IMPERVA®

SOLUTION BRIEF

Securing Amazon ECS with Imperva SecureSphere

The New Cloud: Container Dominated Environments

Today, a number of industries rely on the cloud to facilitate growth and redundancy of their business operations. Much of what has fueled the adoption of public cloud migration is the speed at which applications can be spun up or torn down as virtual machines (in an AWS context, EC2 instances) in a highly programmable fashion.

One of the drawbacks of the virtual machine model is that there are significant time lags in deploying multiple applications through individual instances. In traditional virtualization, each instance contains a different operating system, and a single application can take minutes to deploy as a result. To solve this problem, many AWS users are adopting container technology to deploy applications via Amazon's EC2 Container Service (ECS). Each application is wrapped in its own Docker container, which all operate separately on one OS and remain isolated from one another, allowing users to leverage application-level virtualization. The result is that applications can be spun up within a matter of seconds, adding tremendous efficiency and agility to building out cloud operations.

Challenges with Container Security

When transitioning applications to containers, how do users guard against network threats? While users can regulate authorization and access to the application itself via protections within Amazon's Virtual Private Cloud (VPC), a robust application security service is needed to shield against external network attacks. As a leading security vendor on AWS, Imperva SecureSphere can be deployed within your VPC to provide ironclad protection against open vulnerabilities.

The SecureSphere Solution

SecureSphere Web Application Firewall (WAF) for AWS provides multiple defenses to combat OWASP top ten threats, giving users keen insights into emerging security threats, and keeping cloud deployments compliant with required security standards such as PCI DSS, HIPAA and FIPS.

To protect ECS applications, SecureSphere gateways can be deployed within a VPC in a sandwich deployment between the external and internal ELB.

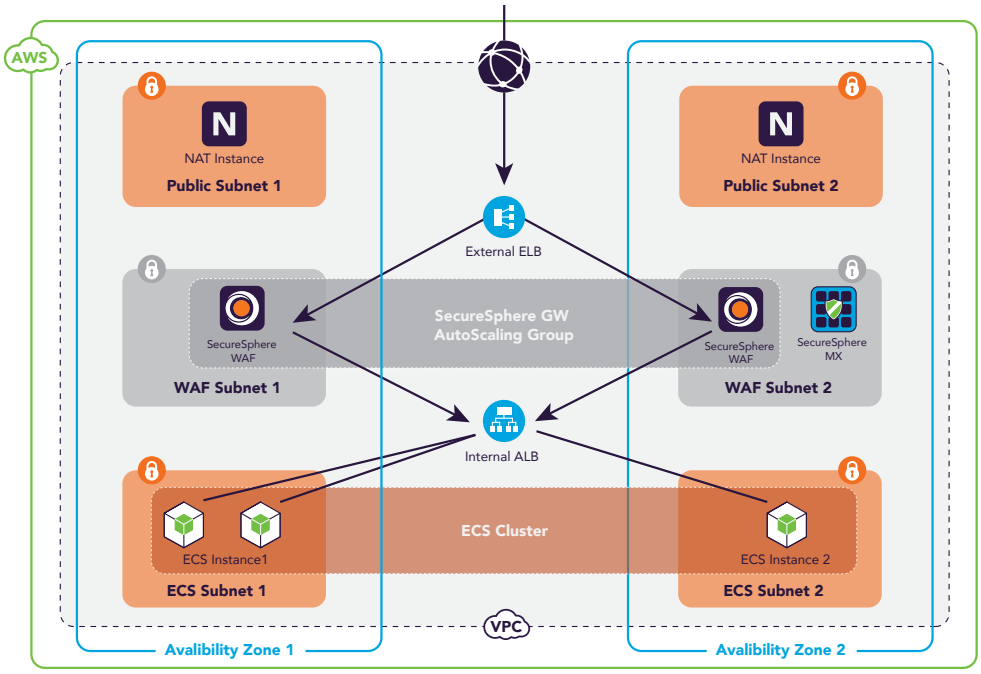

Figure 1 Deployment of SecureSphere and ECS

Importantly, SecureSphere can protect any application on AWS, and is agnostic to whether the application is deployed within an EC2 instance or is containerized via ECS. SecureSphere WAF treats either case as a node of vulnerability, allowing AWS users to easily transition a traditional EC2 deployment to a containerized one, without compromising security.

Benefits of SecureSphere on AWS

For any service running on AWS, Imperva SecureSphere offers a number of security benefits, including:

- Autoscale capability for security on demand–To facilitate highly programmable deployment, SecureSphere offers support for CloudFormation (CF) templates. This allows users to autoscale security on demand by removing the need for manual spin up/down of WAF instances and enabling users to program instantiation of additional gateways as needed, hence reducing boot up time and allowing users to expand their security resources on demand.

- Continue to grow deployments without security bottlenecks–With our AWS offering, API rules can be leveraged to ensure programmable deployment of SecureSphere services using our software development kits (SDKs) ., ensures users can continue to take advantage of the speed and ease of containerized application deployment without security being the bottleneck. Users can create reverse proxy rules, white-lists, and more through using APIs, which will immediately take effect upon spin up of a new EC2 instance.

- Business Continuity– SecureSphere's innovative Dynamic Profiling allows for real-time learning of user behavior such that patterns are recognized to differentiate between legitimate user traffic and suspicious activity, while incorporating changes into an application profile over time to ensure that noted patterns are constantly up to date. This ensures stable business continuity by allowing organizations to protect sensitive web applications without introducing excessive IT overhead or blocking legitimate web traffic.

- Protect against common security vulnerabilities–SecureSphere on AWS carries the same feature support as our on-prem SecureSphere product, with extensive feature support to provide bot protection, IP reputation services, and more. Take advantage of ThreatRadar services, which leverage crowd-sourced intelligence feeds from around the world to gain keen insights into security vulnerabilities and traffic patterns.

- Manage on-prem and cloud gateways from a single management console -- SecureSphere allows users to manage gateways deployed both on-prem and on AWS through a single MX console. This consolidates and simplifies security management for hybrid cloud deployments.

With Imperva SecureSphere, you can ensure that your containerized applications remain highly protected against cybersecurity threats on the cloud. Start your thirty-day trial with SecureSphere on AWS today.