



Cisco TrustSec フィールドの Flexible NetFlow エクスポート

• [Cisco TrustSec フィールドの Flexible NetFlow エクスポート \(1 ページ\)](#)

Cisco TrustSec フィールドの Flexible NetFlow エクスポート

Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、Flexible Netflow (FNF) フローレコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニター、トラブルシューティング、および特定を支援します。

このモジュールでは、Cisco TrustSec と FNF のインタラクションについてと、NetFlow バージョン 9 フローレコードの Cisco TrustSec フィールドを設定しエクスポートする方法を説明します。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの制約事項

- FNF レコードでエクスポートされるセキュリティグループタグ (SGT) 値は、次のシナリオでは 0 になります。
 - 対応するパケットは、信頼されたインターフェイスから、0 の SGT 値とともに受信します。
 - 対応するパケットは SGT なしで受信します。
 - IP-SGT ルックアップ中に SGT が検出されません。(パケットが SGT なしで受信されるため、SGT は同じパケット内に見つかりません)。
 - フローレコードに SGT と接続先グループタグ (DGT) のフィールド (またはこの 2 つのどちらかのフィールドだけ) が含まれる場合、両方の値を適用できないとしても、SGT と DGT に値 0 を設定したフローが作成されます。フローレコードには、SGT および DGT フィールドと一緒に、送信元および宛先 IP アドレスが含まれる必要があります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートに関する情報

Flexible NetFlow の Cisco TrustSec フィールド

FNF フローレコード内の Cisco TrustSec フィールド、送信元 SGT および宛先 DGT は、管理者によるフローとアイデンティティ情報の関連付けに役立ちます。ネットワークエンジニアは、これにより、顧客がネットワークリソースおよびアプリケーションリソースをどのように利用しているのかについて詳しく理解できます。この情報を使用して、潜在的なセキュリティやポリシーの違反を検出して解決するために、アクセスおよびアプリケーションリソースを効率的に計画して割り当てることができます。

Cisco TrustSec フィールドは入力/出力 FNF、ユニキャスト/マルチキャストトラフィックでサポートされています。

次のテーブルに、Cisco TrustSec 用の NetFlow バージョン 9 の企業固有フィールドタイプを示します。これは、Cisco TrustSec の送信元/宛先 SGT の FNF テンプレートで使用されます。

| フローフィールドタイプ | 説明 |
|-------------------|------------------------|
| CTS_SRC_GROUP_TAG | Cisco TrustSec 送信元 SGT |
| CTS_DST_GROUP_TAG | Cisco TrustSec 宛先 SGT |

FNF フローレコードで既存の一致するフィールドに加えて、Cisco TrustSec フィールドが設定されます。次の設定を使用して、Cisco TrustSec フローオブジェクトをキーフィールドまたは非キーフィールドとして FNF フローレコードに追加し、パケット用の送信元と宛先の SGT を設定します。

match flow cts {source | destination} group-tag コマンドは、キーフィールドとして Cisco TrustSec フィールドを指定するため、対応するフローレコード以下で設定されます。キーフィールドはフローを差別化するものです。各フローには、一連の一意の値が設定されています。フローレコードをフローモニターで使用するには、1 つ以上のキーフィールドが必要になります。送信元 SGT、宛先 SGT、またはその両方に同時に **match** コマンドを設定できます。

フローレコードは、フローモニター下で設定され、フローモニターはインターフェイスに適用されます。FNF データをエクスポートするには、フローエクスポートを設定し、フローモニター以下に追加する必要があります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定方法

次のセクションでは、Cisco TrustSec フィールドの FNF エクスポートを構成するさまざまなタスクについて説明します。

フローレコードのキーフィールドとしての Cisco TrustSec フィールドの設定

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | flow record record-name 例 : Device (config)# flow record cts-record-ipv4 | FNF フローレコードを作成するか、または既存の FNF フローレコードを変更して、Flexible NetFlow フローレコード コンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> このコマンドでは、既存のフローレコードを変更することもできます。 |
| ステップ 4 | match ipv4 protocol 例 : Device (config-flow-record)# match ipv4 protocol | (任意) フローレコードのキーフィールドとして IPv4 プロトコルを設定します。 |
| ステップ 5 | match ipv4 source address 例 : Device (config-flow-record)# match ipv4 source address | (任意) IPv4 送信元アドレスをフローレコードのキーフィールドとして設定します。 |
| ステップ 6 | match ipv4 destination address 例 : Device (config-flow-record)# match ipv4 destination address | (任意) IPv4 宛先アドレスをフローレコードのキーフィールドとして設定します。 |
| ステップ 7 | match transport source-port 例 : Device (config-flow-record)# match transport source-port | (オプション) フローレコードのキーフィールドとして、トランスポート送信元ポートを設定します。 |

| | コマンドまたはアクション | 目的 |
|---------|---|---|
| ステップ 8 | match transport destination-port 例 : <pre>Device(config-flow-record)# match transport destination-port</pre> | (オプション) フローレコードのキーフィールドとして、トランスポート宛先ポートを設定します。 |
| ステップ 9 | match flow direction 例 : <pre>Device(config-flow-record)# match flow direction</pre> | (オプション) フローがモニターされる方向をキーフィールドとして設定します。 |
| ステップ 10 | match flow cts {source destination} group-tag 例 : <pre>Device(config-flow-record)# match flow cts source group-tag</pre> <pre>Device(config-flow-record)# match flow cts destination group-tag</pre> | FNF フローレコード内のレコードのキーフィールドとして、Cisco TrustSec の送信元グループタグまたは接続先グループタグを設定します。 <ul style="list-style-type: none"> • 入力 : <ul style="list-style-type: none"> • 着信パケットでは、ヘッダーがある場合、SGT にはヘッダーと同じ値が反映されます。値がない場合は、0 が示されます。 • DGT 値は入力ポートの SGACL 設定に依存しません。 • 出力 : <ul style="list-style-type: none"> • propagate-sgt コマンドまたは Cisco TrustSec のどちらかが出力インターフェイス上で無効化されていると、SGT は 0 になります。 • 発信パケットで、SGT または DGT に対応する SGACL 設定が存在すれば、DGT は 0 以外の数値になります。 • SGACL が出力ポートまたは VLAN で無効化されているか、またはグローバル SGACL の適用を無効化されている場合、DGT は 0 になります。 |

| | コマンドまたはアクション | 目的 |
|---------|--|--|
| ステップ 11 | end 例 : Device (config-flow-record) # end | Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 |

NetFlow での SGT 名のエクスポートの設定

フローエクスポートごとに、1つの宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフローエクスポートを設定してフローモニターに割り当てる必要があります。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | flow exporter <i>exporter-name</i> 例 : Device (config) # flow exporter EXPORTER-1 | フローエクスポートを作成するか、または既存のフローエクスポートを変更して、Flexible NetFlow フローエクスポート コンフィギュレーション モードを開始します。 |
| ステップ 4 | destination {<i>ip-address</i> <i>hostname</i>} [vrf <i>vrf-name</i>] 例 : Device (config-flow-exporter) # destination 172.16.10.2 | エクスポートの宛先システムの IP アドレスまたはホスト名を指定します。 |
| ステップ 5 | option cts-sgt-table [timeout <i>seconds</i>] 例 : Device (config-flow-exporter) # option cts-sgt-table timeout 1200 | エクスポートの SGT ID-to-name テーブルオプションを選択します。 <ul style="list-style-type: none"> このオプションにより、FNFはSGTをセキュリティグループ名にマッピングする Cisco TrustSec 環境データテーブルをエクスポートできます。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 6 | end 例 : Device(config-flow-exporter)# end | Flexible NetFlow フロー エクスポート コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 |

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定例

次のセクションでは、Cisco TrustSec フィールドの FNF エクスポートの設定に関する例を示します。

例：フローレコードのキーフィールドとしての Cisco TrustSec フィールドの設定

次の例は、Cisco TrustSec フローオブジェクトを、IPv4 Flexible NetFlow フローレコードのキーフィールドとして設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
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)# match flow direction
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# end
```

例：NetFlow での SGT 名のエクスポートの設定

次に、NetFlow で SGT 名のエクスポートを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# option cts-sgt-table timeout 1200
Device(config-flow-exporter)# end
```

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

| リリース | 機能 | 機能情報 |
|------------------------------|---|--|
| Cisco IOS XE Everest 16.5.1a | Cisco TrustSec フィールドの Flexible NetFlow エクスポート | Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、FNF フローレコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニター、トラブルシューティング、および特定を支援します。 |

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

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。