DATASHEET

FortiGate®/FortiWiFi™-60C

Integrated Threat Management for Front Line Locations

Enterprise-Class Protection for Remote Offices, Retail, and Customer Premise Equipment

The FortiGate-60C and FortiWiFi-60C multi-threat security platforms deliver comprehensive enterprise-class protection for smaller locations at an affordable price. The FortiGate/FortiWiFi-60 series platforms make it easy for you to protect your smaller locations, branch offices, customer premise equipment (CPE) and retail networks. With the FortiGate platforms' integrated set of essential security technologies, you can deploy a single device that protects all of your applications and data. The simple per-device pricing, integrated management console, and remote management capabilities significantly reduce your costs associated with deploying and managing complete protection.

Comprehensive Protection and Optional Wireless

The FortiGate multi-threat security platforms deliver an unmatched range of security technologies. They integrate firewall, IPSec and SSL VPN, antivirus, antispam, intrusion prevention, and web filtering into a single device at a single price. They also include data loss prevention (DLP), application control, and endpoint NAC. In addition, Fortinet's FortiGuard® Labs is on duty around the clock and around the world, looking for any changes in the threat landscape. FortiGuard Labs deliver dynamic threat updates to protect your network against emerging threats.

The FortiWiFi-60C gives you the convenience of wireless while delivering the protection and performance you need. Its dual-band capability and support for 802.11a/b/g/n standards ensures compatibility with your existing infrastructure. The FortiWiFi-60C's multiple SSID feature support multiple wireless access networks, enabling unencrypted guest or contractor access to the Internet while keeping corporate network access limited and secure.

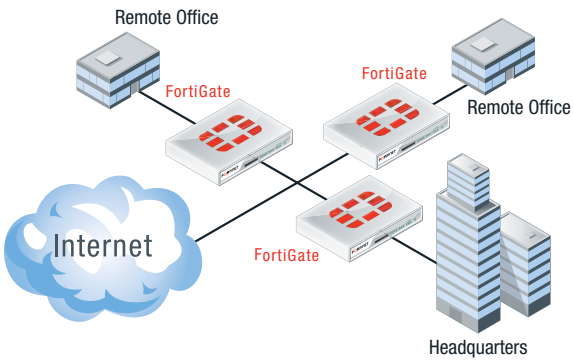
Purpose-Built Performance and Reliability

Fortinet's purpose-built hardware and software prevent your network security from becoming your network bottleneck. The FortiASIC processors maximize throughput while preventing unauthorized access and eliminating unwanted traffic from your network. The purpose-built FortiOS operating system minimizes delays in processing your data while efficiently enforcing your policies.

FortiGate/FortiWifi-60C Benefits

The FortiGate product family provides cost-effective, comprehensive protection against network, content, and application-level threats. In addition, FortiGate/FortiWiFi-60C platforms offer these benefits:

- Segment internal traffic and provide full security for perimeter-bound traffic with gigabit firewall throughput combined with switched internal ports and dedicated WAN ports
- Upgradeable SDHC storage for local log records and graphical reports
- Optional WAN optimization and web caching features for improved network performance
- Deploy secure networks quickly and easily with support for ExpressCard and USB-based wireless broadband
- Simplify configuration and deployment with the FortiExplorer setup utility



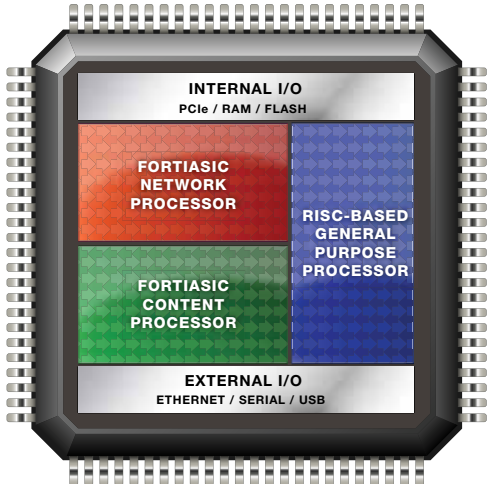
FORTIGATE IN THE DISTRIBUTED ENTERPRISE

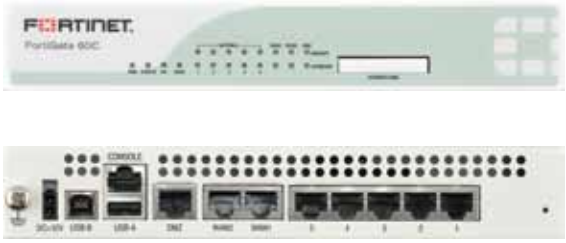
Industry Certification

ICSA labs CERTIFIED IPSEC-BASIC
ICSA labs CERTIFIED FIREWALL-CORPORATE
ICSA labs CERTIFIED NETWORK IPS
ICSA labs CERTIFIED ANTI-VIRUS
ICSA labs CERTIFIED SSL VPN

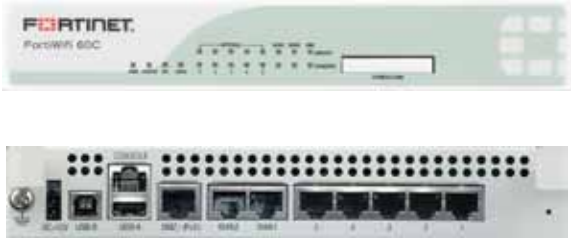
The Fortinet FS1 System-on-a-Chip

Fortinet has integrated FortiASIC acceleration logic together with a RISC-based main processor and other system components to form the FS1 SoC. The advantage that this design offers, in addition to simplifying the appliance design, is that it allows FortiGate appliances which use the FS1 SoC to deliver very impressive performance numbers for smaller networks.





FortiGate-60C



FortiWiFi-60C

(Wireless antennas not shown)

FortiGuard and FortiCare Services

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, application control, vulnerability and compliance management, and database security services.

For more information about FortiGuard Services, please visit www.fortiguard.com.

FortiGuard Subscription Services						
Product	**Antivirus**	**Intrusion Prevention**	**Web Filtering**	**Antispam**	**Application Control**	**Vulnerability & Compliance**
FortiGate-60C	Supported	Supported	Supported	Supported	Supported	Supported
FortiWiFi-60C	Supported	Supported	Supported	Supported	Supported	Supported

FortiCare™ Support Services offerings provide global support for all Fortinet products and services. Customer satisfaction and responsiveness is Fortinet's number one priority. With FortiCare support, customers can be assured that their Fortinet security products are performing optimally and protecting their corporate assets with the best security technology at the best possible price.

Fortinet offers end-users multiple options for FortiCare contracts so that they can obtain the right level of support for their organization's needs. Attractively priced options include 24x7 support with advanced hardware replacement, 8x5 support with enhanced Web features, Premium Support with technical account management, and Premium RMA support with enhanced service levels.

Additionally, Fortinet Professional Services can be engaged for projects with critical deadlines projects that are large in scope, or initial deployments.

FortiOS 4.0 Software—Raising The Bar

FortiOS 4.0: Redefining Network Security

FortiOS 4.0 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 the power of FortiASIC processors. FortiOS software enables a comprehensive suite of security services: Firewall, VPN, intrusion prevention, antivirus/antispyware, antispam, web filtering, application control, data loss prevention, and end point network access control.

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 carrier-class UTM services. Coupled with the FortiOS security hardened Operating System, FortiASIC delivers extreme performance and security.

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)
- 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 Certvified (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)

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)

USER AUTHENTICATION OPTIONS
- Local Database
- Windows Active Directory (AD) Integration
- External RADIUS/LDAP Integration
- Xauth over RADIUS for IPSEC VPN
- RSA SecurID Support
- LDAP Group Support

DATA CENTER OPTIMIZATION
- Web Server Caching
- TCP Multiplexing
- HTTPS Offloading

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
- File Quarantine Support
- IPv6 Support

WEB FILTERING
- 76 Unique Categories
- 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

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

VIRTUAL DOMAINS (VDOMs)
- Separate Firewall/Routing Domains
- Separate Administrative Domains
- Separate VLAN Interfaces
- 10 VDOM License Standard, Upgradable to More

TRAFFIC SHAPING
- Policy-based Traffic Shaping
- Differentiated Services (DiffServ) Support
- Guarantee/Max/Priority Bandwidth
- Shaping via Accounting, Traffic Quotas, and Per-IP

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

MANAGEMENT/ADMINISTRATION
- 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
- Optional FortiManager Central Management

LOGGING/MONITORING
- Local Event 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 / Reporting
- Optional FortiGuard Analysis and Management Service

Firewall

Fortinet firewall technology delivers industry-leading performance for network and application firewalling including Web 2.0 application policies based on the application identity, up to and beyond 10 Gbps throughput. Our technology identifies traffic patterns and links them to the use of specific applications, such as instant messaging and peer-to-peer applications, permitting application access control. By coupling application intelligence with firewall technology, the FortiGate platform is able to deliver real-time security with integrated application content level inspection, thereby simplifying security deployments.

Firewall	
Highlights	NAT, PAT and Transparement (Bridge)
	Policy-Based NAT
	SIP/H.323/SCCP NAT Traversal
	VLAN Tagging (802.1Q)
	IPv6 Support

Performance	
Model	FortiGate-60C / FortiWiFi-60C
Firewall (1518 Byte)	1 Gbps
Firewall (512 Byte)	1 Gbps

Intrusion Prevention

IPS technology provides protection against current and emerging network level threats. In addition to signature-based detection, we perform anomaly-based detection whereby our system alerts users to traffic that fits a profile matching attack behavior. This behavior is then analyzed by our threat research team to identify threats as they emerge and generate new signatures that will be incorporated into our FortiGuard services.

Intrusion Prevention System	
Features Supported	Automatic Attack Database Update
	Protocol Anomaly Support
	IPS and DoS Prevention Sensor
	Custom Signature Support
	IPv6 Support

Performance	
Model	FortiGate-60C / FortiWiFi-60C
IPS Throughput	60 Mbps

Antivirus / Antispyware

Antivirus content inspection technology provides protection against virus, spyware, worms, phishing and other forms of malware being transmitted over the network infrastructure. By intercepting application content in transit, and reassembling the data into user expected content, the FortiGate Antivirus features ensures that malicious threats hidden within legitimate application content is identified and removed from the data stream destined for internal (or external) recipients. The addition of Fortinet's FortiGuard subscription services ensured each FortiGate has access to updated malware signatures, resulting in high level of accuracy and detection capabilities including emerging and newly discovered viruses. ICSA Labs has certified our antivirus functionality.

Antivirus	
Features Supported	Proxy Antirus
	Flow-based Antirus
	File Quarantine
	IPv6 Support

Performance	
Model	FortiGate-60C / FortiWiFi-60C
Antivurs	20 Mbps

VPN

Fortinet VPN technology provides secure communications between multiple networks and hosts, through both secure socket layer, or SSL, and IPsec VPN technologies, leveraging our custom FortiASIC to provide hardware acceleration for high-performance communications and data privacy. Benefits include the ability to enforce complete content inspection and multi-threat security as part of VPN communications, including antivirus, Intrusion Prevention System, or IPS, and Web filtering. Additional features include traffic optimization providing prioritization for traffic across VPNs.

VPN	
Hightlights	IPSec and SSL VPN
	DES, 3DES, AES and SHA-1/MD5 Authentication
	PPTP, L2TP, VPN Client Pass Through
	SSL Single Sign-On Bookmarks
	Two-Factor Authentication

Performance	
Model	FortiGate-60C / FortiWiFi-60C
IPSec VPN	70 Mbps
Recommend # of SSL Users	60

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.

WAN Optimization	
Model Supported	FortiGate 60C / FortiWiFi-60C with optional 16GB SD Card
Highlights	Gateway-to-Gateway Optimization
	Bi-directional Gateway-to-client Optimization
	Web Caching
	Secure Tunnel
	Transparent Mode

SSL Inspection

SSL-Encrypted Traffic Inspection protects clients and web and application servers from malicious SSL-encrypted traffic, to which many security devices are 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 threats within encrypted traffic flows.

SSL Inspection	
Highlights	Protocol: HTTPS, SMTPS, POP3S, IMAPS
	Inspection support: Antivirus, Web Filtering, Antispam, Data Loss Prevention
	SSL Offload

End-Point 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.

Endpoint Network Access Control (NAC)	
Highlights	Monitor & Control Hosts Running FortiClient
	Vulnerability Scanning of Network Nodes
	Quarantine Portal
	Application Detection and Control
	Built-in Application Database

Data Loss Prevention

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.

Data Loss Prevention (DLP)	
Highlights	Identification And Control Over Data in Motion
	Built-in Pattern Database
	RegEx Based Matching Engine
	Common File Format Inspection
	International Character Sets Supported

Web Filtering

Web filtering technology is a pro-active defense feature that identifies known locations of malware and blocks access to these malicious sources. In addition, the technology enables administrators to enforce policies based on website content categories ensuring users are not accessing content that is inappropriate for their work environment. The technology restricts access to denied categories based on the policy by comparing each Web address request to a Fortinet hosted database.

Web Filtering	
Highlights	HTTP/HTTPS Filtering
	URL / Keyword / Phrase Block
	Blocks Java Applet, Cookies or Active X
	MIME Content Header Filtering
	IPv6 Support

Logging, Reporting & Monitoring

FortiGate units provide extensive logging capabilities for traffic, system, and network protection functions. They also allow you to compile reports from the detailed log information gathered. Reports provide historical and current analysis of network activity to help identify security issues that will reduce and prevent network misuse and abuse.

Logging and Monitoring	
Highlights	Internal Log storage and Report Generation
	Graphical Real-Time and Historical Monitoring
	Graphical Report Scheduling Support
	Optional FortiAnalyzer Logging (including per VDOM)
	Optional FortiGuard Analysis and Management Service

Virtual Domains

Virtual Domains (VDOMs) enable a single FortiGate system to function as multiple independent virtual FortiGate systems. Each VDOM contains its own virtual interfaces, security profiles, routing table, administration, and many other features. FortiGate VDOMs reduce the complexity in physical network by virtualizing different security resources over a common platform, greatly reducing the power and footprint required by multiple point solutions.

Virtual Domains	
Features Highlight	Separate Firewall / Routing Domains
	Separate Administrative Domains
	Separate VLAN Interfaces
VDOMs (Max / Default)	10 / 10

High Availability

High Availability (HA) configurations enhance reliability and increase performance by clustering multiple FortiGate appliances into a single entity. FortiGate High Availability supports Active-Active and Active-Passive options to provide maximum flexibility for utilizing each member within the HA cluster. The HA feature is included as part of the FortiOS operation system and is available with almost every FortiGate model.

High Availability (HA)	
Highlights	Active-Active and Active-Passive
	Stateful Failover (FW and VPN)
	Link State Monitor and Failover
	Device Failure Detection and Notification
	Server Load Balancing

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.

Application Control	
Highlights	Identify and Control Over 1000 Applications
	Traffic Shaping (Per Application)
	Control Popular IM/P2P Apps Regardless of Port / Protocol
	Popular Applications include: AOL-IM Yahoo MSN KaZaa ICQ Gnutella BitTorrent MySpace WinNY Skype eDonkey Facebook and more

Wireless Controller

The Wireless controller integrated into every FortiGate platform centralizes the management and monitoring of all FortiAP secure access points. All wireless traffic is directed to the FortiGate multi-threat security platform and undergoes identity-aware firewall policies and UTM engine inspection, with only authorized wireless traffic being forwarded. From a single console you can control network access, update policies quickly and easily, and monitor compliance.

Wireless Controller	
Highlights	Managed and Monitor FortiAP product
	Rogue AP Detection, Control and Reporting
	Virtual AP with different SSID

Setup / Configuration Options

Fortinet provides administrators with a variety of methods for configuring FortiGate appliances for initial deployment. The newest method of configuration for FortiGate-60 series uses the FortiExplorer setup wizard over a USB connection to your PC. The wizard guides users through the minimal setup required to get the FortiGate device deployed quickly and easily.

Setup / Configuration Options	
Highlights	FortiExplorer Setup Wizard over USB (FG-60C/FWF-60C Only)
	Web-based User Interface
	Command Line Interface (CLI) over serial connection
	Pre-Configured settings from USB drive

FortiGate-60 Series Specification Summary

Technical Specifications	FortiGate-60C	FortiWiFi-60C
Hardware Specifications		
10/100/1000 Internal Switch Interfaces (Copper, RJ-45)	5	5
10/100 WAN Interfaces (Copper, RJ-45)	2	2
10/100 DMZ Interfaces (Copper, RJ-45)	1	1
Console (Copper, RJ-45)	1	1
USB Interfaces	2 (1 Type-A, 1 Type-B)	2 (1 Type-A, 1 Type-B)
ExpressCard Slot	1	1
SDHC Slot	1 (4 GB SDHC Included / Max 32 GB)	1 (4 GB SDHC Included / Max 32 GB)
Wireless Standards Supported	N/A	802.11 a/b/g/n
Power-over-Ethernet (PoE) Support	No	Yes
System Performance		
Firewall Throughput (1518 byte UDP packets)	1 Gbps	
Firewall Throughput (512 byte UDP packets)	1 Gbps	
IPSec VPN Throughput	70 Mbps	
IPS Throughput	60 Mbps	
Antivirus Throughput (Proxy)	20 Mbps	
Gateway-to-Gateway IPSec VPN Tunnels (System/VDOM)	500/50	
Client-to-Gateway IPSec VPN Tunnels	300	
Concurrent Sessions	80,000	
New Sessions/Sec	3,000	
Concurrent SSL VPN Users (Recommended Max)	60	
Firewall Policies (System/VDOM)	5,000/500	
Virtual Domains (Max / Default)	10 / 10	
Unlimited User Licenses	Yes	
Dimensions		
Height x Width x Length (in)	1.44 x 8.5 x 5.81 in	
Height x Width x Length (cm)	3.66 x 21.592 x 14.76 cm	
Weight	1.9 lbs (.86 kg)	2.1 lbs (.95 kg)
Wall Mountable	Yes	
Environment		
Power Required	100-240 VAC, 50-60 Hz, 1.5 Amp max	
Power Consumption (AVG)	15.7W	19W
Heat Dissipation	53.6 BTU	64.8 BTU
Operating Temperature	32 – 104 deg F (0 – 40 deg C)	
Storage Temperature	-13 to 158 deg F (-25 to 70 deg C)	
Humidity	5 to 95% non-condensing	
Compliance & Certification		
Compliance	FCC Part 15, UL/CUL, C Tick, CE, VCCI	
Certification	ICSA Labs: Firewall, Antivirus, IPSec VPN, SSL VPN, Intrusion Prevention	

Antivirus performance is measured based on HTTP traffic with 32 Kbyte file attachments and IPS performance is measured based on UDP traffic with 512 byte packet size. Actual performance may vary depending on network traffic and environments.

Ordering Information

SKU	Description
FG-60C	Dual 10/100 WAN ports, 10/100 DMZ port, 5-port 10/100/1000 internal switch, SD slot (SDHC), 2 USB, and ExpressCard slot, includes 4GB SDHC card
FWF-60C	Wireless (802.11a/b/g/n), Dual 10/100 WAN ports, 10/100 DMZ port, 5-port 10/100/1000 internal switch, SD slot (SDHC), 2 USB, and ExpressCard slot, includes 4GB SDHC card and PoE support
FG-60C-BDL	FortiGate-60C, 1 Yr. FortiGuard Standard Security Services (AV/IPS/WF/AS), 1 Yr. 8x5 Enhanced FortiCare support, return/replace, firmware upgrades
FWF-60C-BDL	FortiWiFi-60C, 1 Yr. FortiGuard Standard Security Services (AV/IPS/WF/AS), 1 Yr. 8x5 Enhanced FortiCare support, return/replace, firmware upgrades

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

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