FTD-pakketdruppels oplossen (tcp-not-syn) wanneer " Verbeterde toepassing en URL-detectie" Is ingeschakeld op inline interfaces met asymmetrische verkeersstroom

Inhoud

uitgifte

Firewall Threat Defence (FTD)-apparaten die zijn geconfigureerd met inline-interfacesets, laten TCP-retourverkeer vallen met de reden voor de versnelde beveiligingsroute (ASP) tcp-not-syn. Dit gebeurt onmiddellijk nadat de functie TLS Server Identity Discovery (TSID) is ingeschakeld — met name de optie "Enhanced application and URL Detection". In oudere versies van Firewall Management Center (FMC) wordt de optie "Early application detection and URL categorization" genoemd. De TCP SYN-ACK-pakketten op het retourpad worden verwijderd door hetzelfde FTD-apparaat dat de oorspronkelijke SYN doorstuurde, waardoor TCP-sessies niet kunnen worden ingesteld.

Het probleem manifesteert zich als wijdverbreide TCP-connectiviteitsstoringen en is niet beperkt tot TLS-verkeer. Deze symptomen worden waargenomen wanneer de functie is ingeschakeld:

- TCP SYN-ACK-pakketten op het retourpad worden gedropt met ASP drop reden tcp-not-syn.
- Nieuwe TCP-sessies worden niet weergegeven in de FTD-verbindingstabel.
- Hoge ASP-valtellers hopen zich snel op, zoals wordt geïllustreerd door deze uitvoer die ongeveer 10 minuten na het inschakelen van de functie is vastgelegd:

<#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

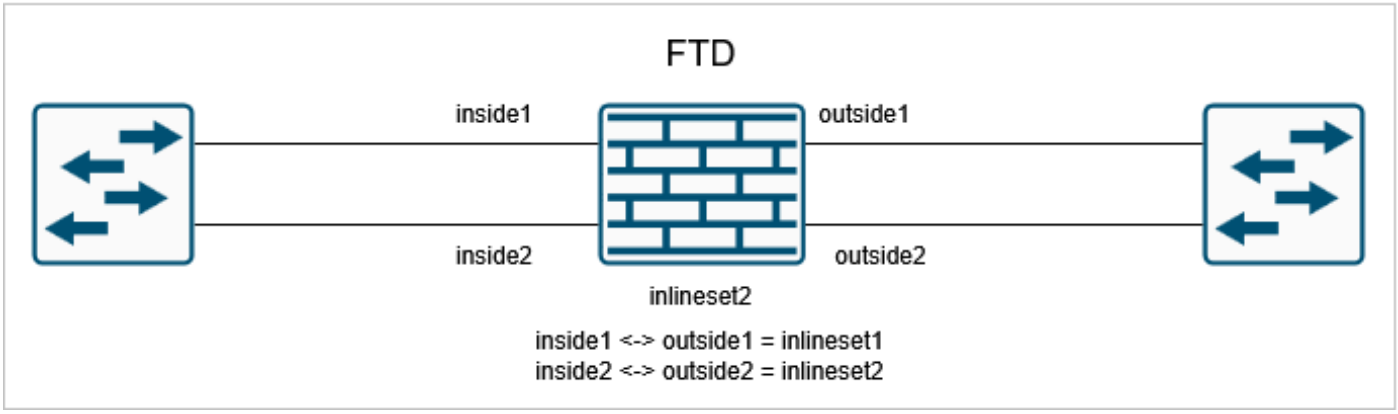

 TCP RST/FIN out of order (tcp-rstfin-ooo)                                   4
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                             995
 Dropped pending packets in a closed socket (np-socket-closed)               3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)  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

milieu

- Het platform is ontwikkeld door Cisco Firepower 4115. Ook andere platformen kunnen worden getroffen.
- FTD-softwareversie: 7.6.4. Ook andere softwareversies kunnen worden beïnvloed.
- FMC-softwareversie: 10.1.0. Ook andere softwareversies kunnen worden beïnvloed.
- FTD met inline interface sets.
- FTD heeft ten minste twee inline-interfaceparen: inlineset1 en inlineset2 (of er zijn twee verschillende FTD's met elk één inline-set).
- Asymmetrische verkeersstroom aanwezig in de omgeving: TCP SYN verdwijnt via de outside1-interface terwijl de overeenkomstige TCP SYN-ACK terugkeert via de outside2-interface op hetzelfde FTD-apparaat.
- De TSID-functie is ingeschakeld op FTD.

Topologie



resolutie

De aanbevolen resolutie om de tcp-not-syn-drops te stoppen en de TCP-connectiviteit via de inline FTD-interfaces te herstellen, is om de optie "Enhanced application and URL Detection" binnen TSID uit te schakelen. Hierdoor kan de TCP State Bypass actief blijven op de inline-interfacesets, wat nodig is om asymmetrische verkeersstromen in de omgeving op te vangen.

Schakel "Enhanced application and URL Detection" uit in FMC

Navigeer naar: Beleid > Toegangsbeheer > [Uw toegangscontrolebeleid] > Geavanceerd > TLS Server Identity Discovery. Schakel het selectievakje "Verbeterde toepassing en URL-detectie" uit of schakel het uit en implementeer het beleid vervolgens op de getroffen FTD-apparaten.

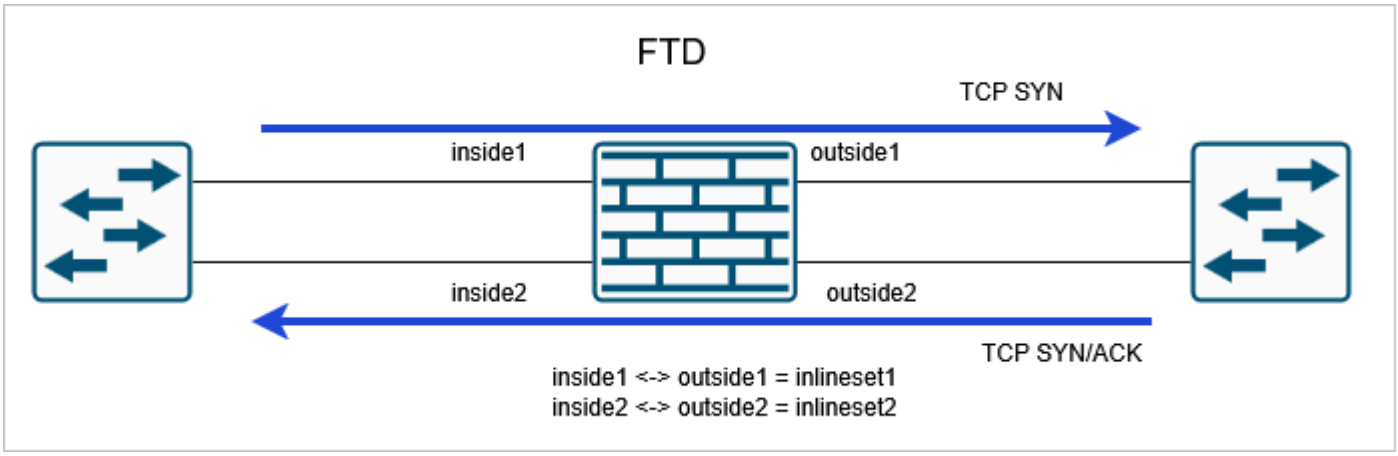
Nadat de functie is uitgeschakeld, verschijnen er nieuwe sessies in de verbindingstabel, waarmee wordt bevestigd dat TCP-verbindingen de drierichtingshandshake met succes voltooien.

Opmerking: als TSID is uitgeschakeld, kan de FTD het servercertificaat niet meer zien in TLS 1.3-sessies. Toepassings- en URL-regels komen minder nauwkeurig overeen met verkeer op gecodeerd verkeer.

Oorzaak

De hoofdoorzaak van de tcp-not-syn drops is een incompatibiliteit tussen de TLS Server Identity Discovery-functie en TCP State Bypass op inline interface sets in FTD.

Standaard is TCP State Bypass ingeschakeld voor verkeer dat door inline-interfaces op FTD gaat. TCP State Bypass is ontworpen om asymmetrisch verkeer mogelijk te maken - waarbij de voorwaartse en terugkeerpaden van een TCP-verbinding verschillende interfaces of zelfs verschillende apparaten kunnen doorlopen - zonder dat de FTD strikte TCP-statustracking afdwingt. Dit is een noodzakelijk gedrag in omgevingen waar routeringsasymmetrie aanwezig is:

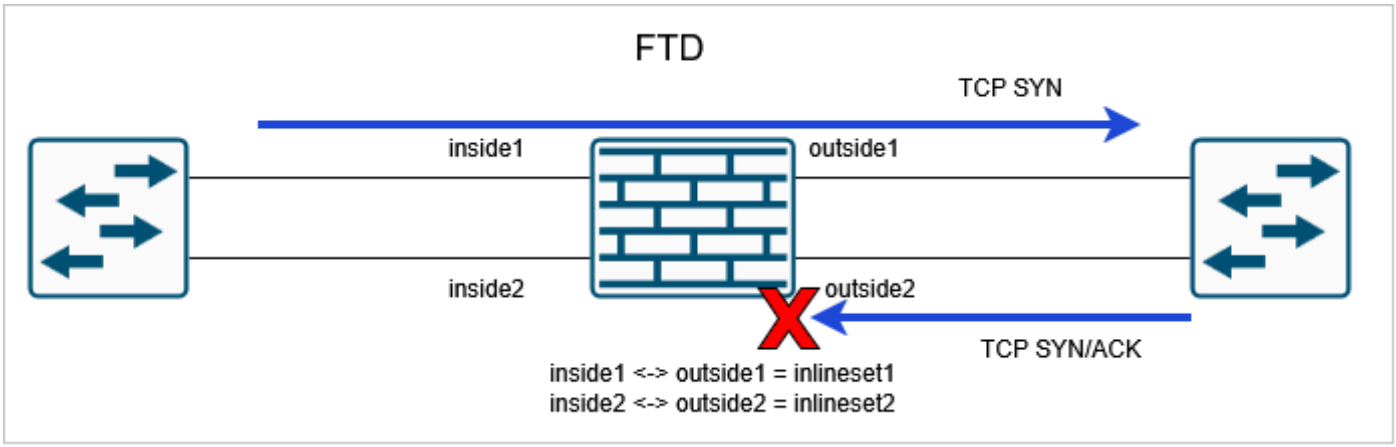


Asymmetrische TCP-stroom door FTD-inline-sets wanneer TSID is uitgeschakeld.

Wanneer echter een van deze functies is ingeschakeld, overschrijft het FTD-systeem TCP State Bypass en begint het met het uitvoeren van volledige TCP-statuscontroles op inline-interfaceverkeer:

- De optie "Enhanced application and URL Detection" onder TLS Server Identity Discovery.
- Een actief TLS/SSL-decoderingsbeleid.

Zodra TCP-statuscontroles zijn uitgevoerd, volgt de FTD de volledige TCP-handshake-reeks. In omgevingen met asymmetrische routering — waar bijvoorbeeld het TCP SYN-pakket via de outside1-interface afsluit, maar de overeenkomstige TCP SYN-ACK via de outside-interface op hetzelfde apparaat terugkeert — herkent de FTD de SYN-ACK niet als behorend tot een bekende, bijgehouden TCP-sessie. Omdat de SYN-ACK op een andere interface aankomt dan verwacht en er geen corresponderende SYN op die interface werd gezien, classificeert de FTD het als een niet-SYN-pakket voor een onbekende verbinding en laat het vallen met de ASP-dropreden tcp-not-syn.



Asymmetrische TCP-stroom door FTD-inline-sets wanneer TSID is ingeschakeld.

Gerelateerde inhoud

- Cisco Bug ID CSCwp84746 — Documentatie: TLS Server Identity Discovery incompatibiliteit met TCP State Bypass op inline-set interfaces
- Cisco Bug ID CSCwx42897 — DOC: TLS Server Identity Discovery overschrijft TCP State Bypass op inline-set interfaces, waardoor TCP-verkeer wordt verwijderd (tcp-not-syn)
- Cisco Bug ID CSCwx42901 — Voeg een waarschuwing toe bij het inschakelen van "Early application detection and URL categorization" (TSID) dat het TCP State Bypass uitschakelt op inline-set interfaces
- Cisco-documentatie — Richtlijnen voor TCP State Bypass (inclusief TLS Server Identity Discovery-beperking)
- Casestudy - Asymmetrisch verkeer door inline sets
- Cisco Technote — Hoe FTD- en FMC-bundels voor probleemoplossing te genereren
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.