New Zealand Utility Bolsters Security Posture, Cost Savings and Productivity Gains with Palo Alto Networks

"The visibility we have with the Palo Alto Networks Next-Generation Security Platform is amazing. We have virtually eliminated our security infections. Our security risk posture is tenfold what it was before we migrated over to Palo Alto Networks."

Andy Simpson | Head of Information Technology | *The Lines Company*

Industry
Utility

Challenge
Address aged Fortinet® firewalls security deficiencies and lack of transparent visibility across network infrastructure by migrating to an integrated security platform.

Solution
Palo Alto Networks® Next-Generation Security Platform protects data centres, satellite offices, and hundreds of SCADA devices from security intrusions, malicious cyberthreats and ransomware.

Subscriptions:
Threat Prevention, URL Filtering (PAN-DB), WildFire, GlobalProtect

Appliances:
Palo Alto Networks Next-Generation Firewalls used for securing two main corporate office locations in high availability design and supporting the SCADA power grid network.

Services
Partner-Enabled Premium Support

Results
- Addressed 100+ resident security vulnerabilities not identified by existing products
- Reduced time to complete incident reviews tenfold
- Avoided $50,000 in IPS and network antivirus scanning upgrades
- Realized 40% reduction in network bandwidth consumption
- Shaved number of user security rules by 30%
- Bolstered security posture dramatically

Background
The Lines Company delivers electricity through its electricity network grid to citizens and businesses spanning a vast and rugged region of the North Island of New Zealand. The distribution area covers 13,700 square kilometres and is one of the largest network areas in New Zealand with no major urban centre. About two and a half years ago, The Lines Company determined that its IT infrastructure was nearing end of life and needed to be revitalized from the ground up. WAN, infrastructure hosting, server and storage, user workspace, applications and the billing system were all due for a major overhaul.

Summary
The new Head of Information Technology at The Lines Company, Andy Simpson, embarked on a series of initiatives not only to refresh the organization's IT infrastructure but also to rethink each of the areas as well. One of the biggest challenges Simpson and his team tackled was network security. Management of the company's firewalls was time-consuming, and the IT team had to remediate security issues on a daily basis.

After evaluating different options, The Lines Company selected the Palo Alto Networks Next-Generation Security Platform. In addition to bolstering its security posture dramatically, The Lines Company improved the productivity of its IT team with an approximate savings of a half a full-time employee (FTE) and avoiding upgrades in its IPS and network antivirus scanning software a combined estimated savings of $100,000 in year one. The Lines Company also realized upwards of a 40 percent reduction in network bandwidth consumption whilst shaving the number of security rules by 30 percent.

IT Revitalization Includes Security
When Andy Simpson joined The Lines Company about two and a half years ago, he faced a significant set of challenges. The organization's IT infrastructure had reached end of life and needed to be rebuilt from the ground up. "We literally had IT infrastructure components that dated from the 1990s," he says.

A community-owned utility that serves customers scattered across a highly rugged landscape on the North Island of New Zealand, The Lines Company recruited and hired Simpson because he possessed the know-how and experience to help them revitalize their IT infrastructure. Security was one of the top issues he needed to tackle.

The organization relied on Fortinet security firewalls, and there were various issues with them that Simpson and his team

"All of the different components that comprise the Palo Alto Networks Next-Generation Security Platform give us the ability to manage security in a highly automated fashion, enabling us to get on to other tasks that allow IT to be more visible and productive within the business."

Andy Simpson | Head of Information Technology | *The Lines Company*

wanted to solve. In addition to being time-consuming to manage, and failing to provide transparent visibility across the organization's entire network infrastructure, the Fortinet firewalls were not configured to meet business continuity requirements.

A Completely New Approach to Security

In mid-2015, Simpson began a search to replace or upgrade the Fortinet firewalls. "We weren't simply looking for firewalls, but rather we wanted a platform that would give us a much more holistic approach to security, and would be the best fit for the newly-designed, highly available infrastructure," Simpson remembers. He and his team performed due diligence, looking at five different options that included Cisco®, F5®, Fortinet, Juniper®, and Palo Alto Networks®.

"We wanted to take a completely different approach to how we manage security, and we elected to do a four-week trial with Palo Alto Networks," Simpson says. "The ease of management of the Next-Generation Firewalls was very impressive. What really sold us was the fact that Threat Prevention and WildFire pinpointed a list of over 100 security infections that had been within our environment, in many instances, for a long period of time. It was truly an eye opening investigation as to the level of protection the existing combination of antivirus and firewalls provided." Palo Alto Networks WildFire™ is a cloud-based threat analysis service that analyses files and links globally and designates those that haven't been seen before for further investigation. Threat Prevention inspects and stops cyberthreats that move laterally across the network.

The Details of Protection

Getting approval to move forward with the acquisition of the Palo Alto Networks Next-Generation Security Platform was relatively simple for Simpson following submission of the business case. "Our CFO Kevin Barnes understood the importance of maintaining a robust security posture without incurring the high cost of personnel expenditure," he says. Simpson also said "CryptoLocker was ravaging other organizations at about the same time, and we believed that the Palo Alto Networks Next-Generation Security Platform was the best defence at this time."

Simpson and his team also combined a change of telco provider with the firewall replacement realizing a substantial cost reduction in telecommunications costs per month. With the help of Palo Alto Networks NextWave Channel Partner Network Service Providers (NSP) Limited, The Lines Company, after several months of planning and new telco circuit implementations, completed the full migration on to the Next-Generation Security Platform, all within less than one month. "We have a long-standing relationship with Palo Alto Networks partner NSP, and they have proven to be a very good technology partner for us," Simpson says.

To protect two data centre locations, The Lines Company has two Palo Alto Networks next-generation firewalls that are configured redundantly to ensure business continuity in the event of a seismic event or a facility failure. For The Lines Company's six depot locations, all traffic is routed to the two data centre locations for full visibility and protection of the enterprise. NSP worked with Simpson and his team to create various user and application rules based on security and business policies. "An entire building can be lost, including IT services and critical 0800 phone lines, and the business will still operate," Simpson comments. "ICS staff are supported between the two sites and a separate Palo Alto Networks platform is deployed for secure access to radio and critical SCADA equipment".

A virtual wire deployment is used by The Lines Company in intersite configuration to allow scanning of traffic across the organization's private fibre circuit and VLAN's. Border gateway protocol (BGP) is used by the service provider of The Lines Company for failover in the event the primary telecommunications fibre circuit fails. Routing information protocol (RIP) is used by the Palo Alto Networks next-generation firewalls, along with internet service access, in the event there is a primary connection failure. Open shortest path first (OSPF) is used by remote depots for connectivity to the two primary office sites.

For protection of the segmented Supervisory Control and Data Acquisition (SCADA) network, The Lines Company also relies on Palo Alto Networks next-generation firewalls. Industrial Control Systems (ICS) protocols for SCADA have a separate secured connection that allows only specific controlled access to devices. SCADA-controlled PCs have no internet presence; rather, they rely on logistically separated jump boxes for transmission of data to outside sources. In the event of an interruption in services to

"The Palo Alto Networks Next-Generation Security Platform is one of multiple security toolsets that we use to protect our SCADA network.""

Andy Simpson | Head of Information Technology | *The Lines Company*

the control room, a separate Palo Alto Networks next-generation firewall platform is installed to ensure The Lines Company maintains availability to SCADA devices.

Subscribing to Business Value

One of the challenges The Lines Company wanted to overcome was a previously complex and time-consuming task of developing and managing rules in the aged Fortinet environment. "We were actually creating rules that circumvented existing rules," Simpson states. "And this was entirely because it was so difficult to manage all of the ongoing requirements from staff during our new infrastructure and application deployments, as well as supporting a growing MEP business unit. It simply wasn't possible to do with a traditional firewall. With the User-ID™ technologies and App-ID™, we are easily able to filter all of the way down to an actual user and individual application, looking at things such as a user's session on the network." With Palo Alto Networks, Simpson reports his team reduced the number of security rules by 30 percent. "And we're much better protected at the same time," he adds.

In addition to WildFire and Threat Prevention subscriptions, The Lines Company also uses URL Filtering (PAN-DB). Simpson really likes how he can use it to block group-based streaming media content. "The results have been fabulous," he says. "We've been able to reduce network traffic by 40 percent. We also have immensely better visibility across our users and what URLs they are visiting." Active Directory® integration with URL Filtering is another capability Simpson finds useful. "We can quickly and easily create Active Directory profile groups for specific streaming media use cases," he says. "We particularly like the fact that we can tie the access controls directly into our Active Directory groups. It saves us a lot of time and work configuring manual rules."

GlobalProtect™ network security for endpoints is used to protect remote users, mobile devices, and Secure Socket Layer (SSL) connections. "Our integrated security platform approach is taken down to the level of the endpoint with GlobalProtect," Simpson observes.

Protecting its SCADA network is a top priority for The Lines Company. "For some of our customers such as hospitals and medical centres, we're talking about critical scenarios if the power stays off," Simpson says. "In other instances, we're talking about important infrastructure such as irrigation systems for farmers and water systems for municipalities. The Palo Alto Networks Next-Generation Security Platform is one of multiple security toolsets that we use to protect our SCADA network."

Migration to the Palo Alto Network Next-Generation Security Platform is generating cost savings and productivity gains for The Lines Company on a couple of fronts. As Palo Alto Networks takes less time to manage, Simpson estimates he is saving half a full-time headcount, approximately $50,000 annually. "Not only did we initially lack visibility, but we were constantly cleaning terminal servers and user laptops and desktops on a daily basis," Simpson says. "When I first started the IT staff, at times, did not know systems were compromised except for the fact that performance was impacted. The visibility we have with the Palo Alto Networks Next-Generation Security Platform is amazing. We have virtually eliminated our security infection rate. Our security risk posture is 10 times what it was before we migrated over to Palo Alto Networks."

A second cost savings benefit is connected to the ability of The Lines Company to avoid upgrades of its intrusion protection system (IPS) and network antivirus scanning software across both data centre locations, estimated at approximately $50,000 in hardware and software costs.

Threat remediation is another area where The Lines Company is seeing value. For example, the malware and infections that Simpson's team found through Threat Prevention and WildFire, when they were first deployed in the summer of 2015, took an entire week to remediate, and this involved several staff members and contractors. This added up to more than 200 staff hours, considerable cost and unplanned work. And when it comes to investigating security incidents, the reporting capabilities in the Next-Generation Security Platform streamlines the process. Previously, it took Simpson and his team up to five hours to pull individual data and security logs together from different sources for a consistent view of a single event. With Palo Alto Networks in place, they can perform the same task in 30 minutes, a tenfold reduction in time.

"Our integrated security platform approach is taken down to the level of the endpoint with GlobalProtect."

Andy Simpson | Head of Information Technology | *The Lines Company*

The Lines Company has seen significant improvements following deployment of the Palo Alto Networks Next-Generation Security Platform. The following assessment was provided by industry auditors following their completion of a Cyber Security Review last year: "A number of changes have recently been made to the corporate IT infrastructure. These changes provide an excellent platform for continuing to improve the overall security posture of The Lines Company. The corporate network architecture, the selected firewalls, the backup and replication capability and general choice of technologies are consistent with an organisation committed to improving their security posture."

Sleeping at Night With Full Visibility

When asked to summarize his recommendations for peers who are rethinking their security networks and looking at Palo Alto Networks, Simpson notes they "shouldn't complete a proof of concept with Palo Alto Networks on a Friday or right before they plan to go on an extended break. They will not be able to sleep at night knowing what threats they have currently lurking in their existing network now discovered."

Simpson also likes the fact that Palo Alto Networks is easy to manage. "My staff and I don't need to spend weeks configuring the firewalls for the outcome we need," he sums up. "Once we went live, all of the reporting and out-of-box functionality works as designed. There's really little configuration other than firewall rules and specific connection-related issues to tackle. All of the different components that comprise the Palo Alto Networks Next-Generation Security Platform give us the ability to manage security in a highly automated fashion, enabling IT to be more productive and visible within the business."