

在CSF中排除故障並驗證URL類別

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[背景資訊](#)

[架構](#)

[步驟 1:在FMC中查詢URL類別](#)

[步驟 2:檢視URL過濾整合設定](#)

[步驟 3:使用系統支援跟蹤確認裝置上的URL類別](#)

[步驟 4:將類別編號解析為類別名稱](#)

[驗證](#)

[爭議按鈕](#)

[疑難排解](#)

簡介

本文檔介紹如何驗證安全防火牆和FMC上的URL類別分配，以確保裝置使用相同的URL分類。

必要條件

您必須為裝置啟用URL過濾許可證，雲服務整合處於正常狀態，以及包含URL過濾並在配置URL條件後已部署的訪問控制策略。

需求

思科建議您瞭解以下主題：

- Firepower管理中心(FMC)URL過濾和類別查詢
- 思科安全防火牆(CSF)流量檢測和策略評估
- URL分類和信譽行為，基於CSF 6.5版開始的Talos

採用元件

本檔案介紹Cisco Secure Firewall和FMC 6.5版及更新版本中的可用功能。本指南中的示例使用7.6.5版。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於以下產品和版本：

- 安全防火牆管理中心(FMC)
- 思科安全防火牆(CSF)
- URL過濾和雲服務整合

背景資訊

URL過濾依賴於在流量檢測期間評估的類別資料庫。FMC儲存目標的URL類別資訊，並且裝置在檢查流量時執行運行時查詢。當FMC、裝置或雲資料庫之間不匹配時，即使訪問控制策略配置正確，策略結果也可能不一致。

驗證的一個重要部分是確認URL類別分配在FMC和裝置之間是一致的。URL類別查詢受雲服務整合設定和裝置快取的影響。如果快取刷新設定被禁用或條目生存期過長，則在Talos更新分類後，過時類別資料仍可繼續使用。

架構

啟用URL過濾時，裝置首先檢查本地URL快取。如果快取中不存在該類別，則裝置可以查詢本地資料庫或思科雲。裝置在檢測期間使用其本地URL資料庫和查詢快取，並且與Talos進行通訊以下載和更新URL過濾資料。在FMC管理的裝置上，Beakerd在FMC上運行，並在CSF上處於等待狀態。如果CSF是本地管理的，則進程在裝置本身上運行。

Talos傳送多個大小的完整資料庫包，這些資料庫包儲存在/var/sf/cloud_download/cisco下。

以下是Talos中的資料庫檔案可能具有的外觀的一些示例：

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



附註：資料庫檔案以cisco_uridb開頭，然後列出大小（小、中或大）。大小因使用的硬體而異。

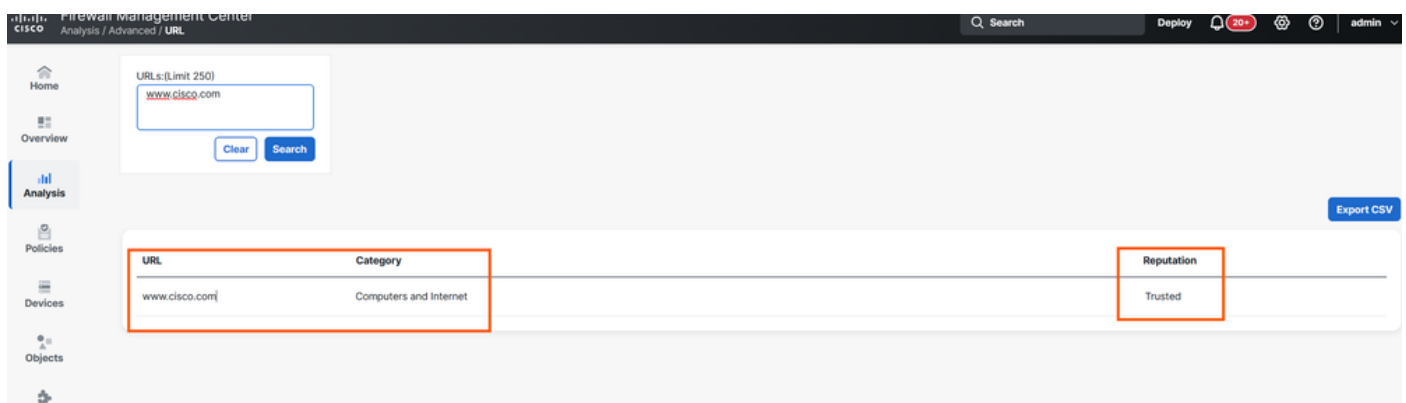
步驟 1:在FMC中查詢URL類別

FMC維護一個本地URL資料庫，該資料庫將URL目標對映到其分配的類別。這是驗證URL分類方式時建議的第一步。

在FMC中導航至位置Analysis > Advanced > URL。

輸入要調查的URL，並檢查其分配的類別。

在下面顯示的示例中，www.cisco.com列在「Computers and Internet（電腦和網際網路）」類別下。



步驟 2:檢視URL過濾整合設定

URL過濾整合設定確定FMC和CSF裝置從何處獲取其URL類別資料庫。每台裝置維護自己的本地資料庫以進行URL查詢，並可向思科雲查詢其他或更新的URL智慧。

在FMC中導航到Integration > Other Integrations > Cloud Services以檢查這些設定。

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

驗證整合是否正常，以及URL查詢快取是否配置為根據預期策略時間進行刷新。



注意：URL查詢快取可以保留先前檢索的類別和信譽結果。如果快取過期被禁用或配置為較長的生存期，裝置可以在Talos更新分類後繼續使用快取資訊，這可能導致裝置結果與當前FMC或Talos查詢暫時不同。

步驟 3:使用系統支援跟蹤確認裝置上的URL類別

要驗證CSF裝置對URL的分類方式是否與FMC相同，請從裝置CLI運行系統支援跟蹤。這顯示Snort檢查引擎如何評估流量，以及檢查連線時返回哪個URL類別。

在FTD CLI上，輸入system support trace命令並回應互動式提示：

```
> 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
```



附註：在本例中，173.37.145.84是www.cisco.com的IP地址。使用與您正在調查的URL對應的目標IP地址。

輸出示例：

```
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, c
```

在此輸出中，URL返回類別ID 2003。下一步說明如何將該數值解析為相應的類別名稱。

步驟 4:將類別編號解析為類別名稱

裝置上的URL類別查詢返回數字類別ID。要將該數字對映到人類可讀的類別名稱，請在裝置上開啟 `aup_categories.json` 檔案。

在專家模式下導航到CSF上的 `/var/sf/cloud_download/` 目錄。確保您處於root使用者模式。

開啟類別定義檔案：

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

搜尋跟蹤輸出中返回的類別ID。類別2003的條目示例：

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

```
"type": "aup_cats",  
"state": "active"  
}
```



附註：所有CSF裝置的類別ID號一致。在每個CSF裝置上，相同的數字ID對映到相同的類別名稱。

驗證

使用步驟1至4的輸出確認FMC資料庫與裝置上的Snort引擎之間的URL類別分配一致。

在此範例中：

- FMC資料庫將www.cisco.com列為電腦和網際網路。
- 裝置CLI返回類別ID 2003，該類別對映到「電腦」和「網際網路」。

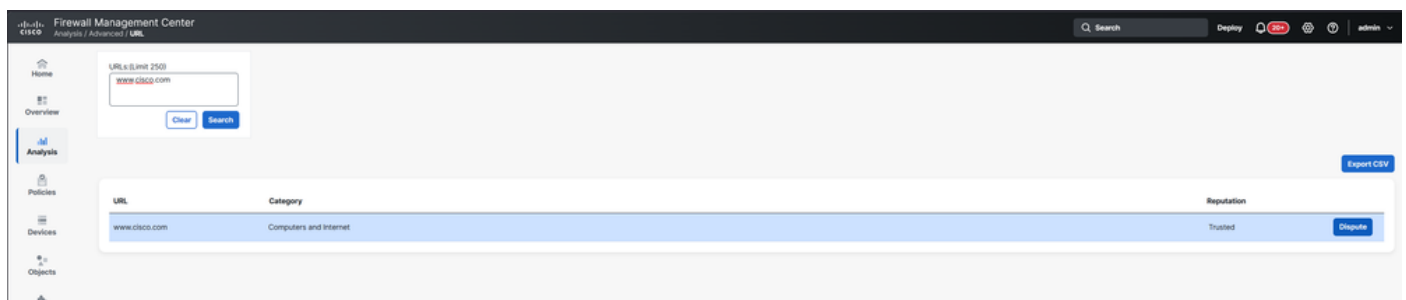
兩個源都同意，這確認正在應用的URL過濾策略對於此URL是一致的。

爭議按鈕

如果您認為URL被歸類為不正確的類別，您可以向Talosh提交爭議。

在FMC中導覽至Analysis > Advanced > URL：

鍵入URL，按一下Search，然後將滑鼠懸停在URL條目上，然後選擇Disrupt。



這將開啟Talosh爭議頁面，以便相應的來源可以複查和更正分類。

疑難排解

如果分類與預期不符，請檢視以下領域：

- 確認URL過濾許可證已啟用並分配給裝置。
- 驗證雲服務的運行狀況和與Talos的連線。
- 檢查裝置快取和快取刷新設定，確認過時條目不會被重複使用。
- 檢查FMC上是否正在為FMC管理的裝置運行燒錄進程。

對於FMC管理的裝置，在FMC專家模式下運行以下命令以確認進程處於活動狀態：

```
pmtool status | grep beakerd
```



附註：如果您在FMC管理的安全防火牆中運行此命令，則此進程可能處於等待狀態。如果安全防火牆是本地管理的，則進程處於運行狀態。

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）。