Filtragem URL em um exemplo da configuração de sistema de FireSIGHT

Índice

Introdução

Este documento descreve as etapas para configurar a Filtragem URL no sistema de FireSIGHT. A característica da Filtragem URL no centro de gerenciamento de FireSIGHT permite que você escreva uma circunstância em uma regra do controle de acesso a fim determinar o tráfego que atravessa um baseado na rede em pedidos NON-cifrados URL pelos anfitriões monitorados.

Pré-requisitos

Requisitos

Este documento tem algumas algumas exigências específicas para a licença da Filtragem URL e a porta.

Exigência da licença da Filtragem URL

Um centro de gerenciamento de FireSIGHT exige uma licença da Filtragem URL a fim contactar periodicamente a nuvem para uma atualização na informação de URL. Você pode adicionar a categoria e as condições reputação-baseadas URL às regras do controle de acesso sem uma Filtragem URL licenciam; porém você não pode aplicar a política do controle de acesso até que você adicione primeiramente uma licença da Filtragem URL ao centro de gerenciamento de FireSIGHT, a seguir permita-o nos dispositivos visados pela política.

Se uma licença da Filtragem URL expira, o controle de acesso ordena com a categoria e as condições reputação-baseadas URL param de filtrar URL, e o centro de gerenciamento de FireSIGHT já não contacta o serviço da nuvem. Sem uma licença da Filtragem URL, as URL

individuais ou os grupos de URL podem ser ajustados para reservar ou obstruir, mas os dados da categoria ou da reputação URL não podem ser usados a fim filtrar o tráfego de rede.

Exigência da porta

Um sistema de FireSIGHT usa as portas 443/HTTPS e 80/HTTP a fim comunicar-se com o serviço da nuvem. A porta 443/HTTPS deve ser aberta bidirecional, e o acesso de entrada para mover 80/HTTP deve ser permitido no centro de gerenciamento de FireSIGHT.

Componentes Utilizados

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

- Dispositivos de FirePOWER: 7000 Series, 8000 Series
- Dispositivo virtual do sistema da prevenção de intrusão da próxima geração (NGIPS)
- Ferramenta de segurança adaptável (ASA) FirePOWER
- Versão de software 5.2 de Sourcefire ou mais atrasado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

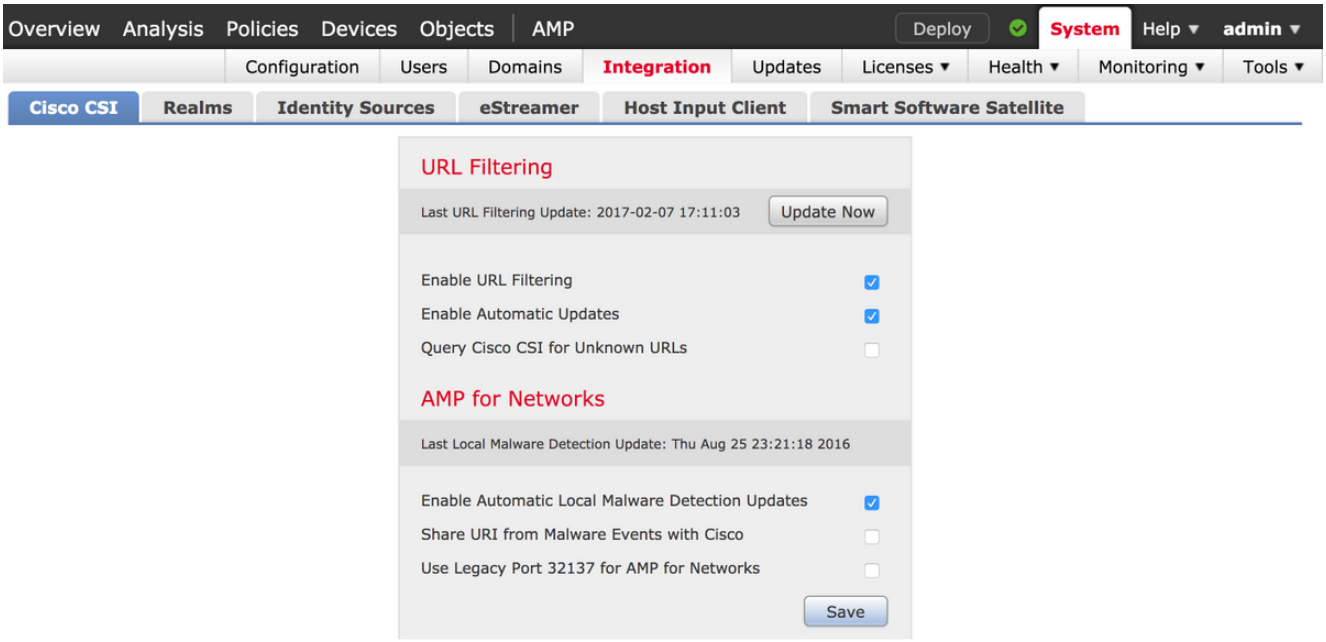
Permita a Filtragem URL no centro de gerenciamento de FireSIGHT

A fim permitir a Filtragem URL, termine estas etapas:

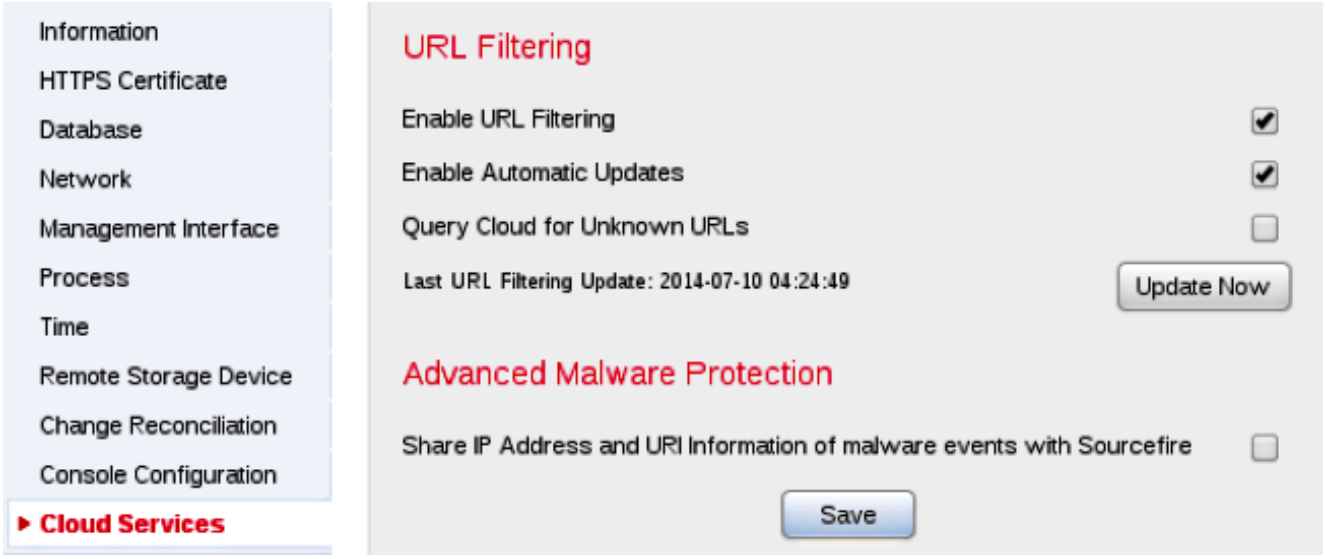
1. Log na relação de usuário de web do centro de gerenciamento de FireSIGHT.

2. A navegação é diferente baseada na versão de software que você executa:

   Na versão 6.1.x, escolha o **sistema > a integração > o Cisco CSI**.



Na versão 5.x, escolha o **sistema > o Local > a configuração**. Escolha **serviços da nuvem**.



3. Verifique a caixa de verificação da **Filtragem URL da possibilidade** a fim permitir a Filtragem URL.
4. Opcionalmente, verifique a caixa de verificação **automática das atualizações da possibilidade** a fim permitir atualizações automáticas. Esta opção permite que o sistema contacte o serviço da nuvem numa base regular a fim obter atualizações aos dados URL nos grupos dos dados locais do dispositivo.

   Note: Embora o serviço da nuvem atualize tipicamente seus dados uma vez pelo dia, se você permite automático o atualiza força o centro de gerenciamento de FireSIGHT a verificar cada 30 minutos a fim se certificar de que a informação é sempre atual. Embora as atualizações diárias tendessem a ser pequenas, se foi mais de cinco dias desde a última atualização, os dados novos da Filtragem URL puderam tomar até 20 minutos para transferir. Uma vez que as atualizações foram transferidas, pôde tomar até 30 minutos para executar a atualização própria.

5. Opcionalmente, verifique a **nuvem da pergunta para ver se há URL desconhecidas** para caixa de verificação desconhecida URL a fim perguntar o serviço da nuvem para URL

desconhecidas. Esta opção permite que o sistema pergunte a nuvem de Sourcefire quando alguém em sua rede monitorada tenta consultar a uma URL que não esteja no grupo dos dados locais. Se a nuvem não conhece a categoria ou a reputação de uma URL, ou se o centro de gerenciamento de FireSIGHT não pode contactar a nuvem, a URL não combina regras do controle de acesso com a categoria ou as condições reputação-baseadas URL.

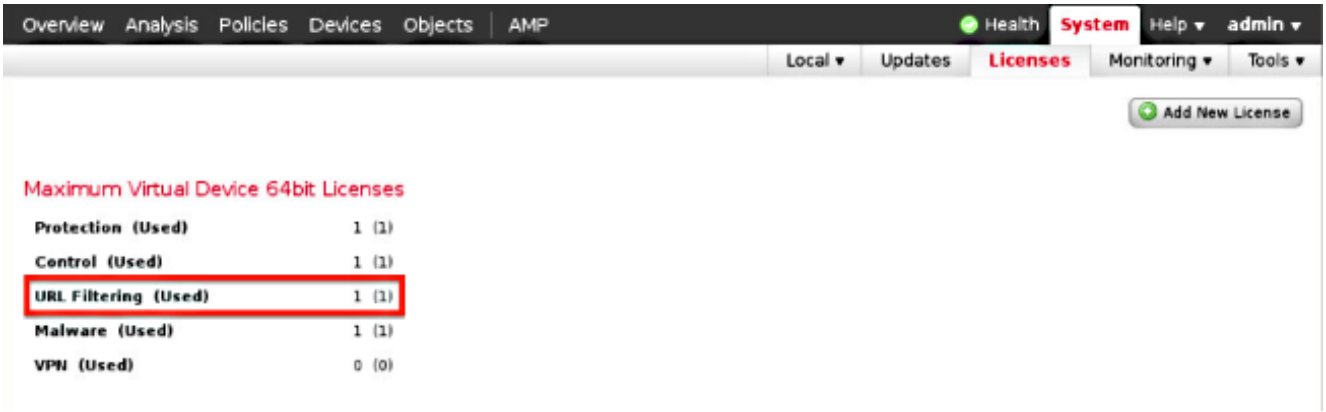
Note: Você não pode atribuir categorias ou reputações às URL manualmente. Desabilite esta opção se você não quer suas URL uncategorized ser catalogado pela nuvem de Sourcefire, por exemplo, para razões da privacidade.

6. Click **Save**. Os ajustes da Filtragem URL salvar.

Note: Baseado no intervalo de tempo desde que a Filtragem URL foi permitida por último, ou se este é a primeira vez você permitiu a Filtragem URL, um centro de gerenciamento de FireSIGHT recupera os dados da Filtragem URL do serviço da nuvem.

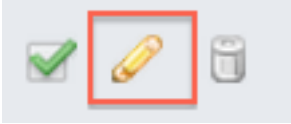
Aplique a licença da Filtragem URL em um dispositivo gerenciado

1. Verifique se a licença da Filtragem URL é instalada no centro de gerenciamento de FireSIGHT. Vá à página do **sistema > das licenças** a fim encontrar uma lista de licenças.

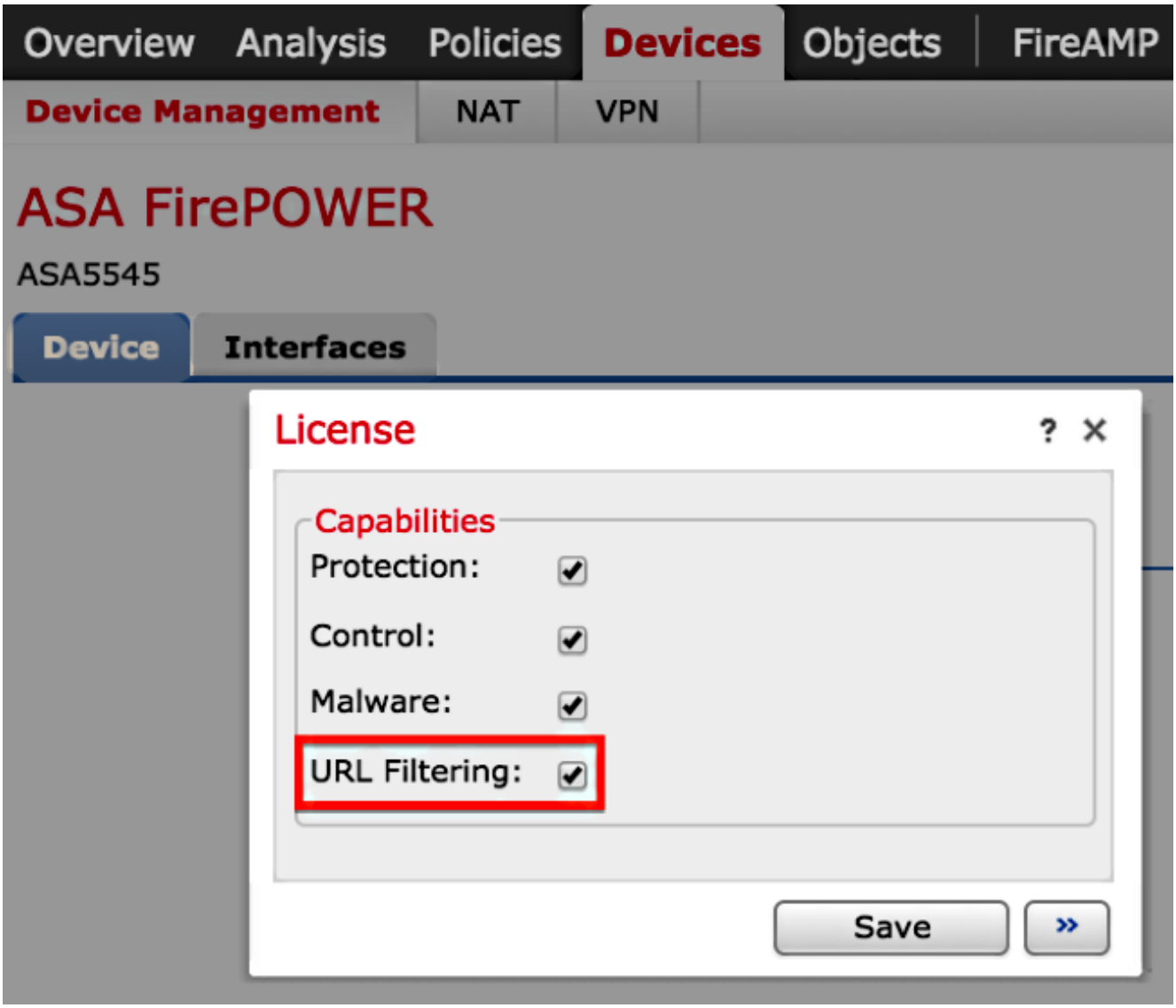


2. Vá à página dos **dispositivos > do Gerenciamento de dispositivos**, e verifique se a licença da Filtragem URL é aplicada no dispositivo que monitora o tráfego.

3. Se a licença da Filtragem URL não é aplicada em um dispositivo, clique o ícone do **lápis** a fim editar os ajustes. O ícone é ficado situado ao lado do nome de dispositivo.



4. Você pode permitir a licença da Filtragem URL em um dispositivo da aba dos **dispositivos**.



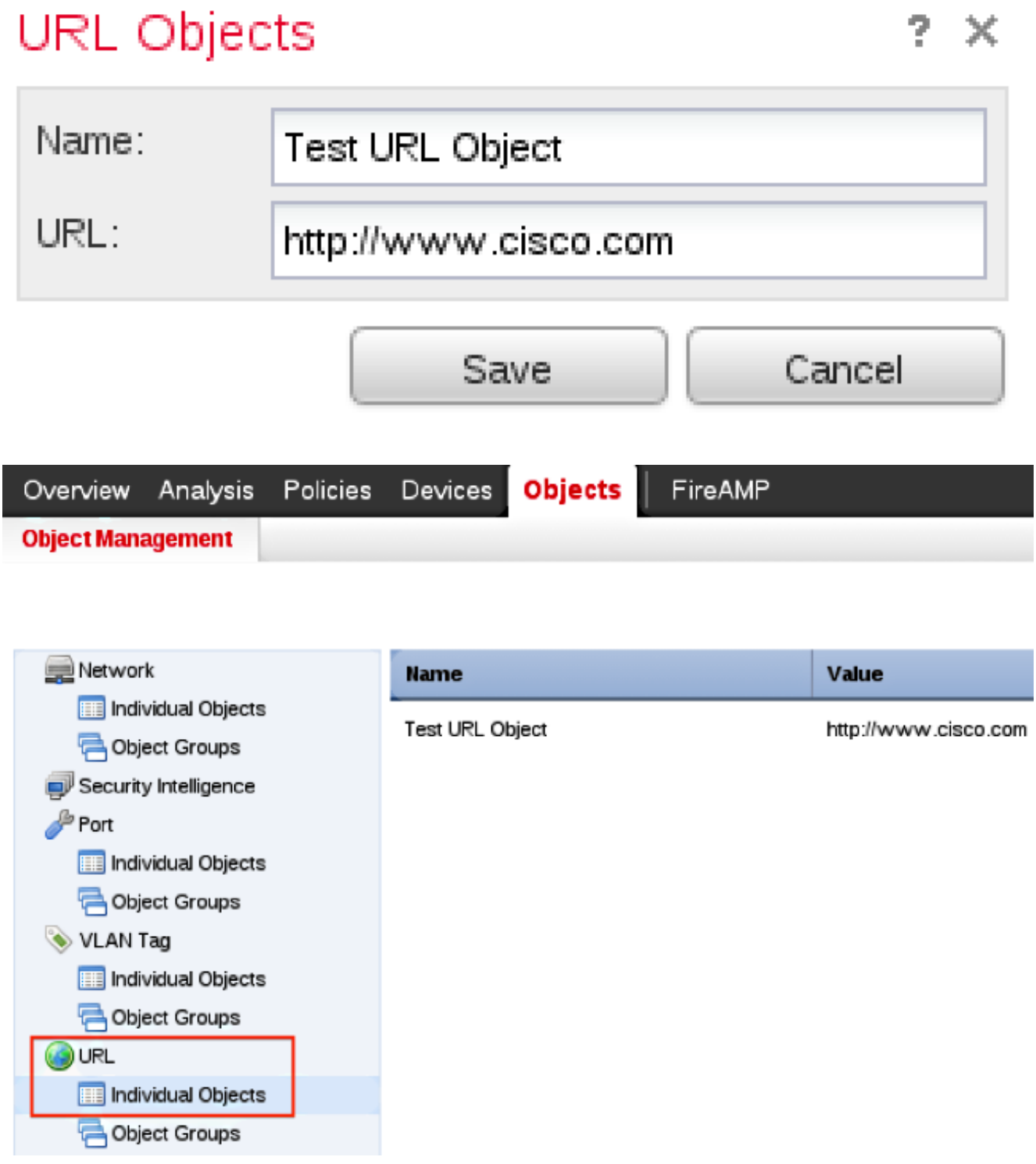
5. Depois que você permite uma licença e salvar suas mudanças, você igualmente deve clicar **aplica mudanças** a fim aplicar a licença em seu dispositivo gerenciado.

Exclusão de um local específico da categoria obstruída URL

O centro de gerenciamento de FireSIGHT não permite que você tenha uma avaliação local das URL que cancelam as avaliações fornecidas Sourcefire da categoria do padrão. A fim realizar esta tarefa, você deve usar uma política do controle de acesso. Estas instruções descrevem como usar um objeto URL em uma regra do controle de acesso a fim excluir um local específico de uma categoria do bloco.

1. Vá aos **objetos > à** página do **Gerenciamento do objeto**.

2. **Escolha objetos individuais** para a URL, e clique o botão **adicionar URL**. O indicador dos **objetos URL** aparece.

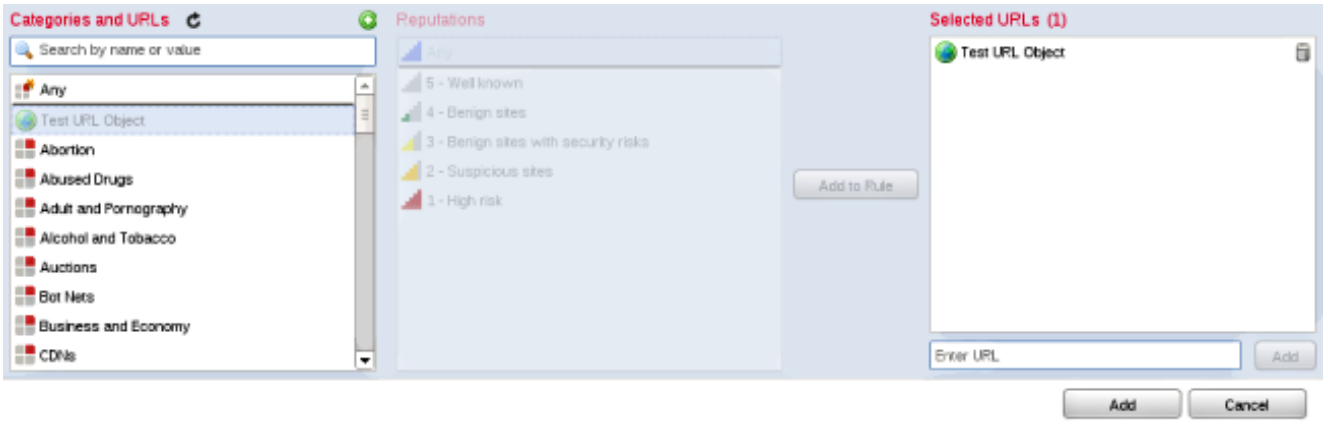


3. Depois que você salvar as mudanças, escolha **políticas > controle de acesso** e clique o ícone do **lápis** a fim editar a política do controle de acesso.

4. O clique **adiciona a regra**.

5. Adicionar seu objeto URL à regra com a ação **reservar** e coloque-o acima da regra da

categoria URL, de modo que sua ação da regra seja avaliada primeiramente.



6. Depois que você adiciona a regra, clique a **salvaguarda e aplique-a**. Salvar as mudanças novas e aplica a política do controle de acesso aos dispositivos controlados.

Verificar

Para a informação Verify ou Troubleshoot, refira as **edições da pesquisa de defeitos com a Filtragem URL no** artigo do **sistema de FireSIGHT** ligado na seção Informação Relacionada.

Troubleshooting

Para a informação Verify ou Troubleshoot, refira as **edições da pesquisa de defeitos com a Filtragem URL no** artigo do **sistema de FireSIGHT** ligado na seção Informação Relacionada.

Informações Relacionadas

- Pesquise defeitos edições com a Filtragem URL no sistema de FireSIGHT
- Suporte Técnico e Documentação - Cisco Systems