在RV132W或RV134W VPN路由器上配置攻击保护

目标

利用攻击保护，您可以保护您的网络免受常见类型的攻击，例如发现、泛洪和回声风暴。当路由器默认启用攻击保护时，您可以调整参数，使网络更敏感且更快速地响应它可能检测到的攻击。

本文旨在展示如何在RV132W和RV134W VPN路由器上配置攻击保护。

适用设备

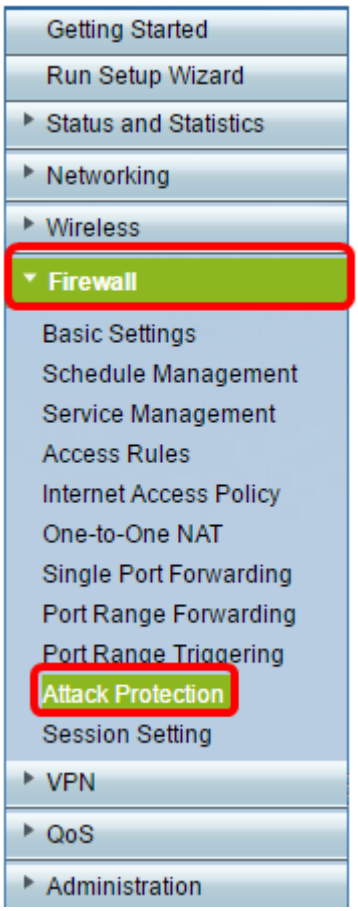
- RV 132W
- RV134W

软件版本

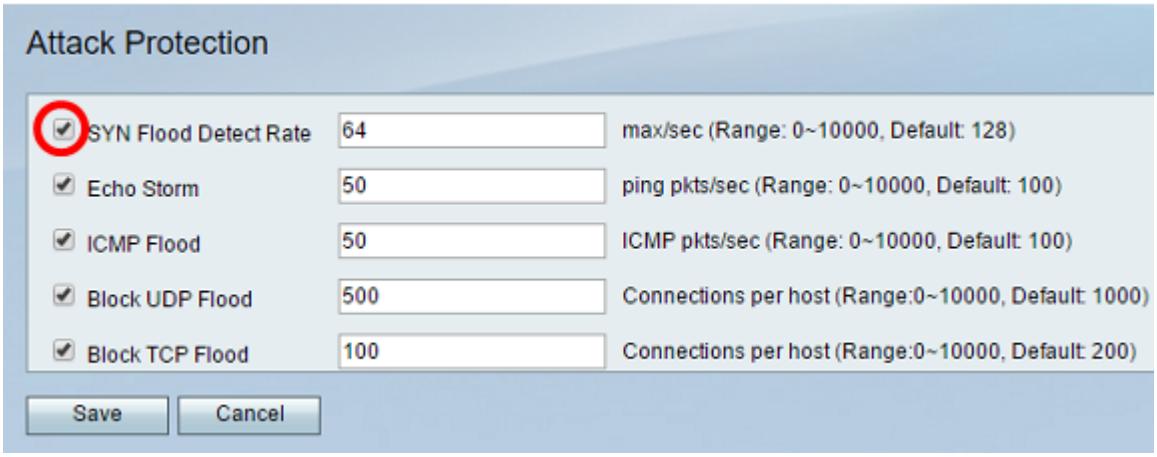
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

配置攻击保护

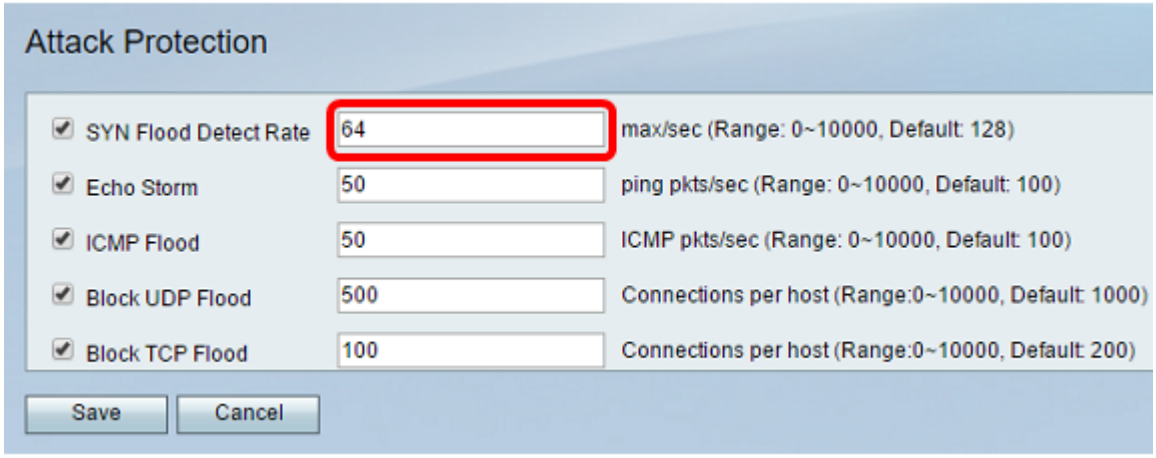
步骤1:登录到基于Web的实用程序，然后选择**Firewall > Attack Protection**。



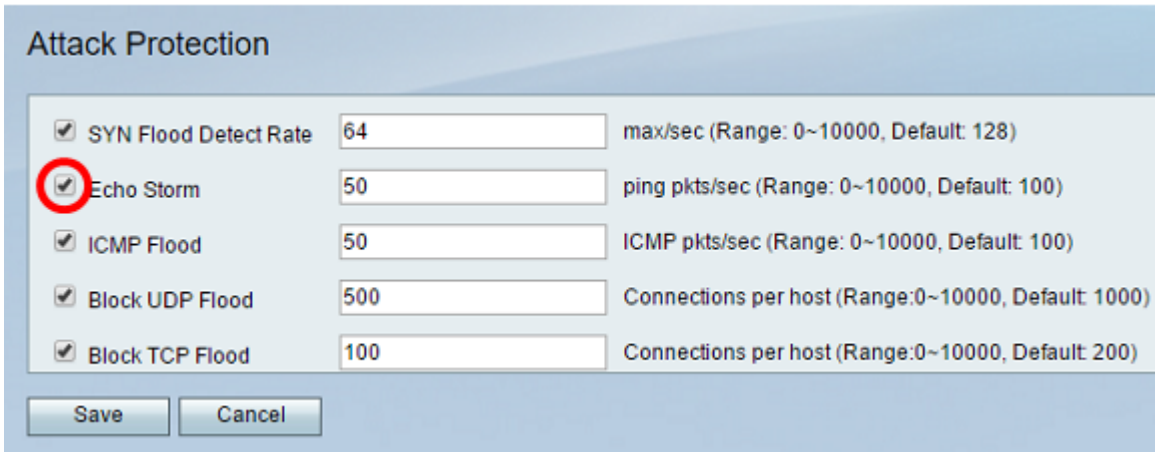
第二步：确保选中SYN Flood Detect Rate复选框以确保功能处于活动状态。默认情况下会选中此项。



第三步：在*SYN Flood Detect Rate*字段中输入值。默认值为每秒128个SYN数据包。您可以输入一个介于0到10000之间的值。它将是每秒导致安全设备确定发生SYN泛洪入侵的SYN数据包数。如果值为0，则表示SYN泛洪检测功能已禁用。在本示例中，输入的值为64。这意味着设备将以每秒仅64个SYN数据包的速度检测SYN泛洪入侵，使其比默认配置更敏感。

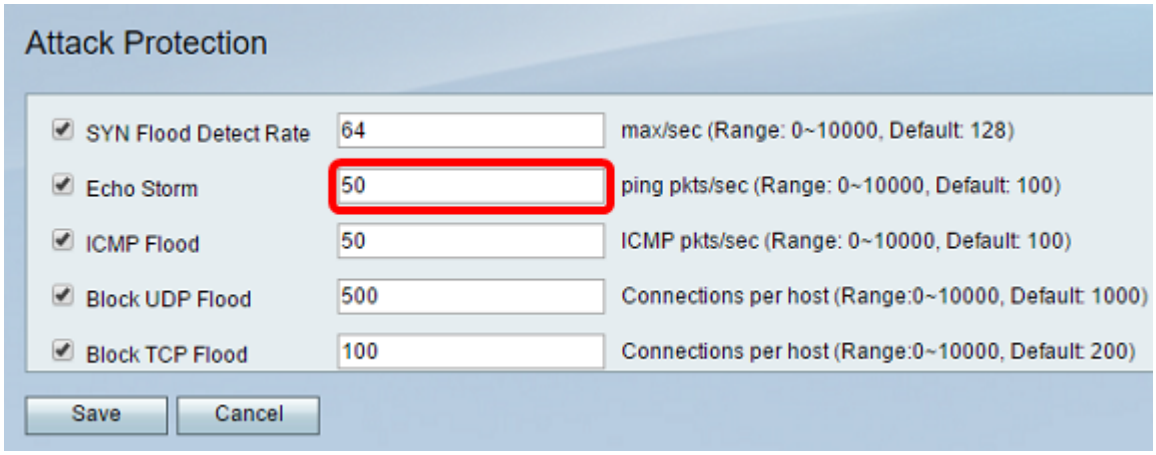


第四步：确认已选中Echo Storm复选框以确保功能处于活动状态。默认情况下会选中此项。

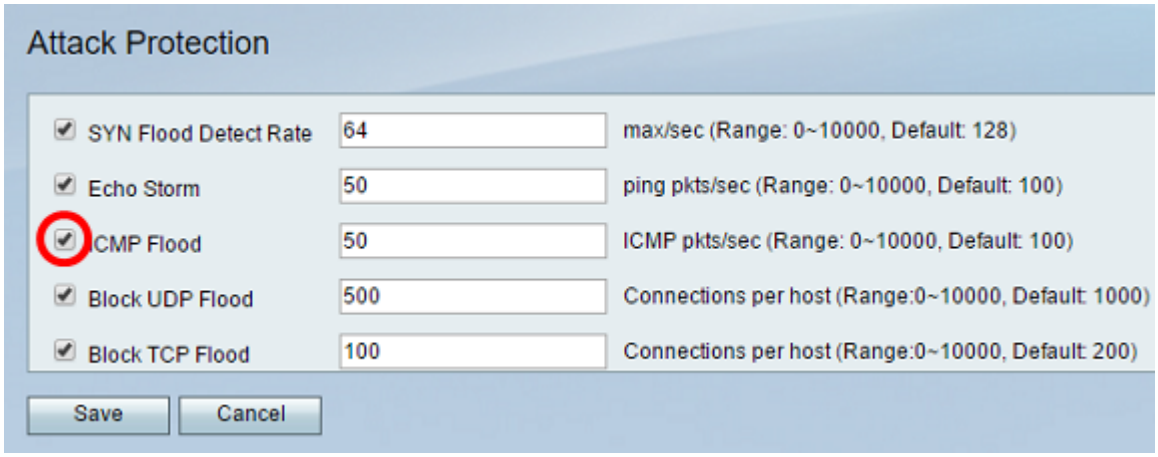


第五步：在*Echo Storm*字段中输入值。默认值为每秒100次ping。您可以输入一个介于0到10000之间的值。它是指每秒使安全设备确定发生回声风暴入侵事件的ping次数。如果值为0，则表示已禁用回声风暴功能。

注意：在本示例中，设备将仅以每秒50次ping检测回应风暴事件。

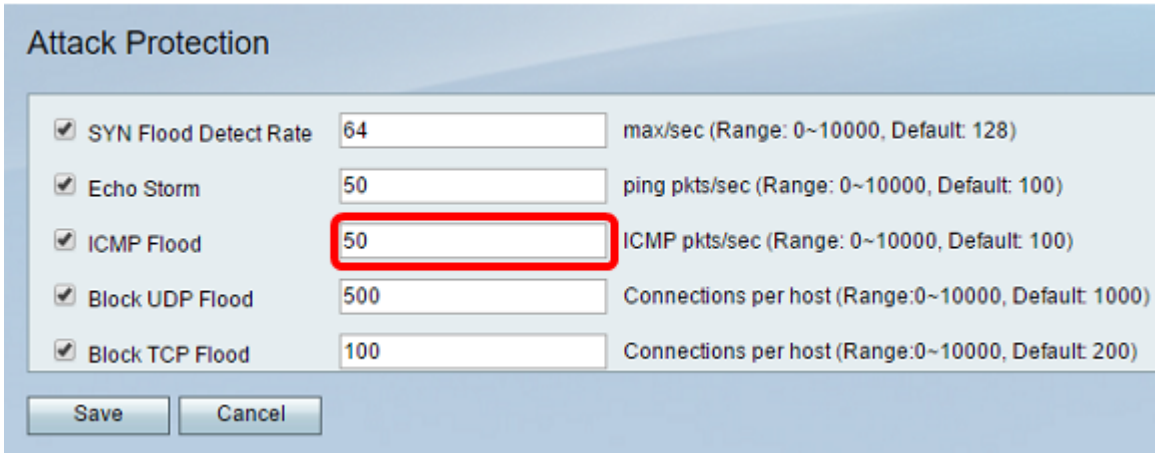


第六步：确保已选中Internet Control Message Protocol(ICMP)Flood复选框以确保功能处于活动状态。默认情况下会选中此功能。

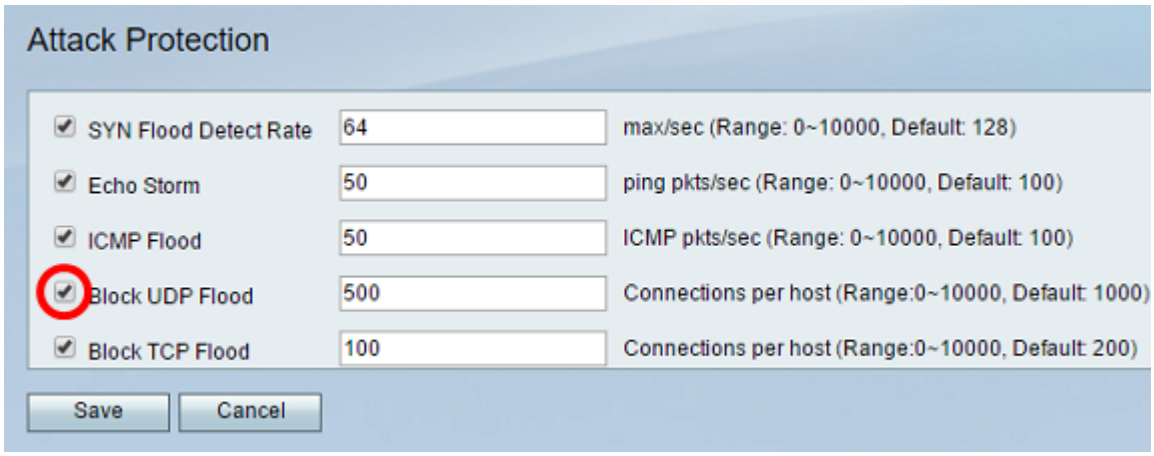


步骤 7.在*ICMP Flood*字段中输入数值。默认值为每秒100个ICMP数据包。您可以输入一个介于0到10000之间的值。它是每秒导致安全设备确定发生ICMP泛洪入侵事件的ICMP数据包数。如果值为0，则表示ICMP泛洪功能已禁用。

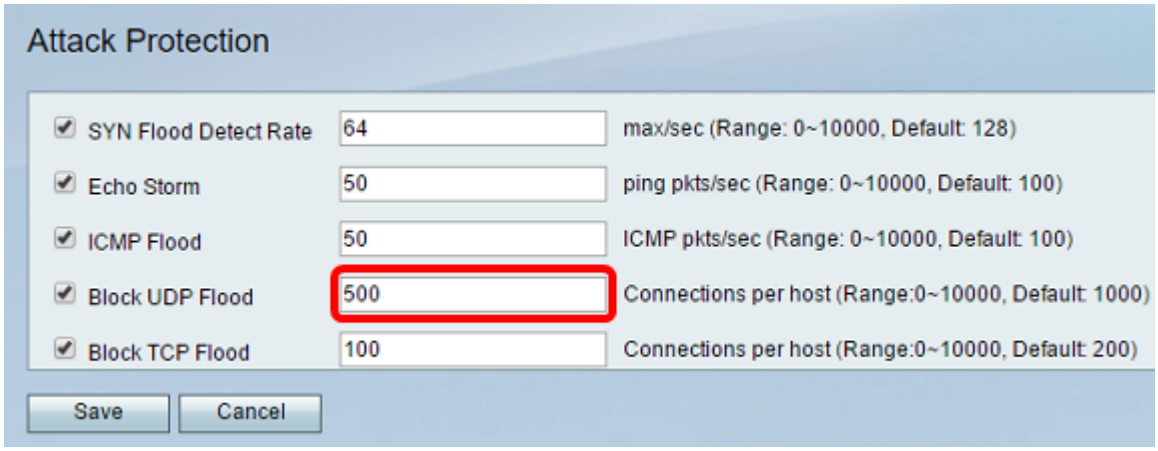
注意：在本示例中，输入的值为50，使其对ICMP泛洪的敏感度高于其默认设置。



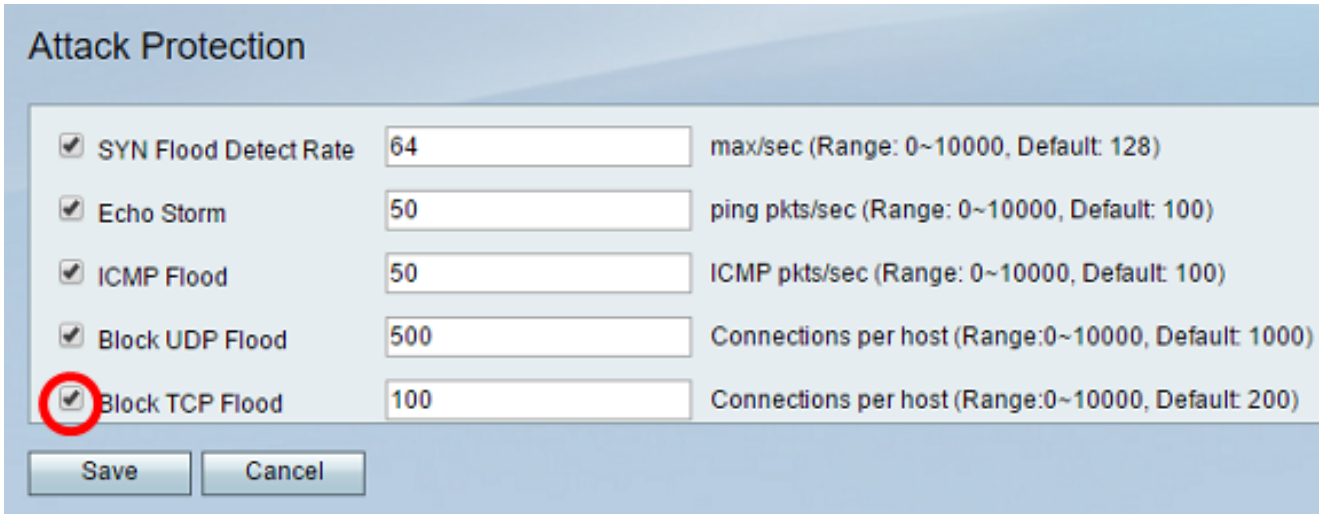
步骤 8确保选中Block UDP Flood复选框以确保功能处于活动状态，并防止安全设备每秒从局域网(LAN)上的单台计算机接受超过150个同时活动的用户数据报协议(UDP)连接。默认情况下选中此选项。



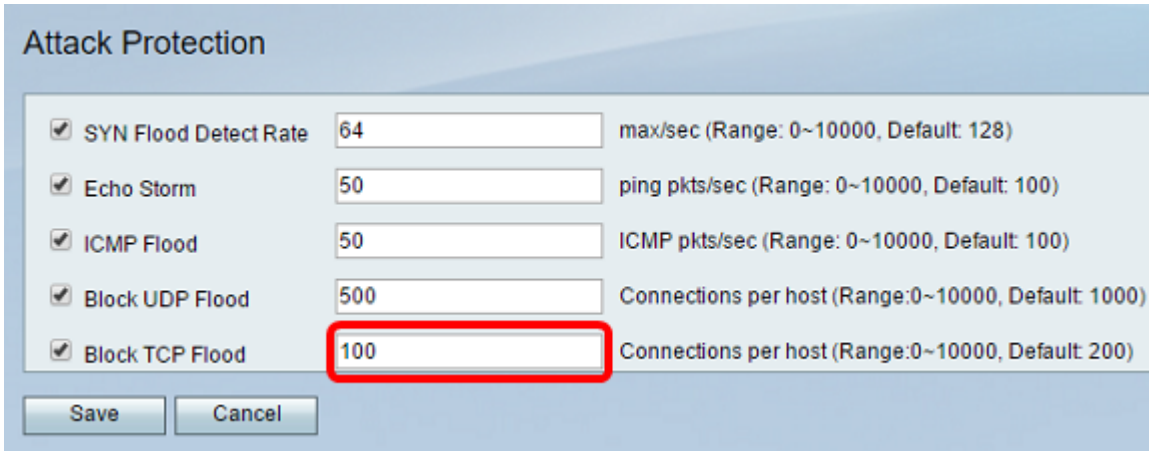
步骤 9在*Block UDP Flood*字段中输入一个介于0到10000之间的值。默认值为 1000。在本例中，输入的值为500，使其更加敏感。



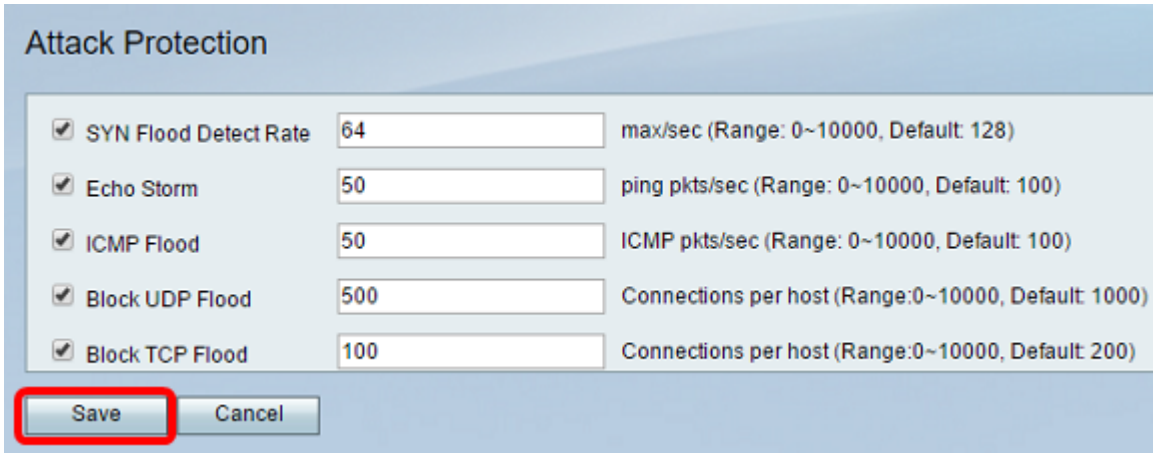
步骤 10验证是否已选中Block TCP Flood复选框以丢弃所有无效的传输控制协议(TCP)数据包。默认情况下选中此选项。



步骤 11在*Block TCP Flood*字段中输入一个介于0到10000之间的值，以保护您的网络免受SYN泛洪攻击。默认值为 200。在本例中，输入100，使其更加敏感。



步骤 12Click **Save**.



现在，您应该已经在RV132W或RV134W路由器上成功配置了攻击保护。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。