FORTINET

Defining Security for Today's Cloud Environments

Security Without Compromise

Table of Contents

FORTINET

Introduction

Enterprises have rapidly incorporated cloud computing over the last decade. Private cloud infrastructure (including virtualization and software-defined networking) is in the process of transforming onpremise data centers, which host the majority of enterprise server workloads around the world. At the same time, enterprises embracing public clouds at an unprecedented rate, with most connecting back to on-premise environments in a true hybrid cloud. But the problem of ever-evolving persistent threats makes protection of end-users and sensitive data an increasingly urgent concern, considering that accelerated infrastructural changes might expose new defensive gaps.

As today's enterprise data centers evolve from static internal environments to a mix of private, public, and hybrid clouds, organizations need to augment traditional firewalls and security appliances (deployed for north-south traffic at the network edge) with expanded protection for east-west traffic, both within internal networks and across clouds.

01: Stretching Beyond Static Security

Cloud computing really encompasses a number of different deployment methodologies and approaches that complement each other. But despite the disparate types of deployments, they share common characteristics and benefits that define the very notion of cloud computing.

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

To maintain a strong security posture in private, public, and hybrid clouds, organizations need to increase security to keep pace with these more dynamic and fast-paced environments. There are two specific areas that require additional attention to protect critical assets and users from outside threats.

Scaling Protection

Cloud computing enables rapid development and delivery of highly scalable applications. But this capability isn't worth much if an organization can't maintain the trust of users by ensuring confidentiality and data privacy at the same time.

Security needs elasticity to scale with the cloud infrastructure itself and to provide transparent protection without slowing down the business. As applications spin up and down with user demand in both private and public clouds, appropriate security rules should be automatically provisioned to new wvirtual machine instances.

Segmentation

With the IT efficiencies gained by pooling resources (e.g., compute, storage, network) through technologies such as virtualization and software-defined networking (SDN), cloud environments have become increasingly aggregated, to the point where entire data centers can be consolidated. The mix of data center traffic has shifted from north-south to east-west as these software-defined environments continually optimize underlying hardware utilization and efficiency on flatter scale-out architectures.

If a hacker or advanced threat breaches the cloud perimeter via a single vulnerable application, however, there's typically little to protect critical assets within the flat and open internal network. To minimize that serious potential for damage and loss, organizations need to isolate business units and applications. Networks need to be intelligently segmented into functional security zones to control east-west traffic.

02: New Defenses for Cloud Environments

In terms of elastic security, today's cloud environments require physical firewalls that provide highly scalable north-south data center firewall and network security protection at the edge of the private cloud. They also need virtual firewalls that provide north-south protection for public clouds.

High-performance firewalls and network security appliances need to scale vertically to meet volume and performance demands, as well as lateral scalability to seamlessly track and secure data from IoT/endpoints, across the distributed network/data center, and into the cloud.

- **Private cloud - scaling protection** automates service insertion and chaining of security appliances in virtual and software-defined networks. It also auto-provisions firewall and security rules to new web and app instances.
- **Public cloud - scaling protection** auto-scales network security capacity with elastic workloads, while auto-provisioning firewall and security rules to new web and app instances.
- **Hybrid - scaling protection** provides site-to-site VPN connectivity to migrate workloads to provider clouds, as well as remote VPN access to administer workloads in the cloud.

End-to-end segmentation provides deep visibility into traffic that moves east-west across the distributed network, limits the spread of malware, and allows for the identification and quarantining of infected devices. A robust end-to-end segmentation strategy includes internal segmentation firewalling across data centers, campuses, and branch offices.

- **Private cloud - segmentation** isolates applications and data in increasingly consolidated environments. It employs end-to-end segmentation between private cloud, campus, and branch offices. Organizations should also consider an even finer micro-segmentation strategy—firewalling workloads regardless of physical network topology, down to a single virtual workload.
- **Public cloud - segmentation** solates applications and workloads while ensuring privacy and compliance in hosted provider environments.
- **Hybrid cloud - segmentation** targets the persistent connections between private and public clouds and inspects the traffic between the two. Additional layers of protection are critical within hybrid cloud environments, especially considering the increasingly porous nature of network perimeters.

The underlying security infrastructure should offer automatic awareness of dynamic changes in the cloud environment to provide seamless protection. It's not enough to detect bad traffic or block malware using discrete security devices. Security should be integrated into SIEM and other analytics in private and public clouds, with the ability to orchestrate changes to security policy/posture automatically in response to incidents and events. The individual elements need to work together as an integrated security system with true visibility and control.

Solutions should also be 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 softwaredefined data centers and clouds. This enables security that dynamically adapts to the evolving network architecture and the changing threat landscape.

03: How To Choose a Cloud Security Solution

When evaluating a security solution, there are a few general questions to start with.

- **Is it scalable?** A comprehensive security strategy must be elastic in both depth (performance and deep inspection) and breadth (end-to-end).
- **Is it aware?** You need to not only track how data flows in and out of your network, but also how it moves within the perimeter and who has access to it.
- **Is it really secure?** The different tools that protect your network need to work together as an integrated system with visibility and control.
- **Is it actionable?** You need a common set of threat intelligence and centralized orchestration that allows security to dynamically adapt as new threats are discovered.
- **How open is it?** Well-defined, open APIs allow technology partners to become part of the fabric—helping to maximize investments while dynamically adapting to changes.

Other specific features to look for might include:

- **Software-defined security:** Look for a unified security platform with a single OS to enable orchestration and automation across physical, virtual, and cloud-based security.
- **Integration:** Solutions should integrate with VMware vSphere and NSX environments as well as public cloud environments like AWS and Azure to provide on-demand provisioning, pay-as-you-go pricing, elastic auto-scaling, and unified analytics that enhance protection and visibility.
- **Single-Pane-of-Glass Visibility and Control:** Your security solution should include centralized management with a consolidated view of policies and events—regardless of physical, virtual, or cloud infrastructure.

Conclusion

The evolving enterprise network combined with the transition to a digital business model present some of the biggest current challenges to network security. Rapid adoption of private, public, and hybrid clouds is driving the evolution of cloud security.

The next generation of agile and elastic security solutions must transcend the static nature of their forebears to fundamentally scale protection while providing segmentation within and across cloud environments—helping organizations embrace the benefits of an evolving infrastructure while anticipating the attack vectors of current and emerging threats.

www.fortinet.com

81782-A-0-EN

October 25, 2019 10:12 PM

eb-defining-security-for-todays-cloud-environment