

FMC signale le trafic Cisco Smart Licensing comme toos.cisco.com lorsque le TSID est activé

Table des matières

Problème

Firepower Management Center (FMC) et Firepower Threat Defense (FTD) signalent le trafic HTTPS de Cisco Smart Licensing comme `toos.cisco.com` au lieu de `tools.cisco.com`.

Le trafic de licences d'appareils Cisco (ASA, routeurs, commutateurs) est bloqué par des politiques basées sur les URL ou Security Intelligence, ce qui peut entraîner l'expiration de la licence.

Le trafic lui-même est légitime et destiné à l'infrastructure de licence Cisco.

Environnement

- Gamme de produits : Pare-feu sécurisé Cisco
- Type de trafic : Licence Cisco Smart (HTTPS/TCP 443)
- Fonction TSID (TLS Server Identity) activée

Résolution

Symptômes

- FMC connection events ou FTD system support trace show :

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 17:35:38	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 19:16:47	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 19:16:36	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

- Les commandes Smart Licensing (par exemple, license smart renew auth) échouent.
- Filtrage des URL / Blocage des stratégies Security Intelligence sur toos.cisco.com.
- La capture de paquets confirme que le trafic est envoyé aux adresses IP de licence Cisco (comme tools1.cisco.com).
- La désactivation de TSID entraîne le rapport tools.cisco.com de FMC.

Étapes de dépannage/investigation

Confirmer le trafic de licences Smart

Sur le périphérique Cisco (exemple : ASA) :

license smart renew auth

Capturer le trafic sur le périphérique Cisco (exemple ASA)

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

Exportez la capture et confirmez que l'adresse IP de destination est résolue vers les hôtes de licence Cisco :

tools1.cisco.com

Capturer ou suivre le trafic sur FTD

Capture de paquets (CLI FTD)

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

Suivi de support système

```
system support trace
```

Recherchez des entrées de journal similaires à :

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

Vérification de la configuration TSID dans FMC

- Accédez à Access Control Policy
- Modifier la règle applicable
- Vérifier les paramètres avancés
- Confirmer que la découverte d'identité de serveur TLS (TSID) est activée

Valider l'impact TSID (test facultatif)

- Désactiver le TSID sur la règle
- Déployer une stratégie
- Réexécution de la tentative de licence

Remarque - Comportement attendu : FMC signale `tools.cisco.com` lorsque le TSID est désactivé

Certificat du serveur de contrôle (facultatif)

À partir des outils de capture de paquets ou du navigateur, vérifiez :

- La liste SAN inclut `tools.cisco.com` comme première entrée

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
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	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: tools.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-ss1.cisco.com
GeneralName: dNSName (2)	0410 6f 6c 73 32 2d 73 73 31 2e 63 69 73 63 6f 2e 63	tools2-ss1.cisco.com
dNSName: tools1.cisco.com	0420 6f 6d 30 1d 06 03 55 1d 0e 04 16 04 14 04 31 2f	tools1.cisco.com
dNSName: tools2.cisco.com	0430 6a ec 1e 3e ae 89 c8 99 62 6e 6a ae 73 34 fa 76	tools2.cisco.com
dNSName: tools3.cisco.com	0440 e2 30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06	tools3.cisco.com
dNSName: tools1-ss2.cisco.com	0450 01 05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02	tools1-ss2.cisco.com
dNSName: tools2.cisco.com	0460 30 82 01 80 06 0a 2b 06 01 04 01 d6 79 02 04 02	tools2.cisco.com
dNSName: tools3.cisco.com	0470 04 82 01 70 04 82 01 6c 01 6a 00 77 00 d7 6d 7d	tools3.cisco.com
dNSName: tools1.cisco.com	0480 10 d1 a7 f5 77 c2 c7 e9 5f d7 00 bf f9 82 c9 33	tools1.cisco.com
dNSName: tools1-ss2.cisco.com	0490 5a 65 e1 d0 b3 01 73 17 c0 c8 c5 69 77 00 00 01	tools1-ss2.cisco.com
dNSName: tools2-ss1.cisco.com	04a0 99 51 49 fb a5 00 00 04 03 00 48 30 46 02 21 00	tools2-ss1.cisco.com
dNSName: tools2.cisco.com	04b0 e5 9a cb d6 61 9e 56 68 ef 11 e2 1d 09 41 b4 14	tools2.cisco.com
dNSName: tools3.cisco.com	04c0 bb 5e 90 34 7b ad 8e 83 cd 76 d3 6b 30 40 61 c2	tools3.cisco.com
dNSName: tools2-ss1.cisco.com	04d0 02 21 00 c3 d6 d1 3b 23 f5 69 d7 a3 7e 8c e2 29	tools2-ss1.cisco.com

Résolution / Traitement recommandé

Aucun défaut. Le comportement est par conception. Conseillez l'une des options suivantes :

- 1.- Autoriser `toos.cisco.com` dans le filtrage des URL / stratégies de sécurité adaptative
- 2.- Autoriser le trafic Cisco Smart Licensing en : Catégorie d'URL ou modèle de domaine plus large

Motif

Comportement TSID par conception lorsque TLS ClientHello ne contient pas SNI.

Lorsque le TSID est activé et que le SNI est manquant, FMC détermine l'identité du serveur à l'aide des attributs de certificat dans l'ordre suivant :

- 1.- Dénomination commune (NC)
- 2.- Autre nom du premier sujet (SAN)
- 3.- Unité organisationnelle (OU)

Les certificats du serveur Cisco Smart Licensing contiennent `toos.cisco.com` comme première entrée SAN.

Par conséquent, FMC signale `toos.cisco.com` même si :

- Résolution DNS correcte
- L'adresse IP de destination appartient à l'infrastructure de licence Cisco
- L'intégrité du trafic n'est pas affectée

Cela a un impact sur les rapports URL et l'application des politiques uniquement.

Autres informations utiles

- [Détection des identités du serveur TLS](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.