Cisco ASA

Detection Strategy Guide

July 2025

Product Overview

The Cisco ASA is a series of network security devices that provide firewall, VPN, and intrusion prevention capabilities to protect corporate networks and data centers. As a firewall, the ASA inspects network traffic and enforces access control policies to block unauthorized access and malicious activity at the network perimeter. In addition to stateful firewall inspection, Cisco ASAs offer a range of integrated security services, including remote access VPN (AnyConnect) and site-to-site VPN, ensuring secure connectivity for a distributed workforce. Its security features help defend against a variety of network-based attacks and provide a foundational layer of security for an organization's infrastructure.

Detection Strategy for Network Integrations

Detection

Network traffic monitoring is a critical element of our detection strategy, offering insight into the activity of data as it moves across an organization's systems. The network traffic data source focuses on network connection creation, content, and flow. We pull this information into our detection pipeline as events in the form of both security alerts and raw telemetry (depending on the integration). When a threat is detected, our automated response bot, Ruxie, takes action by enriching evidence fields with first- and third-party threat intelligence.

Response

Network technologies are utilized for support across many types of Expel Alerts such as endpoint and cloud. The main focus of the response strategy is on source IP, destination IP, and domain tracking to identify related connections, along with user activity summaries to give extra alert context.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for Cisco ASA

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Cisco ASA, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported platforms	■ Cisco ASA
Cisco ASA detection rules support	No.
Detection rules written by Expel	Yes.
Auto remediations	No.
Investigative support through Workbench	Yes.
Hunting support	No. Hunting is not currently available for this integration.

Additional Details and Common Questions

Console Access

A vendor alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.