APPLICATION MIGRATION TO THE CLOUD: A 3 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 and legal losses. And if the business is unable to respond to market demands in a timely fashion, its very existence comes into question.

This white paper presents a structural approach for bridging the network security gap before and during the process of migrating applications to 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 application network connectivity and associated firewall rules
3) **Superstructure** – ensure a process for network security management across the hybrid environment

With these three components, the security team will have the essential groundwork in place and be ready for the migration process.

The Foundation: Know What Applications You Have

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

Enterprise applications, which are the more complex applications in your datacenter, usually serve many business units and can span multiple geographies and even different company subsidiaries. In most cases the IT team is aware of them, and while the documentation of these applications and their connectivity may not be perfect it is a good starting point for the migration process, although there may still be a need to update it.

In addition, many departments or business units purchase their own applications, such as BI solutions or marketing tools. Some of these applications may be SaaS-based, and others will likely be installed on corporate servers. For these types of applications, the documentation likely never existed. In most cases
their architecture isn’t complex and 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 different key stakeholders in each department and in each geography. A second more cost effective way is by using automation solutions.

Once the list of applications - the foundation - is in place we can move onto the next stage in the process of closing the security gap in the cloud migration project: understanding each application’s attributes, such as number of servers, associated business processes and network connectivity. These attributes help determine the complexity involved in migrating the application.

The Substructure – Understand Existing Application Network Connectivity and Relevant Firewall Rules

There are several attributes that can affect how complex is it to migrate an application to the cloud, including the application’s network connectivity and the firewall rules that allow/deny the application network connectivity.

Mapping network connectivity provides a deeper understanding of network traffic complexity, which in turn provides meaningful insight into the flows you will need to migrate and maintain in the cloud (see fig 1). Additionally, this information will tell you how many applications depended on a specific server. The more applications that utilize a server, the harder it is to migrate a specific application that depends on that server or it may be necessary to migrate the server itself or at least 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, and the more firewall rules needed the greater the complexity. Furthermore, this mapping allows you to identify and then decommission firewall rules which will no longer be necessary post migration, which in turn will help you reduce the attack surface of your network.

So how do you generate documentation of application connectivity? The obvious choice is to utilize automation solutions that can automatically map the different network traffic flows, servers and firewall rules to each application. For those who do not have such a solution documenting this information manually will provide the necessary information.

**The Superstructure – Ensure You Have a Process for Managing Network Security Across the Hybrid Environment**

Whether you move all your applications to the cloud or just a few of them, and whether you use one cloud vendor or multiple vendors, you now need to manage and maintain security and compliance across an on-premise network over which you have complete control, as well as a network the resides outside of your corporate domain. 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 most organizations, collaboration between the teams is needed which, of course, adds 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 reduce costs. While you might believe this is a simple task, in reality each cloud provider has different network security tools that you need to familiarize yourself with.

There are several ways to manage security across the hybrid cloud environment. You can manage the environment manually, which is slow, time-consuming and error prone. You can use the cloud provider’s native controls to manage the cloud network security together with 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 hybrid estate, and their limited capabilities may not sufficiently support your organization’s security posture. Alternatively, there are 3rd party automated network security policy management solutions that support span the entire hybrid environment which can assist in managing the entire network security estate.
Summary

Moving applications to the cloud is happening and security is lagging – jeopardizing both the company’s security and its agility. By identifying, mapping connectivity and managing the hybrid environment, you can overcome these problems and bridge the gaps to ensure a successful migration to the cloud.

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 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.