# TECHNICAL WORKBOOK

## PCI Compliance in AWS

Report Date: 2 July 2018

Authors: Jordan Wiseman, QSA
Andrew Plato

ANITIAN

# COPYRIGHT

For permission requests, write to the publisher, at the address below:

Anitian / Sherlock Cloud Security
9780 SW Shady Ln, Suite 100
Portland OR, 97223
info@anitian.com
https://anitian.com
https://sherlockcloud.io

# TABLE OF CONTENTS

# 1. EXECUTIVE SUMMARY

This workbook will help you build cloud environments in Amazon Web Services (AWS) that are compliant with the Payment Card Industry Data Security Standard (PCI DSS).

## 1.1. Intended Audience

The intended audience for this workbook includes:

- People and organizations who need to make their AWS environment(s) PCI compliant
- PCI Qualified Security Assessors (QSA) assessing Cardholder Data Environments (CDEs) running in AWS.

## 1.2. Premises

This section lists Anitian's assumptions and premises that influence the content of this workbook.

### 1.2.1. As Is Disclaimer

Anitian is a Qualified Assessor Company (QSAC) and the author of this workbook. The content in this workbook is based upon Anitian's interpretations of the PCI DSS. This content is provided "as is" with no guarantees expressed or implied. The content of this document is subject to change without notice. Likewise, future changes to the AWS environment may alter some of the guidance in this document.

Your QSA may have different interpretations of the PCI DSS than Anitian and the content of this workbook.

None of the content in this workbook is intended to replace or supersede the requirements of the PCI DSS.

### 1.2.2. Intent

The purpose of this workbook is to provide guidance on making AWS environments PCI compliant. While this workbook covers PCI compliance for AWS, it does not offer step-by-step instructions on assessing PCI for AWS environments.

### 1.2.3. Prerequisite Knowledge

Readers of this workbook need to be familiar with:

- The PCI DSS, currently at version 3.2.1
- How to manage an AWS environment
- The PCI Standards Council's Cloud Computing Guidelines v3

### 1.2.4. PCI Scoping

While this workbook discusses PCI scope reduction and segmentation within AWS, it is not a comprehensive guide on PCI scope. Consult with your PCI QSA or the PCI Standards Council for more information on scope reduction strategies.

### 1.2.5. Compensating Controls

This workbook does not address compensating controls for AWS implementations. While you may use compensating controls in AWS, a PCI QSA must validate those controls in alignment with the requirements of the PCI DSS.

# 2. AWS PCI COMPLIANCE OVERVIEW

This section provides a general overview of AWS PCI compliance.

For additional details, see Amazon's AWS PCI Level 1 FAQ.

## 2.1. AWS PCI Compliance Status

AWS is currently a PCI DSS-compliant Level 1 Service Provider. Merchants and other service providers can use AWS to establish their own PCI-compliant environments. However, AWS compliance is a shared responsibility model. Although AWS is PCI DSS compliant, that does not mean customer environments are automatically compliant.

AWS customers are responsible PCI compliance in their environment. This includes AWS service configurations, guest operating systems, and requisite security controls (IDS, anti-virus, etc.).

AWS's PCI compliance allows customers to accelerate their own compliance. Since AWS is a PCI-compliant service provider, customers do not need to assess AWS's compliant infrastructure. A PCI assessor only needs to review AWS's Attestation of Compliance (AOC) and Responsibility Matrix documents to validate the compliance of the infrastructure.

## 2.2. AWS PCI Compliance Scope

Amazon's AWS Service Provider validation assessment for PCI compliance includes the AWS Management Environment and underlying infrastructure.

The table below lists the AWS services that are included in PCI compliance as of July 2018:

| SERVICE | DESCRIPTION |
|---|---|
| Amazon API Gateway | Accepts and processes API calls |
| Amazon Cloud Directory | Cloud-native directory service |
| Amazon CloudFront | Content delivery web service |
| Amazon CloudWatch Logs | Log file monitoring service |
| Amazon Cognito | Mobile and Web app single sign-on (SSO) |
| Amazon Connect | Customer service contact center service |
| Amazon DynamoDB | Scalable and highly available NoSQL data store |
| Amazon Elastic Block Store (EBS) | Block-level storage for EC2 instances |
| Amazon Elastic Compute Cloud (EC2) | Scalable cloud machine instances |

| SERVICE | DESCRIPTION |
|---|---|
| Amazon Elastic Container Registry | Registry for storing, managing, and deploying Docker images |
| Amazon Elastic Container Service (ECS) | Scalable, hosted Docker container instances |
| Amazon Elastic File System | Scalable, cloud-based file system |
| Amazon Elastic MapReduce (EMR) | Big data services |
| Amazon ElasticCache for Redis | High-performance, in-memory data store for Redis clients |
| Amazon Glacier | Data archival storage |
| Amazon Inspector | Automated security assessment service |
| Amazon Kenesis Data Streams | Streaming data capture and emission |
| Amazon Macie | Machine learning tool for data discovery, analysis, classification, and protection |
| Amazon Polly | Text to speech service |
| Amazon QuickSight | Business intelligence, analysis, and visualization service |
| Amazon Redshift | High-capacity data warehousing |
| Amazon Relational Database Service (RDS) | Database as a service |
| Amazon Route 53 | Scalable and highly available Domain Name System |
| Amazon S3 Transfer Acceleration | Data transfer service for S3 buckets that uses Amazon CloudFront to automatically optimize transfer performance |
| Amazon SageMaker | Machine learning services for applications |
| Amazon Simple Notification Service (SNS) | Flexible pub/sub messaging and mobile notification service |
| Amazon Simple Queue Service (SQS) | Message queuing service |
| Amazon Simple Storage Service (S3) | Store and retrieve any amount of data |
| Amazon Simple Workflow Service (SWF) | Service for coordinating application components |

| SERVICE | DESCRIPTION |
|---|---|
| Amazon SimpleDB | Highly available and flexible non-relational data store |
| Amazon Virtual Private Cloud (VPC) | A logically isolated portion of the AWS network, functioning as a private network. |
| Amazon WorkDocs | Electronic document management system (EDMS) |
| Amazon WorkSpaces | Desktop-as-a-Service (DaaS) solution |
| Auto Scaling | Automated, event-based instance provisioning |
| AWS CloudFormation | Creates and deploys templates of AWS resources |
| AWS CloudHSM | Cloud access to hardware security modules |
| AWS CloudTrail | Reporting on AWS API calls |
| AWS CodeBuild | Service to compile, test, and package source code |
| AWS CodeCommit | Secure, scalable Git repositories for code. |
| AWS Config | AWS resource inventory, change history, and change notifications |
| AWS Database Migration Service (DMS) | Migrates data to and from most widely used commercial and open-source databases |
| AWS Direct Connect | Direct, private, dedicated connection to AWS |
| AWS Directory Service for Microsoft Active Directory | AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as AWS Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud |
| AWS Elastic Beanstalk | Web application deployment and provisioning |
| AWS Firewall Manager | Centralized repository for managing AWS Web Application Firewall rules across multiple accounts and/or applications |
| AWS Identity and Access Management (IAM) | Access controls and key management |
| AWS Key Management Services (KMS) | Data encryption key management |
| AWS Lambda | Serverless, event-driven code execution |

| SERVICE | DESCRIPTION |
|---|---|
| AWS Managed Services | AWS service that manages customer's AWS infrastructure on their behalf |
| AWS Management Console | Web interface for managing all AWS services |
| AWS OpsWorks Stacks | Manage cloud and on-premise servers as layered application stacks. |
| AWS Service Catalog | Central management and control of AWS services that are approved for use in your organization |
| AWS Shield | Distributed denial of service (DDoS) protections for AWS hosted applications. |
| AWS Snowball | Secure transfer service for petabyte sized data sets using special hardware appliance |
| AWS Snowball Edge | Secure transfer service for terabyte sized data sets using special hardware appliance |
| AWS Snowmobile | Secure transfer service for petabyte sized data sets using purpose-built shipping container to retrieve and move data from your data center to the cloud |
| AWS Storage Gateway | Storage service that allows on-premise systems to seamlessly use AWS cloud storage |
| AWS Systems Manager | Unified interface for monitoring multiple AWS services |
| AWS Web Application Firewall (AWS WAF) | Protection for CloudFront-accelerated web sites from web-based attacks |
| AWS X-Ray | Analysis and debugging service for distributed applications |
| Elastic Load Balancing (ELB) | Application fault tolerance and load balancing |
| Lambda@Edge | Service to optimize Lambda code operations based on the geo-location of the requestor |

The following regions, availability zones and edge locations are in-scope for PCI compliance as of July 2018:

- US East (Northern Virginia)
- US East (Ohio)
- US West (Oregon)
- US West (Northern California)
- AWS GovCloud (US-West)
- Canada (Central)
- EU (Ireland)
- Europe (Frankfurt)
- Europe (London)
- Europe (Paris)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- South America (São Paulo)

### 2.2.1. Out of Scope AWS Services

AWS is constantly developing and deploying new services. While not all AWS services are covered under the PCI attestation, you can still use out-of-scope services. If you use an out-scope-service, your PCI assessor must review them to ensure your configuration meets compliance requirements.

For example, *AWS Certificate Manager* is not in scope as of the most recent AWS Service Provider Assessment. If you use *AWS Certificate Manager* for your in-scope web applications, you must demonstrate that your usage meets the relevant PCI requirements. However, *AWS Certificate Manager* runs on AWS's compliant infrastructure. Therefore, while the service itself is not compliant, the infrastructure it runs on is compliant.

## 2.3. AWS PCI Compliance Responsibility

Determining who is responsible for PCI requirements is one of the more complex aspects of cloud hosting. This section outlines how to define and organize a PCI compliance assessment for an AWS hosted environment.

This workbook outlines the areas where AWS can cover compliance requirements, and where you must cover them yourself. It is important that you consult the AWS PCI DSS "Responsibility Matrix," which defines exactly what AWS covers. Appendix B contains a summary of this matrix. If AWS does not cover a requirement, or if there is shared coverage, then your organization has responsibility to ensure the requirement is met.

Furthermore, you cannot arbitrarily choose to ignore a PCI requirement. You must meet all the requirements. However, it is possible that not all requirements are relevant to your organization. Your QSA can clarify those that apply and those that do not.

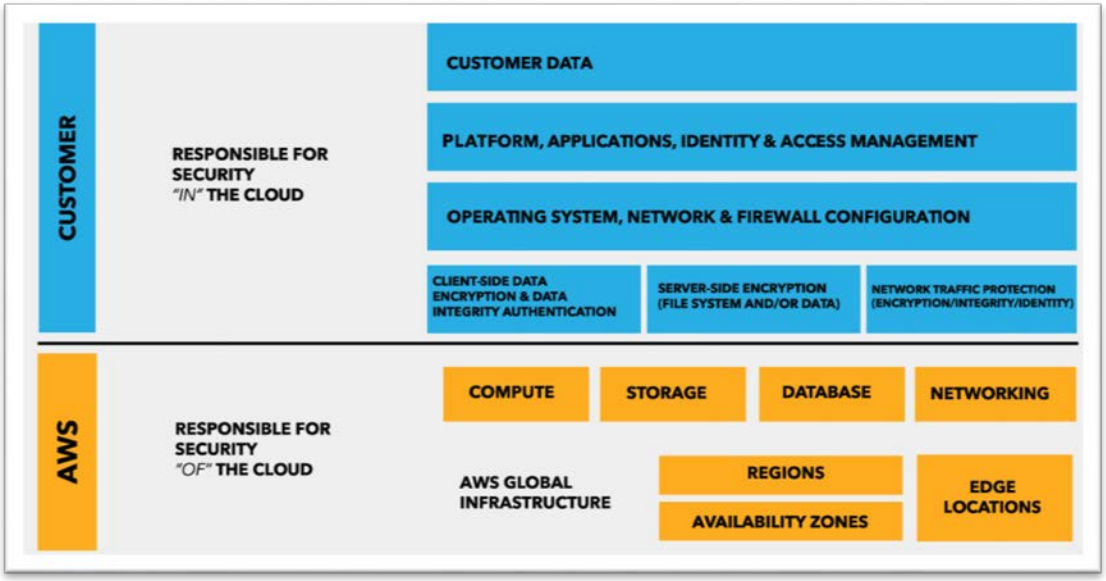

CUSTOMER
RESPONSIBLE FOR SECURITY "IN" THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)
AWS
RESPONSIBLE FOR SECURITY "OF" THE CLOUD
COMPUTE
STORAGE
DATABASE
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

*Figure 1 – Overview of AWS Shared Responsibility*

### 2.3.1. Amazon Responsibility - Security of the Cloud

Amazon is responsible for maintaining a PCI-compliant environment you can use to accelerate your compliance. This is "security ***of*** the cloud." AWS validates compliance annually and documents the results in AWS's Attestation of Compliance (AOC) document. As an AWS customer, you may request a copy via the Artifact service in the AWS Management Console.

### 2.3.2. Customer Reasonability - Security in the Cloud

You are responsible for designing, building, and maintaining a compliant environment in AWS.  This is "security ***in*** the cloud."

When you build your environment in AWS, part of the environment is compliant because it uses AWS's compliant infrastructure.  However, you are ultimately responsibility for PCI compliance for your organization (not AWS).

The specifics are defined in the "Responsibility Matrix" as shown in Appendix B.

# 3. GENERAL PCI DSS GUIDANCE

This section contains general guidance and strategies for meeting the twelve top-level PCI requirements using AWS services.

## 3.1. Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

The following AWS services can help support the firewall and network segmentation requirements of PCI:

- Amazon Virtual Private Clouds (VPCs)
- Amazon EC2 Security Groups
- VPC Network ACLs

The topics below describe the strategies and considerations for utilizing these services for compliance with Requirement 1.

### VPCs

VPCs are logically isolated portions of the AWS network that create private networks within a customer's AWS account. VPCs allow for customers to have multiple environments with no connectivity between them, as if they were air-gapped physical networks. The AWS network prevents packets with malformed or modified addresses from hopping across VPC boundaries. VPCs are designed without the need for layer two broadcast traffic. This vastly reduces the possibility of spoofing IP addresses within the AWS platform, and meets the intent of Requirement 1.3.3 for customer environments using VPCs.

It is possible to purposely connect VPCs to other networks. For example, Internet Gateways combined with NAT instances, Elastic IPs, and other resources can provide Internet access. VPC Peering and properly configured routing tables can connect VPCs to each other. And, as we will see in Section 4 below, it is also possible to use VPNs or AWS Direct Connect to extend on premise networks into the cloud.

NOTE: All subnets within the same VPC have a default route between them that cannot be removed.

### EC2 Security Groups

Security Groups are stateful firewall components in AWS EC2, which track established connections and only allow return traffic associated with the session. Security Group access control lists (ACLs) can be used to restrict traffic to and from instances at the IP address, port, and protocol level, for compliance with Requirement 1.3.6.

### VPC Network ACLs

VPC Network ACLs apply at the subnet level and can help segment CDE networks from other networks in your AWS Account. However, they are not stateful and (on their own) cannot be used to meet Requirement 1.3.6.

### Other Strategies and Considerations

For simple environments, like those in the reference architectures Section 4 describes, Anitian recommends using a dedicated cloud firewall AMI. Not only are these clearly stateful firewalls, but they can also offer many additional (and important) security functions, like intrusion prevention (Requirement 11.4 specifies the need for IDS/IPS).

There are several firewall Amazon Machine Images (AMIs) in the AWS Marketplace from companies such as Fortinet, Palo Alto, and CheckPoint. These firewall instances may require specific licensing from the vendor, but can provide familiar management interfaces and advanced capabilities.

For more complex or dynamic AWS architectures, like those employing Auto Scaling to ensure sufficient application capacity to meet demand, traditional firewalls can complicate managing the environment and limit scalability. For these setups, Security Groups and host-based firewalls can be used to achieve segmentation for the CDE.

## 3.2. Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

The following AWS service can help support the host hardening requirements of PCI:

- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS CloudFormation
- AWS OpsWorks Stacks

The strategies and considerations for utilizing Amazon EC2 for compliance with Requirement 3 are discussed below.

### Amazon EC2

When you use an Amazon-provided AMI to launch an EC2 instance, AWS generates unique passwords for the administrator or root accounts, and encrypts these credentials using customer-specific private keys. This helps support compliance with Requirement 2.1.

You can also create custom AMIs based on your documented configuration and security standards. These can be used as to launch new instances and help ensure, and demonstrate compliance, with Requirement 2.2.

### Amazon CloudFormation

Just like custom AMIs allow you to launch images based on your standards, CloudFormation allows you to build templates (described in JSON or YAML) for entire AWS environments. These templates help eliminate human error in the build process, and can ensure your AWS environments are built according to your documented standards.

You can even use the CloudFormer tool to create templates based on AWS resources you are already running. This allows rapid environment duplication, providing a likely-compliant starting place for new AWS environments.

### AWS OpsWorks Stacks

Extending the idea of template-based environments, AWS OpsWorks Stacks leverages Chef to fully automate the deployment, configuration, and scaling of the resources needed for an application.

NOTE: PCI assessments must be performed against the production. The process and resulting ROC, SAQ, and AOC documents, cannot be used to certify a template or reference architecture. OpsWorks Stacks, CloudFormation templates, and custom AMIs can save time and ensure consistency when building AWS environments, but they do not guarantee PCI compliance.

### Other Strategies and Considerations

If you use non-Amazon images, then you are responsible for ensuring that the defaults are changed. Consult with the relevant documentation for those images.

The AWS AOC covers the underlying security configuration management for the AWS services. However, it is your responsibility to create and implement security configuration standards for your EC2 instances. There are various solutions in the AWS marketplace that may assist with this requirement.

NOTE: Anitian has created hardened AMIs for all available OSes, as both base servers and with a hardened web server. They include a supporting Security Configuration Standard documenting the hardening steps performed, as required by PCI DSS Requirement 2.2.

## 3.3. Requirement 3: Protect Stored Cardholder Data

The following AWS services can help support the encryption and key management requirements of PCI for cardholder data (CHD) at rest:

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Services (KMS)
- AWS CloudHSM
- Amazon Relational Database Service (Amazon RDS)

The strategies and considerations for utilizing these services for compliance with Requirement 3 are described below.

### Amazon EBS

AWS supports several different ways to store information securely. EBS non-root volumes and S3 buckets support volume-level encryption using AES-256. For EBS volumes, EBS manages encryption keys using a FIPS 140-2 compliant infrastructure.

If you store CHD (such as DB files on the file system of a dedicated DB server instance) on an instance's encrypted volume, additional encryption is required for the CHD in order to comply with Requirement 3.4.1. This is not unique to AWS, but is cited for completeness and clarification.

NOTE: Not all EC2 instance types support encrypted EBS volumes. See EBS encryption.

### Amazon S3

Amazon S3 is a simple data storage service. It can encrypt stored objects with AES-256, and supports three different mechanisms for key management (see Server Side Encryption).

- **Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)**

  When SSE-S3 is enabled for an object in an S3 bucket (in the Management Console), S3 encrypts the object with a unique data encryption key. This data encryption key is itself encrypted with a master key that the S3 service rotates annually.

- **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)**

  SSE-KMS uses an envelope key to encrypt each object's data encryption key. This allows greater control of who can decrypt data, and provides an audit log of key usage. KMS is discussed in the next section.

- **Server-Side Encryption with Customer-Provided Keys (SSE-C)**

SSE-C allows you to use your own key and manage yourself. S3 never stores this key, only a message authentication hash of it to validate later use of the key when attempting to retrieve data.

By default, S3 is configured to use the SSE-S3. To use KMS or customer-supplied keys, you must specify the key management type when uploading the object via the console or the REST API. For further details, refer to S3 Upload Objects.

### AWS KMS

KMS is AWS's encryption key management service. KMS provides automatic key rotation on an annual basis through the Management Console. See Amazon's KMS Cryptographic Details document for additional information.

AWS KMS also has a documented API for programmatic or third-party vendor support.

KMS uses a customer master key (CMK) as the key encrypting key (KEK), and a backing key as the data encryption key. Enabling key rotation rotates the backing key.

When you enable key rotation, a new CMK and associated backing key (HBK) are generated annually. These new keys are used going forward, and the old CMK/HBKs remain available for decryption only. You can also manually create a new CMK/HBK at any time and set it as the currently active key.

NOTE: If you disable a CMK/HBK, it is no longer available to use, but attached EBS volumes that rely on the now-disabled key will continue to work. If that volume is detached from an Instance, you will have to re-enable the key to use the volume again.

CloudTrail logs all of the AWS KMS actions (key creation, data encryption, key rotation, etc.) to the CloudTrail log files in the user-specified S3 bucket.

### AWS CloudHSM

AWS also supports direct access from a VPC to dedicated, customer-specific hardware-based High Security Modules for certain encryption-related functions. AWS provides command line tools and software libraries for key management, encryption, and verification functions.

Like AWS KMS, CloudHSM integrates with CloudTrail to record all API calls to the CloudHSM service, including those made through the AWS console or via the provided libraries.

### Amazon RDS

In addition to encrypted storage, Amazon RDS also supports two different methods of database encryption. RDS encrypts the underlying storage using Amazon KMS managed keys. This protects the data at rest. RDS also supports Transparent Data Encryption (TDE) for Microsoft SQL and Oracle instances.

IAM policies control who can access RDS instances, and what actions they can perform. The databases within an RDS instance, however, rely on their own internal platform-specific mechanisms to manage access to data. Make sure to configure PCI-relevant account and password policies within CDE databases in RDS.

### Other Strategies and Considerations

If you run your own DB on an EC2 instance, you are fully responsible for managing the encryption of any CHD within the DB. This encryption should be performed using the standard strategies appropriate for the database engine in use. Common examples are programmatic-data encryption of CHD prior to storage, or database encryption using technology like Transparent Data Encryption.

The AWS Snowball and Storage Gateway services transfer large amounts of data into or out of AWS, storing some or all the data on-premise for a time. These services are not covered under AWS's AOC, but they do encrypt the data at rest. If you use these services, you will need to document this as part of meeting Requirement 3. See https://aws.amazon.com/snowball/faqs/#security and http://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html (respectively) for more details.

## 3.4. Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

These AWS components can help support the transit encryption requirements of PCI:

- Elastic load balancers
- Network ACLs
- Security Groups
- Customer Gateways
- Virtual Private Gateways
- VPN Connections
- AWS Direct Connect

### EC2 Load Balancers and Encryption

EC2 Load Balancers can offload encryption processing for secure communications for both internal and external connections.  Load balancers are the easiest way to ensure compliance with PCI DSS.

Without a load balancer, you must configure your own application and host with proper encryption protocols. That configuration would be outside the scope of AWS and therefore this workbook.

As of June 30, 2018, PCI DSS 3.2.1 does not permit the use of older SSL or TLS 1.0 protocols. You must use TLSv1.1 or preferably v1.2.

AWS fully supports TLSv1.1 and v1.2 on Application Load Balancers (ALB) and previous- generation EC2 Classic Load Balancers (CLB).  Network Load Balancers (NLB) do not support encryption and should not be used for external access to compliant environments.

You can read more about configuring load balancers here.

- HTTPS Listeners for Application Load Balancer
- Predefined SSL Security Policies for Classic Load Balancers

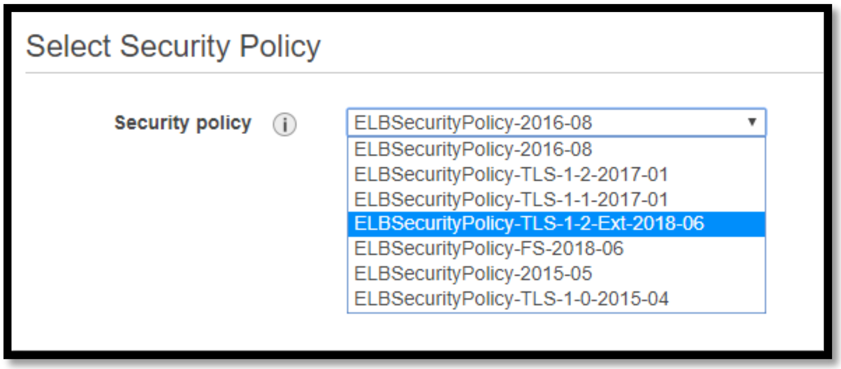
Encryption protocol negotiation between a client and load balancer is configured using security policies.  AWS provides predefined security policies that outline the negotiation process.

Some policies support all three TLS versions and therefore are not PCI compliant. You must use a policy that supports only TLSv1.2 or both v1.1 and v1.2.

### Setting Up Application Load Balancer Encryption

When configuring an ALB, use **ELBSecurityPolicy-TLS 1-2-Ext-2018-06** or **ELBSecurityPolicy-TLS 1-2-2017-**01. These policies support only TLSv1.2.

**ELBSecurityPolicy-TLS 1-1-2017-01** is also compliant and supports TLS v1.1 and v1.2.



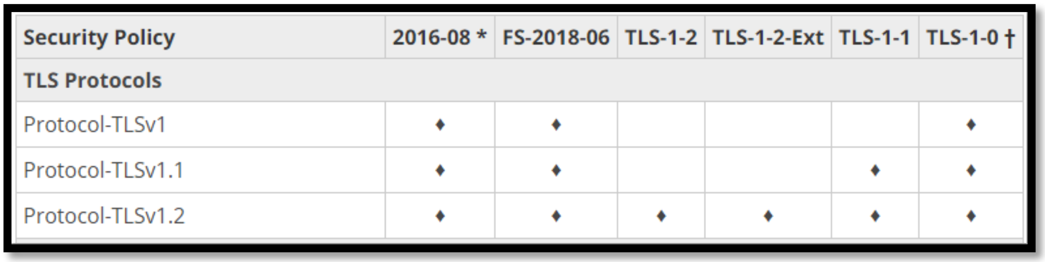
Select Security Policy

Security policy: ELBSecurityPolicy-2016-08

ELBSecurityPolicy-2016-08
ELBSecurityPolicy-TLS-1-2-2017-01
ELBSecurityPolicy-TLS-1-1-2017-01
ELBSecurityPolicy-TLS-1-2-Ext-2018-06
ELBSecurityPolicy-FS-2018-06
ELBSecurityPolicy-2015-05
ELBSecurityPolicy-TLS-1-0-2015-04

*Figure 2 – Application Load Balancer Security Policies*

As the chart below shows, other policies support v1.0, as well as 1.1, and 1.2 and are not PCI 3.2.1 compliant. If you use these other policies, external vulnerability scans (ASV scans) may report a non-compliant state with these policies.

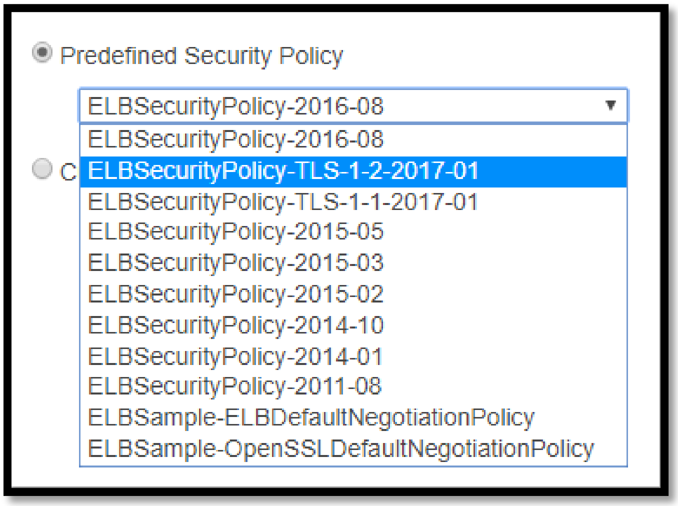


| Security Policy | 2016-08 * | FS-2018-06 | TLS-1-2 | TLS-1-2-Ext | TLS-1-1 | TLS-1-0 † |
|---|---|---|---|---|---|---|
| **TLS Protocols** | | | | | | |
| Protocol-TLSv1 | ♦ | ♦ | | | | ♦ |
| Protocol-TLSv1.1 | ♦ | ♦ | | | ♦ | ♦ |
| Protocol-TLSv1.2 | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ |

*Figure 3 – Application Load Balancer protocol map*

### Configuring Classic Load Balancers

For classic load balancers, select either **ELBSecurityPolicy-TLS-1-2-2017-01**, which only supports v1.2 or **ELBSecurityPolicy-TLS-1-1-2017-01,** which supports both v1.1 or v1.2.



● Predefined Security Policy

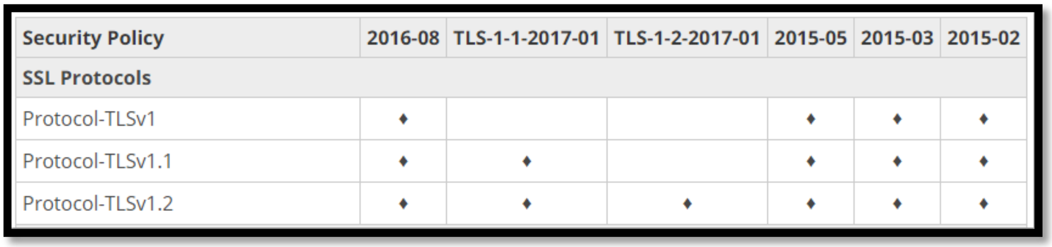
ELBSecurityPolicy-2016-08 ▾

- ELBSecurityPolicy-2016-08
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2015-05
- ELBSecurityPolicy-2015-03
- ELBSecurityPolicy-2015-02
- ELBSecurityPolicy-2014-10
- ELBSecurityPolicy-2014-01
- ELBSecurityPolicy-2011-08
- ELBSample-ELBDefaultNegotiationPolicy
- ELBSample-OpenSSLDefaultNegotiationPolicy

○ C

*Figure 4 – Classic Load Balancer policies*

As you can see, CLBs also have policies that support all three TLS versions.



| Security Policy | 2016-08 | TLS-1-1-2017-01 | TLS-1-2-2017-01 | 2015-05 | 2015-03 | 2015-02 |
|---|---|---|---|---|---|---|
| **SSL Protocols** | | | | | | |
| Protocol-TLSv1 | ♦ | | | ♦ | ♦ | ♦ |
| Protocol-TLSv1.1 | ♦ | ♦ | | ♦ | ♦ | ♦ |
| Protocol-TLSv1.2 | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ |

*Figure 5 -- Classic Load Balancer protocol map*

AWS may change the names of these policies and capabilities. It is important you do not use any policy that supports v1.0.

If you define your own policies, do not allow use of TLSv1 or SSLv3 protocols.

### Security Groups and Network ACLs

Security Groups and Network ACLs can block the use of insecure protocols based on network port.

### Customer Gateways, Virtual Private Gateways, and VPN Connections

Customer Gateways, Virtual Private Gateways, and VPN Connections enable you to set up encrypted VPN tunnels into an AWS VPC. AWS supports a wide range of common VPN solutions (see the VPC FAQ), as well as a generic text configuration file. AWS automatically creates the VPN settings so you can configure your endpoint to match. After creating a VPN connection in the VPN Connections section of the VPC dashboard, you can download the configuration file needed to set up the customer endpoint. View the configuration file to validate the encryption used (SHA1/AES 128). See Section *4.3.4.8 Create the VPN Connection* for implementation details.

### AWS Direct Connect

Direct Connect provides a dedicated high-speed connection between customer environments and AWS . Direct Connect is not encrypted so you will need to verify the privacy of the circuit. Depending on implementation, additional controls might be needed to comply with Requirement 4.1.

### Other Strategies and Considerations

It is your responsibility to configure secure transit encryption for Internet-facing services running on EC2 instances such as web servers. This should be included as part of the host hardening for Requirement 2.

VPNs can be implemented on commercial firewalls or VPN AMIs running in the environment. You are responsible for configuring the device to ensure alignment with Requirement 4.

The AWS Snowball and Storage Gateway services are not covered under AWS's AOC, but they do encrypt in transit. Document use of these services to meet requirement 4. See https://aws.amazon.com/snowball/faqs/#security and http://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html (respectively) for more details.

## 3.5. Requirement 5: Protect All Systems Against Malware and Regularly Update Anti-Virus Software or Programs

AWS does not provide anti-virus protection for EC2 instances. You are responsible for ensuring that all instances run appropriate anti-virus scans as well as log and report, as defined in PCI Requirement 5.

The AWS Marketplace offers numerous antimalware products. Anitian's managed security platform, Sherlock offers endpoint security.

## 3.6. Requirement 6: Develop and Maintain Secure Systems and Applications

AWS does not provide vulnerability and patch management of EC2 instances. While the AMIs are updated periodically, launched and running instances must be managed like any other host. For example, for the list of updates to the Amazon Linux AMI see the AWS Linux Security Center.

There are vulnerability and patch management solutions available in the AWS Marketplace that can assist with complying with Requirement 6.1 and 6.2.

Additionally, there are no AWS services that directly address the PCI requirements for secure software development (Req. 6.3) and change control (Req. 6.4). While not directly related to the PCI requirements, CodeDeploy and CodeCommit can assist with general source code management and deployment.

However, network segmentation technologies (discussed in Requirement 1 above) can separate production and development environments (Req. 6.4.1).

NOTE: AWS Config records changes to resources within AWS itself, but not to applications and within EC2 instances.

### AWS WAF and Amazon CloudFront

The AWS Web Application Firewall (WAF) is a PCI DSS-validated automated technical solution that can help meet PCI DSS Requirement 6.6. The WAF service helps protect publicly-facing web sites that use Amazon CloudFront or Application Load Balancers from web-based attacks.

Requirement 6.6 can be met either with a WAF or web application security testing. Anitian always recommends that web application security testing be performed in conjunction with any WAF deployment, so that the WAF can be tuned to explicitly address any known vulnerabilities with the web application.

Anitian provides web application testing. Our Sherlock managed security solution also offers managed WAF.

## 3.7. Requirement 7: Restrict Access to Cardholder Data By Business Need To Know

The following AWS components can help support the access control requirements of PCI:

- AWS Identity and Access Management (IAM)
- AWS Directory Service
- AWS Cognito

### IAM

The IAM service is a fundamental component of any AWS environment, helping you control access to your AWS resources.  You can use the users, groups, and roles within IAM to build a role-based access control model to AWS.  IAM is also where you manage KMS encryption keys.

The service supports federated access, allowing you provide access to AWS resources to users from external systems.  IAM supports two different form of identity federation:

- **Web Identity Federation (OpenID Connect)**

  Using OpenID Connect, you can provide temporary, role-based access to perform specific tasks with AWS resources.  Users are identified and authenticated via a third party like Amazon, Google, or Apple.  For example, you could allow a mobile user to write to an AWS Simple Queue Service queue, an S3 bucket, or other service, without needing to manage individual IAM users for each person.

- **SAML 2.0 Federation**

  Integrating with a SAML 2.0 identity provider allows you to provide users from trusted systems access for to login to the AWS Management Console or call AWS APIs without needing IAM user accounts.  Existing users in your on-premise Active Directory or SSO solution can be delegated access to your AWS environment, using the credentials and processes they are familiar with.

Whether you use native IAM users, roles, and groups; OpenID Connect; your own Active Directory instance; or another SAML v2 provider; it is your responsibility to manage access rights within the IAM service.

NOTE: IAM is only used for identity and access management to AWS resources. It does not support managing access to operating systems and applications running on EC2 instances.

### AWS Directory Service

A collection of directory related services, AWS Directory Service allows you to host application and user directories in the cloud, including Microsoft Active Directory (AD) or AD-compatible directories.

- **Amazon Cloud Directory**

  A multi-tenant and highly scalable directory for application-specific objects. Cloud Directory is graph-based, and supports multiple schemas and different hierarchical views that allow pivoting to different organizational schemes. This directory is not really designed for federation or for migrating on-premise directories, but is a good selection for custom application uses.

- **Amazon Cognito**

  Technically a separate service, Cognito is designed to support mobile application identity and access management needs, and even supports federation via OpenID Connect and multi-factor authentication.

- **AWS Directory Service for Microsoft Active Directory (Enterprise Edition)**

  Also referred to as AWS Microsoft AD, this is a fully AWS-hosted AD forest. You can establish one- and two-way inter-forest trusts (including with on-premise forests), extend its schema, and even implement fine-grain password policies.

- **AD Connector**

  This a proxy service that forwards requests to your existing, on-premise AD infrastructure. Using the AD Connector allows you to use all your existing tools, Group Policy objects, and any other AD-integrated solutions with AWS.

- **Simple AD**

  Based on Samba 4, Simple AD is a Microsoft Active Directory compatible directory service. It can be used with IAM to control access to AWS resources, and supports all the common features of AD, including user accounts, groups, and even Group Policy.

NOTE: While these services can support role-based access control schemes, they do not all support the password, account lockout, and other settings necessary to meet Requirement 8. See the discussion in Section 3.8 below for further details.

### Other Strategies and Considerations

You will need to define, document, and implement the role-based access systems implemented with IAM and AWS Directory Service. This includes all the user roles that need access to CHD, all the users that hold those roles, the authorizations for all those users, and what permissions are necessary for those roles to carry out their tasks.

If you rely on non-IAM identity providers, including AWS Directory Services, make sure you include them in your documentation. This includes user roles that have Administrative access to those systems.

## 3.8. Requirement 8: Identify and Authenticate Access to System Components

The following AWS services can help support the account management requirements of PCI:

- AWS Identity and Access Management (IAM)
- AWS Directory Service
- AWS Cognito

### IAM

IAM supports password and account policies in accordance with Requirement 8.1 and 8.2, except for account lockouts for invalid login attempts (Req. 8.1.6), minimum lockout durations (Req. 8.1.7), and idle session timeouts (Req. 8.1.8).

Meeting PCI requirements with IAM requires using an additional identity provider that can enforce these requirements.

### Directory Service

Each AWS Directory Service directory supports can help identify and authorize users for your applications.  Most can even be used as identity providers with IAM. However, they all support different password and account policies.  Using these directory services with systems in your PCI assessment scope may require additional controls.

- **Amazon Cloud Directory**

  Cloud Directory is designed to store, manage, and provide access to application-specific objects.  It is not designed as an identity or access management system, and does not include these feature by default. Although such a system could employ Cloud Directory as its data store, you will have to build it from scratch.

- **Amazon Cognito**

  Like IAM, Cognito does not support password policy settings for for account lockouts for invalid login attempts (Req. 8.1.6), minimum lockout durations (Req. 8.1.7), and idle session timeouts (Req. 8.1.8).  Cognito also does not support password expiration (Req. 8.2.4) or settings to prevent users from reusing their last four passwords (Req. 8.2.5).

  Additional controls or logic within your mobile app will be necessary to meet Requirements 8.1 and 8.2, when relying on Cognito for user management.

  Cognito does support multi-factor authentication, and can help meet Requirement 8.3.1 if your mobile application supports administrative access.

- **AWS Directory Service for Microsoft Active Directory (Enterprise Edition)**

AWS Microsoft AD can help comply with Requirement 8 using fine-grained password policies. You will need to use standard Microsoft tools like the Active Directory Administrative Center to configure these policy settings. For more information, see the Manage Fine-Grained Password Policies in Microsoft AD.

- **AD Connector**

  Since AD connector connects to an on-premise AD environment, it allows you to leverage all the features and capabilities of a full Active Directory environment. This includes all the password and account Group Policy settings necessary to meet Requirement 8.

- **Simple AD**

  While Simple AD supports using standard AD tools to manage the system, it is Samba 4 based and you have limited control over password and account policies via Group Policy. You can create GPOs containing password and account lockout policy settings, but these will only apply to local accounts on domain members.

  Setting password and account lockout policies to meet Requirement 8 in Samba 4 requires the `samba-tool` utility. These settings are domain-wide, and must be set manually.

  Fine-grained password policies are not supported in Samba 4.

### Other Strategies and Considerations

It is the customer's responsibility to ensure that all password and account policies are configured to meet Requirement 8. This is true for IAM and AWS Directory Service, and for any directory you may setup to run on EC2 instances.

## 3.9. Requirement 9: Restrict Physical Access to Cardholder Data

AWS handles the physical security of all data centers and infrastructure for AWS services. If you host your entire PCI environment in AWS, then Requirement 9 are covered under AWS's Service Provider AOC.

AWS's AOC does not cover any in-scope assets hosted outside of AWS. Nor does it cover the handling of media that may contain CHD you download, transfer, or backup to locations outside of AWS.

### Other Strategies and Considerations

The AWS Snowball and Storage Gateway services rely on physical or virtual on-premise devices (media) to transfer large amounts of data into or out of AWS. These services are not covered under AWS's AOC; if you use one, you will be responsible for Requirements 9.5-9.8 related to the use of the service.

## 3.10. Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

The following AWS services can help support the log management requirements of PCI:

- AWS CloudTrail
- S3

### CloudTrail

The AWS CloudTrail service can assist with tracking and monitoring access to resources within an AWS account. The primary components supported by CloudTrail are log aggregation, alerting, and retention (Req. 10.5 to 10.7).

It is your responsibility to create an S3 bucket to receive and store the log files, and ensure that Cloud Trail is enabled to capture the required security events (Req. 10.2).

The CloudTrail Event Record Body supports all specific elements in Requirement 10.3; for further information, see the Event Reference Record.

### S3

Retention policies for CloudTrail data are configured in S3. By default, the retention period is infinite, but is fully configurable (see Lifecycle Configuration).

NOTE: For a cost-effective way to comply with Requirement 10.7, you can use S3 Lifecycle Configuration to set the retention period to 90 days and automatically archive older data to the Amazon Glacier storage service for long-term retention (required to be at least one year).

Additionally, you must enable access control on the S3 bucket storing the CloudTrail logs. This must include limiting bucket write access to CloudTrail and bucket read access to authorized users.

### Other Strategies and Considerations

Amazon's CloudTrail is a basic logging service that can fulfill the PCI requirements for logging. While CloudTrail provides audit logging for access to AWS resources, it does not log events and activity for the applications you run on AWS.

There are several Security Information and Event Management (SIEM) solutions available in the AWS Marketplace. Anitian's managed security platform, Sherlock, offers managed SIEM that is fully PCI compliant.

If you have an on-premise SIEM product, CloudTrail supports an API that your SIEM product may be able to use to collect its logs. Check with your SIEM vendor for additional information.

You must configure EC2 instances for network time protocol (NTP) to comply with Requirement 10.4.

## 3.11. Requirement 11: Regularly Test Security Systems and Processes

AWS's AOC fully covers detection of rogue wireless access points (Req. 11.1).

AWS does not provide vulnerability scanning, (Req. 11.2), penetration testing (Req. 11.3), intrusion prevention (Req. 11.4) or file change detection (Req. 11.5) within EC2 instances.  However, there are numerous solutions in the AWS marketplace supporting many of these requirements.

Anitian and our AWS managed security platform Sherlock provides these services.

NOTE: Penetration testing must be scheduled and approved through AWS.  See AWS Penetration Testing for further details

## 3.12. Requirement 12: Maintain a Policy That Addresses Information Security For All Personnel

AWS does not provide any of the policy documentation as defined in Requirement 12 (and other PCI requirements).  You will need to write this material on your own.

Anitian can help write these policies for you.

## 3.13. Appendix A.1:  Shared Hosting Providers Must Protect the Cardholder Data Environment

If you provide shared hosting as part of your EC2 instances, you are fully responsible for protecting your customers' CHD.  You will need to segment and isolate the CDE correctly to comply with Requirement A.1.  The following services can assist with this:

- Requirement 1 – VPCs, Security Groups
- Requirements 7 and 8 – IAM and Directory Service

## 3.14. Appendix A.2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections

This specific appendix to the PCI DSS is not relevant to AWS. This applies to terminals in use on-premise and the support of TLSv1.0.

However, for all in-scope services, AWS maintains TLS 1.1 or greater for customer's PCI workloads. AWS does provide a TLSv1.0 policy for customers with non-PCI workloads. Make sure you always use TLSv1.1 or greater for PCI compliance.

## 3.15. Appendix A.3: Designated Entities Supplemental Validation (DESV)

For some organizations, a card brand or acquirer may require that an entity is a Designated Entity, and therefore has to meet the additional requirements in PCI DSS 3.2 Appendix A.3.

NOTE: Becoming a Designated Entity is a formal process, so if you have not had this mandated by a card brand or Acquirer, it does not apply.

The basic guidelines for being declared a Designated Entities are entities that:

- Handle large volumes of CHD
- Aggregate CHD from multiple places or other companies
- Have had multiple or significant CHD breaches

The additional requirements for Designated Entities generally concern formalizing one’s PCI compliance program. The components of AWS supporting the various sub-requirements of A.3 are discussed below.

### 3.15.1. DE.1 Implement a PCI DSS compliance program.

AWS does not provide any of the policy or procedure documentation as defined in DE.1 (and other PCI requirements). You will need to write this material on your own.

### 3.15.2. DE.2 Document and validate PCI DSS scope.

There are no AWS services that directly address the DE.2 requirements for validating PCI DSS scope, that the scope is accurate based on segmentation control testing and CHD discovery processes, and that it remains valid following organizational and technical changes.

However, there are some AWS services, like those noted in Section 3 above, that can help supply information in efforts to meet this additional validation requirement. For example:

- AWS Config can identify changes to AWS components, helping to determine if the AWS-hosted CDE network or segmentation has changed.

- S3 supports programmatic and command-line access to stored objects, assisting in CHD discovery efforts.
- CloudTrail and CloudWatch can be used to detect changes to the environment that may affect your assessment scope or state of compliance.
- IAM can be used to assign read-only access to AWS components, allowing Governance, Risk, and Compliance (GRC) solutions or personnel to gather evidence.

NOTE: Don't forget: penetration testing, even to test segmentation, must be scheduled and approved through AWS. See AWS Penetration Testing for further details.

### 3.15.3. DE.3 Validate PCI DSS is incorporated into business-as-usual (BAU) activities.

Specific AWS services are assessed annually against the current PCI DSS version. Those AWS services that are covered in the AWS assessment scope are documented in AWS's Service Provider AOC. As mentioned above in Section 2, AWS customers may request a copy of that AOC (with a signed non-disclosure agreement).

Consulting AWS's AOC and the AWS PCI DSS "Responsibility Matrix" will help you determine if all the technologies used in your CDE have been, currently are, and will continue to meet the applicable PCI requirements.

### 3.15.4. DE.4 Control and manage logical access to the cardholder data environment.

Like for DE.2 above, there are no AWS services that directly address the semi-annual access reviews DE.4 requires. However, there are some AWS services, like those noted in Section 3, that can help supply information in efforts to meet this additional validation requirement. For example:

#### IAM

IAM to inventory assigned access policies and determine what access users and groups have to AWS resources that are in the assessment scope.

NOTE: While access to most AWS resources is controlled via IAM policies, access can be directly assigned in some instances. S3, for example, can have bucket access policies that are difficult to enumerate per-user.

#### AWS Directory Service

If you use any AWS Directory Service for identity and access management within your environment, access to the service itself within AWS will also need to be documented and reviewed at least every six months.

### 3.15.5. DE.5 Identify and respond to suspicious events.

AWS does not provide incident detection, response, or analysis methodologies as required in DE.5 (and other PCI requirements). You will need to write this material on your own.

However, CloudTrail, CloudWatch, and Config can be used to detect suspicious events or unexpected configuration changes, in support of an incident response program.

# 4. REFERENCE ARCHITECTURES

This section defines three common AWS reference architectures to help you build or assess a PCI-compliant environment.

1. **Dedicated**: An AWS PCI environment that is not connected to anything else.
2. **Segmented**: A CDE and in-scope systems within a larger AWS environment.
3. **Connected**: An environment that has both AWS and on-premise items.

These reference architectures use Microsoft Windows platforms for the web and application tiers, and Amazon RDS for the database tier.  While other OS platforms may have slightly different configurations, the architectures are generally the same.

NOTE: Determining the scope of compliance in an AWS hosted environment is largely the same as scoping an on-premise environment.  The scope of compliance is dependent upon the cardholder data flows and segmentation strategies in use.

## 4.1. Architecture 1: Dedicated

This architecture demonstrates an e-commerce website hosted in a dedicated Amazon AWS account and contained in a single, private network.

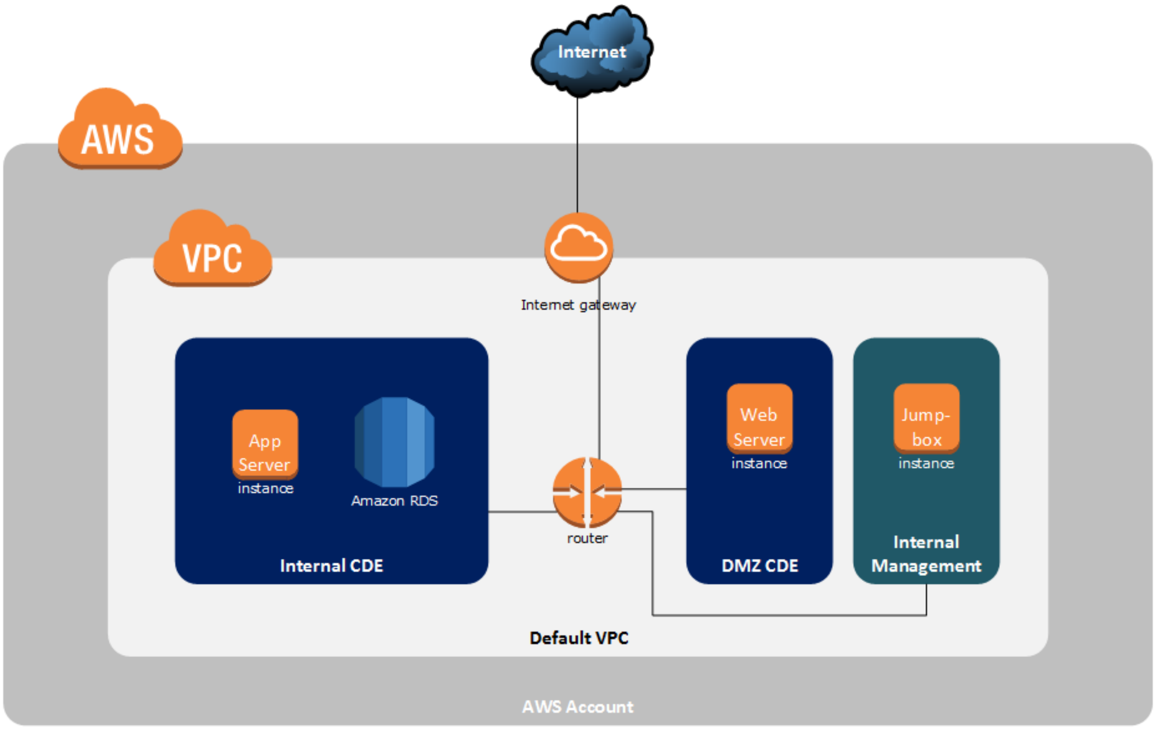


*Figure 6 - Stand-alone e-commerce website architecture*

### 4.1.1. Overview

In the Dedicated reference architecture, there are three subnets in the default VPC:

- DMZ CDE
- Internal CDE
- Internal Management

The DMZ is an Internet-facing network containing the web server EC2 instance.

The In-scope Internal subnet contains a Jumpbox used to manage and provide support, security, patching, and other required services to the CDE Instances.

The Internal subnet is only accessible by the DMZ and in-scope instances via Security Groups (described in detail below), and contains an application server instance and RDS.

NOTE: Anitian has created a CloudFormation script using hardened AMIs for implementing the reference architectures.

### 4.1.2. PCI Scope

The CDE is comprised of the systems in the two CDE subnets:

- Web Server
- Application Server
- RDS DB instance

For this scope, the web server accepts CHD, which then flows through the application tier to the DB for storage.

The Jumpbox does not transmit, process, store, or otherwise handle cardholder data in this architecture.  Placing the jumpbox in a dedicated management network segregates it from the CDE but does not remove it from the PCI assessment scope. This happens because it directly connects to and can impact the security of hosts in the CDE.

### 4.1.3. Applicable AWS Services

The following AWS services help support compliance with PCI 3.2 requirements for this architecture:

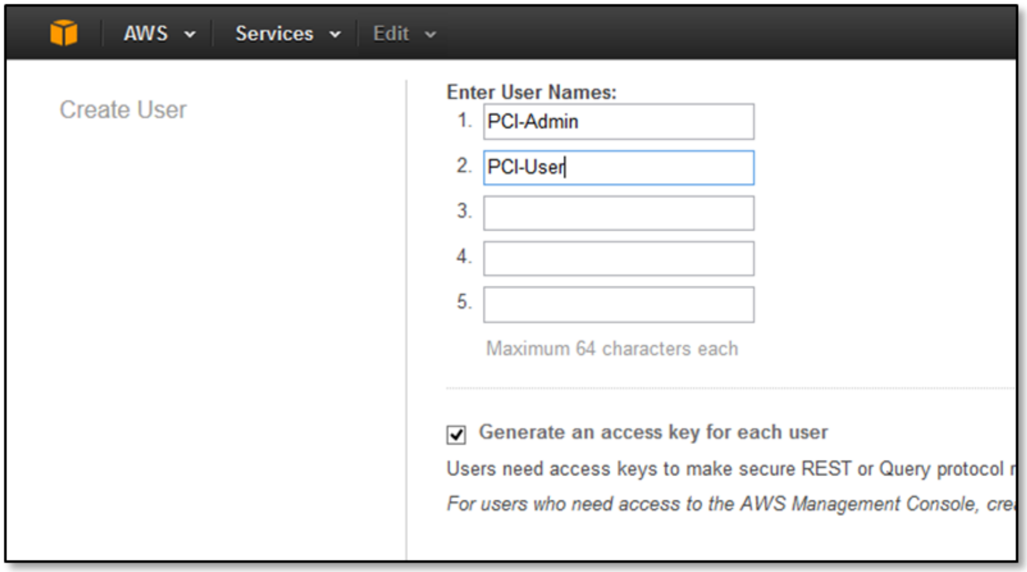
| AWS SERVICE | PCI REQUIREMENTS SUPPORTED |
|---|---|
| • IAM<br>• KMS | 2.2.4, 3.4, 3.5, 3.5.22-3, 3.6, 3.6.1-5, 3.6.7, 6.4.1-2, 7.1, 7.1.1-3, 7.2, 7.2.1-3, 8.1, 8.1.1-2, 8.2, 8.2.1, 8.2.3-6, 8.3, 8.3.1, A.1.2 |
| • S3 | 3.1, 3.4, 10.5, 10.5.1-5, 10.7 |
| • CloudTrail<br>• CloudWatch | 10.1, 10.2, 10.2.2-7, 10.3, 10.3.1-6, 10.5, 10.5.1-5, 10.7, A.1.3 |
| • EC2<br>• Security Groups<br>• AMIs<br>• EBS | 1.1, 1.1.4, 1.2, 1.2.1, 1.3, 1.3.1-7, 2.1,4.1, 6.4.1 |
| • RDS | 3.4 |
| • Config | 2.4, 11.5 |
| • VPC | 1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7 |

### 4.1.4. Build Out

This section describes the primary steps for building out the reference architecture.

#### 4.1.4.1. Create IAM Groups and Assign Permissions

First, define who can access and who can manage the environment.  AWS requires you to explicitly define all your accounts and passwords, which ensures there are no shared defaults.



Enter User Names:

1. PCI-Admin
2. PCI-User
3. 
4. 
5.

Maximum 64 characters each

☑ Generate an access key for each user

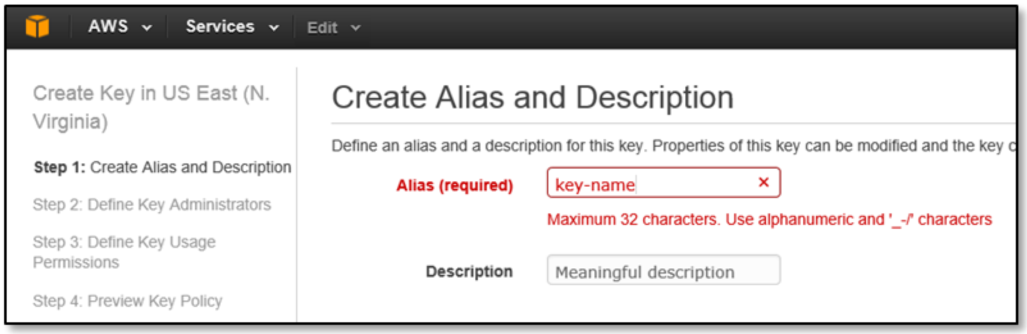
Users need access keys to make secure REST or Query protocol r

*For users who need access to the AWS Management Console, cre*

*Figure 7 – Create users*

### 4.1.4.2. Create Storage Encryption Keys

Use KMS to create keys for encrypting data storage locations. In this architecture, there will need to be at least one key created for the database instance that will contain cardholder data (CHD).


AWS
Services
Edit
Create Key in US East (N. Virginia)
Step 1: Create Alias and Description
Step 2: Define Key Administrators
Step 3: Define Key Usage Permissions
Step 4: Preview Key Policy

Create Alias and Description

Define an alias and a description for this key. Properties of this key can be modified and the key c

Alias (required): key-name

Maximum 32 characters. Use alphanumeric and '_-/' characters

Description: Meaningful description

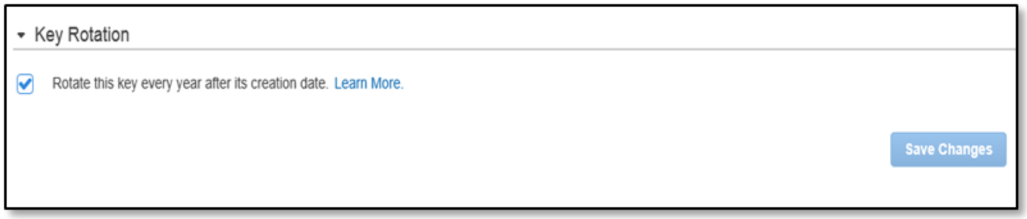
*Figure 8 – KMS configuration*

In AWS, you can separately assign permissions to manage an encryption key and use it for encryption, which allows for enforcing least-privilege.

NOTE: While non-root volumes attached to AWS instances can also be encrypted using KMS keys, the disk encryption is transparent to the operating system running in the instance. Management of access to the data on an encrypted disk is not separate and independent from the operating system, as required by PCI Requirement 3.4.1.

It is best practice, and a PCI requirement (Req. 3.6.4), to change encryption keys used to protect data on a regular basis. This limits how long a compromised key is usable.

After creating the key, click on its URL in the Encryption Keys section of the Identity and Access Management AWS service. The Key Rotation setting is in the listed properties for the selected key. This allows you to automate key rotation within a designated cryptoperiod in alignment with Requirement 3.6.4.



▾ Key Rotation

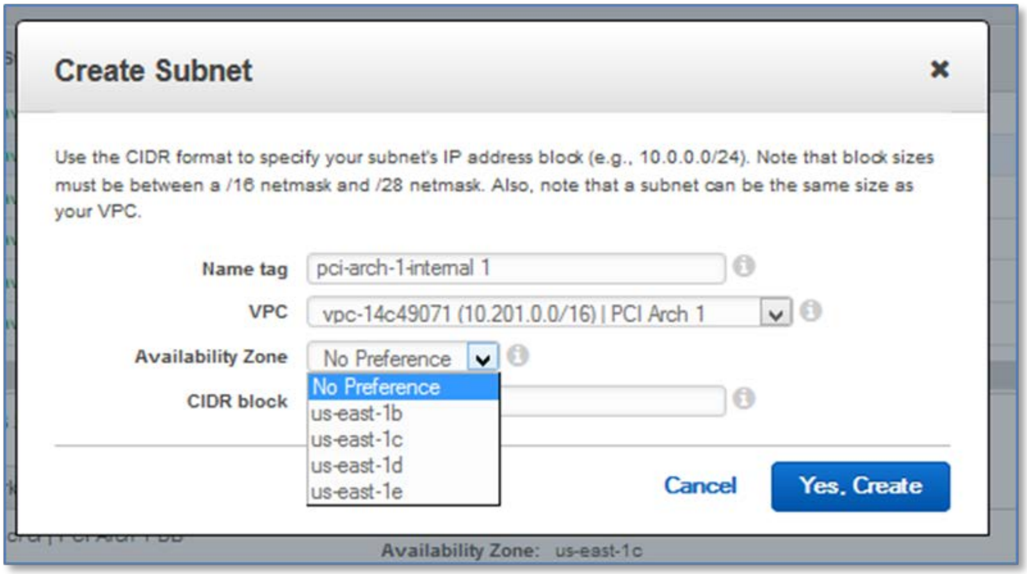
☑ Rotate this key every year after its creation date. Learn More.

*Figure 9 – Key rotation option*

### 4.1.4.3. Create Subnets

For this architecture, you need at least four separate subnets:

- A DMZ subnet for the web server.
- A management subnet for the Jumpbox.
- Two internal subnets for the application and database systems.
    - These internal subnets need be in different availability zones, so that we can setup RDS redundancy in a later step.



Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag: pci-arch-1-internal 1

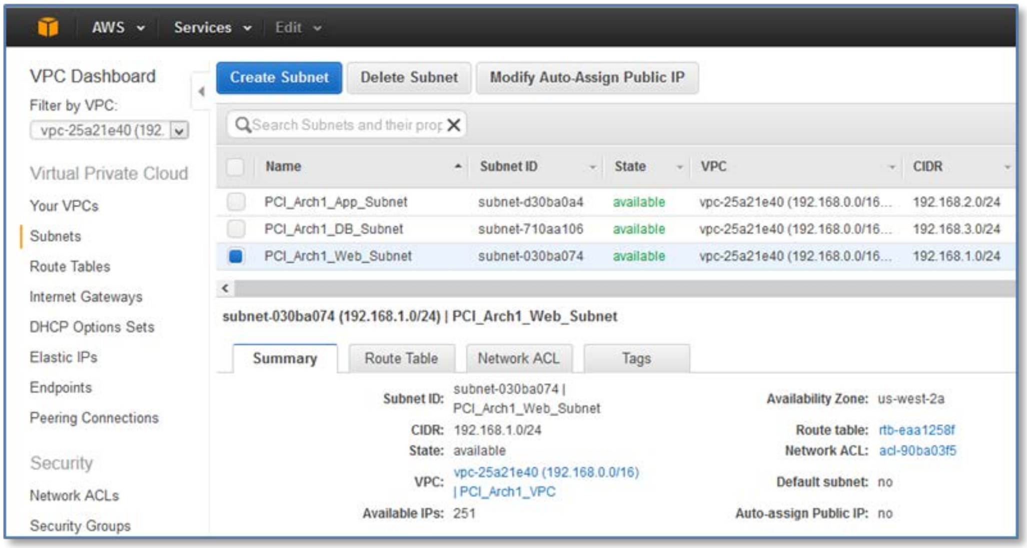
VPC: vpc-14c49071 (10.201.0.0/16) | PCI Arch 1

Availability Zone: No Preference

CIDR block:

*Figure 10 – Configuring a subnet*

Use the VPC service management page in the AWS console to configure subnets, even for the Default VPC EC2 Classic uses.



| | Name | Subnet ID | State | VPC | CIDR |
|---|---|---|---|---|---|
| □ | PCI_Arch1_App_Subnet | subnet-d30ba0a4 | available | vpc-25a21e40 (192.168.0.0/16... | 192.168.2.0/24 |
| □ | PCI_Arch1_DB_Subnet | subnet-710aa106 | available | vpc-25a21e40 (192.168.0.0/16... | 192.168.3.0/24 |
| ■ | PCI_Arch1_Web_Subnet | subnet-030ba074 | available | vpc-25a21e40 (192.168.0.0/16... | 192.168.1.0/24 |

subnet-030ba074 (192.168.1.0/24) | PCI_Arch1_Web_Subnet

Subnet ID: subnet-030ba074 | PCI_Arch1_Web_Subnet

CIDR: 192.168.1.0/24

State: available

VPC: vpc-25a21e40 (192.168.0.0/16) | PCI_Arch1_VPC

Available IPs: 251

Availability Zone: us-west-2a

Route table: rtb-eaa1258f

Network ACL: acl-90ba03f5

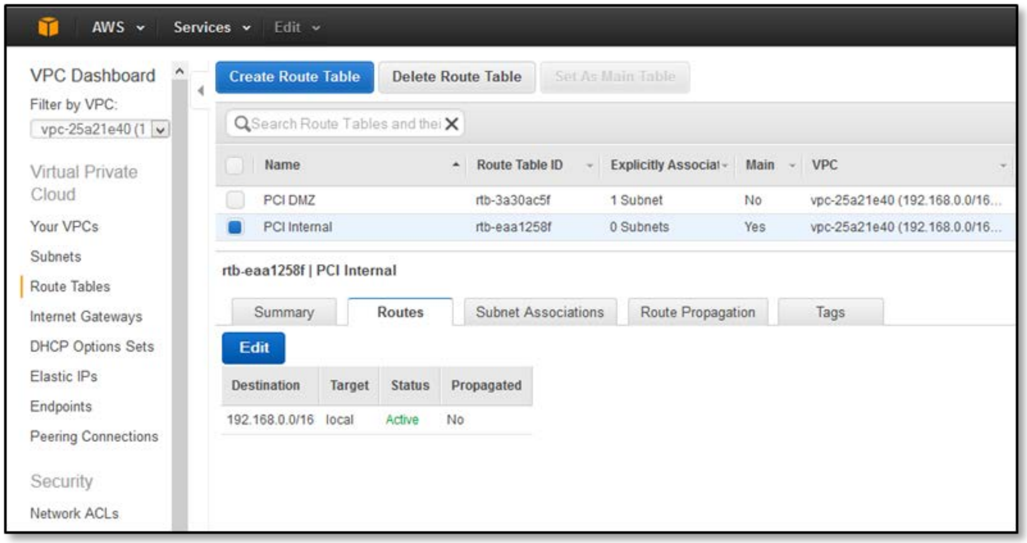
Default subnet: no

Auto-assign Public IP: no

*Figure 11 - VPC Service Management page with three new subnets*

### 4.1.4.4. Configure Routing

When creating a new subnet, it will use the main route table for the VPC that will include one route allowing internal traffic for that subnet only.



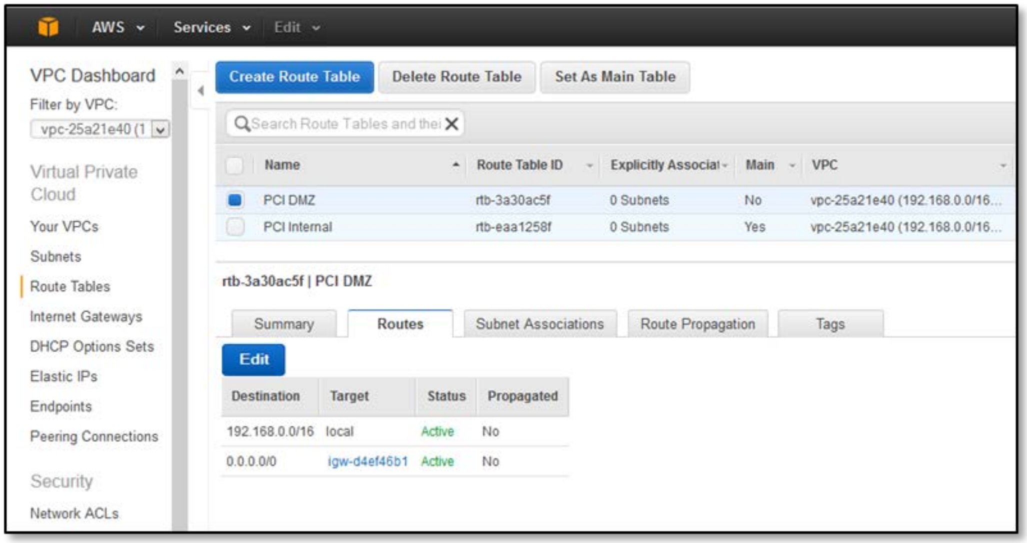
| | Name | Route Table ID | Explicitly Associat | Main | VPC |
|---|---|---|---|---|---|
| □ | PCI DMZ | rtb-3a30ac5f | 1 Subnet | No | vpc-25a21e40 (192.168.0.0/16... |
| ■ | PCI Internal | rtb-eaa1258f | 0 Subnets | Yes | vpc-25a21e40 (192.168.0.0/16... |

rtb-eaa1258f | PCI Internal

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local | Active | No |

*Figure 12 - Internal route*

Only the DMZ and Management subnets need to have routes to the Internet Gateway. This ensures only instances in these subnets support direct inbound or outbound Internet connections.



| | Name | Route Table ID | Explicitly Associat | Main | VPC |
|---|---|---|---|---|---|
| ■ | PCI DMZ | rtb-3a30ac5f | 0 Subnets | No | vpc-25a21e40 (192.168.0.0/16... |
| □ | PCI Internal | rtb-eaa1258f | 0 Subnets | Yes | vpc-25a21e40 (192.168.0.0/16... |

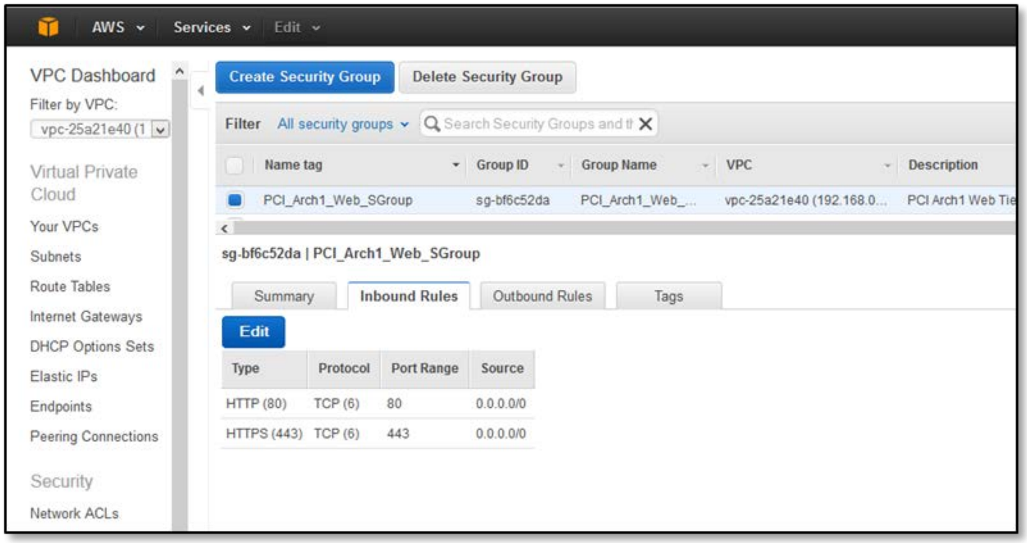
rtb-3a30ac5f | PCI DMZ

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local | Active | No |
| 0.0.0.0/0 | igw-d4ef46b1 | Active | No |

*Figure 13 - Gateway route for DMZ*

### 4.1.4.5. Create Security Groups

Security groups function like inbound firewalls. They restrict incoming instance network access to predefined sources, IP protocols, and TCP or UDP ports.



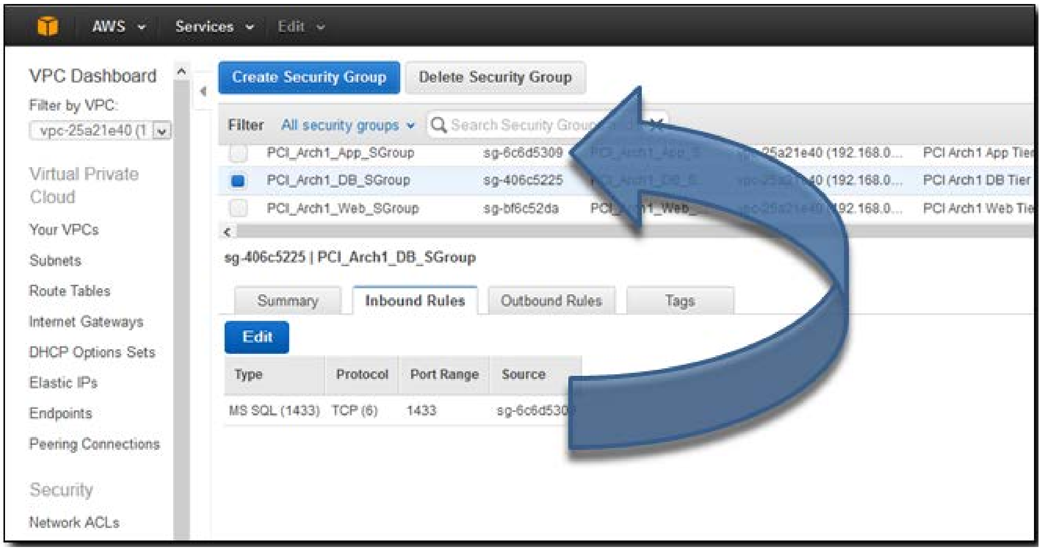
| Name tag | Group ID | Group Name | VPC | Description |
|---|---|---|---|---|
| PCI_Arch1_Web_SGroup | sg-bf6c52da | PCI_Arch1_Web_... | vpc-25a21e40 (192.168.0.... | PCI Arch1 Web Tie |

sg-bf6c52da | PCI_Arch1_Web_SGroup

| Type | Protocol | Port Range | Source |
|---|---|---|---|
| HTTP (80) | TCP (6) | 80 | 0.0.0.0/0 |
| HTTPS (443) | TCP (6) | 443 | 0.0.0.0/0 |

*Figure 14 - Security Group Rules*

They can also reference other Security Group(s) in the same VPC as allowed sources. For example, you can reference the application servers Security Group to restrict access to a Microsoft SQL Server to only instances in that group.



| Name tag | Group ID | Group Name | VPC | Description |
|---|---|---|---|---|
| PCI_Arch1_App_SGroup | sg-6c6d5309 | PCI_Arch1_App_S | vpc-25a21e40 (192.168.0.... | PCI Arch1 App Tier |
| PCI_Arch1_DB_SGroup | sg-406c5225 | PCI_Arch1_DB_S | vpc-25a21e40 (192.168.0.... | PCI Arch1 DB Tier |
| PCI_Arch1_Web_SGroup | sg-bf6c52da | PCI_Arch1_Web_ | vpc-25a21e40 (192.168.0.... | PCI Arch1 Web Tie |

sg-406c5225 | PCI_Arch1_DB_SGroup

| Type | Protocol | Port Range | Source |
|---|---|---|---|
| MS SQL (1433) | TCP (6) | 1433 | sg-6c6d530 |

*Figure 15 - Security Groups are stateful and block all access not explicitly allowed*

This architecture uses five Security Groups to accomplish the architecture depicted:

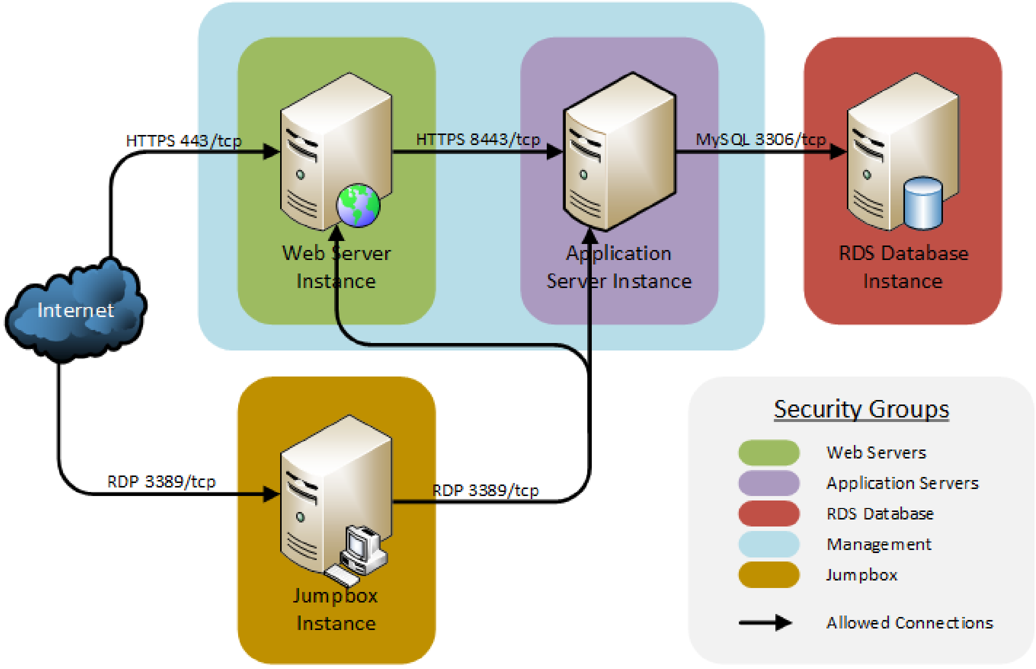
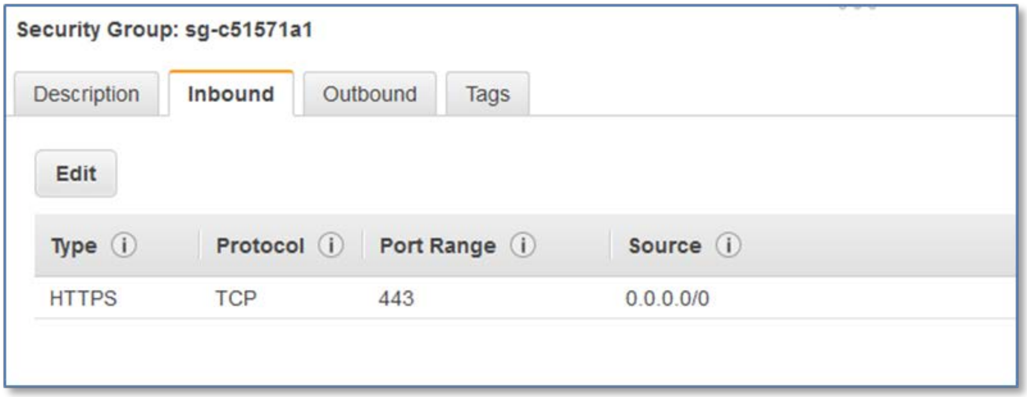


*Figure 16 - Logical Firewall / Security Group Design*

## Web Server Security Group

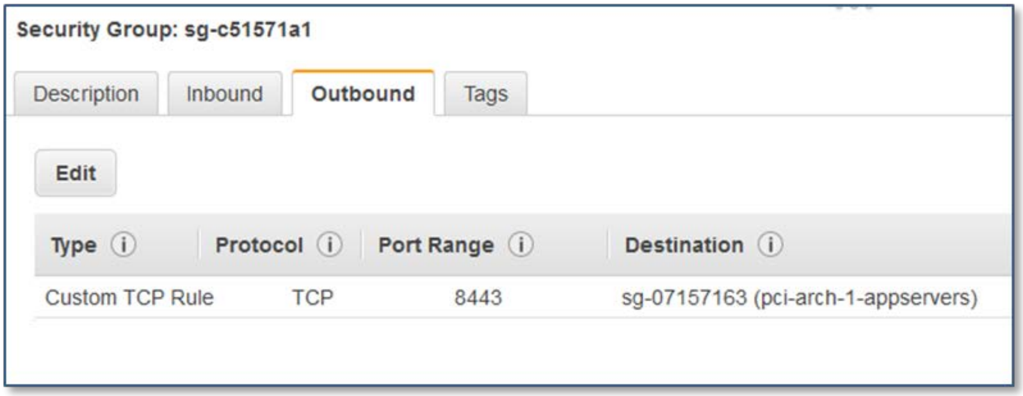
This group allows inbound web client connections from anywhere and outbound web services connections to internal application servers.



**Security Group: sg-c51571a1**

| Type | Protocol | Port Range | Source |
|---|---|---|---|
| HTTPS | TCP | 443 | 0.0.0.0/0 |

*Figure 17 - Web Server Security Group Inbound Rules*



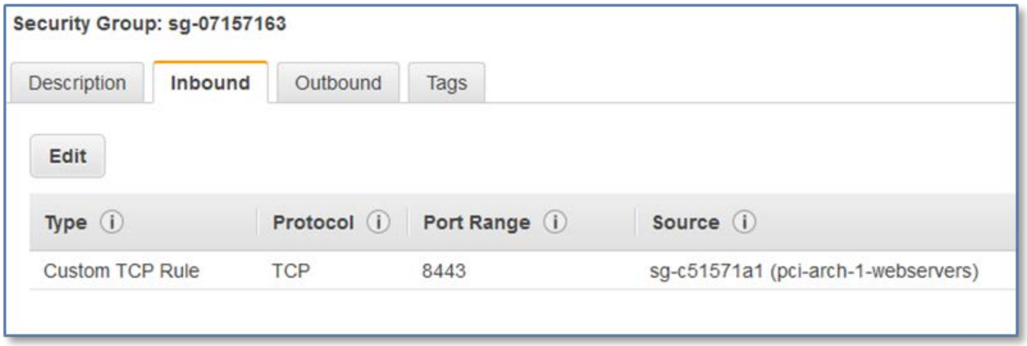
Security Group: sg-c51571a1

| Type | Protocol | Port Range | Destination |
|---|---|---|---|
| Custom TCP Rule | TCP | 8443 | sg-07157163 (pci-arch-1-appservers) |

*Figure 18 - Web Server Security Group Outbound Rules*

## Application Server Security Group

This Security Group allows incoming web service connections from the web servers to the application servers.

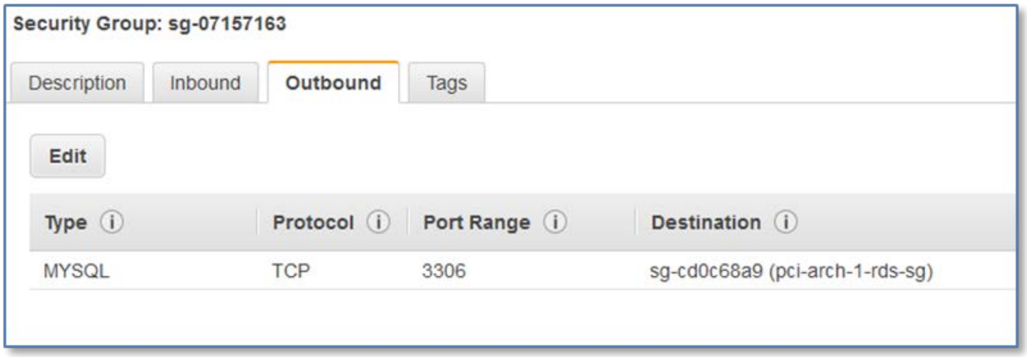


Security Group: sg-07157163

| Type | Protocol | Port Range | Source |
|---|---|---|---|
| Custom TCP Rule | TCP | 8443 | sg-c51571a1 (pci-arch-1-webservers) |

*Figure 19 - App Server Security Group Inbound Rules*

The group allows outbound MySQL connections to the RDS database instances.



Security Group: sg-07157163

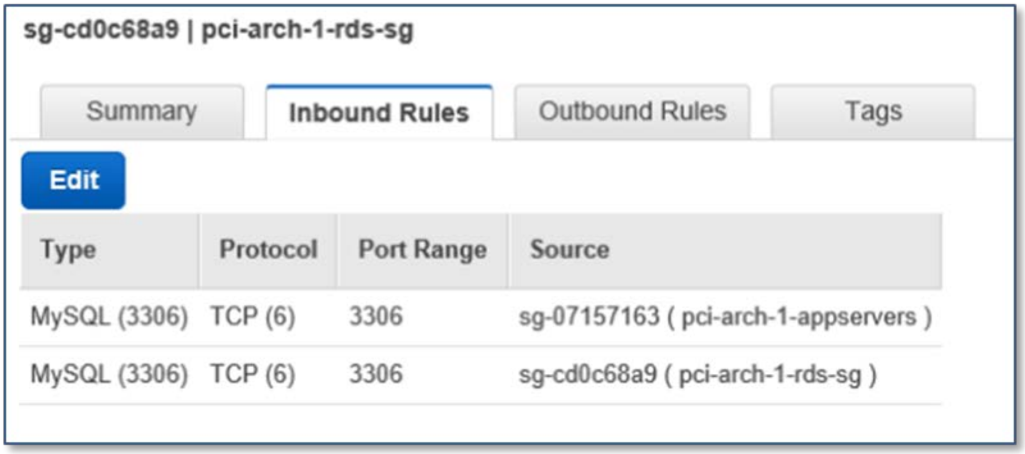
| Type | Protocol | Port Range | Destination |
|---|---|---|---|
| MYSQL | TCP | 3306 | sg-cd0c68a9 (pci-arch-1-rds-sg) |

*Figure 20 - Application server security group outbound rules*

## Database (RDS) Security Group

Security Groups can secure network access to RDS instances, although RDS only uses the inbound rules.

These rules allow MySQL connections from the application servers and from other RDS instances in the group to support database replication.



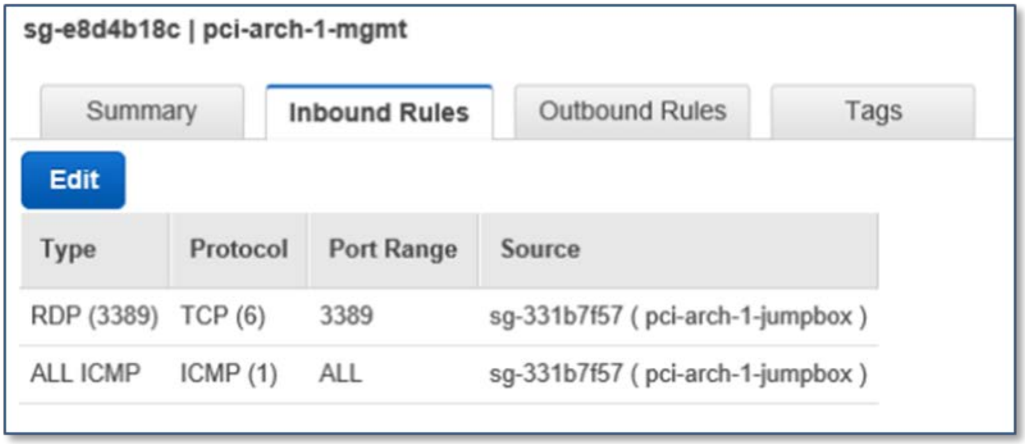
**sg-cd0c68a9 | pci-arch-1-rds-sg**

| Type | Protocol | Port Range | Source |
|---|---|---|---|
| MySQL (3306) | TCP (6) | 3306 | sg-07157163 ( pci-arch-1-appservers ) |
| MySQL (3306) | TCP (6) | 3306 | sg-cd0c68a9 ( pci-arch-1-rds-sg ) |

*Figure 21 - DB Server Security Group Inbound Rules*

### Management Security Group

The Management Security Group is a special group that allows RDP and ICMP connections from the Jumpbox to all instances for management purposes.



**sg-e8d4b18c | pci-arch-1-mgmt**

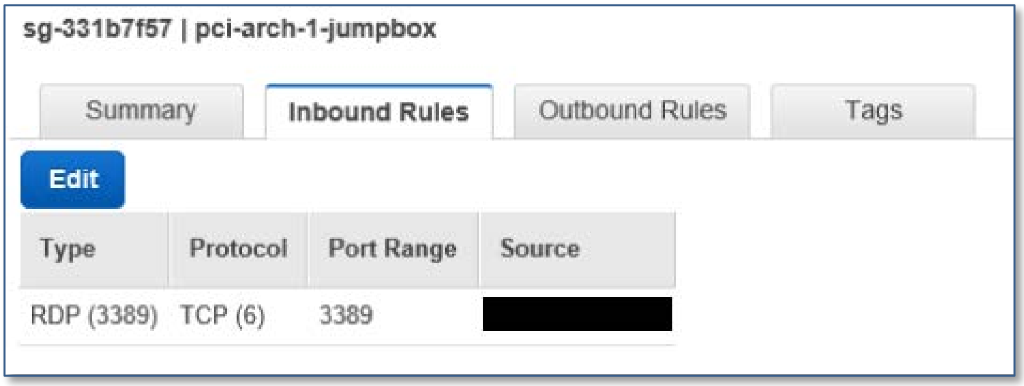
| Type | Protocol | Port Range | Source |
|---|---|---|---|
| RDP (3389) | TCP (6) | 3389 | sg-331b7f57 ( pci-arch-1-jumpbox ) |
| ALL ICMP | ICMP (1) | ALL | sg-331b7f57 ( pci-arch-1-jumpbox ) |

*Figure 22 - Management Server Security Group Inbound Rules*

### Jump Box Security Group

The Jumpbox itself only needs to allow connections from the public IP address of your company's network.

NOTE: You must implement two-factor authentication for remote access to meet Requirement 8.3. There are numerous third-party products that can support this for a Windows or Linux system. AWS does not natively support two-factor authentication for remote access to EC2 instances. However, AWS does support multi-factor authentication to AWS itself. For more information, see AWS MFA details and pricing at http://aws.amazon.com/iam/details/mfa/.

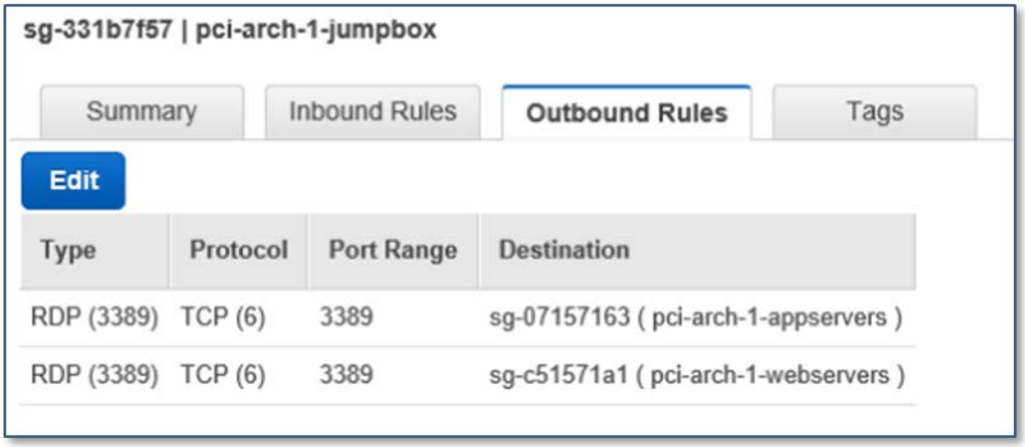


sg-331b7f57 | pci-arch-1-jumpbox

| Type | Protocol | Port Range | Source |
|---|---|---|---|
| RDP (3389) | TCP (6) | 3389 | [redacted] |

*Figure 23 - Jumpbox Server Security Group Inbound Rules*

The Jumpbox will need outbound communication to the web and application servers for management purposes.



sg-331b7f57 | pci-arch-1-jumpbox

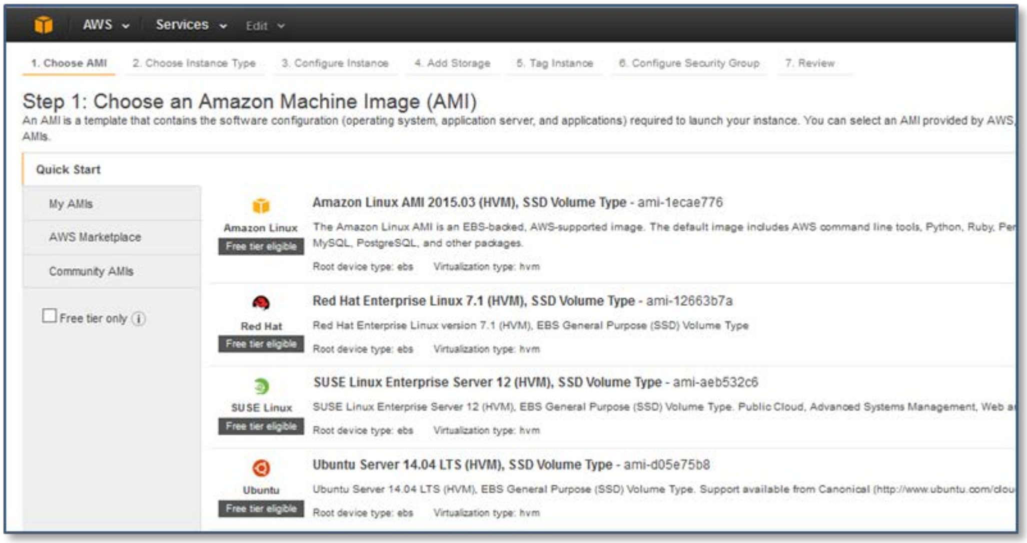
| Type | Protocol | Port Range | Destination |
|---|---|---|---|
| RDP (3389) | TCP (6) | 3389 | sg-07157163 ( pci-arch-1-appservers ) |
| RDP (3389) | TCP (6) | 3389 | sg-c51571a1 ( pci-arch-1-webservers ) |

*Figure 24 - Jumpbox Server Security Group Outbound Rules*

### 4.1.4.6. Create Hardened AMIs from secured instances

PCI requires the development of secure configuration standards for all system components. AWS allows development of one secure instance that will serve as a template for the creation of pre-secured systems.

Launch a new instance for each of the types needed for deployment. For this architecture, a web server, an application server, and an application or base server instance for the Jumpbox are required (the database will use the AWS RDS service).



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, AMIs.

**Amazon Linux AMI 2015.03 (HVM), SSD Volume Type** - ami-1ecae776

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Per MySQL, PostgreSQL, and other packages.

Root device type: ebs Virtualization type: hvm

**Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type** - ami-12663b7a

Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm

**SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type** - ami-aeb532c6

SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web a

Root device type: ebs Virtualization type: hvm

**Ubuntu Server 14.04 LTS (HVM), SSD Volume Type** - ami-d05e75b8

Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/clou

Root device type: ebs Virtualization type: hvm

*Figure 25 - Choosing AMI for deploying instances*

These instances will only exist long enough to perform host hardening and configuration steps. Make sure each of these instances are part of the Jumpbox Security Group, are in the Management subnet, and have an Elastic IP or Public IP so that you can remotely connect to and manage them.

Public IPs are provisioned by AWS when an instance is launched. This is automatic in the Default VPC but configurable by subnet in other VPCs (see the Amazon VPC User Guide for further information).

Elastic IPs (EIPs) are managed by a customer and associated with the AWS account not a specific instance. You can reassign which instance uses a specific EIP without the address changing.

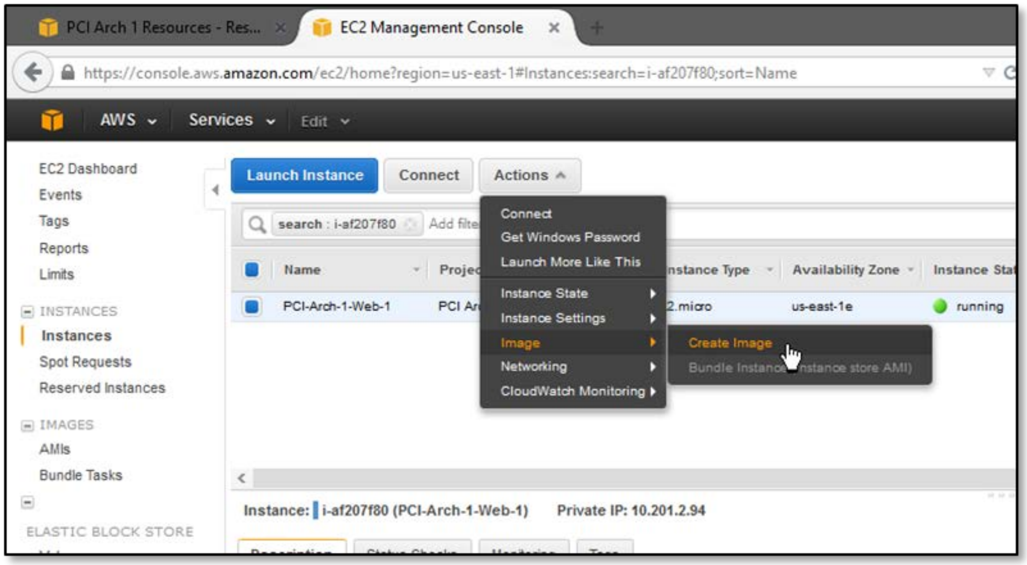
Connect to and harden your instance. Make sure you document all steps taken to secure the instance because your assessor will need to review these.

---

NOTE: Alternately, you can use Anitian's pre-hardened AMIs, which include a security configuration standard document. These are available in the AWS Marketplace.

---

Once you are finished and the instance is ready, power it off and create a custom AMI from it.



| Name | Projec | nstance Type | Availability Zone | Instance Stat |
|---|---|---|---|---|
| PCI-Arch-1-Web-1 | PCI Ar | 2.micro | us-east-1e | running |

Instance: i-af207f80 (PCI-Arch-1-Web-1) Private IP: 10.201.2.94

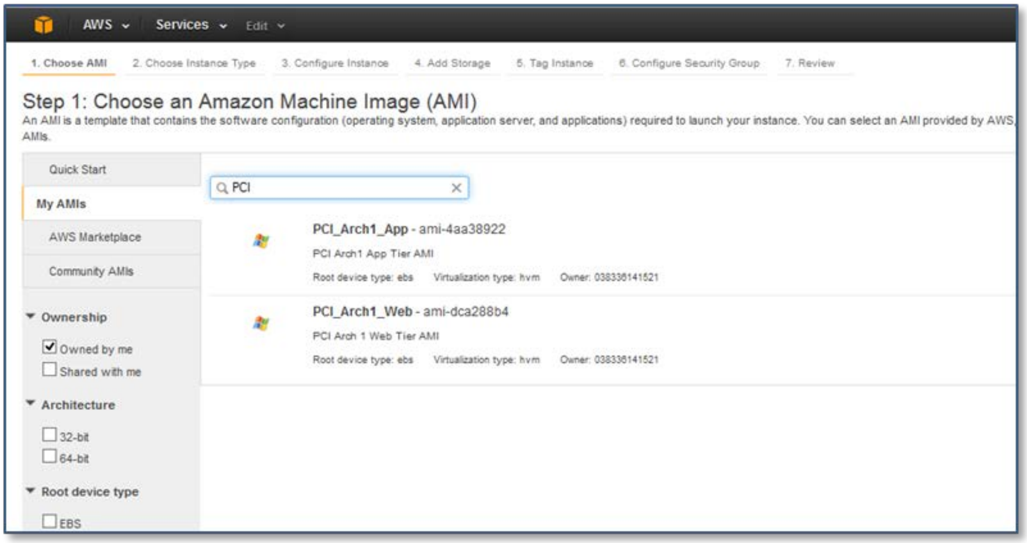
*Figure 26 - Creating AMI from hardened instance*

### 4.1.4.7. Launch Instances from Hardened AMI

This architecture needs a minimum of three instances:

- Jumpbox instance
  - Used to manage the environment remotely.
  - In the Management subnet, it will need an EIP or a public IP.
- Web server instance
  - Front-end to the e-commerce application.
  - In the DMZ subnet it will need an EIP or a public IP.
- Application server instance
  - App tier running middleware that brokers connectivity between web servers and DB (RDS in this example).
  - In the internal subnet,  the instanceis only accessible by the web server and Jumpbox and  the only one with access to the DB.

Launch the EC2 instances from the newly created AMIs.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, AMIs.

PCI

PCI_Arch1_App - ami-4aa38922
PCI Arch1 App Tier AMI
Root device type: ebs Virtualization type: hvm Owner: 038336141521

PCI_Arch1_Web - ami-dca288b4
PCI Arch 1 Web Tier AMI
Root device type: ebs Virtualization type: hvm Owner: 038336141521

Ownership
☑ Owned by me
☐ Shared with me

Architecture
☐ 32-bit
☐ 64-bit

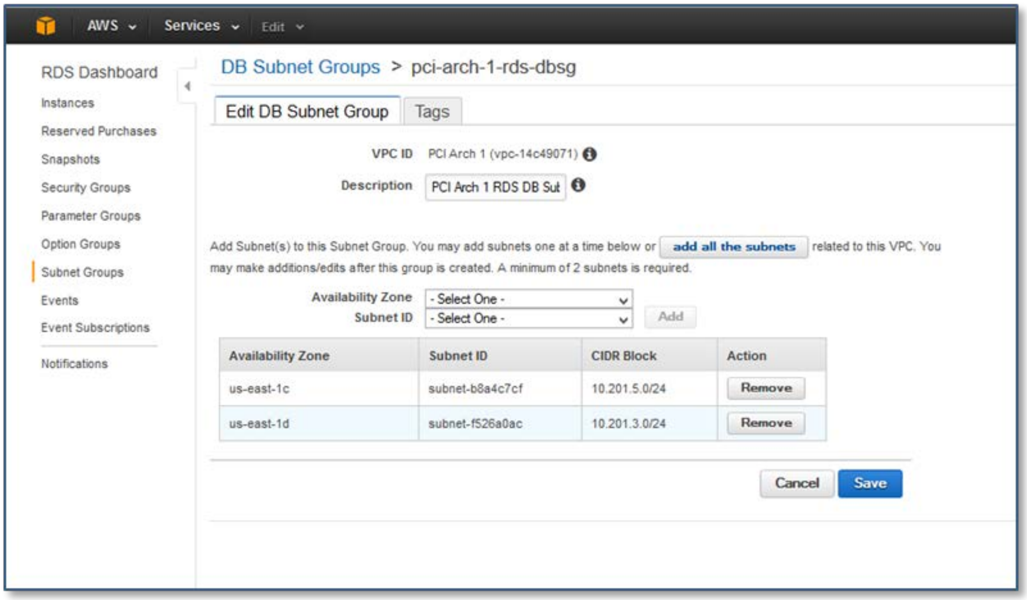
Root device type
☐ EBS

*Figure 27 - Launching instances from AMIs*

### 4.1.4.8. Create Subnet Group

Subnet Groups allow RDS to determine where redundant instances need to be located to survive the failure of the primary instance.

Manage Subnet Groups from the RDS service management page.  Create one that contains the two Internal CDE subnets created earlier.



VPC ID PCI Arch 1 (vpc-14c49071)

Description PCI Arch 1 RDS DB Sut

Add Subnet(s) to this Subnet Group. You may add subnets one at a time below or add all the subnets related to this VPC. You may make additions/edits after this group is created. A minimum of 2 subnets is required.

Availability Zone - Select One -
Subnet ID - Select One -

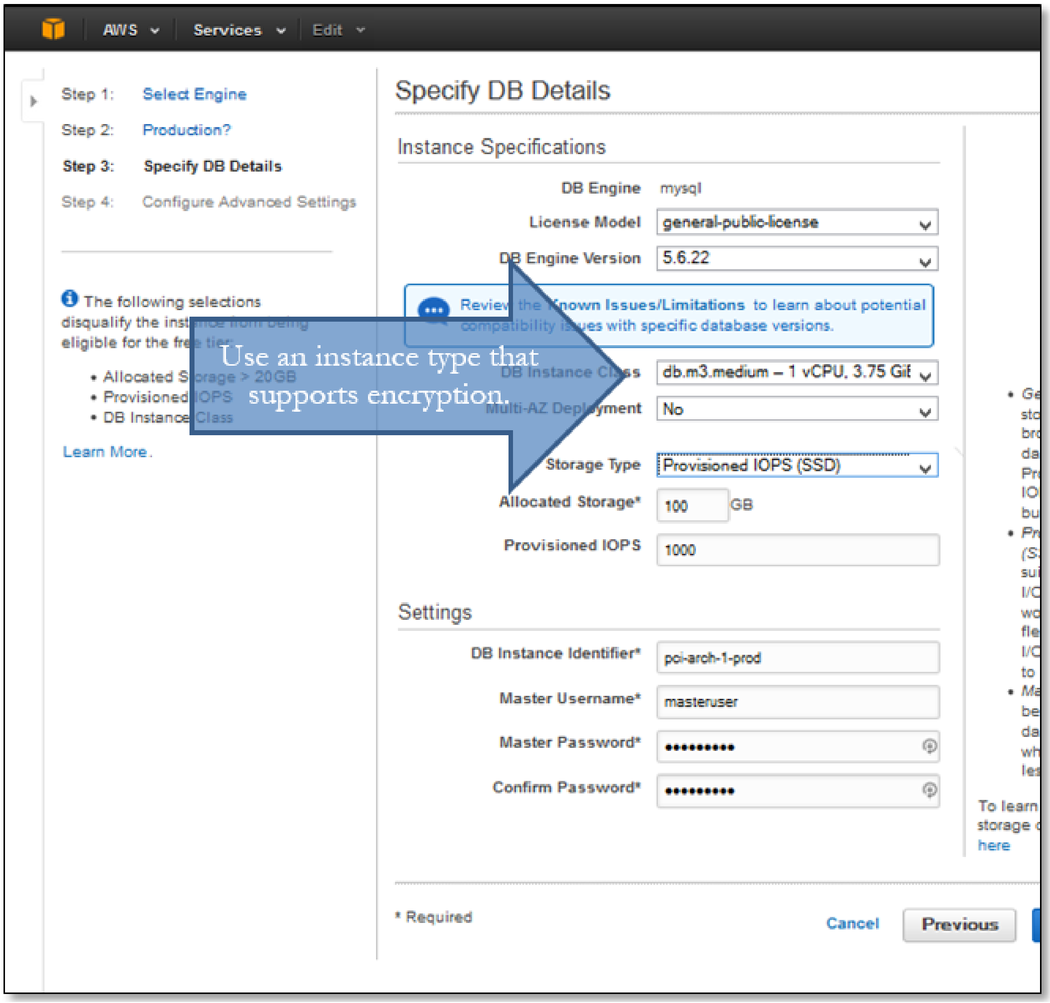
| Availability Zone | Subnet ID | CIDR Block | Action |
|---|---|---|---|
| us-east-1c | subnet-b8a4c7cf | 10.201.5.0/24 | Remove |
| us-east-1d | subnet-f526a0ac | 10.201.3.0/24 | Remove |

*Figure 28 - Creating RDS subnets*

### 4.1.4.9. Create Encrypted RDS Instance

Using the KMS key and Subnet Group already created, launch the encrypted RDS instance that will store CHD.

When creating the RDS instance, a few settings need special attention to meet PCI requirements. The DB instance Class needs to be db.m3.medium or higher to support encryption.



Use an instance type that supports encryption.

The following selections disqualify the instance from being eligible for the free tier:

- Allocated Storage > 20GB
- Provisioned IOPS
- DB Instance Class

Specify DB Details

Instance Specifications

| | |
|---|---|
| DB Engine | mysql |
| License Model | general-public-license |
| DB Engine Version | 5.6.22 |

Review the Known Issues/Limitations to learn about potential compatibility issues with specific database versions.

| | |
|---|---|
| DB Instance Class | db.m3.medium – 1 vCPU, 3.75 GiE |
| Multi-AZ Deployment | No |
| Storage Type | Provisioned IOPS (SSD) |
| Allocated Storage* | 100 GB |
| Provisioned IOPS | 1000 |

Settings

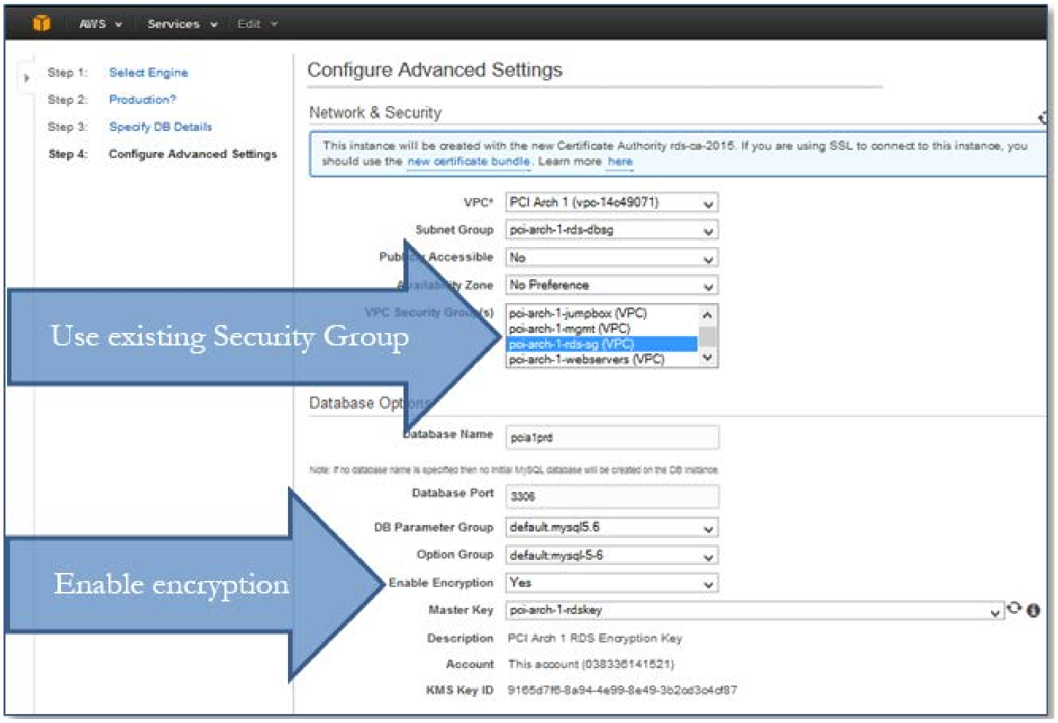
| | |
|---|---|
| DB Instance Identifier* | pci-arch-1-prod |
| Master Username* | masteruser |
| Master Password* | •••••••••• |
| Confirm Password* | •••••••••• |

* Required

*Figure 29 - Selecting instance class that supports encryption*

Additionally, ensure that you:

- Select the RDS Security Group created earlier to ensure AWS does not create a new “default” Security Group.
- Select “Yes” for Enable Encryption and choose the KMS key created earlier.



Step 1: Select Engine
Step 2: Production?
Step 3: Specify DB Details
Step 4: Configure Advanced Settings

Configure Advanced Settings

Network & Security

This instance will be created with the new Certificate Authority rds-ca-2015. If you are using SSL to connect to this instance, you should use the new certificate bundle. Learn more here

VPC*: PCI Arch 1 (vpc-14c49071)
Subnet Group: pci-arch-1-rds-dbsg
Publicly Accessible: No
Availability Zone: No Preference
VPC Security Group(s): pci-arch-1-jumpbox (VPC), pci-arch-1-mgmt (VPC), pci-arch-1-rds-sg (VPC), pci-arch-1-webservers (VPC)

Database Options

Database Name: pcia1prd

Note: If no database name is specified then no initial MySQL database will be created on the DB instance.

Database Port: 3306
DB Parameter Group: default.mysql5.6
Option Group: default:mysql-5-6
Enable Encryption: Yes
Master Key: pci-arch-1-rdskey
Description: PCI Arch 1 RDS Encryption Key
Account: This account (038336141521)
KMS Key ID: 9165d7f6-8a94-4e99-8e49-3b2ed3c4df87

*Figure 30 - Selecting Security Group and key for enabling encryption*

### 4.1.4.10. Install application software

Once the RDS DB instance is finished provisioning, the environment is ready.

NOTE: The steps in this build focus on leveraging the AWS services for compliance. Numerous additional PCI requirements will need to be addressed to ensure this environment is compliant including (but not limited to) anti-virus, patch management, log management, vulnerability management, and file integrity monitoring.

## 4.2. Architecture 2: Segmented

This architecture builds upon the previous design. It demonstrates an e-commerce website segmented from other systems in an existing Amazon AWS environment.

Segmenting the CDE systems from the rest of an AWS account limits the scope of PCI compliance.

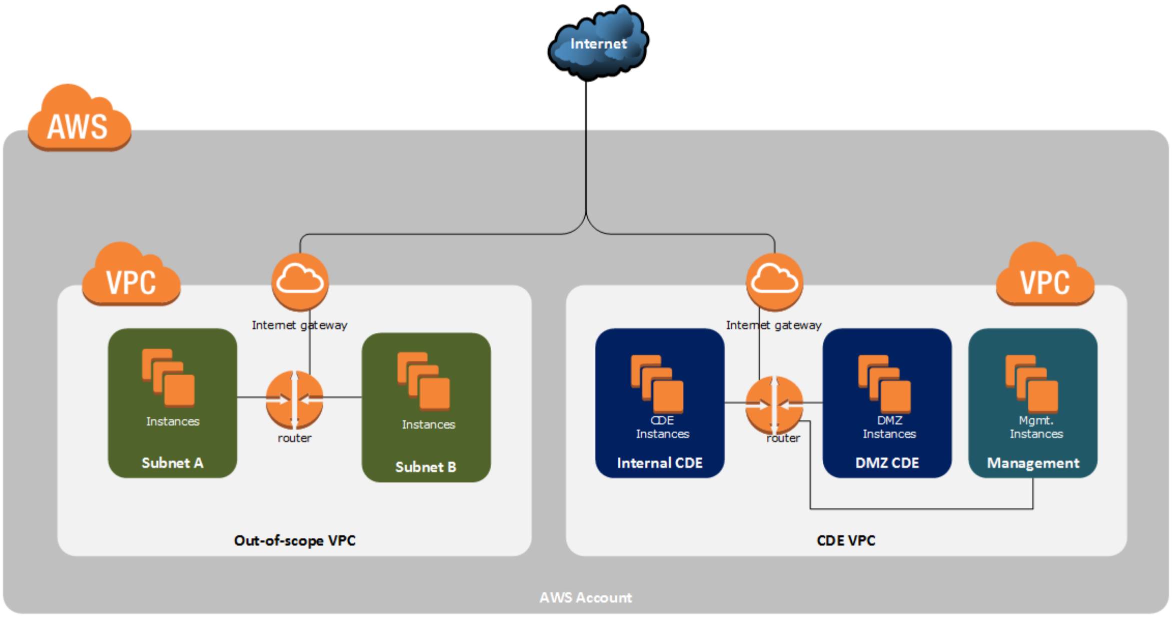


*Figure 31 - Architecture of segmented CDE within broader AWS environment*

### 4.2.1. Overview

In the Segmented reference architecture, there are two private networks contained in separate VPCs:

- CDE VPC
  - Contains the DMZ CDE, the Management, and Internal CDE subnets.
- Out-of-scope VPC
  - Contains two subnets in private networks segmented from the CDE.

The systems and subnets in the CDE VPC network are the same as those in the first architecture. The new VPC represents additional systems and subnets that do not require connectivity to any CDE systems. This architecture demonstrates how to remove the new VPC from the PCI assessment scope through segmentation.

To segment the out-of-scope networks, they must not connect to the CDE. In a traditional environment, this is typically accomplished using firewall policies, switch ACLs, VLANs, or other network segmentation and isolation technologies.

In AWS, you can combine Security Groups and VPCs to satisfy the firewall and router configuration needs of Requirement 1.2. As discussed above, Security Groups control traffic into and out of Instances. VPCs represent separate, isolated, private network spaces within the AWS network. They each use their own private address space and are isolated from other networks and other resources in an AWS account. They provide the most direct way to implement true network segmentation for PCI scope reduction.

NOTE: To ensure that the CDE VPC in this reference architecture is segmented from the out-of-scope VPC, VPC peering must not be setup between them. This could bring the non-CDE VPC into the assessment scope (which is an appropriate strategy in some circumstances, but not used in this example).

### 4.2.2. PCI Scope

The CDE is comprised of the following instances in this architecture all contained within the private CDE VPC network:

- Web server
- App server
- RDS DB

The new VPC is out-of-scope for PCI due to network segmentation as discussed below.

### 4.2.3. Applicable AWS Services

The following AWS services support compliance with PCI requirements for this architecture:

| AWS SERVICE | PCI REQUIREMENTS SUPPORTED |
|---|---|
| • IAM<br>• KMS | 2.2.4, 3.4, 3.5, 3.5.2-3, 3.6, 3.6.1-5, 3.6.7, 6.4.1-2, 7.1, 7.1.1-3, 7.2, 7.2.1-3, 8.1, 8.1.1-2, 8.2, 8.2.1, 8.2.3-6, 8.3, 8.3.1, A.1.2 |
| • S3 | 3.1, 3.4, 10.5, 10.5.1-5, 10.7 |
| • CloudTrail<br>• CloudWatch | 10.1, 10.2, 10.2.2-7, 10.3, 10.3.1-6, 10.5, 10.5.1-5, 10.7, A.1.3 |
| • EC2<br>• Security Groups<br>• AMIs<br>• EBS | 1.1, 1.1.4, 1.2, 1.2.1, 1.3, 1.3.1-7, 2.1, 4.1, 6.4.1 |
| • RDS | 3.4 |
| • Config | 2.4, 11.5 |

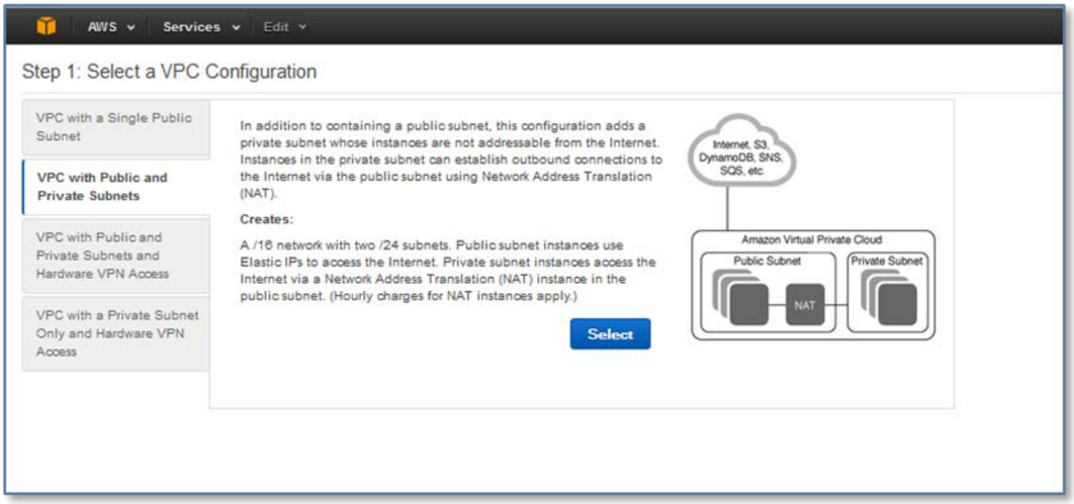
| | |
|---|---|
| • VPC | 1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7 |

### 4.2.4. Build Out

This section describes the primary steps to build out the reference architecture.

#### 4.2.4.1. Create a VPC

Create a new VPC network to contain and segregate the out-of-scope instances from the CDE instances created in the first architecture.


AWS
Services
Edit
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
Select
Internet, S3, DynamoDB, SNS, SQS, etc.
Amazon Virtual Private Cloud
Public Subnet
Private Subnet
NAT

Step 1: Select a VPC Configuration

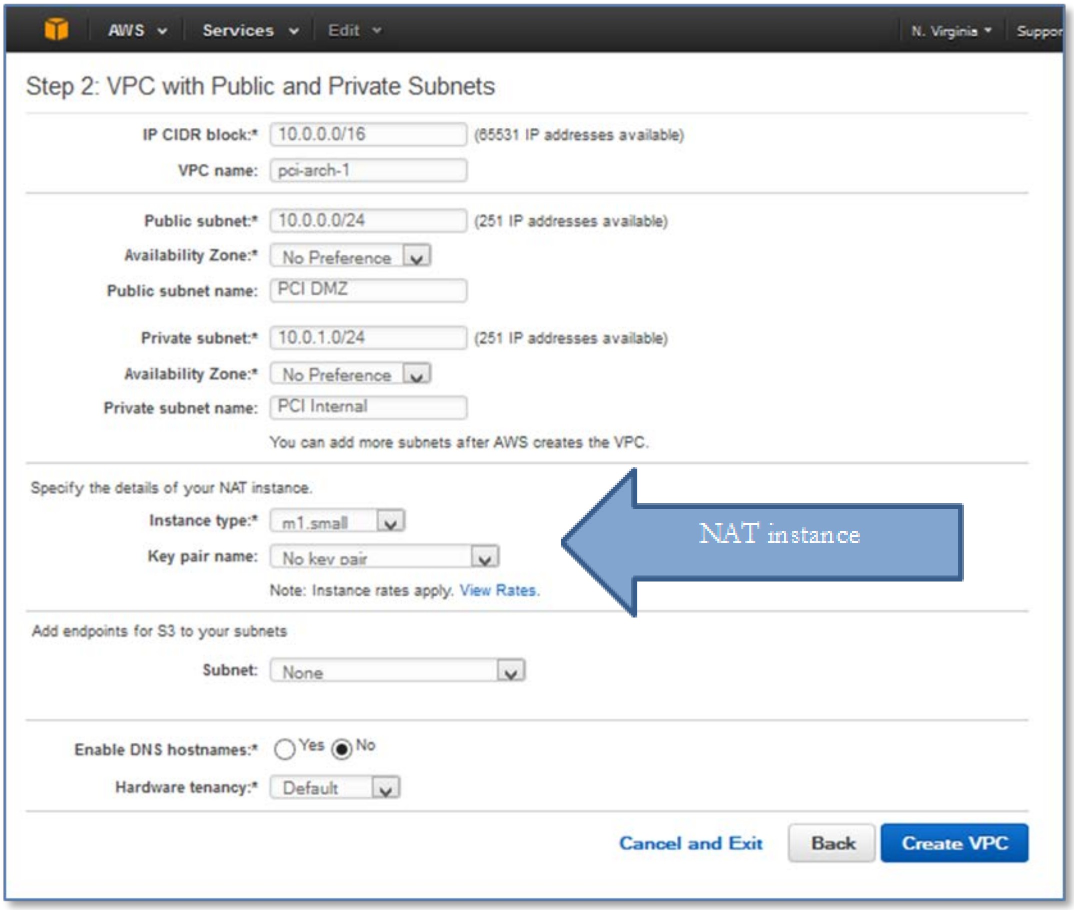
In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

**Creates:**

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply.)

*Figure 32 – Creating a new VPC*

The new VPC includes a NAT instance designed to work like an Internet gateway router for the private subnet.  Once the VPN is created, you can delete this NAT instance to prevent other instances in the new subnets from accessing the Internet.



Step 2: VPC with Public and Private Subnets

IP CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

VPC name: pci-arch-1

Public subnet:* 10.0.0.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Public subnet name: PCI DMZ

Private subnet:* 10.0.1.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Private subnet name: PCI Internal

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT instance.

Instance type:* m1.small

Key pair name: No key pair

Note: Instance rates apply. View Rates.

NAT instance

Add endpoints for S3 to your subnets

Subnet: None

Enable DNS hostnames:* ○ Yes ● No

Hardware tenancy:* Default

*Figure 33 – Configure the new VPC*

### 4.2.4.2. Create IAM Users, Groups and KMS Keys

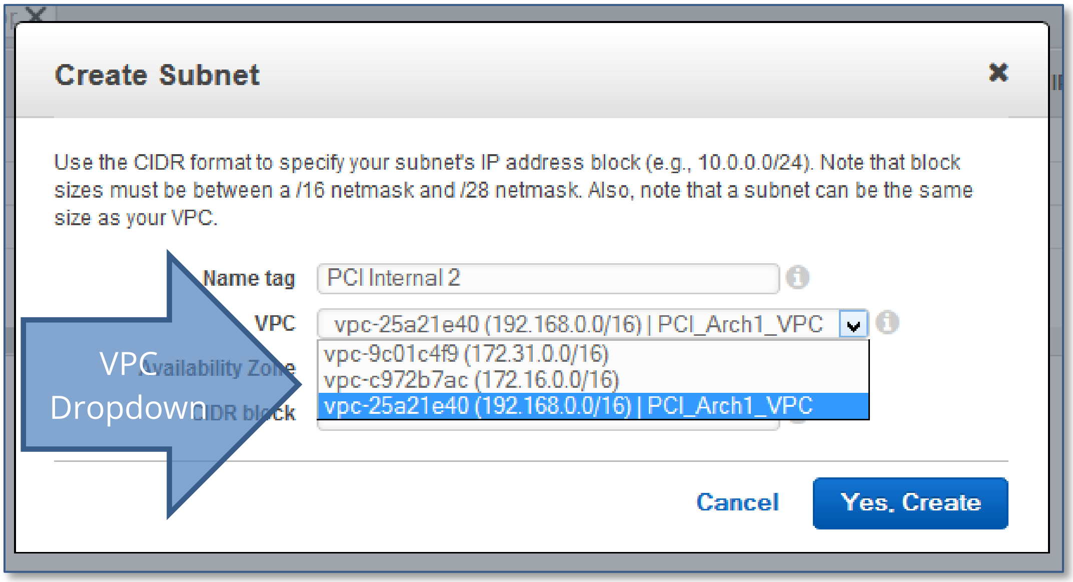
IAM resources are not region or VPC-specific. All resources within an AWS account share the same IAM resources.

Create these as outlined above in Sections 4.1.4.1 and 4.1.4.2.

### 4.2.4.3. Create Resource in the VPC

When creating resources, be sure to select the newly created VPC in the “VPC” dropdown of each resource creation wizard.

NOTE: Not all AWS resources are specific to a single VPC or region. If a resource cannot be found on the VPC Dashboard, try looking in the EC2 service management console.



Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag: PCI Internal 2

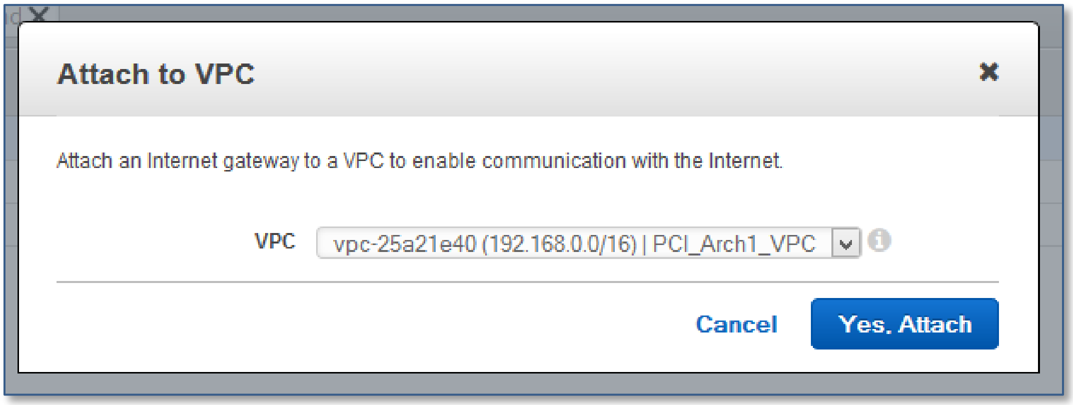
VPC: vpc-25a21e40 (192.168.0.0/16) | PCI_Arch1_VPC

vpc-9c01c4f9 (172.31.0.0/16)
vpc-c972b7ac (172.16.0.0/16)
vpc-25a21e40 (192.168.0.0/16) | PCI_Arch1_VPC

*Figure 34 – Create VPC subnet*

### 4.2.4.4. Internet Access

The VPC network will need its own Internet gateway. Create the gateway and attach it to the VPC.



Attach to VPC

Attach an Internet gateway to a VPC to enable communication with the Internet.

VPC: vpc-25a21e40 (192.168.0.0/16) | PCI_Arch1_VPC

*Figure 35 – Attaching an Internet Gateway to a VPC*

## 4.3. Architecture 3: Connected

This architecture represents connecting an on-premise CDE into an Amazon AWS environment.

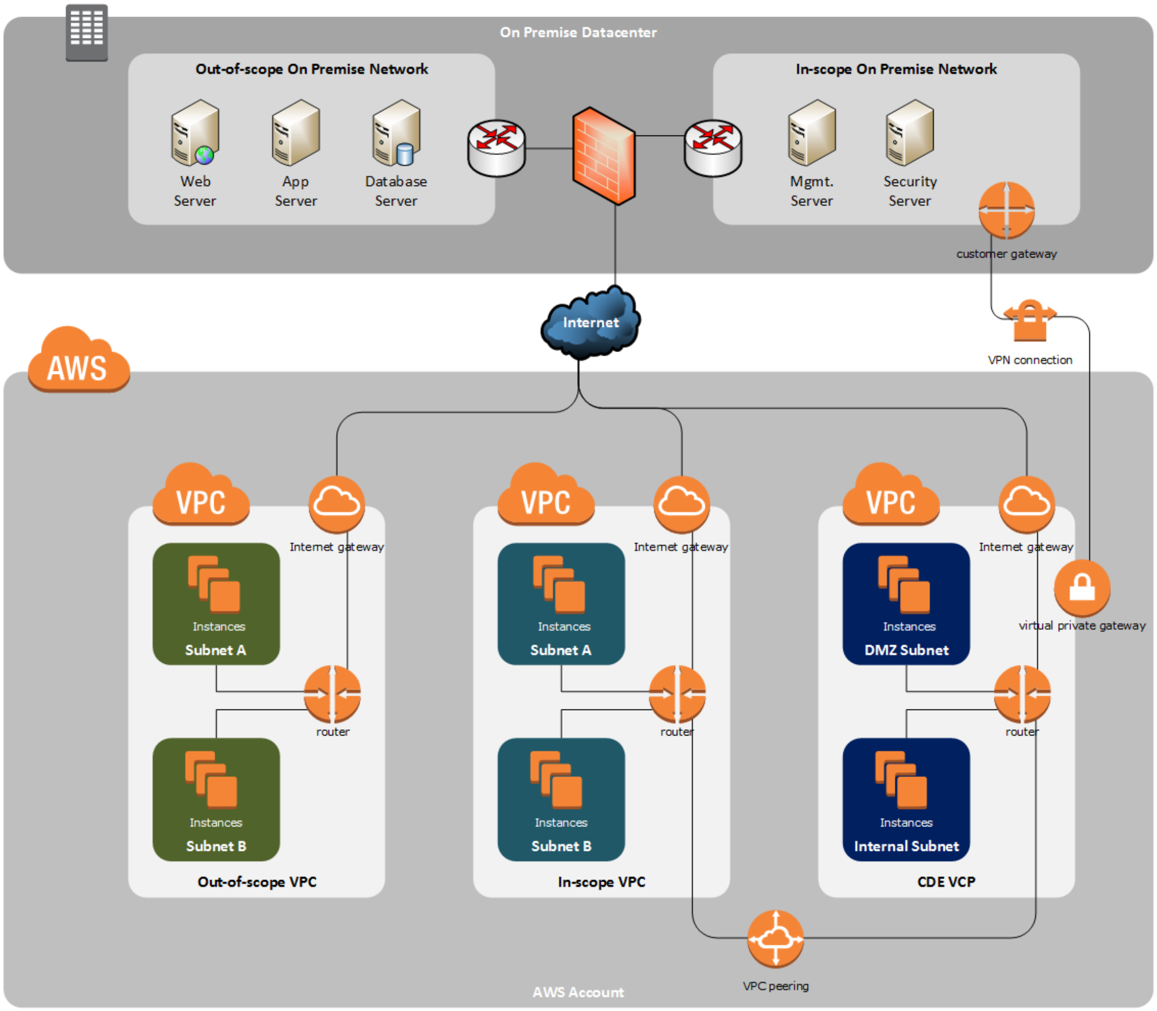


*Figure 36 – Connected on-premise systems into AWS CDE*

### 4.3.1. Overview

In the Connected reference architecture, there are three private networks in AWS and two typical on-premise networks.

### AWS Networks

1. CDE VPC

   This is the VPC from Architecture 1 with a DMZ and internal CDE subnet.

2. Out-of-scope VPC

   This is the new VPC from Architecture 2 segmented with no VPC peering.

3. In-Scope VPC

This is a new VPC and is connected to the CDE via VPC peering.

### On-premise Networks

1. In-Scope On-Premise Network

   This is a customer network segment connected to the AWS CDE via a VPN.
2. Out-of-scope On-Premise Network

   This is a customer network segmented from the in-scope customer network and AWS.

Extending an on-premise network into a VPC in AWS is no different than setting up other business-to-business VPN connections. In a typical VPN setup, IPsec tunnels provide private communication for two or more trusted networks across untrusted networks like the Internet. The same technology can be used to provide access to a private VPC network from other VPCs or even on-premise environments.

It is also possible to set up a direct, private, non-VPN connection into AWS using the Direct Connect service. Direct Connect supports high bandwidth links and can be combined with 802.1q VLAN tagging to support logical segmentation. As Section 3.4 above notes, connections using Direct Connect are not encrypted. Additional controls including a VPN or TLS may still be necessary to comply with PCI 4.1 if the direct network connection is not private.

This architecture does not include its own Jumpbox as the on-premise and in-scope management systems can administer the AWS CDE systems without changes to the assessment scope.

### 4.3.2. PCI Scope

The PCI assessment scope in this reference architecture consists of:

- The CDE VPC network (web, app, and database tiers).
- The In-Scope VPC network in AWS.
- The In-Scope On-Premise network.

The two in-scope networks do not have CHD but are connected to the CDE. This architecture demonstrates two common use cases for connected in-scope systems:

- The In-Scope VPC in AWS has systems that perform analytics on the CDE web application without accessing CHD.
- The In-Scope, On-Premise Network has systems that provide security controls for the CDE such as anti-malware and patch management.

The two out-of-scope networks in this reference architecture have no network connectivity to the AWS CDE as discussed in Section 4.3.1 above.

### 4.3.3. Applicable AWS Services

The following AWS services help support compliance with PCI requirements for this architecture.

| AWS SERVICE | PCI REQUIREMENTS SUPPORTED |
|---|---|
| • IAM<br>• KMS | 2.2.4, 3.4, 3.5, 3.5.2-3, 3.6, 3.6.1-5, 3.6.7, 6.4.1-2, 7.1, 7.1.1-3, 7.2, 7.2.1-3, 8.1, 8.1.1-2, 8.2, 8.2.1, 8.2.3-6, 8.3, 8.3.1, A.1.2 |
| • S3 | 3.1, 3.4, 10.5, 10.5.1-5, 10.7 |
| • CloudTrail<br>• CloudWatch | 10.1, 10.2, 10.2.2-7, 10.3, 10.3.1-6, 10.5, 10.5.1-5, 10.7, A.1.3 |
| • EC2<br>• Security Groups<br>• AMIs<br>• EBS | 1.1, 1.1.4, 1.2, 1.2.1, 1.3, 1.3.1-7, 2.1, 4.1, 6.4.1 |
| • RDS | 3.4 |
| • Config | 2.4, 11.5 |
| • VPC | 1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7 |

### 4.3.4. Build Out

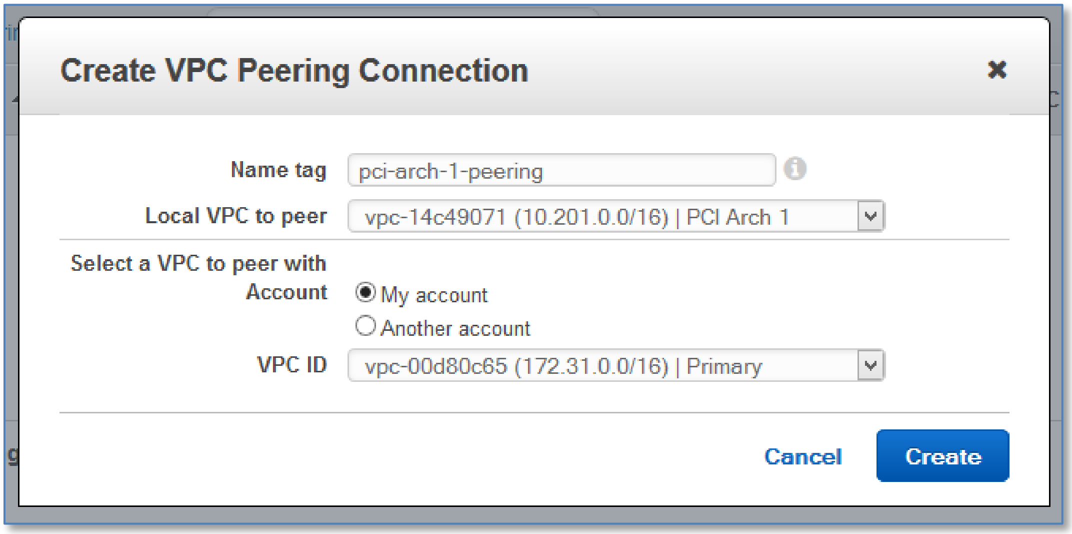
This section describes the primary steps for building out the reference architecture.

#### 4.3.4.1. Create a VPC

Build the In-Scope VPC as per the steps in Architecture 2: Segmented CDE described in Section 4.2 above.

#### 4.3.4.2. Create a VPC Peering Connection

Create a VPC Peering connection between the CDE VPC and the newly created In-Scope VPC.



Create VPC Peering Connection

Name tag: pci-arch-1-peering

Local VPC to peer: vpc-14c49071 (10.201.0.0/16) | PCI Arch 1

Select a VPC to peer with

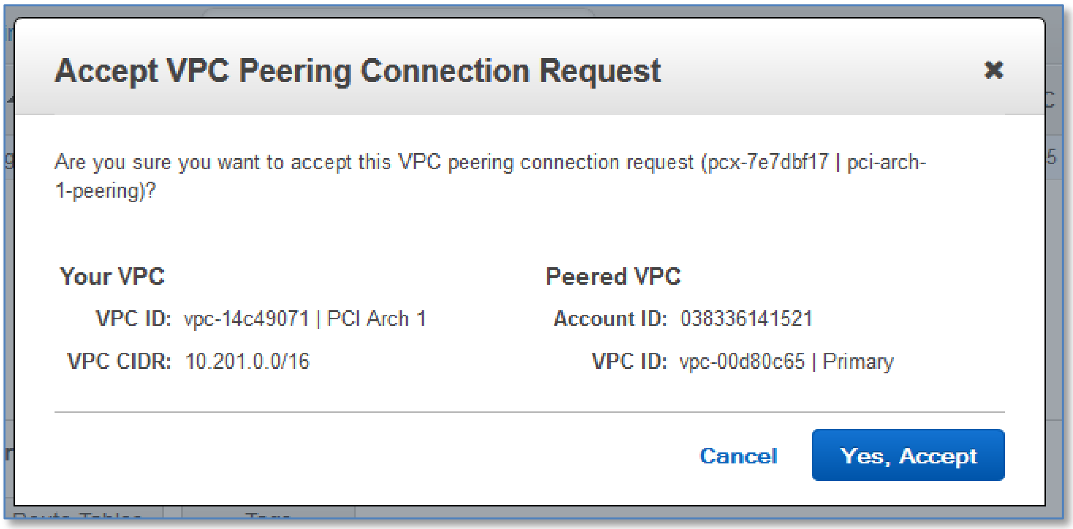
Account: ● My account ○ Another account

VPC ID: vpc-00d80c65 (172.31.0.0/16) | Primary

*Figure 37 – Creating a VPC Peering Connection*

### 4.3.4.3. Accept the VPC Peering Connection

After creating the VPC Peering connection, the peering request must be accepted. This is necessary as VPC Peering is supported between VPCs in different AWS accounts.



Accept VPC Peering Connection Request

Are you sure you want to accept this VPC peering connection request (pcx-7e7dbf17 | pci-arch-1-peering)?

Your VPC

VPC ID: vpc-14c49071 | PCI Arch 1

VPC CIDR: 10.201.0.0/16

Peered VPC

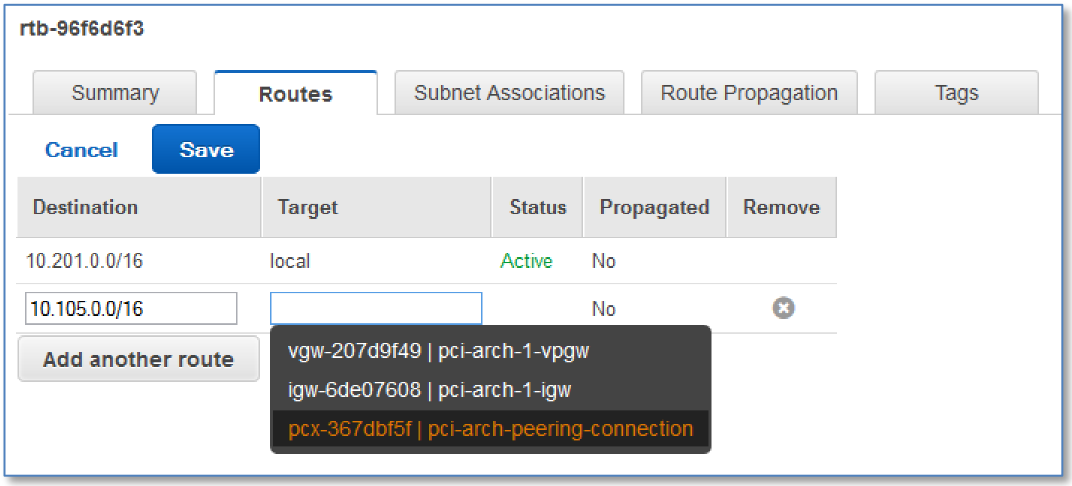
Account ID: 038336141521

VPC ID: vpc-00d80c65 | Primary

*Figure 38 – Accepting a VPC Peering Request*

### 4.3.4.4. Add Routes through the VPC Peering Connection

Once the VPC Peering connection is accepted, you will be able to add routes to the peered VPC in the CDE VPC routing tables.  Do not forget to add return routes from the In-Scope VPC.


rtb-96f6d6f3
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
Add another route

| Destination | Target | Status | Propagated | Remove |
|---|---|---|---|---|
| 10.201.0.0/16 | local | Active | No | |
| 10.105.0.0/16 | | | No | ⊗ |

vgw-207d9f49 | pci-arch-1-vpgw
igw-6de07608 | pci-arch-1-igw
pcx-367dbf5f | pci-arch-peering-connection

*Figure 39 – Adding a Route to a Peered VPC*

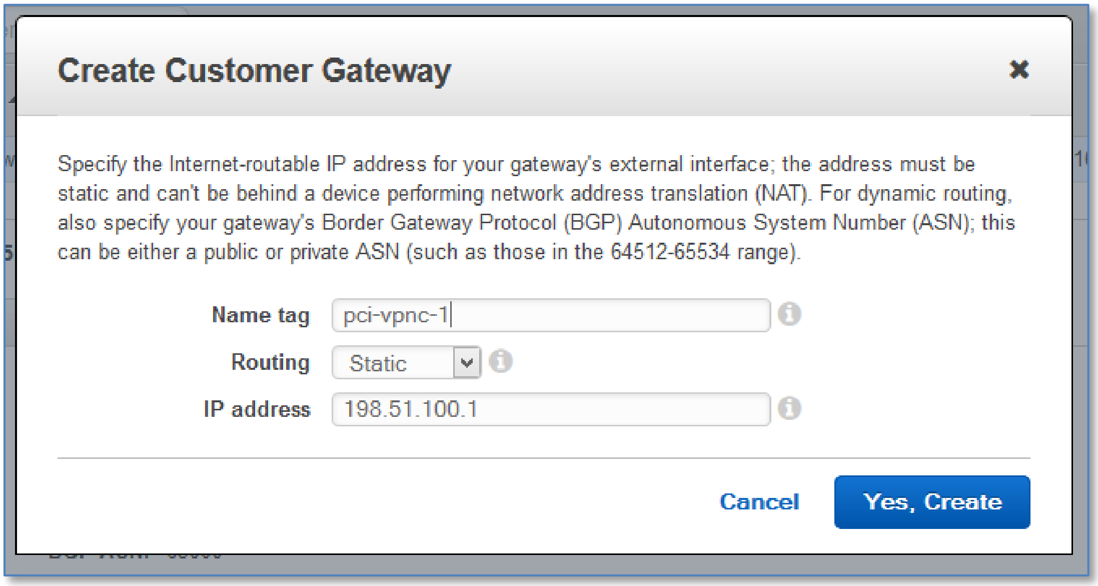
### 4.3.4.5. Leverage In-Scope VPC Resources

After the routes are added, the In-Scope VPC systems including the analytic systems cited in this example, will be able to access the CDE.

NOTE: You will need to modify the CDE Security Groups or create new ones to allow connections from the In-Scope CDE to the appropriate CDE Instances.

### 4.3.4.6. Create a Customer Gateway

Within the CDE VPC, create a Customer Gateway. This resource in AWS represents a VPN concentrator at a client site.



Specify the Internet-routable IP address for your gateway's external interface; the address must be static and can't be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name tag: pci-vpnc-1

Routing: Static

IP address: 198.51.100.1

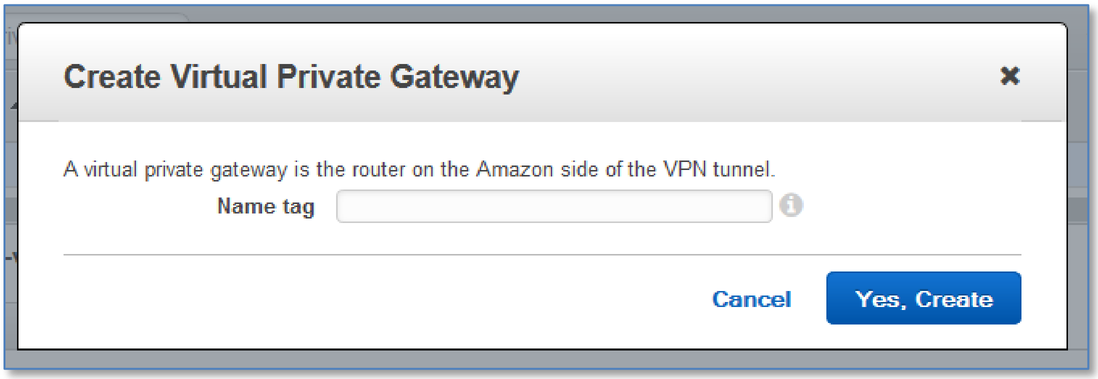
*Figure 40 – Creating a Customer Gateway*

NOTE: Customer Gateways also support dynamic IP routing using BGP. If dynamic is selected. The gateway will also need the ASN for the network of the remote IP address.

### 4.3.4.7. Create a Virtual Private Gateway

Within the VPC, create a Virtual Private Gateway (VPG). This resource in AWS represents an AWS routing target for a VPN connection.

Like an Internet Gateway, this VPG is a specialized network interface used to send and receive external traffic. Attach the VPG to the VPC after creating it.



Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag

*Figure 41 – Creating a Virtual Private Gateway*

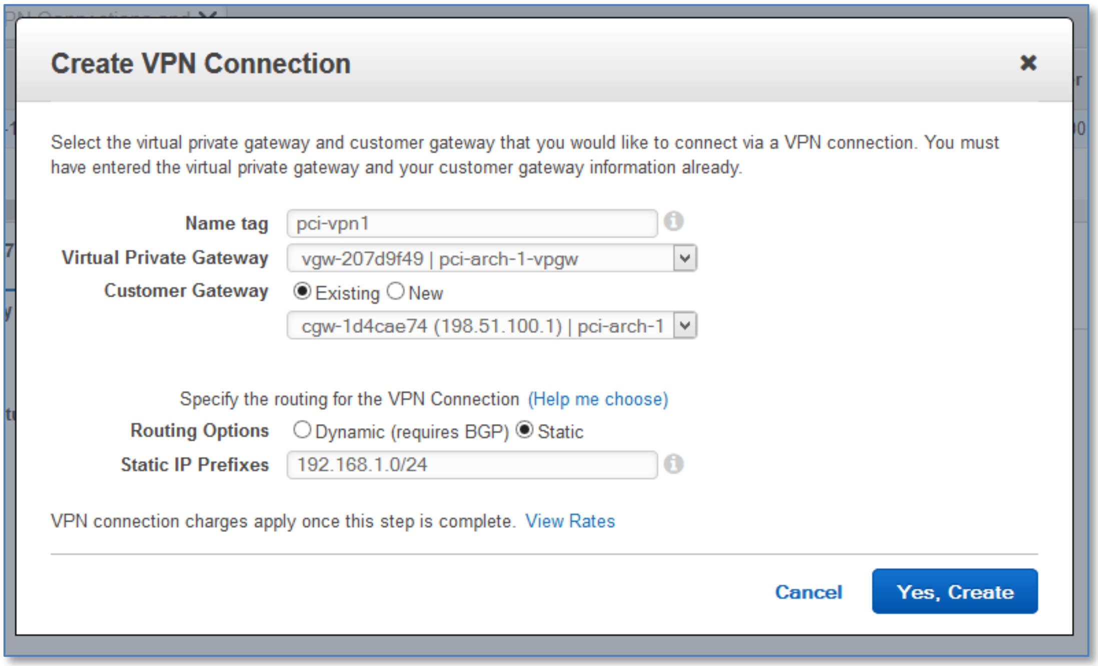
### 4.3.4.8. Create the VPN Connection

AWS supports industry-standard IPsec VPN connections. The VPN AWS resource provides the connection between the VPG and the Customer Gateway.

For the VPN, specify the VPG and the Customer Gateway created above.

The “Static IP Prefixes” item is the remote IP subnet to route through the VPN connection.

NOTE: The VPN connection includes two AWS side endpoints for redundancy.



**Create VPN Connection**

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.

Name tag: pci-vpn1

Virtual Private Gateway: vgw-207d9f49 | pci-arch-1-vpgw

Customer Gateway: ● Existing ○ New

cgw-1d4cae74 (198.51.100.1) | pci-arch-1

Specify the routing for the VPN Connection (Help me choose)

Routing Options: ○ Dynamic (requires BGP) ● Static

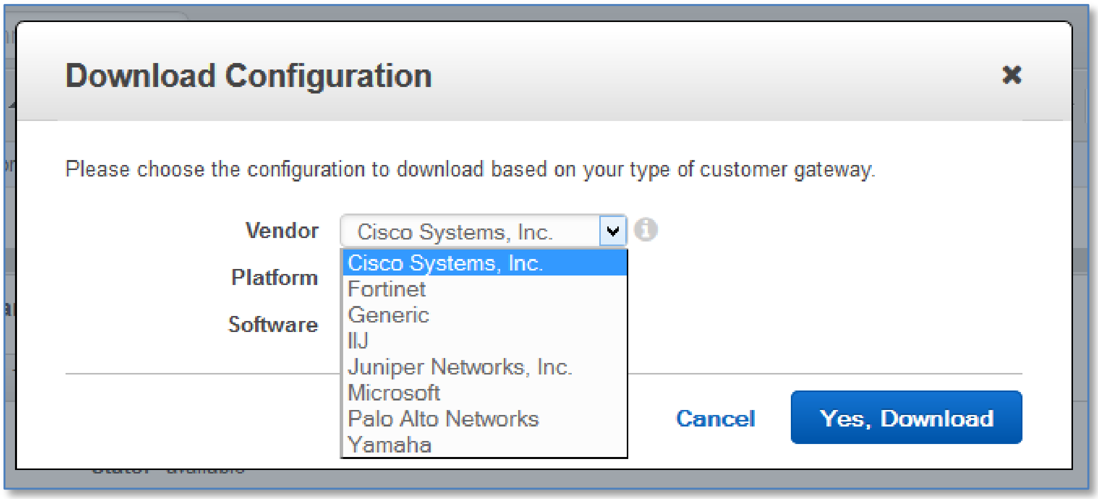
Static IP Prefixes: 192.168.1.0/24

VPN connection charges apply once this step is complete. View Rates

*Figure 42 – Creating a VPN Connection*

### 4.3.4.9. Download IPsec Configuration Details

Download the configuration needed for the on-premise VPN concentrators. AWS supports native configuration files for a variety of firewall/VPN manufacturers such as Cisco and Fortinet.



**Download Configuration**

Please choose the configuration to download based on your type of customer gateway.

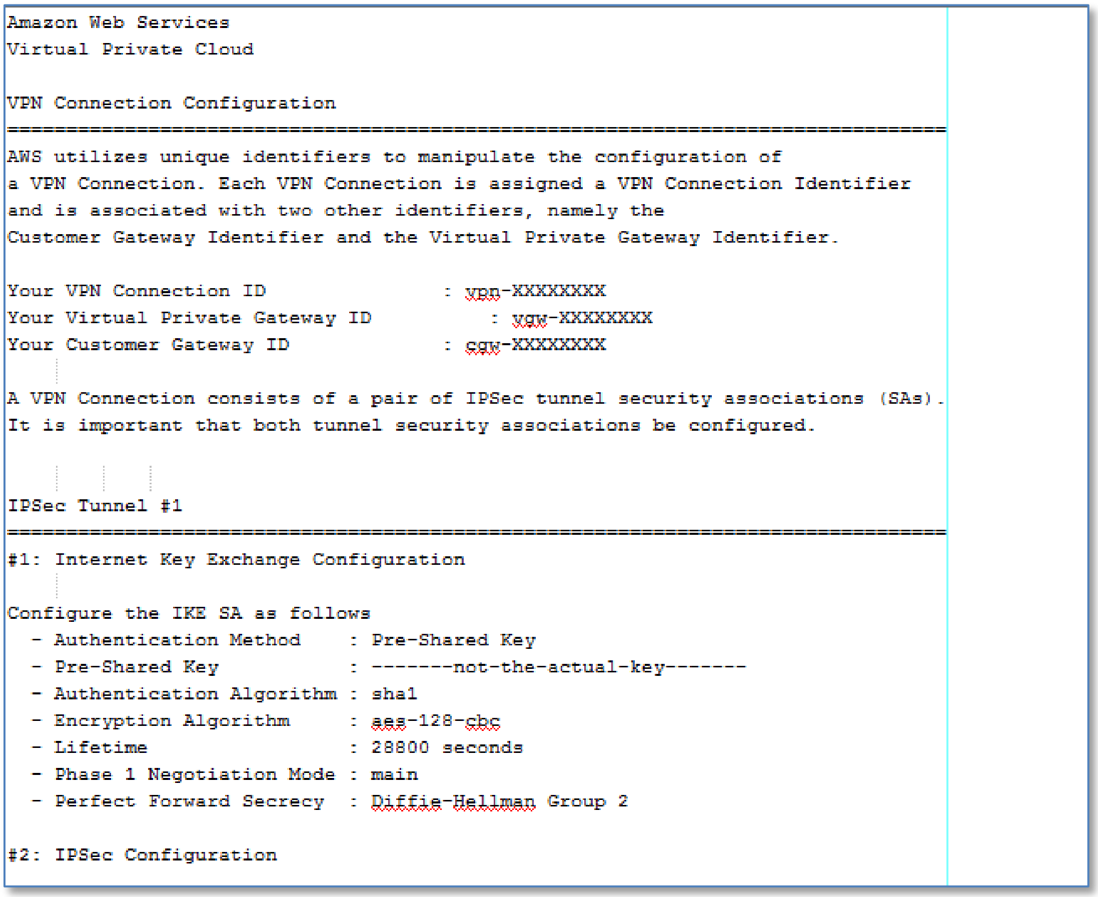
Vendor: Cisco Systems, Inc.

Platform

Software

*Figure 43 – Downloading the VPN Configuration*

There is a Generic option that allows the download of a text file containing the VPN connection details if you have a device not listed.

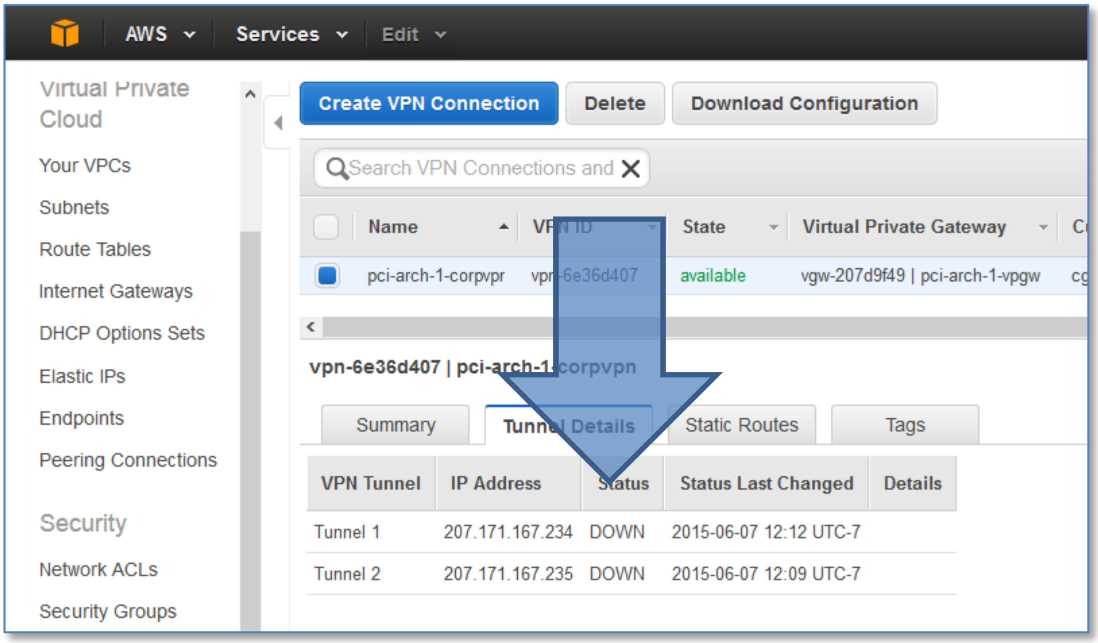


```
Amazon Web Services
Virtual Private Cloud

VPN Connection Configuration
================================================================================
AWS utilizes unique identifiers to manipulate the configuration of
a VPN Connection. Each VPN Connection is assigned a VPN Connection Identifier
and is associated with two other identifiers, namely the
Customer Gateway Identifier and the Virtual Private Gateway Identifier.

Your VPN Connection ID                 : vpn-XXXXXXXX
Your Virtual Private Gateway ID            : vgw-XXXXXXXX
Your Customer Gateway ID               : cgw-XXXXXXXX

A VPN Connection consists of a pair of IPSec tunnel security associations (SAs).
It is important that both tunnel security associations be configured.


IPSec Tunnel #1
================================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : -------not-the-actual-key-------
  - Authentication Algorithm : sha1
  - Encryption Algorithm     : aes-128-cbc
  - Lifetime                 : 28800 seconds
  - Phase 1 Negotiation Mode : main
  - Perfect Forward Secrecy  : Diffie-Hellman Group 2

#2: IPSec Configuration
```

*Figure 44 – Example Generic VPN Configuration File*

### 4.3.4.10. Verify VPN Tunnel Status

After configuring the on-premise Client VPN endpoints, verify the VPN's  location . View the tunnel's status from the "Tunnel Details" tab of the VPN resource details pane.



| Name | VPN ID | State | Virtual Private Gateway | Cu |
|---|---|---|---|---|
| pci-arch-1-corpvpr | vpn-6e36d407 | available | vgw-207d9f49 \| pci-arch-1-vpgw | cg |

vpn-6e36d407 | pci-arch-1-corpvpn

| VPN Tunnel | IP Address | Status | Status Last Changed | Details |
|---|---|---|---|---|
| Tunnel 1 | 207.171.167.234 | DOWN | 2015-06-07 12:12 UTC-7 | |
| Tunnel 2 | 207.171.167.235 | DOWN | 2015-06-07 12:09 UTC-7 | |

*Viewing the VPN tunnels status*

### 4.3.4.11. Leverage On-Premise Resources

After the VPN tunnels come up, the on-premise, in-scope systems will be available for use within the AWS CDE including the AV and patch management consoles cited in this example.

# 5. CONCLUSION

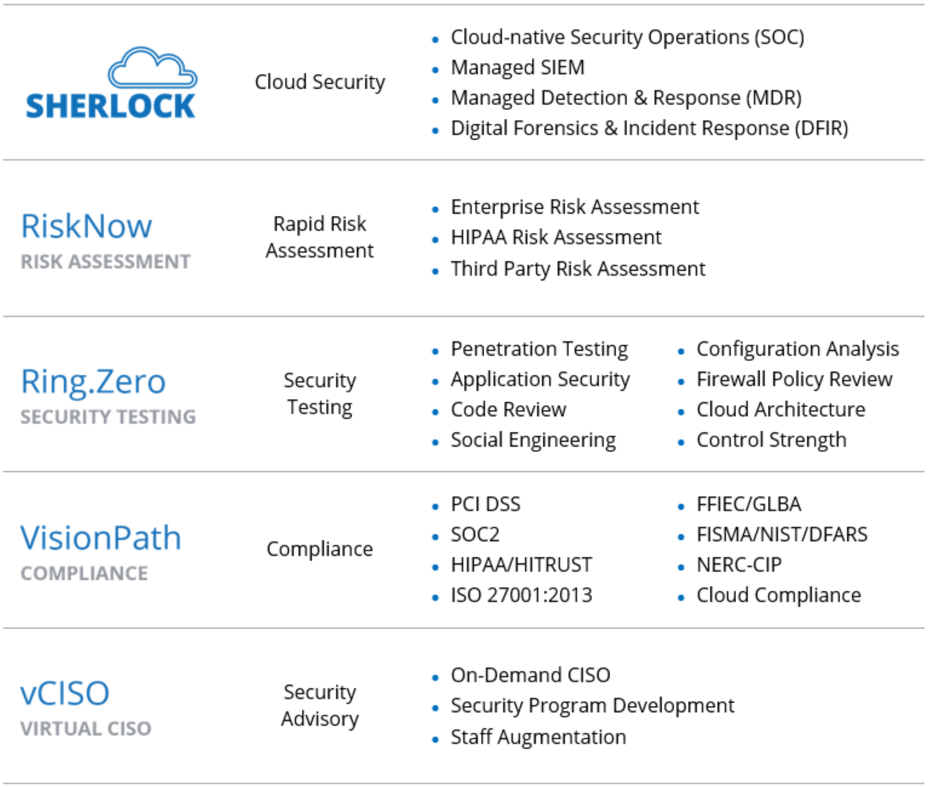
AWS is a powerful cloud platform that offers numerous capabilities to support a fully PCI-compliant environment.  It is important that you and your PCI assessor understand these capabilities.

This workbook clarifies some of these issues.  Achieving PCI compliance is a function of how effectively you deploy, configure, manage, and document the environment. Compliance requires an understanding of how AWS natively supports PCI requirements so you can use them correctly.

## 5.1. Support

If you need support with AWS, you should contact Amazon's AWS technical support.

Anitian can help as well.  Our five information security practices offer a comprehensive set of compliance, penetration testing, and managed security services.



| | | | |
|---|---|---|---|
| SHERLOCK | Cloud Security | • Cloud-native Security Operations (SOC)<br>• Managed SIEM<br>• Managed Detection & Response (MDR)<br>• Digital Forensics & Incident Response (DFIR) | |
| RiskNow<br>RISK ASSESSMENT | Rapid Risk Assessment | • Enterprise Risk Assessment<br>• HIPAA Risk Assessment<br>• Third Party Risk Assessment | |
| Ring.Zero<br>SECURITY TESTING | Security Testing | • Penetration Testing<br>• Application Security<br>• Code Review<br>• Social Engineering | • Configuration Analysis<br>• Firewall Policy Review<br>• Cloud Architecture<br>• Control Strength |
| VisionPath<br>COMPLIANCE | Compliance | • PCI DSS<br>• SOC2<br>• HIPAA/HITRUST<br>• ISO 27001:2013 | • FFIEC/GLBA<br>• FISMA/NIST/DFARS<br>• NERC-CIP<br>• Cloud Compliance |
| vCISO<br>VIRTUAL CISO | Security Advisory | • On-Demand CISO<br>• Security Program Development<br>• Staff Augmentation | |

Contact us at: 888-264-8456, email info@anitian.com, or visit our site at anitian.com.

# APPENDIX A. AWS PCI DSS RESPONSIBILTIY MATRIX SUMMARY

The following table summarizes the responsibilities for PCI compliance between AWS and customers.

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| **Requirement 1**: Install and maintain a firewall configuration to protect cardholder data. | • **All In-Scope Services:** AWS maintains instance isolation for host operating systems and the AWS Management Environment including host operating system, hypervisor, firewall configuration, and baseline firewall rules.<br>• AWS meets all requirements for implementing and managing firewalls for the AWS management environment.<br>• **Amazon EC2 and Amazon ECS:** Amazon VPC Security Groups and network ACLs implement stateful inspection network access control and are suitable for compliant network segmentation | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for security group definitions and network access control rules. |

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| **Requirement 2**: Do not use Supplier-supplied defaults for system passwords and other security parameters. | • **All In-Scope Services:** AWS develops and maintains configuration and hardening standards for the AWS Management Environment that provides the virtualization technologies and applications for providing cloud services.<br>• AWS maintains configuration and hardening standards for the underlying operating systems and platforms for these services. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for changing default vendor configurations, security controls, and vendor default passwords.<br>• **All In-Scope Services:** AWS customers are responsible for secure and compliant configuration for all customer-configurable items. This may include OS configuration for Amazon EC2 and Amazon ECS instances, logging and log retention for data base services, or permissions for AWS management functions. |
| **Requirement 3**: Protect stored cardholder data. | • **All In-Scope Services:** AWS Key Management Service (AWS KMS) secures keys using hardware security modules and provides functions to use and manage keys.<br>• AWS CloudHSM secures keys and provides cryptographic functions using customer-dedicated hardware security modules. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for changing default vendor configurations, security controls, and vendor default passwords.<br>• **All In-Scope Services:** AWS customers are responsible for implementing encryption on all applicable internal and external network connections. (This may require use of AWS optional API encryption).<br>• **AWS KMS and AWS CloudHSM:** AWS customers are responsible for the creation, usage, and management of encryption keys in accordance with PCI Data Security Standards. |

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| **Requirement 4**: Encrypt transmission of cardholder data across open, public networks. | • **All In-Scope Services:** AWS encrypts access and manages encryption within the AWS Management Environment. | • **All In-Scope Services:** AWS customers are responsible for implementing encryption on all applicable internal and external network connections. (This may require use of AWS optional API encryption). |
| **Requirement 5**: Use and regularly update anti-virus software or programs. | • **All In-Scope Services:** AWS manages anti-virus software for the AWS Management Environment and, where appropriate, for identified services. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for implementing anti-virus software on customer-managed OS instances commonly subject to malware. |

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| **Requirement 6**: Develop and maintain secure systems and applications. | • **All In-Scope Services:** AWS maintains security patching, development, and change control of the applications that support the services included in the assessment including web interfaces, APIs, access controls, provisioning, and deployment mechanisms.<br>• AWS develops and manages changes to applications that support the services included in the assessment including web interfaces, APIs, access controls, provisioning, and deployment mechanisms. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for monitoring published OS and application vulnerabilities and patching on instances.<br>• Customers are required to use documented change control for all configurations and customer code.<br>• Customers who develop custom code that is used to transmit, process, or store credit card data must comply with requirements for secure development and testing.<br>• **AWS Web Application Firewall (AWS WAF):** Customers are responsible for protecting their web applications from common web exploits. This includes (but not limited to) configuring access control lists and web application firewall rules for filtering traffic to and from their web applications. |

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| **Requirement 7:** Restrict access to cardholder data by business need-to- know. | • **All In-Scope Services:** AWS maintains the access controls related to underlying infrastructure systems and the AWS Management Environment. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for access control within all OS instances.<br>• **All In-Scope Services:** AWS customers are responsible for configurable access controls within the services such as database users within Amazon RDS.<br>• **AWS IAM & AWS Credentials:** AWS customers are responsible for managing access to all AWS services that are included in their CDE. AWS IAM can be used to configure resource management and AWS configuration roles and permissions. Customers are responsible for configuring AWS account and session controls to meet PCI requirements. Customers must be aware of AWS guidelines for credentials and access control for AWS resource management. |

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| **Requirement 8:** Assign a unique ID to each person with computer access. | • **All In-Scope Services:** AWS provides each user in the AWS Management Environment a unique ID.<br>• AWS provides additional security options that enable AWS customers to further protect their AWS Account and control access: AWS Identity and Access Management (AWS IAM), Multi-Factor Authentication (MFA), and Key Rotation. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for access control within all OS instances.<br>• **All In-Scope Services:** AWS customers are responsible for configurable access controls within the services such as database users within Amazon RDS.<br>• **AWS IAM & AWS Credentials:** AWS customers are responsible for managing access to all AWS services that are included in their CDE. AWS IAM can be used to manage resource management and AWS configuration roles and permissions. Customers are responsible for configuring AWS account and session controls to meet requirements. Customers must be aware of AWS guidelines for credentials and access control for AWS resource management. |
| **Requirement 9:** Restrict physical access to cardholder data. | • **All In-Scope Services:** AWS maintains the physical security and media handling controls for the services included in the assessment. | • **All In-Scope Services:** Any media created outside of the AWS environment is the sole responsibility of the customer. |

| | | |
|---|---|---|
| **Requirement 10:** Track and monitor all access to network resources and cardholder data. | • **All In-Scope Services:** AWS maintains and monitors audit logs for the AWS Management Environment and AWS service infrastructure. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for logging within all OS instances.<br>• **AWS IAM & AWS Console:** User activity logs of resource management activities via the console and command line are available to users via Amazon AWS CloudTrail. Amazon AWS CloudTrail must be used to record and monitor AWS resource management activities.<br>• **Amazon S3:** Users are responsible for configuring bucket logging and monitoring logs.<br>• **Amazon RDS & Amazon Redshift:** Users are responsible for configuring database access logging and monitoring logs.<br>• **Amazon EMR:** Customers using Amazon EMR to store cardholder data are responsible for logging access.<br>• **Amazon SimpleDB & Amazon DynamoDB:** Customers using these databases are responsible for access logging.<br>• **AWS Config:** Customers using AWS Config to store configuration data and resource inventory are responsible for access logging and monitoring logs.<br>• **AWS WAF:** Customers using AWS WAF to protect public facing applications including application databases that |

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| | | store cardholder data are responsible for logging access and monitoring logs.<br>• **Elastic Load Balancing**: Customers using Elastic Load Balancing can monitor applications in real time integrating with Cloud Watch.<br>• **All In-Scope Services:** AWS customers are responsible for configuration of logging within the services. AWS CloudTrail can be used to log all AWS API calls.<br>• Customers are responsible for monitoring logs for security events. Log monitoring may be implemented with CloudWatch or 3rd party services. |
| **Requirement 11:** Regularly test security systems and processes. | • **All In-Scope Services:** AWS manages rogue wireless access point detection, vulnerability and penetration testing, intrusion detection, and file integrity monitoring for the AWS Management Environment and the identified services.<br>• AWS implements and monitors IDS/IPS on networks that implement AWS services. | • **Amazon EC2 and Amazon ECS:** AWS customers are responsible for internal and external scanning and penetration testing of their instances and virtual networks. Customers must follow AWS processes for scanning and penetration testing: http://aws.amazon.com/security/penetration-testing/.<br>• AWS customers are responsible for implementing IDS functionality typically using Host-based IDS (HIDS) on network segments they implement and manage. |

| REQUIREMENT | AWS RESPONSIBILITY | CUSTOMER RESPONSIBILITY |
|---|---|---|
| **Requirement 12:** Maintain a policy that addresses information security for employees and contractors. | • **All In-Scope Services:** AWS maintains security policies and procedures, security awareness training, security incident response plan, and human resource processes that align with PCI requirements. | • **All In-Scope Services:** AWS customers are responsible for all policies and procedures. AWS customers should include AWS as an infrastructure provider for Req. 12.8. Alerts from AWS should be part of the IRP for Req. 12.10. |
| **Requirement A1:** Shared hosting providers must protect the cardholder data environment. | • **All In-Scope Services:** AWS customer instances and data are protected by instance isolation and other security measures in the AWS Management Environment. | • **All In-Scope Services:** AWS customers may also be considered a shared hosting provider if they run applications or store data for their customers. In this case, customers are responsible for protecting their customer's data within AWS services. |
| **Appendix A2:** Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections | • This appendix concerns on-premise, point-of-sale terminals and is not applicable to AWS.<br>• However, the use of TLSv1.1 and/or v1.2 is required, and AWS fully supports these protocols. | • **All In-Scope Services**: AWS maintains TLSv1.1 or greater to support customer's PCI workloads. AWS provides a minimum-security policy of TLSv1.0 for customers with non-PCI workloads that still require it. AWS customers are responsible for initiating TLS connections that use TLSv1.1 or greater for PCI compliance. |

# APPENDIX B. CITATIONS

The following table summarizes all links referenced throughout this technical workbook.

| SECTION | RESOURCE | LINK |
|---|---|---|
| 1.2.3 | PCI DSS version 3.1 | https://www.pcisecuritystandards.org/security_standards/documents.php |
| 1.2.3 | Manage AWS Environments | http://aws.amazon.com/getting-started/ |
| 1.2.3 | PCI Cloud Computing Guidelines | https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf |
| 2.0 | AWS PCI Level 1 FAQ | http://aws.amazon.com/compliance/pci-dss-level-1-faqs |
| 2.3.1 | Request copy of AWS AOC | http://aws.amazon.com/compliance/contact/ |
| 3.3 | EBS Encryption | http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#EBSEncryption_supported_instances |
| 3.3 | Amazon S3 Server Side Encryption | http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html |
| 3.3 | Amazon S3 Upload Objects | http://docs.aws.amazon.com/AmazonS3/latest/UG/UploadingObjectsintoAmazonS3.html |
| 3.3 | AWS KMS Cryptographic Details | https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf |
| 3.3 | AWS KMS API Key Rotation | http://docs.aws.amazon.com/kms/latest/APIReference/API_EnableKeyRotation.html |
| 3.3 | AWS KMS Manual Key Creation | http://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html |
| 3.3 | Logging using CloudTrail | http://docs.aws.amazon.com/kms/latest/developerguide/logging-using-cloudtrail.html |
| 3.4 | ELB Security Policies Table | http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-security-policy-table.html |

| SECTION | RESOURCE | LINK |
|---|---|---|
| 3.4 | ELB Configuration | https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html |
| 3.4 | VPC FAQ | http://aws.amazon.com/vpc/faqs/ |
| 3.6 | AWS Linux Security Center | https://alas.aws.amazon.com/ |
| 3.7 | Admin Guide Directory Management | http://docs.aws.amazon.com/directoryservice/latest/adminguide/directory_management.html |
| 3.8 | Directory Service – Create a Directory | http://docs.aws.amazon.com/directoryservice/latest/adminguide/create_directory.html |
| 3.10 | CloudTrail Event Reference Record | http://docs.aws.amazon.com/awscloudtrail/latest/userguide/event_reference_record_body.html |
| 3.10 | Amazon S3 Lifecycle Configuration | http://docs.aws.amazon.com/AmazonS3/latest/UG/LifecycleConfiguration.html |
| 3.10, 3.11 | Sherlock Cloud Security | https://www.anitian.com/services-main/sherlock/ |
| 3.10 | Sherlock Managed SIEM | https://www.anitian.com/services-main/managed-siem |
| 3.11, 3.15 | AWS Penetration Testing Information | http://aws.amazon.com/security/penetration-testing |
| 3.11 | Anitian Penetration Testing Services | https://www.anitian.com/services-main/penetration-testing |
| 4.1.4.6 | Amazon VPC User Guide | http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#subnet-public-ip |
| 5.1 | AWS Technical Support | https://aws.amazon.com/premiumsupport/ |
| 5.1 | Anitian Website | www.anitian.com |