NetFlow Collector インプリメンテーション ノート バージョン 9.1

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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 5500 Series Configuration Guide using the CLI*』の「Using NSEL and Syslog Messages」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、発信元（発信側）と送信先（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。

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 5500 Series Configuration Guide using the CLI*』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 5500 Series Configuration Guide using the CLI*』および『*Cisco ASA 5500 Series Command Reference*』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

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
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			
NF_F_XLATE_SRC_ADDR_IPV4	40001	4	マッピングされた発信元 IPv4 アドレス
NF_F_XLATE_DST_ADDR_IPV4	40002	4	マッピングされた送信先 IPv4 アドレス
NF_F_XLATE_SRC_PORT	40003	2	マッピングされた発信元ポート
NF_F_XLATE_DST_PORT	40004	2	マッピングされた送信先ポート
ステータスまたはイベント フィールド			
NF_F_FW_EVENT	40005	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。
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_BYTES	85	4	フローの合計バイト数

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
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。
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	20	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。

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	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。
> 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。

表 3　　拡張イベント ID の値 （続き）

拡張イベント ID	イベント	説明
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	インターフェイス サービスへの ASA 接続の試みが拒否されました。たとえば、このメッセージは、ASA が、権限のない SNMP 管理ステーションからの SNMP 要求を受信したときに、SNMP サービスとともに表示されます。
1004	フロー拒否	TCP の最初のパケットが TCP SYN パケットでなかったために、フローが拒否されました。
> 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

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。
- 現在 IPv46 および IPv64 フロー用のテンプレートが用意されているイベント タイプはありません。
- IPv6 テンプレートには xlate フィールドはありません。

- 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づいて、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。

（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 レコードの解析には、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 IPv4 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_BYTES、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 IPv4 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_BYTES、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の IPv6 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_FW_EVENTp、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FLOW_BYTES、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME
最大ユーザ名サイズの IPv6 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_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FLOW_BYTES、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 IPv4 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_FLOW_BYTES、NF_F_FLOW_CREATE_TIME_MSEC、NF_F_INGRESS_ACL_ID、NF_F_EGRESS_ACL_ID、NF_F_USERNAME

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）

最大ユーザ名サイズ（65 文字）の拡張 IPv4 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_FLOW_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 IPv6 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_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FLOW_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 IPv6 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_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FLOW_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
IPv4 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

表 6　フロー拒否イベント用テンプレート （続き）

説明	フィールド
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
IPv6 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_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
IPv4 フロー終了	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_BYTES
IPv6 フロー終了	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_FW_EVENT、NF_F_FW_EXT_EVENT、NF_F_EVENT_TIME_MSEC、NF_F_FLOW_BYTES

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 5500 Series Configuration Guide using the CLI*』および『*Cisco ASA 5500 Series Command Reference*』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
NF_F_FLOW_BYTES	0

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）
NF_F_EVENT_TIME_MSEC	1187374131808

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_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 とのやり取りに基づいて、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 3 種類（作成、ティアダウン、および拒否）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 3 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*』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/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は 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がデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/