

SecurityBrief New Zealand: We add Fortinet capability to connectivity offering - blueAPACHE

Canonical: <https://www.blueapache.com/blog/security-brief-new-zealand-blueapache-adds-fortinet-capability-to-connectivity-offering>

Details:

21 July 2022: We have added Fortinet Security Fabric-powered software-defined wide area networking (SD-WAN), next-generation firewalls (NGFWs), and secure access service edge solutions (SASE) to our emPOWER Connectivity offering. This completes the final phase of our \$6 million, multi-phase refresh of the core emPOWER network infrastructure. emPOWER Connectivity is a managed fabric that provides secure connectivity from any location, on demand including across global data centres, private and public clouds, physical premises, and remote access, which organisations can leverage to gain competitive advantage and scale capacity globally, the company states. With the addition of these complementary Fortinet solutions, the offering has been enhanced, giving customers a broader choice of services and capabilities to meet their core connectivity and security needs. The upgrade provides the global managed services company with an extended and fit-for-purpose managed connectivity offering for mid- to large-sized enterprises, supporting our ability to service customers on a global scale. Michael Zuppa, general manager technology within our business, says, "The market is changing and, along with it, the dynamic of how IT services and applications are consumed. This is being driven by changing laws and regulations, increasing IT security threats, and the shift towards hybrid work environments made possible by the accelerated adoption of Software-as-a-Service (SaaS) and advanced tools that let employees work from anywhere, anytime." He comments, "we wanted to expand our managed fabric that provides secure connectivity with SD-WAN, NGFW, and SASE to provide consistent enforcement and time to value with automation efficiency. To do this, we needed a fabric approach that would extend across all layers and levels of the network regardless of location or topology of standard or traditional-based networks.

"Fortinet, with its security fabric approach, was the ideal technology partner to help blueAPACHE achieve these objectives. With these enhanced capabilities, emPOWER Connectivity continues to address the changing landscape delivering a more consistent user experience as well as greater transparency and visibility through a real-time self-service portal and reliable security enforcement."

Tim Fitzgerald, channel director at Fortinet, says, "Fortinet and blueAPACHE share a true partnership and are committed to developing industry-leading solutions that remove complexity and address customer challenges and pain points, which presents great opportunities for growth.

"In June 2022 blueAPACHE achieved advanced partner status with a specialisation in SD-WAN and in February 2022 was awarded the Australian Growth Partner of the Year in the Fortinet Partner of the Year Awards. Fortinet continues to invest in its partners like blueAPACHE to drive training and certifications that let them deliver enhanced expertise to customers and address the skills gap in the market by offering training and certifications to its people."

Zuppa concludes, "blueAPACHE 100% owns, controls, and is responsible for the entire end-to-end networks and infrastructure that we manage. Each service that we deliver is underpinned by market-leading vendors to ensure best-of-breed service delivery.

"our strategic alignment with Fortinet lets us better support emerging organisations as they move into new geographies and we have enabled our global data centre footprint with Fortinet. "By partnering with leading global vendors, blueAPACHE can continue to deliver more opportunities and broader

service offerings to our customers across Australia and worldwide as well as offering training and certification opportunities to our global workforce.”

[Click here to view the full article](#)

A note on this page

The announcement above was published by Security Brief New Zealand on 21 July 2022; job titles, partnership status and investment details are historical. The sections below identify deployment and contract questions for a New Zealand buyer, using the published service material. They do not establish the configuration or terms of a particular engagement.

What SD-WAN, NGFW and SASE each do

Component	What it is	What problem it solves
SD-WAN	Software-defined wide area networking. The Connectivity brochure describes hybrid MPLS/internet and hub-and-spoke architecture options.	Agree the transports, application policies, failover behaviour and performance tests for each site; routing is configuration-dependent.
NGFW	Next-generation firewall. The brochure lists intrusion prevention, malware protection, application control, web filtering and antispam capabilities.	Confirm the features, licences and inspection policies included, and who maintains them.
SASE	Secure access service edge, combining networking and security capabilities for distributed access.	Confirm the enforcement locations, traffic paths, policies and measured user experience; the service name alone does not establish the nearest enforcement point.

For a New Zealand deployment, compare the proposed traffic paths and enforcement locations against application needs. Backhaul, internet breakout, cloud location and carrier routing can affect performance. Test representative applications and failover scenarios rather than assuming a geographic or latency advantage from SASE alone.

The network underneath, and where it reaches

We publish the emPOWER Network as a Cisco ASR-based private MPLS backbone that we own and operate, with:

Direct connectivity into 165+ data centres worldwide.

Tier 1 carrier-agnostic connectivity with redundant transmission paths between points of presence across the United States, Europe (London), Asia (Singapore) and Pacific (Australia) .

Proactive 24/7 network monitoring , 365 days a year.

The cited network material lists core points of presence in the United States, London, Singapore and Australia, and separately describes access to data centres including New Zealand locations. It does not establish the actual path between your New Zealand sites. Ask for the proposed topology,

interconnection locations and normal and failover routing.

That question should be settled explicitly for any New Zealand deployment, because it affects latency, resilience and, depending on the data involved, jurisdiction.

On vendors: the announcement adds Fortinet at the edge and security layer. The core is Cisco. These are complementary rather than substitutional, consistent with the announcement's own description of the Fortinet solutions as "complementary".

The two SD-WAN architectures published

Hybrid MPLS and internet SD-WAN , using both transports, or a combination.

Hub-and-spoke secure SD-WAN , using dedicated emPOWER Connectivity appliances with highly available SD-WAN hubs and hosted SD-WAN firewalls located in multiple data centres on the emPOWER Network.

Additional appliances at customer sites enable further internet services and allow local internet breakout bandwidth to scale on demand. For a New Zealand site, assess local breakout alongside security inspection, destination-cloud location and carrier routing; it does not by itself guarantee a wholly domestic traffic path.

Capabilities described in the Connectivity brochure

Confirm which capabilities apply to the proposed site design and service scope.

Capability	Brochure description
Redundant design	Multiple carriers, multiple media types, multiple CPE devices and firewalls in high-availability configuration
MPLS data services	Extends the corporate private network without a VPN; each office becomes another IP address on the network
Quality of Service	End-to-end QoS, with us working with the customer to define business-critical applications and apply policy; voice and video can be prioritised
Internet scalability	emPOWER Internet bandwidth scaled up or down on request, as part of IX peering infrastructure
Public cloud connectivity	Direct connection to Azure or AWS, with a secondary VPN-over-internet route for redundancy
Unified threat protection	Intrusion prevention, advanced malware protection, application control, web filtering, antispam, with 24x7 support
Remote access	Always-on VPN, configurable with single sign-on and multi-factor authentication; confirm termination locations and routing
Cloud connection	Direct connection to emPOWER Cloud, with backup and disaster recovery capabilities subject to the agreed scope; the ISO certificate concerns the ISMS, not individual service certification

Voice	Microsoft Teams Direct Routing, SIP trunking, hosted PBX and contact centre
Device management	Continuous monitoring, OS patching, configuration documentation, nightly configuration backups and change management on the CPEs and firewalls we provide

The location of support staff does not establish where VPN traffic terminates. Ask for the available termination options, authentication design and routing for New Zealand users.

The availability figure, and its condition

We publish a minimum 99.99 per cent uptime , subject to conditions, and the conditions are the substance. The figure applies to sites configured with multiple carriers, multiple media types such as fibre and fixed wireless, multiple CPE devices and firewalls in high-availability configuration, redundant transmission paths between points of presence, and dual firewalls and dual carriage at each site.

Check carrier and physical-path diversity at each proposed site before relying on the headline figure.

The support hours distinction

Function	Published availability
Service Desk (phone, email, client web portal)	7:00am to 7:00pm on business days
Priority network monitoring and NOC	24/7
Unified threat protection support	24/7

The brochure distinguishes round-the-clock monitoring and threat-protection support from the business-hours service desk. Confirm the applicable support window, timezone, holidays and after-hours escalation for the purchased services, including daylight-saving differences. Those brochure hours alone do not establish a gap in a particular customer's coverage.

Regulatory position for a New Zealand buyer

Our service material refers to several security frameworks. Assess each against your organisation's own obligations and the proposed service scope.

Reference	What to establish for a New Zealand engagement
ISO/IEC 27001:2022 certificate 202507-118	Check the ISMS scope, locations and current certification evidence. The certificate does not certify individual services or establish compliance with every local obligation.
ASD Essential Eight, APRA CPS 234 and NIST	Ask for the exact scope and supporting assessment evidence behind the published alignment or compliance statements. They do not by themselves determine the obligations applicable to a New Zealand customer.
Privacy and cross-border information handling	Assess the actual information flows, recipients, processing roles and contractual safeguards. The

	New Zealand Privacy Commissioner explains Principle 12 on disclosure outside New Zealand ; its application depends on the arrangement.
Data residency	Our data-sovereignty material describes Australian hosting. Specify any New Zealand residency requirement and confirm primary, backup, recovery and support-access locations in the proposed service. Australian hosting material alone does not prove where every customer's data is stored or accessed.

Two claims worth reading precisely

"blueAPACHE 100% owns, controls, and is responsible for the entire end-to-end networks and infrastructure that we manage." The final qualifier does real work. Our material describes ownership and operation of the MPLS core separately from interconnection with 165+ data centre locations. Owning the network is not the same as owning every facility it reaches.

MPLS security: We design and configure our core network to protect connectivity. Network design must also address endpoint security, access controls and the wider customer environment. Our team can explain the controls relevant to your solution.

Contract terms

Clauses 3.26–3.27 of the referenced General Terms v3.6 allow suspension or cancellation on specified grounds, including reasonable suspicion of security compromise. Fees for the suspended service do not accrue during that suspension; notice must be as extensive as reasonably possible and both parties must use best efforts to identify a solution. This contractual right is not an incident-containment runbook.

Clause 24.2 separately permits termination or suspension for specified grounds, including uncured payment or listed contractual breaches, subject to its notice and cure provisions. Clause 24.3 addresses fees and reinstatement for that form of suspension.

Clause 27.13 of the referenced General Terms v3.6 specifies Victorian law and exclusive jurisdiction of Victorian courts and courts competent to hear appeals. Confirm the version and negotiated variations governing a cross-border engagement.

Network topology: obtain the actual New Zealand inter-site routing and failover design; the brochure's PoP list is not a routing guarantee.

Remote access: confirm VPN termination options and routing; do not infer them from the service desk's location.

Support: the Connectivity brochure gives service-desk hours without a timezone; confirm the applicable Schedule, timezone, holidays and after-hours arrangements.

Residency: document required storage, processing, backup and access locations and check them against the proposed service.

Contract: check clause 27.13 and any variations in the governing document set.

Availability: obtain the applicable Network Schedule, measurement window, exclusions, credits and target for each site configuration. The brochure's headline figure does not establish these details.

Pricing: obtain a customer-specific quote. The 2022 article's \$6 million refresh figure describes blueAPACHE's investment and does not state a currency.

Capacity: specify required bandwidth, port speeds, growth options and delivery lead times.

Security handling: confirm any detection, response or triage targets in the purchased security service's documentation.

What did blueAPACHE announce on 21 July 2022?

The historical announcement reported the addition of Fortinet Security Fabric-powered SD-WAN, next-generation firewalls and SASE solutions to emPOWER Connectivity.

What broader project does this Fortinet capability addition complete for you?

The July 2022 article said the addition completed the final phase of blueAPACHE's \$6 million, multi-phase core-network refresh. This is historical investment context, not a customer price.

What is emPOWER Connectivity?

The July 2022 article described emPOWER Connectivity as a managed fabric connecting data centres, private and public clouds, premises and remote users. Confirm current coverage and design for your locations.

What role and comments did the July 2022 article attribute to Michael Zuppa?

The July 2022 article identified Michael Zuppa as general manager technology at that time. He described changing regulation, security threats, hybrid work and SaaS adoption as drivers for the upgrade.

Why did blueAPACHE choose Fortinet for the 2022 enhancement?

Michael Zuppa said Fortinet's fabric approach suited the aim of extending consistent security enforcement and automation across different network layers, locations and topologies.

What recognitions have you received from Fortinet, according to Tim Fitzgerald?

In the July 2022 article, Tim Fitzgerald cited advanced partner status with an SD-WAN specialisation in June 2022 and Australian Growth Partner of the Year recognition in February 2022.

What benefits do you say customers gain from the enhanced emPOWER Connectivity offering?

The July 2022 announcement described broader connectivity and security choices, a more consistent user experience, visibility through a real-time self-service portal and security enforcement. These are the benefits stated in that historical announcement.

How did the 2022 article describe blueAPACHE's network ownership?

The article quoted Michael Zuppa describing blueAPACHE as owning, controlling and being responsible for the end-to-end networks and infrastructure it manages. This is a dated statement about the managed infrastructure; it does not mean blueAPACHE owns every interconnected facility.