Australian National Rail Operator Conquering the Tyranny of Distance while Halving Annual Networking Costs

Ip.Glass Case Study

"By deploying Fortinet, we're cutting our entire network costs in half. You don't often go to your CFO and say, 'actually, we're going to get something better for less'. And when I say less, I mean that by deploying Fortinet, we've cut our annual network costs in half. All of a sudden, our CFO is really excited about networking."
– Paul Williams, CIO, Pacific National

Customer
Pacific National

Industry
Rail freight

Location
Sydney, Australia

Business Impact

- A 50% saving on annual networking costs and a two-year ROI
- Improved security posture through granular security controls and greater visibility of network traffic
- Improved user experience and employee health and wellbeing at remote sites
- Improvements in network performance, redundancy, and resilience
- Ability to provision connectivity to new sites in days rather than months.

Pacific National is Australia's largest private rail freight company, transporting intermodal containers, grain, steel, coal and other bulk commodities and playing an essential role in supporting Australia's supply chain. With 3,400 employees and 86 sites across the country, Pacific National represents about 70% of all intermodal traffic in Australia and runs more than 800 weekly train services.

It's not just the scale and remoteness of Pacific National's operations that creates challenges. "Rail is deceptively simple from the outside and devilishly complicated from the inside. There's a lot of complexity involved in maintaining what in rail is called being a 'healthy train' - that means you're on track and you're on time," says Paul Williams, Chief Information Officer at Pacific National.

Core to Pacific National's operations is its Transport Management System (TMS), a bespoke system that has grown over 25 years to manage most aspects of the business – "there's virtually nothing we can do without TMS being up and running," explains Williams.

The company had been running on a traditional hub-and-spoke private MPLS network that was very costly to manage and offered low bandwidth and limited redundancy, with most sites connected via one piece of fibre to a single exchange. However, plans to modernise its TMS with best-of-breed replacement components from the marketplace meant that Pacific National needed a more agile and responsive network. The network also needed to provide the robustness, security and redundancy required to operate Pacific National's mission-critical applications.

Ip.Glass Case Study

To emphasise the criticality of the network and core systems, in disaster recovery testing Pacific National works to a four-hour recovery time objective on its TMS. "Our business could probably survive a couple of hours before we start having to cancel trains," says Steve Carroll, Information Technology Infrastructure Manager, Pacific National.

Security-first SD-WAN

As a critical infrastructure organisation, cybersecurity was critical for Pacific National in selecting a replacement networking technology. Having a firewall deployed to every location was a key factor in the decision to choose Fortinet's Secure SD-Branch solution, providing greater security enablement at the edge and in Pacific National's data centres, as well as giving their local breakouts quicker internet speeds and better Wi-Fi at all 86 sites.

"Fortinet has a long history in security, and by choosing a vendor whose strong suit is security that really opened up a whole range of other benefits," says Williams.

Working with Fortinet partner and network and security services provider Ip.Glass, Pacific National deployed a Fortinet Secure SD-Branch solution that consists of a FortiGate next-generation firewall, FortiSwitch switch and FortiAP wireless access points at all 86 sites, together with FortiExtender cellular gateways at those sites with 4G and 5G access. In the data centre, Pacific National upgraded several firewalls, proxies and routers to Fortinet solutions.

"The SD-WAN project was an absolute joy, working with Ip.Glass and Fortinet, giving our engineers new technology to play with, and being able to modernise the technology across our whole network landscape from a data centre and site perspective. We see Ip.Glass as an extension of our IT team; their engineers really understand our business and our network, they came to every site with us, and they've shown a passion for it," says Carroll.

While there was initially some apprehension about deploying so many remote firewalls, having Ip.Glass provide 24/7 management and monitoring of every Fortinet security and network device has allayed that concern. The ease of management provided by Fortinet's single pane of glass means that Pacific National is reaping the benefits of granular control and visibility of security and traffic at each site, without impacting on network speed for users. It's also provided separation between Pacific National's IT and OT networks, which is fast becoming the default standard in cybersecurity.

"Essentially, you don't want any of the traffic going across from your office network into your SCADA network. You want that really locked down, so having a firewall and being able to put virtual networks in place at each site has delivered significant benefits. We now also have local internet breakout, so if a user is connecting to an Internet service like YouTube, the traffic doesn't have to go back via the firewall in our data centre, it goes straight out to the internet, which is infinitely faster and more cost-effective. From a cybersecurity perspective, we're thinking of bad actors as not just people outside our network trying to get in but people inside our network trying to exploit things as well, so controlling every port on every switch everywhere, and not having those open for anyone to connect to is critical for our security posture," says Williams.

Solving the Tyranny of Distance

While ensuring the security and continuity of services and operations is core to the objectives of Pacific National's IT team, the impact on users is just as important. One of the challenges has been in providing connectivity and services to train drivers, and ensuring their health and wellbeing, particularly in remote locations.

In describing that remoteness, both Williams and Carroll cite the example of Cook, which is on the longest straight section of railway in the world – 478 kilometres – in the Nullarbor. Train crews might spend up to three days at a time in Cook.

"Before Fortinet, drivers staying in our barracks in Cook couldn't get a decent internet connection. Now with Fortinet we've been able to deploy redundant connections and give all our drivers iPhones so they can FaceTime their families and they can watch Netflix. For their mental health and wellbeing that's of paramount importance to us – not from a technology perspective – but looking after our employees and keeping them safe," says Carroll.

"The benefits of Fortinet Secure SD-WAN and Secure SD-Branch are that every site now has Wi-Fi, higher bandwidth, faster internet speed and redundant connections so if a network link goes down, there's 4G that they can fall back on."

As a result of the project, Pacific National has had a major reduction in network outages due to deploying a highly redundant solution including multiple active-active internet links to each site. The combination of links has been designed to provide both carrier-level redundancy and a mix of wired and wireless internet links. Remote locations, such as Cook and other sites, also significantly benefit from the Starlink satellite connection providing low latency high-speed connection in the areas not serviceable by NBN, fibre and 4G technologies.

Reducing Cost and Increasing Agility

While Pacific National now has diverse carrier services available for both fibre and cellular connections to each site, it has been able to reduce its annual carriage and managed services by 50% compared to its previous network technology solution. Ip.Glass has removed the administrative load on Pacific National by seamlessly managing the diverse set of telecommunications providers on its behalf.

"By deploying Fortinet, we're cutting our entire network costs in half. You don't often go to your CFO and say, 'actually, we're going to get something better for less'. And when I say less, I mean that by deploying Fortinet, we've cut our annual network costs in half. All of a sudden, our CFO is really excited about networking," says Williams.

However, Willams also points out the agility the new SD-WAN infrastructure has given Pacific National.

"In the past on our private network, depending on where it was, we'd have to wait months to get fibre run to that site. Now, it's a lot quicker to stand up a site. We can send a rack out to a site with all the switches, firewalls and other equipment, and get that site up and running within days."

That agility also comes with the advanced security capabilities that are a must-have for a critical infrastructure provider essential to Australia's supply chain. That will enable Pacific National to continue to execute on its systems modernisation strategy, ensuring mission-critical services continue to operate as the company increases the level of automation and adoption of advanced technologies and applications across the business.

"We've got a more reliable, robust, agile, cost-effective and higher bandwidth network than we had before. So, as a result, deploying Fortinet was a complete no-brainer," concludes Williams.

About Ip.Glass

Ip.Glass are a specialist network and network security services provider, delivering complex enterprise services, while maintaining flexibility, agility and being easy to engage and work with.

Phone: 1800 945 305

Email: getintouch@ipglass.com.au

**Address: Office 19, 33 Waterloo Road
Macquarie Park, NSW Australia**

Web: https://ip.glass