



FortiGate[®]-30B

FortWiFi[™]-30B

Security and Connectivity for Remote Workers and Offices

Securing Remote Sites

Large organizations wanting to provide secure access to remote teleworkers, retail outlets, and branch offices are facing an evolved dilemma: while granting access to these remote sites has become relatively easy, ensuring the remote sites are secure by remotely deploying numerous security devices and software is unfeasible. In order to secure both the data in transit and the remote networks from which data originates, a single device uniting firewall, VPN, intrusion prevention, Web filtering, antivirus, and antispyware specifically designed for remote branch offices, retail outlets, and telecommuters is required.

Retail Outlets and Branch Offices

Dedicated IPSec VPN tunnels have become a standard method of providing access and conveying real time inventory and sales information to corporate headquarters. Once connected, these networks can introduce malware and trojans acquired by their endpoints if the remote network is not adequately protected. Multiple security enforcement technologies such as firewall, intrusion prevention, and antivirus/antimalware must be deployed in order to maintain compliance with PCI, HIPPA, and GLBA regulations. With multiple internal security ports, the FortiGate-30B and FortiWiFi-30B offer complete network security protection and dedicated VPN access in a single device that can be provisioned and managed from anywhere in the world.

Remote Teleworkers

Security concerns similar to that of the retail or branch offices exist for remote teleworkers as well. Unprotected home networks can introduce a barrage of threats to the distributed network. Remotely deploying multiple devices and software solutions at teleworker sites creates a deployment and maintenance nightmare—for both IT administrators and teleworkers. Security risks are compounded with teleworker network usage by other family members, who must be kept separate from work-related access. The FortiGate-30B and FortiWiFi-30B offer a complete solution that provides total network protection for the teleworker’s entire network, while simultaneously offering dedicated VPN access to corporate resources. Multiple internal security ports support multiple devices on the internal interface, and authentication techniques ensure that only the teleworker’s endpoint is allowed access to corporate resources.

Central Management

Regardless of the type of network the FortiGate-30B or FortiWiFi-30B is deployed in, centralized management is a critical component of the remote office and branch office architecture. Fortinet’s FortiManager and FortiAnalyzer products ensure complete centralized control over remote devices regardless of the deployment size.

DATASHEET



The FortiGate Product Family: Integrated Multi-Threat Protection

The FortiGate product family provides cost-effective, comprehensive protection against network, content, and application-level threats. It defends your environment from complex, sophisticated attacks without degrading network availability and affecting application performance.

FortiGate platforms combine the purpose-built FortiOS[™] security operating system with custom FortiASIC processors and other hardware to provide a comprehensive and high-performance array of security and networking functions.

The FortiGate product family delivers the highest level of network, content, and application security for enterprises of all sizes, while reducing total cost of ownership. With Fortinet, you deploy the network security you need to protect your intellectual property, preserve the privacy of critical customer information, and maintain regulatory compliance.

Features

Benefits

Unified Security Architecture

Multi-threat protection from a single device increases security and lowers costs

Unlimited User Licensing

Hassle-free unlimited user licensing increases ease of deployment and maintenance

Multi-Ported Wired / Wireless Interfaces

Multiple physical network interfaces and optional wireless connectivity allow flexible productivity and better security through multiple security zones

Desktop Form-Factor

Compact and lightweight for unobtrusive placement or mounting

Industry Certification



COMMON CRITERIA
EAL 4+ CERTIFIED

ICSA labs
CERTIFIED SSL VPN

™



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, antispyware, application control, data loss prevention, and end point network access control.

While the FortiGate-30B and FortiWiFi-30B provide full enterprise-class UTM inspection including firewall, intrusion prevention, web filtering, antivirus, antispyware / antimalware, and antispam; advanced configuration and routing options are limited over other FortiGate models. See the table below for a comparison of features.

Technical Specifications	FortiGate-30B	FortiWiFi-30B
Hardware Specifications		
10/100 Internal Switch Interfaces (Copper, RJ-45)	3	4
10/100 WAN Interface (Copper, RJ-45)		1
Console (Copper, RJ-45)		1
USB Interface		1
WLAN Support	N/A	802.11 b/g
System Performance		
Firewall Throughput (1518 byte UDP packets)		100 Mbps
Firewall Throughput (512 byte UDP packets)		30 Mbps
IPSec VPN Throughput		5 Mbps
IPS Throughput		10 Mbps
Antivirus Throughput		5 Mbps
Gateway-to-Gateway IPSec VPN Tunnels		5
Client-to-Gateway IPSec VPN Tunnels		5
Concurrent Sessions		5,000
New Sessions/Sec		1,000
Concurrent SSL VPN Users (Recommended Max)		None
Firewall Policies (Max)		200
Virtual Domains (Max / Default)		None
Unlimited User Licenses		Yes
Dimensions		
Height x Width x Length (in)	1.3 x 6.8 x 5.2 in	1.4 x 8.6 x 5.8 in
Height x Width x Length (cm)	3.2 x 17.2 x 13.2 cm	3.5 x 22 x 14.7 cm
Weight	0.8 lb (0.36 Kg)	1.5 lb (0.68 Kg)
Wall Mountable	No	
Environment		
Power Required	100 -240 VAC 50-60 Hz, 1 Amp (Max)	
Power Consumption (AVG)	6 W	7 W
Heat Dissipation	20 BTU	24 BTU
Operating Temperature	32 to 104 deg F (0 - 40 deg C)	
Storage Temperature	-31 to 158 deg F (-35 to 70 deg C)	
Humidity	20 to 80% non-condensing	
Compliance		
	FCC Class A Part 15, / CE Mark	
Certifications		
	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.		

Feature	FortiGate-30B FortiWiFi-30B	All Other FortiGate Models
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		●

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
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784

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.