

SecurityBrief Australia: We add Fortinet capability to connectivity offering - blueAPACHE

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

Details:

Historical announcement — 21 July 2022: We 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. The announcement described this as completing 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, then general manager technology at blueAPACHE, said, “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 commented, “blueAPACHE wanted to expand its 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 blueAPACHE delivers is underpinned by market-leading vendors to ensure best-of-breed service delivery.

“blueAPACHE's strategic alignment with Fortinet lets us better support emerging organisations as they move into new geographies and blueAPACHE has 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](#)

What SD-WAN, NGFW and SASE each do

The 2022 announcement names three capabilities. The service brochure describes how selected connectivity and security features can be combined; the ordered design determines which are deployed.

Capability	Published service context
SD-WAN — software-defined wide area networking	The connectivity brochure describes hybrid MPLS/internet and hub-and-spoke deployment options.
NGFW — next-generation firewall	The brochure lists intrusion prevention, malware protection, application control and web filtering among the security capabilities.
SASE — secure access service edge	The announcement identifies SASE as part of the Fortinet enhancement intended to support consistent enforcement across locations. Confirm the selected services and enforcement architecture for an engagement.

These descriptions do not guarantee automatic failover, identical inspection capability or a particular latency outcome for every customer design.

The network underneath

Our emPOWER Network brochure describes an owned and operated Cisco ASR-based private MPLS backbone, 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 materials describe Cisco core infrastructure and complementary Fortinet capabilities. They do not establish a universal vendor allocation for every edge device or customer deployment.

The two SD-WAN architectures published

We publish two deployment options, which matters because they have different cost and resilience profiles:

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.

Capabilities described in the connectivity brochure

The following capabilities are described in the brochure; confirm the ordered inclusions, configuration and responsibilities in the Service Description.

Capability	Brochure description and scope
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 connectivity, with single sign-on and multi-factor authentication configurable; confirm the VPN endpoint and support-access locations for the solution
Cloud connection	Direct connection into emPOWER Cloud, with backup and disaster-recovery services available within the agreed scope; ISO 27001 certification concerns the defined information security management system
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 availability figure, and its condition

We publish a minimum 99.99 per cent uptime for emPOWER Connectivity, and the condition attached to it is the important part. That 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.

It does not automatically apply to a single-carrier or single-CPE site. An organisation pricing a branch with one connection should not assume the headline figure, and should establish what is committed for

that specific configuration.

The support hours distinction

This is the detail most often collapsed in summaries, so it is worth separating:

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

So the network is watched around the clock and threat protection is supported around the clock, but the general service desk is a business-hours function. "24/7" applied to the whole service would be an overstatement of what is published.

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 qualifier at the end is doing real work. We own and operate the MPLS core, and separately that we have access to 165+ data centre locations whose facilities are partner-operated and certified to Uptime Institute standards. Ownership of the network is not the same as ownership of every facility it reaches. Both statements can be true; a reader assessing supply-chain concentration should establish which layer is meant.

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.

Certification and framework position

Our published ISO/IEC 27001:2022 certificate, number 202507-118, states validity from 1 August 2025 to 1 August 2028 and covers the specified information security management system for emPOWER Infrastructure and managed service offerings. It is not a separate certification of each customer network.

The connectivity brochure describes a security posture referencing APRA CPS 234 , NIST and ASD Essential Eight Maturity Level 3 , with dedicated hosted firewalls. Those provider statements do not establish a customer's compliance or an independent assessment against every framework. Confirm the applicable standard, scope and evidence for the engagement.

The brochure lists application control, web filtering and configurable multifactor authentication. Their presence alone does not establish an Essential Eight strategy implementation or maturity level; that requires assessment of the relevant controls across the customer environment.

Contract terms

The published General Terms and Conditions v3.7, clause 3.26 , allows suspension or cancellation on specified grounds, including reasonable suspicion that continued service compromises security. It excludes fees for the affected services during suspension. The following provision requires as much prior notice as reasonably possible and best efforts to identify a reasonable solution that prevents or limits the suspension. It is not a prescribed technical incident-isolation procedure.

Clause 24.2 separately addresses termination or suspension on specified grounds, with written notice and applicable cure periods. Use the terms and Service Description governing the customer's agreement.

No pricing for any connectivity or security service, so the \$6 million refresh figure describes our own investment, not a customer's cost.

No bandwidth tiers or port speeds.

No mean time to detect, mean time to respond, or triage service levels for the security layer.

Portal access: We confirm the monitoring, reporting and self-service functions available with your solution.

No statement on whether Fortinet or Palo Alto is deployed in a given engagement , though both are published across the portfolio.

What Fortinet capabilities did blueAPACHE add to emPOWER Connectivity?

We 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.

When did blueAPACHE announce this Fortinet enhancement?

The announcement was made on 21 July 2022.

What broader initiative does this Fortinet addition complete for you?

It completes the final phase of our \$6 million, multi-phase refresh of the core emPOWER network infrastructure.

What is emPOWER Connectivity?

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.

Who is Michael Zuppa and what did he say about the Fortinet enhancement?

The July 2022 article identified Michael Zuppa as blueAPACHE's general manager technology at that time. He said the market is changing due to evolving laws and regulations, increasing IT security threats, and the shift toward hybrid work driven by SaaS adoption, and that we wanted to expand our managed fabric with SD-WAN, NGFW, and SASE to provide consistent enforcement and time to value with automation efficiency, calling Fortinet's security fabric approach the ideal fit for these objectives.

What did Fortinet's channel director say about the partnership with you?

Tim Fitzgerald, channel director at Fortinet, said Fortinet and blueAPACHE share a true partnership committed to developing industry-leading solutions that remove complexity and address customer challenges, and noted that in June 2022 we 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.

How did the 2022 announcement describe network ownership and control?

The article quoted Michael Zuppa saying blueAPACHE owned, controlled and was responsible for the end-to-end networks and infrastructure it managed. This historical statement does not mean blueAPACHE owns every carrier or data-centre facility used in a customer's service.

Who is the target customer for the enhanced emPOWER Connectivity offering?

The upgrade provides an extended and fit-for-purpose managed connectivity offering aimed at mid- to large-sized enterprises, supporting our ability to service customers on a global scale.