



Insight into

Security Event Management

Advantages in using eIQ Syslog Server™ for Firewall Syslog Data Collection and Management

Network Security Analyzer includes the eIQ Syslog Server that allows you to collect, normalize and manage syslog data from all leading firewalls. Once you use eIQ Syslog Server, a third party syslog server is not required and should not be used with Network Security Analyzer. This document highlights the advantages and benefits in using eIQ Syslog Server.

The eIQ Syslog Server is an integral part of the Network Security Analyzer Edition and should not be confused with SyslogAnalyzer which is an entirely different & separate eIQ Networks product for Windows/Unix server reporting.

- The eIQ Syslog Server is typically installed into the same hardware platform as the Network Security Analyzer product – however it can be optionally installed into a separate machine platform. The primary reason for a separate installation of the eIQ Syslog Server is when the overall load processing volume is very high.

- The eIQ Syslog Server saves significant disk space by automatically writing to a compressed file. This will result in significant savings on a monthly and yearly basis for a large or busy customer generating GB of logs per day. For example a customer generating 4GB of logs per day would normally require about 120GB per month of disk space to store these logs. Or 1.4TB of storage per year. This would cost this customer approximately over \$70,000 just for procuring storage. On the other hand if this customer uses eIQ Syslog server, then they only need about 12GB per month or 140GB per year to store raw logs, which could easily be purchased for less than \$5,000.

- In addition, the eIQ Syslog Server saves network bandwidth by transferring only the “delta” (change in data) in compressed format over the network. This speeds the reporting and facilitates ‘near real time’ information reporting. Transferring only delta format saves money in usage sensitive distributed WAN environments.

- The eIQ Syslog Server saves log data into normalized and standard Open Log File Format™ (OLF) log format from multiple firewalls from different vendors.

- Distributed eIQ Syslog Server helps you localize the log collection thus reducing the syslog traffic over the WAN. Changes to all distributed Syslog Servers can be applied from Network Security Analyzer main console.

- eIQ Syslog Server automatically detects and collects log data from all configured Firewalls. Users configure only the firewalls so they are enabled to permit the eIQ Syslog Server to ‘listen’ to the syslog messages. There is no additional configuration required within eIQ Syslog Server.

- User configurable delta file transfer helps meet your unique requirements based on log file size, network bandwidth, and system resources.