



# FortiGate/FortiWiFi®-20C

## The Power of Unified Threat Management

The FortiGate-20C and FortiWiFi-20C consolidate comprehensive security functions in a single device to protect the smallest locations against today's network, content, and application-level threats. Organizations needing to provide secure access to remote teleworkers, retail outlets, and small branch offices require a device designed for the specific requirements of those locations. The FortiGate-20C and FortiWiFi-20C combine enterprise-grade performance and protection into a small form factor at an entry-level price. The FortiGate-20C and FortiWiFi-20C are also ideal for Service Providers seeking to deliver highly differentiated security services via customer premise equipment (CPE).

### The Power of Unified Threat Management

The FortiGate-20C and FortiWiFi-20C appliances give you the ability to deploy a wide range of Fortinet's UTM inspection capabilities, including firewall, IPS, application control, VPN, and web filtering all at a single low price. They combine the purpose-built FortiOS™ 4.0 security operating system with the Fortinet System on a Chip purpose-built processor, delivering unmatched price and performance advantages.

Each appliance also supports FortiGuard® security subscription services to deliver dynamic, automated updates and ensure up-to-date protection against sophisticated threats. In addition, the devices support a web-based GUI, single pane of glass management console, and on-board reporting.

By consolidating multiple security enforcement technologies into a single appliance, the FortiGate-20C and FortiWiFi-20C eliminate disparate hardware devices and software solutions to greatly simplify secure remote access and reduce total cost of ownership. They ensure that only authorized endpoints are allowed access to corporate resources, and the appliances' granular application control prevents unauthorized applications. For example, security administrators can easily set up policies to allow the usage of social media web sites while restricting access to the chat and download functions.

### FortiGate Consolidated Security Solutions

Fortinet's consolidated security solutions provide an integrated set of core security and network services in a single, easy-to-manage, high-performance appliance that is capable of supporting a wide range of deployment scenarios. The FortiWiFi-20C adds a built-in wireless access point to the multi-threat protection of FortiGate appliances. With the FortiWiFi-20C, your security and wireless needs can be met in one device. This combination allows you to reduce costs and simplify deployment as it eliminates the need for a separate wireless access point.

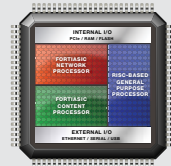


### FortiOS 4.3: Redefining Network Security

FortiOS 4.3 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 the FortiASIC content and network processors. FortiOS software enables a comprehensive suite of security services: Firewall, VPN, intrusion prevention, application control, antivirus, antispam, web filtering, data loss prevention, and end point network access control.

### The Fortinet System-on-a-Chip

The FortiGate-20C and FortiWiFi-20C series utilize the Fortinet System-on-a-chip (SoC). Integrating FortiASIC acceleration logic together with a RISC-based main processor and other system components, the SoC simplifies appliance design and enables breakthrough performance for smaller networks. The FS1 and resulting FortiGate/FortiWiFi-20C series appliances allow large distributed enterprises to provide integrated, multi-threat protection across all points on their network without sacrificing performance.



Feature	Benefit
Unified Security Architecture	Multi-threat protection from a single device increases security and lowers costs.
Simple Licensing	Hassle-free unlimited user licensing and comprehensive feature increases ease of deployment and maintenance.
Multi-Port Wired / Wireless Interfaces	Multiple network interfaces and optional wireless connectivity enable flexible deployment and improve protection with multiple security zones.
Desktop Form-Factor	Compact, lightweight and designed for small environments.

Technical Specifications	FortiGate-20C	FortiWiFi-20C
<b>HARDWARE SPECIFICATIONS</b>		
LAN 10/100/1000 Interfaces (Switched)	4	4
WAN 10/100/1000 Interface	1	1
Wireless Interface	N/A	802.11 a/b/g/n
USB (Client/Server)	1/1	1/1
RJ45 Serial Console	0	0
<b>SYSTEM PERFORMANCE</b>		
Firewall Throughput (1514 byte UDP)	20 Mbps	
Firewall Throughput (66 byte UDP)	20 Mbps	
Firewall Throughput (512 byte UDP)	20 Mbps	
IPSec VPN Throughput (512 byte packet)	20 Mbps	
IPS Throughput	20 Mbps	
Antivirus Throughput (Proxy Based)	20 Mbps	
Antivirus Throughput (Flow Based)	20 Mbps	
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	5 / 5	
Client-to-Gateway IPSec VPN Tunnels	5	
Concurrent Sessions (TCP)	10,000	
New Sessions/Sec (TCP)	1,000	
Policies (Max)	200	
Unlimited User Licenses	Yes	
Mean Time Between Failures	More than 5 years	
<b>DIMENSIONS</b>		
Height	1.4 in (35 mm)	
Width	8.5 in (215 mm)	
Length	7.1 in (180 mm)	
Weight	1 lb (0.5 kg)	
Wall Mountable	Yes	
AC Power	100-240 VAC, 60-50 Hz	
Heat Dissipation	TBD	
Power Consumption (AVG)	TBD	
Redundant Power Supply	No	
<b>ENVIRONMENT</b>		
Operating temperature	32 - 104 °F (0 - 40 °C)	
Storage temperature	-13 - 158 °F (-25 - 70 °C)	
Humidity	20 to 90% non-condensing	
Compliance	FCC Class A Part 15, UL/CUL, CE, C Tick, VCCI	
Certifications	ICSA Labs: Firewall, SSL VPN, IPS, Antivirus	

The FortiGate-20C and FortiWiFi-20C provide full enterprise class UTM inspection including firewall, intrusion prevention, application control, web filtering, antivirus / antimalware, and antispam. Advanced configuration and routing options are limited over other FortiGate models. See the table below for a comparison of features.

Feature	FortiGate-20C FortiWiFi-20C	FortiGate-40C and above
Full UTM Inspection (Firewall, IPS, Antivirus, and Web Filtering)	•	•
Automatic Updates	•	•
Web-Based GUI	•	•
Centralized Management / Reporting	•	•
IPSec VPN	•	•
Application Control	•	•
Data Leakage Prevention	•	•
SSL Inspection		•
WAN Optimization		•
SSL VPN		•
Dynamic Routing (RIP, OSPF, BGP, and PIM)		•
Virtual Domain		•
VLAN Support		•
High Availability		•
Server Load Balancing		•
Traffic Shaping		•

All performance values are "up to" and vary depending on system configuration. Antivirus performance is benchmarked using HTTP traffic (32 Kbyte objects). IPS performance is measured base on NSS like test methodology with 44K HTTP files.

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

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and replace" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

## 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  
300 Beach Road #20-01, The Concourse  
Singapore 199555  
Tel: +65-6513-3734  
Fax: +65-6295-0015



Copyright© 2011 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.