

Identificar e Solucionar Problemas e Verificar a Categoria de URL no CSF

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Informações de Apoio](#)

[Arquitetura](#)

[Passo 1: Pesquise a categoria de URL no FMC](#)

[Passo 2: Examinar Configurações de Integração de Filtragem de URL](#)

[Passo 3: Confirme a categoria de URL no dispositivo usando o rastreamento de suporte do sistema](#)

[Passo 4: Resolver o número da categoria para um nome de categoria](#)

[Verificar](#)

[Botão Contestar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como verificar as atribuições de categoria de URL no Firewall Seguro e no FMC para garantir que o dispositivo esteja usando a mesma classificação de URL.

Pré-requisitos

Você deve ter a licença de Filtragem de URL habilitada para o dispositivo, a integração de Serviços em Nuvem em um estado íntegro e uma política de controle de acesso que inclua a filtragem de URL e tenha sido implantada após a condição de URL ser configurada.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Filtragem de URL e pesquisas de categoria do Firepower Management Center (FMC)
- Inspeção de tráfego e avaliação de políticas do Cisco Secure Firewall (CSF)
- Categorização de URL e comportamento de reputação, que é baseado no Talos a partir da versão 6.5 do CSF

Componentes Utilizados

Este documento descreve a funcionalidade disponível no Cisco Secure Firewall e no FMC versões 6.5 e posteriores. Os exemplos neste guia usam a versão 7.6.5.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com estes produtos e versões:

- Centro de gerenciamento seguro de firewall (FMC)
- Cisco Secure Firewall (CSF)
- Filtragem de URL e integrações de serviços em nuvem

Informações de Apoio

A filtragem de URL depende de um banco de dados de categoria que é avaliado durante a inspeção de tráfego. O FMC armazena as informações de categoria de URL para um destino e o dispositivo executa uma pesquisa de tempo de execução quando o tráfego é inspecionado. Quando há uma incompatibilidade entre o FMC, o dispositivo ou o banco de dados em nuvem, os resultados da política podem parecer inconsistentes mesmo quando a política de controle de acesso está configurada corretamente.

Uma parte importante da verificação é confirmar que a atribuição da categoria de URL é consistente no FMC e no dispositivo. A pesquisa de categoria de URL é influenciada pelas configurações de integração dos Serviços em Nuvem e pelo cache do dispositivo. Se a configuração de atualização do cache estiver desabilitada ou o tempo de vida da entrada for muito longo, os dados de categoria obsoletos poderão permanecer em uso depois que o Talos atualizar a classificação.

Arquitetura

Quando a filtragem de URL está habilitada, o dispositivo primeiro verifica o cache de URL local. Se a categoria ainda não estiver presente no cache, o dispositivo poderá consultar o banco de dados local ou a nuvem da Cisco. O dispositivo usa o banco de dados de URL local e o cache de pesquisa durante a inspeção, e o beakerd se comunica com o Talos para baixar e atualizar dados de filtragem de URL. Em dispositivos gerenciados pelo FMC, o bico é executado no FMC e está em estado de espera no CSF. Se o CSF for gerenciado localmente, o processo será executado no próprio dispositivo.

O Talos envia pacotes completos de bancos de dados em vários tamanhos, que são armazenados em `/var/sf/cloud_download/cisco`.

Aqui estão alguns exemplos de como podem ser os arquivos de banco de dados do Talos:

- `cisco_uridb_large_1541554243` (500 MB)
- `cisco_uridb_medium_1541553645` (125 MB)
- `cisco_uridb_small_1541553061` (33 MB)



Note: Os arquivos do banco de dados começam com `cisco_uridb` e, em seguida, o tamanho é listado (pequeno, médio ou grande). Os tamanhos podem variar dependendo do hardware que está sendo usado.

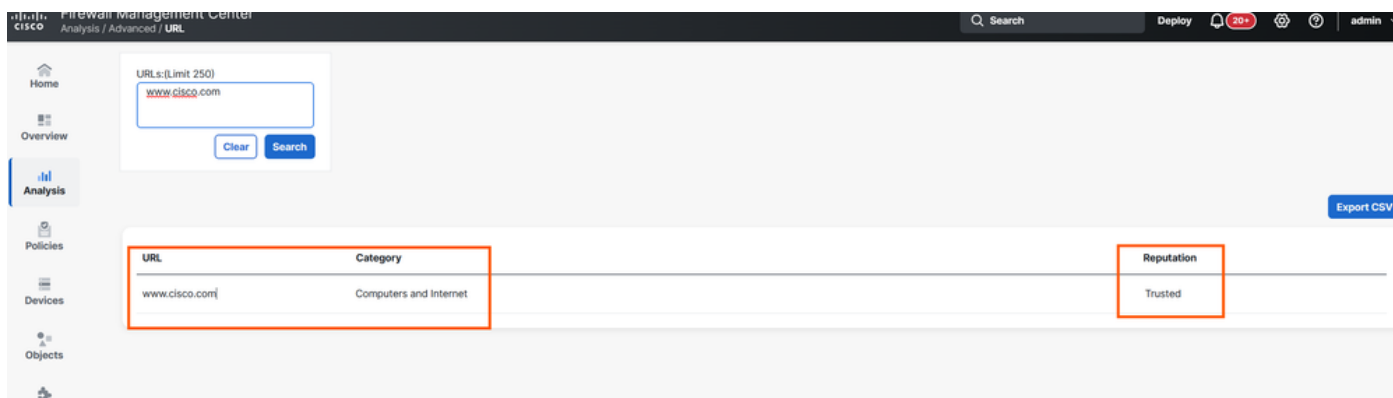
Passo 1: Pesquise a categoria de URL no FMC

O FMC mantém um banco de dados de URL local que mapeia os destinos de URL para as categorias que lhe foram atribuídas. Esta é a primeira etapa recomendada ao validar como uma URL está sendo classificada.

Navegue até o local `Analysis > Advanced > URL` no FMC.

Insira a URL que você deseja investigar e revise sua categoria atribuída.

No exemplo mostrado abaixo, www.cisco.com está listado na categoria Computadores e Internet.



Passo 2: Examinar Configurações de Integração de Filtragem de URL

As configurações de integração de filtragem de URL determinam onde o FMC e o dispositivo CSF originam seu banco de dados de categoria de URL. Cada dispositivo mantém seu próprio banco de dados local para pesquisa de URL e pode consultar o Cisco Cloud para obter inteligência de URL adicional ou atualizada.

Navegue até Integração > Outras integrações > Serviços em nuvem no FMC para revisar essas configurações.

URL Filtering

Last URL Filtering Update: 2026-08-26 10:28:52 [Update Now](#)

Enable Automatic Updates

URL Query Source

Local Database Only

Local Database and Cisco Cloud

Cisco Cloud Only

Cached URLs Expire

After 2 hours

[Dispute URL categories and reputations](#)

Save

Verifique se a integração está íntegra e se o cache de pesquisa de URL está configurado para ser atualizado de acordo com o tempo de política esperado.



Caution: O cache de pesquisa de URL pode reter a categoria recuperada anteriormente e os resultados de reputação. Se a expiração do cache for desativada ou configurada com uma vida útil longa, o dispositivo poderá continuar usando informações armazenadas em cache depois que o Talos atualizar a classificação, o que pode fazer com que o resultado do dispositivo seja temporariamente diferente da consulta atual do FMC ou do Talos.

Passo 3: Confirme a categoria de URL no dispositivo usando o rastreamento de suporte do sistema

Para verificar se o dispositivo CSF categoriza o URL da mesma maneira que o FMC, execute um rastreamento de suporte do sistema a partir da CLI do dispositivo. Isso mostra como o

mecanismo de inspeção Snort avalia o tráfego e qual categoria de URL é retornada quando a conexão é inspecionada.

Na CLI do FTD, insira o comando `system support trace` e responda aos prompts interativos:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 173.37.145.84
Please specify a server port: 443
```



Note: Neste exemplo, 173.37.145.84 é o endereço IP para www.cisco.com. Use o endereço IP destino que corresponde ao URL que você está investigando.

Saída de exemplo:

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1: returned from url lookup, url_info is 90 2003
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1 URL lookup for www.cisco.com/ found rep 90, 2003
```

Nesta saída, o URL retorna um ID de categoria de 2003. A próxima etapa explica como resolver esse valor numérico para o nome da categoria correspondente.

Passo 4: Resolver o número da categoria para um nome de categoria

A pesquisa de categoria de URL no dispositivo retorna uma ID de categoria numérica. Para mapear esse número para um nome de categoria legível, abra o arquivo `aup_categories.json` no dispositivo.

Navegue para o diretório `/var/sf/cloud_download/` no CSF no modo expert. Verifique se você está no modo de usuário raiz.

Abra o arquivo de definições de categoria:

```
root@firepower:/var/sf/cloud_download# less aup_categories.json
```

Procure a ID de categoria retornada na saída de rastreamento. Exemplo de entrada para a categoria 2003:

```
{
  "id": 2003,
  "uuid": "abba9b63-bb10-4729-b901-2e2aa0f02003",
  "mnemonic": "comp",
  "name": "Computers and Internet",
  "type": "aup_cats",
  "state": "active"
}
```



Note: Os números de ID de categoria são consistentes em todos os dispositivos CSF. A mesma ID numérica é mapeada para o mesmo nome de categoria em cada dispositivo CSF.

Verificar

Use o resultado das Etapas 1 a 4 para confirmar se a atribuição da categoria de URL é consistente entre o banco de dados do FMC e o mecanismo Snort no dispositivo.

Neste exemplo:

- O banco de dados do FMC lista www.cisco.com como Computers and Internet (Computadores e Internet).
- A CLI do dispositivo retorna a ID de categoria 2003, que é mapeada para Computadores e Internet.

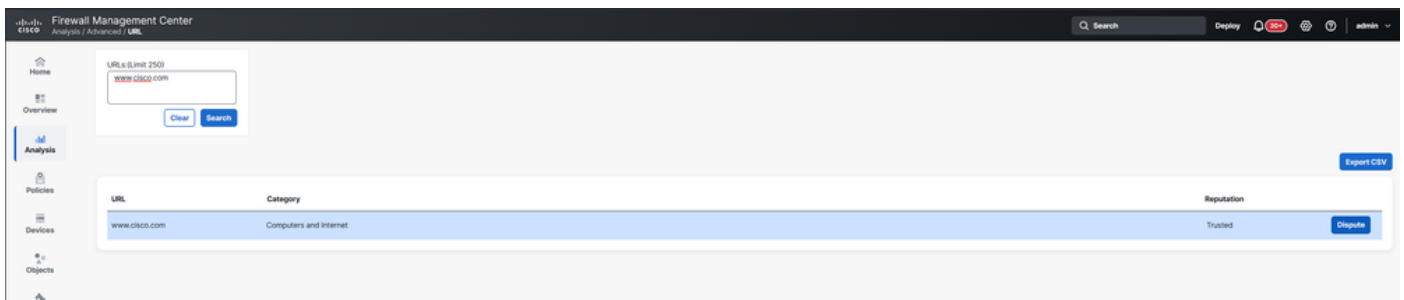
As duas fontes concordam, o que confirma que a política de filtragem de URL que está sendo aplicada é consistente para essa URL.

Botão Contestar

Se você acreditar que um URL foi classificado em uma categoria incorreta, poderá enviar uma contestação para o Talos.

Navegue até Analysis > Advanced > URL no FMC:

Digite o URL, clique em Pesquisar, passe o mouse sobre a entrada URL e selecione Dispute.



Isso abre a página de contestação do Talos para que a classificação possa ser revisada e corrigida pela fonte apropriada.

Troubleshooting

Se a classificação não corresponder às expectativas, revise estas áreas:

- Confirme se a licença de filtragem de URL está habilitada e atribuída ao dispositivo.
- Verifique a integridade dos serviços em nuvem e a conexão com o Talos.
- Inspecione o cache do dispositivo e as configurações de atualização do cache para confirmar se as entradas obsoletas não estão sendo reutilizadas.
- Verificar se o processo de frenagem está em execução no FMC para dispositivos gerenciados pelo FMC.

Para dispositivos gerenciados pelo FMC, execute este comando no modo de especialista do FMC para confirmar se o processo está ativo:

```
pmtool status | grep beakerd
```



Note: Se você executar esse comando em um firewall seguro gerenciado pelo FMC, o processo poderá ser visto em estado de espera. Se o Firewall Seguro for gerenciado localmente, o processo será visto em um estado de execução.

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.