RV315W VPN路由器上的拒絕服務(DoS)保護配置

目標

阻斷服務(DoS)保護通過防止具有特定IP地址的資料包進入網路提高了網路安全性。DoS用於阻止分散式拒絕服務(DDoS)攻擊。DDoS攻擊會向網路傳送大量請求，從而限制網路資源的可用性。DoS保護可以檢測這些攻擊，並消除包含惡意內容的資料包。本文說明如何在RV315W VPN路由器上配置DoS保護。

適用的裝置

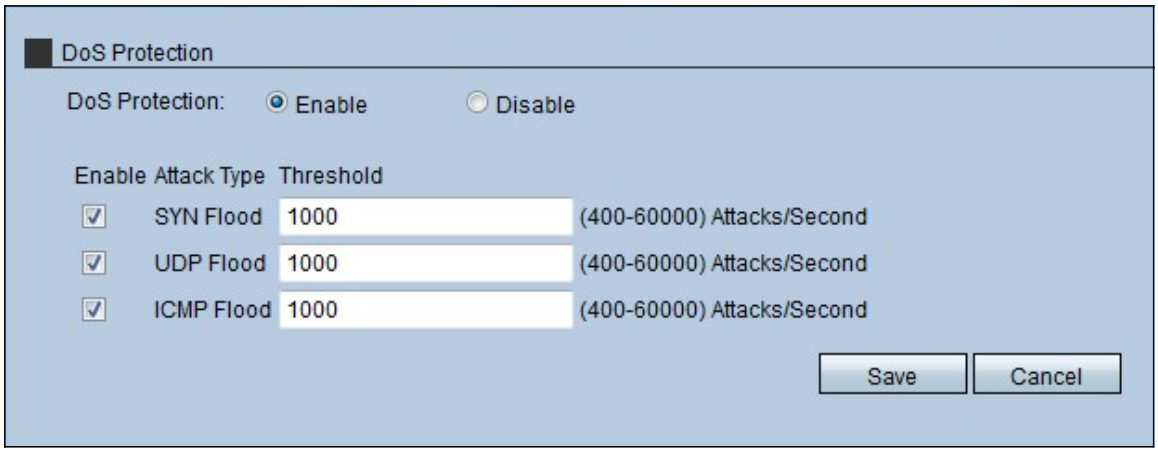
·RV315W

軟體版本

•1.01.03

拒絕服務保護

步驟1.登入到Web配置實用程式並選擇**Security > DoS Protection**。將打*開DoS Protection*頁面：



步驟2.按一下**Enable**單選按鈕在RV315W上啟用DoS保護。

步驟3.（可選）選中DoS保護在RV315W上阻止的攻擊型別的覈取方塊。有三種型別的攻擊：

·SYN泛洪 — 輸入最大數量；在SYN Flood（SYN泛洪）欄位中，RV315W在DoS保護工作之前必須遭受的SYN泛洪攻擊。當攻擊者向裝置傳送大量SYN消息以禁用裝置上的合法流量時，就會發生SYN泛洪攻擊。

·UDP泛洪 — 在「UDP泛洪」欄位中輸入RV315W在DoS保護工作之前必須遭受的最大UDP泛洪攻擊數量。使用者資料包協定(UDP)泛洪攻擊是指攻擊者向裝置上的隨機埠傳送大量UDP資料包。結果，裝置拒絕訪問合法流量，並允許訪問可能損壞網路的惡意資料。

·ICMP泛洪 — 在「UDP泛洪」欄位中輸入RV315W在DoS保護工作之前必須遭受的最大ICMP泛洪攻擊數量。當攻擊者向裝置傳送大量IP地址時，就會發生網際網路控制管理協定

(ICMP)泛洪攻擊，這些地址看起來是不安全的主機但實際上是安全的。因此，裝置拒絕這些主機訪問網路，並允許連線攻擊者可以傳送的新IP主機。

步驟4.按一下「Save」。