FORTINET

WHITE PAPER

Securing Your Public and Hybrid Cloud

Scale and Segment Cloud Security on Demand

Introduction

Virtualization is generally the first step when business paces from traditional data center onto the cloud migration journey. Cloud by definition is a pool of API resources that can be rapidly provisioned or released through cloud service providers' APIs for enabling ubiquitous, elastic, scalable, on-demand access to a shared pool of configurable compute, networking, and storage resources. The nature of "software-defined" everything in the cloud makes it easier to implement with great privileges and yet come even great responsibility for security implementation. Cloud migration is not a one-way street, and it's very common to see hybrid cloud deployments based on business workloads coexisting in the enterprise both on premise and at hosted cloud providers.

Fortinet Cloud Security enables organizations to securely and elastically scale protection to their private, public, and hybrid cloud infrastructure and workloads, and to segment both within the cloud and between endpoints, enterprise networks, and the cloud.

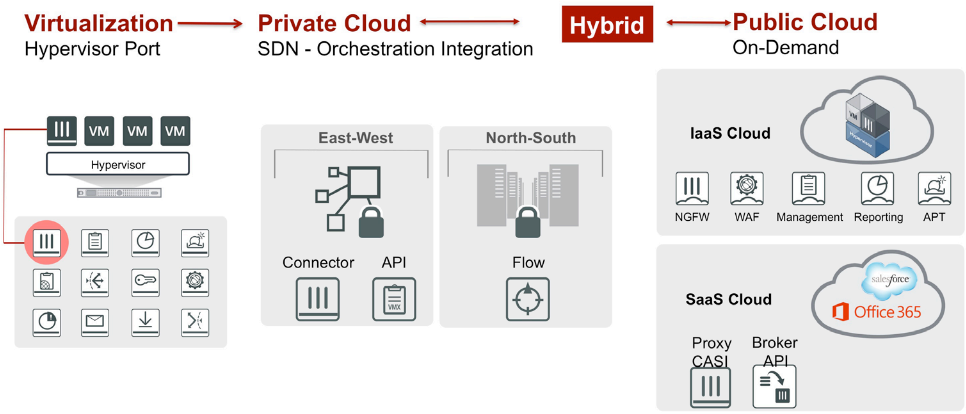

FIGURE 1: SECURITY FOR THE CLOUD

Security Paradigm Shift

Unlike an organization independently building a data center infrastructure, cloud-based infrastructure as a service (IaaS) is built and aggregated through pools of resources and is designed to be elastic to scale with organizational demand. The leasing and subscription model changes how security is designed and implemented, as cloud consumption transitions from traditional CAPEX to OPEX in the public cloud. The security paradigm shifted from protecting a big-perimeter walled garden to micro-segmented security control of business workloads. IT infrastructure becomes shifted from end-to-end complete data center ownership to owning just enough for the workload to operate in the cloud. IT architecture becomes shifted from static approaches to elastic capacity with on-demand metering consumption. This paradigm shift applies to both cloud ingress/egress (northbound-southbound) and lateral (eastbound-westbound) network traffic flow.

Legacy Data Center	Cloud (Public/Private/Hybrid)
• Big-perimeter "walled garden"	• Micro-perimeters per workloads
• End-to-end ownership	• Own just enough
• Build it all yourself	• Focus on your core value
• Server-centric approach	• Service-centric
• Self-managed services	• Platform services
• Static architecture	• Continuously evolving
• De-centralized administration	• Central control plane (API)

FIGURE 2: SECURITY PARADIGM SHIFTED

According to Gartner's strategic planning assumptions on "How to Make Cloud IaaS More Secure Than Your Data Center":

- Through 2020, workloads that exploit public cloud IaaS capabilities to improve security protection will suffer at least 60% fewer security incidents than those in traditional data centers.
- Through 2020, 95% of cloud security failures will be the customer's fault.
- Through 2020, 99% of vulnerabilities exploited will continue to be ones known of by security and IT professionals for at least one year.

As the cloud IaaS technology continues to evolve and mature, the majority of the security responsibility falls on how the business secures and governs the applications and data on cloud IaaS.

Well-defined Roles in Securing the Public Cloud

For securing the public cloud, it is imperative to follow the "Shared Responsibility" model as espoused by industry groups like the Cloud Security Alliance (CSA) and providers including Amazon AWS and Microsoft Azure. These can be divided into two components — *Security OF the Cloud and Security IN the Cloud*.

Security OF the Cloud comprises what the cloud provider, such as AWS and Azure, will provide. This represents literally all data center components for the cloud IaaS.

Security IN the Cloud comprises what cloud tenants are responsible for implementing with their security solutions.

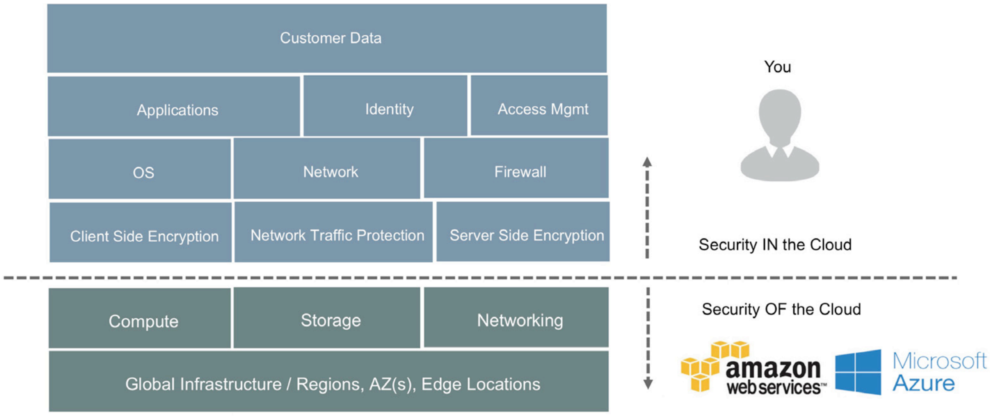

FIGURE 3: SHARED RESPONSIBILITY - REDUCE SECURITY COST + MAINTAIN FLEXIBILITY, ACCESS, AND CONTROL

Legacy security technologies coming into the cloud are still using appliance-based solutions, host-based agents, and manual audits. To achieve a truly consistent security posture in the cloud, businesses need to make the new mentality shift to move critical data away from the monolithic host-centric security model and start leveraging components available from public cloud-based web services. Rather than simply acquiring standalone security appliance that introduce security management challenges, they should instead consider cloud security solutions with centralized management and visibility across all deployment nodes. Point solutions today without extensions into cloud APIs are due to fail when they hit the point of scaling elastically in the cloud.

Fortinet Security Solutions for Public Clouds

Cloud deployment is not meant to replicate what it's done in the traditional data center. Fortinet has purposefully built cloud appliances for Amazon Web Services (AWS) CloudFormation or Microsoft Azure Resource Manager (ARM) templates to take advantage of cloud API-driven functionalities.

The Fortinet Security Fabric-ready APIs fully support AWS and Azure and help extend the security intelligence across the cloud. Fortinet further embraces AWS Auto Scaling web services to provide better capacity planning through automation.

With a global presence across all regions in public clouds, Fortinet further helps customers and partners meet their security goal of providing applications and data close to their geographical user bases. Geopolitical compliance can be further provided through Fortinet FortiOS intelligence and reporting.

Fortinet Security Fabric for the Cloud

The Fortinet Security Fabric extends Fortinet's cloud security solutions across the entire enterprise attack surface. Virtualization is a core component of the security fabric that enables applications and data to be delivered efficiently in an on-demand manner through software-defined orchestration. Business workloads can be replicated and automated through preconfigured templates to increase agility and high availability.

It is also critical to have single-pane-of-glass management and to own the control plane over cloud resource abstraction, so that businesses can embrace this new dynamic, automated, services-oriented architecture and improve control and visibility in varying cloud deployments.

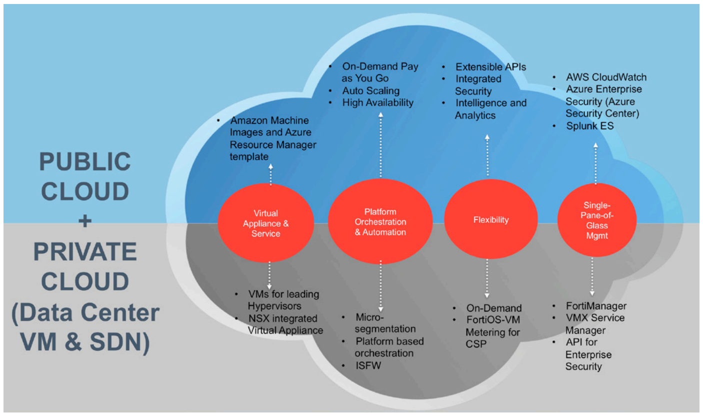
PUBLIC CLOUD
+
PRIVATE CLOUD (Data Center VM & SDN)
Amazon Machine Images and Azure Resource Manager template
On-Demand Pay as You Go
Auto Scaling
High Availability
Extensible APIs
Integrated Security
Intelligence and Analytics
AWS CloudWatch
Azure Enterprise Security (Azure Security Center)
Splunk ES
Virtual Appliance & Service
Platform Orchestration & Automation
Flexibility
Single-Pane-of-Glass Mgmt
VMs for leading Hypervisors
NSX integrated Virtual Appliance
Micro-segmentation
Platform based orchestration
ISFW
On-Demand
FortiOS-VM Metering for CSP
FortiManager
VMX Service Manager
API for Enterprise Security

FIGURE 4: FORTINET SECURITY FABRIC FOR CLOUD SECURITY

Fortinet supports on-demand hourly and annual metering subscriptions in the cloud marketplace, as well as bring your own license (BYOL) for perpetual consumption. As clouds are driven by the need to reduce CAPEX and OPEX expenditures. Fortinet provides the broadest set of service-driven portfolios that can be deployed in micro-segmented clouds without compromising holistic security intelligence.

The key principles of cloud security implementation in the Fortinet Security Fabric are:

- Scalable – high-performance firewalls and network security appliances that scale from IoT to branch offices to the enterprise campus to the hybrid cloud
- Aware – integrated with underlying cloud infrastructure to be aware of dynamic changes in the cloud environment and to provide seamless protection
- Secure – micro-segmentation and internal segmentation in the hybrid cloud extended with end-to-end segmentation across the entire attack surface
- Actionable – integrated into SIEM and other analytics in private and public clouds, with the ability to orchestrate changes to FortiGate and other Fortinet security policy/posture automatically in response to incidents and events
- Open – built on an extensible platform with programmatic APIs (REST and JSON) and other interfaces to integrate with hypervisors, SDN controllers, cloud management, orchestration tools, and software-defined data center and cloud

Hybrid IT Infrastructure

A hybrid cloud that mixes on-premise data centers/private clouds with public clouds requires rigorous management. Fortinet helps organizations build a cohesive security infrastructure that is easy to deploy, manage, and extend. Using the fabric-ready API framework, Fortinet seamlessly integrates orchestration and automation to work across the mixed cloud environments. This increased agility, flexible consumption, and automation help DevOps teams own the control plane and respond to changes in the cloud environment more efficiently.

Fortinet helps maintain consistency in security posture across clouds with a familiar look and feel in tools and resources. By extending the data center with consistent management, organizations can get enterprise-grade performance and security in the data center and in the cloud, as well as meet changing business needs with greater flexibility and capacity on demand.

FortiGate Security Platform

The FortiGate family of physical and virtual security appliances provides the foundation for securing private and public cloud environments. High-end physical FortiGate appliances provide highly scalable north-south data center firewall and network security protection at the edge or core of the private cloud. Virtual FortiGate appliances provide north-south protection for public clouds, as well as east-west segmentation within and across the hybrid cloud.

All FortiGate physical and virtual security appliances share a common FortiOS firmware with consolidated multi-function security, from firewall to intrusion prevention to next-gen firewall to anti-malware to web filtering, and more, and receive consistent FortiGuard threat and content updates from Fortinet's fully in-house FortiGuard Labs threat research team.

Fortinet Virtual Appliances

In addition to the flagship FortiGate platform, nearly a dozen other Fortinet security and networking solutions are available, not just as physical appliances but also as virtual appliances, from web application security to sandboxing to analytics to application delivery, for deployment in private and public cloud environments.

Agile Software-Defined Security

Fortinet's Security Fabric for the clouds enables orchestration and automation of both physical and virtual FortiGate security appliances in the hybrid cloud. Through a rich set of RESTful and other programmatic APIs, FortiGate appliances can be tightly orchestrated and automated with leading software-defined cloud platforms.

Orchestration in the Public Cloud

FortiGate security solutions are tightly orchestrated with leading public clouds like AWS and Azure to provide on-demand provisioning, pay-as-you-go pricing, elastic auto-scaling, and unified security analytics that enhance protection and visibility in the public cloud environment.

Single-Pane-of-Glass Visibility and Control

A workload should have the same secure and compliant posture regardless of whether it is running in a private cloud or public cloud, or whether it may migrate from one to another in a hybrid strategy. Fortinet's central management solutions, including FortiManager and FortiAnalyzer, provide a single consolidated view of security policies, governance reporting, and event monitoring regardless of physical, virtual, or cloud infrastructure, and across private, public, and hybrid clouds.

Conclusion

Rapid enterprise adoption of private and public clouds is driving the evolution of cloud security. Agile and elastic cloud security solutions need to fundamentally scale protection and segmentation within and across cloud environments. Fortinet's FortiGate security platform and cloud security solutions secure private, public, and hybrid clouds, and extend protection seamlessly via the Fortinet Security Fabric across the entire enterprise from IoT to data center to cloud.

FORTINET

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
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Aug 5, 2016