ManageEngine® Firewall Analyzer

Product Brochure

Security and Device Management, Log Analysis of Firewall, VPN and Proxy Server

Firewall is an important perimeter security device that protects your network from external attacks. An optimally tuned Firewall will ensure better security of the network. Security tools like Firewalls, VPN, and Proxy Servers generate a huge quantity of logs, which can be mined to generate a wealth of security information reports.

ManageEngine® Firewall Analyzer is a web-based, cross-platform, Firewall management and security devices log analysis tool that helps security administrators to understand how secured is their network. Firewall Analyzer analyzes the rules and configurations of the Firewalls, to optimize the performance. In turn, achieve tighter control over the network security. It analyzes logs from different network periphery security devices and generates useful reports and graphs. Capacity planning, policy enforcement, and security contingency planning are some of the critical decisions that are made simpler using Firewall Analyzer.

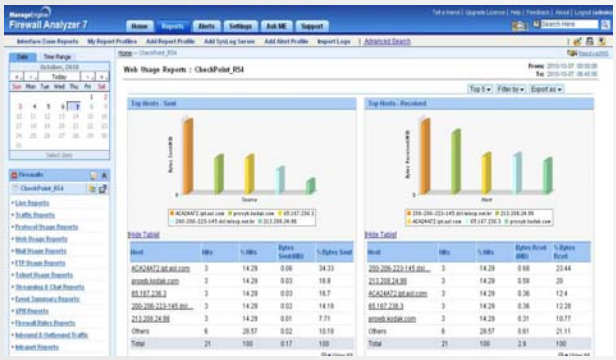
How can Firewall Analyzer help you?

- Analyze efficiency of firewall rules and modify them if needed
- Monitor Firewall configuration changes in real-time and modify to make it more secured
- Audit the security provided by the Firewall and analyze the strength of configuration
- Analyze incoming and outgoing live traffic/bandwidth patterns using log and SNMP
- Diagnose the cause of improper live Firewall connections
- Identify top Web users, and top websites accessed
- Project trends in user activity and network activity
- Identify potential virus attacks and hack attempts
- Alert on firewalls generating specific and anomalous log events
- Determine the complete security posture of the enterprise

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

Key Features

- Enterprise-wide View of Network Activity
- Firewall Change Management
- Firewall Security Audit and Configuration Analysis
- Real-time, Threshold-based Alerting
- Virus, Attack and Security Analysis
- Live Bandwidth reports with logs & SNMP
- Diagnose live rogue Firewalls connections
- On-Demand and Real-time Reports
- Advanced Data Search and Reporting
- Scheduled and Secured Log Archiving
- Support for most Leading Firewalls



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

ManageEngine® Firewall Analyzer

Product Brochure

Features and Benefits

Firewall Change Management – monitor the 'who', 'when' & 'what' of changes in the Firewall configuration

Security Audit and Configuration Analysis – get detailed security audit reports of Firewall and analysis of the effectiveness of the configurations

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

Live Bandwidth Reports – check the accurate bandwidth usage in real-time with both log and SNMP data

Diagnose Live Connections – helps to identify the live Firewall connection and diagnose the cause of the problem

Instant Reports – generate over 100 pre-defined reports on bandwidth usage, security events, and more.

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

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

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

Custom Reports – define reporting criteria, set graph parameters, and save reports.

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

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

Built-in Database – comes with an integrated MySQL database that is already configured to store all log data. Extended support for MS SQL

Flexible & Secured Log Archiving – archive all log data at flexible intervals in encrypted format and tamper-proof.

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

MSSP support – user-based firewall views and rebranding aid Managed Security Service Providers (MSSPs) to manage multiple client networks.

Distributed Edition

Monitors security devices distributed around the globe and manage them from a central location.
Massive Scalability achieved with distributed monitoring.
Suitable for SOCs, MSP/MSSPs and Large Enterprises

Firewall Compatibility

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

* Visit our website for the latest compatibility list

Trend reports on traffic, protocol usage, and events help you identify usage patterns and peak hours

For more information

Website: www.fwanalyzer.com
Email : fwanalyzer-support@manageengine.com
Phone : +1 888 720 9500

Hardware Requirements: Pentium Dual Core, 2GHz, 2GB RAM, 5GB disk space for the product, monitor that supports 1024x768 resolution
Platform Requirements: Windows™ 2000,XP,Vista,7, Windows™ 2000,2003,2008 Servers or Linux - RedHat 8.0/9.0,Mandrake/Mandriva,SuSE,Fedora,CentOS