Configuração básica de firewall nos roteadores RV320 e RV325

Objetivo

Este artigo explica como definir as configurações básicas de firewall no RV32x VPN Router Series.

Um firewall é um conjunto de recursos projetados para manter uma rede segura. Um roteador é considerado um firewall de hardware forte. Isso se deve ao fato de que os roteadores podem inspecionar todo o tráfego de entrada e descartar todos os pacotes indesejados. Os firewalls de rede protegem uma rede de computadores interna (casa, escola, intranet empresarial) contra o acesso mal-intencionado externo. Os firewalls de rede também podem ser configurados para limitar o acesso externo de usuários internos.

Dispositivos aplicáveis

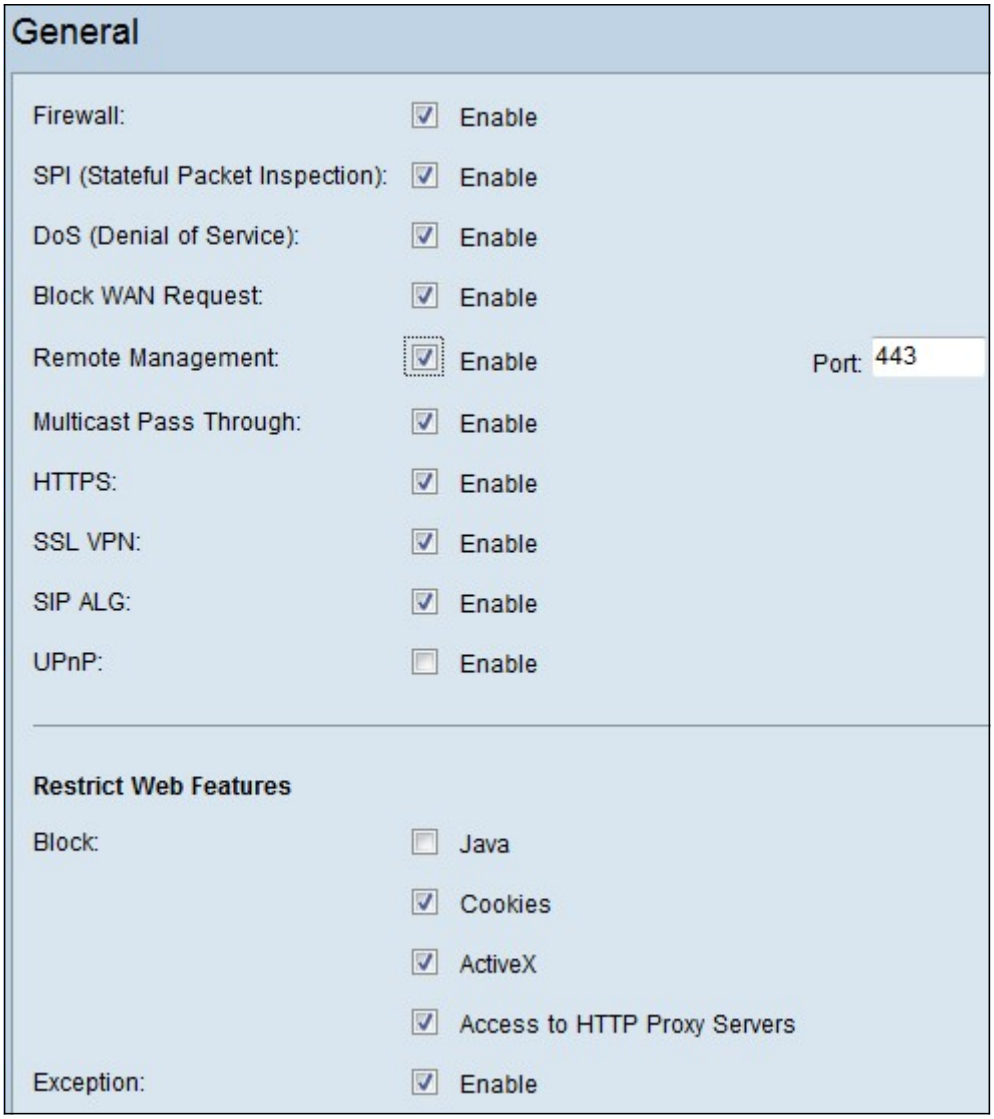
- Roteador VPN WAN duplo RV320
- Roteador VPN WAN duplo RV325 Gigabit

Versão de software

- v1.1.0.09

Configurações básicas

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Firewall > General**. A página *Geral* é aberta:



Etapa 2. Com base nos seus requisitos, marque a caixa de seleção **Habilitar** que corresponde aos recursos que você deseja habilitar.

- Firewall — Os firewalls do roteador podem ser desligados (desativados) ou podem ser habilitados para filtrar certos tipos de tráfego de rede por meio das chamadas regras de firewall. Um firewall pode ser usado para filtrar todo o tráfego de entrada e saída e com base.
- SPI (Stateful Packet Inspection) — Monitora o estado das conexões de rede, como fluxos TCP e comunicação UDP. O firewall distingue pacotes legítimos para diferentes tipos de conexões. Apenas os pacotes que correspondem a uma conexão ativa conhecida são permitidos pelo firewall, todos os outros são rejeitados.
- DoS (Denial of Service, Negação de serviço) — Usado para proteger uma rede de um ataque de negação de serviço distribuído (DDoS). Os ataques de DDoS têm o objetivo de inundar uma rede até o ponto em que os recursos da rede ficam indisponíveis. O RV320 usa proteção DoS para proteger a rede através da restrição e remoção de pacotes indesejados.
- Block WAN Request (Bloquear solicitação de WAN) — Bloqueia todas as solicitações de ping para o roteador a partir da porta WAN.
- Gerenciamento remoto — Permite acesso ao roteador a partir de uma rede WAN remota.
  - Porta — insira um número de porta para gerenciar remotamente.
- Multicast Pass Through — Permite que mensagens de multicast IP passem pelo dispositivo.
- HTTPS (Hypertext Transfer Protocol Secure) — É um protocolo de comunicação para comunicação segura em uma rede de computadores. Ele fornece criptografia bidirecional de

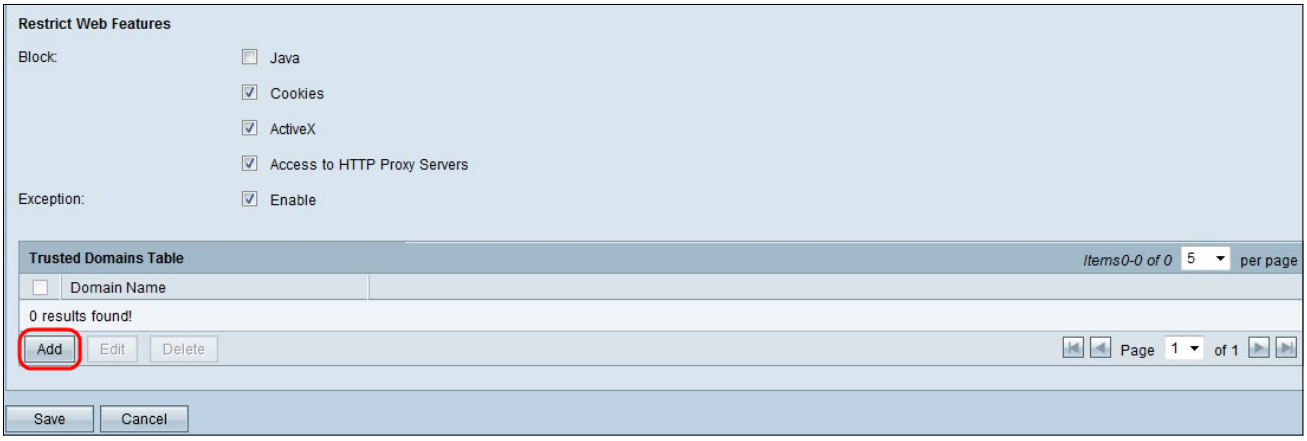
cliente e servidor.
- SSL VPN — Permite uma conexão VPN SSL feita através do roteador.
- ALG SIP — O SIP ALG oferece funcionalidade que permite o tráfego de Voz sobre IP que vai do lado privado para o público e do lado privado para o lado privado do firewall quando o endereço de rede e a conversão de porta (NAPT) são usados. O NAPT é o tipo mais comum de conversão de endereço de rede.
- UPnP (Universal Plug and Play) — Permite a descoberta automática de dispositivos que podem se comunicar com o roteador.

Etapa 3. Com base nos seus requisitos, marque a caixa de seleção **Habilitar** que corresponde aos recursos que você deseja bloquear.

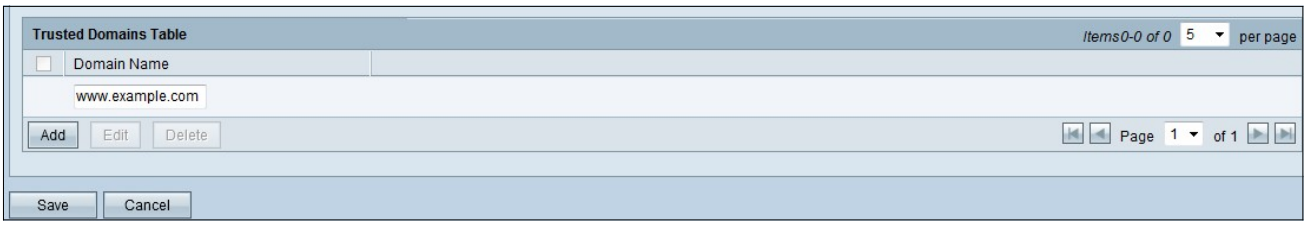
- Java — Marcar esta caixa de seleção impede que os miniaplicativos Java sejam baixados e executados. O Java é uma linguagem de programação comum usada por muitos sites. No entanto, os miniaplicativos java feitos para fins mal-intencionados podem representar uma ameaça à segurança de uma rede. Após o download, um miniaplicativo java hostil pode explorar recursos de rede.
- Cookies — Cookies são criados por sites para armazenar informações sobre usuários. Os cookies podem rastrear o histórico do usuário na Web, o que pode levar a uma invasão de privacidade.
- AtiveX — AtiveX é um tipo de miniaplicativo usado por muitos sites. Embora geralmente seguro, quando um miniaplicativo AtiveX mal-intencionado é instalado em um computador, ele pode fazer qualquer coisa que um usuário possa fazer. Ele pode inserir código prejudicial no sistema operacional, navegar em uma intranet segura, alterar uma senha ou recuperar e enviar documentos.
- Acesso a servidores proxy HTTP — Os servidores proxy são servidores que fornecem um link entre duas redes separadas. Os servidores proxy mal-intencionados podem gravar todos os dados não criptografados enviados a eles, como logins ou senhas.
- Exceção — Permite os recursos selecionados (Java, Cookies, AtiveX ou Acesso a servidores proxy HTTP), mas restringe todos os recursos não selecionados em domínios confiáveis configurados. Um domínio que é confiável e tem acesso à rede confiável. Você pode configurar um domínio confiável que permita aos usuários de um domínio externo acessar seus recursos de rede. Se esta opção estiver desabilitada, um domínio confiável permitirá todos os recursos.

Note: Economizador de tempo: se você não marcou a caixa de seleção Exceção, ignore a etapa 4 .

Etapa 4. Clique em Adicionar, insira um novo domínio confiável e clique em Salvar para criar um domínio confiável.

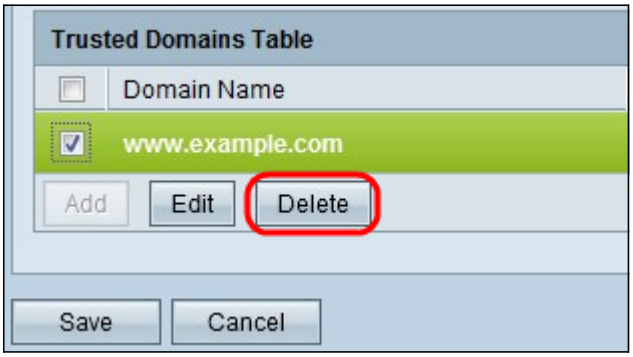


Etapa 5. Clique em Salvar para atualizar as alterações.



Etapa 6. (Opcional) Para Editar o nome do domínio confiável, marque a caixa de seleção do domínio confiável que deseja editar, clique em Editar, edite o nome do domínio e clique em Salvar.

Passo 7. (Opcional) Para excluir um domínio na lista Domínio confiável, marque a caixa de seleção do domínio confiável que deseja excluir e clique em Excluir.



Exibir um vídeo relacionado a este artigo...

Clique aqui para ver outras palestras técnicas da Cisco