

Gateway to Gateway Virtual Private Network (VPN) Configuration on RV320 and RV325 VPN Router Series

Objective

VPNs are used to form very secure connections over two endpoints, over 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 in one end to logically appear to be part of the same remote network on the other end. This enables data and resources to be shared more easily and securely over the internet. The configuration must be done on both sides of the connection for a successful gateway-to-gateway VPN connection to be established. The purpose of this article is to guide you with the configuration of a gateway-to-gateway VPN connection on the RV32x VPN Router Series.

Applicable Devices

- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

Software Version

- v1.1.0.09

Gateway to Gateway

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

Gateway to Gateway

Add a New Tunnel

Tunnel No.

Tunnel Name:

Interface:

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type:

IP Address:

Local Security Group Type:

IP Address:

Subnet Mask:

Remote Group Setup

Remote Security Gateway Type:

IP Address:

Remote Security Group Type:

IP Address:

Subnet Mask:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

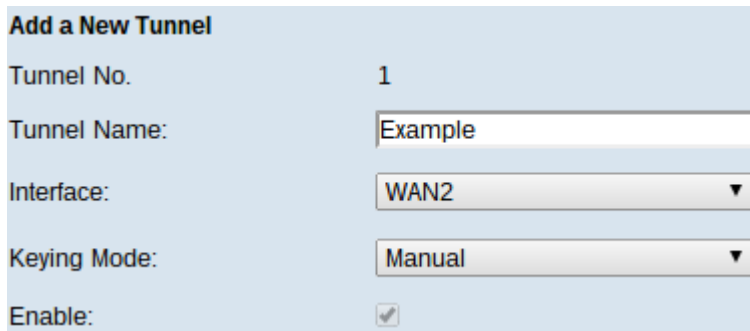
Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

In order for the VPN connection to work properly, the Internet Protocol Security (IPSec) values on both sides of the connection must be the same. Both sides of the connection must belong to different Local Area Networks (LANs), and at least one of the routers to be identifiable by a static IP address or a dynamic DNS hostname.

Add a New Tunnel



Add a New Tunnel	
Tunnel No.	1
Tunnel Name:	Example
Interface:	WAN2 ▼
Keying Mode:	Manual ▼
Enable:	<input checked="" type="checkbox"/>

- Tunnel No. — Displays the current tunnel that is going to be created. The router supports 100 tunnels.

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 router.
- WAN2 — The WAN2/DMZ port of the router. Only displays in the drop-down menu if it has been configured as a WAN and not a Demilitarize Zone (DMZ) port.
- USB1 — The USB1 port of the router. Only works if there is a 3G/4G/LTE USB dongle attached to the port.
- USB2 — The USB2 port of the router. Only works if there is a 3G/4G/LTE USB dongle attached to the port.

Step 3. From the Keying Mode drop-down list choose the tunnel security to use.

- Manual — This option lets you manually configure the key instead of negotiating the key with the other side of the VPN connection.
- IKE with Preshared key — Choose this option to enable the Internet Key Exchange Protocol (IKE) which sets up a security association in the VPN tunnel. IKE uses a preshared key to authenticate a remote peer.
- IKE with Certificate — Choose this option to enable the Internet Key Exchange (IKE) protocol with certificate which offers a more secure way to automatically generate and exchange preshared keys to establish more authenticated and secure communications for the tunnel.

Step 4. Check the Enable check box to enable the VPN tunnel. By default it is enabled.

Local Group Setup

These settings should match the "Remote Group Setup" settings for the router on the other end of the VPN tunnel.

Note: If Manual or IKE with Preshared key was selected from the Keying Mode drop-down list from Step 3 of Add a New Tunnel start from Step 1 and skip Steps 2 to 4. If IKE with Certificate was selected skip Step 1.

Local Group Setup

Local Security Gateway Type: IP + Email Address(USER FQDN) Authentication ▼

IP Address: 0.0.0.0

Email Address: example @ router.com

Local Security Group Type: IP Range ▼

Begin IP: 192.168.1.1

End IP: 192.168.1.254

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

- IP Only — Access to the tunnel is possible through a static WAN IP only. You can choose this option if only the router has any static WAN IP. The static WAN IP address is an auto generated 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 is an auto generated 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 is an auto generated 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.

Note: The following changes on the Local Group Setup area change when working with IKE with Certificate.

Local Group Setup

Local Security Gateway Type: IP + Certificate ▼

IP Address: 0.0.0.0

Local Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52 ▼

Self-Generator Import Certificate

Local Security Group Type: Subnet ▼

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.128

The Local Security Gateway Type drop-down list becomes uneditable and displays IP + Certificate. This is the LAN resource that can use the tunnel. The IP Address field displays the WAN IP address of the device. It is not user editable.

Step 2. Choose a certificate from the Local Certificate drop-down list. Certificates provide stronger authentication security on the VPN connections.

Step 3. (Optional) Click the **Self-Generator** button to display the *Certificate Generator* window to configure and generate certificates.

Step 4. (Optional) Click the **Import Certificate** button to display the *My Certificate* window to view and configure certificates.

Step 5. From the Local Security Group Type drop-down list choose one of the following:

- IP Address — This option lets you specify one device that can use this VPN tunnel. You only need to enter the IP address of the device in the IP address field.
- Subnet — Choose this option to allow all devices that belong to the same subnet to use the VPN tunnel. You need to enter the network IP address in the IP Address field and its respective subnet mask in the Subnet Mask field.
- IP Range — Choose this option to specify a range of devices that can use the VPN tunnel. You need to enter the first IP address and the last IP address of the range of devices in the Begin IP field and End IP field.

Remote Group Setup

These settings should match the "Local Group Setup" settings for the router on the other end of the VPN tunnel.

Note: If Manual or IKE with Preshared key was selected from the Keying Mode drop-down list from Step 3 of Add a New Tunnel start from Step 1 and skip Steps 2 to 5. Or if IKE with Certificate was selected skip Step 1.

Remote Group Setup

Remote Security Gateway Type: IP Only

IP by DNS Resolved : example.com

Remote Security Group Type: IP

IP Address: 192.0.2.4

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

- IP Only — Access to the tunnel is possible through a static WAN IP only. 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.
- IP + Domain Name (FQDN) Authentication — Access to the tunnel is possible through a static IP address and a registered domain of the router. 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. If you choose this option, enter the name of the registered

Domain in the Domain Name field.

- 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.

Note: If both routers have dynamic IP addresses DO NOT choose Dynamic IP + Email Address for both gateways.

Note: The Following changes on the Remote Group Setup area change when working with IKE with Certificate.

Remote Group Setup

Remote Security Gateway Type: IP + Certificate

IP by DNS Resolved : example.com

Remote Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Import Remote Certificate Authorize CSR

Remote Security Group Type: IP

IP Address: 192.0.2.4

The Remote Security Gateway Type drop-down list becomes uneditable and displays IP + Certificate. This is the LAN resource that can use the tunnel.

Step 2. 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 remote router in the IP by DNS Resolved field

Step 3. Choose a certificate from the Remote Certificate drop-down list. Certificates provide stronger authentication security on the VPN connections.

Step 4. (Optional) Click the **Import Remote Certificate** button to import a new certificate.

Step 5. (Optional) Click the **Authorize CSR** button to identify the certificate with a digital signing request.

Step 6. From the Local Security Group Type drop-down list choose one of the following:

- IP Address — This option lets you specify one device that can use this VPN tunnel. You only need to enter the IP address of the device in the IP address field.

- Subnet — Choose this option to allow all devices that belong to the same subnet to use the VPN tunnel. You need to enter the network IP address in the IP Address field and its respective subnet mask in the Subnet Mask field.
- IP Range — Choose this option to specify a range of devices that can use the VPN tunnel. You need to enter the first IP address and the last IP address of the range of devices. In the Begin IP field and End IP field.

IPSec Setup

For the encryption to be properly setup between the two ends of the VPN tunnel they must both have the exact same settings. IPSec in this case creates a secure authentication between the two devices. It does so in two phases.

IPSec Setup for Manual Keying Mode

Only available if Manual was selected from the Keying Mode drop-down list from Step 3 of Add a New Tunnel. This is a custom security mode to generate a new security key by yourself and to not negotiation with the key. It is the best to use during troubleshooting and small static environment.

IPSec Setup		
Incoming SPI:	<input type="text" value="100A"/>	(Range: 100-FFFFFFFF, Default: 100)
Outgoing SPI:	<input type="text" value="1BCD"/>	(Range: 100-FFFFFFFF, Default: 100)
Encryption:	<input type="text" value="DES"/>	
Authentication:	<input type="text" value="SHA1"/>	
Encryption Key:	<input type="text" value="ABC12675BC0ACD"/>	(HEX Number, DES: 16bits, 3DES: 48bits)
Authentication Key:	<input type="text" value="AC67BCD00A12876CB"/>	(HEX Number, MD5: 32bits, SHA1: 40bits)

Step 1. Enter the unique hexadecimal value for incoming Security Parameter Index (SPI) in the Incoming SPI field. SPI is carried in Encapsulating Security Payload (ESP) Protocol header which together determine the protection for the incoming packet. You can enter from 100 to FFFFFFFF.

Step 2. Enter the unique hexadecimal value for SPI in the Outgoing SPI field. SPI is carried in ESP header which together determine the protection for the outgoing packet. You can enter from 100 to FFFFFFFF.

Note: The incoming and outgoing SPI should match each other at both ends in order to establish a tunnel.

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

- DES — DES (Data Encryption Standard) is a 56-bit old, more backward compatible, encryption method which is not so secure as it is easy to break.
- 3DES — 3DES (Triple Data Encryption Standard) is a 168 bit, simple encryption method to increase the key size through encrypts the data for three times which provides more security then DES.

Step 4. Choose the appropriate authentication method from the Authentication drop-down list. The recommended authentication is SHA1. The VPN tunnel needs to use the same authentication method for both of its ends.

- MD5 — MD5 (Message Digest Algorithm-5) represents 32 digit hexadecimal hash function which provide protection to the data from malicious attack by the checksum calculation.
- SHA1 — SHA1 (Secure Hash Algorithm version 1) is a 160-bit hash function which is more secure than MD5.

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 the Authentication Key field. If you choose MD5 as authentication method in Step 4, enter a 32 digit hexadecimal value. If you choose SHA as authentication method in Step 4, enter a 40 digit hexadecimal value. The VPN tunnel needs to use the same preshared key for both of its ends.

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

IPSec Setup for IKE with Preshared key

Only available if IKE with Preshared key was selected from the Keying Mode drop-down list from Step 3 of Add a New Tunnel.

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication: MD5

Phase 1 SA Lifetime: 25000 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 360 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key: ABC12345DEFG6789!@#

Preshared Key Strength Meter:

Advanced +

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 cryptography key exchange protocol which is used during Phase 1 connection to share a secret key to authenticate communication.

- Group 1 - 768 bit — Represents 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.
- Group 2 - 1024 bit — Represents higher strength key and more secure authentication group. It needs some time to compute the IKE keys.
- Group 5 - 1536 bit — Represents the lowest strength key and the most insecure authentication group. It needs less time to compute the IKE keys. It is preferred if the speed of the network is low.

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) is 56-bit, old encryption method which is not very secure encryption method in today's world.
- 3DES — Triple Data Encryption Standard (3DES) is a 168-bit, simple encryption method to increase the key size through encrypts the data for 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 — Is 192-bit encryption method which transforms the plain text into cipher text through 12 cycles repetitions.
- AES-256 — Is a 256-bit encryption method which transforms the plain text into cipher text through 14 cycles repetitions.

Step 3. Choose the appropriate 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) represents 32 digit hexadecimal hash function which provide protection to the data from malicious attack by the checksum calculation.
- SHA1 — A 160-bit hash function which is more secure than MD5.

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

Step 5. Check Perfect Forward Secrecy check box to provide more protection to the keys. This option allows to generate a new key if any key is compromised. The encrypted data is only compromised through the compromised key. So it provides more secure and authenticate communication as it secures other keys though a key is compromised. This is a recommended action as it provides more security.

Step 6. Choose the appropriate Phase 2 DH Group from the Phase 2 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. DH is a cryptographic key exchange protocol which is used during Phase 1 connection to share secret key to authenticate communication.

- Group 1 - 768 bit — Represents 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.
- Group 2 - 1024 bit — Represents higher strength key and more secure authentication group. It needs some time to compute the IKE keys.
- Group 5 - 1536 bit — Represents the lowest strength key and the most insecure authentication group. It needs less time to compute the IKE keys. It is preferred if the speed of the network is low.

Note: As any new key is not generated, you do not need to configure Phase 2 DH Group if you uncheck Perfect Forward Secrecy in Step 5.

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.

- DES — DES is 56-bit, old encryption method which is not very secure encryption method in today's world.
- 3DES — 3DES is a 168-bit, simple encryption method to increase the key size through encrypts the data for three times which provides more security than DES.
- AES-128 — AES is 128-bit encryption method which transforms the plain text into cipher text through 10 cycles repetitions.
- AES-192 — Is 192-bit encryption method which transforms the plain text into cipher text through 12 cycles repetitions.
- AES-256 — Is a 256-bit encryption method which transforms the plain text into cipher text through 14 cycles repetitions.

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 of its ends.

- MD5 — MD5 represents 32 digit hexadecimal 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.
- Null — No authentication method is used.

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

Step 10. Check the Minimum Preshared Key Complexity check box if you want to enable strength meter for the preshared key.

Step 11. Enter a key which is shared previously between the IKE peers in the Preshared Key field. Up to 30 hexadecimal and character can be used as a 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 secure.

The Preshared Key Strength Meter shows the strength of the preshared key through color bars. Red indicates weak strength, yellow indicates acceptable strength and green indicates strong strength.

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

IPSec Setup for IKE with Certificate

Only available if IKE with Certificate was selected from the Keying Mode drop-down list from Step 3 of Add a New Tunnel.

IPSec Setup

Phase 1 DH Group: Group 2 - 1024 bit ▼

Phase 1 Encryption : DES ▼

Phase 1 Authentication: MD5 ▼

Phase 1 SA Lifetime: 88029 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit ▼

Phase 2 Encryption: DES ▼

Phase 2 Authentication: MD5 ▼

Phase 2 SA Lifetime: 560 sec (Range: 120-28800, Default: 3600)

Advanced +

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 SA (Security Association) between the two ends of the tunnel to support secure authenticate communication. DH is a cryptographic key exchange protocol which is used during Phase 1 connection to share secret key to authenticate communication.

- Group 1 - 768 bit — Represents highest strength key and the most secure authentication group. But it needs more time to compute the IKE keys. It is preferred if the speed of the network is high.
- Group 2 - 1024 bit — Represents higher strength key and more secure authentication group. But it needs some time to compute the IKE keys.
- Group 5 - 1536 bit — Represents the lowest strength key and the most insecure authentication group. It needs less time to compute the IKE keys. It is preferred if the speed of the network is low.

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 — DES is 56-bit, old encryption method which is not very secure encryption method in today's world.

- 3DES — 3DES is a 168-bit, simple encryption method to increase the key size through encrypts the data for three times which provides more security than DES.
- AES-128 — AES is 128-bit encryption method which transforms the plain text into cipher text through 10 cycles repetitions.
- AES-192 — Is 192-bit encryption method which transforms the plain text into cipher text through 12 cycles repetitions.
- AES-256 — Is a 256-bit encryption method which transforms the plain text into cipher text through 14 cycles repetitions.

Step 3. Choose the appropriate 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 — MD5 represents 32 digit hexadecimal hash function which provide protection to the data from malicious attack by the checksum calculation.
- SHA1 — A 160-bit hash function which is more secure than MD5.

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

Step 5. Check Perfect Forward Secrecy check box to provide more protection to the keys. This option allows to generate a new key if any key is compromised. The encrypted data is only compromised through the compromised key. So it provides more secure and authenticated communication as it secures other keys when another key is compromised. This is a recommended action as it provides more security.

Step 6. Choose the appropriate Phase 2 DH Group from the Phase 2 DH Group drop-down list. Phase 1 is used to establish the simplex, logical SA between the two ends of the tunnel to support secure authenticate communication. DH is a cryptographic key exchange protocol which is used during Phase 1 connection to share secret key to authenticate communication.

- Group 1 - 768 bit — Represents highest strength key and the most secure authentication group. But it needs more time to compute the IKE keys. It is preferred if the speed of the network is high.
- Group 2 - 1024 bit — Represents higher strength key and more secure authentication group. But it needs some time to compute the IKE keys.
- Group 5 - 1536 bit — Represents the lowest strength key and the most insecure authentication group. It needs less time to compute the IKE keys. It is preferred if the speed of the network is low.

Note: As any new key is not generated, you do not need to configure Phase 2 DH Group if you unchecked Perfect Forward Secrecy in Step 5.

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.

- DES — DES is 56-bit, old encryption method which is not very secure encryption method in today's world.

- 3DES — 3DES is a 168-bit, simple encryption method to increase the key size through encrypts the data for three times which provides more security than DES.
- AES-128 — AES is 128-bit encryption method which transforms the plain text into cipher text through 10 cycles repetitions.
- AES-192 — Is 192-bit encryption method which transforms the plain text into cipher text through 12 cycles repetitions.
- AES-256 — Is a 256-bit encryption method which transforms the plain text into cipher text through 14 cycles repetitions.

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 of its ends.

- MD5 — MD5 represents 32 digit hexadecimal hash function which provide protection to the data from malicious attack by the checksum calculation.
- SHA1 — SHA1 is a 160 bit hash function which is more secure than MD5.
- Null — No authentication method is used.

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

Step 10. Click **Save** to save the settings.

(Optional) IPSec Advance Setup for IKE with Certificate and IKE with Preshared key

The advance options are available if IKE with Certificate or IKE with Presahred key was selected from the Keying Mode drop-down list from Step 3 of Add a New Tunnel. The same settings are available for both types of keying modes.

Step 1. Click the **Advanced+** button to display the advance IPSec options.

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm MD5 ▾

NetBIOS Broadcast

Multicast Passthrough

NAT Traversal

Dead Peer Detection Interval sec (Range: 10-999, Default: 10)

Extended Authentication

IPsec Host

User Name:

Password:

Edge Device Default - Local Database ▾ Add/Edit

Tunnel Backup

Remote Backup IP Address:

Local Interface: WAN1 ▾

VPN Tunnel Backup Idle Time: sec (Range: 30-999, Default: 30)

Split DNS

DNS Server 1:

DNS Server 2: (Optional)

Domain Name 1:

Domain Name 2: (Optional)

Domain Name 3: (Optional)

Domain Name 4: (Optional)

Step 2. Check Aggressive Mode check box if your network speed is low. It exchanges the IDs of the end points of the tunnel in clear text during SA connection, which requires less time to exchange but less secure.

Step 3. Check Compress (Support IP Payload Compression Protocol (IPComp)) check box if you want to compress the size of IP datagram. IPComp is a IP compression protocol which is used to compress the size of IP datagram, if the network speed is low and the user wants to quickly transmit the data without any loss through the slow network.

Step 4. Check Keep-Alive check box if you always want the connection of the VPN tunnel remain active. It helps to re-establish the connections immediately if any connection becomes inactive.

Step 5. Check the AH Hash Algorithm check box if you want to authentication the Authenticate Header (AH). AH provides authentication to data origin, data integrity through checksum and protection is extended into the IP header. The tunnel should have same algorithm for both of its sides.

- MD5 — MD5 represents 128 digit hexadecimal hash function which provide protection to the data from malicious attack by the checksum calculation.

- SHA1 — SHA1 is a 160 bit hash function which is more secure than MD5.

Step 6. Check NetBIOS Broadcast if you want to allow non-routable traffic through the VPN tunnel. The default is unchecked. NetBIOS is used to detect network resources like printers, computers etc. in the network through some software applications and Windows features like Network Neighborhood.

Step 7. If your VPN router is behind a NAT gateway, check the box to enable NAT traversal. Network Address Translation (NAT) enables users with private LAN addresses to access Internet resources by using a publicly routable IP address as the source address. However, for inbound traffic, the NAT gateway has no automatic method of translating the public IP address to a particular destination on the private LAN. This issue prevents successful IPSec exchanges. NAT traversal sets up this inbound translation. The same setting must be used on both ends of the tunnel.

Step 8. Check Dead Peer Detection Interval to check the liveness of the VPN tunnel through hello or ACK in a periodic manner. If you check this check box, enter the duration or interval in seconds of the hello messages you want.

Step 9. Check Extended Authentication to use an IPSec host username and password to authenticate VPN clients or to use the database found in User Management. This must be enable in both devices for it to work. Click the **IPSec Host** radio button to use IPSec host and username and enter the username and password in the User Name field and the Password field. Or Click the **Edge Device** radio button to use a database. Choose the desired database from the Edge Device drop-down list.

Step 10. Check Tunnel Backup check box to enable tunnel backup. This feature is available when Dead Peer Detection Interval has been checked. The feature enables the device to reestablish the VPN tunnel via an alternative WAN interface or IP address.

- Remote Backup IP Address — An alternative IP for the remote peer. Enter it or the WAN IP that was already set for the remote gateway in this field.
- Local Interface — The WAN interface used to reestablish the connection. Choose the desired interface from the drop-down list.
- VPN Tunnel Backup Idle Time — The time chosen for when to use the backup tunnel if the primary tunnel is not connected. Enter it in seconds.

Step 11. Check the Split DNS check box to enable split DNS. This feature allows to send DNS request to a defined DNS server based on specified domain names. Enter the DNS server names in the DNS Server 1 and DNS Server 2 fields and enter the domain names in the Domain Name # fields.

Step 12. Click **Save** to finish configuring the device.