

# FortiGate-50 -100 Series Frequently Asked Questions

FAQ



## Hardware Questions

### **Q: What is SOHO/ROBO?**

A: SOHO stands for Small Office/Home Office which is usually associated with offices of less than 10 people or computers. ROBO stands for Remote Office/Branch Office which is usually associated with offices of less than 100 people.

### **Q: What type of SOHO/ROBO security appliances does Fortinet offer?**

A: Fortinet's FortiGate systems are purpose-built appliances that provide comprehensive security capabilities including firewall, anti-virus, anti-spyware, intrusion detection and prevention, VPN, web content filtering, spam filtering, spyware/grayware filtering, and management tools. Fortinet's line of small-to-medium business, enterprise (ROBO)/(SOHO) and Managed Security Service Provider (MSSP) Customer Premise Equipment (CPE) network security appliances offer comprehensive protection to distributed networks, meeting the needs for an array of mission critical applications such as Email, Web, VOIP, IM, and P2P with extensive management, logging, and reporting capabilities.

### **Q: What is different about Fortinet's security appliances?**

A: This family of multi-threat security appliances offers an extremely good price/performance ratio with appliances that offer up to 100 Mbps of firewall throughput for under \$1000. The FortiGate-50B through 100A series also offers a wide variety of network access options including 10/100 Ethernet ports, multi-port LAN switching, ADSL modem, WiFi access, and dial back-up modem options for centralized management benefits. The new FortiGate-60B also offers an open PC card slot providing the flexibility needed for different deployment scenario.

### **Q: What different SOHO/ROBO models does Fortinet offer?**

A: Fortinet offers a wide family of small security appliances that provide many basic and advanced networking and security functions:

- FortiGate-50B series offers a simple low cost multi-threat security gateway with 3 port switch and 2 WAN interfaces and model with WiFi interface.
- FortiGate-60B series offers additional hardware features including a 6 port switch, 1 DMZ, 2 WAN interfaces, built-in analog modem for backup as well as an open PC Card slot for 3G Wireless WAN (WWAN) options. Model with 802.11 a/b/g WiFi interface is also available.
- FortiGate-100A offers dual WAN interfaces, dual DMZ, and a 4 port switch, as well as higher performance that may be required for large enterprise branch offices.

### **Q: Are the smaller FortiGate appliances rack mountable?**

A: Generally speaking these are desktop or table-top style appliances with no fans, rubber feet and an external in-line block type power supply. However Fortinet does offer a rack mount kit designed strictly for the FG-50B, FW-50B and FG-60/60M models. It holds two of these units side by side in a 19 inch standard rack. The kit is available for ordering from Fortinet or its resellers and is Fortinet part number FG-RMKIT. The FG-60B, FW-60B, FG-60ADSL and FG-100A are somewhat larger and won't fit into the FG-RMKIT, so you would have to purchase a separate shelf (not available from Fortinet) for each unit that you wish to rack mount.

**Q: Does the FortiGate-60B and FortiWifi-60B offer optional analog modem?**

A: Both FortiGate-60B and FortiWifi-60B come with built-in analog modem as default. Unlike the FG-60 series, you do not need to order specific SKUs with an analog modem.

**Q: What type of PC Cards will be supported by the FG-60B and FW-60B?**

A: The FG-60B and FW-60B has a Type II PC Card slot located in the front. A list of FortiOS supported PC cards will be published on the FortiCare Knowledge Center as well as the FortiOS Release Notes after the product release of the FG60B and FW-60B. The initial plan is to support a range of 3G Wireless WAN PC cards to enable broadband wireless connectivity with different wireless service providers. Customer should refer to the list of supported PC cards to ensure hardware and software interoperability.

**Q: Does the FG-60B and FW-60B ship with any PC card?**

A: No PC card is shipped with the FG-60B and FW-60B. Customers are recommended to review the list of supported PC cards in FortiCare Knowledge Center and the Release Notes before purchasing the PC card.

**Q: How do I enable 3G wireless on the FG-60B or FW-60B?**

A: End-user will need to purchase the FortiOS supported 3G PC card and service contract from the broadband wireless service provider. Install the PC card in the FG-60B or FW-60B and follow the configuration steps in the FortiOS Administration Guide to connect to the broadband wireless service provider's network.

**Q: Can the FW-60B support 3G wireless and 802.11 Wifi simultaneously?**

A: Yes, the FW-60B can support 3G wireless and 802.11 Wifi simultaneously. The FW-60B has 802.11 a/b/g Wifi module built-in, it leaves the PC Card slot open for any supported 3G wireless module.

## Software Questions

**Q: What is FortiOS?**

A: FortiOS is the multi-layered security software that runs on all FortiGate products. It is a proprietary security hardened operating system that provides all of the multi-threat security functions. FortiOS provides the capability to manage FortiGate devices either via a secure GUI web-based user interface or a command line user interface.

**Q: What is the latest version of FortiOS?**

A: Version 3.0 is the latest major release of FortiOS. It was released to the public in January 2006. Since then, two maintenance releases have been made available to customers.

**Q: What type of security modules does FortiOS offer?**

A: Fortinet's FortiGate systems provide the industry's broadest suite of best in class security protections in a single platform, inclusive of firewall, IPSEC VPN, SSL VPN, antivirus, antispymware, intrusion detection/prevention system, web content filtering, antispam and traffic shaping functionality. Deployed as an integrated or standalone solution, FortiGate systems detect and eliminate today's threats as well as emerging bended threats that cannot be detected and eliminated by competitive solutions.

**Q: Can I use the dual WAN interfaces for load balancing traffic?**

A: Yes you can. There are a couple of methods for doing this. One is to use the built-in Equal Cost Multi-Path (ECMP) routing mechanism offered in version 3.0 MR2 and above. This method uses a simple hash algorithm to automatically balance sessions between two or more equal cost routes. The other is to use policy-based routing rules (available since version 2.8) to manually send some traffic to one port and other traffic to a different port. You can route based on source or destination IP addresses or based on protocol type / TCP or UDP port numbers, or any combination of the above.

## Security Subscription Services

**Q: What subscription services are available?**

A: All standard FortiGate product security subscription services are available on each FortiGate appliance.

Security subscription services are inclusive of the FortiGuard Antivirus, IPS, Web Filtering, and Antispam services. Security subscription service bundles are also available to save cost over buying each service separately. No user licensing or user restrictions exist on any model.

**Q: How often are these subscription services updated?**

A: Each FortiGuard service has constantly upgraded databases in order to keep your FortiGate units up to date to protect against recent cyber threats. The signature and vulnerability based Anti-Virus, Anti-Spyware and Intrusion Prevention System services have the ability to automatically push real-time updates to registered and configured units at any time 24 hours a day. The real-time services inclusive of Antispam and Web Content Filtering are constantly upgraded databases that maintain the highest possible accuracy.

**Q: How does Fortinet subscription service response time compare to the industry?**

A: Fortinet's FortiGuard subscription services with Service Level Agreement and FortiGuard Distribution Network provides Fortinet customers with the highest responsiveness of security vendors in both response time of creating new signatures to new exploits and breadth of coverage for anti-virus, anti-spyware, web content filtering, intrusion prevention and anti-spam.

## Security Deployment Scenarios

**Q: What security modules are recommended for SOHO/ROBO deployments?**

A: Small/remote offices are just as likely to be affected by today's malware and threats as bigger locations. That's why you need a full multi-threat security system including Firewall, VPN, antivirus, antispymware, intrusion prevention system, web content filtering, and antispam capabilities. The FortiGate systems are ideal for this environment since they come with all these features pre-installed and you can just enable the ones you need or all of them with no extra licensing charges or user restrictions.

**Q: What security modules are recommended for MSSP (managed security service providers)?**

A: MSSP typically need a flexible CPE platform that can be remotely managed and can have many security options available for flexible security service offering. All FortiGate models come with built-in remote management tools that allow centralized security policy management and remote event monitoring for control via a security operations center. Additional products available such as FortiManager and /or FortiAnalyzer provide the management tools to administer remote sites and scales from a multiple branch office network up to a global multi-domain operation.

**Q: What security modules are recommended for perimeter security?**

A: Perimeter networks generally require Firewall and VPN (IPSEC and/or SSL) features and also will benefit from IPS and Antivirus protection. In some deployment scenarios where compliance requirements are in place that restrict access to specific web content, Web Content Filtering protection may be appropriate.

## Performance & Throughput

**Q: What is the expected FW performance per unit? What are the performance assumptions?**

A: The FG-50B series offers 50 Mbps of firewall throughput. The FG-60B series and the FG-100A provides up to 100 Mbps of firewall throughput. This assumes 1518 byte UDP packets and bi-directional traffic.

**Q: What is the expected VPN performance per unit? What are the performance assumptions?**

A: The FG-50B series offers 48 Mbps of 3DES IPsec VPN throughput. The FG-60B series provides up to 64 Mbps of 3DES IPsec VPN throughput. The FG-100A offers up to 40 Mbps of 3DES IPsec VPN performance. This assumes 1480 byte UDP packets.

**Q: What is the expected IPS performance per unit? What are the performance assumptions?**

A: The FG-50B series offers over 40 Mbps IPS throughputs. The FG-60B series can provide over 45 Mbps of IPS throughputs. The FG-100A can provide over 80 Mbps of IPS throughput. This assumes 1518 byte UDP packets.

**Q: What is the expected AV performance per unit? What are the performance assumptions?**

A: The FG-50B series offers over 19 Mbps of AV throughput. The FG-60B series and the FG-100A can provide over 20 Mbps of AV throughput. This assumes HTTP traffic with 32 K file size attachments.

**Q: Can I cluster these units?**

A: Yes, all FortiGate models support high availability (HA) features with choice of active-passive or active-active with load balancing options.

Copyright 2006 Fortinet, Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

#### Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

#### Disclaimer

Although Fortinet has attempted to provide accurate information in these materials, Fortinet assumes no legal responsibility for the accuracy or completeness of the information. Please note that no Fortinet statements herein constitute or contain any guarantee, warranty or legally binding representation. All materials contained in this publication are subject to change without notice, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FAQ109 0607 R5