SECURING VMWARE CLOUD ON AWS

IT leaders need a well-planned strategy for successful hybrid cloud adoption. VMware Cloud on AWS brings VMware's enterprise class Software-Defined Data Center (SDDC) software to Amazon's public cloud. In the cloud digital transformation, more enterprises adopt the hybrid cloud approach. However, common challenges emerge for enterprise IT leaders on the hybrid cloud including:

- Migration complexity with multiple virtual machine packages
- Incongruent networks and protocol handshakes result in operational and management inconsistency
- Differing security baseline makes end-to-end workload visibility and control impossible

VMware is the platform of choice for hundreds and thousands of on-premises data centers worldwide. VMware Cloud for AWS is an on-demand service, running on a dedicated, elastic, bare-metal AWS infrastructure. It is powered by VMware Cloud Foundation™, the unified SDDC platform that integrates vSphere, VMware vSAN™, and VMware NSX® virtualization technologies. VMware Cloud on AWS brings the exact VMware SDDC stack onto AWS through a seamless solution account integration. The joint solution eliminates the need to stitch together multiple management tools and allows traditional IT to continue to use VMware vCenter tools for workload orchestration in a hybrid deployment.

FORTIGATE NEXT-GENERATION FIREWALL ON VMWARE

FortiGate next-generation firewall virtual appliances for VMware vSphere and vCloud provide proven security while realizing the flexibility and benefits of VM-based packaging: unmatched ROI, rapid provisioning, east-west traffic visibility, unlimited scalability, and consolidation. FortiGate is ideal to scale and segment the hybrid cloud. The virtual appliance delivers consistent policies across hypervisor and cloud platforms and secures app migration between private and public clouds.

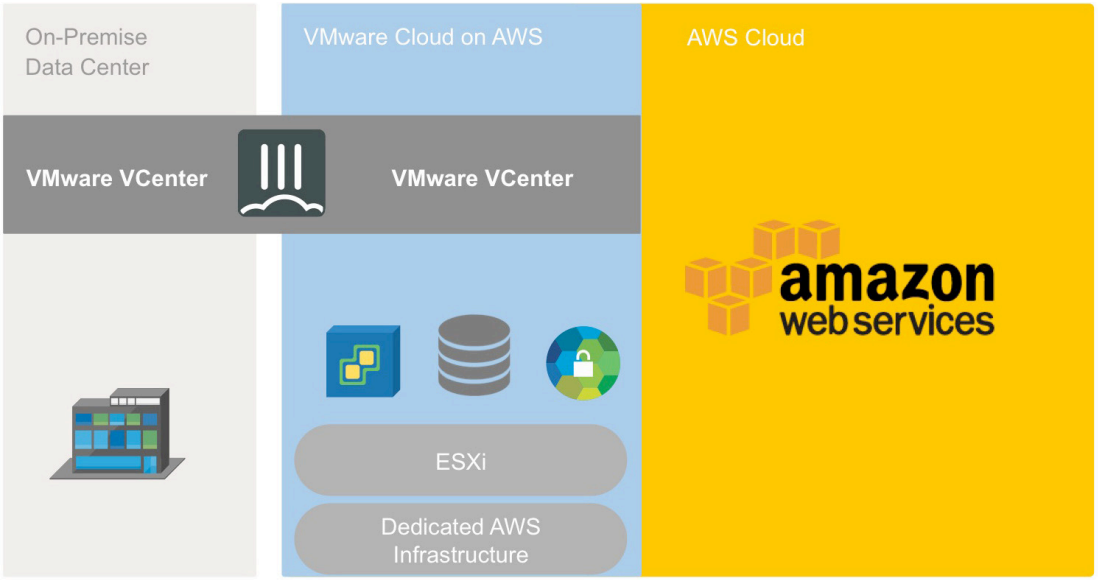

FIGURE 1: VMWARE CLOUD ON AWS ACCESS FLOW

ADVANCED SECURITY IN ALL PUBLIC AWS REGIONS

FortiGate virtual appliance and CloudFormation templates are available in all AWS regions today with flexible Bring-Your-Own-License (BYOL) perpetual license and Pay-As-You-Go (PAYG) hourly on-demand license options. Fortinet FortiGate virtual firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features. Application control, antivirus, IPS, web filtering, and VPN, along with advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, work in concert to identify and mitigate the latest complex security threats. The security-hardened FortiOS operating system is purpose-built for inspection and identification of malware and fully supports direct Single Root I/O Virtualization (SR-IOV) for higher and more consistent performance.

When moving workloads from vCenter environment to AWS with elastic distributed resources services (EDRS), organizations can continue to enforce consistent security policies using FortiGate firewalls on both sides without service disruption.

SINGLE LOGICAL VIEW FOR HYBRID CAPABILITY ENABLEMENT

VMware Cloud on AWS is an on-demand VMware service sold and supported by VMware. It offers the common control plane across the hybrid use cases. A new solution account is automatically created by VMware to streamline the SDDC stack deployment in AWS. Customers can choose AWS regions for data-center extension to AWS geographic availability zone using their own AWS account for application migration, disaster recovery/secondary backup site, instant cloud bursting, or data solvency concerns, etc.

FORTINET SECURITY FABRIC FOR HYBRID CLOUD COLLABORATIVE SECURITY

The Fortinet Security Fabric's core foundation is built on Fortinet's Enterprise Firewalls—for branch, campus, data-center, and internal segmentation deployment—all interconnected by a single, unified operating system for simplified and coordinated deployment and control. Our Enterprise Firewall solution allows segmentation of network elements, enforcing traffic, device, and data separation for stronger control. And, as new threats become known, all firewalls in the environment can be dynamically updated to protect against them.

INTEGRAL CLOUD SECURITY

As enterprise networks expand, the Fortinet Security Fabric can scale deep into the cloud. Virtual firewalls can be deployed in your private cloud, as well as in your public cloud IaaS environments, for north-south and east-west microsegmentation. Coupling Fortinet's Cloud Security with your existing enterprise firewall deployment seamlessly extends the same powerful security at scale, as well as the same intelligence and dynamic risk mitigation to applications located either in the cloud or on-premises.

Customers will be able to run any application across vSphere-based private, public and hybrid cloud environments. It will be delivered, sold and supported by VMware as an on-demand, elastically scalable service and customers will be able to leverage the global footprint and breadth of services from AWS.

With the security consistency on VMware architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive business value from use of the AWS and VMware hybrid cloud experience without compromise.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

August 25, 2017 11:19 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:SB-VMware-for-Cloud:sb-fgvm-vmc-on-aws