Defina as configurações básicas do firewall no RV34x Series Router

Objetivo

O objetivo deste artigo é explicar como configurar as configurações básicas de firewall no RV34x Series Router.

Introduction

O objetivo principal de um firewall é controlar o tráfego de rede de entrada e saída analisando os pacotes de dados e determinando se eles devem ou não ser permitidos com base em um conjunto de regras predeterminado. Um roteador é considerado um firewall de hardware forte devido a funções que permitem a filtragem de dados de entrada. Um firewall de rede cria uma ponte entre uma rede interna que se supõe ser segura e confiável e outra rede, geralmente uma internetwork externa, como a Internet, que se supõe não ser segura e não confiável.

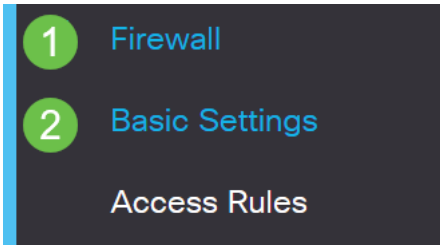
Dispositivos aplicáveis | Versão do firmware

- Série RV34x | 1.0.03.21 (Download da versão mais recente)

Definir configurações básicas do firewall

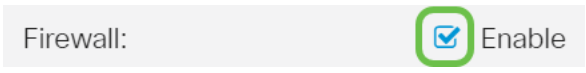
Passo 1

Faça login na Interface de usuário da Web (UI) e escolha **Firewall >Basic Settings**.



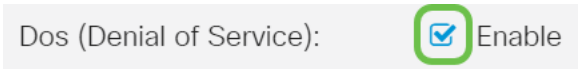
Passo 2

Marque a caixa de seleção **Enable** Firewall (Ativar firewall) para ativar o recurso Firewall. Iss está habilitado por padrão.



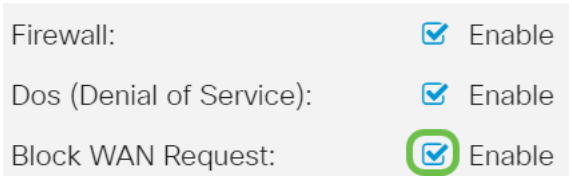
Etapa 3

Marque a caixa de seleção **Habilitar** dos (Negação de serviço) para proteger sua rede contra ataques de DoS. Iss está habilitado por padrão.



Passo 4

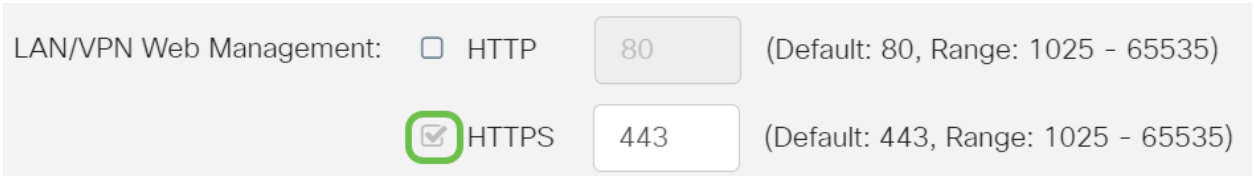
Marque a caixa de seleção **Enable** Block WAN Request para negar solicitações de ping ao RV34x Series Router. Iss está habilitado por padrão.



Etapa 5

Na área LAN/VPN Web Management, marque a caixa de seleção **HTTP** e/ou **HTTPS** para ativar o tráfego desses protocolos. Para este exemplo, a caixa de seleção HTTPS está marcada.

- HTTP — O Hyper Text Transfer Protocol é um protocolo de transferência de dados usado na Internet.
- HTTPS — O protocolo de transferência de Hyper Text Secure é uma versão segura do HTTP que criptografa pacotes para aumentar a segurança.

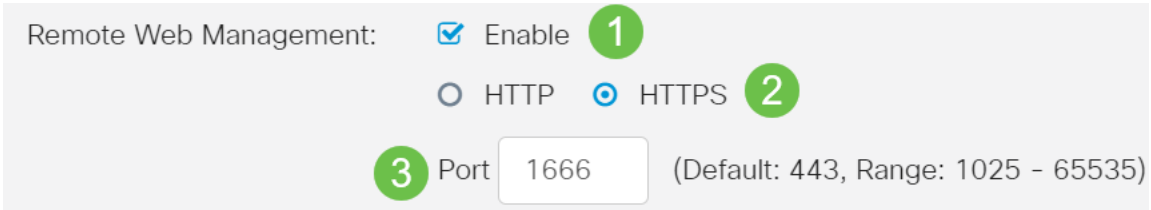


Etapa 6 (Opcional)

Marque a caixa de seleção **Habilitar** Gerenciamento Remoto da Web para habilitar o gerenciamento remoto. Caso contrário, vá para o passo 8.

Escolha o tipo de protocolo usado para se conectar ao firewall escolhendo um botão de opção. As opções são **HTTP** e **HTTPS**.

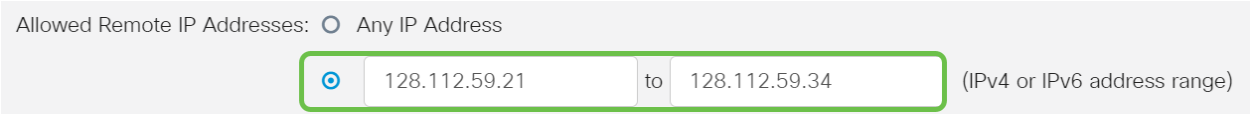
Insira um número de porta que varie entre 1025 e 65535, o que é permitido para o gerenciamento remoto. O padrão é 443. Neste exemplo, 1666 é usado.



Etapa 7

Na área Allowed Remote IP Addresses (Endereços IP remotos permitidos), escolha

um botão de opção para permitir que qualquer endereço IP acesse a rede remotamente ou para especificar um intervalo de endereços IPv4 ou IPv6. Para este exemplo, foi escolhido um Intervalo de IP. Neste exemplo, o endereço IP inicial é 128.112.59.21 e o endereço IP final é 128.112.59.34.



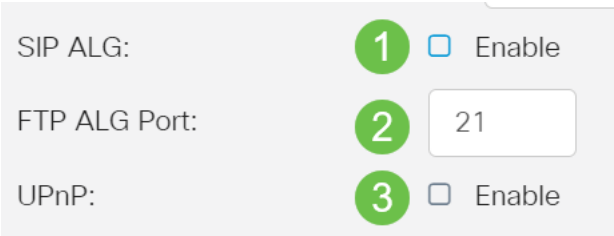
Etapa 8 (Opcional)

Marque a caixa de seleção **Habilitar** ALG SIP para habilitar o Session Initiation Protocol (SIP) Application Layer Gateway (ALG) para passar pelo Firewall. Esse recurso pode ser ativado para ajudar os pacotes SIP a passar pelo firewall. Um pacote SIP é usado para iniciar conexões de tráfego de voz. Se o seu provedor de VoIP usar um protocolo de passagem de Conversão de Endereço de Rede (NAT - Network Address Translation) diferente, esse recurso poderá ser desabilitado, que é a configuração padrão.

Especifique a porta FTP de SIP ALG no campo *Porta ALG FTP*. O padrão é 21.

Marque a caixa de seleção **Habilitar** UPnP para habilitar o UPnP (Universal Plug and Play). Por padrão, este recurso está desabilitado.

Para este exemplo, essas opções são mantidas desabilitadas.



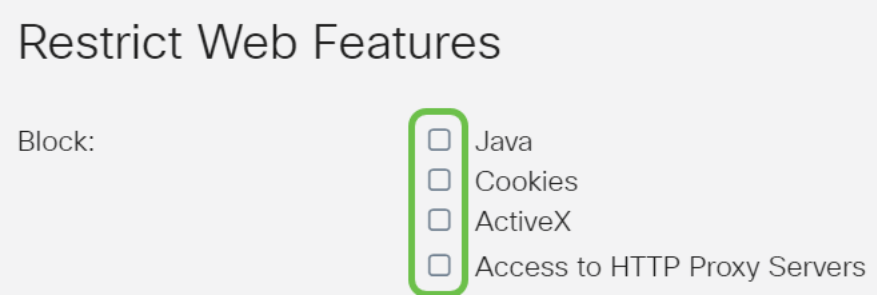
Etapa 9 (Opcional)

Na área Restringir recurso da Web, marque as caixas de seleção dos tipos de recursos da Web a serem bloqueados na área Bloquear. Por padrão, essas caixas de seleção são desativadas. As opções são:

Java — Todos os elementos da Web que contêm esse tipo de elemento da Web serão bloqueados. Essa configuração pode ajudar a evitar ataques da Web baseados em Java.
Cookies — Cookies são dados armazenados no computador para ajudar os sites a entender quem os está acessando. Bloqueá-los pode impedir que cookies mal-intencionados acessem dados.
AtiveX — é um plug-in desenvolvido pela Microsoft para melhorar a experiência de navegação. Bloqueá-lo pode impedir que plug-ins AtiveX mal-intencionados prejudiquem os dispositivos de rede.
Acesso ao servidor proxy HTTP — os servidores proxy HTTP ocultam detalhes de usuários finais de hackers. Eles funcionam como intermediários para que um cliente não acesse a Internet diretamente. No entanto, se os usuários locais tiverem acesso aos servidores proxy de WAN, poderão encontrar uma maneira de contornar os filtros

de conteúdo no roteador para acessar sites da Internet bloqueados pelo roteador.

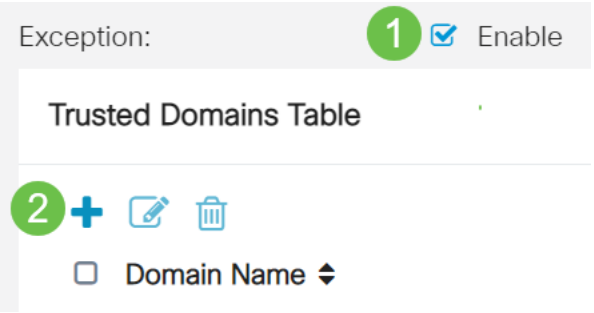
Para este exemplo, as caixas de seleção são deixadas desabilitadas.



Etapa 11 (Opcional)

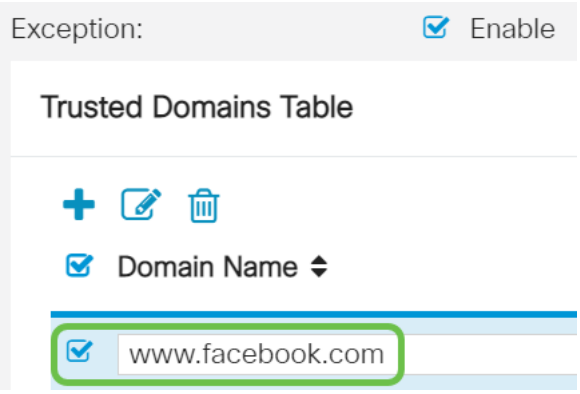
Marque a caixa de seleção **Enable** Exception para permitir somente recursos da Web selecionados, como Java, Cookies, AtiveX ou Acesso a servidores proxy HTTP e restringir todos os outros. Por padrão, isso é desativado. Para este exemplo, ele é deixado desabilitado.

Na Tabela Domínios confiáveis, clique no **ícone Adicionar** para adicionar domínios confiáveis ou com permissão para acessar na rede.



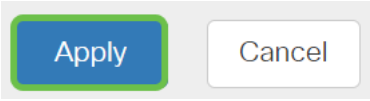
Etapa 12

No campo *Domain Name*, insira um nome de domínio para o qual será concedido acesso à rede. Para este exemplo, www.facebook.com é usado.



Passo 13

Clique em Apply.



Etapa 14 (Opcional)

Para salvar a configuração permanentemente, vá para a página Copiar/salvar configuração ou clique no **ícone salvar** na parte superior da página.

Conclusão

Agora você deve ter configurado com êxito as configurações básicas de firewall no seu roteador RV34x Series.