Configuration de la protection contre les dénis de service (DoS) sur le routeur VPN RV315W

Objectif

La protection par déni de service (DoS) augmente la sécurité du réseau en empêchant les paquets avec certaines adresses IP d'entrer dans le réseau. Le déni de service (DoS) est utilisé pour arrêter les attaques par déni de service distribué (DDoS). Les attaques DDoS inondent le réseau de demandes supplémentaires qui limitent la disponibilité des ressources réseau. La protection DoS détecte ces attaques et élimine les paquets contenant des intentions malveillantes. Cet article explique comment configurer la protection DoS sur le routeur VPN RV315W.

Périphérique applicable

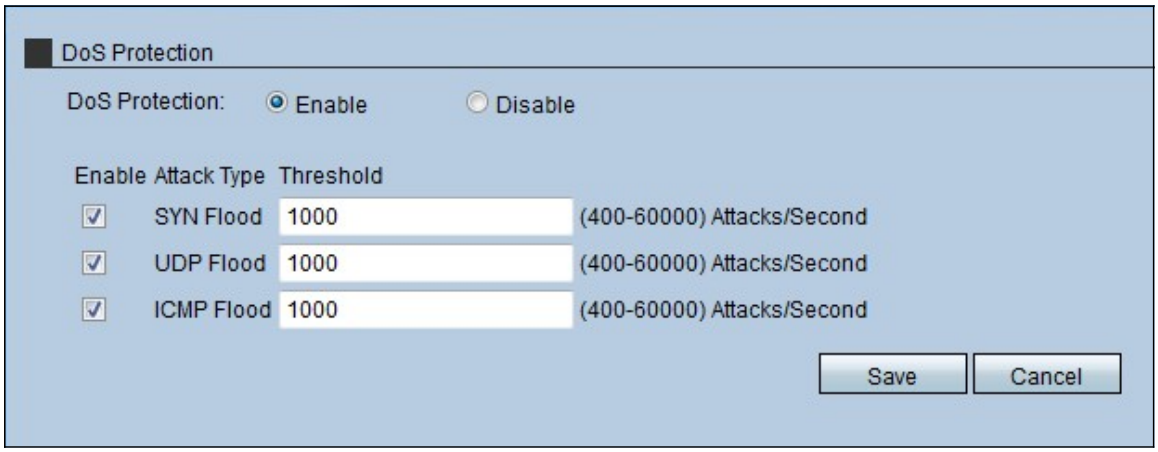
·RV315W

Version du logiciel

•1.01.03

Protection contre le déni de service

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > DoS Protection**. La page *DoS Protection* s'ouvre :



Étape 2. Cliquez sur la case d'option **Enable** pour activer la protection DoS sur le RV315W.

Étape 3. (Facultatif) Cochez la case du type d'attaque que la protection DoS empêche sur le RV315W. Il existe trois types d'attaques :

·SYN Flood : saisissez la quantité maximale de ; Attaques par inondation SYN que le RV315W doit subir avant que la protection DoS ne fonctionne dans le champ Inondation SYN. L'attaque par inondation SYN se produit lorsque le pirate envoie une grande quantité de messages SYN au périphérique afin de désactiver le trafic légitime sur le périphérique.

·UDP Flood : saisissez la quantité maximale d'attaques UDP que le RV315W doit subir

avant que la protection DoS ne fonctionne dans le champ UDP Flood. L'attaque par inondation UDP (User Datagram Protocol) se produit lorsque le pirate envoie une grande quantité de paquets UDP à des ports aléatoires sur le périphérique. Par conséquent, le périphérique refuse l'accès au trafic légitime et autorise l'accès aux données malveillantes susceptibles d'endommager le réseau.

·ICMP Flood : saisissez la quantité maximale d'attaques par inondation ICMP que le RV315W doit subir avant que la protection DoS ne fonctionne dans le champ UDP Flood. Une attaque par inondation ICMP (Internet Control Management Protocol) se produit lorsque le pirate envoie une grande quantité d'adresses IP au périphérique qui ressemble à un hôte non sécurisé mais qui sont en réalité sécurisées. Pour cette raison, le périphérique refuse l’accès de ces hôtes au réseau et autorise la connexion d’un nouvel hôte IP que le pirate peut envoyer.

Étape 4. Click **Save**.