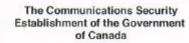
## **FIPS 140-2 Validation Certificate**



The National Institute of Standards and Technology of the United States of America





Certificate No. 467

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

## FortiGate-3000 and FortiGate-3600 by Fortinet, Inc.

(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Designated Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

FortiGate-3000 and FortiGate-3600 by Fortinet, Inc.

(Hardware Versions: FortiGate-3000 (build xx20) and FortiGate-3600 (build xx20), Firmware Version: 2.50. build 219.040616: Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: _		DOMUS IT Security Laboratory, NVLAP LAB CODE 200017-0, CRYPTIK Version 5.8	
is as follows:			
Cryptographic Module Specification:	Level 2	Cryptographic Module Ports and Interf	aces: Level 2
Roles, Services, and Authentication:	Level 2	Finite State Model:	Level 2
Physical Security:	Level 2	Cryptographic Key Management:	Level 2
(Multi-Chip Standalone) EMI/EMC:	Level 2	Self Tests:	Level 2
Design Assurance:	Level 2	Mitigation of Other Attacks:	Level 2
Operational Environment:	Level N/A	tested in the following configuration(s)	: N/A
The following FIPS approved Cryptograp		e-DES (Cert. #237); AES (Cert. #128); SHS (Cort. #213, vend	
The Cryptographic module also contains	the following non-FIPS approv	/ed algorithms: DES; Diffie-Hellman (key a	greement); MD5; HMAC-N
	Overall Level	Achieved: 2	
Signed on behalf of the Government of the United States		Signed on behalf of the Government of Canada	
Signature:		Signature: and tank	
Dated: de ozou	2004	Dated: Other	4,2014
Chief, Computer Security Division		Director, Industry Program Group	
National Institute of Standards and Technology		Communications Security Establishment	

National Institute of Standards and Technology