Schema: Intrusion Tables

This chapter contains information on the schema and supported joins for intrusion events, the packets that triggered the events, and the associated rule messages.

For more information, see the sections listed in the following table.

Table 4-1 Schema for Intrusion Tables

See...	For the table that stores information on...	Version
intrusion_event, page 4-1	Intrusion events, which include the date, time, type of exploit, and contextual information about the source and target of an attack.	4.10.x+
intrusion_event_packet, page 4-7	The content of the packet or packets that triggered an intrusion event.	4.10.x+
rule_message, page 4-8	Rule messages for intrusion events, including the associated generator ID (GID), signature ID (SID), and version data.	4.10.x+
rule_documentation, page 4-9	Information on rules, including the attack scenarios, affected systems, and information on when the rule was created and by whom.	5.2+

intrusion_event

The **`intrusion_event`** table contains information on possible intrusions identified by the FireSIGHT System. For each possible intrusion, the system generates an event and an associated record in the database, which contains the date, time, type of exploit, access control policy and rule, intrusion policy and rule, and other contextual information about the source and target of the attack.

Tip For packet-based events, a copy of the packet or packets that triggered the event may also be available; see intrusion_event_packet Sample Query, page 4-8.

For more information, see the following sections:

- `intrusion_event Fields, page 4-2`
- `intrusion_event Joins, page 4-6`
- `intrusion_event Sample Query, page 4-7`

intrusion_event Fields

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

Table 4-2 intrusion_event Fields

Field	Description
`access_control_policy_name`	The access control policy associated with the intrusion policy that generated the intrusion event. Note that the access control policy name and access control rule name combination is unique for a Defense Center.
`access_control_policy_UUID`	The UUID of the access control policy associated with the intrusion policy that generated the intrusion event.
`access_control_rule_id`	The internal identification number of the access control rule associated with the intrusion policy that generated the intrusion event.
`access_control_rule_name`	The name of the access control rule associated with the intrusion policy that generated the intrusion event. Note that the access control rule name is unique within a policy but not across different policies.
`application_protocol_id`	The internal identification number of the application protocol.
`application_protocol_name`	One of: • the name of the application, if a positive identification can be made • `pending` if the system requires more data • blank if there is no application information in the connection
`blocked`	The value indicating what happened to the packet that triggered the intrusion event: • `0` — Packet not dropped • `1` — Packet dropped (inline, switched, or routed deployment) • `2` — Packet that triggered the event would have been dropped, if the intrusion policy had been applied to a device configured in inline, switched, or routed deployment
`client_application_id`	The internal identification number of 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. • `null` if there is no application information in the connection
`connection_sec`	UNIX timestamp (seconds since 00:00:00 01/01/1970) of the connection event associated with the intrusion event.
`counter`	Number that is incremented for each connection event in a given second, and is used to differentiate among multiple connection events that happen during the same second.
`detection_engine_name`	Field deprecated in Version 5.0. Returns `null` for all queries.
`detection_engine_uuid`	Field deprecated in Version 5.0. Returns `null` for all queries.

Table 4-2 intrusion_event Fields (continued)

Field	Description
dst_continent_name	The name of the continent of the destination host. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica
dst_country_id	Code for the country of the destination host.
dst_country_name	Name of the country of the destination host.
dst_ip_address	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.
dst_ip_address_v6	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.
dst_ipaddr	A binary representation of the IPv4 or IPv6 address for the destination host involved in the triggering event.
dst_port	Either: • the destination port number, if the event protocol type is TCP or UDP • the ICMP code, if the event protocol type is ICMP
dst_user_dept	The department of the destination user.
dst_user_email	The email address of the destination user.
dst_user_first_name	The first name of the destination user.
dst_user_id	The internal identification number for the destination user; that is, the user who last logged into the destination host before the intrusion event occurred.
dst_user_last_name	The last name of the destination user.
dst_user_last_seen_sec	The UNIX timestamp of the date and time when the system last reported a login for the destination user.
dst_user_last_updated_sec	The UNIX timestamp of the date and time when the system last updated the destination user's record.
dst_user_name	The user name for the destination user.
dst_user_phone	The telephone number for the destination user.
event_id	The internal identification number for the event. Uniquely identifies an event on the Defense Center.
event_time_sec	The UNIX timestamp of the date and time when the event packet was captured.
event_time_usec	The microsecond increment of the event timestamp. If microsecond resolution is not available, this value is 0.

Table 4-2 intrusion_event Fields (continued)

Field	Description
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.
impact	The impact flag value of the event. Integer values are: • 1 — Red (vulnerable) • 2 — Orange (potentially vulnerable) • 3 — Yellow (currently not vulnerable) • 4 — Blue (unknown target) • 5 — Gray (unknown impact)
instance_id	Numerical ID of the Snort instance on the managed device that generated the event.
interface_egress_name	The name of the interface for the outbound traffic.
interface_ingress_name	The name of the interface for the inbound traffic.
intrusion_event_policy_uuid	A unique identifier for the intrusion policy that triggered the intrusion event.
intrusion_event_policy_name	The intrusion policy that generated the intrusion event.
ioc_count	Number of indications of compromise found in the event.
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.
priority	The priority for the rule classification associated with the event. Rule priority is set in the user interface.
protocol_name	The text name of the traffic protocol associated with the intrusion event.
protocol_num	The IANA number of the protocol as listed in http://www.iana.org/assignments/protocol-numbers.
reviewed	Whether the intrusion event has been marked as reviewed: • 1 — Reviewed • 0 — Not reviewed
rule_classification	The description of the rule classification associated with the intrusion event, which usually describes the attack detected by the rule that triggered the event. For example: A Network Trojan was Detected.
rule_classification_id	The identification number for the rule classification associated with the intrusion event.
rule_generator	The component that generated the intrusion event. The generator can be either a rules engine, decoder, or preprocessor.
rule_generator_id	The generator ID (GID) of the component named in rule_generator that generated the intrusion event.

Table 4-2 intrusion_event Fields (continued)

Field	Description
rule_message	Explanatory text for the event. For rule-based intrusion events, the message is generated from the rule. For decoder- and preprocessor-based events, the message is hard coded.
rule_revision	The revision number of the rule associated with the intrusion event.
rule_signature_id	The signature ID (SID) for the intrusion event. Identifies the specific rule, decoder message, or preprocessor message that caused the event to be generated.
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_zone_egress_name	The egress security zone in the intrusion event that triggered the policy violation.
security_zone_ingress_name	The ingress security zone in the intrusion event that triggered the policy violation.
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 generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
src_continent_name	The name of the continent of the destination host. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica
src_country_id	Code for the country of the destination host.
src_country_name	Name of the country of the destination host.
src_ip_address	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_ip_address_v6	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_ipaddr	A binary representation of the IPv4 or IPv6 address for the source host involved in the triggering event.
src_port	Either: • the source port number, if the event protocol type is TCP or UDP • the ICMP type, if the event protocol type is ICMP
src_user_dept	The department of the source user.
src_user_email	The email address for the source user.
src_user_first_name	The first name of the source user.

Table 4-2 intrusion_event Fields (continued)

Field	Description
src_user_id	The internal identification number for the source user; that is, the user who last logged into the source host before the intrusion event occurred.
src_user_last_name	The last name of the source user.
src_user_last_seen_sec	The UNIX timestamp of the date and time the system last reported a login for the source user.
src_user_last_updated_sec	The UNIX timestamp of the date and time the source user's record was last updated.
src_user_name	The user name for the source user.
src_user_phone	The source user's phone number.
vlan_id	The identification number of the innermost VLAN associated with the packet that triggered the intrusion event.
web_application_id	The internal identification number of the web application that was used in the intrusion event, if applicable.
web_application_name	The web application that was used in the intrusion event, if applicable. 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

intrusion_event Joins

The following table describes the joins you can perform on the **intrusion_event** table.

Table 4-3 intrusion_event 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
dst_ipaddr or src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

intrusion_event Sample Query

The following query returns the 25 most common unreviewed intrusion event results, sorted in descending order based on `Count`.

```
SELECT rule_message, priority, rule_classification, count(*) as Count

FROM intrusion_event

WHERE reviewed="0"

GROUP BY rule_message, priority, rule_classification

ORDER BY Count DESCLIMIT 0, 25;
```

intrusion_event_packet

The **`intrusion_event_packet`** table contains information on content of the packet or packets that triggered an intrusion event. Keep in mind if you prohibited packet transfer from your managed devices to the Defense Center, the **`intrusion_event_packet`** table contains no data.

For more information, see the following sections:

- intrusion_event_packet Fields, page 4-7
- intrusion_event_packet Joins, page 4-8
- intrusion_event_packet Sample Query, page 4-8

intrusion_event_packet Fields

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

Table 4-4 intrusion_event_packet Fields

Field	Description
`detection_engine_name`	Field deprecated in Version 5.0. Returns `null` for all queries.
`detection_engine_uuid`	Field deprecated in Version 5.0. Returns `null` for all queries.
`event_id`	The identification number for the event. The ID is unique on a given managed device.
`linktype`	An internal key that indicates the format of the packet's outer layer; used by the managed device to correctly decode the packet. Only link type `1` is supported.
`packet_data`	The contents of the packet that triggered the event.
`packet_time_sec`	The UNIX timestamp of the date and time the event packet was captured.
`packet_time_usec`	The microsecond increment of the event timestamp. If microsecond resolution is not available, this value is `0`.
`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 generated the intrusion event.
`sensor_uuid`	A unique identifier for the managed device, or `0` if `sensor_name` is `null`.

intrusion_event_packet Joins

You cannot perform joins on the **intrusion_event_packet** table.

intrusion_event_packet Sample Query

The following query returns the packet information for all packets matching the selected event ID.

```
SELECT event_id, packet_time_sec, sensor_address, packet_data
FROM intrusion_event_packet
WHERE event_id="1";
```

rule_message

The **rule_message** table is a master list of the rule messages for intrusion rules. Each rule message is accompanied by its identifying information.

For more information, see the following sections:

- rule_message Fields, page 4-8
- rule_message Joins, page 4-8
- rule_message Sample Query, page 4-9

rule_message Fields

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

Table 4-5 rule_message Fields

Field	Description
generator_id	The GID of the component that triggers the rule.
message	The message associated with the rule that is triggered.
rev_uuid	A unique identifier for the rule revision.
revision	The revision number for the rule.
signature_id	The rule identification number as it is rendered in the appliance user interface.
uuid	A unique identifier for the rule.

rule_message Joins

You cannot perform joins on the **rule_message** table.

rule_message Sample Query

The following query returns the intrusion rule message for the intrusion rule that has a GID of `1` and a SID of `1200`.

```
SELECT generator_id, signature_id, revision, message

FROM rule_message

WHERE generator_id="1"

AND signature_id="1200";
```

rule_documentation

The **`rule_documentation`** table contains information about rules used to generate alerts.

For more information, see the following sections:

- rule_documentation Fields, page 4-9
- rule_documentation Joins, page 4-10
- rule_documentation Sample Query, page 4-10

rule_documentation Fields

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

Table 4-6 rule_documentation Fields

Field	Description
`additional_references`	Additional information and references.
`affected_systems`	Systems affected by the vulnerability.
`attack_scenarios`	Examples of possible attacks.
`contributors`	Contact information for the author of the rule and other relevant documentation.
`corrective_action`	Information regarding patches, upgrades, or other means to remove or mitigate the vulnerability.
`detailed_information`	Information regarding the underlying vulnerability, what the rule actually looks for, and what systems are affected.
`ease_of_attack`	Whether the attack is considered simple, medium, hard, or difficult, and whether or not it can be performed using a script.
`false_negatives`	Examples that may result in a false negative. The default value is `None Known`.
`false_positives`	Examples that may result in a false positive. The default value is `None Known`.
`impact`	How a compromise that uses this vulnerability may impact various systems.
`rule_revision`	Rule revision number.
`rule_signature_id`	Rule identification number that corresponds with the event.
`summary`	Explanation of the threat or vulnerability.
`updated`	The UNIX timestamp of the date and time the rule was last updated.

rule_documentation Joins

You cannot perform joins on the **rule_documentation** table.

rule_documentation Sample Query

The following query returns the attack scenarios, corrective action, impact, and summary for the intrusion rule that has an ID of 1.

```
SELECT attack_scenarios, corrective_action, impact, summary

FROM rule_documentation

WHERE rule_signature_id="1";
```