



FortiAnalyzer™

Centralized logging, analysis and reporting



Comprehensive Visualization of Your Network

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. 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. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

Key Features & Benefits

Graphical Summary Reports	Provides network-wide reporting of events, activities and trends occurring on FortiGate® and third-party devices.
Network Event Correlation	Allows IT administrators to quickly identify and react to network security threats across the network.
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 email filtering.
Seamless Integration with the Fortinet Product Portfolio	Tight integration 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).
Virtual and Physical Appliance Form Factors	Available for VMware, Hyper-V and multiple hardware appliance form factors.

Fortinet's Versatile Management Solution

Networks are constantly evolving due to threats, organizational growth or new regulatory/business requirements. Traditional analysis products focus on recording and identifying company-wide threats through logging, analysis and reporting over time.

FortiAnalyzer offers enterprise class features to identify these threats, but also provides flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements while aggregating logs in a hierarchical, tiered logging topology.

Key tenets of Fortinet's management versatility:

- Diversity of form factors
- Architectural flexibility
- Highly customizable
- Simple licensing



FortiCare
Worldwide 24x7 Support
support.fortinet.com



FortiGuard
Threat Research & Response
www.fortiguard.com



Fortinet
Developer Network
Worldwide Developer Community

www.fortinet.com

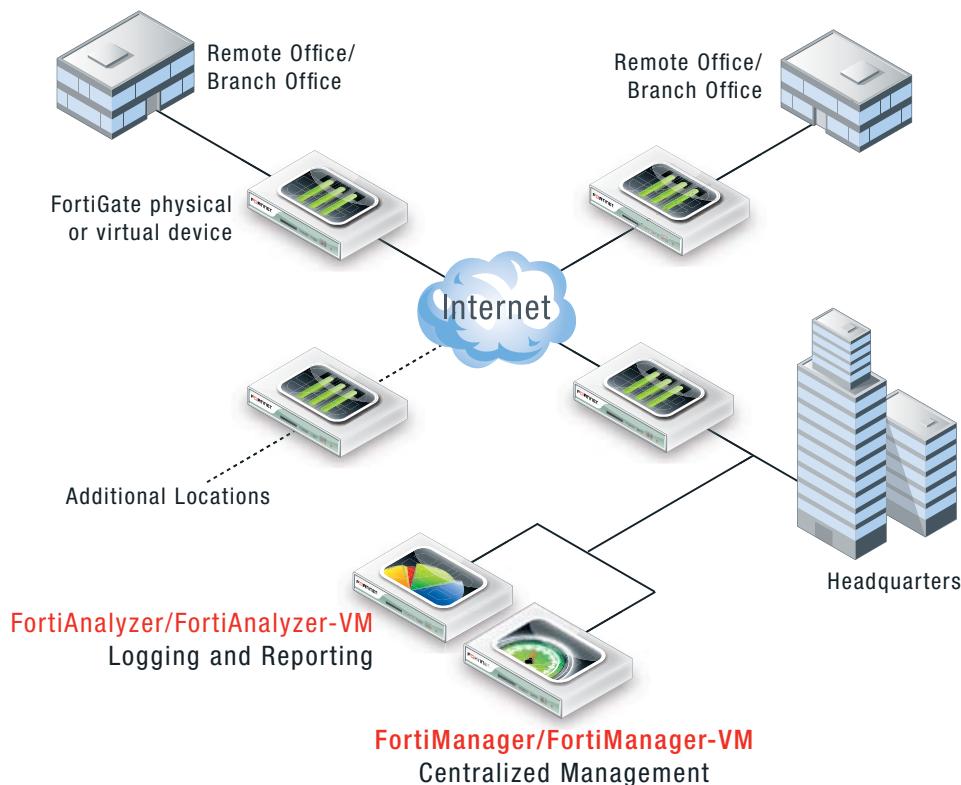
HIGHLIGHTS

Reporting and Visualization Tools

- **UTM & Traffic Summary Reports**
Regularly analyze the security profile and traffic/bandwidth patterns with a new consolidated UTM/Traffic report.
- **Built-in Report Templates**
Utilize or modify the PDF templates to display colorful, comprehensive, graphical network security and usage reports.
- **Import/Export Templates**
After building a report, export and modify the configuration on another FortiAnalyzer or different ADOM.
- **Event Management**
Raise and monitor important events to present the IT administrator with unprecedented insight into potentially anomalous behavior.
- **Drill-downs**
Generate ad-hoc graphical views of summary traffic, web, email and threat activity.

JSON and XML (Web Services) APIs

- APIs are available on all FortiAnalyzer hardware models and virtual machines
- JSON API — Allows MSSPs/large enterprises to manipulate FortiAnalyzer reports, charts/datasets and objects
- XML API — Enables IT administrators to quickly provision/configure FortiAnalyzer and generate reports
- Access tools, sample code, documentation and interact with the Fortinet developer community by subscribing to the Fortinet Developer Network (FNDN)



Log Viewer

- View logs in real-time or historical
- Select from traffic, event and UTM logs
- Browse by device, ADOM or in aggregate
- Log filtering and search capabilities
- Granular inspection with the log details pane
- Intuitive icons for countries, applications, etc.

DLP Archiving

- Investigate DLP content archives
- Supported archive types include: email, HTTP, FTP, IM
- View archive text or download files

Alerting

- Comprehensive alert builder
- Trigger off of severity levels, specific events, actions and destinations
- Set varying thresholds by number of events within a certain timeframe
- View or search through historical alerts
- Notify via email/SNMP or raise a syslog event

Better with FortiManager

- Enterprise-class device management
- Familiar GUI for full network control
- Available as integrated solution with FortiAnalyzer

FortiAnalyzer 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

SPECIFICATIONS

	FORTIANALYZER-200D	FORTIANALYZER-300D	FORTIANALYZER-1000D	FORTIANALYZER-2000B	FORTIANALYZER-3000D	FORTIANALYZER-4000B
Capacity and Performance						
GB/Day of Logs	5	15	25	75	250	Unlimited*
Sessions/Day	18 M	55 M	85 M	260 M	850 M	Unlimited*
Maximum Log Rate (Standalone Mode)	350	625	1,000	3,000	10,000	Unlimited*
Average Retention at 5 GB Logs/Day	3 months	1 year	2 years	3 years	4 years	6 years
Devices/ADOMs/VDOMs Supported (Max)	150	200	2,000	2,000	2,000	2,000
Hardware Specifications						
Form Factor	1 RU Rackmount	1 RU Rackmount	2 RU Rackmount	2 RU Rackmount	2 RU Rackmount	3 RU Rackmount
Total Interfaces	4x GbE	4x GbE	6x GbE, 2x GbE SFP	6x GbE	4x GbE, 2x GbE SFP	2x GbE, 2x GbE SFP
Number of Hard Drives	1	2	4	2 (6 Drives Max)	8	6 (24 Drives Max)
Removable Hard Drives	No	No	Yes	Yes	Yes	Yes
Storage Capacity	1x 1 TB	2x 2 TB	4x 2 TB	2x 2 TB (12 TB Max)	8x 2 TB (16 TB Max)	6x 1 TB (24 TB Max)
RAID Storage Management	No	Yes (mirrored)	Yes (0, 1, 5, 6, 10, 50, 60)	Yes (0, 1, 5, 10, 50)	Yes (0, 1, 5, 6, 10, 50, 60)	Yes (0, 1, 5, 6, 10, 50, 60)
Redundant Hot Swap Power Supplies	No	No	Yes	Yes	Yes	Yes
Dimensions						
Height x Width x Length (in)	1.8 x 17.1 x 13.9	1.7 x 17.1 x 14.3	3.5 x 17.2 x 14.5	3.4 x 17.4 x 26.8	3.4 x 20 x 29.7	6.9 x 19.1 x 27.2
Height x Width x Length (cm)	4.5 x 43.3 x 35.2	4.4 x 43.5 x 36.4	9 x 43.8 x 36.8	8.6 x 44.3 x 68.1	8.7 x 48.2 x 75.5	17.5 x 48.5 x 69.0
Weight	13.4 lbs (6.1 kg)	15.9 lbs (7.2 kg)	30.6 lbs (13.9 kg)	63 lbs (28.6 kg)	71.5 lbs (32.5 kg)	94.5 lbs (43 kg)
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, 5 Amp Max	100–240 VAC, 50–60 Hz, 9 Amp Max	100–240 VAC, 50–60 Hz, 9 Amp Max	100–240 VAC, 50–60 Hz, 11.5 Amp Max
Power Consumption (AVG)	60 W	162 W	133 W	200 W	393 W	420 W for 6 HDD
Heat Dissipation	205 BTU/h	666 BTU/h	546 BTU/h	519 BTU/h	2153 BTU/h	1433.7 BTU/h (6 drives) 2034.6 BTU/h (12 drives)
Operating Temperature	32–104°F (0–40°C)	50–95°F (10–35°C)	32–104°F (0–40°C)	50–95°F (10–35°C)	50–95°F (10–35°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-35–70°C)	-40–158°F (-40–70°C)	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)	-40–149°F (-40–65°C)	-13–158°F (-25–70°C)
Humidity	5–95% non-condensing	8–90% non-condensing	5–95% non-condensing	5–95% non-condensing	20–90% non-condensing	5–95% 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	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, 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
Capacity and Performance					
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
Hypervisor Support	VMware ESX/ESXi 4.0/4.1/5.0/5.1, Microsoft Hyper-V 2008 R2 / 2012				
Network Interface Support (Min / Max)	1 / 4				
vCPUs (Min / Max)	1 / Unlimited				
Memory Support (Min / Max)	1 GB / Unlimited				
* Only restricted to the hardware platform performance (e.g. there are no software licensing limitations)					
** Unlimited GB/Day when deployed in collector mode					



GLOBAL HEADQUARTERS

Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE

120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE

300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE

Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright © 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

產品	效能	Description	作業版本
FG-FW-Base Fortinet 網路防火牆 500Mbps	網路防火牆 500Mbps	提供防火牆控管存取政策,使用者身份辨識,IPSEC VPN, SSL VPN, SLB(主機負載平衡) 及 無線網路控制器 (Wireless Controller)	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
FG-FW-1000-UG Fortinet 網路防火牆 頻寬升級 1Gbps	網路防火牆 頻寬升級 1Gbps		
FG-VM01/VM02/VM04/VM08 Fortinet 網路防火牆 (授權方式: 依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網路防火牆 支援 1 CPU		
FG-NGFW-Base Fortinet 新世代網路防火牆 500Mbps (含 FW, IPS, Application Control, AV, Web Filtering and Antispam)	新世代網路防火牆 500Mbps	提供防火牆控管存取政策,使用者身份辨識,IPSEC VPN, SSL VPN, SLB(主機負載平衡), 無線網路控制器 (Wireless Controller), 入侵防禦, 應用程式控管, 防毒, 不當網頁過濾, 防垃圾郵件	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
FG-NGFW-1000-UG Fortinet 新世代網路防火牆 頻寬升級 1Gbps (含 FW, IPS, Application Control, AV, Web Filtering and Antispam)	新世代網路防火牆 頻寬升級 1Gbps		
FG-VM01/VM02/VM04/VM08 Fortinet 新世代網路防火牆 500Mbps (含 FW, IPS, Application Control, AV, Web Filtering and Antispam) (授權方式: 依照 CPU 數量 1/2/4/8 四個授權方式出貨)	新世代網路防火牆 支援 1 CPU		
FMG-VM-Base Fortinet 集中管理系統	集中管理系統 10 台設備	Fortinet 防火牆管理, 設定和集中派送 (政策, 資安防禦資料庫) 的中央管理系統, 支援 10 台設備	Vmware Hyper-V AWS
FMG-VM-10-UG Fortinet 集中管理系統	集中管理平台設備 數量升級 - 10 台設備		
FAZ-VM-BASE Fortinet 集中日誌報表系統	集中日誌報表系統	Fortinet 防火牆的集中日誌報表管理系統	Vmware Hyper-V AWS
FAZ-VM-GB1 Fortinet 集中日誌報表系統 紀錄數量升級 - 1 GB/Day	集中日誌報表系統 紀錄數量升級 - 1 GB/Day		
FSA-VM Fortinet 先進威脅防護系統 (ATP)	先進威脅防護系統 (ATP)	即時執行沙箱檢測, 提供虛擬的運行環境來分析高風險或可疑的程式, 研判威脅完整的生命週期, 協助用戶智慧地立即偵測出既存與新興的 網路威脅。	VMware

FWB-Base Fortinet 網站應用程式防火牆(WAF) 25Mbps	網站應用程式防火牆(WAF) 25Mbps	提供網站應用程式防火牆功能（WAF），網頁防置換，網頁自動備份及回復等功能	Vmware Hyper-V Citrix Xen Open Xen AWS
FWB-100-UG Fortinet 網站應用程式防火牆(WAF) 頻寬升級 100Mbps	網站應用程式防火牆(WAF) 頻寬升級 100Mbps		
FWB-VM01/VM02/VM04/VM08 Fortinet 網站應用程式防火牆(WAF) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網站應用程式防火牆(WAF) 支援 1 CPU		
FAD-Base Fortinet 主機負載平衡系統 (SLB) 1Gbps	主機負載平衡系統(SLB) 1Gbps	支援網路的主機負載平衡，全球服務負載平衡（GSLB）及線路負載平衡（LLB）等功能	VMware
FAD-1000-UG Fortinet 主機負載平衡系統 (SLB) 頻寬升級 1Gbps	主機負載平衡系統(SLB) 頻寬升級 1Gbps		
FAD-VM01/VM02/VM04/VM08 Fortinet 主機負載平衡系統(SLB) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	主機負載平衡系統(SLB) 支援 1 CPU		
FML-Base Fortinet 反垃圾郵件及郵件保全系統 100 人版	反垃圾郵件及郵件保全系統 100 人版	提供電子郵件主機功能、過濾並攔截垃圾郵件	VMware Hyper-V Citrix Xen KVM
FML-300-UG Fortinet 反垃圾郵件及郵件保全系統 使用者數量升級 300 人	反垃圾郵件及郵件保全系統 使用者數量升級 300 人		
FML-VM01/VM02/VM04/VM08 Fortinet 反垃圾郵件及郵件保全系統 (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	反垃圾郵件及郵件保全系統 支援 1 CPU		
FAC-VM-Base Fortinet 身份認證系統 (Authenticator) 100 人版	身份認證系統(Authenticator) 100 人版	整合 RADIUS、LDAP 伺服器，提供標準及安全的雙因子認證	VMWare Hyper-V
FAC-VM-100-UG Fortinet 身份認證系統 (Authenticator) 使用者數量升級 100 人	身份認證系統(Authenticator) 使用者數量升級 100 人		