

启用TSID时，FMC将思科智能许可流量报告为 toos.cisco.com

目录

问题

Firepower管理中心(FMC)和Firepower威胁防御(FTD)将思科智能许可HTTPS流量报告为toos.cisco.com，而不是tools.cisco.com。

这会导致思科设备许可流量（ASA、路由器、交换机）被基于URL的策略或安全情报策略阻止，可能导致许可证过期。

流量本身是合法的，并且发往思科许可基础设施。

环境

- 产品系列：思科安全防火墙
- 流量类型:思科智能许可(HTTPS/TCP 443)
- 已启用TLS服务器标识(TSID)功能

分辨率

症状

- FMC连接事件或FTD系统支持跟踪显示：

Time	Event Type	Action	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	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

- 智能许可命令(例如 , license smart renew auth)失败。
- URL过滤/安全情报策略阻止toos.cisco.com。
- 数据包捕获确认流量已发送到思科许可IP(如tools1.cisco.com)。
- 禁用TSID会导致FMC报告tools.cisco.com。

故障排除/调查步骤

确认智能许可流量

在Cisco设备上(例如 : ASA):

```
license smart renew auth
```

捕获思科设备上的流量 (ASA示例)

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

导出捕获并确认目标IP解析到思科许可主机：

```
tools1.cisco.com
```

在FTD上捕获或跟踪流量

数据包捕获(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
```

系统支持跟踪

```
system support trace
```

查找类似于以下内容的日志条目：

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

验证FMC中的TSID配置

- 导航到“访问控制策略”
- 编辑适用的规则
- 检查高级设置
- 确认已启用TLS服务器身份发现(TSID)

验证TSID影响（可选测试）

- 在规则上禁用TSID
- 部署策略
- 重新运行许可尝试

注意 — 预期行为：禁用TSID时，FMC报告tools.cisco.com

检查服务器证书（可选）

从数据包捕获或浏览器工具中确认：

- SAN列表将tools.cisco.com作为第一个条目

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.c
GeneralNames: 7 items	03d0	6f 6d 82 10 74 6f 6f 6c	73 32 2e 63 69 73 63 6f	om..tool s2.cis
GeneralName: dNSName (2)	03e0	2e 63 6f 6d 82 10 74 6f	6f 6c 73 33 2e 63 69 73	.com..to ols3.cis
dNSName: toos.cisco.com	03f0	63 6f 2e 63 6f 6d 82 14	74 6f 6f 6c 73 31 2d 73	co.com.. tools1-s
GeneralName: dNSName (2)	0400	73 32 2e 63 69 73 63 6f	2e 63 6f 6d 82 14 74 6f	s2.cisco .com..to
dNSName: tools.cisco.com	0410	6f 6c 73 32 2d 73 73 31	2e 63 69 73 63 6f 2e 63	ols2-ssl1.cisco.c
GeneralName: dNSName (2)	0420	6f 6d 30 1d 06 03 55 1d	0e 04 16 04 14 04 31 2f	om0..U.1/
dNSName: tools2.cisco.com	0430	6a ec 1e 3e ae 89 c8 99	62 6e 6a ae 73 34 fa 76	j..>..U.bnj:s4.v
GeneralName: dNSName (2)	0440	e2 30 1d 06 03 55 1d 25	04 16 30 14 06 08 2b 06	.0..U.% ..0..+
dNSName: tools1.cisco.com	0450	01 05 05 07 03 01 06 08	2b 06 01 05 05 07 03 02+.....
GeneralName: dNSName (2)	0460	30 82 01 80 06 0a 2b 06	01 04 01 d6 79 02 04 02	0.....+.....
dNSName: tools2.cisco.com	0470	04 82 01 70 04 82 01 6c	01 6a 00 77 00 07 6d 7d	...p..l .j.w..m)
GeneralName: dNSName (2)	0480	10 d1 a7 f5 77 c2 c7 e9	5f d7 00 bf f9 82 c9 33	...w... ..3
dNSName: tools3.cisco.com	0490	5a 65 e1 0d b3 01 73 17	c0 c8 c5 69 77 00 00 01	Ze...s...iw...3
GeneralName: dNSName (2)	04a0	99 51 49 fb a5 00 00 04	03 00 48 30 46 02 21 00	-QI...s...iH0F..!
dNSName: tools1-ss2.cisco.com	04b0	e5 9a cb d6 61 9e 56 68	ef 11 e2 1d 09 41 b4 14	...a.Vh...A..
GeneralName: dNSName (2)	04c0	bb 5e 90 34 7b ad 8e 83	cd 76 d3 6b 30 40 61 c2	!..4{...v.k0@a
dNSName: tools2-ss1.cisco.com	04d0	02 21 00 c3 d6 d1 3b 23	f5 69 d7 a3 7e 8c e2 29	!..6..l;# ..i..62)
Extension (id-ce-subjectKeyIdentifier)	04e0	b7 ba 9e 36 9d 31 18 7c	b2 1d d2 11 26 32 b1 bf	...6..l;# ..i..62)
Extension (id-ce-extKeyUsage)	04f0	8b bc f2 00 76 00 d8 09	55 3b 94 4f 7a ff c8 16	...v... U; 0z...
Extension (SignedCertificateTimestampList)	0500	19 6f 94 4f 85 ab b0 f8	fc 5e 87 55 26 0f 15 d1	..o-0... ..^US...
algorithmIdentifier (sha256WithRSAEncryption)	0510	2e 72 bb 45 4b 14 00 00	01 99 51 49 fb e5 00 00	..r.EK... ..QI...
Padding: 0	0520	04 03 00 47 30 45 02 21	00 bd b0 59 b5 04 51 6d	...G0E..! ...Y..Om
encrypted [...]: 76cf52f15d1a06b20821ea0536ad2c5fab7f6e...	0530	9c e3 bf 57 74 19 fd f9	48 fd c1 da bf 24 21 70	...Wt... H...\$!p
Certificate Length: 1754	0540	56 65 85 ed 8a ce 4a e1	b7 02 20 3d 73 49 3a ee	Ve...J... ..=sI:

解决方案/推荐处理

没有缺陷。行为是由设计决定的。建议以下选项之一：

1. — 在URL过滤/安全情报策略中允许tools.cisco.com

2. — 通过以下方式允许思科智能许可流量：URL类别或更广泛的域模式

原因

当TLS ClientHello不包含SNI时的按设计TSID行为。

启用TSID且缺少SNI时，FMC使用证书属性按以下顺序确定服务器身份：

1. — 公用名称(CN)
2. — 第一个主题备用名称(SAN)
3. 组织单位

思科智能许可服务器证书包含toos.cisco.com作为第一个SAN条目。
因此，FMC报告toos.cisco.com，即使：

- DNS解析正确
- 目标IP属于思科许可基础设施
- 流量完整性不受影响

这只会影响URL报告和策略实施。

相关内容

- [TLS服务器身份发现](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。