Basic Virtual Private Network (VPN) Configuration on the RV110W VPN Firewall

Objective

A Virtual Private Network (VPN) is a way to connect endpoints on different networks together over a public network, such as the Internet. This allows users who are away from a local network (such as an office) to securely connect to that network over the Internet. The *Basic VPN Setup* page helps you to set up a VPN tunnel for a Gateway to Gateway connection.

This article explains how to configure basic VPN on the RV110W VPN Firewall.

Applicable Device

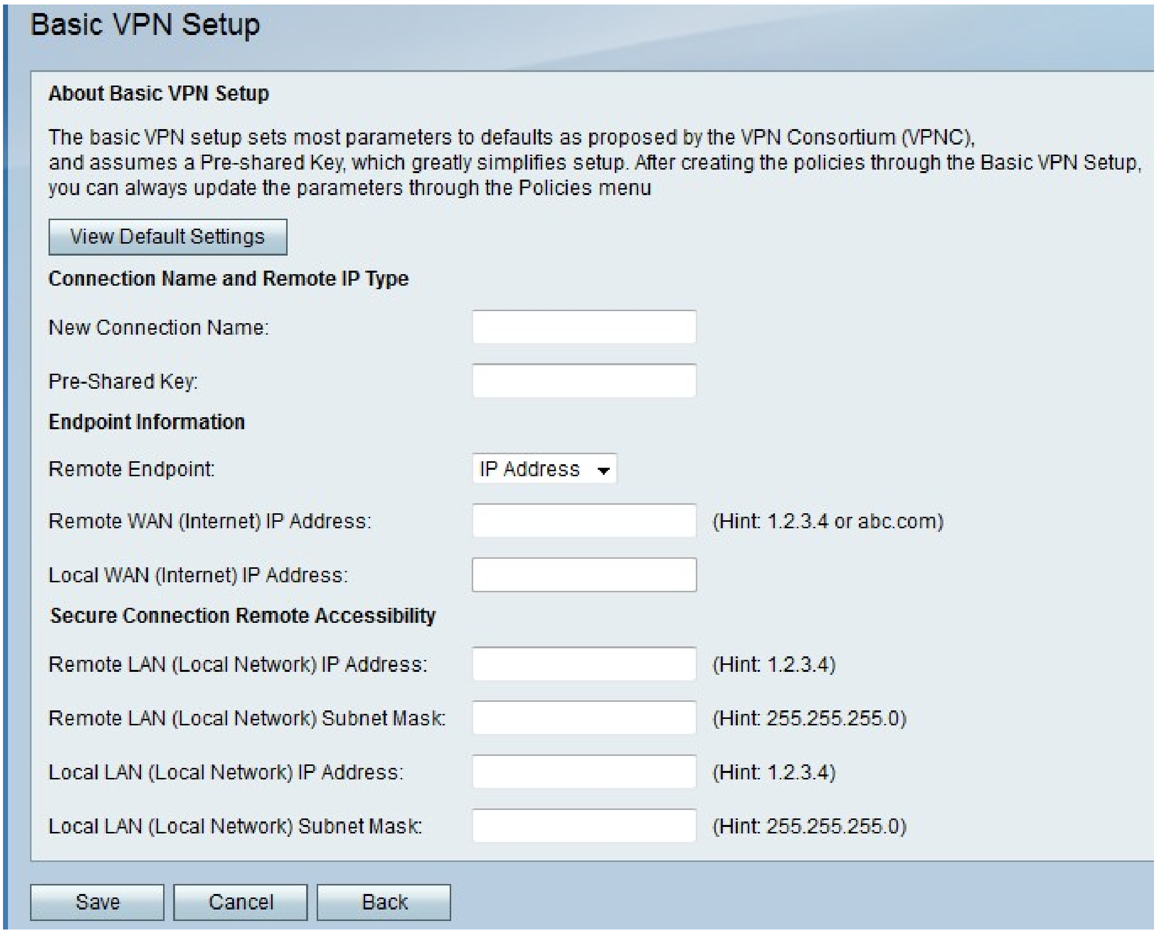
- RV110W

Software Version

- 1.2.0.9

Basic VPN Setup Configuration

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



About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup, you can always update the parameters through the Policies menu

Connection Name and Remote IP Type

New Connection Name:

Pre-Shared Key:

Endpoint Information

Remote Endpoint: IP Address

Remote WAN (Internet) IP Address: (Hint: 1.2.3.4 or abc.com)

Local WAN (Internet) IP Address:

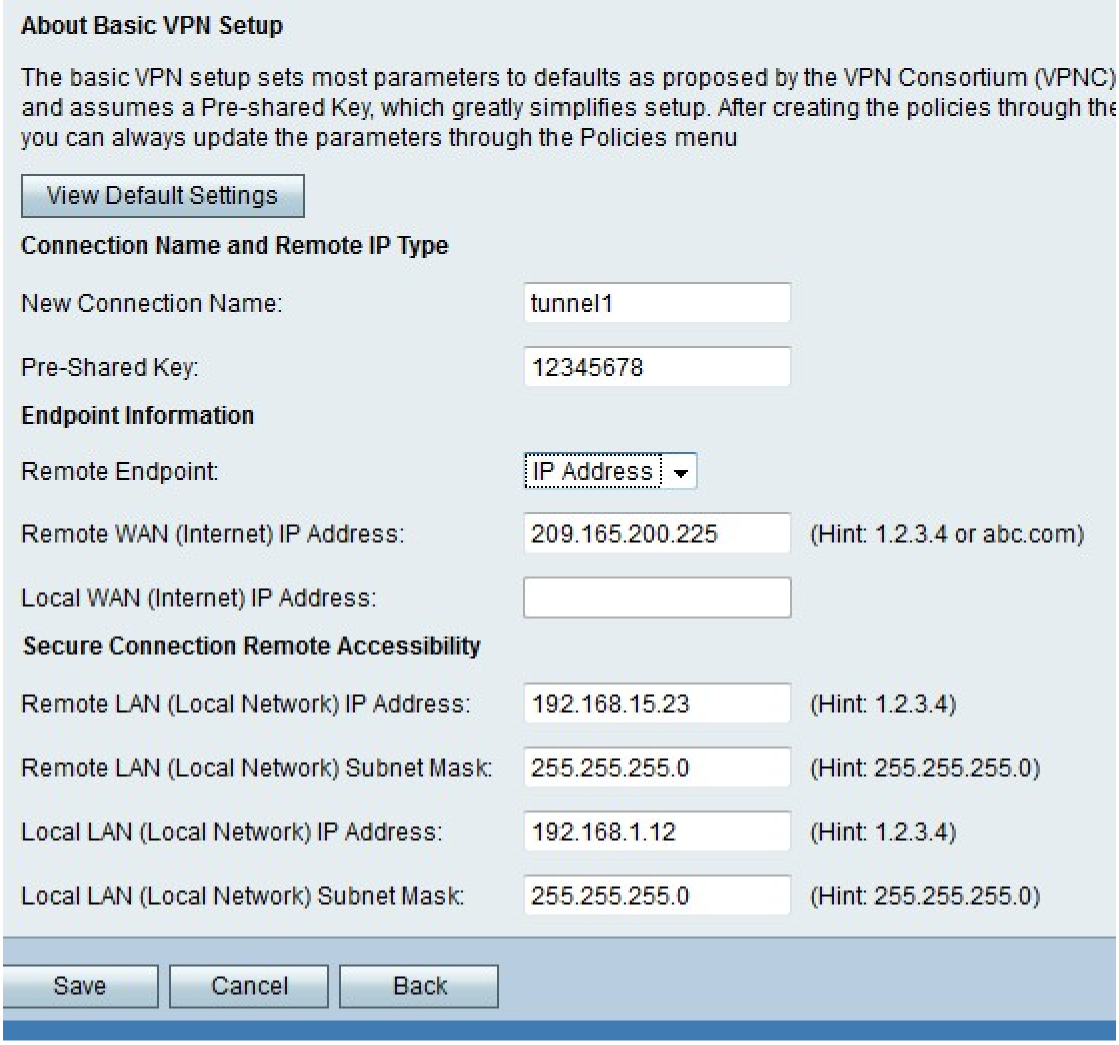
Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address: (Hint: 1.2.3.4)

Remote LAN (Local Network) Subnet Mask: (Hint: 255.255.255.0)

Local LAN (Local Network) IP Address: (Hint: 1.2.3.4)

Local LAN (Local Network) Subnet Mask: (Hint: 255.255.255.0)



About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC) and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the you can always update the parameters through the Policies menu

Connection Name and Remote IP Type

New Connection Name: tunnel1

Pre-Shared Key: 12345678

Endpoint Information

Remote Endpoint: IP Address

Remote WAN (Internet) IP Address: 209.165.200.225 (Hint: 1.2.3.4 or abc.com)

Local WAN (Internet) IP Address:

Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address: 192.168.15.23 (Hint: 1.2.3.4)

Remote LAN (Local Network) Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Local LAN (Local Network) IP Address: 192.168.1.12 (Hint: 1.2.3.4)

Local LAN (Local Network) Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Note: To review the basic settings of the VPN tunnel, click **View Default Settings**.

Step 2. Enter a name for the connection in the New Connection Name field. This name is used for management purposes.

Step 3. Enter a password in the Pre-Shared Key field. The VPN Client or remote gateway needs this key to establish a VPN connection. This key must have a length of at least 8 characters.

Step 4. Choose the type of end point for the VPN from the Remote Endpoint drop-down list. There are two possible endpoints:

- IP Address — The IP address will be used to identify the remote gateway.
- FQDN (Fully Qualified Domain Name) — The domain name is used to identify the remote gateway.

Step 5. Enter the IP Address or domain name of the remote gateway in the Remote WAN (Internet) IP Address field.

Step 6. Enter the IP Address or domain name of the local gateway in the Local WAN (Internet) IP Address field.

Step 7. Enter the remote IP address of the remote LAN in the Remote LAN (Local Network) IP Address field.

Step 8. Enter the remote subnet mask of the remote LAN in the Remote LAN (Local Network) Subnet Mask field.

Step 9. Enter the local IP address of the local LAN in the Local LAN (Local Network) IP Address field.

Note: The local IP of the remote LAN and the local IP of the local LAN should be in different subnets.

Step 10. Enter the local subnet mask of the local LAN in the Local LAN (Local Network) Subnet Mask field.

Step 11. Click **Save** to apply settings.