

Connection and Security-Related Connection Events

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

- Connection events, on page 1
- Connection and Security-Related Connection Event Fields, on page 4
- View Connection and Security-Related Connection Event Tables , on page 27
- View the connection summary page, on page 32
- History for Connection and Security Intelligence Events, on page 33

Connection events

A connection event is a log that records connections that your managed devices monitor. It includes *Security-Related connection events*. These are connections that the reputation-based Security Intelligence feature blocks. It also provides granular control over which connections to log, when to log them, and where to store the data.

Connection event detection sources

Connection events generally include transactions detected by:

- Access control policies
- Decryption policies
- Prefilter policies (captured by prefilter or tunnel rules)
- DNS Block lists
- URL Block lists
- Network (IP address) Block lists

Settings in rules and policies give you granular control over which connections you log, when you log them, and where you store the data.

For more information, refer to Connection Logging.

Related Topics

Security intelligence

Connection vs. security-related connection events

A *Security-Related connection event* is a connection event that

- is generated whenever a session is blocked or monitored by the reputation-based Security Intelligence feature, and
- has an identical corresponding connection event that can be viewed and analyzed independently.

Event processing and storage

The system creates an identical connection event for every Security-Related connection event. You can view and analyze Security-Related connection events independently. The system stores and prunes these events separately.

The system enforces Security Intelligence before more resource-intensive evaluations. When Security Intelligence blocks a connection, the resulting event lacks information from subsequent evaluations, such as user identity.

Note In this guide, information about connection events also pertains to Security-Related connection events, unless otherwise noted.

NetFlow connections

NetFlow connections are unidirectional end-of-connection events that

- supplement connection data gathered by managed devices,
- are generated from records broadcast by NetFlow exporters, and
- are logged in the Secure Firewall Management Center database.

NetFlow connection characteristics

The system logs NetFlow records as unidirectional end-of-connection events in the Secure Firewall Management Center database. The available information for these connections differs somewhat from connections detected by your access control policy. For more information, refer to Differences between NetFlow and managed device data.

Related Topics

NetFlow data

Connection summaries (aggregated data for graphs)

Connection summaries are collections of aggregated data that

- aggregate connection data over 5-minute intervals,

- generate connection graphs and traffic profiles, and
- support custom workflows based on connection summary data.

The 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.

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 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. NetFlow exporters generate unidirectional connections. The system increments a summary's connection count by 2 for every NetFlow-based connection.

There are no connection summaries specifically for Security-Related connection events, although the system can aggregate corresponding end-of-connection events into connection summary data.

Note Connection summaries do not contain all 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.

Long-running connections

A long-running connection is a monitored session that

- spans two or more five-minute intervals during which the system aggregates connection data,
- increases the connection count only when the session starts, and
- uses estimated calculations based on constant rates rather than actual data for each interval.

Connection counting and traffic calculation behavior

When the system calculates the number of packets and bytes for long-running connections, it does not report actual transmission data for each five-minute interval. Instead, it uses a constant transmission rate and calculates estimates based on the total number of packets and bytes transmitted, connection length, and the connection portion in each interval.

Combined connection summaries from external responders

A combined connection summary is a data optimization technique that

- reduces connection data storage space by aggregating summaries when one host is not on the monitored network,
- improves connection graph rendering performance by combining connections that meet summary aggregation criteria, and
- displays `external` instead of an IP address for non-monitored hosts in connection summaries and graphs.

Aggregation criteria and display behavior

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
- except for the IP address of the external host, the connections in the summaries meet the summary aggregation criteria

When viewing connection summaries in the **Events & Logs** > **+ Show more** > **Connection** submenu pages, and when working with connection graphs, the system displays `external` instead of an IP address for the non-monitored hosts.

Note 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-Related Connection Event Fields

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

Access Control Policy (Syslog: ACPolicy)

The access control policy that monitored the connection.

Access Control Rule (Syslog: AccessControlRuleName)

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 Firewall 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 number of matching Monitor rules is displayed, 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 (Syslog: AccessControlRuleAction)

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.

Action	Description
Allow	Connections either allowed by access control explicitly, or allowed because a user bypassed an interactive block.
Block, Block with reset	Blocked connections, including: • tunnels and other connections blocked by the prefilter policy • connections blocked by Security Intelligence. • encrypted connections blocked by an SSL policy. • connections where an exploit was blocked by an intrusion policy. • connections where a file (including malware) was blocked by a file policy. For connections where the system blocks an intrusion or file, system displays `Block`, even though you use access control Allow rules to invoke deep inspection.
Fastpath	Non-encrypted tunnels and other connections fastpathed by the prefilter policy.
Interactive Block, Interactive Block with reset	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.
Trust	Connections trusted by access control. The system logs trusted TCP connections differently depending on the device model.
Default Action	Connections handled by the access control policy's default action.
(Blank/empty)	The connection closed before enough packets had passed to match a rule. This can happen only if a facility other than access control, such as intrusion prevention, causes the connection to be logged.

Application Protocol (Syslog: ApplicationProtocol)

In the Firewall Management Center web interface, this value 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.

Authentication Source

Contains one of the following values based on which type of authentication is being used:

- **Passive Identity Source** for the Passive Identity Agent
- **SAML Captive Portal** for the Azure AD (SAML) realm configured to be a captive portal

For more information, refer to the *Cisco Secure Firewall Management Center Device Configuration Guide*.

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 (Syslog: Client, ClientVersion)

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.

Connection Counter (Syslog Only)

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Connection Instance ID (Syslog Only)

The Snort instance that processed the connection event. This field has no significance on its own.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

ConnectionDuration (Syslog Only)

This field exists only as a syslog field; it does not exist in the Firewall Management Center web interface. (The web interface conveys this information using the First Packet and Last Packet columns.)

This field has a value only when logging occurs at the end of the connection. For a start-of-connection syslog message, this field is not output, as it is not known at that time.

For an end-of-connection syslog message, this field indicates the number of seconds between the first packet and the last packet, which may be zero for a short connection. For example, if the timestamp of the syslog is 12:34:56 and the ConnectionDuration is 5, then the first packet was seen at 12:34:51.

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.

Decrypt Peer

The IP address of the VPN peer (peer's IKE address) which decrypts the packet for the associated connection.

You must enable logging setting for access control policy rule to log at the beginning of connection and end of connection to view the VPN peer IP address. If you enable the bypass Access Control Policy for decrypted traffic (sysopt connection permit-vpn) option, you cannot view details for decrypted traffic.

Decryption Policy (Syslog: SSLPolicy)

The decryption policy that handled the connection.

If TLS server identity discovery is enabled in the access control policy advanced settings, and there is no decryption policy associated with the access control policy, this field holds `none` for all decryption events.

Decryption Rule (Syslog: SSLRuleName)

The decryption 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 field displays the name of the rule that handled the connection, followed by the monitor rule name.

Detection Type (Syslog: DetectionType)

This field shows the source of detection of a client application. It displays **AppID** or **Encrypted Visibility** when:

- The Encrypted Visibility Engine identifies the client application from TLS traffic, this field displays **Encrypted Visibility Engine**.

  This field displays **Encrypted Visibility Engine** also when the client application is identified from SSH or STUN protocol traffic.

- Applications are not to process names, this field displays **AppID**, indicating that the engine that identified the client application was AppID.

Destination Port/ICMP Code (Syslog: Separate fields - DstPort, ICMPCode)

In the Firewall Management Center web interface, these values constrain summaries and graphs.

The port or ICMP code used by the session responder.

DestinationSecurityGroup (Syslog Only)

This field holds the text value associated with the numeric value in **DestinationSecurityGroupTag**, if available. If the group name is not available as a text value, then this field contains the same integer value as the DestinationSecurityGroupTag field.

DestinationSecurityGroupType (Syslog Only)

This field displays the source from which a security group tag was obtained.

Value	Description
Inline	Destination SGT value is from packet
Session Directory	Destination SGT value is from ISE via session directory topic
SXP	Destination SGT value is from ISE via SXP topic

Destination SGT (Syslog: DestinationSecurityGroupTag)

The numeric Security Group Tag (SGT) attribute of the destination involved in the connection.

The Destination SGT value is obtained from the source specified in the **DestinationSecurityGroupType** field.

Device

In the Firewall Management Center web interface, this value 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.

DeviceUUID (Syslog Only)

The unique identifier of the firewall device that generated an event.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

DNS Query (Syslog: DNSQuery)

The DNS query submitted in a connection to the name server to look up a domain name.

This field can also hold the domain name for URL filtering matches when DNS filtering is enabled. In this case, the URL field will be blank and the URL Category and URL Reputation fields contain the values associated with the domain.

For more information about DNS filtering, refer to DNS filtering.

DNS Record Type (Syslog: DNSRecordType)

The type of the DNS resource record used to resolve a DNS query submitted in a connection.

DNS Response (Syslog: DNSResponseType)

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

DNS Sinkhole Name (Syslog: DNS_Sinkhole)

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

DNS TTL (Syslog: DNS_TTL)

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

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 Firewall Management Center for multitenancy.

Encrypt Peer

The IP address of the VPN peer (peer's IKE address) which encrypts the packet for the associated connection.

You must enable logging setting for access control policy rule to log at the beginning of connection and end of connection to view the VPN peer IP address.

EVE Fingerprint (Syslog: EncryptedVisibilityFingerprint)

The fingerprint detected by the Encrypted Visibility Engine (EVE) for the session. EVE analyzes the initial handshake of encrypted protocols to generate a unique fingerprint for the session.

For TLS-based sessions, the fingerprint is derived from the TLS client hello packet.

For SSH sessions, the fingerprint is derived from the SSH key exchange initiation. Note that SSH fingerprints are typically longer than TLS fingerprints. For STUN sessions, the fingerprint is derived from the STUN binding request attributes.

Access to view additional details on the Secure Firewall Application Detectors page is currently available to users with Cisco email addresses.

EVE Process Name (Syslog: EncryptedVisibilityProcessName)

The process or client application identified by the Encrypted Visibility Engine (EVE) during its analysis of the encrypted session's initial handshake.

For TLS sessions, this is derived from the TLS client hello packet.

For SSH and STUN sessions, the process name is derived from the respective protocol handshakes. The identified process names for SSH and STUN are mapped to known applications via AppID for policy enforcement.

EVE Process Confidence Score (Syslog: EncryptedVisibilityConfidenceScore)

The confidence value in the range 0-100% that the encrypted visibility engine has detected the right process. For example, if the process name is Firefox and if the confidence score is 80%, it means that the engine is 80% confident that the process it has detected is Firefox.

EVE Threat Confidence (Syslog: EncryptedVisibilityThreatConfidence)

The probability level that the process detected by the encrypted visibility engine contains threat. This field indicates the bands (Very High, High, Medium, Low, or Very Low) based on the value in the threat confidence score.

EVE Threat Confidence Score (Syslog: EncryptedVisibilityThreatConfidenceScore)

The confidence value in the range 0-100% that the process detected by the encrypted visibility engine contains threat. If the threat confidence score is very high, say 90%, then the Encrypted Visibility Process Name field displays "Malware."

Endpoint Location

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

Endpoint Profile (Syslog: Endpoint Profile)

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

Event Priority (Syslog Only)

Whether or not the connection event is a high priority event. `High` priority events are connection events that are associated with an intrusion, Security Intelligence, file, or malware event. All other events are `Low` priority.

Files (Syslog: FileCount)

The number of files (including malware files) detected or blocked in a connection associated with one or more file events.

In the Firewall Management Center web interface, 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.

First Packet or Last Packet (Syslog: See the ConnectionDuration field)

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

First Packet Time (Syslog Only)

The time the system encountered the first packet.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

HTTP Referrer (Syslog: HTTPReferer)

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).

HTTP Response Code (Syslog: HTTPResponse)

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

Ingress/Egress Interface (Syslog: IngressInterface, EgressInterface)

The ingress or egress interface associated with the connection. If your deployment includes an asymmetric routing configuration, the ingress and egress interface may not belong to the same inline pair.

Ingress/Egress Security Zone (Syslog: IngressZone, EgressZone)

The ingress or egress security zone associated with the connection.

For rezoned encapsulated connections, the ingress field displays the tunnel zone you assigned, instead of the original ingress security zone. The egress field is blank.

Ingress Virtual Router/Egress Virtual Router (Syslog: IngressVRF, EgressVRF)

In networks using virtual routing, the names of the virtual routers through which traffic entered and exited the network.

Initiator/Responder Bytes (Syslog: InitiatorBytes, ResponderBytes)

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

Initiator/Responder Continent

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

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 IP (Syslog: SrcIP, DstIP)

In the Firewall Management Center web interface, these values constrain summaries and graphs.

The IP address (and host name, if DNS resolution is enabled) of the session initiator or responder.

See also Initiator and responder, source and destination, and sender and receiver fields, on page 22.

In the Firewall Management Center web interface, the host icon identifies the IP address that caused the connection to be blocked.

For plaintext, passthrough tunnels either blocked or fastpathed by the prefilter policy, initiator and responder IP addresses represent the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.

Initiator/Responder Packets (Syslog: InitiatorPackets, ResponderPackets)

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

Initiator User (Syslog: User)

In the Firewall Management Center web interface, this value 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

If applicable, the username is preceded by `<realm>\`.

See also Initiator and responder, source and destination, and sender and receiver fields, on page 22.

Inspection Duration (Syslog: InspectionMicroseconds)

Total time taken to inspect packets associated with a connection, in microseconds. The duration is measured from the initial packet reception to the completion of the inspection process. This value helps to determine the complete processing time spent on inspecting packets for each connection.

Inspection Packets (Syslog: InspectedPacketCount)

Total number of packets that have been inspected for a specific connection.

Intrusion Events (Syslog: IPSCount)

The number of intrusion events, if any, associated with the connection.

In the Firewall Management Center web interface, the **View Intrusion Events icon** links to a list of events.

IOC

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

MITRE ATT&CK

Progression graph for viewing the progress of an attack in the ATT&CK framework at any given time during an event. Supports an expanded view in a new pane, detailing MITRE tactics, techniques, and progression graphs.

- Click the progression graph to see the details of the MITRE ATT&CK for an event. The MITRE ATT&CK window shows the tactic, technique, subtechnique, and the link to the MITRE page.
- In the window showing the details, click **Details** to view the general description of the technique.

NAT Source/Destination IP (Syslog: NAT_InitiatorIP, NAT_ResponderIP)

The NAT translated IP address of the session initiator or responder.

NAT Source/Destination Port (Syslog: NAT_InitiatorPort, NAT_ResponderPort)

The NAT translated port of the session initiator or responder.

NetBIOS Domain (Syslog: NetBIOSDomain)

The NetBIOS domain used in the session.

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.

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.

Network Analysis Policy (Syslog: NAPPolicy)

The network analysis policy (NAP), if any, associated with the generation of the event.

Original Client Country

The country where the original client IP address belongs. To obtain this value, the system extracts the original client IP address from an X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header, then maps it to the country using the geolocation database (GeoDB). To populate this field, you must enable an access control rule that handles proxied traffic based on its original client.

Original Client IP (Syslog: originalClientSrcIP)

The original client IP address from an X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header. To populate this field, you must enable an access control rule that handles proxied traffic based on its original client.

Other Enrichment

Non-MITRE information associated with an event that supports an expanded view.

Prefilter Policy (Syslog: Prefilter Policy)

The prefilter policy that handled the connection.

Protocol (Syslog: Protocol)

In the Firewall Management Center web interface:

- This value constrains summaries and graphs.
- This field is available only as a search field.

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.

QoS-Applied Interface

For rate-limited connections, the name of the interface where you applied rate limiting.

QoS-Dropped Initiator/Responder Bytes

The number of bytes dropped from the session initiator or session responder due to rate limiting.

QoS-Dropped Initiator/Responder Packets

The number of packets dropped from the session initiator or session responder due to rate limiting.

QoS Policy

The QoS policy that rate limited the connection.

QoS Rule

The QoS rule that rate limited the connection.

QUIC Session ID

A 64 bit internal session identifier to uniquely identify a QUIC connection within the firewall.

QUIC Stream ID

A 62-bit stream identifier to uniquely identify a stream within a QUIC connection.

Reason (Syslog: AccessControlRuleReason)

The reason or reasons the connection was logged, in many situations. For a full list, refer to Connection event reasons, on page 23.

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.

Referenced Host (Syslog: ReferencedHost)

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

SecIntMatchingIP (Syslog Only)

Which IP address matched.

Possible values: **`None`**, **`Destination`**, or **`Source`**.

Security Context (Syslog: Context)

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

Security Intelligence Category (Syslog: URLSICategory, DNSSICategory , IPReputationSICategory)

The name of the object that represents or contains the blocked URL, domain, or IP address in the connection. The Security Intelligence category can be the name of a network object or group, a Block list, a custom Security Intelligence list or feed, a TID category related to an observation, or one of the categories in the Intelligence Feed.

In the Firewall Management Center web interface, DNS, Network (IP address), and URL Security Intelligence connection events are combined into a single category field. In syslog messages, those events are specific by type.

Security-related connection events include security intelligence events and other connection events such as the ones that triggered intrusion or malware events. The **Security Intelligence Summary** workflow displays all the security intelligence events by their category and count. The events without a security intelligence category are grouped and displayed with the count only.

For more information about the categories in the Intelligence Feed, refer to Security intelligence categories.

Source Device

In the Firewall Management Center web interface, this value 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`.

Source Port/ICMP Type (Syslog: SrcPort, ICMPType)

In the Firewall Management Center web interface, these values constrain summaries and graphs.

The port or ICMP type used by the session initiator.

SourceSecurityGroup (Syslog Only)

This field holds the text value associated with the numeric value in **SourceSecurityGroupTag**, if available. If the group name is not available as a text value, then this field contains the same integer value as the SourceSecurityGroupTag field. Tags can be obtained from inline devices (no source SGT name specified) or from ISE (which specifies a source).

SourceSecurityGroupType (Syslog Only)

This field displays the source from which a security group tag was obtained.

Value	Description
Inline	Source SGT value is from packet
Session Directory	Source SGT value is from ISE via session directory topic
SXP	Source SGT value is from ISE via SXP topic

Source SGT (Syslog: SourceSecurityGroupTag)

The numeric representation of 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.

TLS Actual Action (Syslog: SSLActualAction)

In the Firewall Management Center web interface, this field is a search field only.

The system displays field values in the **TLS Status** field on search workflow pages.

The action the system applied to encrypted traffic in the SSL policy.

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

TLS Certificate Information (Syslog: SSLCertificate)

In the Firewall Management Center web interface, this field is a search field 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

TLS Certificate Status (Syslog: SSLServerCertStatus)

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`.

TLS Cipher Suite (Syslog: SSSLCipherSuite)

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

TLS Encryption applied to the connection

This field is available only as a search field in the Secure Firewall Management Center web interface.

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

TLS Expected Action (Syslog: SSLExpectedAction)

In the Firewall Management Center web interface, this field is a search field only.

The action the system expected to apply to encrypted traffic, given the SSL rule in effect.

Enter any of the values listed for TLS **Actual Action**.

TLS Failure Reason (Syslog: SSLFlowStatus)

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
- Incomplete Handshake

- 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 **TLS Status** field on the search workflow pages.

TLS Flow Error

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

TLS Flow Flags

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

The message OVER_SUBSCRIBED is displayed if your managed device is overloaded. For more information, refer to Troubleshoot TLS/SSL oversubscription.

TLS Flow Messages

The keywords below indicate encrypted traffic is associated with the specified message type exchanged between client and server during the TLS/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
- SERVER_NAME_MISMATCH

  The server certificate seen in the session has a Common Name or SAN values not corresponding to the destined domain name.

- CERTIFICATE_CACHE_HIT

  A certificate matching the destined domain name was found in the cache.

- CERTIFICATE_CACHE_MISS

  A certificate matching the destined domain name was not found in the cache.

The message HEARTBEAT is displayed if applications are using the TLS/SSL heartbeat extension. For more information, refer to TLS heartbeat.

TLS Session ID (Syslog: SSLSessionID)

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

TLS Status

The action associated with the **TLS 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 TLS/SSL handshake error), the lock icon is dimmed.

If the system fails to decrypt an encrypted connection, it displays the **TLS Actual Action** (undecryptable traffic action) taken, as well as the **TLS 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)`.

If the SSL handshake of an encrypted connection is incomplete and the system fails to decrypt the traffic, TLS **Status** field displays `Unknown (Incomplete Handshake)`.

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

TLS Subject/Issuer Country

This field is available only in the Firewall Management Center web interface, and only as a search field.

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

TLS Ticket ID (Syslog: SSLTicketID)

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

SSLURLCategory (Syslog Only)

URL categories for the URL visited in the encrypted connection.

This field exists only as a syslog field; in the Firewall Management Center web interface, values in this field are included in the URL Category column.

See also **URL**.

TLS Version (Syslog: SSLVersion)

The TLS/SSL protocol version used to encrypt the connection:

- Unknown
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSv1.2
- TLSv1.3

TCP Flags (Syslog: TCPFlags)

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.

TLS Client SNI (Syslog: SSLServerName)

This field displays the Server Name Indication (SNI) value in a TLS **ClientHello** message. The SNI value in a TLS **ClientHello** message indicates the hostname to which the client is trying to connect.

Total Packets

This field is available only as a search field.

The total number of packets transmitted in the connection.

Traffic (KB)

This field is available only as a search field.

The total amount of data transmitted in the connection, in kilobytes.

Tunnel/Prefilter Rule (Syslog: Tunnel or Prefilter Rule)

The tunnel rule, prefilter rule, or prefilter policy default action that handled the connection.

URL, URL Category, and URL Reputation (Syslog: URL, URLCategory and SSLURLCategory, URLReputation)

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

For an event to display URL category and reputation, you must include the applicable URL rules in an access control policy and configure the rule with URL category and URL reputation under the **URLs** tab.

URL category and reputation do not appear in an event if the connection is processed before it matches a URL rule.

If the URL column is empty and DNS filtering is enabled, the DNS Query field shows the domain, and the URL Category and URL Reputation values apply to the domain.

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

See also **SSLURLCategory**, above.

User Agent (Syslog: UserAgent)

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

VLAN ID (Syslog: VLAN_ID)

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

VPN Action

VPN action associated with the connection.

Possible values are:

- **Encrypt**: VPN encrypts the traffic for the logged connection. See **Encrypt Peer** column to know the IP address of the VPN peer which encrypts the connection.
- **Decrypt**: VPN decrypts the traffic for the logged connection. See **Encrypt Peer** column to know the IP address of the VPN peer which decrypts the connection.
- **VPN Routing**: The traffic transitions through the VPN tunnel. VPN performs decryption at the beginning of connection and encryption at the end of connection. See **Encrypt Peer** and **Decrypt Peer** columns to know the IP addresses of the VPN peers which encrypts and decrypts the connection.

Web Application (Syslog: WebApplication)

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.

Zero Trust Application

Name of the application for which the end user requested access.

Zero Trust Application Group

Name of the application group if the rule matched-application is part of an application group.

Zero Trust Application Host

IP address or the hostname requested by the user device for accessing the application.

Zero Trust Application Policy

Name of the rule matched-zero trust application policy.

Zero Trust Origin User

Unique ID of the user device that requested access to the private application.

Zero Trust Proxy

Domain name of the zero trust proxy that intercepted the network traffic.

Zero Trust Rule

Name of the rule matched for the connection request.

Zero Trust Status

Status of the zero trust access request, indicating whether it was successful or unsuccessful.

Zero Trust Tunnel ID

The unique ID of the tunnel that is established between the Secure Client and the Firewall Threat Defense device during zero trust access. User can access multiple private applications using the same tunnel in a session.

Connection and Security-Related Connection Event data overview

In the Secure Firewall Management Center web interface, you can view and search connection and Security-Related connection events using tabular and graphical workflows under the **Events & Logs** > **+ Show more** > **Connection** > **Security-Related Events**.



Note For each Security-Related connection event, there is an identical, separately stored connection event. Each Security-Related connection event has a populated **Security Intelligence Category** field.

The information available for any individual event can vary depending on how, why, and when the system logged the connection.

Search constraints

Fields marked with an asterisk (*****) on search pages constrain connection graphs and connection summaries. Because connection graphs are based on connection summaries, the same criteria that constrain connection summaries also constrain connection graphs.

If invalid search constraints are used for connection summaries, and the results are viewed in a connection summary page within a custom workflow, they are labeled as not applicable (N/A) and marked with a strikethrough.

Syslog fields

Most fields appear both in the Secure Firewall Management Center web interface and as syslog messages. Fields without a listed syslog equivalent are not available in syslog messages. A few fields are syslog-only, as noted, and few others are separate fields in syslog messages but are consolidated fields in the web interface or vice-versa.

Initiator and responder, source and destination, and sender and receiver fields

A field category is a classification of network event terminology that

- distinguishes between different roles in network connections, security events, and file transfers,
- applies to specific event types such as connection, intrusion, and file/malware events, and
- represents different aspects of network communication flow that may not always align with each other.

Field terminology comparison

These field types have different relationships based on the event context.

Table 1: Comparison of terms

Fields	Event Type	Description
Initiator/Responder	Connection	The initiator and responder of the connection. The connection initiator is not necessarily the same as the intrusion source or the malware file sender.
Source/Destination	Intrusion	The source and destination of the attack. The source of an intrusion event can be the initiator or the responder of the connection.
Sender/Receiver **(Sending..., Receiving...)**	File, Malware	The sender and receiver of a file or malware. The file sender is not necessarily the connection initiator. Files may be uploaded or downloaded.

Connection event reasons

Lists the reasons for connection events logged by the system, including descriptions for each reason.

The Reason field in a connection event displays why the connection was logged. Each reason corresponds to specific actions or circumstances in the connection event.

The table lists each connection event reason logged by the system, with a description of what triggers each reason and the resulting system action.

Reason	Description
Content Restriction	The system modified the packet to enforce content restrictions related to the Safe Search feature.
DNS Block	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.
DNS Monitor	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.
Elephant Flow	The connection is large enough to be considered an elephant flow, which is a flow that can be large enough to affect overall system performance. By default, elephant flows are larger than 1GB/10 seconds. You can adjust the byte and time thresholds for identifying elephant flows in the Firewall Threat Defense CLI using the **system support elephant-flow-detection** command. For more information, refer to the *Cisco Secure Firewall Threat Defense Command Reference*. **Note** A flow is considered as elephant flow only when both the byte and time thresholds are surpassed. You can create a custom dashboard to correlate elephant flows and other interrelated metrics, for example, CPU metrics such as Snort, System, and Physical Cores. For more information, refer to System Monitoring and Troubleshooting chapter.
Elephant Flow Exempted	This reason appears when an elephant flow is detected and matches the L4 ACL rules that exempt certain flows from remediation.
Encrypted Visibility Block	Connections that are blocked by the Encrypted Visibility Engine.
Encrypted Visibility IoC	Indications of Compromise (IoC) events detected by Encrypted Visibility Engine for connection events with high and very high malware confidence level. IoC events are triggered for encrypted sessions generated from a host using a malicious client. You can view information, such as IP address, MAC address, and OS information of the malicious host, and the timestamp of the suspicious activity.
Encrypted Visibility Exempt	Connections allowed bypassing the Encrypted Visibility Engine block action.
File Block	The connection contained a file or malware file that the system prevented from being transmitted. File Block reason is always paired with an action of Block.

Reason	Description
File Custom Detection	The connection contained a file on the custom detection list that the system prevented from being transmitted.
File Monitor	The system detected a particular type of file in the connection.
File Resume Allow	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.
File Resume Block	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.
Intelligent App Bypass	The Intelligent Application Bypass (IAB) mode: • If the action is Trust, IAB was in bypass mode. Matching traffic passed without further inspection. • If the action is Allow, IAB was in test mode. Matching traffic was available for further inspection.
Intrusion Block	Snort3 Engine: When there is a "would have dropped" result, the connection event reason is blank, instead of "Intrusion block." The "would have dropped" event is treated the same as "Allow" in regards to the connection event reason being populated.
Intrusion Monitor	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.
IP Block	The system denied the connection without inspection, based on the IP address and Security Intelligence data. A reason of IP Block is always paired with an action of Block.
IP Monitor	The system would have denied the connection based on the IP address and Security Intelligence data, but you configured the system to monitor, rather than deny, the connection.
SSL Block	The system blocked an encrypted connection based on the TLS/SSL inspection configuration. A reason of SSL Block is always paired with an action of Block.
URL Block	The system denied the connection without inspection, based on the URL and Security Intelligence data. A reason of URL Block is always paired with an action of Block.
URL Monitor	The system would have denied the connection based on the URL and Security Intelligence data, but you configured the system to monitor, rather than deny, the connection.
User Bypass	The system initially blocked a user’s HTTP request, but the user clicked through a warning page to view the site. A reason of User Bypass is always paired with an action of Allow.

Reason	Description
Pending Rule Match	The connection ended before the rule evaluation was complete and no rule was matched during that connection. The system logs this connection with the pending rule for evaluation and 'Allow' action.

Requirements for populating connection event fields

A connection event field population requirement is a system condition that

- determines what information appears in connection events based on multiple system factors,
- depends on appliance models, licensing, traffic characteristics, and detection methods, and
- varies according to evaluation stage, logging method, and specific system configurations.

Factors affecting connection event field population

Several factors determine which fields are populated in connection events:

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.

Traffic Characteristics

The system reports only information that is 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; refer to Differences between NetFlow and managed device data.

Evaluation Stage

Each type of traffic inspection and control occurs where it provides 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. Configure your system to log end-of-connection data for connection graphs and summaries to display data.



Note Security-related connection events include security intelligence events and other connection events, such as the ones that triggered intrusion or malware events. The **Security Intelligence Summary** workflow groups the security-related connection events that do not have a security intelligence category and displays the count without a **Security Intelligence Category** value.

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.
- The Security Group Tag (SGT) fields are populated only if you configure ISE as an identity source or add custom SGT rule conditions.
- Prefilter-related fields (including tunnel zone information in security zone fields) are populated only in connections handled by a prefilter policy.
- TLS/SSL-related fields are populated only in encrypted connections handled by a decryption policy. You can view the values of the fields using a Do Not Decrypt rule action if you do not need to decrypt the traffic.
- 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.
- QoS-related fields are populated only in connections subject to rate limiting.
- 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 Secure Firewall 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.

For the connection event to display URL category and reputation, you must include the applicable URL rules in an access control policy and configure the rule with URL category and URL reputation under the **URLs** tab. URL category and reputation do not appear in an event if the connection is processed before it matches a URL rule.

Related Topics

Differences between NetFlow and managed device data

Information available in connection event fields

The table lists the conditions in which the system populates connection and security intelligence fields. Columns represent different event types:

- Origin: Direct (events representing connections detected and handled by a system-managed device)
- Origin: NetFlow (events representing connections exported by a NetFlow exporter)
- Logging: Start (events representing connections logged at their beginning)
- Logging: End (events representing connections logged at their end)

A "yes" in the table means the system can populate a field but only reports detectable information in network traffic. For example, TLS/SSL-related fields populate only for encrypted connections handled by a decryption policy.

Connection Event Field	Origin: Direct	Origin: NetFlow	Logging: Start	Logging: End
Access Control Policy	yes	no	yes	yes
Access Control Rule	yes	no	yes	yes
Action	yes	no	yes	yes
Application Protocol	yes	yes	if available	yes
Application Protocol Category & Tag	yes	yes	if available	yes
Client Application	yes	no	if available	yes
Client Application Category & Tag	yes	no	if available	yes
Payload Application	yes	no	if available	yes
Payload Application Category & Tag	yes	no	if available	yes
Web Application	yes	no	if available	yes
Web Application Category & Tag	yes	no	if available	yes

View Connection and Security-Related Connection Event Tables

You can use the Firewall Management Center to view a table of connection or Security-Related connection 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.

Note that **Connection Events** table view displays **1 of Many** instead of how many pages of events are available if your system generates more than 25 connection events.

Before you begin

You must be an Admin or Security Analyst user to perform this task.

Follow these steps to view and interact with connection and security intelligence event tables.

Procedure

Step 1 Choose either of the following:

- **Events & Logs** > **+ Show more** > **Connection** > **Events** (for connection events)
- **Events & Logs** > **+ Show more** > **Connection** > **Security-Related 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, refer to Change the time window.
- Data Source: If data is stored remotely using Security Analytics and Logging (On Premises), and you have good reason to change the data source, choose a data source. For important information about this option, refer to Work in Firewall Management Center with connection events stored on a Secure Network Analytics appliance.
- Field Names: To learn more about the contents of the columns in the table, refer to Connection and Security-Related Connection Event Fields, on page 4.

Note In the table view of events, multiple fields are hidden by default. To change the fields that appear, click the Disable Column ✕ in any column name to display a field chooser.

- Additional information: To view data in available sources external to your system, right-click an event value. The options you see depend on the data type and include public sources; other sources depend on

the resources you have configured. For more information, refer to Event investigation using web-based resources.

- External intelligence: To gather intelligence about an event, right-click an event value in the table and choose from a Cisco or third-party intelligence source. For example, you can get details about a suspicious IP address from Cisco Talos. The options you see depend on the data type and the integrations that are configured on your system. For more information, refer to Event investigation using web-based resources.
- Host Profile: To view the host profile for an IP address, click **Host Profile** or, for hosts with active indications of compromise (IOC) tags, **Compromised Host** 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**, or for users associated with IOCs, **Red User**.
- Files and Malware: To view the files, including malware, detected or blocked in a connection, click **View Files** and proceed as described in View files and malware detected in a connection, on page 30.
- Intrusion Events: To view the intrusion events associated with a connection, as well as their priority and impact, click **Intrusion Events** in the **Intrusion Events** column and proceed as described in View intrusion events for a connection, on page 31.

Note To quickly view intrusion, file, or malware events associated with one or more connections, check the connections using the check boxes in the table, 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 blocked by Security Intelligence. You can only see this information for a Security Intelligence event if you configured Security Intelligence to monitor, rather than block, connections.

- Certificate: To view details about an available certificate used to encrypt a connection, click **Enabled Lock** in the **SSL Status** column.
- Constrain: To constrain the columns that appear, click **Close** (✕) in the column heading that you want to hide. In the pop-up window that appears, click **Apply**.

Note 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: (Security-Related connection event tables only). 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: For more information, refer to Use drill-down pages.

Note 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: For more information, refer to 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

Workflows
Configure event view settings

View files and malware detected in a connection

View file events associated with connections that match access control rules with file policies to identify detected files and malware.

If you associate a file policy with one or more access control rules, the system can detect files (including malware) in matching traffic. Use the **Events & Logs** > **+ Show more** > **Connection** > **Events** menu options to see the file events, if any, associated with the connections logged by those rules. Instead of a list of files, the Secure Firewall Management Center displays view files () in the **Files** column. The number on the view files 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:

- Malware events detected by Secure Endpoint ("endpoint-based malware events") are not associated with connections. Those events are imported from your Secure Endpoint 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.

Before you begin

You must be an Admin or Security Analyst user to perform this task.

Follow these steps to view files and malware detected in a connection:

Procedure

Step 1 Go to **Events & Logs** > **+ Show more** > **Connection** > **Events** and choose the relevant option.

Step 2 While using a connection event table, click **View Files**.
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 3 You have the following choices:

- View: To view a table view of file events, click a **File's View**.
- View: To view details in a table view of malware events, click a **Malware File's View**.
- Track: To track the file's transmission through your network, click a **File's Trajectory**.

- View: To view details on all of the connection's detected file or malware events detected by Malware Defense ("network-based malware events"), click **View File Events** or **View Malware Events**.

Related Topics

Workflows
Configure event view settings

View intrusion events for a connection

Enable detailed analysis of intrusion events linked to active or logged connections, including their priority and the potential impact to your network.

If you associate an intrusion policy with an access control rule or default action, the system can detect exploits in matching traffic. Use the **Events & Logs** > **+ Show more** > **Connection** > **Events** menu options to 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.

Before you begin

You must be an Admin or Security Analyst user to perform this task.

Follow these steps to view intrusion events for a connection.

Procedure

Step 1 Go to **Events & Logs** > **+ Show more** > **Connection** > **Events** and choose the relevant option.

Step 2 While using a connection event table, click **Intrusion Events** in the **Intrusion Events** column.

Step 3 In the pop-up window that appears:

- Click a **Listed Event's View** to view details in the packet view.
- Click **View Intrusion Events** to view details on all of the connection's associated intrusion events.

Related Topics

Workflows
Configure event view settings

Encrypted connection certificate details

You can use options under the **Events & Logs** > **+ Show more** > **Connection** menu to display the public key certificate (if available) used to encrypt a connection handled by the system. The certificate contains the information listed in this reference.

The table lists and describes the certificate attributes you can view when displaying the public key certificate for encrypted connections handled by the system.

Table 2: Encrypted connection certificate details

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

Related Topics

Workflows
Configure event view settings

View the connection summary page

Display summary graphs of network connections to analyze activity by time interval, device, or other criteria.

The connection summary page provides aggregated graphs that help monitor network activity. Only users with specific role permissions can access this page. Graphs are organized by criteria such as connection count over chosen intervals; however, you cannot drill down into individual connection events from these summaries.

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 **Insights & Reports** > **Dashboard**.

Step 2 Click **Switch**, and then choose **Connection Summary**.

Step 3 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 4 To manipulate and analyze the connection graphs, proceed as described in Use connection event graphs.

Tip To detach a connection graph so you can perform further analysis without affecting the default time range, click **View**.

History for Connection and Security Intelligence Events

Documents the history and details of connection and security intelligence events, including feature updates and changes across various versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Improved connection monitoring for Zero Trust Access sessions	7.7.10	Any	Introduced these connection event fields for zero trust access sessions, allowing you to monitor and investigate zero trust access incidents more effectively. • Zero Trust Application Host • Zero Trust Origin User • Zero Trust Proxy • Zero Trust Rule • Zero Trust Status • Zero Trust Tunnel ID New/modified Screens: **Analysis** > **Connections Header** > **Events**.
New Connection Event Reason - Elephant Flow.	7.1	Any	Refer to Connection event reasons, on page 23.
NAT Translated IP Address and Port	7.1	Any	Four new fields are added to the connection and security intelligence event table: • NAT Source IP • NAT Destination IP • NAT Source Port • NAT Destination Port
Ability to choose a data source when working with certain events stored remotely	7.0	Any	Refer to History for workflows.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
DNS filtering	7.0 6.7 (Beta feature)	Any	When DNS filtering is enabled: • The DNS Query field may hold the domain associated with DNS filtering matches. • If the URL field is empty but DNS Query, URL Category, and URL Reputation have values, the event was generated by the DNS filtering feature, and the category and reputation apply to the domain specified in DNS Query. • Refer to *DNS Filtering and Events* in the *Cisco Secure Firewall Management Center Device Configuration Guide* .
Removal of support for custom tables for connection events	6.6	Any	You can no longer create custom tables for connection events. If you upgrade, any pre-existing custom tables for connection events are still available but always return no results. There is no change to other types of custom tables. New/Modified screens: The Tables option on **Analysis** > **Advanced Custom Tables** Platform: Firewall Management Center
Removal of ability to Delete and Delete All connection events	6.6	Any	The Delete and Delete All buttons have been removed from connection events table pages. To purge all connection events, refer to Data Purge and Storage. New/Modified screens: **Analysis** > **Connections** > **Events** Platform: Firewall Management Center
New fields for VRF and SGT	6.6	Any	• Ingress Virtual Router (Syslog: IngressVRF) • Egress Virtual Router (Syslog: EgressVRF) • DestinationSecurityGroupType (Syslog only) • SourceSecurityGroupType (Syslog only)

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New and changed Security Group Tag fields	6.5	Any	Changes to fields in the Firewall Management Center web interface: • Changed fields: Security Group Tag is now Source SGT • New fields: Destination SGT Changes to syslog fields: • Changed fields: SecurityGroup is now SourceSecurityGroupTag • New fields: • SourceSecurityGroup • DestinationSecurityGroup • DestinationSecurityGroupTag Supported Platforms: Firewall Management Center, managed devices
New syslog field: Event Priority	6.5	Any	This field identifies connection events as High priority when they are associated with intrusion, file, malware, or Security Intelligence events.
Unique identifier for connection event in syslogs	6.4.0.4	Any	The following syslog fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.