Configuratie van toepassingsniveau gateway voor RV315W VPN-routers

Doel

Wanneer een apparaat achter de router een toepassing gebruikt waarvoor de router de dienst van de Gateway (ALG) van het Toepassingsniveau heeft ingeschakeld, vertaalt de router het privé IP-adres van het apparaat in de gegevensstroom naar een openbaar IP-adres. Het registreert ook sessiepoortnummers en maakt dynamisch impliciet NAT poorttransport voor dat toepassingsverkeer om van WAN naar LAN in te schakelen, laat Application Level Gateway (ALG) bepaalde NAT onverenigbare toepassingen toe om correct te werken. Een aanval op Denial of Service (DoS) is wanneer een aanvaller een website met verkeer overspoelt, waardoor de mogelijkheid van websites om te functioneren wordt beperkt. Dit artikel legt uit hoe u de DoS Protection op de RV315W VPN-router kunt configureren.

Toepassbaar apparaat

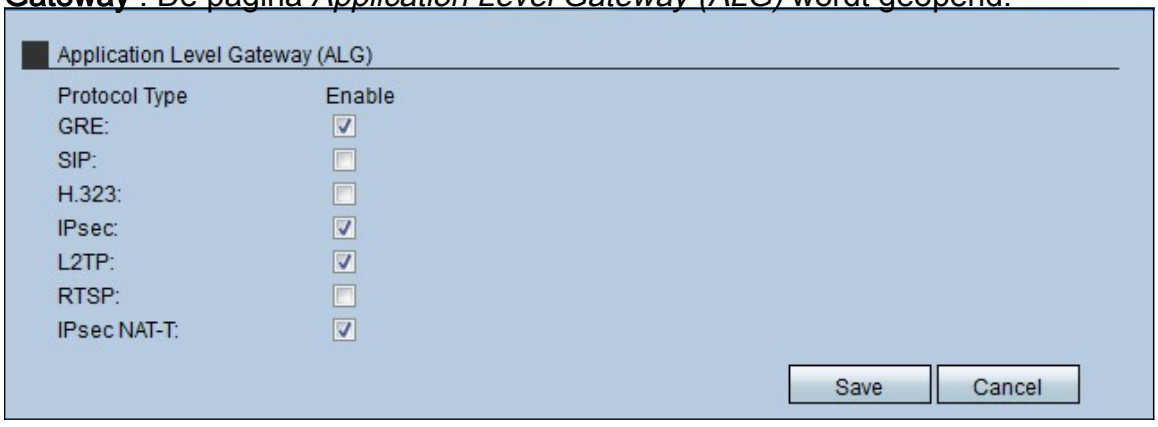
- RV315W

Softwareversie

•1.01.03

Gateway voor toepassingsniveau

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security >Application Level Gateway** . De pagina *Application Level Gateway (ALG)* wordt geopend:



Stap 2. Controleer het aanvinkvakje **Enable** van het protocoltype dat de RV315W gebruikt om de gateway waterpas te stellen. De mogelijke protocollen zijn:

- GRE — Generic Routing Encapsulation (GRE) is een protocol dat de informatie inkapselt wanneer de gegevens een poortverbinding gebruiken (point to point) en via IP-netwerken wordt verzonden.
- SIP — Het Session Initiation Protocol (SIP) is een protocol voor Application Layer Control (signalering) dat betrekking heeft op het instellen, wijzigen en afbreken van spraak- en multimedia-sessies via het internet. Schakel het SIP ALG in wanneer spraakapparaten

zoals UC500, UC300 of SIP-telefoons op het netwerk achter de router zijn aangesloten.

- H.323 — Een standaard teleconferentieprotocolreeks die audio-, gegevens- en videoconferencing-software biedt. Het staat voor point-to-point en multipoint communicatie tussen clientcomputers toe via een pakketgebaseerd netwerk dat geen gegarandeerde kwaliteit van de service biedt.
- IPsec - Internet Protocol Security (IPsec) wordt gebruikt om IP-pakketten te bevestigen en te versleutelen. Dit protocol is zeer nuttig omdat het de bescherming garandeert van de gegevens die naar een host worden verzonden.
- L2TP — Layer 2 Tunneling Protocol (L2TP) is een protocol dat door serviceproviders wordt gebruikt en dat een punt toestaat om een verbinding te richten, maar met de toepassing van Layer 2 voor beveiliging.
- RTSP — Real Time Streaming Protocol (RTSP) is een protocol dat het verkeer van media in een gateway (punt naar punt) controleert en beheert, zodat de gebruiker de media in real time kan besturen.
- IPsec NAT-T — is de combinatie van IPsec en NAT die impliceert dat het pakket met het IPsec-protocol wordt verzonden maar tegelijkertijd datagrammen voor de Network Address Translation (NAT) maakt die versleuteld zijn om het beveiligingsniveau te verbeteren.

Stap 3. Klik op **Opslaan**.