Tutorial

Security Group 설정

(Setting up Security Group)

October 2024

SAMSUNG SDS

시나리오 구성

Security Group 설정

학습 목표

#Virtual Private Cloud(VPC) #Subnet #Security Group

본 **Security Group 설정** 시나리오는 관리 목적으로 SSH(22), RDP(3389) 포트를 허용하는 규칙, 웹 서비스를 위해 VPC 내부-외부 간 80(http), 443(HTTPS) 포트를 허용하는 규칙, DB Service를 위한 규칙과 각 서버 그룹간 통신을 위한 2866포트 규칙을 Security Group 별로 구성되어 있습니다. Samsung Cloud Platform의 Virtual Server, Database 등 클라우드 상품을 사용하기 위해서는 사전에 Security Group이 먼저 생성되어야 합니다.

Security Group은 Virtual Server 단위 또는 IP 단위로 접근제어가 가능합니다. Security Group 정책 설정을 통해 VPC 내부 네트워크 트래픽 제어가 가능하며, 직접 Security Group을 생성하고 기본적으로 필요한 Security Group 정책을 설정할 수 있습니다.

Security Group의 Rule은 Security Group과 연결된 인스턴스에 도달할 수 있는 Inbound 트래픽과 인스턴스에서 나갈 수 있는 Outbound 트래픽을 제어하는 규칙들을 사용자가 직접 관리할 수 있도록 제공하고 있습니다.

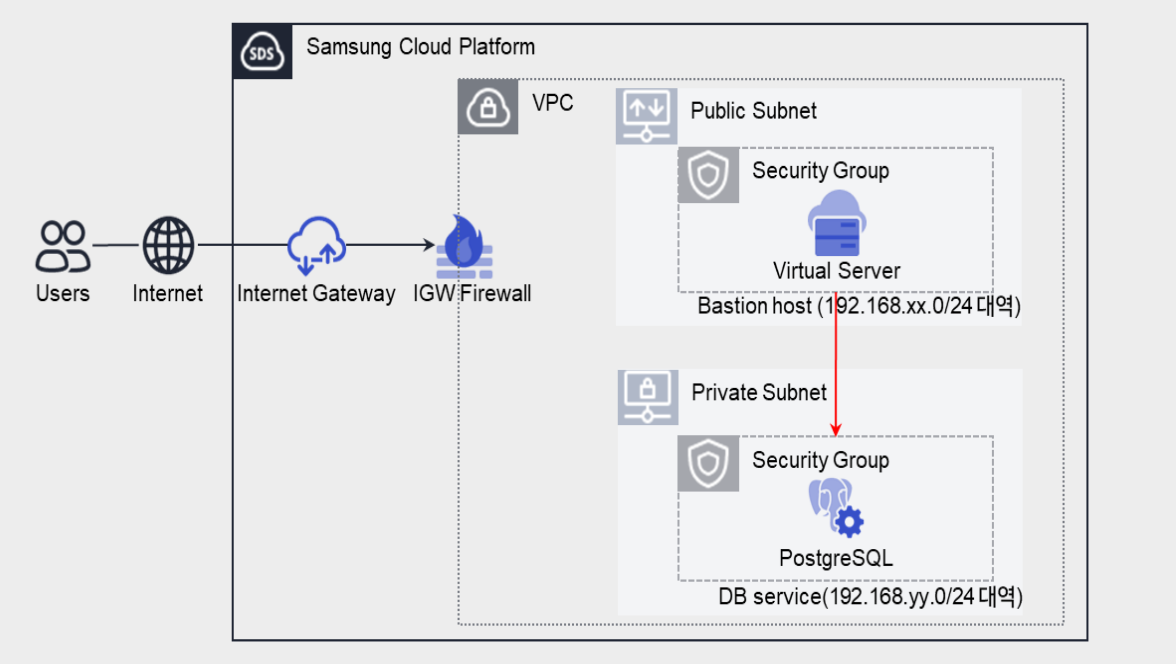

그림 1. Security Group 설정 시나리오 구성도

사전 작업

<사용되는 상품 리스트>

- Virtual Server
- VPC
- Security Group

따라하기

네트워크 환경 구성하기

1. VPC 상품 신청하기

    ① **Networking > VPC > VPC** 메뉴에서 **상품신청** 버튼을 클릭하세요. **VPC-VPC 신청** 화면으로 이동합니다.

    ② **VPC 신청** 화면에서 VPC 필수 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	VPC명	VPCtest

    ③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

2. Bastion Host 용 Public Subnet 서비스 생성하기

    ① **Networking > VPC > 서브넷** 메뉴에서 **상품신청** 버튼을 클릭하세요. **VPC-서브넷 생성** 화면으로 이동합니다.

    ② **서브넷 생성** 화면에서 해당 Subnet 의 필수 정보를 입력하세요.

    - Bastion Host 구성을 위한 Public Subnet 생성

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	VPC	생성한 VPC 선택
	사용 용도	일반 – Public
	서브넷명	PUBSUBtest
	IP 대역	192.168.xx.0/24

    ③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

3. Database 용 Private Subnet 서비스 생성하기

① **Networking > VPC > 서브넷** 메뉴에서 **상품신청** 버튼을 클릭하세요. **VPC-서브넷 생성** 화면으로 이동합니다.

② **서브넷 생성** 화면에서 해당 Subnet 의 필수 정보를 입력하세요.

- Database 구성을 위한 Private Subnet 생성

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	VPC	생성한 VPC 선택
	사용 용도	일반 – Private
	서브넷명	DBSUBtest
	IP 대역	192.168.yy.0/24

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

4. Bastion Host 용 Virtual Server 상품 신청하기

① **Compute > Virtual Server > Virtual Server 메뉴**에서 **상품신청** 버튼을 클릭하세요. **Virtual Server-Virtual Server 신청** 화면으로 이동합니다.

② **Virtual Server-Virtual Server 신청** 화면에서 이미지를 선택하고, 상품 구성 및 필수 정보를 입력하세요.

- 서버에 접속하기 위한 Key pair 는 기존에 생성된 Key 를 선택하거나 새롭게 생성할 수 있습니다.
- 미리 생성한 VPC, Subnet, Security Group 을 선택하여 연결하기 위해 적용 정책은 '**서버별 설정**'을 선택하세요.

화면	필수 입력 요소 항목	입력 값
이미지 선택	이미지	표준 - Windows
	이미지 버전	Windows 2019 Standard ENG (64bit)
상품 구성	서버 수	1
	(Block Storage) 기본 OS	bs-bastionTest
필수 정보 입력	서버 Key pair	생성한 Key pair 선택
	서버명 Prefix	bastionTest

네트워크 설정 - NAT	사용
네트워크 설정 - NAT IP	예약된 Public IP 선택
Security Group	생성한 Bastion Host용 Security Group 선택

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

5. Database 용 PostgreSQL 상품 신청하기

① **Database > PostgreSQL(DBaaS)** 메뉴에서 **상품신청** 버튼을 클릭하세요. **PostgreSQL(DBaaS) 신청** 화면으로 이동합니다.

② **PostgreSQL(DBaaS) 신청** 화면에서 이미지를 선택하고, 상품 구성 및 필수 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
이미지 선택	이미지	PostgreSQL Community
	이미지버전	PostgreSQL Community 15.5
상품 구성	서버명(Prefix)	pdb-test
	클러스터명	pdbclsTest
	상품 유형 – Block Stoage	(DATA) 10GB
	네트워크 – VPC	생성한 VPC 선택
	네트워크 – 일반 서브넷	생성한 Private Subnet 선택
	Security Group	생성한 Database용 Security Group 선택
필수 정보 입력	Database명	db Test
	Database 사용자	usrtest
	Database 비밀번호	사용할 비밀번호 입력
	Database 비밀번호 확인	사용할 비밀번호 입력
	Database Port 번호	2866
Replica 구성	Replica 구성	사용 안함

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

Security Group 구성하기

6. Bastion Host 용 Security Group 상품 신청하기

① **Networking > Security Group** 메뉴에서 **상품신청** 버튼을 클릭하세요. **Security Group 신청** 화면으로 이동합니다.

② **Security Group 신청** 화면에서 해당 Security Group 의 필수 정보를 입력하세요.

- Bastion Host 용 Security Group 생성

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	Security Group 명	BastionSGtest
	VPC	생성한 VPC 선택
	로깅 여부	사용 안함

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

7. Database 용 Security Group 상품 신청하기

① **Networking > Security Group** 메뉴에서 **상품신청** 버튼을 클릭하세요. **Security Group 신청** 화면으로 이동합니다.

② **Security Group 신청** 화면에서 해당 Security Group 의 필수 정보를 입력하세요.

- Database 용 Security Group 생성

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	Security Group 명	DBSGtest
	VPC	생성한 VPC 선택
	로깅 여부	사용 안함

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

Security Group 보안 규칙 추가하기

8. Bastion Host 용 Security Group 보안 규칙 추가하기

① **Networking > Security Group** 메뉴에서 **자원관리** 버튼을 클릭하세요. **Security Group 목록** 화면으로 이동합니다.

② **Security Group 목록** 화면에서 미리 생성한 Security Group 을 선택하세요.

③ **Security Group 상세** 화면의 **규칙** 탭에서 **규칙 추가** 버튼을 클릭하세요. **규칙 추가** 창이 팝업창이 열립니다.

④ **규칙 추가** 팝업창에서 해당 트래픽 관련 필수 정보를 입력하고, **확인** 버튼을 클릭하세요.

- Google 검색 창에서 “What is my ip”로 검색하면 사용자의 공인 IP 주소를 확인할 수 있습니다.

- 사용자 PC IP 에서 Bastion Host 로 들어오는 Inbound 트래픽 허용

화면	필수 입력 요소 항목	입력 값
규칙 추가 #1	방향	Inbound 규칙
	대상주소	사용자 PC 공인 IP 주소
	프로토콜	TCP
	허용포트	RDP(3389)

- Bastion Host 에서 Database 로 들어오는 Inbound 트래픽 허용

화면	필수 입력 요소 항목	입력 값
규칙 추가 #2	방향	Outbound 규칙
	대상주소	Bastion Host IP (192.168.xx.xx)
	프로토콜	TCP
	허용포트	직접입력(2286)

- Bastion Host 에서 Database 로 들어가는 Outbound 트래픽 허용

화면	필수 입력 요소 항목	입력 값
규칙 추가 #3	방향	Outbound 규칙
	대상주소	Database IP (192.168.yy.yy)
	프로토콜	TCP
	허용포트	직접입력(2286)

9. Database 용 Security Group 보안 규칙 추가하기

① **Networking > Security Group** 메뉴에서 **자원관리** 버튼을 클릭하세요. **Security Group 목록** 화면으로 이동합니다.

② **Security Group 목록** 화면에서 미리 생성한 Security Group 을 선택하세요.

③ **Security Group 상세** 화면의 **규칙** 탭에서 **규칙 추가** 버튼을 클릭하세요. **규칙 추가** 창이 팝업창이 열립니다.

④ **규칙 추가** 팝업창에서 해당 트래픽 관련 필수 정보를 입력하고, **확인** 버튼을 클릭하세요.

- Database 서비스 통신을 위한 Inbound 트래픽 허용

화면	필수 입력 요소 항목	입력 값
규칙 추가	방향	Inbound 규칙
	대상주소	Database IP (192.168.yy.yy)
	프로토콜	TCP
	허용포트	직접입력(2866)

정리하기

- Samsung Cloud Platform 에 IP 를 가진 컴포넌트들(Virtual Server, Database, Kubernetes Node 등)을 생성하기 위해서는 가상의 논리적 방화벽인 Security Group 이 반드시 필요합니다.
- 사용자는 Security Group 정책 설정을 통해 Security Group 내부로 들어올 트래픽에 대해 접근 제어를 할 수 있습니다.
- 기본적으로 Virtual Server 당, 즉 하나의 Security Group 당 100 개까지 Rule 설정이 가능합니다.
- Security Group 의 기본 정책은 Deny All 입니다. 기본적으로 Inbound/Outbound 에 Deny Rule 이 적용되어 있으며, 필요에 따라 Allow Rule 만 적용 가능합니다. 따라서 Rule 의 우선 순서는 없습니다.
- Security Group 의 경우에는 클라우드 자원 생성 시 적용한 자원의 IP 에 적용되는 정책이므로 허용하고자 하는 IP 만 등록합니다. (Inbound 의 경우에는 Source IP, Outbound 의 경우에는 Target IP 지정)
- 정밀한 접근 제어 및 관리를 위해서는 각 Virtual Server 또는 Database별로 동일한 보안 규칙을 공유하는 그룹끼리만 Security Group 규칙을 적용하는 것이 좋습니다.

- In/Outbound All Open(Any IP, Any Port) 오픈 정책은 클라우드 자원을 외부의 위협에 그대로 노출시킬 수 있습니다. 가능하면 필요한 IP 와 포트를 특정하여 정책을 설정해야 합니다.