Samsung Cloud Platform

Networking

Security Group

VM의 트래픽을 제어하는 가상 방화벽

Security Group은 클라우드 상의 가상 서버에서 발생하는 인바운드/아웃바운드 트래픽을 제어하는 가상의 논리적 방화벽입니다. VM 및 Database, Kubernetes Engine에서 발생하는 트랙픽에 허용 규칙을 설정하여 허가 받지 않은 트래픽을 필터링함으로써 가상의 네트워크 환경을 안전하게 보호할 수 있습니다.

높은 보안성

외부 인터넷이나 내부의 다른 VM에서 해당 VM과 주고 받는 인바운드 트래픽과 아웃바운드 트래픽에 대해 IP 주소와 포트 단위로 접근 정책을 설정하여, 허용된 트래픽만 접근이 가능하도록 함으로써 높은 보안성을 제공합니다.

편리한 보안규칙 설정

방화벽 보안 규칙 설정을 위해 서버에 직접 접근하지 않고도 웹 기반의 콘솔을 통해 인바운드 트래픽과 아웃바운드 트래픽에 대한 별도의 규칙 설정이 가능하며, 지정한 규칙마다 프로토콜과 포트 번호를 기준으로 허가 받지 않은 트래픽을 필터링 할 수 있습니다.
또한 방화벽 규칙 일괄 적용 기능을 제공하여 작업 시간을 단축하고 규칙 누락의 위험없이 손쉬운 방화벽 적용이 가능합니다.

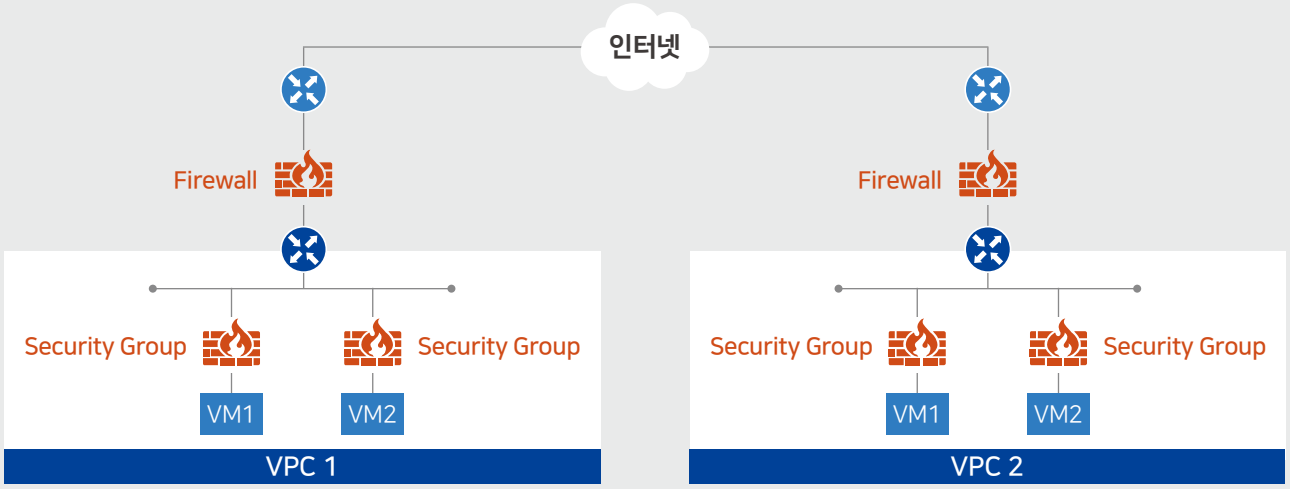
쉽고 간편한 네트워크 관리

웹 기반 콘솔을 통해 VM에 필요한 Security Group을 간편하게 생성할 수 있으며, 대상 주소 IP, 서브넷, 프로토콜/포트, 적용범위 등 적용 규칙을 편리하게 설정 및 관리할 수 있습니다.

손쉬운 로그 관리

Security Group에서 발생한 방화벽 로그를 사용자의 스토리지 자원을 활용하여 Security Group 별로 저장할 수 있습니다. Allow/Deny 로그를 저장할 수 있어 이슈 발생 시 빠른 원인 파악과 복구가 가능합니다.

서비스 구성도



주요 기능

- **Security Group 생성**
  - Distributed Firewall (VPC 내에서 VM간 통신을 제어하는 논리적 방화벽)
  - Virtual Server, GPU Server, Auto-Scaling Group, Database, Elasticsearch, Kubernetes Engine에서 사용할 Security Group 생성
  - Security Group을 사용하는 자원을 중심으로 인바운드는 출발지 IP, 아웃바운드는 목적지 IP만 설정하여 여러 자원에서 재사용 가능
- **Security Group 규칙 설정**
  - 대상 주소 IP 설정, 프로토콜/포트 설정, 인바운드/아웃바운드 설정
  - 규칙을 범위로 적용 (IP/Port를 ','와 '-'를 사용하여 다수의 주소 적용)
- **Allow/Deny 로그 저장**
  - Security Group 생성 시 로그 저장 여부 선택, 동일 프로젝트 내 Object Storage를 지정하여 저장 설정
  - 시간 별로 대상 주소 IP, Port, Allow/Deny 여부 저장

요금 기준

- **과금**
  - Security Group 서비스는 무료 제공

FOR MORE INFORMATION

SAMSUNG SDS

www.samsungsds.com / cloud.samsungsds.com
contact.sds@samsung.com / scp_sales@samsung.com
youtube.com/samsungsds