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

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

SD-Routing 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、ネットワーキング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、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 エクスポータ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。

- **フローエクスポータ**

  フローエクスポータでは、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。フローエクスポータは、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。フローエクスポータは、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タを作成して、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タを作成し、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タ、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タ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 フローエクスポータ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
```

```
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-visiblility-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-visiblility-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-visiblility-v4 input
Device(config-if)# ip flow monitor fnf-flow-level-visiblility-v4 output
Device(config-if)# ipv6 flow monitor fnf-flow-level-visiblility-v6 input
```

```
Device(config-if)# ipv6 flow monitor fnf-flow-level-visiblility-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性化できます。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-Routing 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-Routing 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タを作成します。
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タを作成します。

```
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-urlf-url-hash
Device(config-flow-record)# collect ulogging utd-urlf-url-category
Device(config-flow-record)# collect ulogging utd-urlf-url-reputation
Device(config-flow-record)# collect ulogging utd-urlf-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。

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。