

Viewing Events

You can view real-time events logged against the traffic inspected by the ASA FirePOWER module.

Note The module only caches the most recent 100 events in memory.

For more information, see the following sections:

- Accessing ASA FirePOWER Real-Time Events, page 37-1
- Understanding ASA FirePOWER Event Types, page 37-2
- Event Fields in ASA FirePOWER Events, page 37-3
- Intrusion Rule Classifications, page 37-12

Accessing ASA FirePOWER Real-Time Events

You can view events detected by the ASA FirePOWER module in several predefined event views or create a custom event view to view the event fields you select.

Note The module only caches the most recent 100 events in memory.

To view ASA FirePOWER events:

Step 1 Select **Monitoring > ASA FirePOWER Monitoring > Real-time Eventing**.

Step 2 You have two choices:

- Click an existing tab for the type of event you want to view: connection events, security intelligence events, intrusion events, file events, or malware events.
- Click the + icon to create a custom event view and select the event fields you want to include in the view.

For more information, see Understanding ASA FirePOWER Event Types, page 37-2 and Event Fields in ASA FirePOWER Events, page 37-3.

Understanding ASA FirePOWER Event Types

The ASA FirePOWER module provides real-time event viewing of event fields from five event types: connection events, security intelligence events, intrusion events, file events, and malware events.

Connection Events

Connection logs, called *connection events*, contain data about the detected sessions. The information available for any individual connection event depends on several factors, but in general 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 access control rule (or other configuration) in which policy handled the traffic, whether the connection was allowed or blocked, and so on

Various settings in access control give you granular control over which connections you log, when you log them, and where you store the data. You can log any connection that your access control policies can successfully handle. You can enable connection logging in the following situations:

- when a connection is blacklisted (blocked) or monitored by the reputation-based Security Intelligence feature
- when a connection is handled by an access control rule or the access control default action

In addition to the logging that you configure, the system automatically logs most connections where the system detects a prohibited file, malware, or intrusion attempt.

Security Intelligence Events

When you enable Security Intelligence logging, blacklist matches automatically generate *Security Intelligence events* as well as connection events. A Security Intelligence event is a special kind of connection event that you can view and analyze separately. For detailed information on configuring connection logging, including Security Intelligence blacklisting decisions, see Logging Connections in Network Traffic, page 36-1.

Tip General information about connection events also pertains to Security Intelligence events, unless otherwise noted. For more information on Security Intelligence, see Blacklisting Using Security Intelligence IP Address Reputation, page 5-1.

Intrusion Events

The system examines the packets that traverse your network for malicious activity that could affect the availability, integrity, and confidentiality of a host and its data. When the system identifies a possible intrusion, it generates an *intrusion event*, which is a record of the date, time, type of exploit, and contextual information about the source of the attack and its target.

File Events

File events represent files that the system detected, and optionally blocked, in network traffic.

The system logs the file events generated when a managed device detects or blocks a file in network traffic, according to the rules in currently applied file policies.

Malware Events

Malware events represent malware files detected, and optionally blocked, in network traffic by the system.

With a Malware license, your ASA FirePOWER module can detect malware in network traffic as part of your overall access control configuration; see Understanding and Creating File Policies, page 35-4.

The following scenarios can lead to generating malware events:

- If a managed device detects one of a set of specific file types, the ASA FirePOWER module performs a malware cloud lookup, which returns a file disposition to the ASA FirePOWER module of `Malware`, `Clean`, or `Unknown`.
- If the ASA FirePOWER module cannot establish a connection with the cloud, or the cloud is otherwise unavailable, the file disposition is `Unavailable`. You may see a small percentage of events with this disposition; this is expected behavior.
- If the managed device detects a file on the clean list, the ASA FirePOWER module assigns a file disposition of `Clean` to the file.

The ASA FirePOWER module logs records of files' detection and dispositions, along with other contextual data, as malware events.

Files detected in network traffic and identified as malware by the ASA FirePOWER module generate both a file event and a malware event. This is because to detect malware in a file, the system must first detect the file itself.

Event Fields in ASA FirePOWER Events

Action

For connection or security intelligence events, the action associated with the access control rule or default action that logged the connection:

- `Allow` represents explicitly allowed and user-bypassed interactively blocked connections.
- `Trust` represents trusted connections. TCP connections detected by a trust rule on the first packet only generate an end-of-connection event. The system generates the event one hour after the final session packet.
- `Block` and `Block with reset` represent blocked connections. The system also associates the `Block` action with connections blacklisted by Security Intelligence, connections where an exploit was detected by an intrusion policy, and connections where a file was blocked by a file policy.
- `Interactive Block` and `Interactive Block with reset` mark the beginning-of-connection event that you can log 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, any additional connection events you log for the session have an action of `Allow`.
- `Default Action` indicates the connection was handled by the default action.
- 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`.

For file or malware events, the file rule action associated with the rule action for the rule the file matched, and any associated file rule action options.

Allowed Connection

Whether the system allowed the traffic flow for the event.

Application

The application detected in the connection.

Application 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.

Application Categories

Categories 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.

Application Tag

Tags that characterize the application to help you understand the application's function.

Block Type

The type of block specified in the access control rule matching the traffic flow in the event: block or interactive block.

Client

The client application detected in the connection.

If the system cannot identify the specific client used in the connection, this field displays `client` appended to the application protocol name to provide a generic name, for example, `FTP client`.

Client Business Relevance

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

Client Categories

Categories that characterize the client detected in the traffic to help you understand the client's function.

Client Risk

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

Client Tag

Tags that characterize the client detected in the traffic to help you understand the client's function.

Client Version

The version of the client detected in the connection.

Connection

The unique ID for the traffic flow, internally generated.

Connection Blocktype Indicator

The type of block specified in the access control rule matching the traffic flow in the event: block or interactive block.

Connection Bytes

The total bytes for the connection.

Connection Time

The time for the beginning of the connection.

Connection Timestamp

The time the connection was detected.

Context

The metadata identifying the security context through which the traffic passed. Note that the system only populates this field for devices in multiple context mode.

Denied Connection

Whether the system denied the traffic flow for the event.

Destination Country and Continent

The country and continent of the receiving host.

Destination IP

The IP address used by the receiving host.

Destination Port, Destination Port Icode, Destination Port/ICMP Code

The destination port or ICMP code used by the session responder.

Direction

The direction of transmission for a file.

Disposition

One of the following file dispositions:

- `Malware` indicates that the cloud categorized the file as malware.
- `Clean` indicates that the cloud categorized the file as clean, or that a user added the file to the clean list.
- `Unknown` indicates that a malware cloud lookup occurred before the cloud assigned a disposition. The file is uncategorized.
- `Custom Detection` indicates that a user added the file to the custom detection list.

- `Unavailable` indicates that the ASA FirePOWER module could not perform a malware cloud lookup. You may see a small percentage of events with this disposition; this is expected behavior.
- `N/A` indicates a Detect Files or Block Files rule handled the file and the ASA FirePOWER module did not perform a malware cloud lookup.

Egress Interface

The egress interface associated with the connection. Note that, if your deployment includes an asynchronous routing configuration, the ingress and egress interface may belong to the same interface set.

Egress Security Zone

The egress security zone associated with the connection.

Event

The event type.

Event Microseconds

The time, in microseconds, when the event was detected.

Event Seconds

The time, in seconds, when the event was detected.

Event Type

The type of event.

File Category

The general categories of file type, for example: `Office Documents`, `Archive`, `Multimedia`, `Executables`, `PDF files`, `Encoded`, `Graphics`, or `System Files`.

File Event Timestamp

The time and date the file or malware file was created.

File Name

The name of the file or malware file.

File SHA256

The SHA-256 hash value of the file.

File Size

The size of the file or malware file, in kilobytes.

File Type

The file type of the file or malware file, for example, `HTML` or `MSEXE`.

File/Malware Policy

The file policy associated with the generation of the event.

Filelog Blocktype Indicator

The type of block specified in the file rule matching the traffic flow in the event: block or interactive block.

Firewall Policy Rules/SI Category

The name of the blacklisted object that represents or contains the blacklisted IP address in the connection. The Security Intelligence category can be the name of a network object or group, the global blacklist, a custom Security Intelligence list or feed, or one of the categories in the Intelligence Feed. Note that this field is only populated if the **Reason** is `IP Block` or `IP Monitor`; entries in Security Intelligence event views always display a reason.

Firewall Rule

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

First Packet

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

HTTP Referrer

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

IDS Classification

The classification where the rule that generated the event belongs. See the Rule Classifications table for a list of rule classification names and numbers.

Impact

The impact level in this field indicates the correlation between intrusion data, network discovery data, and vulnerability information.

Impact Flag

See Impact.

Ingress Interface

The ingress interface associated with the connection. Note that, if your deployment includes an asynchronous routing configuration, the ingress and egress interface may belong to the same interface set.

Ingress Security Zone

The ingress security zone associated with the connection.

Initiator Bytes

The total number of bytes transmitted by the session initiator.

Initiator Country and Continent

When a routable IP is detected, the country and continent associated with the host IP address that initiated the session.

Initiator IP

The host IP address (and host name, if DNS resolution is enabled) that initiated the session responder.

Initiator Packets

The total number of packets transmitted by the session initiator.

Inline Result

One of the following:

- a black down arrow, indicating that the system dropped the packet that triggered the rule
- a gray down arrow, indicating that IPS would have dropped the packet if you enabled the **Drop when Inline** intrusion policy option (in an inline deployment), or if a Drop and Generate rule generated the event while the system was pruning
- blank, indicating that the triggered rule was not set to Drop and Generate Events
- Note that the system does not drop packets in a passive deployment, including when an inline interface is in tap mode, regardless of the rule state or the inline drop behavior of the intrusion policy.

IPS Blocktype Indicator

The action of the intrusion rule matching the traffic flow in the event.

Last Packet

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

MPLS Label

The Multiprotocol Label Switching label associated with the packet that triggered this intrusion event.

Malware Blocktype Indicator

The type of block specified in the file rule matching the traffic flow in the event: block or interactive block.

Message

The explanatory text for the event.

For rule-based intrusion events, the event message is pulled from the rule. For decoder- and preprocessor-based events, the event message is hard coded.

For malware events, any additional information associated with the malware event. For network-based malware events, this field is populated only for files whose disposition has changed.

Monitor Rules

Up to eight Monitor rules matched by that connection.

Netbios Domain

The NetBIOS domain used in the session.

Original Client Country and Continent

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

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.

Policy

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

Policy Revision

The revision of the access control, file, intrusion, or network analysis policy (NAP), if any, associated with the generation of the event.

Priority

The event priority as determined by the Cisco VRT.

Protocol

The protocol detected in the connection.

Reason

The reason or reasons the connection was logged, in the following situations:

- `User Bypass` indicates that the system initially blocked a user's HTTP request, but the user chose to continue to the originally requested site by clicking through a warning page. A reason of `User Bypass` is always paired with an action of `Allow`.
- `IP Block` indicates that the system denied the connection without inspection, based on Security Intelligence data. A reason of `IP Block` is always paired with an action of `Block`.
- `IP Monitor` indicates that the system would have denied the connection based on Security Intelligence data, but you configured the system to monitor, rather than deny, the connection.
- `File Monitor` indicates that the system detected a particular type of file in the connection.
- `File Block` indicates the connection contained a file or malware file that the system prevented from being transmitted. A reason of `File Block` is always paired with an action of `Block`.
- `File Custom Detection` indicates the connection contained a file on the custom detection list that the system prevented from being transmitted.
- `File Resume Allow` indicates that file transmission was originally blocked by a Block Files or Block Malware file rule. After a new access control policy was applied that allowed the file, the HTTP session automatically resumed. Note that this reason only appears in inline deployments.
- `File Resume Block` indicates that file transmission was originally allowed by a Detect Files or Malware Cloud Lookup file rule. After a new access control policy was applied that blocked the file, the HTTP session automatically stopped. Note that this reason only appears in inline deployments.

- `Intrusion Block` indicates the system blocked or would have blocked an exploit (intrusion policy violation) detected in the connection. A reason of `Intrusion Block` is paired with an action of `Block` for blocked exploits and `Allow` for would-have-blocked exploits.
- `Intrusion Monitor` indicates 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**.
- `Content Restriction` indicates the system modified the packet to enforce content restrictions related to either the Safe Search or YouTube EDU feature.

Receive Times

The time the destination host or responder responded to the event.

Referenced Host

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

Responder Bytes

The total number of bytes transmitted by the session responder.

Responder Country and Continent

When a routable IP is detected, the country and continent associated with the host IP address for the session responder.

Responder Packets

The total number of packets transmitted by the session responder.

Responder IP

The host IP address (and host name, if DNS resolution is enabled) that responded to the session initiator.

Security Group Tag Name

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.

Signature

The signature ID of the intrusion rule matching the traffic for the event.

Source Country and Continent

The country and continent of the sending host.

Source IP

The IP address used by the sending host in an intrusion event.

Source or Destination

The host originating or receiving the connection for the event.

Source Port, Source Port Type, Source Port/ICMP Type

The source port or ICMP type used by the session initiator.

TCP Flags

The TCP flags detected in the connection.

URL

The URL requested by the monitored host during the session.

URL Category

The category associated with the URL requested by the monitored host during the session, if available.

URL Reputation

The reputation associated with the URL requested by the monitored host during the session, if available.

URL Reputation Score

The reputation score associated with the URL requested by the monitored host during the session, if available.

User

The user of the host (**Receiving IP**) where the event occurred.

User Agent

User agent application information extracted from HTTP traffic detected in the connection.

VLAN

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

Web App Business Relevance

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

Web App Categories

Categories that characterize the web application detected in the traffic to help you understand the web application's function.

Web App Risk

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

Web App Tag

Tags that characterize the web application detected in the traffic to help you understand the web application's function.

Web Application

The web application detected in the traffic.

Intrusion Rule Classifications

Intrusion rules include an attack classification. The following table lists the name and number for each classification

Table 37-1 Rule Classifications

Number	Classification Name	Description
1	not-suspicious	Not Suspicious Traffic
2	unknown	Unknown Traffic
3	bad-unknown	Potentially Bad Traffic
4	attempted-recon	Attempted Information Leak
5	successful-recon-limited	Information Leak
6	successful-recon-largescale	Large Scale Information Leak
7	attempted-dos	Attempted Denial of Service
8	successful-dos	Denial of Service
9	attempted-user	Attempted User Privilege Gain
10	unsuccessful-user	Unsuccessful User Privilege Gain
11	successful-user	Successful User Privilege Gain
12	attempted-admin	Attempted Administrator Privilege Gain
13	successful-admin	Successful Administrator Privilege Gain
14	rpc-portmap-decode	Decode of an RPC Query
15	shellcode-detect	Executable Code was Detected
16	string-detect	A Suspicious String was Detected
17	suspicious-filename-detect	A Suspicious Filename was Detected
18	suspicious-login	An Attempted Login Using a Suspicious Username was Detected
19	system-call-detect	A System Call was Detected
20	tcp-connection	A TCP Connection was Detected
21	trojan-activity	A Network Trojan was Detected
22	unusual-client-port-connection	A Client was Using an Unusual Port
23	network-scan	Detection of a Network Scan
24	denial-of-service	Detection of a Denial of Service Attack
25	non-standard-protocol	Detection of a Non-Standard Protocol or Event
26	protocol-command-decode	Generic Protocol Command Decode
27	web-application-activity	Access to a Potentially Vulnerable Web Application
28	web-application-attack	Web Application Attack
29	misc-activity	Misc Activity
30	misc-attack	Misc Attack
31	icmp-event	Generic ICMP Event

Table 37-1 Rule Classifications

Number	Classification Name	Description
32	inappropriate-content	Inappropriate Content was Detected
33	policy-violation	Potential Corporate Privacy Violation
34	default-login-attempt	Attempt to Login By a Default Username and Password
35	sdf	Sensitive Data
36	malware-cnc	Known malware command and control traffic
37	client-side-exploit	Known client side exploit attempt
38	file-format	Known malicious file or file based exploit