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

Flexible NetFlow の Cisco TrustSec フィールド

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。

（注） Flexible NetFlow レコード、および IP パケットの Cisco TrustSec フィールドの記録は、IPv4 パケットでのみ機能します。IPv6 パケットは、Cisco TrustSec フィールドのキャプチャをサポートしていません。

Flexible Netflow（FNF）フローレコード内の Cisco TrustSec フィールド、送信元セキュリティグループタグ（SGT）および宛先セキュリティグループタグ（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、顧客のネットワーク リソースおよびアプリケーション リソースの利用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 FNF およびユニキャスト/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 V9 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/宛先ソース グループ タグの FNF テンプレートで使用されます。

ID	説明
CTS_SRC_GROUP_TAG	Cisco Trusted Security 送信元グループ タグ
CTS_DST_GROUP_TAG	Cisco Trusted Security 宛先グループ タグ

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、パケットの送信元と宛先のセキュリティグループタグを設定します。

collect flow cts {source | destination} group-tag コマンドは、非キーフィールドとして Cisco TrustSec フィールドを指定するため、フローレコードで設定されます。非キー フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。

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、フローモニター以下に追加する必要があります。

フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **match ipv4 protocol**
5. **match ipv4 source address**
6. **match ipv4 destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **collect flow cts source group-tag**
10. **collect flow cts destination group-tag**
11. **collect counter packets**
12. **end**

手順の詳細

	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`	Flexible Netflow（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。
ステップ 4	**match ipv4 protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	（オプション）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。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
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。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
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。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
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	**collect flow cts source group-tag** 例： `Device(config-flow-record)# collect flow cts source group-tag`	（オプション）FNF フローレコード内の Cisco TrustSec 送信元セキュリティグループタグ（SGT）を非キーフィールドとして設定します。
ステップ 10	**collect flow cts destination group-tag** 例： `Device(config-flow-record)# collect flow cts destination group-tag`	（オプション）FNF フローレコード内の Cisco TrustSec 宛先セキュリティグループタグ（DGT）を非キーフィールドとして設定します。
ステップ 11	**collect counter packets** 例： `Device(config-flow-record)# collect counter packets`	（オプション）フローで確認されるパケット数を非キー フィールドとして設定し、フローから合計パケット数を収集します。
ステップ 12	**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。

フロー エクスポータの設定

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 モニターに割り当てる必要があります。

始める前に

フロー レコードを作成していることを確認します。詳細については、「フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定」の項および「フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**

3. **flow exporter** *exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
5. **end**

手順の詳細

	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	**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。

フロー モニタの設定

始める前に

フロー エクスポータをデータ エクスポート用のフロー モニタに追加するには、フロー エクスポータを作成していることを確認します。詳細については、「フローエクスポータの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**

3. **flow monitor** *monitor-name*
4. **record** *record-name*
5. **exporter** *exporter-name*
6. **end**

手順の詳細

	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 monitor** *monitor-name* 例： `Device(config)# flow monitor FLOW-MONITOR-1`	フロー モニタを作成するか、または既存のフロー モニタを変更して、Flexible NetFlow フロー モニタ 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	**record** *record-name* 例： `Device(config-flow-monitor)# record cts-record-ipv4`	フロー モニターのレコードを指定します。
ステップ 5	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter EXPORTER-1`	フロー モニタのエクスポータを指定します。
ステップ 6	**end** 例： `Device(config-flow-monitor)# end`	Flexible NetFlow フロー モニタ 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。

インターフェイスへのフロー モニタの適用

フロー モニタをアクティベートするには、フロー モニタを 1 つ以上のインターフェイスに適用する必要があります。

始める前に

フロー モニタを作成していることを確認します。詳細については、「フロー モニタの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow monitor** *monitor-name* **input**
5. **end**

手順の詳細

	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	**interface** *type number* 例： `Device(config)# interface Gi1/1`	インターフェイスを指定し、インターフェイス 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	**ip flow monitor** *monitor-name* **input** 例： `Device (config-if)# ip flow monitor FLOW-MONITOR-1 input`	作成済みのフローモニタを、トラフィックの分析対象となるインターフェイスに割り当てることで、そのフロー モニタをアクティブにします。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

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

手順の概要

1. **enable**
2. **show flow record** *record-name*
3. **show flow exporter** *exporter-name*
4. **show flow monitor** *monitor-name*
5. **show flow monitor** *monitor-name* **cache**
6. **show flow interface** *type number*

手順の詳細

ステップ 1 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）。

例：

```
Device> enable
```

ステップ 2 show flow record *record-name*

指定した Flexible Netflow（FNF）フロー レコードの詳細を表示します。

例：

```
Device> show flow record cts-recordipv4

flow record cts-recordipv4:
  Description:        User defined
  No. of users:       1
  Total field space:  30 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface output
    collect flow direction
    collect flow cts source group-tag
    collect flow cts destination group-tag
```

```
    collect counter packets
```

ステップ 3 **show flow exporter** *exporter-name*

指定した FNF フロー エクスポータの現在のステータスを表示します。

例：

```
Device> show flow exporter EXPORTER-1

Flow Exporter EXPORTER-1:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 100.100.100.1
    Source IP address:      3.3.3.2
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            65252
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

ステップ 4 **show flow monitor** *monitor-name*

指定した FNF フロー モニタのステータスと統計情報を表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       User defined
  Flow Record:       cts-recordipv4
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:                 normal (Platform cache)
    Status:               allocated
    Size:                 200000 entries
    Inactive Timeout:     60 secs
    Active Timeout:       1800 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
    Trans end aging:      off
```

ステップ 5 **show flow monitor** *monitor-name* **cache**

指定した FNF フロー モニタ キャッシュのコンテンツを表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1 cache
```

```
  Cache type:                               Normal
  Cache size:                               4096
  Current entries:                          2
  High Watermark:                           2

  Flows added:                              6
  Flows aged:                               4
    - Active timeout      (1800 secs)       0
    - Inactive timeout    (15 secs)         4
    - Event aged                            0
    - Watermark aged                        0
    - Emergency aged                        0

  IPV4 SOURCE ADDRESS:                      10.1.0.1
  IPV4 DESTINATION ADDRESS:                 172.16.2.0
  TRNS SOURCE PORT:                         58817
  TRNS DESTINATION PORT:                    23
  FLOW DIRECTION:                           Input
  IP PROTOCOL:                              6
  SOURCE GROUP TAG:                         100
  DESTINATION GROUP TAG:                    200
  counter packets:                          10

  IPV4 SOURCE ADDRESS:                      172.16.2.0
  IPV4 DESTINATION ADDRESS:                 10.1.0.1
  TRNS SOURCE PORT:                         23
  TRNS DESTINATION PORT:                    58817
  FLOW DIRECTION:                           Output
  IP PROTOCOL:                              6
  SOURCE GROUP TAG:                         200
  DESTINATION GROUP TAG:                    100
  counter packets:                          8
```

ステップ 6 **show flow interface** *type number*

指定したインターフェイスに適用されるFNFフローモニタの詳細を表示します。フローモニタがインターフェイスに適用されない場合、出力は空になります。

例：

```
Device>  show flow interface Gi1/1

Interface GigabitEthernet1/1
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
```

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

例：フローレコードの非キーフィールドとしてのCiscoTrustSec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 レコードの非キー 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)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# end
```

例：フロー エクスポータの設定

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# end
```

例：フロー モニタの設定

```
Device> enable
Device# configure terminal
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record cts-record-ipv4
Device(config-flow-monitor)# exporter EXPORTER-1
Device(config-flow-monitor)# end
```

例：インターフェイス上のフロー モニタの適用

次の例は、トラフィックを分析するインターフェイスにIPv4フローモニタを適用することで、このフロー モニタをアクティベートする方法を示します。IPv6 フローモニターをアクティベートするには、 **ip** キーワードを **ipv6** キーワードと置き換えます。

```
Device> enable
Device# configure terminal
Device(config)# interface Gi1/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# end
```

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。