AKAMAI WHITE PAPER

Five Tough Problems Moving a Traditional Network Security Perimeter to the Cloud

Akamai
FASTER FORWARD

Introduction

To gain a competitive advantage, to innovate faster, or just to get stuff done quicker, organizations are accelerating their use of cloud computing services like Amazon's Web Services (AWS). Moving an application into the cloud means getting instant access to an almost infinite amount of compute resources, but it also means putting your application on a network you do not control, without the level of security enterprises have traditionally had in their data centers. The challenge is: How do you take advantage of the agility the cloud affords you while securing your applications in the cloud from Internet threats and still give users easy, fast access to those applications?

The first step most enterprises take is to look at traditional solutions deployed in the data center and move them to the cloud. At first glance, it's easy to imagine building the same network security perimeter in the cloud as in the traditional data center. This, however, overlooks two fundamental differences between the cloud and the data center:

1. The network in the cloud is abstracted away from the users. Some network functionality is exposed, but there is no direct access to router and switch configuration.
2. Numerous compute clouds and Virtual Private Clouds (VPCs) can be created and destroyed in minutes by users — this is a main component of their value. Data centers, by contrast, are built over months and years.

These two key differences make using traditional methods difficult to engineer, very costly, and in some cases can limit the effectiveness of the network security. The first leads to challenges building the traditional perimeter in each cloud; the second indicates issues managing these perimeters across multiple dynamic cloud environments. The result is five really tough problems companies have to overcome to provide security in the cloud:

1. **Cost -** Building a Big Stack of Security Appliances
2. **Complexity -** Building an Overlay Network in the Cloud
3. **Control -** Connecting Authentication and Access controls
4. **Policy Management -** Multiple Clouds, Many Security Appliances
5. **Trusted Path -** Getting Users to the Right Cloud

Overcoming these challenges means high cost, complexity, and long, risky, implementations.

Hard Problem #1: Cost – Building a Big Stack of Security Appliances

Virtual Private Network (VPN) gateways have never been a secure application access methodology. With a VPN, one set of compromised credentials can give an attacker free run of everything on that network. Thus, companies have traditionally built network perimeters, or Demilitarized Zones (DMZ), providing several network security layers using a portfolio of networking appliances, including:

- Firewalls
- DDoS protection appliances
- Application Delivery Controllers (ADCs)
- Intrusion Detection/Prevention systems (ADS/IPS)
- Web Application Firewalls (WAFs)
- Authentication, Authorization, and Auditing (AAA) servers
- WAN Optimization
- Application visibility appliances
- ...and others

Today, almost any networking or network security product is available in a virtual appliance form-factor, allowing them to be instantiated in the cloud and stacked together. It may not be necessary to replicate all of these legacy functions to secure a cloud perimeter, but their acquisition cost alone can lead to annual licensing costs in excess of $100,000.

Just like in a physical data center network, each virtual appliance in the secure perimeter stack is a point of management. Each appliance must be administered, policies and configurations managed, and appliance interactions debugged – all of which add significant operational costs to the perimeter. Thus, the three-year cost to build, run, and manage a perimeter with virtual appliances can easily run into hundreds of thousands of dollars per cloud.

Hard Problem #2: Complexity – Building the Overlay Network in the Cloud

In the physical network, you could simply cable the output of one appliance to the input of the next or use capabilities like policy-based routing, web-cache communications protocol, and other features built into the routers and switches in your network. However, in the cloud, the network of an Infrastructure-as-a-Service (IaaS) or Cloud computing provider is an abstraction. Those services automatically handle normal routing and switching to ensure that traffic arrives at its final destination.

That is great until you want to start controlling how the traffic flows through their network. IaaS providers do not let you reconfigure their network. That means you need to create an overlay network to engineer your traffic so it flows through multiple security appliances. To create the overlay, you must instantiate, manage, and configure software routers and switches. Or you could look to the new crop of Software Defined Network (SDN) companies for a more integrated solution.

Implementing SDN in the cloud may seem cool and sexy to the network engineering team, but most will have to climb the SDN learning curve. To the company, this means additional time and engineering expense, on top of the additional cost of evaluating and licensing one of the variety of SDN solutions now on the market.

Hard Problem #3: Control – Connecting Authentication and Access Controls

It's simple to spin up a new cloud. It takes minutes to create a new VPC in AWS, and why wouldn't you want to have many clouds? Segmenting the traditional network with VLANs has long been a common practice. Creating multiple clouds — one for each project and one for each department — just makes sense. But every cloud is an independent network, and that means access to each one needs to be built separately.

Authenticating users to resources in the cloud can be accomplished in many ways. For security reasons, however, most companies want a single unified "source of truth" for managing their users and associated access controls. Typically, enterprises use Active Directory (AD) as their single source of truth, with the AD server running on premise in the data center.

Clearly, when the perimeter is in the cloud and the directory in the data center, there is some engineering just to provide secure connectivity between the two. Organizations using local AD as the main authentication source often establish IPsec tunnels from the cloud to the data center. This requires complex rerouting mechanisms and, potentially, overlay networks if the AD is also reachable through a VPC in a different zone.

Another challenge arises if you are using AD for your employees but a separate directory for your customers, partners, and other third parties. Specifically, once you have your AD problem solved, you may need to integrate a SAML identity provider into your cloud infrastructure. Different trust zones, network segmentations, and multiple directories — all this adds up to complexity that slows agility to a crawl and tends to result in security vulnerabilities over time.

Hard Problem #4: Policy Management – Multiple Clouds, Many Security Appliances

The challenge of managing policy grows rapidly as you add multiple clouds. If each cloud has its own perimeter with many networking and security products, maintaining consistency of policy is a real problem. Getting policies out of sync, inconsistently, or slowly applying patches and updates to all these devices leads to increased security vulnerabilities.

Hard Problem #5: Trusted Path – Getting Users to the Right Cloud

Users are mobile. Most access to your applications is from your users on the Internet, and they do not care where their applications are. They expect an easy way to reach them on whatever device they may have. How do you create a trusted path between your users and the applications they need, when users can be anywhere and these applications can reside in multiple clouds?

The traditional solution for connecting users on the Internet to your internal network has been the VPN. Each cloud requires its own VPN. From a user's perspective, a VPN is a pain — clients must be installed on every device, which come with misconfigurations, platform OS support, payload/MTU adjustments, and reduced battery life (in the case of mobile endpoints), etc. If a user has to install multiple VPNs and figure out which one to use to get to which application, they will likely revolt. Thus IT is now forced to build a trusted routing infrastructure to get users to the right cloud, a project with even greater complexity than building the perimeter in the cloud.

Solve all 5 Problems with Enterprise Application Access (EAA)

EAA enables a superior path of getting back the security and control of your data center in the public cloud. It delivers instant application security for enterprise cloud computing environments. EAA puts a highly secure perimeter around each of your cloud applications, protecting them from breaches, loss, and hijacking while providing users easy authenticated access to the apps they need.

No More Security or Network Appliances: EAA integrates the functionality of the traditional network security perimeter into an easy-to-use service that can be deployed in minutes.

No More Complex Overlay Networks: EAA's unique architecture allows you to lock down all inbound access to your clouds, effectively isolating your clouds from the Internet and moving the attack surface to the EAA Edge. No changes and no overlays are needed to the network inside the cloud.

User Authentication to Your Directory or Any Directory: EAA authenticates users to your directory, wherever it is — an AD in your data center, a SAML IDP, or even a Google Directory. EAA provides access controls (group, device type, location, OS, and more) and adds two-factor and multi-factor authentication, giving you full control over who gets in with protection against compromised credentials.

Single Pane of Glass Management: EAA works in any cloud, AWS, VMware, Google, and OpenStack, as well as your data center. Using EAA, you get a single pane of glass to manage a consistent policy for security and access control to all your applications across all your clouds.

Unified Trusted Path: EAA automatically connects your users on the Internet to the applications they are trying to reach — no matter what cloud those apps are in. EAA provides an end-to-end secured path between any users' device and the applications.

Akamai FASTER FORWARD