Quality-of-Service (DoS) Protection-configuratie op de RV315W VPN-router

Doel

Bescherming tegen IP-adres (Denial of Service) verhoogt de netwerkbeveiliging door te voorkomen dat pakketten met bepaalde IP-adressen het netwerk binnendringen. DoS wordt gebruikt om de aanvallen van Distributed Denial of Service (DDoS) te stoppen. De aanvallen van DDoS overspoelen het netwerk met extra verzoeken die de beschikbaarheid van netwerkmiddelen beperken. Bescherm de partij deze aanvallen en elimineert pakketten met inhoud van kwaadwillige bedoeling. Dit artikel legt uit hoe u de DoS Protection op de RV315W VPN-router kunt configureren.

Toepassbaar apparaat

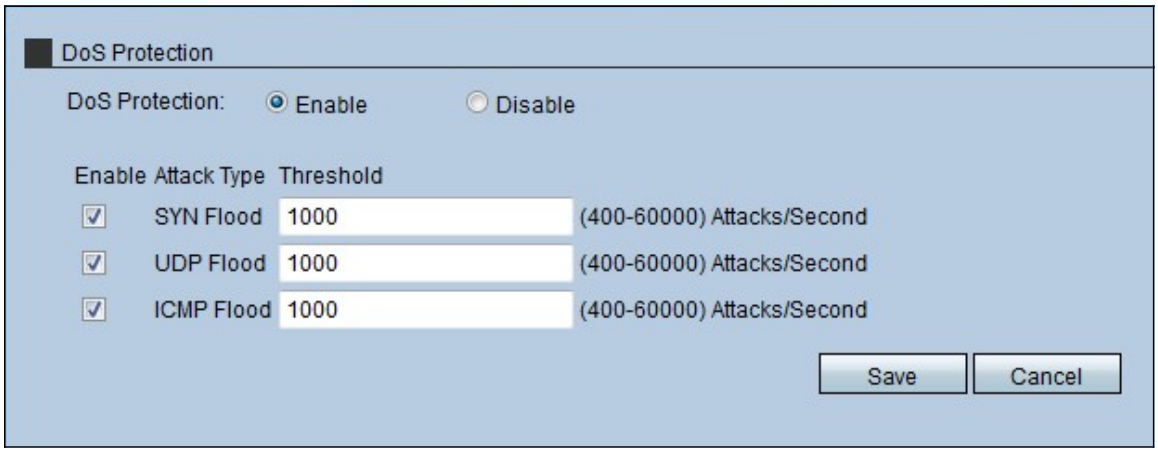
- RV315W

Softwareversie

•1.01.03

Servicebescherming weigeren

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > DoS Protection**. De pagina *DoS Protection* wordt geopend:



Stap 2. Klik op de radioknop **Enable** om DoS-bescherming in te schakelen op de RV315W.

Stap 3. (Optioneel) Controleer het aankruisvakje van het type aanval dat door de DoS-beveiliging op de RV315W wordt voorkomen. Er zijn drie soorten aanvallen:

- SYN-overstroming — Voer de maximumhoeveelheid in van: SYN-aanvallen op overstromingen die de RV315W moeten ondergaan voordat de DoS-bescherming in het SYN-veld werkt. De SYN-overstroming doet zich voor wanneer de aanvaller een grote hoeveelheid SYN-berichten naar het apparaat stuurt om legitiem verkeer op het apparaat uit te schakelen.

- UDP-overstromingen — Voer de maximale hoeveelheid UDP-overstromingen in die de RV315W moet lijden voordat de DoS-bescherming op het UDP-gebied werkt. De User Datagram Protocol (UDP) Vloeraanval geschiedt wanneer de aanvaller een grote hoeveelheid UDP-pakketten naar willekeurige poorten op het apparaat stuurt. Als resultaat hiervan ontkent het apparaat toegang voor legaal verkeer en verleent toegang voor kwaadwillige gegevens die het netwerk kunnen beschadigen.

- ICMP Flood — Voer de maximale hoeveelheid ICMP-overstromingsaanvallen in die de RV315W moet ondergaan voordat DoS-bescherming in het UDP-veld Flood werkt. Een ICMP-Overslag (Internet Control Management Protocol) doet zich voor wanneer de aanvaller een grote hoeveelheid IP-adressen naar het apparaat stuurt die er op onveilige host lijken maar in werkelijkheid veilig zijn. Om deze reden, ontkent het apparaat de toegang van die gastheer tot het netwerk en staat de verbinding van nieuwe IP gastheer toe die de aanslagpleger kan verzenden.

Stap 4. Klik op **Opslaan**.