

FortiGate® Virtual Appliances

Multi-Threat Security for Virtual Environments

FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. Moreover, FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

Proven Success in Virtual Environments

Fortinet introduced Virtual Domain (VDM) 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 to customer by providing the ability to deploy our security solution 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.

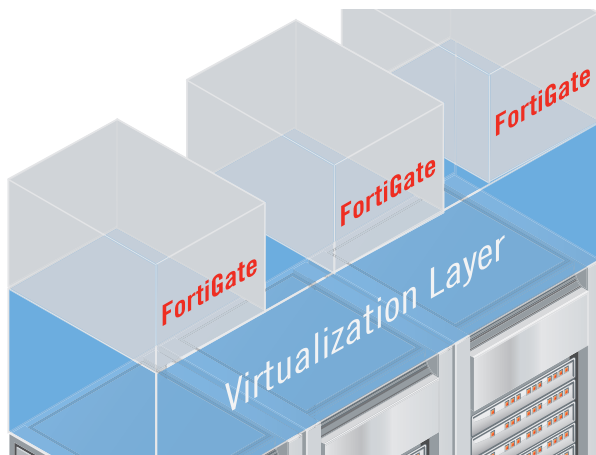
Multi-Threat Security

Using the advanced FortiOS operating system, FortiGate appliances effectively neutralize a wide range of security threats facing your virtualized environment. Whether deployed at the edge as a front-line defense, or deep within the virtual infrastructure for inter-zone security, FortiGate appliances protect your infrastructure with some of the most effective security available today.

FortiGate Virtual Appliance Benefits

FortiGate virtual appliances offer protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating system. In addition, the appliances offer these benefits:

- Increased visibility within virtualized infrastructure
- Rapid deployment capability
- Ability to manage virtual appliances and physical appliances from a single pane of glass management platform
- Simple licensing with no per-user fees



FortiGate Virtual Appliances deployed inside the virtual infrastructure

FortiGate Certifications



The Fortinet Virtual Appliance Family

Fortinet virtual appliances include the following models

FortiGate-VM multi-threat security

- Consolidated security in a virtual form factor
- Two, Four, and Eight virtual CPU (vCPU) licenses available

FortiManager-VM centralized management

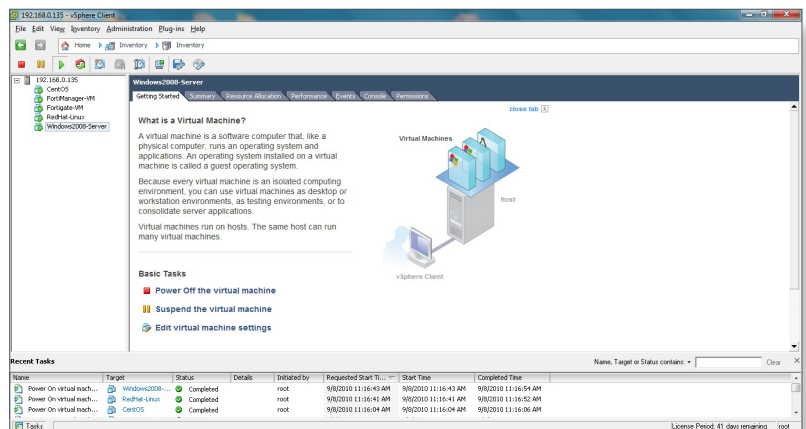
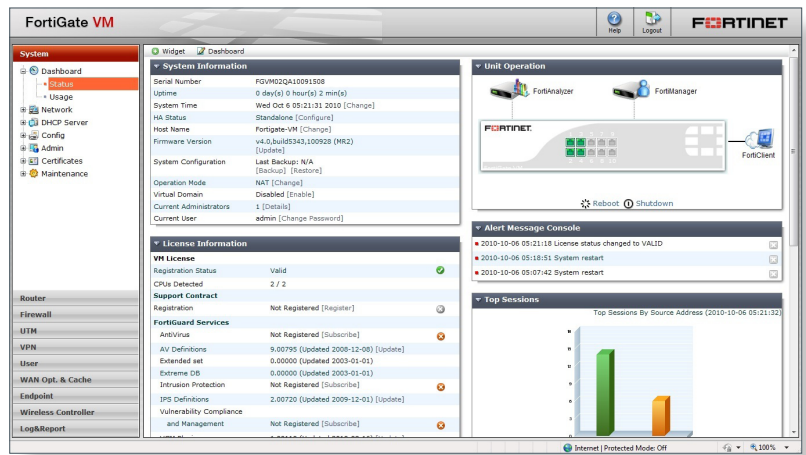
- Command and control for Fortinet infrastructure
- Up to 5,000 Fortinet devices
- Up to 120,000 FortiClient endpoint security agents

FortiAnalyzer-VM centralized analysis and reporting

- Aggregate log data for forensic analysis
- Perform vulnerability assessments of networked hosts
- Generate graphical reports to aid in demonstrating compliance

FortiMail-VM messaging security

- Block spam and malware from users' inboxes
- Archive mail for compliance and e-discovery purposes



FortiGuard and FortiCare Services

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, antispam, application control, vulnerability and compliance management, and database security services.

For more information about FortiGuard Services, please visit www.fortiguards.com.

FortiGuard Subscription Services						
Product	Antivirus	Intrusion Prevention	Web Filtering	Antispam	Application Control	Vulnerability & Compliance
FortiGate Virtual Appliance	Supported	Supported	Supported	Supported	Supported	Supported

FortiCare™ Support Services offerings provide global support for all Fortinet products and services. Customer satisfaction and responsiveness is Fortinet's number one priority. With FortiCare support, customers can be assured that their Fortinet security products are performing optimally and protecting their corporate assets with the best security technology at the best possible price.

Fortinet offers end-users multiple options for FortiCare contracts so that they can obtain the right level of support for their organization's needs. Attractively priced options include 24x7 support with advanced hardware replacement, 8x5 support with enhanced Web features, Premium Support with technical account management, and Premium RMA support with enhanced service levels.

Additionally, Fortinet Professional Services can be engaged for projects with critical deadlines projects that are large in scope, or initial deployments.

FortiOS 4.0 Software—Raising The Bar

FortiOS 4.0: Redefining Network Security

FortiOS 4.0 is the software foundation of FortiGate multi-threat security platforms. Developed solely for security, performance, and reliability, it is a purpose-built operating system that leverages the power of FortiASIC processors. FortiOS software enables a comprehensive suite of security services: Firewall, VPN, intrusion prevention, antivirus/antispyware, antispam, web filtering, application control, data loss prevention, SSL inspection, and end point network access control.

FIREWALL

- ICSA Labs Certified (Enterprise Firewall)
- NAT, PAT, Transparent (Bridge)
- Routing Mode (RIP, OSPF, BGP, Multicast)
- Policy-Based NAT
- Virtual Domains (NAT/Transparent mode)
- VLAN Tagging (802.1Q)
- Group-Based Authentication & Scheduling
- SIP/H.323 /SCCP NAT Traversal
- WINS Support
- Granular Per-Policy Protection Profiles
- Explicit Proxy Support

VIRTUAL PRIVATE NETWORK (VPN)

- ICSA Labs Certified (IPSec)
- PPTP, IPSec, and SSL
- Dedicated Tunnels
- DES, 3DES, and AES Encryption Support
- SHA-1/MD5 Authentication
- PPTP, L2TP, VPN Client Pass Through
- Hub and Spoke VPN Support
- IKE Certificate Authentication (v1 & v2)
- IPSec NAT Traversal
- Automatic IPSec Configuration
- Dead Peer Detection
- RSA SecurID Support
- SSL Single Sign-On Bookmarks
- SSL Two-Factor Authentication
- LDAP Group Authentication (SSL)

NETWORKING/ROUTING

- Multiple WAN Link Support
- PPPoE Support
- DHCP Client/Server
- Policy-Based Routing
- Dynamic Routing for IPv4 and IPv6 (RIP, OSPF, BGP, & Multicast for IPv4)
- Multi-Zone Support
- Route Between Zones
- Route Between Virtual LANs (VDMs)
- Multi-Link Aggregation (802.3ad)
- IPv6 Support (Firewall, DNS, Transparent Mode, SIP, Dynamic Routing, Administrative Access, Management)

USER AUTHENTICATION OPTIONS

- Local Database
- Windows Active Directory (AD) Integration
- External RADIUS/LDAP Integration
- Xauth over RADIUS for IPSEC VPN
- RSA SecurID Support
- LDAP Group Support

DATA CENTER OPTIMIZATION

- Web Server Caching
- TCP Multiplexing
- HTTPS Offloading

The Virtual Appliance Advantage

Virtual appliances complement traditional Fortinet hardware appliances. They provide deeper integration with your virtualized environment while offering all of the security, networking, and management services the hardware appliances are known for. They offer you greater choice in infrastructure design, with the ability to include hardware, virtual appliances, or a combination of both—all managed from a single pane of glass management platform.

ANTIVIRUS

- ICSA Labs Certified (Gateway Antivirus)
- Includes Antispyware and Worm Prevention
- HTTP/HTTPS SMTP/SMTPS
- POP3/POP3S IMAP/IMAPS
- FTP IM Protocols
- Automatic "Push" Content Updates from FortiGuard
- File Quarantine Support
- IPv6 Support

WEB FILTERING

- 76 Unique Categories
- FortiGuard Web Filtering Service Categorizes over 2 Billion Web pages
- HTTP/HTTPS Filtering
- URL/Keyword/Phrase Block
- URL Exempt List
- Content Profiles
- Blocks Java Applet, Cookies, Active X
- MIME Content Header Filtering
- IPv6 Support

APPLICATION CONTROL

- Identify and Control Over 1000 Applications
- Control Popular IM/P2P Apps Regardless of Port/Protocol:
- AOL-IM Yahoo MSN KaZaa
- ICQ Gnutella BitTorrent MySpace
- WinNY Skype eDonkey Facebook

HIGH AVAILABILITY (HA)

- Active-Active, Active-Passive
- Stateful Failover (FW and VPN)
- Device Failure Detection and Notification
- Link Status Monitor
- Link failover
- Server Load Balancing

WAN OPTIMIZATION

- Bi-Directional / Gateway to Client/Gateway
- Integrated Caching and Protocol Optimization
- Accelerates CIFS/FTP/MAPI/HTTP/HTTPS/ Generic TCP

VIRTUAL DOMAINS (VDMs)

- Separate Firewall/ Routing Domains
- Separate Administrative Domains
- Separate VLAN Interfaces
- 10 VDOM License Standard, Upgradable to More

TRAFFIC SHAPING

- Policy-based Traffic Shaping
- Differentiated Services (DiffServ) Support
- Guarantee/Max/Priority Bandwidth
- Shaping via Accounting, Traffic Quotas, and Per-IP

INTRUSION PREVENTION SYSTEM (IPS)

- ICSA Labs Certified (NIPS)
- Protection From Over 3000 Threats
- Protocol Anomaly Support
- Custom Signature Support
- Automatic Attack Database Update
- IPv6 Support

DATA LOSS PREVENTION (DLP)

- Identification and Control Over Sensitive Data in Motion
- Built-in Pattern Database
- RegEx-based Matching Engine for Customized Patterns
- Configurable Actions (block/log)
- Supports IM, HTTP/HTTPS, and More
- Many Popular File Types Supported
- International Character Sets Supported

ANTISPAM

- Support for SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
- Real-Time Blacklist/Open Relay Database Server
- MIME Header Check
- Keyword/Phrase Filtering
- IP Address Blacklist/Exempt List
- Automatic Real-Time Updates From FortiGuard Network

ENDPOINT COMPLIANCE AND CONTROL

- Monitor & Control Hosts Running FortiClient
- Endpoint Security

MANAGEMENT/ADMINISTRATION

- Console Interface (RS-232)
- WebUI (HTTP/HTTPS)
- Telnet / Secure Command Shell (SSH)
- Command Line Interface
- Role-Based Administration
- Multi-language Support: English, Japanese, Korean, Spanish, Chinese (Simplified & Traditional), French
- Multiple Administrators and User Levels
- Upgrades and Changes via TFTP and WebUI
- System Software Rollback
- Configurable Password Policy
- Optional FortiManager Central Management

LOGGING/MONITORING

- Local Event Logging
- Log to Remote Syslog/WELF server
- Graphical Real-Time and Historical Monitoring
- SNMP
- Email Notification of Viruses And Attacks
- VPN Tunnel Monitor
- Optional FortiAnalyzer Logging / Reporting
- Optional FortiGuard Analysis and Management Service

Firewall

Fortinet firewall technology delivers industry-leading performance for network and application firewalling, including Web 2.0 application policies based on the application identity. Our technology identifies traffic patterns and links them to the use of specific applications, such as instant messaging and peer-to-peer applications, permitting application access control. By coupling application intelligence with firewall technology, the FortiGate platform is able to deliver real-time security with integrated application content level inspection, thereby simplifying security deployments.

Firewall	
Features	NAT, PAT and Transparent (Bridge) Policy-Based NAT SIP/H.323/SCCP NAT Traversal VLAN Tagging (802.1Q) IPv6 Support
Performance	
2 vCPU	1.6 Gbps
4 vCPU	1.6 Gbps
8 vCPU	TBD

Antivirus / Antispyware

Antivirus content inspection technology provides protection against virus, spyware, worms, phishing, and other forms of malware being transmitted over the network infrastructure. By intercepting application content in transit, and reassembling the data into user expected content, the FortiGate Antivirus service ensures that malicious threats hidden within legitimate application content is identified and removed from the data stream destined for internal (or external) recipients. FortiGuard subscription services ensure that each FortiGate has access to updated malware signatures, resulting in high levels of accuracy and detection capabilities, including emerging and newly discovered viruses.

Antivirus	
Features	Automatic Database Updates Proxy Antivirus Flow-based Antivirus File Quarantine IPv6 Support
Performance	
2 vCPU	325 Mbps
4 vCPU	645 Mbps
8 vCPU	TBD

Intrusion Prevention

IPS technology provides protection against current and emerging network level threats. In addition to signature-based detection, we perform anomaly-based detection whereby our system alerts users to traffic that fits a profile-matching attack behavior. This behavior is then analyzed by our threat research team to identify threats as they emerge and generate new signatures that will be incorporated into our FortiGuard services.

Intrusion Prevention System	
Features	Automatic Database Updates Protocol Anomaly Support IPS and DoS Prevention Sensor Custom Signature Support IPv6 Support
Performance	
2 vCPU	TBD
4 vCPU	TBD
8 vCPU	TBD

VPN

Fortinet VPN technology provides secure communications between multiple networks and hosts, using SSL and IPSec VPN technologies. Both services leverage our custom FortiASIC processors to provide acceleration in the encryption and decryption steps. Benefits of the FortiGate VPN service include the ability to enforce complete content inspection and multi-threat security as part of the VPN service, including antivirus, intrusion prevention, and Web filtering. The FortiGate virtual appliance also supports traffic optimization, providing prioritization for critical communications traversing VPN tunnels.

VPN	
Features	IPSec and SSL VPN DES, 3DES, AES and SHA-1/MD5 Authentication PPTP, L2TP, VPN Client Pass Through SSL Single Sign-On Bookmarks Two-Factor Authentication
Performance	
IPSec VPN	TBD
Recommended Max # of SSL Users	
2 vCPU	15,000
4 vCPU	20,000
8 vCPU	30,000

WAN Optimization

With WAN Optimization, you can accelerate applications over your wide area links while ensuring multi-threat security. FortiOS 4.0 software not only eliminates unnecessary and malicious traffic as one of its core capabilities, it also optimizes legitimate traffic and reduces the amount of bandwidth required to transmit data between applications and servers across the WAN. This results in improved performance of applications and network services, as well as helping to avoid additional higher-bandwidth provisioning requirements.

WAN Optimization

Features	Gateway-to-Gateway Optimization Bi-directional Gateway-to-client Optimization Web Caching Secure Tunnel Transparent Mode
----------	--

Endpoint NAC

Endpoint NAC enforces the use of the FortiClient Endpoint Security application (either Standard or Premium editions) on your network. The feature verifies the installation of the version of the FortiClient application, ensures that antivirus signatures are up-to-date, and ensures that the FortiClient firewall is enabled before allowing the traffic from that endpoint to pass through the FortiGate platform. You also have the option to quarantine endpoints running applications that violate policies and require remediation.

Endpoint Network Access Control (NAC)

Features	Monitor & Control Hosts Running FortiClient Vulnerability Scanning of Network Nodes Quarantine Portal Application Detection and Control Built-in Application Database
----------	---

Web Filtering

Web filtering technology is a pro-active defense feature that identifies known locations of malware and blocks access to these malicious sources. In addition, the technology enables administrators to enforce policies based on website content categories ensuring users are not accessing content that is inappropriate for their work environment. The technology restricts access to denied categories based on the policy by comparing each Web address request to a Fortinet hosted database.

Web Filtering

Features	HTTP/HTTPS Filtering URL / Keyword / Phrase Block Blocks Java Applet, Cookies or Active X MIME Content Header Filtering IPv6 Support
----------	--

SSL Inspection

SSL-Encrypted Traffic Inspection protects clients as well as web and application servers from malicious SSL-encrypted traffic, to which many security devices are blind. SSL Inspection intercepts encrypted traffic and inspects it for threats, prior to routing it to its final destination. SSL Inspection applies to both client-oriented SSL traffic (such as users connecting to an SSL-encrypted hosted CRM site) and inbound traffic to an organization's own web and application servers. You now have the ability to enforce appropriate use policies on inappropriate encrypted web content, and protect servers from threats within encrypted traffic flows.

SSL Inspection

Features	Protocol: HTTPS, SMTPS, POP3S, IMAPS Inspection support: Antivirus, Web Filtering, Antispam, Data Loss Prevention SSL Offload
----------	---

Data Loss Prevention

It is imperative for you to control the vast amount of confidential, regulated, and proprietary data traversing your network. Working across multiple applications (including those encrypting their communications), DLP uses a sophisticated pattern-matching engine to identify and then prevent the communication of sensitive information outside the network perimeter. In addition to protecting your organization's critical information, DLP also provides audit trails for data and files to aid in demonstrating policy compliance. You can use the wide range of configurable actions to log, block, and archive data, as well as ban or quarantine users.

Data Loss Prevention (DLP)

Features	Identification and Control Over Data in Motion Built-in Pattern Database RegEx Based Matching Engine Common File Format Inspection International Character Sets Supported
----------	---

Logging, Reporting & Monitoring

FortiGate units provide extensive logging capabilities for traffic, system, and network protection functions. They also allow you to compile reports from the detailed log information gathered. Reports provide historical and current analysis of network activity to help identify security issues that will reduce and prevent network misuse and abuse.

Logging and Monitoring

Features	Internal Log storage and Report Generation Graphical Real-Time and Historical Monitoring Graphical Report Scheduling Support Optional FortiAnalyzer Logging (including per VDOM) Optional FortiGuard Analysis and Management Service
----------	--

High Availability

High Availability (HA) configurations enhance reliability and increase performance by clustering multiple FortiGate appliances into a single entity. FortiGate High Availability supports Active-Active and Active-Passive options to provide maximum flexibility for utilizing each member within the HA cluster. The HA feature is included as part of the FortiOS operation system and is available with almost every FortiGate model.

High Availability (HA)	
Features	Active-Active and Active-Passive Stateful Failover (FW and VPN) Link State Monitor and Failover Device Failure Detection and Notification Server Load Balancing

Virtual Domains

Virtual Domains (VDOMs) enable a single FortiGate system to function as multiple independent virtual FortiGate systems. Each VDOM contains its own virtual interfaces, security profiles, routing table, administration, and many other features. FortiGate VDOMs reduce the complexity of securing disparate networks by virtualizing security resources on the FortiGate platform, greatly reducing the power and footprint required as compared to multiple point products.

Virtual Domains	
Features	Separate Firewall / Routing Domains Separate Administrative Domains Separate VLAN Interfaces
VDOMs (Max / Default)	
2 vCPU	25 / 10
4 vCPU	100 / 10
8 vCPU	250 / 10

Application Control

Application control enables you to define and enforce policies for thousands of applications running on your endpoints, regardless of the port or the protocol used for communication. Application classification and control is essential to manage the explosion of new web-based applications bombarding networks today, as most application traffic looks like normal web traffic to traditional firewalls. Fortinet's application control technology identifies application traffic and then applies security policies defined by the administrator. The end result is more flexible and granular policy control, with deeper visibility into your network traffic.

Application Control	
Features	Identify and Control Over 1,200 Applications Traffic Shaping (Per Application) Control Popular IM/P2P Apps Regardless of Port / Protocol Popular Applications include: AOL-IM Yahoo MSN KaZaa ICQ Gnutella BitTorrent MySpace WinNY Skype eDonkey Facebook and more

Setup / Configuration Options

Fortinet provides administrators with a variety of methods for configuring FortiGate appliances for initial deployment.

Setup / Configuration Options	
Features	Web-based User Interface Command Line Interface (CLI) over serial connection Policy-based provisioning via FortiManager

	FortiGate Virtual Appliance (2 vCPU)	FortiGate Virtual Appliance (4 vCPU)	FortiGate Virtual Appliance (8 vCPU)
Technical Specifications			
Hypervisors Supported	VMware ESXi/ESX 3.5/4.0/4.1	VMware ESXi/ESX 3.5/4.0/4.1	VMware ESXi/ESX 3.5/4.0/4.1
Max vCPUs Supported	2	4	8
Max Network Interfaces Supported	10	10	10
10-GbE Interface Support	Yes	Yes	Yes
10/100/1000 Interfaces	Yes	Yes	Yes
Virtual Machine Storage Required (Minimum)	30 GB	30 GB	30 GB
Virtual Machine Memory Required (Minimum)	512 MB	512 MB	512 MB
System Performance			
Firewall Throughput (UDP packets)	1.6 Gbps	1.6 Gbps	TBD
IPSec VPN Throughput (AES256+SHA1)	TBD	TBD	TBD
IPS Throughput	TBD	TBD	TBD
Antivirus Throughput	325 Mbps	645 Mbps	TBD
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	TBD	TBD	TBD
Client-to-Gateway IPSec VPN Tunnels (System / VDOM)	TBD	TBD	TBD
Concurrent IPSec VPN Tunnels	32,000	48,000	64,000
Concurrent Sessions	800,000	1.15 M	TBD
New Sessions/Sec	15,000	25,000	35,000
Concurrent SSL-VPN Users (Recommended Max)	15,000	25,000	30,000
Firewall Policies (VDOM/System)	TBD	TBD	TBD
Virtual Domains (Max / Default)	25 / 10	100 / 10	250 / 10
Unlimited User Licenses	Yes	Yes	Yes
Available for Order	Yes	Yes	Call

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 FortiGate virtual appliance.

Antivirus performance is measured based on HTTP traffic with 32 KB file attachments.

FortiGate Virtual Appliance multi-threat security appliances also include

Multiple Deployment Modes (Transparent/Routing)
 Advanced Layer-2/3 Routing Capabilities
 High Availability
 Virtual Domains (VDOMs)
 Data Center Traffic Optimization
 Traffic Shaping and Prioritization
 WAN Optimization
 Multiple Device Authentication Options

MANAGEMENT OPTIONS

Local Web-Based Management Interface
 Command Line Management Interface (CLI)
 Local Event Logging
 Centralized Management (FortiManager Appliance Required)
 Centralized Event Logging (FortiAnalyzer Appliance Required)

Ordering Info	
Product Description	SKU
FortiGate Virtual Appliance (2 vCPU)	FG-VM02
FortiGate Virtual Appliance (4 vCPU)	FG-VM04
FortiGate Virtual Appliance (8 vCPU)	FG-VM08
Optional Accessories	SKU
Virtual Domain (VDOM) Upgrade License 11-25	FG-VDOM-25
Virtual Domain (VDOM) Upgrade License 26-50	FG-VDOM-50
Virtual Domain (VDOM) Upgrade License 51-100	FG-VDOM-100
Virtual Domain (VDOM) Upgrade License 101-250	FG-VDOM-250
Virtual Domain (VDOM) Upgrade License 11-250	FG-VDOM

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



Copyright © 2010 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. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.