Security

Intrusion Detection Systems and Intrusion Prevention Systems for EC2 Instances

AWS Shared Responsibility Model

The AWS Cloud is architected with security as the highest priority. Security is designed into multiple layers of the AWS environment with a data center and network architecture built to help protect even the most security sensitive organizations. AWS takes responsibility for security of the cloud while organizations, on the other hand, are responsible for their security configuration in the cloud (see figure 1). With this approach organizations are able to implement the security configuration that is best for them. Amazon Elastic Compute Cloud (Amazon EC2) offers organizations a virtual compute environment for running a variety of workloads. With the Shared Responsibility Model organizations are responsible for the configuration that they implement to ensure their compute instances and the assets within them are secure. AWS services and third-party offerings enable you to help protect your instances, and strengthen your overall security posture.

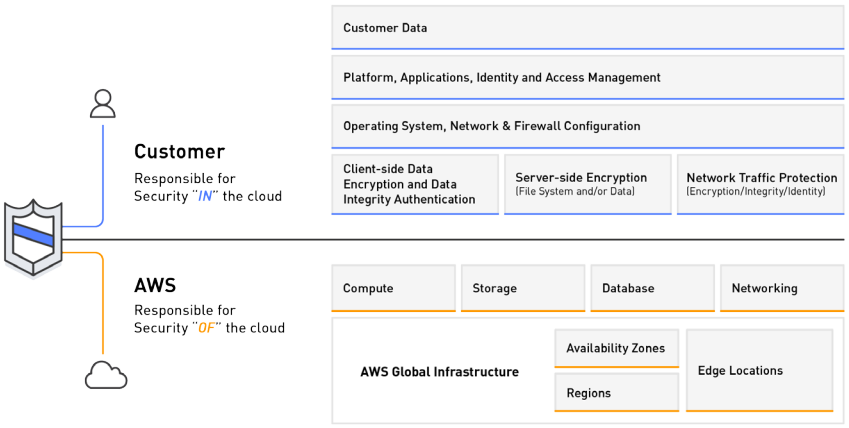

Figure 1: The AWS Shared Responsibility Model

EC2 Instance IDS/IPS

Intrusion Detection Systems (IDS) monitor networks and/or systems for malicious activity or policy violation, and report them to systems administrators or to a security information and event management (SIEM) system. Intrusion Prevention Systems (IPS) are positioned behind firewalls and provide an additional layer of security by scanning and analyzing suspicious content for potential threats. Placed in the direct communication path, an IPS will take automatic action on suspicious traffic within the network.

EC2 Instance IDS/IPS Challenges:

Patching

Organizations can fall into the habit of reactively patching their EC2 instances after a vulnerability or bug has been detected, causing them to spend more time and effort fixing problems rather than preventing them. In order to stay one step ahead of potential attacks, patching should be done proactively. Vulnerability assessments should be conducted on a regular basis to ensure that critical security patches can be applied quickly.

Controlling Network Access

Amazon Virtual Private Cloud (Amazon VPC) security groups act as a virtual firewall for your EC2 instance. Security groups allow you to add rules that control inbound and outbound traffic to your EC2 instance. It is up to you to add rules to the security groups to control traffic at a level that you deem appropriate. Like proactive patching, security group rules should be regularly evaluated to ensure they are up to date and protecting against unauthorized access to your EC2 instance and the applications running on your EC2 instance.

IDS/IPS Components:

IDS/IPS solutions offer key features to help protect your EC2 instances and the applications running on your EC2 instances. IDS features typically include: alerting administrators of possible incidents, logging information, and reporting attempts. In addition to IDS features, Intrusion Prevention Systems are designed to actively prevent or block intrusions that are detected. This may include taking action against attacks by dropping malicious packets, blocking traffic from the source address, and resetting the connection altogether. AWS solutions and third party IDS/IPS offerings in AWS Marketplace are designed to help organizations manage and enforce policies, and identify and deter malicious activity.

Detect Vulnerabilities in your EC2 Instances

- **Host Intrusion Detection Systems:** Monitor inbound and outbound packets from the EC2 instance, and may evaluate system files for changes.
- **Behavioral Monitoring:** Can be considered an anomaly-based intrusion detection system, which deals with malicious insiders as well as targeted external attacks.

IDS solutions in AWS Marketplace can be combined with various AWS services such as Amazon CloudWatch, a monitoring service for resources and applications you run on AWS. Additional services like Amazon Inspector, an automated security assessment service, can also be complemented by offerings in AWS Marketplace.

Protect Your EC2 Instances from Attacks

- **Next Generation Firewalls**: Provide much of same protections as standard firewalls, while also adding application-level inspection, intrusion prevention, and full-stack visibility.
- **Intrusion Prevention Solutions**: Include always-on detection to safeguard your EC2 instances and protect against instrusion or attacks.

Software vendor offerings in AWS Marketplace offer a variety of firewalls and IPS to fit your particular environment. Launching IDS/IPS solutions from AWS Marketplace offers the flexibility to change deployments as needed.

Respond to Intrusion or Attacks Against your EC2 Instances

- **Endpoint Detection & Response Solutions:** Context-aware endpoint monitors that record and report detailed system-level activities. This allows threat analysts to rapidly assess the nature and extent of incidents and take the proper measures to respond to it.

Get Started with IDS/IPS Software in AWS Marketplace

Find and deploy the solution you need in minutes

Save money with pay-as-you-go pricing

Scale globally across all AWS Regions