Zscaler™ Nanolog Streaming Service

Seamlessly transmit Zscaler Web and Cloud Firewall logs to your SIEM in real time

SOLUTION FEATURES

- Transmit logs from all users and locations to the SIEM in real time
- Customizable to send specific log fields based on complex log filters
- Seamless integration with the corporate SIEM

SOLUTION BENEFITS

- Enables correlation of Web and Cloud Firewall logs with other logs stored in the SIEM
- Ensures compliance with regulatory mandates on local log archival
- Supports historical log analysis (greater than 6 months)

LEARN MORE

www.zscaler.com

Speak with a specialist:
1-866-902-7811

Zscaler's patented Nanolog Streaming Service delivers Web and Firewall logs from all users in all locations. In real time.

Zscaler Nanolog Streaming Service consolidates logs from all users, globally, into a central repository that is determined by customers, where administrators can view and mine transaction data by user, device, application and location in real time.

For organizations that need to transfer their Zscaler logs to their enterprise SIEM, Zscaler provides Nanolog Streaming Service (NSS) and NSS Live. The difference being that NSS has the ability to buffer logs to protect against loss during SIEM downtime. NSS is provided as a virtual machine installed within the customer's network. NSS connects to the cloud Nanologs and streams out all logs for the company to the corporate SIEM or other storage devices in real-time. The protocol used by NSS to retrieve logs from the cloud is highly secure and guarantees that the logs cannot be tampered with in transit.

By using NSS, Zscaler customers can ensure compliance with regulatory mandates on local log archival. Sending web log data to the SIEM also facilitates log correlation from multiple devices, thus allowing organizations to analyze traffic patterns across their entire network. Additionally, organizations can leverage log data in the SIEM to conduct extended historical analysis (> 6 months).
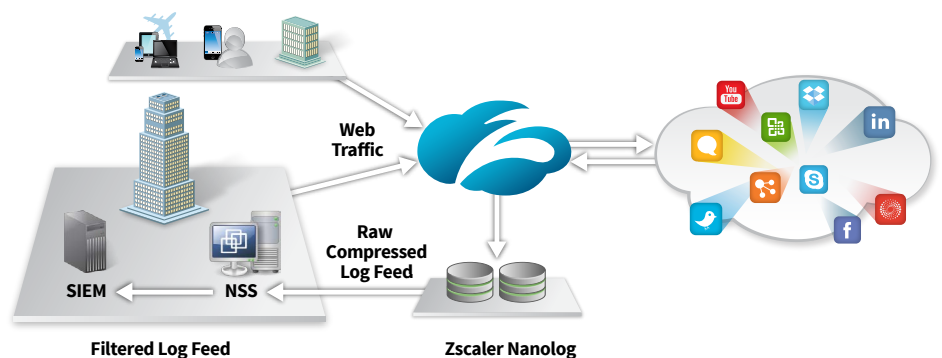
Key Features

Comprehensive, real-time log

- Includes logs from all users, across all devices and locations
- No batch reporting, logs are transmitted to the SIEM in real time
- Failover protection – 1 hour log buffer to protect against log loss during SIEM downtime
  - Failover protection is not available with NSS Live

Customizable to organization's data needs

- Configure filters to pre-process logs (on criteria such as user, data type, event type) and send only relevant logs to the SIEM
- Send up to 8 streams of logs, each with different filters and formats, to different SIEMs
- Obfuscate user name in the log records to comply with legal requirements

Seamless integration with multiple SIEMS:

- Supports any ASCII log format. Convert logs to any format that any SIEM or Syslog can accept
- Partnerships with leading SIEM solutions including QRadar, Splunk, and Microsoft

Easy Deployment

- Nanolog Streaming Server software available as a virtual appliance downloadable from the Zscaler portal
- Requires only outbound connections to the cloud—can be deployed behind NAT or Firewall

Easy Maintenance

- Optional remote assistance available for advanced troubleshooting without punching a hole in the firewall
- Auto-update of the software

Official Partners