FORTINET

WHITE PAPER

Scale and Segment the Cloud

Fortinet Solutions for Private, Public, and Hybrid Clouds

Introduction

In the past decade, enterprises have been adopting cloud computing at an unprecedented pace, with Gartner Research projecting IT spending on public cloud-based infrastructure services to surpass $24 billion in 2016, and associated management and security to surpass $8 billion. Meanwhile, private cloud infrastructure including virtualization and software-defined networking (SDN) is rapidly transforming on-premise data centers, which still host the majority of enterprise server workloads worldwide. At the same time, heightened awareness and concerns of advanced malware and threats make it urgent to protect end users and data, regardless of where workloads and applications reside.

Cloud Benefits

- Elastic capacity and scale
- Agile provisioning and deployment
- On-demand consumption and pricing

Cloud Security Requirements

- Scale protection with elastic workloads
- Segment traffic within and across clouds
- Ensure single-pane-of-glass visibility and control

Types of Cloud Deployments

How are organizations embracing the cloud today? Rapidly maturing technologies mean that cloud computing really encompasses a number of different deployment methodologies and approaches that complement each other.

Public cloud – Perhaps the most visible type of cloud computing are the public cloud services offered by Amazon Web Services (AWS), Microsoft Azure, and other telcos and service providers. Also commonly referred to as infrastructure as a service (IaaS), public clouds evolved from the physical hosting of dedicated server space (e.g., cages, power, cooling) to more agile models for hosting applications and workloads logically encapsulated as virtual servers and typically running on shared multitenant infrastructure.

While the most basic form of IaaS is virtualized compute services (i.e., hosting of virtual machines), public clouds deliver infrastructure ranging from storage to networking to security as cloud-based services. Furthermore, many public clouds also offer platform-as-a-service (PaaS) capabilities such as databases, analytics, and web services.

Private cloud – Within the internal data center, enterprises had been adopting server virtualization, as initially popularized by VMware, for IT efficiency and data center consolidation for a number of years before serving as a foundation of private cloud computing. But the notion of private clouds is more than just a virtualized data center; instead, internal data centers are being transformed by successive waves of technology from softwaredefined networking (SDN) to SD-WAN, tiered storage, and other so-called software-defined data center (SDDC) technologies. These converged and orchestrated layers of logical infrastructure enable internal IT teams, or rather IT as a service (ITaaS), to deliver internal infrastructure with the same flexibility and often economies as offered by public cloud providers.

Hybrid cloud – Today's reality is that rather than treating public cloud vs. private cloud as an either-or choice, most organizations are moving to long-term strategies of deploying servers and applications on a combination of both private and public cloud infrastructure. The persistence of both internal and externally hosted platforms additionally dictates migration of large volumes of data and applications, persistent site-to-site connectivity, and stretching of network topologies across the WAN.

Software as a service (SaaS) – As an alternative to deploying applications on cloud-based infrastructure, IT organizations can instead choose to procure web-based applications designed from the ground up to be delivered from the cloud, including popular applications like Salesforce.com, Office 365, and Dropbox. While appearing to be very different from IaaS clouds like AWS, software as a service (SaaS) really represents another fundamental cloud computing approach where the underlying infrastructure, from compute to security, is the responsibility of the SaaS vendor (who may in turn deploy on another provider's IaaS/PaaS platform).

Benefits of the Cloud

Despite the disparate types of cloud deployments, they are unified in common characteristics and benefits that define the very notion of cloud computing.

First, cloud environments are designed to scale elastically to much larger capacities than traditional IT environments, especially when talking about provider clouds designed for multi-tenant economies of scale. Elasticity is not just about being able to handle very large capacities, but also the ability to ramp capacity up and down quickly on demand for applications of any size and scale.

Next, through software-defined abstraction and virtualization, monolithic hardware can be organized into more logical units that can be more easily orchestrated and automated for differing needs. This provides agility to provision, configure, and deploy infrastructure and applications nimbly and quickly for different organizations, business units, or projects, while still maintaining high efficiency of utilization of the underlying IT resources.

Finally, organizations increasingly expect to be able to consume infrastructure on demand, starting and stopping instantly, and paying for only the capacity they need at any given time on a metered (i.e., utility-based) model. While more common with public computing resources, organizations are increasingly looking to shift IT costs from capex- to opex-based pricing models regardless of where the infrastructure resides.

Key Security Considerations for Cloud Environments

Organizations need to continue to maintain a strong security posture in private and public clouds, even increase security to deal with the more dynamic and fast-paced cloud environment as compared to previously static data centers.

	Private Cloud	Public Cloud	Hybrid Cloud
Scale protection	■ Automate service insertion and chaining of security appliances in virtual and software-defined networks ■ Auto-provision firewall and security rules to new web and app instances	■ Autoscale network security capacity with elastic workloads ■ Auto-provision firewall and security rules to new web	■ Provide site-to-site VPN connectivity to migrate workloads to provider clouds ■ Provide remote VPN access to administer workloads in the cloud
Segment traffic	■ Isolate applications and data in increasingly consolidated environments ■ Micro-segment increased east-west traffic in virtual and software-defined environments ■ End-to-end segmentation between private cloud, campus, and branch offices	■ Isolate applications and workloads ■ Ensure privacy and compliance in hosted provider environments	■ Segment persistent connections between private and public clouds ■ Inspect persistent traffic between clouds ■ Inspect for leakage of data between internal network and provider cloud

Scaling Protection for the Cloud

IT organizations themselves, often in conjunction with a DevOps deployment philosophy, are often being driven by C-level or line-of-business efforts to accelerate IT and the business itself, such as through social, local, and mobile initiatives. So while initially adopted for non-critical test and development purposes, cloud computing today is often being used in production for developing and delivering highly scalable applications rapidly to customers, partners, and other end users.

At the same time, ensuring user confidentiality and data privacy is paramount, so that a security breach does not violate the very user trust and relationships that are the goal in the first place. Security needs to scale with the cloud infrastructure itself, so that it can provide transparent protection without slowing down the business. So as applications spin up and down with user demand in both private and public clouds, appropriate security rules should be automatically provisioned to new virtual machine instances.

In private clouds, IT teams are rolling out softwaredefined networking and other SDDC technologies on top of virtualization to rapidly provision and deploy applications. With these increasingly abstract and logical networks, security teams need to orchestrate the service

insertion and chaining of firewall and network security capacity automatically as networks and applications themselves are stood up at the logical layer, and with virtualization hosts and switches and the physical layer.

In public clouds, cloud providers are responsible for delivering agile compute and networking infrastructure on demand, but enterprise tenants are generally responsible for procuring virtualized security such as intrusion prevention and anti-malware for their workloads. Security should be orchestrated to itself be available on a pay-as-you-go basis just like the underlying compute infrastructure, and furthermore to maximize OPEX efficiency by automatically scaling firewall and security capacity with the workload capacity.

What about the hybrid cloud? Organizations are increasingly shifting existing and new application from internal data centers to cloud providers as they gain familiarity with public clouds, and they need secure VPN connections to migrate large volumes of data from the internal network to the cloud provider. They also need to provide remote VPN access for administrators and developers to deploy and manage those applications in the cloud. As most organizations are planning for a persistent hybrid cloud strategy, they require persistent site-to-site VPN connections between their edge firewalls at both the private cloud and public cloud.

Segmenting the Cloud

With the IT efficiencies gained by pooling compute, storage, and network resources through virtualization, SDN, and other technologies, private and public clouds have become increasingly aggregated environments, where not just servers but entire data centers have been consolidated into fewer cloud environments. The mix of data center traffic has further shifted from north-south to east-west as these software-defined environments continually optimize underlying hardware utilization and efficiency on flatter scale-out architectures.

All of this means it is more critical than ever to isolate business units and applications and segment eastwest traffic to minimize the impact of a hacker or advanced threat that breaches the cloud perimeter via a single weak or vulnerable application. Organizations should employ an end-to-end segmentation strategy, including internal segmentation firewalling within and across data centers, campuses, and branch offices. Within the private cloud, advances in network virtualization and orchestration mean organizations can and should consider an even finer micro-segmentation strategy that can firewall workloads irrespective of physical network topology, even down to a single virtual workload.

Many organizations are employing hybrid cloud strategies where public clouds are used to host more exposed public-facing workloads with less sensitive data; therefore, public clouds with persistent VPN connections should be segmented from private clouds that need to be more secured. Conversely, some organizations may use the public cloud to host some sensitive data, such as credit card data subject to PCI compliance, to alleviate strict industry compliance and regulations on the private cloud. Segmentation between the public and private portions of the hybrid cloud is equally important in this approach. Besides firewalling and intrusion prevention, data leakage protection (DLP) and monitoring may be important in either or both directions to ensure that sensitive data does not cross cloud boundaries, again to limit the damage or loss of a breach in a single-cloud environment.

Regardless of whether applications reside in a private or public cloud, data subject to regulatory compliance needs to be properly secured according to industry regulations such as PCI, HIPAA, FISMA, etc., with the added complication that enterprise tenants do not fully own and control the shared infrastructure in public clouds. The shared responsibility model for IaaS and SaaS divides security responsibility between tenants and providers, but both halves are critical to fully demonstrating and delivering compliance.

Fortinet Solutions for Cloud Security

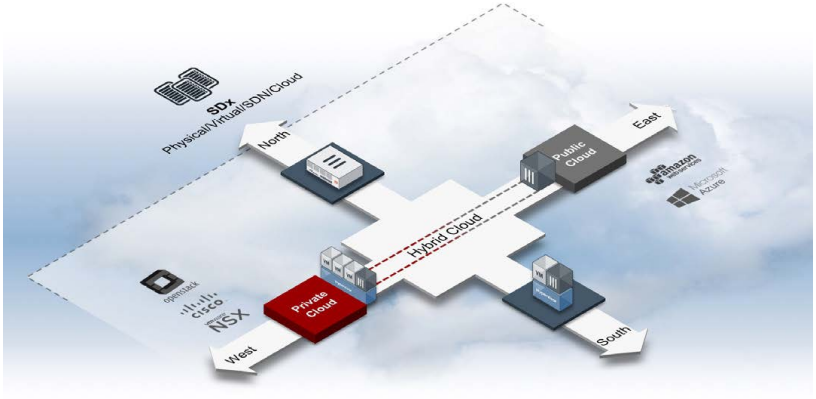

Figure 1: Cloud Security.

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 inhouse 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 Software-Defined Security (SDS) framework enables orchestration and automation of both physical and virtual FortiGate security appliances in private environments. Through a rich set of RESTful and other programmatic APIs, FortiGate appliances can be tightly orchestrated and automated with leading hypervisors, SDN controllers, and other orchestration platforms.

The FortiGate VMX solution for VMware NSX provides purpose-built integration with VMware vSphere and NSX environments, while FortiGate connectors for Cisco ACI, OpenStack, and HPE VAN SDN Controller provide out-of-box orchestration of existing FortiGate appliances with other leading SDN controllers.

Orchestration in the Public Cloud

FortiGate security solutions are tightly orchestrated with leading public clouds like AWS and Azure toprovide 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.

Security as a Service for Cloud and Managed Service Providers

Enhanced capabilities enable cloud and managed service providers to provide seamless Fortinet security as a cloud or managed service. Third-party validations by ETSI, EANTC, NIA, and other industry bodies of FortiGate virtual appliances to be orchestrated as virtual network functions (VNF) in multi-vendor network function virtualization (NFV) service chains enhance service interoperability and agility, while new pay-per-use models expand the availability of ondemand security offerings from a wide range of service providers.

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 and events regardless of physical, virtual, or cloud infrastructure, and across private, public, and hybrid clouds.

Fortinet Security Fabric Extends Intelligence Across the Cloud

The Fortinet Security Fabric extends Fortinet's cloud security solutions across the entire enterprise attack surface, via global and local threat intelligence. In addition, the integration of Fortinet's cloud security with the Fortinet Security Fabric enables:

- **Scalability** – high-performance firewalls and network security appliances that scale from IoT to branch offices to the enterprise campus to the hybrid cloud
- **Awareness** – integrated with underlying cloud infrastructure to be aware of dynamic changes in the cloud environment and to provide seamless protection
- **Security** – micro-segmentation and internal segmentation in the hybrid cloud extended with end-to-end segmentation across the entire attack surface
- **Actionability** – integrated into SIEM and other analytics in private and public cloud, with ability to orchestrate changes to FortiGate and other Fortinet security policy/posture automatically in response to incidents and events
- **Openness** – 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

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 segmention within and across cloud environments. Fortinet's FortiGate security platform and cloud security solutions secure private, public, and hybrid cloud, and extend protection seamlessly via the Fortinet Security Fabric across the entire enterprise from IoT to campus to cloud.

October 10, 2019 9:01 AM

488919-A-0-EN

D:\Fortinet\White Paper\Scale and Segment the Cloud\wp-scale-and-segment-the-cloud