WHITE PAPER

Fortinet and Megaport Multi-cloud

Overview

Multi-cloud architectures are becoming increasingly important for organizations to distribute workloads and applications across the many Infrastructure-as-a-Service (IaaS) platforms available today. In some cases, a single business-critical application may be tied to private cloud, public cloud, and hybrid cloud infrastructure services. Regardless of the many variations of application and cloud architectures, the network is a key element of delivering a multi-cloud solution.

North-south and east-west traffic flows are no longer confined to a single location. An end user's application workflow may generate network traffic flows from their edge device to systems in multiple clouds and geographic regions. Back-end systems and shared services may generate traffic flows between clouds to support near-real-time transaction processing, data replication, and disaster recovery services.

Network Security, Performance, and Resiliency

Fortinet FortiGate supports both next-generation firewall (NGFW) and software-defined wide-area networking (SD-WAN) functions, and is available in physical, virtual, cloud, and container formats. Fortinet Secure SD-WAN establishes secure, high-performance connectivity to applications running on hybrid-cloud and multi-cloud environments. Fortinet Secure SD-WAN:

- Simplifies cloud on-ramp for users and multi-cloud security with security-driven networking, which consolidates security and networking functions
- Delivers consistent security posture across on-premises, cloud, and multi-cloud deployments with the same network security and segmentation policies across the enterprise IT environment
- Enables the best application experience by prioritizing critical application traffic and increasing connection resiliency

The Fortinet Security Fabric is the industry's highest-performing cybersecurity mesh platform, powered by the operating system FortiOS. It spans across an entire network linking different security sensors and tools together to collect, coordinate, and respond to malicious behavior in real time and can be used to coordinate the behavior of different Fortinet products in the network, including FortiGate NGFW and Secure SD-WAN. The Fortinet Security Fabric can tap into Megaport's global Network-as-a-Service (NaaS) backbone to provide software-defined cloud interconnect (SDCI) services with a FortiGate-VM running on the Megaport Virtual Edge (MVE) platform.

Megaport's NaaS platform is purpose-built to support customers who have built cloud infrastructure and applications into their IT estate. As the cloud ecosystem has matured, a multi-cloud approach has become the de facto standard among enterprises. According to ESG Research's 2022 State of Network Transformation Survey, 90% of enterprises are using two or more clouds. Sixty percent are using three or more clouds. Three core connectivity scenarios arise from this evolution:

1. Site-to-cloud
2. Intra-cloud (data traffic between instances in a single cloud provider's platform)
3. Inter-cloud (data traffic between two or more separate cloud providers' platforms)

Each scenario has its own unique attributes and complexities. In addition, all can be utilized simultaneously, furthering the need for thoughtful network design to balance security, performance, and scalability. In this solution brief, we will focus on #1 and #3.

Megaport's network fabric spans across 760+ data center locations by partnering with over 100 unique data center operators (DCOs) globally. The extensive footprint allows dedicated, private, and secure connectivity to roughly 250 NNI/peering on-ramps to service providers, including AWS, Azure, Google Cloud Platform (GCP), and Oracle. Layered on top of this diverse and resilient network infrastructure is Megaport's native software-defined provisioning and management platform.

Strategic and Virtualized Network Points-of-presence (PoP)

MVE is a network functions virtualization (NFV) compute platform hosted in Megaport-enabled data centers in 25 countries. MVE enables Fortinet customers and MSPs to host a virtual FortiGate appliance with direct network access to Megaport's full NaaS capabilities.

Data center and network transit resilience is built into MVE. Each MVE region has the equivalent of CSP "availability zones" where at least two physically diverse data center operators may be chosen (i.e., Dallas region includes Cologix, CyrusOne, and Digital Realty). In addition, MVE also includes diverse internet transit to the virtual SD-WAN appliance with Border Gateway Protocol (BGP) peering to at least two ISPs within the region.

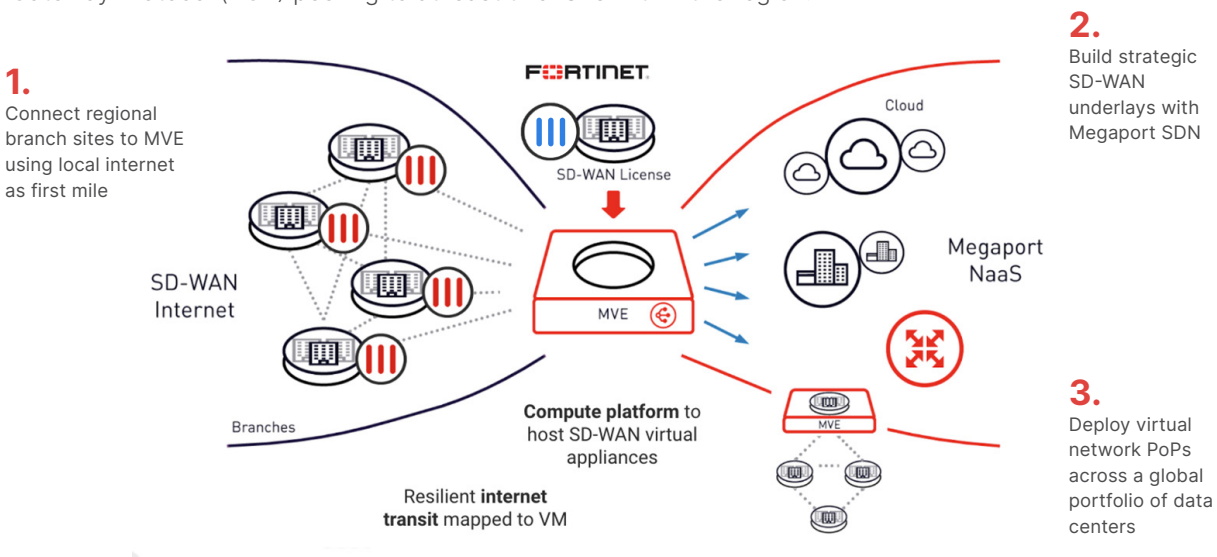

Figure 1: MVE enables Fortinet customers and MSPs to host a virtual FortiGate appliance with direct network access to Megaport's full NaaS capabilities

A FortiGate-VM on MVE is provisioned with dedicated internet transit and public IPv4/IPv6 IP space. The branch FortiGate NGFWs use their own internet transit to build SD-WAN overlay tunnels to the FortiGate-VM on MVE. The MVE and branches are within the same region and use the internet as the first mile/local loop for low-cost, low-latency access, joining the branch to a powerful middle-mile (and in most cases, last-mile) connectivity to CSP. The FortiGate is also a foundational element to a Fortinet Secure Access Service Edge (SASE) architecture that is tightly integrated with FortiClient, FortiAP, and other products. The MVE and FortiGate solution provides network and security design capabilities to address many use cases.

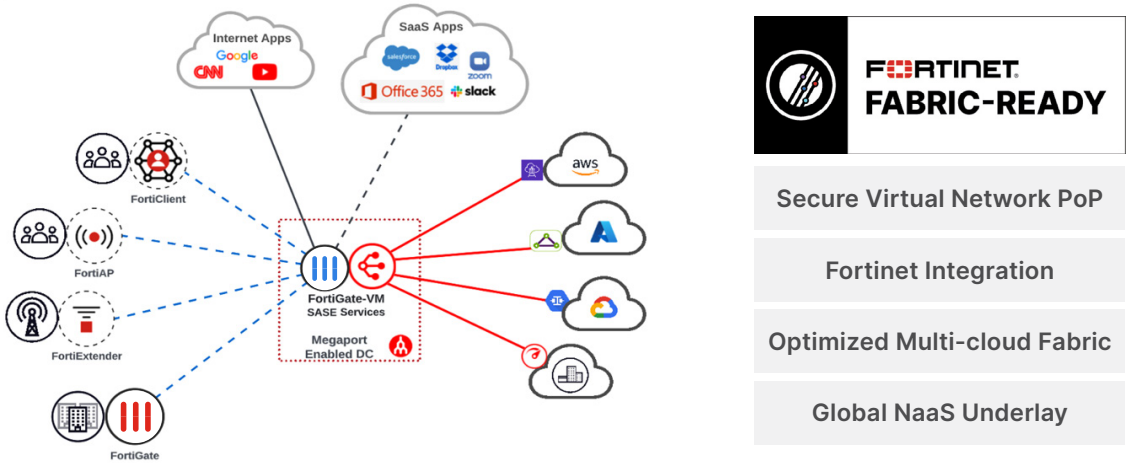

Figure 2: Fortinet Security Fabric and Megaport Virtual Edge

Provisioning Speed and Agility

Customers may deploy their FortiGate-VM on MVE through the Megaport SDN portal or use APIs to automate the provisioning of VMs and virtual cross-connects (VXCs).

Within minutes, a FortiGate-VM is instantiated in a data center within a specified region. Once installed, customers can provision SD-WAN tunnels from their regional branches, HQ, and data center FortiGate appliances using their existing internet connections.

From here, VXCs may be deployed to one of Megaport's over 250 cloud on-ramps, including Azure ExpressRoute, AWS Direct Connect, and GCP Partner Interconnect. The FortiGate-VM on MVE is now a regional multi-cloud hub for critical network segments by aggregating branch and user connections to applications and workloads over private, Layer-2 connections with dedicated bandwidth and low latency.

MVE and VXC services are dynamic and scalable. Private clouds and other remote regions with FortiGate-enabled MVEs can be interconnected with VXCs within minutes. Not only does Megaport simplify the deployment process, it also provides the ability to scale bandwidth up or down on demand. The automation tools used by DevOps teams may now extend to the network to increase or decrease bandwidth capacity based on data utilization forecasting, resulting in optimized infrastructure cost controls.

SASE Integrated and Optimized Multi-cloud Solution

Simple service insertion at any PoP in the Megaport ecosystem enables a single security context and policy set across the entire distributed architecture. SDN awareness, regardless of the location of the FortiGate-VM—be it in private or public cloud locations, in a collocation or PoP—allows policy frameworks to be created around business intent that dynamically respond to changes in the virtualized environment. Take the example of an enterprise resource planning (ERP) transaction where a service is being replicated or a database is being called between Azure and AWS. A FortiGate-VM located in an MVE PoP can source information about workloads in both of these environments to inform a single policy about access or risk between those multi-cloud resources. Policies and metadata can can be managed further from a centralized location in the customer's IT estate, regardless of the FortiGate form factor or location.

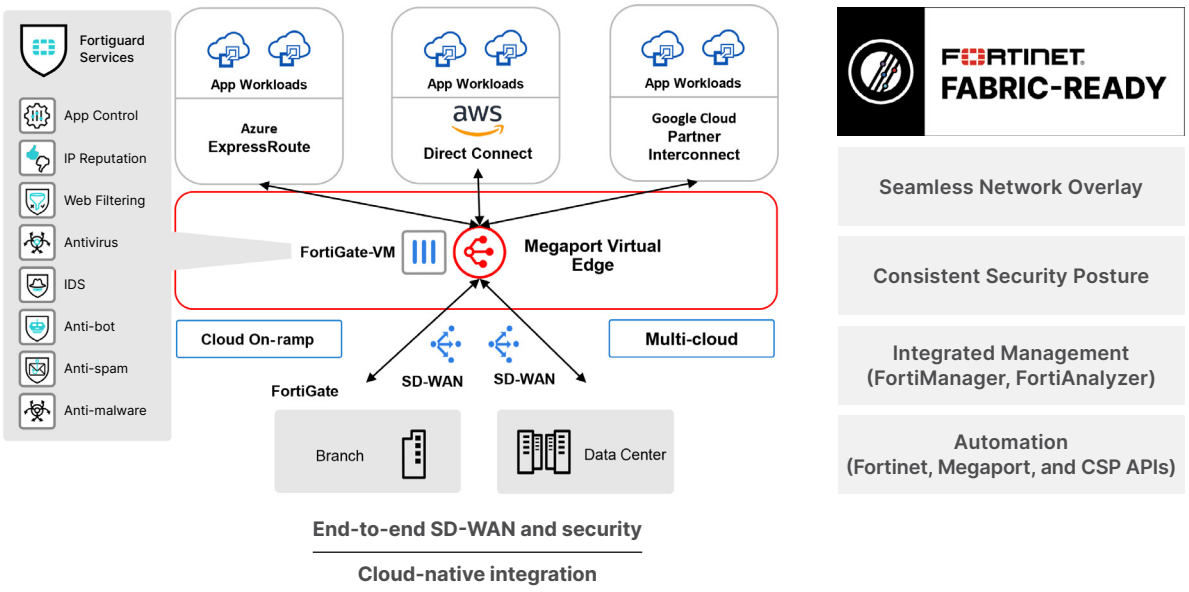

Figure 3: Security into and across clouds: Multi-cloud SD-WAN

The Megaport NaaS platform enables businesses to build their own virtual network PoPs across multiple regions across the globe. Each regional FortiGate MVE not only provides a secure multi-cloud hub but may also be used to interconnect regions. Long-haul connectivity segments between NAM, EMEA, and APAC may be provisioned to build a customized Layer-2 private global backbone. These connections between regions may facilitate data flows (transactional, replication, migration, etc.) between private, public, and hybrid-cloud architectures. Integrating Fortinet Secure SD-WAN and security services with such a powerful network underlay allows enterprises to build and manage their own middle-mile fabric that was previously controlled and constrained by legacy carriers.

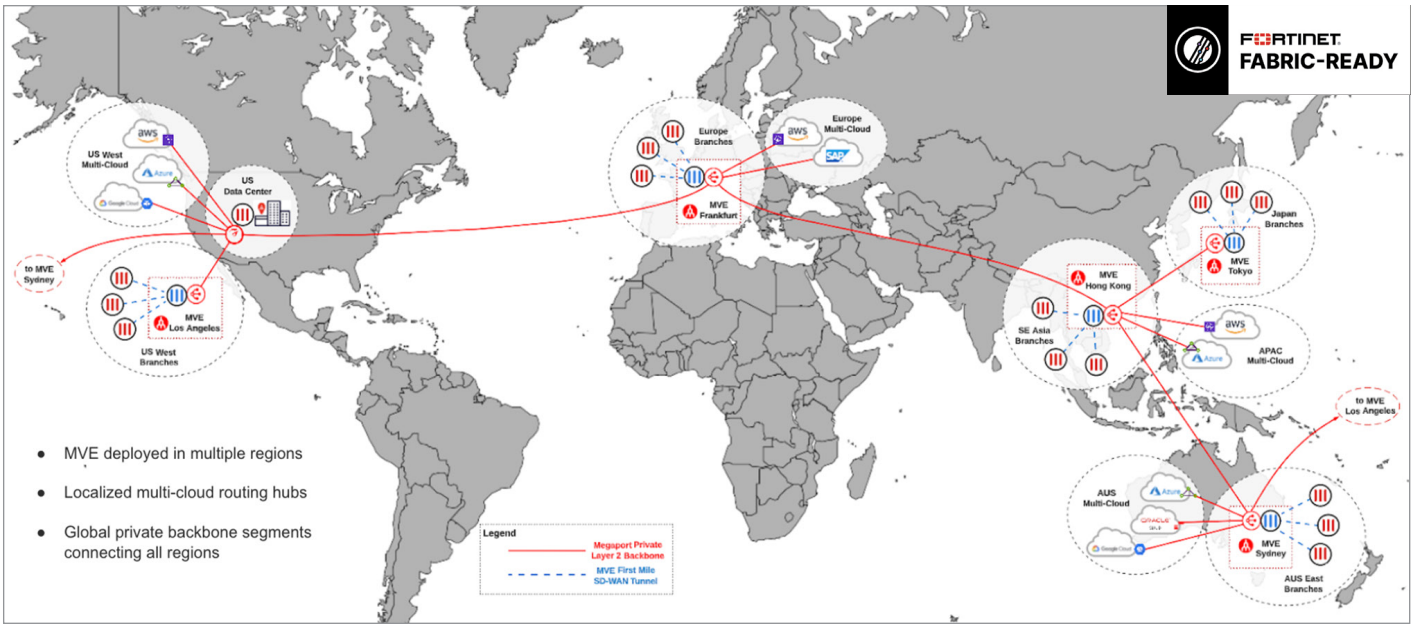

Figure 4: Regional to global hybrid-cloud connectivity

MVE delivers a hybrid SD-WAN "transport" with the benefits of predictable latency, dynamic provisioning, private Layer-2 connectivity, and dedicated bandwidth, making it a preferred solution over multiprotocol label switching (MPLS) for many customers.

Today's enterprise networks must embrace digital transformation to quickly adapt and deliver for their customers, and leveraging networking technologies is key. At its core, SD-WAN is all about shaping and steering application traffic across multiple WAN transports. Inserting MVE into your enterprise SD-WAN fabric gives your business greater flexibility, control over your data flow, cost optimization, and the agility to adapt to ever-changing business environments.

Use Case

Customers achieve low-latency multi-cloud connectivity with Fortinet Secure SD-WAN and Megaport's global private software-defined network (SDN).

- Megaport's global SDN provides both dynamic provisioning of a Secure SD-WAN virtual FortiGate and private connectivity between cloud, data center, and regional branch locations.
- MVE and Fortinet Secure SD-WAN secure multi-cloud connectivity without impacting performance.
- Fortinet Next-Generation Firewall and Secure SD-WAN services combined with Megaport's global NaaS enable customers to optimize their network performance, scalability, and security posture.
- Utilizing Megaport's NaaS with Fortinet Secure SD-WAN maximizes the customer's quality of experience through improved application performance while minimizing cloud egress costs.

The network edge has increasingly become a critical element for connecting users to applications now hosted across many locations and platforms. Maintaining security, performance, and reliability over internet connectivity continues to present growing challenges. MVE now extends the Fortinet Security Fabric into the middle and last miles of a customer's global WAN infrastructure.

An MVE hosting a Fortinet Secure SD-WAN VM in a region acts as a WAN hub for critical network segments by aggregating branch and user connections to critical workloads over private, Layer-2 connections with dedicated bandwidth and low latency. The Fortinet Secure SD-WAN on MVE can directly connect to cloud on-ramps (such as Azure ExpressRoute, AWS Direct Connect, and GCP Interconnect), or to private clouds and other remote regions hosted on MVE. These private connections over the Megaport backbone combined with the FortiGate NGFW and SD-WAN services provide a new level of high-performing, secure connectivity and control. Application traffic flowing between clouds, data centers, and regional branches is more secure and performance optimized.

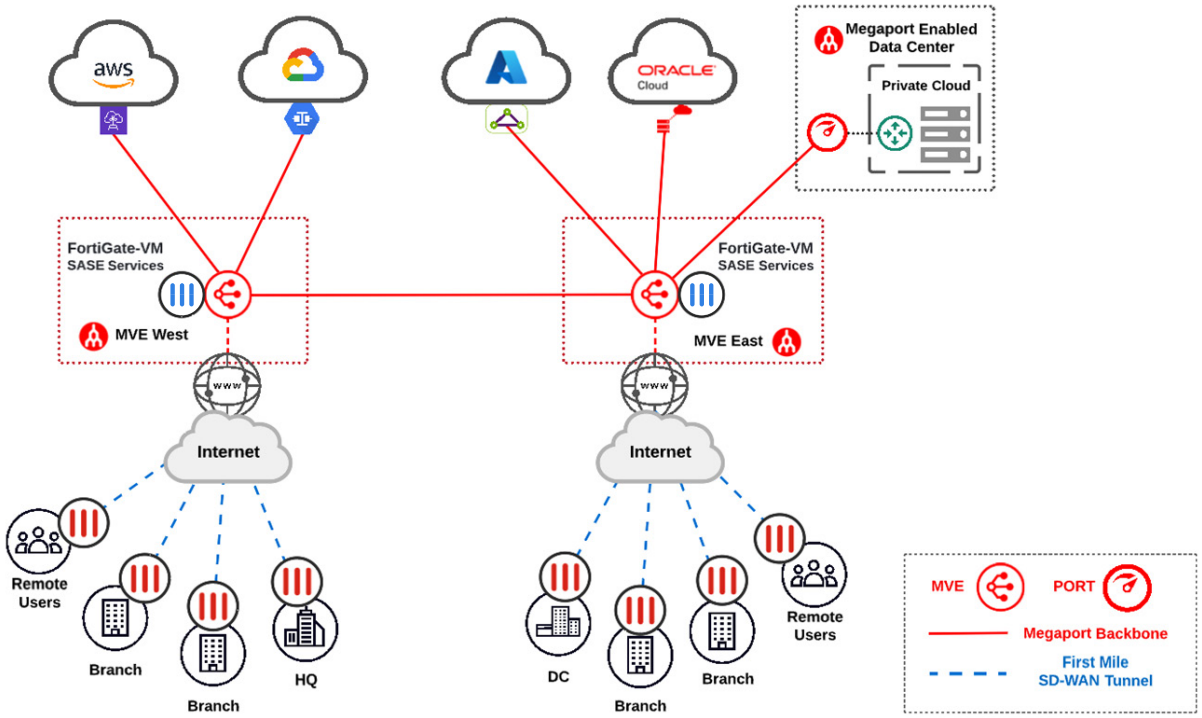

Figure 5: The solution integrates the entire WAN architecture via FortiGate

About Fortinet

Fortinet makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 580,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About Megaport

Megaport is a leading provider of Network as a Service (NaaS) solutions. The company's global Software Defined Network (SDN) helps businesses rapidly connect their network to services via an easy-to-use portal or our open API. Megaport offers agile networking capabilities that reduce operating costs and increase speed to market compared to traditional networking solutions. Megaport partners with the world's top cloud service providers, including AWS, Microsoft Azure, and Google Cloud, as well as the largest data centre operators, systems integrators and managed service providers in the world. Megaport is an ISO/IEC 27001-certified company.

August 30, 2022 7:35 PM

1711210-0-0-EN