



Fortinet Announces Secure Wireless LAN Strategy with Introduction of Thin Access Points

Fortinet (NASDAQ: FTNT) - a leading network security provider and worldwide leader of unified threat management (UTM) solutions - today introduced a secure wireless LAN strategy with a new enterprise-class FortiAP thin access point (AP) product line.

The FortiAP-210 and FortiAP-220, which support the latest IEEE 802.11n standards, are designed to provide wireless networking capabilities for mid-enterprise and service-provider customers with a total user-base or distributed networks of 250-5,000 users.

The FortiAP line will work in conjunction with Fortinets FortiGate multi-threat security appliances acting as the thin access-point controller, to provide a single platform that combines high-performance wireless networking with the industrys broadest integrated network protection. In addition, the FortiGate platform enables customers to have a highly scalable infrastructure with the ability to manage a few to several thousand access points within a wireless LAN.

Fortinets entry into the wireless LAN market gives current customers a way to create converged wired and wireless networks with the same powerful protection under a familiar, simplified and cost-effective management platform with no additional controller investment, said Michael Xie, CTO and founder, Fortinet. New customers will be able to experience a high-performance, secure wireless LAN environment that offers the broadest protection of any consolidated security offering on the market. Overall, todays FortiAP introduction is a key step in Fortinets growth strategy to extend our security reach into broader and deeper parts of the network.

FortiAP Line-up/FortiGate
Controllers

The FortiAP product line is the first manifestation of Fortinets broader secure enterprise class WLAN strategy. As the initial products in the FortiAP line, the single-radio/dual-band FortiAP-210 and the dual-radio/dual-band FortiAP-220 offer reliable coverage, consistent high performance, and competitive and high-value price points as compared to similar products in their class. The FortiAP line can be used to roll out wireless network access to employees, retail locations, warehouses, point of sale locations or hot spots for guest use.

Key benefits of the FortiAP line:

Next-generation, fully 802.11n-compliant access point

High throughput with dual concurrent radio: 300 Mbps-600Mbps

Rich set of enterprise-class AP capability

Ideal for dense office, campus, branch office and retail

Dedicated radio for air monitor to protect against rogue APs for PCI compliance

Internal design conceals antenna to reduce chance of vandalism

Lower cost of deployment with integrated Power over Ethernet (POE)

Highest value at competitive price

All FortiGate appliances from the FortiGate-60 Series on up will be able to act as controllers for the FortiAP, giving customers flexibility and scalability to choose from the broadest range of controllers offered by any single vendor. FortiGate appliances will also be able to act as a single point of management for both wired and wireless LANs. In addition to the existing broad security feature set offered on FortiGate devices, the FortiGate access point controllers will also include WLAN management and wireless IPS.

Each FortiGate platform is capable of delivering centralized management of all access points and devices. From a single console, customers can control network access, quickly and easily update policies, and help monitor regulatory compliance.

Today, wireless LANs are at risk, if not more so, than wired networks. In fact, some recent high-profile hacking cases have involved drive-by trolling of exposed wireless networks of retail establishments, resulting in the theft of thousands of consumer credit card accounts.

Until now, there have been few options for organisations that want to protect both their wired and wireless LANs with the same network and application security solution. The new FortiAP thin access points, together with the FortiGate product line, enable an integrated threat management schema for wireless networks in the same way that Fortinet has been able to provide for wired networks. In fact, wireless traffic needs more protection because it is a shared medium, which provides greater opportunity for network risks such as data leakage, denial of service attacks or the overuse of bandwidth causing network

performance degradation.

The FortiAP/FortiGate

architecture will tunnel all the wireless traffic back to the UTM engine to undergo intrusion prevention and cleansing, identity-aware policy, and Layer 7 application prioritization to achieve a high-performing, fortified wireless LAN infrastructure. In addition, FortiAP uses standards-based CAPWAP (Control and Provisioning of Wireless Access Points) protocol for connecting thin access points as compared to proprietary methods used by competitors.

In addition to mid-enterprise organisations and service providers, retail industry customers will find the FortiAP/FortiGate solution ideal for meeting PCI DSS Wireless Guidelines, which require the detection of rogue wireless access points and intrusion prevention.

Availability

FortiAP thin access points will begin shipping in Q3. Existing customers with valid support agreements will be able to upgrade their FortiGate operating system to act as an enterprise WLAN controller at no additional charge.

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.

###

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, FortiDB, FortiWeb and FortiAP. 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 press release contains forward-looking statements that involve risks and uncertainties. These statements include statements regarding our intentions and plans related to our secure wireless LAN and thin access point strategies and related products and product functionalities. Future circumstances might differ from the assumptions on which such statements are based and results may differ from such forward-looking statements based on changed circumstances, changed strategies and other reasons. All forward-looking statements reflect our opinions only as of the date of this release, and we undertake no obligation to revise or publicly release the results of any revision of these forward-looking statements in light of new information or future events.

FTNT-O