Netskope CASB and Next Gen SWG

Detection Strategy Guide

June, 2025

Product Overview

Netskope CASB and Next Gen SWG are cloud-based web security solutions that prevent malware, detect advanced threats, filter by category, protect data, and control app use for any user, location, or device.

Netskope is a focused integration for Expel. We use it to catch early-stage network indicators of compromise. Individual detections within this stage will change over time as threats evolve and we refine our detection portfolio based on real-world performance. To get the most value from this integration, we use it within correlated detections, correlate the behavior to endpoint activity, and surface it for our SOC as an investigative source. DLP alerts may be enabled by Workbench configuration to generate automatic Verify Actions.

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.

What We Support for Netskope CASB and Next Gen SWG

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 Netskope CASB and Next Gen SWG, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported event log sources	■ Netskope platform alerts The Netskope platform has one central aggregation endpoint for all alerts from all platform modules.
Netskope CASB and Next Gen SWG 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 User ■ Query IP ■ Query Domain ■ Network Vendor ■ Recent Events Workflow ■ Network Connections to EDR Workflow ■ Domain Info Workflow
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.

Use Cases Not Supported

Common web browsing activity and blocked traffic for “policy based” offenses are not reviewed by SOC analysts.