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

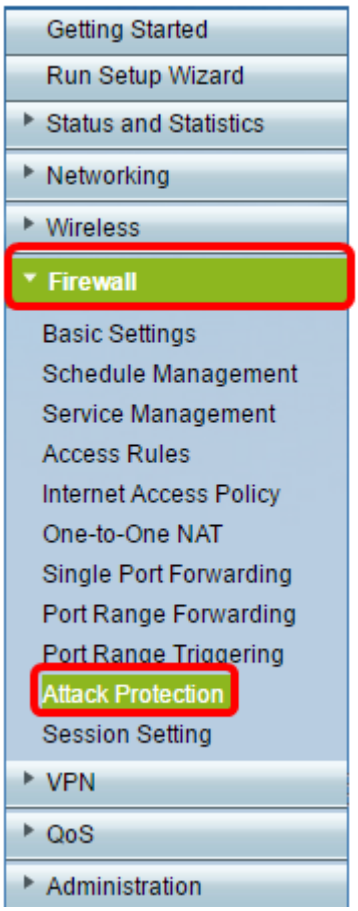
- RV 132 W
- RV134W

Versão de software

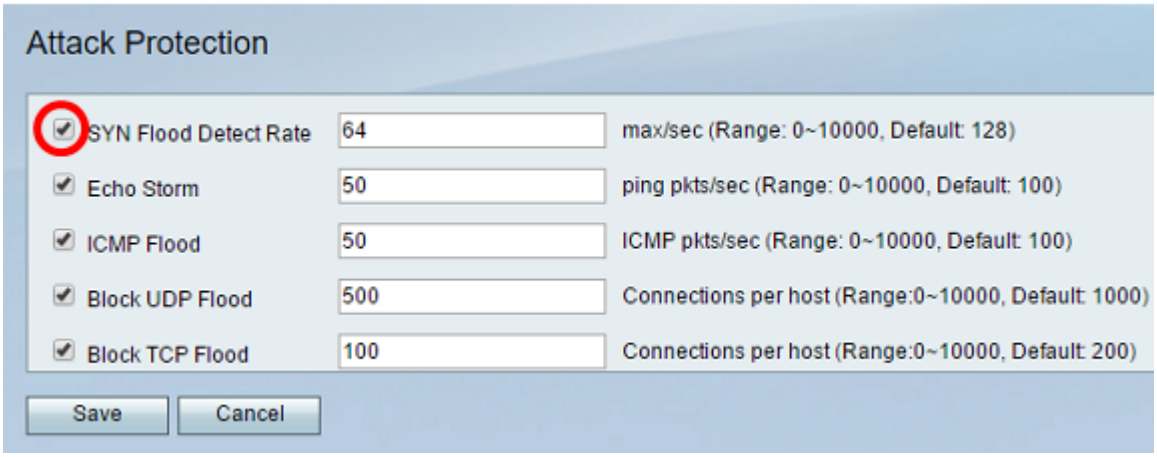
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

Configurar a proteção contra ataques

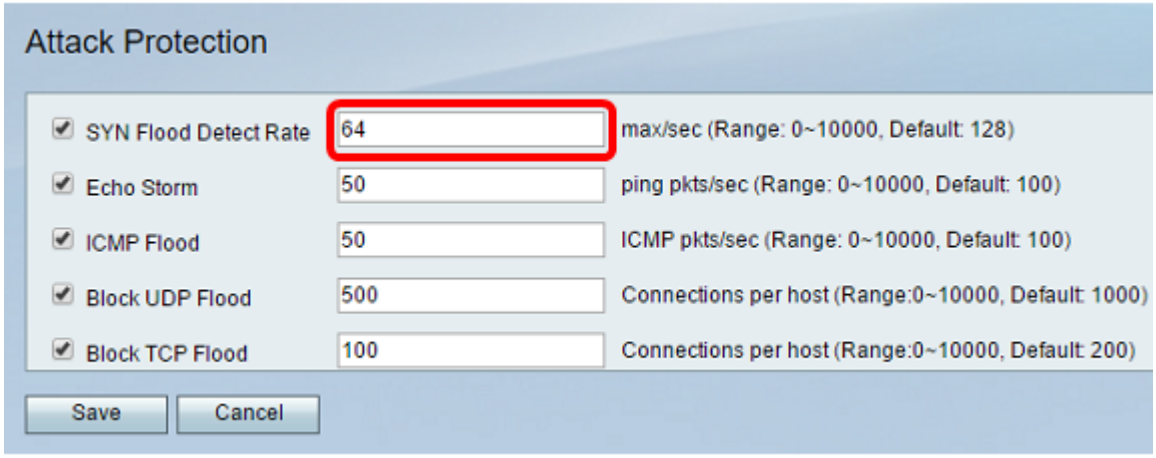
Etapa 1. Faça login no utilitário baseado na Web e escolha **Firewall > Attack Protection**.



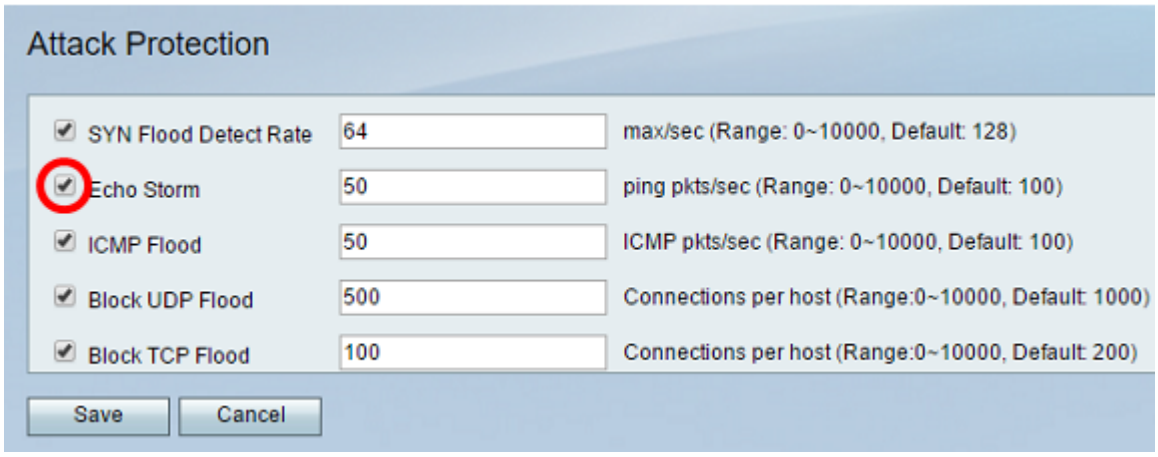
Etapa 2. Verifique se a caixa de seleção SYN Flood Detect Rate está marcada para garantir que o recurso esteja ativo. Essa opção é marcada por padrão.



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.

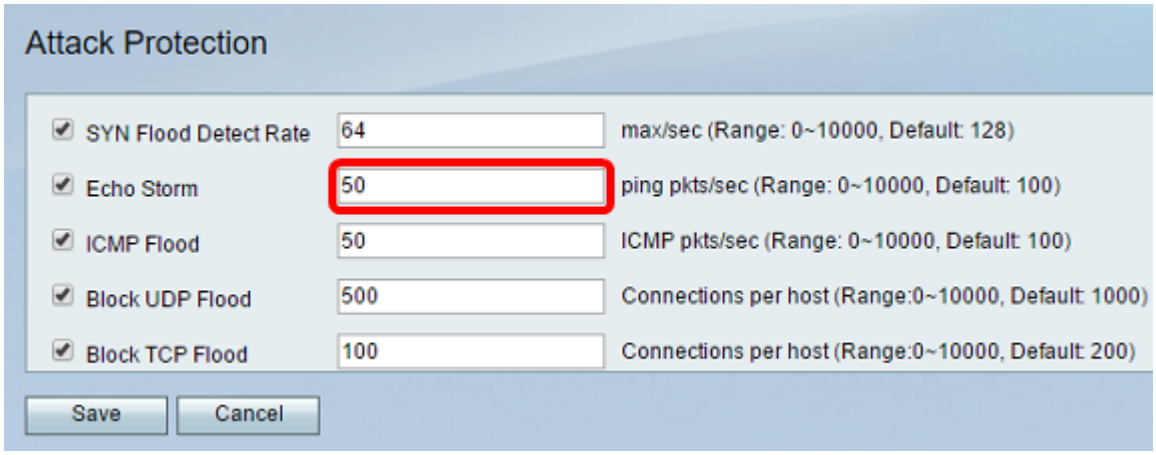


Etapa 4. Verifique se a caixa de seleção Tempestade de eco está marcada para garantir que o recurso esteja ativo. Essa opção é marcada por padrão.

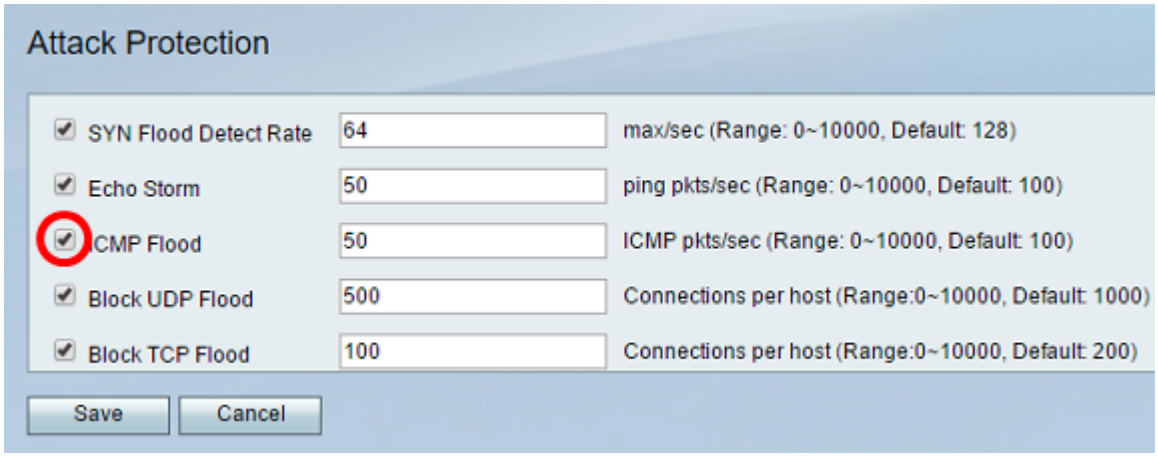


Etapa 5. Insira um valor no campo *Echo Storm*. O valor padrão é 100 pings por segundo. Você pode digitar um valor de 0 a 10000. Será o número de pings por segundo que fará com que o Security Appliance determine que um evento de intrusão de tempestade de eco está ocorrendo. Um valor zero indicará que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

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

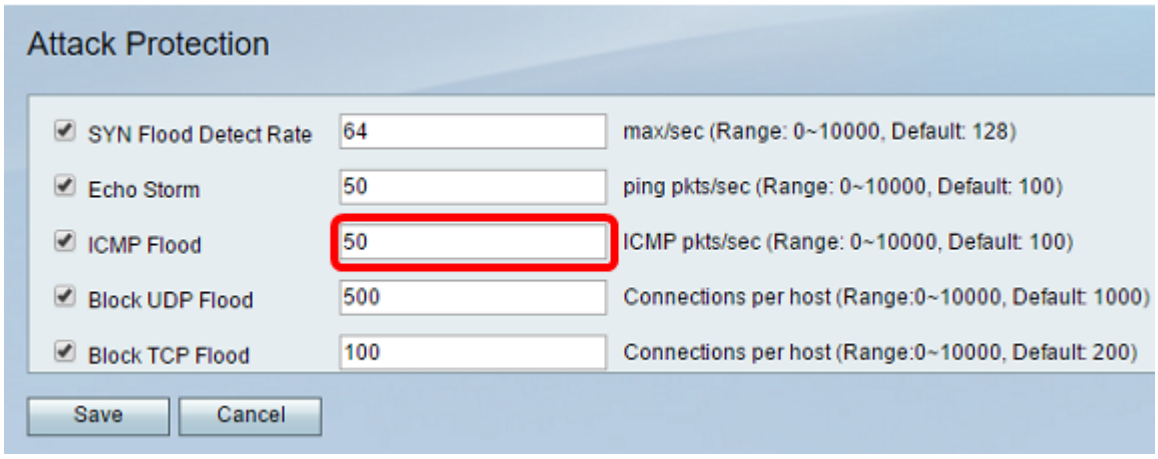


Etapa 6. Verifique se a caixa de seleção Inundação do Internet Control Message Protocol (ICMP) está marcada para garantir que o recurso esteja ativo. Este recurso está marcado por padrão.

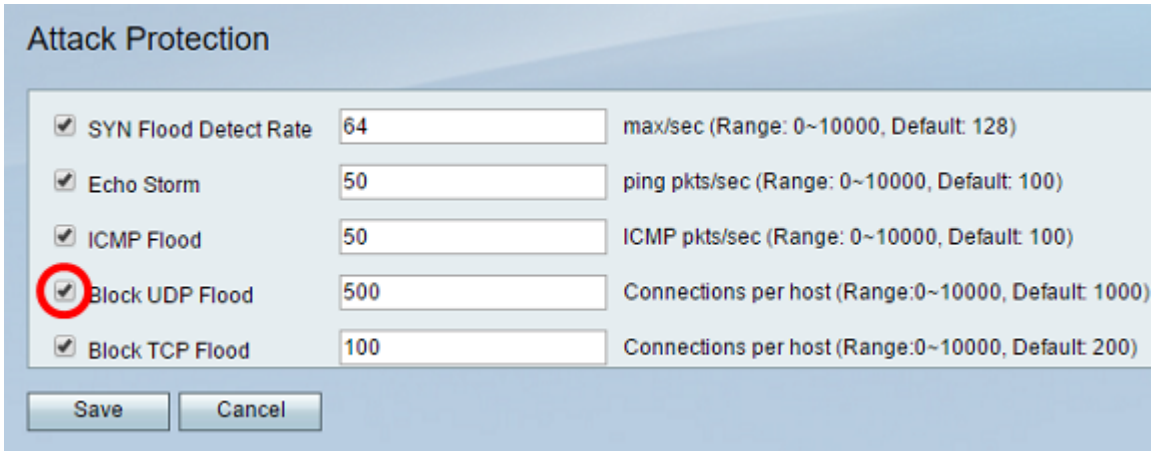


Passo 7. Insira um valor numérico no campo *Inundação ICMP*. O valor padrão é 100 pacotes ICMP por segundo. Você pode digitar um valor de 0 a 10000. Será o número de pacotes ICMP por segundo que fará com que o Security Appliance determine que um evento de invasão de inundação ICMP está ocorrendo. Um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

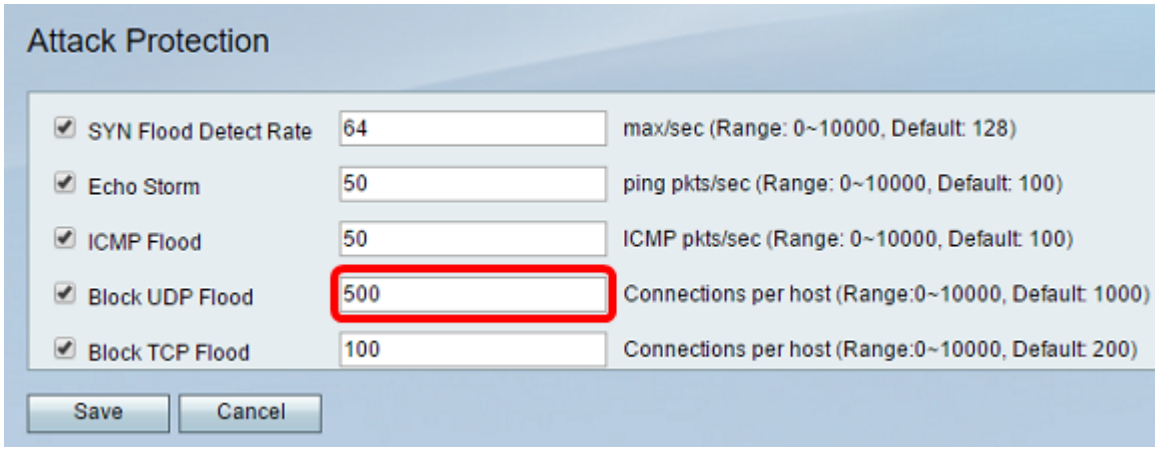


Etapa 8. Verifique se a caixa de seleção Bloquear Inundação de UDP está marcada para garantir que o recurso esteja ativo e para impedir que o Security Appliance aceite mais de 150 conexões simultâneas ativas de Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol) por segundo de um único computador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

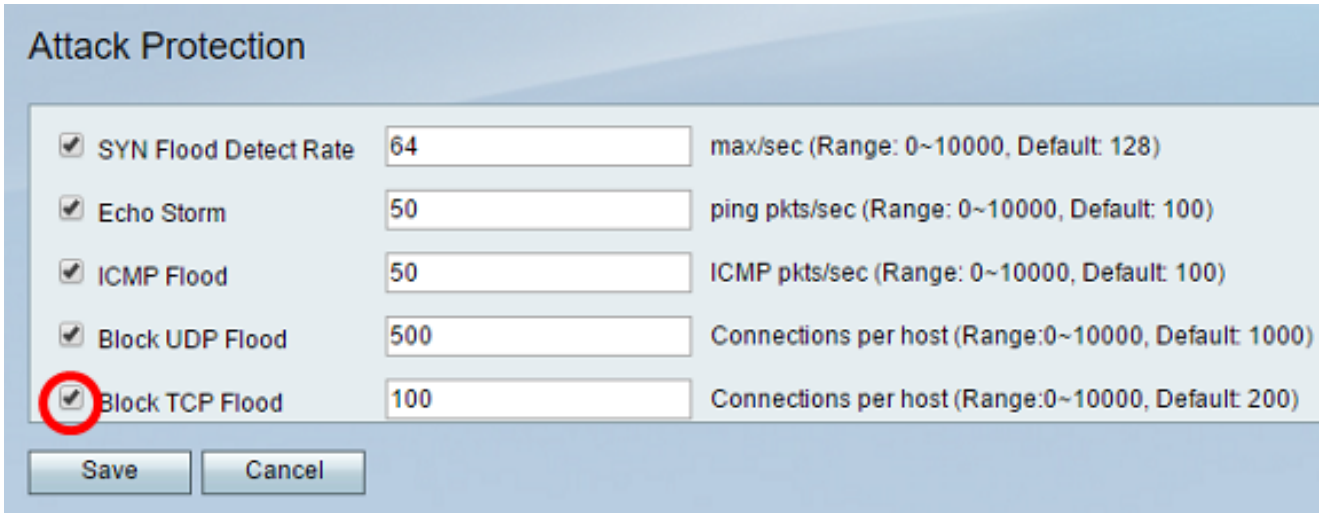


Etapa 9. Insira um valor de 0 a 10000 no campo *Block UDP Flood*. O valor padrão é 1000.

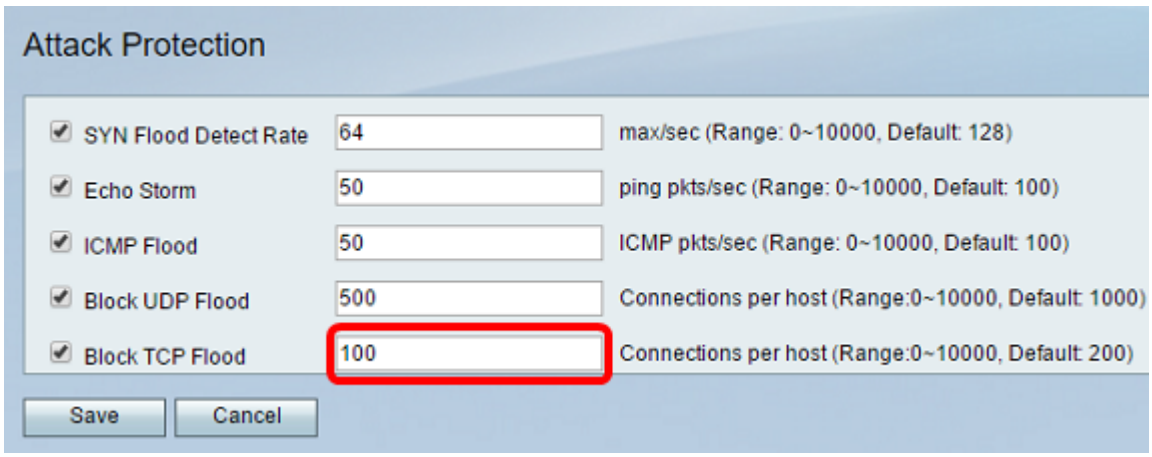
Neste exemplo, o valor inserido é 500, tornando-o mais sensível.



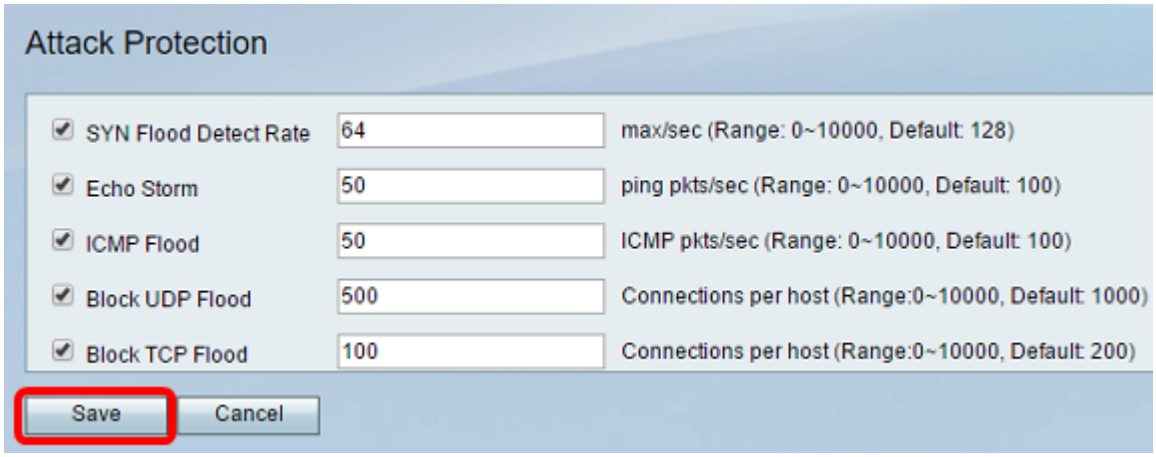
Etapa 10. Verifique se a caixa de seleção Bloquear Inundação de TCP está marcada para descartar todos os pacotes TCP inválidos. Essa opção é marcada por padrão.



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.



Etapa 12. Click **Save**.



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.