Résolution des problèmes d'incompatibilité entre le filtrage de contenu Meraki MX et Umbrella

Table des matières

Introduction

Ce document décrit comment résoudre les problèmes d'incompatibilité entre le filtrage de contenu Meraki MX et Umbrella.

Problème

Lorsque vous utilisez le filtrage de contenu Meraki MX optimisé par Cisco Talos, les clients peuvent rencontrer des incohérences avec certaines fonctions de filtrage de DNS Umbrella.

- Page de bloc incorrecte (pages de bloc personnalisées non appliquées)
- Fonctionnalité de contournement de page de blocage non affichée
- Erreur « 401 Unauthorized » pour les sites utilisant le proxy intelligent
- Les tests Policy-Debug montrent une organisation / un ID d'origine / un ID d'ensemble incorrect

Solution

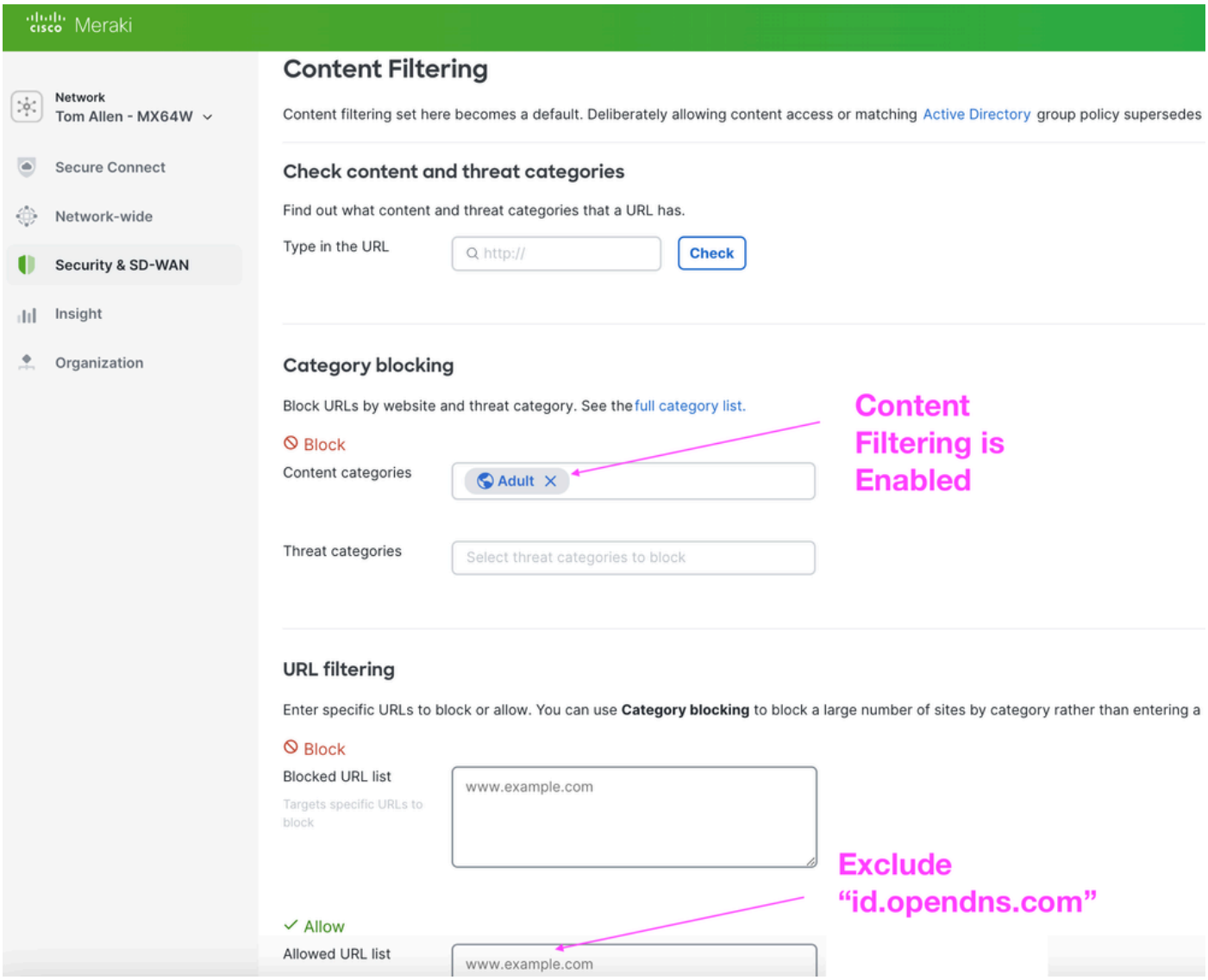
Excluez ce domaine de la fonction de filtrage de contenu Meraki MX à l'aide de la liste « URL autorisées » du tableau de bord Meraki.

```
id.opendns.com
```

Le filtrage du contenu est configuré dans les emplacements suivants du tableau de bord Meraki :

- Dans Security & SD-WAN > Content Filtering (Global settings)

- Dans Network-wide > Group policies (Stratégies pouvant être attribuées aux utilisateurs ou aux SSID)



21399526244628

Vous pouvez également désactiver complètement le filtrage de contenu Meraki (supprimer tous les blocs de catégorie) pour utiliser uniquement le filtrage Umbrella.

Cause première

Cisco Umbrella utilise une redirection unique à l'échelle mondiale vers http://*.id.opendns.com lorsque le trafic arrive pour la première fois sur nos sites d'envoi de pages de blocage, de proxy intelligent ou de débogage des politiques. Cette redirection est nécessaire pour générer une recherche DNS unique au niveau mondial. Ce DNS unique nous permet d'authentifier le trafic au niveau de la couche DNS et de déterminer l'identité correcte de l'utilisateur/périphérique/réseau.

Meraki MX Content Filtering effectue ses propres contrôles de réputation. Lorsque le site http://*.id.opendns.com est visité, le filtrage de contenu Meraki MX peut générer des recherches DNS dupliquées pour le même domaine, ce qui interrompt ce processus d'authentification. Par

conséquent, Cisco Umbrella n'est pas en mesure de déterminer l'identité utilisateur/périphérique/réseau correcte.

Ce problème n'empêche pas Cisco Umbrella d'appliquer des blocs de contenu/sécurité, mais empêche l'affichage du texte/logo/personnalisation correct de la page de blocage.

Autres causes

Ce comportement peut également être provoqué par des proxys Web HTTP ou des filtres Web sur site. Les étapes de configuration obligatoires sont requises pour l'utilisation d'Umbrella DNS avec un proxy HTTP.

Exemple : Policy-Debug

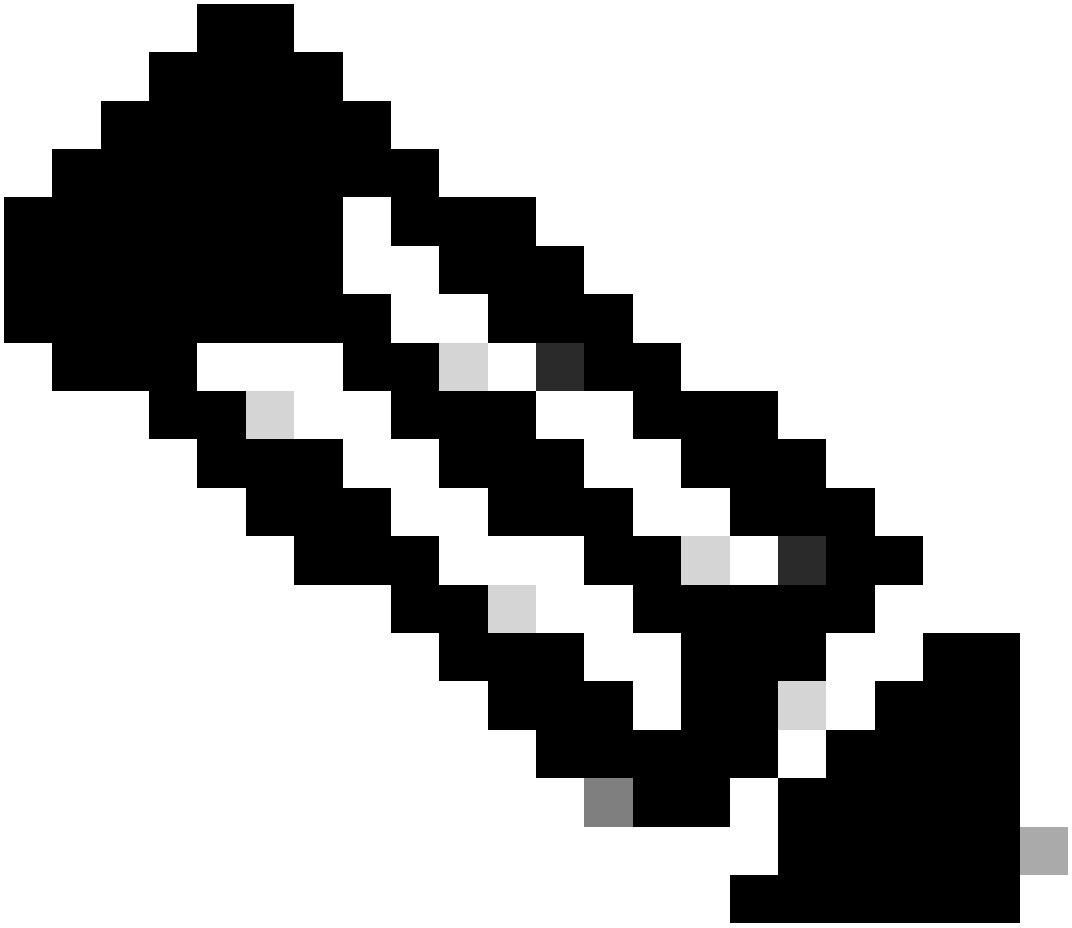
Un indicateur de ce problème est lorsque les informations sur le https://policy-debug.checkumbrella.com/ montrent un ID d'organisation incorrect. L'ID peut être affiché sous la forme « 0 », « 2 » ou un ID qui n'est pas associé à l'organisation attendue.

<#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
```

Exemple : Proxy intelligent

Un indicateur de ce problème est lorsque le serveur iproxy retourne un '401' inattendu pour certains sites (y compris http://proxy.opendnstest.com) même lorsque le client dispose d'une licence pour le proxy intelligent. L'erreur est renvoyée par le serveur.



Remarque : Le proxy intelligent n'est utilisé que pour certains sites qui ont une réputation « grise » ou suspecte, de sorte que le problème n'apparaît que dans des circonstances spécifiques.

Exemple : Bloquer les pages

Un indicateur de ce problème est lorsque la page de blocage n'affiche aucune personnalisation spécifique à l'organisation. La page de blocage est toujours affichée, mais contient la marque « Cisco Umbrella » par défaut au lieu de logos/texte personnalisés. Bloquer les utilisateurs/codes de contournement de page est manquant.

21399518458644

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.