

HOW GML FIJI SECURED AZURE ERP CONNECTION WITH SD-WAN AND ZTNA

From the core in Suva to Business Central in Azure

GOLDEN MANUFACTURERS LIMITED

Golden Manufacturers Limited (GML) in Suva, Fiji depended on one working VPN tunnel to reach its Azure ERP. We rebuilt that connection and tested automatic failover before completing the deployment.

PROBLEM

Lack of redundancy, as one HQ devices carrying the traffic to cloud and need of secure remote access.

SOLUTION

Sprint Networks installed two devices in HA mode at head office, Suva and configured two SD-WAN tunnels towards cloud, added a virtual firewall instance on Azure and enabled secure remote access.

RESULT

Redundant and secured network, if one link fails traffic moves to another link automatically, prioritised ERP traffic helped business applications run smoothly during busy periods and authorised staff able to connect securely from remote locations by ZTNA (Zero Trust Network Access).

01 / THE CHALLENGE

ONE WORKING TUNNEL CARRIED TOO MUCH RISK

GML makes the cartons, packaging and labels behind some of Fiji's best-known products. Orders, inventory, production and deliveries are coordinated through Microsoft Dynamics 365 Business Central, hosted in Azure. People across the business need a dependable way to reach it.

Two VPN tunnels were configured through a single firewall at Suva HQ. Only one worked. If that path failed or deteriorated, there was no effective automatic switch to another route. The firewall itself was another single point of failure.

GML wanted to reduce that exposure and give employees secure access to the ERP when working remotely. Its IT team also needed a clearer view of the connection when investigating problems. Those requirements shaped the rebuild.

WHAT CHANGED FOR GML

Before	After
One firewall at headquarter	Two appliances at headquarter
Two VPN tunnels configured; only one working	Two operational SD-WAN tunnels over Vodafone and Digicel internet
No effective automatic path change	Automatic switching with successful failover testing
Secure remote ERP access needed	ZTNA access for authorised remote employees
ERP traffic without deliberate priority	Business Central traffic prioritised
Limited network visibility	GUI based analytics for troubleshooting

START IN THE SYDNEY LAB

Before we changed GML's live network, we built a smaller working version in our Sydney lab. The simulation recreated the important parts of the proposed HQ and Azure setup so we could check the configuration and traffic behaviour together.

That gave our engineers a place to work through the design before it carried production ERP traffic. The project developed from proof of concept to production over months, with deployment completed in January 2026.

02 / THE SOLUTION

BUILD THE CONNECTION FROM HQ INTO AZURE

Two appliances at headquarters

We installed two Versa appliances at Suva HQ. Each box can provide firewall, switching and routing functions alongside SD-WAN traffic control. The pair gives GML hardware redundancy at HQ. We also installed Cisco core switches to support the local network. The central change was removing the ERP connection's dependency on one HQ appliance.

Two carrier paths with automatic switching

Vodafone and Digicel internet services carry the two SD-WAN tunnels towards Azure. One tunnel normally carries the load. The second is used automatically when the primary reaches capacity, experiences difficulties or fails. GML now has a configured response when its preferred path can no longer carry traffic as intended.

A virtual endpoint in Azure

One virtual firewall instance sits inside GML's Azure environment, extending the SD-WAN connection to the cloud side of Business Central. This design brings firewall functionality and traffic policies into the connection between headquarters and the ERP.

THE CURRENT CONNECTION



Vodafone and Digicel provide the HQ internet paths. One tunnel normally carries the load; the second is used automatically when needed.

03 / THE RESULT

SECURE ACCESS AND A TESTED WAY TO SWITCH

GIVE ERP TRAFFIC AND REMOTE USERS THE ACCESS THEY NEED

We prioritised Business Central traffic over general internet use. For GML, that means the application coordinating the business receives deliberate priority when it shares network capacity with browsing, downloads and other traffic.

We also introduced Zero Trust Network Access (ZTNA) for authorised remote employees. It gives them secure access to Business Central at the application level, without first granting broad access to the office network. That addresses the second part of GML's original requirement: reaching the ERP securely while away from the site.

TEST WHAT HAPPENS WHEN THE PATH FAILS

A redundant design is only useful if traffic moves when a path fails. We tested automatic switching between the two operational tunnels and confirmed it worked successfully. That is the practical difference from the old setup: GML now has a working alternative and a tested mechanism to use it.

The two HQ appliances address the former dependency on one physical device. Together with the separate carrier paths, they strengthen the route from Suva into Azure.

GIVE THE IT TEAM A CLEARER VIEW

New analytics gives GML's IT team detailed information about network and application traffic. That makes it easier to narrow down where a problem is occurring and gives the team better evidence for troubleshooting.

Handover mattered too. We walked GML's team through the new interface so they could use the platform in day-to-day operations. After the installation, IT Manager Prasanna Sooriyabandara wrote:

Hi Sprint Networks Team,

Thanks again for coming in and setting up the VERSA firewall Last week. Everything seems to be running smoothly,

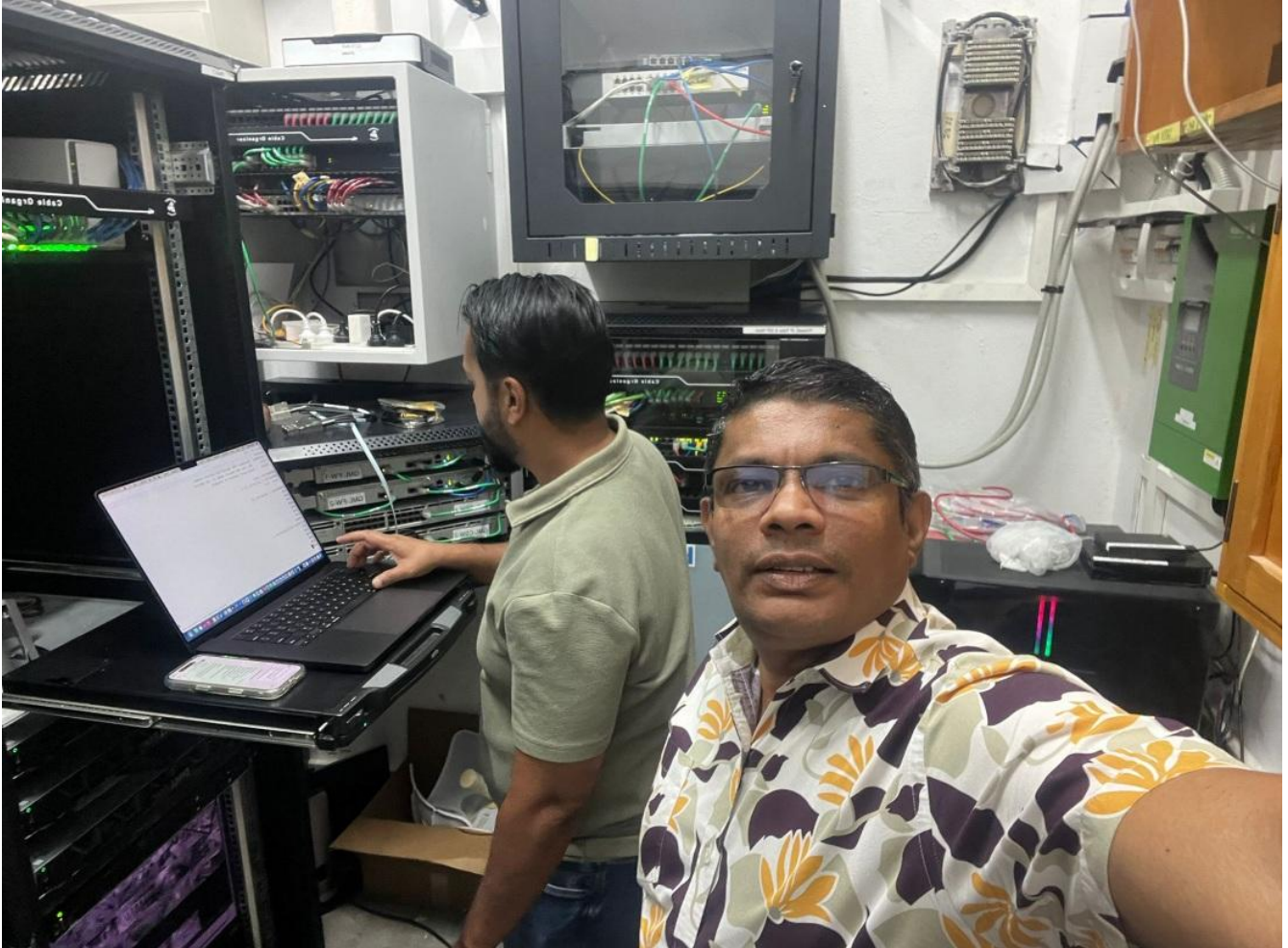
I really appreciate how quickly your Team handled the configuration and for walking us through the new interface.

The added layer of security is a vital step in protecting our Group of company assets. We truly value the dedication you & your Team show in keeping our infrastructure safe and efficient.

Cheers,

*Prasanna Sooriyabandara
IT Manager*

ON SITE AT GML



Sprint Networks engineer on-site at Golden Manufacturers Limited headquarters, Suva, Fiji (Jan 2026).

PLAN THE NEXT BRANCH CONNECTION

GML's branches currently reach Business Central over MPLS connections into Suva HQ, then use the HQ-to-Azure SD-WAN connection. MPLS connects branches to headquarters; Vodafone and Digicel internet services carry the tunnels from headquarters towards Azure.

The design also provides a route for the next phase. With a Versa device, suitable internet connectivity and the required configuration at a branch, that site could connect directly to Azure. It would no longer need to send ERP traffic through HQ first. This remains a future option for GML.

For businesses considering the same move, Sprint Networks can review which branches are ready for direct cloud access and plan the transition around their existing connections.

05 / CONNECT WITH SPRINT NETWORKS

REVIEW YOUR ROUTE FROM USERS TO THE CLOUD

GML now has tested automatic tunnel failover, redundant HQ appliances and secure remote ERP access. Its IT team has better visibility, and Business Central traffic receives priority. The next stage of branch connectivity can build on that foundation.

Sprint Networks reviews the full path from your users to the cloud. If you are running a cloud-hosted ERP in Fiji or PNG and relying on a single connection, the conversation starts here.

VISIT OUR WEBSITEsprintnetworks.com.au

EMAIL OUR TEAMinfo@sprintnetworks.com

EXPLORE MORE CASE STUDIESsprintnetworks.com.au/case-studies

FOLLOW US ON LINKEDINlinkedin.com/company/sprint-networks

WATCH OUR NETWORK VIDEOS[Sprint Networks on YouTube](#)
