目次

概要

この資料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 トラッキング機能を説明していたものです。

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 インターフェイスで設定される IPS 4200 シリーズ アプライアンス。
- TCP プロトコルおよびトラフィックフローのナレッジ。

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。

- ソフトウェア リリース 7.1(7)との IPS 4270

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。

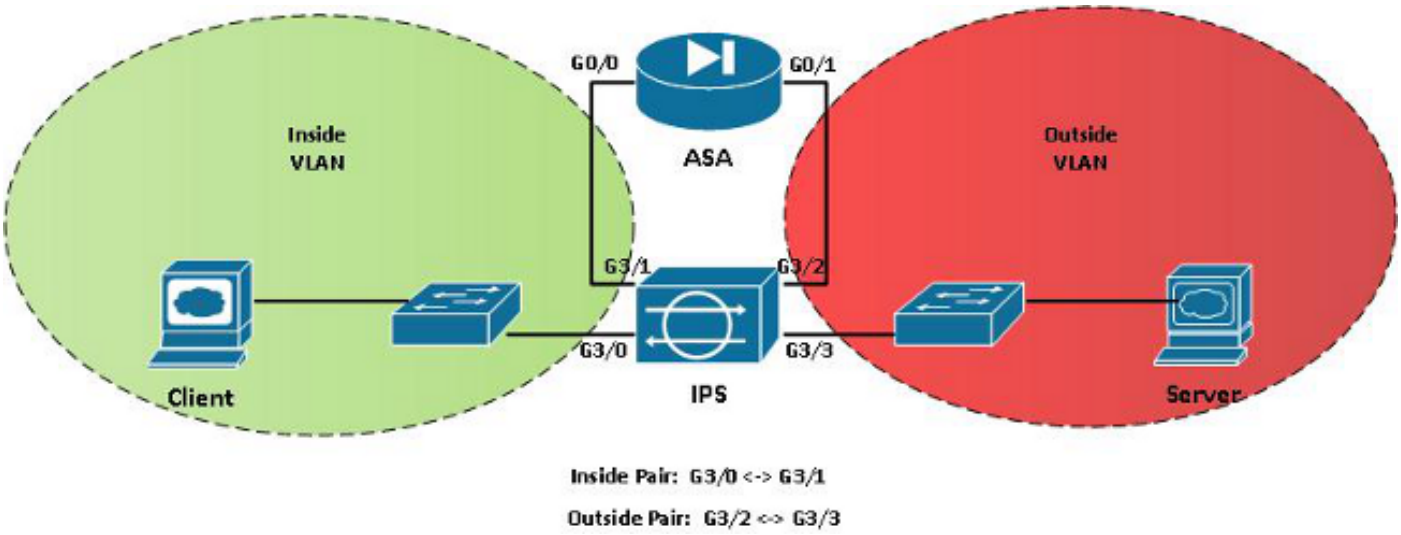
表記法

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

ある特定のインライン IPS デプロイメントシナリオでは、TCP ストリームからのパケットはノーマライザー エンジンによって二度見られる場合があります不適当なストリーム トラッキングが理由でドロップという結果に終る。 この状況は一般的に トラフィックが複数のバーチャルLAN（VLAN）または単一 仮想 なセンサーによって監察されるインターフェイス ペアによってルーティングされるとき経験されます。 この問題は非対称的なトラフィックがトラッキングする適切なストリームのためにマージするようにする必要によって更に方向のためのトラフィックが異なるVLAN かインターフェイスから受信されるとき複雑になります。

ネットワーク図



問題

このネットワーク トポロジでは、内部ネットワークのクライアントは外部ネットワークのサーバに HTTP接続を始めます。 ネットワークセグメントは両方とも適応性があるセキュリティ アプライアンス モデル（ASA）ファイアウォールで分かれます。 この設計では、単一 IPS アプライアンスは 2 組のインライン インターフェイス ペアとの両方の内部および外部 VLAN に叩くために設定されます。 クライアントがサーバにセッションを始めるとき、TCP SYN（同期して下さい）パケットは IPS および ASA を通してこのパス（送信 ストリーム）を選択します:

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**

パケットが ASA の内部インターフェイスの方の内部インターフェイス ペアをおよび横断すると同時に送信 ストリームが **vs0** 仮想 なセンサーによって、クライアントが送信 する TCP SYN 見られた後パケットが Webサーバの方の outside インターフェイス ペアを横断する時再度。 対称シナリオでは、同じ状況は SYN ACK（確認応答）のリターンパスおよび後続パケットに Webサーバから発生します。 IPS が単一 TCP 接続にストリームを結合するように試みるとき混同した

ノーマライザーおよび破棄された パケットという結果に終る接続の各パケットの重複は観察されます。 IPS がこの状況に遭遇するかどうか確認するために、**提示統計 virt** コマンドの出力は起動する、また多数の修正され、拒否されたパケットおよび接続示したものです多数の 1330 の TCP ノーマライザ シグニチャ。

解決策

モード オプションを**トラッキングするインライン TCP セッションが**これのような状況を克服するのに利用することができます。 設定することができる 3 つの可能性のあるモードがあります:

1. **仮想 なセンサー (デフォルト設定)** -サーバ パケットは第 2 インターフェイス ペアで見られるが、クライアント パケットが 1 つのインライン ペアで見られる非対称的な配備状況の監視。 2 つのインターフェイス ペアは接続の両側を見るために一緒に監視する必要があります。
2. **インターフェイスおよび VLAN** -これは 2つ以上のインライン インターフェイス ペアが同じ仮想 なセンサーに割り当てられるこの資料で示されているトポロジーの例へ回避策です。 有効に されてこのオプションが TCP 接続はノーマライザーが各々のインライン ペアのために TCP セッションを独自にトラッキングするようにする複数のペアを横断するかもしれません。
3. **VLAN だけ**-これは最初の 2 つのオプションの非常にまれな組み合せで、複数の非対称的なネットワークの組み合せを監視するために使用されます。 左インターフェイス ペアの **VLAN 1 に**クライアント パケットがあり、サーバ パケットがある右のインターフェイス ペアの **VLAN 1** と結合する必要があります。 この場合、トラフィックはすべてのインターフェイス ペアを渡って集約されますが、VLAN で分離します。 たとえば、すべてのインターフェイスを渡る VLAN 1 パケットは一緒に入れられます; すべてのインターフェイスからの VLAN 2 パケットは一緒に入れられますが、VLAN 1 および VLAN 2 パケットは TCP セッション トラッキングのために決して一緒に入れられません。

上記のトポロジーの例に関しては、問題が解決されますこと 2 つの方法があります:

解決策 1

自身の仮想 なセンサーに各々のインライン インターフェイス ペアを移動して下さい。 たとえば、**vs0** の 1 つのペアおよび **vs1** の 1 ペア。 この方式は通常 4 つのインライン ペアより小さいとき推奨されます (4 台の仮想 なセンサーのプラットフォーム制限が理由で)。 ノーマライザーは 2 個別の接続として重複したストリームを扱います。

解決策 2

インターフェイスするためにモード**および VLAN を**トラッキングするインライン TCP セッションを設定して下さい。 この方式は、単一 仮想 なセンサーに複数のインライン ペアを置かせる 4 つ以上のインライン ペアがあるとき推奨されます。 ノーマライザーは同じ仮想 なセンサー内の全く異なる接続として異なるインライン ペアのパケットを処理します。

設定

インライン インターフェイス ペアごとの仮想 なセンサーを分ける設定はここにあります:

インターフェイスおよび VLAN のための設定はここにあります:

確認

- **提示統計 virt を**使用して下さい **| 廃棄される**のための **b TCP ノーマライザ段階 statistics コマンド**およびリビュー、**複写**、**否定されて**、か **SendAck パケットは** TCP ノーマライザのゼロ以外の統計情報を**送信 しました**。
- **提示統計 virt を**使用して下さい **|** 前のコマンドからの TCP Normalier 統計情報と共に起動 した 1330 のシグ二チャのための **b 毎シグ二チャ SigEvent 数**コマンドおよび確認。

関連情報

- IPS 7.0 のための Cisco 侵入防御システム センサー CLI コンフィギュレーション ガイド-モードをトラッキングするインライン TCP セッション
- IPS 7.1 のための Cisco 侵入防御システム マネージャ Express コンフィギュレーション ガイド-モードをトラッキングするインライン TCP セッション
- テクニカルサポートとドキュメント - Cisco Systems