APPLICATIONS IN THE CLOUD: A THREE-LAYERED, STRUCTURAL APPROACH TO NETWORK SECURITY

An AlgoSec Whitepaper

Introduction

Digital transformation is redefining the business world, and IT needs to keep up and respond faster than ever before. One way to do so is by moving business applications to the cloud where businesses can benefit from increased agility while minimizing costs.

While there are many processes involved in migrating applications to the cloud, network security is often neglected. When this happens, applications are deployed in the cloud with inadequate security and compliance measures in place, or, conversely, the security team steps in and halts the migration process. With either option, the company is at risk: inadequate security makes it easier for hackers to access the network and mount an attack against the company – exposing the company to financial losses and legal repercussions. Moreover, if the business is unable to respond to market demands in a timely fashion, its very existence could come into question.

This white paper presents a structural approach for bridging the network security gap before and during the process of migrating applications and managing network security policies in the cloud.

In your cloud migration project, you should evaluate and plan your network security requirements and architecture through a three-layered structural approach that contains the following components:

1) **Foundation** – application discovery to know your application set
2) **Substructure** – evaluation of existing applications' network connectivity requirements and associated firewall rules
3) **Superstructure** – ensuring a process for network security management across the hybrid environment

With these three components, the security team will have the essential groundwork in place to be ready to migrate applications to the cloud.

The Foundation: Know What Applications You Have

Obtaining an inventory of applications is the foundation of both your security and the migration to the cloud. However, the process of discovering all the applications used by the business is not a trivial task. Most businesses typically have two types of applications – enterprise and departmental.

Enterprise applications, the more complex applications in your datacenter, usually serve many business units and can span multiple geographies and even company subsidiaries. In most cases, the IT team is well-aware of them. While the documentation of these applications with their connectivity requirements may not be perfect, that's a good starting point for the migration process. Note that there may still be a need to update the documentation.

Many departments or business units purchase their own *department applications* such as Business Intelligence solutions or marketing tools. Some of these applications may be SaaS-based while others are installed on corporate servers. For these types of applications, it is likely that documentation never existed. Fortunately, in most cases, their architecture isn't complex. It should be relatively easy to obtain the necessary connectivity information needed to migrate them to the cloud. However, the key here is to know that these applications exist.

There are two ways to generate a list of applications. The first requires using consultants to conduct thorough interviews with the various stakeholders in each department and in each geography. A second, more cost-effective and efficient way, is by using automation solutions.

Once the list of applications – the foundation – is in place, you can move onto the next stage in the process of closing the security gap as you migrate to the cloud: understanding each application's attributes, such as number of servers, associated business processes and network connectivity requirements. These attributes help determine the complexity involved in migrating applications.

The Substructure: Understand Existing Application Network Connectivity Requirements and Relevant Firewall Rules

There are several attributes that can affect the complexity of migrating an application to the cloud, including the application's network connectivity requirements and the firewall rules that allow/deny that connectivity.

Mapping network connectivity provides a deeper understanding of network traffic complexity which, in turn, provides insight into the flows you will need to migrate and maintain with the application in the cloud (see Figure 1). Additionally, this information will tell you how many applications are dependent on a specific server. The more applications that utilize a server, the harder it is to migrate an application that depends on that server. It may be necessary to migrate the server itself or to migrate multiple applications at the same time.

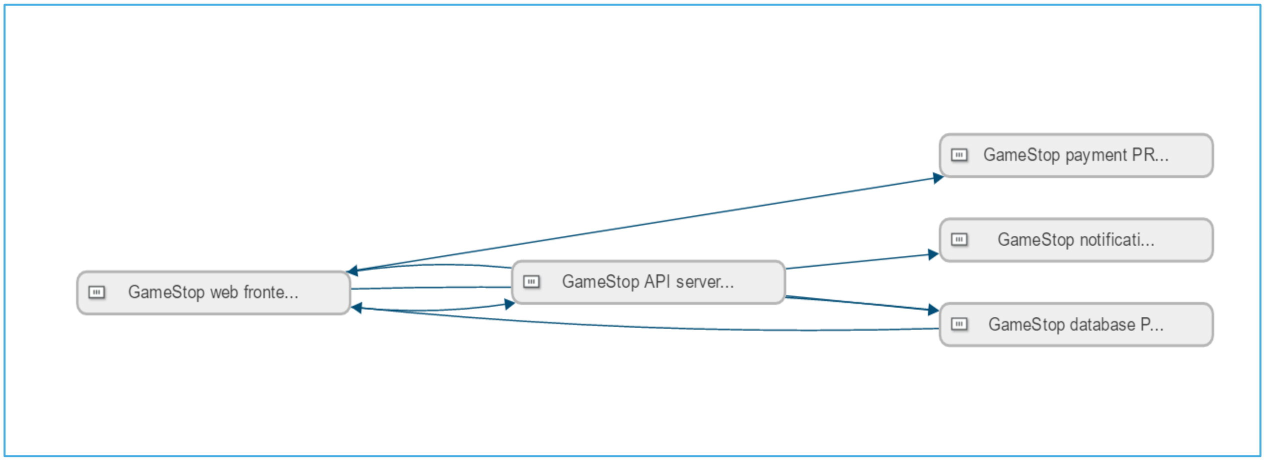

Figure 1. Mapping network traffic flows

Mapping the firewall rules provides insight into the security measures you will need to put in place once the application has been migrated to the cloud. As a rule of thumb, the more firewall rules required, the greater the complexity. This mapping allows you to identify and decommission firewall rules that are no longer necessary post migration. Decommissioning firewall rules reduces the attack surface of your network.

So how do you generate documentation of application connectivity? The obvious choice is to employ a solution that automatically maps the various network traffic flows, servers and firewall rules for each application. If you do not have access to such an automation solution, manually documenting all of these manually, however tedious, will provide the necessary information.

The Superstructure: Ensuring a Process for Network Security Management in the Cloud and Hybrid Environments

Whether you move all your applications to the cloud or just a few of them, and whether you use one or multiple cloud vendors, you now need to manage and maintain the security and compliance in the cloud just as you did in your on-premise network over which you have complete control. Establishing a route from a server in the cloud to a server on the on-premise network requires an intimate understanding of both the cloud security controls and the on-premise security devices. Where there are separate cloud and on-premise network security teams, as is the norm in many businesses, collaboration between the teams is needed which, of course, adds its own complexity.

Another point to consider is that once applications are deployed in the cloud, you will likely want to be able to move between cloud providers ‘at the speed of the cloud’ to avoid vendor lock-in and to minimize costs. While you might be led to believe that this is a simple requirement, in reality, each cloud provider has its own, unique network security controls with which you need to familiarize yourself.

There are several ways to manage security across the hybrid cloud environment.

1. You can manage the environment manually, which is slow, time-consuming and error-prone.

2. You can use the cloud provider’s native controls to manage the cloud network security in addition to the existing tools and methodology you currently use for your on-premise environment. However, bear in mind that cloud security controls do not provide a holistic view of security across your entire estate and their limited capabilities may not sufficiently support your business’s security posture.

3. Alternatively, there are 3rd party automated network security policy management solutions that span the entire hybrid environment which can assist in managing the entire network security estate.

Summary

Business are moving applications to the cloud every day, yet security gaps are putting them at risk in terms of compliance and agility. By applying a three-layered structural approach—identifying applications that are good candidates for migration to the cloud, mapping their connectivity and managing the environment—you can bridge the gaps to ensure a successful cloud implementation.

Additional resources:

- Application Connectivity: There's a Map for That
- Migrating Business Applications to AWS? Tips on Where to Start

About AlgoSec

AlgoSec enables the world's largest and most complex organizations to manage network security based on what matters most – the applications that power their business. Over 1,500 of the world's leading organizations, including 20 of the Fortune 50, rely on AlgoSec to automate and orchestrate network security policy management across cloud and on-premise networks, to drive business agility, security and compliance. AlgoSec has provided the industry's only money-back guarantee since 2005.

algosec

Global Headquarters
65 Challenger Road,
Suite 310
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
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

AlgoSec.com