Application Level Gateway Configuration on RV315W VPN Routers

Objective

When a device behind the router uses an application for which the router has Application-Level Gateway (ALG) service enabled, the router translates the private IP address of the device inside the data stream to a public IP address. It also records session port numbers and dynamically creates implicit NAT port forwarding for that application traffic to come in from the WAN to the LAN, Application Level Gateway (ALG) allows certain NAT incompatible applications to operate properly. A Denial of Service (DoS) atack is when an attacker floods a website with traffic, limiting the websites ability to function. This article explains how to configure DoS Protection on the RV315W VPN Router.

Applicable Device

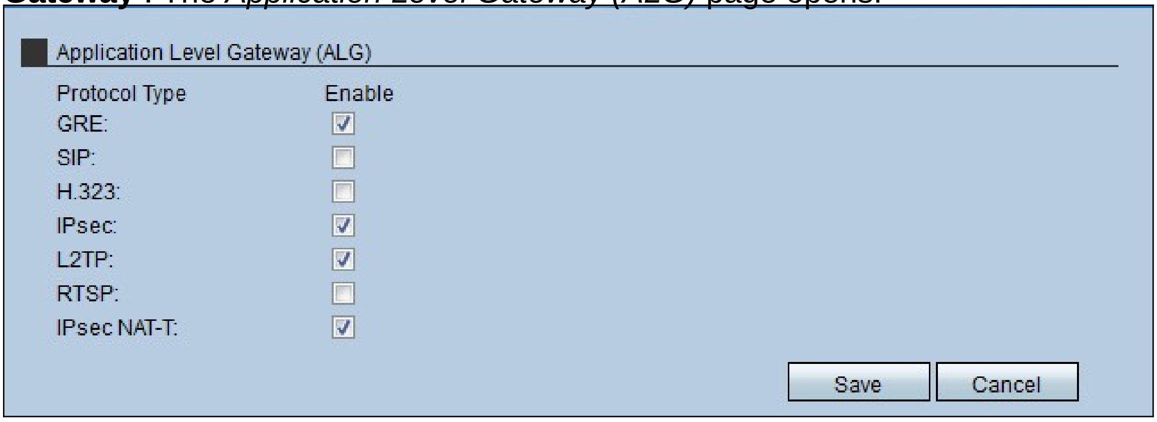
- RV315W

Software Version

- 1.01.03

Application Level Gateway

Step 1. Log in to the web configuration utility and choose **Security >Application Level Gateway** . The *Application Level Gateway (ALG)* page opens:



Application Level Gateway (ALG)

Protocol Type	Enable
GRE:	☑
SIP:	☐
H.323:	☐
IPsec:	☑
L2TP:	☑
RTSP:	☐
IPsec NAT-T:	☑

Step 2. Check the **Enable** check box of the Protocol type that the RV315W uses to level the gateway. The possible protocols are:

- GRE — Generic Routing Encapsulation (GRE) is a protocol that encapsulates the information when the data uses a gateway connection (point to point) and is sent over IP networks.
- SIP — The Session Initiation Protocol (SIP) is an application layer control (signaling) protocol that handles the set up, modification, and tear down of voice and multimedia sessions over the Internet. Enable the SIP ALG when voice devices such as UC500, UC300, or SIP phones are connected to the network behind the router.
- H.323 — A standard teleconferencing protocol suite that provides audio, data, and video

conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service.
- IPsec — Internet Protocol Security (IPsec) is used to authenticate and encrypt IP packets. This protocol is very useful because it assures the protection of the data that is sent to a host.
- L2TP — Layer 2 Tunneling Protocol (L2TP) is a protocol used by service providers that allows a point to point connection, but with the application of layer 2 for security.
- RTSP — Real Time Streaming Protocol (RTSP) is a protocol that controls and manage the traffic of media in a gateway (point to point), this feature allows the user to control the media in real time.
- IPsec NAT-T — Is the combination of IPsec and NAT that implies that the packet is sent with the IPsec protocol but creates, at the same time, datagrams for the Network Address Translation (NAT) that are encrypted to enhance the security level.

Step 3. Click **Save**.