Hillstone Security Audit Platform

HSA-10 / HSA-5 / HSA-3

ISPs, universities, large enterprises, government agencies, and large data centers generate millions of events everyday. They require high performance log storage and near instantaneous query results to analyze an explosion of data generated by today' s Next Generation Firewalls. Hillstone' s Security Audit Platform transforms log data into security intelligence with split-second searches that provide instant visibility into billions of log records. Hillstone' s Security Audit Platform collects and collates NAT, Threat, URL and Session logs and provides granular search capabilities that provide real-time visibility into network traffic.

Product Highlights

Network Visibility

Log records provide visibility into network activity and help meet compliance regulations. But running log queries across millions of log records can take hours with traditional log management systems. Nevertheless, without effective log management, companies deny themselves the intelligence provided by their own environments and expose themselves to unbridled security events. Hillstone's Security Audit Platform provides powerful, easy to use queries, which quickly provide instant visibility into millions of log records.

High Performance Log Processing

Large enterprises can generate up to 100 gigabytes of log data per day. Being able to scale to these data rates is an important aspect to log retention. Hillstone's Security Audit Platform supports standard syslog as well as a very high performance binary protocol that can receive up to 100,000 events per second from NAT traffic. It can dynamically scale storage to meet retention/compliance requirements via distributed load balancing or by sending specific logs to specific servers.

www.hillstonenet.com
Phone: 1-800-889-9860

Highlight

Powerful Queries

Hillstone's Security Audit Platform allows users to easily create and save queries that run on demand or on a scheduled basis. It can search across source IP, destination IP, URL, public IP and time. In addition, Hillstone's NAT logs can translate a public IP address into a private IP address/port and user name. This provides powerful forensic detail in environments that use NAT and need visibility into the private network.

Key Features

Device Monitoring

- Device KPI monitoring
- Ratio analysis of log storage type
- Trend analysis of device and log type
- Monitoring of sending device

Log management

- NAT, Session, URL, mail, IM on/offline and threat prevention log
- Can import and analyze Syslogs from third-party devices
- Multi-condition combination searches
- Log aggregation
- Supports log transmission via SSL
- Saving search conditions
- Background search tasks
- Distributed queries for multi-devices

Report Management

- Built-in multiple report templates
- Customizable report
- HTML and PDF format report files

System Management

- Trusted host settings
- Importing/exporting of logs
- Log forwarding
- Distributed search settings
- Role-based management: administrator, operator and auditor

Product Specification

Specification	HSA-10	HSA-5	HSA-3
Performance	NAT: 100,000 EPS Syslog: 10,000 EPS	NAT: 50,000 EPS Syslog: 5,000 EPS	NAT: 30,000 EPS Syslog: 3,000 EPS
Storage	NAT Log: 90 days for 10G link	NAT Log: 90 days for 5G link	NAT Log: 90 days for 3G link
HDD	8 TB	4 TB	2 TB
Fixed I/O Ports	2 x GE	2 x GE	2 x GE
RAID Levels	RAID 5	RAID 0	RAID 0
Power Supply	Single/Dual	Single	Single
Form Factor	2U	1U	1U