Konfiguration des DoS-Schutzes (Denial of Service) auf dem RV315W VPN-Router

Ziel

Der Denial of Service (DoS)-Schutz erhöht die Netzwerksicherheit, indem verhindert wird, dass Pakete mit bestimmten IP-Adressen in das Netzwerk gelangen. DoS wird verwendet, um DDoS-Angriffe (Distributed Denial of Service) zu stoppen. DDoS-Angriffe überschwemmen das Netzwerk mit zusätzlichen Anfragen, die die Verfügbarkeit von Netzwerkressourcen einschränken. Beim DoS-Schutz werden diese Angriffe erkannt und Pakete mit böswilligen Absichten entfernt. In diesem Artikel wird erläutert, wie der DoS-Schutz auf dem RV315W VPN-Router konfiguriert wird.

Anwendbares Gerät

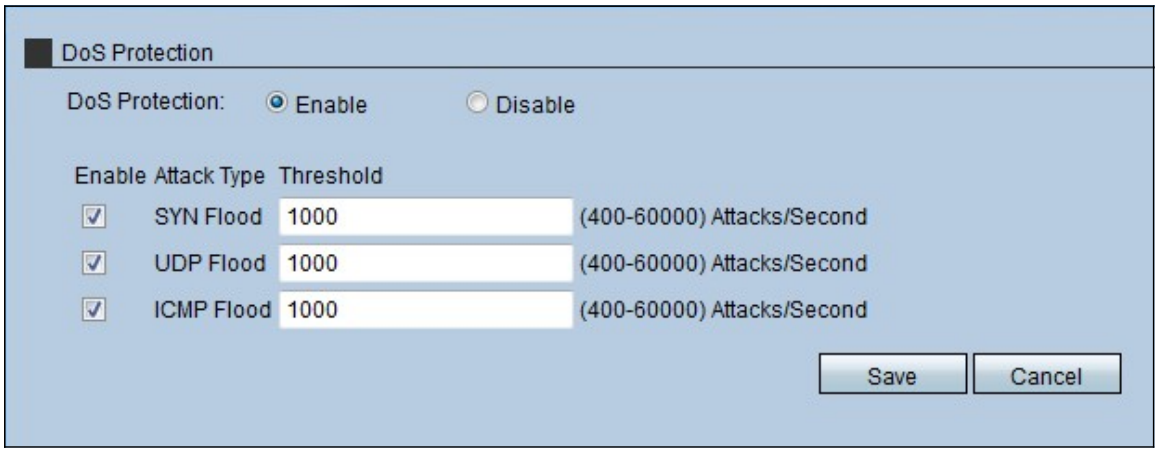
RV315W

Softwareversion

·1.01.03

Denial of Service Protection

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > DoS Protection aus**. Die Seite *DoS-Schutz* wird geöffnet:



Schritt 2: Klicken Sie auf das Optionsfeld **Aktivieren**, um den DoS-Schutz auf der RV315W zu aktivieren.

Schritt 3: (Optional) Aktivieren Sie das Kontrollkästchen der Art des Angriffs, der durch den DoS-Schutz auf der RV315W verhindert wird. Es gibt drei Arten von Angriffen:

·SYN Flood - Geben Sie die maximale Menge von ein. SYN-Flood-Angriffe, die der RV315W erleiden muss, bevor der DoS-Schutz im SYN Flood-Feld funktioniert. Der SYN Flood-Angriff wird durchgeführt, wenn der Angreifer eine große Anzahl von SYN-Nachrichten an das Gerät sendet, um legitimen Datenverkehr auf dem Gerät zu deaktivieren.

·UDP Flood - Geben Sie die maximale Anzahl von UDP-Flood-Angriffen ein, die der RV315W erleiden muss, bevor der DoS-Schutz im UDP-Flood-Bereich funktioniert. Der UDP-Flood-Angriff (User Datagram Protocol) wird ausgelöst, wenn der Angreifer eine große Anzahl von UDP-Paketen an beliebige Ports auf dem Gerät sendet. Daher verweigert das Gerät den Zugriff für legitimen Datenverkehr und ermöglicht den Zugriff auf schädliche Daten, die das Netzwerk beschädigen können.

·ICMP Flood - Geben Sie die maximale Anzahl an ICMP-Flood-Angriffen ein, die der RV315W erleiden muss, bevor der DoS-Schutz im UDP-Flood-Feld funktioniert. Ein ICMP-Flood-Angriff (Internet Control Management Protocol) tritt auf, wenn der Angreifer eine große Anzahl von IP-Adressen an das Gerät sendet, die wie unsicherer Host aussehen, aber in Wirklichkeit sicher sind. Aus diesem Grund verweigert das Gerät den Zugriff dieser Hosts auf das Netzwerk und ermöglicht die Verbindung eines neuen IP-Hosts, den der Angreifer senden kann.

Schritt 4: Klicken Sie auf **Speichern**.