



Barfoot & Thompson Secures Distributed Network with Fortinet

Fortinet (NASDAQ: FTNT) - a leading network security provider and worldwide leader of unified threat management (UTM) solutions - today announced that Barfoot & Thompson, New Zealand's largest privately owned real estate company, has deployed FortiGate-60B appliances at its branch locations in New Zealand. Barfoot & Thompson has also deployed Fortinet's analysis and management appliances, FortiAnalyzer and FortiManager.

Barfoot &

Thompson is New Zealand's largest privately owned real estate company. The company has more than 1,200 salespeople in 65 branches selling residential, lifestyle/rural and commercial real estate throughout Auckland and Northland, and residential property managers in 51 of its branches. Barfoot & Thompson is the market leader in Auckland selling around one in three homes sold by real estate agents.

Barfoot &

Thompson's previous network security solution was complex and expensive to operate, incorporating dual dedicated bandwidth to branch offices, as well as outsourced firewall and outsourced Web filtering services. After consulting with their partner Datacom, New Zealand's largest locally owned full service IT company, Barfoot & Thompson decided to evaluate network security solutions from several major vendors. After carefully evaluating performance, reliability and security capabilities, the Fortinet solution was found to outperform other security appliances, achieving higher throughput while identifying more security threats. The Fortinet solution also allowed Barfoot & Thompson to consolidate and simplify their complex mix of in-house and outsourced network security and hosting arrangements.

I was surprised by the level of functionality and performance available in the Fortinet network security appliances. With the FortiGate appliances we have been able to enormously reduce our data network costs, improve data transfer speeds, and improve data security, said Simon Casey, Chief Information Officer at Barfoot & Thompson. The Fortinet appliances have simplified our network architecture, and we are confident that the Fortinet appliances will block any malicious traffic trying to get into our network.

Barfoot &

Thompson started its Fortinet deployment with two pilot sites followed by a

project phase deployed at 10 branches. During the deployment phase they were able to standardise and automate many of the tasks associated with the deployment to each branch office. Success with this phase gave business stakeholders the confidence to support a full rollout to all other branch offices.

Since the initial pilot, Barfoot & Thompson has deployed FortiGate-60B appliances to all of its 65 branch offices. The appliances have been configured to provide intrusion protection, antivirus, antispyware, Web filtering, VPN connectivity to the head office, load balancing and failover between ADSL lines. Barfoot & Thompson can now add wireless network failover at anytime.

FortiManager-400B centralised management appliance and the FortiAnalyzer-400 centralised reporting solutions are reducing management complexity and allow for much more detailed analysis of network usage as well as easily and automatically creating monthly and ad hoc network reports.

Distributed

enterprises need to protect their networks as much as core networks do. Just because data isn't sitting at the corporate headquarters doesn't mean that it doesn't need to be protected, said Charlie Cote, regional director for Fortinet Australian and New Zealand. Fortinet's end-to-end security solutions allow enterprises like Barfoot & Thompson to protect critical assets no matter where they sit within the network infrastructure.

Fortinet's FortiGate systems are ASIC-accelerated security appliances that integrate essential security and network functionalities such as firewall, VPN, intrusion prevention, Web filtering, antivirus, anti-spam, data leakage protection, application control, traffic shaping and WAN acceleration. All FortiGate systems are kept up to date automatically by Fortinet's FortiGuard Network, which helps ensure protection against the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, other unwanted network traffic and more - around the clock and around the world.

About Fortinet (www.fortinet.com)

Fortinet is a leading provider of network security appliances and the market leader in Unified Threat Management or UTM. Fortinet solutions were built from the ground up to integrate multiple levels of security protection -- including firewall, VPN, antivirus, intrusion prevention, Web filtering, spyware prevention and antispyware -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in five programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, Network IPS and Antispyware. Fortinet is based in Sunnyvale, California.

Copyright

2009 Fortinet, Inc. All rights reserved. The symbols and denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates, including, but not limited to,

the following trademarks: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiDB, FortiWeb and FortiCarrier. Other trademarks belong to their respective owners. Fortinet has not independently verified statements above attributed to other parties, and Fortinet does not independently endorse any such statements.

###

FTNT-O