FortiAnalyzer

Central Logging and Analysis for Fortinet Solutions

Datasheet

Real-Time Blended Threat Management with Reporting, Logging, Alerting and Content Archiving

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 on demand (VOD), Enterprise networks are rapidly expanding and dramatically growing in complexity. As a result, monitoring and enforcing acceptable use policies, identifying and blocking new blended 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 records including traffic, event, virus, attack, Web content, and email data may be archived, filtered and mined for compliance or historical analysis purposes. A comprehensive suite of standard reports are built-in, as well as the flexibility to customize unique reports. FortiAnalyzer also provides 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.

Key Solution Features and Benefits

Network event correlation	Allows IT administrators to more quickly identify and react to network security threats across the network.
Streamlined report creation, standardization and customization	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™ devices.
Full range of log records	Including traffic, event, virus, attack, Web content filtering, and email filtering data that helps meet regulatory requirements, such as HIPAA and other data/customer privacy regulations.
Centralized quarantining and content	Provides reliable archiving of content data, such as email content, IM chat and file transfers, as well as quarantine 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 other Fortinet products	Tight integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interface.

FortiAnalyzer-400

FortiAnalyzer-100B

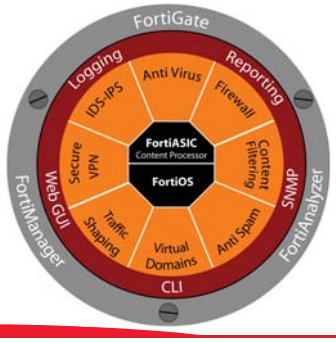
FortiAnalyzer-800

FortiAnalyzer-2000

FortiAnalyzer-4000A

Knowledge is the Key to Dynamic Security Management

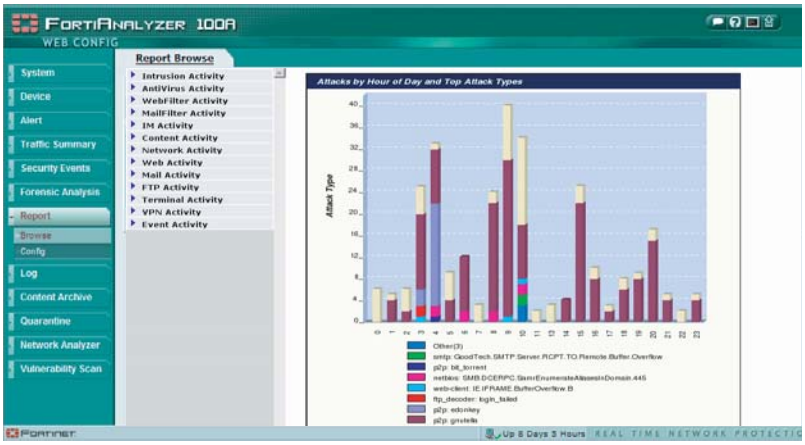
Security threats are becoming much more dynamic with attacks now being launched only days after the announcement of a vulnerability and spreading rapidly to their intended targets. Businesses must immediately recognize new vulnerabilities or attacks and implement protective measures before the damage is done. FortiAnalyzer is a critical tool providing not only granular logging and reporting but providing discovery, analysis and reports to block or mitigate threats. A Forensic Analysis tool captures information on user activities and provides detailed usage reports while a Vulnerability Analysis tool can automatically detect un-patched servers and hosts. Seamless integration with FortiManager provides a complete security management solution across your network.



Centralized Logging & Reporting with FortiAnalyzer Integration for Complete Knowledge and Control

Security Reporting—Security Management

FortiAnalyzer is a centralized solution to the logging and reporting challenges in today's complex and dynamic security environments. Implemented on scalable, high-performance platforms. FortiAnalyzer captures granular information across the entire range of security threats, not just the Firewall or IPS elements, and delivers the information in reports that are easy to configure, understand and use.

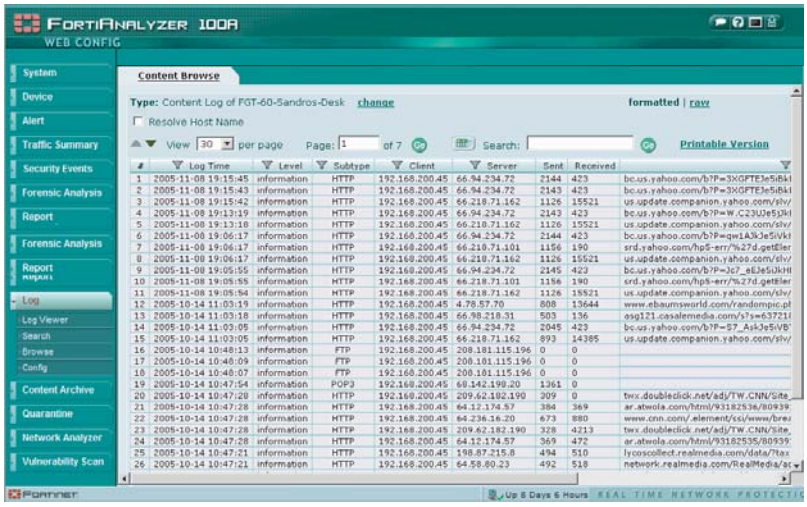


Understanding the Dynamic Security Environment

Not only are the security threats more complex in today's business environment, but new regulatory, compliance and legal mandates also require businesses to not only understand activities on their networks but to proactively implement and enforce such regulatory requirements and to be responsible for acceptable use policies. FortiAnalyzer provides hundreds for standard reports as well as the ability to fully customize reports to unique business needs. Reports can be tailored to and delivered in the exact formats needed based on user requirements. Profile-based Administration allows unique access privileges and rights to be assigned to different users based on requirements and needs.

Content Logging & Data Mining

Network-wide log aggregation and archiving is critical to identifying security threats and managing network usage. In addition to in-depth, real-time logging and reporting, FortiAnalyzer enables detailed content logging of user activities and network traffic. Activity can be monitored in real-time or logged, archived and later mined as needed. Activity be tracked by user, protocol, source, destination, etc. and the actual content exchanged in a session can be captured. Not only is content logging critical in order to implement regulatory mandates such as HIPAA and SOX compliance but absolutely required to enforce acceptable use policies and to protect valuable corporate assets and intellectual property.



FortiAnalyzer





Feature	FortiAnalyzer-100B	FortiAnalyzer-400	FortiAnalyzer-800	FortiAnalyzer-2000	FortiAnalyzer-4000A
Security Hardened Platform	Yes	Yes	Yes	Yes	Yes
Number of Licensed Network Devices *	10	200	250	500	700
Number of FortiClient Devices	100	2000	2500	5000	5000
Number of FortiMail Devices	50	100	100	200	200
10/100 Ethernet	4	3	2	0	0
10/100/1000 Ethernet	0	0	0	4	2
Number of Hard Drives	1	4	4	6	12
Total Hard Drive Capacity	250GB	1TB	1TB Std / 1.6TB Opt	1.5TB Std / 2.4TB Opt	3.0 TB Std / 4.8 TB Opt
RAID Storage Management	n/a	Yes (0, 1, 5)	Yes (0, 1, 5)	Yes (0, 1, 5, 10, 50)	Yes (0, 1, 5, 10, 50)
LCD Display	No	Yes	Yes	Yes	No
Redundant Hot Swap Power Supplies	n/a	Yes	Yes	Yes	Yes
Dimensions (H, W, L)	2 x 13.5 x 6.75 in (5 x 33.7 x 17.5 cm)	9.5 x 6.6 x 14.5 in (24.1 x 16.7 x 36.8 cm)	1.75 x 16.9 x 22.4 in (4.45 x 42.9 x 56.9 cm)	3.5 x 17.5 x 29 in (8.9 x 44.5 x 73.7 cm)	3.5 x 19 x 27 in (8.9 x 48.3 x 68.6 cm)
Weight	4.4 lbs (2 kg)	23 lbs (10.4 kg)	26.5 lbs (12 kg)	53.4 lbs (24.2 kg)	68 lbs (30.8 kg)
Rack Mountable	n/a	n/a	Yes	Yes	Yes
Input Voltage	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Input Current	0.8A	4A	4A	9A	9A
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	FG-50-100A	FG-50-800	FG-50-800	All	All

* A licensed network device may be one of the following types:
(1) FortiGate device without VDOM mode enabled
or (1) VDOM if FortiGate device is running in multiple VDOM mode

FortiAnalyzer Logging and Reporting Features

FortiAnalyzer supports the following logging, reporting and analysis features:

Log Aggregation & Archiving	Analyze logs from multiple devices, by user, or by group of users, and generate a variety of reports that enable you to proactively secure networks as threats arise, avoid network abuses, manage bandwidth, monitor Web site visits, and ensure appropriate usage policies.
Data Mining, Trend and Forensic Analysis	Archived content is data mined to report on types of traffic on your networks as well as actual content of data transferred in Web, FTP, email and IM traffic. Security event summaries identify unwanted traffic in the network and the top traffic producers, while traffic summaries identify the type of traffic on your network. Reports identify high volume users, information leakage events and acceptable use policy violations. A Forensic Analysis tools is available to analyze archived content to track user activities by user-name, email address, or IM name. Supports FortiGuard™ Web Filtering reports to show Web site access and blocked Web sites per user.
Central Quarantine	For FortiGate units that do not have a hard disk, the FortiAnalyzer offers the ability to quarantine infected or suspicious files entering your network environment. A quarantine browser allows you to view the files to determine whether they are dangerous or not.
Log Browser	Log Browser enables you to view any log file or messages from registered devices. All log files and messages are searchable and can be filtered to drill down and locate specific information.
Real-Time Log Viewer	Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic or IM message traffic.
Additional Tools: Network Analyzer	The Network Analyzer allows any available interface on the FortiAnalyzer to be used to monitor traffic on a segment of network. The FortiAnalyzer network analyzer functions as a sniffer to capture traffic data, save it to the FortiAnalyzer hard disk and display the data.
Vulnerability Scanner	Vulnerability scanner identifies vulnerabilities on a host or server, such as a mail server, FTP server or other UNIX or Windows host and generates vulnerability reports showing potential weaknesses to attacks that may exist for a selected device.

Standardized Reporting

FortiAnalyzer enables the knowledge needed to secure your network through a comprehensive suite of standard reports and the total flexibility to customize unique reports. Network knowledge can be flexibly archived, filtered and mined for compliance or historical analysis purposes.

Real-Time Log Viewer

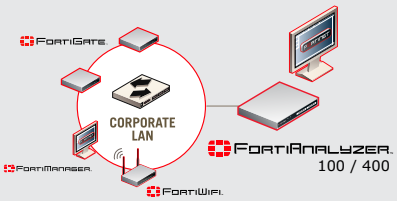
The ability to monitor network, traffic and user events in real-time or browse historical for specific events provides powerful insight into network security threats, performance and user behavior.

Granular Information

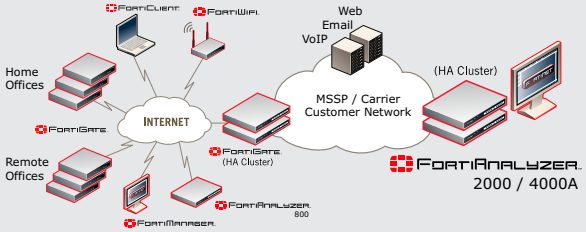
FortiAnalyzer drills deep and provides the granular level of reporting necessary to really understand what is happening on your network. Historically, or in real-time, view log and content information, analyze network traffic and utilize advanced Forensic Analysis to track user activities down to the content level.

TYPICAL APPLICATIONS

FortiAnalyzer-100B	FortiAnalyzer-400	FortiAnalyzer-800	FortiAnalyzer-2000	FortiAnalyzer-4000A
Small FortiGate Networks up to 10 devices	Mid-Sized FortiGate Networks up to 200 devices	Mid-Sized FortiGate Networks up to 250 devices	Large / Very Large FortiGate Networks up to 500 devices	



Small-Medium Enterprise Network
with Central Logging / Reporting



Enterprise / MSSP / Carrier Networks
Multiple Layered Log Aggregation and Customer Access

TECHNICAL SPECIFICATIONS: FortiAnalyzer provides the following 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
Example Reports Include:
- Attacks: By FortiGate Unit, by Hour Of The Day, by Category, and by Top Sources
- Viruses: Top Viruses Detected, Viruses Detected by Protocol
- Events: By Firewall, Overall Events Triggered, Security Events Triggered, & Events Triggered by Day of Week
- Mail Usage: Top Mail Users by Inbound and Outbound Web Usage Reports
- Web Usage: Top Web Users, Top Blocked Sites, and Top Client Attempts to Blocked Sites
- Bandwidth Usage: Top Bandwidth Users, Bandwidth by Day and by Hour, and Bandwidth Usage by Protocol Family
- Protocols: Top Protocols Used, Top FTP Users, & Top Telnet Users

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 & File Attachments 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 Reports
View Detailed Reports

Supported Devices
All Fortinet FortiGate Models
FortiClient Mobile
FortiClient PC
FortiManager
Any Syslog Compatible Device

FortiCare™ Support Services
Includes:
- 24 X 7 X 365 FortiCare Web Service *
- Email Technical Support **
- 1-Year Limited Hardware Warranty
- 90-Day Limited Software Warranty

* Annual renewal required to maintain service
** 24 X 7 Telephone Technical Support available.

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
Room 2429-2431, 24/F Sun Hung Kai Centre
No.30 Harbour Road, WanChai, Hong Kong
Tel +852-3171-3000
Fax +852-3171-3008