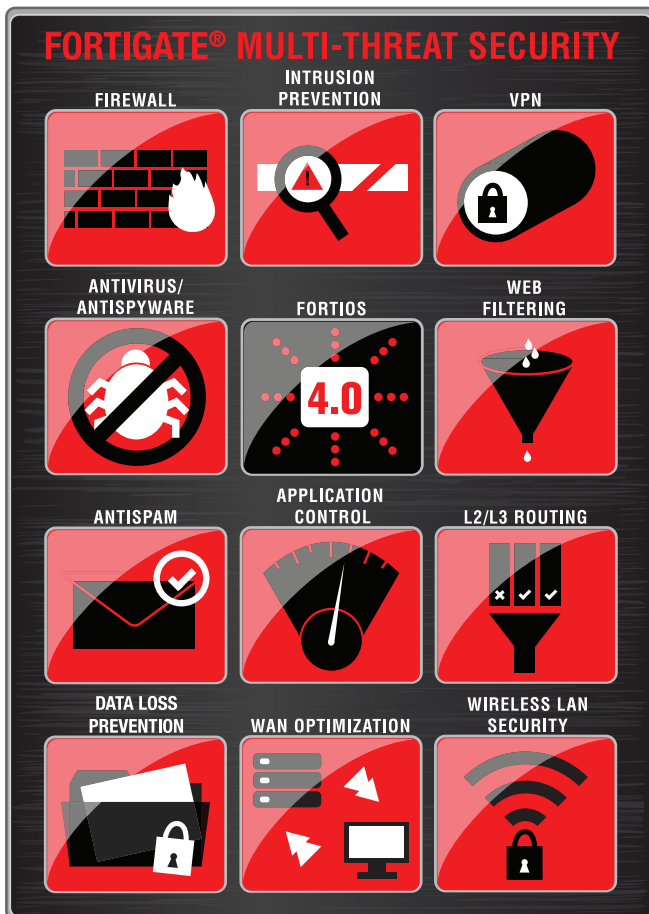# FORTINET®

FortiOS™ Software

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. FortiOS 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 some of the highest levels of security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with dynamic 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 network 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 content and network 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. It also includes Data Loss Prevention (DLP), WAN optimization, application control, SSL-encrypted traffic inspection, and endpoint Network Access Control (NAC). FortiOS 4.0 software delivers on its mission to enable secure business communications while offering the best security, performance, and total cost of ownership possible.

FORTIGATE® MULTI-THREAT SECURITY

FIREWALL — INTRUSION PREVENTION — VPN
ANTIVIRUS/ANTISPYWARE — FORTIOS 4.0 — WEB FILTERING
ANTISPAM — APPLICATION CONTROL — L2/L3 ROUTING
DATA LOSS PREVENTION — WAN OPTIMIZATION — WIRELESS LAN SECURITY

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.

> *"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 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.

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
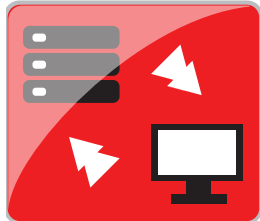
WAN Optimization

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)
Routing Mode (RIP, OSPF, BGP, Multicast)
Policy-Based NAT
Virtual Domains (NAT/Transparent mode)
VLAN Tagging (802.1Q)
User 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)

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
IPv6 Support

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
MIME Content Header Filtering
IPv6 Support

APPLICATION CONTROL
Identifiy 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
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

FortiOS Networking Services

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 (VDOMS)
Multi-Link Aggregation (802.3ad)
IPv6 Support (Firewall, DNS, Transparent Mode, SIP, Dynamic Routing, Administrative Access, Management)

TRAFFIC SHAPING
Policy-based 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
10 VDOM License Standard, Upgradable to More

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: 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
Central Management via FortiManager (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 (including per-VDOM)
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
LDAP Group Support

ICSAlabs CERTIFIED ANTI-VIRUS   ICSAlabs CERTIFIED IPSEC-BASIC   ICSAlabs CERTIFIED NETWORK IPS   ICSAlabs CERTIFIED FIREWALL-CORPORATE

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 control, 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 "return and repair" hardware 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.

F🔳RTINET®

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

FORTIOS-41-BRO-1009-R1