Pesquise defeitos edições com Filtragem URL em um sistema de FireSIGHT

Índice

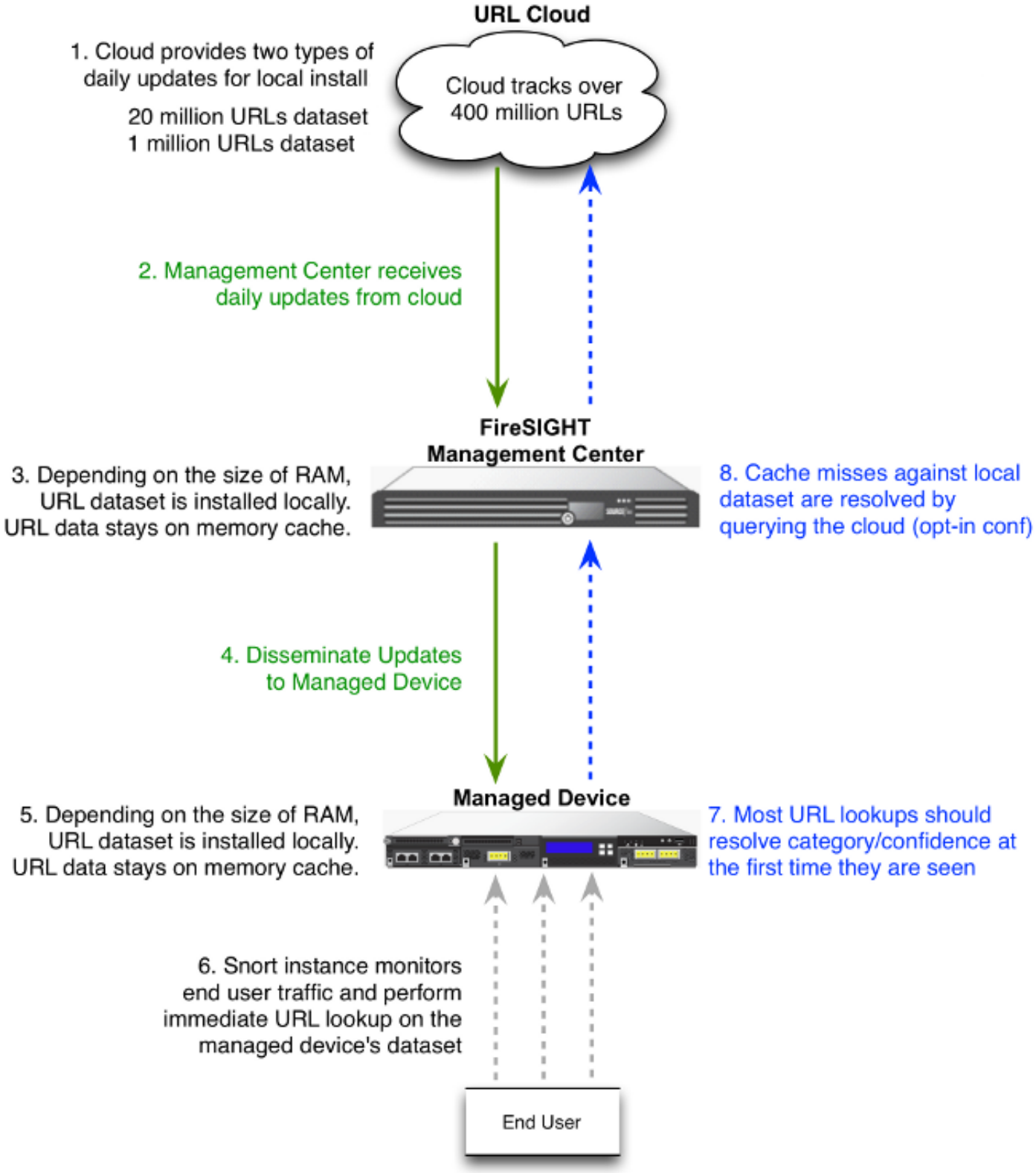
Introdução

Este documento descreve problemas comuns com Filtragem URL. A característica da Filtragem URL no centro de gerenciamento de FireSIGHT categoriza o tráfego de anfitriões monitorados e permite que você escreva uma circunstância em uma regra do controle de acesso baseada na reputação.

Processo de consulta da Filtragem URL

A fim acelerar o processo de consulta URL, a Filtragem URL fornece um conjunto de dados que seja instalado em um sistema da potência de fogo localmente. O dependente em cima da quantidade de memória (RAM) disponível em um dispositivo, lá é dois tipos de conjunto de dados:

Tipo de conjunto de dados	Requisito de memória	
	Na versão 5.3	Na versão 5.4 ou mais recente
20 milhão conjunto de dados URL	>2GB	>3.4 GB
1 milhão conjunto de dados URL	<= 2GB	<= 3.4 GB



Problemas de conectividade da nuvem

Passo 1: Verifique as licenças

A licença é instalada?

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 o permite nos dispositivos visados pela política.

A licença é expirada?

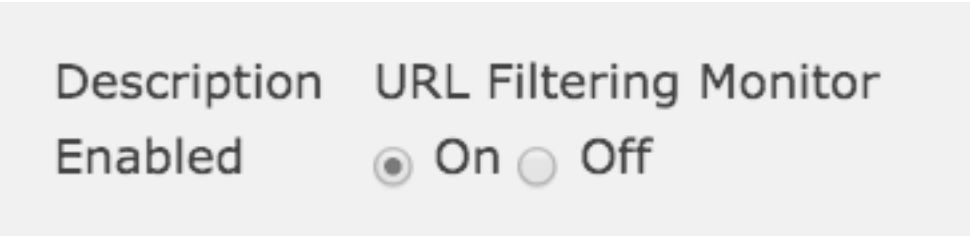
Se uma licença da Filtragem URL expira, o controle de acesso ordena com a categoria e as condições reputação-baseadas URL param de filtrar URL, e o centro de gerenciamento de FireSIGHT já não contacta o serviço da nuvem.

> Dica: Leia a Filtragem URL em um exemplo da configuração de sistema de FireSIGHT a fim aprender como permitir a característica da Filtragem URL em um sistema de FireSIGHT e aplicar a licença da Filtragem URL em um dispositivo gerenciado.

Passo 2: Verifique alertas da saúde

O módulo do monitor da Filtragem URL segue comunicações entre o centro de gerenciamento de FireSIGHT e a nuvem de Cisco, onde o sistema obtém seus dados da Filtragem URL (categoria e reputação) para URL geralmente visitadas. O módulo do monitor da Filtragem URL igualmente segue comunicações entre um centro de gerenciamento de FireSIGHT e todos os dispositivos gerenciado onde você permitiu a Filtragem URL.

A fim permitir a Filtragem URL monitore o módulo, vão à página da **configuração das normas da saúde**, escolhem o **monitor da Filtragem URL**. Clique **sobre o** botão de rádio para a opção **permitida** a fim permitir o uso do módulo para testes do estado de saúde. Você deve aplicar a política sanitária ao centro de gerenciamento de FireSIGHT se você quer seus ajustes tomar o efeito.



- **Alerta crítico**: Se o centro de gerenciamento de FireSIGHT não se comunica com sucesso com nem não se recupera uma atualização da nuvem, a classificação do estado para mudanças desse módulo a *crítico*.
- **Alerta de advertência**: Se o centro de gerenciamento de FireSIGHT se comunica com sucesso com a nuvem, o status de módulo muda a *advertir* se o centro de gerenciamento não pode empurrar dados novos da Filtragem URL para seus dispositivos gerenciado.

Passo 3: Verifique ajustes DNS

Um centro de gerenciamento de FireSIGHT comunica-se com estes server durante a consulta da nuvem:

```
database.brightcloud.com
service.brightcloud.com
```

Uma vez que você se certifica de que ambos os server estão permitidos no Firewall, execute estes comandos no centro de gerenciamento de FireSIGHT e verifique se o centro de gerenciamento pode resolver os nomes:

admin@FireSIGHT:~$ **sudo nslookup database.brightcloud.com** admin@FireSIGHT:~$ **sudo nslookup service.brightcloud.com**

Passo 4: Verifique a Conectividade às portas exigidas

Os sistemas de FireSIGHT usam as portas 443/HTTPS e 80/HTTP a fim comunicar-se com o serviço da nuvem.

Uma vez que você confirma que o centro de gerenciamento pode executar um `nslookup` bem sucedido, verifique a Conectividade à porta 80 e à porta 443 com `telnet`. O base de dados URL está transferido com `database.brightcloud.com na` porta 443, quando as perguntas desconhecidas URL forem feitas em `service.brightcloud.com na` porta 80.

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

Esta saída é um exemplo de uma `conexão Telnet` bem sucedida a `database.brightcloud.com`.

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

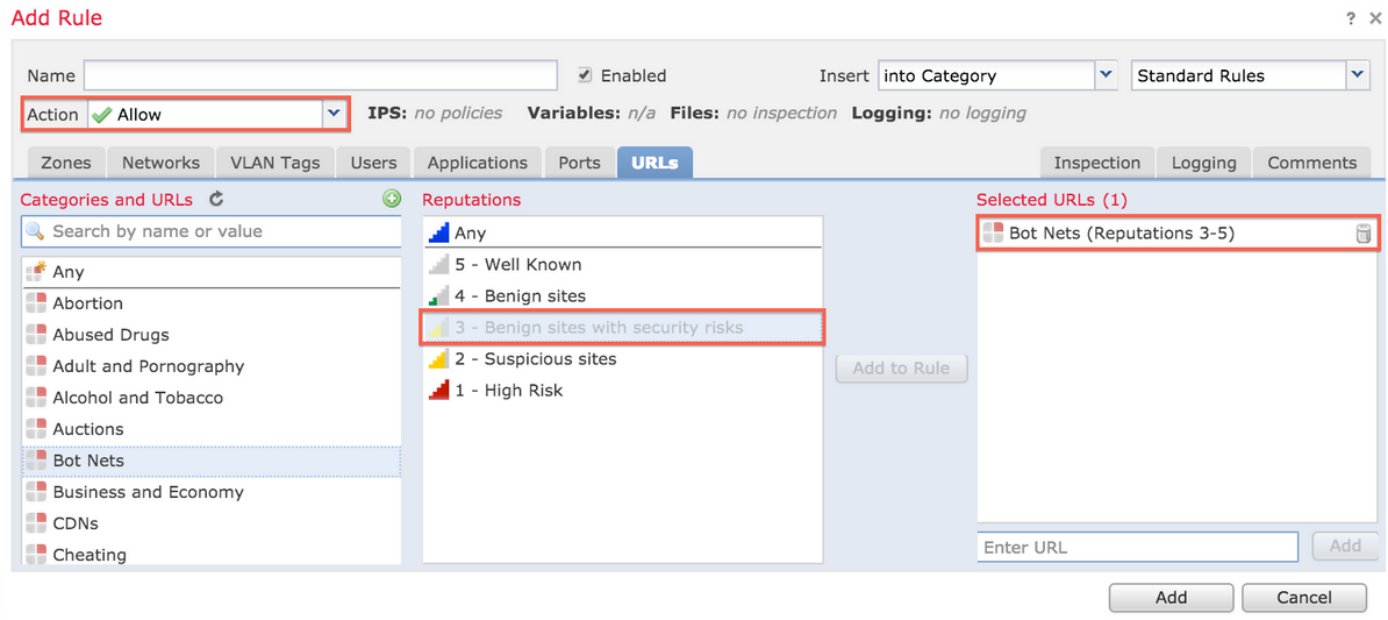
Controle de acesso e edições de Miscategorization

Problema 1: A URL com nível Unselected da reputação é permitida/obstruída

Se você observa uma URL está permitida ou obstruída, mas você não selecionou a reputação em nível dessa URL em sua regra do controle de acesso, lê esta seção a fim compreender como uma regra de Filtragem URL trabalha.

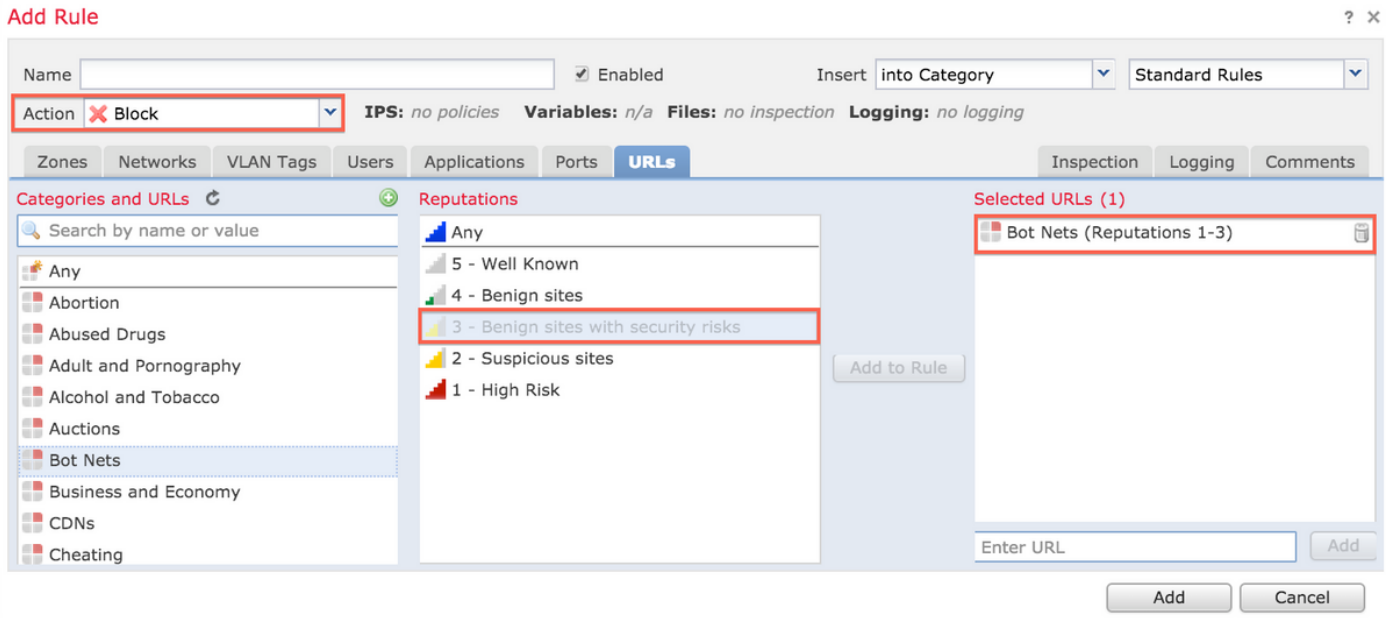
A ação da regra é reserva

Quando você cria uma regra **para permitir o** tráfego baseado em um nível da reputação, a seleção de um nível da reputação igualmente seleciona todos os níveis da reputação menos seguros do que o nível que você selecionou originalmente. Por exemplo, se você configura uma regra para permitir *locais benignos com riscos de segurança* (nível 3), igualmente permite automaticamente *locais benignos* (nível 4) e (nível 5) locais *conhecidos*.



A ação da regra é bloco

Quando você cria uma regra **para obstruir o** tráfego baseado em um nível da reputação, a seleção de um nível da reputação igualmente seleciona todos os níveis da reputação mais severos do que o nível que você selecionou originalmente. Por exemplo, se você configura uma regra para obstruir *locais benignos com riscos de segurança* (nível 3), igualmente obstrui automaticamente *locais suspeitos* (nível 2) e locais do *alto risco* (nível 1).



Matriz da seleção URL

Nível selecionado da reputação	Ação selecionada da regra				
	Alto risco	**Local suspeito**	**Local benigno com risco de segurança**	**Local benigno**	**Conhe**
1 - Alto risco	O bloco, reserva	Reserve	Reserve	Reserve	Reser
2 - Locais suspeitos	Bloco	O bloco, reserva	Reserve	Reserve	Reser
3 - Locais benignos com risco de segurança	Bloco	Bloco	O bloco, reserva	Reserve	Reser
4 - Locais benignos	Bloco	Bloco	Bloco	O bloco, reserva	Reser
5 - Conhecido	Bloco	Bloco	Bloco	Bloco	O bloc reserv

Problema 2: O convite não trabalha na regra do controle de acesso

O sistema de FireSIGHT não apoia a especificação de um convite em uma condição URL. Esta circunstância pôde não alerta em `cisco.com`.

`*cisco*.com`

Além, uma URL incompleta pôde combinar contra o outro tráfego que causa um resultado indesejado. Quando você especifica URL individuais em condições URL, você deve com cuidado considerar o outro tráfego que pôde ser afetado. Por exemplo, considere uma encenação onde você queira obstruir explicitamente `cisco.com`. Contudo, a harmonização do substring significa que isso obstruir `cisco.com` igualmente obstrui `sanfrancisco.com`, que não puderam ser sua

intenção.

Quando você incorpora uma URL, incorpore o Domain Name e omita a informação do subdomínio. Por exemplo, datilografe `cisco.com` um pouco do que `www.cisco.com`. Quando você usa `cisco.com em uma` regra **reservar**, os usuários poderiam consultar a qualqueras um URL: `http://cisco.com`
`http://cisco.com/newcisco`
`http://www.cisco.com`

Problema 3: A categoria e a reputação URL não são povoadas

Se uma URL não está em um base de dados local e é a primeira vez que a URL está vista no tráfego, uma categoria ou uma reputação não puderam ser povoadas. Isto significa que a primeira vez que uma URL desconhecida é vista, não combina a regra AC. Às vezes as consultas URL para URL geralmente visitadas não puderam resolver na primeira vez que uma URL é vista. Esta edição é fixada na versão 5.3.0.3, 5.3.1.2, e 5.4.0.2, 5.4.1.1.

Informações Relacionadas

- Configuração da Filtragem URL em um sistema de FireSIGHT
- Suporte Técnico e Documentação - Cisco Systems