DATASHEET

NSFOCUS

NSFOCUS LAS

Log Audit System

OVERVIEW

NSFOCUS Log Audit System is a comprehensive log management platform built on big data architecture. By leveraging advanced big data technologies for massive-scale log collection, heterogeneous device log normalization, and security event correlation analysis, NSFOCUS LAS enables full lifecycle log management across enterprise environments.

The platform helps security operations and IT teams monitor and respond to cybersecurity events throughout all stages of incident management — including proactive risk discovery, real-time analysis and traceability, post-incident investigation and digital forensics. NSFOCUS LAS also assists organizations in supporting international cybersecurity and compliance frameworks such as SOX, PCI DSS, NIST, GDPR, ISO 27001 and many other industry security standards.

LOG COLLECTION

NSFOCUS Log Audit System provides comprehensive log collection capabilities, supporting both active and passive collection methods for a wide range of log sources, including NSFOCUS products, third-party security devices, network devices, databases, Windows/Linux hosts, web servers, application systems, and virtualization platforms. The system supports the collection, analysis, and retrieval of both IPv4 and IPv6 logs, and offers distributed external collectors to enable cross-network log acquisition in complex environments.

AUTOMATIC LOG ONBOARDING

NSFOCUS LAS features built-in intelligent parsing models that automatically match newly received log data against predefined and custom parsing rules. Based on the matching results, the system associates logs with the most relevant rule set, enabling intelligent normalization and standardized log parsing.

LOG STORAGE

NSFOCUS LAS supports the storage of both raw and normalized logs with customizable retention policies. The platform provides up to 10:1 compressed storage, data encryption, and log integrity verification to ensure data security and reliability. In addition, duplicate logs can be aggregated and consolidated to reduce storage consumption. The system also supports storage expansion, NFS network file sharing, and S3-compatible cloud storage, enabling flexible and scalable storage architectures for diverse enterprise requirements.

LOG SEARCH AND RETRIEVAL

NSFOCUS LAS delivers flexible and powerful log search capabilities, supporting full-text search, key-value queries, Boolean logic, bracket expressions, regular expressions, and fuzzy matching. The platform also enhances operational efficiency through convenient search management features, including saved searches and the ability to import previously defined search conditions.

EVENT ALERTING

NSFOCUS LAS transforms traditional “log recording” into actionable “security event extraction.” The system includes a rich library of built-in event correlation rules and supports user-defined custom event rules based on operational requirements. Specific events can trigger real-time alert notifications, enabling security teams to rapidly identify and respond to potential threats.

KEY BENEFITS

High-Speed Log Search
Delivers second-level search performance across billions of log records, supporting full-text, fuzzy, and regular expression searches. Search conditions can also be saved as reusable templates for improved operational efficiency.

Long-Term Log Retention
Provides up to 10:1 compressed storage efficiency, enabling longer retention with the same storage capacity. Supports scalable external storage options including NFS, S3, and (S)FTP for massive log storage requirements.

Comprehensive Compliance Readiness
Supports customizable log retention policies to meet regulatory requirements, including long-term log retention. Provides multi-factor authentication, log integrity verification, and 3rd party platform compatibility to help organizations address compliance, security assessment, and localization requirements.

Comprehensive Log Collection
Combines active and passive collection methods, supporting logs from mainstream network devices, security devices, databases, operating systems, middleware, and applications.

Advanced Audit Visibility
Offers flexible auditing capabilities with customizable dashboards and specialized audit views for common host and web server scenarios, enabling clear analysis of complex log data.

ASSET MANAGEMENT

NSFOCUS LAS provides both active and passive asset discovery capabilities, enabling automatic identification of assets from collected logs. Assets can be categorized based on organizational structure, business systems, geographic locations, asset groups, and other dimensions, providing a unified and comprehensive asset visibility view. The platform also supports drill-down analysis for asset-related alerts and associated events, enabling real-time asset monitoring and security tracking.

CUSTOM REPORTING

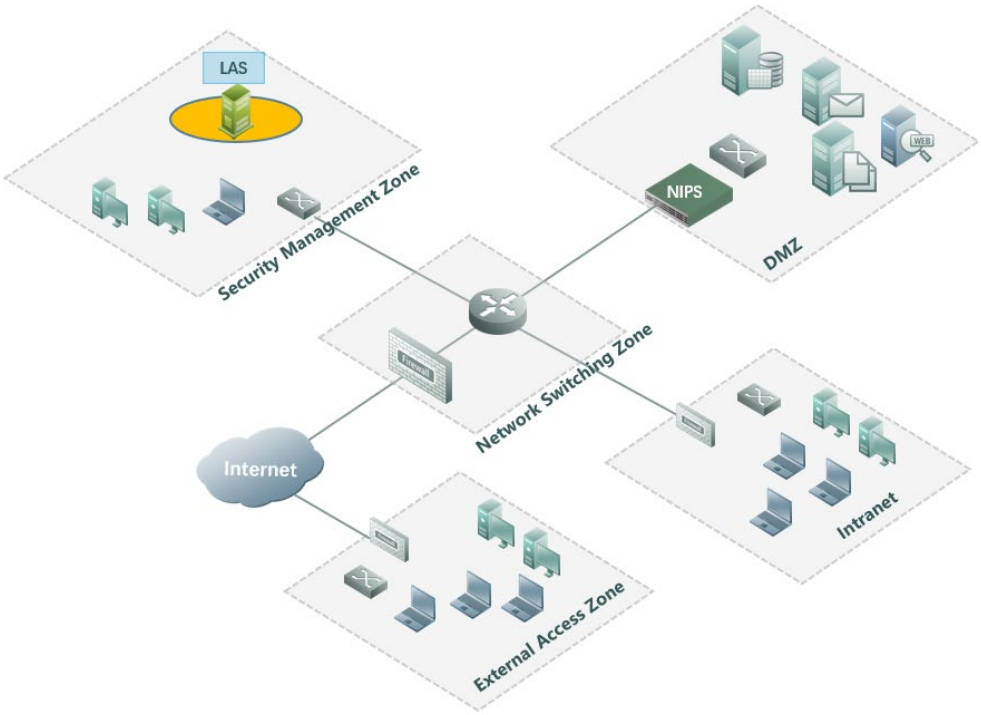
NSFOCUS LAS includes built-in compliance report templates aligned with industry standards such as SOX, PCI DSS, NIST, GDPR and ISO 27001, while also supporting highly flexible custom report generation. Users can customize report layouts, reference statistical data, define titles, and configure report content according to business requirements. The system supports real-time reports, scheduled reports, and recurring report generation tasks, with multiple export formats and customizable report branding options to meet diverse operational and compliance reporting needs.

DEPLOYMENT

NSFOCUS LAS is available in both hardware appliance and software editions, supporting multiple deployment models. Typical deployment scenarios include the following:

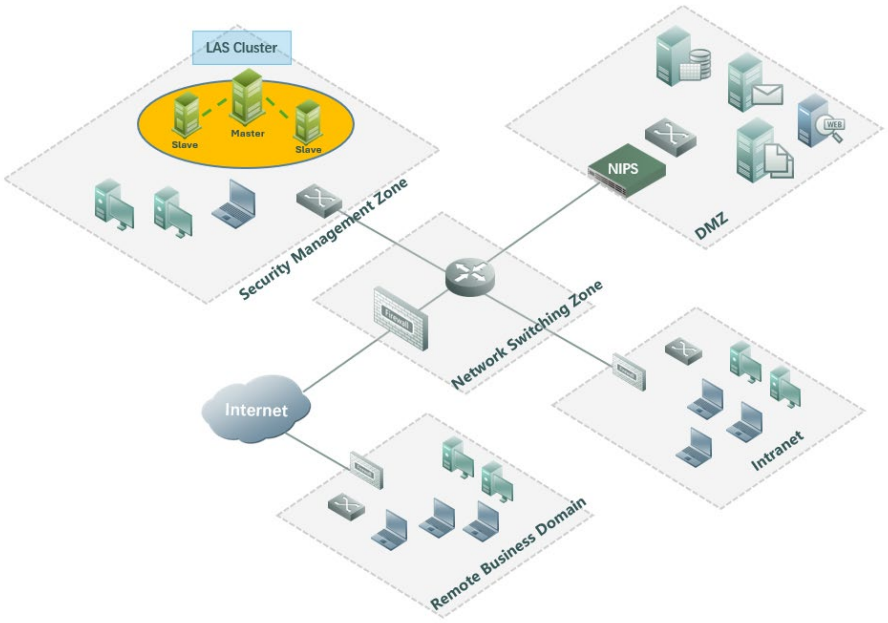
Standalone Deployment

In a standalone deployment scenario, NSFOCUS Log Audit System can be deployed out-of-band within the customer network to centrally collect logs from IT infrastructure, application systems, databases, security devices, and hosts. The platform provides comprehensive log collection, centralized storage, and correlation analysis capabilities, while generating alert notifications for identified security issues, helping organizations improve security visibility and meet compliance requirements.



Cluster Deployment

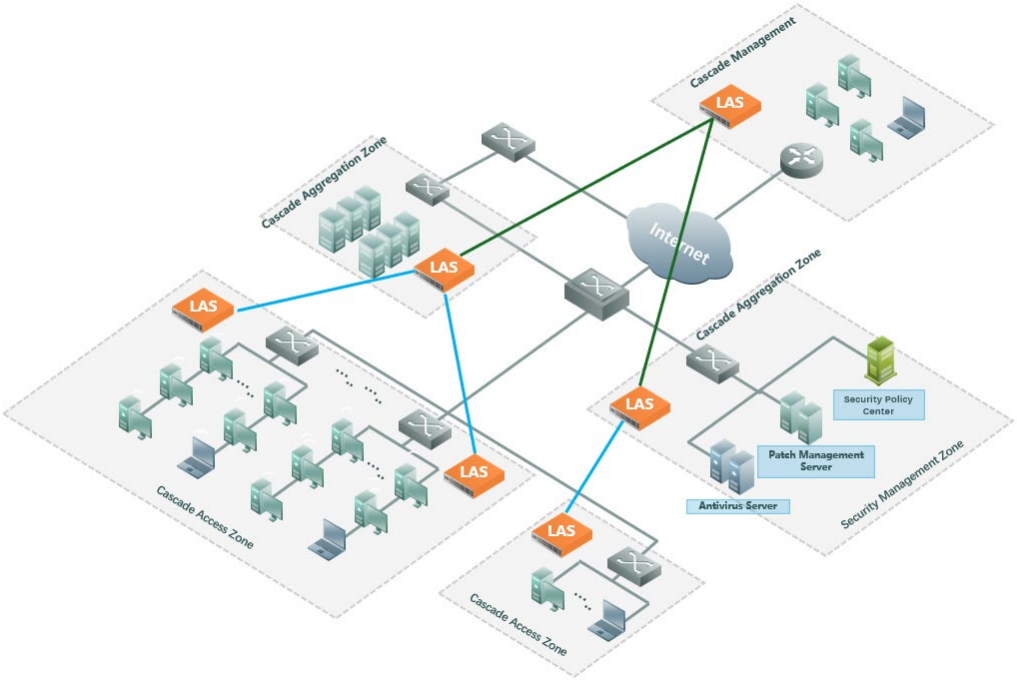
In cluster deployment scenarios, NSFOCUS Log Audit System consists of a master node and one or more slave nodes. Leveraging a distributed computing architecture, the system distributes log normalization and log ingestion workloads across multiple compute nodes, significantly enhancing overall processing performance, scalability, and storage capacity.



Cascading Deployment

Cascading deployment is designed for large enterprises and organizations with branch offices or multi-tier administrative structures. Each branch can deploy its own local management center to collect, analyze, and store logs independently. Based on centralized management policies, logs and security events can also be aggregated and forwarded to upper-level management centers for unified analysis and administration.

Through cascading deployment, NSFOCUS Log Audit System enables multiple audit centers to process enterprise-wide logs in parallel, significantly improving overall data processing efficiency while meeting the operational and regulatory requirements of hierarchical security management architectures.



Hardware Specifications

Model	LASNX3-HD4000	LASNX3-HD6000	LASNX3-HD7000
Average Log Processing Performance	7000 EPS (Events Per Second)	10000 EPS	13000 EPS
Peak Log Processing Performance	8000 EPS	13000 EPS	17000 EPS
Recommended Maximum Log Source	700	1000	1400
CPU	2 Cores 4 Threads	4 Cores 8 Threads	4 Cores 8 Threads
Memory	32G	32G	64G
Hard Disk	8T / 16T	4T*3 / 8T*3 / 16T*3, RAID5	4T*3 / 8T*3 / 16T*3, RAID5
Cluster Deployment	NO	YES	YES
Extension Slot	4	4	4
Optional Extension Interface	4GE/4SFP/2SFP+/4SFP+/4GE(Bypass)	4GE/4SFP/2SFP+/4SFP+/4GE(Bypass)	4GE/4SFP/2SFP+/4SFP+/4GE (Bypass)
Management Port	1*GE	1*GE	1*GE
Console	1*RJ45	1*RJ45	1*RJ45
USB Interface	2	2	2
Dimension (W*D*H)	435mm*560mm*88mm	435mm*560mm*88mm	435mm*560mm*88mm
Weight	20kg	20kg	20kg
Power Supply	Redundant power supply, 100-240V AC, 300W	Redundant power supply, 100-240V AC, 550W	Redundant power supply, 100-240V AC550W
MTBF	>100,000 hrs.	>100,000 hrs.	>100,000 hrs.
Operating Temperature	0 - 40℃	0 - 40℃	0 - 40℃
Operating Humidity	10% - 95% RH	10% - 95% RH	10% - 95% RH

Software Performance and Recommended Configurations

Model		LASNX3-VN100	LASNX3-VN500	LASNX3-VN1000	LASNX3-VN2000
Average Log Processing Performance		500EPS	2000EPS	5000EPS	10000EPS
Recommended Maximum Log Source Capacity		50	100	500	1000
Cluster Deployment		NO	NO	YES	YES
Resources Required	**vCPU**	8C	8C	16C	32C
	Memory	16G	32G	64G	128G
	Hard Disk*	⩾4T	⩾8T	⩾24T	⩾48T
Supported Virtualization Platform	**VM Platform Compatibility**	KVM-X86, VMware, Xen, Hyper-V			
	Public Cloud Compatibility	AWS, Azure, Alibaba Cloud, Huawei Cloud, Tencent Cloud, China Telecom Tianyi Cloud,			
	Private Cloud Compatibility	OpenStack			
	Image Formats	OVA, QCOW2, VHD, RAW			