

CASE STUDY · CYBERSECURITY · CONSTRUCTION

HOW HORNIBROOK NGI

REBUILT ITS SECURITY FOUNDATIONS

WITH SPRINT NETWORKS

From a vulnerable network to controlled, monitored access in one week.

1 week

From first audit in Lae to full go-live

4 layers

Firewall, secure zones, remote access and zero trust

24/7

Monitored by the Sprint Networks team

0

Security incidents in the six months since go-live

AT A GLANCE

Hornibrook NGI spotted suspicious activity on its network. Its main firewall was old and had known weak spots. Sprint Networks flew to Lae, found the gaps and rebuilt the network's security in one week, without slowing the business down.

THE PROBLEM

An outdated firewall with known vulnerabilities, suspicious activity on the network and remote access open to the internet.

[Read the challenge →](#)

THE SOLUTION

A next-generation firewall, secure network zones, protection for remote staff and zero-trust access to the ERP.

[See what we built →](#)

THE RESULT

Protection in every direction, a faster ERP for every user, 24/7 monitoring and no incidents since go-live.

[View the results →](#)

INSIDE

[01 The challenge](#)[02 One week](#)[03 The solution](#)[04 Safe access](#)[05 Results](#)[06 Talk to us](#)

01 THE CHALLENGE

A VULNERABLE NETWORK COULD NOT WAIT

Hornibrook NGI is a construction and civil engineering business with its head office in Lae and teams working on projects across Papua New Guinea. Its people rely on the ERP system for projects, purchasing, stock, payroll and finance, from the office, from site and on the road.

In early 2026, Hornibrook detected suspicious activity on its network. The firewall protecting head office was already past its supported life. The business was running on a network that could be compromised at any time, and it needed help fast.

WHAT SPRINT NETWORKS FOUND



An outdated firewall

The firewall software had not been updated and carried publicly known security holes.

Why it matters: attackers scan the internet for exactly these devices. An unpatched firewall can become the way in.



A flat network

Computers, servers, Wi-Fi, printers and cameras all sat together with nothing between them.

Why it matters: one infected laptop could reach the ERP server and everything else.



Open remote access

Remote access was open to anyone on the internet, protected by a password alone.

Why it matters: a guessed or stolen password could open the door to the whole business.

On top of this, the firewall was recording events, but nobody was reviewing them. Warning signs could go unnoticed for weeks.

WHY OLD FIREWALLS BECOME A TARGET

A firewall is the front door of a business network. Like any software, it has bugs, and vendors release updates to fix them. The moment a fix is published, attackers know exactly where to look.

Automated tools scan the internet around the clock for firewalls that have not been updated. In Lae, Port Moresby or Sydney, the risk is the same. The fix was not just a new box. Hornibrook needed a security foundation built around how the business actually works.

02 ONE WEEK, START TO FINISH

EVERY DAY EXPOSED WAS A DAY AT RISK

Speed mattered. Sprint Networks engineers flew from Sydney to Lae in March 2026 and worked on site with Hornibrook's team until the job was done.



On site
 Engineers in Lae, side by side with Hornibrook's IT team

After hours
 Changeover done outside the working day, so the business kept running

Same week
 Remote staff connected and monitoring live before the team left

WHAT CHANGED FOR HORNIBROOK

AREA	BEFORE	AFTER
Firewall	✗ Ageing firewall with known vulnerabilities	✓ Next-generation firewall with active security controls
Inside the network	✗ One flat network where everything could reach everything	✓ Separate security zones with controlled traffic paths
Remote access	✗ Open to the internet	✓ Zero-trust access with multi-factor sign-in
Staff on the road	✗ No security checks for the remote employees	✓ Same security checks wherever they work
ERP performance	✗ Competed with all other network traffic	✓ ERP traffic identified and given priority
Visibility	✗ Logs recorded but not reviewed	✓ Sprint Networks 24/7 monitoring

03 THE SOLUTION

BUILD SECURITY AROUND HOW WORK GETS DONE

The new design had to work for one main office, project sites that change, and staff who work away from the office. Every path into the business had to be checked and controlled.

A next-generation firewall at head office

Sprint Networks replaced the ageing firewall with a next-generation firewall. It does not just decide who gets in. It looks inside the traffic too.

- ◆ Spots and blocks known attacks
- ◆ Stops harmful files and ransomware
- ◆ Blocks phishing and bad websites
- ◆ Recognises important business traffic
- ◆ Cuts unwanted traffic from overseas

Secure zones inside the network

Think of an open-plan office turned into rooms with locked doors. The network was split into separate zones, and traffic between them must pass the firewall.

If one device is ever compromised, the problem stays in one place instead of spreading across the business.

Servers

ERP and business systems, approved users only

Staff

Office computers and laptops

Wi-Fi and guests

Internet only, no route to business systems

Devices

Printers and cameras, kept apart



WHAT THE HORNIBROOK FIREWALL CONTROLS

04 PROTECTING ACCESS

SAFER WORK FROM ANYWHERE

For Hornibrook leadership, the question was simple: can our people do their work without leaving the business open to risk? The answer had to work at head office, on site, at home and on the road.

IN THE OFFICE

Inspected by the firewall

Everything going in and out of head office is checked by the next-generation firewall.



ON SITE, AT HOME, ON THE ROAD

Protected in the cloud

A small security client on each laptop applies the same checks wherever a person works, on any connection.



REACHING THE ERP

Zero trust, every time

Staff sign in with multi-factor authentication and reach only approved applications, never the whole office network.



AROUND THE CLOCK

Watched 24/7

Sprint Networks monitors the whole environment and acts fast on anything unusual.



HOW A REMOTE LOGIN WORKS NOW

1

Staff member

opens their laptop on site, at home or on the road



2

Identity checked

multi-factor sign-in proves it is really them



3

Traffic checked

the security client screens for threats



4

ERP only

access to approved apps, never the whole network

SECURITY THAT DOES NOT SLOW THE BUSINESS

Internet links in PNG can be limited, and one big download or video call can make the ERP feel slow. Sprint Networks set the network to recognise ERP traffic and put it first, so people in the office, on site or working remotely get a fast, steady connection while everything is still checked for threats.

What if a password is stolen?

The attacker still has to pass multi-factor sign-in, and even then could only reach specific applications, not the network.

What if a laptop is infected?

Secure zones keep the problem contained, and 24/7 monitoring means Sprint Networks knows about it fast.

05 THE RESULTS

PROTECTED IN EVERY DIRECTION

Six months after go-live, Hornibrook runs on a network where every path in is checked, the ERP stays fast, and someone is always watching.

0

Incidents since go-live

No security incidents in the six months since March 2026.

7 days

From audit to live

The window of risk was kept as short as possible.

24/7

Eyes on the network

Unusual activity is spotted and acted on, day or night.

Open doors closed

Outdated software gone and remote access no longer exposed to the internet.

Problems stay contained

Secure zones stop one compromised device from spreading to the rest.

Business keeps moving

ERP traffic comes first, so staff work from anywhere without slowdowns.



We were in dire need of a security solution that would best fit our network and Sprint Networks gave us a solution that did that and more. The team at Sprint Networks are professional, friendly, and extremely knowledgeable.

Stephanie Eka · IT Manager, Hornibrook NGI

SERVICES DELIVERED

Security audit ↗

Next-generation firewall ↗

Secure network zones ↗

Secure remote work (SASE) ↗

Zero-trust ERP access ↗

ERP traffic priority ↗

24/7 security monitoring ↗

THE LESSON FOR PACIFIC BUSINESSES

A firewall is not a set-and-forget device. Without updates, good design and someone watching it, it quietly turns from protection into a weak point. Construction, mining, logistics and energy businesses across the Pacific share Hornibrook's set-up: one main office, sites that come and go, and people who need core systems from anywhere. Hornibrook acted quickly when the warning signs appeared, and that made all the difference.

REVIEW THE PATH INTO YOUR BUSINESS

An old firewall, a flat network or a remote login protected only by a password can each become a real risk, especially when your core systems support people across many sites.

IS YOUR BUSINESS IN THE SAME POSITION?

☐ Your firewall is several years old, or nobody is sure when it was last updated☐ Staff reach your ERP or files from home or project sites☐ Remote access relies on a username and password alone☐ Every device in the office sits on the same network☐ Nobody watches your network outside business hours☐ You have noticed strange logins, slow systems or odd emails

Tap the boxes that apply. Ticked even one? It is worth a conversation.

BOOK A FREE SECURITY CHECK

A senior Sprint Networks engineer will look at your network, show you where the gaps are and explain how to close them, quickly and with minimal disruption.

[Book your free check →](#)[Chat on WhatsApp](#)

VISIT OUR WEBSITE

sprintnetworks.com.au

EMAIL OUR TEAM

info@sprintnetworks.com

EXPLORE MORE CASE STUDIES

sprintnetworks.com.au/case-studies

CONNECT ON LINKEDIN

linkedin.com/company/sprint-networks

About Sprint Networks. Sprint Networks designs, secures and manages business networks across Papua New Guinea, Fiji, the Solomon Islands and the wider Pacific, with offices in Port Moresby and Sydney. We are vendor-agnostic and test every solution in real Pacific conditions before it reaches a client's network.