



Article ID: 4989

VPN Policy Configuration on RV130 and RV130W

Objective

The VPN Policy features allow you to configure VPN settings for Automatic Policy, Manual Policy, and Encryption and Integrity Algorithms.

Before configuring VPN Policy, verify that you have created an Internet Key Exchange (IKE) Policy. Refer to [Internet Key Exchange \(IKE\) Policy Settings on RV130 and RV130W VPN Routers](#) for more information.

The objective of this document is to show you how to set the VPN Policies on the Cisco Small Business RV130 and RV130W VPN Firewall.

Applicable Devices

- RV130
- RV130W

VPN Policy Configuration on the RV130 and RV130W

Step 1. Log in to the web configuration utility and choose **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup**. The *Advanced VPN Setup* page opens:

Advanced VPN Setup

NAT Traversal: ☐ Enable

IKE Policy Table							
<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group
<input type="checkbox"/>	testkey	Local WAN IP	Remote WAN IP	Main	AES-128	SHA-1	Group1 (768 bit)
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Algorithm	Local	Remote
<input type="checkbox"/> No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>							

Step 2. In the *VPN Policy Table* section, click **Add Row**.

Advanced VPN Setup

NAT Traversal: ☐ Enable

IKE Policy Table							
<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group
<input type="checkbox"/>	testkey	Local WAN IP	Remote WAN IP	Main	AES-128	SHA-1	Group1 (768 bit)
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Algorithm	Local	Remote
<input type="checkbox"/> No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>							

The following page appears:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Auto Policy ▾

Remote Endpoint:

IP Address ▾

(Hint: 1.2.3.4 or abc.com)

NetBios Enabled:

☐

Local Traffic Selection

Local IP:

Subnet ▾

IP Address:

(Hint: 1.2.3.4)

Subnet Mask:

(Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

Subnet ▾

IP Address:

(Hint: 1.2.3.4)

Subnet Mask:

(Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

0x

SPI-Outgoing:

0x

Manual Encryption Algorithm:

AES-128 ▾

Key-In:

Key-Out:

Manual Integrity Algorithm:

SHA-1 ▾

Key-In:

Key-Out:

Auto Policy Parameters

IPSec SA Lifetime:

3600

Seconds (Range: 30 - 86400, Default: 3600)

Encryption Algorithm:

AES-128 ▾

Integrity Algorithm:

SHA-1 ▾

PFS Key Group:

☐ Enable

DH Group:

Group 1(768 bit) ▾

Select IKE Policy:

testkey ▾

View

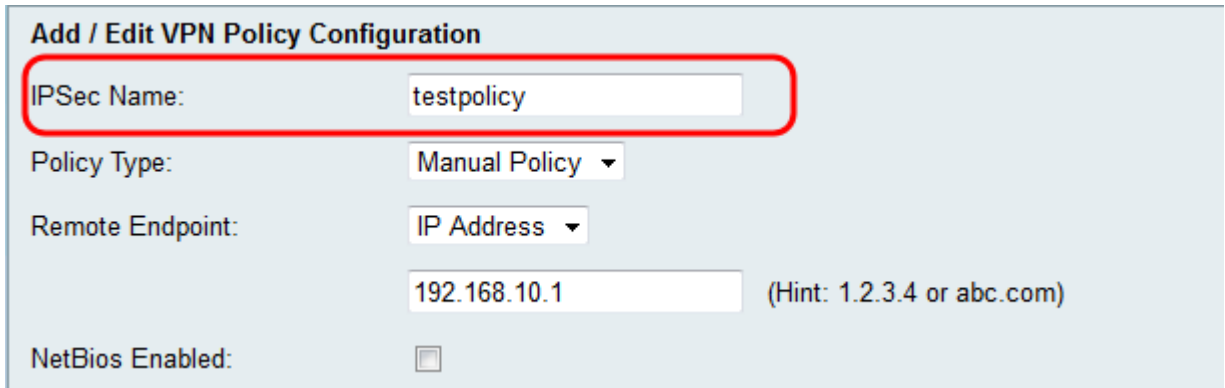
Save

Cancel

Back

Add/Edit VPN Policy Configuration

Step 1. Enter a unique name in the *IPSec Name* field for the policy to be set.



Add / Edit VPN Policy Configuration

IPSec Name:

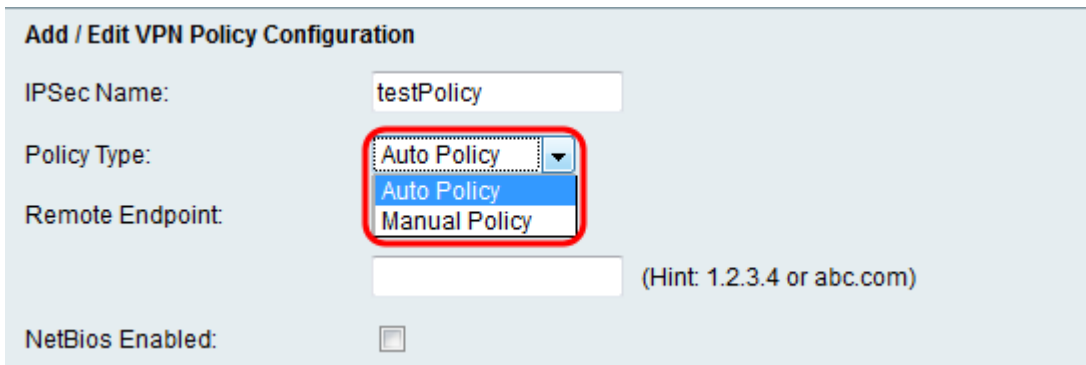
Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

NetBios Enabled: ☐

Step 2. Choose the appropriate policy type from the *Policy Type* drop-down list.



Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

NetBios Enabled: ☐

The available options are defined as follows:

- Auto Policy — Policy parameters are set automatically. If this selection is chosen, make sure that your IKE protocol automatically negotiates between the two VPN endpoints.
- Manual Policy — All settings for the VPN tunnel are manually input for each endpoint.

Step 3. Choose the type of IP identifier that would identify the gateway at the remote endpoint in the *Remote Endpoint* drop-down list.

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

IP Address

IP Address

FQDN

 (Hint: 1.2.3.4 or abc.com)

NetBios Enabled: ☐

The available options are defined as follows:

- IP Address — Unique string of numbers separated by periods that identifies each machine using the Internet Protocol to communicate over a network.
- FQDN (Fully Qualified Domain Name) — Complete domain name for a specific computer, or host, or the Internet. The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN for a hypothetical mail server might be *mymail.companyname.org*. The hostname is *mymail*, and the host is located within the domain *companyname.org*. This option can only be enabled when **Manual Policy** is selected in Step 4.

Step 4. Depending on which option you chose in Step 3, enter the IP Address or FQDN, into the field below.

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

NetBios Enabled: ☐

Step 5. To enable NetBIOS broadcasts to travel across the VPN tunnel, check the **Enable** checkbox.

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

NetBios Enabled: ☒

Local Traffic Selection

Step 1. Choose the type of identifier that you want to provide for the end point in the *Local IP* drop-down list.

Local Traffic Selection

Local IP:

IP Address:

Subnet Mask: (Hint: 1.2.3.4)

(Hint: 255.255.255.0)

The available options are defined as follows:

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

Step 2. Enter the IP address of the client that will be part of the VPN in the *IP Address* field. If **Subnet** is selected in Step 1, enter the range of IP addresses.

Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Step 3. (Optional) If **Subnet** is selected in step 1, enter the subnet mask of the client in the *Subnet Mask* field.

Local Traffic Selection

Local IP: Subnet ▼

IP Address: 192.168.1.2 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.255 (Hint: 255.255.255.0)

Remote Traffic Selection

Step 1. Choose the type of identifier that you want to provide for the end point in the *Remote IP* field.

Remote Traffic Selection

Remote IP: Single ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

The available options are defined as follows:

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

Step 2. Enter the IP address of the host that will be part of the VPN in the *IP Address* field. If **Subnet** is selected in Step 1, enter the range of IP addresses.

Remote Traffic Selection

Remote IP: Subnet ▼

IP Address: 192.168.1.100 (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Step 3. (Optional) If **Subnet** is selected in Step 1, enter the subnet mask of the host in the *Subnet Mask* field.

Remote Traffic Selection

Remote IP: Subnet ▼

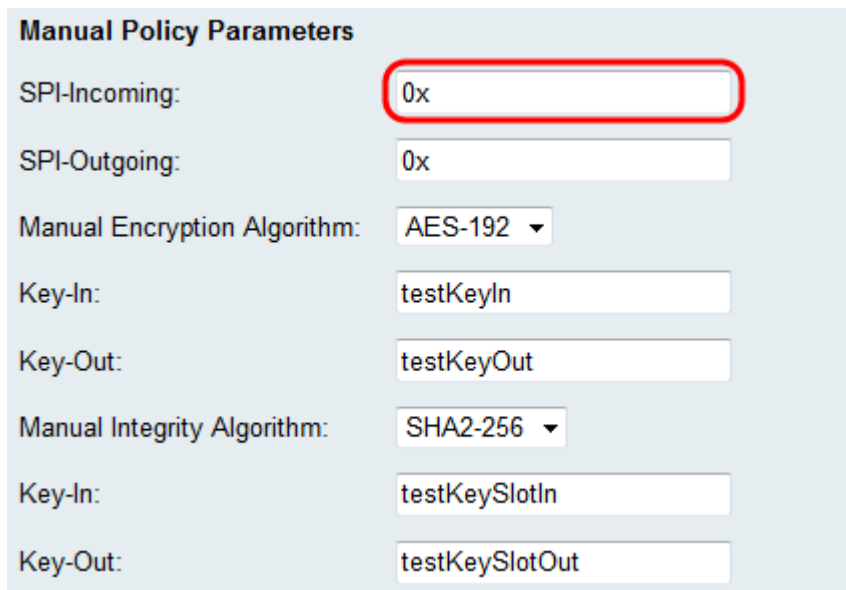
IP Address: 192.168.1.100 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

Note: These fields can only be edited if **Manual Policy** is selected in step 2 of the *Add/Edit VPN Policy Configuration* section.

Step 1. Enter a hexadecimal value between 3 and 8 in the *SPI-Incoming* field. Stateful Packet Inspection (SPI) is a technology referred to as Deep Packet Inspection (DPI). SPI implements a number of security features that help keep your computer network safe. Any value is acceptable as long as you verify that the remote VPN endpoint has the same value in its SPI-Outgoing field.



The screenshot shows a configuration form titled "Manual Policy Parameters" with a light blue background. It contains several fields for configuring VPN policy parameters. The "SPI-Incoming" field is highlighted with a red border and contains the text "0x". The "SPI-Outgoing" field also contains "0x". The "Manual Encryption Algorithm" is set to "AES-192" with a dropdown arrow. The "Key-In" field contains "testKeyIn" and the "Key-Out" field contains "testKeyOut". The "Manual Integrity Algorithm" is set to "SHA2-256" with a dropdown arrow. The "Key-In" field for integrity contains "testKeySlotIn" and the "Key-Out" field contains "testKeySlotOut".

Manual Policy Parameters	
SPI-Incoming:	0x
SPI-Outgoing:	0x
Manual Encryption Algorithm:	AES-192 ▼
Key-In:	testKeyIn
Key-Out:	testKeyOut
Manual Integrity Algorithm:	SHA2-256 ▼
Key-In:	testKeySlotIn
Key-Out:	testKeySlotOut

Step 2. Enter a hexadecimal value between 3 and 8 in the *SPI-Outgoing* field. Any value is acceptable as long as you verify that the remote VPN endpoint has the same value in its SPI-Incoming field.

Manual Policy Parameters

SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Manual Encryption Algorithm:	<input type="text" value="AES-192"/>
Key-In:	<input type="text" value="testKeyIn"/>
Key-Out:	<input type="text" value="testKeyOut"/>
Manual Integrity Algorithm:	<input type="text" value="SHA2-256"/>
Key-In:	<input type="text" value="testKeySlotIn"/>
Key-Out:	<input type="text" value="testKeySlotOut"/>

Step 3. Choose the appropriate Encryption Algorithms from the *Manual Encryption Algorithm* drop-down list. The default and recommended option is AES-128 for its high security and fast performance.

Manual Policy Parameters

SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Manual Encryption Algorithm:	<input type="text" value="AES-192"/>
Key-In:	<input type="text" value="testKeyIn"/>
Key-Out:	<input type="text" value="testKeyOut"/>
Manual Integrity Algorithm:	<input type="text" value="SHA2-256"/>
Key-In:	<input type="text" value="testKeySlotIn"/>
Key-Out:	<input type="text" value="testKeySlotOut"/>

The available options are defined as follows:

- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should only be used if one endpoint solely supports DES.
- 3DES — Triple Data Encryption Standard (3DES) performs DES three times but varies the key size from 168 bits to 112 bits, and from 112 bits to 56 bits

depending on the round of DES performed. 3DES is more secure than DES but less secure 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 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.
- AESGCM — AESGCM 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 — AESCCM is a generic authenticated encryption block cipher mode. CCM is well suited for use in compact software implementations.

Step 4. Enter the encryption key of the inbound policy in the *Key-In* field.

The screenshot shows a configuration form titled "Manual Policy Parameters" with the following fields and values:

Field	Value
SPI-Incoming:	0x
SPI-Outgoing:	0x
Manual Encryption Algorithm:	AES-192
Key-In:	testKeyIn
Key-Out:	testKeyOut
Manual Integrity Algorithm:	SHA2-256
Key-In:	testKeySlotIn
Key-Out:	testKeySlotOut

The "Key-In" field for the encryption algorithm is highlighted with a red circle.

Step 5. Enter the encryption key of the outbound policy in the *Key-Out* field.

Manual Policy Parameters

SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Manual Encryption Algorithm:	<input type="text" value="AES-192"/>
Key-In:	<input type="text" value="testKeyIn"/>
Key-Out:	<input type="text" value="testKeyOut"/>
Manual Integrity Algorithm:	<input type="text" value="SHA2-256"/>
Key-In:	<input type="text" value="testKeySlotIn"/>
Key-Out:	<input type="text" value="testKeySlotOut"/>

Step 6. Choose the appropriate Integrity Algorithm from the *Manual Integrity Algorithm* drop-down list. The algorithm will verify the integrity of the data. SHA2-256 is recommended as it is more secure than SHA-1 and MD5.

Manual Policy Parameters

SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Manual Encryption Algorithm:	<input type="text" value="AES-192"/>
Key-In:	<input type="text" value="testKeyIn"/>
Key-Out:	<input type="text" value="testKeyOut"/>
Manual Integrity Algorithm:	<input type="text" value="SHA2-256"/>
Key-In:	<input type="text" value="testKeySlotIn"/>
Key-Out:	<input type="text" value="testKeySlotOut"/>

The available options are defined as follows:

- 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, 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.
- MD5 — Message-Digest Algorithm 5 (MD5) uses a 128-bit hash value for authentication. MD5 is less secure, but faster than SHA-1 and SHA2-256.

Step 7. Enter the integrity key of the inbound policy in the *Key-In* field.

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Manual Encryption Algorithm:	<input type="text" value="AES-192"/>
Key-In:	<input type="text" value="testKeyIn"/>
Key-Out:	<input type="text" value="testKeyOut"/>
Manual Integrity Algorithm:	<input type="text" value="SHA2-256"/>
Key-In:	<input type="text" value="testKeySlotIn"/>
Key-Out:	<input type="text" value="testKeySlotOut"/>

Step 8. Enter the integrity key of the outbound policy in the *Key-Out* field.

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="0x"/>
SPI-Outgoing:	<input type="text" value="0x"/>
Manual Encryption Algorithm:	<input type="text" value="AES-192"/>
Key-In:	<input type="text" value="testKeyIn"/>
Key-Out:	<input type="text" value="testKeyOut"/>
Manual Integrity Algorithm:	<input type="text" value="SHA2-256"/>
Key-In:	<input type="text" value="testKeySlotIn"/>
Key-Out:	<input type="text" value="testKeySlotOut"/>

Auto Policy Parameters

Note: These fields can only be edited if **Auto Policy** is selected in step 2 of the *Add/Edit VPN Policy Configuration* section. Also, you must have created an Internet Key Exchange (IKE) Policy prior to configuring this section. To create an IKE Policy, refer to [Internet Key Exchange \(IKE\) Policy Settings on the RV130 and RV130W VPN Routers](#).

Step 1. In the *IPSec SA Lifetime* field, enter the duration of the security association in seconds. The default value is 3600 seconds, and the range is between 30-86400 seconds.

The screenshot shows the 'Auto Policy Parameters' configuration page. The 'IPSec SA Lifetime' field is highlighted with a red rectangle and contains the value '3600'. To the right of the field, it says 'Seconds (Range: 30 - 86400, Default: 3600)'. Other fields include 'Encryption Algorithm' (AES-128), 'Integrity Algorithm' (SHA-1), 'PFS Key Group' (unchecked), 'DH Group' (Group 1(768 bit)), and 'Select IKE Policy' (testkey). A 'View' button is at the bottom.

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
DH Group:	Group 1(768 bit)
Select IKE Policy:	testkey
<button>View</button>	

Step 2. Choose the appropriate Encryption Algorithm from the *Encryption Algorithm* drop-down list. The default and recommended option is AES-128 for its high security and fast performance.

The screenshot shows the 'Auto Policy Parameters' configuration page. The 'Encryption Algorithm' field is highlighted with a red rectangle and contains the value 'AES-128'. Other fields include 'IPSec SA Lifetime' (3600), 'Integrity Algorithm' (SHA-1), 'PFS Key Group' (unchecked), 'DH Group' (Group 1(768 bit)), and 'Select IKE Policy' (testkey). A 'View' button is at the bottom.

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
DH Group:	Group 1(768 bit)
Select IKE Policy:	testkey
<button>View</button>	

The available options are defined as follows:

- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should only be used if one endpoint solely supports DES.
- 3DES — Triple Data Encryption Standard (3DES) performs DES three times but varies the key size from 168 bits to 112 bits, and from 112 bits to 56 bits depending on the round of DES performed. 3DES is more secure than DES but less secure 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 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.
- AESGCM — AESGCM 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 — AESCCM is a generic authenticated encryption block cipher mode. CCM is well suited for use in compact software implementations.

Step 3. Choose the appropriate Integrity Algorithm from the *Integrity Algorithm* drop-down list. The algorithm will verify the integrity of the data. SHA2-256 is recommended as it is more secure than SHA-1 and MD5.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group: ☐ Enable

DH Group: Group 1(768 bit)

Select IKE Policy: testkey

View

The available options are defined as follows:

- 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, 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.
- MD5 — Message-Digest Algorithm 5 (MD5) uses a 128-bit hash value for authentication. MD5 is less secure, but faster than SHA-1 and SHA2-256.

Step 4. (Optional) To enable Perfect Forward Secrecy (PFS) to improve security, check the **Enable** checkbox in the *PFS Key Group* field. PFS creates an additional layer of security in protecting your data by ensuring a new DH key whenever a security association for the VPN connection is renegotiated. The process is done in case the previously generated DH key is compromised in transit. Skip to Step 6 if the *PFS Key Group* is not enabled.

Auto Policy Parameters

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: ☒ Enable

DH Group:

Select IKE Policy:

Step 5. (Optional) If Perfect Forward Secrecy is enabled in Step 4, choose the appropriate Diffie-Hellman key-exchange group from the *DH Group* field.

Auto Policy Parameters

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: ☐ Enable

DH Group:

Select IKE Policy:

Step 6. Choose the appropriate IKE Policy from the *Select IKE Policy* drop-down list.

Auto Policy Parameters

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: ☐ Enable

DH Group:

Select IKE Policy:

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

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

NetBios Enabled: ☐

Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Manual Encryption Algorithm:

Key-In:

Key-Out:

Manual Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: ☐ Enable

DH Group:

Select IKE Policy: