CHAPTER 82

NetFlow セキュア イベント ロギング（NSEL）の設定

この章では、NetFlow Secure Event Logging（NSEL; NetFlow セキュア イベント ロギング）を設定する方法、NetFlow バージョン 9 テクノロジーに構築されているセキュリティ ロギングのメカニズム、および NSEL を経由したイベントと syslog メッセージの処理方法について説明します。

この章は、次の項で構成されています。

NSEL に関する情報

この項では、次のトピックについて取り上げます。

ASA および ASASM は NetFlow バージョン 9 サービスをサポートしています。NetFlow サービスの詳細については、「RFC」（P.82-12）を参照してください。

ASA および ASASM の NSEL の実装は、フロー内の重要なイベントを示すレコードだけをエクスポートするステートフルな IP フロー トラッキング方法を提供します。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。NSEL イベントはフロー ステータスについてのデータをエクスポートするために使用され、ステートの変更を引き起こしたイベントによってトリガーされます。

追跡される重要なイベントには、flow-create、flow-teardown、flow-denied（EtherType ACL によって拒否されるフローを除く）および flow-update が含まれます。また、NSEL の ASA および ASASM 実装が定期 NSEL イベントと flow-update イベントを生成して、フローの期間の定期的なバイト カウンタを提供します。これらのイベントは通常、タイム ドリブンです。このため、従来の NetFlow でよりインラインとなりますが、これらのイベントはそのフローの状態変更によってもトリガーされます。

（注）　flow-update イベント機能は、バージョン 8.4(5) だけで使用できます。これはバージョン 9.0(1) 以降では使用できません。

各 NSEL レコードにはイベント ID と拡張イベント ID フィールドがあり、これらによってフロー イベントが記述されます。

ASA および ASASM の NSEL の実装によって、次の主な機能が提供されます。

- flow-create、flow-teardown、および flow-denied イベントを追跡し、適切な NSEL データ レコードを生成します。
- フローの進行を記述するテンプレートを定義およびエクスポートします。テンプレートは、NetFlow を経由してエクスポートされるデータ レコードの形式を記述します。各イベントには、それぞれに関連付けられているいくつかのレコード形式またはテンプレートがあります。
- トラックによって NSEL コレクタが設定され、テンプレートとデータ レコードが UDP 経由の NetFlow だけによってそれらの設定された NSEL コレクタに配信されます。
- テンプレート情報を定期的に NSEL コレクタに送信します。コレクタは通常、フロー レコードを受信する前にテンプレート定義を受信します。
- モジュラ ポリシー フレームワークを通してトラフィックとイベント タイプに基づいて NSEL イベントをフィルタリングしてから、さまざまなコレクタにレコードを送信します。トラフィックはクラスが設定される順序に基づいて照合されます。一致が見つかると、その他のクラスはチェックされません。サポートされているイベント タイプは、flow-create、flow-denied、flow-teardown、およびすべてです。レコードはさまざまなコレクタに送信できます。たとえば、2 つのコレクタを使用して、次の操作を実行できます。
  - access list 1 が collector 1 に一致するすべての flow-denied イベントのログを記録します。
  - collector 1 に対するすべての flow-create イベントのログを記録します。
  - collector 2 に対するすべての flow-teardown イベントのログを記録します。
- flow-create イベントのエクスポートを遅延させます。

NSEL メッセージと syslog メッセージの使用

表 82-1 に同等の NSEL イベント、イベント ID、および拡張イベント ID を持つ syslog メッセージを示します。拡張イベント ID は、イベントについての詳細を提供します（入力または出力のどちらの ACL がフローを拒否したかなど）。

（注）　NetFlow のフロー情報のエクスポートをイネーブルにすると、表 82-1 に示した syslog メッセージが冗長になります。パフォーマンスの向上のためには、同じ情報が NetFlow を通してエクスポートされるため、冗長な syslog メッセージをディセーブルにすることをお勧めします。「NetFlow 関連の syslog メッセージのディセーブル化と再イネーブル化」（P.82-8）の手順を実行することによって、個別の syslog メッセージをイネーブルまたはディセーブルにできます。

表 82-1　syslog メッセージと同等の NSEL イベント

syslog メッセージ	説明	NSEL イベント ID	NSEL 拡張イベント ID
106100	ACL が発生するたびに生成されます。	1：フローが作成されました（ACL がフローを許可した場合）。 3：フローが拒否されました（ACL がフローを拒否した場合）。	0：ACL がフローを許可した場合。 1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
106015	最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。	3：フローが拒否されました。	1004：最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。
106023	**access-group** コマンドによってインターフェイスに接続された ACL によってフローが拒否された場合。	3：フローが拒否されました。	1001：入力 ACL によってフローが拒否されました。 1002：出力 ACL によってフローが拒否されました。
302013、302015、302017、302020	TCP、UDP、GRE、および ICMP 接続の作成。	1：フローが作成されました。	0：無視します。
302014、302016、302018、302021	TCP、UDP、GRE、および ICMP 接続のティアダウン。	2：フローが削除されました。	0：無視します。 > 2000：フローが切断されました。
313001	デバイスへの ICMP パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
313008	デバイスへの ICMP v6 パケットが拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。
710003	デバイス インターフェイスへの接続の試行が拒否されました。	3：フローが拒否されました。	1003：To-the-box フローが設定のために拒否されました。

（注） NSEL メッセージと syslog メッセージの両方がイネーブルにされている場合、2 つのロギング タイプ間が時系列順になる保証はありません。

クラスタリングの NSEL の使用

各 ASA は、そのユニット ローカル IP アドレスを使用して、コレクタへの独自の接続を確立します。エクスポート パケットのヘッダーのフィールドには、システムのアップ タイム、UNIX タイム（クラスタ間で同期される）、およびシーケンス番号が含まれます。これらのフィールドは、すべて個々の ASA に対してローカルです。NSEL コレクタは、パケットの送信元ポートの組み合わせを使用して、異なるエクスポータを区切ります。

各 ASA は、テンプレートを個別に管理し、アドバタイズします。ASA がクラスタ内アップグレードをサポートするため、特定の時点で、異なるユニットが異なるイメージ バージョンを実行する場合があります。その結果、各 ASA がサポートするテンプレートが異なる可能性があります。

（注）　クラスタリングは ASA 5580 および 5585-X でのみ使用できます。クラスタリングの詳細については、第 7 章「ASA のクラスタの設定」を参照してください。

NSEL のライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

NSEL の前提条件

NSEL には次の前提条件があります。

- IP アドレスとホスト名の割り当ては、NetFlow 設定の全体を通して固有である必要があります。
- NSEL を使用するには、少なくとも 1 つの設定済みのコレクタが必要です。
- モジュラ ポリシー フレームワークを経由してフィルタを設定するには、NSEL コレクタを設定する必要があります。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

class-map、**match access-list**、および **match any** コマンドで IPv6 がサポートされています。

その他のガイドラインと制限事項

- **flow-export enable** コマンドを使用して flow-export アクションを以前に設定しており、以降のバージョンにアップグレードしている場合、**policy-map** コマンドで説明されているように、設定は自動的に新しいモジュラ ポリシー フレームワーク **flow-export event-type** コマンドに変換されます。
- flow-export アクションは、インターフェイスに基づいたポリシーではサポートされません。flow-export アクションは class-map で **match access-list**、**match any**、または **class-default** コマンドだけを使用して設定できます。グローバル サービス ポリシー内だけで flow-export アクションを適用できます。
- NetFlow レコードの帯域幅使用状況を表示するには（リアルタイムには利用できません）、脅威検出機能を使用する必要があります。

- ASA 5580 および 5585-X のみがクラスタリングをサポートします。
- NetFlow レコードは送信元と宛先のアドレスが両方とも IPv4 または IPv6 である接続だけに送信されます。NetFlow レコードは NAT64 または NAT46 などの混合トラフィックとの接続用に送信されません。

NSEL の設定

この項では、NSEL を設定する方法について説明します。次の項目を取り上げます。

NSEL コレクタの設定

NSEL コレクタを設定するには、次のコマンドを入力します。

コマンド	目的
flow-export destination *interface-name ipv4-address|hostname udp-port* **例：** `hostname (config)# flow-export destination inside 209.165.200.225 2002`	NetFlow の送信先となる NSEL コレクタを追加、編集、または削除します。**destination** キーワードは NSEL コレクタが設定されていることを示します。*interface-name* 引数はコレクタが到達するために使用する ASA および ASA サービス モジュール インターフェイスの名前です。*ipv4-address* 引数は、コレクタ アプリケーションを実行しているマシンの IP アドレスです。*hostname* 引数は、コレクタの宛先 IP アドレスまたは名前です。*udp-port* 引数は NetFlow パケットの送信先である UDP ポート番号です。最大 5 つのコレクタを設定できます。コレクタを設定すると、すべての設定した NSEL コレクタにテンプレート レコードが自動的に送信されます。 **（注）** コレクタ アプリケーションが Event Time フィールドを使用してイベントを相互に関連付けていることを確認してください。

次の作業

「モジュラ ポリシー フレームワークを使用した flow-export アクションの設定」（P.82-6）を参照してください。

モジュラ ポリシー フレームワークを使用した flow-export アクションの設定

すべてのクラスを flow-export アクションを使用して定義することによって NSEL イベントをエクスポートするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**class-map** *flow_export_class* **例：** `hostname (config-pmap)# class-map flow_export_class`	NSEL イベントをエクスポートする必要があるトラフィックを識別するクラス マップを定義します。*flow_export_class* 引数は、クラス マップの名前です。
ステップ 2	次のいずれかのオプションを選択します。	
	match access-list *flow_export_acl* **例：** `hostname (config-cmap)# match access-list flow_export_acl`	特定のトラフィックと照合するアクセス リストを設定します。*flow_export_acl* 引数は、アクセス リストの名前です。
	match any **例：** `hostname (config-cmap)# match any`	任意のトラフィックと照合します。
ステップ 3	**policy-map** *flow_export_policy* **例：** `hostname(config)# policy-map flow_export_policy`	定義されたクラスに対する flow-export アクションを適用するポリシー マップを定義します。*flow_export_policy* 引数は、ポリシー マップの名前です。 ステップ 6 に従って新しいポリシー マップを作成してグローバルに適用するには、残りのインスペクション ポリシーを無効にする必要があります。 または、NetFlow クラスを既存のポリシーに挿入するには、**policy-map global_policy** コマンドの後に **class flow_export_class** コマンドを入力します。 モジュラ ポリシー フレームワークの作成または変更の詳細については、第 36 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください
ステップ 4	**class** *flow_export_class* **例：** `hostname (config-pmap)# class flow_export_class`	flow-export アクションを適用するクラスを定義します。*flow_export_class* 引数はクラスの名前です。

	コマンド	目的
ステップ 5	**flow-export event-type** *event-type* **destination** *flow_export_host1 [flow_export_host2]* **例：** `hostname (config-pmap-c)# flow-export event-type all destination 209.165.200.230`	flow-export アクションを設定します。**event_type** キーワードはフィルタリングされるサポートされているイベントの名前です。*flow_export_host* 引数は、ホストの IP アドレスです。**destination** キーワードは設定されたコレクタの IP アドレスです。
ステップ 6	**service-policy** *flow_export_policy* **global** **例：** `hostname (config)# service-policy flow_export_policy global`	サービス ポリシーをグローバルに追加または編集します。*flow_export_policy* 引数は、ポリシー マップの名前です。

次の作業

「テンプレート タイムアウト間隔の設定」（P.82-7）を参照してください。

テンプレート タイムアウト間隔の設定

テンプレート タイムアウト間隔を設定するには、次のコマンドを入力します。

コマンド	目的
flow-export template timeout-rate *minutes* **例：** `hostname (config)# flow-export template timeout-rate 15`	テンプレート レコードがすべての設定された出力先に送信される間隔を指定します。**template** キーワードは、テンプレート固有の設定を示します。**timeout-rate** キーワードは、テンプレートが再送信されるまでの時間を指定します。*minutes* 引数には、テンプレートが再送信されるときの分単位の時間間隔を指定します。デフォルト値は 30 分です。

次の作業

「flow-create イベントの遅延」（P.82-7）を参照してください。

flow-create イベントの遅延

flow-create イベントの送信を遅延させるには、次のコマンドを入力します。

コマンド	目的
flow-export delay flow-create *seconds* **例：** `hostname (config)# flow-export delay flow-create 10`	flow-create イベントの送信を指定した秒数遅らせます。*seconds* 引数は、遅延として許可された時間を秒単位で示します。このコマンドが設定されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。設定されている遅延よりも前にフローが切断された場合は、flow-create イベントは送信されません。その代わりに拡張フロー ティアダウン イベントが送信されます。

次の作業

「NetFlow 関連の syslog メッセージのディセーブル化と再イネーブル化」（P.82-8）を参照してください。

NetFlow 関連の syslog メッセージのディセーブル化と再イネーブル化

NetFlow 関連の syslog メッセージをディセーブルにしてから再度イネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**logging flow-export-syslogs disable** **例：** `hostname(config)# logging flow-export-syslogs disable`	NSEL のために冗長になった syslog メッセージをディセーブルにします。 **（注）** グローバル コンフィギュレーション モードでこのコマンドを実行しても、設定には保存されません。**no logging message** *xxxxxx* コマンドだけがコンフィギュレーションに格納されます。
ステップ 2	**logging message** *xxxxxx* **例：** `hostname(config)# logging message 302013`	個別に syslog メッセージを再イネーブルにします。*xxxxxx* は再イネーブルする指定した syslog メッセージです。
ステップ 3	**logging flow-export-syslogs enable** **例：** `hostname(config)# logging flow-export-syslogs enable`	すべての NSEL イベントを同時に再イネーブルにします。

次の作業

「ランタイム カウンタのクリア」（P.82-8）を参照してください。

ランタイム カウンタのクリア

ランタイム カウンタをリセットするには、次のコマンドを入力します。

コマンド	目的
clear flow-export counters **例：** `hostname# clear flow-export counters`	NSEL のすべてのランタイム カウンタをゼロにリセットします。

次の作業

「NSEL のモニタリング」（P.82-9）を参照してください。

NSEL のモニタリング

syslog メッセージを使用して、エラーのトラブルシューティングを行ったり、システムの使用状況およびパフォーマンスをモニタできます。ログ バッファに保存されているリアルタイムの syslog メッセージは、別のウィンドウで表示でき、メッセージの説明、メッセージの詳細、およびエラーを解決するために必要に応じて実行する推奨アクションが含まれています。詳細については、「NSEL メッセージと syslog メッセージの使用」（P.82-2）を参照してください。

NSEL モニタリング コマンド

NSEL をモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show flow-export counters	NSEL に対する統計データとエラー データを含む、ランタイム カウンタを表示します。
show running-config flow-export	現在設定されている NetFlow コマンドを示します。
show logging flow-export-syslogs	NSEL イベントによってキャプチャされたすべての syslog メッセージを表示します。
show running-config logging	ディセーブル化された syslog メッセージを表示します。ディセーブル化された syslog メッセージは NetFlow を経由して同じ情報をエクスポートするため、冗長な syslog メッセージです。

例

次に、flow-export カウンタを表示する例を示します。

```
hostname (config)# show flow-export counters

destination: inside 209.165.200.225 2055

Statistics:
   packets sent                 250
Errors:
   block allocation errors        0
   invalid interface              0
   template send failure          0
   no route to collector          0
   source port allocation         0
```

次に、flow-export 遅延コンフィギュレーションを表示する例を示します。

```
hostname (config)# show running-config flow-export delay
flow-export delay flow-create 30
```

次に、flow-export 宛先コンフィギュレーションを表示する例を示します。

```
hostname (config)# show running-config flow-export destination
```

```
flow-export destination inside 192.68.10.70 9996
```

次に、flow-export テンプレート コンフィギュレーションを表示する例を示します。

```
hostname (config)# show running-config flow-export template
flow-export template  timeout-rate 1
```

次に、flow-export syslog メッセージを表示する例を示します。

```
hostname# show logging flow-export-syslogs

Syslog ID       Type                          Status
302013          Flow Created                  Enabled
302015          Flow Created                  Enabled
302017          Flow Created                  Enabled
302020          Flow Created                  Enabled
302014          Flow Deleted                  Enabled
302016          Flow Deleted                  Enabled
302018          Flow Deleted                  Enabled
302021          Flow Deleted                  Enabled
106015          Flow Denied                   Enabled
106023          Flow Denied                   Enabled
313001          Flow Denied                   Enabled
313008          Flow Denied                   Enabled
710003          Flow Denied                   Enabled
106100          Flow Created/Denied           Enabled
```

次に、現在の syslog メッセージの設定を表示する例を示します。

```
hostname (config)# show running-config logging

no logging message 313008
no logging message 313001
```

NSEL の設定例

次に、すでに設定されている指定コレクタを使用して NSEL イベントをフィルタリングする例を示します。

- **flow-export destination inside 209.165.200.2055**
- **flow-export destination outside 209.165.201.29 2055**
- **flow-export destination outside 209.165.201.27 2055**

ホスト 209.165.200.224 と 209.165.201.224 から 209.165.200.230 までの間のすべてのイベントのログを記録し、209.165.201.29 へのその他のすべてのイベントのログを記録します。

```
hostname (config)# access-list flow_export_acl permit ip host 209.165.200.224 host
209.165.201.224
hostname (config)# class-map flow_export_class
hostname (config-cmap)# match access-list flow_export_acl
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class flow_export_class
hostname (config-pmap-c)# flow-export event-type all destination 209.165.200.230
hostname (config-pmap)# class class-default
hostname (config-pmap-c)# flow-export event-type all destination 209.165.201.29
hostname (config)# service-policy flow_export_policy global
```

209.165.200.230 への flow-create イベント、209.165.201.29 への flow-teardown イベント、および 209.165.201.27 への flow-denied イベントのログを記録します。

```
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class class-default
hostname (config-pmap-c)# flow-export event-type flow-creation destination 209.165.200.230
hostname (config-pmap-c)# flow-export event-type flow-teardown destination 209.165.201.29
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
hostname (config)# service-policy flow_export_policy global
```

ホスト 209.165.200.224 と 209.165.200.230 から 209.165.201.29 までの間の flow-create イベントのログを記録し、209.165.201.27 へのすべての flow-denied イベントのログを記録します。

```
hostname (config)# access-list flow_export_acl permit ip host 209.165.200.224 host
209.165.200.230
hostname (config)# class-map flow_export_class
hostname (config)# match access-list flow_export_acl
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class flow_export_class
hostname (config-pmap-c)# flow-export event-type flow-creation destination 209.165.200.29
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
hostname (config-pmap)# class class-default
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
hostname (config)# service-policy flow_export_policy global
```

（注） flow_export_acl については次のコマンドを入力する必要があります。

```
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
```

これは、最初の一致が検出された後トラフィックがチェックされないからです。*flow_export_acl* に一致する flow-denied イベントを記録するには、アクションを明示的に定義する必要があります。

ホスト 209.165.201.27 と 209.165.201.50 から 209.165.201.27 までの間のトラフィックを除くすべてのトラフィックのログを記録します。

```
hostname (config)# access-list flow_export_acl deny ip host 209.165.201.30 host
209.165.201.50
hostname (config)# access-list flow_export_acl permit ip any any
hostname (config)# class-map flow_export_class
hostname (config-cmap)# match access-list flow_export_acl
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class flow_export_class
hostname (config-pmap-c)# flow-export event-type all destination 209.165.201.27
hostname (config)# service-policy flow_export_policy global
```

関連情報

syslog サーバを設定するには、第 81 章「ロギングの設定」を参照してください。

その他の参考資料

NSEL の実装に関するその他の情報については、次の項を参照してください。

- 「関連資料」（P.82-12）
- 「RFC」（P.82-12）

関連資料

関連項目	ドキュメント名
「NSEL メッセージと syslog メッセージの使用」（P.82-2）	*syslog メッセージ ガイド*
ASA および ASA サービス モジュール での NSEL の実装に関する情報	*『Cisco ASA 5500 Series Implementation Note for NetFlow Collectors』* 次の URL にある資料を参照してください。 https://supportforums.cisco.com/docs/DOC-6113
ASDM を使用した ASA および ASA サービス モジュール での NetFlow の設定	次の URL にある資料を参照してください。 https://supportforums.cisco.com/docs/DOC-6114

RFC

RFC	タイトル
3954	『Cisco Systems NetFlow Services Export Version 9』

NSEL の機能履歴

表 82-2 に、機能に関する各変更およびこれらの変更が加えられたプラットフォーム リリースを示します。

表 82-2　NSEL の機能履歴

機能名	プラットフォーム リリース	機能情報
NetFlow	8.1(1)	NetFlow 機能は、NetFlow プロトコルを使用したフローに基づくイベントのロギングにより ASA のロギング機能を拡張します。NetFlow バージョン 9 サービスは、開始から終了までのフローの進行についての情報をエクスポートするために使用されます。NetFlow の実装はフローの有効期間における重要なイベントを示すレコードをエクスポートします。この実装は定期的にフローに関するデータをエクスポートする従来の NetFlow とは異なります。NetFlow モジュールは、アクセス リストによって拒否されたフローについてのレコードもエクスポートします。ASA 5580 を設定すると、NetFlow を使用して flow create、flow teardown、および flow denied（ACL によって拒否されたフローだけがレポートされます）イベントを送信できます。 **clear flow-export counters**、**flow-export enable**、**flow-export destination**、**flow-export template timeout-rate**、**logging flow-export syslogs enable**、**logging flow-export syslogs disable**、**show flow-export counters**、**show logging flow-export-syslogs** コマンドが導入されました。
NetFlow フィルタリング	8.1(2)	トラフィックとイベント タイプに基づいて NetFlow イベントをフィルタリングしてから、さまざまなコレクタにレコードを送信できます。たとえば、すべての flow-create イベントのログを 1 つのコレクタに記録し、flow-denied イベントのログを別のコレクタに記録できます。 **class**、**class-map**、**flow-export event-type destination**、**match access-list**、**policy-map**、**service-policy** コマンドが変更されました。 有効期間が短いフローの場合、NetFlow コレクタは、2 つのイベント（flow create イベントと flow teardown イベント）の代わりに 1 つのイベントを処理できるという利点があります。flow-create イベントを送信する前に遅延を設定できます。タイマーの期限が切れる前にフローが切断された場合は、flow teardown イベントだけが送信されます。teardown イベントには、そのフローに関するすべての情報が含まれ、情報の損失は発生しません。 **flow-export delay flow-create** コマンドが導入されました。
NSEL	8.2(1)	NetFlow 機能は、ASA のすべての使用可能なモデルに移植されました。
クラスタリング	9.0(1)	NetFlow 機能は、クラスタリングをサポートします。
NSEL		新しい NetFlow エラー カウンタ（送信元ポート割り当ての失敗）が追加されました。 **show flow-export counters** コマンドが変更されました。 フロー トラフィックの定期的なバイト カウンタを提供するために flow-update イベントが導入されました。flow-update イベントが NetFlow コレクタに送信される時間間隔を変更できます。flow-update レコードを送信するコレクタをフィルタリングできます。 **（注）** flow-update イベント機能は、バージョン 8.4(5) だけで使用できます。バージョン 9.0(1) 以降では使用できません。