Press Release –

Media Contact:

Jennifer Leggio
Fortinet, Inc.
+1-408-486-7876
jleggio@fortinet.com

Fortinet Enhances FortiWeb Web Application Firewall Family to Help Customers Safeguard Confidential and Regulated Data

FortiWeb 4.0 MR2 Firmware Upgrade Delivers Expanded Attack Protection Capabilities, New FortiWeb VM Virtual Appliance and Enhanced Centralized Reporting,

SUNNYVALE, Calif., January 31, 2011- Fortinet® (NASDAQ: FTNT) - a leading network security provider and the worldwide leader of unified threat management (UTM) solutions– today announced a major firmware release for its FortiWeb™ web application firewall family. FortiWeb appliances provide enterprises, application service providers, Security-as-a-Service (SaaS) and Managed Security Service Provider (MSSP) customers with significantly expanded security capabilities designed to harden and simplify protection of critical web-based applications containing regulated and confidential data. FortiWeb 4.0 MR2 firmware features a broad range of substantial enhancements that include seamless integration with Fortinet's FortiAnalyzer™ centralized reporting appliances and a new FortiWeb-VM virtual appliance for VMware ESX and ESXi 3.5/4.0 platforms. Expanded attack protection schemes are also included to help organizations more easily achieve and maintain compliance with Payment Card Industry Data Security Standards (PCI DSS 6.6) and help prevent identity theft, financial fraud and corporate espionage associated with strategic web applications.

The FortiWeb family of integrated web application and XML firewall appliances deliver this specialized, layered application threat protection. These appliances are unique in consolidating web application firewall, XML filtering, web traffic acceleration and application traffic balancing into a single device. Equipped with FortiWeb 4.0 MR2 firmware, FortiWeb appliances leverage advanced techniques to provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting. A new Web Vulnerability

Scanner is also provided as another layer of visibility to help detect existing vulnerabilities targeting specific web applications. This capability is critical to help achieve and maintain compliance with the most current PCI DSS 6.5 and 6.6 specifications designed to secure web applications that process, store or transmit payment card data. These specifications require web application firewalls and vulnerability assessment capabilities, both of which are provided by Fortinet in a single device.

With the release of FortiWeb 4.0 MR2, FortiWeb appliances are now fully integrated with Fortinet's family of FortiAnalyzer reporting and analysis appliances. As a result, security administrators can centrally manage all logs and reports gathered from multiple FortiWeb devices deployed throughout an organization, another capability unique to Fortinet. The new firmware release also provides new PCI reports that allow administrators to report on their PCI compliance status quickly. In addition, a new attack widget offers a timely overview of attacks launched against protected applications, separated by event logs and attack logs.

A key attribute of FortiWeb 4.0 MR2 is the new FortiWeb-VM, a virtual appliance for VMware ESX and ESXi 3.5/4.0 platforms. This enables FortiWeb application security controls to be installed within virtual environments to help mitigate "blind spots" that historically have made virtual switch layer traffic "invisible" and the enforcement of security policies very complex. With FortiWeb VM, organizations can rapidly provision security throughout virtualized infrastructures whenever and wherever it is needed.

With the new FortiWeb 4.0 MR2 firmware, FortiWeb appliances now have additional security and usability capabilities that include:

- Robust protection against remote file inclusion attacks
- File upload restrictions that now control which file types (jpg, exe, zip, etc) can be uploaded to web applications
- Data loss prevention enhancements that enable customers to mask credit card numbers in server replies to prevent sensitive data leakage
- Authentication of users via Radius servers
- Scheduled and automatic FTP backups

- A new import/export tool for specific security policies and the ability to automatically clone those policies

“Web applications are an essential foundation for conducting business today which is why organizations now place a premium on protecting highly sensitive and regulated Web application data,” said Michael Xie, founder, CTO and vice president of engineering at Fortinet. “The consequences of compromised web application data can be devastating. Identity theft, corporate espionage, financial fraud, negative impact on brand equity and the potential for a backlash in customer loyalty are just a few examples. That’s why we are relentless in bringing innovative web application security measures to market. This latest release of our FortiWeb firmware is yet another example of our commitment to help secure our customers’ web application infrastructures.”

Availability

The FortiWeb 4.0 MR2 firmware release is 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 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.

###

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