Firewall High-Speed Logging

The Firewall High-Speed Logging feature supports the high-speed logging (HSL) of firewall messages by using NetFlow Version 9 as the export format.

This module describes how to configure HSL for zone-based policy firewalls.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Firewall High-Speed Logging

Firewall High-Speed Logging Overview

Zone-based firewalls support high-speed logging (HSL). When HSL is configured, a firewall provides a log of packets that flow through routing devices (similar to the NetFlow Version 9 records) to an external collector. Records are sent when sessions are created and destroyed. Session records contain the full 5-tuple information (the source IP address, destination IP address, source port, destination port, and protocol). A tuple is an ordered list of elements.

HSL allows a firewall to log records with minimum impact to packet processing. The firewall uses buffered mode for HSL. In buffered mode, a firewall logs records directly to the high-speed logger buffer, and exports of packets separately.

A firewall logs the following types of events:

- Audit—Session creation and removal notifications.
- Alert—Half-open and maximum-open TCP session notifications.
- Drop—Packet-drop notifications.
- Pass—Packet-pass (based on the configured rate limit) notifications.
- Summary—Policy-drop and pass-summary notifications.

The NetFlow collector issues the **show platform software interface F0 brief** command to map the FW_SRC_INTF_ID and FW_DST_INTF_ID interface IDs to the interface name.

The following sample output from the **show platform software interface F0 brief** command shows that the ID column maps the interface ID to the interface name (Name column):

```
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 Field ID Descriptions

The following table lists NetFlow field IDs used within the firewall NetFlow templates:

Table 1: NetFlow Field IDs

Field ID	Type	Length	Description
NetFlow ID Fields (Layer 3 IPv4)			
FW_SRC_ADDR_IPV4	8	4	Source IPv4 address
FW_DST_ADDR_IPV4	12	4	Destination IPv4 address
FW_SRC_ADDR_IPV6	27	16	Source IPv6 address
FW_DST_ADDR_IPV6	28	16	Destination IPv6 address
FW_PROTOCOL	4	1	IP protocol value
FW_IPV4_IDENT	54	4	IPv4 identification
FW_IP_PROTOCOL_VERSION	60	1	IP protocol version
Flow ID Fields (Layer 4)			
FW_TCP_FLAGS	6	1	TCP flags
FW_SRC_PORT	7	2	Source port
FW_DST_PORT	11	2	Destination port
FW_ICMP_TYPE	176	1	ICMP [1] type value

Field ID	Type	Length	Description
FW_ICMP_CODE	177	1	ICMP code value
FW_ICMP_IPV6_TYPE	178	1	ICMP Version 6 (ICMPv6) type value
FW_ICMP_IPV6_CODE	179	1	ICMPv6 code value
FW_TCP_SEQ	184	4	TCP sequence number
FW_TCP_ACK	185	4	TCP acknowledgment number
Flow ID Fields (Layer 7)			
FW_L7_PROTOCOL_ID	95	2	Layer 7 protocol ID. Identifies the Layer 7 application classification used by firewall inspection. Normal records use 2 bytes, but optional records use 4 bytes.
Flow Name Fields (Layer 7)			
FLOW_FIELD_L7_PROTOCOL_NAME	96	32	Layer 7 protocol name. Identifies the Layer 7 protocol name that corresponds to the Layer 7 protocol ID (FW_L7_PROTOCOL_ID).
Flow ID Fields (Interface)			
FW_SRC_INTF_ID	10	2	Ingress SNMP [2] ifIndex
FW_DST_INTF_ID	14	2	Egress SNMP ifIndex
FW_SRC_VRF_ID	234	4	Ingress (initiator) VRF [3] ID
FW_DST_VRF_ID	235	4	Egress (responder) VRF ID
FW_VRF_NAME	236	32	VRF name
Mapped Flow ID Fields (Network Address Translation)			
FW_XLATE_SRC_ADDR_IPV4	225	4	Mapped source IPv4 address
FW_XLATE_DST_ADDR_IPV4	226	4	Mapped destination IPv4 address
FW_XLATE_SRC_PORT	227	2	Mapped source port
FW_XLATE_DST_PORT	228	2	Mapped destination port
Status and Event Fields			

Field ID	Type	Length	Description
FW_EVENT	233	1	High level event codes • 0—Ignore (invalid) • 1—Flow created • 2—Flow deleted • 3—Flow denied • 4—Flow alert
FW_EXT_EVENT	35,001	2	Extended event code. For normal records the length is 2 byte, and 4 byte for optional records.
Timestamp and Statistics Fields			
FW_EVENT_TIME_MSEC	323	8	Time, in milliseconds, (time since 0000 hours UTC [4] January 1, 1970) when the event occurred (if the event is a microevent, use 324 and 325, if it is a nanoevent)
FW_INITIATOR_OCTETS	231	4	Total number of Layer 4 payload bytes in the packet flow that arrives from the initiator
FW_RESPONDER_OCTETS	232	4	Total number of Layer 4 payload bytes in the packet flow that arrives from the responder
AAA Fields			
FW_USERNAME	40,000	20 or 64 depending on the template	AAA [5] user name
FW_USERNAME_MAX	40,000	64	AAA user name of the maximum permitted size
Alert Fields			
FW_HALFOPEN_CNT	35,012	4	Half-open session entry count
FW_BLACKOUT_SECS	35,004	4	Time, in seconds, when the destination is blacked out or unavailable
FW_HALFOPEN_HIGH	35,005	4	Configured maximum rate of TCP half-open session entries logged in one minute

Field ID	Type	Length	Description
FW_HALFOPEN_RATE	35,006	4	Current rate of TCP half-open session entries logged in one minute
FW_MAX_SESSIONS	35,008	4	Maximum number of sessions allowed for this zone pair or class ID
Miscellaneous			
FW_ZONEPAIR_ID	35,007	4	Zone pair ID
FW_CLASS_ID	51	4	Class ID
FW_ZONEPAIR_NAME	35,009	64	Zone pair name
FW_CLASS_NAME	100	64	Class name
FW_EXT_EVENT_DESC	35,010	32	Extended event description
FLOW_FIELD_CTS_SRC_GROUP_TAG	34000	2	Cisco Trustsec source tag
FW_SUMMARY_PKT_CNT	35,011	4	Number of packets represented by the drop/pass summary record
FW_EVENT_LEVEL	33003	4	Defines the level of the logged event • 0x01—Per box • 0x02—VRF • 0x03—Zone • 0x04—Class map • Other values are undefined
FW_EVENT_LEVEL_ID	33,004	4	Defines the identifier for the FW_EVENT_LEVEL field • If FW_EVENT_LEVEL is 0x02 (VRF), this field represents VRF_ID. • If FW_EVENT_LEVEL is 0x03 (zone), this field represents ZONE_ID. • If FW_EVENT_LEVEL is 0x04 (class map), this field represents CLASS_ID. • In all other cases the field ID will be 0 (zero). If FW_EVENT_LEVEL is not present, the value of this field must be zero.

Field ID	Type	Length	Description
FW_CONFIGURED_VALUE	33,005	4	Value that represents the configured half-open, aggressive-aging, and event-rate monitoring limit. The interpretation of this field value depends on the associated FW_EXT_EVENT field.
FW_ERM_EXT_EVENT	33,006	2	Extended event-rate monitoring code
FW_ERM_EXT_EVENT_DESC	33,007	N (string)	Extended event-rate monitoring event description string

[1] Internet Control Message Protocol
[2] Simple Network Management Protocol
[3] virtual routing and forwarding
[4] Coordinated Universal Time
[5] Authentication, Authorization, and Accounting

HSL Messages

The following are sample syslog messages from an Cisco ASR 1000 Series Aggregation Services Router:

Table 2: Syslog Messages and Their Templates

Message Identifier	Message Description	HSL Template
FW-6-DROP_PKT Type: Info	Dropping %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u %s %s Explanation: Packet dropped by firewall inspection. %s: tcp/udp/icmp/unknown prot/L7 prot %s:interface %CA:%u ip/ip6 addr: port %s:%s: zone pair name/ class name %s "due to" %s: fw_ext_event name %u ip ident %s: if tcp, tcp seq/ack number and tcp flags %s: username	FW_TEMPLATE_DROP_V4 or FW_TEMPLATE_DROP_V6

Message Identifier	Message Description	HSL Template
FW-6-SESS_AUDIT_TRAIL_START Type: Info	(target:class)-(%s:%s):Start %s session: initiator (%CA:%u) -- responder (%CA:%u) from %s %s %s Explanation: Start of an inspection session. This message is issued at the start of each inspection session and it records the source/destination addresses and ports. %s:%s: zonepair name: class name %s: l4/l7 protocolname %CA:%u ip/ip6 addr: port %s : interface %s : username %s : TODO Actual log: *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 or FW_TEMPLATE_START_AUDIT_V6

Message Identifier	Message Description	HSL Template
FW-6-SESS_AUDIT_TRAIL Type: Info	(target:class)-(%s:%s):Stop %s session: initiator (%CA:%u) sent %u bytes -- responder (%CA:%u) sent %u bytes , from %s %s Explanation: Per-session transaction log of network activities. This message is issued at the end of each inspection session, and it records the source/destination addresses and ports, and the number of bytes transmitted by the client and the server. %s:%s: zonepair name: class name %s: l4/l7 protocolname %CA:%u ip/ip6 addr: port %u bytes counters %s: interface %s : TODO Actual log: *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 or FW_TEMPLATE_STOP_AUDIT_V6
FW-4-UNBLOCK_HOST Type: Warning	(target:class)-(%s:%s):New TCP connections to host %CA no longer blocked Explanation: New TCP connection attempts to the specified host are no longer blocked. This message indicates that the blocking of new TCP connection attempts to the specified host has been removed. %s:%s: zonepair name: class name %CA: ip/ip6 addr	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW_EXT_ALERT_UNBLOCK_HOST

Message Identifier	Message Description	HSL Template
FW-4-HOST_TCP_ALERT_ON Type: Warning	"(target:class)-(%s:%s):Max tcp half-open connections (%u) exceeded for host %CA. Explanation: Exceeded the max-incomplete host limit for half-open TCP connections. This message indicates that a high number of half-open connections is coming to a protected server, and this may indicate that a SYN flood attack is in progress. %s:%s: zonepair name: class name %u: half open cnt %CA: ip/ip6 addr	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW_EXT_ALERT_HOST_TCP_ALERT_ON
FW-2-BLOCK_HOST Type: Critical	(target:class)-(%s:%s):Blocking new TCP connections to host %CA for %u minute%s (half-open count %u exceeded). Explanation: Exceeded the max-incomplete host threshold for TCP connections. Any subsequent new TCP connection attempts to the specified host is denied, and the blocking option is configured to block all subsequent new connections. The blocking will be removed when the configured block time expires. %s:%s: zonepair name: class name %CA: ip/ip6 addr %u blackout min %s: s if > 1 min blackout time %u: half open counter	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 or FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6 with fw_ext_event id: FW_EXT_ALERT_BLOCK_HOST

Message Identifier	Message Description	HSL Template
FW-4-ALERT_ON Type: Warning	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u Explanation : Either the max-incomplete high threshold of half-open connections or the new connection initiation rate has been exceeded. This error message indicates that an unusually high rate of new connections is coming through the firewall, and a DOS attack may be in progress. This message is issued only when the max-incomplete high threshold is crossed. %s:%s: zonepair name: class name %s: "getting aggressive" %u/%u halfopen cnt/high %u: current rate	FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_ON
FW-4-ALERT_OFF Type: Warning	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u Explanation: Either the number of half-open connections or the new connection initiation rate has gone below the max-incomplete low threshold. This message indicates that the rate of incoming new connections has slowed down and new connections are issued only when the max-incomplete low threshold is crossed. %s:%s: zonepair name: class name %s: "calming down" %u/%u halfopen cnt/high %u: current rate	FW_TEMPLATE_ALERT_HALFOPEN_V4 or FW_TEMPLATE_ALERT_HALFOPEN_V6: with fw_ext_event id FW_EXT_SESS_RATE_ALERT_OFF

Message Identifier	Message Description	HSL Template
FW-4-SESSIONS_MAXIMUM Type: Warning	Number of sessions for the firewall policy on "(target:class)-(%s:%s) exceeds the configured sessions maximum value %u Explanation: The number of established sessions have crossed the configured sessions maximum limit. %s:%s: zonepair name: class name %u: max session	FW_TEMPLATE_ALERT_MAX_SESSION
FW-6-PASS_PKT Type: Info	Passing %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u Explanation: Packet is passed by firewall inspection. %s: tcp/udp/icmp/unknown prot %s:interface %CA:%u src ip/ip6 addr: port %CA:%u dst ip/ip6 addr: port %s:%s: zonepair name: class name %s %s: "due to", "PASS action found in policy-map" %u: ip ident	FW_TEMPLATE_PASS_V4 or FW_TEMPLATE_PASS_V6
FW-6-LOG_SUMMARY Type: Info	%u packet%s %s from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s Explanation : Log summary for the number of packets dropped/passed %u %s: pkt_cnt, "s were" or "was" %s: "dropped"/ "passed" %s: interface %CA:%u src ip/ip6 addr: port %CA:%u dst ip/ip6 addr: port %s:%s: zonepair name: class name %s: username	FW_TEMPLATE_SUMMARY_V4 or FW_TEMPLATE_SUMMARY_V6 with FW_EVENT: 3 - drop 4 - pass

Firewall Extended Events

The event name of the firewall extended event maps the firewall extended event value to an event ID. Use the event name option record to obtain the mapping between an event value and an event ID.

Extended events are not part of standard firewall events (inspect, pass, or drop).

The following table describes the firewall extended events applicable prior to Cisco IOS XE Release 3.9S.

Table 3: Firewall Extended Events and Event Descriptions for Releases earlier than Cisco IOS XE Release 3.9S

Value	Event ID	Description
0	FW_EXT_LOG_NONE	No specific extended event.
1	FW_EXT_ALERT_UNBLOCK_HOST	New TCP connection attempts to the specified host are no longer blocked.
2	FW_EXT_ALERT_HOST_TCP_ALERT_ON	Maximum incomplete host limit for half-open TCP connections are exceeded.
3	FW_EXT_ALERT_BLOCK_HOST	All subsequent new TCP connection attempts to the specified host are denied because the maximum incomplete host threshold of half-open TCP connections is exceeded, and the blocking option is configured to block subsequent new connections.
4	FW_EXT_SESS_RATE_ALERT_ON	Maximum incomplete high threshold of half-open connections is exceeded, or the new connection initiation rate is exceeded.
5	FW_EXT_SESS_RATE_ALERT_OFF	Number of half-open TCP connections is below the maximum incomplete low threshold, or the new connection initiation rate has gone below the maximum incomplete low threshold.
6	FW_EXT_RESET	Reset connection.
7	FW_EXT_DROP	Drop connection.
10	FW_EXT_L4_NO_NEW_SESSION	No new session is allowed.
12	FW_EXT_L4_INVALID_SEG	Invalid TCP segment.
13	FW_EXT_L4_INVALID_SEQ	Invalid TCP sequence number.
14	FW_EXT_L4_INVALID_ACK	Invalid TCP acknowledgment (ACK).
15	FW_EXT_L4_INVALID_FLAGS	Invalid TCP flags.
16	FW_EXT_L4_INVALID_CHKSM	Invalid TCP checksum.
18	FW_EXT_L4_INVALID_WINDOW_SCALE	Invalid TCP window scale.

Value	Event ID	Description
19	FW_EXT_L4_INVALID_TCP_OPTIONS	Invalid TCP options.
20	FW_EXT_L4_INVALID_HDR	Invalid Layer 4 header.
21	FW_EXT_L4_OOO_INVALID_SEG	OoO [6] invalid segment.
24	FW_EXT_L4_SYNFLOOD_DROP	Synchronized (SYN) flood packets are dropped.
25	FW_EXT_L4_SCB_CLOSED	Session is closed while receiving packets.
26	FW_EXT_L4_INTERNAL_ERR	Firewall internal error.
27	FW_EXT_L4_OOO_SEG	OoO segment.
28	FW_EXT_L4_RETRANS_INVALID_FLAGS	Invalid retransmitted packet.
29	FW_EXT_L4_SYN_IN_WIN	Invalid SYN flag.
30	FW_EXT_L4_RST_IN_WIN	Invalid reset (RST) flag.
31	FW_EXT_L4_STRAY_SEG	Stray TCP segment.
32	FW_EXT_L4_RST_TO_RESP	Sending reset message to the responder.
33	FW_EXT_L4_CLOSE_SCB	Closing a session.
34	FW_EXT_L4_ICMP_INVAL_RET	Invalid ICMP [7] packet.
37	FW_EXT_L4_MAX_HALFSESSION	Maximum half-open session limit is exceeded.
38	FW_EXT_NO_RESOURCE	Resources (memory) are not available.
40	FW_EXT_INVALID_ZONE	Invalid zone.
41	FW_EXT_NO_ZONE_PAIR	Zone pairs are not available.
42	FW_EXT_NO_TRAFFIC_ALLOWED	Traffic is not allowed.
43	FW_EXT_FRAGMENT	Packet fragments are dropped.
44	FW_EXT_PAM_DROP	PAM [8] action is dropped.
45	FW_EXT_NOT_INITIATOR	Not a session-initiating packet. Occurs due to one of the following reasons: • If the protocol is TCP, the first packet is not a SYN packet. • If the protocol is ICMP, the first packet is not an ECHO or a TIMESTAMP packet.

Value	Event ID	Description
48	FW_EXT_ICMP_ERROR_PKTS_BURST	ICMP error packets came in burst mode. In burst mode, packets are sent repeatedly without waiting for a response from the responder interface.
49	FW_EXT_ICMP_ERROR_MULTIPLE_UNREACH	More than one ICMP error of type "destination unreachable" is received.
50	FW_EXT_ICMP_ERROR_L4_INVALID_SEQ	Embedded packet in the ICMP error message has an invalid sequence number.
51	FW_EXT_ICMP_ERROR_L4_INVALID_ACK	Embedded packet in the ICMP error message has an invalid acknowledge (ACK) number.
52	FW_EXT_MAX	Never used.

[6] Out-of-Order
[7] Internet Control Message Protocol
[8] Port-to-Application Mapping

The following table describes the firewall extended events from that are applicable to Cisco IOS XE Release 3.9S and later releases.

Table 4: Firewall Extended Events and Event Descriptions for Cisco IOS XE Release 3.9S and Later Releases

Value	Event ID	Description
0	FW_EXT_LOG_NONE	No specific extended event.
1	FW_EXT_FW_DROP_L4_TYPE_INVALID_HDR	Small datagram that cannot contain the Layer 4 ICMP, TCP, or UDP headers.
2	FW_EXT_FW_DROP_L4_TYPE_INVALID_ACK_FLAG	Did not contain an ACK flag, or a RST flag was set in the SYN/ACK packet during the TCP three-way handshake and the packet had an invalid sequence number.
3	FW_EXT_FW_DROP_L4_TYPE_INVALID_ACK_NUM	Occurs due to one of the following reasons: • When a packet's ACK value is less than the connection's oldest unacknowledged sequence number. • When a packet's ACK value is greater than the connection's next sequence number. • For SYN/ACK or ACK packets received during the three-way handshake, the sequence number is not equal to the initial sequence number plus 1.

Value	Event ID	Description
4	FW_EXT_FW_DROP_L4_TYPE_INVALID _TCP_INITIATOR	The first packet of a flow was not a SYN packet.
5	FW_EXT_FW_DROP_L4_TYPE_SYN _WITH_DATA	The SYN packet contains the payload and these SYN packet is not supported.
6	FW_EXT_FW_DROP_L4_TYPE_INVALI D_TCP_WIN_SCALE_OPTION	Invalid length for the TCP window-scale option.
7	FW_EXT_FW_DROP_L4_TYPE_INVALID _SEG_SYNSENT_STATE	An invalid TCP segment was received in the SYNSENT state. Occurs due to one of the following reasons: • SYN/ACK has a payload. • SYN/ACK has other flags (push [PSH], urgent [URG], finish [FIN]) set. • Retransmit SYN message with a payload or invalid TCP flags (ACK, PSH, URG, FIN, RST) was received. • A non-SYN packet was received from the initiator.
8	FW_EXT_FW_DROP_L4_TYPE_INVALID _SEG_SYNRCVD_STATE	A retransmitted SYN packet contains a payload or received a packet from the responder.
9	FW_EXT_FW_DROP_L4_TYPE_INVALID _SEG_PKT_TOO_OLD	Packet is older (lesser than) than the receiver's current TCP window.
10	FW_EXT_FW_DROP_L4_TYPE_INVALID _SEG_PKT_WIN_OVERFLOW	The sequence number of the packet is outside (greater than) the receiver's TCP window.
11	FW_EXT_FW_DROP_L4_TYPE_INVALID _SEG_PYLD_AFTER_FIN_SEND	A packet containing a payload was received from the sender after a FIN message was received.
12	FW_EXT_FW_DROP_L4_TYPE_INVALID _FLAGS	TCP flags associated with the packet are not valid. This may occur for the following reasons: • Extra flags along with the SYN flag, are set in the initial packet. Only the SYN flag is allowed in the initial packet. • Expected SYN/ACK did not contain a SYN flag, or the SYN/ACK contained extraneous flags in the second packet of the three-way handshake.

Value	Event ID	Description
13	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEQ	Invalid sequence number. Occurs due to one of the following reasons: • The sequence number is less than the ISN [9]. • The sequence number is equal to the ISN but not equal to a SYN packet. • If the receive window size is zero and the packet contains data, or if the sequence number is greater than the last ACK number. • Sequence number falls beyond the TCP window.
14	FW_EXT_FW_DROP_L4_TYPE_RETRANS _INVALID_FLAGS	A retransmitted packet was already acknowledged by the receiver.
15	FW_EXT_FW_DROP_L4_TYPE_L7_OOO _SEG	The packet contains a TCP segment that arrived prior to the expected next segment.
16	FW_EXT_FW_DROP_L4_TYPE_SYN _FLOOD_DROP	Maximum-incomplete sessions configured for the policy have been exceeded and the host is in block time.
17	FW_EXT_FW_DROP_L4_TYPE_MAX _HALFSESSION	Exceeded the number of allowed half-open sessions.
18	FW_EXT_FW_DROP_L4_TYPE_ TOO_MANY_PKTS	Exceeded the maximum number of simultaneous inspectable packets allowed per flow. The number is currently set to allow 25 simultaneous packets to be inspected. The simultaneous inspection prevents any one flow from monopolizing more than its share of processor resources.
19	FW_EXT_FW_DROP_L4_TYPE_TOO _MANY_ICMP_ERR_PKTS	Exceeded the maximum number of ICMP error packets allowed per flow. This log is triggered by the firewall base inspection.
20	FW_EXT_FW_DROP_L4_TYPE_UNEXPECT _TCP_PYLD	Retransmitted SYN/ACK from the responder included a payload. Payloads are not allowed during a TCP three-way handshake negotiation.
21	FW_EXT_FW_DROP_L4_TYPE_INTERNAL _ERR_UNDEFINED_DIR	Packet direction is undefined.

Value	Event ID	Description
22	FW_EXT_FW_DROP_L4_TYPE_SYN _IN_WIN	A TCP packet of an established session arrived with the SYN flag set. A SYN flag is not allowed after the initial two packets of the three-way handshake.
23	FW_EXT_FW_DROP_L4_TYPE_RST _IN_WIN	A TCP packet with the RST flag set was received with a sequence number that is outside the last received acknowledgment. The packet may be sent out of order.
24	FW_EXT_FW_DROP_L4_TYPE_ STRAY_SEG	An unexpected packet was received after the flow was torn down, or a packet was received from the responder before the initiator sent a valid SYN flag.
25	FW_EXT_FW_DROP_L4_TYPE_ RST_TO_RESP	A SYN/ACK flag was expected from the responder. However, a packet with an invalid sequence number was received. The zone-based firewall sent a RST flag to the responder.
26	FW_EXT_FW_DROP_L4_TYPE _I NTERNAL_ERR_ICMP_NO_NAT	The ICMP packet is NAT [10] translated; but internal NAT information is missing. An internal error.
27	FW_EXT_FW_DROP_L4_TYPE _ INTERNAL_ERR_ICMP_ALLOC_FAIL	Failed to allocate an ICMP error packet during an ICMP inspection.
28	FW_EXT_FW_DROP_L4_TYPE _INTERNAL_ERR_ICMP_GET_STAT_BLK_FAIL	The classification result did not have the required statistics memory. The policy information was not properly downloaded to the data plane.
29	FW_EXT_FW_DROP_L4_TYPE _INTERNAL_ERR_ICMP_DIR_NOT_IDENTIFIED	Packet direction is not defined.
30	FW_EXT_FW_DROP_L4_TYPE_ ICMP_SCB_CLOSE	Received an ICMP packet while the session is being torn down.
31	FW_EXT_FW_DROP_L4_TYPE_ ICMP_PKT_NO_IP_HDR	No IP header in the payload of the ICMP error packet.
32	FW_EXT_FW_DROP_L4_TYPE_ ICMP_ERROR_NO _IP_NO_ICMP	The ICMP error packet has no IP or ICMP, which is probably due to a malformed packet.
33	FW_EXT_FW_DROP_L4_TYPE_ ICMP_ERROR _PKTS_BURST	The ICMP error packet exceeded the burst limit of 10
34	FW_EXT_FW_DROP_L4_TYPE_ ICMP_ERROR _MULTIPLE_UNREACH	The ICMP error packet exceeded the “Unreachable” limit. Only the first unreachable packet is allowed to pass.

Value	Event ID	Description
35	FW_EXT_FW_DROP_L4_TYPE_ ICMP_ERROR _L4_INVALID_SEQ	The sequence number of the embedded packet does not match the sequence number of the TCP packet that triggers the ICMP error packet.
36	FW_EXT_FW_DROP_L4_TYPE_ ICMP_ERROR _L4_INVALID_ACK	The TCP packet contained in an ICMP error packet payload has an ACK flag that was not seen before.
37	FW_EXT_FW_DROP_L4_TYPE_ ICMP_PKT_TOO _SHORT	The ICMP error packet length is less than the IP header length plus the ICMP header length.
38	FW_EXT_FW_DROP_L4_TYPE_ SESSION_LIMIT	Resources exceeded the session limit while promoting for an imprecise channel.
39	FW_EXT_FW_DROP_L4_TYPE_ SCB_CLOSE	A TCP packet was received on a closed session.
40	FW_EXT_FW_DROP_INSP_TYPE_ POLICY_NOT_PRESENT	A policy is not present in a zone pair.
41	FW_EXT_FW_DROP_INSP_TYPE_ SESS_MISS_POLICY _NOT_PRESENT	A zone pair is configured in the same zone, but the zone does not have any policies.
44	FW_EXT_FW_DROP_INSP_TYPE_ CLASS_ACTION_DROP	The classification action is to drop the non-ICMP, TCP, and UDP packets.
45	FW_EXT_FW_DROP_INSP_TYPE_ PAM_LOOKUP_FAIL	The classification action is to drop the PAM entry.
48	FW_EXT_FW_DROP_INSP_TYPE_ INTERNAL_ERR_ GET_STAT_BLK_FAIL	Failed to get the statistic block from the classification result bytes.
49	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_SYNCOOKIE _MAX_DST	The maximum entry limit for SYN flood packets is reached.
50	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_INTERNAL _ERR_ALLOC_FAIL	Cannot allocate memory for the destination table entry.
51	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_SYN_COOKIE _TRIGGER	The SYN cookie logic is triggered. Indicates that the SYN/ACK with the SYN cookie was sent and the original SYN packet was dropped.
52	FW_EXT_FW_DROP_POLICY_ TYPE_FRAG_DROP	The first fragment of a VFR [11] packet is dropped and all associated remaining fragments will be dropped.
53	FW_EXT_FW_DROP_POLICY_ TYPE_ACTION_DROP	The classification action is to drop the packet.

Value	Event ID	Description
54	FW_EXT_FW_DROP_POLICY_ TYPE_ICMP_ACTION_DROP	The policy action of the ICMP embedded packet is DROP.
55	FW_EXT_FW_DROP_L7_TYPE_ NO_SEG	Layer 7 ALG [12] does not inspect inspect-segmented packets.
56	FW_EXT_FW_DROP_L7_TYPE_ NO_FRAG	Layer 7 ALG does not inspect fragmented packets.
57	FW_EXT_FW_DROP_L7_TYPE_ UNKNOWN_PROTO	Unknown application protocol type.
58	FW_EXT_FW_DROP_L7_TYPE_ ALG_RET_DROP	Layer 7 ALG inspection resulted in a packet drop.
59	FW_EXT_FW_DROP_NONSESSION _TYPE	Session creation has failed.
60	FW_EXT_FW_DROP_NO_NEW _SESSION_TYPE	During initial HA [13] states, a new session is not allowed.
61	FW_EXT_FW_DROP_NOT_ INITIATOR_TYPE	Not a session initiator packet.
62	FW_EXT_FW_DROP_INVALID _ZONE_TYPE	When default zones are not enabled, traffic is only allowed between interfaces that are associated with security zones.
64	FW_EXT_FW_DROP_NO_ FORWARDING_TYPE	The firewall is not configured.
65	FW_EXT_FW_DROP_ BACKPRESSURE_TYPE	The firewall backpressure can be enabled if HSL [14] is enabled, and the HSL logger was unable to send a log message. Backpressure will remain enabled until HSL is able to send a log.
66	FW_EXT_FW_DROP_L4_TYPE_INTERNAL _ERR _SYNFLOOD_ALLOC_HOSTDB_FAIL	During SYN processing, host rate limits are tracked. The host entry could not be allocated.
67	FW_EXT_FW_DROP_L4_TYPE_ SYNFLOOD_BLACKOUT_DROP	If the configured half-open connection limit is exceeded and blackout time is configured, all new connections to the specified IP address are dropped.
68	FW_EXT_FW_DROP_L7_TYPE_ PROMOTE_FAIL_NO_ZONE_PAIR	A failed policy. When an ALG attempts to promote a session because no zone pairs are configured, the policy fails.
69	FW_EXT_FW_DROP_L7_TYPE_ PROMOTE_FAIL_NO_POLICY	A failed policy. When an ALG attempts to promote a session due to no policy, the policy fails.

Value	Event ID	Description
	FW_EXT_FW_DROP_L4_TYPE_ONEFW _SCB_CLOSE	A packet is received after the Context-Aware firewall (CXSC) requested a teardown.
	FW_EXT_FW_DROP_L4_TYPE_ONEFW _FAIL_CLOSE	CXSC is not running.

[9] initial sequence number
[10] Network Address Translation
[11] virtual fragmentation and reassembly
[12] application layer gateway
[13] high availability
[14] high-speed logging

How to Configure Firewall High-Speed Logging

Enabling High-Speed Logging for Global Parameter Maps

By default, high-speed logging (HSL) is not enabled and firewall logs are sent to a logger buffer located in the Route Processor (RP) or the console. When HSL is enabled, logs are sent to an off-box, high-speed log collector. Parameter maps provide a means of performing actions on the traffic that reaches a firewall and a global parameter map applies to the entire firewall session table. Perform this task to enable high-speed logging for global parameter maps.

SUMMARY STEPS

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**parameter-map type inspect global** **Example:** `Device(config)# parameter-map type inspect global`	Configures a global parameter map and enters parameter-map type inspect configuration mode.
Step 4	**log dropped-packets** **Example:** `Device(config-profile)# log dropped-packets`	Enables dropped-packet logging.
Step 5	**log flow-export v9 udp destination** *ip-address port-number* **Example:** `Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000`	Enables NetFlow event logging and provides the IP address and the port number of the log collector.
Step 6	**log flow-export template timeout-rate** *seconds* **Example:** `Device(config-profile) log flow-export template timeout-rate 5000`	Specifies the template timeout value.
Step 7	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Enabling High-Speed Logging for Firewall Actions

Perform this task enable high-speed logging if you have configured inspect-type parameter maps. Parameter maps specify inspection behavior for the firewall and inspection parameter-maps for the firewall are configured as the inspect type.

SUMMARY STEPS

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect parameter-map-hsl`	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** keyword, and enters parameter-map type inspect configuration mode.
Step 4	**audit-trail on** **Example:** `Device(config-profile)# audit-trail on`	Enables audit trail messages. • You can enable audit-trail to a parameter map to record the start, stop, and duration of a connection or session, and the source and destination IP addresses.
Step 5	**alert on** **Example:** `Device(config-profile)# alert on`	Enables stateful-packet inspection alert messages that are displayed on the console.
Step 6	**one-minute** {**low** *number-of-connections* | **high** *number-of-connections*} **Example:** `Device(config-profile)# one-minute high 10000`	Defines the number of new unestablished sessions that cause the system to start deleting half-open sessions and stop deleting half-open sessions.
Step 7	**tcp max-incomplete host** *threshold* **Example:** `Device(config-profile)# tcp max-incomplete host 100`	Specifies the threshold and blocking time values for TCP host-specific, denial of service (DoS) detection and prevention.
Step 8	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and returns to global configuration mode.
Step 9	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect policy-map-hsl`	Creates an inspect-type policy map and enters policy map configuration mode.
Step 10	**class type inspect** *class-map-name* **Example:**	Specifies the traffic class on which an action is to be performed and enters policy-map class configuration mode.

	Command or Action	Purpose
	`Device(config-pmap)# class type inspect class-map-tcp`	
Step 11	**inspect** *parameter-map-name* **Example:** `Device(config-pmap-c)# inspect parameter-map-hsl`	(Optional) Enables stateful packet inspection.
Step 12	**end** **Example:** `Device(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to privileged EXEC mode.

Configuration Examples for Firewall High-Speed Logging

Example: Enabling High-Speed Logging for Global Parameter Maps

The following example shows how to enable logging of dropped packets, and to log error messages in NetFlow Version 9 format to an external IP address:

```
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
```

Example: Enabling High-Speed Logging for Firewall Actions

The following example shows how to configure high-speed logging (HSL) for inspect-type parameter-map parameter-map-hsl.

```
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
```

Additional References for Firewall High-Speed Logging

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Security commands	• 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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Firewall High-Speed Logging

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for Firewall High-Speed Logging

Feature Name	Releases	Feature Information
Firewall High-Speed Logging	Cisco IOS XE Release 2.1	The Firewall High-Speed Logging Support feature introduces support for the firewall HSL using NetFlow Version 9 as the export format. The following commands were introduced or modified: **log dropped-packet**, **log flow-export v9 udp destination**, **log flow-export template timeout-rate**, **parameter-map type inspect global**.

Feature Name	Releases	Feature Information
Configuring Zone-based Firewall using High-Speed Logging	Cisco IOS XE Gibraltar 16.11.1	In this release, support was added for the source interface. The following commands were introduced or modified: **log flow-export v9 udp destination source interface** *interface-name*