AWS 아키텍처 설계

Chapter 05. AWS Network 1

설계 시나리오

AWS를 사용하는 수많은 다른 고객들의 리소스와 조직의 리소스를 격리할 수 있는 논리적인 네트워크 환경이 필요하다.

AWS 서비스 중 이러한 요구 사항을 충족할 수 있는 서비스는 무엇이 있을까?

VPC (Virtual Private Cloud)

01

Amazon VPC(Virtual Private Cloud)

Amazon VPC

- 사용자가 정의하는 논리적으로 격리된 가상 네트워크
- AWS 리소스에 대한 논리적인 격리 제공 (회사/조직/부서 등)
- AWS 리소스에 대한 Access Control 및 보안 구성 제공

Amazon VPC

Amazon VPC

- AWS 계정 전용 가상 네트워크 환경.
- VPC에 특정 CIDR 범위를 지정. (IPv4/IPv6)
- VPC에 접근하는 트래픽에 대해 Inbound/Outbound Access 규칙을 적용.

Amazon VPC

VPC 배포 범위

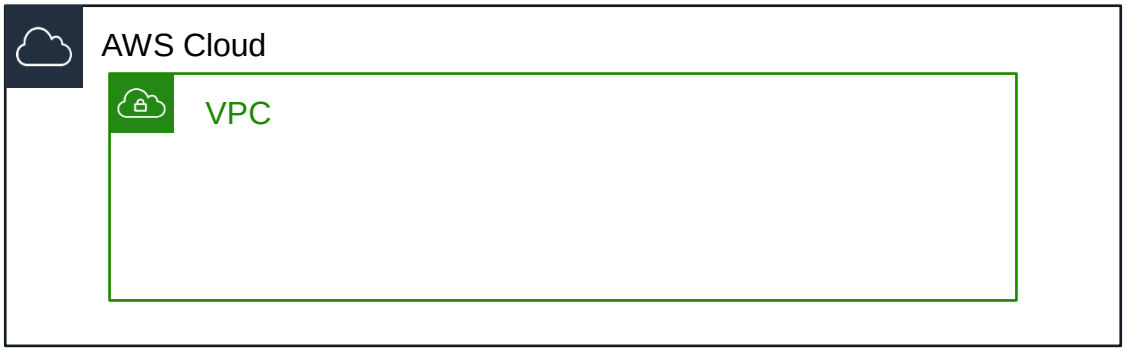
- VPC는 리전을 선택하여 배포.

  해당 리전의 모든 가용 영역을 선택하여 리소스를 배치할 수 있다.

하나의 VPC를 사용하는 경우

- **하나의 VPC만 사용되는 경우는 많지 않다.**

  - 소규모 단일 애플리케이션 / 간단한 자격 증명 관리 / 고성능 컴퓨팅(HPC)

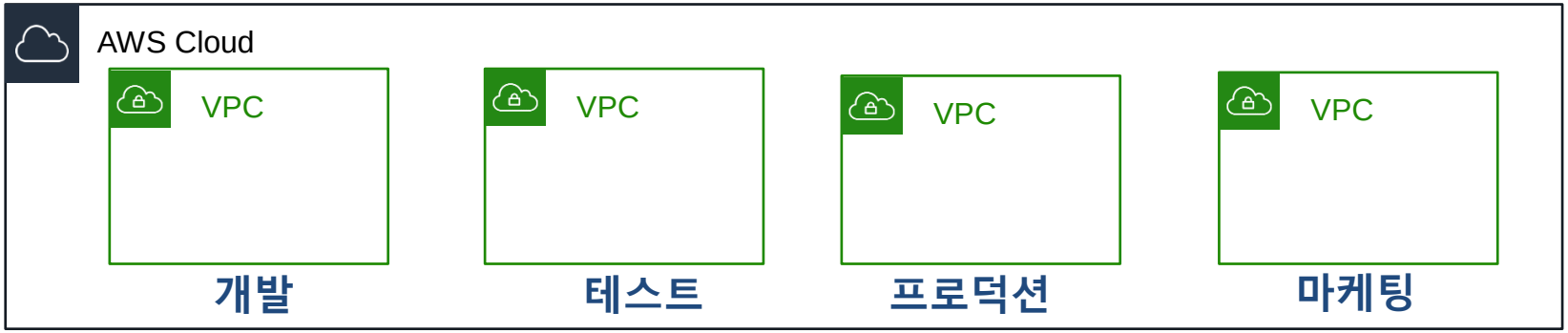


- **일반적인 실제 운영 환경의 경우 다음과 같은 방법으로 다수의 VPC를 사용.**

Multi VPC 및 Multi Account

Multi VPC 패턴

- **하나의 AWS 계정 안에서 다수의 VPC를 생성하는 패턴.**
  - 하나의 팀에서 여러 환경을 관리하는 경우.
- **계정마다 리전당 VPC는 5개로 제한. (Soft limit)**



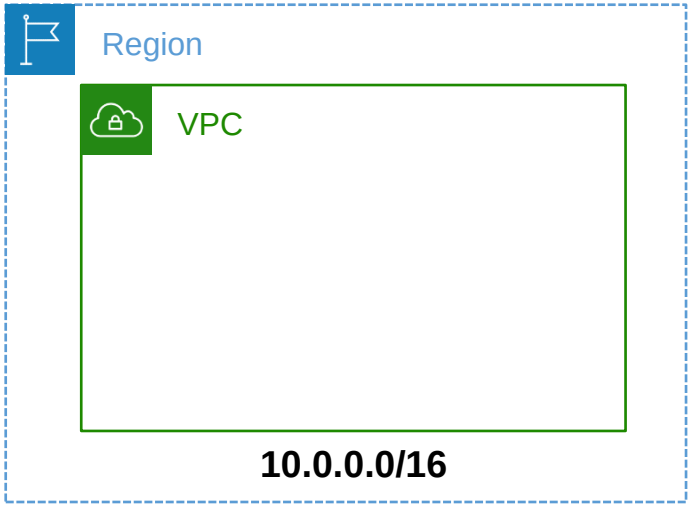
- **각 담당자가 동일 AWS 계정을 사용할 경우 실수로 다른 환경 리소스를 변경하거나 보안적인 문제가 발생할 위험이 있다.**
- **보안 규정상 관리 편의성보다 완벽한 워크로드 격리를 요구 받을 수 있다.**

Multi Account 패턴

- **다수의 AWS 계정을 사용하는 패턴.**
  - 각 팀에서 **독립된 환경**을 관리하는 경우.
- **담당자는 자신이 관리하는 AWS 리소스만 표시.**
  - 보안 문제와 관리적인 실수를 줄일 수 있다.
- **다른 계정 자원에 접근을 해야하는 경우 교차 계정 액세스를 사용.**

VPC IP 주소

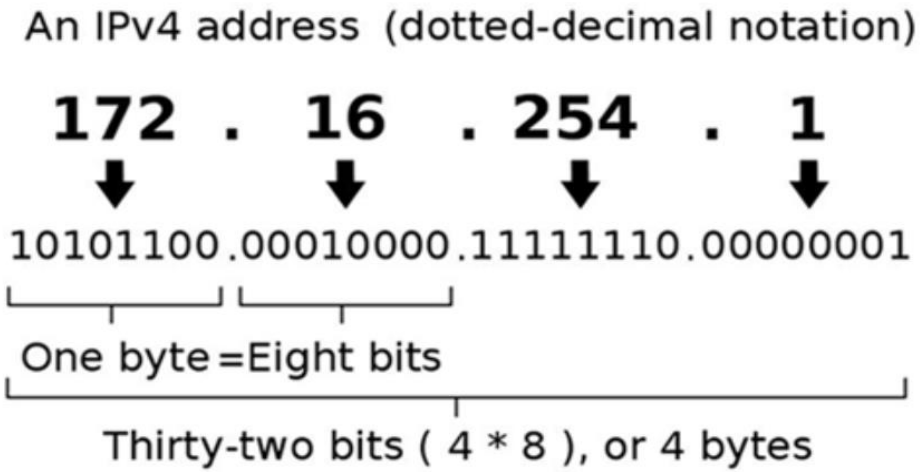
- 각 VPC에 **사설 IP 대역**을 할당.
- VPC 내부에 배치되는 AWS 리소스들은 해당 사설 IP 주소 대역을 사용.
- **BYOIP**(Bring Your Own IP) 지원.



- **CIDR**(Classless Inter-Domain Routing) 표기법 사용.

IPv4 Addressing

- IPv4 주소 구조



Internet Protocol v4 Address

- 사용 가능한 IPv4 주소는?

  => 2^32 = 4,294,967,296개

  00000000.00000000.00000000.00000000 (0.0.0.0)

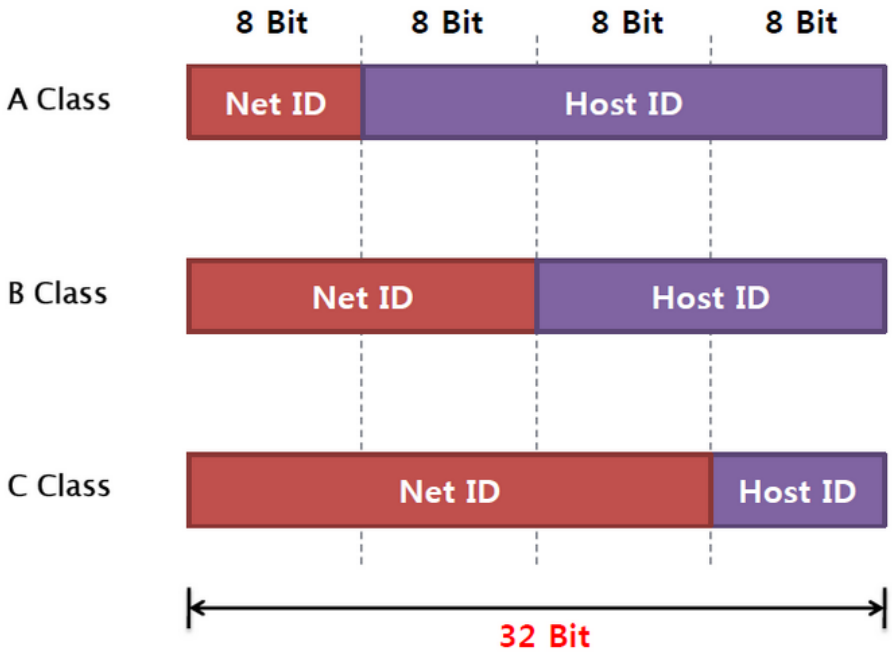
  ~

  11111111.11111111.11111111.11111111(255.255.255.255)

IPv4 Addressing

- **Classful**

Class	HOB	NET ID Bits	Host ID Bits	No of Networks	Host Per Network	Start Address	End Address
Class A	0	8	24	2^7=128	2^{24}=16,777,216	0.0.0.0	127.255.255.255
Class B	10	16	16	2^{14}=16,384	2^{16}=65,536	128.0.0.0	191.255.255.255
Class C	110	24	8	2^{21}=2,097,152	2^8=256	192.0.0.0	223.255.255.255



IPv4 Addressing

- **CIDR(Classless Inter Domain Routing)**

CIDR	IP 주소
/16	65,536
/17	32,768
/18	16,384
/19	8,192
/20	4,096
/21	2,048
/22	1,024
/23	512
/24	254
….	….
/28	16

<Ex>

10.0.0.0/16 => 10.0.0.0 ~ 10.0.255.255

10.0.0.0/24 => 10.0.0.0 ~ 10.0.0.255

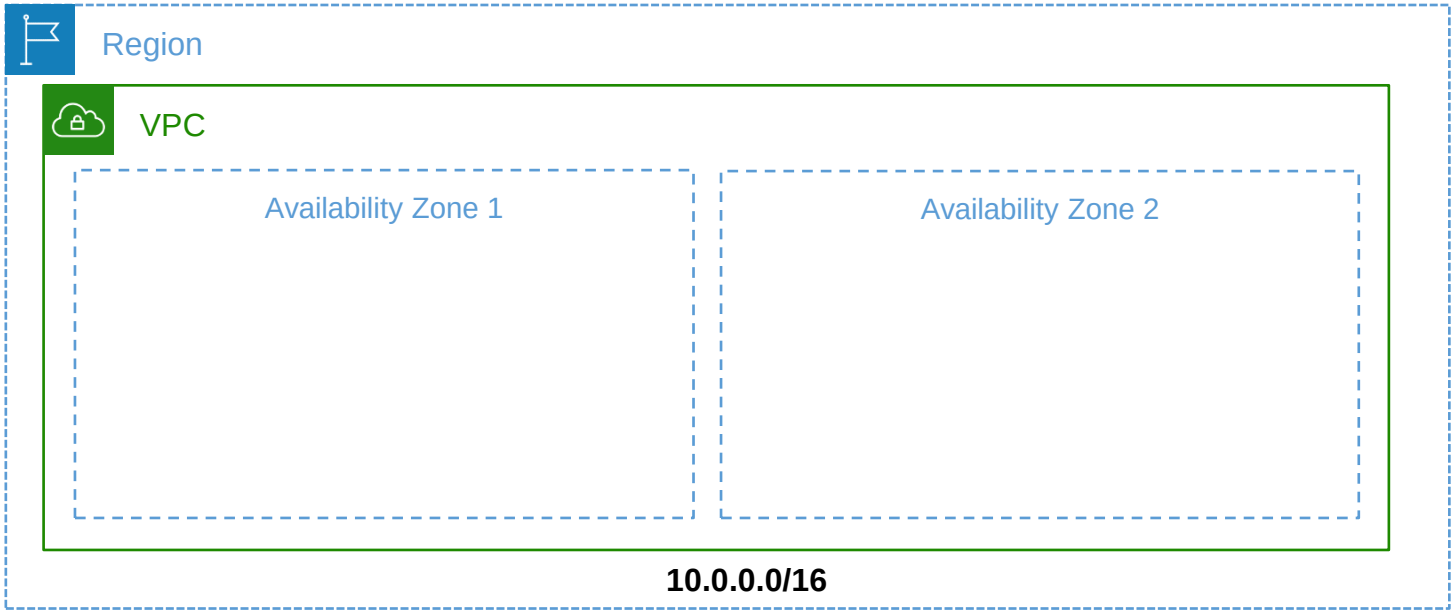
10.0.1.100/32 => 10.0.1.100

0.0.0.0/0 => 0.0.0.0 ~ 255.255.255.255

10.0.2.0/23 => ???

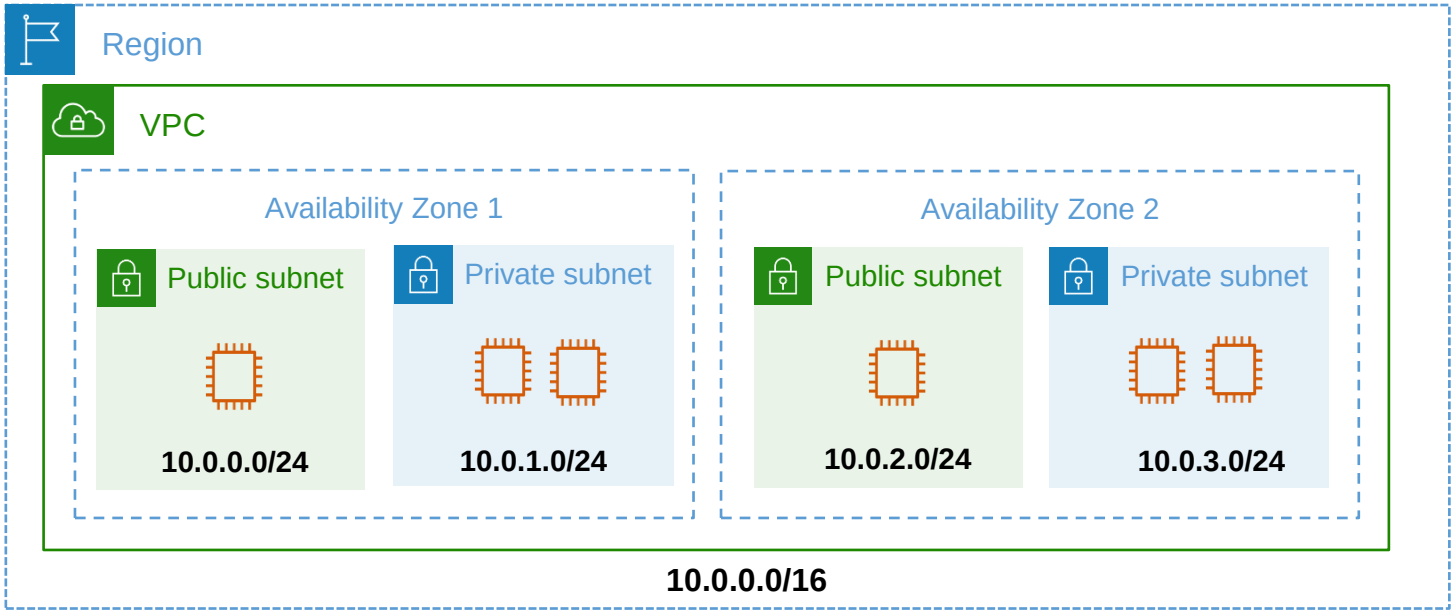
Subnet

- VPC를 Subnet으로 분할하여 사용.
- Subnet은 하나의 가용 영역 안에 위치.
- 하나의 가용 영역 안에 다수의 Subnet이 포함될 수 있음.
- Subnet마다 5개의 IP 주소는 예약되어 있음.



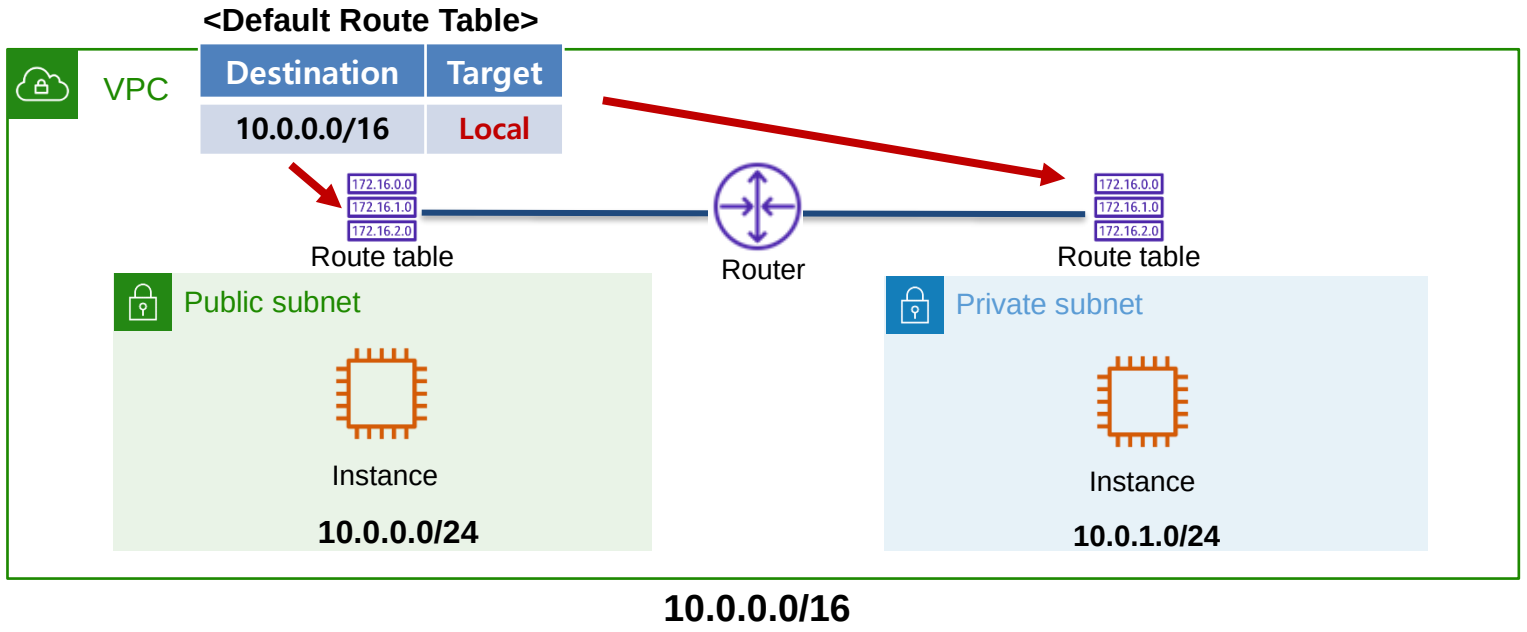
Subnet

- VPC를 Subnet으로 분할하여 사용.
- Subnet은 하나의 가용 영역 안에 위치.
- 하나의 가용 영역 안에 다수의 Subnet이 포함될 수 있음.
- Subnet마다 5개의 IP 주소는 예약되어 있음.



Route Table

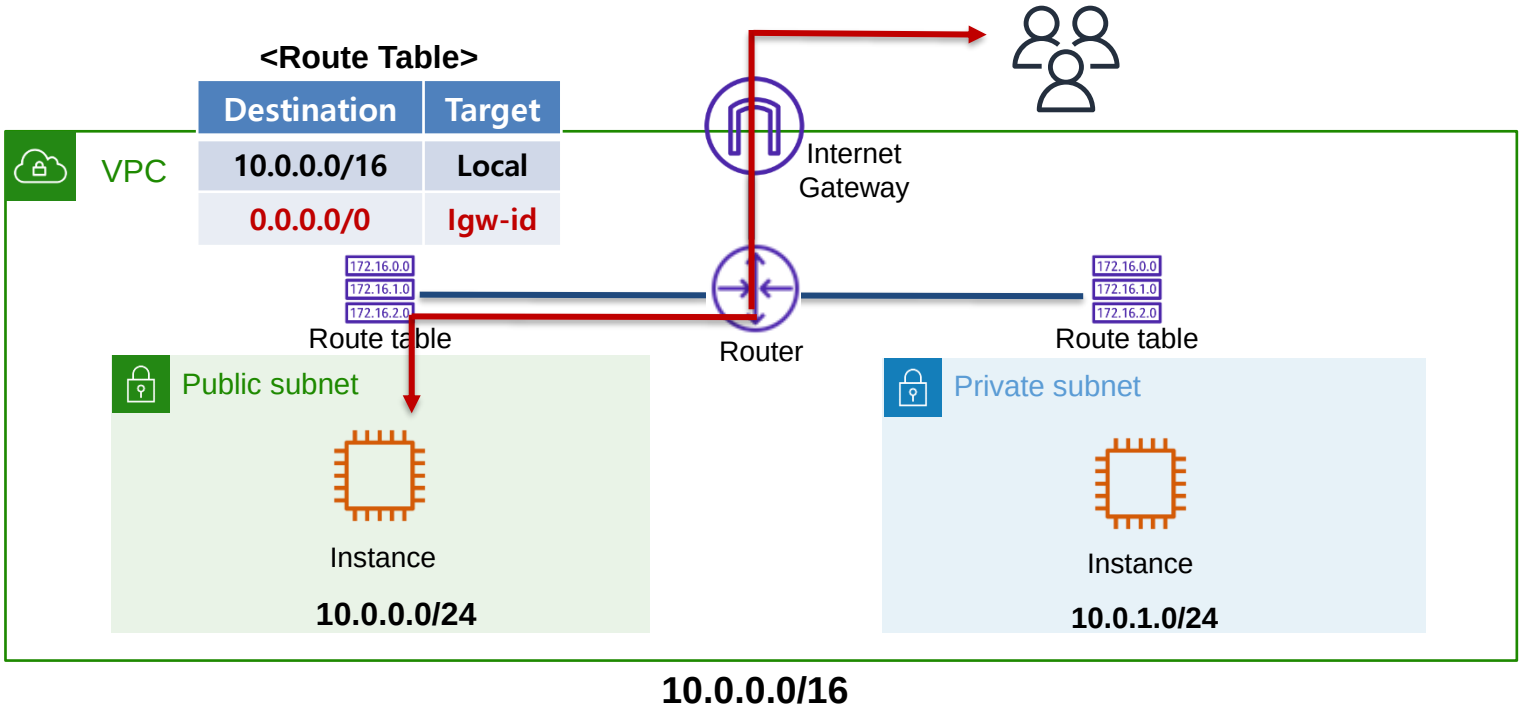
- **VPC마다 해당 VPC 내부 경로 정보를 갖는 디폴트 라우팅 테이블이 존재.**
- **Subnet마다 라우팅 테이블이 연결되어 있어야 한다.**
  - 관리자가 별도로 설정하지 않을 경우 **디폴트 라우팅 테이블**이 연결.
    기본적으로 동일 VPC 내부 Subnet은 서로 네트워크 도달성을 갖는다.
- **관리자가 별도의 사용자 지정 라우팅 테이블 생성 후 Subnet에 연결 가능.**



Internet Gateway / Public Subnet

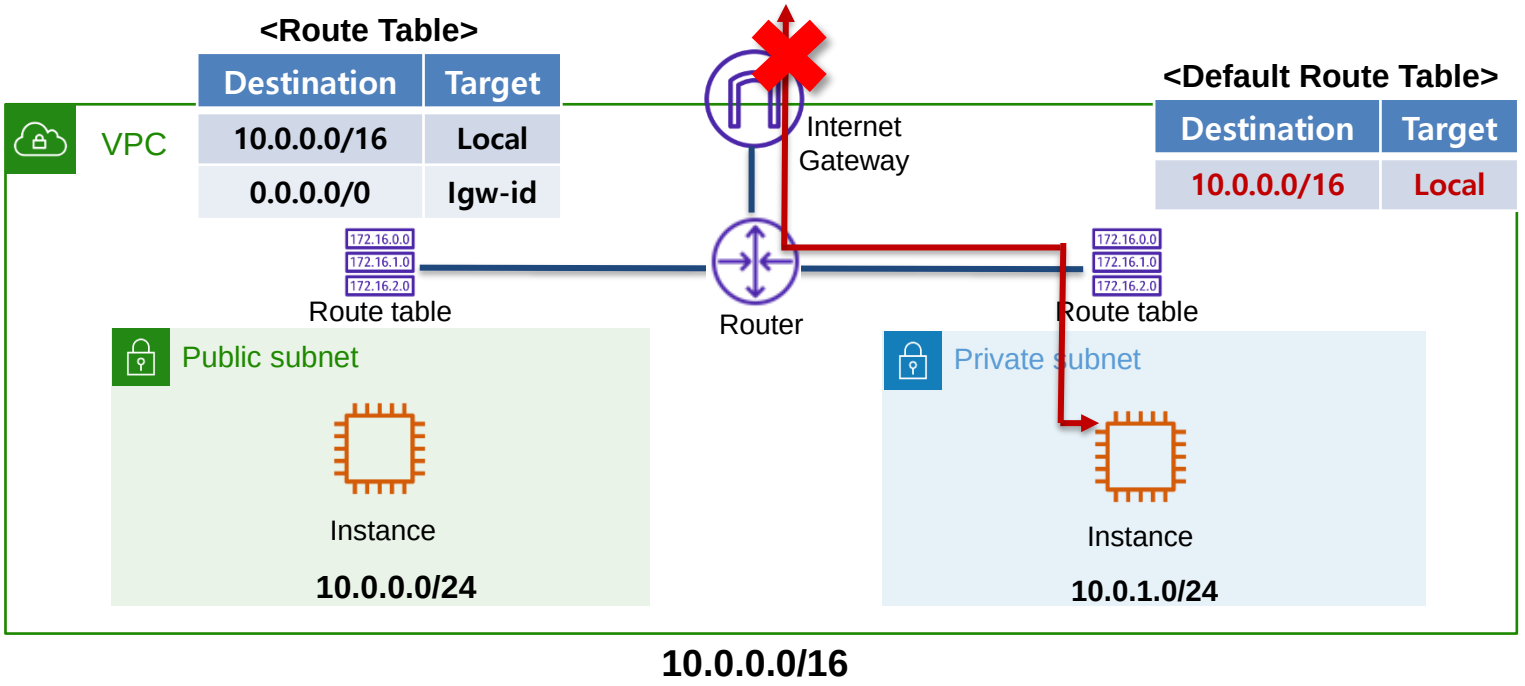
- VPC 내부 리소스와 인터넷 사이의 통신을 가능하게 하는 게이트웨이.
- 수평 확장되고 가용성이 높은 중복 구성 요소.
- 인터넷 게이트웨이에 대한 경로를 갖는 Subnet을 **Public Subnet**이라고 한다.

Internet gateway



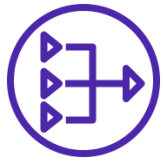
Private Subnet

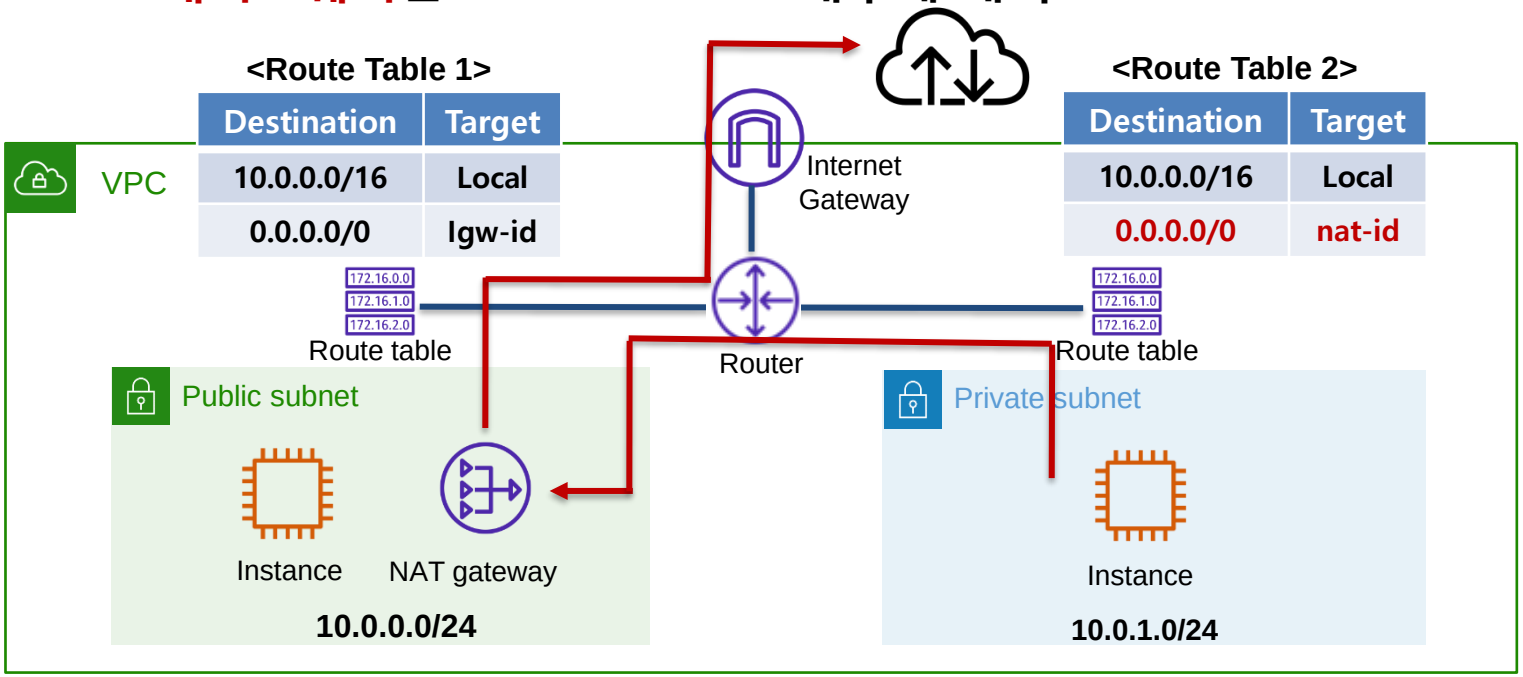
- 인터넷 게이트웨이에 대한 경로가 라우팅 테이블에 없는 Subnet을 Private Subnet이라고 한다.
- 인터넷에서 VPC 내부 리소스에 대한 직접적인 접근이 불가능.
- Private Subnet 내부 리소스가 업데이트/패치를 위해 인터넷과 통신해야 하는 경우 어떻게 해야 하는가?



NAT Gateway / Private Subnet

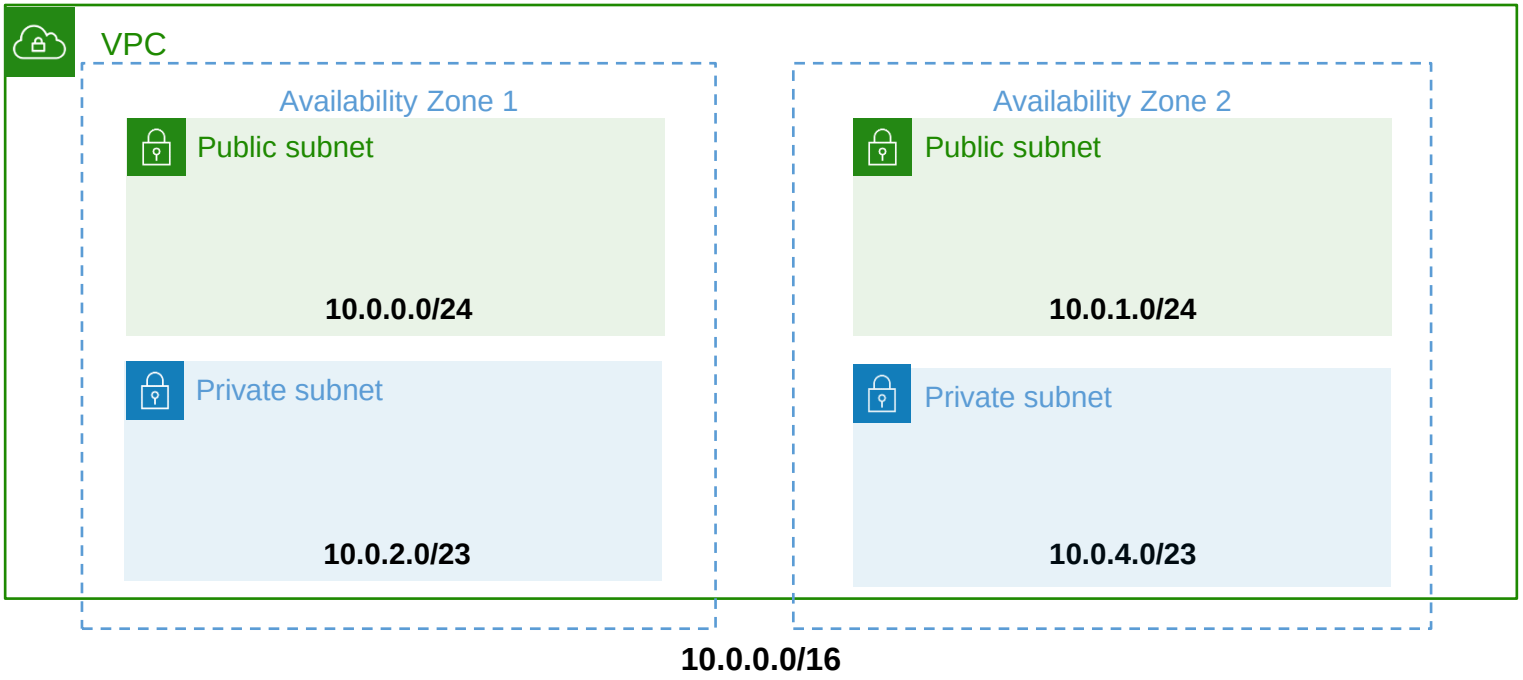
- **NAT 게이트웨이**는 **Private Subnet 인스턴스**가 인터넷, 또는 기타 AWS 서비스와 연결이 가능하도록 한다.
- 반대로 인터넷 사용자는 Private Subnet 내부 인스턴스 접근이 불가능.
- **NAT 게이트웨이**는 **Public Subnet** 내부에 배치.





Subnet 구성

- 인터넷 사용자의 직접 액세스를 허용하는 리소스는 Public Subnet에 배치.
- 온프레미스 환경과 다르게 일반적으로 큰 크기의 Subnet을 고려.
- 기본은 가용 영역마다 각각 1개의 Public Subnet/Private Subnet을 배치.
- 일반적으로 Private Subnet에 배치되는 리소스가 더 많다.



Elastic Network Interface (ENI)

- **인스턴스에 연결할 수 있는 가상 네트워크 인터페이스.**
- **Subnet 안에 생성된 각 인스턴스에는 Primary Network Interface가 연결되어 있다.**
- **Primary Network Interface는 연결을 해제할 수 없지만 ENI를 생성하여 추가로 연결하는 것은 가능.**
- **추가로 생성한 ENI는 동일 가용 영역의 다른 인스턴스로 이동이 가능하다. (다음 정보도 같이 이동)**
  - MAC 주소 / 사설 IP 주소 / EIP 주소
- **2개 이상의 ENI를 사용하는 경우**
  - 관리 네트워크 생성 / VPC에서 네트워크 및 보안 어플라이언스 사용

Elastic network interface

Elastic IP address (EIP)

- Public Subnet 인스턴스에 공인 IPv4 주소를 할당하면 기본적으로 동적 IP 주소가 연결됨.
- 인스턴스 및 네트워크 인터페이스에 고정 IP 주소 연결이 필요한 경우 탄력적 IP 주소를 사용.
- EIP는 리전당 5개로 제한. IPv6는 지원되지 않는다.
- 실행 중인 인스턴스에 연결된 EIP 한 개는 무료로 사용.

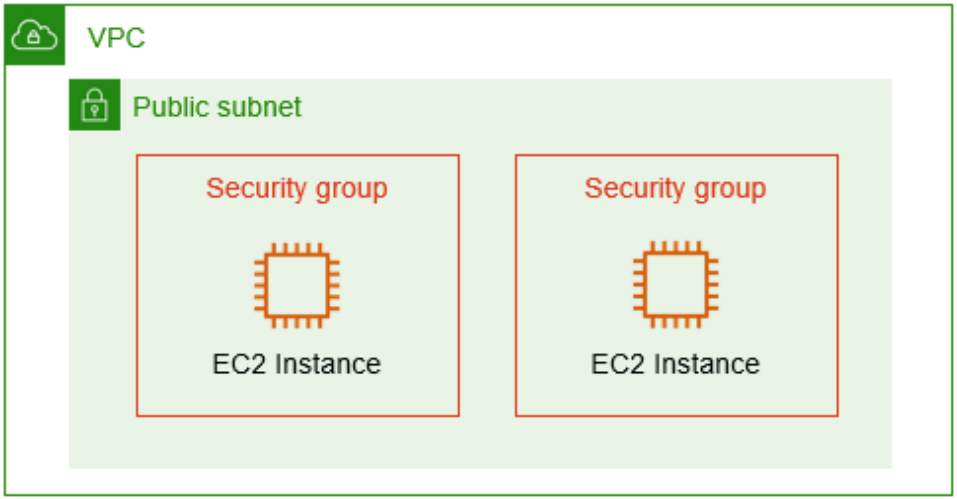
Elastic IP address

02 AWS 네트워크 기본 보안 구성

Security Group

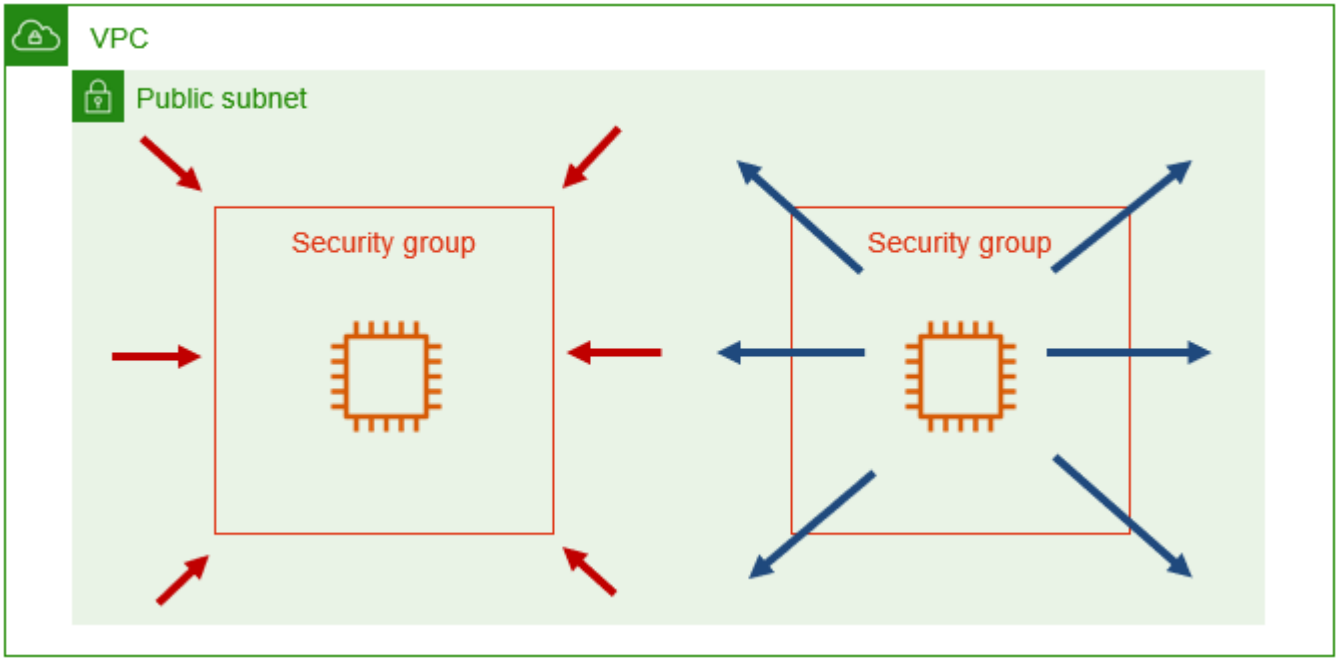
- **인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할.**

- **서브넷 수준이 아니라 인스턴스 수준에서 작동.**
  - 서브넷의 각 인스턴스를 서로 다른 보안 그룹에 할당 가능.
- **IP 주소/포트 번호를 사용하여 정책 구성.**
- **Stateful 방화벽 동작.**
- **허용 정책만 가능**



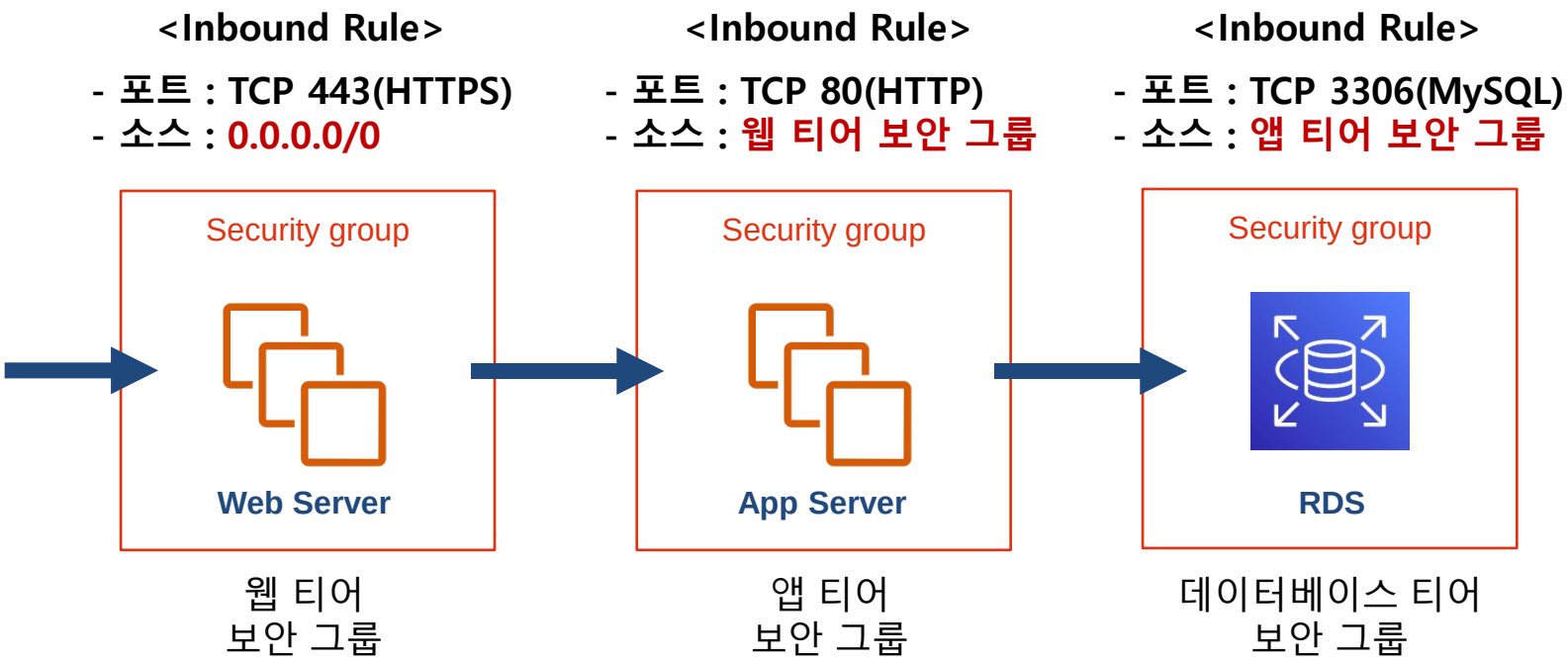
Security Group

- **Security Group 기본 구성**
  - Inbound : 모든 트래픽 차단
  - Outbound : 모든 트래픽 허용



Security Group

- **보안 그룹 사용 예 :**



NACL(Network ACL)

- 서브넷 경계의 방화벽 역할을 수행.
- IP 주소/포트 번호를 사용하여 정책 구성.
- 기본적으로 모든 Inbound/Outbound 트래픽을 허용
- Stateless 방화벽 동작.

인바운드 규칙 (2) — 인바운드 규칙 편집

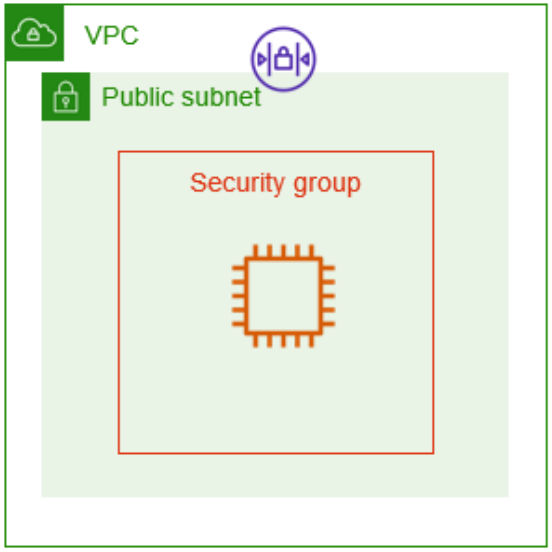
인바운드 규칙 필터링 — 1

규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부
100	모든 트래픽	모두	모두	0.0.0.0/0	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

아웃바운드 규칙 (2) — 아웃바운드 규칙 편집

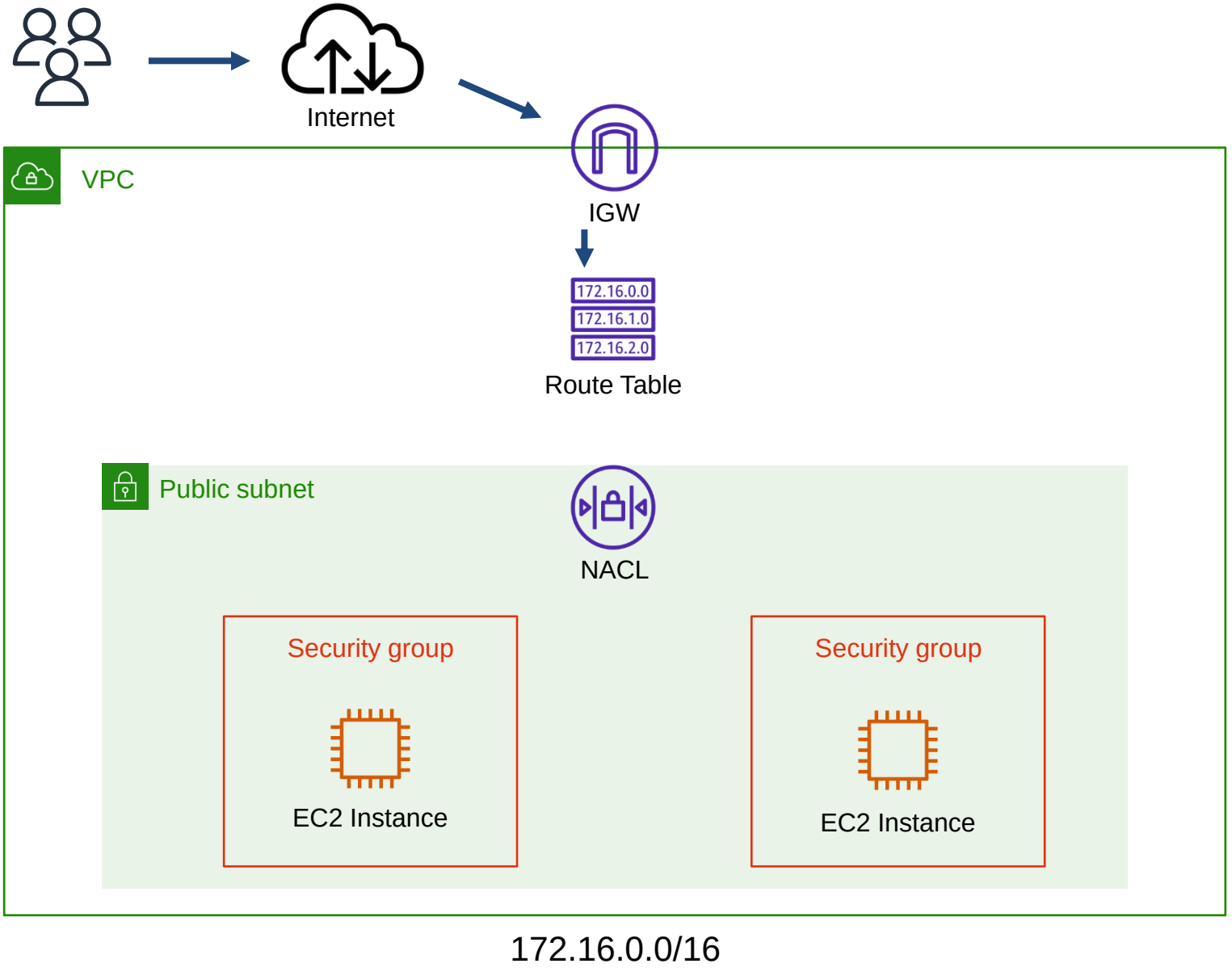
아웃바운드 규칙 필터링 — 1

규칙 번호	유형	프로토콜	포트 범위	대상	허용/거부
100	모든 트래픽	모두	모두	0.0.0.0/0	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

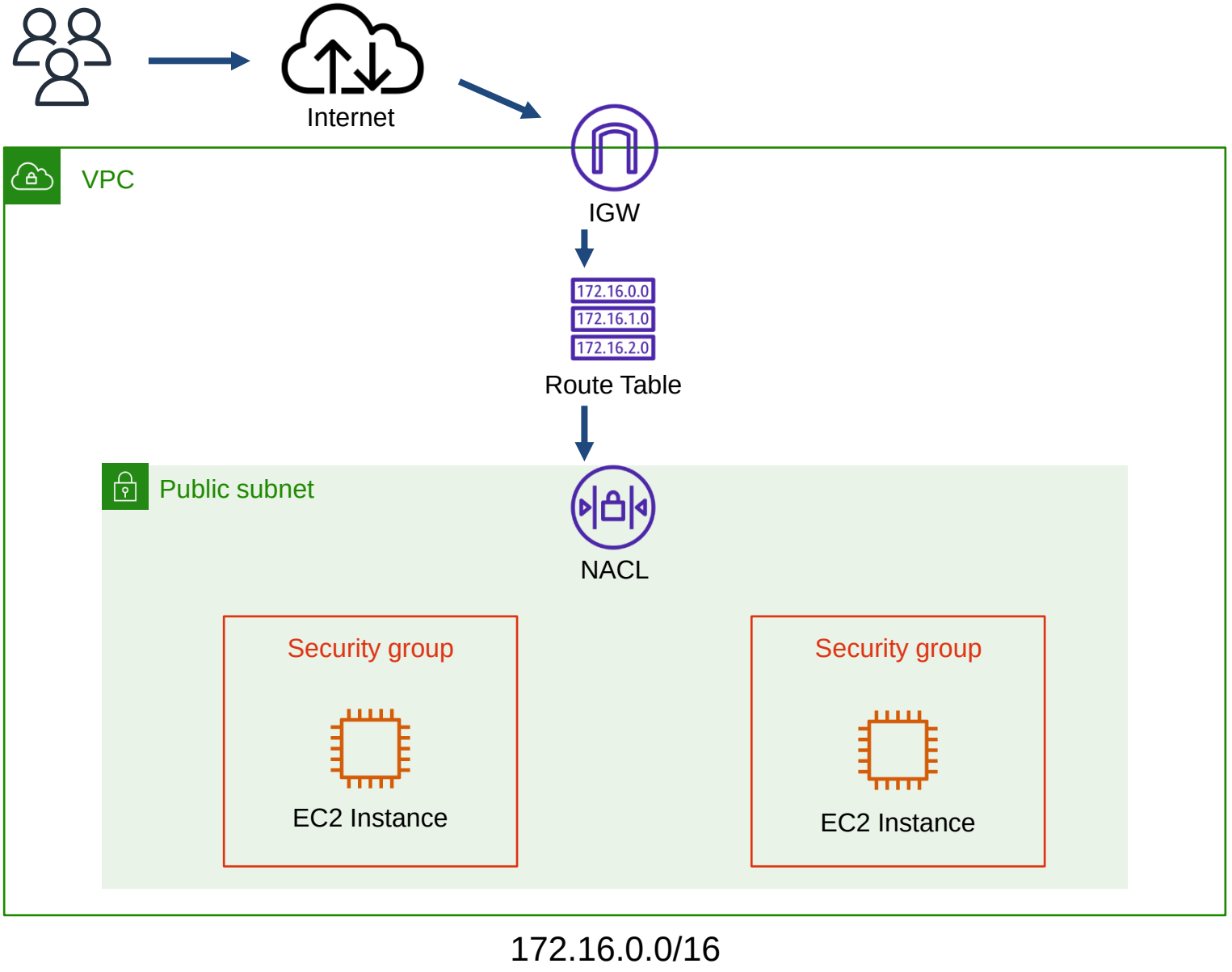


03 정리

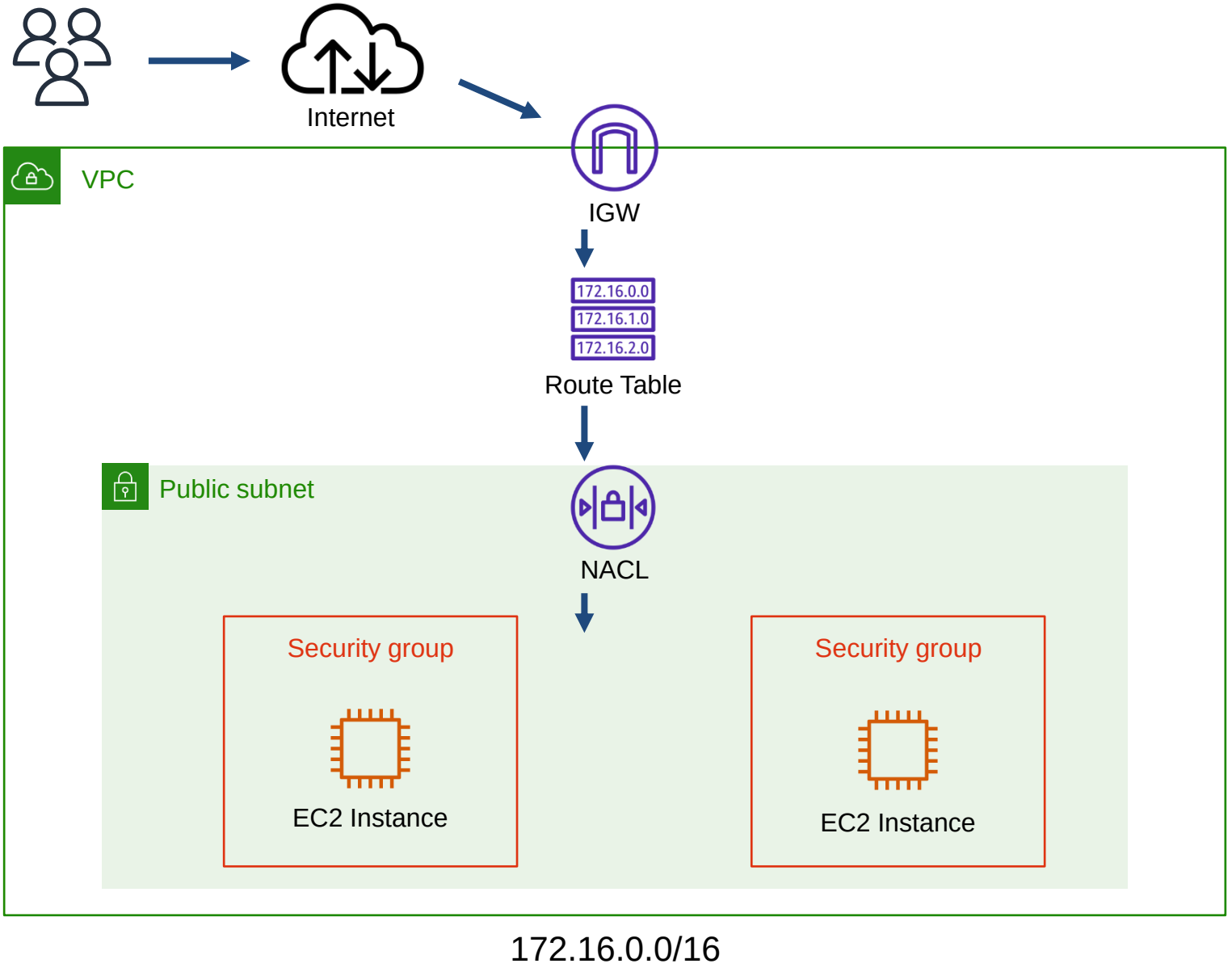
다중 계층 방어


Internet
VPC
IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Public subnet
NACL
Security group
EC2 Instance
Security group
EC2 Instance
172.16.0.0/16

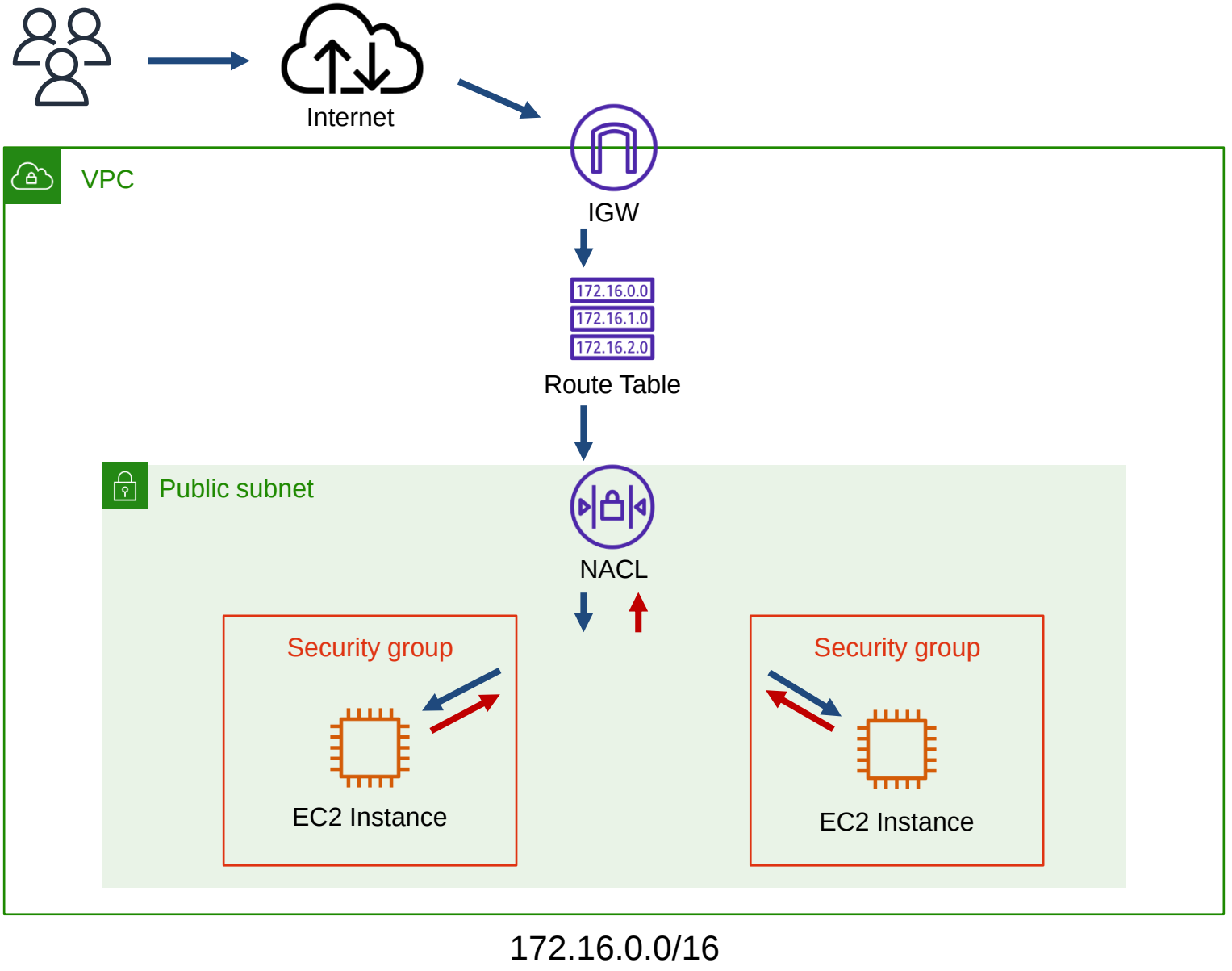
다중 계층 방어


Internet
VPC
IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Public subnet
NACL
Security group
EC2 Instance
Security group
EC2 Instance
172.16.0.0/16

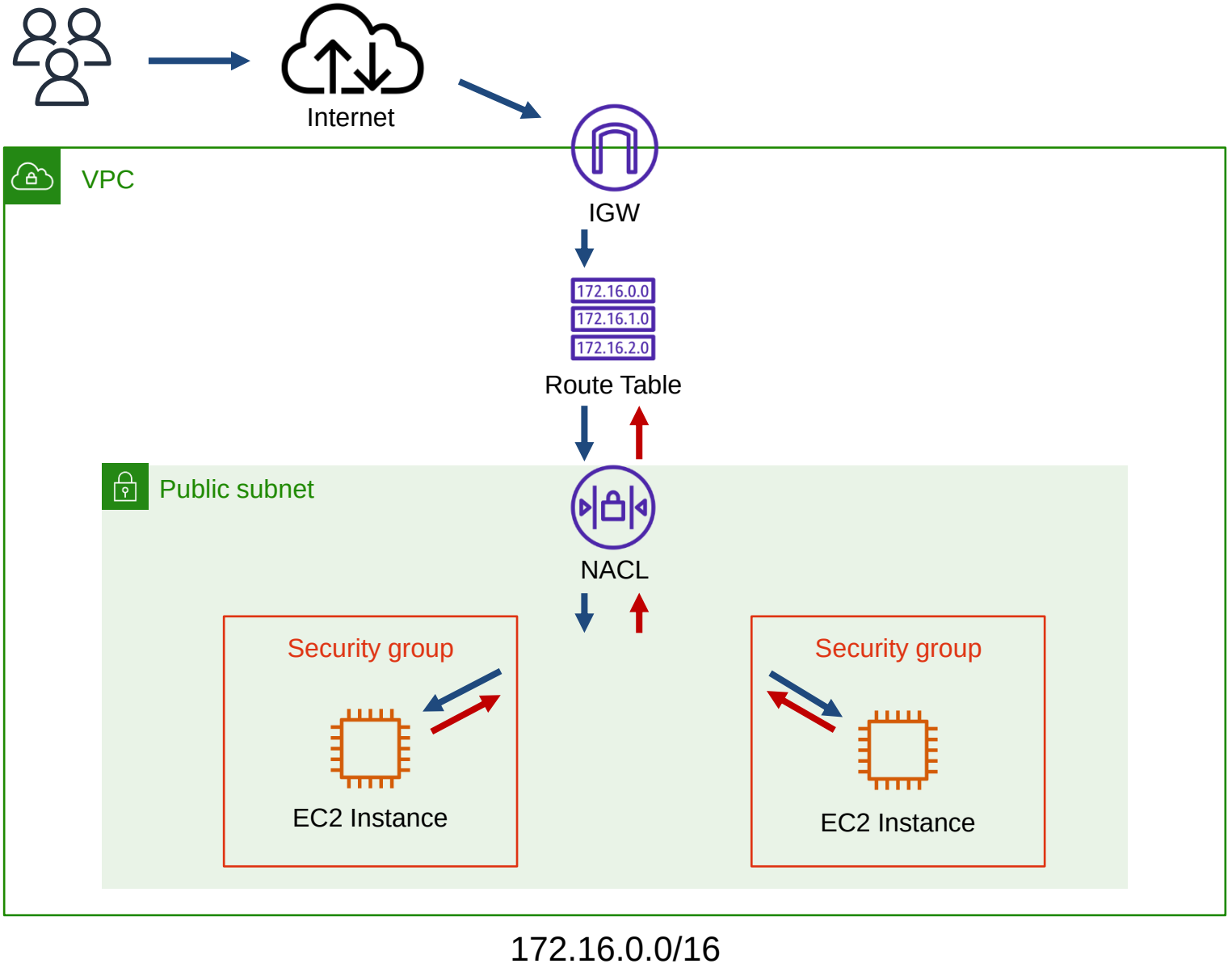
다중 계층 방어


Internet
VPC
IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Public subnet
NACL
Security group
EC2 Instance
Security group
EC2 Instance
172.16.0.0/16

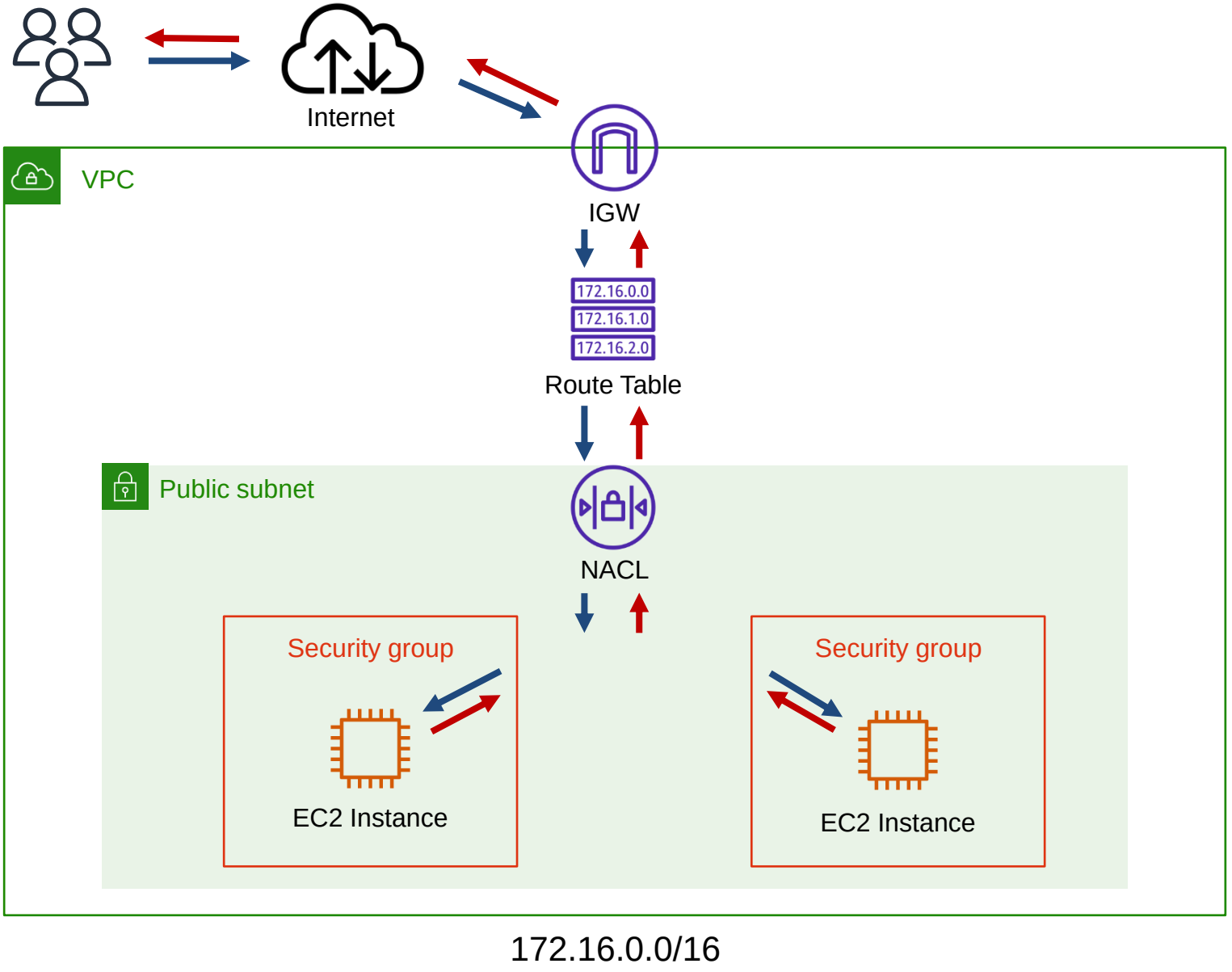
다중 계층 방어


Internet
VPC
IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Public subnet
NACL
Security group
EC2 Instance
Security group
EC2 Instance
172.16.0.0/16

다중 계층 방어

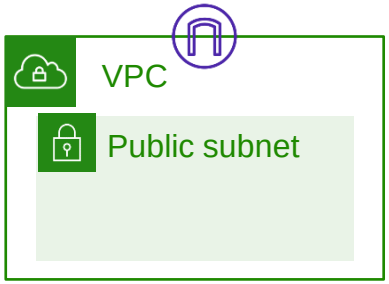

Internet
VPC
IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Public subnet
NACL
Security group
EC2 Instance
Security group
EC2 Instance
172.16.0.0/16

다중 계층 방어


Internet
VPC
IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Public subnet
NACL
Security group
EC2 Instance
Security group
EC2 Instance
172.16.0.0/16

VPC 내부로 트래픽 전송

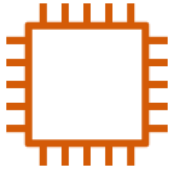
- **인터넷을 통해 VPC의 Subnet 내부 인스턴스에 접근하기 위해서는 다음 내용을 확인.**



VPC에 IGW 연결

Route Table

라우팅 테이블에
IGW 경로 등록



인스턴스에 공인
IP 주소 할당

NACL과 Security
Group 정책 확인