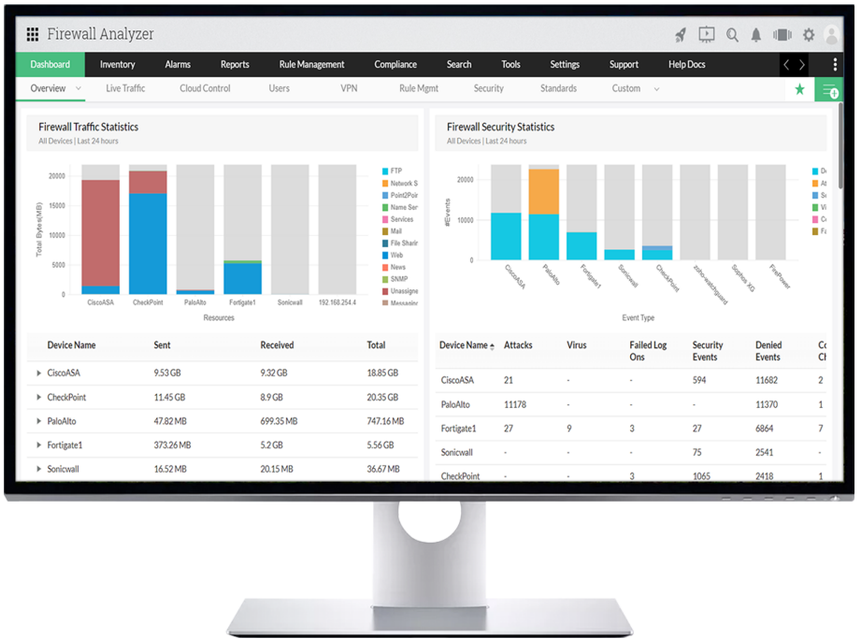
Firewall Analyzer - Manage your firewall policy and secure your network.



Firewall Analyzer is a log, policy and configuration management software. It offers CLI and API based configuration monitoring. It supports Telnet, SSH, and SCP protocol for security and traffic analysis. It also helps security admins track policy changes, optimize firewall performance and maintain compliance standards.

Firewall Analyzer at a glance

- Helps manage and optimize firewall policies
- Automates firewall rule administration
- Tracks configuration and rule changes
- Helps schedule configuration backup
- Executes regular audit compliance checks
- Performs periodic security audits
- Alerts security events in real-time
- Tracks VPN usage and generates VPN reports
- Displays the current security status of firewalls
- Tracks employee internet usage
- Monitors and alerts when bandwidth is exceeded
- Collects, consolidates, and analyzes firewall logs

Firewall Analyzer supports more than 50 vendors

Check Point	Paloalto	Cisco	Fortinet	Juniper	Sonicwall
WatchGuard	Huawei	pfSense	Cyberoam	Sophos	and more...

Firewall Analyzer technology partners

WatchGuard™

CHECK POINT™
YOU DESERVE THE BEST SECURITY

paloalto® NETWORKS

Feature Highlights

Firewall policy management

Gain visibility on firewall rules. Detect and record redundancy, generalization, correlation, shadow, and grouping anomalies in your firewall. Gain insight on how to improve performance by changing the rule order and reducing overly permissive rules. Automate firewall rule administration and also determine if a new rule can impact the existing rule set negatively.

Configuration monitoring and backup

View the complete trail of all changes applied to your firewall configurations. Find out who made what changes, when, and why. Get real-time alerts directly on your mobile. Ensure that all the configurations changes made in your firewall device are captured and backup is scheduled periodically.

Out-of-the-box reports

Firewall Analyzer generates detailed reports on traffic, protocol usage, web usage, mail usage, FTP usage, Telnet usage, streaming & chat, event summary, VPN, firewall rules, change management, intranet, internet, security, attack, spam, protocol trend, traffic trend, VPN trend, inbound & outbound traffic.

Security analysis

Identify security attacks, viruses, and other anomalies in your network. Perform forensic analysis to pinpoint threats. Know which viruses are active on your network, including the hosts that are affected. Use the advanced search capabilities to effortlessly mine for security incidents in the raw firewall logs.

Firewall compliance and auditing

Automate firewall audit reports and ensure continuous compliance. Get out-of-the-box reports on regulatory mandates such as PCI-DSS, ISO 27001, NIST, SANS, NERC-CIP, SOX, HIPAA and GDPR. Analyze the impact and severity of vulnerabilities with security audit reports.

Network bandwidth and VPN monitoring

Keep track of internal threats by analyzing and identifying the users responsible, the websites visited, and the websites which exposed the network to attacks. Monitor VPN activity and usage, identify high bandwidth consumption, track destination URLs, and block unwanted traffic.

Firewall Analyzer is available in 3 editions

Standard — Starts at $395

- Supports up to 60 Devices
- Multi-vendor security devices support
- Off-the-shelf monitoring for virtual firewalls
- Proxy servers, & VPN devices
- Network Traffic Analysis
- Network Security Reporting
- Alert Management
- Forensic Analysis

Professional — Starts at $595

- Supports up to 60 devices
- All features of Standard edition +
- Firewall rule management
- Configuration change management
- Employee internet activity reports
- Firewall security audit reports
- Web-application usage reports
- Firewall connection diagnosis
- Advanced alert management
- AD & RADIUS user authentication

Enterprise — Starts at $8395

- Supports up to 1200 devices
- All features of Professional edition +
- Monitors multi-geographical locations
- Site specific reports
- Web-client rebranding
- Client & user specific views

Minimum System Requirements

CPU: Intel Xeon Quad Core 3.5 GHz
RAM Size: 8 GB of RAM
HardDrive: 25 GB/day for 500 logs/second

Operating System

i) Windows: 11 (or) Windows Server 2025/ 2022/ 2019/ 2016

ii) Linux: Ubuntu 16 to 25/ CentOS 7/ CentOS Stream 9 and 10/ Fedora 42/ Red Hat 7 to 10/ Opensuse 15/ Debian 11 to 13/ Rocky 10/ BOSS 10

Web Browsers:

Chrome, Mozilla Firefox, and Microsoft Edge.

Database:

PostgreSQL (version 14.20), MS SQL 2022 (from build 128452), MS SQL 2019, MS SQL 2017, MS SQL 2016

Our Customers

Get Quote

Download 30-day free trial

© Copyright 2026 ZOHO Corp. All Rights Reserved.