SAMSUNG SDS

VPC 네트워크 환경 구성

(Configuring VPC Network

A DESCRIPTION OF THE PARTY OF T

The second second

M. LINE HARD

I A LEAN AND A LEAN AND A REAL PROVIDED AND A REAL

INTERCOLUMN THE

AND IN THE REAL PROPERTY OF - HEITERSON

Environment)

October 2024

Copyright 2024. Samsung SDS Co., Ltd. All rights reserved.

Contents

1.	학습목표	1
2.	들어가기	1
3.	사전 요구사항	4
4.	따라하기	5
5.	정리하기	20

1. 학습목표

- VPC(Virtual Private Cloud)의 개념을 이해합니다.
- VPC 생성 후 하나 이상의 서브넷 생성을 통해 네트워크 망을 분리 구성할 수 있습 니다
- VPC Firewall 정책 설정을 통해 VPC 내/외부 네트워크 트래픽 제어를 할 수 있습니다.
- Internet Gateway를 통하여 VPC와 외부 네트워크를 연결할 수 있습니다.
- 인터넷 사용이 가능한 Public 서브넷과 인터넷 사용이 불가한 Private 서브넷을 구 성할 수 있습니다.

2. 들어가기



2.2 관련 용어

No.	용 어	설 명
1	VPC (Virtual Private Cloud)	 -사용자가 정의하는 가상의 네트워크로 클라우드 상에 논리적으로 격리된 네트워크 공간을 할당하여 가상 네트워크에서 SCP 리소스를 이용할 수 있는 서비스 -관리자가 고객사별로 Uplink (외부연결 Network: 그룹망, 인터넷)를 사전에 설정하면 사용자는 해당 Uplink 하위에 VPC 를 생성함. 즉, 접속하는 망 특성에 따라 인터넷과 내부 네트워크에 연결하여 이용할 수 있음 -사용 목적에 따라 여러 개의 VPC 를 생성하여 타 사용자 그룹과 분리하여 독립적으로 운영할 수 있음
2	Subnet	 -VPC 의 IP 주소를 나누어 리소스가 배치되는 주소 범위를 의미하며, 서브넷 없이 VPC 를 이용할 수는 없음 -또한 하나의 VPC 안에 여러 개의 Subnet 이 존재할 수 있으며, IP 를 사용할 수 있는 가용 존의 크기를 고려해 적절한 크기의 Subnet 들을 분산해서 사용함 -Public Subnet 은 Virtual Server 에 1:1 공인 NAT IP 를 설정할 수 있는 Subnet 이며, Private Subnet 은 Virtual Server 에 1:1 공인 NAT IP 를 설정할 수 없는 Subnet 임 -Local Subnet 은 다른 서브넷 연결 또는 외부 접속이 되지 않고, VM 간의 직접 연결만을 허용하는 서브넷
3	Firewall	-VPC (Virtual Private Cloud)에서 발생하는 인바운드/아웃바운드 트래픽을 제어하는 가상의 논리적 방화벽 -외부와 VPC 내부 사이의 경계 방화벽으로 VPC 내부 Subnet/VM 간 통신은 제어가 불가함 -보안 정책에 따라 목적지(Destination)/출발지(Source) IP 에 대한 Inbound/Outbound Allow/Deny 정책 적용 가능, 또한 정책의 우선 순위(순서) 정의할 수 있음 -Rule Quota(Limitation)는 프로젝트 당 1,000 개(VPC 당 200~1000)의 정책 적용이 가능하며, 서비스는 무료 제공
4	NAT (Network Address Translation)	-IP 패킷의 TCP/UDP 포트 숫자와 소스 및 목적지의 IP 주소 등을 재기록 하면서 라우터를 통해 네트워크 트래픽을 주고받는 기술 - IPv4 의 주소 부족 문제를 해결하기 위한 방법으로서 고려되었으며, 주로 비공인(사설, local) 네트워크 주소를 사용하는 망에서 외부의 공인망(public, 예를 들면 인터넷)과의 통신을 위해서 네트워크 주소를 변환하는 것 -고객이 특정 NAT IP 를 Reserve 해서 사용할 수 있도록 IP Reserve 기능 사용 가능

No.	용 어	설 명
5	VPN (Virtual Private Network)	-네트워크 간에 터널링 및 암호화 기법을 사용해 만든 가상 사설망 네트워크 -외부 고객 네트워크와 SDS 클라우드 네트워크를 IPSec 기반의 암호화된 가상 전용망으로 연결하는 서비스
6	Direct Connect	-고객사 내부 네트워크 연결을 위한 상품으로 인터넷/VPN 이 아닌 전용선을 통해, 고객사 네트워크와 통신 제공
7	Internet Gateway	-VPC가 외부 인터넷과 통신이 가능하도록 제공하는 업링크 인터넷 연 결
8	VPC Peering	-VPC 간의 1:1 Private 통신 기능 제공
9	Transit Gateway	-다수 VPC간 연결, 고객사망 연결, 다른 위치/PJT Transit gateway 와 연결
10	NAT Gateway	-NAT IP가 매핑되지 않은 Virtual Server의 인터넷 사용을 위해 Outbound트래픽에 대해서 1개의 대표 공인IP로 매핑

3. 사전 요구사항

3.1 프로젝트 선택

- Samsung Cloud Platform Console 에 로그인 시 전체 프로젝트 대시보드 화면이 보입니다. 좌측 상단의 '프로젝트를 선택하세요'를 클릭하여 실습에 사용할 프로젝트를 선택하세요.

Samsung Cloud Platform Enter	erprise	프로젝트를 선택하세요.	^	대시보드	
Cverview ^	전치	프로젝트명으로 검색	Q		
대시보드		Home		00	740
모든 프로젝트			- 11		
상품 탐색					치기
서비스 상태 조회			, i	ž	연세
🔄 Marketplace				다야하	
SW Catalog			, 2 2	기슬력을 되슬력을 적의 클라우드	
闻 Bookmarks		플랫폼을 제공합니다. 고객의 수준의 가용성과 보안 서비스 클라우드 환경을 쉽고 편리하	업무 목 를 제공하 게 사용하	텍에 맞는 높은 ¦는 유연한 ነ세요.	지난
				자세히보기 〉	

3.2 위치(가용영역) 선택

- 프로젝트를 선택하셨으면 상품을 생성할 위치를 선택하여야 합니다.
- 좌측메뉴의 모든 상품 클릭한 후 실습에 사용할 위치를 선택합니다.
 - WEST Region: KR-WEST-1, KR-WEST-2, KR-WEST
 - EAST Region: KR-EAST-1

Samsung Cloud	Platform Enterpris	e	~	모든 상품	+
Project	^	모든 상품 위치	KR-WEST-2	^	(i)
			KR-WEST-1		
대시보드		Compute	KR-WEST-2		Virtual Server 🎖
프로젝트 개요			KR-WEST		
권한관리(IAM)		intual Ser	KR-FAST-1		설명 및 주요기능
비용관리		Virtual			
자원과리		Custom	Image		virtual Server – CP0,
		Migratic	on Image		클라우드 환경에서 개발
E Product	^	Placem	ent Group		1. 쉽고 편리한 컴퓨팅 환
			러레아다		웹 기반 콘솔을 통해 VM 개입 없이도 손쉽게 증석
모든 상품		IN 전원인	1경 예약		
		GPU Serve	r	~	2. 다양안 유영의 상품 사 사저 전이되 VM Spac (
🕎 Marketplace	^	Auto-Scalir	ng	\sim	
SW Catalog		Virtual Ser	ver DR	\sim	- 일만 VM : 일만적으로
		Bare Metal	Server		- 대용량 VM : 일반 VM
3₩ 전덕		Dare Metal			3. 강력한 보안 적용
Bookmarks		Multi-node	GPU Cluster	~	Security Group 서비스
DUDKIIIdIKS		HPC Cluste	r		눈덩일 수 있습니다.

4. 따라하기

4.1 VPC 상품 신청하기

 ① 모든 상품 → Networking → VPC → VPC 를 선택한 후 [상품신청] 버튼을 클릭합니다.

※ 프로젝트 하나당 생성 가능한 VPC의 개수는 최대 5개입니다.

Project	^	모든 상품 위치 KR-WEST-2	✓ ① 2E % B O Q
대시보드			
프로젝트 개요		Compute (9)	> VPC 상품 정보
권한관리(IAM)		Virtual Server	^ 설명 및 주요기능 릴리즈 노트 가이드 및 문서
비용관리		Virtual Server	VDC는 코라이드 하거에서 노키지이르 도리티 그게 저요. LM 네르의ㅋ 고가은 제코지는 사프이니다. LL요 모지에 따라 Dublic Subact. Drusta Subact 그리그, 서비 카이 투시의
자원관리		Custom Image	바란은 물러부는 편하게 전력적으로 적용한 또한 적물 책으라는 이용을 제공하는 이용을 해야하는 이용을 해야 하는 이용을 가지 않는 것이다. Sublick, Fillette Sublick, 그런 또 지하 전력 이용 전을 위한 소 이이며, VPC
		Migration Image	가는 20년 동생 VPC 간 연결 구성이 가능합니다. Pering을 통해 VPC 간 연결 구성이 가능합니다.
Product	^	Placement Group	1. 안전한 가상 네트워크 환경
모든 상품		IP 일괄변경 예약	클라우드 환경에서 안백하게 독립된 가상의 네트워크를 제공하며, VPC와 연결된 모든 구간에 사용자가 설정 가능한 방화벽 및 로그 관리 기능을 제공합니다. 따라서 클라우드 환경에서도 보안적으로 안전하게 고객이 전하는 특징적인 네트워크 환경을 구축할 수 있습니다.
		GPU Server	· 2. 다양한 서브넷 음신 제공
Marketplace	^	Auto-Scaling	VPC 내에서 용도와 및게 네트워크를 구성할 수 있도록 입반 시코보넷(Public/Private)과 세바탕간의 통신을 위한 로칠 서브넷으로 세문화하여 재공합니다. 또한 서버의 클러스터 구성 등 사용자가 서브넷 가야하라는 것이 나는 지수 않는 사용자가 서브넷 가야하라는 것이 나는 지수 않는 것이 나는 것이 않는 것이 없는 것이 않는 것이 없는 것이 없는 것이 않는 것이 않는 것이 없는 것이 않는 것이 없는 않은 것이 없는 않아.
SW Catalog		Virtual Server DR	나의 사실/P을 시장에서 사용될 수 있는 Witual P을 제상하여 다양한 세비 구장이 가중합니다. ▼ 2. 기요금요 //문란의 그 거기 개신
SW 관리		Bare Metal Server	3. 사용포는 데트워크 가장과 제어 VPC Peering을 통해 VPC간 사실IP 기반의 통신 연결 기능을 제공하며, NAT Gateway, Internet Gateway를 자유롭게 선택하여 편리하게 네트워크 구성이 가능합니다. 연결 구간 별로 방좌벽과 로그
all market and		Multi-node GPU Cluster	관리 기능을 제공하며, 라우팅 설정을 통해 사용자가 손쉽게 트레픽을 제어할 수 있습니다.
Bookmarks			4. 효율적인 네트워크 운영 이다네 여겼다. 피아하 네트워크에 귀개나 내보면 여겼다. 피아하 네트워크 든 다야하 문제에 네트워크를 노키제이곤 가려하게 그셔하이르며 그 네요이 드키 네트워크 이코카에 비해 비요 중송재이곤 귀개
		Cloud Functions	전에 있는 것 같은 이 물로 한 이는 위스가 보거가 제작이 안물가 물건한 제품가 이 이 것은 가지가 제공 유가를 한 가지구도 안전하게 가장을 느꼈기 또 아이가 물러져드며, 또 한 안터넷 연결이 안된 VPC에서도 Object Storage 점속이 가능하도록 실제되어 대응량 데이터를 효율적으로 저장할 수 있습니다.
		Planned Compute	
		Storage (6)	v.
		Database (7)	v
		Data Analytics (10)	v
		Application Service (4)	v
		Container (3)	v
		👷 Networking (15)	~
		VPC	A
		VPC	
		서브넷	
		Public IP	
		NAT Gateway	
		Internet Gateway	
		VPC Peering	
		Routing Table	
		Production	사건한테 너희 정종건정

② 상품신청(VPC) 상세화면에서 VPC 명을 입력, 중복체크 한 후 다음 버튼을 클릭합니다.

[입력정보] - VPC 명: 명명규칙 참고하여 VPC 명 기입 ("VPC" + 본인 ID, 예시: VPCxx) - 태그: 태그추가 버튼을 눌러 생성. (Key, Value 값 설정, 예시: Key: SCP Value: Userxx)

< VPC - VPC 신청 🕒	위치 KR-EAST-1	v .		모	특상품 > VPC - VPC 신청
필수 정보 입력				∠ 필수정보입력	•••• 신청 정보 확인
VPC명 *	VPCxx 사용 가능한 이름입니다.	<u>중</u> 복체크 5/1		■ 예상 금액 신청한 상품 총 1개	
알평 DNS Service IP ①	50자 어대도 접역하세요. 192.168.254.254	0/50		VPC	₩ 0
VPC 생성 후, 원하는 IP대역을 인터넷 통신을 원하는 경우, Ir	100자 이하의 검색어를 입력 + 신규 생성/적용	태그 추가			
추가 정보 입력	관련 정보가 없습	선택한 자원에 태그를 추가/수정/삭제 할 수 있습니다. 자원마다 최대 기존 태그 선택	# 50개까지 태그 등록이 가능합니다. 신규태그 추가는 상품신	청 완료 후 적용됩니다.	
테그 (1)	태그 주가 ① 신규태그 추가는 상품신청 완				
					0/50
		신규생성/적용 총 0		생	ġ
		Key *	Value		_
			관련 정보가 없습니다.		
				취소	확인

생성	신규생성/적용 총0
Value	Key *
Iserxx 적용 🛞	SCP
Isenox	SCP

선택한 자원에 태그	!를 추가/수정/삭제 할 수 있습니다. 자원마다 최!	대 50개까지 태그 등록이 가능합니다. 신규태그 추가는 상품신청 완료 후 적용됩니다.	
기존 태그 선택	SCP:Usenx ×		
			1/5
신규생성/적용 총	1		1/5 생성
신규생성/적용 총	1 Key *	Vatue	1/5 생성

< VPC - VPC 신청	위치 KR-EAST-1 V		· 모든상품 > VPC - VPC 신청
필수 정보 입력		∠ 필수 정보 1	<mark>입력</mark> ···· 신청 정보 확인
VPC명 *	VPCxx 중복체크 사용 가능한 이름입니다. 5/17	■ 예상 금액	
설명 DNS Service IP ①	50자 이내로 알락하세요. 192.168.254.254 0/50	VPC	₩ 0
VPC 생성 후, 원하는 IP대역 인터넷 통신을 원하는 경우,	I은 압력하여 서브랫은 생성하시기 바랍니다. Internet Gateway를 생성하여 VPC와 연결할 수 있습니다.	운영 중, 자원/서비스 추가 비용 	응은 별도 청구됩니다. 총 예상 금액(1개월)
추가 정보 입력			₩ 0
태그 1 🛈	태그 추가 SCP:Userxx × ● 신규태그 추가는 상품신청 완료 후 적용됩니다.		
			다음

③ VPC 신청 정보 확인에서 프로젝트명, VPC 명을 확인한 후 이상이 없으면 완료 버튼을 클릭합니다. VPC 를 구성하면 Internet Outbound Traffic 요금과 Public

IP, NAT Gateway, VPC Peering 추가 기능 선택 시 요금이 과금됩니다.

< VPC - VPC 신청 : 위치: KR-EAST-1	> 모든상품 > VPC - VPC 신청
신청 정보 확인	필수 정보 압력 🗶 신청 정보 확인
	신정한 상품 총 1개
VPC	₩ 0
VPCB VPCxx	
	예상 금액 ₩ 0
	이전 완료

④ 상품신청 팝업화면에서 확인 버튼을 클릭하여 VPC 상품신청을 완료합니다.

취소	확인
	취소

⑤ 생성된 VPC 를 확인합니다.

VPC							
총 1 🗆 20 개씩 보기 \vee		All	Му	100자 이하의 검색어를 입력하세	R.	Q 상세검색	상품신청
VPC명 三	VPC ID	IG	N 연결	생성일시 🖅	위치 三	상태	
VPCxx		0	사용			Active	상품해지

4.2 IGW 연결하기

① VPC 가 외부 인터넷과 통신이 가능하도록 Internet Gateway 를 연결합니다.
 모든 상품 → Networking → VPC → Internet Gateway 를 선택한 후

'IGW 생성' 버	튼을 클릭합니다.		
Samsung Cloud Platform En	RE 상품 비위치 KR-WEST-2	+ × 0	·모든상품 () 12 [
대신보드 교문적표 개요 관련관리(IAM) 비용관리 자원관리 Product ^ IZE 상용 W Catalog SW 관리 SW 관리 57 P Bookmarks	Compute (9) Virtual Server Virtual Server Custom mage Migration mage Migration mage Placement Group IP 일괄번경 여약 GPU Server CPU Server CPU Server Auto-Scaling Virtual Server R Mutti-node GPU Cluster Cloud Functions Planned Compute Storage (6) Storage (6) Data Analytics (10) Data Server (1) QPC Application Service (4) VPC Adus? VPC Adus? VPC Adus? VPC Adus? VPC Adus? VPC Adus? VPC MAT Gateway VPCPPereing Routing Table Containe Containe Containe Containe Routing Table Containe Contain	설명 및 주요가능 요리 도 지 기의 및 맞서 내 다 가 다 한 반 다 가 하 다 되 한 가 너 데 및 가 하 다 더 가 하 다 다 한 다 가 하 다 다 한 다 가 하 다 다 한 다 가 하 다 다 한 다 가 하 다 다 한 다 가 하 다 다 한 다 하 가 하 다 다 한 다 하 가 하 다 다 한 다 하 가 하 다 다 한 다 하 가 하 다 다 한 다 하 가 하 다 다 한 다 하 가 하 다 다 한 다 하 가 하 다 다 한 다 한 다 한 다 한 다 한 다 한 다 한 다 한 다 한	

② Internet Gateway 필수정보입력 화면에서 Internet Gateway 를 연결할 VPC 를 선택한 후 다음 버튼을 클릭합니다. Firewall 사용을 체크하고, Firewall 로깅 여부는 선택을 해제합니다. 하단의 Firewall 사용 체크 시, Firewall 이 자동으로 생성되며, 로깅 여부 체크 시 Firewall 의 로그를 저장할 Object Storage 버킷을 지정해야 합니다.

마지막으로 태그추가 버튼을 눌러 태그를 지정합니다.

VPC 생성 시 사용한 태그를 적용해 줍니다.

VPC - Internet	Gateway 생성 위치 KR-EAST-1 🗸	모든상품 > VPC - Internet Gateway ?
필수 정보 입력		✓ 뻗수 정보 압력 ···· 신청 정보 확인
VPC *	VPCxx ~	
구분 *	Internet Gateway	· 예상 금액 신청한 상품 총 1개
Internet Gateway명	IGW_VPCxx	
설명	50자 아내로 입력하세요. 0/50	Internet Gateway ₩ 0 트래픽 사용량에 따른 추가 요금이 과금될 수 있습니다.
Default 라우팅이 지정되지	지 않은 VPC만 Internet Gateway 신청이 가능합니다.	
Firewall 사용 🕕	✓ 사용	총 예상 금액(1개월)
Firewall 로깅 여부	· 사용	WO
	로그 저장을 사용하는 경우로그 저장소를 먼저 설정해야 합니다. 로그 저장소를 설명하면 로그 저장에 대한 Object Storage 요궁이 과금됩니다. NAT 로킹은 위에서는 (IP/C-Internet Gateway상세)에서 NAT 로깅 설정을 해야 합니다. 로그 저장소 설정 바로가기 100자 이야의 김색어를 입력하세요. Q.	
추가 정보 입력	+ 신규 생성/작용 ✓ SCP-Userxx	
H1 1	테그추가 SCP:Usenxx ×	
	① 신규태그 추가는 상품신청 완료 후 직용됩니다.	
		다음

③ Internet Gateway 신청 정보 확인에서 Internet Gateway 에 연결된 VPC 명을 확인한 후 이상이 없으면 완료 버튼을 클릭합니다.

< VPC - Internet Gateway 생성 : 위치: KR-EAST-1			> 모든상품 > VPC - Internet Gateway 생성
신청 정보 확인			필수 정보 입력 … 🗶 신청 정보 확인
			신청안 상품 총 1개 달 예상 청구 금액(월 기준) 약 ₩ 0
Internet Gateway			₩ 0
Internet Gateway명 IGW_VPCxx	VPC명	VPCxx	
			예상 금액 🛛 ₩ 🛛
			이전 완료

④ 상품신청 팝업화면에서 확인 버튼을 클릭하여 Internet Gateway 상품신청을 완료합니다.

상품신청		×
상품신청을 하시겠습니까?		
	취소	확인

⑤ 생성된 Internet Gateway 를 확인합니다.

Internet Gateway						
총 1 🗆 20 개씩 보기 \vee	All	Мy	Internet Gateway명을 입력	력하세요. (Q 상세검색	IGW 생성
Internet Gateway명 三	VPC명 三		구분	생성일시 + 🗄	상태	
IGW_VPCxx	VPCxx		Internet Gateway		Attached	÷

4.3 Subnet 추가하기

① 앞 단계에서 생성한 VPC 내에 서브넷을 생성하는 단계입니다. 모든 상품 → Networking → VPC → 서브넷을 선택한 후 '서브넷 생성' 버튼을 클릭합니다.



② 아래 항목을 참고하여 VPC 및 사용용도 선택, 서브넷명, IP 대역을 기입, 중복체크를 수행한 후 다음 버튼을 클릭합니다.

[입력정보]

1. Bastion Host 용 Public Subnet - 사용용도: 일반 → Public 을 선택합니다. - 서브넷명: 명명규칙 참고하여 서브넷 명 기입 ("PUBSUB" + 본인 ID, 예시: PUBSUBxx) - IP 대역: 명명규칙 참고하여 서브넷 IP 대역 기입 (예시: 192.168.xx.0/24) 후 중복체크 실행 2. 웹서비스용 Private Subnet - 사용용도: 일반 → Private 을 선택합니다. - 서브넷명: 명명규칙 참고하여 서브넷 명 기입 ("PRISUB" + 본인 ID, 예시: PRISUBxx) - IP 대역: 명명규칙 참고하여 서브넷 IP 대역 기입 (예시: 192.168.yy.0/24) 후 중복체크 실행 3. DB Service 용 Private Subnet (laaS/DB 실습에서만 사용) -사용용도: 일반 → Private 을 선택합니다. -서브넷명: 명명규칙 참고하여 서브넷 명 기입 ("DBSUB" + 본인 ID, 예시: DBSUBxx) - IP 대역: 명명규칙 참고하여 서브넷 IP 대역 기입 (예시: 192.168.zz.0/24) 후 중복체크 실행

③ 서브넷 신청 정보 확인에서 VPC 명, 서브넷명을 확인한 후 이상이 없으면 완료 버튼을 클릭합니다.

④ 상품신청 팝업화면에서 확인 버튼을 클릭하여 서브넷 상품신청을 완료합니다.

청 정보 확인		필수 정보 입력 🚥 🖊 신청 정보 회
		신청한 상품 문
서브넷		₩ (
셔브넷링 PUBSUBixx	VPC8 VPCx	
		예상금액 ₩ (

VPC - 서브넷 싱	방성 □위치 KR-EAST-1 ∨			모든상품 > VPC - 서브
수 정보 입력			∠ 필수 정보	<mark>보입력</mark> ···· 신청정보확
: *	VPCxx	~		
용도 * (1)	일반 로컬		예상 금액 신청한 상품 총 12	개
	Public Private		서비네	** 0
넷명 *		중복체크		
역 * (j	NS편 두 교는 시트였장입니다. 192.168.0.0/24	중복체크		총 예상 금액(1개월)
	사용 가능한 IP 입니다.			₩ 0
way	192.106.0.1 50자 이내로 입력하세요.			
		0/ 50		
저나이려	+ 신규 생성/적용			
97 B 4	SCP:Userx			
1 (1)	태그 추가 SCP:Userxx × ① 신규태그 추가는 상품신청 완료 후 적용됩니다.			
	④ 신규테그 추가는 상품신청 환료 후 적용됩니다.			

상품신청		×
상품신청을 하시겠습니까?		
	취소	확인

- ⑤ 하나의 서브넷을 생성했으면 아래의 서브넷 자원관리 화면에서 [서브넷 생성]을 클릭해서 다른 서브넷을 만듭니다. 상태가 'Creating'이더라도 상관없이 진행할 수 있습니다.
- ⑥ 모든 서브넷을 생성했으면 서브넷이 모두 맞게 생성되었는지 확인합니다. 특히 VPC 와 CIDR 이 제대로 입력되었는지 다시 한번 확인해봅시다.

서브넷								
총 3 🗆 20 개씩 보기 ∨			All	My 100자 (이하의 검색어를 입력	력하세요.	Q 상세검색	서브넷 생성
서브넷명 三	서브넷 ID	VPC명 三	IP 대역 드	사용 용도	Gateway	생성일시 🖅	상태	
DBSUBxx	SUBNET	VPCxx	192.168.1…	일반	192.168		Creat…	삭제
PRISUBxx	SUBNET	VPCxx	192.168.5…	일반	192.168		Creat…	삭제
PUBSUBxx	SUBNET	VPCxx	192.168.0…	일반	192.168		Active	삭제

4.4 Firewall 규칙 추가하기

① VPC 의 방화벽 기능을 사용하기 위하여 모든 상품 → Networking → Firewall 화면으로 들어갑니다. 앞서 IGW 생성시, Firewall 사용에 체크하였다면, Firewall

이 생성되어 있습니다. (자원관리 탭에서 확인)

Popiert C C
que Image de la constante Jarde de la constante <t< td=""></t<>
Global CDN

 ② 앞 단계에서 생성한 VPC - Internet Gateway 의 Firewall 상태가 'Active'인 것을 확인합니다. 목록에서 해당 Firewall 을 클릭하여 Firewall 상세 화면으로 진입합니다. (Firewall 명칭 제일 뒷부분의 본인이 생성한 VPC 명을 확인합니다. 예) FW_IGW_VPCxx)

Firewall								
총 1 20개씩 보기 ∨					100자 이하의	검색어를 입력하	세요.	Q 상세검색
Firewall명 三	Firewall 구분 三	VPC 명 +=	연결명	Fire	wall 규칙 수	로깅 여부	위치 三	상태
FW_IGW_VPCxx	Internet Gateway	VPCxx	IGW_VPCxx		0	미사용	KR-EAST-1	 Active

③ Firewall 상세 화면에서 '규칙' 탭으로 이동합니다.

< Firewall 상세 + FW_	JGW_VPCxx		> 자원관리 > Firewall 상세 (> [건
Active	02 024 4		
상세정보	규칙 태그 작업이력		
프로젝트명		위치	KR-EAST-1
상품/서비스	firewall	자원 유형	firewall
자원명	FW_IGW_VPCxx	자원 ID	FIREWALL-m6CYIcw8qnmNdpAVOS_j
생성자		생성일시	2023-06-27 11:21:04 (Asia/Seoul, GMT +09:00)
수정일시	2023-06-27 11:21:09 (Asia/Seoul, GMT +09:00)		
SRN	srn:public:KR-EAST-1:KOREA-EAST-1-SCP-B001:PR0JECT-88pFHL6-tEjSDesnC	_GPkd:firewall:firewall/FIREWALL-	m6CYIcw8qnmNdpAVOS_j ርታ
Firewall명	FW_IGW_VPCxx	Firewall ID	FIREWALL-m6CYIcw8qnmNdpAVOS_j
Firewall 구분	Internet Gateway	VPC 명	VPCxx
연결명	IGW_VPCxx	VPC ID	VPC-i3t9ScNMqTjOhQ5qFm0rkh
Firewall 규칙 수	07#	프로젝트 Firewall 규칙 수 🕕	0개 / 최대 1,000개
로깅 여부 🕑	 미사용 	로그 저장소 (j)	

④ '규칙추가' 버튼을 클릭합니다.

Firewall 상세 🗆	FW_IGW_VPCxx								> 자원관리	> Firewal	II 상세 O
• Active		연결해제									
상세정보	규칙	태그	작업이력								
총 0 20 개씩 보기 ∨	엑셀 다운로드	규칙 추가 규칙 일괄	입력 I Inbound 🗌	Outbound 🗌 In	-Out		100자 이하의	검색어를 입력하세요		Q	상세검색
순서	규칙 ID	규칙 Index 🕕	출발지 IP	목적지 IP	서비스	동작	방향	활성 여부	설명		상태
				과려 저!	- 기 없습니다.						
					- 1 and had 1 1 1						

⑤ 규칙추가 화면에서 Inbound/Outbound 영역의 각 보안 적용 사항을 작성합니다.

[정책 설정 실습]

아래의 내용을 참고하여 Firewall 정책 설정을 실습해 봅니다, 기본적인 인터넷 사용을 Internet Gateway 를 통해 VPC 내부-외부 간 80(http), 443(https) 포트를 열어보는 정책과 이후 실습에서 사용할 Bastion host 로의 접속을 위한 22(ssh),

3389(RDP)포트를 여는 실습을 진행합니다.

[입력정보]

- 출발지 주소: 출발지 주소 입력
- 목적지 주소: 목적지 주소 입력
- 허용포트: 직접 입력 또는 Well Known Port 선택 가능
- 방향: Inbound/Outbound 선택

* Google 검색창에서 "What is my ip"로 검색하면 내 PC 의 Public IP 를 확인할 수 있습니다.

출발지 주소	목적지 주소	허용 포트	프 토 포	동작	방향	용도
0.0.0.0/0 (인터넷)	192.168.zz.0/27 (LB서비스 IP 대역)	HTTP (80)	TCP	Allow	Inbound	인터넷에서 Load Balancer 의 IP대역으로 오는 웹서비 스 인바운드 트래픽 허용
내 PC IP	192.168.zz.0/27 (LB 서비스 IP 대역)	SSH (22) RDP(3389)	TCP	Allow	Inbound	내 PC에서 Bastion host 앞의 Load Balancer로 오 는 인바운드 관리자 트래픽 허용
192.168.xx.0/24 (PUBSUBxx IP대역)	0.0.0.0/0 (인터넷)	HTTP (80) HTTPS(443)	TCP	Allow	Outbound	Public Subnet에서 인터넷 으로 가는 시스템 업데이 트, 웹서비스 응답용 아웃 바운드 트래픽 허용
192.168.yy.0/24 (PRISUB IP대역)	0.0.0.0/0 (인터넷)	HTTP (80) HTTPS(443)	TCP	Allow	Outbound	Private Subnet에서 인터 넷으로 가는 시스템 업데이 트, 웹서비스 응답용 아웃 바운드 트래픽 허용

규칙 추가				×
출발지 IP * (ì)	0.0.0/0			
목적지 IP *	192.168.150.27			
프로토콜	ТСР	UDP	ICMP	ALL
허용포트 * 🛈	HTTP	∨ 80		추가
	ТСР	80		
	UDP			
	ICMP			
동작	Allow	Deny]	
방향	Inbound	Outbound	In-Out]
규칙 위치	선택해주세요.	∨ 최초 입력		~
설명	100자 이내로 입력하세	요.		
				0/100
			[취소 확인

[VPC F/W 정책 설정 Tip]

- SCP 의 보안 정책은 Deny All 이 기본입니다. 정책 간 우선 순위가 적용되니 순서를 잘 정하여 In/Outbound 설정을 하시기 바랍니다.
- 실제 환경에서 정책 설정을 계획할 때에는 정책 우선순위와 IP 입력 방식(다수 IP 입력, 대역입력, 범위 입력) 최적화 등을 통해 설정 정책의 수를 줄일 수 있습니다.
- 외부-내부 서브넷 대역 간 정책을 설정하는 경우 내부 대역 부분에는 NAT IP 대역이 아닌 내부 IP 대역으로 설정하셔야 합니다.
- '신청 중인 정책이 있습니다.' 라는 메세지가 나오는 경우 잠시 대기 후 앞서 신청한 정책 반영 확인 후 진행이 가능합니다.

- 잘못 반영한 정책의 경우 'Firewall 상세' 화면에서 목록을 선택하신 후 하단의 수정버튼을 클릭하시면 수정이 가능합니다.

[VPC 방화벽 적용 범위]

Firewall 은 VPC 내부와 외부 간의 경계 방화벽 역할을 하며 VPC 내 서브넷 또는 VM 간의 통신은 제어를 할 수 없습니다. 해당 부분에 대한 통제는 다음에 나올 Security Group 에서 수행합니다.

[주의사항]

Inbound All Open(Any IP, Any Port) 오픈 정책은 클라우드 자원을 외부의 위협에 그대로 노출시킬 수 있습니다. 가능하면 필요한 IP 와 포트를 특정하여 정책을 설정할 필요가 있습니다. 이는 Outbound 정책도 마찬가지이며, 뒤에 나올 Security Group 또한 마찬가지입니다.

⑥ 적용된 Firewall 적용 정책들을 목록에서 확인할 수 있습니다.

	Firewall 상세 : Fw_IGW_VPCix ·										원관리 > Firewall 상세	ΘĽ
• Activ	/e		연결해제									
상세	정보	규칙	태그	작업이	력							
총 4 🛛 20 개북	찍보기 >	엑셀 다운로드 🛛 규	칙 추가 규칙 일종	1입력 🗌 Inbound	Outbound	In-Out		100자 이	하의 검색어를 입력히	하세요.	Q 상사	네검색
	순서	규칙ID	규칙 Index ①	출발지 IP	목적지 IP	서비스	동작	방향	활성 여부	설명	상태	
	12	FIREWALL_RUL…	48793	192.168.50.0/24	0.0.0/0	TCP 80, 443, 53	Allow	OutBound	활성화	-	Active	- E
	25	FIREWALL_RUL…	48792	192.168.0.0/24	0.0.0/0	TCP 80, 443	Allow	OutBound	활성화	-	Active	- 1
	50	FIREWALL_RUL	48791	내 PC IP	192.168.1	TCP 22, 3389	Allow	Inbound	활성화	-	Active	
	100	FIREWALL_RUL	48788	0.0.0/0	192.168.1	TCP 80	Allow	Inbound	활성화	-	Active	

5. 정리하기

- SCP에 클라우드 자원을 생성하기 위해서는 가상 네트워크 공간인 VPC가 반드시 필요합니다.
- 사용자는 VPC 내에 별도로 분리된 서브넷을 생성하여 클라우드 자원 생성 시 서브넷 대역 내의 IP를 할당합니다.
- 하나의 과제 내에는 <u>5개의 VPC</u>를 생성할 수 있습니다. 전체 시스템이 큰 경우 개별 서브 시스템의 규모와 밀접도를 고려하여 VPC를 적절히 분리할 필요가 있습니다.
- VPC 내/외부 네트워크 트래픽 통제는 Firewall의 정책 설정을 통해서 할 수 있습니다.