Palo Alto Networks Next Gen Firewall

Detection Strategy Guide

June, 2025

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.

Product Overview

Palo Alto Networks (PAN) has one of the most common Next-Generation Firewalls (NGFW) on the market. Beyond standard firewall functions like allowing and blocking traffic, PAN offers intelligent threat prevention, URL filtering, and advanced malware analysis capabilities through WildFire. The PA-Series NGFWs employ a unique single-pass architecture that enables comprehensive Layer 7 security by identifying applications regardless of port, protocol, evasive techniques, or encryption (TLS/SSL). These firewalls are designed to stop the most evasive threats with machine learning-driven threat prevention, and can capture PCAPs when alerts are generated for forensic analysis.

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 (the initial construction of a network connection such as socket information, and src and dst IP and Ports), network traffic content (logged network traffic data showing both protocol header and body values like PCAP), and network traffic flow (summarized network packet data, with metrics, such as protocol headers and volume like netflow or http logs).

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. Additional Ruxie actions query a wide span of technologies directly to arm analysts with key pieces of investigative information and related events.

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.

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.

What We Support for Palo Alto Networks Next Gen Firewall

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** exp**e**ct **t**his) that we support for Palo Alto Networks Next Gen Firewall, you can view the Detections page in Workbench, or ask your Sales or Support rep for the most recent download.

Supported versions	Version 6+
Supported event log sources	■ Spyware ■ Wildfire ■ Wildfire-Virus ■ Virus ■ Vulnerability
Palo Alto Networks Next Gen Firewall detection rules support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query IP ■ Query User ■ Query Domain ■ Query Netflow ■ Query File ■ Acquire PCAP
Hunting support	Yes, if logs are sent to a supported SIEM (SumoLogic or Splunk) and Expel has API access to extract the data. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help understanding the hypotheses and objectives for each hunting technique. For a full list of techniques by integration, see Hunting Techniques in the Help Center.

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.

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.

Use Cases Not Supported

- Expel does not have the ability to mark alerts as resolved in the PAN NGFW console via Workbench.
- Expel does not support PAN NGFW actions for containment or for remediation actions.

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.