

# Configuring VPN Setup Wizard on the RV160 and RV260

## Objective

This document shows you how to configure VPN Setup Wizard on the RV160 and RV260.

## Introduction

Technology has evolved and business is often conducted outside of the office. Devices are more mobile and employees often work from home or as they travel. This can cause some security vulnerabilities. A Virtual Private Network (VPN) is a great way to connect remote workers to a secured network. A VPN allows a remote host to act as if they were connected to the onsite secured network.

A VPN establishes an encrypted connection over a less secure network like the Internet. It ensures the appropriate level of security to the connected systems. A tunnel is established as a private network that can send data securely by using industry-standard encryption and authentication techniques to secure the data sent. A remote-access VPN usually relies on either Internet Protocol Security (IPsec) or Secure Socket Layer (SSL) to secure the connection.

VPNs provide Layer 2 access to the target network; these require a tunneling protocol such as Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) running across the base IPsec connection. The IPsec VPN supports site-to-site VPN for a gateway-to-gateway tunnel. For example, a user can configure VPN tunnel at a branch-site to connect to the router at corporate site, so that the branch site can securely access corporate network. IPsec VPN also supports client-to-server VPN for host-to-gateway tunnel. The client to server VPN is useful when connecting from Laptop/PC from home to a corporate network through VPN server.

The RV160 series router supports 10 tunnels and the RV260 series router supports 20 tunnels. The VPN Setup Wizard guides the user when configuring a secure connection for a site-to-site IPsec tunnel. This simplifies the configuration by avoiding complex and optional parameters, so any user can set up the IPsec tunnel in a fast and efficient manner.

## Applicable Devices

- RV160
- RV260

## Software Version

- 1.0.0.13

## VPN Setup Wizard Configuration on Local Router

Step 1. Log into the web configuration page on your local router.

**Note:** We will refer the local router as Router A and the remote router as Router B. In this document, we will be using two RV160 to demonstrate the VPN Setup Wizard.



## Router

cisco

---

●●●●●●●●

---

English ▼

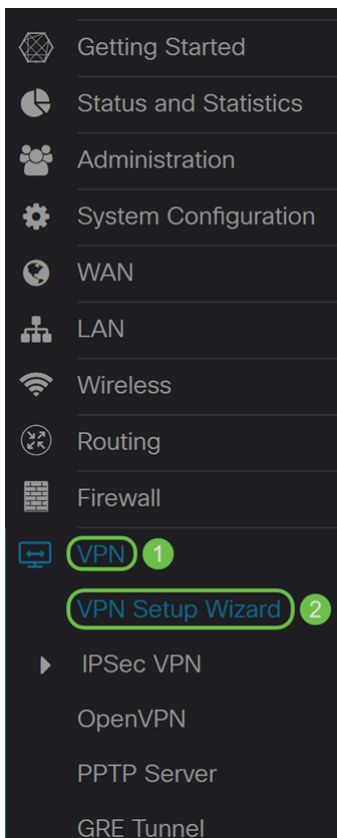
---

Login

©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. Navigate to **VPN > VPN Setup Wizard**.



Step 3. In the *Getting Started* section, enter a connection name in the **Enter a connection name** field. We entered in **HomeOffice** as our connection name.

## VPN Setup Wizard (Site-to-Site)

---

### 1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPSec VPN tunnel.

### 2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

### 3. Local and Remote Networks

Enter a connection name: 

### 4. Profile

Interface: WAN

### 5. Summary

Next

Cancel

Step 4. In the *Interface* field, select an interface from the drop-down list if you are using an RV260. The RV160 only has a WAN link so you will not be able to select an interface from the drop-down list. Click **Next** to proceed to the *Remote Router Settings* section.

## VPN Setup Wizard (Site-to-Site)

---

### 1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPSec VPN tunnel.

### 2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

### 3. Local and Remote Networks

Enter a connection name: 

### 4. Profile

Interface: WAN

### 5. Summary

Next

Cancel

Step 5. Select a *Remote Connection Type* from the drop-down list. Select either **Static IP** or **FQDN** (Fully Qualified Domain Name) and then enter either the WAN IP address or the

FQDN of the gateway that you wish to connect in the *Remote Address* field. In this example, **Static IP** was selected and the remote router WAN IP address (Router B) was entered. Then click **Next** to move to the next section.

## VPN Setup Wizard (Site-to-Site)

---

✓ 1. Getting Started

Remote Connection Type :  1

2. Remote Router Settings

Remote Address :  2

3. Local and Remote Networks

4. Profile

5. Summary

---

3

Back **Next** Cancel

Step 6. In the *Local and Remote Network* section, under the *Local Traffic Selection*, select the Local IP (**Subnet**, **Single**, or **Any**) from the drop-down list. If you select **Subnet**, enter the subnet IP address and subnet mask. If you select **Single**, enter an IP address. If **Any** was selected, go to the next step to configure the *Remote Traffic Selection*.

## VPN Setup Wizard (Site-to-Site)

---

✓ 1. Getting Started

✓ 2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Local Traffic Selection:

Any

Remote Traffic Selection:

Subnet

IP Address:

Subnet Mask:

Back

Next

Cancel

Step 7. In the *Remote Traffic Selection*, select the *Remote IP* (**Subnet**, **Single**, or **Any**) from the drop-down list. If you select **Subnet**, enter the subnet IP address and subnet mask of the remote router (Router B). If you select **Single**, enter the IP address. Then click **Next** to configure the *Profile* section.

**Note:** If you have selected **Any** for *Local Traffic Selection*, then you must select either **Subnet** or **Single** for the *Remote Traffic Selection*.

## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Local Traffic Selection:

Any

Remote Traffic Selection:

Subnet

IP Address:

10.1.1.0

Subnet Mask:

255.255.255.0

4

Back

Next

Cancel

Step 8. In the *Profile* section, select a name for IPsec profile from the drop-down list. For this demonstration, **new-profile** was selected as the IPsec profile.

# VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version: new-profile

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back Next Cancel

Step 9. Choose **IKEv1** (Internet Key Exchange Version 1) or **IKEv2** (Internet Key Exchange Version 2) as your *IKE Version*. IKE is a hybrid protocol that implements the Oakley key exchange and the Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations. IKEv2 is more efficient because it takes less packets to do the key exchange and supports more authentication options, while IKEv1 only does shared key and certificate based authentication. In this example, **IKEv1** was selected as our IKE version.

**Note:** If your device supports IKEv2 then it is recommended to use IKEv2. If your devices doesn't support IKEv2 then use IKEv1. Both routers (local and remote) need to use the same IKE version and security settings.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back Next Cancel

Step 10. In the *Phase 1 Options* section, select a DH (Diffie-Hellman) group (**Group 2 – 1024 bit** or **Group 5 - 1536 bit**) from the drop-down list. DH is a key exchange protocol, with two groups of different prime key lengths: Group 2 has up to 1,024 bits, and Group 5 has up to 1,536 bits. We will be using **Group 2 – 1024 bit** for this demonstration.

**Note:** For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected by default.



## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back

Next

Cancel

Step 11. Select an encryption option (**3DES, AES-128, AES-192, or AES-256**) from the drop-down list. This method determines the algorithm used to encrypt or decrypt Encapsulating Security Payload (ESP)/Internet Security Association and Key Management Protocol (ISAKMP) packets. Triple Data Encryption Standard (3DES) uses DES encryption three times but is now a legacy algorithm. This means that it should only be used when there's no better alternatives since it still provides a marginal but acceptable security level. Users should only use it if it's required for backwards compatibility as it's vulnerable to some "block collision" attacks. 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. It is recommended to use AES instead of 3DES. In this example, we will use **AES-192** as our encryption option.

**Note:** Here are some additional resources that may help: [Configuring Security for VPNs with IPSec](#) and [Next Generation Encryption](#).

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back Next Cancel

Step 12. The authentication method determines how the Encapsulating Security Payload Protocol (ESP) header packets are validated. The MD5 is a one-way hashing algorithm that produces a 128-bit digest. The SHA1 is a one-way hashing algorithm that produces a 160-bit digest while SHA2-256 produces a 256-bit digest. SHA2-256 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method. Select an authentication (**MD5**, **SHA1**, or **SHA2-256**). **SHA2-256** was selected for this example.

# VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile:

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime (sec.):  ?

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Step 13. 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 the default value of **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.

# VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.):

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Step 14. Enter in the **Pre-shared Key** to use to authenticate the remote IKE peer. You can enter up to 30 keyboard characters or hexadecimal values, such as My\_@123 or 4d795f40313233. Both ends of the VPN tunnel must use the same Pre-shared Key.

**Note:** We recommend that you change the Pre-shared Key periodically to maximize VPN security.

# VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): 28800

Pre-shared Key: ●●●●●●

Show Pre-shared Key:  Enable

Phase II Options

Back Next Cancel

Step 15. In the *Phase II Options* section, select a protocol from the drop-down list.

- **ESP** – Select ESP for data encryption and enter the encryption.
- **AH** – Select this for data integrity in situations where data is not secret but must be authenticated.

# VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key:  Enable

Phase II Options

Protocol Selection: ESP

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy:  Enable

Save as a new profile

Back Next Cancel

Step 16. Select an encryption option (**3DES, AES-128, AES-192, or AES-256**) from the drop-down list. This method determines the algorithm used to encrypt or decrypt Encapsulating Security Payload (ESP)/Internet Security Association and Key Management Protocol (ISAKMP) packets. Triple Data Encryption Standard (3DES) uses DES encryption three times but is now a legacy algorithm. This means that it should only be used when there's no better alternatives since it still provides a marginal but acceptable security level. Users should only use it if it's required for backwards compatibility as it's vulnerable to some "block collision" attacks. 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. It is recommended to use AES instead of 3DES. In this example, we will use **AES-192** as our encryption option.

**Note:** Here are some additional resources that may help: [Configuring Security for VPNs with IPsec](#) and [Next Generation Encryption](#).

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key:  Enable

Phase II Options

Protocol Selection: ESP

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy:  Enable

Save as a new profile

Back Next Cancel

Step 17. The authentication method determines how the Encapsulating Security Payload Protocol (ESP) header packets are validated. The MD5 is a one-way hashing algorithm that produces a 128-bit digest. The SHA1 is a one-way hashing algorithm that produces a 160-bit digest while SHA2-256 produces a 256-bit digest. SHA2-256 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method. Select an authentication (**MD5**, **SHA1**, or **SHA2-256**). **SHA2-256** was selected for this example.

# VPN Setup Wizard (Site-to-Site)


✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

**4. Profile**

5. Summary

SA Lifetime (sec.): 

3600

Pre-shared Key:

●●●●●●

Show Pre-shared Key:

Enable

## Phase II Options

Protocol Selection:


ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.): 

3600

Perfect Forward Secrecy:  Enable

Save as a new profile

Back

Next

Cancel

Step 18. Enter in the *SA Lifetime (Sec)* which is the amount of time, in seconds, that a VPN tunnel (IPsec SA) is active in this phase. The default value for Phase 2 is 3600 seconds.



# VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●

Show Pre-shared Key:  Enable

Phase II Options

Protocol Selection: ESP

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): ? 3600

Perfect Forward Secrecy:  Enable

Save as a new profile

Back Next Cancel

Step 19. When Perfect Forward Secrecy (PFS) is enabled, IKE Phase 2 negotiation generates new key material 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. If checked, select a *DH Group*. In this example **Group2 – 1024 bit** is used.

# VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

Show Pre-shared Key:


 Enable

## Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime (sec.): 

Perfect Forward Secrecy:

 Enable 1

DH Group:

2 

Save as a new profile

Back

Next

Cancel

Step 20. In the *Save as a new profile*, enter a name for the new profile you have just created. Click **Next** to see the summary of your VPN configuration.

# VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

Show Pre-shared Key:

Enable

## Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime (sec.): ?

Perfect Forward Secrecy:  Enable

DH Group:

Save as a new profile 1

Back

2 Next

Cancel

Step 21. Verify the information and then click **Submit**.

## VPN Setup Wizard (Site-to-Site)

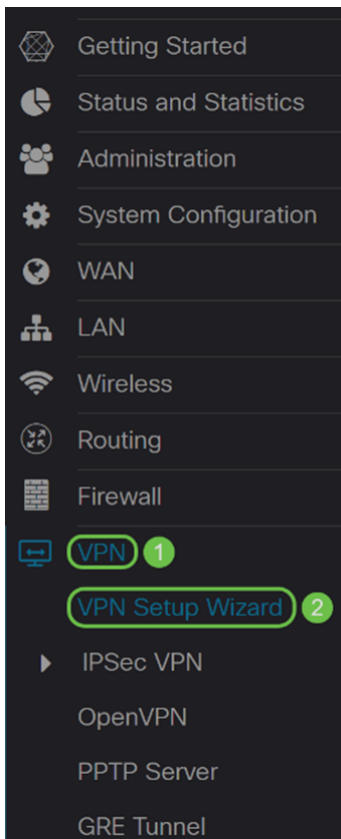
✓ 1. Getting Started	(sec.):	-----	
✓ 2. Remote Router Settings	Pre-shared Key:	Test123	
✓ 3. Local and Remote Networks	Phase II Options		Remote Group
✓ 4. Profile	Protocol Selection:	ESP	Remote IP Type: Subnet
5. Summary	Encryption:	AES-192	IP Address: 10.1.1.0
	Authentication:	SHA2-256	Subnet: 255.255.255.0
	SA Lifetime (sec.):	3600	
	Perfect Forward Secrecy:	Enable	
	DH Group:	Group2 - 1024 bit	

Back Submit Cancel

### VPN Setup Wizard Configuration on Remote Router

On the remote router, you would need to configure the same security settings as your local router but use the local router IP address as the remote traffic.

Step 1. Log into the web configuration page on your remote router (Router B) and navigate to **VPN > VPN Setup Wizard**.



Step 2. Enter a connection name and choose the interface that will be used for the VPN if you are using an RV260. The RV160 only has a WAN link so you will not be able to select an interface from the drop-down. Then click **Next** to continue.

## VPN Setup Wizard (Site-to-Site)

### 1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPsec VPN tunnel.

### 2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

### 3. Local and Remote Networks

Enter a connection name:

### 4. Profile

Interface: WAN

### 5. Summary

Step 3. In the *Remote Router Settings*, select the *Remote Connection Type* and then enter the WAN IP address of Router A. Then click **Next** to continue to the next section.

# VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Remote Connection Type : Static IP 1

Remote Address : ? 140. 2

3

Back Next Cancel

Step 4. Select the local and remote traffic. If you have selected **Subnet** in the *Remote Traffic Selection* field, enter in the private IP address subnet of Router A. Then click **Next** to configure the *Profile* section.

# VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

Local Traffic Selection:

Any

1

✓ 2. Remote Router Settings

Remote Traffic Selection:

Subnet

2

3. Local and Remote Networks

IP Address:

192.168.2.0

3

Subnet Mask:

255.255.255.0

4

4. Profile

5. Summary

5

Back

Next

Cancel

Step 5. In the *Profile* section, select the same security settings as Router A. We have also entered the same pre-shared key as Router A. Then click **Next** to go to the *Summary* page.

Phase I Options:

# VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile:

1 new-profile

IKE Version:

2  IKEv1  IKEv2

## Phase I Options

DH Group:

3 Group2 - 1024 bit

Encryption:

4 AES-192

Authentication:

5 SHA2-256

SA Lifetime (sec.):

? 6 28800

Pre-shared Key:

7 ●●●●●●

Show Pre-shared Key:

Enable

## Phase II Options

Back

Next

Cancel

Phase II Options:



# VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

**4. Profile**

5. Summary

Pre-shared key:

Show Pre-shared Key:  Enable

## Phase II Options

Protocol Selection:

1 ESP

Encryption:

2 AES-192

Authentication:

3 SHA2-256

SA Lifetime (sec.):

4 3600

Perfect Forward Secrecy:

5  Enable

DH Group:

6 Group2 - 1024 bit

Save as a new profile

7 RemoteOffice

8

Back

**Next**

Cancel

Step 6. In the *Summary* page, verify that the information that you have just configured is correct. Then click **Submit** to create your Site-to-Site VPN.

# VPN Setup Wizard (Site-to-Site)

<input checked="" type="checkbox"/> 1. Getting Started	(sec.):	-----	
<input checked="" type="checkbox"/> 2. Remote Router Settings	Pre-shared Key:	Test123	
<input checked="" type="checkbox"/> 3. Local and Remote Networks	Phase II Options		Remote Group
<input checked="" type="checkbox"/> 4. Profile	Protocol Selection:	ESP	Remote IP Type: Subnet
<input checked="" type="checkbox"/> 5. Summary	Encryption:	AES-192	IP Address: 192.168.2.0
	Authentication:	SHA2-256	Subnet: 255.255.255.0
	SA Lifetime (sec.):	3600	
	Perfect Forward Secrecy:	Enable	
	DH Group:	Group2 - 1024 bit	

**Note:** 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. To do this, click the **Save** button that appears at the top of your page or navigate to **Administration > Configuration Management**. Then, make sure your *Source* is **Running Configuration** and *Destination* is **Startup Configuration**. Click **Apply**.

## Conclusion

You should have successfully configured a Site-to-Site VPN using the VPN Setup Wizard. Follow the steps below to verify that your Site-to-Site VPN is connected.

Step 1. To verify that your connection has been established, you should see a *Connected* status when you navigate to **VPN > IPSec VPN > Site-to-Site**.

Site-to-Site								Apply	Cancel
Number of Connections: 1 connected, 1 configured, maximum 10 supported.									
+	+	+							
<input type="checkbox"/>	Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions	
<input type="checkbox"/>	RemoteOffice	140.1.1.1	WAN	VPNTest	0.0.0.0/0	192.168.2.0/24	Connected		

Step 2. Navigate to **Status and Statistics > VPN Status** and make sure that the Site-to-Site tunnel is *Enabled* and *UP*.

# VPN Status

## Site-to-Site Tunnel Status

1 Tunnel(s) Used    9 Tunnel(s) Available  
1 Tunnel(s) Enabled    1 Tunnel(s) Defined

### Connection Table



Column Display Selection

<input type="checkbox"/>	No.	Name	Enable	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Action
<input type="checkbox"/>	1	RemoteOffice	Enable	UP	aes192-sha256	0.0.0.0/0	192.168.2.0/24	140. [redacted]	