Solucionar problemas com filtragem de URL em um sistema FireSIGHT

Contents

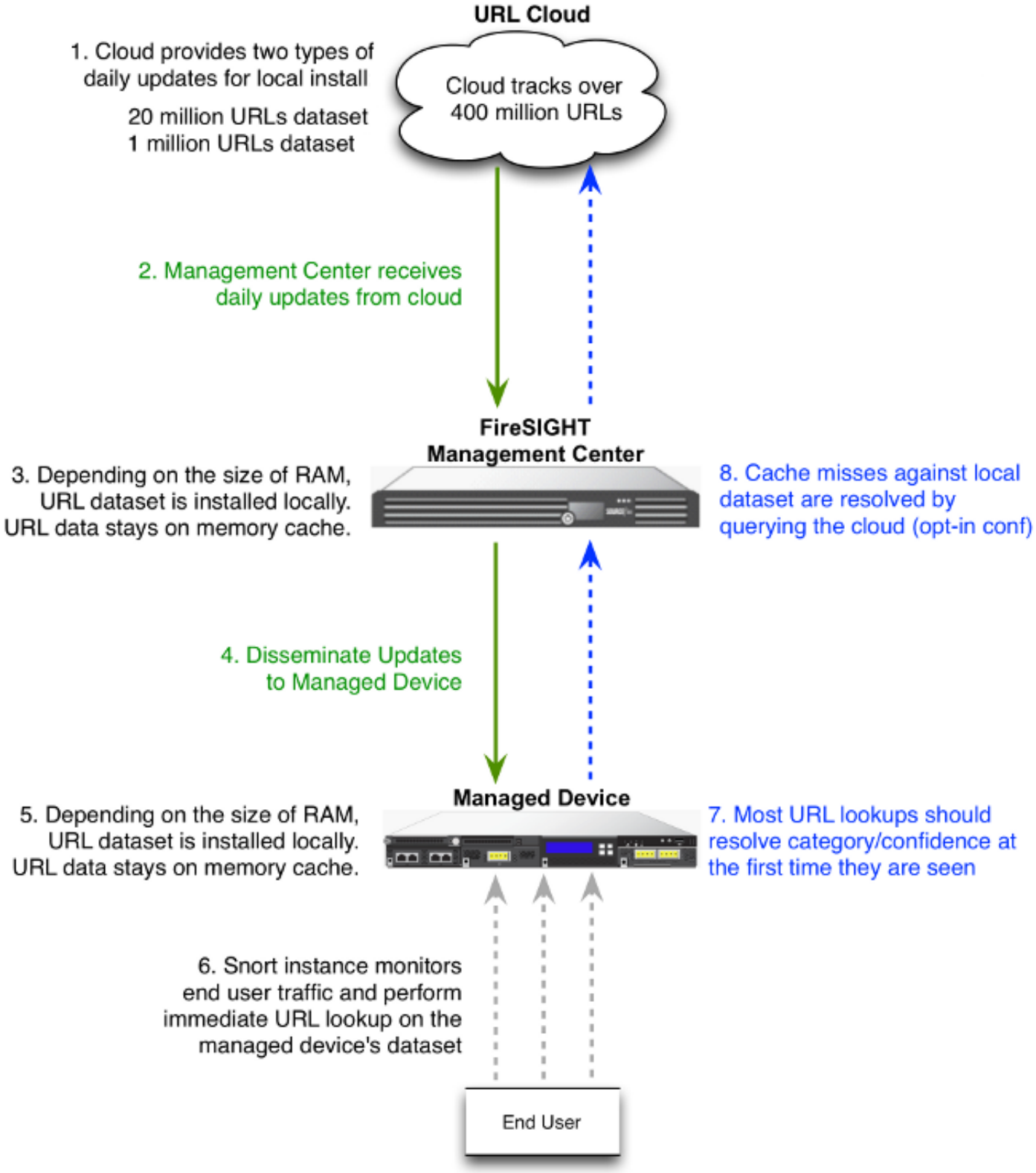
Introduction

Este documento descreve problemas comuns com a filtragem de URL. O recurso de filtragem de URL no FireSIGHT Management Center categoriza o tráfego de hosts monitorados e permite gravar uma condição em uma regra de controle de acesso com base na reputação.

Processo de pesquisa de filtragem de URL

Para acelerar o processo de pesquisa de URL, a filtragem de URL fornece um conjunto de dados instalado localmente em um Firepower System. Dependendo da quantidade de memória (RAM) disponível em um dispositivo, há dois tipos de conjuntos de dados:

Tipo de Conjunto de Dados	Requisito de memória	
	Na versão 5.3	Na versão 5.4 ou superior
Conjunto de dados de 20 milhões de URLs	>2 GB	>3,4 GB
Conjunto de dados de 1 milhão de URLs	<= 2 GB	<= 3,4 GB



Problemas de conectividade de nuvem

Passo 1: Verifique as licenças

A licença está instalada?

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, não é possível aplicar a política de controle de acesso até que você adicione uma licença de filtragem de URL ao FireSIGHT

Management Center e, em seguida, habilite-a nos dispositivos de destino da política.

A licença expirou?

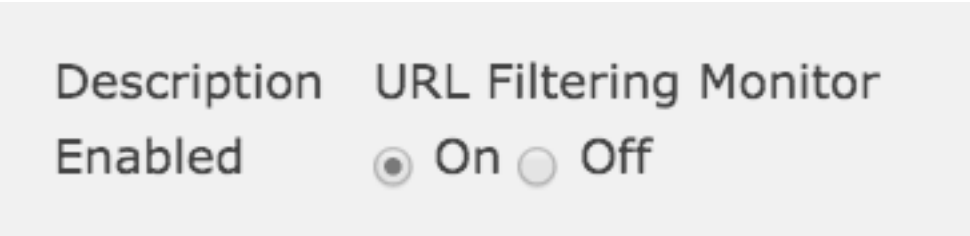
Se uma licença de filtragem de URL expirar, as regras de controle de acesso com condições de URL baseadas em categoria e reputação deixarão de filtrar URLs e o FireSIGHT Management Center não contatará mais o serviço de nuvem.

> **Tip**: Leia o Exemplo de configuração de filtragem de URL em um sistema FireSIGHT para saber como habilitar o recurso de filtragem de URL em um sistema FireSIGHT e aplicar a licença de filtragem de URL em um dispositivo gerenciado.

Passo 2: Verificar Alertas de Integridade

O módulo Monitor de filtragem de URL rastreia as comunicações entre o FireSIGHT Management Center e a nuvem da Cisco, onde o sistema obtém seus dados de filtragem de URL (categoria e reputação) para URLs visitados com frequência. O módulo Monitor de filtragem de URL também rastreia comunicações entre um FireSIGHT Management Center e qualquer dispositivo gerenciado no qual você tenha habilitado a filtragem de URL.

Para habilitar o módulo Monitor de filtragem de URL, vá para a página **Configuração de política de integridade**, escolha **Monitor de filtragem de URL**. Clique no botão de opção **On** da opção **Enabled** para habilitar o uso do módulo para o teste de status de integridade. Você deve aplicar a política de integridade ao FireSIGHT Management Center se desejar que suas configurações sejam aplicadas.



- **Alerta crítico**: Se o FireSIGHT Management Center não conseguir se comunicar com a nuvem ou recuperar uma atualização da nuvem, a classificação de status desse módulo será alterada para *Crítico*.
- **Alerta de aviso**: Se o FireSIGHT Management Center se comunicar com êxito com a nuvem, o status do módulo mudará para *Aviso* se o Management Center não puder enviar novos dados de filtragem de URL para seus dispositivos gerenciados.

Passo 3: Verificar Configurações DNS

Um FireSIGHT Management Center se comunica com esses servidores durante a pesquisa na nuvem:

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

Quando você tiver certeza de que os dois servidores têm permissão no firewall, execute estes comandos no FireSIGHT Management Center e verifique se o Management Center pode resolver

os nomes:

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

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

Passo 4: Verifique a conectividade para as portas necessárias

Os FireSIGHT Systems usam as portas 443/HTTPS e 80/HTTP para se comunicar com o serviço de nuvem.

Depois de confirmar que o Management Center é capaz de executar um nslookup bem-sucedido, verifique a conectividade com a porta 80 e a porta 443 com telnet. O banco de dados de URL é baixado com database.brightcloud.com na porta 443, enquanto as consultas de URL desconhecidas são 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 com database.brightcloud.com.

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

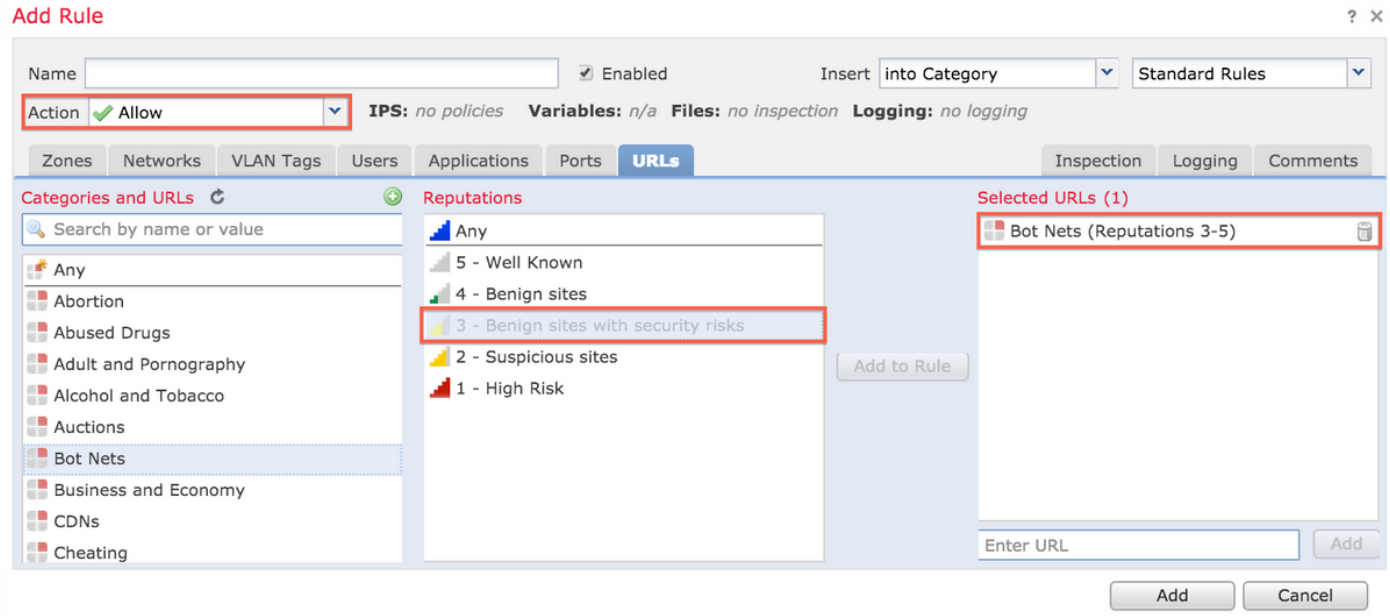
Problemas de controle de acesso e erros de categorização

Problema 1: A URL com nível de reputação não selecionado é permitida/bloqueada

Se você perceber que um URL é permitido ou bloqueado, mas não selecionou o nível de reputação desse URL em sua Regra de controle de acesso, leia esta seção para entender como funciona uma regra de filtragem de URL.

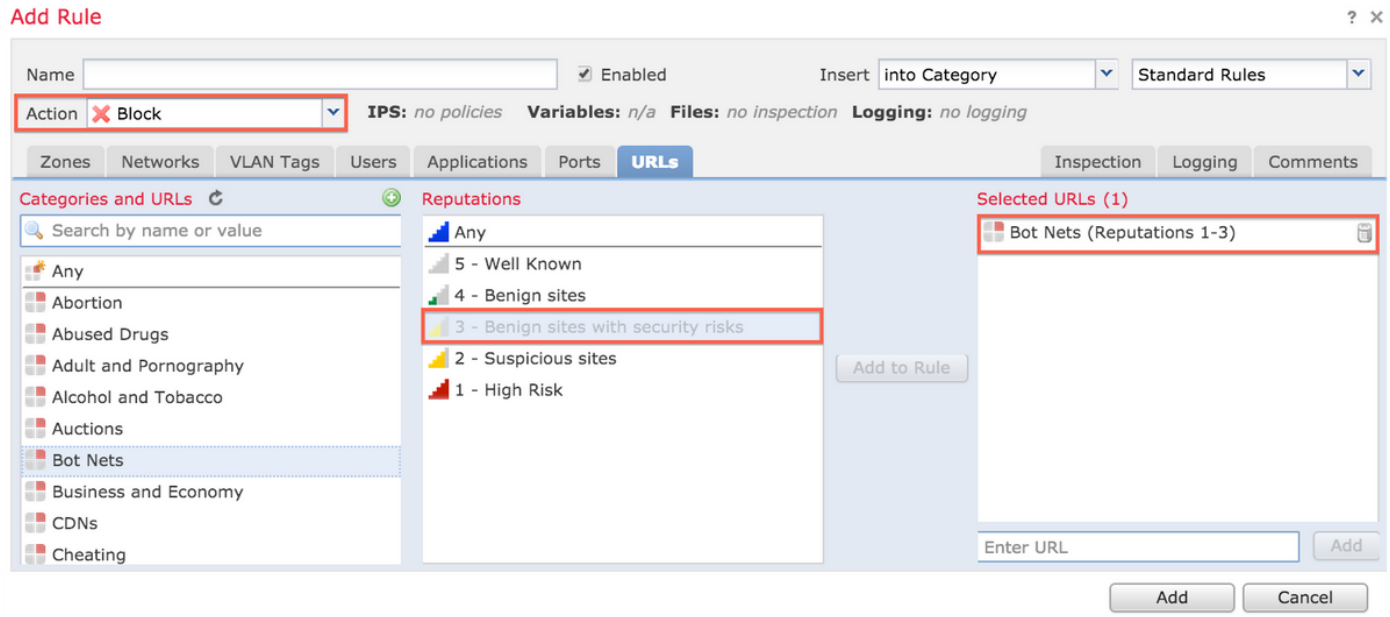
A ação da regra é permitir

Quando você cria uma regra para **Permitir** tráfego com base em um nível de reputação, a seleção de um nível de reputação também seleciona todos os níveis de reputação menos seguros do que o nível selecionado originalmente. Por exemplo, se você configurar uma regra para permitir *sites benignos com riscos de segurança* (nível 3), ela também permitirá automaticamente *sites benignos* (nível 4) e *bem conhecidos* (nível 5).



A ação da regra é bloquear

Quando você cria uma regra para **Bloquear** o tráfego com base em um nível de reputação, a seleção de um nível de reputação também seleciona todos os níveis de reputação mais severos do que o nível selecionado originalmente. Por exemplo, se você configurar uma regra para bloquear *Sites Benignos com riscos de segurança* (nível 3), ela também bloqueará automaticamente *Sites suspeitos* (nível 2) e *Sites de alto risco* (nível 1).



Matriz de seleção de URL

Nível de reputação selecionado	Ação da regra selecionada				
	Alto risco	**Site suspeito**	**Site benigno com risco à segurança**	**Local benigno**	**Bem conhec**
1 - Alto risco	Bloquear, Permitir	Permissão	Permissão	Permissão	Permis
2 - Sites suspeitos	Bloqueio	Bloquear, Permitir	Permissão	Permissão	Permis
3 - Sites benignos com risco	Bloqueio	Bloqueio	Bloquear, Permitir	Permissão	Permis

à segurança					
4 - Locais Benignos	Bloqueio	Bloqueio	Bloqueio	Bloquear, Permitir	Permis
5 - Bem conhecido	Bloqueio	Bloqueio	Bloqueio	Bloqueio	Bloque Permiti

Problema 2: O caractere curinga não funciona na regra de controle de acesso

O FireSIGHT System não suporta a especificação de um curinga em uma condição de URL. Essa condição pode falhar ao alertar em cisco.com.

```
*cisco*.com
```

Além disso, um URL incompleto pode ser comparado a outro tráfego, o que causa um resultado indesejado. Ao especificar URLs individuais em condições de URL, você deve considerar cuidadosamente outro tráfego que possa ser afetado. Por exemplo, considere um cenário em que você deseja bloquear explicitamente o cisco.com. No entanto, a correspondência de substring significa que bloquear cisco.com também bloqueia sanfrancisco.com, o que pode não ser sua intenção.

Ao inserir um URL, insira o nome de domínio e omita as informações de subdomínio. Por exemplo, digite cisco.com em vez de www.cisco.com. Quando você usa cisco.com em uma regra Allow, os usuários podem navegar para qualquer um destes URLs:

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

Problema 3: A categoria e a reputação da URL não são preenchidas

Se um URL não estiver em um banco de dados local e for a primeira vez que o URL for visto no tráfego, uma categoria ou reputação poderá não ser preenchida. Isso significa que a primeira vez que uma URL desconhecida é vista, ela não corresponde à regra AC. Às vezes, as pesquisas de URLs comumente visitados podem não resolver na primeira vez que um URL é visto. Esse problema é corrigido nas versões 5.3.0.3, 5.3.1.2 e 5.4.0.2, 5.4.1.1.

Informações Relacionadas

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