



Fortinet Adds WAN Optimisation and SSL Inspection to FortiGate Security Appliances

Fortinet - a market-leading network security provider and worldwide leader of unified threat management (UTM) solutions - today announced its FortiOS 4.0 operating system, a major firmware upgrade which integrates hundreds of new features to significantly improve the value and functionality of its FortiGate multi-threat security appliances.

Four of the most notable features of Fortinet's new OS are advanced application controls, data leakage protection (DLP), WAN optimisation and SSL traffic inspection. The combination of these new features will help customers to secure their networks, protect data, and accelerate applications.

Most existing FortiGate customers with active maintenance contracts can upgrade to the new OS at no additional cost.*

Charles Cote, Fortinet regional director for Australia and New Zealand commented, "Businesses across Australia and New Zealand are telling us they want to get more out of their existing IT investments, and are looking to achieve more with their existing security budget. FortiOS 4.0 is a simple firmware upgrade, which improves security for your applications and data, and makes it possible to speed up your applications and optimise your WAN."

FortiOS 4.0 allows businesses to consolidate multiple advanced networking and security services into a single, easy to maintain appliance. This helps to reduce both the carbon and physical footprints of datacentres, while simplify IT support requirements, and reducing CAPEX/OPEX.

FortiOS 4.0: Enhanced,
Accelerated, Secured

The rich set of functionalities that FortiOS 4.0 brings to FortiGate appliances will dramatically enhance security and network performance as detailed below:

Application Control Traffic is recognised by the application which is generating it, instead of the port or protocol observed. More than 1000 applications are automatically recognized. This facilitates control over evasive applications that use non-standard ports, port-hopping, or tunneling within trusted ports and protocols; **Data Leakage Prevention** Helps to

identify and prevent the communication of sensitive information outside of the network boundaries. DLP works across any application, and is also effective where traffic is SSL-encrypted. Configurable actions provides audit trails for data and files, and make it easier for organisations that need to demonstrate compliance with government regulations governing data privacy. WAN Optimisation FortiOS 4.0 is able to accelerate applications over WAN connections while ensuring multi-threat security enforcement. This not only increases network performance, it also reduces bandwidth and server resource requirements. Faster response times for applications can also improve user productivity. FortiGate models with local storage capabilities are required to take advantage of this feature. SSL Inspection to increase security and policy control among encrypted traffic streams; inspects otherwise hidden communication; increased protection for secure web and application servers; improved visibility into network traffic.

Additional information on FortiOS 4.0 and other Fortinet products can be accessed at <http://www.fortinet.com/products>. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog at <http://blog.fortinet.com>. All existing FortiGate customers with active maintenance contracts can upgrade to the new OS at little to no additional cost.*

About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, web filtering, spyware prevention, and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and a unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting capabilities. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, SSL VPN, Network IPS, and Anti-spam. Fortinet is privately held and based in Sunnyvale, California.

Copyright 2009 Fortinet, Inc. All rights reserved. The symbols and denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinets 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, FortiDB and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements herein attributed to third parties and Fortinet does not

separately endorse any such statements.

* Less than five percent of current FortiGate appliances will be unable to upgrade to FortiOS 4.0 due to hardware requirements