Solucione problemas de incompatibilidade entre a filtragem de conteúdo e o Umbrella do Meraki MX

Contents

Introdução

Este documento descreve como solucionar problemas de incompatibilidade entre a filtragem de conteúdo do Meraki MX e o Umbrella.

Problema

Ao usar a filtragem de conteúdo Meraki MX fornecida pelo Cisco Talos, os clientes podem enfrentar inconsistências com alguns recursos de filtragem de DNS Umbrella.

- Página de bloqueio incorreta (páginas de bloqueio personalizadas não aplicadas)
- Recurso de desvio de página de bloqueio não exibido
- Erro "401 não autorizado" para sites que usam o Proxy Inteligente
- Os testes Policy-Debug mostram Org / Origin ID/ BundleID incorretos

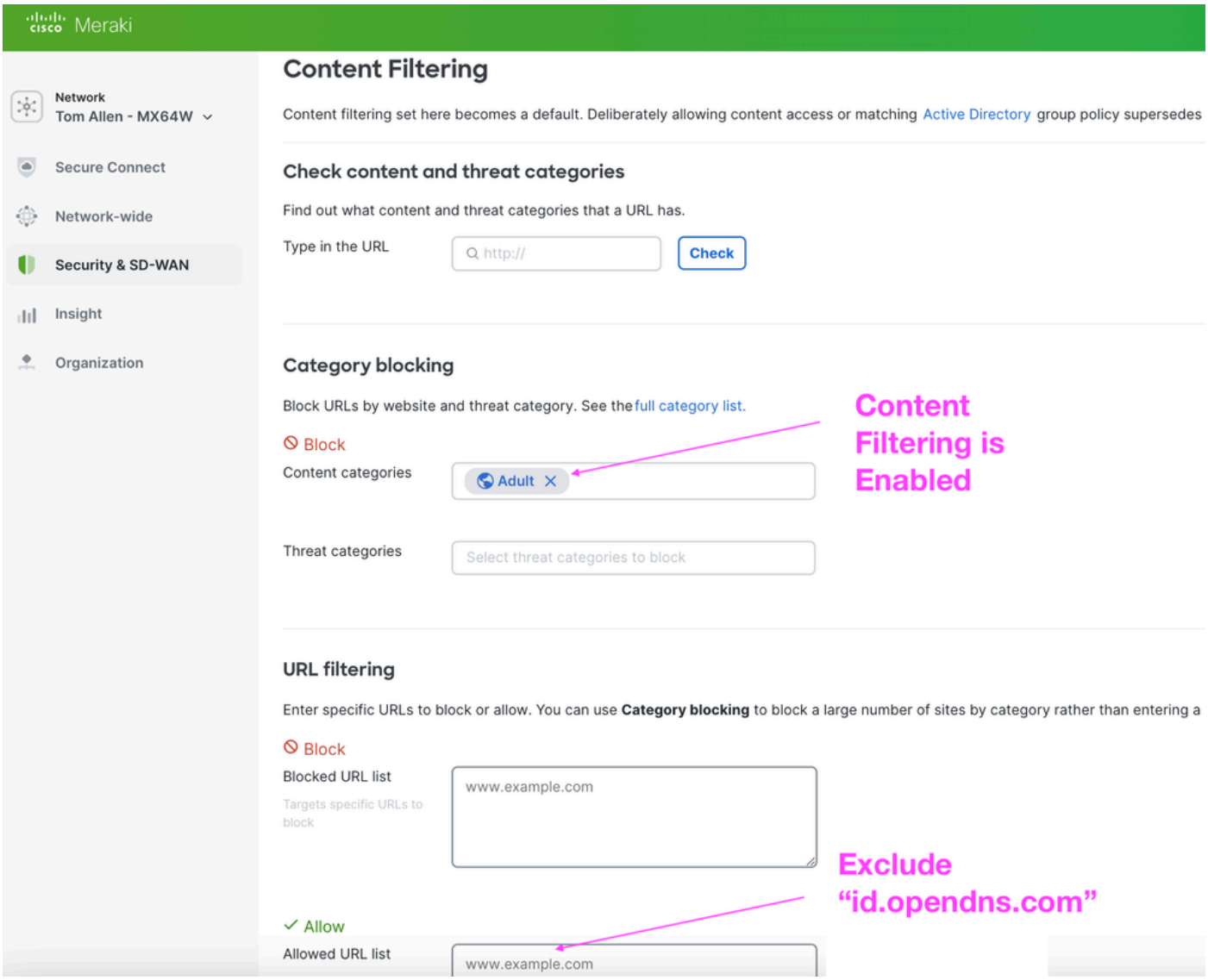
Solução

Exclua esse domínio do recurso de filtragem de conteúdo Meraki MX usando a lista "URL permitido" no painel da Meraki.

```
id.opendns.com
```

A filtragem de conteúdo é configurada nestes locais no painel da Meraki:

- Em Segurança e SD-WAN > Filtragem de conteúdo (Configurações globais)
- Em Network-wide > Group policies (Políticas que podem ser atribuídas a usuários ou SSIDs)



21399526244628

Como alternativa, desabilite completamente a filtragem de conteúdo da Meraki (remova todos os blocos de categoria) para usar apenas a filtragem Umbrella.

Causa raiz

O Cisco Umbrella usa um redirecionamento globalmente exclusivo para http://*.id.opendns.com quando o tráfego chega pela primeira vez em nossos sites de Destino de Página de Bloqueio, Proxy Inteligente ou Depuração de Políticas. Este redirecionamento é necessário para gerar uma pesquisa de DNS globalmente exclusiva. Esse DNS exclusivo nos permite autenticar o tráfego na camada DNS e, por sua vez, determinar a identidade correta de usuário/dispositivo/rede.

O filtro de conteúdo Meraki MX executa suas próprias verificações de reputação. Quando o http://*.id.opendns.com é visitado, a filtragem de conteúdo do Meraki MX pode gerar pesquisas de DNS duplicadas para o mesmo domínio que interrompe esse processo de autenticação. Portanto,

o Cisco Umbrella não é capaz de determinar a identidade correta de usuário/dispositivo/rede.

Esse problema não impede que o Cisco Umbrella imponha blocos de conteúdo/segurança, mas impede que o texto/logotipo/personalização da página de bloqueio correta seja exibido.

Causas alternativas

Esse comportamento também pode ser causado com proxies da Web HTTP locais ou filtros da Web. São necessárias etapas obrigatórias de configuração para usar o DNS Umbrella com um proxy HTTP.

Exemplo: Policy-Debug

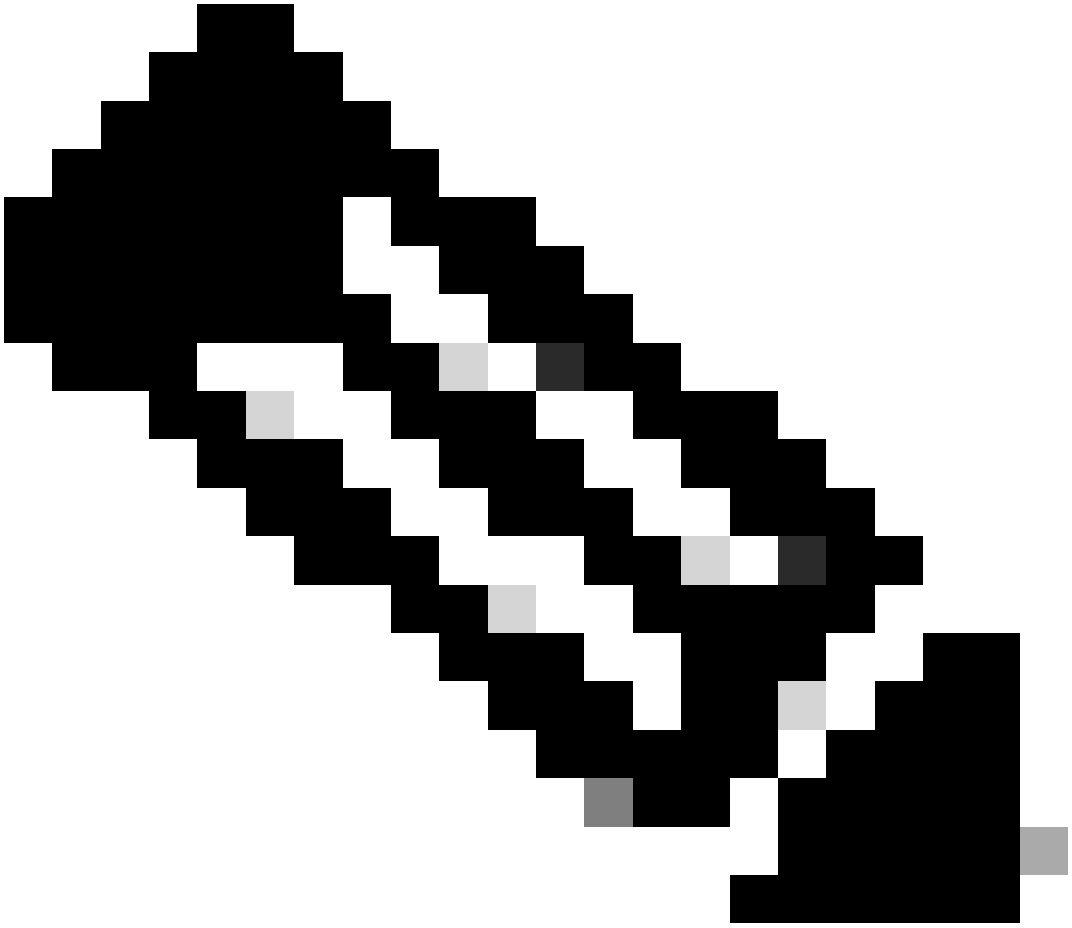
Um indicador desse problema ocorre quando as informações em https://policy-debug.checkumbrella.com/ mostram uma ID da Org incorreta. A ID pode ser exibida como '0', '2' ou uma ID que não esteja associada à org esperada.

<#root>

```
[GENERAL]
Org ID: 0. <<<<<. Incorrect Org ID
Bundle ID: XXXX
Origin ID: XXXX
Other origins:
Host: policy-debug.checkumbrella.com
Internal IP: x.x.x.x
Time: Fri, 29 Sep 2023 16:16:22.182335 UTC
```

Exemplo: Proxy inteligente

Um indicador desse problema é quando o servidor iproxy retorna um '401' inesperado para alguns sites (incluindo http://proxy.opendnstest.com) mesmo quando o cliente está licenciado para proxy inteligente. O erro é retornado do servidor.



Note: O Proxy inteligente é usado apenas para alguns sites que têm uma reputação "cinza" ou suspeita, portanto o problema aparece apenas em circunstâncias específicas.

Exemplo: Bloquear Páginas

Um indicador desse problema ocorre quando a página de bloqueio não exibe nenhuma personalização específica da empresa. A página de bloqueio ainda é exibida, mas contém a marca padrão 'Cisco Umbrella' em vez de logotipos/textos personalizados. Bloquear usuários/códigos de desvio de página ausente.

21399518458644

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.