Configurações de firewall gerais no Roteadores RV016, RV042, RV042G e RV082 VPN

Objetivo

Um Firewall protege uma rede interna de uma rede externa tal como o Internet. Os Firewall são vitais à segurança de rede. Diversos ajustes diferentes estão disponíveis que pode permitir ou desabilitar os serviços específicos baseados em suas necessidades da Segurança.

O objetivo deste artigo é mostrar como permitir ou desabilitar configurações de firewall gerais no Roteadores RV016, RV042, RV042G, e RV082 VPN.

Dispositivos aplicáveis

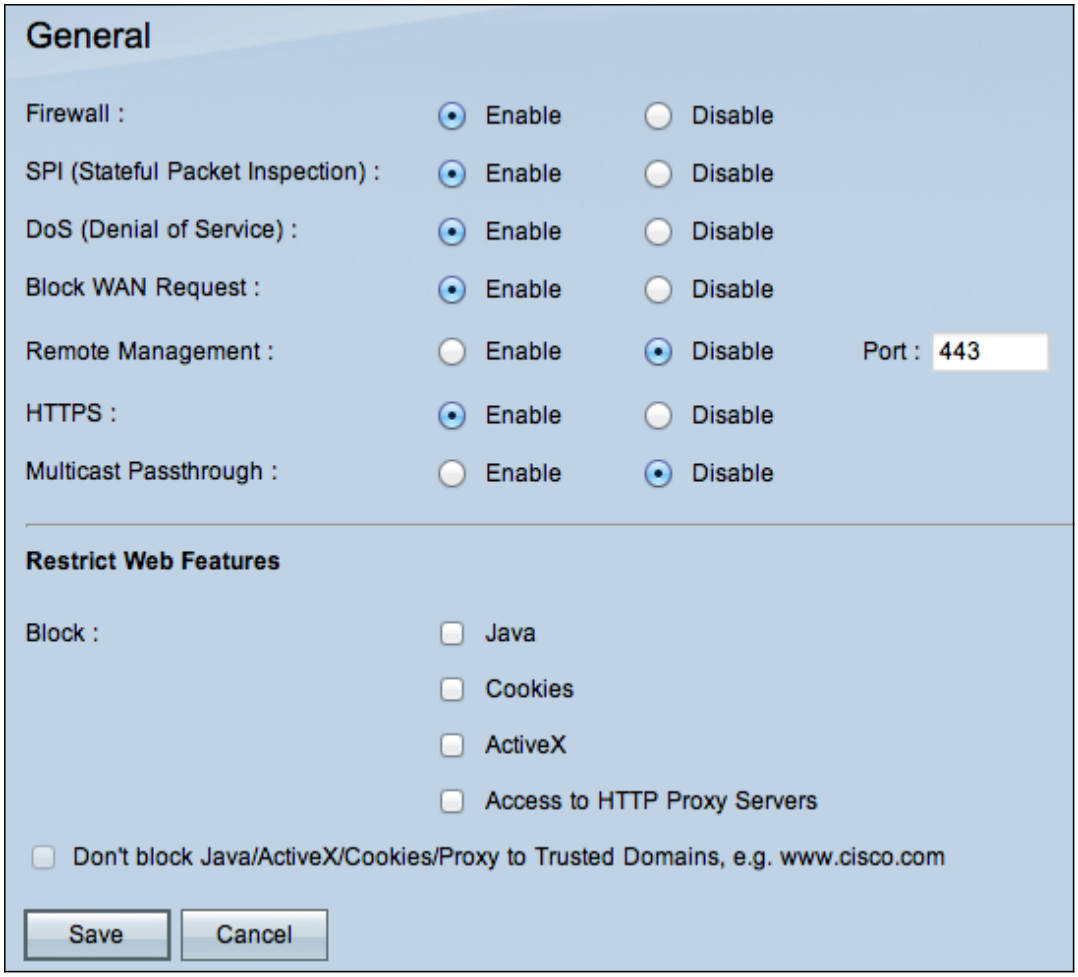
- RV016
- RV042
- RV042G
- RV082

Versão de software

- v4.2.1.02

Configurações de firewall gerais

Etapa 1. Entre a utilidade de configuração de roteador e escolha o **Firewall > o general**. A página *geral* abre:



Etapa 2. Clique a **possibilidade** ou **desabilite o** botão de rádio para permitir ou desabilitar os ajustes disponíveis no Firewall conforme requisições de usuário.

Os seguintes campos são descritos como segue:

• Firewall — Quando esta característica é permitida, o roteador executará a inspeção de pacote de informação profunda em todo o tráfego que dirige este roteador e deixa cair os pacotes que não seguem o comportamento de protocolo predefinido.

• SPI (inspeção de pacote de informação do stateful) — O Firewall do roteador usa a inspeção de pacote de informação do stateful (SPI) para rever o tráfego no Firewall. Monitora o estado de conexões de rede tais como córregos e comunicação UDP TCP. O Firewall distingue pacotes legítimos para tipos de conexão diferentes e somente os pacotes que combinam uma conexão ativa conhecida são permitidos pelo Firewall, todos os outro são rejeitados.

• Dos (recusa de serviço) — Quando esta característica é permitida, o roteador impedirá os ataques DOS (recusa de serviço) que vêm do Internet. Os ataques DOS fazem com que o CPU de seu roteador seja ocupado de modo que não possa proporcionar serviços ao tráfego regular.

• Pedido MACILENTO do bloco — Quando isto é permitido, o roteador ignorará solicitações de ping do Internet assim que parecerá ser hidden. Isto ajuda a fornecer a Segurança escondendo as portas de rede assim que os trespassers não têm o acesso à rede facilmente.

• Gerenciamento remoto — Quando esta característica é permitida, o roteador permite que o utilitário de configuração da Web esteja alcançado do Internet. Entre no número de porta

que será aberto aos anfitriões no lado WAN. A configuração padrão é 443. Esta porta deve ser especificada quando o usuário estabelece uma conexão remota.

• HTTPS — Quando permitido, o utilitário de configuração da Web pode ser alcançado através de uma sessão HTTPS do lado WAN em vez do HTTP regular. Isto terá sua sessão da web remota protegida por algoritmos de criptografia SSL. Se a característica HTTPS é deficiente os usuários não podem conectar com o uso de QuickVPN. Se desabilitado, usa uma menos fixa a conexão de HTTP.

• Transmissão do Multicast — Se um proxy de IGMP é executado atualmente no roteador, quando a transmissão do Multicast está permitida o roteador permitirá que o tráfego do Protocolo IP multicast venha dentro do Internet.

Nota: Para desabilitar o Firewall, a senha de administrador deve ser mudada do padrão. Os campos *SPI* (inspeção de pacote de informação do stateful), *DoS* (recusa de serviço), do *pedido MACILENTO do bloco* e do *Gerenciamento remoto* são esmaecidas para fora.

Etapa 3. Na área das características da Web da limitação, verifique alguns ou todas as caixas de seleção para restringir a característica correspondente.

• Javas — A Java é um linguagem de programação para Web site. Para obstruir Javas, verifique a caixa de verificação das **Javas**. Se você nega Javas, a seguir você não pode poder alcançar as websites escritas neste linguagem de programação, assim que é seguro ir adiante e obstruir Java applets se o dispositivo conectado ao roteador não precisa de alcançar os Web site criados com as Javas. Por outro lado, os Cyber-criminosos usam Javas como uma parte integral de seu ataque, que é determinar o OS e lança um ataque OS-especificado quando você visita os Web site que estão contaminados pelo malware. Por exemplo, quando você visita um Web site cortado, um arquivo do FRASCO (Java Archive) é provocado que peça que você execute sua função mas é usado secretamente para determinar o OS do computador.

• Cookie — Um Cookie é dados armazenados no PC e usados por websites quando os usuários interagem com elas. Para obstruir Cookie, verifique a caixa de verificação dos **Cookie**. Se você deseja obstruir Cookie, a seguir os Web site não podem salvar nenhuma informação precedente da visita quando alcançados do dispositivo. O benefício é que os Cookie maliciosos (terceira parte que segue Cookie) não salvar, que levanta um risco de segurança.

• ActiveX — ActiveX é um componente de software de Microsoft Windows que possa ser usado para desenvolver aplicativos ou controlar programas pequenos como o adicionar-ONS usado em websites. Se você permite ActiveX, pode ajudar a melhorar sua experiência quando você consulta; permite que os Web site executem animações e outros programas similares. Por outro lado, há um risco potencial se você visita os página da web que contêm o software malicioso de ActiveX desenvolvido pelos cyber-criminosos que podem causar dano ao computador. Para obstruir ActiveX, verifique a caixa de verificação de **ActiveX**. Se você obstrui ActiveX, você pode ter problemas se você quer alcançar determinadas websites que usam ActiveX para executar.

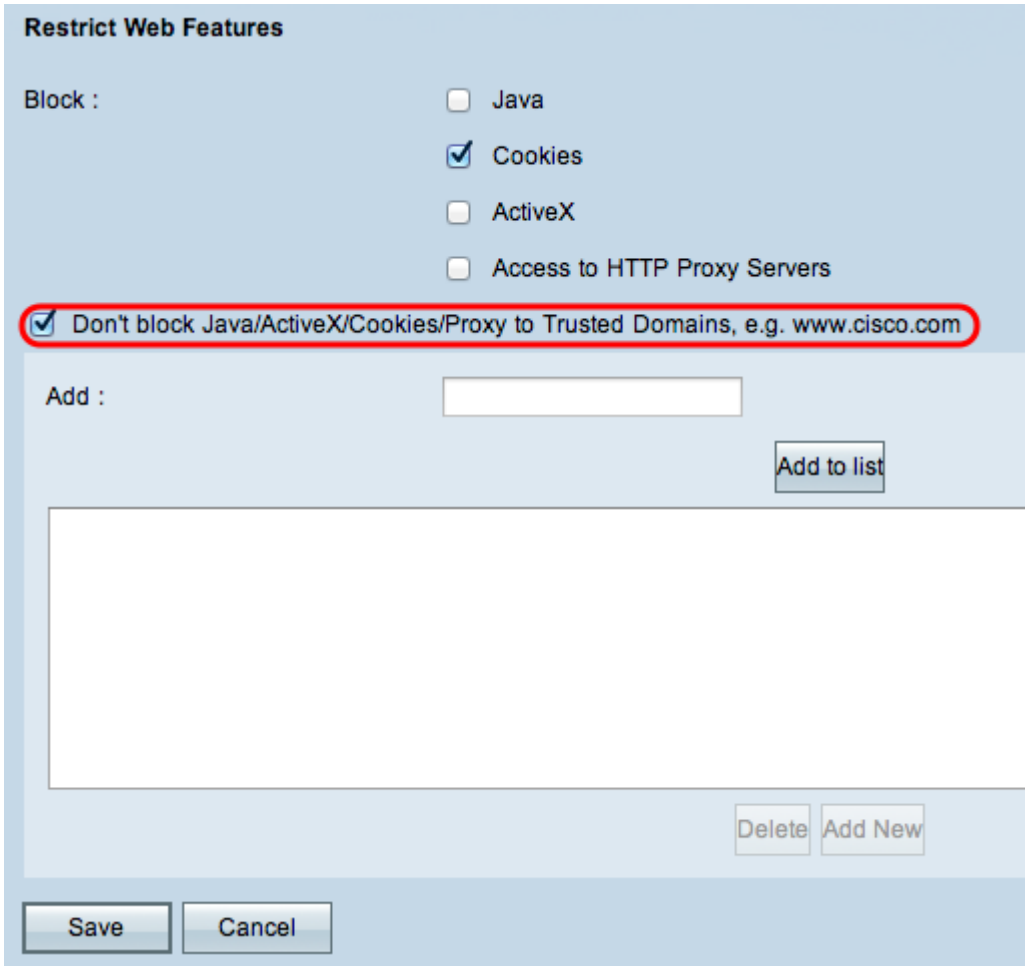
• Alcance ao proxy o Server do HTTP — Se você deseja surfar anonimamente através de um servidor proxy e negar o acesso ao servidor proxy, verifique o **acesso à** caixa de verificação do **Server do HTTP do proxy**. Os servidores proxy HTTP escondem detalhes de utilizadores finais dos hacker. Trabalham porque os intermediários e assim você não alcançam o Internet diretamente. Contudo, se os usuários locais têm o acesso aos servidores proxy MACILENTOS, podem poder encontrar uma maneira em torno dos filtros

satisfeitos no roteador e alcançar as websites obstruídas pelo roteador.

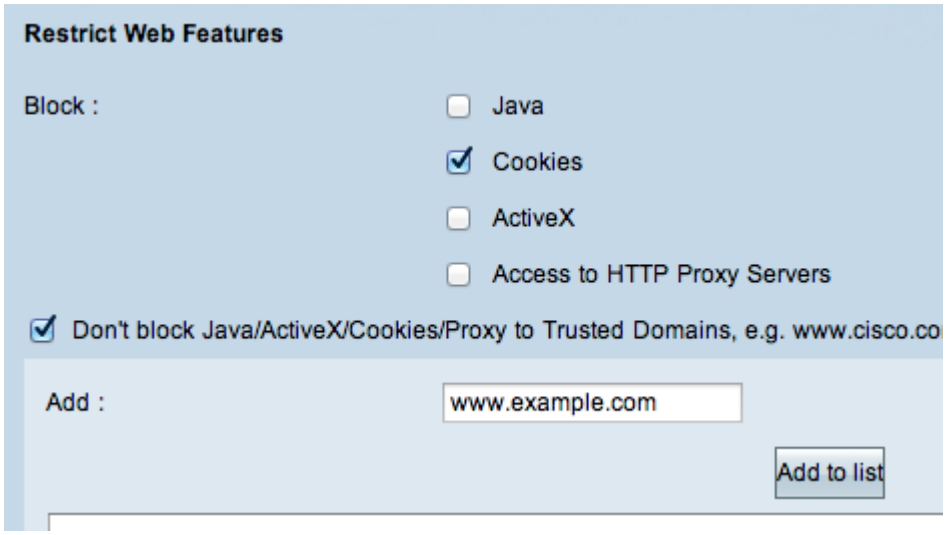
Etapa 4. **Salvaguarda do** clique a fim salvar os ajustes.

Adicionar domínios confiável

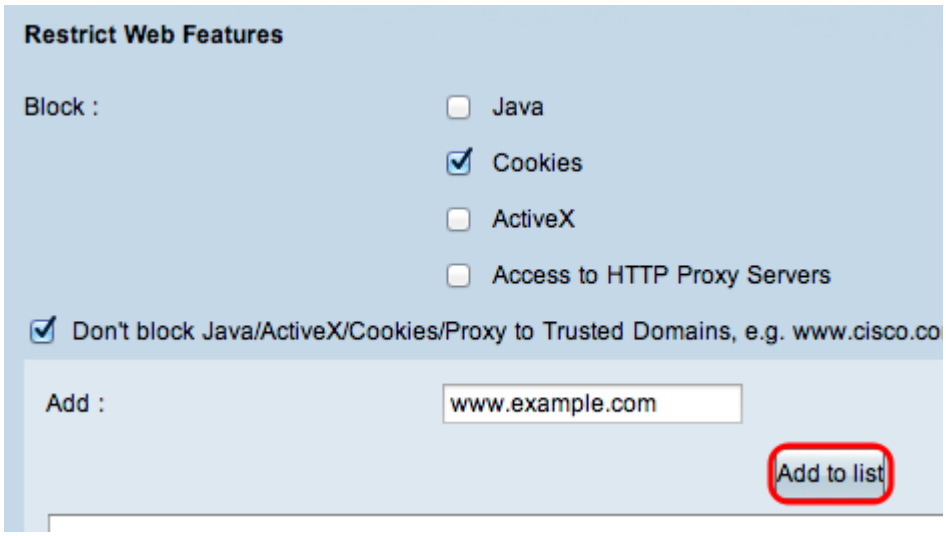
Mesmo que uma das características da Web possa ser obstruído, o usuário pode permitir que estas características sejam permitidas para domínios confiável especificados.



Etapa1. Verifique **não obstruem Javas/ActiveX/Cookie/proxy ao** botão dos **domínios confiável**. Isto estará somente disponível se o usuário escolheu obstruir algumas das características da Web em etapa 3 de *configurações de firewall gerais*.



Etapa 2. No campo *adicionar*, incorpore o domínio a ser adicionado à lista do domínio confiável.

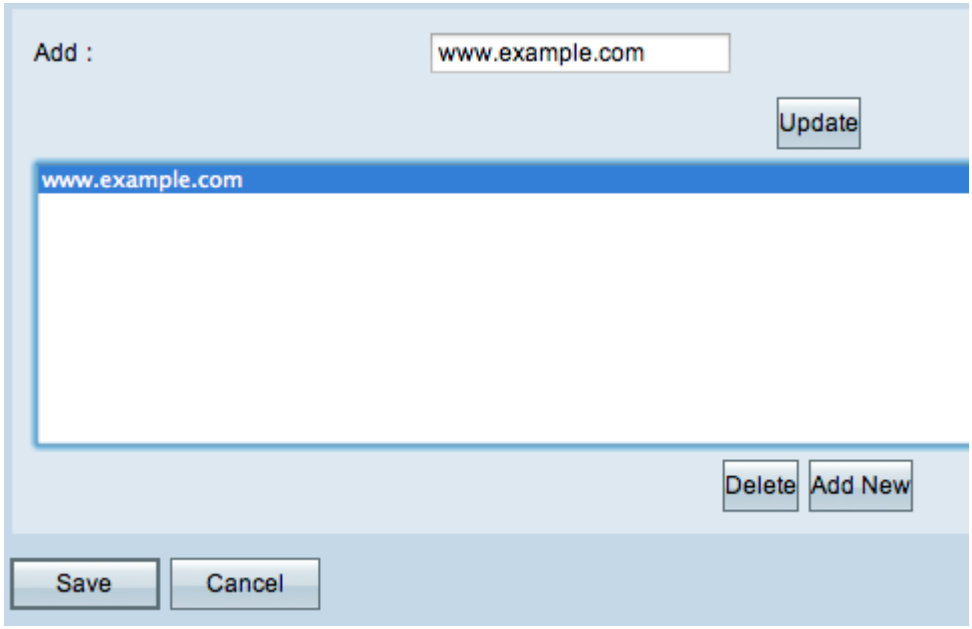


Etapa 3. O clique **adiciona para alistar.** O domínio é adicionado à lista confiada.

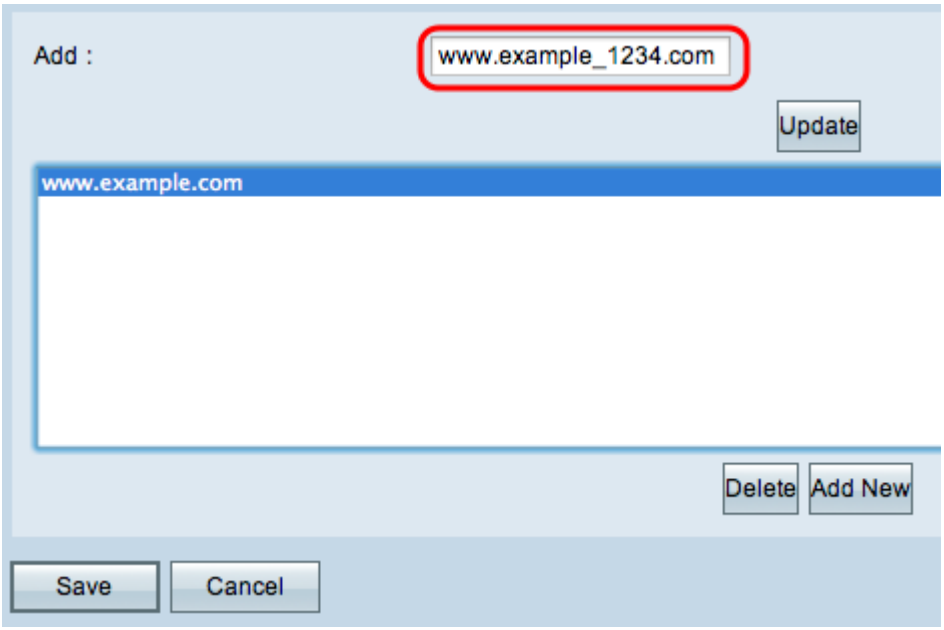
Etapa 4. **Salvaguarda do** clique para salvar as mudanças.

Atualize um domínio confiável

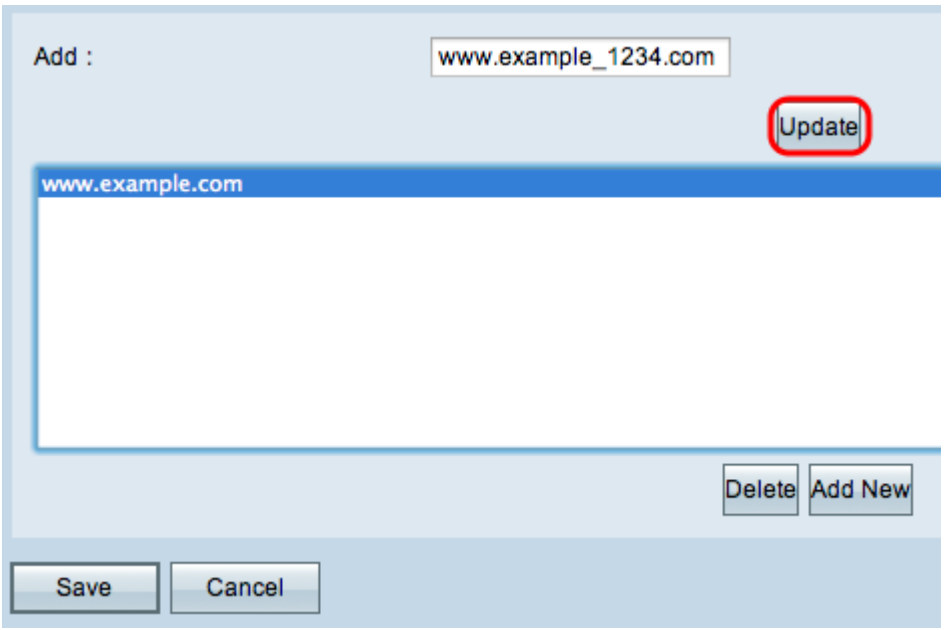
Esta seção guia o usuário em como editar um domínio confiável.



Etapa 1. Escolha o domínio que você gostaria de editar da lista do domínio confiável.



Etapa 2. No campo *adicionar*, incorpore o Domain Name actualizado para o domínio exigido.

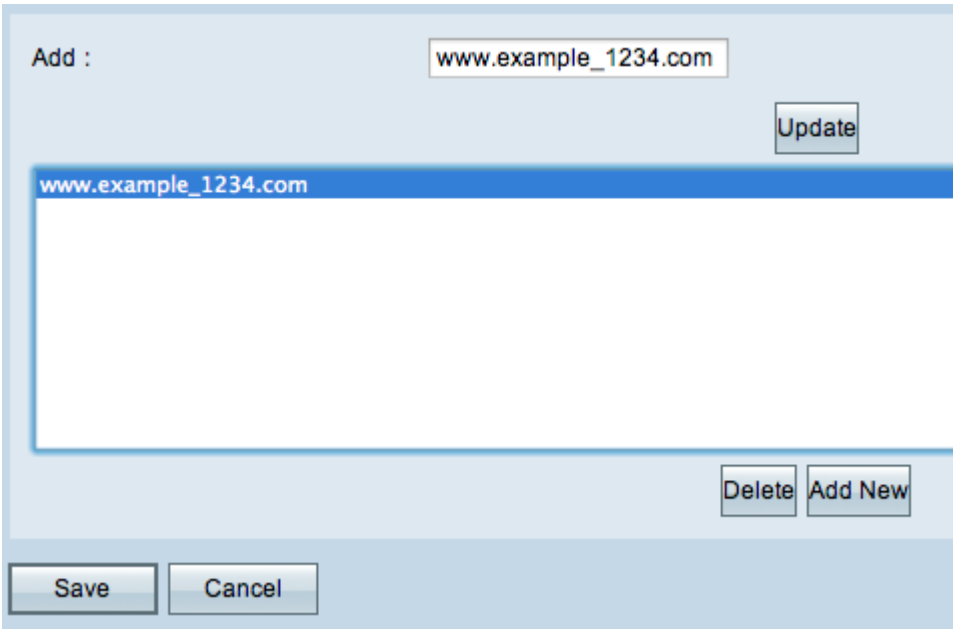


Etapa 3. **Atualização do** clique.

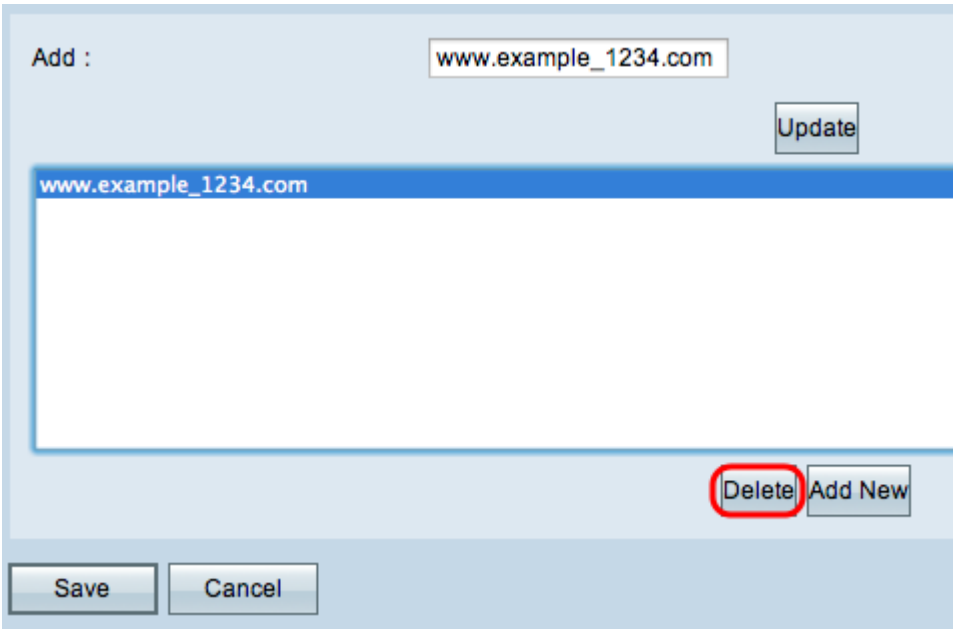
Etapa 4. **Salvaguarda do** clique para salvar as mudanças.

Suprima de um domínio confiável

Esta seção guia o usuário em como suprimir de um domínio confiável.



Etapa 1. Escolha o domínio de que você gostaria de suprimir.



Etapa 2. **Supressão do** clique. O domínio é suprimido.

Etapa 3. **Salvaguarda do** clique para salvar as mudanças.