非対称トラフィックフローのインラインインターフェイスで"；拡張アプリケーションおよびURL検出"；が有効になっている場合のFTDパケットドロップ(tcp-not-syn)のトラブルシューティング

内容

問題

インラインインターフェイスセットを使用して設定されたファイアウォール脅威対策(FTD)アプライアンスが、高速セキュリティパス(ASP)ドロップの理由がtcp-not-synであるTCPリターントラフィックをドロップします。これは、TLSサーバID検出(TSID)機能、特に「拡張アプリケーションおよびURL検出」オプションが有効になった直後に発生します。古いFirewall Management Center(FMC)バージョンでは、このオプションは「早期アプリケーション検出とURL分類」と呼ばれています。 リターンパス上のTCP SYN-ACKパケットは、元のSYNを転送したのと同じFTDデバイスによってドロップされ、TCPセッションの確立を妨げます。

この問題は、広範なTCP接続障害として現れ、TLSトラフィックに限定されません。この機能を有効にすると、次の症状が発生します。

- リターンパスのTCP SYN-ACKパケットは、ASPドロップ理由tcp-not-synでドロップされます。
- 新しいTCPセッションがFTD接続テーブルに表示されない。
- 高いASPドロップカウンタは、この機能がイネーブルになった約10分後にキャプチャされた次の出力に示すように、急速に蓄積されます。

<#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

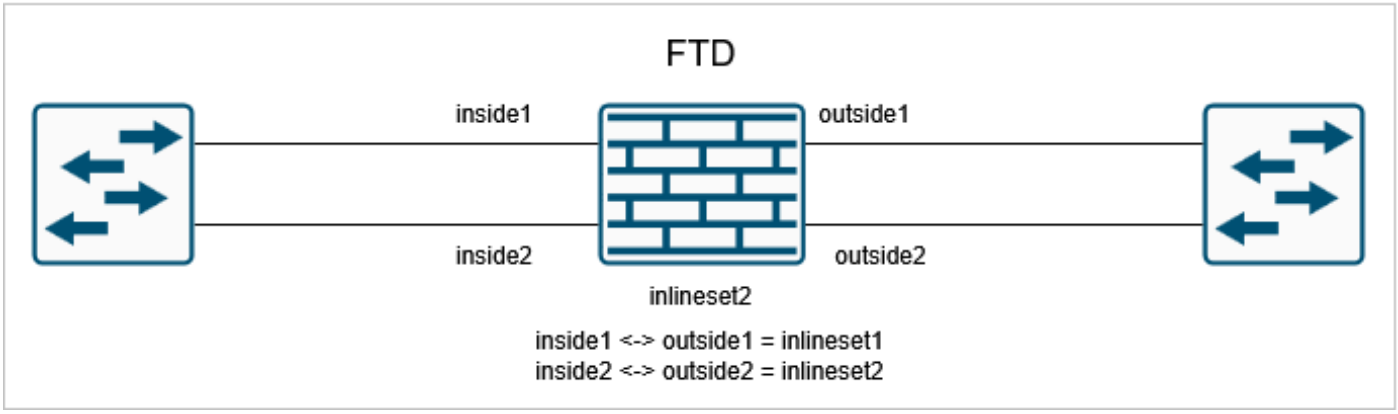
 TCP RST/FIN out of order (tcp-rstfin-ooo)                                     4
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                               995
 Dropped pending packets in a closed socket (np-socket-closed)                 3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)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

環境

- プラットフォーム：Cisco Firepower 4115他のプラットフォームも影響を受ける可能性があります。
- FTDソフトウェアバージョン：7.6.4他のソフトウェアバージョンも影響を受ける可能性があります。
- FMCソフトウェアバージョン：10.1.0他のソフトウェアバージョンも影響を受ける可能性があります。
- インラインインターフェイスセットを使用したFTD。
- FTDには、少なくとも2つのインラインインターフェイスペア、inlineset1とinlineset2があります（または、それぞれ1つのインラインセットを持つ2つの異なるFTDがあります）。
- 環境内に非対称のトラフィックフローが存在する場合：TCP SYNはoutside1インターフェイスを介して出力され、対応するTCP SYN-ACKは同じFTDデバイス上のoutside2インターフェイスを介して返されます。
- TSID機能がFTDで有効になっている。

トポロジ



解決方法

tcp-not-synドロップを停止し、インラインFTDインターフェイス経由でTCP接続を復元する場合の推奨される解決策は、TSIDで「拡張アプリケーションおよびURL検出」オプションを無効にすることです。これにより、TCP状態バイパスがインラインインターフェイスセットでアクティブのままになります。これは、環境内の非対称トラフィックフローに対応するために必要です。

FMCで「拡張アプリケーションとURL検出」を無効にする

Policies > Access Control > [Your Access Control Policy] > Advanced > TLS Server Identity Discoveryの順に選択します。「拡張アプリケーションおよびURL検出」チェックボックスのチェックを外すか無効にしてから、該当するFTDデバイスにポリシーを展開します。

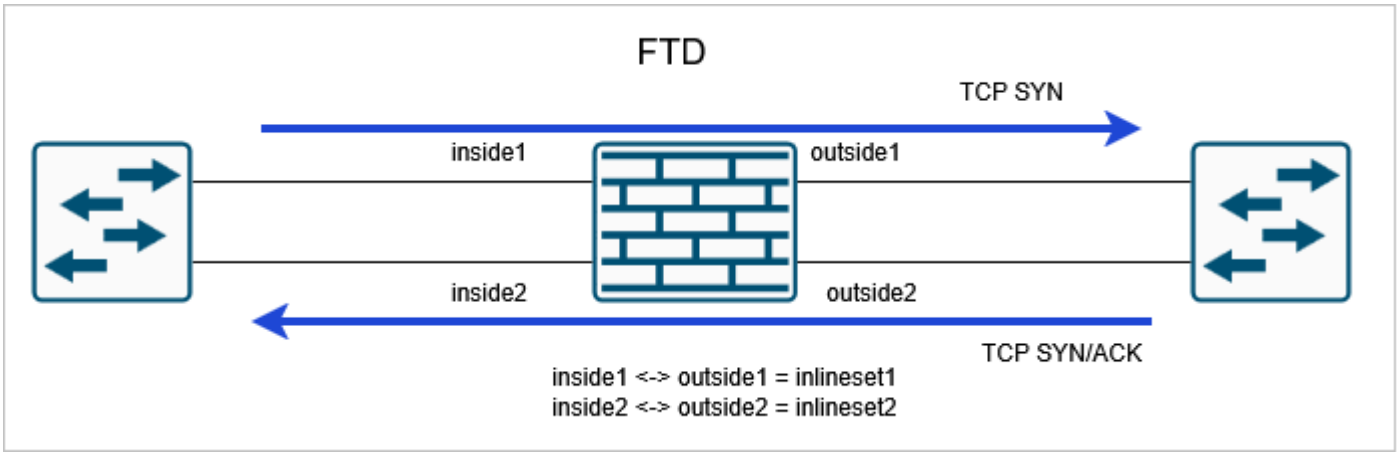
この機能を無効にすると、新しいセッションが接続テーブルに表示され、TCP接続が3ウェイハンドシェイクを正常に完了していることが確認されます。

注:TSIDが無効になっていると、FTDはTLS 1.3セッションでサーバ証明書を参照できなくなります。アプリケーションとURLのルールでは、暗号化されたトラフィック上のトラフィックの照合の精度が低くなります。

原因

tcp-not-synドロップの根本的な原因は、FTDのインラインインターフェイスセットでのTLSサーバIDディスカバリ機能とTCP状態バイパスとの間の互換性がないことです。

デフォルトでは、FTDのインラインインターフェイスを通過するトラフィックに対して、TCP状態バイパスが有効になっています。TCP状態バイパスは、非対称トラフィックを許可するように設計されています。非対称トラフィックでは、TCP接続の転送パスと戻りパスが異なるインターフェイスを通過したり、異なるデバイスを通過したりすることができ、FTDが厳密なTCP状態追跡を実施する必要はありません。これは、ルーティングの非対称が存在する環境で必要な動作です。

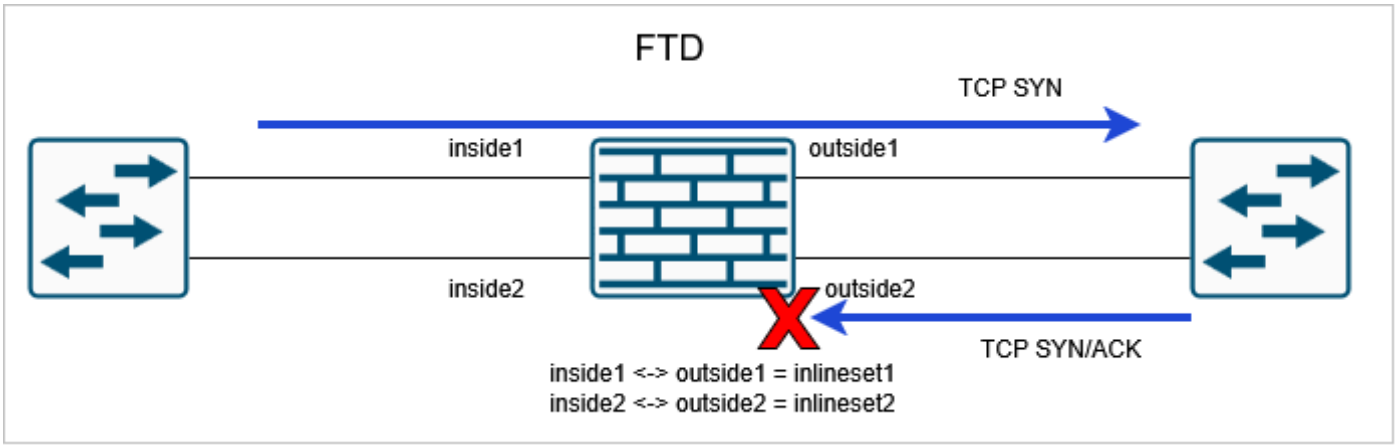


TSIDが無効な場合の、FTDインラインセットを介した非対称TCPフロー。

ただし、次のいずれかの機能が有効になっている場合、FTDシステムはTCP状態バイパスを上書きし、インラインインターフェイストラフィックに対して完全なTCP状態チェックの実行を開始します。

- TLS Server Identity Discoveryの下の「Enhanced application and URL Detection」オプション
- 任意のアクティブなTLS/SSL復号化ポリシー。

TCP状態チェックが適用されると、FTDは完全なTCPハンドシェイクシーケンスを追跡します。非対称ルーティングの環境では、たとえば、TCP SYNパケットがoutside1インターフェイス経由で送信され、対応するTCP SYN-ACKが同じデバイスのoutsideインターフェイス経由で返される場合、FTDではSYN-ACKが既知の追跡されたTCPセッションに属するものとして認識されません。SYN-ACKが予想とは異なるインターフェイスに到着し、そのインターフェイス上に対応するSYNが見つからなかったため、FTDは不明な接続に対してそれを非SYNパケットに分類し、ASPドロップの理由をtcp-not-synとしてそれをドロップします。



TSIDが有効な場合、FTDインラインセットを介した非対称TCPフロー。

関連コンテンツ

- Cisco Bug ID CSCwp84746（登録ユーザ専用）：ドキュメント：インラインセットインターフェイスでのTCP状態バイパスを使用したTLSサーバID検出の非互換性
- Cisco Bug ID CSCwx42897（登録ユーザ専用）:DOC:TLSサーバID検出がインラインセットインターフェイスのTCP状態バイパスを上書きし、TCPトラフィックがドロップされる(tcp-not-syn)
- Cisco Bug ID CSCwx42901（登録ユーザ専用）:「Early Application Detection and URL categorization」(TSID)を有効にしたときに、インラインセットインターフェイスでTCP状態バイパスを無効にする警告が追加されました
- シスコのドキュメント：TCP状態バイパスのガイドライン（TLSサーバID検出の制限を含む）
- ケーススタディ：インラインセットを介した非対称トラフィック
- Cisco Technote:FTDおよびFMCのトラブルシューティングバンドルの生成方法
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。