



FortiGate®-80 Series

Affordable, Enterprise-Class Protection

Proven Security for Remote Offices, Retail, and Customer Premise Equipment

The FortiGate-80 Series multi-threat security platforms deliver comprehensive enterprise-class protection at a low price. The FortiGate-80 Series platforms make it easy and affordable for you to protect your remote 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

Fortinet's market-leading security technology and research provide unmatched protection against today's sophisticated multi-vector threats. 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.

The FortiGate-80 Series specifically address many policy enforcement requirements included in government or industry regulations, such as the PCI Data Security Standard. They also support migration to new industry standards such as IPv6, supporting dynamic routing or both IPv4 and IPv6 networks. In addition, Fortinet's Global Threat Research Team and ICSA Labs-certified inspection engines ensure that you have the best possible protection in your network.

DATASHEET



Primary Features & Benefits

Enterprise-grade protection for smaller networks

- Enables smaller environments to deploy FortiGate's unmatched protection and performance at an affordable price

Redundant connectivity methods

- Dual 10/100/1000 Ethernet, dial modem (FG-80CM model), and optional 3G wireless offer redundant WAN connections to ensure availability of data

Centralized Management

- FortiManager and FortiAnalyzer centralized management and reporting appliances simplify the deployment, monitoring, and maintenance of the security infrastructure

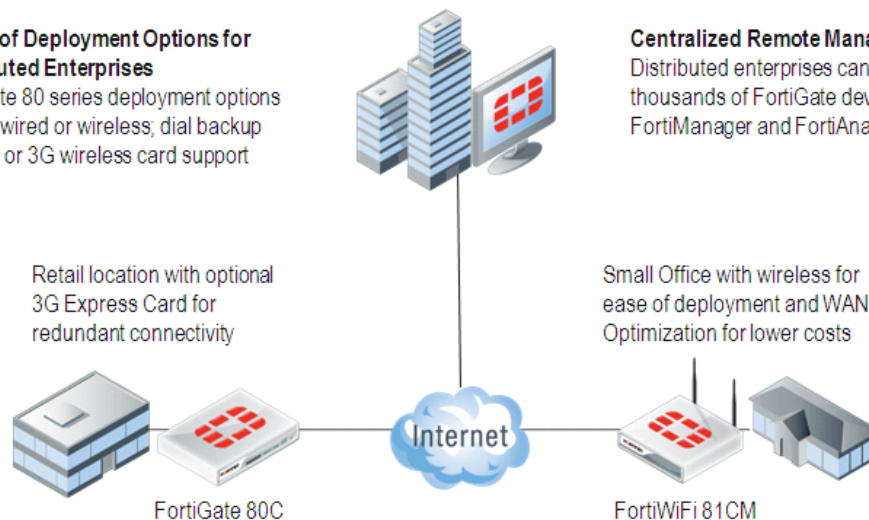
80 Series Deployment Options

Range of Deployment Options for Distributed Enterprises

FortiGate 80 series deployment options include wired or wireless; dial backup modem or 3G wireless card support

Centralized Remote Management

Distributed enterprises can manage thousands of FortiGate devices with FortiManager and FortiAnalyzer



FortiGate-80C and -80CM

The FortiGate-80C/80CM platforms offer dual WAN Gigabit Ethernet (10/100/1000) links, for load balancing or redundant ISP connections deliver high availability and scalability to small or home office application. Six Fast Ethernet (10/100) internal security zone or switch ports and one dedicated DMZ port eliminate need for additional networking devices, reducing investment and management burden. The FortiGate-80C/CM platforms provide an ExpressCard slot for optional 3G wireless WAN connectivity such as EV-DO, W-CDMA, HSPA and GPRS, which provides mobile network connectivity for remote deployments or backup data connectivity in the event of a network failure. The FortiGate-80CM platform gives you the additional convenience and reliability of analog modem.



FortiGate-80C



FortiGate-80CM

FortiWiFi-80CM and -81CM

The FortiWiFi-80CM/81CM multi-threat security platforms deliver comprehensive enterprise-class protection and performance at a low price. With the FortiWiFi platforms' integrated set of essential security technologies, you can deploy a single device that protects your applications and data against today's sophisticated, multi-vector threats.



FortiWiFi-80CM

The internal storage in the FortiWiFi-81CM also enables local caching of data for policy compliance or WAN optimization. WAN optimization lowers your networking costs and improves your application and network performance by reducing the amount of data transmitted over your WAN. Fortinet's Global Threat Research Team and ICISA Labs-certified inspection engines ensure that you have the best possible protection in your network.



FortiWiFi-81CM

FortiGuard / FortiCare Service or Product Specific Info

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 on FortiGuard Service, please visit www.fotiguard.com.

FortiGuard Subscription Services						
	Antivirus	Intrusion Prevention	Web Filtering	Antispam	Application Control	Vulnerability & Compliance
FortiGate-80C	Supported	Supported	Supported	Supported	Supported	Supported
FortiGate-80CM	Supported	Supported	Supported	Supported	Supported	Supported
FortiWiFi-80CM	Supported	Supported	Supported	Supported	Supported	Supported
FortiWiFi-81CM	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 power of the FortiASIC content and network processors. FortiOS software enables a comprehensive suite of security services: Firewall, VPN, intrusion prevention, antivirus/antispam, antispam, web filtering, application control, data loss prevention, and end point network access control.

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)

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)

FIREWALL 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/SMTSPS
- POP3/POP3S IMAP/IMAPS
- FTP IM Protocols
- Automatic "Push" Content Updates from FortiGuard
- File Quarantine Support
- 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

- 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

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

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.

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/SMTSPS, 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 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

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	
Features Highlight	NAT, PAT and Transparent (Bridge) Policy-Based NAT SIP/H.323/SCCP NAT Traversal VLAN Tagging (802.1Q) IPv6 Support
Performance	
Model	FortiGate 80C/80CM, FortiWiFi-80CM/81CM
Firewall (1518 Byte)	700 Mbps
Firewall (512 Byte)	350 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 Antivirus Flow-based Antivirus File Quarantine IPv6 Support
Performance	
Model	FortiGate 80C/80CM, FortiWiFi-80CM/81CM
Antivirus	50 Mbps

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 80C/80CM, FortiWiFi-80CM/81CM
IPS Throughput	100 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	
Features Highlight	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 80C/80CM, FortiWiFi-80CM/81CM
IPSec VPN	80 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	FortiWiFi-81CM
Features Highlight	Gateway-to-Gateway Optimization Bi-directional Gateway-to-client Optimization Web Caching Secure Tunnel Transparent Mode

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)

Features Highlight	Monitor & Control Hosts Running FortiClient Vulnerability Scanning of Network Nodes Quarantine Portal Application Detection and Control Built-in Application Database
--------------------	---

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

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

SSL 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

SSL Inspection

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

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)

Features Highlight	Identification And Control Over Data in Motion Built-in Pattern Database RegEx Based Matching Engine Common File Format Inspection International Character Sets Supported
--------------------	---

Logging & 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

Features Highlight	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 Domain

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

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

High Availability

High Availability (HA) configuration enhances reliability and increases performance by clustering multiple FortiGate appliances into a single entity. FortiGate High Availability supports Active-Active and Active-Passive options to provide the maximum flexibility for utilizing each member within the HA cluster. HA feature is included as part of the FortiOS operation system so end-users can benefit from the reliability enhancement without the extra cost.

High Availability (HA)	
Features Highlight	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	
Features Highlight	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

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

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



FortiGate-80 Series Specification Summary

Technical Specifications	FortiGate-80C	FortiGate-80CM	FortiWiFi-80CM	FortiWiFi-81CM
Hardware Specifications				
10/100/1000 WAN Interfaces (Copper, RJ-45)	2	2	2	2
10/100 Internal Switch Interfaces (Copper, RJ-45)	6	6	6	6
10/100 DMZ Interfaces (Copper, RJ-45)	1	1	1	1
Console (Copper, RJ-45)	1	1	1	1
USB Interfaces	2	2	2	2
ExpressCard Slot	1	1	1	1
WLAN Support		N/A	802.11 a/n or b/g/n	
Analog Modem	N/A		Yes	
Internal Storage		N/A		32 GB
System Performance				
Firewall Throughput (1518 byte UDP packets)	700 Mbps			
Firewall Throughput (512 byte UDP packets)	350 Mbps			
IPSec VPN Throughput	80 Mbps			
IPS Throughput	100 Mbps			
Antivirus Throughput (Proxy)	50 Mbps			
Gateway-to-Gateway IPSec VPN Tunnels	200			
Client-to-Gateway IPSec VPN Tunnels	300			
Concurrent Sessions	100,000			
New Sessions/Sec	5,000			
Concurrent SSL-VPN Users (Recommended Max)	60			
SSL-VPN Throughput	50 Mbps			
Firewall Policies (Max)	2,000			
Virtual Domains (Max / Default)	10 / 10			
Unlimited User Licenses	Yes			
Dimensions				
Height x Width x Length (in)	1.75 x 10.87 x 6.13 in			
Height x Width x Length (cm)	4.45 x 27.61 x 15.57 cm			
Weight	3.5 lbs (1.59 kg)			
Wall Mountable	Yes			
Environment				
Power Required	100-240 VAC, 50-60 Hz, 0.8 Amp max			
Power Consumption (AVG)	32W	32 W	44 W	45 W
BTU	108 BTU	108 BTU	150 BTU	151 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 Class A Part 15, / CE Mark			
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 Info	
Product	SKU
FortiGate-80C Security Appliance Bundle *	FG-80C-BDL
FortiGate-80CM Security Appliance Bundle	FG-80CM-BDL
FortiWiFi-80CM Security Appliance Bundle	FWF-80CM-BDL
FortiWiFi-81CM Security Appliance Bundle	FWF-81CM-BDL
Optional Accessories	SKU
DC Adapter for the FG-80C, FG-80CM, FWF-80CM, FWF-81CM	SP-FG80-PDC
Wall Mount Kit (with express card lock)	SP-FG-50B-60B-MOUNT

* Bundle Includes 1 Yr of FortiGuard / FortiCare Service

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
300 Beach Road
20-01 The Concourse
Singapore 199555
Tel: +65-6513-3730
Fax: +65-6223-6784

Industry Certifications



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.