Fehlerbehebung bei FTD-Paketverlusten (tcp-not-syn) bei "erweiterter Anwendungs- und URL-Erkennung" Ist an Inline-Schnittstellen mit asymmetrischem Datenverkehrsfluss aktiviert

Inhalt

Problem

Firewall Threat Defense (FTD)-Appliances, die mit Inline-Schnittstellensätzen konfiguriert sind, verwerfen TCP-Rückverkehr mit dem Accelerated Security Path (ASP)-Verwerfungsgrund tcp-not-syn. Dies geschieht unmittelbar nach der TLS-TSID-Funktion (Server Identity Discovery), insbesondere nach Aktivierung der Option "Enhanced application and URL Detection". In älteren Versionen des Firewall Management Center (FMC) heißt die Option "Frühe Anwendungserkennung und URL-Kategorisierung". Die TCP-SYN-ACK-Pakete auf dem Rückgabepfad werden von demselben FTD-Gerät verworfen, das die ursprüngliche SYN weitergeleitet hat. Dadurch wird verhindert, dass TCP-Sitzungen aufgebaut werden.

Das Problem tritt als weitverbreitetes Problem bei der TCP-Verbindung auf und ist nicht auf TLS-Datenverkehr beschränkt. Diese Symptome treten auf, wenn die Funktion aktiviert ist:

- TCP-SYN-ACK-Pakete auf dem Rückgabepfad werden mit dem ASP-Verwerfungsgrund tcp-not-syn verworfen.
- Neue TCP-Sitzungen werden nicht in der FTD-Verbindungstabelle angezeigt.
- Die hohen ASP-Zähler für das Herunterfallen akkumulieren schnell, wie diese Ausgabe zeigt, die ca. 10 Minuten nach Aktivierung der Funktion erfasst wurde:

<#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

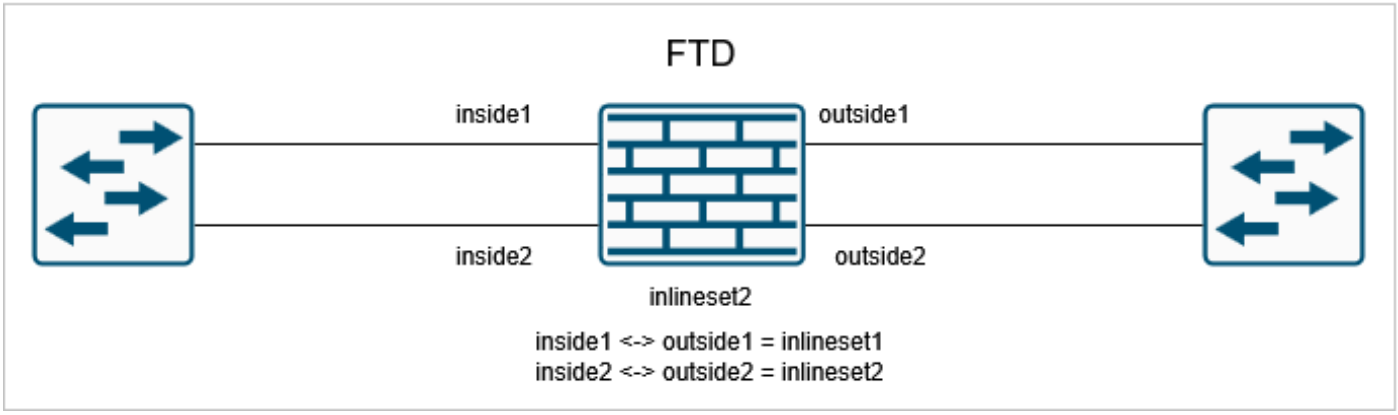

 TCP RST/FIN out of order (tcp-rstfin-ooo)                                   4
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                             995
 Dropped pending packets in a closed socket (np-socket-closed)               3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)               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
```

Umwelt

- Plattform: Cisco Firepower 4115 Auch andere Plattformen können betroffen sein.
- FTD-Softwareversion: 7.6.4. Andere Softwareversionen können ebenfalls betroffen sein.
- FMC-Softwareversion: 10.1.0. Andere Softwareversionen können ebenfalls betroffen sein.
- FTD mit Inline-Schnittstellensätzen.
- FTD verfügt über mindestens zwei Inline-Schnittstellenpaare: inlineset1 und inlineset2 (oder es gibt zwei verschiedene FTDs mit jeweils einem Inline-Set).
- Asymmetrischer Datenverkehrsfluss in der Umgebung: TCP SYN wird über die outside1-Schnittstelle ausgegangen, während das entsprechende TCP SYN-ACK über die outside2-Schnittstelle auf demselben FTD-Gerät zurückkehrt.
- Die TSID-Funktion ist auf FTD aktiviert.

Topologie



Auflösung

Die empfohlene Auflösung, um tcp-not-syn-Drops zu stoppen und die TCP-Verbindung über die Inline-FTD-Schnittstellen wiederherzustellen, besteht darin, die Option "Erweiterte Anwendungs- und URL-Erkennung" innerhalb von TSID zu deaktivieren. Auf diese Weise bleibt die TCP-Zustandsumgehung für die Inline-Schnittstellensätze aktiv, was erforderlich ist, um asymmetrischen Datenverkehr in der Umgebung zu ermöglichen.

"Erweiterte Anwendungs- und URL-Erkennung" in FMC deaktivieren

Navigieren Sie zu: Policies > Access Control > [Your Access Control Policy] > Advanced > TLS Server Identity Discovery. Deaktivieren Sie das Kontrollkästchen "Erweiterte Anwendungs- und URL-Erkennung", und stellen Sie die Richtlinie dann für die betroffenen FTD-Geräte bereit.

Nach der Deaktivierung der Funktion werden neue Sitzungen in der Verbindungstabelle angezeigt, um zu bestätigen, dass die TCP-Verbindungen den Drei-Wege-Handshake erfolgreich abgeschlossen haben.

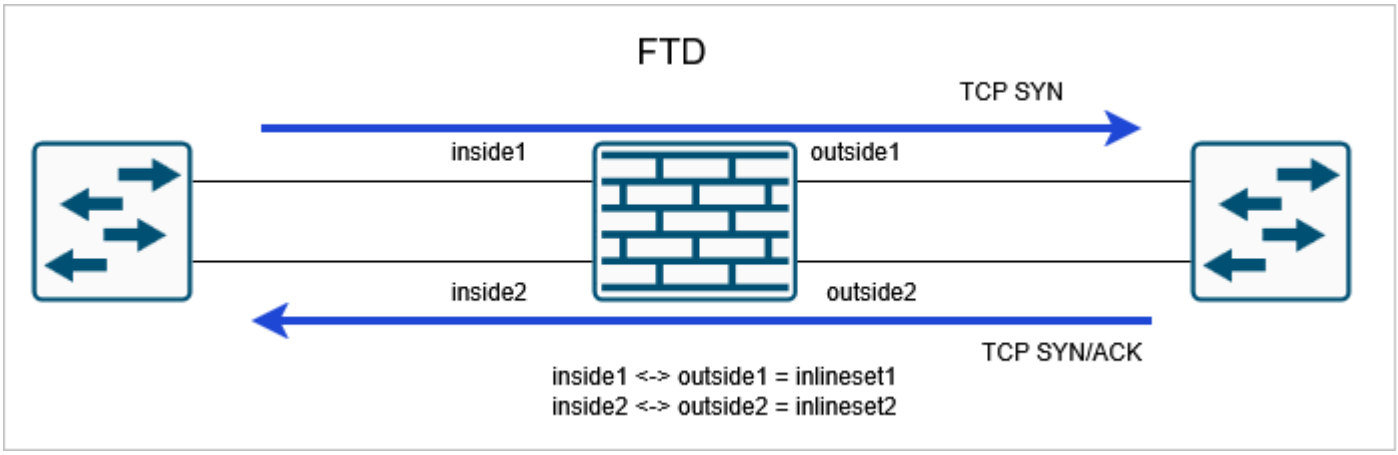


Anmerkung: Wenn TSID deaktiviert ist, kann die FTD das Serverzertifikat in TLS 1.3-Sitzungen nicht mehr sehen. Anwendungs- und URL-Regeln gleichen Datenverkehr mit verschlüsseltem Datenverkehr weniger genau ab.

Ursache

Die Ursache für die TCP-Nicht-Syn-Drops ist eine Inkompatibilität zwischen der TLS-Serveridentitätserkennungsfunktion und TCP-Zustandsumgehung bei Inline-Schnittstellensätzen in FTD.

Standardmäßig ist für Datenverkehr, der Inline-Schnittstellen auf FTD durchläuft, TCP-Zustandsumgehung aktiviert. TCP State Bypass ist so konzipiert, dass asymmetrischer Datenverkehr - bei dem der Vor- und Rückpfad einer TCP-Verbindung verschiedene Schnittstellen oder sogar verschiedene Geräte durchlaufen kann - passieren kann, ohne dass die FTD eine strikte TCP-Statusverfolgung durchsetzt. Dies ist in Umgebungen mit asymmetrischer Routing-Struktur erforderlich:

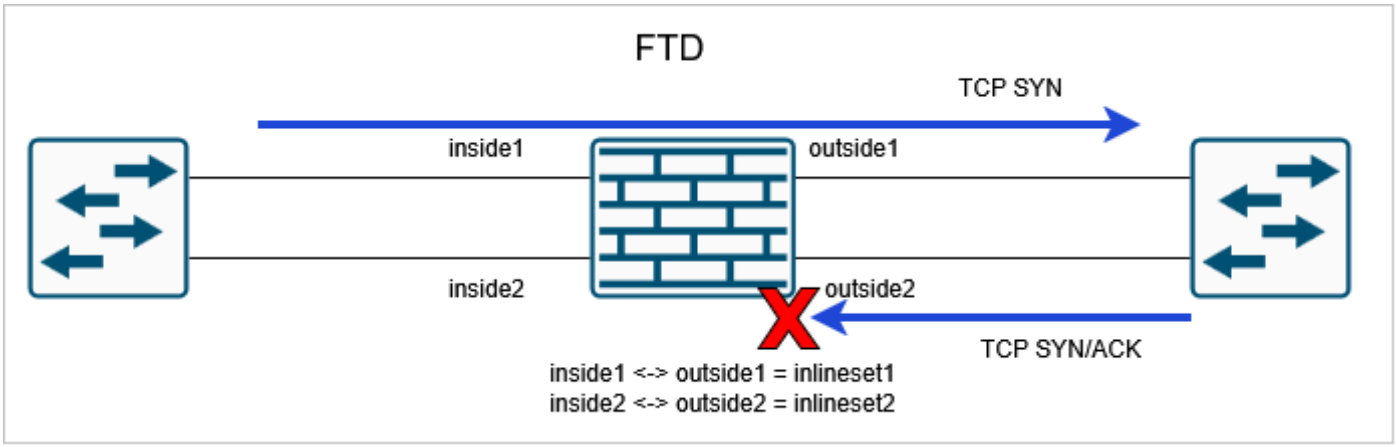


Asymmetrischer TCP-Fluss durch FTD-Inline-Sets, wenn TSID deaktiviert ist.

Wenn jedoch eine dieser Funktionen aktiviert ist, überschreibt das FTD-System die TCP-Zustandsumgehung und führt vollständige TCP-Zustandsüberprüfungen für den Inline-Schnittstellenverkehr durch:

- Die Option "Erweiterte Anwendungs- und URL-Erkennung" unter "TLS Server Identity Discovery".
- Jede aktive TLS/SSL-Entschlüsselungsrichtlinie.

Sobald die TCP-Zustandsprüfungen durchgesetzt wurden, verfolgt die FTD die vollständige TCP-Handshake-Sequenz. In Umgebungen mit asymmetrischem Routing, in denen beispielsweise das TCP SYN-Paket über die outside1-Schnittstelle austritt, die entsprechende TCP SYN-ACK jedoch über die externe Schnittstelle auf demselben Gerät zurückkehrt, erkennt die FTD das SYN-ACK nicht als zu einer bekannten, verfolgten TCP-Sitzung gehörend. Da die SYN-ACK auf einer anderen Schnittstelle ankommt als erwartet und keine entsprechende SYN auf dieser Schnittstelle erkannt wurde, klassifiziert die FTD sie als Nicht-SYN-Paket für eine unbekannte Verbindung und verwirft sie mit dem ASP-Verwerfungsgrund tcp-not-syn.



Asymmetrischer TCP-Fluss durch FTD-Inline-Sets, wenn TSID aktiviert ist.

Verwandte Inhalte

- Cisco Bug-ID CSCwp84746 — Dokumentation: Inkompatibilität der TLS-Serveridentitätserkennung mit der TCP-Zustandsumgehung an Inline-Set-Schnittstellen
- Cisco Bug-ID CSCwx42897 - DOC: Die TLS-Serveridentitätserkennung überschreibt die TCP-Zustandsumgehung an Inline-Set-Schnittstellen, wodurch der TCP-Datenverkehr verworfen wird (tcp-not-syn).
- Cisco Bug-ID CSCwx42901 - Fügen Sie eine Warnung hinzu, wenn Sie "Early Application Detection and URL Kategorization" (TSID) aktivieren, dass TCP State Bypass auf Inline-Set-Schnittstellen deaktiviert ist.
- Cisco-Dokumentation - Richtlinien für die TCP-Zustandsumgehung (einschließlich der Einschränkung für die TLS-Serveridentitätserkennung)
- Anwenderbericht: Asymmetrischer Datenverkehr durch Inline-Sets
- Cisco TechNote - So generieren Sie FTD- und FMC-Fehlerbehebungspakete
- Technischer Support und Downloads von Cisco

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.