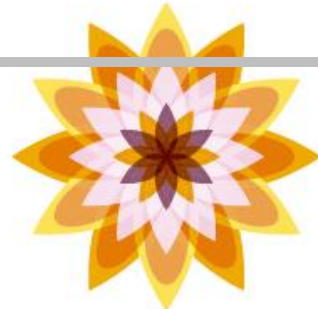
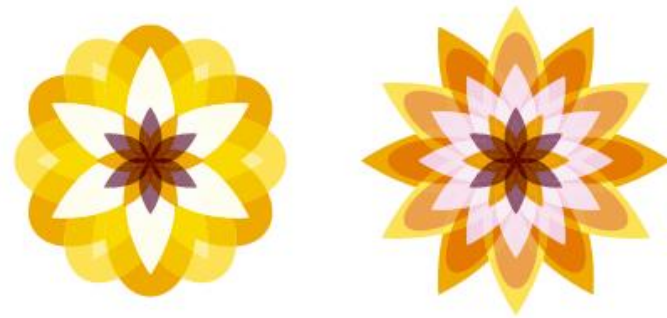


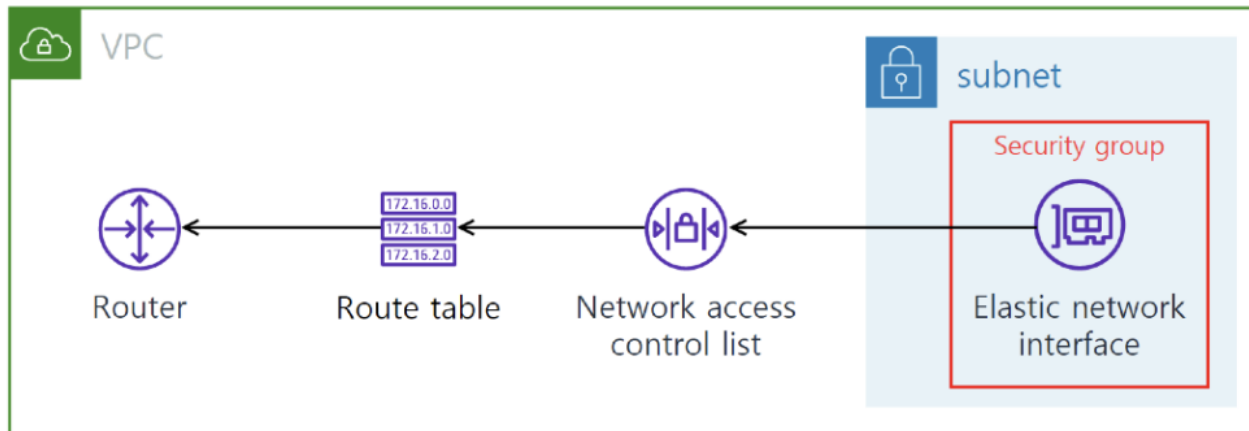
Chapter 04

나만의 가상 네트워크 공간 만들기



■ VPC와 VPC 네트워킹

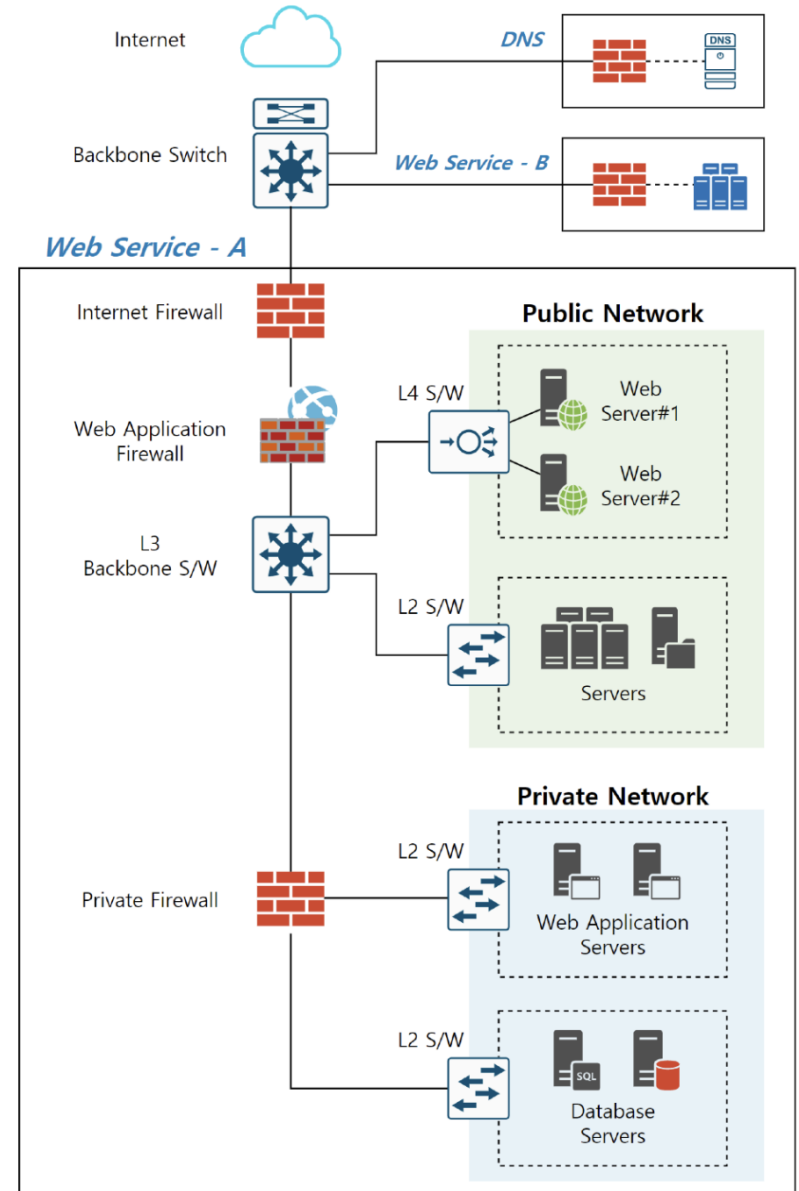
- VPC 네트워킹은 VPC 환경을 사용하는 리소스가 통신할 수 있도록 네트워크 구성을 설정하는 행위, 또는 그 네트워크 구성 자체를 뜻한다.
- AWS 서비스가 네트워크 인터페이스를 사용하면 자동으로 보안 그룹, 네트워크 ACL 그리고 라우팅 테이블의 통제를 받게 된다.
- 이를 두고 서비스가 VPC 네트워킹을 사용한다고 말한다.



1. VPC

■ VPC와 온프레미스의 비교

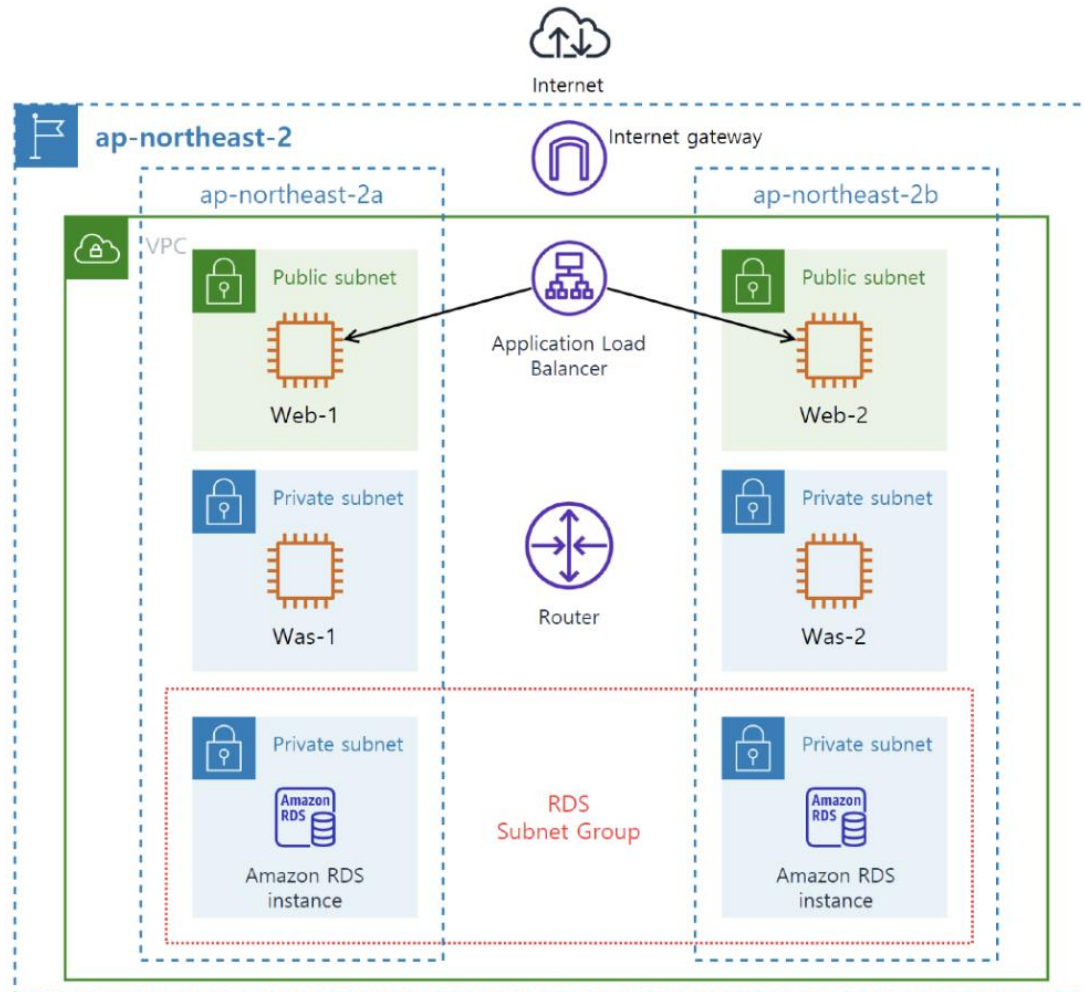
- 온프레미스 환경은 VPC와 어떤 차이가 있을까?
- 그림은 웹 서비스를 제공하는 온프레미스의 네트워크 구성이다.



1. VPC

■ VPC와 온프레미스의 비교

- 온프레미스 네트워크를 VPC로 옮겨보자.



■ VPC와 온프레미스의 비교

- 이처럼 소규모 네트워크를 VPC에서는 서브넷으로 매핑할 수 있다.
- 그리고 L4 스위치는 로드밸런서가, 방화벽은 VPC의 보안 그룹과 네트워크 ACL이 그 역할을 대신하고 있다.
- L3 백본 스위치는 라우터가 담당하지만 AWS 라우터 생성 없이 가상의 라우팅 테이블만으로 트래픽 경로 제어가 가능하다.
- 뿐만 아니라 인터넷 게이트웨이를 라우팅 타겟으로 설정하면 서브넷을 퍼블릭으로 활용할 수도 있다.

1. VPC

■ CIDR 블록

- VPC 네트워크 규모는 CIDR(Classless Inter-Domain Routing)이 결정한다.
- 그림은 기존 클래스 방식과 CIDR의 비교 자료다.

방식	클래스	네트워크 주소	호스트 IP 범위	호스트 IP 개수
Class	A	92.0.0.0/ 8	92.0.0.0 ~ 92.255.255.255	$2^{24} - 2 = 16,777,214$
	B	92.75.0.0/ 16	92.75.0.0 ~ 92.75.255.255	$2^{16} - 2 = 65,534$
	C	92.75.162.0/ 24	92.75.162.0 ~ 92.75.162.255	$2^8 - 2 = 254$



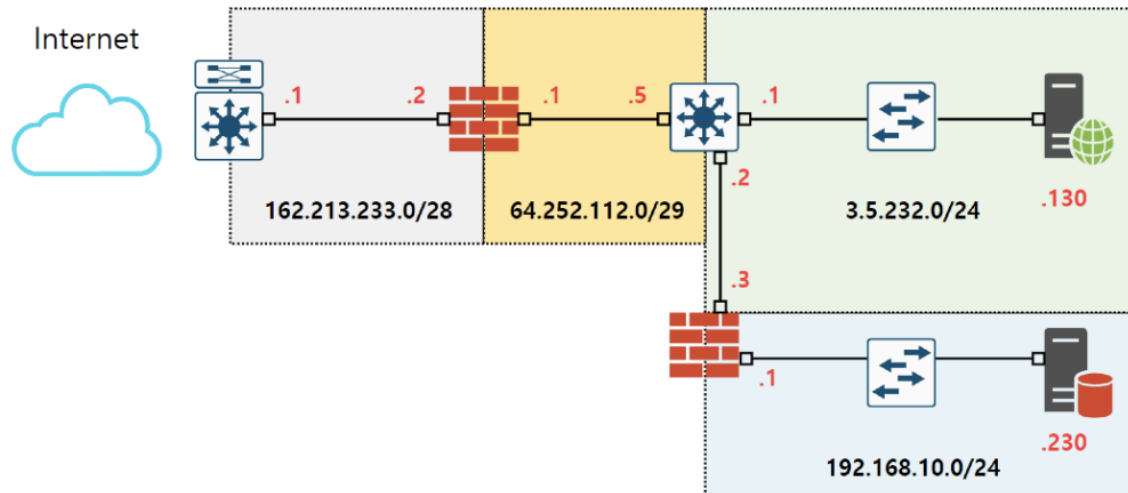
방식	mask	네트워크 주소	호스트 IP 범위	호스트 IP 개수
CIDR	20 bits	92.75.0.0/ 20	92.75.0.0 ~ 92.75.15.255 (92.75.00000000.0) ~ (92.75.00001111.255)	$2^{12} - 2 = 4,094$

- AWS에서는 VPC의 CIDR 블록 범위를 16 ~ 28 사이로 제한하고 있다.
- 그러므로 14 ~ 65,534 범위 IP를 사용할 수 있다.
- 참고 사항으로 VPC의 CIDR을 서브넷 CIDR로 나눠 사용하면 각 서브넷 CIDR 블록(예. 10.0.0.0/24)의 첫 4개 IP 주소(예. 10.0.0.0 ~ 10.0.0.3)와 마지막 IP 주소(예. 10.0.0.255)는 AWS에서 예약한 주소이므로 사용할 수 없다.

1. VPC

■ 퍼블릭 CIDR 전략

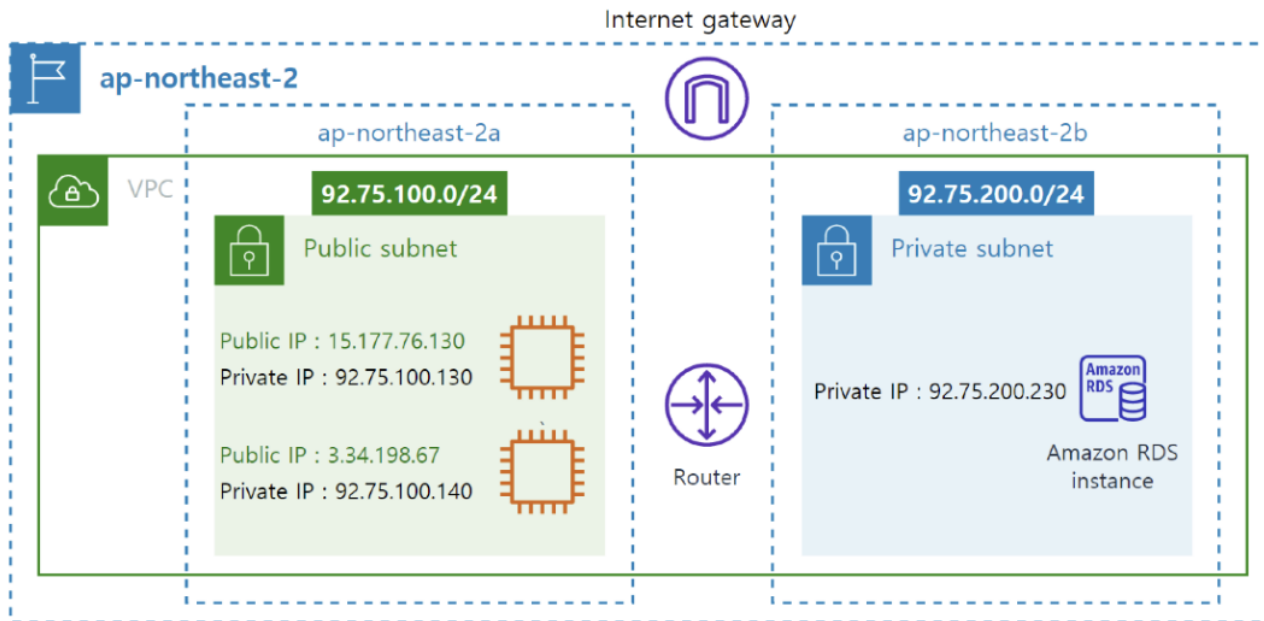
- VPC 환경은 IP 절약 측면에서도 장점이 있다.
- 온프레미스는 일반적으로 퍼블릭 서버에 퍼블릭 IP를 할당하고, 프라이빗 서버는 프라이빗 IP를 할당한다.
- 프라이빗 IP는 인터넷이 불가능한 내부 영역에 해당하므로 원하는 네트워크를 마음대로 정의해서 사용할 수 있지만 퍼블릭 IP는 ISP에서 부여한 IP만 사용할 수 있으며 별도 비용이 발생하므로, 회사에서 선점한 퍼블릭 CIDR은 비용 절감을 고려해 여러 서브넷으로 나눠 사용한다.



1. VPC

■ 퍼블릭 CIDR 전략

- 그럼 VPC는 어떠한가?
- 그림은 퍼블릭 IP가 할당된 인스턴스 2개를 보여준다.
- AWS의 모든 인스턴스는 생성 시점에 프라이빗 IP가 자동 할당된다.
- 인터넷 접속을 위해 퍼블릭 IP를 설정해야 한다면 인스턴스 생성 시점에 퍼블릭 IP를 할당하거나 생성 이후에 탄력적 IP를 할당하는 방법이 있다.



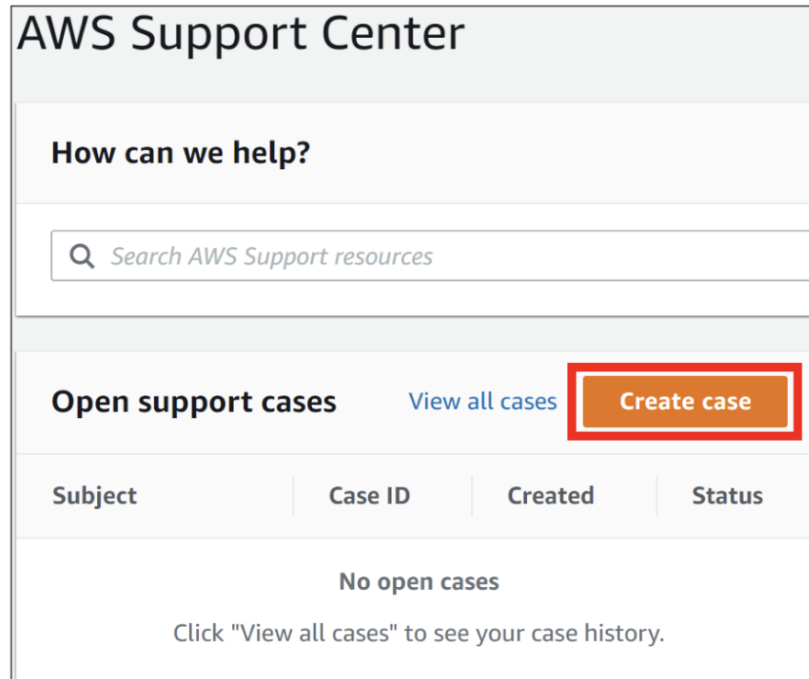
■ 퍼블릭 CIDR 전략

- 온프레미스가 서브넷의 CIDR 일부를 퍼블릭 IP로 사용한 것과는 달리 AWS는 프라이빗 CIDR과는 무관하게 인스턴스가 필요할 때만 퍼블릭 IP를 할당할 수 있다.
- VPC는 퍼블릭 CIDR에 구속받지 않으므로 퍼블릭 IP 연결과 해제가 보다 자유롭다.
- 또 VPC는 온프레미스의 백본과 방화벽, 그리고 스위치 등 네트워크 장비 일체가 필요 없다.

1. VPC

■ VPC 네트워킹 리소스 할당량 조정

- VPC는 리전마다 생성할 수 있는 최대 한도가 정해져 있다.
- 이를 할당량(Quotas)이라 한다.
- AWS는 용량 관리 목적으로 VPC 리소스를 제한하고 있으나 별도 요청해 증설할 수 있다.
- 다음 순서에 따라 진행한다.
 - AWS 지원 센터에 접속해 Create case(사례 생성) 버튼을 클릭한다.



The screenshot shows the AWS Support Center interface. At the top, it says "AWS Support Center". Below that, there's a section "How can we help?" with a search bar containing the text "Search AWS Support resources". Underneath the search bar, there's a section "Open support cases" with a link "View all cases" and a button "Create case" which is highlighted with a red box. Below this, there's a table with headers "Subject", "Case ID", "Created", and "Status". The table is currently empty, and below it, it says "No open cases" and "Click 'View all cases' to see your case history."

Subject	Case ID	Created	Status
No open cases			
Click "View all cases" to see your case history.			

1. VPC

■ VPC 네트워킹 리소스 할당량 조정

■ 다음 순서에 따라 진행한다.

- 3가지 옵션 중 Service limit increase(서비스 한도 증가) 버튼을 선택한다.
- Limit type은 VPC, Severity는 General question을 선택한다.

The screenshot shows the 'Create case' interface in the AWS console. At the top, there are three radio button options: 'Account and billing support', 'Service limit increase', and 'Technical support'. The 'Service limit increase' option is selected and highlighted with a red box. Below these options is the 'Case details' section. It contains two dropdown menus: 'Limit type' with 'VPC' selected, and 'Severity' with 'General question' selected. Both dropdowns are also highlighted with red boxes. To the right of the dropdowns is an 'Announcement' box with a title 'Service Quota increases are moving to the new Service Quotas dashboard.' and a button labeled 'Service Quotas dashboard' with an external link icon.

Create case [Info](#)

Account and billing support ☐
Assistance with account and billing-related inquiries

Service limit increase ☒
Requests to increase the service limit of your AWS resources

Technical support ☐
Service-related technical issues and third-party applications

Case details

Limit type
VPC ▼

Severity [Info](#)
General question ▼

Announcement
Service Quota increases are moving to the new Service Quotas dashboard.
You can use the Service Quotas dashboard to view and manage your quotas for AWS services from a central location. Not all services are supported at this time. [Learn more.](#)
[Service Quotas dashboard](#) ↗

1. VPC

■ VPC 네트워킹 리소스 할당량 조정

- 다음 순서에 따라 진행한다.
 - 화면 아래로 스크롤하면 Request(요청) 선택 화면이 나타난다.
 - 리전과 요청할 한도 타입을 선택하고, 한도 개수를 입력한다.

Request 1

Region

Asia Pacific (Seoul) ▼

Limit

VPCs per Region ▼

New limit value

10

1. VPC

■ VPC 네트워킹 리소스 할당량 조정

■ 다음 순서에 따라 진행한다.

- Use case description에 할당량 증가 요청 사유를 입력하고 그림처럼 언어, 연락 수단, 이메일을 차례로 입력한다.
- 완료하면 Submit을 클릭한다.

▼ Contact options

Preferred contact language

English ▼

Contact methods [Info](#)

Web

Via email and Support Center
We will get back to you within
24 hours

Chat

Chat online with a
representative

Phone

We call you back at your
number

Additional contacts - optional [Info](#)

When we contact you via email, we will copy the correspondence to the following email addresses

5styl3mov@gmail.com

Use commas or semicolons to separate email addresses - Maximum 10 email addresses (9 remaining) or 200 characters (182 remaining)

Cancel

Submit

1. VPC

■ VPC 네트워킹 리소스 할당량 조정

- 다음 순서에 따라 진행한다.
 - 생성한 사례는 Case History에서 다시 확인할 수 있다.

Case history Info					Create case
<input type="text" value="Filter cases by subject, severity, type or status"/>		View cases created in:		< 1 > ⚙	
		English ▼			
Created ▼	Subject ▼	Severity ▼	Case ID ▼	Case Type ▼	
May 30, 2021, 04:53 AM	Limit Increase: VPC	General question	8402703981	Service limits	

■ VPC 네트워킹 리소스 할당량 조정

■ 다음 순서에 따라 진행한다.

- 요청 종류에 따라 소요되는 시간이 달라진다.
- 특별한 검토가 필요 없으면 10분 이내 다음과 같은 완료 메일을 받을 수 있다.

Hello,

We have approved and processed your limit increase request(s). It can sometimes take up to 30 minutes for this to propagate and become available for use. I hope this helps, but please reopen this case if you encounter any issues.


Summary of limit(s) requested for increase:

[AP_NORTHEAST_2]: VPC / VPCs per Region, New Limit = 10

1. VPC

■ 기본 VPC란?

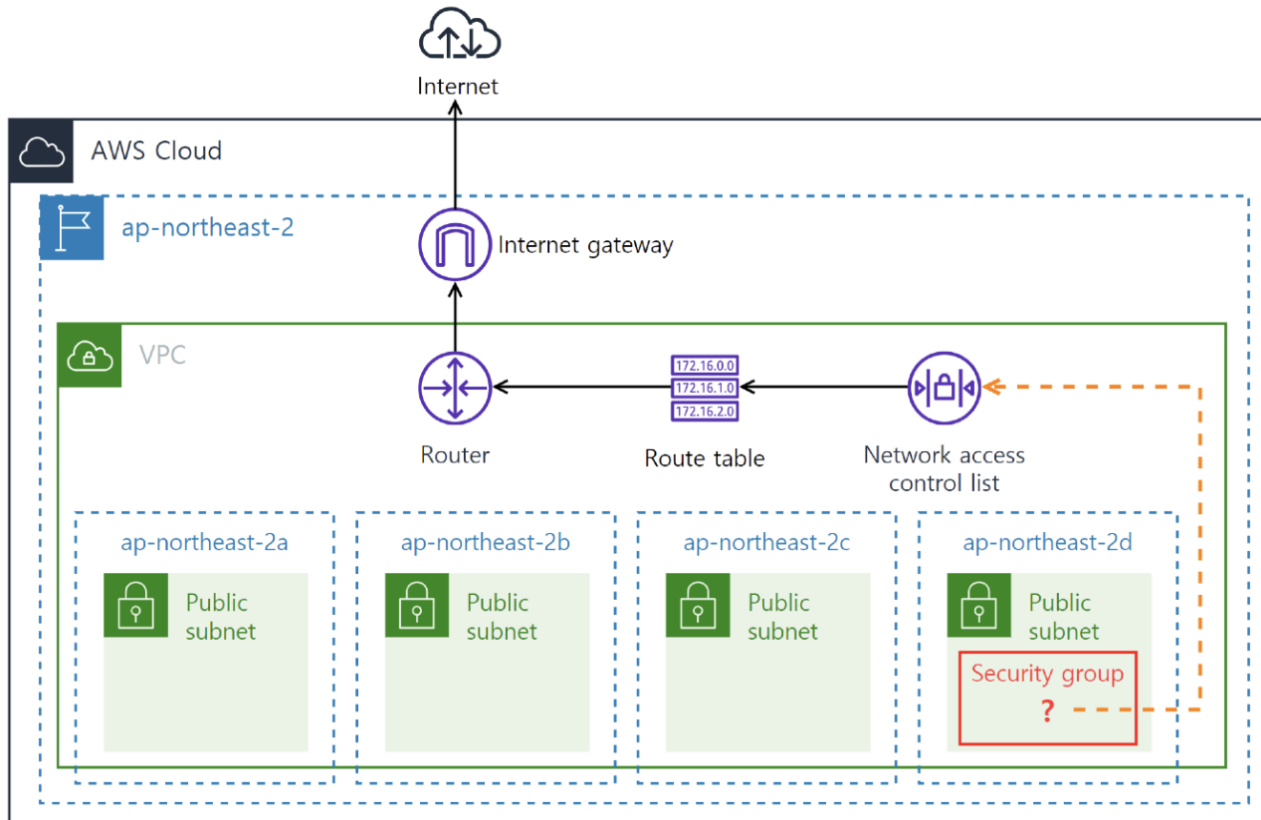
- 그림은 서울 리전의 VPC 대시보드 화면이다.
- 계정을 생성한 후 별도 작업을 하지 않았다면 이 화면을 볼 수 있다.
- VPC 네트워킹을 구성하는 리소스 이름과 개수가 이 곳에 표시된다.

리전별 리소스  리소스 새로 고침	
다음 Amazon VPC 리소스를 사용하고 있습니다.	
VPC 모든 리전 보기 ▼	서울 1
NAT 게이트웨이 모든 리전 보기 ▼	서울 0
서브넷 모든 리전 보기 ▼	서울 4
VPC 피어링 연결 모든 리전 보기 ▼	서울 0
라우팅 테이블 모든 리전 보기 ▼	서울 1
네트워크 ACL 모든 리전 보기 ▼	서울 1
인터넷 게이트웨이 모든 리전 보기 ▼	서울 1
보안 그룹 모든 리전 보기 ▼	서울 1
외부 전용 인터넷 게이트웨이 모든 리전 보기 ▼	서울 0
고객 게이트웨이 모든 리전 보기 ▼	서울 0

1. VPC

■ 기본 VPC란?

- 다음은 이 VPC 대시보드 현황을 토폴로지로 표현한 그림이다.
- 그림에서 생성된 기본 VPC 1개, 가용 영역마다 생성된 퍼블릭 서브넷 4개, 그리고 VPC 통제 3요소(보안 그룹, 네트워크 ACL, 라우팅 테이블)를 볼 수 있다.



■ 기본 VPC란?

- 이처럼 AWS는 고객이 네트워크 인터페이스만 갖추면 서비스를 즉각 개시할 수 있도록, VPC 환경을 미리 마련해 뒀다.
- 이를 기본 VPC(Default VPC)라 한다.
- 앞의 그림에서 가용 영역 서브넷에 인스턴스 레벨의 서비스를 생성하면 네트워크 인터페이스가 자동으로 생성된다.
- 그 네트워크 인터페이스에 보안 그룹을 연결하고 원하는 환경에 맞게 네트워크 ACL과 라우팅 테이블을 설정하면 통신이 시작될 것이다.
- 또한 인터넷 게이트웨이는 VPC 네트워킹의 필수 요소가 아니지만 인스턴스만 만들면 즉시 인터넷을 사용할 수 있도록 기본 VPC가 준비한 리소스다.
- 물론 라우팅 테이블 타겟에도 인터넷 게이트웨이가 지정돼 있다.
- 기본 VPC와 그 기반 요소들은 우리가 원해서 만든 리소스가 아니다.
- 심지어 모든 리전에 기본 생성돼 있어 비용 납부 의무가 없다.
- 그러나 인터넷 게이트웨이를 지나는 트래픽이 발생한다면 그에 따른 요금은 부과된다.

1. VPC

■ 기본 VPC란?

- 그림은 기본 VPC와 기본 서브넷을 함께 보여준다.
- 기본 VPC 개념과는 별개로 모든 VPC는 자신이 기본으로 사용하는 라우팅 테이블과 네트워크 ACL이 있다.
- 이를 기본 라우팅 테이블, 기본 네트워크 ACL이라 한다.

VPC (1) 정보							작업 ▼	VPC 생성
Q VPC 필터링							< 1 >	⚙
<input type="checkbox"/>	VPC ID ▼	IPv4 CIDR	기본 라우팅 테이블 ▼	기본 네트워크 ACL ▼	기본 VPC			
<input type="checkbox"/>	vpc-1868e173	172.31.0.0/16	rtb-f093c59b	acl-00512b6b	예			

서브넷 (4) 정보								작업 ▼	서브넷 생성
Q 서브넷 필터링								< 1 >	⚙
<input type="checkbox"/>	서브넷 ID ▼	VPC ▼	IPv4 CIDR ▼	가용 영역 ▼	라우팅 테이블 ▼	네트워크 ACL ▼	기본 서브넷		
<input type="checkbox"/>	subnet-ad42ade2	vpc-1868e173	172.31.32.0/20	ap-northeast-2c	rtb-f093c59b	acl-00512b6b	예		
<input type="checkbox"/>	subnet-6e388305	vpc-1868e173	172.31.0.0/20	ap-northeast-2a	rtb-f093c59b	acl-00512b6b	예		
<input type="checkbox"/>	subnet-6983f712	vpc-1868e173	172.31.16.0/20	ap-northeast-2b	rtb-f093c59b	acl-00512b6b	예		
<input type="checkbox"/>	subnet-5122da0e	vpc-1868e173	172.31.48.0/20	ap-northeast-2d	rtb-f093c59b	acl-00512b6b	예		

1. VPC

■ 기본(Default)의 위험성

- 그림은 기본 VPC의 기본 보안 그룹이다.

보안 그룹 (1) 정보		🔄	작업 ▼	보안 그룹 생성
🔍 보안 그룹 필터링		< 1 > ⚙️		
<input type="checkbox"/>	보안 그룹 ID ▼	VPC ID ▼	인바운드 규칙 수 ▼	아웃바운드 규칙 수
<input type="checkbox"/>	sg-44b0b939	vpc-1868e173	1 권한 항목	1 권한 항목

- 보안 그룹 ID를 클릭하면 그림처럼 인바운드와 아웃바운드 규칙이 탭으로 구분돼 있다.

인바운드 규칙 (1)				인바운드 규칙 편집
유형	프로토콜	포트 범위	소스	설명 - 선택 사항
모든 트래픽	전체	전체	sg-44b0b939 / default	-

아웃바운드 규칙 (1)				아웃바운드 규칙 편집
유형	프로토콜	포트 범위	대상	설명 - 선택 사항
모든 트래픽	전체	전체	0.0.0.0/0	-

■ 기본(Default)의 위험성

- 문제는 기본 저장된 규칙이다.
- 그림의 빨강 박스는 VPC가 생성될 때 기본 보안 그룹에 자동 생성된 규칙이다.
- 아웃바운드 기본 규칙은 모든 형태의 트래픽을 어느 곳으로도 전송할 수 있는 막강한 권한이 있다.
- 대부분의 보안 사고나 자료 유출은 이 규칙 때문에 발생한다.
- 악성코드에 감염된 인스턴스는 2차 해킹에 필요한 자료를 모아 C&C 서버로 전송할 수 있다.
- 온프레미스도 예외는 아니다.
- 보안그룹은 수명 주기 동안 네트워크 인터페이스에 다중 연결 가능한 성질이 있다.
- 그러므로 무분별하게 사용하면 콘솔 화면만으로 어느 인스턴스에서 보안 그룹을 사용하는지 일일이 판별하기 어렵다.
- 따라서 불필요 보안 그룹은 주기적으로 점검해 반드시 삭제해야 한다.
- 사용 중인 보안 그룹이라면 필요한 IP와 포트로 제한하는지 검사해야 할 것이다.

■ 기본(Default)의 위험성

- 그림은 기본 보안 그룹 삭제를 시도한 모습이다.
- 그림 기본 보안 그룹은 어떻게 관리해야 할까?
- 사실 보안 그룹의 규칙은 없어도 된다.
- 즉, 보안 그룹 내부 규칙을 삭제하는 방식으로 관리한다.
- 보안 강화 측면에서 기본 VPC는 삭제하고 별도의 VPC를 생성한 후 필요한 환경만 만들어 나갈 것을 권장한다.

보안 그룹 (1/1) 정보

작업 ▲ 보안

태그 관리
기한 경과 규칙 관리
새 보안 그룹에 복사
보안 그룹 삭제

<input checked="" type="checkbox"/>	보안 그룹 ID	VPC ID
<input checked="" type="checkbox"/>	sg-44b0b939	vpc-1868e173

1 권한 항목

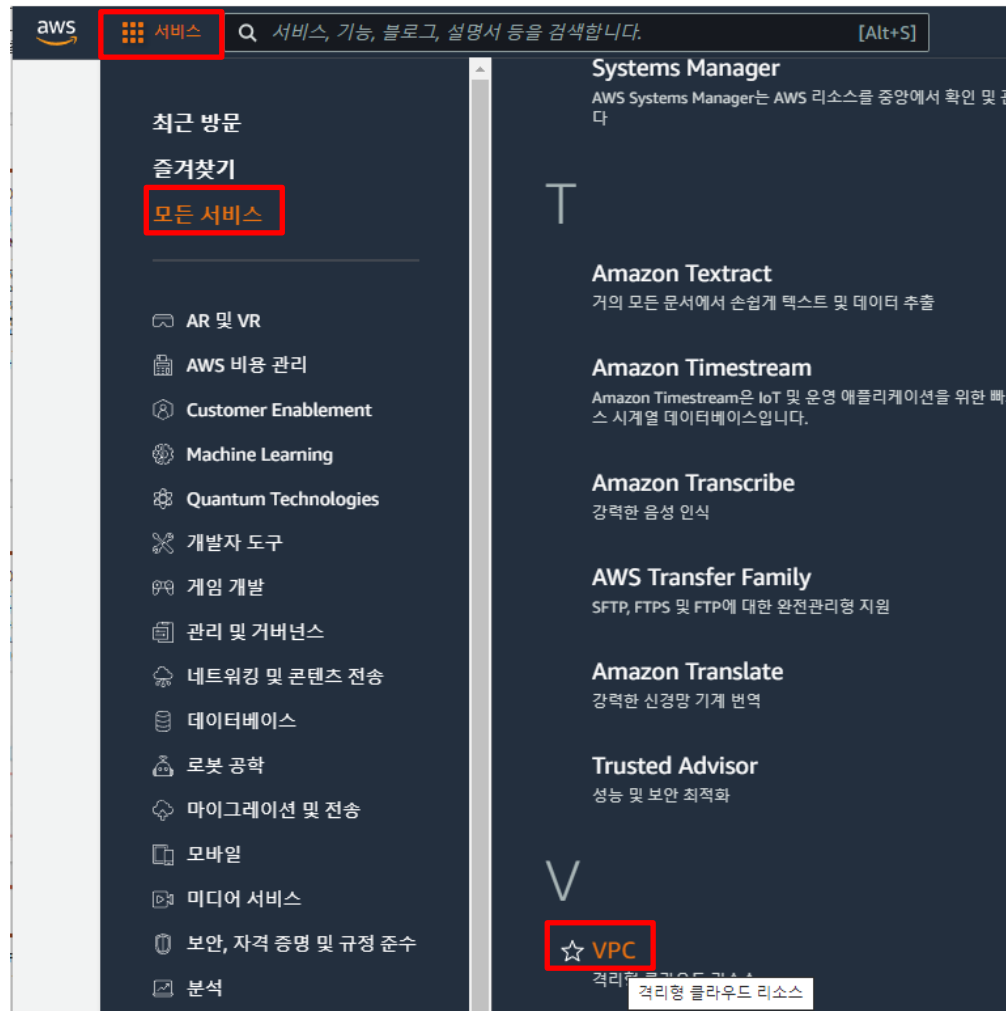
⚠ 일부 보안 그룹은 삭제할 수 없습니다.
다음 보안 그룹은 삭제할 수 없습니다. 이러한 보안 그룹은 기본 보안 그룹이거나 다른 보안 그룹에서 참조하거나, 인스턴스 또는 네트워크 인터페이스와 연결되어 있습니다.

보안 그룹	상태	이유
sg-44b0b939 default	삭제되지 않을 예정	이는 기본 보안 그룹입니다. 기본 보안 그룹은 삭제할 수 없습니다.

1. VPC

■ 실습. 기본 VPC 삭제

■ 서비스 > VPC 선택



1. VPC

■ 실습. 기본 VPC 삭제

■ VPC 선택

VPC 생성

EC2 인스턴스 시작

참고: 인스턴스는 아시아 태평양 리전에서 시작됩니다.

리전별 리소스 [리소스 새로 고침](#)

다음 Amazon VPC 리소스를 사용하고 있습니다.

VPC 모든 리전 보기 ▼	아시아 태평양 1	NAT 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
서브넷 모든 리전 보기 ▼	아시아 태평양 4	VPC 피어링 연결 모든 리전 보기 ▼	아시아 태평양 0
라우팅 테이블 모든 리전 보기 ▼	아시아 태평양 1	네트워크 ACL 모든 리전 보기 ▼	아시아 태평양 1
인터넷 게이트웨이 모든 리전 보기 ▼	아시아 태평양 1	보안 그룹 모든 리전 보기 ▼	아시아 태평양 6
외부 전용 인터넷 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0	고객 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
DHCP 옵션 세트 모든 리전 보기 ▼	아시아 태평양 1	가상 프라이빗 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
탄력적 IP 모든 리전 보기 ▼	아시아 태평양 0	사이트 간 VPN 연결 모든 리전 보기 ▼	아시아 태평양 0
엔드포인트 모든 리전 보기 ▼	아시아 태평양 0	실행 중인 인스턴스 모든 리전 보기 ▼	아시아 태평양 0
엔드포인트 서비스 모든 리전 보기 ▼	아시아 태평양 0		

1. VPC

■ 실습. 기본 VPC 삭제

- 기본 VPC 선택 > 작업 > VPC 삭제

The screenshot shows the AWS Management Console interface for VPCs. The title is 'VPC (1/1) 정보'. Below the title is a search bar labeled 'VPC 필터링'. A table lists the VPCs with columns: Name, VPC ID, 상태 (Status), and IPv4 CIDR. One VPC is listed: '기본 VPC' (Default VPC) with ID 'vpc-8369fae8', status 'Available', and CIDR '172.31.0.0/16'. The '기본 VPC' row is highlighted in blue, and its selection checkbox is checked and highlighted with a red box. To the right of the table, the '작업' (Actions) menu is open, showing a list of actions: '기본 VPC 생성', '플로우 로그 생성', 'CIDR 편집', 'DHCP 옵션 세트 편집', 'DNS 호스트 이름 편집', 'DNS 확인 편집', '미들박스 경로 관리', '태그 관리', and 'VPC 삭제'. The 'VPC 삭제' option is highlighted with a red box.

<input checked="" type="checkbox"/>	Name	VPC ID	상태	IPv4 CIDR
<input checked="" type="checkbox"/>	기본 VPC	vpc-8369fae8	Available	172.31.0.0/16

- 기본 VPC 생성
- 플로우 로그 생성
- CIDR 편집
- DHCP 옵션 세트 편집
- DNS 호스트 이름 편집
- DNS 확인 편집
- 미들박스 경로 관리
- 태그 관리
- VPC 삭제

■ 실습. 기본 VPC 삭제

- VPC 삭제 버튼을 클릭하면 경고 메시지와 함께 의사 재확인 팝업창이 나타난다.
- 가이드에 따라 진행한 후 삭제 버튼을 클릭하면 기본 VPC와 관련된 모든 리소스가 삭제된다.

VPC 삭제

-

vpc-8369fae8

Available

또한 삭제됩니다.

다음 10 리소스도 영구적으로 삭제되며 나중에 복구할 수 없습니다.

이름	리소스 ID	상태
-	igw-d3d791bb	Available
-	sg-0099ca1e30d406e9a	-
-	sg-02192d3459c3c8f2f	-
-	sg-046434a4e2ce20d31	-
-	sg-07b0497fb30e78bb9	-
-	sg-0d1c52860898734cb	-
-	subnet-a6ff3df9	Available
-	subnet-f0a656bf	Available
-	subnet-503cb13b	Available
-	subnet-d8ea94a3	Available

경고: 이 기본 VPC를 삭제하는 경우, 다른 VPC에서 서브넷을 지정하거나 새 기본 VPC를 생성하지 않으면 이 리전에서 인스턴스를 시작할 수 없습니다.

☒ 기본 VPC를 삭제하려고 합니다.

삭제를 확인하려면 필드에 기본 VPC 삭제를 입력하십시오.

기본 VPC 삭제

취소

삭제

■ 실습. 기본 VPC 삭제

- VPC 삭제 버튼을 클릭하면 경고 메시지와 함께 의사 재확인 팝업창이 나타난다.
- 가이드에 따라 진행한 후 삭제 버튼을 클릭하면 기본 VPC와 관련된 모든 리소스가 삭제된다.

VPC 삭제

-

vpc-8369fae8

Available

또한 삭제됩니다.

다음 10 리소스도 영구적으로 삭제되며 나중에 복구할 수 없습니다.

이름	리소스 ID	상태
-	igw-d3d791bb	Available
-	sg-0099ca1e30d406e9a	-
-	sg-02192d3459c3c8f2f	-
-	sg-046434a4e2ce20d31	-
-	sg-07b0497fb30e78bb9	-
-	sg-0d1c52860898734cb	-
-	subnet-a6ff3df9	Available
-	subnet-f0a656bf	Available
-	subnet-503cb13b	Available
-	subnet-d8ea94a3	Available

경고: 이 기본 VPC를 삭제하는 경우, 다른 VPC에서 서브넷을 지정하거나 새 기본 VPC를 생성하지 않으면 이 리전에서 인스턴스를 시작할 수 없습니다.

☒ 기본 VPC를 삭제하려고 합니다.

삭제를 확인하려면 필드에 기본 VPC 삭제를 입력하십시오.

기본 VPC 삭제

취소

삭제

1. VPC

■ 실습. 기본 VPC 삭제

- 대시보드에서 모든 리소스가 삭제됐는지 확인해보자.

🕒 vpc-8369fae8 및 10 기타 리소스를 삭제했습니다.

▶ 세부 정보

VPC 생성 EC2 인스턴스 시작

참고: 인스턴스는 아시아 태평양 리전에서 시작됩니다.

리전별 리소스 [리소스 새로 고침](#)

다음 Amazon VPC 리소스를 사용하고 있습니다.

VPC 모든 리전 보기 ▼	아시아 태평양 0	NAT 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
서브넷 모든 리전 보기 ▼	아시아 태평양 0	VPC 피어링 연결 모든 리전 보기 ▼	아시아 태평양 0
라우팅 테이블 모든 리전 보기 ▼	아시아 태평양 0	네트워크 ACL 모든 리전 보기 ▼	아시아 태평양 0
인터넷 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0	보안 그룹 모든 리전 보기 ▼	아시아 태평양 0
외부 전용 인터넷 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0	고객 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
DHCP 옵션 세트 모든 리전 보기 ▼	아시아 태평양 1	가상 프라이빗 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
탄력적 IP 모든 리전 보기 ▼	아시아 태평양 0	사이트 간 VPN 연결 모든 리전 보기 ▼	아시아 태평양 0
엔드포인트 모든 리전 보기 ▼	아시아 태평양 0	실행 중인 인스턴스 모든 리전 보기 ▼	아시아 태평양 0

1. VPC

■ 실습. VPC 생성

- 기본 VPC 삭제까지 마쳤으면 이제 새로운 VPC를 만들어보자.
- VPC 메뉴로 들어간다.

aws 서비스 Q 서비스, 기능, 블로그, 설명서 등을 검색합니다. [Alt+S]

새로운 VPC 환경
의견을 알려주세요

VPC 대시보드

EC2 글로벌 보기 New

VPC로 필터링:

VPC 선택 ▼

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

✓ vpc-8369fae8 및 10 기타 리소스를 삭제했습니다.

▶ 세부 정보

VPC 생성 EC2 인스턴스 시작

참고: 인스턴스는 아시아 태평양 리전에서 시작됩니다.

리전별 리소스 리소스 새로 고침

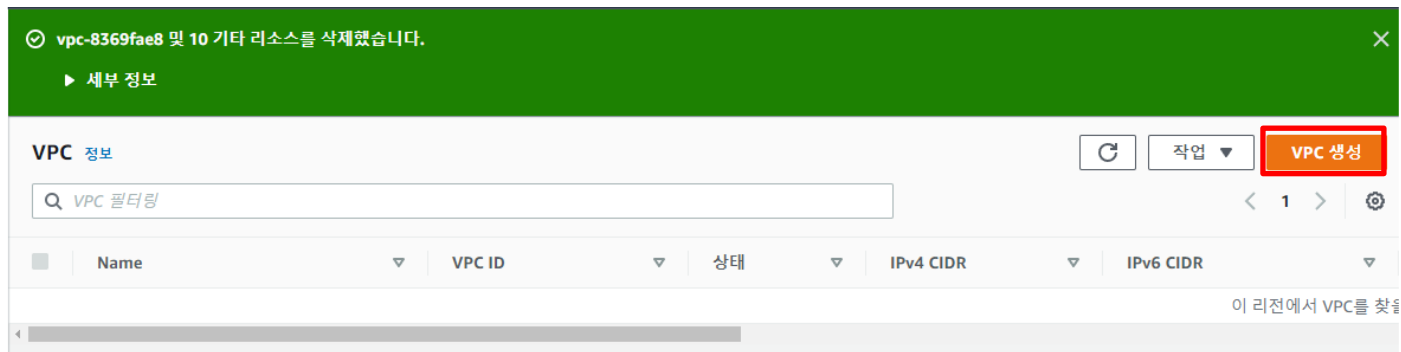
다음 Amazon VPC 리소스를 사용하고 있습니다.

VPC 모든 리전 보기 ▼	아시아 태평양 0	NAT 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
서브넷 모든 리전 보기 ▼	아시아 태평양 0	VPC 피어링 연결 모든 리전 보기 ▼	아시아 태평양 0
라우팅 테이블 모든 리전 보기 ▼	아시아 태평양 0	네트워크 ACL 모든 리전 보기 ▼	아시아 태평양 0

1. VPC

■ 실습. VPC 생성

- 기본 VPC를 삭제했으므로 아무런 VPC도 없는 상태다.
- 그림에서 우측 상단 VPC 생성 버튼을 클릭한다.



■ 실습. VPC 생성

- VPC 이름과 16~28 범위의 CIDR을 입력하고 VPC 생성을 클릭한다.
- 이름 태그는 선택 사항이지만 대규모 시스템으로 확장돼 WC가 많아지면 구분이 어렵다.
- 가급적 태그를 입력해 검색기로 활용한다.

VPC > VPC > VPC 생성

VPC 생성 정보

VPC는 AWS 클라우드의 격리된 부분으로서, Amazon EC2 인스턴스와 같은 AWS 객체로 채워집니다.

VPC 설정

생성할 리소스 정보
VPC 리소스 또는 VPC 및 기타 네트워킹 리소스만 생성합니다.

☒ VPC만 ☐ VPC 등

이름 태그 - 선택 사항
'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

IPv4 CIDR 블록 정보
☒ IPv4 CIDR 수동 입력 ☐ IPAM 할당 IPv4 CIDR 블록

IPv4 CIDR

IPv6 CIDR 블록 정보
☒ IPv6 CIDR 블록 없음 ☐ IPAM 할당 IPv6 CIDR 블록 ☐ Amazon 제공 IPv6 CIDR 블록 ☐ 내가 소유한 IPv6 CIDR

테넌시 정보

1. VPC

■ 실습. VPC 생성

- VPC 생성을 완료하면 기본 VPC 여부, CIDR, 기본 라우팅 테이블과 네트워크 ACL 등 VPC 관련 정보가 나타난다.

VPC > VPC > vpc-00bea3185b4d9d017

vpc-00bea3185b4d9d017 / my-NewVPC 작업 ▼

세부 정보 [정보](#)

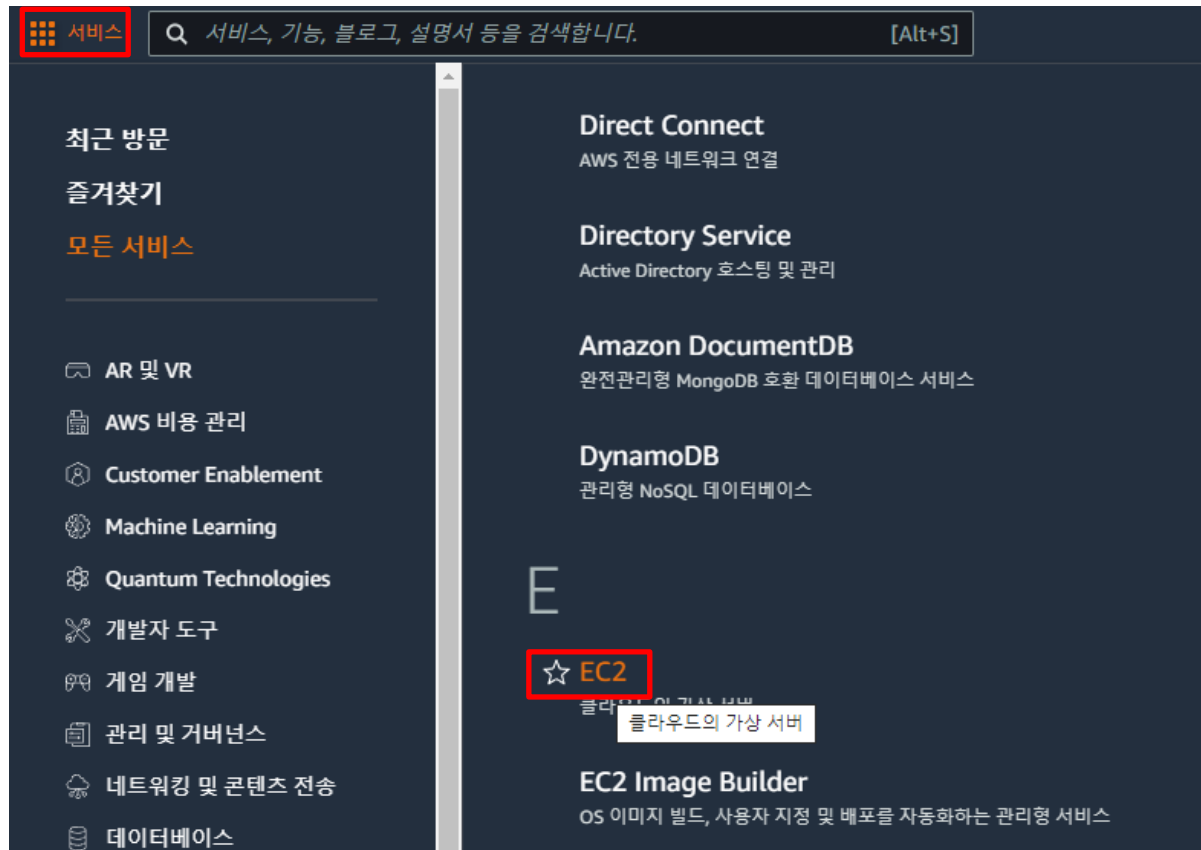
VPC ID vpc-00bea3185b4d9d017	상태 Available	DNS 호스트 이름 비활성화됨	DNS 확인 활성화됨
테넌시 Default	DHCP 옵션 세트 dopt-f6296e9d	기본 라우팅 테이블 rtb-0608ef5be42893aea	기본 네트워크 ACL acl-0bee5d7ee87f4cd15
기본 VPC 아니요	IPv4 CIDR 92.75.0.0/16	IPv6 풀 -	IPv6 CIDR(네트워크 경계 그룹) -
Route 53 Resolver DNS 방화벽 규칙 그룹 -	소유자 ID 262663767358		

- VPC에 서브넷을 생성하면 그림과 같이 기본 라우팅 테이블과 기본 네트워크 ACL이 생성되고 서브넷에 자동 연결된다.

1. VPC

■ 실습. VPC 생성

- EC2 대시보드에 들어가면 기본 보안 그룹도 확인할 수 있다.
- 기본 보안 그룹 규칙을 모두 삭제하자.
- 서비스 > EC2 선택



1. VPC

■ 실습. VPC 생성

- EC2 대시보드 > 보안그룹 선택

리소스

EC2 글로벌 보기 ↗ ↺ ⚙

아시아 태평양 (서울) 리전에서 다음 Amazon EC2 리소스를 사용하고 있음:

인스턴스(실행 중)	0	로드 밸런서	0	배치 그룹	0
보안 그룹	1	볼륨	0	스냅샷	0
인스턴스	0	전용 호스트	0	키 페어	2
탄력적 IP	0				

i AWS Launch Wizard for SQL Server를 사용하여 AWS에서 Microsoft SQL Server Always On 가용성 그룹을 손쉽게 크기 조정, 구성 및 배포할 수 있습니다. 자세히 알아보기 **×**

1. VPC

■ 실습. VPC 생성

- [인바운드 규칙 편집] 선택

sg-0800f83494a37045b - default

세부 정보 | **인바운드 규칙** | 아웃바운드 규칙 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. [Reachability Analyzer 실행](#) X

인바운드 규칙 (1/1)

🔄 태그 관리 **인바운드 규칙 편집**

🔍 보안 그룹 규칙 필터

<input checked="" type="checkbox"/>	Name	보안 그룹 규칙 ID	IP 버전	유형	프로토콜	포트 범위
<input checked="" type="checkbox"/>	-	sgr-000a9270b45a48...	-	모든 트래픽	전체	전체

1. VPC

■ 실습. VPC 생성

- [삭제] > [규칙 저장]을 순서대로 클릭

인바운드 규칙 정보

보안 그룹 규칙 ID	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보
sgr-000a9270b45a48025	모든 트래픽 ▼	전체	전체	사용자 ... ▼	

규칙 추가

sg-0800f83494a37045b

×

삭제

취소

변경 사항 미리 보기

규칙 저장

1. VPC

■ 실습. VPC 생성

- 아웃바운드 규칙 > [아웃바운드 규칙 편집]을 선택



sg-0800f83494a37045b - default

세부 정보 | 인바운드 규칙 | **아웃바운드 규칙** | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. [Reachability Analyzer 실행](#)

아웃바운드 규칙 (1/1) [태그 관리](#) **아웃바운드 규칙 편집**

보안 그룹 규칙 필터

<input checked="" type="checkbox"/>	Name	보안 그룹 규칙 ID	IP 버전	유형	프로토콜	포트 범위
<input checked="" type="checkbox"/>	-	sgr-05e4a742b06eb72f2	IPv4	모든 트래픽	전체	전체

1. VPC

■ 실습. VPC 생성

- [삭제] > [규칙 저장]을 순서대로 클릭

아웃바운드 규칙 편집 [정보](#)

아웃바운드 규칙은 인스턴스를 나가도록 허용된 발신 트래픽을 제어합니다.

아웃바운드 규칙 [정보](#)

보안 그룹 규칙 ID	유형 정보	프로토콜 정보	포트 범위 정보	대상 정보	설명 - 선택 사항 정보
sgr-05e4a742b06eb72f2	모든 트래픽 ▼	전체	전체	사용자 ... ▼ 0.0.0.0/0 ✕	<div>삭제</div>

규칙 추가

취소

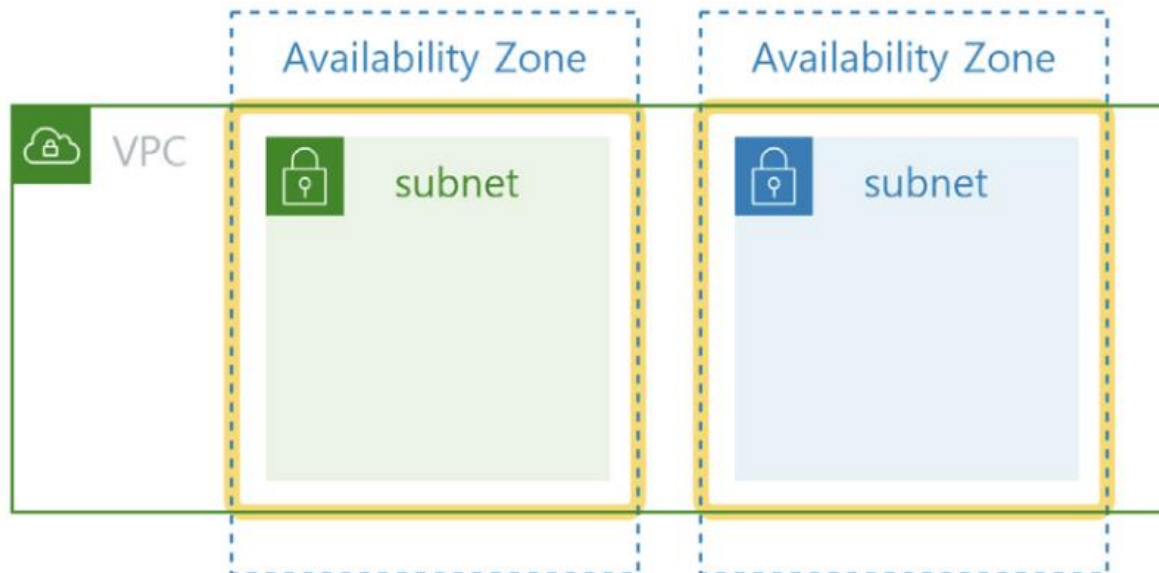
변경 사항 미리 보기

규칙 저장

2. 서브넷

■ 서브넷 = 가용 영역 \cap VPC

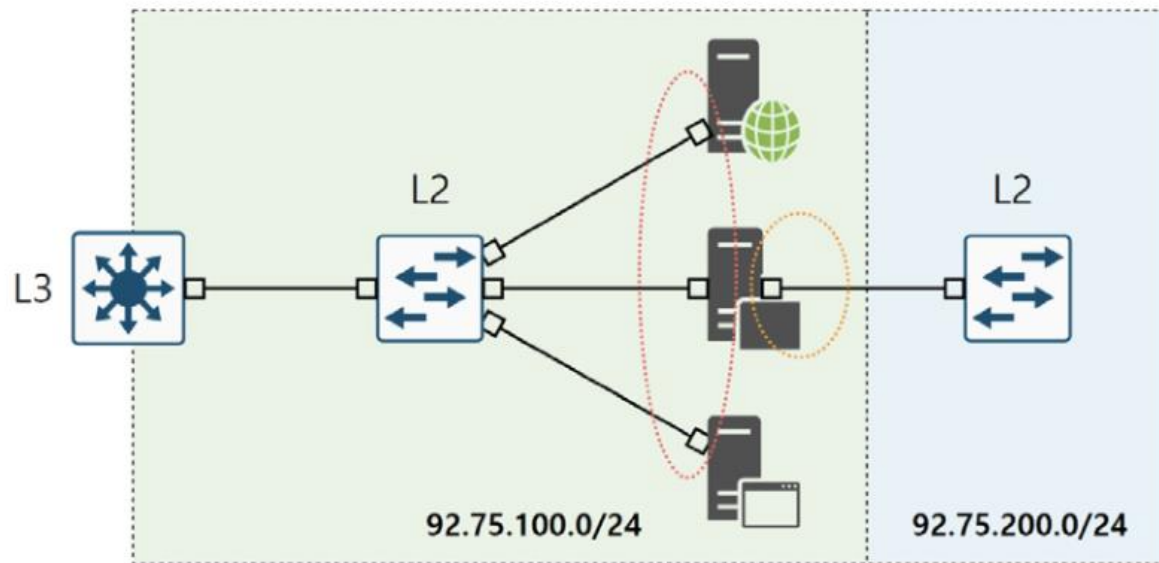
- 서브넷은 VPC와 가용 영역 모두에 포함되는 공간이다.
- 그러므로 서브넷은 그림의 노랑 경계를 넘어 존재할 수 없다.



2. 서브넷

■ 서브넷의 역할

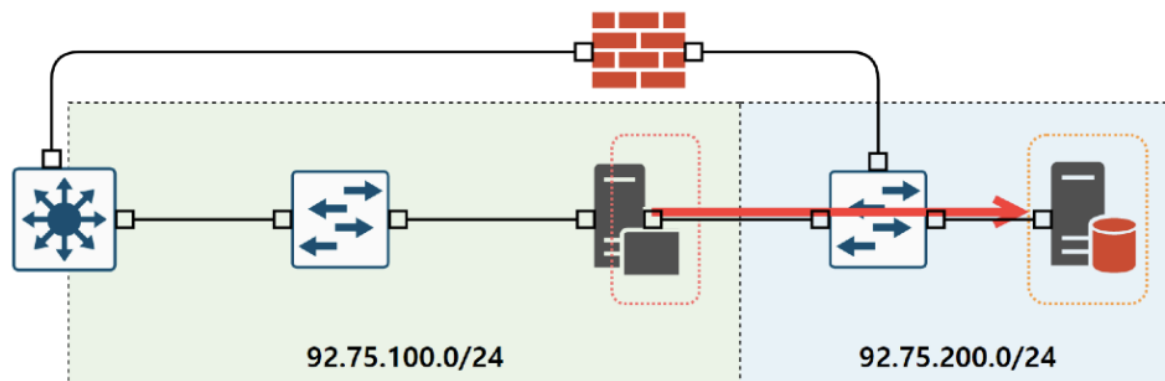
- 온프레미스도 다르지 않다.
- 서버팜 내부에 서버를 둔다고 하지만, 서버팜 스위치에 실제 연결된 것은 서버의 NIC(Network Interface Card, 네트워크 인터페이스 카드)다.



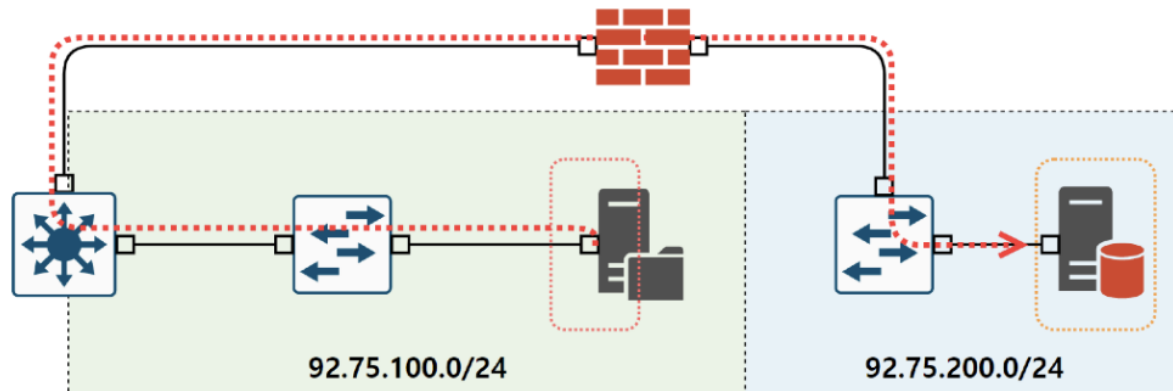
2. 서브넷

■ 서브넷 우회 경로의 근원

- 그림은 서버가 방화벽을 통과하지 않고 자체 NIC로 DB에 직접 접근하는 모습을 나타낸다.
- 네트워크로 접속할 땐 네트워크 인터페이스가 아닌 라우팅에 의존해야 한다.



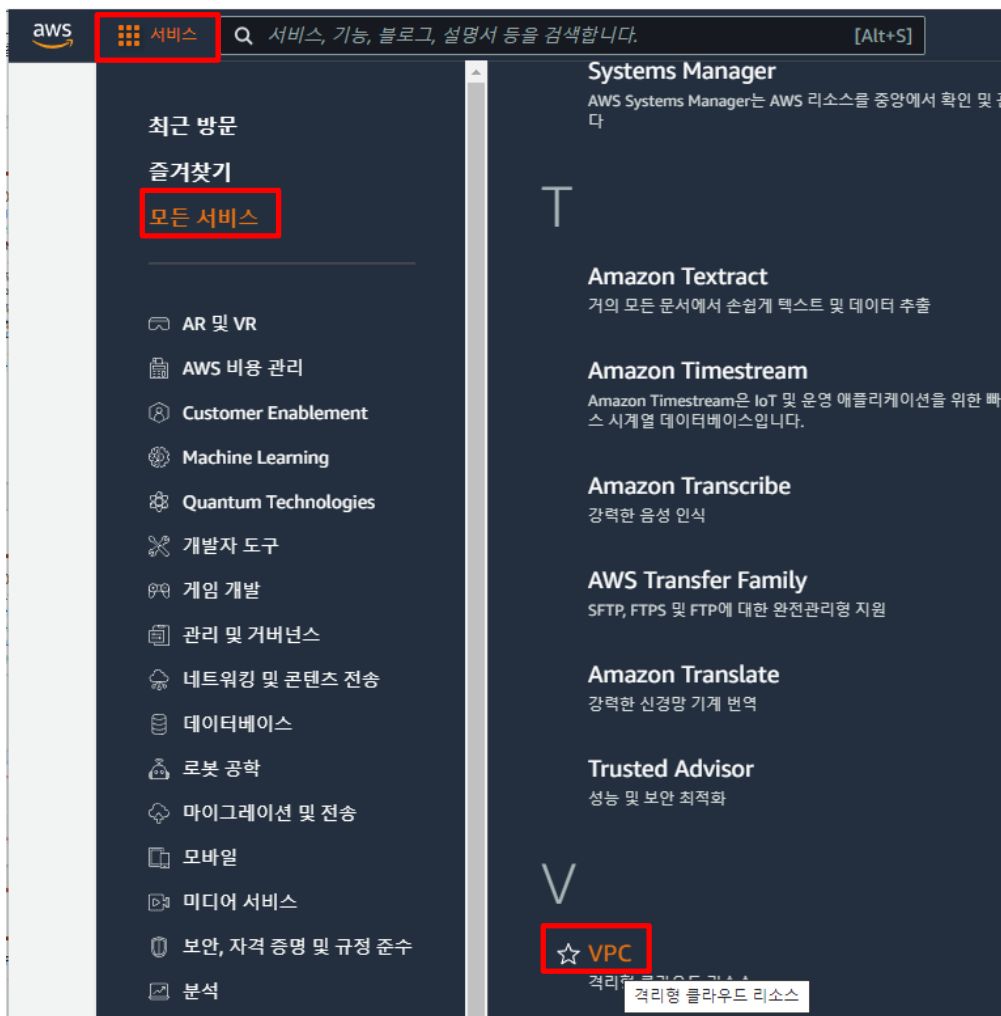
- 다음 그림은 NIC가 아닌 라우팅으로 DB에 접근하는 네트워크 구성이다.



2. 서브넷

■ 실습. 서브넷 생성 예제

- 서브넷 메뉴에 진입한다.
- 서비스 > VPC 선택



2. 서브넷

■ 실습. 서브넷 생성 예제

■ 서브넷 선택

VPC 생성

EC2 인스턴스 시작

참고: 인스턴스는 아시아 태평양 리전에서 시작됩니다.

리전별 리소스 [리소스 새로 고침](#)

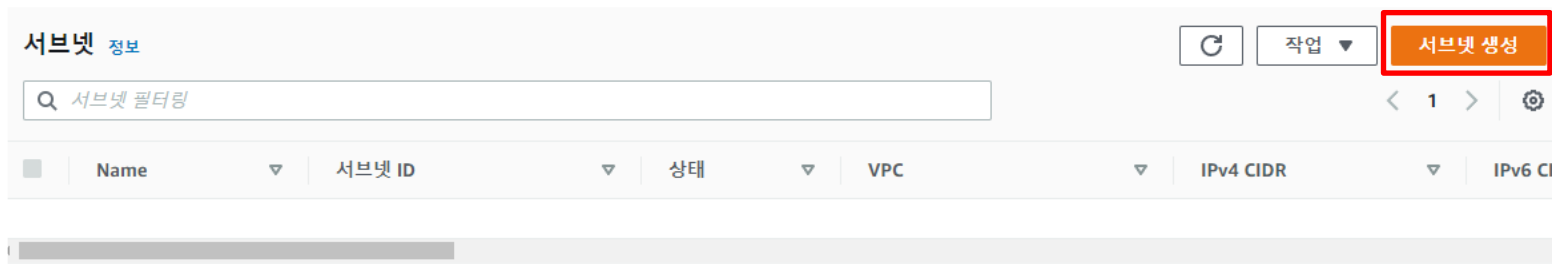
다음 Amazon VPC 리소스를 사용하고 있습니다.

VPC 모든 리전 보기 ▼	아시아 태평양 1	NAT 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
서브넷 모든 리전 보기 ▼	아시아 태평양 0	VPC 피어링 연결 모든 리전 보기 ▼	아시아 태평양 0
라우팅 테이블 모든 리전 보기 ▼	아시아 태평양 1	네트워크 ACL 모든 리전 보기 ▼	아시아 태평양 1
인터넷 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0	보안 그룹 모든 리전 보기 ▼	아시아 태평양 1
외부 전용 인터넷 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0	고객 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
DHCP 옵션 세트 모든 리전 보기 ▼	아시아 태평양 1	가상 프라이빗 게이트웨이 모든 리전 보기 ▼	아시아 태평양 0
탄력적 IP 모든 리전 보기 ▼	아시아 태평양 0	사이트 간 VPN 연결 모든 리전 보기 ▼	아시아 태평양 0

2. 서브넷

■ 실습. 서브넷 생성 예제

- 앞절에서 기본 VPC를 삭제했으므로 기본 서브넷도 자동 삭제됐다.
- 우측 상단 서브넷 생성 버튼을 클릭한다.



2. 서브넷

■ 실습. 서브넷 생성 예제

- 서브넷은 가용 영역과 VPC의 공통 영역이므로, 이 2가지를 모두 지정해야 한다.
- 우선 앞에서 만든 VPC를 선택한다.

VPC > 서브넷 > 서브넷 생성

서브넷 생성 정보

VPC

VPC ID
이 VPC에 서브넷을 생성합니다.

VPC 선택

Q |

vpc-00bea3185b4d9d017 (my-NewVPC)
92.75.0.0/16

서브넷의 CIDR 블록 및 가용 영역을 지정합니다.

새 서브넷을 생성하려면 먼저 VPC를 선택합니다.

새 서브넷 추가

취소

서브넷 생성

2. 서브넷

■ 실습. 서브넷 생성 예제

- 생성할 서브넷 정보를 입력한다.
- 이 단계에서 가용 영역을 지정한다.

서브넷 설정

서브넷의 CIDR 블록 및 가용 영역을 지정합니다.

1/1개 서브넷

서브넷 이름
'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

PUB-WEB-2a-92.75.100

이름은 최대 256자까지 입력할 수 있습니다.

가용 영역 정보
서브넷이 상주할 영역을 선택합니다. 선택하지 않으면 Amazon이 자동으로 선택합니다.

아시아 태평양 (서울) / ap-northeast-2a

IPv4 CIDR 블록 정보

92.75.100.0/24

▼ 태그 - 선택 사항

키	값 - 선택 사항
Name	PUB-WEB-2a-92.75.100

새 태그 추가

49글(를) 태그.개 더 추가할 수 있습니다.

제거

새 서브넷 추가

취소 **서브넷 생성**

2. 서브넷

■ 실습. 서브넷 생성 예제

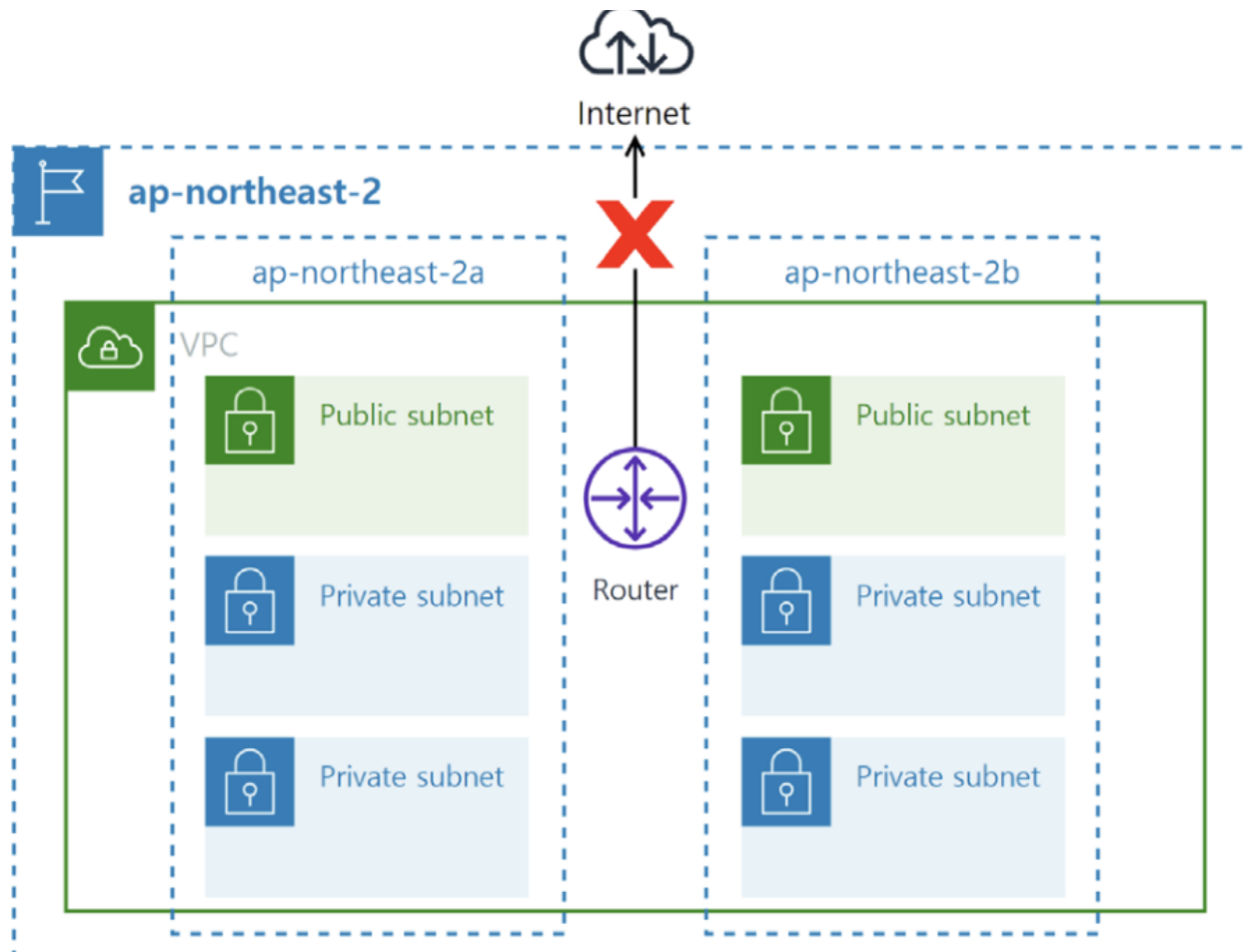
- 위 내용을 참고해 다음 6개 서브넷을 생성해보자.
 - 퍼블릭 서브넷 : PUB-WEB-2a-92.75.100, PUB-WEB-2b-92.75.200
 - 프라이빗 서브넷 : PRI-WAS-2a-92.75.10, PRI-WAS-2b-92.75.20, PRI-DB-2a-92.75.1, PRI-DB-2b-92.75.2
- 목록에 6개 서브넷을 확인할 수 있다.

서브넷 (6) 정보						
Q 서브넷 필터링						
Name ▼	서브넷 ID ▼	IPv4 CIDR ▼	가용 영역 ▼	라우팅 테이블 ▼	네트워크 ACL	
PUB-WEB-2b-92.75.200	subnet-04cb036c6534817fa	92.75.200.0/24	ap-northeast-2b	rtb-068c3c3d56e83e7c7	acl-0631fd4d1c5ce0a60	
PUB-WEB-2a-92.75.100	subnet-0765bc7c7bd1b3b09	92.75.100.0/24	ap-northeast-2a	rtb-068c3c3d56e83e7c7	acl-0631fd4d1c5ce0a60	
PRI-WAS-2b-92.75.20	subnet-098a731873c43792e	92.75.20.0/24	ap-northeast-2b	rtb-068c3c3d56e83e7c7	acl-0631fd4d1c5ce0a60	
PRI-WAS-2a-92.75.10	subnet-0b985a2d487fd363c	92.75.10.0/24	ap-northeast-2a	rtb-068c3c3d56e83e7c7	acl-0631fd4d1c5ce0a60	
PRI-DB-2b-92.75.2	subnet-0e556740d35b9b5b6	92.75.2.0/24	ap-northeast-2b	rtb-068c3c3d56e83e7c7	acl-0631fd4d1c5ce0a60	
PRI-DB-2a-92.75.1	subnet-0a8f690278a26e95f	92.75.1.0/24	ap-northeast-2a	rtb-068c3c3d56e83e7c7	acl-0631fd4d1c5ce0a60	

2. 서브넷

■ 실습. 서브넷 생성 예제

- 서브넷이 생성되면서 VPC의 기본 라우팅 테이블과 기본 네트워크 ACL이 자동 연결됐다.
- 다음 그림은 서브넷 6개를 생성한 토폴로지다.





Thank You
