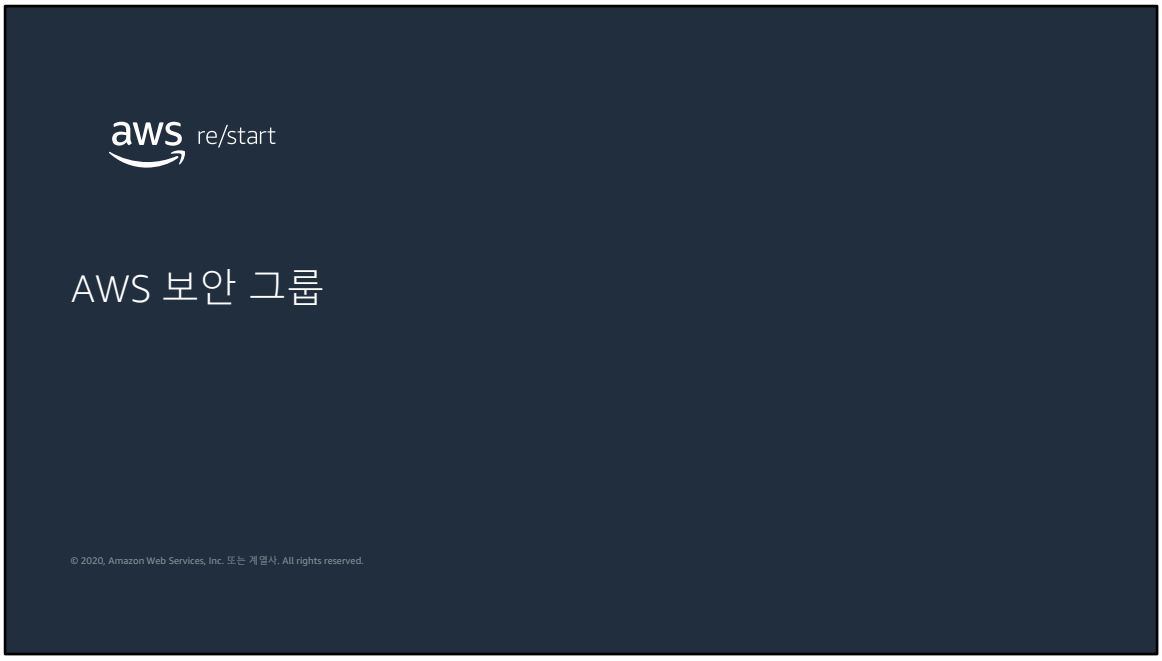


AWS 클라우드의 보안은 AWS에서 가장 중점을 두는 부분입니다. 이 강의에서는 AWS 보안 그룹을 사용하여 Virtual Private Cloud(VPC)의 보안을 강화하는 방법을 알아봅니다.

교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- 보안 그룹을 설명하고 보안 그룹이 데이터 보호에 어떻게 도움이 되는지 설명합니다.

주요 용어:

- 보안 그룹
- 네트워크 액세스 제어 목록(네트워크 ACL)
- 키 페어

이 강의에서는 AWS 보안 그룹의 기능과 이점에 관해 배웁니다.

AWS 보안 그룹

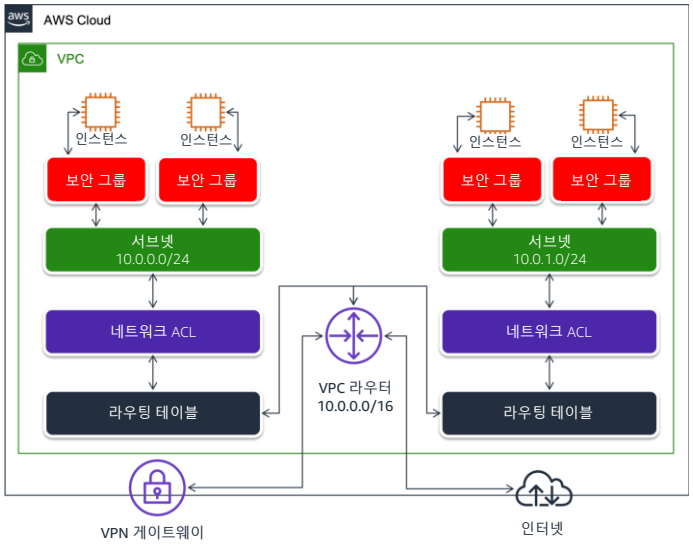
주요 기능

- 보안 그룹은 가상 서버의 내장된 방화벽과 같은 역할을 합니다.
- 보안 그룹 규칙은 인스턴스에 액세스할 수 있는 사람을 결정합니다.
- 보안 그룹은 상태 기반입니다.

AWS에서 보안 그룹은 가상 서버의 내장된 방화벽과 같은 역할을 합니다. 보안 그룹을 사용하면 인스턴스의 액세스 가능성을 완벽하게 제어할 수 있습니다.

가장 기본적인 수준에서 보자면, 보안 그룹은 인스턴스에 대한 트래픽을 필터링하는 또 다른 방법이라고 할 수 있습니다. 어떤 트래픽을 허용할지 차단할지 제어할 수 있도록 하는 것입니다. 인스턴스에 액세스할 수 있는 사람을 결정하려면 보안 그룹 규칙을 구성합니다. 규칙은 인스턴스를 완전히 프라이빗하게 유지하는 것에서부터 완전히 퍼블릭으로 만드는 것까지 다양합니다.

Amazon VPC 및 보안 그룹



aws re/start

Amazon Virtual Private Cloud(Amazon VPC)에서는 VPC에 대한 보안을 강화하고 모니터링할 수 있는 다양한 기능을 다음과 같이 제공합니다.

- 보안 그룹은 연결된 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 방화벽 역할을 합니다. 보안 그룹은 인스턴스 수준에서 인바운드 및 아웃바운드 트래픽을 모두 제어합니다.
- 네트워크 액세스 제어 목록(네트워크 ACL)은 연결된 서브넷의 방화벽 역할을 합니다. 네트워크 ACL은 서브넷 수준에서 인바운드 및 아웃바운드 트래픽을 모두 제어합니다.
- Amazon EC2는 퍼블릭 키 암호화 기법을 사용하여 로그인 정보를 암호화하고 복호화합니다.
- 퍼블릭 키 암호화 기법에서는 공개 키를 사용하여 데이터 조각을 암호화합니다. 그러면 수신자는 프라이빗 키를 사용해 이 데이터를 복호화합니다. 프라이빗 키와 퍼블릭 키를 **키 페어**라고 합니다. 인스턴스에 로그인하려면 다음 액션을 수행합니다.
    - 키 페어를 생성합니다.

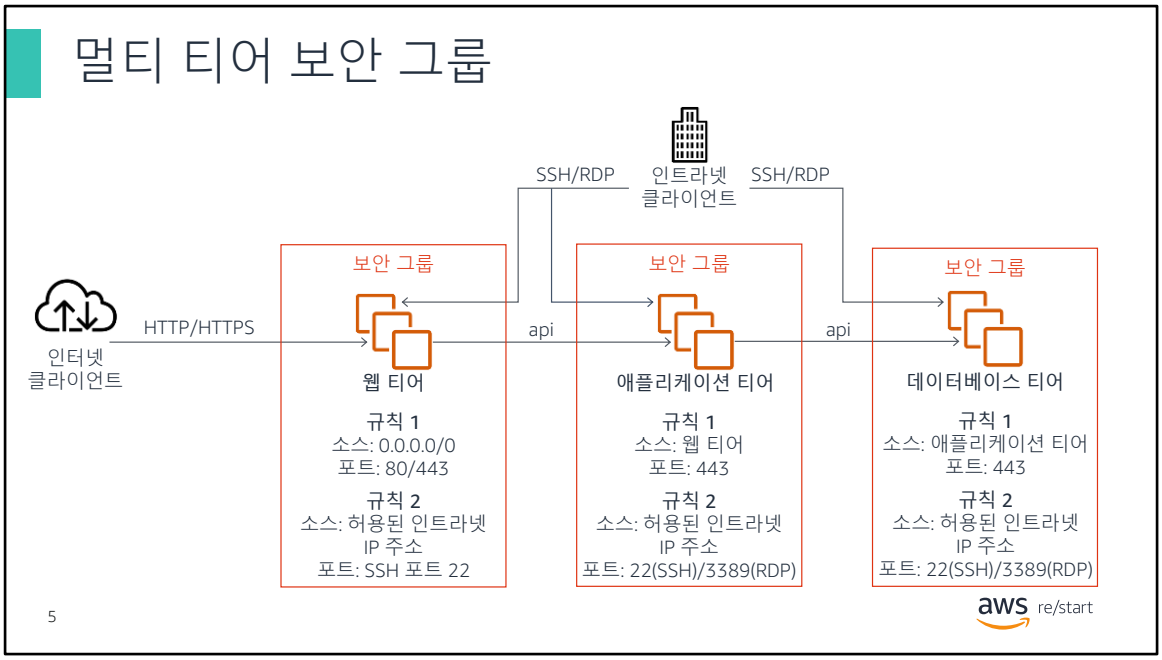
- 인스턴스를 시작할 때 키 페어의 이름을 지정합니다.
- 인스턴스에 연결할 때 프라이빗 키를 제공합니다.

Linux 인스턴스는 암호가 없으므로 Secure Shell(SSH)을 사용하여 로그인하는 데 키 페어를 사용합니다.

Microsoft Windows 인스턴스는 Remote Desktop Protocol(RDP)을 통해 로그인할 수 있도록 관리자 암호를 획득하기 위해 키 페어를 요구합니다.

보안 그룹은 상태 기반이지만 네트워크 ACL은 무상태 방식입니다.

- **상태 기반**이란 컴퓨터가 일반적으로 그 목적으로 지정된 스토리지 설정에 값을 설정하여 상호 작용 상태를 추적하는 것을 의미합니다.
- **무상태 방식**이란 발신자 또는 수신기에 정보가 유지되지 않는다는 뜻입니다. 각 상호 작용 요청은 수반하는 정보에 기반해서만 처리해야 합니다.



이 다이어그램은 기본적인 3티어 웹 애플리케이션 아키텍처에 적용된 AWS 보안 그룹 설계의 예시입니다. 이 멀티 티어 웹 아키텍처를 위해 각기 다른 보안 그룹 규칙이 생성되었습니다.

웹 티어부터 보자면, 정의된 규칙이 소스 0.0.0.0/0을 선택하여 **포트 80/443**을 사용하는 인터넷의 어느 곳에서나 트래픽을 허용합니다.

애플리케이션 티어의 경우, 보안 그룹이 보안 HTTPS 포트(443)를 사용하는 웹 티어에서 오는 트래픽만 허용합니다. 마찬가지로, 데이터베이스 티어는 포트 443을 사용하는 애플리케이션 티어에서 오는 트래픽만 허용합니다.

마지막으로, 모든 티어에서 SSH 포트 22 또는 RDP 포트 3389를 통해 기업 네트워크(인트라넷)의 허용된 IP 주소에서 원격 관리를 허용하기 위해 규칙이 생성되었습니다.

자세한 내용은 **Amazon VPC 사용 설명서**의 VPC의 보안 그룹을 참조하십시오.

핵심 사항

- AWS는 하나 이상의 인스턴스에 대한 트래픽을 제어할 수 있는, **보안 그룹**이라는 **가상 방화벽**을 제공합니다.
- 보안 그룹은 **상태 기반**입니다.
- 인스턴스에 대한 액세스를 제어하려면 **보안 그룹 규칙**을 만듭니다.
- 보안 그룹은 **AWS Management Console**에서 관리할 수 있습니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- AWS는 하나 이상의 인스턴스에 대한 트래픽을 제어할 수 있는, 보안 그룹이라는 가상 방화벽을 제공합니다.
- 보안 그룹은 상태 기반입니다.
- 인스턴스에 대한 액세스를 제어하려면 보안 그룹 규칙을 만듭니다.
- 보안 그룹은 AWS Management Console에서 관리할 수 있습니다.