Fortinet Extends UTM Including Application Control Capabilities to SOHO, SMB and Remote Branch Office Markets

New Entry-Level FortiGate-20C, FortiWiFi-20C, FortiGate-40C and FortiWiFi-40C Appliances Consolidate Essential Security Functions in Single Device With Breakthrough Price/Performance

SUNNYVALE, CA -- (MARKET WIRE) -- 10/03/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced the introduction of two new consolidated security appliances that bring the many benefits of enterprise-class UTM, including advanced application control, to small businesses, remote offices and retail outlets. Fortinet is unique in providing enterprise-class security solutions to customer that range from telecommuters to global enterprises.

The entry-level FortiGate-20C and FortiWiFi-20C products feature an elegant new form factor that consolidates broad security functions in a single device to protect even the smallest locations against today's network, content and application-level threats. The FortiGate-20C, FortiWiFi-20C, FortiGate-40C and FortiWiFi-40C are also ideal for Service Providers seeking to deliver highly differentiated security services via customer premise equipment (CPE). Fortinet's FortiManager and FortiAnalyzer platforms can centrally manage the FortiGate appliances, greatly simplifying deployment and management for large distributed organizations that may have thousands of devices working to preserve the privacy of critical customer information, protecting intellectual property and maintaining policy compliance.

The FortiGate-20C, FortiWiFi-20C, FortiGate-40C and FortiWiFi-40C appliances coupled with the purpose-built FortiOS™ 4.3 security operating system give customers the ability to deploy Fortinet's UTM inspection capabilities, including firewall, IPS, application control, VPN and Web filtering. Each appliance also supports FortiGuard® security subscription services that deliver dynamic, automated updates to help ensure up-to-date protection against sophisticated threats. In addition, the new appliances support a Web-based GUI, single pane of glass management console and on-board reporting, as well as data loss prevention, vulnerability management, and WAN optimization. These combined capabilities, uniquely delivered by Fortinet in this product class, are essential to helping to secure data in transit as well as the remote networks from which data is originating.

Protecting Retail Outlets and Branch Offices
With five 10/100/1000 switchable LAN ports, two 10/100/1000 WAN ports and 4 GB of internal storage, the FortiGate-40C and FortiWiFi-40C appliances are ideal for securing access to retail outlets and branch offices. Supporting dedicated IPsec VPN tunnels that have become a standard method of providing access and delivery of real time inventory and sales information to corporate headquarters, the appliances capitalize on multiple security enforcement technologies to protect against malware that can be acquired by endpoints in unprotected remote networks. This provides organizations with a strategic and cost-effective solution -- that can be provisioned and managed from anywhere in the world -- to maintain compliance with PCI, HIPAA and GLBA regulations.

Securing Telecommuters
By consolidating multiple security enforcement technologies into a single appliance, the FortiGate-20C and FortiWiFi-20C eliminate disparate hardware devices and software solutions to greatly simplify secure access of telecommuters at a substantially reduced total cost of ownership. In addition to providing powerful authentication techniques to ensure that only authorized telecommuter endpoints are allowed access to corporate resources, the appliances' granular application control enforces "whitelisting" to ensure only authorized applications can be accessed. For example, security administrators can easily set up policies to allow the usage of Facebook while restricting access to the chat function or disabling the ability to click on links within friends' posts. These are common sources of malware, phishing attacks and/or advanced persistent threats. Application control can also be used to completely deny recreational peer-to-peer applications such as MafiaWars, not only to block a source of potential malware, but to deny productivity-killing distractions on company time.

"As workforces and work places become increasingly distributed, the need to secure remote sites, retail outlets and telecommuters with a cost-effective, simple to deploy and highly consolidated security solution has never been greater," said Michael Xie, cofounder, CTO and vice president of engineering at Fortinet. "The introduction of our new entry-level FortiGate appliances are in direct response to this market dynamic. By adding strategic security appliances to our entry-level product portfolio, Fortinet is uniquely positioned to offer comprehensive security solutions that can address the needs of single and remote workers at Fortune 500 enterprises."

Availability
The FortiGate-20C, FortiWiFi-20C, FortiGate-40C and FortiWiFi-40C appliances will be available later this quarter.

[*Editors note*: please see accompanying Fortinet announcement on the new FortiGate-600C and FortiGate-1000C appliances.]

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.

FTNT-O

Media Contact:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet