

# CASE STUDY

## Southern Cross Hospitals



# Hospital Network Finds Prescription for Healthy Network Security



Southern Cross  
Hospitals

---

“One of the things we liked about the Palo Alto Networks Next-Generation Firewalls is that we could enable all the features we wanted and get the same high throughput. That meant a consistent user experience at the sites.”

Tony Allwood | IS Solution Architect | *Southern Cross Hospitals*

---

### Customer Overview

Southern Cross Hospitals comprises a national network of ten wholly-owned and eight joint venture medical facilities, it provides accreditation to 925 credentialed surgeons and anesthetists and surgical healthcare for 75,000 patients annually, including publicly-funded patients receiving services under contract for District Health Boards and the ACC, plus a significant number of charitable surgeries. It is the country's largest private surgical sector employer of registered nurses and continues to expand the size and scope of its capabilities to provide a growing number of New Zealanders with high-quality hospital care.

### Industry

Healthcare

### Challenge

Improve Internet performance and site resilience for individual hospitals while maintaining central control to ensure high levels of network security.

### Solution

Palo Alto Networks® Next-Generation Security Platform to distribute individual next-generation firewalls across multiple sites, with centralized policy management and visibility to prevent cyber threats and unwanted network traffic from compromising hospital systems.

### Subscriptions

Threat Prevention, URL Filtering (with PAN-DB), WildFire™, Panorama™

### Appliances

PA-3020 (8), PA-500 (10)

### Results

- Increased network visibility and control over Internet traffic
- Improved Internet performance and resilience for multiple sites
- Consistent implementation of rule sets for stronger security
- Reduced configuration changes and updates
- Strengthened protection against zero-day exploits

### Story Summary

Southern Cross Hospitals is New Zealand's largest network of private surgical hospitals. To consistently deliver excellence in health services, Southern Cross Hospitals relies on a high-performing, highly available information network to connect facilities across the country. With a growing number of computer, medical, and facility management devices connected to its network, Southern Cross Hospitals faced growing cyberthreats from many directions.

By installing Palo Alto Networks Next-Generation Security Platform, Southern Cross Hospitals updated its security infrastructure to prevent sophisticated attacks, such as zero-day exploits, from compromising critical hospital systems. The new platform enables Southern Cross Hospitals to deploy next-generation firewalls at each of its hospital facilities, yet manage the infrastructure from a central vantage point. This dramatically improved Internet performance and resilience, while improving visibility and control of network traffic.

### New Life for Network Security

Southern Cross Hospitals is a not-for-profit healthcare organization that offers predominantly elective surgery through a network of ten wholly owned and eight joint venture medical facilities across New Zealand. It is the largest such provider in a competitive market that demands excellence and affordability. This applies not just to healthcare services, but also the information network underpinning those services.

Tony Allwood, IS Solution Architect for Southern Cross Hospitals, explains, “Our previous approach was based on a wide area network (WAN). Local WAN circuits are expensive, so there would have been significant costs to increase our WAN bandwidth. But with high speed Internet becoming less expensive, there was a business case to deploy firewalls to each site. This provides each hospital with direct Internet access using a design that improves security and resilience.”

### Thorough Examination Leads to Better Outcomes

Southern Cross Hospitals conducted a thorough evaluation of several network security offerings, ultimately choosing The Palo Alto Networks Next-Generation Security Platform.

---

“WildFire is a real point of difference for Palo Alto Networks. We’re now much more able to deal with zero-day exploits and malware packaged in ways that traditional antivirus software can’t keep up with.”

**Tony Allwood** | IS Solution Architect | *Southern Cross Hospitals*

---

Healthcare is unique in that many specialized devices may be connected to the one network—everything from PCs and laptops, to vital signs monitors and building management systems.

The Palo Alto Networks platform consists of a Next-Generation Firewall, Threat Intelligence Cloud, and Advanced Endpoint Protection. It delivers application, user, and content visibility and control, as well as protection against cyber threats. The threat intelligence cloud provides central intelligence capabilities and automates the delivery of preventative measures against cyberattacks.

Allwood said, “During our evaluation, we saw solutions that had promise, but if we turned on the features needed, performance would drop. With the Palo Alto solution we could enable all the features needed and get the same high throughput. That meant a consistent user experience at all sites.”

Southern Cross Hospitals deployed seven PA-3020 and nine PA-500 next-generation firewalls at each of its healthcare facilities. The PA-3020 firewalls serve larger sites with robust, 24/7 operational requirements, while the PA-500 firewalls were ideal for smaller sites with fewer users. The deployment also includes subscriptions for Threat Prevention, URL Filtering with PAN-DB, and WildFire.

In addition, Southern Cross Hospitals manages the entire distributed security infrastructure with Palo Alto Networks Panorama network security management.

Allwood explains, “Panorama enabled us to get the best of both worlds. We maximize performance and resilience for our facilities by distributing network security to each site, yet it’s still like having one Internet link from a management point of view. It’s a lot easier with a centralized platform to build your rule sets and make sure they’re consistent across all the sites.”

### **Cure for Zero-Day Exploits**

With the Palo Alto Networks Next-Generation Security Platform, Southern Cross Hospitals improved visibility of network traffic. It also strengthened protection against a host of sophisticated cyber threats.

“WildFire is a real point of difference for Palo Alto Networks,” says Allwood. “We’re now much better able to deal with zero-day

exploits and malware packaged in ways that traditional antivirus software can’t keep up with.

“It’s a comfort that we benefit from what other Palo Alto Networks customers are seeing through the WildFire cloud. With the recent rise in ransomware and some big zero-day exploits, we’re confident Palo Alto Networks is preventing issues that we might otherwise have faced if we were relying solely on a signature-based antivirus solution.”

### **Forensics Uncover Potential Vulnerabilities**

Panorama further enhances the value of network visibility for Southern Cross Hospitals with detailed logging and forensic capabilities.

“Panorama gave us the insights and tools that allow us to tidy up the network and circumvent any security issues before they arise,” says Allwood.

Network security management with Panorama also enables the IS team to accelerate time to deliver new and updated services across the hospital network.

He adds that Panorama also simplifies troubleshooting. Instead of sifting through data from each site the IS team has a single vantage point from which to find and quickly resolve an issue.

### **Healthy Network Means Happy Customers**

By enabling Southern Cross Hospitals to distribute individual firewalls to each of its facilities, the Palo Alto Networks platform helped the organization avoid a substantial increase in WAN costs.

Allwood explains, “With the Palo Alto Networks platform we improved network performance for our hospitals and strengthened our overall business resilience. We’ve also been able to ensure patients Internet access (such as YouTube) without impacting our corporate or clinical systems.

“Our end users are happier, our managers are happier, and our IS team is happier because we’re not worrying about the network. Instead, we’re able to focus on strategic projects to help improve hospital services.”