AWS Essentials

9. 보안을 고려한 구성

Tacademy

CONTENTS

학습 목표

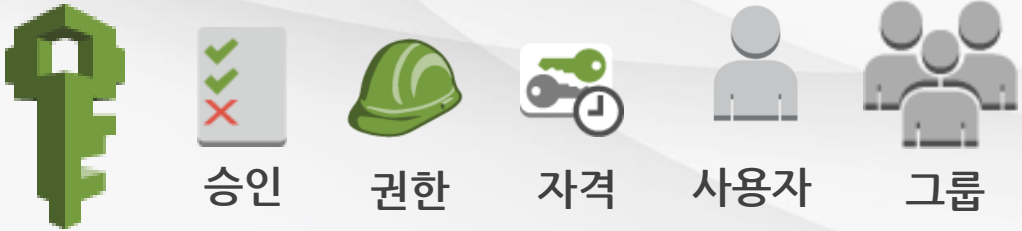
- AWS의 사용자 및 권한의 보안을 고려한 구성을 이해할 수 있습니다.
- AWS의 어플리케이션 레벨의 보안에 대해 이해할 수 있습니다.
- AWS상에서 데이터의 전송과 저장의 보안에 대해 이해할 수 있습니다.

1. AWS 사용자 및 권한의 보안

Identity and Access Management(IAM)

사용자의 AWS 서비스와 리소스에 대한 **액세스**를 안전하게 통제하며 **접근 권한과 인증 등을 중앙 관리**하는 서비스이다.

- IAM을 사용하여 AWS 계정 안에 여러 사용자들 각각의 권한과 인증을 관리할 수 있다.
- 암호 및 액세스 키를 서로 공유할 필요가 없으며 관리자가 손쉽고 안전하게 사용자 권한을 운영하는 것이 가능하다.



Identity and Access Management(IAM)

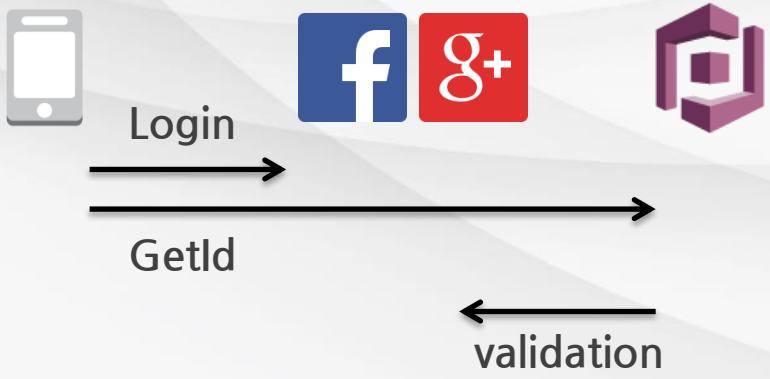
❖ IAM 요소

- Role : 특정 AWS 리소스에 액세스하기 위한 권한의 집합
- Policies : 특정 AWS 리소스를 수행하거나 작업 목적의 단위이며 권한과 연결되어 사용자 혹은 그룹에 정책이 할당
- Group, User : 사용자를 그룹에 구성 가능하며 각각 정책들을 연결하여 접근 및 작업을 하는 주체
- Resource Based Policy : 리소스 단위로 권한을 부여할 작업과 영향 받는 리소스를 지정하고 사용자를 명시적으로 지정하여 정책을 부여

Cognito

Google, Facebook 및 Amazon과 같은 **자격 증명 공급자 활용** 및 **자체 자격 증명 솔루션**을 사용하여 **사용자 인증을 간편하고 안전하게 관리** 하는 서비스이다.

- 완전 관리형 사용자 관리 서비스이며, 보안 및 확장의 고민으로부터 자유롭고, 비용 효율적이다.



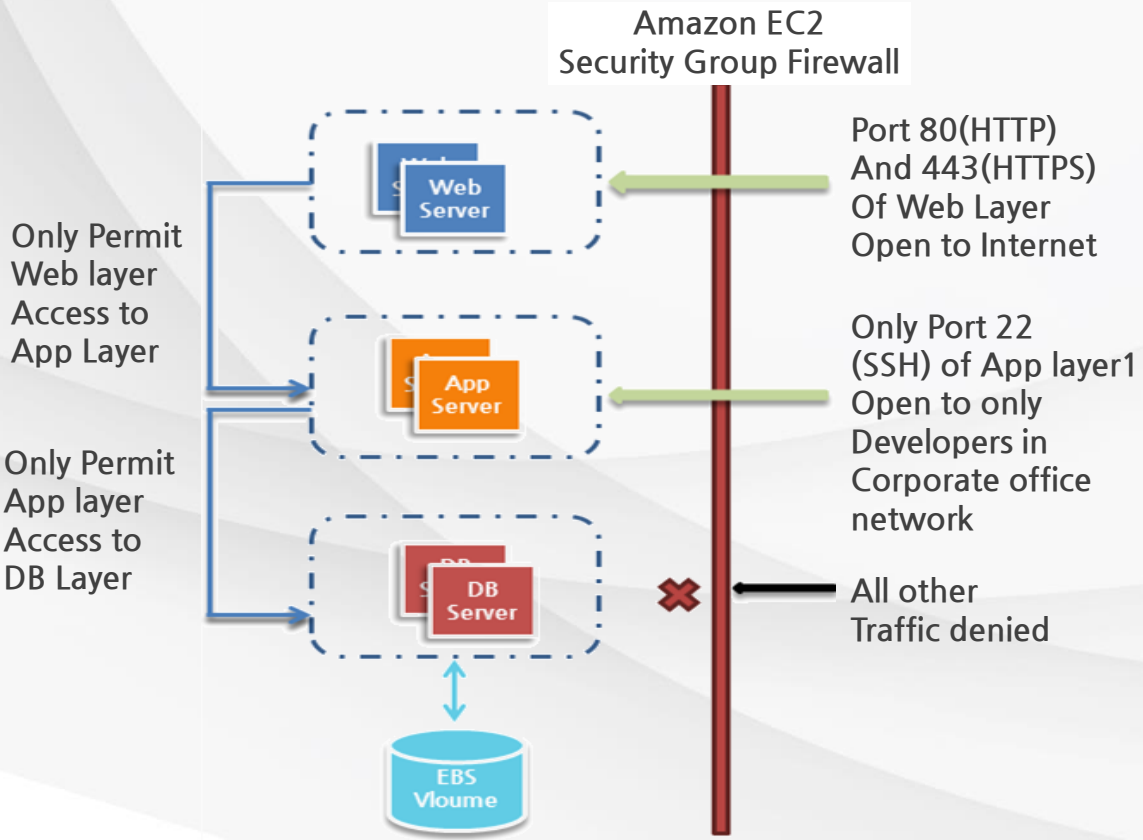
2. AWS 어플리케이션 보안

Security Group

하나 이상의 인스턴스에 대한 트래픽 규칙의 묶음을 정의하며 보안그룹에 있는 **인스턴스의 트래픽을 제어하는 방화벽 역할**을 수행한다.

- 들어오는(인바운드) 트래픽과 나가는(아웃바운드) 트래픽을 제어한다.
- 그룹의 규칙은 언제든지 변경 가능하며 자동으로 해당 그룹에 있는 인스턴스에 적용된다.

Security Group



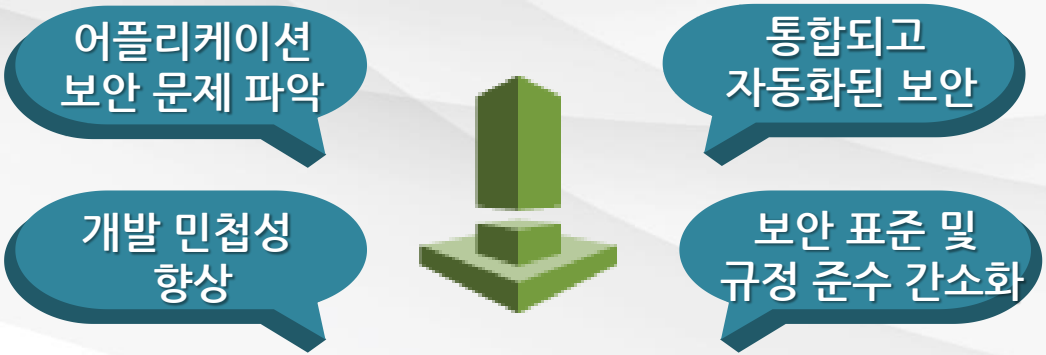
AMI 보안

- 가상 인스턴스의 기본이 되는 이미지인 AMI(Amazon Machine Image)를 주기적으로 패치하여 이미지에 최신 보안을 적용한다.
- 새로운 패치가 적용된 AMI로 재배포하여 어플리케이션의 정상동작 유무를 확인하고 모든 인스턴스에 적용하도록 한다.
- 보안 체크사항을 테스트 스크립트를 통해 확인하고 프로세스를 자동화시킨다.

Inspector

어플리케이션의 **취약점**과 **모범 사례** 등을 자동으로 평가하여 보안 및 규정 준수를 개선시키도록 지원하는 서비스이다.

- 인스턴스에 에이전트를 설치 및 수집 방식이며 Inspector에서 취약성 관련 수백 개 규칙들을 수행한다.
- 정기적으로 AWS에서 최신의 보안 규칙을 업데이트하여 최신의 설정으로 평가한다.



Inspector

❖ 규칙 패키지

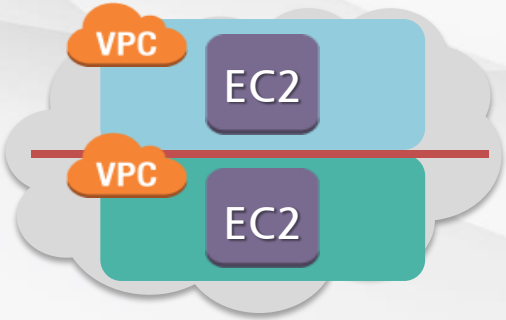
- Common Vulnerabilities and Exposures : 보안 취약점과 공개된 위험 노출에 대한 참조 방법 등을 제공한다. https://cve.mitre.org/
- CIS Operating System Security Configuration Benchmarks : 보안을 향상 시키기 위해 잘 정의되고, 합의된 업계 모범사례들을 제공한다. https://benchmarks.cisecurity.org/
- Security Best Practices : 시스템의 설정 혹은 구성이 보안적인지 확인할 수 있도록 다양한 사례를 제시한다.
- Runtime Behavior Analysis : 인스턴스들의 평가 항목을 통해 행동 상태를 분석하고 보다 안전하게 구성하는 지침을 제공한다.

3. AWS 네트워크 및 데이터 보안

VPC

분리된 가상 네트워크 블록이며 사용자가 직접 네트워크 구성 토폴로지를 정의하여 IP 주소 범위, 라우팅 테이블, 게이트웨이 및 보안 설정을 커스텀하게 구성 가능하다.

- EC2 인스턴스 및 AWS 리소스들이 VPC 네트워크 위에 실행이 되며 해당 VPC의 흐름을 로깅할 수 있다.
- 라우팅 테이블 및 게이트웨이를 통해 인터넷과 단절되거나 사내에서만 연동할 수 있게 네트워크 구성이 가능하다.



VPC

❖구성 시나리오

- **단일 퍼블릭 서브넷 VPC** : 단일 티어 퍼블릭 웹 어플리케이션을 구성하는 경우

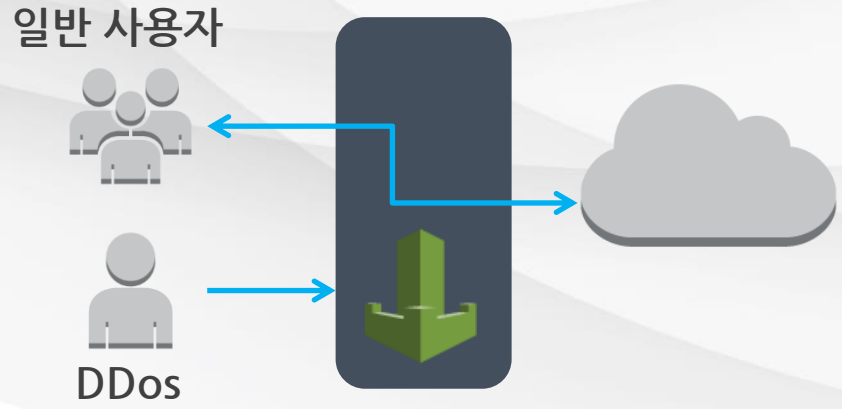
- **퍼블릭과 프라이빗이 공존하는 VPC** : 다중 티어 어플리케이션에 적합하다.
  예) 퍼블릭에 WEB서버를 배치하고 DB서버는 프라이빗 서브넷에 배치

- **VPN 액세스를 제공하는 VPC** : 온프라미스 환경과 클라우드를 사설 통신으로 확장하는 구성

WAF

일반적인 **웹 취약점 공격**으로부터 웹 어플리케이션을 보호하는 목적을 가진 웹 어플리케이션 **방화벽**이다.

- 과도한 리소스 사용 공격, SQL 명령어 인젝션, 교차 사이트 스크립팅과 같은 일반적인 공격 패턴을 차단하고 커스텀하게 설계된 규칙을 생성할 수 있으며 종량제 구조로 비용 효율적이다.



학습정리

지금까지 [보안을 고려한 구성]에 대해서 살펴보았습니다.

AWS 사용자 및 권한의 보안

IAM을 통해서 AWS 리소스의 권한과 정책을 안전하고 손쉽게 관리하고
Cognito를 통해 사용자를 자체 혹은 자격 증명 제공자를 통해 인증하여
손쉽게 보안 레벨을 향상시킨다.

AWS 어플리케이션의 보안

- Security Group을 통해서 트래픽 레벨에서 인스턴스의 보안을 관리하고
  정기적인 AMI의 패치를 통해 최신의 보안 정책을 유지한다.
- Inspector으로 어플리케이션 레벨의 취약점을 분석해 보안 수준을 높인다.

AWS 네트워크 및 데이터 보안

VPC를 통해 가상 네트워크 토폴로지를 정의, 관리하며
WAF를 통해 웹 취약점 공격을 대비하여 서비스 보안 수준을 높인다.