Troubleshoot FTD Packet Drops (tcp-not-syn) when "Enhanced application and URL Detection" Is Enabled on Inline Interfaces with Asymmetric Traffic Flow

Contents

Issue

Firewall Threat Defense (FTD) appliances configured with inline interface sets drop TCP return traffic with the Accelerated Security Path (ASP) drop reason **tcp-not-syn**. This occurs immediately after the TLS Server Identity Discovery (TSID) feature — specifically the "**Enhanced application and URL Detection**" option is enabled. In older Firewall Management Center (FMC) versions the option is called **"Early application detection and URL categorization"**. The TCP SYN-ACK packets on the return path are dropped by the same FTD device that forwarded the original SYN, preventing TCP sessions from being established.

The issue manifests as widespread TCP connectivity failures and is not limited to TLS traffic. These symptoms are observed when the feature is enabled:

- TCP SYN-ACK packets on the return path are dropped with ASP drop reason **tcp-not-syn**.
- New TCP sessions do not appear in the FTD connection table.
- High ASP drop counters accumulate rapidly, as illustrated by this output captured approximately 10 minutes after the feature was enabled:

<#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
```

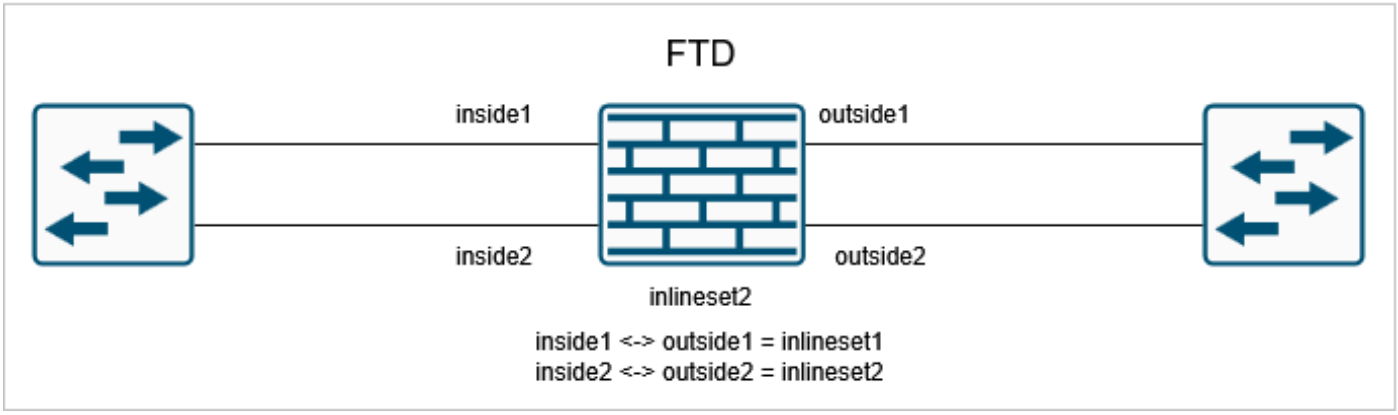
```
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)                1
 TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)                1
 Blocked or blacklisted by the reputation preprocessor (reputation)           1

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

Environment

- Platform: Cisco Firepower 4115. Other platforms can be also affected.
- FTD Software Version: 7.6.4. Other software versions can be also affected.
- FMC Software Version: 10.1.0. Other software versions can be also affected.
- FTD with inline interface sets.
- FTD has at least two inline interface pairs: **inlineset1** and **inlineset2** (or there are two different FTDs with one inline-set each).
- Asymmetric traffic flow present in the environment: TCP SYN egresses via the **outside1** interface while the corresponding TCP SYN-ACK returns via the **outside2** interface on the same FTD device.
- TSID feature is enabled on FTD.

Topology



Resolution

The recommended resolution to stop the **tcp-not-syn** drops and restore TCP connectivity through the inline

FTD interfaces is to disable the **"Enhanced application and URL Detection"** option within TSID. This allows the TCP State Bypass to remain active on the inline interface sets, which is necessary to accommodate asymmetric traffic flows in the environment.

Disable "Enhanced application and URL Detection" in FMC

Navigate to: **Policies > Access Control > [Your Access Control Policy] > Advanced > TLS Server Identity Discovery.** Uncheck or disable the **"Enhanced application and URL Detection"** checkbox, then deploy the policy to the affected FTD devices.

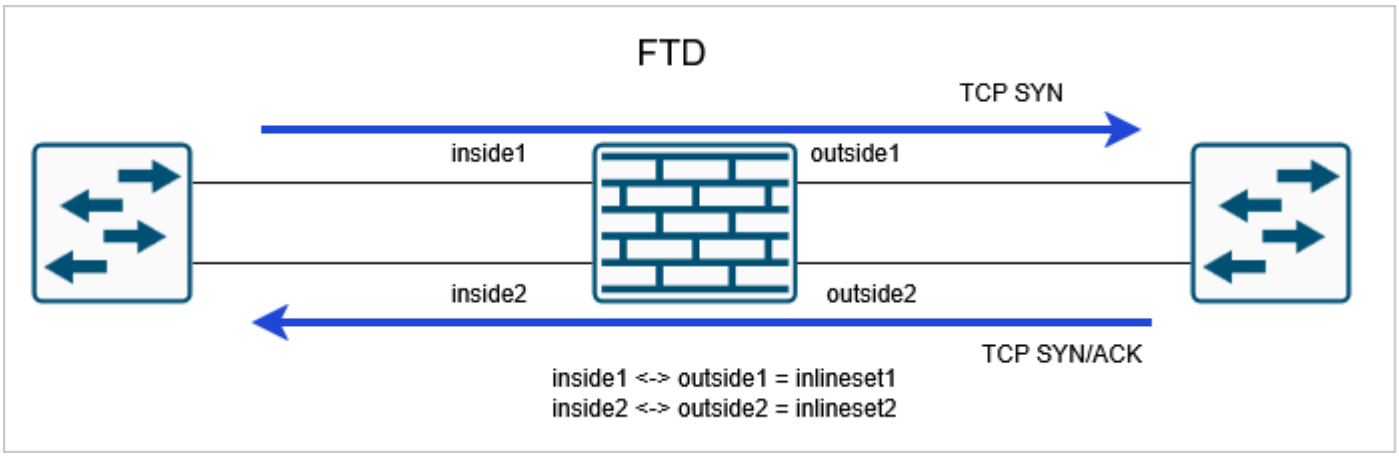
After disabling the feature, new sessions appear in the connection table, confirming that TCP connections are completing the three-way handshake successfully.

Note: With TSID disabled the FTD can no longer see the server certificate in TLS 1.3 sessions. Application and URL rules match traffic less accurately on encrypted traffic.

Cause

The root cause of the **tcp-not-syn** drops is an incompatibility between the **TLS Server Identity Discovery** feature and **TCP State Bypass** on inline interface sets in FTD.

By default, for traffic passing through inline interfaces on FTD, **TCP State Bypass is enabled**. TCP State Bypass is designed to allow asymmetric traffic — where the forward and return paths of a TCP connection can traverse different interfaces or even different devices — to pass without the FTD enforcing strict TCP state tracking. This is a necessary behavior in environments where routing asymmetry is present:

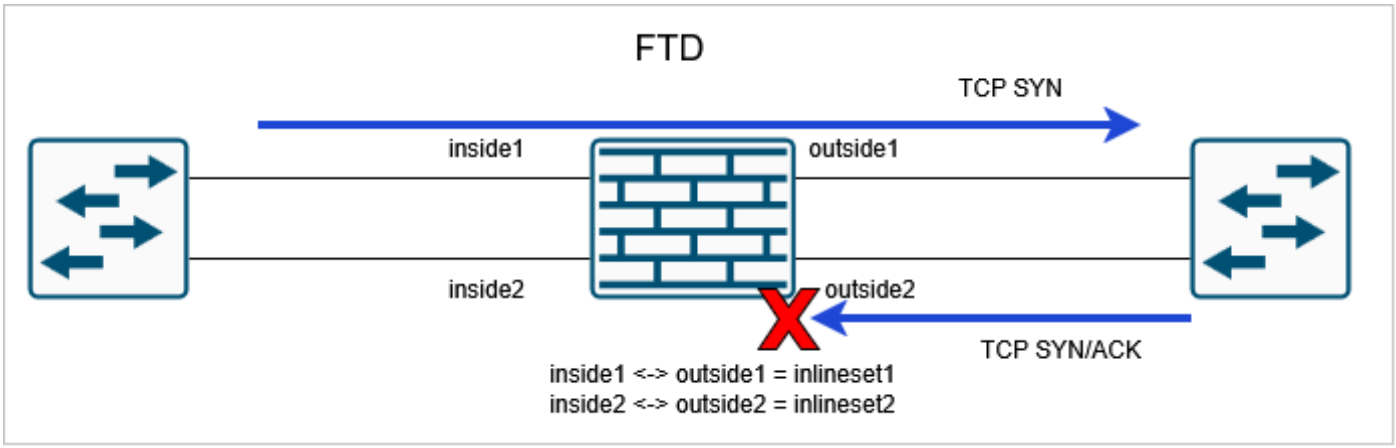


Asymmetric TCP flow through FTD inline sets when TSID is disabled.

However, when either of these features is enabled, the FTD system overrides TCP State Bypass and begins performing full TCP state checks on inline interface traffic:

- The **"Enhanced application and URL Detection"** option under TLS Server Identity Discovery.
- Any active TLS/SSL decryption policy.

Once TCP state checks are enforced, the FTD tracks the full TCP handshake sequence. In environments with asymmetric routing — where, for example, the TCP SYN packet exits via the **outside1** interface but the corresponding TCP SYN-ACK returns via the **outside** interface on the same device — the FTD does not recognize the SYN-ACK as belonging to a known, tracked TCP session. Because the SYN-ACK arrives on a different interface than expected and no corresponding SYN was seen on that interface, the FTD classifies it as a non-SYN packet for an unknown connection and drops it with the ASP drop reason **tcp-not-syn**.



Asymmetric TCP flow through FTD inline sets when TSID is enabled.

Related Content

- Cisco Bug ID CSCwp84746 — Documentation: TLS Server Identity Discovery incompatibility with TCP State Bypass on inline-set interfaces
- Cisco Bug ID CSCwx42897 — DOC: TLS Server Identity Discovery overrides TCP State Bypass on inline-set interfaces, causing TCP traffic to be dropped (tcp-not-syn)
- Cisco Bug ID CSCwx42901 — Add a warning when enabling "Early application detection and URL categorization" (TSID) that it disables TCP State Bypass on inline-set interfaces
- Cisco Documentation — Guidelines for TCP State Bypass (includes TLS Server Identity Discovery restriction)

- Case Study - Asymmetric traffic through inline sets
- Cisco Technote — How to Generate FTD and FMC Troubleshoot Bundles
- Cisco Technical Support & Downloads