evan360®

Security & Infrastructure

OVERVIEW

The infrastructure view (fig.1) is an Amazon Web Services (AWS) hosted deployment of the EVAN360 cloud application. Security is a key consideration in the overall design of the EVAN360 infrastructure. Separating key infrastructure components into private security groups ensures maximum protection of our customer's information and EVAN360's intellectual assets. The intended purpose of this document is to outline the security boundaries and to provide a description of each infrastructure component's purpose.

Note: Descriptions work from left to right then up and down.

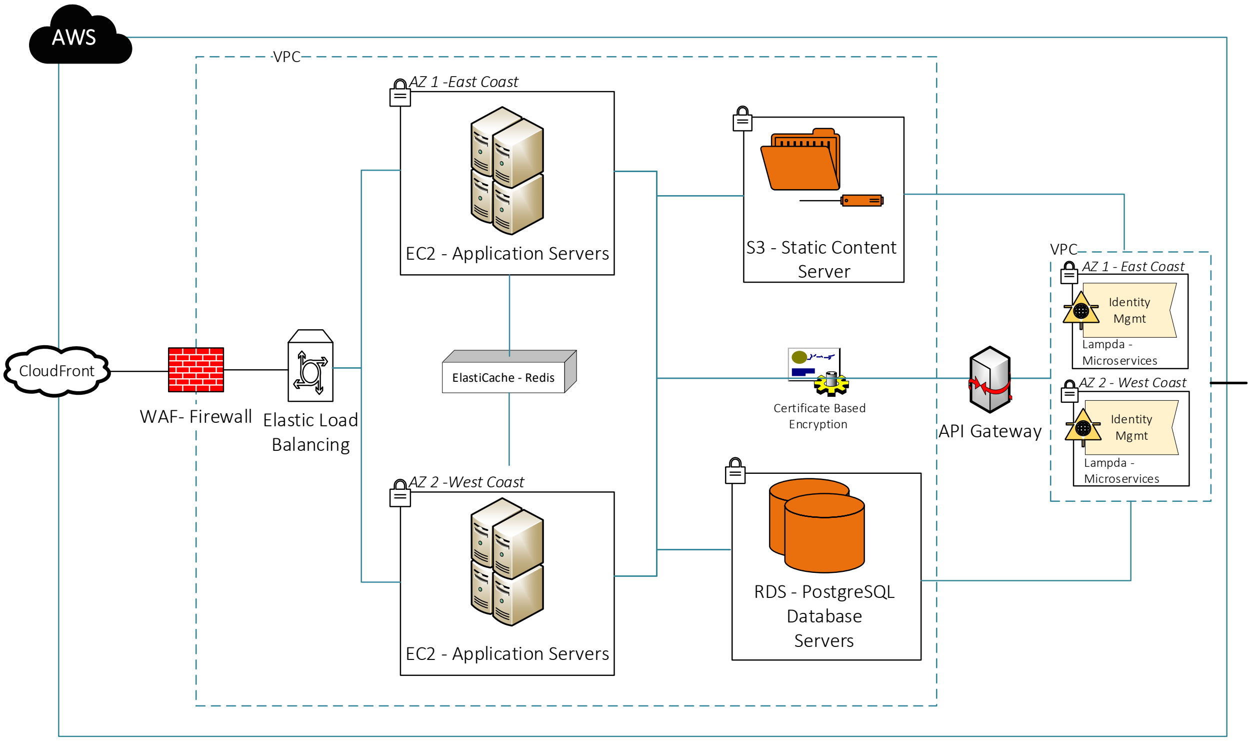

Figure 1: EVAN360 IT Infrastructure View

AWS CLOUDFRONT

All access to the EVAN360 application must come through CloudFront. CloudFront is a Content Delivery Network service offered by AWS to serve up EVAN360 application content for very quick access. CloudFront also can be configured to control origin access control. EVAN360 employs CloudFront to be that first line of defense for against malicious attacks by preventing traffic originating from various countries notorious for distributing US based applications. Countries like North Korea, Iran and China are just a few of those countries that complete access is blocked by CloudFront.

AWS WEB APPLICATION FIREWALL (WAF)

Once internet traffic (HTTP and HTTPS) passes through CloudFront, it must get past the EVAN360 firewall. AWS WAF is a web application firewall that protects the EVAN360 Infrastructure from common application and database vulnerabilities a potential hacker can exploit. The EVAN360 WAF is configured to block any internet traffic deemed an attack. Common attacks such as SQL Injection, Cross Site Scripting and Remote Code Execution are just a few website vulnerabilities prevented by the WAF. The WAF also serves as the gateway into the EVAN360 secure private network or the AWS Virtual Private Cloud (AWS VPC)

AWS VIRTUAL PRIVATE CLOUD (VPC)

No internet traffic can enter VPC unless it passes through the WAF. VPC configuration is important for all the different EVAN360 servers to communicate each other without worrying about any other security infrastructure components such as the firewall. Without a VPC in place, every application and database server would have to have a WAF in front of it to prevent hackers from hacking our infrastructure. Even though all the different infrastructure components are seemly wide open to communicate with each other, security is still applied both at the server layer and at the application and database layer. Access to any EVAN360 resource within the VPC still must pass through the AWS Identity and Access Management (IAM) service. IAM enables authentication and authorization and uses permissions to allow and deny access to AWS resources such as the applications server or the database server. Once internet traffic is inside the VPC, it's routed to the application servers trough AWS's Elastic Load Balancing service.

AWS ELASTIC LOAD BALANCING

Once internet traffic (HTTP and HTTPS) routes into the VPC, the Elastic Load Balancing service automatically passes the request to one of the application servers. This serves two purposes. One, to balance traffic so to prevent slowdowns from occurring when EVAN360 is busy. The second main purpose is to make sure the EVAN360 application is always available in case of a hardware or software failure on any given application server (AWS EC2).

AWS ELASTIC COMPUTE CLOUD (EC2)

The heart of the EVAN360 application lives here. AWS EC2 services are our application servers. This is where all the code is deployed and where all the integrations happens. The EC2 servers are designed to scale both up and down as requirements change and usage increases. EC2 is designed to easily integrate with all the other infrastructure components within the VPC. Seamlessly communicating with other infrastructure components is the key to speed and the EC2 servers stay synchronized through the use of AWS ElastiCache.

AWS ELASTICACHE

What makes EVAN360 extremely fast is ElastiCache. ElastiCache is there for performance and acts as a broker to move session data and information into memory for quick access. EVAN360 employs Redis (**Re**mote **Di**ctionary **S**erver) as it's ElastiCache service.

AWS SIMPLE STORAGE SERVICE (S3)

Simple storage is all this really is and S3 acts very much like a file server for a variety of different purposes. The main purpose of S3 is to serve as a place to store files, such as EVAN360 session recordings and archiving. S3 is also where our backups are stored ensuring quick restoration of information when or if needed.

AWS RELATIONAL DATABASE SERVICE (RDS)

RDS is the database component of the EVAN360 Infrastructure and is where all EVAN360 configuration, user, provider, session and application data is stored. The database is a PostgreSQL database engine and is used by both EC2 and Lambda (*described later in this document*) to retrieve and store transactional data.

AWS API GATEWAY

The API Gateway provides access to EVAN360 microservices layer. Microservice-based application architecture allows for applications that can scale by developing small, distinct components, managed separately from the core application hosted on EC2. The idea behind microservices is that it allows for changes to occur without a large redeployment of code. As our application grows, managing these types of services become easier and reduces risk. The API Gateway makes access to these types of services easy to develop against and secure.

AWS LAMBDA

AWS Lambda automatically runs certain application components of the EVAN360 application without requiring Application Servers (EC2 Servers). What that means is that there are no administration activities required to maintain those pieces of the application hosted on Lambda. EVAN360 uses Lambda to run our Application Security Microservices. As EVAN360 users access our application, traffic is routed through the API Gateway to the Lambda Microservice for authentication and authorization. Having this architecture in place will allow for simpler connections to external application security platforms like Active Directory and Ping IAM. For added security, the EVAN360 Application Security Microservices hosted on Lambda sit within its own Virtual Private Cloud.