

在RV132W或RV134W VPN路由器上配置攻擊保護

目標

利用攻擊保護，您可以保護網路免受常見型別的攻擊，例如發現、泛洪和回聲風暴。雖然路由器預設啟用攻擊保護，但您可以調整引數以使網路更敏感，對它可能檢測到的攻擊做出更及時的響應。

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. 登入基於Web的實用程式，並選擇Firewall > Attack Protection。

Getting Started

Run Setup Wizard

▶ Status and Statistics

▶ Networking

▶ Wireless

▼ **Firewall**

Basic Settings

Schedule Management

Service Management

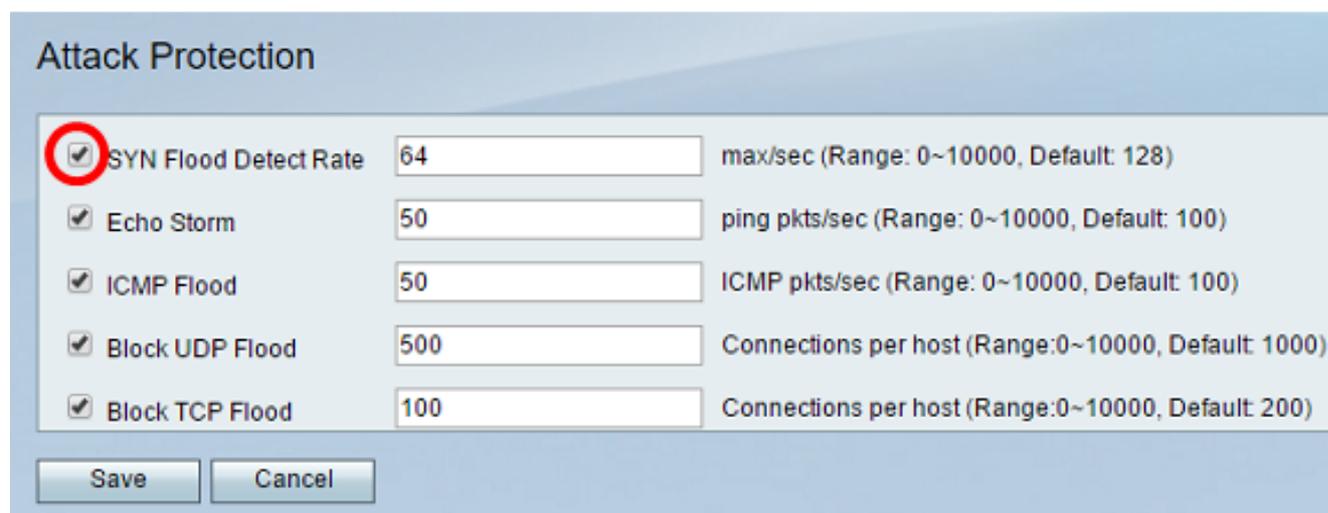
Access Rules

Internet Access Policy

One-to-One NAT

Single Port Forwarding

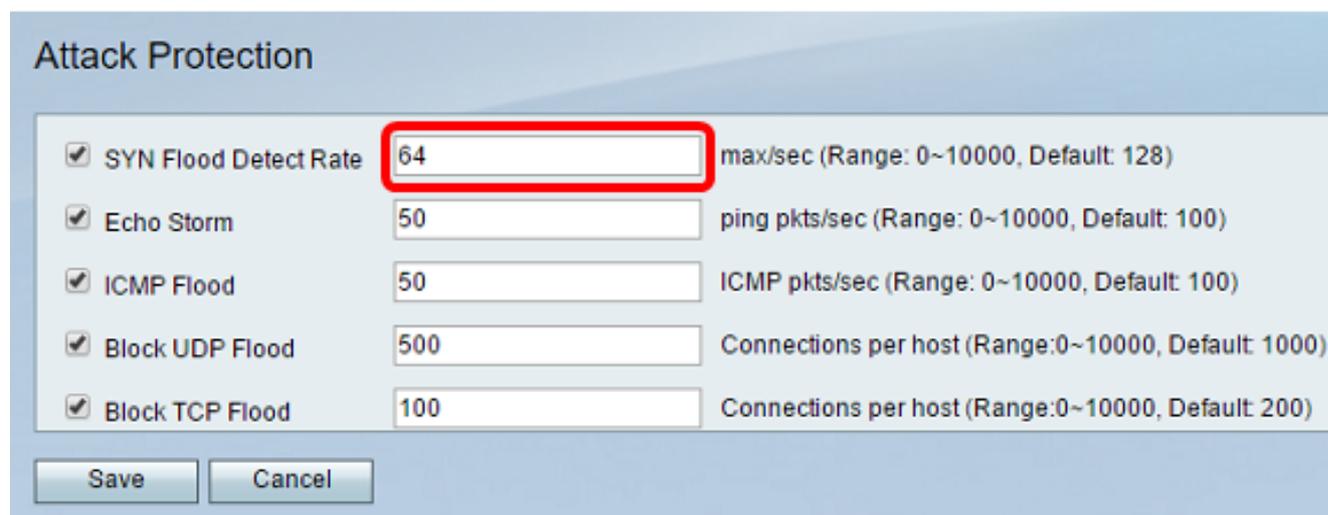
步驟 2. 確保選中了 SYN 泛洪檢測速率覈取方塊以確保該功能處於活動狀態。依預設，會核取此選項。



Option	Value	Unit / Range
<input checked="" type="checkbox"/> SYN Flood Detect Rate	64	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/> Echo Storm	50	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> ICMP Flood	50	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> Block UDP Flood	500	Connections per host (Range: 0~10000, Default: 1000)
<input checked="" type="checkbox"/> Block TCP Flood	100	Connections per host (Range: 0~10000, Default: 200)

Buttons: Save, Cancel

步驟 3. 在 SYN Flood Detect Rate 欄位中輸入值。預設值為 128 SYN 資料包/秒。您可以輸入一個介於 0 到 10000 之間的值。它將是每秒的 SYN 資料包數，使安全裝置確定發生 SYN 泛洪入侵。如果值為 0，則表示 SYN 泛洪檢測功能已停用。在此範例中，輸入的值為 64。這意味著裝置檢測到的 SYN 泛洪入侵僅為每秒 64 個 SYN 資料包，因此比預設配置更敏感。



Option	Value	Unit / Range
<input checked="" type="checkbox"/> SYN Flood Detect Rate	64	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/> Echo Storm	50	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> ICMP Flood	50	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> Block UDP Flood	500	Connections per host (Range: 0~10000, Default: 1000)
<input checked="" type="checkbox"/> Block TCP Flood	100	Connections per host (Range: 0~10000, Default: 200)

Buttons: Save, Cancel

步驟 4. 確認已選中 Echo Storm 覈取方塊，以確保該功能處於活動狀態。依預設，會核取此選項。

Attack Protection

<input checked="" type="checkbox"/> SYN Flood Detect Rate	<input type="text" value="64"/>	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/> Echo Storm	<input type="text" value="50"/>	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> ICMP Flood	<input type="text" value="50"/>	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> Block UDP Flood	<input type="text" value="500"/>	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/> Block TCP Flood	<input type="text" value="100"/>	Connections per host (Range:0~10000, Default: 200)

步驟 5. 在 Echo Storm 欄位中輸入值。預設值是每秒 100 次 ping。您可以輸入一個介於 0 到 10000 之間的值。它是每秒 ping 的次數，它將使安全裝置確定發生了回聲風暴入侵事件。如果值為 0，則表示已停用回聲風暴功能。

注意：在本示例中，裝置檢測到回聲風暴事件時每秒僅偵測 50 次 ping。

Attack Protection

<input checked="" type="checkbox"/> SYN Flood Detect Rate	<input type="text" value="64"/>	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/> Echo Storm	<input type="text" value="50"/>	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> ICMP Flood	<input type="text" value="50"/>	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> Block UDP Flood	<input type="text" value="500"/>	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/> Block TCP Flood	<input type="text" value="100"/>	Connections per host (Range:0~10000, Default: 200)

步驟 6. 確認已選中 Internet Control Message Protocol (ICMP) Flood (網際網路控制消息協定 (ICMP) 泛洪) 覈取方塊以確保該功能處於活動狀態。依預設，會核取此功能。

Attack Protection

<input checked="" type="checkbox"/>	SYN Flood Detect Rate	64	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/>	Echo Storm	50	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	ICMP Flood	50	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	Block UDP Flood	500	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/>	Block TCP Flood	100	Connections per host (Range:0~10000, Default: 200)

步驟 7. 在ICMP Flood欄位中輸入數值。預設值為100 ICMP資料包/秒。您可以輸入一個介於0到10000之間的值。它將是每秒的ICMP資料包數，使安全裝置確定發生了ICMP泛洪入侵事件。如果值為0，則表示ICMP泛洪功能已停用。

注意：在本示例中，輸入的值為50，因此它對ICMP泛洪的敏感度高於其預設設定。

Attack Protection

<input checked="" type="checkbox"/>	SYN Flood Detect Rate	64	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/>	Echo Storm	50	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	ICMP Flood	50	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	Block UDP Flood	500	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/>	Block TCP Flood	100	Connections per host (Range:0~10000, Default: 200)

步驟 8. 確保選中了Block UDP Flood竅取方塊，以確保該功能處於活動狀態，並防止安全裝置從區域網(LAN)上的單台電腦上接收每秒超過150個同時處於活動狀態的使用者資料包協定(UDP)連線。此選項預設為核取。

Attack Protection

<input checked="" type="checkbox"/>	SYN Flood Detect Rate	<input type="text" value="64"/>	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/>	Echo Storm	<input type="text" value="50"/>	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	ICMP Flood	<input type="text" value="50"/>	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	Block UDP Flood	<input type="text" value="500"/>	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/>	Block TCP Flood	<input type="text" value="100"/>	Connections per host (Range:0~10000, Default: 200)

步驟 9. 在Block UDP Flood欄位中輸入從0到10000的值。預設值為 1000。在此範例中，輸入的值為500，因此比較敏感。

Attack Protection

<input checked="" type="checkbox"/>	SYN Flood Detect Rate	<input type="text" value="64"/>	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/>	Echo Storm	<input type="text" value="50"/>	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	ICMP Flood	<input type="text" value="50"/>	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	Block UDP Flood	<input type="text" value="500"/>	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/>	Block TCP Flood	<input type="text" value="100"/>	Connections per host (Range:0~10000, Default: 200)

步驟 10. 驗證是否已選中Block TCP Flood竅取方塊以丟棄所有無效的傳輸控制協定(TCP)資料包。此選項預設為核取。

Attack Protection

<input checked="" type="checkbox"/>	SYN Flood Detect Rate	<input type="text" value="64"/>	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/>	Echo Storm	<input type="text" value="50"/>	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	ICMP Flood	<input type="text" value="50"/>	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/>	Block UDP Flood	<input type="text" value="500"/>	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/>	Block TCP Flood	<input type="text" value="100"/>	Connections per host (Range:0~10000, Default: 200)

步驟 11. 在Block TCP Flood欄位中輸入從0到10000的值，以保護您的網路免受SYN泛洪攻擊。預設值為 200。在本例中，輸入100，使其更加敏感。

Setting	Value	Unit / Range / Default
<input checked="" type="checkbox"/> SYN Flood Detect Rate	64	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/> Echo Storm	50	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> ICMP Flood	50	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> Block UDP Flood	500	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/> Block TCP Flood	100	Connections per host (Range:0~10000, Default: 200)

Buttons: Save, Cancel

步驟 12. 按一下Save。

Setting	Value	Unit / Range / Default
<input checked="" type="checkbox"/> SYN Flood Detect Rate	64	max/sec (Range: 0~10000, Default: 128)
<input checked="" type="checkbox"/> Echo Storm	50	ping pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> ICMP Flood	50	ICMP pkts/sec (Range: 0~10000, Default: 100)
<input checked="" type="checkbox"/> Block UDP Flood	500	Connections per host (Range:0~10000, Default: 1000)
<input checked="" type="checkbox"/> Block TCP Flood	100	Connections per host (Range:0~10000, Default: 200)

Buttons: Save, Cancel

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）。