



# CHAPTER 14

## NetFlow

この章では、Netflow に関する問題を識別して解決する方法について説明します。

この章は、次の内容で構成されています。

- 「NetFlow 情報」(P.14-1)
- 「NetFlow トラブルシューティング コマンド」(P.14-2)
- 「NetFlow の一般的な問題」(P.14-3)

## NetFlow 情報

NetFlow は、IP トラフィックを評価し、IP トラフィックがどこでどのようにして流れているかを理解することを可能にするテクノロジーです。NetFlow は、アカウントリング、ネットワーク モニタリング、およびネットワーク プランニングで使用できるデータを収集します。

フローとは、ソース インターフェイス（またはサブインターフェイス）に到達し、一連の基準に一致するパケットの一方向ストリームです。同じ送信元/宛先 IP アドレス、送信元/宛先ポート、プロトコル インターフェイス、サービス クラスを持つすべてのパケットがグループ化されて 1 つのフローに入れられ、パケットとバイトが集計されます。これにより、大量のネットワーク情報が NetFlow キャッシュと呼ばれるデータベースに凝縮されます。

フローは、収集する基準を定義することにより作成します。フロー情報から、次の情報がわかります。

- 送信元アドレスから、誰がトラフィックを送信したかがわかります。
- 宛先アドレスから、誰がトラフィックを受信するかがわかります。
- ポートは、トラフィックを使用するアプリケーションの特性を示します。
- サービスクラスからは、トラフィックの優先度がわかります。
- デバイス インターフェイスから、トラフィックがネットワーク デバイスによってどのように使用されるかがわかります。
- 集約されたパケットとバイトは、トラフィックの量を示します。

フロー レコードは、フロー内のパケット、フローごとに収集されるカウンタのタイプなどの NetFlow が収集する情報を定義します。新しいフロー レコードを自分で定義することもできれば、定義済みの Nexus 1000V フロー レコードを使用することもできます。

NetFlow の設定の詳細については、『Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)』を参照してください。

## NetFlow トラブルシューティング コマンド

ここに挙げるコマンドは、NetFlow 関連の問題のトラブルシューティングに使用できるものです。

- **debug logfile filename** : このコマンドは、次のデバッグ コマンドの出力をブートフラッシュ内に保存されるファイルにリダイレクトします。
  - **debug nfm all**
  - **debug sf\_nf\_srv all**
- **vemdebug netflow dump policy** : このコマンドでは、VEM 上のインターフェイスに正しいポリシーがインストールされているかどうかを検証できます。このコマンドの出力は、vemlog 内部バッファに送られます。出力に通常どおりのキャッシュ タイプが表示され、正しいキャッシュ サイズとキャッシュ タイマー値が表示されることを確認してください。

```
Apr 14 12:20:51.504410      19  2    2  16  Debug Port 49 has 1
monitors for dir INPUT traffic IPV4
Apr 14 12:20:51.504412      20  2    2  16  Debug Flow Monitor fml:
Apr 14 12:20:51.504413      21  2    2  16  Debug Description:
fml
Apr 14 12:20:51.504413      22  2    2  16  Debug Monitor ID:
3
Apr 14 12:20:51.504413      23  2    2  16  Debug Cache:
Apr 14 12:20:51.504414      24  2    2  16  Debug Type:
normal
Apr 14 12:20:51.504414      25  2    2  16  Debug Status:
allocated
Apr 14 12:20:51.504415      26  2    2  16  Debug Size:
256 entries
Apr 14 12:20:51.504415      27  2    2  16  Debug Inactive
Timeout: 15 secs
Apr 14 12:20:51.504416      28  2    2  16  Debug Active
Timeout: 1800 secs
```

- **vemdebug netflow dump pakstore** : このコマンドは、インターフェイス上のポリシーについて、pakstore の使用状況をダンプします。出力は、vemlog 内部バッファに送られます。出力に正しいモニタ名とインターフェイスが表示されることを確認してください。

```
Apr 14 12:25:30. 29787      260  0    2  16  Debug Pak Store for
Client: fml
Apr 14 12:25:30. 29793      266  0    2  16  Debug Pak Store for
Client: LTL49
```

- **vemlog debug sfnetflow\_cache all**
- **vemlog debug sfnetflow\_config all**
- **vemlog debug sfnetflow\_flowapi all**

これらのコマンドで、VEM 上のポリシー インストールの NetFlow デバッグが行えます。DPA からの要求を開いて、検証し、コミットするすべての PDL セッションについて、デバッグ メッセージが出力されます。

- **vemlog debug sfnetflow all**

このコマンドで、VEM 上の Netflow ポリシーのパケット パスのデバッグが行えます。NetFlow ポリシーにヒットしたすべてのパケットについて、デバッグ メッセージが出力されます。このコマンドの使用に当たっては、十分注意してください。多数のデバッグ メッセージで大量のトラフィックが発生する場合があります。

次のコマンドでは、NFM プロセス ランタイム設定エラーに関する情報が収集できます。

- **show flow internal event-history errors**

- **show flow internal event-history msgs**
- **show flow internal ddb b**
- **show flow internal mem-stats** (メモリの使用状況とリークのデバッグのために)

次のコマンドでは、sf\_nf\_srv プロセス ラインタイム情報が収集できます。

- **show system internal sf\_nf\_srv event-history errors**
- **show system internal sf\_nf\_srv event-history msgs**
- **show system internal sf\_nf\_srv pdl detailed**
- **show system internal sf\_nf\_srv mem-stats** (メモリの使用状況とリークのデバッグのために)

## NetFlow の一般的な問題

VSM 上での NetFlow の設定に関する一般的な問題は、次のような操作を行おうとしたときに発生します。

- 未定義のレコード、エクスポート、サンプラー、またはモニタを使用した。
- 無効なレコード、エクスポート、サンプラー、またはモニタを使用した。
- レコード、エクスポート、サンプラー、またはモニタをインターフェイスに適用したあとに修正した。
- インターフェイス上のモニタを設定し、それが VEM のメモリ不足を発生させ、検証エラーが発生した。
- NetFlow をポート チャネルで使用した。NetFlow は、ポート チャネルでサポートされていません。

さらに、エクスポートで設定されている UDP ポートと NetFlow Collector でのリスンが有効になっているポートが一致しない場合にも設定エラーが発生します。

## ポリシー検証エラーのデバッグ

VSM 上での何らかの処理が原因で発生したポリシー検証の失敗をデバッグするには、次の手順を実行します。

- 
- ステップ 1** **debug nfm all** コマンドを実行します。
  - ステップ 2** **debug sf\_nf\_srv\_all** コマンドを実行します。
  - ステップ 3** Telnet SSH セッション バッファをファイルに保存します。
  - ステップ 4** **ip flow mon monitor name direction** コマンドを実行します。  
コマンドがもう一度実行され、デバッグ トレースがコンソールに出力されます。
- 

ポリシー検証手順を使用して、フロー レコードの定義やエクスポート機能のトレースなどの操作のログを収集することもできます。

## 統計情報エクスポートのデバッグ

NetFlow 統計情報のエクスポートに関する問題をデバッグするには、次のガイドラインに従ってください。

- 宛先 IP アドレスが VSM から到達できることを確認します。
- エクスポータに設定されている UDP が NetFlow Collector によって使用されるものと一致していることを確認します。
- **show flow exporter** コマンドを実行して、エクスポータの統計情報を表示し、VSM 上でドロップが発生していないか確認します。