



Fortinet FortiOS and FortiAnalyzer Firmware Awarded Federal Information Processing Standards (FIPS) Security Certification

FIPS 140-2 Level 1 Certifications Allow for Greater 'Defense in Depth' to Meet Federal IT Needs

SUNNYVALE, CA -- (MARKET WIRE) -- 11/22/10 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced that FortiOS™, the operating system behind Fortinet's award-winning FortiGate® multi-threat security appliances, and FortiAnalyzer 4.0, the operating system supporting the company's FortiAnalyzer centralized reporting appliances, have earned FIPS 140-2 Level 1 certification from the National Institute of Standards and Technology (NIST).

Today's Federal government is tasked to do more with less, as budgets are significantly limited and, at the same time, unrelenting cyber criminals are organizing and developing highly-evolved threats in an ongoing attempt to circumvent traditional security infrastructures. FIPS certification was created to address these new threats by requiring a higher level of performance from cryptographic modules used in Federal government agency networks.

"With limited Federal resources available for new security initiatives, we're seeing IT workers rallying around defense in depth, which offers multiple layers of security defense placed throughout an IT system," said Phil Fuster, vice president of Federal operations for Fortinet. "Our FIPS-certified multi-threat security solutions fit perfectly into this enhanced security model."

In addition to FIPS, Fortinet's FortiOS and FortiGate security appliances have received Common Criteria Elevated Assurance Level 4 (EAL4+) and U.S. Army IA APL certification.

FortiAnalyzer securely aggregates log data from Fortinet devices and other syslog-compatible devices. By using a broad suite of easily-customized reports, FortiAnalyzer can filter and review records, including traffic, event, virus, attack, Web content, and email data, then mine the data to determine security stance and help customers meet their regulatory compliance requirements.

FortiOS is the operating system behind the FortiGate multi-threat network security appliances. Fortinet's FortiGate systems are ASIC-accelerated security appliances that integrate core security and network functionalities including firewall, SSL and IPsec VPN, antivirus, intrusion prevention, Web filtering, antispam, application control, data loss prevention, SSL traffic inspection and WAN optimization.

About FIPS (www.nist.gov)

FIPS is a set of standards that describe document processing, provide standard algorithms for searching and provide other information processing standards for security modules used to protect government networks. The Cryptographic Module Validation Program (CMVP), headed by NIST, provides module and algorithm testing for FIPS 140-2, which applies to Federal agencies using validated cryptographic modules to protect sensitive government data in computer and telecommunication systems. FIPS 140-2 provides stringent third-party assurance of security claims on any product containing cryptography that may be purchased by a government agency.

About Fortinet (www.fortinet.com)

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

Copyright © 2010 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiDB and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties, such as the National Institute of Standards and Technology, and Fortinet does not independently endorse such statements. This news release may contain forward-looking statements that involve uncertainties and assumptions. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially

from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements, including but not limited to, any statements related to expected trends in cybercriminal activity. These trends are difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O

[Add to Digg](#) [Bookmark with del.icio.us](#) [Add to Newsvine](#)

Media Contact:

Rick Popko

Fortinet, Inc.

+1-408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media