# Firepower Management Center で一部の TCP 接続イベントが間違った方向に表示される

## 内容



## 概要

このドキュメントでは、FirePOWER Management Center（FMC）で TCP 接続イベントが逆方向（イニシエータ IP が TCP 接続のサーバ IP であり、レスポンダ IP が TCP 接続のクライアント IP である）で表示される原因と、その緩和手順について説明します。

> **注**：このようなイベントが発生する理由はさまざまです。このドキュメントでは、この症状の最も一般的な原因について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- FirePOWER 技術
- 適応型セキュリティ アプライアンス（ASA）の基礎知識
- Transmission Control Protocol（TCP）タイミング メカニズムの知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 6.0.1 以降が稼働する ASA Firepower Threat Defense（5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X）
- ソフトウェア バージョン 6.0.1 以降が稼働する ASA Firepower Threat Defense（5512-X、5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、FP9300、FP4100）
- Firepower モジュールを搭載し、ソフトウェア バージョン 6.0.0 以降が稼働する ASA（5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X,5515-X, ASA 5525-X, ASA 5545-

X, ASA 5555-X, ASA 5585-X ）
- Firepower Management Center （ FMC ）バージョン 6.0.0 以降。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

# 背景

TCP 接続では、**クライアントは開始パケットを送信する IP を指します。**管理対象デバイス（センサーまたは FTD ）が接続の開始 TCP パケットを確認すると、FirePOWER Management Center が接続イベントを生成します。

エンドポイントにより誤ってクローズされなかった接続が、長期にわたって使用可能なメモリを消費しないようにするため、TCP 接続の状態を追跡するデバイスでは**アイドル タイムアウトが定義されています。**FirePOWER で確立された TCP 接続のデフォルト アイドル タイムアウトは **3 分**です。3 分以上にわたってアイドルである TCP 接続は、FirePOWER IPS センサーにより追跡されません。

タイムアウト後の後続のパケットは新しいTCPフローとして扱われ、このパケットに一致するルールに従って転送決定が行われます。パケットがサーバから送信されると、サーバのIPがこの新しいフローのイニシエータとして記録されます。このルールでロギングが有効な場合、Firepower Management Center で接続イベントが生成されます。

> **注：**設定されているポリシーに基づき、タイムアウト後に到着したパケットの転送に関する決定は、開始 TCP パケットのときの決定とは異なります。設定されているデフォルト アクションが「Block」の場合、パケットがドロップされます。

この症状の例として、以下にスクリーンショットを示します。

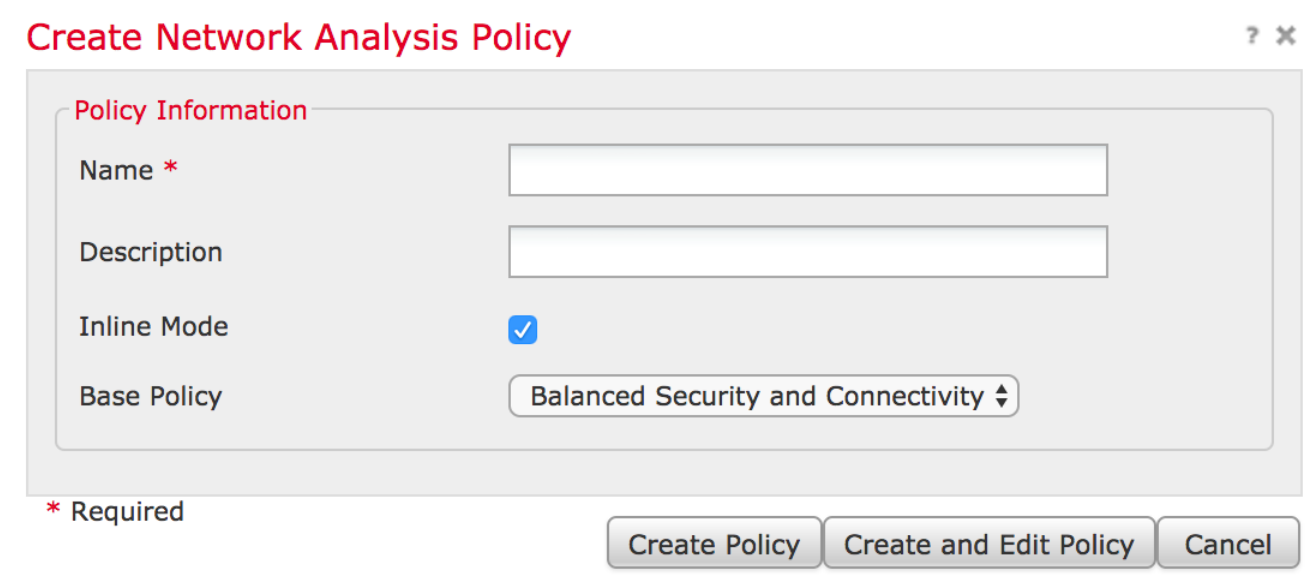
| | First Packet | Last Packet | Action | Reason | Initiator IP | Initiator Country | Responder IP | Responder Country | Ingress Security Zone | Egress Security Zone | Source Port / ICMP Type | Destination Port / ICMP Code |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2017-05-12 17:48:05 | | Block | | 10.32.38.30 | | 192.168.38.30 | | | | 443 (https) / tcp | 44705 / tcp |
| | 2017-05-12 17:39:13 | | Allow | | 192.168.38.30 | | 10.32.38.30 | | | | 44705 / tcp | 443 (https) / tcp |

# 解決方法

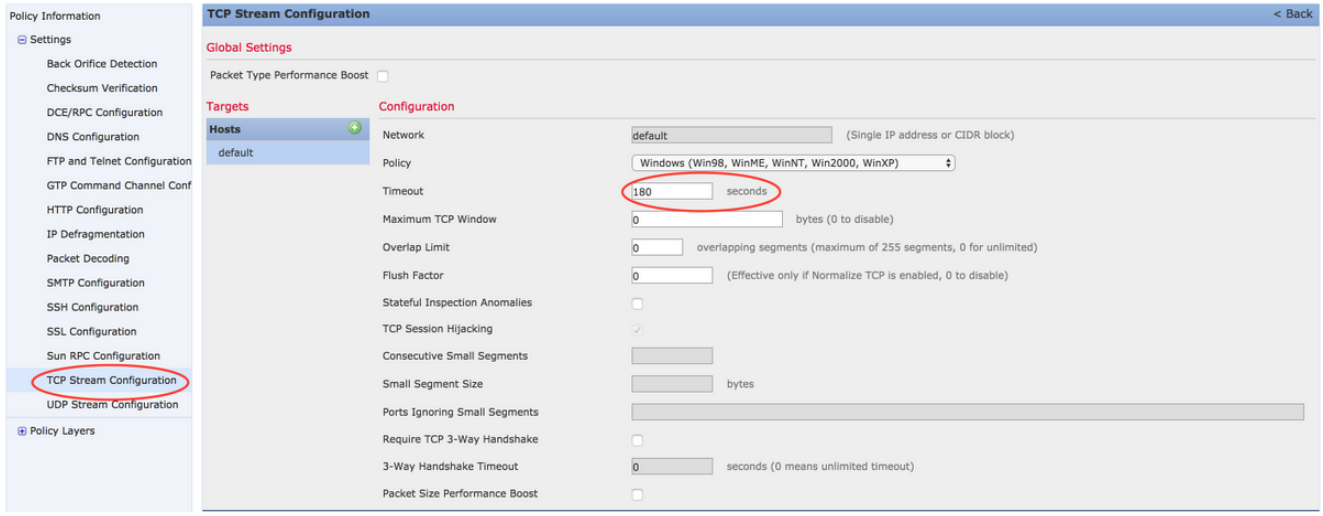
前述の問題は、TCP 接続の [Timeout] **を増加することで緩和できます。**タイムアウトを変更するには、次の手順に従います s 。

1. [Policies] > [Access Control] > [Intrusion] の順に選択します。
2. 右上隅に移動し、[Network Access Policy] を選択します。

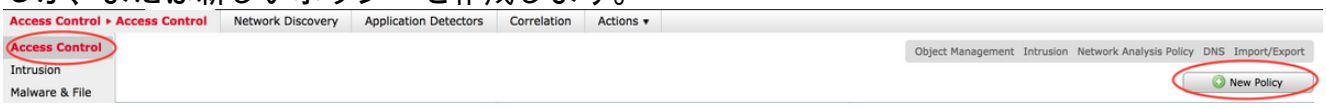

3. [Create Policy] を選択し、名前を選択し、[Create and Edit Policy] をクリックします。[Base Policy] **は変更しないでください。**



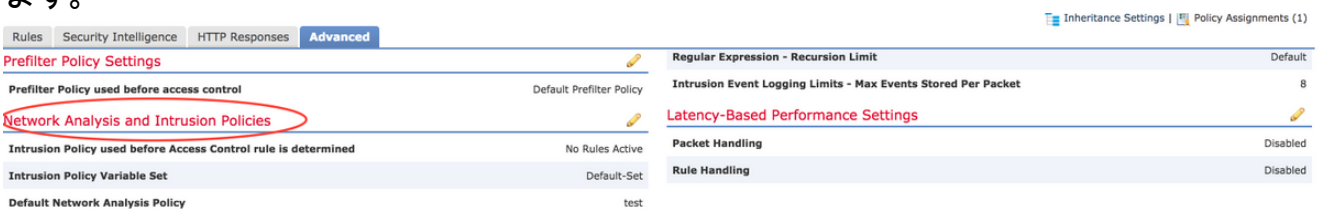

4. [Settings] オプションを展開し、[TCP Stream Configuration] を選択します。
5. 設定セクションに移動し、[Timeout] **の値を必要な値に変更します。**




6. [Policies] > [Access Control] > [Access Control] の順に移動します。
7. [Edit] オプションを選択し、関連する管理対象デバイスに適用されているポリシーを編集するか、または新しいポリシーを作成します。




8. アクセス ポリシーの [Advanced] **タブを選択します。**
9. [Network Analysis and Intrusion Policies] **セクションに移動し、[Edit]** アイコンをクリックします。




10. [Default Network Analysis Policy] のドロップダウン メニューから、ステップ 2 で作成したポリシーを選択します。
11. [OK] をクリックし、変更を保存します。
12. [Deploy] オプションをクリックし、関連する管理対象デバイスにポリシーを導入します。

**注意**：タイムアウトを増加するとメモリ使用率が高くなることが想定されます。

FirePOWER は、長期にわたってエンドポイントによりクローズされていないフローを追跡する必要があります。メモリ使用率が実際にどのように上昇するかは、ネットワーク アプリケーションで TCP 接続をアイドルにする期間に応じて異なるため、固有ネットワークごとに異なります。

## 結論

TCP 接続のアイドル タイムアウトのベンチマークは、ネットワークによって異なります。これは、使用されているアプリケーションに完全に依存しています。ネットワーク アプリケーションで TCP 接続をアイドルにしている期間を観察することで、最適な値を確立する必要があります。Cisco ASA での FirePOWER サービス モジュールに関連する問題のために、最適な値を減らすことができない場合は、ASA のタイムアウト値までタイムアウトを徐々に増加することで調整できます。

## 関連情報

- ASA 向け Cisco Firepower Threat Defense クイック スタート ガイド
- テクニカル サポートとドキュメント – Cisco Systems
- ASA Firepower クイック スタート ガイド