Connection and Security Intelligence Events

The following topics describe how to use connection and security events tables.

- About Connection Events, page 1
- Connection and Security Intelligence Event Fields, page 3
- Using Connection and Security Intelligence Event Tables, page 22
- Viewing the Connection Summary Page, page 26

About Connection Events

The system can generate logs of the connections its managed devices detect. These logs are called connection events. Settings in rules and policies give you granular control over which connections you log, when you log them, and where you store the data. Special connection events, called Security Intelligence events, represent connections blacklisted (blocked) by the reputation-based Security Intelligence feature. For detailed information, see Connection Logging.

Related Topics
- About Security Intelligence

Connection vs. Security Intelligence Events

A Security Intelligence event is a connection event that is generated whenever a session is blacklisted (blocked) or monitored by the reputation-based Security Intelligence feature.

However, for every Security Intelligence event, there is an identical connection event you can view and analyze Security Intelligence events independently. The system also stores and prunes Security Intelligence events separately.

Note that the system enforces Security Intelligence before more resource-intensive evaluations. When a connection is blocked by Security Intelligence, the resulting event does not contain the information that the system would have gathered from subsequent evaluation, for example, user identity.
NetFlow Connections

To supplement the connection data gathered by your managed devices, you can use records broadcast by NetFlow exporters to generate connection events. This is especially useful if the NetFlow exporters are monitoring different networks than those monitored by your managed devices.

The system logs NetFlow records as unidirectional end-of-connection events in the Firepower Management Center database. The available information for these connections differs somewhat from connections detected by your access control policy; see Differences between NetFlow and Managed Device Data.

Related Topics

- Netflow Data in the Firepower System

Connection Summaries (Aggregated Data for Graphs)

The Firepower System aggregates connection data collected over five-minute intervals into connection summaries, which the system uses to generate connection graphs and traffic profiles. Optionally, you can create custom workflows based on connection summary data, which you use in the same way as you use workflows based on individual connection events.

Note that there are no connection summaries specifically for Security Intelligence events, although corresponding end-of-connection events can be aggregated into connection summary data.

To be aggregated, multiple connections must:

- represent the end of connections
- have the same source and destination IP addresses, and use the same port on the responder (destination) host
- use the same protocol (TCP or UDP)
- use the same application protocol
- either be detected by the same Firepower System managed device or by the same NetFlow exporter

Each connection summary includes total traffic statistics, as well as the number of connections in the summary. Because NetFlow exporters generate unidirectional connections, a summary’s connection count is incremented by two for every connection based on NetFlow data.

Note that connection summaries do not contain all of the information associated with the summaries’ aggregated connections. For example, because client information is not used to aggregate connections into connection summaries, summaries do not contain client information.
Long-Running Connections

If a monitored session spans two or more five-minute intervals over which connection data is aggregated, the connection is considered a long-running connection. When calculating the number of connections in a connection summary, the system increments the count only for the five-minute interval in which a long-running connection was initiated.

Also, when calculating the number of packets and bytes transmitted by the initiator and responder in a long-running connection, the system does not report the number of packets and bytes that were actually transmitted during each five-minute interval. Instead, the system assumes a constant rate of transmission and calculates estimated figures based on the total number of packets and bytes transmitted, the length of the connection, and what portion of the connection occurred during each five-minute interval.

Combined Connection Summaries from External Responders

To reduce the space required to store connection data and speed up the rendering of connection graphs, the system combines connection summaries when:

- one of the hosts involved in the connection is not on your monitored network
- other than the IP address of the external host, the connections in the summaries meet the summary aggregation criteria

When viewing connection summaries in the event viewer and when working with connection graphs, the system displays external instead of an IP address for the non-monitored hosts.

As a consequence of this aggregation, if you attempt to drill down to the table view of connection data (that is, access data on individual connections) from a connection summary or graph that involves an external responder, the table view contains no information.

Connection and Security Intelligence Event Fields

Connection and Security Intelligence events, which you can view and search using tabular and graphical workflows, contain the fields described below. Keep in mind that the information available for any individual event can vary depending on how, why, and when the system logged the connection.

For each Security Intelligence event, there is an identical, separately stored connection event. All Security Intelligence events have a populated Security Intelligence Category field.

Because connection graphs are based on connection summaries, the same criteria that constrain connection summaries also constrain connection graphs. Fields marked with an asterisk (*) on search pages constrain connection graphs and connection summaries. If you search connection summaries using invalid search constraints and view your results using a connection summary page in a custom workflow, the invalid constraints are labeled as not applicable (N/A) and are marked with a strikethrough.

General Information

Access Control Policy

The access control policy that monitored the connection.
Access Control Rule

The access control rule or default action that handled the connection, as well as up to eight Monitor rules matched by that connection.

If the connection matched one Monitor rule, the Firepower Management Center displays the name of the rule that handled the connection, followed by the Monitor rule name. If the connection matched more than one Monitor rule, the event viewer displays how many Monitor rules it matched, for example, `Default Action + 2 Monitor Rules`.

To display a pop-up window with a list of the first eight Monitor rules matched by the connection, click `N Monitor Rules`.

Action

The action associated with the configuration that logged the connection.

For Security Intelligence-monitored connections, the action is that of the first non-Monitor access control rule triggered by the connection, or the default action. Similarly, because traffic matching a Monitor rule is always handled by a subsequent rule or by the default action, the action associated with a connection logged due to a Monitor rule is never Monitor. However, you can still trigger correlation policy violations on connections that match Monitor rules.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Connections either allowed by access control explicitly, or allowed because a user bypassed an interactive block.</td>
</tr>
<tr>
<td>Block, Block with reset</td>
<td>Blocked connections, including:</td>
</tr>
<tr>
<td></td>
<td>• connections blacklisted by Security Intelligence</td>
</tr>
<tr>
<td></td>
<td>• encrypted connections blocked by an SSL policy</td>
</tr>
<tr>
<td></td>
<td>• connections where an exploit was blocked by an intrusion policy</td>
</tr>
<tr>
<td></td>
<td>• connections where a file (including malware) was blocked by a file policy</td>
</tr>
<tr>
<td></td>
<td>For connections where the system blocks an intrusion or file, system displays <code>Block</code>, even though you use access control Allow rules to invoke deep inspection.</td>
</tr>
<tr>
<td>Interactive Block, Interactive Block with reset</td>
<td>Connections logged when the system initially blocks a user's HTTP request using an Interactive Block rule. If the user clicks through the warning page that the system displays, additional connections logged for the session have an action of Allow.</td>
</tr>
<tr>
<td>Trust</td>
<td>Connections trusted by access control. The system logs trusted TCP connections differently depending on the device model; see Logging for Trusted Connections.</td>
</tr>
<tr>
<td>Default Action</td>
<td>Connections handled by the access control policy's default action.</td>
</tr>
</tbody>
</table>
Connections

The number of connections in a connection summary. For long-running connections, that is, connections that span multiple connection summary intervals, only the first connection summary interval is incremented. To view meaningful results for searches using the Connections criterion, use a custom workflow that has a connection summary page.

Count

The number of connections that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows. If you create a custom workflow and do not add the Count column to a drill-down page, each connection is listed individually and packets and bytes are not summed.

Endpoint Location

The IP address of the network device that used ISE to authenticate the user, as identified by ISE.

Endpoint Profile

The user's endpoint device type, as identified by ISE.

First Packet or Last Packet

The date and time the first or last packet of the session was seen.

Initiator/Responder Bytes

The total number of bytes transmitted by the session initiator or session responder.

Initiator/Responder Packets

The total number of packets transmitted by the session initiator.

Initiator User (constrains summaries and graphs)

The user logged into the session initiator. If this field is populated with No Authentication, the user traffic:

- matched an access control policy without an associated identity policy
- did not match any rules in the identity policy

IOC

Whether the event triggered an indication of compromise (IOC) against a host involved in the connection.

Network Analysis Policy

The network analysis policy (NAP), if any, associated with the generation of the event.
Reason
The reason or reasons the connection was logged, in many situations. For a full list, see Connection Event Reasons, on page 16.

Connections with a Reason of IP Block, DNS Block, and URL Block have a threshold of 15 seconds per unique initiator-responder pair. After the system blocks one of those connections, it does not generate connection events for additional blocked connections between those two hosts for the next 15 seconds, regardless of port or protocol.

Security Context
For connections handled by ASA FirePOWER in multiple context mode, the metadata identifying the virtual firewall group through which the traffic passed.

Security Group Tag
The Security Group Tag (SGT) attribute of the packet involved in the connection. The SGT specifies the privileges of a traffic source within a trusted network. Security Group Access (a feature of both Cisco TrustSec and Cisco ISE) applies the attribute as packets enter the network.

Security Intelligence Category
The name of the blacklisted object that represents or contains the blacklisted IP address in the connection. The Security Intelligence category can be the name of a network object or group, a blacklist, a custom Security Intelligence list or feed, or one of the categories in the Intelligence Feed.

For more information about the categories in the Intelligence Feed, see Security Intelligence Options.

TCP Flags
For connections generated from NetFlow data, the TCP flags detected in the connection. When searching this field, enter a list of comma-separated TCP flags to view all connections that have at least one of those flags.

Time
The ending time of the five-minute interval that the system used to aggregate connections in a connection summary. This field is not searchable.

Traffic (KB) (search only)
The total amount of data transmitted in the connection, in kilobytes.

Total Packets (search only)
The total number of packets transmitted in the connection.

Networking
Destination Port/ICMP Code (constrains summaries and graphs)
The port or ICMP code used by the session responder.

DNS Query
The DNS query submitted in a connection to the name server to look up a domain name.
DNS Record Type
The type of the DNS resource record used to resolve a DNS query submitted in a connection.

DNS Response
The DNS response returned in a connection to the name server when queried.

DNS Sinkhole Name
The name of the sinkhole server where the system redirected a connection.

DNS TTL
The number of seconds a DNS server caches the DNS resource record.

HTTP Response Code
The HTTP status code sent in response to a client's HTTP request over a connection.

Ingress/Egress Security Zone
The ingress or egress security zone associated with the connection.

Initiator/Responder IP (constrains summaries and graphs)
The IP address (and host name, if DNS resolution is enabled) of the session initiator or responder. So that you can identify the blacklisted IP address in a blacklisted connection, host icons next to blacklisted IP addresses look slightly different.

Original Client IP
The original client IP address extracted from an X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header. To populate this field, you must enable the HTTP preprocessor Extract Original Client IP Address option in the network analysis policy. Also in the network analysis policy, you can specify up to six custom client IP headers, as well as set the priority order in which the system selects the value for the Original Client IP event field.

Protocol (constrains summaries and graphs, search only)
The transport protocol used in the connection. To search for a specific protocol, use the name or number protocol as listed in http://www.iana.org/assignments/protocol-numbers.

Source Port/ICMP Type (constrains summaries and graphs)
The port or ICMP type used by the session initiator.

VLAN ID
The innermost VLAN ID associated with the packet that triggered the connection.
Geolocation

Initiator/Responder Country
When a routable IP is detected, the country associated with the IP address of the session initiator or responder. The system displays an icon of the country’s flag, and the country’s ISO 3166-1 alpha-3 country code. Hover your pointer over the flag icon to view the country’s full name.

Initiator/Responder Continent
When a routable IP is detected, the continent associated with the IP address for the session initiator or responder.

Device

Device (constrains summaries and graphs)
The managed device that detected the connection or, for connections generated from NetFlow data, the managed device that processed the data.

Domain
The domain of the managed device that detected the connection or, for connections generated from NetFlow data, the domain of the managed device that processed the data. This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Ingress/Egress Interface
The ingress or egress interface associated with the connection. If your deployment includes an asynchronous routing configuration, the ingress and egress interface may belong to the same interface set.
SSL

SSL. Actual Action (search only)

The action the system applied to encrypted traffic in the SSL policy. The system displays field values in the SSL Status field on search workflow pages.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block/Block with reset</td>
<td>Represents blocked encrypted connections.</td>
</tr>
<tr>
<td>Decrypt (Resign)</td>
<td>Represents an outgoing connection decrypted using a re-signed server certificate.</td>
</tr>
<tr>
<td>Decrypt (Replace Key)</td>
<td>Represents an outgoing connection decrypted using a self-signed server certificate with a substituted public key.</td>
</tr>
<tr>
<td>Decrypt (Known Key)</td>
<td>Represents an incoming connection decrypted using a known private key.</td>
</tr>
<tr>
<td>Default Action</td>
<td>Indicates the connection was handled by the default action.</td>
</tr>
<tr>
<td>Do not Decrypt</td>
<td>Represents a connection the system did not decrypt.</td>
</tr>
</tbody>
</table>

SSL Certificate Status

This applies only if you configured a Certificate Status SSL rule condition. If encrypted traffic matches an SSL rule, this field displays one or more of the following server certificate status values:

- Self Signed
- Valid
- Invalid Signature
- Invalid Issuer
- Expired
- Unknown
- Not Valid Yet
- Revoked

If undecryptable traffic matches an SSL rule, this field displays Not Checked.
SSL Certificate Information (search only)

The information stored on the public key certificate used to encrypt traffic, including:

- Subject/Issuer Common Name
- Subject/Issuer Organization
- Subject/Issuer Organization Unit
- Not Valid Before/After
- Serial Number
- Certificate Fingerprint
- Public Key Fingerprint

SSL Cipher Suite

A macro value representing a cipher suite used to encrypt the connection. See [www.iana.org/assignments/tls-parameters/tls-parameters.xhtml](http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml) for cipher suite value designations.

SSL Encryption applied to the connection (search only)

Enter yes or no in the SSL search field to view SSL-encrypted or non-encrypted connections.

SSL Expected Action (search only)

The action the system expected to apply to encrypted traffic, given the SSL rules in effect. Enter any of the values listed for SSL Actual Action.
SSL Failure Reason

The reason the system failed to decrypt encrypted traffic:

- Unknown
- No Match
- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

Field values are displayed in the SSL Status field on the search workflow pages.
SSL Flow Error

The error name and hexadecimal code if an error occurred during the SSL session; Success if no error occurred.

SSL Flow Flags

The first ten debugging level flags for an encrypted connection. On a workflow page, to view all flags, click the ellipsis (...).

SSL Flow Messages

The keywords below indicate encrypted traffic is associated with the specified message type exchanged between client and server during the SSL handshake. See http://tools.ietf.org/html/rfc5246 for more information.

• HELLO_REQUEST
• CLIENT_ALERT
• SERVER_ALERT
• CLIENT HELLO
• SERVER_HELLO
• SERVER_CERTIFICATE
• SERVER_KEY_EXCHANGE
• CERTIFICATE_REQUEST
• SERVER_HELLO_DONE
• CLIENT_CERTIFICATE
• CLIENT_KEY_EXCHANGE
• CERTIFICATE_VERIFY
• CLIENT_CHANGE_CIPHER_SPEC
• CLIENT_FINISHED
• SERVER_CHANGE_CIPHER_SPEC
• SERVER_FINISHED
• NEW_SESSION_TICKET
• HANDSHAKE_OTHER
• APP_DATA_FROM_CLIENT
• APP_DATA_FROM_SERVER

SSL Policy

The SSL policy that handled the connection.
SSL Rule

The SSL rule or default action that handled the connection, as well as the first Monitor rule matched by that connection. If the connection matched a Monitor rule, the Firepower Management Center displays the name of the rule that handled the connection, followed by the Monitor rule name.

SSL Session ID

The hexadecimal Session ID negotiated between the client and server during the SSL handshake.

SSL Status

The action associated with the SSL Actual Action (SSL rule, default action, or undecryptable traffic action) that logged the encrypted connection. The lock icon links to SSL certificate details. If the certificate is unavailable (for example, for connections blocked due to SSL handshake error), the lock icon is dimmed.

If the system fails to decrypt an encrypted connection, it displays the SSL Actual Action (undecryptable traffic action) taken, as well as the SSL Failure Reason. For example, if the system detects traffic encrypted with an unknown cipher suite and allows it without further inspection, this field displays Do Not Decrypt (Unknown Cipher Suite).

When searching this field, enter one or more of the SSL Actual Action and SSL Failure Reason values to view encrypted traffic the system handled or failed to decrypt.

SSL Subject/Issuer Country (search only)

A two-character ISO 3166-1 alpha-2 country code for the subject or issuer country associated with the encryption certificate.

SSL Ticket ID

A hexadecimal hash value of the session ticket information sent during the SSL handshake.

SSL Version

The SSL or TLS protocol versions used to encrypt the connection:

- Unknown
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSv1.2

Application

Application Protocol (constrains summaries and graphs)

The application protocol, which represents communications between hosts, detected in the connection.
Application Protocol Category and Tag
Criteria that characterize the application to help you understand the application's function.

Application Risk
The risk associated with the application traffic detected in the connection: Very High, High, Medium, Low, or Very Low. Each type of application detected in the connection has an associated risk; this field displays the highest of those.

Business Relevance
The business relevance associated with the application traffic detected in the connection: Very High, High, Medium, Low, or Very Low. Each type of application detected in the connection has an associated business relevance; this field displays the lowest (least relevant) of those.

Client and Client Version
The client application and version of that client detected in the connection.
If the system cannot identify the specific client used in the connection, the field displays the word "client" appended to the application protocol name to provide a generic name, for example, FTP client.

Client Category and Tag
Criteria that characterize the application to help you understand the application's function.

HTTP Referrer
The HTTP referrer, which represents the referrer of a requested URL for HTTP traffic detected in the connection (such as a website that provided a link to, or imported a link from, another URL).

Referenced Host
If the protocol in the connection is HTTP or HTTPS, this field displays the host name that the respective protocol was using.

User Agent
The user-agent string application information extracted from HTTP traffic detected in the connection.

Web Application
The web application, which represents the content or requested URL for HTTP traffic detected in the connection.
If the web application does not match the URL for the event, the traffic is probably referred traffic, such as advertisement traffic. If the system detects referred traffic, it stores the referring application (if available) and lists that application as the web application.
If the system cannot identify the specific web application in HTTP traffic, this field displays Web Browsing.

Web Application Category and Tag
Criteria that characterize the application to help you understand the application's function.
URL

URL, URL Category, and URL Reputation

The URL requested by the monitored host during the session and its associated category and reputation, if available.

If the system identifies or blocks an SSL application, the requested URL is in encrypted traffic, so the system identifies the traffic based on an SSL certificate. For SSL applications, therefore, this field indicates the common name contained in the certificate.

NetFlow

NetBIOS Domain

The NetBIOS domain used in the session.

NetFlow Source/Destination Autonomous System

For connections generated from NetFlow data, the border gateway protocol autonomous system number for the source or destination of traffic in the connection.

NetFlow Source/Destination Prefix

For connections generated from NetFlow data, the source or destination IP address ANDed with the source or destination prefix mask.

NetFlow Source/Destination TOS

For connections generated from NetFlow data, the setting for the type-of-service (TOS) byte when connection traffic entered or exited the NetFlow exporter.

NetFlow SNMP Input/Output

For connections generated from NetFlow data, the interface index for the interface where connection traffic entered or exited the NetFlow exporter.

Source Device (constrains summaries and graphs)

The IP address of the NetFlow exporter that broadcast the data used to generate for the connection. If the connection was detected by a managed device, this field displays Firepower.

Associated Events

You cannot use the connection/Security Intelligence events Search page to search for events associated with a connection.

Files

The file events, if any, associated with the connection. The view files icon links to a list of files. The number on the icon indicates the number of files (including malware files) detected or blocked in that connection.
Intrusion Events

The intrusion events, if any, associated with the connection. The view intrusion events icon links to a list of events.

Connection Event Reasons

The Reason field in a connection event displays the reason or reasons the connection was logged, in the following situations:

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Block</td>
<td>The system denied the connection without inspection, based on the domain name and Security Intelligence data. A reason of DNS Block is paired with an action of Block, Domain not found, or Sinkhole, depending on the DNS rule action.</td>
</tr>
<tr>
<td>DNS Monitor</td>
<td>The system would have denied the connection based on the domain name and Security Intelligence data, but you configured the system to monitor, rather than deny, the connection.</td>
</tr>
<tr>
<td>File Block</td>
<td>The connection contained a file or malware file that the system prevented from being transmitted. A reason of File Block is always paired with an action of Block.</td>
</tr>
<tr>
<td>File Custom Detection</td>
<td>The connection contained a file on the custom detection list that the system prevented from being transmitted.</td>
</tr>
<tr>
<td>File Monitor</td>
<td>The system detected a particular type of file in the connection.</td>
</tr>
<tr>
<td>File Resume Allow</td>
<td>File transmission was originally blocked by a Block Files or Block Malware file rule. After a new access control policy allowing the file was deployed, the HTTP session automatically resumed. This reason only appears in inline deployments.</td>
</tr>
<tr>
<td>File Resume Block</td>
<td>File transmission was originally allowed by a Detect Files or Malware Cloud Lookup file rule. After a new access control policy blocking the file was deployed, the HTTP session automatically stopped. This reason only appears in inline deployments.</td>
</tr>
<tr>
<td>Intelligent App Bypass</td>
<td>The Intelligent Application Bypass (IAB) mode:</td>
</tr>
<tr>
<td></td>
<td>• If the action is Trust, IAB was in bypass mode. Matching traffic passed without further inspection.</td>
</tr>
<tr>
<td></td>
<td>• If the action is Allow, IAB was in test mode. Matching traffic was available for further inspection.</td>
</tr>
<tr>
<td>Intrusion Block</td>
<td>The system blocked or would have blocked an exploit (intrusion policy violation) detected in the connection. A reason of Intrusion Block is paired with an action of Block for blocked exploits and Allow for would-have-blocked exploits.</td>
</tr>
<tr>
<td>Intrusion Monitor</td>
<td>The system detected, but did not block, an exploit detected in the connection. This occurs when the state of the triggered intrusion rule is set to Generate Events.</td>
</tr>
</tbody>
</table>
### Requirements for Populating Connection Event Fields

The information available for a connection event, Security Intelligence event, or connection summary depends on several factors.

#### Appliance Model and License

Many features require that you enable specific licensed capabilities on target devices, and many features are only available on some models.

For example, NGIPSv devices do not support SSL inspection. They cannot inspect encrypted traffic; logged connection events do not contain information about encrypted connections.

#### Traffic Characteristics

The system only reports information present (and detectable) in network traffic. For example, there could be no user associated with an initiator host, or no referenced host detected in a connection where the protocol is not DNS, HTTP, or HTTPS.

#### Origin/Detection Method: Traffic-Based Detection vs NetFlow

With the exception of NetFlow-only fields, the information available in NetFlow records is more limited than the information generated by traffic-based detection; see Differences between NetFlow and Managed Device Data.
Evaluation Stage
Each type of traffic inspection and control occurs where it makes the most sense for maximum flexibility and performance.

For example, the system enforces Security Intelligence before more resource-intensive evaluations. When a connection is blocked by Security Intelligence, the resulting event does not contain the information that the system would have gathered from subsequent evaluation, for example, user identity.

Logging Method: Beginning or End of Connection
When the system detects a connection, whether you can log it at its beginning or its end (or both) depends on how you configure the system to detect and handle it.

Beginning-of-connection events do not have information that must be determined by examining traffic over the duration of the session (for example, the total amount of data transmitted or the timestamp of the last packet in the connection). Beginning-of-connection events are also not guaranteed to have information about application or URL traffic in the session, and do not contain any details about the session’s encryption. Beginning-of-connection logging is usually the only option for blocked connections.

Connection Event Type: Individual vs Summary
Connection summaries do not contain all of the information associated with their aggregated connections. For example, because client information is not used to aggregate connections into connection summaries, summaries do not contain client information.

Keep in mind that connection graphs are based on connection summary data, which use only end-of-connection logs. If your system is configured to log only beginning-of-connection data, connection graphs and connection summary event views contain no data.

Other Configurations
Other configurations that affect connection logging include, but are not limited to:

• ISE-related fields are populated only if you configure ISE, in connections associated with users who authenticate via an Active Directory domain controller. Connection events do not contain ISE data for users who authenticate via LDAP, RADIUS, or RSA domain controllers.

• SSL-related fields are populated only in encrypted connections handled by an SSL policy.

• File information fields are populated only in connections logged by access control rules associated with file policies.

• Intrusion information fields are populated only in connections logged by access control rules either associated with intrusion policies or using the default action.

• The Reason field is populated only in specific situations, such as when a user bypasses an Interactive Block configuration.

• The Domain field is only present if you have ever configured the Firepower Management Center for multitenancy.

• An advanced setting in the access control policy controls the number of characters the system stores in the connection log for each URL requested by monitored hosts in HTTP sessions. If you use this setting to disable URL logging, the system does not display individual URLs in the connection log, although you can still view category and reputation data, if it exists.
Related Topics

Differences between NetFlow and Managed Device Data

Information Available in Connection Event Fields

The table in this topic indicates when the system can populate connection and Security Intelligence fields. The columns in the table represent the following event types:

- **Origin: Direct**—Events that represent connections detected and handled by a Firepower System managed device.
- **Origin: NetFlow**—Events that represent connections exported by a NetFlow exporter.
- **Logging: Start**—Events that represent connections logged at their beginning.
- **Logging: End**—Events that represent connections logged at their end.

A "yes" in the table does not mean that the system must populate a connection event field, rather, that it can. The system only reports information present (and detectable) in network traffic. For example, SSL-related fields are populated only for records of encrypted connections handled by an SSL policy.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Policy</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Access Control Rule</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Action</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Application Protocol</td>
<td>yes</td>
<td>yes</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Application Protocol Category &amp; Tag</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Application Risk</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Business Relevance</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Client</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Client Category &amp; Tag</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Client Version</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Connections</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Count</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Destination Port/ICMP Type</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Device</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Domain</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>DNS Query</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>DNS Record Type</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>DNS Response</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>DNS Sinkhole Name</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>DNS TTL</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Egress Interface</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Egress Security Zone</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Endpoint Location</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Endpoint Profile</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Files</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>First Packet</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP Referrer</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP Response Code</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Ingress Interface</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Ingress Security Zone</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Initiator Bytes</td>
<td>yes</td>
<td>yes</td>
<td>not useful</td>
<td>yes</td>
</tr>
<tr>
<td>Initiator Country</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Initiator IP</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Initiator Packets</td>
<td>yes</td>
<td>yes</td>
<td>not useful</td>
<td>yes</td>
</tr>
<tr>
<td>Initiator User</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Intrusion Events</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Intrusion Policy</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>IOC (Indication of Compromise)</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
### Connection Event Field

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Packet</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>NetBIOS Domain</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>NetFlow Source/Destination Autonomous System</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>NetFlow Source/Destination Prefix</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>NetFlow Source/Destination TOS</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>NetFlow SNMP Input/Output</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Network Analysis Policy</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Reason</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Referenced Host</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Responder Bytes</td>
<td>yes</td>
<td>yes</td>
<td>not useful</td>
<td>yes</td>
</tr>
<tr>
<td>Responder Country</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Responder IP</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Responder Packets</td>
<td>yes</td>
<td>yes</td>
<td>not useful</td>
<td>yes</td>
</tr>
<tr>
<td>Security Context (ASA only)</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Security Group Tag (SGT)</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Security Intelligence Category</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Source Device</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Source Port/ICMP Type</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Certificate Status</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Cipher Suite</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Flow Error</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Flow Flags</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Flow Messages</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Policy</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
### Using Connection and Security Intelligence Event Tables

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Rule</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Session ID</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Status</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SSL Version</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>TCP Flags</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Time</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>URL</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>URL Category</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>URL Reputation</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>User Agent</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Web Application</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
<tr>
<td>Web Application Category &amp; Tag</td>
<td>yes</td>
<td>no</td>
<td>if available</td>
<td>yes</td>
</tr>
</tbody>
</table>

You can use the Firepower Management Center to view a table of connection or Security Intelligence events. Then, you can manipulate the event view depending on the information you are looking for.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

The page you see when you access connection graphs differs depending on the workflow you use. You can use a predefined workflow, which terminates in a table view of events. You can also create a custom workflow that displays only the information that matches your specific needs.

When you are using a connection or Security Intelligence workflow table, you can perform many common actions.
Note that when you constrain connection events on a drill-down page, the packets and bytes from identical events are summed. However, if you are using a custom workflow and did not add a **Count** column to a drill-down page, the events are listed individually and packets and bytes are not summed.

**Procedure**

**Step 1** Choose either of the following:

- **Analysis > Connections > Events** (for connection events)
- **Analysis > Connections > Security Intelligence Events**

**Note** If a connection graph appears instead of a table, click (switch workflow) by the workflow title, and choose the predefined **Connection Events** workflow, or a custom workflow. Note that all predefined connection event workflows—including connection graphs—terminate in a table view of connections.

**Step 2** You have the following choices:

- **Time Range** — To adjust the time range, which is useful if no events appear, see Changing the Time Window.
- **Field Names** — To learn more about the contents of the columns in the table, see Connection and Security Intelligence Event Fields, on page 3.
  
  **Tip** In the table view of events, several fields are hidden by default, including the Category and Tag fields for each type of application, NetFlow-related fields, SSL-related fields, and others. To show a hidden field in an event view, expand the search constraints, then click the field name under Disabled Columns.

- **Host Profile** — To view the host profile for an IP address, click the host profile icon ( ), or, for hosts with active indications of compromise (IOC) tags, the compromised host icon ( ) that appears next to the IP address.

- **User Profile** — To view user identity information, click the user icon that appears next to the user identity ( ).

- **Files and Malware** — To view the files, including malware, detected or blocked in a connection, click the view files icon ( ) and proceed as described in Viewing Files and Malware Detected in a Connection, on page 24.

- **Intrusion Events** — To view the intrusion events associated with a connection, as well as their priority and impact, click the intrusion events icon ( ) in the **Intrusion Events** column and proceed as described in Viewing Intrusion Events Associated with a Connection, on page 25.
  
  **Tip** To quickly view intrusion, file, or malware events associated with one or more connections, check the connections using the check boxes in the event viewer, then choose the appropriate option from the **Jump to** drop-down list. Note that because they are blocked before access control rule evaluation, there can be no files or intrusions associated with connections blacklisted by Security Intelligence. You can only see this information for a Security Intelligence event if you configured Security Intelligence to monitor, rather than blacklist, connections.

- **Certificate** — To view details about an available certificate used to encrypt a connection, click an enabled lock icon ( ) in the **SSL Status** column.
• Constrain — To constrain the columns that appear, click the close icon (×) in the column heading that you want to hide. In the pop-up window that appears, click Apply.

 Tip To hide or show other columns, check or clear the appropriate check boxes before you click Apply. To add a disabled column back to the view, expand the search constraints, then click the column name under Disabled Columns.

• Delete Events — To delete some or all items in the current constrained view, check the check boxes next to items you want to delete and click Delete or click Delete All.

• Drill Down — See Using Drill-Down Pages.

 Tip To drill down using one of several Monitor rules that matched a logged connection, click an N Monitor Rules value. In the pop-up window that appears, click the Monitor rule you want to use to constrain connection events.

• Navigate This Page — See Workflow Page Traversal Tools.

• Navigate Between Pages — To navigate between pages in the current workflow, keeping the current constraints, click the appropriate page link at the top left of the workflow page.

• Navigate Between Event Views — To navigate to other event views to view associated events, click Jump to and choose the event view from the drop-down list.

• Sort — To sort data in a workflow, click the column title. Click the column title again to reverse the sort order.

Related Topics

Overview: Workflows
Configuring Event View Settings

Viewing Files and Malware Detected in a Connection

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat or Malware</td>
<td>Protection or Malware</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Any Security Analyst</td>
</tr>
</tbody>
</table>

If you associate a file policy with one or more access control rules, the system can detect files (including malware) in matching traffic. Using the event viewer, you can see the file events, if any, associated with the connections logged by those rules. Instead of a list of files, the Firepower Management Center displays the view files icon (⋮) in the Files column. The number on the icon indicates the number of files (including malware files) detected or blocked in that connection.

Not all file and malware events are associated with connections. Specifically:

• Endpoint-based malware events are not associated with connections. Those events are imported from your AMP for Endpoints deployment.
Many IMAP-capable email clients use a single IMAP session, which ends only when the user exits the application. Although long-running connections are logged by the system, files downloaded in the session are not associated with the connection until the session ends.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

**Procedure**

**Step 1**
While using a connection event table, click the view files icon (9). A pop-up window appears with a list of the files detected in the connection as well as their types, and if applicable, their malware dispositions.

**Step 2**
You have the following choices:

- View — To view a table view of file events, click a file's view icon (9).
- View — To view details in a table view of malware events, click a malware file's view icon (9).
- Track — To track the file's transmission through your network, click a file's trajectory icon (9).
- View — To view details on all of the connection's detected file or network-based malware events, click View File Events or View Malware Events.

### Viewing Intrusion Events Associated with a Connection

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Any Security Analyst</td>
</tr>
</tbody>
</table>

If you associate an intrusion policy with an access control rule or default action, the system can detect exploits in matching traffic. Using the event viewer, you can see the intrusion events, if any, associated with logged connections, as well as their priority and impact.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

**Procedure**

**Step 1**
While using a connection event table, click the intrusion events icon (1) in the **Intrusion Events** column.

**Step 2**
In the pop-up window that appears, you have the following options:

- Click a listed event's view icon (1) to view details in the packet view.
• Click **View Intrusion Events** to view details on all of the connection’s associated intrusion events.

---

## Encrypted Connection Certificate Details

You can use the event viewer to display the public key certificate (if available) used to encrypt a connection handled by the system. The certificate contains the following information.

**Table 1: Encrypted Connection Certificate Details**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject/Issuer Common Name</td>
<td>The host and domain name of the certificate subject or certificate issuer.</td>
</tr>
<tr>
<td>Subject/Issuer Organization</td>
<td>The organization of the certificate subject or certificate issuer.</td>
</tr>
<tr>
<td>Subject/Issuer Organization Unit</td>
<td>The organizational unit of the certificate subject or certificate issuer.</td>
</tr>
<tr>
<td>Not Valid Before/After</td>
<td>The dates when the certificate is valid.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number assigned by the issuing CA.</td>
</tr>
<tr>
<td>Certificate Fingerprint</td>
<td>The SHA hash value used to authenticate the certificate.</td>
</tr>
<tr>
<td>Public Key Fingerprint</td>
<td>The SHA hash value used to authenticate the public key contained within the certificate.</td>
</tr>
</tbody>
</table>

---

## Viewing the Connection Summary Page

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Custom</td>
</tr>
</tbody>
</table>

The Connection Summary page is visible only to users who have custom roles that are restricted by searches on connection events and who have been granted explicit menu-based access to the Connection Summary page. This page provides graphs of the activity on your monitored network organized by different criteria. For example, the Connections over Time graph displays the total number of connections on your monitored network over the interval that you choose.

You can perform almost all the same actions on connection summary graphs that you can perform on connection graphs. However, because the graphs on the Connection Summary page are based on aggregated data, you cannot examine the individual connection events on which the graphs are based. In other words, you cannot drill down to a connection data table view from a connection summary graph.
In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

**Procedure**

**Step 1** Choose Overview > Summary > Connection Summary.

**Step 2** From the Select Device list, choose the device whose summary you want to view, or choose All to view a summary of all devices.

**Step 3** To manipulate and analyze the connection graphs, proceed as described in Using Connection Event Graphs. Tip To detach a connection graph so you can perform further analysis without affecting the default time range, click View.

**Related Topics**

User Role Escalation