"Enhanced application and URL Detection"；时，排除FTD数据包丢弃(tcp-not-syn)故障在使用非对称流量流的内联接口上启用

目录

问题

使用内联接口集配置的防火墙威胁防御(FTD)设备丢弃具有加速安全路径(ASP)丢弃原因tcp-not-syn的TCP返回流量。这在TLS服务器身份发现(TSID)功能(尤其是启用“增强型应用和URL检测”(Enhanced application and URL Detection)选项后立即发生。在较旧的防火墙管理中心(FMC)版本中，该选项称为“早期应用检测和URL分类”。 返回路径上的TCP SYN-ACK数据包会被转发原始SYN的相同FTD设备丢弃，从而无法建立TCP会话。

此问题表现为广泛的TCP连接故障，不限于TLS流量。启用该功能时，会观察到以下症状：

- 返回路径上的TCP SYN-ACK数据包将随ASP丢弃原因tcp-not-syn一起丢弃。
- 新的TCP会话不会显示在FTD连接表中。
- 高ASP丢弃计数器会快速累积，如启用此功能后约10分钟捕获的以下输出所示：

<#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
```

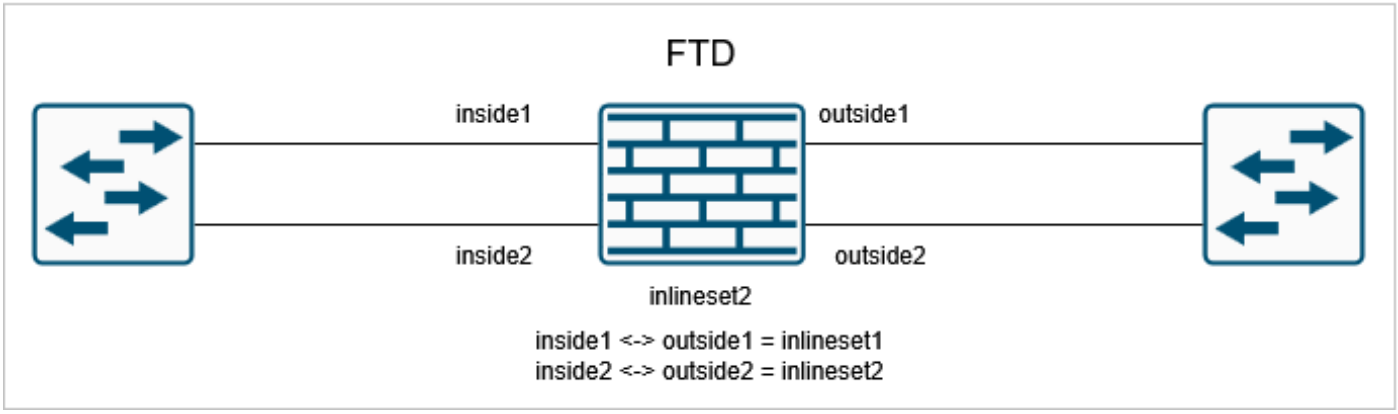
```
 Blocked or blacklisted by the reputation preprocessor (reputation)           1

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

环境

- 平台：Cisco Firepower 4115.其他平台也可能受到影响。
- FTD软件版本：7.6.4.其他软件版本也可能会受到影响。
- FMC软件版本：10.1.0。其他软件版本也可能会受到影响。
- 带有内联接口集的FTD。
- FTD至少有两个内联接口对：inlineset1和inlineset2（或有两个不同的FTD，每个都有一个内联集）。
- 环境中存在不对称流量：TCP SYN通过outside1接口退出，而相应的TCP SYN-ACK通过同一FTD设备上的outside2接口返回。
- FTD上启用了TSID功能。

拓扑



分辨率

建议通过内联FTD接口停止tcp-not-syn丢弃并恢复TCP连接的解决方案是禁用TSID中的“Enhanced application and URL Detection”选项。这允许TCP状态旁路在内联接口集上保持活动状态，这是适应环境中的不对称流量所必需的。

在FMC中禁用“增强的应用和URL检测”

导航至：策略>访问控制> [您的访问控制策略] >高级> TLS服务器身份发现。取消选中或禁用“Enhanced application and URL Detection”复选框，然后将策略部署到受影响的FTD设备。

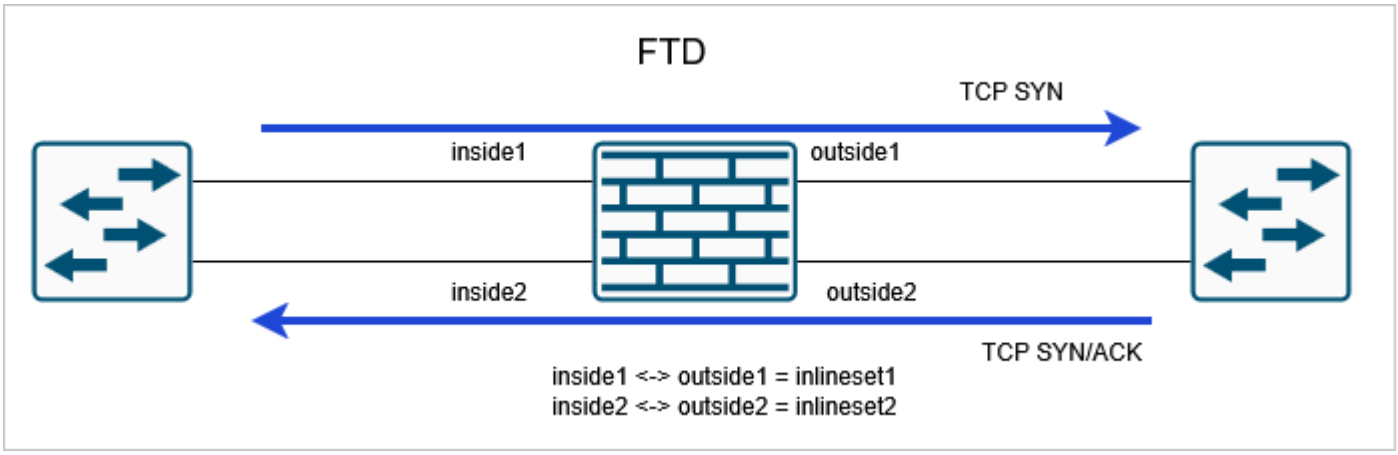
禁用该功能后，连接表中将显示新的会话，确认TCP连接成功完成三次握手。

注意：禁用TSID后，FTD无法再在TLS 1.3会话中看到服务器证书。应用和URL规则在加密流量上匹配流量的准确性较低。

原因

tcp-not-syn丢弃的根本原因是TLS服务器身份发现功能与FTD内联接口集上的TCP状态旁路之间的不兼容。

默认情况下，对于通过FTD上的内联接口的流量，TCP状态旁路处于启用状态。TCP状态旁路旨在允许非对称流量（其中TCP连接的转发和返回路径可以经过不同的接口甚至不同的设备）通过，而不执行FTD强制执行严格TCP状态跟踪。在存在路由不对称的环境中，这是必要行为：

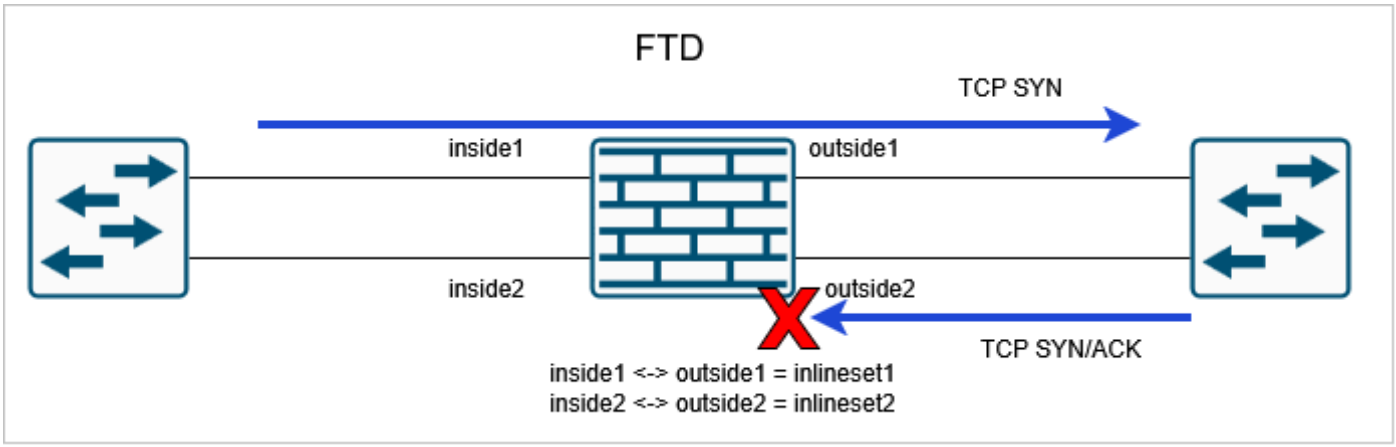


禁用TSID时，非对称TCP流通过FTD内联集。

但是，当启用其中任一功能时，FTD系统覆盖TCP状态旁路，并开始在内联接口流量上执行完整的TCP状态检查：

- TLS Server Identity Discovery下的“Enhanced application and URL Detection”选项。
- 任何活动的TLS/SSL解密策略。

实施TCP状态检查后，FTD将跟踪完整的TCP握手序列。在具有非对称路由的环境中（例如，TCP SYN数据包通过outside1接口退出，但相应的TCP SYN-ACK通过同一设备上的outside接口返回），FTD不会将SYN-ACK识别为属于已知的、跟踪的TCP会话。由于SYN-ACK到达与预期不同的接口，并且在该接口上未发现相应的SYN，因此FTD将其分类为未知连接的非SYN数据包，并使用ASP丢弃原因tcp-not-syn将其丢弃。



启用TSID时，非对称TCP流通过FTD内联集。

相关内容

- Cisco Bug ID CSCwp84746（思科漏洞ID CSCwp）— 文档：TLS服务器身份发现与内联集接口上的TCP状态旁路不兼容
- Cisco Bug ID CSCwx42897（仅限注册用户）— DOC:TLS服务器身份发现覆盖内联集接口上的TCP状态旁路，导致TCP流量被丢弃(tcp-not-syn)
- Cisco Bug ID CSCwx42901 — 启用“Early application detection and URL categorization”（早期应用检测和URL分类）(TSID)时添加警告，表示在内联集接口上禁用TCP状态旁路

- 思科文档 — TCP状态旁路指南（包括TLS服务器身份发现限制）
- 案例研究 — 通过内联集的不对称流量
- Cisco Technote — 如何生成FTD和FMC故障排除捆绑包
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。