Troubleshoot Incompatibility Issues Between Meraki MX Content Filtering and Umbrella

Contents

Introduction

Issue

Solution

Root Cause

Alternative Causes

- Example: Policy-Debug
- Example: Intelligent Proxy
- Example: Block Pages

Introduction

This document describes how to troubleshoot incompatibility issues between Meraki MX content filtering and Umbrella.

Issue

When using Meraki MX Content Filtering Powered by Cisco Talos, customers can face inconsistencies with some Umbrella DNS filtering features.

- Incorrect block page (custom block pages not applied)
- Block page bypass feature not displayed
- "401 Unauthorized" error for sites using Intelligent Proxy
- Policy-Debug tests show incorrect Org / Origin ID/ BundleID

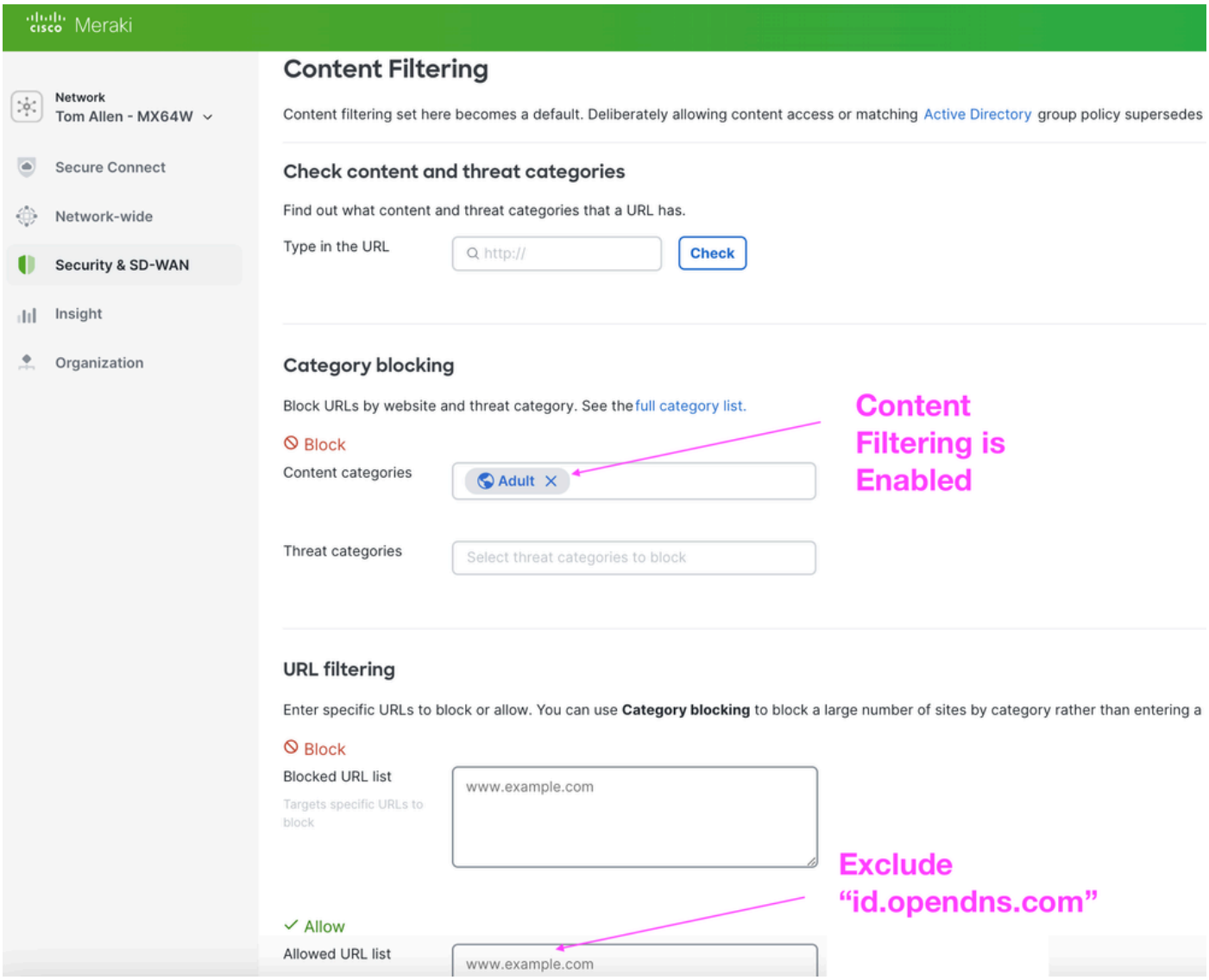
Solution

Exclude this domain from Meraki MX content filtering feature using the "Allowed URL" list on the Meraki Dashboard.

```
id.opendns.com
```

The content filtering is configured in these places on the Meraki Dashboard:

- In **Security & SD-WAN > Content Filtering** (Global settings)
- In **Network-wide > Group policies** (Policies that can be assigned to users or SSIDs)



21399526244628

Alternatively, disable Meraki content filtering completely (remove all category blocks) to use Umbrella filtering only.

Root Cause

Cisco Umbrella uses a globally unique redirect to http://*.id.opendns.com when traffic first arrives at our Block Page Landers, Intelligent Proxy, or Policy-Debug sites. This redirect is required to generate a globally unique DNS lookup. This unique DNS allows us to authenticate traffic at the DNS layer and in turn determine the correct user/device/network identity.

Meraki MX Content Filtering performs its own reputation checks. When the http://*.id.opendns.com is visited the Meraki MX content filtering can generate duplicate DNS lookups for the same domain which breaks this authentication process. Therefore, Cisco Umbrella is unable to determine the correct user/device/network identity.

This problem does not prevent Cisco Umbrella enforcing content/security blocks but does prevent the correct block page text/logo/customization from being displayed.

Alternative Causes

This behavior can also be caused with on-premise HTTP web proxies or web filters. Mandatory configuration steps are required for Using Umbrella DNS with a HTTP proxy.

Example: Policy-Debug

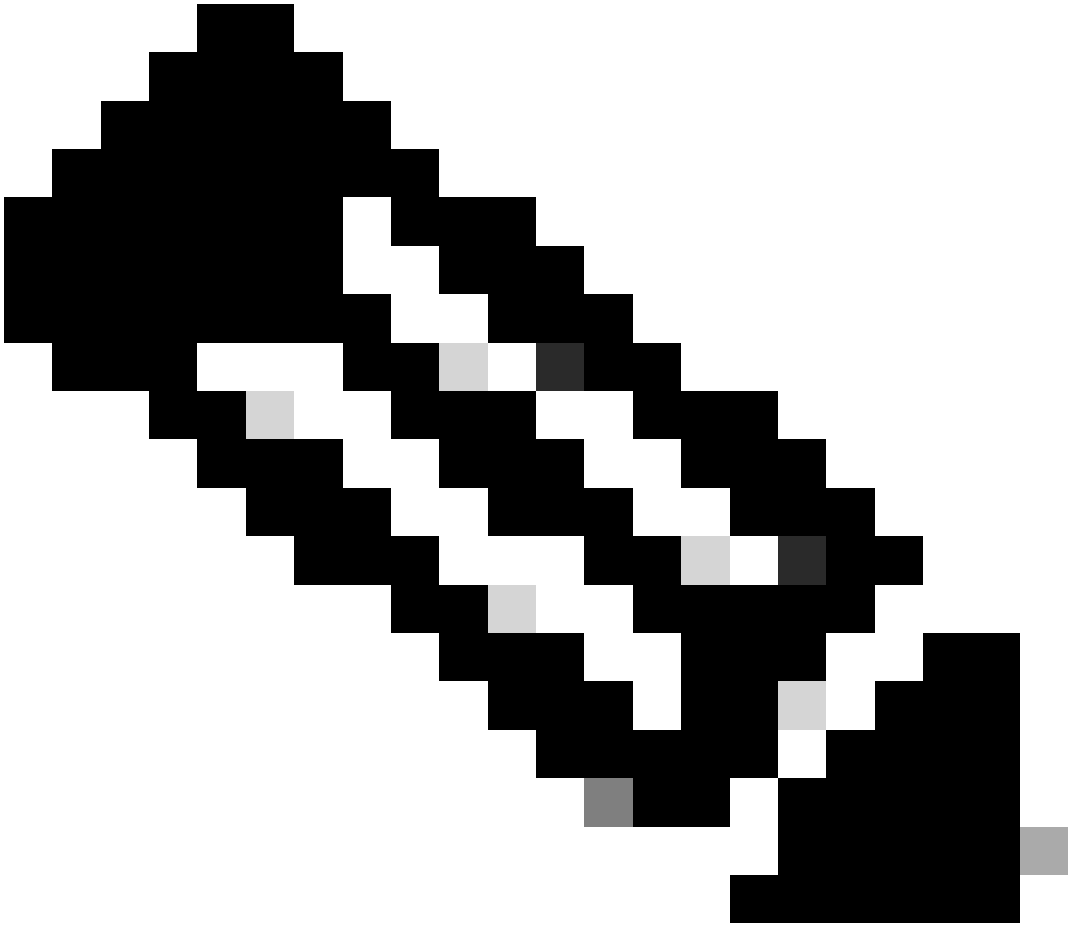
An indicator of this issue is when the information on the https://policy-debug.checkumbrella.com/ shows an incorrect Org ID. The ID can be displayed as '0', '2', or an ID which is not associated with the expected org.

<#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
```

Example: Intelligent Proxy

An indicator of this issue is when the iproxy server returns an unexpected '401' for some sites (including http://proxy.opendnstest.com) even when the customer is licensed for Intelligent proxy. The error is returned from server.



Note: Intelligent Proxy is only used for some sites that have a 'grey' or suspicious reputation so the issue only appears in specific circumstances.

Example: Block Pages

An indicator of this issue is when the block page does not display any org-specific customization. The block page is still displayed but contains the default 'Cisco Umbrella' branding instead of custom logos/text. Block page bypass users/codes is missing.

21399518458644

```
<script id="extension-end-user-informaion-tmp-script" type="text/javascript" src="moz-extension://6ec76
```