VALTIX

WHY VISIBILITY IS ESSENTIAL TO SECURITY IN THE CLOUD

The Role of Visibility in Securing Cloud Applications

Apps Live in the Public Cloud

Apps are being built on public cloud platforms at a rapid pace as enterprises accelerate their cloud migrations. Public clouds offer developers enormous flexibility in how apps are built and deployed. This has resulted in architectures that consist of one or more of the following:

- Security
- Availability
- Confidentiality
- Processing integrity
- Privacy

Apps Are Services-Based

Coincidentally, another tectonic shift is taking place in how apps are built, namely via a services-based approach. Increasingly, apps are built as microservices communicating over well-defined APIs. Often, these APIs are remote or external. This means an app can use several methods to accomplish a task, including:

- Twilio to send text messages
- AWS S3 to store and retrieve images
- Mailchimp to send emails
- Snowflake to store and retrieve rows of data
- Datadog to log events

> ***Traditional data center approaches aren‘t built for securing modern cloud applications.***
> *We are living through an application development renaissance. Organizations are changing both where applications live and how they are built.*

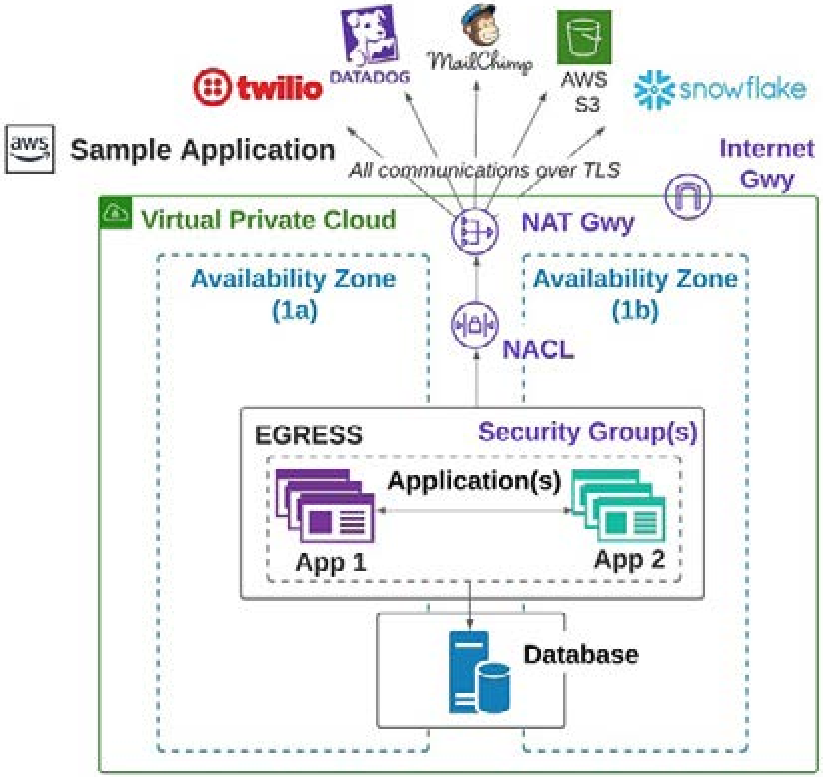

Figure 1: Sample Application Diagram

A New Category of Traffic

This collision of where apps live (public cloud) and how they are built (services-based) is creating a massive new category of traffic: app-initiated connections to software-as-a-service (SaaS), platform-as-a-service (PaaS), and the wide-open Internet. Typically, the service endpoints that apps are connecting to (e.g., https://api.datadoghq.com for Datadog) are identified by a fully qualified domain name (FQDN) or URL, which can translate to hundreds or thousands of Internet Protocol (IP) addresses during resolution. Those IP address lists are dynamic. At the same time, cloud service providers' native security controls, such as access control lists (ACLs), security groups, and route tables, are all IP-address-based.

Thus, to reliably enable these kinds of connections in public clouds, security controls must be relaxed to allow communication to any IP address. This produces a significantly larger exposed attack surface than what enterprises really want opened.

Before enterprises relaxed these controls, communications to external destinations were restricted to safe-listed IP addresses and ranges. So, if an application or a compute resource was compromised, its communication graph was limited to the safe-listed destinations. Now, if those egress security controls are relaxed to allow communications to any IP address, a compromised instance could result in:

- Being part of a command-and-control (C2) server and carrying out nefarious activities, such as malware distribution, cryptocurrency mining, disrupting operations, DDoS attacks, etc.
- Exfiltrating data out of the virtual private cloud (VPC)

Needless to say, enterprises need better management and control of egress traffic to allow these kinds of app- and machine-initiated connections. To put it simply, they must be able to enable a full spectrum of security policies that can be directly used by app and DevOps teams without making it too complicated or requiring constant back-and-forth with security teams for every app and situation.

Want to Secure? Start with Visibility

Given that you cannot secure what you cannot see, how can you gain visibility into egress traffic in public clouds? In the old data center world, there is a clear perimeter for deploying a network security solution. These architectures usually offer a well-defined solution that achieves visibility and enforcement by being in the network path of all traffic.

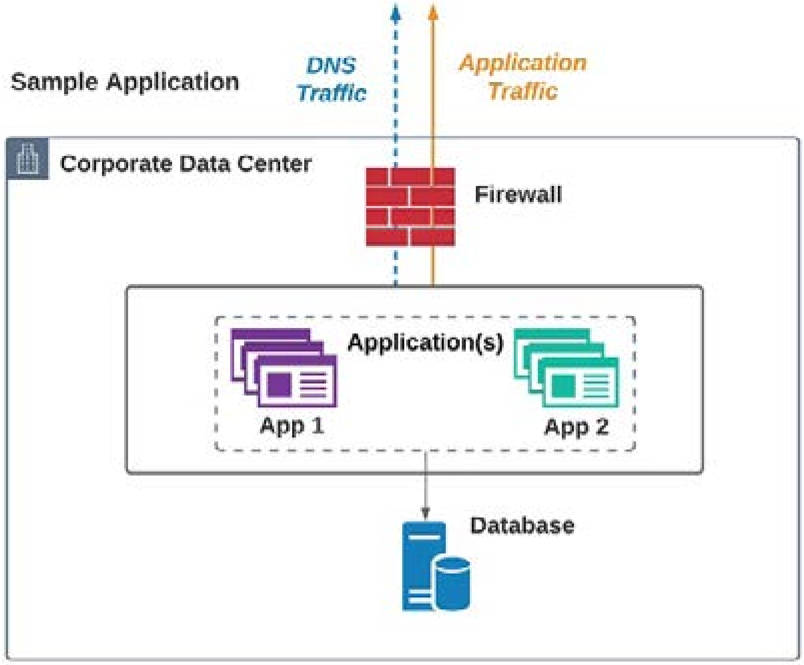

Figure 2: Sample Application Data Center Diagram

Public clouds, on the other hand, don't have a defined perimeter. Every single resource can be exposed to the Internet with a single click — an open security group rule or an ACL, an open route table entry, a public IP address attached to an interface, or some combination of these.

Being in the network path of all traffic in public cloud resources is not only non-trivial — in certain cases, it's impossible. For example, when apps initiate connections to external destinations, the first step is to resolve the destination's DNS. In public clouds, no other resource can be in the path of that traffic because the cloud provider always handles that DNS resolution. Thus, any solution that was designed to operate and excel in the traditional data center will be ineffective in a public cloud for visibility. This is why the traditional network monitoring and security vendors can't provide a coherent solution consisting of both visibility and enforcement in public clouds.

Solving Visibility and Control Problems With the Right Assumptions

The future of application development and infrastructure is in public clouds — and for many organizations, it's not just the future; it's today. Securing data, apps, and services in this new environment is critical for enterprises to defend against breaches, data exfiltration, and the resulting economic losses. Old data center approaches, based on too many assumptions that are no longer true, can't achieve these goals in public clouds. Enterprises must adopt and develop solutions that are born in the cloud and for the cloud with the correct assumptions for the public cloud era.

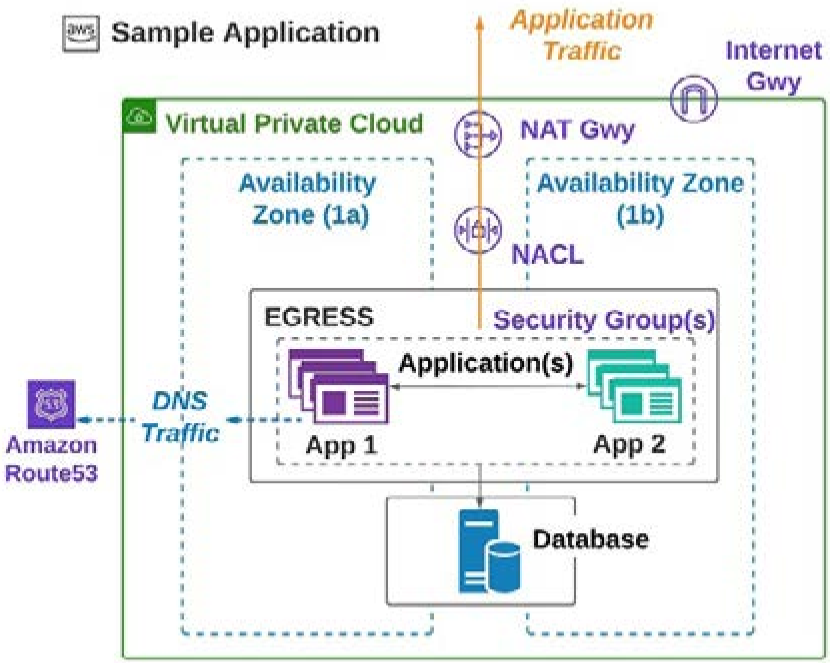

Figure 3: Sample Application Virtual Private Cloud Diagram

VALTIX

WHY VISIBILITY IS ESSENTIAL TO SECURITY IN THE CLOUD

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, Valtix provides an innovative approach to cloud network security that adapts to changes in seconds versus the days or weeks it might take a legacy virtual firewall.*

The result: *security that is more effective 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**.

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

Reprinted with permission from Dark Reading:
https://www.darkreading.com/cloud/the-role-of-visibility-in-securing-cloud-applications/a/d-id/1340468