Sprint Networks

Paradise PRIVATE HOSPITAL



CASE STUDY · HEALTHCARE · PORT MORESBY, PNG

A MORE RESILIENT AND SECURE NETWORK FOR PARADISE PRIVATE HOSPITAL

A network with no single point of failure, protection at every layer, and safe access to patient systems from home.

REDUNDANT
Each internet link on its own firewall

PROTECTED
Network, remote access and email

ZERO TRUST
Remote HMS access from checked devices only

INCIDENT FREE
No security incidents since go-live

PROBLEM →
A growing hospital on a basic network, with two internet links through one device.

SOLUTION →
Redundant firewalls and core, zero trust remote access, plus email security.

RESULT →
Patient systems stay online and protected, and doctors can work safely from home.

70,000+	24/7	170	PNG
patients a year	emergency care	staff	Port Moresby

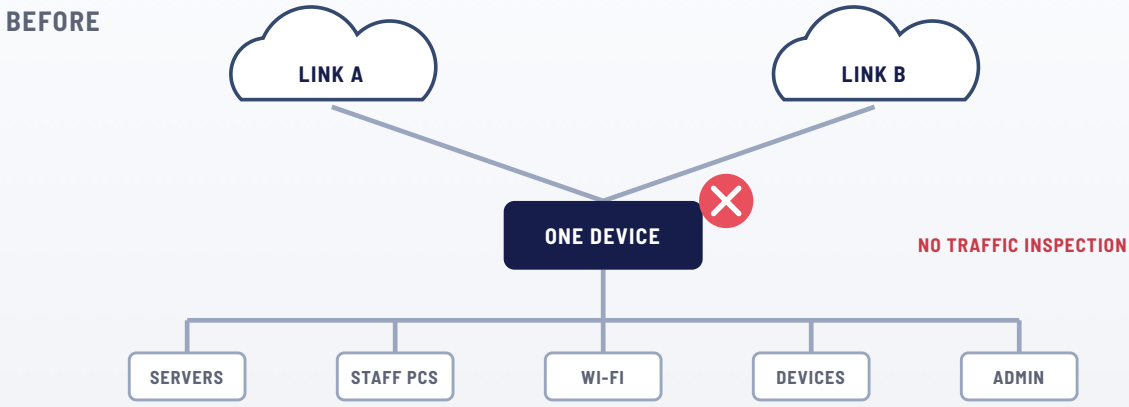
INSIDE

THE CHALLENGE · THE SOLUTION · EVERY LAYER · RESULTS · TALK TO US

01 / THE CHALLENGE

A GROWING HOSPITAL, A BASIC NETWORK

Paradise Private Hospital runs 24-hour emergency care in Port Moresby and cares for more than 70,000 patients a year. As it grew, its network stayed basic and unmanaged.



TWO LINKS, ONE WEAK POINT

Both internet links ran through a single device. If it failed, the whole hospital went offline.

NO REAL PROTECTION

Internet traffic was not checked for attacks, malware or risky websites, and nobody was managing it.

NO SAFE REMOTE ACCESS

Doctors had no secure way to reach the hospital management system (HMS) from home.

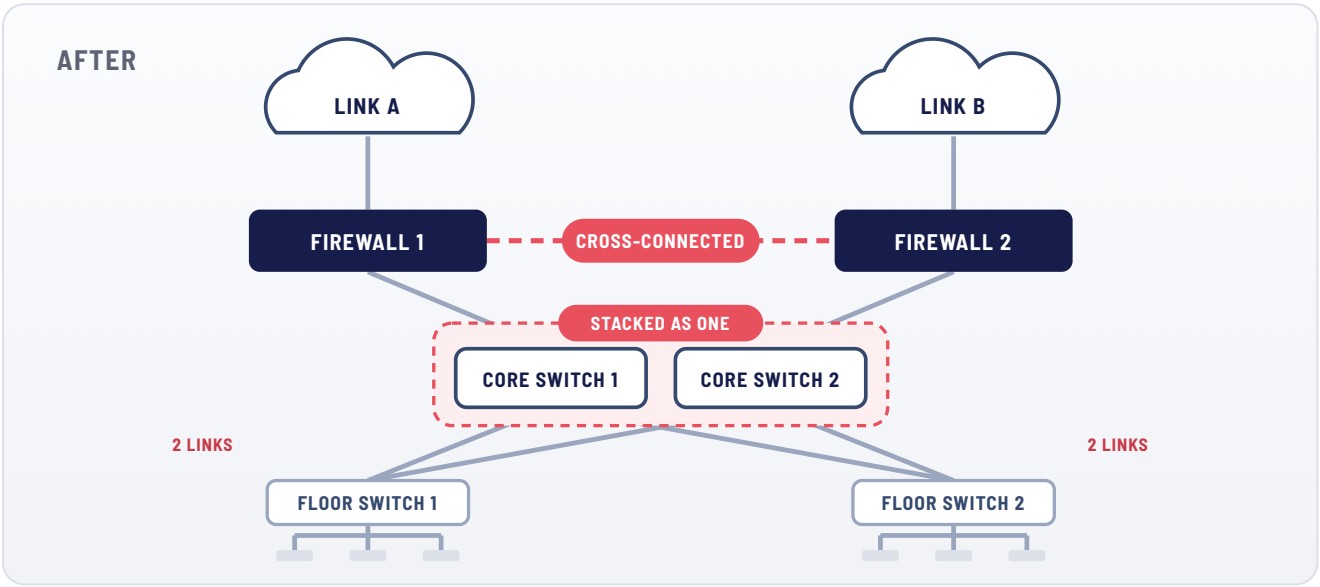
THE GOAL

FIX THE FOUNDATIONS BEFORE AN OUTAGE OR ATTACK FORCES THE ISSUE

02 / THE SOLUTION

NO SINGLE POINT OF FAILURE

Each internet link now has its own firewall, and a stacked pair of core switches connects to every floor switch twice. If a link, a firewall or a switch fails, traffic takes the other path.



WHAT THE FIREWALLS STOP

KNOWN ATTACKS
Blocked at the door

RANSOMWARE
Caught in web traffic

RISKY WEBSITES
Phishing filtered out

OVERSEAS TRAFFIC
Unwanted countries blocked

UNKNOWN APPS
Only approved services

SLOW HMS
Patient system first

IF SOMETHING FAILS

A LINK DROPS
→
Traffic moves to the other link

A FIREWALL FAILS
→
Its partner carries everything

A CORE SWITCH FAILS
→
Its stack partner keeps every floor online

BOTH LINKS WORK EVERY DAY
TRAFFIC IS SHARED ACROSS BOTH LINKS, SO STAFF GET MORE SPEED, AND THE PATIENT SYSTEM KEEPS PRIORITY IF ONE LINK DROPS

03 / PROTECTION AT EVERY LAYER

FROM THE INTERNET LINK TO THE INBOX

Security now covers every way an attack could get in: the network, remote logins and email.

REDUNDANT EDGE
A firewall for each internet link, cross-connected
EARLY 2026

NEXT-GENERATION FIREWALLS
Attacks, ransomware and risky sites blocked
EARLY 2026

ZERO TRUST REMOTE ACCESS
Checked people, checked devices, HMS only
EARLY 2026

EMAIL SECURITY
Phishing and harmful attachments stopped before the inbox
ADDED OCT 2026

HOW A REMOTE LOGIN WORKS

STEP 1
SIGN IN
Password plus a code on the user's phone

STEP 2
DEVICE CHECK
Computer must meet hospital policy

STEP 3
SECURE TUNNEL
An encrypted connection is set up

STEP 4
HMS ONLY
Everything else stays closed

EMAIL SECURITY
Added October 2026

- Phishing emails filtered out
- Harmful links and attachments blocked
- Fake senders and impersonation caught

WHAT ZERO TRUST MEANS

NOBODY IS TRUSTED JUST BECAUSE THEY HAVE A PASSWORD. EVERY LOGIN CHECKS THE PERSON, THE DEVICE AND WHAT THEY CAN REACH.

04 / RESULTS

ONLINE, PROTECTED, READY TO GROW

1 **DESIGN**
PLAN
Built around how the hospital works

2 **PRE-BUILD**
CONFIGURE
Set up before engineers flew in

3 **ON SITE**
TEST
Every failover path proven

4 **EARLY 2026**
GO LIVE
Minimal disruption to staff

5 **OCT 2026**
EXTEND
Email security added

ZERO INCIDENTS
No security incidents since go-live

ALWAYS ON
A link or device can fail without an outage

HMS FIRST
Patient system traffic gets priority

SAFE FROM HOME
A stolen password alone gets nowhere

THREATS STOPPED
Attacks blocked before they reach staff

SAFER INBOX
Phishing stopped before it reaches staff

BEFORE AND AFTER

AREA	BEFORE	AFTER
Internet	✕ Two links, one device	✓ A firewall for each link
Core network	✕ One path for everything	✓ Stacked core, two links to each floor
Firewall	✕ No traffic inspection	✓ Next-generation firewall pair
Remote access	✕ No secure option	✓ Zero trust, HMS only
Email	✕ Basic filtering	✓ Phishing and impersonation blocked

SERVICES DELIVERED

NEXT-GENERATION FIREWALLS → | DUAL INTERNET AND FAILOVER → | SECURE REMOTE ACCESS →

ZERO TRUST ACCESS → | EMAIL SECURITY →

THE LESSON FOR PACIFIC BUSINESSES

A BACKUP LINK IS ONLY AS GOOD AS THE DEVICE IT PLUGS INTO. BUILD RESILIENCE IN WHILE YOU GROW.

05 / TALK TO SPRINT NETWORKS

IS YOUR ORGANISATION IN THE SAME POSITION?

Tick any that sound familiar. If even one does, let's talk.

- [ ] Our backup internet link runs through the same device as the main one.
- [ ] If our firewall or core switch failed, everyone would stop.
- [ ] Nothing checks our internet traffic for attacks or malware.
- [ ] Staff reach our systems from home with just a password.
- [ ] Phishing emails still reach our staff's inboxes.
- [ ] We have grown, but our network has not kept up.

GET A FREE NETWORK AND SECURITY CHECK

A senior Sprint Networks engineer will show you where the risks are and what we would change. No cost, no obligation.

BOOK YOUR FREE CHECK

CHAT ON WHATSAPP

WHAT HAPPENS NEXT

1
WE LISTEN
A short call about your sites and systems.

2
WE REVIEW
Links, firewall, layout, email and remote access.

3
YOU GET A PLAN
Plain-language findings and first steps.

WEBSITE
sprintnetworks.com.au

EMAIL
info@sprintnetworks.com

CASE STUDIES
/case-studies

LINKEDIN
/company/sprint-networks

About Sprint Networks. We design, secure and support networks for banks, hospitals, insurers and businesses across PNG, Fiji, the Solomon Islands and the wider Pacific, from offices in Port Moresby and Sydney. Every solution is tested in real Pacific conditions first.