VPN Policy Configuration on RV180 and RV180W

Objectives

This document showcases the procedure to set the VPN Policies on the Cisco Small Business RV180 and RV180W VPN Firewall.

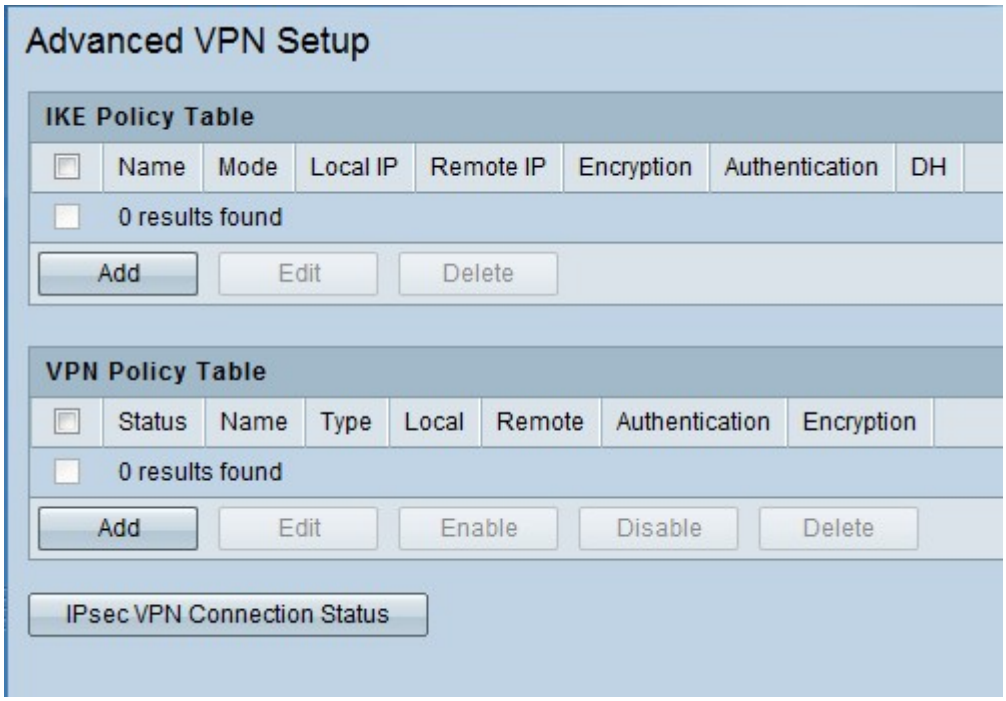
The VPN Policy features allow you to configure VPN settings for Automatic Policy, Manual Policy and the Encryption and Integrity Algorithms.

Applicable Devices

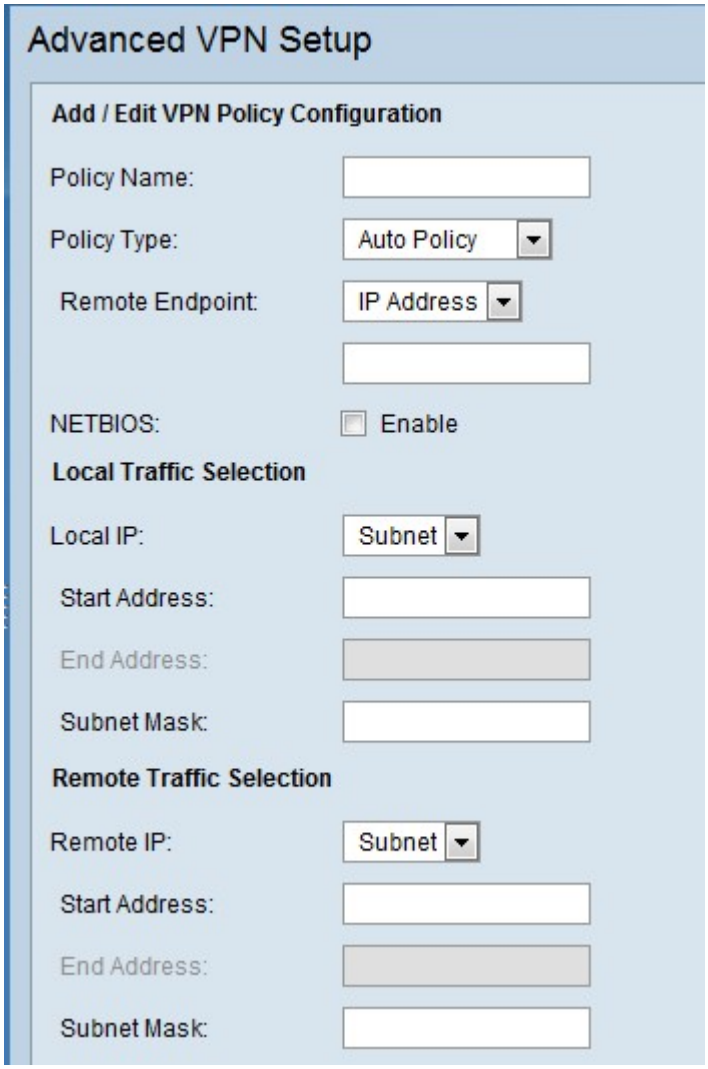
- RV180
- RV180W

VPN Policy Configuration

Step 1. Using Configuration Utility, choose **VPN > IPSec > Advanced VPN Setup**. The *Advanced VPN Setup* page opens.



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



Step 3. Enter a unique name is the Policy Name field for the policy to be set.

Step 4. Choose the appropriate policy type from the **Policy Type** drop-down list.

- Auto Policy — The parameters could be set automatically. In this case in addition to the policies it is required that the IKE(Internet Key Exchange) protocol negotiates between the two VPN Endpoints.

- Manual Policy — In this case all settings which include settings for keys for the VPN tunnel are manually input for each endpoint.

Step 5. Choose the type of IP identifier that would identify the gateway at the remote endpoint from the **Remote Endpoint** drop-down list.

- IP Address — IP address of the gateway on the remote endpoint.
- FQDN (Fully Qualified Domain Name) — Insert the Fully Qualified Domain Name of the gateway on the remore endpoint.

Step 6. To Enable NetBIOS broadcasts to travel across the VPN tunnel, check the **Enable** checkbox.

Local Traffic Selection and Remote Traffic Selection

Step 1. For both areas configure the following settings:

• Local/Remote IP — Choose the type of Identifier that you want to provide for the end point:

  • Any This specifies traffic is from given end point (local or remote). Both cannot be chosen.
  • Single This limits the policy to one host.Insert the IP address of the host that will be part of the VPN in Start IP address field.
  • Range This allows computers within the specified IP address range to connect to the VPN. Insert the Start IP Address and End IP Address in the appropriate fields.
  • Subnet This Allows computers within an IP address range to connect to the VPN. Insert the Start IP Address and End IP Address in the appropriate fields. Also insert the Subnet Mask of the network in the Subnet Mask field.

Split DNS

Split DNS allows the RV120W to acquire the DNS of the remote end point without going through the internet.

Step 1. To Enable Split DNS check the **Enable** check box.

Step 2. In the Domain Name Server 1 field, insert a Domain Name server IP address. This IP address would be used only to resolve the domain inserted in the Domain Name 1 field.

Step 3. In the Domain Name Server 2 field, insert a Domain Name server IP address. This IP address would be used only to resolve the domain inserted in the Domain Name 2 field.

Manual Policy Parameters

Step 1. Insert hexadecimal value between 3 and 8 in the SPI-Incoming and SPI-Outgoing fields.

Step 2. Choose the appropriate Encryption Algorithms from the **Encryption Algorithm** drop-down list.

Step 3. Insert hexadecimal value between 3 and 8 in the SPI-Incoming and SPI-Outgoing fields.

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

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

Step 6. Choose the appropriate Integrity Algorithm from the **Integrity Algorithm** drop-down list. This Algorithm will verify the integrity of the data.

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

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

Auto Policy Parameters

Step 1. In the SA Lifetime field enter duration of the security association. Choose the appropriate unit for SA Lifetime field in the drop-down list.

• Seconds — The default value is 3600 seconds. The minimum value is 300 seconds.
• Kbytes — After the specified value of Kbytes in this field the SA is renegotiated.The

minimum value is 1920000 KB.

Step 2. Choose the appropriate Encryption Algorithms from the **Encryption Algorithm** drop-down list.

Step 3. Choose the appropriate Integrity Algorithm from the **Integrity Algorithm** drop-down list. This Algorithm will verify the integrity of the data.

Step 4. To Enable Perfect Forward Secrecy to improve security , check the **Enable** checkbox. Choose the appropriate Diffie-Hellman key-exchange from the **PFS Key Group field.** drop-down list.

Step 5. Choose the appropriate IKE Policy from the **Select IKE Policy** drop-down list.