FERTINET

Fortinet Strengthens Web Application Protection With Feature-Rich Updates to Its Web Application Firewall Operating System and a New Appliance

FortiWeb 4.0 MR3 First and Only Web Application Firewall to Integrate Web Vulnerability Scanner and Application Delivery Capabilities in Single Appliance

SUNNYVALE, CA -- (MARKET WIRE) -- 08/01/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced a major new release of its FortiWeb™ We application firewall (WAF) family for enterprises, application service, software as a service (SaaS) and managed security service providers (MSSPs). Fortinet's Web application firewall appliances are the industry's first and only systems to integrate a Web vulnerability scanner and advanced application load balancing features in a single device to significantly reduce deployment times and resource utilization while improving application performance.

In addition to the software updates, Fortinet is also introducing the FortiWeb-3000CFsx appliance, which now provides large enterprises, application service and cloud-based service providers with enhanced performance through its fiber fail open interface.

As an integrated WAF and Web vulnerability scanner, FortiWeb 4.0 MR3 is ideal for organizations subject to Payment Card Industry Data Security Standards (PCI-DSS) 6.6, data breach notification requirements such as California State Assembly Bill 1386 or HIPAA compliance. For customers in need of assistance in protecting critical Web applications from attacks such as SQL Injection and Cross-Site Scripting, FortiWeb appliances leverage the built-in Web vulnerability scanner to proactively identify and guard against potential data loss from Open Web Application Security Program (OWASP) Top 10 attack profiles. In addition, as part of this release, FortiWeb 4.0 MR3 features advanced data compression capabilities to improve bandwidth utilization and user response times, as well as the overall performance of application delivery.

New FortiWeb 4.0 MR3 Capabilities

FortiWeb 4.0 MR3 features a wide range of new capabilities that span security and configuration, logging and reporting and ease-of-use, including:

- A new denial of service (DoS) protection scheme provides network and application layer DoS policies.This enables FortiWeb appliances to analyze requests originating from individual users to determine whether they are authentic or masquerading as automated attacks
- A new Period Blocking feature enhances organizational protection by enabling administrators to block users for specified periods of time rather than denying access on the basis of a particular connection
- Advanced compression has also been added to allow for more efficient bandwidth utilization and improved user response time by compressing data retrieval from servers
- New load balancing enhancements provide content-based "health checks" and offer additional alerts in the event of a server failure. For added protection when logging into FortiWeb devices, Radius/LDAP authentication is supported. Plus, access to FortiGuard updates -- providing up-to-the-minute information on breaking threats, vulnerabilities and security research -- are downloadable via proxy.

For improved logging and reporting, FortiWeb is now fully integrated with Fortinet's FortiAnalyzer™ to provide a simplified means of centrally managing all logs and reports from multiple FortiWeb devices. Providing a new analytics interface, FortiWeb appliances now feature tools to help customers understand Web application usage using different vectors such as number of requests, data transferred and attack types all mapped to their geographic location. New alert enhancements are also included, enabling security administrators to receive email and alert notifications for a variety of conditions such as low system resources, server health issues and session limitations.

The FortiWeb family also features an updated and simplified user interface that emulates the FortiGate™ consolidated securi appliances from Fortinet. As a result, system configuration is greatly simplified and key usability features such as error page customization are supported.

"Our worldwide customer base has made it clear that Web application protection is a very high priority," said Michael Xie, founder, CTO and vice president of engineering at Fortinet. "At the same time, given IT and security resource constraints, we are hearing loud and clear the need to consolidate key functionality into a single, multi-purpose appliance that can be managed on a unified basis for deployment simplicity, optimal data protection and maximum resource utilization. The introduction of our new FortiWeb product family underscores our commitment to meeting global customer demands."

Availability
FortiWeb 4.0 MR3 and FortiWeb-3000CFsx appliance are available now.

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 2010 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 © 2011 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. Nothing in the news release constitutes a warranty, guaranty, or contractually binding commitment. 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

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contact:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media