

Tennis Australia Secures Critical Country-Wide Network

"We now have visibility. We can now see any potential attacks in real time and prevent them, and this is very refreshing to say the least. We couldn't do that with our previous firewall so I believe we are now in the best possible position with regards to network protection."

- Steve Wood, Chief Executive Officer, Tennis Australia

About Tennis Australia

Tennis Australia is the sport of tennis' governing body in Australia, with links to affiliated tennis organisations throughout the country. Tennis Australia traces its origins back to 1904 when The Australasian Lawn Tennis Association was formed so that local players could be eligible to compete in the recently created Davis Cup tournament for international teams.

Security Under A Global Spotlight

With a turnover of AUD\$160 million and a mission that encompasses the promotion of tennis at all levels, the organisation is based at Melbourne's world class Rod Laver Arena where 26 courts accommodate everything from casual hire by the public through to staging national and international tournaments. These include The Davis Cup and the Australian Open; one of the world's four Grand Slam events.

Safeguarding the organisation's communications network against disruption is naturally important at all times but critically so for the Australian Open which is held every January at Melbourne Park and attracts 650,000 spectators through the turnstiles and some 10 million unique visitors to the tournament's website. As Tennis Australia CEO Steve Wood points out, "The smooth running of our network is critical to the smooth running of the Open". Wood was a professional tennis player before moving to the business sector and holding a number of positions with leading technology companies, lastly as President of Nortel Australia and New Zealand. He adds that, for the Open, Tennis Australia's 200 staff members are complemented by more than 4,000 temporary staff, a high proportion of whom require access to the network – as do some 1,500 local and international journalists.



Organization:

Tennis Australia

Industry:

Major events, Sports, Leisure

Challenge:

Security & network visibility during peak performance periods – in particular the Australian Open

Solution:

Palo Alto Networks PA-4050 for real time visibility of threats

Results:

- Reduced costs & conserved resources
- Identified & prevent potential threats to the network
- Confidence in network availability when the whole world is watching

“Find me the best network security solution the marketplace has to offer and we’ll buy it.”

Steve Wood,
Chief Executive Officer,
Tennis Australia

Technology to Support Enterprise Risk Management Plan

With Internet threats ever increasing in both volume and sophistication, Steve Wood commissioned the creation of an enterprise risk management program in 2009 to minimise the threat of unwelcome network intrusion. In parallel, he charged his IT team with finding the optimal tool to replace his existing firewall. In his words, “Find me the best network security solution the marketplace has to offer and we’ll buy it”.

Following an exhaustive investigation, the IT team suggested the Palo Alto Networks’ Enterprise Firewall appliance, as demonstrated by the vendor’s Australian Platinum partner, Loop Technology. Wood noted that while Palo Alto Networks was still very new to Australia at that time, the case was compelling and, “We were ready to take the next step and invest. We made the decision and had Loop Technology help us install the system for an evaluation, resulting in us committing to two Palo Alto Networks PA 4050 systems.” The PA 4050 next generation firewall is designed for high speed Internet gateway deployment within an enterprise network environment and Tennis Australia’s deployment includes Intrusion Prevention, Web content management and URL filtering.

Palo Alto Networks’ PA 4050 Deployment in High Availability Conserves Resources

As part of the organisation’s enterprise risk management plan, information security including Palo Alto Networks’ PA 4050 device is now all centralised at Melbourne’s Rod Laver Arena headquarters. Previously Tennis Australia also managed security at its Australia-wide affiliated offices on an individual basis. “Now,” says Wood, “we have it all at our fingertips - here at Tennis Australia, with a redundant device at another location”. This has produced significant savings in time, travel and accommodation costs, as the IT security manager now needs to visit each of the remote offices only occasionally.

Visibility for Threat Visibility and Prevention

The greater benefit though, is delivered by the PA 4050’s level of reporting – which the previous firewall couldn’t offer – and gives Tennis Australia greater confidence in staging a technology incident-free Australian Open. As Steve Wood explains, “We now have visibility and the tools to monitor our firewall activity effectively. We couldn’t do that with our previous firewall so I believe we are now in the best possible position with regards to network protection.”

Next Generation Firewall Technology for Peace-Of-Mind

Leading up to the 2011 Australian Open, Tennis Australia’s Palo Alto Networks solution had been in use for four months and as Wood says, “There could not have been a better period of live stress testing ahead of our most critical event. The system is working perfectly despite our complex environment and this is very comforting.”

He attributes the success of the implementation to good planning and the successful partnership between Palo Alto Networks, Loop Technology and his own people working together to accomplish an overnight implementation. “While we are not first movers with technology, we are fast followers. Loop Technology and Tennis Australia did all the right pre-implementation work – understanding the environment; making sure there would be no hitches with our remote access via Citrix; connectivity for our external vendors and services; and so on.” He concluded, “The Palo Alto Networks solution has done a great job helping us meet our enterprise risk management plan goals”.

