目次

概要

FireSIGHT システムは監視されたネットワークセグメントの新しいホストを検出するときイベントを生成します。それはより少ない自信をもってオペレーティング システムかサービスを、または不正確に検出するかもしれません。 イベントが *未知数*としてマークされる場合、トラフィックが分析されるが、オペレーティング システムは既知フィンガープリントのうちのどれも一致することを意味します。 この資料はチェックリストおよび推奨事項を*未知*イベントを最小に する提供したものです。

前提条件

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- FireSIGHT システム、FirePOWER アプライアンスおよび NGIPS バーチャル アプライアンス
- ソフトウェア バージョン 5.2 以降

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。

トラブルシューティング チェックリスト

FireSIGHT システムが保留中または UNKNOWN 状態にあるイベントを生成すれば、この問題を解決し始めるように下記のステップに従うことができます:

> **注** *未確認*ホストは*不明な* ホストと同じではないです。 *未確認*ホストはオペレーティング システムを識別するためにシステムがまだ十分な情報を収集していないホストです。

チェックリストを解決して下さい	推奨事項
1. FireSIGHT Management Center でどんな VDB バージョンがインストールされていますか。	最新の VDB バージョンにトールされる最新バージョ
2. FireSIGHT ライセンスのホスト制限とは何か。 FireSIGHT によって何ホストが検出するか。	ホスト制限が超過する場合。 ホスト制限が達したと
3. FireSIGHT 管理対象装置から何ホップがホストありますか。	より高いデバイスからホスはトラフィック修正され、
4. ホストと管理対象装置間のあらゆるインライン デバイスがありますか。	インライン デバイスの存オリジナル TCP をかまた報を修正できます。
5. 管理対象装置はあらゆる非同期 ルーティング ネットワークのトラフィックをモニタしていますか。	FireSIGHT システム モニば。
6. あらゆるサービスのために使用されるあらゆる標準外ポートがありますか。 標準外ポートを当たるために設定されるあらゆるカスタム デコーダがありますか。	不適当に設定されたカス

追加データ

すべての上記の推奨事項が続かれるが、まだ不明が、迄またはあるか場合見つけられた未確認ホスト次の data&colon を分析する必要があります;

1. 完全なセッショントラフィック

不正確に識別されるか、または未知か保留中としてマークされるホストからの完全なセッショントラフィック。

2. ファイルのトラブルシューティング

FireSIGHT Management Center および管理対象装置からのファイルのトラブルシューティング。管理対象装置の位置を示すネットワークマップかトポロジーは有用です。

3. パケットキャプチャ（PCAP）

管理対象装置によって受信されるパケットはホストで送信されたパケットと異なるかもしれません。 それはホストと管理対象装置の間で存在 するインライン デバイスを修正するあらゆるヘッダ起こります。 従って、2 PCAPs からのヘッダを比較することを割り当てる両端からの PCAP をキャプチャ することがより適切-ホストおよび管理対象装置です。 パケット間のどのミスマッチによりサービスまたはホストの misidentification を引き起こす場合があります。