FortiOS™ 4.0 Software

FortiGate® Multi-Threat Security

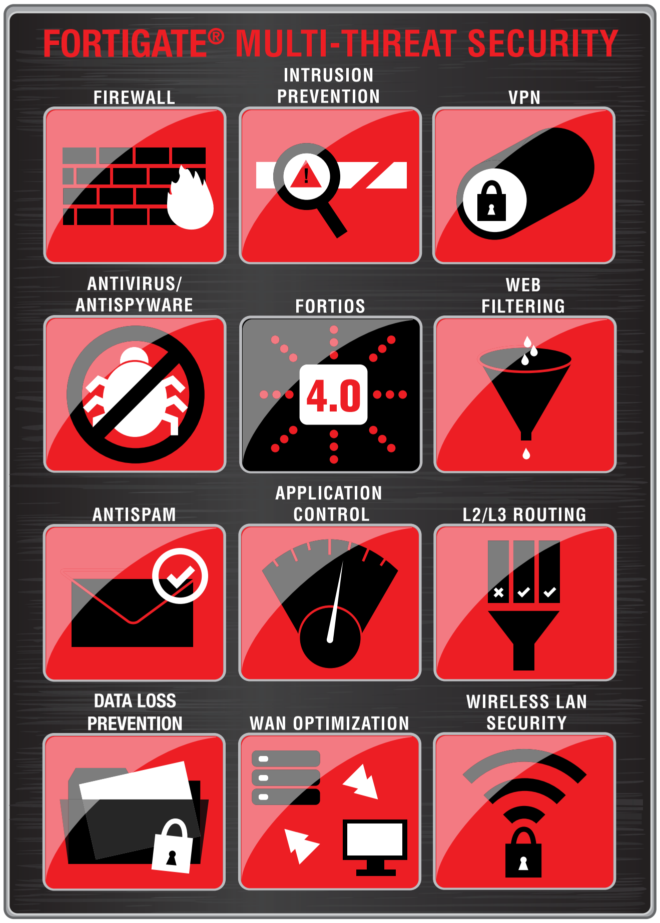
Redefining Network Security

FORTINET®

FortiOS 4.0—Redefining Network Security

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of FortiGate multi-threat network security platforms. Leveraging the hardware acceleration provided by FortiASIC™ content and network processors, FortiOS enables high performance multi-threat security resulting in some of the highest levels of security and performance possible from a single device. When updated with the latest threat intelligence via FortiGuard™ security subscription services, FortiOS is prepared to stop the latest and evolving threats facing networks today.

With the release of FortiOS 4.0, Fortinet has redefined network security *again* by extending the scope of consolidated security and networking capabilities within FortiGate multi-threat network security platforms. While FortiOS 4.0 includes many new features, the most significant additions to the FortiGate platform include Data Loss Prevention (DLP), WAN Optimization, Application Control, and SSL-Encrypted Traffic Inspection. Organizations of all sizes can now benefit from an integrated solution which offers the most comprehensive suite of security and networking services within a single device—the new services in FortiOS 4.0 joining the already included enterprise-class firewall, IPSec VPN, SSL-VPN, Intrusion Prevention, Antivirus, Web Filtering, Antispam, and Layer 2/3 routing services. With over 40 new features, FortiOS 4.0 delivers on its mission to enable secure business communications while offering the best security, performance, and total cost of ownership possible.



Enhanced Security

FortiOS 4.0 security services are designed from the ground up to be integrated, delivering overall security effectiveness that standalone products simply cannot match. The services work together as a system, acting in tandem to provide better visibility and stop threats as early as possible—resulting in less collateral damage.

Improved Value

FortiOS 4.0 provides access to security services that were previously cost prohibitive or too complex to deploy individually. Moreover, the new features of FortiOS 4.0 are available at no additional cost for every eligible FortiGate device with an active maintenance contract.

Simplified Management

FortiOS 4.0 consolidates security infrastructure and simplifies management. Using a unified policy at the device level, and an appliance-based centralized management platform for large deployments, complexity can be dramatically reduced over standalone offerings. Fortinet even offers a service-based management solution for smaller organizations to further simplify security management, fully integrated with FortiOS 4.0.

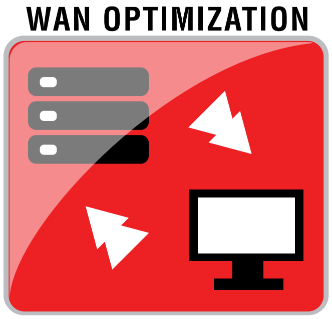
> ***"Changing business processes and threats are driving new requirements for network security. Increasing bandwidth and new application communication (such as Web 2.0) are changing how protocols are used and how data is presented. Software as a service is moving critical data off-site, and an increasing reliance on critical IT is pushing security in new directions."***
>
> Greg Young and John Pescatore, Gartner, Magic Quadrant for Enterprise Firewalls, November 2008.

FortiOS 4.0—Over 40 New Features

With over 40 new features, Fortinet engineers have enhanced virtually every aspect of the operating system, including the addition of two distinct services, Data Loss Prevention and WAN Optimization, which have previously been available as standalone products only. Other features extend existing services, such as an identity-based policy feature, which allows the FortiGate's firewall policies to be defined by user or group. Multiple enhancements to the existing intrusion prevention service allow passive IDS support, and also make the intrusion prevention service IPv6 ready.

Data Loss Prevention (DLP)

With increasingly sensitive, confidential, and proprietary data being communicated across networks, the ability to keep that information within defined network boundaries is imperative. Working across multiple applications (including those encrypting their communications), DLP uses a sophisticated pattern-matching and regular-expression engine to identify then prevent the communication of sensitive information outside of the network perimeter. In addition to protecting an organization's critical information, DLP also provides audit trails for data and files, which can aid in legislative compliance. With configurable DLP actions, organizations can log, block, and archive data as well as ban or quarantine users.



WAN Optimization

With WAN Optimization, customers can accelerate applications over wide area links and, at the same time, ensure multi-threat security enforcement. FortiOS 4.0 not only eliminates unnecessary and malicious traffic as one of its core capabilities, it also now optimizes legitimate traffic by reducing the amount of communication and data transmitted between applications and servers across the WAN. This results in a much faster user experience—increasing productivity—as well as helping to avoid additional higher-bandwidth provisioning requirements.

Application Control

With Application Control, security policy can be defined and enforced for thousands of applications, regardless of the port or the protocol used for communication. With the explosion of new web-based applications bombarding networks today, most of which look like normal web traffic to traditional firewalls, application classification and control is essential. Fortinet's Application Control technology identifies application traffic and then applies security policies easily defined by the administrator. The end result: more flexible, more granular policy control and deeper visibility into network traffic.

SSL-Encrypted Traffic Inspection

SSL-Encrypted Traffic Inspection protects clients and web and application servers from malicious SSL-encrypted traffic which security devices are often blind to. With SSL Inspection, encrypted traffic is intercepted and inspected for threats, prior to being allowed access 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. Inappropriate encrypted web content can now be filtered by appropriate use policies and servers can now be protected from encrypted intrusion attempts and attacks.

FortiGate—Purpose-Built Hardware, Software, and Services

FortiGate platforms are based on an integrated hardware, software, and services architecture specifically designed for improved security and performance in perimeter, core, and data center environments. The FortiASIC™ Content Processor (CP) is a key component in FortiGate security platforms; providing a hardware scanning engine, hardware encryption, and real-time content analysis processing capabilities. The FortiASIC Network Processor (NP) series of processors provides acceleration for firewall, encryption/decryption, signature and heuristic packet scanning, and bandwidth shaping. FortiOS security applications can be selectively enabled to provide a full suite or a unique set security services all within a single platform. The FortiGuard™ network dynamically updates system software and security services such as antivirus, antispam, Web filtering, antispyware, and intrusion prevention to ensure the maximum level of protection is being provided.

FortiOS Security Services

FIREWALL
ICSA Labs Certified (Enterprise Firewall)
NAT, PAT, Transparent (Bridge)
Routing Mode (RIP v1 & v2, OSPF, BGP, & Multicast)
Policy-Based NAT
Virtual Domains (NAT/Transparent mode)
VLAN Tagging (802.1Q)
User Group-Based Authentication
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
IPSec NAT Traversal
Dead Peer Detection
RSA SecurID Support

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 Network
File Quarantine Support
Block by File Size or Type

WEB FILTERING
76 Unique Categories Provided by the 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

APPLICATION CONTROL
Identification 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

INTRUSION PREVENTION SYSTEM (IPS)
ICSA Labs Certified (NIPS)
Protection From Over 3000 Threats
Protocol Anomaly Support
Custom Signature Support
Automatic Attack Database Update

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

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

FortiOS Networking Services

NETWORKING/ROUTING
Multiple WAN Link Support
PPPoE Support
DHCP Client/Server
Policy-Based Routing
Dynamic Routing (RIP v1 & v2, OSPF, BGP, & Multicast)
Multi-Zone Support
Route Between Zones
Route Between Virtual LANs (VDOMS)
Multi-Link Aggregation (802.3ad)
IPv6 Firewall and Management Support

TRAFFIC SHAPING
Policy-based Traffic Shaping
Differentiated Services (DiffServ) Support
Guarantee/Max/Priority Bandwidth

VIRTUAL DOMAINS (VDOMs)
Separate Firewall/Routing domains
Separate Administrative domains
Separate VLAN interfaces
10 VDOM license standard, upgradable with additional license

DATA CENTER OPTIMIZATION
Web Server Caching   TCP Multiplexing
HTTPS Offloading

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
Console Interface (RS-232)
WebUI (HTTP/HTTPS)
Telnet / Secure Command Shell (SSH)
Command Line Interface
Role-Based Administration
Multi-language Support
Multiple Administrators and User Levels
Upgrades and Changes Via TFTP and WebUI
System Software Rollback
Central Management via FortiZManager (optional)

LOGGING/MONITORING
Internal 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
Optional FortiGuard Analysis and Management Service

FIREWALL USER AUTHENTICATION OPTIONS
Local Database
Windows Active Directory (AD) Integration
External RADIUS/LDAP Integration
IP/MAC Address Binding
Xauth over RADIUS for IPSEC VPN
RSA SecurID Support

FORTINET

GLOBAL HEADQUARTERS
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
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33-4-8987-0510
Fax +33-4-8987-0501

APAC SALES OFFICE - SINGAPORE
61 Robinson Road
#09-04 Robinson Centre
Singapore 068893
Tel: +65-6513-3730
Fax: +65-6223-6784