RV315W VPNルータのサービス拒否(DoS)保護設定

目的

Denial of Service（DoS；サービス拒否）保護は、特定のIPアドレスを持つパケットがネットワークに入るのを防ぐことによって、ネットワークセキュリティを強化します。DoSは、Distributed Denial of Service(DDoS)攻撃を阻止するために使用されます。DDoS攻撃は、ネットワークリソースの可用性を制限する追加の要求でネットワークをフラッディングします。DoS保護はこれらの攻撃を検出し、悪意のあるコンテンツを含むパケットを排除します。この記事では、RV315W VPNルータでDoS保護を設定する方法について説明します。

該当するデバイス

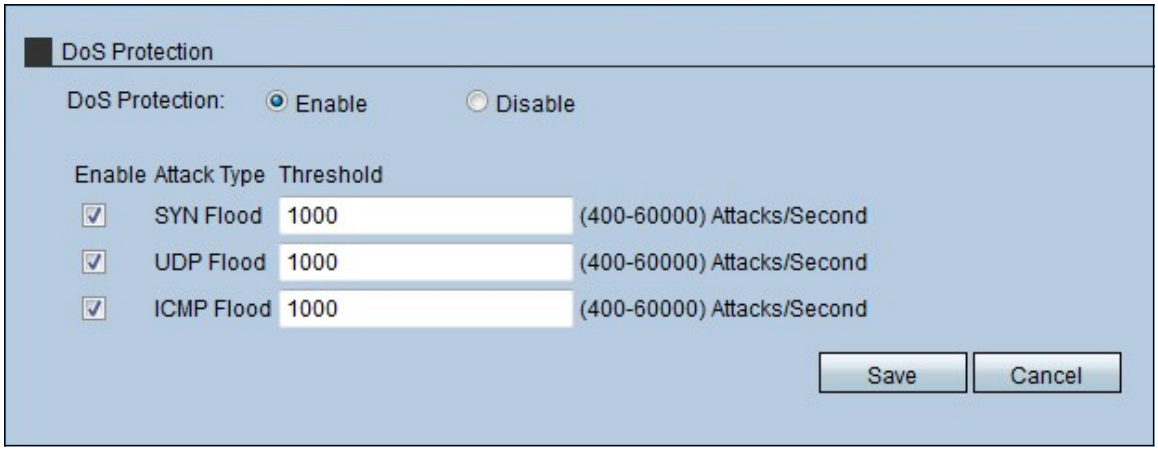
- RV315W

[Software Version]

•1.01.03

DoS保護

ステップ1:Web構成ユーティリティにログインし、[**Security**] > [**DoS Protection**]を選択します。[DoS保*護]*ページが開きます。



ステップ2:[**Enable**]オプションボタンをクリックして、RV315WでDoS保護を有効にします。

ステップ3:（オプション）DoS保護がRV315Wで防止する攻撃のタイプのチェックボックスをオンにします。次の3種類の攻撃があります。

- SYN Flood：最大数を入力します。SYNフラッドフィールドで DoS保護が機能する前に、RV315Wが受ける必要があるSYNフラッド攻撃。SYNフラッド攻撃は、攻撃者が大量のSYNメッセージをデバイスに送信して、デバイス上の正当なトラフィックを無効にしたときに発生します。

- UDPフラッド – RV315Wが受けるUDPフラッド攻撃の最大数を入力します。この数を

超えると、DoS保護がUDP Floodフィールドで機能します。User Datagram Protocol(UDP)フラッド攻撃は、攻撃者が大量のUDPパケットをデバイスのランダムポートに送信すると発生します。その結果、デバイスは正当なトラフィックに対するアクセスを拒否し、悪意のあるデータにアクセスしてネットワークを損傷する可能性があります。

・ ICMPフラッド：UDPフラッドフィールドでDoS保護が動作する前にRV315Wが受ける必要があるICMPフラッド攻撃の最大数を入力します。Internet Control Management Protocol(ICMP)フラッド攻撃は、攻撃者が大量のIPアドレスをデバイスに送信したときに発生します。デバイスは安全ではないように見えますが、実際には安全です。このため、デバイスはこれらのホストのネットワークへのアクセスを拒否し、攻撃者が送信できる新しいIPホストの接続を許可します。

ステップ4:[Save]をクリ**ックします**。