# Basic Firewall Settings Configuration on RV215W

## Objective

A firewall is a set of features designed to keep a network secure. A router is considered a strong hardware firewall. This is due to the fact that routers are able to inspect all inbound traffic and drop any unwanted packets.

This article explains how to configure basic firewall settings on the RV215W.

## Applicable Devices

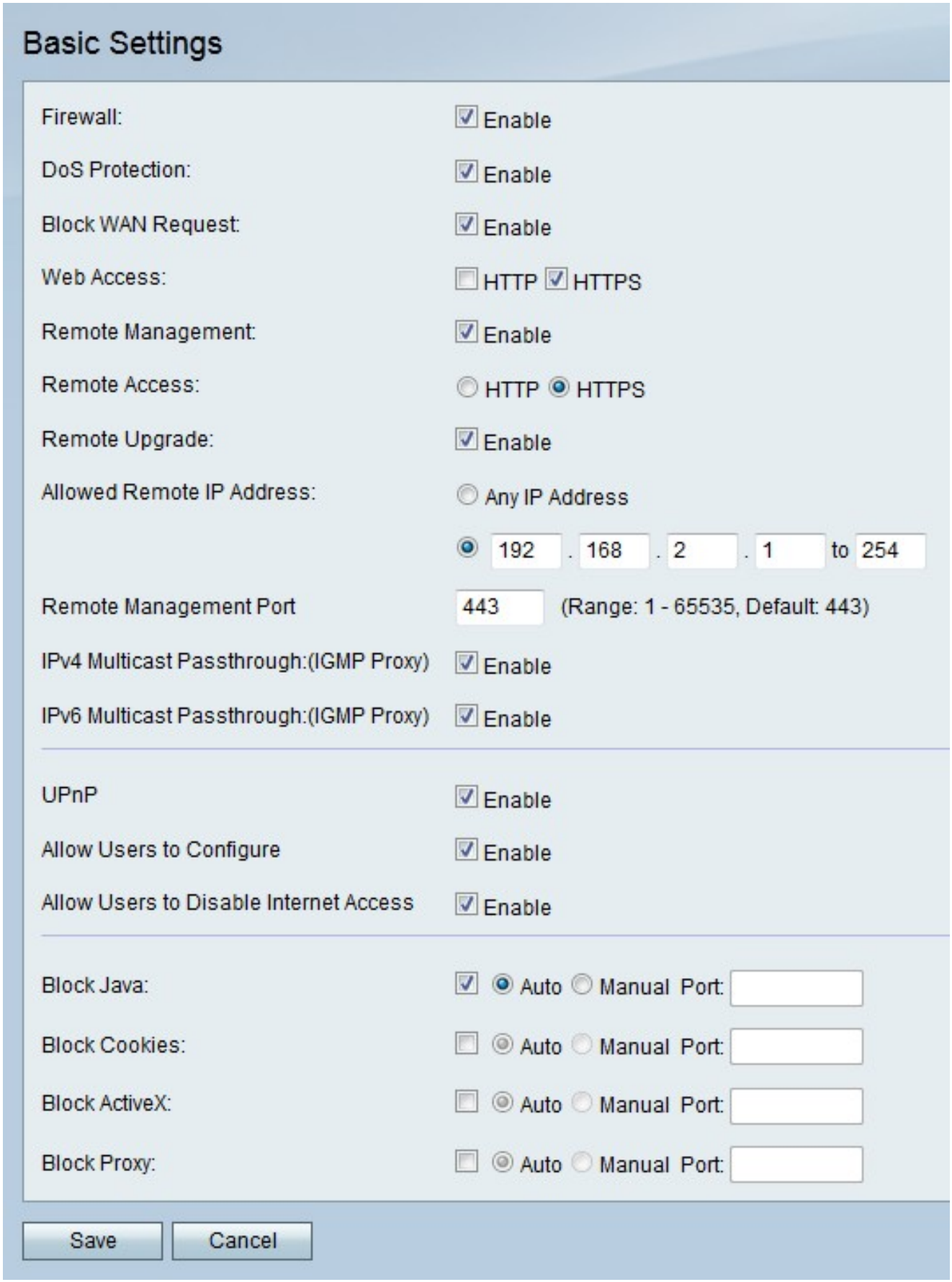
- RV215W

## Software Version

- 1.1.0.5

## Basic Settings

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




Step 2. Check **Enable** in the Firewall field to enable firewall configuration on the RV215W.

Step 3. Check **Enable** in the DoS Protection field to enable Denial of Service (DoS) protection on the RV215W. DoS protection is used to prevent a network from a Distributed Denial of Service (DDoS) attack. DDoS attacks are meant to flood a network to the point where the resources of the network become unavailable. The RV215W uses DoS protection

to protect the network through the restriction and removal of unwanted packets.

Step 4. Check **Enable** in the Block WAN Request field to block all ping requests to the RV215W from the WAN.

Step 5. Check the check box that corresponds to the desired type of web access that can be used to connect to the firewall in the Web Access field.

Step 6. Check **Enable** in the Remote Management field. Remote management allows access of the RV215W from a remote WAN network.

Step 7. Click the radio button that corresponds to the desired type of web access that can be used to connect to the firewall from the remote WAN in the Remote Access field.

Step 8. Check **Remote Upgrade** to allow remote users to upgrade the RV215W.

Step 9. Click the radio button that corresponds to the desired IP addresses that are allowed to access the RV215W remotely in the Allowed Remote IP Address field.

- Any IP Address — All IP addresses are allowed.
- IP Address — Enter a range of IP addresses that are allowed.

Step 10. Enter a port on which remote access is allowed in the Remote Management Port field. A remote user must use the remote port to access the device.

**Note:** The format for remote access is https://<*remote-ip*>:<*remote-port*>

Step 11. Check **Enable** in the IPv4 Multicast Passthrough field to allow IPv4 multicast traffic to come through the RV215W from the internet. IP multicast is a method that is used to send IP datagrams to a designated group of receivers in a single transmission.

Step 12. Check **Enable** in the IPv6 Multicast Passthrough field to allow IPv6 multicast traffic to come through the RV215W from the internet.

Step 13. Check **Enable** in the UPnP field to enable Universal Plug and Play (UPnP). UPnP allows for automatic discovery of devices that can communicate with the RV215W.

Step 14. Check **Enable** in the Allows Users to Configure field to allow users with UPnP capable devices to configure UPnP port-mapping rules. Port-mapping or port forwarding is used to permit communications between external hosts and services provided within a private LAN.

Step 15. Check **Enable** in the Allow Users to Disable Internet Access field to allow users to disable internet access to the device.

Step 16. Check **Block Java** to block java applets from being downloaded. 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. Click the radio button that corresponds to the desired block method.

- Auto — Automatically blocks java.
- Manual Port — Enter a specific port on which to block java.

Step 17. Check **Block Cookies** to filter out cookies from being created by a website.

Cookies are created by websites to store information of these users. Cookies can track the web history of the user which may lead to an invasion of privacy. Click the radio button that corresponds to the desired block method.

- Auto — Automatically block cookies.
- Manual Port — Enter a specific port on which to block cookies.

Step 18. Check **Block ActiveX** to block ActiveX applets from being downloaded. ActiveX is a type of applet that lacks security. Once an 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. Click the radio button that corresponds to the desired block method.

- Auto — Automatically block ActiveX.
- Manual Port — Enter a specific port on which to block ActiveX.

Step 19. Check **Block Proxy** to block proxy servers. 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. Click the radio button that corresponds to the desired block method.

- Auto — Automatically block proxy servers.
- Manual Port — Enter a specific port on which to block proxy servers.

Step 20. Click **Save**.