Configurazione della protezione DoS (Denial of Service) sul router VPN RV315W

Obiettivo

La protezione DoS (Denial of Service) aumenta la sicurezza della rete impedendo l'ingresso nella rete di pacchetti con determinati indirizzi IP. DoS viene utilizzato per arrestare gli attacchi Distributed Denial of Service (DDoS). Gli attacchi DDoS inondano la rete con ulteriori richieste che limitano la disponibilità delle risorse di rete. La protezione DoS rileva questi attacchi ed elimina i pacchetti con contenuto intenzionale. Questo articolo spiega come configurare la protezione DoS sul router VPN RV315W.

Dispositivo applicabile

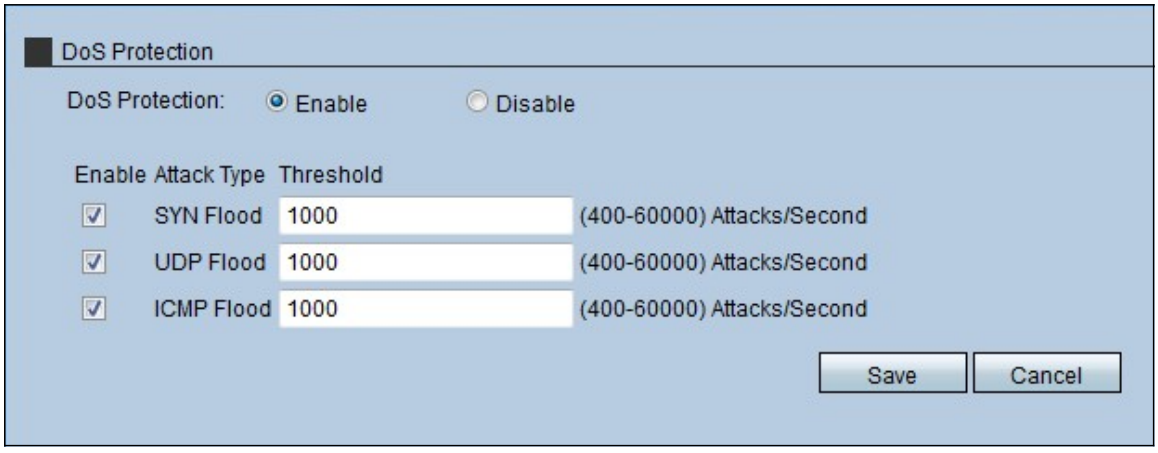
RV315W

Versione del software

•1.01.03

Protezione da Denial of Service

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Protezione DoS**. Viene visualizzata la pagina *Protezione DoS*:



Passaggio 2. Fare clic sul pulsante di opzione **Enable** (Abilita) per abilitare la protezione DoS sull'RV315W.

Passaggio 3. (Facoltativo) Selezionare la casella di controllo relativa al tipo di attacco che la protezione DoS impedisce all'RV315W. Esistono tre tipi di attacchi:

·SYN Flood - Immettere la quantità massima di; SYN flood attacca la RV315W prima che la protezione DoS funzioni nel campo SYN Flood. L'attacco SYN Flood si verifica quando l'autore dell'attacco invia una grande quantità di messaggi SYN al dispositivo per disabilitare il traffico legittimo sul dispositivo.

·UDP Flood: immettere la quantità massima di attacchi di tipo flood UDP che la RV315W

deve subire prima che la protezione DoS funzioni nel campo UDP Flood. L'attacco Flood UDP (User Datagram Protocol) si verifica quando l'utente malintenzionato invia una grande quantità di pacchetti UDP a porte casuali sul dispositivo. Di conseguenza, il dispositivo nega l'accesso per il traffico legittimo e consente l'accesso per i dati dannosi che possono danneggiare la rete.

·ICMP Flood: immettere la quantità massima di attacchi Flood ICMP che la RV315W deve subire prima che la protezione DoS funzioni nel campo UDP Flood. L'attacco Flood del protocollo ICMP (Internet Control Management Protocol) si verifica quando l'utente malintenzionato invia al dispositivo una grande quantità di indirizzi IP che, pur apparendo come host non sicuro, in realtà sono sicuri. Per questo motivo, il dispositivo nega l'accesso di tali host alla rete e consente la connessione di un nuovo host IP che l'utente non autorizzato può inviare.

Passaggio 4. Fare clic su **Salva**.