Configure Attack Prevention Security Features on RV120W and RV220W

Objective

A firewall is mainly used to shield resources of a private network from the users of other networks. Firewalls use a set of programs in the network to perform all operations. Generally, attacks on the network prevent a routers functionality and therefore attack prevention in a firewall is used.

This document explains how to configure attack prevention features on the RV120W and RV220W.

Applicable Devices

- RV120W
- RV220W

Software Version

- v1.0.4.17

Enable Attack Prevention Features

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

Step 2. The user can check the appropriate check boxes to enable the security features which are required. The security features are given below:

- Respond to Ping on WAN (Internet)
- Stealth Mode
- Flood
- Block UDP Flood
- Block Anonymous ICMP Messages
- Block Fragmented Packets
- Block Multicast Packets

Step 2. The user can check the appropriate check boxes to enable the security features which are required. The security features are given below:
• Respond to Ping on WAN (Internet) — This is used to configure the router so it allows the Internet Control Message Protocol (ICMP) ping request on a WAN interface. This feature is the main tool used to solve connectivity problems.

• Stealth Mode — This makes the operations in router secretive and thereby it causes the router not to respond to the port scans from the WAN. Port scans are sometimes done by attackers to find the running services on the host in order to make it liable to danger. If the user enables this feature, it makes the network less prone to discovery and attacks. This feature is enabled by default.

• Flood — This is enabled in order to prevent the flood caused by invalid Transmission Control Protocol (TCP) packets. If this feature is enabled, the router drops all invalid TCP packets. By this it prevents the SYN flood attack, where SYN is a synchronized packet in TCP. A SYN flood attack is an attack in which the attacker sends requests to make the server unresponsive to logical traffic. This feature is enabled by default.

• Block UDP Flood — This is enabled by default so that the router does not accept more than 25 simultaneous, active User Datagram Protocol (UDP) connections from one computer on the LAN. This feature is enabled by default.

• Block Anonymous ICMP Messages — This allows the firewall to secretly block an application and does not send the ICMP alert to the sender which is a feature required by the International Computer Security Association (ICSA). There are some protocols which require ICMP alerts like the Maximum Transmission Unit (MTU) Path Discovery. The user can enable this setting to operate in “stealth” mode. This feature is enabled by default.

• Block Fragmented Packets — This enables the firewall to block the fragmented packets which are needed for the ICSA. This feature is enabled by default.

• Block Multicast Packets — This enables the firewall to block multicast packets which is a feature needed by the ICSA. This feature is enabled by default.

Step 3. Click **Save** to apply all settings.