Schema: Discovery Event and Network Map Tables

This chapter contains information on the schema and supported joins for tables related to discovery events and the Cisco network map.

Your FireSIGHT System generates discovery events continuously as it monitors the traffic produced by your hosts and network devices.

The network map is a repository of information about the network assets reported in discovery events. For each detected host and network device, the network map contains information such as operating system, servers, client applications, host attributes, vulnerabilities, and so on.

Vulnerabilities are descriptions of specific compromises or exploits to which hosts may be susceptible. Cisco maintains its own vulnerability database (VDB), which cross-references the Bugtraq database and MITRE's CVE database. You can also import third-party vulnerability data using the host input feature.

Note that the information about a given host in the network map can vary according to the type of host and the information available in the monitored traffic.

For more information, see the sections listed in the following table. The Version column indicates the FireSIGHT System versions that support each table. While support for deprecated tables continues in the current product release, Cisco **strongly** recommends avoiding the use of deprecated tables and fields, to ensure continued support in the future.

Table 6-1 Schema for Discovery Event and Network Map Tables

See...	For the table that stores information on...	Version
application_host_map, page 6-5	Applications detected on the hosts in your monitored network.	5.0+
application_ip_map, page A-1	The category, tags, productivity, and risk associated with an application detected in your monitored network.	5.2+
application_ip_map, page A-1	The category, tags, productivity, and risk associated with an application detected in your monitored network. deprecated in Version 5.2. Superseded by application_ip_map, page A-1.	5.0-5.1.x
application_tag_map, page 6-9	The tags associated with an application detected in your monitored network.	5.0+
network_discovery_event, page 6-11	Discovery and host input events.	5.0+
rna_host, page 6-12	Basic information on the hosts in your monitored network.	5.2+

Table 6-1 Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
rna_host_attribute, page 6-14	The host attributes associated with each host in your monitored network.	5.2+
rna_host_client_app, page 6-15	The client applications detected on the hosts in your monitored network.	5.2+
rna_host_client_app, page 6-15	The payloads associated with HTTP (web browser) client applications detected on the hosts in your monitored network.	5.2+
rna_host_ioc_state, page 6-21	Stores compromise state for hosts.	5.3+
rna_host_ip_map, page 6-25	Correlates host IDs to MAC addresses for hosts in your monitored network.	5.2+
rna_host_os, page 6-28	The operating systems detected on the hosts in your monitored network.	5.2+
rna_host_os_vulns, page 6-29	The vulnerabilities associated with the hosts in your monitored network.	5.2+
rna_host_protocol, page 6-31	The protocols detected on the hosts in your monitored network.	4.10.x+
rna_host_protocol, page 6-31	The hosts in your monitored network with regard to the managed device that detected them.	5.2+
rna_host_service, page 6-34	The services detected on the hosts in your monitored network.	5.2+
rna_host_service_banner, page 6-36	Headers from network traffic that advertise service vendors and versions (“banners”) for the services detected on hosts in your monitored network.	5.2+
rna_host_service_info, page 6-37	Details of the services detected on the hosts in your monitored network.	5.2+
rna_host_service_payload, page 6-42	The payloads associated with services detected on the hosts in your monitored network.	5.2+
rna_host_service_subtype, page 6-45	The sub-services for the services detected on the hosts in your monitored network.	5.2+
rna_host_service_vulns, page 6-46	The vulnerabilities associated with the services detected on the hosts in your monitored network.	5.2+
rna_host_third_party_vuln, page 6-47	The third-party vulnerabilities associated with the hosts in your monitored network.	5.2+
rna_host_third_party_vuln_bugtraq_id, page 6-49	The third-party vulnerabilities associated with the hosts in your monitored network that are also associated with a vulnerability in the Bugtraq database (`http://www.securityfocus.com/bid/`).	5.2+
rna_host_third_party_vuln_cve_id, page 6-50	The third-party vulnerabilities associated with the hosts in your monitored network that are also associated with a vulnerability in MITRE’s CVE database. (`http://www.cve.mitre.org/`).	5.2+

Table 6-1 Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
rna_host_third_party_vuln_rna_id, page 6-52	The third-party vulnerabilities associated with the hosts in your monitored network that are also associated with a vulnerability in the VDB.	5.2+
rna_ip_host, page A-1	Basic information on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host, page 6-12**.	4.10.x-5.1.x
rna_ip_host_client_app, page A-1	The client applications detected on the hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_client_app, page 6-15**.	4.10.x-5.1.x
rna_ip_host_client_app_payload, page A-1	The payloads associated with HTTP (web browser) client applications detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_client_app, page 6-15**.	4.10.x-5.1.x
rna_ip_host_os, page A-1	The operating systems detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_os, page 6-28**.	4.10.x-5.1.x
rna_ip_host_os_vulns, page A-1	The vulnerabilities associated with the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_os_vulns, page 6-29**.	4.10.x--5.1.x
rna_ip_host_sensor, page A-1	The IP hosts in your monitored network with regard to the managed device that detected them. deprecated in Version 5.2. Superseded by **rna_host_protocol, page 6-31**.	5.0-5.1.x
rna_ip_host_service, page A-1	The services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_service, page 6-34**.	4.10.x-5.1.x
rna_ip_host_service_banner, page A-1	Headers from network traffic that advertise service vendors and versions (“banners”) for the services detected on hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_service_banner, page 6-36**.	4.10.x-5.1.x
rna_ip_host_service_info, page A-1	Details of the services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_service_info, page 6-37**.	4.10.x-5.1.x

Table 6-1 Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
rna_ip_host_service_payload, page A-1	The payloads associated with services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_service_payload, page 6-42**.	4.10.x-5.1.x
rna_ip_host_service_subtype, page A-1	The sub-services for the services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_service_subtype, page 6-45**.	4.10.x-5.1.x
rna_ip_host_service_vulns, page A-1	The vulnerabilities associated with the services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_service_vulns, page 6-46**.	4.10.x-5.1.x
rna_ip_host_third_party_vuln, page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_third_party_vuln, page 6-47**.	4.10.x-5.1.x
rna_ip_host_third_party_vuln_bugtraq_id, page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network that are also associated with a vulnerability in the Bugtraq database (`http://www.securityfocus.com/bid/`). deprecated in Version 5.2. Superseded by **rna_host_third_party_vuln_bugtraq_id, page 6-49**.	4.10.x-5.1.x
rna_ip_host_third_party_vuln_cve_id, page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network that are also associated with a vulnerability in MITRE's CVE database. (`http://www.cve.mitre.org/`). deprecated in Version 5.2. Superseded by **rna_host_third_party_vuln_cve_id, page 6-50**.	4.10.x-5.1.x
rna_ip_host_third_party_vuln_rna_id, page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network that are also associated with a vulnerability in the VDB. deprecated in Version 5.2. Superseded by **rna_host_third_party_vuln_rna_id, page 6-52**.	4.10.x-5.1.x
rna_ip_host_user_history, page A-1	User activity for a particular IP host in your monitored network. deprecated in Version 5.2. Superseded by **user_ipaddr_history, page 6-59**.	4.10.x-5.1.x
rna_mac_host, page A-1	The MAC hosts (hosts without an IP address) in your monitored network.	4.10.x-5.1.x
rna_mac_host_sensor, page A-2	The IP hosts in your monitored network with regard to the managed devices that detected them.	5.0-5.1.x

Table 6-1 Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
rna_mac_ip_map, page A-2	The MAC addresses of the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by **rna_host_ip_map, page 6-25** and **rna_host_mac_map, page 6-27**.	4.10.x-5.1.x
rna_vuln, page 6-54	The vulnerabilities in the Cisco VDB.	4.10.x+
tag_info, page 6-57	The tags that characterize detected applications.	5.0+
url_categories, page 6-58	The categories that characterize URLs accessed from hosts in your monitored network.	5.0+
url_reputations, page 6-58	The reputations that characterize URLs accessed from hosts in your monitored network.	5.0+
user_ipaddr_history, page 6-59	User activity for a particular host in your monitored network.	5.2+

application_host_map

The **application_host_map** table contains information on the categories and tags associated with each application detected on your network.

For more information, see the following sections:

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

application_host_map Fields

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

Table 6-2 application_host_map Fields

Field	Description
application_id	The internal identification number for the application.
application_name	The application name that appears in the user interface.
application_tag_id	This field has been deprecated and will now return null.
business_relevance	The 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	The description of the business relevance (very low, low, medium, high, very high).
host_id	ID number of the host.
risk	An index (from 1 to 5) of the application's risk, where 1 is very low risk and 5 is critical risk.
risk_description	The description of the risk (very low, low, medium, high, critical).

application_host_map Joins

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

Table 6-3 application_host_map Joins

You can join this table on...	And...
application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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 si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

application_host_map Sample Query

The following query returns information about the applications detected on the host with a `host_id` of `8`.

```
SELECT host_id, application_id, application_name, business_relevance, risk
FROM application_host_map
```

```
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

application_info

The **application_info** table contains information about the applications that can be detected on the hosts in your monitored network.

You can retrieve the list of tags associated with an application from the **application_tag_map** table by joining on **application_id**. Similarly, you can retrieve an application's list of associated categories from the **application_host_map** by joining on **application_id**.

For more information, see the following sections:

- application_info Fields, page 6-8
- application_info Joins, page 6-8
- application_info Sample Query, page 6-9

application_info Fields

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

Table 6-4 application_info Fields

Field	Description
application_description	A description of the application.
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).
is_client_application	A true-false flag that indicates if the detected application is a client.
is_server_application	A true-false flag that indicates if the detected application is a server application.
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 risk (very low, low, medium, high, and critical).

application_info Joins

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

Table 6-5 application_info Joins

You can join this table on...	And...
application_id	application_host_map.application_id app_ids_stats_current_timeframe.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id si_connection_log.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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

application_info Sample Query

The following query returns the record for the application with a `host_id` of `8`.

```
SELECT application_id, application_name, application_description, business_relevance,
risk

FROM application_info

WHERE application_id="8";
```

application_tag_map

The **application_tag_map** table contains information on the tags associated with each application detected on your network.

For more information, see the following sections:

- application_tag_map Fields, page 6-10
- application_tag_map Joins, page 6-10
- application_tag_map Sample Query, page 6-10

application_tag_map Fields

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

Table 6-6 application_tag_map Fields

Field	Description
application_id	The internal identification number for the application.
application_name	The application that appears in the user interface.
tag_id	The internal identification number for the tag.
tag_name	The text of the tag that appears in the user interface.
tag_type	One of the following: category or type.

application_tag_map Joins

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

Table 6-7 application_tag_map Joins

You can join this table on...	And...
application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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 si_connection_log.application_protocol_name si_connection_log.application_protocol_id si_connection_log.client_application_id si_connection_log.web_application_id
tag_id	tag_info.tag_id

application_tag_map Sample Query

The following query returns all tag records associated with the specified application.

```
SELECT application_id, application_name, tag_id, tag_name
FROM application_tag_map
WHERE application_name="Active Directory";
```

network_discovery_event

The **network_discovery_event** table contains information on discovery and host input events. The FireSIGHT System generates discovery events when it detects a change on your monitored network, whether by discovering new network features or by detecting changes in previously identified network assets. The FireSIGHT System generates host input events when a user manually modifies the network map by adding, modifying, or deleting network assets.

The **network_discovery_event** table supersedes the deprecated **rna_events** table starting with Version 5.0 of the FireSIGHT System.

For more information, see the following sections:

- network_discovery_event Fields, page 6-11
- network_discovery_event Joins, page 6-12
- network_discovery_event Sample Query, page 6-12

network_discovery_event Fields

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

Table 6-8 network_discovery_event Fields

Field	Description
confidence	The FireSIGHT System-assigned confidence rating (from 0 to 100) for the identification of the service.
description	The description of the event.
event_id	The internal identification number for the event.
event_time_sec	The UNIX timestamp of the date and time the event was generated.
event_time_usec	The microsecond increment of the event timestamp.
event_type	The event type. For example, New Host or Identity Conflict.
ip_address	This field has been deprecated and will now return null.
ipaddr	A binary representation of the IPv4 or IPv6 address for the host involved in the event.
mac_address	The MAC address of the host involved in the event.
mac_vendor	The NIC hardware vendor of the host involved in the event.
port	The port used by the network traffic that triggered the event.
sensor_address	The IP address of the managed device that generated the discovery event. Format is *ipv4_address,ipv6_address*.
sensor_name	The managed device that generated the discovery event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.

Table 6-8 network_discovery_event Fields (continued)

Field	Description
user_dept	The department of the user who last logged into the host.
user_email	The email address of the user who last logged into the host.
user_first_name	The first name of the user who last logged into the host.
user_id	The internal identification number for the user who last logged into the host.
user_last_name	The last name of the user who last logged into the host.
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.
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.
user_name	The user name of the user who last logged into the host.
user_phone	The phone number of the user who last logged into the host.

network_discovery_event Joins

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

Table 6-9 network_discovery_event Joins

You can join this table on...	And...
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

network_discovery_event Sample Query

The following query returns discovery event records that include the user, detecting device name, timestamp, host IP address, and so on within the specified times.

```
SELECT sensor_name, event_time_sec, event_time_usec, event_type, ipaddr, user_id,
hex(mac_address), mac_vendor, port, confidence FROM network_discovery_event
WHERE event_time_sec
BETWEEN UNIX_TIMESTAMP("2013-01-01 00:00:00") AND UNIX_TIMESTAMP("2013-01-01 23:59:59")
ORDER BY event_time_sec DESC, event_time_usec DESC;
```

rna_host

The **rna_host** table contains basic information on the hosts in your monitored network.

This table supersedes **rna_ip_host** as of Version 5.2.

For more information, see the following sections:

- rna_host Fields, page 6-13

rna_host Fields

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

Table 6-10 **rna_host** ***Fields***

Field	Description
criticality	The host criticality level: None, Low, Medium, or High.
hops	The number of network hops from the host to the managed device that detected the host.
host_id	ID number of the host.
host_name	Name of the host.
host_type	The host type: Host, Router, Bridge, NAT Device, or Load Balancer.
jailbroken	A true-false flag indicating whether a mobile device operating system is jailbroken.
last_seen_sec	The UNIX timestamp of the date and time the system last detected host activity.
mobile	A true-false flag indicating whether the detected host is a mobile device.
netbios_name	The host NetBIOS name string.
notes	The contents of the Notes host attribute for the host.
vlan_id	The VLAN identification number, if applicable.
vlan_priority	The priority value included in the VLAN tag.
vlan_type	The type of encapsulated packet that contains the VLAN tag: • 0 — Ethernet • 1 — Token Ring

rna_host Joins

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

Table 6-11 rna_host Joins

You can join this table on...	And...
host_id	application_host_map.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_ioc_state.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host Sample Query

The following query returns 25 **rna_host** records that include the host ID, VLAN ID, when the host was last seen, and the type of host, ordered by the type of host.

```
SELECT host_id, vlan_id, last_seen_sec, host_type
FROM rna_host
ORDER BY host_type
LIMIT 0, 25;
```

rna_host_attribute

The **rna_host_attribute** table contains information on the host attributes associated with each host in your monitored network. It supersedes the deprecated **rna_ip_host_attribute** table.

For more information, see the following sections:

- rna_host_attribute Fields, page 6-14
- rna_host_attribute Joins, page 6-15
- rna_host_attribute Sample Query, page 6-15

rna_host_attribute Fields

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

Table 6-12 rna_host_attribute Fields

Field	Description
attribute_name	The host attribute. For example, Host Criticality or Default White List.
attribute_value	The value of the host attribute.
host_id	ID number of the host.

rna_host_attribute Joins

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

Table 6-13 rna_host_attribute Joins

You can join this table on...	And...
host_id	application_host_map.host_id rna_host.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_attribute Sample Query

The following query returns all host attributes and values associated with the selected host ID.

```
SELECT attribute_name, attribute_value

FROM rna_host_attribute

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_client_app

The **rna_host_client_app** table contains information on the client applications detected on the hosts in your monitored network. It supersedes the deprecated **rna_ip_host_client_app** table.

For more information, see the following sections:

- rna_host_client_app Fields, page 6-16
- rna_host_client_app Joins, page 6-16
- rna_host_client_app Sample Query, page 6-18

rna_host_client_app Fields

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

Table 6-14 rna_host_client_app Fields

Field	Description
application	Field deprecated in Version 5.0. Returns null for all queries.
application_protocol_id	An internal identifier for the detected 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
application_type	Field deprecated in Version 5.0. Returns null for all queries.
client_application_id	The internal identification number for the application, if the application is identifiable.
client_application_name	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.
hits	The number of times the client application was detected.
host_id	ID number of the host.
last_used_sec	The UNIX timestamp of the date and time the system last detected application activity.
version	The version of the application detected on the host.

rna_host_client_app Joins

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

Table 6-15 rna_host_client_app Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

Table 6-15 rna_host_client_app Joins (continued)

You can join this table on...	And...
host_id and application_protocol_id and client_application_id and version	the set of: rna_host_client_app_payload.host_id rna_host_client_app_payload.application_protocol_id rna_host_client_app_payload.client_application_id rna_host_client_app_payload.version
application_protocol_id or client_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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_service_info.application_protocol_id rna_host_service_payload.web_application_id

rna_host_client_app Sample Query

The following query returns information about the client applications detected on the host with `host_id` of `8`.

```
SELECT host_id, client_application_id, client_application_name, version, hits,
application_protocol_id, application_protocol_name, last_used_sec

FROM rna_host_client_app

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_client_app_payload

The **`rna_host_client_app_payload`** table contains information on the payloads in HTTP traffic associated with web applications on hosts detected in your monitored network.

For more information, see the following sections:

- rna_host_client_app_payload Fields, page 6-19
- rna_host_client_app_payload Joins, page 6-20
- rna_host_client_app_payload Sample Query, page 6-21

rna_host_client_app_payload Fields

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

Table 6-16 rna_host_client_app_payload Fields

Field	Description
application	Field deprecated in Version 5.0. Returns null for all queries.
application_protocol_id	An internal identifier for the detected application protocol, if available. For traffic that has characteristics of both client applications and web applications, the client_application_id and web_application_id fields have the same value.
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
application_type	Field deprecated in Version 5.0. Returns null for all queries.
client_application_id	The internal identification number for the client application.
client_application_name	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.
host_id	ID number of the host.
payload_name	Field deprecated in Version 5.0. Returns null for all queries.
payload_type	Field deprecated in Version 5.0. Returns null for all queries.
version	The version of the web application detected on the host.
web_application_id	The internal identification number for the web application, if available. For traffic that has characteristics of both client applications and web applications, the client_application_id and web_application_id fields have the same value.
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.

rna_host_client_app_payload Joins

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

Table 6-17 rna_host_client_app_payload Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

Table 6-17 rna_host_client_app_payload Joins (continued)

You can join this table on...	And...
the set of: host_id, application_protocol_id, client_application_id, version	the set of: rna_host_client_app.host_id rna_host_client_app.application_protocol_id rna_host_client_app.client_application_id rna_host_client_app.version
client_application_id or web_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

rna_host_client_app_payload Sample Query

The following query returns information about the web applications detected on the host with `host_id` of `8`.

```
SELECT host_id, web_application_id, web_application_name, version,
client_application_id, client_application_name

FROM rna_host_client_app_payload

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_ioc_state

The **`rna_host_ioc_state`** table stores the IOC state for hosts in your monitored network.

For more information, see the following sections:

- rna_host_ioc_state Fields, page 6-22
- rna_host_ioc_state Joins, page 6-24
- rna_host_ioc_state Sample Query, page 6-24

rna_host_ioc_state Fields

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

Table 6-18 rna_host_ioc_state Fields

Field	Description
first_seen	Unix timestamp when the compromise was first detected.
first_seen_sensor_address	The IP address of the managed device that first detected the compromise. Format is *ipv4_address,ipv6_address*.
first_seen_sensor_name	The managed device that first detected the compromise.
host_id	ID number of the host.
ioc_category	The category for the compromise. Possible values include: • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
ioc_description	Description of the compromise.

Table 6-18 rna_host_ioc_state Fields (continued)

Field	Description
ioc_event_type	The event type for the compromise. Possible values include: • Adobe Reader launched shell • Dropper Infection Detected by FireAMP • Excel Compromise Detected by FireAMP • Excel launched shell • Impact 1 Intrusion Event — attempted-admin • Impact 1 Intrusion Event — attempted-user • Impact 1 Intrusion Event — successful-admin • Impact 1 Intrusion Event — successful-user • Impact 1 Intrusion Event — web-application-attack • Impact 2 Intrusion Event — attempted-admin • Impact 2 Intrusion Event — attempted-user • Impact 2 Intrusion Event — successful-admin • Impact 2 Intrusion Event — successful-user • Impact 2 Intrusion Event — web-application-attack • Intrusion Event — exploit-kit • Intrusion Event — malware-backdoor • Intrusion Event — malware-CnC • Java Compromise Detected by FireAMP • Java launched shell • PDF Compromise Detected by FireAMP • PowerPoint Compromise Detected by FireAMP • PowerPoint launched shell • QuickTime Compromise Detected by FireAMP • QuickTime launched shell • Security Intelligence Event — CnC • Suspected Botnet Detected by FireAMP • Threat Detected by FireAMP — Subtype is 'executed' • Threat Detected by FireAMP — Subtype is not 'executed' • Threat Detected in File Transfer — Action is not 'block' • Word Compromise Detected by FireAMP • Word launched shell
ioc_id	Unique ID number for the compromise.
is_disabled	Whether this compromise has been disabled.
last_seen	Unix timestamp when this compromise was last detected.

Table 6-18 rna_host_ioc_state Fields (continued)

Field	Description
last_seen_sensor_address	The IP address of the managed device that last detected the compromise. Format is *ipv4_address,ipv6_address*.
last_seen_sensor_name	The managed device that last detected the compromise.

rna_host_ioc_state Joins

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

Table 6-19 rna_host_ioc_state Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_ioc_state Sample Query

The following query returns up to 25 hosts with their ioc within a specified timespan.

```
SELECT host_id, ioc_id

FROM rna_host_ioc_state

WHERE first_seen

BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")

AND UNIX_TIMESTAMP("2011-10-07 23:59:59")

ORDER BY ioc_id DESC

LIMIT 0, 25;
```

rna_host_ip_map

The **rna_host_ip_map** table correlates host IDs to IP addresses for hosts in your monitored network.

For more information, see the following sections:

- rna_host_ip_map Fields, page 6-25
- rna_host_ip_map Joins, page 6-25
- rna_host_ip_map Sample Query, page 6-26

rna_host_ip_map Fields

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

Table 6-20 rna_host_ip_map Fields

Field	Description
host_id	ID number of the host.
ipaddr	A binary representation of the IP address of the host.

rna_host_ip_map Joins

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

Table 6-21 rna_host_ip_map Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
ipaddr	compliance_event.dst_ipaddr compliance_event.src_ipaddr connection_log.initiator_ipaddr connection_log.responder_ipaddr connection_summary.initiator_ipaddr connection_summary.responder_ipaddr fireamp_event.dst_ipaddr fireamp_event.src_ipaddr intrusion_event.dst_ipaddr intrusion_event.src_ipaddr network_discovery_event.ipaddr si_connection_log.initiator_ipaddr si_connection_log.responder_ipaddr user_discovery_event.ipaddr user_ipaddr_history.ipaddr white_list_event.ipaddr

rna_host_ip_map Sample Query

The following query returns MAC information for the selected host.

```
SELECT host_id

FROM rna_host_ip_map

WHERE HEX(ipaddr) = "00000000000000000000FFFF0A0A0A04";
```

rna_host_mac_map

The **rna_host_mac_map** table correlates host IDs to MAC addresses for hosts in your monitored network.

For more information, see the following sections:

- rna_host_mac_map Fields, page 6-27
- rna_host_mac_map Joins, page 6-27
- rna_host_mac_map Sample Query, page 6-28

rna_host_mac_map Fields

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

Table 6-22 rna_host_mac_map Fields

Field	Description
host_id	ID number of the host.
mac_address	The host's MAC address.
mac_vendor	Vendor of the network interface of the detected host.

rna_host_mac_map Joins

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

Table 6-23 rna_host_mac_map Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_mac_map Sample Query

The following query returns MAC information for the host with `host_id` of `8`.

```
SELECT HEX(mac_address)
FROM rna_host_mac_map
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_os

The **`rna_host_os`** table contains information on the operating systems detected on the hosts in your monitored network.

For more information, see the following sections:

- rna_host_os Fields, page 6-28
- rna_host_os Joins, page 6-29
- rna_host_os Sample Query, page 6-29

rna_host_os Fields

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

Table 6-24 rna_host_os Fields

Field	Description
`confidence`	The FireSIGHT System-assigned confidence rating (from `0` to `100`) for the identification of the operating system.
`created_sec`	The UNIX timestamp of the date and time the system first detected host activity.
`host_id`	ID number of the host.
`last_seen_sec`	The UNIX timestamp of the date and time the system last detected host activity.
`os_uuid`	A unique identifier for the operating system detected on the host. The UUID maps to the operating system name, vendor, and version in the Cisco database.
`product`	The operating system detected on the host.
`source_type`	The source of the host's operating system identity: • `User` — Name of the user who entered the data via the web user interface • `Application` — Imported from another application via the host input feature • `Scanner` — Either Nmap or another scanner added through system policy • `rna` — Detected by the FireSIGHT System, either by a discovery event, port match, or pattern match • `NetFlow` — The data was exported by a NetFlow-enabled device
`vendor`	The vendor of the operating system detected on the host.
`version`	The version of the operating system detected on the host.

rna_host_os Joins

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

Table 6-25 rna_host_os Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_os Sample Query

The following query returns operating system information for the host with `host_id` of `8`.

```
SELECT vendor, product, version, source_type, confidence

FROM rna_host_os

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_os_vulns

The **rna_host_os_vulns** table contains information on the vulnerabilities associated with the hosts in your monitored network.

For more information, see the following sections:

- rna_host_os_vulns Fields, page 6-30
- rna_host_os_vulns Joins, page 6-30
- rna_host_os_vulns Sample Query, page 6-30

rna_host_os_vulns Fields

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

Table 6-26 rna_host_os_vulns Fields

Field	Description
host_id	ID number of the host.
invalid	A value indicating whether the vulnerability is valid for the host: • 0 — Vulnerability is valid • 1 — Vulnerability is invalid
rna_vuln_id	An internal identification number for the vulnerability.

rna_host_os_vulns Joins

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

Table 6-27 rna_host_os_vulns Joins

You can join this table on...	And...
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_os_vulns Sample Query

The following query returns the operating system vulnerabilities for the host with host_id of 8.

```
SELECT rna_vuln_id, invalid
FROM rna_host_os_vulns
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_protocol

The **rna_host_protocol** table contains information on the protocols detected on the hosts in your monitored network.

For more information, see the following sections:

- rna_host_protocol Fields, page 6-31
- rna_host_protocol Joins, page 6-31
- rna_host_protocol Sample Query, page 6-32

rna_host_protocol Fields

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

Table 6-28 rna_host_protocol Fields

Field	Description
host_id	ID number of the host.
ip_address	Field deprecated in Version 5.2. Returns null for all queries.
layer	The network layer where the protocol is running: Network or Transport.
mac_address	Field deprecated in Version 5.2. Returns null for all queries.
mac_vendor	Field deprecated in Version 5.2. Returns null for all queries.
protocol_name	The traffic protocol used by the host.
protocol_num	The IANA-specified protocol number for the protocol.

rna_host_protocol Joins

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

Table 6-29 rna_host_protocol Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_protocol Sample Query

The following query returns all protocol records for the host with `host_id` of `8`.

```
SELECT protocol_num, protocol_name

FROM rna_host_protocol

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_sensor

The **rna_host_sensor** table lists the host IP addresses in your monitored network and indicates the managed device that detected each one.

The **rna_host_sensor** table supersedes the deprecated **rna_ip_host_sensor** table starting with Version 5.2 of the FireSIGHT System.

For more information, see the following sections:

- rna_host_sensor Fields, page 6-32
- rna_host_sensor Joins, page 6-33
- rna_host_sensor Sample Query, page 6-33

rna_host_sensor Fields

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

Table 6-30 rna_host_sensor Fields

Field	Description
host_id	ID number of the host.
sensor_address	The IP address of the managed device that generated the discovery event. Format is *ipv4_address,ipv6_address*.
sensor_name	The name of the managed device.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.

rna_host_sensor Joins

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

Table 6-31 rna_host_sensor Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_sensor Sample Query

The following query returns up to 25 hosts, and the sensor that detected them, from the **rna_host_sensor** table.

```
SELECT host_id, sensor_address, sensor_name

FROM rna_host_sensor

LIMIT 0, 25;
```

rna_host_service

The **rna_host_service** table contains general information about the servers detected on the hosts in your managed network through network port and traffic protocol combinations.

For more information, see the following sections:

- rna_host_service Fields, page 6-34
- rna_host_service Joins, page 6-34
- rna_host_service Sample Query, page 6-35

rna_host_service Fields

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

Table 6-32 rna_host_service Fields

Field	Description
confidence	The FireSIGHT System-assigned confidence rating (from 0 to 100) for the identification of the server.
hits	The number of times the server was detected.
host_id	ID number of the host.
last_used_sec	UNIX timestamp of the date and time the system last detected server activity.
port	The port used by the server.
protocol	The traffic protocol: TCP or UDP.

rna_host_service Joins

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

Table 6-33 rna_host_service Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
The set of: host_id port protocol	The set of: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol The set of: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol The set of: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service Sample Query

The following query returns the first 25 detected server records for the host with host_id of 8:

```
SELECT hits, protocol, port, confidence
FROM rna_host_service
WHERE HEX(host_id) = "00000000000000000000000000000008"
LIMIT 0, 25;
```

rna_host_service_banner

The **rna_ip_host_service_banner** table contains header information from network traffic that advertises vendors and versions ("banners") for the servers on hosts in your monitored network. Keep in mind that the FireSIGHT System does not store server banners unless you enable the **Capture Banners** option in the your network discovery policy.

For more information, see the following sections:

- rna_ip_host_service_banner Fields, page 6-36
- rna_host_service_banner Joins, page 6-36
- rna_host_service_banner Sample Query, page 6-37

rna_ip_host_service_banner Fields

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

Table 6-34 rna_host_service_banner Fields

Field	Description
banner	The server banner, that is, the first 256 bytes of the first packet detected for the server.
host_id	ID number of the host.
port	The port used by the server.
protocol	The traffic protocol: TCP or UDP.

rna_host_service_banner Joins

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

Table 6-35 rna_host_service_banner Joins

You can join this table on...	And...
The set of: host_id port protocol	The set of: rna_host_service.host_id rna_host_service.port rna_host_service.protocol The set of: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol The set of: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_banner Sample Query

The following query returns the server banner for the host with `host_id` of `8`.

```
SELECT port, protocol, banner

FROM rna_host_service_banner

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_info

The **`rna_host_service_info`** table contains detailed information about the servers detected on the hosts in your monitored network.

For more information, see the following sections:

- rna_host_service_info Fields, page 6-38
- rna_host_service_info Joins, page 6-39
- rna_host_service_info Sample Query, page 6-41

rna_host_service_info Fields

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

Table 6-36 rna_host_service_info Fields

Field	Description
application_id	Field deprecated in Version 5.0. Returns blank for all queries.
application_protocol_id	An internal identifier for the detected application protocol, if available.
application_protocol_name	One of: • the name of the application protocol, if a positive identification can be made • pending if the system requires more data • blank if there is no application information in the connection
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).
created_sec	The UNIX timestamp of the date and time the system first detected the application protocol.
host_id	ID number of the host.
ip_address	Field deprecated in Version 5.2. Returns null for all queries.
last_used_sec	The UNIX timestamp of the date and time the system last detected server activity.
port	The port used by the server.
protocol	The traffic protocol: TCP or UDP.
risk	An index (from 1 to 5) of the application's risk where 1 is very low risk and 5 is very high risk.
risk_description	A description of the risk (very low, low, medium, high, very high).
service_info_id	An internal identification number for the server.
service_name	Field deprecated in Version 5.0. Returns null for all queries.

Table 6-36 rna_host_service_info Fields (continued)

Field	Description
source_type	The source of the identity of the server: • User — Name of the user who entered the data via the web user interface • Application — Imported from another application via the host input feature • Scanner — Added through NMAP or imported via the host input feature with a source type of Scanner • rna — Detected by the FireSIGHT System, either by a discovery event, port match, or pattern match • NetFlow — The data was exported by a NetFlow-enabled device
vendor	The vendor of the server on the host.
version	The version of the server detected on the host.

rna_host_service_info Joins

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

Table 6-37 rna_host_service_info Joins

You can join this table on...	And...
application_protocol_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_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

Table 6-37 rna_host_service_info Joins (continued)

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
The set of: host_id and port and protocol	The set of: rna_host_service.host_id rna_host_service.port rna_host_service.protocol The set of: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol The set of: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service_info Sample Query

The following query returns information about the application protocols detected on the host with host_id of 8.

```
SELECT host_id, application_protocol_name, version, vendor, created_sec, last_used_sec,
business_relevance, risk

FROM rna_host_service_info

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_payload

The **rna_host_service_payload** table contains information on the web applications associated by the hosts in your monitored network.

For more information, see the following sections:

rna_host_service_payload Fields

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

Table 6-38 rna_host_service_payload Fields

Field	Description
application_id	Field deprecated in Version 5.0. Returns null for all queries.
application_name	Field deprecated in Version 5.0. Returns null for all queries.
host_id	ID number of the host.
ip_address	Field deprecated in Version 5.2. Returns null for all queries.
payload_name	Field deprecated in Version 5.0. Returns null for all queries.
payload_type	Field deprecated in Version 5.0. Returns null for all queries.
port	The port used by the server.
protocol	The traffic protocol: TCP or UDP.
web_application_id	The internal identification number for the web application.
web_application_name	One of: • the name of the web 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

rna_host_service_payload Joins

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

Table 6-39 rna_host_service_payload Joins

You can join this table on...	And...
web_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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

Table 6-39 rna_host_service_payload Joins (continued)

You can join this table on...	And...
The set of: host_id port protocol	The set of: rna_host_service.host_id rna_host_service.port rna_host_service.protocol The set of: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol The set of: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_payload Sample Query

The following query returns information about the web applications detected on the host with `host_id` of `8`.

```
SELECT host_id, web_application_id, web_application_name, port, protocol

FROM rna_host_service_payload

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_subtype

The **rna_host_service_subtype** table contains information on the sub-servers for a server detected on the hosts in your monitored network.

For more information, see the following sections:

- rna_host_service_subtype Fields, page 6-45
- rna_host_service_subtype Joins, page 6-45
- rna_host_service_subtype Sample Query, page 6-46

rna_host_service_subtype Fields

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

Table 6-40 rna_host_service_subtype Fields

Field	Description
host_id	ID number of the host.
port	The port used by the server.
protocol	The traffic protocol: TCP or UDP.
service_name	One of: • the server on the host that is associated with the triggering event • none or blank if data for an identification is unavailable • pending if additional data is required • unknown if the system cannot identify the server based on known server fingerprints
source_type	The source of the identity of the server: • User - name of the user who entered the data via the web user interface • Application - imported from another application via the host input feature • Scanner - added through NMAP or imported via the host input feature with a source type of Scanner • rna - detected by the FireSIGHT System, either by a discovery event, port match, or pattern match • NetFlow - the data was exported by a NetFlow-enabled device
sub_service_name	The sub-server detected on the host.
sub_service_vendor	The vendor of the sub-server detected on the host.
sub_service_version	The version of the sub-server detected on the host.
vendor	The vendor of the server detected on the host.
version	The version of the server detected on the host.

rna_host_service_subtype Joins

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

rna_host_service_subtype Sample Query

The following query returns all detected sub-server records for the host with `host_id` of `8`.

```
SELECT host_id, service_name, version, sub_service_name, sub_service_version,
sub_service_vendor

FROM rna_host_service_subtype

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_vulns

The **`rna_host_service_vulns`** table contains information on the vulnerabilities mapped to the servers detected on the hosts in your monitored network.

For more information, see the following sections:

- rna_host_service_vulns Fields, page 6-46
- rna_host_service_vulns Joins, page 6-47
- rna_host_service_vulns Sample Query, page 6-47

rna_host_service_vulns Fields

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

Table 6-41 rna_host_service_vulns Fields

Field	Description
`application_id`	An internal identification number for the application protocol running on the host.
`application_name`	The application protocol name that appears in the user interface.
`host_id`	ID number of the host.
`invalid`	A value indicating whether the vulnerability is valid for the host running the application protocol: • `0` — Vulnerability is valid • `1` — Vulnerability is invalid
`ip_address`	Field deprecated in Version 5.2. Returns `null` for all queries.
`port`	The port used by the server.
`protocol`	The traffic protocol: `TCP` or `UDP`.
`rna_vuln_id`	An internal identification number for the vulnerability.
`service_name`	Field deprecated in Version 5.0. Returns `null` for all queries.
`vendor`	The vendor of the server detected on the host.
`version`	The version of the server detected on the host.

rna_host_service_vulns Joins

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

Table 6-42 rna_host_service_vulns Joins

You can join this table on...	And...
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_vulns Sample Query

The following query returns information about all server vulnerabilities for the host with `host_id` of `8`.

```
SELECT host_id, rna_vuln_id, vendor, service_name, version, invalid FROM
rna_host_service_vulns
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln

The **rna_host_third_party_vuln** table contains information on the third-party vulnerabilities associated with the hosts in your monitored network. Note that the information in this table is determined by the third-party vulnerability data imported via the host input feature.

For more information, see the following sections:

- rna_host_third_party_vuln Fields, page 6-48
- rna_host_third_party_vuln Joins, page 6-48

- rna_host_third_party_vuln Sample Query, page 6-49

rna_host_third_party_vuln Fields

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

Table 6-43 rna_host_third_party_vuln Fields

Field	Description
description	A description of the vulnerability.
host_id	ID number of the host.
invalid	A value indicating whether the vulnerability is valid for the host: • 0 — Vulnerability is valid • 1 — Vulnerability is invalid
name	The title of the vulnerability.
port	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
protocol	The traffic protocol (TCP or UDP), if the vulnerability is associated with an application using that protocol.
source	The source of the vulnerability.
third_party_vuln_id	An identification number associated with the vulnerability.

rna_host_third_party_vuln Joins

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

Table 6-44 rna_host_third_party_vuln Joins

You can join this table on...	And...
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln Sample Query

The following query returns information about the third party vulnerabilities for host with `host_id` of `8`.

```
SELECT host_id, third_party_vuln_id, name, description, source, invalid
FROM rna_host_third_party_vuln
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_bugtraq_id

The **`rna_host_third_party_vuln_bugtraq_id`** table contains information on the third-party vulnerabilities that are mapped to vulnerabilities in the Bugtraq database and also associated with hosts in your monitored network. Note that the third-party vulnerability data in this table is imported via the host input feature.

For more information, see the following sections:

- rna_host_third_party_vuln_bugtraq_id Fields, page 6-49
- rna_host_third_party_vuln_bugtraq_id Joins, page 6-50
- rna_host_third_party_vuln_bugtraq_id Sample Query, page 6-50

rna_host_third_party_vuln_bugtraq_id Fields

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

Table 6-45 rna_host_third_party_vuln_bugtraq_id Fields

Field	Description
`bugtraq_id`	The Bugtraq database identification number associated with the vulnerability.
`description`	A description of the vulnerability.
`host_id`	ID number of the host.
`invalid`	A value indicating whether the vulnerability is valid for the host: • `0` — Vulnerability is valid • `1` — Vulnerability is invalid
`ip_address`	Field deprecated in Version 5.2. Returns `null` for all queries.
`name`	The name, or title, of the vulnerability.
`port`	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
`protocol`	The traffic protocol (`TCP` or `UDP`), if the vulnerability is associated with an application using that protocol.
`source`	The source of the vulnerability.
`third_party_vuln_id`	The third-party identification number associated with the vulnerability.

rna_host_third_party_vuln_bugtraq_id Joins

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

Table 6-46 rna_host_third_party_vuln_bugtraq_id Joins

You can join this table on...	And...
bugtraq_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_bugtraq_id Sample Query

The following query returns the BugTraq vulnerabilities for the host with `host_id` of `8`.

```
SELECT host_id, third_party_vuln_id, bugtraq_id, name, description, source, invalid
FROM rna_host_third_party_vuln_bugtraq_id
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_cve_id

The **rna_host_third_party_vuln_cve_id** table contains information on the third-party vulnerabilities that are mapped to vulnerabilities in MITRE's CVE database and also associated with the hosts in your monitored network. Note that this table contains third-party vulnerability data imported via the host input feature.

For more information, see the following sections:

- rna_host_third_party_vuln_cve_id Fields, page 6-51
- rna_host_third_party_vuln_cve_id Joins, page 6-51

- rna_host_third_party_vuln_cve_id Sample Query, page 6-52

rna_host_third_party_vuln_cve_id Fields

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

Table 6-47 rna_host_third_party_vuln_cve_id Fields

Field	Description
cve_id	The identification number associated with the vulnerability in MITRE's CVE database.
description	A description of the vulnerability.
host_id	ID number of the host.
invalid	A value indicating whether the vulnerability is valid for the host: • 0 — Vulnerability is valid • 1 — Vulnerability is invalid
ip_address	Field deprecated in Version 5.2. Returns null for all queries.
name	The name, or title, of the vulnerability.
port	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
protocol	The traffic protocol (TCP or UDP), if the vulnerability is associated with an application using that protocol.
source	The source of the vulnerability.
third_party_vuln_id	The identification number associated with the vulnerability.

rna_host_third_party_vuln_cve_id Joins

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

Table 6-48 rna_host_third_party_vuln_cve_id Joins

You can join this table on...	And...
cve_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_cve_id Sample Query

The following query returns the CVE vulnerabilities for the host with `host_id` of `8`.

```
SELECT host_id, third_party_vuln_id, cve_id, name, description, source, invalid

FROM rna_host_third_party_vuln_cve_id

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_rna_id

The **`rna_host_third_party_vuln_rna_id`** table contains information on third-party vulnerabilities that are mapped to vulnerabilities in the Cisco vulnerability database (VDB) and also associated with hosts in your monitored network. Note that the third-party vulnerability data in this table is imported via the host input feature.

For more information, see the following sections:

- rna_host_third_party_vuln_rna_id Fields, page 6-53
- rna_host_third_party_vuln_rna_id Joins, page 6-53
- rna_host_third_party_vuln_rna_id Sample Query, page 6-54

rna_host_third_party_vuln_rna_id Fields

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

Table 6-49 rna_host_third_party_vuln_rna_id Fields

Field	Description
description	A description of the vulnerability.
host_id	ID number of the host.
invalid	A value indicating whether the vulnerability is valid for the host: • 0 — Vulnerability is valid • 1 — Vulnerability is invalid
ip_address	Field deprecated in Version 5.2. Returns null for all queries.
name	The name, or title, of the vulnerability.
port	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
protocol	The traffic protocol (TCP or UDP), if the vulnerability is associated with an application using that protocol.
rna_vuln_id	The vulnerability identification number that Cisco uses to track the vulnerability.
source	The source of the vulnerability.
third_party_vuln_id	The identification number associated with the vulnerability.

rna_host_third_party_vuln_rna_id Joins

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

Table 6-50 rna_host_third_party_vuln_rna_id Joins

You can join this table on...	And...
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os.rna_vuln_id rna_host_service_vulns.rna_vuln_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_rna_id Sample Query

The following query returns all third party vulnerabilities with VDB IDs for the host with `host_id` of `8`.

```
SELECT host_id, third_party_vuln_id, rna_vuln_id, name, description, source, invalid
FROM rna_host_third_party_vuln_rna_id
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_vuln

The **`rna_vuln`** table contains information on the vulnerabilities in the Cisco VDB.

For more information, see the following sections:

- rna_vuln Fields, page 6-54
- rna_vuln Joins, page 6-56
- rna_vuln Sample Query, page 6-56

rna_vuln Fields

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

Table 6-51 rna_vuln Fields

Field	Description
authentication	Whether authentication is required to exploit the vulnerability: • Required • Not Required • Unknown
availability	When the vulnerability can be exploited: • Always • User Initiated • Time Dependent • Unknown
available_exploits	Whether there are available exploits for the vulnerability: • TRUE • FALSE
bugtraq_id	The identification number associated with the vulnerability in the Bugtraq database.
class	The class of vulnerability: • Configuration Error • Boundary Condition Error • Design Error
credibility	How credible the vulnerability is: • Conflicting Reports • Conflicting Details • Single Source • Reliable Source • Multiple Sources • Vendor Confirmed
credit	The person or organization credited with reporting the vulnerability.
ease	The ease of exploiting the vulnerability: • No Exploit Required • Exploit Available • No Exploit Available
effect	Details on what could happen when the vulnerability is exploited.
entry_date	The date the vulnerability was entered in the database.
exploit	Information on where you can find exploits for the vulnerability.
impact	The vulnerability impact, corresponding to the impact level determined through correlation of intrusion data, discovery events, and vulnerability assessments. The value can be from 1 to 10, with 10 being the most severe. The impact value of a vulnerability is determined by the writer of the Bugtraq entry.

Table 6-51 rna_vuln Fields (continued)

Field	Description
local	Indicates whether the vulnerability must be exploited locally: • TRUE • FALSE
long_description	A general description of the vulnerability.
mitigation	A description of how you can mitigate the vulnerability.
modified_date	The date of the most recent modification to the vulnerability, if applicable.
publish_date	The date the vulnerability was published.
remote	Indicates whether the vulnerability can be exploited across a network: • TRUE • FALSE
rna_vuln_id	The Cisco vulnerability ID number that the system uses to track vulnerabilities.
scenario	A description of a scenario where an attacker is exploiting the vulnerability.
short_description	A summary description of the vulnerability.
snort_id	The identification number associated with the vulnerability in the Snort ID (SID) database. That is, if an intrusion rule can detect network traffic that exploits a particular vulnerability, that vulnerability is associated with the intrusion rule's SID.
solution	The solution to the vulnerability.
technical_description	The technical description of the vulnerability.
title	The title of the vulnerability.

rna_vuln Joins

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

Table 6-52 rna_vuln Joins

You can join this table on...	And...
rna_vuln_id or bugtraq_id	rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id

rna_vuln Sample Query

The following query returns information about up to 25 vulnerabilities. The records are sorted in order of most events generated based on the vulnerability.

```
SELECT rna_vuln_id, bugtraq_id, snort_id, title, publish_date, impact, remote, exploit,
long_description, technical_description, solution, count(*) as count

FROM rna_vuln
```

```
GROUP BY rna_vuln_id
ORDER BY rna_vuln_id DESC LIMIT 0, 25;
```

tag_info

The **tag_info** table contains information on the tags that are associated with the applications detected on your network. Note that an application can have multiple associated tags.

For more information, see the following sections:

- tag_info Fields, page 6-57
- tag_info Joins, page 6-57
- tag_info Sample Query, page 6-57

tag_info Fields

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

Table 6-53 tag_info Fields

Field	Description
tag_description	Tag description.
tag_id	Internal identifier for the tag.
tag_name	Text of the tag that appears in the user interface.
tag_type	One of the following: • category • tag

tag_info Joins

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

Table 6-54 tag_info Joins

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

tag_info Sample Query

The following query returns the application tag record for a selected tag ID.

```
SELECT tag_id, tag_name, tag_type, tag_description
FROM tag_info
WHERE tag_id="100";
```

url_categories

The **url_categories** table lists the categories that characterize URLs requested by hosts in your monitored network.

For more information, see the following sections:

- url_categories Fields, page 6-58
- url_categories Joins, page 6-58
- url_categories Sample Query, page 6-58

url_categories Fields

The following table describes the fields in the **url_categories** table.

Table 6-55 url_categories Fields

Field	Description
category_description	The description of the URL category.
category_id	The internal identification number of the URL category.

url_categories Joins

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

url_categories Sample Query

The following query returns a category record for the selected category ID.

```
SELECT category_id, category_description
FROM url_categories
WHERE category_id="1";
```

url_reputations

The **url_reputations** table lists the reputations that characterize URLs requested by hosts in your monitored request.

For more information, see the following sections:

- url_reputations Fields, page 6-59
- url_reputations Joins, page 6-59
- url_reputations Sample Query, page 6-59

url_reputations Fields

The following table describes the fields in the **url_reputations** table.

Table 6-56 url_reputations Fields

Field	Description
reputation_description	The description of the reputation.
reputation_id	An internal identification number for the URL reputation.

url_reputations Joins

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

url_reputations Sample Query

The following query returns URL reputation information for a reputation ID.

```
SELECT reputation_id, reputation_description
FROM url_reputations
WHERE reputation_id="1";
```

user_ipaddr_history

The **user_ipaddr_history** table contains information on user activity for a particular host in your monitored network.

For more information, see the following sections:

- user_ipaddr_history Fields, page 6-59
- user_ipaddr_history Joins, page 6-60
- user_ipaddr_history Sample Query, page 6-61

user_ipaddr_history Fields

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

Table 6-57 user_ipaddr_history Fields

Field	Description
end_time_sec	The UNIX timestamp of the date and time the FireSIGHT System detected a different user logging into the host, marking the assumed end of the previous user's session. Note that the FireSIGHT System does not detect logoffs.
id	An internal identification number for the user history record.
ipaddr	A binary representation of the IP address of the host.

Table 6-57 user_ipaddr_history Fields (continued)

Field	Description
start_time_sec	The UNIX timestamp of the date and time the FireSIGHT System detected the user logging into host.
user_dept	The department of the user.
user_email	The email address of the user.
user_first_name	The first name of the user.
user_id	An internal identification number for the user.
user_last_name	The last name of the user.
user_last_seen_sec	The UNIX timestamp of the date and time the FireSIGHT System last detected user activity for the user.
user_last_updated_sec	The UNIX timestamp of the date and time the FireSIGHT System last updated the user record for the user.
user_name	The user name of the user.
user_phone	The phone number of the user.
user_rna_service	Name of the application protocol being used when the user was detected, if available.

user_ipaddr_history Joins

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

Table 6-58 user_ipaddr_history Joins

You can join this table on...	And...
ipaddr	compliance_event.dst_ipaddr compliance_event.src_ipaddr connection_log.initiator_ipaddr connection_log.responder_ipaddr connection_summary.initiator_ipaddr connection_summary.responder_ipaddr fireamp_event.dst_ipaddr fireamp_event.src_ipaddr intrusion_event.dst_ipaddr intrusion_event.src_ipaddr network_discovery_event.ipaddr rna_host_ip_map.ipaddr si_connection_log.initiator_ipaddr si_connection_log.responder_ipaddr user_discovery_event.ipaddr white_list_event.ipaddr
user_id	discovered_users.user_id user_discovery_event.user_id

user_ipaddr_history Sample Query

The following query returns all user activity records for the selected IP address after the specified start timestamp.

```
SELECT ipaddr, start_time_sec, end_time_sec, user_name, user_rna_service,
user_last_seen_sec, user_last_updated_sec

FROM user_ipaddr_history

WHERE HEX(ipaddr) = "00000000000000000000FFFF0A0A0A04" AND start_time_sec >=
UNIX_TIMESTAMP("2011-10-01 00:00:00");
```