



# FortiOS™ 4.0 Software

## Redefining Enterprise Network Security

## FortiOS 4.0 Software — Redefining Enterprise Network Security

Today's networks are faster than ever, carrying more information and rich content - as well as potentially malicious payloads. The volume and sophistication of hacker-based attacks have also increased, requiring more accurate detection methods and the ability to block threats before they can do serious damage. Simultaneously, cost-reduction programs are forcing IT departments to consolidate network equipment and operating expenses wherever possible.

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of all FortiGate® consolidated security platforms. FortiOS 4.0 software leverages the hardware acceleration provided by custom FortiASIC™ processors, delivering the most comprehensive suite of IPv6-ready security and networking services available within a single device. FortiGuard® Security Subscription Services ensure that FortiOS threat protections are always up to date, defending your network against the latest, most sophisticated and dynamic attacks.

### FortiOS 4.0 Security Features

- Enterprise-class Firewall - IPv6-Ready
- VPN - IPSec and SSL
- SSL-encrypted Traffic Inspection
- Antivirus / Antispyware
- Antispam
- Intrusion Prevention System (IPS)
- Data Loss Prevention (DLP)
- Flow-based Inspection Options
- Web Filtering
- Application Control
- Endpoint Network Access Control (NAC)
- Vulnerability Management
- Monitoring, Logging and Reporting
- WAN Optimization
- Wireless Controller
- VoIP Security
- Central Management
- Virtual Domains
- High Availability
- Layer 2/3 Routing Services
- FortiGuard Security Updates

### Complete Security

Fortinet designed and built 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 to provide better visibility and mitigation of the latest network and application threats, stopping attacks before theft and damage can occur.

### Customized for Performance

FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC processors. This combination of custom hardware and software gives you the best security and performance possible from a single device.

### Increased Simplicity

FortiOS 4.0 software lowers costs and reduces IT staff workloads. Centralized management and analysis ensure consistent policy creation and enforcement while minimizing deployment and configuration challenges. You gain the flexibility of having a unified security policy at the device level along with an appliance-based centralized management platform for large deployments.

### Unique Visibility and Control

Advanced security features such as Flow-based Inspection and Wireless Controller capability allow you to monitor and protect your network from endpoints to core, and from remote offices to headquarters. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

***“A further disrupting factor is the rate of change within enterprise networking — inexorably increasing throughput, more Web-based applications, more complex connections within applications, more complex data centers and more data being presented to customers means that firewalls have had to keep up with features and performance to meet these changing needs”.***

Greg Young and John Pescatore  
Gartner Magic Quadrant for Enterprise Network Firewalls - March 2010.



## FortiOS 4.0 Software — Complete Content and Network Protection

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. FortiOS 4.0 software includes many advanced security and networking features, some of which are highlighted below:



### Application Control

Application control enables you to define and enforce policies for thousands of applications running on your network and endpoints. Newer Web-based applications such as Facebook, Skype, Twitter and Salesforce.com can be detected and controlled at a granular level, regardless of ports and protocols used. Application classification and control is essential to manage the explosion of new Internet-based technologies bombarding networks today.

---



### Antivirus / Antispyware

In addition to three proxy-based antivirus databases, FortiOS also includes a high-performance flow-based antivirus option. The flow-based option allows you to scan files of any size while maintaining the highest levels of performance. In addition, flow-based inspection enables scanning of files within compressed files to detect hidden threats. By providing you the flexibility to choose your antivirus engine, you can balance your performance and security requirements for your environment.

---



### Data Loss Prevention (DLP)

Fortinet DLP identifies sensitive information and blocks transmission to points outside of your network perimeter. A sophisticated pattern-matching engine monitors traffic from multiple applications, such as Web-based email and encrypted instant messaging, and provides audit trails to aid in policy compliance. You can select from a wide range of configurable actions to log, block and archive data, as well as ban or quarantine rogue users. Flow-based DLP options are also available.

---



### Web Filtering

Inappropriate Web surfing and use of Web-based applications can result in lost productivity, network congestion, malware infection and data loss. Web Filtering controls user access to Web-based applications such as instant messaging, peer-to-peer file sharing and streaming media, while blocking phishing sites and blended network attacks. In addition, botnet command and control traffic and fast flux file downloading can be blocked. Flow-based Web filtering options are available.

---



### Wireless Controller

All FortiGate and FortiWiFi™ consolidated security platforms have an integrated wireless controller, enabling centralized management of FortiAP™ secure access points and wireless LANs. Unauthorized wireless traffic is blocked, while allowed traffic is subject to identity-aware multi-threat security inspection. You can control network access, quickly update security policies, and identify and suppress rogue access points - all from a single console.

---



### WAN Optimization

Wide area network (WAN) optimization accelerates applications over your wide area links while ensuring multi-threat security enforcement. FortiOS 4.0 software eliminates unnecessary and malicious traffic and optimizes legitimate traffic by reducing the amount of information transmitted between applications and servers. This improves performance of applications and network services while reducing bandwidth requirements.



## Firewall

Fortinet firewall technology combines ASIC-accelerated stateful inspection with an arsenal of integrated application security engines to quickly identify and block complex threats. FortiGate firewall protection integrates with other key security features such as virtual private network (VPN), antivirus, intrusion prevention, Web filtering, antispam and traffic shaping to deliver multi-layered security that scales from small business appliances to multi-gigabit core network and data center platforms.



## Intrusion Prevention

Intrusion prevention system (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 specific profile-matching the attack behavior. This behavior is then analyzed by our threat research team to identify threats as they emerge and generate new signatures that are incorporated into our FortiGuard services.



## VPN

Fortinet virtual private network technology provides secure communications between multiple networks and hosts using IPSec and SSL VPN protocols. Both services leverage custom FortiASIC processors to accelerate encryption and decryption network traffic. Once the traffic has been decrypted, multi-threat inspection including antivirus, intrusion prevention, and Web filtering can be applied and enforced for all content.



## Antispam

Fortinet antispam technology offers a wealth of features to detect, tag, quarantine, and block spam messages and malicious attachments generated by spambots and compromised systems. FortiGate and FortiWiFi platforms and FortiClient endpoint security agents offer integrated antispam functionality as part of their multi-layered protection, backed by the FortiGuard Antispam Service.

## FortiOS Security Services

### 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
- Explicit Proxy Support (Citrix/TS etc.)
- VoIP Security (SIP Firewall / RTP Pinholing)
- Granular Per-Policy Protection Profiles
- Identity/Application-Based Policy
- Vulnerability Management
- IPv6 Support (NAT / Transparent mode)

### VIRTUAL PRIVATE NETWORK (VPN)

- ICSA Labs Certified (IPSec/SSL-TLS)
- PPTP, IPSec, and L2TP + IPSec Support
- SSL-VPN Concentrator (including 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 / ANTISPYWARE

- 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
- Databases: Standard, Extended, Extreme, Flow
- IPv6 Support

### WEB FILTERING

- 76 Unique Content Categories
- FortiGuard Web Filtering Service Categorizes over 2 Billion Web pages
- 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
- Flow-based Web Filtering

### APPLICATION CONTROL

- Identify and Control Over 1400 Applications
- Traffic-Shaping (Per Application)
- Facebook Application and Category Control
- Differential Services Support 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)
- Customized Patterns
- Supports IM, HTTP/HTTPS, and More
- Many Popular File Types Supported
- International Character Sets Supported
- Document Fingerprinting
- Flow-Based DLP Scanning Mode

### 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 Zones
- Route Between Virtual LANs (VLANs)
- Multi-Link Aggregation (802.3ad)
- IPv6 Support (Firewall, DNS, Transparent Mode, SIP, Dynamic Routing, Admin Access, Management)
- 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

### VIRTUAL DOMAINS (VDOMs)

- Separate Firewall/Routing Domains
- Separate Administrative Domains
- Separate VLAN Interfaces
- 10 VDOM License Std. (more can be added)

### 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
- FortiToken Support

### WIRELESS CONTROLLER

- Unified WiFi and Access Point Management
- Automatic Provisioning of APs
- On-wire Detection and Blocking of Rogue APs
- Virtual APs with Different SSIDs
- Multiple Authentication Methods

## Fortinet Certifications



**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.

### 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](http://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 +65-6513-3734  
Fax +65-6295-0015



Copyright© 2011 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.