

FMC segnala il traffico di Cisco Smart Licensing come toos.cisco.com quando TSID è abilitato

Sommario

Problema

Firepower Management Center (FMC) e Firepower Threat Defense (FTD) segnalano il traffico HTTPS di Cisco Smart Licensing come `tos.cisco.com` anziché `tools.cisco.com`.

In questo modo, il traffico delle licenze dei dispositivi Cisco (ASA, router, switch) viene bloccato da policy basate su URL o Security Intelligence, con la possibilità di una scadenza della licenza.

Il traffico è in sé legittimo e destinato all'infrastruttura di licenze Cisco.

Ambiente

- Famiglia di prodotti: Cisco Secure Firewall
- Tipo di traffico: Cisco Smart Licensing (HTTPS / TCP 443)
- Caratteristica Identità server TLS (TSID) abilitata

Risoluzione

Sintomi

- Gli eventi di connessione FMC o la traccia di supporto del sistema FTD mostrano:

Firewall Management Center
Analysis / Unified Events

Search Deploy 1 2 dmoore

Events Troubleshooting

URL *tools.cisco.com 32 events

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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.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://tools.cisco.com	ALLOW_ALL_CLIENTS_80_443

- I comandi di Smart Licensing (ad esempio, license smart renew auth) hanno esito negativo.
- Filtro URL / Policy di Security Intelligence che bloccano tools.cisco.com.
- L'acquisizione dei pacchetti conferma l'invio del traffico agli IP di licenza Cisco (come tools1.cisco.com).
- La disattivazione di TSID determina la segnalazione da parte di FMC di tools.cisco.com.

Procedura di risoluzione dei problemi/indagine

Conferma traffico di Smart Licensing

Sul dispositivo Cisco (esempio: ASA)

license smart renew auth

Acquisire il traffico sul dispositivo Cisco (esempio ASA)

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

Esportare le risoluzioni IP di acquisizione e conferma sugli host di licenza Cisco:

tools1.cisco.com

Acquisisci o traccia traffico su FTD

Packet Capture (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
```

Traccia supporto di sistema

```
system support trace
```

Cerca voci di registro simili a:

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

Verifica configurazione TSID in FMC

- Passa a Criteri di controllo di accesso
- Modifica la regola applicabile
- Controlla impostazioni avanzate

- Conferma l'abilitazione di TLS Server Identity Discovery (TSID)

Convalida impatto TSID (test facoltativo)

- Disabilita TSID nella regola
- Distribuisci criteri
- Riesegui tentativo di gestione licenze

Nota - Comportamento previsto: FMC segnala `tools.cisco.com` quando TSID è disabilitato

Controlla certificato server (facoltativo)

Dagli strumenti di acquisizione pacchetti o del browser, confermare:

- L'elenco delle SAN include `tools.cisco.com` come prima voce

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 TSec
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 TSec
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 1
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 TSec

Extension (id-ce-subjectAltName)	Hex	Text
Extension Id: 2.5.29.17 (id-ce-subjectAltName)	03b0 0f 74 6f 6f 6c 73 2e 63 69 73 63 6f 2e 63 6f 6d	tools.cisco.com
GeneralNames: 7 items	03d0 6f 6d 82 10 74 6f 6f 6c 73 31 2e 63 69 73 63 6f 2e 63 6f 6d	tools1.cisco.com
GeneralName: dNSName (2)	03e0 2e 63 6f 6d 82 10 74 6f 6f 6c 73 33 2e 63 69 73	tools2.cisco.com
dNSName: toos.cisco.com	03f0 63 6f 2e 63 6f 6d 82 14 74 6f 6f 6c 73 31 2d 73	tools1-s
dNSName: tools.cisco.com	0400 73 32 2e 63 69 73 63 6f 2e 63 6f 6d 82 14 74 6f	s2.cisco.com
GeneralName: dNSName (2)	0410 6f 6c 73 32 2d 73 73 31 2e 63 69 73 63 6f 2e 63	ols2-ssl.cisco.c
dNSName: tools1.cisco.com	0420 6f 6d 30 1d 06 03 55 1d 0e 04 16 04 14 04 31 2f	om0-U
dNSName: tools2.cisco.com	0430 6a ec 1e 3e ae 89 c8 09 62 6e 6a ae 73 34 fa 76	bnj-s4-v
dNSName: tools3.cisco.com	0440 e2 30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06	0-U-%
dNSName: tools1-ss2.cisco.com	0450 01 05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02	+
dNSName: tools2.cisco.com	0460 30 82 01 80 06 0a 2b 06 01 04 01 d6 79 02 04 02	+
dNSName: tools3.cisco.com	0470 04 82 01 70 04 82 01 6c 01 6a 00 77 00 d7 6d 7d	l j-w-m}
dNSName: tools1-ss2.cisco.com	0480 10 d1 a7 f5 77 c2 c7 e9 5f d7 00 bf f9 82 c9 33	w-w-3
dNSName: tools2-ss1.cisco.com	0490 5a 65 e1 d0 b3 01 73 17 c0 c8 c5 69 77 00 00 01	Ze-s-iw
dNSName: tools3.cisco.com	04a0 99 51 49 fb a5 00 00 04 03 00 48 30 46 02 21 00	-QI-H0F-l
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
dNSName: tools2-ss1.cisco.com	04c0 bb 5e 90 34 7b ad 8e 83 cd 76 d3 6b 30 40 61 c2	^4{;v-k0@a
dNSName: tools3-ss1.cisco.com	04d0 02 21 00 c3 d6 d1 3b 23 f5 69 d7 a3 7e 8c e2 29	!;# ;i
Extension (id-ce-subjectKeyIdentifier)	04e0 b7 ba 9e 36 9d 31 18 7c b2 1d d2 11 26 32 b1 bf	6-1- ;i-62
Extension (id-ce-extKeyUsage)	04f0 8b bc f2 00 76 00 d8 09 55 3b 94 4f 7a ff c8 16	U; ;0z
Extension (SignedCertificateTimestampList)	0500 19 6f 94 4f 85 ab b0 f8 fc 5e 87 55 26 0f 15 d1	o-0 ; ;U; ;
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 ;Qm
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 ; ;= ;I ;

Risoluzione / Manipolazione consigliata

Nessun difetto. Il comportamento è di progettazione. Consigliare una delle seguenti opzioni:

- 1.- Consenti a `tos.cisco.com` di applicare il filtro URL/le policy di Security Intelligence
- 2.- Autorizzare il traffico di Cisco Smart Licensing nei seguenti modi: Categoria URL o modello di dominio più ampio

Causa

Comportamento TSID non progettato quando TLS ClientHello non contiene SNI.

Quando TSID è attivato e SNI è mancante, FMC determina l'identità del server utilizzando gli attributi del certificato nell'ordine seguente:

- 1.- Denominazione comune (NC)
- 2.- Nome alternativo del primo soggetto (SAN)
- 3.- Unità organizzativa

I certificati del server Cisco Smart Licensing contengono `tos.cisco.com` come prima voce SAN. Di conseguenza, FMC riporta `tos.cisco.com` anche se:

- Risoluzione DNS corretta
- L'IP di destinazione appartiene all'infrastruttura delle licenze Cisco
- L'integrità del traffico non è compromessa

Questo influisce solo sulla segnalazione degli URL e sull'applicazione delle policy.

Contenuto correlato

- [Individuazione identità server TLS](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).