

FortiAnalyzer™ - 1000B

High-Performance and Cost-Effective Central Logging and Analysis for Fortinet Solutions

Datasheet

Knowledge is Power

To meet the growing demand for Web-enabled applications and new IP-based services, such as multimedia messaging, voice over IP (VoIP), and video applications, enterprise networks are rapidly expanding and dramatically growing in complexity. As a result, monitoring and enforcing acceptable use policies, identifying and blocking new security threats, and complying with emerging governmental regulations requires sophisticated logging and reporting capabilities. Both real-time and historical views of network usage and security information are essential for discovering and addressing vulnerabilities across dispersed networks and user groups. The ability to capture network events usage and content information for forensic purposes, and to comply with governmental regulations regarding privacy and disclosure of security breaches, is absolutely critical. Network and security administrators need a comprehensive set of logging and reporting tools that provide the knowledge required to implement a comprehensive security solution.

Solutions for Dynamic Security Management

The FortiAnalyzer-1000B is a real-time network logging, analyzing, and reporting system that securely aggregates log data from Fortinet and third-party devices. The one Terabyte total hot-swappable hard drives support the processing and storage needs of medium enterprises. A full range of log record types may be archived and mined for compliance or historical analysis purposes. A comprehensive suite of standard graphical reports are built into the system, which also offers the flexibility to customize reports to specific needs. FortiAnalyzer solutions also provide advanced security management functions such as: quarantine archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, Web access, instant messaging and file transfer content.



FortiAnalyzer-1000B

Knowledge is the Key to Dynamic Security Management

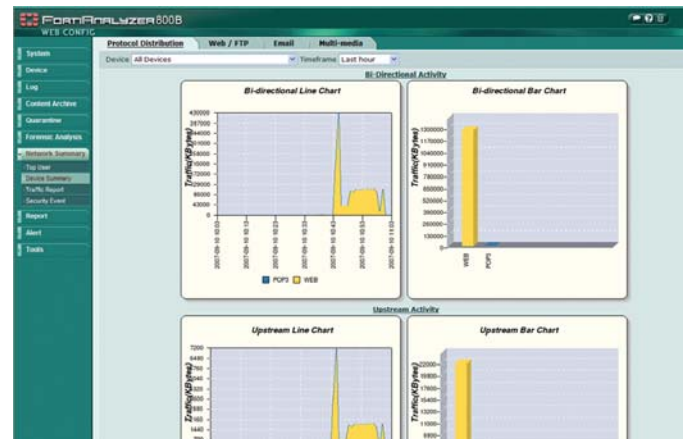
Security threats are becoming much more dynamic with attacks now using multiple vectors to penetrate, then exploit their intended targets. Businesses must immediately recognize new vulnerabilities and threats and implement protective measures before the damage is done. FortiAnalyzer systems are a critical component of the comprehensive Fortinet security solution, providing enterprise-class logging and reporting features necessary to discover, analyze and mitigate threats. The FortiAnalyzer system's forensic analysis capabilities enable detailed user activity reports, while the vulnerability assessment tool can automatically discover, inventory, and assess the security posture of servers and hosts. Complete the security management solution with a FortiManager system for comprehensive and seamless centralized management for your entire network.

Feature	Benefit
Network Event Correlation	Allows IT administrators to more quickly identify and react to network security threats across the network.
Streamlined Graphical Reports	Provides network-wide reporting of events, activities, and trends occurring on FortiGate and third party devices.
Scalable Performance and Capacity	Supports 500 network devices and 5,000 FortiClient™ agents
Centralized Logging of Multiple Record Types	Including traffic activity, system events, viruses, attacks, Web filtering events, and messaging activity/data.
Centralized Content Archiving with Centralized Quarantine	Provides reliable archiving of content data, such as email content, IM chat and file transfers, as well as a centralized quarantine repository for infected files.
Centralized Log Aggregation	Supports flexible deployment scenarios, such as deploying lower cost models in regional offices, and aggregating logs to centralized office.
Seamless Integration with the Fortinet Product Portfolio	Tight integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.

FortiAnalyzer-1000B

Security Hardened Platform	Yes
Number of Licensed Network Devices	500
Number of FortiClient Devices	5,000
10/100/1000 Ethernet	4
Number of Hard Drive Bays	2
Total Hard Drive Capacity	1 x 1.0 TB (2 TB Optional)
RAID Storage Management	Yes (0, 1)
Redundant Hot Swap Power Supplies	Yes
Dimensions	
Height	1.7 inches (4.3 cm)
Width	16.7 inches (42.6 cm)
Length	30.4 inches (77.2 cm)
Weight	36 lbs (16.3 kg)
Rack Mountable	Yes
Input Voltage	100-240VAC VAC
Input Current	10 A
Average Power Consumption (AVG)	260 W
Environment	
Operating temperature	32 to 104 deg F (0 to 40 deg C)
Storage temperature	13 to 158 deg F (-25 to 70 deg C)
Humidity	5 to 95% non-condensing
Regulatory	FCC Class A Part 15 / CE Mark
Recommended FortiGate Models	FortiGate-30 – 3810A

Centralized Logging and Reporting with FortiAnalyzer Solutions— Complete Knowledge and Control



FortiGuard Security Subscription Services

- Antivirus
- Intrusion Prevention
- Web Filtering
- Antispam
- Premier Signature Service (Includes Antivirus and Intrusion Prevention Updates with additional service level agreements)

FortiCare Support Services

- 24/7/365 FortiCare Web-based support
- Technical account management service available
- 24-Hour phone support available
- Professional services available
- 1-Year limited hardware warranty
- 90-Day limited software warranty



GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700 Fax +1-408-235-7737
www.fortinet.com/sales

EMEA SALES OFFICE-FRANCE

Fortinet Incorporated
120 Rue Albert Caquot
06560 Sophia Antipolis, France
Tel +33-4-8987-0510
Fax +33-4-8987-0501

APAC SALES OFFICE-SINGAPORE

3 Temasek Avenue
Level 21 Centennial Tower
Singapore 039190
Tel: +65-6549-7050
Fax: +65-6549-7259