

Configure Advanced Virtual Private Network (VPN) Setup on an RV130 or RV130W Router

Objective

A Virtual Private Network (VPN) is a secure connection established within a network or between networks. VPNs serve to isolate traffic between specified hosts and networks from the traffic of unauthorized hosts and networks. A site-to-site (gateway-to-gateway) VPN connects entire networks to each other, maintaining the security by creating a tunnel over a public domain otherwise known as the Internet. Each site needs only a local connection to the same public network, thereby saving money on long private leasedlines.

VPNs are beneficial to companies in such a way that it is highly scalable, simplifies network topology, and improves productivity by reducing travel time and cost for remote users.

Internet Key Exchange (IKE) is a protocol used to establish a secure connection for communication in a VPN. This secure connection is called a Security Association (SA). You can create IKE policies to define the security parameters to be used in this process such as authentication of the peer, encryption algorithms, and so on. For a VPN to function properly, the IKE policies for both end points should be identical.

This article aims to show how to configure the Advanced VPN Setup on an RV130 or RV130W router, which covers IKE Policy settings and VPN Policy settings.

Applicable Devices

- RV130
- RV130W

Software Version

- 1.0.3.22

Configure Advanced VPN Setup

Add/Edit Internet Key Exchange (IKE) Policy Settings

Step 1. Log in to the web-based utility and choose **VPN > Site-to-Site IPSec VPN >Advanced VPN Setup**.

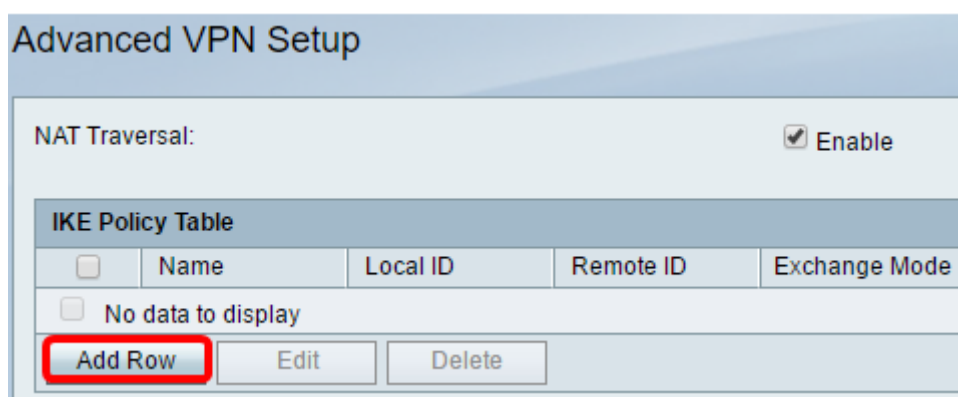


Step 2. (Optional) Check the **Enable** check box in NAT Traversal if you want to enable Network Address Translation (NAT) Traversal for the VPN connection. NAT Traversal allows a VPN connection to be made between gateways that use NAT. Choose this option if your VPN connection passes through a NAT-enabled gateway.



Step 3. In the IKE Policy Table, click **Add Row** to create a new IKE policy.

Note: If basic settings have been configured, then the table below will contain the created basic VPN setting. You can edit an existing IKE policy by checking the check box for the policy and click **Edit**. The Advanced VPN Setup page changes:



Step 4. In the *IKE Name* field, enter a unique name for the IKE policy.

Note: If basic settings have been configured, the connection name created would be set as the IKE Name. In this example, VPN1 is the chosen IKE name.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

Step 5. From the Exchange Mode drop-down list, choose an option.

- Main — This option allows the IKE policy to negotiate the VPN tunnel with higher security than aggressive mode. Click this option if a more secure VPN connection is a priority over a speed of negotiation.
- Aggressive — This option allows the IKE policy to establish a faster but less secure connection than the main mode. Click this option if a faster VPN connection is a priority over a high security.

Note: In this example, Main is chosen.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:	<input type="text" value="VPN1"/>
Exchange Mode:	<input type="text" value="Main"/>
Local	<input type="text" value="Main"/>
Local Identifier Type:	<input type="text" value="Local WAN IP"/>

Step 6. Choose from the Local Identifier Typedrop-down list to identify or specify the Internet Security Association and Key Management Protocol (ISAKMP) of your local router. The options are:

- Local WAN IP — Router uses local Wide Area Network (WAN) IP as the main identifier. This option connects through the Internet. Choosing this option greys out the *Local Identifier* field below.
- IP Address — Clicking this allows you to enter an IP address in the *Local Identifier* field.
- FQDN — A Fully Qualified Domain Name (FQDN) or your domain name such as <http://www.example.com> allows you to enter your domain name or IP address in the *Local Identifier* field.
- User-FQDN — This option is a user email address such as user@email.com. Enter a domain name or an IP address in the *Local Identifier* field.
- DER ASN1 DN — This option is an identifier type for the Distinguished Name (DN) that uses Distinguished Encoding Rules Abstract Syntax Notation One (DER ASN1) to transmit information. This happens when the VPN tunnel is associated with a user certificate. If this is chosen, enter a domain name or an IP address in the *Local Identifier* field.

Note: In this example, Local WAN IP is chosen.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

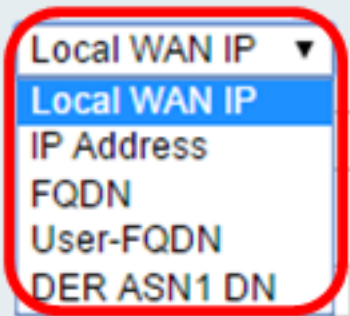
Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:



Step 7. Choose from the Remote Identifier Type drop-down list to identify or specify the Internet Security Association and Key Management Protocol (ISAKMP) of your remote router. The options are Remote WAN IP, IP Address, FQDN, User FQDN, and DER ASN1 DN.

Note: In this example, Remote WAN IP is chosen.

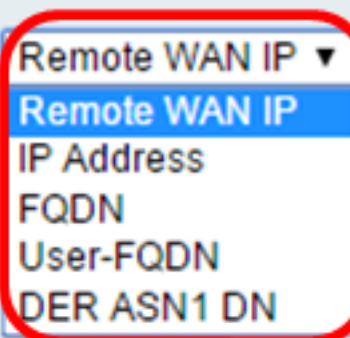
Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

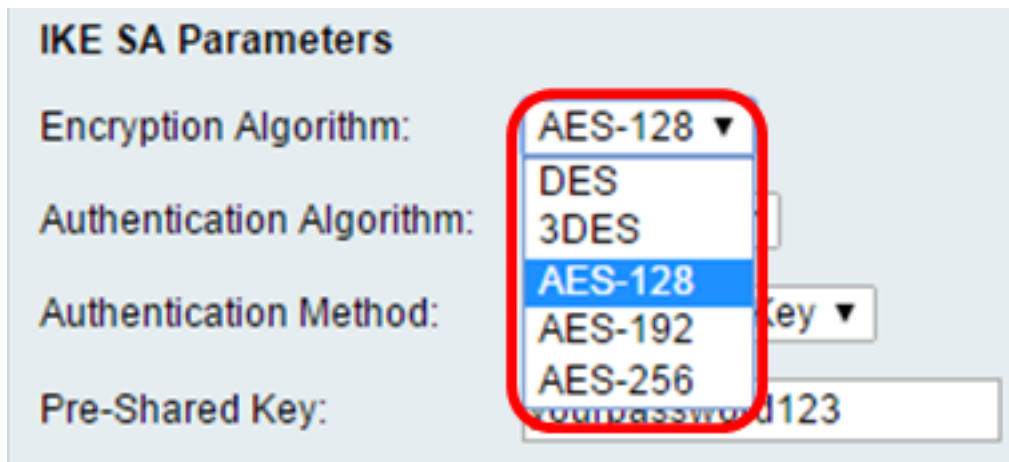


Step 8. Choose an option from the Encryption Algorithm drop-down list.

- DES — Data Encryption Standard (DES) is a 56-bit, old encryption method which is not a very secure encryption method, but may be required for backwards compatibility.
- 3DES — Triple Data Encryption Standard (3DES) is a 168-bit, simple encryption method used to increase the key size because it encrypts the data three times. This provides more security than DES but less security than AES.
- AES-128 — Advanced Encryption Standard with 128-bit key (AES-128) uses a 128-bit key for AES encryption. AES is faster and more secure than DES. In general, AES is also faster and more secure than 3DES. AES-128 is the default encryption algorithm and is faster but less secure than AES-192 and AES-256.

- AES-192 — AES-192 uses a 192-bit key for AES encryption. AES-192 is slower but more secure than AES-128, and faster but less secure than AES-256.
- AES-256 — AES-256 uses a 256-bit key for AES encryption. AES-256 is slower but more secure than AES-128 and AES-192.

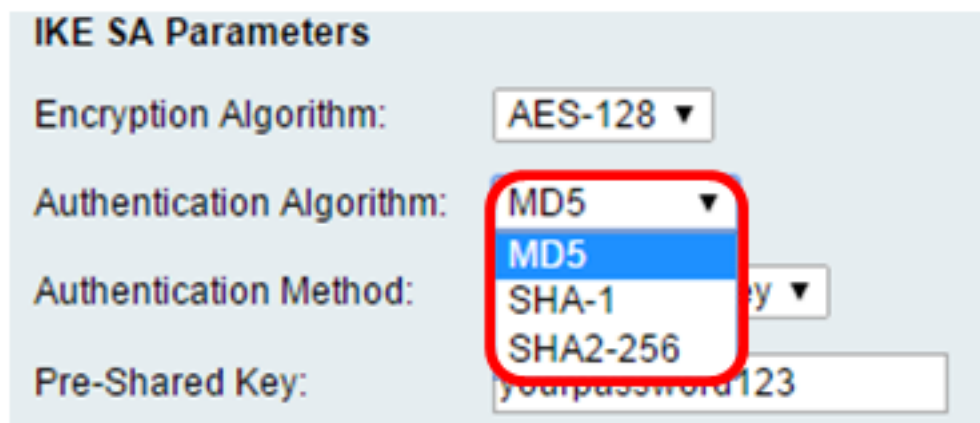
Note: In this example, AES-128 is selected.



Step 9. From the Authentication Algorithm drop-down list, choose from the following options:

- MD5 — Message Digest 5 (MD5) is an authentication algorithm that uses a 128-bit hash value for authentication. MD5 is less secure, but faster than SHA-1 and SHA2-256.
- SHA-1 — Secure Hash Function 1 (SHA-1) uses a 160-bit hash value for authentication. SHA-1 is slower but more secure than MD5. SHA-1 is the default authentication algorithm and is faster but less secure than SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 with a 256-bit hash value (SHA2-256) uses a 256-bit hash value for authentication. SHA2-256 is slower but more secure than MD5 and SHA-1.

Note: In this example, MD5 is chosen.



Step 10. In the Authentication Method drop-down list, choose from the following options:

- Pre-Shared Key — This option requires a password that is shared with the IKE peer.
- RSA-Signature — This option uses certificates to authenticate connection. If this is chosen, Pre-Shared Key field is disabled. Skip to [Step 12](#).

Note: In this example Pre-Shared key is chosen.

IKE SA Parameters

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key:

DH Group: Group2 (1024 bit) ▼

Step 11. In the *Pre-Shared Key* field, enter a password that is between 8 and 49 characters in length.

Note: In this example, yourpassword123 is used.

IKE SA Parameters

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key: yourpassword123

[Step 12.](#) From the DH Group drop-down list, choose which Diffie-Hellman (DH) group algorithm the IKE uses. Hosts in a DH group can exchange keys without the knowledge of each other. The higher the group bit number is, the better the security.

Note: In this example, Group1 is chosen.

DH Group: Group1 (768 bit) ▼

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

Save Cancel Back

Step 13. In the *SA-Lifetime* field, enter how long in seconds an SA for the VPN lasts before

the SA is renewed. The range is from 30 to 86400 seconds. The default is 28800.

DH Group: Group1 (768 bit) ▾
SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection: Enable
DPD Delay: 10 (Range: 10 - 999, Default: 10)
DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Save Cancel Back

[Step 14](#). (Optional) Check the **Enable** Dead Peer Detection check box to enable Dead Peer Detection (DPD). DPD monitors IKE peers to see if a peer has ceased to function or is still alive. If the peer is detected as dead, the device deletes the IPsec and IKE Security Association. DPD prevents the waste of network resources on inactive peers.

Note: If you do not wish to enable Dead Peer Detection, skip to [Step 17](#).

Dead Peer Detection: Enable
DPD Delay: 10 (Range: 10 - 999, Default: 10)
DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Save Cancel Back

Step 15. (Optional) If you enabled DPD in [Step 14](#), enter how often (in seconds) the peer is checked for activity in the *DPD Delay* field.

Note: The DPD Delay is the interval in seconds between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when the IPsec traffic is idle. The default value is 10.

Dead Peer Detection: Enable
DPD Delay: 10 (Range: 10 - 999, Default: 10)
DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Save Cancel Back

Step 16. (Optional) If you enabled DPD in [Step 14](#), enter how many seconds to wait before an inactive peer is dropped in the *DPD Timeout* field.

Note: This is the maximum time that the device should wait to receive a response to the DPD message before considering the peer to be dead. The default value is 30.

Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

[Step 17.](#) Click **Save**.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

Note: The main Advanced VPN Setup page re-appears.

You should now have successfully configured the IKE Policy Settings on your router.

Configure VPN Policy Settings

Note: For a VPN to function properly, the VPN policies for both end points should be identical.

Step 1. In the VPN Policy Table, click **Add Row** to create a new VPN policy.

Note: You can also edit a VPN policy by checking the check box for the policy and click **Edit**. The Advanced VPN Setup page appears:

The screenshot shows the 'Advanced VPN Setup' interface. At the top, there is a 'NAT Traversal' section with a checkbox. Below it is the 'IKE Policy Table' with columns for Name, Local ID, Remote ID, Exchange Mode, and a checkbox. A row is shown with 'VPN1' in the Name column, 'Local WAN IP' in the Local ID column, 'Remote WAN IP' in the Remote ID column, and 'Main' in the Exchange Mode column. Below the table are 'Add Row', 'Edit', and 'Delete' buttons. The 'VPN Policy Table' is below that, with columns for Status, Name, Policy Type, and Encryption. It shows 'No data to display' and has 'Add Row', 'Edit', 'Enable', 'Disable', and 'Delete' buttons. At the bottom are 'Save', 'Cancel', and 'IPSec Connection Status' buttons. The 'Add Row' button in the VPN Policy Table is highlighted with a red box.

Step 2. In the *IPSec Name* field under the Add/Edit VPN Configuration area, enter a name for the VPN policy.

Note: In this example, VPN1 is used.

The screenshot shows the 'Advanced VPN Setup' interface, specifically the 'Add / Edit VPN Policy Configuration' section. It has three fields: 'IPSec Name' with a text input field containing 'VPN1', 'Policy Type' with a dropdown menu showing 'Auto Policy', and 'Remote Endpoint' with a dropdown menu showing 'IP Address'. The 'IPSec Name' field is highlighted with a red box.

[Step 3.](#) From the Policy Type drop-down list, choose an option.

- Manual Policy — 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. Continue the steps until Remote Traffic Selection. Click [here](#) to know the steps.

- Auto Policy — Policy parameters are set automatically. This option uses an IKE policy for data integrity and encryption key exchanges. If this is chosen the configuration settings under the Auto Policy Parameters area are enabled. Click [here](#) to know the steps. Make sure that your IKE protocol automatically negotiates between the two VPN endpoints.

Note: In this example, Auto Policy is chosen.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

Step 4. From the Remote Endpoint drop-down list, choose an option.

- IP Address — This option identifies the remote network by a public IP address.
- FQDN — Complete domain name for a specific computer, or host, or the Internet. The FQDN consists of two parts: the hostname and the domain name. This option can only be enabled when **Auto Policy** is selected in [Step 3](#).

Note: For this example, IP Address is chosen.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

Step 5. In the *Remote Endpoint* field, enter either the public IP address or domain name of the remote address.

Note: In this example, 192.168.2.101 is used.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

VPN1

Policy Type:

Auto Policy ▼

Remote Endpoint:

IP Address ▼

192.168.2.101

Step 6. (Optional) Check the **NetBios Enabled** check box if you want to enable Network Basic Input/Output System (NetBIOS) broadcasts to be sent through the VPN connection. NetBIOS allows hosts to communicate with each other within a Local Area Network (LAN).

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

VPN1

Policy Type:

Auto Policy ▼

Remote Endpoint:

IP Address ▼

192.168.1.102 (Hi

NetBios Enabled:



[Step 7.](#) From the Local IP drop-down list under the Local Traffic Selection area, choose an option.

- Single — Limits the policy to one host.
- Subnet — Allows hosts within an IP address range to connect to the VPN.

Note: In this example, Subnet is chosen.

Local Traffic Selection

Local IP:

Subnet ▼

IP Address:

Single

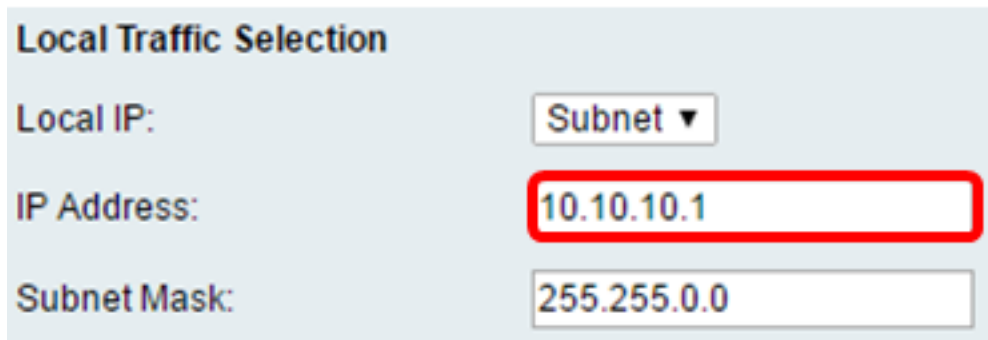
Subnet

Subnet Mask:

255.255.0.0

Step 8. In the IP Address field, enter the host or subnet IP address of the local subnet or host.

Note: In this example, the local subnet IP Address of 10.10.10.1 is used.



Local Traffic Selection

Local IP: Subnet ▼

IP Address: 10.10.10.1

Subnet Mask: 255.255.0.0

Step 9. (Optional) If Subnet is selected in [Step 7](#), enter the subnet mask of the client in the *Subnet Mask* Field. The Subnet Mask field is disabled if Single is chosen in Step 1.

Note: In this example, the subnet mask of 255.255.0.0 is used.



Local Traffic Selection

Local IP: Subnet ▼

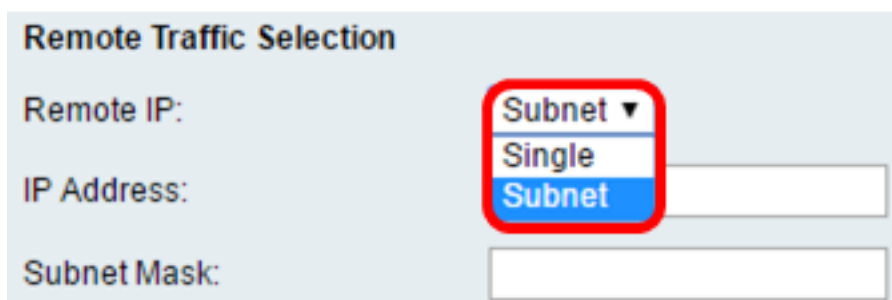
IP Address: 10.10.10.1

Subnet Mask: 255.255.0.0

[Step 10](#). From the Remote IP drop-down list under the Remote Traffic Selection area, choose an option.

- Single — Limits the policy to one host.
- Subnet — Allows hosts within an IP address range to connect to the VPN.

Note: In this example, Subnet is chosen.



Remote Traffic Selection

Remote IP: Subnet ▼

IP Address: [Empty]

Subnet Mask: [Empty]

Step 11. Enter the range of IP addresses of the host that will be part of the VPN in the *IP Address* field. If **Single** is selected in [Step 10](#), enter an IP address.

Note: In the example below, 10.10.11.2 is used.

Remote Traffic Selection

Remote IP:

IP Address:

Subnet Mask:

Step 12. (Optional) If **Subnet** is selected in [Step 10](#), enter the subnet mask of the subnet IP address in the *Subnet Mask* field.

Note: In the example below, 255.255.0.0 is used.

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

[Manual Policy Parameters](#)

Note: These fields can only be edited if **Manual Policy** is chosen.

Step 1. In the *SPI-Incoming* field, enter a three to eight hexadecimal characters for Security Parameter Index (SPI) tag for incoming traffic on the VPN connection. The SPI tag is used to distinguish the traffic of one session from the traffic of other sessions.

Note: For this example, 0xABCD is used.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Step 2. In the *SPI-Outgoing* field, enter three to eight hexadecimal characters for SPI tag for outgoing traffic on the VPN connection.

Note: For this example, 0x1234 is used.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

[Step 3](#). From the Manual Encryption Algorithm drop-down list, choose an option. The options are DES, 3DES, AES-128, AES-192, and AES-256.

Note: In this example, AES-128 is chosen.

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Manual Encryption Algorithm: AES-128 ▼

Key-In: []

Key-Out: []

Manual Integrity Algorithm: SHA-1 ▼

Step 4. In the *Key-In* field, enter a key for the inbound policy. The key length depends on the algorithm chosen in [Step 3](#).

- DES uses an 8-character key.
- 3DES uses a 24-character key.
- AES-128 uses a 16-character key.
- AES-192 uses a 24-character key.
- AES-256 uses a 32-character key.

Note: In this example, 123456789ABCDEFGG is used.

Manual Encryption Algorithm: AES-128 ▼

Key-In: 123456789ABCDEFGG

Key-Out: 123456789ABCDEFGG

Step 5. In the *Key-Out* field, enter a key for the outgoing policy. The key length depends on the algorithm chosen in [Step 3](#).

Note: In this example, 123456789ABCDEFGG is used.

Manual Encryption Algorithm: AES-128 ▼
Key-In: 123456789ABCDEFGG
Key-Out: 123456789ABCDEFGG

[Step 6](#). From the Manual Integrity Algorithm drop-down list, choose an option.

- MD5 — Uses a 128-bit hash value for data integrity. MD5 is less secure but faster than SHA-1 and SHA2-256.
- SHA-1 — Uses a 160-bit hash value for data integrity. SHA-1 is slower but more secure than MD5, and SHA-1 is faster but less secure than SHA2-256.
- SHA2-256 — Uses a 256-bit hash value for data integrity. SHA2-256 is slower but secure than MD5 and SHA-1.

Note: In this example, MD5 is chosen.

Manual Integrity Algorithm: MD5 ▼
Key-In: CDEFG
Key-Out: 123456789ABCDEFGG

Step 7. In the *Key-In field*, enter a key for the inbound policy. The key length depends on the algorithm chosen in [Step 6](#).

- MD5 uses a 16-character key.
- SHA-1 uses a 20-character key.
- SHA2-256 uses a 32-character key.

Note: In this example, 123456789ABCDEFGG is used.

Manual Integrity Algorithm: MD5 ▼
Key-In: 123456789ABCDEFGG
Key-Out: 123456789ABCDEFGG

Step 8. In the *Key-Out field*, enter a key for the outgoing policy. The key length depends on the algorithm chosen in [Step 6](#).

Note: In this example, 123456789ABCDEFGG is used.

Manual Integrity Algorithm:	MD5 ▼
Key-In:	123456789ABCDEFGH
Key-Out:	123456789ABCDEFGH

Auto Policy Parameters

Note: Before you create an Auto VPN Policy, ensure that you create the IKE Policy based on which you want to create the auto VPN policy. These fields can only be edited if **Auto Policy** is selected in [Step 3](#).

Step 1. In the *IPSec SA-Lifetime field*, enter how long in seconds the SA lasts before renewal. The range is from 30-86400. The default is 3600.

Auto Policy Parameters	
IPSec SA Lifetime:	3600 Seconds (Range: 30 - 86400, Default: 3600)
Encryption Algorithm:	AES-128 ▼
Integrity Algorithm:	SHA-1 ▼
PFS Key Group:	<input type="checkbox"/> Enable

Step 2. From the Encryption Algorithm drop-down list, choose an option. The options are:

Note: In this example, AES-128 is chosen.

- DES — A 56-bit, old encryption method which is not a very secure encryption method, but may be required for backwards compatibility.
- 3DES — A 168-bit, simple encryption method used to increase the key size because it encrypts the data three times. This provides more security than DES but less security than AES.
- AES-128 — Uses a 128-bit key for AES encryption. AES is faster and more secure than DES. In general, AES is also faster and more secure than 3DES. AES-128 is faster but less secure than AES-192 and AES-256.
- AES-192 — Uses a 192-bit key for AES encryption. AES-192 is slower but more secure than AES-128, and faster but less secure than AES-256.
- AES-256 — Uses a 256-bit key for AES encryption. AES-256 is slower but more secure than AES-128 and AES-192.
- AESGCM — Advanced Encryption Standard Galois Counter Mode is a generic authenticated encryption block cipher mode. GCM authentication uses operations that are particularly well suited to efficient implementation in hardware, making it especially appealing for high-speed implementations, or for implementations in an efficient and compact circuit.
- AESCCM — Advanced Encryption Standard Counter with CBC-MAC Mode is a generic authenticated encryption block cipher mode. CCM is well suited for use in compact software implementations.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seco

Encryption Algorithm:

Integrity Algorithm: AES-128, 3DES, DES, AES-128, AES-192, AES-256, AESGCM, AESCCM

PFS Key Group:

DH Group:

Select IKE Policy:

View

Save Cancel Back

Step 3. From the Integrity Algorithm drop-down list, choose an option. The options are MD5, SHA-1, and SHA2-256.

Note: In this example, SHA-1 is chosen.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seco

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1, SHA-1, SHA2-256, MD5

PFS Key Group:

DH Group:

Select IKE Policy: VPN1

[Step 4.](#) Check the **Enable** check box in the PFS Key Group to enable Perfect Forward Secrecy (PFS). PFS increases the VPN security, but slows down the speed of connection.

Auto Policy Parameters

IPSec SA Lifetime: Seconds

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

DH Group: ▼

Select IKE Policy: ▼

Step 5. (Optional) If you chose to enable PFS in [Step 4](#), choose a DH group to join from the DH group drop-down list. The higher the group number is, the better the security.

Note: For this example, Group 1 is chosen.

Auto Policy Parameters

IPSec SA Lifetime: Seconds

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

DH Group: ▼

Select IKE Policy: ▼

Step 6. From the Select IKE Policy drop-down list, choose which IKE policy to use for the VPN policy.

Note: In this example, only one IKE policy has been configured so only one policy appears.

Auto Policy Parameters

IPSec SA Lifetime: Seconds (Ra

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

DH Group: ▼

Select IKE Policy: ▼

Step 7. Click **Save**.

Auto Policy Parameters

IPSec SA Lifetime: Seconds (R

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

DH Group: ▼

Select IKE Policy: ▼

Note: The main Advanced VPN Setup page re-appears. A confirmation message that the configuration settings have been saved successfully should appear.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Step 8. Under the VPN Policy table, check a check box to choose a VPN and click **Enable**.

Note: Configured VPN Policy is disabled by default.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

Add Row

Edit

Delete

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Add Row

Edit

Enable

Disable

Delete

Save

Cancel

IPSec Connection Status

Step 9. Click **Save**.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

You should now have successfully configured a VPN Policy on your RV130 or RV130W router.