NetFlow Collector インプリメンテーション ノート バージョン 9.2

このドキュメントでは、ASA 用に NetFlow コレクタの使用を実装する方法を説明します。次の項目で構成されています。

イベント駆動型のデータのエクスポート

ASA は、フローのステートフル トラッキングを実装するので、トラッキングされたフローには、一連の状態変化が生じます。NetFlow は、フローのステータスに関するデータをエクスポートするツールで、状態変化をもたらすイベントによってトリガーされます。トラッキング対象のイベントには、フロー作成、フロー拒否（ACL によって拒否されたフローのみ）、およびフロー ティアダウンが含まれます。

ASA は、フロー トラフィックのバイト カウンタを定期的に提供するために、フロー単位のタイマーを発行して、ステート トラッキングに加えて、定期的な NSEL イベントを生成します。フローの更新イベントとも呼ばれるこの定期的な NSEL イベントは、通常はタイマーで実行され、従来の NetFlow に対応しています。ただし、フロー更新イベントは、フローの状態変化によってトリガーされる場合もあります。

ASA はまた、syslog メッセージもエクスポートしますが、これには同じ情報が含まれています。そこで同じイベントに対して NSEL レコードと syslog メッセージが生成されないように、同じ情報を持つ syslog メッセージをディセーブルにすることで、パフォーマンスの低下を防止できます。重複した syslog メッセージのリストについては、Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）の「Using NSEL and Syslog Messages（NSEL および Syslog メッセージの使用）」の項を参照してください。

双方向のフロー

双方向のフローのほとんどは、すでに内部でアセンブルされ、単一のフローとして扱われています。NSEL が ASA に関してレポートするフロー レコードには、双方向のフローが記載されます。データ レコードでは、送信元（発信側）と宛先（応答側）が明示されるので、コレクタ アプリケーションがフローの方向を区別する必要がある場合は、この情報を使用して判断できます。さらに、一部の NSEL レコードには 2 バイトのカウンタ フィールドである NF_F_FWD_FLOW_DELTA_BYTES と NF_F_REV_FLOW_DELTA_BYTES が含まれ、方向固有のトラフィック データを提供します。

テンプレートの更新

RFC の規定によると、テンプレートは、一定の時間間隔または一定数のデータ レコードがエクスポートされた後、のいずれかの更新間隔でユーザに送信できます。このような更新間隔は、設定可能である必要があります。この実装では、時間間隔によるテンプレートの更新のみをサポートします。データ レコード数に基づくテンプレート更新は、サポートされていません。

オプションのテンプレートとデータ レコード

オプションのテンプレートとデータ レコードは、エクスポートされません。一部のフィールドは、CLI の **show** コマンドによってサポートされています。コレクタ アプリケーションが特定のフィールドに関する追加情報を取得するには、**show** コマンドを実行する必要があります。また、コレクタには、一意のホスト名と IP アドレスが必要です。そうでなければ、検査動作が予測不可能になります。詳細については、「情報モデル」（P.3）および Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）を参照してください。

観測ポイントと観測ドメイン

ASA は観測ドメインで、各インターフェイスも観測ポイントです。フローは、作成インターフェイスに関係なくすべてエクスポートされます。特定のインターフェイスのセットによって作成されたデータに限定し、またはそれらのデータをフィルタリングしてエクスポートするオプションは存在しません。ASA に外部デバイスが接続されている場合、その外部デバイスによって作成されるフローもエクスポートされます。

フローのフィルタリング

特定のフローのレコードだけをエクスポートする必要が生じることがあります。この場合、たとえば、ASA は、ACE に一致するフローの NSEL イベントを生成できます。この方法を使用すれば、NetFlow 用に生成される NSEL イベントの数を制限できます。この実装では、Modular Policy Framework によってトラフィックやイベント タイプごとに NSEL イベントをフィルタリングし、レコードを異なるコレクタに送信する処理がサポートされます。

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。

- すべてのフロー作成イベントをコレクタ 1 にロギングする。
- ACL1 に一致するすべてのフロー拒否イベントをコレクタ 1 にロギングする。
- ACL1 に一致するすべてのイベントをコレクタ 2 にロギングする。

Modular Policy Framework が NetFlow 用に設定されていない場合、NSEL イベントは生成されません。詳細については、Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）およびコマンド リファレンスを参照してください。

トランスポート プロトコル

NetFlow のこの実装は、UDP ペイロードのみをサポートします。

情報モデル

この項では、NetFlow によってエクスポートされるデータ タイプとテンプレートについて説明します。次の項目を取り上げます。

- データ フィールド
- データ レコードとテンプレート

必須データ要素のリストは、イベントに対して生成された syslog メッセージによってエクスポートされ、NSEL レコードのエクスポートをもたらすデータを集約して作成されました。

データ フィールド

表 1 に、ASA から NSEL 経由でエクスポートされるデータ要素を示します。

各列では、次の情報を示します。

- ID：フィールド タイプを表す一意の名前
- タイプ：このフィールド タイプに割り当てられた値
- 長さ：対象の ASA 用にエクスポートされるレコードのフィールド長
- 説明：フィールド タイプの説明

表 1　　NSEL によってエクスポートされるデータ レコード

ID	タイプ	長さ	説明
接続 ID フィールド			
NF_F_CONN_ID	148	4	デバイスの一意のフロー用の ID
フロー ID フィールド（L3 IPv4）			
NF_F_SRC_ADDR_IPV4	8	4	発信元 IPv4 アドレス
NF_F_DST_ADDR_IPV4	12	4	送信先 IPv4 アドレス
NF_F_PROTOCOL	4	1	IP 値
フロー ID フィールド（L3 IPv6）			
NF_F_SRC_ADDR_IPV6	27	16	発信元 IPv6 アドレス
NF_F_DST_ADDR_IPV6	28	16	送信先 IPv6 アドレス
フロー ID フィールド（L4）			
NF_F_SRC_PORT	7	2	送信元ポート
NF_F_DST_PORT	11	2	宛先ポート
NF_F_ICMP_TYPE	176	1	ICMP タイプ値
NF_F_ICMP_CODE	177	1	ICMP コード値
NF_F_ICMP_TYPE_IPV6	178	1	ICMP IPv6 タイプ値
NF_F_ICMP_CODE_IPV6	179	1	ICMP IPv6 コード値
フロー ID フィールド（INTF）			
NF_F_SRC_INTF_ID	10	2	入力 IFC SNMP IF インデックス
NF_F_DST_INTF_ID	14	2	出力 IFC SNMP IF インデックス
マッピングされたフロー ID フィールド（L3 IPv4）			
NF_F_XLATE_SRC_ADDR_IPV4	225	4	NAT 後の送信元 IPv4 アドレス
NF_F_XLATE_DST_ADDR_IPV4	226	4	NAT 後の宛先 IPv4 アドレス
NF_F_XLATE_SRC_PORT	227	2	NATT 後の送信元トランスポート ポート
NF_F_XLATE_DST_PORT	228	2	NATT 後の宛先トランスポート ポート
マッピングされたフロー ID フィールド（L3 IPv6）			
NF_F_XLATE_SRC_ADDR_IPV6	281	16	NAT 後の送信元 IPv6 アドレス
NF_F_XLATE_DST_ADDR_IPV6	282	16	NAT 後の宛先 IPv6 アドレス

表 1　NSEL によってエクスポートされるデータ レコード （続き）

ID	タイプ	長さ	説明
ステータスまたはイベント フィールド			
NF_F_FW_EVENT	233	1	高レベルのイベント コード。表示される値は次のとおりです。 • 0：デフォルト（無視）。 • 1：フローが作成されました。 • 2：フローが削除されました。 • 3：フローが拒否されました。 • 4：フロー アラート • 5：フロー更新
NF_F_FW_EXT_EVENT	33002	2	拡張イベント コード これらの値は、イベントに関する詳細情報を提供します。
タイムスタンプおよび統計情報フィールド			
NF_F_EVENT_TIME_MSEC	323	8	IPFIX から取得されたイベントが発生した時刻。マイクロ秒単位の場合は 324、ナノ秒単位の場合は 325 を使用します。時刻は、0000 UTC 1970/01/01 からの経過時間をミリ秒単位で表示します。
NF_F_FLOW_CREATE_TIME_MSEC	152	8	フローが作成された時刻。フロー作成イベントが先に送信されなかったフローティアダウン イベントに含まれます。フローの持続時間は、フローティアダウン時刻とフロー作成時刻のイベント時刻を使用して判定できます。
NF_F_FWD_FLOW_DELTA_BYTES	231	4	送信元から宛先への差分バイト数。
NF_F_REV_FLOW_DELTA_BYTES	232	4	宛先から送信元への差分バイト数。
ACL フィールド			
NF_F_INGRESS_ACL_ID	33000	12	フローを許可または拒否した入力 ACL すべての ACL ID は、次の 3 つの 4 バイト値で構成されます。 • ACL 名のハッシュ値または ID • ACL 内の ACE のハッシュ値、ID、または行 • 拡張 ACE 設定のハッシュ値または ID
NF_F_EGRESS_ACL_ID	33001	12	フローを許可または拒否した出力 ACL
AAA フィールド			
NF_F_USERNAME	40000	。	AAA ユーザ名
NF_F_USERNAME_MAX	40000	65	最大許可サイズの AAA ユーザ名

イベント ID フィールド

イベント ID フィールドには、NSEL レコードが発生したイベントが記述されます。表 2 では、イベント ID の値を示します。

表 2　　イベント ID の値

イベント ID	説明
0	無視：この値は、フィールドを無視する必要があることを示します。この値は、現在のリリースでは使用されません。
1	フロー作成：この値は、新しいフローが作成されたことを示します。
2	フロー削除：この値は、フローが削除されたことを意味します。
3	フロー拒否：この値は、フローが拒否されたことを意味します。
5	フロー更新：この値は、フローのタイマーが停止またはフローが切断されたことを示します。

拡張イベント ID フィールド

拡張イベント ID は、特定のイベントに関する追加情報を提供します。このフィールドは、製品固有のフィールド ID（33002）を含みます。表 3 では、拡張イベント ID の値を示します。

表 3　　拡張イベント ID の値

拡張イベント ID	イベント	説明
0	Ignore	この値は、フィールドを無視する必要があることを示します。
> 1000	フロー拒否	1000 を超える値は、フローが拒否された理由を表します。
1001	フロー拒否	フローが入力 ACL から拒否されました。
1002	フロー拒否	フローが出力 ACL によって拒否されました。
1003	フロー拒否	考えられる原因は、次のとおりです。 • ASA インターフェイスへの接続の試みが拒否されました。 • デバイスへの ICMP パケットが拒否されました。 • デバイスへの ICMPv6 パケットが拒否されました。
1004	フロー拒否	TCP の最初のパケットが TCP SYN パケットではありませんでした。
> 2000	フロー削除	2000 を超える値は、フローが終了した理由を表します。

イベント時間フィールド

各 NSEL データ レコードには、イベント時間フィールド（NF_F_EVENT_TIME_MSEC）があります。これは、ミリ秒単位でのイベント発生時刻です。NetFlow パケットは、複数のイベントを入れて作成することができます。ただし、NetFlow サービスが複数のイベントの発生を待って NetFlow パケットを作成するので、パケットの送信時刻がイベント発生時刻と必ずしも一致しません。

（注） フローの寿命の中で、異なるイベントが別々の NetFlow パケットによって発行され、発生順とは逆の順序でコレクタに届くことがあります。たとえば、フロー ティアダウン イベントが入ったパケットが、フロー作成イベントの入ったパケットより先に到着することもあります。そのため、コレクタ アプリケーションが、イベント時間フィールドを使用してイベントの前後関係を判断することが重要です。

データ レコードとテンプレート

この項では、さまざまなイベント用にサポートされるテンプレートについて説明します。次の項目を取り上げます。

- フロー作成イベント用テンプレート
- フロー ティアダウン イベント用テンプレート
- フロー拒否イベント用テンプレート
- 拡張フロー ティアダウン イベント用テンプレート
- フローの更新イベント用テンプレート
- フローの更新（タイマー）とフロー更新（ティアダウン）イベント
- フロー更新レコードとフェールオーバー
- フロー更新イベントとクラスタリング

テンプレートは、NetFlow 経由でエクスポートされたデータ レコードの形式を記述します。次のように、各フロー イベントには、いくつかのレコード形式、またはそれに関連付けられたテンプレートがあります。

- テンプレートは、イベントによって異なります。
- IPv4 フローと IPv6 フローの各イベント タイプには、異なるテンプレートが用意されています。
- IPV44、IPV46、IPV64 および IPV66 フローの各イベント タイプには、異なるテンプレートが用意されています。
- フロー作成 / 許可イベントには、フローに関連付けられたユーザ名フィールドのサイズに基いて、さまざまなテンプレートがあります。NetFlow の文字列フィールドのサイズは固定なので、サイズに応じて異なるテンプレートが必要になります。ほとんどの文字列は、最大文字列よりはるかに短いため、考えられる最大文字列に対応するテンプレートをすべての場合に使用すると、帯域幅が無駄になります。ユーザ名フィールドは、2 つのタイプが定義されているため、各カテゴリに 2 つのタイプのテンプレートが存在します。
  - 20 文字未満のユーザ名に対応する一般的なユーザ名サイズ
  - 最大 65 文字までのユーザ名に対応する最大ユーザ名サイズ
  - 各テンプレートには、イベント タイプ フィールドと拡張イベント タイプ フィールドがあります。

- フロー拒否イベントとフロー削除イベントには、IPV46 と IPV64 のテンプレートがあり、宛先 IP アドレスは NAT ルールにより変換されているが、送信元 IP アドレスが NAT ルールにより変換されていないため、送信元と宛先の IP アドレスの IP バージョンが異なります。送信元と宛先の NAT ルールは同時に適用されません（宛先 NAT ルールが最初に適用されます）。このため、両方の NAT ルールが適用される前か、どちらか 1 つの NAT ルールだけが使用可能なときに NetFlow レコードが生成される可能性があります。

  フローを作成するには、送信元と宛先の IP アドレスの IP バージョンが同じである必要があるため、これらの断片的な NAT 変換テンプレートは、フロー作成イベントと遅延フロー作成イベントには必要ではありません。

（注） テンプレート定義は、すべてのコレクタに送信され、データ レコートの解析には、これらの ID と定義を使用する必要があります。

フロー作成イベント用テンプレート

フロー作成イベントは、ASA によってフローが作成されたことを示します。このイベントは、ASA で使用できるフローのログでもあります。表 4 では、フロー作成イベントに使用されるテンプレートについて説明します。

表 4　　フロー作成イベント用テンプレート

説明	フィールド
一般的なユーザ名サイズ（20 文字）の IPv44 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_F_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME
最大ユーザ名サイズ（65 文字）の IPv44 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、 NF_F_SRC_PORT、NF_F_SRC_INTF_ID、 NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、 NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、 NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、 NF_F_FLOW_CREATE_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、 NF_F_USERNAME_MAX

表 4　　フロー作成イベント用テンプレート （続き）

説明	フィールド
一般的なユーザ名サイズ（20 文字）の IPv66 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME
最大ユーザ名サイズ（65 文字）の IPv66 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX
一般的なユーザ名サイズ（20 文字）の IPv46 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME

表 4　フロー作成イベント用テンプレート （続き）

説明	フィールド
最大ユーザ名サイズ（65 文字）の IPv46 フロー作成イベント	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX
一般的なユーザ名サイズ（20 文字）の IPv64 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME
最大ユーザ名サイズ（65 文字）の IPv64 フロー作成	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX

フロー作成イベントのための遅延

存続期間が短いフローの場合、NSEL コレクション デバイスは、フロー作成とフロー ティアダウンを 2 つのイベントとして処理するよりも、単一のイベントとして処理する方が好都合です。そこで、フロー作成イベントの送信を遅らせるための設定可能な CLI パラメータが用意されています。タイマーが切れると、フロー作成イベントが送信されます。しかし、タイマーの期限が切れる前にフローがティアダウンされると、フローティアダウン イベント *のみ*が送信され、フロー作成イベントが送信されません。

フローティアダウン イベントが拡張され、フローに関するすべての情報が入っていれば、情報が失われることはありません。拡張フローティアダウン イベントに対応する新しいテンプレートが導入されています。

拡張フロー ティアダウン イベント用テンプレート

表 5 では、拡張フローティアダウン イベントに使用されるテンプレートについて説明します。

表 5　　拡張フロー ティアダウン イベント用テンプレート

説明	フィールド
一般的なユーザ名サイズ（20 文字）の拡張 IPv44 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME
最大ユーザ名サイズ（65 文字）の拡張 IPv44 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX

表 5　　拡張フロー ティアダウン イベント用テンプレート （続き）

一般的なユーザ名サイズ（20 文字）の拡張 IPv66 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME
最大ユーザ名サイズ（65 文字）の拡張 IPv66 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX
一般的なユーザ名サイズ（20 文字）の拡張 IPv46 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME
最大ユーザ名サイズ（65 文字）の拡張 IPv46 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX

表 5　拡張フロー ティアダウン イベント用テンプレート （続き）

一般的なユーザ名サイズ（20 文字）の拡張 IPv64 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME
最大ユーザ名サイズ（65 文字）の拡張 IPv64 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME_MAX

フロー拒否イベント用テンプレート

フロー拒否イベントは、フローが拒否されたことを示します。表 6 では、フロー拒否イベントに使用されるテンプレートについて説明します。

表 6　フロー拒否イベント用テンプレート

説明	フィールド
IPv44 フロー拒否	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID
IPv4 フロー拒否（xlate フィールドなし）	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID

表 6　　フロー拒否イベント用テンプレート

説明	フィールド
IPv66 フロー拒否	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、 NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_ICMP_CODE_IPV6、 NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、 NF_F_EGRESS_ACL_ID
IPv6 フロー拒否 （xlate フィールドなし）	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、 NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、 NF_F_EVENT_TIME_MSEC、NF_F_INGRESS_ACL_ID、 NF_F_EGRESS_ACL_ID
IPv46 フロー拒否	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、 NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID
IPv46 フロー拒否 （送信元が未変換）	NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、 NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE、NF_F_ICMP_CODE、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID

表 6　フロー拒否イベント用テンプレート

説明	フィールド
IPv64 フロー拒否	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、 NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID
IPv64 フロー拒否 （送信元が未変換）	NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、 NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID

フロー ティアダウン イベント用テンプレート

フロー ティアダウン イベントは、フローが終了したことを示します。表 7 では、フロー ティアダウン イベントに使用されるテンプレートについて説明します。

表 7　フロー ティアダウン イベント用テンプレート

説明	フィールド
IPv44 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、 NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、 NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_FWD_FLOW_DELTA_BYTES、 NF_F_REV_FLOW_DELTA_BYTES、 NF_F_FLOW_CREATE_TIME_MSEC
IPv66 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、 NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、 NF_F_DST_INTF_ID、NF_F_PROTOCOL、 NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、 NF_F_XLATE_SRC_ADDR_IPV6、 NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、 NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、 NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、 NF_F_FWD_FLOW_DELTA_BYTES、 NF_F_REV_FLOW_DELTA_BYTES、 NF_F_FLOW_CREATE_TIME_MSEC

表 7　　フロー ティアダウン イベント用テンプレート

説明	フィールド
IPv46 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC
IPv46 フロー ティアダウン（送信元が未変換）	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV4、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV4、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE、NF_F_ICMP_CODE、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV6、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC
IPv64 フロー ティアダウン	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV4、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC
IPv64 フロー ティアダウン（送信元が未変換）	NF_F_CONN_ID、NF_F_SRC_ADDR_IPV6、NF_F_SRC_PORT、NF_F_SRC_INTF_ID、NF_F_DST_ADDR_IPV6、NF_F_DST_PORT、NF_F_DST_INTF_ID、NF_F_PROTOCOL、NF_F_ICMP_TYPE_IPV6、NF_F_ICMP_CODE_IPV6、NF_F_XLATE_SRC_ADDR_IPV6、NF_F_XLATE_DST_ADDR_IPV4、NF_F_XLATE_SRC_PORT、NF_F_XLATE_DEST_PORT、NF_F_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FWD_FLOW_DELTA_BYTES、NF_F_REV_FLOW_DELTA_BYTES、NF_F_FLOW_CREATE_TIME_MSEC

フローの更新イベント用テンプレート

フロー更新イベントは、フローのフロー更新タイマーが停止したか、フローが切断されたことを示します。このイベントは、フロー トラフィックの定期的バイト カウンタとして機能します。フロー更新イベントは、断片的な NAT 変換のテンプレートを除き、フロー ティアダウン イベントと同じテンプレートを使用します。NF_F_FWD_FLOW_DELTA_BYTES と NF_F_REV_FLOW_DELTA_BYTES フィールドには、最後のタイマー インターバル以降のバイト数が含まれます。NF_F_FW_EXT_EVENT フィールドは未使用であり、フロー更新レコードで無視されます。フロー ティアダウン イベントに使用されるテンプレートについては、表 7 を参照してください。

フローの更新（タイマー）とフロー更新（ティアダウン）イベント

ASA を通過するフローにはフロー更新タイマーが設定され、タイマーが停止すると、NSEL がフロー更新（タイマー）レコードを発行します。設定された時間間隔にフローのアクティビティが存在しない場合、その間隔のフロー更新（タイマー）レコードは送信されません。フロー ティアダウン レコードを伴ったフロー更新（ティアダウン）レコードが送信され、最後の時間間隔のトラフィックが検出されます。最後のインターバルにフローのトラフィックがなかった場合、フロー更新（ティアダウン）レコードは送信されません。また、フローが短期間であった場合（つまり、最初のフロー更新（タイマー）イベントが発生する前にティアダウンが発生した場合）、フロー更新（ティアダウン）レコードは送信されません。

フローの作成時にフロー更新コレクタが設定されていないか、フロー更新イベント中にフロー更新コレクタが削除された場合、フロー更新タイマーは設定されず、再び設定されることもありません。このような状況で、フロー更新（タイマー）イベントやフロー更新（ティアダウン）イベントが再び発生することはありません。

フロー更新レコードとフェールオーバー

フェールオーバーの前後に、フロー更新レコードの一貫性の維持が試行されます。フェールオーバーの発生後、すべてのフロー更新レコードは、直前のアクティブな ASA からの最新の更新に基づいています。この更新は 15 秒ごとにトラフィックが流れている限り発生します。フェールオーバー ペアの生成に時間差が生じた場合、またはアクティブな ASA が定期更新をスタンバイ ASA に送信する前にフェールオーバーが発生した場合、フロー更新レコードは正確でない場合があります。

フロー更新イベントとクラスタリング

1 つの大きな相違が、フェールオーバーおよびクラスタ処理とフロー更新イベントとの相互作用から生じます。クラスタ処理では、所有権の変更前は、フロー ディレクタがアクティブなリフレッシュ タイマーの設定されていない元のフローのスタブ フロー コピーを所持しています。アクティブなリフレッシュ タイマーが設定された完全なフローのコピーは、元のフローの所有者がダウンした後に生成されます。したがって、元のフロー所有者と新しいフロー所有者の間で、フロー更新タイマーの停止時間に顕著な時間オフセットが発生する可能性が高くなります。

クラスタ内でフロー所有権が変更された後、すべてのフロー更新レコードは、フロー ディレクタが受信した最新の更新に基づいています。フロー情報はトラフィックがある限り 15 秒ごとに更新されます。最新のフロー情報を維持するための方法は、フェールオーバー用に提供された方法と同じです。

NetFlow とフェールオーバー

NetFlow データ レコードおよびテンプレートは、アクティブ / スタンバイ フェールオーバー ペアのアクティブ（プライマリ）ASA からのみ送信されます。スタンバイ（セカンダリ）ASA は、NetFlow 関連の情報を送信しません。ただし、フェールオーバー後、セカンダリ ASA は、複製または新規のフローに対するテンプレートと NetFlow レコードの送信を開始します。この 2 つの ASA では、各 NetFlow コレクタの接続元 IP アドレスは同じですが、送信元ポートは異なります。これは NetFlow コレクタがプライマリ装置とセカンダリ装置から送信されるパケットを区別できることを意味します。

アクティブ / アクティブ フェールオーバー ペアでは、両方の ASA が NetFlow データ レコードとテンプレートを同時に送信することがあります。コンテキストごとのアクティブ装置だけが NetFlow パケットを送信し、スタンバイ装置は送信しません。これはアクティブ / スタンバイのシナリオとほぼ同じです。ASA コンテキストとそのコピーでは、NetFlow コレクタの接続元 IP アドレスは同一ですが、送信元ポートは異なります。

フェールオーバー ペアの各 ASA ノード（コンテキスト）は、NetFlow コレクタへの独自の接続を確立し、テンプレートを個別にアドバタイズします。コレクタは NetFlow エクスポータを区別するためにパケットの送信元 IP アドレスと送信元ポートを使用します。

NetFlow とクラスタリング

NetFlow は、管理と通常の両方のデータ インターフェイスでサポートされますが、管理インターフェイスを使用することを推奨します。NetFlow コレクタの接続が管理専用インターフェイスで設定されている場合、クラスタ内の各 ASA は、NetFlow パケットの送信に独自のユニットごとの送信元 IP アドレスと送信元ポートを使用します。NetFlow は、レイヤ 2 モードおよびレイヤ 3 モードでは両方のデータ インターフェイスで使用される場合があります。レイヤ 2 モードのデータ インターフェイスでは、クラスタ内の各 ASA の送信元 IP アドレスは同一ですが、送信元ポートは異なります。レイヤ 2 モードではクラスタを 1 つのデバイスとして認識するように設計されていますが、NetFlow コレクタはクラスタの各ノードを区別できます。レイヤ 3 モードのデータ インターフェイスでは、NetFlow は管理専用インターフェイスと同じ方法で動作します。

クラスタ内の各 ASA ノードは、NetFlow コレクタへの独自の接続を確立し、テンプレートを個別にアドバタイズします。コレクタは NetFlow エクスポータを区別するためにパケットの送信元 IP アドレスと送信元ポートを使用します。

コマンドライン インターフェイス

ASA で NSEL の実装を設定するためのコマンドについては、Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）およびコマンド リファレンスを参照してください。コマンドを使用して、NSEL レコードのフィールドに関する追加情報を表示することもできます。

外部パートナーの実装に関するアドバイス

この項では、イベントを生成するフローの例を示し、ASA 用の新しい NSEL フィールドをサポートするコレクタの実装方法について説明します。次の項目を取り上げます。

- 例 1：PAT インターフェイスを持つ許可されたフロー
- 例 2：PAT インターフェイスを持つ、出力時に拒否されたフロー

例 1：PAT インターフェイスを持つ許可されたフロー

次の例では、PAT インターフェイスを使用する、許可されたフローを示します。出力インターフェイスの IP アドレスは、209.165.200.225 です。ユーザは、User A として認証されます。ACL は指定されていませんが、フローは発信なので、デフォルトで許可されています。図 1 および記載された説明に従い、フロー作成イベントが発行されます。

図 1　　PAT インターフェイスを持つ許可されたフローの例

作成された NSEL レコードには、次のフィールドと値が含まれます。

フィールド	値
NF_F_CONN_ID	xxxx
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	56789
NF_F_SRC_INTF_ID	1
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80
NF_F_DST_INTF_ID	0
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	1024
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	1
NF_F_FW_EXT_EVENT	0
NF_F_EVENT_TIME_MSEC	YYYYYYYY

フィールド	値
NF_F_CONN_ID	xxxx
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	56789
NF_F_SRC_INTF_ID	1
NF_F_INGRESS_ACL_ID	0
NF_F_EGRESS_ACL_ID	0
NF_F_USERNAME	User A

例 2：PAT インターフェイスを持つ、出力時に拒否されたフロー

次の例では、PAT インターフェイスを使用し、出力 ACL によって拒否されたフローを示します。出力インターフェイスの IP アドレスは、209.165.200.225 です。ユーザは、User A として認証されます。入力 ACL（foo）はフローを許可しますが、出力 ACL（bar）がフローを拒否します。次の例に示すように、入力 ACL（foo）は、オブジェクト グループを使用して指定されています。

```
hostname# object-group network host_grp_1
 network-object host 209.165.200.254
 network-object host 209.165.201.1
hostname (config)# access-list foo extended permit tcp object-group host_grp_1 any eq www
hostname (config)# access-list bar extended deny tcp any any
hostname (config)# access-group foo in interface inside
hostname (config)# access-group bar out interface outside
```

図 1 および記載された説明に従い、フロー拒否イベントが発行されます。

作成された NSEL レコードには、次のフィールドと値が含まれます。

フィールド	値
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	37518
NF_F_SRC_INTF_ID	7
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80
NF_F_DST_INTF_ID	8
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	48264
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	3
NF_F_FW_EXT_EVENT	1002（出力 ACL）

フィールド	値
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	37518
NF_F_SRC_INTF_ID	7
NF_F_EVENT_TIME_MSEC	1187374131808
NF_F_INGRESS_ACL_ID	0x102154c1d0e5806e7e5ad93b
NF_F_EGRESS_ACL_ID	0x5da9bb6984434b4b00000000
NF_F_USERNAME	User A

CLI によるデバイス フィールドのデコード

ASA によって入力された一部のフィールド値をデコードするには、デバイスを直接操作する必要があります。これには、*expect* スクリプトなどのダイナミック メカニズムを使用し、イベントを発行したデバイスの CLI から必要な情報を取得することを推奨します。

デバイスは、コンソール、Telnet、および SSH セキュア シェル アクセスをサポートしますが、パフォーマンスとセキュリティの点から、SSH を推奨します。次の項では、ASA とのやり取りに基いて、デコードを必要とするフィールドについて説明します。次の項目について説明します。

- インターフェイス ID フィールド
- ACL ID フィールド
- イベント コード
- 拡張イベント コード

インターフェイス ID フィールド

インターフェイス ID フィールドは、デバイス インターフェイス MIB から SNMP GET 要求を使用してデコードすることもできます。インターフェイス ID フィールドは、MIB をサポートする唯一のフィールドです。

show interface detail コマンドを使用して、デバイス上のすべてのインターフェイスのリストを取得することもできます。この出力には、NetFlow フィールドに送信されたインターフェイス ID の値に対応する、各インターフェイスの下の行が含まれます。次の例で、インターフェイス番号は 8 です。

```
hostname(config)# show interface filter-outside detail
Interface GigabitEthernet4/3 "filter-outside", is up, line protocol is up
Hardware is i82571EB 4CU rev06, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 0015.1715.59c7, MTU 1500
IP address 209.165.200.254, subnet mask 255.255.255.224
532594 packets input, 88376018 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
```

```
675393 packets output, 53208679 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (curr/max packets): hardware (36/511) software (0/0)
output queue (curr/max packets): hardware (59/68) software (0/0)
Traffic Statistics for "filter-outside":
532594 packets input, 78636500 bytes
675393 packets output, 40866215 bytes
10837 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
Control Point Interface States:
Interface number is 8
Interface config status is active
Interface state is active
```

ACL ID フィールド

12 バイトの未加工の ACL ID は、次のように、3 つの構成部分に分割する必要があります。

- 最初の 4 バイトは、ACL 名 ID
- 次の 4 バイトは、ACL エントリ ID（ACE）/ オブジェクト グループ ID
- 最後の 4 バイトは、拡張 ACL エントリ ID

これらの個別の値は、ASA から **show access-list** コマンドを実行した出力によって確認できます。ACL 名 ID は、この出力の ACL の最初の行の末尾にあります。ACE ID は、個別の各 ACL エントリ行の末尾にあります。

（注） アクセス リストでオブジェクト グループを使用している場合、2 番目の 4 バイト ID は実際には ACE ID ではなく、オブジェクトグループ ID です。拡張 ACE ID（最後の 4 バイト部分）は、実際の個別の ACL エントリ ID を表します。次の例では、これらのエントリを示します。

```
hostname(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list foo; 2 elements; name hash: 0x102154c1
access-list foo line 1 extended permit tcp object-group host_grp_1 any eq www 0xd0e5806e
access-list foo line 1 extended permit tcp host 209.165.200.254 any eq www (hitcnt=4)
0x7e5ad93b
access-list foo line 1 extended permit tcp host 209.165.201.1 any eq www (hitcnt=0)
0xe0c1846b
access-list bar; 1 elements; name hash: 0x5da9bb69
access-list bar line 1 extended deny tcp any any (hitcnt=41) 0x84434b4b
```

この例は、例 2：PAT インターフェイスを持つ、出力時に拒否されたフロー の例と似ています。拒否されたフローの例では、ACL ID が、次のように各構成部分に分割されています。

- NF_F_INGRESS_ACL_ID: InAcl: 0x102154c1d0e5806e7e5ad93b

  ここで、0x102154c1 が最初の 4 バイト、0xd0e5806e が 2 番目の 4 バイト、0x7e5ad93b が最後の 4 バイトです。

- NF_F_EGRESS_ACL_ID: 0x5da9bb6984434b4b00000000

  ここで、0x5da9bb69 が最初の 4 バイト、0x84434b4b が 2 番目の 4 バイト、0x00000000 が最後の 4 バイトです。

（注） これらの ID はそれぞれ、**show access-list** コマンドの例の各行に対応しています。

これらの ID から、アクセス リスト *foo* は入力インターフェイスに適用され、アクセス リスト *bar* は出力インターフェイスに適用されたと推定できます。この情報は、**show run access-group** コマンドによっても入手できますが、ACL ID の方が許可または拒否アクションの原因となった個別の ACE を特定できる点で優れています。（拡張イベント コードから判断して）このフローは出力で拒否されているので、入力 ACL ID が特定する ACE 行はフローを許可し、出力 ACL ID が特定する ACE はフローを拒否することがわかります。

イベント コード

ASA は、高レベルのイベント タイプを 4 種類（作成、ティアダウン、拒否、および更新）しか発行しないので、イベント コードをコレクタにハード コードする必要があります。

拡張イベント コード

これら 4 つの高レベルのイベント コードのうち、拡張イベント コードがあるのは、フロー拒否とフロー ティアダウンの 2 つのイベント タイプのみです。フロー拒否イベントでは、表 3 の拡張イベント コードのリストを見れば、そのフローが拒否された理由を十分判断できます。しかし、フロー ティアダウン イベントは、このドキュメントに記載しきれないほど多くのイベント コードがあり、理由が非常に流動的です。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。