



SD-Routing デバイスのモニタリング

First Published: 2024-03-28

Last Modified: 2024-08-27

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

SD-Routing デバイスでのアプリケーション パフォーマンス モニタリング 1

ここで章マップを参照します 1

アプリケーション パフォーマンス モニターに関する情報 1

アプリケーション パフォーマンス モニターのワークフロー 2

アプリケーション パフォーマンス モニタリングの前提条件 2

制限事項 2

アプリケーション パフォーマンス モニターの設定 2

SD-Routing デバイスでのアプリケーション パフォーマンス モニタリングの設定 3

アプリケーション パフォーマンス モニターの確認 4

アプリケーション パフォーマンス モニターの機能情報 5

CHAPTER 2

SD-Routing デバイスでの Flexible NetFlow アプリケーションの可視性 7

Flexible NetFlow アプリケーションの可視性に関する情報 7

SAIE フローを使用した Flexible NetFlow アプリケーションの可視性の前提条件 8

制限事項 8

Flexible NetFlow アプリケーションの可視性の有効化 8

Flexible NetFlow アプリケーションの可視性の設定 9

Cisco SD-WAN Manager を使用した Flexible NetFlow アプリケーションの可視性の確認 10

Flexible NetFlow アプリケーションの可視性の確認 11

SD-Routing デバイスでの Flexible NetFlow アプリケーションの可視性の機能情報 12

CHAPTER 3**SD-Routing デバイスのフローレベル Flexible NetFlow サポート 15**

- フローレベル Flexible NetFlow について 15
- SD-Routing デバイスの Flexible NetFlow モニタリングのタイプ 16
- フローレベル Flexible NetFlow の利点 16
- フローレベル Flexible NetFlow コンポーネント 16
- SD-Routing デバイスで Flexible NetFlow モニターを有効にする方法 17
- フローレベル Flexible NetFlow を設定するための前提条件 18
- フローレベル Flexible NetFlow の設定に関する制限事項 18
- EzPM プロファイルを使用した SD-Routing デバイスでのフローレベル FNF の設定 18
- フローモニターを使用したフローレベル Flexible NetFlow の設定 19
- Security Unified Logging について 21
- デバイスでの Security Unified Logging の設定に関する制限事項 21
- EzPM プロファイルを使用した SD-Routing デバイスでの Security Unified Logging の設定 21
- フローモニターを使用した SD-Routing デバイスでの Security Unified Logging の設定 22
- SD-Routing デバイスのフローレベル Flexible NetFlow の有効化 24
 - 設定グループの作成 24
 - デバイスの関連付けと設定グループの展開 25
 - SD-Routing デバイスでのフローレベルデータのモニター 25
 - SD-Routing デバイスでの Security Unified Logging データのモニター 25

CHAPTER 4**SD-Routing デバイスでのパケットキャプチャ 27**

- パケットキャプチャについて 27
- パケットキャプチャの設定 27
 - 前提条件 27
 - 制限事項 27
 - パケットキャプチャの設定 28
- SD-Routing のパケットキャプチャの機能情報 29

CHAPTER 5**SD-Routing デバイスでの速度テスト 31**

- 速度テストに関する情報 31

速度テストの前提条件	31
インターネット速度テストの実行	31
速度テストの確認	32
速度テストの問題のトラブルシューティング	32
Cisco SD-WAN Manager を使用した SD-Routing デバイスでの速度テストに関する機能情報	33

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© Cisco Systems, Inc. All rights reserved.



CHAPTER 1

SD-Routing デバイスでのアプリケーション パフォーマンス モニタリング

この章では、SD-Routing デバイスでアプリケーションのパフォーマンスをモニターする方法について説明します。ここで説明する内容は、次のとおりです。

- [ここで章マップを参照します, on page 1](#)
- [アプリケーション パフォーマンス モニターに関する情報, on page 1](#)

ここで章マップを参照します

アプリケーションパフォーマンスモニターに関する情報

アプリケーションパフォーマンスモニター機能は、インテントベースのパフォーマンスモニターを設定できる、簡素化されたフレームワークです。この機能を使用すると、クライアントセグメント、ネットワークセグメント、サーバーセグメントでフィルタリングされたエンドツーエンドのアプリケーション パフォーマンスをリアルタイムで表示できます。この情報は、アプリケーションのパフォーマンスを最適化するのに役立ちます。

アプリケーションパフォーマンスモニターは、特定のトラフィックの評価指標を収集するのに使用される、事前定義された設定です。

アプリケーションパフォーマンス モニタリングの主なコンセプト

- **モニタリングプロファイル:** プロファイルは、コンテキストに対して有効または無効にすることができる、事前定義された一連のトラフィックモニターです。この機能の一部として、SD-Routing パフォーマンス プロファイルに、Cisco Catalyst SD-Routing インターフェイスを通過するトラフィックをモニタリングするためのアプリケーション応答時間（ART）集約モニターが含まれるようになりました。SD-Routing パフォーマンス プロファイルには、インテントに基づいてトラフィックをフィルタリングする専用ポリシーがあります。
- **コンテキスト:** インターフェイスの入力トラフィックと出力トラフィックの両方にアタッチされるパフォーマンス モニター ポリシー マップに相当します。コンテキストには、有効に

する必要があるトラフィックモニターに関する情報が含まれます。インターフェイスにコンテキストがアタッチされると、入力トラフィックと出力トラフィックにそれぞれ1つずつ、合計2つのポリシーマップが作成されます。トラフィックモニターで指定されている方向に基づいてポリシーマップがアタッチされると、トラフィックのモニターが開始されます。

アプリケーション パフォーマンス モニターのワークフロー

パフォーマンスモニターは、ダイレクトインターネットアクセス（DIA）インターフェイスでのみ有効にできます。モニタリング対象は、DIA インターフェイスで送受信されるトラフィックのパフォーマンスです。その後、さまざまな show コマンドを使用することで、モニタリングしているアプリケーションの詳細を表示できます。

アプリケーション パフォーマンス モニタリングの前提条件

- Cisco IOS XE Catalyst SD-Routing デバイスの最小ソフトウェアバージョン: Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a

制限事項

アプリケーション パフォーマンス モニターの制限事項は次のとおりです。

- アプリケーション パフォーマンス モニターは、SD-Routing デバイスで ART のみをサポートします。
- このリリースでは、ダイレクトインターネットアクセス（DIA）シナリオのみがサポートされています。
- パフォーマンスのモニタリングは、IPv4 トラフィックでのみサポートされます。IPv6 トラフィックはサポートされていません。
- アプリケーション パフォーマンス モニターは、デバイス上のマルチ アプリケーション集約モニターをサポートしていません。
- APM で使用されるクラスマップは、最大2つのレイヤクラスマップのみをサポートし、3つ以上のレイヤクラスマップをサポートしません。
- Cisco SD-WAN Manager では、SD-Routing デバイスの APM を設定するために、CLI ベースの設定グループのみがサポートされています。

アプリケーション パフォーマンス モニターの設定

DIA インターフェイスでアプリケーション パフォーマンス モニターを有効にし、ART のトラフィック メトリックをモニターできます。

DIA インターフェイスでのパフォーマンスの有効化

次の例は、SD-Routing application-aggregation プロファイルを使用してパフォーマンスモニターのコンテキストを設定する方法を示しています。この設定により、ART トラフィックメトリックのモニタリングが有効になり、特定のインターフェイスに適用されます。

```
class-map match-any APP_PERF_MONITOR_APPS_0
  match protocol attribute application-group amazon-group
  match protocol attribute application-group box-group
  match protocol attribute application-group concur-group
  match protocol attribute application-group dropbox-group
  match protocol attribute application-group google-group
  match protocol attribute application-group gotomeeting-group
  match protocol attribute application-group intuit-group
  match protocol attribute application-group ms-cloud-group
  match protocol attribute application-group oracle-group
  match protocol attribute application-group salesforce-group
  match protocol attribute application-group sugar-crm-group
  match protocol attribute application-group webex-group
  match protocol attribute application-group zendesk-group
  match protocol attribute application-group zoho-crm-group
class-map match-any APP_PERF_MONITOR_FILTERS      --- class-map max 2 layer supported, 3 or
  more layer class-map not supported for APM feature
  match class-map APP_PERF_MONITOR_APPS_0
!
```

この設定例では、パフォーマンスモニターのコンテキストを設定する方法を示します。

```
performance monitor context APP_PM_POLICY profile application-aggregation
  exporter destination local-controller source Null0
  traffic-monitor art-aggregated class-and APP_PERF_MONITOR_FILTERS interval-timeout 300
  sampling-interval 100
```

この設定例では、インターフェイスでパフォーマンスモニターのコンテキストを有効にする方法を示します。

```
interface GigabitEthernet1                                --- DIA
interface(s)
  performance monitor context APP_PM_POLICY
```

SD-Routing デバイスでのアプリケーションパフォーマンス モニタリングの設定

設定グループを作成するには、次の手順を実行します。

Procedure

- | | |
|---------------|---|
| Step 1 | [Cisco IOS XE Catalyst SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] > [Add CLI based Configuration Group] の順に選択します。 |
| Step 2 | [Add CLI based Configuration Group] ポップアップ ダイアログ ボックスで、設定グループ名を入力します。 |
| Step 3 | [Solution Type] ドロップダウンリストをクリックし、SD-Routing デバイスのソリューションタイプとして [sd-routing] を選択します。 |
| Step 4 | [Description] フィールドに機能の説明を入力します |

- Step 5** [Next] をクリックします。
- Step 6** [Load Running Config from Reachable Device] ドロップダウンリストをクリックし、実行構成を選択するか、テキストボックスに構成 CLI を追加します。
- Step 7** [Save] をクリックします。
- Step 8** 設定グループ名の横にある [...] をクリックし、[Edit] を選択します
- Step 9** [Associated Devices] をクリックします。
- Step 10** 1 つ以上のデバイスを選択し、[Deploy] をクリックします

Note

アプリケーション パフォーマンス モニタリングは、パフォーマンス モニター コンテキスト プロファイル およびフローモニターがインターフェイスに接続されている場合、パフォーマンス モニター コンテキスト プロファイル およびフローモニターの変更をサポートしません。

- Step 11** [Configuration] > [Configuration Groups] > [Deploy] をクリックします
- Step 12** 設定グループ名の横にある [...] をクリックし、[Edit] を選択してパフォーマンス モニター コンテキスト プロファイルとフローモニターを変更し、インターフェイスに再接続します。
- Step 13** [Deploy] をクリックします。
- Step 14** [Save] をクリックします。

アプリケーション パフォーマンス モニターの確認

SD-Routing デバイスのアプリケーション パフォーマンス モニターの設定を確認するには、**show performance monitor cache monitor** コマンドを使用します。

```
Device#show performance monitor cache monitor APP_PM_POLICY-art_agg detail format record
```

```
Monitor: APP_PM_POLICY-art_agg
```

```
Data Collection Monitor:
```

```
CAT-art-art-aggregated CTX:0 ID:2947958679|2000002 Epoch:0
```

```
Max number of records: 675000
```

```
Current record count: 7
```

```
High Watermark: 13
```

```
Record added: 14
```

```
Record aged: 7
```

```
Record failed to add: 0
```

```
Synchronized timeout (secs): 300
```

```

FLOW DIRECTION: Output
TIMESTAMP MONITOR START: 14:10:00.000
FLOW OBSPOINT ID: 4294967298
INTERFACE OVERLAY SESSION ID OUTPUT: 0
IP VPN ID: 65535
APPLICATION NAME: layer7 share-point
connection server resp counter: 1477
connection to server netw delay sum: 10822 < --- SND_ samples
connection to server netw delay min: 100
connection to server netw delay max: 103
connection to client netw delay sum: 3559 < --- CND_ samples
connection to client netw delay min: 20
connection to client netw delay max: 198
connection application delay sum: 936

```

```

connection application delay min:      0
connection application delay max:     122
connection responder retrans packets: 2    <---- lost_samples
connection to server netw jitter mean: 0
connection count new:                 108    < ---- SND/CND_counts
connection server packets counter:    2018    <---- total_samples

Latency(SND  ms) = SND_samples/ SND/CND_counts
Latency(CND  ms) = CND_samples/ SND/CND_counts
Loss ratio = lost_samples /total_samples

```

アプリケーションパフォーマンス モニターの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、<https://cfngng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 1: アプリケーションパフォーマンス モニターの機能情報

機能名	リリース	機能情報
Cisco SD-Routing アプリケーションパフォーマンス モニター	Cisco IOS XE リリース 17.13.1a	アプリケーションパフォーマンス モニター機能では、インテントベースのパフォーマンスモニターを設定できる、簡素化されたフレームワークが導入されています。このフレームワークを使用すると、クライアントセグメント、ネットワークセグメント、ネットワークセグメントでフィルタリングされたエンドツーエンドのアプリケーション パフォーマンスをリアルタイムで表示できます。



CHAPTER 2

SD-Routing デバイスでの Flexible NetFlow アプリケーションの可視性

この章では、SD-Routing デバイスで Flexible NetFlow アプリケーションの可視性を設定する方法について説明します。ここで説明する内容は、次のとおりです。

- [Flexible NetFlow アプリケーションの可視性に関する情報, on page 7](#)
- [SAIE フローを使用した Flexible NetFlow アプリケーションの可視性の前提条件, on page 8](#)
- [制限事項, on page 8](#)
- [Flexible NetFlow アプリケーションの可視性の有効化, on page 8](#)
- [Flexible NetFlow アプリケーションの可視性の設定, on page 9](#)
- [SD-Routing デバイスでの Flexible NetFlow アプリケーションの可視性の機能情報, on page 12](#)

Flexible NetFlow アプリケーションの可視性に関する情報

Flexible NetFlow (FNF) は、デバイスを通過するパケットの統計情報を提供します。WAN または LAN インターフェイス上の FNF は、アプリケーションインテリジェンスエンジン (SAIE) を使用して、Cisco SD-Routing デバイスの WAN または LAN インターフェイスに到達するすべてのトラフィック (入力と出力の両方) を可視化します。アプリケーションインテリジェンスエンジンフローは、基本ヘッダー情報を超えてパケットを調べる機能を提供します。SAIE フローは、特定のパケットの内容を判別し、その情報を統計目的で記録するか、パケットに対してアクションを実行します。



Note FNF は、WAN または LAN インターフェイスにのみ適用できます。WAN インターフェイスと LAN インターフェイスの両方に適用しないでください。

デバイスで Flexible NetFlow アプリケーションの可視性を有効にするには、次の方法で Cisco SD-WAN Manager を使用してフローデータ集約を有効にする必要があります。

- パフォーマンス モニター コンテキスト プロファイル (推奨される方法)
- フローエクスポートをローカルコントローラへ

**Note**

既存の FNF モニターがある場合は、新しいパフォーマンスモニターを追加することによるパフォーマンスへの影響を回避するために、既存の FNF モニターのフローエクスポートとしてフローエクスポートをローカルコントローラに追加します。それ以外の場合は、パフォーマンスモニターコンテキストプロファイルを使用できます。

SAIE フローを使用した Flexible NetFlow アプリケーションの可視性の前提条件

前提条件は次のとおりです。

- デバイスが Cisco IOS XE 17.13.1a イメージを実行していることを確認します。
- Cisco SD-WAN Manager でフローデータ集約が有効になっていることを確認します。

制限事項

制限事項は次のとおりです。

- Cisco SD-WAN Application Intelligence Engine (SAIE) による集約統計のみがサポートされます。
- オンデマンドのトラブルシューティングはサポートされません。
- コンテキストプロファイルと FNF エクスポートが同じ名前を使用している場合、**show flow exporter name** コマンドはそのうちの 1 つだけを表示します。
- パフォーマンスモニターコンテキストプロファイルおよびローカルコントローラへのフローエクスポートは、コンテキストプロファイルまたはローカルコントローラへのフローエクスポートのいずれかのみを使用できます。そうでない場合は、パケットをダブルカウントします。
- CLI ベースの設定グループのみがサポートされています。

Flexible NetFlow アプリケーションの可視性の有効化

デバイスのコンテキストプロファイルまたはフローエクスポートを使用して、FNF アプリケーションの可視性を有効にできます。

コンテキスト プロファイル オプション1の設定

このオプションを使用することをお勧めします。次に、デバイスでコンテキストプロファイルを使用してフローデータ集約を有効にする例を示します。

```
performance monitor context FNF profile app-visibility
  exporter destination local-controller source Null0
  traffic-monitor app-visibility-stats
```

```
interface GigabitEthernet5
  performance monitor context FNF
```

デバイスは、インターフェイスに接続されると、このプロファイルを FNF フローモニターに適用します。

フロー エクスポート オプション2の設定

次に、デバイスでフローエクスポートを使用してフローデータ集約を有効にする例を示します。

```
flow exporter fnf-1
  destination local controller
  export-protocol ipfix
  template data timeout 300
  option interface-table timeout 300
  option vrf-table timeout 300
  option application-table timeout 300
  option application-attributes timeout 300
```

```
flow record fnf-app-visibility
  match routing vrf input
  match interface input
  match interface output
  match application name
  collect counter bytes long
  collect counter packets long
```

```
flow monitor fnf-app-visibility
  exporter fnf-1
  cache timeout inactive 10
  cache timeout active 60
  cache entries 5000
  record fnf-app-visibility
```

```
interface GigabitEthernet5
  ip flow monitor fnf-app-visibility input
  ip flow monitor fnf-app-visibility output
  ipv6 flow monitor fnf-app-visibility input
  ipv6 flow monitor fnf-app-visibility output
```

Flexible NetFlow アプリケーションの可視性の設定

SD-Routing デバイスで FNF アプリケーションの可視性を設定するには、次の手順を実行します。

Procedure

-
- Step 1** [Cisco IOS XE Catalyst SD-WAN Manager] のメニューから、[Configuration] > [Configuration Groups] > [Add CLI based Configuration Group] の順に選択します。
- Step 2** [Add CLI configuration Group] ポップアップ ダイアログ ボックスで、設定グループ名を入力します。
- Step 3** [Solution Type] ドロップダウンリストをクリックし、SD-Routing デバイスのソリューションタイプとして [sd-routing] を選択します。
- Step 4** [Description] フィールドに機能の説明を入力します
- Step 5** [Next] をクリックします。
- [Feature Profiles] タブと [Associated Device] タブを含む新しい設定グループページが表示されます。
- Step 6** [Feature Profiles] セクションで、対応する設定を追加します。
- Step 7** [Save] をクリックして、コンフィギュレーションを保存します。
- Step 8** 設定グループ名の横にある [...] をクリックし、[Edit] を選択します
- Step 9** [Associated Devices] をクリックします。
- Step 10** 1 つ以上のデバイスを選択し、[Deploy] をクリックします
- Note**
Flexible Netflow は、パフォーマンス モニター コンテキスト プロファイルおよびフロー モニターがインターフェイスに接続されている場合、パフォーマンス モニター コンテキスト プロファイルおよびフロー モニターの変更をサポートしません。
- Step 11** [Configuration] > [Configuration Groups] > [Deploy] をクリックします
- Step 12** 設定グループ名の横にある [...] をクリックし、[Edit] を選択してパフォーマンス モニター コンテキスト プロファイルとフロー モニターを変更し、インターフェイスに再接続します。
- Step 13** [Deploy] をクリックします。
- Step 14** [Save] をクリックします。
-

Cisco SD-WAN Manager を使用した Flexible NetFlow アプリケーションの可視性の確認

FNF アプリケーションの可視性を確認するには、次の手順を実行します。

Procedure

-
- Step 1** Cisco SD-WAN Manager のメニューから [Monitor] > [Devices] の順に選択し、リストから SD-Routing デバイスを選択します。
- Step 2** 左側のペインで、[SAIE Applications] > [Filter] の順に選択します。

- Step 3** [Filter By] ダイアログボックスで、VPN を選択します。
- Step 4** [Traffic Source] で、[LAN] または [Remote Access] チェックボックスをオンにします。
- Step 5** [Search] をクリックして、選択したフィルタに基づいてフローレコードを検索します。
フローレコードが表示されます。
- Step 6** [Export] をクリックして、フローレコードをローカルシステムにエクスポートします。
- Step 7** [Reset All] をクリックして、すべての検索フィルタをリセットします。

Flexible NetFlow アプリケーションの可視性の確認

SD-Routing FNF アプリケーションの可視性を計算するために使用される基本的なネットワークメトリックを確認するには、**show performance monitor context [profile name] configuration**、**show platform software td-l database content dta fnf-statistics**、および **show performance monitor context fnf traffic monitoring app-visibility-stats cache** コマンドを使用します。

```
Device #show performance monitor context fnf configuration
!=====
! Equivalent Configuration of Context fnf !
!=====
!Exporters
!=====
!
flow exporter fnf-1
description performance monitor context fnf exporter
destination local controller
export-protocol ipfix
template data timeout 300
option interface-table timeout 300 export-spread 0
option vrf-table timeout 300 export-spread 0
option application-table timeout 300 export-spread 0
option application-attributes timeout 300 export-spread 0
!
!Access Lists
!=====
!Class-maps
!=====
!Samplers
!=====
!Records and Monitors
!=====
!
flow record fnf-app-visibility-v4
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visibility-v4
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
```

```

cache timeout active 60
cache entries 5000
record fnf-app-visibility-v4
!
!
flow record fnf-app-visibility-v6
description ezPM record
match routing vrf input
match interface input
match interface output
match application name
collect counter bytes long
collect counter packets long
!
!
flow monitor fnf-app-visibility-v6
description ezPM monitor
exporter fnf-1
cache timeout inactive 10
cache timeout active 60
cache entries 5000
record fnf-app-visibility-v6
!
!Interface Attachments
!=====
interface GigabitEthernet5
ip flow monitor fnf-app-visibility-v4 input
ip flow monitor fnf-app-visibility-v4 output
ipv6 flow monitor fnf-app-visibility-v6 input
ipv6 flow monitor fnf-app-visibility-v6 output

Device# show performance context fnf traffic-monitor app-visibility stats cache
Monitor fnf-app-visibility-v4

```

```

Cache type: Normal (platform cache)
Cache size : 10000
Current entries: 2
High Watermark: 4

Flows added: 6
Flows aged: 4
- Inactive timeout (10sec) 4

```

IP VRF	ID INPUT	INFE INPUT	INTF OUTPUT	APP Name	bytes long	pkts long
=====	=====	=====	=====	=====	=====	=====
1	(1)	Gi3	Gi5	layer7 share-point	1517476	3277
1	(1)	Gi5	Gi3	layer7 share-point	1306568	3463

SD-Routing デバイスでの Flexible NetFlow アプリケーションの可視性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 2: SD-Routing デバイスでの Flexible NetFlow アプリケーションの可視性の機能情報

機能名	リリース	機能情報
SD-Routing デバイスでの Flexible NetFlow アプリケーションの可視性	Cisco IOS XE リリース 17.13.1a	Flexible NetFlow (FNF) の機能は、デバイスを通過するパケットの統計情報を提供し、トンネルまたはサービス VPN の識別に役立ちます。また、SD-Routing Application Intelligence Engine (SAIE) を使用して、Cisco SD-Routing デバイスの VPN0 を通過するすべてのトラフィックを可視化します。



CHAPTER 3

SD-Routing デバイスのフローレベル Flexible NetFlow サポート

この章では、SD-Routing デバイスでフローレベル Flexible NetFlow サポートを設定する方法について説明します。ここで説明する内容は、次のとおりです。

- フローレベル Flexible NetFlow について, on page 15
- SD-Routing デバイスの Flexible NetFlow モニタリングのタイプ, on page 16
- フローレベル Flexible NetFlow の利点, on page 16
- フローレベル Flexible NetFlow コンポーネント, on page 16
- SD-Routing デバイスで Flexible NetFlow モニターを有効にする方法, on page 17
- フローレベル Flexible NetFlow を設定するための前提条件, on page 18
- フローレベル Flexible NetFlow の設定に関する制限事項, on page 18
- EzPM プロファイルを使用した SD-Routing デバイスでのフローレベル FNF の設定, on page 18
- フローモニターを使用したフローレベル Flexible NetFlow の設定, on page 19
- Security Unified Logging について, on page 21
- デバイスでの Security Unified Logging の設定に関する制限事項, on page 21
- EzPM プロファイルを使用した SD-Routing デバイスでの Security Unified Logging の設定, on page 21
- フローモニターを使用した SD-Routing デバイスでの Security Unified Logging の設定, on page 22
- SD-Routing デバイスのフローレベル Flexible NetFlow の有効化, on page 24

フローレベル Flexible NetFlow について

Flexible NetFlow は、特定の要件に合わせてトラフィック分析パラメータをカスタマイズする機能を追加する、元の NetFlow の拡張機能です。Flexible NetFlow では、トラフィック分析のための非常に複雑な構成を作成したり、再利用可能な構成コンポーネントを使用してデータをエクスポートすることが容易になります。

Security Unified Logging (SUL) プロファイルは、アプリケーションレベルおよびフローレベルのプロファイルに存在するすべての情報を含むスーパーセットとして機能します。

詳細なフローレベルの統計が必要ない場合は、FNF モニターに[アプリケーションの可視性](#)を使用できます。または、フローレベルの FNF モニターを有効にして、アプリケーションレベルの統計を含むキャプチャされたすべてのデータを表示することもできます。

LAN インターフェイスまたは WAN インターフェイスのいずれかでフローレベルの可視性モニターを有効にすることで、パケットの二重カウントを回避できます。これにより、LAN から WAN への入力および出力データトラフィックフローが原因のデータの冗長性が回避されます。

IPv4 および IPv6 プロトコルは、パフォーマンス モニター コンテキストがインターフェイスに適用された後、デフォルトで有効になります。ただし、パフォーマンスモニタリングコンテキストを設定することで、IPv4 プロトコルまたは IPv6 プロトコルのいずれかを有効にすることができます。

SD-Router デバイスの Flexible NetFlow モニタリングのタイプ

SD-Router は、次の 3 種類の FNF モニタリング方式をサポートしています。

- 集約 NetFlow アプリケーションの可視性
- フローレベル FNF
- Security Unified Logging (SUL)

フローレベル Flexible NetFlow の利点

フローレベル FNF を有効にすると、次の利点があります。

- フローレベル FNF は、詳細なレベルの統計情報を提供します。
- フローレベル FNF 統計は、オンデマンドの障害対応のために Cisco Catalyst SD-WAN 分析および SD-WAN モニタリングで使用されます。

フローレベル Flexible NetFlow コンポーネント

Flexible NetFlow は、いくつかのバリエーションで一緒に使用して、データエクスポートおよびトラフィック分析を実行できるコンポーネントで構成されます。Flexible NetFlow のユーザー定義のフローレコードおよびコンポーネントの構成によって、最小限の数のコンフィギュレーションコマンドを使用して、ネットワークデバイスでのデータエクスポートおよびトラフィック分析のためのさまざまな設定の作成が容易になります。

各フロー モニターに、フロー レコード、フロー エクスポーター、およびキャッシュ タイプの固有の組み合わせを設定できます。フローエクスポーターの宛先 IP アドレスなどのパラメータを変更す

る場合、フロー エクスポートを使用するすべてのフロー モニターに対して自動的に変更されます。ここでは、Flexible NetFlow コンポーネントのその他の情報を提供します。

- フロー レコード

Flexible NetFlow では、キー フィールドと非キー フィールドの組み合わせをレコードと呼びます。Flexible NetFlow のレコードは Flexible NetFlow フロー モニターに割り当てられ、フロー データの格納に使用されるキャッシュが定義されます。

- フローエクスポート

フローエクスポートでは、フローモニタ キャッシュ内のデータをリモートシステム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。フローエクスポートは、コンフィギュレーションで別のエンティティとして作成されます。フローエクスポートは、フローモニタにデータエクスポート機能を提供するためにフローモニタに割り当てられます。複数のフローエクスポートを作成して、1 つまたは複数のフローモニタに適用すると、いくつかのエクスポート先を指定することができます。1 つのフローエクスポートを作成し、いくつかのフローモニタに適用することができます。

- フローモニター

フローモニターは Flexible NetFlow のコンポーネントであり、ネットワークトラフィックのモニタリングを実行するために、インターフェイスに適用されます。

フローモニターは、ユーザー定義のレコード、オプションのフローエクスポート、およびフロー モニターが最初のインターフェイスに適用されるときに自動的に作成されるキャッシュで構成されます。

フロー データはネットワーク トラフィックから収集され、フロー レコードの key フィールドおよび nonkey フィールドに基づいて監視プロセス中にフロー モニター キャッシュに追加されます。

SD-Routing デバイスで Flexible NetFlow モニターを有効にする方法

フローレベル FNF を有効にするには、次の 2 つの方法があります。

- **EzPM プロファイルの使用:** これは、既存のプロファイルを使用してフローレコードを設定できるシンプルな推奨方法です。EzPM プロファイルを使用すると、アプリケーションの可視性、フローレベルの可視性、および SUL モニターを設定できます。
- **フローモニターの使用:** これは、手動プロセスです。フローレコードを作成し、アプリケーションの可視性、フローレベルの可視性、および SUL のローカルエクスポートにエクスポートします。

フローレベル Flexible NetFlow を設定するための前提条件

Cisco ルータで license boot-level advantage を有効にする必要があります。これにより、EzPM プロファイル CLI サポートを使用するための Network Advantage が得られます。

フローレベル Flexible NetFlow の設定に関する制限事項

次に、フローレベル FNF 設定に関する制限事項を示します。

- Cisco SD-WAN Manager では、CLI ベースの設定グループ、CLI テンプレート、または CLI アドオンプロファイルを使用して、SD-Routing デバイスのフローレベル設定が可能です。
- アプリケーションレベルおよびフローレベルの可視性によって、ターゲットインターフェイスの入力データと出力データの両方をモニターします。サービスインターフェイスとトランスポート インターフェイスの両方で設定されている場合、同じフローのパケットは 2 回カウントされます。
- 部分的にフローレベルレコードフィールドを使用してフローモニターをカスタマイズすることはできません。部分的なフローレベルレコードフィールドがモニターに追加された場合、PSV データは生成されません。
- 1 つのインターフェイスにアプリケーションの可視性、フローレベルの可視性、または SUL プロファイルのいずれかを設定できます。インターフェイスに適用できる EzPM プロファイルは 1 種類だけです。

EzPM プロファイルを使用した SD-Routing デバイスでのフローレベル FNF の設定

フローレベル FNF モニタリングを有効にする場合は、デフォルトの Easy Performance Monitor (EzPM) プロファイルを使用できます。EzPM の詳細については、[こちら](#)を参照してください。

フローレベルの可視性には、アプリケーションレベルの統計情報とフローレベルの統計情報の両方が含まれます。これにより、FNF モニターのアプリケーションレベルの可視性を有効にする必要がなくなります。

Procedure

Step 1 EzPM プロファイルを作成します。

```
Device# configure terminal
Device(config)# performance monitor context context_name profile flow-level-visibility
Device(config-perf-mon)# exporter destination local-controller source Null0
```



```
Device(config-perf-mon)# traffic-monitor flow-level-visibility-stats
Device(config-perf-mon)# end
```

```
Device# configure terminal
Device(config)# interface interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

Step 2 パフォーマンス モニター コンテキストをインターフェイスに適用します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

フローモニターを使用したフローレベル Flexible NetFlow の設定

フローモニターを使用してフローレベル FNF を設定するには、次の手順を実行します。

Procedure

Step 1 FNF フローエクスポートを作成してフローレコードを作成します。

```
Device# configure terminal
Device(config)# flow exporter exporter-name
Device(config-flow-exporter)# destination local controller
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout seconds
Device(config-flow-exporter)# option interface-table
Device(config-flow-exporter)# option vrf-table
Device(config-flow-exporter)# option application-table
Device(config-flow-exporter)# option application-attributes
Device(config-flow-exporter)# exit
```

Step 2 IPv4 トラフィックのフローレベルビューのフローレコードを作成します。

```
Device# configure terminal
Device(config)# flow record flow_level_visibility_ipv4
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
```

フローモニターを使用したフローレベル Flexible NetFlow の設定

```
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect ipv4 dscp
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# end
```

Step 3 IPv6 トラフィックのフローレベルビューのフローレコードを作成します。

```
Device# configure terminal
Device(config)# flow record flow_level_visibility_ipv6
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv6 destination address
Device(config-flow-record)# match ipv6 protocol
Device(config-flow-record)# match ipv6 source address
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect ipv6 dscp
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# end
```

Step 4 フローモニターを有効にして、IPv4 トラフィックのネットワークトラフィックのフローレベルの可視性を実行します。

```
Device# configure terminal
Device(config)# flow monitor fnf-flow-level-visibility-v4
Device(config-flow-monitor)# exporter fnf-1
Device(config-flow-monitor)# record flow_level_visibility_ipv4
Device(config-flow-monitor)# end
```

Step 5 フローモニターを有効にして、IPv6 トラフィックのネットワークトラフィックのフローレベルの可視性を実行します。

```
Device# configure terminal
Device(config)# flow monitor fnf-flow-level-visibility-v6
Device(config-flow-monitor)# exporter fnf-1
Device(config-flow-monitor)# record flow_level_visibility_ipv6
Device(config-flow-monitor)# end
```

Step 6 フローモニターをインターフェイスに適用します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet1
Device(config-if)# ip flow monitor fnf-flow-level-visibility-v4 input
Device(config-if)# ip flow monitor fnf-flow-level-visibility-v4 output
Device(config-if)# ipv6 flow monitor fnf-flow-level-visibility-v6 input
```

```
Device(config-if)# ipv6 flow monitor fnf-flow-level-visibility-v6 output
Device(config-if)# end
```

What to do next

[SD-Routing デバイスでのフローレベルデータのモニター](#)

Security Unified Logging について

Security Unified Logging を使用すると、ゾーンベースのファイアウォールと、IPS、URL-F、AMP などの統合脅威防御機能のログデータを可視化できます。これらの機能は、ブロックされたトラフィック、脅威、サイト、またはマルウェアの理解や、関連付けられたポート、プロトコル、またはアプリケーションでのトラフィックまたはセッションをブロックしたルールを理解するのに役立ちます。

SUL プロファイルにはすべてのフローレベルフィールドが含まれているため、SUL プロファイルがすでに適用されている場合は、フローレベルの可視性をインターフェイスに適用する必要はありません。SUL は、IPv4 と IPv6 の両方のプロトコルをサポートします。

デバイスでの Security Unified Logging の設定に関する制限事項

デバイスで SUL を設定する場合の制限事項は次のとおりです。

- アプリケーションの可視性（集約 FNF）やフローの可視性など、他の FNF プロファイルが設定されている場合は、SUL プロファイルを設定しないでください。これらの 3 つのプロファイルは、データの冗長性を回避するために相互に排他的である必要があります。
- 部分的に SUL レコードフィールドを使用してフローモニターをカスタマイズすることはできません。部分的な SUL レコードフィールドがモニターに追加された場合、PSV データは生成されません。
- 設計上の制限により、SUL モニターは出力方向のみを収集するため、デフォルトでは SUL を LAN および WAN インターフェイスの両方に適用する必要があります。

EzPM プロファイルを使用した SD-Routing デバイスでの Security Unified Logging の設定

SD-Routing デバイスで SUL を設定する場合、次の 2 つの方法が定義されています。

Procedure

Step 1 EzPM プロファイルを設定します。

```
Device# configure terminal
Device(config)# performance monitor context context_name profile security-unified-logging
Device(config-perf-mon)# exporter destination local-controller source Null0
Device(config-perf-mon)# traffic-monitor sul-fnf-config
Device(config-perf-mon)# end
```

Step 2 パフォーマンス モニター コンテキストをインターフェイスに適用します。

```
Device# configure terminal
Device(config)# interface interface-id
Device(config-if)# performance monitor context context-name
Device(config-if)# end
```

What to do next

[SD-Router デバイスでの Security Unified Logging データのモニター](#)

フローモニターを使用した SD-Router デバイスでの Security Unified Logging の設定

フローモニターを使用して SUL を設定するには、次の手順を実行します。

SUMMARY STEPS

1. SUL のフローエクスポートを作成します。
2. フローレコードを設定します。
3. SUL のフローモニターを有効にします。
4. フローモニターをインターフェイスに適用します。

DETAILED STEPS

Procedure

Step 1 SUL のフローエクスポートを作成します。

```
Device# configure terminal
Device(config)# flow exporter sul-1
Device(config-flow-exporter)# destination local controller
Device(config-flow-exporter)# export-protocol ipfix
```

```
Device(config-flow-exporter)# option interface-table
Device(config-flow-exporter)# option vrf-table
Device(config-flow-exporter)# option application-table
Device(config-flow-exporter)# option utd-category-table
Device(config-flow-exporter)# option utd-file-type-table
Device(config-flow-exporter)# option application-attributes
Device(config-flow-exporter)# option c3pl-class-table
Device(config-flow-exporter)# option c3pl-policy-table
Device(config-flow-exporter)# option fw-zone-pair-table
Device(config-flow-exporter)# option fw-zone-table
Device(config-flow-exporter)# option fw-proto-table
Device(config-flow-exporter)# option utd-drop-reason-table
Device(config-flow-exporter)# option sdvt-drop-reason-table
Device(config-flow-exporter)# exit
```

Step 2 フローレコードを設定します。

```
Device# configure terminal
Device(config)# flow record sul-sul-monitor-v4
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# collect ipv4 dscp
Device(config-flow-record)# collect transport tcp flags
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect application name
Device(config-flow-record)# collect flow end-reason
Device(config-flow-record)# collect connection initiator
Device(config-flow-record)# collect connection id long
Device(config-flow-record)# collect ulogging fw-zp-id
Device(config-flow-record)# collect ulogging fw-zone-id-array
Device(config-flow-record)# collect ulogging fw-class-id
Device(config-flow-record)# collect ulogging fw-policy-id
Device(config-flow-record)# collect ulogging fw-proto-id
Device(config-flow-record)# collect ulogging fw-action
Device(config-flow-record)# collect ulogging fw-src-ipv4-addr-translated
Device(config-flow-record)# collect ulogging fw-dst-ipv4-addr-translated
Device(config-flow-record)# collect ulogging fw-src-port-translated
Device(config-flow-record)# collect ulogging fw-dst-port-translated
Device(config-flow-record)# collect ulogging utd-ips-pri
Device(config-flow-record)# collect ulogging utd-ips-sid
Device(config-flow-record)# collect ulogging utd-ips-gid
Device(config-flow-record)# collect ulogging utd-ips-cid
Device(config-flow-record)# collect ulogging utd-urllf-url-hash
Device(config-flow-record)# collect ulogging utd-urllf-url-category
Device(config-flow-record)# collect ulogging utd-urllf-url-reputation
Device(config-flow-record)# collect ulogging utd-urllf-app-name
Device(config-flow-record)# collect ulogging utd-amp-dispos
Device(config-flow-record)# collect ulogging utd-amp-filename-hash
Device(config-flow-record)# collect ulogging utd-amp-file-type
Device(config-flow-record)# collect ulogging utd-amp-file-hash
Device(config-flow-record)# collect ulogging utd-amp-malname-hash
Device(config-flow-record)# collect ulogging utd-drop-reason-id
```

```

Device(config-flow-record)# collect ulogging sdvt-drop-reason-id
Device(config-flow-record)# collect ulogging utd-ips-policy-id
Device(config-flow-record)# collect ulogging utd-ips-action-id
Device(config-flow-record)# collect ulogging utd-urlf-policy-id
Device(config-flow-record)# collect ulogging utd-urlf-action-id
Device(config-flow-record)# collect ulogging utd-amp-policy-id
Device(config-flow-record)# collect ulogging utd-amp-action-id
Device(config-flow-record)# collect ulogging utd-urlf-reason-id
Device(config-flow-record)# collect ulogging flow-direction
Device(config-flow-record)# collect ulogging fw-user-name
Device(config-flow-record)# collect ulogging fw-src-ipv6-addr-translated
Device(config-flow-record)# collect ulogging fw-dst-ipv6-addr-translated
Device(config-flow-record)# end

```

Step 3 SUL のフローモニターを有効にします。

```

Device# configure terminal
Device(config)# flow monitor sul-sul-monitor-v4
Device(config-flow-monitor)# exporter sul-1
Device(config-flow-monitor)# record sul-sul-monitor-v4
Device(config-flow-monitor)# end

```

Step 4 フローモニターをインターフェイスに適用します。

```

Device# configure terminal
Device(config)# interface GigabitEthernet1
Device(config-if)# ip flow monitor sul-sul-monitor-v4 output
Device(config-if)# end

```

What to do next

[SD-Routing デバイスでの Security Unified Logging データのモニター](#)

SD-Routing デバイスのフローレベル Flexible NetFlow の有効化

Cisco SD-WAN Manager を使用してフローレベル FNF を有効にするには、まず設定グループを作成し、次に示す手順を実行します。

設定グループの作成

設定グループを作成するには、次の手順を実行します。

Procedure

Step 1 Cisco Catalyst SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** の順に選択し、**[Solution]** ドロップダウンリストから **[SD-Routing]** ソリューションを選択します。

- Step 2** [Create Configuration Group] をクリックし、ダイアログボックスで名前と説明を入力し、[CLI Configuration Group] を選択して [Create] をクリックします。
- Step 3** [Load Running Config from Reachable Device] ドロップダウンリストから、デバイスを選択します。
- Step 4** CLI が [Config Preview] セクションにロードされたら、[Save] をクリックします。
-

デバイスの関連付けと設定グループの展開

デバイスの設定を関連付けて展開するには、次の手順を実行します。

Procedure

- Step 1** 設定グループ名の横にある [(...)] をクリックし、[Edit] を選択します。
- Step 2** [Deployment] ペインで、[Add] をクリックし、関連付けるデバイスを選択します。
- Step 3** 1 つ以上のデバイスを選択し、[Deploy] をクリックします。
- Step 4** [Save] をクリックします。
-

SD-Routing デバイスでのフローレベルデータのモニター

デバイスの接続先 IP、接続先ポート、送信元 IP などのフローレベルの情報を表示およびモニターするには、次の手順を実行します。

Procedure

- Step 1** Cisco SD-WAN Manager のメニューから **[Monitor]** > **[Devices]** の順に選択し、リストから SD-Routing デバイスを選択します。
- Step 2** 左側のペインで、**[SAIE Applications]** > **[Filter]** の順に選択します。
- Step 3** [Filter By] ダイアログボックスで [VPN] を選択し、[Search] をクリックして、選択したフィルタに基づいてフローレコードを検索します。
- Step 4** [Export] をクリックして、フローレコードをローカルシステムにエクスポートします。
-

SD-Routing デバイスでの Security Unified Logging データのモニター

デバイスで SUL データをモニターするには、次の手順を実行します。

Procedure

-
- Step 1** Cisco SD-WAN Manager のメニューから **[Monitor] > [Devices]** の順に選択し、リストから SD-Routing デバイスを選択します。
- Step 2** 左側のペインから、**[Connection Events] > [Filter]** の順に選択します。
- Step 3** [Filter By] ダイアログボックスで [VPN] を選択し、[Search] をクリックして、選択したフィルタに基づいてフローレコードを検索します。
-



CHAPTER 4

SD-Routing デバイスでのパケットキャプチャ

この章では、SD-Routing デバイスでパケットキャプチャを設定する方法について説明します。ここで説明する内容は、次のとおりです。

- [パケットキャプチャについて, on page 27](#)
- [パケットキャプチャの設定, on page 27](#)
- [SD-Routing のパケットキャプチャの機能情報, on page 29](#)

パケットキャプチャについて

パケットキャプチャ機能を使用すると、SD-Routing デバイスのトラフィックをキャプチャして分析できます。選択した VRF でターゲットインターフェイスを選択することで、パケットキャプチャを開始できます。また、送信元 IP アドレス、宛先 IP アドレス、レイヤ 4 プロトコル番号などを指定することで、単純なトラフィックフィルタを設定できます。

パケットキャプチャの設定

前提条件

- Cisco IOS XE Catalyst SD-Routing デバイスの最小ソフトウェアバージョン: Cisco IOS XE Catalyst SD-WAN リリース 17.13.1。
- [Administration]>[Settings] ページでデータストリームが有効になっていることを確認します。

制限事項

制限事項は次のとおりです。

- xDSL (ATM/イーサネット インターフェイス) はサポートされていません。
- ダイナミック仮想アクセスインターフェイスは、FlexVPN でのみサポートされます。

- ループバック インターフェイスはサポートされていません
- BDI およびレイヤ 2 EFP/サービス インスタンス インターフェイスはサポートされていません。

パケットキャプチャの設定

パケットキャプチャを設定するには、次の手順を実行します。

Procedure

-
- Step 1** Cisco SD-WAN Manager のメニューから **[Monitor] > [Devices]** の順に選択します。
- Step 2** デバイスを選択するには、**[Hostname]** 列でデバイス名をクリックします。
- Step 3** 左ペインで **[Troubleshooting]** をクリックし、**[Packet Capture]** をクリックします。
- Step 4** **[VPN]** フィールドで、インターフェイスをフィルタリングするための **VPN** を選択します。
- Step 5** **[Interface corresponding to the VPN]** フィールドで、パケットをキャプチャするターゲットインターフェイスを選択します。
- Step 6** （任意）**[Traffic Filters]** をクリックして、関連するトラフィックのみをキャプチャするようにフィルタを設定します。これにより、ネットワークの負荷が軽減され、特定のパケットの分析が容易になります。
- a) **[Source IP]** フィールドに、パケットをキャプチャするデバイスの送信元 IP アドレスを入力します。
 - b) **[Destination IP]** フィールドに、パケットをキャプチャするデバイスの宛先 IP アドレスを入力します。
 - c) **[Source Port]** フィールドに送信元ポート番号を入力します。
 - d) **[Destination Port]** フィールドに宛先ポート番号を入力します。

Note

送信元ポートと宛先ポートは、プロトコルが 6（TCP）または 17（UDP）の場合にのみ適用されます。

- e) トグルボタンを使用して双方向フィルタを有効にし、送信元 IP トラフィックと宛先 IP トラフィックの両方をフィルタリングします。

- Step 7** **[Start]** をクリックします。

Cisco SD-WAN Manager は、指定されたフィルタを使用してパケットのキャプチャを開始します。

- Step 8** **[Force Stop]** またはタイムアウトオプションを使用して、パケットキャプチャを停止できます。また、5MB のパケットをキャプチャすると、パケットキャプチャは自動的に停止します。

- Step 9** **[Download]** アイコンをクリックして、パケットキャプチャファイルをシステムにダウンロードします。

Note

パケットキャプチャプロセスの実行中は、**[Packet Capture]** ページを更新したり、ページから移動したりしないでください。

SD-Routing のパケットキャプチャの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 3: SD-Routing のパケットキャプチャの機能情報

機能名	リリース	機能情報
SD-Routing のパケットキャプチャ	Cisco IOS XE リリース 17.13.1a	この機能を使用すると、双方向 IPv6 トラフィックデータをキャプチャして SD-Routing デバイスの接続をトラブルシューティングするオプションを設定できます。



CHAPTER 5

SD-Routing デバイスでの速度テスト

この章では、SD-Routing デバイスで速度テストを設定する方法について説明します。ここで説明する内容は、次のとおりです。

- [速度テストに関する情報, on page 31](#)
- [速度テストの前提条件, on page 31](#)
- [インターネット速度テストの実行, on page 31](#)
- [Cisco SD-WAN Manager を使用した SD-Routing デバイスでの速度テストに関する機能情報, on page 33](#)

速度テストに関する情報

インターネット速度テスト: Cisco SD-WAN Manager はネットワーク速度をテストします。Cisco SD-WAN Manager は、デバイスをクライアントサイトとして指定し、iperf3 サーバーをリモートサイトとして指定します。iperf3 サーバーの IP アドレス（またはドメイン名）とポート番号を指定できます。

速度テストでは、送信元デバイスから選択または指定した iperf3 サーバーへのアップロード速度と、iperf3 サーバーから送信元デバイスへのダウンロード速度を測定します。

速度テストの前提条件

速度テストには、ターゲットデバイスのデバイスホスト名が必要です。また、データストリームを有効にする必要があります。データストリームを有効にするには、[Settings] ページに移動し、[Settings] > [Data Stream] を選択します。

インターネット速度テストの実行

速度テストを実行するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから **[Monitor] > [Devices]** の順に選択します。

2. デバイスを選択するには、[Hostname] 列でデバイス名をクリックします。
3. 左ペインで [Troubleshooting] をクリックします。
4. [Connectivity] 領域で、[Speed Test] をクリックします。
5. 次を指定します。
 - [Source Interface]: ドロップダウンリストから、ローカルデバイスの送信元インターフェイスを選択します。
 - [Destination Device]: ドロップダウンリストから [Internet] を選択します。
 - [iPerf3 Server]: (オプション) ドメイン名または iPerf3 サーバーの IP アドレスを IPv4 形式で入力します。
 - [Server Port Range]: (オプション) サーバーポートまたはポート範囲を入力します。たとえば、5201、5210、または 5201 ~ 5205 などです。
6. [Start Test] をクリックします。
速度テストの結果が表示されます。

速度テストの確認

速度テストが正常に実行されると、[Speed Test] ページに次の詳細が表示されます。

- 右ペインの中央に、速度テストの結果が表示されます。
- クロックは、最近取得した回線速度の結果を報告します。
- アップロード速度を測定する場合、パケットは送信元デバイスから iPerf3 サーバーに送信され、送信元デバイスは宛先から確認応答を受信します。
ダウンロード速度を測定する場合、パケットは iPerf3 サーバーから送信元デバイスに送信され、宛先デバイスは送信元から確認応答を受信します。

速度テストの問題のトラブルシューティング

次の表に、速度テストのトラブルシューティング情報を示します。

Table 4: トラブルシューティング シナリオ

エラー情報	考えられる根本的な原因
iperf サーバーアドレスの解決に失敗しました	DNS サーバーがエッジデバイスで設定されていないか、エッジデバイスで設定された DNS サーバーから iperf サーバーを解決できません。

エラー情報	考えられる根本的な原因
速度テストのサーバーに到達できません	速度テストサーバーの ping に失敗しました。エッジデバイスがサーバー IP に到達できません。
iPerf クライアント: ストリームに接続できません: リソースが一時的に使用できません	速度テストサーバーに接続できません。アクセスは、アクセス制御リスト (ACL) の権限によってブロックされている可能性があります。
iPerf クライアント: サーバーに接続できません	iPerf3 サーバーは、ユーザー指定のポートまたはデフォルトポート 5201 でテスト サービスを提供していません。
デバイスエラー: 速度テストが進行中です	選択した送信元または宛先デバイスが速度テストを実行しているため、新しいテストを開始できません。
デバイスエラー: サーバー設定の読み取りに失敗しました	データストリーム設定がありません。 回避策: SD-Routing デバイスで CLI コマンドを実行し、SD-Routing 制御接続をクリアすると、問題を解決できます。
速度テストセッションがタイムアウトになりました	速度テストが180秒以内に正常に完了しませんでした。これは、速度テスト中に SD-Routing デバイスが Cisco SD-WAN Manager への制御接続を失ったためである可能性があります。

Cisco SD-WAN Manager を使用した SD-Routing デバイスでの速度テストに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 5: Cisco SD-WAN Manager を使用した SD-Routing デバイスでの速度テストに関する機能情報

機能名	リリース情報	説明
速度テスト	Cisco IOS XE 17.13.1	Cisco SD-WAN Manager を使用すると、デバイスと iPerf3 サーバー間のネットワーク速度と使用可能な帯域幅を測定できます。速度テストでは、送信元デバイスから宛先デバイスへのアップロードおよびダウンロードの速度を測定します。

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。