Firewall Configuration on the RV315W VPN Router

Objective

A firewall builds a bridge between a secure internal network and an insecure external network. The firewall controls the incoming and outgoing network traffic analysis of data packets. This article explains how to block different features such as proxy, cookies, etc, on the RV315W VPN Router.

Applicable Device

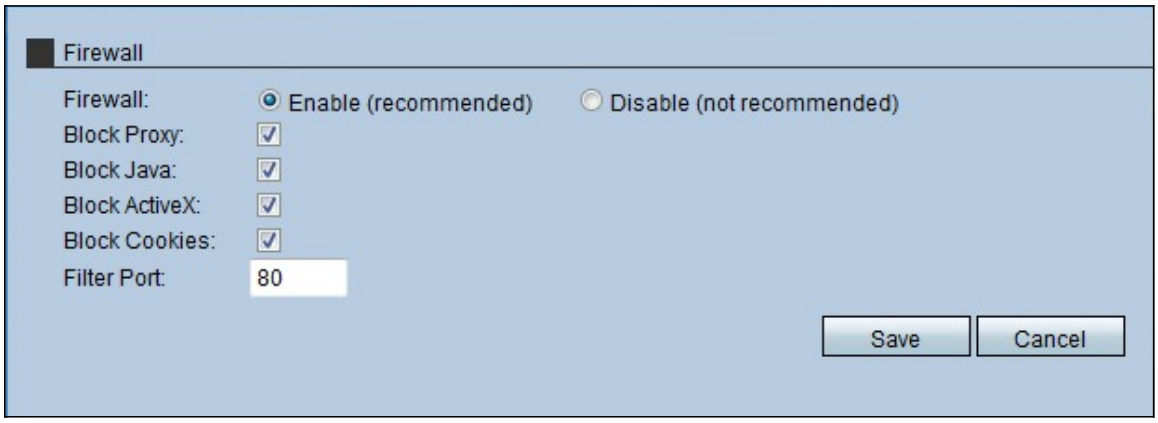
- RV315W

Software Version

- 1.01.03

Firewall Configuration

Step 1. Log in to the web configuration utility and choose **Security > Firewall**. The *Firewall* page opens:



Step 2. Click the **Enable** radio button to enable the firewall features on the RV315W.

Note: Steps 3 to 7 are optional steps.

Step 3. Check the **Block Proxy** check box to block the proxy on the device. Proxy servers are servers that provide a link between two separate networks. Malicious proxy servers can record any unencrypted data that is sent to them such as logins or passwords.

Step 4. Check the **Block Java** check box to block the java applets from being downloaded. Java is a common programming language used by many websites. However, java applets that are made for malicious intent can pose a security threat to a network. Once downloaded, a hostile java applet can exploit network resources.

Step 5. Check the **Block ActiveX** check box to block the ActiveX applications from being downloaded. ActiveX is a type of applet that is used by many websites. Though generally

safe, once a malicious ActiveX applet is installed on a computer, it can do anything a user can do. It may insert harmful code into the operating system, surf a secure intranet, change a password, or retrieve and send documents.

Step 6. Check the **Block Cookies** check box to block the Cookies applications from being downloaded. Cookies are created by websites to store information about users. Cookies can track the web history of the user which may lead to an invasion of privacy.

Step 7. Enter the port number that the device uses to filter the HTTP traffic in the Filter Port field. This traffic control is only done to the HTTP traffic. HyperText Transfer Protocol (HTTP) is used to access and distribute information on the Internet through the use of the connection that the server and host establish.

Step 8. Click **Save** to save the changes made in the firewall configuration.