Securing the Public Cloud with Fortinet

Introduction

Fast deployment, reduced costs, and efficient use of resources; these are just a few of the reasons enterprises and information technology departments the world over are looking to Amazon Web Services. With a feature-rich offering and plenty of compute sizes and options, more and more of them are getting drawn to this world where the words agility and flexibility have new meaning.

The Power of the Public Cloud

It all started with the emergence of virtualization technology. Enterprises today are thrilled with the ability to share compute resources across various applications and assets within their organization. This has led to an IT revolution, vastly reducing both equipment costs and power consumption of data centers. While the power of this technology is clear, it still involves physically deploying these shared compute nodes, and as the data center grows, there is still significant time and effort that go into not just adding nodes to accommodate growing needs, but also handling all the networking and security requirements that come with this.

With the ready availability of public cloud resources today, bringing up a new deployment or growing an existing one can be carried out at the click of a button. This flexibility and agility significantly reduces the time to market and greatly simplifies managing of both high availability and scaling while affording universal accessibility.
Protecting the Public Cloud

The one caveat with using public clouds is that it provides a completely new attack surface with the potential to let in millions of new threats if not protected properly. For a public or hybrid cloud to be successful, it is essential to protect it with the same zeal that one would protect the data center and other key assets on-premise.

Encrypted Transport

When an enterprise needs to bring up a resource, the IT Department usually has the luxury of deploying it in the safety of a closed-off lab. Bringing up similar networks in AWS require protection from the get-go. While this might be as simple as deploying a private subnet, which will need to go through a protected gateway, the effectiveness of the protection afforded by this gateway is key. In effect, when working on such a setup, everything is remote. A good VPN service is a must to be able to protect this “remote access” traffic flowing over the Internet.

Perimeter Protection

Much like the local data center, a public cloud deployment requires a solid layer of perimeter protection. While the AWS native firewall provides a good first layer of protection, it is not sufficient. With support for a rich set of features and the capability to protect against a multitude of threats, it is essential for the perimeter firewall to provide quality protection with exceptional security effectiveness while keeping up with the performance requirements.

Scalable Protection

It is also essential that the protection provided is extremely scalable and capable of both scaling up and scaling down with load so as to reduce costs while capably servicing the application throughput.

Application Protection

While the fully functional NGFW is capable of protecting against many diverse threats, protecting application servers is a completely different paradigm. For instance, application servers need to be protected against attacks such as cross-site scripting, SQL injection, and DDoS. Email servers need to be protected against a different set of attack vectors, like anti-spam, malware attachments, and dangerous links in emails. It is essential to protect these services just as one would in a private data center.

Effective Security

When it comes to security effectiveness, there is no compromise. Even a small drop of .01% in the security effectiveness scales up to thousands of missed threats. It is therefore essential to pick a trusted and well-validated security product.

The success of any organization’s public cloud strategy will to a large extent hinge on the effectiveness with which these assets are protected.

Fortinet Security Fabric Extended to the Public Cloud

Just as Fortinet has a diverse portfolio of products meant to cover the entire attack surface on-premise, it also has a rich product offering that covers the various threat vectors to which any AWS deployment could be exposed.

All these products receive the renowned FortiGuard updates and are able to provide third-party-validated and extremely effective security. With recommendations from NSS Labs and VB100 Comparatives, among others, Fortinet devices have unmatched third-party validation and provide industry-best protection in all areas.

This portfolio includes the following devices:

**FortiGate VM**

Much like any other network, a deployment based in the public cloud requires both perimeter protection and internal segmentation to protect the various resources hosted there. The FortiGate VM is an extremely agile, fully functional enterprise firewall. It uses the tried and tested FortiOS operating system and is capable of VPN, IPS, app control, web filtering, anti-malware, etc., much like its hardware counterparts. It is kept up to date through the renowned FortiGuard Labs updates and protects against the latest threats. It is available in various instance sizes on AWS to support any and all sizes of deployments.

**FortiWeb VM**

While public cloud deployments are used for many different purposes, a majority of them include some form of application hosting. The servers’ hosting applications frequently can be threatened with various forms of attacks, including the targeting of specific web server vulnerabilities such as cross-site scripting attacks, DDoS attacks, etc. Built to protect the most valuable of application resources, the FortiWeb uses state-of-the-art technology with intelligence gathered from FortiGuard Labs to secure key resources.
FortiMail VM
One of the common methods used to compromise networks is through preying upon unsuspecting and at times unintentionally careless end-users. This is done by sending forms of vulnerabilities, malware, and unsafe links through emails. While protecting email is a different paradigm than protecting traditional network security, successfully protecting against email attacks is a part of the solution and it needs to be used in tight coupling with network security. The FortiMail VM on AWS is able to protect any cloud-based email services, including protecting Office 365 on AWS-based networks.

FortiManager VM
To effectively secure a network, it is essential to have visibility and capability to orchestrate the network in an automated fashion. This helps keep a closer watch on the network while minimizing the likelihood of configuration missteps. The FortiManager is capable of managing large networks and can provide a single pane of glass to watch, manage, and control the entire Fortinet Fabric for both AWS-only and hybrid cloud scenarios.

FortiAnalyzer VM
FortiAnalyzer platforms integrate network logging, analytics, and reporting into a single system, delivering increased knowledge of security events throughout the network. The FortiAnalyzer VM minimizes the effort required to monitor and maintain acceptable use policies, and identifies attack patterns to help you fine-tune your policies. Available in a multitude of sizes, organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining, and malicious file quarantining.

While each of these products provides a different type of protection to have a well-protected network, it is essential to build a security fabric with these devices. Furthermore, with the ability to auto scale, the FortiGate and FortiWeb adapt to serve the requirements of the setup while keeping costs down.

Further in this document, we will cover a few deployment scenarios and use cases for protecting your public cloud deployment using Fortinet Solutions.

Protecting the Public Cloud Deployment
The rest of this document details a few potential deployment scenarios for the public cloud.
The Hybrid Cloud Deployment
As shown below, Fortinet is able to completely secure the entire hybrid cloud deployment. From providing perimeter protection in the public cloud and application security, to protection at the data center edge and east-west protection within the data center, the Fortinet Security Fabric provides a completely secure end-to-end security solution.

FortManager and FortiAnalyzer are able to provide single-pane-of-glass visibility to make management and monitoring very simple and intuitive.

- It supports an array of advanced encryption algorithms and is able to secure all communication between the VPC and the data center.
- By using FortiManager, the VPN configuration can be pushed to multiple FortiGates, completely automating the deployment of the VPN infrastructure.
- With ample choice as to the instance size in use, the FortiGate on AWS is able to scale to suit performance needs.

Between auto scaling and a diverse instance-type support, Fortinet’s VMs are also able to suit all demands both in terms of traffic and high-availability requirements.

Securing Communication to the Data Center Over VPN
The FortiGate can be deployed such that it acts as the VPN terminator on the AWS side. By doing this, the FortiGate firewall brings up a VPN tunnel to the private data center, setting up a highly secure hybrid cloud deployment.

Once deployed, the FortiGate establishes an encrypted channel of communication between the AWS VPC and the data center.
Highly Available Public Cloud Data Center

It is an AWS best practice to architect the setup housed in redundant availability zones (AZ) in each VPC. This ensures failover redundancy and maximum uptime in the event of any instance failure.

In most active/passive high-availability (HA) setups on AWS, on failure, manual intervention is needed to switch over to the backup. Fortinet provides a truly automated HA solution to address this. In case of any failure, HA failover and reversion can be automatically triggered.

Fortinet’s free Python script automates the process. The script monitors both active and passive firewalls. Should the primary firewall go down for any reason, it makes the appropriate API calls to automate the route table changes, thus ensuring maximum uptime.

Alternately, Fortinet also supports the use of the AWS Elastic Load Balancer to automatically distribute the load across multiple AZs. These methods also work with the FortiWeb Web Application Firewall.

Efficient Use of Compute Using AWS Auto Scaling

AWS Auto Scaling ensures you have the correct number of EC2 instances available to handle the load for your application.

By creating collections of EC2 instances, called auto scaling groups, the user is able to specify a minimum and maximum number of instances in each auto scaling group.

AWS Auto Scaling automatically ensures that your group never goes above/below this size. When there is a need, or in times of heavy use, additional instances will be automatically spun up to ensure that demands are met, while adhering to cost considerations and budget limits.

With zero manual intervention, Fortinet devices are able to use AWS Auto Scaling to ensure the security posture scales up and down to match the EC2 instances. As new devices are spun up, they enforce the same security policies.

Figure: Auto Scaling FortiGate Protection

Email Protection with FortiMail VM

FortiMail VM is able to provide protection for any public cloud-hosted email servers as well as for Office 365. Easily deployed in the AWS VPC, the FortiMail VM is able to act either as the complete mail server or as a gateway to the mail server while inspecting any email sent to or from the email server. It is also able to:

Apply Data Loss Prevention and Identity-Based Encryption – Detect sensitive information using defined data patterns and ensure secure delivery with no additional hardware or software to install, no user provisioning, and no recipient pre-enrollment.

Prevent Phishing and Other Advanced Threats – Apply embedded URL inspection, top-rated anti-malware, and optional sandbox integration to detect highly targeted attacks.

Identify and Block Spamming Endpoints – Carriers and service providers prevent blacklisting of legitimate subscribers by identifying and blocking endpoints sending spam.

Figure: Automated High-Availability FortiGate Protecting AWS EC2 VM Instances
No Per-User or Per-Mailbox Pricing – Complete, multi-layered antivirus, anti-spam, anti-spyware, and anti-phishing protection for an unlimited number of users. Greatly reduces TCO.

Centralized Management and Analytics
With the option to be deployed in the cloud, FortiManager and FortiAnalyzer are able to provide a single point from which to control, manage, and monitor the entire deployment. It is fully capable of handling both public cloud and hybrid cloud use cases.

The FortiManager is highly scalable and can support deployments of all sizes. It is able to orchestrate the entire network by pushing uniform policies across devices. It is also capable of orchestrating simple and complex VPN deployments, greatly simplifying network management while ensuring the necessary security.

It is also engineered to assist with policy and device auditing, and is able to prove compliance and track any deviations from required security policy.

Summary
With Fortinet as the security solution for their public cloud deployment, enterprises the world over are able to successfully transition from legacy “brick and mortar” data centers to both hybrid and fully public cloud deployments worry-free. For more information, please visit https://www.fortinet.com/aws.