# Firepowerデータパスのトラブルシューティングフェーズ7:侵入ポリシー

## 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に関する情報や、その他のデータパスのトラブルシューティングに関する記事へのリンクについては、概要記事を参照してください。

この記事では、Firepowerデータパスのトラブルシューティングの7番目のフェーズ、侵入ポリシー機能について説明します。

## 前提条件

- この記事は、侵入ポリシーを実行するすべての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バージョン6.2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い

## 侵入ポリシーフェーズのトラブルシューティング

## 「trace」ツールを使用した侵入ポリシーのドロップの検出（FTDのみ）

システムサポートトレースツールは、FTDコマンドラインインターフェイス(CLI)から実行できます。 これは、Snortの内部の動作に深く掘り下げられる点を除き、アクセスコントロールポリシーのフェーズで説明されているファイアウォールエンジンのデバッグツールに似ています。これは、対象トラフィックで侵入ポリシールールがトリガーされているかどうかを確認するのに役立

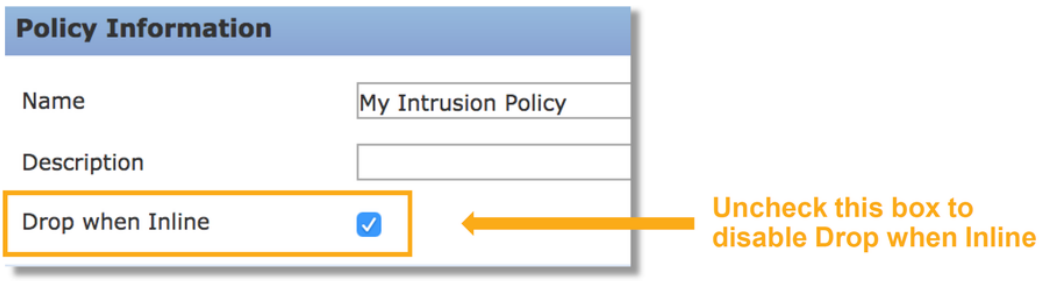
ちます。

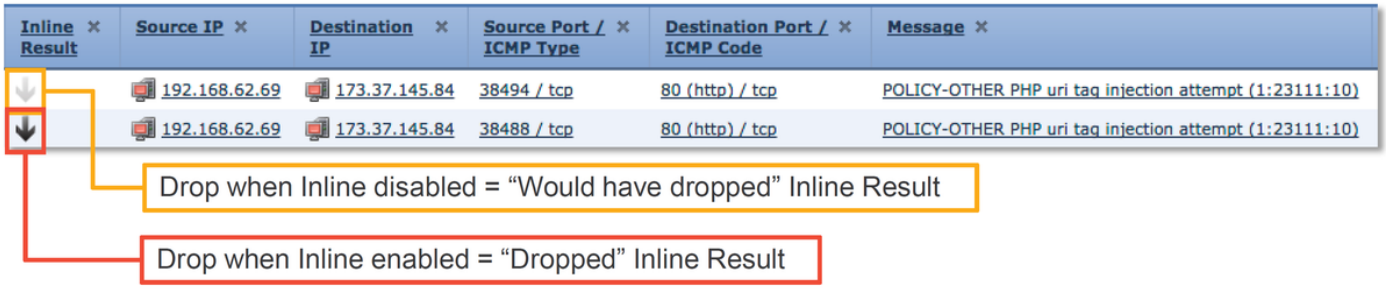
次の例では、IPアドレス192.168.62.6のホストからのトラフィックが侵入ポリシールール(この場合は1:23111)でブロックされています

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

Snortによって適用されたアクションがドロップされていることに**注目してください**。Snortによってドロップが検出されると、その特定のセッションがブラックリストに登録され、追加のパケットもドロップされます。

Snortがドロップアクションを実行できる理由**は、[インラ**イン時にドロップ]オプションが侵入ポリシー内で有効になっているためです。これは、侵入ポリシー内の最初のランディングページで確認できます。Firepower Management Center(FMC)で、**[Policies] > [Access Control] > [Intrusion]に移動**し、該当するポリシーの横にある編集アイコンをクリックします。




「インライン時にドロップ」が無効になっている場合、Snortは問題のパケットをドロップしなくなりますが、侵入イベントで「ドロップされたか」というインライン結果をアラートします。

「インラインでのドロップ」が無効になっている場合、トレース出力には、対象のトラフィック

・ **セッション**に対するドロップ・アクションが表示されます。

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

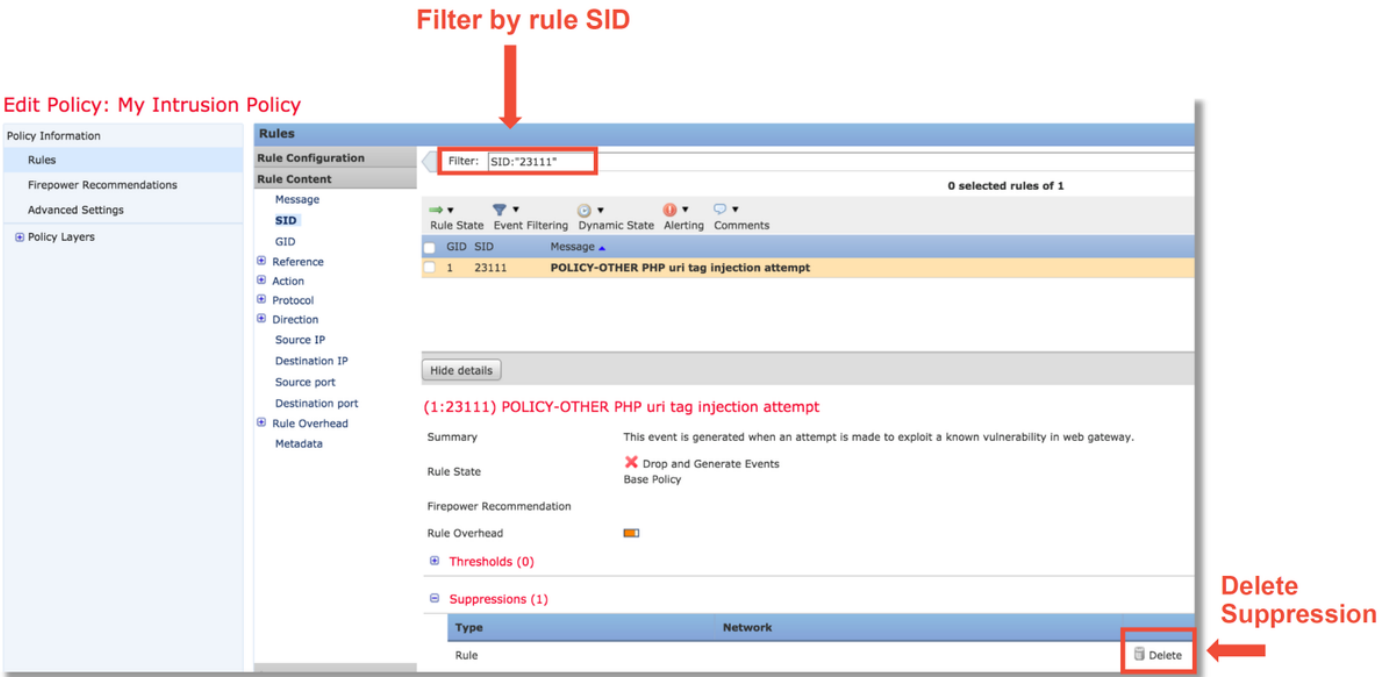
# 侵入ポリシーの抑制の確認

Snortは、侵入イベントをFMCに送信せずに（サイレントドロップ）トラフィックをドロップできます。 これは、抑制を設定することで実現**されます。**侵入ポリシーで抑制が設定されているかどうかを確認するには、次に示すように、バックエンドでエキスパートシェルをチェックします。

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name       : My Intrusion Policy
```

「My Intrusion Policy」という侵入ポリシーには、1:23111ルールの抑制が含まれていることに注意してください。したがって、このルールが原因で、イベントなしでトラフィックをドロップできます。これは、トレースユーティリティが引き続き発生しているドロップを示すため、有用である理由の1つです。

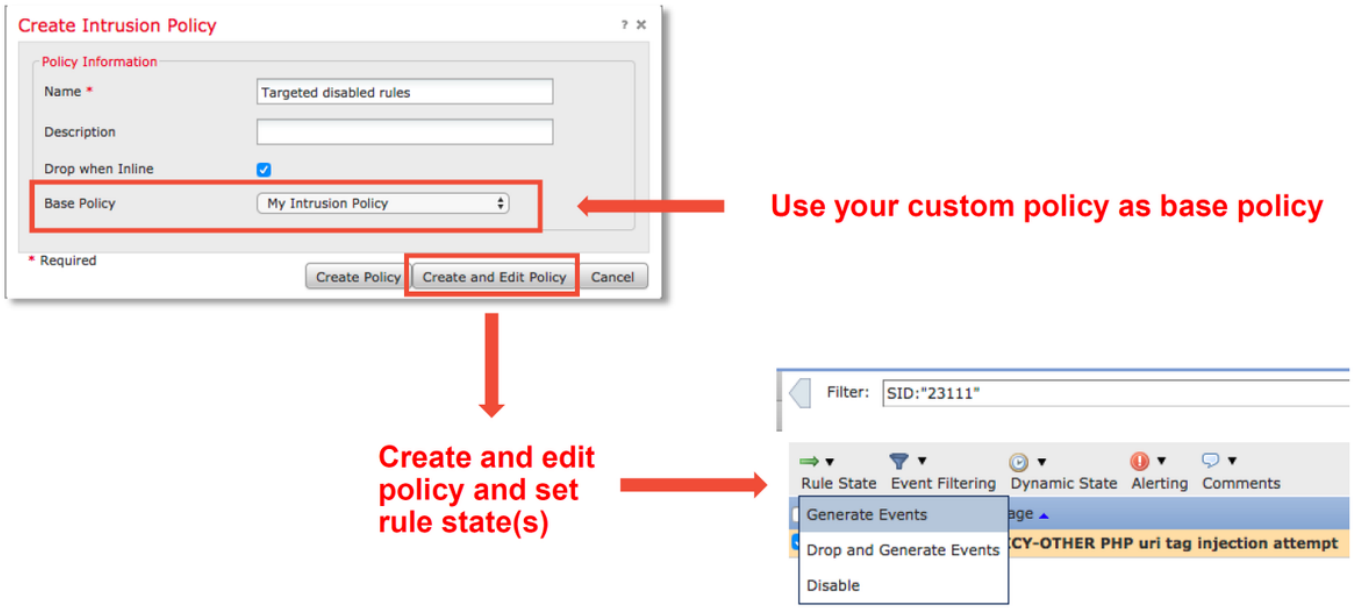
抑制を削除するには、[Intrusion Policy Rules]ビューで該当するルールをフィル**タ**できます。次に示すように、省略を削除するオプションが表示されます。



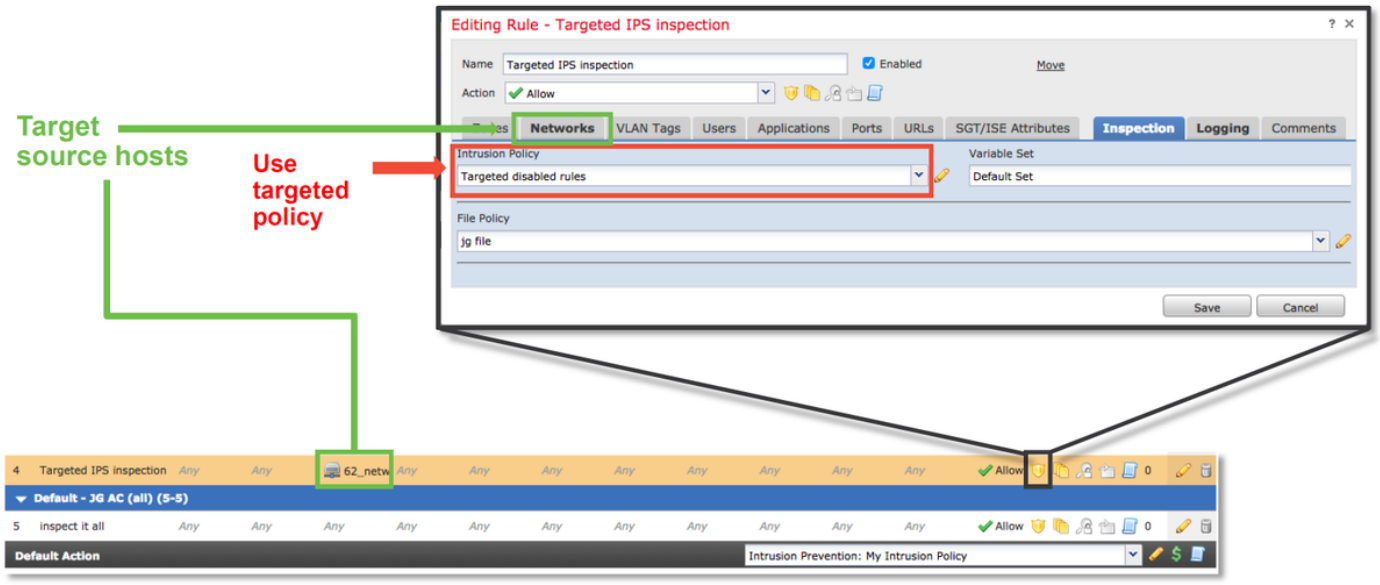

# ターゲット侵入ポリシーの作成

特定の侵入ポリシールールによってトラフィックがドロップされている場合、対象のトラフィックをドロップしたくない場合もありますが、ルールを無効にしたくない場合もあります。ソリューションは、攻撃ルールを無効にして新しい侵入ポリシーを作成し、ターゲットホストからのトラフィックを評価させます。

新しい侵入ポリシーを作成する方法の図を示します([Policies] > [Access Control] > [Intrusion]の下)。




新しい侵入ポリシーを作成した後、新しいアクセスコントロールポリシールール内で使用できます。このルールは、以前に元の侵入ポリシーによってトラフィックがドロップされていた対象のホストを対象にします。



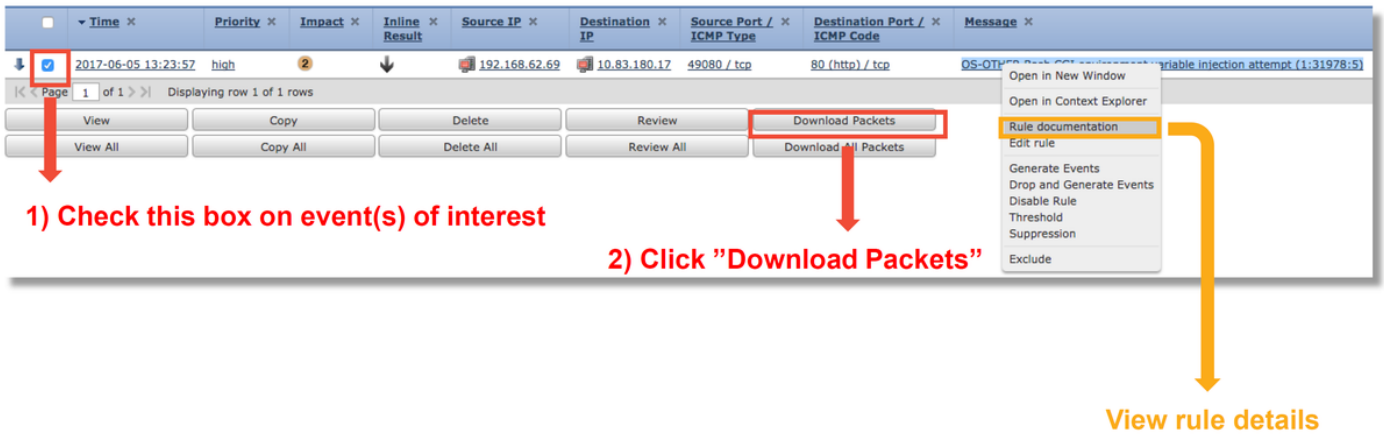

# 誤検出トラブルシューティング

一般的なケースのシナリオは、侵入イベントの誤検出です。誤検出のケースを開く前に確認できる項目がいくつかあります。

1. [Table View of Intrusion Events]ページで、該当するイベントのチェックボックスをオンにします

2. [Download Packets]をクリックして、侵入イベントがトリガーされたときにSnortによってキャプチャされたパケットを取得します。

3. 「メッセージ」列のルール名を右クリックし、「ルールのドキュメント」を選択して、ルールの構文とその他の関連情報を確認します。




次に、上記の例でイベントをトリガーしたルールのルール構文を示します。このルールのFMCからダウンロードしたパケットキャプチャ(PCAP)ファイルに対して検証できるルールの部分は、太字で示されています。

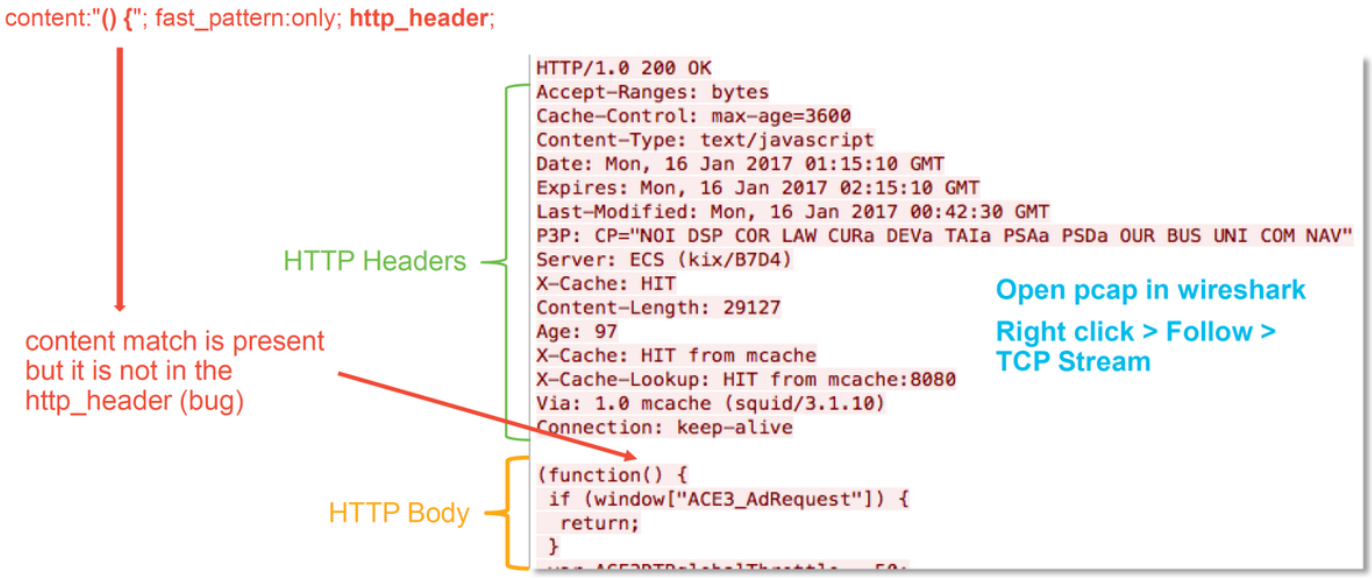
alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg:"OS-OTHER Bash CGI環境変数インジェクションの試み";\
**フロー：to_server，確立；**\
**コンテンツ："() {";fast_pattern：のみ；http_header;**\

**メタデータ：**policybalanced-ipsdrop、policy max-detect-ipsdrop、policy security-ipsdrop、ruleset community、**service http**;\
参照：cve,2014-6271;参照：cve,2014-6277;参照：cve,2014-6278;参照：cve,2014-7169;\
clustype:attempted-admin;\
sid:31978;rev:5;)

これらの最初の手順に従って分析プロセスを実行し、トラフィックがトリガーされたルールに一致する必要があるかどうかを確認できます。

1.トラフィックが一致したアクセスコントロールルールを確認します。この情報は、[Intrusion Events]タブの列の一部として表示されます。
2.上記のアクセスコントロールルールで使用されている変数セットを見つけます。その後、変数セットは、「オブジェクト」(Objects) > **「オブジェクト管理」(Object Management) > 「変数セット」(Variable Sets)で確認できます**
3. PCAPファイル内のIPアドレスが変数と一致していることを確認します(この場合、**$EXTERNAL_NET変数に含まれるホスト**が、**$HOME_NET変数の設定に含まれるホストに接続**します)
4.フローの場合は、フルセッション/接続をキャプチャする必要があります。Snortは、パフォーマンス上の理由により、フロー全体をキャプチャできませんでした。ただし、ほとんどの場合、flow:establishedのルールがルールのトリガー時にセッションが確立されていたため、snortルールでこのオプションを確認するために完全なPCAPファイルが必要ないと仮定しても安全です。しかし、それがトリガーされた理由をより深く理解しておくと役に立つかもしれません。
5.サービス**httpに関**しては、WiresharkのPCAPファイルを見て、HTTPトラフィックと同じかどうかを確認します。ホストに対してネットワーク検出が有効になっていて、以前にアプリケーション「HTTP」が見つかった場合、セッションでサービスが一致する可能性があります。

この情報を念頭に置いて、FMCからダウンロードされたパケットをWiresharkでさらに確認できます。PCAPファイルを評価して、トリガーされたイベントがfalse positiveであるかどうかを判断できます。




上の図では、ルールが検出した内容がPCAPファイルに存在しました – "() {"

ただし、このルールは、パケットのHTTPヘッダーでコンテンツを検出するように指定します – **http_header**

この場合、コンテンツはHTTP本文で見つかりました。したがって、これは誤検出です。ただし、ルールが誤って書かれているという意味では、誤検出ではありません。ルールは正しく、この

場合は改善できません。この例では、Snortのバグが発生し、Snortでバッファが混乱する可能性があります。これは、Snortがhttp_headersを正しく識別していないことを意味します。

この場合、デバイスが実行されているバージョンのsnort/IPSエンジンの既存のバグを確認できます。バグがない場合は、Cisco Technical Assistance Center(TAC)でケースをオープンできます。このような問題を調査するには、完全なセッションキャプチャが必要です。シスコチームは、Snortがその状態になった方法を確認する必要があります。これは、1つのパケットで実行することはできません。

### 真の正の例

次の図は、同じ侵入イベントのパケット分析を示しています。今回は、コンテンツがHTTPヘッダーに表示されるため、イベントは真の正の値になります。


## TACに提供するデータ

| Data | 手順 |
| --- | --- |
| トラフィックを検査する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.c |
| FMCからダウンロードされたパケットキャプチャ | 手順については、 |
| トレース出力など、収集された関連するCLI出力**を確認**します | 手順については、 |

## 次のステップ

侵入ポリシーコンポーネントが問題の原因ではないと判断された場合、次のステップは、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です。

ここをクリックして、最後の記事に進んでください。