

# FortiGate™ -50-100 Series

Remote/Branch Office  
Small-Medium Business  
Customer Premise Equipment

Datasheet

## Unified Threat Management Solutions

### Blended Security Threats Within The Enterprise

Network security violations can be devastating to businesses. Intellectual property, revenue, customer and company records, and other mission critical resources are at risk. As larger companies work to increasingly lock down their networks, more and more security threats are being targeted at smaller companies. Small office/home offices (SOHO) often lack the infrastructure to meet the technical sophistication of today's complex blended-attack methods and remote offices/branch offices (ROBO) often lack the on-site expertise to tackle such complex security issues. Point-based security appliances are inadequately equipped to protect against these types of attacks because of the multitude of attack vectors used. The Fortinet FortiGate series of SOHO and ROBO security appliances tightly integrate multi-threat protection onto a purpose-built platform to effectively block application- and network-borne attacks—attacks that, if successful, can result in lost productivity and lost revenue.

### Cost-Effective Security Platform

The Fortinet FortiGate series of security appliances deliver high performance, multi-threat protection at a compelling cost that is ideal for securing smaller locations. Complete Unified Threat Management (UTM) features including firewall, VPN, intrusion prevention, Web filtering, antispam, antivirus, antispyware, traffic shaping and IM/P2P controls prevent blended attacks or unauthorized use from interrupting business. All FortiGate devices support High Availability (HA) configurations to ensure maximum uptime. FortiGate appliances operate in either transparent or routing modes and are available with integrated multi-port switches and modems, all of which enable FortiGate devices to adapt to any network environment. Moreover, with Fortinet FortiGuard Security Subscription Services, the FortiGate-50 thru -100 Series become an affordable and easy-to-manage security solution for an enterprise's remote/branch offices, a service provider's customer premise equipment (CPE) or as an all-in-one solution for small-to-medium businesses.

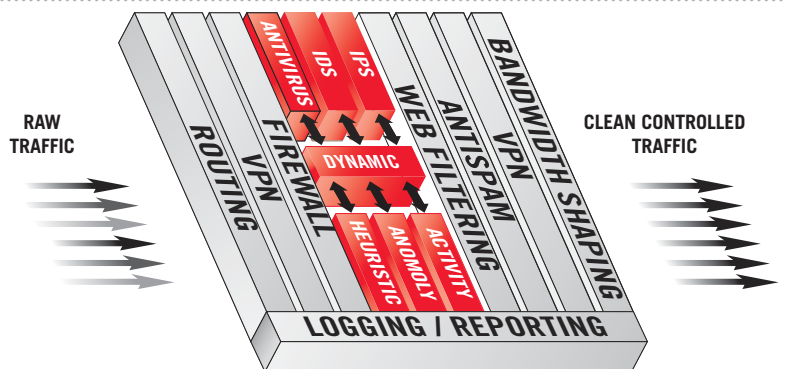


### Key Solution Features and Benefits

<ul style="list-style-type: none"> <li>Industry proven, multi-threat security architecture for small/home offices and remote/branch offices</li> </ul>	Delivers powerful, integrated application security ideal for protecting against today's complex threats
<ul style="list-style-type: none"> <li>Extremely high price/performance ratio with unlimited number of users</li> </ul>	Low total cost of ownership, high performance via custom ASIC, and wide range of deployment options matches complex network security requirements
<ul style="list-style-type: none"> <li>Easy-to-deploy, easy-to-manage appliance form factor</li> </ul>	Allows for rapid deployment to quickly secure SOHO/ROBO office networks
<ul style="list-style-type: none"> <li>Modular software and hardware architecture</li> </ul>	Enables rapid support of new technologies, such as VoIP, IM, and P2P, to be secured without interruptions in service
<ul style="list-style-type: none"> <li>Strong centralized management and analysis with customized and detailed logging and reporting tools</li> </ul>	FortiAnalyzer and FortiManager offer extensive reporting, logging, and data archiving options for regulatory compliance, trending, or baselining

### The FortiGate Multi-Threat Security Inspection Model

Fortinet's award-winning security inspection engines offer unparalleled levels of protection against blended threats. Fully integrated routing, firewall, encryption, intrusion prevention, antivirus, antispam, Web filtering and traffic shaping modules means that all traffic is inspected upon entry into and exit from your network to ensure that communication is clean and controlled.



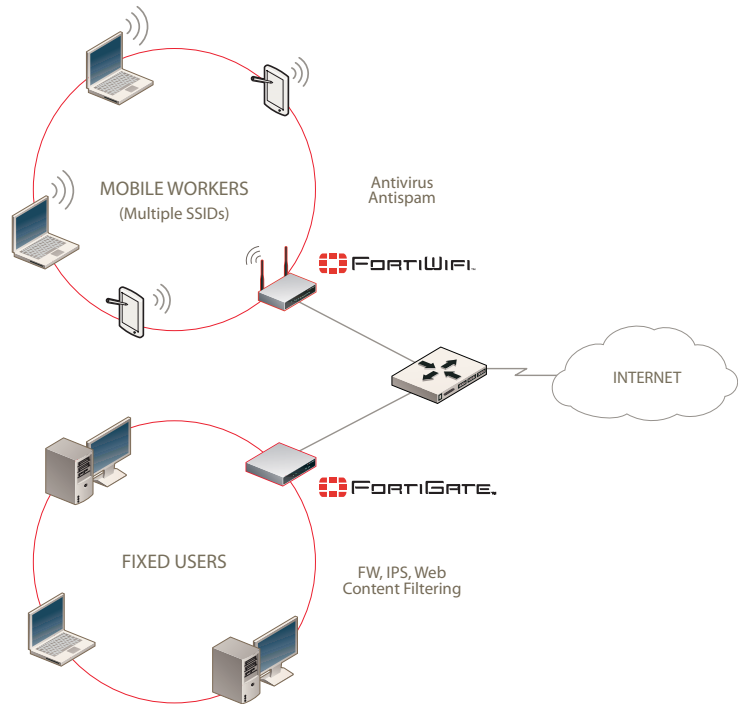
FortiGate Multi-Threat Security Illustrated

**The complete line of Fortinet SOHO and ROBO solutions are designed to secure business networks.**

**Next-Generation SOHO/ROBO Security**

Antivirus + Antispam + Firewall + Intrusion Prevention System + Web Content Filtering

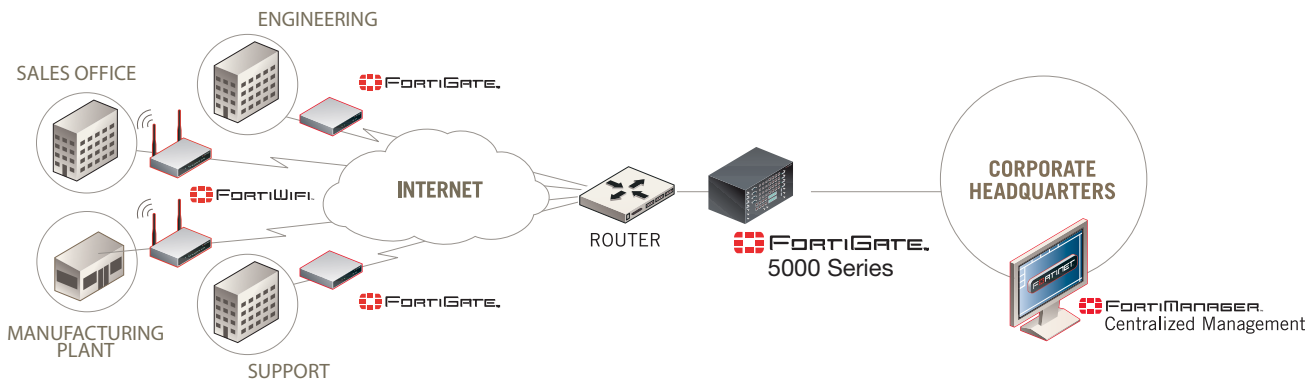
Through the integration of essential security technologies, Fortinet protects both mobile workers and workstations at SOHO and ROBO locations. The FortiWifi series offers the ability to broadcast multiple SSIDs (Service Set Identifiers), maximizing infrastructure flexibility in multi-provider environments and conserving spectrum. Moreover, different security policies can be set for each SSID, increasing security flexibility. To keep resources safe, Fortinet’s advanced antivirus, antispyware, antispam, and intrusion prevention systems utilize a combination of signature and heuristic detection engines to provide multi-layered, real-time protection against a multitude of attacks before they can enter a network gateway. High performance is achieved and maintained through the use of the integrated FortiASIC processor.



**Enterprise ROBO Deployment**

Firewall + VPN + Secure Messaging (Email, IM & P2P security)

Businesses now operate without extensive boundaries. Workers at various remote offices are tasked with vastly different business processes: some use messaging applications while others use database applications. Both are equally protected using Fortinet security solutions. Sales offices that use email and IM applications are protected from blended threats that use multiple methods to attack a system: viruses that spawn dormant Trojans, rootkits, and bots, for example. Combining Fortinet’s antivirus and antispam technology with IM and P2P controls, employees are assured that email and IM messaging remain secure and won’t result in lost revenue or lost data. Application and database users, such as a remote manufacturing site, are guaranteed secure connectivity—via firewalls and VPNs—to the application servers it uses at the central office. Finally, Fortinet offers a complete management solution for centralized monitoring, reporting, logging, and analysis to ensure that remote offices remain up and running.



**Managed Security Service Provider Customer Premise Equipment Deployment**

Firewall + Intrusion Prevention + Antivirus + Web Content Filtering

Managed Security Service Providers (MSSPs) can distribute FortiGate appliances throughout their Customer Premise Equipment (CPE) deployments because of the wide array of connectivity options and the modular security architecture. Different customers can be protected in different ways, according to their needs. For example, one set of customers can be protected with a firewall and intrusion prevention system, while another can be protected with a firewall and web content filtering. MSSPs can centrally monitor and manage all customers using FortiManager and FortiAnalyzer for end-to-end reporting, logging, and even forensic analysis of security events.

## Fortinet Unified Security Solutions

- 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, antispam, web content filtering, and antispam
- Automated updates of antivirus/antispam 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 FortiOS is ICSA Labs-certified and offers a comprehensive command-line interface

### Technical Specifications



HARDWARE SPECIFICATIONS	FortiGate-50B	FortiWiFi-50B	FortiGate-60B	FortiWiFi-60B	FortiGate-60ADSL	FortiGate-100A
LAN Switching						
Interfaces	3	3	6	6	4	4
WAN Interfaces	2	2	2	2	2	2
DMZ Interfaces			1	1	1	2
Analog Modem			Yes	Yes		
ADSL Interface					Annex A	
Wireless LAN						
802.11a/b/g		802.11 b/g		802.11 a/b/g		
USB Ports	2	2	2	2	2	2
Power Over Ethernet (PoE)		Yes				
PC Card Slot*			Yes	Yes		
Supported VDoms	10	10	10	10	10	10
* PC card is sold separately						
<b>SYSTEM PERFORMANCE</b>						
Firewall/VPN 3DES	50/48 Mbps	50/48 Mbps	100/64 Mbps	100/64 Mbps	70/20 Mbps	100/40 Mbps
Concurrent sessions	25,000	25,000	70,000	70,000	50,000	200,000
New Sessions/Second	2,000	2,000	3,000	3,000	2,000	4,000
Site-to-Site IPSec VPN						
Tunnels	20	20	50	50	50	80
Antivirus Throughput	19 Mbps	19 Mbps	20 Mbps	20 Mbps	15 Mbps	20 Mbps
<b>DIMENSIONS</b>						
(H, W, L, weight)	1.38 inches	1.38 inches	1.75 inches	1.75 inches	1.75 inches	1.75 inches
	8.63 inches	8.63 inches	10.87 inches	10.87 inches	10.87 inches	10.87 inches
	5.8 inches	5.8 inches	6.13 inches	6.13 inches	6.13 inches	6.13 inches
	1.5 lbs (0.68 kg)	1.5 lbs (0.68 kg)	5.5 lbs (2.5 kg)	5.5 lbs (2.5 kg)	3.35 lbs (1.5 kg)	1.5 lbs (0.68 kg)
<b>POWER CONSUMPTION (AVG)</b>						
	6W	6W	15W	15W	12W	14W
<b>COMPLIANCE</b>						
	FCC Class A (FG-100A), FCC Class B (FG-50-60), Part 15, UL/CUL, C Tick, CE, VCCI					
<b>AC POWER REQUIRED</b>						
	100-240 VAC, 50-60 Hz, 0.8 Amp (Max)					
<b>CERTIFICATIONS</b>						
	ICSA Labs Certified: Firewall, Antivirus, IPS, IPSec VPN, SSL-VPN NSS Labs Approved (UTM), Common Criteria (EAL 4+), FIPS 140-2 (Please contact your Fortinet Sales Representative for a complete list of product certifications)					
<b>ENVIRONMENTAL</b>						
	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					

#### The Fortinet ASIC-based Advantage

The FortiASIC family of content processors (CP) and network processors (NP) form the foundation of Fortinet's unique technology. FortiASIC-CP series use an intelligent, proprietary content scanning engine that accelerates the compute-intensive actions which generally perform slowly on general purpose processors. They also contain acceleration algorithms for encryption so that FortiGate can perform antivirus scanning on VPN tunnels ensuring clean and controlled communications. FortiASIC-NP series use proprietary network processor acceleration, delivering extreme performance and security at a compelling total cost of ownership.

#### The Complete FortiGate Solution

Fortinet's multi-threat security solutions include an integrated, all-in-one security appliance and optional FortiCare™ Support and FortiGuard™ Security Subscription Services. These offerings include everything from technical support, security content updates, hardware warranty and hardware exchange service to ensure that your investment remains current and your corporate resources are protected against the latest blended threats.

## Technical Specifications



FortiGate-50B

FortiWiFi-50B

FortiGate-60B

FortiWiFi-60B

FortiGate-60ADSL

FortiGate-100A

### All FortiGate solutions offer the following features:

#### 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 & SSL)  
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

#### 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/SMT/POP3/IMAP/FTP/IM and Encrypted VPN Tunnels  
Automatic "Push" Virus Database Update  
File Quarantine Support  
Block by File Size or Type

#### WEB FILTERING

URL/Keyword/Phrase Block  
URL Exempt List  
Content Profiles  
Blocks Java Applet, Cookies, Active X  
FortiGuard Web Filtering Support

#### ANTISPAM

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

#### 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  
Route Between Zones  
Route Between Virtual LANs (VDOMS)  
Multi-Link Aggregation (802.3ad)

#### 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 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

#### 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 (VDOMS)

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

#### HIGH AVAILABILITY (HA)

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

#### INSTANT MESSENGER / PEER-TO-PEER ACCESS CONTROL

AOL-IM	Yahoo	MSN
ICQ	Gnutella	BitTorrent
WinNY	Skype	eDonkey
KaZaa		

### FortiGuard Security Subscription Services

Includes:

- Automatic push updates from the FortiGuard Network for antivirus and intrusion prevention security content.
- Complete Wildlist virus protection from over 4,500 active malware threats from FortiGuard's database of over 60,000 malware threats.
- 76 rated Web categories for greater control and accuracy.
- Web filtering for more than 29 million rated domains and 2 billion rated Web pages.
- Real time spam queries to ensure accurate filtering of unsolicited bulk mail.

### FortiCare Support Services

Includes:

- 24/7/365 FortiCare Web-based support
- 1-Year limited hardware warranty
- Technical account management service available
- 8x5 telephone-based technical support (24x7 - optional)
- 90-day limited software warranty
- Professional services available



# 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](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-HONG KONG

Fortinet Incorporated  
Room 2429-2431, 244F Sun Hung Kai Centre  
No.30 Harbour Road, WanChai, Hong Kong  
Tel +852-3171-3000  
Fax +852-3171-3008