

Connection Logging

The following topics describe how to configure the system to log connections made by hosts on your monitored network:

- Connection logging, on page 1
- Connection logging limitations, on page 10
- Best practices for connection logging, on page 11
- Connection logging, on page 14
- Application-aware and protocol-aware syslogs, on page 18

Connection logging

Connection logging is a system feature that

- generates logs of connections detected by managed devices known as *connection events*,
- provides granular control through rules and policies over which connections to log, when to log them, and where to store the data, and
- creates special connection events called *security-related connection events* that represent connections blocked by the reputation-based Security Intelligence feature.

Connection event data

Connection events contain data about the detected sessions. The specific data available for any event can vary, but generally includes:

- Basic connection properties: timestamp, source and destination IP address, ingress and egress zones, the device that handled the connection, and so on
- Additional connection properties discovered or inferred by the system: applications, requested URLs, or users associated with the connection, and so on
- Metadata about why the connection was logged: which configuration handled the traffic, whether the connection was allowed or blocked, details about encrypted and decrypted connections, and so on

Log connections according to the security and compliance needs of your organization. When setting up connection logging, remember that the system can log a connection for multiple reasons. Disabling logging in one place does not guarantee that matching connections will not get logged elsewhere.

The information contained in a connection event depends on factors such as traffic characteristics and relevant configuration.



Note You can supplement the connection logs gathered by your managed devices with connection data generated from exported NetFlow records. This is particularly useful if you have NetFlow-enabled routers or other devices monitoring networks that managed devices cannot access.

Logged connections

Logged connections are network connections that

- are automatically saved to the Firewall Management Center database as end-of-connection events,
- generate logs regardless of other logging configurations unless connection event storage is disabled, and
- include connections associated with intrusions, file and malware events, intelligent application bypass, and monitored traffic.

Connection types and logging behavior

The system automatically logs specific connection types based on their association with security events and traffic monitoring.

Connection types that generate automatic logs:

- Connections associated with intrusions: The system automatically logs connections associated with intrusion events, unless the connection is handled by the access control policy's default action.
- Connections associated with file and malware events: The system automatically logs connections associated with file and malware events.
- Connections associated with intelligent application bypass: The system automatically logs bypassed and would-have-bypassed connections associated with IAB.
- Monitored connections: The system always logs the ends of connections for monitored traffic, even if the traffic matches no other rules and you do not enable default action logging.



Note File events generated by inspecting NetBIOS-SSN (SMB) traffic do not immediately generate connection events because the client and server establish a persistent connection. The system generates connection events after the client or server ends the session.

Special behavior for default action connections:

- When an intrusion policy associated with the access control default action generates an intrusion event, the system does *not* automatically log the end of the associated connection. Instead, you must explicitly enable default action connection logging.

- However, if you enable beginning-of-connection logging for the default action, the system *does* log the end of the connection when an associated intrusion policy triggers, in addition to logging the beginning of the connection.

For more information about monitored connections, refer to Logging for monitored connections, on page 4.

Other Connections You Can Log

So that you log only critical connections, enable connection logging on a per-rule basis. If you enable connection logging for a rule, the system logs all connections handled by that rule.

You can also log connections handled by policy default actions. Depending on the rule or default action (and for access control, a rule's inspection configuration), your logging options differ.

Prefilter Policy: Rules and Default Action

You can log connections (including entire plaintext, passthrough tunnels) that you fastpath or block with a prefilter policy.

Prefiltering uses outer-header criteria to handle traffic. For tunnels that you log, the resulting connection events contain information from the outer, encapsulation headers.

For traffic subject to further analysis, logging in the prefilter policy is disabled, although matching connections may still be logged by other configurations. The system performs all further analysis using inner headers, that is, the system independently handles and logs each connection within an allowed tunnel.

Decryption Policy: Rules and Default Action

You can log connections that match a decryption rule or decryption policy default action.

For blocked connections, the system immediately ends the session and generates an event. For monitored connections and connections that you pass to access control rules, the system generates an event when the session ends.

Access Control Policy: Security Intelligence Decisions

You can log a connection whenever it is blocked by the reputation-based Security Intelligence feature.

Optionally, and recommended in passive deployments, you can use a monitor-only setting for Security Intelligence filtering. This allows the system to further analyze connections that would have been blocked by Security Intelligence, but still log the match. Security Intelligence monitoring also allows you to create traffic profiles using Security Intelligence information.

When the system logs a connection event as the result of Security Intelligence filtering, it also logs a matching Security Intelligence event, which is a special kind of connection event that you can view and analyze separately, and that is also stored and pruned separately. So that you can identify the matching IP address in the connection, host icons beside blocked and monitored IP addresses look slightly different in the tables on the pages under the **Events & Logs** > **+ Show more** > **Connection** > **Events** menus.

Access Control Policy: Rules and Default Action

You can log connections that match an access control rule or access control policy default action.

Related Topics

Rules and policy actions effect on logging, on page 4

Rules and policy actions effect on logging

Rules and policy actions effect on logging is a traffic handling mechanism that

- determines how the system inspects and handles matching traffic,
- controls when and how details about matching traffic can be logged, and
- provides metadata about why the connection was logged, including which configurations handled the traffic.

Connection event metadata

Connection events contain metadata about why the connection was logged, including which configurations handled the traffic. Where you can configure connection logging, rule actions, and policy default actions determine not only how the system inspects and handles matching traffic, but also when and how you can log details about matching traffic.

Related Topics

Connection and Security-Related Connection Event Fields

Logging for fastpathed connections

Logging for fastpathed connections is a monitoring capability that

- records connection events for traffic that matches tunnel rules and prefilter rules with **Fastpath** actions,
- captures information for non-encrypted tunnels including outer session details for tunnel rules, and
- provides limited information in connection events since fastpathed traffic bypasses access control and QoS processing.

Supported traffic types

You can log fastpathed connections and non-encrypted tunnels, which include traffic matching these rules and actions in the prefilter policy:

- Tunnel rules—**Fastpath** action (logs the outer session)
- Prefilter rules—**Fastpath** action

Fastpathed traffic bypasses the rest of access control and QoS, so connection events for fastpathed connections contain limited information.

Logging for monitored connections

Logging for monitored connections is a system function that

- automatically logs connection ends for traffic matching specific monitoring configurations,
- operates independently of default action logging settings, and
- consolidates multiple Monitor rule matches into single connection events.

Monitored traffic configurations

The system always logs the ends of connections for traffic matching these configurations, even if the traffic matches no other rules and you do not enable default action logging:

- Security Intelligence: Block lists set to monitor (also generates a Security Intelligence event)
- SSL rules: **Monitor** action
- Access control rules: **Monitor** action

The system does not generate a separate event each time a single connection matches a Monitor rule. Because a single connection can match multiple Monitor rules, each connection event can include and display information on the first eight Monitor access control rules that the connection matches, as well as the first matching SSL Monitor rule.

Similarly, if you send connection events to an external syslog or SNMP trap server, the system does not send a separate alert each time a single connection matches a Monitor rule. Rather, the alert that the system sends at the end of the connection contains information on the Monitor rules the connection matched.

Logging for trusted connections

Logging for trusted connections is a system capability that

- records the beginnings and ends of trusted connections for traffic matching access control rules with **Trust** action
- captures events for traffic matching the access control default action **Trust All Traffic**, and
- generates limited information because trusted connections are not subject to deep inspection or discovery.

Trusted connection logging behavior

You can log the beginnings and ends of trusted connections, which include traffic matching these rules and actions:

- Access control rules: **Trust** action
- Access control default action: **Trust All Traffic**



Note Although you *can* log trusted connections, we recommend you do not do so because trusted connections are not subject to deep inspection or discovery, so connection events for trusted connections contain limited information.

TCP connections detected by a Trust rule on the first packet generate only an end-of-connection event. The system generates the event one hour after the final session packet.

Logging for blocked connections

Logging for blocked connections is a security feature that

- records traffic matching blocking rules and actions across multiple policy types,
- generates connection events with different timing based on the blocking mechanism, and

- provides visibility into denied traffic for security monitoring and analysis.

Blocked connection types

You can log blocked connections, which include traffic matching these rules and actions:

- Tunnel rules—**Block**
- Prefilter rules—**Block**
- Prefilter default action—**Block all tunnel traffic**
- Security Intelligence—Block lists not set to Monitor (also generates a Security Intelligence event)
- Decryption rules—**Block** and **Block with reset**
- SSL default action—**Block** and **Block with reset**
- Access control rules—**Block**, **Block with reset**, and **Interactive Block**
- Access control default action—**Block All Traffic**

Only devices deployed inline (that is, using routed, switched, or transparent interfaces, or inline interface pairs) can block traffic. Because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection.



Caution Firewall Threat Defense device logs end-of-connection events for TCP connections where the three-way handshake does not complete, including SYN-only, SYN-SYN/ACK (no ACK), and SYN-RST/ACK scenarios (except when TLS Identity is enabled). These logs provide visibility into incomplete or suspicious connection attempts. However, logging blocked TCP connections during a Denial of Service (DoS) attack can affect system performance and overwhelm the database with multiple similar events. Before you enable logging for a Block rule, consider whether the rule monitors traffic on an Internet-facing interface or other interface vulnerable to DoS attack.

Beginning vs. end-of-connection logging for blocked connections

When you log a blocked connection, how the system logs it depends on why the connection was blocked. This is important to keep in mind when configuring correlation rules based on connection logs:

- For decryption rules and decryption policy default actions that block encrypted traffic, the system logs **end**-of-connection events. This is because the system cannot determine if a connection is encrypted using the first packet in the session.
- For other blocking actions, the system logs **beginning**-of-connection events. Matching traffic is denied without further inspection.

Logging bypassed interactive blocks

Interactive blocking access control rules, which cause the system to display a warning page when a user browses to a prohibited website, allow you to configure end-of-connection logging. This is because if the user clicks through the warning page, the connection is considered a new, allowed connection which the system can monitor and log.

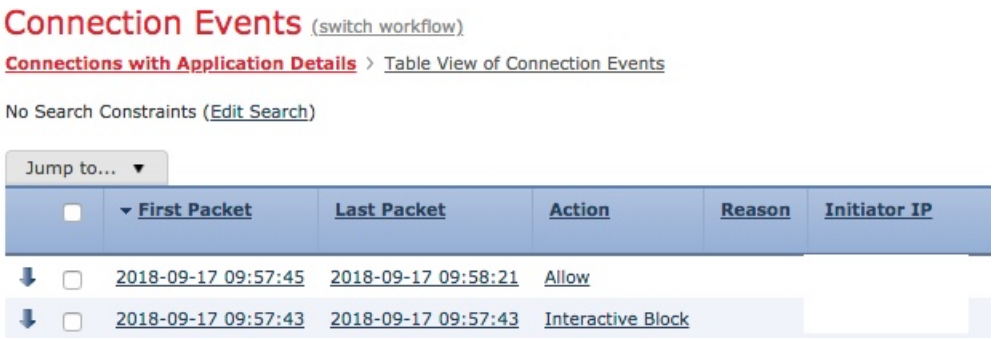
Therefore, for packets that match an Interactive Block or Interactive Block with Reset rule, the system can generate these connection events:

- A beginning-of-connection event when a user's request is initially blocked and the warning page is displayed; this event has an associated action of **Interactive Block** or **Interactive Block with Reset**
- Multiple beginning- or end-of-connection events if the user clicks through the warning page and loads the originally requested page; these events have an associated action of **Allow** and a reason of **User Bypass**

Interactive block example

The following figure shows an example of an interactive block followed by allow.

Figure 1: Interactive block followed by allow



Logging for allowed connections

Logging for allowed connections is a security feature that

- generates file and malware events when file policies detect or block files during traffic inspection, and
- provides configurable logging options on a per-access-control-rule basis.

Connection logging details

You can log allowed connections, which includes traffic matching the following rules and actions:

- SSL rules—**Decrypt** action
- SSL rules—**Do not decrypt** action
- SSL default action—**Do not decrypt**
- Access control rules—**Allow** action
- Access control default action—**Network Discovery Only** and any intrusion prevention option

Enabling logging for these configurations ensures the connection is logged, while also permitting (or specifying) the next phase of inspection and traffic handling. SSL logging is always end-of-connection; access control configurations also allow beginning-of-connection logging.

Although the **Analyze** action in tunnel and prefilter rules also allows connections to continue with access control, logging is disabled for rules with this action. Matching connections may still be logged by other configurations. Allowed tunnels might have their encapsulated sessions evaluated and logged individually.

When you allow traffic with an access control rule or default action, you can use an associated intrusion policy to further inspect traffic and block intrusions. For access control rules, you can also use a file policy to detect and block prohibited files, including malware. Unless you disable connection event storage, the system automatically logs most allowed connections associated with intrusion, file, and malware events. For detailed information, refer to Logged connections, on page 2.

Connections with encrypted payloads are not subject to deep inspection, so connection events for encrypted connections contain limited information.

When a file policy detects or blocks a file, it logs one of these events to the Firewall Management Center database:

- *File events*, which represent detected or blocked files, including malware files.
- *Malware events*, which represent detected or blocked malware files only.
- *Retrospective malware events*, which are generated when the malware disposition for a previously detected file changes.

You can disable this logging on a per-access-control-rule basis. You can also disable file and malware event storage entirely.

Note We recommend you leave file and malware event logging enabled.

Connection logging modes

A connection logging mode is a connection monitoring approach that

- provides two distinct timing options for capturing connection events,
- handles blocked traffic differently than allowed traffic, and
- requires optimization choices to balance performance with information completeness.

Connection logging timing and exceptions

You can log a connection at its beginning or its end, with specific exceptions for blocked traffic:

- Blocked traffic: Because blocked traffic is immediately denied without further inspection, only beginning-of-connection events are typically available for logging; there is no unique end-of-connection to log.
- Blocked encrypted traffic: When you enable connection logging in a decryption policy, the system logs end-of-connection rather than beginning-of-connection events. This occurs because the system cannot determine if a connection is encrypted with the first packet and therefore cannot immediately block encrypted sessions.

To optimize performance, log either the beginning or the end of any connection, but not both. Monitoring a connection for any reason forces end-of-connection logging. For a single non-blocked connection, the

end-of-connection event contains all information present in the beginning-of-connection event, as well as data gathered over the duration of the session.

The table presents differences between beginning and end-of-connection events, along with the advantages of logging each.

Table 1: Comparing beginning and end-of-connection events

Attributes	Beginning-of-Connection Events	End-of-Connection Events
Can be generated...	When the system detects the beginning of a connection (or, after the first few packets if event generation depends on application or URL identification).	When the system: • Detects the close of a connection. • Does not detect the end of a connection after a period of time. • Can no longer track the session due to memory constraints.
Can be logged for...	All connections except those blocked by the decryption policy.	Most connections.
Contain...	Only information that can be determined in the first packet (or the first few packets, if event generation depends on application or URL identification).	All information in the beginning-of-connection event, plus information 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. **Note** The connection event does not count the amount of data transmitted after the threat defense returns a snort verdict for the connection or if you fastpath the connection.
Are useful...	If you want to log: • Blocked connections. • Only the beginning of a connection because the end-of-connection information does not matter to you.	If you want to: • Log encrypted connections handled by a decryption policy. • Perform any kind of detailed analysis on, or trigger correlation rules using, information collected over the duration of the session. • View connection summaries (aggregated connection data) in custom workflows, view connection data in graphical format, or create and use traffic profiles.

Secure Firewall Management Center vs external logging

A log storage option in the Firewall Management Center enables analysis of connection and Security Intelligence event logs through dashboards, event views, traffic profiling, and correlation policies. The number of stored

events depends on the model. Logging usually occurs at connection end, with critical connections logged automatically. Events can also be sent externally via syslog or SNMP traps using alert responses or specific configurations, influencing log storage and processing methods.

Secure Firewall Management Center logging features

If you store connection and Security Intelligence event logs on the Firewall Management Center, you can use the system's reporting, analysis, and data correlation features. For example:

- Dashboards and the Context Explorer provide you with graphical, at-a-glance views of the connections logged by the system.
- Event views (most of the options available under the Analysis menu) present detailed information on the connections logged by the system, which you can display in a graphical or tabular format or summarize in a report.
- Traffic profiling uses connection data to create a profile of your normal network traffic that you can then use as a baseline against which to detect and track anomalous behavior.
- Correlation policies allow you to generate events and trigger responses (such as alerts or external remediations) to specific types of connections or traffic profile changes.

The number of events the Firewall Management Center can store depends on its model.

Note To use these features, you **must** log connections (and in most cases, the end of those connections rather than the beginning). This is why the system automatically logs critical connections—those associated with logged intrusions, prohibited files, and malware.

You can also log events to an external syslog or SNMP trap server, or to other external tools, using these options:

- For external logging on any device:

  A connection you configure called an *alert response*.

- For external logging on Firewall Threat Defense devices:

  Refer to *About Configuring Syslog* and *Configure SNMP Traps* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

- For additional options related to external logging:

  Refer to Event Analysis Using External Tools.

Related Topics

Configuring external alerts with alert responses

Connection logging limitations

Connection logging limitations are restrictions that prevent certain types of network connections from being logged by firewall systems.

Connection types that cannot be logged

Connection logging cannot capture information for these connection types:

- The outer session of a plaintext, passthrough tunnel whose encapsulated connections are inspected by access control.
- TCP connections if the three-way handshake is not completed, to avoid denial-of-service attacks against your firewalls. To monitor or debug failed connections, you can use the **show asp drops** CLI command or the packet capture feature (Packet capture).

If a connection event does not contain the information you think it should, refer to Requirements for populating connection event fields and Information available in connection event fields.

Event viewer event appearances

Event viewer event appearances are the display characteristics that

- require manual page refreshes for events under the Analysis menu,
- typically display events within seconds of detection, but may experience delays under heavy traffic or system operations, and
- show all connection events logged per defined rules without filtering options for unified logging.

Event display characteristics

These points are applicable to all types of events:

- If you are looking at a page under the Analysis menu, you must refresh the page to display new events.
- Events generally are available for viewing within a few seconds of the time the traffic was detected. However, there can be an arbitrary delay under situations such as: Exceptionally heavy traffic conditions; the Firewall Management Center is managing a lot of devices on a low-bandwidth network; or during operations such as event backup which pause event processing.
- All the connection events logged as per the defined rules appear in the event viewer. An option to filter the events is not available for the unified logging of the connection events.

Best practices for connection logging

Best practices for connection logging are guidelines that

- ensure you log only critical connections by enabling connection logging on a per-access-control-rule basis,
- help avoid logging unnecessary traffic such as trusted connections or infrastructure traffic not related to your service offering, and
- optimize storage and performance by preventing duplicate logging and configuring appropriate event limits.

Connections that are always logged

The system automatically logs these connections:

- Some connections associated with detected files, malware, intrusions, and Intelligent Application Bypass (IAB).

  For more information, refer to Logged connections, on page 2.

- Monitored connections.

  For more information, refer to Logging for monitored connections, on page 4.

Connections to never log

Do not enable logging for the following:

- Access control rules with a Trust action.

  Trusted connections are not subject to deep inspection or discovery, so connection events for trusted connections contain limited information.

- Do not enable logging for Block rules in passive deployments. To log connections that the system would have blocked if your devices were deployed inline, use a Monitor rule instead of a Block rule.

  Only devices deployed inline (that is, using routed, switched, or transparent interfaces, or inline interface pairs) can block traffic. Because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection.

- Traffic you're not interested in. Examples follow:

  - Specific allowed traffic, such as DNS requests to a trusted DNS host.
  - Infrastructure traffic that is not related to your service offering.

  (As previously mentioned, you can still monitor this traffic for threats.)

As discussed in Logged connections, on page 2, even if you disable logging for the preceding, intrusion events, malware, and IAB are still logged.

Avoid logging what is being logged elsewhere

If another device or service is logging connection data for a network segment, disable logging for that segment's data in the Firewall Management Center. Examples:

- If a router logs connection events on the same network segment as the Firewall Management Center, avoid logging the same connections on the Firewall Management Center unless you need those connection events for something else, such as correlation policies or traffic profiles.

  For more information about correlation policies, refer to Correlation policies and rules. For more information about traffic profiles, refer to Introduction to traffic profiles.

- If you use Secure Network Analytics to leverage NetFlow records reported from switches and routers to identify potential behavioral anomalies and suspicious traffic patterns, you can disable connection logging for rules monitoring those segments and instead rely on Secure Network Analytics for behavioral analytics for those parts of your network.

  For more information, consult the Secure Network Analytics documentation.

Log either the beginning or end of the connection (not both)

If you have a choice between beginning and end-of-connection logging, enable end-of-connection logging. This is because end-of-connection logs information from beginning-of-connection events, as well as information gathered over the duration of the session.

Log the beginning of connections only if you want to log blocked connections, or if end-of-connection information does not matter to you.

For more information, refer to Connection logging modes, on page 8.

Logging for blocked traffic

Because blocked traffic is immediately denied without further inspection, usually you can log only beginning-of-connection events.

For more information, refer to Logging for blocked connections, on page 5.

Log events to an external location

If your company's security policy permits it, you can save disk space on your Firewall Management Center by streaming logs to an external source using any of the following:

- eStreamer, which enables you to stream logs from a Firewall Management Center to a custom-developed client application. For more information, refer to the *Secure Firewall Management Center Event Streamer Integration Guide* .

  You can integrate the Splunk server to receive events directly from Firewall Management Center or from its managed devices. For details about the Splunk configuration procedure, refer to the *Cisco Secure Firewall Management Center Administration Guide*.

- Syslog or SNMP trap are referred to as alert responses. For more information, refer to Configuring external alerts with alert responses.

Specify the maximum number of event records

Consider the minimum and maximum number of records that can be stored in the database for each event type. For example, a virtual Firewall Management Center can store a maximum of 50 million connection events. Additionally, other event types have their own configurable limits. Go to **Administration** > **Configuration** > **Database** to adjust these limits to meet your storage and performance needs.

For a list of all Firewall Management Center models and their event database sizes, refer to Database event limits.

Control what is displayed in connection events

To specify the number of rows displayed in connection events, click your username in the upper right of the Firewall Management Center, click **User Preferences**, and then click the **Event View Settings**tab. The maximum you can set is 1000 events per page.

Set up connection event reports

To make sure you do not miss connection events, you can set up automated reports in .csv format and optionally schedule them to occur at a regular interval. For more information, refer to the following:

- To create a report template, click **Events & Logs** > **+ Show more** > **Connection** > **Events** and then from the event view page, click **Create Report**. For more information, refer to Create a report template from an event view.
- Schedule tasks (**Administration** > **Advanced** > **Scheduling**): Scheduling.

Connection logging

Connection logging is a network monitoring feature that records network connection activities to match various rules and conditions.

Logging connections with tunnel and prefilter rules

This task enables logging for prefilter policy rules to monitor and analyze connection events for troubleshooting and security analysis purposes.

The prefilter policy applies to Secure Firewall Threat Defense devices only.

Before you begin

- Set the rule action to **Block** or **Fastpath**. Logging is disabled for the **Analyze** action, which allows connections to continue with access control, where other configurations determine their handling and logging.
- Logging is performed on inner flows, not on the encapsulating flow.

Follow these steps to configure logging for tunnel and prefilter rules:

Procedure

Step 1 In the prefilter policy editor, click **Edit** (✎) next to the rule where you want to configure logging.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 2 Click **Logging**.

Step 3 Specify whether you want to **Log at Beginning of Connection** or **Log at End of Connection**.

To optimize performance, log either the beginning or the end of any connection, but not both. Because blocked traffic is immediately denied without further inspection, you cannot log end-of-connection events for Block rules.

Step 4 Specify where to send connection events:

Step 5 Click **Save** to save the rule.

Step 6 Click **Save** to save the prefilter policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Configure logging for decryptable connections with TLS/SSLDecryption rules

Logging decryptable connections allows you to track and analyze traffic that is being monitored by decryption rules. This is particularly important for security analysis and compliance requirements.

Procedure

Step 1 In the decryption policy editor, click **Edit** ( ) next to the rule where you want to configure logging.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 2 Click **Logging**.

Step 3 Check the **Log at End of Connection** check box.

For monitored traffic, end-of-connection logging is required.

Step 4 Specify where to send connection events.

Send events to the event viewer if you want to perform Firewall Management Center-based analysis on these connection events. For monitored traffic, this is required.

Step 5 Click **Save** to save the rule.

Step 6 Click **Save** to save the decryption policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Logging connections with security intelligence

Enable Security Intelligence logging to monitor and analyze network connections, IP addresses, URLs, and domain names for security threats and policy compliance.

The Security Intelligence policy requires the Threat Smart License.

Procedure

Step 1 In the access control policy editor, click **Security Intelligence**.

Step 2 Click the **Logging** ( ) icon to enable Security Intelligence logging using the following criteria:

- By IP address: Click the logging icon next to **Networks**.

- By URL: Click the logging icon next to **URLs**.
- By Domain Name: Click the logging icon next to the **DNS Policy** drop-down list.

If the logging icon is disabled, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 3 Check the **Log Connections** check box.

Step 4 Specify where to send connection and Security-Related connection events.

Send events to the event viewer if you want to perform Firewall Management Center-based analysis, or if you set a Block list to monitor-only.

Step 5 Click **OK** to set logging options.

Step 6 Click **Save** to save the policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Logging connections with access control rules

Depending on your choices for the rule action and deep inspection options, your logging options differ; refer to Rules and policy actions effect on logging, on page 4.

Procedure

Step 1 In the access control policy editor, click **Edit** (✎) next to the rule where you want to configure logging.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 2 Click **Logging**.

Step 3 Specify whether you want to **Log at Beginning of Connection** or **Log at End of Connection**.

To optimize performance, log either the beginning or the end of any connection, but not both.

Step 4 (Optional) Check the **Log Files** check box to log file and malware events associated with the connection.

It is recommended to leave this option enabled.

Step 5 Specify where to send the connection events:

- **Event Viewers**: Send events to the Firewall Management Center. Send events to an on-premises Firewall Management Center if you have configured it to perform event analytics only.
- **Syslog Server**: Configure the policy's default syslog destination under **More** > **Logging**. Enable syslog logging in the applicable rules and configure overrides where required. The managed Threat Defense device must have network connectivity to the configured syslog receiver. For more information, refer to Send Cloud-Delivered Firewall Management Center-Managed Events to SAL (SaaS) Using Syslog.

Show Overrides: Displays the options to override the settings configured in the access control policy.

- **Override Severity**: When you choose this option and select a severity for the rule, connection events for this rule will have the selected severity regardless of the severity configured in the Logging tab in Access Control Policy.
- **Override Default Syslog Destination**: Send the syslog generated for the connection event for this rule to destination specified in this alert.

- **SNMP Trap**: Connection events are sent to the selected SNMP trap.

Step 6 Click **Confirm**.

Step 7 Click **Apply** to save the rule.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Logging connections with a policy default action

A policy's default action determines how the system handles traffic that matches none of the rules in the policy (except Monitor rules in access control and decryption policies, which match and log—but do not handle or inspect—traffic).

Logging settings for the decryption policies default action also govern how the system logs undecryptable sessions.

Before you begin

For prefilter default action logging, set the default action to **Block all tunnel traffic**. Logging is disabled for the **Allow all tunnel traffic** action, which allows connections to continue with access control, where other configurations determine their handling and logging.

Procedure

Step 1 In the policy editor, click the **Default Logging and Inspection** next to the **Default Action** drop-down list.

Step 2 Specify when you want to log matching connections:

- Log at Beginning of Connection: Not supported for SSL default actions.
- Log at End of Connection: Not supported if you choose the access control **Block All Traffic** default action or the prefilter **Block all tunnel traffic** default action.

To optimize performance, log either the beginning or the end of any connection, but not both.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration. In an access control policy, the configuration may also be inherited from an ancestor policy.

Step 3 Specify where to send connection events.

Send events to the event viewer if you want to perform Firewall Management Center-based analysis on these connection events.

Step 4 Click **Apply**.

Step 5 Click **Save** to save the policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Limiting logging of long URLs

End-of-connection events for HTTP traffic record the URL requested by monitored hosts. Disabling or limiting the number of stored URL characters may improve system performance. Disabling URL logging (storing zero characters) does not affect URL filtering. The system filters traffic based on requested URLs even though the system does not record them.

Procedure

Step 1 In the access control policy editor, click **More** > **Advanced Settings**, then click **Edit** (✎) next to **General Settings**.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 2 Enter the **Maximum URL characters to store in connection events**.

Step 3 Click **OK**.

Step 4 Click **Save** to save the policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Application-aware and protocol-aware syslogs

Application-aware and protocol-aware syslogs are a logging mechanism that

- generate logs that include application-specific and protocol-specific traffic data,
- provide enhanced network visibility through comprehensive data collection, and
- use the Snort 3 engine's deep packet inspection capabilities to extract protocol data.

Advanced logging protocols

The Firewall Threat Defense device generates these logs alongside existing connection, intrusion, file, and malware events. As syslogs, you can send these logs to external event management solutions for analysis. When enabled, advanced logging provides a configurable solution for sending these logs from the Firewall Threat Defense device to destination such as Splunk or a syslog alert server.

Advanced logging supports these protocols.

Table 2: Protocols supported by advanced logging

Protocol	Description
CONN	Logs the data collected from end-of-connection events, including the transport protocol, service protocol, and session duration.
DNS	Logs the data collected from responses to TCP and UDP DNS sessions, including commands, their arguments, response codes, and response messages.
FTP	Logs the commands and data exchanged during an FTP session, including the command and its arguments, response codes, and response messages.
HTTP	Logs the data collected from the HTTP responses, including the HTTP method, header, and status code.
NOTICE	Logs the data collected for intrusion events, including the GID:SID pair, rule messages, and associated references.
WEIRD	Logs the data about anomalies detected in traffic flow.

For more information about application log fields, refer to Advanced Logging Syslog Fields.

Advanced logging guidelines and limitations

Advanced logging guidelines and limitations are operational constraints and performance considerations that

- affect network performance when configured without proper filtering,
- require selective configuration to avoid device memory consumption issues, and
- have specific platform and version requirements for support.

Advanced logging restrictions and requirements

Consider these guidelines when implementing advanced logging:

- Advanced logging can degrade network performance if used without filters in the access control rule. To reduce the volume of logs, use access control rules to filter specific traffic types and use networks and ports to limit logging to a particular network configuration.
- Enabling advanced logging for all protocols can impact the Firewall Threat Defense device's performance. Configure advanced logging selectively to avoid increased device memory consumption.

- Advanced logging is supported only on Snort 3-based Firewall Threat Defense devices running Version 10.0 or later.
- Advanced logging does not support sending logs to a syslog server configured in the platform settings. To send events to the default logging destination configured in the access control policy, you must configure a syslog alert server as the default logging destination.
- Advanced logging does not support Splunk profiles that use data interfaces for sending events to Splunk. To send events to Splunk, you must configure the Splunk profile to use the management interface for sending events. For more information about configuring a Splunk profile, refer to Splunk integration: Send events directly from Firewall Management Center.

Enable advanced logging

Configure the Firewall Threat Defense device to generate Snort 3 inspector logs that include application-specific and protocol-specific data and send these logs to event management solutions for analysis.

Caution Advanced logging might cause a performance drop within the network if used without the filters configured in the access control rule. Filter the specific traffic types using the access control rules to reduce the volume of logged traffic. Use the networks and ports in the access control rules to limit logging to a particular network configuration.

Before you begin

- Ensure that connection logging is enabled in your access control policy.
- Ensure that you have configured the logging destination, such as Splunk or the local syslog server, to which you want to send the logs.

Procedure

Step 1 Choose **Policies** > **Security policies** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy that you want to edit.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 In the access control policy editor, select **Advanced Settings** from the **More** drop-down menu at the end of the packet flow line.

Step 4 Click the **Edit** (✎) icon next to **Advanced Logging**.

Step 5 Check the **Enable advanced logging** check box to enable logging.

Step 6 Choose the log file format. By default, JSON format is selected.

Step 7 You can send event logs to the default logging destination configured in the access control policy's logging settings, or to one or more of the following destinations:

- **All Splunk profiles**
- **Syslog**

Note

- If you choose to send event logs to the default logging destination configured in the access control policy, note that advanced logging does not support sending logs to the syslog server configured in the platform settings. You must configure a syslog alert server as the default logging destination.
- If you choose the **All Splunk profiles** option, note that advanced logs are sent to all Splunk profiles configured for a Firewall Threat Defense device.
- Advanced logging does not support Splunk profiles that use data interfaces for sending events to Splunk. To send events to Splunk, you must configure the Splunk profiles to use the management interface for sending events.

Caution Sending advanced logging syslog to multiple destinations might impact device's performance.

- Click **Save**.

Step 8 Click **Save** to save the policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Configure protocols for advanced logging

Advanced logging for application protocols allows you to monitor and analyze network connections by capturing detailed information about specific application protocols. This feature is configured at the access control policy level and can be applied to individual rules within the policy.

Before you begin

Ensure that you have enabled the advanced logging feature for the access control policy that you want to modify.

Follow these steps to configure protocols for advanced logging:

Procedure

Step 1 Choose **Policies** > **Security policies** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 In the access control policy editor, you have the options to add a new rule or edit an existing rule.

- To add a new rule, click **Add Rule**.
- To edit an existing rule, click **Edit** (✎).

Step 4 Click **Advanced Logging**.

Step 5 Check the check box next to the application protocol for which you want to log the connection.



Caution Enabling logging for all the protocols in a Firewall Threat Defense device might affect its performance, because the device must extract data, convert it to targeted formatting, and send it to the configured destination.

Step 6 Click **Confirm**.

Step 7 Click **Apply** to save the rule.

Step 8 Click **Save** to save the policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Monitor and troubleshoot advanced logging

To collect statistics of the advanced logging events and to get health alerts, you must enable the **Snort 3 Statistics** module in your Firewall Threat Defense device's health policy (**Troubleshooting** > **+ Show more** > **Health** > **Policies**). When enabled, you can monitor metrics such as the number of advanced logging events that are dropped, failed to send, or sent successfully.

To view these health metrics, navigate to **Troubleshooting** > **Health** > **Monitor** and then add the metrics to a dashboard by selecting them from the **Snort 3 Performance Statistics** group.

Advanced Logging events failed to transmit to syslog servers

This alert appears when the syslog messages fail to transmit due to a connection issue with the syslog server or a configuration error.

- Check the status of your syslog server to ensure it is operational and accessible.
- Verify the syslog configuration within the Firewall Management Center for any errors.

Advanced logging events to syslog servers were dropped

This alert appears when syslog messages are dropped due to memory overflow in the Firewall Threat Defense device, suggesting that the device cannot process logs at the current rate.

Review your advanced logging configuration. Consider applying more granular filters in your access control rules to reduce the volume of logs generated, or selectively enable advanced logging for fewer protocols, to decrease device memory consumption. For more information, refer to Advanced logging guidelines and limitations, on page 19.