

# Configureer aanvalsbescherming op de RV132W of RV134W VPN-router

## Doel

Met Attack Protection kunt u uw netwerk beveiligen tegen gebruikelijke soorten aanvallen zoals detectie, overstrooming en echostormen. Terwijl de router de Bescherming van de Aanval die door gebrek wordt toegelaten heeft, kunt u de parameters aanpassen om het netwerk gevoeliger en ontvankelijker aan aanvallen te maken het kan ontdekken.

Dit artikel laat zien hoe u Attack Protection kunt configureren op de RV132W en de RV134W VPN-router.

## Toepasselijke apparaten

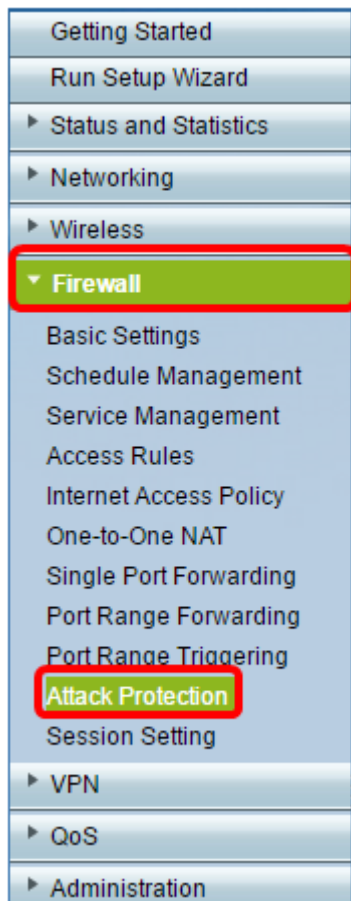
- RV 132 W
- RV134W

## Softwareversie

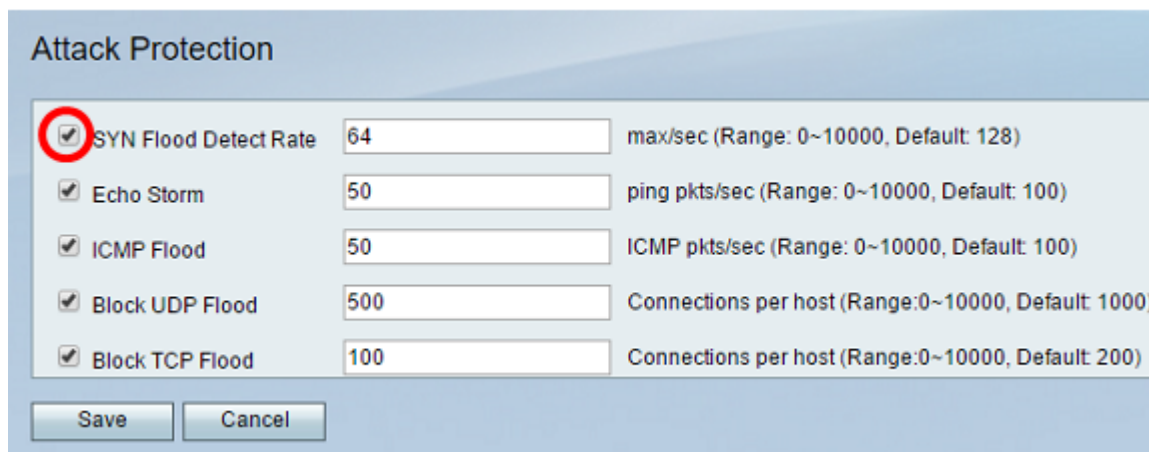
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

## Aanvalsbescherming configureren

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en kies **Firewall > Attack Protection**.



Stap 2. Controleer of het aanvinkvakje SYN Flood Detect Rate is ingeschakeld om er zeker van te zijn dat de functie actief is. Dit wordt standaard gecontroleerd.



Stap 3. Voer een waarde in bij het veld *SYN Flood Detect Rate*. De standaardwaarde is 128 SYN-pakketten per seconde. U kunt een waarde van 0 tot 10000 invoeren. Dit is het aantal SYN-pakketten per seconde dat ervoor zal zorgen dat het beveiligingstoestel bepaalt dat er een SYN-overstroming optreedt. Een waarde van nul geeft aan dat de functie SYN Flood Detection is uitgeschakeld. In dit voorbeeld is de ingevoerde waarde 64. Dit betekent dat het apparaat een SYN-overstroming met slechts 64 SYN-pakketten per seconde zal detecteren, waardoor het gevoeliger is dan de standaardconfiguratie.

**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)

Stap 4. Controleer of het aanvinkvakje Echo Storm is ingeschakeld om er zeker van te zijn dat de functie actief is. Dit wordt standaard gecontroleerd.

**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)

Stap 5. Voer een waarde in in het veld *Echo Storm*. De standaardwaarde is 100 pings per seconde. U kunt een waarde van 0 tot 10000 invoeren. Het aantal pings per seconde is dat ervoor zorgt dat het security apparaat bepaalt dat er een echostorm inbraakgebeurtenis optreedt. Een waarde van nul geeft aan dat de functie Echo Storm is uitgeschakeld.

**Opmerking:** in dit voorbeeld detecteert het apparaat een Echo-stormgebeurtenis met slechts 50 pings per seconde.

**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)

Stap 6. Controleer of het selectievakje Internet Control Message Protocol (ICMP) op Flood is ingeschakeld om er zeker van te zijn dat de functie actief is. Deze optie is standaard ingeschakeld.

**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)

Save Cancel

Stap 7. Voer een numerieke waarde in in het veld *ICMP-overstroming*. De standaardwaarde is 100 ICMP-pakketten per seconde. U kunt een waarde van 0 tot 10000 invoeren. Dit is het aantal ICMP-pakketten per seconde dat ervoor zal zorgen dat het security apparaat bepaalt dat er een ICMP-overstroming inbraakgebeurtenis plaatsvindt. Een waarde van nul geeft aan dat de functie ICMP-overstroming is uitgeschakeld.

**Opmerking:** in dit voorbeeld is de ingevoerde waarde 50, waardoor deze gevoeliger is voor ICMP-overstroming dan voor de standaardinstelling.

**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)

Save Cancel

Stap 8. Controleer of het aanvinkvakje Block UDP Flood (UDP) is ingeschakeld om ervoor te zorgen dat de functie actief is en om te voorkomen dat het security apparaat meer dan 150 gelijktijdige actieve User Datagram Protocol (UDP)-verbindingen per seconde accepteert vanaf één computer op het Local Area Network (LAN). Deze optie is standaard ingeschakeld.

**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)

Save Cancel

Stap 9. Voer een waarde in van 0 tot 10000 in het veld *UDP-overstroming blokkeren*. De

standaardwaarde is 1000. In dit voorbeeld is de ingevoerde waarde 500, waardoor deze gevoeliger is.

The screenshot shows the 'Attack Protection' configuration window. It contains five rows of settings, each with a checked checkbox, a text input field, and a label with a range and default value. The 'Block UDP Flood' row has a red box around the input field containing '500'. The other rows are: 'SYN Flood Detect Rate' (64, max/sec, Range: 0~10000, Default: 128), 'Echo Storm' (50, ping pkts/sec, Range: 0~10000, Default: 100), 'ICMP Flood' (50, ICMP pkts/sec, Range: 0~10000, Default: 100), and 'Block TCP Flood' (100, Connections per host, Range: 0~10000, Default: 200). At the bottom are 'Save' and 'Cancel' buttons.

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

Stap 10. Controleer of het aanvinkvakje Block TCP Flood is ingeschakeld om alle ongeldige TCP-pakketten (Transmission Control Protocol) te laten vallen. Deze optie is standaard ingeschakeld.

The screenshot shows the 'Attack Protection' configuration window. The checkbox for 'Block TCP Flood' is highlighted with a red circle. The other settings are the same as in the previous screenshot. The 'Save' and 'Cancel' buttons are at the bottom.

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

Stap 11. Voer een waarde in van 0 tot 10000 in het veld *Block TCP Flood* om uw netwerk te beschermen tegen een SYN flood aanval. De standaardwaarde is 200. In dit voorbeeld worden er 100 ingevoerd, waardoor het gevoeliger wordt.

The screenshot shows the 'Attack Protection' configuration window. The 'Block TCP Flood' input field is highlighted with a red box and contains the value '100'. The other settings are the same as in the previous screenshot. The 'Save' and 'Cancel' buttons are at the bottom.

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

Stap 12. Klik op **Save** (Opslaan).

### 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)

U moet nu met succes Attack Protection op uw RV132W of RV134W router hebben geconfigureerd.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.