Where Technology Means More®

Normalizing Policy in a Multi-cloud World

Contents

Introduction

We live in a distributed world. Customers access services and goods from around the globe daily, all while staying constantly connected and informed, thanks to the supercomputer they carry in their pocket. Maintaining business relevance in this world requires new application delivery models.

Cloud is a common answer to this question, but that is an oversimplification. Clouds are both private and public, with variants of each. Infrastructure, platform, and software as a service (IaaS, PaaS, SaaS) all have distinct advantages for certain requirements. In order to have the right tools for the job, multi-cloud solutions have become the norm.

Combinations of SaaS applications for CRM, productivity, collaboration, etc. are integrated with IaaS workloads and in many cases tied back to existing private infrastructure. The enterprise network is integrated with cloud assets and applications are now decentralized and delivered from a variety of global points.

Problem Statement

The first issue that arises from this is foundational. How do you ensure connectivity and performance in a distributed world? Gone are the days where a bank of VPN concentrators can funnel all of your employees back to all your off/on-premises applications. In today’s world, both the applications and employees are as likely to be distributed as they are to be in one place.

As this IT domain stretches further, visibility, and security become more challenging. In general, it’s harder to secure what you can’t see. That means the traffic happening directly between a remote user and a SaaS application is a trouble spot. Regaining visibility into this distributed traffic is a key first step.

Once visibility is established security can be enhanced. The issue now becomes policy. While a set of global policies can be defined for an application, those policies will be interpreted differently by each public or private cloud they reside on. Without a tool to normalize these ‘policy’ definitions, each new environment exponentially increases the risk and overhead for involved IT operations.

Background

Imagine booking a ticket online for your dream vacation. There is a good chance that web portal is being served by IaaS running in the cloud. Those cloud workloads may then be connected via VPN back to a private data center where a mainframe server processes data from a combination of cloud and local storage. All of the data created may then be fed to another cloud for Artificial Intelligence and Machine Learning (AI/ML) processing.

That’s one of a never-ending number of multi-cloud examples happening today. These use cases are often built as ‘one-off’ architectures. This creates complexity and risk as small IT silos are built to support specialized application behavior. This same one-off behavior complicates security. The results of this complexity show up as risks and decreased operational efficiency.

As applications were distributing, so were customers and teams. Remote work in some form is here for the long haul, whether it’s a first choice or a business continuity plan, it’s there. As work becomes remote, customers do the same. If they can’t be supported remotely, they find new companies to work with.

In the past, our IT systems were mostly designed with central consolidated hubs. Focal points where all things connected at some point, an enterprise network, a data center, etc. That hub provided centralized visibility, and therefore would be used as the focal point for security and other policy. Those hubs no longer exist.

Now the connectivity is fully decentralized. Users access on-premises assets through secure tunnels while directly accessing SaaS applications without ever crossing IT provided assets. This increases the attack surface while decreasing visibility. This is a bad combination. Making matters worse is the lack of quality controls and troubleshooting visibility.

Solution

The first step towards policy normalization is ensuring global visibility and connectivity for a distributed world. Your applications and users can only produce when connected, and it’s critical to have visibility into those connections. The connectivity must be adaptable and responsive.

Enterprise architectures like Cisco SD-WAN solutions are tailor fit to this use case. Cisco’s SD-WAN solution provides connectivity integration for everything from 5G Cellular to MPLS circuits, allowing a point of central visibility and control for all of your internal and external connections. It then provides Cloud On-Ramp capabilities to provide seamless connectivity to public cloud resources.

By integrating Cisco SD-WAN into your multi-cloud delivery you gain visibility and control. This leads to better user experience and application performance. It also provides the foundation for an integrated security architecture.

From the end-user to the cloud connection, Cisco’s security architecture provides the identity and access solutions to ensure secure connectivity. And your user Edge devices are protected by Cisco’s Umbrella security, providing protection from phishing and other exploits through Domain Name System (DNS) security. Umbrella transparently protects your users from malicious sites from trusted and customizable block lists.

Cisco’s CloudLock provides the other end of the spectrum. As a Cloud Access Security Broker (CASB), it provides an advanced set of security tools for users, applications and data in the cloud. Your data is continuously monitored through Data Loss Prevention (DLP) while apps are protected by CloudLock Apps Firewall.

To maintain security agility while delivering multi-cloud resources, it’s wise to work towards normalizing policy across platforms. Policy can be thought of as connectivity, security, and quality. That normalization requires an ability to globally define policy in an abstracted fashion so that it can be applied to disparate infrastructure.

An example would be global policy for a web app. When the app is deployed to Cloud A, the policy is translated into Cloud A's enforcement. If the app were moved to Cloud B, that same policy would be used to translate into Cloud B's enforcement.

This policy abstraction provides several benefits.

- Reduced risk with a single policy repository to maintain.
- Consistent policy enforcement.
- Enhanced cloud portability.
- Lower operational overhead.
- Increased operational agility.

This type of policy abstraction can be achieved across the multi-cloud network utilizing Cisco's Application Centric Infrastructure (ACI). ACI, as a component of a data center architecture, can be thought of as a policy automation engine. It stores policy in an abstracted fashion, and it can deliver that policy on-premises and multi-cloud. This provides normalization for a large portion of policy requirements. It also enhances operational efficiency through automating the provisioning of network policy.

To further normalize policy, Cisco provides an industry leading multi-cloud workload protection engine with Cisco Secure Workload (Tetration). Secure Workload provides policy discovery, automated policy build, and policy enforcement across public and private cloud resources. Because this enforcement is delivered at the workload level, Secure Workload ensures that security policy is normalized across any environment the workload resides in.

This normalization can be taken even further with enhanced visibility into the applications across clouds. With Cisco's AppDynamics any performance issues across your multi-cloud stack can be quickly detected and remediated. Meanwhile, the visibility it provides will assist with any migration or disaster recovery planning initiatives now or in the future.

Finally, we must connect our teams and customers wherever they are, and wherever they work. This requires flexible solutions for collaboration that seamlessly transition with users from desktop to mobile, and from the office to home. Cisco's collaboration suite, including Cisco

Unified Call Manager (UCM) Cloud, are design to deliver exactly that while integrating seamlessly into Cisco's SD-WAN and security solutions for highly efficient and secure operations.

Conclusion

Maintaining agility and operational costs, while distributing users and applications, is no easy task. Luckily, it's been a long time coming and the products and services have advanced to meet the challenge. The technology exists to normalize security policy for your users and applications centrally, and ensure that policy is enforced consistently wherever they are. The ePlus team are experts at bringing these technologies together to meet unique business challenges.

References

1. Cisco – https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/cloud-aci.html?dtid=osscdc000283
2. Cisco - https://www.cisco.com/c/en/us/products/security/tetration/index.html?dtid=osscdc000283