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、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か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、フローモニタ下で設定され、フローモニタ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 エクスポータを設定し、フロー モニタ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。 • 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。 • 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： `Device(config-flow-record)# match transport destination-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート宛先ポートを設定します。
ステップ 9	**match flow direction** 例： `Device(config-flow-record)# match flow direction`	（オプション）フローがモニタ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：
	`Device(config-flow-record)# match flow cts source group-tag`
	`Device(config-flow-record)# match flow cts destination group-tag`
		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。
		• 入力：
		• 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：
		• **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

フローエクスポータごとに、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 エクスポータを設定してフロー モニタ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。 • 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** *exporter-name* 例： `Device(config)# flow exporter EXPORTER-1`	フロー エクスポータを作成するか、または既存のフロー エクスポータを変更して、Flexible NetFlow フロー エクスポータ 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** {*ip-address* | *hostname*} [**vrf** *vrf-name*] 例： `Device(config-flow-exporter)# destination 172.16.10.2`	エクスポータの宛先システムの 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** *seconds*] 例： `Device(config-flow-exporter)# option cts-sgt-table timeout 1200`	エクスポータの SGT ID-to-name テーブルオプションを選択します。 • 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 エクスポータ 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 Fuji 16.9.2	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、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 からアクセスします。