

Contents

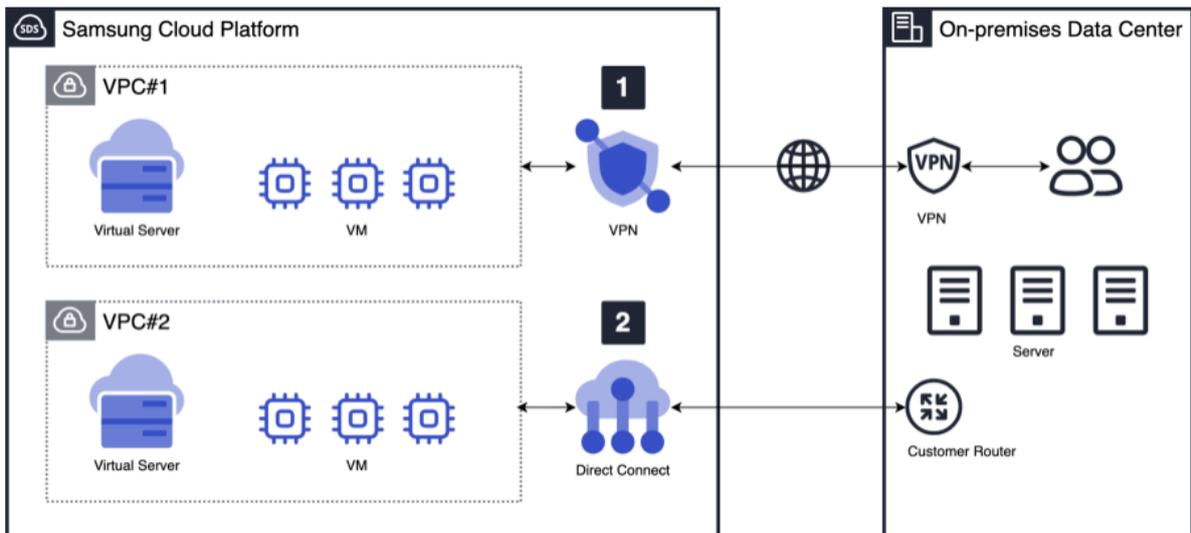
1. 학습목표	1
2. 들어가기	1
3. 사전 요구사항	4
4. 따라하기	5
5. 정리하기	20

1. 학습목표

- VPC(Virtual Private Cloud)의 개념을 이해합니다.
- VPC 생성 후 하나 이상의 서브넷 생성을 통해 네트워크 망을 분리 구성할 수 있습니다
- 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 불가능한 Private 서브넷을 구성할 수 있습니다.

2. 들어가기

2.1 서비스 개념도



2.2 관련 용어

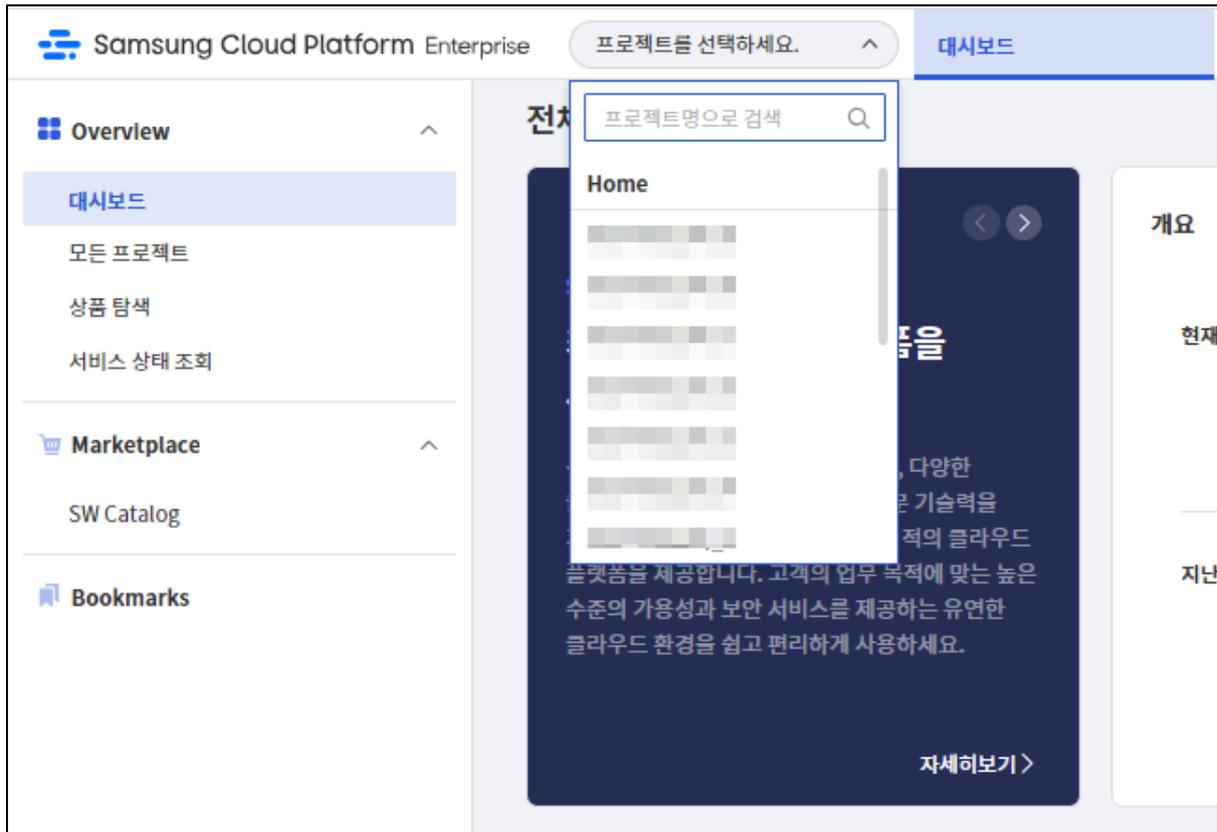
No.	용어	설명
1	VPC (Virtual Private Cloud)	<ul style="list-style-type: none"> -사용자가 정의하는 가상의 네트워크로 클라우드 상에 논리적으로 격리된 네트워크 공간을 할당하여 가상 네트워크에서 SCP 리소스를 이용할 수 있는 서비스 -관리자가 고객사별로 Uplink (외부연결 Network: 그룹망, 인터넷)를 사전에 설정하면 사용자는 해당 Uplink 하위에 VPC 를 생성함. 즉, 접속하는 망 특성에 따라 인터넷과 내부 네트워크에 연결하여 이용할 수 있음 -사용 목적에 따라 여러 개의 VPC 를 생성하여 타 사용자 그룹과 분리하여 독립적으로 운영할 수 있음
2	Subnet	<ul style="list-style-type: none"> -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	<ul style="list-style-type: none"> -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)	<ul style="list-style-type: none"> -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 연결
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

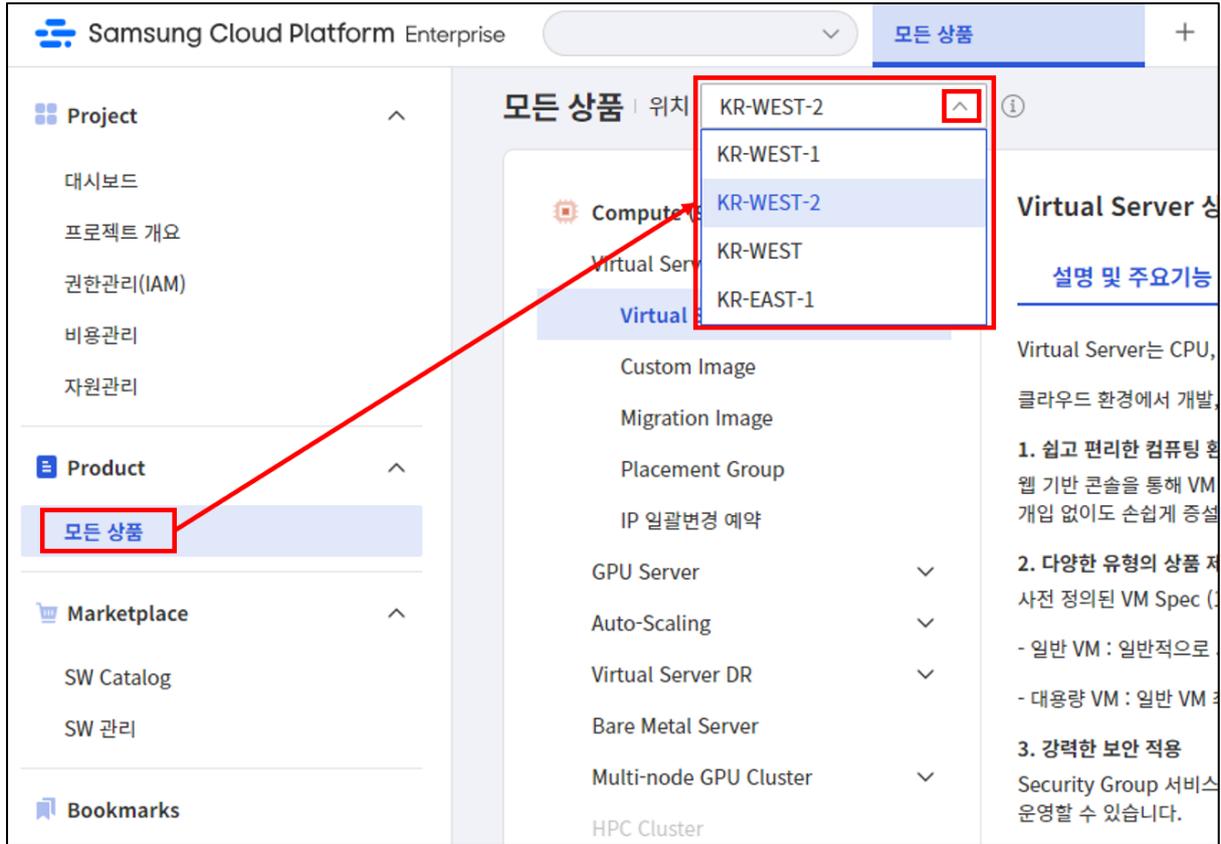
3.1 프로젝트 선택

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



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

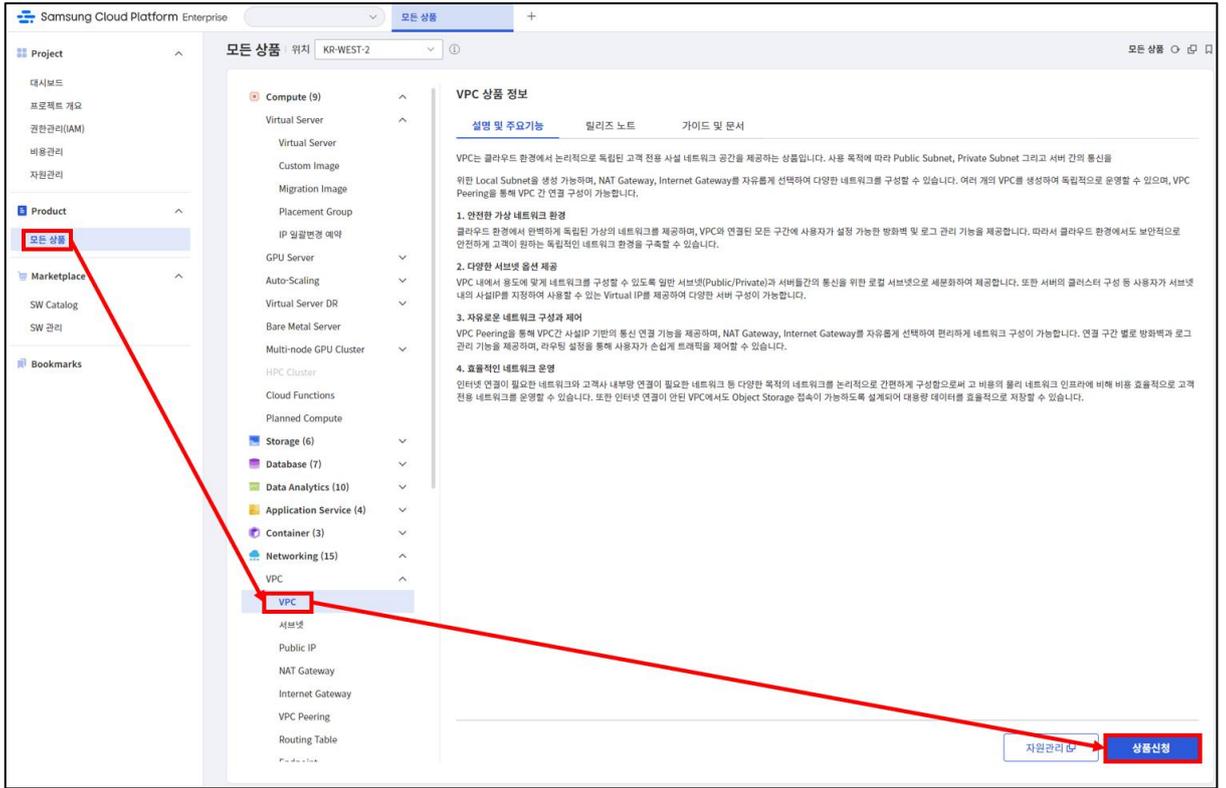


4. 따라하기

4.1 VPC 상품 신청하기

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

※ 프로젝트 하나당 생성 가능한 VPC 의 개수는 최대 5 개입니다.



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 | 모든상품 > VPC - VPC 신청

필수 정보 입력 필수 정보 입력 ... 신청 정보 확인

VPC명 * 중복체크

설명

DNS Service IP ①

VPC 생성 후, 원하는 IP대역을 인터넷 통신을 원하는 경우, IP 신규 생성/적용

추가 정보 입력 태그 추가

태그 추가 ✕

선택한 자원에 태그를 추가/수정/삭제 할 수 있습니다. 자원이 최대 50개까지 태그 등록이 가능합니다. 신규태그 추가는 상품신청 완료 후 적용됩니다.

기존 태그 선택

신규 생성/적용 총 0 생성

Key *	Value
 관련 정보가 없습니다.	

취소 확인

신규 생성/적용 총 0 생성

Key *	Value
SCP	Userxx 적용 ✕

태그 추가

선택한 자원에 태그를 추가/수정/삭제 할 수 있습니다. 자원마다 최대 50개까지 태그 등록이 가능합니다. 신규태그 추가는 상품신청 완료 후 적용됩니다.

기존 태그 선택 SCP:Userxx X

1/50

신규 생성/적용 총 1 생성

Key *	Value
SCP	Userxx X

취소 확인

< VPC - VPC 신청 | 위치 KR-EAST-1 | 모른상품 > VPC - VPC 신청

필수 정보 입력 필수 정보 입력 신청 정보 확인

VPC명 * VPCxx 중복체크
사용 가능한 이름입니다. 5/17

설명 50자 이내로 입력하세요. 0/50

DNS Service IP ① 192.168.254.254

VPC 생성 후, 원하는 IP대역을 입력하여 서브넷을 생성하시기 바랍니다.
 인터넷 통신을 원하는 경우, Internet Gateway를 생성하여 VPC와 연결할 수 있습니다.

추가 정보 입력

태그 1 ① 태그 추가 SCP:Userxx X
 ① 신규태그 추가는 상품신청 완료 후 적용됩니다.

예상 금액
 신청한 상품 총 1개

VPC ₩ 0
운영 중, 자원/서비스 추가 비용은 별도 청구됩니다.

총 예상 금액(1개월)
₩ 0

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.

④ 상품신청 팝업화면에서 확인 버튼을 클릭하여 VPC 상품신청을 완료합니다.

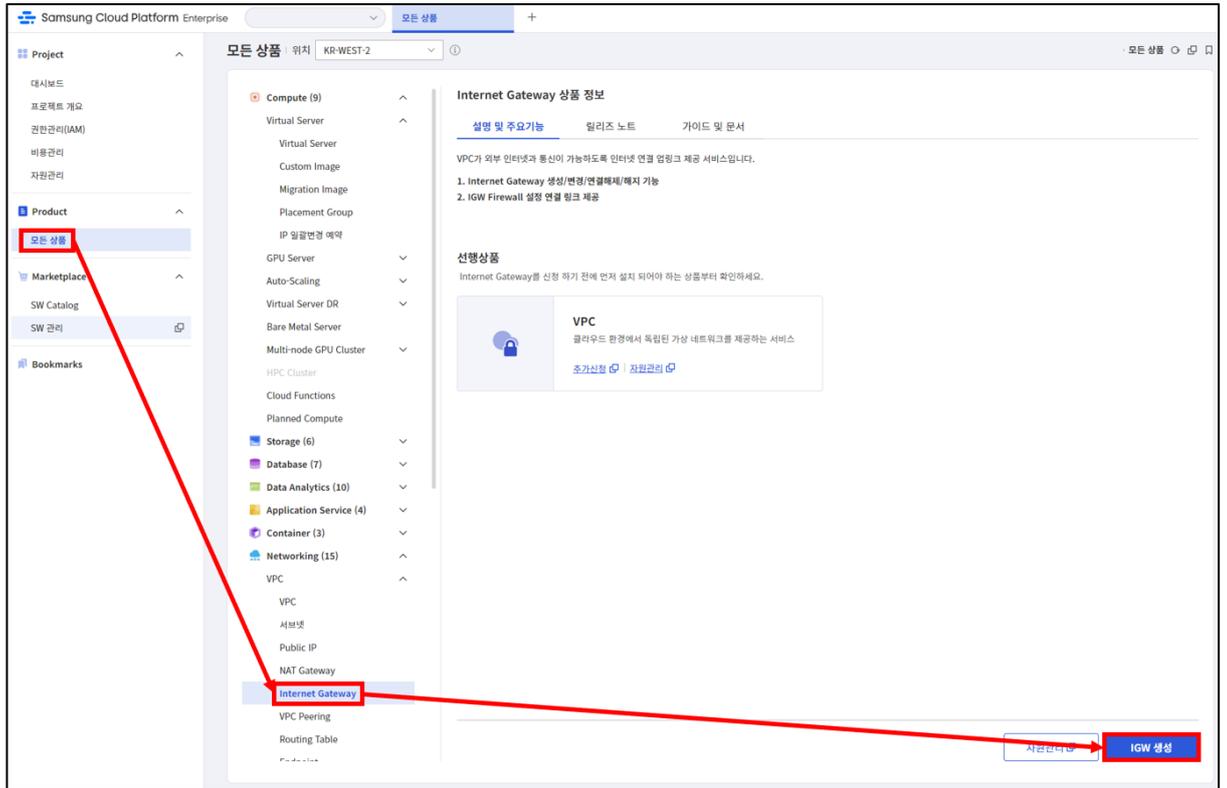
⑤ 생성된 VPC 를 확인합니다.

VPC명	VPC ID	IGW 연결	생성일시	위치	상태	상품해지
VPCxx		미사용			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' 버튼을 클릭합니다.



- 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.

필수 정보 입력

VPC * VPCcxx

구분 * Internet Gateway

Internet Gateway명 IGW_VPCcxx

설명 50자 이내로 입력하세요. 0/50

Default 라우팅이 지정되지 않은 VPC만 Internet Gateway 신청이 가능합니다.

Firewall 사용 사용

Firewall 로깅 여부 사용

로그 저장소 사용하는 경우 로그 저장소를 먼저 설정해야 합니다.
로그 저장소를 설정하면, 로그 저장에 대한 Object Storage 요금이 과금됩니다.
NAT 로깅을 위해서는 [VPC>Internet Gateway상세]에서 NAT 로깅 설정을 해야 합니다.
[로그 저장소 설정 바로가기](#)

100자 이하의 검색어를 입력하세요. 🔍

+ 신규 생성/적용

SCP:Usercxx

태그 1 태그 추가 SCP:Usercxx ×

● 신규태그 추가는 상품신청 완료 후 적용됩니다.

다음

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

신청 정보 확인

신청한 상품 총 1개

예상 청구 금액(월 기준) | 약 ₩ 0

Internet Gateway	VPC명	예상 금액
Internet Gateway명 IGW_VPCcxx	VPC명 VPCcxx	₩ 0

이전 완료

④ 상품신청 팝업화면에서 확인 버튼을 클릭하여 Internet Gateway 상품신청을 완료합니다.



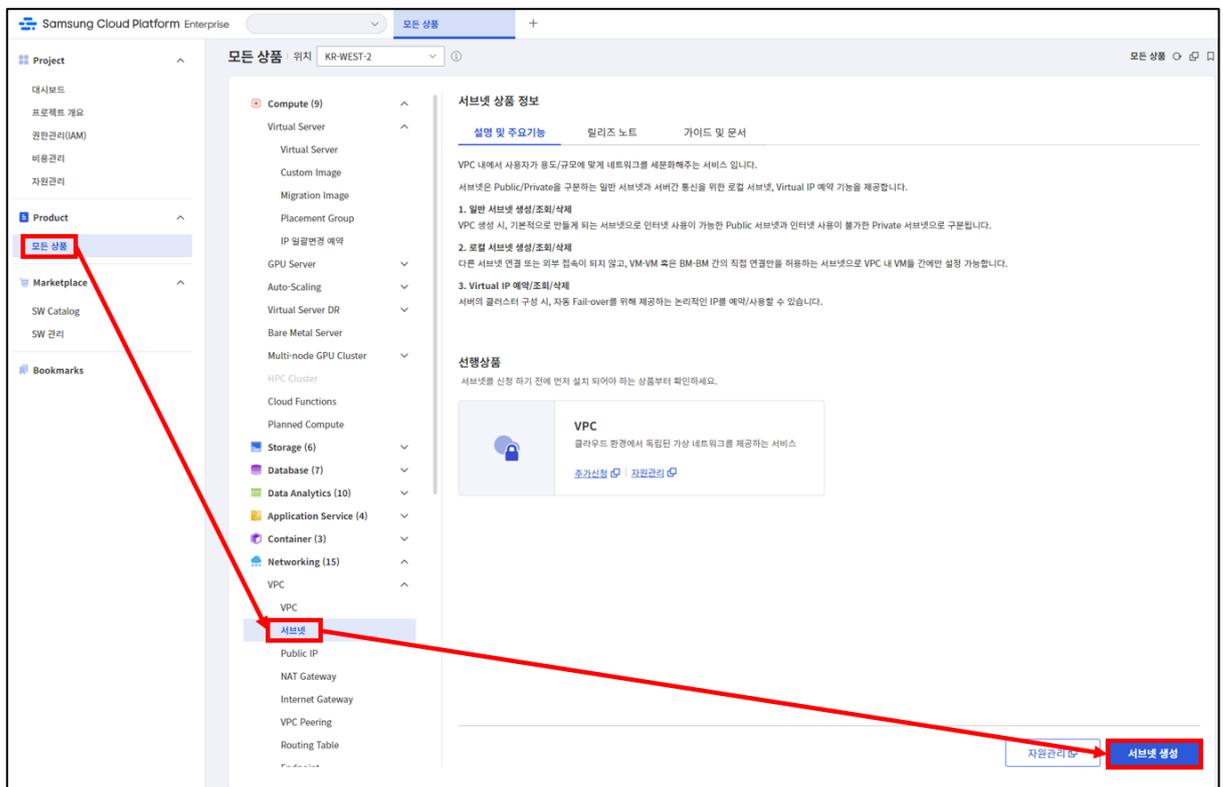
⑤ 생성된 Internet Gateway 를 확인합니다.



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 (IaaS/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.

< VPC - 서브넷 생성 | 위치: KR-EAST-1 | 모든상품 > VPC - 서브넷 생성

필수 정보 입력 필수 정보 입력 ... 신청 정보 확인

VPC * VPCxx

사용 용도 * 일반 로컬

Public Private

서브넷명 * PUBSUbxx 중복체크

IP 대역 * 192.168.0.0/24 중복체크

Gateway 192.168.0.1

설명 50자 이내로 입력하세요.

100자 이하의 검색어를 입력하세요.

추가 정보 입력 + 신규 생성/적용

SCP:Userxxx

태그 1 SCP:Userxxx

신규태그 추가는 상품신청 완료 후 적용됩니다.

예상 금액
신청된 상품 총 1개

서브넷 ₩ 0

총 예상 금액(1개월)
₩ 0

< VPC - 서브넷 생성 | 위치: KR-EAST-1 | 모든상품 > VPC - 서브넷 생성

신청 정보 확인 필수 정보 입력 ... 신청 정보 확인

신청된 상품 총 1개

예상 청구 금액(월 기준) | 약 ₩ 0

서브넷 ₩ 0

서브넷명	PUBSUbxx	VPC명	VPCxx
------	----------	------	-------

예상 금액 ₩ 0

④ 상품신청 팝업화면에서 확인 버튼을 클릭하여 서브넷 상품신청을 완료합니다.



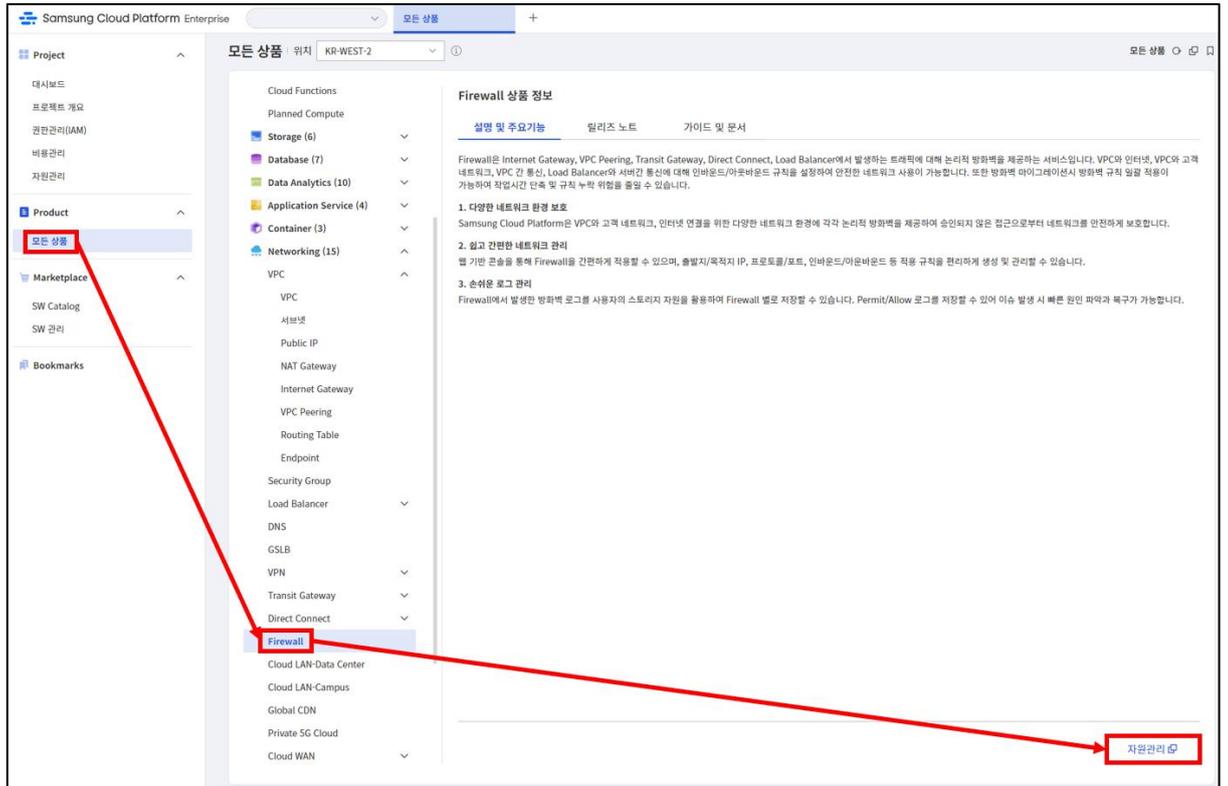
- ⑤ 하나의 서브넷을 생성했으면 아래의 서브넷 자원관리 화면에서 [서브넷 생성]을 클릭해서 다른 서브넷을 만듭니다.
상태가 'Creating'이더라도 상관없이 진행할 수 있습니다.
- ⑥ 모든 서브넷을 생성했으면 서브넷이 모두 맞게 생성되었는지 확인합니다. 특히 VPC 와 CIDR 이 제대로 입력되었는지 다시 한번 확인해봅시다.

서브넷								
총 3 20 개씩 보기 ▾		All My		100자 이하의 검색어를 입력하세요. 🔍			상세검색	서브넷 생성
서브넷명	서브넷 ID	VPC명	IP 대역	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 VPC의 방화벽 기능을 사용하기 위하여 모든 상품 → Networking → Firewall 화면으로 들어갑니다. 앞서 IGW 생성시, Firewall 사용에 체크하였다면, Firewall

이 생성되어 있습니다. (자원관리 탭에서 확인)



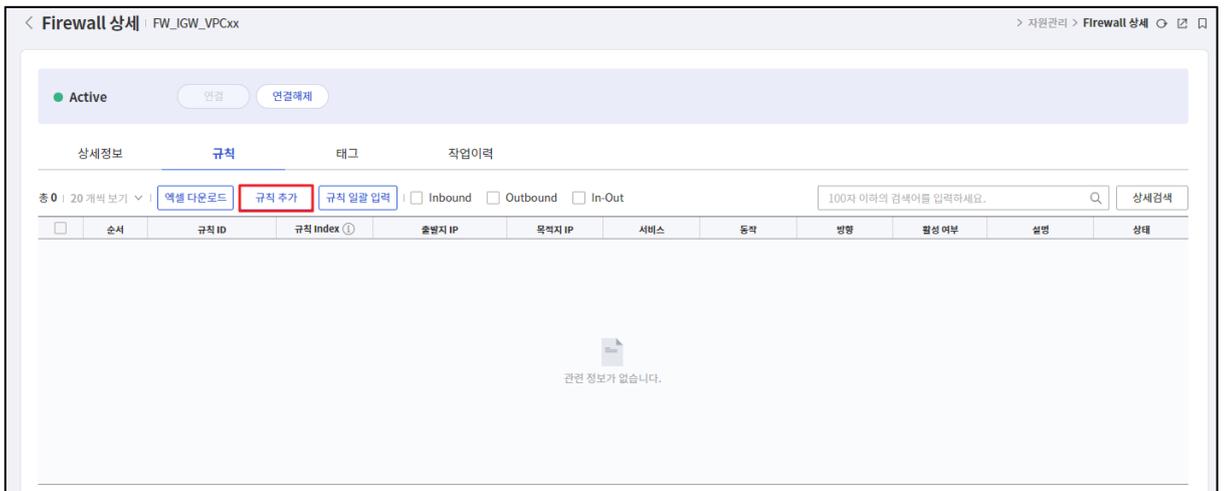
- ② 앞 단계에서 생성한 VPC - Internet Gateway의 Firewall 상태가 'Active'인 것을 확인합니다. 목록에서 해당 Firewall을 클릭하여 Firewall 상세 화면으로 진입합니다. (Firewall 명칭 제일 뒷부분의 본인이 생성한 VPC 명을 확인합니다. 예) FW_IGW_VPCxx)

Firewall명	Firewall 구분	VPC 명	연결명	Firewall 규칙 수	로그 여부	위치	상태
FW_IGW_VPCxx	Internet Gateway	VPCxx	IGW_VPCxx	0	미사용	KR-EAST-1	Active

③ Firewall 상세 화면에서 '규칙' 탭으로 이동합니다.



④ '규칙추가' 버튼을 클릭합니다.



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	프로토콜	동작	방향	용도
0.0.0.0/0 (인터넷)	192.168.zz.0/27 (LB서비스 IP 대역)	HTTP (80)	TCP	Allow	Inbound	인터넷에서 Load Balancer의 IP대역으로 오는 웹서비스 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 오는 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 인터넷으로 가는 시스템 업데이트, 웹서비스 응답용 아웃바운드 트래픽 허용
192.168.yy.0/24 (PRISUB IP대역)	0.0.0.0/0 (인터넷)	HTTP (80) HTTPS(443)	TCP	Allow	Outbound	Private Subnet에서 인터넷으로 가는 시스템 업데이트, 웹서비스 응답용 아웃바운드 트래픽 허용

규칙 추가 ✕

출발지 IP * ⓘ

목적지 IP * ⓘ

프로토콜 TCP UDP ICMP ALL

허용 포트 * ⓘ HTTP 80 추가

TCP

UDP

ICMP

동작 Allow Deny

방향 Inbound Outbound In-Out

규칙 위치 선택해주세요. 최초 입력

설명

0/100

취소
확인

[VPC F/W 정책 설정 Tip]

- SCP의 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 메시지가 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]

Firewall은 VPC 내부와 외부 간의 경계 방화벽 역할을 하며 VPC 내 서버넷 또는 VM 간의 통신은 제어를 할 수 없습니다.

해당 부분에 대한 통제는 다음에 나올 Security Group에서 수행합니다.

[주의사항]

Inbound All Open(Any IP, Any Port) 오픈 정책은 클라우드 자원을 외부의 위협에 그대로 노출시킬 수 있습니다. 가능하면 필요한 IP와 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.

순서	규칙 ID	규칙 Index	출발지 IP	목적지 IP	서비스	동작	방향	활성 여부	설명	상태
12	FIREWALL_RUL...	48793	192.168.50.0/24	0.0.0.0/0	TCP 80, 443, 53	Allow	OutBound	활성화	-	Active
25	FIREWALL_RUL...	48792	192.168.0.0/24	0.0.0.0/0	TCP 80, 443	Allow	OutBound	활성화	-	Active
50	FIREWALL_RUL...	48791	내 PC IP	192.168.1...	TCP 22, 3389	Allow	Inbound	활성화	-	Active
100	FIREWALL_RUL...	48788	0.0.0.0/0	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 서버넷을 생성하여 클라우드 자원 생성 시 서버넷 대역 내의 IP를 할당합니다.
- 하나의 과제 내에는 5개의 VPC를 생성할 수 있습니다. 전체 시스템이 큰 경우 개별 서버 시스템의 규모와 밀접도를 고려하여 VPC를 적절히 분리할 필요가 있습니다.
- VPC 내/외부 네트워크 트래픽 통제는 Firewall의 정책 설정을 통해서 할 수 있습니다.