FORTINET

A Multi-cloud IT Infrastructure Demands 3 Key Requirements from Networking and Security

More than 90 percent of enterprises are adopting a multi-cloud strategy[1], and as they expand across multiple Infrastructure-as-a-Service (IaaS) cloud providers, their networking and security architectures must evolve. Specifically, enterprises are seeking a simplified and consistent way to connect their applications and workloads, improve the application experience for their users, streamline operations and costs with automation, increase their visibility into traffic patterns, and effectively apply consistent controls to reduce cybersecurity risks.

Here are three key requirements for networking and security when enterprises look to deploying applications across multiple IaaS clouds.

1. **Common networking and security policy and enforcement framework for repeatable deployments.** One of the key challenges for multi-cloud deployments is that public cloud providers have different proprietary architectures built on frameworks, application programming interfaces (APIs), and toolsets specific to each one. The right multi-cloud solution provides a networking and security architecture that spans across these clouds, leverages the native features and functions of each cloud, abstracts that functionality with APIs, and then manages these connections dynamically using automation.
2. **Application-aware networking for better user experience.** Another important challenge with current networking technologies connecting multiple clouds is the underlying transport's lack of awareness of different types of applications. It is important for the network to be application-aware to maximize the use of available resources, network conditions and capacity, control unimportant traffic, and understand end-user experience in order to deliver consistent performance for an organization's critical applications.

Some recent studies show that approximately 8 in 10 enterprises have moved beyond a "one cloud fits all" approach and are using two or more clouds to accelerate their digital transformation.

Enterprises are considering multi-cloud for their IT to:

1. Increase redundancy and resiliency
2. Decrease reliance on any one cloud provider
3. Leverage expertise and best-of-breed services
4. Meet data sovereignty requirements
5. Improve cost savings

3. **Integrated networking and security architecture for effectiveness and efficiency.** Multi-cloud deployments won't reach their full performance potential if networking and security are separated. Each layer tends to use different technologies from different vendors. This causes gaps in coverage, which makes the deployment vulnerable to attacks. Central oversight, coordinated enforcement, and integrated communications between networking and security layers will close the gaps and reduce the potential for attacks significantly through intelligent deep packet inspection and segmentation of the network traffic flowing between applications and workloads across the multiple clouds.

Next-stage Considerations

There are fundamental differences in architecture between on-premises, hybrid cloud, and multi-cloud deployment models. Cloud infrastructure is largely API-driven and it is designed for horizontal scaling (or scale-out) and rapid changes. In addition to that, it requires deep integration with underlying cloud platforms.

Security must be integrated with the network layer leveraging both cloud-native constructs (such as security groups) and advanced security such as intrusion prevention system (IPS), end-to-end high-performance encryption to protect network traffic, etc.

Enterprises adopting a multi-cloud approach can therefore benefit from a software-defined wide-area networking (SD-WAN) solution that provides a programmable, consistent, and cost-effective framework purpose-built for multi-cloud deployments.

[1] Kim Weins, "Cloud Computing Trends: 2020 State of the Cloud Report," Flexera, May 21, 2020.

July 31, 2020 7:13 AM

736813-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:POV:POV - Secure SD-WAN for MultiCloud:POV-Secure-SD-WAN-for-multicloud