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.

Vulnerability Management
Fortinet offers an enhanced scanning capability that utilizes a dynamic signature dataset to detect devices on your network, catalog vulnerabilities, and recommend remediation. Additional capabilities include device discovery, mapping, asset definition and prioritization, and customized reporting. An optional Vulnerability Management subscription provides frequent updates developed by the FortiGuard Labs with up-to-date vulnerability scan data to keep abreast of current threats.

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 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.
**Seamless Integration with the Fortinet Product Portfolio** | Tight integration maximizes performance and allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.
FortiAnalyzerOS 4.1 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 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 300 Predefined Reports plus customization
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
- Wan-Opt log information
Log Aggregation to Centralized FortiAnalyzer
FortiClient Specific Reports
SQL Database Integration

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

Vulnerability and Compliance Management Scanning
Basic set of vulnerability signatures included with 4.1 OS, updates available as optional subscription
Detect vulnerabilities / recommend remediation Group/report by asset class
CVE compatibility with search by CVE names
PCI DSS scans and reports

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 for specific events provides powerful insight into network security threats, performance and user behavior.

Supported Devices
FortiGate Multi-Threat Security Systems
FortiMail Messaging Security Systems
FortiClient Endpoint Security Suite
FortiManager Centralized Management
Any Syslog-Compatible Device
FortiAnalyzer 100C | 400B | 1000C | 2000B | 4000B

### Hardware Specification

<table>
<thead>
<tr>
<th>Feature</th>
<th>100C</th>
<th>400B</th>
<th>1000C</th>
<th>2000B</th>
<th>4000B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Hardened Platform</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/10/100/1000 Ethernet</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>10/100 Ethernet</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1GbE SPF</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Number of Hard Drives</td>
<td>1x 1 TB std.</td>
<td>1x 500 GB std.</td>
<td>1x 1 TB std.</td>
<td>3x 1 TB opt.</td>
<td>2x 1 TB std.</td>
</tr>
<tr>
<td>Hard Drive Capacity</td>
<td>1 TB</td>
<td>500 GB std.</td>
<td>1 TB std.</td>
<td>4 TB max.</td>
<td>2 TB std.</td>
</tr>
<tr>
<td>RAID Storage Management</td>
<td>No</td>
<td>No (Yes 0, 1 with opt. HDD)</td>
<td>No (Yes 0, 1, 10 with opt. HDD)</td>
<td>Yes</td>
<td>Yes (0, 1, 5, 10, 50, 60; default is 50)</td>
</tr>
<tr>
<td>Number of Logs (RAID 0)</td>
<td>912,680,550</td>
<td>912,680,550</td>
<td>3,865,470,566</td>
<td>5,798,205,850</td>
<td>16,384,000,000</td>
</tr>
<tr>
<td>Redundant Hot Swap Power Supplies</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### System Performance

<table>
<thead>
<tr>
<th>Feature</th>
<th>100C</th>
<th>400B</th>
<th>1000C</th>
<th>2000B</th>
<th>4000B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Performance (Logs / Sec)</td>
<td>Up to 200</td>
<td>Up to 500</td>
<td>Up to 1,000</td>
<td>Up to 3,000</td>
<td>Up to 6,000</td>
</tr>
<tr>
<td>Data Receive Rate</td>
<td>800 Kbps</td>
<td>2 Mbps</td>
<td>4 Mbps</td>
<td>12 Mbps</td>
<td>24 Mbps</td>
</tr>
<tr>
<td>Number of Licensed Network Devices</td>
<td>100</td>
<td>200</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
</tr>
<tr>
<td>Number of FortiClient Agents</td>
<td>100</td>
<td>2,000</td>
<td>No Restriction</td>
<td>No Restriction</td>
<td>No Restriction</td>
</tr>
<tr>
<td>FortiGate Models Supported</td>
<td>All Models</td>
<td>All Models</td>
<td>All Models</td>
<td>All Models</td>
<td>All Modules</td>
</tr>
<tr>
<td>Dimensions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td>1.75 in (4.4 cm)</td>
<td>1.7 in (4.3 cm)</td>
<td>1.7 in (4.3 cm)</td>
<td>3.4 in (8.6 cm)</td>
<td>6.89 in (17.5cm)</td>
</tr>
<tr>
<td>Width</td>
<td>15 in (38 cm)</td>
<td>15.1 in (43.8 cm)</td>
<td>17.1 in (43.4 cm)</td>
<td>17.4 in (44.3 cm)</td>
<td>19.09 in (48.5 cm)</td>
</tr>
<tr>
<td>Length</td>
<td>6.3 in (16 cm)</td>
<td>14.5 in (36.8 cm)</td>
<td>24.7 in (62.7 cm)</td>
<td>28.6 in (68.1 cm)</td>
<td>27.17 in (69.0 cm)</td>
</tr>
<tr>
<td>Weight</td>
<td>4 lbs (1.8 kg)</td>
<td>10 lbs (4.5 kg)</td>
<td>35.0 lbs (15.9 kg)</td>
<td>57.5 lbs (26.1 kg)</td>
<td>94.5 lbs (43kg)</td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Environment

<table>
<thead>
<tr>
<th>Feature</th>
<th>100C</th>
<th>400B</th>
<th>1000C</th>
<th>2000B</th>
<th>4000B</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Power Required</td>
<td>100 – 240 VAC, 50 – 60 Hz, 1.5 Amp (Max)</td>
<td>100 – 240 VAC, 50 – 60 Hz, 4 Amp (Max)</td>
<td>100 – 240 VAC, 50 – 60 Hz, 7 Amp (Max)</td>
<td>100 – 240 VAC, 50 – 60 Hz, 8 Amp (Max)</td>
<td>100-240 VAC, 50 – 60 Hz, 5.5 - 11.5 Amps (Max)</td>
</tr>
<tr>
<td>Power Consumption (AVG)</td>
<td>56W</td>
<td>83W</td>
<td>189W</td>
<td>152W</td>
<td>420W for 6 HDD</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>190.4 BTU</td>
<td>283 BTU</td>
<td>643.6 BTU</td>
<td>519 BTU</td>
<td>1433.7 BTU (6 drives)</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>32 – 104 deg F (0 – 40 deg C)</td>
<td>32 – 95 deg F (0 – 35 deg C)</td>
<td>32 – 95 deg F (0 – 35 deg C)</td>
<td>32 – 104 deg F (0 – 40 deg C)</td>
<td>32 – 104 deg F (0 – 40 deg C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-13 – 158 deg F (-25 – 70 deg C)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Humidity</td>
<td>5 to 95% non-condensing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Compliance

- FCC Class A Part 15, UL/CUL, C Tick, CE, VCCI

---

1. A licensed network device is defined as:
   - One (1) FortiGate device without Virtual Domain (VDOM) mode enabled,
   - One (1) VDOM if FortiGate device is running in multiple VDOM mode
   - One (1) Third-party SYSLOG compatible device

---

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispm, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with “return and replace” hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.