Multi-Cloud Security Network Policy and Configuration Management

An AlgoSec Whitepaper

Introduction

Digitally transforming their businesses with numerous new applications, mobility and big data, enterprises are rapidly expanding their networks. Taking advantage of cost and performance improvements, enterprise networks extend way beyond the traditional perimeter and now incorporate software-defined networks (SDN), micro-segmentation and multiple clouds.

The typical medium or large enterprise now manages a dynamic *heterogeneous network* that includes:

- Data centers
- Public clouds
- Private clouds

Traditional network security policy management within the data center has always been challenging enough. Multiple firewalls from different vendors, thousands of rules and hundreds of weekly or monthly changes call for their own careful management and automation. But as the network estate becomes even wider and more complex, coherent security policy now has to extend across the entire heterogeneous network that includes multiple public clouds (e.g., AWS, MS Azure, Google Cloud Platform), each with its own language and methods.

In the world of multi-cloud deployments, the need for cloud vendor-agnostic, holistic security policy automation becomes essential.

In this paper, we will discuss the major security policy issues that concern enterprises as they expand their networks across multiple clouds. We will explain how AlgoSec delivers a comprehensive, unified, vendor-agnostic automation solution that enables security managers to reduce risk, improve compliance and boost efficiency across the heterogeneous network including multi-clouds.

Where the Data Center Meets the Cloud

In the data center, AlgoSec automates network security policy *device vendor-agnostically*—that is, it provides a unified console from which security teams can holistically manage security policy across multiple data centers and network segments that include many firewalls and other network devices. The AlgoSec solution is vendor-agnostic, enabling security teams to use a common security interface to handle policy management regardless of type of network device.

The AlgoSec solution is able to tie security-policy management to business processes and applications, proactively assessing risk, ensuring continuous compliance in addition to quick provisioning, change, migration and decommissioning of network connectivity for business applications.

That businesses are migrating applications to private and public clouds doesn't change anything for AlgoSec. Neither do virtualization nor multi-cloud deployments. In fact, the accelerating deployment of heterogeneous networks greatly increases the need for an automated Network Security Policy Management (NSPM) solution like AlgoSec.

Migration to the Cloud and Virtualization – a Growing Trend

The network landscape of today differs radically from what we knew only a few years ago. For a variety of quantifiable reasons that include productivity, agility and costs, enterprises are migrating their applications to public and private clouds.

Public Clouds

Migration of applications to public clouds has become an indispensable strategy for enterprises as public clouds bring a great many advantages. The most popular of the public clouds, AWS, Microsoft Azure and Google Cloud Platform, have become part of the computing fabric of millions of enterprises.

Because of the proliferation of easy-to-use and cost-effective public clouds, enterprises leverage multiple cloud vendors. IDC estimates that nearly 80 percent of IT organizations are currently deploying, or are planning to deploy, multi-cloud environments. A study conducted by Microsoft and 451 Research, The Digital Revolution Powered by Cloud, stated that nearly a third of organizations already work with three or four cloud vendors.

The embrace of the multi-cloud environment can be attributed to the advantages each cloud vendor has to offer such as unique functions, proximity and pricing models. Since application requirements can vary greatly and require specific functions and capabilities to operate optimally, matching them to specific cloud vendors is important. Various cloud environments offer the functions and tools that deliver the best capabilities out of each application. Some public clouds excel in cost advantages, others in availability, still others in compute power. Businesses evaluate the advantages of each cloud to take advantage of the functions that will best support each application. Enterprises also worry about lock-in—a commitment to a single cloud vendor—that might turn them into a captive customer allowing that vendor to dictate the terms of service and costs. Businesses avoid lock-in by deploying applications across multiple clouds.

Private Clouds

As enterprises transform digitally, their data and applications grow exponentially. Network managers are constantly challenged to re-consider the network infrastructure that will best support business needs now and into the foreseeable future. Today, *private cloud* is one of their main considerations.

Private cloud is a type of cloud computing that delivers advantages similar to public cloud, including scalability and self-service, but through a proprietary architecture that the enterprises maintain themselves. While public clouds deliver services to any number of enterprises, a single enterprise establishes its own private cloud dedicated to its own needs. Therefore, private cloud is the best choice for enterprises who wish to control all the aspects of their computing and where it is easier to manage security and regulatory compliance.

According to Market Research Future, although not as widely adopted as the public cloud, the global private cloud market is still expected to grow explosively at 26% CAGR between 2017 and 2023 and reach a valuation of more that USD 50B by 2023.

Hybrid Networks

As a result of the distinct advantages and disadvantages of each type of cloud implementation, most enterprises utilize two or three types of environments: traditional data center processing, private clouds and public clouds, in many cases, employing multiple vendors for the cloud environments. Taken together, they give rise to the *heterogeneous network environment* or *hybrid network*.

Network Security Challenges in the Hybrid Network

Running applications across the hybrid network can prove eminently useful for business teams but extraordinarily challenging for security teams. The complexity of the heterogeneous environment introduces a new level of security policy management challenges.

We identify seven major challenges that must be addressed to ensure security and compliance across hybrid networks.

1. Visibility

The more heterogenous the network, the more complex it becomes. Complexity is the enemy of security. Across the vast landscape of physical equipment, virtual firewalls, and public-cloud network security groups, security teams find it difficult to obtain a clear picture of application-connectivity requirements and overall network security.

You can't protect what you can't see. Visibility is essential to security and rapid incident response. Obtaining full visibility across the entire hybrid network requires a deep understanding of the hybrid network's topology and the flows between:

- On-premise networks and cloud providers
- Multiple public cloud environments
- VPCs and v-NETs
- Regions within the same cloud providers
- Cloud environments and the internet

A study sponsored by Forbes surveyed professionals in enterprise IT departments about their cloud infrastructures. More than one-third said they lack visibility into their application operations in the public cloud.

Independent market research company, Vanson Bourne, conducted a survey to investigate the state of network security. In Hide and Seek: Cybersecurity and the Cloud, two-thirds of respondents cited network "blind spots" as a major obstacle to effective data protection.

Ixia's recent survey of senior IT staff in various organizations regarding their cloud security concerns concurred. The top concern with cloud adoption was the ability to achieve full visibility.

2. Maintaining Compliance Posture

Put bluntly, compliance is absolutely necessary for the business but is a nuisance for the IT staff. With the recent introduction of the GDPR and the growing body of legal and industrial regulations, compliance is taking up more and more effort and time of IT departments and especially security staff.

Keeping up with the numerous regulations that are found in a growing number of geographies and industries is challenging enough in a single-cloud-provider environment. Compliance challenges multiply rapidly in heterogeneous environments due to:

- The need to apply compliance processes for each regulation for each network entity
- Service contract terms and SLAs across the estate
- Compliance methodologies that work for one cloud vendor don't necessarily work for another

- Audits are point-in-time exercises, but most regulations require continuous compliance, tough to achieve in a dynamic environment
- Compliance needs to be documented for every entity and vendor, very tedious and time-consuming, and a drain on scant resources

The essence of information security regulations such as PCI-DSS, GLBA and HIPAA is to ensure the confidentiality and integrity of sensitive information. While these regulations are addressed by the best practices that IT departments have continuously implemented for years, the challenges are rapidly expanding in the heterogeneous environment. Due to the chronic lack of IT and security staff, teams are incessantly pulled in different directions. In many cases, it’s gotten to the point where IT staff are busy putting out security and operational fires and have little time to perform the critical strategic work such as addressing compliance issues at the network and cloud level. Multiple clouds just make the task that much harder.

3. Identifying and Mitigating Risks

Due to the dynamic nature of the hybrid (on-prem and cloud) network, numerous changes to security policies are likely to ensue. These changes will be implemented on all the devices that direct traffic and will likely be performed by the multiple stakeholders involved in the hybrid network such as application developers and DevOps in addition to cloud and security teams.

The ever-transforming environment necessitates close attention as risk may be introduced inadvertently by these changes. The risks within the complex hybrid-cloud estate will likely be too numerous and complex to be identified manually. Therefore, it’s imperative to obtain a dashboard that depicts all risks on a single screen. This dashboard should indicate the severity, the affected devices and rules, and the changes required to remediate each risk. The dashboard also requires the ability to notify pro-actively (via alarm) whenever the network is exposed to new risks.

4. Managing Application Connectivity

The growing body of applications requires a complex, multi-tiered, distributed and interconnected architecture supported by elaborate communication paths that cross other applications, servers and databases.

A Symantec analysis found that while most CIOs think their organizations use only 30 or 40 cloud applications, in fact, most have adopted an average of 928!

Even if they get a grip on their current application volume, network and security teams can’t consider themselves in control. There are constant upgrades and changes, and new applications to deploy, connect and secure. Business users demand that they be up and running immediately while security is hard-pressed to keep up.

Trying to manage application connectivity across on-premise, private and public clouds, each with multiple vendors, is prohibitively expensive in time and effort.

5. Managing Policies

Maintaining a clean set of firewall rules is a critical network-management function. Difficult enough in the data center, things really get out of hand when networks cross borders into the cloud. Private clouds add unique security controls such as ACI contracts and distributed firewalls. And each public cloud has its unique security controls such as cloud-native security groups, cloud-vendor firewalls (e.g., Azure firewall and AWS WAF), and 3rd-party cloud firewalls by the traditional firewall vendors (e.g., CloudGuard from Checkpoint and Palo Alto Networks' VM series). The proliferation of security controls that make up the hybrid, multi-cloud network multiplies policy-management complexity.

Maintaining a clean set of firewall rules is a critical firewall management function. Difficult enough in the data center, things really get out of hand when networks cross borders into the cloud. Adding more than one cloud further multiples the policy-management complexity.

Unwieldy rulesets are not just a technical nuisance, they also introduce business risks, such as open ports, unneeded VPN tunnels and conflicting rules that create the backdoor entry points that hackers love. Bloated rulesets significantly complicate auditing processes that require the careful review of each rule and its related business justification.

Examples of firewall rules that institute problems include:

- Unused rules
- Shadowed rules
- Expired rules
- Unattached objects (rules that refer to non-existent entities such as users who have left the company)
- Rules that are not ordered optimally (e.g., the rule that is "most hit" is near the bottom of the rule list)

These problems drive organizations to take on ad hoc firewall "cleanup" or "recertification" projects. The problems are magnified in enterprises with:

- A large number of traditional physical firewalls
- Firewalls from multiple vendors (Checkpoint, Cisco, Palo Alto Networks)
- Different types of platforms (on-prem, private cloud, public cloud)
- Different types of security controls (traditional firewalls, security groups, etc.)

Such complexities contribute to a lack of visibility, poor accountability, and undetected network breaches. They accumulate unnecessary costs for the business and waste precious IT time.

Enterprises across the board are well aware of the need to get a handle on security controls. Research by ESG indicates that 70 percent of organizations plan to unify security controls for all server workloads across public clouds and on-premises resources over the next two years.

6. Enforcing Security-Policy Consistency

The only constant in today's IT environment is change. Today, change occurs at a breakneck pace. As business needs transform (due to rapid business growth, mergers and acquisitions, new applications, decommissioning of old applications, new and departing users, evolving networks, new cyber threats), so must security policies—and fast.

Managing change can lead to major headaches for IT, security and cloud management teams who try to enforce consistent security policies across the heterogenous network. Maintaining consistency across the hybrid and multi-cloud network meets with many problems such as:

- Each security entity has a different way to manage policy changes. Lack of intricate understanding of the proper management of changes for each security entity can lead to critical business risks as benign as legitimate traffic blockage all the way to the entire business network going offline.
- Manual workflows and change management processes that are unique for each security entity can substantially slow down the change process, impeding IT agility.
- Some enterprises with a very complex heterogeneous network are so concerned about change control and its potential negative impact that they may resort to network freezes during peak business times so as not to suffer inexplicable outages.
- Changes are slow. It can take several days—sometimes weeks—to process a single change in a complex enterprise environment. Enterprises may implement hundreds of changes each month.
- It's difficult to assess the risk of a proposed change.
- The change process in a hybrid network involves disparate teams (security, networking, cloud, business owners). These teams speak different languages and have different objectives. They lack a unifying factor.

7. Handling Multiple Management Consoles

Each cloud vendor provides its own *console* that facilitates the day-to-day management of its cloud accounts and provides services such as monitoring cloud-resource usage, calculating current costs and the managing security credentials. In addition, each firewall vendor offers its own unique management console to manage all of its devices. Each vendor's console comes with its own language and GUI. To make network-wide policy changes that span firewalls and clouds, security staff must access multiple consoles forcing enterprises to employ a legion of experts just to implement even a simple change. Changes have to be meticulously coordinated across the many management consoles slowing down progress and introducing potential for errors.

8. Lack of Skilled Staff with Cloud-Security Knowledge

Despite all the advancements we have made in network security in recent years, enterprises still endure regular cyberattacks that continue to cause billions of dollars in damages. Effective network security professionals are now more important than ever. Yet, despite the urgent need (and handsome salaries), the world suffers from a severe scarcity in able and certified personnel. According to a recent McAfee study, The ramifications of the skills shortage on cloud security, IT leaders need to increase their security staffs by 24% to adequately manage their current threat landscape. But these people are simply not available.

The absence of adequately trained security professionals leaves gaps in many aspects of modern-day security infrastructure. In their report on security deficiencies, ESG found that 33% of responders indicated that their biggest deficiency was cloud security specialists followed by 28% who pointed to a deficiency with network security specialists and 27% who suffer a shortage of security analysts.

A security officer with expertise in any cloud environment needs to be familiar with the best practices of incident response and also must be proficient in cloud security practices such as identity access management (IAM), deployment automation and cloud regulatory compliance.

The requisite qualifications are amplified when the same officer needs to manage multiple cloud vendors. As security varies with each vendor. the multi-cloud security officer must know the security nuances of each cloud vendor and stay up to date with the ongoing security advancements of each. It is practically impossible to find such people.

Many network and cloud security positions remain unfilled forcing organizations to compromise.

The AlgoSec Solution for Heterogeneous Environments

AlgoSec delivers business-driven security management across on-premise, SDN, hybrid-cloud and multi-cloud environments. With AlgoSec, enterprises maintain a uniform security policy across their entire network estate. From a single console, security teams can see across their on-prem and virtual networks and into all their clouds. They obtain accurate policy change automation across their physical and virtual firewalls as well as into their public cloud deployments.

The AlgoSec approach bestows numerous critical benefits on the enterprise:

1) Visibility across the hybrid cloud and multi-cloud from a business-application perspective
2) Uniform security policy across complex hybrid cloud and multi-cloud environments
3) Compliance assurance across the hybrid cloud multi-cloud environments
4) Hybrid-cloud and multi-cloud security policy change automation with zero touch
5) Increased agility and responsiveness to business needs
6) Accelerated application delivery
7) Optimal training of security personnel—one console, one language—for the entire heterogeneous network

Executive Summary

AlgoSec delivers the acute visibility, automation and unified solution for managing the entire volume of hybrid-cloud security policies, configurations and controls to achieve and maintain security and compliance. Maintaining a robust security posture in such a complex environment that includes on-premise network equipment from multiple vendors, SDN, virtual, private and public cloud infrastructures necessitates *automation*.

AlgoSec is the leading automation solution for network security policy management. Used by 1,800 customers in over 80 countries, AlgoSec delivers end-to-end visibility and analysis of the hybrid network security infrastructure (including real and virtual firewalls, routers and cloud security groups), as well as business applications and their connectivity flows—across cloud, SDN and on-premise enterprise networks.

AlgoSec automates time-consuming and error-prone manual security-policy changes with zero touch, proactively assessing risk and ensuring continuous compliance. AlgoSec quickly provisions, modifies, migrates and decommissions network connectivity for business applications.

To discover more about Algosec's business-driven security management solution, visit www.algosec.com, or click here to request a demo.

Global Headquarters
65 Challenger Road,
Suite 320
Ridgefield Park
NJ 07660, USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
Tel: +44 207-099-7545

APAC Headquarters
Centennial Tower, Level 21
3 Temasek Avenue
Singapore 039190
Tel: +65 6549 7415

AlgoSec.com