

FortiGate®-30B FortiWiFi™-30B

Security and Connectivity
for Remote Workers
and Offices

Datasheet

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 antispayware 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.



FortiWiFi-30B



FortiGate-30B

Images are not to scale

Feature	Benefit
• 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-Port 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

FortiGate Multi-Threat Security

Fortinet’s multi-layered security solutions efficiently and economically provide an integrated set of security services in a single, easy-to-manage high-performance appliance that is capable of supporting a wide range of deployment scenarios. In addition, FortiCare and FortiGuard Subscription Services include everything from technical support, antivirus updates, antispayware, antispam, to Web content filtering to ensure that security environments remain current and corporate resources are protected against the latest blended threats. FortiGate systems come with a one-year limited hardware warranty and a 90-day limited software warranty.



TECHNICAL SPECIFICATIONS

HARDWARE SPECIFICATIONS

	FortiGate-30B	FortiWiFi-30B
10/100 Internal Switch Interfaces (Base-T).....	3	4
10/100 WAN Interfaces (Base-T)	1	1
WiFi (802.11b/g)	No	Yes

SYSTEM PERFORMANCE

Firewall Throughput (1518 Byte UDP Packets)	100Mbps	100Mbps
Firewall Throughput (512 Byte UDP Packets)	30Mbps	30Mbps
IPSec VPN Throughput (AES/DES)	5 Mbps	5 Mbps
Antivirus Throughput	5 Mbps	5 Mbps
IPS Throughput	10 Mbps	10 Mbps
Static IPSec VPN Tunnels.....	5	5
Concurrent IPSec VPN Tunnels.....	5	5
Concurrent Sessions	5,000	5,000
New Sessions / Sec	1,000	1,000
Security Policies (Max)	200	200
Unlimited User License (Per Device Licensing).....	Yes	Yes

DIMENSIONS

Height.....	1.25 in (31.75 mm)	1.38 in (35.05 mm)
Width.....	6.75 in (171.45 mm)	8.63 in (219.20 mm)
Length.....	5.2 in (132.08 mm)	5.8 in (147.32 mm)
Weight	0.8 lb (0.36 kg)	1.5 lb (0.68 kg)
Power Required	100 - 240 VAC.....	
	50-60 Hz, 1 Amp (Max)	
Power Consumption (AVG).....	6 W	6W

ENVIRONMENT

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 B, UL/CB/CUL, C Tick, CE, VCCI
Certifications	ICSA Labs: Firewall, IPSec, SSL-TLS, IPS, Antivirus

Antivirus performance is benchmarked using HTTP traffic (32 Kbyte Objects)

FortiGate-30B / FortiWiFi-30B Features

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

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

- Antivirus
- Intrusion Prevention
- Web Filtering
- Antispam
- Premier Signature Service
Includes Antivirus and Intrusion Prevention Updates with additional service level agreements

FortiCare™ Support Services

- 24/7/365 Web-Based Technical Support
- Technical Account Management Service (Optional)
- 24-Hour Phone-Based Support (Optional)
- Professional Services (Optional)
- 1-Year Limited Hardware Warranty
- 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