



*Raw
Log Search*

*Manage
Firewall
Configuration
Changes*

*Real-Time
Alerts*

*Detect
Network
Anomalies*

*Measure
Network Traffic
& Bandwidth*

*Monitor
Employee
Internet
Usage*

*Archive
Firewall Logs*

*Security
Compliance
Reports*

*Log
Collection*

Unlock the Real Value of your Network Security Devices

Why Analyze Firewall Logs?

Just deploying the Firewall in itself will not secure your network, but the log data from your firewall needs to be continuously monitored and analyzed. There is a wealth of vital information in your firewall logs. With these logs you can detect network intrusion, virus attacks, denial of service attacks, anomalous behaviors, employee web activities, web traffic analysis and much more. These logs also allow you to plan your bandwidth requirement based on the bandwidth usage across the firewalls. But manually monitoring and analyzing these logs is a time consuming task, complex, and is always prone to human error.

So how do you manage this complexity? ManageEngine Firewall Analyzer is the solution for analyzing your firewall logs automatically. Firewall Analyzer analyzes logs from firewalls and generates real time alert notifications, security and bandwidth reports. It also empowers administrators by providing comprehensive reports about the security events and in turn they can take steps to mitigate the security.

Also, Firewall Analyzer alerts you in real-time when any configuration changes are made on your firewall and tells you 'who' made 'what' changes, 'when' and 'why'.



“ The strengths of Firewall Analyzer are agent-less architecture and web based client interface. The best thing that impressed me is the ability to view all the Firewalls through a single dashboard ”

Nicholas Batchelor,
 Senior System Administrator, South Gloucestershire Council

Why Choose Firewall Analyzer?

Unlock the real value of your security devices

- Supports an extensive array of perimeter logs which includes firewalls, VPNs, IDS/IPS & Proxy logs
- Provides a wide variety of reports for external threat monitoring, change management & compliance

Productivity improvement for IT / MSSP

- From product deployment to report generation in minutes!
- Real-time alerts to security events enable IT to respond instantaneously to security threats

Meet dynamic business needs quickly

- Rapidly transforms perimeter device logs into actionable information
- Receive reports in user friendly formats in PDF & CSV formats

Attractive TCO & rapid ROI

- No additional hardware required, minimal IT overhead, ease-of-deployment and ease-of-use ensures a low TCO and rapid ROI
- Starts at \$395/year



Log Collection

- Agentless log collection
- Collects logs from network perimeter security devices such as Firewalls, Proxy servers, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), and Virtual Private Networks (VPN)



Security Compliance Reports

- Compliance Reports validates the network security by auditing and analyzing the device configuration
- Generate security reports such as successful logins, successful logoffs, failed logins and the commands executed by the users in multiple report formats, like PDF and CSV



Detect Network Anomalies

- Get detailed information on possible network attacks and security breaches in your network
- Know which viruses are active on the network, the hosts that have been affected, and more



Monitor Employee Internet Usage

- Monitor the internet overuse or misuse by the employees in your organization.
- Get notifications when an employee tries to access restricted sites, like streaming, chat sites, etc.



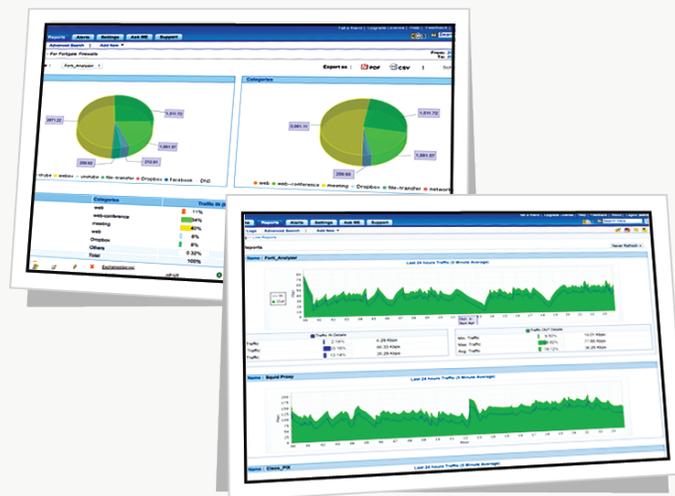
Manage Firewall Configuration Changes

- Know 'who' made 'what' changes, 'when' and 'why' to your Firewall configuration in Real-time
- Get a complete trail of all the changes done to your Firewall configuration



Raw Log Search

- Quickly & easily finds the data you're looking for using advanced raw log search & generate instant reports based on search results



- Pinpoint the exact log entry which caused the security activity in minutes



Measure Network Traffic & Bandwidth

- Find out who is using the bandwidth, how much, when, and what sites are being accessed
- Perform network behavioral analysis by monitoring for sudden spikes in bandwidth consumption, get in-depth details about users accessing web applications like Skype, Facebook, Youtube etc. and the amount of bandwidth consumed by these web applications



Real-time Alerts

- Get alert notifications for anomalous events and specific events in Real-time
- Automatic alerting allows you to receive alert notifications directly via Email, SMS or Program execution.



Archive Firewall Logs

- Automatically archives all Firewalls logs to a centralized repository
- Archived log files are encrypted to make it secure and are hashed & time-stamped to make it tamper-proof

Minimum System Requirements: Pentium Dual Core, 1GHz, 2GB RAM, 5GB disk space, Windows™ 2000,XP, Vista,7, Windows™ 2000,2003,2008 Servers or Linux

Trusted By



best of
INTEROP
Awards 2012

