CHAPTER 42

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.42-8）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、および flow-denied（EtherType ACL によって拒否されるフローを除く）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 9.0(1) では使用できません。バージョン 8.4(5) および 9.1(2) で使用できます。

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。
- フロー更新イベントがトリガーされ、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。サポートされるイベント タイプは、flow-create、flow-denied、flow-teardown、flow-update、all 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。
  - ACL 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。
  - collector 1 に対するすべての flow-update 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 42-1 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 42-1 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。

表 42-1　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）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 IP アドレスと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 10 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 event-type all** 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、NSEL は必要に応じて flow-update レコードの発行を自動的に開始します。
- 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。

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。

NetFlow の使用方法

[NetFlow] ペインでは、パケットのフローに関するデータの転送をイネーブルにできます。このペインにアクセスするには、[Configuration] > [Device Management] > [Logging] > [NetFlow] を選択します。

（注）　NetFlow コンフィギュレーション全体で IP アドレスとホスト名の割り当てが一意である必要があります。

NetFlow を使用するには、次の手順を実行します。

ステップ 1　テンプレート タイムアウト レートを分単位で入力します。テンプレート タイムアウト レートとは、設定されたすべてのコレクタにテンプレート レコードが送信される時間間隔です。デフォルト値は 30 分です。

ステップ 2　フロー更新間隔を入力します。これは、フロー更新イベント間の時間間隔を分単位に指定するものです。有効な値は、1 ～ 60 分です。デフォルト値は 1 分です。

ステップ 3　フロー作成イベントのエクスポートを遅延させ、フロー ティアダウン イベントをフロー作成イベントとは別に単独で処理する場合は、[Delay export of flow creation events for short-lived flows] チェックボックスをオンにし、遅延の秒数を [Delay By] フィールドに入力します。

ステップ 4　NetFlow パケットの送信先となるコレクタを指定します。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場合は、まず [Add] をクリックして [Add NetFlow Collector] ダイアログボックスを表示します。それ以降は、次の手順を実行します。

a. NetFlow パケットの送信先となるインターフェイスを、ドロップダウン リストから選択します。

b. IP アドレスまたはホスト名、および UDP ポート番号を、それぞれ該当するフィールドに入力します。

c. [OK] をクリックします。

ステップ 5　さらに別のコレクタも設定する場合は、コレクタごとにステップ 4 を繰り返します。

ステップ 6　コレクタの詳細設定を変更する場合は、コレクタを選択し、[Edit] をクリックします。設定したコレクタを削除する場合は、そのコレクタを選択し、[Delete] をクリックします。

ステップ 7　NetFlow がイネーブルになっている場合、一部の syslog メッセージに重複が生じます。これは、同一の情報が NetFlow を介してエクスポートされるためです。システムのパフォーマンスを維持するためにも、重複により不要となった syslog メッセージはすべてディセーブルにすることをお勧めします。不要な syslog メッセージをすべてディセーブルにする場合は、[Disable redundant syslog messages] チェックボックスをオンにします。不要な syslog メッセージおよびそのステータスを表示する場合は、[Show Redundant Syslog Messages] をクリックします。

[Redundant Syslog Messages] ダイアログボックスが表示されます。不要な syslog メッセージの番号が、[Syslog ID] フィールドに表示されます。[Disabled] フィールドには、指定した syslog メッセージがディセーブルになっているかどうかが表示されます。[OK] をクリックして、このダイアログボックスを閉じます。

不要な syslog メッセージを個別にディセーブルにする場合は、[Configuration] > [Device Management] > [Logging] > [Syslog Setup] を選択します。

ステップ 8　[Apply] をクリックして変更内容を保存します。新しい設定内容を入力する場合は、[Reset] をクリックします。

次の作業

「NetFlow イベントと設定済みコレクタとの対応付け」（P.42-6）を参照してください。

NetFlow イベントと設定済みコレクタとの対応付け

NetFlow コレクタの設定が完了すると、それらの設定済みコレクタと NetFlow イベントを対応付けることができます。

送信する NetFlow イベントおよびその宛先となるコレクタを指定するには、次の手順を実行します。

ステップ 1　ASDM のメイン アプリケーション ウィンドウで、[Configuration] > [Firewal]l > [Service Policy Rules] を選択します。

ステップ 2　サービス ポリシー ルールを追加するには、次の手順を実行します。

a. [Add] をクリックして、[Add Service Policy Rule Wizard] を表示します。サービス ポリシー ルールに関する詳細については、ファイアウォール コンフィギュレーション ガイドの“Adding a Service Policy Rule for Through Traffic” section on page 41-19 を参照してください。

b. [Global - applies to all interfaces] オプション ボタンをクリックして、ルールをグローバル ポリシーに適用します。[Next] をクリックします。

c. [Source and Destination IP Address (uses ACL)] チェックボックスまたは [Any traffic] チェックボックスをトラフィック一致基準としてオンにするか、[Use class-default as traffic class] オプション ボタンをクリックします。[Next] をクリックして、[Rule Actions] 画面に進みます。

（注）　NetFlow のアクションは、グローバル サービス ポリシー ルールに対してだけ使用可能で、その適用対象は class-default トラフィック クラス、およびトラフィック照合基準として [Source and Destination IP Address (uses ACL)] または [Any Traffic] が選択されているトラフィック クラスに限定されます。

ステップ 3　[Rule Actions] 画面で、[NetFlow] タブをクリックします。

ステップ 4　フロー イベントを設定する場合は、まず [Add] をクリックして [Add Flow Event] ダイアログボックスを表示します。それ以降は、次の手順を実行します。

a. ドロップダウン リストから、フロー イベント タイプを選択します。選択できるイベントは、[created]、[torn down]、[denied]、[updated]、[all] です。

（注）　flow-update イベント機能は、バージョン 9.0（1）では使用できません。バージョン 8.4(5) および 9.1(2) で使用できます。

b. [Send] カラムで、イベントの宛先となるコレクタを選択します。コレクタは、対応するチェックボックスをオンにすると選択できます。

c. コレクタを追加、編集、削除する場合、または他の NetFlow 設定値（syslog メッセージなど）を設定する場合は、[Manage] をクリックして、[Manage NetFlow Collectors] ダイアログボックスを表示します。[OK] をクリックして、[Manage NetFlow Collectors] ダイアログボックスを閉じ、[Add Flow Event] ダイアログボックスに戻ります。コレクタの設定方法の詳細については、「NetFlow の使用方法」（P.42-5）のステップ 4 を参照してください。

ステップ 5　[OK] をクリックして、[Add Flow Event] を閉じ、[NetFlow] タブに戻ります。

ステップ 6　フロー イベント エントリを変更する場合は、リストからエントリを選択し、[Edit] をクリックします。フロー イベント エントリを削除する場合は、リストからエントリを選択し、[Delete] をクリックします。

ステップ 7　[Finish] をクリックして、ウィザードを終了します。

ステップ 8　NetFlow サービス ポリシー ルールを編集するには、次の手順を実行します。

a. [Service Policy Rules] テーブルで選択し、[Edit] をクリックします。

b. [Rule Actions] タブをクリックし、さらに [NetFlow] タブをクリックします。

次の作業

「NSEL のモニタリング」（P.42-7）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.42-2）を参照してください。

NSEL をモニタするには、次のペインを参照してください。

パス	目的
[Tools] > [Command Line Interface] **show flow-export counters** コマンドを入力し、[Send] をクリックします。	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。
[Tools] > [Command Line Interface] **show logging flow-export-syslogs** と入力し、[Send] を押します。	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。
[Tools] > [Command Line Interface] **show running-config flow-export** コマンドを入力し、[Send] をクリックします。	現在設定されている NetFlow コマンドを示します。
[Tools] > [Command Line Interface] **show running-config logging** コマンドを入力し、[Send] をクリックします。	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。

関連情報

syslog サーバを設定するには、第 41 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.42-8）
- 「RFC」（P.42-8）

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.42-2）	*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 42-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 42-2　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、ACL 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。 次の画面が導入されました。[Configuration] > [Device Management] > [Logging] > [NetFlow]。
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。 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。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules]。
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。 **（注）**　flow-update イベント機能は、バージョン 9.0(1) では使用できません。
NSEL	9.1(2)	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。 次の画面が変更になりました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule Wizard - Rule Actions] > [NetFlow] > [Add Flow Event] [Configuration] > [Device Management] > [Logging] > [NetFlow]。