

LOGZILLA DOCUMENTATION

Cisco Firepower

LogZilla App Store application: Cisco Firepower

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/cisco-firepower

Overview

Cisco Firepower provides application control, intrusion protection, anti-malware, and URL filtering for Cisco network devices. The Firepower Management Center (FMC) provides centralized management.

Firepower-specific security events (430xxx) include intrusion detection, malware alerts, file events, and connection logging. Standard FTD syslog messages (106xxx, 302xxx, 722xxx, etc.) are processed by the Cisco ASA app since they share the same format.

App Function

- Parse 430xxx security events (intrusion, connection, file, malware)
- Parse FirepowerExternal events from eStreamer
- Extract network metadata from comma-separated KV format
- Map security events to MITRE ATT&CK techniques
- Detect torrent connections

Vendor Documentation

- [Cisco Firepower Management Center Configuration Guide](https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html) (https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html)
- [Cisco Firepower Threat Defense Syslog Messages](https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_ftd_syslog_guide.html) (https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_ftd_syslog_guide.html)

Device Configuration

Configure Firepower devices to send syslog messages to LogZilla:

Log into the Firepower Management Center

Navigate to **Devices > Platform Settings**

Select or create a platform settings policy

Click **Syslog** in the left menu

Enable syslog and configure:

- **Syslog Server:** LogZilla server IP address
- **Port:** 514
- **Protocol:** UDP or TCP

Deploy the policy to managed devices

Verification

Generate test traffic or trigger a security event, then verify events appear in LogZilla with the mnemonic `%FTD-x-430xxx` or `%FTD-x-722xxx`.

Incoming Log Format

Two log formats are processed by the Firepower app:

- **Security events (430xxx)** - Comma-separated KV pairs with mnemonic prefix
- **FirepowerExternal** - eStreamer events with key="value" format

Parsed Metadata Fields

Tag Name	Example	Description
Event Class	security	Cross-vendor event classification
Event Type	intrusion	Specific event type (intrusion, malware, access_denied)
Security Alert	Intrusion	Security event type (430xxx)
MitreId	T1190	MITRE ATT&CK technique ID
MITRE Tactic	Initial Access	MITRE ATT&CK tactic
SrcIP	192.168.1.100	Source IP address
DstIP	8.8.8.8	Destination IP address
DstPort	https	Destination port with service name
Protocol	TCP	Network protocol
SrcInt	inside	Source/ingress interface

Tag Name	Example	Description
DstInt	outside	Destination/egress interface
SrcZone	Inside-ASA	Source security zone
DstZone	Outside-ASA	Destination security zone
Action	Allow	Access control rule action
Rule	Permit Any	Access control rule name
NAP Policy	Balanced Security	Network analysis policy
Torrent	10.1.1.1 -> 8.8.8.8:6884	Detected torrent connection

Log Examples

Security Event (430002 - Connection Start)

```
%FTD-6-430002: EventPriority: Low, DeviceUUID: b2433c5c-a6a1-11eb-a6e7-be0b9833091f,
InstanceID: 2, FirstPacketSecond: 2021-04-30T11:31:19Z, ConnectionID: 4,
AccessControlRuleAction: Allow, SrcIP: 172.16.10.10, DstIP: 172.16.20.10,
ICMPType: Echo Request, ICMPCode: No Code, Protocol: icmp, IngressInterface: inside,
EgressInterface: outside, ACPolicy: Default Allow All Traffic,
AccessControlRuleName: test, Client: ICMP client, ApplicationProtocol: ICMP,
InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 74, ResponderBytes: 0,
NAPPolicy: Balanced Security and Connectivity
```

FirepowerExternal Event

```
FirepowerExternal: Protocol="TCP" SrcIP="10.1.1.100" DstIP="8.8.8.8"
SrcPort="54321" DstPort="443" Action="Allow"
```

Triggers

Trigger	Description
Cisco Firepower: MITRE ATT&CK Threat Detected	Alerts on any MITRE-mapped threat
Cisco Firepower: Malware Detected	Alerts on malware detection (actionable)
Cisco Firepower: Intrusion Detected	Alerts on intrusion detection (actionable)
Cisco Firepower: Traffic Blocked	Marks blocked traffic as actionable
Cisco Firepower: File Policy Violation	Alerts on file policy violations
Cisco Firepower: Torrent Activity	Alerts on torrent connections (policy violation)