Defina as configurações gerais de firewall em RV016, RV042, RV042G e RV082

Objetivo

Por padrão, o firewall integrado para RV016, RV042, RV042G e RV082 bloqueia determinados tipos de tráfego. Os tipos de tráfego bloqueados, como HTTPS, solicitações TCP e ICMP e tráfego de gerenciamento remoto, podem ser ajustados. O próprio firewall também pode ser ativado ou desativado. Além disso, certos aspectos dos sites que podem ser vulnerabilidades de segurança também podem ser bloqueados. Esses recursos do site, quando desbloqueados, podem armazenar dados potencialmente prejudiciais em seu computador.

O objetivo deste documento é mostrar como definir as configurações gerais de firewall no RV016, RV042, RV042G e RV082.

Dispositivos aplicáveis

â€¢RV016

â€¢RV042

â€¢RV042G

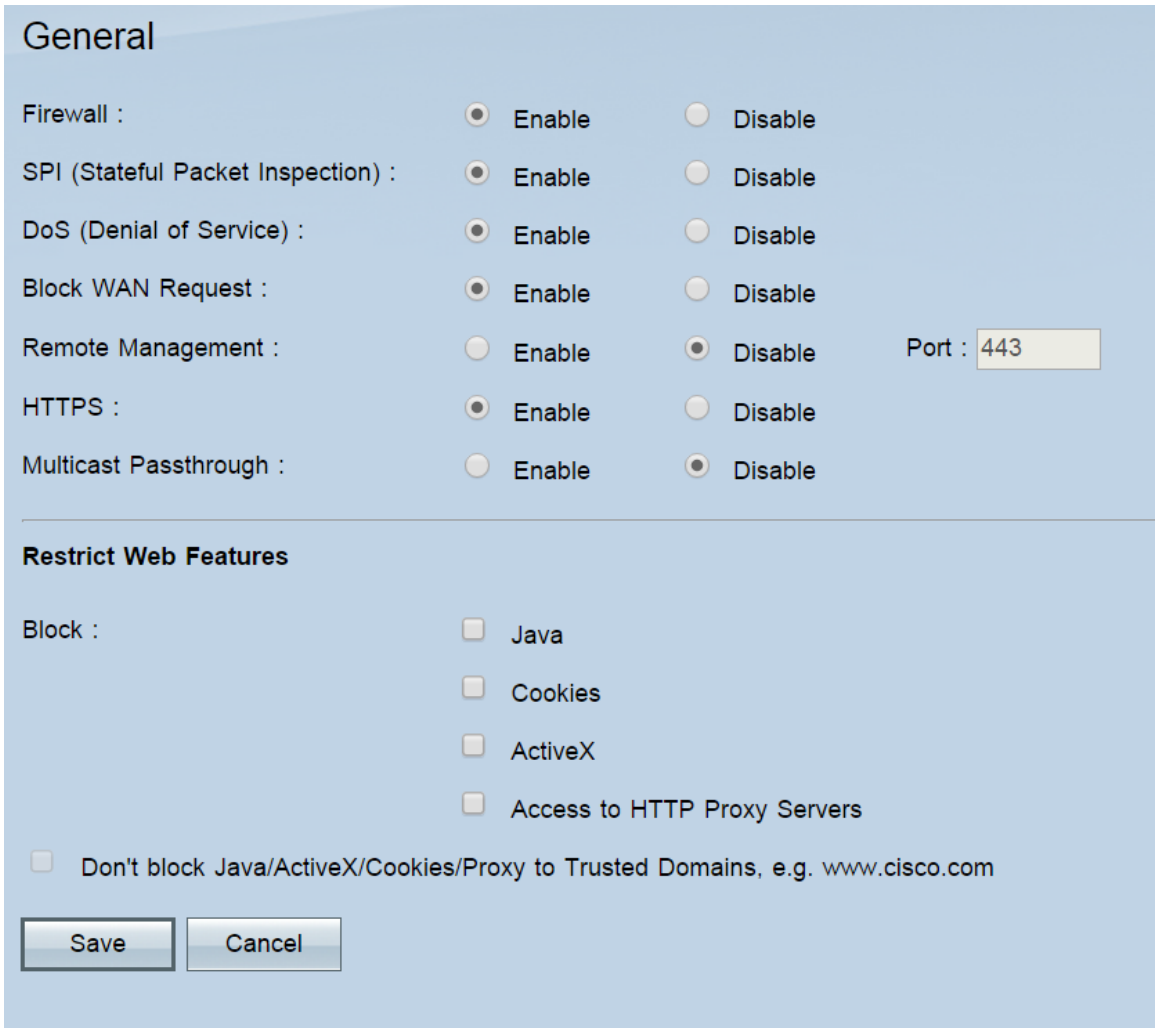
â€¢RV082

Versão de software

â€¢v4.2.3.06

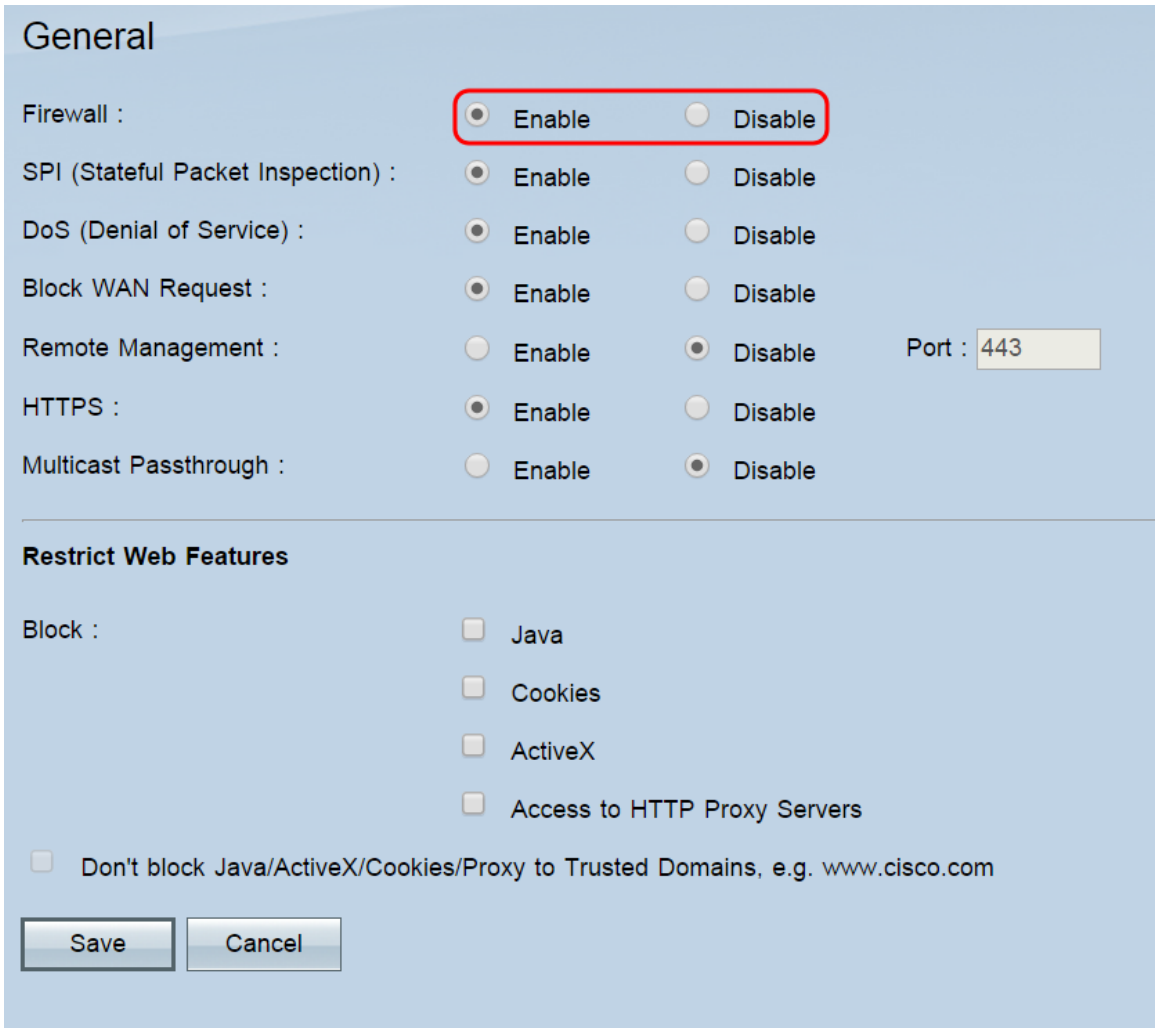
Definindo configurações gerais de firewall

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



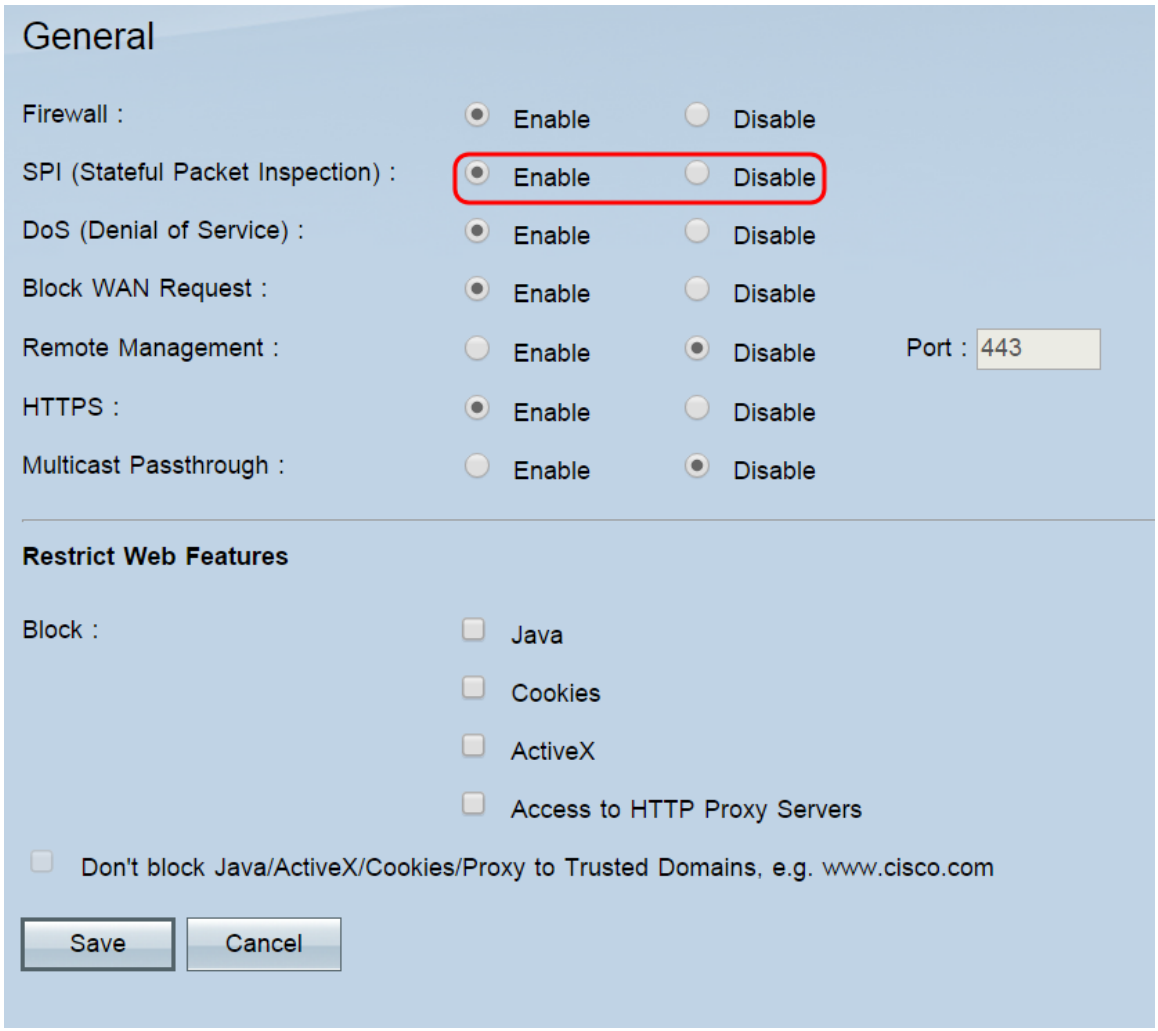
Recursos gerais

Etapa 1. No campo *Firewall*, selecione um botão de opção para **Ativar** ou **Desativar** o firewall. O firewall está ativado por padrão; não é recomendável desativá-lo. Desativar o firewall também desativa as Regras de acesso e os Filtros de conteúdo.

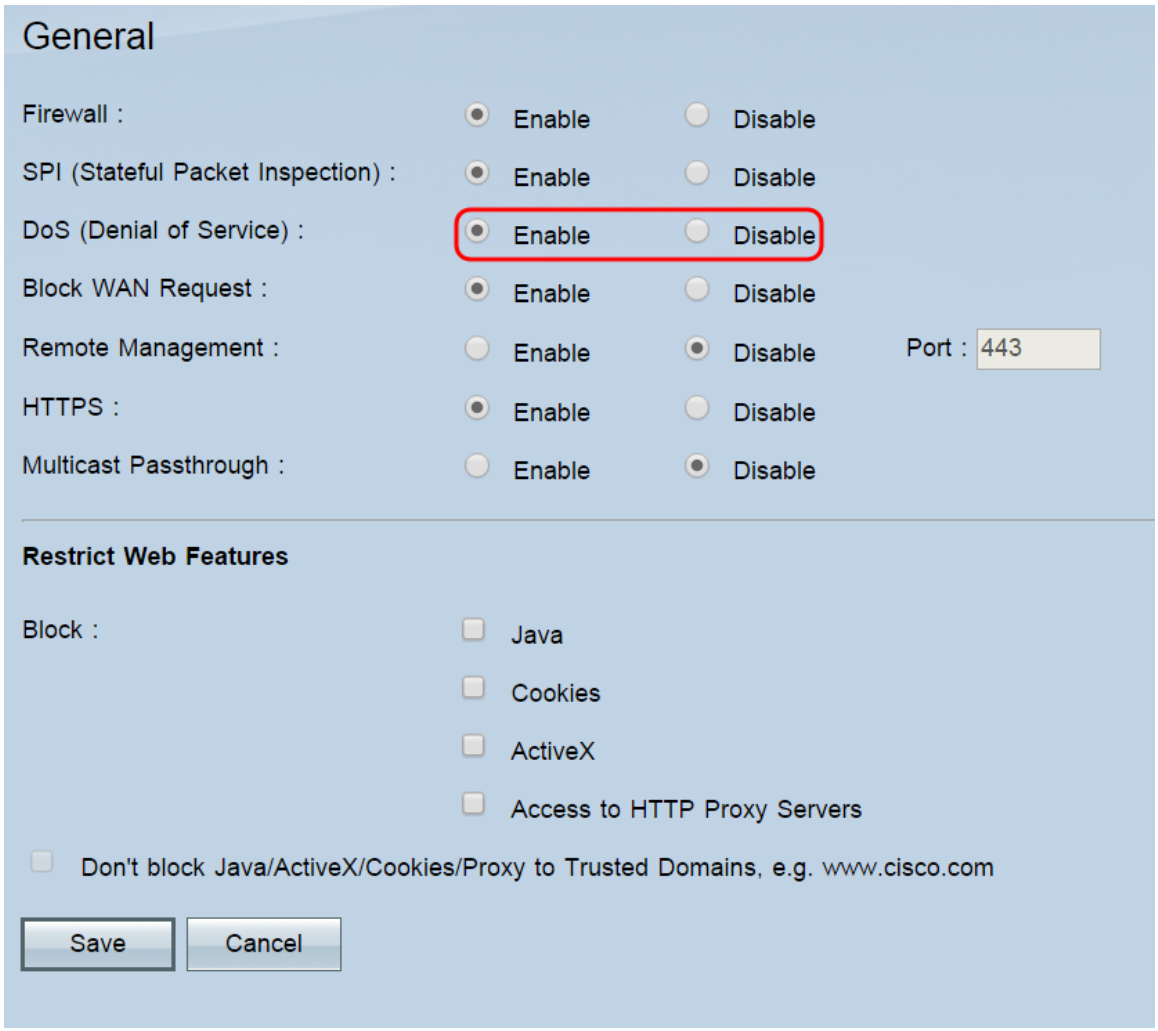


Observação: se você quiser desativar o firewall e ainda estiver usando a senha de administrador padrão, uma mensagem será exibida avisando que você precisa alterar a senha; você não poderá desativar o firewall até fazer isso. Clique em **OK** para continuar na página de senha ou em **Cancelar** para permanecer nesta página.

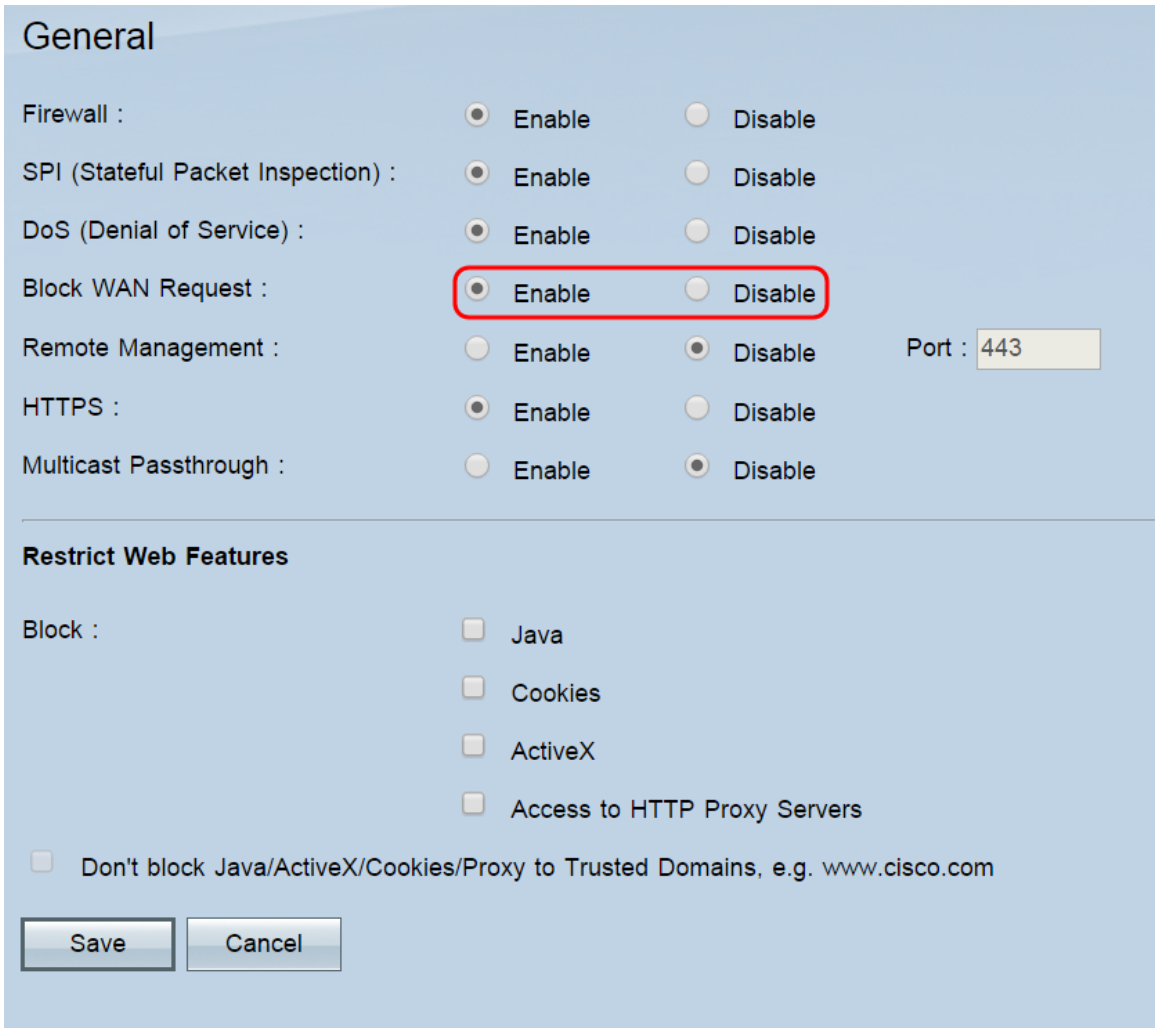
Etapa 2. No SPI (Stateful Package Inspection), selecione o botão de opção **Enable** ou **Disable**. O SPI é ativado por padrão. Esse recurso permite que o roteador inspecione todos os pacotes antes de enviá-los para processamento. Isso só poderá ser ativado se o firewall estiver ativado.



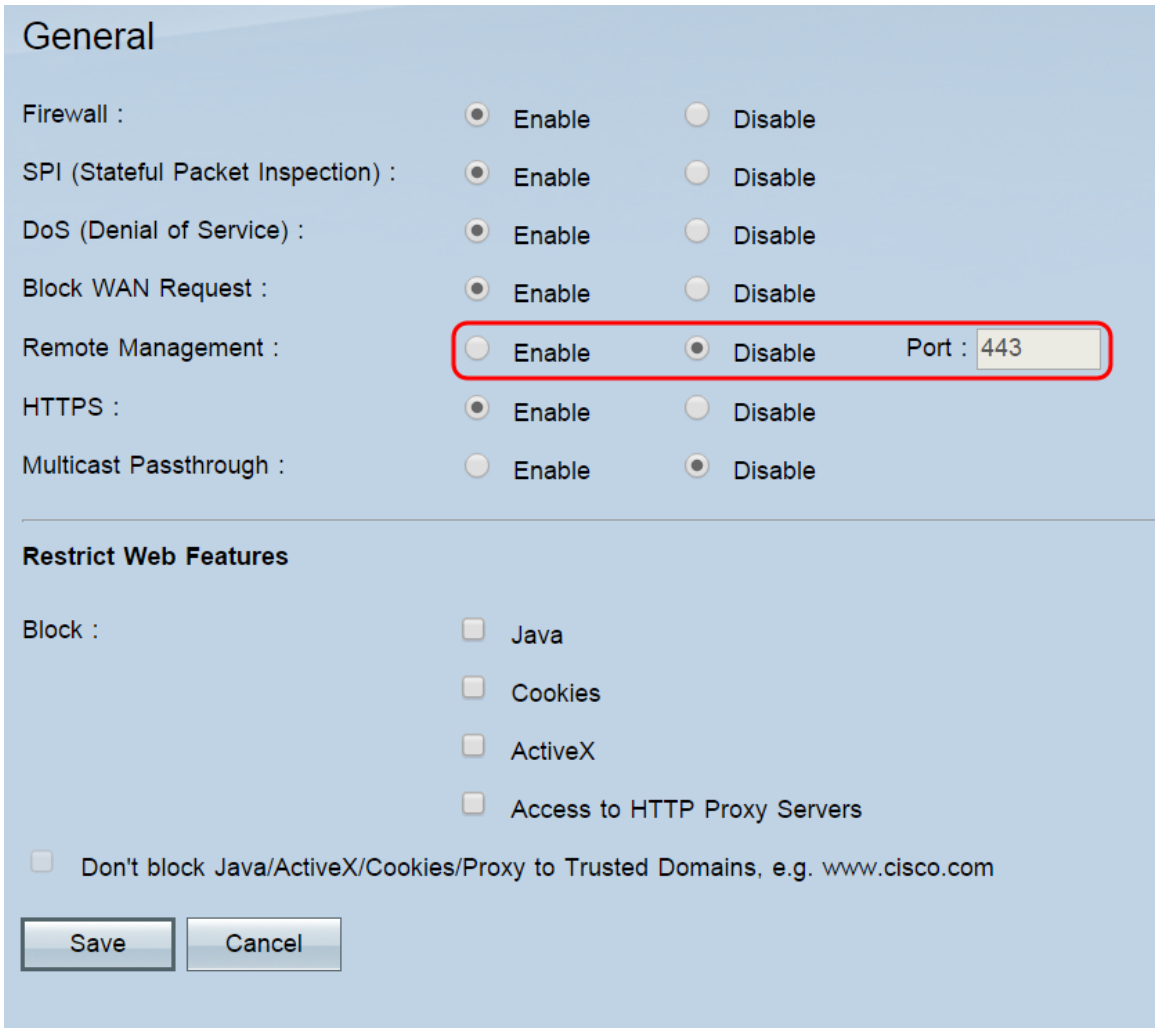
Etapa 3. No campo *DoS (Denial of Service)*, selecione o botão de opção **Enable** ou **Disable**. O DoS está ativado por padrão. Esse recurso impede que a rede interna seja atacada por ataques externos (como SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing e ataques de remontagem). Isso só poderá ser ativado se o firewall estiver ativado.



Etapa 4. No campo *Block WAN Request*, selecione o botão de opção **Enable** ou **Disable**. Block WAN Request (Bloquear solicitação de WAN) é habilitada por padrão. Esse recurso permite que o roteador descarte solicitações TCP e ICMP não aceitas da WAN, evitando que hackers localizem o roteador fazendo ping no endereço IP da WAN. Isso só poderá ser ativado se o firewall estiver ativado.



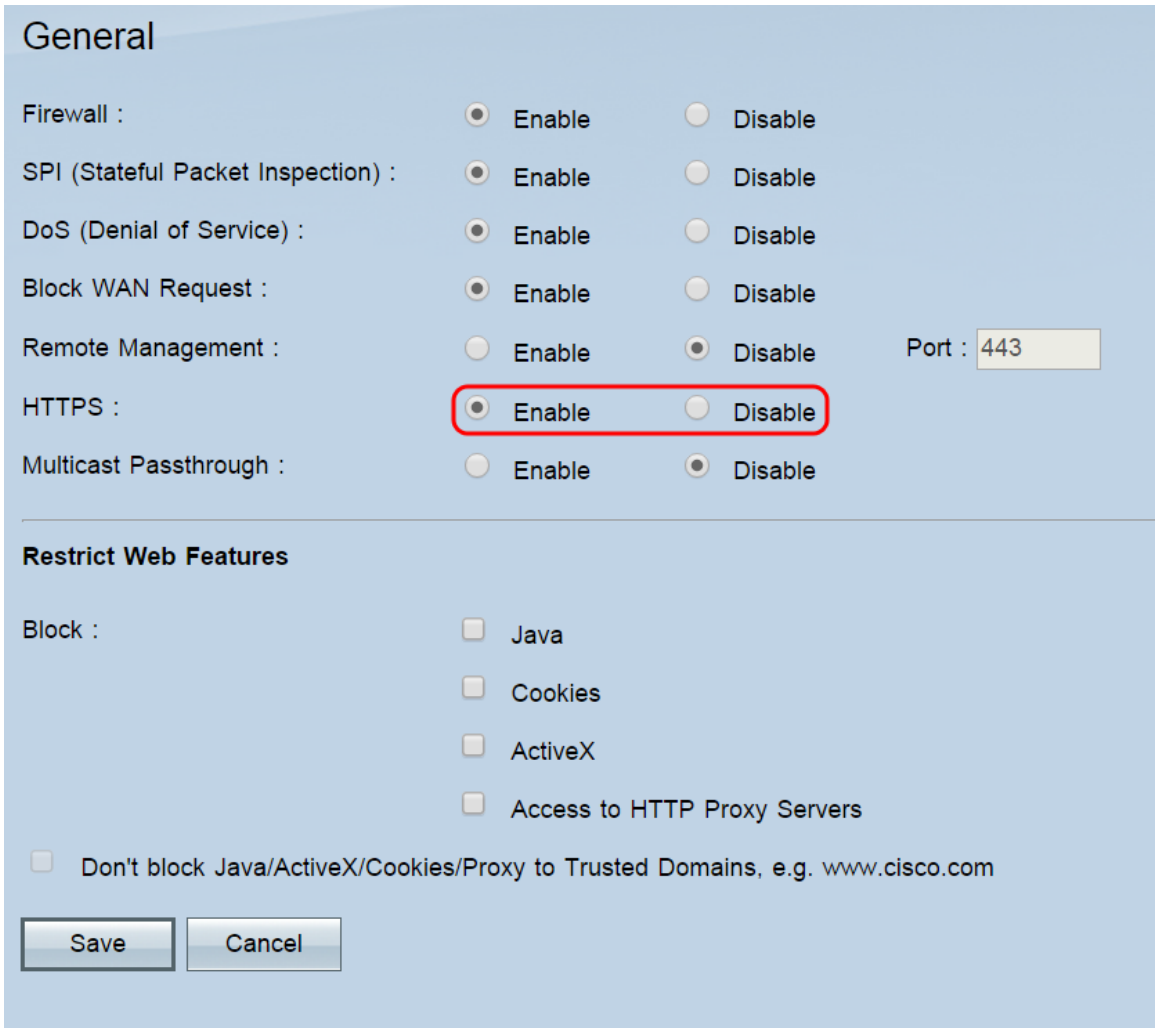
Etapa 5. No campo *Remote Management*, selecione o botão de opção **Enable** ou **Disable**. O Gerenciamento remoto está desabilitado por padrão. Esse recurso permite que você se conecte ao utilitário de configuração da Web do roteador de qualquer lugar na Internet. Se você habilitar esse recurso, poderá definir a porta usada para conexões remotas no campo Porta. O padrão é 443.



Observação: se você estiver usando a senha de administrador padrão, uma mensagem será exibida avisando que você precisa alterar a senha; clique em **OK** para continuar na página de senha ou em **Cancelar** para permanecer nesta página. A alteração da senha é necessária para impedir que usuários não autorizados acessem o roteador com a senha padrão.

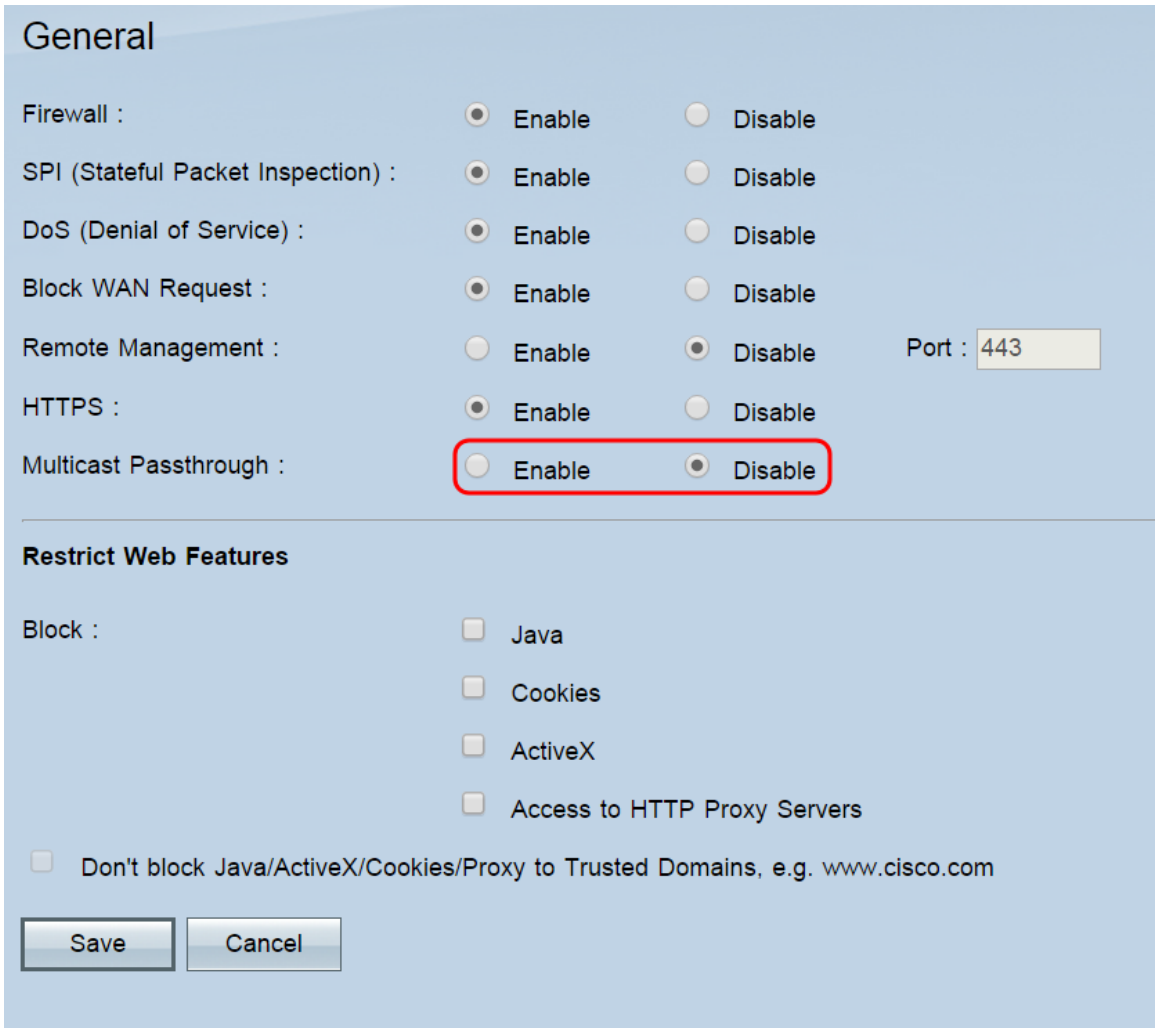
Observação: quando o gerenciamento remoto está habilitado, você pode acessar o utilitário de configuração da Web de qualquer navegador digitando **http://<endereço IP WAN do roteador>:<porta>**. Se o HTTPS estiver habilitado, insira **https://<endereço IP WAN do roteador>:<porta>**.

Etapa 6. No campo *HTTPS*, selecione o botão de opção **Enable** ou **Disable**. O HTTPS é habilitado por padrão. Este recurso permite sessões HTTP seguras.



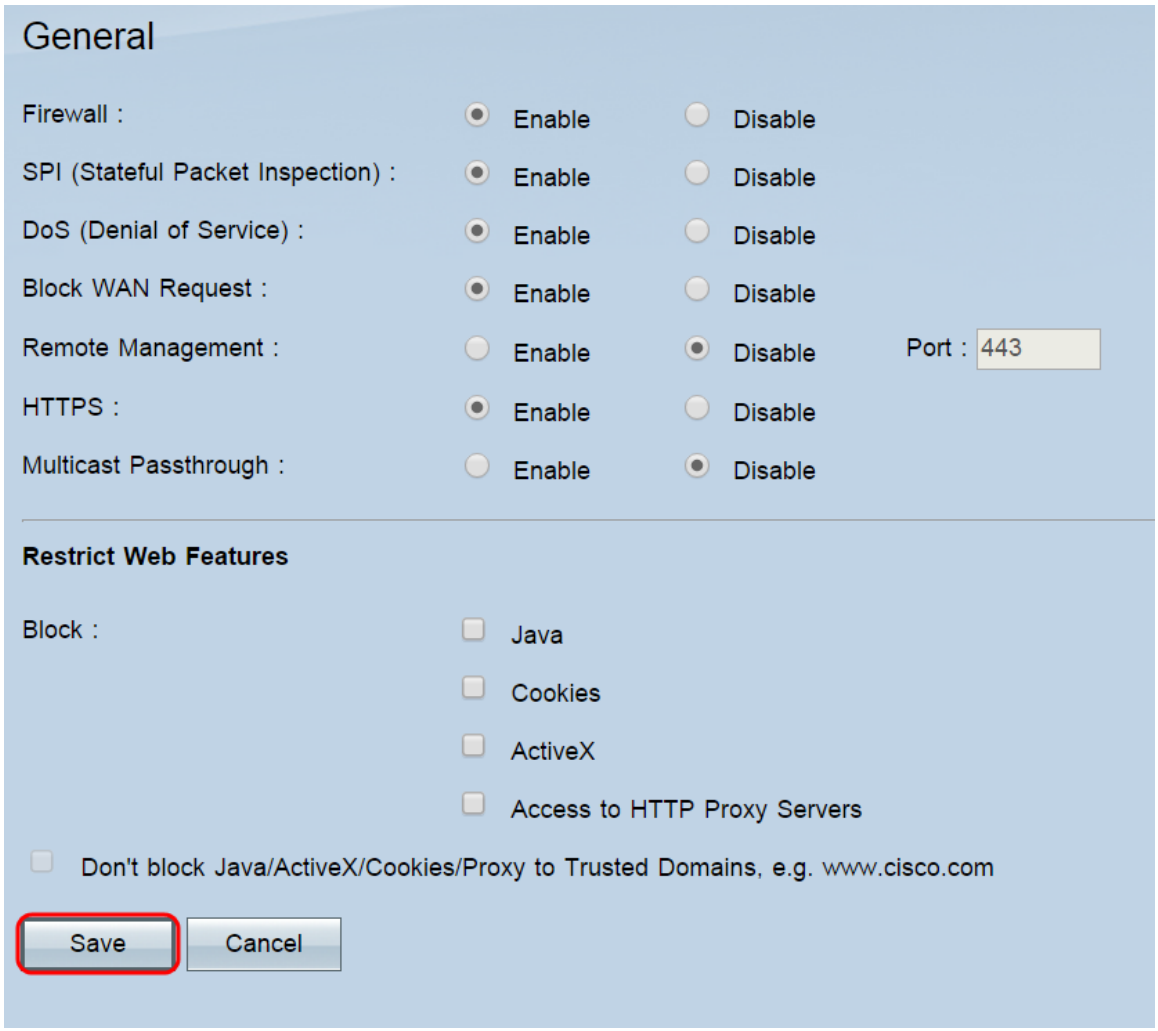
Observação: se esse recurso estiver desabilitado, os usuários não poderão se conectar usando a QuickVPN.

Passo 7. No campo *Multicast Passthrough*, selecione o botão de opção **Enable** ou **Disable**. A passagem multicast é desativada por padrão. Esse recurso permite que os pacotes multicast IP sejam transmitidos para seus dispositivos LAN correspondentes e é usado para jogos de Internet, videoconferência e aplicativos multimídia.



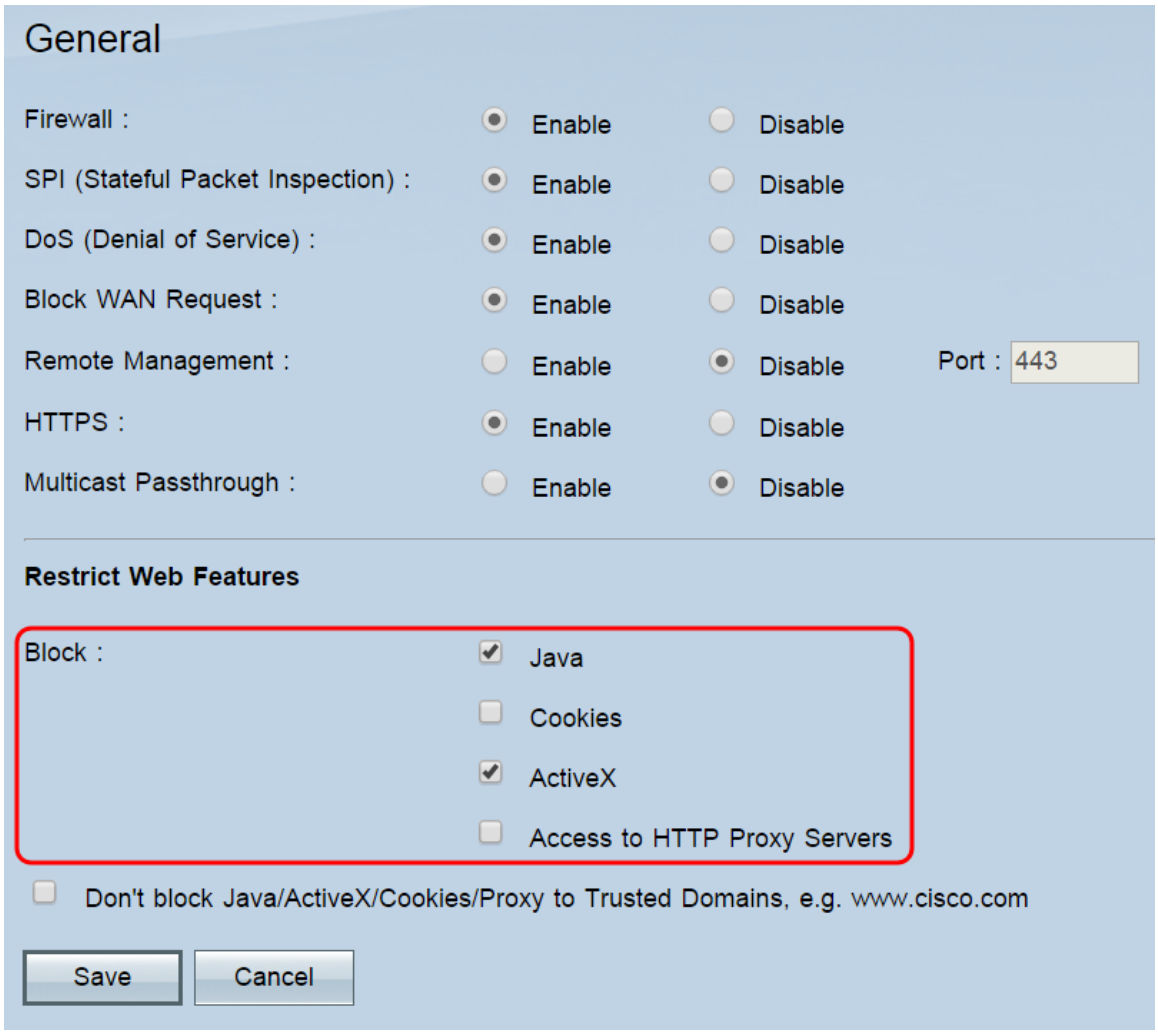
Observação: RV016, RV042, RV042G e RV082 não suportam a passagem de tráfego multicast em um túnel IPSec.

Etapa 8. Click **Save**.



Recursos da Web

Etapa 1. No campo *Bloquear*, marque as caixas de seleção dos recursos da Web que deseja bloquear no firewall. Se desejar permitir recursos bloqueados para alguns domínios, esses domínios poderão ser adicionados a uma lista de exceções na Etapa 2. Nenhum dos recursos está bloqueado por padrão.



As opções são:

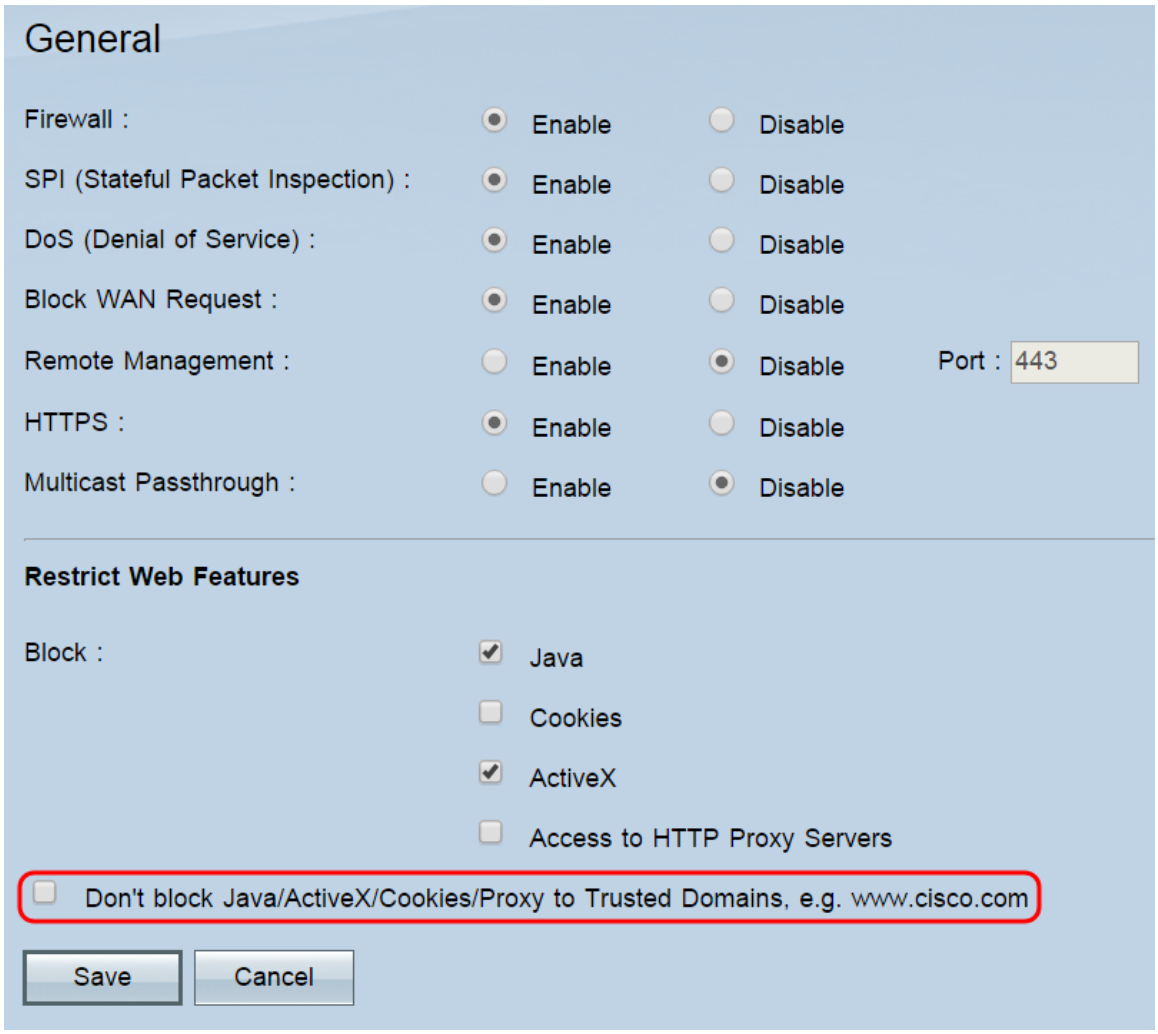
· Java â€" Java é uma linguagem de programação para sites da Web. Marcar esta caixa de seleção bloqueará miniaplicativos Java (pequenos programas incorporados em páginas da Web, mas executados fora do navegador da Web), mas pode fazer com que os sites que usam este recurso operem incorretamente.

· Cookies â€" Um cookie são dados que um site armazena localmente no PC de um usuário. O bloqueio de cookies pode fazer com que os sites que dependem deles se comportem incorretamente.

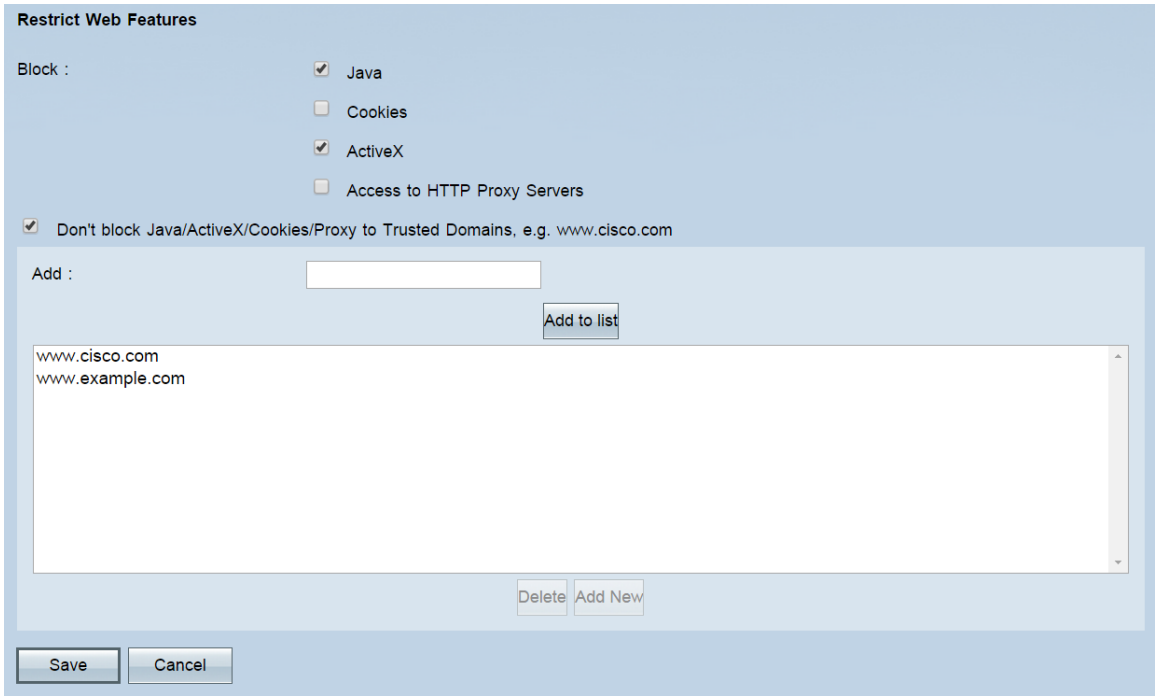
· AtiveX â€" AtiveX é uma estrutura de software desenvolvida pela Microsoft. Essa estrutura pode ser usada para executar determinadas partes de páginas da Web. Marcar esta caixa bloqueará esses componentes, mas pode fazer com que os sites que usam o AtiveX funcionem incorretamente.

· Acesso a servidores proxy HTTP â€" Marque esta caixa se quiser bloquear o acesso a servidores proxy HTTP. O uso de servidores proxy de WAN pode comprometer a segurança do roteador.

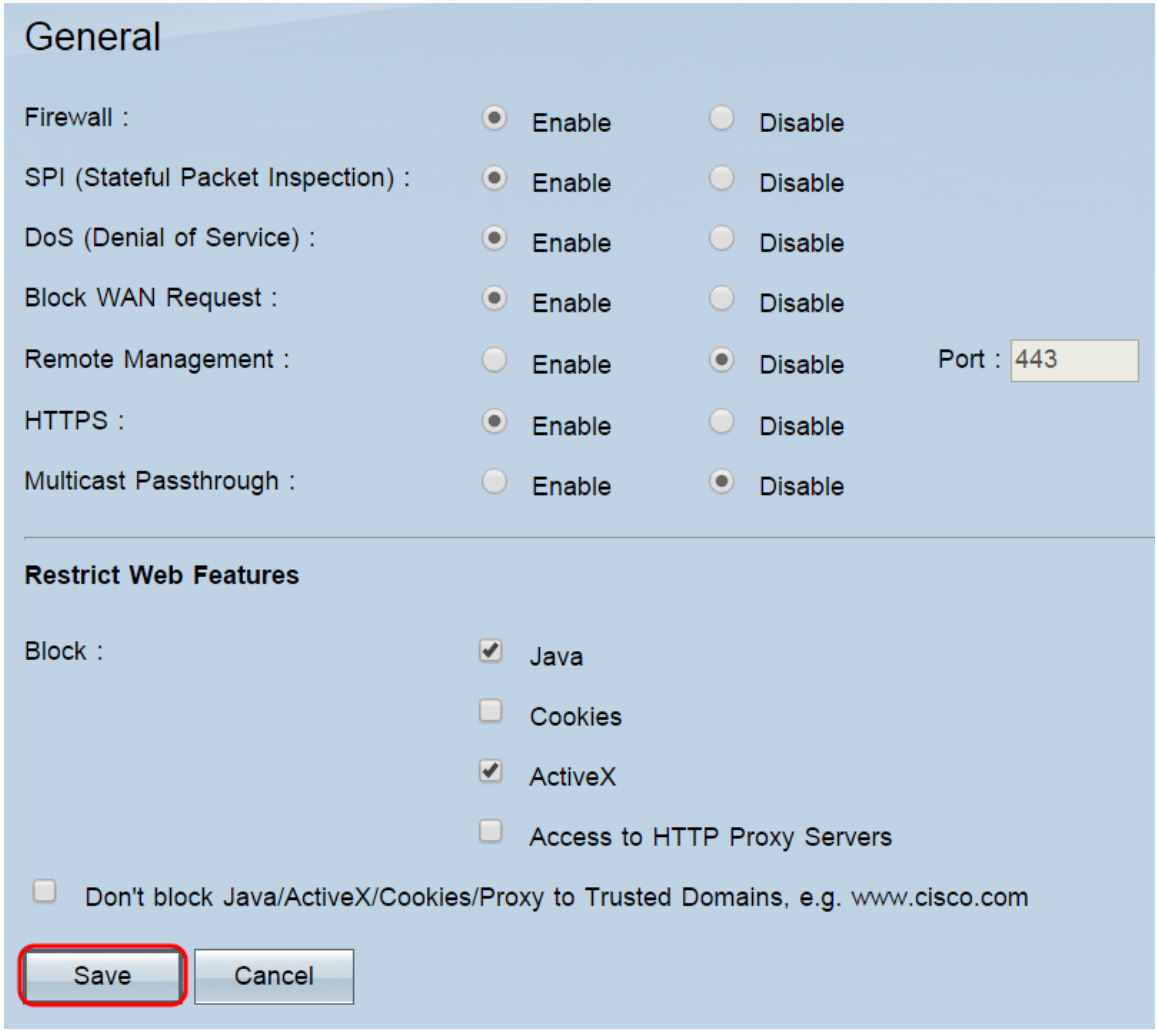
Etapa 2. Marque a caixa de seleção **Não bloquear Java/AtiveX/Cookies/Proxy para domínios confiáveis** para abrir a lista de domínios confiáveis, onde você pode adicionar ou remover domínios em que recursos da Web bloqueados são permitidos. Esse campo fica desmarcado por padrão e só estará disponível se você tiver marcado uma caixa anterior para bloquear um recurso. Se estiver desmarcada, os recursos serão bloqueados para todos os sites.



Etapa 3. (Opcional) Se você marcou a caixa de seleção **Não bloquear Java/AtiveX/Cookies/Proxy para domínios confiáveis**, uma lista de domínios confiáveis será exibida. Para adicionar um domínio à lista, insira-o no campo *Add* e clique em **Add to List**. Se desejar modificar um domínio existente, clique nele na lista, edite-o no campo *Add* e clique em **Update**. Para excluir um domínio da lista, clique nele na lista e clique em **Excluir**.



Etapa 4. Click **Save**.



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.