Security Analytics and Logging (SAL)

Cisco Partner
https://cs.co/1page

Security Analytics and Logging (SAL) provides large scale central management of firewall logs data, both as a cloud-hosted service or on-premises appliance hosted application. This allows firewalls to directly log to the cloud or on-prem and uses API integrations for presenting the data back to the user in platform of their choice.

Benefits:

Simplify security management. Greatly reduce false positives with high-fidelity alerts and simplified policy orchestration.

Provide better intelligence to harmonize policy management. Monitor your networks and deploy behavioral-based analytics on firewall logs and network telemetry.

Enhance threat detection across the organization. Detect internal and external threats or suspicious activity by proactively monitoring network behavior. Using advanced analytics powered by Secure Network Analytics SaaS, detect threats such as C&C attacks, ransomware, DDoS attacks, illicit cryptomining, known malware, and insider threats.

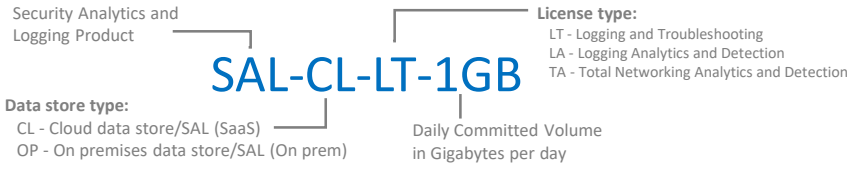
Meet compliance mandates. Enable logging and analytics capabilities to easily monitor your organization for compliance with industry regulations such as PCI, HIPAA, FISMA, and more.

Packages:

Logging and Troubleshooting (LT): The first tier offers log viewing for FTD and ASA models. This live event viewer includes download capabilities and a base storage period of 3 months, which can be upgraded to 1, 2, or 3 yrs.

Logging Analytics and Detection (LA): The second-tier correlates firewall log data leveraging Cisco Secure Network Analytics, as well as trigger new alerts customized for SAL logs. Users can access alerts based solely on firewall log data like malware event observation, IDS notice spike, potentially harmful hidden file extension, and many more.

Total Network Analytics and Detection (TA): The third and final tier offers consolidated analysis on the combined dataset of firewall, internal, and even public cloud logs for comprehensive threat detection. This unlocks its full potential. With this license, get more effective threat detections and protection at the perimeter, inside your network, and in the public cloud.



Feature Matrix:

	SAL On Prem Single Node	SAL On Prem Multi Node	SAL (SaaS)
NGFW Event Logging [3]	✓	✓	✓
FTD Data-Plane Logging	✗	Short-term Roadmap	Future Dev
ASA Events Logging [3]	✗	Short-term Roadmap	✓
Event Viewing in Dev. Manager	FMC	FMC	CDO
Cross-launch from Dev. Manager	FMC	FMC	CDO
Remote Query by Manager (APIs) [2]	FMC	FMC	CDO
Behavioral Threat Detections	✗	Future Dev	✓
Sustained logging rate EPS Events Per Sec (EPS)	20,000 eps (2.25TB/Day)	Virtual: 50,000 eps (5.6TB/day) HW: 100,000 eps (11.2TB/day)	Cloud scale (unlimited)
Avg. Retention at sustained rate [1]	~25 days	~30 days	3 years (extendable)
Appliance / Architecture	Standalone SNA Mgmt. Console (Virtual or HW)	SNA: Mgmt. Console, Flow Collector and Data Store (Virtual or HW)	Cloud Hosted (SaaS)
Point of logs ingest	SNA Mgt Console	SNA Flow Collector	Direct to Cloud/SEC

[1] The on-prem retention in days is based on average deployment conditions.
[2] SAL (Op) Remote Query enabled via an integration between FMC 7.0+ and SNA 7.3.2+
[3] Firewalls running FPR 6.4+ or ASA 9.12+ supported

FAQs:

Q: Do I have to buy CDO to buy SAL (SaaS)?
A: No. SAL's event viewer in CDO is included as part of the SAL license/ trial.

Q: Can I retrieve log files from SAL (SaaS) in the Cloud or SAL (On prem)?
A: Yes. SAL customers can download data from the Cisco Cloud to their local machine.

Q: What log types does SAL support?
A: SAL (SaaS) supports Cisco Firewalls (FTD & ASA) managed by FMC, CDO, FDM, CSM, ASDM or ASA-CLI. Also, logs from network endpoints. SAL (On Prem) only supports FTD-NGFW logging.

Resources:

SalesConnect Ordering Guide | Data Sheets At-a-Glance | Documents Config Guides | FAQ FTD Log Estimator | 60-Day Trial Public page

Example SKU: ***SAL-CL-LT-1GB***