

Configure a proteção contra ataques no roteador VPN RV132W ou RV134W

Objetivo

A proteção contra ataques permite que você proteja sua rede contra tipos comuns de ataques, como descoberta, inundação e tempestades de eco. Embora o roteador tenha a proteção contra ataques ativada por padrão, você pode ajustar os parâmetros para tornar a rede mais sensível e mais responsiva aos ataques que ela possa detectar.

Este artigo tem como objetivo mostrar como configurar a Proteção contra Ataque no RV132W e no Roteador VPN RV134W.

Dispositivos aplicáveis

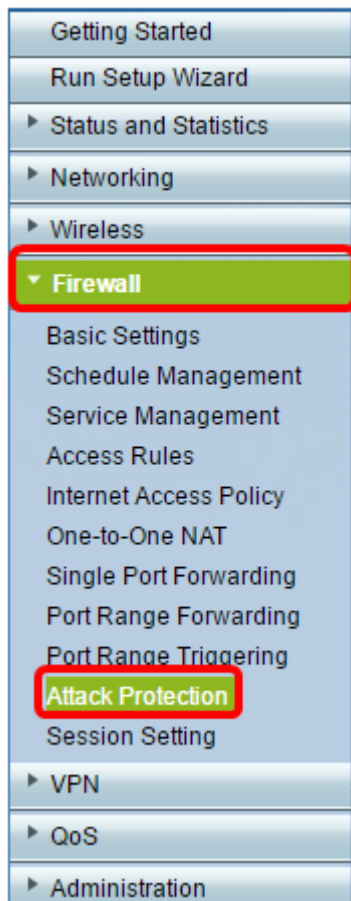
- RV 132 W
- RV134W

Versão de software

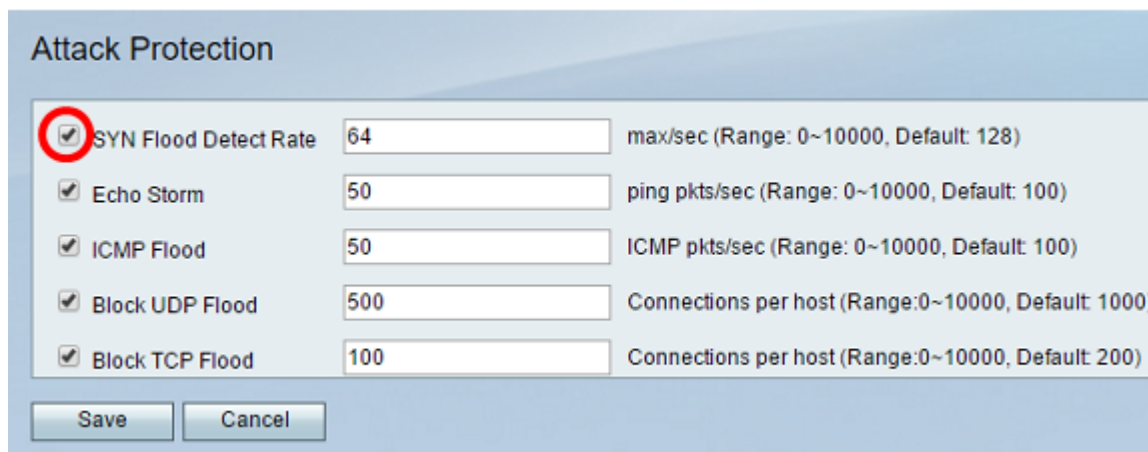
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

Configurar a proteção contra ataques

Etapa 1. Faça login no utilitário baseado na Web e escolha **Firewall > Attack Protection**.



Etapa 2. Verifique se a caixa de seleção SYN Flood Detect Rate está marcada para garantir que o recurso esteja ativo. Essa opção é marcada por padrão.



Etapa 3. Informe um valor no campo *SYN Flood Detect Rate*. O valor padrão é 128 pacotes SYN por segundo. Você pode digitar um valor de 0 a 10000. Será o número de pacotes SYN por segundo que fará com que o Security Appliance determine que uma invasão de inundação SYN está ocorrendo. Um valor zero indicará que o recurso Detecção de Inundação SYN está desabilitado. Neste exemplo, o valor inserido é 64. Isso significa que o dispositivo detectaria uma invasão de inundação SYN em apenas 64 pacotes SYN por segundo, tornando-a mais sensível do que a configuração padrão.

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)

Etapa 4. Verifique se a caixa de seleção Tempestade de eco está marcada para garantir que o recurso esteja ativo. Essa opção é marcada por padrão.

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)

Etapa 5. Insira um valor no campo *Echo Storm*. O valor padrão é 100 pings por segundo. Você pode digitar um valor de 0 a 10000. Será o número de pings por segundo que fará com que o Security Appliance determine que um evento de intrusão de tempestade de eco está ocorrendo. Um valor zero indicará que o recurso Tempestade de Eco está desativado.

Observação: neste exemplo, o equipamento detectaria um evento de Echo Storm a apenas 50 pings por segundo.

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)

Etapa 6. Verifique se a caixa de seleção Inundação do Internet Control Message Protocol (ICMP) está marcada para garantir que o recurso esteja ativo. Este recurso está marcado por padrão.

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

Passo 7. Insira um valor numérico no campo *Inundação ICMP*. O valor padrão é 100 pacotes ICMP por segundo. Você pode digitar um valor de 0 a 10000. Será o número de pacotes ICMP por segundo que fará com que o Security Appliance determine que um evento de invasão de inundação ICMP está ocorrendo. Um valor zero indicará que o recurso Inundação ICMP está desabilitado.

Observação: neste exemplo, o valor inserido é 50, tornando-o mais sensível à inundação de ICMP do que sua configuração padrão.

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

Etapa 8. Verifique se a caixa de seleção Bloquear Inundação de UDP está marcada para garantir que o recurso esteja ativo e para impedir que o Security Appliance aceite mais de 150 conexões simultâneas ativas de Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol) por segundo de um único computador na Rede Local (LAN - Local Area Network). Essa opção é marcada por padrão.

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

Etapa 9. Insira um valor de 0 a 10000 no campo *Block UDP Flood*. O valor padrão é 1000.

Neste exemplo, o valor inserido é 500, tornando-o mais sensível.

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 the value '500' entered in the text input field, which is highlighted with a red rectangular box. The other rows are: 'SYN Flood Detect Rate' (64), 'Echo Storm' (50), 'ICMP Flood' (50), and 'Block TCP Flood' (100). At the bottom, there are 'Save' and 'Cancel' buttons.

Option	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)

Etapa 10. Verifique se a caixa de seleção Bloquear Inundação de TCP está marcada para descartar todos os pacotes TCP inválidos. Essa opção é marcada por padrão.

The screenshot shows the 'Attack Protection' configuration window. The 'Block TCP Flood' checkbox is highlighted with a red circle. The value '100' is entered in the text input field next to it. The other settings are the same as in the previous screenshot. At the bottom, there are 'Save' and 'Cancel' buttons.

Option	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)

Etapa 11. Insira um valor de 0 a 10000 no campo *Block TCP Flood* para proteger sua rede de um ataque de inundação SYN. O valor padrão é 200. Neste exemplo, 100 é inserido, tornando-o mais sensível.

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

Option	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)

Etapa 12. Click **Save**.

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)

Agora você deve ter configurado com êxito a Proteção contra ataques em seu roteador RV132W ou RV134W.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.