



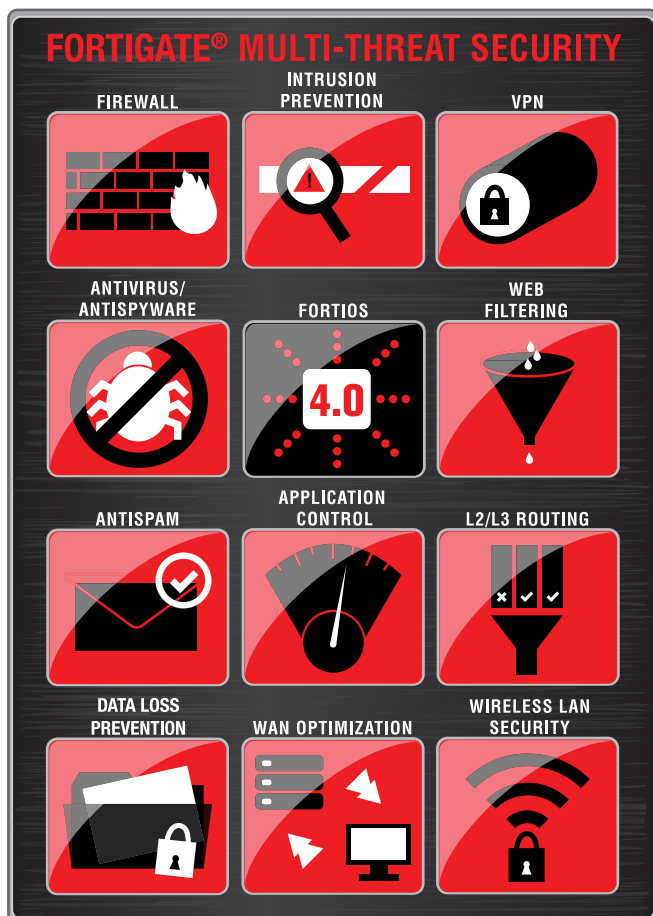
# FortiOS™ 4.0 Software

**Redefining Network Security**

## FortiOS 4.0 Software—Redefining Network Security

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of FortiGate multi-threat security platforms. FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC™ content and network processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with expert threat intelligence delivered via FortiGuard® Security Subscription Services.

FortiOS 4.0 software redefines network security by extending the scope of integrated security and networking capabilities within the FortiGate multi-threat security platform. Regardless of the size of your organization, you can benefit from the most comprehensive suite of security and networking services within a single device on the market today. FortiOS 4.0 software includes a wide range of features that increase your security while reducing your operating and capital costs. FortiGate platforms combine enterprise-class firewall, IPSec VPN, SSL-VPN, intrusion prevention, antivirus, web filtering, antispam, and Layer 2/3 routing services. The latest release also adds Data Loss Prevention (DLP), WAN optimization, application control, SSL-encrypted traffic inspection, endpoint Network Access Control (NAC), enhanced VoIP Security, and Vulnerability Management capabilities. FortiOS 4.0 software delivers on its mission to enable secure business communications while offering the best performance and lowest cost of ownership.



***“Changing business processes and threats are driving new requirements for network security. Increasing bandwidth and new application communication (such as Web 2.0) are changing how protocols are used and how data is presented. Software as a service is moving critical data off-site, and an increasing reliance on critical IT is pushing security in new directions.”***

Greg Young and John Pescatore, Gartner, Magic Quadrant for Enterprise Firewalls, November 2008.

### Enhanced Security

Fortinet designed FortiOS 4.0 security services from the ground up to deliver integrated performance and effectiveness that standalone products simply cannot match. The services work together as a system, acting in tandem to provide you with better visibility and the ability to stop threats against your network and applications as early as possible, before damage can occur.

### Improved Value

FortiOS 4.0 software provides you with access to security services that you may have considered cost-prohibitive or overly complex to deploy individually. Moreover, the new features of FortiOS 4.0 software are available at no additional cost for every eligible FortiGate device with an active maintenance contract.

### Simplified Management

FortiOS 4.0 software consolidates your security infrastructure and simplifies your management requirements, lowering your costs and reducing the workload of your IT staff. It dramatically reduces the complexity of deploying defense-in-depth compared with stand-alone products. You have the flexibility of a unified policy at the device level and an appliance-based centralized management platform for large deployments. Fortinet even offers a service-based management solution for smaller organizations to further simplify security management, fully integrated with FortiOS 4.0 software.



## FortiOS 4.0 Software—Raising The Bar

Fortinet continues to increase the breadth and depth of security and networking services included in the FortiOS purpose-built operating system. By adding new functionality and enhancing the performance of existing services, FortiOS software continues to demonstrate why it remains the gold standard for multi-threat security. In the past, the only way organizations could deploy these technologies was by adding more stand-alone products, which also increased deployment, configuration, and management costs.

### ANTIVIRUS/ ANTISPYWARE



## Antivirus

FortiOS gives you the choice of up to four options for protection from malware. In addition to three proxy-based antivirus databases, FortiOS also now includes a high-performance flow-based antivirus option. The new flow-based option scans files as they pass through the device, allowing you to scan files of any size and still maintain the highest levels of performance. By providing you the flexibility to choose your antivirus engine, you can balance your performance and security requirements for your environment.

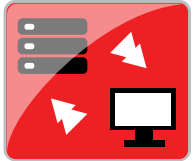
### DATA LOSS PREVENTION



## Data Loss Prevention (DLP)

It is imperative for you to control the vast amount of confidential, regulated, and proprietary data traversing your network, and keep it within defined network boundaries. 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 policy compliance. You can use the wide range of configurable actions to log, block, and archive data, as well as ban or quarantine users.

### WAN OPTIMIZATION



## WAN Optimization

With WAN Optimization, you can accelerate applications over your wide area links while ensuring multi-threat security enforcement. FortiOS 4.0 software not only eliminates unnecessary and malicious traffic as one of its core capabilities, it also optimizes legitimate traffic by reducing the amount of communication and data transmitted 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.

### APPLICATION CONTROL



## 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 easily defined by the administrator. The end result is more flexible and granular policy control, with deeper visibility into your network traffic.

### SSL INSPECTION



## SSL-Encrypted Traffic Inspection

SSL-Encrypted Traffic Inspection protects clients and web and application servers from malicious SSL-encrypted traffic, to which most security devices are often 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 destined 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 encrypted intrusion attempts and other encrypted attacks.

### ENDPOINT NAC



## Endpoint Network Access Control (NAC)

Endpoint NAC enforces the use of the FortiClient Endpoint Security application (either Standard or Premium editions) on your network. It verifies the installation of the most recent version of the FortiClient application, up-to-date antivirus signatures, and enabled firewall 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.

## FortiOS Security Services

### FIREWALL

ICSA Labs Certified (Enterprise Firewall)  
NAT, PAT, Transparent (Bridge)  
Policy-Based NAT  
VLAN Tagging (802.1Q)  
User Group-Based Authentication & Scheduling  
SIP/H.323 /SCCP NAT Traversal  
WINS Support  
Explicit Proxy Support (incl. Citrix/TS Support)  
VoIP Security (SIP Firewall / RTP Pinholing)  
IPv6 Support (NAT / Transparent mode)  
Identity/Application-Based Policy

### VIRTUAL PRIVATE NETWORK (VPN)

ICSA Labs Certified (IPSec/SSL-TLS)  
PPTP, IPSec, and L2TP + IPSec Support  
SSL-VPN Concentrator (incl. iPhone client support)  
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)

### ANTIVIRUS

ICSA Labs Certified (Gateway Antivirus)  
Includes Antispyware and Worm Prevention  
Protocols: HTTP/HTTPS SMTP/SMTPS  
POP3/POP3S IMAP/IMAPS  
FTP Major IM Protocols  
Flow-Based Antivirus Scanning Mode  
Automatic "Push" Content Updates  
File Quarantine Support  
IPv6 Support  
Databases: Standard, Extended, Extreme, and Flow

### WEB FILTERING

76 Unique Content Categories / 2+ Billion Unique URLs  
HTTP/HTTPS Filtering  
Web Filtering Time-Based Quota  
URL/Keyword/Phrase Block  
URL/Category Exempt  
Blocks Java Applet, Cookies, Active X  
MIME Content Header Filtering  
IPv6 Support

### APPLICATION CONTROL

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

### 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 of 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  
Vulnerability Scanning of Network Nodes

## FortiOS Networking Services

### NETWORKING/ROUTING

Multiple WAN Link Support  
PPPoE Support  
DHCP Client/Server  
Policy-Based Routing  
Dynamic Routing for IPv4 (RIP, OSPF, IS-IS, BGP, & Multicast protocols)  
Dynamic Routing for IPv6 (RIP, OSPF, & BGP)  
Multi-Zone Support  
Route Between Virtual LANs (VLANs)  
Multi-Link Aggregation (802.3ad)  
VRRP and Link Failure Control  
sFlow Client

### TRAFFIC SHAPING

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

### VIRTUAL DOMAINS (VDOMs)

Separate Firewall/Routing Domains  
Separate Administrative Domains  
Separate VLAN Interfaces

### DATA CENTER OPTIMIZATION

Web Server Caching TCP Multiplexing  
HTTPS Offloading WCCP Support

### 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  
Requires a FortiGate device with Hard Drive

## FortiOS Management Services

### MANAGEMENT/ADMINISTRATION OPTIONS

Web UI (HTTP/HTTPS), Telnet / Secure Command Shell (SSH), and Command Line Interface (CLI)  
Role-Based Administration  
Multi-language Support: English, Japanese, Korean, Spanish, Chinese (Simplified & Traditional), French  
Multiple Administrators and User Levels  
System Software Rollback  
Configurable Password Policy  
Customizable Dashboard Widgets (Web UI)  
Central Management via FortiManager (optional)

### LOGGING/MONITORING/VULNERABILITY MGMT

Network Vulnerability Scanning  
Graphical Report Scheduling Support  
Graphical Real-Time and Historical Monitoring  
Local and Remote Syslog/WELF server logging  
SNMP Support  
Email Notification of Events  
VPN Tunnel Monitor  
Optional FortiAnalyzer Logging (including per-VDOM)  
Optional FortiGuard Analysis and Management Service

### FIREWALL USER AUTHENTICATION OPTIONS

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



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, vulnerability management, web application firewall, 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 hardware return for 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.

## FORTINET®

### 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  
61 Robinson Road, #09-04 Robinson Centre  
Singapore 068893  
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.