Configuración de Application Level Gateway en Routers VPN RV315W

Objetivo

Cuando un dispositivo detrás del router utiliza una aplicación para la que el router tiene activado el servicio Application-Level Gateway (ALG), el router traduce la dirección IP privada del dispositivo dentro del flujo de datos a una dirección IP pública. También registra los números de puerto de sesión y crea de forma dinámica el reenvío de puertos NAT implícito para que el tráfico de la aplicación entre la WAN y la LAN, la puerta de enlace de nivel de aplicación (ALG) permite que ciertas aplicaciones incompatibles con NAT funcionen correctamente. Un ataque de denegación de servicio (DoS) se produce cuando un atacante inunda un sitio web con tráfico, lo que limita la capacidad de los sitios web para funcionar. En este artículo se explica cómo configurar la protección DoS en el router VPN RV315W.

Dispositivo aplicable

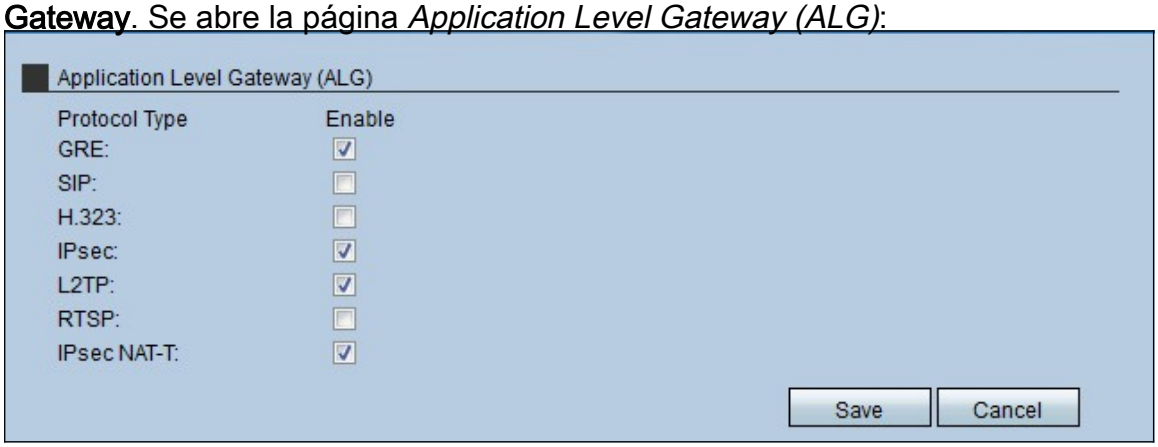
·RV315W

Versión del software

•1.01.03

Gateway del Nivel de Aplicación

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > Application Level Gateway**. Se abre la página *Application Level Gateway (ALG)*:



Paso 2. Marque la casilla de verificación **Enable** del tipo de protocolo que el RV315W utiliza para nivelar la gateway. Los protocolos posibles son:

·GRE: Generic Routing Encapsulation (GRE) es un protocolo que encapsula la información cuando los datos utilizan una conexión de gateway (punto a punto) y se envían a través de redes IP.
· SIP: el protocolo de inicio de sesión (SIP) es un protocolo de control de capa de aplicación (señalización) que gestiona la configuración, modificación y eliminación de sesiones de voz y multimedia a través de Internet. Habilite el ALG SIP cuando los dispositivos de voz como UC500, UC300 o teléfonos SIP estén conectados a la red detrás

del router.
· H.323: Conjunto de protocolos de teleconferencia estándar que proporciona audio, datos y videoconferencias. Permite la comunicación en tiempo real punto a punto y multipunto entre equipos cliente a través de una red basada en paquetes que no proporciona una calidad de servicio garantizada.
· IPSec: la seguridad de protocolo de Internet (IPsec) se utiliza para autenticar y cifrar paquetes IP. Este protocolo es muy útil porque asegura la protección de los datos que se envían a un host.
· L2TP: el protocolo de túnel de capa 2 (L2TP) es un protocolo utilizado por los proveedores de servicios que permite una conexión punto a punto, pero con la aplicación de la capa 2 para la seguridad.
· RTSP: protocolo de transmisión en tiempo real (RTSP) es un protocolo que controla y gestiona el tráfico de medios en una gateway (punto a punto), esta función permite al usuario controlar los medios en tiempo real.
· IPsec NAT-T: es la combinación de IPsec y NAT que implica que el paquete se envía con el protocolo IPsec pero crea, al mismo tiempo, datagramas para la traducción de direcciones de red (NAT) que se cifran para mejorar el nivel de seguridad.

Paso 3. Click **Save**.