

# Fortinet Bypass Modules

## Hardware Bypass Options for FortiGate® Multi-Threat Security Systems

### Ensure Network Continuity

IT administrators are faced with the challenge of securing a network while also ensuring that the network is always available. For critical network segments, this could mean that network availability is valued over ensuring that all traffic is inspected for malicious activity. High availability solutions, where a system fails over to either an active or standby unit, can reduce the risk of a network outage while still providing security services. However, to further reduce the risk of a network outage due to a power failure or a security device malfunction, bypassing the device altogether with a fail-to-wire solution can ensure network continuity at times when security cannot be provided.

Fortinet ASM-CX4 and ASM-FX2 modules provide bypass functionality to FortiGate multi-threat security systems equipped with an available single-width Advanced Mezzanine Card (AMC) expansion bay. The ASM-CX4 is a single-width AMC module which provides four (4) 10/100/1000 copper (RJ-45) Ethernet interfaces for two protected segments of network traffic. The ASM-FX2 is a single-width AMC module which provides two (2) gigabit fiber (LC, 850nm) Ethernet interfaces for a single protected segment of network traffic. Operating in transparent mode during normal operation, both modules automatically bridge network traffic in the event of a system failure or power outage to ensure mission-critical network continuity.

### FortiGate Multi-Threat Security Solutions

FortiGate multi-threat security solutions provide an integrated set of security services in a single, easy-to-manage platform that is capable of supporting a wide range of deployment scenarios. FortiGate systems provide essential security services, with fully integrated firewall, virtual private network (VPN), intrusion prevention, antivirus/antispyware, web filtering, antispam, and application control. To ensure that the security effectiveness of the FortiGate solutions remains at the highest levels possible, Fortinet offers FortiGuard® subscription services that include antivirus updates, intrusion prevention updates, an antispam rating service, and a Web filtering rating service. A wide range of hardware models is available for any network size—from the remote office or branch office to the high-speed core or data center.



### FortiOS 4.0 Software Redefines Networks Security

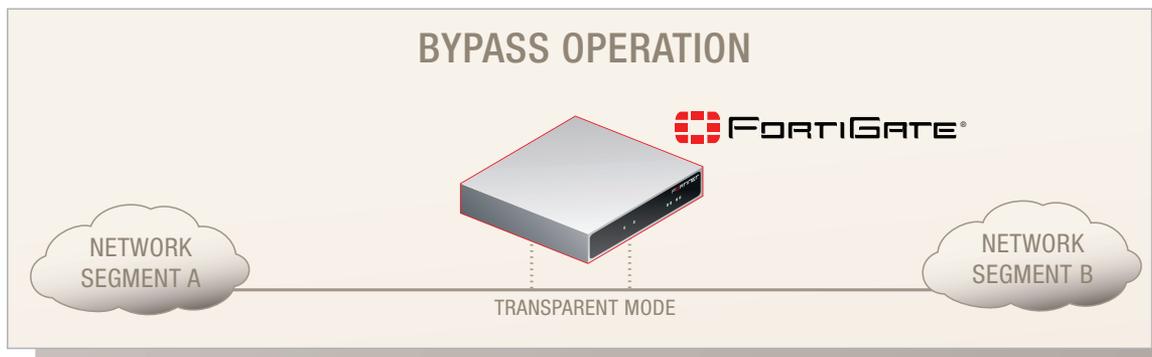
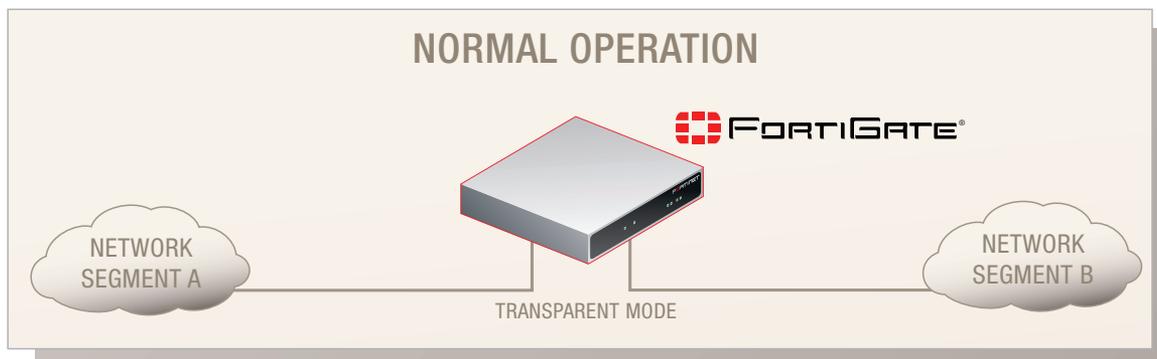
FortiOS 4.0 is a purpose-built operating system that leverages the power of specialized FortiASIC hardware to offer increased levels of security and performance. Fortinet developed FortiOS 4.0 software solely for the FortiGate multi-threat security platform. FortiOS software enables a comprehensive suite of security services – firewall, VPN, intrusion prevention, antimalware, antispam, web filtering, application control, data loss prevention, vulnerability management, and end point network access control.

### The FortiASIC Advantage

FortiASIC processors power FortiGate platforms. With exclusive hardware, the purpose built, high-performance network, security, and content processors use intelligent and proprietary digital engines to accelerate resource-intensive security services.

Challenge	Solution
<b>Fail-to-Wire Bypass</b>	Maximize network uptime by using Fortinet bypass modules to automatically fail-to-wire in the event of a power outage or any other type of event that would cause the host device to degrade the availability of the network segment. The modules automatically return to normal operating mode when conditions permit.
<b>Modular Form Factor</b>	Empowers customers with the ability to add bypass to existing systems with an available single-width AMC expansion bay or to customize a new solution to match defined requirements.
<b>FortiOS™ Integration</b>	Increases the administrator's ability to monitor and control the bypass status of interfaces remotely, with the ability to view mode of operation, manually switch interfaces into bypass or normal operation mode, and configure thresholds for automatic bypass fail-to-wire.

Technical Specification	ASM-CX4	ASM-FX2
<b>HARDWARE</b>		
10/100/1000 Interfaces (Copper, RJ-45)	4	0
1Gb Optical Interfaces (Fiber, LC, 850nm)	0	2
AMC Expansion Slots Required	1 Single-Width	1 Single-Width
<b>MODULE PERFORMANCE</b>		
Normal Operation	Varies, Dependant on System Performance	
Bypass Operation	Link Speed	
Power Required	Up to 2 circuits, 100 - 240 VAC, 60 - 50 Hz, 8 - 5 Amp (Max)	
<b>ENVIRONMENT</b>		
Operating temperature	32 to 104 deg F (0 - 40 deg C)	
Storage temperature	-13 to 158 deg F (-25 to 70 deg C)	
Humidity	5 to 90% non-condensing	
Compliance	FCC Class A, Part 15, UL/CUL, C Tick, CE, VCCI	



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.