Schema: Connection Log Tables

This chapter contains information on the schema and supported joins for connection data.

For more information, see the sections listed in the following table. The Version column indicates the Database Access versions supported by each listed table.

Table 7-1 Schema for Connection Log Tables

See...	For the table that stores information on...	Version
connection_log, page 7-1	Individual connections. Supersedes deprecated table **rna_flow**.	5.0+
connection_summary, page 7-12	Connection log summaries. Supersedes deprecated table **rna_flow_summary**.	5.0+
si_connection_log, page 7-16	Individual connections. Used for security intelligence.	5.3+

connection_log

The **connection_log** table contains information on connection events. The FireSIGHT System generates a connection event when a connection between a monitored host and any other host is established; the event contains detailed information about the monitored traffic.

The **connection_log** table supersedes the deprecated **rna_flow** table starting with Version 5.0 of the FireSIGHT System.

For more information, see the following sections:

- connection_log Fields, page 7-1
- connection_log Joins, page 7-12
- connection_log Sample Query, page 7-12

connection_log Fields

The following table describes the database fields you can access in the **connection_log** table.

Table 7-2 connection_log Fields

Field	Description
access_control_policy_name	The access control policy that contains the access control rule (or default action) that logged the connection.
access_control_policy_UUID	The UUID of the access control policy that contains the access control rule (or default action) that logged the connection.
access_control_reason	The reason that the access control rule logged the connection. One or more of the following: • IP Block • IP Monitor • User Bypass • File Monitor • File Block • Intrusion Monitor • Intrusion Block • File Resume Block • File Resume Allow • File Custom Detection • SSL Block • DNS Block • DNS Monitor • URL Block • URL Monitor • HTTP Injection • Intelligent App Bypass • blank if there is no connection logged
access_control_rule_action	The action associated with the access control rule (or default action): allow, block, and so on.
access_control_rule_id	An internal identification number for the rule.
access_control_rule_name	The access control rule (or default action) that logged the connection.
application_protocol_id	An internal identification number of the application protocol.
application_protocol_name	One of: • the name of the application, if a positive identification can be made • unknown if the system cannot identify the server based on known server fingerprints • pending if the system requires more data • blank if there is no application information in the connection
bytes_recv	The total number of bytes transmitted by the session responder.
bytes_sent	Total number of bytes transmitted by the session initiator.
cert_valid_end_date	The Unix timestamp on which the SSL certificate used in the connection ceases to be valid.

Table 7-2 connection_log Fields (continued)

Field	Description
cert_valid_start_date	The Unix timestamp when the SSL certificate used in the connection was issued.
client_application_id	An internal identification number for the client application that was used in the intrusion event.
client_application_name	The client application, if available, that was used in the intrusion event. One of: • the name of the application, if a positive identification can be made. • a generic client name if the system detects a client application but cannot identify a specific one. • blank if there is no client application information in the connection.
client_application_version	The version of the client application.
connection_type	The detection source for the connection information. Either: • rna, if detected by a Cisco device • netflow, if exported by a NetFlow-enabled device
counter	Counter for the intrusion event associated with the connection event.
file_count	The number of files identified by Snort in a session. A record is generated for each file identified in the session.
first_packet_sec	The UNIX timestamp of the date and time the first packet of the session was seen.
flow_id	An internal identification number for the connection.
icmp_code	ICMP code if the event is ICMP traffic, or null if the event was not generated from ICMP traffic.
icmp_type	ICMP type if the event is ICMP traffic, or null if the event was not generated from ICMP traffic.
initiator_continent_name	The name of the continent of the host that initiated the session: ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica
initiator_country_id	Code for the country of the host that initiated the session.
initiator_country_name	Name of the country of the host that initiated the session.
initiator_ip	Field deprecated in Version 5.2. Due to backwards compatibility the value in this field is not set to null, but it is not reliable.
initiator_ip_address	Field deprecated in Version 5.0. Returns null for all queries.

Table 7-2 connection_log Fields (continued)

Field	Description
initiator_ipaddr	A binary representation of the IP address of the host that initiated the session.
initiator_ipv4	Field deprecated in Version 5.2. Returns null for all queries.
initiator_port	The port used by the session initiator.
initiator_user_dept	The department of the user who last logged into the initiator host.
initiator_user_email	The email address of the user who last logged into the initiator host.
initiator_user_first_name	The first name of the user who last logged into the initiator host.
initiator_user_id	An internal identification number for the user who last logged into the initiator host.
initiator_user_last_name	The last name of the user who last logged into the initiator host.
initiator_user_last_seen_sec	The UNIX timestamp of the date and time the FireSIGHT System last detected user activity for the user who last logged into the initiator host.
initiator_user_last_updated_sec	The UNIX timestamp of the date and time the FireSIGHT System last updated the user record for the user who last logged into the initiator host.
initiator_user_name	The user name of the user who last logged into the initiator host.
initiator_user_phone	The phone number of the user who last logged into the initiator host.
instance_id	Numerical ID of the Snort instance on the managed device that generated the event.
interface_egress_name	The ingress interface associated with the connection.
interface_ingress_name	The egress interface associated with the connection.
ioc_count	Number of indications of compromise found in the connection.
ips_event_count	The number of intrusion events generated in the connection prior to intrusion event thresholding.
last_packet_sec	The UNIX timestamp of the date and time the last packet of the session was seen.
monitor_rule_id_1	The ID of the first monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_1.
monitor_rule_id_2	The ID of the second monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_2.
monitor_rule_id_3	The ID of the third monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_3.
monitor_rule_id_4	The ID of the fourth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_4.
monitor_rule_id_5	The ID of the fifth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_5.
monitor_rule_id_6	The ID of the sixth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_6.
monitor_rule_id_7	The ID of the seventh monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_7.

Table 7-2 connection_log Fields (continued)

Field	Description
monitor_rule_id_8	The ID of the eighth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_8.
monitor_rule_name_1	The name of the first monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_1.
monitor_rule_name_2	The name of the second monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_2.
monitor_rule_name_3	The name of the third monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_3.
monitor_rule_name_4	The name of the fourth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_4.
monitor_rule_name_5	The name of the fifth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_5.
monitor_rule_name_6	The name of the sixth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_6.
monitor_rule_name_7	The name of the seventh monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_7.
monitor_rule_name_8	The name of the eighth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_8.
netbios_domain	The NetBIOS domain used in the connection.
netflow_dst_as	Netflow autonomous system number of the destination, either origin or peer.
netflow_dst_mask	Netflow destination address prefix mask.
netflow_dst_tos	Type of service from the IP header when packets are flowing from the destination to the source.
netflow_snmp_in	ID of the interface used by packets flowing from the source to the destination.
netflow_snmp_out	ID of the interface used by packets flowing from the destination to the source.
netflow_src_as	Netflow autonomous system number of the source, either origin or peer.
netflow_src_mask	Netflow source address prefix mask.
netflow_src_tos	Type of service from the IP header when packets are flowing from the source to the destination.
network_analysis_policy_name	The network analysis policy associated with the intrusion policy that generated the intrusion event.
network_analysis_policy_UUID	The UUID of the network analysis policy associated with the intrusion policy that generated the intrusion event.
packets_recv	The total number of packets received by the host that initiated the session.
packets_sent	The total number of packets transmitted by the host that initiated the session.
protocol_name	The name of the protocol used in the connection.

Table 7-2 connection_log Fields (continued)

Field	Description
protocol_num	The IANA number of the protocol as listed in http://www.iana.org/assignments/protocol-numbers.
responder_continent_name	The name of the continent of the host that responded to the session initiator: ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica
responder_country_id	Code for the country of the host that responded to the session initiator.
responder_country_name	Name of the country of the host that responded to the session initiator.
responder_ip	Field deprecated in Version 5.2. Due to backwards compatibility the value in this field is not set to null, but it is not reliable.
responder_ip_address	Field deprecated in Version 5.2. Returns null for all queries.
responder_ipaddr	A binary representation of the IPv4 or IPv6 address for the host that responded to the session initiator.
responder_ipv4	Field deprecated in Version 5.2. Returns null for all queries.
responder_port	The port used by the session responder.
responder_user_dept	The department of the user who last logged into the host that responded to the session initiator.
responder_user_email	The email address of the user who last logged into the host that responded to the session initiator.
responder_user_first_name	The first name of the user who last logged into the host that responded to the session initiator.
responder_user_id	An internal identification number for the user who last logged into the host that responded to the session initiator.
responder_user_last_name	The last name of the user who last logged into the host that responded to the session initiator.
responder_user_last_seen_sec	The UNIX timestamp of the date and time the FireSIGHT System last detected user activity for the user who last logged into the host that responded to the session initiator.
responder_user_last_updated_sec	The UNIX timestamp of the date and time the FireSIGHT System last updated the user record for the user who last logged into the host that responded to the session initiator.
responder_user_name	The user name of the user who last logged into the host that responded to the session initiator.
responder_user_phone	The phone number of the user who last logged into the host that responded to the session initiator.

Table 7-2 connection_log Fields (continued)

Field	Description
security_context	Description of the security context (virtual firewall) that the traffic passed through. Note that the system only populates this field for ASA FirePOWER devices in multi-context mode.
security_intelligence_category	The Security Intelligence category associated with the connection.
security_intelligence_ip	Whether the Security Intelligence-monitored IP address associated with the connection is a source IP (src) or destination IP (dst).
security_zone_egress_name	The egress security zone in the connection event.
security_zone_ingress_name	The ingress security zone in the connection event.
sensor_address	The IP address of the managed device that generated the event. Format is ipv4 address,ipv6 address.
sensor_name	The name of the managed device that monitored the session.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
source_device	Field deprecated in Version 5.0. Returns null for all queries.
src_device_ip	Field deprecated in Version 5.2. Due to backwards compatibility the value in this field is not set to null, but it is not reliable.
src_device_ipaddr	Either: • A binary representation of the IP address of the NetFlow-enabled device that exported the connection data • 0, for connections detected by Cisco managed devices.
src_device_ipv4	• Field deprecated in Version 5.2. Returns null for all queries.
ssl_actual_action	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include: • Unknown • Do Not Decrypt • Block • Block With Reset • Decrypt (Known Key) • Decrypt (Replace Key) • Decrypt (Resign)
ssl_cipher_suite	Encryption suite used by the SSL connection. The value is stored in decimal format. See www.iana.org/assignments/tls-parameters/tls-parameters.xhtml for the cipher suite designated by the value.

Table 7-2 connection_log Fields (continued)

Field	Description
ssl_expected_action	The action which should be performed on the connection based on the SSL Rule. Possible values include: • *Unknown* • *Do Not Decrypt* • *Block* • *Block With Reset* • *Decrypt (Known Key)* • *Decrypt (Replace Key)* • *Decrypt (Resign)*
ssl_flow_flags	The debugging level flags for an encrypted connection. Possible values include: • 0x00000001 — NSE_FLOW__VALID — must be set for other fields to be valid • 0x00000002 — NSE_FLOW__INITIALIZED — internal structures ready for processing • 0x00000004 — NSE_FLOW__INTERCEPT — SSL session has been intercepted

Table 7-2 connection_log Fields (continued)

Field	Description
ssl_flow_messages	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information. • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER

Table 7-2 connection_log Fields (continued)

Field	Description
ssl_flow_status	Status of the SSL Flow. These values describe the reason behind the action taken or the error message seen. Possible values include: • 'Unknown' • 'No Match' • 'Success' • 'Uncached Session' • 'Unknown Cipher Suite' • 'Unsupported Cipher Suite' • 'Unsupported SSL Version' • 'SSL Compression Used' • 'Session Undecryptable in Passive Mode' • 'Handshake Error' • 'Decryption Error' • 'Pending Server Name Category Lookup' • 'Pending Common Name Category Lookup' • 'Internal Error' • 'Network Parameters Unavailable' • 'Invalid Server Certificate Handle' • 'Server Certificate Fingerprint Unavailable' • 'Cannot Cache Subject DN' • 'Cannot Cache Issuer DN' • 'Unknown SSL Version' • 'External Certificate List Unavailable' • 'External Certificate Fingerprint Unavailable' • 'Internal Certificate List Invalid' • 'Internal Certificate List Unavailable' • 'Internal Certificate Unavailable' • 'Internal Certificate Fingerprint Unavailable' • 'Server Certificate Validation Unavailable' • 'Server Certificate Validation Failure' • 'Invalid Action'
ssl_issuer_common_name	Issuer Common name from the SSL certificate. This is typically the host and domain name of the certificate issuer, but may contain other information.
ssl_issuer_country	The country of the SSL certificate issuer.

Table 7-2 connection_log Fields (continued)

Field	Description
ssl_issuer_organization	The organization of the SSL certificate issuer.
ssl_issuer_organization_unit	The organizational unit of the SSL certificate issuer.
ssl_policy_action	The default action configured for the policy when no rules match.
ssl_policy_name	ID number of the SSL policy that handled the connection.
ssl_policy_reason	The reason the SSL policy logged the SSL session.
ssl_rule_action	The action selected in the user interface for the SSL rule (`allow`, `block`, and so forth).
ssl_rule_name	ID number of the SSL rule or default action that handled the connection.
ssl_serial_number	The serial number of the SSL certificate, assigned by the issuing CA.
ssl_server_name	Name provided in the server name indication in the SSL Client Hello.
ssl_subject_common_name	Subject Common name from the SSL certificate. This is typically the host and domain name of the certificate subject, but may contain other information.
ssl_subject_country	The country of the SSL certificate subject.
ssl_subject_organization	The organization of the SSL certificate subject.
ssl_subject_organization_unit	The organizational unit of the SSL certificate subject.
ssl_url_category	Category of the flow as identified from the server name and certificate common name.
ssl_version	The SSL or TLS protocol version used to encrypt the connection.
tcp_flags	The TCP flags detected in the session.
url	The URL requested by the monitored host during the session, if available.
url_category	The category of the URL requested by the monitored host.
url_reputation	The reputation of the URL requested by the monitored host. One of the following: • `1` — High risk • `2` — Suspicious sites • `3` — Benign sites with security risks • `4` — Benign sites • `5` — Well known
web_application_id	An internal identification number for the web application.
web_application_name	One of: • the name of the application, if a positive identification can be made. • `web browsing` if the system detects an application protocol of HTTP but cannot identify a specific web application. • blank if the connection has no HTTP traffic.

connection_log Joins

The following table describes the joins you can perform using the **connection_log** table.

Table 7-3 connection_log Joins

You can join this table on...	And...
application_protocol_id or client_application_id or web_application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
initiator_ipaddr or responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

connection_log Sample Query

The following query returns up to 25 connection event records from the **connection_log** table, sorted in descending order based on packet timestamps.

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation

FROM connection_log

WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00" ) ORDER BY
first_packet_sec

DESC, last_packet_sec DESC LIMIT 0, 25;
```

connection_summary

The **connection_summary** table contains information on connection summaries or aggregated connections. The FireSIGHT System aggregates connections over five-minute intervals. To be aggregated, connections must:

- have the same source and destination IP addresses
- use the same protocol
- use the same application
- either be detected by the same managed device (for sessions detected by managed devices with FireSIGHT) or be exported by the same NetFlow-enabled device and processed by the same managed device

The aggregated data in a connection summary includes the total number of packets and bytes sent by the initiator and responder hosts, as well as the number of connections in the summary.

The **connection_summary** table supersedes the deprecated **rna_flow_summary** table starting with Version 5.0 of the FireSIGHT System.

For more information, see the following sections:

- connection_summary Fields, page 7-13
- connection_summary Joins, page 7-15
- connection_summary Sample Query, page 7-15

connection_summary Fields

The following table describes the database fields you can access in the **connection_summary** table.

Table 7-4 connection_summary Fields

Field	Description
application_protocol_id	An internal identification number for the application protocol.
application_protocol_name	One of: • the name of the application, if a positive identification can be made • unknown if the system cannot identify the server based on known server fingerprints • pending if the system requires more data • blank if there is no application information in the connection
bytes_recv	The total number of bytes transmitted by the session responder.
bytes_sent	The total number of bytes transmitted by the session initiator.
connection_type	The detection source for the connection information. Either: • rna, if detected by a Cisco device • netflow, if exported by a NetFlow-enabled device
flow_type	Field deprecated in Version 5.0. Returns null for all queries.
id	An internal identification number for the connection summary.
initiator_ip_address	Field deprecated in Version 5.2. Returns null for all queries.
initiator_ipaddr	A binary representation of the IP address of the host that initiated the session.
initiator_user_dept	The department of the user who last logged into the initiator host.
initiator_user_email	The email address of the user who last logged into the initiator host.
initiator_user_first_name	The first name of the user who last logged into the initiator host.
initiator_user_id	An internal identification number for the user who last logged into the initiator host.
initiator_user_last_name	The last name of the user who last logged into the initiator host.
initiator_user_last_seen_sec	The UNIX timestamp of the date and time the FireSIGHT System last detected user activity for the user who last logged into the initiator host.

Table 7-4 connection_summary Fields (continued)

Field	Description
initiator_user_last_updated_sec	The UNIX timestamp of the date and time the FireSIGHT System last updated the user record for the user who last logged into the initiator host.
initiator_user_name	The user name of the user who last logged into the initiator host.
initiator_user_phone	The phone number of the user who last logged into the initiator host.
interface_egress_name	The ingress interface associated with the connection.
interface_ingress_name	The egress interface associated with the connection.
num_connections	The number of connections in the summary. For long-running connections, that is, connections that span multiple connection summary intervals, only the first connection summary is incremented.
packets_recv	The total number of packets transmitted by the session responder.
packets_sent	The total number of packets transmitted by the session initiator.
protocol_name	The name of the protocol used in the aggregated sessions.
protocol_num	The IANA number of the protocol as listed in http://www.iana.org/assignments/protocol-numbers.
responder_ip_address	Field deprecated in Version 5.2. Returns null for all queries.
responder_ipaddr	A binary representation of the IP address of the host that responded to the initiator of the aggregated sessions.
responder_port	The port used by the responder in the aggregated sessions.
responder_user_dept	The department of the user who last logged into the host that responded to the initiator of the aggregated sessions.
responder_user_email	The email address of the user who last logged into the host that responded to the initiator of the aggregated sessions.
responder_user_first_name	The first name of the user who last logged into the host that responded to the initiator of the aggregated sessions.
responder_user_id	An internal identification number for the user who last logged into the host that responded to the initiator of the aggregated sessions.
responder_user_last_name	The last name of the user who last logged into the host that responded to the initiator of the aggregated sessions.
responder_user_last_seen_sec	The UNIX timestamp of the date and time the FireSIGHT System last detected user activity for the user who last logged into the host that responded to the initiator of the aggregated sessions.
responder_user_last_updated_sec	The UNIX timestamp of the date and time the FireSIGHT System last updated the user record for the user who last logged into the host that responded to the session initiator.
responder_user_name	The user name of the user who last logged into the host that responded to the initiator of the aggregated sessions.
responder_user_phone	The phone number of the user who last logged into the host that responded to the initiator of the aggregated sessions.
security_zone_egress_name	The egress security zone in the connection event.
security_zone_ingress_name	The ingress security zone in the connection event.

Table 7-4 connection_summary Fields (continued)

Field	Description
sensor_address	The IP address of the managed device that generated the event. Format is *ipv4_address,ipv6_address*.
sensor_name	The name of the managed device that monitored the aggregated sessions.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
source_device	The identification of the source device, which is either: • the IP address of the NetFlow-enabled device that exported the data for the connection • FireSIGHT if the connection was detected by a Cisco managed device
start_time_sec	The UNIX timestamp of the date and time the five-minute interval used to aggregate the sessions in the summary started.

connection_summary Joins

The following table describes the joins you can perform using the **connection_summary** table.

Table 7-5 connection_summary Joins

You can join this table on...	And...
application_protocol_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
initiator_ipaddr or responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

connection_summary Sample Query

The following query returns up to five connection event summary records detected by the selected device.

```
SELECT initiator_ipaddr, responder_ipaddr, protocol_name, application_protocol_id,
source_device, sensor_name, sensor_address, packets_recv, packets_sent, bytes_recv,
bytes_sent, connection_type, num_connections

FROM connection_summary

WHERE sensor_name='linden' limit 5;
```

si_connection_log

The **si_connection_log** table contains information on security intelligence events. The FireSIGHT System generates a Security Intelligence event when a connection is blacklisted or monitored by Security Intelligence; the event contains detailed information about the monitored traffic.

For more information, see the following sections:

- si_connection_log Fields, page 7-16
- si_connection_log Joins, page 7-26
- si_connection_log Sample Query, page 7-26

si_connection_log Fields

The following table describes the database fields you can access in the **si_connection_log** table.

Table 7-6 si_connection_log Fields

Field	Description
access_control_policy_name	The access control policy that contains the access control rule (or default action) that logged the connection.
access_control_policy_UUID	The UUID of the access control policy that contains the access control rule (or default action) that logged the connection.
access_control_reason	The reason that the access control rule logged the connection. One or more of the following: • IP Block • IP Monitor • User Bypass • File Monitor • File Block • Intrusion Monitor • Intrusion Block • File Resume Block • File Resume Allow • File Custom Detection • SSL Block • DNS Block • DNS Monitor • URL Block • URL Monitor • HTTP Injection • Intelligent App Bypass • blank if there is no connection logged
access_control_rule_action	The action associated with the access control rule (or default action): allow, block, and so on.
access_control_rule_id	An internal identification number for the rule.

Table 7-6 si_connection_log Fields (continued)

Field	Description
access_control_rule_name	The access control rule (or default action) that logged the connection.
application_protocol_id	An internal identification number of the application protocol.
application_protocol_name	One of: • the name of the application, if a positive identification can be made • unknown if the system cannot identify the server based on known server fingerprints • pending if the system requires more data • blank if there is no application information in the connection
bytes_recv	The total number of bytes transmitted by the session responder.
bytes_sent	Total number of bytes transmitted by the session initiator.
cert_valid_end_date	The Unix timestamp on which the SSL certificate used in the connection ceases to be valid.
cert_valid_start_date	The Unix timestamp when the SSL certificate used in the connection was issued.
client_application_id	An internal identification number for the client application that was used in the intrusion event.
client_application_name	The client application, if available, that was used in the intrusion event. One of: • the name of the application, if a positive identification can be made • a generic client name if the system detects a client application but cannot identify a specific one • blank if there is no client application information in the connection
client_application_version	The version of the client application.
connection_type	The detection source for the connection information. Either: • rna, if detected by a Cisco device • netflow, if exported by a NetFlow-enabled device
counter	Counter for the intrusion event associated with the connection event.
file_count	The number of files identified by snort in a session. A record is generated for each file identified in the session.
first_packet_sec	The UNIX timestamp of the date and time the first packet of the session was seen.
icmp_code	ICMP code if the event is ICMP traffic, or null if the event was not generated from ICMP traffic.
icmp_type	ICMP type if the event is ICMP traffic, or null if the event was not generated from ICMP traffic.

Table 7-6 si_connection_log Fields (continued)

Field	Description
initiator_continent_name	The name of the continent of the host that initiated the session. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica
initiator_country_id	Code for the country of the host that initiated the session.
initiator_country_name	Name of the country of the host that initiated the session.
initiator_ipaddr	A binary representation of the IP address of the host that initiated the session.
initiator_port	The port used by the session initiator.
initiator_user_dept	The department of the user who last logged into the initiator host.
initiator_user_email	The email address of the user who last logged into the initiator host.
initiator_user_first_name	The first name of the user who last logged into the initiator host.
initiator_user_id	An internal identification number for the user who last logged into the initiator host.
initiator_user_last_name	The last name of the user who last logged into the initiator host.
initiator_user_last_seen_sec	The UNIX timestamp of the date and time the FireSIGHT System last detected user activity for the user who last logged into the initiator host.
initiator_user_last_updated_sec	The UNIX timestamp of the date and time the FireSIGHT System last updated the user record for the user who last logged into the initiator host.
initiator_user_name	The user name of the user who last logged into the initiator host.
initiator_user_phone	The phone number of the user who last logged into the initiator host.
instance_id	Numerical ID of the Snort instance on the managed device that generated the event.
interface_egress_name	The ingress interface associated with the connection.
interface_ingress_name	The egress interface associated with the connection.
ioc_count	Number of indications of compromise found in the connection.
ips_event_count	The number of intrusion events generated in the connection prior to intrusion event thresholding.
last_packet_sec	The UNIX timestamp of the date and time the last packet of the session was seen.
monitor_rule_id_1	The ID of the first monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_1.

Table 7-6 si_connection_log Fields (continued)

Field	Description
monitor_rule_id_2	The ID of the second monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_2.
monitor_rule_id_3	The ID of the third monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_3.
monitor_rule_id_4	The ID of the fourth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_4.
monitor_rule_id_5	The ID of the fifth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_5.
monitor_rule_id_6	The ID of the sixth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_6.
monitor_rule_id_7	The ID of the seventh monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_7.
monitor_rule_id_8	The ID of the eighth monitor rule associated with the connection. This ID is associated with the name stored in monitor_rule_name_8.
monitor_rule_name_1	The name of the first monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_1.
monitor_rule_name_2	The name of the second monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_2.
monitor_rule_name_3	The name of the third monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_3.
monitor_rule_name_4	The name of the fourth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_4.
monitor_rule_name_5	The name of the fifth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_5.
monitor_rule_name_6	The name of the sixth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_6.
monitor_rule_name_7	The name of the seventh monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_7.
monitor_rule_name_8	The name of the eighth monitor rule associated with the connection. This name is associated with the ID stored in monitor_rule_id_8.
netbios_domain	The NetBIOS domain used in the connection.
netflow_dst_as	Netflow autonomous system number of the destination, either origin or peer.
netflow_dst_mask	Netflow destination address prefix mask.
netflow_dst_tos	Type of service from the IP header when packets are flowing from the destination to the source.
netflow_snmp_in	ID of the interface used by packets flowing from the source to the destination.
netflow_snmp_out	ID of the interface used by packets flowing from the destination to the source.
netflow_src_as	Netflow autonomous system number of the source, either origin or peer.

Table 7-6 si_connection_log Fields (continued)

Field	Description
netflow_src_mask	Netflow source address prefix mask.
netflow_src_tos	Type of service from the IP header when packets are flowing from the source to the destination.
network_analysis_policy_name	The network analysis policy associated with the intrusion policy that generated the intrusion event.
network_analysis_policy_UUID	The UUID of the network analysis policy associated with the intrusion policy that generated the intrusion event.
packets_recv	The total number of packets received by the host that initiated the session.
packets_sent	The total number of packets transmitted by the host that initiated the session.
protocol_name	The name of the protocol used in the connection.
protocol_num	The IANA number of the protocol as listed in http://www.iana.org/assignments/protocol-numbers.
responder_continent_name	The name of the continent of the host that responded to the session initiator. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica
responder_country_id	Code for the country of the host that responded to the session initiator.
responder_country_name	Name of the country of the host that responded to the session initiator.
responder_ipaddr	A binary representation of the IPv4 or IPv6 address for the host that responded to the session initiator.
responder_port	The port used by the session responder.
responder_user_dept	The department of the user who last logged into the host that responded to the session initiator.
responder_user_email	The email address of the user who last logged into the host that responded to the session initiator.
responder_user_first_name	The first name of the user who last logged into the host that responded to the session initiator.
responder_user_id	An internal identification number for the user who last logged into the host that responded to the session initiator.
responder_user_last_name	The last name of the user who last logged into the host that responded to the session initiator.

Table 7-6 si_connection_log Fields (continued)

Field	Description
responder_user_last_seen_sec	The UNIX timestamp of the date and time the FireSIGHT System last detected user activity for the user who last logged into the host that responded to the session initiator.
responder_user_last_updated_sec	The UNIX timestamp of the date and time the FireSIGHT System last updated the user record for the user who last logged into the host that responded to the session initiator.
responder_user_name	The user name of the user who last logged into the host that responded to the session initiator.
responder_user_phone	The phone number of the user who last logged into the host that responded to the session initiator.
security_context	Description of the security context (virtual firewall) that the traffic passed through. Note that the system only populates this field for ASA FirePOWER devices in multi-context mode.
security_intelligence_category	The Security Intelligence category associated with the connection.
security_intelligence_ip	Whether the Security Intelligence-monitored IP address associated with the connection is a source IP (`src`) or destination IP (`dst`).
security_zone_egress_name	The egress security zone in the connection event.
security_zone_ingress_name	The ingress security zone in the connection event.
sensor_address	The IP address of the managed device that generated the event. Format is `ipv4 address,ipv6 address`.
sensor_name	The name of the managed device that monitored the session.
sensor_uuid	A unique identifier for the managed device, or `0` if `sensor_name` is `null`.
src_device_ipaddr	Either: • A binary representation of the IP address of the NetFlow-enabled device that exported the connection data • `0`, for connections detected by Cisco managed devices.
ssl_actual_action	The action performed on the connection based on the SSL Rule. This may differ from the expected action, as the action as specified in the rule may be impossible. Possible values include: • `'Unknown'` • `'Do Not Decrypt'` • `'Block'` • `'Block With Reset'` • `'Decrypt (Known Key)'` • `'Decrypt (Replace Key)'` • `'Decrypt (Resign)'`

Table 7-6 si_connection_log Fields (continued)

Field	Description
ssl_cipher_suite	Encryption suite used by the SSL connection. The value is stored in decimal format. See www.iana.org/assignments/tls-parameters/tls-parameters.xhtml for the cipher suite designated by the value.
ssl_expected_action	The action which should be performed on the connection based on the SSL Rule. Possible values include: • 'Unknown' • 'Do Not Decrypt' • 'Block' • 'Block With Reset' • 'Decrypt (Known Key)' • 'Decrypt (Replace Key)' • 'Decrypt (Resign)'
ssl_flow_flags	The debugging level flags for an encrypted connection. Possible values include: • 0x00000001 — NSE_FLOW__VALID — must be set for other fields to be valid • 0x00000002 — NSE_FLOW__INITIALIZED — internal structures ready for processing • 0x00000004 — NSE_FLOW__INTERCEPT — SSL session has been intercepted

Table 7-6 si_connection_log Fields (continued)

Field	Description
ssl_flow_messages	The messages exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information. • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER

Table 7-6 si_connection_log Fields (continued)

Field	Description
ssl_flow_status	Status of the SSL Flow. These values describe the reason behind the action taken or the error message seen. Possible values include: • 'Unknown' • 'No Match' • 'Success' • 'Uncached Session' • 'Unknown Cipher Suite' • 'Unsupported Cipher Suite' • 'Unsupported SSL Version' • 'SSL Compression Used' • 'Session Undecryptable in Passive Mode' • 'Handshake Error' • 'Decryption Error' • 'Pending Server Name Category Lookup' • 'Pending Common Name Category Lookup' • 'Internal Error' • 'Network Parameters Unavailable' • 'Invalid Server Certificate Handle' • 'Server Certificate Fingerprint Unavailable' • 'Cannot Cache Subject DN' • 'Cannot Cache Issuer DN' • 'Unknown SSL Version' • 'External Certificate List Unavailable' • 'External Certificate Fingerprint Unavailable' • 'Internal Certificate List Invalid' • 'Internal Certificate List Unavailable' • 'Internal Certificate Unavailable' • 'Internal Certificate Fingerprint Unavailable' • 'Server Certificate Validation Unavailable' • 'Server Certificate Validation Failure' • 'Invalid Action'
ssl_issuer_common_name	Issuer Common name from the SSL certificate. This is typically the host and domain name of the certificate issuer, but may contain other information.
ssl_issuer_country	The country of the SSL certificate issuer.

Table 7-6 si_connection_log Fields (continued)

Field	Description
ssl_issuer_organization	The organization of the SSL certificate issuer.
ssl_issuer_organization_unit	The organizational unit of the SSL certificate issuer.
ssl_policy_action	The default action configured for the policy when no rules match.
ssl_policy_name	ID number of the SSL policy that handled the connection.
ssl_policy_reason	The reason the SSL policy logged the SSL session.
ssl_rule_action	The action selected in the user interface for the SSL rule (`allow`, `block`, and so forth).
ssl_rule_name	ID number of the SSL rule or default action that handled the connection.
ssl_serial_number	The serial number of the SSL certificate, assigned by the issuing CA.
ssl_server_name	Name provided in the server name indication in the SSL Client Hello.
ssl_subject_common_name	Subject Common name from the SSL certificate. This is typically the host and domain name of the certificate subject, but may contain other information.
ssl_subject_country	The country of the SSL certificate subject.
ssl_subject_organization	The organization of the SSL certificate subject.
ssl_subject_organization_unit	The organizational unit of the SSL certificate subject.
ssl_url_category	Category of the flow as identified from the server name and certificate common name.
ssl_version	The SSL or TLS protocol version used to encrypt the connection.
tcp_flags	The TCP flags detected in the session.
url	The URL requested by the monitored host during the session, if available.
url_category	The category of the URL requested by the monitored host.
url_reputation	The reputation of the URL requested by the monitored host. One of the following: • `1` — High risk • `2` — Suspicious sites • `3` — Benign sites with security risks • `4` — Benign sites • `5` — Well known
web_application_id	An internal identification number for the web application.
web_application_name	One of: • the name of the application, if a positive identification can be made. • `web browsing` if the system detects an application protocol of HTTP but cannot identify a specific web application. • blank if the connection has no HTTP traffic.

si_connection_log Joins

The following table describes the joins you can perform using the **si_connection_log** table.

Table 7-7 si_connection_log Joins

You can join this table on...	And...
application_protocol_name or application_id or client_application_id or web_application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
initiator_ipaddr or responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

si_connection_log Sample Query

The following query returns up to 25 connection event records from the **si_connection_log** table, sorted in descending order based on packet timestamps.

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation

FROM si_connection_log

WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY
first_packet_sec

DESC, last_packet_sec DESC LIMIT 0, 25;
```