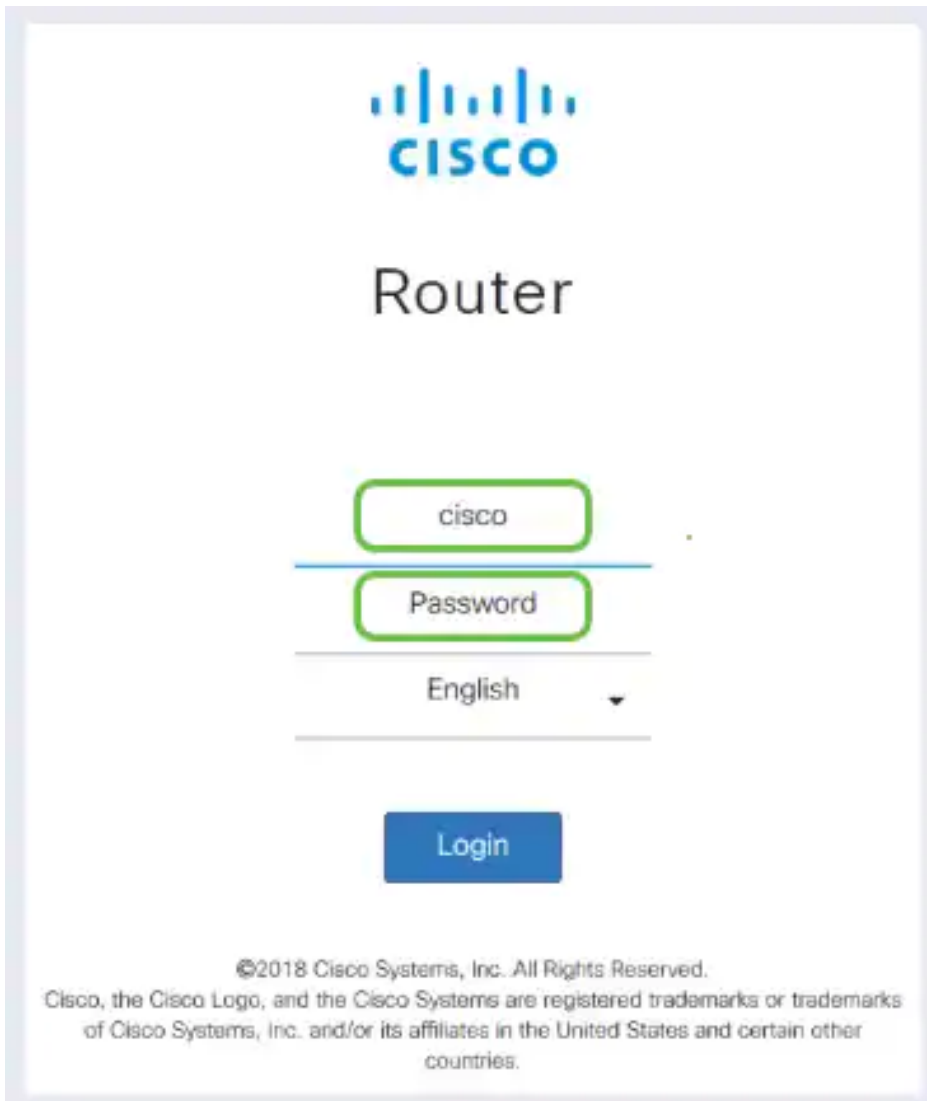
Le routeur est maintenant configuré avec tous les paramètres nécessaires pour prendre en charge une connexion OpenVPN Client. Comme vous avez déjà téléchargé le modèle de configuration client sur votre périphérique, celui qui se termine dans `.ovpn`, vous pouvez passer à la section [Configuration du client OpenVPN sur l'ordinateur](#). Si vous décidez de déployer OpenVPN pour votre entreprise, vous pouvez suivre les étapes de cette section suivante.

Configuration d'OpenVPN sur un routeur RV160/RV260

Il s'agit d'un processus plus compliqué, car il s'agit d'obtenir une AC d'un tiers, ce qui coûte de l'argent. Vous devez également envoyer le modèle de configuration du client VPN, se terminant par `.ovpn`, à tous les clients afin qu'ils puissent configurer leur périphérique. Les clients ont besoin de plusieurs paramètres identiques au routeur pour pouvoir communiquer. Le meilleur, c'est que pour un coût minimal, vous et vos employés pouvez utiliser Internet et mener vos affaires en toute sécurité.

Étape 1. Connectez-vous au routeur à l'aide de vos informations d'identification. Le nom d'utilisateur et le mot de passe par défaut sont `cisco`.

Note: Il est fortement recommandé de remplacer tous les mots de passe par quelque chose de plus complexe. Sinon, c'est comme laisser la clé à votre porte verrouillée sur le pas de la porte.



Étape 2. Vous devez obtenir un certificat. Accédez à **Administration > Certificate > Generate CSR/Certificate...** Voici comment créer la demande de certificat.

The image shows the Cisco Router's Certificate management interface. The left sidebar contains a menu with "Administration" (1) and "Certificate" (2) highlighted. The main area displays a "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 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 | | |

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

Étape 3. Demandez un *certificat signé par un certificat CA*. Pour cela, accédez à **Administration > Certificate**.

- Sélectionnez *Demande de signature de certificat* dans le menu déroulant
- Entrez un nom de certificat
- Saisissez l'adresse IP, le nom de domaine complet (FQDN) ou l'adresse e-mail. La saisie de l'adresse IP est le choix le plus courant.
- Saisissez votre pays
- Entrez votre État
- Saisissez votre nom de localité, généralement votre ville
- Saisissez votre nom d'organisation
- Saisissez le nom de votre unité d'organisation
- Saisissez votre adresse e-mail
- Entrer la longueur de cryptage de clé, 2048 est recommandé

Cliquez sur le bouton supérieur droit **Générer**

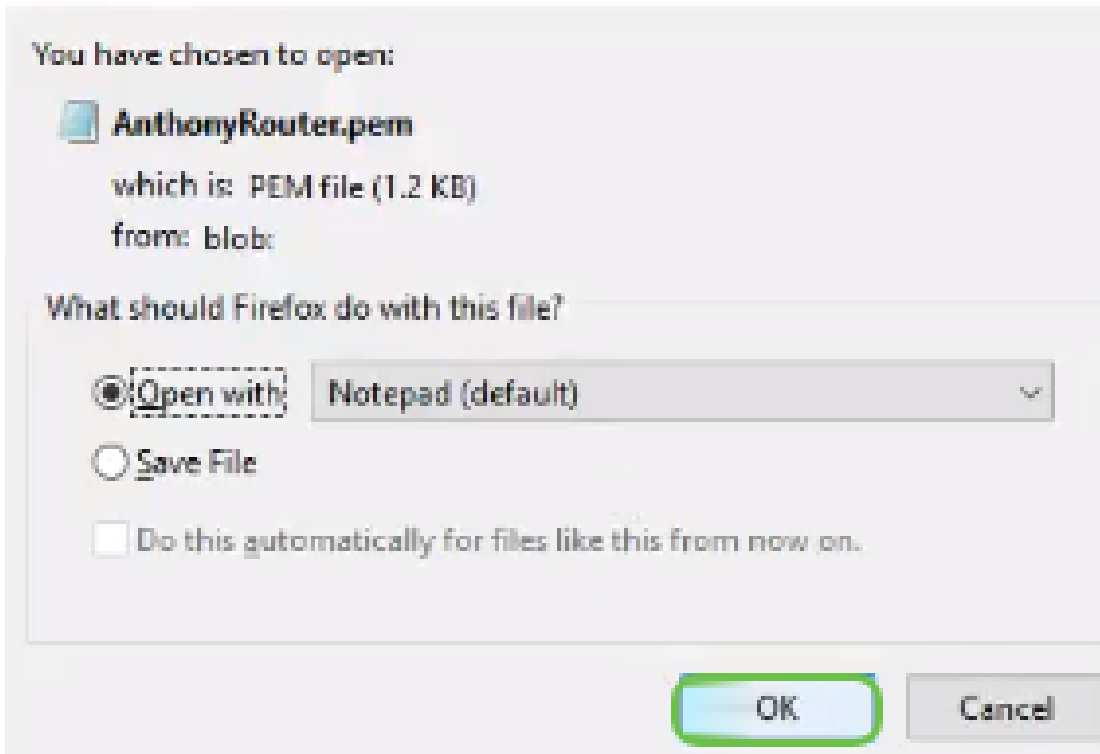
Étape 4. Sélectionnez cette option pour l'exporter en cliquant sur la flèche vers le haut sous Action.

| 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 | CertTest_CA | - | 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 | AnthonyRouterImport | - | Local Certificate | CiscoTest-DC1-CA | From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00 | | |

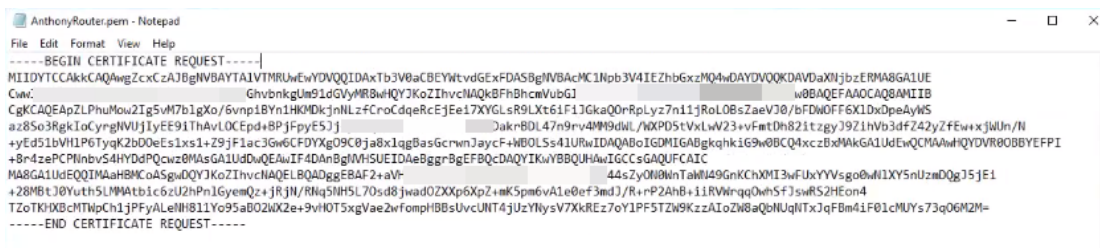
Étape 5. Cet écran s'affiche. Cliquez sur **Exporter**.

Étape 6. Sélectionnez *Ouvrir avec et Bloc-notes* (par défaut) dans le menu déroulant. Click OK.

Opening AnthonyRouter.pem

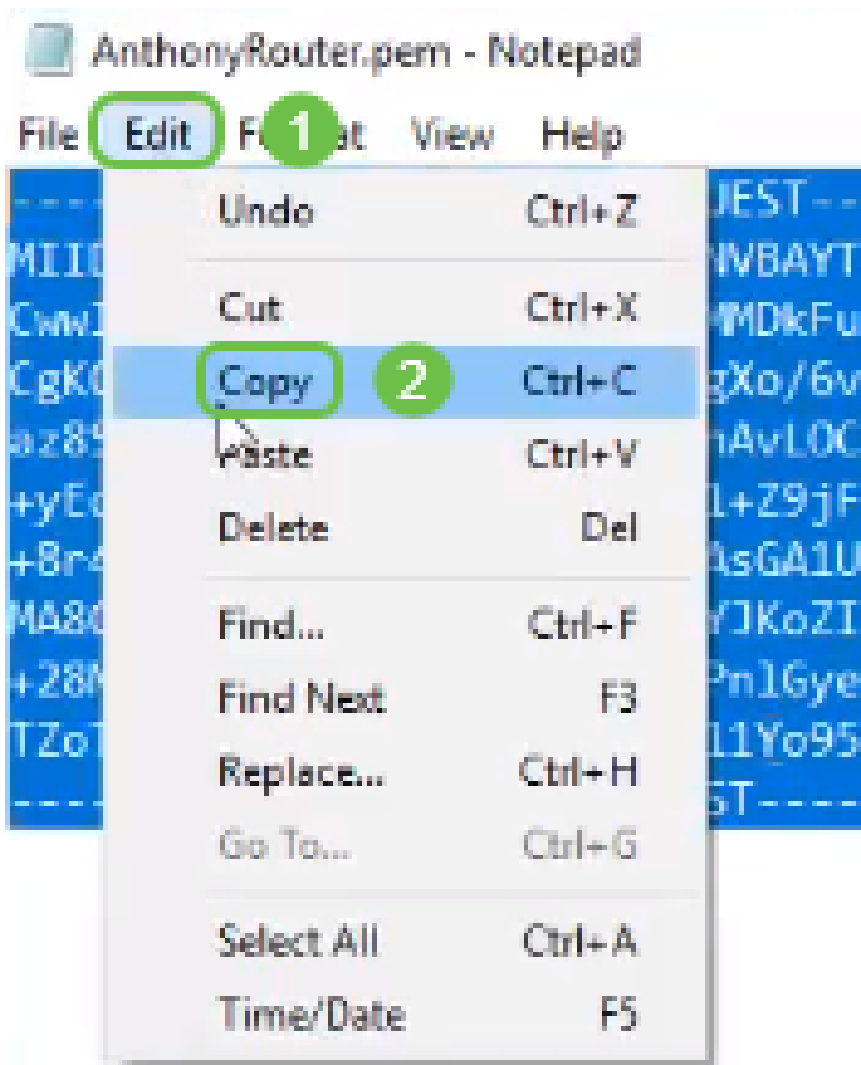


Étape 7. Un fichier XML s'ouvre.



Note: Assurez-vous que la DEMANDE DE CERTIFICAT DE DÉBUT et la DEMANDE DE CERTIFICAT DE FIN se trouvent chacune sur leurs propres lignes, comme indiqué ci-dessus.

Étape 8. En haut de l'écran, cliquez sur **Modifier** et sélectionnez **Copier** dans le menu déroulant.



Étape 9. Choisissez un site tiers réputé pour faire la demande de certificat. Vous devez coller le fichier XML copié dans le cadre de la demande.

Note: Si vous avez un serveur de certificats interne sur votre réseau, vous pouvez l'utiliser à la place, mais ce n'est pas courant.

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):

```
TZoTKHXBcMTWpCh1jPFy8LeNH811Yo95aBO2WX2e  
cUNT4jUzYNyaV7XkREz7oY1PF5TZW9KzzAIo2W8a  
3qO6K2M=  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

Étape 10. Une fois que vous avez été vérifié, vous pouvez choisir *Télécharger le certificat*.

Certificate Issued

The certificate you requested was issued to you.

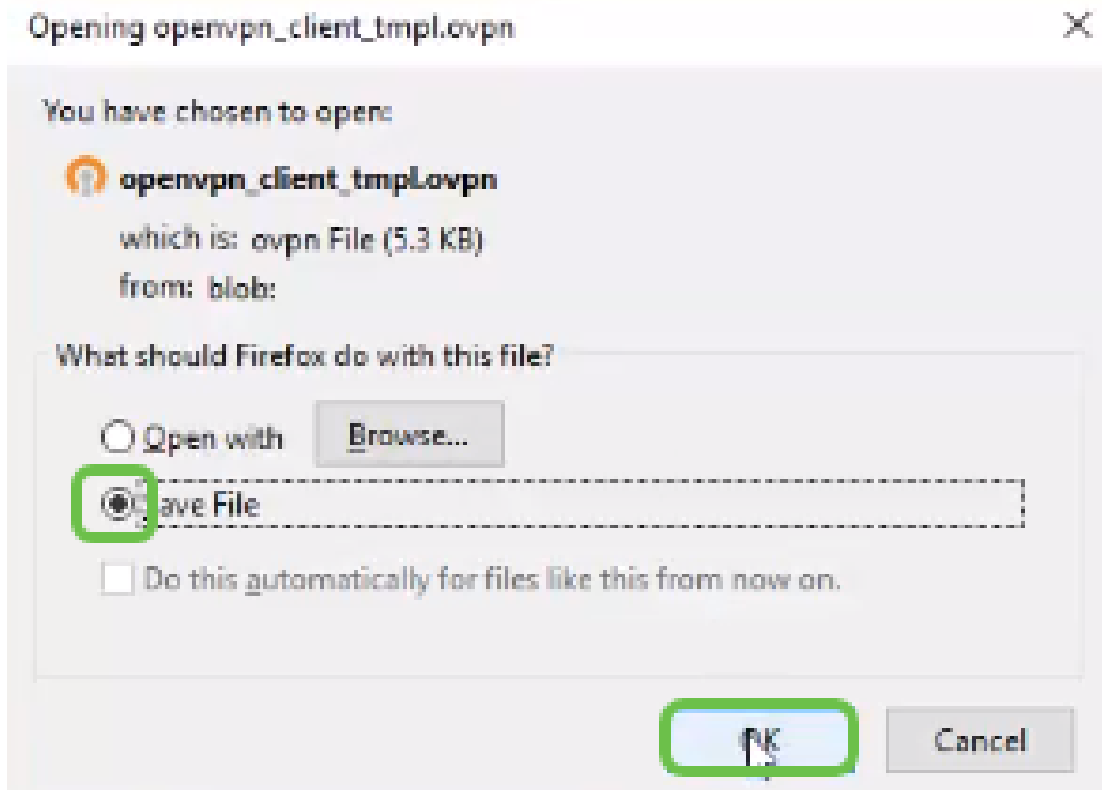
DER encoded or Base 64 encoded



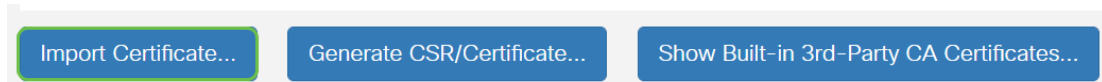
[Download certificate](#)

[Download certificate chain](#)

Étape 11. Activez la case d'option pour *enregistrer le fichier* et cliquez sur **OK**.



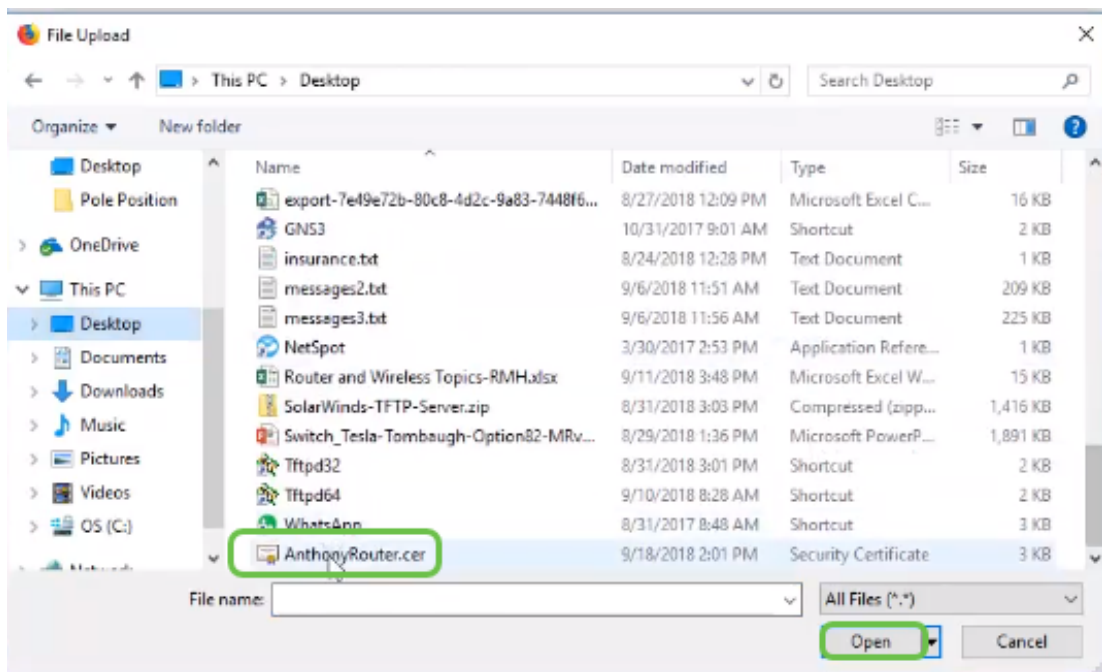
Étape 12. Une fois enregistré, sélectionnez la case d'option correspondant à ce certificat et cliquez sur l'icône **flèche vers le bas**.



Étape 13. Cet écran s'ouvre. Sélectionnez **Parcourir....**



Étape 14. Choisissez le fichier du certificat et cliquez sur **Ouvrir**.



Étape 15. Entrez le *nom du certificat* à importer et cliquez sur **Télécharger**.

Import Signed-Certificate

Type: Local Certificate

Certificate Name:

Upload Certificate file

Import from PC

Browse...

AnthonyRouter.cer

Import from USB



Browse...

No file is selected

Upload

Cancel

Étape 16. Vous recevrez une notification indiquant que le certificat a été importé avec succès. Click OK.

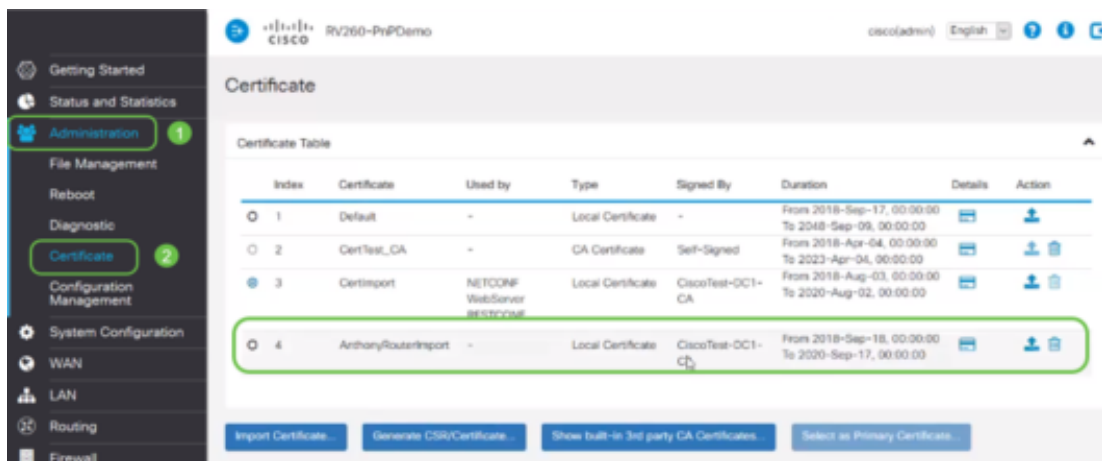
Information

Import certificate successfully!

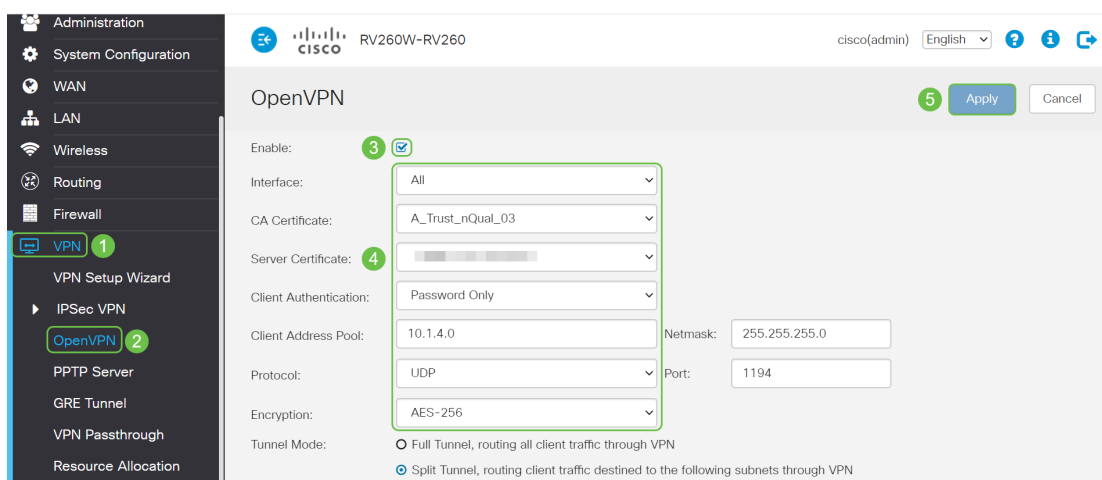
OK

Étape 17. Accédez à **Administration > Certificate**. Le certificat a été chargé.

Note: Dans cet exemple, un serveur de certificats local a été utilisé.



Étape 18. Accédez à **VPN > OpenVPN**. La page OpenVPN s'ouvre. Complétez ce qui suit avec vos informations.



- Cochez la case *Activer*. Sélectionnez l'interface qui va autoriser le trafic. Dans ce cas, un réseau étendu (WAN) et sélectionnez un certificat d'autorité de certification (CA)
- Sélectionnez le *certificat CA* dans le menu déroulant
- Sélectionnez le *certificat serveur* que vous avez téléchargé dans le menu déroulant
- Sélectionnez *Authentification du client*. Si vous sélectionnez Mot de passe, ils doivent s'authentifier avec un mot de passe. Si vous sélectionnez Mot de passe + Certificat, le client doit également posséder un certificat. Ceci est plus sécurisé, mais ajoute au coût du VPN, car il doit acheter une CA distincte.
- Entrez le *pool d'adresses du client*. Choisissez une adresse IP sur un sous-réseau réseau qui n'est utilisé nulle part ailleurs dans l'entreprise. Vous pouvez sélectionner une plage réservée et choisir une plage non utilisée ailleurs.
- Sélectionnez la forme de *chiffrement*. Assurez-vous que le chiffrement est identique au client. DES et 3DES ne sont pas recommandés et ne doivent être utilisés que pour la rétrocompatibilité.
- Choisissez *Full Tunnel Mode* si vous voulez que tout le trafic client passe par le VPN ou le tunnel partagé si vous voulez seulement spécifier quel trafic passe par le VPN
- L'adresse IP *DNS1* peut être un serveur DNS interne dédié, la même adresse IP de votre passerelle par défaut fournie par votre fournisseur d'accès Internet (FAI), sur une machine virtuelle ou un serveur DNS de confiance sur Internet.

Cliquez sur **Apply** pour enregistrer la configuration.

Étape 19 (Option 1). Vous pouvez envoyer cette configuration par e-mail au client. Cochez la case *Envoyer un e-mail*. Saisissez une adresse e-mail. Ajoutez un titre *Objet* pour l'e-mail. Cliquez sur **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. 2

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): nick@cisco.com 3

Email Subject: OpenVPN Client Config

4 **Generate**

Étape 20. (Option 2). Sélectionnez *Exporter le modèle de configuration du client (.ovpn)* et cliquez sur **Générer**.

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 **Generate**

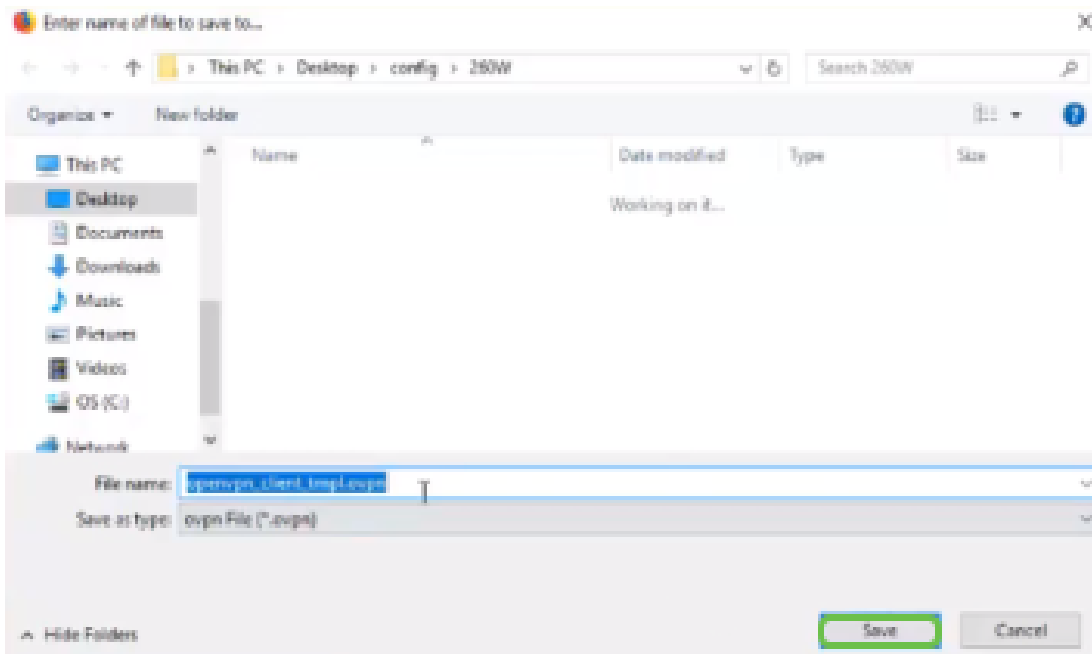
Étape 21. Vous recevrez une confirmation de réussite. Cliquez OK.

Information

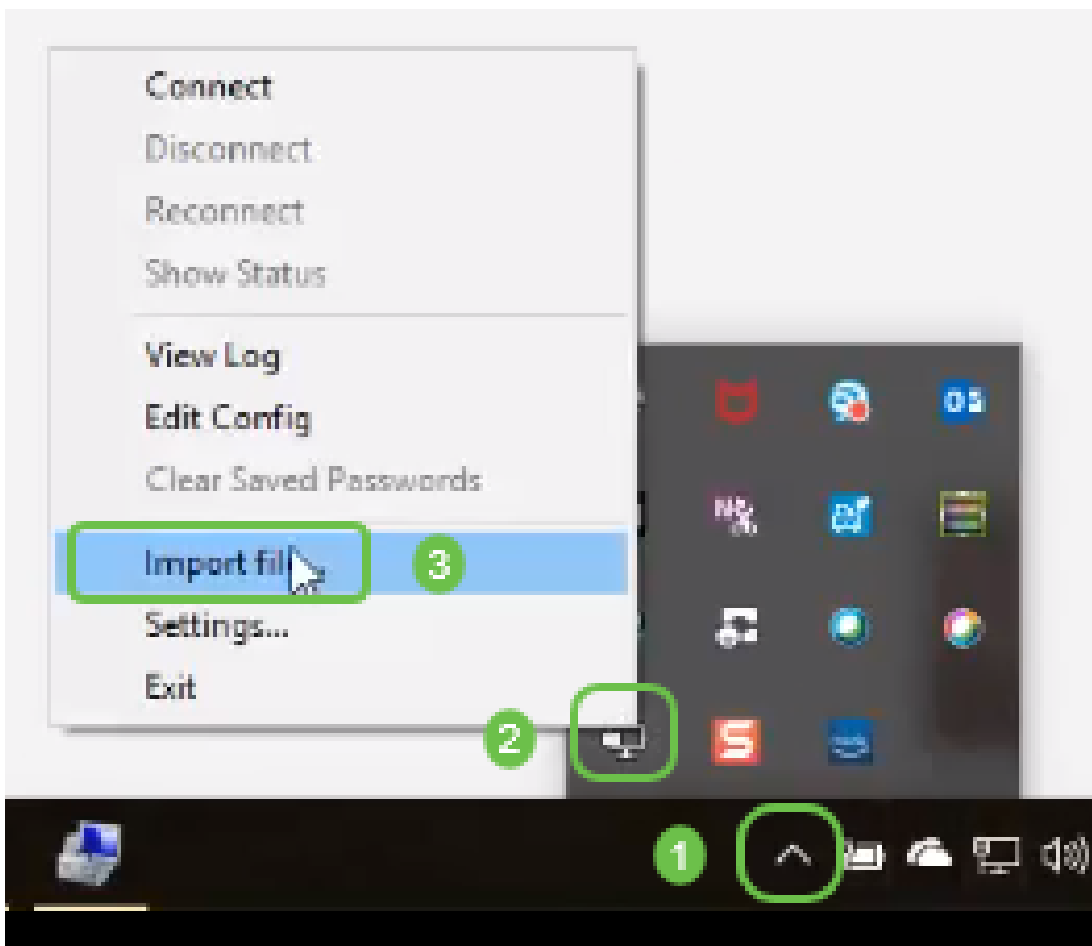
 Export client configuration template downloaded successfully!

OK

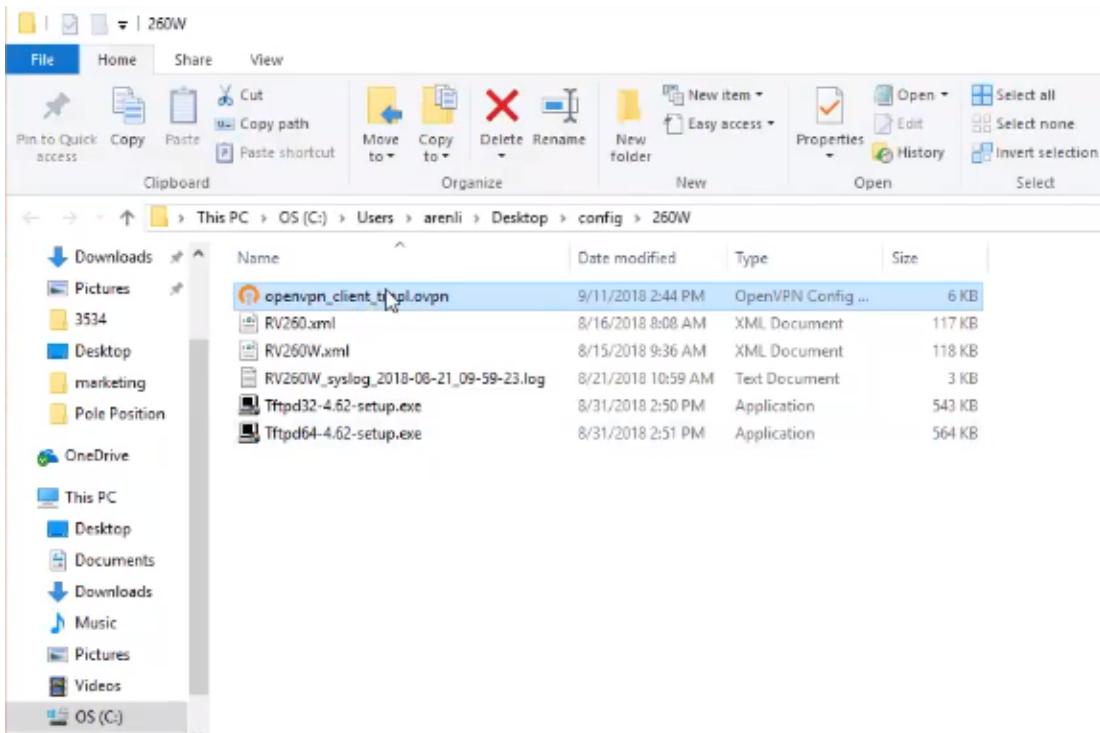
Étape 22. Cliquez **Save**.



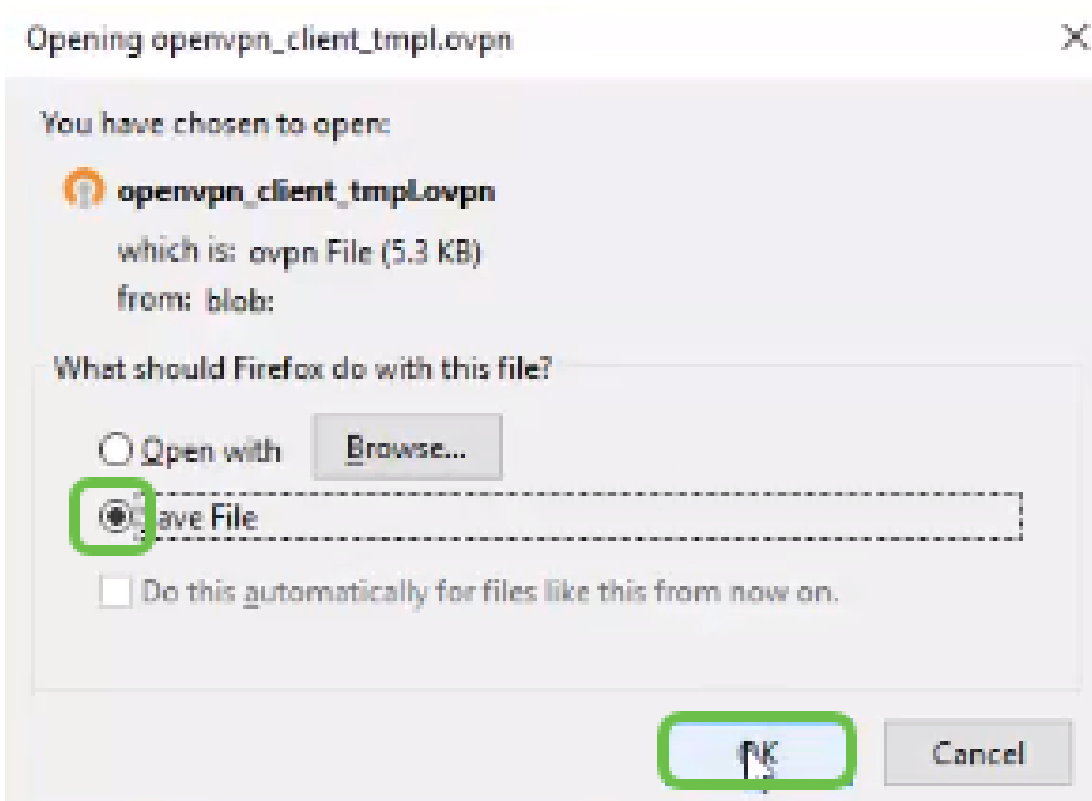
Étape 23. En bas à droite de votre bureau et cliquez pour ouvrir OpenVPN. Cliquez avec le bouton droit de la souris pour ouvrir le menu déroulant. Cliquez sur *Importer le fichier*.



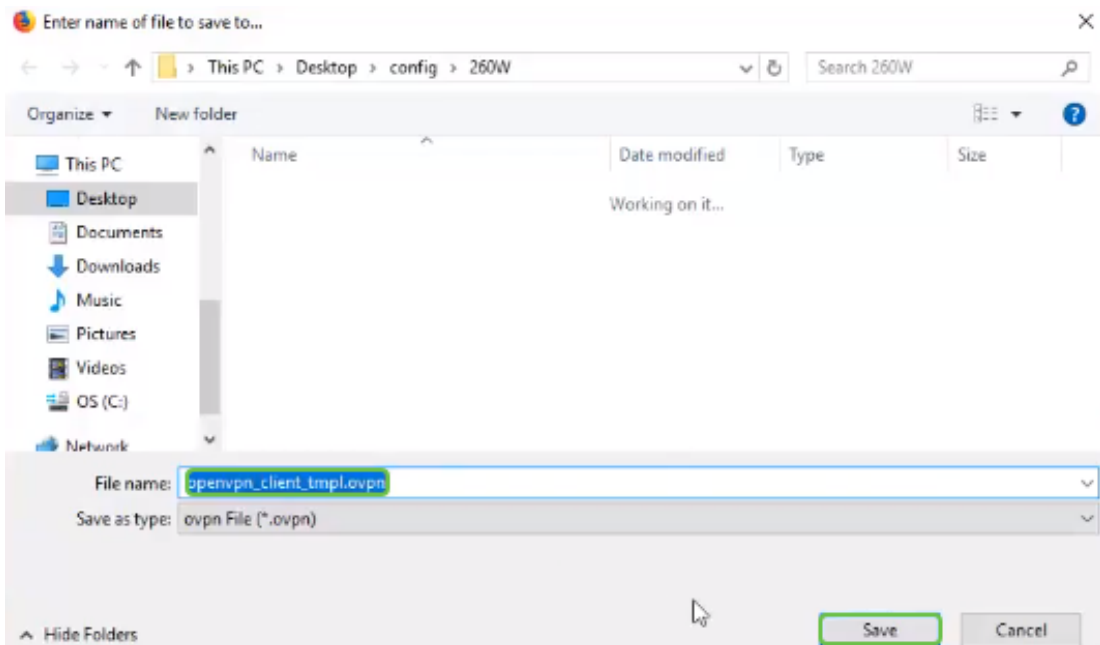
Étape 24. Sélectionnez le fichier OpenVPN qui se termine dans *.ovpn*.



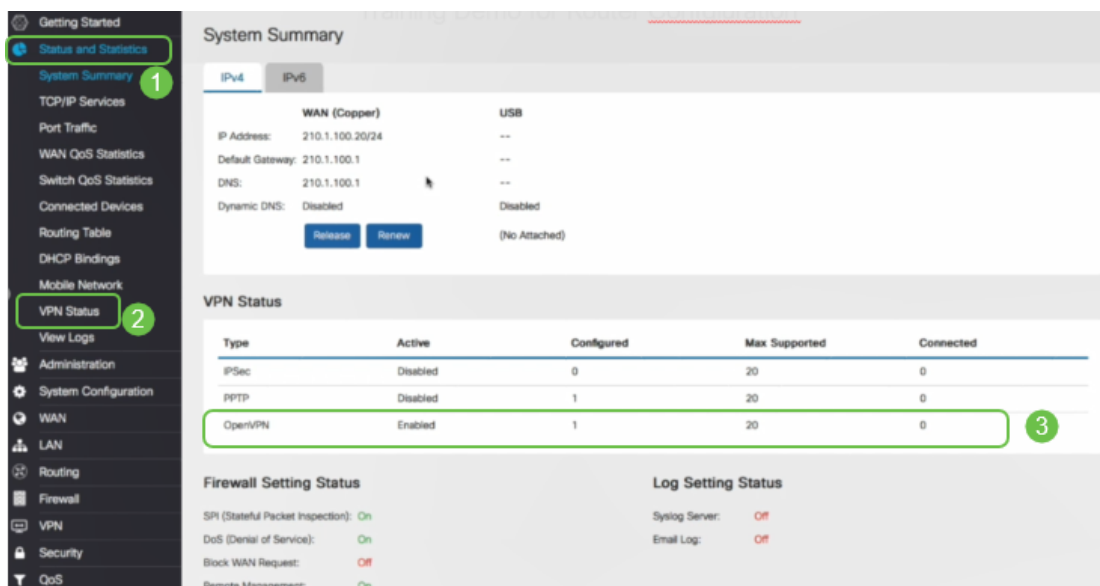
Étape 25. Activez la case d'option *Enregistrer le fichier* et cliquez sur **OK**.



Étape 26. Modifiez le nom du fichier si vous le souhaitez, mais laissez *.ovpn* à la fin du nom du fichier. Cliquez **Save**.



Étape 27. Accédez à **Status and Statistics > VPN Status**. Vous pouvez faire défiler la liste vers le bas pour obtenir des informations plus détaillées.



Le routeur est maintenant configuré avec tous les paramètres nécessaires pour prendre en charge une connexion OpenVPN Client pour votre évaluation personnelle.

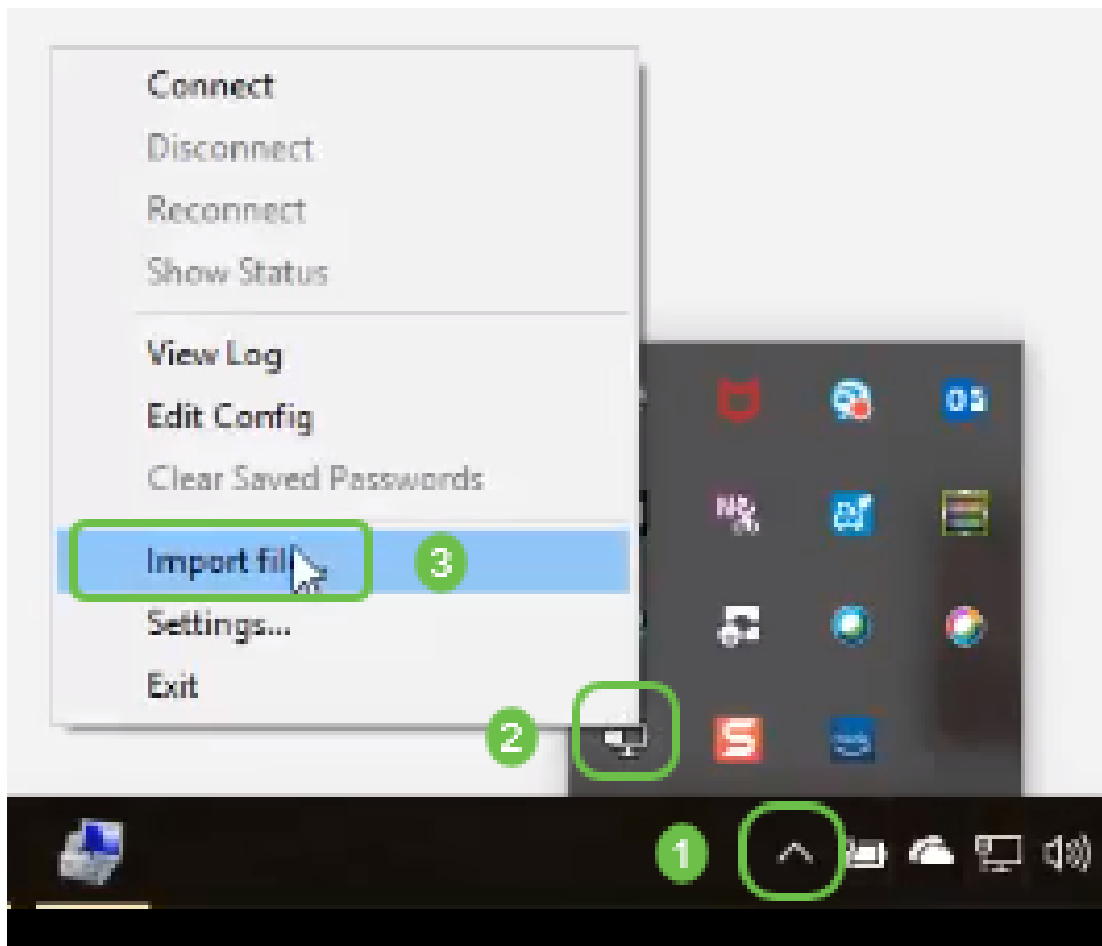
Configuration du client OpenVPN sur l'ordinateur

Chaque client OpenVPN doit effectuer les tâches suivantes comme condition préalable :

- Téléchargez l'application OpenVPN sur votre périphérique.
- Ouvrez et enregistrez le fichier de configuration qui a été envoyé aux étapes 19 à 22 de la section précédente. Le fichier de configuration se termine dans *.ovpn*.

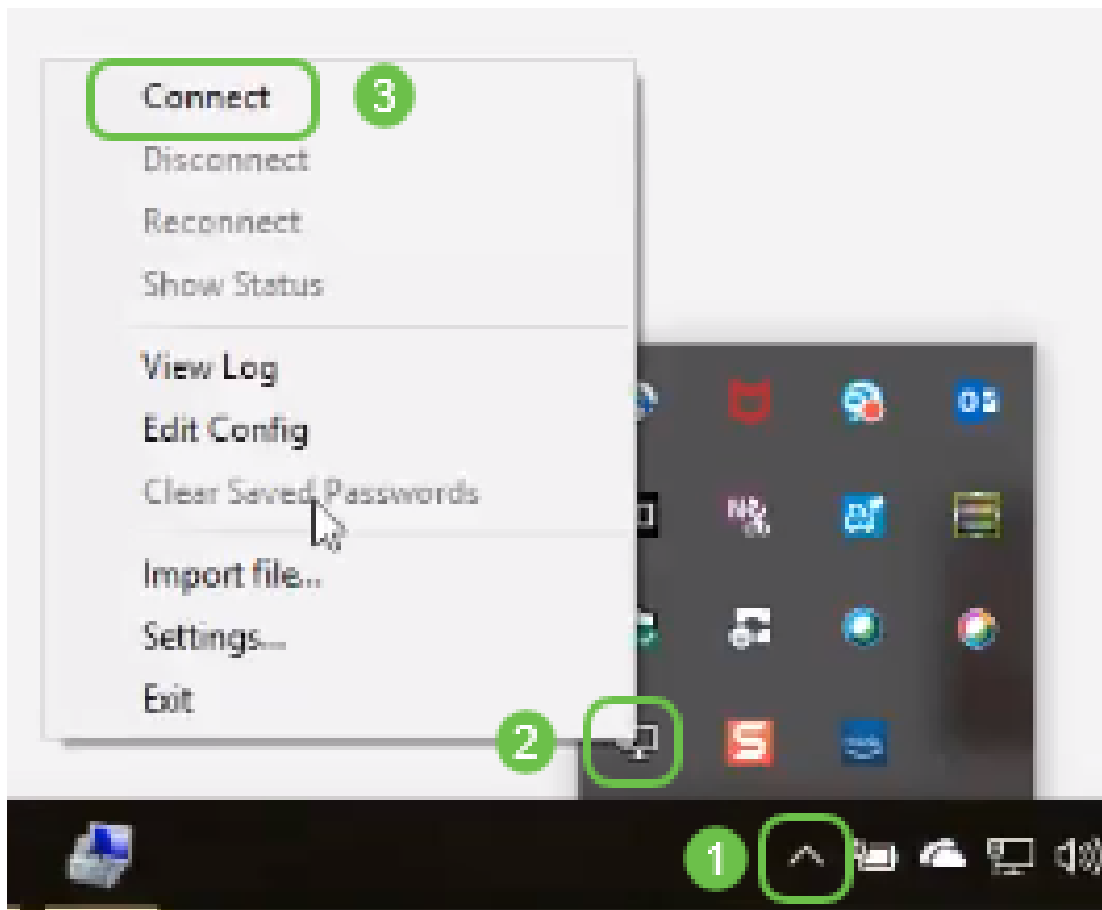
Note: Cette configuration est spécifiquement destinée à Windows 10.

Étape 1. Accédez à l'icône représentant une flèche située en bas à droite du bureau et cliquez sur pour ouvrir l'icône OpenVPN. Cliquez avec le bouton droit de la souris et sélectionnez *Importer un fichier*.

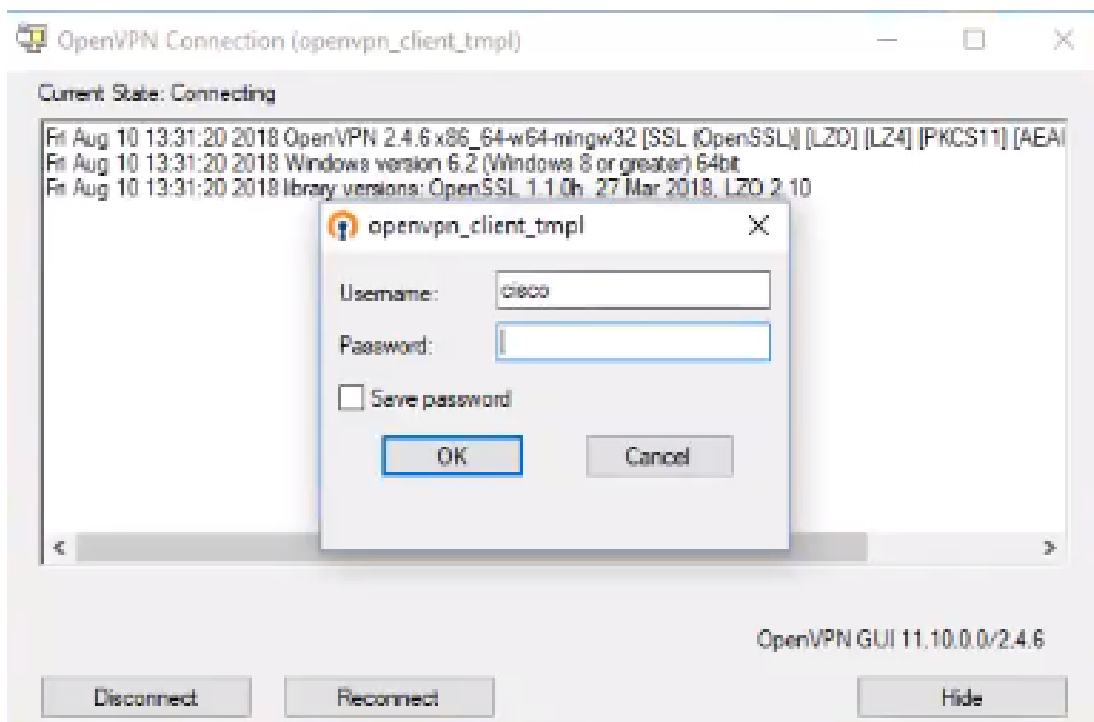


Note: L'icône est en noir et blanc, ce qui indique qu'elle n'est pas en cours d'exécution. Une fois qu'elle est en cours d'exécution, l'icône s'affiche en couleur.

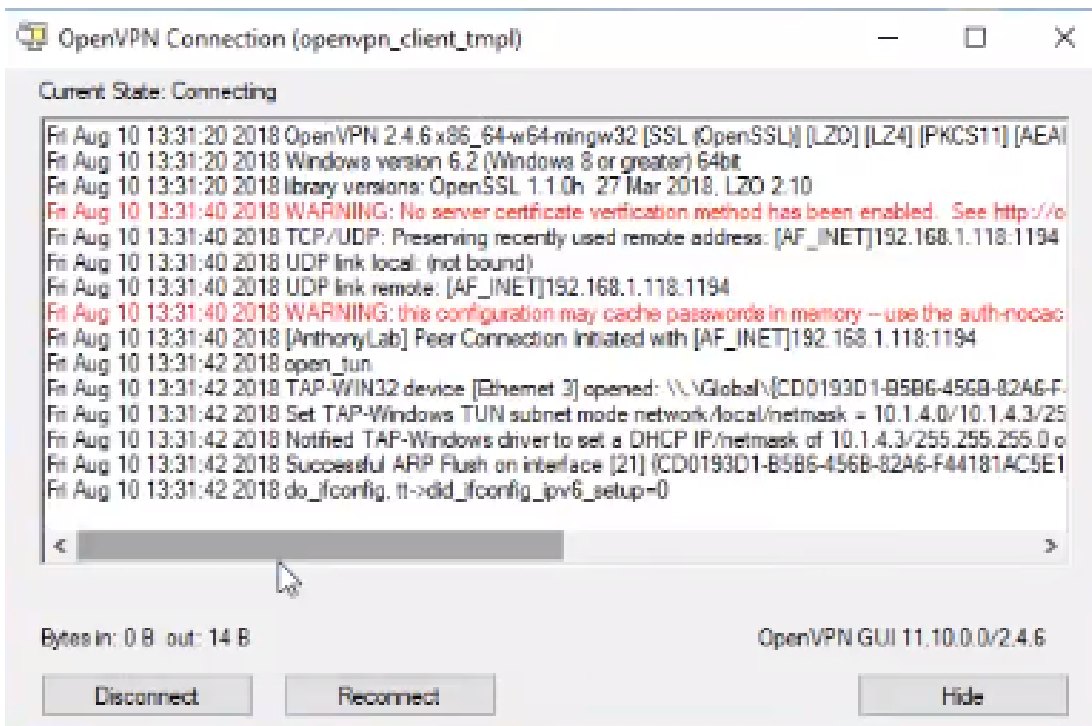
Étape 2. Cliquez sur la *flèche vers le haut*. Cliquez sur l'icône OpenVPN. Cliquez avec le bouton droit de la souris et sélectionnez *Connexion* dans le menu déroulant.



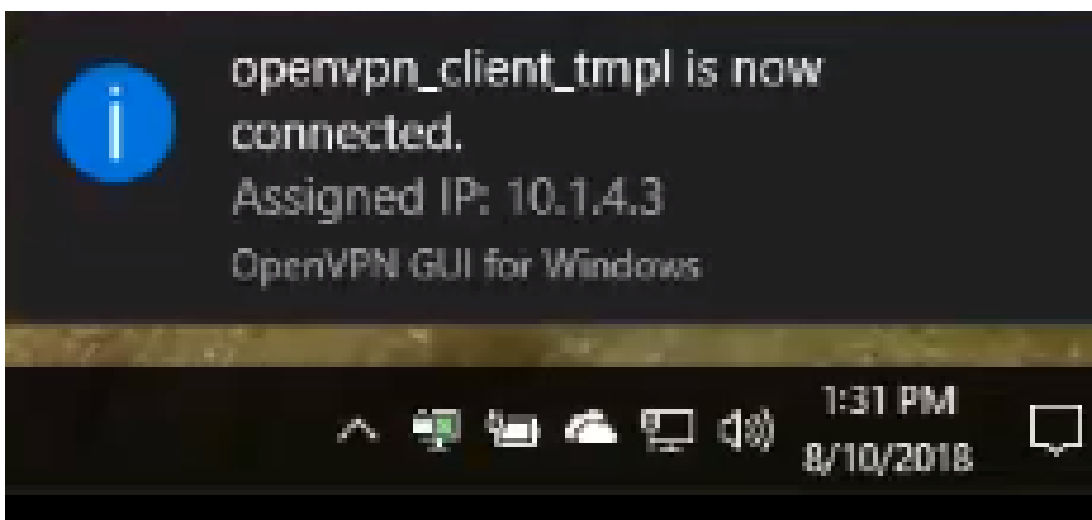
Étape 3. Saisissez le nom d'utilisateur et mot de passe.



Étape 4. La fenêtre affiche la connexion OpenVPN ainsi que certaines données de journal.

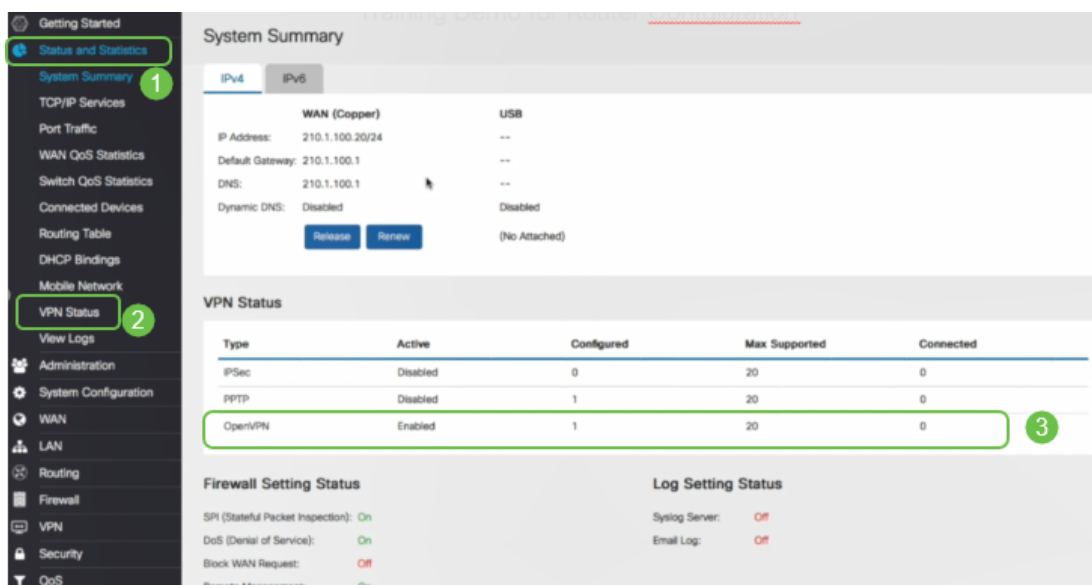


Étape 5. Un journal système doit signaler qu'il existe une connexion.



Étape 6. Le client VPN doit être en mesure de tunnel les informations entrantes et sortantes via OpenVPN. Il est possible de configurer la connexion automatique dans les paramètres OpenVPN.

Étape 7. L'administrateur peut confirmer l'état du VPN en accédant à **Status and Statistics > VPN Status** sur le routeur.



Conclusion

Vous devez maintenant avoir correctement installé OpenVPN sur votre routeur RV160 ou RV260 et sur le site client VPN.

Pour les discussions de communauté sur OpenVPN, cliquez [ici](#) et faites une recherche pour OpenVPN.

[Afficher une vidéo relative à cet article...](#)

[Cliquez ici pour afficher d'autres présentations techniques de Cisco](#)