



National Native Title Tribunal Resolves in Favour of WatchGuard

Sydney – February 3, 2009 – WatchGuard Technologies, a global leader in extensible network security and connectivity solutions, and Perth-based integrator, Expanse IT, have been chosen to supply the National Native Title Tribunal (NNTT) with a secure site-to-site Virtual Private Network for the organisation's mobile workforce requirements and distributed network of offices. Once fully deployed next month, WatchGuard will help save on managed Wide Area Network (WAN) costs, secure inter-site Internet traffic and reduce carbon emissions.

The WatchGuard deployment includes two Firebox X Peak™ 5500e Unified Threat Management (UTM) appliances which will be implemented in the organisation's Perth and Melbourne head offices.

In addition, six Firebox X Edge e-Series55e units will be installed at remote office locations, including Melbourne, Sydney, Cairns, Darwin, Brisbane & Adelaide. These appliances are capable of fully integrated unified threat management, have no user limits and provide 100Mbps firewall throughput and 35 Mbps VPN throughput. They also include Anti-spyware, Anti-spam, Anti-virus, URL filtering, intrusion prevention and deep application inspection. These integrated capabilities have reduced reliance on previously disparate hardware solutions and therefore provide power and license savings to the organisation.

Martin Dart, Information Services Manager at the National Native Title Tribunal, said, "We're building a WAN in the cloud using WatchGuard and its VPN tunneling technology as our primary links. The deployment will also facilitate high availability which the organisation needs to ensure uptime, complete with load balancing and redundancy."

The WatchGuard Peak appliances will facilitate secure access to the Internet and centrally held corporate data from remote locations, including business files, email and web applications. Around 50 laptop users and all teleworkers will also have seamless and secure access to centrally held data through point-to-point access on the VPN.

"WatchGuard will also easily integrate with our in-house software and WAN/LAN configurations, and we have confidence in its ability to manage all of our email and web browsing traffic needs," says Dart.

The Firebox Peak appliances replace Cisco PIX firewalls and a private IP WAN which operated across six interstate offices on slow 96-384KB TPIPS links. The system was unable to provide the cost-effective connectivity required to scale in line with the organisation's remote workforce requirements, and a desire to develop new intranet-based web applications.

"The Cisco firewalls were also inflexible as they had hard coded routing, and we would have required additional devices to achieve full threat protection. We needed control and manageability of our logs and ubiquitous ability from our VPN to facilitate connections from anywhere, anytime. With WatchGuard, our employees can use their home PCs to connect to the server via a simple but secure management console.

"WatchGuard will now form our gateway to route traffic to where it is required to go. In addition, as part of our strategy to ensure business continuity, Melbourne will act as a mirror site to Perth. If Perth goes down, our interstate clients will retain connectivity to Melbourne, with the Firebox replicated and with access to another internet connection for redundancy," says Dart.

WatchGuard Peak appliances offer zero day protection out of the box, with up to two-gigabit-per-second firewall throughput. They provide organisations with full proxy firewall capabilities to prevent attacks from outside of the network as well as viruses, worms, or spyware brought in knowingly or unknowingly by internal users. In addition, the WatchGuard's suite of security services help boost protection in critical attack areas, including intrusion prevention.

In addition, real-time monitoring will allow the organisation to troubleshoot problems instantaneously and ensure that they are diagnosing the correct issues. Centralised management also enables the organisation to enforce security policies across all locations and users.

The National Native Title Tribunal is an Australian Government agency set up under the Native Title Act 1993 to assist with the resolution of native title issues.

In selecting WatchGuard, NNTT worked closely with Expanse IT, a WatchGuard partner headquartered in Perth. Expanse IT reviewed the existing infrastructure and assisted in the correct sizing, specification and selection of the optimum combination of WatchGuard products to meet NNTT's needs.

"Overall, the WatchGuard architecture is simple, attractive and we're very happy with the results to date," says Dart.

About WatchGuard Technologies, Inc.

Since 1996, WatchGuard Technologies, Inc. has been the advanced technology leader of network security solutions, providing mission-critical security to hundreds of thousands of businesses worldwide. The WatchGuard Firebox X family of wired and wireless unified threat management appliances and WatchGuard SSL VPN remote access solutions provide extensible network security, unparalleled network visibility, management and control. WatchGuard products are backed by WatchGuard LiveSecurity Service, an innovative support, maintenance, and education program. WatchGuard is headquartered in Seattle and has offices serving North America, Europe, Asia Pacific, and Latin America. To learn more, visit <http://www.watchguard.com/>