



Fortinet Expands Web Application Firewall Family with New Appliances for Enterprises and Cloud-based Service Providers

Fortinet (NASDAQ: FTNT) - a leading network security provider and a worldwide leader of unified threat management (UTM) solutions today announced two new appliances for its FortiWeb family of web application firewalls: the FortiWeb-1000C, designed for mid-to-large enterprises, and FortiWeb-3000C, the flagship system for high-end enterprises, application service and cloud-based service providers.

The FortiWeb-1000C and 3000C appliances are integrated web application and XML firewalls that protect against attacks targeted at web applications and web services infrastructure.

Because they provide detailed visibility into an organisation's threat landscape, the FortiWeb application firewalls eliminate the need to manage separate web and threat management tools and consoles. Not only does this streamline security efforts and reduce infrastructure complexity, it drastically reduces the time required to protect regulated data and achieve regulatory compliance.

Each appliance is equipped with the new FortiWeb 4.0 MR1 firmware that is designed to provide maximum protection for web applications containing sensitive data subject to Payment Card Industry (PCI) guidelines. The new web application firewalls also blunt potentially crippling attacks such as SQL injection and cross-site scripting, and help prevent security breaches from exposing highly sensitive data loss, such as credit card numbers and personally identifiable information.

With the addition of the FortiWeb-1000C and FortiWeb-3000C, Fortinet now offers four web application firewall appliances to provide retail and payment, financial services and healthcare customers with a full range of deployment options. In the case of retail and payment customers, the new FortiWeb products greatly minimise the complexity of complying with PCI Data Security Standard (DSS) section 6.5 and

6.6, as well as the rampant problems of identity theft and financial fraud. The FortiWeb-1000C and FortiWeb-3000C also provide robust patient data protection as part of HIPAA compliance for healthcare organisations.

The need to protect web applications that contain sensitive credit, financial or personal information from increasingly sophisticated attacks and data loss has never been greater, said Paula Musich, senior analyst, Current Analysis. The simple fact of the matter is that organisations are deploying web applications and regulated Internet-facing data more broadly than ever. For hackers and cyber-criminals, that's like painting a giant bulls-eye on those applications, which gather credit card data and personally identifiable information with minimal protection in place. That's why putting in place sophisticated web protection and threat management solutions with powerful policy enforcement capabilities should be a standard practice for any organisation doing business on the web.

To preserve optimal web application performance, the FortiWeb application firewalls leverage an intelligent, application-aware load-balancing engine to distribute traffic and route content across multiple web servers. This load balancing increases application performance, improves resource utilisation and application stability while reducing service response times.

Whats New in FortiWeb Application Firewalls

The release of FortiWeb 4.0 MR1 provides a series of major enhancements to the new FortiWeb-1000C and FortiWeb-3000C application firewalls, including:

Policy
wizard and pre-defined policies allows for one click deployments and eases the process of rules creation greatly

Advanced alert tool -- makes it easy to sift through hundreds of alerts, identify repetitive attackers using various aggregation fields and quickly understand the nature of attacks.

Enhanced Protocol Constraints
enforces policies that ensure any access to the web application is done in accordance with the HTTP RFC standard.

Extended signatures and DLP -- allows

customers to create their own granular signatures and data loss prevention patterns from a FortiWeb graphical user interface for any type of event, in addition to the pre-defined application signatures and data loss prevention rules.

Customer demand for more powerful web application infrastructure security is soaring due to a combination of evolving attacks, security breaches, regulatory compliance and web defacement incidents, said Michael Xie, founder, CTO and vice president of engineering at Fortinet. At the same time, more content is being delivered via the web, and both cloud providers and large enterprises need robust security solutions that can protect web application infrastructures without affecting application performance. The addition of the FortiWeb-1000C and FortiWeb-3000C appliances to the FortiWeb product family directly addresses this demand. These new platforms can play a pivotal role in helping preserve the security and uninterrupted operation of our customers web application infrastructures.

Availability

The FortiWeb-1000C and FortiWeb-3000C are available now.

Fortinet products are distributed in Australia by Ingram Micro, Firewall Systems, and Whitegold Solutions. Fortinet products are distributed in New Zealand by Ingram Micro and Firewall Systems.

About Fortinet (www.fortinet.com)

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a 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, FortiAP, FortiDB and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties 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. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O