FortiAnalyzer Virtual Appliances

Centralized Logging, Analysis, and Reporting On A Virtual Platform

DATASHEET

Enhanced Visibility With FortiAnalyzer-VM

FortiAnalyzer-VM integrates network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout a network. Utilizing virtualization technology, FortiAnalyzer-VM is a software-based version of the FortiAnalyzer hardware appliance and is designed to run on VMware™ virtualization platforms. It offers all the features of the FortiAnalyzer hardware appliance.

FortiAnalyzer-VM provides organizations of any size with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining and vulnerability assessment. 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 virtual appliance family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns that can be used to fine tune the security policy, thwarting future attackers. In addition, FortiAnalyzer-VM provides detailed data capture that can be used for forensic purposes to comply with regulations and policies regarding privacy and disclosure of information security breaches.

Proven Success in Virtual Environments

Fortinet introduced Virtual Domain (VDOM) technology in 2004. Since that time, we have offered virtualized security to service providers and enterprises alike. With the addition of the virtual appliance form factor, Fortinet now provides greater choice and flexibility by providing the ability to deploy Fortinet security solutions within an existing virtualization infrastructure.

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. Fortinet allows you to build the security solution that's right for your environment, which often includes a mix of virtual and physical IT infrastructure. We also allow you to manage your Fortinet security from a single pane of glass management platform, allowing you to control and manage hardware appliances, virtual appliances, or a combination of both.

Security Event Information Management

You can put time back in your day by deploying a FortiAnalyzer-VM into your security infrastructure, creating a single view of your security events, archived content, and vulnerability assessments. FortiAnalyzer-VM accepts 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. FortiAnalyzer-VM central data archiving, file quarantine and vulnerability assessment functionality further reduces the amount of time you need to spend managing the range of security activity in your enterprise or organization.

Vulnerability Management

FortiAnalyzer-VM offers an enhanced scanning capability that utilizes a dynamic signature dataset to detect vulnerabilities and recommend remediation. Additional capabilities include device discovery, mapping, assets definition, asset 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.

Virtualized infrastructure continues to transform today's IT landscape. From Virtual LANs to servers and user desktops, the IT environment as a whole is increasingly becoming part of a virtualized cloud. The virtual appliance offers all of the features of our traditional hardware-based FortiAnalyzer appliances in a form factor that leverages your existing investment in virtualization technology.

The FortiAnalyzer Difference

FortiAnalyzer-VM delivers complete security oversight with granular graphical reporting. Its breadth of data collection functions eliminate blind spots in understanding 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/ theft occurs. The FortiAnalyzer-VM's forensic analysis tool enables detailed user activity reports, while the vulnerability assessment tool automatically discovers, inventories and assesses the security posture of servers and hosts within the network infrastructure.

FortiAnalyzer-VM systems come with a 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.
Compute resources on demand	Allows IT administrators to add vCPU and vRAM as needed, increasing performance without replacing hardware.

FortiAnalyzer-VM provides the following features

Hypervisors Supported

VMware ESX/ESXi 5.0/4.1/4.0/3.5

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
Support For Network Attached Storage (NAS) via Hypervisor
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:

- 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
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 and Compliance Management Scanning

Basic set of vulnerability signatures included with 4.3 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 data 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
- FortiWeb Web Application Security
- FortiManager Centralized Management
- Any Syslog-Compatible Device

	FortiAnalyzer VM-100	FortiAnalyzer VM-400	FortiAnalyzer VM-1000	FortiAnalyzer VM-2000	FortiAnalyzer VM-4000	FortiAnalyzer VM-Unlimited
Hardware Platform Requirements						
Internal Storage*	1 TB	2 TB	8 TB	12 TB	16 TB	16 TB
External SQL Database	1 TB	2 TB	8 TB	12 TB	24 TB	Unlimited
Number of Licensed Network Devices	100	200	2,000	2,000	2,000	Unlimited Software limit of 10,000
Number of ADOMs Supported	1	10	50	100	250	250
vCPU Support (Min / Max)	1 / Unlimited					
Memory Support (Min / Max)	1 GB / Unlimited					
System Performance						
Standalone Mode Performance (Logs / Sec)	Up to 200	Up to 625	Up to 1,000	Up to 3,000	Up to 6,000	Up to 10,000
Data Receive Rate	800 Kbps	2.5 Mbps	4 Mbps	12 Mbps	24 Mbps	30 Mbps

*Internal storage limit includes internal database, raw logs and archives.

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: +65-6513-3730
Fax: +65-6223-6784

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using a Dell PowerEdge R715 server (AMD Opteron Processor 6128 CPU 2Ghz) running VMware ESXi 4.1 with 3GB of RAM assigned to the FortiAnalyzer virtual appliance.

FAZVM-DAT-R4-201207