

# Azure 실습 3 - Network

## Azure 가상 네트워킹 관리(AZ-104, 모듈 04)

### AZ-104: Azure 관리자를 위한 가상 네트워크 구성 및 관리

인터넷은 어떤 원리로 운영되고 있는 걸까?

<https://youtu.be/Pwf-YG--Zsg>

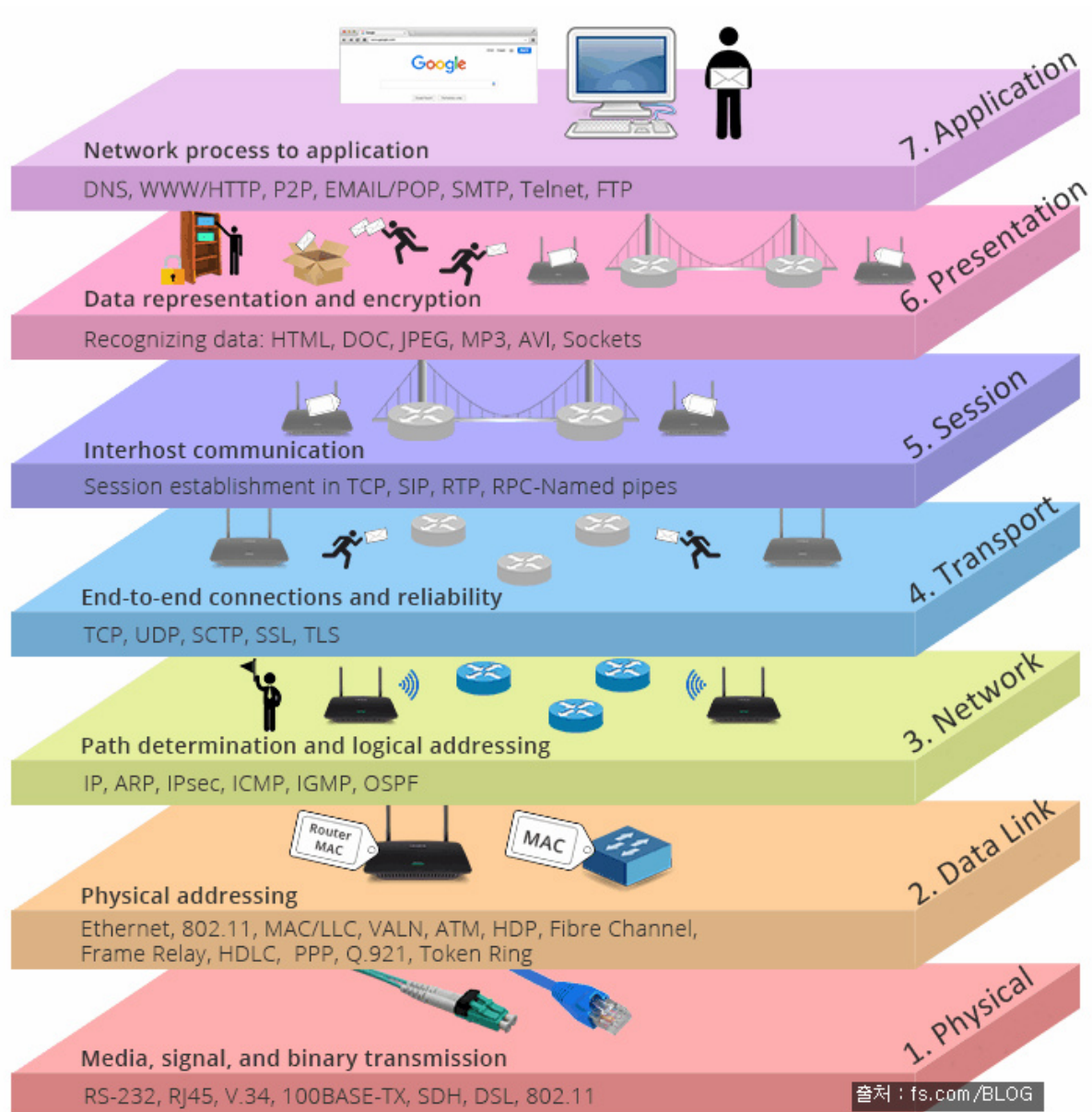
인터넷은 어떻게 작동될까요?

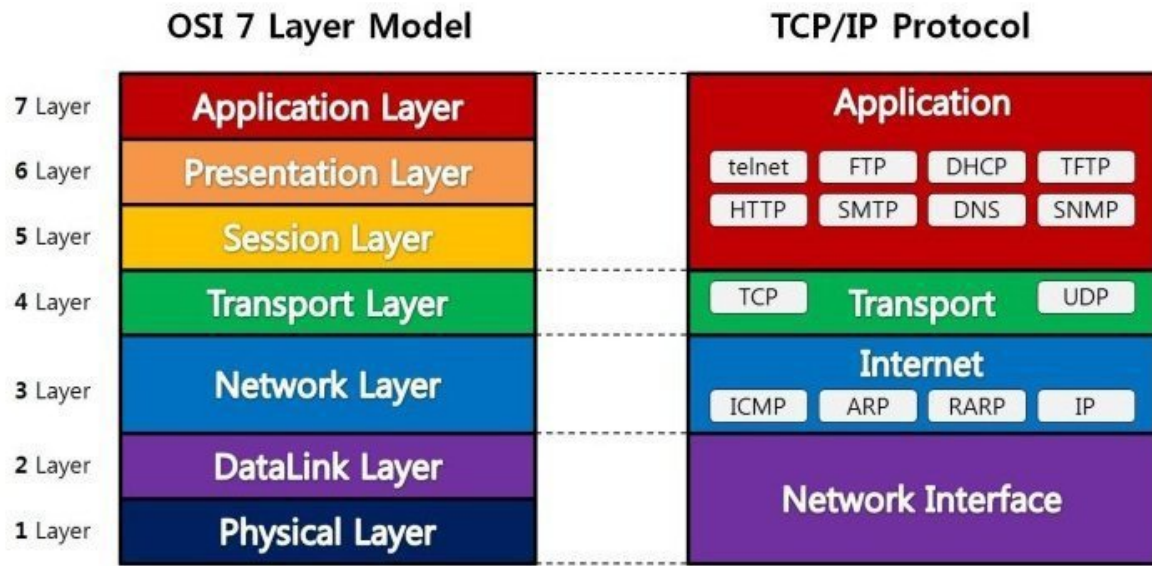
<https://youtu.be/o5yBI59wRbY>

그림으로 배우는 네트워크 이야기 [OSI 7 Layer/네트워크]

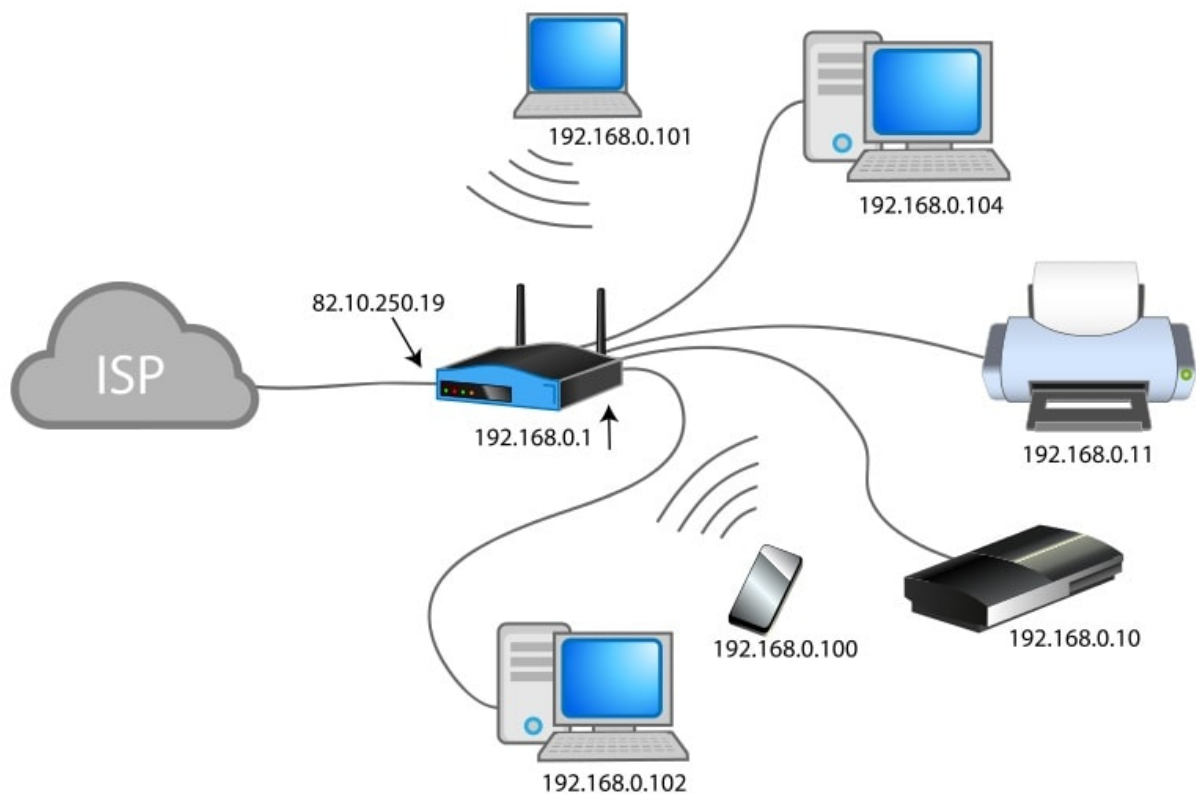
<https://youtu.be/aTPy201F0AA>

### OSI 7 Layer과 네트워크 장비





**인터넷(Internet)**은 Inter-networking(인터넷들의 연결)의 약자로,  
쉽게 표현하면 **라우터들(L3)의 집합**



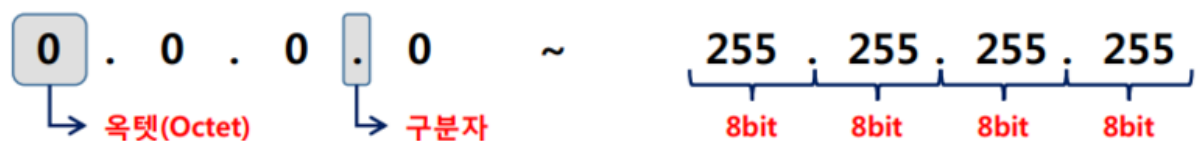
**Public Network**

**공중망(Public Network)**은 사설망과 대칭되는 개념으로 불특정 다수의 사용자에게 서비스를 제공하는 통신망으로 우리가 흔히 쓰고 있는 인터넷이 대표적인 공중망이라고 볼 수 있다.

## IP 주소(v4)

인터넷(Public Network)에 연결하기 위해서는 IP주소(공인IP)가 있어야 하고 이 IP는 전세계에서 유일해야 되나 모든 컴퓨터에 IP를 할당 할 수 없음.

한정된 IP로 인터넷을 사용하기 위해 여러가지 방법들이 제시됨.



32비트의 값을 가지며 비트의 나열만으로는 파악하기 어려우므로 8비트씩 끊어 0~255의 10진수로 나타내며 각 숫자는 점(.)으로 구분. 최대 약 43억개지만 실제로는 훨씬 적음.

## Network ID와 Host ID



IP를 Network ID와 Host ID로 구분

각 Network ID에서 첫번째 주소는 **Network Address** (호스트부를 모두 비트 '0'채움. 네트워크 자체를 식별하기 위해 사용)

마지막 주소는 **Boardcast** (호스트부를 모두 비트 '1'채움. 네트워크 자체를 식별하기 위해 사용)

(Azure에서 서브넷 구성시 위 IP 2개는 사용 가능한 주소 개수에서 제외됨)

## Subnet(부분망)

한정된 IP자원을 효율적으로 분배하기 위해 네트워크 영역과 호스트 영역을 쪼개는 작업을 Subnetting이라고 하며 Subnetting을 하기 위해 쓰이는 것이 Subnet Mask.

2진수로 연속된 '1'과 연속한 '0'로 구성된 숫자로 IP주소와 논리 AND연산. (논리 AND 연산은  $1 \text{ AND } 1 = 1, 1 \text{ AND } 0 = 0, 0 \text{ AND } 1 = 0, 0 \text{ AND } 0 = 0$ )

Subnet mask 표기법 -> 1.1.1.0 (255.255.255.0)

**CIDR(prefix)** 표기법 -> 1.1.1.0/24

CIDR to IPv4 Conversion

<https://www.ipaddressguide.com/cidr>

### Private Network(사설망)

사설망이란 특정한 회사나 조직이 소유하고 독점적으로 사용하는 네트워크를 의미한다.

위키피디아에서는 “**사설 IP 주소 공간을 이용하는 네트워크이며 RFC 1918과 RFC 4193 표준을 준수한다. 이러한 주소는 가정, 사무실, 기업 랜에 쓰인다**”라고 설명하고 있다.

쉽게 말해서 우리가 가정에서 공유기 내부에서 사설 IP로 사용하고 있는 네트워크가 대표적인 사설망이라고 보면 된다.

### 사설IP 주소(RFC 1918)

네트워크 주소	IP 범위	주소 개수
10.0.0.0/8 (255.0.0.0)	10.0.0.0~10.255.255.255	16,777,216
172.16.0.0/12 (255.240.0.0)	172.16.0.0~172.31.255.255	1,048,576
192.168.0.0/16 (255.255.0.0)	192.168.0.0~192.168.255.255	65,536

**Azure에서 가상 네트워크(Vnet)가 사설망을 구축.**

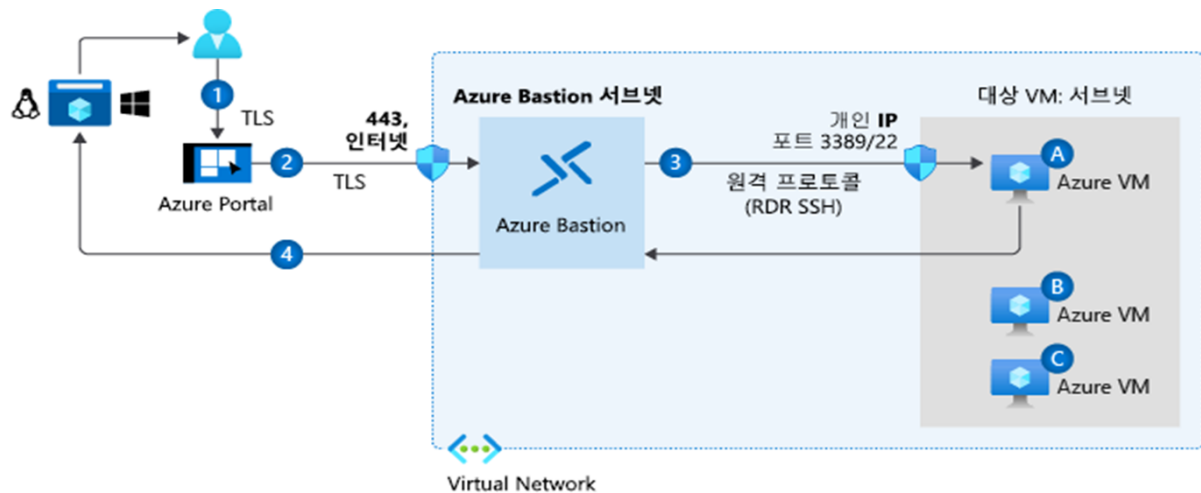
### NAT

HTTP → 인터넷을 여는 열쇠 : 서버와 클라이언트

<https://youtu.be/yBPyzaccbkc>

### Azure Bastion

Bastion, JumpBox



- Azure Bastion을 사용하여 Azure Portal을 통해 가상 머신에 연결

## 1. 가상 네트워크(VNet, Virtual Networks) 구성

AWS VPC(Virtual Private Cloud) : <https://aws.amazon.com/ko/vpc/>

### Virtual Network(VNet)



- Azure 배포에 대한 IP 주소 지정 스키마 디자인(샌드박스)
- Windows Server IaaS VM IP 주소 지정 및 라우팅 구현

### 실습

빠른 시작: Azure 포털을 사용하여 가상 네트워크 만들기

자습서: Azure Portal을 사용하여 가상 네트워크 피어링으로 가상 네트워크 연결

## 2. 네트워크 보안 그룹(NSG, Network Security Group)

AWS SG(Security Group) :

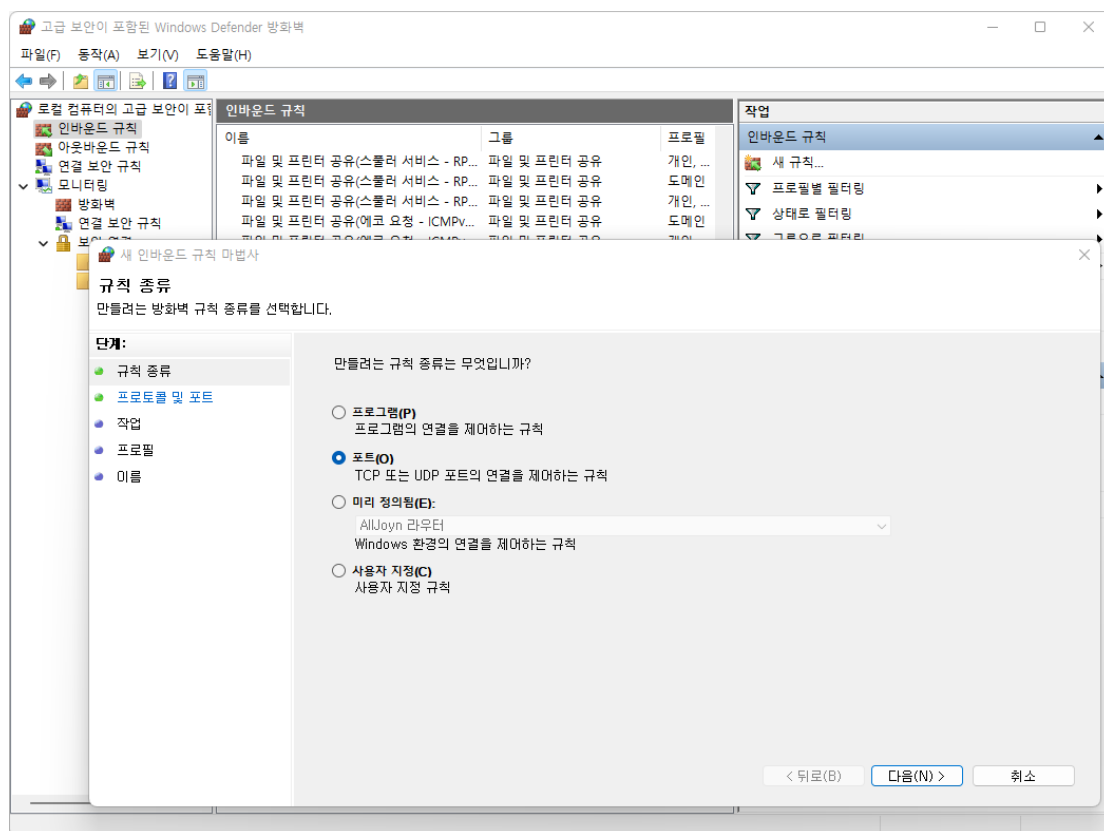
[https://docs.aws.amazon.com/ko\\_kr/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_SecurityGroups.html)

### Windows Defender

윈도우에도 방화벽이 포함되어 있음

검색 → Windows Defender → 고급 설정

- 인바운드/아웃바운드  
새규칙 → Port
- 모니터링 → 방화벽 → ICMP 활성화

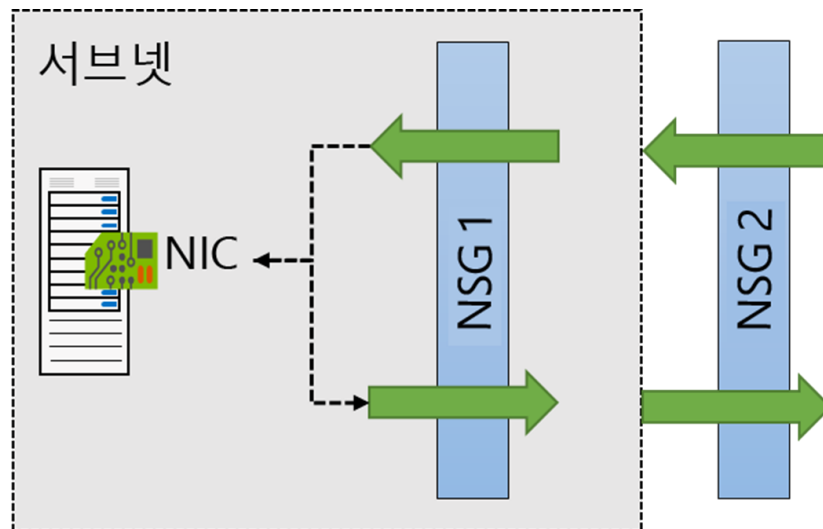


## 리눅스 방화벽, 포트 및 IP 접근제어

<https://wiki.kreonet.net/linux-guide/ip-51119587.html>

## Network Security Group

서브넷과 NIC에 대해 독립적으로 적용



네트워크 인터페이스: **vm01990**  
가상 네트워크/서브넷: **vnet01/subnet0**

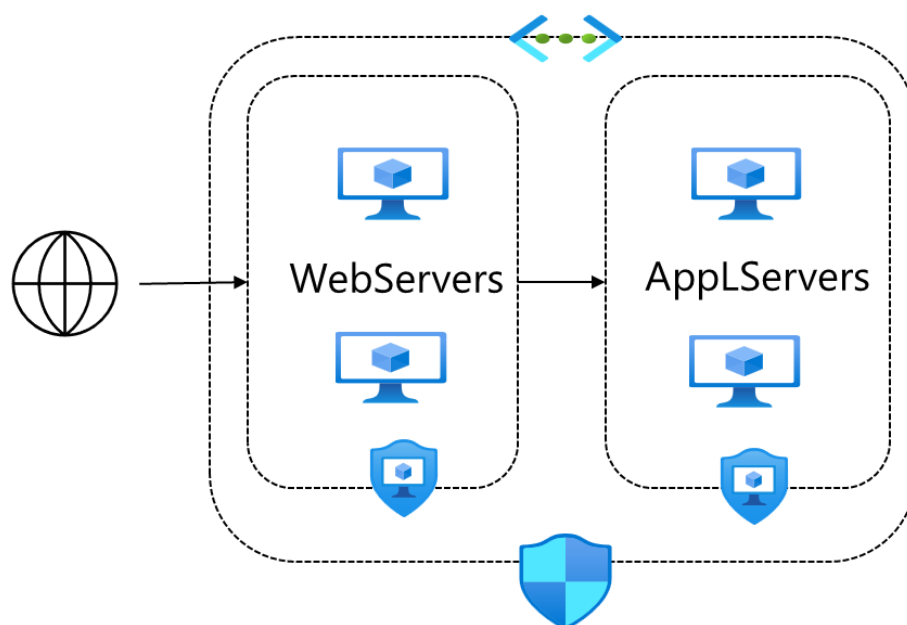
유효한 보안 규칙  
NIC 공용 IP:

토폴로지

NIC 프라이빗 IP: **10.4.0.4**

가속화된 네트워킹: 사용 안 함

## Application Security Group





원본	대상	포트
인터넷	WebServers	80, 443
WebServers	SQLServers	1533

- 네트워크 보안 그룹 및 서비스 엔드포인트를 사용하여 Azure 리소스에 대한 액세스 보호 및 격리(샌드박스)

## 실습

네트워크 트래픽 필터링 - 자습서

PaaS 리소스에 대한 네트워크 액세스 제한 - 자습서

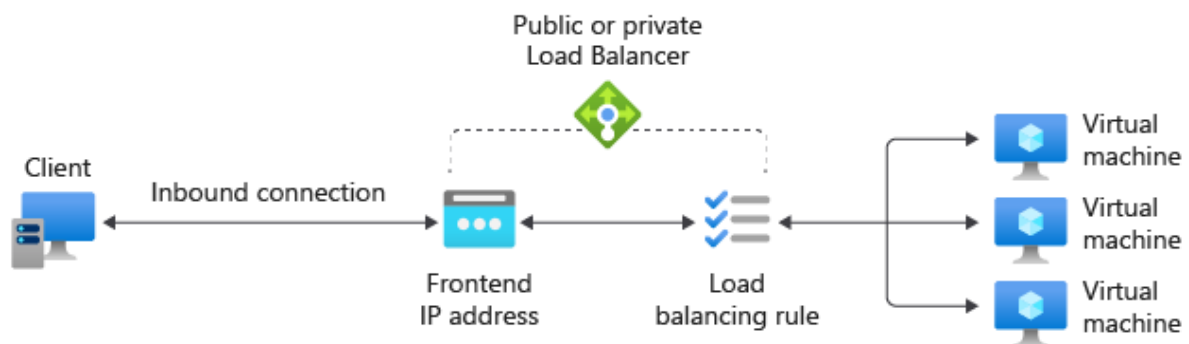
→ PaaS 진행 후에 실습

## 3. Azure Load Balancer 구성

L4

AWS Network Load Balancer :

[https://docs.aws.amazon.com/ko\\_kr/elasticloadbalancing/latest/network/introduction.html](https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/network/introduction.html)



- Azure Load Balancer 구성
- Azure Load Balancer를 사용하여 애플리케이션 확장성 및 복원력 개선(샌드박스)
- Azure에서 비HTTP(S) 트래픽 부하 분산

## Azure Load Balancer SKU

<https://docs.microsoft.com/ko-kr/azure/load-balancer/skus#skus>

## 실습

- 공용 부하 분산 장치 만들기

→ NAT Gateway를 생성하지 않고 실습 진행.

방법 1. 부하분산장치 만들때 인바운드 규칙의 부하 분산 규칙 생성시 “기본 아웃바운드 액세스를 사용합니다”로 설정한다.

방법 2. 부하분산장치 SKU를 Basic으로 생성. 가상머신 만들시 가용성 집합 1개를 추가해서 2개 VM에서 사용

- 내부 부하 분산 장치 만들기

SKU를 Basic(기본)으로 선택하고 NAT Gateway 생성하지 않음.

- 각 VM 마다 인바운드 NAT 규칙 만들기

SKU를 Basic(기본)으로 선택하고 NAT Gateway 생성하지 않음.

## 랩

