

Configuration of Gateway to Gateway VPN on RV016, RV042, RV042G and RV082 VPN Routers

Objective

A Virtual Private Network (VPN) is used to form a secure connection between two endpoints over a public or shared Internet, through what is called a VPN tunnel. More specifically, a gateway-to-gateway VPN connection allows for two routers to securely connect to each other and for a client on one end to logically appear as if they are a part of the network on the other end. This enables data and resources to be shared more easily and securely over the Internet.

Configuration must be done on both routers to enable a gateway-to-gateway VPN. The configurations done in the *Local Group Setup* and *Remote Group Setup* sections should be reversed between the two routers so that the local group of one is the remote group of the other.

The objective of this document is to explain how to configure Gateway-to-Gateway VPN on RV016, RV042, RV042G and RV082 VPN Series Routers.

Applicable Devices

- RV016
- RV042
- RV042G
- RV082

Software Version

- v4.2.2.08

Configure Gateway to Gateway VPN

Step 1. Log in to the Router Configuration Utility and choose **VPN > Gateway to Gateway**. The *Gateway to Gateway* page opens:

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Remote Group Setup

Remote Security Gateway Type :

:

Remote Security Group Type :

IP Address :

Subnet Mask :

To configure gateway to gateway VPN the following features need to be configured:

1. [Add a New Tunnel](#)
2. [Local Group Setup](#)
3. [Remote Group Setup](#)
4. [IPSec Setup](#)

Add a New Tunnel

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Tunnel No. is a read only field that displays the current tunnel that is going to be created.

Step 1. Enter a name for the VPN tunnel in the Tunnel Name field. It does not have to match the name used at the other end of the tunnel.

Step 2. From the Interface drop-down list choose the Wide Area Network (WAN) port to use for the tunnel.

- WAN1 — The dedicated WAN port of the RV0XX series VPN routers.
- WAN2 — The WAN2/DMZ port of the RV0XX Series VPN routers. Only displays in the drop-down menu if it has been configured as a WAN and not a Demilitarize Zone (DMZ) port.

Step 3. (Optional) To enable the VPN, check the check box in the **Enable** field. The VPN is enabled by default.

Local Group Setup

Note: The configuration for the local group setup on one router should be the same as the configuration for the remote group setup on the other router.

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Step 1. Choose the appropriate router identification method to establish a VPN tunnel from the Local Security Gateway Type drop-down list.

- IP Only — The local router (this router) is recognized by a static IP address. You can only choose this option if the router has a static WAN IP. The static WAN IP address appears automatically in the IP Address field.
- IP + Domain Name (FQDN) Authentication — Access to the tunnel is possible through a static IP address and a registered domain. If you choose this option, enter the name of the registered domain in the Domain Name field. The static WAN IP address appears automatically in the IP Address field.
- IP + E-mail Addr.(USER FQDN) Authentication — Access to the tunnel is possible through a static IP address and an email address. If you choose this option, enter the email address in the Email Address field. The static WAN IP address appears automatically in the IP Address field.
- Dynamic IP + Domain Name (FQDN) Authentication — Access to the tunnel is possible through a dynamic IP address and a registered domain. If you choose this option, enter the name of the registered domain in the Domain Name field.
- Dynamic IP + Email Addr.(USER FQDN) Authentication — Access to the tunnel is possible through a dynamic IP address and an email address. If you choose this option, enter the email address in the Email Address field.

Step 2. Choose the appropriate local LAN user or group of users who can access the VPN tunnel from the Local Security Group drop-down list. The default is Subnet.

- IP — Only one LAN device can access the VPN tunnel. If you choose this option, enter the IP address of the LAN device in the IP Address field.
- Subnet — All LAN devices on a specific subnet can access the tunnel. If you choose this option, enter the subnetwork IP address and subnet mask of the LAN devices in the IP Address and Subnet Mask field respectively. The default mask is 255.255.255.0.
- IP Range — A range of LAN devices can access the tunnel. If you choose this option, enter the starting and ending IP address in the Begin IP and End IP fields respectively.

Step 3. Click **Save** to save the settings.

Remote Group Setup

Note: The configuration for the remote group setup on one router should be the same as the configuration for the local group setup on the other router.

Local Group Setup

Local Security Gateway Type :

Email Address : @

IP Address :

Local Security Group Type :

IP Address :

Remote Group Setup

Remote Security Gateway Type :

:

Remote Security Group Type :

IP Address :

Subnet Mask :

Step 1. From the Remote Security Gateway Type drop-down list, choose the method to identify the remote router to establish the VPN tunnel.

- **IP Only** — Access to the tunnel is possible through a static WAN IP. If you know the IP address of the remote router, choose IP address from the drop-down list directly below the Remote Security Gateway Type field and enter the IP address. Choose IP by DNS Resolved if you do not know the IP address but know the domain name and enter the domain name of the router in the IP by DNS Resolved field.
- **IP + Domain Name (FQDN) Authentication** — Access to the tunnel is possible through a static IP address and a registered domain for the router. If you know the IP address of the remote router, choose IP address on the drop-down list directly below the Remote Security Gateway Type field and enter the address. Choose IP by DNS Resolved if you do not know the IP address but know the domain name and enter the domain name of the router in the IP by DNS Resolved field. Enter the domain name of the router in the Domain Name field regardless of which method you choose to identify it by.
- **IP + Email Addr.(USER FQDN) Authentication** — Access to the tunnel is possible through a static IP address and an email address. If you know the IP address of the remote router, choose IP address on the drop-down list directly below Remote Security Gateway Type field and enter the address. Choose IP by DNS Resolved if you do not know the IP address but know the domain name and enter the domain name of the router in the IP by DNS Resolved field. Enter the e-mail Address in the Email Address field.
- **Dynamic IP + Domain Name (FQDN) Authentication** — Access to the tunnel is possible through a dynamic IP address and a registered domain. If you choose this option, enter the name of the registered domain in the Domain Name field.
- **Dynamic IP + Email Addr.(USER FQDN) Authentication** — Access to the tunnel is possible through a dynamic IP address and an email address. If you choose this option, enter the Email Address in the Email Address field.

Step 2. Choose the appropriate remote LAN user or group of users who can access the VPN tunnel from the Remote Security Group Type drop-down list.

- IP — Only one specific LAN device can access to the tunnel. If you choose this option, enter the IP address of the LAN device in the IP Address field.
- Subnet — All LAN devices on a specific subnet can access to the tunnel. If you choose this option, enter the subnetwork IP address and subnet mask of the LAN devices in the IP Address and Subnet Mask field respectively.
- IP Range — A range of LAN devices can access to the tunnel. If you choose this option, enter the starting and ending IP address in the Begin IP and End IP fields respectively.

Note: The two routers at the ends of the tunnel cannot be on the same subnet.

Step 3. Click **Save** to save the settings.

IPSec Setup

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Internet Protocol Security (IPSec) is an internet layer security protocol which provides end-to-end security through authentication and encryption during any communication session.

Note: Both ends of the VPN need to have the same methods of encryption, decryption, and authentication to work properly. Enter the same IPSec Setup settings for both routers.

IPSec Setup

Keying Mode : IKE with Preshared key
Manual
IKE with Preshared key

Phase 1 DH Group : Manual
IKE with Preshared key

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Step 1. Choose the appropriate mode of key management to ensure security from the Keying Mode drop-down list. The default mode is IKE with Preshared key.

- [Manual](#) — A custom security mode to generate a new security key by yourself and no negotiation with the key. It is the best to use during troubleshooting and in a small static environment.
- [IKE with Preshared key](#) — Internet Key Exchange (IKE) protocol is used to automatically generate and exchange a preshared key to establish authenticate communication for the tunnel.

IPSec Setup for Manual Keying Mode

IPSec Setup

Keying Mode : Manual

Incoming SPI : 101

Outgoing SPI : 101

Encryption : DES

Authentication : MD5


Encryption Key :

Authentication Key :

Step 1. Enter the unique hexadecimal value for incoming Security Parameter Index (SPI) in the Incoming SPI field. SPI is carried in the Encapsulating Security Payload Protocol (ESP) header and determines the protection for the incoming packet. You can enter a value from 100 to ffffffff. The incoming SPI of the local router needs to match with the outgoing SPI of the remote router.

Step 2. Enter the unique hexadecimal value for outgoing Security Parameter Index (SPI) in the Outgoing SPI field. You can enter a value from 100 to ffffffff. The outgoing SPI of the remote router need to match with the incoming SPI of the local router.

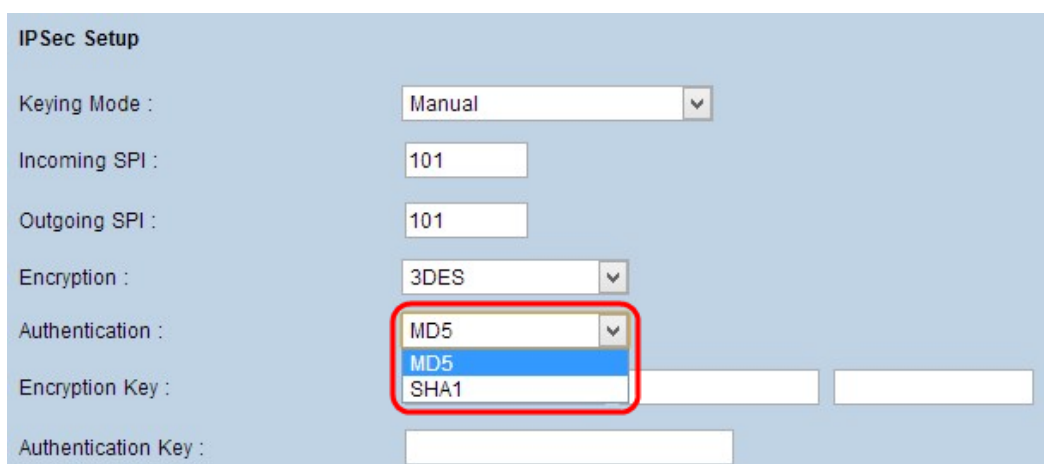
Note: No two tunnels can have the same SPI.



The screenshot shows the 'IPSec Setup' configuration page. The 'Keying Mode' is set to 'Manual'. Both 'Incoming SPI' and 'Outgoing SPI' fields contain the value '101'. The 'Encryption' dropdown menu is open, showing 'DES' as the selected option, with 'DES' and '3DES' as visible options. The 'Authentication' dropdown is not yet open. There are empty input fields for 'Encryption Key' and 'Authentication Key'.

Step 3. Choose the appropriate encryption method for the data from the Encryption drop-down list. The recommended encryption is 3DES. The VPN tunnel needs to use the same encryption method on both ends.

- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should be only used if one endpoint only supports DES.
- 3DES — Triple Data Encryption Standard (3DES) is a 168 bit, simple encryption method. 3DES encrypts the data three times, which provides more security then DES.



The screenshot shows the 'IPSec Setup' configuration page. The 'Keying Mode' is set to 'Manual'. Both 'Incoming SPI' and 'Outgoing SPI' fields contain the value '101'. The 'Encryption' dropdown menu is set to '3DES'. The 'Authentication' dropdown menu is open, showing 'MD5' as the selected option, with 'MD5' and 'SHA1' as visible options. There are empty input fields for 'Encryption Key' and 'Authentication Key'.

Step 4. Choose the appropriate authentication method for the data from the Authentication drop-down list. The recommended authentication is SHA1 as it is more secure than MD5. The VPN tunnel needs to use the same authentication method for both ends.

- MD5 — Message Digest Algorithm-5 (MD5) is a 128 bit hash function which provides

protection to the data from malicious attack by the checksum calculation.

- SHA1 — Secure Hash Algorithm version 1 (SHA1) is a 160 bit hash function which is more secure than MD5 but it takes more time to compute.

The screenshot shows the 'IPSec Setup' configuration page. It includes the following fields and values:

- Keying Mode : Manual
- Incoming SPI : 101
- Outgoing SPI : 101
- Encryption : 3DES
- Authentication : SHA1
- Encryption Key : acb1230000000000 ab456fbc00000000 87600bca00000000
- Authentication Key : acbd123400000000000000000000000000000000

A red rectangular box highlights the Encryption Key and Authentication Key fields.

Step 5. Enter the key to encrypt and decrypt data in the Encryption Key field. If you choose DES as encryption method in Step 3, enter a 16 digit hexadecimal value. If you choose 3DES as encryption method in Step 3, enter a 40 digit hexadecimal value.

Step 6. Enter a pre-shared key to authenticate the traffic in Authentication Key field. If you choose MD5 as authentication method in step 4, enter 32 digit hexadecimal value. If you choose SHA1 as authentication method in Step 4, enter 40 digit hexadecimal value. If you do not add enough digits, zeroes will be appended to the end until there are enough digits. The VPN tunnel needs to use the same pre-shared key for both of the ends.

Step 7. Click **Save** to save the settings.

IKE with Preshared Key Mode Configuration

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : **Group 1 - 768 bit**

Phase 1 Encryption : MD5

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Step 1. Choose the appropriate Phase 1 DH Group from the Phase 1 DH Group drop-down list. Phase 1 is used to establish the simplex, logical security association (SA) between the two ends of the tunnel to support secure authenticate communication. Diffie-Hellman (DH) is a cryptographic key exchange protocol which is used to determine the strength of the key during Phase 1 and it also shares the secret key to authenticate the communication.

- Group 1 - 768 bit —The lowest strength key and the most insecure authentication group but takes the least amount of time to compute the IKE keys. This option is preferred if the speed of the network is low.
- Group 2 - 1024 bit — A higher strength key and more secure authentication group than group 1 but it takes more time to compute the IKE keys.
- Group 5 - 1536 bit — The highest strength key and the most secure authentication group. It needs more time to compute the IKE keys. It is preferred if the speed of the network is high.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : DES

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Step 2. Choose the appropriate Phase 1 Encryption to encrypt the key from the Phase 1 Encryption drop-down list. AES-128, AES-192, or AES-256 are recommended. The VPN tunnel needs to use the same encryption method for both of its ends.

- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should be only used if one endpoint only supports DES.
- 3DES — Triple Data Encryption Standard (3DES) is a 168 bit, simple encryption method. 3DES encrypts the data three times, which provides more security than DES.
- AES-128 — Advanced Encryption Standard (AES) is 128 bit encryption method which transforms the plain text into cipher text through 10 cycles repetitions.
- AES-192 — Advanced Encryption Standard (AES) is 192 bit encryption method which transforms the plain text into cipher text through 12 cycles repetitions. AES-192 is more secure than AES-128.
- AES-256 — Advanced Encryption Standard (AES) is 256 bit encryption method which transforms the plain text into cipher text through 14 cycles repetitions. AES-256 is the most secure encryption method.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Step 3. Choose the appropriate Phase 1 authentication method from the Phase 1 Authentication drop-down list. The VPN tunnel needs to use the same authentication method for both of its ends. SHA1 is recommended.

- MD5 — Message Digest Algorithm-5 (MD5) is a 128 bit hash function which provide protection to the data from malicious attack by the checksum calculation.
- SHA1 — Secure Hash Algorithm version 1 (SHA1) is a 160 bit hash function which is more secure than MD5 but it takes more time to compute.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :


Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Step 4. Enter the amount of time in seconds that the Phase 1 keys are valid and the VPN tunnel remains active in the Phase 1 SA Life Time field.

Step 5. Check the **Perfect Forward Secrecy** check box to provide more protection to the keys. This option allows the router to generate a new key if any key is compromised. The encrypted data is only compromised through the compromised key. This is a recommended action as it provides more security.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

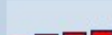
Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Step 6. Choose the appropriate Phase 2 DH Group from the Phase 2 DH Group drop-down list. Phase 2 uses security association and is used to determine the security of the data packet as it passes through the two end points.

- Group 1 - 768 bit —The lowest strength key and the most insecure authentication group, but takes the least amount of time to compute the IKE keys. This option is preferred if the speed of the network is low.
- Group 2 - 1024 bit — A higher strength key and more secure authentication group than group 1, but takes more time to compute the IKE keys.
- Group 5 - 1536 bit — The highest strength key and the most secure authentication group. It needs more time to compute the IKE keys. It is preferred if the speed of the network is high.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 bit

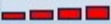
Phase 2 Encryption : **DES**

Phase 2 Authentication :

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

The image shows a screenshot of the 'IPSec Setup' configuration page. The 'Phase 2 Encryption' dropdown menu is open, showing options: DES (highlighted in blue), NULL, 3DES, AES-128, AES-192, and AES-256. A red rectangle highlights the dropdown menu.

Step 7. Choose the appropriate Phase 2 Encryption to encrypt the key from the Phase 2 Encryption drop-down list. AES-128, AES-192, or AES-256 are recommended. The VPN tunnel needs to use the same encryption method for both of its ends.

- NULL — No encryption is used.
- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should be only used if one endpoint only supports DES.
- 3DES — Triple Data Encryption Standard (3DES) is a 168 bit, simple encryption method. 3DES encrypts the data three times, which provides more security than DES.
- AES-128 — Advanced Encryption Standard (AES) is 128 bit encryption method which transforms the plain text into cipher text through 10 cycle repetitions.
- AES-192 — Advanced Encryption Standard (AES) is 192 bit encryption method which transforms the plain text into cipher text through 12 cycle repetitions. AES-192 is more secured than AES-128.
- AES-256 — Advanced Encryption Standard (AES) is 256 bit encryption method which transforms the plain text into cipher text through 14 cycle repetitions. AES-256 is the most secure encryption method.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 bit


Phase 2 Encryption : DES

Phase 2 Authentication : MD5
NULL
MD5
SHA1

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Step 8. Choose the appropriate authentication method from the Phase 2 Authentication drop-down list. The VPN tunnel needs to use the same authentication method for both ends. SHA1 is recommended.

- MD5 — Message Digest Algorithm-5 (MD5) is a 128 bit hexadecimal hash function which provides protection to the data from malicious attack by the checksum calculation.
- SHA1 — Secure Hash Algorithm version 1 (SHA1) is a 160 bit hash function which is more secure than MD5 but it takes more time to compute.
- Null — No authentication method is used.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :


Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Step 9. Enter the amount of time in seconds that the Phase 2 keys are valid and the VPN tunnel remains active in the Phase 2 SA Life Time field.

Step 10. Enter a key which is shared previously between the IKE peers to authenticate the peers in the Preshared Key field. Up to 30 hexadecimal and character can be used as the preshared key. The VPN tunnel needs to use the same preshared key for both of its ends.

Note: It is strongly recommended to frequently change the preshared key between the IKE peers so the VPN remains secured.

Step 11. (Optional) If you want to enable strength meter for the preshared key, check the **Minimum Preshared Key Complexity** check box. It is used for determine the strength of the pre-shared key through color bars.

- Preshared Key Strength Meter — This shows the strength of the preshared key through colored bars. Red indicates weak strength, yellow indicates acceptable strength, and green indicates strong strength.

Step 12. Click **Save** to save the settings.

Note: If you want to configure the options available in the *Advanced* section for Gateway to Gateway VPN refer to the article, [Configure Advanced Settings for Gateway to Gateway VPN on RV016, RV042, RV042G, and RV082 VPN Routers](#).