# 기술 워크북

## AWS 클라우드에서 PCI 규정 준수


보고일: 2017 년 1 월 20 일 Friday PM 7:15:53

작성자: Adam Gaydosh, QSA

Jordan Wiseman, QSA


ANITIAN

ANITIAN

# COPYRIGHT



Anitian Corporation

9780 SW Shady Ln, Suite 100

Portland OR, 97223

info@anitian.com

www.anitian.com

ANITIAN

# 목차

# 1. 요약

이 워크북에서는 PCI DSS(지불 카드 산업 데이터 보안 표준)를 준수하는 Amazon Web Service 에서 환경을 구축하기 위한 지침을 제공합니다.

## 1.1. 대상

이 워크북의 대상에는 다음이 포함됩니다.

- AWS 에서 PCI DSS 호환 환경을 구축하고자 하는 조직.
- AWS 에서 실행되는 CDE(카드 소지자 데이터 환경)를 평가하는 PCI QSA(공인 보안 평가자) 및 기타.

이 워크북은 규정을 준수하는 AWS 환경을 구축하는 고객에게 지침을 제공합니다.

## 1.2. 전제

이 단원에는 이 워크북의 내용에 영향을 미치는 Anitian 의 가정과 전제 조건이 나열되어 있습니다.

### 1.2.1. 최신 면책 조항

Anitian 은 QSAC(Qualified Security Assessor Company)이며 이 워크북의 작성자입니다. 이 워크북의 내용은 Anitian 의 PCI 에 대한 해석을 기반으로 합니다. 이 내용은 명시적 또는 암시적 보장 없이 "있는 그대로" 제공됩니다. 이 문서의 내용은 통지 없이 변경될 수 있습니다. 마찬가지로, AWS 환경의 추가 변경에 따라 이 문서의 일부 지침이 바뀔 수 있습니다.

PCI 평가자는 이 워크북의 지침 및 Anitian 의 해석과 다른 의견을 가질 수 있습니다.

이 워크북의 내용으로 PCI DSS 의 요구 사항을 대체하거나 대신할 수 없습니다.

### 1.2.2. 목적

이 워크북의 목적은 AWS 에서 PCI 규정 준수 환경을 배포하기 위한 지침을 제공하는 것입니다. 아래 단원에서는 다양한 PCI 요구 사항을 준수하기 위해 여러 AWS 서비스를 활용하는 방법을 간단히 설명합니다.

이 워크북에서는 공식적인 규정 준수는 물론 PCI 규정 준수 준비 상태를 확인하는 데 유용한 AWS 측면을 다루지만, AWS 환경 평가를 실시하기 위한 단계별 지침은 소개하지 않습니다. 그러나 PCI 규정에 맞는 AWS 환경을 이해한다는 점에서는 QSA 에 도움이 됩니다.

### 1.2.3. 선수 지식

독자는 다음을 이해해야 합니다.

- PCI DSS, 현재 버전 3.2
- AWS 환경을 관리하는 방법
- PCI 표준 위원회의 클라우드 컴퓨팅 지침

### 1.2.4. PCI 범위

이 워크북에서는 AWS 내에서 PCI 범위 축소 및 세분화를 다루지만, 전반적인 PCI DSS 규정 준수 면에서 이 문제에 대한 종합적인 가이드는 아닙니다. 범위 축소 전략에 대한 자세한 내용은 PCI QSA(Qualified Security Assessor) 또는 PCI 표준 위원회에 문의하십시오.

### 1.2.5. 보상 컨트롤

이 워크북에서는 AWS 구현에 대한 보상 컨트롤을 다루지 않습니다. 그러나 PCI 규정에 따라 평가자의 확인을 받은 경우에는 AWS 에서 보상 컨트롤을 사용할 수 있습니다.

# 2. AWS PCI 규정 준수 개요

이 단원에서는 AWS PCI 규정 준수의 일반적인 개요를 제공합니다.

자세한 내용은 Amazon 의 AWS PCI 레벨 1 FAQ 를 참조하십시오.

## 2.1. AWS PCI 규정 준수 상태

AWS 는 현재 PCI DSS 규정 준수 레벨 1 서비스 공급자입니다. 가맹점 및 기타 서비스 공급자는 AWS 를 사용하여 자체 PCI 규정 준수 환경을 설정할 수 있습니다. 그러나 AWS 는 공동 책임 모델을 기반으로 운영됩니다. AWS 가 PCI DSS 규정을 준수한다는 이유만으로 호스팅 대상 고객의 환경에까지 해당 규정이 자동으로 확대 적용되는 것은 아닙니다.

AWS 고객은 AWS 내 환경과 관련된 PCI 규정 준수의 모든 측면을 책임집니다. 여기에는 AWS 서비스 구성, 게스트 운영 체제 및 필수 보안 컨트롤(IDS, 바이러스 백신 등)이 포함됩니다.

AWS 가 PCI 규정을 준수하는 서비스 공급자이기는 하지만, AWS 호스팅을 이용하는 조직에서도 반드시 PCI 규정에 따라 AWS 인프라를 평가해야 하는 것은 아닙니다. 평가자는 인프라의 규정 준수 여부를 확인하기 위해 AWS 의 AOC(규정 준수 증명) 및 책임 매트릭스 문서만 검토하면 됩니다.

## 2.2. AWS PCI 규정 준수 범위

PCI 규정 준수에 대한 Amazon 의 AWS 서비스 공급자 확인 평가에는 AWS 관리 환경과 AWS GovCloud(미국) 리전 등의 기본 인프라가 포함됩니다.

최신 AWS PCI DSS 평가에는 대부분의 AWS 서비스가 포함되었습니다. 아래 목록에 이러한 규정 준수 서비스와 해당 기능이 설명되어 있습니다.

| 서비스 | 설명 |
|---|---|
| Auto Scaling | 자동화된 이벤트 기반 인스턴스 프로비저닝 |
| AWS CloudFormation | AWS 리소스의 템플릿 생성 및 배포 |
| Amazon CloudFront | 콘텐츠 전송 웹 서비스 |
| AWS CloudHSM | 하드웨어 보안 모듈에 대한 클라우드 액세스 |
| AWS CloudTrail | AWS API 호출에 대한 보고 |
| AWS Direct Connect | AWS 에 대한 직접적, 프라이빗, 전용 연결 |
| Amazon DynamoDB(DDB) | 확장 가능하고 가용성 높은 NoSQL 데이터 스토어 |
| Amazon Elastic Beanstalk | 웹 애플리케이션 배포 및 프로비저닝 |
| Amazon Elastic Block Store(EBS) | EC2 인스턴스에 대한 블록 레벨 스토리지 |
| Amazon Elastic Compute Cloud(EC2) | 확장 가능한 클라우드 머신 인스턴스 |
| Elastic Load Balancing(ELB) | 애플리케이션 내결함성 및 로드 밸런싱 |

| | |
|---|---|
| Elastic MapReduce(EMR) | 빅 데이터 서비스 |
| Amazon Glacier | 데이터 보관 스토리지 |
| AWS Management Console | 모든 AWS 서비스 관리용 웹 인터페이스 |
| AWS Identity and Access Management(IAM) | 액세스 컨트롤 및 키 관리 |
| AWS Key Management Service(KMS) | 데이터 암호화 키 관리 |
| Amazon Redshift | 고용량 데이터 웨어하우징 |
| Amazon Relational Database Service(RDS) | DBaaS(Database as a service) |
| Amazon Route 53 | 확장 가능하고 가용성 높은 Domain Name System(DNS) |
| Amazon Simple Storage Service(S3) | 모든 용량의 데이터 저장 및 검색 |
| Amazon SimpleDB(SDB) | 가용성 높고 유연한 비 관계형 데이터 스토어 |
| Amazon Simple Queuing Service(SQS) | 메시지 대기열 서비스 |
| Amazon Simple Work Flow(SWF) | 애플리케이션 구성 요소를 조정하기 위한 서비스 |
| Amazon Virtual Private Cloud(VPC) | 논리적으로 분리되어 프라이빗 네트워크로 기능하는 AWS 네트워크의 부분 |
| Amazon EC2 Container Service(Amazon ECS) | 호스팅된 확장형 도커 컨테이너 인스턴스 |
| AWS Config | AWS 리소스 인벤토리, 변경 기록, 변경 알림 |
| AWS 웹 애플리케이션 방화벽(AWS WAF) | 웹 기반 공격으로부터 CloudFront 가속화 웹 사이트 보호 |

AWS 에 대한 PCI 규정 준수는 다음 리전, 가용 영역 및 엣지 로케이션에 적용됩니다(2015 년 7 월 기준).

- 미국 동부(버지니아 북부)
- 미국 서부(오레곤)
- 미국 서부(캘리포니아 북부)
- AWS GovCloud(미국)(오리건)
- EU(아일랜드)
- 아시아 태평양(싱가포르)
- 아시아 태평양(도쿄)
- 아시아 태평양(시드니)
- 남아메리카(상파울루)

### 2.2.1. 범위 외부의 AWS 서비스

AWS 는 새로운 서비스를 끊임없이 개발하여 배포하고 있습니다. AWS 의 현재 PCI 증명에서 새로운 서비스를 모두 다루는 것은 아니지만, 사용자 환경에서는 여전히 해당 서비스를 이용할 수 있습니다. 해당 서비스를 사용하는 경우 평가자가 구성을 검토하여 PCI 규정을 준수하는지 확인해야 합니다.

예를 들어 *AWS Certificate Manager* 는 최신 AWS 서비스 공급자 평가를 기준으로 범위에 속하지 않습니다. 범위 내 웹 애플리케이션에 *AWS Certificate Manager* 를 쓰는 경우, 해당 PCI 요건에 부합하는 사용임을 증명해야 합니다. 그러나 *AWS Certificate Manager* 는 AWS 의 규정 준수 인프라에서 실행됩니다. 따라서 서비스 자체는 규정을 준수하는 것이 아니지만, 서비스가 실행되는 인프라는 규정에 맞을 수 있습니다.

## 2.3. AWS PCI 규정 준수 책임

PCI 요구 사항에 대한 책임 당사자를 결정하는 것은 클라우드 호스팅의 가장 복잡한 측면 중 하나입니다. 이 단원에서는 AWS 호스팅 환경에 대한 PCI 규정 준수 평가를 정의 및 구성하는 방법을 대략적으로 설명합니다.

이 워크북에서는 규정 준수를 위한 요구 사항 중 AWS 에서 처리할 수 있는 부분과 고객이 직접 처리해야 하는 부분을 소개합니다. AWS 가 처리하는 부분이 정확히 정의된 AWS PCI DSS "책임 매트릭스"를 참조하십시오. 부록 B 에 이 매트릭스가 요약되어 있습니다. AWS 가 처리하지 않는 요구 사항 또는 공동 책임 범위에 대해서는 고객 조직 측에서 요구 사항이 충족되도록 할 책임이 있습니다.

또한 고객은 임의로 PCI 요구 사항을 무시할 수 없으며, 모든 요구 사항을 충족해야 합니다. 그러나 고객 조직과 관련이 없는 요구 사항도 있을 수 있습니다. 고객에게 해당되는 요구 사항과 그렇지 않은 요구 사항은 PCI 평가자가 명확히 설명해 줍니다.

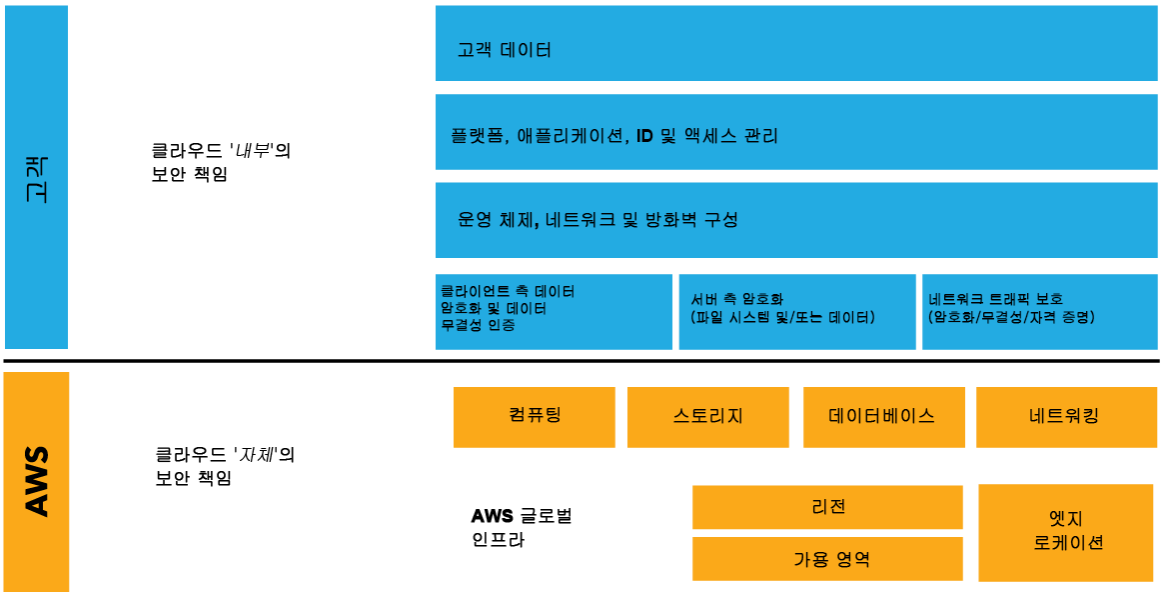


그림 1 – AWS 공동 책임 개요

### 2.3.1. Amazon 책임 - 클라우드 *자체의* 보안

Amazon 은 고객이 규정 준수를 위해 사용할 수 있는 PCI 규격 환경을 유지 관리할 책임이 있습니다. 이것을 "클라우드 ***자체의*** 보안"이라고 합니다. AWS 는 매년 준수 여부를 검증하여 그 결과를 AWS 의 규정 준수 증명서(AOC)에 기록합니다. AWS 고객은 복사본을 요청할 수 있습니다(서명된 비공개 계약 포함).

### 2.3.2. 고객 책임 - 클라우드 *내부의* 보안

고객은 AWS 에서 규정 준수 환경을 설계, 구축 및 유지 관리할 책임이 있습니다. 이것을 "클라우드 ***내부의*** 보안"이라고 합니다.

AWS 에서 환경을 구축할 때 해당 환경의 일부가 AWS 의 규정 준수 인프라를 사용하기 때문에 규정을 준수합니다. 그러나 PCI 규정 준수에 대한 최종 책임은 고객의 조직(AWS 가 아님)에 있습니다. 자세한 내용은 부록 B 의 "책임 매트릭스"를 참조하십시오.

# 3. 일반 PCI DSS 지침

이 단원에는 AWS 서비스를 사용하여 12 가지 최상위 PCI 요구 사항을 충족하기 위한 일반적인 지침과 전략이 나와 있습니다.

## 3.1. 요구 사항 1: 카드 소지자 데이터를 보호하기 위한 방화벽 구성 설치 및 유지 관리

다음 AWS 서비스는 PCI 에 대한 방화벽 및 네트워크 조각화 요구 사항을 지원하는 데 도움이 될 수 있습니다.

- Amazon Virtual Private Cloud(Amazon VPC)
- Amazon EC2 보안 그룹
- VPC 네트워크 ACL

아래 항목에서는 이러한 서비스를 활용하여 요구 사항 1 을 준수하기 위한 전략과 고려 사항을 설명합니다.

### Amazon VPC

VPC 는 논리적으로 분리되어 고객의 AWS 계정 내부에서 프라이빗 네트워크를 생성하는 AWS 네트워크의 부분입니다. VPC 를 사용하면 고객은 마치 인터넷에 연결되지 않은 실제 네트워크인 것처럼 서로 연결되지 않은 여러 환경을 설정할 수 있습니다. AWS 네트워크는 양식이 잘못되었거나 주소가 수정된 패킷이 VPC 경계 주위에 호핑하지 않도록 방지합니다. VPC 는 설계 시 L2 브로드캐스트 트래픽이 필요하지 않습니다. 그러면 AWS 플랫폼 내부에서 IP 주소의 스푸핑 가능성이 크게 줄어들고, VPC 를 사용하는 고객 환경에 대하여 요구 사항 1.3.3 의 의도를 충족합니다. 게다가 AWS 를 플랫폼으로 사용하는 것은 AOC 에 명시된 바와 같이 요구 사항 1.3.3 을 준수합니다. 이렇게 되면 AWS 는 AWS 주변에서 인바운드 트래픽을 필터링하고 스푸핑 방지를 실행하는 상태가 됩니다. VPC 내부의 스푸핑 방지 기능은 고객에게도 혜택이 돌아가지만, 사용자 네트워크로 향하는 모든 인바운드 연결에 스푸핑 방지 대책이 작용하는지 반드시 검증해야 합니다.

VPC 를 일부로 다른 네트워크로 연결하는 일은 가능합니다. 예를 들어 NAT 인스턴스, 탄력적 IP, 기타 리소스와 결합한 인터넷 게이트웨이는 인터넷 액세스를 제공할 수 있습니다. VPC 피어링과 구성이 불량한 라우팅 테이블은 VPN 끼리 연결할 수 있습니다. 그리고 아래 단원 4 에서 확인하겠지만, 온프레미스 네트워크를 클라우드로 확장하기 위해 VPN 또는 AWS Direct Connect 를 사용하는 것도 가능합니다.

**NOTE:** *동일한 VPC 내의 모든 서브넷 사이에는 제거할 수 없는 기본 경로가 있습니다.*

### EC2 보안 그룹

보안 그룹은 설정된 연결을 추적하고 세션과 연결된 트래픽만 반환하는 AWS EC2 의 상태 저장 방화벽 구성 요소입니다. 보안 그룹 ACL(액세스 제어 목록)은 요구 사항 1.3.6 을 준수하기 위해 IP 주소, 포트 및 프로토콜 레벨에서 인스턴스의 왕복 트래픽을 제한하는 데 사용할 수 있습니다.

### VPC 네트워크 ACL

VPC 네트워크 ACL 은 서브넷 레벨에서 적용되지만, 상태 저장 방식이 아니며 이것만으로는 요구 사항 1.3.6 을 충족할 수 없습니다.

### 기타 전략 및 고려 사항

단원 4 에 나오는 참조 아키텍처처럼 단순한 환경에서는 전용 클라우드 방화벽 AMI 를 사용하라는 것이 Anitian 의 권고 사항입니다. 이것은 분명히 상태 저장 방화벽일 뿐 아니라, 침입 방지 등 여러 가지 중요 보안 기능도 추가로 제공할 수 있습니다(요구 사항 11.4 에서 IDS/IPS 의 필요성 지정).

AWS Marketplace 에는 Fortinet, Palo Alto, CheckPoint 등 여러 회사의 방화벽 Amazon 머신 이미지(AMI)가 있습니다. 이러한 방화벽 인스턴스는 공급업체의 특정 라이선스가 필요할 수 있지만, 친숙한 관리 인터페이스와 고급 기능을 제공합니다.

요구에 맞는 충분한 애플리케이션 용량을 확보하기 위해 Auto Scaling 을 쓰는 등 더 복잡하거나 동적인 AWS 아키텍처에 기존 방화벽을 쓰면 환경을 관리하기가 복잡합니다. 이런 환경에서는 보안 그룹과 호스트 기반의 방화벽을 써서 CDE 를 위한 세분화를 달성할 수 있습니다.

## 3.2. 요구 사항 2: 시스템 암호 및 기타 보안 파라미터에 공급업체에서 제공한 기본값 사용 안 함

다음 AWS 서비스는 PCI 의 호스트 강화 요구 사항을 지원하는 데 도움이 될 수 있습니다.

- Amazon Elastic Compute Cloud(Amazon EC2)

Amazon EC2 를 활용하여 요구 사항 3 을 준수하기 위한 전략과 고려 사항은 아래에서 설명합니다.

### Amazon EC2

Amazon 에서 제공하는 AMI 를 사용하여 EC2 인스턴스를 생성할 때, AWS 는 고유하게 생성된 프라이빗 키로 암호화된 고유의 관리자 및 루트 암호를 생성합니다. 이 기능은 요구 사항 2.1 준수를 지원하는 데 도움이 됩니다.

또한 기본 사용자 계정이 없으므로 명시적으로 생성해야 합니다.

### 기타 전략 및 고려 사항

비 Amazon 이미지를 사용하는 경우 기본값이 변경되는지 확인할 책임이 있습니다. 해당 이미지에 대한 관련 설명서를 참조하십시오.

AWS AOC 는 AWS 서비스에 대한 기본 보안 구성 관리를 다룹니다. 그러나 EC2 인스턴스에 대한 보안 구성 표준을 생성하고 구현하는 것은 고객의 책임입니다. AWS Marketplace 에는 이 요구 사항에 도움이 될 수 있는 다양한 솔루션이 있습니다.

---

**NOTE:** *Anitian 은 베이스 서버 및 강화된 웹 서버로 사용 가능한 모든 OS 에 대해 강화된 AMI 를 생성했습니다. 여기에는 PCI DSS 요구 사항 2.2 에 요구한 대로 수행된 강화 단계를 기록한 보안 구성 표준 지원이 포함됩니다.*

---

## 3.3. 요구 사항 3: 저장된 카드 소지자 데이터 보호

다음 AWS 서비스는 저장된 카드 소지자 데이터(CHD)에 대한 PCI 의 암호화 및 키 관리 요구 사항을 지원하는 데 도움이 될 수 있습니다.

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

이러한 서비스를 활용하여 요구 사항 3 을 준수하기 위한 전략과 고려 사항은 아래에서 설명합니다.

### Amazon EBS

AWS 는 정보를 안전하게 저장하기 위한 다양한 방법을 지원합니다. EBS 루트가 아닌 볼륨과 S3 버킷은 AES-256 을 사용하는 볼륨 레벨 암호화를 지원합니다. EBS 볼륨의 경우 EBS 는 FIPS 140-2 규정 준수 인프라를 사용하여 암호화 키를 관리합니다.

인스턴스의 암호화된 볼륨에 CHD(예: 전용 DB 서버 인스턴스의 파일 시스템에 있는 DB 파일)를 저장하는 경우, CHD 가 요구 사항 3.4.1 을 준수하려면 추가 암호화가 필요합니다. 이 사항은 AWS 에 고유하지 않으며 완전성 및 명확성을 위해 언급됩니다.

---

**NOTE:** *모든 EC2 인스턴스 유형이 암호화된 EBS 볼륨을 지원하는 것은 아닙니다. EBS 암호화를 참조하십시오.*

---

### Amazon S3

Amazon S3 는 단순 데이터 스토리지 서비스입니다. 이 서비스는 AES-256 을 사용하여 저장된 객체를 암호화할 수 있으며, 세 가지 키 관리 메커니즘을 지원합니다 (서버 측 암호화 참조).

- **Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3)**

  S3 버킷(Management Console 안에서)의 객체에 대해 SSE-S3 를 활성화하면 S3 는 고유의 데이터 암호화 키를 사용하여 객체를 암호화합니다. 이 데이터 암호화 키는 S3 서비스가 매년 교체하는 마스터 키로 암호화됩니다.

- **AWS KMS 관리형 키를 사용한 서버 측 암호화(SSE-KMS)**

  SSE-KMS 는 엔벌로프 키를 이용해 각 객체의 데이터 암호화 키를 암호화합니다. 이렇게 하면 데이터 암호화 주체에 대한 통제력이 커지며 키 사용의 감사 로그가 제공됩니다. KMS 는 다음 단원에서 논의합니다.

- **고객 제공 키를 사용한 서버 측 암호화(SSE-C)**

  SSE-C 를 사용하면 자신을 키를 사용하고 직접 관리할 수 있습니다. S3 는 이 키를 저장하지 않으며, 나중에 데이터를 가져올 때 키 사용을 확인할 수 있도록 메시지 인증 해시만 저장합니다.

기본적으로 S3 는 SSE-S3 를 사용하도록 구성됩니다. KMS 또는 고객이 제공하는 키를 사용하려면 콘솔이나 REST API 를 통해 객체를 업로드할 때 키 관리 유형을 지정해야 합니다. 자세한 내용은 S3 업로드 객체를 참조하십시오.

### AWS KMS

KMS 는 AWS 의 암호화 키 관리 서비스입니다. KMS 는 매년 Management Console 을 통해 자동 키 교체를 제공합니다. 자세한 내용은 Amazon 의 KMS 암호화 세부 정보 문서를 참조하십시오.

AWS KMS 에는 프로그래밍 방식 혹은 타사 지원을 위한 API 문서도 있습니다.

KMS 는 고객 마스터 키(CMK)를 키 암호화 키(KEK)로 사용하고, 백업 키는 데이터 암호화 키로 사용합니다. 키 암호화를 활성화하면 백업 키를 교체합니다.

키 교체를 활성화하면 매년 새 CMK 와 관련 백업 키(HBK)를 생성합니다. 이렇게 새로 생성된 키를 앞으로 계속 사용하며, 기존의 CMK/HBK 는 암호화에만 활용합니다. 또한 언제든지 수동으로 새 CMK/HBK 를 생성하고 현재 활성화된 키로 지정할 수 있습니다.

**NOTE:** *CMK/HBK 를 비활성화하면 더 이상 사용할 수 없지만, 현재 비활성화된 키에 의존하는 연결된 EBS 볼륨이 계속 작동합니다. 그 볼륨을 인스턴스에서 분리할 경우 키를 다시 활성화해야 그 볼륨을 다시 사용할 수 있습니다.*

CloudTrail 은 모든 AWS KMS 작업(키 생성, 데이터 암호화, 키 교체 등)을 사용자가 지정한 S3 버킷에 있는 CloudTrail 로그 파일에 기록합니다.

### Amazon RDS

Amazon RDS 는 암호화 스토리지 외에도 두 가지 데이터베이스 암호화 방법을 지원합니다. RDS 는 Amazon KMS 관리 키를 이용해 기본 스토리지를 암호화합니다. 이렇게 해서 저장된 데이터를 보호합니다. RDS 는 또한 Microsoft SQL 및 Oracle 인스턴스에 대해 Transparent Data Encryption(TDE)을 지원합니다.

IAM 정책은 RDS 인스턴스에 액세스할 수 있는 사람과 수행할 수 있는 작업을 제어합니다. 그러나 RDS 인스턴스의 데이터베이스는 내부의 자체적인 플랫폼별 메커니즘을 이용하여 데이터 액세스를 관리합니다. RDS 의 CDE 데이터베이스에서 PCI 관련 계정 및 암호 정책을 구성해야 합니다.

## 기타 전략 및 고려 사항

EC2 인스턴스에서 자체 DB 를 실행하는 경우 고객은 DB 내에 있는 모든 CHD 의 암호화를 전적으로 관리할 책임이 있습니다. 사용 중인 특정 DB 에 적합한 표준 전략을 사용하여 이 암호화를 수행해야 합니다. 일반적인 예에는 필드 또는 열 레벨에서 CHD 의 프로그래밍 방식 암호화 또는 MS SQL 용 TDE 와 같은 DB 인스턴스 레벨의 암호화가 있습니다.

## 3.4. 요구 사항 4: 개방형 퍼블릭 네트워크를 통한 카드 소지자 데이터의 전송 암호화

다음 AWS 구성 요소는 PCI 의 전송 암호화 요구 사항을 지원하는 데 도움이 될 수 있습니다.

- 탄력적 로드 밸런서
- 네트워크 ACL
- 보안 그룹
- 고객 게이트웨이
- 가상 프라이빗 게이트웨이
- VPN 연결
- AWS Direct Connect

이러한 서비스를 활용하여 요구 사항 4 를 준수하기 위한 전략과 고려 사항은 아래에서 설명합니다.

### 탄력적 로드 밸런서

탄력적 로드 밸런서는 SSL/TLS 를 지원하며 내부 및 외부 연결용 보안 통신을 위해 암호화 처리를 오프로드합니다. SSL/TLS 협상은 보안 정책을 사용하여 구성됩니다. AWS 는 수많은 사전 정의 보안 정책을 제공합니다(자세한 내용은 ELB 보안 정책 테이블 참조). 고객이 직접 생성할 수도 있습니다. 보안 정책을 사용하여 SSL 프로토콜과 암호를 정의할 수 있으며, SSL 핸드셰이크 중 클라이언트 서버 협상을 위한 순서 기본 설정도 정의할 수 있습니다.

---

NOTE: *PCI DSS 3.1 에는 이렇게 명시되어 있습니다. "SSL 및 조기 TLS 는강력한 암호화로 간주되지 않으며 2016 년 6 월 30 일 이후에는 보안 컨트롤로 사용할 수 없습니다."*

---

### 보안 그룹 및 네트워크 ACL

보안 그룹과 네트워크 ACL 은 네트워크 포트를 기반으로 안전하지 않은 프로토콜 사용을 차단할 수 있습니다.

### 고객 게이트웨이, 가상 프라이빗 게이트웨이 및 VPN 연결

고객 게이트웨이, 가상 프라이빗 게이트웨이 및 VPN 연결을 사용하면 AWS VPC 로 연결되는 암호화된 VPN 터널을 설정할 수 있습니다. AWS 는 다양한 일반적인 VPN 솔루션을 지원하며(VPC FAQ 참조), 일반적인 텍스트 구성 파일도 지원합니다. 일치하는 엔드포인트를 구성할 수 있도록 AWS 에서 VPN 설정이 자동으로 생성됩니다. VPN 연결을 생성한 후(VPC 대시보드의 VPN 연결 섹션), 고객 엔드포인트를 설정하는 데 필요한 구성 파일을 다운로드할 수 있습니다. 사용된 암호화 방법은 구성 파일에서 확인할 수 있습니다(SHA1/AES 128). 구현의 세부 정보는 아래 4.3.4.5 단원을 참조하십시오.

### AWS Direct Connect

Direct Connect 는 MPLS 와 마찬가지로 고객 환경과 AWS 간의 전용 고속 연결을 제공합니다. Direct Connect 자체는 암호화된 연결이 아니므로 회로의 개인 전보 보호를 확인해야 합니다. 구현에 따라 요구 사항 4.1 을 준수하기 위해 추가 컨트롤이 필요할 수 있습니다.

### 기타 전략 및 고려 사항

웹 서버와 같이 EC2 인스턴스에서 실행되는 인터넷 경계 서비스에 대해 보안 전송 암호화를 구성하는 것은 고객의 책임입니다. 요구 사항 2 를 위한 호스트 강화 과정에서 이 작업을 실행해야 합니다.

또한 환경 내에서 실행되는 상업용 방화벽 또는 VPN AMI 에서 VPN 을 구현할 수도 있습니다. 고객은 요구 사항 4 에 따라 장치를 구성할 책임이 있습니다.

## 3.5. 요구 사항 5: 모든 시스템을 모든 맬웨어로부터 보호하고, 정기적으로 바이러스 백신 소프트웨어 또는 프로그램 업데이트

AWS 는 EC2 인스턴스에 대한 바이러스 백신 보호를 제공하지 않습니다. 고객은 PCI 요구 사항 5 에 정의된 대로 모든 인스턴스에 대해 적절한 바이러스 백신 검사를 실행하도록 할 책임이 있습니다.

AWS Marketplace 에서 수많은 바이러스 백신 솔루션을 사용할 수 있습니다.

## 3.6. 요구 사항 6: 보안 시스템 및 애플리케이션 개발 및 유지 관리

AWS 는 EC2 인스턴스에 대한 취약성 및 패치 관리를 제공하지 않습니다. AMI 는 정기적으로 업데이트되지만, 시작되어 실행 중인 인스턴스는 다른 호스트와 같이 관리해야 합니다. 예를 들어, Amazon Linux AMI 에 대한 업데이트 목록은 AWS Linux 보안 센터를 참조하십시오.

AWS Marketplace 에서 요구 사항 6.1 및 6.2 를 준수하는 데 도움이 되는 취약성 및 패치 관리 솔루션을 사용할 수 있습니다.

한편, 보안 소프트웨어 개발(요구 사항 6.3) 및 변경 컨트롤(요구 사항 6.4)에 대한 PCI 요구 사항을 직접 처리하는 AWS 서비스는 없습니다. 6.4). CodeDeploy 및 CodeCommit 는 PCI 요구 사항과 직접 관련은 없지만 일반적인 소스 코드 관리 및 배포에 이용할 수 있습니다.

단, 네트워크 조각화 기술(위의 요구 사항 1 에서 설명)로 프로덕션 환경과 개발 환경을 분리할 수 있습니다(요구 사항 6.4.1).

**NOTE:** *AWS Config 는 AWS 자체의 리소스 변경 사항을 기록하지만, EC2 인스턴스 내의 애플리케이션 변경 사항은 기록하지 않습니다.*

### AWS WAF 와 Amazon CloudFront

AWS WAF(웹 애플리케이션 방화벽)는 PCI DSS 검증을 마친 자동 기술 솔루션으로 PCI DSS 요구 사항 6.6 을 충족합니다. WAF 서비스는 콘텐츠 전송 가속화를 위해 Amazon CloudFront 를 이용하는 퍼블릭 웹사이트를 웹 기반 공격으로부터 보호하도록 지원합니다.

NOTE: *Amazon CloudFront 자체는 위 단원 2.2 의 PCI 준수 AWS 서비스 목록에 없으나, AWS WAF 는 CloudFront 가속화된 웹 애플리케이션만 보호합니다.*

요구 사항 6.6 은 WAF 또는 웹 애플리케이션 보안 테스트로 충족할 수 있습니다. Anitian 은 항상 모든 WAF 배포 시 웹 애플리케이션의 알려진 취약성을 모두 확실히 해결하는 방향으로 준비하도록 웹 애플리케이션 보안 테스트를 함께 수행할 것을 권장합니다.

## 3.7. 요구 사항 7: 업무상 알 필요가 있는 사용자만 카드 소지자 데이터에 액세스할 수 있도록 제한

다음 AWS 구성 요소는 PCI 의 액세스 제어 요구 사항을 지원하는 데 도움이 될 수 있습니다.

- AWS Identity and Access Management(IAM)
- AWS 디렉터리 서비스

### IAM

IAM 서비스는 AWS 내의 역할 기반 액세스 제어를 지원합니다. 그러나 IAM 서비스 내에서 사용자 역할 및 권한을 관리하는 것은 고객의 책임입니다.

IAM 은 사용자, 그룹 및 역할과 암호화 키 관리를 지원합니다.

### Directory Service

Directory Service 는 Simple AD 라고 부르는 인스턴스를 한 개 이상 생성할 수 있는 Microsoft Active Directory(AD) 호환 디렉터리 서비스입니다. 이 인스턴스를 독립형 Simple AD 로 배포하거나 온프레미스 Microsoft AD 인프라에 연결할 수 있습니다.

디렉터리 서비스는 AWS 리소스에 대한 액세스를 관리할 수 있으며 Microsoft AD 호환 시스템과 애플리케이션도 관리할 수 있습니다.

Windows Server 내에 포함된 Microsoft Active Directory Administration 도구와 같은 타사 도구를 사용하여 AWS Directory Service 를 관리해야 합니다. 자세한 내용은 관리자 가이드 디렉터리 관리를 참조하십시오.

**NOTE:** *Simple AD 디렉터리는 Microsoft Active Directory 웹 서비스 인터페이스를 지원하지 않습니다.*

### 기타 전략 및 고려 사항

최소 권한이 명확히 설명된 상태로 모든 사용자 역할과 권한이 기록되었는지 확인하는 것은 고객의 책임입니다.

## 3.8. 요구 사항 8: 시스템 구성 요소에 대한 액세스 식별 및 인증

다음 AWS 서비스는 PCI 의 계정 관리 요구 사항을 지원하는 데 도움이 될 수 있습니다.

- IAM
- Directory Service

### IAM

IAM 은 잘못된 로그인 시도에 대한 계정 잠금(요구 사항 8.1.6), 최소 잠금 기간(요구 사항 8.1.7), 유효 세션 시간 초과(요구 사항 8.1.8) 등 예외적인 경우를 제외하고 요구 사항 8 에 따라 암호 정책을 지원합니다. IAM 으로 이를 충족하려면 PCI 규격의 외부 자격 증명 제공자를 이용하여 이러한 요구 사항 또는 Directory Service 를 적용해야 합니다.

**NOTE:** *IAM 은 EC2 인스턴스와 애플리케이션의 인증이 아닌, AWS 리소스에 대한 확인 및 액세스 관리에만 사용합니다.*

### Directory Service

Simple AD 는 Microsoft AD 가 사용하는 모든 암호 및 계정 정책 설정을 지원하여, 요구 사항 8 을 완전히 지원합니다(디렉터리 생성 참조).

### 기타 전략 및 고려 사항

EC2 인스턴스에서 실행되는 디렉터리 서비스의 경우, 요구 사항 8 에 따라 모든 암호 정책이 구성되었는지 확인하는 것은 고객의 책임입니다.

## 3.9. 요구 사항 9: 카드 소지자 데이터에 대한 물리적 접근 제한

AWS 의 AOC 는 요구 사항 9 에 대한 AWS 의 물리적 보안을 자세히 다룹니다. AWS 에서 전체 PCI 환경을 호스트하는 한 이 요구 사항은 해결됩니다.

AWS 의 AOC 는 AWS 외부에서 호스팅되는 범위 내 자산을 제외합니다.

## 3.10. 요구 사항 10: 네트워크 리소스 및 카드 소지자 데이터에 대한 모든 액세스 추적 및 모니터링

다음 AWS 서비스는 PCI 의 로그 관리 요구 사항을 지원하는 데 도움이 될 수 있습니다.

- AWS CloudTrail
- S3

### CloudTrail

AWS CloudTrail 서비스는 AWS 계정 내부의 리소스 액세스를 추적하고 모니터링하는 데 도움이 될 수 있습니다. CloudTrail 에서 지원되는 기본 구성 요소는 집계, 알림 및 보존입니다(요구 사항 10.5~10.7).

S3 버킷을 만들어 로그 파일을 수신하고 저장하며, CloudTrail 에서 필수 보안 이벤트 캡처를 활성화하도록(요구 사항 10.2) 확인하는 것은 고객의 책임입니다.

CloudTrail Event Record Body 는 요구 사항 10.3 의 특정 요소를 모두 지원합니다. 자세한 내용은 이벤트 참조 레코드를 참조하십시오.

### S3

CloudTrail 데이터에 대한 보존 정책은 S3 에 구성되어 있습니다. 기본적으로 보존 기간은 무제한이지만, 사용자가 완전히 구성 가능합니다(수명 주기 구성 참조).

**NOTE:** *요구 사항 10.7 을 비용 효율적으로 준수하는 방법으로, S3 수명 주기 구성을 사용해 보존 기간을 90 일로 설정하고 오래된 데이터를 장기 보존용(일 년 이상 필수적) Amazon Glacier 스토리지 서비스로 자동 보관할 수 있습니다.*

또한 CloudTrail 로그를 저장하는 S3 버킷에서 액세스 제어를 활성화해야 합니다. 여기에는 버킷 쓰기 액세스를 CloudTrail 로 제한하고 버킷 읽기 액세스를 권한 있는 사용자로 제한하는 작업이 포함됩니다.

### 기타 전략 및 고려 사항

Amazon 의 CloudTrail 은 로깅에 대한 PCI 요구 사항을 이행하는 기본 로깅 서비스입니다. CloudTrail 은 AWS 리소스 액세스에 대한 감사 로깅을 제공하지만 사용자가 AWS 에서 실행한 애플리케이션의 이벤트와 작업은 기록하지 않습니다. AWS Marketplace 에는 애플리케이션 로그 관리를 도와주는 Amazon 머신 이미지(AMI)가 Splunk, HP(ArcSight), Alert Logic 같은 회사에서 여럿 출시되어 있습니다.

보안 정보 및 이벤트 관리(SIEM) 제품을 이미 사용 중이라면, CloudTrail 은 그 제품으로 로그 수집이나 고급 이벤트 상호 연관에 사용하는 API 를 지원합니다. 자세한 내용은 SIEM 공급업체에 문의하십시오.

NTP(Network Time Protocol)가 요구 사항 10.4 를 준수하도록 EC2 인스턴스를 구성해야 합니다.

## 3.11. 요구 사항 11: 정기적으로 보안 시스템 및 프로세스 테스트

AWS 의 AOC 에서 불법 무선 액세스 지점의 감지를 자세히 다룹니다(요구 사항 11.1).

AWS 는 EC2 인스턴스 내에서 취약성 검사(요구 사항 11.2), 침투 테스트(요구 사항 11.3), 침입 방지(요구 사항 11.4) 또는 파일 변경 감지(요구 사항 11.5)를 제공하지 않습니다. 그러나 AWS Marketplace 에는 이러한 여러 요구 사항을 지원하는 수많은 솔루션이 있습니다. Anitian 은 네트워크 침투 테스트를 제공하며 웹 애플리케이션 보안 테스트도 제공합니다.

**NOTE:** *AWS 를 통해 침투 테스트를 예약하고 승인해야 합니다. 자세한 내용은 AWS 침투 테스트를 참조하십시오.*

## 3.12. 요구 사항 12: 모든 직원에게 정보 보안을 요구하는 정책 유지

AWS 는 요구 사항 12(및 기타 PCI 요구 사항)에 지정된 정책 문서를 제공하지 않습니다. 이 자료를 고객이 직접 작성해야 합니다.

## 3.13. 부록 A.1: 공유 호스팅 공급자는 카드 소지자 데이터 환경을 보호해야 함

EC2 인스턴스의 일부로 공유 호스팅을 제공하는 경우 사용자는 고객의 CHD 를 보호할 책임이 있습니다. 요구 사항 A.1 를 준수하도록 CDE 를 올바르게 조각화하고 분리해야 합니다. 다음 서비스는 이 작업에 도움이 될 수 있습니다.

- 요구 사항 1 - VPC, 보안 그룹
- 요구 사항 7 및 8 - IAM 및 Directory Service

## 3.14. 부록 A.2: SSL/조기 TLS 를 사용하는 엔터티를 위한 PCI DSS 추가 요구 사항

부록 A.2 를 특별히 지원하는 AWS 구성 요소는 없습니다. TLS 를 사용하는 모든 AWS 서비스는 TLS 버전 1.2 를 지원합니다.

## 3.15. 부록 A.3: 지정 엔터티 부가 검증(DESV: Designated Entities Supplemental Validation)

일부 조직에서 카드 브랜드 또는 취득자가 엔터티를 지정 엔터티로 요구할 수 있으며, 이에 따라 PCI DSS 3.2 부록 A.3 의 추가 요구 사항을 충족해야 합니다.

NOTE: *지정 엔터티가 되는 것은 공적인 프로세스이므로 카드 브랜드 혹은 취득자가 이를 의무화하지 않았다면 적용되지 않습니다.*

지정 엔터티로 선언하려는 엔터티는 반드시 기본 지침을 따라야 합니다.

- 대량의 CHD 취급
- 여러 장소 또는 다른 기업에서 CHD 집계
- 여러 번 또는 중대한 CHD 침해 경험

게다가 지정 엔터티에 대한 요구 사항이 일반적으로 우려하는 것은 PCI 준수 프로그램의 공식화입니다. A.3 의 하위 요건을 지원하는 AWS 구성 요소는 아래에서 다룹니다.

### 3.15.1. DE.1 PCI DSS 규정 준수 프로그램 실행

AWS 는 DE.1(및 기타 PCI 요구 사항)에 지정된 정책 또는 절차 문서를 제공하지 않습니다. 이 자료를 고객이 직접 작성해야 합니다.

### 3.15.2. DE.2 PCI DSS 범위 문서화 및 검증

세분화 제어 테스트와 CHD 검색 절차를 기반으로 정확하면서도 조직 및 기술 변화 이후에도 유효한 PCI DSS 범위 검증에 대하여 DE.2 요구 조건을 직접 다루는 AWS 서비스는 없습니다.

그러나 위 단원 3 에서 명시한 것처럼 이러한 추가적 검증 요구 사항을 충족하는 노력에서 정보 공급에 도움이 되는 AWS 서비스는 있습니다. 예:

- AWS Config 는 AWS 구성 요소의 변동을 식별하여 AWS 호스팅 CDE 네트워크 혹은 세분화의 변동 여부를 판단할 수 있습니다.
- S3 는 저장된 객체에 프로그래밍 및 명령줄 액세스를 지원하여 CHD 검색 노력을 지원합니다.
- CloudTrail 과 CloudWatch 는 평가 범위나 규정 준수 상태에 영향을 주는 환경 변화를 감지하는 데 사용할 수 있습니다.
- IAM 을 사용해 AWS 구성 요소에 읽기 전용 액세스를 할당하면 GRC(관리, 위험 및 규정 준수) 솔루션을 허용하거나 담당자가 증거를 수집할 수 있습니다.

---

NOTE: *테스트 세분화조차도 AWS 를 통해 침투 테스트를 예약하고 승인해야 한다는 사실을 잊지 마십시오. 자세한 내용은 AWS 침투 테스트를 참조하십시오.*

---

### 3.15.3. DE.3 PCI DSS 가 일상 비즈니스(BAU) 활동에 통합되었는지 검증

특정 AWS 서비스는 매년 현재 PCI DSS 버전에 대비하여 평가합니다. AWS 평가 범위에 들어간 AWS 서비스는 AWS 의 서비스 공급자 AOC 로 문서화됩니다. 위 단원 2 에서 언급했듯이, AWS 고객은 해당 AOC 의 사본을 요청할 수 있습니다(비밀 유지 계약 체결 시).

AWS 의 AOC 와 AWS PCI DSS "책임 매트릭스"를 참고하면 사용자의 CDE 가 과거와 현재, 미래에 사용하는 모든 기술이 PCI 요구 사항을 충족하는지 알 수 있습니다.

### 3.15.4. DE.4 카드 소지자 데이터 환경에 대한 논리적 액세스 제어 및 관리

위 DE.2 처럼, DE.4 에서 요구하는 연 2 회 액세스 리뷰를 직접 처리하는 AWS 서비스는 없습니다. 그러나 단원 3 에서 명시한 것처럼 이러한 추가적 검증 요구 사항을 충족하는 노력에서 정보 공급에 도움이 되는 AWS 서비스는 있습니다. 예:

#### IAM

인벤토리에 할당된 IAM 은 정책에 액세스하여 평가 범위에 있는 AWS 리소스에 대한 사용자와 그룹의 액세스 권한을 판단합니다.

NOTE: *대부분의 AWS 리소스 액세스는 IAM 정책에서 제어하지만, 어떤 인스턴스에는 액세스를 바로 할당할 수 있습니다. 예를 들어 S3 는 사용자당 열거하기가 까다로운 버킷 액세스 정책이 있을 수 있습니다.*

#### Directory Service

사용자 환경에서 자격 증명 및 액세스 관리용으로 Directory Service 를 사용할 경우, AWS 안의 서비스 자체에 액세스한 기록도 문서화하고 6 개월에 한 번 이상 검토해야 합니다.

### 3.15.5. DE.5 의심스러운 이벤트 식별 및 대응

AWS 는 DE.5(및 기타 PCI 요구 사항)에서 요구하는 사고 감지, 대응 또는 분석 방법론을 제공하지 않습니다. 이 자료를 고객이 직접 작성해야 합니다.

그러나 CloudTrail 과 CloudWatch 를 의심스러운 이벤트 감지에 사용해 사고 대응 프로그램을 지원할 수 있습니다.

# 4. 참조 아키텍처

이 단원에서는 PCI 규정 준수 환경을 구축하거나 액세스하는 데 도움이 되는 세 가지 일반적인 AWS 참조 아키텍처를 정의합니다.

1. **전용**: 다른 환경에 연결되지 않은 AWS PCI 환경
2. **조각화**: 더 큰 AWS 환경에 속하는 CDE 및 범위 내 시스템
3. **Connected**: AWS 및 온프레미스 항목이 모두 있는 환경

이러한 참조 아키텍처는 Microsoft Windows 플랫폼을 웹 및 애플리케이션 티어에 사용하고 Amazon RDS 를 데이터베이스 티어에 사용합니다. 다른 OS 플랫폼에는 약간 다른 구성이 있을 수 있지만, 아키텍처는 일반적으로 동일합니다.

**NOTE:** *AWS 호스팅 환경에서 규정 준수 범위를 결정하는 것은 온프레미스 환경의 범위 설정과 대체로 동일합니다. 규정 준수의 범위는 카드 소지자 데이터의 흐름과 사용 중인 세분화 전략에 따라 좌우됩니다.*

## 4.1. 아키텍처 1: 전용

이 아키텍처는 전용 Amazon AWS 계정에 호스팅되고 단일한 프라이빗 네트워크에 포함된 전자 상거래 웹 사이트를 보여 줍니다.

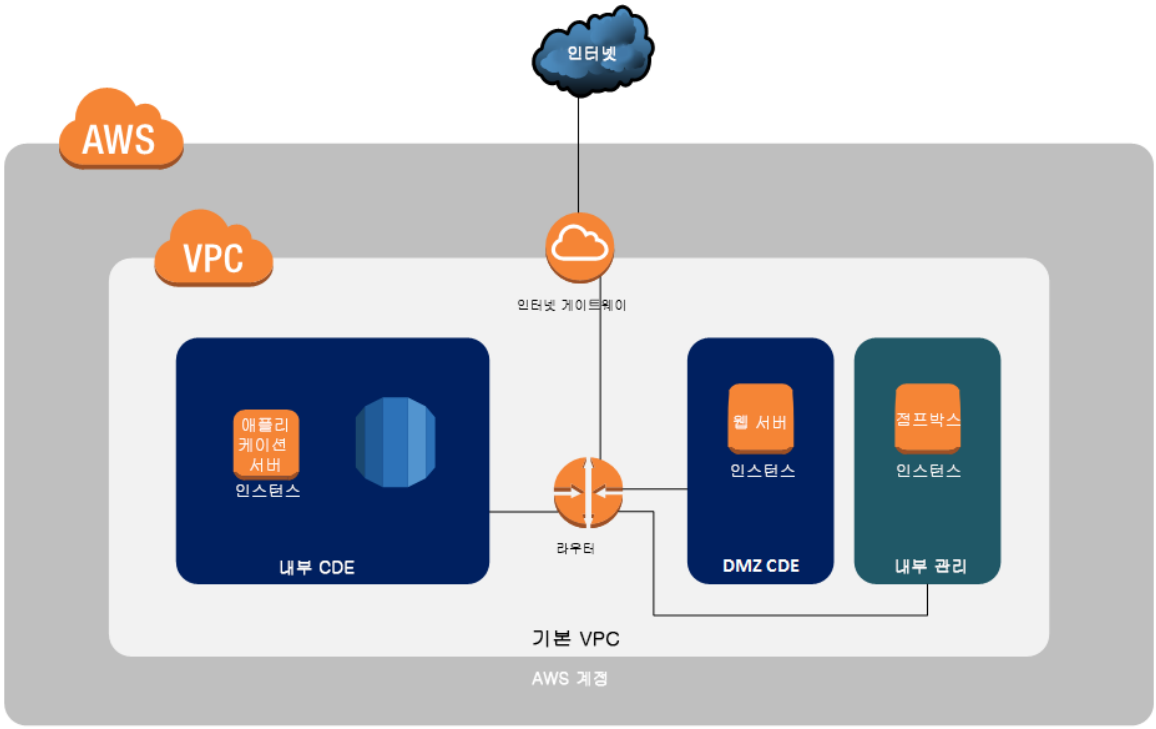



*그림 2 - 독립형 전자 상거래 웹 사이트 아키텍처*

### 4.1.1. 개요

전용 참조 아키텍처에는 기본 VPC 에 서브넷이 세 개 있습니다.

- DMZ CDE
- 내부 CDE
- 내부 관리

DMZ 는 웹 서버 EC2 인스턴스가 포함된 인터넷 경계 네트워크입니다.

범위 내 내부 서브넷에 점프박스가 포함되어 있으며, 이것은 CDE 인스턴스에 지원, 보안, 패치 적용, 기타 필수 서비스를 제공하고 관리하는 데 사용합니다.

내부 서브넷은 보안 그룹을 통해 DMZ 범위 내 인스턴스만 액세스할 수 있으며(아래에서 자세히 설명됨), 애플리케이션 서버 인스턴스 및 RDS 가 포함됩니다.

---

**NOTE:** *Anitian 은 참조 아키텍처를 실행하기 위해 강화 AMI 를 이용해 CloudFormation 스크립트를 생성합니다.*

---

### 4.1.2. PCI 범위

CDE 는 두 CDE 서브넷 안의 여러 시스템으로 구성됩니다.

- 웹 서버
- 애플리케이션 서버
- RDS DB 인스턴스

이 범위의 경우 웹 서버는 CHD 를 수락한 다음, CHD 는 애플리케이션 티어를 통해 스토리지용 DB 로 흐릅니다.

점프박스는 이 아키텍처에서 카드 소지자 데이터를 전송하거나, 처리하거나, 저장하거나, 혹은 달리 취급하지 않습니다. 점프박스를 전용 관리 네트워크에 놓으면 CDE 에서 격리되지만, CDE 내부의 호스트에 직접 연결되고 그 보안에 영향을 줄 수 있기 때문에 PCI 평가 범위에서는 제거되지 않습니다.

### 4.1.3. 적용 가능한 AWS 서비스

다음 AWS 서비스는 이 아키텍처에 대한 PCI 3.2 요구 사항 준수를 지원하는 데 도움이 됩니다.

| AWS 서비스 | 지원되는 PCI 요구 사항 |
|---|---|
| • 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>• 보안 그룹<br>• AMI<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 |
| • 구성 | 2.4, 11.5 |
| • VPC | 1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7 |

### 4.1.4. 확장 구축

이 단원에서는 참조 아키텍처를 확장 구축하기 위한 기본 단계를 설명합니다.

#### 4.1.4.1. IAM 그룹 생성 및 권한 할당

먼저, 누가 환경에 액세스할 수 있고 누가 환경을 관리할 수 있는지를 정의합니다. AWS 에서는 공유 기본값이 없도록 모든 계정과 암호를 명시적으로 정의해야 합니다.

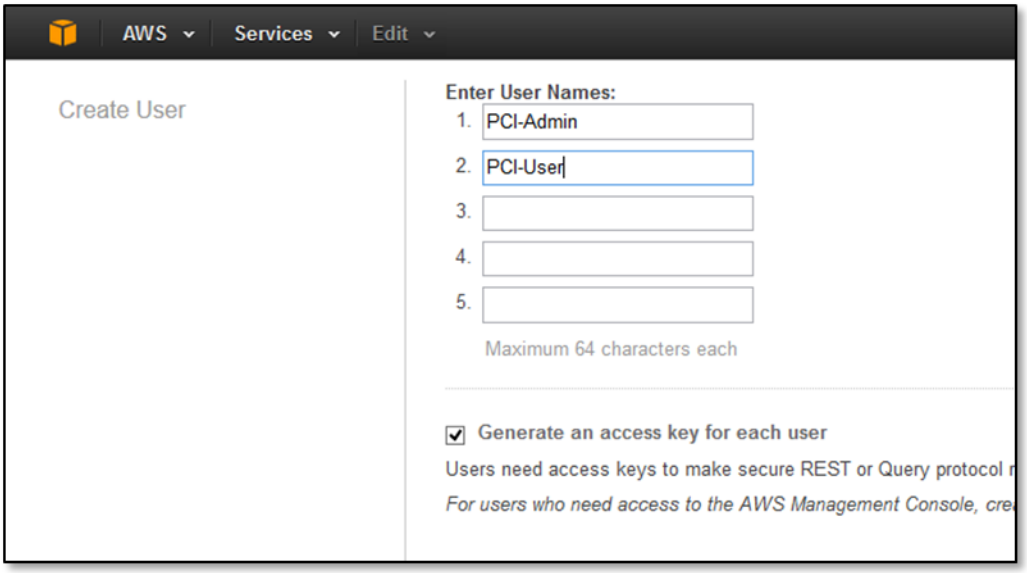



*그림 3 – 사용자 생성*

#### 4.1.4.2. 스토리지 암호화 키 생성

KMS 를 이용해 데이터 스토리지 위치를 암호화할 키를 생성합니다. 이 아키텍처에서는 카드 소지자 데이터(CHD)가 포함될 데이터베이스 인스턴스에 대해 최소 하나의 키가 생성되어야 합니다.

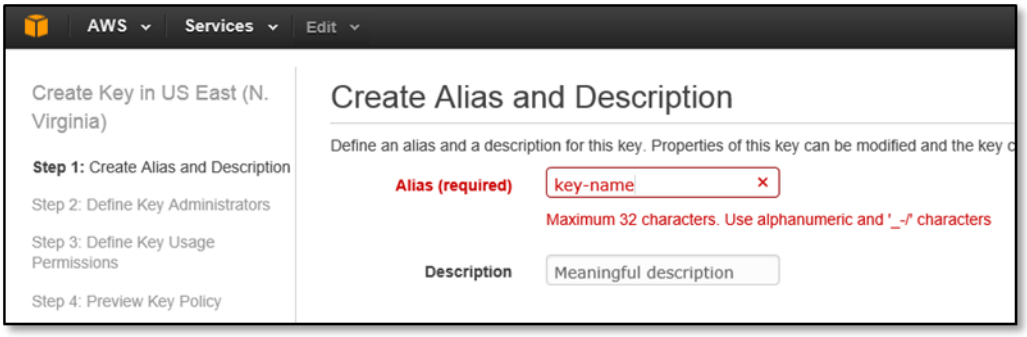



*그림 4 – KMS 구성*

AWS 에서는 암호화 키 관리 권한과 암호화 키 사용 권한을 따로 할당할 수 있으며, 이 방법으로 최소 권한을 강화할 수 있습니다.

**NOTE:** *AWS 인스턴스에 연결된 루트가 아닌 볼륨도 KMS 키를 사용하여 암호화할 수 있으며, 해당 인스턴스에서 실행되는 운영 체제에서 디스크 암호화를 투명하게 확인할 수 있습니다. PCI 요구 사항 3.4.1 에 따라, 암호화된 디스크에 있는 데이터의 액세스 관리는 운영 체제와 분리되지 않으며 독립적이 아닙니다.*

모범 사례 및 PCI 요구 사항(요구 사항 3.6.4)에 따르면 데이터 보호를 위한 암호화 키를 정기적으로 변경해야 합니다. 이렇게 하면 손상된 키의 사용 기간이 제한됩니다.

키를 생성한 후 Identity and Access Management AWS 서비스의 [Encryption Keys] 섹션에서 해당 URL 을 클릭합니다. [Key Rotation] 설정은 선택한 키에 대해 나열된 속성 안에 있습니다. 이 설정을 사용하면 요구 사항 3.6.4 에 따라 지정된 암호화 기간 내에 키 교체를 자동화할 수 있습니다.


*그림 5 – 키 교체 옵션*

#### 4.1.4.3. 서브넷 생성

이 아키텍처에는 별도의 서브넷 네 개가 필요합니다.

- 웹 서버용 DMZ 서브넷
- 점프박스용 관리 서브넷

- 애플리케이션과 데이터베이스 시스템을 위한 내부 서브넷 두 개
  - 이러한 내부 서브넷은 가용 영역이 달라야 나중 단계에서 RDS 중복을 설정할 수 있습니다.

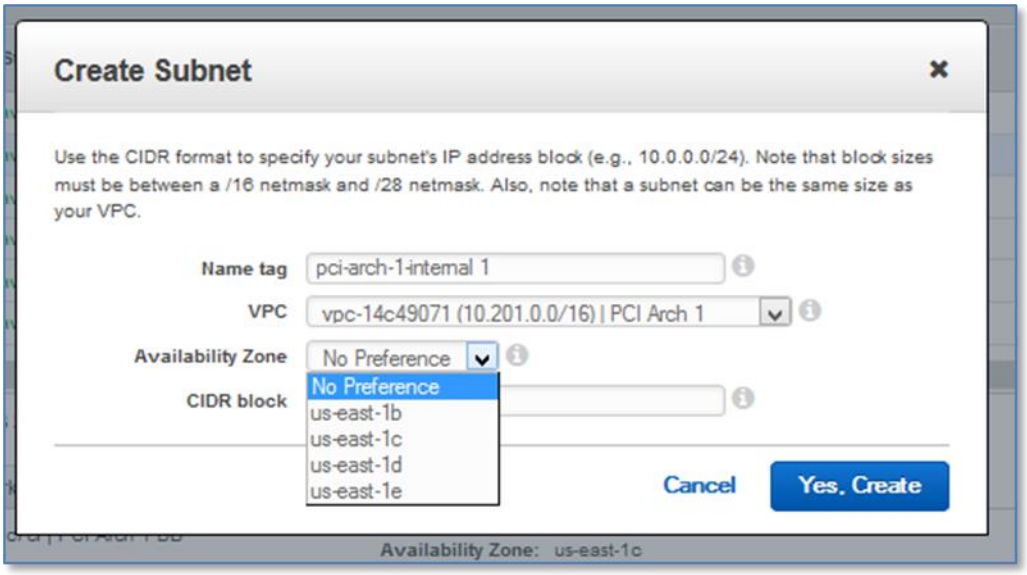



*그림 6 – 서브넷 구성*

기본 VPC EC2 Classic 을 사용하는 경우에도 AWS 콘솔에서 VPC 서비스 관리 페이지를 사용하여 서브넷을 구성합니다.

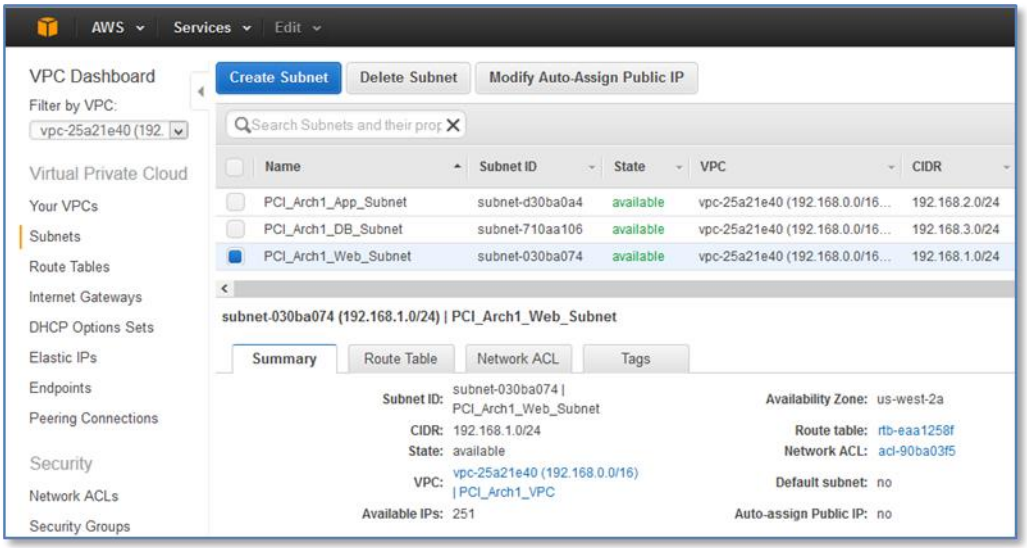



*그림 7 - 새로운 서브넷 세 개가 있는 VPC 서비스 관리 페이지*

#### 4.1.4.4. 라우팅 구성

새로운 서브넷을 생성할 때, 경로 하나가 포함될 기본 라우팅 테이블을 VPC 에 사용하여 해당 서브넷에만 내부 트래픽을 허용합니다.

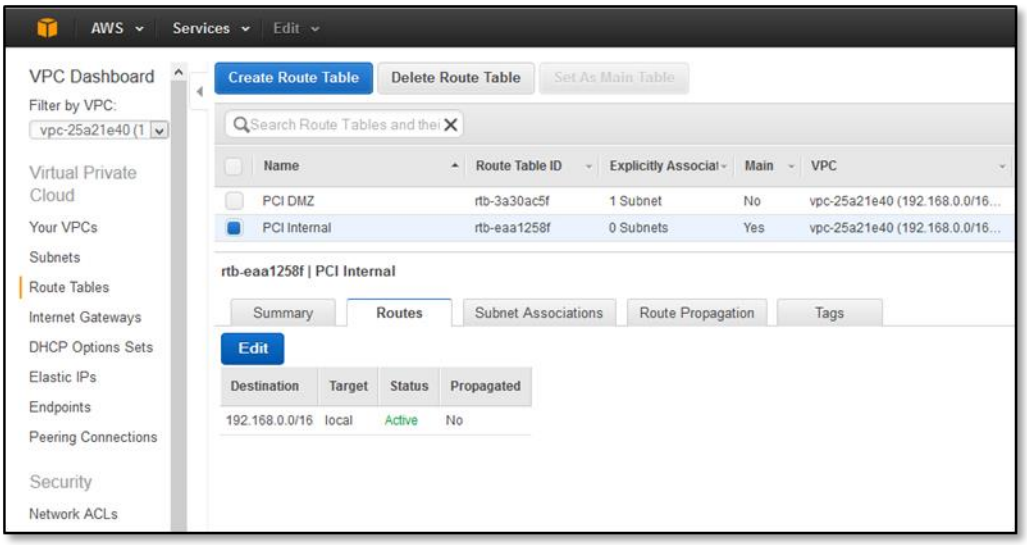



*그림 8 - 내부 경로*

DMZ 및 관리 서브넷에만 인터넷 게이트웨이에 대한 경로가 있어야 합니다. 이렇게 하면 이들 서브넷의 인스턴스만 직접 인바운드 또는 아웃바운드 인터넷 연결을 지원할 수 있습니다.

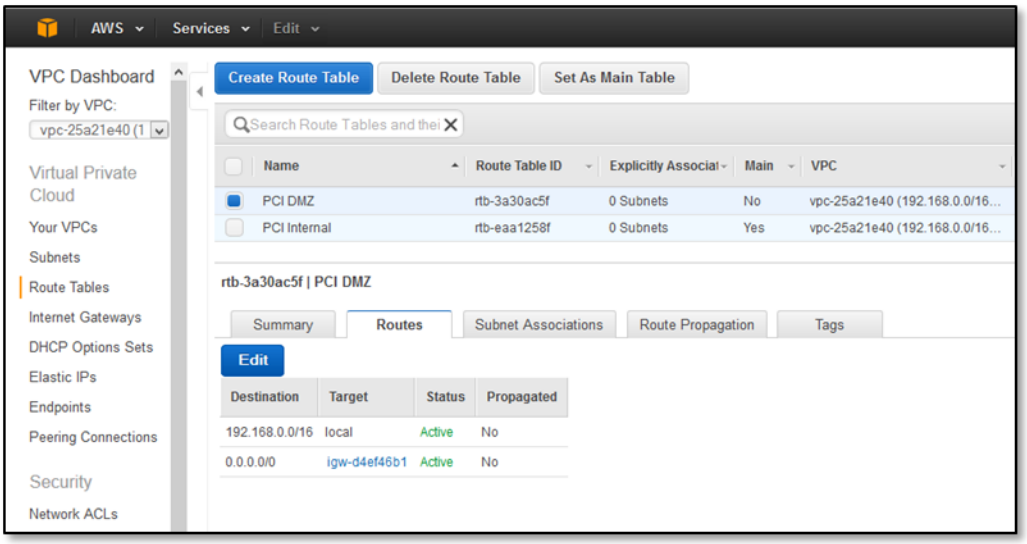



*그림 9 - DMZ 의 게이트웨이 경로*

#### 4.1.4.5. 보안 그룹 생성

보안 그룹은 인바운드 방화벽과 같이 작동합니다. 이 기능은 수신 인스턴스 네트워크 액세스를 사전 정의된 소스, IP 프로토콜 및 TCP 또는 UDP 포트로 제한합니다.

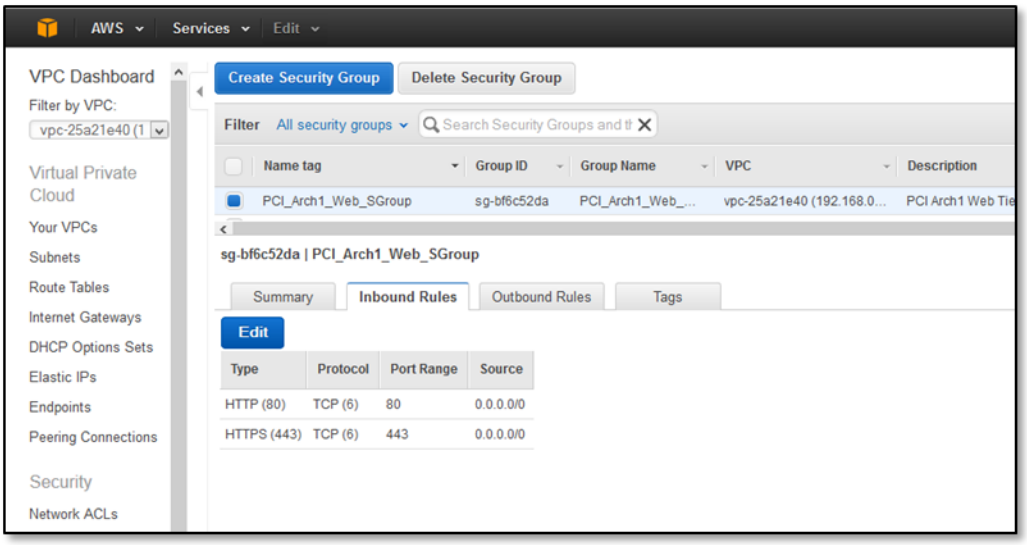



*그림 10 - 보안 그룹 규칙*

또한 이 보안 그룹은 동일한 VPC 의 다른 보안 그룹을 허용된 소스로 참조할 수 있습니다. 예를 들어, 애플리케이션 서버 보안 그룹을 참조하여 Microsoft SQL Server 에 대한 액세스를 해당 그룹의 인스턴스로만 제한할 수 있습니다.

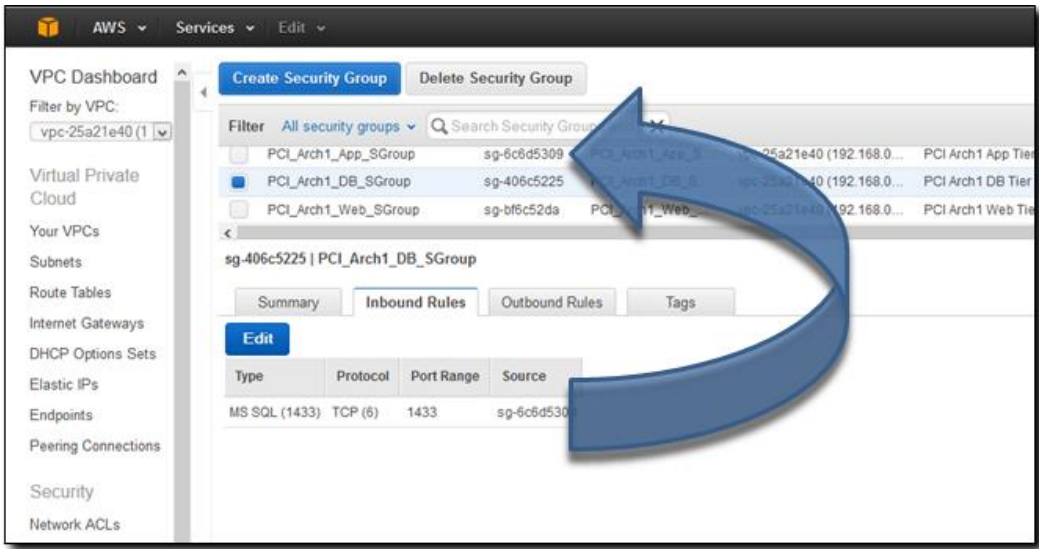



*그림 11 - 보안 그룹은 상태 저장이며 명시적으로 허용되지 않은 모든 액세스를 차단함*

이 아키텍처는 다섯 개의 보안 그룹을 사용하여 설명된 아키텍처를 완성합니다.

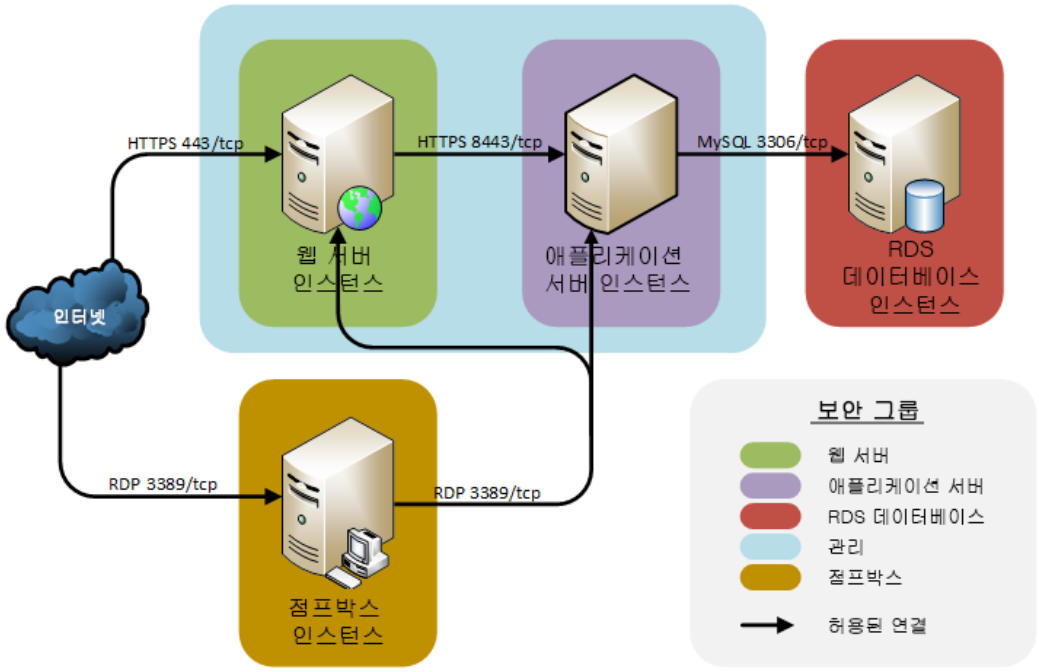



*그림 12 - 논리적 방화벽/보안 그룹 설계*

### 웹 서버 보안 그룹

이 그룹은 어떤 위치에서든 인바운드 웹 클라이언트 연결을 허용하고 내부 애플리케이션 서버로 아웃바운드 웹 서비스 연결을 허용합니다.

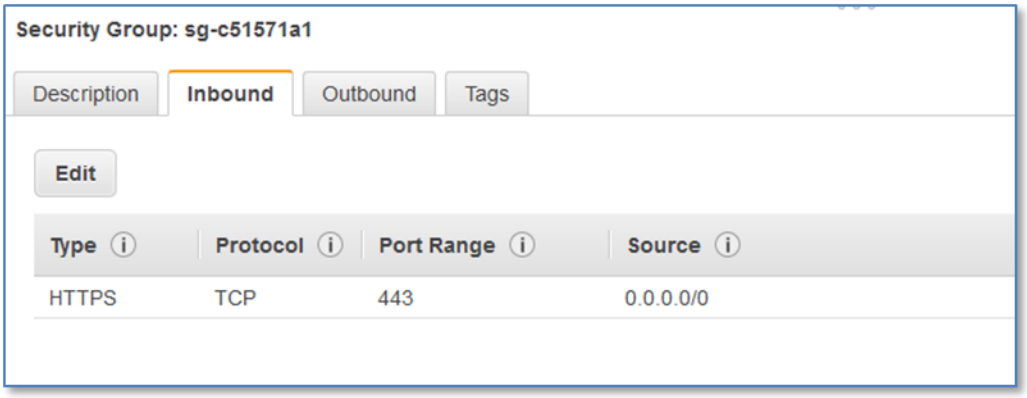



*그림 13 - 웹 서버 보안 그룹 인바운드 규칙*

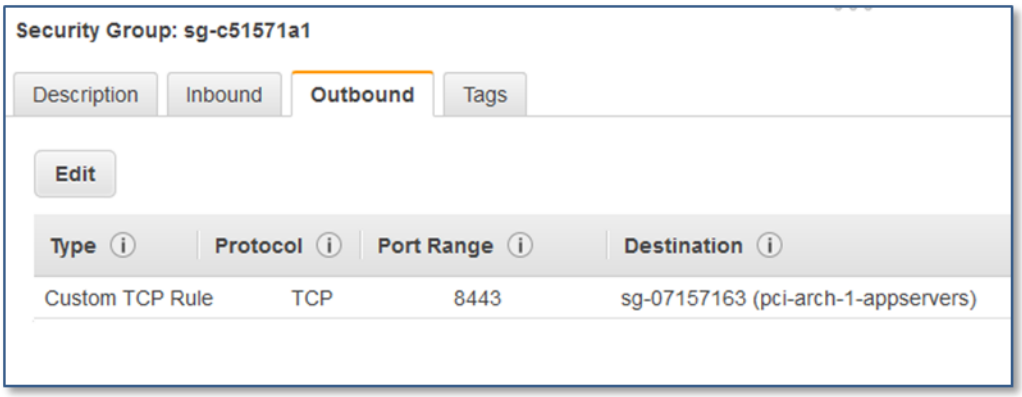



*그림 14 - 웹 서버 보안 그룹 아웃바운드 규칙*

### 애플리케이션 서버 보안 그룹

이 보안 그룹은 웹 서버에서 애플리케이션 서버로 수신 웹 서비스 연결을 허용합니다.

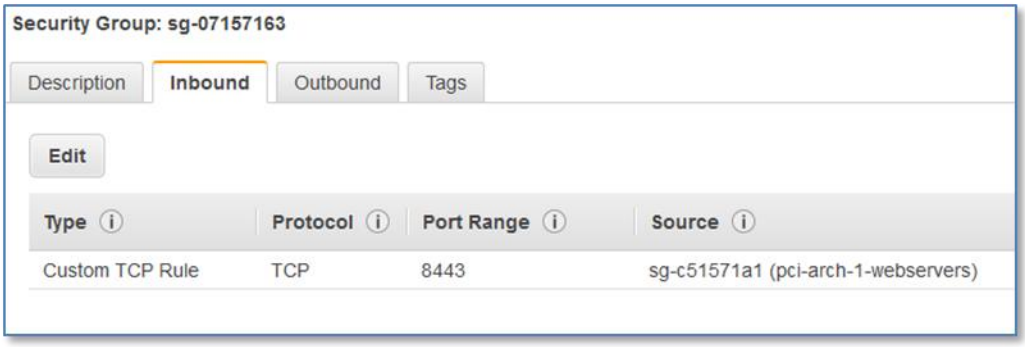



*그림 15 - 애플리케이션 서버 보안 그룹 인바운드 규칙*

이 그룹은 RDS 데이터베이스 인스턴스로 아웃바운드 MySQL 연결을 허용합니다.

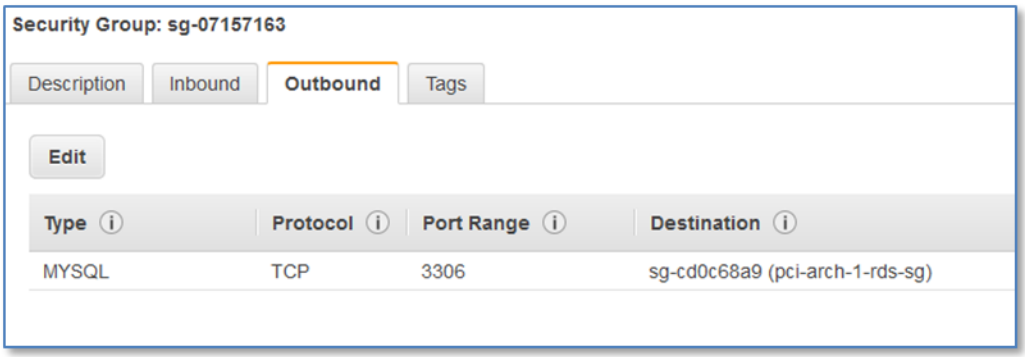



*그림 16 - 애플리케이션 서버 보안 그룹 아웃바운드 규칙*

### 데이터베이스(RDS) 보안 그룹

RDS 는 인바운드 규칙만 사용하지만, 보안 그룹은 RDS 인스턴스에 대한 네트워크 연결을 보호할 수 있습니다.

이 규칙은 애플리케이션 서버 및 그룹 내 다른 RDS 인스턴스에서 MySQL 연결을 허용하여 데이터베이스 복제를 지원합니다.

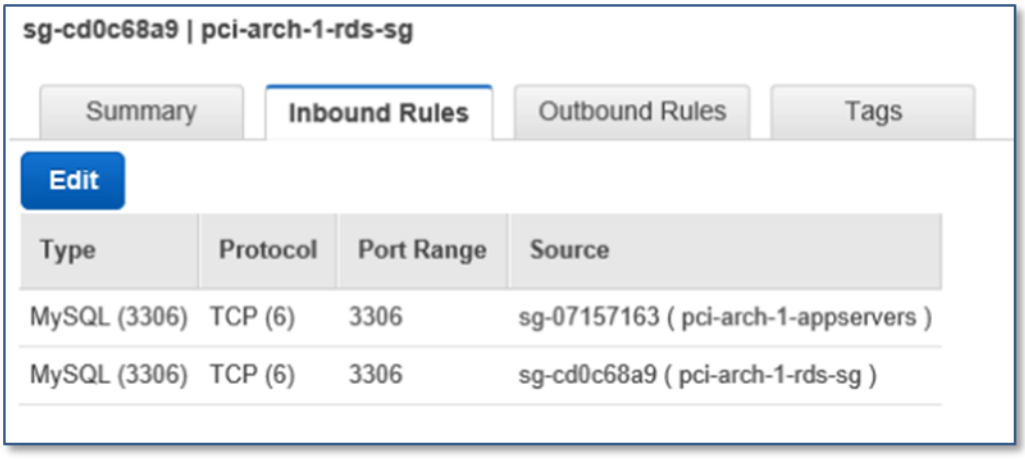



*그림 17 - DB 서버 보안 그룹 인바운드 규칙*

### 관리 보안 그룹

관리 보안 그룹은 관리용으로 점프박스에서 모든 인스턴스로 RDP 와 ICMP 연결을 허용하는 특수 그룹입니다.

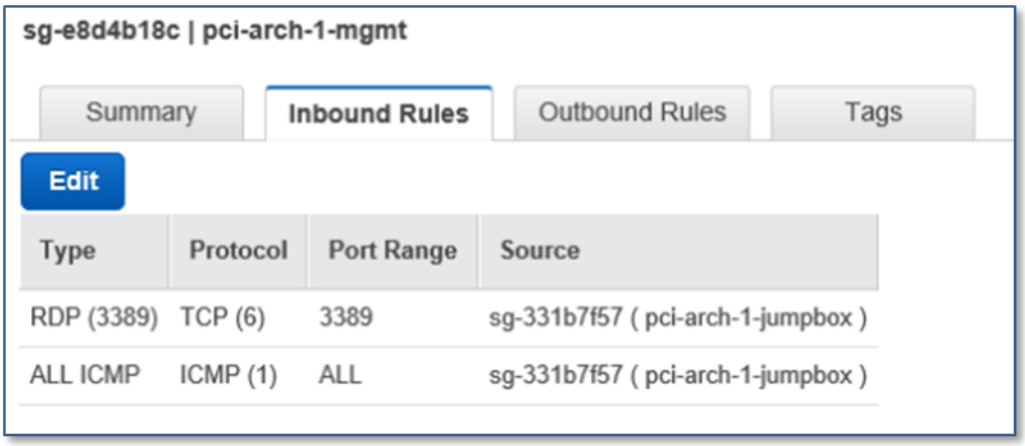



*그림 18 - 관리 서버 보안 그룹 인바운드 규칙*

### 점프박스 보안 그룹

점프박스 자체는 회사 네트워크의 퍼블릭 IP 주소에서만 연결을 허용해야 합니다.

**NOTE:** *요구 사항 8.3 을 충족하려면 원격 액세스에 대한 2 팩터 인증을 구현해야 합니다. Windows 또는 Linux 시스템에 대해 이 기능을 지원할 수 있는 수많은 타사 제품이 있습니다. AWS 는 EC2 인스턴스에 원격 액세스하기 위한 2 팩터 인증을 기본적으로 지원하지 않습니다. 그러나 AWS 자체는 EC2 에 대한 멀티 팩터 인증을 지원합니다. 자세한 내용은 다음 위치의 AWS MFA 세부 정보 및 가격을 참조하십시오.*
*http://aws.amazon.com/iam/details/mfa/*

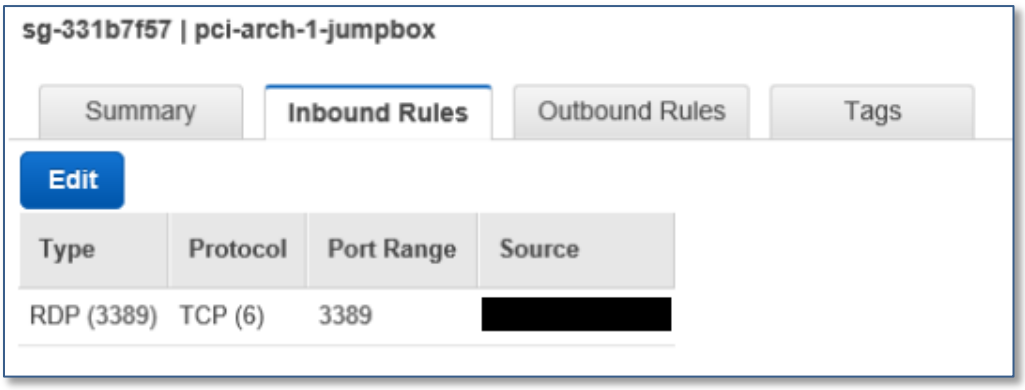



*그림 19 - 점프박스 서버 보안 그룹 인바운드 규칙*

점프박스에는 관리용으로 웹 및 애플리케이션 서버에 대한 아웃바운드 통신이 필요합니다.

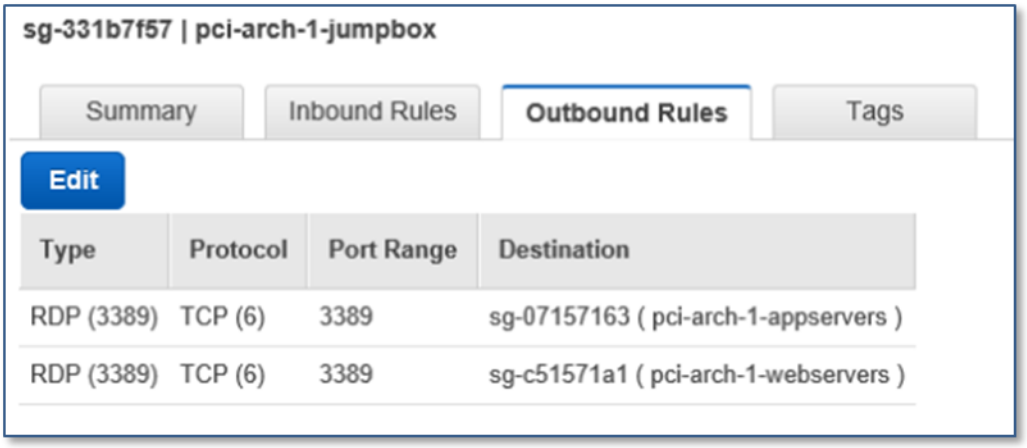



*그림 20 - 점프박스 서버 보안 그룹 아웃바운드 규칙*

#### 4.1.4.6. 보안 인스턴스에서 강화된 AMI 생성

PCI 에는 모든 시스템 구성 요소에 대한 보안 구성 표준의 개발이 필요합니다. AWS 에서는 사전 보안 시스템 생성용 템플릿으로 사용할 보안 인스턴스 하나를 생성할 수 있습니다. 배포에 필요한 각 유형에 대해 새로운 인스턴스를 시작합니다. 이 아키텍처의 경우 웹 서버와 애플리케이션 서버, 점프박스용 애플리케이션 또는 기본 서버 인스턴스가 필요합니다(데이터베이스는 AWS RDS 서비스를 사용함).

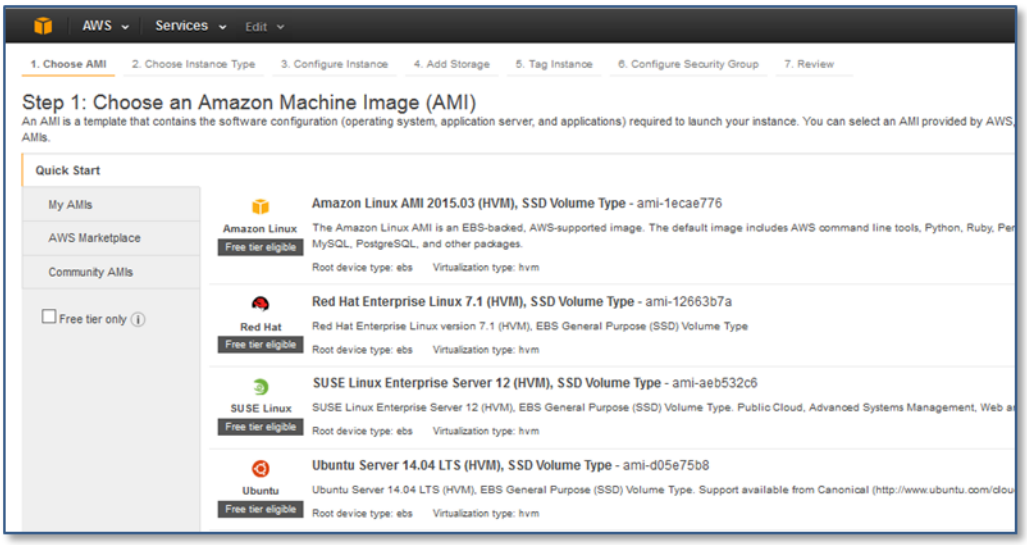



*그림 21 - 인스턴스 배포를 위한 AMI 선택*

이러한 인스턴스의 수명은 호스팅 강화와 구성 단계 수행에 필요한 기간만큼만 지속됩니다. 원격으로 인스턴스에 연결하고 관리할 수 있도록 각 인스턴스가 점프박스 보안 그룹에 속하고, 관리 서브넷 안에 있으며, 탄력적 IP 또는 퍼블릭 IP 를 사용하는지 확인합니다.

퍼블릭 IP 는 인스턴스를 시작할 때 AWS 에서 프로비저닝됩니다. 이 기능은 기본 VPC 에서 자동이지만, 다른 VPC 에서 서브넷별로 구성할 수 있습니다(자세한 내용은 Amazon VPC 사용 설명서 참조).

EIP(탄력적 IP)는 고객이 관리하고 특정 인스턴스가 아닌 AWS 계정과 연관됩니다. 주소 변경 없이 어떤 인스턴스가 특정 EIP 를 사용하는지를 재할당할 수 있습니다.

인스턴스에 연결하고 강화합니다. 평가자가 검토해야 하므로 인스턴스를 보호하기 위해 취한 모든 조치를 기록해야 합니다.

**NOTE:** *그 대신, 보안 구성 표준 문서가 포함된 Anitian 의 사전 강화 AMI 를 사용할 수 있습니다. 이 제품은 AWS Marketplace 에서 사용할 수 있습니다.*

완료되고 인스턴스가 준비되면 전원을 끄고 해당 인스턴스에서 사용자 지정 AMI 를 생성합니다.

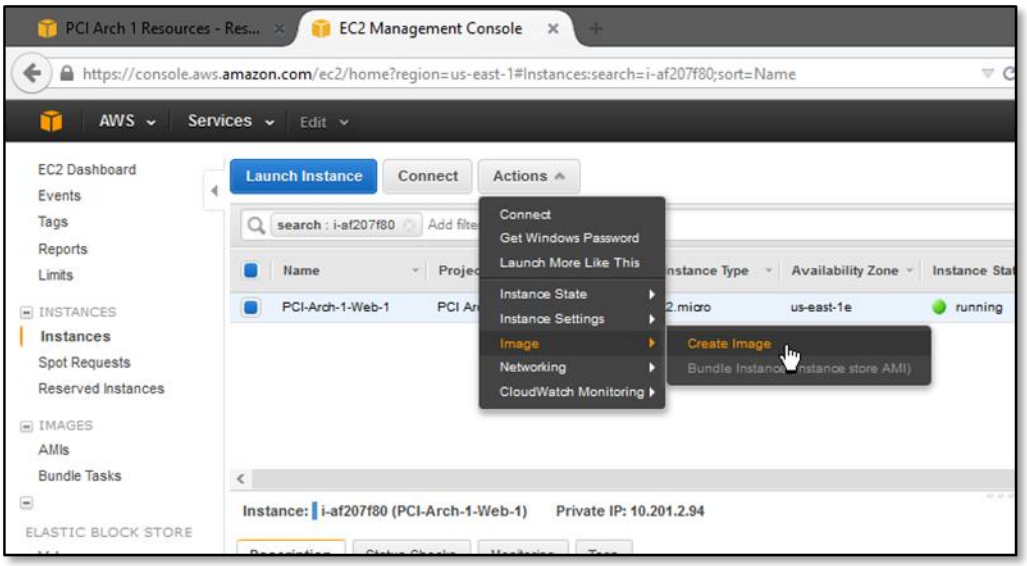



*그림 22 - 강화된 인스턴스에서 AMI 생성*

#### 4.1.4.7. 강화된 AMI 에서 인스턴스 시작

이 아키텍처에는 최소 세 개의 인스턴스가 필요합니다.

- 점프박스 인스턴스
  - 원격으로 환경을 관리하기 위해 사용됨
  - 관리 서브넷에서는 EIP 또는 퍼블릭 IP 필요
- 웹 서버 인스턴스
  - 전자 상거래 애플리케이션에 대한 프런트 엔드
  - DMZ 서브넷에서는 EIP 또는 퍼블릭 IP 필요
- 애플리케이션 서버 인스턴스
  - 웹 서버와 DB 간의 연결을 중개하는 미들웨어를 실행하는 애플리케이션 티어(이 예에서는 RDS)
  - 내부 서브넷에서는 웹 서버와 점프박스에서만 액세스 가능하며, DB 에 액세스할 수 있는 유일한 인스턴스입니다.

새로 생성된 AMI 에서 EC2 인스턴스를 시작합니다.

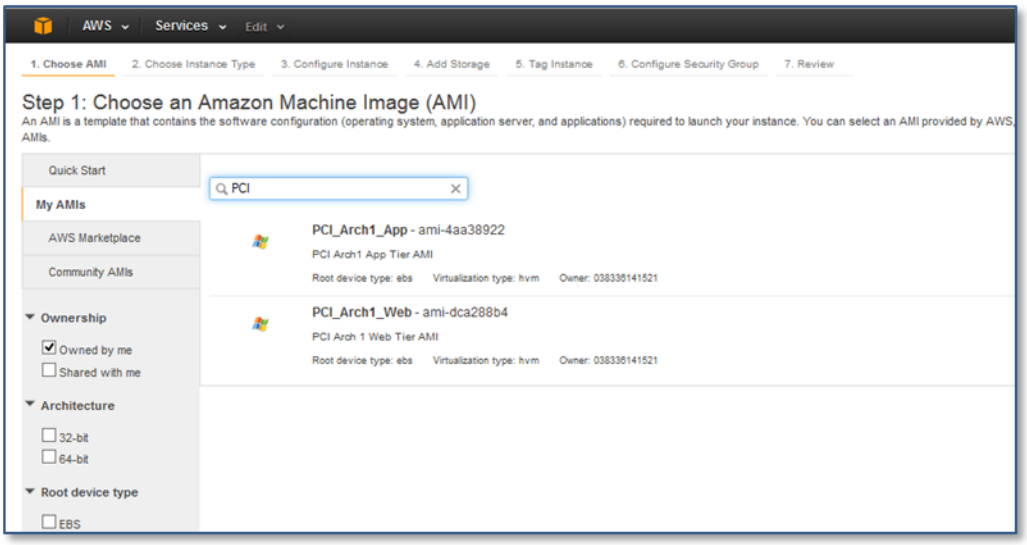



*그림 23 - AMI 에서 인스턴스 시작*

#### 4.1.4.8. 서브넷 그룹 생성

서브넷 그룹을 생성하면 RDS 에서 기본 인스턴스의 오류에서 복원하기 위해 중복 인스턴스를 배치할 위치를 결정할 수 있습니다.

RDS 서비스 관리 페이지에서 서브넷 그룹을 관리합니다. 이전에 생성한 내부 CDE 서브넷 두 개가 포함된 그룹을 하나 생성합니다.

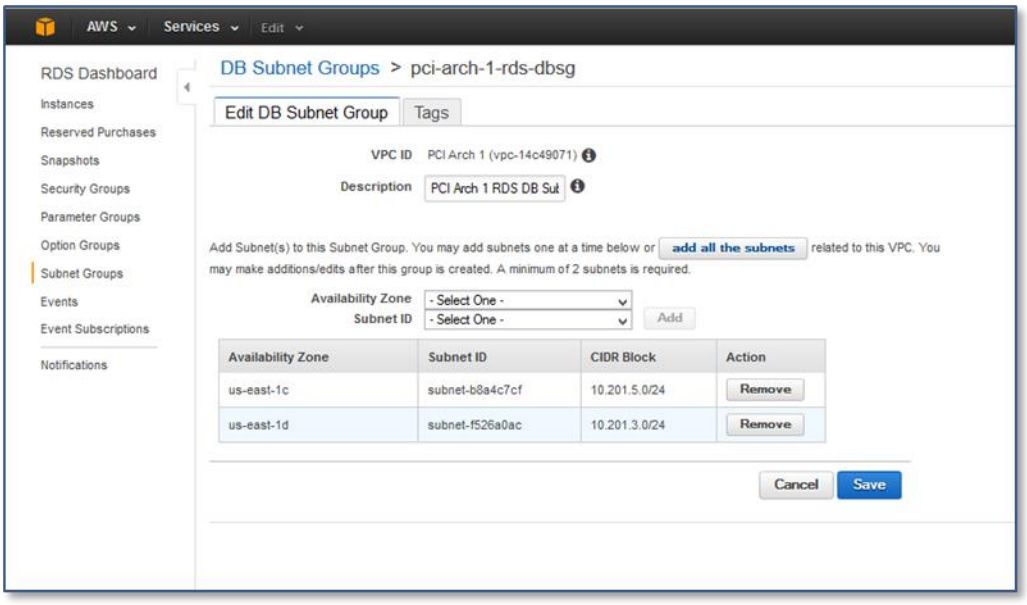



*그림 24 - RDS 서브넷 생성*

#### 4.1.4.9. 암호화된 RDS 인스턴스 생성

KMS 키와 이미 생성된 서브넷 그룹을 사용하여 CHD 를 저장할 암호화된 RDS 인스턴스를 시작합니다.

RDS 인스턴스를 생성할 때 PCI 요구 사항을 충족하기 위해 몇 가지 설정에 각별히 주의해야 합니다. 암호화를 지원하려면 DB 인스턴스 클래스가 db.m3.medium 이상이어야 합니다.

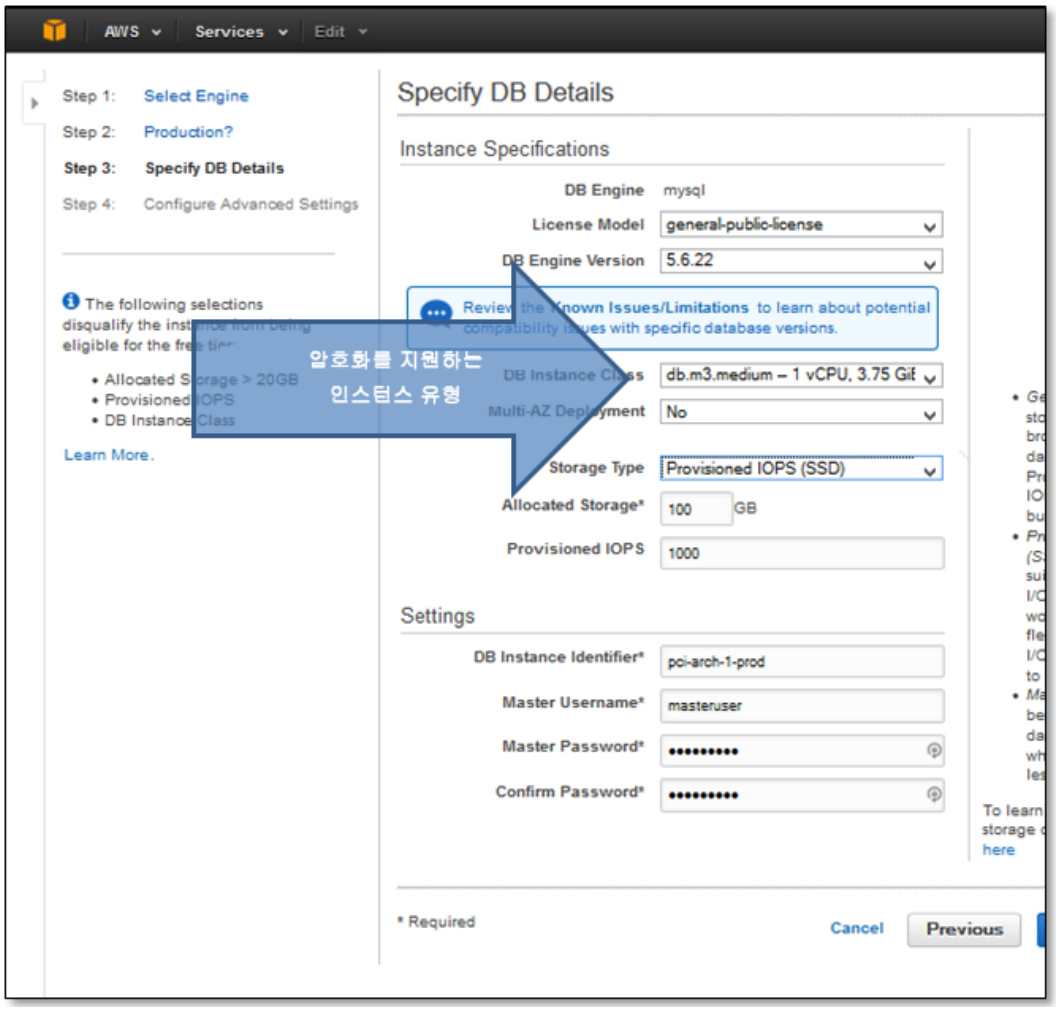



*그림 25 - 암호화를 지원하는 인스턴스 클래스 선택*

추가로 다음을 수행해야 합니다.

- AWS 에서 새로운 "기본" 보안 그룹을 생성하지 않으려면 앞서 생성한 RDS 보안 그룹을 선택합니다.
- [Enable Encryption]에 대해 [Yes]를 선택하고, 이전에 생성된 KMS 키를 선택합니다.

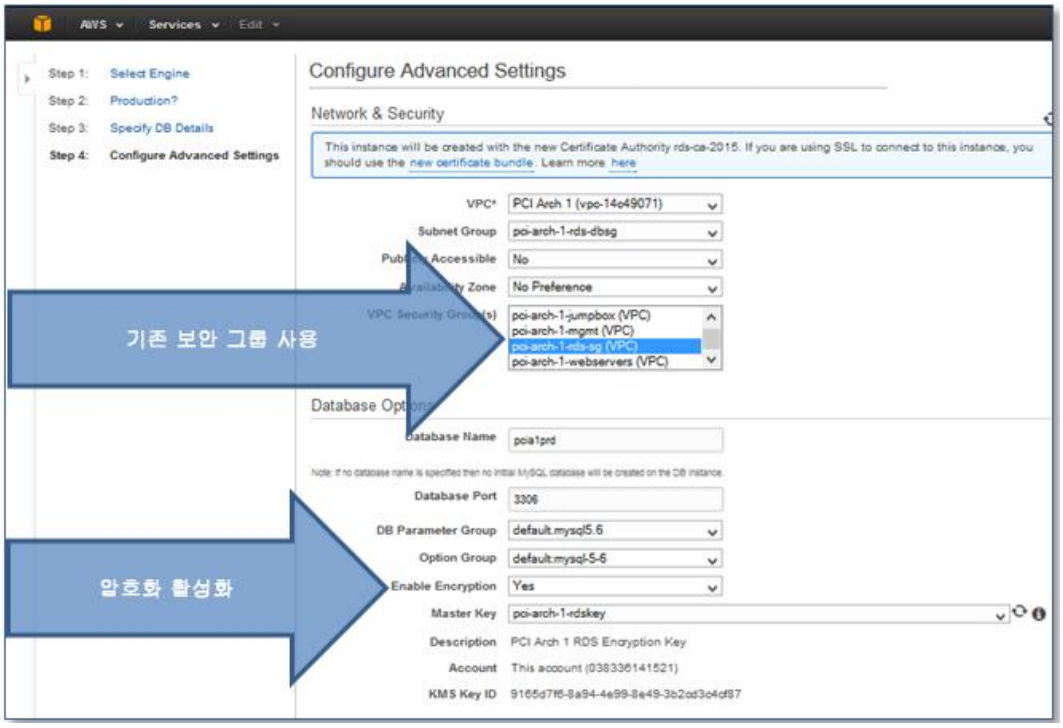



*그림 26 - 보안 그룹 및 암호화를 활성화하기 위한 키 선택*

#### 4.1.4.10. 애플리케이션 소프트웨어 설치

RDS DB 인스턴스의 프로비저닝이 완료되면 환경이 준비됩니다.

**NOTE:** *이 빌드의 단계는 AWS 서비스를 활용한 규정 준수에 중점을 둡니다. 이 환경이 규정을 준수하려면 바이러스 백신, 패치 관리, 로그 관리, 취약성 관리, 파일 무결성 모니터링 등을 포함하되 이에 국한되지 않는 수많은 추가 PCI 요구 사항을 처리해야 합니다.*

## 4.2. 아키텍처 2: 조각화

이 아키텍처는 이전의 설계를 기반으로 구축됩니다. 이 아키텍처는 기존 Amazon AWS 환경의 다른 시스템에서 조각화된 전자 상거래 웹 사이트를 보여 줍니다.

AWS 계정의 나머지 부분에서 CDE 시스템을 조각화하면 PCI 규정 준수의 범위가 제한됩니다.

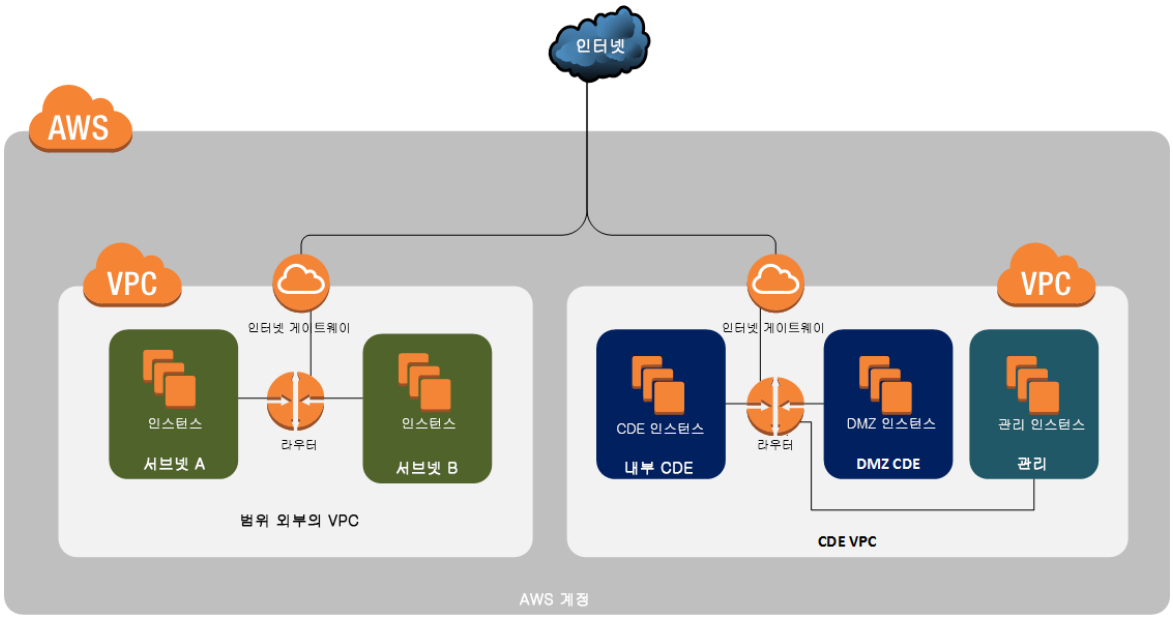



*그림 27 - 더 광범위한 AWS 환경 내에서 조각화된 CDE 의 아키텍처*

### 4.2.1. 개요

조각화된 참조 아키텍처에는 별도의 VPC 에 포함된 프라이빗 네트워크가 두 개 있습니다.

- CDE VPC
  - DMZ CDE, 관리 및 내부 CDE 서브넷 포함
- 범위 외부의 VPC
  - CDE 에서 조각화된 프라이빗 네트워크에 두 개의 서브넷 포함

CDE VPC 네트워크의 시스템 및 서브넷은 첫 번째 아키텍처의 시스템 및 서브넷과 동일합니다. 새로운 VPC 는 모든 CDE 시스템에 연결할 필요가 없는 AWS 의 추가 시스템 및 서브넷을 나타냅니다. 이 아키텍처는 조각화를 통해 PCI 평가 범위에서 새로운 VPC 를 제거하는 방법을 보여 줍니다.

범위 외부의 네트워크를 조각화하려면 CDE 에 연결해서는 안 됩니다. 기존 환경에서는 흔히 방화벽 정책과 스위치 ACL, VLAN, 기타 네트워크 조각화와 격리 기술을 이용해서 달성했습니다.

AWS 에서는 보안 그룹과 VPC 를 결합하여 요구 조건 1.2 의 방화벽 및 라우터 구성 요건을 충족할 수 있습니다. 앞에 나온 대로 보안 그룹은 인스턴스로 들어가고 나오는 트래픽을 제어합니다. VPC 는 AWS 네트워크 내부에서 별도의 격리된 프라이빗 네트워크 공간을 나타냅니다. 각각이 자체적인 프라이빗 주소 공간을 사용하며 AWS 계정의 다른 리소스, 다른 네트워크와 격리됩니다. 이 VPC 는 PCI 범위 축소를 위해 진정한 네트워크 조각화를 가장 직접적으로 구현하는 방법입니다.

**NOTE:** *이 참조 아키텍처의 CDE VPC 를 범위 밖 VPC 에서 조각화하려면 둘 사이에서 VPC 피어링을 설정하면 안 됩니다. 둘 사이에서 설정하면 비 CDE VPC 가 평가 범위로 들어옵니다(일부 환경에서는 적절한 전략이지만, 이 예에서는 사용되지 않음).*

### 4.2.2. PCI 범위

CDE 는 이 아키텍처에 있는 다음 인스턴스로 구성되며 모든 인스턴스는 프라이빗 CDE VPC 네트워크 내에 포함됩니다.

- 웹 서버
- 애플리케이션 서버
- RDS DB

새로운 VPC 는 아래 설명과 같이 네트워크 조각화로 인해 PCI 에 대해 범위 밖에 있습니다.

### 4.2.3. 적용 가능한 AWS 서비스

다음 AWS 서비스는 이 아키텍처에 대한 PCI 요구 사항 준수를 지원하는 데 도움이 됩니다.

| AWS 서비스 | 지원되는 PCI 요구 사항 |
|---|---|
| • 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>• 보안 그룹<br>• AMI<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 |
| • 구성 | 2.4, 11.5 |
| • VPC | 1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7 |

### 4.2.4. 확장 구축

이 단원에서는 참조 아키텍처를 확장 구축하기 위한 기본 단계를 설명합니다.

#### 4.2.4.1. VPC 생성

첫 번째 아키텍처에서 생성된 CDE 인스턴스에서 범위 외부의 인스턴스를 포함하고 격리하기 위해 새로운 VPC 네트워크를 생성합니다.

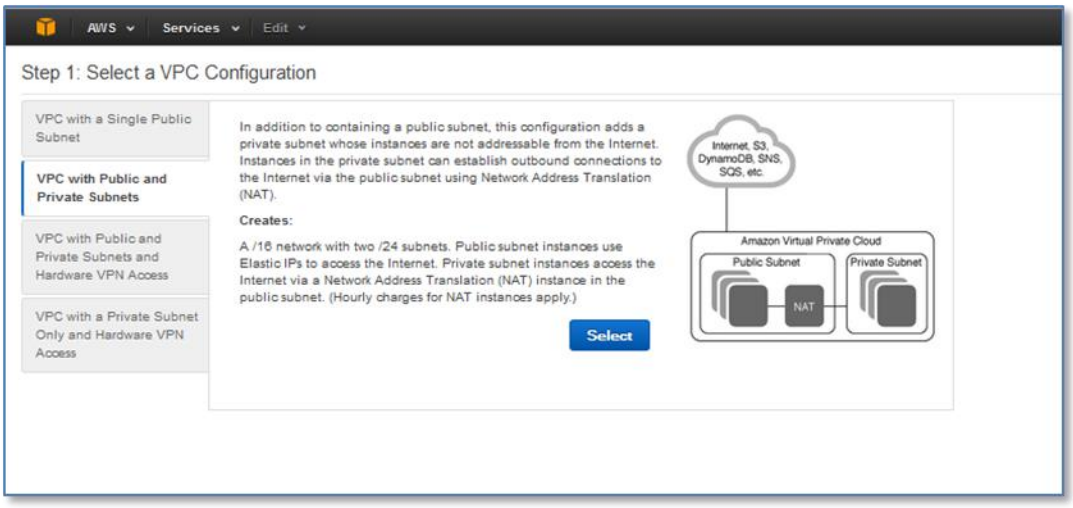



*그림 28 - 새로운 VPC 생성*

새로운 VPC 에는 프라이빗 서브넷용 인터넷 게이트웨이 라우터와 유사하게 작동하도록 설계된 NAT 인스턴스가 포함됩니다. 일단 VPN 이 생성되면 이 NAT 인스턴스를 삭제하여 새 서브넷의 다른 인스턴스가 인터넷에 액세스하지 못하도록 할 수 있습니다.

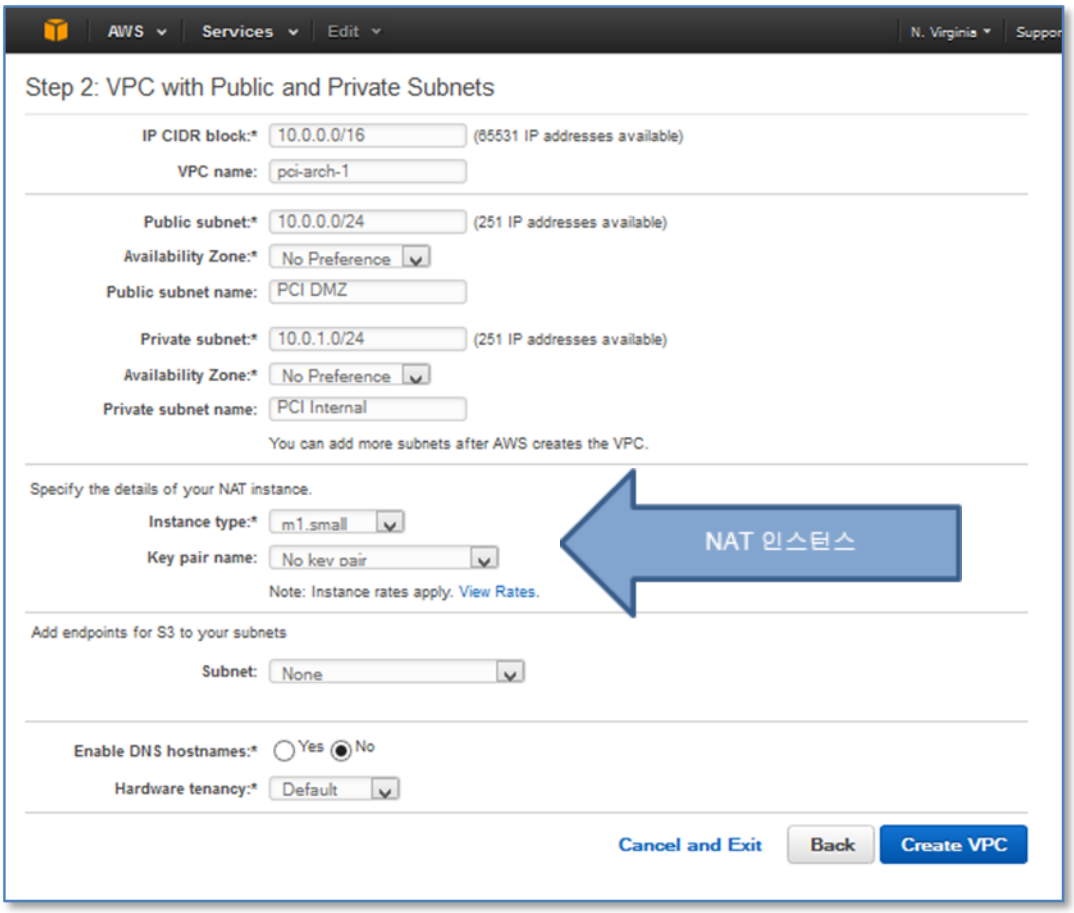



*그림 29 - 새로운 VPC 구성*

#### 4.2.4.2. IAM 사용자와 그룹 및 KMS 키 생성

IAM 리소스는 리전 또는 VPC 에 특정하지 않습니다. AWS 계정 내의 모든 리소스는 동일한 IAM 리소스를 공유합니다.

위의 4.1.4.1 및 4.1.4.2 단원에 설명된 대로 이 사용자와 그룹을 생성합니다.

#### 4.2.4.3. VPC 에서 리소스 생성

리소스를 생성할 때는 각 리소스 생성 마법사의 [VPC] 드롭다운에서 새로 생성된 VPC 를 선택해야 합니다.

**NOTE:** *모든 AWS 리소스가 단일 VPC 나 리전에 특정한 것은 아닙니다. VPC 대시보드에서 리소스를 못 찾으면 EC2 서비스 관리 콘솔에서 찾아보십시오.*

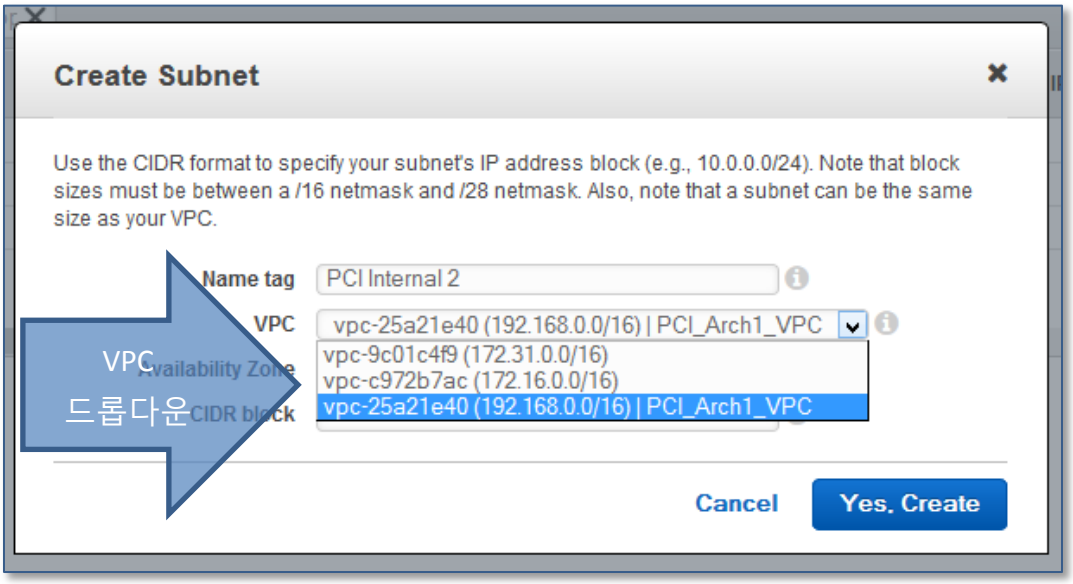



*그림 30 - VPC 서브넷 생성*

#### 4.2.4.4. 인터넷 액세스

VPC 네트워크는 자체적인 인터넷 게이트웨이가 필요합니다. 게이트웨이를 생성한 다음 VPC 에 연결합니다.

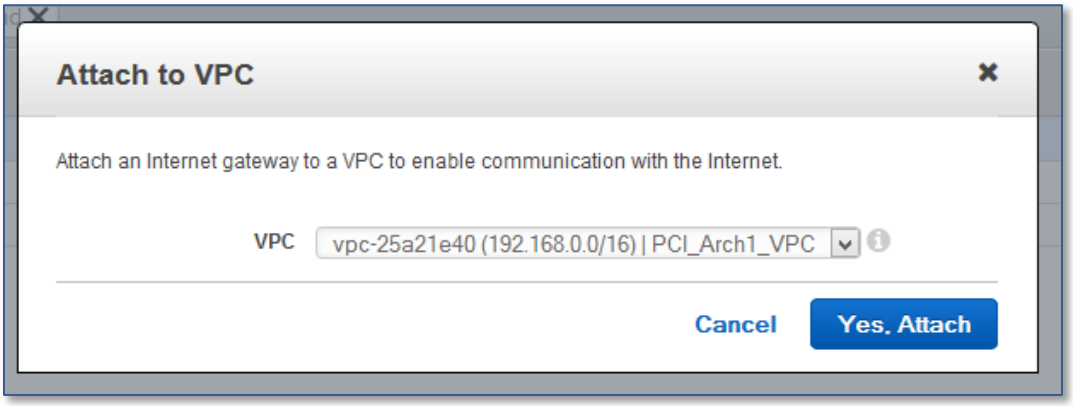



*그림 31 - VPC 에 인터넷 게이트웨이 연결*

## 4.3. 아키텍처 3: Connected

이 아키텍처는 온프레미스 CDE 를 Amazon AWS 환경에 연결하는 작업을 나타냅니다.

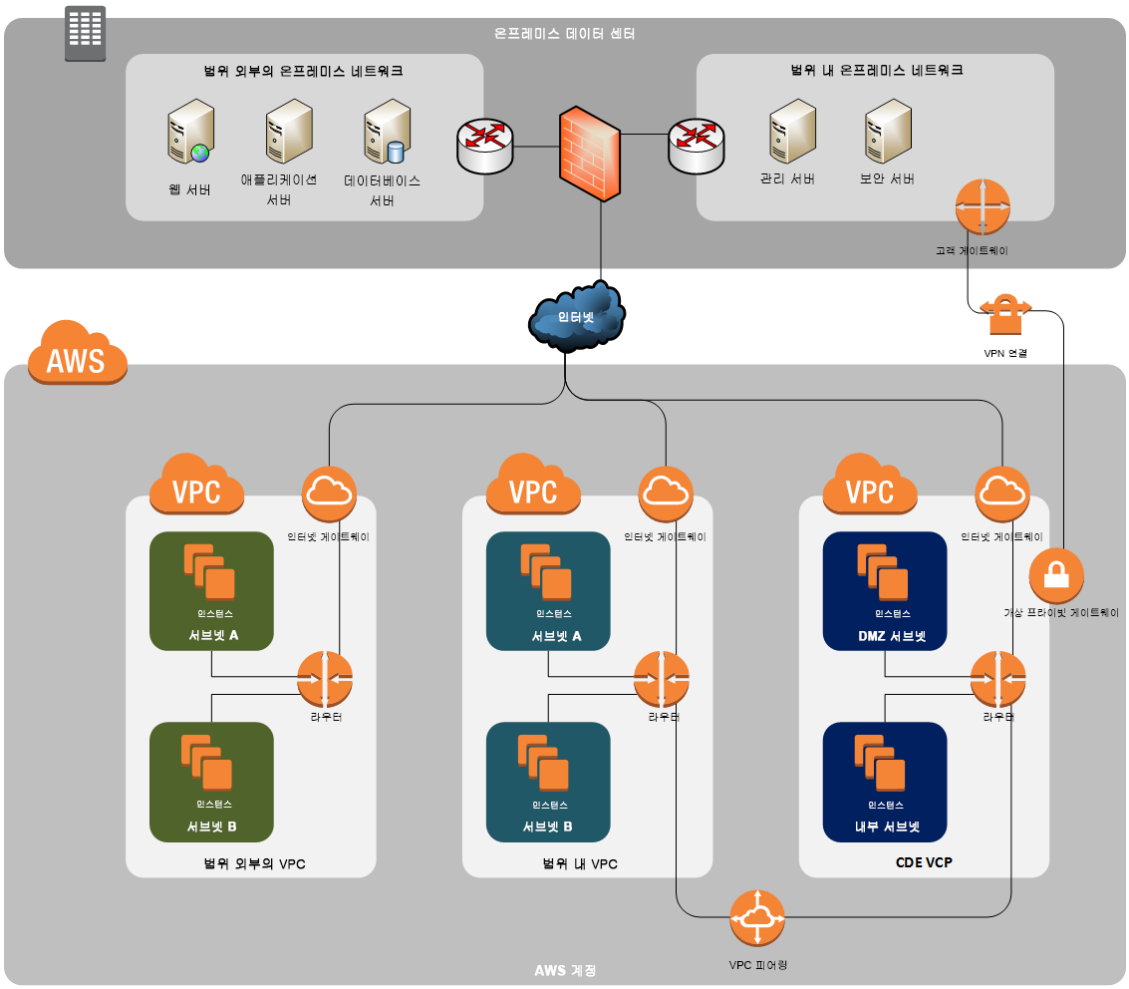



*그림 32 - AWS CDE 에 연결된 온프레미스 시스템*

### 4.3.1. 개요

연결된 참조 아키텍처에는 AWS 에 있는 프라이빗 네트워크 세 개와 일반 온프레미스 네트워크 두 개가 있습니다.

#### AWS 네트워크

1. **CDE VPC**

   DMZ 및 내부 CDE 서브넷이 있는 아키텍처 1 의 VPC 입니다.

2. **범위 외부의 VPC**

   VPC 피어링 없이 완전히 조각화된 아키텍처 2 으 새로운 VPC 입니다.

3. **범위 내 VPC**

   새로운 VPC 입니다. VPC 피어링을 통해 CDE 에 연결됩니다.

### 온프레미스 네트워크

1. **범위 내 온프레미스 네트워크**

   VPN 을 통해 AWS CDE 에 연결된 고객 네트워크 세그먼트입니다.

2. **범위 외부의 온프레미스 네트워크**

   범위 내 고객 네트워크 및 AWS 에서 조각화된 고객 네트워크입니다.

온프레미스 네트워크를 AWS 의 VPC 로 확장하는 작업은 다른 비즈니스 간 VPN 연결을 설정하는 작업과 다르지 않습니다. 일반 VPN 설정에서 IPsec 터널은 인터넷처럼 신뢰할 수 없는 네트워크를 통틀어 믿을 만한 네트워크 둘 이상을 위한 프라이빗 통신을 제공합니다. 동일한 기술을 이용해 다른 VPC 에서 혹은 온프레미스 환경에서조차 프라이빗 VPC 네트워크로 액세스를 제공합니다.

Direct Connect 서비스를 사용하여 AWS 로 직접 프라이빗 비 VPN 연결을 설정할 수도 있습니다. Direct Connect 는 고대역폭 링크를 지원하며 논리적 조각화를 지원하기 위해 802.1q VLAN 태깅과 결합할 수 있습니다. 위 3.4 단원의 참고와 같이, Direct Connect 를 사용한 연결은 암호화되지 않습니다. 직접 네트워크 연결이 프라이빗이 아닌 경우 PCI 4.1 을 준수하기 위해 VPN 이나 TLS 사용과 같은 추가 컨트롤이 여전히 필요할 수 있습니다.

온프레미스 범위 내 관리 시스템이 평가 범위를 변경하지 않고 AWS CDE 시스템을 관리할 수 있으므로 이 아키텍처에는 자체 점프박스가 포함되지 않습니다.

## 4.3.2. PCI 범위

이 참조 아키텍처의 PCI 평가 범위는 다음으로 구성됩니다.

- CDE VPC 네트워크(웹, 애플리케이션 및 데이터베이스 티어)
- AWS 의 범위 내 VPC 네트워크
- 범위 내 온프레미스 네트워크

두 개의 범위 내 네트워크에는 CHD 가 없지만, CDE 에 연결됩니다. 이 아키텍처는 연결된 범위 내 시스템에 대한 두 개의 일반 사용 사례를 보여 줍니다.

- AWS 의 범위 내 VPC 에는 CHD 에 액세스하지 않고 CDE 웹 애플리케이션에서 분석을 수행하는 시스템이 있습니다.
- 범위 내 온프레미스 네트워크에는 맬웨어 방지 및 패치 관리와 같이 CDE 용 보안 컨트롤을 제공하는 시스템이 있습니다.

이 참조 아키텍처에서 범위 외부의 네트워크 두 개에는 위 4.3.1 단원에 설명된 AWS CDE 에 대한 네트워크 연결이 없습니다.

## 4.3.3. 적용 가능한 AWS 서비스

다음 AWS 서비스는 이 아키텍처에 대한 PCI 요구 사항 준수를 지원하는 데 도움이 됩니다.

| AWS 서비스 | 지원되는 PCI 요구 사항 |
|---|---|
| • 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 | 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 |

| | |
|---|---|
| • CloudWatch | |
| • EC2<br>• 보안 그룹<br>• AMI<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 |
| • 구성 | 2.4, 11.5 |
| • VPC | 1.2, 1.2.1, 1.3, 1.3.1-4, 1.3.6-7 |

### 4.3.4. 확장 구축

이 단원에서는 참조 아키텍처를 확장 구축하기 위한 기본 단계를 설명합니다.

#### 4.3.4.1. VPC 생성

위 4.2 단원의 설명과 같이 아키텍처 2: 조각화된 CDE 의 단계에 따라 범위 내 VPC 를 구축합니다.

#### 4.3.4.2. VPC 피어링 연결 생성

CDE VPC 와 새로 생성된 범위 내 VPC 간에 VPC 피어링 연결을 생성합니다.

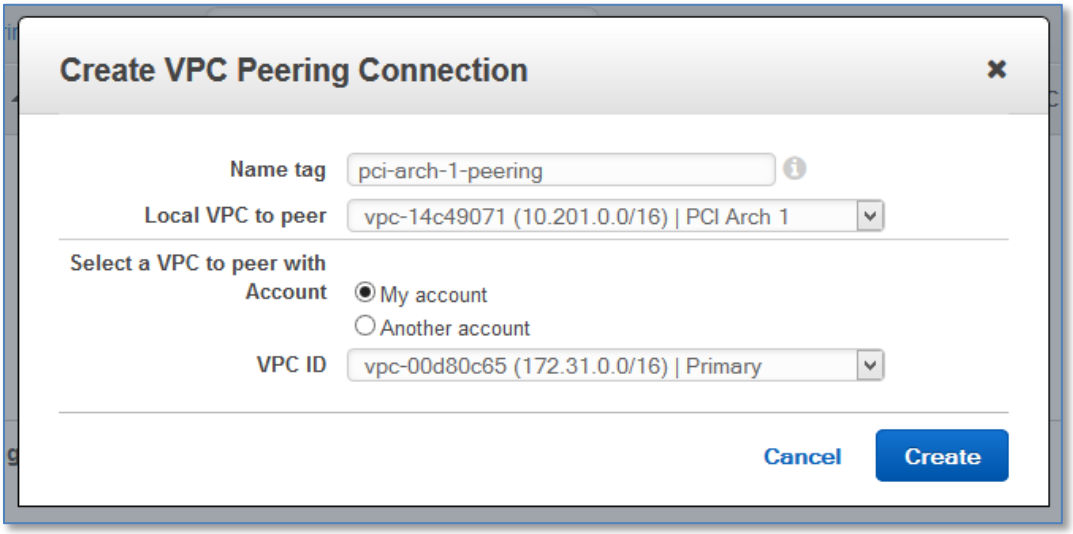



*그림 33 - VPC 피어링 연결 생성*

#### 4.3.4.3. VPC 피어링 연결 허용

VPC 피어링 연결을 생성한 후 피어링 요청을 수락해야 합니다. 다른 AWS 계정에 대해 VPC 간에 피어링이 지원되기 때문에 이 작업이 필요합니다.

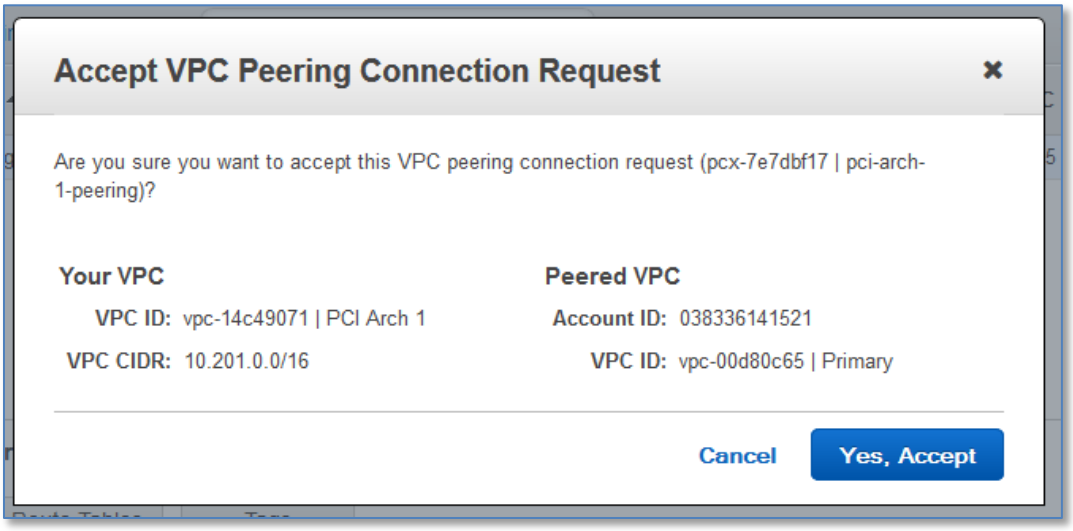



*그림 34 - VPC 피어링 요청 수락*

#### 4.3.4.4. VPC 피어링 연결을 통해 경로 추가

VPC 피어링 연결이 허용되면 피어링된 VPC 에 대한 경로를 CDE VPC 의 라우팅 테이블에 추가할 수 있습니다. 범위 내 VPC 에서 반환 경로를 잊지 말고 추가해야 합니다.

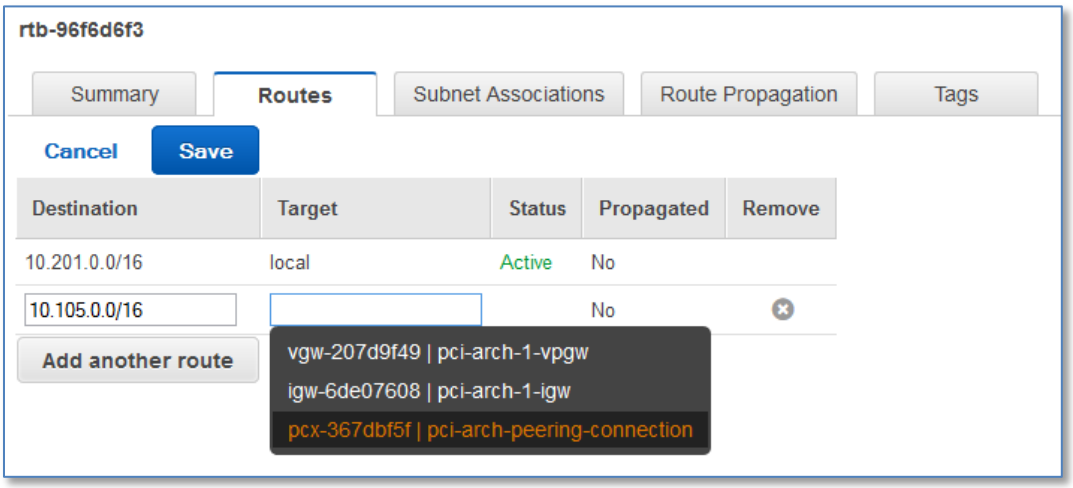



*그림 35 - 피어링된 VPC 에 대한 경로 추가*

#### 4.3.4.5. 범위 내 VPC 리소스 활용

경로가 추가된 후, 이 예에 인용된 분석 시스템과 같은 범위 내 VPC 시스템은 CDE 에 액세스할 수 있습니다.

**NOTE:** *범위 내 CDE 가 적절한 CDE 인스턴스에 연결되도록 허용하려면 CDE 보안 그룹을 수정하거나 새로 만들어야 합니다.*

#### 4.3.4.6. 고객 게이트웨이 생성

CDE VPC 내에서 고객 게이트웨이를 생성합니다. AWS 에서 이 리소스는 클라이언트 사이트의 VPN 집선기를 나타냅니다.

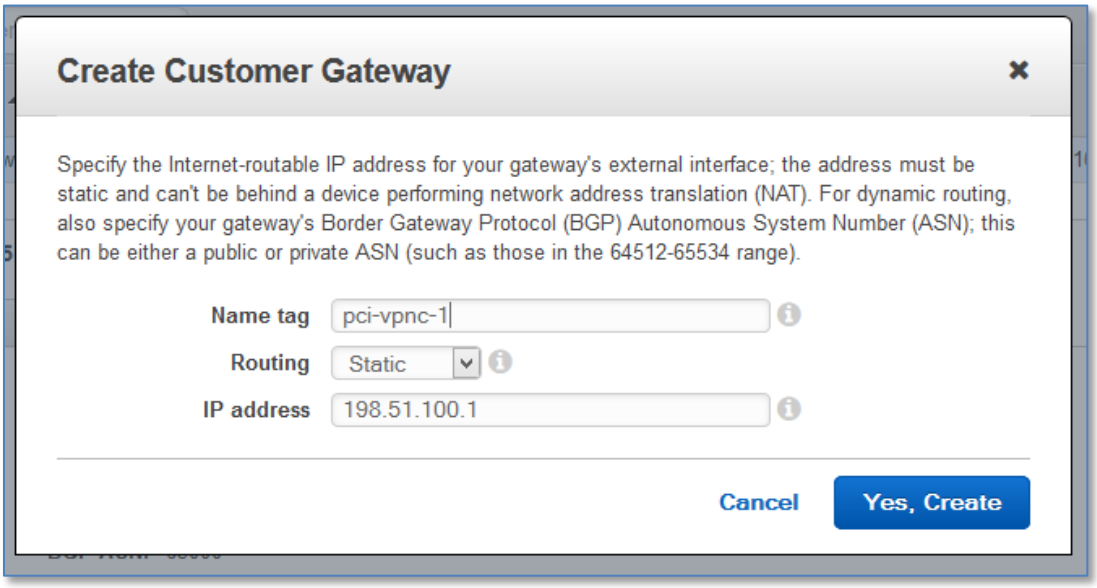



*그림 36 - 고객 게이트웨이 생성*

**NOTE:** *고객 게이트웨이는 BGP 를 사용하는 동적 IP 라우팅도 지원합니다. 동적을 선택하는 경우 게이트웨이에는 원격 IP 주소의 네트워크에 대한 ASN 도 필요합니다.*

#### 4.3.4.7. 가상 프라이빗 게이트웨이 생성

VPC 내에서 Virtual Private Cloud(VPC)를 생성합니다. AWS 에서 이 리소스는 VPN 연결을 위한 AWS 라우팅 대상을 나타냅니다.

인터넷 게이트웨이와 마찬가지로, 이 VPG 는 외부 트래픽을 보내고 받는 데 사용되는 전문 네트워크 인터페이스입니다. 생성한 후 VPG 를 VPC 에 연결합니다.

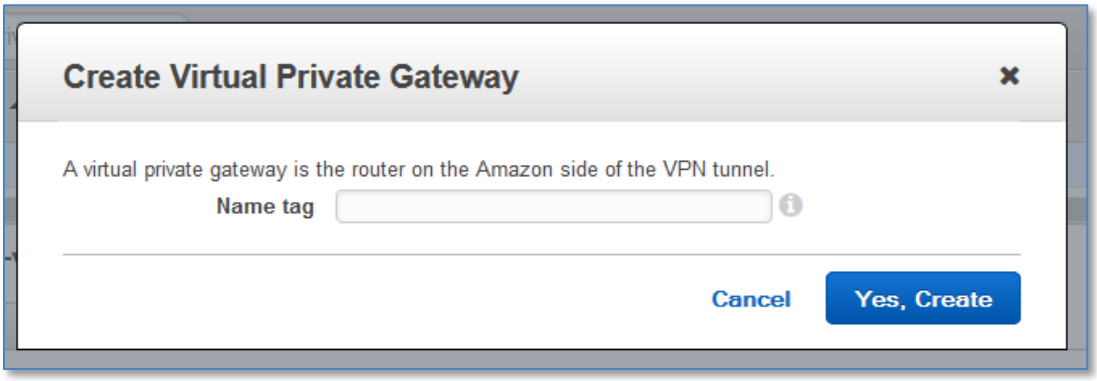



*그림 37 - 가상 프라이빗 게이트웨이 생성*

#### 4.3.4.8. VPN 연결 생성

AWS 는 산업 표준 IPsec VPN 연결을 지원합니다. VPN AWS 리소스는 VPG 와 고객 게이트웨이 간의 연결을 제공합니다.

VPN 에 대해 VPG 와 위에서 생성한 고객 게이트웨이를 지정합니다.

[Static IP Prefixes] 항목은 VPN 연결을 통해 라우팅할 원격 IP 서브넷입니다.

**NOTE:** *VPN 연결에는 중복성을 위한 두 개의 AWS 측 엔드포인트가 포함됩니다.*

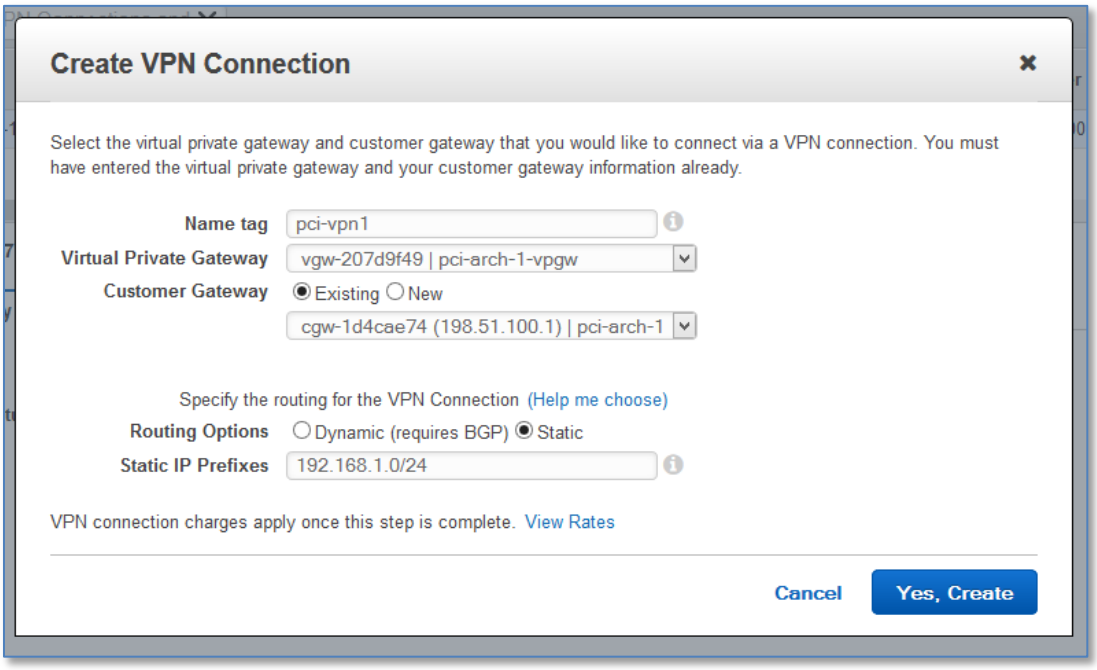



*그림 38 - VPN 연결 생성*

#### 4.3.4.9. IPsec 구성 세부 정보 다운로드

온프레미스 VPN 연결에 필요한 구성을 다운로드합니다. AWS 는 Cisco 및 Fortinet 과 같은 다양한 방화벽/VPN 제조업체에 대한 기본 구성 파일을 지원합니다.

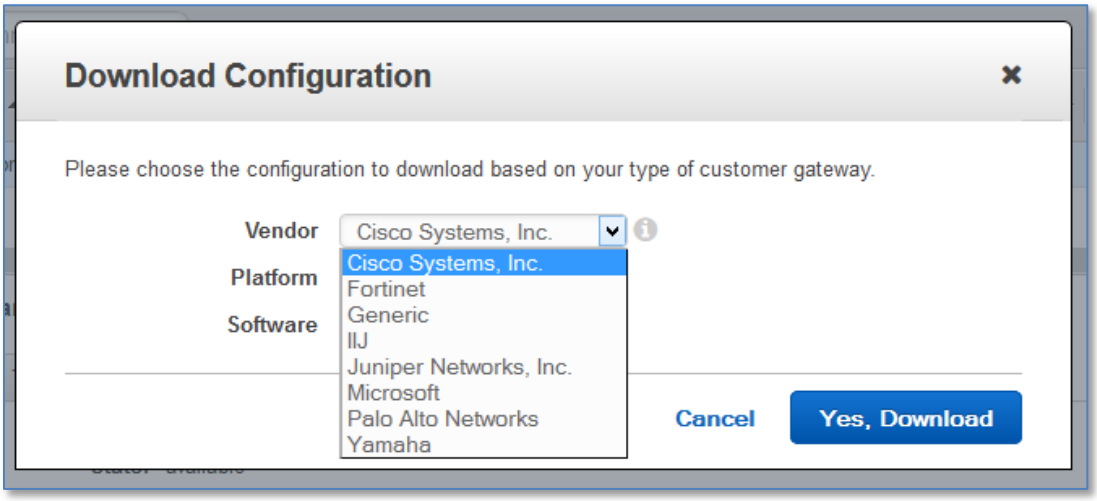



*그림 39 - VPN 구성 다운로드*

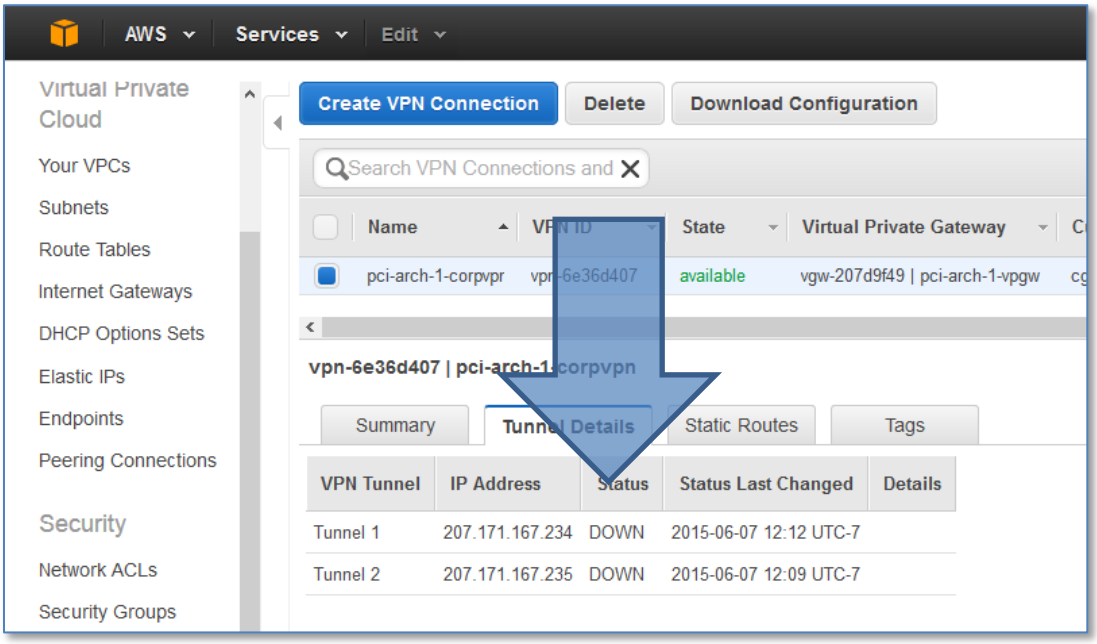
나열되지 않은 장치가 있는 경우, [Generic] 옵션으로 VPN 연결 세부 정보가 포함된 텍스트 파일을 다운로드할 수 있습니다.

```
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
```

*그림 40 - 일반 VPN 구성 파일 예*

#### 4.3.4.10. VPN 터널 상태 확인

온프레미스 클라이언트 VPN 엔드포인트를 구성한 후 VPN 이 나타날 수 있는지 확인합니다. VPN 리소스 세부 정보 창의 [Tunnel Details] 탭에서 터널 상태를 봅니다.




*VPN 터널 상태 보기*

#### 4.3.4.11. 온프레미스 리소스 활용

VPN 터널이 나타난 후, 이 예에서 인용된 AV 및 패치 관리 콘솔과 같은 AWS CDE 내에서 온프레미스 범위 내 시스템을 사용할 수 있습니다.

# 5. 결론

AWS 는 완전 PCI 규정 준수 환경을 지원하기 위해 수많은 기능을 제공하는 강력한 클라우드 플랫폼입니다. 그러나 고객과 고객의 PCI 평가자는 이 기능을 이해해야 합니다.

이 워크북에서는 이러한 몇 가지 문제를 명확하게 설명합니다. 궁극적으로 PCI 규정 준수를 달성하면 환경을 효과적으로 배포, 구성, 관리 및 기록할 수 있습니다. AWS 는 PCI 규정 준수를 위한 뛰어난 플랫폼을 제공하지만, 이 플랫폼을 올바르게 사용하려면 AWS 가 다양한 PCI 요구 사항을 기본적으로 지원하는 방식을 이해해야 합니다.

## 5.1. 지원

AWS 에서 지원이 필요한 경우 Amazon 의 AWS 기술 지원에 문의해야 합니다.

컨설팅 또는 평가 서비스가 필요한 경우 Anitian 이 도움이 될 수 있습니다. Anitian 은 침투 테스트, 취약성 검사, 기술 통합 및 QSA 평가를 포함한 포괄적인 PCI 규정 준수 서비스 제품군을 제공합니다.

전화 888-264-8456, 이메일 info@anitian.com 으로 문의하거나 사이트 www.anitian.com 을 방문하십시오.

# APPENDIX A. AWS PCI DSS 책임 매트릭스 요약

다음 표에는 AWS 와 고객 간 PCI 규정 준수 책임이 요약되어 있습니다.

| 요구 사항 | AWS 책임 | 고객 책임 |
|---|---|---|
| **요구 사항 1**: 카드 소지자 데이터를 보호하기 위한 방화벽 구성 설치 및 유지 관리. | • **범위 내 모든 서비스:** AWS 는 호스트 운영 체제 및 AWS 관리 환경(호스트 운영 체제, 하이퍼바이저, 방화벽 구성 및 기준 방화벽 규칙 포함)에 대한 인스턴스 격리를 유지 관리합니다.<br>• AWS 는 AWS 관리 환경에 대한 방화벽을 구현하고 관리하기 위한 모든 요구 사항을 충족합니다.<br>• **Amazon EC2 및 Amazon ECS:** Amazon VPC 보안 그룹과 네트워크 ACL 은 연결 상태 검사 네트워크 액세스 제어를 구현하며 호환되는 네트워크 조각화에 적합합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 보안 그룹 정의 및 네트워크 액세스 제어 규칙을 책임집니다. |
| **요구 사항 2**: 시스템 암호 및 기타 보안 파라미터에 공급자에서 제공한 기본값 사용 안 함 | • **범위 내 모든 서비스:** AWS 는 클라우드 서비스 제공을 위한 가상화 기술과 애플리케이션을 제공하는 AWS 관리 환경에 대해 구성 및 강화 표준을 개발하고 유지 관리합니다.<br>• AWS 는 구성을 유지 관리하고 기본 운영 체제 및 이러한 서비스용 플랫폼에 대한 보안 표준을 강화합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 기본 공급업체 구성, 보안 제어, 공급업체 기본 암호를 책임집니다.<br>• **범위 내 모든 서비스:** AWS 고객은 고객이 구성할 수 있는 모든 항목에 대한 보안과 규정 준수 구성을 책임집니다. 여기에는 Amazon EC2 및 Amazon ECS 인스턴스에 대한 운영 체제(OS) 구성, 데이터베이스 서비스에 대한 로깅 및 로그 보존, 또는 AWS 관리 기능에 대한 권한이 포함될 수 있습니다. |

| | | |
|---|---|---|
| **요구 사항 3**: 저장된 카드 소지자 데이터 보호. | • **범위 내 모든 서비스:** AWS KMS(Key Management Service)는 하드웨어 보안 모듈을 이용해 키를 보호하며 키를 사용하고 관리하는 기능을 제공합니다.<br>• AWS CloudHSM 은 고객 전용 하드웨어 보안 모듈을 이용해 키를 보호하며 암호화 기능을 제공합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 기본 공급업체 구성, 보안 제어, 공급업체 기본 암호를 책임집니다.<br>• **범위 내 모든 서비스:** AWS 고객은 적용 가능한 모든 내부 및 외부 네트워크 연결에서 암호화를 구현할 책임이 있습니다. (AWS 옵션인 API 암호화를 사용해야 할 수 있습니다).<br>• **AWS KMS 및 AWS CloudHSM:** AWS 고객은 PCI 데이터 보안 표준(DSS)에 따라 암호화 키의 생성과 사용 및 관리를 책임집니다. |
| **요구 사항 4**: 개방형 퍼블릭 네트워크를 통한 카드 소지자 데이터의 전송 암호화. | • **범위 내 모든 서비스:** AWS 는 AWS 관리 환경 내에서 액세스를 암호화하고 암호화를 관리합니다. | • **범위 내 모든 서비스:** AWS 고객은 적용 가능한 모든 내부 및 외부 네트워크 연결에서 암호화를 구현할 책임이 있습니다. (AWS 옵션인 API 암호화를 사용해야 할 수 있습니다). |
| **요구 사항 5**: 바이러스 백신 소프트웨어 또는 프로그램을 사용하고 정기적으로 업데이트 | • **범위 내 모든 서비스:** AWS 는 AWS 관리 환경의 바이러스 백신 소프트웨어는 물론 필요한 경우 확인된 서비스에 대한 바이러스 백신 소프트웨어를 관리합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 일반적으로 맬웨어의 영향을 받는 고객 관리형 OS 인스턴스에서 바이러스 백신 소프트웨어를 구현할 책임이 있습니다. |
| **요구 사항 6**: 보안 시스템 및 애플리케이션 개발 및 유지 관리. | • **범위 내 모든 서비스:** AWS 는 웹 인터페이스, API, 액세스 제어, 프로비저닝 및 배포 메커니즘을 포함하여 평가에 포함된 서비스를 지원하는 애플리케이션의 보안 패치, 개발 및 변경 제어를 유지 관리합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 게시된 OS 및 애플리케이션 취약성을 모니터링하고 인스턴스에 패치할 책임이 있습니다.<br>• 고객은 모든 구성 및 고객 코드에 대해 문서화된 변경 제어를 사용해야 합니다.<br>• 신용카드 데이터를 전송, 처리 및 저장하는 데 사용되는 사용자 지정 코드를 개발하는 고객은 보안 개발 및 테스트에 대한 요구 사항을 준수해야 합니다. |

| | | |
|---|---|---|
| | • AWS 는 웹 인터페이스, API, 액세스 제어, 프로비저닝 및 배포 메커니즘을 포함하여 평가에 포함된 서비스를 지원하는 애플리케이션의 변경을 개발하고 관리합니다. | • **AWS 웹 애플리케이션 방화벽(AWS WAF):** 고객은 일반적인 웹 공격으로부터 자신의 웹 애플리케이션을 보호할 책임이 있습니다. 여기에는 자신의 웹 애플리케이션을 오가는 트래픽 필터링에 대한 액세스 통제 목록과 웹 애플리케이션 방화벽 규칙 구성이 포함됩니다(이에 국한되지 않음). |
| **요구 사항 7:** 업무상 알 필요가 있는 사용자만 카드 소지자 데이터에 액세스할 수 있도록 제한 | • **범위 내 모든 서비스:** AWS 는 기본 인프라 시스템 및 AWS 관리 환경과 관련된 액세스 제어를 유지 관리합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 모든 OS 인스턴스 내 액세스 제어에 대한 책임이 있습니다.<br>• **범위 내 모든 서비스:** AWS 고객은 Amazon RDS 내부의 데이터베이스 사용자처럼 서비스 안에서 구성 가능한 액세스 통제에 책임이 있습니다.<br>• **AWS IAM 및 AWS 자격 증명:** AWS 고객은 CDE 에 포함된 모든 AWS 서비스에 대한 액세스를 관리할 책임이 있습니다. AWS IAM 을 사용하여 리소스 관리와 AWS 구성 역할 및 권한을 구성할 수 있습니다. 고객은 PCI 요구 사항에 맞게 AWS 계정 및 세션 제어를 구성할 책임이 있습니다. 고객은 AWS 리소스 관리의 자격 증명과 액세스 제어에 대한 AWS 지침을 인식해야 합니다. |
| **요구 사항 8:** 컴퓨터에 액세스하는 각 사용자에게 고유한 ID 를 할당합니다. | • **범위 내 모든 서비스:** AWS 는 AWS 관리 환경의 각 사용자에게 고유의 ID 를 제공합니다.<br>• AWS 는 AWS 고객이 AWS 계정을 더욱 보호하고 액세스를 제어할 수 있는 추가 보안 옵션을 제공합니다. 예를 들면, AWS Identity and Access Management(AWS | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 모든 OS 인스턴스 내 액세스 제어에 대한 책임이 있습니다.<br>• **범위 내 모든 서비스:** AWS 고객은 Amazon RDS 내부의 데이터베이스 사용자처럼 서비스 안에서 구성 가능한 액세스 통제에 책임이 있습니다.<br>• **AWS IAM 및 AWS 자격 증명:** AWS 고객은 CDE 에 포함된 모든 AWS 서비스에 대한 액세스를 관리할 책임이 있습니다. AWS IAM 을 사용하여 리소스 관리와 AWS 구성 |

| | | |
|---|---|---|
| | IAM), Multi-Factor Authentication(MFA), 키 교체 등이 있습니다. | 역할 및 권한을 관리할 수 있습니다. 고객은 요구 사항에 맞게 AWS 계정 및 세션 제어를 구성할 책임이 있습니다. 고객은 AWS 리소스 관리의 자격 증명과 액세스 제어에 대한 AWS 지침을 인식해야 합니다. |
| **요구 사항 9:** 카드 소지자 데이터에 대한 물리적인 액세스를 제한합니다. | • **범위 내 모든 서비스:** AWS 는 평가에 포함된 서비스의 물리적 보안 및 미디어 처리 제어를 유지 관리합니다. | • **범위 내 모든 서비스:** AWS 환경 밖에서 생성한 모든 미디어는 고객의 단독 책임입니다. |
| **요구 사항 10:** 네트워크 리소스 및 카드 소지자 데이터에 대한 모든 액세스 추적 및 모니터링. | • **범위 내 모든 서비스:** AWS 는 AWS 관리 환경과 AWS 서비스 인프라에 대한 감사 로그를 유지하고 모니터링합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 모든 OS 인스턴스 내의 로깅을 책임집니다.<br>• **AWS IAM 및 AWS 콘솔:** 콘솔 및 명령줄에서 실행한 리소스 관리 활동에 대한 사용자 활동 로그를 Amazon AWS CloudTrail 을 통해 확인할 수 있습니다. AWS 리소스 관리 활동을 기록하고 모니터링하는 데는 Amazon AWS CloudTrail 을 사용해야 합니다.<br>• **Amazon S3:** 사용자는 버킷 로깅의 구성과 로그 모니터링을 책임집니다.<br>• **Amazon RDS 및 Amazon Redshift:** 사용자는 데이터베이스 액세스 로깅의 구성과 로그 모니터링에 책임이 있습니다.<br>• **Amazon EMR:** Amazon EMR 을 사용해 카드 소지자 데이터를 저장하는 고객은 로깅 액세스에 책임이 있습니다.<br>• **Amazon SimpleDB 및 Amazon DynamoDB:** 이런 데이터베이스를 사용하는 고객은 로깅 액세스에 책임이 있습니다.<br>• **AWS Config:** AWS Config 를 사용해 구성 데이터와 리소스 인벤토리를 저장하는 고객은 로깅 액세스와 로그 모니터링에 책임이 있습니다. |

| | | |
|---|---|---|
| | | • **AWS WAF:** AWS WAF 를 사용해 카드 소지자 데이터를 저장하는 애플리케이션 데이터베이스를 포함하여 퍼블릭 애플리케이션을 보호하는 고객은 로깅 액세스와 모니터링에 책임이 있습니다.<br>• **범위 내 모든 서비스:** AWS 고객은 서비스 내의 로깅 구성을 책임집니다. AWS CloudTrail 은 모든 AWS API 호출 로그에 사용할 수 있습니다.<br>• 고객은 보안 이벤트를 위한 로그 모니터링을 책임집니다. 로그 모니터링은 CloudWatch 또는 타사 서비스로 수행할 수도 있습니다. |
| **요구 사항 11:** 정기적으로 보안 시스템 및 프로세스 테스트. | • **범위 내 모든 서비스:** AWS 는 AWS 관리 환경 및 식별된 서비스에 대해 불법 무선 액세스 지점 감지, 취약성 및 침투 테스트, 침입 감지 및 파일 무결성 모니터링을 관리합니다.<br>• AWS 는 AWS 서비스를 구현하는 네트워크에서 IDS/IPS 를 구현하고 모니터링합니다. | • **Amazon EC2 및 Amazon ECS:** AWS 고객은 인스턴스 및 가상 네트워크의 내부 및 외부 검사와 침투 테스트를 책임집니다. 고객은 검사 및 침투 테스트를 위한 AWS 프로세스를 따라야 합니다. http://aws.amazon.com/security/penetration-testing/.<br>• AWS 고객은 일반적으로 고객이 구현하고 관리하는 호스트 기반 IDS(HIDS) 네트워크 세그먼트를 사용하여 IDS 기능을 구현할 책임이 있습니다. |
| **요구 사항 12:** 직원 및 계약업체에 대한 정보 보안 처리 정책을 유지 관리 | • **범위 내 모든 서비스:** AWS 는 PCI 요구 사항에 따른 보안 정책 및 절차, 보안 인식 교육, 보안 사고 대응 계획, 인적 자원 프로세스를 유지 관리합니다. | • **범위 내 모든 서비스:** AWS 고객은 모든 정책과 절차를 책임집니다. AWS 고객은 요구 사항 12.8 에 따라 AWS 를 인프라 공급자로 포함시켜야 합니다. AWS 알림은 요구 사항 12.10 에 대한 IRP 에 포함되어야 합니다. |

| | | |
|---|---|---|
| **요구 사항 A:** 공유 호스팅 공급자는 카드 소지자 데이터 환경을 보호해야 함. | • **범위 내 모든 서비스:** AWS 고객 인스턴스 및 데이터는 AWS 관리 환경에서 인스턴스 격리 및 기타 보안 조치를 통해 보호됩니다. | • **범위 내 모든 서비스:** AWS 고객은 자체 고객에 대한 응용 프로그램을 실행하거나 데이터를 저장하는 경우 공유 호스팅 공급자로 간주될 수도 있습니다. 이 경우 고객은 AWS 서비스 내에서 자체 고객의 데이터를 보호할 책임이 있습니다. |
| **부록 A2:** SSL/조기 TLS 를 사용하는 엔터티를 위한 PCI DSS 추가 요구 사항 | • **범위 내 모든 서비스:** AWS 는 TLS 1.1 이상을 이용해 AWS 관리 환경 내에서 액세스를 암호화하고 전송 암호화를 관리합니다. | • **범위 내 모든 서비스:** 2018 년 6 월 30 일까지 TLS 1.1 이상을 이용하거나 TLS 1.1 이상으로 업그레이드할 책임은 AWS 고객에게 있습니다. 카드 소지자 데이터 환경이 TLS 1.0 또는 SSLv3 일 경우, AWS 고객은 2018 년 6 월 30 일 기한까지 TLS 1.1 이상으로 옮길 마이그레이션 플랜과 공식 위험 완화를 개발할 책임이 있습니다. |

# APPENDIX B. 인용

다음 표에서는 이 기술 워크북에서 참조된 모든 링크를 요약합니다.

| 단원 | Resource | Link |
|---|---|---|
| 1.2.3 | PCI DSS 버전 3.1 | https://www.pcisecuritystandards.org/security_standards/documents.php |
| 1.2.3 | AWS 환경 관리 | http://aws.amazon.com/getting-started/ |
| 1.2.3 | PCI 클라우드 컴퓨팅 지침 | https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf |
| 2 | AWS PCI 레벨 1 FAQ | http://aws.amazon.com/compliance/pci-dss-level-1-faqs |
| 2.3.1 | AWS AOC 의 복사본 요청 | http://aws.amazon.com/compliance/contact/ |
| 3.3 | EBS 암호화 | http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#EBSEncryption_supported_instances |
| 3.3 | Amazon S3 서버 측 암호화 | http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html |
| 3.3 | Amazon S3 업로드 객체 | http://docs.aws.amazon.com/AmazonS3/latest/UG/UploadingObjectsintoAmazonS3.html |
| 3.3 | AWS KMS 암호화 세부 정보 | https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf |
| 3.3 | AWS KMS API 키 교체 | http://docs.aws.amazon.com/kms/latest/APIReference/API_EnableKeyRotation.html |
| 3.3 | AWS KMS 수동 키 생성 | http://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html |
| 3.3 | CloudTrail 을 사용한 로깅 | http://docs.aws.amazon.com/kms/latest/developerguide/logging-using-cloudtrail.html |
| 3.4 | ELB 보안 정책 테이블 | http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-security-policy-table.html |
| 3.4 | VPC FAQ | http://aws.amazon.com/vpc/faqs/ |
| 3.6 | AWS Linux 보안 센터 | https://alas.aws.amazon.com/ |
| 3.7 | 관리자 가이드 디렉터리 관리 | http://docs.aws.amazon.com/directoryservice/latest/adminguide/directory_management.html |
| 3.8 | 디렉터리 서비스 - 디렉터리 생성 | http://docs.aws.amazon.com/directoryservice/latest/adminguide/create_directory.html |

| | | |
|---|---|---|
| 3.10 | CloudTrail 이벤트 참조 레코드 | http://docs.aws.amazon.com/awscloudtrail/latest/userguide/event_reference_record_body.html |
| 3.10 | Amazon S3 수명 주기 구성 | http://docs.aws.amazon.com/AmazonS3/latest/UG/LifecycleConfiguration.html |
| 3.11, 3.15 | AWS 침투 테스트 정보 | http://aws.amazon.com/security/penetration-testing |
| 4.1.4.6 | Amazon VPC 사용 설명서 | http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#subnet-public-ip |
| 5.1 | AWS 기술 지원 | https://aws.amazon.com/premiumsupport/ |
| 5.1 | Anitian 웹 사이트 | www.anitian.com |