

RV160和RV260路由器上的OpenVPN

目标

本文的目的是指导您在RV160或RV260路由器上设置OpenVPN，以及在计算机上设置OpenVPN的VPN客户端。

适用设备

- RV160
- RV260

软件版本

- 1.0.00.15

目录

[在RV160/RV260路由器上设置演示OpenVPN](#)

[在RV160/RV260路由器上设置OpenVPN](#)

[在设置演示OpenVPN后使用自签名证书登录](#)

[计算机上的OpenVPN客户端设置](#)

简介

OpenVPN是可设置并用于虚拟专用网络(VPN)的免费开源应用。它使用客户端 — 服务器连接在服务器和远程客户端位置之间通过互联网提供安全通信。

OpenVPN使用OpenSSL加密UDP和TCP以传输流量。VPN提供安全的保护隧道，由于它通过VPN连接加密从您的计算机发送的数据，因此不易受到黑客攻击。例如，如果您在公共场所（如机场）使用WiFi，则会阻止其他用户看到您的数据、交易和查询。与HTTPS非常相似，它加密两个端点之间发送的数据。

设置OpenVPN的最重要步骤之一是从证书颁发机构(CA)获取证书。这用于身份验证。从任意数量的第三方站点购买证书。这是证明您的站点是安全的官方方式。本质上，CA是可信赖的来源，用于验证您是合法企业且可信。对于OpenVPN，您只需以最低成本获得较低级别的证书。CA会签出您，一旦他们验证您的信息，他们会向您颁发证书。此证书可以作为文件下载到您的计算机上。然后，您可以进入路由器（或VPN服务器）并上传它。请注意，客户端使用OpenVPN时不需要证书，它只是通过路由器进行验证。

先决条件

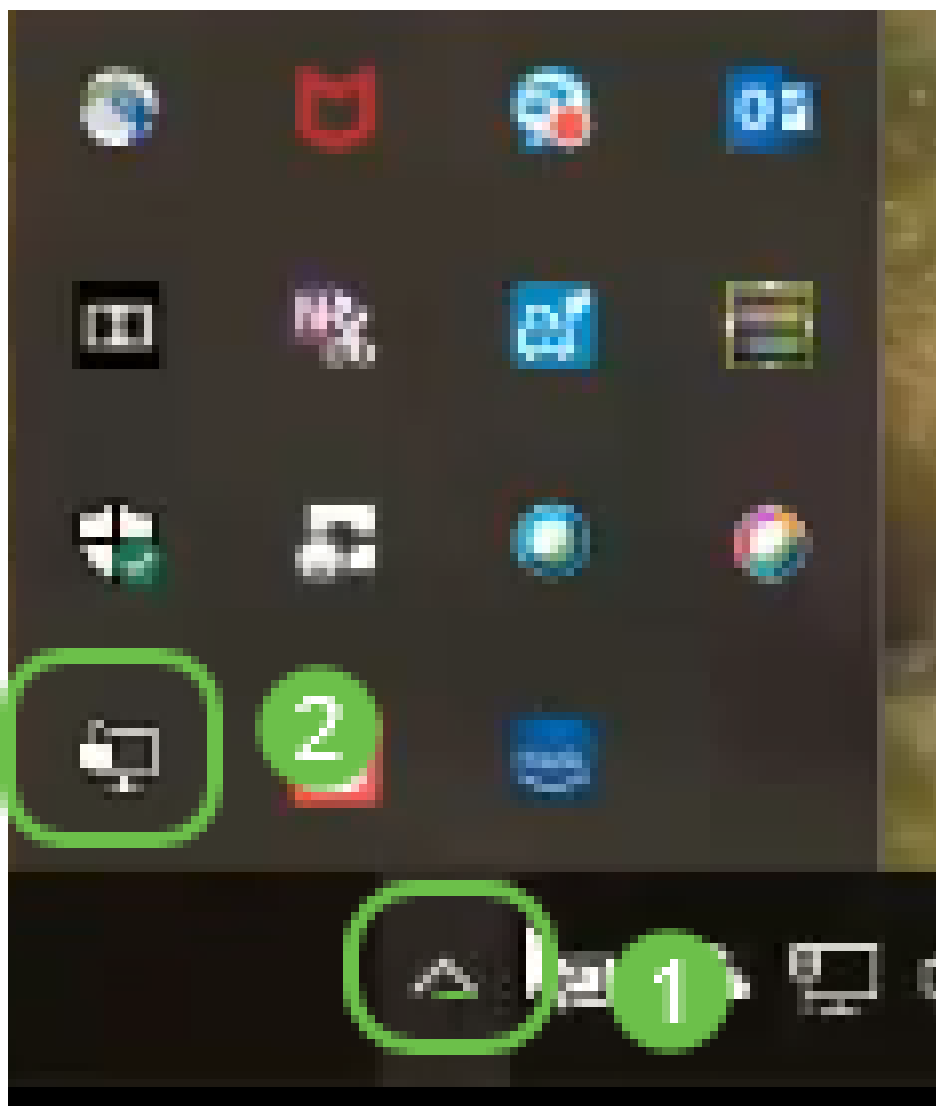
将OpenVPN应用安装到系统。单击[此处](#)转到OpenVPN网站。

有关OpenVPN的详细信息以及您可能遇到的许多问题的答案，请单击[此处](#)。

注意：此设置特定于Windows 10。



安装OpenVPN后，应用程序应显示在桌面上或任务栏右侧的小图标上。OpenVPN客户端也需要安装此。



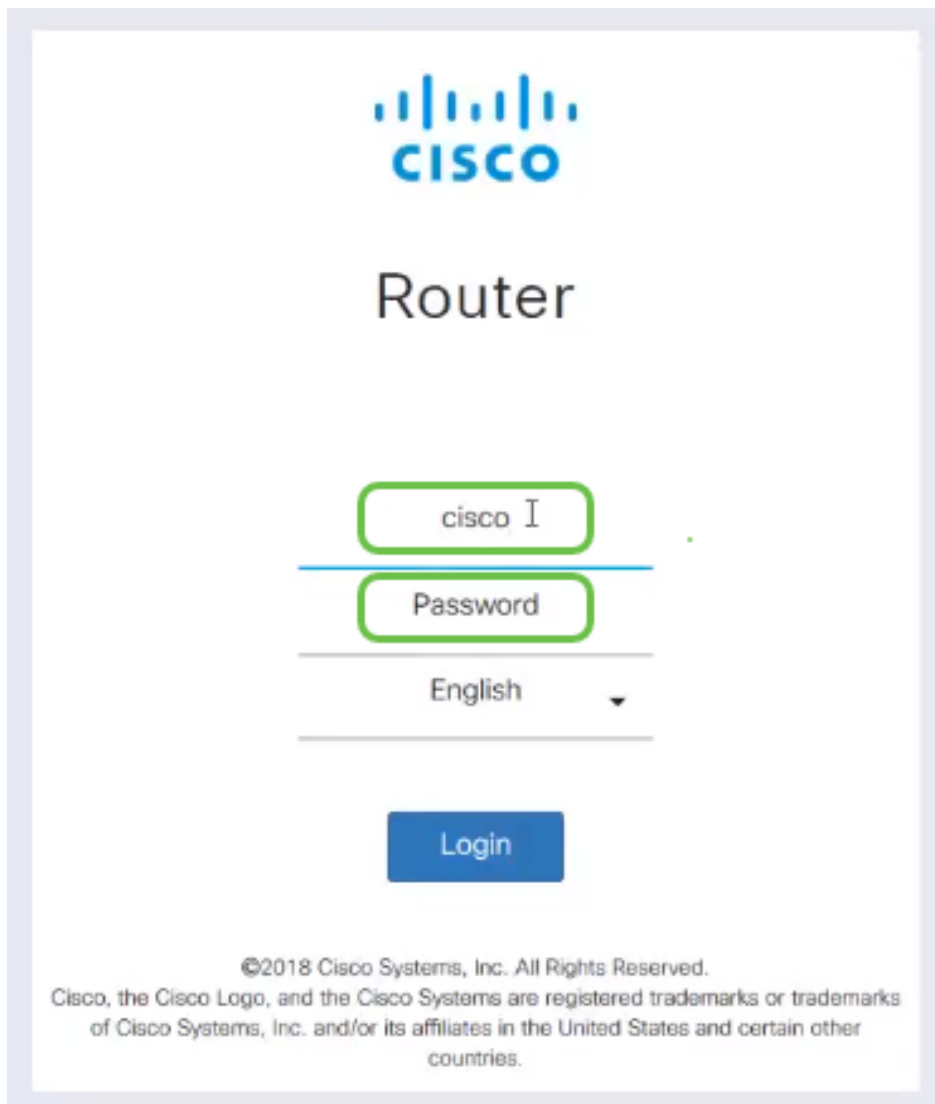
确保在所有设备上设置正确的系统时间。创建证书之前，必须在路由器上完全同步正确的系统时间。这通常是自动完成的，但如果遇到问题，这是检查的好地方。

在RV160/RV260路由器上设置演示OpenVPN

如果要在为CA支付费用之前尝试OpenVPN，可以创建自签名证书。这是查看OpenVPN是否是您希望为您的企业部署的免费方式。如果您已经知道要购买CA，可以跳过本文的此部分，直接转到[在RV160/RV260路由器上设置OpenVPN](#)。

步骤1.使用您的凭证登录路由器。默认用户名和密码为cisco。

注意：强烈建议您将所有密码更改为更复杂的密码。否则，就像把钥匙丢到门口上锁的门上一样。



步骤2.您需要在路由器上获取证书。导航至管理 > 证书 > 生成CSR/证书.....这是如何创建证书请求



步骤3.请求CA证书。

- 从下拉菜单中选择CA Certificate
- 输入证书名称
- 输入IP地址、完全限定域名(FQDN)或电子邮件。输入IP地址是最常见的选择。
- 输入您所在的国家/地区
- 输入您的省/自治区
- 输入您所在地的名称，通常是您所在的城市
- 输入您的组织名称
- 输入您的组织单位名称
- 输入您的电子邮件地址
- 输入密钥加密长度，建议使用2048

单击右上角的“生成”按钮。

步骤4.您还需要服务器证书。此由CA证书签名的证书将由您刚创建的CA证书签名。

步骤5.请求CA证书签名的证书。

- 从下拉菜单中选择证书签名请求
- 输入证书名称
- 输入IP地址、完全限定域名(FQDN)或电子邮件。输入IP地址是最常见的选择。
- 输入您所在的国家/地区
- 输入您的省/自治区
- 输入您所在地的名称，通常是您所在的城市
- 输入您的组织名称
- 输入您的组织单位名称
- 输入您的电子邮件地址
- 输入密钥加密长度，建议使用2048
- 从下拉菜单中选择适当的证书颁发机构

单击右上角的“生成”按钮。

步骤6. 导航至System Configuration > User Groups。选择加号图标以添加新组。

Group	Web Login /NETCONF /RESTCONF	Lobby Ambassa...	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP	Captive Portal
Ambassa...	Disable	Enable	Disable	Disable	Disable	Disable	Disable	Enable
admin	Admin	Enable	Enable	Enable	Enable	Enable	Enable	Enable
guest	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable

步骤7. 输入组名称，单击单选按钮On以打开OpenVPN。单击 Apply。

User Groups 3 Apply Cancel

Group Name: 1

Local User Membership List

+ 🗑️

<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:

+ 🗑️

<input type="checkbox"/>	#	Connection Name

Client to Site VPN:

+ 🗑️

<input type="checkbox"/>	#	Group Name

OpenVPN: 2 On Off

PPTP VPN: On Off

802.1x: On Off

Lobby Ambassador: On Off

步骤8.在“系统配置”菜单中导航，然后单击“用户帐户”。在本地用户下，单击加号图标。

- Getting Started
- Status and Statistics
- Administration
- System Configuration
- Initial Router Setup
- System
- Time
- Log
- Email
- User Accounts 1
- User Groups
- IP Address Groups
- SNMP
- Discovery-Bonjour
- LLDP
- Automatic Updates
- Schedules

User Accounts Apply Cancel

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


2
+ 🗑️ 📄 📥 📤

<input type="checkbox"/>	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.

步骤9.填写以下信息。确保从下拉菜单中选择OpenVPN。单击 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

所有依赖项都已完成，现在可以为路由器配置OpenVPN。

步骤10.导航到VPN > OpenVPN。将打开OpenVPN页面。填写页面上的每个框，确保从下拉菜单中选择之前创建的证书。

Getting Started

Status and Statistics

Administration

System Configuration

WAN

LAN

Wireless

Routing

Firewall

VPN **1**

VPN Setup Wizard

IPSec VPN

OpenVPN **2**

OpenVPN **5**

Enable: **3**

Interface:

CA Certificate:

Server Certificate:

Client Authentication: **4**

Client Address Pool: Netmask:

Protocol: Port:

Encryption:

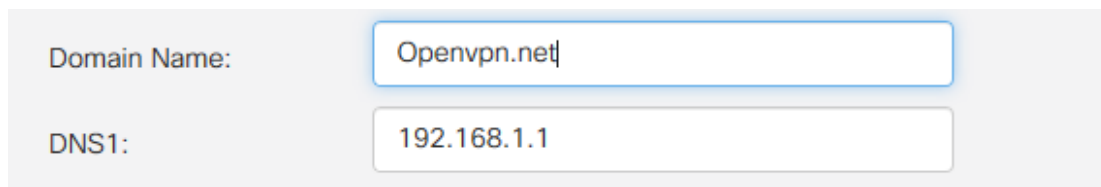
Tunnel Mode: Full Tunnel, routing all client traffic through VPN Split Tunnel, routing client traffic destined to the following subnets through VPN

- 选中启用框。选择允许流量的接口。在本例中为广域网(WAN)，并选择证书颁发机构(CA)证书。
- 从下拉菜单中选择CA证书
- 从下拉菜单中选择您下载的服务器证书
- 选择“Client Authentication”。如果选择Password，则需要使用密码进行身份验证。如果选择密码+证书，则客户端还必须具有证书。这更加安全，但会增加VPN的成本，因为他

们需要购买单独的CA。

- 输入客户端地址池。在网络子网中选择公司其他任何地方都未使用的IP地址。从保留范围中选择，并选择不在其他位置使用的范围。
- 选择加密形式。确保加密与客户端相同。不建议使用DES和3DES，应仅用于向后兼容。
- 如果只想指定通过VPN的流量，请选择拆分隧道。对于VPN，需要拆分隧道。当您希望所有客户端流量通过VPN时，在其他情况下会选择全通道模式。

步骤11.向下滚动页面，填写“域名”和DNS1。



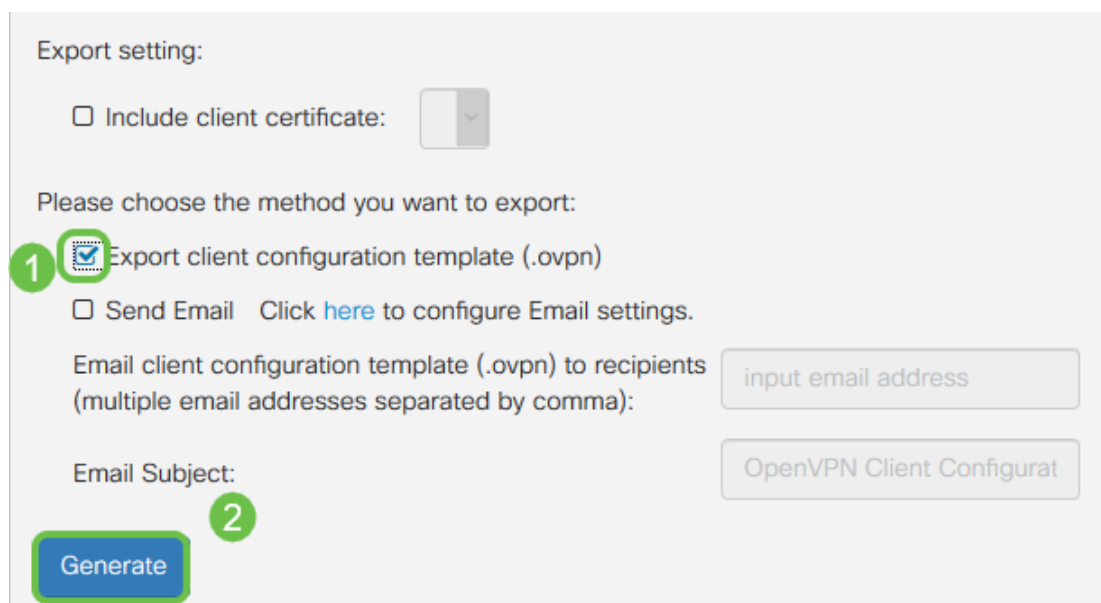
Domain Name:

DNS1:

注意：DNS1 IP地址可以是专用的内部DNS服务器、Internet服务提供商(ISP)、虚拟机上提供的默认网关的相同IP地址，也可以是Internet上的受信任DNS服务器。

步骤12.单击**Apply**以在路由器上保存配置。

步骤13.保留在同一页，然后进一步滚动。生成要安装在OpenVPN客户端上的配置模板。此文件具有.ovpn扩展名，将由OpenVPN客户端使用。选中导出客户端配置模板(.ovpn)的框，然后单击生成。这会将文件下载到您的计算机上。



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

步骤14.导航至Status and Statistics > VPN Status。您可以向下滚动以获取更详细的信息。

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

本文的下一部分很重要，因为它说明了如何使用自签名证书登录。

在设置演示OpenVPN后使用自签名证书登录

使用自签名证书登录时，尝试登录时可能会出现警告弹出窗口。您需要点击Advanced、Proceed、Trust或其他选项（具体取决于您的Web浏览器）才能继续。

此时，您可能会收到警告，称其不安全。您可以选择继续、添加例外或高级。这取决于Web浏览器。

在本例中，Chrome用于Web浏览器。出现此消息，单击“Advanced”。



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

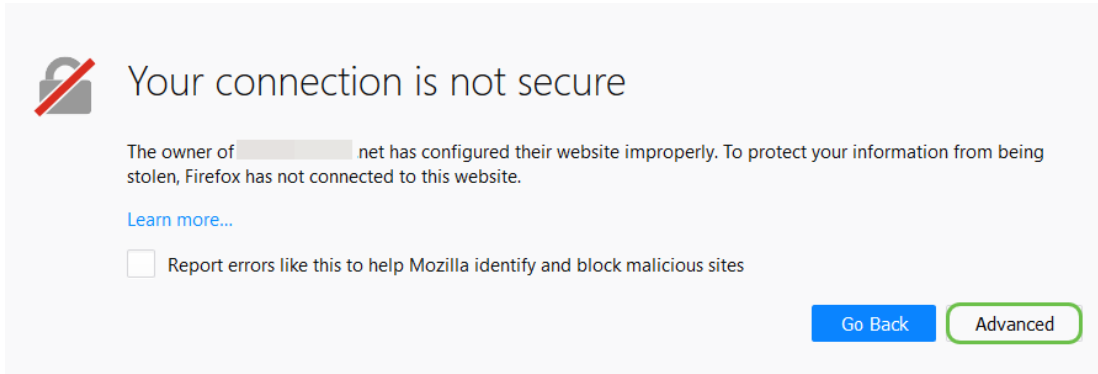
BACK TO SAFETY

将会打开一个新屏幕，您需要单击“继续到您的website.net（不安全）”

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)

以下是将Firefox用作Web浏览器时访问设备警告的示例。单击“Advanced(高级)”。



Your connection is not secure

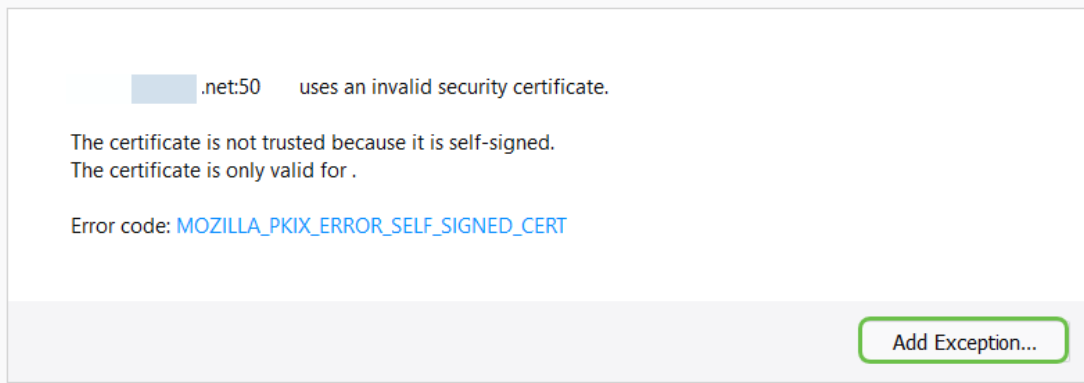
The owner of net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

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

[Go Back](#) [Advanced](#)

单击添加例外.....



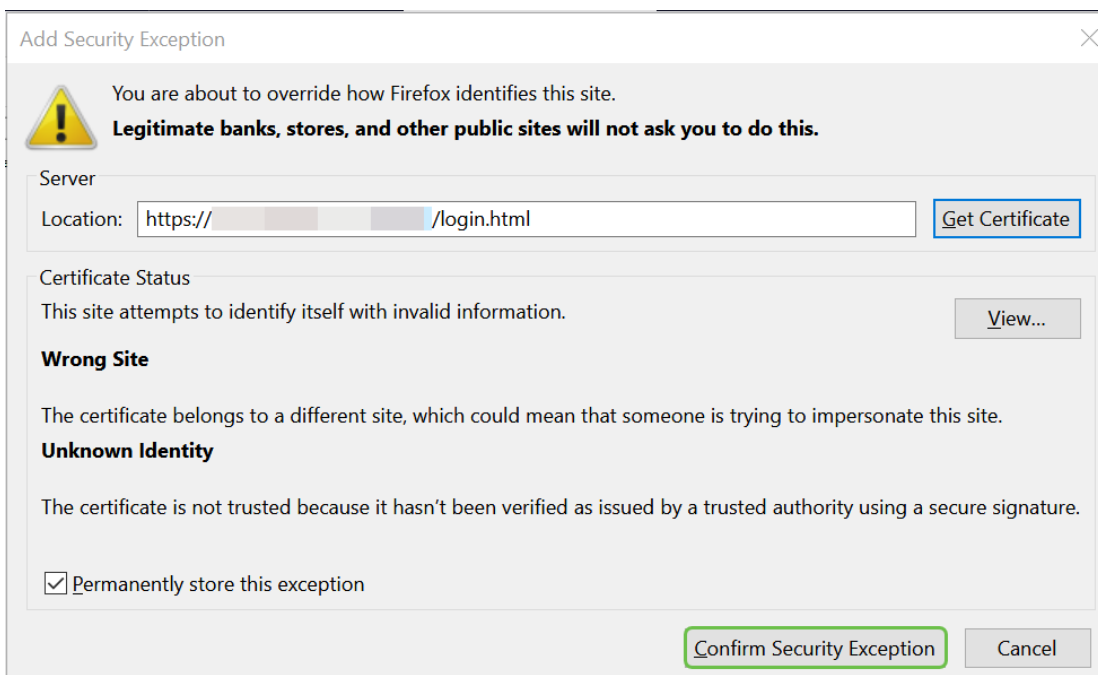
 .net:50 uses an invalid security certificate.

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...](#)

最后，您必须单击“确认安全异常”。



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: / /login.html"/> [Get Certificate](#)

Certificate Status

This site attempts to identify itself with invalid information. [View...](#)

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

[Confirm Security Exception](#) [Cancel](#)

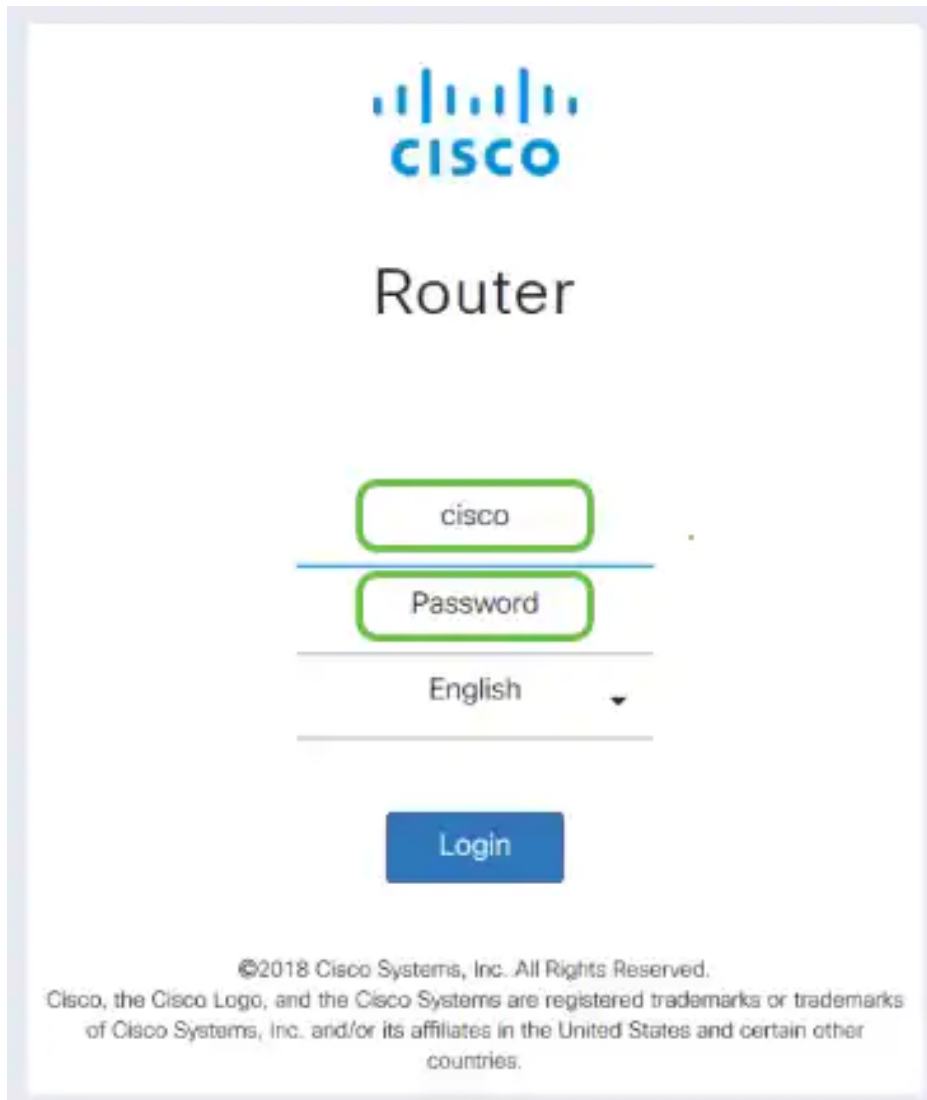
现在，路由器已配置了支持OpenVPN客户端连接所需的所有参数。由于您已将客户端配置模板下载到您的设备(以.ovpn结尾的模板)，因此可以转到“计算机上的[OpenVPN客户端设置](#)”部分。如果您决定为公司部署OpenVPN，可以执行下一节中的步骤。

在RV160/RV260路由器上设置OpenVPN

这是一个更复杂的过程，因为它涉及从第三方获取CA，而这需要资金。您还需要将以.ovpn结尾的VPN客户端配置模板发送给所有客户端，以便它们可以在其设备上设置。客户端需要与路由器相同的多种设置才能通信。最好的是，您和您的员工能够以最低的成本使用互联网，更安全地开展业务。

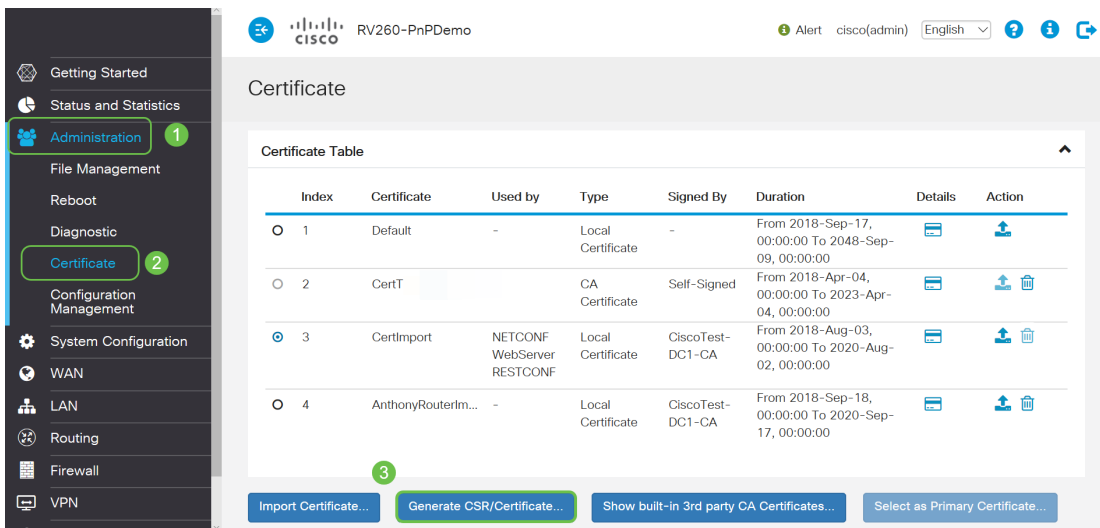
步骤1.使用您的凭证登录路由器。默认用户名和密码为*cisco*。

注意：强烈建议您将所有密码更改为更复杂的密码。否则，就像把钥匙丢到门口上锁的门上一样。

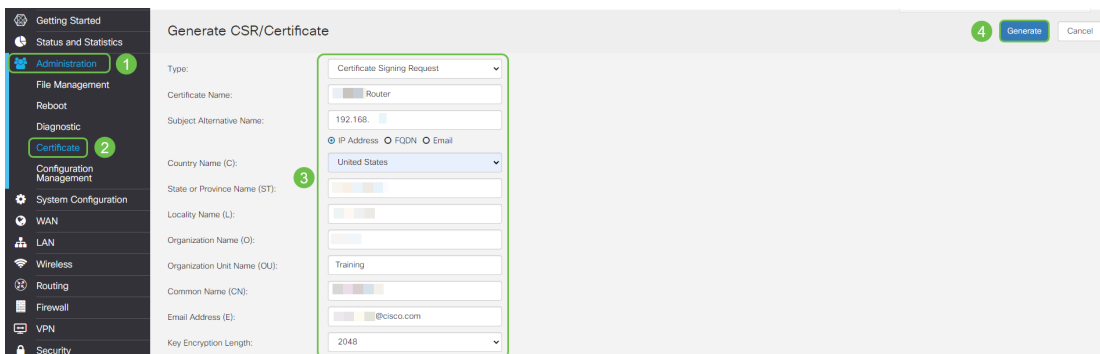


The image shows the login interface of a Cisco Router. At the top is the Cisco logo. Below it, the word "Router" is displayed. There are three input fields: the first contains "cisco", the second is labeled "Password", and the third is labeled "English" with a dropdown arrow. A blue "Login" button is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

步骤2.您必须获得证书。导航至**管理 > 证书 > 生成CSR/证书.....**这是如何创建证书请求。



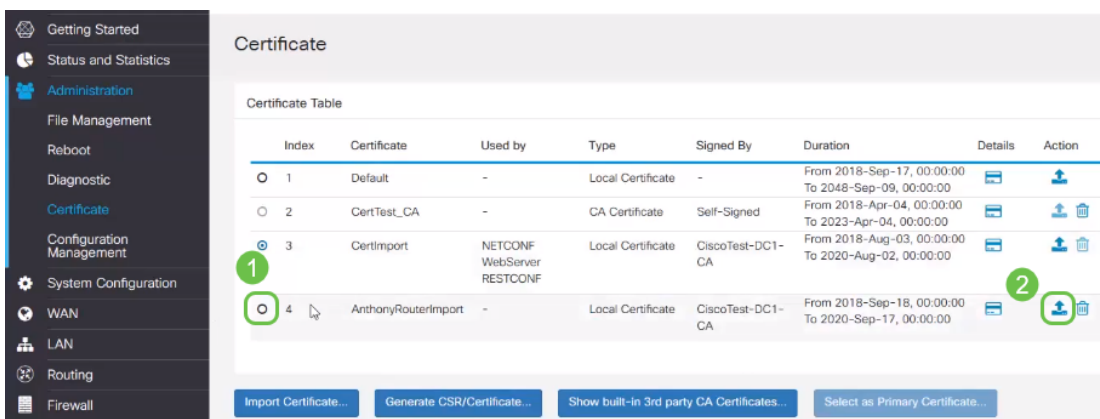
步骤3.请求由CA证书签名的证书。导航至Administration > **Certificate**即可找到此证书。



- 从下拉菜单中选择证书签名请求
- 输入证书名称
- 输入IP地址、完全限定域名(FQDN)或电子邮件。输入IP地址是最常见的选择。
- 输入您所在的国家/地区
- 输入您的省/自治区
- 输入您所在地的名称，通常是您所在的城市
- 输入您的组织名称
- 输入您的组织单位名称
- 输入您的电子邮件地址
- 输入密钥加密长度，建议使用2048

单击右上角的“生成”按钮

步骤4.通过点击操作(Action)下的向上箭头选择将其导出。



步骤5.此屏幕将出现。单击Export。

Export Certificate



Export as PEM format

Export to:

PC USB

Export

Cancel

步骤6. 从下拉菜单中选择“打开方式”和“记事本”（默认）。Click OK.

Opening AnthonyRouter.pem



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

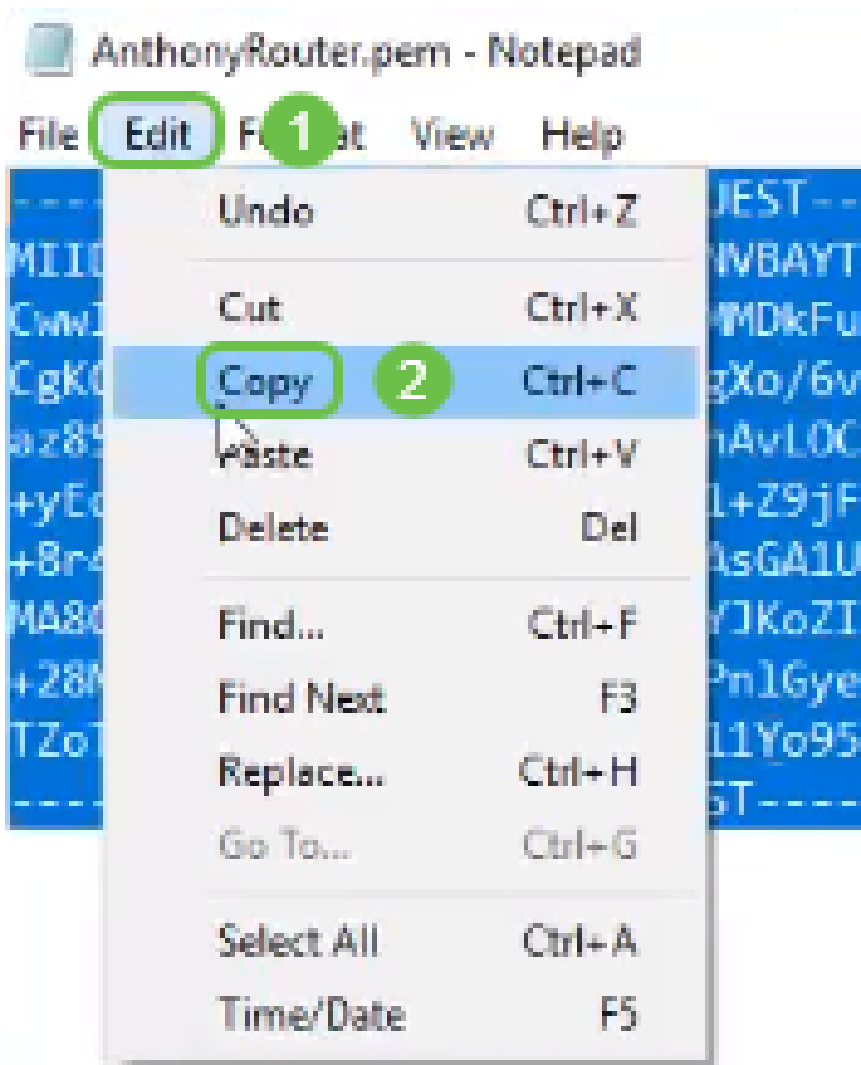
Cancel

步骤7. 将打开XML文件。

```
AnthonyRouter.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIIDYTCBAAQCAAwgZcxCAJ8gNBAYTAIVTRUwEwYDQVQIDAAxTb3V0aCBEYwtdGEwFDASBgWBAcMCINb3V4IEZhbGxzMQ4wDAYDVQQKDAVDAWJjZERMMA8GA1UE
Cw: GvbnkgUw91dG9yYWRwYXN0eS1xS1s1Z29jF1ac3Gw6CFDYXg09C8ja8x1qgBasGcrwnJajcF+MBOL5s41UfWIDAQABoIGDMIGABgkqhkiG9w0BCCQ4xczBxMAkGA1UdEwQCMAMwIhYDVR00BBEYFPI
+eF51bVH1P6TyqK2b0DeS1xS1s1Z29jF1ac3Gw6CFDYXg09C8ja8x1qgBasGcrwnJajcF+MBOL5s41UfWIDAQABoIGDMIGABgkqhkiG9w0BCCQ4xczBxMAkGA1UdEwQCMAMwIhYDVR00BBEYFPI
+84zePCPInbvS4HYDdPQcwz0MAsGA1UdDwQEAwIF4DAnBgIwH5UEIDAeBgggrBgEFBQcDAQYIKwYBBQUHwIGCCsGAQUFCAIC
MA8GA1UdEQQIMAAHBMCoASgUdQYJKoZIhvcNAQEBQADggEBAF2+aVf
+28MBtJ0YuthSLMMAtbic6zUzHPnIGyemQz+JRjN/RNq5NHSL70sd8jwadOZXp6XpZ+mK5pm6vA1e0ef3mdJ/R+rP2Ahb+11RWmq0wh5f3swRS2HEon4
TzTKfIXBcMTWpCh1jPFyALeNH811Yo95aB02WX2e+9vH0T5xgVae2wFomphBBsUvcUNT4jUzYnysV7XkrREz7oY1PF5T2W9KzA1oZw8aQbNUqNTx3qFbM41F01cMUYs73q06M2M=
-----END CERTIFICATE REQUEST-----
```

注意：确保BEGIN CERTIFICATE REQUEST和END CERTIFICATE REQUEST分别位于各自的行中，如上所示。

步骤8. 在屏幕顶部单击“编辑”，然后从下拉菜单中选择“复制”。



步骤9.选择信誉良好的第三方站点以发出证书请求。您需要将复制的XML文件粘贴为请求的一部分。

注意：如果您的网络上有内部证书服务器，则可以改用该服务器，但这并不常见。

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

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

步骤10.验证完毕后，您可以选择“下载证书”。

Certificate Issued

The certificate you requested was issued to you.

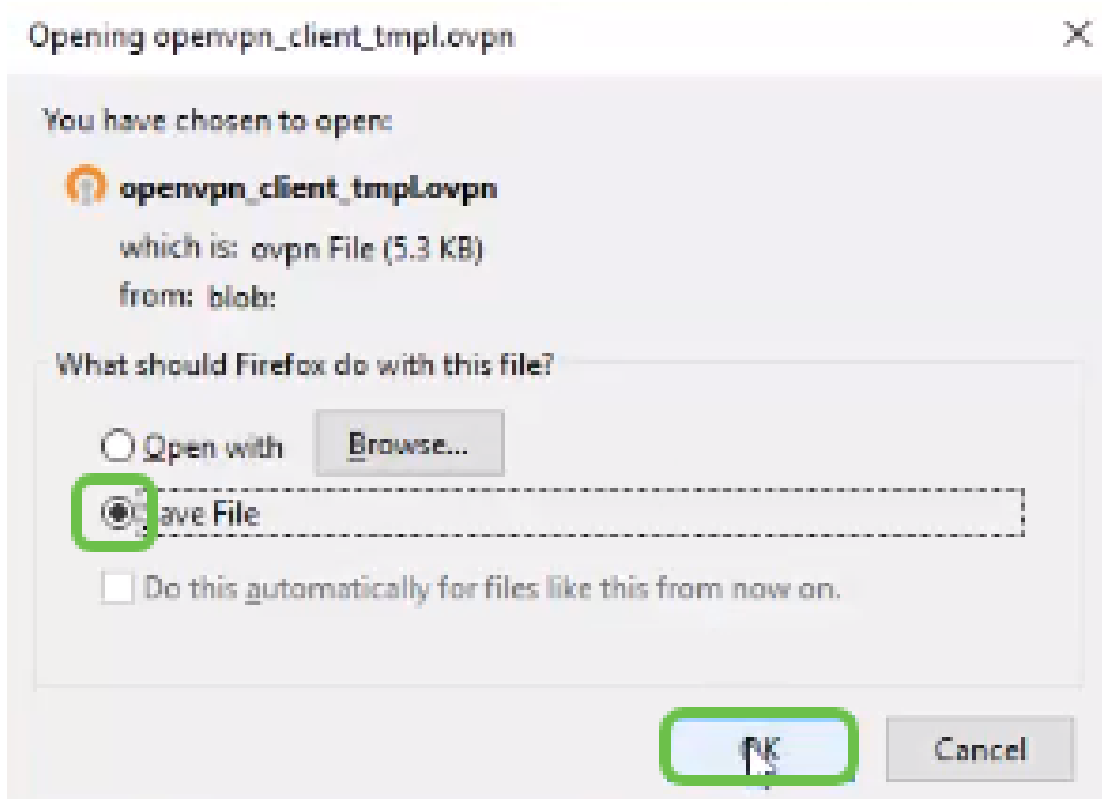
DER encoded or Base 64 encoded



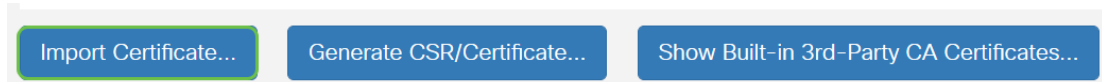
[Download certificate](#)

[Download certificate chain](#)

步骤11.单击单选按钮以保存文件，然后单击确定。



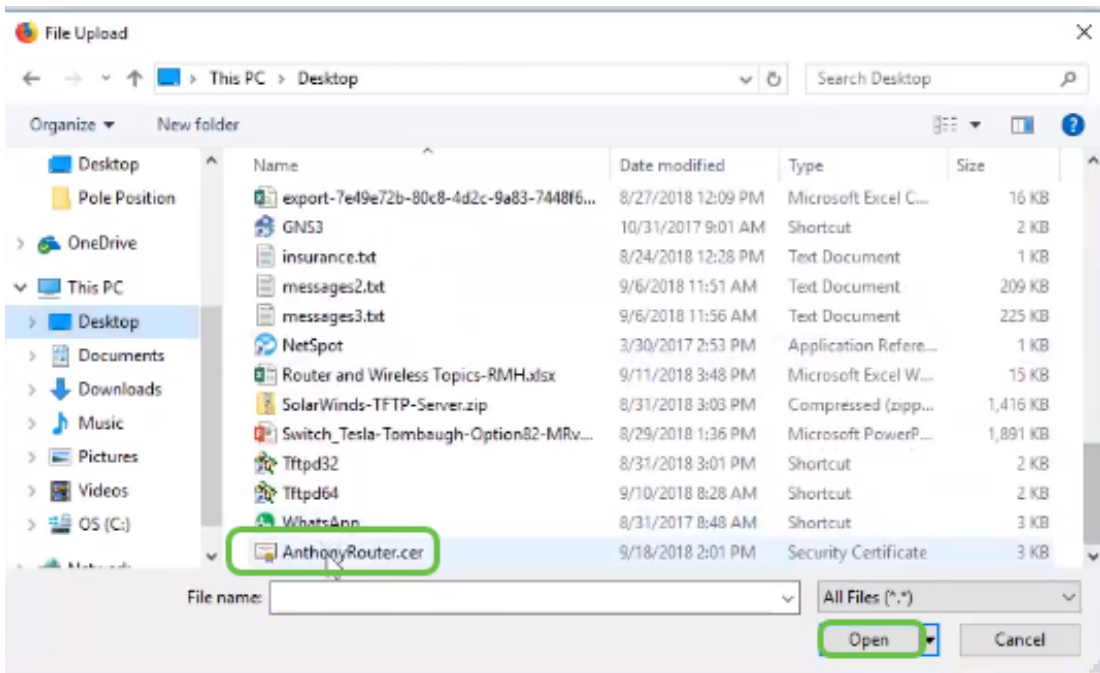
步骤12.保存后，选择该证书的单选按钮，然后单击向下箭头图标。



步骤13.此屏幕将打开。选择浏览.....。



步骤14.选择证书的文件，然后单击“打开”。



步骤15.输入要导入的证书名称，然后单击上传。

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

步骤16.您将收到证书已成功导入的通知。Click OK.

Information

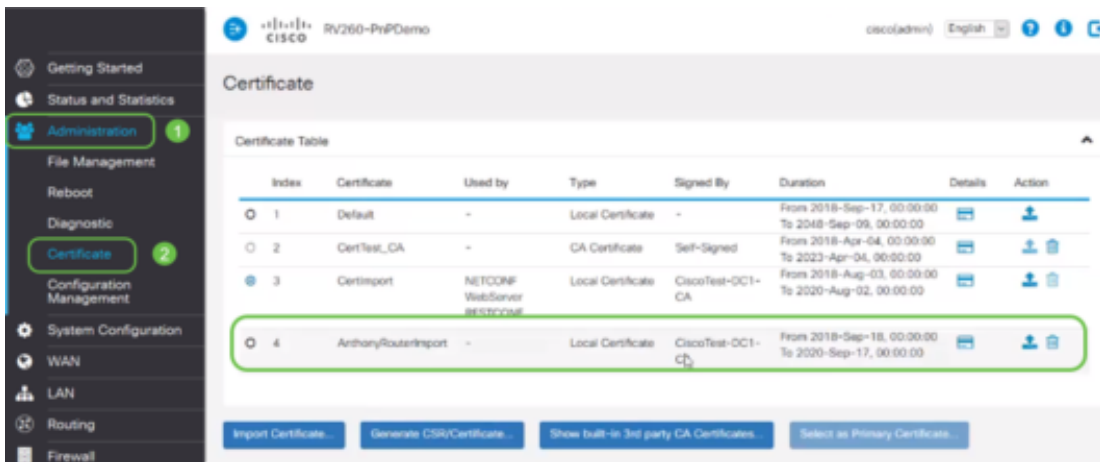


Import certificate successfully!

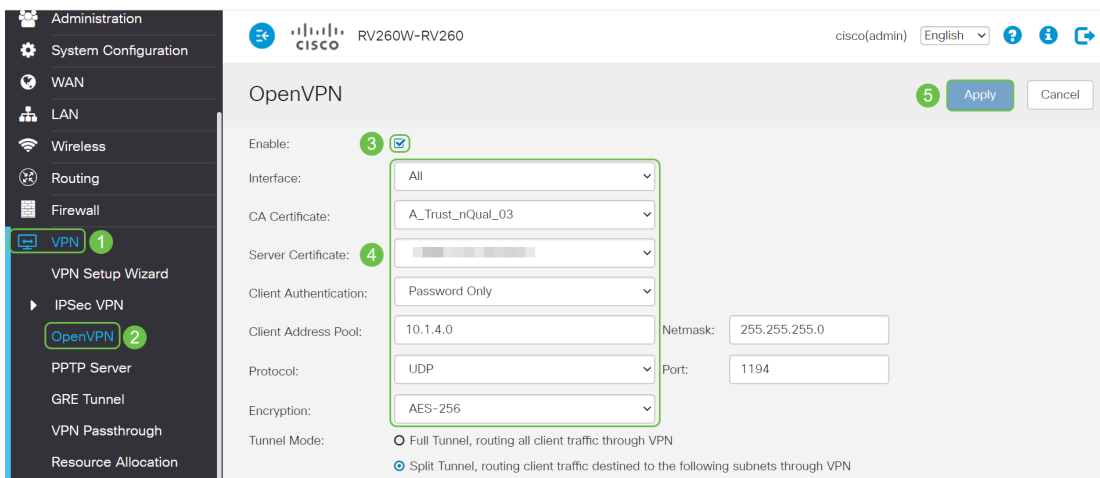
OK

步骤17.导航至Administration > Certificate。证书已加载。

注意：在本例中，使用了本地证书服务器。



步骤18.导航到VPN > OpenVPN。将打开OpenVPN页面。使用您的信息完成以下操作。



- 选中启用框。选择允许流量的接口。在本例中为广域网(WAN)，并选择证书颁发机构(CA)证书
- 从下拉菜单中选择CA证书
- 从下拉菜单中选择您下载的服务器证书
- 选择“Client Authentication”。如果选择Password，则需要使用密码进行身份验证。如果选择密码+证书，则客户端还必须具有证书。这更加安全，但会增加VPN的成本，因为他们需要购买单独的CA。
- 输入客户端地址池。在网络子网中选择公司其他任何地方都未使用的IP地址。从保留范围中选择，并选择不在其他位置使用的范围。
- 选择加密形式。确保加密与客户端相同。不建议使用DES和3DES，应仅用于向后兼容。
- 如果希望所有客户端流量通过VPN，请选择Full Tunnel Mode；如果只想指定哪些流量通过VPN，请选择Split tunnel
- DNS1 IP地址可以是专用的内部DNS服务器、Internet服务提供商(ISP)、虚拟机上提供的默认网关的相同IP地址，或者Internet上的受信任DNS服务器。

单击Apply以保存配置。

第19步（选项1）。您可以将此配置通过电子邮件发送给客户端。选中Send Email(发送电子邮件)。输入电子邮件地址。为电子邮件添加主题标题。单击生成。

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@cisico.com

Email Subject: OpenVPN Client Config

Generate

步骤20. (选项2)。选择导出客户端配置模板(.ovpn)，然后单击生成。

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

Generate

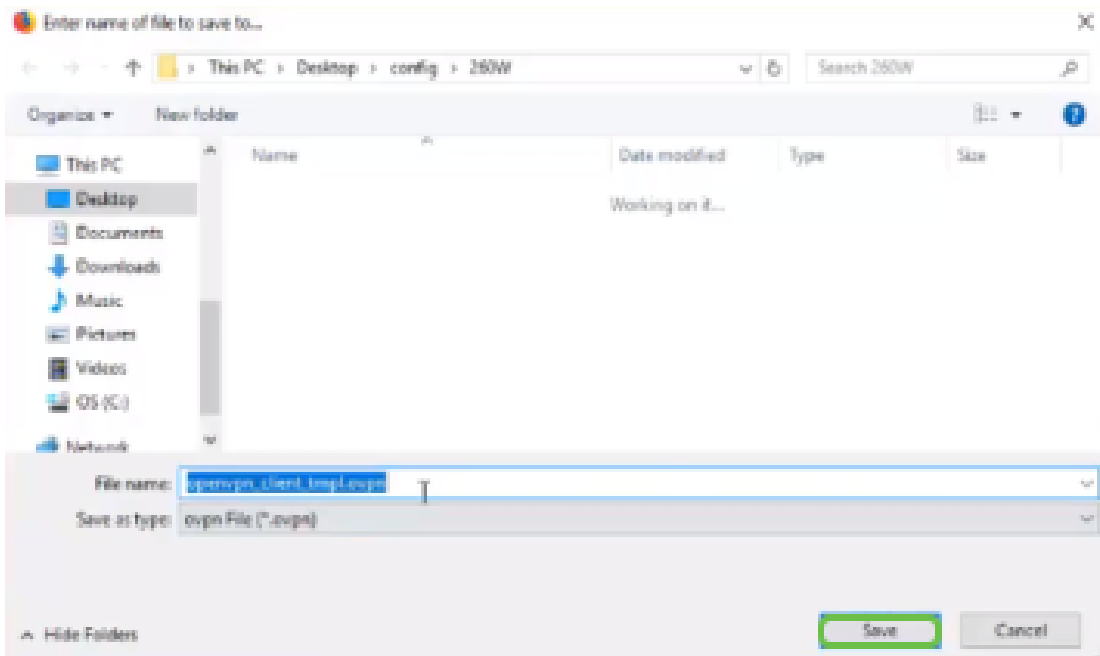
步骤21.您将收到成功的确认。Click OK.

Information

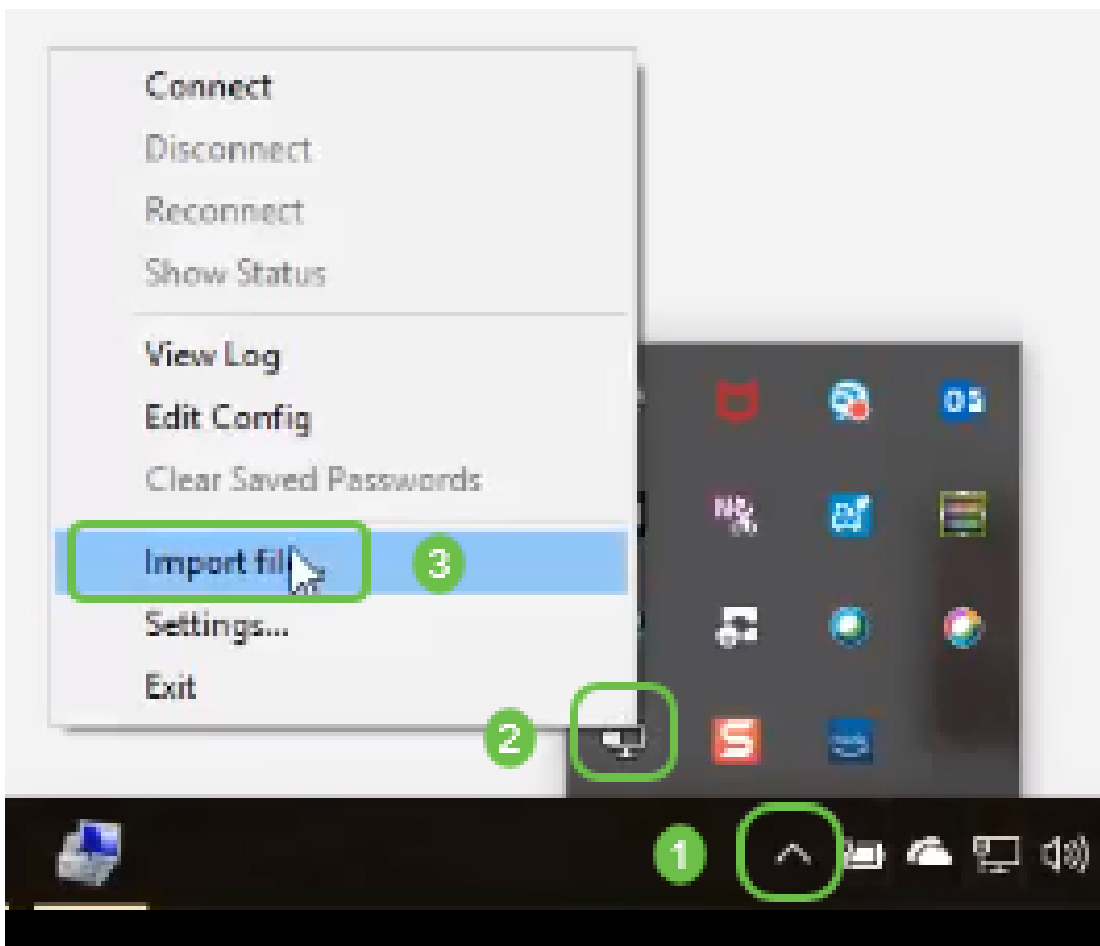
 Export client configuration template downloaded successfully!

OK

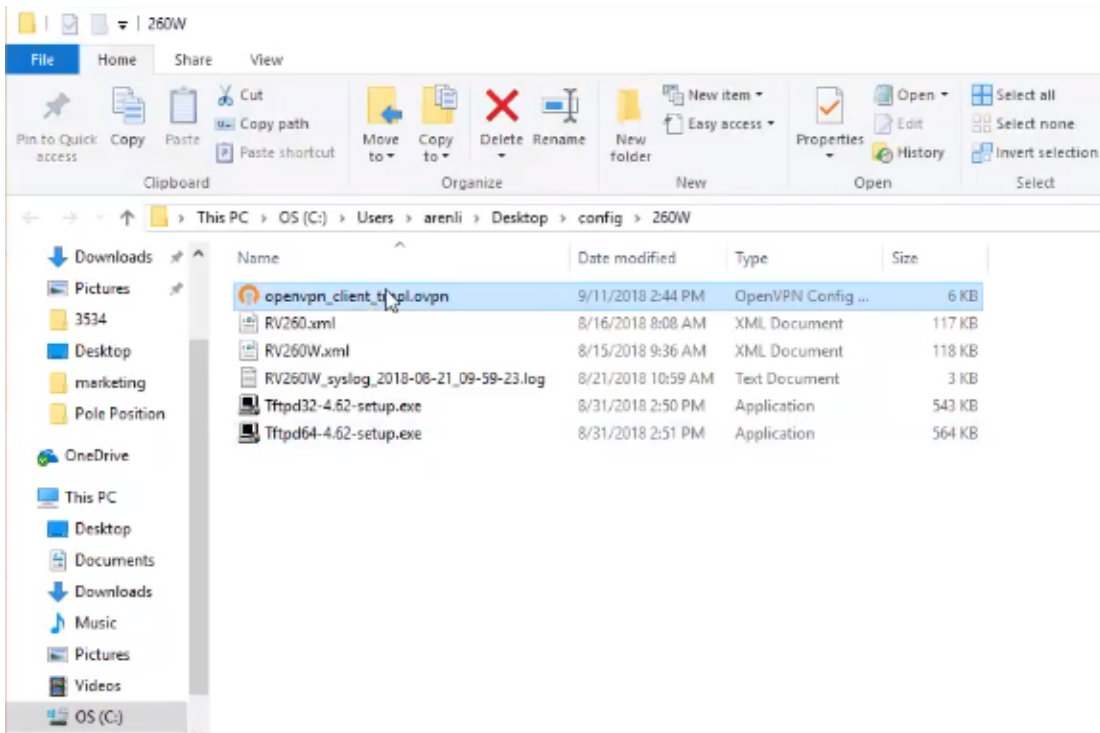
步骤22.单击Save。



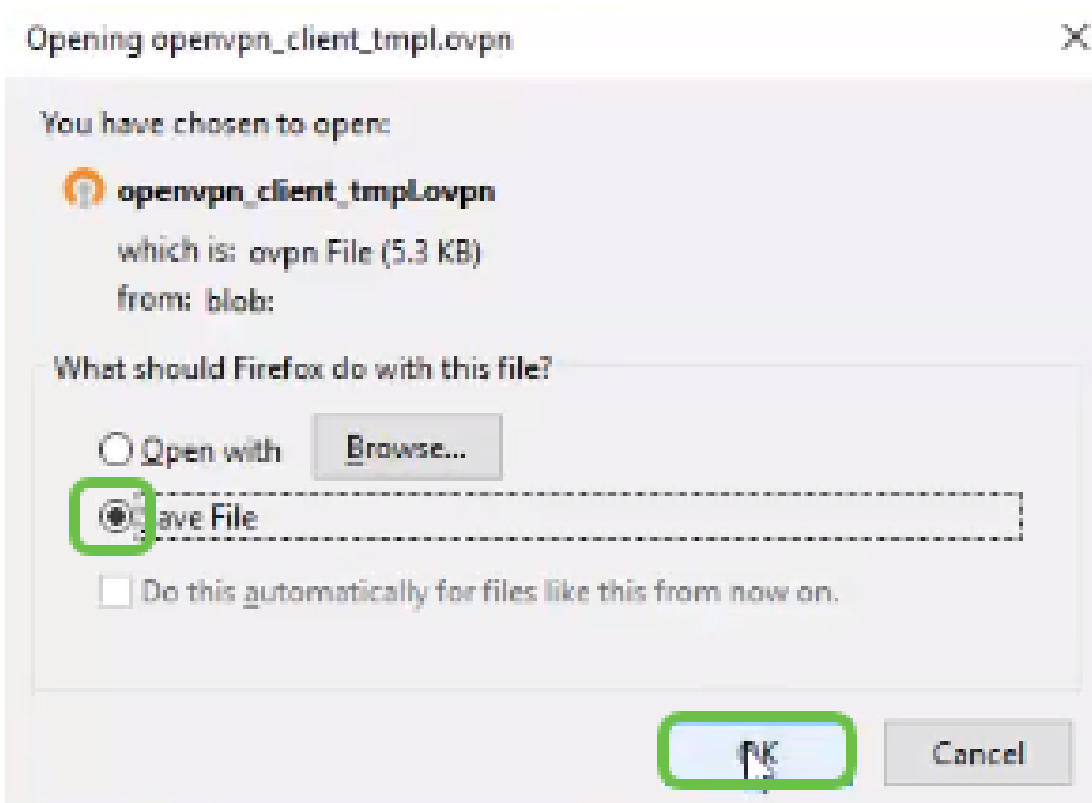
步骤23.在桌面右下角单击打开OpenVPN。右键单击打开下拉菜单。单击“导入文件”。



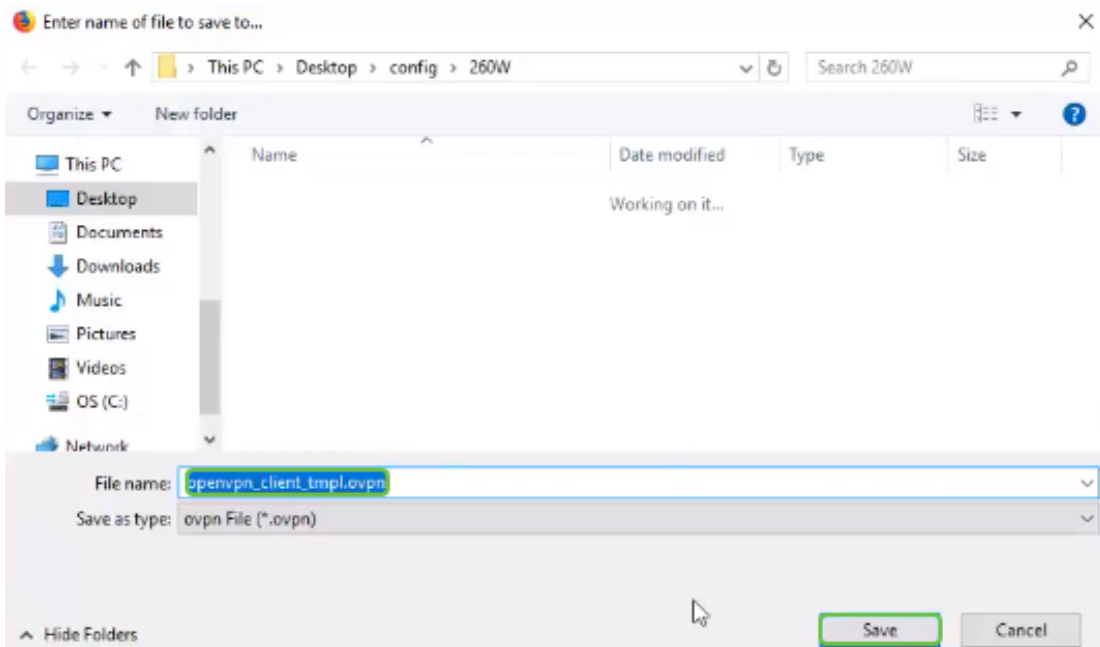
步骤24.选择以.ovpn结尾的OpenVPN文件。



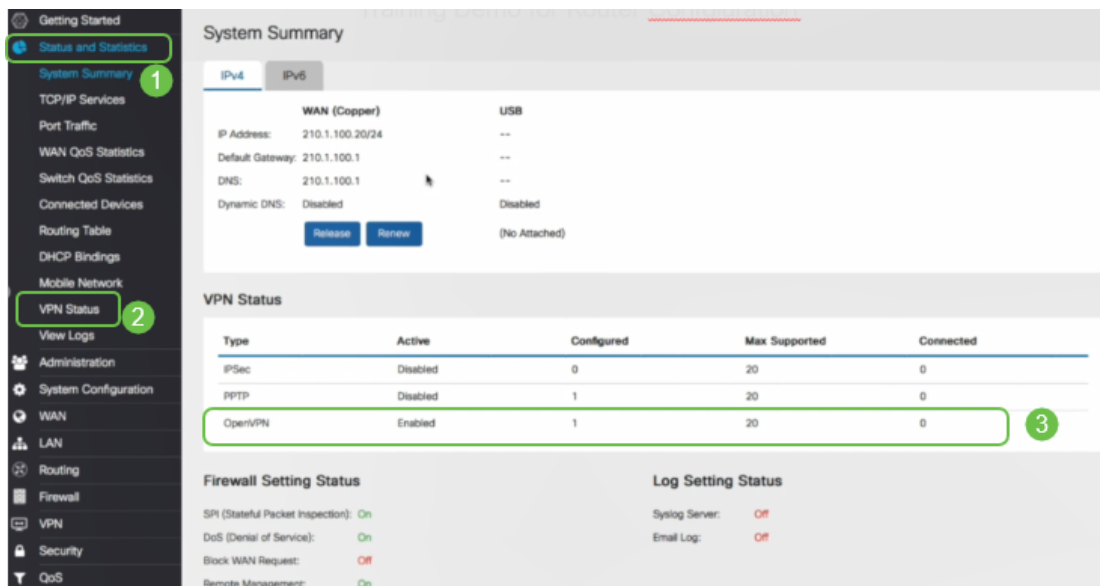
步骤25.单击单选按钮“保存文件”，然后单击确定。



步骤26.如果选择，请更改文件名，但将。ovpn留在文件名末尾。Click Save.



步骤27. 导航至 **Status and Statistics > VPN Status**。您可以向下滚动以获取更详细的信息。



现在，路由器已配置了支持个人试用版OpenVPN客户端连接所需的所有参数。

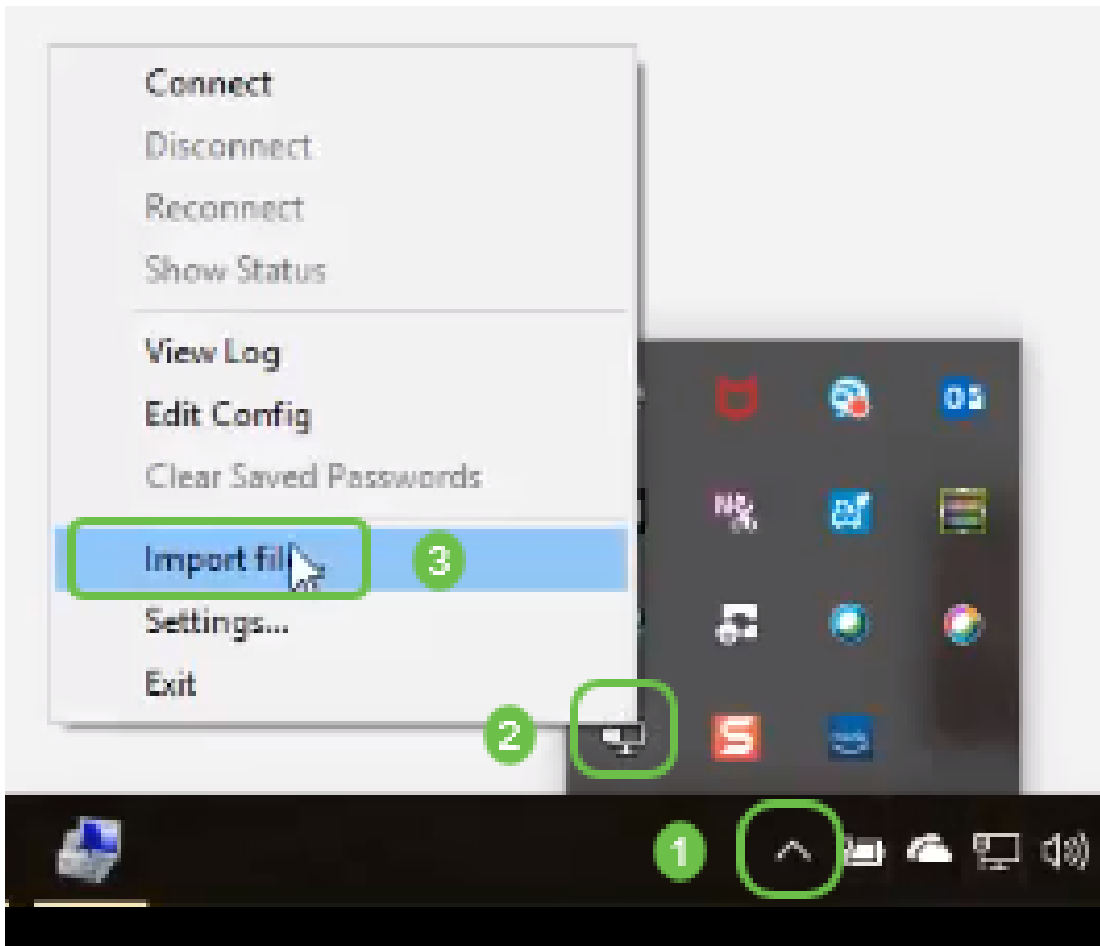
计算机上的OpenVPN客户端设置

每个OpenVPN客户端都需要执行以下任务作为前提条件：

- 在设备上下载OpenVPN应用。
- 打开并保存在上一节步骤19-22中发送的配置文件。配置文件以.ovpn结尾。

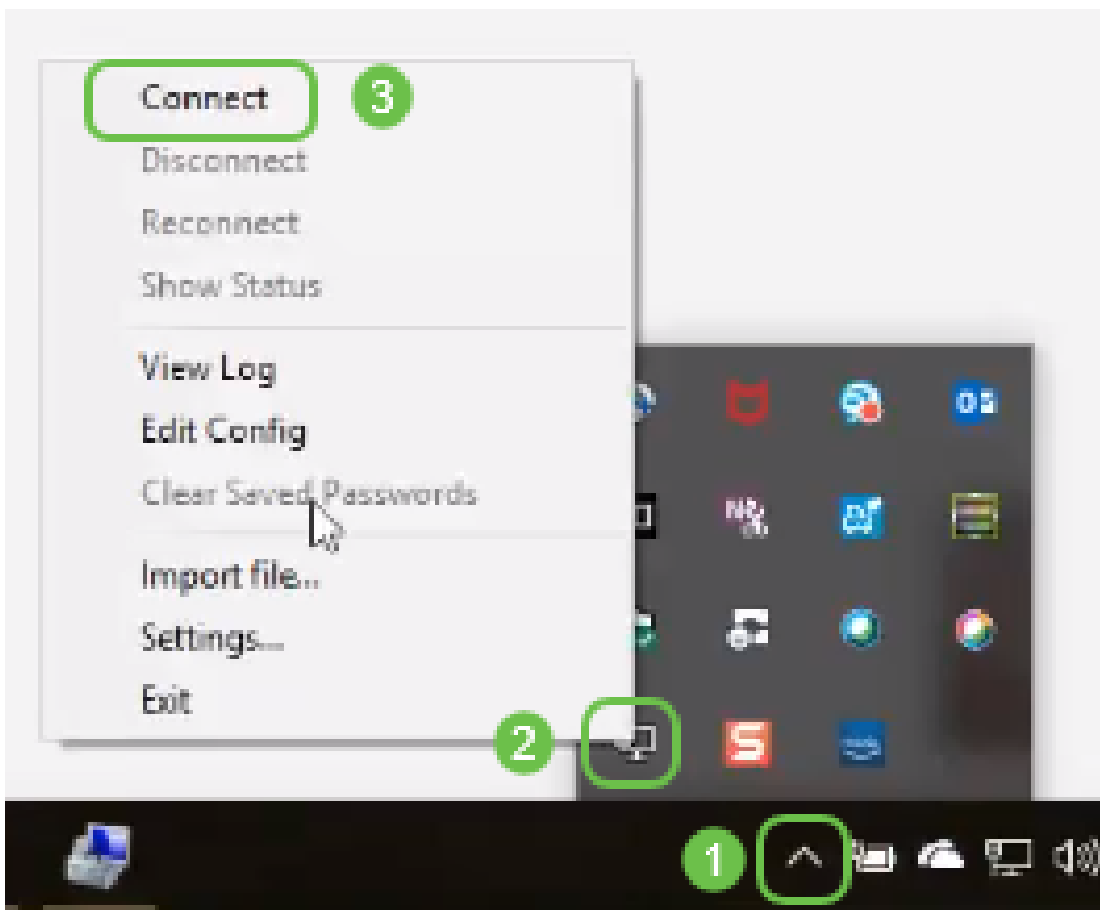
注意：此设置专门用于Windows 10。

步骤1. 导航至桌面右下角的箭头图标，然后单击以打开OpenVPN图标。右键单击并选择“导入文件”。

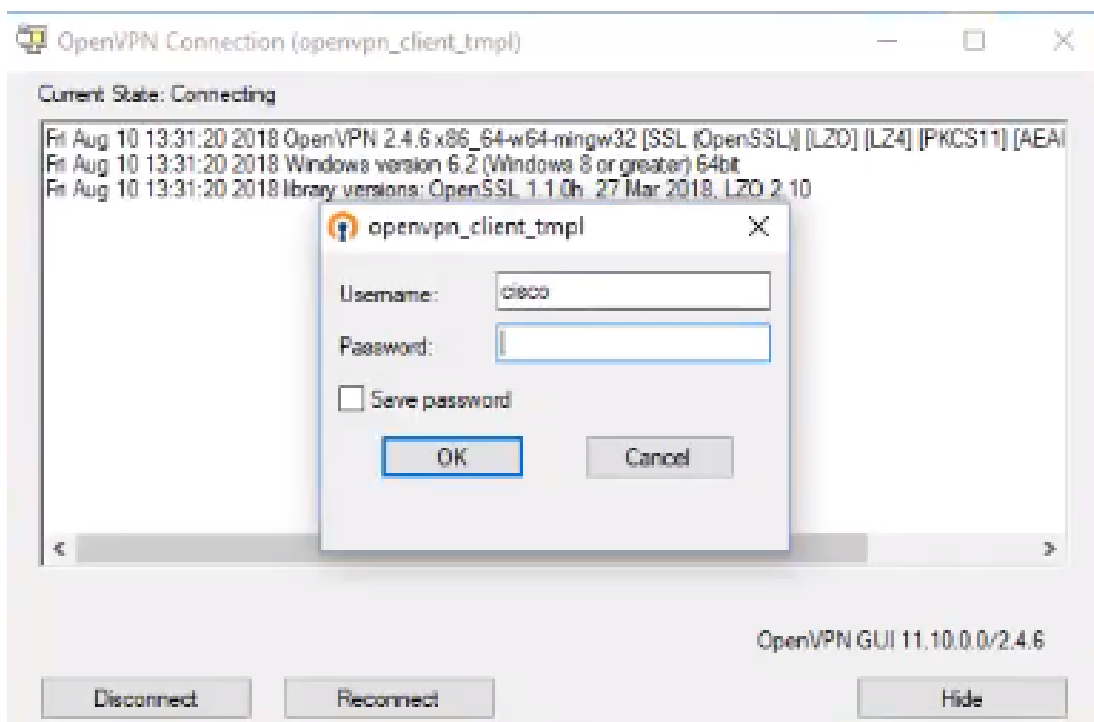


注意：图标为黑白，表示当前未运行。运行后，图标将以颜色显示。

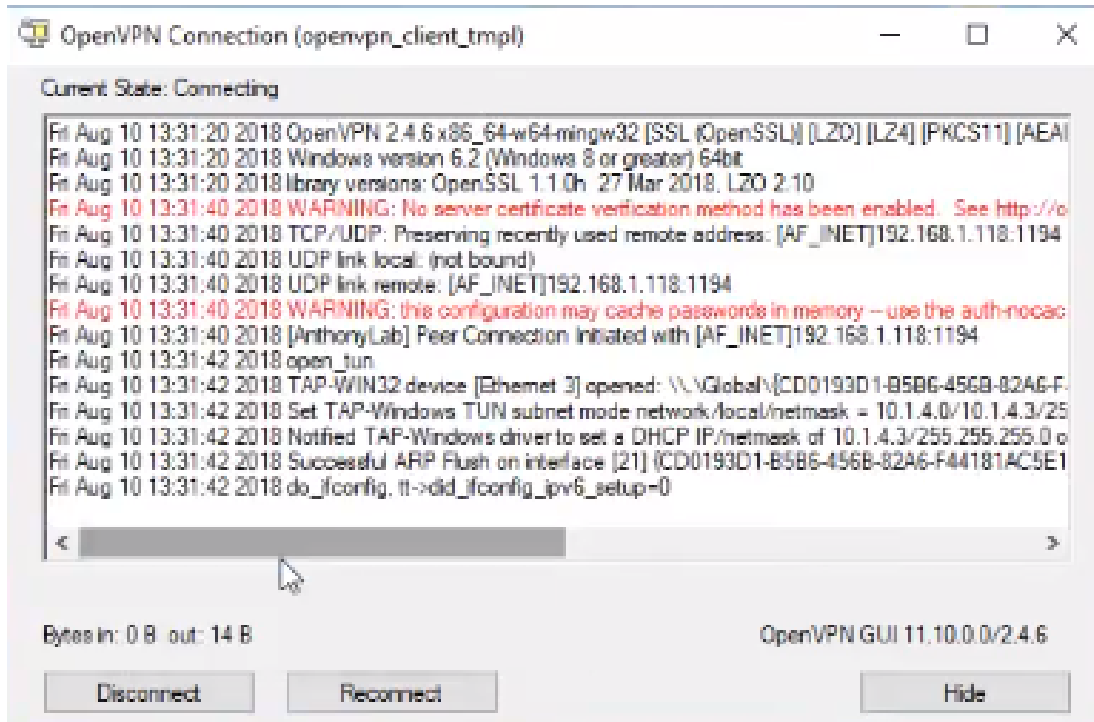
步骤2.单击上箭头。点击OpenVPN图标。右键单击，然后从下拉菜单中选择“连接”。



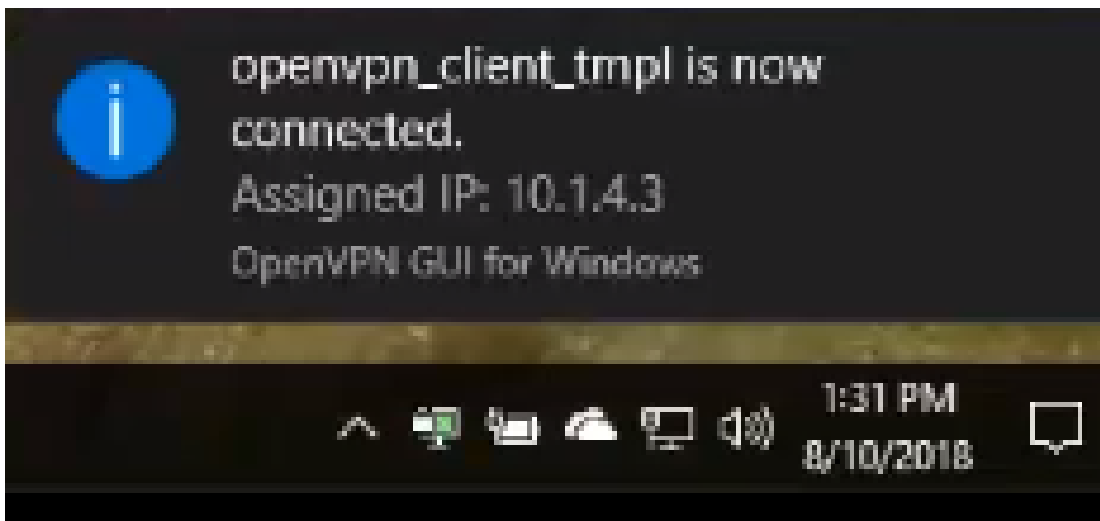
步骤3.输入用户名和密码。



步骤4. 该窗口将显示OpenVPN连接和一些日志数据。

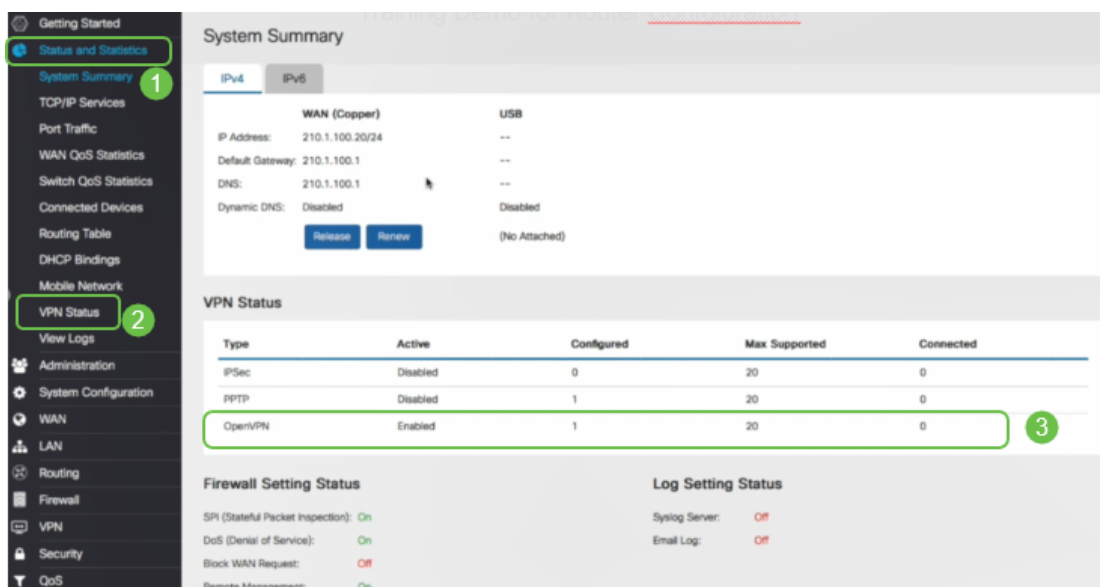


步骤5. 系统日志应提示存在连接。



步骤6. VPN客户端应能安全地通过OpenVPN传输传入和传出信息。这可设置为在OpenVPN设置中自动连接。

步骤7. 管理员可以通过导航到路由器上的Status and Statistics > VPN Status来确认VPN状态。



结论

现在，您应该已在RV160或RV260路由器和VPN客户端站点成功安装OpenVPN。

有关OpenVPN的社区讨论，请[单击](#)此处搜索OpenVPN。

查看与本文相关的视频.....

[单击此处查看思科提供的其他技术讲座](#)