STEPHEN KAMITU MUNGUTI

PCI DSS COMPLAINT AWS ARCHITECTURE

AMAZON AWS HOSTED ECOMMERCE WEB APP

Kamitu.sm@gmail.com

5/23/2020

This document describes a proposed architecture of an AWS hosted ecommerce website conforming to the PCI DSS recommendations

Table of Contents

1. Introduction

PCI applies to all companies that process, transmit, or store cardholder (or sensitive) data of service providers, merchants, processors, or issuers.

Since AWS is PCI DSS compliant, it means that any organization that uses AWS products and services to process, transmit, or store cardholder data may depend on the technology infrastructure of AWS to acquire and manage their PCI certification.

The primary twelve requirements for PCI DSS can be broadly classified under these six areas:

1. **Construct and Maintain a Secure Network:** This entails using a firewall to protect data without the use of vendor-supplied security protocols.

2. **Protect Cardholder Data:** Protection of sensitive data is enabled through encryption in public networks.

3. **Maintain a Vulnerability Management Program:** Vulnerability of the data network is reduced by installing antivirus software or programs to protect all systems against malware.

4. **Implement Strong Access Control Measures:** Access control is implemented by restricting access to cardholder data and by incorporating identity authentication before access to system components.

5. **Monitor and Test Networks Regularly:** Access must be tracked and monitored on all network resources, and regular security system checks must be conducted.

6. **Maintain an Information Security Policy:** A reference policy must document the steps and procedures that need to be followed by all personnel handling secure data.

2. The Architecture

The architecture below is proposed.

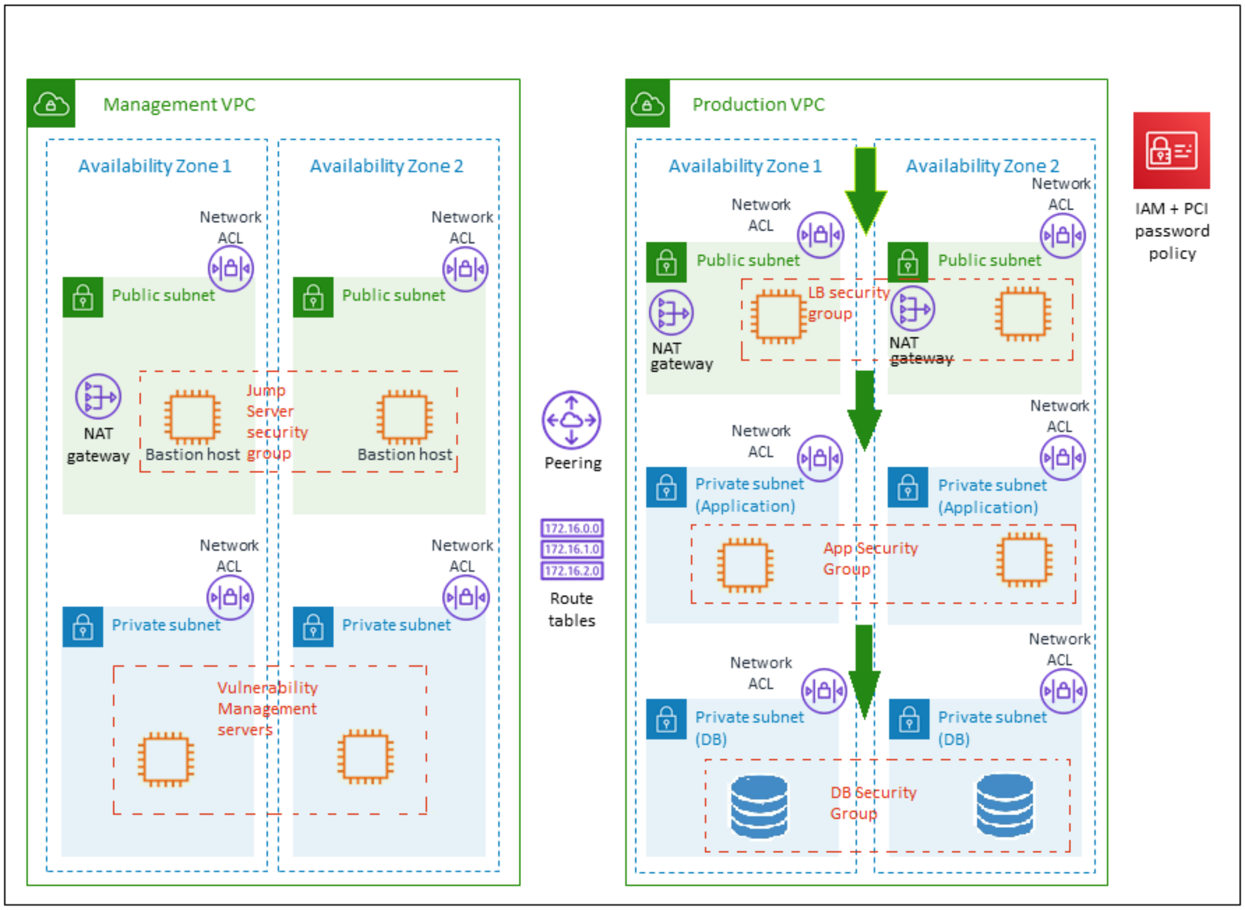

Fig 1.1 PCI DSS Compliant Architecture

The architecture is assuming a multi-tier web application employing load balancers, application servers and database servers. It is assumed that the reader is aware of Amazon networking and security concepts especially:

- Availability zones and regions
- VPC
- Public and Private subnets
- VPC peering and route tables
- NAT gateway for allowing internet access to the private subnets
- Security groups for EC2 instances
- Network ACL for subnets

2.1 Architecture rationale

The architecture includes the following features depending on the requirements being addressed:

1. **Construct and Maintain a Secure Network**

   - Standard, external-facing virtual private cloud (VPC) Multi-AZ architecture with separate subnets for different application tiers and private (back-end) subnets for the application and the database.
   - Managed network address translation (NAT) gateways to allow outbound internet access for resources in the private subnets.
   - Only load balancers are allowed in production public subnets, alternatively one could employ AWS load balancers.
   - VPC peering between the management and production VPC to allow for management of the production infrastructure.
   - Network access control list (network ACL) rules on subnets to filter traffic.
   - Security groups for EC2/DB associated compute resources for easy firewall rule grouping and as an additional security measure. Remember to restrict SSH/Management traffic to the bastion host only.

2. **Protect Cardholder Data**

   - SSL enabled load balancers for all customer traffic, disable all http traffic
   - PCI-compliant password policy for website customers
   - Encrypted EBS or Amazon RDS for DB compute resources

3. **Maintain a Vulnerability Management Program**

   - Installing antivirus software or programs to protect systems against malware.

4. **Implement Strong Access Control Measures**

   - A secured bastion login host to facilitate command-line Secure Shell (SSH) access to Amazon Elastic Compute Cloud (Amazon EC2) instances for troubleshooting and systems administration activities.
   - Basic AWS Identity and Access Management (IAM) configuration with custom IAM policies, with associated groups, roles, and instance profiles. Roles are to be assigned appropriately to different administrators.
   - PCI-compliant password policy for IAM users

5. **Monitor and Test Networks Regularly:**

   - Monitor activities on the bastion host. This could employ CyberArk or similar products that will provide visibility on all activities carried out by system and database administrators.

- Vulnerability management servers which include logging servers (splunk, grafana, ELK), vulnerability scanners and antivirus managers. AWS tools such as CloudWatch could be employed too as logging servers.

6. **Maintain an Information Security Policy:**
    - A reference policy must document the steps and procedures that need to be followed by all personnel handling secure data.

What is meant by PCI compliant password policy?

The following requirements must be met for a password policy to be considered PCI-DSS compliant

1. Require a minimum length of at least seven characters.
2. Contain both numeric and alphabetic characters.
3. Users to change passwords at least every 90 days.
4. Password parameters are set to require that new passwords cannot be the same as the four previously used passwords.
5. First-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use
6. User accounts are temporarily locked-out after not more than six invalid access attempts.
7. Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.
8. System/session idle time out features have been set to 15 minutes or less.
9. Passwords are protected with strong cryptography during transmission and storage.