

# FortiGate™ -50-100 Series

Remote/Branch Office  
Small-Medium Business  
Customer Premise Equipment

Datasheet

## Unified Threat Management Solutions

### Blended Security Threats Within Small Businesses and Enterprises

Cyber crime and network attacks pose serious threats to small 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.

### Cost-Effective Security Platform

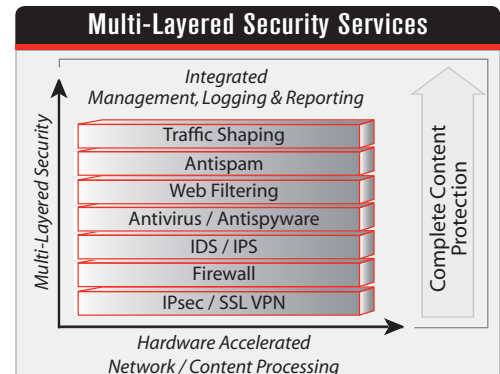
The Fortinet FortiGate series of security appliances deliver high performance, multi-threat protection at a compelling cost that is ideal for securing smaller locations. Complete Unified Threat Management (UTM) features including firewall, VPN, intrusion prevention, Web filtering, antispam, antivirus, 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, integrated WiFi access points and PC Card slots for 3G/UMTS 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 Problems	Solutions
<ul style="list-style-type: none"> <li>Small Offices and Home Offices (SOHO) are particularly vulnerable to cyber attacks due to the lack of resources and budgets to combat complex network and content based threats</li> </ul>	All-in-one Unified Threat Management (UTM) system provides multi-layer threat protection with automatic updates all in a cost-effective package
<ul style="list-style-type: none"> <li>Deploying multiple point-products from different vendors does not provide integrated protection from blended threats and is costly to own and complex to maintain</li> </ul>	UTM security solutions provide tightly integrated protection services with a unified management, logging and reporting interface
<ul style="list-style-type: none"> <li>Adoption of WiFi wireless technology opens another window for attack from inside of the network</li> </ul>	Built-in WiFi wireless ensures the same level of protection across both wired and wireless networks
<ul style="list-style-type: none"> <li>SOX and PCI compliance requirements adds a new dimension of complexity to logging and reporting</li> </ul>	Unified tools with a common user interface simplify analyzing, reporting and managing compliance



### Fortinet's Multi-Layered Security Solution

Fortinet's multi-layered security solutions efficiently and economically provide an integrated set of security services in a single, easy-to-manage high-performance appliance that is capable of supporting a wide range of deployment scenarios. In addition, FortiGuard Subscription Services include everything from technical support, antivirus updates, antispyware, antispam, and Web content filtering to ensure that your security environment remains current and your corporate resources are protected against the latest blended threats. FortiGate systems come with a one-year limited hardware warranty and 90-day limited software warranty.

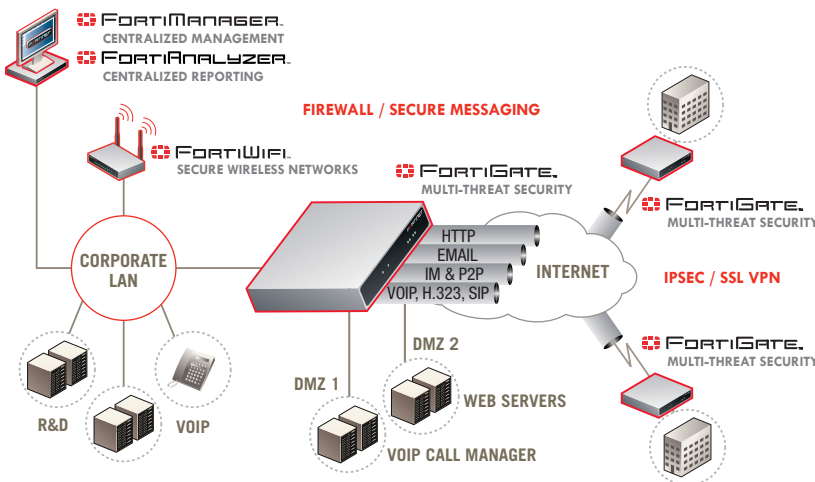
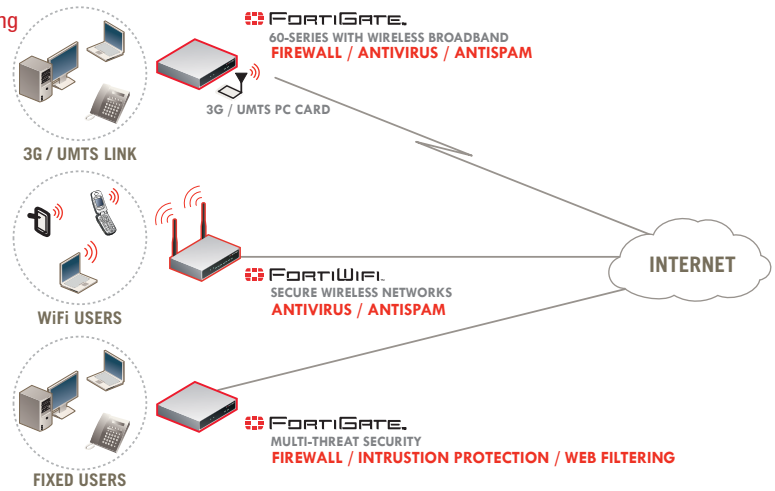


## FortiGate 50-100 series appliances are designed to secure small size offices and businesses.

### Secure Wired and Wireless Gateways for Small Business

Firewall + Antivirus + Antispam + Intrusion Prevention + Web Filtering

Through the integration of essential security technologies, Fortinet protects both mobile workers and workstations at SOHO and ROBO locations. To keep resources safe, Fortinet's advanced antivirus, antispam, and intrusion prevention systems utilize the integrated FortiASIC processor and a combination of signature and heuristic detection engines to provide multi-layered, real-time protection against a multitude of attacks. 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. FortiGate 60-series models provide a PC card slot that allows a 3G/UMTS PC card to be used for secure network connectivity.



### Enterprise ROBO Deployment

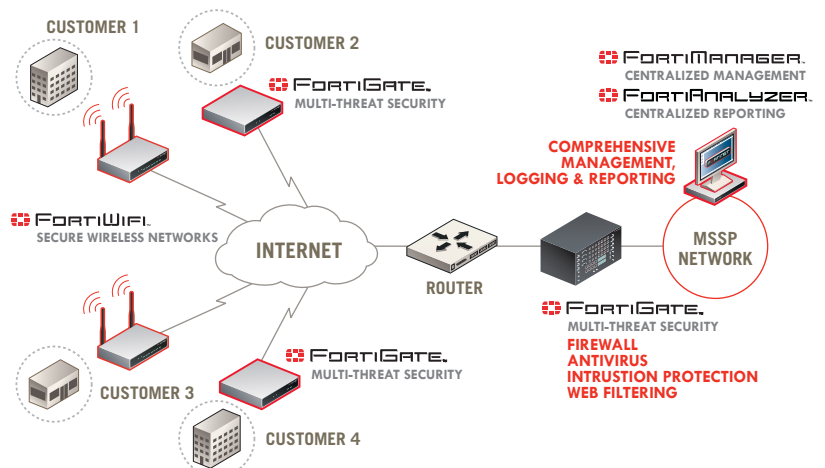
Firewall + VPN + Secure Messaging (Email, IM and P2P)

Workers at various remote offices are tasked with vastly different business processes: some use messaging applications while others use database applications. 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 Deployment

Firewall + Antivirus + Intrusion Prevention + Web 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.



## Technical Specifications



HARDWARE SPECIFICATIONS	FortiGate-50B	FortiWiFi-50B	FortiGate-60B	FortiWiFi-60B	FortiGate-100A
LAN Switching Interfaces	3	3	6	6	4
WAN Interfaces	2	2	2	2	2
DMZ Interfaces			1	1	2
Analog Modem			Yes	Yes	
Wireless LAN 802.11a/b/g		802.11 b/g		802.11 a/b/g	
USB Ports	2	2	2	2	2
Power Over Ethernet (PoE)		Yes			
PC Card Slot*			Yes	Yes	
Supported VDOMs	10	10	10	10	10
* PC card is sold separately					
<b>SYSTEM PERFORMANCE *</b>					
Firewall Throughput	50 Mbps	50 Mbps	100 Mbps	100 Mbps	100 Mbps
VPN 3DES Throughput	48 Mbps	48 Mbps	64 Mbps	64 Mbps	40 Mbps
Antivirus Throughput	19 Mbps	19 Mbps	20 Mbps	20 Mbps	20 Mbps
IPS Throughput	30 Mbps	30 Mbps	60 Mbps	60 Mbps	70 Mbps
Dedicated IPsec VPN Tunnels	20	20	50	50	80
Unlimited User Licenses	Yes	Yes	Yes	Yes	Yes
Concurrent sessions	25,000	25,000	70,000	70,000	200,000
New Sessions/Second	2,000	2,000	3,000	3,000	4,000
Policies	2,000	2,000	2,000	2,000	2,000
* 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					
<b>DIMENSIONS</b> (H, W, L, weight)	1.38 inches 8.63 inches 5.8 inches 1.5 lbs	1.38 inches 8.63 inches 5.8 inches 1.5 lbs	1.75 inches 10.87 inches 6.13 inches 5.5 lbs	1.75 inches 10.87 inches 6.13 inches 5.5 lbs	1.75 inches 10.87 inches 6.13 inches 3.35 lbs
<b>AC POWER REQUIRED</b>	100-240 VAC, 50-60 Hz, 8.0 Amp (Max)				
<b>POWER CONSUMPTION (AVG)</b>	6W	6W	15W	15W	14W
<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				
<b>COMPLIANCE</b>	FCC Class A Part 15 (FG-100A), FCC Class B Part 15 (FG-50-60), UL/CUL, C Tick, CE, VCCI				
<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)				

### 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

### Fortinet's ASIC-Based Advantage

FortiASIC is the foundation of Fortinet's unique hardware technology. FortiASIC is a family of purpose built, high-performance network and content processors that uses an intelligent proprietary content scanning engine and multiple algorithms to accelerate compute-intensive security services. FortiASIC provides the performance required to deliver enterprise and carriers-class UTM services. Coupled with the FortiOS security hardened Operating System, FortiASIC delivers extreme performance and security.

### FortiOS: Developed for Security

FortiOS is the software foundation of FortiGate multi-threat security platforms. Developed solely for security, performance and reliability, it is a purpose-built operating system that leverages power of the the FortiASIC content and network processors. FortiOS enables a comprehensive suite of security services – content inspection firewall, IPS, antivirus, web filtering, antispam, IM/P2P, virtual network security and bandwidth shaping. FortiOS is a complete suite of UTM security services and is certified for Common Criteria EAL 4+.

## FortiGate-50-100 Series



### FortiGate-50-100-series platforms provide the following security 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/SMTP/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 with Routing Between Zones  
Route Between Virtual LANs (VDOMS)

#### 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

#### 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

With FortiGuard™ Security Subscription services enabled, customers can rest assured that their Fortinet security platforms are performing optimally and protecting their corporate assets with the latest security intelligence. FortiGuard services deliver the latest security content directly to Fortinet products. Fortinet offers four standard subscription services: Antivirus, Intrusion Prevention, Web Filtering and Antispam services to protect against multiple types of new and emerging threats. FortiGuard services are updated by the Fortinet Global Threat Research Team, a team of experts working around the clock and around the world to keep Fortinet customers secure. The Fortinet Global Threat Research Team enables Fortinet to deliver comprehensive multi-threat protection, including zero-day protection from new and emerging threats. The FortiGuard Network is a network of global data centers that automatically deliver updates quickly and reliably to Fortinet products.

For customers requiring guaranteed response time to suspicious malware threats, Fortinet offers a premier version of the FortiGuard Antivirus Security Subscription service. Along with Service Level Agreements (SLAs), the premier service provides the customer with a direct conduit to the Fortinet Global Threat Research Team.

Fortinet also offers a premier version of the FortiGuard Web Filtering Security Subscription service. This higher-tier service offering includes guaranteed SLAs and a larger quota for rating URLs submitted to the Fortinet Global Threat Research Team.

### FortiCare Support Services

Includes:

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