LOGZILLA DOCUMENTATION

Cisco ASA

Rules, dashboards, and triggers for Cisco Adaptive Security Appliances

LogZilla App Store · Generated June 12, 2026 · logzilla.ai/docs/logzilla-appstore/cisco—asa

Overview

Cisco Adaptive Security Appliance (ASA) is a network security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. ASA devices provide security services for networks of all sizes, from small offices to large enterprise data centers. Cisco Firepower Threat Defense (FTD) devices are also supported.

App Function

- Parse Cisco ASA and FTD syslog messages and extract network security metadata
- Map security events to MITRE ATT&CK techniques for threat intelligence
- Create user tags for source and destination IP addresses, ports, and interfaces
- Extract firewall action (Allow/Deny/Drop) for traffic disposition analysis
- Process connection buildup and teardown events for network monitoring
- Extract user authentication and authorization details
- Generate mapped IP address information for NAT translations

Vendor Documentation

- Cisco ASA Series (https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html)
- ASA Syslog Configuration Guide (https://www.cisco.com/c/en/us/td/docs/security/asa/asa920/configuration/general/asa-920-general-config/monitor-syslog.html)
- ASA System Log Messages (https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog.html)

Device Configuration

Configure the Cisco ASA or FTD device to send syslog messages to LogZilla:

Log into the ASA via CLI or ASDM

Configure the logging destination:

```
logging enable
logging host inside <logzilla-ip> udp/514
logging trap informational
logging device-id hostname
```

Save the configuration:

```
write memory
```

Verification

Generate test traffic or trigger a configuration change, then verify events appear in LogZilla by selecting the User Tags menu for `Vendor` -> `Cisco` and `Product` -> `ASA` or `FTD`.

Incoming Log Format

Cisco ASA logs use standard syslog format with Cisco mnemonic identifiers. Messages follow the pattern:

```
%ASA-[severity]-[message_id]: [message_text]
```

The message text contains structured information about security events, connection states, authentication attempts, and network translations.

Parsed Metadata Fields

The Cisco ASA app extracts the following user tags from log messages:

Tag Name	Example	Description
`Vendor`	`Cisco`	Vendor name (always Cisco)
`Product`	`ASA`	Product name (ASA or FTD)
`Event Class`	`security`	Event classification (network, security, auth, ha, system)
`Event Type`	`access_denied`	Specific event type (login_failure, intrusion, scan_detected, attack, access_denied)
`Action`	`Deny`	Firewall action (Allow, Deny, Drop)
`MitreId`	`T1498`	MITRE ATT&CK technique ID (enables UI lookup)
`MITRE Tactic`	`Impact`	MITRE ATT&CK tactic name
`SrcIP`	`192.168.1.100`	Source IP address

Tag Name	Example	Description
DstIP	10.0.0.50	Destination IP address
SrcNAT	203.0.113.10	NAT translated source IP
DstNAT	198.51.100.20	NAT translated destination IP
SrcInt	inside	Source interface name
DstInt	outside	Destination interface name
DstPort	443	Destination port number
Protocol	TCP	Network protocol
User	john.doe	Username for authentication events

Supported Message Types

The app processes all ASA/FTD syslog messages and categorizes them by prefix:

Prefix	Event Class	Description
105xxx	ha	Failover and HA events
106xxx	security	Denied connections, ACL hits
111xxx	config	Configuration changes
113xxx	auth	AAA authentication events
302xxx	network	Connection build/teardown
305xxx	network	NAT translations
605xxx	auth	Login events
722xxx	auth	VPN session events
733xxx	security	Threat detection (DDoS, scanning)

MITRE ATT&CK Mappings

Security-relevant messages are mapped to MITRE ATT&CK techniques:

Message ID	Technique	Tactic
733100-733105	T1498	Impact (DDoS)
733101-733103	T1046	Discovery (Scanning)
106016, 106021	T1557	Credential Access (Spoofing)
106xxx (denied)	T1071	Command and Control
113005-113015	T1110	Credential Access (Brute Force)
722051	T1133	Initial Access (VPN)

Log Examples

Dynamic NAT Translation

```
%ASA-6-305009: Built dynamic translation from inside:192.168.1.100 to outside:203.0.113.10
```

Connection Buildup

```
%ASA-6-302013: Built inbound TCP connection 12345 for outside:203.0.113.50/443 (203.0.113.50/443) to
inside:192.168.1.100/54321 (192.168.1.100/54321)
```

Access Denied

```
%ASA-4-106023: Deny tcp src outside:203.0.113.100/12345 dst inside:192.168.1.50/80 by access-group
"outside_access_in" [0x0, 0x0]
```

Authentication Event

```
%ASA-6-113009: AAA retrieved default group policy (VPN_Policy) for user = john.doe
```

Threat Detection

```
%ASA-4-733100: [Scanning] drop rate 1 exceeded. Current burst rate is 10 per second
```

Triggers

The app includes the following triggers:

Trigger Name	Description	Actionable
Cisco ASA: DDoS Attack Detected	Threat detection rate exceeded (T1498)	Yes
Cisco ASA: Network Scanning Detected	Scanning activity detected (T1046)	Yes
Cisco ASA: IP Spoofing Attack	IP spoofing attempt (T1557)	Yes
Cisco ASA: Blocked C2 Communication	Denied traffic with C2 indicators (T1071)	Yes
Cisco ASA: Brute Force Attempt	Authentication failures (T1110)	Yes
Cisco ASA: External Remote Access	VPN session events (T1133)	Yes
Cisco ASA: Failover Event	HA/Failover state changes	Yes
Cisco ASA: MITRE ATT&CK Detection	Any event with MITRE mapping	Yes