在RV132W或RV134W VPN路由器上配置攻擊保護

目標

攻擊保護使您能夠保護您的網路免受常見型別的攻擊，如發現、泛洪和回聲風暴。當路由器預設啟用攻擊保護時，您可以調整引數以使網路更敏感且更快速地對它可能檢測到的攻擊作出響應。

本文旨在展示如何在RV132W和RV134W VPN路由器上配置攻擊保護。

適用裝置

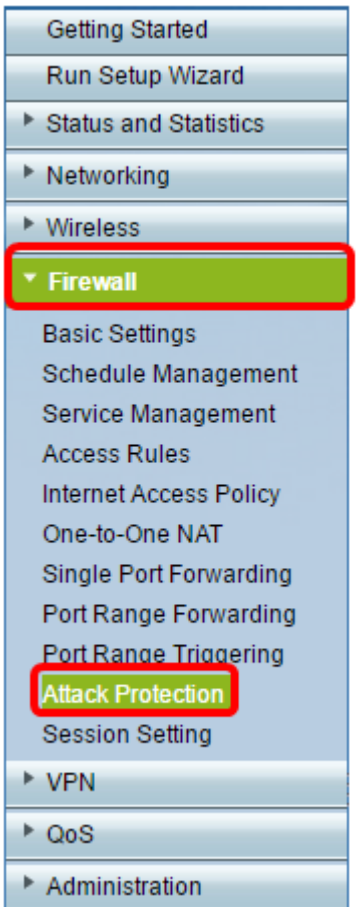
- RV 132W
- RV134W

軟體版本

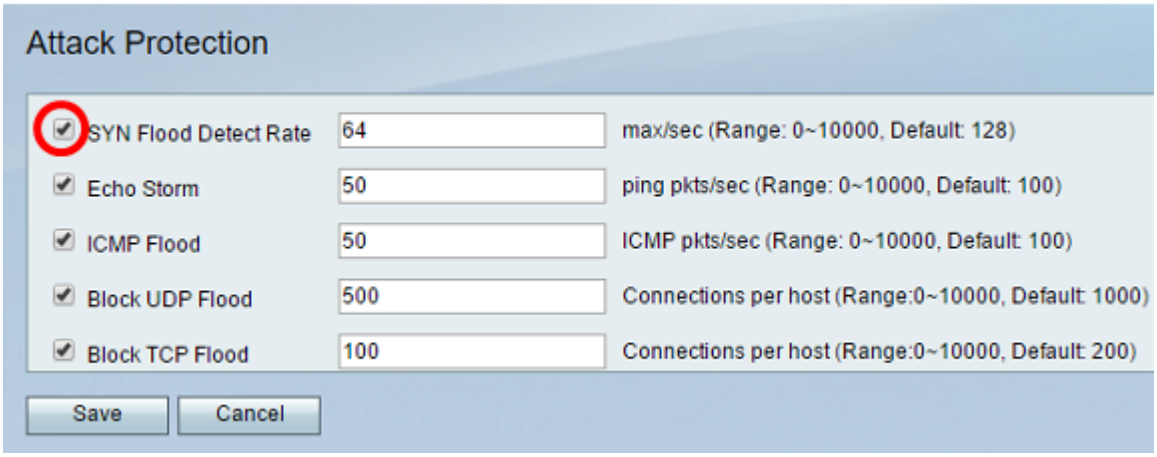
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

配置攻擊保護

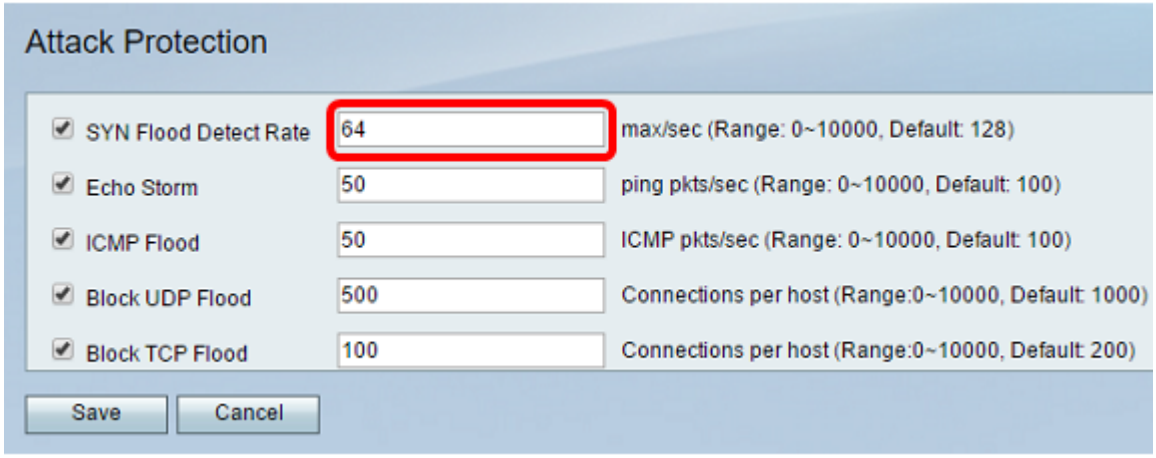
步驟1.登入到基於Web的實用程式，然後選擇**Firewall > Attack Protection**。



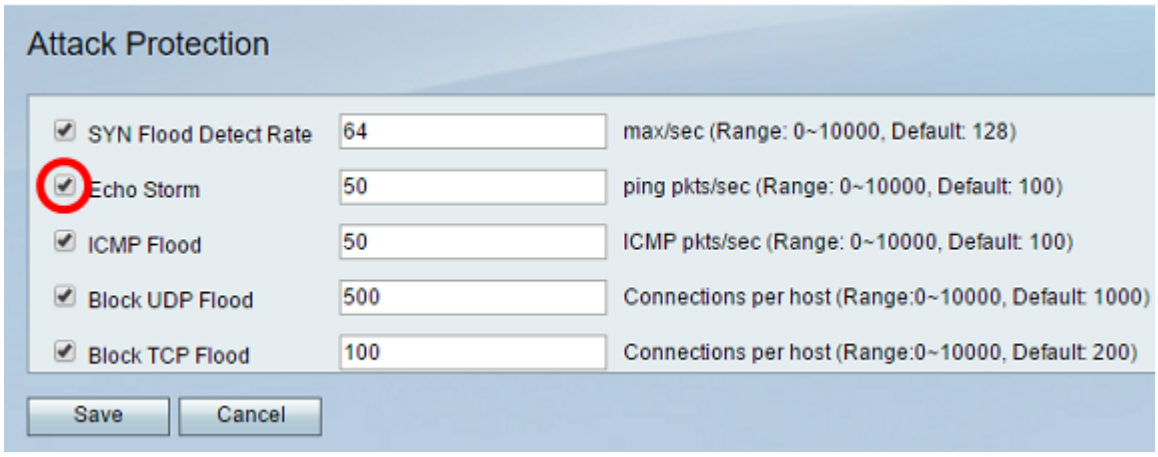
步驟2.驗證是否已選中SYN泛洪檢測速率覈取方塊以確保功能處於活動狀態。預設情況下會選中此項。



步驟3.在*SYN Flood Detect Rate*欄位中輸入值。預設值為128 SYN資料包每秒。您可以輸入一個介於0到10000之間的值。它將使安全裝置確定發生SYN泛洪入侵的SYN每秒資料包數。如果值為0，則表示SYN泛洪檢測功能已禁用。在本例中，輸入的值為64。這意味著裝置將以每秒64個SYN資料包的速度檢測SYN泛洪入侵，使其比預設配置更敏感。

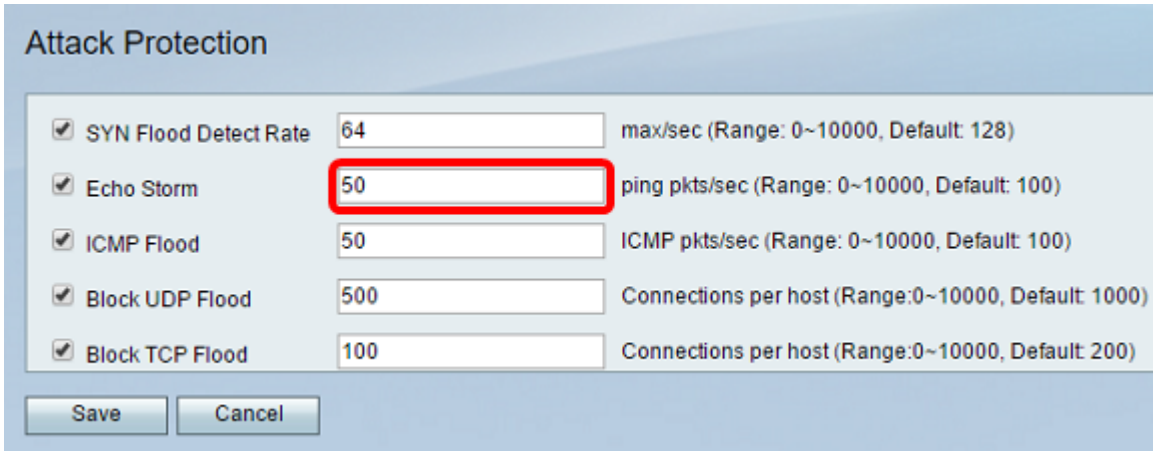


步驟4.確認已選中Echo Storm覈取方塊以確保功能處於活動狀態。預設情況下會選中此項。

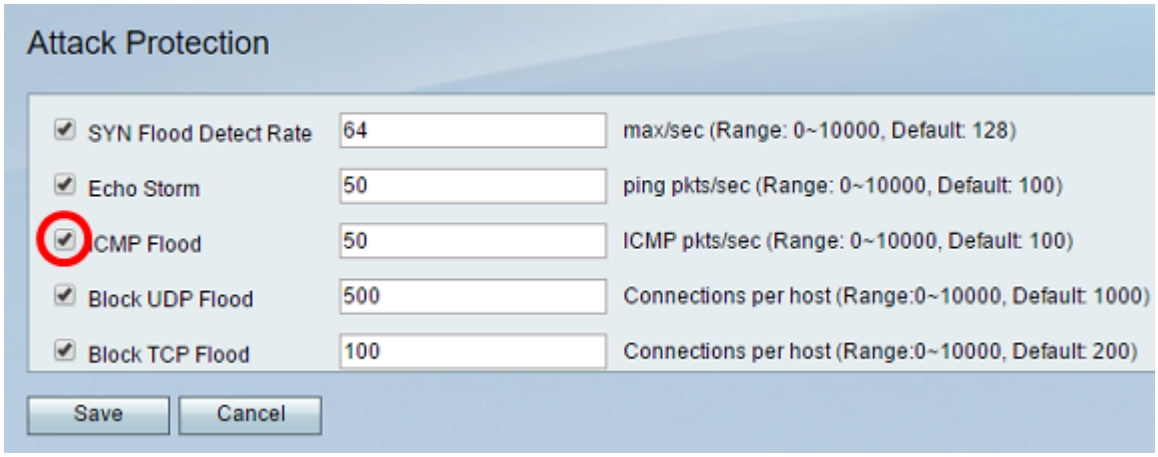


步驟5.在*Echo Storm*欄位中輸入值。預設值為每秒100次ping。您可以輸入一個介於0到10000之間的值。它將是每秒的ping次數，它將使安全裝置確定正在發生回應風暴入侵事件。如果值為0，則表示已禁用「回聲風暴」功能。

注意：在本示例中，裝置僅以每秒50次ping操作來檢測回聲風暴事件。

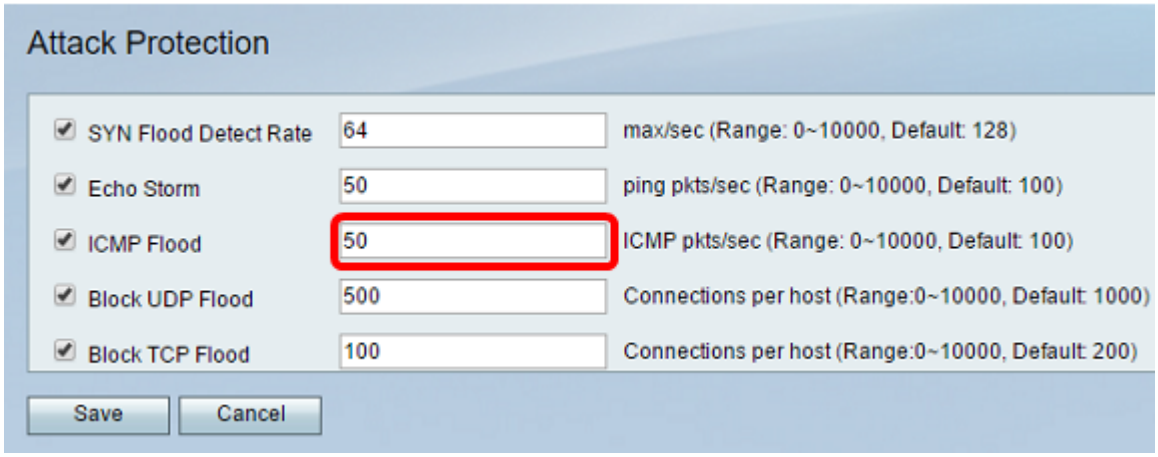


步驟6.確認已選中Internet Control Message Protocol(ICMP)Flood覈取方塊以確保功能處於活動狀態。預設情況下會檢查此功能。

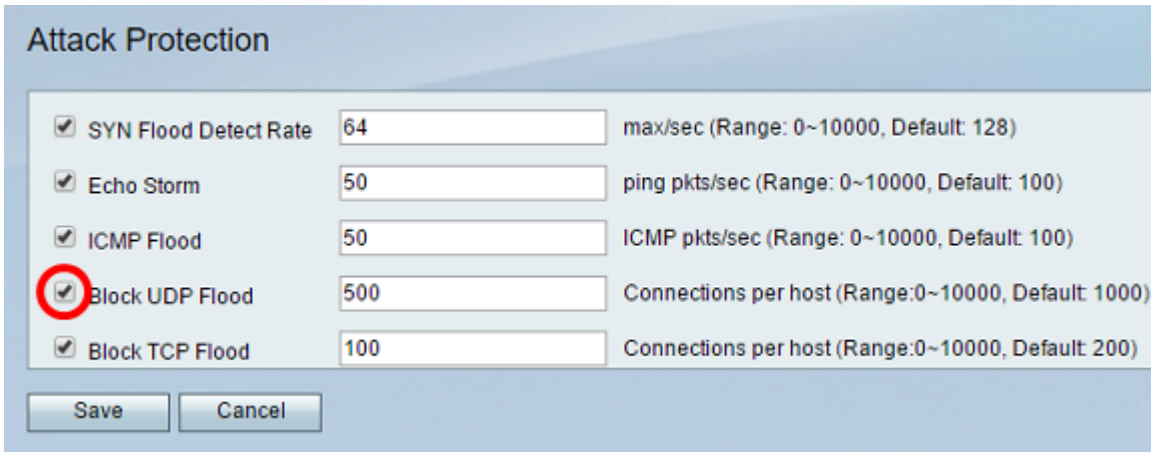


步驟7.在*ICMP Flood*欄位中輸入數值。預設值為100 ICMP封包每秒。您可以輸入一個介於0到10000之間的值。它將是每秒導致安全裝置確定發生ICMP泛洪入侵事件的ICMP資料包數。如果值為0，則表示ICMP泛洪功能已禁用。

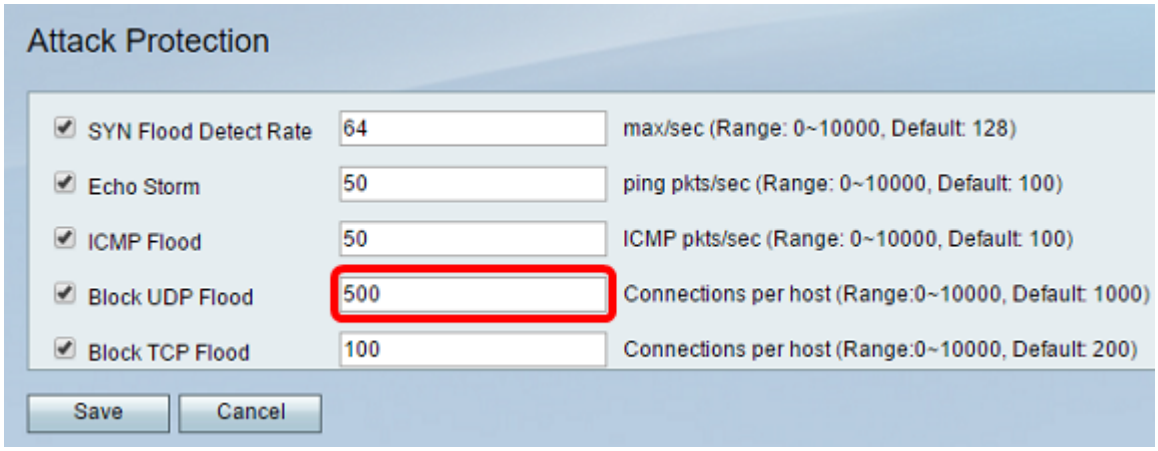
注意：在本範例中，輸入的值為50，使其對ICMP泛洪的敏感度高於其預設值。



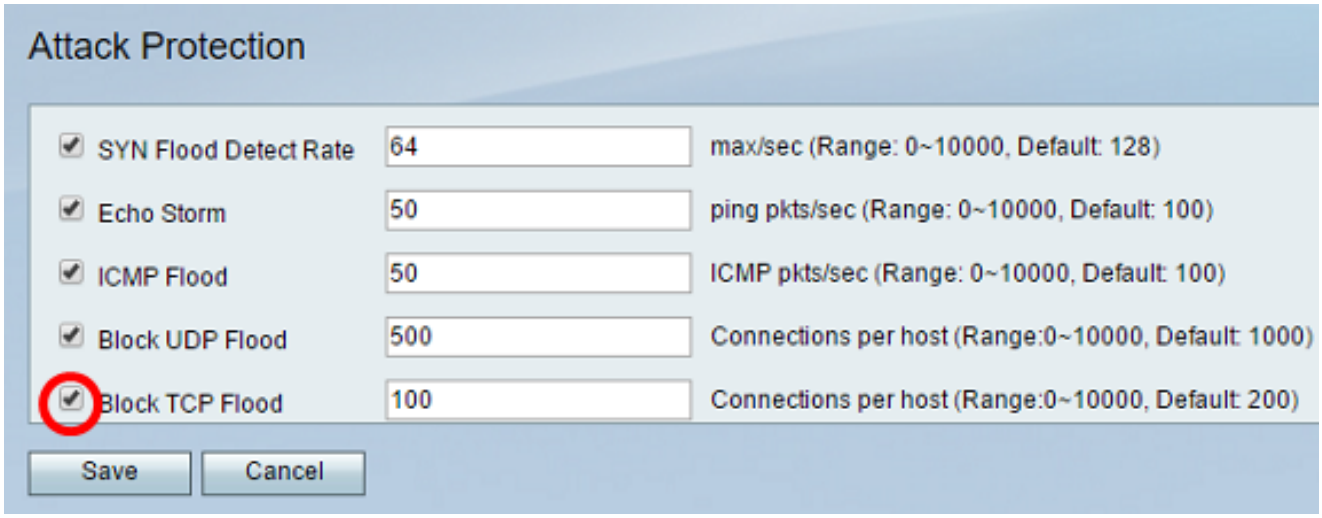
步驟8.確保選中Block UDP Flood（阻止UDP泛洪）覈取方塊以確保該功能處於活動狀態，並防止安全裝置每秒從區域網(LAN)上的單台電腦接受超過150個同時活動的使用者資料包協定(UDP)連線。預設情況下會選中此選項。



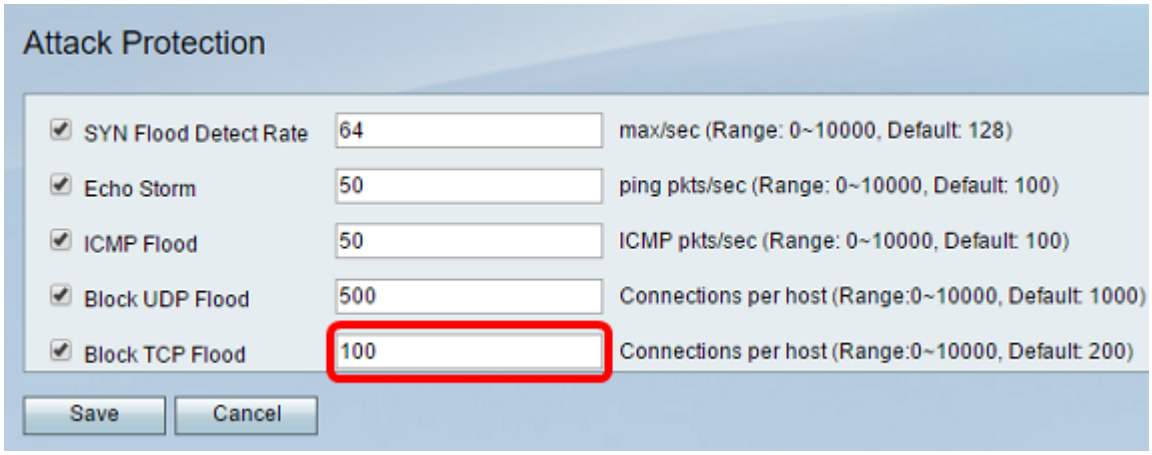
步驟9.在*Block UDP Flood*欄位中輸入從0到10000的值。預設值為 1000。在本例中，輸入的值為500，使其更敏感。



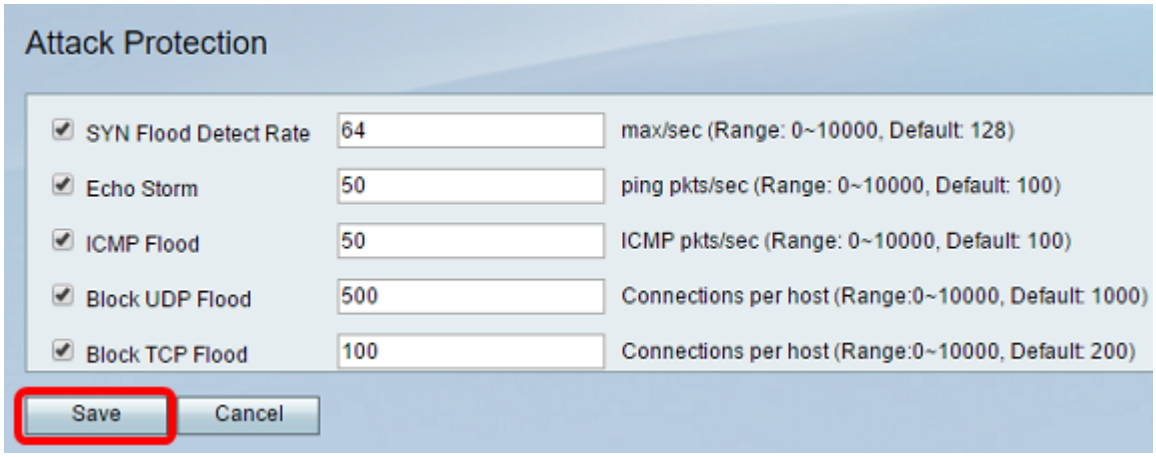
步驟10.驗證是否已選中Block TCP Flood覈取方塊以丟棄所有無效的傳輸控制協定(TCP)資料包。預設情況下會選中此選項。



步驟11.在*Block TCP Flood*欄位中輸入從0到10000的值，保護您的網路免受SYN泛洪攻擊。預設值為 200。在此範例中，輸入100，使其更為敏感。



步驟12.按一下「**Save**」。



現在，您應該已經在RV132W或RV134W路由器上成功配置了攻擊保護。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。