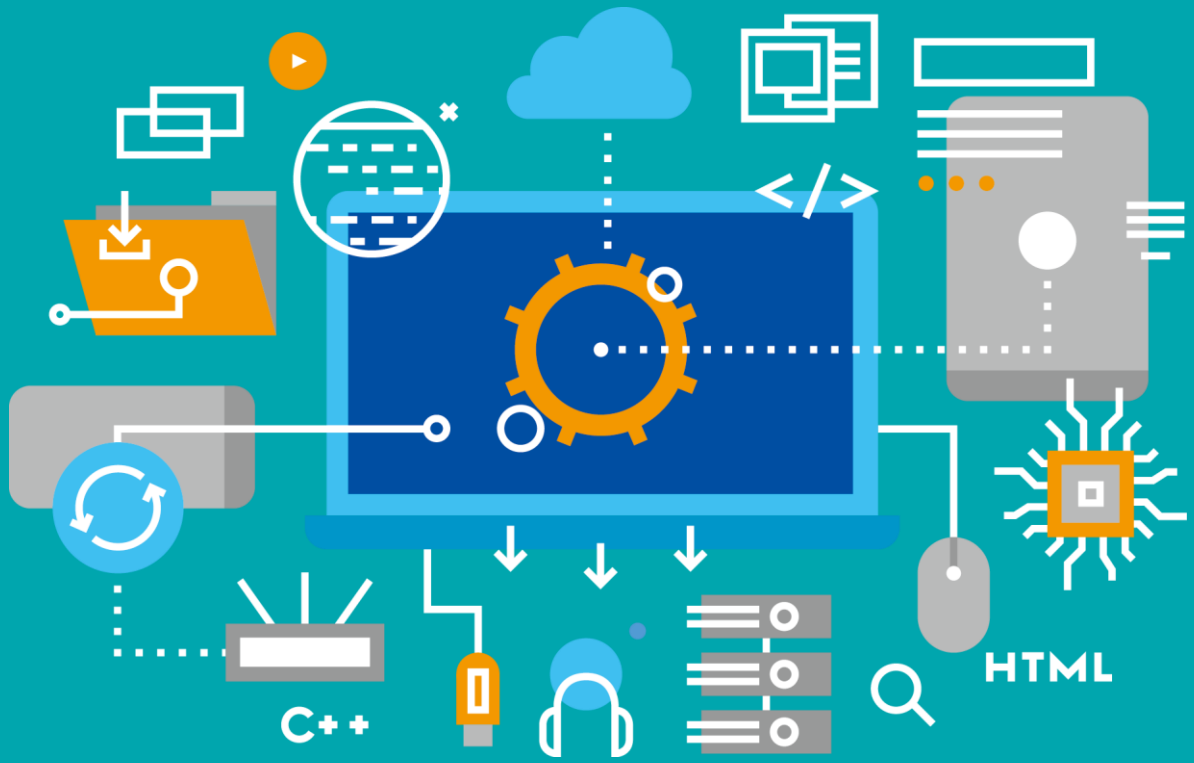
동양미래대학교

DMMU

동양미래대학교 전문기술 석사과정

클라우드와 네트워크 보안

Dongyang Mirae University

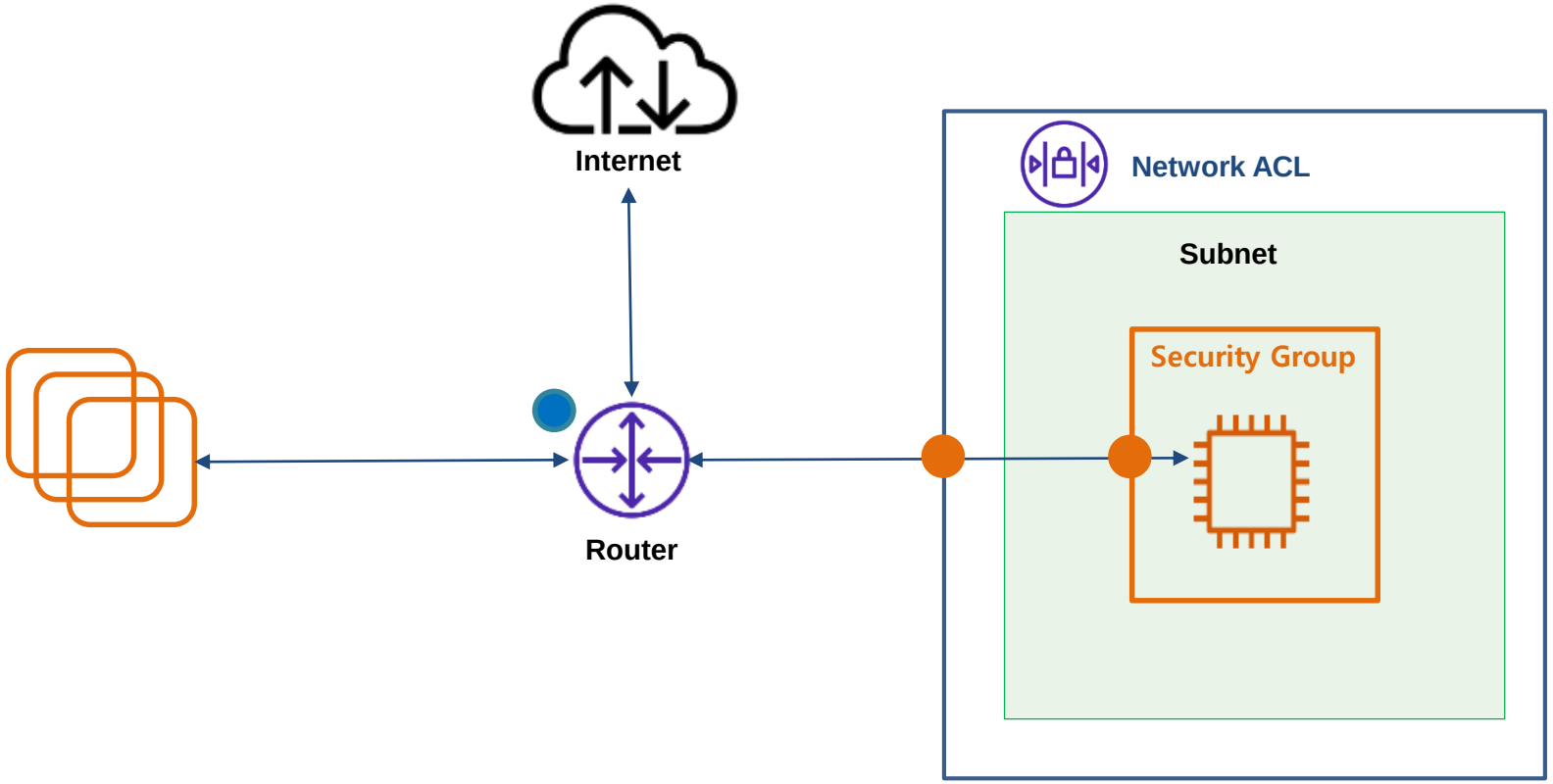


5장

- 접근제어 : 보안 그룹과 네트워크 ACL

Access Control

Routing Control



- **접근 제어 (Access Control)** :

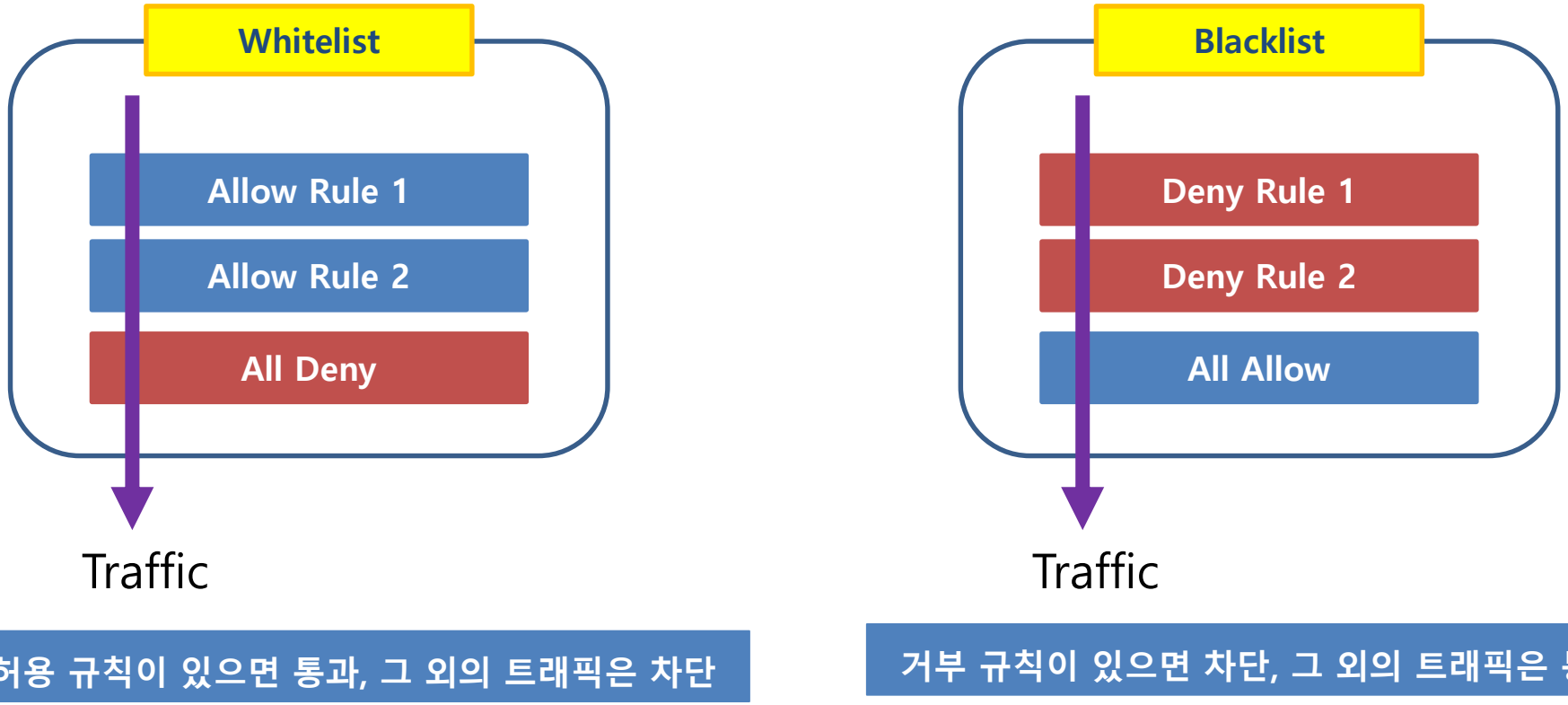
  필요한 트래픽만 허용하고, 불필요한 트래픽은 차단

온프레미스 : 방화벽(firewall)을 통해 접근을 제어

VPC : 보안그룹(Security Group)과 네트워크 ACL(Network Access Control List)이 접근을 제어

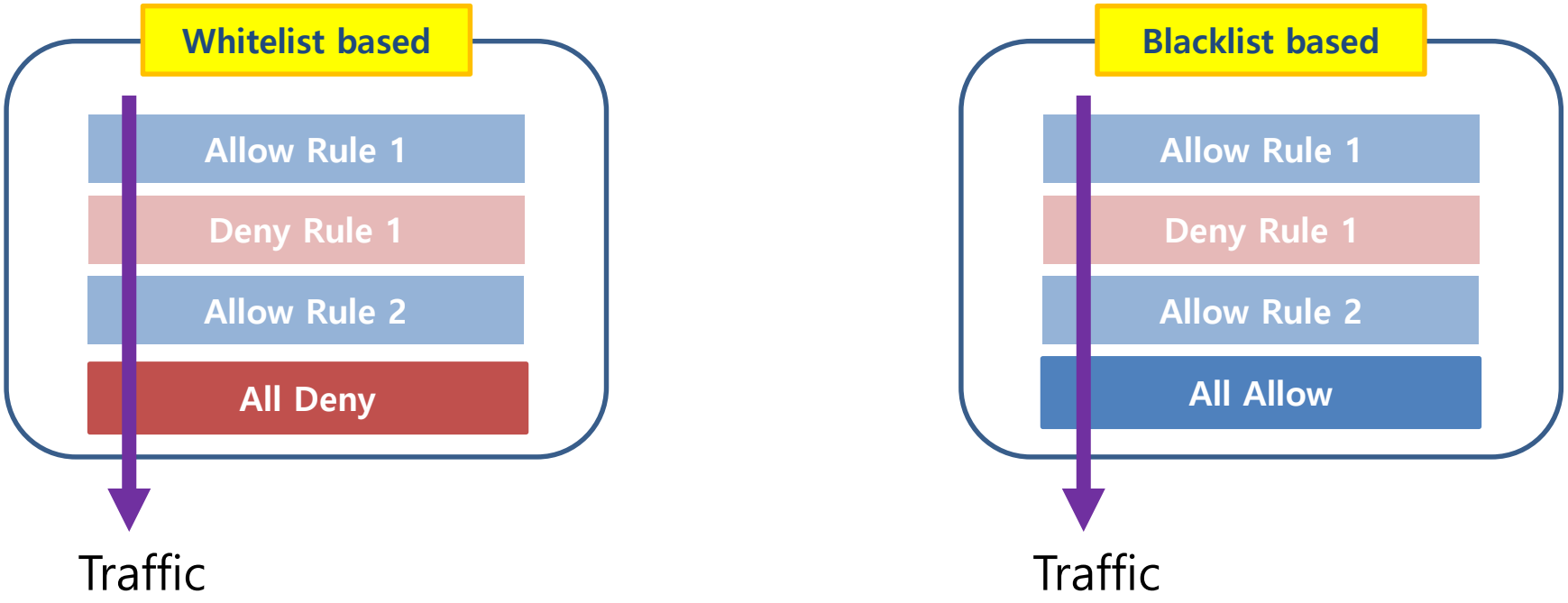
- **접근 제어 (Access Control) 방식 비교** :

  Whitelist 방식 vs. Blacklist 방식



접근 제어 (Access Control) 방식 비교 : Whitelist 방식 vs. Blacklist 방식

Hybrid

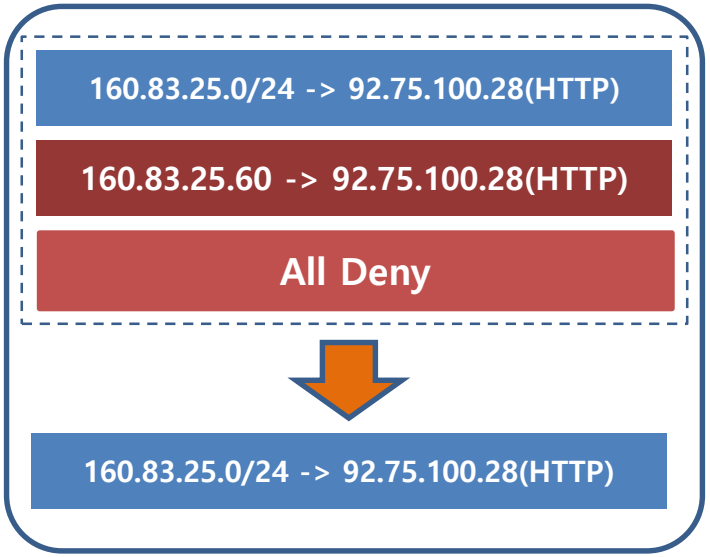


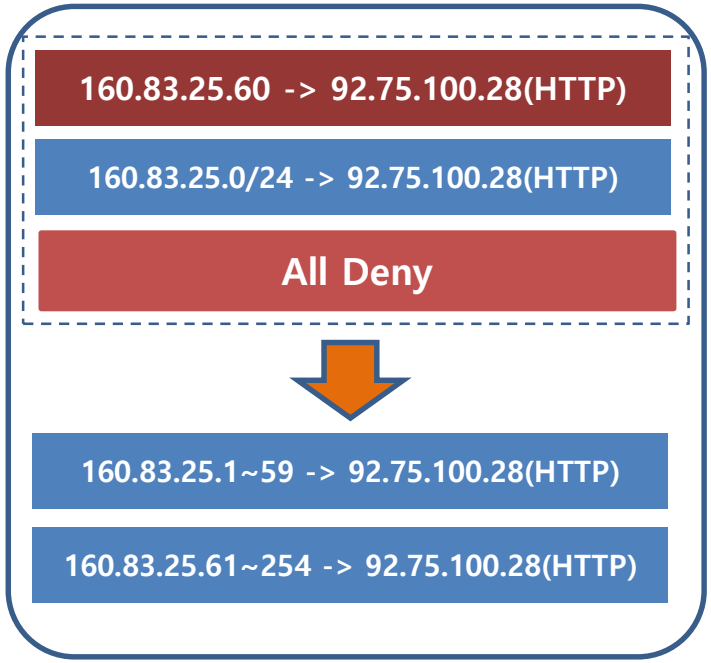
Whitelist 기반 결합방식
- 모든 거부 규칙을 최하단에 놓고, 허용과 거부 규칙 혼합

Blacklist 기반 결합방식
- 모든 허용 규칙을 최하단에 놓고, 허용과 거부 규칙 혼합

접근 제어 (Access Control) 방식 비교 : Whitelist 방식 vs. Blacklist 방식

Hybrid – 규칙(rule) 적용 순서에 따라 허용 가능 트래픽 범위가 달라짐





결합방식(Hybrid)은 규칙의 적용 순서가 중요하므로, 규칙마다 규칙번호(Rule Number)가 존재

- 트래픽이 들어오면 낮은 번호의 규칙부터 적용 됨
- 온프레미스 방화벽에서는 규칙번호를 시퀀스(SEQ)라고 표현

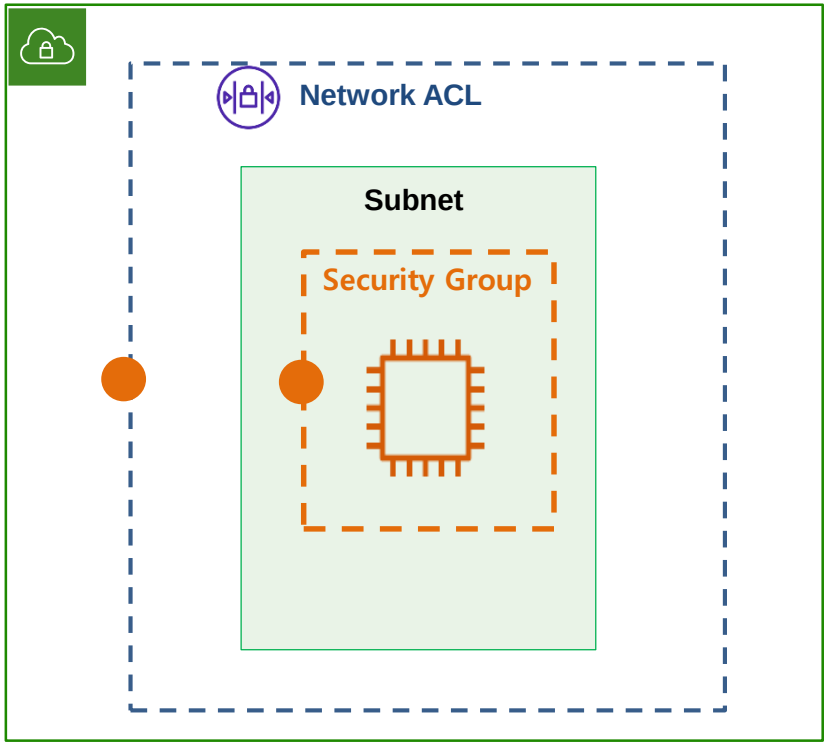
- **AWS에서의 접근 제어 (Access Control)**

보안그룹(SG : Security Group) – Whitelist 방식 적용

네트워크 ACL – Hybrid 방식 적용

SG는 규칙 번호를 사용하지 않음 (규칙 순서가 무의미 함)
NACL은 규칙 번호를 사용 (규칙 순서가 중요)

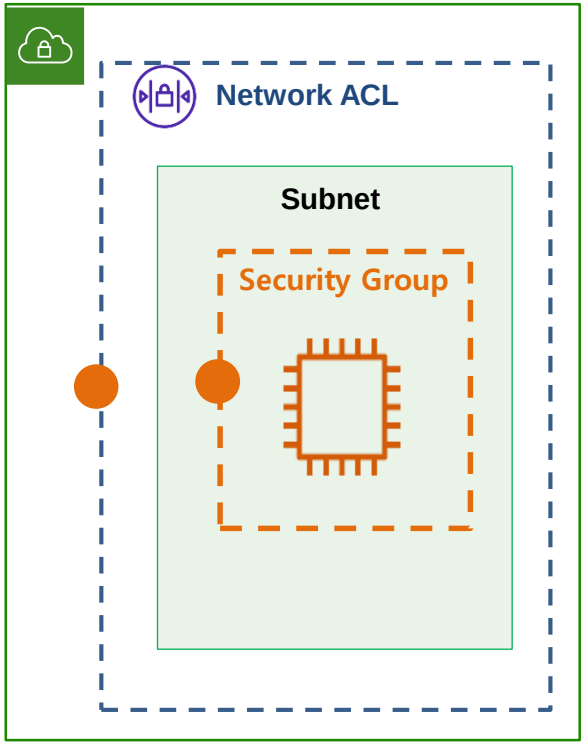
- 보안 그룹 (Security Group)



보안그룹(SG : Security Group) – Whitelist 방식 적용

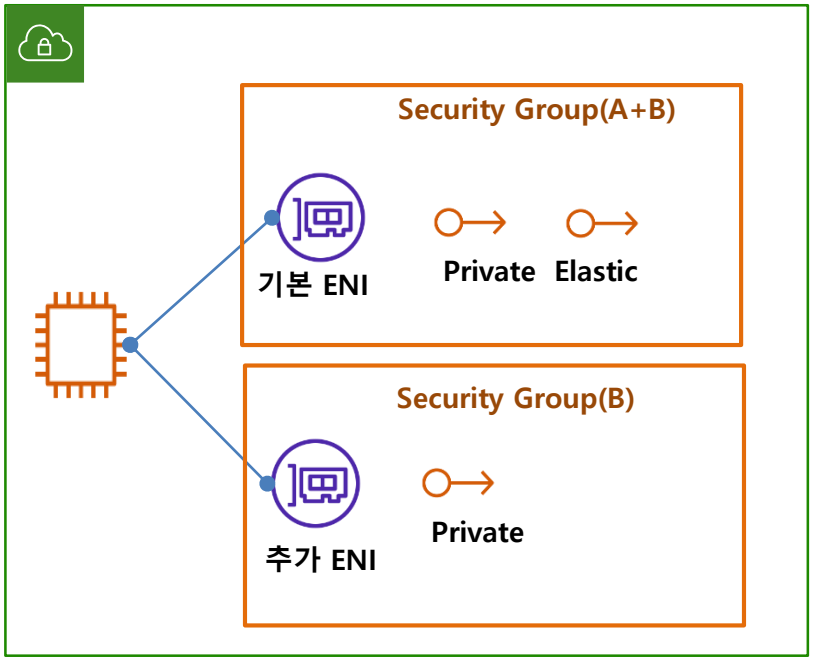
- ENI(Elastic Network Interface)로 들어오거나 나가는 트래픽 접근을 제어

  - SG의 연결 대상은 ENI이며, 수명 주기 동안 다른 ENI에 연결 가능
  - SG는 어떤 ENI에도 연결하지 않은 상태로 존재 가능함
  - 반대로 **컴퓨팅 ENI**는 반드시 SG에 연결되어 있어야 함
  - 1개 SG를 여러 ENI에 연결 가능(1:N)
  - 여러 SG를 1개의 ENI에 연결 가능(N:1) – 하나의 서비스에 여러 역할 부여
  - VPC가 생성되면 **기본 SG**도 함께 생성(기본 SG 수와 VPC 수는 동일함)



보안그룹(SG : Security Group) – Whitelist 방식 적용

- ENI(Elastic Network Interface)로 들어오거나 나가는 트래픽 접근을 제어



- ❖ SG(B)는 기본 ENI와 추가 ENI에 연결됨 (1:N 연결)
- ❖ 기본 ENI에 SG(A)와 SG(B)가 연결됨 (N:1 연결)
- ❖ SG는 화이트리스트 방식으로 규칙간 순서가 중용하지 않음
- ✓ ENI에 SG(A)나 SG(B) 중 것을 먼저 연결해도 허용 규칙을 순서 없이 적용

보안그룹(SG : Security Group) – 규칙 형태

- 온프레미스 방화벽 규칙

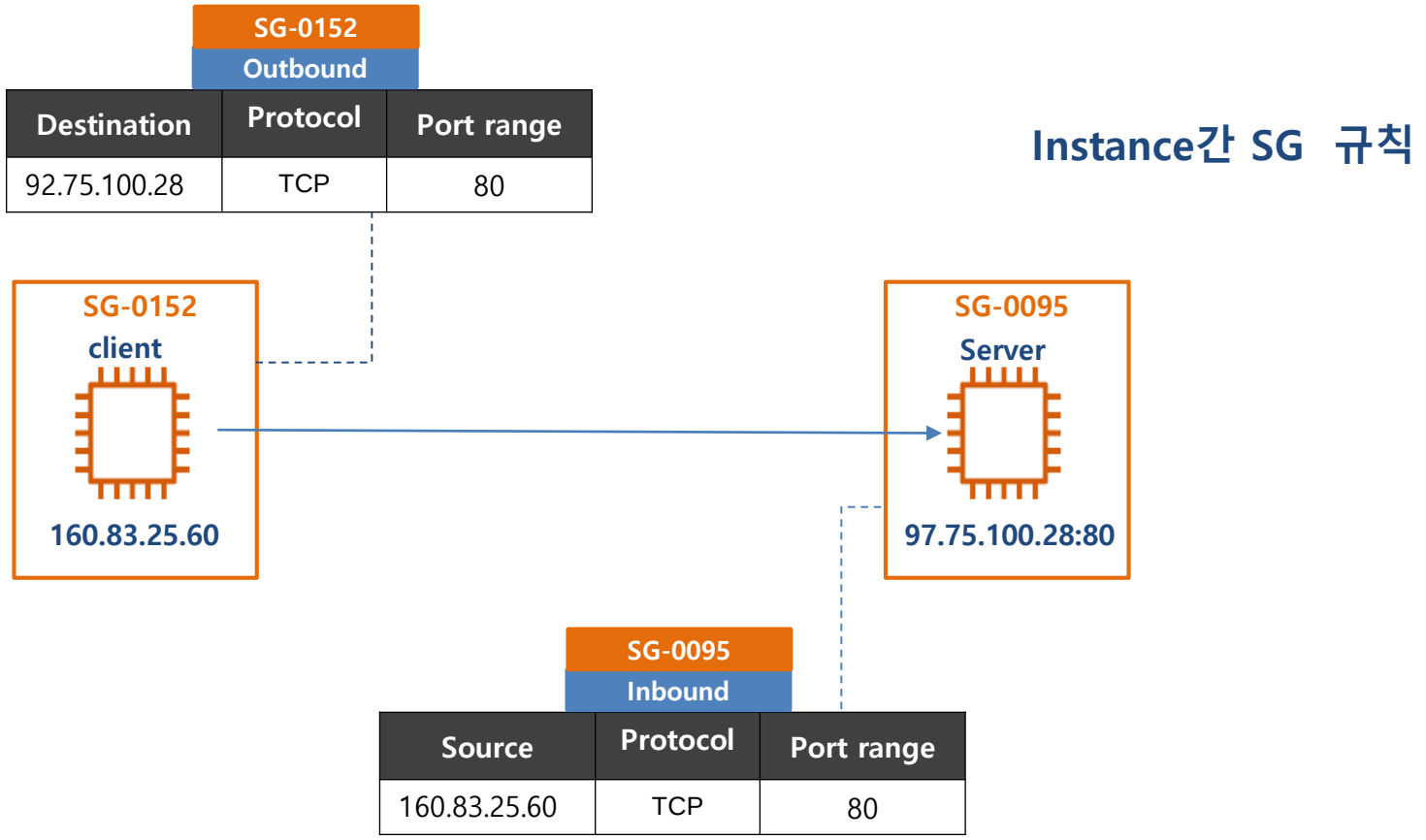
Allow/Deny	Source	Destination	Protocol	Port Range
Allow	160.83.25.60	92.75.100.28	TCP	80
Allow	92.75.100.28	160.83.25.60	TCP	22

- 출발지 IP, 목적지 IP, 프로토콜 유형, 포트번호를 저장
- 유입되는 트래픽이 각 규칙과 일치하는 경우 허용하거나 차단함

보안그룹(SG : Security Group) – 규칙 형태

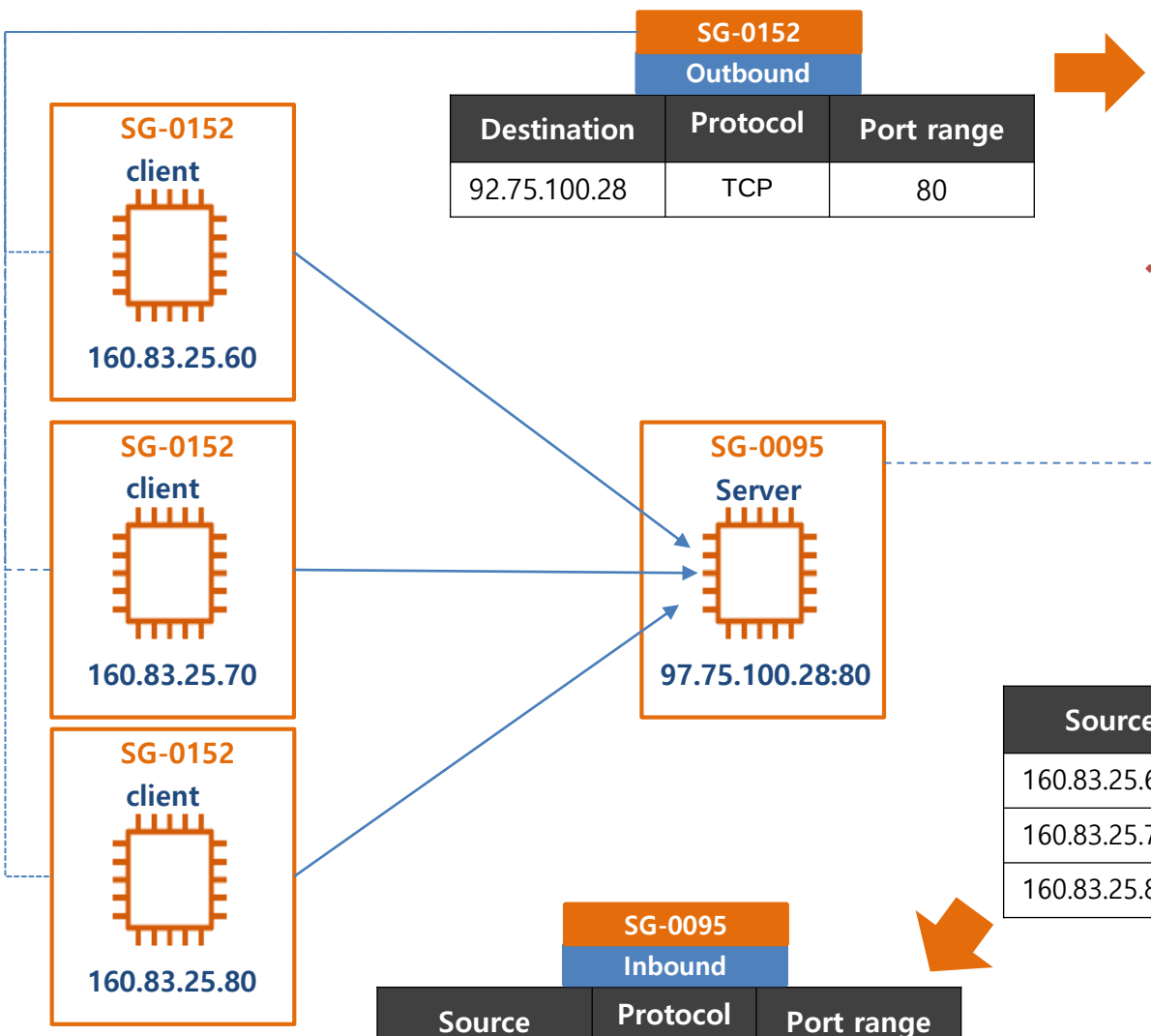
- AWS 보안 그룹 : 연결 대상은 ENI
  - ❖ ENI로 들어오거나 나가는 트래픽을 통제
  - ❖ Inbound / Outbound 트래픽 규칙을 개별관리함
  - ❖ Inbound 트래픽의 목적지 IP, Outbound 트래픽의 발신지 IP 관리 불필요
  - ✓ 일반적으로 온프레미스 환경의 방화벽은 Inbound / Outbound 트래픽 규칙을 별도 관리하지 않고, 소스와 대상 모두 규칙 하나로 입력 관리

● 보안그룹(SG : Security Group) – Inbound / Outbound 규칙 개별 관리함



● 보안그룹(SG : Security Group)

클라이언트 수가 많아지면 ?



SG-0152 Outbound

Destination	Protocol	Port range
92.75.100.28	TCP	80

SG-0152 Outbound

Destination	Protocol	Port range
SG-0095	TCP	80

❖ SG-0095를 사용하는 컴퓨팅 서비스로 접속 허용

SG-0095 Inbound

Source	Protocol	Port range
160.83.25.60	TCP	80
160.83.25.70	TCP	80
160.83.25.80	TCP	80

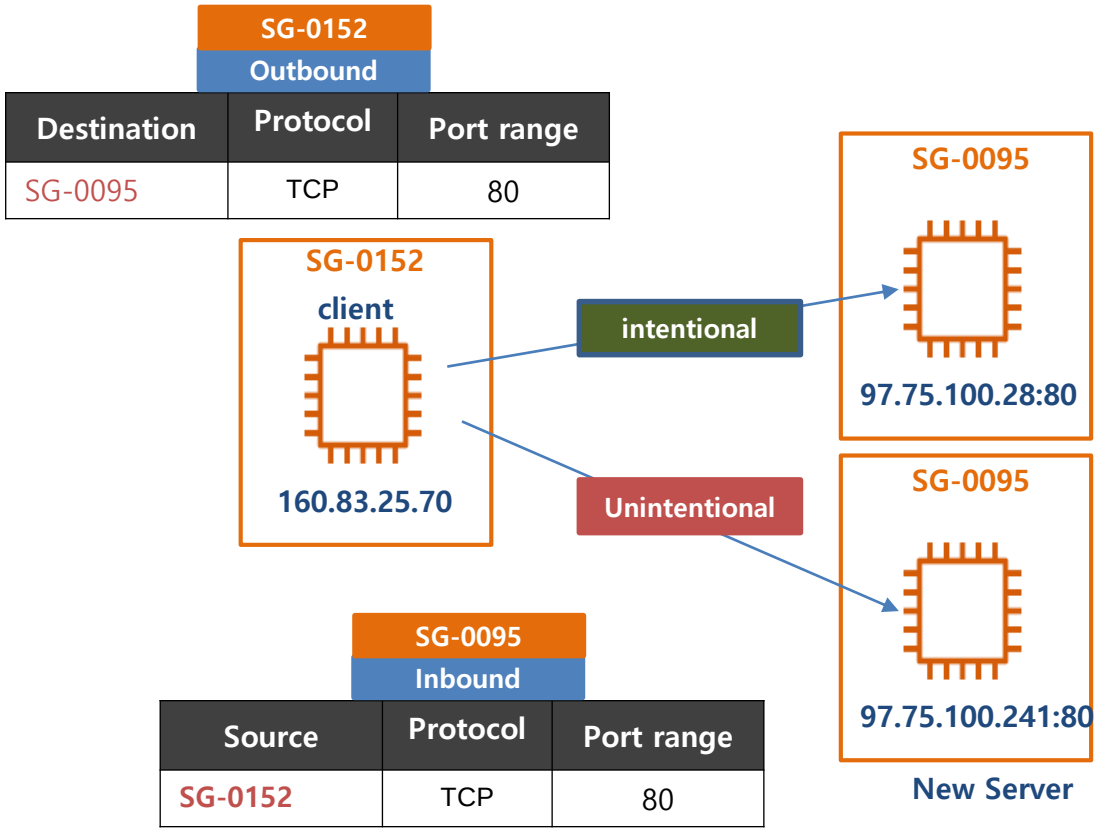
SG-0095 Inbound

Source	Protocol	Port range
SG-0152	TCP	80

❖ SG-0152를 사용하는 컴퓨팅 서비스의 접속 허용

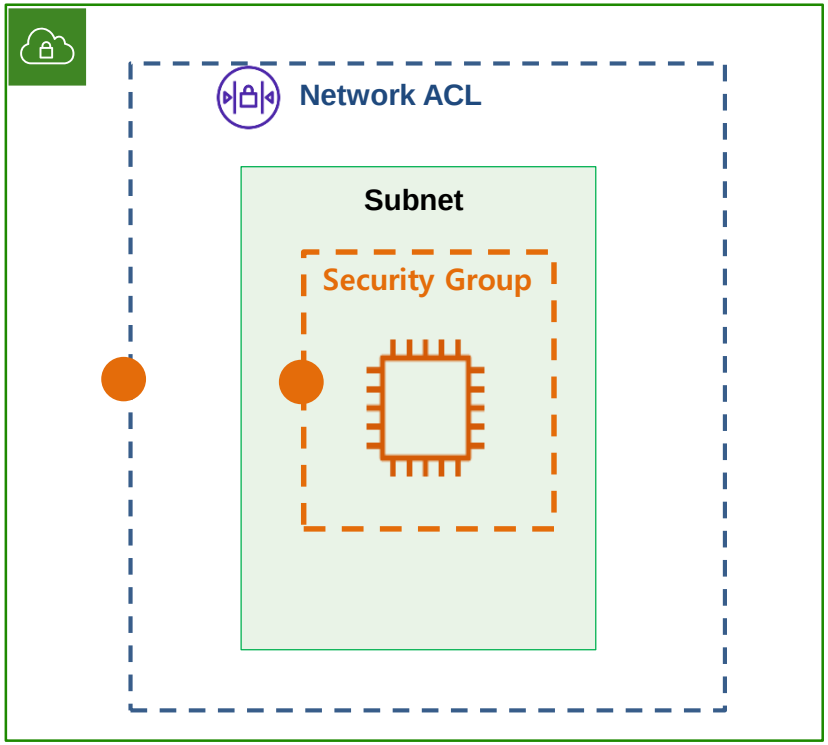
보안그룹(SG : Security Group)

의도하지 않은 접속 허용



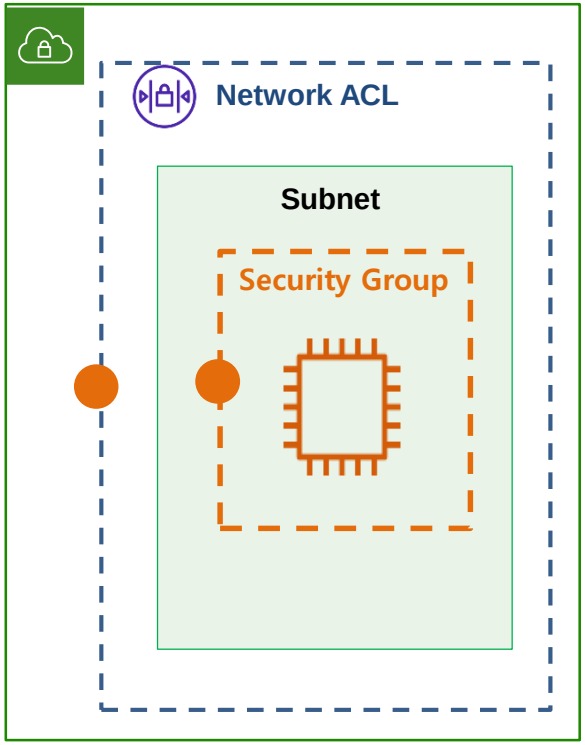
- ❖ 컴퓨팅 ENI는 반드시 SG에 연결해야 함
- ❖ 인스턴스 생성 단계에서 ENI 기본 장착하므로 SG 역시 인스턴스 생성시 함께 선택 연결하도록 설계됨
- ✓ 불필요한 SG는 인스턴스에서 반드시 해제

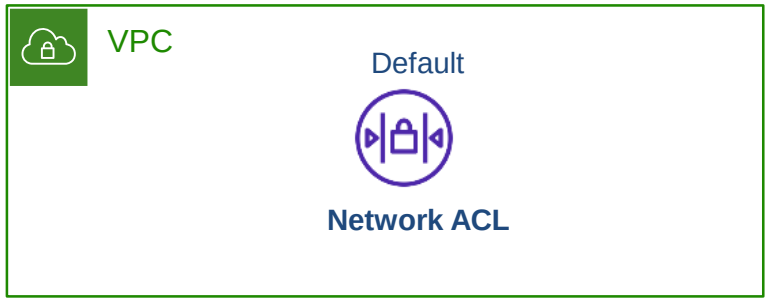
네트워크 ACL



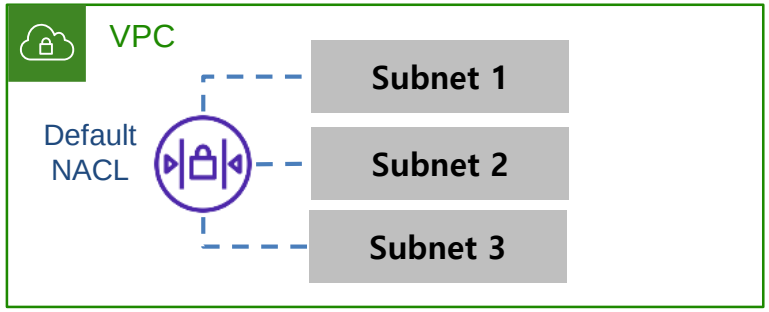
네트워크 ACL – 서브넷을 통과하는 트래픽 접근을 제어

- NACL의 연결 대상은 서브넷이며, 수명 주기 동안 다른 서브넷에 연결 가능
- NACL 는 어떤 서브넷에도 연결하지 않은 상태로 존재 가능함
- 반대로 **서브넷은** 반드시 NACL에 연결되어 있어야 함
- VPC가 생성되면 **기본 NACL**도 함께 생성(기본 NACL 수와 VPC 수는 동일함)
- 서브넷을 생성하면 무조건 기본 NACL에 자동 연결 된다.

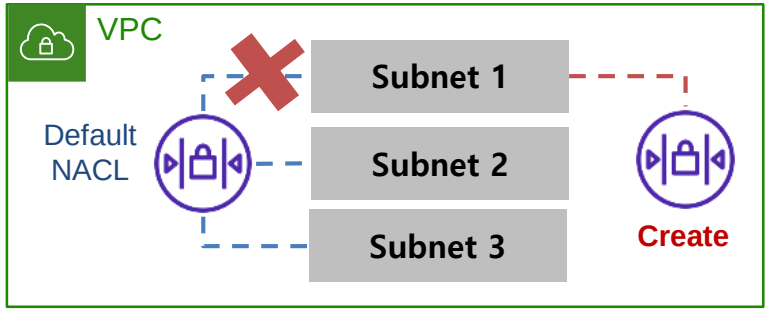




❖ VPC 생성시에 기본 NACL(default)도 함께 생성됨

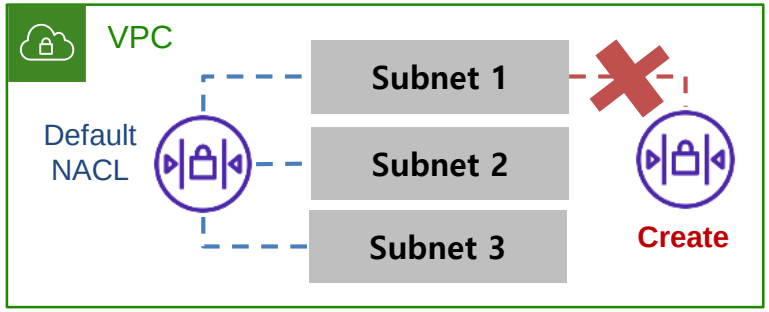


❖ VPC에 서브넷을 만들면 기본 NACL에 자동 연결됨



❖ 새로운 NACL을 만들어 subnet 1에 연결하면,
기존 연결은 자동으로 끊어짐

❖ 서브넷은 단 하나의 NACL만 연결 가능



❖ subnet 1에 연결된 NACL을 해제하면 기본 NACK과 자동으로 연결됨

❖ 서브넷은 반드시 하나의 NACL과 연결 되어야 함

NACL 규칙 형태 - 화이트 리스트 기반 결합 제어

- NACL은 허용과 거부 규칙을 결합한 화이트 리스트 기반 결합 제어 방식
  - 차단 규칙도 적용 가능
- 결합 방식을 사용하므로 **허용/거부** 규칙이 나눠져 있음
- 규칙의 순서가 중요하므로 규칙 번호 순서에 따른 트래픽 접근 제어

인바운드 규칙

규칙번호	유형	프로토콜	포트범위	소스	허용/거부
100	HTTP(80)	TCP(6)	80	160.83.25.60/32	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

- NACL 최하단에는 삭제 불가능한 모든 차단 규칙이 적용되어 있음

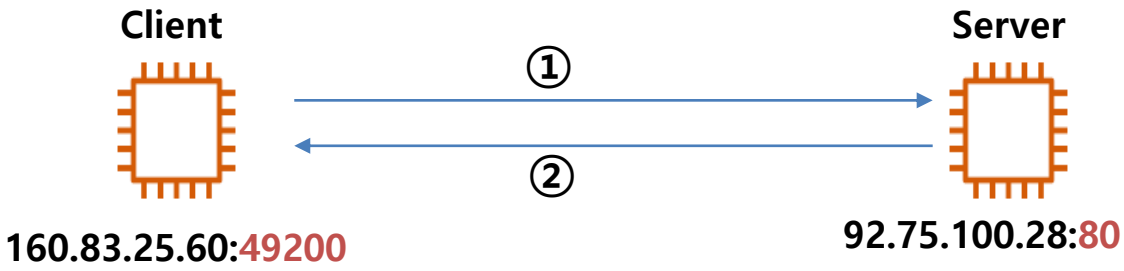
NACL 규칙 형태

인바운드 규칙

규칙번호	유형	프로토콜	포트범위	소스	허용/거부
100	HTTP(80)	TCP(6)	80	160.83.25.60/32	Allow
200	모든 트래픽	모두	모두	0.0.0.0/0	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

- NACL 규칙 적용 순서는 [100 -> 200 -> *] 순서 임
- 모든 거부 규칙 상단에 모두 허용 규칙을 적용하면, 모든 거부 규칙은 무용지물이 되고 블랙리스트 기반 결합방식으로 활용 가능

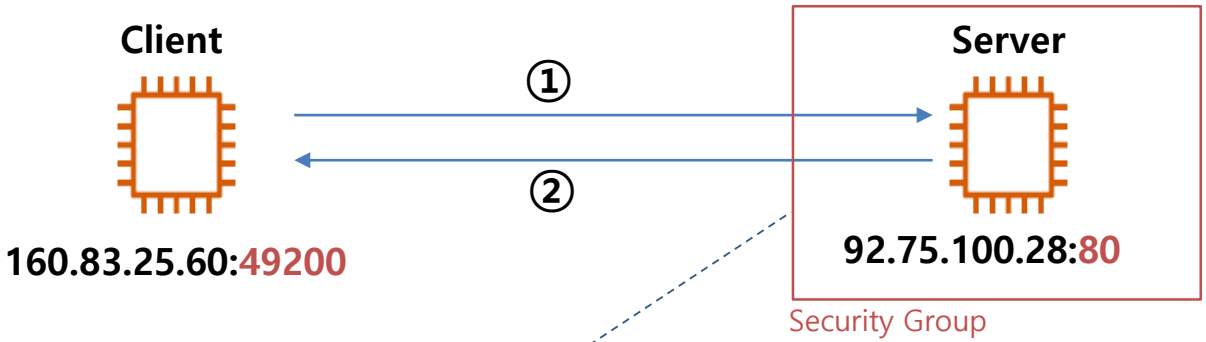
접근제어 방식 비교 : stateful vs. stateledd



① 클라이언트(160.83.25.60)는 운영체제에서 할당받은 포트(49200)로
서버(92.75.100.28)의 포트(80)으로 접속

② 서버는 접속한 포트(80)으로 클라이언트 포트(49200)에 접속하여 새션을 형성하고 데이터 송수신

접근제어 방식 비교 : stateful vs. stateless



Inbound

Source	Protocol	Port range
160.83.25.60	TCP	80

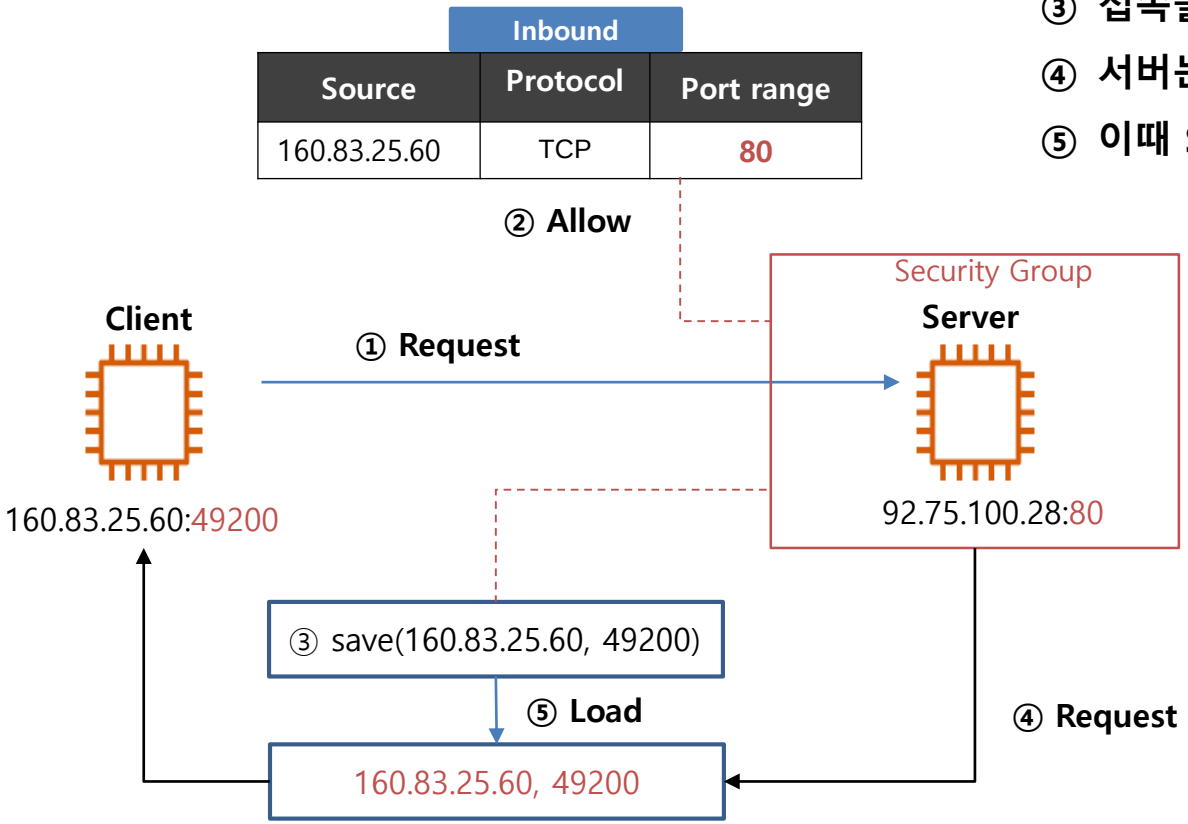
Outbound

Destination	Protocol	Port range
160.83.25.60	TCP	49200

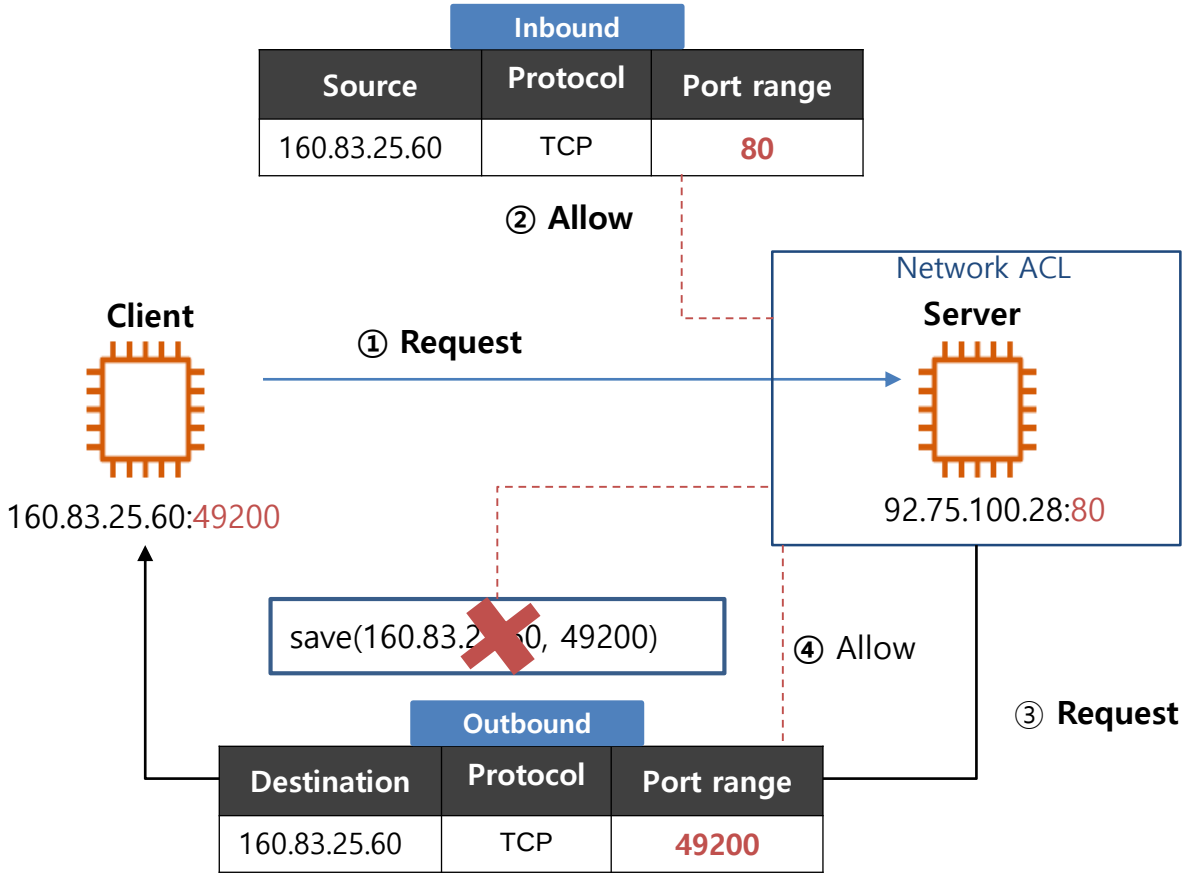
- 클라이언트가 운영체제에서 할당받은 포트(49200)는 동적 포트(Dynamic Port) 영역
- 동적 포트(Dynamic Port) : 49152 ~16384
- 클라언트 포트 번호가 범위 내에서 변하므로 규칙 설정이 어려움

보안 그룹(SG): stateful

① 클라이언트가 서버에 데이터 요청
② 서버에 연결된 SG가 요청 트래픽을 확인해 허용 여부를 결정
③ 접속을 요청한 클라이언트의 IP와 포트를 저장
④ 서버는 다시 클라이언트에 응답
⑤ 이때 SG는 (3)에 저장한 IP와 포트로 접속 허용



네트워크 ACL : stateless



❖ 네트워크 ACL에서는 Inbound, Outbound 규칙 모두 저장되어 있어야 함

NACL 규칙 – Outbound 트래픽 허용 규칙

아웃바운드 규칙

규칙번호	유형	프로토콜	포트범위	소스	허용/거부
100	사용자 지정 TCP	49152-65535	80	160.83.25.60/32	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

- 운영체제 종류마다 동적 포트 범위가 다름
- 모든 포트 허용을 권장

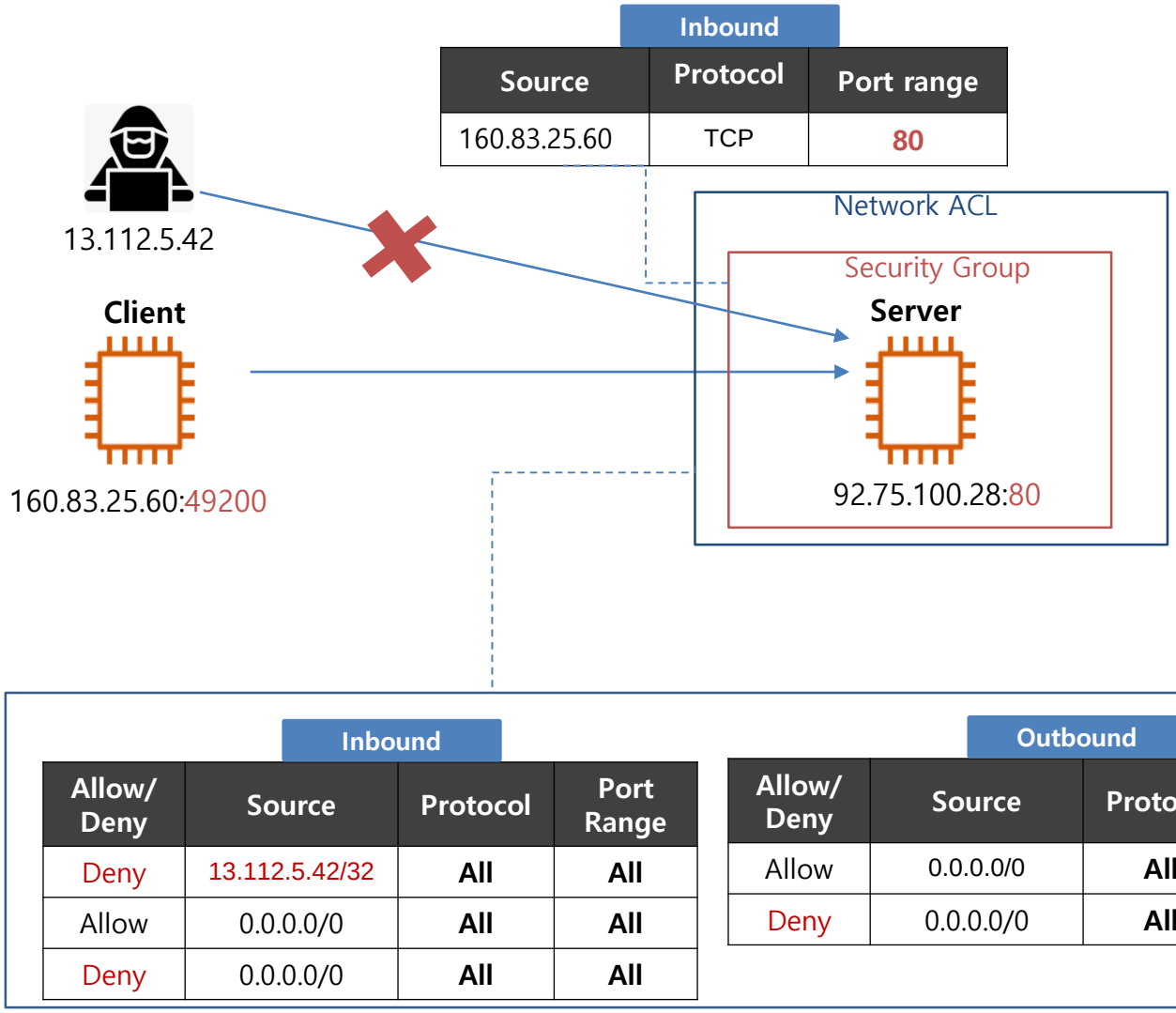
NACL 규칙 – Outbound 트래픽 허용 규칙

아웃바운드 규칙 – Whitelist 방식 지정 예

규칙번호	유형	프로토콜	포트범위	소스	허용/거부
100	사용자 지정 TCP	49152-65535	80	160.83.25.60/32	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

?

- Inbound 규칙에 허용한 IP를 Outbound 규칙에도 적용해야 함
- 이때 클라이언트의 동적 포트를 모두 허용해야 함
- SG에 신규 허용 규칙을 등록할 때마다 NACL에도 함께 등록 해야함



[NACL – 블랙리스트 기반 관리]

❖ 서브넷의 인스턴스가 공통으로 차단할 트래픽은 NACL에 적용

❖ 그 밖의 모든 트래픽은 NACL에서 허용

[SG – 화이트리스트 기반 제어]

❖ 개별 인스턴스에 대한 접근 제어는 SG로 관리

Inbound

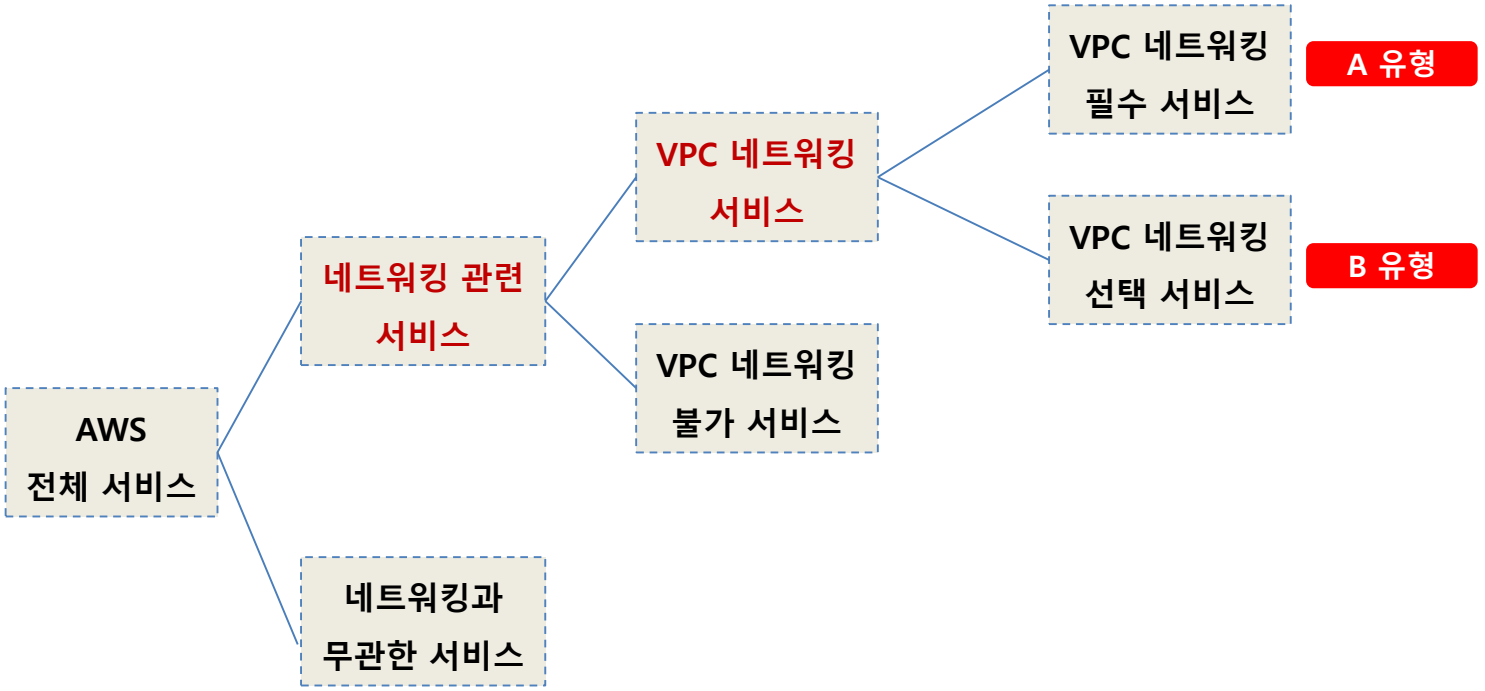
Allow/ Deny	Source	Protocol	Port Range
Deny	13.112.5.42/32	All	All
Allow	0.0.0.0/0	All	All
Deny	0.0.0.0/0	All	All

Outbound

Allow/ Deny	Source	Protocol	Port Range
Allow	0.0.0.0/0	All	All
Deny	0.0.0.0/0	All	All

VPC 네트워킹

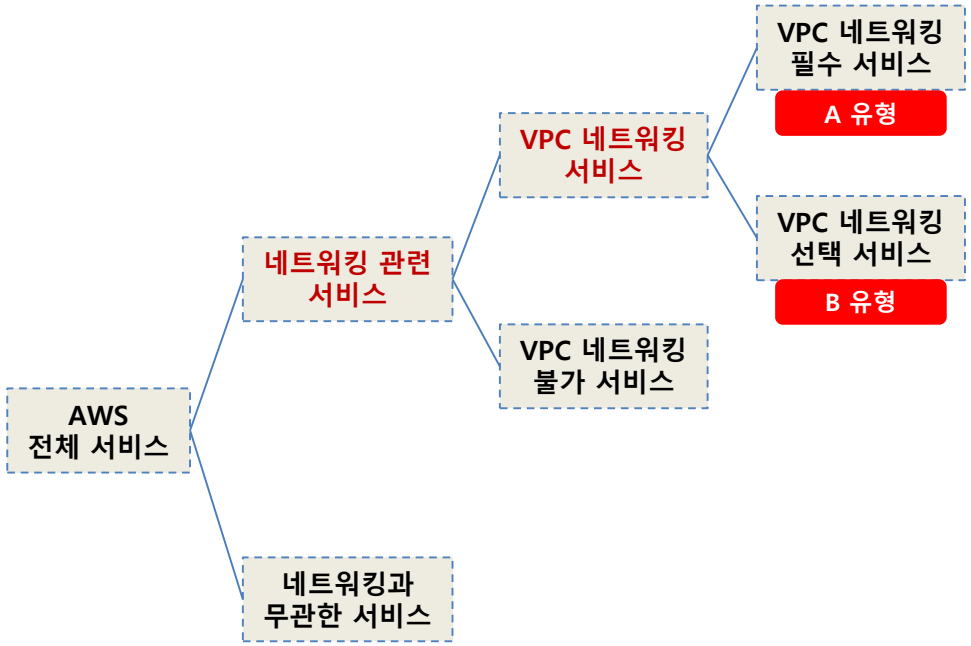
- 온프레미스와 최대한 유사하면서도 쉽게 관리할 수 있는 네트워크 플랫폼
- 계정 전용 가상 클라우드 공간



VPC 네트워킹

❖ 온프레미스와 최대한 유사하면서도 쉽게 관리할 수 있는 네트워크 플랫폼

❖ 계정 전용 가상 클라우드 공간



[VPC 네트워킹 필수 서비스]

❖ VPC상에 존재하는 모든 서비스

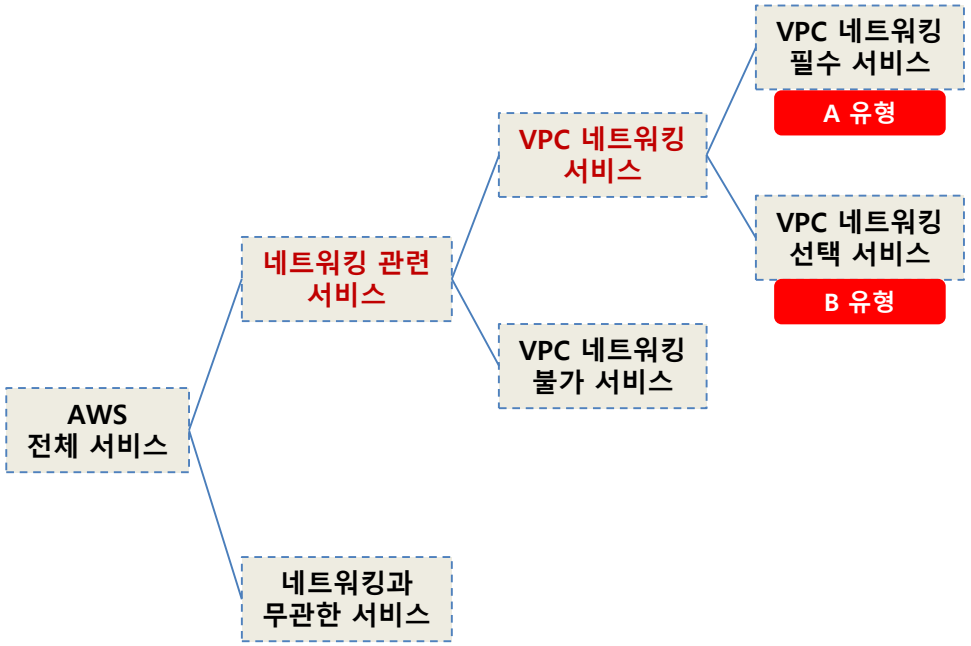
❖ 인스턴스나 RDS 처럼 가상머신에 ENI를 연결해서 통신하는 서비스

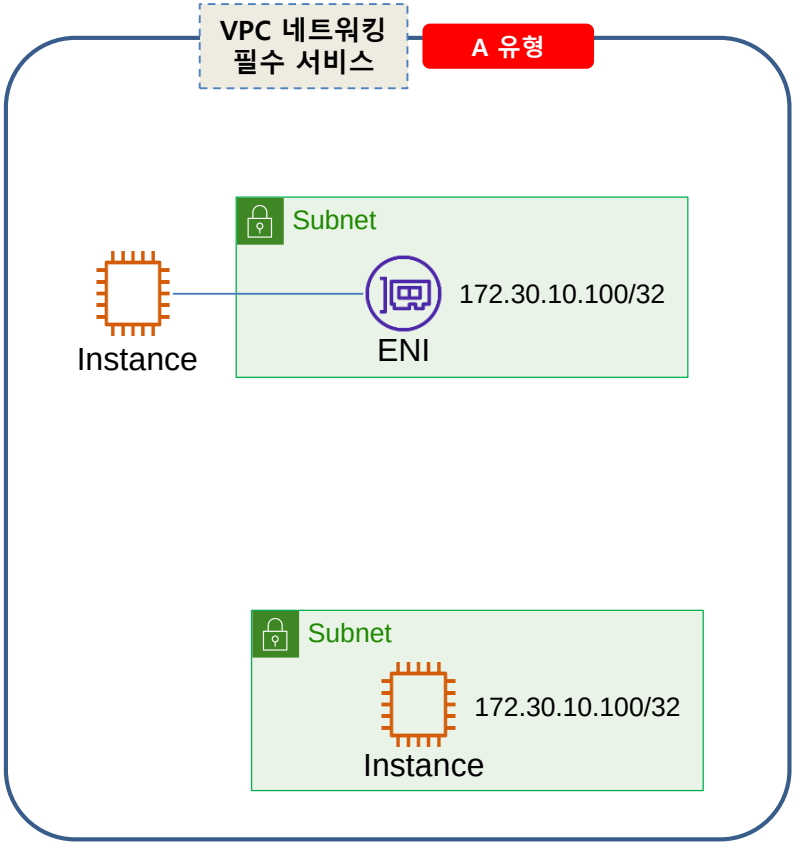
❖ VPC 상에 존재하는 모든 서비스는 ENI가 반드시 연결되어 있어야 함

❖ 인스턴스가 서브넷 공간에 놓여 있는 모습 자체가 ENI 존재를 표현

VPC 네트워킹

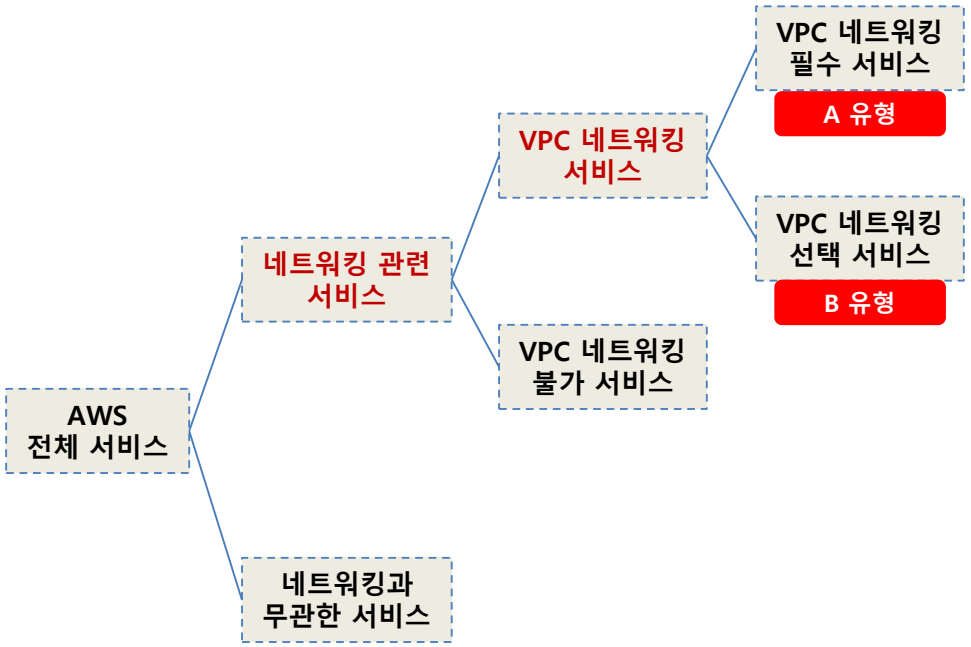
- ❖ 온프레미스와 최대한 유사하면서도 쉽게 관리할 수 있는 네트워크 플랫폼
- ❖ 계정 전용 가상 클라우드 공간

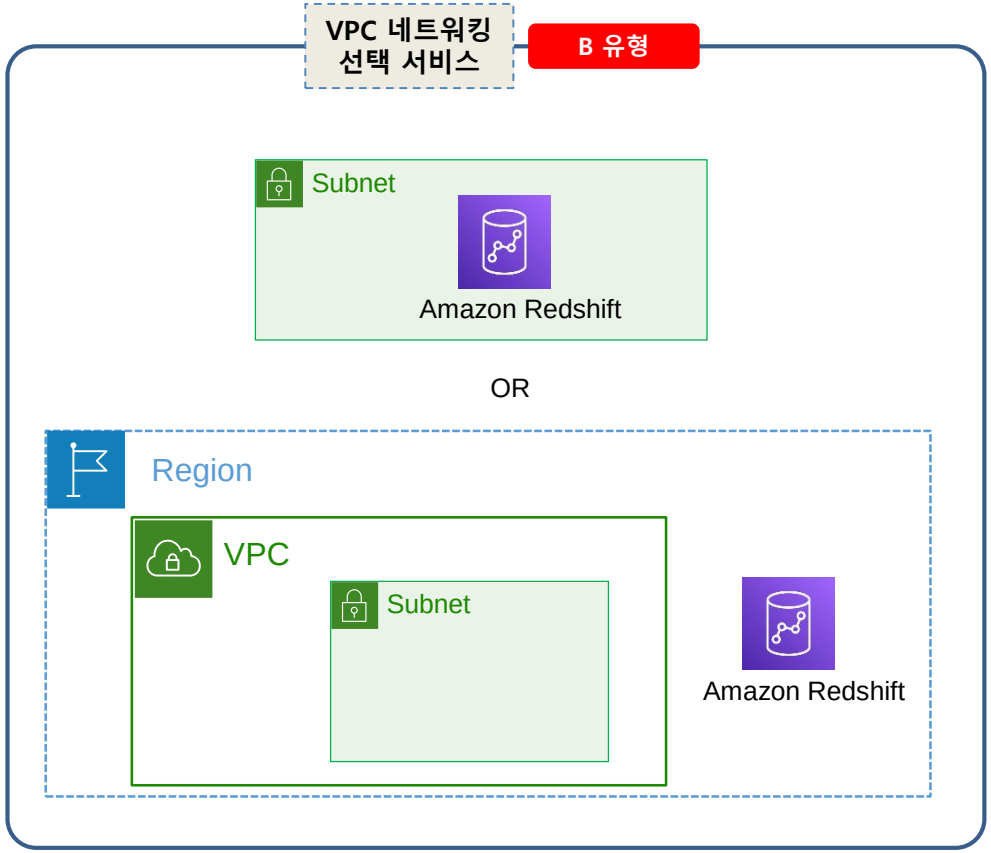




VPC 네트워킹

- ❖ 온프레미스와 최대한 유사하면서도 쉽게 관리할 수 있는 네트워크 플랫폼
- ❖ 계정 전용 가상 클라우드 공간

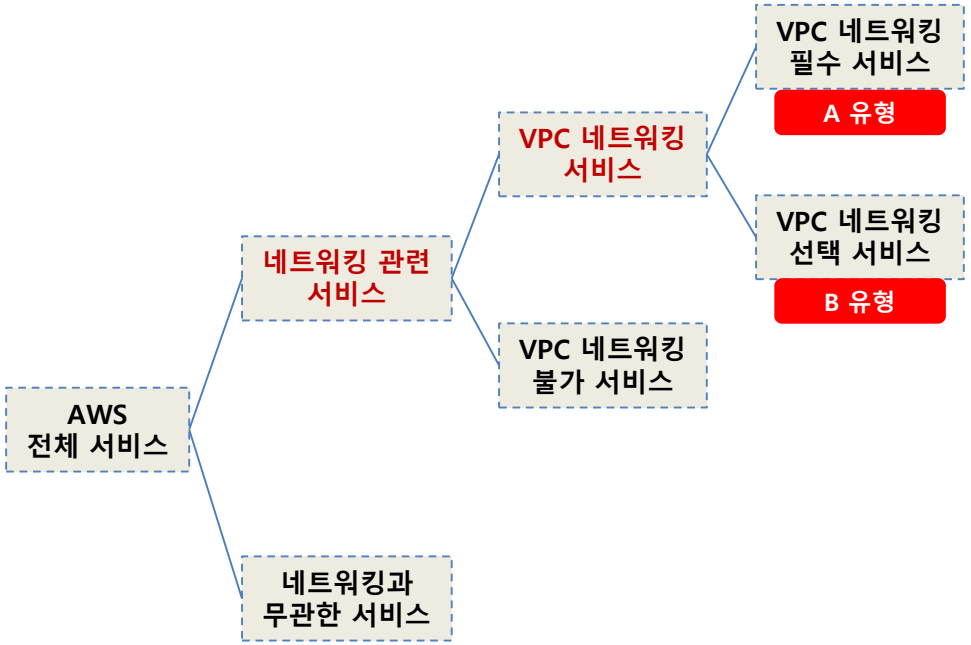




VPC 네트워킹

❖ 온프레미스와 최대한 유사하면서도 쉽게 관리할 수 있는 네트워크 플랫폼

❖ 계정 전용 가상 클라우드 공간



[VPC 네트워킹 기본 규칙]

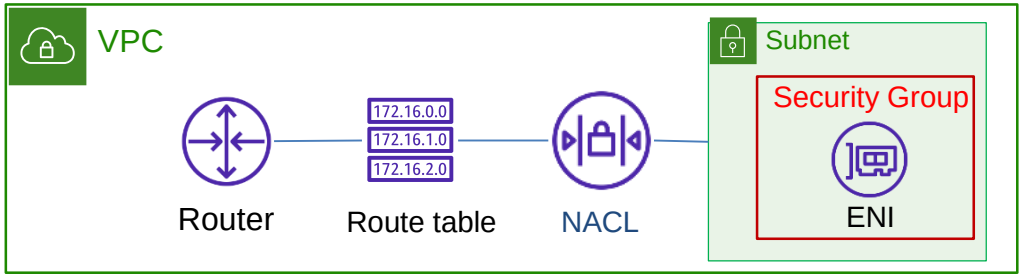
❖ 보안그룹(SG)을 반드시 수반하는 **네트워크 인터페이스**가 있다

- 보안 그룹에 따라 컴퓨팅 ENI와 라우팅 ENI로 분류

❖ **서브넷**이 있어야 그 안에 **네트워크 인터페이스**를 생성 가능

❖ VPC 생성되어야 서브넷을 생성 가능

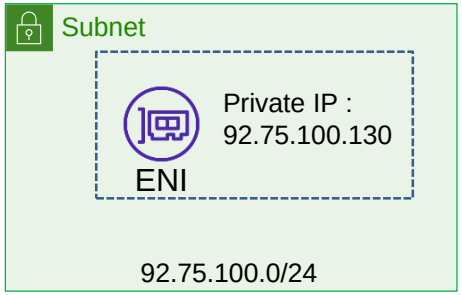
❖ 서브넷에는 무조건 **라우팅 테이블**과 **네트워크 ACL**이 연결됨



탄력적 네트워크 인터페이스 (ENI : Elastic network Interface)

- 온프레미스의 NIC(Network Interface Card)에 상응하는 가상 장치
- VPC의 네트워킹은 반드시 ENI를 기반으로 함

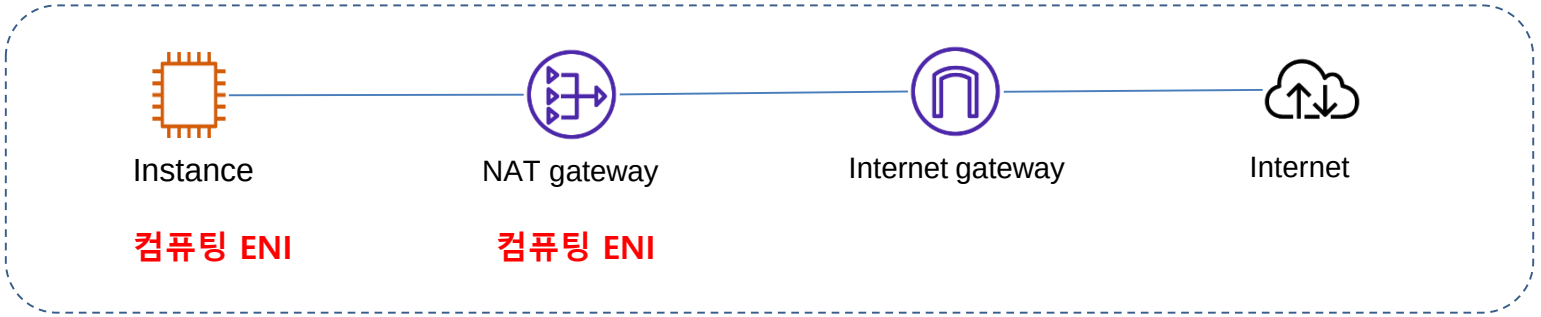
- ENI는 서브넷에 생성하므로, 최소 1개의 Private IP 주소 소유
- 서브넷 CIDR 블록 범위 내에서 Private IP를 직접 지정하거나 자동 할당이 가능
- ENI는 VPC 서비스에 연결된 상태로 존재해야 함



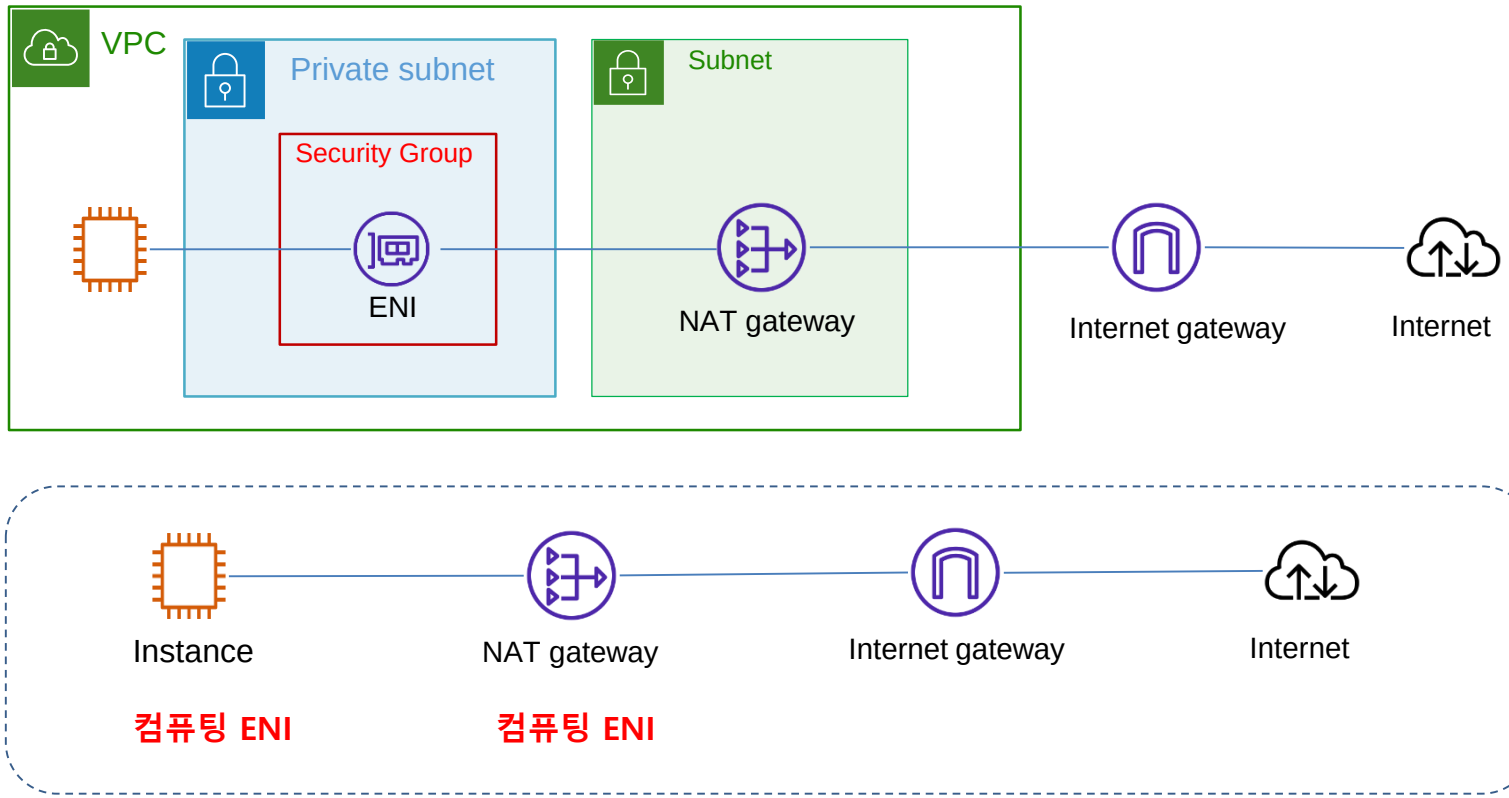
탄력적 네트워크 인터페이스 (ENI) 유형

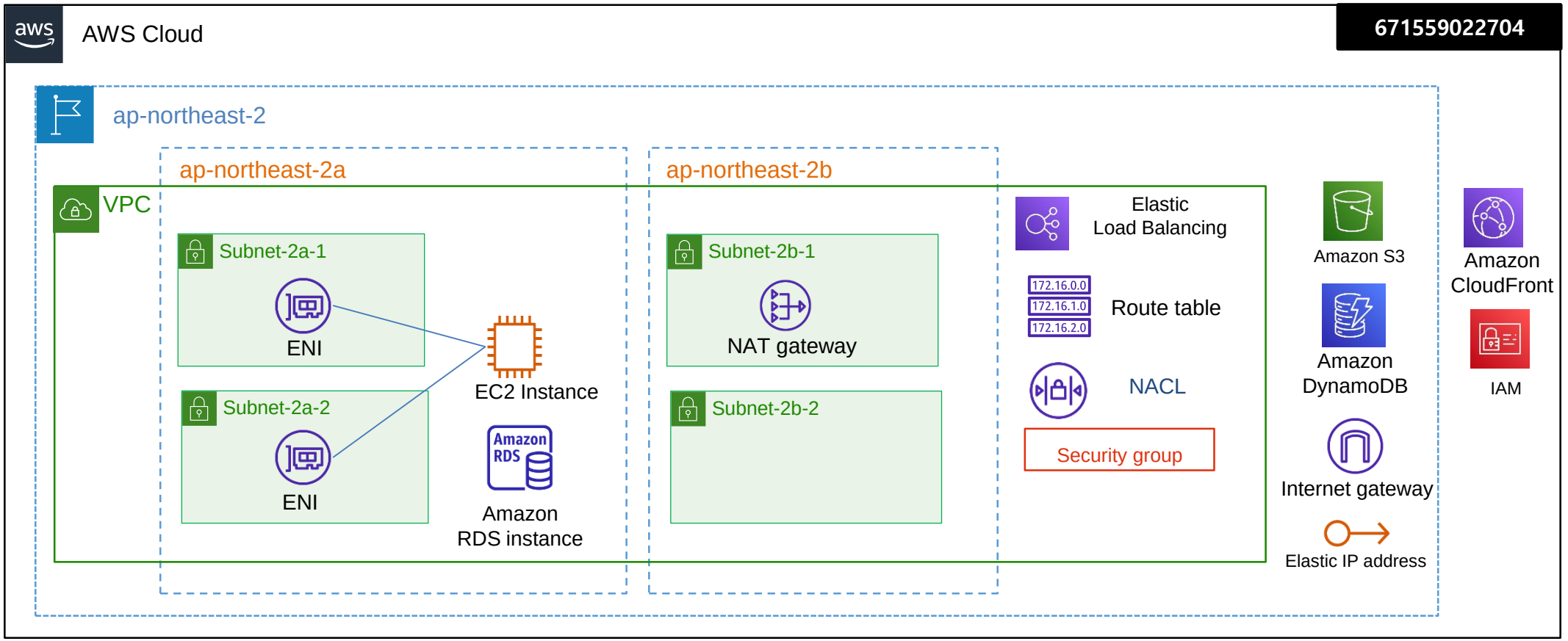
❖ ENI에 연결된 서비스 종류

- 컴퓨팅 ENI : 데이터 처리가 주 역할인 서비스에 연결된 ENI
  - instance, Lambda, EFS
  - 애플리케이션 실행, 컴퓨팅, 스토리지 등 데이터 가공과 저장이 주 역할
- 라우팅 ENI : 트래픽 전송이 주 역할인 서비스에 연결된 ENI
  - NAT Gateway, 전송 게이트웨이와 같은 네트워크 디바이스
  - 트래픽 전송이 주 역할



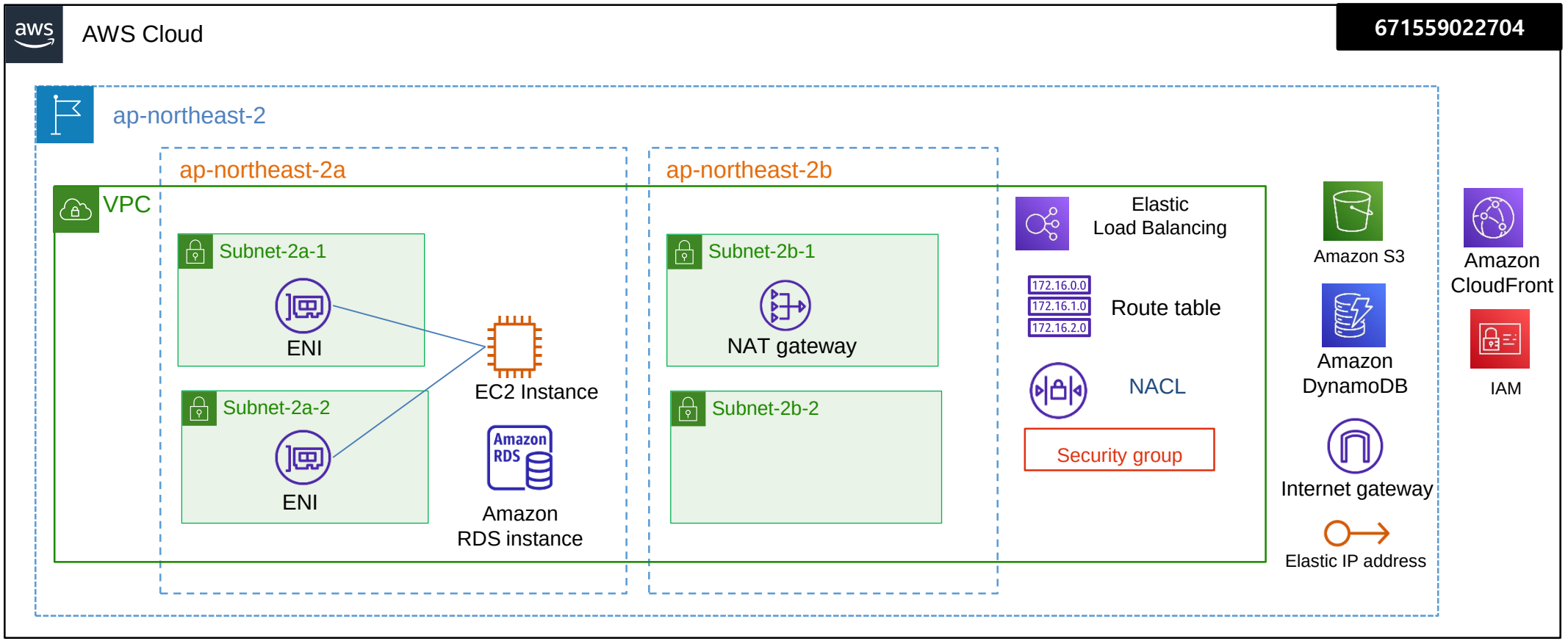
탄력적 네트워크 인터페이스 (ENI) 유형



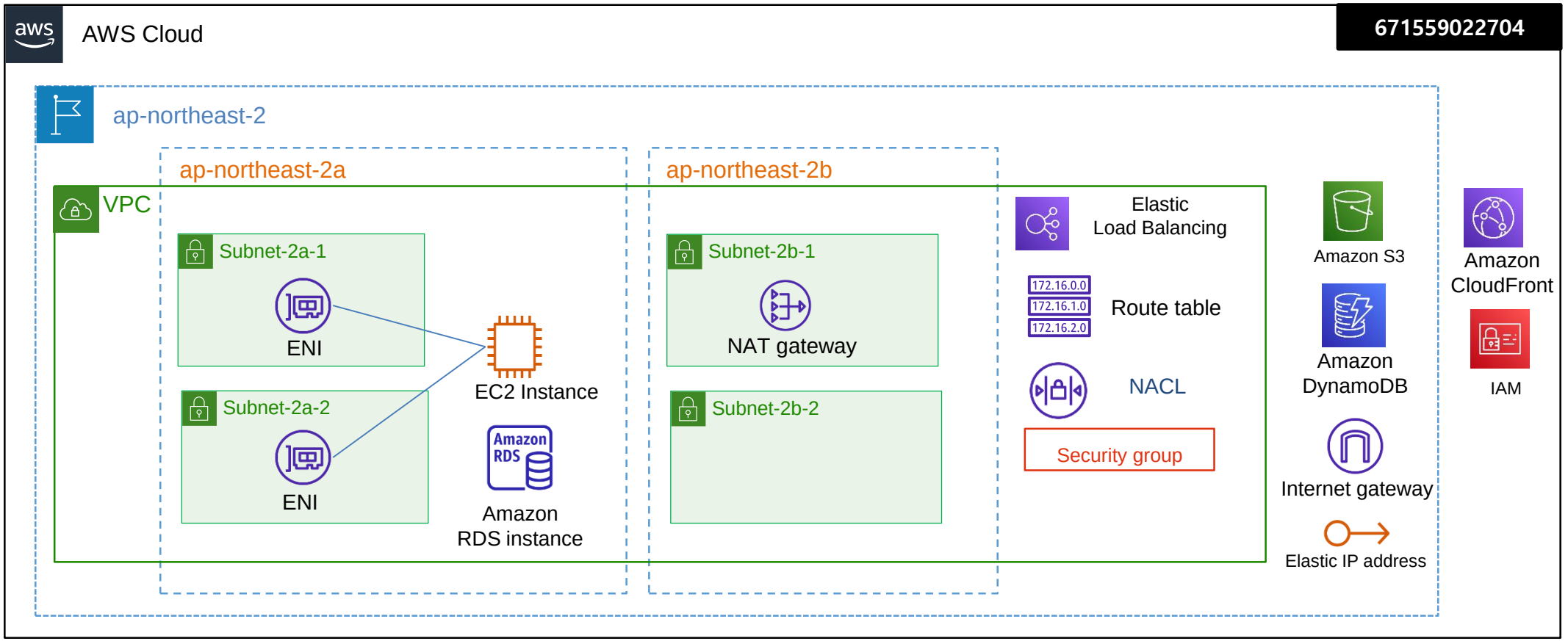


구성요소	역할	Parent	연결 대상	비고
ENI(Elastic Network Interface)	컴퓨팅(트래픽 전달)	Subnet	인스턴스 또는 VPC 서비스	
EIP(Elastic IP Address)	컴퓨팅(트래픽 전달)	Region	[기본, 보조] Private IP	ENI가 장착된 Private IP에 연결됨
인스턴스	컴퓨팅(트래픽 생성)	AZ, VPC	-	

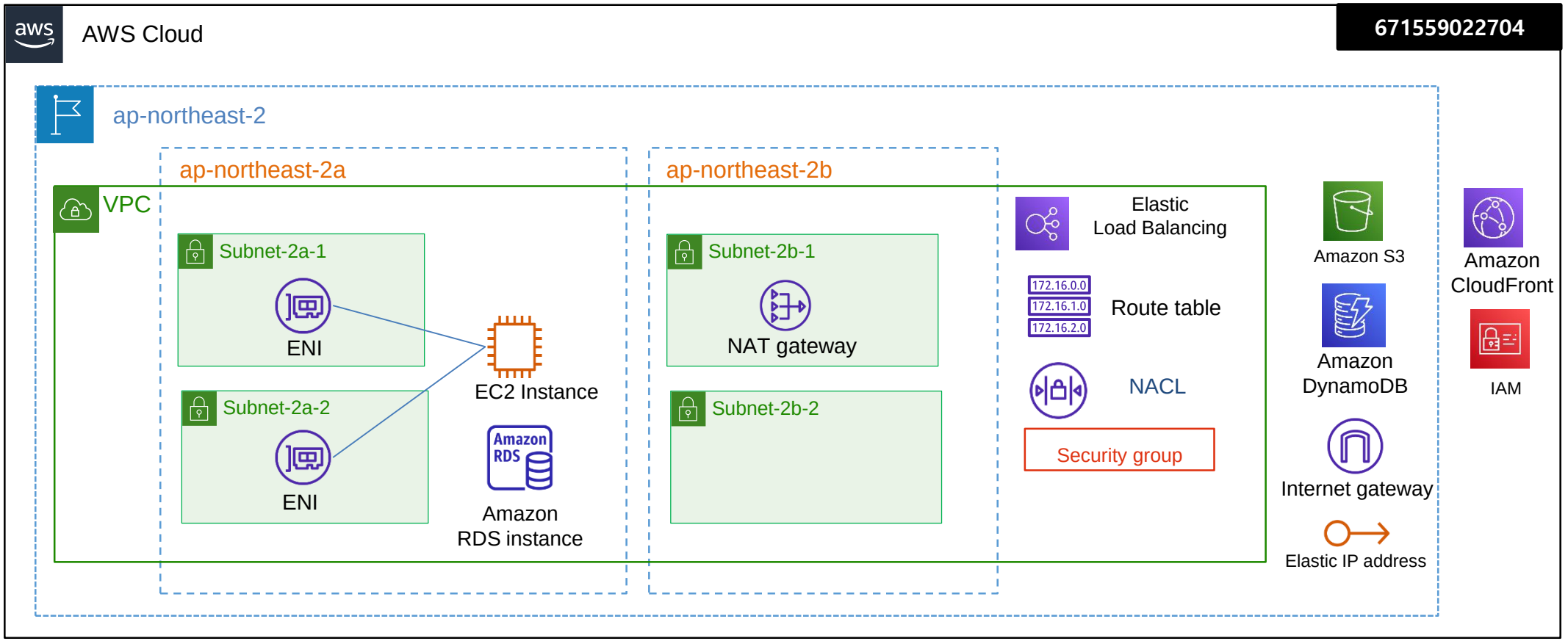
ENI



구성요소	역할	Parent	연결 대상	비고
NAT Gateway	연결(경로 제어)	Subnet	-	라우팅 ENI 사용 서비스로 SG사용 안함
NACL	연결(접근 제어)	VPC	subnet	
보안그룹(SG)	연결(접근 제어)	VPC	ENI	



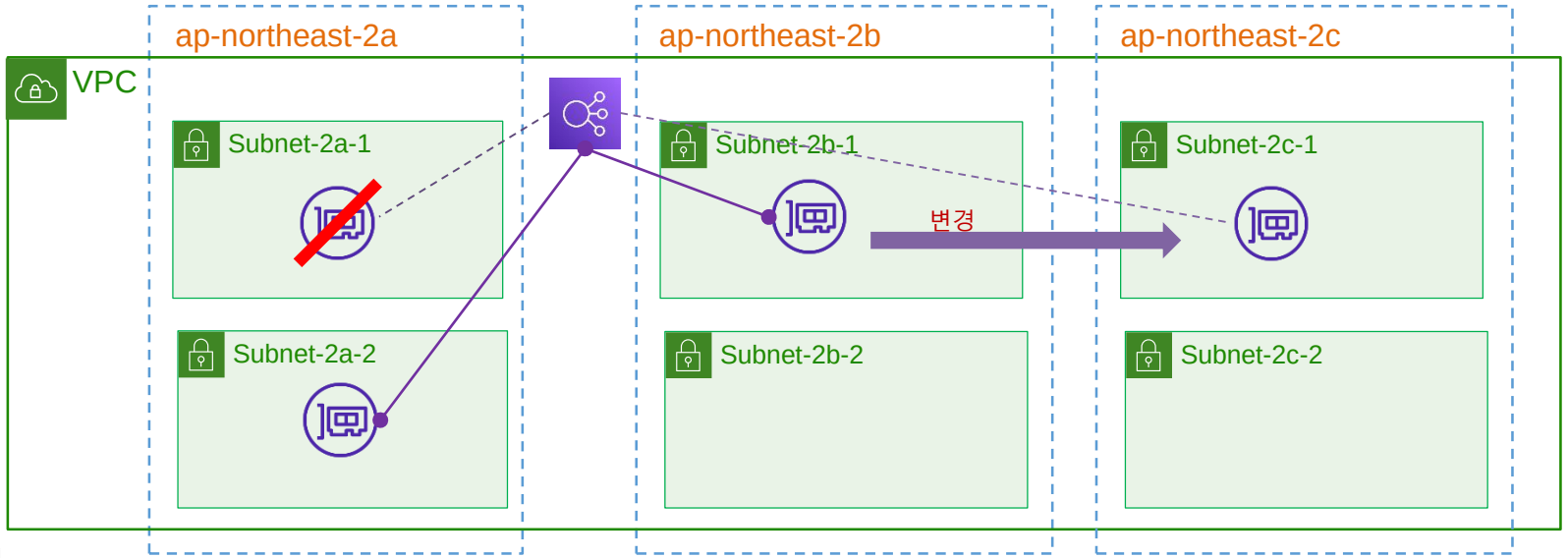
구성요소	역할	Parent	연결 대상	비고
라우팅 테이블	연결(경로 제어)	VPC	subnet	라우팅 ENI 사용 서비스로 SG사용 안함
인터넷 게이트웨이	연결(경로 제어)	Region	VPC	
보안그룹(SG)	연결(접근 제어)	VPC	ENI	



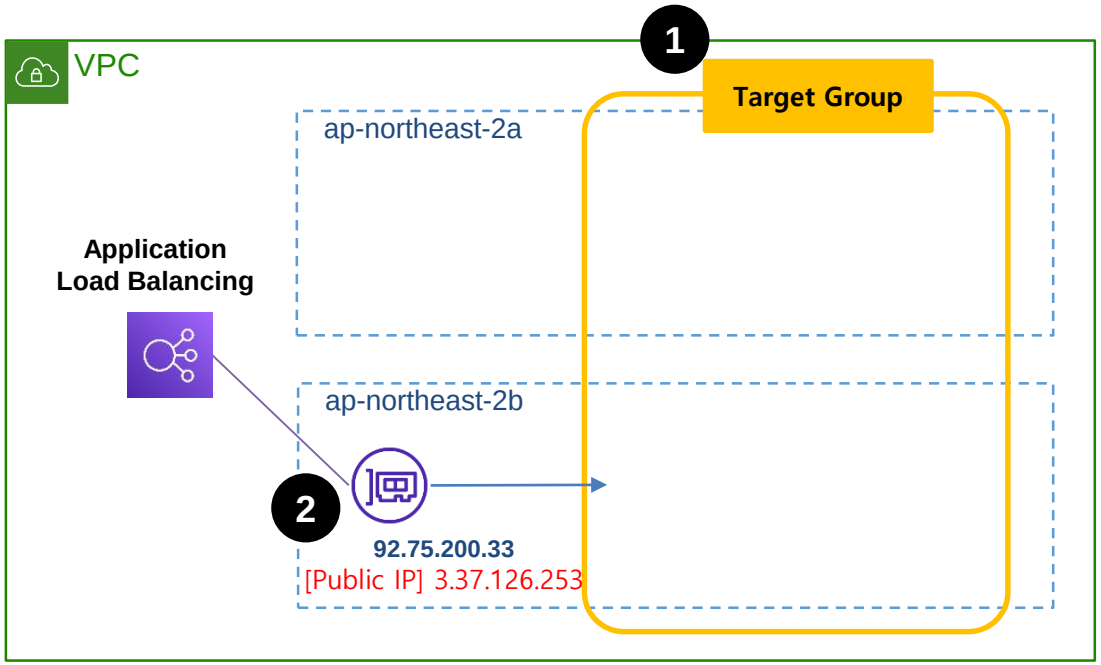
구성요소	역할	Parent	연결 대상	비고
ELB(ALB)	연결(분산 제어)	VPC	-	
ELB(NLB)	연결(분산 제어)	Region	Endpoint Service	ENI 연결 가능(고정 node)

ALB와 NLB

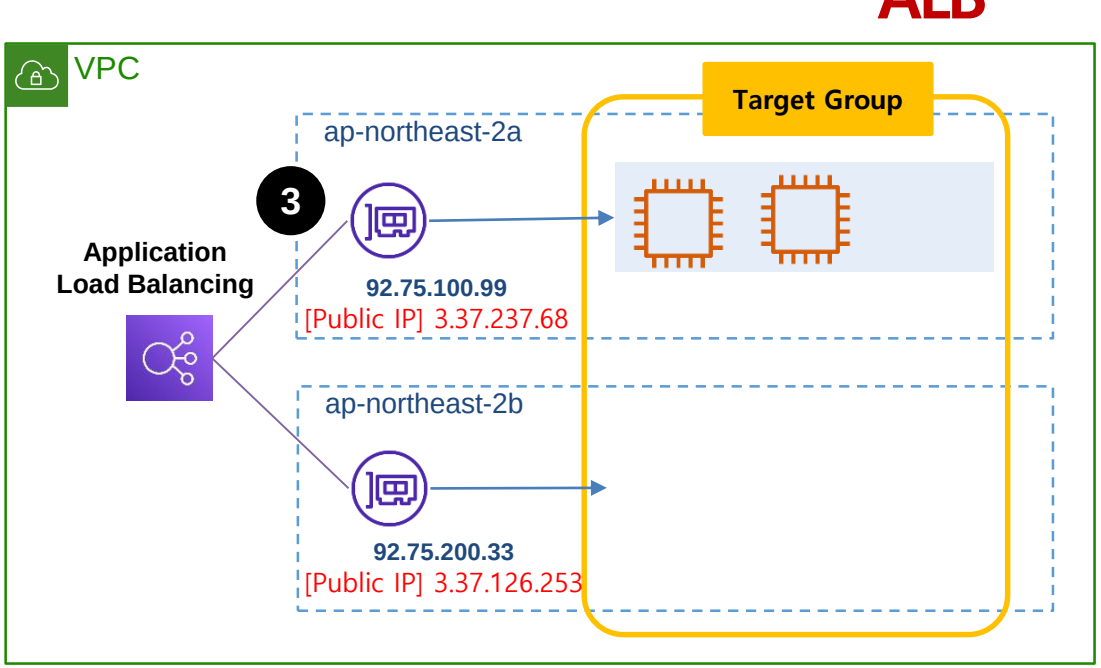
Domain Name	ALB	NLB	CLB	GWLB
가용영역 선택	최소 2개	최소 1개		
가용영역별 선택 가능한 Subnet 수	1개 (가용 영역별 1개의 노드만 생성 가능)			
가용영역 범위	추가, 변경, 삭제 가능	추가만 가능	추가, 변경, 삭제 가능	변경 불가
노드에 EIP 연결 가능	불가	가능	불가	불가



ALB와 NLB



ALB



1
- ALB 생성시 2개의 가용영역을 선택(2a, 2b)
- ALB에 대상이 없는 대상그룹(target group)을 연결

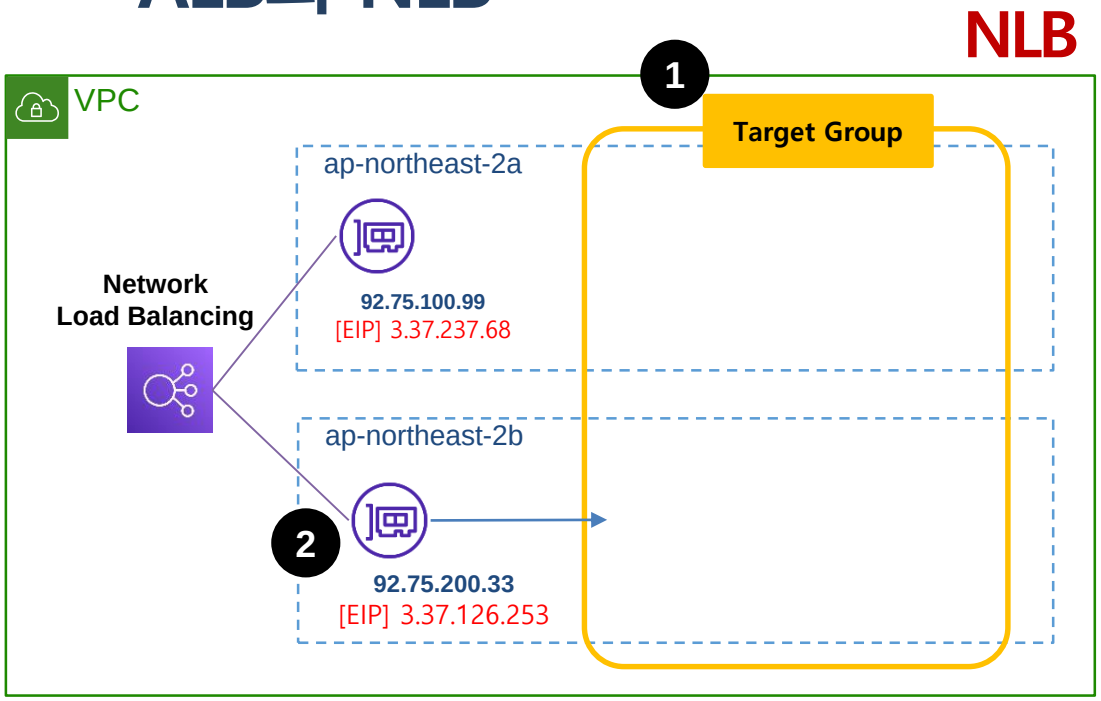
2
- ALB는 노드를 모든 가용영역에 생성하지 않고, 랜덤하게 한곳에만 생성 (예: 가용영역 2b에 생성)

3
- 로드밸런싱 대상 인스턴스가 가용영역 2a에 등록되면
- 가용영역 2a에 노드를 추가 생성함
- 기존 대상 인스탄스가 중지되면, 노드를 제거하기도 함

❖ ALB는 노드를 가변 적으로 운영함

ALB는 노드에 고정 public IP(EIP)를 할당하지 않고 자동할당 public IP를 할당함

ALB와 NLB



1 • NLB 생성시 2개의 가용영역을 선택(2a, 2b)
• ALB에 대상이 없는 대상그룹(target group)을 연결
2 • NLB는 로드밸런싱 대상의 유무와 상관없이 모든 가용영역에 노드를 생성함

NLB는 노드에 고정 public IP(EIP)를 할당함