

排除Meraki MX內容過濾和Umbrella之間的不相容問題

目錄

[簡介](#)

[問題](#)

[解決方案](#)

[根本原因](#)

[其他原因](#)

[範例：Policy-Bug](#)

[範例：智慧代理](#)

[範例：阻止頁面](#)

簡介

本文檔介紹如何解決Meraki MX內容過濾和Umbrella之間的不相容問題。

問題

使用由Cisco Talos支援的[Meraki MX內容過濾](#)時，客戶可能會遇到某些Umbrella DNS過濾功能不一致的情況。

- 塊頁不正確（未應用自定義塊頁）
- 未顯示阻止頁面繞過功能
- 使用智慧代理的站點出現「401 Unauthorized」錯誤
- [Policy-Debug測試](#)顯示組織/源ID/捆綁包ID不正確

解決方案

使用Meraki控制面板上的「允許的URL」清單從Meraki MX內容過濾功能中排除此域。

id.opendns.com

在Meraki控制面板上的以下位置配置內容過濾：

- 在Security & SD-WAN > 內容過濾（全域性設定）中
- 在Network-wide > Group policies（可以分配給使用者或SSID的策略）中

Content Filtering

Content filtering set here becomes a default. Deliberately allowing content access or matching [Active Directory](#) group policy supersedes

Check content and threat categories

Find out what content and threat categories that a URL has.

Type in the URL

Category blocking

Block URLs by website and threat category. See the [full category list](#).

Block

Content categories

Threat categories

URL filtering

Enter specific URLs to block or allow. You can use **Category blocking** to block a large number of sites by category rather than entering a

Block

Blocked URL list
Targets specific URLs to block

Allow

Allowed URL list

Content Filtering is Enabled

Exclude "id.opendns.com"

21399526244628

或者，完全禁用Meraki內容過濾（刪除所有類別塊），以便僅使用Umbrella過濾。

根本原因

當流量首次到達我們的阻止頁面登入器、智慧代理或策略調試站點時，思科Umbrella使用全域性唯一重定向到http://*.id.opendns.com。生成全域性唯一的DNS查詢需要此重定向。此唯一的DNS允許我們在DNS層對流量進行身份驗證，進而確定正確的使用者/裝置/網路身份。

[Meraki MX內容過濾](#)執行自己的信譽檢查。當訪問http://*.id.opendns.com時，Meraki MX內容過濾可為同一域生成重複的DNS查詢，從而中斷此身份驗證過程。因此，Cisco Umbrella無法確定正確的使用者/裝置/網路身份。

此問題不會阻止Cisco Umbrella強制實施內容/安全塊，但會阻止顯示正確的塊頁面文本/徽標/自定義。

其他原因

此行為也可能會由內部HTTP Web代理或Web過濾器導致。將Umbrella DNS與HTTP代理結合使用需要執行強制配置步驟。

範例： Policy-Bug

<https://policy-debug.checkumbrella.com/>上的資訊顯示不正確的組織ID時，就說明了此問題。ID可以顯示為「0」、「2」或與預期組織不關聯的ID。

<#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

範例： 智慧代理

此問題的一個跡象是，即使客戶獲得了智慧代理的許可證，Iproxy伺服器仍會為某些站點(包括<http://proxy.opendnstest.com>)返回意外的「401」。從伺服器返回錯誤。



附註：智慧代理僅用於具有「灰色」或可疑聲譽的某些站點，因此問題僅出現在特定環境中。

範例： 阻止頁面

此問題的一個指示因素是塊頁面未顯示任何組織特定的自定義。阻止頁面仍然顯示，但包含預設的「Cisco Umbrella」品牌而不是自定義徽標/文本。缺少阻止頁面繞過使用者/代碼。



This site is blocked.

www.888.com

> [Administrative Bypass](#)

Sorry, www.888.com has been blocked by your network administrator.

> [Report an incorrect block](#)

> [Diagnostic Info](#)

[Terms](#) | [Privacy Policy](#) | [Contact](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。