Quick Virtual Private Network (VPN) setup on RV220W and RV120W

Objectives

A Virtual Private Network (VPN) is a network that uses a public telecommunication infrastructure and their technology such as the Internet, to provide remote offices or individual users with secure access to their organization's network. Most VPN implementations use the Internet as the public infrastructure and a variety of specialized protocols to support private communications through the Internet. VPN follows a client and server approach. VPN clients authenticate users, encrypt data, and manage sessions with VPN servers using a technique called tunneling.

This document explains how to setup quick VPN on the RV220W and RV120W.

Note: Download the latest firmware from www.cisco.com and save it in your computer.

Applicable Devices

- RV120W
- RV220W

Software Download URL

https://www.cisco.com/cisco/software/release.html?mdfid=283118607&flowid=24581&softwareid=282465795&release=1.4.2.1&relind=AVAILABLE&rellifecycle=&reltype=latest

Software Version

- v1.0.4.17

Step-by-Step Procedure to Setup Quick Virtual Private Network

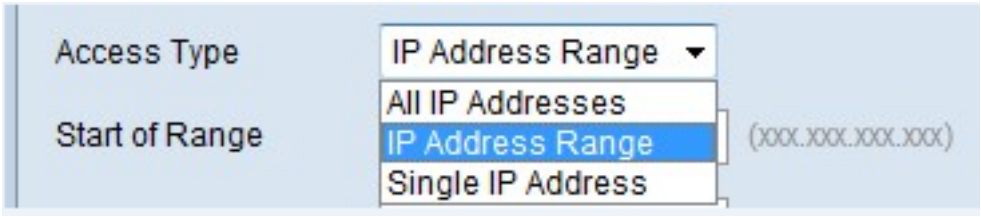
Enable Remote Management

Remote Management allows you to access and control the device without any physical connection to the actual unit. Enabling remote management allows you to access the device from a remote WAN network. The device manager is accessed from a computer on the LAN by using the device's LAN IP address and HTTP.

Step 1. Log in to the web configuration utility and choose **Administration > Remote Management**. The *Remote Management* page opens:

Step 2. Check the **Remote Management** check box to enable remote management.

Note: If this feature is not enabled, Cisco QuickVPN and SSL VPN access will not function.



Step 3. Choose the type of access to grant in the Access Type drop-down menu:

- All IP Addresses — Allows any IP address to access the device. User will have to change the default password before you choose this option.
- IP Address Range —Allows any IP address in the configured range to access the device. Enter the starting IP address for the allowed range in the Start of Range field. Enter the ending IP address for the allowed range in the End of Range field.
- Single IP Address — Restricts access to a device with a single IP address (for example, the computer you use to access the Device Manager). In the IP Address field, enter the IP Address of the PC to be given remote management permissions.

Step 4. Enter the port number used for the remote connection in the Port Number field. Port number 443 is set by default.

Note: If any other port number except 443 or 60443 is configured, Cisco QuickVPN will not function.

Step 5. Check the **Remote SNMP** check box to enable Simple Network Management Protocol (SNMP) and to be used remotely to manage the device.

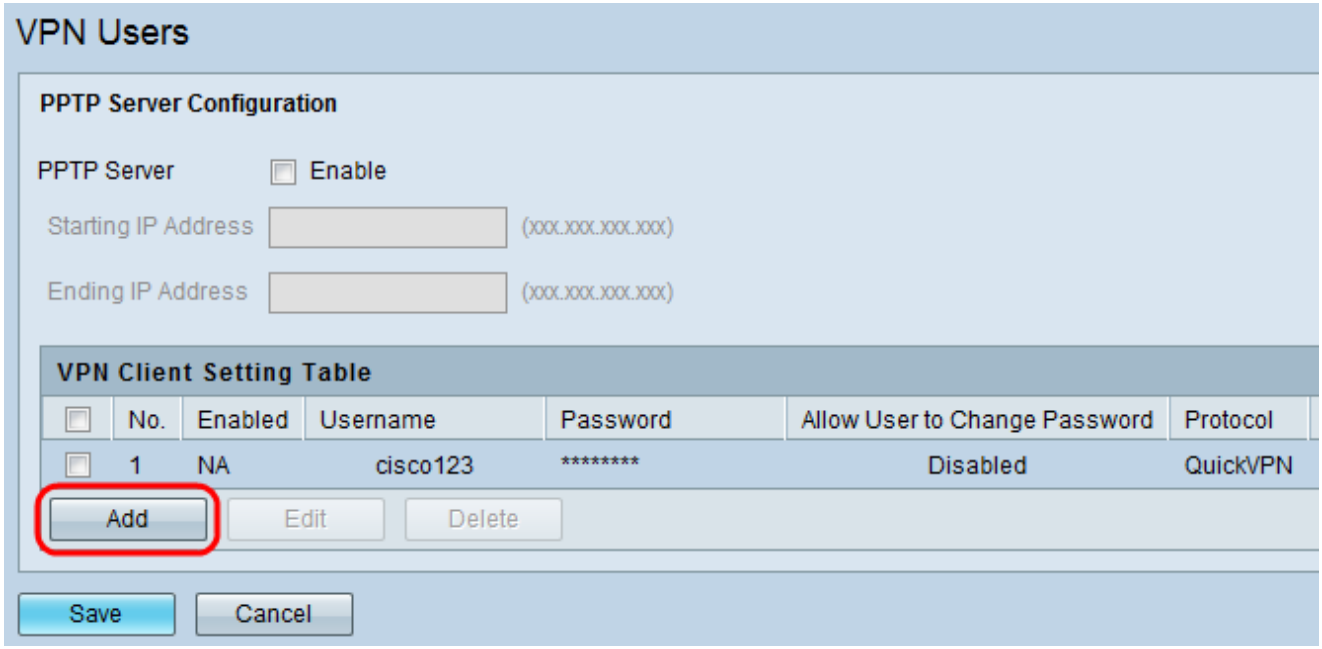
Step 6. Click **Save** to apply settings.

Note: When remote management is enabled, the device is accessible to anyone who knows its IP address. Since a malicious WAN user can reconfigure the device and misuse it in many ways, do change the administrator and any guest passwords before the feature is enabled.

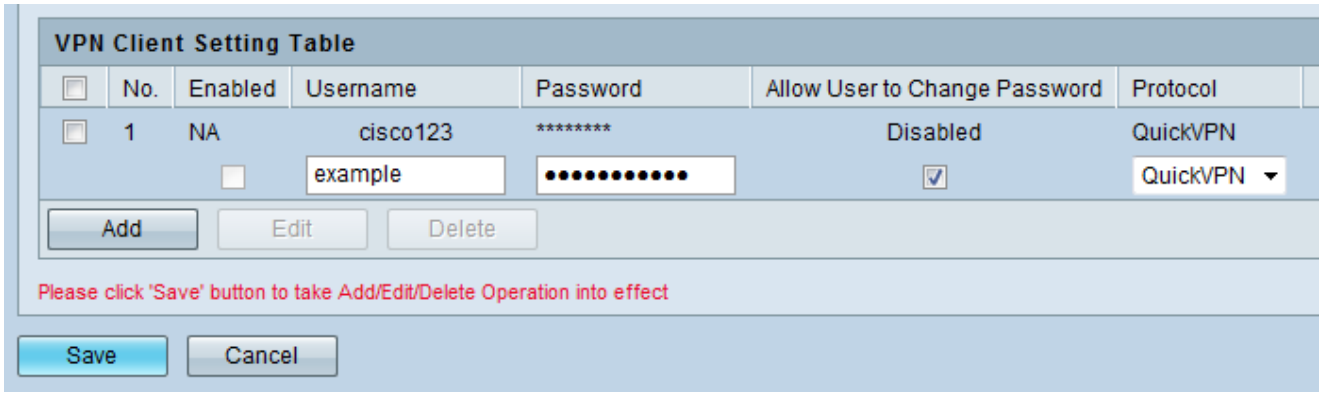
Internet Protocol Security (IPsec) Users Configuration

Internet Protocol Security (IPsec) is a protocol suite for securing IP communications by authentication and encryption of each IP packet of a communication session. IPsec also includes protocols for to establish mutual authentication between agents at the start of every session and negotiation of cryptographic keys to be used during the session.

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



Step 2. Click **Add** to add a client in the VPN Client Setting table.



Step 3. Enter the username or the unique identifier for the XAUTH user in the Username field.

Step 4. Enter password in the Password field.

Step 5. Check the **Allow User to Change Password** check box to allow the QuickVPN user to change this password.

Step 6. Choose the protocol type from the Protocol drop-down menu:

- QuickVPN — Allows a remote user to access the device from any other LAN connection knowing device's IP address.
- PPTP —Allows Point-to-Point Tunneling Protocol to access the device remotely.
- XAUTH — Allows authentication of users with methods in addition to authentication

method mentioned in IKE SA parameters. XAUTH has to be configured in one the following modes:

– NOne — This mode disables XAUTH.

– IPsec Host— Router is authenticated by a remote gateway with a username and password combination. In this particular mode, router acts as a VPN Client of remote gateway.

– User Database — This mode user account created in the router are used to authenticate the users.