CHAPTER 5

Schema: Statistics Tracking Tables

This chapter contains information on the schema and supported joins for application and URL statistics tracking tables. These tables collect statistical information on:

- access control and intrusion events by application and by user
- bandwidth usage and connection decisions by application and by user
- bandwidth usage and connection decisions by URL reputation (risk) and by URL business relevance

For links to details on each table, see the following table.

Table 5-1 Application and URL Statistics Tables

See	For the table that stores statistics on...	Version
app_ids_stats_current_timeframe, page 5-4	Access control and intrusion protection activity, by application and a range of application attributes.	5.0+
app_stats_current_timeframe, page 5-6	Traffic volume and system access control activity (connections allowed or denied), by application and a range of application attributes.	5.0+
geolocation_stats_current_timeframe, page 5-7	Access control activity by location.	5.2+
ids_impact_stats_current_timeframe, page 5-9	Statistics for intrusion events (connections blocked and would have dropped) by impact levels.	5.1.1+
session_stats_current_timeframe, page 5-10	Contain statistics for all connections. Statistics can be extracted based on bytes, connection, sensor, and time.	5.2+
ssl_stats_current_timeframe, page 5-11	Contain statistics for SSL connections. Statistics can be extracted based on bytes, connection, sensor, and time.	5.4+
storage_stats_by_disposition_current_timeframe, page 5-14	Contain statistics for files based on disposition. Statistics can be extracted based on bytes, disposition, sensor, and time.	5.3+
storage_stats_by_file_type_current_timeframe, page 5-15	Contain statistics for files based on file type. Statistics can be extracted based on bytes, file type, sensor, and time.	5.3+
transmission_stats_by_file_type_current_timeframe, page 5-16	Contain statistics for connections based on file type. Statistics can be extracted based on bytes, connection, file type, sensor, and time.	5.3+
url_category_stats_current_timeframe, page 5-17	Traffic volume and system access control activity (connections allowed or denied), by the category of the requested website.	5.0+

Table 5-1 Application and URL Statistics Tables (continued)

See	For the table that stores statistics on...	Version
url_reputation_stats_current_timeframe, page 5-19	Traffic volume and system access control activity (connections allowed or denied), by the reputation of the requested website.	5.0+
user_ids_stats_current_timeframe, page 5-20	Access control and intrusion protection activity, by user.	5.0+
user_stats_current_timeframe, page 5-21	Traffic volume and system access control activity (connections allowed or denied), by user.	5.0+

Understanding Statistics Tracking Tables

A table's name ends with **current_day**, **current_month**, or **current_year** to indicate the timeframe of its data. For example, the **app_ids_stats_current_***timeframe* describes **app_stats_current_day**, **app_stats_current_month**, and **app_stats_current_year**. The **app_stats_current_year** table stores statistics for 360 days; the **current_month** table stores statistics for 30 days.

Each time the Defense Center receives raw counts from managed devices in your network, it updates all three table types, but does so at successively coarser resolution. The **current_day** table has the finest resolution (15 seconds or 5 minutes, depending on the particular table); the **current_year** table has the coarsest resolution (24 hours). See Storage Characteristics for Statistics Tracking Tables, page 5-2 for specific information.

Storage Characteristics for Statistics Tracking Tables

See the following table for important details.

Table 5-2 Storage Characteristics of Statistics Tables

Table Type	Interval (Resolution)	Storage Lifespan
current_day	15 seconds for **app_ids_stats_current_***timeframe* and **user_ids_stats_current_***timeframe*	current interval plus all intervals in the preceding 24 hours
	5 minutes for **app_stats_current_***timeframe*, **user_stats_current_***timeframe*, **url_category_stats_current_***timeframe*, and **url_reputation_stats_current_***timeframe*	current interval plus all intervals in the preceding 24 hours
current_month	one hour	current hour plus the hours stretching back 30 days
current_year	24 hours	current day plus the preceding 360 days

A storage interval is defined by its start time. For example, the **current_month** table contains counts for the hour 10:00:00 - 10:59:59 as one record with a timestamp of 10:00:00. Note that a day begins at 00:00:00 and ends at 23:59:59. Interval start times are stored as UNIX timestamps (GMT).

Specifying Time Intervals When Querying Statistics Tables

The effective time interval for a query is defined by both the table and the `time_start_sec` field in the query.

For example, if your SQL statement specifies `time_start_sec` = `6:00:00`, the interval varies for each table type:

- for **`current_day`** tables: either `6:00:00` to `6:00:14` (for 15 second tables) or `6:00:00` to `6:04:59` (for 5 minute tables).
- for **`current_month`** tables: `6:00:00` to `6:59:59`.
- for **`current_year`** tables: `0:00:00` to `23:59:59` on the following day.

The simplest way to retrieve data is to state the interval start time. For example, to retrieve from the **`app_ids_stats_current_day`** table, specify one of the following:

```
00:00:00
00:00:15
00:00:30
23:59:45
```

If your query contains a timestamp that is other than an interval start time, the system modifies the request as follows:

- rounds up the start time to the nearest interval time
- rounds down the end time to the nearest interval time

For example, the following query rounds up the start time:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 12:30:00");
```

and is the same as:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 01:00:00");
```

When querying a range of intervals, the starting time interval is rounded up, and the ending time interval is rounded down. For example:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 12:59:00") and
UNIX_TIMESTAMP("2011-12-10 16:28:00");
```

is changed to:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 13:00:00") and
UNIX_TIMESTAMP("2011-12-12 16:00:00");
```

If your query interval extends beyond a table's time frame, you can usually obtain the additional data from another table, although the data in the other table will have a coarser resolution. For example, to retrieve bandwidth usage for the past two days, you can get results for yesterday from the **`current_day`** table (at 5 minute resolution), but you can get statistics for the previous day only from **`current_month`** (in hour chunks) or **`current_year`** (in day chunks).

app_ids_stats_current_timeframe

The **app_ids_stats_current_***timeframe* tables contain statistics about application activity and intrusion events on your monitored network. Statistics can be extracted per detected application, per application type (application protocol, client application, or web application), and also per risk and business relevance of the application. The tables also track blocked connections due to intrusion policy violations and the estimated potential impact of an intrusion.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **app_ids_stats_current_***timeframe* tables, see the following sections:

- app_ids_stats_current_timeframe Fields, page 5-4
- app_ids_stats_current_timeframe Joins, page 5-5
- app_ids_stats_current_timeframe Sample Query, page 5-5

app_ids_stats_current_timeframe Fields

The following table describes the fields you can access in the **app_ids_stats_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-3 app_ids_stats_current_timeframe Fields

Field	Description
application_id	The internal identification number for the application.
application_name	The application name that appears in the user interface.
blocked	Number of connections blocked due to violation of an intrusion policy.
business_relevance	An index (from 1 to 5) of the application's relevance to business productivity where 1 is very low and 5 is very high.
business_relevance_description	A description of business relevance (very low, low, medium, high, very high).
impact_level_1	The number of impact level 1 (vulnerable) intrusion events recorded for the application.
impact_level_2	The number of impact level 2 (potentially vulnerable) intrusion events.
impact_level_3	The number of impact level 3 (host currently not vulnerable) intrusion events.
impact_level_4	The number of impact level 4 (unknown target) intrusion events.
impact_level_5	The number of impact level 5 (unknown vulnerability) intrusion events.
is_client_application	A true-false flag that indicates if the detected application is a client application.
is_server_application	A true-false flag that indicates if the detected application is an application protocol.
is_web_application	A true-false flag that indicates if the detected application is a web application.
risk	An index (from 1 to 5) of the application's estimated risk where 1 is very low risk and 5 is critical risk.

Table 5-3 app_ids_stats_current_timeframe Fields (continued)

Field	Description
risk_description	A description of the estimated risk (very low, low, medium, high, critical).
sensor_address	The IP address of the managed device that generated the event. Format is *ipv4_address,ipv6_address*.
sensor_id	ID of the device that provided the event.
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.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
would_have_dropped	Number of packets that would have been dropped if the intrusion policy had been configured to drop packets in an inline deployment.

app_ids_stats_current_timeframe Joins

The following table describes the joins you can perform on the **app_ids_stats_current_***timeframe* tables.

Table 5-4 app_ids_stats_current_timeframe Joins

You can join this table on...	And...
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

app_ids_stats_current_timeframe Sample Query

The following query returns up to 25 application records from the **app_ids_stats_current_month** table. Each record contains the number of blocked connections and intrusion events for the application over the time interval.

```
SELECT from_unixtime(start_time_sec), sum(blocked)

FROM app_ids_stats_current_day

WHERE start_time_sec = unix_timestamp("2013-12-15");
```

app_stats_current_timeframe

The **app_stats_current_***timeframe* tables contain statistics on bandwidth usage and access control actions (connection allowed or denied), by application and by device that monitored the traffic. You can filter these statistics by the business relevance, estimated risk, and type of the application.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **app_stats_current_***timeframe* tables, see the following sections:

- app_stats_current_timeframe Fields, page 5-6
- app_stats_current_timeframe Joins, page 5-7
- app_stats_current_timeframe Sample Query, page 5-7

app_stats_current_timeframe Fields

The following table describes the fields you can access in the **app_stats_current_***timeframe* tables.

Table 5-5 app_stats_current_timeframe Fields

Field	Description
application_id	The internal identification number for the application.
application_name	The application name that appears in the user interface.
business_relevance	An index (from 1 to 5) of the application's relevance to business productivity where 1 is very low and 5 is very high.
business_relevance_description	A description of business relevance (very low, low, medium, high, very high).
bytes_in	The bytes of inbound traffic for the application during the specified interval.
bytes_out	The bytes of outbound traffic for the application during the specified interval.
connections_allowed	The number of connections allowed.
connections_denied	The number of connections denied due to violation of an access control policy.
is_client_application	A true-false flag that indicates if the detected application is a client application.
is_server_application	A true-false flag that indicates if the detected application is an application protocol.
is_web_application	A true-false flag that indicates if the detected application is a web application.
risk	An index (from 1 to 5) of the application's estimated risk where 1 is very low risk and 5 is critical risk.
risk_description	A description of the estimated risk (very low, low, medium, high, critical).
sensor_address	The IP address of the managed device that monitored the traffic. Format is *ipv4_address,ipv6_address*.
sensor_id	The internal identification number of the managed device that detected the traffic.

Table 5-5 app_stats_current_timeframe Fields (continued)

Field	Description
sensor_name	The name of the managed device that detected the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

app_stats_current_timeframe Joins

The following table describes the joins you can perform on the **app_stats_current_***timeframe* tables.

Table 5-6 app_stats_current_timeframe Joins

You can join this table on...	And...
application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service.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

app_stats_current_timeframe Sample Query

The following query returns the inbound and outbound traffic load associated with applications that have low business relevance and high risk in the period of a day, for all managed devices connected to the Defense Center.

```
SELECT start_time_sec, sum(bytes_in), sum(bytes_out)

FROM app_stats_current_day

WHERE business_relevance <= 2

AND risk >= 4 AND start_time_sec = unix_timestamp("2013-12-15");
```

geolocation_stats_current_timeframe

The **geolocation_stats_***timeframe* tables contain statistics regarding intrusion events based on location levels. Statistics can be extracted based on impact level, device, and how the packets are handled.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **geolocation_stats_current_***timeframe* tables, see the following sections:

- geolocation_stats_current_timeframe Fields, page 5-8

- geolocation_stats_current_timeframe Joins, page 5-9
- geolocation_stats_current_timeframe Sample Query, page 5-9

geolocation_stats_current_timeframe Fields

The following table describes the fields you can access in the **geolocation_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-7 geolocation_stats_current_timeframe Fields

Field	Description
bytes_from	The total number of bytes transmitted by the session responder.
bytes_to	Total number of bytes transmitted by the session initiator.
destination_continent	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
destination_country	Code for the country of the destination host.
flows_allowed	The number of flows allowed.
flows_denied	The number of flows denied due to violation of an access control policy.
sensor_address	The IP address of the managed device that generated the event. Format is *ipv4_address,ipv6_address*.
sensor_id	ID of the device that provided the event.
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.
source_continent	The name of the continent of the source host. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica

Table 5-7 geolocation_stats_current_timeframe Fields (continued)

Field	Description
`source_country`	Code for the country of the source host.
`start_time_sec`	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

geolocation_stats_current_timeframe Joins

You cannot perform joins on the **geolocation_stats_current**_*timeframe* tables.

geolocation_stats_current_timeframe Sample Query

The following query returns source country and sensor name for the first 25 connection events from Asia during the current day.

```
SELECT sensor_name, source_continent

FROM geolocation_stats_current_year

WHERE destination_continent='as'

LIMIT 20;
```

ids_impact_stats_current_timeframe

The **ids_impact_stats**_*timeframe* tables contain statistics regarding intrusion events based on impact levels. Statistics can be extracted based on impact level, device, and how the packets are handled.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **ids_impact_stats_current**_*timeframe* tables, see the following sections:

- ids_impact_stats_current_timeframe Fields, page 5-9
- ids_impact_stats_current_timeframe Joins, page 5-10
- ids_impact_stats_current_timeframe Sample Query, page 5-10

ids_impact_stats_current_timeframe Fields

The following table describes the fields you can access in the **ids_impact_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-8 ids_impact_stats_current_timeframe Fields

Field	Description
blocked	Number of connections blocked due to violation of an intrusion policy.
impact_level_1	The number of impact level 1 (vulnerable) intrusion events recorded for the application.
impact_level_2	The number of impact level 2 (potentially vulnerable) intrusion events.
impact_level_3	The number of impact level 3 (host currently not vulnerable) intrusion events.
impact_level_4	The number of impact level 4 (unknown target) intrusion events.
impact_level_5	The number of impact level 5 (unknown vulnerability) intrusion events.
sensor_address	The IP address of the managed device that generated the event. Format is *ipv4_address,ipv6_address*.
sensor_id	ID of the device that provided the event.
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.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
would_have_dropped	Number of packets that would have been dropped if the intrusion policy had been set to drop packets in an inline deployment.

ids_impact_stats_current_timeframe Joins

You cannot perform joins on the **ids_impact_stats_current_***timeframe* tables.

ids_impact_stats_current_timeframe Sample Query

The following query returns the first 25 blocked and would_have_dropped events during the current day.

```
SELECT blocked, would_have_dropped

FROM ids_impact_stats_current_year

LIMIT 25;
```

session_stats_current_timeframe

The **session_stats_***timeframe* tables contain statistics for all connections. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **session_stats_current_***timeframe* tables, see the following sections:

- session_stats_current_timeframe Fields, page 5-11

- session_stats_current_timeframe Joins, page 5-11
- session_stats_current_timeframe Sample Query, page 5-11

session_stats_current_timeframe Fields

The following table describes the fields you can access in the **session_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-9 session_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
connections_allowed	The number of connections allowed for the specified URL category.
connections_denied	The number of connections denied for the specified URL category due to violation of an access control policy.
id	This field is not used and will always return 0.
sensor_address	The IP address of the managed device that generated the event. Format is *ipv4_address,ipv6_address*.
sensor_id	ID of the device that provided the event.
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.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

session_stats_current_timeframe Joins

You cannot perform joins on the **session_stats_current**_*timeframe* tables.

session_stats_current_timeframe Sample Query

The following query returns the number of denied and allowed connections for each sensor, in descending order by sensor_name during the current day.

```
SELECT sensor_name, connections_denied, connections_allowed

FROM session_stats_current_day

ORDER BY sensor_id DESC;
```

ssl_stats_current_timeframe

The **ssl_stats_current**_*timeframe* tables contain statistics for SSL connections. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **ssl_stats_current_***timeframe* tables, see the following sections:

- ssl_stats_current_timeframe Fields, page 5-12
- ssl_stats_current_timeframe Joins, page 5-13
- ssl_stats_current_timeframe Sample Query, page 5-14

ssl_stats_current_timeframe Fields

The following table describes the fields you can access in the **ssl_stats_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-10 ssl_stats_current_timeframe Fields

Field	Description
block	Number of SSL sessions dropped with no reset.
block_with_reset	Number of SSL sessions dropped with reset.
cached_session	Number of SSL sessions found in the session cache.
cannot_determine_verdict	Number of handshake errors that occurred while evaluating SSL rules.
cert_expired	Number of SSL sessions in which the certificate was expired.
cert_invalid_issuer	Number of SSL sessions in which the certificate issuer was either not valid or not found in the Trusted CA list.
cert_invalid_signature	Number of SSL sessions in which the certificate had an invalid signature.
cert_not_checked	Number of SSL sessions in which the certificate was not checked.
cert_not_yet_valid	Number of SSL sessions in which the certificate was not yet valid.
cert_revoked	Number of SSL sessions in which the certificate had been revoked.
cert_self_signed	Number of SSL sessions in which the certificate was self-signed.
cert_unknown	Number of SSL sessions in which the certificate status was unknown.
cert_valid	Number of SSL sessions in which the certificate was valid.
cert_validation_cache_hit	Number of times a certificate was found in the validation cache.
cert_validation_cache_miss	Number of times a certificate was not found in the validation cache.
decrypt_resign_self_signed	Number of times an SSL session using a self-signed certificate was decrypted using the decrypt-resign method.
decrypt_resign_self_signed_replace_key_only	Number of times an SSL session using a self-signed certificate was decrypted using the decrypt-resign with replace key only method.
decrypt_resign_signed_cert	Number of times an SSL session using a signed certificate was decrypted using the decrypt-resign method.
decrypt_with_known_key	Number of times an SSL session was decrypted using the known-key method.
decryption_error	Number of SSL sessions which suffered an error during decryption.
do_not_decrypt	Number of times an SSL session was found but not decrypted.
handshake_error	Number of handshake errors that occurred prior to evaluating SSL rules.

Table 5-10 ssl_stats_current_timeframe Fields (continued)

Field	Description
`orig_cert_cache_hit`	Number of times an original certificate was found in the cache.
`orig_cert_cache_miss`	Number of times an original certificate was not found in the cache.
`resigned_cert_cache_hit`	Number of times a resigned certificate was found in the cache.
`resigned_cert_cache_miss`	Number of times a resigned certificate was not found in the cache.
`sensor_address`	The IP address of the managed device that generated the event. Format is *`ipv4_address,ipv6_address`*.
`sensor_id`	ID of the device that provided the event.
`sensor_name`	The name of the managed device that generated the event.
`sensor_uuid`	A unique identifier for the managed device, or `0` if `sensor_name` is `null`.
`session_cache_hit`	Number of times an SSL session ID or ticket was found in the cache.
`session_cache_miss`	Number of times an SSL session ID or ticket was not found in the cache.
`session_incorrectly_identified_as_ssl`	Number of sessions that were incorrectly identified as using SSL.
`ssl_compression`	Number of sessions that used SSL compression.
`ssl_sessions_decrypted`	Number of SSL sessions that were successfully decrypted.
`ssl_sessions_not_decrypted`	Number of SSL sessions that were not successfully decrypted.
`ssl_sessions_reused_by_id`	Number of times an SSL session reused an ID.
`ssl_sessions_reused_by_ticket`	Number of times an SSL session reused a ticket.
`ssl_sessions_with_errors`	Number of SSL sessions which have errors.
`ssl_v20`	Number of SSL sessions using SSL version 2.0
`ssl_v30`	Number of SSL sessions using SSL version 3.0
`ssl_version_unknown`	Number of SSL sessions using an unknown SSL version.
`start_time_sec`	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
`tls_v10`	Number of SSL sessions using TLS version 1.0
`tls_v11`	Number of SSL sessions using TLS version 1.1
`tls_v12`	Number of SSL sessions using TLS version 1.2
`total_ssl_sessions`	Total number of SSL sessions detected.
`uncached_session`	Number of times that a cache miss on an ID or ticket prevented decryption.
`undecryptable_in_passive_mode`	Number of SSL sessions that could not be decrypted because the device is in passive mode.
`unknown_cipher_suite`	Number of SSL sessions using an unknown cipher suite.
`unsupported_cipher_suite`	Number of SSL sessions using a cipher suite which is known but not supported.

ssl_stats_current_timeframe Joins

You cannot perform joins on the **`ssl_stats_current_`***`timeframe`* tables.

ssl_stats_current_timeframe Sample Query

The following query returns the number of SSL sessions, sessions that were decrypted, sessions that were not decrypted, and sessions which cannot be decrypted in passive mode for each sensor, in descending order by `sensor_name` during the current day.

```
SELECT sensor_name, total_ssl_sessions, ssl_sessions_decrypted,
ssl_sessions_not_decrypted, undecryptable_in_passive_mode

FROM ssl_stats_current_day

ORDER BY sensor_id DESC;
```

storage_stats_by_disposition_current_timeframe

The **`storage_stats_by_disposition_`***`timeframe`* tables contain statistics for stores files. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **`current_day`**, **`current_month`**, and **`current_year`** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **`storage_stats_by_disposition_`***`timeframe`* tables, see the following sections:

- `storage_stats_by_disposition_current_timeframe Fields, page 5-14`
- `storage_stats_by_disposition_current_timeframe Joins, page 5-15`
- `storage_stats_by_disposition_current_timeframe Sample Query, page 5-15`

storage_stats_by_disposition_current_timeframe Fields

The following table describes the fields you can access in the **`storage_stats_by_disposition_current_`***`timeframe`* tables. All tables of this type contain the same fields.

Table 5-11 storage_stats_by_disposition_current_timeframe Fields

Field	Description
`bytes_written`	The size of the file, in bytes.
`disposition`	The malware status of the file. Possible values include: • `CLEAN` — The file is clean and does not contain malware. • `UNKNOWN` — It is unknown whether the file contains malware. • `MALWARE` — The file contains malware. • `UNAVAILABLE` — The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request. • `CUSTOM SIGNATURE` — The file matches a user-defined hash, and is treated in a fashion designated by the user.
`number_dropped`	Number of files of this disposition dropped.
`number_stored`	Number of files of this disposition stored.

Table 5-11 storage_stats_by_disposition_current_timeframe Fields (continued)

Field	Description
`sensor`	ID of the device that detected the file.
`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`.
`start_time_sec`	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

storage_stats_by_disposition_current_timeframe Joins

You cannot perform joins on the **`session_stats_current_`***`timeframe`* tables.

storage_stats_by_disposition_current_timeframe Sample Query

The following query returns the number of dropped and stored files for each sensor, in descending order by `sensor_name` during the current day.

```
SELECT sensor_name, number_dropped, number_stored

FROM storage_stats_by_disposition_current_day

ORDER BY sensor_name DESC;
```

storage_stats_by_file_type_current_timeframe

The **`storage_stats_by_file_type_current_`***`timeframe`* tables contain statistics for stored files by file type. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **`current_day`**, **`current_month`**, and **`current_year`** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **`storage_stats_by_file_type_current_`***`timeframe`* tables, see the following sections:

- storage_stats_by_file_type_current_timeframe Fields, page 5-15
- storage_stats_by_file_type_current_timeframe Joins, page 5-16
- storage_stats_by_file_type_current_timeframe Sample Query, page 5-16

storage_stats_by_file_type_current_timeframe Fields

The following table describes the fields you can access in the **`storage_stats_by_file_type_current_`***`timeframe`* tables. All tables of this type contain the same fields.

Table 5-12 storage_stats_by_file_type_current_timeframe Fields

Field	Description
`bytes_written`	The size of the file, in bytes.
`file_type`	The file type of the detected or quarantined file.
`file_type_id`	ID number that maps to the file type.
`number_dropped`	Number of files of this type dropped.
`number_stored`	Number of files of this type stored.
sensor	ID of the device that detected the file.
`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`.
`start_time_sec`	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

storage_stats_by_file_type_current_timeframe Joins

You cannot perform joins on the **session_stats_current_***timeframe* tables.

storage_stats_by_file_type_current_timeframe Sample Query

The following query returns the number of dropped and stored files for each sensor, in descending order by `file_type` during the current day.

```
SELECT sensor_name, number_dropped, number_stored, file_type

FROM storage_stats_by_file_type_current_day

ORDER BY file_type DESC;
```

transmission_stats_by_file_type_current_timeframe

The **transmission_stats_by_file_type_current_***timeframe* tables contain statistics for stored files by file type. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **transmission_stats_by_file_type_current_***timeframe* tables, see the following sections:

- transmission_stats_by_file_type_current_timeframe Fields, page 5-17
- transmission_stats_by_file_type_current_timeframe Joins, page 5-17
- transmission_stats_by_file_type_current_timeframe Sample Query, page 5-17

transmission_stats_by_file_type_current_timeframe Fields

The following table describes the fields you can access in the **storage_stats_by_file_type_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-13 transmission_stats_by_file_type_current_timeframe Fields

Field	Description
bytes_sent	The number of transmitted bytes.
file_type	The file type of the detected or quarantined file.
file_type_id	ID number that maps to the file type.
number_dropped	Number of files of this type dropped.
number_sent	Number of files of this type sent.
sensor	ID of the device that detected the file.
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.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

transmission_stats_by_file_type_current_timeframe Joins

You cannot perform joins on the **transmission_stats_current_***timeframe* tables.

transmission_stats_by_file_type_current_timeframe Sample Query

The following query returns the number of dropped and sent connections for each sensor, in descending order by file_type during the current day.

```
SELECT sensor_name, number_dropped, number_sent, file_type

FROM transmission_stats_by_file_type_current_day

ORDER BY file_type DESC;
```

url_category_stats_current_timeframe

The **url_category_stats_current_***timeframe* tables contain statistics on the bandwidth usage and connections associated with requests to URLs in specified URL categories. You can also constrain queries on the managed device that monitored the traffic.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **url_category_stats_current_***timeframe* tables, see the following sections:

- url_category_stats_current_timeframe Fields, page 5-18
- url_category_stats_current_timeframe Joins, page 5-18
- url_category_stats_current_timeframe Sample Query, page 5-18

url_category_stats_current_timeframe Fields

The following table describes the fields you can access in the **url_category_stats_current**_*timeframe* tables.

Table 5-14 url_category_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
category	The category of the URL.
connections_allowed	The number of connections allowed for the specified URL category.
connections_denied	The number of connections denied for the specified URL category due to violation of an access control policy.
sensor_address	The IP address of the managed device that monitored the traffic. Format is *ipv4_address,ipv6_address*.
sensor_id	The internal identification number of the managed device that detected the traffic.
sensor_name	The managed device that monitored the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

url_category_stats_current_timeframe Joins

You cannot perform joins on the **url_category_stats_current**_*timeframe* tables.

url_category_stats_current_timeframe Sample Query

The following query returns up to 25 URL category records. Each record contains the bytes of associated inbound and outbound traffic, as well as allowed and denied connections, over the specified time interval.

```
SELECT category, sensor_name, sensor_address, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied

FROM url_category_stats_current_year

WHERE category="Games"

LIMIT 0, 25;
```

url_reputation_stats_current_timeframe

The **url_reputation_stats_current_***timeframe* tables contain statistics on the bandwidth usage and connections associated with requests to URLs with specified reputations. Query results can also be constrained on the managed device that monitored the traffic.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information on the **url_reputation_stats_current_***timeframe* tables, see the following sections:

- url_reputation_stats_current_timeframe Fields, page 5-19
- url_reputation_stats_current_timeframe Joins, page 5-20
- url_reputation_stats_current_timeframe Sample Query, page 5-20

url_reputation_stats_current_timeframe Fields

The following table describes the fields you can access in the **url_category_stats_current_***timeframe* tables.

Table 5-15 url_reputation_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
connections_allowed	The number of connections allowed.
connections_denied	The number of connections denied due to violation of an access control policy.
reputation	The risk associated with the requested URL. One of the following: • High risk • Suspicious site • Benign site with security risks • Benign site • Well known • Risk unknown
sensor_address	The IP address of the managed device that monitored the traffic. Format is *ipv4_address,ipv6_address*.
sensor_id	Internal identification number of the managed device that monitored the traffic.
sensor_name	The name of the managed device that monitored the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

url_reputation_stats_current_timeframe Joins

You cannot perform joins on the **url_reputation_stats_current_***timeframe* tables.

url_reputation_stats_current_timeframe Sample Query

The following query returns up to 25 URL reputation records from the **url_reputation_stats_current_month** table. Each record contains the bytes of inbound and outbound traffic, as well as allowed and denied connections over the measurement time interval.

```
SELECT sensor_name, sensor_address, reputation, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied

FROM url_reputation_stats_current_year

WHERE reputation="High risk"

LIMIT 0, 25;
```

user_ids_stats_current_timeframe

The **user_ids_stats_current_***timeframe* tables are round-robin tables that contain statistics on access filtering and impact statistics by user.

For an understanding of the **current_day**, **current_month**, and **current_year** tables in this type, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For general information on using the round robin statistics tables, see Understanding Statistics Tracking Tables, page 5-2.

For more information on the **user_ids_stats_current_***timeframe* tables, see the following sections:

- user_ids_stats_current_timeframe Fields, page 5-20
- user_ids_stats_current_timeframe Joins, page 5-21
- user_ids_stats_current_timeframe Sample Query, page 5-21

user_ids_stats_current_timeframe Fields

The following table describes the fields you can access in the **user_ids_stats_current_***timeframe* tables.

Table 5-16 user_ids_stats_current_timeframe Fields

Field	Description
blocked	The number of connections blocked due to violation of an intrusion policy.
impact_level_1	The number of impact level 1 (vulnerable) intrusion events recorded for the user.
impact_level_2	The number of impact level 2 (potentially vulnerable) intrusion events recorded for the user.
impact_level_3	The number of impact level 3 (host currently not vulnerable) intrusion events recorded for the user.

Table 5-16 user_ids_stats_current_timeframe Fields (continued)

Field	Description
`impact_level_4`	The number of impact level 4 (unknown target) intrusion events recorded for the user.
`impact_level_5`	The number of impact level 5 (unknown vulnerability) intrusion events recorded for the user.
`sensor_address`	The IP address of the managed device that monitored the traffic. Format is *`ipv4_address,ipv6_address`*.
`sensor_id`	The internal identification number of the managed device that detected the traffic.
`sensor_name`	The name of the managed device that detected the traffic.
`sensor_uuid`	A unique identifier for the managed device, or `0` if `sensor_name` is `null`.
`start_time_sec`	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
`user_id`	An internal identification number for the user who last logged into the host.
`username`	The user name of the user who last logged into the host.
`would_have_dropped`	Number of packets that would have been dropped if the intrusion policy had been configured to drop packets in an inline deployment.

user_ids_stats_current_timeframe Joins

You cannot perform joins on the **`user_ids_stats_current_`***`timeframe`* tables.

user_ids_stats_current_timeframe Sample Query

The following query returns up to 25 user records from the **`user_ids_stats_current_month`** table. Each record contains the number of blocked connections and intrusion events for the selected `username`.

```
SELECT username, start_time_sec, blocked, impact_level_1, impact_level_2,
impact_level_3, impact_level_4, impact_level_5 FROM user_ids_stats_current_year

WHERE username="username"

LIMIT 0, 25;
```

user_stats_current_timeframe

The **`user_stats_current_`***`timeframe`* tables contain statistics on bandwidth usage and access control actions (connection allowed or denied) by user. You can also constrain queries on the managed device that monitored the traffic.

For an understanding of the **`current_day`**, **`current_month`**, and **`current_year`** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-2.

For more information, see the following sections:

- `user_stats_current_timeframe Fields, page 5-22`

user_stats_current_timeframe Fields

The following table describes the fields you can access in the **user_stats_current_***timeframe* tables.

Table 5-17 user_stats_current_timeframe Fields

Field	Description
bytes_in	The number of bytes of inbound traffic for the user in the measured interval.
bytes_out	The number of bytes of outbound traffic for the user in the measured interval.
connections_allowed	The number of connections allowed for this user in the measured time frame.
connections_denied	The number of connections denied for this user due to violation of an access control policy.
sensor_address	The IP address of the managed device that monitored the traffic. Format is *ipv4_address,ipv6_address*.
sensor_id	The internal identification number of the managed device that detected the traffic.
sensor_name	The name of the managed device that detected the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
user_id	The internal identification number for the user who last logged into the host that generated the traffic.
username	User name for the user who last logged into the host that generated the traffic.

user_stats_current_timeframe Joins

You cannot perform joins on the **user_stats_current_***timeframe* tables.

user_stats_current_timeframe Sample Query

The following query returns up to 25 user records. Each record contains the bytes of inbound and outbound traffic, as well as allowed and denied connections over the measurement time interval.

```
SELECT sensor_name, sensor_address, username, start_time_sec, bytes_in, bytes_out,

connections_allowed, connections_denied

FROM user_stats_current_year

WHERE username="username" LIMIT 0, 25;
```