IPS のインライン TCP セッション トラッキング モード

目次

概要

このドキュメントでは、侵入防御システム（IPS）アプライアンスのインライン TCP セッション トラッキング機能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。

- インライン インターフェイスを使用して設定されている IPS 4200 シリーズ アプライアンス。
- TCP プロトコルとトラフィック フローの知識。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- IPS 4270（ソフトウェア リリース 7.1(7)）

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

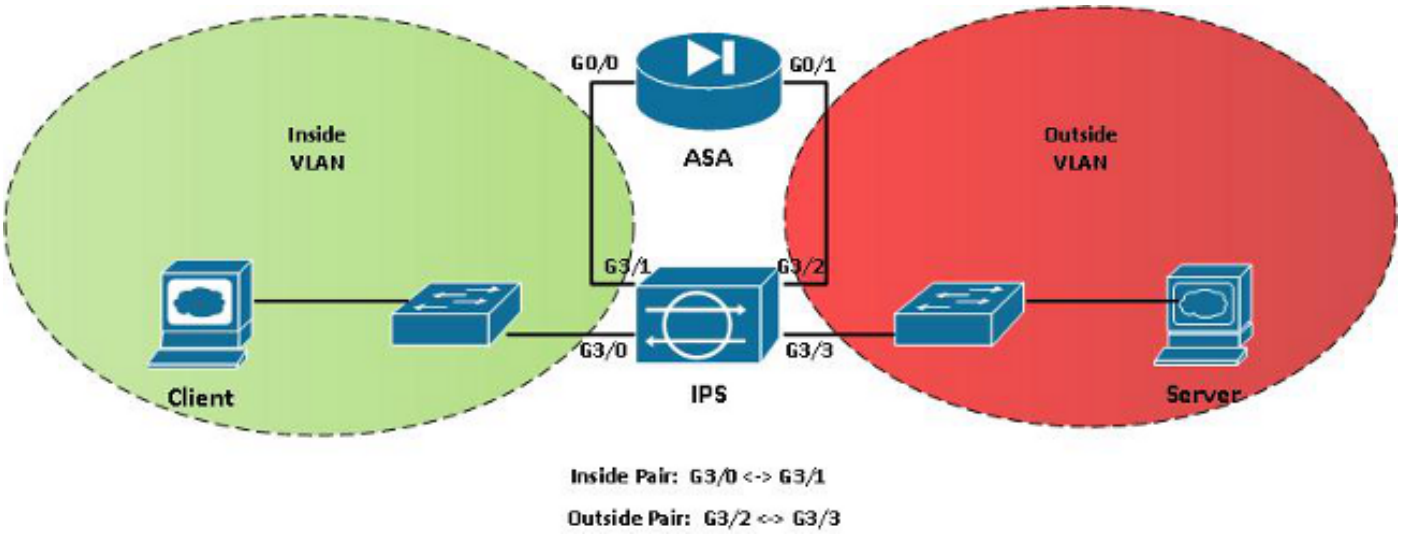
表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

特定のインライン IPS 導入シナリオでは、TCP ストリームからのパケットは、Normalizer エンジンにより 2 回検出されます。この結果、不適切なストリームの追跡が原因でドロップが発生します。 通常この状況が発生するのは、トラフィックが複数の仮想ローカル エリア ネットワーク（VLAN）、または 1 つの仮想センサーによりモニタされるインターフェイス ペアを経由してルーティングされる場合です。 また、いずれかの方向のトラフィックがそれぞれ異なる VLAN またはインターフェイスから受信された場合に、ストリームを適切に追跡するために非対称トラフィックをマージできるようにする必要があることから、問題がより複雑化します。

ネットワーク図



問題

このネットワーク トポロジでは、内部ネットワーク上のクライアントが外部ネットワークのサーバへの HTTP 接続を開始します。 これらのネットワーク セグメントはいずれも、適応型セキュリティ アプライアンス（ASA）ファイアウォールにより分離されています。 この設計では、1 台の IPS アプライアンスが 2 つのインライン インターフェイス ペアを使用して内部および外部両方の VLAN に接続するように設定されています。 クライアントがサーバとのセッションを開始すると、TCP SYN（同期）パケットが、IPS と ASA を通過する次のパス（アウトバウンド ストリーム）を移動します。

クライアント > IPS G3/0 > *vs0* > IPS G3/1 > ASA G0/0 > ASA G0/1 > IPS G3/2 > *vs0* > IPS G3/3 > **サーバ**

クライアントから送信された TCP SYN は、アウトバウンド ストリームの後、パケットが ASA の内部インターフェイスへ向かって内部インターフェイス ペアを通過すると、**vs0** 仮想センサーにより検出されます。また、これらのパケットが Web サーバへ向かって外部インターフェイス ペアを通過するときに再度検出されます。 対称的なシナリオでは、Web サーバからの SYN ACK（肯定確認応答）とその後続パケットのリターン パスで同様の状況が発生します。 IPS がストリームを 1 つの TCP 接続に結合しようとすると、接続ですべてのパケットの重複が検出され、その結果 Normalizer が混乱し、パケットがドロップされます。 IPS でこの状況が発生しているかどうかは、**show stat virt** コマンドの出力に、大量の 1330 TCP Normalizer シグニチャが起動しており、また大量のパケットと接続が変更および拒否されていることが示されていることで確認できます。

解決策

このような状況を解決するには、[Inline TCP Session Tracking Mode] オプションを使用できます。 次の 3 種類のモードを設定できます。

1. **Virtual Sensor（デフォルト設定）**：クライアント パケットが 1 つのインライン ペアで検出され、サーバ パケットが 2 番目のインターフェイス ペアで検出される非対称導入状況をモニタします。 接続の両端を確認するには、2 つのインターフェイス ペアをまとめてモニタする必要があります。
2. **Interface and VLAN**：これは、このドキュメントに示すトポロジの例（複数のインライン インターフェイス ペアが同一の仮想センサーに割り当てられているトポロジ）に対する回避策です。 このオプションが有効な場合、TCP 接続は複数のペアを通過し、これにより Normalizer がインライン ペアごとに個別に TCP セッションを追跡できます。
3. **VLAN Only**：これは、最初の 2 つのオプションの非常に珍しい組み合わせであり、複数の非対称ネットワークの組み合わせをモニタするときに使用されます。 左側のインターフェイス ペアの **VLAN 1** にはクライアント パケットがあり、右側のインターフェイス ペアの **VLAN 1**（サーバ パケットがある VLAN）と結合する必要があります。 この場合、すべてのインターフェイス ペアにわたってトラフィックが集約されますが、VLAN ごとに分離されます。 たとえば、すべてのインターフェイスの VLAN 1 パケットがまとめられ、 すべてのインターフェイスの VLAN 2 パケットがまとめられますが、VLAN 1 パケットと VLAN 2 パケットが TCP セッション追跡のためにまとめられることはありません。

上記のトポロジ例では、2 通りの方法で問題を解決できます。

解決策 1

各インライン インターフェイス ペアを専用の仮想センサーに移動する。 たとえば、1 つのペアを **vs0** に移動し、別のペアを **vs1** に移動します。 インライン ペアの数が 4 未満の場合、一般にこの方法が推奨されます（プラットフォームでの仮想センサー制限数が 4 であるため）。 Normalizer は重複ストリームを 2 つの個別の接続として扱います。

解決策 2

インライン TCP セッション トラッキング モードを [Interface and VLAN] に設定します。 インライン ペアの数が 4 を超える場合、一般にこの方法が推奨されます。これは、複数のインライン ペアを 1 つの仮想センサーに強制的に配置するためです。 Normalizer は異なるインライン ペアのパケットを、同一仮想センサー内の完全に異なる接続として扱います。

設定

インライン インターフェイス ペア別に仮想センサーを切り離すための設定を次に示します。

```
IPS4510-01# conf t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Inside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# virtual-sensor vs1

IPS4510-01(config-ana-vir)# logical-interface To-ASA-Outside subinterface-number 0

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

IPS4510-01(config)# exit
```

インターフェイスと VLAN の設定を次に示します。

```
IPS4510-01# config t

IPS4510-01(config)# service analysis-engine

IPS4510-01(config-ana)# virtual-sensor vs0

IPS4510-01(config-ana-vir)# inline-tcp-session interface-and-vlan

IPS4510-01(config-ana-vir)# exit

IPS4510-01(config-ana)# exit

Apply Changes?[yes]: yes

Warning: Change of TCP session tracking mode will not take effect until restart.

IPS4510-01(config)# exit

IPS4510-01# reset
```

確認

- **show stat virt | b TCP Normalizer stage statistics** コマンドを使用し、TCP Normalizer で非ゼロの [Dropped]、[Duplicate]、[Denied]、または [SendAck Packets Sent] 統計を確認します。
- **show stat virt | b Per-Signature SigEvent count** コマンドを使用して、起動された 1330 シグニチャを、前述のコマンドからの TCP Normalizer 統計と組み合わせて確認します。

関連情報

- Cisco Intrusion Prevention System Sensor CLI コンフィギュレーション ガイド for IPS 7.0 - インライン TCP セッション トラッキング モード
- Cisco Intrusion Prevention System Manager Express コンフィギュレーション ガイド for IPS 7.1 - インライン TCP セッション トラッキング モード
- テクニカルサポートとドキュメント - Cisco Systems