ユースケース：エレファントフロー検出結果を構成する

エレファントフローについて

エレファントフローは（合計バイト数が）非常に大きく、ネットワークリンク上で測定される、TCP（または他のプロトコル）フローによって設定される比較的長期間実行されるネットワーク接続です。デフォルトでは、エレファントフローとは 1 GB/10 秒を超えるフローまたは接続です。これらのフローは、Snort コアでのパフォーマンス拘束または問題の原因となります。エレファントフローは、過剰な量の CPU リソースを消費し、検出リソースの他の競合フローに影響を与え、遅延やパケットドロップの増加などの問題を引き起こす可能性があるため、重要です。

エレファントフローの検出と修復の利点

- エレファントフロー設定により、カスタマイズと、エレファントフローをバイパスまたはスロットルするオプションが可能になります。
- 信頼できるトラフィックをバイパスしながら、疑わしいトラフィックの Snort インスペクションを提供するために、選択したアプリケーションに基づいてフローをバイパスまたはスロットルすることを選択できます。

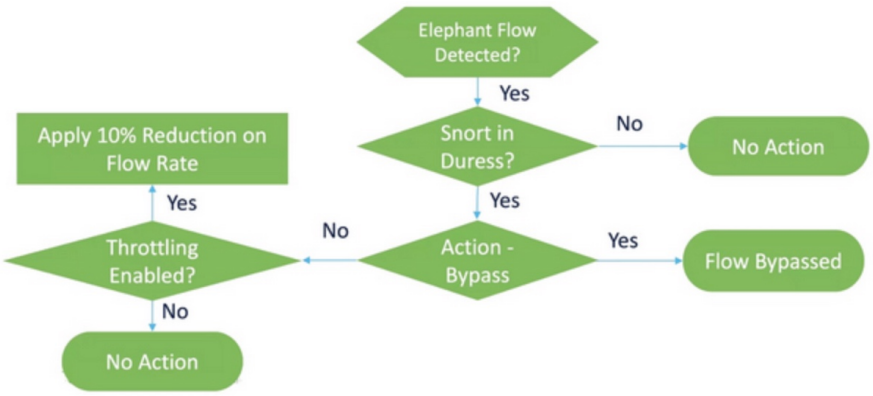
- エレファントフロー修復は、特定の要件に応じて、内部アプリケーション用に優先順位を付けて、より多くの帯域幅を解放するのに役立ちます。

エレファントフローのワークフロー

設定されたパラメータに基づいてエレファントフローが検出された場合、フローをバイパスするかスロットルするかを選択できます。フローがバイパスされると、トラフィックは Snort インスペクションなしで通過できます。スロットリングは、フローのスループットが減少することを意味します。フローレートの削減は、CPU 使用率が設定済みしきい値を下回るまで 10% ずつ減少します。バイパスまたはスロットリングは、エレファントフローが特定され、追加の CPU および時間枠パラメータが満たされた後に行われます。許可ルールで設定済みの場合、エレファントフローを識別する前に、侵入ポリシーはフローを処理します。これは、ほとんどの攻撃が接続の非常に早い段階で検出されるため、エレファントフローが完全に未検査の状態でシステムを通過できないことを意味します。

フローの処理方法を理解するには、次のフロー図を参照してください。

図 *1:* エレファントフローのワークフロー



システムが Snort の抑制状態（パフォーマンスの問題）を検出しない限り、アクションは実行されません。システムは、フローが大きいという理由だけでフローをスロットルまたはバイパスしません。また、スロットルとバイパスのアクションは相互に排他的です。つまり、フローをバイパスまたはスロットルすることはできますが、両方を行うことはできません。

抑制の原因となるすべてのエレファントフローをバイパスしたくない場合は、バイパスオプションを特定のアプリケーションのみに制限できます。パフォーマンスをスロットリングすることなく、信頼するアプリケーションの接続を優先することができます。バイパスする必要があるアプリケーションを設定できますが、残りのフロー（抑制の原因となる）はスロットリングされます。これにより、他の信頼できないアプリケーションフローは、帯域幅が削減されても、引き続き完全な Snort インスペクションを受信します。

ビジネスシナリオの例

データセンターでは、クラスタ間のデータのレプリケーション、仮想マシンの統合、データベースのバックアップなど、いくつかのアクティビティが発生しています。組織内のユーザーは、OTTでビデオを視聴したり、ダウンロードしたりしている可能性があります。このようなアクティビティによる帯域幅の利用は、エレファントフローを引き起こし、ネットワークの速度を低下させ、重要なタスクのパフォーマンスに影響を与える可能性があります。ネットワーク管理者（特定の要件によっては異なります）として、帯域幅の問題を引き起こしている大規模なフローを可視化し、それらを修復する必要があります。

たとえば、エレファント フロー パラメータを設定して、Webex トラフィック（組織がリアルタイムのビデオ会議に使用）のSnortインスペクションをバイパスし、その他のアプリケーションまたは接続（ビデオ、映画など）をスロットリングする方法を見てみましょう。

前提条件

- Management Center 7.2.0 以降を実行していること、および管理対象の Threat Defense も 7.2.0 以降であることを確認します。
- エレファントフロー検出を有効にするだけでは、追加の接続イベントは生成されません。エレファントフロー検出は、すでに Management Center のログに記録されている一致する接続にエレファントフロー表記を追加します。**これらのイベントをログに記録するには、アクセス コントロール ポリシーで接続ロギングを有効にする必要があります。**特定のルールに対してこれを行うか、エレファントフローを含むすべての接続をログに記録するモニタールールを追加できます。

エレファント フロー パラメータの設定

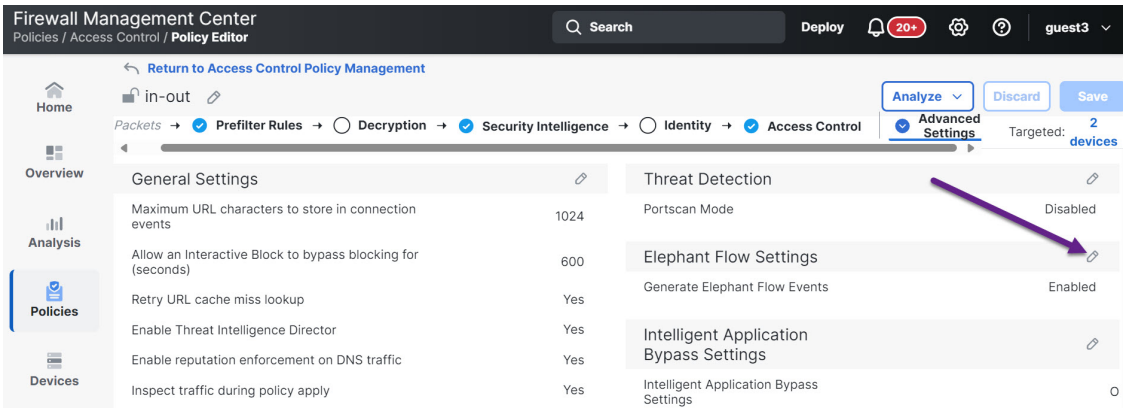
手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある **Edit** (✎) をクリックします。

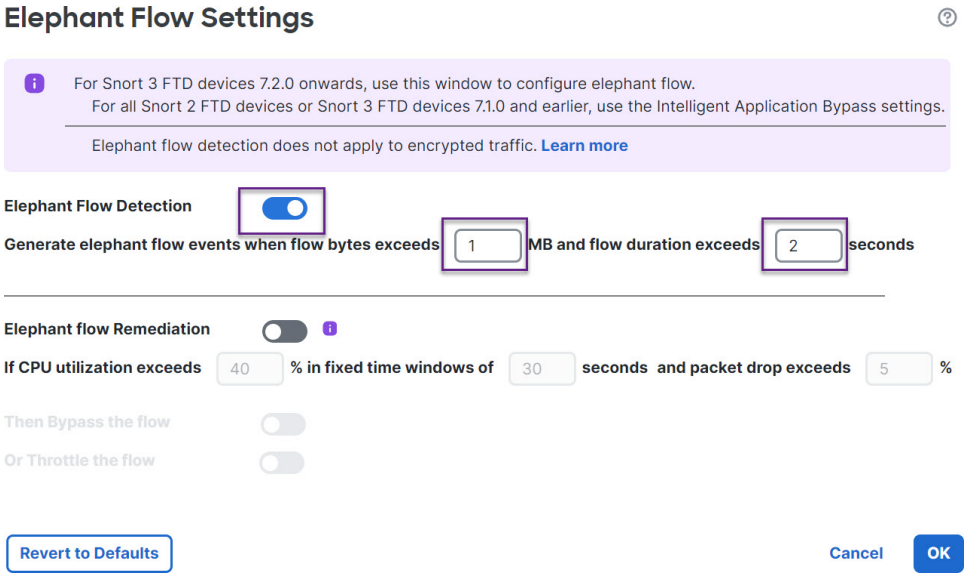
ステップ 3 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 4 **[エレファントフロー設定（Elephant Flow Settings）]** の横にある **Edit** (✎) をクリックします。



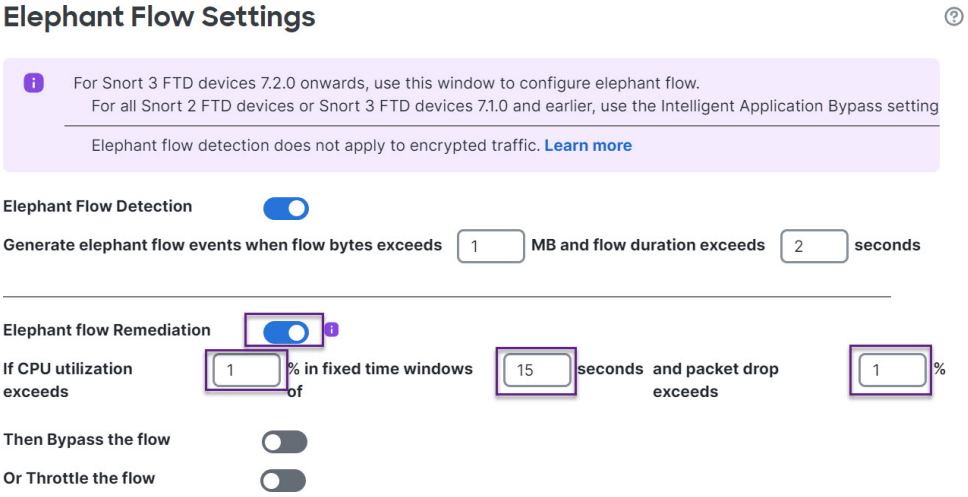
ステップ 5 [エレファントフロー検出（Elephant Flow Detection）] トグルボタンはデフォルトで有効になっています。デフォルト設定では、検出のみが有効になり、デフォルトアクションは設定されません。検出設定では、システム内のエレファントフローを識別できるように、フローのバイト数と期間を調整できます。

テスト設定として、次の図に示すように、フローのバイト数と期間のパラメータを設定します。

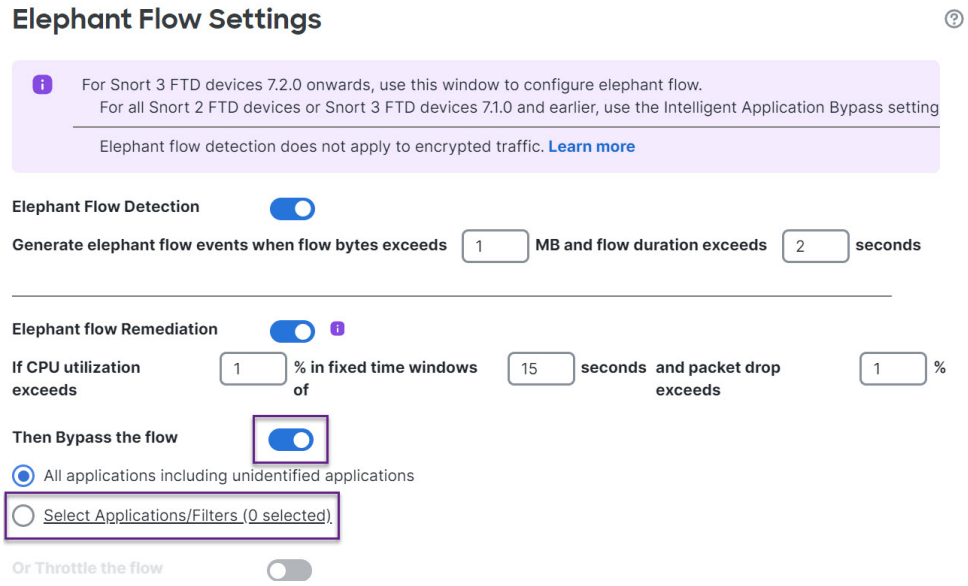


ステップ 6 [エレファントフローの修復（Elephant Flow Remediation）] トグルボタンを有効にします。エレファントフローが検出された場合、フローをバイパスするかスロットルするかを選択できます。フローのバイパスとは、トラフィックが Snort インスペクションなしで通過できることを意味します。スロットリングは、フローのスループットが減少することを意味します。このレートは、CPU 使用率が設定済みしきい値を下回るまで 10% ずつ減少します。

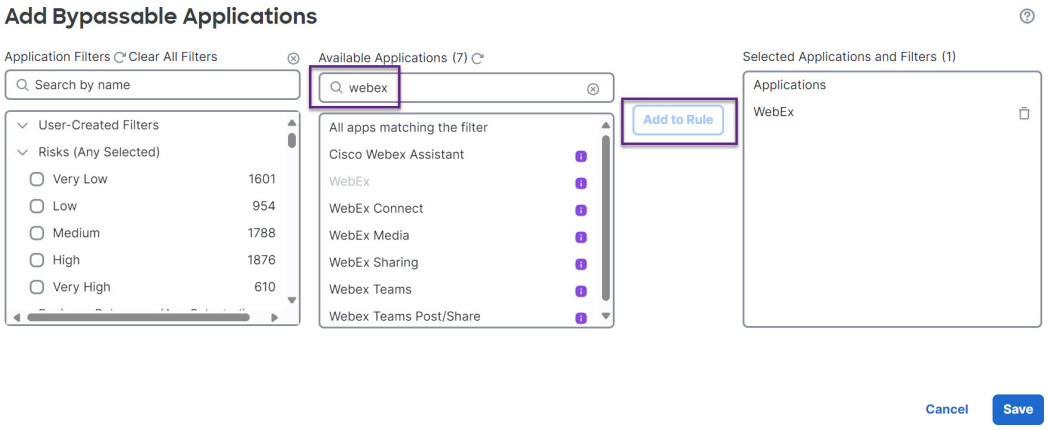
テスト設定として、次の図に示すようにエレファントフロー修復パラメータを設定します。



ステップ 7 [フローのバイパス（Bypass the flow）] トグルボタンを有効にし、[アプリケーション/フィルタの選択（Select Applications/Filters）] ラジオボタンをクリックします。



ステップ 8 [アプリケーションフィルタ（Application Filters）] で、**Webex** アプリケーションを検索して選択し、ルールに追加して [保存（Save）] をクリックします。つまり、設定されたパラメータに基づいて、これらの Webex 接続がエレファントフローとして検出された場合、Webex 接続は信頼され、優先されるため、Snort インスペクションがスキップされます。



ステップ 9 [スロットル（Throttle）] トグルボタンを有効にして、残りのフローをスロットルします（抑制の原因となります）。これにより、Snort の抑制条件が満たされるまで、他のすべてのフローの速度が 10% ずつ低下します。

ステップ 10 [OK] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。「設定変更の展開」を参照してください。

エレファントフローのイベントの表示

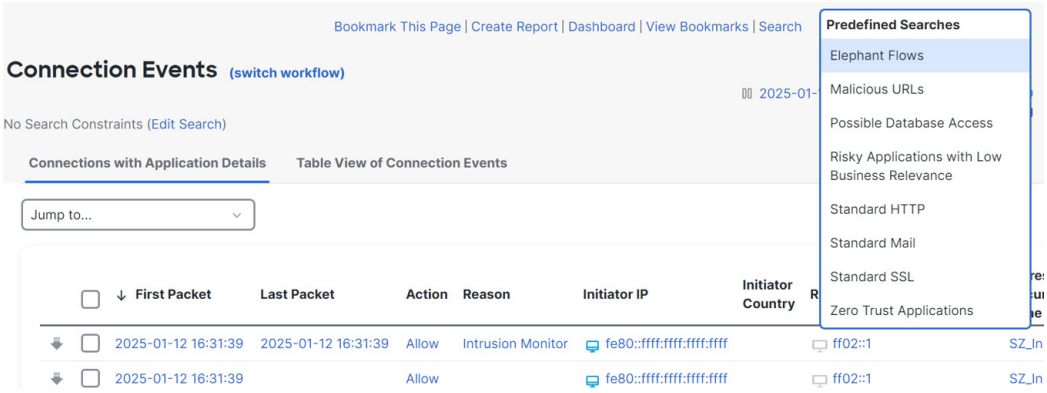
エレファントフロー設定を構成した後、接続イベントをモニターして、フローが検出、バイパス、またはスロットリングされているかどうかを確認します。この情報は、接続イベントの [理由（Reason）] フィールドで確認できます。エレファントフロー接続の 3 つのタイプは次のとおりです。

- エレファントフロー（Elephant Flow）
- エレファントフローがスロットリングされている（Elephant Flow Throttled）
- エレファントフローが信頼されている（Elephant Flow Trusted）

手順

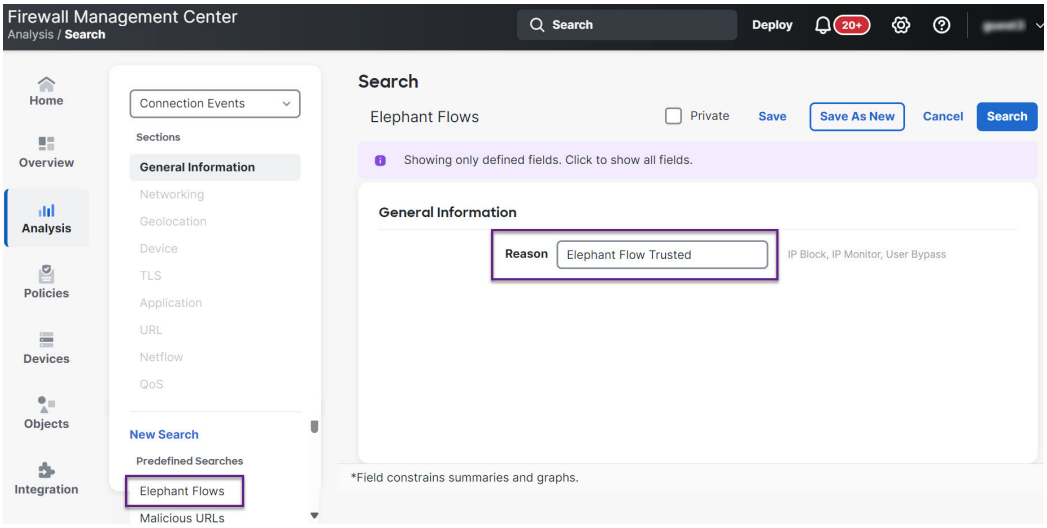
ステップ 1 **[分析（Analysis）]>[接続（Connections）]>[イベント（Events）]**を選択します。[統合されたイベント（Unified Events）] ビューアからイベントを表示することもできます。

ステップ 2 [接続イベント（Connection Events）] ページで、[定義済み検索（Predefined Search）] ドロップダウンリストから [エレファントフロー（Elephant Flows）] を選択してエレファントフローイベントを表示します。

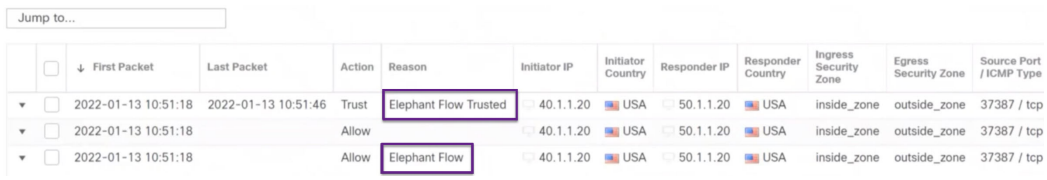


ヒント

Elephant Flow Trusted または **Elephant Flow Throttled** のイベントタイプを表示するには、ページの左上隅にある [検索の編集（Edit Search）] リンクをクリックし、[理由（Reason）] フィールドで、左側のパネルの [エレファントフロー（Elephant Flows）] を選択します。検索する内容に応じて、**Elephant Flow Trusted** または **Elephant Flow Throttled** と入力します。



ステップ 3 フローの途中で検出されたエレファントフローを表示すると、[理由（Reason）] フィールドに [エレファントフロー（Elephant Flow）] と表示されます。フローの最後にバイパスされると、[理由（Reason）] フィールドに [エレファントフローが信頼されている（Elephant Flow Trusted）] と表示されます。



エレファントフロー修復除外の設定

修復から除外する必要があるフローのL4アクセス制御リスト（ACL）ルールを設定できます。フローがエレファントフローとして検出され、それが、定義されたルールに一致する場合、そのフローは修復アクションから除外されます。

始める前に

Management Center 7.4.0 以降を実行している必要があり、管理対象 Threat Defense も 7.4.0 以降である必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

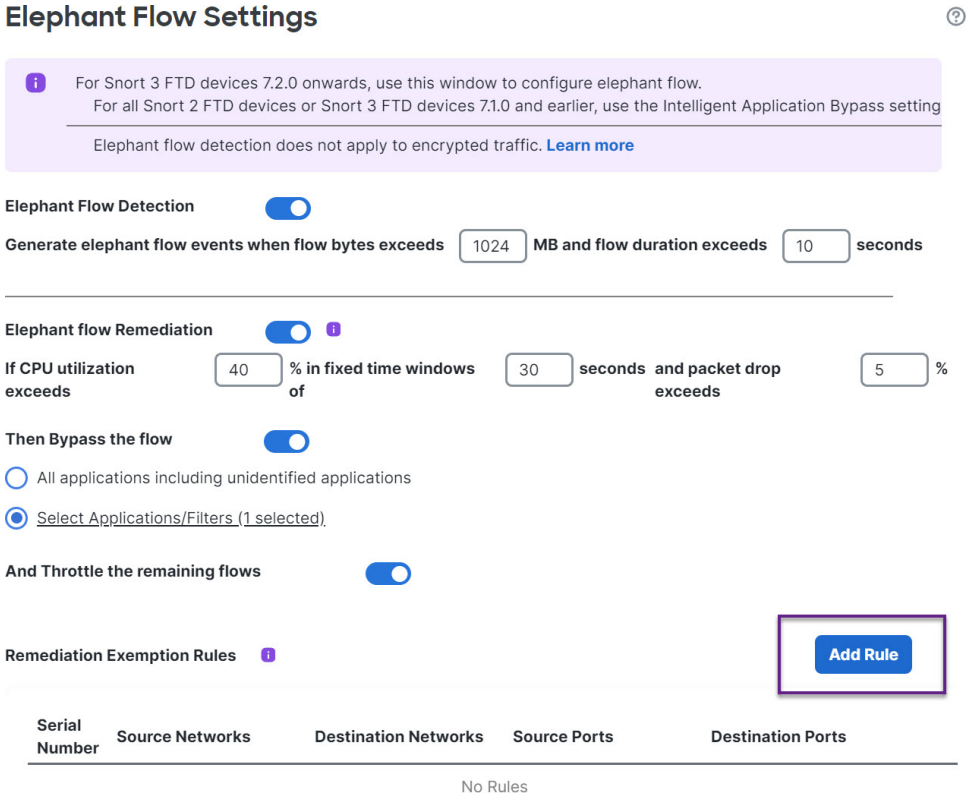
ステップ 2 編集するアクセス コントロール ポリシーの横にある **Edit** (✎) をクリックします。

ステップ 3 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

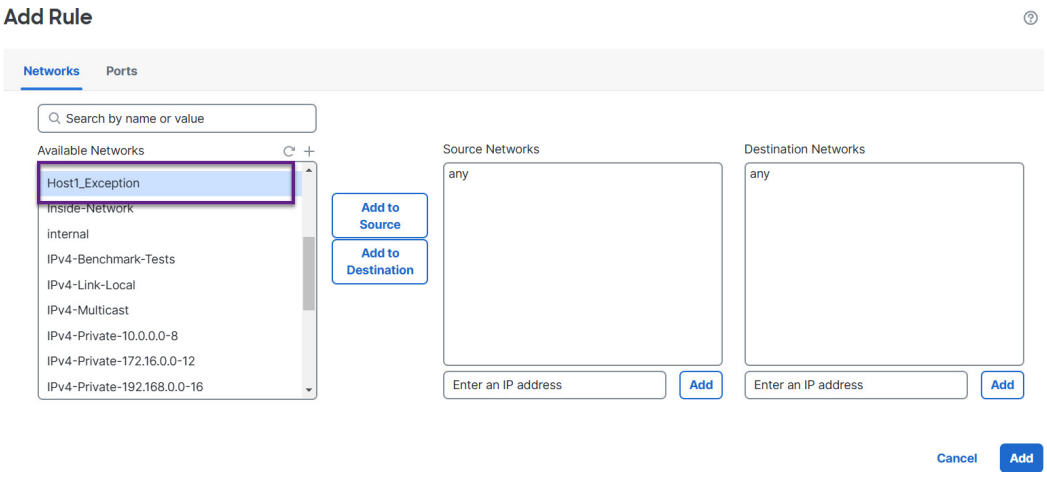
ステップ 4 **[エレファントフロー設定（Elephant Flow Settings）]** の横にある **Edit** (✎) をクリックします。

ステップ 5 エレファントフロー検出および修復パラメータが設定されていることを確認します。エレファント フロー パラメータの設定 （3 ページ） を参照してください。

ステップ 6 [修復除外ルール（Remediation Exemption Rules）] の横にある [ルールの追加（Add Rule）] ボタンをクリックします。



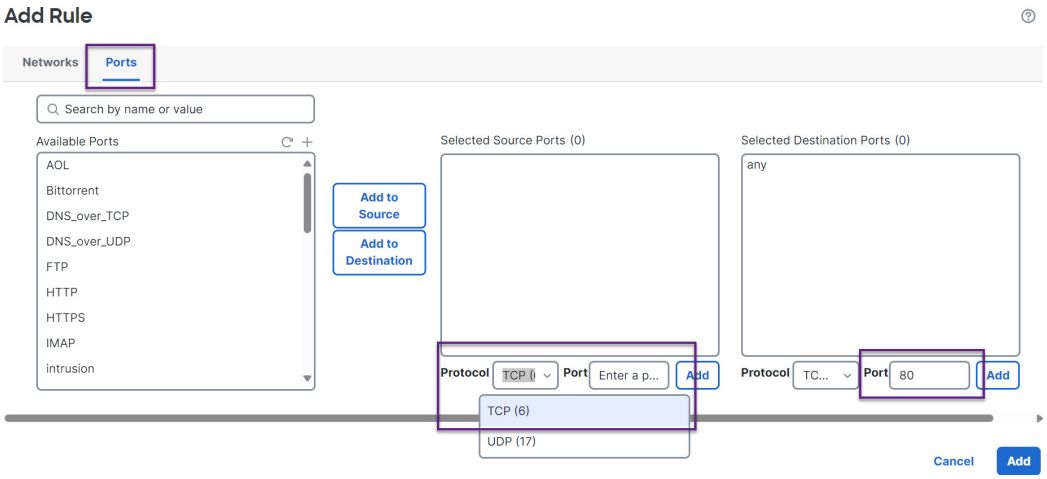
ステップ 7 [使用可能なネットワーク（Available Networks）] のリストから、エレファントフロー修復から除外する設定済みホストを選択します。この例では、「Host1_Exception」というホストを作成しました。



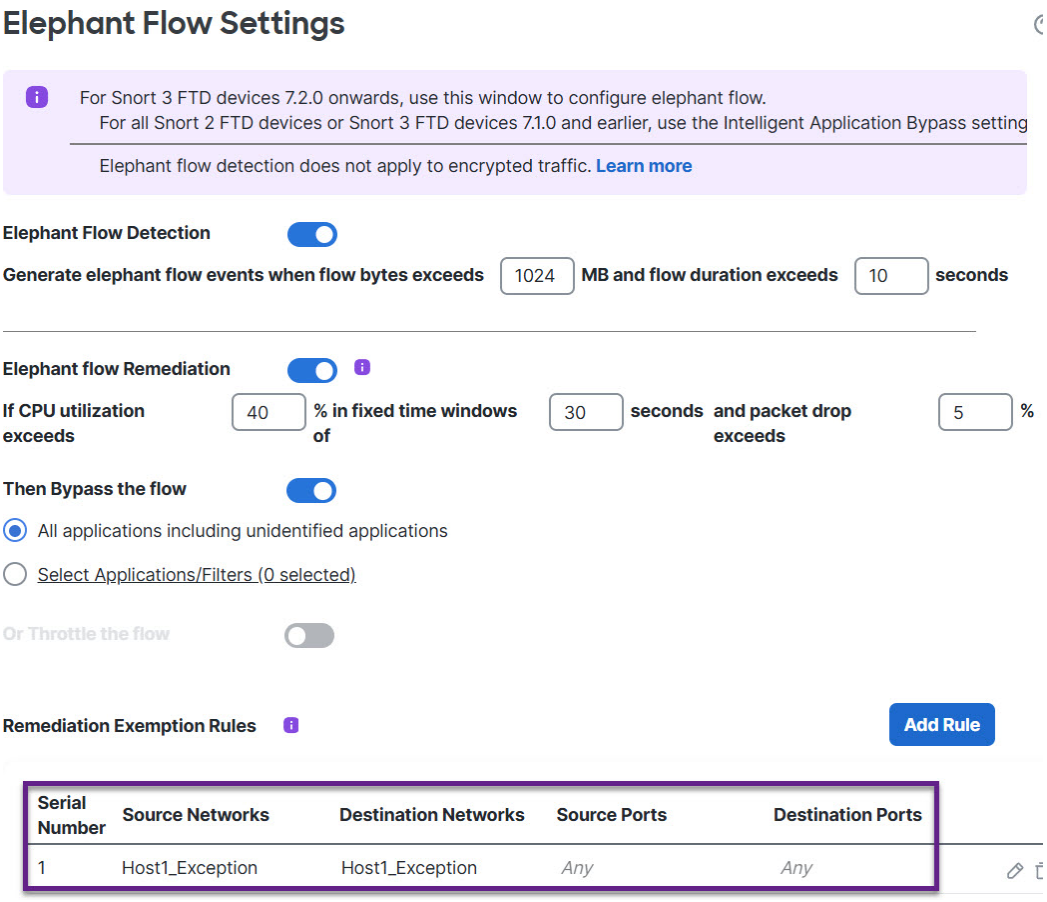
ステップ 8 必要に応じて、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、このホストを送信元または宛先に追加します。

ステップ 9 [ポート（Ports）] タブをクリックします。

ステップ 10 送信元ポートとして、[プロトコル：TCP（Protocol as TCP）] を選択し、宛先ポートとして **80** を入力し、[追加（Add）] をクリックします。



ステップ 11　[OK] をクリックします。



ステップ 12　[保存（Save）] をクリックします。

次のタスク

設定変更を展開します。「設定変更の展開」を参照してください。

エレファントフロー修復除外のイベントの表示

手順

ステップ 1 **[分析（Analysis）]**>**[接続（Connections）]**>**[イベント（Events）]**を選択します。[統合されたイベント（Unified Events）] ビューアからイベントを表示することもできます。

ステップ 2 修復から除外されたエレファントフローを表示します。[理由（Reason）] フィールドに [エレファントフロー除外（Elephant Flow Exempted）] と表示されます。

その他の参考資料

概念の詳細については、このガイドの「Snort 3 のエレファントフロー検出」の章または次のリンクの内容を参照してください。

- エレファントフローの検出

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。