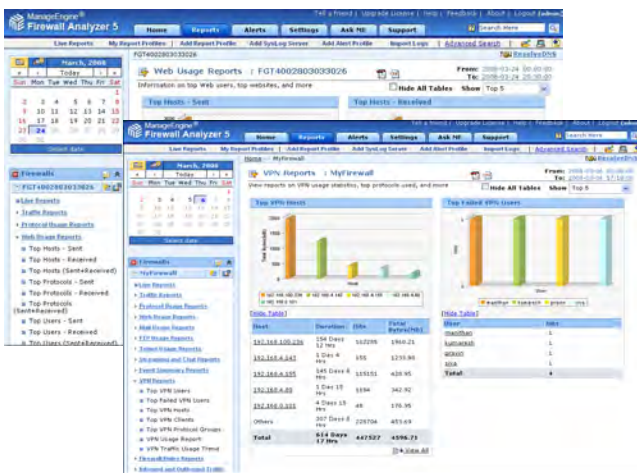


Firewall, VPN, and Proxy Server Log Analysis

Security tools like Firewalls, VPN, and Proxy Servers generate a huge quantity of traffic logs, which can be mined to generate a wealth of security information reports. ManageEngine® Firewall Analyzer is a web-based, cross-platform, log analysis tool that helps network administrators and managed security service providers (MSSP) to understand how bandwidth is being used in their network. Firewall Analyzer analyzes logs from different firewalls and generates real-time reports and graphs. Forensic analysis, capacity planning, policy enforcement, and security compromises are some of the critical decisions that are made simpler using Firewall Analyzer.

Key Features

- Enterprise-wide View of Network Activity
- Support for most Leading Firewalls
- Raw Log search
- Unused Firewall Rules Report
- On-Demand and Real-time Reports
- Advanced Data Analysis and Scheduled Reporting
- Scheduled, Customizable Log Archiving
- Historical Trending
- Real-time, Threshold-based Alerting
- Alert Administration
- Virus, Attack and Security Analysis



The Dashboard shows you all the information you need to see at one place

How can Firewall Analyzer help you?

- Analyze incoming and outgoing traffic/bandwidth patterns
- Identify top Web users, and top websites accessed
- Project trends in user activity and network activity
- Identify potential virus attacks and hack attempts
- Determine bandwidth utilization by host, protocol, an destination
- Forensic analysis using raw logs search
- Admin reports for complying regulations
- Alert on firewalls generating specific log events
- Administer the Alerts to track remediation
- Optimize efficiency of firewall rules and remove or modify them, if needed
- Determine the complete security posture of the enterprise

Web Usage Reports with multiple level drill downs show you the top hosts, top protocols, and websites that have been accessed

Features & Benefits

Multiple Device Support – support for most leading enterprise firewalls, VPN, IDS, and proxy servers.

MSSP support – user-based firewall views, anomaly detection filters for network behavioral analysis aid Managed Security Service Providers to manage multiple client networks.

Forensic Analysis – use the raw log search to find out the exact log data which indicated the security event under investigation.

Real-time Alerting – set threshold-based alerts and instant e-mail notifications when alerts are triggered.

Administer Alerting – to track the remediation by network administrators administer the alerts.

Flexible and Scheduled Log Archiving – archive all log data, or modify archiving intervals depending on disk space.

Capacity Planning – view traffic, VPN trends and determine usage patterns and peak hours for better planning of network capacity.

Instant Reports – generate over 100 pre-defined reports on bandwidth usage, protocol usage, and more. Reports can be exported to PDF format.

Powerful Multi-level Drill-down – drill down from traffic reports to see top hosts, top protocols, top websites, and to the core raw log level.

Security Analysis – analyze denied requests, top denied URLs, and more.

VPN / Squid Proxy Reports – view live VPN users, VPN statistics, VPN usage details, squid usage, top talkers, website details, and more.

Custom Reports – define reporting criteria, set graph parameters, use aggregated and raw log search and save reports.

Scheduled Reporting – set up schedules for reports to be generated and emailed automatically.

Admin Reports – pre-built reports for regulatory compliance audit

Anytime, Anywhere Access & Management – web-based user interface lets you view event details in realtime from any system on the network.

Built-in Database – comes with an integrated MySQL database that is already configured to store all log data. No external database configurations are needed.

Host OS Support – Can be installed and run on Windows and Linux systems making it suitable for deployment in a wide range of enterprises.

Firewall Compatibility

- ARKOON
- Astaro
- Avenail
- BlueCoat
- Check Point
- Cimcor
- Cisco PIX
- CyberGuard
- FreeBSD
- Fortinet
- GTA (GNAT)
- Ingate
- Identiforce
- Lucent
- Microsoft ISA
- Netopia
- NetASQ
- NetScreen
- Network-1
- Recourse Technologies
- St.Bernard
- Snort
- SonicWALL
- Squid Proxy
- SunScreen
- WatchGuard
- Zywall
- 3Com

* Visit our website for the latest compatibility list



Trend reports on traffic, protocol usage, and events help you identify usage patterns for capacity planning

For more information

Website: www.fwanalyzer.com

Email : support@fwanalyzer.com

Phone : +1 888 720 9500