啟用TSID時，FMC將思科智慧許可流量報告為toos.cisco.com

目錄

問題

Firepower管理中心(FMC)和Firepower威脅防禦(FTD)將思科智慧許可HTTPS流量報告為`toos.cisco.com`，而不是`tools.cisco.com`。
這會導致思科裝置許可流量（ASA、路由器、交換機）被基於URL或安全智慧策略阻止，可能導致許可證過期。

流量本身是合法的，且目的地為思科授權基礎架構。

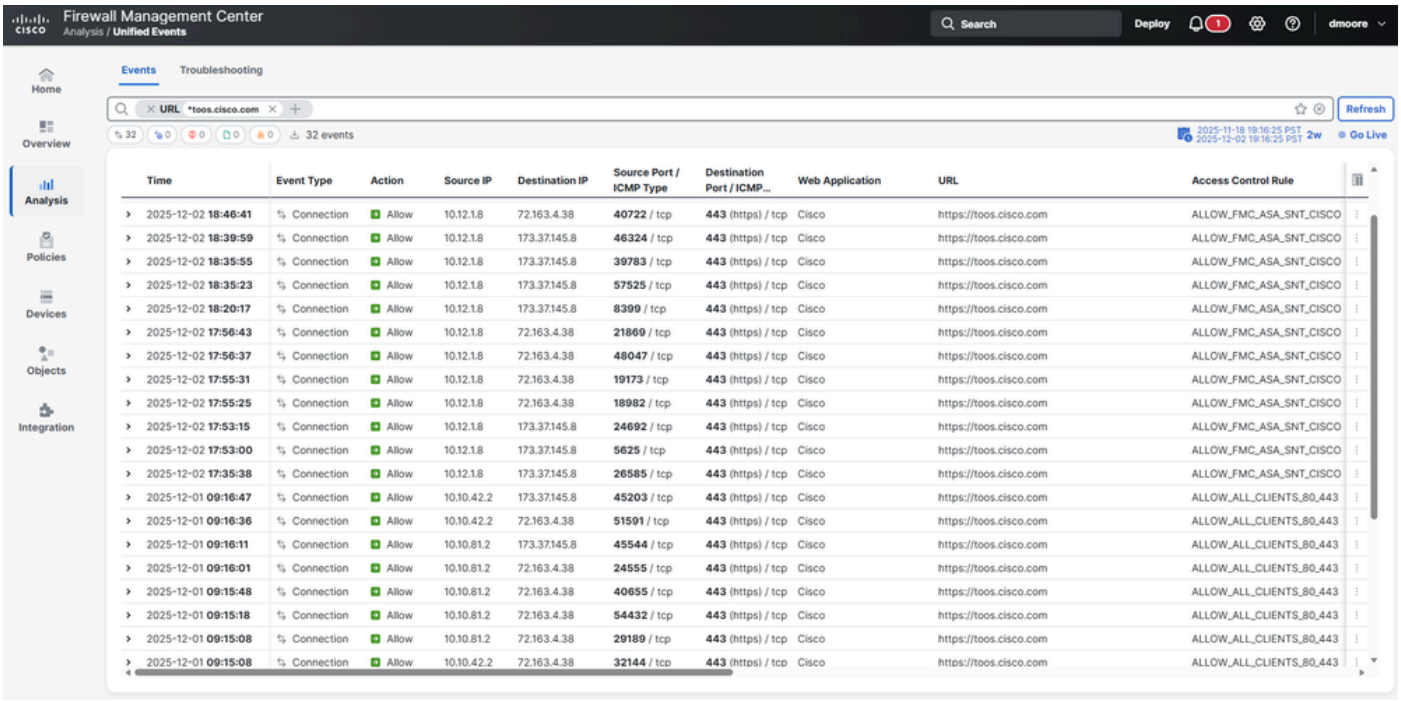
環境

- 產品系列:思科安全防火牆
- 流量型別:思科智慧授權(HTTPS/TCP 443)
- 已啟用TLS伺服器標識(TSID)功能

解析

症狀

- FMC連線事件或FTD系統支援跟蹤顯示：



- 智慧許可命令(例如，`license smart renew auth`)失敗。
- URL過濾/安全情報策略阻止`toos.cisco.com`。
- 封包擷取會確認流量是否已傳送到Cisco授權IP(例如`tools1.cisco.com`)。
- 禁用TSID會導致FMC報告`tools.cisco.com`。

疑難排解/調查步驟

確認智慧許可流量

在Cisco裝置上(例如：ASA):

```
license smart renew auth
```

捕獲思科裝置上的流量（ASA示例）

```
capture LIC interface outside trace detail match tcp host <ASA_IP> any eq 443
show capture LIC
```

匯出捕獲並確認目標IP解析到思科許可主機：

```
tools1.cisco.com
```

在FTD上擷取或追蹤流量

封包擷取(FTD CLI)

```
capture capin interface <inside> match tcp host <DEVICE_IP> any eq 443
capture capout interface <outside> match tcp host <DEVICE_IP> any eq 443
```

系統支援跟蹤

```
system support trace
```

查詢類似以下內容的日誌條目：

```
url toos.cisco.com
```

驗證FMC中的TSID配置

- 導航到訪問控制策略
- 編輯適用的規則
- 檢查高級設定
- 確認TLS伺服器身份發現(TSID)已啟用

驗證TSID影響（可選測試）

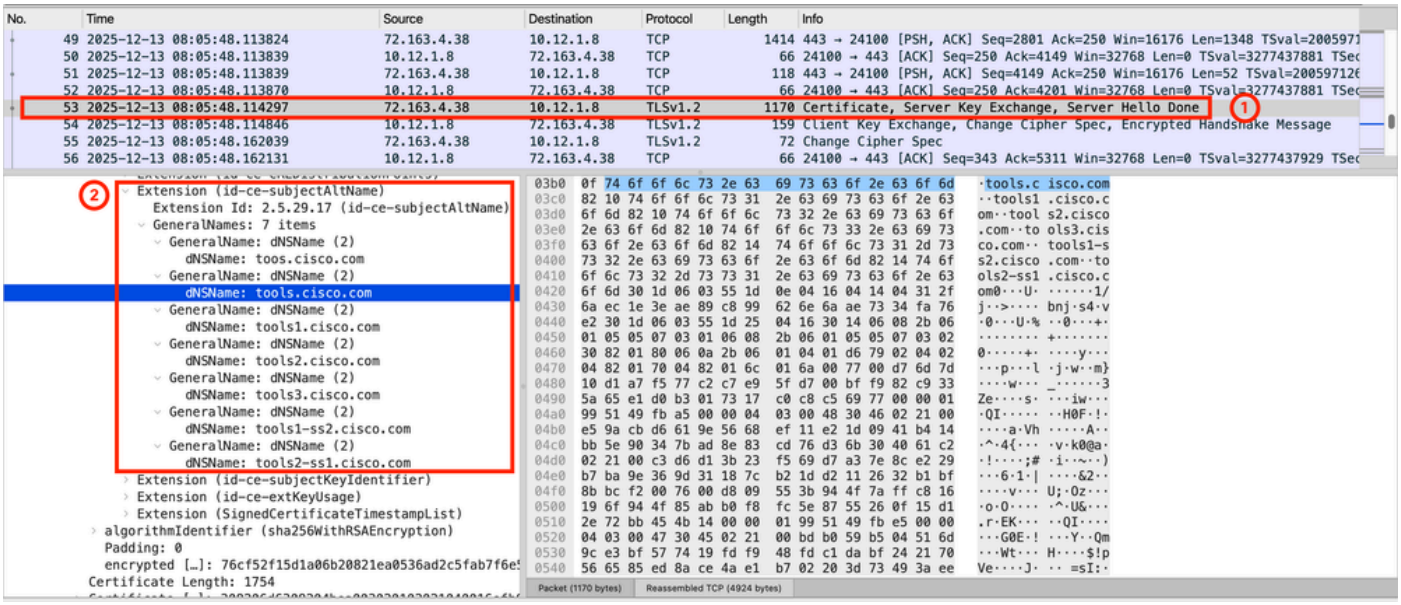
- 禁用規則上的TSID
- 部署策略
- 重新運行許可嘗試

注意 — 預期行為：禁用TSID時，FMC報告`tools.cisco.com`

檢查伺服器證書（可選）

在資料包捕獲或瀏覽器工具中，確認：

- SAN清單包含`toos.cisco.com`作為第一個條目



解決方案/建議處理

沒有缺陷。行為是設計好的。建議以下選項之一：

1. — 在URL篩選/安全情報策略中允許`toos.cisco.com`

2. — 通過以下方式允許思科智慧許可流量：URL類別或更廣泛的域模式

原因

當TLS ClientHello不包含SNI時的設計TSID行為。

啟用TSID且缺少SNI時，FMC將使用證書屬性按以下順序確定伺服器身份：

1. — 通用名稱(CN)

2. — 第一個主題備用名稱(SAN)

3.組織單位

Cisco智慧許可伺服器證書包含`toos.cisco.com`作為第一個SAN條目。
因此，FMC報告`toos.cisco.com`，即使：

- DNS解析正確
- 目標IP屬於思科許可基礎設施
- 流量完整性不受影響

這僅影響URL報告和策略實施。

相關內容

- TLS伺服器身份發現

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）。