Standard VPC를 활용한 Virtual Server 기반 DMZ 웹 서비스

개요

레거시 환경에서 높은 수준의 가용성과 확장성을 제공하는 웹호스팅 인프라를 구축하기 위해서는 복잡한 솔루션 설치가 필요하며 안정성 확보를 위하여 Peak 시에 대비한 용량 산정이 불가피했습니다. 이는 곧 리드타임과 운영비의 증가로 이어져 서비스 및 이익률에 좋지 않은 영향을 주었습니다.

SDS Cloud는 구성 즉시 인터넷 통신이 가능한 고객전용 네트워크(Standard VPC)와 확장성이 뛰어난 컴퓨팅 상품, 웹서비스를 위한 보안 상품들을 바탕으로 필요한 만큼의 웹 서비스 인프라를 빠르게 제공합니다. 이 문서에서는 SDS Cloud에서 Standard VPC를 활용한 Virtual Server 기반 DMZ 웹 서비스 아키텍처를 설명합니다.

아키텍처 다이어그램

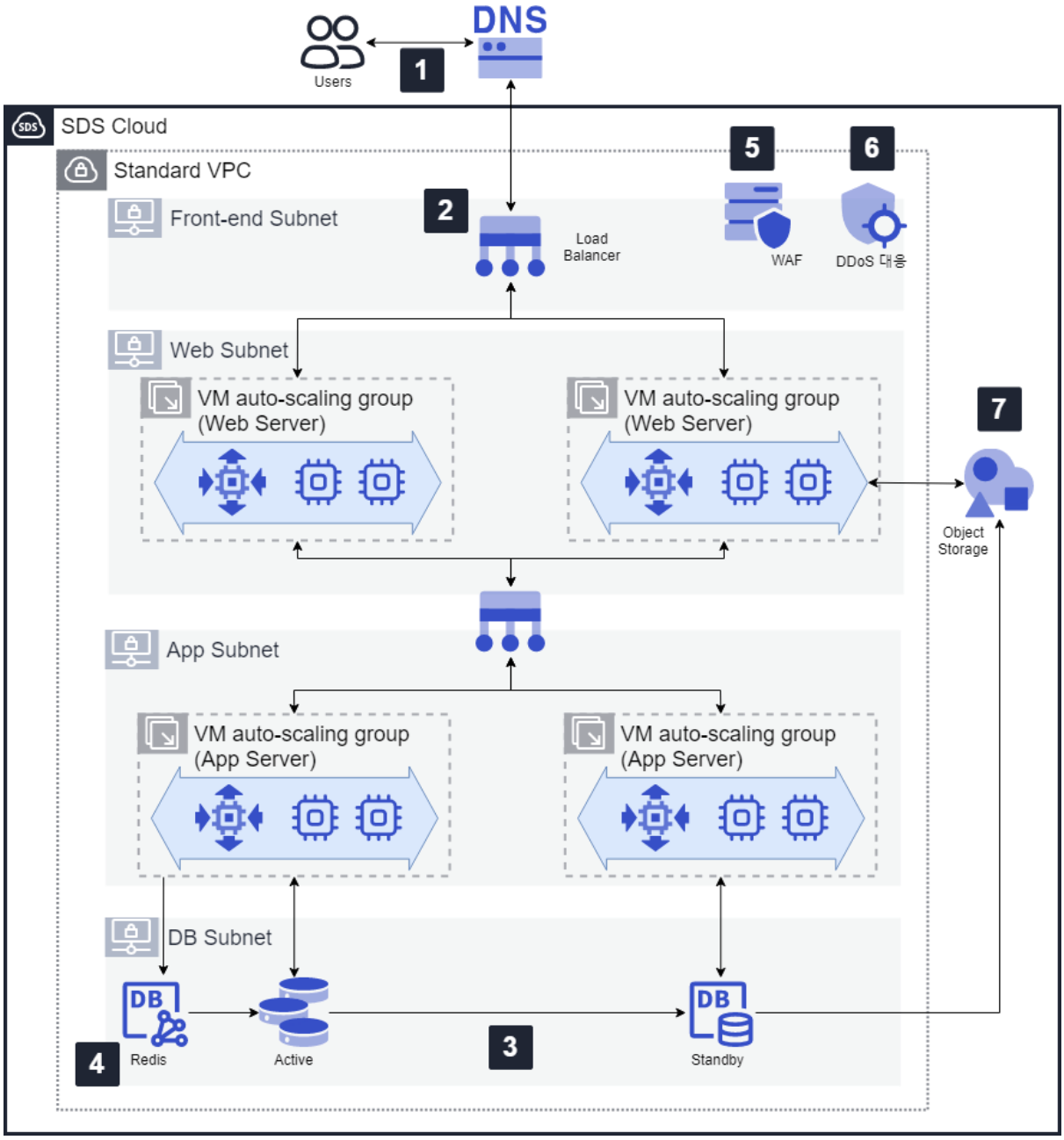

Figure 1. SDS Cloud를 활용한 DMZ 웹서비스 아키텍처 예시

1. **DNS** 서비스에서 외부에 오픈할 Domain Name을 설정하고 **Load Balancer**의 서비스IP와 연결한다. **Load Balancer** 서비스IP는 인터넷을 통한 접속이 가능한 Standard **VPC**에서 할당 받는다.
2. **Load Balancer** 는 웹 요청 트래픽을 다중 **VM Auto-Scaling** 그룹으로 분배하여 서비스 안정성을 높인다.
3. 관계형 데이터베이스는 가용성을 높이기 위해 이중화 구성한다. 7종의 관계형 데이터베이스 엔진을 선택 할 수 있다.

4. NoSQL 데이터베이스 서비스를 관계형 데이터베이스의 캐시로 활용하여 빈번한 요청의 응답시간을 줄일 수 있다.
5. **WAF** 서비스는 XSS나 SQL 인젝션과 같은 공격 트래픽으로부터 웹서버를 보호한다.
6. **DDoS 대응** 서비스를 이용하면 외부의 DDoS 공격에 자동 대응한다.
7. **Object Storage** 에 이미지나 비디오와 같은 정적 콘텐트를 저장하거나 데이터베이스 백업 용도로 활용 할 수 있다.

사용 사례

A. Standard **VPC**를 통한 퍼블릭 웹 서비스 제공

Standard **VPC**에서 제공하는 공인IP를 이용해 통해 퍼블릭 웹 서비스를 구성할 수 있습니다. **DNS**서비스로 해당 공인IP에 대한 Domain name을 손쉽게 등록 할 수 있습니다.

B. 서비스형 보안솔루션과 보안그룹 적용을 통한 웹보안성 확보

인터넷에 열려있는 웹서버의 보안성을 확보하기 위해 서비스형 보안솔루션을 구성할 수 있습니다. **WAF** 서비스에서는 웹사이트 트래픽을 모니터링 하여 공격을 탐지하고 차단합니다. **DDoS 대응** 서비스에서는 웹서버에 집중적으로 트래픽을 유발하여 서비스를 무력화 시키는 DDoS 공격을 탐지하고 차단합니다. 최소한의 허용정책으로 보안그룹을 설정하여 외부 공격으로부터 인프라를 보호할 수 있습니다.

선결 사항

없음

제약 사항

DDoS 대응 상품의 신청과 정책요청 시 별도 서비스 요청이 필요합니다.

고려 사항

A. 보안

보안정책 구성 시 외부에서 직접 접속이 필요한 **Load Balancer** 와 직접 접속이 필요하

지 않은 내부 인프라용 보안그룹을 구분하여 별도의 보안 정책을 적용 할 수 있습니다.

Security Group for VPC 서비스에서 서브넷별 허용 규칙을 설정하거나 **Security Group for VM** 서비스에서 Virtual Server 별 허용 규칙을 설정하여 불필요한 호스트의 네트워크 접근을 제어 합니다.

B. 서버리스

향후 **Cloud Functions** 서비스와 **API Gateway** 서비스 등을 이용하여 서버리스 웹 애플리케이션으로의 변화를 고려 할 수 있습니다.

관련 상품

- VPC
- DNS
- Load Balancer
- Security Group
- Virtual Server
- VM Auto-Scaling
- DB Service
- WAF
- DDoS 대응
- Object Storage
- Cloud Functions (‘21년 출시 예정)

관련 문서

- 웹 호스팅