THE CLOUD ARCHITECT'S GUIDE TO NETWORK SECURITY

Table of Contents

Overview

According to a recent IDC report, public cloud spending accelerated by 34% in 2020, while non-cloud IT infrastructure declined by almost 9%.[1] Cloud architects already understand the benefits of public cloud and are trying to help their organizations reap the benefits. These include faster application lifecycles, quicker time-to-value, rapid deployments with the support of continuous integration/continuous delivery (CI/CD) pipelines, and delivering innovation at an ever-increasing pace.

But at the same time, network security in public cloud deployments isn't keeping pace. Most solutions cannot provide enterprise-grade threat prevention or adequately defend these highly dynamic environments from advanced threat vectors. Regardless of the specific cloud service provider (CSP), every organization's data is processed and stored under the Shared Responsibility Model—along with many other security factors to consider.[2]

For anyone who's not a trained security expert, this can quickly become a daunting exercise. This eBook is designed to help cloud architects with some of the more important factors to consider when designing a security solution for cloud-native applications.

[1] "Public Cloud IT Infrastructure Revenue Growth Remained Strong in Third Quarter of 2020, According to IDC," IDC, January 12, 2021.
[2] "Cloud shared responsibility models are misunderstood, report says," CIO Dive, September 3, 2020.

Why is Network Security in the Cloud Different?

Public cloud environments are highly virtualized, dynamic, service-based, software-defined platforms. They provide a base architecture for operating anything from elastic compute, to containers and serverless designs, to services for building today's enterprise applications.

By its very nature, public cloud networking is not implemented in the same way as traditional data center networking. "Link-state" is replaced with application programming interface (API) calls. There are also a plethora of CSP network constructs to consider, including network address translation (NAT) gateways, transit, and virtual private network (VPN) gateways, as well as load balancers and their intrinsic network behaviors.

Many architectures utilize public cloud as a logical extension of an on-premise network, while others adopt a "Zero-Trust" Architecture (both externally and internally). When properly architected and configured, virtual private cloud/virtual network (VPC/VNet) and transit network constructs allow for true network segmentation and a "minimum blast radius" posture. Additionally, the concepts of centralization or decentralization within a CSP region, across regions, or across CSPs can be implemented depending on the application.

Lastly, residing on the cloud network architecture are the applications themselves—which are specifically built to auto-scale based on demand.

In short, the unique characteristics of cloud networks combined with the dynamic functionality of applications creates a pressing need for purpose-built, public cloud security.

A cloud network security solution must be flexible enough to accommodate your chosen architecture, considering both current and future states.

A cloud network security solution must have the inherent ability to learn and adapt to the dynamic nature of different applications and automatically provide protection in a similar auto-scaling manner.

The Shared Responsibility Model for Network Security

The shared security responsibility model means that a CSP covers some aspects of protecting a cloud deployment, while you and your security team provide the balance. As you architect various applications and workloads into the public cloud environment, the first fundamental for a successful implementation is understanding where the CSP's responsibilities end and where yours begin.

The second most important thing to understand is that you and your CSP do not share responsibility for a single, common security area. Whether you are using a server-based infrastructure-as-a-service (IaaS) instance, serverless system, Containers, or a platform-as-a-service (PaaS) cloud service, you are always responsible for the security of what is under your control. Put very simply—if you can control or configure it, then you need to secure it.

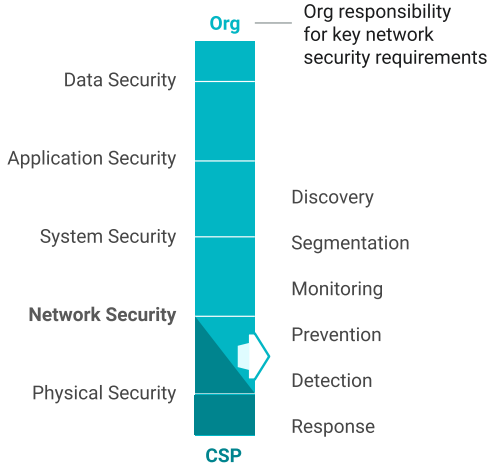

Figure 1: Shared responsibility for public cloud security

For anything under your control—threat detection, alerting, and security responses are your responsibility.

Most CSPs offer outstanding security guardrails. These may include network security groups (SGs/NSGs), network access control lists (NACLs), identity and access management (IAM) roles, robust distributed denial-of-service (DDoS) protection in the Layer 3/4 data plane, along with guidelines for the requisite physical security of hardware, underlying network access, and data centers themselves.

Make full use of CSP-provided guardrails. This means diligence in configuring available SGs, NACLs, IAM roles for "least privilege," and explicit routing.

When it comes to applications, you are solely responsible for securing anything that involves data, information, identity, access, and the configuration of services implemented. You also must take care to protect anything that connects with the public cloud—including on-premises data centers, user VPNs, as well as internal and external parties accessing your applications.

Data breaches are getting more expensive and they're frequently occurring due to misconfigured public clouds—19% of breaches happen because IT teams fail to properly protect the assets found within their cloud infrastructure. The dynamic nature of the public cloud makes misconfigurations even more difficult to minimize.[3]

[3] "Many data breaches are being caused by misconfigured clouds," TechRadar, May 5, 2021.

What Comprises Network Security in the Cloud and Where Do I Start?

When it comes to network security in the cloud, there are many possibilities to what architects could perceive as the key capabilities needed. For the purposes of this guide, we're really referring to the security of applications and infrustructure within public cloud environments like AWS, Azure, and GCP (aka. cloud network security). We are not referring to the cloud access security required to authenticate and authorize users for access to applications.

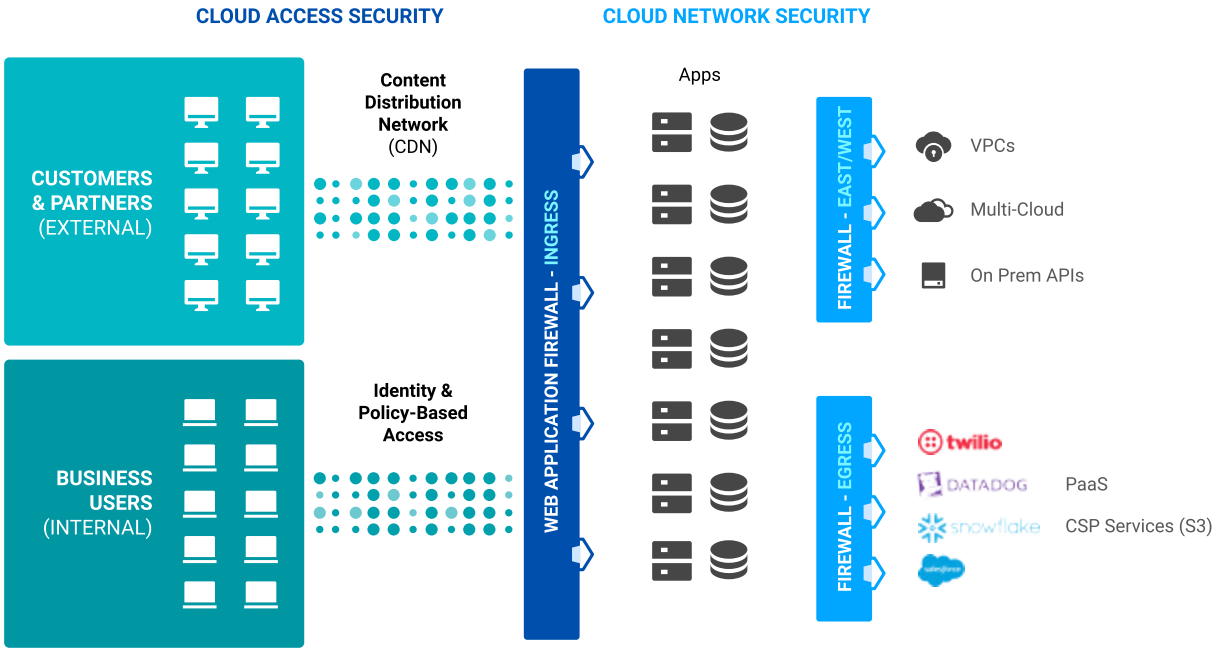

Figure 2: Cloud network security is essential to an overall cloud security architecture

For cloud network security, we break down the requirements into different network segment functionalities:

Ingress. This network segment includes any external access to your cloud deployment. Some examples include general public access to a website or application, partner access to an API Gateway, or an on-premises connection to a cloud storage service. The direction is inbound and client-initiated.

Egress. This network segment covers what your cloud deployment needs to access to perform an operation or function. Some examples may include accessing payment gateways, developer APIs, SaaS services, software repositories, or external URLs hosted on the internet. The direction is outbound and initiated on the application side.

East-West. This network segment describes the lateral movement within the cloud environment itself. This includes communications such as inter-VPC/VNet, inter-region, endpoint services, private links, or PaaS constructs. These can be either client or server-initiated.

Why is this important? Best practice application architecture in the public cloud requires network segmentation around each application. This can create a sprawl of virtual networks (VPCs/VNet) that has to be secured. Each of these network segments has its own attack vector with a fundamentally unique threat profile. Therefore, each segment requires different types of network security functions. To manage the network security posture for each, let's examine which network security functions are relevant by network segment, hardware, underlying network access, and data centers themselves.

When it comes to applications, you are solely responsible for securing anything that involves data, information, identity, access, and the configuration of services implemented. You also must take care to protect anything that connects with the public cloud—including on-premises data centers, user VPNs, as well as internal and external parties accessing your applications.

NETWORK SECURITY FUNCTION	INGRESS	EGRESS	EAST-WEST
Web Application Firewall (WAF)	✔	-	**
Intrusion Detection/ Prevention (IDS/IPS)	✔	✔	✔
AntiVirus Detection/ Blocking	✔	✔	**
URL/FQDN Filtering (includes Explicit and Category based profiles)	-	✔	✔
Data Loss Prevention (DLP)	-	✔	✔
Layer7 DoS	✔	-	✔
Malicious IP Blocking	✔	✔	-
GeoIP Blocking	✔	-	**
Threat Packet Captures	✔	✔	✔

** Optional, dependent on architecture.

Determine your specific network security requirements based on your application architecture. You may need only one or all three network security functions.

Be sure to look into the network security function implementation itself. Are the security rulesets for WAF and IDS/IPS manually or automatically updated? Who provides the threat intelligence source?

Ensure the chosen cloud network security solution and vendor can provide the requisite compliance coverage for your specific application and the data it processes. Ask for a SOC 2® report—which is standardized by the American Institute of Certified Public Accountants (AICPA).[4]

[4] "SOC 2® - SOC for Service Organizations: Trust Services Criteria," AICPA, accessed June 9, 2021.

Compliance Considerations

In addition to network security, cloud architects must also take compliance into consideration. For these purposes, compliance means adherence to established standards, industry regulations, or laws (regional/national/state) that specifically determine how certain types of data must be handled. This may include encryption, where data can be stored (and for how long), and most importantly who is permitted to access it.

Some common examples include the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and the European Union's General Data Protection Regulation (GDPR). These become relevant to the network security architecture because compliance dictates controls that must be assessed and audited against five trust services:

- Security
- Availability
- Confidentiality
- Processing integrity
- Privacy

While achieving compliance does not inherently ensure security, it can provide a solid foundation for the security best practices that pertain to your organization. How is this different to on-prem compliance? Choosing to utilize a CSP shifts the dynamic to include an additional responsibility to ensure your CSP is in fact compliant with all of the different and applicable regulatory mandates for your data.

Best Practices of Multi-cloud Network Security Architecture

Cloud architects are well aware of the many differences between CSPs in almost all respects but particularly with regard to networking—from simple load balancer behavior, to underlying architecture constraints, and everything in between. Increasingly however, it is often desirable to take advantage of services offered by a specific CSP in your architecture. Maybe you inherit a different CSP deployment through a company acquisition. Or perhaps a financial decision requires engagement with more than one CSP at a time. Regardless of the specific situation, multi-cloud considerations cannot be overlooked when it comes to choosing an effective and appropriate network security solution.

Look for a true decoupled control and dataplane. A centralized control plane across CSPs provides consistent corporate security policy from a single management console. It also allows for visibility of security events across complex environments with correlation to specific applications and policies, while your data and dataplane remains yours.

Your security solution should not become a point product designed for a single CSP. Change happens—and re-architecture is both costly and disruptive.

Choose a cloud network security vendor that can help you fully leverage individual public clouds and also scale horizontally to other clouds.

Embracing a Cloud Network Security Platform (CNSP)

A cloud network security platform (CNSP) is different from both on-premises and self-managed security. The principal difference is that CNSP providers offer security capabilities as a cloud service. CNSPs are rapidly evolving—some CSPs are even introducing entry-level options. When evaluating different CNSP options, you should consider the provider's ability to deliver on three essential capabilities:

Visibility into cloud assets to drive security policy and threat identification.

Asset identification should include context and understanding of the business purpose of the resource in order to apply risk-based policy and the appropriate security controls. By capturing visibility through the network across many disparate teams, applications, and cloud providers, a CNSP provides better security that is continuous by design. Visibility into network telemetry from the cloud provider can be unlocked and then enriched with threat intelligence and/or exported to security and information event management (SIEM). Operations teams benefit as well with an updated source of truth about the key applications and assets across multiple cloud accounts and virtual networks.

Multi-cloud security through a single console.

A CNSP can provide an abstraction layer that simplifies multi-cloud security with a unified management console. Security teams gain the ability to apply one policy that can span multiple clouds. Operations teams benefit from reducing the need to maintain cloud provider-specific infrastructure and a reduction in overall cloud provider lock-in.

Cloud-native scale to enable business agility.

Security only works if it can adapt to the scale of the resources it's meant to protect. A CNSP should be seamless to the cloud apps it protects. New apps and infrastructure should be continuously discovered and security policy automatically deployed based on the technology asset's business context. Elasticity should occur as business demand requires it. At the end of the day, security in the cloud should just work—enabling security teams to focus on strategic objectives and not operating the tools.

Checklist: What Can I Do to Immediately Improve My Security Posture?

1. **Embrace the native cloud provider's security guardrails.** These excellent supports may include security groups, NACLs, proper route configuration, and correctly configured networking constructs (e.g. network load balancers, network gateways).

2. **Understand the data flow.** In order to assess the protection requirements, you need to know how data goes both to and from your cloud applications and their dependencies. What are the threat vectors for ingress, egress, and east-west lateral movement of data?

3. **Get contextual visibility to apply valid controls.** You can't protect anything that you can't see - particularly when grappling with cloud sprawl complications. Cloud asset identification should include context and understanding of the business purpose of the resource in order to apply risk-based policies and the appropriate security controls.

4. **A single management process.** According to Gartner, "Through 2025, 99% of cloud security failures will be the customer's fault." Centralized administration helps decrease the likelihood of misconfigurations, along with the inability to quantify risk.

5. **Implement alerting with context.** Alerting that lacks specific contextual details requires human analysis and intervention. These kinds of obligatory manual processes delay time-to-knowledge and eventual resolution.

6. **Implement effective logging.** Logging supports the search and query experience when performing audits and security incident response activities. It must include details about specific activity usage. You need to know not just source IP, but destination, protocol, content and application function, and more.

7. **Architect towards a "zero trust network."** Zero trust refers to an evolving set of cybersecurity solutions that shift defenses from static, network-based perimeters to instead protect resources, assets, and applications wherever they reside. Zero trust assumes there is no implicit trust based solely on physical/network location or application ownership. It supports security practices that are both granular and dynamic, with controls that are aware of application context.

8. **Agility and ability.** Deploy purpose-built cloud network security designed to meet your specific requirements (including compliance) with flexibility for growth and/or multiple CSPs. It should provide elasticity in lock-step with business demand. Your solution should deliver security that simply works as advertised, is easy to deploy, and that integrates seamlessly with the cloud application it protects.

About Valtix

Valtix is on a mission to enable organizations with security at the speed of the cloud. The first multi-cloud network security platform delivered as a service, Valtix was built to combine robust security with cloud-first simplicity and on-demand scale. Powered by a cloud-native architecture that is 10x faster, Valtix provides an innovative approach to cloud network security called Dynamic Multi-Cloud Policy (™), which links continuous visibility with advanced security controls. The result: security that is more effective, adaptable to change, and aligned to cloud agility requirements. With Valtix, organizations don't have to compromise in the cloud. They can meet critical security and compliance requirements without inhibiting the speed of the business.

Get started with a free trial and a cloud visibility report at **Valtix.com**

THE CLOUD ARCHITECT'S GUIDE TO NETWORK SECURITY

HQ - Santa Clara, USA
800# Mission College Blvd 2350
95054 Santa Clara, CA
650.420.6014
info@valtix.com