特定のSnortインスタンスによって処理されるトラフィックの判別

内容

はじめに

このドキュメントでは、Cisco Firepower Threat Defense(FTD)環境の特定のSnortインスタンスによって処理されるトラフィックを判別する方法について説明します。

前提条件

要件

次の製品に関する知識があることが推奨されます。

- セキュアなFirepower Management Center(FMC)
- セキュアなFirepower Threat Defense(FTD)
- SyslogおよびSNMP
- REST API

使用するコンポーネント

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。このドキュメント内で使用されているデバイスはすべて、クリアな設定（デフォルト）から作業を始めています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

1. CLIコマンドの使用

FTDデバイスのCommand Line Interface（CLI；コマンドラインインターフェイス）を使用すると、Snortインスタンスとそれらが処理するトラフィックに関する詳細情報にアクセスできます。

- このコマンドは、実行中のSnortプロセスの詳細を提供します。

show snort instances

コマンド出力の例を次に示します。

> show snort instances

Total number of instances available - 1 +----------+----------+ | INSTANCE | PID | +----------+----------+ | **1** | **4765** | <<< One instance available and its process ID +----------+----------+

- Snortインスタンスによって処理されるトラフィック統計情報の詳細については、次のコマンドを使用できます。これにより、処理されたパケット数、ドロップされたパケット数、各Snortインスタンスによって生成されたアラート数など、さまざまな統計情報が表示されます。

show snort statistics

コマンド出力の例を次に示します。

> show snort statistics Packet Counters: Passed Packets 3791881977 Blocked Packets 707722 Injected Packets 87 **Packets bypassed (Snort Down) 253403701** <<< Packets bypassed **Packets bypassed (Snort Busy) 0** Flow Counters: Fast-Forwarded Flows 294816 Blacklisted Flows 227 Miscellaneous Counters: Start-of-Flow events 0 End-of-Flow events 317032 Denied flow events 14230 Frames forwarded to Snort before drop 0 Inject packets dropped 0 TCP Ack bypass Packets 6412936 TCP Meta-Ack Packets 2729907 Portscan Events 0 Packet decode optimized 21608793 Packet decode legacy 6558642

show asp inspect-dp snort

コマンド出力の例を次に示します。

> show asp inspect-dp snort

SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- ----- ---------- ---------- ---------- -------- 0 16450 8% (7%| 0%) 2.2 K 0 READY 1 16453 9% (8%| 0%) 2.2 K 0 READY 2 16451 6% (5%| 1%) 2.3 K 0 READY 3 16454 5% (5%| 0%) 2.2 K 1 READY 4 16456 6% (6%| 0%) 2.3 K 0 READY 5 16457 6% (6%| 0%) 2.3 K 0 READY 6 16458 6% (5%| 0%) 2.2 K 1 READY 7 16459 4% (4%| 0%) 2.3 K 0 READY 8 16452 9% (8%| 1%) 2.2 K 0 READY **9 16455 100% (100%| 0%) 2.2 K 5 READY** <<<< High CPU utilization 10 16460 7% (6%| 0%) 2.2 K 0 READY -- ----- ---------- ---------- ---------- ---------- Summary 15% (14%| 0%) 24.6 K 7

-

Firepower Management Center(FMC)の使用

FMCを通じてFTDデバイスを管理している場合、Webインターフェイスからトラフィックと Snortインスタンスに関する詳細な洞察とレポートを取得できます。

- モニタリング

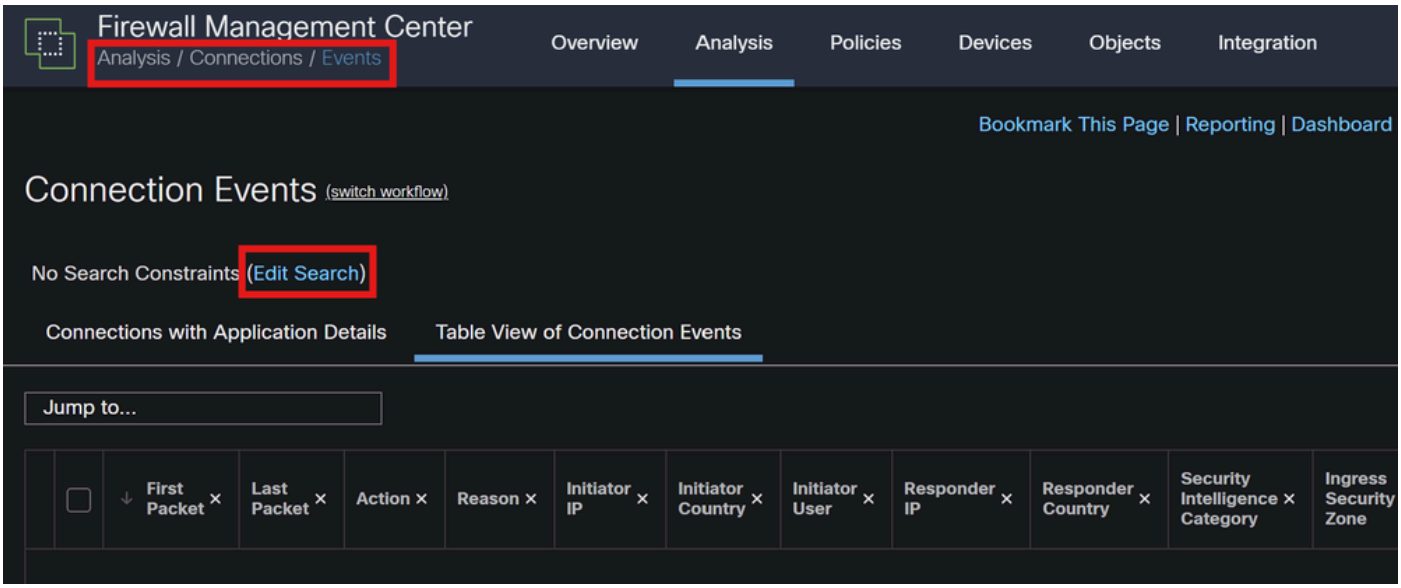
FMCダッシュボード：ダッシュボードに移動し、Snortインスタンスを含むシステムステータスの概要を確認できます。

ヘルスモニタリング：ヘルスモニタリングセクションでは、処理トラフィックを含むSnortプロセスに関する詳細な統計情報を取得できます。

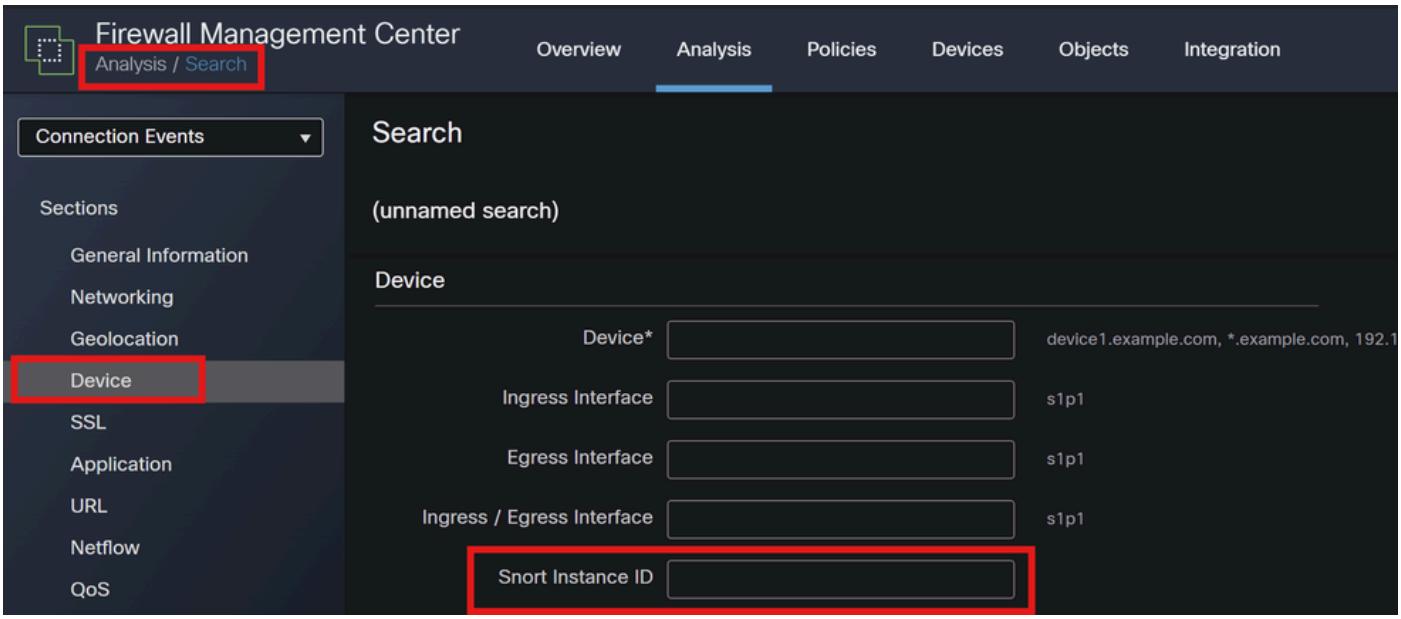
- 分析

分析：**分析>接続イベントに移動します。**

フィルタ：フィルタを使用して、対象の特定のSnortインスタンスまたはトラフィックにデータを絞り込みます。



接続イベント



*Snort*インスタンス*ID*

- **SyslogおよびSNMPの使用**

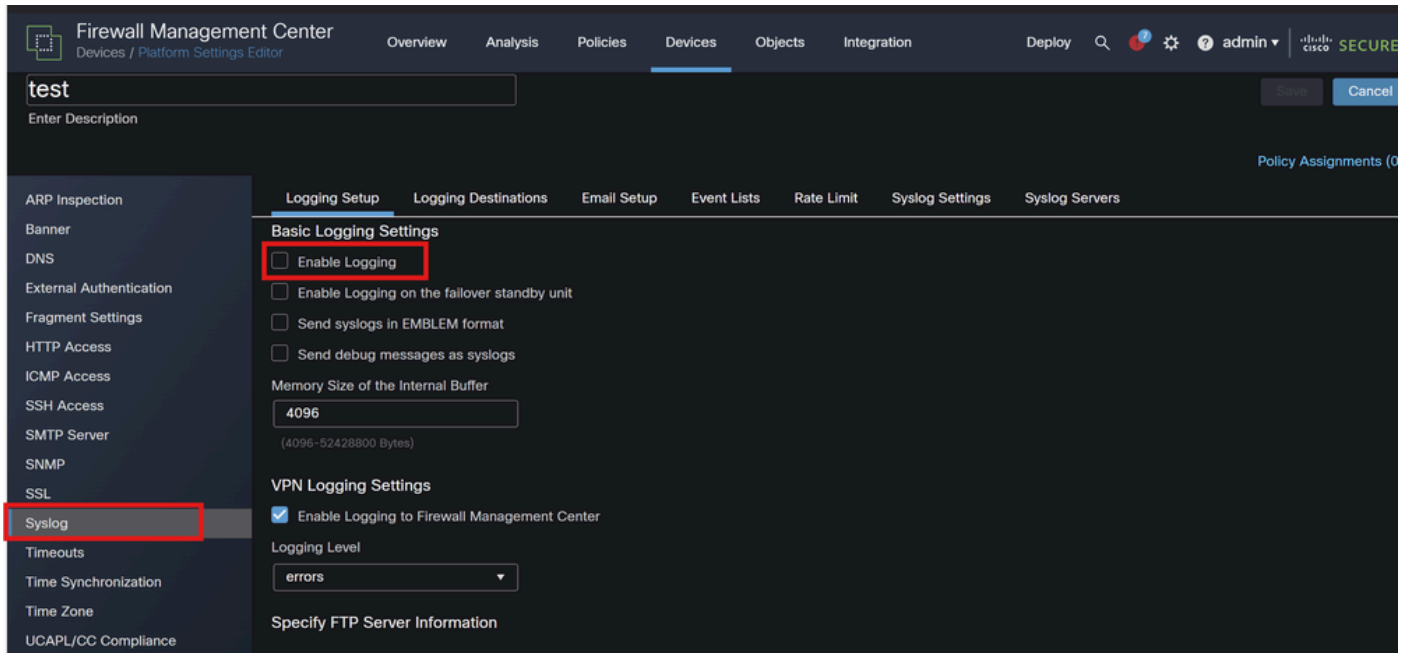
syslogメッセージまたはSNMPトラップを外部モニタリングシステムに送信するようにFTDを設定し、そこでトラフィックデータを分析できます。

- Syslogの設定

デバイス：FMCで、デバイス>プラットフォーム設定に移動します。

ポリシーの作成または編集：適切なプラットフォーム設定ポリシーを選択します。

Syslog:Snortアラートと統計情報を含めるようにsyslogを設定します。

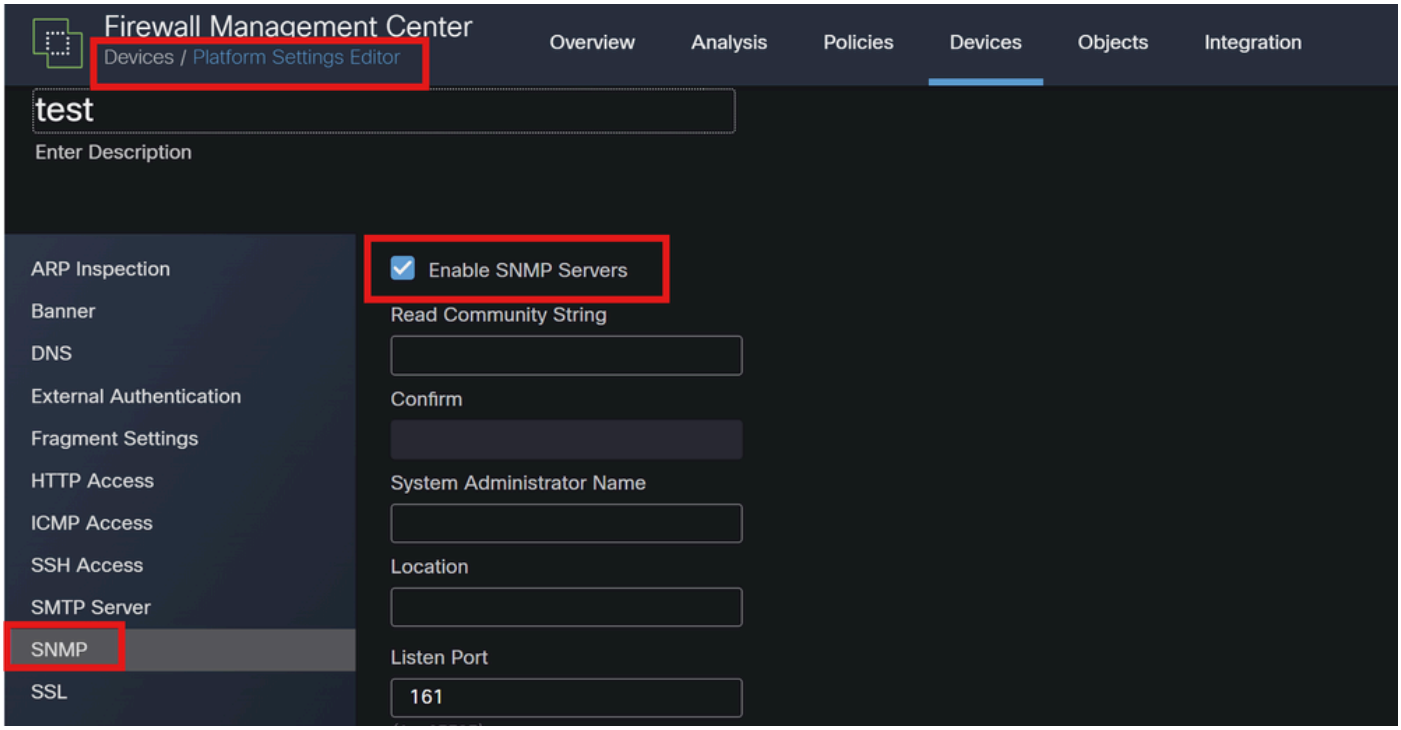


*Syslog*の設定

- SNMP の設定（ SNMP Configuration ）

SNMP設定：syslogと同様に、**Devices** > **Platform Settings**でSNMPを設定します。

Traps:Snortインスタンスの統計情報に対して、必要なSNMPトラップが有効になっていることを確認します。



SNMP の設定（ *SNMP Configuration* ）

4. カスタム・スクリプトの使用

上級ユーザは、FTD REST APIを使用してSnortインスタンスに関する統計情報を収集するカスタムスクリプトを作成できます。このアプローチでは、スクリプトとAPIの使用方法に精通している必要があります。

- REST API

APIアクセス：FMCでAPIアクセスが有効になっていることを確認します。

APIコール：適切なAPIコールを使用して、Snortの統計情報およびトラフィックデータを取得します。

これにより、特定のSnortインスタンスで処理されるトラフィックを判別するために解析および分析できるJSONデータが返されます。

これらの方法を組み合わせることで、Cisco FTD導入環境の各Snortインスタンスで処理されるトラフィックを包括的に把握できます。

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。