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.

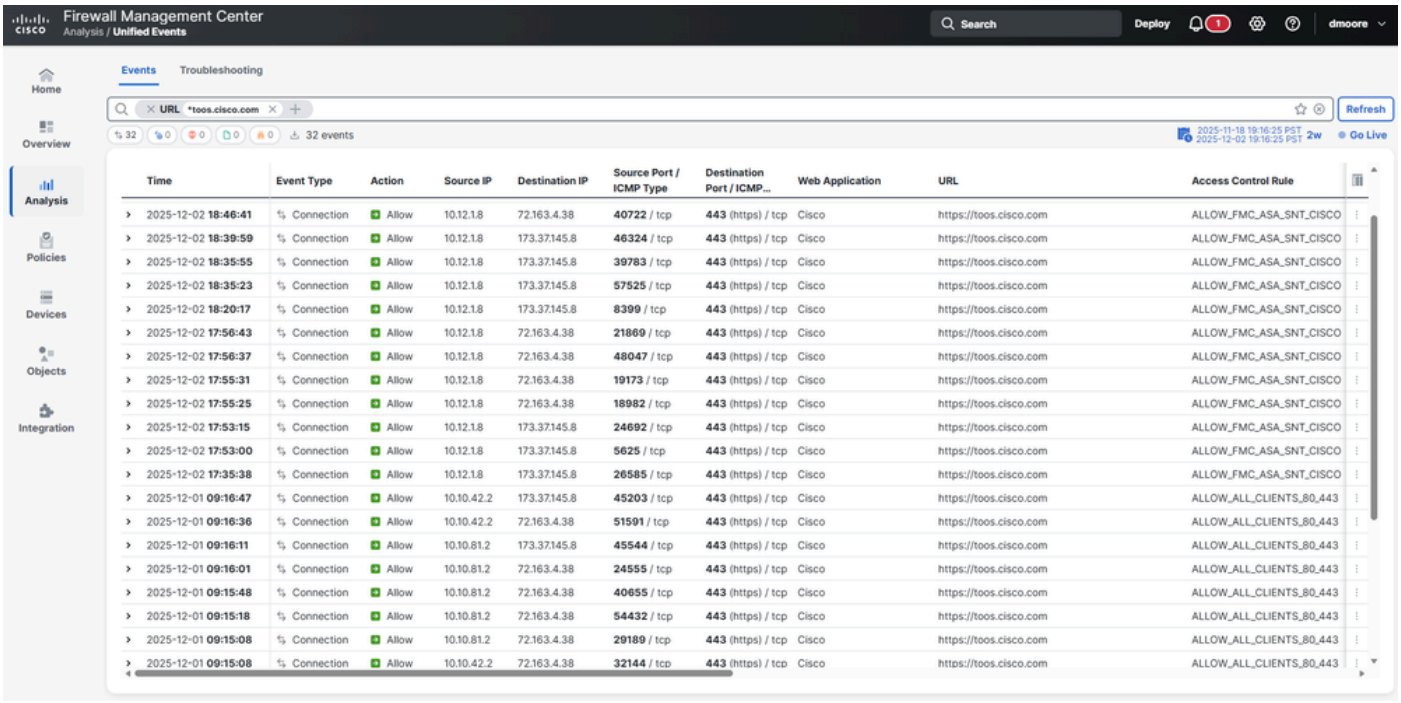
Environnement

- 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 :



- 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
```

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)

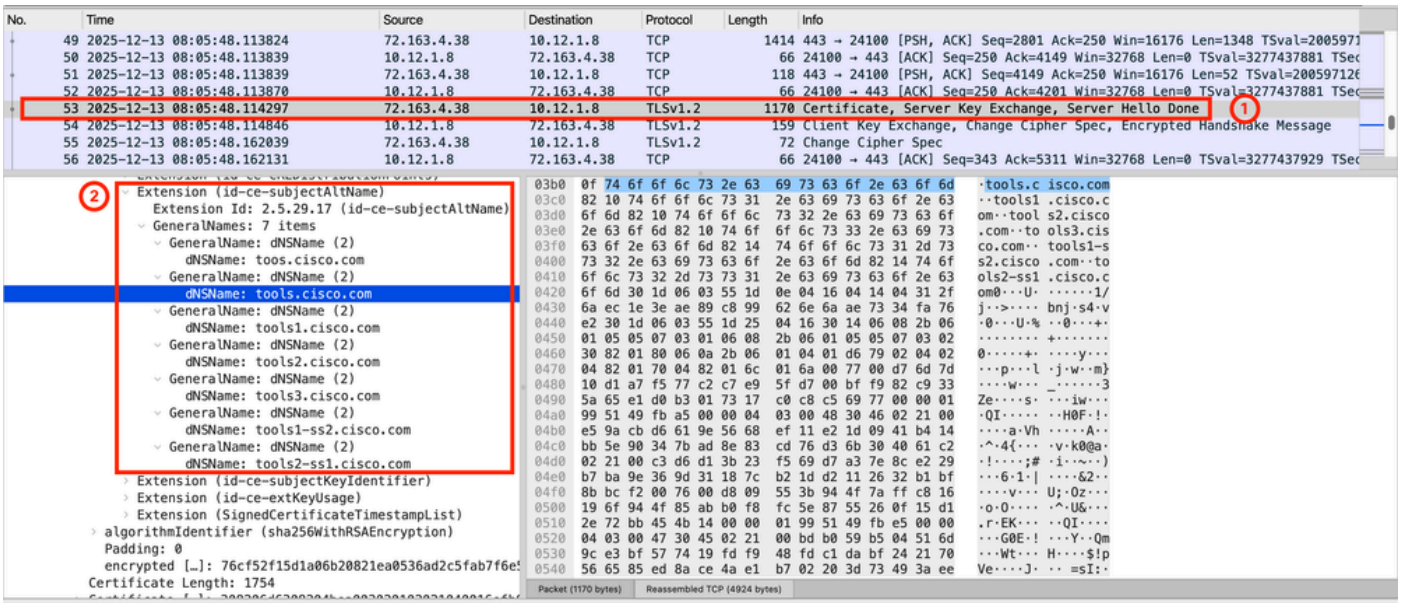
- Désactiver le TSID sur la règle
- Déployer une stratégie
- Réexécution de la tentative de licence

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 `toos.cisco.com` comme première entrée



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.