Dépanner les pertes de paquets FTD (tcp-not-syn) lorsque "Application améliorée et détection d'URL" Est activé sur les interfaces en ligne avec un flux de trafic asymétrique

Table des matières

Problème

Les appliances Firewall Threat Defense (FTD) configurées avec des jeux d'interfaces en ligne suppriment le trafic TCP de retour avec la raison d'abandon ASP (Accelerated Security Path) tcp-not-syn. Cela se produit immédiatement après l'activation de la fonctionnalité TSID (TLS Server Identity Discovery), en particulier l'option "Enhanced application and URL Detection". Dans les versions plus anciennes de Firewall Management Center (FMC), l'option est appelée "Détection précoce des applications et catégorisation des URL". Les paquets TCP SYN-ACK sur le chemin de retour sont abandonnés par le même périphérique FTD qui a transféré le SYN d'origine, empêchant ainsi l'établissement de sessions TCP.

Le problème se manifeste par des pannes de connectivité TCP généralisées et ne se limite pas au trafic TLS. Ces symptômes sont observés lorsque la fonctionnalité est activée :

- Les paquets TCP SYN-ACK sur le chemin de retour sont abandonnés avec la raison d'abandon ASP tcp-not-syn.
- Les nouvelles sessions TCP n'apparaissent pas dans la table de connexion FTD.
- Les compteurs de pertes ASP élevés s'accumulent rapidement, comme illustré par ce résultat capturé environ 10 minutes après l'activation de la fonctionnalité :

<#root>

```
device#

show asp drop


Frame drop:
 Flow is denied by configured rule (acl-drop)                                  1
```

```
 First TCP packet not SYN (tcp-not-syn)                                  34802

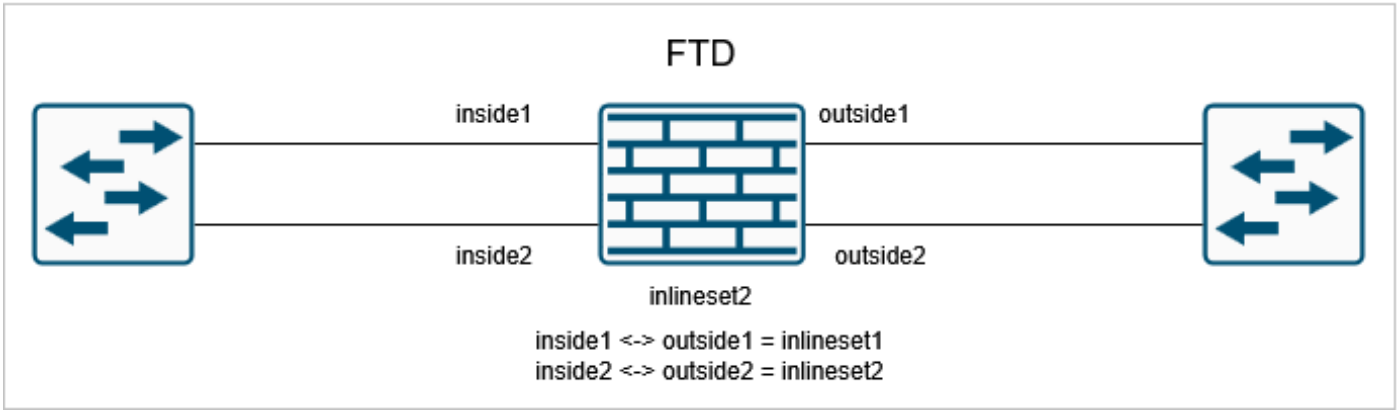

 TCP RST/FIN out of order (tcp-rstfin-ooo)                                   4
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                             995
 Dropped pending packets in a closed socket (np-socket-closed)               3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)               1
 TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)               1
 Blocked or blacklisted by the reputation preprocessor (reputation)          1

Last clearing: 16:50:21 CEST Oct 24 2026 by enable_1
```

Environnement

- Plate-forme : Cisco Firepower 4115. D'autres plates-formes peuvent également être affectées.
- Version du logiciel FTD : 7.6.4. D’autres versions logicielles peuvent également être affectées.
- Version du logiciel FMC : 10.1.0. D’autres versions logicielles peuvent également être affectées.
- FTD avec ensembles d'interfaces en ligne.
- FTD comporte au moins deux paires d’interfaces en ligne : inlineset1 et inlineset2 (ou il y a deux FTD différents avec un inline-set chacun).
- Flux de trafic asymétrique présent dans l'environnement : Le protocole TCP SYN sort par l'interface outside1 tandis que le protocole TCP SYN-ACK correspondant revient par l'interface outside2 sur le même périphérique FTD.
- La fonction TSID est activée sur FTD.

Topologie



Résolution

La résolution recommandée pour arrêter les abandons tcp-not-syn et restaurer la connectivité TCP via les interfaces FTD en ligne est de désactiver l'option "Enhanced application and URL Detection" dans TSID. Cela permet au contournement d'état TCP de rester actif sur les ensembles d'interfaces en ligne, ce qui est nécessaire pour prendre en charge les flux de trafic asymétriques dans l'environnement.

Désactiver la détection améliorée des applications et des URL dans FMC

Naviguez jusqu'à l'adresse : Stratégies > Contrôle d'accès > [Votre stratégie de contrôle d'accès] > Avancé > Détection d'identité du serveur TLS. Décochez ou désactivez la case "Détection améliorée des applications et des URL", puis déployez la stratégie sur les périphériques FTD concernés.

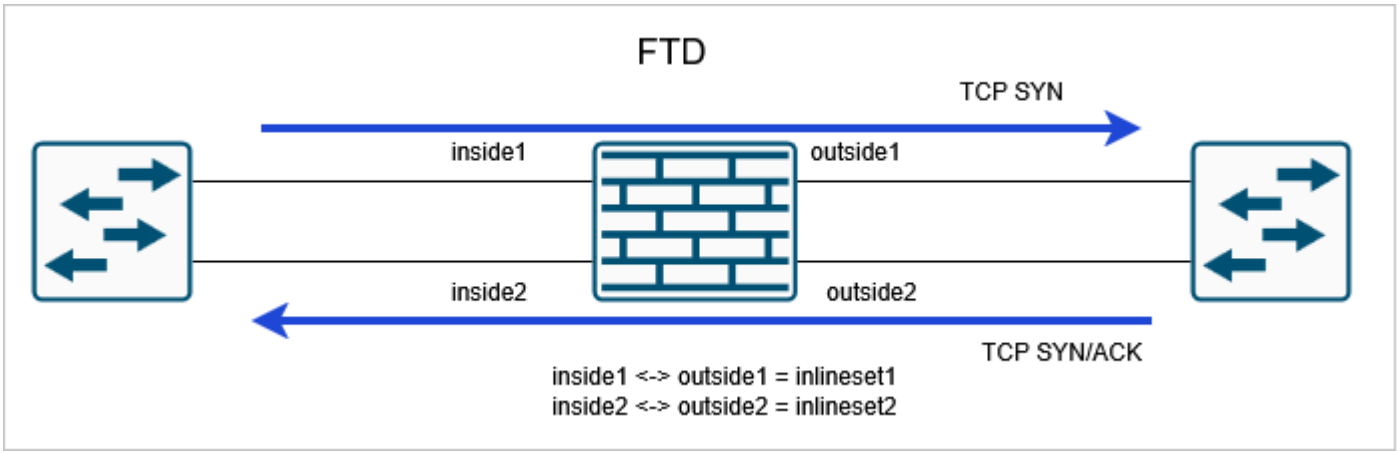
Une fois la fonction désactivée, de nouvelles sessions apparaissent dans la table de connexion, confirmant que les connexions TCP terminent la connexion en trois étapes avec succès.

Remarque : Lorsque le TSID est désactivé, le FTD ne peut plus voir le certificat du serveur dans les sessions TLS 1.3. Les règles d'application et d'URL correspondent moins précisément au trafic chiffré.

Motif

La cause principale des abandons tcp-not-syn est une incompatibilité entre la fonctionnalité TLS Server Identity Discovery et le contournement d'état TCP sur les ensembles d'interfaces en ligne dans FTD.

Par défaut, pour le trafic passant par les interfaces en ligne sur FTD, le contournement d'état TCP est activé. Le contournement d'état TCP est conçu pour permettre au trafic asymétrique (où les chemins d'aller et de retour d'une connexion TCP peuvent traverser différentes interfaces ou même différents périphériques) de passer sans que le FTD n'impose un suivi d'état TCP strict. Il s'agit d'un comportement nécessaire dans les environnements présentant une asymétrie de routage :

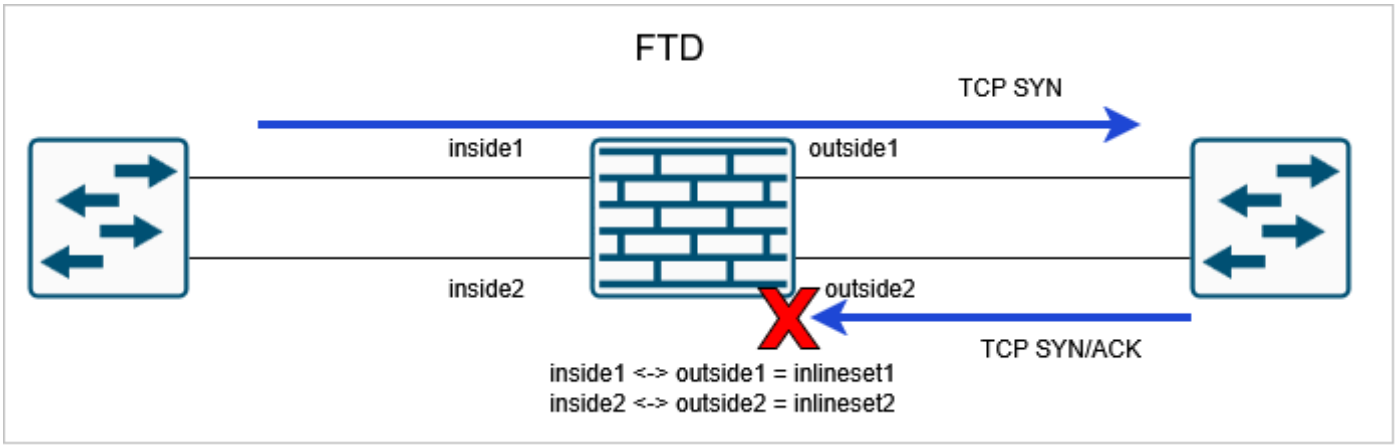


Flux TCP asymétrique à travers les ensembles en ligne FTD lorsque le TSID est désactivé.

Cependant, lorsque l'une de ces fonctions est activée, le système FTD remplace le contournement d'état TCP et commence à effectuer des vérifications d'état TCP complètes sur le trafic d'interface en ligne :

- L'option "Détection améliorée des applications et des URL" sous Détection des identités du serveur TLS.
- Toute stratégie de décodage TLS/SSL active.

Une fois les vérifications d'état TCP appliquées, le FTD effectue le suivi de la séquence d'échange TCP complète. Dans les environnements avec routage asymétrique — où, par exemple, le paquet SYN TCP sort par l'interface outside1 mais le paquet SYN-ACK TCP correspondant retourne par l'interface outside sur le même périphérique — le FTD ne reconnaît pas le paquet SYN-ACK comme appartenant à une session TCP connue et suivie. Comme le SYN-ACK arrive sur une interface différente de celle attendue et qu'aucun SYN correspondant n'a été vu sur cette interface, le FTD le classe comme un paquet non-SYN pour une connexion inconnue et l'abandonne avec la raison d'abandon ASP tcp-not-syn.



Flux TCP asymétrique à travers les ensembles FTD en ligne lorsque le TSID est activé.

Autres informations utiles

- ID de bogue Cisco CSCwp84746 — Documentation : Incompatibilité de la détection d'identité du serveur TLS avec le contournement d'état TCP sur les interfaces en ligne
- ID de bogue Cisco CSCwx42897 — DOC : La détection d'identité du serveur TLS remplace le contournement d'état TCP sur les interfaces en ligne, provoquant l'abandon du trafic TCP (tcp-not-syn)
- ID de bogue Cisco CSCwx42901 — Ajout d'un avertissement lors de l'activation de la détection précoce des applications et de la catégorisation des URL (TSID) indiquant qu'il désactive le contournement d'état TCP sur les interfaces en ligne
- Documentation Cisco — Directives pour le contournement de l'état TCP (inclut la restriction TLS Server Identity Discovery)
- Étude de cas - Trafic asymétrique à travers les ensembles en ligne
- Note technique Cisco — Comment générer des bundles FTD et FMC pour le dépannage
- Assistance technique de Cisco et téléchargements

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.