HOW SHOULD I SECURE MY CLOUD?

Native CSP vs. Third-Party Controls

CHALLENGE WITH SERIOUS CONSEQUENCES

93% of cloud deployments were misconfigured, leading to >200 breaches in the past 2 years

Increased Complexity for Security Teams, Increased Risk for Breaches

The rapid movement from on-premise to the public cloud has created an entirely different paradigm for implementing network segmentation and controlling access. With on-premise infrastructure, the network security team accepts firewall rule change requests, then implements and validates them – and the network security team has full visibility.

With cloud infrastructure, network security teams are no longer the gatekeeper of rules and security policies. Infrastructure is implemented as code with a new set of nomenclature based on containerized software (VPCs, security groups, pods, namespaces, etc.), and security policies are often implemented by developers.

This new environment is also highly distributed, with additional capabilities provided by Cloud Service Providers themselves. An example of this would be an Amazon Web Services policy may be found at security groups for instances and Network Access Controls List for subnets. An Amazon Elastic Kubernetes Service policy may be written for pods or for a namespace.

Traditional firewall vendors (Palo Alto Networks, Cisco, Juniper, Fortinet, etc.) have also made their products available as software that can be deployed into the cloud.

Complexity adds to risk and people are being breached. According to "The State of DevSecOps report by Accurics," there were misconfigurations in 93 percent of cloud deployments, which contributed to more than 200 breaches over the past two years.

Determining what mix of tools (native cloud and third-party) and how to have the security team maintain some semblance of control is a significant challenge. Next, we'll take a look at some of the key players in both segments and then provide some guidelines on how an organization can design their cloud security infrastructure around them.

REDSEAL

Native Cloud Service Provider (CSP) Infrastructure Security

Cloud Service Providers such as AWS, Azure, and Google Cloud Platform provide basic network infrastructure services and have introduced cloud-based firewalls.

Amazon Web Services (AWS)

AWS basic networking controls include Network Access Controls (NACL) applied to subnets and Security Groups (SG) applied to instances. AWS also offers a stateful firewall that enables enforcement of policies preventing VPCs from accessing domains with unauthorized protocols and includes an intrusion prevention system (IPS) that provides active traffic flow inspection and web filtering.

Azure

Azure Virtual Network (VNet) enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the Internet, and on-premises networks. Network security groups and application security groups can define multiple inbound and outbound security rules that enable filtering of traffic to and from resources by source and destination IP address, port, and protocol.

Azure Firewall is a stateful firewall that includes threat intelligence-based filtering and VPS and Express Route gateways. Optional premium services include TLS inspection, IDPS engine, and URL filtering.

Google Cloud Platform (GCP)

Google VPC firewall rules allow or deny connections to or from virtual machine (VM) instances based on a user specified configurations. Enabled VPC firewall rules are always enforced, protecting instances similar to AWS security groups.

Every VPC network functions as a distributed firewall. While firewall rules are defined at the network level, connections are allowed or denied on a per-instance basis.

Third-Party Cloud Infrastructure Security

Major security infrastructure vendors now offer virtual firewalls that can be deployed into the Cloud Service Provider environment and provide scalable, next generation firewall application control, antivirus and VPN services:

Palo Alto VM-Series

The Palo Alto VM-Series stateful next generation firewall allows native integration with subscription services, such as Threat Prevention, DNS Security, and WildFire to apply application-specific policies that block exploits, and prevent malware. VM-Series virtual firewalls deployed in multiple public and private cloud environments can all be managed from the same console, which enables security teams to deliver a uniform policy model to each environment.

Cisco Firepower Threat Defense (formerly Cisco NGFWv)

Cisco Firepower includes next generation IPS, advanced malware protection, URL filtering, and application visibility and control. The advanced threat defense options including NGIPS, security intelligence, advanced malware protection, URL filtering, application visibility and control, and VPN. Cisco also offers a centralized management console with the SecureX offering.

FortiGate Next-Generation Firewall

FortiGate Next-Generation Firewall is a stateful firewall that includes application control, antivirus, IPS, Web filtering and VPN along with advanced features such as an extreme threat database, vulnerability management and flow-based inspection.

Juniper SRX Next Generation Firewall

The vSRX Next Generation Virtual Firewall solution includes a stateful firewall and advanced security services that include intrusion detection and prevention (IPS), and application visibility and control through AppSecure.

Design Considerations

Third-Party or Native Cloud Capabilities

Security teams now have to decide between new offerings from CSPs or cloud offerings from established network security providers. Here are six criteria to consider when evaluating these options:

1. Is the network a hybrid of on-premise and cloud?

If there is a hybrid environment, staff already familiar with traditional on-premise firewalls may be more comfortable moving to the virtualized firewalls provided by vendors whose products and policies are already in use. Additionally, those vendors provide centralized consoles that manage both on-premise and cloud-based firewalls, which allows more flexibility in migrating applications to the CSP.

Alternatively, the workload could be split between the on-premise firewall team and another team that utilizes the security services provided by the CSPs, but this approach may increase costs (personnel/ training) and the increase the complexity of maintaining a consistent security posture.

2. Are multiple cloud services in use?

Multi-cloud deployments are popular for cost reasons and to avoid vendor lock-in. But using native security controls across multiple CSPs may actually increase costs (labor intensive translation of policies from one CSP to another) and introduce configuration errors.

If only a single CSP environment is in place, developing expertise in CSP native cloud security infrastructure services may be a good investment.

3. Does staff have DevOps knowledge and process?

Implementing security into a DevSecOps process is difficult because the team needs to develop expertise in each CSP and their respective Kubernetes implementations. Security teams need to work closely with development teams to construct policies that developers can implement. If staff is still coming up to speed in a "cloud-first" world, then third-party firewalls to manage traffic and segmentation may be more straightforward.

If a strong DevSecOps process is in place with deep cloud expertise on the security team, the use of native CSP controls may be a better choice.

4. Is L7 policy is a requirement?

Cloud native security controls such as VPC and VNets provide for segmentation but for Layer 7 filtering only provide IDPS offerings. Currently both AWS and Azure firewalls do not provide Layer 7 application-level filtering. If you need to write Layer 7 policy, a virtual third party NGFW is currently the best option.

5. Are there requirements for best in class IPS, Threat Prevention, URL filtering?

CSPs do provide NIPS and threat prevention found in third-party firewalls. However, firewall vendors who have been in business for decades are likely to have more features and capabilities than the nascent offers of the CSPs. For customers who want to have these capabilities at the network layer, third-party firewalls are an excellent choice.

Alternatively, if plans include other tools such as Endpoint Detection & Response (EDR) and Web Application Firewall (WAF) for threat prevention and URL filtering, native CSP controls may suffice.

6. Cost vs. Features

CSPs provide strong segmentation ability through VPCs and VNets with no additional charge per use of VPC or VNet. They do provide advanced "pay for options" for features such as AWS Network Firewall and Azure Firewall. For example, currently AWS Network Firewall charges $0.395 per endpoint hour and $0.065 per GB processed.

The use of third-party firewalls requires the license of the third-party firewall vendor in addition to the compute cost to run the service. For example, running a Palo Alto VM series FW in AWS will include the cost of firewall license plus the use of a EC2 m5.2xlarge instance at $0.384 per hour. Organizations should consider the cost benefit of the additional capability of a third-party firewall.

Summary

CSPs are rapidly innovating to create native network security features. Established networking security players have created virtual versions of their best-in-class next generation firewalls. For smaller, agile, cloud-first companies who are cost sensitive, the CSP's native controls may meet your requirements. Larger organizations who are probably hybrid, multi-cloud, and need advanced features will likely choose a third-party solution.

Regardless of how your infrastructure is designed, having a tool like RedSeal helps you see and secure your entire network fabric.

RedSeal Shows Your Inventory and Access Across Your Clouds

RedSeal's cloud security solution brings all your network environments—public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on-premises—into one comprehensive, dynamic visualization. If your cloud security design considerations involve the use of third-party vendors, only RedSeal allows you to interpret access controls across both cloud-native and third-party virtual firewalls.

To learn how RedSeal can help you answer these questions, please visit www.redseal.net/cloud-security or email us at info@redseal.net.

Unlike RedSeal, most security tools only work in one network environment, leaving security teams with common concerns such as:

- What resources do we have across all our public cloud and on-premises environments? What access is possible?
- Are any of these resources unintentionally exposed to the internet?
- Do our cloud deployments meet security best practices?
- How do we validate our cloud network segmentation policies?
- Are we remediating the riskiest vulnerabilities in the cloud first?

ABOUT REDSEAL (redseal.net)

RedSeal – through its cloud security solution and professional services -- helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises – into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.