



DATASHEET

FortiGate® -200 to -800 Series

Multi-Layer Security Appliances for Mid-Size Organizations

Blended Security Threats

Network security threats could be devastating to networks. Intellectual property, revenue, customer and company records, and other mission-critical resources. Point-products providing security solutions for specific purposes may provide adequate protection against specific single-threaded threats, however blended-threats and attacks utilize a multitude of attack vectors. Assembling an array of point products is costly and requires significant expertise to engineer, maintain and manage. Most small to medium size businesses cannot afford such overhead, yet should tragedy strike the potential business costs are enormous. Fortunately cost-effective, evergreen multi-threat protection is now available to businesses of any size. The FortiGate-200 through -800 series of advanced security systems integrate all-in-one multi-threat protection into cost-effective plug-n-play security platforms that effectively block today's blended attacks including intrusion attempts, viruses, worms, phishing, spyware, spam and many other types of malware. The Fortinet FortiGuard® global 24x7 threat detection and update service provides the networking industry's fastest response time to ensure latest security threats are detected and automatic security updates are available before your business is impacted.

Security Platforms That Meet the Challenge

FortiGate security platforms are based on Fortinet's revolutionary FortiASIC™ Content Processor technology, which enables a comprehensive suite of real-time security solutions while delivering the highest levels of network performance. The FortiGate-200-800 series platforms provide a complete security solution including content inspection firewall, IPSEC and SSL VPN, intrusion prevention, web filtering, antispam, antivirus, antispyware, endpoint control, and application control that prevent blended attacks, as well as providing integrated traffic shaping functions, making them the most cost effective, convenient and powerful network protection solutions available. In addition, Fortinet's per-device security subscriptions and turnkey appliance design makes them an affordable and easy-to-manage security solution for small-to-medium enterprises.



FortiOS 4.0 Software Redefines Networks Security

FortiOS 4.0 is a purpose-built operating system that leverages the power of specialized FortiASIC hardware to offer increased levels of security and performance. Fortinet developed FortiOS 4.0 software solely for the FortiGate multi-threat security platform. FortiOS software enables a comprehensive suite of security services – firewall, VPN, intrusion prevention, antimalware, antispam, web filtering, application control, data loss prevention, vulnerability management, and end point network access control.

The FortiASIC Advantage

FortiASIC processors power FortiGate platforms. With exclusive hardware, the purpose built, high-performance network, security, and content processors use intelligent and proprietary digital engines to accelerate resource-intensive security services.

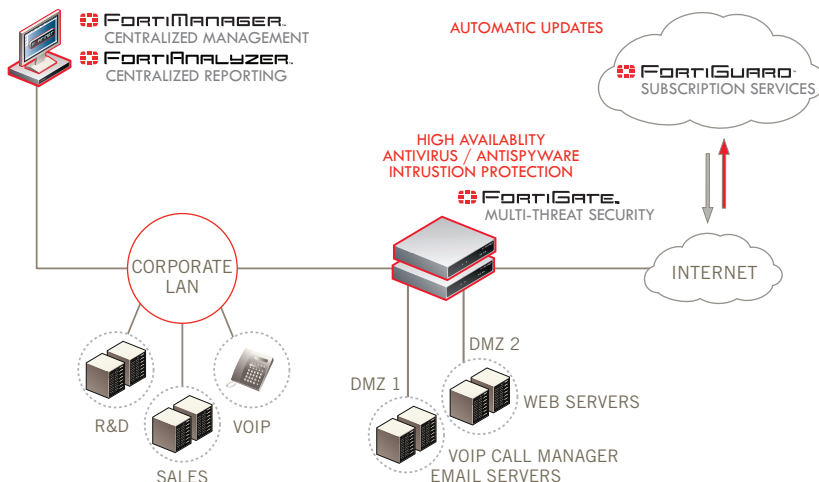
Features	Benefits
All-inclusive, cost-effective security solution	Fortinet offers a lower total cost of ownership with the most complete set of functions including: antivirus, intrusion prevention, antispyware, web content filtering, and antispam
Automated updates of antivirus/antispyware and IPS security content	Around-the-clock protection against the latest threats. Virus and intrusion encyclopedia covers more than 60,000 different threats
High performance custom hardware	The Fortinet FortiASIC delivers superior performance and reliability, ensuring that the security appliance does not become a network bottleneck
Integrated multi-port switch	Eliminates the need for external switches and provides enhanced connectivity options
Secure Web UI for easy deployment and management	Quick and easy configuration wizard walks administrators through initial setup and graphical user interface offers at-a-glance security event and performance monitoring
Security hardened custom Operating System (OS)	Underlying FortiOSTM is ICSA Labs-certified and offers a comprehensive command-line interface

Fortinet's family of mid-range security appliances are designed for mid-size enterprise networks.

Secure Web Access

Firewall + Antivirus + Web Filtering

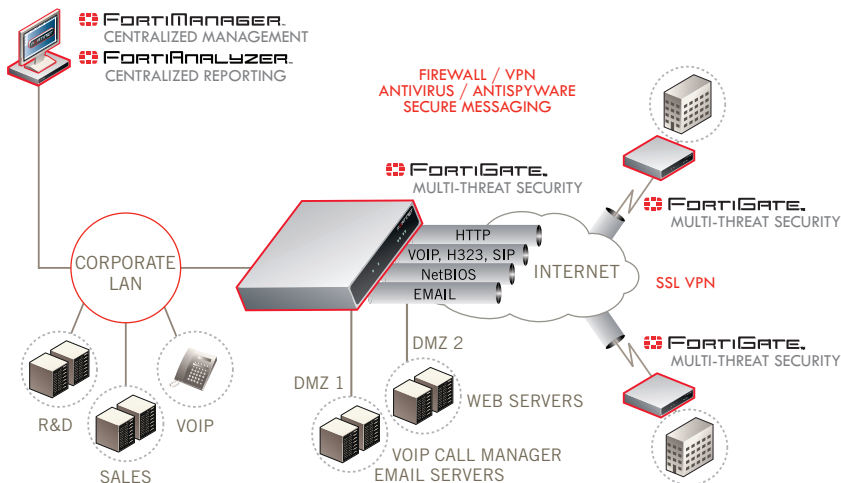
The primary source of threats to the Enterprise network is undoubtedly from uncontrolled employee access to the Internet and Web-based services. Yet today every business not only relies on the Internet for productivity enhancements and competitive advantage, but literally depends on the Internet for business success. With all the benefits of the Internet, also come potential risks such as viruses and worms that disrupt services or destroy valuable data, and a myriad of security challenges including information theft/leakage, inappropriate usage and the need to comply with regulatory mandates. The FortiGate-200-800 series of mid-range security appliances provide a turn-key suite of ICSA Labs certified multi-layered security applications to stop blended attacks from affecting your business.



Secure Perimeter Access

Firewall + VPN+ Intrusion Prevention + Antivirus

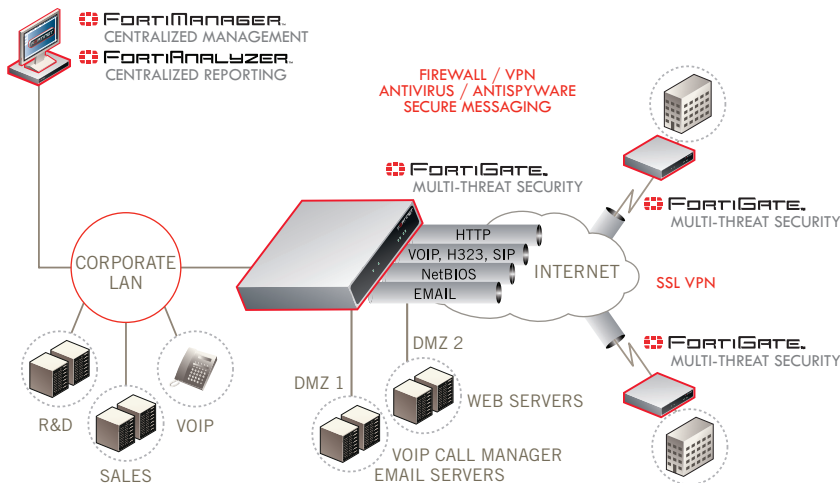
Enterprises often have complex network topologies and, therefore, complex network security requirements. Typical deployments mean linking several sites together—ranging from home offices to larger remote offices—and ensuring that the security implementation is seamless. Security devices for these environments need to provide a wide variety of performance metrics and connectivity options. Fortinet's line of mid-range security appliances offer integrated 4-port switches, 10/100/1000 Ethernet ports, up to 1 Gbps firewall throughput, and up to 200 Mbps VPN throughput. These options include the full security suite of ICSA Labs certified multi-layered security applications to stop blended attacks from affecting your enterprise's productivity.



Secure Messaging Access

Antispam+ Antivirus + IM / P2P Controls

The FortiGate line of security appliances has a flexible architecture that allows each one to quickly adapt to emerging technologies and threats such as IM, P2P, and VOIP applications and identity theft methods such as spyware, phishing, and pharming attacks. Flexible deployment options such as NAT, Route, and Transparent modes allow FortiGate devices to be easily deployed into most network designs. Core networking features, such as High Availability (HA) and support for dynamic routing protocols like RIP, OSPF, and BGP, allow them to be deployed into complex full mesh network environments that require maximum network availability.



Technical Specifications



	FortiGate-200A	FortiGate-224B	FortiGate-300A	FortiGate-400A	FortiGate-500A	FortiGate-800/800F
HARDWARE SPECIFICATION						
Total 10/100 Interfaces	8	26	4	4	8	4
Switch Interfaces	4	24	n/a	n/a	4	n/a
Configurable Ports	n/a	n/a	4	4	4	4
Fixed WAN / DMZ Ports	2/2	2	n/a	n/a	n/a	n/a
Total 10/100/1000 Interfaces (Copper)	n/a	2 (switched)	2	2	2	4 (FG-800 only)
1Gb SFP Interfaces (Fiber)	n/a	n/a	n/a	n/a	n/a	4 (FG-800F only)
SYSTEM PERFORMANCE						
Firewall Throughput (1518 Byte Pkt)	180 Mbps	180 Mbps	1.2 Gbps	1.2 Gbps	1.2 Gbps	2 Gbps
Firewall Throughput (512 Byte)	150 Mbps	150 Mbps	400 Mbps	500 Mbps	600 Mbps	1 Gbps
IPSec VPN Throughput	70 Mbps	70 Mbps	120 Mbps	140 Mbps	150 Mbps	200 Mbps
Antivirus Throughput	30 Mbps	30 Mbps	70 Mbps	100 Mbps	120 Mbps	150 Mbps
IPS Throughput	100 Mbps	100 Mbps	200 Mbps	300 Mbps	400 Mbps	600 Mbps
Gateway-to-Gateway IPSec VPN Tunnels	200	200	1,500	3,000	3,000	3,000
Client-to-Gateway IPSec VPN Tunnels	200	200	1,500	3,000	3,000	3,000
Unlimited User Licenses	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent Sessions	400,000	400,000	400,000	500,000	500,000	800,000
New Sessions/Second	4K	4K	10K	10K	10K	10K
Number of SSL Users (Recommended)	100	100	200	300	400	500
Policies	2,000	2,000	5,000	5,000	8,000	20,000
Virtual Domains (Max / Default)	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10
*	Antivirus performance is measured based on HTTP traffic with 32Kbyte file attachments and IPS performance is measured base on UDP traffic with 512 byte packet size.					
	Actual performance may vary depends on network traffic and environment					
DIMENSIONS						
Height x Width x Length (in)	1.75 x 16.8 x 10	1.75 x 16.8 x 10	1.75 x 16.8 x 10	1.75 x 17 x 12.6	1.75 x 17 x 12.6	1.75 x 16.75x 12
Height x Width x Length (cm)	4.4 x 42.7 x 25.4	4.4 x 42.7 x 25.4	4.4 x 42.7 x 25.4	4.4 x 43.2 x 32	4.4 x 43.2 x 32	4.4 x 42.7 x 30.5
Weight	7.3 lbs (3.3 kg)	7.3 lbs (3.3 kg)	7.3 lbs (3.3 kg)	11.9 lbs (5.4 kg)	11.9 lbs (5.4 kg)	10 lbs (4.5 kg)
Rack Mountable	Yes	Yes	Yes	Yes	Yes	Yes
AC Power Required	100-240 VAC, 50-60 Hz, 8.0 Amp (Max)					
Power Consumption (Avg)	100W	110W	120W	130W	140W	100W
ENVIRONMENTAL						
Operating temperature	32 to 104 deg F (0 to 40 deg C)					
Storage temperature	-13 to 158 deg F (-25 to 70 deg C)					
Humidity:	5 to 95% non-condensing					
COMPLIANCE	FCC Class A Part 15, UL/CUL, C Tick, CE, VCCI					
CERTIFICATIONS	ICSA Labs: Firewall, IPSec, SSL, Antivirus, IPS					

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 NAT Traversal
 WINS Support
 Customized Protection Profiles

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)

INTRUSION PREVENTION SYSTEM (IPS)

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

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
 MIME Content Header Filtering

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

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

TRAFFIC SHAPING

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

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 with Routing Between Zones
 Route Between Virtual LANs (VDMs)

MANAGEMENT/ADMINISTRATION OPTIONS

Console Interface (RS-232)
 WebUI (HTTP/HTTPS) and Command Line Interface
 Telnet / Secure Command Shell (SSH)
 Role-Based Administration
 Multi-language Support

Multiple Administrators and User Levels
 Upgrades and Changes Via FTP and WebUI
 System Software Rollback
 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

ENDPOINT COMPLIANCE AND CONTROL

Monitor & Control Hosts Running FortiClient Endpoint Security

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

VIRTUAL DOMAINS (VDMs)

Separate Firewall/Routing domains
 Separate Administrative domains
 Separate VLAN interfaces
 10 VDMs (standard)

HIGH AVAILABILITY (HA)

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

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



FortiGate-200A

FortiGate-224B



FortiGate-300A

FortiGate-400A



FortiGate-500A

FortiGate-800

FortiGate-800F

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 and compliance management, application 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 replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 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

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.