Securing the AWS cloud environment integrated with Palo Alto Networks

THE CHALLENGE

Secure Utility needs to reinforce the security of its cellular router environment with a Palo Alto Firewall system, in order to provide secure access to connectivity data from cellular devices to AT&T's APN network in order to offer secure remote connectivity solutions to different customers.

Secure Utility has already deployed its environment on the AWS "standalone architecture" and now requires a Firewall with high availability to meet AT&T VPN requirements to deploy its solution with APN services on the AWS network, as well as allowing it to scale in and out, supporting new customers in regions such as Great Britain and Europe (Germany, Switzerland, Austria).

THE SOLUTION

Nub8 after the analysis of the current situation, the needs and expectations of Secure Utility, the following services are defined:

- Assessment and re-architecture of the customer's AWS public cloud infrastructure.
- Design and provisioning of Palo Alto HA Firewall solution
- Design, implementation and testing of the adjusted AWS public cloud architecture.

The solution designed by Nub8 for Secure Utility seeks high availability (active/passive scheme), performance, security and efficiency in cloud resource utilization and involves:

- Compute and storage capacities
- Identity and Access Management (IAM)
- Network resources
- Security components

The solution includes components and services deployed in the Amazon Web Services (AWS) cloud in order to take advantage of benefits related to scalability, flexibility, pay-per-use, among others. The WAF was incorporated into the architecture in order to protect the web application against the most common vulnerabilities such as: SQLi, XSS, brute force, DDoS, IP reputation, etc, in addition to allowing Secure Utility to create custom, application-specific rules that block attack patterns to ensure availability, secure resources and prevent excessive resource consumption.

SERVICES AND SOLUTIONS USED:

Additional components (compute, networking and security) of Secure Utility's HA solution are listed below.

- ➢ Load Balancer
- ➢ SNS
- ➢ Cloud Watch
- ➢ Cloud Trail
- ➢ Systems Manager
- ➢ S3
- ➢ Kinesis
- ➢ WAF

Provides secure remote connectivity for buildings, utilities and deployed assets. Its solutions are scalable and support all existing operational technologies in buildings, life safety and security systems.

The solution's multi-layer defense provides a secure private network with prioritized LTE connection, segregated at the back-end of most mobile operator networks, not on the public Internet. The remote connection to the secure private cellular network is protected by a managed, bank-grade firewall, updated in real time to defend against both upstream and downstream threats.

SOLUTION ARCHITECTURE:
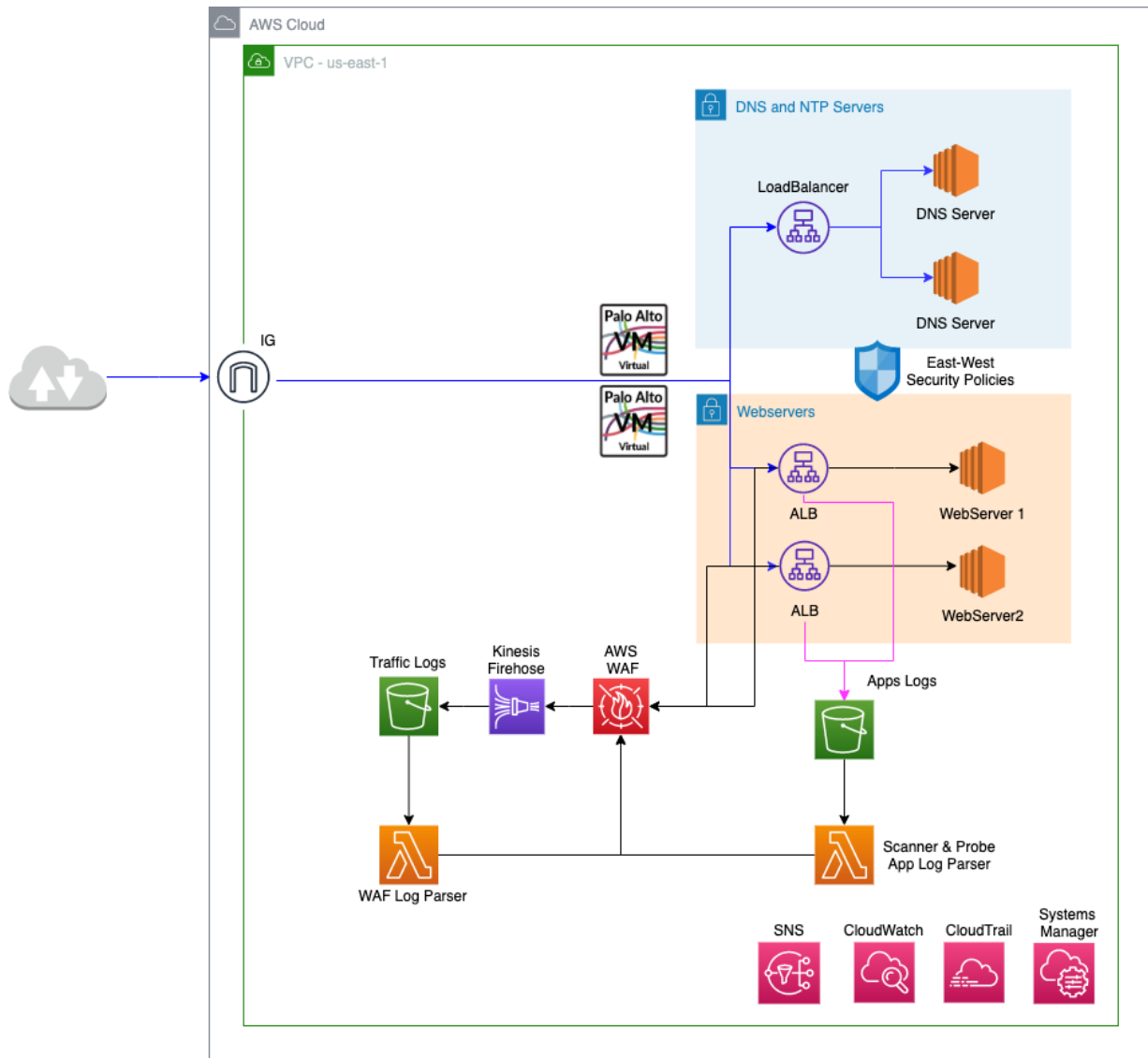
THE BENEFITS

- Optimized AWS public cloud infrastructure based on the Well Architecture Framework
- Cloud environment with enhanced security via Palo Alto firewall
- Reduced downtime, data theft and security breaches
- Flexibility and scalability
- High-performance solution
- Protection against new and emerging threats
- Protection against common web application vulnerabilities
- Optimized resource consumption