Configuration de passerelle de niveau application sur des routeurs VPN RV315W

Objectif

Quand un périphérique derrière le routeur utilise une application pour laquelle le routeur prend le service activé de la passerelle de niveau application (ALG), le routeur traduit l'adresse IP privée du périphérique à l'intérieur du flux de données à une adresse IP publique. Il enregistre également des numéros de port de session et crée dynamiquement la transmission du port NAT implicite pour que ce trafic de l'application entre du WAN au RÉSEAU LOCAL, la passerelle de niveau application (ALG) permet à certaines applications incompatibles NAT pour fonctionner correctement. Un atack du Déni de service (DOS) est quand un attaquant inonde un site Web avec le trafic, limitant la capacité de sites Web de fonctionner. Cet article explique comment configurer la protection DOS sur le routeur VPN RV315W.

Périphérique applicable

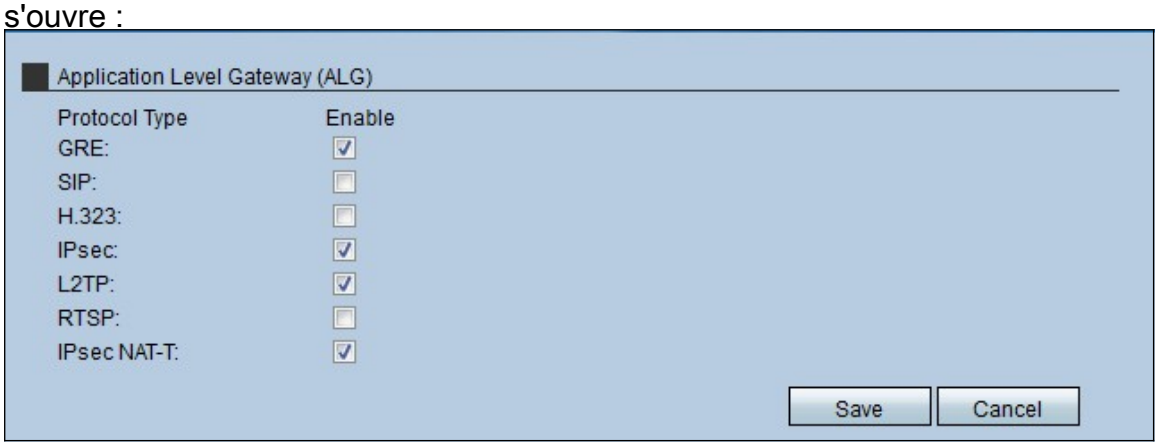
• RV315W

Version de logiciel

• 1.01.03

Passerelle de niveau application

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **passerelle de niveau de >Application de Sécurité**. La page de la *passerelle de niveau application (ALG)* s'ouvre :



Étape 2. Cochez la case d'**enable du** type de Protocol que le RV315W l'utilise pour niveler la passerelle. Les protocoles possibles sont :

• GRE — L'Encapsulation de routage générique (GRE) est un protocole qui encapsule les informations quand les données utilisent une connexion de passerelle (point par point) et est envoyé au-dessus des réseaux IP.
• SIP — Le Protocole SIP (Session Initiation Protocol) est un protocole de contrôle de couche application (signalisation) qui manipule l'installation, modification, et démolit des

sessions de Voix et de multimédia au-dessus de l'Internet. Activez le SIP ALG quand des périphériques vocaux tels qu'UC500, UC300, ou téléphones SIP sont connectés au réseau derrière le routeur.
• H.323 — Une suite de protocole standard de téléconférence qui fournit l'audio, les données, et la vidéoconférence. Il tient compte du Point à point en temps réel et de la transmission multipoint entre les ordinateurs client au-dessus d'un réseau paquet paquet qui ne fournit pas une qualité de service garantie.
• IPsec — L'IPSec (IPsec) est utilisé pour authentifier et chiffrer des paquets IP. Ce protocole est très utile parce qu'il assure la protection des données qui sont envoyées à un hôte.
• L2TP — Le Layer 2 Tunneling Protocol (L2TP) est un protocole utilisé par des fournisseurs de services qui permet une connexion point par point, mais avec l'application d'une couche 2 pour la Sécurité.
• RTSP — Le Protocole RTSP (Real-Time Streaming Protocol) est un protocole que les contrôles et gèrent le trafic des medias dans une passerelle (point par point), cette caractéristique permet à l'utilisateur pour contrôler les medias en temps réel.
• IPsec NAT-T — Est la combinaison d'IPsec et la NAT qui implique que le paquet est envoyé avec le protocole IPsec mais crée, en même temps, les datagrammes pour le Traduction d'adresses de réseau (NAT) qui sont chiffrés pour améliorer le niveau de Sécurité.

Étape 3. **Sauvegarde de** clic.