

Set Up and Use TheGreenBow IPsec VPN Client to Connect with RV160 and RV260 Routers

Objective

The objective of this document is to set up and use TheGreenBow IPsec VPN Client to connect with the RV160 and RV260 routers.

Introduction

A Virtual Private Network (VPN) connection allows users to access, send, and receive data to and from a private network by means of going through a public or shared network such as the Internet but still ensuring a secure connection to an underlying network infrastructure to protect the private network and its resources.

A VPN tunnel establishes a private network that can send data securely using encryption and authentication. Corporate offices often use a VPN connection since it is both useful and necessary to allow their employees to have access to their private network even if they are outside the office.

The VPN allows a remote host, or client, to act as if they were located on the same local network. The RV160 router supports up to 10 VPN tunnels, and the RV260 supports up to 20. A VPN connection can be set up between the router and an endpoint after the router has been configured for Internet connection. The VPN client is entirely dependent on the settings of the VPN router to be able to establish a connection. The settings must match exactly or they cannot communicate.

TheGreenBow VPN Client is a third-party VPN client application that makes it possible for a host device to configure a secure connection for client-to-site IPsec tunnel with the RV160 and RV260 series routers.

Benefits of using a VPN Connection

Using a VPN connection helps protect confidential network data and resources.

It provides convenience and accessibility for remote workers or corporate employees since they will be able to easily access the main office without having to be physically present and yet, maintain the security of the private network and its resources.

Communication using a VPN connection provides a higher level of security compared to other methods of remote communication. An advanced encryption algorithm makes this possible, protecting the private network from unauthorized access.

The actual geographic locations of the users are protected and not exposed to the public or shared networks like the Internet.

A VPN allows new users or a group of users to be added without the need for additional components or a complicated configuration.

Risks of using a VPN Connection

There can be security risks due to misconfiguration. Since the design and implementation of a VPN can be complicated, it is necessary to entrust the task of configuring the connection to a highly knowledgeable and experienced professional in order to make sure that the security of the private network would not be compromised.

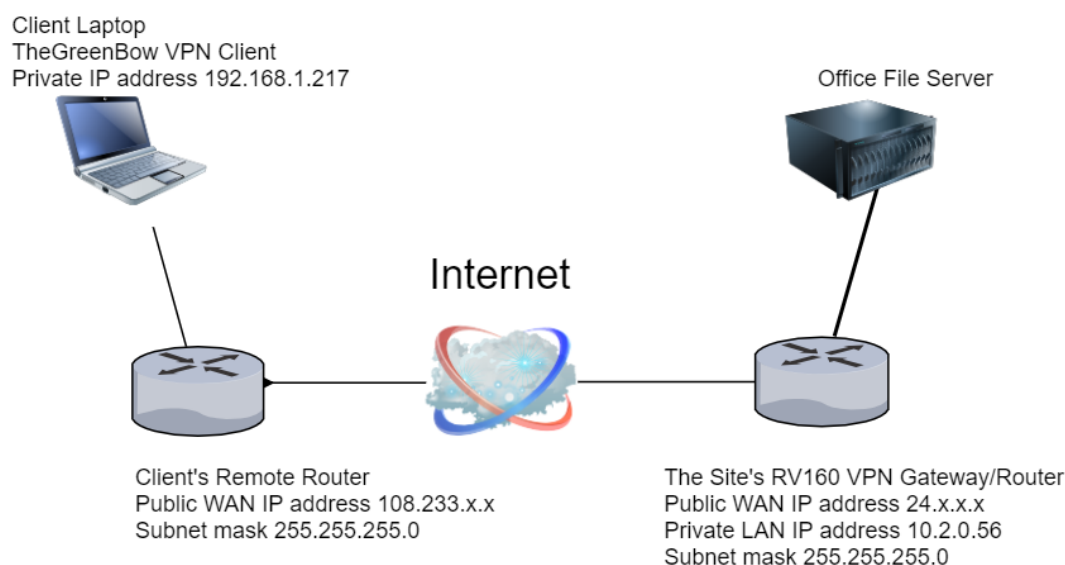
It may be less reliable. Since a VPN connection requires an Internet connection, it is important to have a provider with a proven and tested reputation to provide excellent Internet service and guarantee minimal to no downtime.

If a situation occurs where there is a need to add new infrastructure or a new set of configurations, technical issues may arise due to incompatibility especially if it involves different products or vendors other than the ones you are already using.

Slow connection speeds can occur. If you are using a VPN client which provides free VPN service, it may be expected that your connection would also be slow since these providers do not prioritize connection speeds. In this article, we will be using a paid third party which should eliminate this issue.

Basic Topology of the Client-to-Site Network

This is the basic layout of the Network for setup. The Public WAN IP addresses have been partially blurred, or are showing an x in place of actual numbers to protect this network from attacks.



This article will walk through the steps needed to configure the RV160 or RV260 router at the site for the following:

- A User Group — **VPNUsers**
- User Accounts (one or more users) that will be allowed access as a client
- An IPsec Profile — **TheGreenBow**
- A Client-to-Site Profile — **Client**
- You will also be shown how to view the VPN Status at the site once the client is connected

Note: You can use any name for the User Group, IPsec Profile, and Client-to-Site Profile. The names listed are just examples.

This article also explains the steps that each client would take to configure TheGreenBow VPN on their computer:

- Download and set up TheGreenBow VPN Client Software
- Configure the Phase 1 and 2 Settings for the client
- Start and verify a VPN Connection as a client

It is essential that every setting on the router on site matches the client settings. If your configuration does not lead to a successful VPN connection, check all settings to make sure they match. The example shown in this article is just one way to set up the connection.

Table of Contents

Configure on the RV160 or RV260 Router at the Site

[Create a User Group](#)

[Create a User Account](#)

[Configure IPsec Profile](#)

[Configure the Phase 1 and 2 Settings](#)

[Create a Client-to-Site Profile](#)

Configure at the Client Location

[Configure Phase 1 Settings](#)

[Configure Tunnel Settings](#)

[Start a VPN Connection as a Client](#)

Check Connectivity on the RV160 or RV260

[Verify the VPN Status at the Site](#)

Applicable Devices

- RV160
- RV260

Software Version

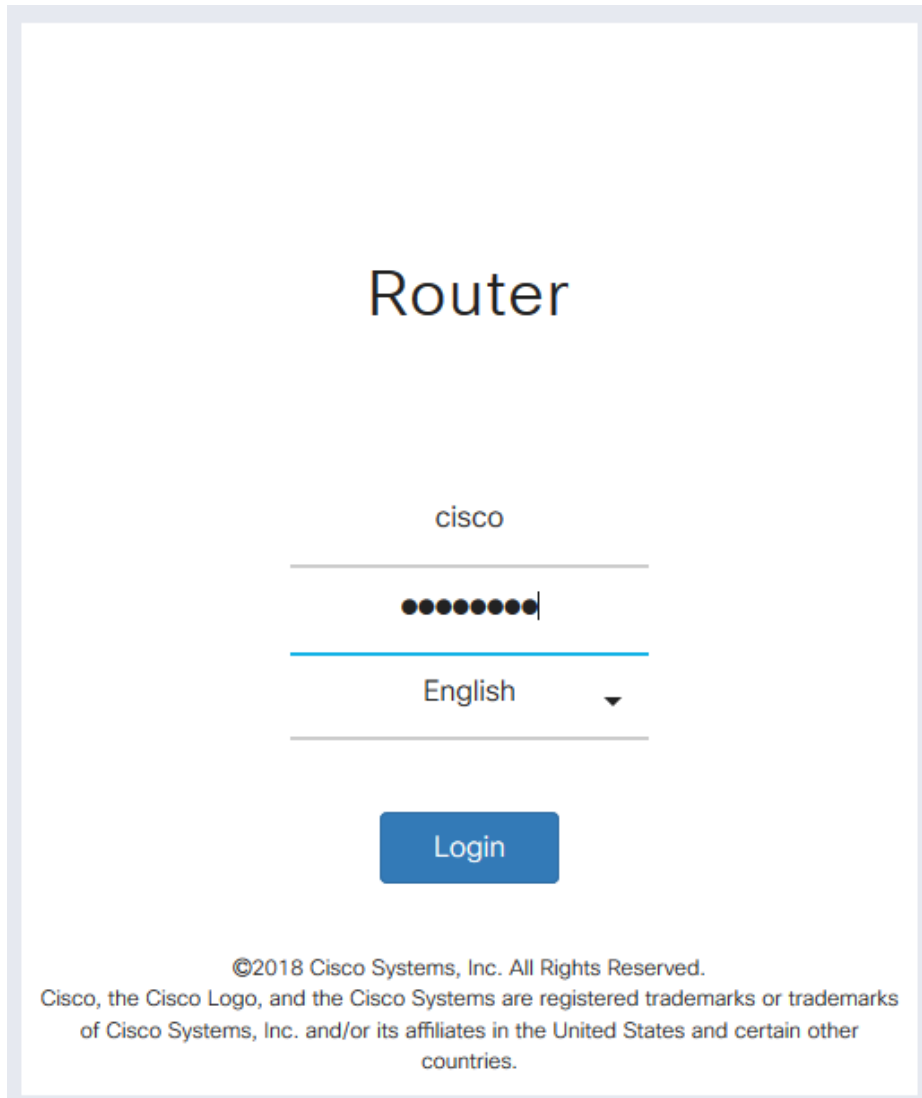
- 1.0.00.15

Configure VPN Client at the Site on the RV160 or RV260 router

Create a User Group

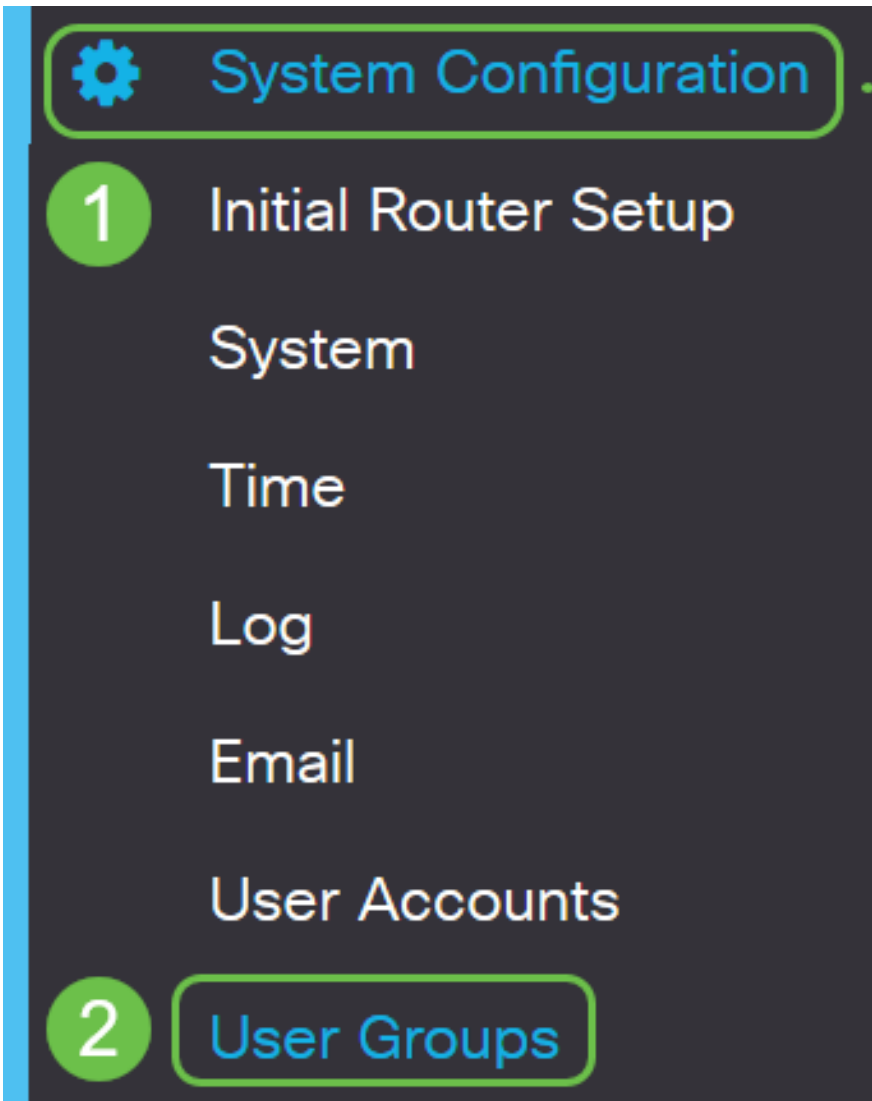
Important Note: Please leave the default admin account in the admin group and create a new user account and user group for TheGreenBow. If you move your admin account to a different group, you will prevent yourself from logging into the router.

Step 1. Log in to the web-based utility of the router.

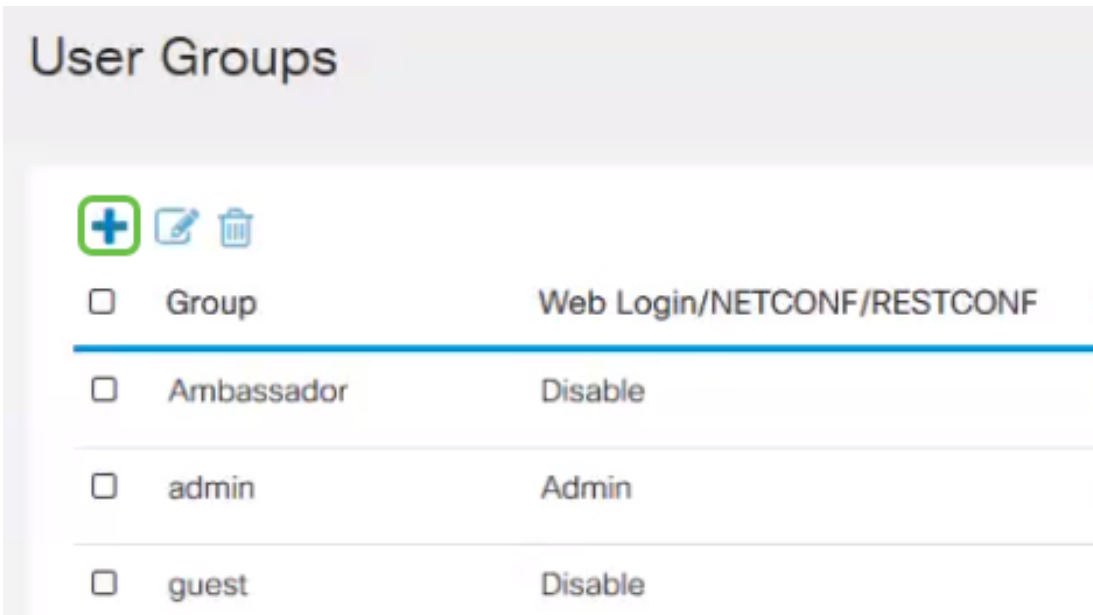


The screenshot shows the login interface for a Cisco Router. At the top, the word "Router" is displayed in a large, black, sans-serif font. Below this, the username "cisco" is entered into a text field. The password field is masked with ten black dots. A language selection dropdown menu is set to "English" with a downward-pointing arrow. A blue "Login" button is positioned below the form fields. 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."

Step 2. Select **System Configuration > User Groups**.



Step 3. Click the **plus** icon to add a User Group.



Step 4. In the Overview area, enter the name of the group in the *Group Name* field.

User Groups

Group Name:

Local User Membership List



Step 5. Under *Local User Membership List*, click the **plus** icon and select the user from the drop-down list. If you want to add more, press the **plus** icon again and select another member to be added. Members can only be part of one group. If you do not have all of the users entered already, you can add more in the [Create a User Account](#) section.

Local User Membership List

1



User

1 John

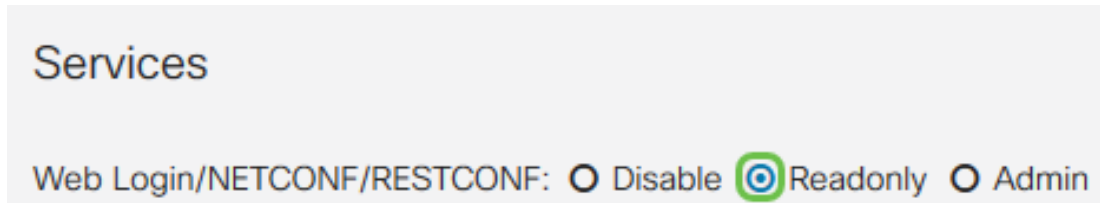
2 Kevin

3 **2** Teri

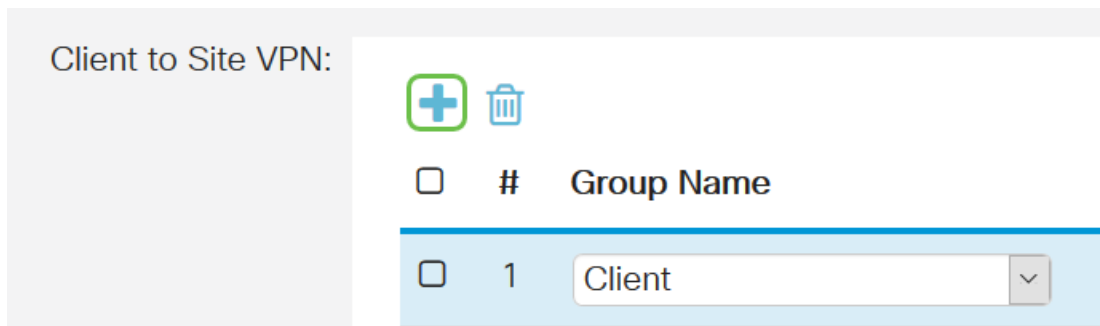
Step 6. Under *Services*, choose a permission to be granted to the users in the group. The options

are:

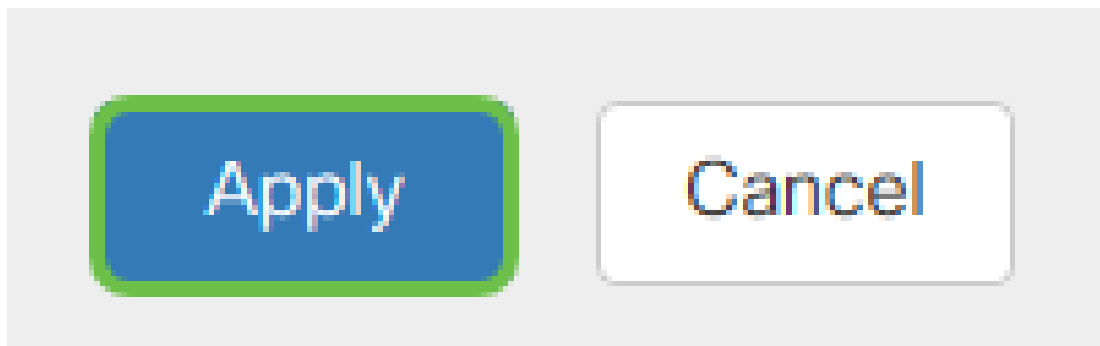
- Disabled — This option means that members of the group are not permitted to access the web-based utility through a browser.
- Readonly — This option means that the members of the group can only read the status of the system after they log in. They cannot edit any of the settings.
- Admin — This option gives the members of the group read and write privileges, and be able to configure the system status.



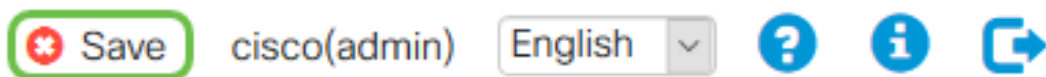
Step 7. Click the **plus** icon to add an existing Client-to-Site VPN. If you have not configured this, you can find information in this article under the section [Create a Client-to-Site Profile](#).




Step 8. Click **Apply**.



Step 9. Click **Save**.



Step 10. Click **Apply** once again to save the Running Configuration to the Startup Configuration.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC
Startup configuration: 2019-Jan-29, 17:52:43 UTC
Mirror Configuration: 2019-Jan-27, 23:00:07 UTC
Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.
To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Step 11. When you receive the confirmation, click **OK**.

Information ✕

 Running configuration saved to startup configuration



You should now have successfully created a user group on the RV160 or RV260 Series Router.

Create a User Account

Step 1. Log in to the web-based utility of the router and choose **System Configuration > User Accounts**.



System Configuration

1

Initial Router Setup

System

Time

Log

Email

2

User Accounts

User Groups

Step 2. In the *Local Users* area, click the **add** icon.

Local Users



Username

John


Kevin

Teri

cisco

Step 3. Enter a name for the user in the *Username* field, the password, and the group you want to add the user to from the drop-down menu. Click **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: 2

Confirm Password: 3



Password Strength meter: 

Group: 4


5

Note: When the client sets up TheGreenBow Client on their computer, they would log in with this same username and password.

Step 4. Click **Save**.

cisco(admin) English   

Step 5. Click **Apply** once again to save the Running Configuration to the Startup Configuration.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Step 6. When you receive the confirmation, click **OK**.

Information ×

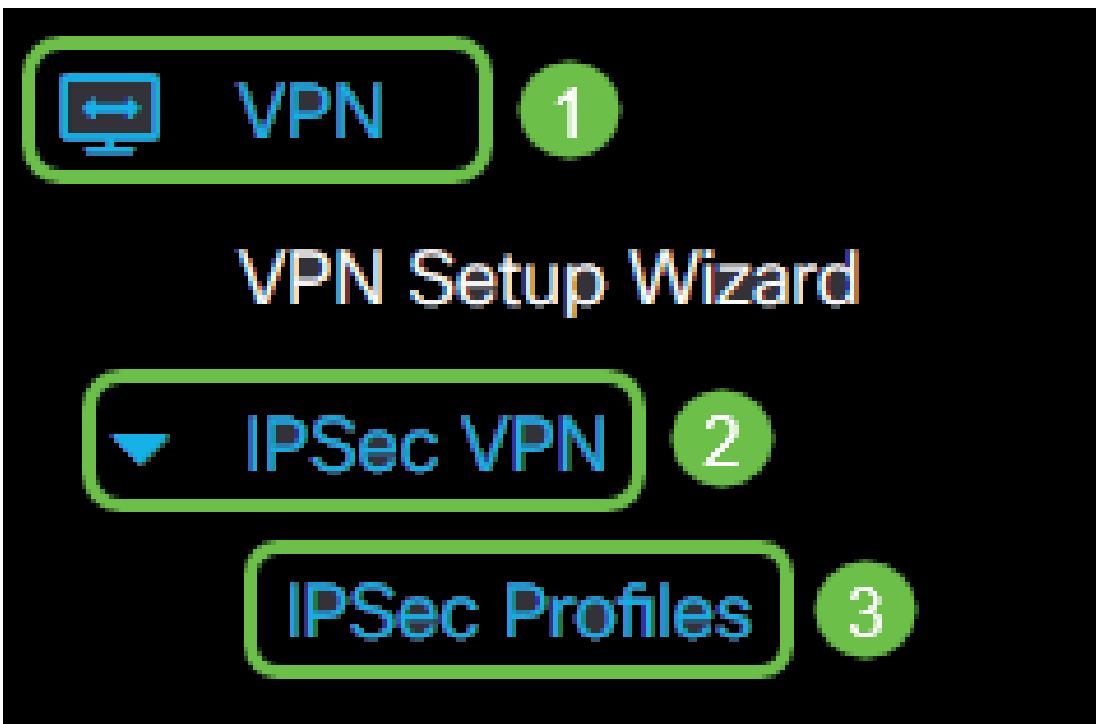
i Running configuration saved to startup configuration

OK

You should now have created a User Account on your RV160 or RV260 router.

Configure IPsec Profile

Step 1. Log in to the web-based utility of the RV160 or RV260 router and choose **VPN > IPsec VPN > IPsec Profiles**.



Step 2. The IPsec Profiles Table shows the existing profiles. Click the **plus** icon to create a new profile.

IPSec Profiles



Name

Default

Amazon_Web_Services

Microsoft_Azure

VPNTTest

Note: Amazon_Web_Services, Default, and Microsoft_Azure are default profiles.

Step 3. Create a name for the profile in the *Profile Name* field. The profile name must contain only alphanumeric characters and an underscore (_) for special characters.

Add/Edit a New IPSec Profile

Profile Name:

TheGreenBow

Keying Mode:

Auto Manual

IKE Version:

IKEv1 IKEv2

Step 4. Click a radio button to determine the key exchange method the profile will use to authenticate. The options are:

- Auto — Policy parameters are set automatically. This option uses an Internet Key Exchange (IKE) policy for data integrity and encryption key exchanges. If this is chosen, the configuration settings under the Auto Policy Parameters area are enabled.

- Manual — This option allows you to manually configure the keys for data encryption and integrity for the VPN tunnel. If this is chosen, the configuration settings under the Manual Policy Parameters area are enabled. This is not widely used.

Add/Edit a New IPSec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Note: For this example, **Auto** was chosen.

Step 5. Select the IKE Version. Be sure when you set up TheGreenBow on the client side, the same version is selected.

Add/Edit a New IPSec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Configure the Phase 1 and 2 Settings

Step 1. In the Phase 1 Options area, choose the appropriate Diffie-Hellman (DH) group to be used with the key in Phase 1 from the *DH Group* drop-down list. Diffie-Hellman is a cryptographic key exchange protocol which is used in the connection to exchange pre-shared key sets. The strength of the algorithm is determined by bits. The options are:

- Group2-1024 bit — This option computes the key slower, but is more secure than Group 1.
- Group5-1536 bit — This option computes the key the slowest, but is the most secure.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

28800

Step 2. From the *Encryption* drop-down list, choose an encryption method to encrypt and decrypt Encapsulating Security Payload (ESP) and Internet Security Association and Key Management Protocol (ISAKMP). The options are:

- 3DES — Triple Data Encryption Standard. Not recommended. Only use it if it's required for backwards compatibility as it's vulnerable to some "block collision" attacks.
- AES-128 — Advanced Encryption Standard uses a 128-bit key. Advanced Encryption Standard (AES) is a cryptographic algorithm that is designed to be more secure than DES. AES uses a larger key size which ensures that the only known approach to decrypt a message is for an intruder to try every possible key.
- AES-192 — Advanced Encryption Standard uses a 192-bit key.
- AES-256 — Advanced Encryption Standard uses a 256-bit key. This is the most secure encryption option.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

AES-128

Authentication:

MD5

SA Lifetime:

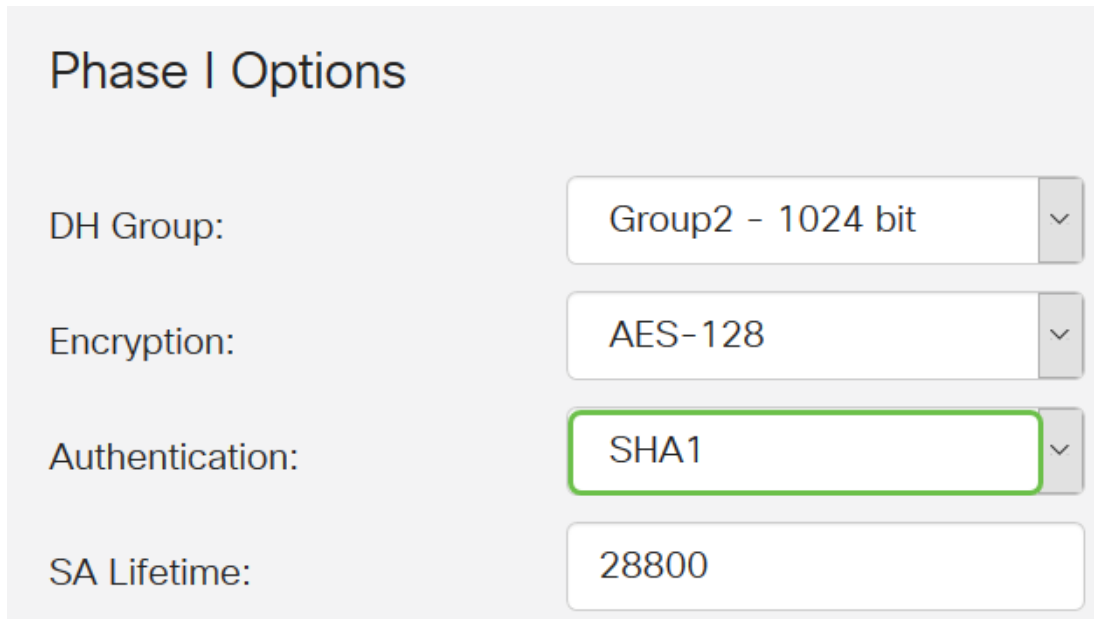
28800

Note: AES is the standard method of encryption over DES and 3DES for its greater performance and security. Lengthening the AES key will increase security with a drop in performance.

Step 3. From the *Authentication* drop-down list, choose an authentication method that will determine how ESP and ISAKMP are authenticated. The options are:

- MD5 — Message-Digest Algorithm has a 128-bit hash value.
- SHA-1 — Secure Hash Algorithm has a 160-bit hash value.
- SHA2-256 — Secure Hash Algorithm with a 256-bit hash value. This is the most secure and recommended algorithm.

Note: Make sure that both ends of the VPN tunnel use the same authentication method.



The image shows a configuration window titled "Phase I Options". It contains four settings:

- DH Group:** A dropdown menu with "Group2 - 1024 bit" selected.
- Encryption:** A dropdown menu with "AES-128" selected.
- Authentication:** A dropdown menu with "SHA1" selected. This field is highlighted with a green border.
- SA Lifetime:** A text input field containing the value "28800".

Note: MD5 and SHA are both cryptographic hash functions. They take a piece of data, compact it, and create a unique hexadecimal output that typically cannot be reproduced. In this example, SHA1 is chosen.

Step 4. In the *SA Lifetime* field, enter a value between 120 and 86400. The default value is 28800. The *SA Lifetime (Sec)* tells you the amount of time, in seconds, an IKE SA is active in this phase. A new Security Association (SA) is negotiated before the lifetime expires to ensure that a new SA is ready to be used when the old one expires. The default is 28800 and the range is from 120 to 86400. We will be using 28800 seconds as our SA Lifetime for Phase I.

Note: It is recommended that your SA Lifetime in Phase I is longer than your Phase II SA Lifetime. If you make your Phase I shorter than Phase II, then you will be having to renegotiate the tunnel back and forth frequently as opposed to the data tunnel. Data tunnel is what needs more security so it is better to have the lifetime in Phase II to be shorter than Phase I.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

AES-128

Authentication:

SHA1

SA Lifetime:

28800

Step 5. From the *Protocol Selection* drop-down list in the Phase II Options area, choose a protocol type to apply to the second phase of the negotiation. The options are:

- ESP — This option is also known as Encapsulating Security Payload. This option encapsulates the data to be protected. If this option is chosen, proceed to Step 6 to choose an encryption method.
- AH — This option is also known as Authentication Header (AH). It is a security protocol which provides data authentication and optional anti-replay service. AH is embedded in the IP datagram to be protected. If this option is chosen, skip to Step 7.

Phase II Options

Protocol Selection:

ESP

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

3600

Perfect Forward Secrecy:

Enable

DH Group:

Group2 - 1024 bit

Step 6. If ESP was chosen in Step 6, choose an *Encryption*. The options are:

- 3DES — Triple Data Encryption Standard
- AES-128 — Advanced Encryption Standard uses a 128-bit key.
- AES-192 — Advanced Encryption Standard uses a 192-bit key.
- AES-256 — Advanced Encryption Standard uses a 256-bit key.

Phase II Options

Protocol Selection:	ESP	▼
Encryption:	AES-128	▼
Authentication:	MD5	▼
SA Lifetime:	3600	
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	Group2 - 1024 bit	▼

Step 7. From the *Authentication* drop-down list, choose an authentication method that will determine how ESP and ISAKMP are authenticated. The options are:

- MD5 — Message-Digest Algorithm has a 128-bit hash value.
- SHA-1 — Secure Hash Algorithm has a 160-bit hash value.
- SHA2-256 — Secure Hash Algorithm with a 256-bit hash value.

Phase II Options

Protocol Selection:	ESP	▼
Encryption:	AES-128	▼
Authentication:	SHA1	▼
SA Lifetime:	3600	
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	Group2 - 1024 bit	▼

Step 8. In the *SA Lifetime* field, enter a value between 120 and 28800. This is the length of time the IKE SA will remain active in this phase. The default value is 3600.

Phase II Options

Protocol Selection:

ESP

Encryption:

AES-128

Authentication:

SHA1

SA Lifetime:

3600

Step 9. (Optional) Check the **Enable** Perfect Forward Secrecy check box to generate a new key for IPsec traffic encryption and authentication. Perfect Forward Secrecy is used to improve the security of communications transmitted across the Internet using public key cryptography. Check the box to enable this feature, or uncheck the box to disable this feature. This feature is recommended.

Perfect Forward Secrecy:

Enable

DH Group:

Group2 - 1024 bit

Step 10. From the *DH Group* drop-down list, choose a DH group to be used with the key in Phase 2. The options are:

- Group2-1024 bit — This option computes the key faster, but is less secure.
- Group5-1536 bit — This option computes the key the slowest, but is the most secure.

Phase II Options

Protocol Selection:

ESP

Encryption:

AES-128

Authentication:

SHA1

SA Lifetime:

3600

Perfect Forward Secrecy:

Enable

DH Group:

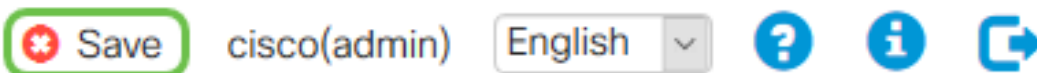
Group2 - 1024 bit

Step 11. Click **Apply**.

Apply

Cancel

Step 12. Click **Save** to save the configuration permanently.



Step 13. Click **Apply** once again to save the Running Configuration to the Startup Configuration.

Configuration Management Apply

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

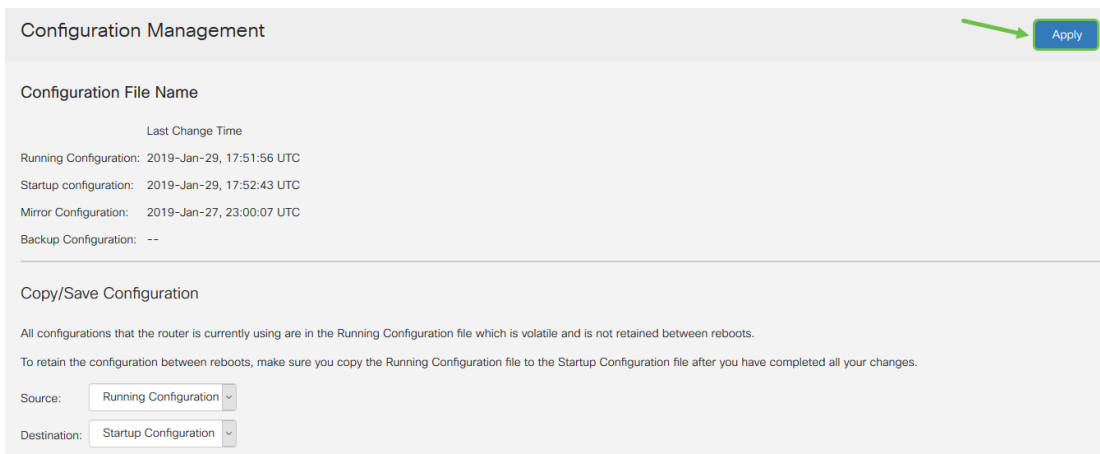
All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source: Running Configuration

Destination: Startup Configuration

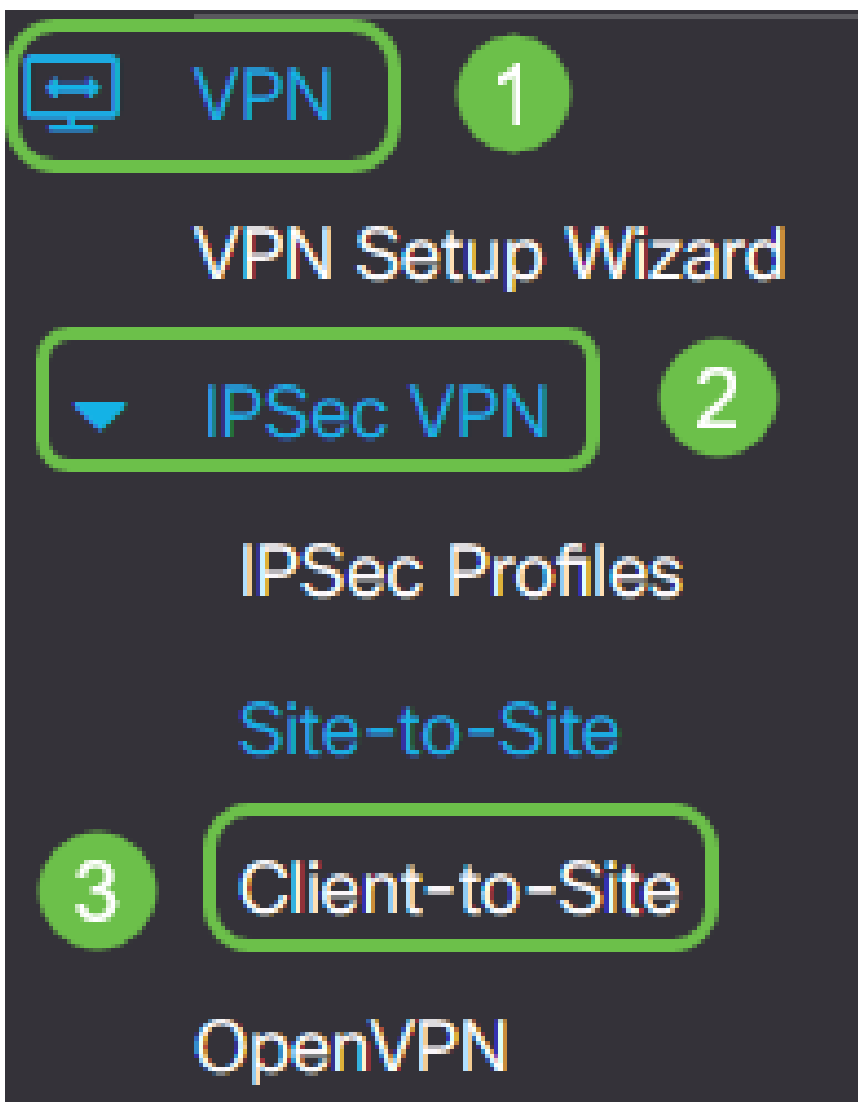
Step 14. When you receive the confirmation, click **OK**.



You should now have successfully configured an IPsec Profile on your RV160 or RV260 router.

Create a Client-to-Site Profile

Step 1. Choose **VPN > IPsec VPN > Client-to-Site** .



Step 2. Click the **plus** icon.

IPSec Profiles



<input type="checkbox"/>	Name	Policy	IKE Version
<input type="checkbox"/>	Default	Auto	IKEv1
<input type="checkbox"/>	Amazon_Web_Services	Auto	IKEv1
<input type="checkbox"/>	Microsoft_Azure	Auto	IKEv1

Step 3. Under the Basic Settings tab, check the **Enable** check box to ensure that the VPN profile is active.

Add/Edit a New Tunnel

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

Step 4. Enter a name for the VPN connection in the *Tunnel Name* field.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

IPSec Profile:

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

Step 5. Choose the IPsec Profile to be used from the *IPsec* drop-down list.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

IPSec Profile:

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

Step 6. Choose the Interface from the *Interface* drop-down list.

Basic Settings | Advanced Settings

Enable:

Tunnel Name: Client

IPSec Profile: TheGreenBow (Auto Profile (IKEv1) is chosen.)

Interface: WAN

⚠️ Configure higher lifetimes if this profile is used for Windows Clients.

Note: The options depend on the model of router you are using. In this example, WAN is chosen.

Step 7. Choose an IKE authentication method. The options are:

- Pre-shared Key — This option will let us use a shared password for the VPN connection.
- Certificate — This option uses a digital certificate that contains information such as the name, or IP address, serial number, expiration date of the certificate, and a copy of the public key of the bearer of the certificate.

IKE Authentication Method

Pre-shared Key:

Please enter a valid Preshared Key.

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate: Default

Note: A Pre-shared key can be whatever you want it to be, it just has to match at the site and with the client when they set up TheGreenBow Client on their computer.

Step 8. Enter the connection password in the *Pre-shared Key* field.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable


Certificate: Default

Step 9. (Optional) Uncheck the *Minimum Pre-shared Key Complexity* **Enable** check box to be able to use a simple password.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter: 

Minimum Preshared Key Complexity: Enable

Certificate:


Note: In this example, Minimum Pre-shared Key Complexity is left enabled.

Step 10. (Optional) Check the *Show Pre-shared Key* **Enable** check box to show the password in plain text.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter: 

Minimum Preshared Key Complexity: Enable

Certificate:

Note: In this example, Show Pre-shared key is left disabled.

Step 11. Choose a local identifier from the *Local Identifier* drop-down list. The options are:

- Local WAN IP — This option uses the IP address of the Wide Area Network (WAN) Interface of the VPN gateway.
- IP Address — This option allows you to manually enter an IP address for the VPN connection. This is the WAN IP address of the router at the site (office).
- FQDN — This option is also known as Fully Qualified Domain Name (FQDN). It lets you use a complete domain name for a specific computer on the Internet.
- User FQDN — This option lets you use a complete domain name for a specific user on the Internet.

Local Identifier:

Remote Identifier:

Note: In this example, IP Address is chosen and the WAN IP Address of the router at the site is entered. In this example, 24.x.x.x has been entered. The complete address has been blurred for privacy purposes.

Step 12. Choose an identifier for the remote host. The options are:

- IP Address — This option uses the WAN IP address of the VPN client. To find out the WAN IP address you can enter “what is my IP” into your web browser. This is the client IP address.
- FQDN — Fully Qualified Domain Name. This option lets you use a complete domain name for a specific computer on the Internet.
- User FQDN — This option lets you use a complete domain name for a specific user on the Internet.

Note: In this example, IP Address is chosen and the current IPv4 address of the router at the location of the client is entered. This can be determined by doing a search for “What’s my IP address” in your web browser. This address can change so if you have problems connecting after a successful configuration, this can be an area to check and change on both the client and at the site.

Local Identifier:

Remote Identifier: 1 2

Step 13. (Optional) Check the **Extended Authentication** check box to activate the feature. When activated, this will provide an additional level of authentication that will require remote users to key in their credentials before being granted access to the VPN.

Extended Authentication +

Group Name

Step 14. (Optional) Choose the group that will be using extended authentication by clicking the **plus** icon and select the user from the drop-down list.

Extended Authentication 1

Group Name

CiscoTest123

KevGroupTest

2

Note: In this example, **VPNUsers** is chosen.

Step 15. Under *Pool Range for Client LAN*, enter the first IP and end IP address that can be

assigned to a VPN client. This needs to be a pool of addresses that doesn't overlap with the site addresses. These may be referred to as virtual interfaces. If you receive a message that a virtual interface needs to be changed this is where you would fix that.

Pool Range for Client LAN:

Start IP:

1

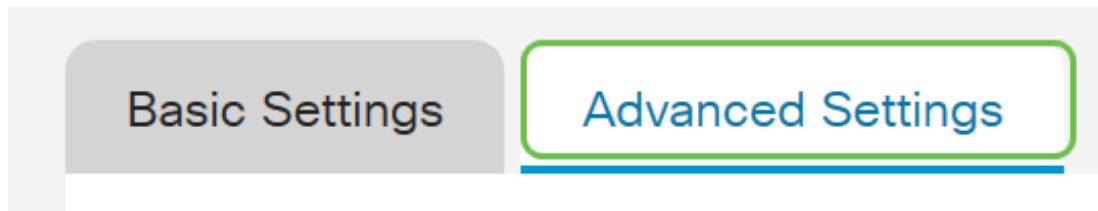
10.2.1.1

End IP:

2

10.2.1.100

Step 16. Select the **Advanced Settings** Tab.



Step 17. (Optional) Scroll down to the bottom of the page and select **Aggressive Mode**. Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IP security (IPsec) peer and to initiate an Internet Key Exchange (IKE) aggressive mode negotiation with the tunnel. For more information on Aggressive Mode vs. Main Mode click [here](#).

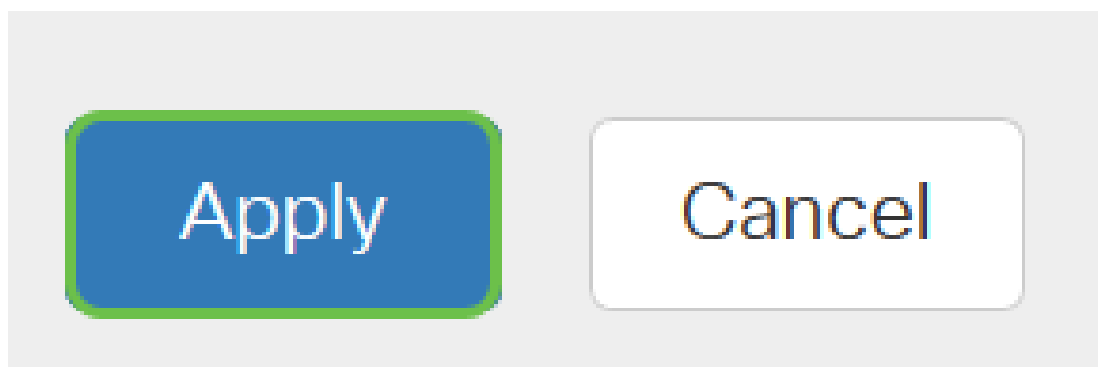
Additional Settings

Aggressive Mode

Compress (Support IP Payload Compression Protocol (IPComp))

Note: The Compress check box enables the router to propose compression when it starts a connection. This protocol reduces the size of IP datagrams. If the responder rejects this proposal, then the router does not implement compression. When the router is the responder, it accepts compression, even if compression is not enabled. If you enable this feature for this router, you would need to enable it on the remote router (the other end of the tunnel). In this example, *Compress* was left unchecked.

Step 18. Click **Apply**.



Step 19. Click **Save**.



cisco(admin)

English



Step 20. Click **Apply** once again to save the Running Configuration to the Startup Configuration.

Configuration Management Apply

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Step 21. When you receive the confirmation, click **OK**.

Information



Running configuration saved to startup configuration

OK

You should now have configured the Client-to-Site Tunnel on the router for TheGreenBow VPN Client.

Configure TheGreenBow VPN Client on the Computer of the Remote Worker

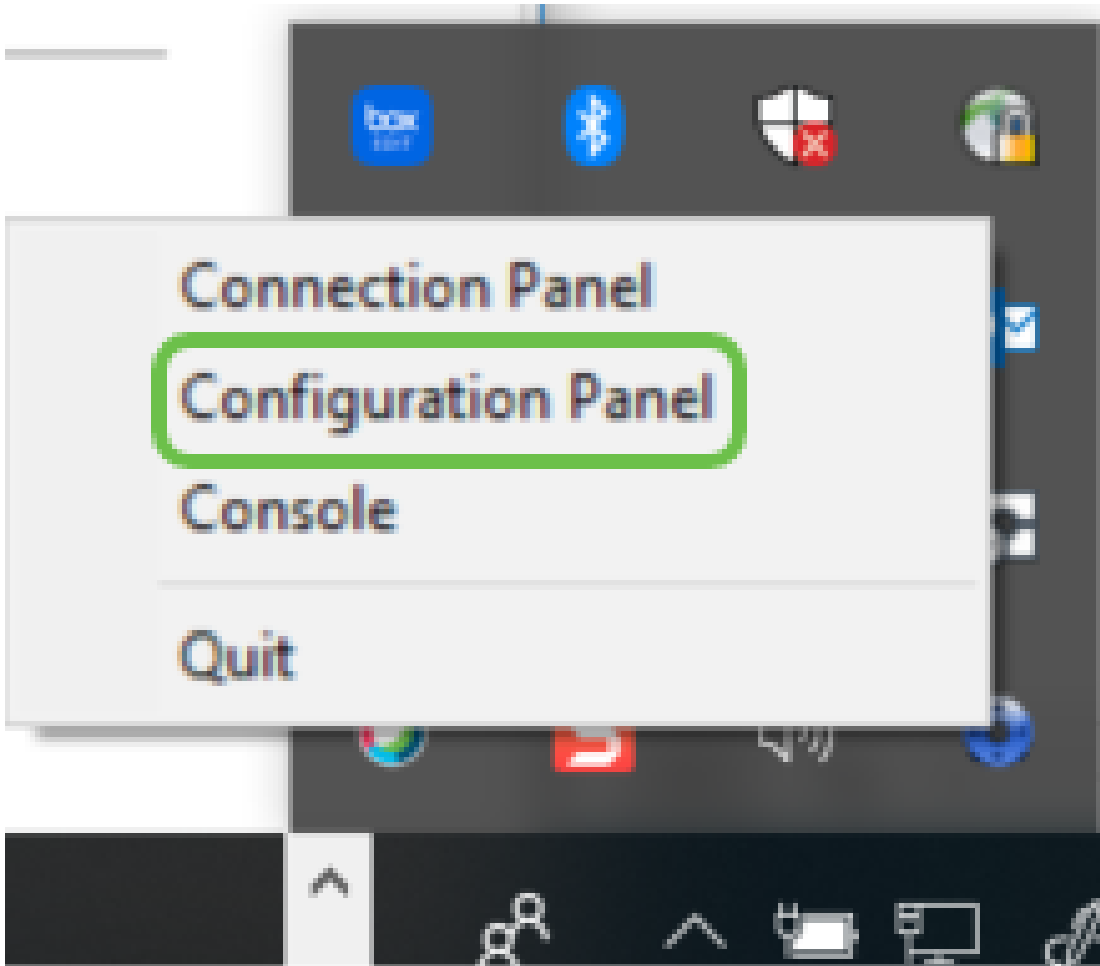
Configure Phase 1 Settings

To download the latest release of TheGreenBow IPsec VPN Client software, click [here](#).

Step 1. Right-click TheGreenBow VPN Client icon. This is located on the lower right corner of the taskbar.

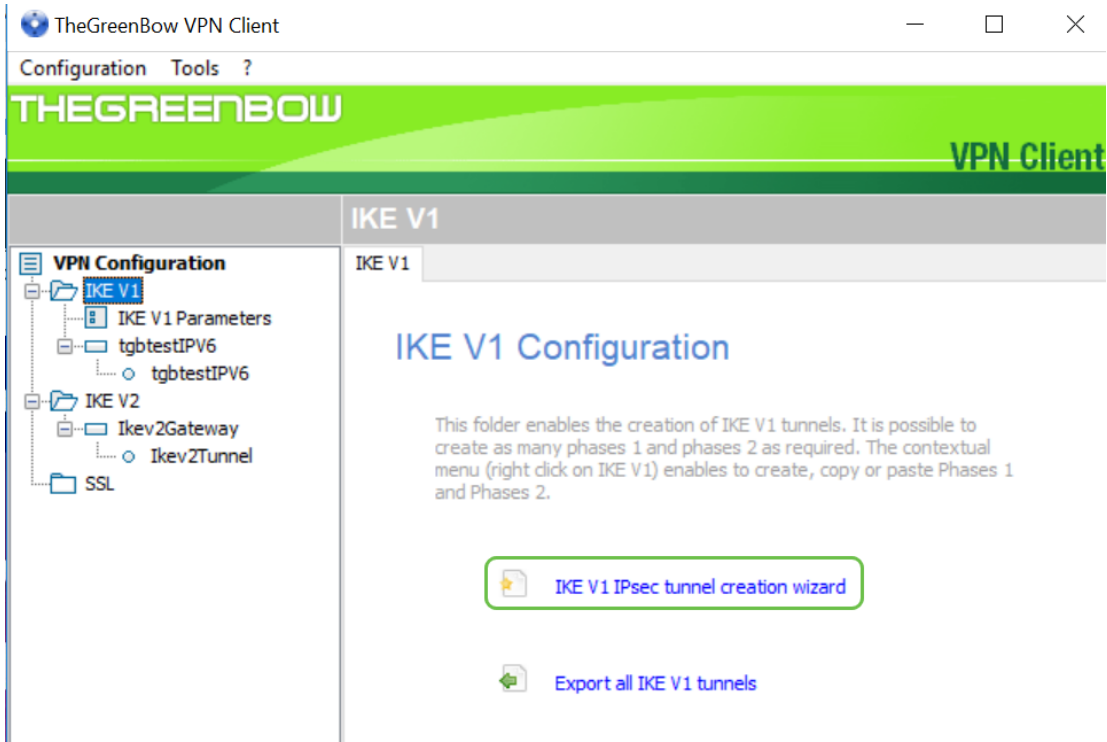


Step 2. Select **Configuration Panel**.



Note: This is an example on a Windows computer. This may vary depending on the software you use.

Step 3. Select **IKE V1 IPsec tunnel creation wizard**.



Note: In this example, IKE Version 1 is being configured. If you would like to configure IKE Version 2, you would follow the same steps but right-click on the IKE V2 folder. You would also need to select IKEv2 for the IPsec profile on the router at the site.

Step 4. Fill in the public WAN IP address of the router at the site (office) where the file server is located, the Preshared Key, and the private internal address of the remote network on site. Click **Next**. In this example, the site is 24.x.x.x. The last three octets (sets of numbers in this IP address) have been replaced with an x to protect this network. You would enter the full IP address.

VPN Configuration Wizard



VPN tunnel parameters

2/3

Enter the following parameters for the VPN tunnel:

IP or DNS public (external) address:
of the remote gateway 1

Preshared key: 2

IP private (internal) address:
of the remote network 3

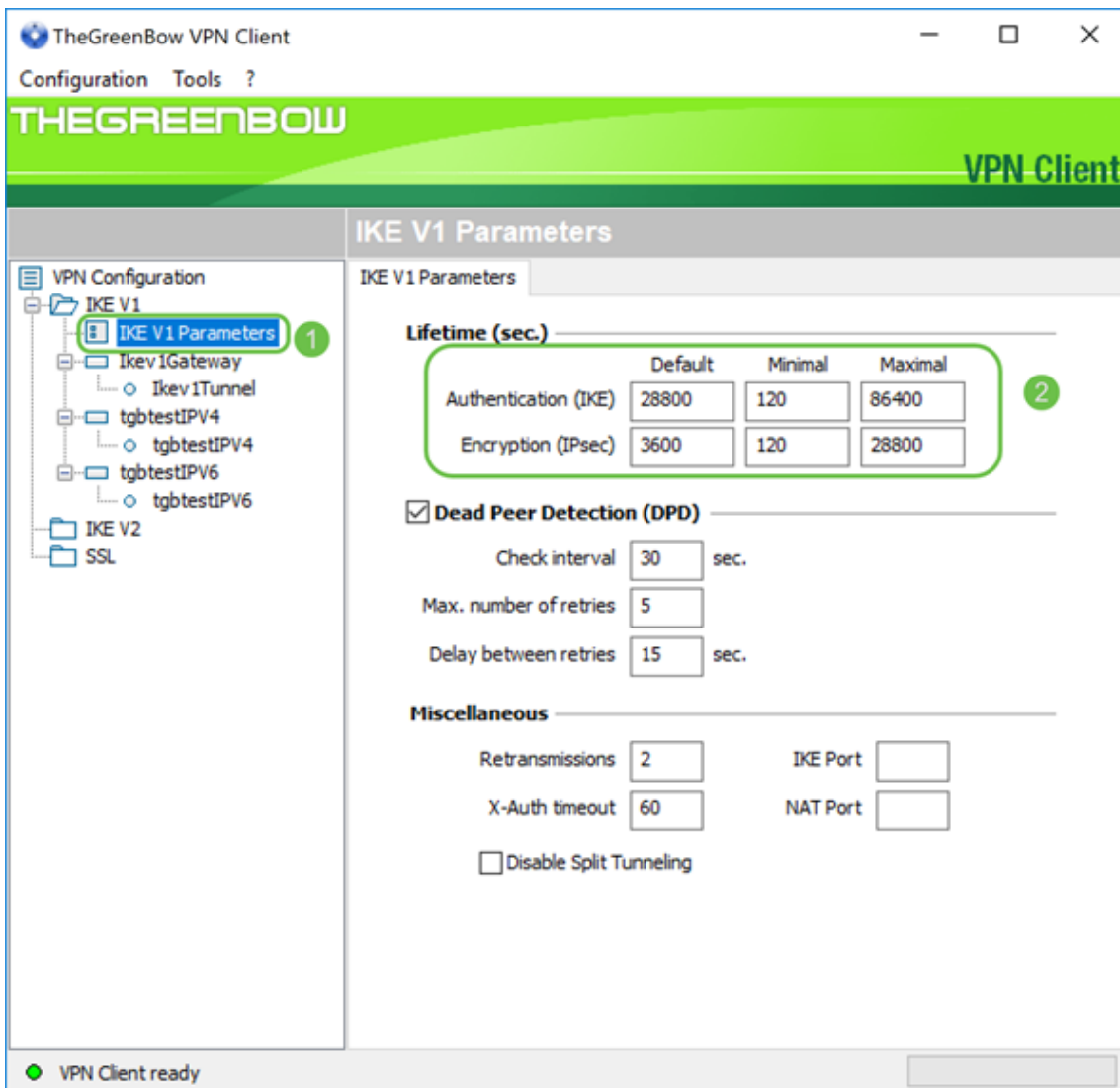
< Previous **Next >** 4 Cancel

Step 5. Click **Finish**.

You may change these parameters anytime directly with the main interface.

< Previous **Finish** Cancel

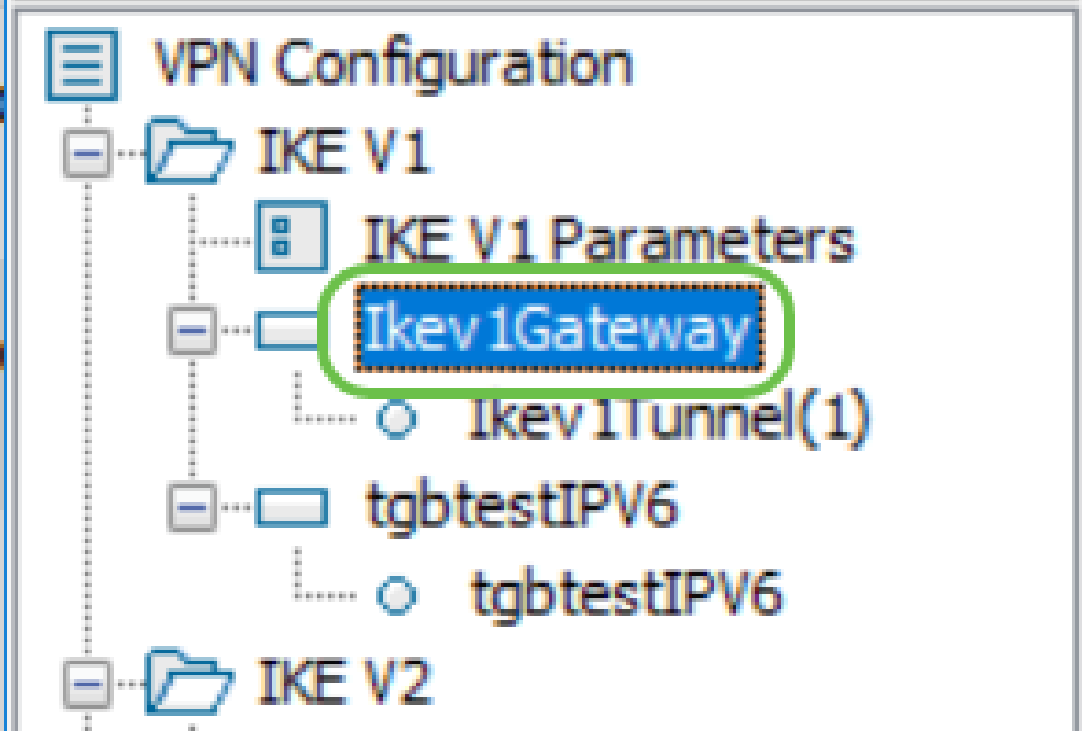
Step 6 (Optional) You can change the IKE V1 Parameters. TheGreenBow Default, Minimal, and Maximal lifetime can be adjusted. In this location you can enter whatever the range of the lifetime that the router accepts.



Step 7. Click on the gateway you created.

Configuration Tools ?

THEGREENBOW



Step 8. In the *Authentication* tab under *Addresses* you will see a drop-down list of local addresses. You can choose one or select **Any**, as shown below.

Configuration Tools ?

THEGREENBOW

VPN

Ikev1Gateway: Authentication

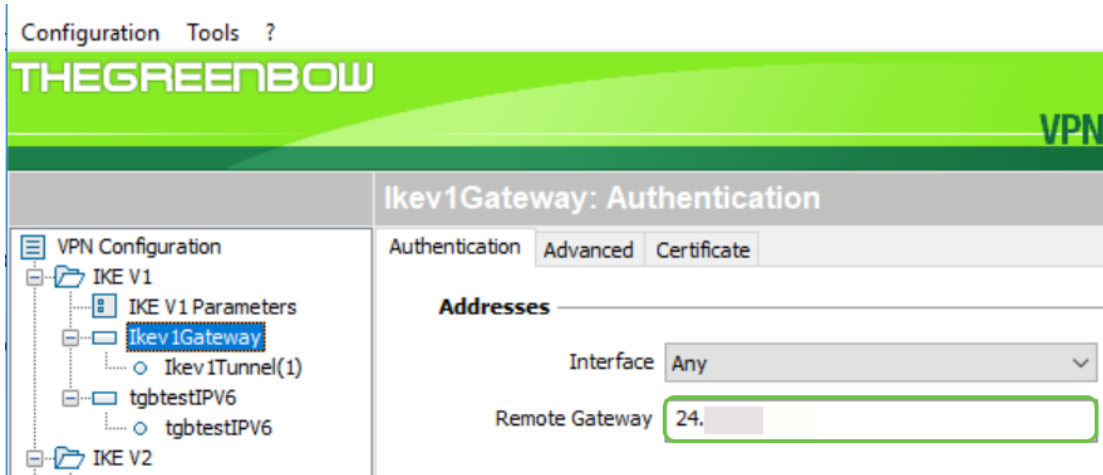
Authentication | Advanced | Certificate

Addresses

Interface: Any

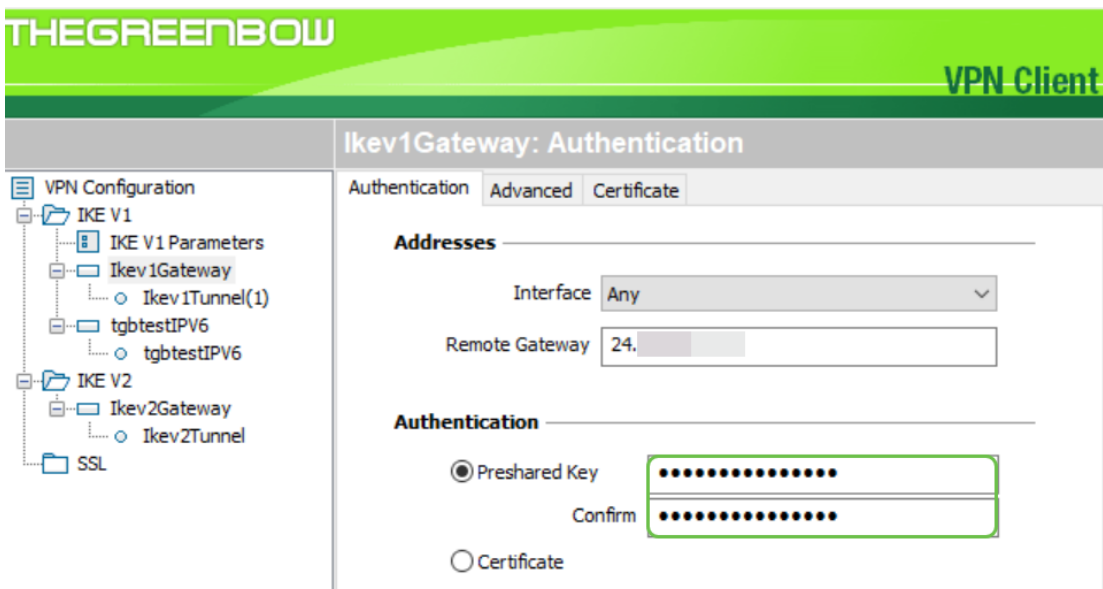
Remote Gateway:

Step 9. Enter the address of the remote gateway in the *Remote Gateway* field. This can be an IP address or a DNS name. This is the address of the public IP address for router at the site (office).



Step 10. Under *Authentication*, choose the authentication type. The options are:

- Preshared Key — This option will let the user use a password that has been configured on the VPN gateway. The password has to be matched by the user to be able to establish a VPN tunnel.
- Certificate — This option will utilize a certificate to complete the handshake between the VPN Client and the VPN Gateway.



Note: In this example, the Pre-shared Key that was configured on the router was entered and confirmed.

Step 11. Under *IKE*, set the Encryption, Authentication, and Key Group settings to match the configuration of the router.

IKE

Encryption	AES 128	▼
Authentication	SHA-1	▼
Key Group	DH2 (1024)	▼

Step 12. Click the **Advanced** tab.

Ikev1Gateway: Authentication

Authentication **Advanced** Certificate

Step 13. Under Advanced features, check the **Mode Config** and the **Aggressive Mode** check box. The Aggressive Mode was selected on the RV160 in the Client-to-Site profile of this example. Leave the NAT-T setting to Automatic.

VPN Client

thegreenbowvpn: Authentication

Authentication Advanced Certificate

Advanced features

1 Mode Config

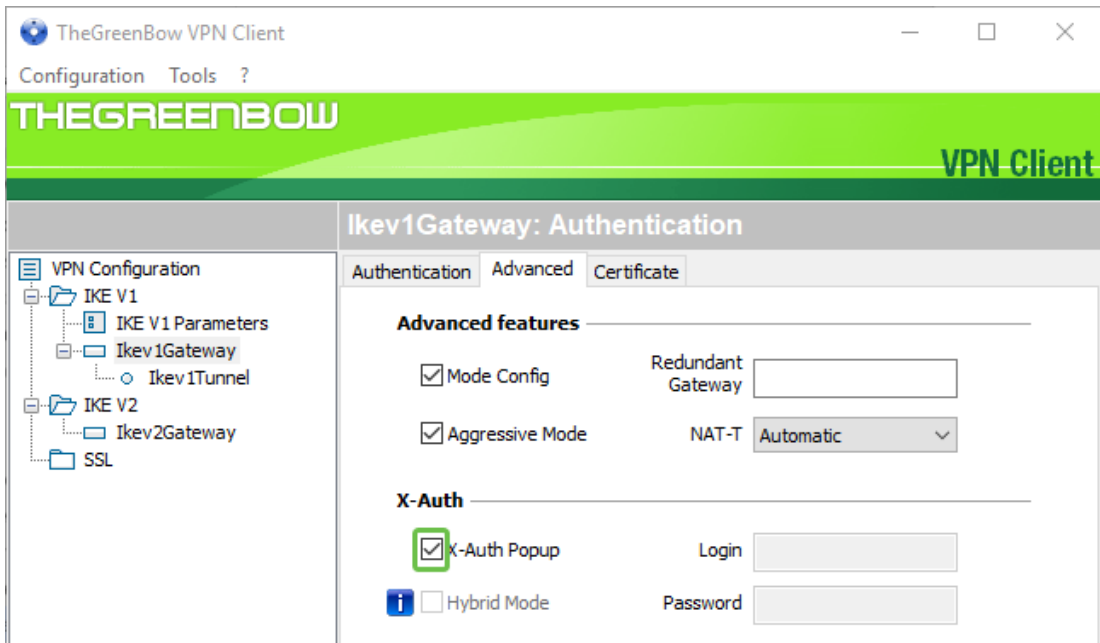
2 Aggressive Mode

Redundant Gateway

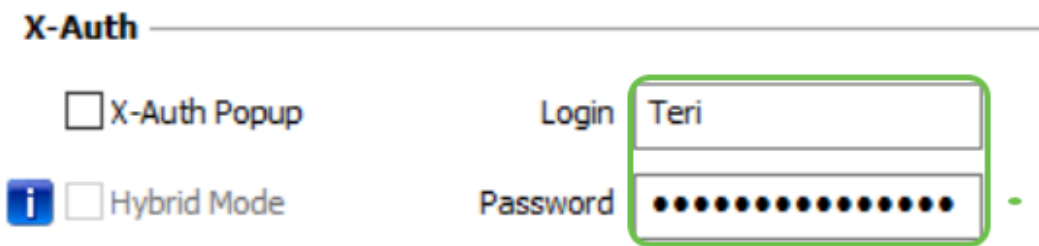
NAT-T Automatic ▼

Note: With Mode Config enabled, TheGreenBow VPN Client will pull settings from the VPN gateway to attempt to establish a tunnel. NAT-T makes establishing a connection faster.

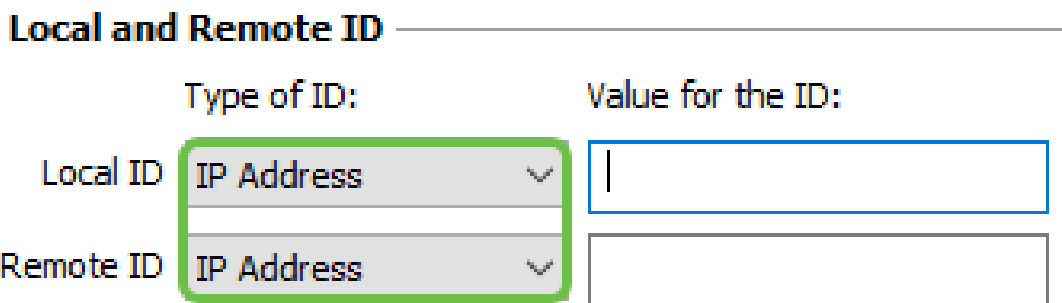
Step 14. (Optional) Under *X-Auth*, you can check the **X-Auth Popup** check box to automatically pull up the login window when starting a connection. The login window is where the user enters their credentials to be able to complete the tunnel.



Step 15. (Optional) If you don't select *X-Auth Popup*, enter your username in the *Login* field. This is the user name that was entered when a user account was created in the VPN gateway and password at the site.



Step 16. Under *Local and Remote ID*, set the Local ID and the Remote ID to match the settings of the VPN gateway.



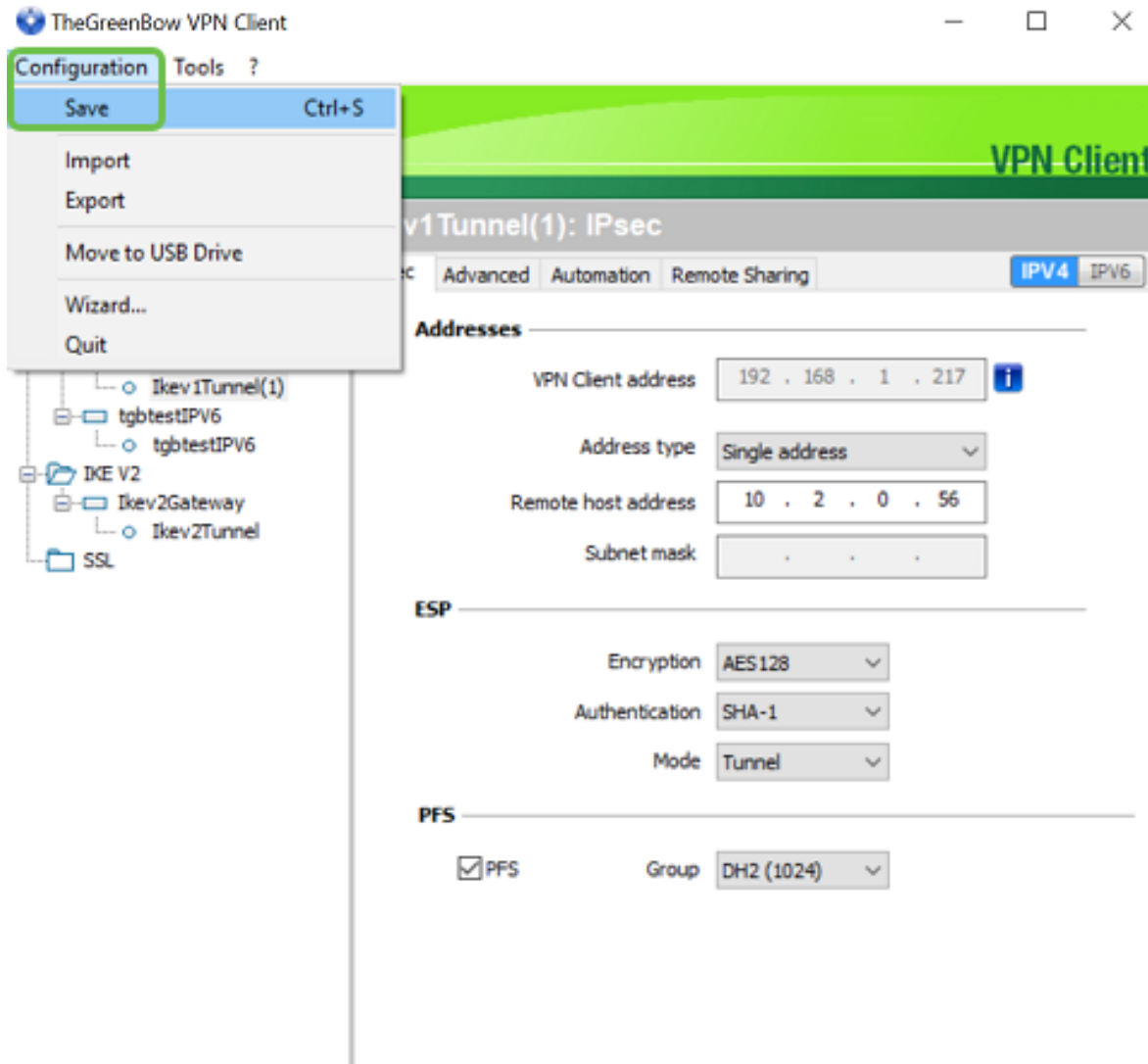
Note: In this example, both Local ID and Remote ID are set to IP Address to match the settings of the RV160 or RV260 VPN gateway.

Step 17. Under *Value for the ID*, enter the local ID and remote ID in their respective fields. The local ID is the WAN IP address for the client. This can be found by doing a web search for "What's my IP". The remote ID is the WAN IP address of the router at the site.

Local and Remote ID

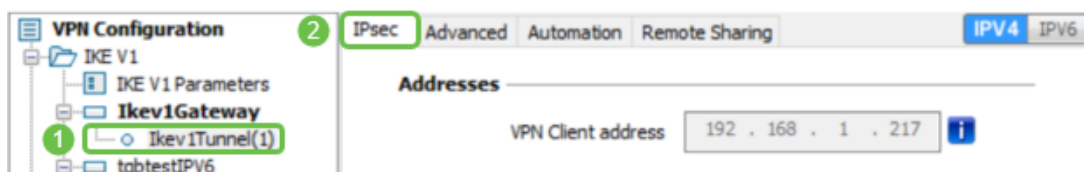
	Type of ID:	Value for the ID:
Local ID	IP Address	108.233.
Remote ID	IP Address	24.

Step 18. Click **Configuration** and choose **Save**.



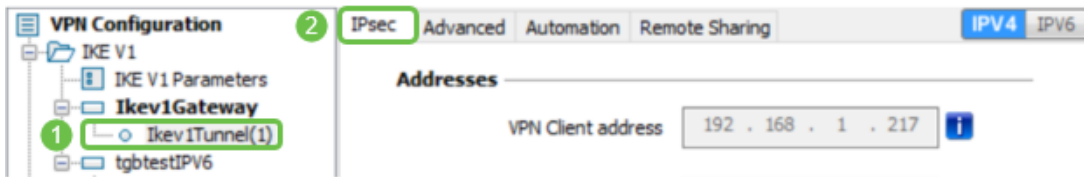
Configure Tunnel Settings

Step 1. Click the **Ikev1Tunnel(1)** (yours may have a different name) and the **IPsec** tab. The VPN Client address is automatically populated if you selected Mode Config in the Ikev1Gateway advanced settings. This displays the local IP address of the computer/laptop at the remote location.



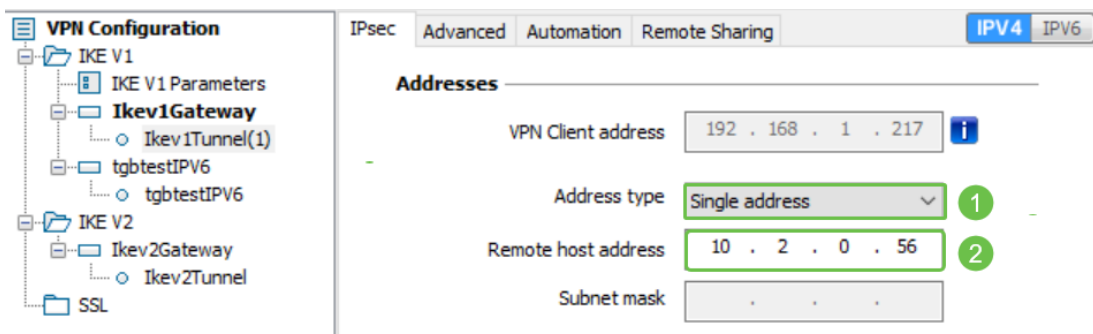
Step 2. Choose the address type that the VPN client can access from the *Address type* drop-down

list. This can be a Single address, Range of addresses, or a Subnet address. The default, Subnet address, automatically includes the VPN Client address (the local IP address of the computer), Remote LAN address, and Subnet mask. If Single address or Range of addresses is selected, these fields will need to be filled in manually. Enter the network address that should be accessed by the VPN tunnel in the *Remote LAN address* field and the subnet mask of the remote network in the *Subnet mask* field.

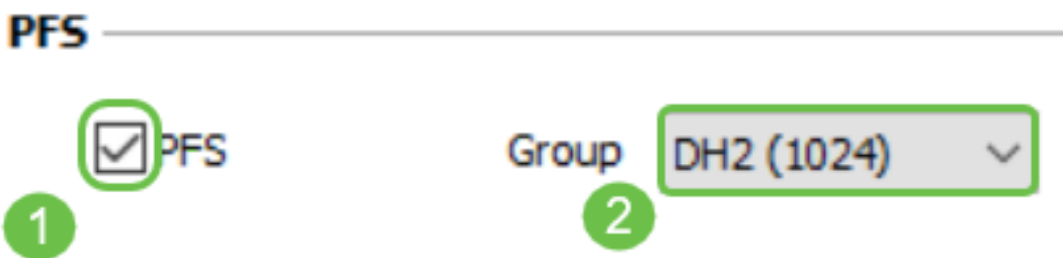


Note: In this example, Single address was chosen and the local IP address of the router at the site is entered.

Step 3. Under *ESP*, set the Encryption, Authentication, and Mode to match the settings of the VPN gateway at the site (office).



Step 4. (Optional) Under *PFS*, check the **PFS** check box to enable Perfect Forward Secrecy (PFS). PFS generates random keys for encrypting the session. Select a PFS group setting from the *Group* drop-down list. If it was enabled on the router, it should also be enabled here.









Step 5. (Optional) Right-click on the name of the Ikev1Gateway and click on the rename section if you would like to rename it.

TheGreenBow VPN Client

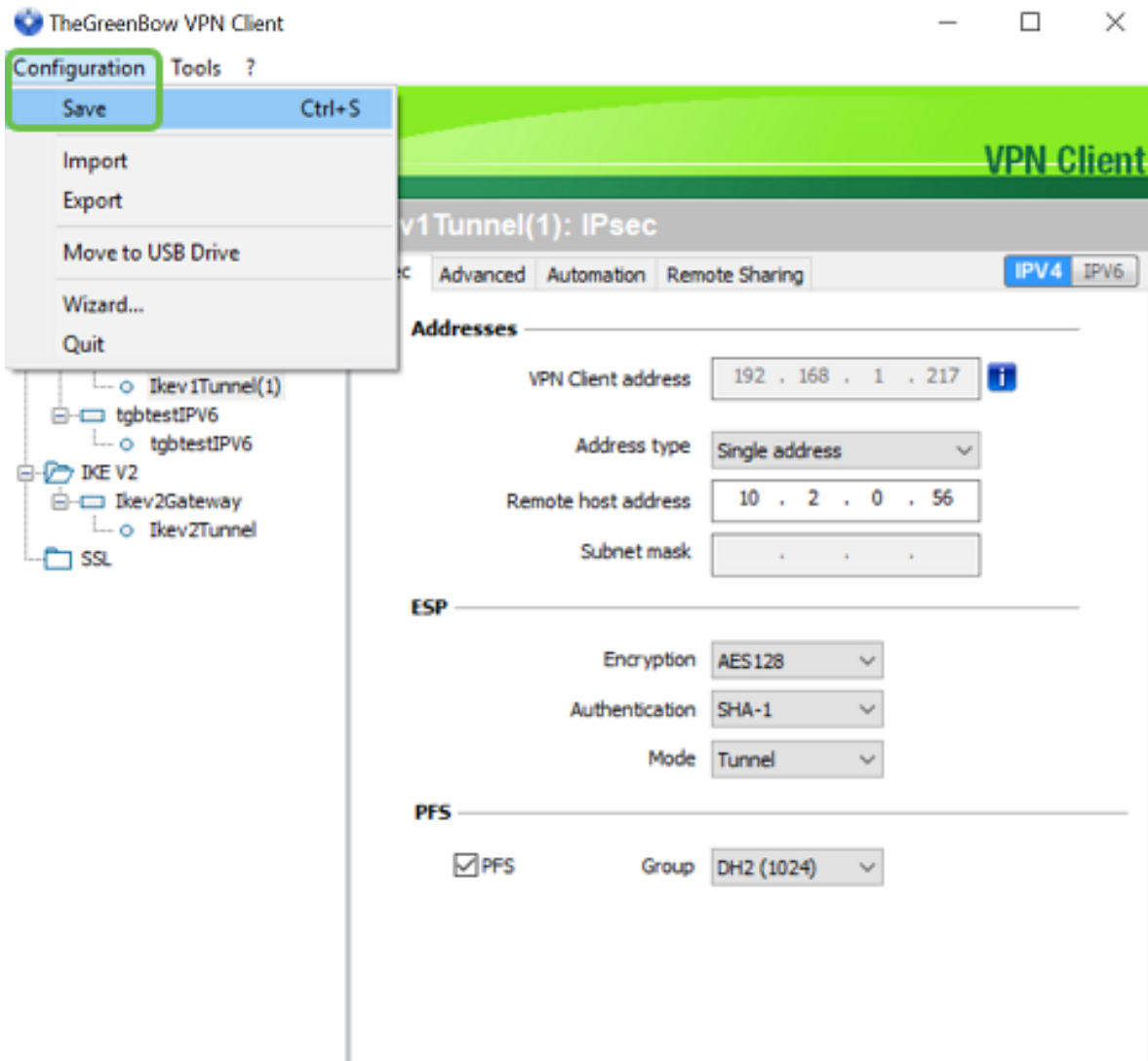
Configuration Tools ?

THEGREENBOW

VPN Configuration

-  IKE V1
 -  IKE V1 Parameters
 -  Ikev1Gateway
 -  Ikev1Tunnel
 -  **Connection_to_Office**
 -  Ikev1Gateway(2)

Step 6. Click **Configuration** and choose **Save**.



You should now have successfully configured TheGreenBow VPN Client to connect to the RV160 or RV260 router through VPN.

Start a VPN Connection as a Client

Step 1. Since you have TheGreenBow open, you can right-click on the tunnel and select **Open Tunnel to begin a connection**.

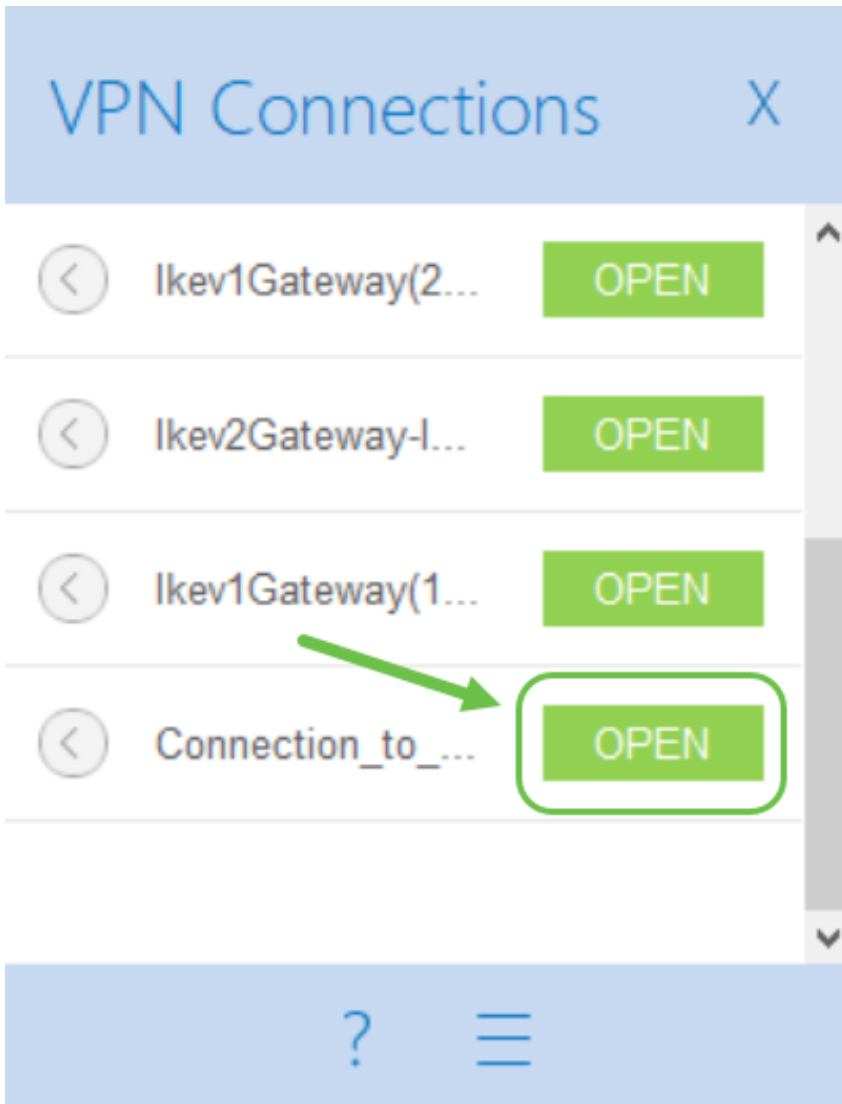
Open tunnel	Ctrl+O
Export	
Copy	Ctrl+C
Rename	F2
Delete	Del

Note: You can also open a tunnel by double-clicking on the tunnel.

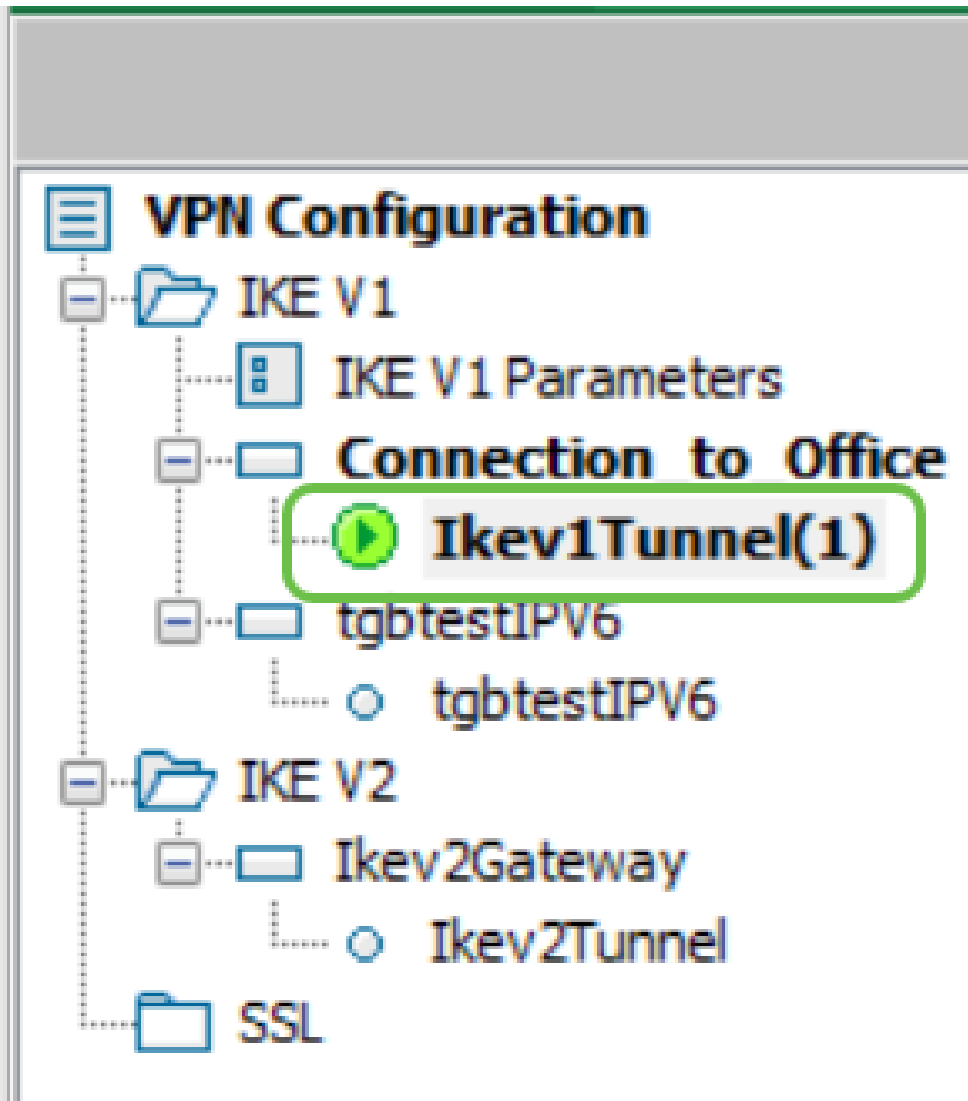
Step 2. (Optional) If you are beginning a new session and had closed TheGreenBow, click **TheGreenBow VPN Client** icon on the right side of the screen.



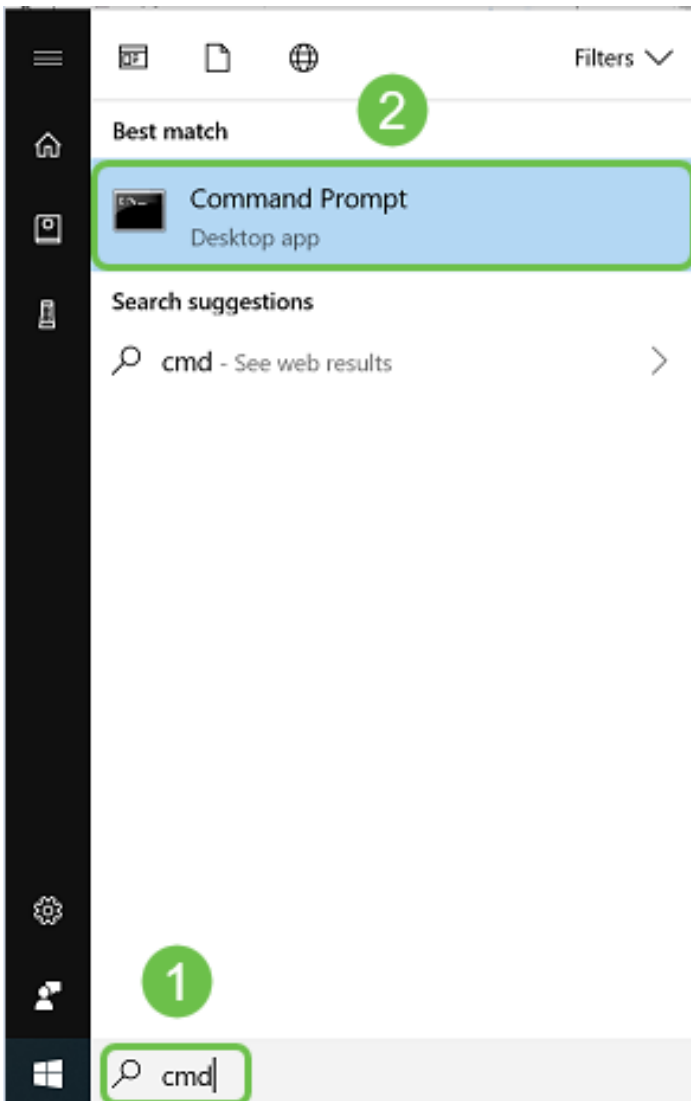
Step 3. (Optional) This step is only necessary if you are setting up a new session and followed Step 2. Choose the VPN connection that you need to use and then click **OPEN**. The VPN connection should start automatically.



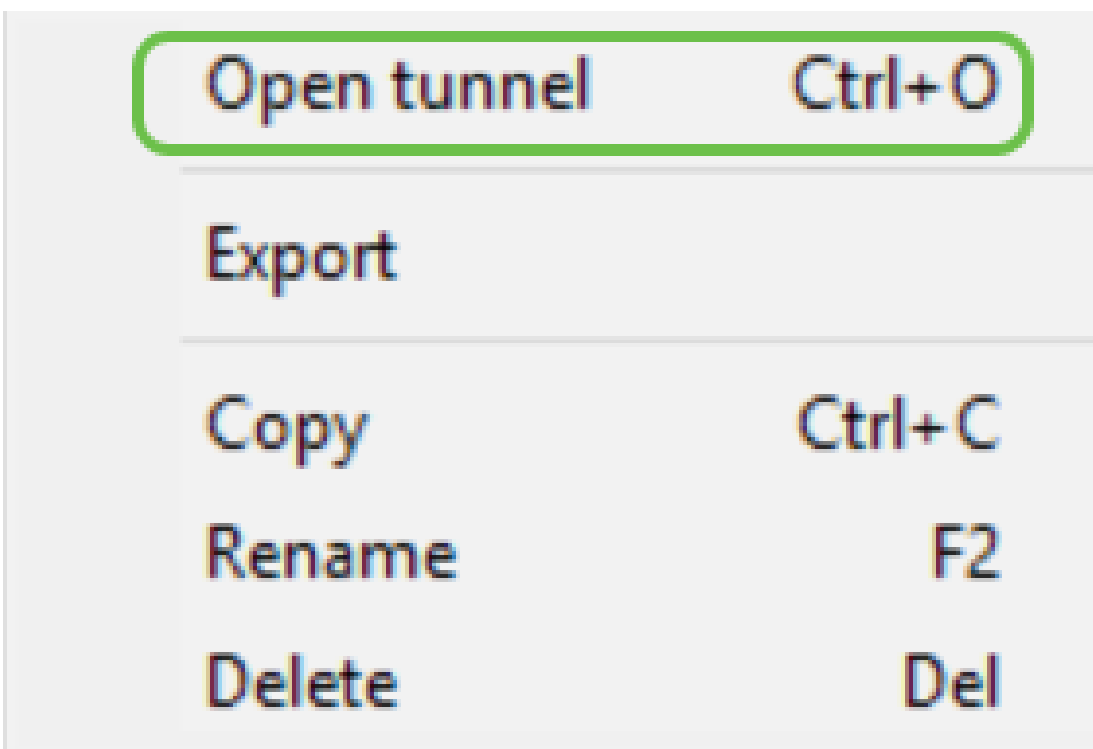
Step 4. When the tunnel is connected a green circle will appear next to the tunnel. If you see an exclamation mark you can click on it to find the error.



Step 5. (Optional) To verify that you are connected, access the command prompt from the client computer.



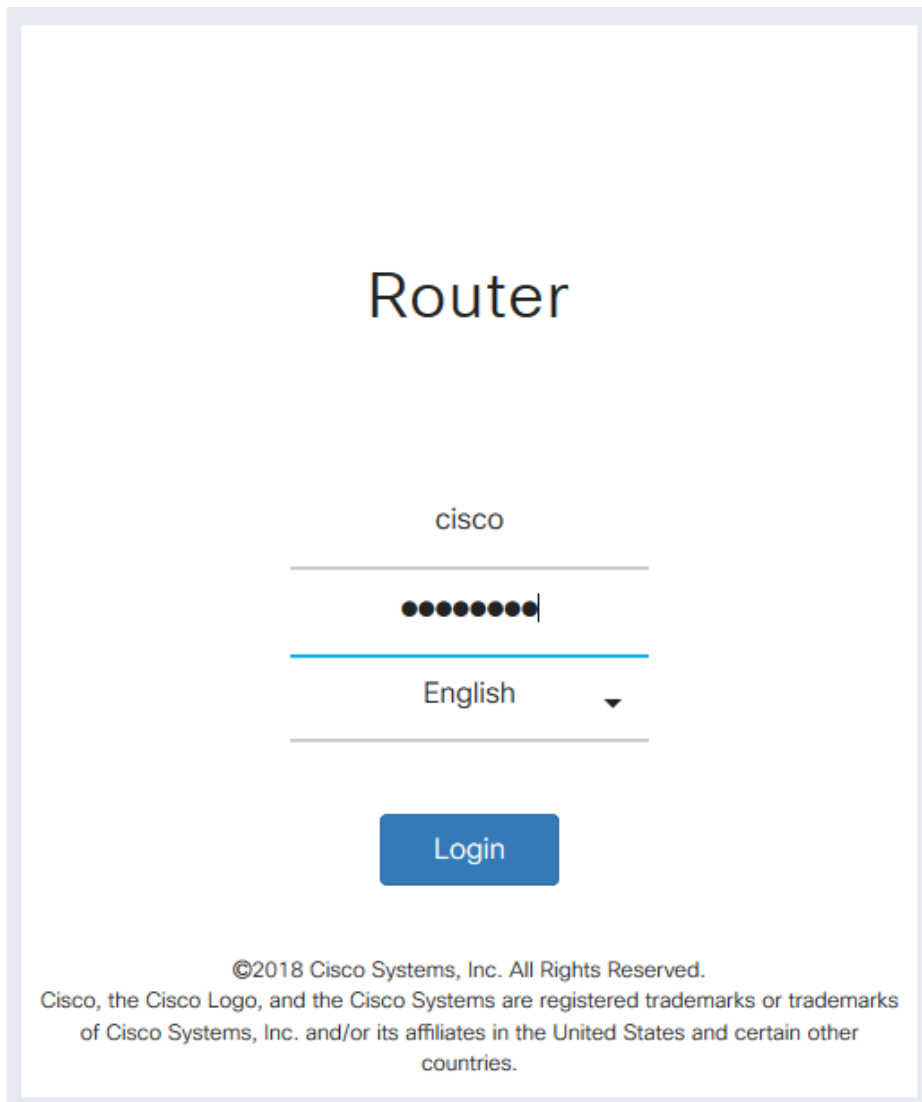
Step 6. (Optional) Enter ping and then the private LAN IP address of the router at the site. If you receive replies you are connected.



Verify VPN Status

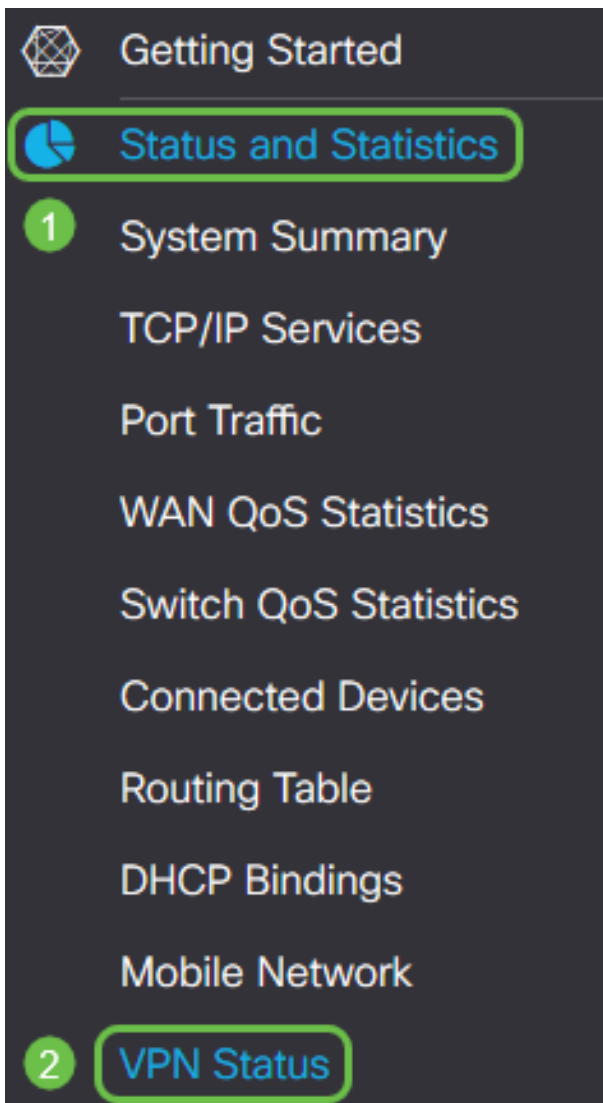
Verify the VPN Status at the Site

Step 1. Login to the web-based utility of the VPN gateway of the RV160 or RV260.



The screenshot shows the login interface for a Cisco Router. At the top, the word "Router" is displayed in a large, black, sans-serif font. Below this, the username "cisco" is entered into a text field. The password field is masked with ten black dots and a vertical cursor on the right. Below the password field, the language is set to "English" with a downward-pointing arrow indicating a dropdown menu. A blue "Login" button is positioned below the language selection. 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."

Step 2. Choose **Status and Statistics > VPN Status**.



Step 3. Under *Client-to-Site Tunnel Status*, check the *Connections* column of the *Connection Table*. You should see the VPN connection confirmed.

Client to Site VPN Status

Connection Table

+ [edit] [delete]

<input type="checkbox"/>	Group/Tunnel Name	Connections	Phase2 Enc/Auth/Grp	Local Group	Action
<input type="checkbox"/>	Client	1	aes128-sha1-modp1024	0.0.0.0/0	

Step 4. Click on the **eye** icon to see more details.

Client to Site VPN Status




Connection Table

+ [edit] [delete]

<input type="checkbox"/>	Group/Tunnel Name	Connections	Phase2 Enc/Auth/Grp	Local Group	Action
<input type="checkbox"/>	Client	1	aes128-sha1-modp1024	0.0.0.0/0	

Step 5. The details of the Client-to-Site VPN Status are shown here. You will notice the WAN IP address of the client, the local IP address that was assigned from the pool of addresses that was configured at setup. It also shows bytes and packets sent and received as well as the connection

time. If you would like to disconnect the client, click the blue **broken chain** icon under *Action*. Click the **x** in the upper right corner to close after inspection.

Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action 
108.233. 	10.2.1.1	0	14273	0	181	5 mins.	

Conclusion

You should now have successfully set up and verified the VPN connection on the RV160 or RV260 router, and have TheGreenBow VPN Client configured to connect to the router through VPN as well.