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 ファイアウォールで HSL を設定する方法について説明します。

ファイアウォール高速ロギングに関する機能情報

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 *1:* ファイアウォール高速ロギングに関する機能情報

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 リリース 2.1	ファイアウォール高速ロギング サポート機能は、NetFlow バージョン 9 をエクスポート形式として使用したファイアウォール HSL の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**。

機能名	リリース	機能情報
高速ロギングを使用したゾーンベースファイアウォールの設定	Cisco IOS XE Gibraltar 16.11.1	このリリースでは、送信元インターフェイスのサポートが追加されました。 次のコマンドが導入または変更されました。**log flow-export v9 udp destination source interface** *interface-name*

ファイアウォール高速ロギングに関する情報

ファイアウォール高速ロギングの概要

ゾーンベース ファイアウォールでは、高速ロギング（HSL）がサポートされています。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 レコードと同様に）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。レコードは、セッションの作成時と破棄時に送信されます。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、要素の番号付きリストです。

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レコードを直接記録し、パケットを個別にエクスポートします。

（注） 高速ロギング（HSL）は、VASI インターフェイスを介してルーティングできません。

（注） ゾーンベース ファイアウォールでは、最大 4 つの HSL 宛先を設定できます。

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。

次に示す **show platform software interface F0 brief** コマンドの出力例は、[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、ファイアウォールの NetFlow テンプレート内で使用される NetFlow フィールド ID を記載します。

表 *2 : 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_DST_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 ID
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

フィールド ID	タイプ	長さ	説明
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。通常のレコードでは 2 バイトを使用しますが、オプション レコードでは 4 バイトを使用します。
フロー名フィールド（レイヤ 7）			
FLOW_FIELD_L7_PROTOCOL_NAME	96	32	レイヤ 7 プロトコル名。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（イニシエータ）VRF（[3]）ID
FW_DST_VRF_ID	235	4	出力（レスポンダ）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

フィールド ID	タイプ	長さ	説明
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
FW_EXT_EVENT	35,001	2	拡張イベント コード通常のレコードでの長さは2バイト、オプションレコードでの長さは4バイトです。
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間（ミリ秒単位）（1970 年 1 月 1 日 00:00（UTC[4]）からの経過時間。イベントがマイクロイベントの場合は 324、ナノイベントの場合は 325 を使用）
FW_INITIATOR_OCTETS	231	4	イニシエータから到着したパケットフローに含まれるレイヤ4ペイロードの合計バイト数
FW_RESPONDER_OCTETS	232	4	レスポンダから到着したパケットフローに含まれるレイヤ4ペイロードの合計バイト数
AAA フィールド			
FW_USERNAME	40,000	テンプレートに応じて20または64	AAA（[5]）ユーザ名
FW_USERNAME_MAX	40,000	64	最大許容サイズの AAA ユーザ名
アラート フィールド			

フィールド ID	タイプ	長さ	説明
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	宛先がブロックされたか、使用できなかった時間（秒単位）
FW_HALFOPEN_HIGH	35,005	4	1 分間でログに記録される TCP ハーフオープン セッション エントリ数に対して設定された最大レート
FW_HALFOPEN_RATE	35,006	4	1 分間でログに記録される TCP ハーフオープン セッション エントリ数の現在のレート
FW_MAX_SESSIONS	35,008	4	このゾーン ペアまたはクラス ID に許可される最大セッション数
その他（Miscellaneous）			
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 ペア名
FW_CLASS_NAME	100	64	クラス名
FW_EXT_EVENT_DESC	35,010	32	拡張イベントの説明
FLOW_FIELD_CTS_SRC_GROUP_TAG	34000	2	Cisco TrustSec ソース タグ
FW_SUMMARY_PKT_CNT	35,011	4	ドロップ/パス サマリ レコードに示されたパケット数
FW_EVENT_LEVEL	33003	4	ログに記録されたイベントのレベルを定義します。 • 0x01：ボックスごと • 0x02：VRF • 0x03：ゾーン • 0x04：クラス マップ • その他の値は未定義

フィールド ID	タイプ	長さ	説明
FW_EVENT_LEVEL_ID	33,004	4	FW_EVENT_LEVEL フィールドの ID を定義します。 • 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。 • その他すべてのクラスでは、このフィールド 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になります。
FW_CONFIGURED_VALUE	33,005	4	設定済みのハーフオープン、アグレッシブ エージング、およびイベント レート モニタリングの制限を表す値。このフィールドの値の意味は、関連付けられた FW_EXT_EVENT フィールドによって異なります。
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 イベントを説明する文字列

[1] Internet Control Message Protocol
[2] Simple Network Management Protocol
[3] Virtual Routing and Forwarding
[4] 協定世界時
[5] 認証、認可、アカウンティング

HSL メッセージ

以下に、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータからの Syslog メッセージの例を記載します。

表 *3: Syslog* メッセージおよびそのテンプレート

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-DROP_PKT タイプ：情報	Dropping %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u %s %s 説明：ファイアウォールインスペクションによりパケットがドロップされました。 %s：tcp/udp/icmp/不明なプロトコル/L7 プロトコル %s：インターフェイス %CA:%u：IP/IP6 アドレス:ポート %s:%s：ゾーンペアの名前/クラス名 %s：「原因（due to）」 %s：fw_ext_event 名 %u：IP 識別子 %s：TCP の場合、TCP SEQ/ACK 番号および TCP フラグ %s：ユーザ名	FW_TEMPLATE_DROP_V4 または FW_TEMPLATE_DROP_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-SESS_AUDIT_TRAIL_START タイプ：情報	(target:class)-(%s:%s):Start %s session: initiator (%CA:%u) -- responder (%CA:%u) from %s %s %s 説明：インスペクションセッションが開始されました。このメッセージは、各インスペクションセッションの開始時に発行され、送信元/宛先アドレスおよびポートを記録します。 %s:%s：ゾーンペアの名前/クラス名 %s：L4/L7 プロトコル名 %CA:%u：IP/IP6 アドレス:ポート %s：インターフェイス %s：ユーザ名 %s：TODO 実際のログ： *Jan 21 20:13:01.078: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:125 TS:00000010570290947309 %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session: initiator (10.1.1.1:43365) -- responder (10.3.21.1:23) from FastEthernet0/1/0	FW_TEMPLATE_START_AUDIT_V4 または FW_TEMPLATE_START_AUDIT_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-SESS_AUDIT_TRAIL タイプ：情報	(target:class)-(%s:%s):Stop %s session: initiator (%CA:%u) sent %u bytes -- responder (%CA:%u) sent %u bytes , from %s %s 説明：ネットワーク アクティビティのセッションごとのトランザクション ログ。このメッセージは、各インスペクションセッションの終了時に発行され、送信元/宛先アドレスおよびポート、クライアントとサーバから送信されたバイト数を記録します。 %s:%s：ゾーンペアの名前/クラス名 %s：L4/L7 プロトコル名 %CA:%u：IP/IP6 アドレス:ポート %u：バイト カウンタ %s：インターフェイス %s：TODO 実際のログ： *Jan 21 20:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-6-SESS_AUDIT_TRAIL: Stop tcp session: initiator (10.1.1.1:43365) sent 35 bytes -- responder (11.1.1.1:23) sent 95 bytes, from FastEthernet0/1/0	FW_TEMPLATE_STOP_AUDIT_V4 または FW_TEMPLATE_STOP_AUDIT_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-4-UNBLOCK_HOST タイプ：警告	(target:class)-(%s:%s):New TCP connections to host %CA no longer blocked 説明：指定のホストへの新しい TCP 接続試行がブロックされなくなりました。このメッセージは、指定のホストへの新しい TCP 接続試行のブロッキングが解除されたことを意味します。 %s:%s：ゾーンペアの名前/クラス名 %CA：IP/IP6 アドレス	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 または FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6、fw_ext_event ID：FW_EXT_ALERT_UNBLOCK_HOST
FW4HOST_TCP_ALERT_ON タイプ：警告	"(target:class)-(%s:%s):Max tcp half-open connections (%u) exceeded for host %CA. 説明：ハーフオープン TCP 接続の max-incomplete host 制限を超えました。このメッセージは、保護対象のサーバに対するハーフオープン接続数が多く、SYN フラッド攻撃が進行中であることを示す可能性があることを意味します。 %s:%s：ゾーンペアの名前/クラス名 %u：ハーフオープン接続数 %CA：IP/IP6 アドレス	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 または FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6、fw_ext_event ID：FW_EXT_ALERT_HOST_TCP_ALERT_ON

メッセージ ID	メッセージの説明	HSL テンプレート
FW-2-BLOCK_HOST タイプ：クリティカル	(target:class)-(%s:%s):Blocking new TCP connections to host %CA for %u minute%s (half-open count %u exceeded). 説明：ハーフオープン TCP 接続の max-incomplete host しきい値を超えました。指定のホストに対する以降の新しい TCP 接続試行は拒否され、ブロッキング オプションが以降の新しい接続すべてをブロックするように設定されます。設定されたブロック時間が満了すると、ブロッキングが解除されます。 %s:%s：ゾーン ペアの名前/クラス名 %CA：IP/IP6 アドレス %u：ブロック時間（分） %s：ブロック時間が 1 分を超える場合「s」 %u：ハーフオープン カウンタ	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 または FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6、fw_ext_event ID：FW_EXT_ALERT_BLOCK_HOST

メッセージ ID	メッセージの説明	HSL テンプレート
FW-4-ALERT_ON タイプ：警告	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u 説明：ハーフオープン接続の max-incomplete high しきい値または新しい接続開始レートのいずれかを超えました。このエラーメッセージは、ファイアウォールからの新しい着信接続レートが異常に高く、DOS攻撃が進行中であることを示す可能性があることを意味します。このメッセージが発行されるのは、max-incomplete high しきい値を上回った場合のみです。 %s:%s：ゾーンペアの名前/クラス名 %s：「アグレッシブな状態（getting aggressive）」 %u/%u：ハーフオープン接続数/高 %u：現在のレート	FW_TEMPLATE_ALERT_HALFOPEN_V4 または FW_TEMPLATE_ALERT_HALFOPEN_V6、fw_ext_event ID：FW_EXT_SESS_RATE_ALERT_ON
FW-4-ALERT_OFF タイプ：警告	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u 説明：ハーフオープン接続数または新しい接続開始レートのいずれかが、max-incomplete low しきい値を下回りました。このメッセージは、新しい着信接続のレートが低下したことを意味します。新しい接続は、max-incomplete low しきい値を下回った場合にのみ実行されます。 %s:%s：ゾーンペアの名前/クラス名 %s：「沈静化中（calming down）」 %u/%u：ハーフオープン接続数/高 %u：現在のレート	FW_TEMPLATE_ALERT_HALFOPEN_V4 または FW_TEMPLATE_ALERT_HALFOPEN_V6、fw_ext_event ID：FW_EXT_SESS_RATE_ALERT_OFF

メッセージ ID	メッセージの説明	HSL テンプレート
FW-4-SESSIONS_MAXIMUM タイプ：警告	Number of sessions for the firewall policy on "(target:class)-(%s:%s) exceeds the configured sessions maximum value %u 説明：確立済みの セッション数が、設定されているセッション最大数の制限を超えました。 %s:%s：ゾーンペアの名前/クラス名 %u：最大セッション数	FW_TEMPLATE_ALERT_MAX_SESSION
FW-6-PASS_PKT タイプ：情報	Passing %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u 説明：ファイアウォールインスペクションによりパケットが渡されました。 %s：tcp/udp/icmp/不明なプロトコル %s：インターフェイス %CA:%u：送信元 IP/IP6 アドレス:ポート %CA:%u：宛先 IP/IP6 アドレス:ポート %s:%s：ゾーンペアの名前/クラス名 %s %s：「原因（due to）」、「ポリシーマップで PASS アクションを検出（PASS action found in policy-map）」 %u：IP 識別子	FW_TEMPLATE_PASS_V4 または FW_TEMPLATE_PASS_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-LOG_SUMMARY タイプ：情報	%u packet%s %s from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s 説明：ドロップされたパケット数と渡されたパケット数のログサマリ %u %s：パケット数、「s were」または「was」 %s：「ドロップ（dropped）」/「パス（passed）」 %s：インターフェイス %CA:%u：送信元 IP/IP6 アドレス:ポート %CA:%u：宛先 IP/IP6 アドレス:ポート %s:%s：ゾーンペアの名前/クラス名 %s：ユーザ名	FW_TEMPLATE_SUMMARY_V4 または FW_TEMPLATE_SUMMARY_V6、FW_EVENT として 3 - drop 4 - pass を使用

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により、ファイアウォール拡張イベント値とイベント ID が対応付けられます。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 の対応付けを確認します。

拡張イベントは標準ファイアウォールイベント（inpect、pass、drop）の一部ではありません。

次の表に、Cisco IOS XE リリース 3.9S より前のリリースに適用されるファイアウォール拡張イベントについて説明します。

表 *4 : Cisco IOS XE* リリース *3.9S* 以前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	指定したホストに対する新規の TCP 接続試行はブロックされません。
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	指定されたホストに対する後続の TCP 接続試行はすべて拒否されます。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、かつ後続の新規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、または新規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 接続の数が、最大不完全下限しきい値を下回っているか、または新規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	新規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 パケットがドロップされます。
25	FW_EXT_L4_SCB_CLOSED	セッションがパケット受信中にセッションが終了しました。
26	FW_EXT_L4_INTERNAL_ERR	ファイアウォールの内部エラーです。

値	イベント ID	説明
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ています。
38	FW_EXT_NO_RESOURCE	リソース（メモリ）が使用できません。
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ていません。
43	FW_EXT_FRAGMENT	パケット フラグメントがドロップされます。
44	FW_EXT_PAM_DROP	PAM[8]アクションがドロップされます。
45	FW_EXT_NOT_INITIATOR	セッション開始パケットではありません。 これは、次のいずれかの理由で発生します。 • プロトコルが TCP の場合、1 番目のパケットが SYN パケットではありません。 • プロトコルが ICMP の場合、1 番目のパケットが ECHO パケットまたは TIMESTAMP パケットではありません。

値	イベント ID	説明
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、応答側インターフェイスからの応答を待たずにパケットが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ICMPエラーを複数受信しました。
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] Internet Control Message Protocol
[8] Port-to-Application Mapping

次の表では、Cisco IOS XE リリース 3.9S 以降のリリースに適用されるファイアウォール拡張イベントについて説明します。

表 *5 : Cisco IOS XE* リリース *3.9S* 以降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_FW_DROP_L4_TYPE_INVALID_HDR	レイヤ 4 ICMP、TCP、または UDP ヘッダーを組み込むことができない小さいデータグラム。
2	FW_EXT_FW_DROP_L4_TYPE_INVALID_ACK_FLAG	ACK フラグが含まれていないか、または TCP スリーウェイ ハンドシェイクにおいてSYN/ACKパケットにRSTフラグが設定されており、パケットに無効なシーケンス番号がありました。

値	イベント ID	説明
3	FW_EXT_FW_DROP_L4_TYPE_INVALID_ACK_NUM	これは、次のいずれかの理由で発生します。 • パケットの ACK 値が、接続の最も古い応答未確認シーケンス番号よりも小さい場合。 • パケットの ACK 値が、接続の次のシーケンス番号よりも大きい場合。 • スリーウェイ ハンドシェイク中に受信した SYN/ACK または ACK パケットで、シーケンス番号が初期シーケンス番号に 1 を加算した値と等しくない場合。
4	FW_EXT_FW_DROP_L4_TYPE_INVALID_TCP_INITIATOR	フローの 1 番目のパケットが SYN パケットではありませんでした。
5	FW_EXT_FW_DROP_L4_TYPE_SYN_WITH_DATA	SYN パケットにペイロードが含まれています。このような SYN パケットはサポートされていません。
6	FW_EXT_FW_DROP_L4_TYPE_INVALID_TCP_WIN_SCALE_OPTION	TCP ウィンドウ スケール オプションの長さが無効です。
7	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_SYNSENT_STATE	SYNSENT 状態の無効な TCP セグメントを受信しました。 これは、次のいずれかの理由で発生します。 • SYN/ACK にペイロードが含まれています。 • SYN/ACK にその他のフラグ（push（PSH）、urgent（URG）、finish（FIN））が設定されています。 • ペイロードまたは無効な TCP フラグ（ACK、PSH、URG、FIN、RST）が設定されている再送信 SYN メッセージを受信しました。 • イニシエータから SYN 以外のパケットを受信しました。

値	イベント ID	説明
8	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_SYNRCVD_STATE	再送信された SYN パケットにペイロードが含まれているか、または応答側からパケットを受信しました。
9	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_PKT_TOO_OLD	パケットが、受信側の現在の TCP ウィンドウよりも古い（小さい）パケットです。
10	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_PKT_WIN_OVERFLOW	パケットのシーケンス番号は、受信側の TCP ウィンドウの範囲外（大きい）です。
11	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_PYLD_AFTER_FIN_SEND	FIN メッセージの受信後に、ペイロードを含むパケットを送信元から受信しました。
12	FW_EXT_FW_DROP_L4_TYPE_INVALID_FLAGS	パケットに関連付けられた TCP フラグが無効です。この問題は、次の理由で発生する場合があります。 • 初期パケットで、SYN フラグとともにその他のフラグが設定されていた。初期パケットでは SYN フラグだけが許可されています。 • 予期される SYN/ACK に SYN フラグが含まれていなかったか、SYN/ACK にスリーウェイ ハンドシェイクの 2 番目のパケットの余分なフラグが含まれていました。

値	イベント ID	説明
13	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEQ	無効なシーケンス番号。 これは、次のいずれかの理由で発生します。 • シーケンス番号が ISN [9] よりも小さい。 • シーケンス番号が ISN と等しく、SYN パケットと等しくない。 • 受信ウィンドウ サイズがゼロでパケットにデータが含まれている場合、またはシーケンス番号が最終 ACK 番号よりも大きい場合。 • シーケンス番号が TCP ウィンドウの範囲外である。
14	FW_EXT_FW_DROP_L4_TYPE_RETRANS _INVALID_FLAGS	再送信されたパケットは、受信側によりすでに確認応答済みです。
15	FW_EXT_FW_DROP_L4_TYPE_L7_OOO _SEG	パケットに、予期されている次のセグメントよりも前に到着した TCP セグメントが含まれています。
16	FW_EXT_FW_DROP_L4_TYPE_SYN _FLOOD_DROP	ポリシーに設定されている最大最大不完全セッション数を越え、ホストがブロック期間に入りました。
17	FW_EXT_FW_DROP_L4_TYPE_MAX _HALFSESSION	許可されているハーフオープン セッションの数を超えました。
18	FW_EXT_FW_DROP_L4_TYPE_ TOO_MANY_PKTS	フローあたりの同時インスペクション可能なパケットの最大数を超えました。現在、最大 25 個の同時パケットのインスペクションが許可されています。同時インスペクションにより、1 つのフローがプロセッサ リソースを占有することが防止されます。
19	FW_EXT_FW_DROP_L4_TYPE_TOO _MANY_ICMP_ERR_PKTS	フローあたりの ICMP エラー パケット最大数を超えました。このログは、ファイアウォール ベース インスペクションによってトリガーされます。

値	イベント ID	説明
20	FW_EXT_FW_DROP_L4_TYPE_UNEXPECT _TCP_PYLD	レスポンダから再送信された SYN/ACK にペイロードが含まれています。TCP スリーウェイ ハンドシェイク ネゴシエーションの実行中はペイロードは許可されません。
21	FW_EXT_FW_DROP_L4_TYPE_INTERNAL _ERR_UNDEFINED_DIR	パケットの方向が未定義です。
22	FW_EXT_FW_DROP_L4_TYPE_SYN _IN_WIN	確立されたセッションの TCP パケットが、SYN フラグが設定された状態で到着しました。スリーウェイ ハンドシェイクの最初の 2 つのパケットの後は、SYN フラグは許可されていません。
23	FW_EXT_FW_DROP_L4_TYPE_RST _IN_WIN	RST フラグが設定された TCP パケットを受信しましたが、そのシーケンス番号が最後に受信した確認応答の外部でした。このパケットは誤った順序で送信された可能性があります。
24	FW_EXT_FW_DROP_L4_TYPE_ STRAY_SEG	フローの切断後に予期しないパケットを受信したか、またはイニシエータが有効な SYN フラグを送信する前に応答側からパケットを受信しました。
25	FW_EXT_FW_DROP_L4_TYPE_RST_TO_RESP	応答側からの SYN/ACK フラグが予期されていました。しかし、無効なシーケンス番号のパケットを受信しました。ゾーンベース ファイアウォールから RST フラグが応答側に送信されました。
26	FW_EXT_FW_DROP_L4_TYPE _I NTERNAL_ERR_ICMP_NO_NAT	ICMP パケットは NAT [10]変換されていますが、内部 NAT 情報がありません。内部エラーです。
27	FW_EXT_FW_DROP_L4_TYPE _ INTERNAL_ERR_ICMP_ALLOC_FAIL	ICMP インスペクション中に ICMP エラー パケットを割り当てることができませんでした。
28	FW_EXT_FW_DROP_L4_TYPE _INTERNAL_ERR_ICMP_GET_STAT_BLK_FAIL	分類結果に、必要な統計情報メモリがありませんでした。ポリシー情報がデータ プレーンに正しくダウンロードされていません。

値	イベント ID	説明
29	FW_EXT_FW_DROP_L4_TYPE _INTERNAL_ERR_ICMP_DIR_NOT_IDENTIFIED	パケットの方向が未定義です。
30	FW_EXT_FW_DROP_L4_TYPE_ ICMP_SCB_CLOSE	セッションの切断中にICMPパケットを受信しました。
31	FW_EXT_FW_DROP_L4_TYPE_ ICMP_PKT_NO_IP_HDR	ICMPエラーパケットのペイロードにIP ヘッダーがありません。
32	FW_EXT_FW_DROP_L4_TYPE_ ICMP_ERROR_NO _IP_NO_ICMP	ICMP エラー パケットに IP または ICMPがありません。これは、不正なパケットが原因で発生している可能性があります。
33	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _PKTS_BURST	ICMPエラーパケットがバースト制限10 を超えています。
34	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _MULTIPLE_UNREACH	ICMPエラーパケットが「到達不能」制限を超えています。1番目の到達不能パケットだけが通過できます。
35	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _L4_INVALID_SEQ	埋め込みパケットのシーケンス番号が、ICMPエラーパケットをトリガーした TCP パケットのシーケンス番号と一致しません。
36	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _L4_INVALID_ACK	ICMP エラー パケット ペイロードに含まれている TCP パケットに、これまでに確認されていない ACK フラグが含まれています。
37	FW_EXT_FW_DROP_L4_TYPE_ ICMP_PKT_TOO _SHORT	ICMP エラー パケットの長さが、IP ヘッダー長とICMPヘッダー長の合計よりも短くなっています。
38	FW_EXT_FW_DROP_L4_TYPE_ SESSION_LIMIT	不明確なチャネルの入力を求めている間に、リソースがセッション制限を超えました。
39	FW_EXT_FW_DROP_L4_TYPE_ SCB_CLOSE	終了したセッションで TCP パケットが受信されました。
40	FW_EXT_FW_DROP_INSP_TYPE_ POLICY_NOT_PRESENT	ゾーン ペア内にポリシーがありません。

値	イベント ID	説明
41	FW_EXT_FW_DROP_INSP_TYPE_ SESS_MISS_POLICY _NOT_PRESENT	ゾーン ペアは同一ゾーンで設定されていますが、このゾーンにポリシーが含まれていません。
44	FW_EXT_FW_DROP_INSP_TYPE_ CLASS_ACTION_DROP	分類アクションは、ICMP、TCP、および UDP 以外のパケットのドロップです。
45	FW_EXT_FW_DROP_INSP_TYPE_ PAM_LOOKUP_FAIL	分類アクションは、PAM エントリのドロップです。
48	FW_EXT_FW_DROP_INSP_TYPE_ INTERNAL_ERR_ GET_STAT_BLK_FAIL	分類結果バイトから統計ブロックを取得できませんでした。
49	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_SYNCOOKIE _MAX_DST	SYN フラッド パケットの最大エントリ制限に達しました。
50	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_INTERNAL _ERR_ALLOC_FAIL	宛先テーブル エントリにメモリを割り当てることができません。
51	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_SYN_COOKIE _TRIGGER	SYN Cookie ロジックがトリガーされました。SYN Cookie を含む SYN/ACK が送信され、元の SYN パケットがドロップされたことを示します。
52	FW_EXT_FW_DROP_POLICY_ TYPE_FRAG_DROP	VFR[11]パケットの 1 番目のフラグメントがドロップされ、関連付けられているその他のフラグメントがすべてドロップされます。
53	FW_EXT_FW_DROP_POLICY_ TYPE_ACTION_DROP	分類アクションは、パケットのドロップです。
54	FW_EXT_FW_DROP_POLICY_ TYPE_ICMP_ACTION_DROP	ICMP 埋め込みパケットのポリシー アクションは DROP です。
55	FW_EXT_FW_DROP_L7_TYPE_ NO_SEG	レイヤ 7 ALG[12]は、検査セグメント化パケットを検査しません。
56	FW_EXT_FW_DROP_L7_TYPE_ NO_FRAG	レイヤ 7 ALG は、フラグメント化パケットを検査しません。
57	FW_EXT_FW_DROP_L7_TYPE_ UNKNOWN_PROTO	不明なアプリケーション プロトコル タイプ。
58	FW_EXT_FW_DROP_L7_TYPE_ ALG_RET_DROP	レイヤ 7 ALG インスペクションの結果、パケットがドロップされました。

値	イベント ID	説明
59	FW_EXT_FW_DROP_NONSESSION _TYPE	セッションの作成に失敗しました。
60	FW_EXT_FW_DROP_NO_NEW _SESSION_TYPE	初期 HA [13]状態では新規セッションは許可されていません。
61	FW_EXT_FW_DROP_NOT_ INITIATOR_TYPE	セッション イニシエータ パケットではありません。
62	FW_EXT_FW_DROP_INVALID _ZONE_TYPE	デフォルトのゾーンが無効な場合、セキュリティ ゾーンに関連付けられているインターフェイス間でのみトラフィックが許可されます。
64	FW_EXT_FW_DROP_NO_FORWARDING_TYPE	ファイアウォールが設定されていません。
65	FW_EXT_FW_DROP_ BACKPRESSURE_TYPE	ファイアウォール バックプレッシャを有効にできるのは、HSL [14]が有効であり、かつ HSL ロガーがログ メッセージを送信できない場合です。バックプレッシャは、HSL がログを送信できるようになるまで有効なままになります。
66	FW_EXT_FW_DROP_L4_TYPE_INTERNAL _ERR _SYNFLOOD_ALLOC_HOSTDB_FAIL	SYN 処理中にホスト レート制限が追跡されます。ホスト エントリを割り当てることができませんでした。
67	FW_EXT_FW_DROP_L4_TYPE_ SYNFLOOD_BLACKOUT_DROP	ブラックアウト時間が設定されている場合に、設定されているハーフオープン接続の制限を超えると、指定されている IP アドレスへの新規接続はすべてドロップされます。
68	FW_EXT_FW_DROP_L7_TYPE_ PROMOTE_FAIL_NO_ZONE_PAIR	失敗したポリシー。ゾーン ペアが設定されていないために AGL がセッションのレベルを上げようとすると、ポリシーが失敗します。
69	FW_EXT_FW_DROP_L7_TYPE_ PROMOTE_FAIL_NO_POLICY	失敗したポリシー。ポリシーがないために ALG がセッションのレベルを上げようとすると、ポリシーが失敗します。

値	イベント ID	説明
	FW_EXT_FW_DROP_L4_TYPE_ONEFW_SCB_CLOSE	コンテキスト認識型ファイウォール（CXSC）がティアダウンを要求した後でパケットを受信しました。
	FW_EXT_FW_DROP_L4_TYPE_ONEFW_FAIL_CLOSE	CXSC が動作していません。

[9] 初期シーケンス番号
[10] ネットワーク アドレス変換
[11] フラグメンテーション再構成
[12] アプリケーション レイヤ ゲートウェイ
[13] ハイ アベイラビリティ
[14] 高速ロギング

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有効化

デフォルトでは、高速ロギング（HSL）は有効ではなく、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、ログはボックス外の高速ログ コレクタに送信されます。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対して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有効にするには、次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 モードを有効にします。 • 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 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。
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 モードを終了して、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有効化

検査タイプ パラメータ マップを設定している場合、高速ロギングを有効にするには、次の作業を実行します。パラメータマップはファイアウォールのインスペクション動作を指定し、ファイアウォールのインスペクション パラメータマップは検査タイプとして設定されます。

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** しきい値
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 モードを有効にします。 • 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** *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、その他の **inspect** キーワードに関連するパラメータに対する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有効にして、接続またはセッションの開始、停止、および継続時間、および送信元と宛先の IP アドレスを記録できます。
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** しきい値 例： `Device(config-profile)# tcp max-incomplete host 100`	TCP ホスト固有のサービス妨害（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 モードを終了して、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
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 マップを作成して、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。
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有効化

次に、ドロップされたパケットのロギングを有効にし、NetFlow バージョン 9 形式のエラー メッセージを外部 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有効化

次に、inspect-type parameter-map parameter-map-hsl の高速ロギング（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に関する追加情報

関連資料

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

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。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

翻訳について
このドキュメントは、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。