Firewall Logs on the RV315W VPN Router

Objective

A log is a set of messages that describes system events. Logs provide an administrator an alert when a feature is does not operate correctly, which allows the administrator to take action. One of the Logs that the RV315W can generate is a firewall log. A firewall builds a bridge between a secure internal network and an insecure external network and controls the incoming and outgoing network traffic analysis of the data packets.This article explains how to configure firewall logs on the RV315W VPN Router.

The following articles contain more information for system logging on the RV315W.

- To view the logs locally on the RV315W, refer to the *View Logs on the RV315W VPN Router* article.
- To configure which logs are generated on the RV315W, refer *to* the *Log Facilities on the RV315W VPN Router* article.
- To configure the log settings for local, USB, email, and syslog storage; refer to the *Log Settings on the RV315W VPN Router* article.

Applicable Device

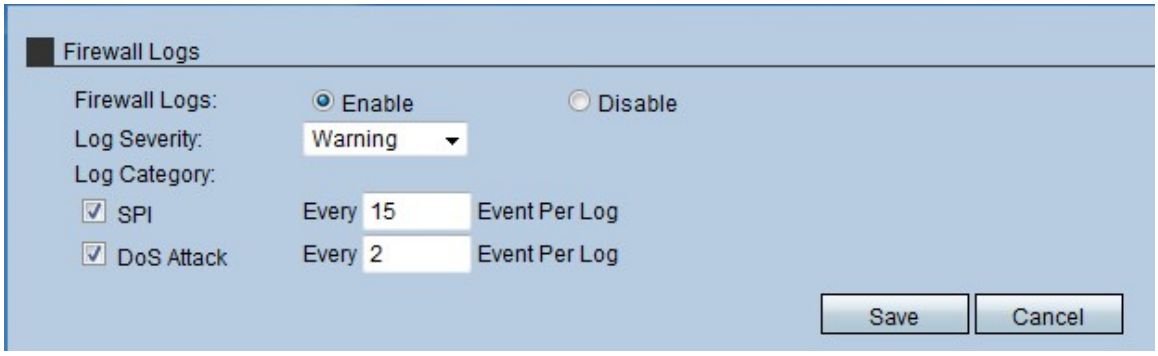
- RV315W

Software Version

- 1.01.03

Firewall Logs

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



Step 2. In the Firewall Logs field, click the **Enable** radio button to allow the RV315W to generate firewall logs.

Step 3. From the Log Severity drop-down list, choose the level of severity of the RV315W generated logs. The list is ordered from highest severity to lowest severity:

- Emergency — Generates a Log when the firewall in the device has an emergency because an attack has taken place.

- Critical — Generates a Log when the firewall in the device is in a critical condition because an attack has taken place.

- Error — Generates a Log when the firewall in the device has an error.

- Warning — Generates a Log when the firewall in the device has detected a possible problem.

- Notification — Sends a Log when the firewall in the device has an notification of the status.

- Information — Sends a Log about the status of the firewall in the device.

- Debugging — Generates a Log in the device to analyze and solve potential problems that the firewall can have.

Note: When the level of severity is chosen from the drop-down list, the administrator receives the log that are generated for that event plus events that have higher severity in the list. For example, when Error is chosen, the RV315W creates logs for Error, Critical, and Emergency.

Step 4. Check the check box of the log category that the RV315W has to create a log from the Log Category area. There are two possible categories:

- SPI — Enter the quantity of events that have to be recorded per log for each SPI log category. System Packet Interface (SPI) is used to send packets through a specific channel. This distribution uses different frames and interfaces.

- DoS Attack — Enter the quantity of events that have to be recorded per log for each DoS Attack log category. Denial of Service (DOS) is used to protect 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 becomes unavailable.

Step 5. Click **Save**.