TCP終了後のFMCトラフィックドロップによる古いACKパケットのトラブルシューティング

内容

問題

このドキュメントでは、FTDがFMCからクライアントシステムへのリターントラフィック用のacl-dropイベントを記録する理由、特にクライアントからのRSTパケットによってTCP接続がすでに終了している後に着信するACKパケットについて説明します。ドロップは、WindowsのTCPスタックの動作とFMCのRFC 793準拠のACK生成との間でマイクロ秒レベルの競合状態が発生したことが原因です。サービスへの影響はなく、修復も不要です。

注：これは正常な動作です。このパターンが確認されたら、acl-dropイベントを安全にフィルタリングして、モニタリングシステムで除外できます。

症状：

- FTDファイアウォールログに、FMCからクライアントシステムへのリターントラフィックのacl-dropイベントが表示されます（この例ではJumpHost）。
- ドロップは、FMCとクライアントシステム間のTCPポート443(HTTPS)接続で発生します
- FMCユニファイドイベントでは、イベントはブロックされたパケットとして表示されます
- キャプチャに表示されるドロップ理由コード：tcp-rstfin-ooo、tcp-not-syn、acl-drop
- ログに記録された廃棄にもかかわらず、実際のサービスへの影響は見られません

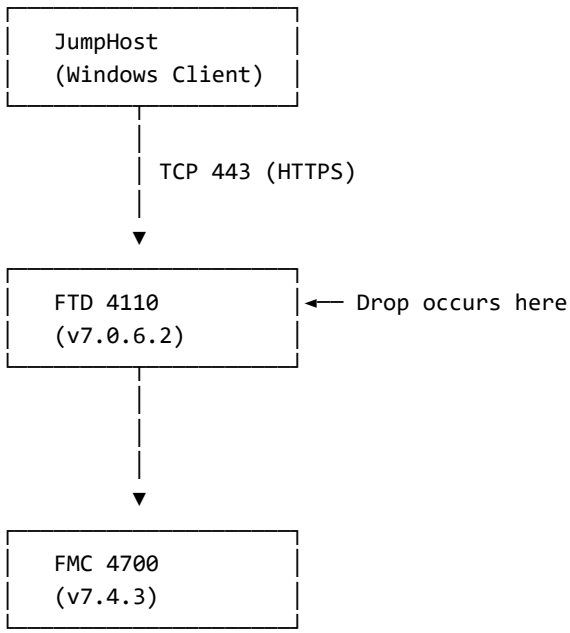
環境

・ ファイアウォール：バージョン7.0.x、7.2.x、7.4.x以降（FPR-1000/2100/3100/4100/4200/9300またはFTDv）を実行するCisco Secure Firewall Threat Defense(FTD)

・ Management Center：バージョン7.2.x、7.4.x以降を実行するCisco Secure Firewall Management Center(FMC)4600/4700/FMCv

・ クライアントシステム：Windows OS（JumpHost、ワークステーション、またはサーバ）がHTTPS(TCP 443)経由でブラウザ/API経由で接続

単純なトポロジ



解決方法

パケットシーケンス

ログに記録されたドロップの前には、常に次のシーケンスが続きます。

```
Packet Flow & Timing Collision:
```

Step	Packet Direction	TCP Flags	Delta Timing	Description / State
1.	FMC ——► Client	[FIN, ACK]	T=0	FMC initiates graceful session close.
2.	Client → FMC	[ACK]	+0.2 ms	Client acknowledges FMC FIN.
3.	Client → FMC	[FIN, ACK]	+3ms - 13s	Application closes its half of socket.
4.	Client → FMC	[RST, ACK]	+15 - 31 µs	Windows immediately destroys socket.
5.	[FTD Firewall Action]	---	Immediate	FTD receives RST, purges connection from st
6.	FMC ——► Client	[ACK]	+0.06 - 2.2 ms	RFC 793 mandatory ACK for Step 3 FIN arrives.
7.	[FTD Firewall Action]	[acl-drop]	Immediate	No state table entry found -> Dropped as ac



注：ステップ5と7はコリジョンポイントです。RSTによって即座にステートが削除され（ステップ6）、ステートの削除から次のパケット評価サイクルまでの間に、FMCの必須ACK（ステップ7）がウィンドウに到達します。

TACの調査方法

古くなったACKのドロップが疑われる場合の調査では、次の3階層の相関プロセスを使用します。

ステップ1：データの収集

- 入力インターフェイス、出力インターフェイス、およびaspドロップでのFTDパケットキャプチャ
- ポート443でフィルタリングされたFMCからのTCPダンプ

```
> system support diagnostic-cli
ciscoasa# capture ASP_DROP type asp-drop acl-drop
ciscoasa# show capture ASP_DROP | include 443
1: 10:14:22.102345 10.10.32.15.443 > 10.10.10.50.55137: Flags [.], ack 3829104, win 501, length 0 (acl-
```

ステップ2：抽出と関連付け

・ asp drop captureから5タプルを抽出すると、ドロップと理由(tcp-rstfin-ooo、tcp-not-syn、acl-drop)が表示されます。

・ 入力および出力キャプチャを使用して接続状態テーブルを再構築します。SYN、FIN/RST、および正確なタイムスタンプを特定します。

・ ドロップ、入力/出力キャプチャのタイムスタンプを、セッションのサポート終了タイムスタンプと関連付けます。

```
ciscoasa# show capture CAP_IN | include 10.10.10.50.55137
10:14:22.102110 10.10.10.50.55137 > 10.10.32.15.443: Flags [F.], seq 3829103, ack 1024
10:14:22.102128 10.10.10.50.55137 > 10.10.32.15.443: Flags [R.], seq 3829104, ack 1024
10:14:22.102345 10.10.32.15.443 > 10.10.10.50.55137: Flags [.], ack 3829104 (DROPPED)
```

注:FMCのACKシーケンスは、FINシーケンス番号$+ 1$に対する確認応答を送信します。確認応答は、すでに終了している接続に対するRFC応答であることを示します。

ステップ3：パターンの確認

- ドロップの確認は、RSTが処理された後にのみ行われ、アクティブセッション中には行われません
- ドロップされたパケットがシーケンス番号= FIN_Seq + 1のACKであることを確認します（RFC 793の必須応答）。
- ドロップイベントに対応するアプリケーション障害がないことを確認します

ヒント：参照ケース(SR 700468261)では、55セッション中54セッションが最終パケットとしてRSTを示しています。あるセッション（ポート55137）では、FMCのACKがRSTの0.024ミリ秒後に到達し、競合状態のタイミングを直接示していました。

解決方法

修復は必要ありません。この動作は、TCP RFC標準およびステートフルファイアウォール設計に

完全に準拠しています。不具合、パフォーマンスの低下、データの消失は生じません。

エスカレーションするタイミング

警告：このドロップパターンだけに基づいてエスカレーションしないでください。次のセクションの条件が満たされた場合にのみエスカレーションします。

- ドロップは、RSTまたはFIN/ACK交換の後ではなく、アクティブセッション中に発生します
- アプリケーション障害、セッションタイムアウト、またはFMC GUIのアクセス不能が発生する
- 接続ボリュームの増加に対応せずに、ドロップ量が時間とともに増加する
- ドロップパターンは、この記事で説明した順序とは異なります

原因

このドロップは、3つの独立して正しい動作の間のマイクロ秒タイムスケールでの競合状態に起因します。

1. Windows TCPスタック最適化：リモートエンドがすでにFINを送信しているソケットをWindowsアプリケーションが閉じると、Windowsは直ちにFIN-ACKを送信します。これは、メモリとTCP制御ブロックを即時に解放するための15 ~ 31秒内のRST-ACKの後です。
2. FTDステートフル接続の削除：RSTパケットを受信すると、FTDはただちにティアダウンし、ステートフルなセキュリティ整合性を維持するために状態テーブル(conn table)から接続エントリを消去します。
3. FMC RFC 793準拠：RFC 793仕様に従い、FMC TCPスタックはクライアントのFIN（シーケンス$+ 1$）を確認応答するACKを生成します。 システムのスケジューリングと伝搬遅延が原因で、このACKはFTDに到達します。
   0.06:RSTがすでに接続をフラッシュした後2.2ミリ秒。
4. FTDドロップ評価：一致する接続が状態テーブルに存在せず、パケットには（SYNではなく）ACKフラグだけがあるため、FTDはアクセスコントロールリスト(ACL)に対してそれを評価します。 out-of-state ACKを明示的に許可しない場合、FTDはacl-drop / tcp-not-synとしてパケットをドロップします。

関連コンテンツ

- RFC 793：伝送制御プロトコル
- ASPドロップの理由
- SRリファレンス：700468261（社内）

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。