Denial of Service (DoS) Protection Configuration on the RV315W VPN Router

Objective

Denial of Service (DoS) protection increases network security through the prevention of packets with certain IP addresses from entering the network. DoS is used to stop Distributed Denial of Service (DDoS) attacks. DDoS attacks flood the network with additional requests that limit the availability of network resources. DoS protection detects these attacks and eliminates packets with content of malicious intent. This article explains how to configure DoS Protection on the RV315W VPN Router.

Applicable Device

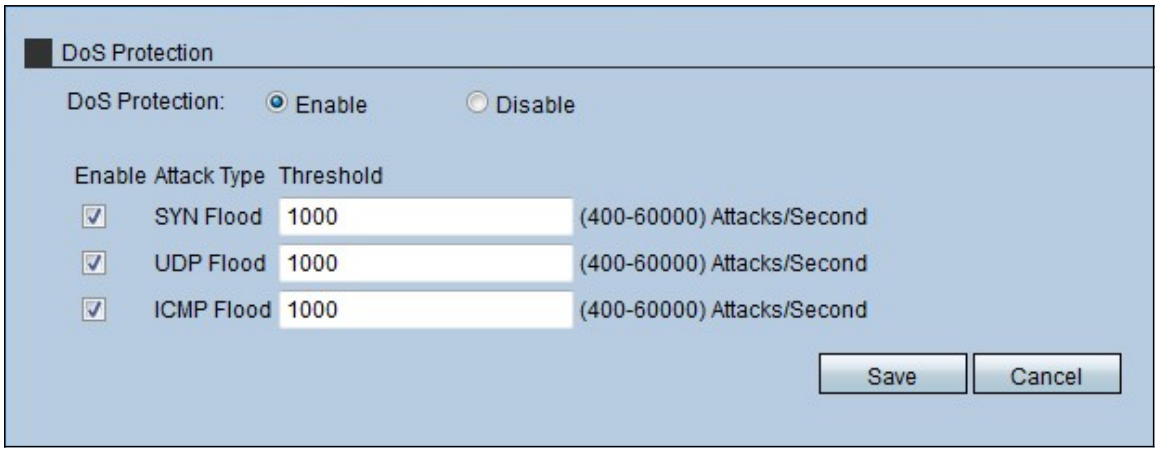
- RV315W

Software Version

- 1.01.03

Denial of Service Protection

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



Step 2. Click the **Enable** radio button to enable DoS protection on the RV315W.

Step 3. (Optional) Check the check box of the type of attack that the DoS protection prevents on the RV315W. There are three types of attacks:

- SYN Flood — Enter the maximum quantity of; SYN flood attacks that the RV315W has to suffer before DoS protection works in the SYN Flood field. The SYN Flood Attack occurs when the attacker sends a large quantity of SYN messages to the device in order to disable legitimate traffic on the device.

- UDP Flood — Enter the maximum quantity of UDP flood attacks that the RV315W has to suffer before DoS protection works in the UDP Flood field. The User Datagram Protocol

(UDP) Flood Attack occurs when the attacker send a large quantity of UDP packets to random ports on the device. As a result, the device denies access for legitimate traffic and allows access for malicious data that can damage the network.

• ICMP Flood — Enter the maximum quantity of ICMP flood attacks that the RV315W has to suffer before DoS protection works in the UDP Flood field. An Internet Control Management Protocol (ICMP) Flood Attack occurs when the attacker send a large quantity of IP addresses to the device which look like insecure host but in reality are secure. For this reason, the device denies access of those host to the network and allows the connection of new IP host that the attacker can send.

Step 4. Click **Save**.