ファイアウォール高速ロギング

ファイアウォール高速ロギング機能は、エクスポート フォーマットとして NetFlow バージョン 9 を使用して、ファイアウォール メッセージの高速ロギング（HSL）をサポートします。

このモジュールでは、ゾーンベース ポリシー ファイアウォールに HSL を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ファイアウォール高速ロギングについて

ファイアウォール高速ロギングの概要

ゾーンベース ファイアウォールは、高速ロギング（HSL）をサポートします。 HSL が設定されている場合、ファイアウォールは、（NetFlow バージョン 9 レコードと同様）ルーティング デバイスを介して外部コレクタに伝送されるパケットのログを提供します。 セッションが作成されたとき、および破棄されたときに、レコードが送信されます。 セッション レコードには、完全な 5 タプル情報（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が含まれます。 タプルは、要素の順序付きリストです。

HSL により、ファイアウォールは、パケット処理への影響を最小限に抑えてレコードをログに記録できます。 ファイアウォールは HSL にバッファ モードを使用します。 バッファ モードでは、ファイアウォールは、高速ロガー バッファに直接記録し、パケットを個別にエクスポートします。

ファイアウォールは、次のタイプのイベントをログに記録します。

- 監査：セッションの作成および削除の通知。
- アラート：ハーフオープンおよび最大オープン TCP セッションの通知。
- ドロップ：パケット ドロップの通知。
- 通過：（設定済みレート制限に基づく）パケット通過の通知。
- サマリー：ポリシー ドロップと通過サマリーの通知。

NetFlow コレクタは、**show platform software interface F0 brief** コマンドを発行して、インターフェイス名に FW_SRC_INTF_ID および FW_DST_INTF_ID インターフェイス ID をマッピングします。

show platform software interface F0 brief コマンドの次の出力例は、[ID] カラムがインターフェイス ID をインターフェイス名（[Name] カラム）にマッピングすることを示しています。

```
Device# show platform software interface F0 brief

Name                          ID      QFP ID
GigabitEthernet0/2/0          16         9
GigabitEthernet0/2/1          17        10
GigabitEthernet0/2/2          18        11
GigabitEthernet0/2/3          19        12
```

NetFlow フィールド ID の説明

次の表に、ファイアウォール Netflow テンプレート内で使用される NetFlow フィールド ID をリストします。

表 *1*：*NetFlow* フィールド *ID*

フィールド ID	タイプ	長さ	説明
NetFlow ID フィールド（レイヤ 3 IPv4）			
FW_SRC_ADDR_IPV4	8	4	発信元 IPv4 アドレス
FW_DST_ADDR_IPV4	12	4	送信先 IPv4 アドレス
FW_SRC_ADDR_IPV6	27	16	発信元 IPv6 アドレス
FW_SRC_ADDR_IPV6	28	16	送信先 IPv6 アドレス
FW_PROTOCOL	4	1	IP プロトコル値
FW_IPV4_IDENT	54	4	IPv4 識別名
FW_IP_PROTOCOL_VERSION	60	1	IP プロトコル バージョン
フロー ID フィールド（レイヤ 4）			
FW_TCP_FLAGS	6	1	TCP フラグ
FW_SRC_PORT	7	2	送信元ポート
FW_DST_PORT	11	2	宛先ポート
FW_ICMP_TYPE	176	1	ICMP [1] タイプ値
FW_ICMP_CODE	177	1	ICMP コード値
FW_ICMP_IPV6_TYPE	178	1	ICMP バージョン 6（ICMPv6）タイプ値
FW_ICMP_IPV6_CODE	179	1	ICMPv6 コード値
FW_TCP_SEQ	184	4	TCP シーケンス番号
FW_TCP_ACK	185	4	TCP 確認応答番号
フロー ID フィールド（レイヤ 7）			
FW_L7_PROTOCOL_ID	95	2	レイヤ 7 プロトコル ID。 ファイアウォールインスペクションで使用されるレイヤ 7 アプリケーション分類を識別します。

フィールド ID	タイプ	長さ	説明
フロー名フィールド（レイヤ 7）			
FLOW_FIELD_L7_PROTOCOL_NAME	96	32	レイヤ 7 プロトコルの名前。 レイヤ 7 プロトコル ID（FW_L7_PROTOCOL_ID）に対応するレイヤ 7 プロトコル名を識別します。
フロー ID フィールド（インターフェイス）			
FW_SRC_INTF_ID	10	2	入力 SNMP [2] ifIndex
FW_DST_INTF_ID	14	2	出力 SNMP ifIndex
FW_SRC_VRF_ID	234	4	入力（発信側）VRF [3] ID
FW_DST_VRF_ID	235	5	出力（応答側）VRF ID
FW_VRF_NAME	236	32	VRF 名
マッピングされたフロー ID フィールド（ネットワーク アドレス変換）			
FW_XLATE_SRC_ADDR_IPV4	225	4	マッピングされた発信元 IPv4 アドレス
FW_XLATE_DST_ADDR_IPV4	226	4	マッピングされた送信先 IPv4 アドレス
FW_XLATE_SRC_PORT	227	2	マッピングされた発信元ポート
FW_XLATE_DST_PORT	228	2	マッピングされた送信先ポート
ステータスおよびイベント フィールド			
FW_EVENT	233	1	高レベルのイベント コード • 0：無視（無効） • 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

フィールド ID	タイプ	長さ	説明
FW_EXT_EVENT	35,001	1	拡張イベント コード
タイムスタンプおよび統計情報フィールド			
FW_EVENT_TIME_MSEC	323	8	イベントが発生した時刻。0000 UTC [4] 1970/01/01 からの経過時間がミリ秒単位で表示され、イベントが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
FW_INITIATOR_OCTETS	231	8	発信側から着信したパケット フロー内のレイヤ 4 ペイロード バイトの総数
FW_RESPONDER_OCTETS	232	8	応答側から着信したパケット フロー内のレイヤ 4 ペイロード バイトの総数
AAA フィールド			
FW_USERNAME	40,000	20	AAA [5] ユーザ名
FW_USERNAME_MAX	40,000	64	最大許可サイズの AAA ユーザ名
アラート フィールド			
FW_HALFOPEN_CNT	35,012	4	ハーフオープン セッション エントリ数
FW_BLACKOUT_SECS	35,004	4	宛先がブラックアウトしていたか、または利用不可であった時間（秒単位）
FW_HALFOPEN_HIGH	35,005	4	1 分間ログに記録される TCP ハーフオープン セッション エントリの設定済み最大レート
FW_HALFOPEN_RATE	35,006	4	1 分間ログに記録される TCP ハーフオープン セッション エントリの現在のレート
FW_MAX_SESSIONS	35,008	4	このゾーン ペアまたはクラス ID に許可されたセッションの最大数

フィールド ID	タイプ	長さ	説明
その他			
FW_ZONEPAIR_ID	35,007	4	ゾーン ペア ID
FW_CLASS_ID	51	4	クラス ID
FW_ZONEPAIR_NAME	35,009	64	ゾーン ペアの名前
FW_CLASS_NAME	100	64	クラス名
FW_EXT_EVENT_DESC	35,010	64	拡張イベントの説明
FW_SUMMARY_PKT_CNT	35,011	4	ドロップ/通過サマリー レコードで表されるパケット数
FW_EVENT_LEVEL	33003	1	記録されたイベントのレベルの定義 • 0x01：ボックス単位 • 0x02：VRF • 0x03：ゾーン • 0x04：クラス マップ • 他の値は未定義
FW_EVENT_LEVEL_ID	33,004	4	FW_EVENT_LEVEL フィールドの識別子の定義 • FW_EVENT_LEVEL が 0x02（VRF）の場合、このフィールドは VRF_ID を表します。 • FW_EVENT_LEVEL が 0x03（ゾーン）の場合、このフィールドは ZONE_ID を表します。 • FW_EVENT_LEVEL が 0x04（クラス マップ）の場合、このフィールドは CLASS_ID を表します。 • その他の場合、フィールド ID は 0（ゼロ）になります。FW_EVENT_LEVEL が存在しない場合、このフィールドの値はゼロである必要があります。

フィールド ID	タイプ	長さ	説明
FW_CONFIGURED_VALUE	33,005	4	設定されたハーフオープン、アグレッシブエージング、およびイベントレートモニタリング制限を表す値です。このフィールド値の解釈は、関連する FW_EXT_EVENT フィールドによって決まります。
FW_ERM_EXT_EVENT	33,006	2	拡張イベント レート モニタリング コード
FW_ERM_EXT_EVENT_DESC	33,007	N（文字列）	拡張イベント レート モニタリング イベントの説明文字列

1 インターネット制御メッセージ プロトコル（ICMP）
2 簡易ネットワーク管理プロトコル
3 仮想ルーティングおよび転送
4 協定世界時
5 認証、許可、アカウンティング

ファイアウォール拡張イベント

ファイアウォール拡張イベントのイベント名は、ファイアウォール拡張イベント値をイベント ID にマッピングします。 イベント名オプション レコードを使用して、イベント値とイベント ID 間のマッピングを取得します。

拡張イベントは、通常のファイアウォール イベント（inspect、pass、または drop）の一部ではありません。

次の表で、Cisco IOS XE Release 3.8S 以前のリリースに適用可能なファイアウォール拡張イベントについて説明します。

表 *2*：*Cisco IOS XE Release 3.9S* よりも前のリリースのファイアウォール拡張イベントおよびイベントの説明

値	イベント ID	説明
0	FW_EXT_LOG_NONE	特定の拡張イベントはありません。
1	FW_EXT_ALERT_UNBLOCK_HOST	指定したホストへの新規 TCP 接続試行がブロックされなくなります。
2	FW_EXT_ALERT_HOST_TCP_ALERT_ON	ハーフオープン TCP 接続の最大不完全ホスト制限を超えました。

値	イベント ID	説明
3	FW_EXT_ALERT_BLOCK_HOST	指定したホストへの以降のすべての新しい TCP 接続試行は拒否されます。これは、ハーフオープン TCP 接続の最大不完全ホストしきい値を超えており、かつ以降の新しい接続をブロックするようにブロッキング オプションが設定されているためです。
4	FW_EXT_SESS_RATE_ALERT_ON	ハーフオープン接続の最大不完全上限しきい値を超えたか、または新しい接続開始レートを超えました。
5	FW_EXT_SESS_RATE_ALERT_OFF	ハーフオープン TCP 接続数が、最大不完全下限しきい値を下回っているか、または新しい接続開始レートが最大不完全下限しきい値を下回りました。
6	FW_EXT_RESET	接続をリセットします。
7	FW_EXT_DROP	接続をドロップします。
10	FW_EXT_L4_NO_NEW_SESSION	新しいセッションは許可されません。
12	FW_EXT_L4_INVALID_SEG	無効な TCP セグメント。
13	FW_EXT_L4_INVALID_SEQ	無効な TCP シーケンス番号。
14	FW_EXT_L4_INVALID_ACK	無効な TCP 確認応答（ACK）。
15	FW_EXT_L4_INVALID_FLAGS	無効な TCP フラグ。
16	FW_EXT_L4_INVALID_CHKSM	無効な TCP チェックサム。
18	FW_EXT_L4_INVALID_WINDOW_SCALE	無効な TCP ウィンドウ スケール。
19	FW_EXT_L4_INVALID_TCP_OPTIONS	無効な TCP オプション。
20	FW_EXT_L4_INVALID_HDR	無効なレイヤ 4 ヘッダー。
21	FW_EXT_L4_OOO_INVALID_SEG	OoO [6] 無効セグメント。
24	FW_EXT_L4_SYNFLOOD_DROP	同期（SYN）フラッドパケットはドロップされます。

値	イベント ID	説明
25	FW_EXT_L4_SCB_CLOSED	セッションは、パケットを受信する一方で、閉じます。
26	FW_EXT_L4_INTERNAL_ERR	ファイアウォールの内部エラーです。
27	FW_EXT_L4_OOO_SEG	OoO セグメント。
28	FW_EXT_L4_RETRANS_INVALID_FLAGS	無効な再送信されたパケット。
29	FW_EXT_L4_SYN_IN_WIN	無効な SYN フラグ。
30	FW_EXT_L4_RST_IN_WIN	無効なリセット（RST）フラグ。
31	FW_EXT_L4_STRAY_SEG	遊離 TCP セグメント。
32	FW_EXT_L4_RST_TO_RESP	応答側へのリセットメッセージの送信。
33	FW_EXT_L4_CLOSE_SCB	セッションの終了。
34	FW_EXT_L4_ICMP_INVAL_RET	無効な ICMP [7] パケット。
37	FW_EXT_L4_MAX_HALFSESSION	最大ハーフオープン セッション制限を超えました。
38	FW_EXT_NO_RESOURCE	リソース（メモリ）は使用できません。
40	FW_EXT_INVALID_ZONE	無効なゾーン。
41	FW_EXT_NO_ZONE_PAIR	ゾーン ペアは使用できません。
42	FW_EXT_NO_TRAFFIC_ALLOWED	トラフィックは許可されません。
43	FW_EXT_FRAGMENT	パケット フラグメントはドロップされます。
44	FW_EXT_PAM_DROP	PAM[8] アクションはドロップされます。

値	イベント ID	説明
45	FW_EXT_NOT_INITIATOR	セッション開始パケットではありません。 次のいずれかの理由により発生します。 • プロトコルが TCP の場合、最初のパケットが SYN パケットではない。 • プロトコルが ICMP の場合、最初のパケットがエコーまたはタイムスタンプ パケットではない。
48	FW_EXT_ICMP_ERROR_PKTS_BURST	ICMP エラー パケットがバースト モードになりました。バーストモードでは、パケットは、応答側インターフェイスからの応答を待機しないで繰り返し送信されます。
49	FW_EXT_ICMP_ERROR_MULTIPLE_UNREACH	「宛先到達不能」タイプの複数の ICMP エラーを受信しました。
50	FW_EXT_ICMP_ERROR_L4_INVALID_SEQ	ICMP エラー メッセージに埋め込まれたパケットに無効なシーケンス番号があります。
51	FW_EXT_ICMP_ERROR_L4_INVALID_ACK	ICMP エラー メッセージに埋め込まれたパケットに無効な確認応答（ACK）番号があります。
52	FW_EXT_MAX	未使用。

[6] 順序外
[7] インターネット制御メッセージ プロトコル（ICMP）
[8] ポートツーアプリケーション マッピング

ファイアウォール高速ロギングの設定方法

グローバル パラメータ マップの高速ロギングのイネーブル化

デフォルトでは、高速ロギング（HSL）はイネーブルではなく、ファイアウォールのログはルート プロセッサ（RP）またはコンソールのロガー バッファに送信されます。 HSL をイネーブルに

すると、ログは装置外の高速ログ収集装置に送信されます。パラメータマップは、ファイアウォールに到達するトラフィックに対するアクションを実行する手段を提供し、グローバル パラメータマップは、ファイアウォール セッション テーブル全体に適用されます。 グローバル パラメータマップの高速ロギングをイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **log dropped-packets**
5. **log flow-export v9 udp destination** *ip-address port-number*
6. **log flow-export template timeout-rate** *seconds*
7. **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 モードをイネーブルにします。 • 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	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査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	**log dropped-packets** 例： `Device(config-profile)# log dropped-packets`	ドロップされたパケットのロギングをイネーブルにします。
ステップ 5	**log flow-export v9 udp destination** *ip-address port-number* 例： `Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000`	NetFlow イベント ロギングをイネーブルにし、ログ コレクタの IP アドレスとポート番号を提供します。

	コマンドまたはアクション	目的
ステップ 6	**log flow-export template timeout-rate** *seconds* 例： `Device(config-profile) log flow-export template timeout-rate 5000`	テンプレートのタイムアウト値を指定します。
ステップ 7	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査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。

ファイアウォール アクションの高速ロギングのイネーブル化

検査タイプパラメータマップを設定している場合は、この作業を実行して高速ロギングをイネーブルにします。パラメータマップはファイアウォールの検査動作を指定し、ファイアウォールの検査パラメータ マップは検査タイプとして設定されています。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **audit-trail on**
5. **alert on**
6. **one-minute** {**low** *number-of-connections* | **high** *number-of-connections*}
7. **tcp max-incomplete host** *threshold*
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect** *parameter-map-name*
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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect parameter-map-hsl`	接続しきい値、タイムアウト、および **inspect** キーワードに関連するその他のパラメータの検査パラメータ マップを設定し、パラメータ マップ タイプ検査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	**audit-trail on** 例： `Device(config-profile)# audit-trail on`	監査証跡メッセージをイネーブルにします。 • パラメータ マップに対する監査証跡をイネーブルにして、接続またはセッションの開始、停止、期間や、送信元と宛先の IP アドレスを記録することができます。
ステップ 5	**alert on** 例： `Device(config-profile)# alert on`	コンソールに表示されるステートフル パケット インスペクション アラート メッセージをイネーブルにします。
ステップ 6	**one-minute** {**low** *number-of-connections* | **high** *number-of-connections*} 例： `Device(config-profile)# one-minute high 10000`	システムによるハーフオープン セッションの削除の開始と停止を起動する新規の未確立セッションの数を定義します。
ステップ 7	**tcp max-incomplete host** *threshold* 例： `Device(config-profile)# tcp max-incomplete host 100`	TCP ホスト固有のサービス拒否（DoS）の検出および回避のために、しきい値とブロックする時間値を指定します。
ステップ 8	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect policy-map-hsl`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect class-map-tcp`	アクションを実行する対象のトラフィック クラスを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect parameter-map-hsl`	（任意）ステートフルパケットインスペクションをイネーブルにします。
ステップ 12	**end** 例： `Device(config-pmap-c)# end`	ポリシー マップ クラス 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。

ファイアウォール高速ロギングの設定例

例：グローバル パラメータ マップの高速ロギングのイネーブル化

次に、ドロップされたパケットのロギングをイネーブルにし、エラー メッセージを NetFlow バージョン 9 フォーマットで外部 IP アドレスに記録する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# log dropped-packets
Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000
Device(config-profile)# log flow-export template timeout-rate 5000
Device(config-profile)# end
```

例：ファイアウォール アクションの高速ロギングのイネーブル化

次に、検査タイプ パラメータ マップ parameter-map-hsl に高速ロギング（HSL）を設定する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type inspect parameter-map-hsl
Device(config-profile)# audit trail on
Device(config-profile)# alert on
Device(config-profile)# one-minute high 10000
Device(config-profile)# tcp max-incomplete host 100
Device(config-profile)# exit
Device(config)# poliy-map type inspect policy-map-hsl
Device(config-pmap)# class type inspect class-map-tcp
Device(config-pmap-c)# inspect parameter-map-hsl
Device(config-pmap-c)# end
```

ファイアウォール高速ロギングの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール高速ロギングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *3*：ファイアウォール高速ロギングの機能情報

機能名	リリース	機能情報
ファイアウォール高速ロギング	Cisco IOS XE Release 2.1	ファイアウォール高速ロギング サポート機能は、エクスポート フォーマットとして NetFlow バージョン 9 を使用するファイアウォール HSL に対するサポートを導入します。 次のコマンドが導入または変更されました。**log dropped-packet**、**log flow-export v9 udp destination**、**log flow-export template timeout-rate**、**parameter-map type inspect global**。