Cisco Secure Network Analytics

Cisco Secure Network Analytics 7.4 へのNSEL エクスポートに向けたASA 統合

目次

概要

このドキュメントでは、Adaptive Security Device Manager（ASDM）を使用して Stealthwatch フロー収集インフラストラクチャに NetFlow セキュア イベント ロギング（NSEL）をエクスポートするように、Cisco 適応型セキュリティ アプライアンス（ASA）を設定するために必要な設定オプションについて説明します。Stealthwatch システムは ASA OS v9.1(5) および ASDM v7.1(4) を実行する ASA でテスト済みです。

> v7.4.0 では、Cisco Stealthwatch Enterprise 製品のブランド名を Cisco Secure Network Analytics に変更しました。詳細なリストについては、リリース ノート を参照してください。このガイドでは、以前の製品名である Stealthwatch が必要に応じて明確さを維持するために使用され、Stealthwatch Management Console や SMC などの用語も使用されています。

対象読者

このドキュメントは、Stealthwatch にデータを送信するように Cisco ASA を設定する必要がある担当者を対象としています。

はじめる前に

このドキュメントの手順を完了するには、次の情報が必要になります。

- ASA からデータを受け取る Stealthwatch フロー コレクタの IP アドレス
- フロー コレクタにデータを送信する ASA のインターフェイス
- NetFlow の転送に使用する UDP ポート番号

プロセスの概要

この設定プロセスでは、このドキュメントの説明に従って次の手順を実行します。

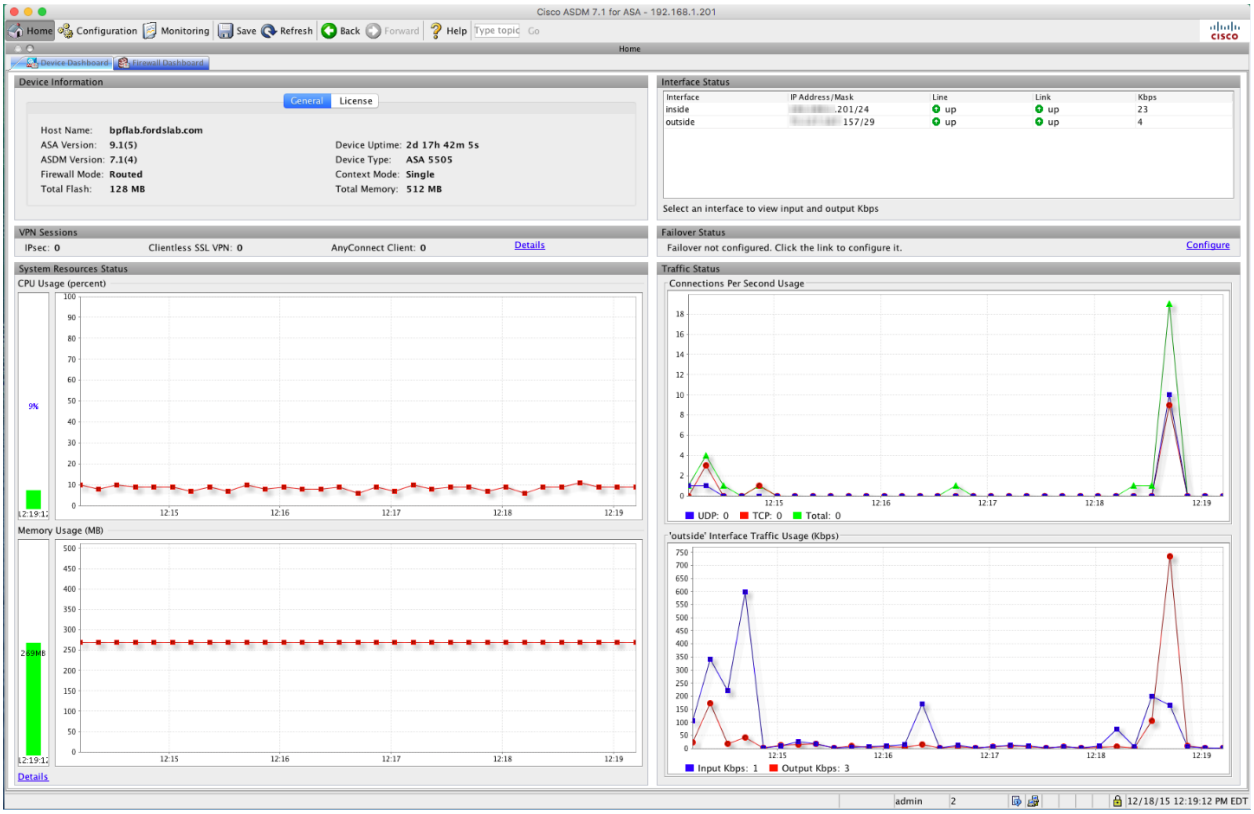
NetFlow のエクスポート オプションの定義

NetFlow の作成条件の設定

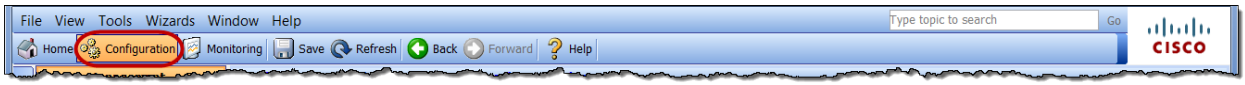
NetFlow のエクスポート オプションの定義

ASA からの NetFlow データのエクスポートに関連するさまざまなオプション（関連するタイマーやエクスポート先など）を設定するには、次の手順を実行します

1. ASDM にログインします。ホームページが開きます。



2. [設定（Configuration）] をクリックして [設定（Configuration）] ページを開きます。

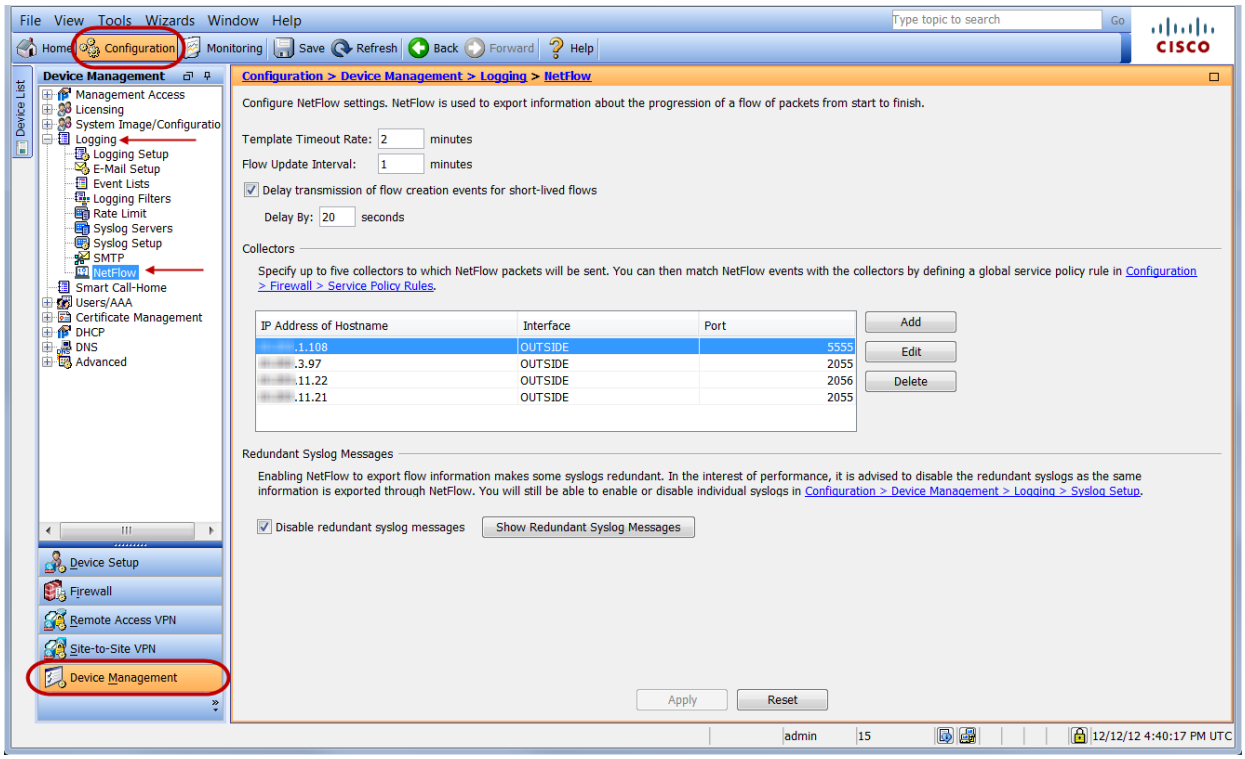


3. 次の手順を実行して [NetFlow] ページにアクセスします。

   a. 左側のナビゲーション ウィンドウの下部にある [デバイス管理（Device Management）] をクリックします。

   b. 左側のナビゲーション ウィンドウにあるツリーで、[ロギング（Logging）] > [NetFlow] を選択します。

   [NetFlow] ページが開きます。



4. 次の手順を実行します。

   a. [テンプレートタイムアウトレート（Template Timeout Rate）] フィールドで、テンプレートの更新が ASA から送信される頻度を定義します。

      - この値は 5 分以下に設定することをお勧めします。次の例では、テンプレートの更新が 10 分ごとに行われます。

   b. [フロー更新間隔（Flow Update Interval）] フィールドで、長時間フローのステータスの更新が ASA から送信される頻度を定義します。

      - この値は 1 分に設定することをお勧めします。

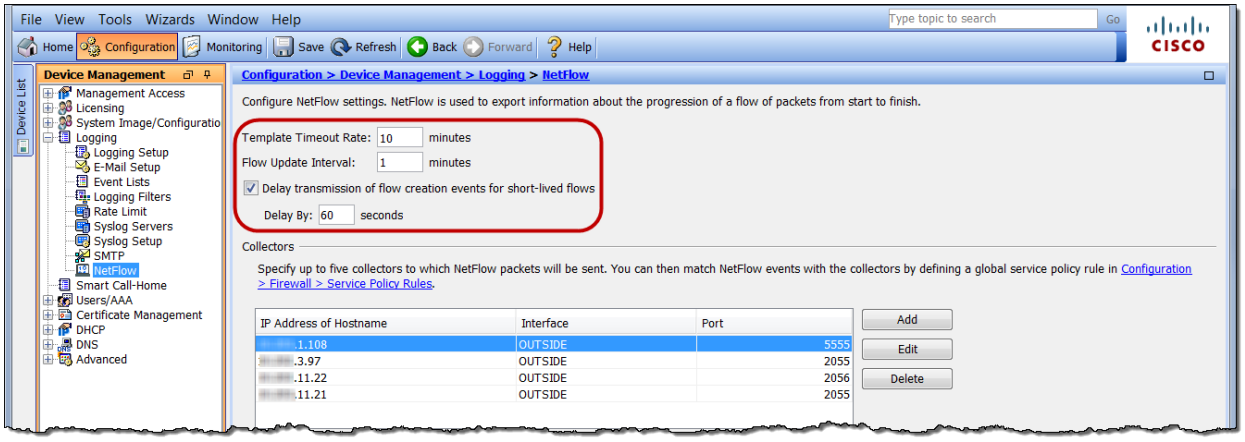
   c. [短時間フローのフロー作成イベントの遅延転送（Delay transmission of flow creation events for short-lived flows）] チェック ボックスをオンにします。

   d. [遅延時間（Delay By）] フィールドに「**60**」と入力し、レコードがキャッシュに保持される時間を 60 秒に設定します。この値は推奨されるアクティブ タイムアウト値と一致するため、以下が実現します。

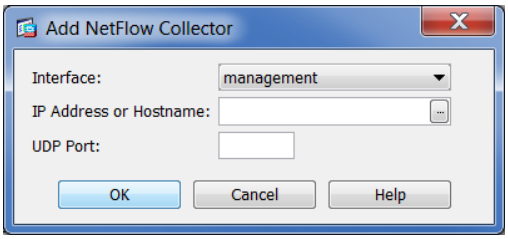
      - ASA からエクスポートされるフロー イベントの数が減少します。
      - データ レポートを著しく変更せずにライセンスの影響が軽減されます。

      [短時間フローのフロー作成イベントの遅延転送（Delay transmission of flow creation events for short-lived flows）] チェック ボックスをオンにした場合、フロー作成イベント後 60 秒未満でフローが期限切れになると、レコードは 1 つのみ送信されます（フロー作成とティアダウンのそれぞれに対して 1 つずつ送信されるのではない）。

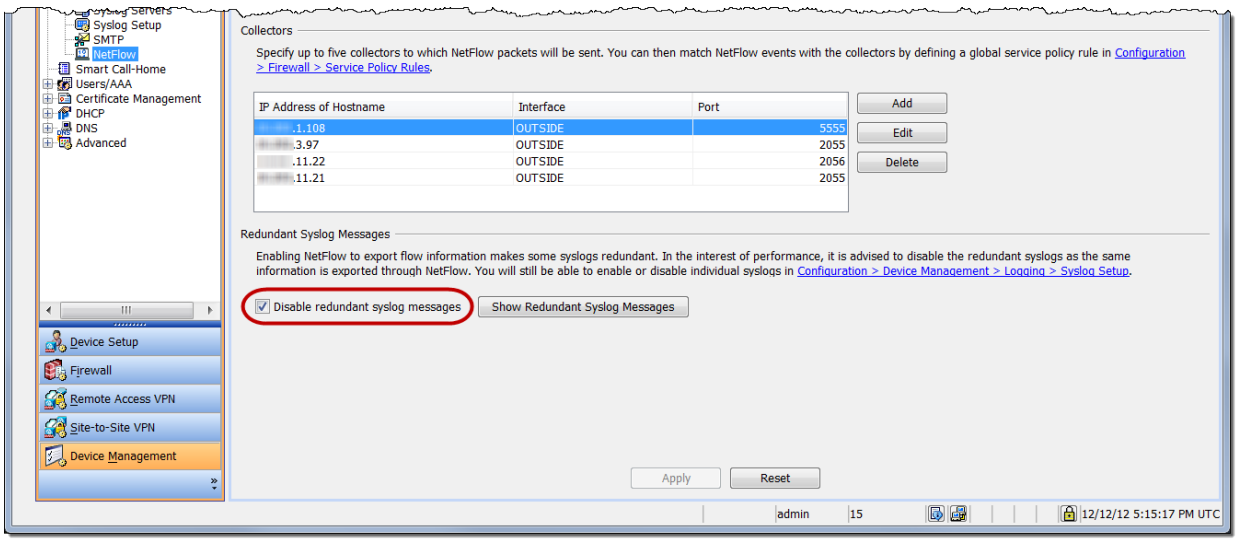
ご利用の環境でパフォーマンスへの影響について具体的な懸念がある場合は、Cisco ASA サポート チームに連絡してください。



5. [追加(Add)]をクリックします。[NetFlowコレクタの追加(Add NetFlow Collector)]ダイアログが開きます。



6. 以下のようにフィールドに入力します。
   - [インターフェイス(Interface)]フィールドでドロップダウン矢印をクリックし、フロー コレクタに NetFlow データを送信する ASA のインターフェイスを定義します。
   - [IPアドレスまたはホスト名(IP Address or Hostname)]フィールドに、ASA からデータを受信するフロー コレクタの IP アドレスを入力します。
   - [UDPポート(UDP Port)]フィールドに、NetFlow の転送に使用するポート番号を入力します。
7. [OK] をクリックします。[Netflow] ページが開き、[コレクタ(Collectors)] セクションに新しいフロー コレクタの情報が表示されます。
8. パフォーマンス上の理由から、[冗長なsyslogメッセージを無効にする(Disable redundant syslog messages)] チェック ボックスをオフにすることをお勧めします。ただし、パフォーマンスに関する具体的な懸念事項がある場合はシスコサポートチームに確認する必要があります。

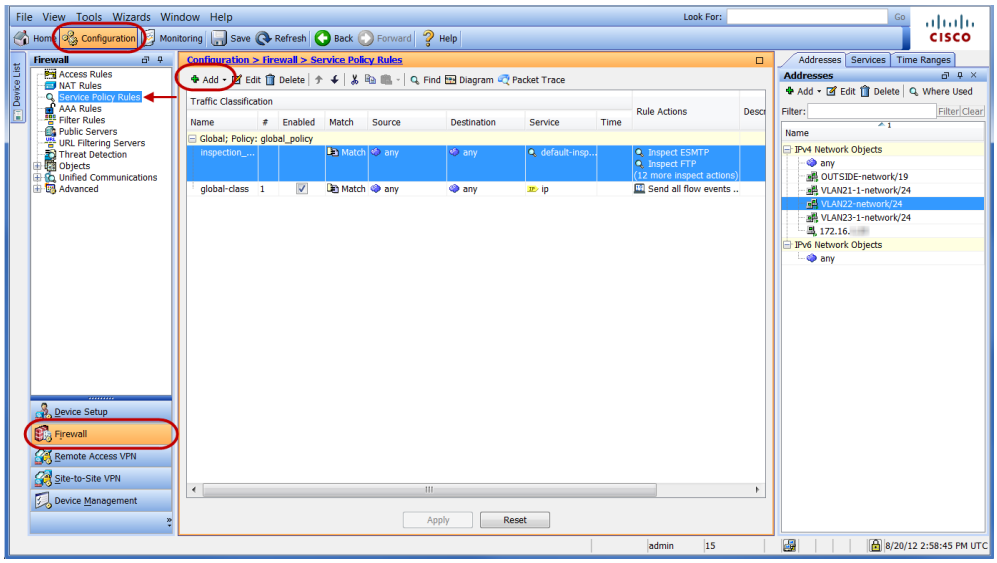


9. このガイドの「NetFlowの作成条件の設定」に進みます。

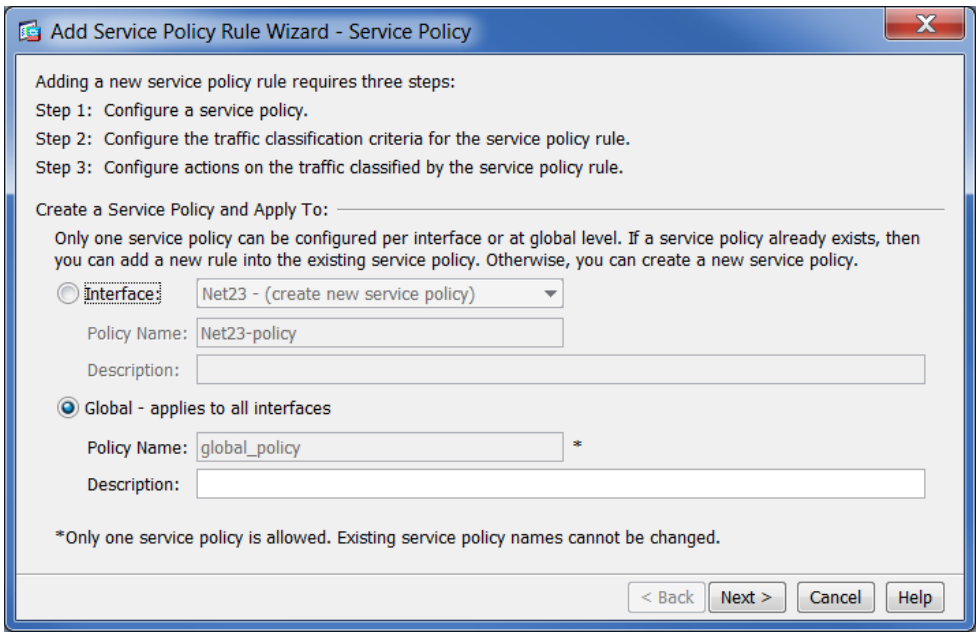
NetFlow の作成条件の設定

定義済みのフロー コレクタにエクスポートできる NetFlow イベントの作成条件を定義するには、次の手順を実行します。

1. 左側のナビゲーション ウィンドウの下部にある [ファイアウォール（Firewall）] をクリックします。
2. 左側のナビゲーション ウィンドウにあるツリーで、[サービスポリシールール（Service Policy Rules）] をクリックし、そのページを表示します。



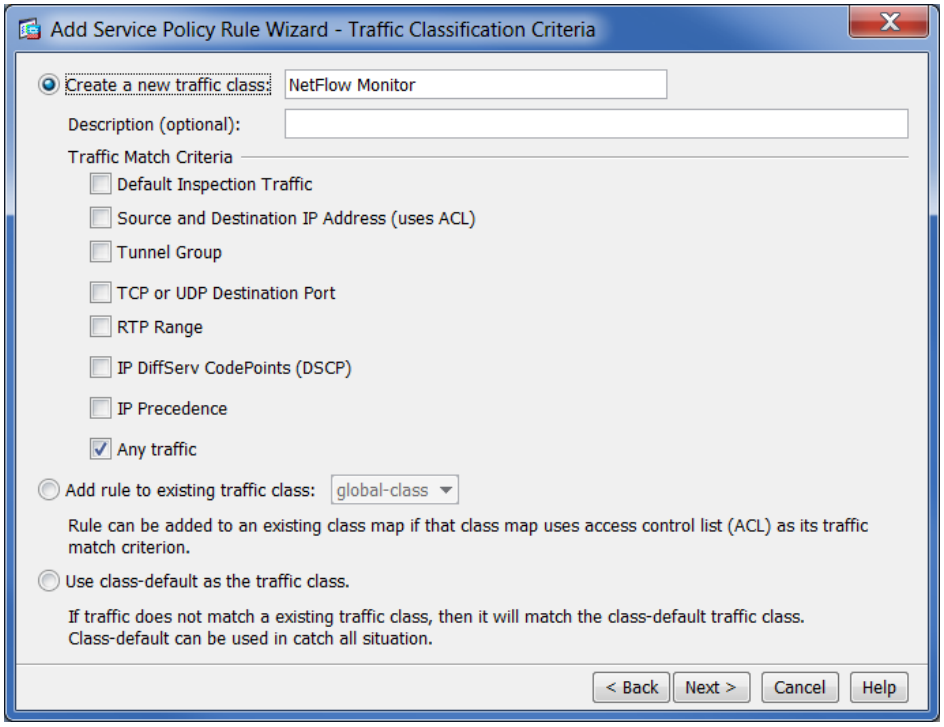
3. ツールバーで、[追加（Add）] をクリックします。[サービスポリシールールの追加ウィザード：サービスポリシー（Add Service Policy Rule Wizard: Service Policy）] ページが開きます。



4. [グローバル – すべてのインターフェイスに適用(Global – applies to all interfaces)] オプションを選択して、すべての ASA インターフェイスで NetFlow 統計情報の収集を許可し、ASA ファイアウォールの NetFlow ロギング機能を活用することをお勧めします。

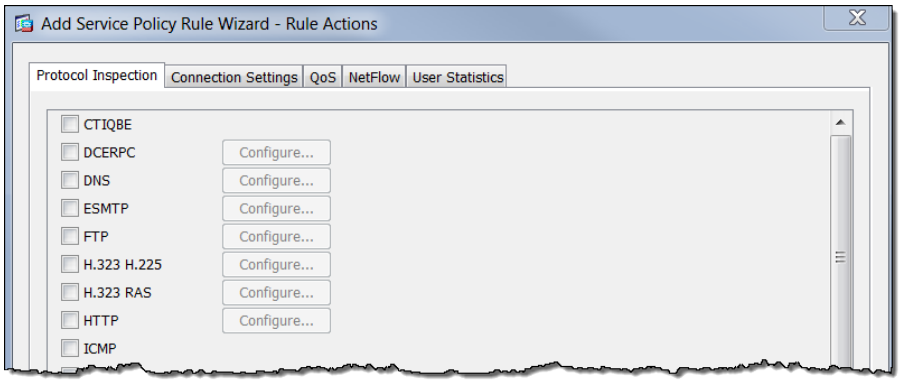
   特定のインターフェイスを選択してフロー出力とロギングを制限できます。

5. [次へ(Next)] をクリックします。[サービスポリシールールの追加ウィザード:トラフィック分類基準(Add Service Policy Rule Wizard: Traffic Classification Criteria)] ページが開きます。

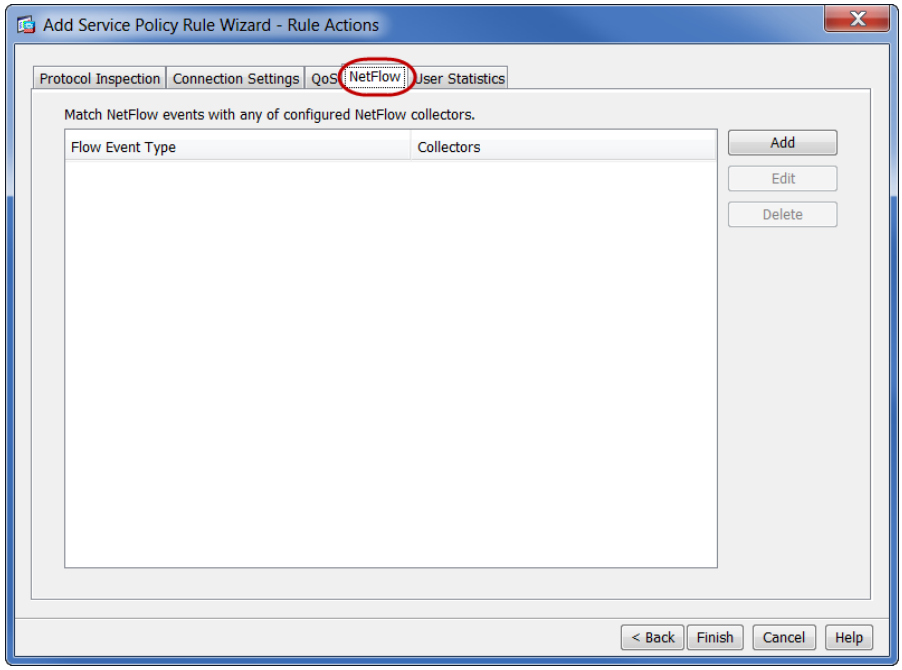


6. 次の手順を実行します。
   - [新しいトラフィッククラスの作成(Create a new traffic class)] オプションを選択します。
   - [新しいトラフィッククラスの作成(Create a new traffic class)] フィールドに、「NetFlow Monitor」と入力します。
   - [すべてのトラフィック(Any traffic)] チェック ボックスをオンにして、選択したインターフェイスを通過するすべてのタイプのトラフィックをモニターします。

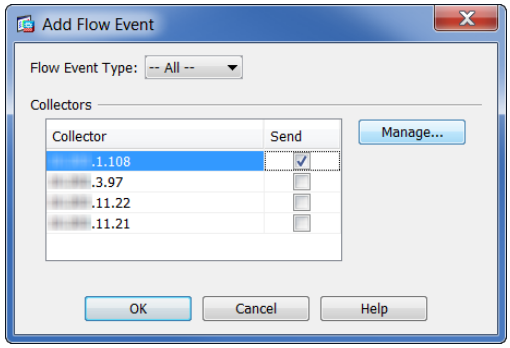
7. [次へ(Next)] をクリックします。[サービスポリシールールの追加ウィザード:ルールアクション(Add Service Policy Rule Wizard: Rule Actions)] ページが開きます。



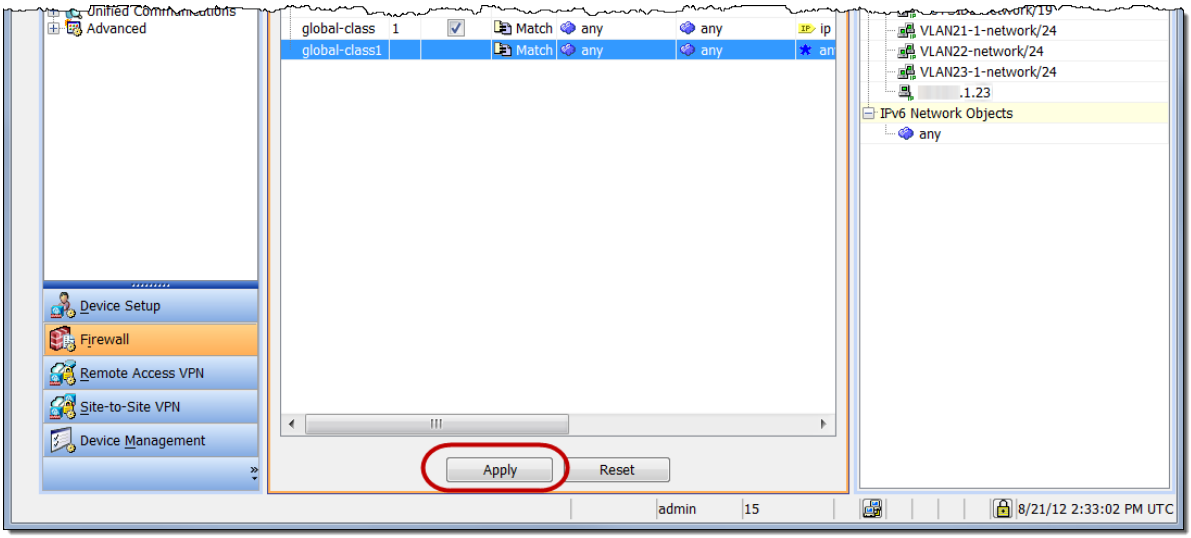
8. [NetFlow] タブをクリックします。



9. [追加(Add)] をクリックします。[フローイベントの追加(Add Flow Event)] ダイアログが開きます。



10. 次の手順を実行します。
    - [フローイベントタイプ（Flow Event Type）] フィールドで、ドロップダウン矢印をクリックして [すべて（All）] を選択します。これは、すべてのタイプの NSEL レコードが Cisco ASA によって生成されることを指定します。
    - [コレクタ（Collectors）] セクションで、以前に設定したフロー コレクタの IP アドレスに対応するチェック ボックスをオンにします。
11. [OK] をクリックします。[サービスポリシールール（Service Policy Rules）] ページが開いて新しいサービス ポリシーが表示されます。



12. [適用（Apply）] をクリックします。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報