

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：

Time	Event Type	Action	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Type	Web Application	URL	Access Control Rule
2025-12-02 18:46:41	Connection	Allow	10.12.1.8	72.163.4.38	40722 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:39:59	Connection	Allow	10.12.1.8	173.37.145.8	46324 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:35:55	Connection	Allow	10.12.1.8	173.37.145.8	39783 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:35:23	Connection	Allow	10.12.1.8	173.37.145.8	57525 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:20:17	Connection	Allow	10.12.1.8	173.37.145.8	8399 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:56:43	Connection	Allow	10.12.1.8	72.163.4.38	21869 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:56:37	Connection	Allow	10.12.1.8	72.163.4.38	48047 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:55:31	Connection	Allow	10.12.1.8	72.163.4.38	19173 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:55:25	Connection	Allow	10.12.1.8	72.163.4.38	18982 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:53:15	Connection	Allow	10.12.1.8	173.37.145.8	24692 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:53:00	Connection	Allow	10.12.1.8	173.37.145.8	5625 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:35:38	Connection	Allow	10.12.1.8	173.37.145.8	26585 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-01 09:16:47	Connection	Allow	10.10.42.2	173.37.145.8	45203 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:16:36	Connection	Allow	10.10.42.2	72.163.4.38	51591 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:16:11	Connection	Allow	10.10.81.2	173.37.145.8	45544 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:16:01	Connection	Allow	10.10.81.2	72.163.4.38	24555 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:48	Connection	Allow	10.10.81.2	72.163.4.38	40655 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:18	Connection	Allow	10.10.81.2	72.163.4.38	54432 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:08	Connection	Allow	10.10.81.2	72.163.4.38	29189 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:08	Connection	Allow	10.10.42.2	72.163.4.38	32144 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443

- 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tools.cisco.com作為第一個條目

No.	Time	Source	Destination	Protocol	Length	Info
49	2025-12-13 08:05:48.113824	72.163.4.38	10.12.1.8	TCP	1414	443 → 24100 [PSH, ACK] Seq=2801 Ack=250 Win=16176 Len=1348 TSval=200597126
50	2025-12-13 08:05:48.113839	10.12.1.8	72.163.4.38	TCP	66	24100 → 443 [ACK] Seq=250 Ack=4149 Win=32768 Len=0 TSval=3277437881 TSecr=200597126
51	2025-12-13 08:05:48.113839	72.163.4.38	10.12.1.8	TCP	118	443 → 24100 [PSH, ACK] Seq=4149 Ack=250 Win=16176 Len=52 TSval=200597126
52	2025-12-13 08:05:48.113870	10.12.1.8	72.163.4.38	TCP	66	24100 → 443 [ACK] Seq=250 Ack=4201 Win=32768 Len=0 TSval=3277437881 TSecr=200597126
53	2025-12-13 08:05:48.114297	72.163.4.38	10.12.1.8	TLSv1.2	1170	Certificate, Server Key Exchange, Server Hello Done
54	2025-12-13 08:05:48.114846	10.12.1.8	72.163.4.38	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
55	2025-12-13 08:05:48.162039	72.163.4.38	10.12.1.8	TLSv1.2	72	Change Cipher Spec
56	2025-12-13 08:05:48.162131	10.12.1.8	72.163.4.38	TCP	66	24100 → 443 [ACK] Seq=343 Ack=5311 Win=32768 Len=0 TSval=3277437929 TSecr=200597126

Extension (id-ce-subjectAltName)	03b0	0f 74 6f 6f 6c 73 2e 63	69 73 63 6f 2e 63 6f 6d	tools.cisco.com
Extension Id: 2.5.29.17 (id-ce-subjectAltName)	03c0	82 10 74 6f 6f 6c 73 31	2e 63 69 73 63 6f 2e 63	tools1.cisco.com
GeneralNames: 7 items	03d0	6f 6d 82 10 74 6f 6f 6c	73 32 2e 63 69 73 63 6f	tools2.cisco.com
GeneralName: dNSName (2)	03e0	2e 63 6f 6d 82 10 74 6f	6f 6c 73 33 2e 63 69 73	tools3.cisco.com
dNSName: toos.cisco.com	03f0	63 6f 2e 63 6f 6d 82 14	74 6f 6f 6c 73 31 2d 73	tools1-s2.cisco.com
GeneralName: dNSName (2)	0400	73 32 2e 63 69 73 63 6f	2e 63 6f 6d 82 14 74 6f	tools2-s1.cisco.com
dNSName: tools.cisco.com	0410	6f 6c 73 32 2d 73 73 31	2e 63 69 73 63 6f 2e 63	tools2-ssl.cisco.com
GeneralName: dNSName (2)	0420	6f 6d 30 1d 06 03 55 1d	0e 04 16 04 14 04 31 2f	tools1.cisco.com
dNSName: tools1.cisco.com	0430	6a ec 1e 3e ae 89 c8 99	62 6e 6a ae 73 34 fa 76	tools2.cisco.com
GeneralName: dNSName (2)	0440	e2 30 1d 06 03 55 1d 25	04 16 30 14 06 08 2b 06	tools3.cisco.com
dNSName: tools2.cisco.com	0450	01 05 05 07 03 01 06 08	2b 06 01 05 05 07 03 02	tools1-s2.cisco.com
GeneralName: dNSName (2)	0460	30 82 01 80 06 0a 2b 06	01 04 01 d6 79 02 04 02	tools.cisco.com
dNSName: tools2.cisco.com	0470	04 82 01 70 04 82 01 6c	01 6a 00 77 00 07 6d 7d	tools1.cisco.com
GeneralName: dNSName (2)	0480	10 d1 a7 f5 77 c2 c7 e9	5f d7 00 bf f9 82 c9 33	tools2.cisco.com
dNSName: tools3.cisco.com	0490	5a 65 e1 0d b3 01 73 17	c0 c8 c5 69 77 00 00 01	tools1-s2.cisco.com
GeneralName: dNSName (2)	04a0	99 51 49 fb a5 00 00 04	03 00 48 30 46 02 21 00	tools.cisco.com
dNSName: tools1-ss2.cisco.com	04b0	e5 9a cb d6 61 9e 56 68	ef 11 e2 1d 09 41 b4 14	tools2-ssl.cisco.com
GeneralName: dNSName (2)	04c0	bb 5e 90 34 7b ad 8e 83	cd 76 d3 6b 30 40 61 c2	tools1.cisco.com
dNSName: tools2-ssl.cisco.com	04d0	02 21 00 c3 d6 d1 3b 23	f5 69 d7 a3 7e 8c e2 29	tools2.cisco.com

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tools.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）。