Konfigurieren des Angriffsschutzes auf dem RV132W oder RV134W VPN-Router

Ziel

Der Schutz vor Angriffen ermöglicht Ihnen, Ihr Netzwerk vor gängigen Angriffen wie Erkennung, Überflutung und Echo-Stürmen zu schützen. Während der Angriffsschutz auf dem Router standardmäßig aktiviert ist, können Sie die Parameter anpassen, um das Netzwerk empfindlicher und reaktionsfähiger auf möglicherweise erkannte Angriffe zu machen.

In diesem Artikel wird erläutert, wie Sie den Schutz vor Angriffen auf dem RV132W und dem RV134W VPN-Router konfigurieren.

Unterstützte Geräte

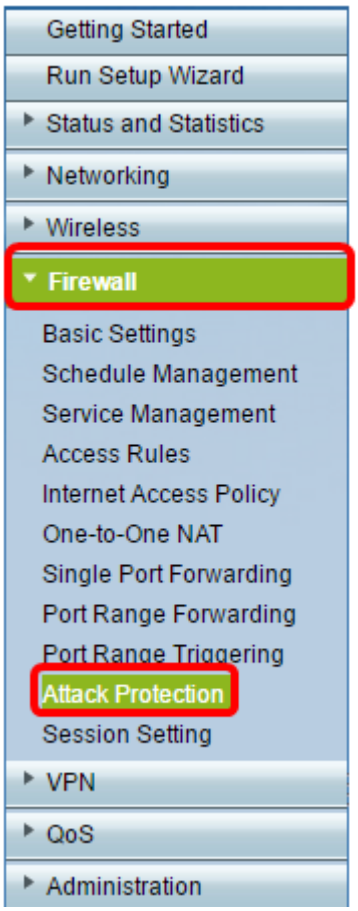
- RV 132 W
- RV134W

Software-Version

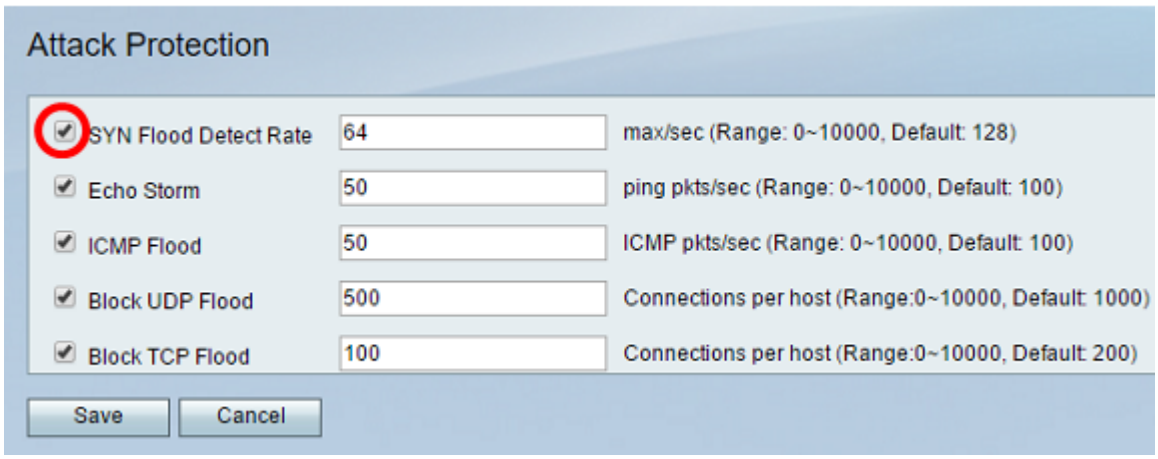
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

Konfigurieren des Angriffsschutzes

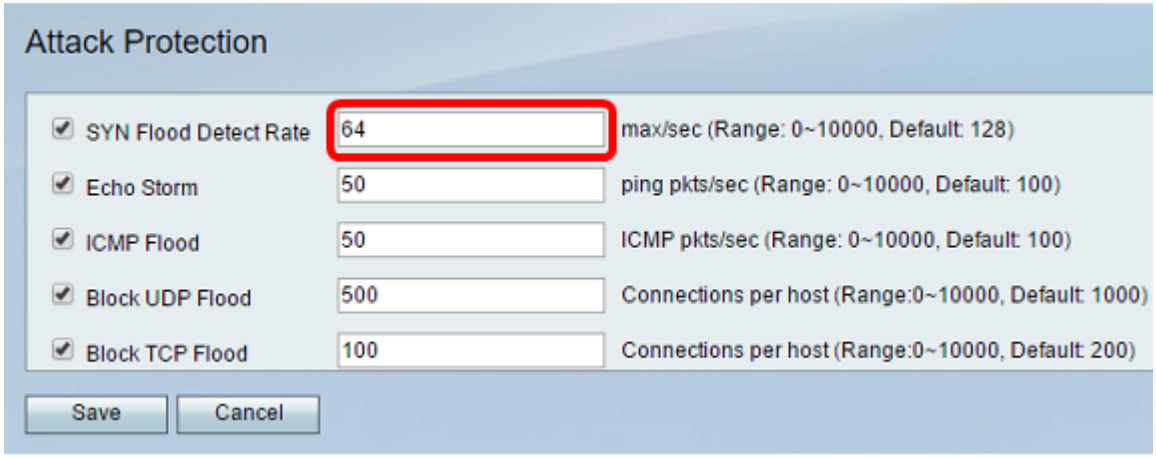
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Firewall > Attack Protection aus**.



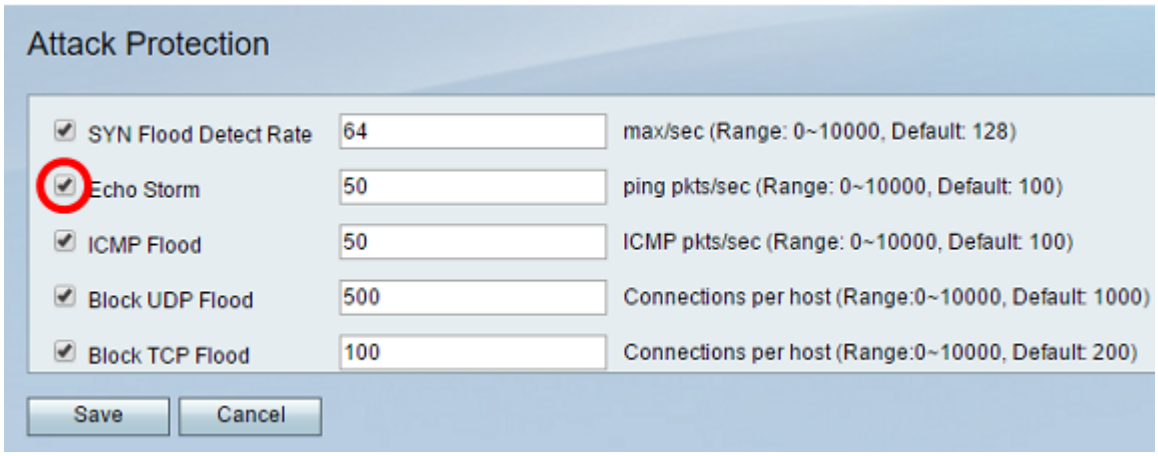
Schritt 2: Vergewissern Sie sich, dass das Kontrollkästchen SYN Flood Detect Rate (Erkennungsrate SYN Flood) aktiviert ist, um sicherzustellen, dass die Funktion aktiviert ist. Dies ist standardmäßig aktiviert.



Schritt 3: Geben Sie im Feld *SYN Flood Detect Rate (Erkennungsrate SYN Flood) einen* Wert ein. Der Standardwert ist 128 SYN-Pakete pro Sekunde. Sie können einen Wert zwischen 0 und 10000 eingeben. Dies ist die Anzahl der SYN-Pakete pro Sekunde, die die Sicherheits-Appliance veranlasst, einen SYN-Flood-Angriff zu ermitteln. Ein Wert von 0 zeigt an, dass die SYN Flood Detection-Funktion deaktiviert ist. In diesem Beispiel ist der eingegebene Wert 64. Das bedeutet, dass die Appliance einen SYN-Flood-Angriff mit nur 64 SYN-Paketen pro Sekunde erkennen würde, was sie empfindlicher macht als die Standardkonfiguration.

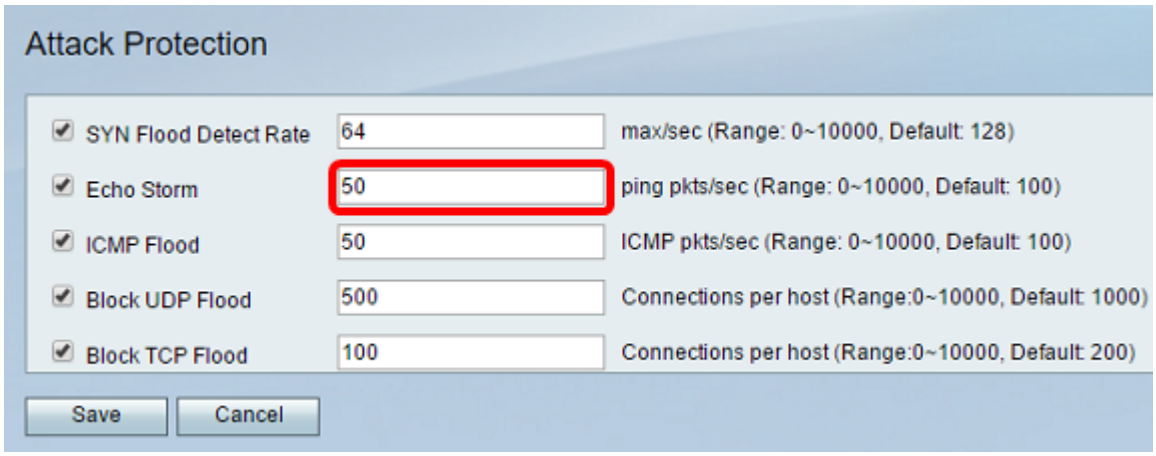


Schritt 4: Vergewissern Sie sich, dass das Kontrollkästchen "Echo Storm" aktiviert ist, um sicherzustellen, dass die Funktion aktiviert ist. Dies ist standardmäßig aktiviert.

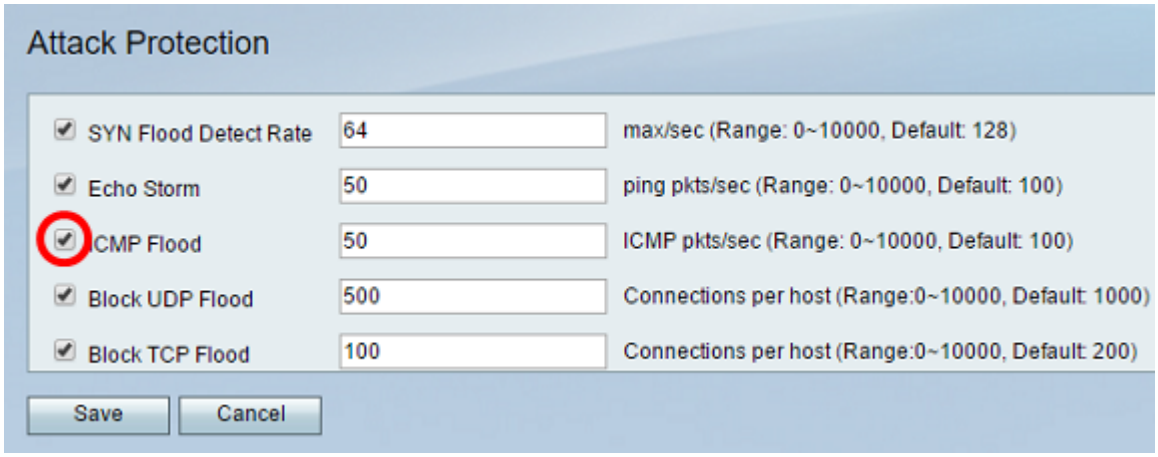


Schritt 5: Geben Sie im Feld *Echo Storm* (*Echo-Sturm*) einen Wert ein. Der Standardwert ist 100 Pings pro Sekunde. Sie können einen Wert zwischen 0 und 10000 eingeben. Dies ist die Anzahl der Pings pro Sekunde, die die Sicherheits-Appliance veranlasst, das Auftreten eines Echo-Sturm-Angriffsereignisses zu bestimmen. Ein Wert von Null bedeutet, dass die Funktion "Echo Storm" deaktiviert ist.

Hinweis: In diesem Beispiel erkennt die Appliance ein Echo Storm-Ereignis mit nur 50 Pings pro Sekunde.

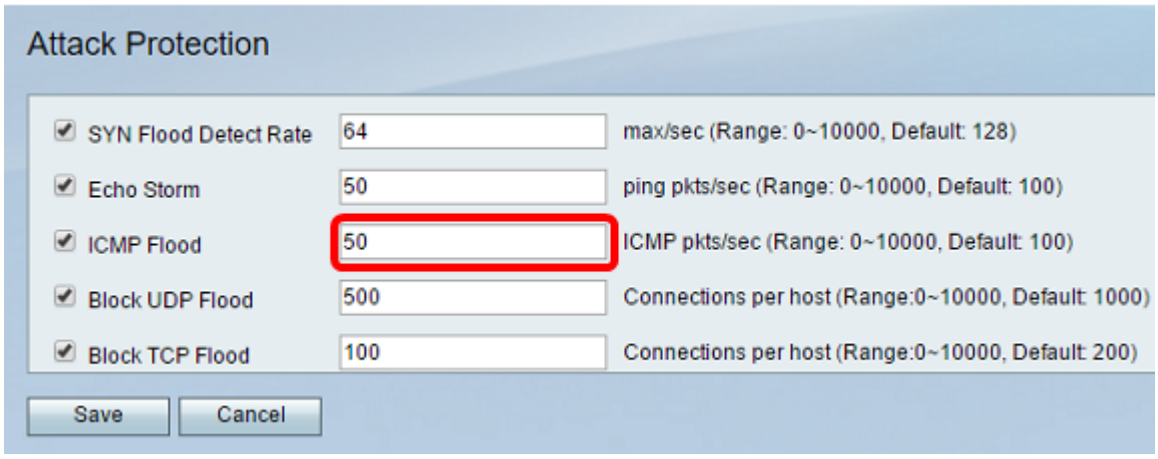


Schritt 6: Vergewissern Sie sich, dass das Kontrollkästchen Internet Control Message Protocol (ICMP) Flood aktiviert ist, um sicherzustellen, dass die Funktion aktiviert ist. Diese Funktion ist standardmäßig aktiviert.

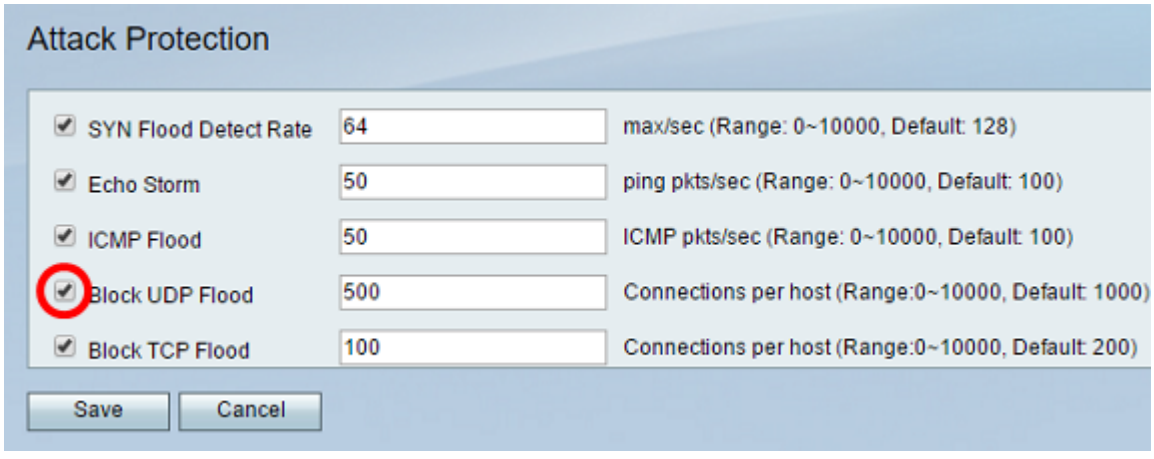


Schritt 7. Geben Sie im Feld *ICMP Flood* einen numerischen Wert ein. Der Standardwert ist 100 ICMP-Pakete pro Sekunde. Sie können einen Wert zwischen 0 und 10000 eingeben. Dies ist die Anzahl der ICMP-Pakete pro Sekunde, die die Sicherheits-Appliance veranlasst, das Auftreten eines ICMP-Flood-Angriffsereignisses zu bestimmen. Ein Wert von 0 zeigt an, dass die ICMP-Flood-Funktion deaktiviert ist.

Hinweis: In diesem Beispiel ist der eingegebene Wert 50, wodurch er empfindlicher auf ICMP-Flooding reagiert als seine Standardeinstellung.

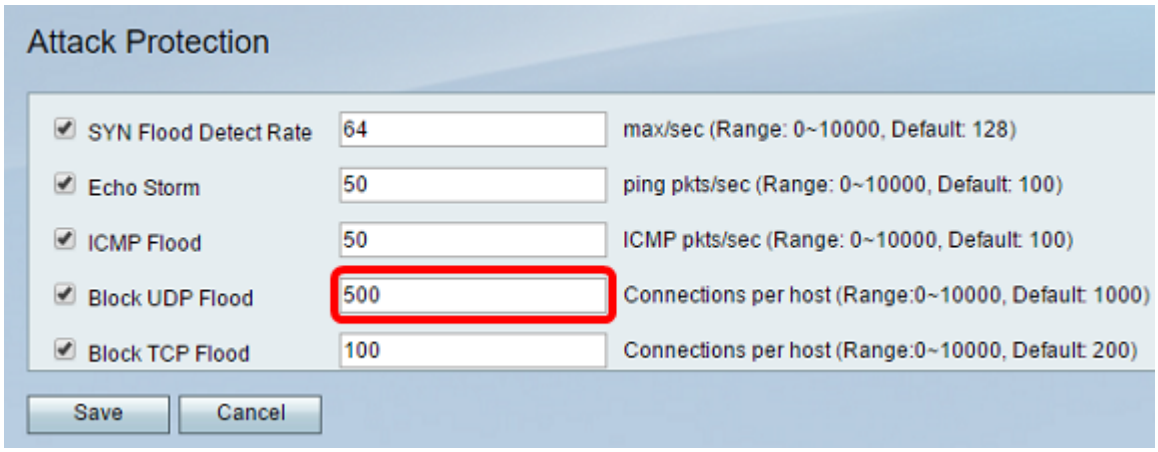


Schritt 8: Vergewissern Sie sich, dass das Kontrollkästchen UDP Flood blockieren aktiviert ist, um sicherzustellen, dass die Funktion aktiviert ist, und um zu verhindern, dass die Sicherheits-Appliance mehr als 150 gleichzeitige aktive User Datagram Protocol (UDP)-Verbindungen pro Sekunde von einem einzelnen Computer im LAN akzeptiert. Diese Option ist standardmäßig aktiviert.

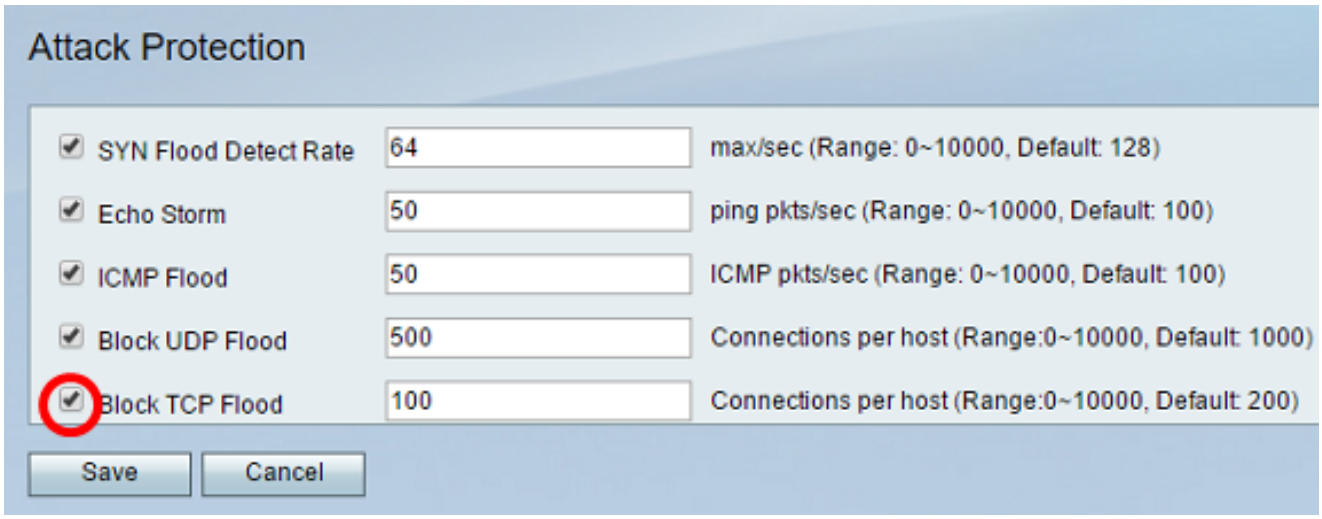


Schritt 9. Geben Sie im Feld *Block UDP Flood* (*UDP-Flood blockieren) einen* Wert zwischen

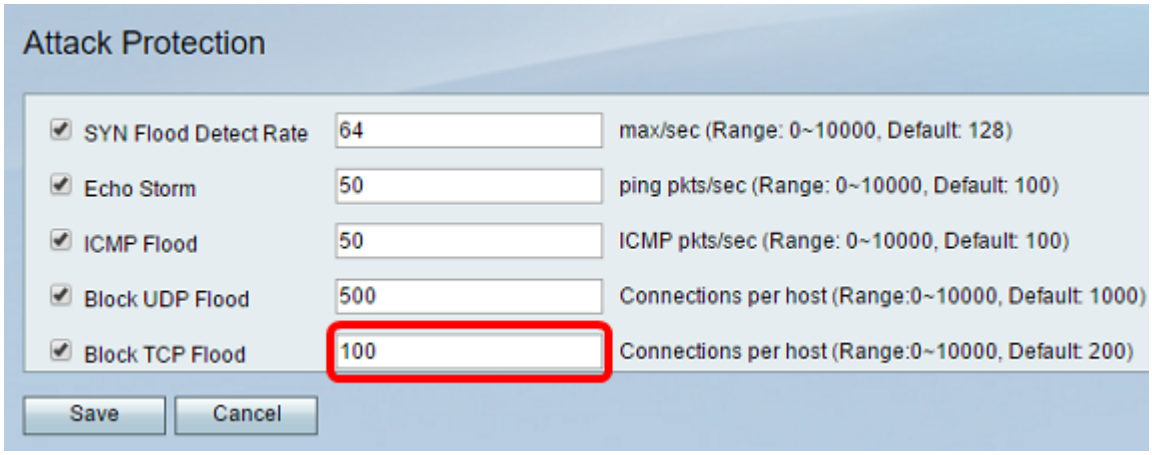
0 und 10000 ein. Der Standardwert ist 1000. In diesem Beispiel ist der eingegebene Wert 500, wodurch er empfindlicher wird.



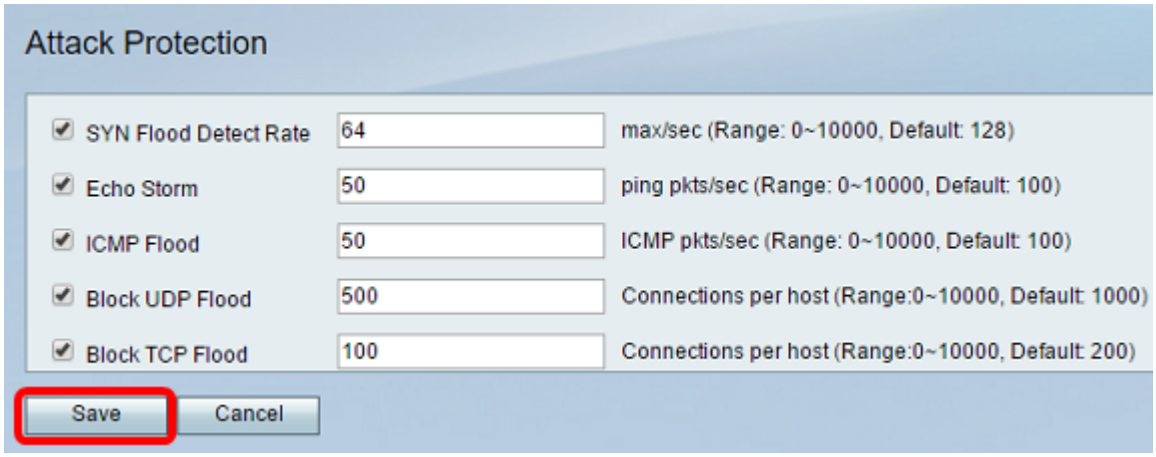
Schritt 10. Vergewissern Sie sich, dass das Kontrollkästchen TCP Flood blockieren aktiviert ist, um alle ungültigen TCP-Pakete (Transmission Control Protocol) zu löschen. Diese Option ist standardmäßig aktiviert.



Schritt 11. Geben Sie im Feld *TCP Flood blockieren* einen Wert zwischen 0 und 10000 ein, um Ihr Netzwerk vor einem SYN-Flood-Angriff zu schützen. Der Standardwert ist 200. In diesem Beispiel wird 100 eingegeben, wodurch die Eingabe empfindlicher wird.



Schritt 12: Klicken Sie auf **Speichern**.



Sie sollten jetzt den Angriffsschutz für Ihren RV132W oder RV134W Router erfolgreich konfiguriert haben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.