フローコレクタの無視リスト機能の設定

内容

はじめに

このドキュメントでは、無視リストを使用して特定の工クスポータからの着信NetFlowを拒否するようにSNAフローコレクタを設定する方法について説明します。

背景説明

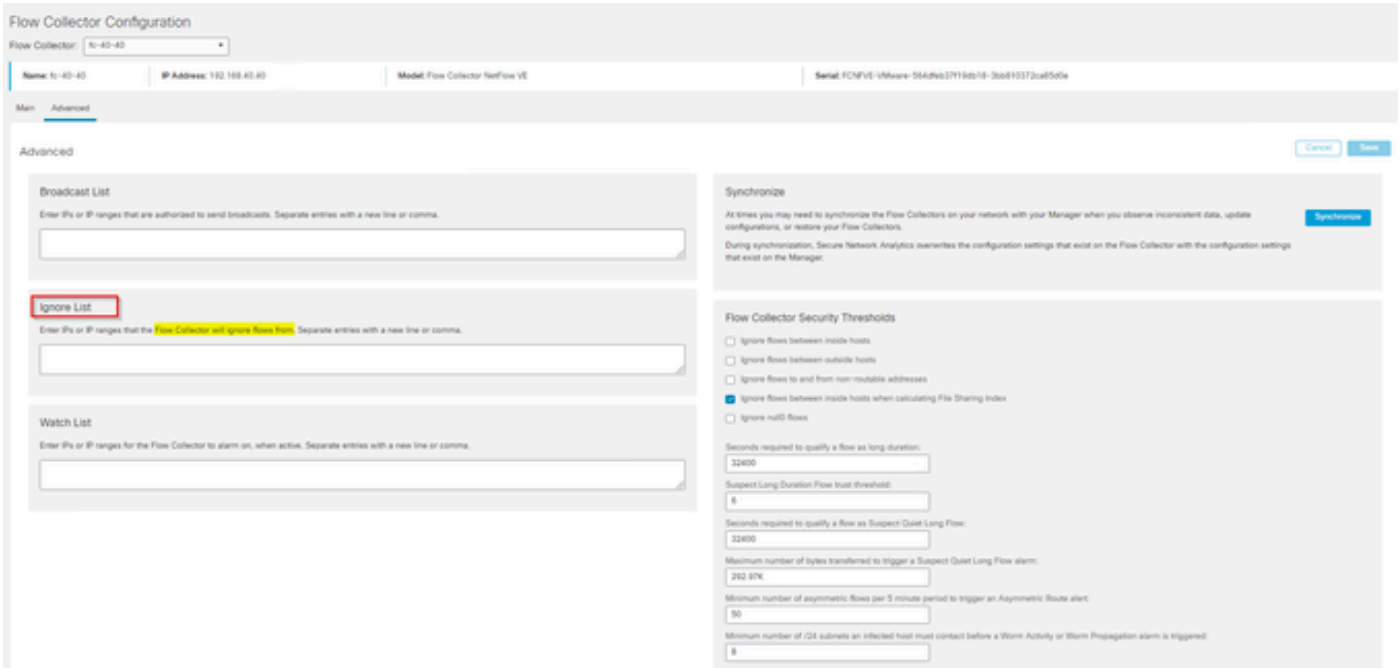
「特定の工クスポータからの着信NetFlowを拒否するようにSNAフローコレクタに指示する方法はありますか」という質問が提起されることがよくあります。

答えは「はい」です。これは、フローコレクタの「リストを無視」機能を使用して行われます。

設定

無視リスト機能はフローコレクタに固有です。 SNA 7.xの新しいバージョンでは、この機能はSNA Manager Web UIのフローコレクタ設定ページ内で使用できます。

このページを使用して、Flow Collectorcompletelyignoreconstrafficの対象となるホストまたはサブネットの数を無制限に指定します。 Flowコレクタがこれらの IPアドレスに起因するトラフィックを検出する場合、そのトラフィックはグラフまたはテーブルから除外されます。 無視されるホストとの間でやり取りされるすべてのトラフィックを信頼できることを確認してください。Secure Network Analysisでは、このトラフィックは分析されず、これらのホストを含むようにスプーフィングされたトラフィックも分析されません。これらのホスト/サブネットのいずれかを含むネットワークで攻撃が開始された場合、Flowコレクタは攻撃を報告できません。



FAQ

スマートライセンスのフロー/秒(FPS)計算での無視リストの効果は何ですか。

正解：ホストのIPアドレスまたは範囲を無視リストに追加すると、これらのフローがSMCに送信されスマートライセンスレポートに使用される計算済みFPSレートにカウントされなくなります。 SMCダッシュボードに表示されるフロー傾向グラフには、フローは表示されず、カウントされません。

クライアントがスプリットトンネルモードでNVMフローを処理する場合、ignore list機能はどのように使用されますか。

お客様は、AnyConnectを設定して、オンネットワークおよびオフネットワークのトラフィック（別名スプリットトンネル）を送信できます。オフネットワークトラフィックはエンドポイントローカルIPアドレスを使用し、ほとんどの場合、IPが重複しています。SNAはIPのオーバーラップをサポートしていません。スプリットトンネルの問題を回避するためにIgnore List機能を使用することが推奨されており、これによりNVMベースのフローの利点を検出に残すことができます。

この使用例では、「無視リスト」を設定して、フローキャッシュからのオフネットワークNVMフロー→flow_stats、フロー検索、カスタムセキュリティイベントを防止します

1. IPアドレスとネットワークマスクを無視リストに追加します(192.168.1.0/24、127.0.0.1/24の追加など)。
2. nvm_flowsに引き続きNVMフローが取り込まれていることを確認します
3. srcまたはdst IPがIgnore Listに含まれている場合、flow_statsにNVMフローがないことを確認します

エクスポータ全体からのフローを無視するために無視リストを使用できますか。 いいえ。無視リストはエクスポータのデータではなくフローデータに基づいているため、エクスポータのIPアド

レスを無視リストに追加すると、エクスポータのIPアドレスがフローの送信元または宛先としてリストされているフローデータは実質的に無視され、その特定のエクスポータからのすべてのフローレコードは無視されません

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。