

Splunk Integration with Aruba CX 10000 with Pensando

Integration Overview

Pensando ensures that any customer can easily build on the power of their existing Splunk environment by providing integrated access to data available from the Pensando Distributed Services Platform. Pensando/Splunk integration supports the ingestion of IPFIX and Syslog records gathered by the platform from each Aruba CX 10000 with Pensando Distributed Services Switch (DSS) deployed within the data center.

Pensando/Splunk integration aids Network and Security Operations in one of their most fundamental tasks: identifying issues as early as possible, before they grow into major problems. With security now part of the data center fabric, insights into East/West traffic is simplified.

Each DSS reports connection data on each flow it secures. New use-case-specific visualizations simplify the security operations teams' ability to leverage this information at any time.



The net result: **Operations can immediately uncover workload and workload connection issues and begin remediation in real time.**

Pensando has designed views to support the NOC team as well as the SOC team, showing contextual information from the platform's integrated firewall, based on aggregated DSS data.

Use Cases Supported

- **Threat Management.** Gain rapid insight into firewall policy violations and find applications that are behaving contrary to the policies they are mapped to. Quickly determine if there is a rule issue, an application communication issue, or an actual break/infection that needs to be addressed.
- **Security Policy Utilization.** Easily review each security policy usage. Number of workloads protected by each policy, bi-directional network utilization and connections for each workload.