Secure Network Analytics仮想アプライアンスネットワークインターフェイスの設定の制限

内容

問題

Secure Network Analytics(SNA)とNon Data Storeの導入シナリオを評価していました。ここでは、Flow Collectorに仮想化プラットフォーム経由で割り当てられた複数のネットワークインターフェイスがあります。

具体的には次のような疑問が生じました。

- 仮想フローコレクタが2つのNICで動作できるかどうか（1つはSNA内部通信用、もう1つはNetFlow受信用）
- 内部通信セグメントがインターネットにアクセスできない場合に、脅威フィードを取得するために複数のNICを使用して仮想マネージャアプライアンスを設定できるかどうか

環境

- 7.6.0より前のSecure Network Analytics(Stealthwatch)バージョン
- すべてのSNAコンポーネント（マネージャ、フローコレクタ）の仮想アプライアンスバージョン
- 分離された内部通信とNetFlow受信セグメントを持つネットワークアーキテクチャ

解決方法

Cisco Secure Network Analytics(SNA)Flow Collectorは2つのNICインターフェイスで導入でき、こ

の動作はラボ環境で検証されています。

1. 管理アクセスとNetFlow受信の2つのインターフェイス

- フローコレクタは、管理アクセス用の1つのインターフェイスと、NetFlow受信専用の2番目のインターフェイスで構成できます。
- ただし、管理アクセスはいずれかのインターフェイス（管理またはNetFlow）を介して到達可能なままです。 現在、インターフェイスを目的に限定するオプションはありません。

2. 2つのインターフェイス：NetFlow受信と脅威フィード受信

- 脅威フィードのアップデートは、Flow Collectorからのインターネットアクセスを使用して取得されます。
- 管理インターフェイスIPがインターネットに直接アクセスできない場合は、2番目のインターフェイスが引き続きNetFlowを受信している間も、フローコレクタで利用可能なプロキシオプションをこの要件を満たすように設定できます。

範囲に関する重要な注意事項
どちらのシナリオもラボのセットアップで完全に検証されたものであり、『SNA設計ガイド』には記載されていません。したがって、これらは公式に公開された設計の推奨事項ではなく、実際の動作として扱う必要があります。このような導入を計画しているお客様は、まず自社のテスト環境で検証することをお勧めします。

原因

この動作は、Secure Network Analytics Flow Collectorアプライアンスアーキテクチャの設計に基づいています。アプライアンスは追加のNICの割り当てをサポートし、プライマリインターフェイスが管理に使用されている間は、そのセカンダリインターフェイスでテレメトリ(NetFlow)を受信できます。ただし、アプライアンスソフトウェアでは、すべての設定済みおよびアドレス指定インターフェイスにバインドされた管理サービス（アプライアンス管理UI、SSH、およびSNAアプライアンス間通信）が実行され、インターフェイスごとのサービスバインディングやアクセスコントロールオプションは公開されません。その結果、管理アクセスはどちらのNICからも到達可能であり、その目的で指定されたインターフェイスに制限できません。

同様に、脅威フィードの取得は特定のNICに関連付けられていません。更新プロセスは単にアプライアンスのルーティングテーブルに基づいてアウトバウンド接続を開始するので、インターネットへの有効なパスを持つインターフェイスは要求に対応します。管理インターフェイスにインターネットへの直接的な到達可能性がない場合は、アプライアンス管理内のプロキシ設定オプシ

ョンが、承認されたプロキシ・サーバーを介してアウトバウンド要求をリレーします。これにより、インターフェイスの役割を変更しなくても、脅威フィードを正常に更新できます。

マルチNICフローコレクタの導入とインターフェイスの役割の分離については『Secure Network Analytics設計ガイド』では取り上げていないため、この動作はサポート対象外ではなく文書化されておらず、調査結果はラボでの検証のみに基づいています。

関連コンテンツ

- Secure Network Analytics Virtual Editionアプライアンスインストールガイド

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。