FORTINET

Network Security for Every Flavor of Cloud

Table of Contents

FORTINET

Introduction

Cloud security must address unique requirements within each of its iterations. **Public** cloud relies on shared infrastructure and the need to operate in a common security model. **Private** cloud requires a software-defined approach to security due to the lack of visibility posed by east-west traffic and virtualized services. **Hybrid** cloud poses the challenge of combining critical internal resources with external connections and data sources, which increases the need to segment resources on the network.

Today's cloud security solutions can't just be designed to prevent attacks. They must assume that sooner or later there will be some sort of breach—yet remain resilient to ensure the protection of assets and users.

01: Security Matching the Cloud Paradigm

Fortinet's cloud security is designed to match the nature of the cloud itself—providing a dynamic resource that can change rapidly for protection across its various deployments (public, private, and hybrid).

Scalable—Security must match the scalability and elasticity of cloud workloads. Therefore, automation is a key feature of Fortinet cloud security. Risk and access policies are defined in advance so that when new devices enter the network to accommodate more users or additional bandwidth in the cloud environment, the devices will be configured automatically.

Single Pane of Glass—Policy, enforcement, and automation must be applied consistently across both static and dynamic resources with a single view of the overall security posture. Within our solution, workloads or systems categorized with a common risk profile are treated the same as they enter or exit the network— regardless of whether they are in your data center or your provider's.

Segmented—The ability to segment systems, workloads, or even specific network components is critical to managing business risk. The cloud also introduces new concerns regarding compliance. When data can traverse and even leave your network via the public cloud, data compliance must be enforced to ensure monitoring and control of specific traffic, applications, or data types.

02: Public Cloud Security

Public cloud represents the most high-profile security concern. Business leaders and users have only recently overcome the inherent skepticism of relinquishing control of their infrastructure, as well assharing systems and bandwidth with unknown third parties.

Fortinet's cloud security solution enables secure workloads in public clouds to ensure privacy and confidentiality while leveraging the benefits of scalability, metering, and time to market.

Shared Security Model—A shared security model provides two critical things:

- Security **"of" the cloud** includes all the data centers delivered by the cloud provider, which they are responsible for securing.
- Security **"in" the cloud** consists of what you, the cloud subscriber, provide in terms of data and applications in the cloud, which you are responsible for securing.

Fortinet cloud security addresses customer components such as your data and applications, operating systems, access and identity management, encryption, and network traffic. This complements the provider's security features to provide complete and compliant protection.

Provider Integration—Our solution also is designed for tight integration with your public cloud provider's security framework to protect compute power, storage, and networking. It also provides a common dashboard to view both sides and manage all aspects of security.

Fortinet public cloud security includes:

- Support for all of the top-five public cloud platforms: AWS, Azure, Google, IBM, and Oracle
- Support for leading Software-as-a-Service platforms, such as Office 365 and Salesforce.com (SaaS is another key form of public cloud that is as important to secure as Infrastructure-as-a-Service.)
- Cloud-ready multi-tenancy and virtual domain support for network segmentation
- Native cloud orchestration to automate autoscaling, high availability, and segmentation
- Extensible management interface—APIs foradditional cloud automation and orchestration

03: Private Cloud Security

Virtualization serves as the building block that enables all forms of cloud computing—and it's an especially important consideration for private cloud security. Layered on top of that are software-defined networking (SDN) and other kinds of software-defined infrastructure that create agile private clouds evolving out of traditional data centers.

Fortinet's software-defined security solution is certified by leading SDN and network function virtualization (NFV) platforms and can be applied to any data center transformed into a cloud environment.

Shared Security Model—With the growth of SDN, networking resources are no longer physically tied to dedicated hardware. Instead, they operate as services in the data center with the ability to function across physical elements or locations. Similarly, Fortinet's private cloud solution was designed to offer security "services" that can be dynamically configured and provisioned. This evolutionary approach extends security to each conceptual layer of the network architecture—from data plane to control plane to management plane.

Application-Centric Security—While many applications share the same physical infrastructure in a private cloud, they typically don't present the same risks. Fortinet cloud security isolates data and applications as the data center continues to consolidate. As east-west traffic increases in software-defined environments, our solution offers micro-segmentation to further separate specific types of traffic.

Fortinet private cloud security includes:

- Support for leading SDN platforms, including VMware NSX, Cisco ACI, and OpenStack
- Additional NFV orchestration for service insertion and chaining in multi-tenant service provider environments and clouds
- Multi-tenant and virtual domain support for network segmentation and security service function deployment
- Extensible management interface—APIs for cloud automation/orchestration
- Integrated single-pane-of-glass management
- Unmatched portfolio breadth and flexible deployment options

04: Hybrid Cloud

Most organizations are in the process of moving from an on-premises data center to a public cloud service and planning to maintain a combination of both conventional IT and public cloud deployments. Building a dynamic hybrid cloud requires open and secure migration of large volumes of data and applications, reliable site-to-site connectivity, and stretching of network topologies across the WAN.

Fortinet's hybrid cloud solution gives your security team visibility to see the entire picture—including end-to-end management, segmentation, and securing external connections.

Single-Pane-of-Glass Management—With resources spread across both the physical and virtual realms, security professionals shouldn't flip between multiple dashboards for visibility or operate without central analytics for threat intelligence. Fortinet's hybrid cloud solution provides a single, integrated view across all systems operating in the cloud and enables centralized management. This allows you to track data flows across the entire network in a format that makes that information relevant and actionable.

Segmentation—Fortinet's hybrid cloud security identifies business units and critical applications not directly associated with mixed hybrid environments and segments them to minimize the impact in the event of a breach. It also enables the ability to inspect persistent traffic between cloud segments to protect against data loss and to make sure that data is routed based on risk and policy.

Secure Connectivity—Migrating data between locations, loading large datasets from external sources, and taking advantage of third-party, cloud-based analytics services—these all require discreet connections to external networks. Our solution provides the right protection based on the risk profile of these unique network connections. It also enables robust VPN functionality, including the ability to provide secure temporary access to resources when needed, while protecting the rest of the network.

Fortinet hybrid cloud security includes:

- Auto scale of network security efficiency and capacity planning
- Centralized management for automatic provisioning
- Site-to-site VPN connectivity
- Segmentation of persistent connections
- Full visibility and control into security logs for better compliance governance

Conclusion

Fortinet is the only company with security solutions for network, endpoint, application, data center, cloud, and access that are designed to work together as an integrated security fabric and provide true end-to-end protection.

Our purpose-built cloud security solution collaborates with key Fortinet products for varying cloud deployment models, while allowing for centralized management, open API integrations, metering consumption, cloud platform orchestration, and automation.

The Fortinet Security Fabric shares threat intelligence dynamically with the rest of the interconnected security infrastructure. This reduces the need for multiple touch points and redundant policies across cloud premises and ensures governance over multilayered security boundaries.

FORTINET

www.fortinet.com

144489-A-0-EN

October 26, 2019 4:54 AM

eb-network-security-for-every-flavor-of-cloud