FortiAnalyzer™-1000B

Centralized Logging, Analysis, and Reporting

Datasheet

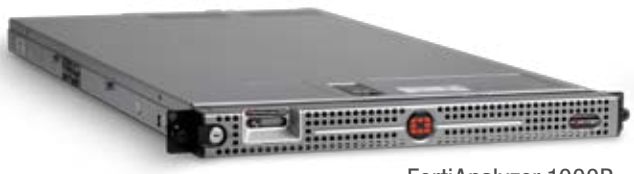
Centralized Management Solutions for Fortinet Systems

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 growing in size and complexity. As a result, monitoring and enforcing acceptable use policies, identifying and blocking emmerging 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 event, 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 complete multi-layered security solution.

Solutions for Dynamic Security Management

The FortiAnalyzer family of real-time network logging, analyzing, and reporting systems are a series of dedicated network hardware appliances that securely aggregate log data from Fortinet devices and third-party devices. A full range of log record types may be archived, filtered, and mined for compliance or historical analysis purposes. A comprehensive suite of standard graphical reports are built-in to 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 or attacks 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 tool enables detailed user activity reports, while the vulnerability assesment tool can automatically discover, inventory and assess the security posture of servers and hosts. Complete the Fortinet security management solution with a FortiManager system for comprehensive and seamless centralized management for your entire network.

Key Features and Benefits

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	FortiAnalyzer family models support thousands of FortiGate and 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	Full integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.

Technical Specifications

SYSTEM SPECIFICATIONS — FortiAnalyzer-1000B

Log Performance.....Up to 1,000 Logs / Sec
Operating System .....Hardened FortiAnalyzer OS
Platform Support.....Any FortiGate model
Any FortiMail model
FortiClient PC

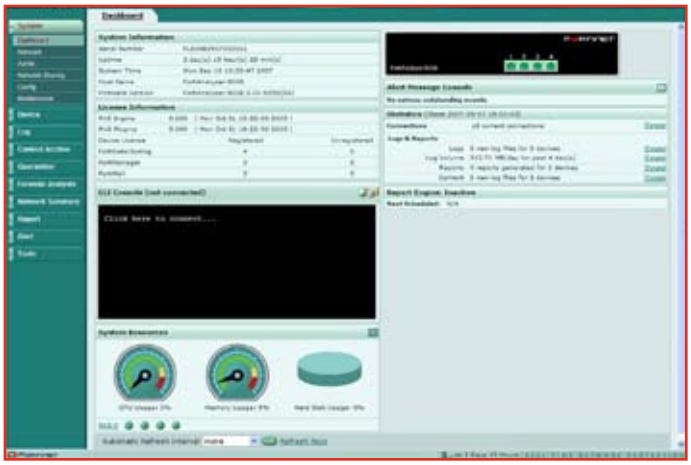
HARDWARE SPECIFICATIONS

10/100/1000 Interfaces (Copper, RJ-45).....4
Hard Drive Bays 2
Hard Drive Included..... 1 x 1.0 TB
(2 TB with optional second drive)
RAID Support .....RAID 0 or 1 (Second drive required)
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..... 100-240V AC
Input Current..... 10 A (Max)
Average Power Consumption (Avg).....260 W

ENVIRONMENTAL

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), UL/CUL, C Tick, CE, VCCI



FORTIANALYZER OS FEATURES

GENERAL SYSTEM FUNCTIONS
Profile-Based Administration
Secure Web Based User Interface Encrypted Communication & Authentication Between FortiAnalyzer Server and FortiGate Devices
Mail Server Alert Output
Connect / Sync FortiAnalyzer
SNMP Traps
Syslog Server Support
RAID Configurations
Change / View RAID Level
Support For Network Attached Storage (NAS)
Launch Management Modules
Launch Administration Console
Configure Basic System Settings
Online Help
Add/Change/Delete a FortiGate Device
View Device Groups
View Blocked Devices
View Alerts / Alert Events
Alert Message Console
View FortiManager Connection Status
View System Information / Resources
View License Information
View Statistics
View Operational History
View Session Information
Backup / Restore
Restore Factory Default System Settings
Format Log Disks
Change the Firmware
Change the Host Name

NETWORK ANALYZER
Real-Time Traffic Viewer
Historical Traffic Viewer
Customizable Traffic Analyzer Log
Search Network Traffic Logs

CENTRAL QUARANTINE
Configure Quarantine Settings
View Quarantined Files List

LOG ANALYSIS & REPORTING
View/Search/Manage Logs
Automatic Log Watch
Profile-Based Reporting
Over 300 Predefined Reports
Log Aggregation to Centralized FortiAnalyzer
FortiClient Specific Reports

FORENSIC ANALYSIS
Track User Activities by Username, Email Address, or IM Name
Supports FortiGuard Web Filtering Reports to Show Web Site Access And Blocked Web Sites Per User
Configurable Report Parameters including:
- Profiles
- Devices
- Scope
- Types
- Format
- Schedule
- Output

Customized Report Output
Reports on Demand
Report Browsing

CONTENT ARCHIVING / DATA MINING
All Functions of Log Analysis & Reporting
View by Traffic Type
View Content Including:
- HTTP (Web URLs)
- FTP (Filenames)
- Email (Text)
- Instant Messaging (Text)

View Security Event Summaries
View Traffic Summaries
View Top Traffic Producers

LOG BROWSER AND REAL-TIME LOG VIEWER
Real-Time Log Viewer
Historical Log Viewer
Customized Log Views
Log Filtering
Log Search
Log Rolling
Top Users
View Web Traffic
View Email Traffic
View FTP Traffic
View Instant Messaging and P2P Traffic
Filter Traffic Summaries
Device Summary
Traffic Reports Including:
- Event (Admin Auditing)
- Viruses Detected
- Attack (IPS Attacks)
- Web Content Filtering
- Email Filtering
- Content (Web, Email, IM)

VULNERABILITY SCANNER
Configure Vulnerability Scan Jobs
Run Vulnerability Scan Jobs
View Summary / Detailed Reports

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 Web-Based Technical Support
- Technical Account Management Service (Optional)
- 24-Hour Phone-Based Support (Optional)
- Professional Services (Optional)
- 1-Year Limited Hardware Warranty
- 90-Day Limited Software Warranty

FORTINET

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-HONG KONG
Fortinet Incorporated
61 Robinson Road
#09-04 Robinson Centre
Singapore 068893
Tel: +65-6513-3730
Fax: +65-6223-6784