FORTINET

FortiAnalyzer™

Centralized Logging, Analysis and Reporting

Enhanced Visibility With FortiAnalyzer Platforms

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. They provide organizations of any size with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining and vulnerability management. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet appliances and third-party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

Security Event Information Management

You can put time back in your day by deploying a FortiAnalyzer platform into your security infrastructure, creating a single view of your security events, archived content, and vulnerability assessments. FortiAnalyzer platforms accept a full range of data from Fortinet solutions, including traffic, event, virus, attack, content filtering, and email filtering data. It eliminates the need to manually search multiple log files or manually analyze multiple consoles when performing forensic analysis or network auditing. A FortiAnalyzer platform's central data archiving, file quarantine and vulnerability assessment further reduce the amount of time you need to spend managing the range of security activity in your enterprise or organization.

Choice of Form Factor

Very few organizations use 100% hardware IT infrastructure or 100% virtual IT infrastructure today, creating a need for both hardware appliances and virtual appliances in your security strategy. FortiAnalyzer can be deployed as either hardware or a virtual appliance to fit your environment, which may include a mix of virtual and physical IT infrastructure. FortiAnalyzer will log events from FortiOS-based hardware appliances, virtual appliances, or a combination of both.

The FortiAnalyzer Difference

A FortiAnalyzer platform delivers complete security oversight with granular graphical reporting. Its breadth of data collection functions eliminate blind spots in your security posture. Its unique forensic analysis tools provide you with the ability to discover, analyze, and mitigate threats before perimeter breach or data loss. The FortiAnalyzer system's forensic analysis tool enables detailed user activity reports, while the vulnerability management tool automatically discovers, inventories and assesses the security posture of servers and hosts within the network infrastructure.

FortiAnalyzer systems come with a one-year limited hardware warranty and 90-day limited software warranty.

Features	Benefits
Network Event Correlation	Allows IT administrators to quickly identify and react to network security threats across the network.
Graphical Summary 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, and can dynamically scale storage based on retention/compliance requirements.
Centralized Logging of Multiple Record Types	Including traffic activity, system events, viruses, attacks, Web filtering events, and messaging activity/data.
Seamless Integration with the Fortinet Product Portfolio	Tight integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.
Choice of Standalone, Collector or Analyzer mode	Can be deployed as an individual unit or optimized for a specific operation (such as Store & Forward or Analytics)

FortiAnalyzer provides the following features

General System Functions

Profile-Based Administration
Secure Web Based User Interface for 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 Statistics
View Operational History
View Session Information
Backup / Restore
Restore Factory Default System Settings
Format Log Disks
Migrate data from FortiAnalyzer to another
Per-ADOM Dashboard

DLP Archive / Data Mining

All Functions of Log Analysis & Reporting
  with additional tools to detect and analyze
  data losses
View by Traffic Type
View Content Including: HTTP (Web URLs),
  FTP (Filenames), Email (Text), and Instant
  Messaging (Text)
View Security Event Summaries
View Traffic Summaries
View Top Traffic Producers

Network Analyzer

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

Log Analysis & Reporting

View/Search/Manage Logs
Automatic Log Watch
Profile-Based Reporting
Over 450 Predefined Reports plus customization
Example Reports Include:
- 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
- Wan-Opt log information

Log Aggregation to Centralized FortiAnalyzer
FortiClient Specific Reports
SQL Database Integration
SQL support for all features – including alerts,
  dashboard widgets, log viewer, FortiClient,
  and FortiMail
SQL Query / Schema tools

Central Quarantine

Configure Quarantine Settings
View Quarantined Files List
Quarantine Release API
Quarantine Summary by type of file, reason it
  was detected, first and last detected times,
  total unique quarantine files, and total number
  of detections for each type and reason

Forensic Analysis

E-Discovery
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 and Output
Customized Report Output
Reports on Demand
Report Browsing

Log Browser And
Real-Time Log Viewer

Web 2.0 Style, Real-Time Log Viewer
Historical & Custom Log Views
Log Filtering, Search, and Rolling
View Web, Email and/or 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)

Graphic Reporting

FortiAnalyzer systems empower the network
or security administrator with the knowledge
needed to secure their networks through a
comprehensive suite of standard graphical
reports and the total flexibility to customize
custom reports. Network knowledge can be
archived, filtered and mined for compliance
or historical analysis purposes.

Granular Information

The FortiAnalyzer User Interface (UI) enables
administrators to drill deep within security log
data to provide the granular level of reporting
necessary to understand what is happening
on your network. Historical or real-time
views allow administrators to analyze log
and content information, as well as network
traffic. The advanced forensic analysis tools
allow the administrator to track user activities
to the content level.

Real-Time Log Viewer

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

Supported Devices

- FortiGate Multi-Threat Security Systems
- FortiMail Messaging Security Systems
- FortiClient Endpoint Security Suite
- FortiWeb Web Application Security
- FortiManager Centralized Management
- Any Syslog-Compatible Device

FortiAnalyzer	200D	400C	1000C	2000B	4000B
Capacity and Performance					
GB/Day of Logs	5	15	25	75	150
Sessions/Day	18 M	55 M	85 M	260 M	520 M
Maximum Log Rate (Standalone Mode)	350	625	1,000	3,000	6,000
Average Retention at 5 GB Logs/Day	3 months	6 months	2 years	3 years	6 years
Devices/ADOMs/VDOMs Supported (Max)	150	200	2,000	2,000	2,000
Hardware Specification					
Security Hardened Platform	Yes	Yes	Yes	Yes	Yes
Total Interfaces	4x GbE	4x GbE	4x GbE	6x GbE	2x GbE, 2x GbE SFP
Number of Hard Drives	1	1	1 (4 Drives Max)	2 (6 Drives Max)	6 (24 Drives Max)
Removable Hard Drives	No	No	Yes	Yes	Yes
Storage Capacity	1x 1 TB	1x 2 TB	1x 2 TB (8 TB Max)	2x 2 TB (12 TB Max)	6x 1 TB (24 TB Max)
RAID Storage Management	No	No	No (Yes with Optional Drives 0, 1, 10)	Yes (0, 1, 5, 10, 50)	Yes (0, 1, 5, 6, 10, 50, 60)
Redundant Hot Swap Power Supplies	No	No	No	Yes	Yes
Dimensions					
Height x Width x Length	1.8 x 17.1 x 13.9 in (45 x 433 x 352 mm)	1.7 x 17.1 x 14.7 in (44 x 435 x 364 mm)	1.7 x 17.1 x 24.7 in (43 x 434 x 627 mm)	3.4 x 17.4 x 26.8 in (86 x 443 x 681 mm)	6.9 x 19.1 x 27.2 in (175 x 485 x 690 mm)
Weight	13.4 lbs (6.1 kg)	14.7 lbs (6.7 kg)	35.0 lbs (15.9 kg)	63 lbs (28.6 kg)	94.5 lbs (43 kg)
Form Factor	Rack mount, 1 RU	Rack mount, 1 RU	Rack mount, 1 RU	Rack mount, 2 RU	Rack mount, 3 RU
Environment					
AC Power Supply	100 – 240 VAC, 50 – 60 Hz, 6 Amp Max	100 – 240 VAC, 50 – 60 Hz, 4 Amp Max	100 – 240 VAC, 50 – 60 Hz, 7.5 Amp Max	100 – 240 VAC, 50 – 60 Hz, 9 Amp Max	100 – 240 VAC, 50 – 60 Hz, 11.5 Amps Max
Power Consumption (AVG)	60W	100W	189W	200W	420W for 6 HDD
Heat Dissipation	205 BTU/h	411 BTU/h	643.6 BTU/h	519 BTU/h	1433.7 BTU/h (6 drives) 2034.6 BTU/h (12 drives)
Operating Temperature	32–104 °F (0–40 °C)	50–90 °F (10–35 °C)	32–95 °F (0–35 °C)	50–95 °F (10–35 °C)	32–104 °F (0–40 °C)
Storage Temperature	-13–158 °F (-25–70 °C)	-40–149 °F (-40–65 °C)			-13–158 °F (-25–70 °C)
Humidity	5 to 95% non-condensing	10 to 90% non-condensing	5 to 95% non-condensing		
Compliance					
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C Tick, VCCI, CE, BSMI, UL/cUL, CB, NOM, GOST	FCC Part 15 Class A, C Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, C Tick, VCCI, CE, BSMI, UL/cUL, CB

	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
GB/Day of Logs	1 incl.	+1	+5	+25	+100
Sessions/Day	3.5 M	3.5 M	18 M	85 M	360 M
Device Quota	200 GB	+200 GB	+1 TB	+8 TB	+16 TB
Devices/ADOMs/VDOMs Supported (Max)	10,000	10,000	10,000	10,000	10,000
Hypervisors Supported	VMware ESXi / ESX 4.0 /4.1/5.0				
Virtual Machine Form Factor	Open Virtualization Format (OVF)				
vCPUs (Min / Max)	1 / Unlimited				
Memory Support (Min / Max)	1 GB / Unlimited				

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
Fortinet Incorporated
300 Beach Road 20-01, The Concourse
Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015

F:RTINET®