Cisco Secure Network Analytics

v7.4 フローセンサーとロードバランサの統合ガイド

目次

はじめに

ロードバランサがネットワーク上のリソースの前にインストールされている場合、可視性が不明瞭になり、Stealthwatch システムでの脅威の検出が低下する可能性があります。

ロードバランサと FlowSensor を設定するには、このガイドの手順を使用します。この設定によって、クライアント側とサーバー側のフローが一緒にスティッチングされるため、外部ホストは内部ホストに接続し、フローセンサーと Stealthwatch システムで可視性と強化されたセキュリティを提供できます。

> 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

このガイドの主な対象者には、Stealthwatch システムの設定を担当する管理者が含まれています。

はじめる前に

このガイドの手順を開始する前に、次の手順を実行する必要があります。

- Stealthwatch システムが通信していることを確認します。Stealthwatch デスクトップクライアントに移動します。アラーム テーブルを確認し、アクティブな [管理チャネルダウン(Management Channel Down)] アラームまたは [フェールオーバーチャネルダウン(Failover Channel Down)] アラームがないことを確認します。
- Stealthwatch システムアプライアンスのライセンスがアクティブであることを確認します。

ロード バランサの設定

ロードバランサを設定するには、次の手順を使用します。HTTP の場合は、X-Forwarded-For（XFF）オプションを無効にし、iRule を作成して、仮想サーバーのリソースを有効にします。既存の iRule を使用する場合は、ここに記載されている情報を使用して変更できます。正常に統合するには、このセクションの手順をネットワーク内のすべてのロードバランサに適用します。

このガイドの手順では、例として F5 ロードバランサの設定を示していますが、この設定はすべてのタイプのロードバランサで使用できます。

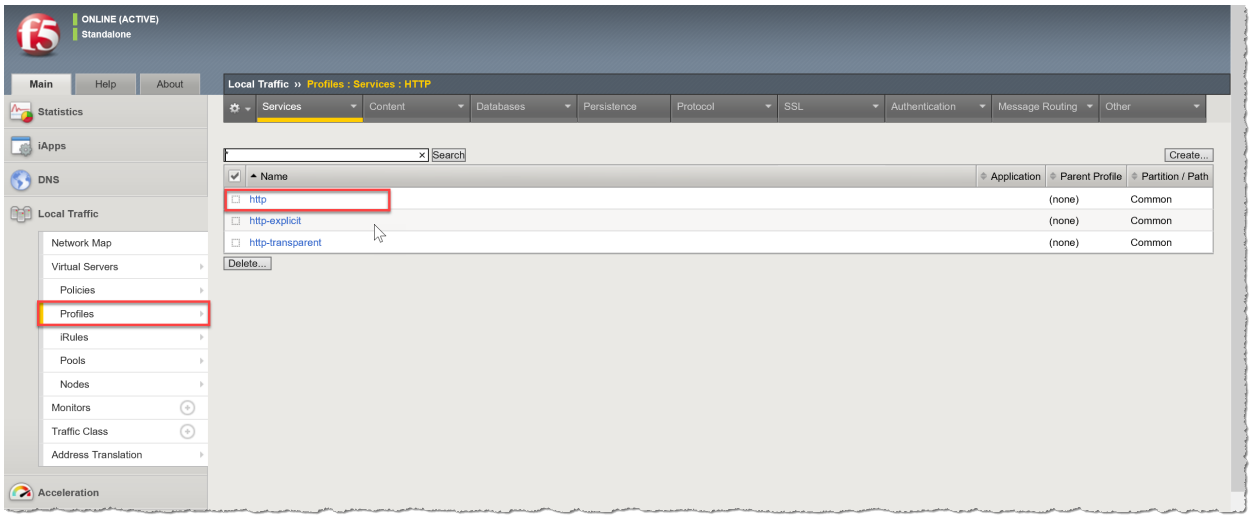
HTTP の XFF オプションの無効化

HTTP の XFF オプションを無効にするには、次の手順を使用します。

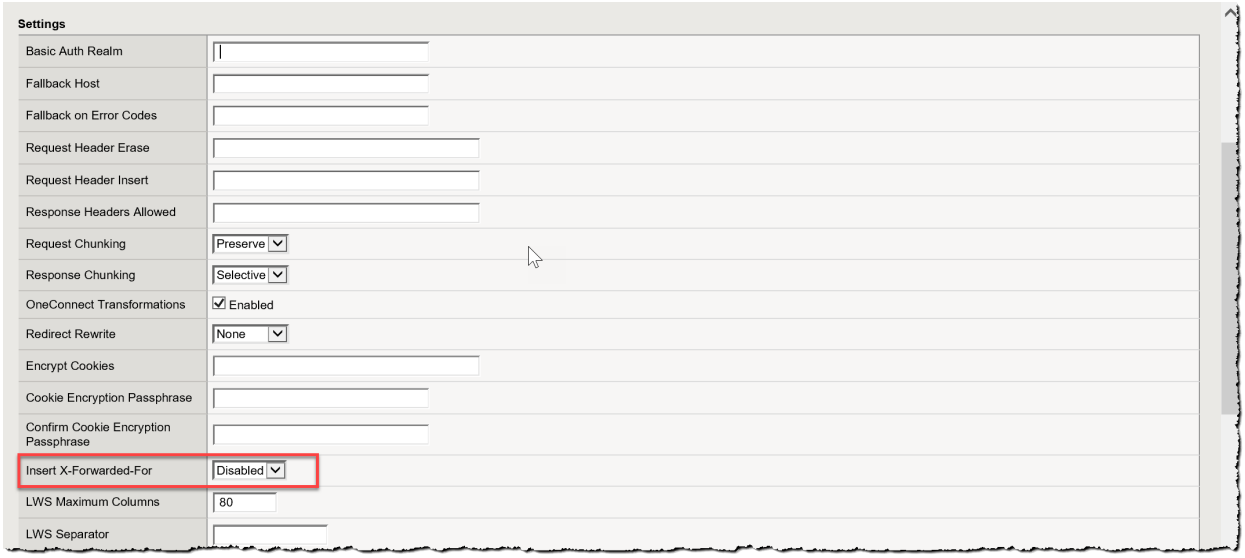
XFF HTTP ヘッダーにデータを挿入するための組み込み機能は、次の手順に従い F5 ロードバランサで無効にする必要があります。

1. F5 ロードバランサ設定ユーティリティにログインします。
2. [メイン（Main）] タブで、[ローカルトラフィック（Local Traffic）] をクリックします。
3. [プロファイル（Profiles）] > [サービス（Services）] > [HTTP] の順にクリックします。

[サービス（Services）] メニューに HTTP が表示されない場合は、ステップ 8 に進みます。



4. [http] をクリックします。
5. [設定（Settngs）] で [X-Forwarded-Forの挿入（Insert X-Forwarded-For）] を見つけます。
6. ドロップダウンリストから [無効（Disabled）] を選択します（または、[有効（Enabled）] チェックボックスをオフにしてクリアします）。



7. [更新(Update)] ボタンをクリックします。
8. [サービス(Services)] メニューから、[高速 HTTP(Fast HTTP)] をクリックします。

[サービス(Services)] メニューに [高速HTTP(Fast HTTP)] がない場合は、このセクションの残りの手順をスキップします。[iRuleの作成(Creating the iRule)] に進みます。

9. [X-Forwarded-Forの挿入(Insert X-Forwarded-For)] を見つけます。
10. ドロップダウンリストから [無効(Disabled)] を選択します(または、[有効(Enabled)] チェックボックスをオフにしてクリアします)。
11. [更新(Update)] ボタンをクリックして、保存して終了します。
12. [iRuleの作成(Creating the iRule)] に進みます。

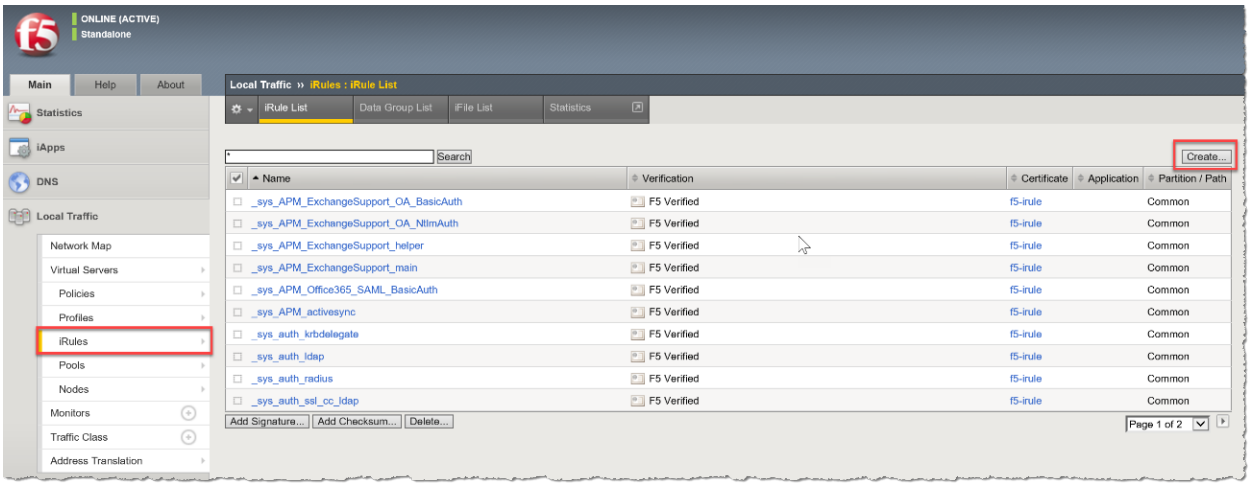
iRuleの作成

XFF ヘッダーの iRule を追加するには、次の手順を使用します。この手順は、ロードバランサの IP アドレスをマッピングし、正確なポートおよびプロトコル情報を FlowSensor に報告するために使用します。

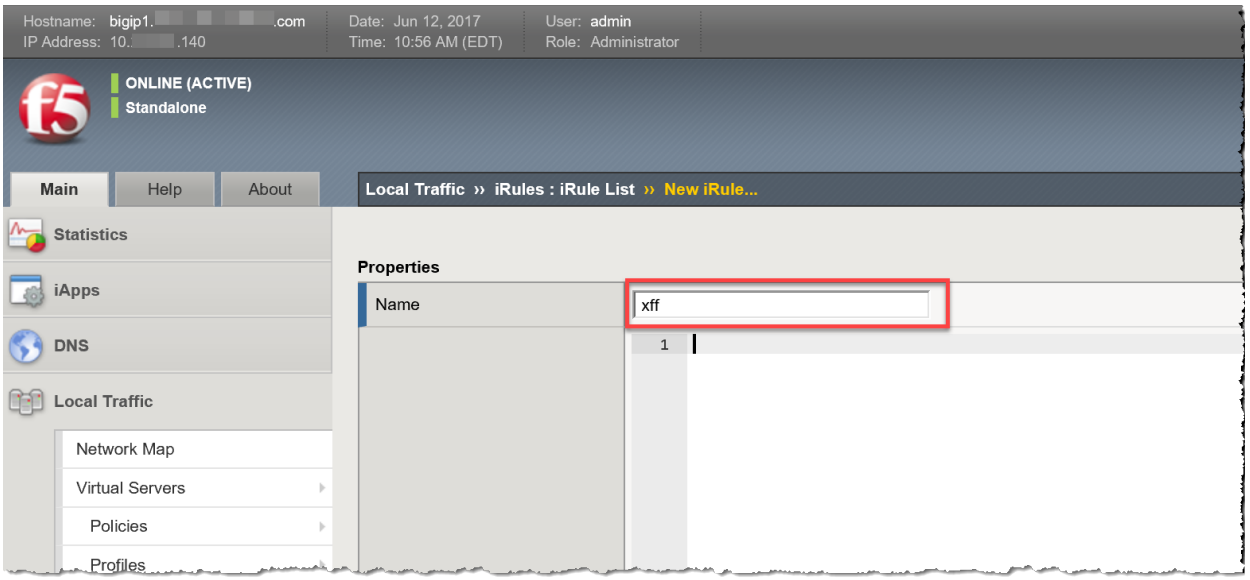
既存の iRule を使用する場合は、ここに記載されている情報を使用して変更できます。

F5 ロードバランサで XFF ヘッダーの iRule を作成するには、次の手順を実行します。

1. [メイン(Main)] タブで、[ローカルトラフィック(Local Traffic)] をクリックします。
2. [iRules] をクリックします。
3. [Create] ボタンをクリックします。



4. [名前(Name)]フィールドに、「xff」と入力します。



続行...

5. 次のテキストをコピーして、[定義（Definition）] フィールドに貼り付けます。

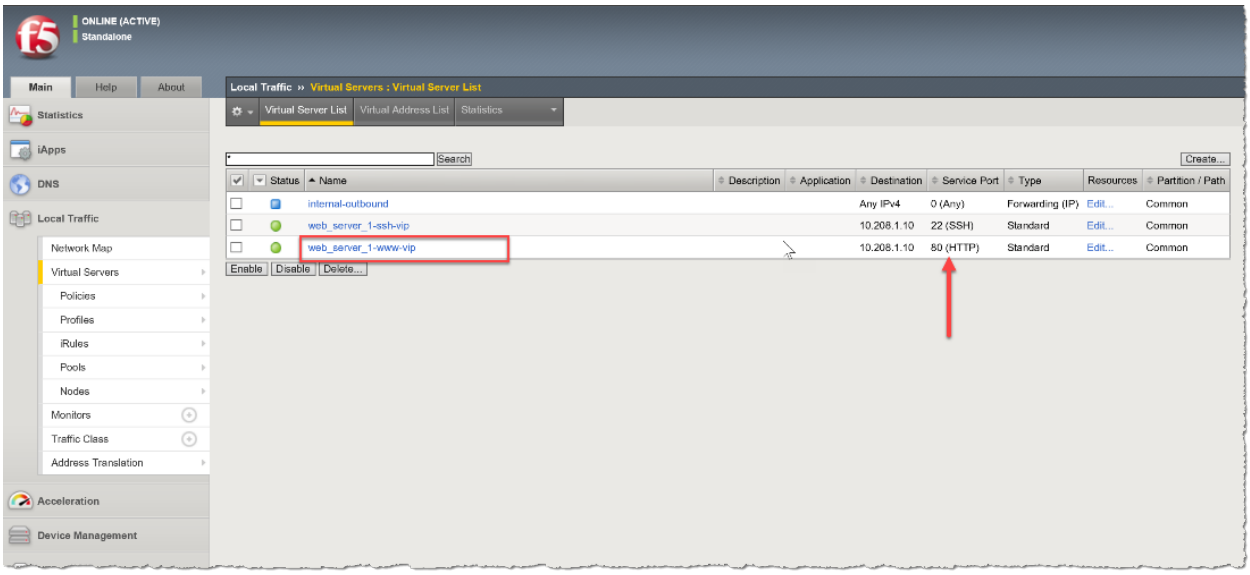
```
when CLIENT_ACCEPTED {
  if { [PROFILE::exists clientssl] } then {
    set client_protocol "https"
    set local_port 443
  } else {
    set client_protocol "http"
    set local_port 80
  }
}
when HTTP_REQUEST {
  if { [HTTP::header exists "X-Forwarded-For"] } {
    HTTP::header replace X-Forwarded-For "[HTTP::header X-Forwarded-For], [IP::client_addr]"
  } else {
    HTTP::header insert "X-Forwarded-For" [IP::client_addr]
  }
  if { [HTTP::header exists "X-Forwarded-Proto"] } {
    HTTP::header replace X-Forwarded-Proto "[HTTP::header X-Forwarded-Proto], $client_protocol"
  } else {
    HTTP::header insert "X-Forwarded-Proto" $client_protocol
  }
  if { [HTTP::header exists "X-Forwarded-Port"] } {
    HTTP::header replace X-Forwarded-Port "[HTTP::header X-Forwarded-Port], [TCP::client_port]"
  } else {
    HTTP::header insert "X-Forwarded-Port" [TCP::client_port]
  }
  if { [HTTP::header exists "X-Forwarded-Host"] } {
    HTTP::header replace X-Forwarded-Host "[HTTP::header X-Forwarded-Host], [IP::local_addr]:$local_port"
  } else {
    HTTP::header insert "X-Forwarded-Host" [IP::local_addr]:$local_port
  }
}
```

6. [終了（Finished）] ボタンをクリックして、保存して終了します。
7. 「仮想サーバーのリソースとしての iRule の追加」に進みます。

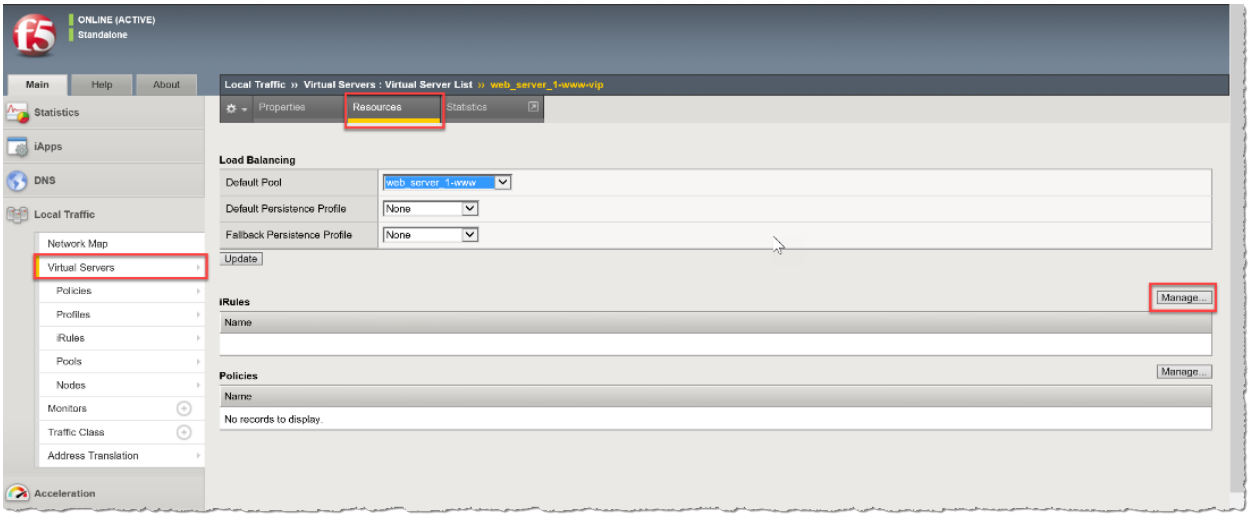
仮想サーバーのリソースとしての iRule の追加

仮想サーバーを有効にするには、新しい XFF iRule を F5 ロードバランサのリソースとして追加する必要があります。この手順により、ロードバランサが XFF ヘッダーを報告できるようになります。

1. [メイン(Main)] タブで、[ローカルトラフィック(Local Traffic)] をクリックします。
2. [仮想サーバー(Virtual Servers)] をクリックします。
3. [サービスポート(Service Port)] を検索し、デバイスで処理されるトラフィックを処理しているサービスポート 80(HTTP)または 443(HTTPS)を見つけます。[仮想サーバー名(Virtual Server Name)] をクリックします。

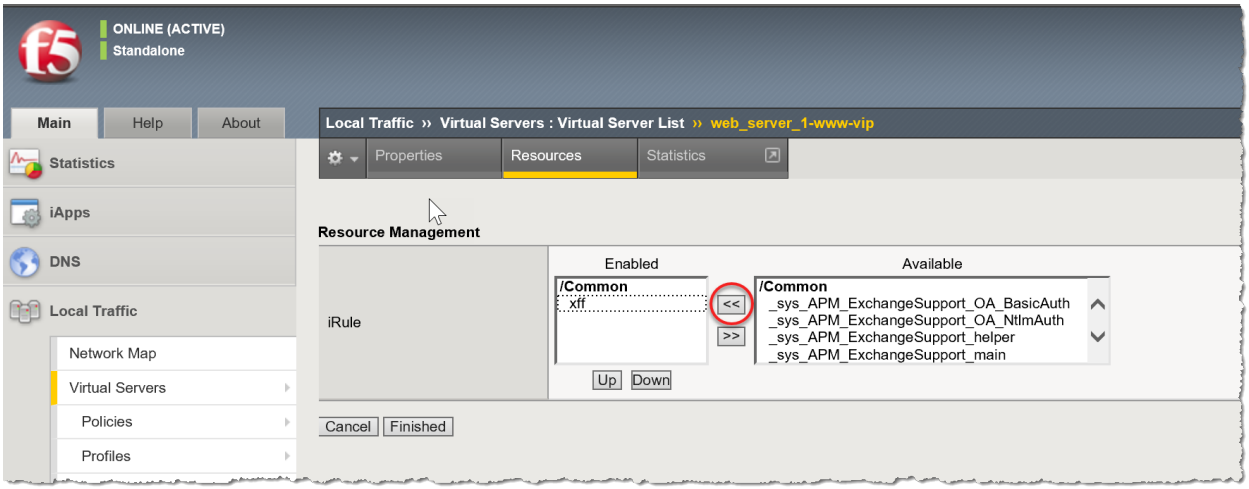


4. [リソース(Resources)] タブをクリックします。
5. [IRules] セクションで、[管理(Manage)] ボタンをクリックします。



6. 使用可能な iRules をスクロールして、新しい XFF iRule を見つけます。[XFF iRule] をクリックして選択します。

7. [<<] ボタンをクリックして、[有効（Enabled）] ボックスに XFF iRule を追加します。



8. [終了（Finished）] ボタンをクリックして、保存して終了します。

ネットワーク内のすべてのロードバランサの設定

ネットワークに複数のロードバランサが連結されている場合は、「FlowSensor での XFF 処理の有効化」に進む前に、「ロードバランサの設定」セクションの前述の手順を各ロードバランサに適用します。

各ロードバランサを設定すると、XFF 情報が保持されて付加されます。この設定では、FlowSensor は変換されたホストにある元のロードバランサの IP アドレスのみを報告します。

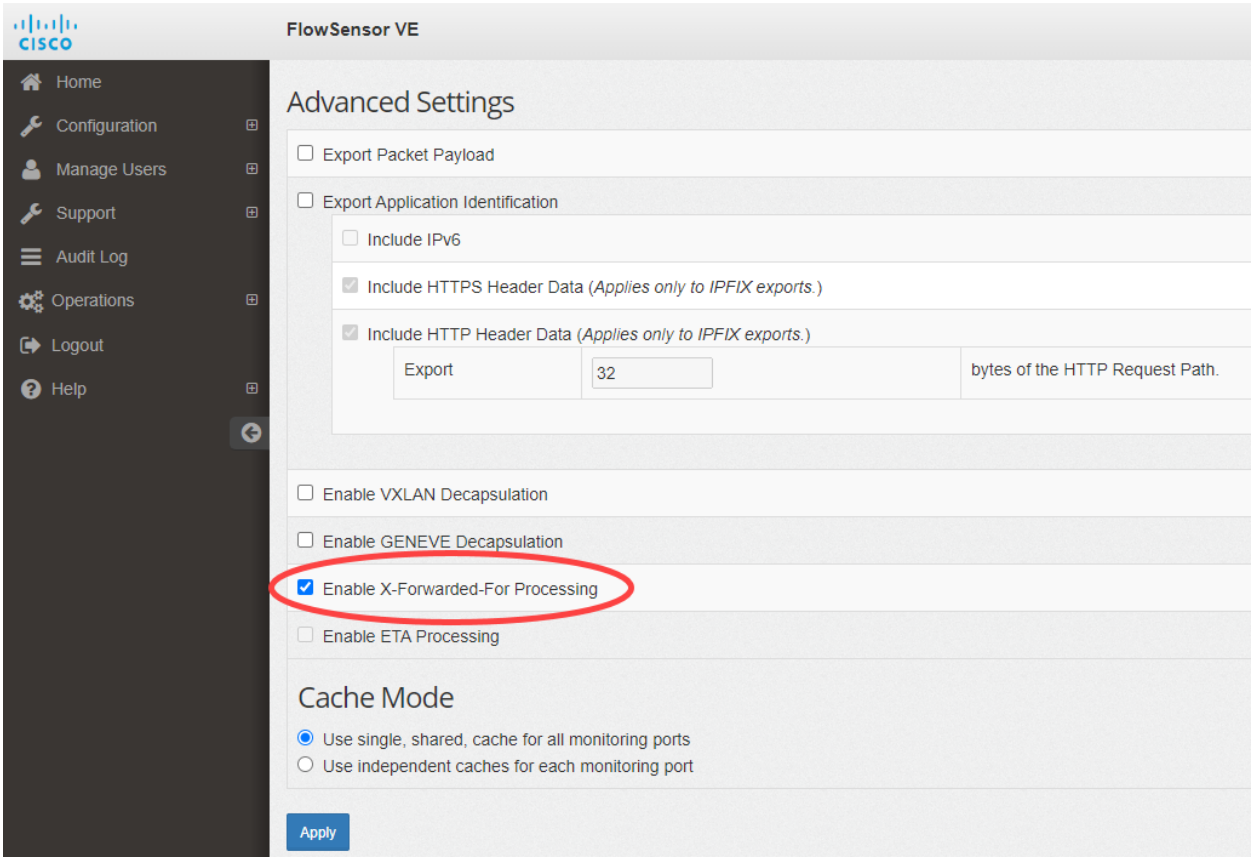
ロードバランサの設定手順には、次の手順が含まれます。

- HTTP の XFF オプションの無効化
- iRule の作成
- 仮想サーバーのリソースとしての iRule の追加

FlowSensor での XFF 処理の有効化

FlowSensor の XFF ヘッダーフィールドを処理するには、次の手順を実行します。

1. StealthWatch Management Console にログインします。
2. ⚙ ([グローバル設定(Global Settings)]) アイコン をクリックし、[集中管理(Central Management)] をクリックします。
3. フローセンサーの ••• ([省略記号(Ellipsis)]) アイコン をクリックし、[アプライアンス統計情報の表示(View Appliance Statistics)] をクリックします。フローセンサーの管理インターフェイスが開きます。
4. [設定(Configuration)] > [詳細設定(Advanced Settings)] をクリックします。
5. [X-Forwarded-For処理の有効化(Enable X-Forwarded-For-Processing)] チェックボックスをオンにします。



5. [適用(Apply)] ボタンをクリックします。
6. ロードバランサのサポートを受けているネットワーク内のすべての FlowSensor で、これらの手順を繰り返します。
7. 「設定の確認」に進みます。

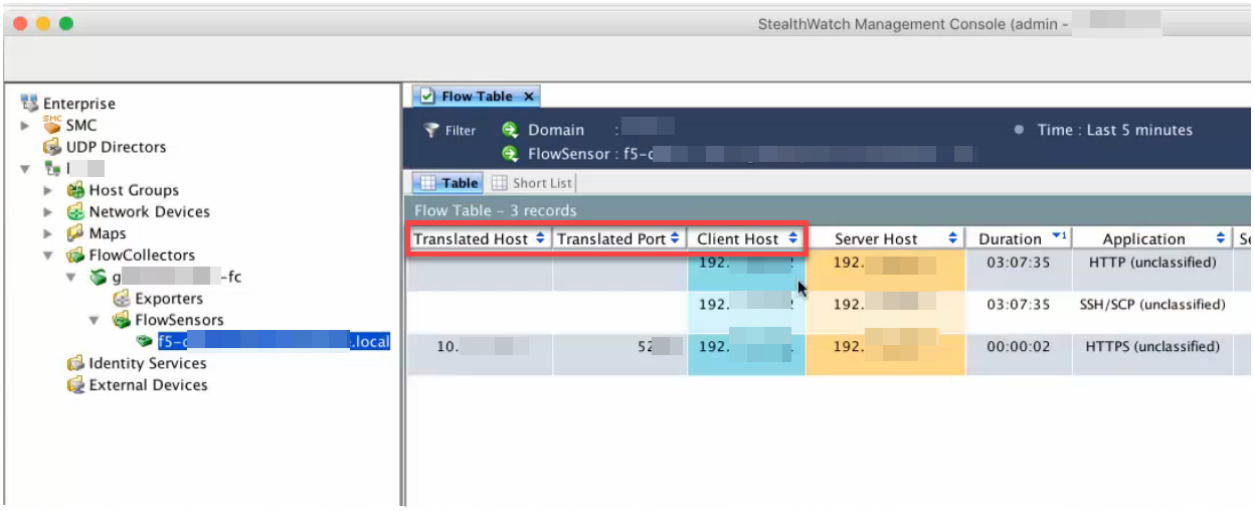
設定の確認

ロードバランサの設定を確認するには、Stealthwatch デスクトップクライアントまたは Stealthwatch Web アプリケーションにログインします。デスクトップクライアントは、ロードバランサの IP アドレスとポートを提供し、Web クライアントはロードバランサの IP アドレスを提供します。

Stealthwatch デスクトップクライアントの設定の確認

デスクトップクライアントのロードバランサの IP アドレスとポートを確認するには、次の手順を使用します。

1. F5 ロードバランサの前にあるクライアント上に X-Forwarded-For トラフィックを生成するには、ロードバランサの背後にある Web サーバーのブラウザを使用して、デスクトップクライアントにログインします。
2. [エンタープライズツリー(Enterprise Tree)] で FlowSensor を見つけます。FlowSensor の名前(または IP アドレス)を右クリックします。
3. [フロー(Flow)] > [フローテーブル(Flow Table)] をクリックします。
4. [変換されたホスト(Translated Host)] 列と [変換されたポート(Translated Port)] 列を確認して、F5 ロードバランサの IP アドレスとポートが表示されていることを確認します。
    - 変換されたホスト(ロードバランサの IP アドレス)
    - 変換されたポート(ロードバランサのポート)



フローテーブルへの列の追加(デスクトップクライアント)

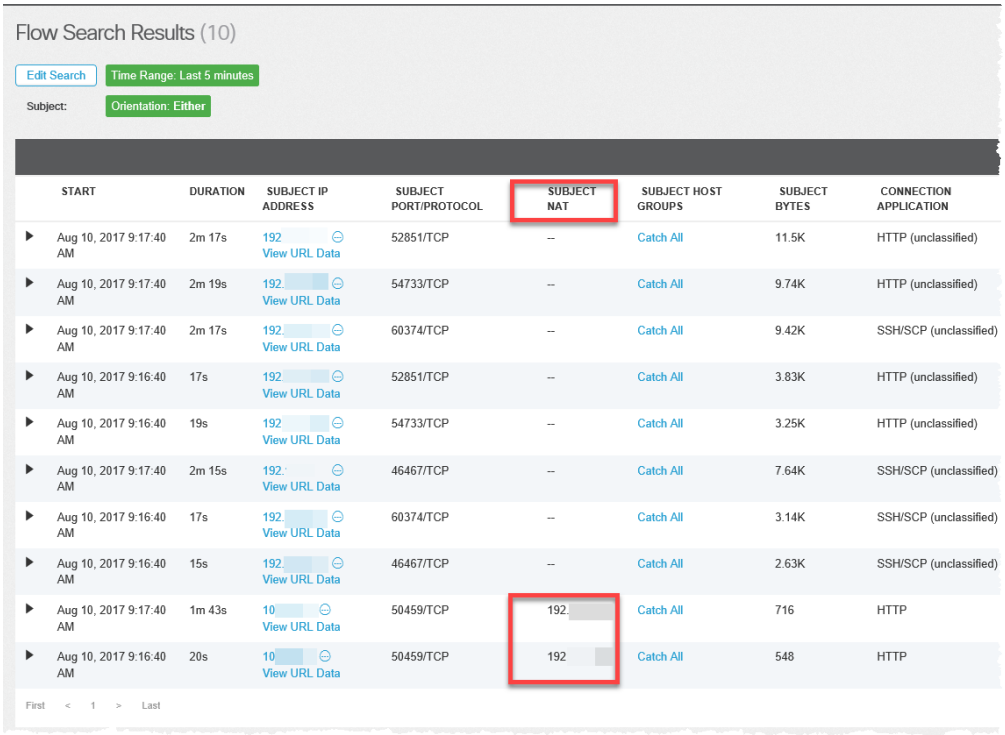
[変換されたホスト(Translated Host)] 列と [変換されたポート(Translated Port)] 列がデスクトップクライアントのフローテーブルに表示されない場合は、次の手順を実行します。

1. 任意の列を右クリックします。
2. リストをスクロールします。T の列に到達するまで、[追加(More)] を選択します。
3. [変換されたホスト(Translated Host)] と [変換されたポート(Translated Port)] をクリックして、フローテーブルに追加します。

Stealthwatch Web アプリケーションの設定の確認

Web アプリケーションのロードバランサの IP アドレスを確認するには、次の手順を使用します。変換されたポートは、Web アプリケーションでは使用できません。ポートを確認するには、「SMC デスクトップクライアントの設定の確認」を参照してください。

1. （F5 ロードバランサの背後にある）サーバー上の Web ページを開きます。
2. SMC にログインします。
3. [分析（Analyze）] > [フロー検索（Flow Search）] をクリックします。
4. [検索（Search）] をクリックします。
5. フロー検索の結果にフローが表示されたら、[列の管理（Manage Columns）] をクリックします。
6. チェックボックスをオンにして、[ピアNAT（Peer NAT）] と [サブジェクトNAT（Subject NAT）] にチェックマークを追加します。
7. [設定（Set）] をクリックします。
8. ロードバランサの IP アドレスが [ピアNAT（Peer NAT）] 列または [サブジェクトNAT（Subject NAT）] 列に表示されていることを確認します。
   この列は、フローの方向によって決まります。



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