



# FortiGate<sup>®</sup>/FortiWiFi<sup>™</sup>-80 Series

## Integrated Threat Management for Small Networks

The FortiGate/FortiWiFi-80C Series are compact, all-in-one security appliances that deliver Fortinet's Connected UTM. Ideal for small business, remote, customer premise equipment (CPE) and retail networks, these appliances offer the network security, connectivity and performance you need at a single low per-device price.

### Advanced Protection and Wireless Connectivity

You get advanced threat protection, including firewall, application control, advanced threat protection, IPS, VPN, and web filtering, all from one device that's easy to deploy and manage. With our FortiGuard<sup>®</sup> security subscription services you'll have automated protection against today's sophisticated threats.

Reduce the need for additional wireless access points by integrating a high-bandwidth "fat-client" into your FortiGate with the FortiWiFi-80C. It's also a great option to secure mobile devices in BYOD environments with automatic device identification and customizable access and security policies.

VDOMs on the FortiGate/FortiWiFi-80C, let you segment networks to enable guest and employee access, or protect things like cardholder data. You get the flexibility to match your business needs and meet compliance standards like PCI and HIPAA.

### All-in-one High Performance Network Security

Built on the foundation FortiOS 5, the 80C series provides an integrated set of essential security technologies to protect all of your applications and data. You get the industry's best firewall plus the latest in Advanced Threat Protection, Intrusion Protection, Web-filtering and many new features like Sandboxing, Feature Select Options for simplifying configurations and deployments, and Contextual Visibility for enhanced reporting and management.

DATASHEET



Enterprise-Class Protection that's Easy to Deploy and Manage

- 1.9 Gbps throughput performance ensures your network security won't be a bottleneck
- Integrated switch simplifies your network infrastructure
- Up to 2x WAN GE interfaces, 7x GE LAN switch ports and 1x ExpressCard expansion slot
- Runs on FortiOS 5 – the most powerful security operating system in the world delivers more protection for fighting advanced threats, more control to simplify configurations and deployments, and more contextual visibility for enhanced reporting and management

Feature	Benefit
Unified Security	Multi-threat protection from a single device increases security and lowers costs
Simplified Licensing	Unlimited user licensing and comprehensive features
Multi-Port Interfaces	Multiple network interfaces and optional wireless connectivity enable data segmentation for compliance and flexible deployment



## 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	
Feature Highlights	NAT, PAT and Transparent (Bridge) Policy-Based NAT SIP/H.323/SCCP NAT Traversal VLAN Tagging (802.1Q) IPv6 Support
Performance	
Firewall (1518 Byte)	1.9 Gbps
Firewall (512 Byte)	700 Mbps
Firewall (64 Byte)	120 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	
Antivirus (Proxy-based)	50 Mbps
Antivirus (Flow-based)	190 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	
IPS Throughput	350 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, IPS and Web filtering. Additional features include traffic optimization providing prioritization for traffic across VPNs.

VPN	
Feature Highlights	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	
IPSec VPN	140 Mbps
SSL VPN	70 Mbps
Recommend # of SSL Users	60

## 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
--------------------	---

## Virtual Domain

Virtual Domain (VDM) enables 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 reduce the complexity of your 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
VDMs (Max / Default)	10 / 10

## 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 1800 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

## 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. The 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

## 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. 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

Technical Specifications	FortiGate-80C	FortiGate-80CM	FortiWiFi-80CM
<b>Hardware Specifications</b>			
10/100/1000 WAN Interfaces (Copper, RJ-45)	2	2	2
10/100 Internal Switch Interfaces (Copper, RJ-45)	6	6	6
10/100 DMZ Interfaces (Copper, RJ-45)	1	1	1
Management Console Interface (Copper, RJ-45)	1	1	1
USB Interfaces	2	2	2
ExpressCard Slot	1	1	1
WLAN Support	-	-	802.11 a/n or b/g/n
Modem Port	-	Yes	Yes
<b>System Performance</b>			
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	1900 / 700 / 120 Mbps		
Firewall Latency (64 byte UDP packets)	45 µs		
Firewall Throughput (Packets Per Second)	180 Kpps		
Concurrent Sessions (TCP)	1 Million		
New Sessions/Sec (TCP)	12,000		
Firewall Policies	5,000		
IPSec VPN Throughput (512 byte packets)	140 Mbps		
Gateway-to-Gateway IPSec VPN Tunnels	200		
Client-to-Gateway IPSec VPN Tunnels	1,000		
SSL-VPN Throughput	70 Mbps		
Concurrent SSL-VPN Users (Recommended Max)	100		
IPS Throughput	350 Mbps		
Antivirus Throughput (Proxy Based / Flow Based)	50 / 190 Mbps		
Virtual Domains (Default / Max)	10 / 10		
Max Number of FortiAPs (Total / Tunnel Mode)	32 / 16		
Max Number of FortiTokens	100		
Max Number of Registered FortiClients	200		
High Availability Configurations	Active/Active, Active/Passive, Clustering		
Unlimited User Licenses	Yes		
<b>Dimensions</b>			
Height x Width x Length	1.75 x 10.87 x 6.13 in (4.45 x 27.61 x 15.57 cm)		
Weight	3.3 lb (1.5 kg)		
Wall Mountable	Yes		
<b>Environment</b>			
Power Required	100-240 VAC, 50-60 Hz		
Power Consumption (AVG / Max)	25 / 30 W	26 / 31.2 W	28 / 33.6 W
Heat Dissipation	102.3 BTU	106.5 BTU	115 BTU
Operating Temperature	32 – 104 deg F (0 – 40 deg C)		
Storage Temperature	-31 – 158 deg F (-35 – 70 deg C)		
Humidity	20 to 95% non-condensing		
<b>Compliance &amp; Certification</b>			
Compliance	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB		
Certification	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN		
All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files.			

Ordering Info	
Unit	SKU
FortiGate-80C	FG-80C
FortiGate-80CM	FG-80CM
FortiWiFi-80CM	FWF-80CM
Optional Accessories	SKU
DC Adapter for the FG-80C, FG-80CM, FWF-80CM	SP-FG80-PDC
Wall Mount Kit (with express card lock)	SP-FG-50B-60B-MOUNT

**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, 199555 Singapore  
Tel: +65-6513-3734  
Fax: +65-6295-0015

**Industry Certifications**

**FORTINET**

Copyright © 2013 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, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, 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.