Firepowerデータパスのトラブルシューティング フェーズ8:ネットワーク分析ポリシー

内容

概要

この記事は、Firepowerシステムのデータパスを体系的にトラブルシューティングし、Firepowerのコンポーネントがトラフィックに影響を与えているかどうかを判断する方法を説明する一連の記事の一部です。Firepowerプラットフォームのアーキテクチャと、その他のデータパスのトラブルシューティング記事へのリンクについては、「概要」の記事を参照してください。

この記事では、Firepowerのデータパスのトラブルシューティングの8番目の段階であるネットワーク分析ポリシー機能について説明します。

前提条件

- この記事は、すべてのFirepowerプラットフォームに適用されます
  トレース**機能**は、Firepower Threat Defense(FTD)プラットフォームのソフトウェアバージョン6.2.0以降でのみ使用できます。
- オープンソースSnortの知識は役に立ちますが、必須ではありません オープンソースSnortの詳細については、https://www.snort.org/を参照してくださ[い](#)

ネットワーク分析ポリシー機能のトラブルシューティング

ネットワーク分析ポリシー(NAP)には、特定されたアプリケーションに基づいてトラフィックの検査を実行するSnortプリプロセッサ設定が含まれています。プリプロセッサには、設定に基づい

てトラフィックをドロップする機能があります。この記事では、NAP構成を確認し、プリプロセッサのドロップを確認する方法について説明します。

> **注**：プリプロセッサルールには、「1」または「3」（つまり129、119、124）以外のジェネレータID(GID)があります。 GIDからプリプロセッサへのマッピングの詳細については、FMC構成ガイドを参照してください。

「trace」ツールを使用したプリプロセッサドロップの検出（FTDのみ）

システム**サポートトレースツ**ールを使用して、プリプロセッサレベルで実行されるドロップを検出できます。

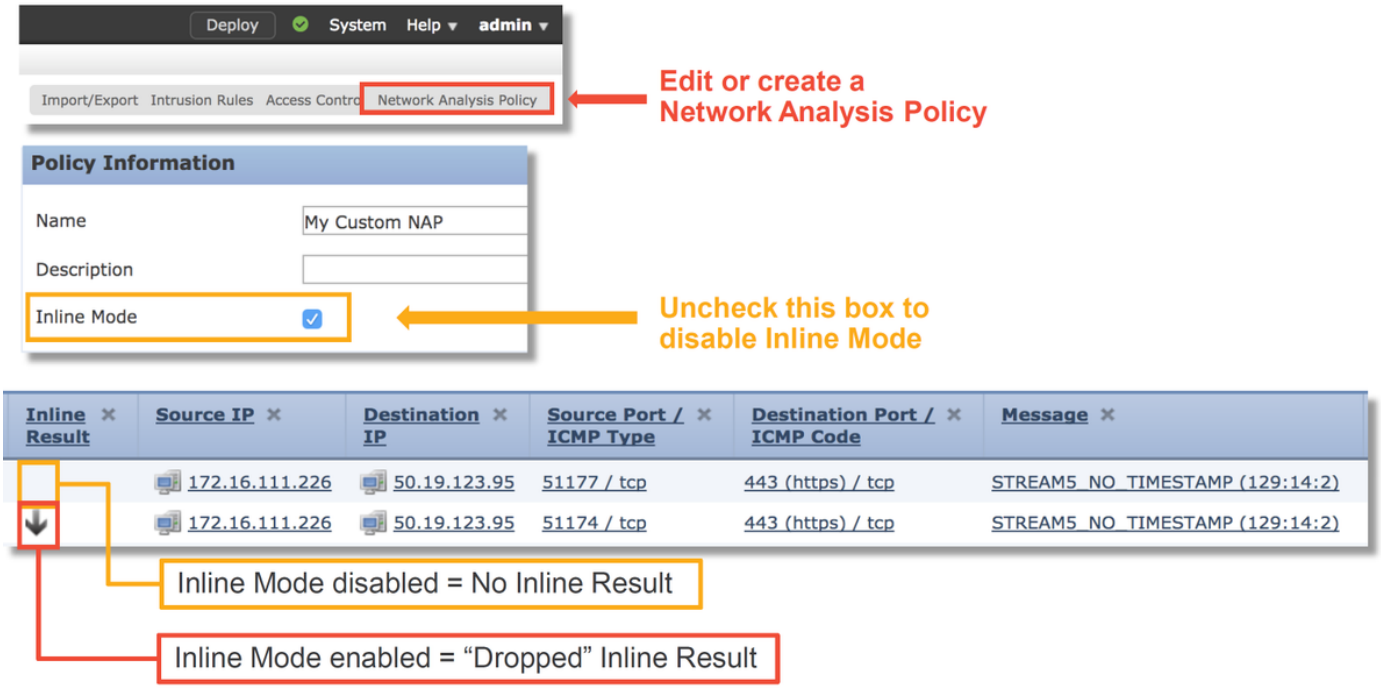
次の例では、TCP正規化プリプロセッサが異常を検出しました。その結果、トラフィックはルール**129:14によってドロップさ**れ、TCPストリーム内でタイムスタンプが欠落していることを探します。

```
> system support trace

[omitted for brevity…]

172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 - 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or
unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 AppID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 Starting with minimum 3, 'block urls', and SrcZone first with zones -1 -> -1, geo 0 ->
0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ===> Blocked by Stream
```

> **注**：**TCP** Stream Configuration**プロプロセッサ**はトラフィックをドロップしますが、インライン正規化プリプロセッサも有効**になっているため**、ドロップできます。インライン正規化の詳細については、この記事を参照してください。

NAP構成の確認

Firepower Management Center(FMC)のUIで、NAPを[Policies] > [Access Control] > [Intrusion]の下**に表示できます**。次に、右上の[Network Analysis Policy]オプションをクリックします。このオプションをクリックすると、NAPを表示し、新しいポリシーを作成し、既存のポリシーを編集できます。

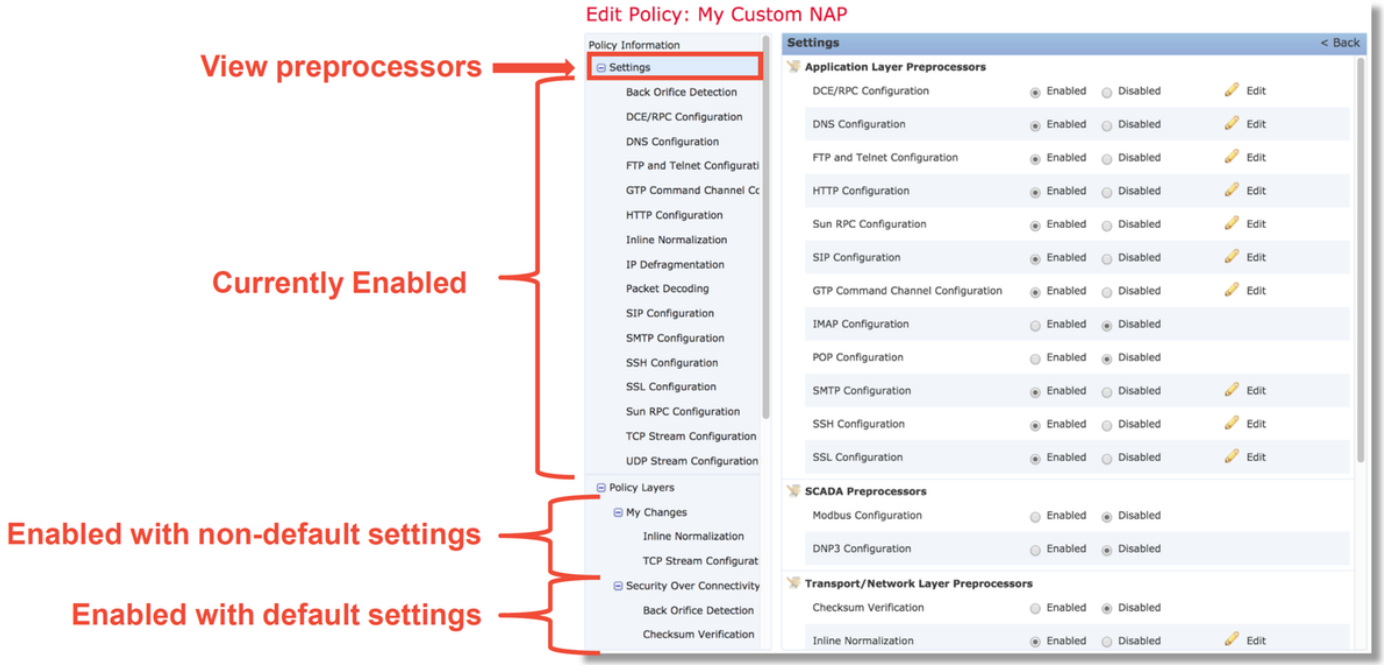


上の図に示すように、NAPには「インラインモード」機能が含まれています。これは、侵入ポリシーの「インライン時にドロップ」オプションに相当します。NAPによるトラフィックのドロップを防ぐ簡単な手順は、[インラインモード]をオフにすることです。NAPによって生成された侵入イベントは、インラインモードが無効な状態で[インライン結果]タブに何も表示されません。

NAP設定の表示

NAP内で、現在の設定を表示できます。これには、有効なプリプロセッサの総数と、

次の図に示すように、プリプロセッサはデフォルト以外の設定（手動で微調整したもの）で有効にされ、デフォルト設定で有効にされます。

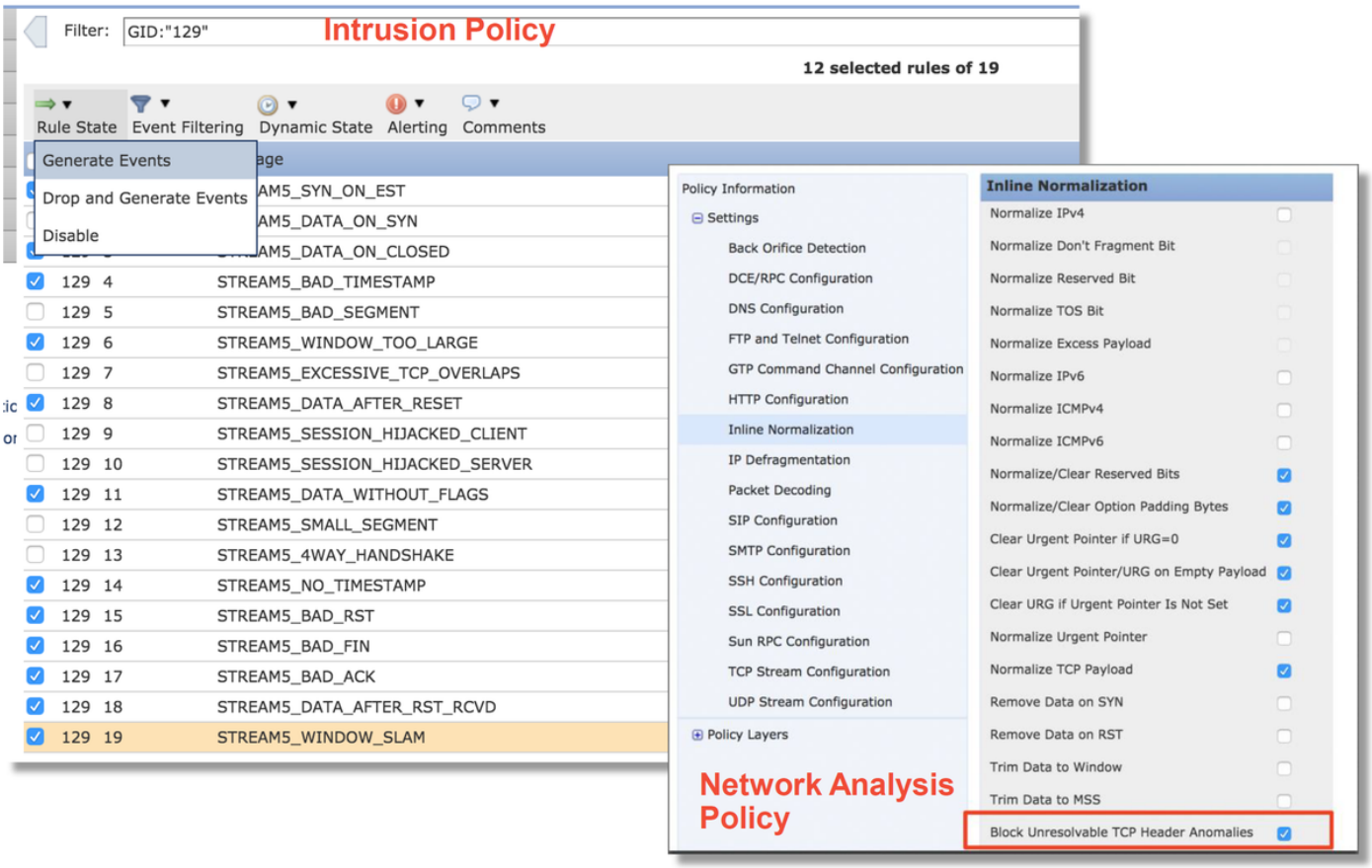


サイレントドロップを引き起こす可能性のあるNAP設定

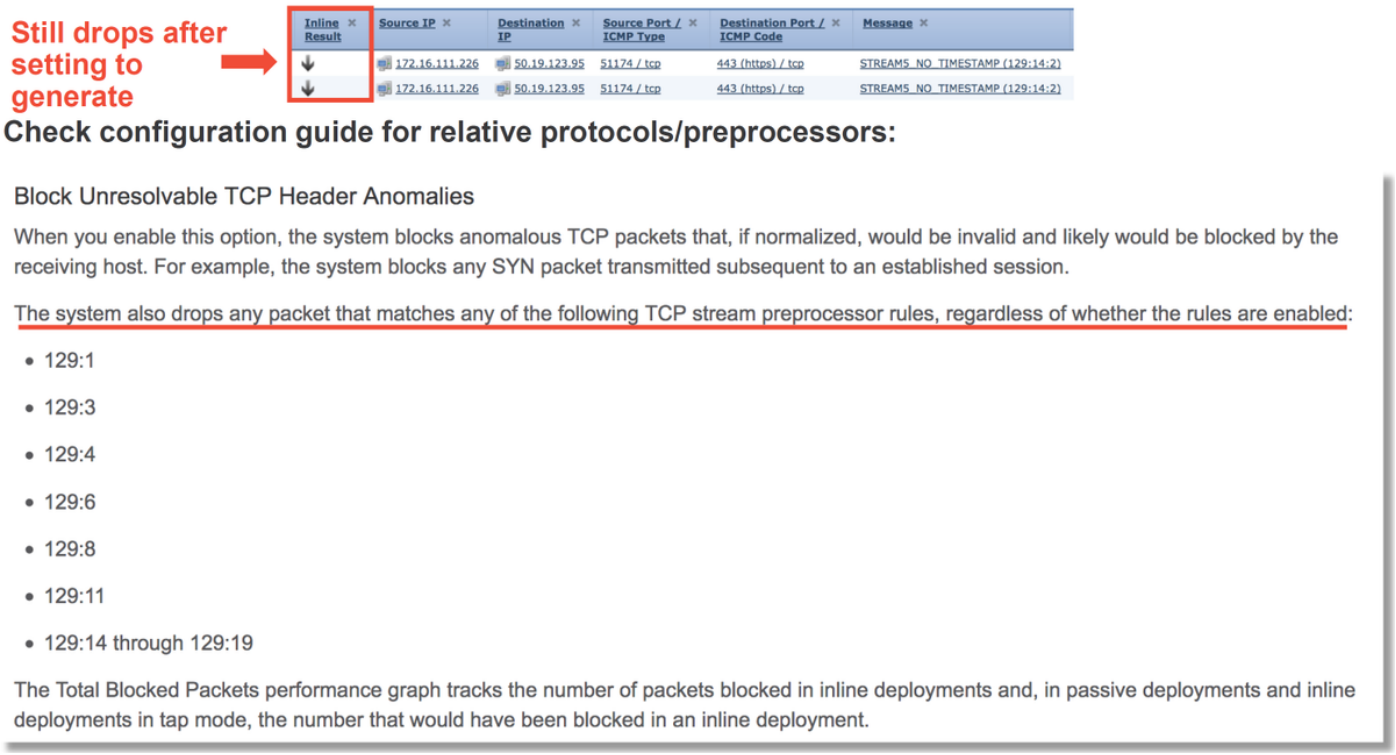
トレースセクションで説明した例では、ルールTCPストリーム構成ルール129:14がトラフィックをドロップしています。これは、システムサポートトレースの出力を調べることによって決まります。ただし、該当するルールがそれぞれの侵入ポリシー内で有効になっていない場合、FMCには侵入イベントは送信されません。

この問題が発生する理由は、Block Unresolvable TCP Header Anomalyと呼ばれるインライン正規化プロプロセッサ内の設定が原因です。このオプションは、基本的に、特定のGID 129ルールがTCPストリームの異常を検出したときに、Snortがブロックアクションを実行できるようにします。

Block Unresolvable TCP Header Anloaturesが有効な場合は、次の図に従ってGID 129ルールをオンにすることをお勧めします。



GID 129ルールをオンにすると、FMCがトラフィックに対してアクションを実行するときに、侵入イベントが送信されます。ただし、[Block Unresolvable TCP Header Promises]が有効である限り、侵入ポリシーの[Rule State]が[Generate Events]に設定されている場合でも、トラフィックをドロップする可能性があります。この動作については、『FMCコンフィギュレーションガイド』で説明します。



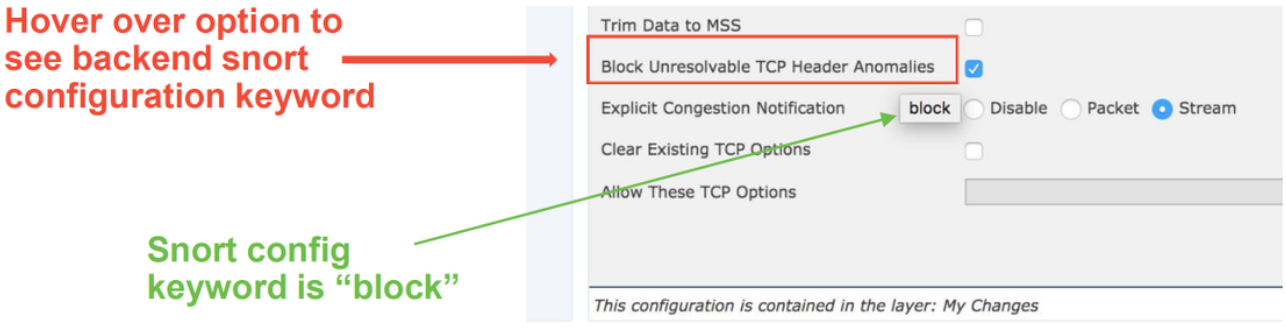
上記のドキュメントは、この記事に記載されていま す(バージョン6.4については、この記事の投稿時点で最新のバージョン)。

バックエンド設定の確認

プリプロセッサの動作には、FMCに反映されずに特定の設定をバックエンドで有効にできるという複雑さのレイヤが追加されています。考えられる理由を次に示します。

- 他の有効な機能では、プリプロセッサ設定を強制的に有効にする機能があります（主にファイルポリシーです）
- 一部の侵入ポリシールールでは、検出を実行するために特定のプリプロセッサオプションが必要です
- 不具合は挙動を起こすことがある CSCuz50295 – 「マルウェアブロックを使用したファイルポリシーにより、ブロックフラグを使用したTCP正規化が可能になる」という例が見られました。

バックエンドの構成を確認する前に、バックエンドのSnort構成ファイルで使用されるSnortキーワードは、NAP内の特定の設定にカーソルを合わせると表示されることに注意してください。次の図を参照してください。



[NAP]タブの**[ブロック未解決TCPヘッダー異常]**オプションは、バックエンドの**block**キーワードに変換されます。この情報を念頭に置いて、バックエンドの設定をエキスパートシェルから確認できます。

```
root@ciscoasa:~# de_info.pl

DE Name         : Primary Detection Engine (c9ef19d6-e187-11e6-ba76-99617d53da68)
DE Type         : ids
DE Description  : Primary detection engine for device c9ef19d6-e187-11e6-ba76-99617d53da68
DE Resources    : 1
DE UUID         : 0d82120c-e188-11e6-8606-a4827d53da68

root@ciscoasa:~# cd /var/sf/detection_engines/0d82120c-e188-11e6-8606-a4827d53da68/network_analysis/
root@ciscoasa: network_analysis# ls
b50f27b0-e31a-11e6-b866-dd9e65c01d56  object_b50f27b0-e31a-11e6-b866-dd9e65c01d56  snort.conf.b50f27b0-e31a-11e6-b866-
dd9e65c01d56  snort.conf.b50f27b0-e31a-11e6-b866-dd9e65c01d56.default
root@ciscoasa: network_analysis# cat b50f27b0-e31a-11e6-b866-dd9e65c01d56/normalize.conf
#
# generated from My Changes
#
preprocessor normalize_tcp: ips, rsv, pad, req_urg, req_pay, req_urp, block
```

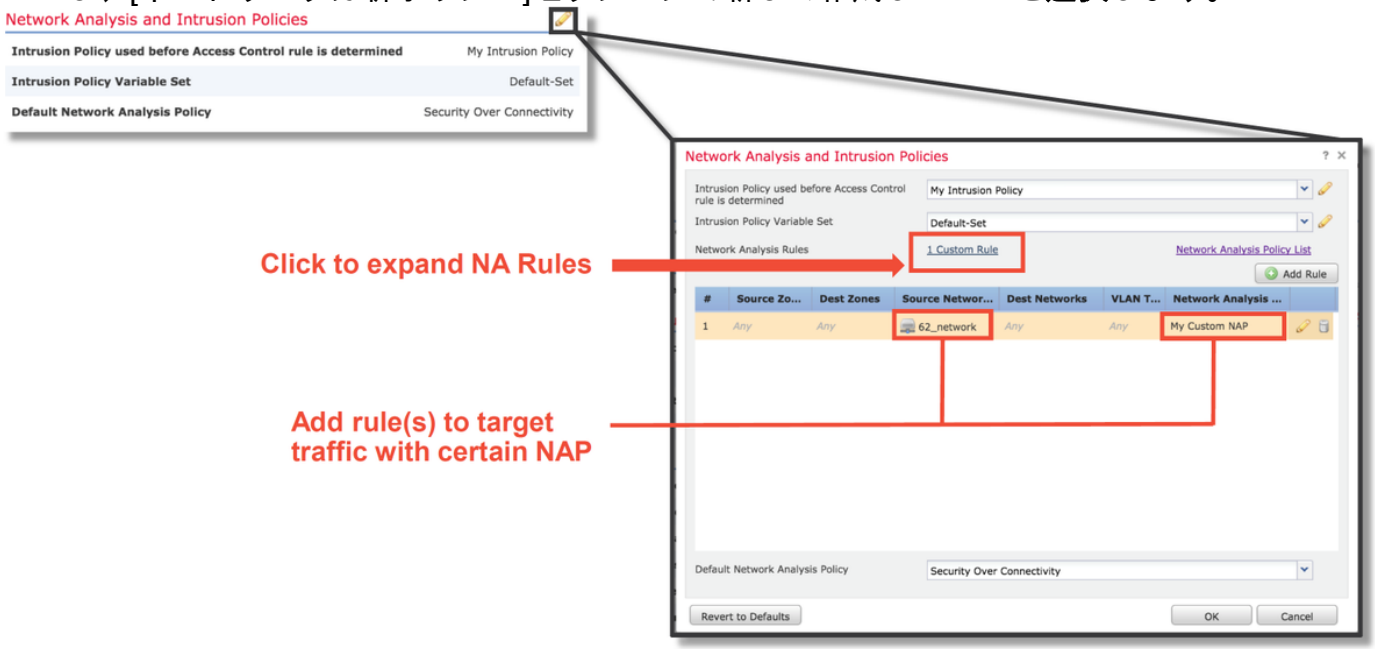
"block" option is enabled in normalize.conf

ターゲットNAPの作成

特定のホストがプリプロセッサイベントをトリガーしている場合は、カスタムNAPを使用して、そのホストとの間のトラフィックを検査できます。カスタムNAPでは、問題の原因となっている設定を無効にすることができます。

これらは、ターゲットNAPを実装するための手順です。

1. この記事の「NAP構成の確認」セクションで説明されている手順に従ってNAPを作成します。
2. アクセスコント**ロールポ**リシーの[詳細設定]タブで、[ネットワーク分析と侵入ポ**リシー]セクションに移動**します。[ルール**の追**加]をクリックし、対象のホストを使用してルールを作成し、[ネットワーク分析ポリシー]セクションで新しく作成したNAPを**選択**します。

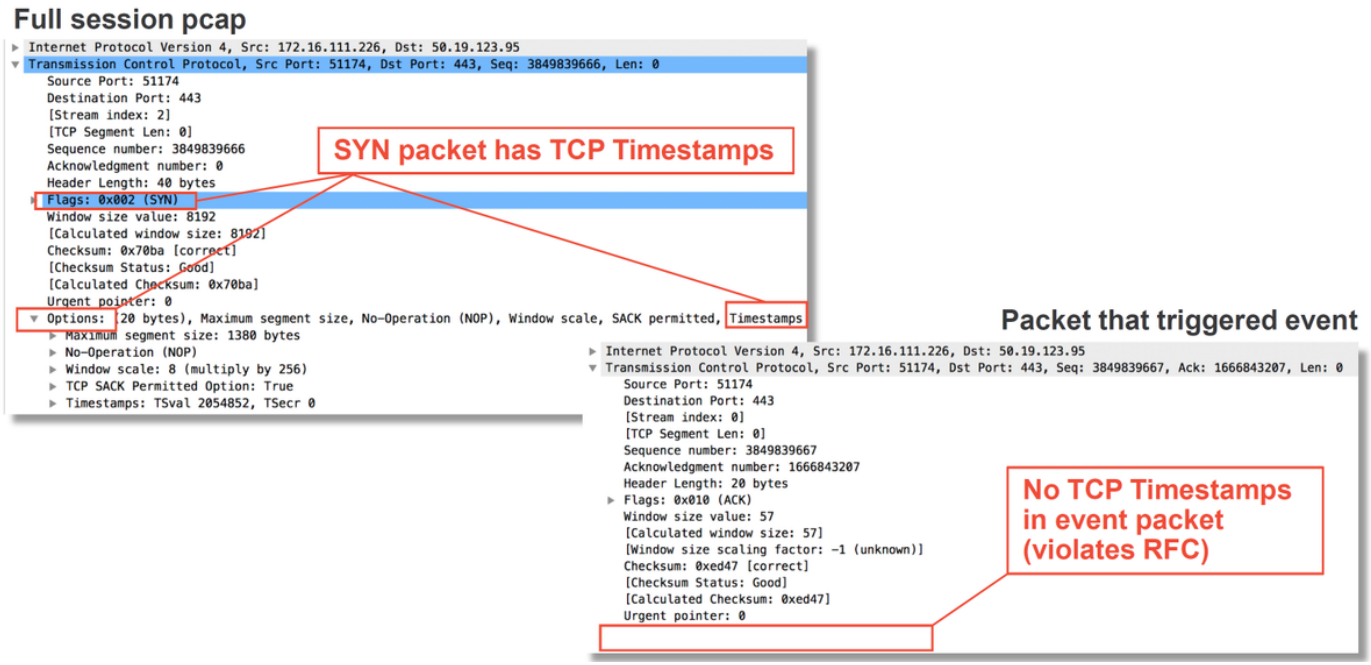


偽陽性分析

プリプロセッサルールの侵入イベントの誤検出のチェックは、ルールの評価に使用されるSnortルール（GIDが1および3である）とは大きく異なります。

プリプロセッサルールイベントに対して誤検出を実行するには、TCPストリーム内の異常を探すために完全なセッションキャプチャが必要です。

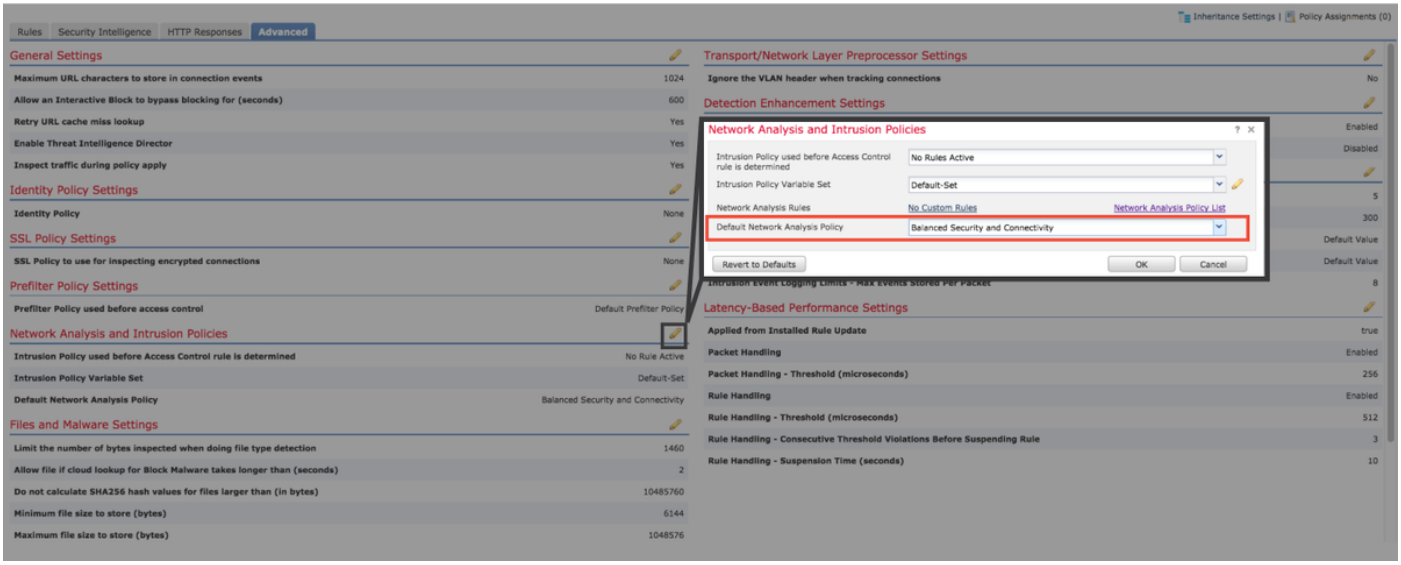
次の例では、ルール**129:14に対してfalse positive分析が実行され**ています。これは、上記の例でトラフィックがドロップされていることを示しています。129:14**は、タイムスタンプが欠落しているTCPストリームを探している**ため、次に示すパケットキャプチャ分析によってルールがトリガーされた理由を明確に確認できます。



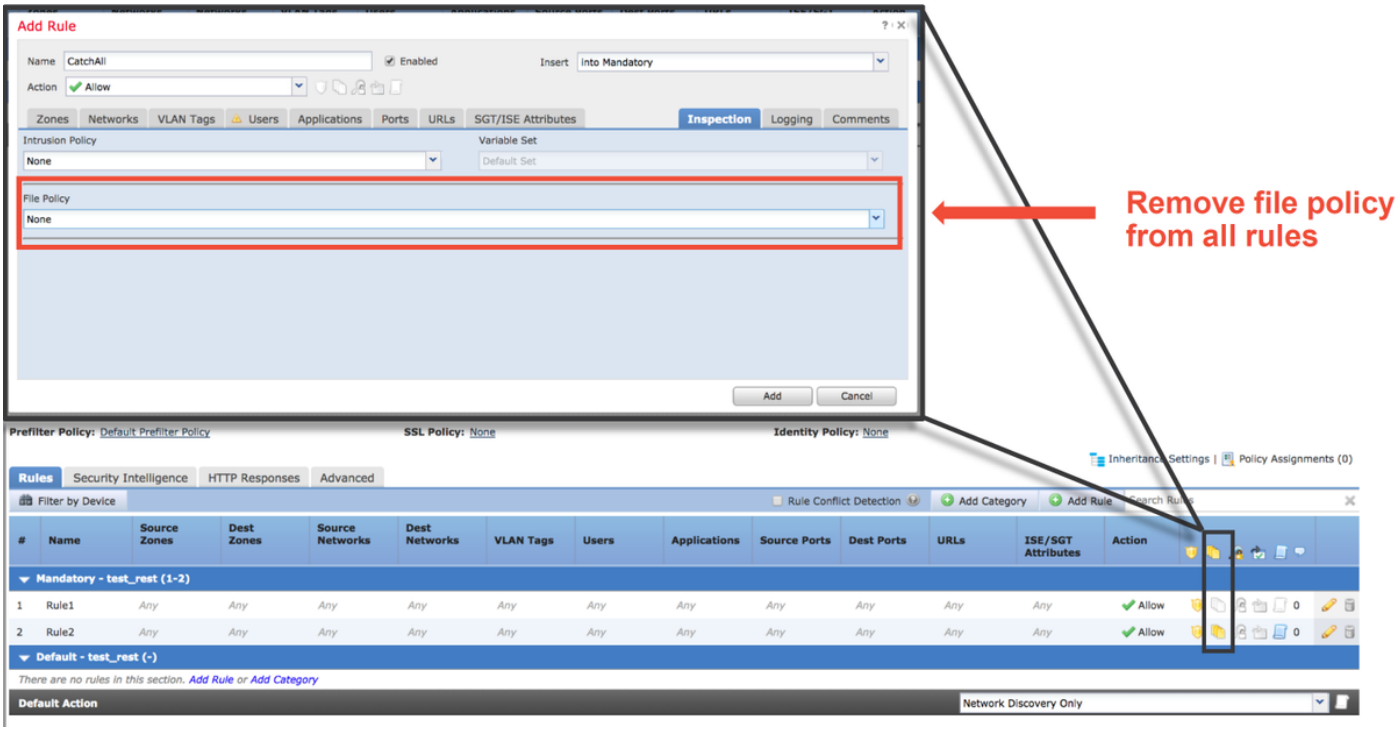
緩和手順

NAPで発生する可能性のある問題を迅速に軽減するには、次の手順を実行します。

- カスタムNAPを使用していて、NAP設定でトラフィックがドロップされているかどうかがわからない場合は、[セキュリティと接続のバランス]または[セキュリティを介した接続]ポリシーで置き換えてみてください。



- [カスタムルール]が使用されている場合は、NAPを上記のいずれかのデフォルトに設定してください
- アクセスコントロールルールでファイルポリシーが使用されている場合は、ファイルポリシーでFMCに反映されないバックエンドのプリプロセッサ設定を有効にできるため、一時的に削除する必要があります。



各プロトコルには異なるプリプロセッサがあり、それらのトラブルシューティングはプリプロセッサに固有である可能性があります。この記事では、各プリプロセッサの設定とトラブルシューティング方法については説明しません。

各プリプロセッサのマニュアルを参照して、各オプションの動作を詳しく調べることができます。これは、特定のプリプロセッサのトラブルシューティングに役立ちます。

TACに提供するデータ

Data	手順
Firepowerデバイスからのファイルのトラブルシューティング	http://www.cisco.com/c/en/us/support/docs

Firepowerデバイスからのフルセッションパケットキャプチャ http://www.cisco.com/c/en/us/support/docs