Exemplo de configuração de filtragem de URL em um sistema FireSIGHT

Contents

Introduction

Este documento descreve as etapas para configurar a filtragem de URL no sistema FireSIGHT. O recurso de filtragem de URL no FireSIGHT Management Center permite gravar uma condição em uma regra de controle de acesso para determinar o tráfego que atravessa uma rede com base em solicitações de URL não criptografadas pelos hosts monitorados.

Prerequisites

Requirements

Este documento tem alguns requisitos específicos para a Licença de filtragem de URL e a porta.

Requisito de Licença de Filtragem de URL

Um FireSIGHT Management Center requer uma licença de filtragem de URL para entrar em contato com a nuvem periodicamente para obter uma atualização das informações de URL. Você pode adicionar condições de URL baseadas em categoria e reputação para acessar regras de controle sem uma licença de filtragem de URL; no entanto, você não pode aplicar a política de controle de acesso até adicionar uma licença de filtragem de URL ao FireSIGHT Management Center e, em seguida, ativá-la nos dispositivos de destino da política.

Se uma licença de filtragem de URL expirar, as regras de controle de acesso com condições de URL baseadas em categoria e reputação deixarão de filtrar URLs e o FireSIGHT Management Center não contatará mais o serviço de nuvem. Sem uma licença de filtragem de URL, URLs individuais ou grupos de URLs podem ser definidos para permitir ou bloquear, mas a categoria de

URL ou os dados de reputação não podem ser usados para filtrar o tráfego de rede.

Requisito de porta

Um sistema FireSIGHT usa as portas 443/HTTPS e 80/HTTP para se comunicar com o serviço de nuvem. A porta 443/HTTPS deve ser aberta bidirecionalmente e o acesso de entrada à porta 80/HTTP deve ser permitido no FireSIGHT Management Center.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Dispositivos FirePOWER: Série 7000, Série 8000
- Dispositivo virtual NGIPS (Sistema de prevenção de intrusão de próxima geração)
- Dispositivo de segurança adaptável (ASA) FirePOWER
- Software Sourcefire versão 5.2 ou posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

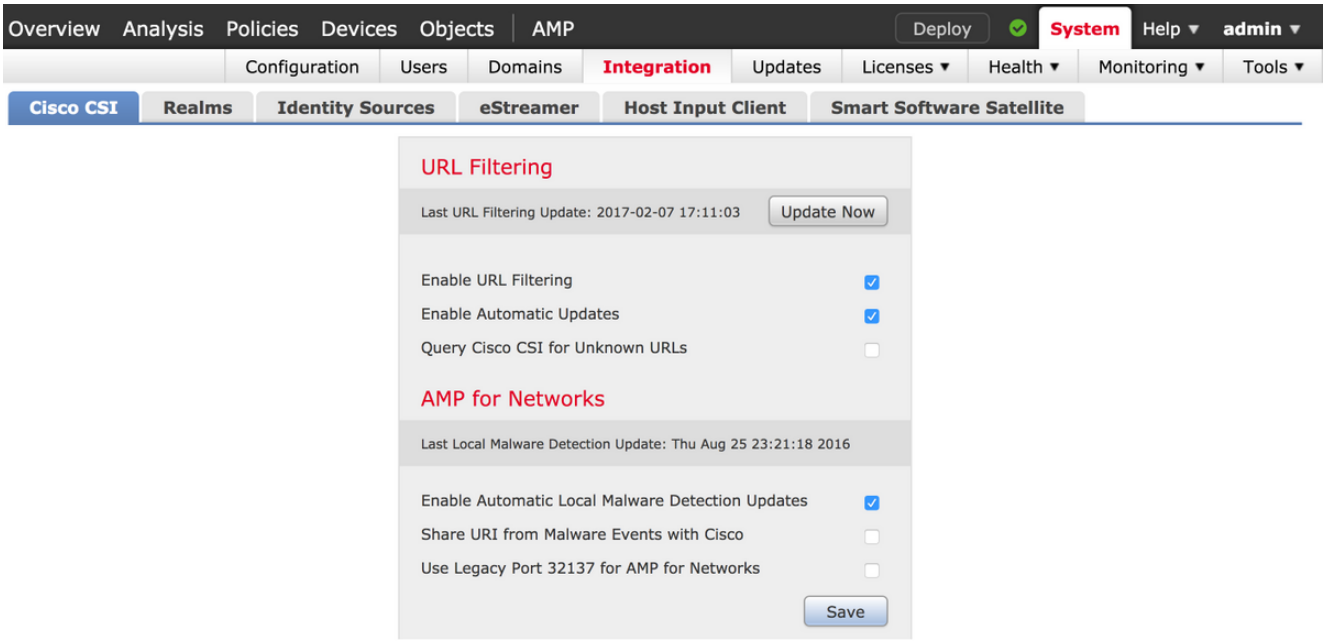
Habilitar filtragem de URL no FireSIGHT Management Center

Para habilitar a filtragem de URL, siga estas etapas:

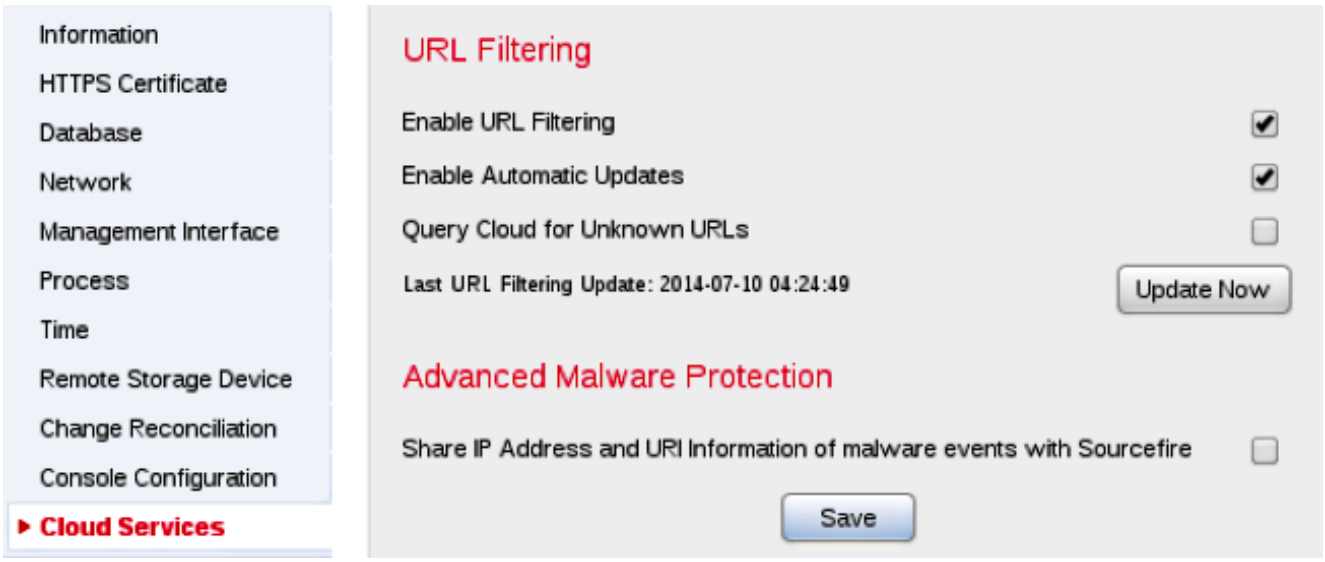
1. Faça login na interface de usuário da Web do FireSIGHT Management Center.

2. A navegação é diferente com base na versão do software executada:

   Na versão 6.1.x, selecione **System > Integration > Cisco CSI**.



Na Versão 5.x, escolha **System > Local > Configuration**. Escolha **Cloud Services**.



3. Marque a caixa de seleção **Enable URL Filtering** para habilitar a filtragem de URL.
4. Como opção, marque a caixa de seleção **Enable Automatic Updates** para habilitar as atualizações automáticas. Essa opção permite que o sistema entre em contato com o serviço de nuvem regularmente para obter atualizações dos dados de URL nos conjuntos de dados locais do equipamento.

   Note: Embora o serviço de nuvem geralmente atualize seus dados uma vez por dia, se você habilitar as atualizações automáticas, ele forçará o FireSIGHT Management Center a verificar a cada 30 minutos para garantir que as informações estejam sempre atualizadas. Embora as atualizações diárias tendem a ser pequenas, se já se passaram mais de cinco dias desde a última atualização, novos dados de filtragem de URL podem levar até 20 minutos para serem baixados. Após o download das atualizações, pode levar até 30 minutos para executar a atualização.

5. Opcionalmente, marque a caixa de seleção **Consultar Nuvem para URLs Desconhecidos** para consultar o serviço de nuvem para URLs desconhecidos. Essa opção permite que o sistema consulte a nuvem da Sourcefire quando alguém em sua rede monitorada tentar

navegar para uma URL que não esteja no conjunto de dados local. Se a nuvem não souber a categoria ou a reputação de um URL, ou se o FireSIGHT Management Center não puder entrar em contato com a nuvem, o URL não corresponderá às regras de controle de acesso com condições de URL baseadas em categoria ou reputação.

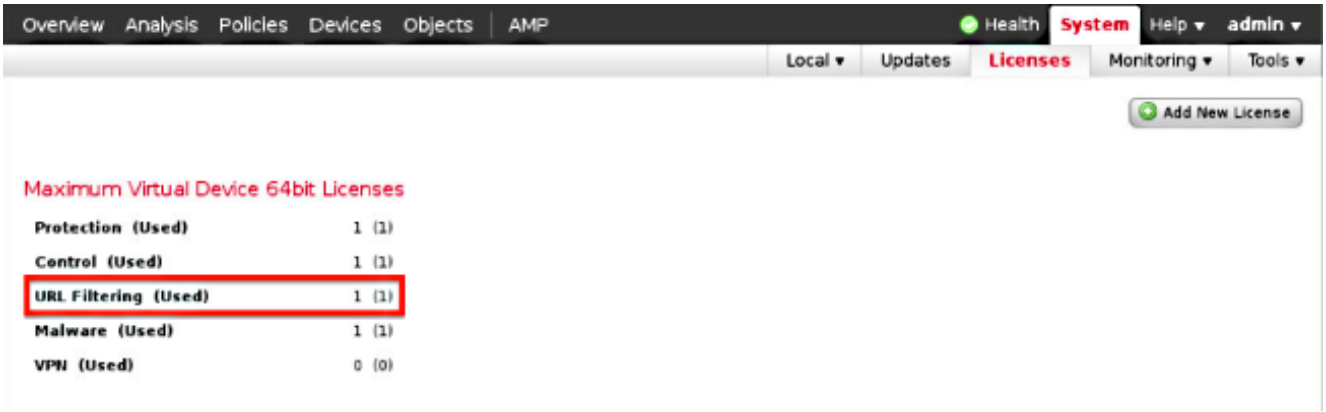
Note: Não é possível atribuir categorias ou reputações a URLs manualmente. Desative essa opção se não quiser que seus URLs sem categoria sejam catalogados pela nuvem da Sourcefire, por exemplo, por motivos de privacidade.

6. Click **Save**. As configurações de filtragem de URL são salvas.

Note: Com base no período de tempo desde que a Filtragem de URL foi habilitada pela última vez, ou se esta for a primeira vez que você habilitou a Filtragem de URL, um FireSIGHT Management Center recuperará os dados de Filtragem de URL do serviço de nuvem.

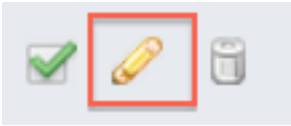
Aplicar licença de filtragem de URL em um dispositivo gerenciado

1. Verifique se a licença de filtragem de URL está instalada no FireSIGHT Management Center. Acesse a página **System > Licenses** para encontrar uma lista de licenças.

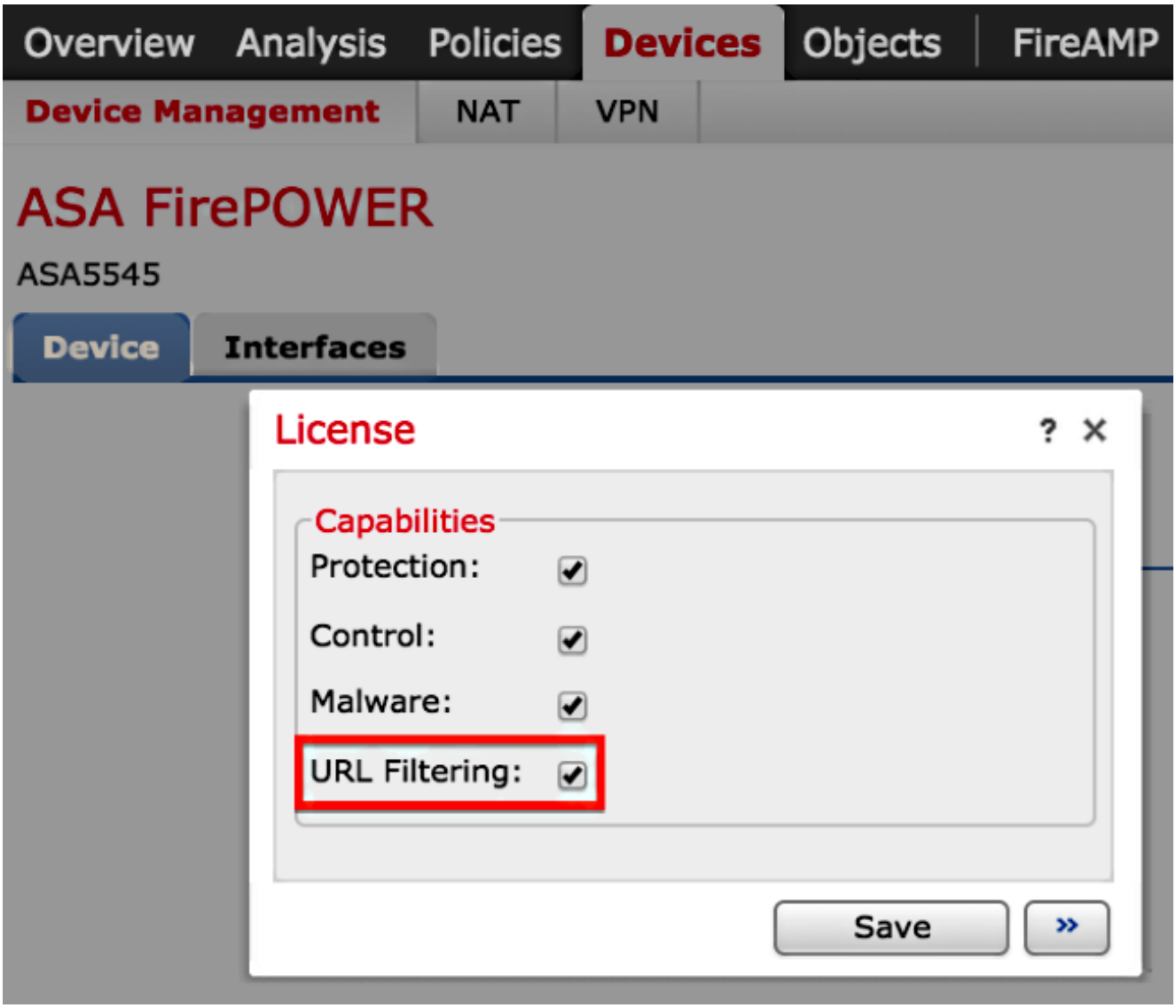


2. Vá para a página **Devices > Device Management** e verifique se a licença de filtragem de URL é aplicada no dispositivo que monitora o tráfego.

3. Se a licença de filtragem de URL não for aplicada a um dispositivo, clique no ícone do **lápis** para editar as configurações. O ícone está localizado ao lado do nome do dispositivo.



4. Você pode habilitar a licença de filtragem de URL em um dispositivo na guia **Dispositivos**.



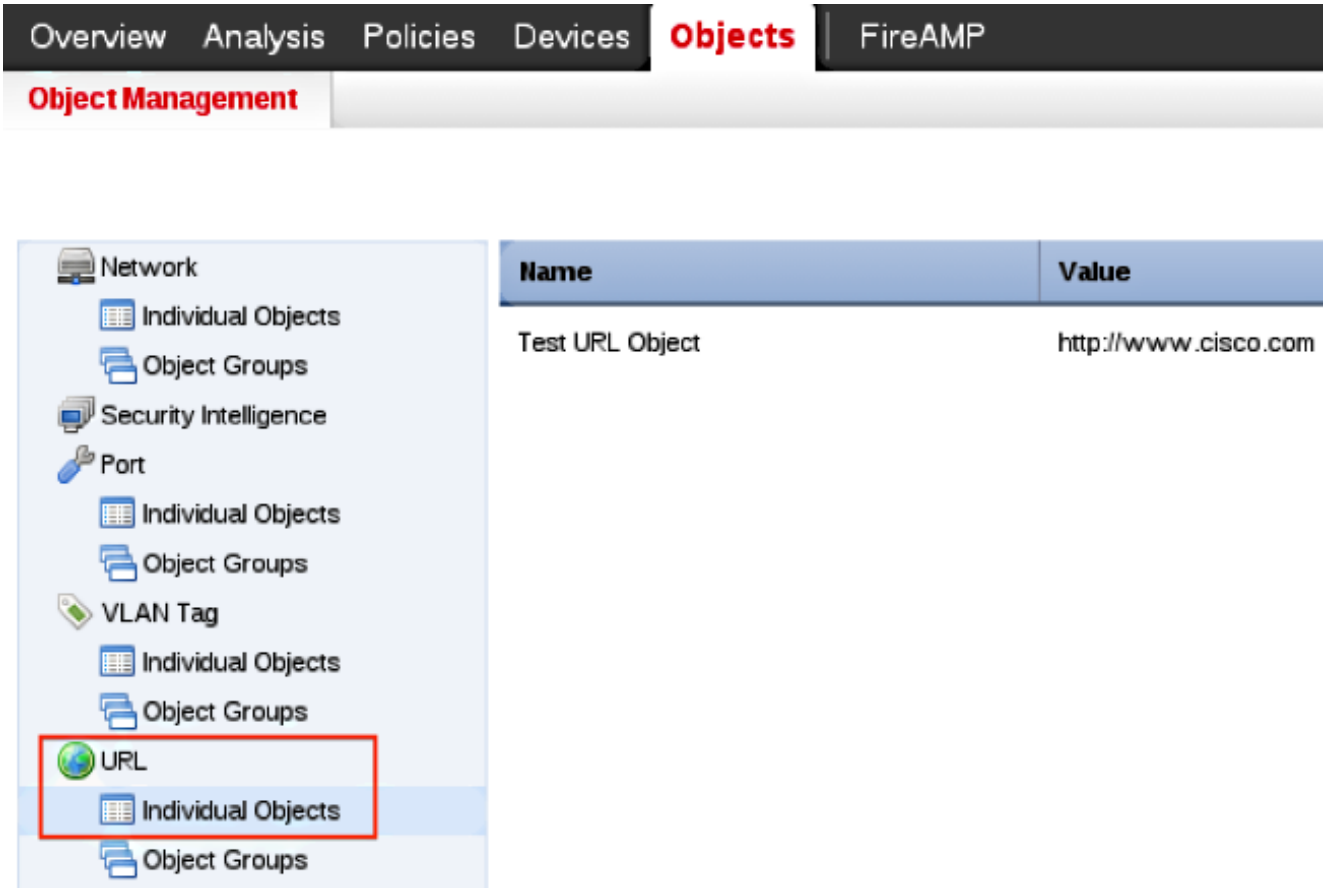
5. Depois de habilitar uma licença e salvar suas alterações, você também deve clicar em **Aplicar alterações** para aplicar a licença em seu dispositivo gerenciado.

Exclusão de um Site Específico da Categoria de URL Bloqueada

O FireSIGHT Management Center não permite que você tenha uma classificação local de URLs que substituam as classificações de categoria padrão fornecidas pela Sourcefire. Para realizar essa tarefa, você deve usar uma política de Controle de acesso. Essas instruções descrevem como usar um objeto de URL em uma regra de Controle de Acesso para excluir um site específico de uma categoria de bloqueio.

1. Vá para a página **Objetos > Gerenciamento** de Objetos.

2. **Escolha Objetos Individuais** para URL e clique no botão **Adicionar URL**. A janela **URL Objects** é exibida.

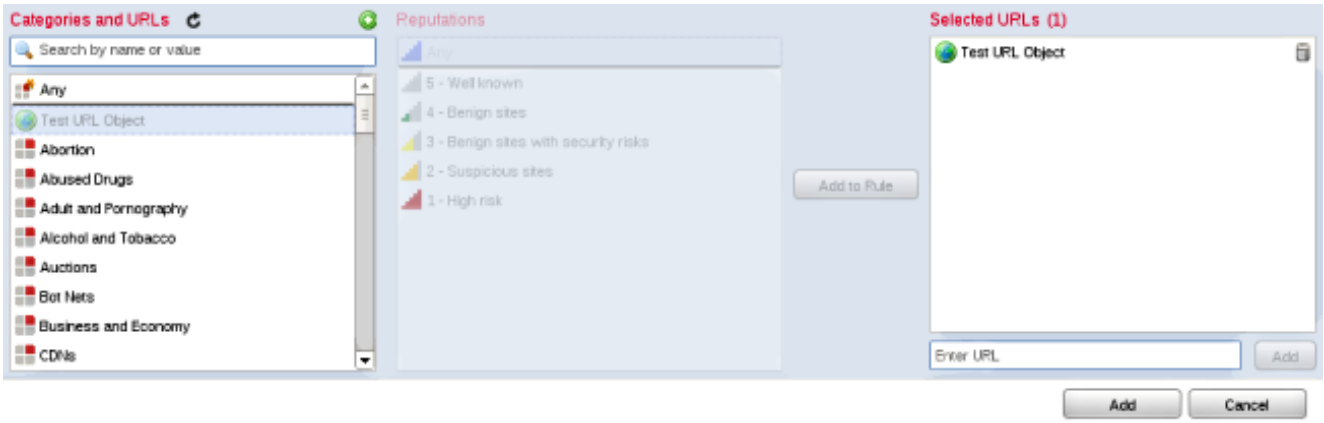


3. Depois de salvar as alterações, escolha **Policies > Access Control** e clique no ícone do **lápis** para editar a política de Access Control.

4. Clique em Adicionar regra.

5. Adicione o Objeto de URL à regra com a ação **Permitir** e coloque-o acima da regra Categoria

de URL, para que a ação da regra seja avaliada primeiro.



6. Depois de adicionar a regra, clique em **Salvar e aplicar**. Ele salva as novas alterações e aplica a política de controle de acesso aos dispositivos gerenciados.

Verificar

Para obter informações de verificação ou solução de problemas, consulte o artigo **Troubleshooting Issues with URL Filtering on FireSIGHT System** na seção Related Information.

Troubleshoot

Para obter informações sobre verificação ou solução de problemas, consulte o **Solucionar problemas com filtragem de URL no sistema FireSIGHT** vinculado na seção Informações Relacionadas.

Informações Relacionadas

- Solucionar problemas com filtragem de URL no sistema FireSIGHT
- Suporte Técnico e Documentação - Cisco Systems

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.

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.