

# FMC meldet Cisco Smart Licensing-Datenverkehr als toos.cisco.com, wenn TSID aktiviert ist

## Inhalt

---

---

## Problem

Firepower Management Center (FMC) und Firepower Threat Defense (FTD) melden HTTPS-Datenverkehr von Cisco Smart Licensing als `toos.cisco.com` anstatt als `tools.cisco.com`. Dies führt dazu, dass der Lizenzierungsverkehr für Cisco Geräte (ASA, Router, Switches) durch URL-basierte oder Security Intelligence-Richtlinien blockiert wird, was zum Lizenzablauf führen kann.

Der Datenverkehr selbst ist legitim und an die Lizenzierungsinfrastruktur von Cisco gerichtet.

## Umwelt

- Produktfamilie: Sichere Firewall von Cisco
- Datenverkehrstyp: Cisco Smart Licensing (HTTPS/TCP 443)
- TLS-TSID-Funktion aktiviert

## Auflösung

## Symptome

- Ablaufverfolgung von FMC-Verbindungsereignissen oder FTD-Systemunterstützung:

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	21809 / 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 17:53:00	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

- Die Smart Licensing-Befehle (z. B. die Lizenz-Smart Renew-Authentifizierung) schlagen fehl.
- URL-Filterung/Sicherheitsintelligenzrichtlinien blockieren toos.cisco.com.
- Durch die Paketerfassung wird bestätigt, dass der Datenverkehr an lizenzierende IPs von Cisco gesendet wird (wie tools1.cisco.com).
- Wenn Sie TSID deaktivieren, meldet FMC toos.cisco.com.

## Schritte zur Fehlerbehebung/Untersuchung

### Smart Licensing-Datenverkehr bestätigen

Auf dem Cisco Gerät (Beispiel: ASA):

```
license smart renew auth
```

## Erfassung von Datenverkehr auf einem Cisco Gerät (ASA-Beispiel)

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

Exportieren Sie die Erfassung und bestätigen Sie die Auflösung der Ziel-IP-Adresse in Cisco Lizenzierungshosts:

[tools1.cisco.com](https://tools1.cisco.com)

## Erfassung oder Verfolgung von Datenverkehr auf FTD

### Paketerfassung (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
```

### Trace zur Systemunterstützung

```
system support trace
```

Suchen Sie nach Protokolleinträgen wie:

[url toos.cisco.com](https://tools.cisco.com)

## Überprüfung der TSID-Konfiguration im FMC

- Navigieren zur Zugriffskontrollrichtlinie
- Bearbeiten der entsprechenden Regel
- Erweiterte Einstellungen überprüfen
- Bestätigung, dass die TLS-Serveridentitätserkennung (TSID) aktiviert ist

### Validierung der TSID-Auswirkungen (optionaler Test)

- TSID für Regel deaktivieren
- Bereitstellen von Richtlinien
- Lizenzierungsversuch erneut ausführen

Hinweis - Erwartetes Verhalten: FMC meldet `tools.cisco.com`, wenn TSID deaktiviert ist

### Serverzertifikat inspizieren (optional)

Bestätigen Sie in den Paketerfassungs- oder Browser-Tools Folgendes:

- SAN-Liste enthält als ersten Eintrag `tools.cisco.com`

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=2005971
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 TSecv=113839
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 TSecv=113839
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 TSecv=113870
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 08:05:48.162839	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 TSecv=162131

  

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
dNSName: tools.cisco.com	0400 73 32 2e 63 69 73 63 6f 2e 63 6f 6d 82 14 74 6f	tools2-s1.cisco.com
dNSName: tools1.cisco.com	0410 6f 6c 73 32 2d 73 73 31 2e 63 69 73 63 6f 2e 63	tools3-s1.cisco.com
dNSName: tools2.cisco.com	0420 6f 6d 30 1d 06 03 55 1d 0e 04 16 04 14 04 31 2f	tools4.cisco.com
dNSName: tools3.cisco.com	0430 6a ec 1e 3e ae 89 c8 99 62 6e 6a ae 73 34 fa 76	tools5.cisco.com
dNSName: tools4.cisco.com	0440 e2 30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06	tools6.cisco.com
dNSName: tools5.cisco.com	0450 01 05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02	tools7.cisco.com
dNSName: tools6.cisco.com	0460 30 82 01 80 06 0a 2b 06 01 04 01 d6 79 02 04 02	tools8.cisco.com
dNSName: tools7.cisco.com	0470 04 82 01 70 04 82 01 6c 01 6a 00 77 00 d7 6d 7d	tools9.cisco.com
dNSName: tools8.cisco.com	0480 10 d1 a7 f5 77 c2 c7 e9 5f d7 00 bf f9 82 c9 33	tools10.cisco.com
dNSName: tools9.cisco.com	0490 5a 65 e1 d0 b3 01 73 17 c0 c8 c5 69 77 00 00 01	tools11.cisco.com
dNSName: tools10.cisco.com	04a0 99 51 49 fb a5 00 00 04 03 00 48 30 46 02 21 00	tools12.cisco.com
dNSName: tools11.cisco.com	04b0 e5 9a cb d6 61 9e 56 68 ef 11 e2 1d 09 41 b4 14	tools13.cisco.com
dNSName: tools12.cisco.com	04c0 bb 5e 90 34 7b ad 8e 83 cd 76 d3 6b 30 40 61 c2	tools14.cisco.com
dNSName: tools13.cisco.com	04d0 02 21 00 c3 d6 d1 3b 23 f5 69 d7 a3 7e 8c e2 29	tools15.cisco.com

## Lösung/Empfohlene Vorgehensweise

Kein Defekt. Verhalten ist Absicht. Empfehlen Sie eine der folgenden Optionen:

- 1.- Lassen Sie `toos.cisco.com` in URL-Filterung / Sicherheitsintelligenzrichtlinien zu
- 2.- Zulassen von Cisco Smart Licensing-Datenverkehr durch: URL-Kategorie oder umfassenderes Domänenmuster

## Ursache

TSID-Verhalten nach Entwurf, wenn TLS ClientHello kein SNI enthält

Wenn TSID aktiviert ist und SNI fehlt, bestimmt FMC die Serveridentität mithilfe der Zertifikatattribute in der folgenden Reihenfolge:

- 1.- Gattungsbezeichnung (KN)
- 2.- Alternativer Name des ersten Betreffs (SAN)
- 3.- Organisationseinheit (OU)

Cisco Smart Licensing-Serverzertifikate enthalten `toos.cisco.com` als ersten SAN-Eintrag. FMC meldet `toos.cisco.com` daraufhin, obwohl:

- Die DNS-Auflösung ist richtig.
- Die Ziel-IP-Adresse gehört zur Lizenzierungsinfrastruktur von Cisco.
- Die Integrität des Datenverkehrs wird nicht beeinträchtigt.

Dies betrifft nur URL-Berichte und die Richtliniendurchsetzung.

## Verwandte Inhalte

- [TLS-Serveridentitätserkennung](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.