

클라우드 컴퓨팅 입문

Network

이 자료는 Elixirr의 사전 서면 승인 없이 외부에 배포하기 위해 그 일부를 배포, 인용 또는 복제 할 수 없습니다.

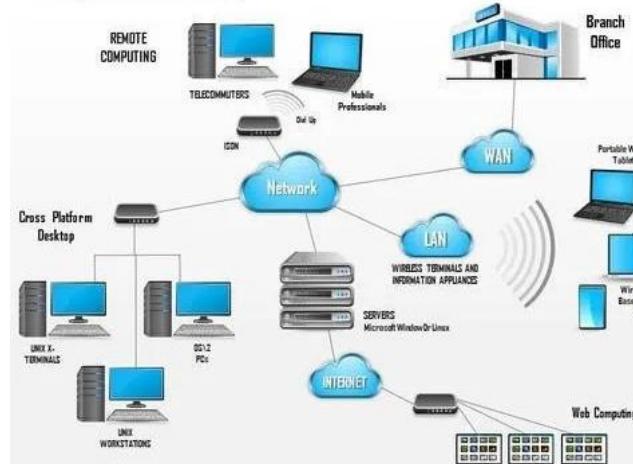
© Copyright Elixirr

Network 기본 개념

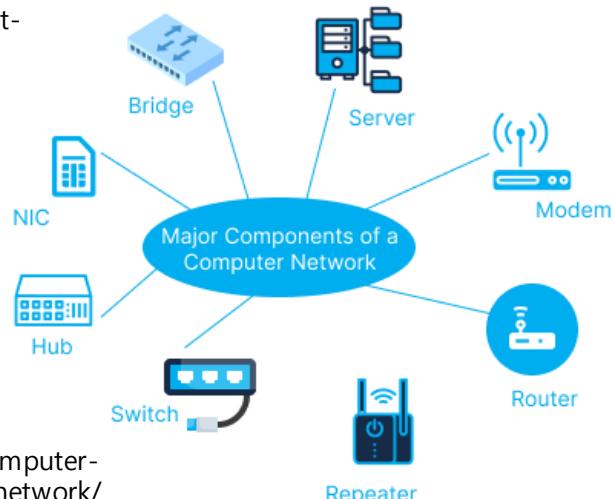
Computer Networking

컴퓨터 네트워킹이란 컴퓨터들을 유/무선으로 연결하여 사용하는 것을 말합니다.

Computer Networking



<https://zibras.medium.com/essentials-of-computer-networking-and-internet-protocols-ccd75fac3877>



<https://www.prepbytes.com/blog/computer-network/components-of-computer-network/>

Ask  ChatGPT

Computer Networking?

컴퓨터 네트워킹은 **컴퓨터와 다른 장치들을 연결하여 자원과 정보를 공유하는** 것을 말합니다. 이러한 연결은 **유선 또는 무선**으로 이루어질 수 있습니다.

- **통신:** 네트워크는 장치들이 서로 대화할 수 있게 합니다. 예를 들어, 이메일을 보낼 때 컴퓨터는 네트워크를 사용하여 수신자에게 이메일을 전달합니다.
- **자원 공유:** 장치들은 프린터, 파일, 인터넷 연결 같은 자원을 공유할 수 있습니다. 즉, 컴퓨터마다 별도의 프린터가 필요하지 않다는 의미입니다.

실제 사례

우리는 일상 생활 중 다양한 형태의 컴퓨터 네트워크를 접하게 됩니다. 이때 각각의 네트워크는 그 사용분야의 특성을 감안한 다양한 프로토콜이 사용되게 됩니다.

적용 사례

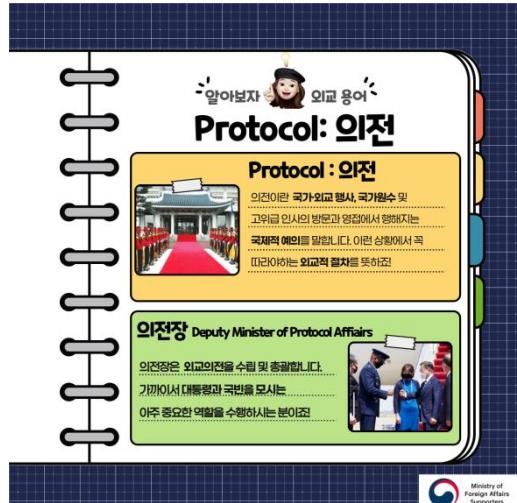
- **가정용 네트워크:** 집에서 사용하는 Wi-Fi 네트워크는 가족의 모든 기기를 인터넷에 연결합니다. 스마트폰, 태블릿, 노트북 등이 이 네트워크를 통해 인터넷에 접속할 수 있습니다.
- **회사 네트워크:** 회사에서는 여러 컴퓨터와 프린터가 네트워크로 연결되어 있어 직원들이 파일을 공유하고 인쇄 작업을 할 수 있습니다.
- **인터넷 카페:** 여러 대의 컴퓨터가 인터넷에 연결되어 있어 손님들이 동시에 웹 서핑이나 게임을 할 수 있습니다.
- **클라우드 서비스:** Google Drive나 Dropbox 같은 클라우드 스토리지는 인터넷을 통해 파일을 업로드하고 다운로드할 수 있게 해줍니다. 이를 통해 사용자는 어디서나 파일에 접근할 수 있습니다.
- **스마트 홈:** 네트워크를 통해 스마트 조명, 보안 카메라, 온도 조절기 등을 제어할 수 있습니다. 이를 통해 집안의 여러 장치를 스마트폰으로 관리할 수 있습니다.

프로토콜

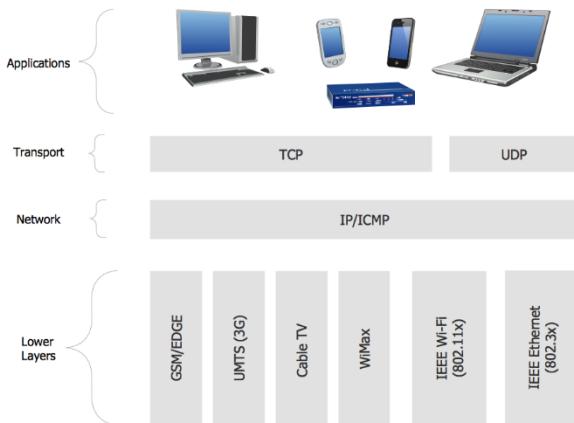
- **가정용 네트워크:**
 - Wi-Fi: 무선 연결을 위한 프로토콜입니다.
 - DHCP: IP 주소를 자동으로 할당합니다.
 - DNS: 도메인 이름을 IP 주소로 변환합니다.
- **회사 네트워크:**
 - Ethernet: 유선 연결을 위한 프로토콜입니다.
 - VPN: 안전한 원격 접속을 위한 프로토콜입니다.
 - SMTP/IMAP/POP3: 이메일 송수신을 위한 프로토콜입니다.
- **인터넷 카페:**
 - HTTP/HTTPS: 웹 페이지를 전송하는 프로토콜입니다.
 - FTP: 파일 전송을 위한 프로토콜입니다.
- **클라우드 서비스:**
 - HTTPS: 안전한 웹 트래픽을 위한 프로토콜입니다.
 - REST/GraphQL: API 호출을 위한 프로토콜입니다.
- **스마트 홈:**
 - Zigbee/Z-Wave: 스마트 기기 간 통신을 위한 프로토콜입니다.
 - MQTT: IoT 기기 간 메시지 전송을 위한 프로토콜입니다.

프로토콜

프로토콜이란 컴퓨터 네트워킹에서 데이터 전송을 위한 규칙과 표준의 집합입니다. 프로토콜은 장치 간에 정보를 효율적이고 정확하게 주고받을 수 있도록 합니다.



<https://blog.naver.com/mofakr/222542306905>

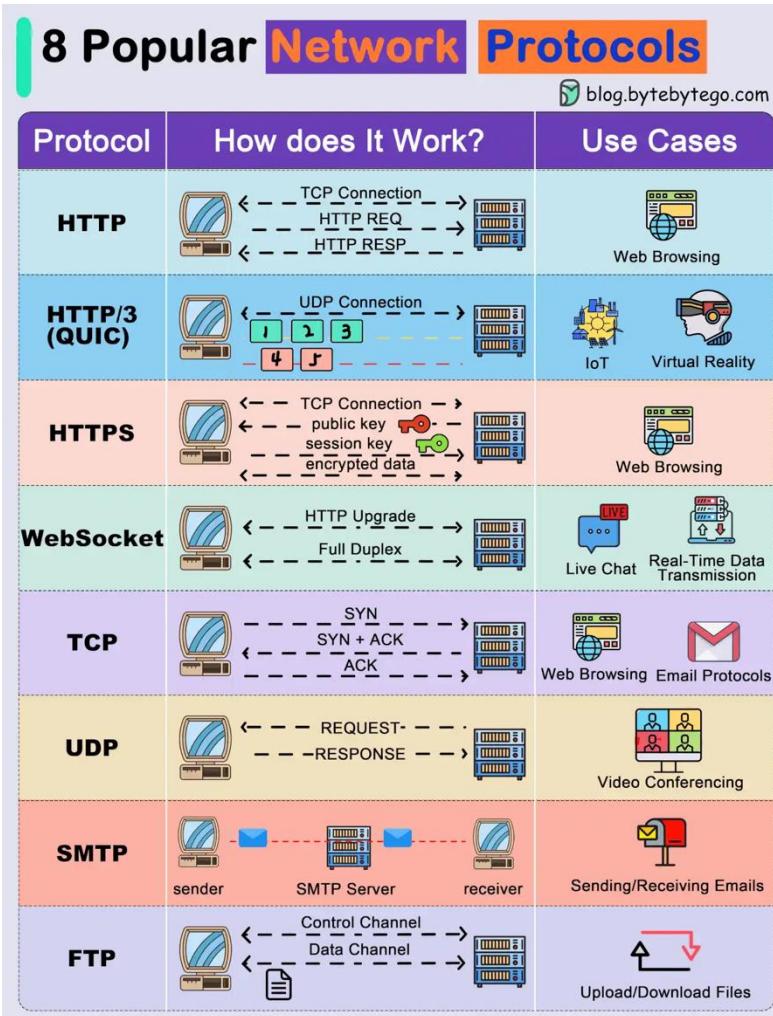


<https://www.conceptdraw.com/How-To-Guide/network-protocols>

- Ask ChatGPT Protocol
- 표준화 필요:** 다양한 제조업체의 장치들이 서로 통신할 수 있도록 공통의 언어가 필요했습니다. 프로토콜은 이러한 표준화된 언어를 제공합니다.
 - 상호 운용성:** 프로토콜은 서로 다른 시스템과 네트워크가 호환되도록 보장합니다. 예를 들어, 이메일 프로토콜(SMTP)은 다양한 이메일 서비스 간의 메시지 전송을 가능하게 합니다.
 - 효율성과 신뢰성:** 데이터 전송 중 오류를 줄이고 전송 속도를 최적화하기 위해 프로토콜이 개발되었습니다. 예를 들어, TCP는 데이터가 손실되지 않도록 보장합니다.
 - 보안:** 안전한 데이터 전송을 위한 암호화 및 인증 방법을 포함할 수 있습니다. HTTPS는 웹 트래픽을 보호합니다.

8 popular Network protocols

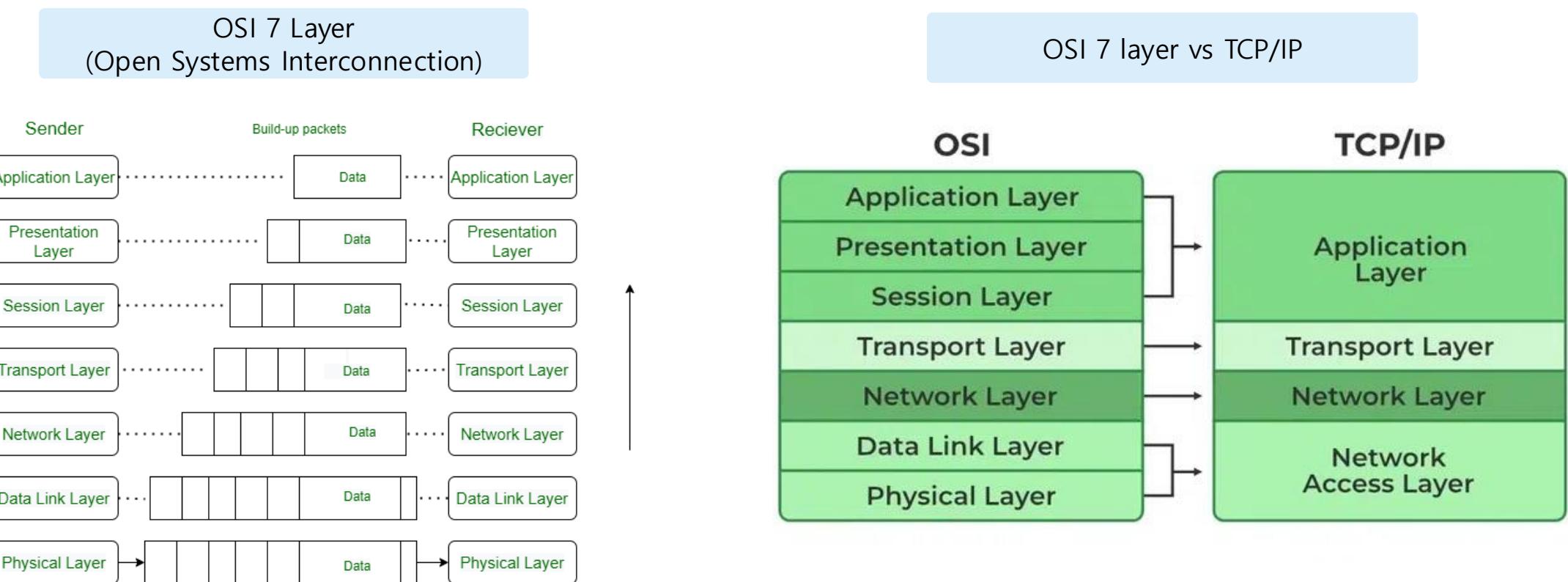
다음은 자주 사용되는 대표적인 네트워크 프로토콜 등입니다.



- HTTP (HyperText Transfer Protocol)
HTML 문서와 같은 리소스를 가져오기 위한 용도. Web에서 데이터 교환의 기반. 클라이언트-서버
- HTTP/3
HTTP의 차세대 개정판. 모바일 중심의 인터넷 사용을 위해 설계된 QUIC에서 실행. TCP 대신 UDP를 사용하여 웹 페이지 응답 속도가 빨라짐
- HTTPS (HyperText Transfer Protocol Secure)
HTTP를 확장하고 보안 통신을 위해 암호화 사용
- WebSocket
TCP를 통해 full-duplex 지원. 백엔드 서버에서 데이터를 실시간으로 가져오기 용이. 온라인 게임, 주식 매매, 메시징 등에서 실시간 통신을 위해 사용
- TCP (Transmission Control Protocol)
인터넷을 통해 패킷을 전송하고 네트워크를 통해 데이터와 메시지를 성공적으로 전달하도록 설계 많은 애플리케이션 계층 프로토콜이 TCP 기반
- UDP (User Datagram Protocol)
연결을 하지 않고 직접 패킷을 보냄. 실시간 통신에서는 패킷을 가끔씩 삭제하는 것이 기다리는 것보다 낫기 때문.
- SMTP (Simple Mail Transfer Protocol)
한 사용자에서 다른 사용자로 전자 메일을 전송하는 표준 프로토콜
- FTP (File Transfer Protocol)
클라이언트와 서버 사이에 파일을 전송

Layered Architecture

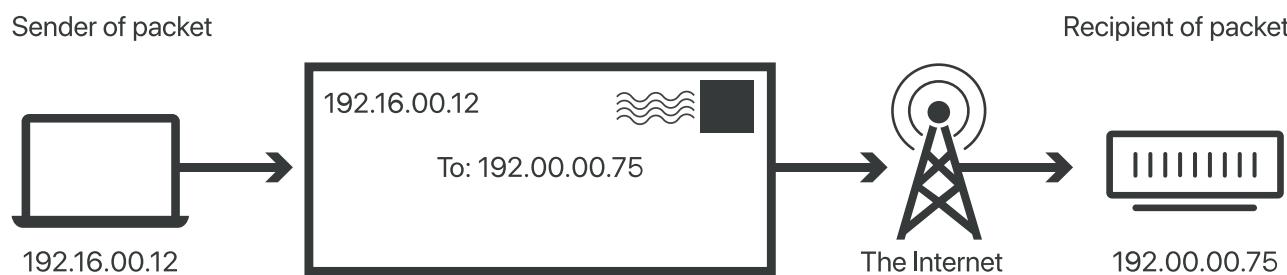
컴퓨터 네트워크는 보통 그 기능을 각각 특정 통신 구성요소를 담당하는 여러 계층으로 나눠서 구성하게 되며, 이러한 계층적 아키텍처를 통해 복잡한 통신 프로세스를 관리하기 쉽도록 작은 활동으로 나눠서 구성하게 됩니다.



IP 프로토콜

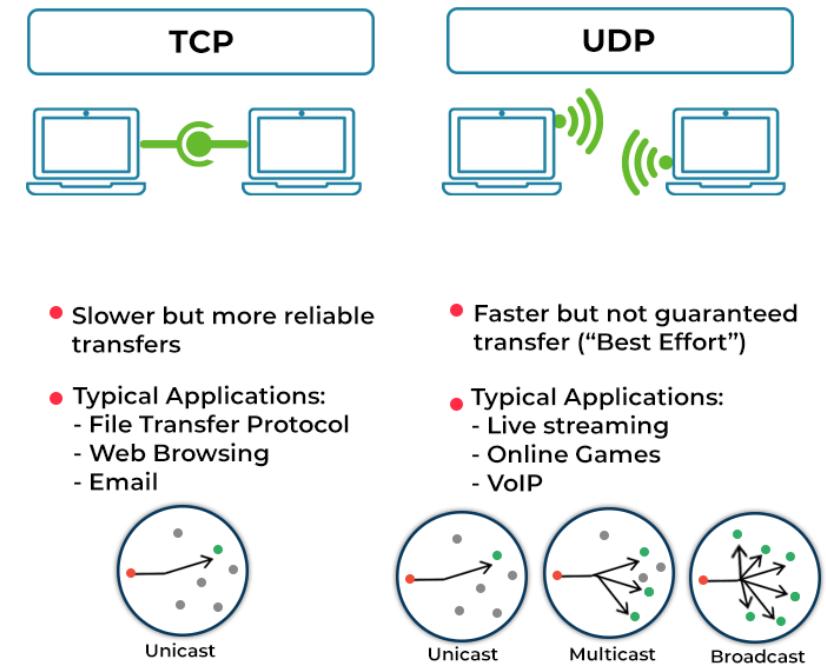
인터넷 프로토콜(IP)은 데이터 패킷이 네트워크를 통해 이동하고 올바른 대상에 도착할 수 있도록 데이터 패킷을 라우팅하고 주소를 지정하기 위한 프로토콜 또는 규칙의 집합입니다.

- 인터넷을 통과하는 데이터는 패킷이라고 하는 더 작은 조각으로 나뉩니다.
- IP 정보는 각 패킷에 첨부되며, 이 정보는 라우터가 패킷을 올바른 위치로 보내는 데 도움이 됩니다.
- 인터넷에 연결하는 모든 장치나 도메인에는 IP 주소가 할당되며, 패킷이 연결된 IP 주소로 전달되면 데이터가 필요한 곳에 도착합니다.



<https://www.cloudflare.com/ko-kr/learning/network-layer/internet-protocol/>

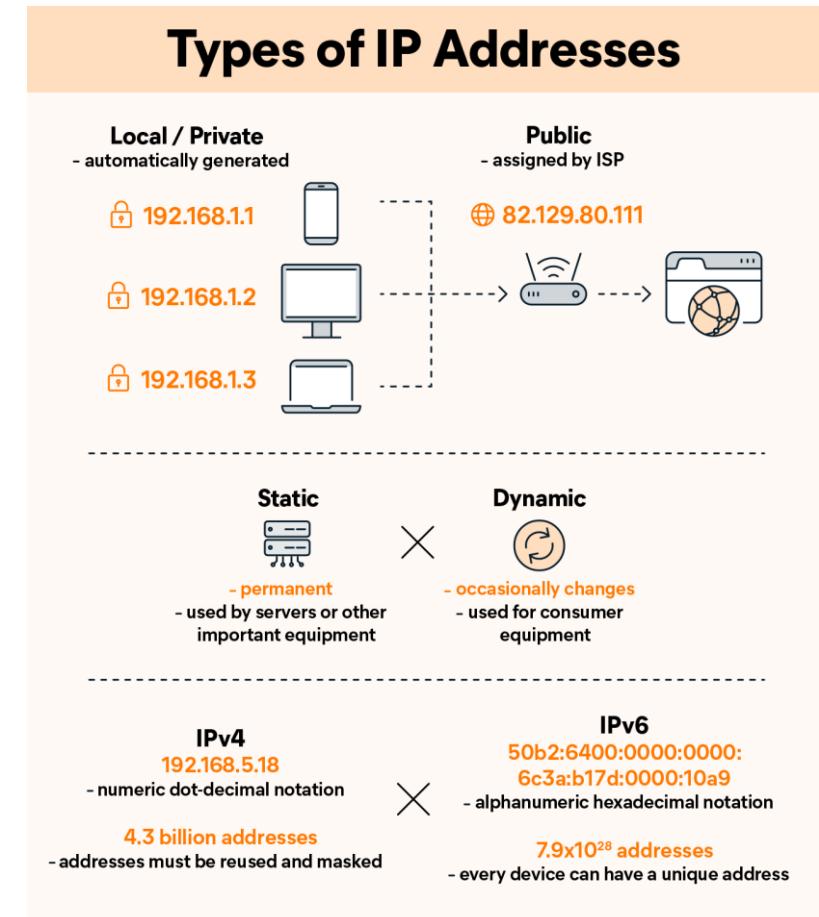
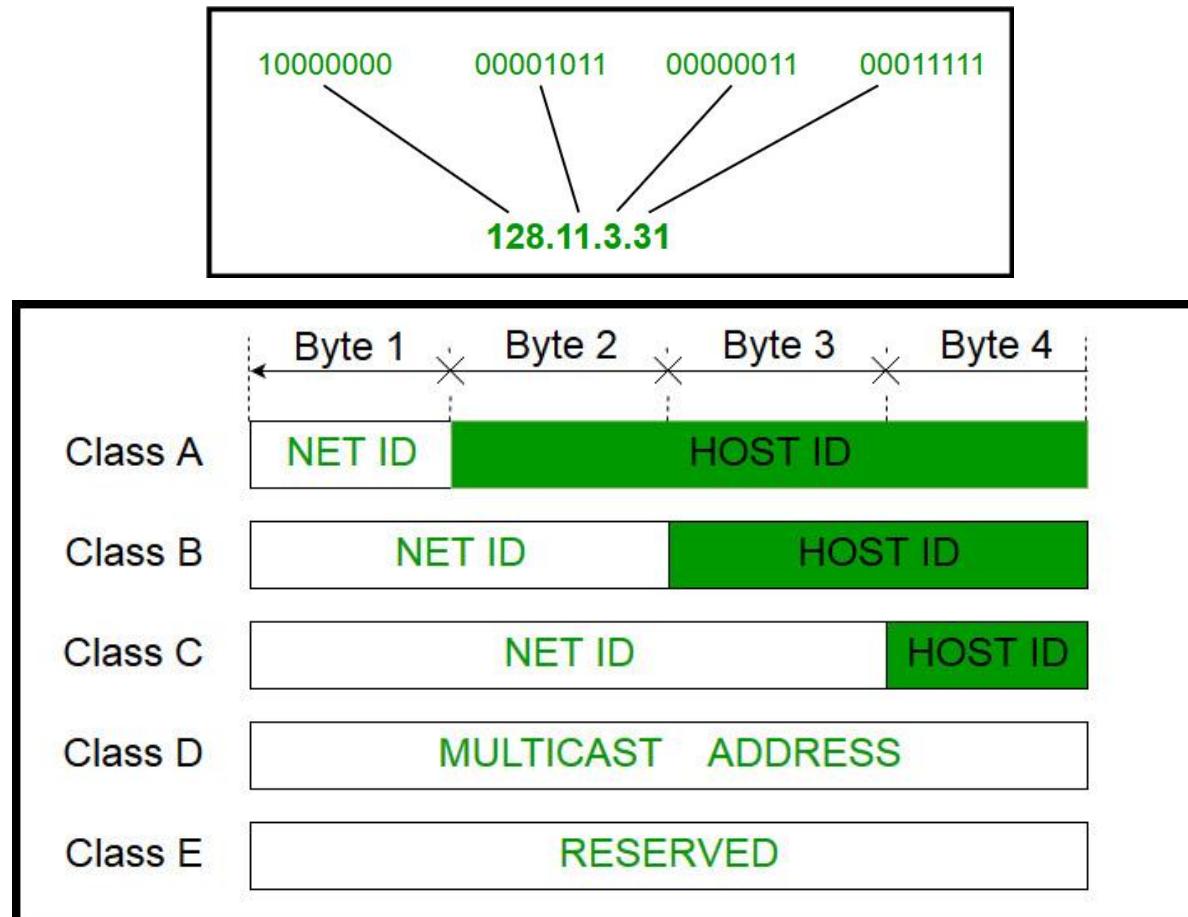
TOOLBOX™ KEY DIFFERENCES BETWEEN TCP AND UDP FOR ORGANIZATIONS



<https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/>

IP Address

IP 주소란 인터넷 프로토콜 주소의 줄임말로, 네트워크에 연결된 장치를 식별하는 고유한 숫자 주소입니다. IP 주소는 컴퓨터와 기타 디바이스가 인터넷에서 서로를 찾고 통신할 수 있도록 합니다.



<https://www.geeksforgeeks.org/introduction-of-classful-ip-addressing/>

<https://www.avast.com/c-what-is-an-ip-address>

Public vs Private IP Address

IP 주소는 그 용도에 따라 Public과 Private으로 나눌 수 있습니다.

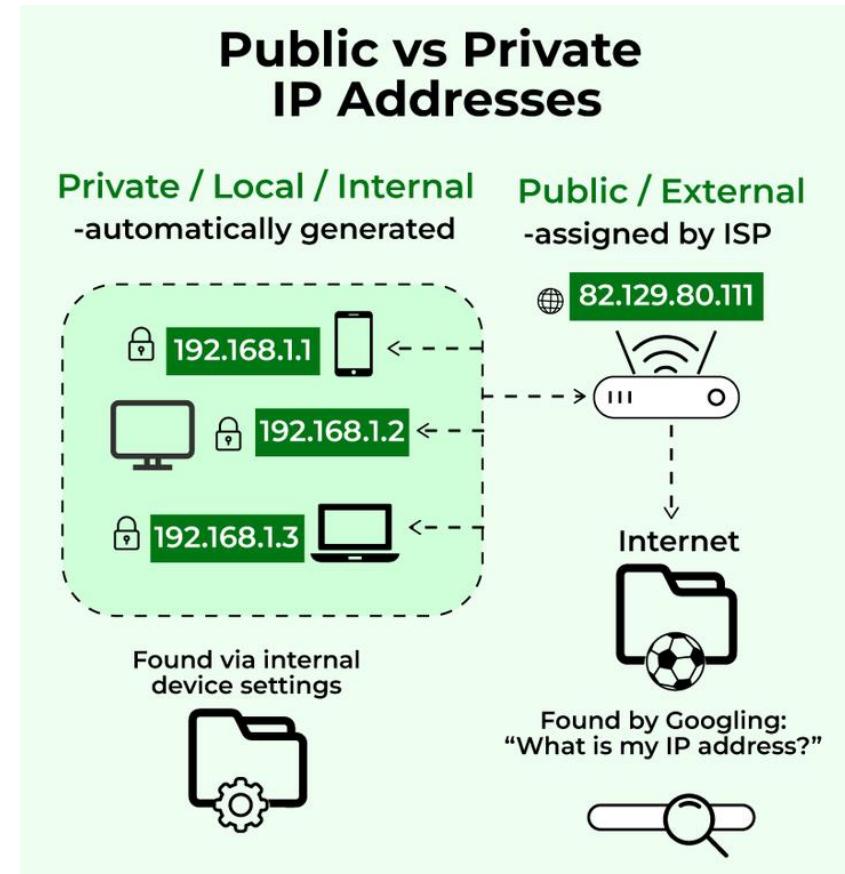
- 용도: Public IP는 인터넷 통신용, Private IP는 내부 네트워크 통신용
- 할당 주체: Public IP는 ISP가 할당, Private IP는 네트워크 관리자가 할당
- 고유성: Public IP는 전 세계적으로 고유, Private IP는 네트워크 내에서만 고유
- 접근성: Public IP는 인터넷에서 직접 접근 가능, Private IP는 NAT 등의 기술을 통해 간접적으로만 접근 가능
- 보안: Private IP는 외부에서 직접 접근할 수 없어 상대적으로 더 안전

Class A Private IP Range: 10.0.0.0 – 10.255.255.255

Class B Private IP Range: 172.16.0.0 – 172.31.255.255

Class C Private IP Range: 192.168.0.0 – 192.168.255.255

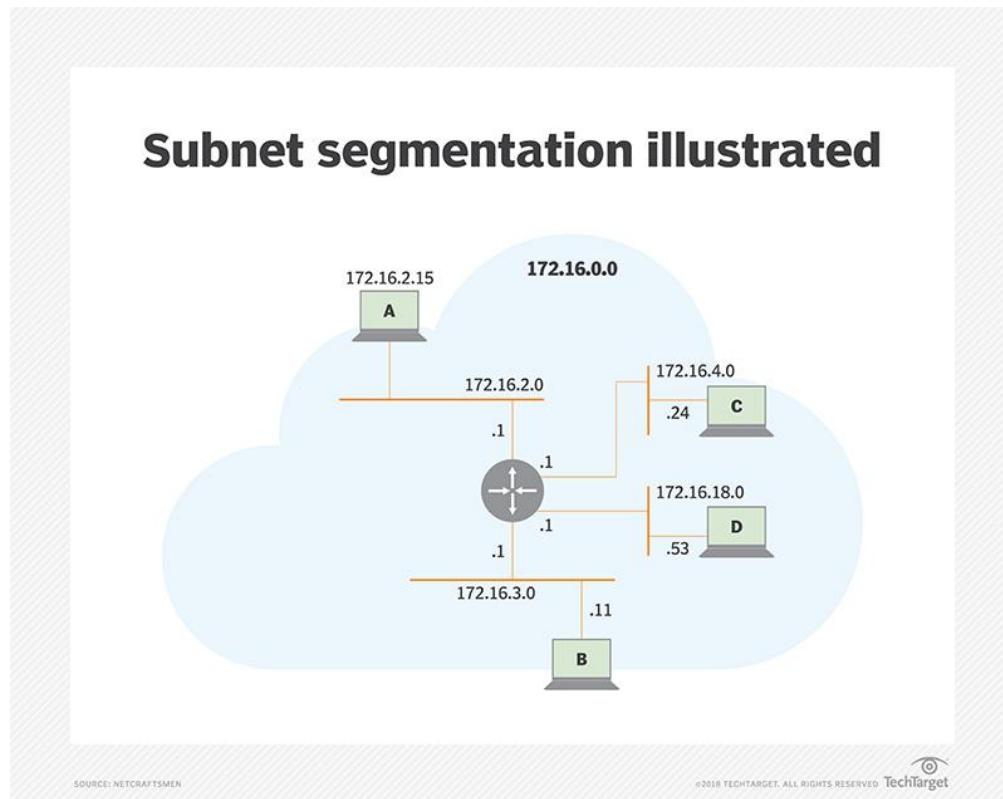
Let's Check your IP with ipconfig (Windows) or ifconfig (POSIX)



<https://www.geeksforgeeks.org/difference-between-private-and-public-ip-addresses/>

Subnetworking

Subnetworking(서브네트워킹)은 큰 네트워크를 더 작은 논리적 세그먼트로 나누는 과정입니다.



<https://www.techtarget.com/searchnetworking/definition/subnet>

Ask  perplexity

Subnetworking

작동원리

- IP 주소 공간을 더 작은 단위로 분할
- 서브넷 마스크를 사용하여 IP 주소의 네트워크 부분과 호스트 부분을 구분
- 각 서브넷은 고유한 IP 주소 범위를 할당 받음

주요 이점

- 네트워크 성능 향상: 불필요한 트래픽을 줄여 네트워크 혼잡을 감소
- 보안 강화: 네트워크를 분리하여 보안 위협의 확산을 제한
- IP 주소 관리 효율화: 제한된 IP 주소를 더 효율적으로 할당, 관리
- 라우팅 최적화: 데이터 패킷이 최적의 경로로 이동
- 네트워크 관리 단순화: 논리적 그룹화를 통해 네트워크 관리 용이

CIDR Notation

CIDR(Classless Inter-Domain Routing) Notation은 IP 주소와 네트워크 프리픽스를 간결하게 표현하는 방법입니다.

NetworkProGuide CIDR/IPv4 Cheat Sheet				
Subnets			Classful Ranges	
CIDR	Subnet Mask	# of Addresses	Wildcard	A 0.0.0.0 - 127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255	B 128.0.0.0 - 191.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255	C 192.0.0.0 - 223.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255	D 224.0.0.0 - 239.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255	E 240.0.0.0 - 255.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255	
/5	248.0.0.0	134,217,728	7.255.255.255	
/6	252.0.0.0	67,108,664	3.255.255.255	RFC 1918 10.0.0.0 - 10.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255	localhost 127.0.0.0 - 127.255.255.255
/8	255.0.0.0	16,777,216	0.255.255.255	RFC 1918 172.16.0.0 - 172.31.255.255
/9	255.128.0.0	8,388,608	0.127.255.255	RFC 1918 192.168.0.0 - 192.168.255.255
/10	255.192.0.0	4,194,304	0.63.255.255	
/11	255.224.0.0	2,097,152	0.31.255.255	
/12	255.240.0.0	1,048,576	0.15.255.255	
/13	255.248.0.0	524,288	0.7.255.255	
/14	255.252.0.0	262,144	0.3.255.255	
/15	255.254.0.0	131,072	0.1.255.255	
/16	255.255.0.0	65,536	0.0.255.255	
/17	255.255.128.0	32,768	0.0.127.255	
/18	255.255.192.0	16,384	0.0.63.255	
/19	255.255.224.0	8,192	0.0.31.255	
/20	255.255.240.0	4,096	0.0.15.255	
/21	255.255.248.0	2,048	0.0.7.255	
/22	255.255.252.0	1,024	0.0.3.255	
Decimal to Binary				
/23	255.255.254.0	512	0.0.1.255	Subnet Mask Wildcard
/24	255.255.255.0	256	0.0.0.255	0 0000 0000 255 1111 1111
/25	255.255.255.128	128	0.0.0.127	128 1000 0000 127 0111 1111
/26	255.255.255.192	64	0.0.0.63	192 1100 0000 63 0011 1111
/27	255.255.255.224	32	0.0.0.31	224 1110 0000 31 0001 1111
/28	255.255.255.240	16	0.0.0.15	240 1111 0000 15 0000 1111
/29	255.255.255.248	8	0.0.0.7	248 1111 1000 7 0000 0111
/30	255.255.255.252	4	0.0.0.3	252 1111 1100 3 0000 0011
/31	255.255.255.254	2	0.0.0.1	254 1111 1110 1 0000 0001
/32	255.255.255.255	1	0.0.0.0	255 1111 1111 0 0000 0000

<https://networkproguide.com/cidr-subnet-mask-ipv4-cheat-sheet/>



Subnetworking

기본 구조

- IP 주소 뒤에 슬래시(/)를 붙이고 네트워크 비트수 표기
- 예: 192.168.1.0/24

작동 원리

- 슬래시 뒤의 숫자는 네트워크 프리픽스의 비트 수
- 남은 비트는 호스트 부분을 의미

장점

- IP 주소 할당의 유연성 증가 (필요한 만큼만 할당 가능)
- 라우팅 테이블 크기 감소
- 효율적 IP 주소 사용

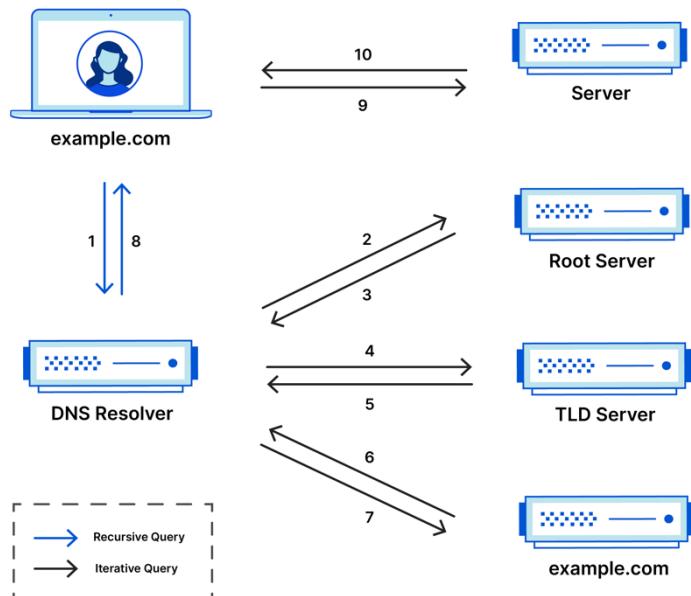
예시

- 192.168.1.0/24의 경우
- 사용 가능한 IP 주소: 192.168.1.0 – 192.168.1.255

DNS (Domain Name System)

DNS(Domain Name System)는 인터넷의 핵심 인프라 중 하나로, 도메인 이름을 IP 주소로 변환하는 시스템입니다.

Complete DNS Lookup and Webpage Query



<https://www.cloudflare.com/learning/dns/what-is-dns/>

Ask  perplexity

DNS

목적

- 사람이 읽기 쉬운 도메인 이름을 (예: www.example.com) 컴퓨터가 이해할 수 있는 IP 주소 (예: 192.0.2.1)로 변환

구조

- 계층적이고 분산된 데이터베이스 시스템
- 전 세계에 분산된 DNS 서버들이 협력하여 작동

주요 구성 요소

- DNS Resolver: 클라이언트 쿼리를 받아 처리하는 서버
- Root DNS Server: 최상위 도메인 정보 관리
- TLD(Top-Level Domain) 서버: .com, .org 등 최상위 도메인 관리
- 권한있는 네임서버: 특정 도메인의 DNS 레코드를 직접 관리

DNS record

DNS 레코드는 도메인 이름 시스템(DNS)에서 도메인 이름에 대한 정보를 제공하는 데이터베이스 항목입니다. DNS 레코드는 사람이 읽을 수 있는 도메인 이름(예: example.com)을 컴퓨터가 네트워크에서 서로를 식별하는 데 사용하는 IP 주소(예: 192.0.2.1)로 변환하는 데 도움을 줍니다.

NAME	TYPE	TTL	VALUE
@	NS	172800	ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info.
@	SOA	3600	Email: msnhost.microsoft.com Host: ns1-01.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 2016031500
txt	TXT	3600	The quick brown fox jumps over the la... ...
www	A	300	1.2.3.4 ...

Ask  perplexity

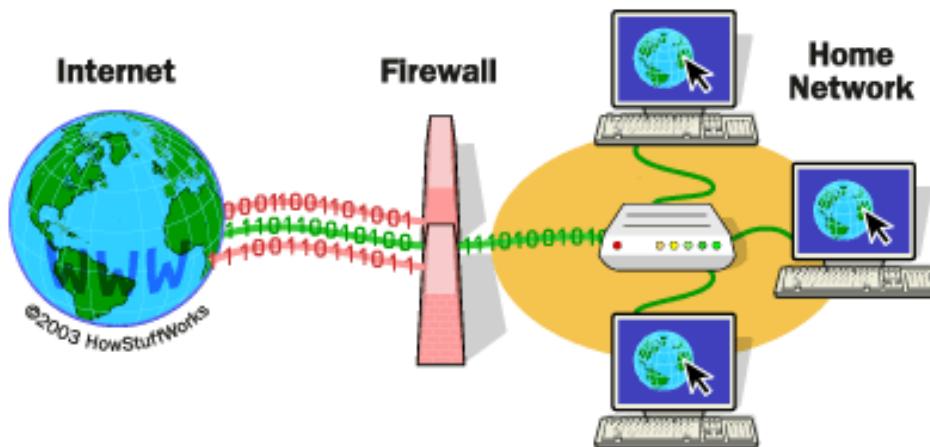
DNS

일반적인 레코드 유형

- A 레코드:** 도메인 이름을 IPv4 주소에 매핑합니다.
- AAAA 레코드:** 도메인 이름을 IPv6 주소에 매핑합니다.
- CNAME 레코드:** 다른 도메인 이름의 별칭을 제공하여 여러 도메인이 단일 IP 주소를 가리키도록 합니다.
- MX 레코드:** 도메인을 위한 메일 교환 서버를 지정합니다.
- TXT 레코드:** 도메인 소유자가 DNS에 텍스트를 삽입할 수 있게 합니다. 주로 검증 및 보안 목적으로 사용됩니다.

Firewall

컴퓨터에서 방화벽은 네트워크의 보안 담당자와 같습니다. 주된 역할은 컴퓨터나 네트워크로 들어오고 나가는 트래픽을 제어하는 것입니다.



<https://www.comodo.com/resources/home/how-firewalls-work.php>

Ask  perplexity

Firewall

원치 않는 접근 차단

- 방화벽은 데이터 패킷(정보의 조각)을 확인하고, 설정한 규칙에 따라 허용할지 차단할지를 결정

위협으로부터 보호

- 악성 소프트웨어(바이러스나 해커 등)가 시스템을 손상시키거나 정보를 훔치는 것을 막는 데 도움

하드웨어와 소프트웨어

- 하드웨어 방화벽: 네트워크와 인터넷 사이에 위치한 물리적 장치
- 소프트웨어 방화벽: 컴퓨터에 설치된 프로그램으로, 트래픽을 모니터링하고 제어

Port

컴퓨터 네트워크에서 포트는 장치 내의 특정 프로세스나 서비스를 식별하는 통신 끝점입니다.



<https://infinity-cable-products.com/blogs/hardware/what-is-an-ethernet-port>

Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

Ask  perplexity

Port

숫자 식별자

- 포트는 0에서 65535까지의 숫자로 식별
 - 잘 알려진 포트 (0-1023): 일반적인 프로토콜에 사용
(예: HTTP는 포트 80, HTTPS는 포트 443 사용)
 - 등록된 포트 (1024-49151): 사용자 애플리케이션과 프로세스에 사용
 - 동적 또는 개인 포트 (49152-65535): 임시 연결에 사용

프로토콜 연관성

- 포트는 프로토콜(TCP or UDP 등)과 함께 작동하여 통신 설정.
예: 웹 서버는 HTTP 요청을 수신하기 위해 포트 80에서 대기

데이터 라우팅

- 데이터 패킷이 장치에 도착하면, 패킷 헤더의 포트 번호가 운영 체제에 어떤 애플리케이션이나 서비스가 데이터를 처리해야 하는지를 알려줌

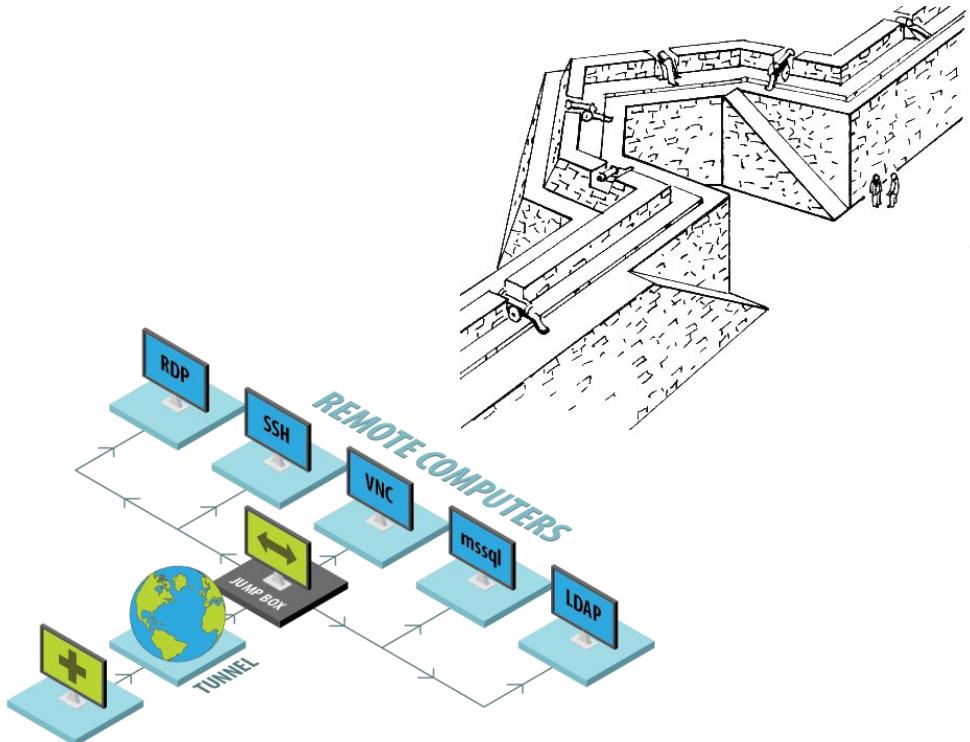
Ingress / Egress

Ingress와 Egress 단어 뜻 그대로 네트워크 트래픽이 들어오고 나가는 것을 말합니다.



Jump Box, Jump Server, Bastion Host

우리말로 요새를 뜻하는 Bastion의 단어 뜻에서 알 수 있듯이, Jump box/Jump server/Bastion Host는 보안 네트워크 (내부)와 외부 네트워크 사이의 게이트웨이 역할을 하는 컴퓨터입니다.



<https://help.islonline.com/56320/374626>

Ask  perplexity

Jump Box

목적

- 보안 액세스: 제어된 액세스 지점을 제공하여 승인된 사용자만 연결 가능. 그리고는 내부 시스템 액세스 가능
- 격리: 내부 리소스를 직접적인 액세스로 분리하여 공격 줄임

기능

- 인증: 사용자는 일반적으로 SSH 키 또는 다단계 인증
- 감사로그: 모든 사용자 활동 기록
- 액세스 제어: 특정 사용자나 IP 주소만 연결할 수 있도록 엄격한 액세스 제어 가능

배치

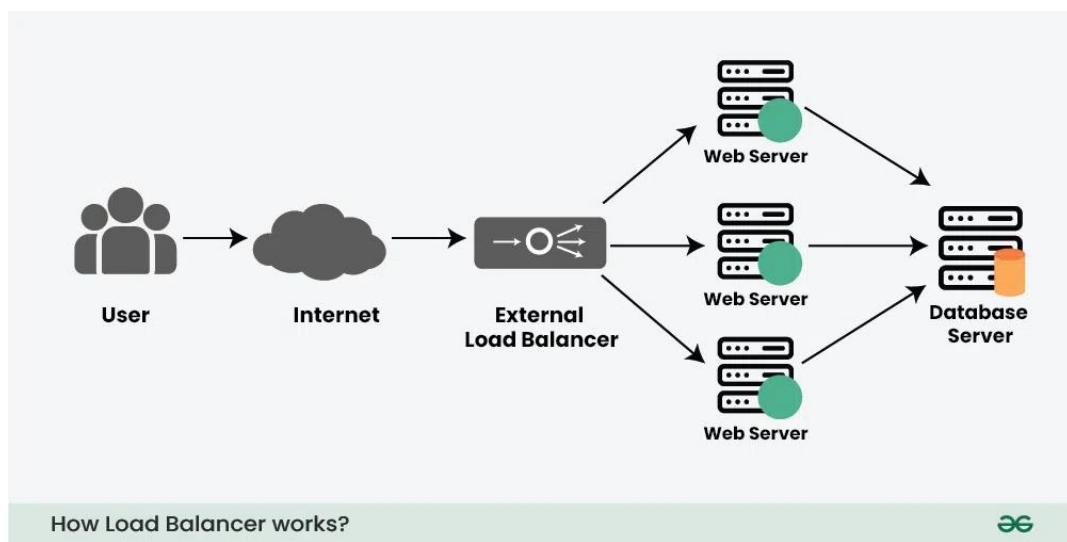
- 일반적으로 DMS에 배치되거나 인터넷에 직접 노출. 내부 시스템은 방화벽 뒤

사례

- 원격 근무 혹은 원격 관리

Load balancer

로드 밸런서(Load Balancer)는 네트워크 트래픽을 여러 서버에 균등하게 분산시키는 장치 또는 소프트웨어입니다.



Ask perplexity

Load balancer

클라이언트와 서버 그룹 사이에 위치하여 들어오는 트래픽을 여러 서버에 고르게 분배합니다

- 특정 서버의 과부하 방지
- 전체 시스템의 가용성 및 응답 시간 향상
- 서비스의 안정성 제고

유형

- L4 로드 밸런서: Transport layer에서 동작하며 IP 주소와 포트 번호를 기반으로 단순히 부하 분산
- L7 로드 밸런서: Application layer에서 동작하며 HTTP 헤더, URL, 쿠키 등의 정보를 통해 세밀한 트래픽 제어 가능

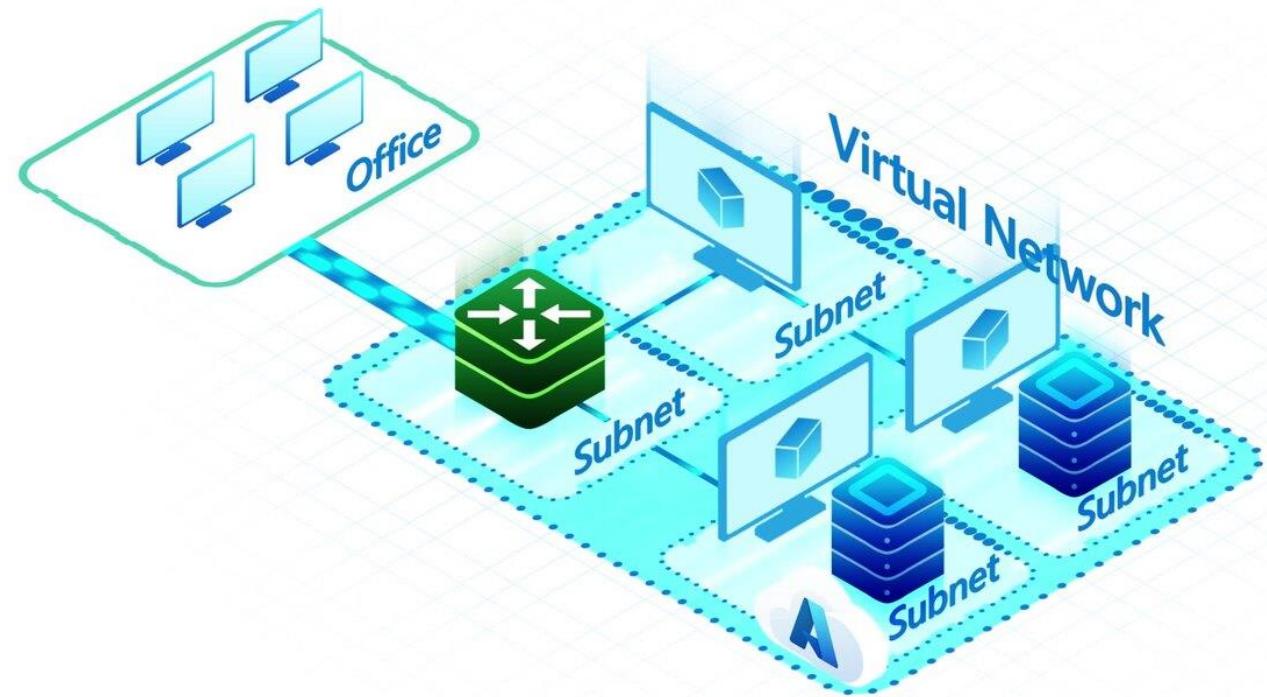
트래픽 출처에 따라

- 외부 로드 밸런서: 인터넷 트래픽을 내부 서버로 분산
- 내부 로드 밸런서: 내부 네트워크에서 트래픽 분산

Cloud specific Networking

What is Azure Virtual Network?

Azure 가상 네트워크는 Azure에서 사설 네트워크를 구축하기 위한 기본적인 구성 요소를 제공하는 서비스입니다. 이 서비스의 인스턴스(가상 네트워크)는 다양한 유형의 Azure 리소스 (예: 가상 머신)가 내부적으로 또는 인터넷 및 온-프레미스 네트워크와 안전하게 통신할 수 있도록 합니다.

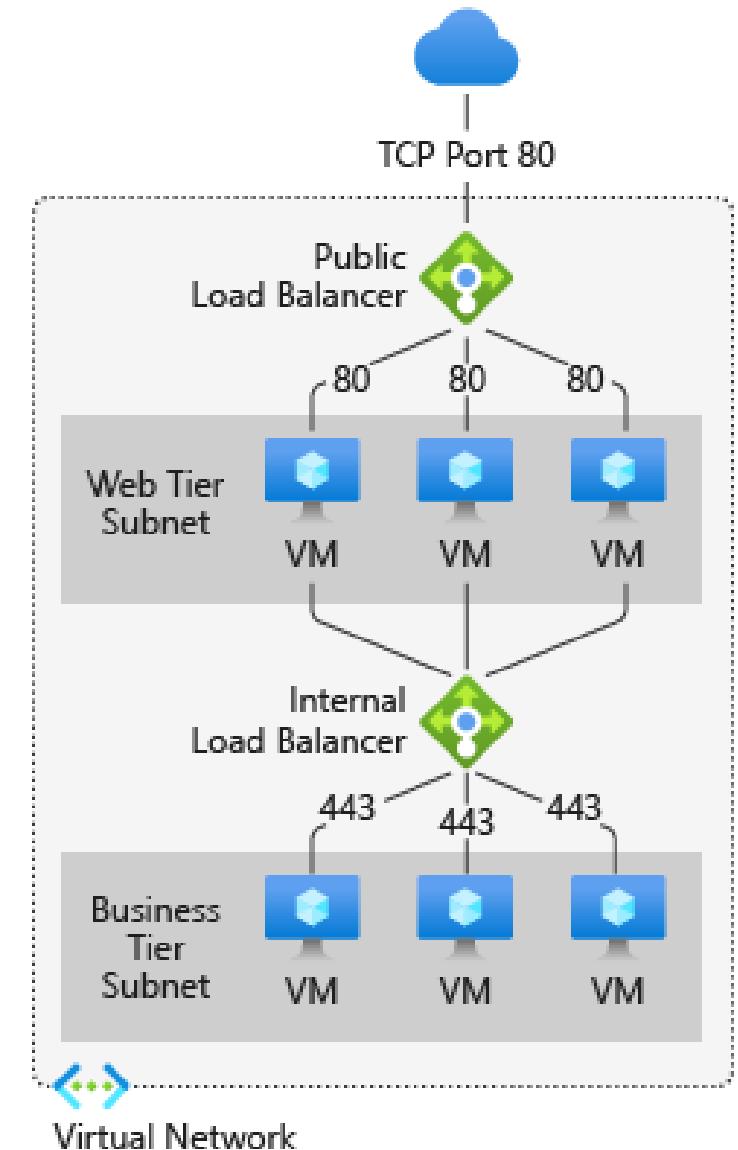


https://learn.microsoft.com/_themes/docs.theme/master/en-us/_themes/global/video-embed.html?id=6b5b138e-8406-406e-8b34-40bdadfc6d&locale=en-us&embedUrl=%2Fazure%2Fvirtual-network%2Fvirtual-networks-overview

Azure Virtual Network

Azure Virtual Network는 Azure의 프라이빗 네트워크에 대한 기본 구성 요소를 제공하는 서비스입니다. 서비스 인스턴스(가상 네트워크)를 사용하면 다양한 종류의 Azure 리소스에서 서로, 인터넷 및 온-프레미스 네트워크와 안전하게 통신할 수 있습니다. 이러한 Azure 리소스에는 VM(가상 머신)이 포함됩니다.

- Azure DNS: 자체 DNS 도메인 관리
- Virtual Network (vNET): Azure 네트워크의 논리적으로 분리된 셕션
- Network Security Groups: 서브넷 또는 NIC레벨의 가상 방화벽
- ExpressRoute: 온프레미스에서 VNET으로의 50 Mbps-10 Gbps 연결
- Virtual WAN: 다양한 네트워크 연결을 라우팅하는 중앙 집중식 네트워크
- Virtual Network Gateway: VNet과 로컬 네트워크 간의 사이트 간 VPN 연결
- Network Interfaces: IP 프로토콜을 사용하여 VM이 통신할 수 있도록 하는 가상 네트워크 장치

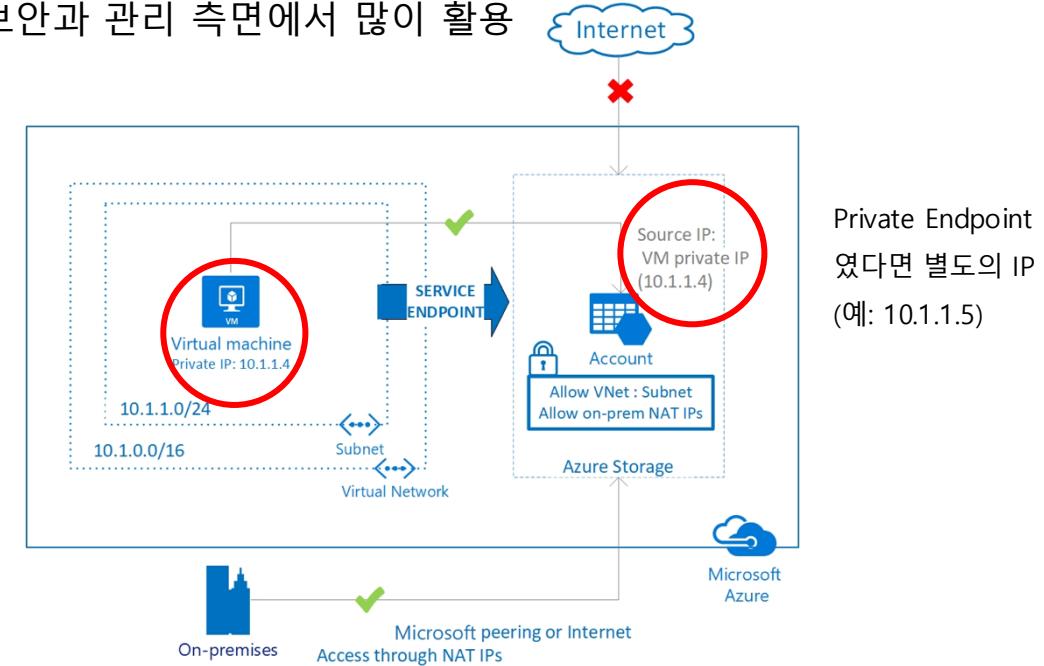


Azure Service Endpoint

가상 네트워크(VNet) 내 리소스가 인터넷을 거치지 않고, 전용 경로(Azure 백본)를 통해 PaaS 서비스에 안전하게 연결할 수 있도록 하는 기능입니다.

- Azure 서비스 엔드포인트(Azure Service Endpoint)는 Azure 가상 네트워크(VNet) 내 리소스가 Azure PaaS 서비스(예: Azure Storage, Azure SQL Database 등)에 **인터넷을 거치지 않고 Azure 백본 네트워크를 통해 직접 안전하게 연결할 수 있도록 해주는 기능**
- 이를 통해 **가상 네트워크 내부에서 해당 Azure 서비스로 가는 트래픽이 Azure 공용 인터넷을 통하지 않고 전용 경로로 처리되어 보안과 성능이 향상됨**
- 서비스 엔드포인트는 가상 네트워크의 특정 서브넷에서 설정하며, 해당 서브넷 내의 리소스가 해당 서비스에 직접 접근할 수 있도록 허용

서비스 엔드포인트는 주로 Azure Storage, SQL Database, Key Vault, Event Hubs, Service Bus 등 다양한 Azure 관리형 서비스에 적용할 수 있어 네트워크 보안과 관리 측면에서 많이 활용



<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

NOTE: 이와 대비되는 개념인 Private Endpoint은 PaaS 서비스에 우리 가상 네트워크의 사설 IP(Private IP)를 직접 부여하여, 외부 서비스를 마치 내부 리소스처럼 연결하는 방식입니다.

Subnet

서브넷(Subnet)은 **큰 네트워크를 더 작은 네트워크로 나누는 것을 말합니다.** 이를 통해 네트워크를 효율적으로 관리하고, 트래픽을 분산시키며, 보안을 강화할 수 있습니다. 각 서브넷은 자체 IP 주소 범위를 가지며, 이를 통해 네트워크 자원을 논리적으로 분리하고 조직의 필요에 맞게 구성할 수 있습니다.

Subnet in Azure

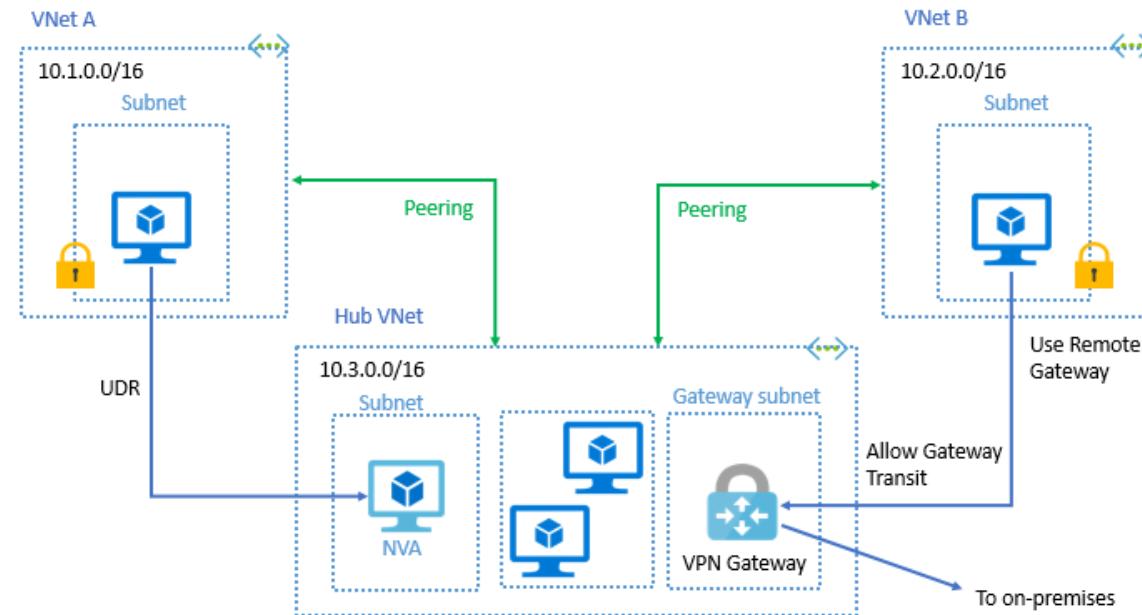
- 서브넷은 가상 네트워크를 하나 이상의 서브넷으로 분할하고, 각 서브넷에 가상 네트워크 주소 공간의 일부를 할당할 수 있게 해줍니다. 그런 다음 특정 서브넷에 Azure 자원을 배포할 수 있습니다.
- 전통적인 네트워크와 마찬가지로 서브넷을 사용하면 가상 네트워크 주소 공간을 조직의 내부 네트워크에 적합한 세그먼트로 분할할 수 있습니다.
- 세분화(Segmentation)는 주소 할당 효율성을 향상시킵니다.
- 네트워크 보안 그룹을 사용하여 서브넷 내 자원을 보호할 수 있습니다.

Public vs Private?

- Public 및 Private subnet은 외부 인터넷으로부터 접근이 가능한지 여부에 따라 나뉨
- Azure는 현재까지는 private과 public subnet을 별도로 나누지 않고, 구성을 어떻게 하는가에 따라 외부 인터넷 접근 여부를 결정하였음
- Private Subnet이라는 기능이 현재 preview 단계에 있어서 향후에는 이 기능이 공식적으로 반영이 될 수 있음

VNet Peering (가상 네트워크 피어링)

가상 네트워크 피어링을 사용하면 Azure에서 두 개 이상의 가상 네트워크를 원활하게 연결할 수 있습니다. 가상 네트워크는 연결하기 위해 **하나로 표시됩니다**. 피어링된 가상 네트워크에 있는 가상 머신 간의 트래픽은 Microsoft 백본 인프라를 사용합니다. 동일한 네트워크에 있는 가상 컴퓨터 간의 트래픽과 마찬가지로 트래픽은 Microsoft 개인 네트워크만을 통해 라우팅됩니다.



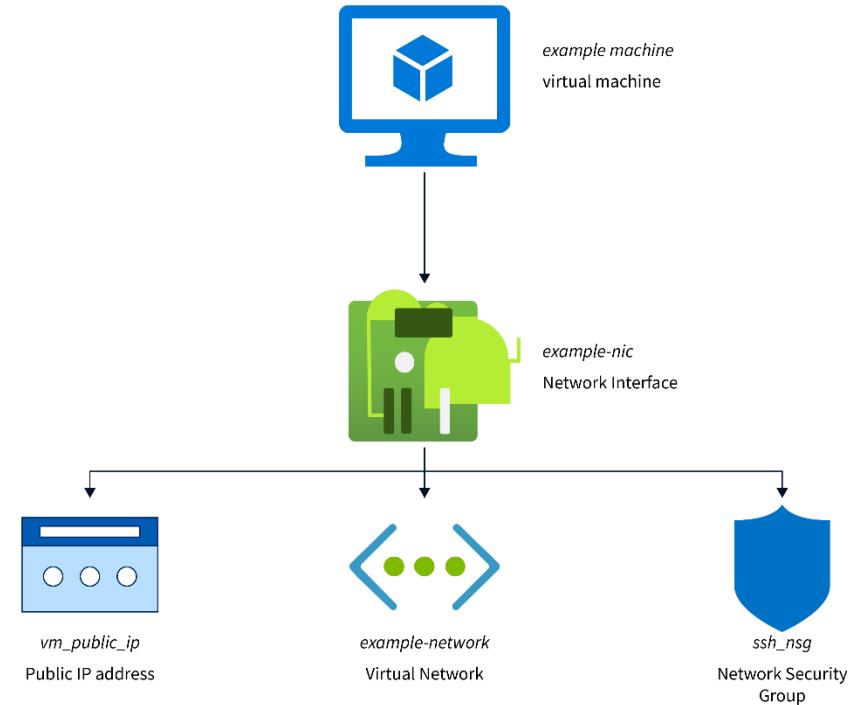
- Regional Vnet Peering: 하나의 영역 내에서 2개의 vNet을 피어링
- Global Vnet Peering: 2개의 서로 다른 영역에서 vNet을 피어링

Network Interface

네트워크 인터페이스는 컴퓨터와 사설 또는 공용 네트워크 간의 연결 지점입니다. 하드웨어 기반(예: 컴퓨터의 네트워크 인터페이스 카드(NIC)) 또는 소프트웨어 기반(예: 가상화 환경의 가상 NIC)일 수 있습니다.

Azure 네트워크 인터페이스(NIC)

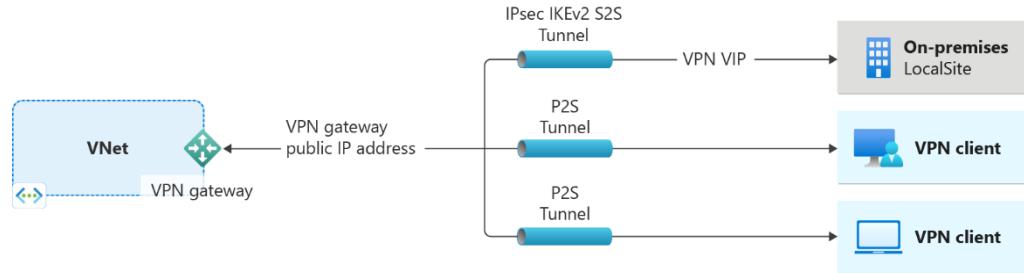
- Azure 가상 머신(VM)이 서로, 인터넷, 그리고 온프레미스 네트워크와 IP 프로토콜을 사용하여 통신할 수 있도록 하는 가상 네트워크 장치입니다. Azure의 각 NIC는 여러 IP 주소를 가질 수 있으며, 가상 네트워크(VNet) 내의 다양한 서브 네트에 연결될 수 있습니다. Azure NIC는 VM의 네트워크 구성(IP 주소 지정, 네트워크 보안 그룹 규칙, 관련 로드 밸런서 포함)을 정의하는 데 필수적입니다.



<https://www.scaler.com/topics/azure/network-interface-in-azure/>

Virtual Network Gateways

Azure virtual network에서 제공하는 소프트웨어 VPN입니다.



- Azure VPN Gateway는 공용 인터넷을 통해 Azure 가상 네트워크와 온-프레미스간에 **암호화된 트래픽**을 보내는 데 사용할 수 있는 서비스입니다. VPN Gateway를 사용하여 Microsoft 네트워크를 통해 Azure 가상 네트워크 간에 암호화된 트래픽을 보낼 수도 있습니다.
- VPN Gateway는 VPN Gateway라는 특정 유형의 Azure 가상 네트워크 게이트웨이를 사용합니다. 동일한 VPN Gateway에 여러 연결을 만들 수 있습니다. 여러 연결을 만들 때 모든 VPN 터널은 사용 가능한 게이트웨이 대역폭을 공유합니다.



VPN(가상 사설 네트워크, Virtual Private Network)은 공용 네트워크(예: 인터넷)를 통해 개인 네트워크를 안전하게 연결하는 기술입니다. VPN을 사용하면 **데이터가 암호화되어 전송**되므로, **원격지에서 안전하게 내부 네트워크에 접근**할 수 있습니다. 이를 통해 사용자는 외부에서 내부 네트워크 자원에 안전하게 접근하거나 인터넷 활동을 보호할 수 있습니다. VPN을 사용하기 위해서는 터널링 프로토콜, 암호화, 인증, IPSec과 같은 기술이 필요합니다.

Azure DNS

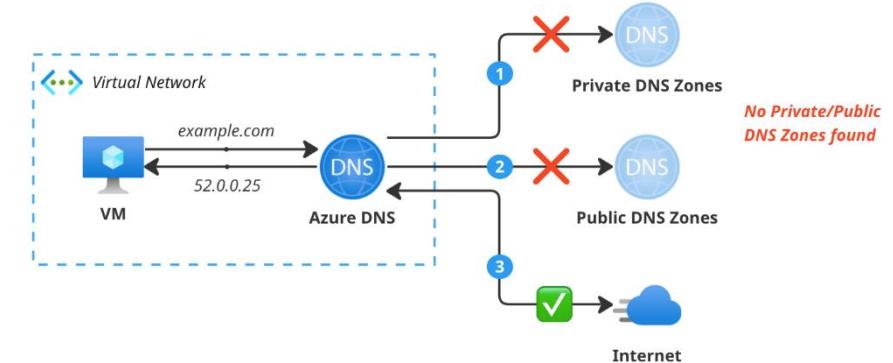
Azure DNS는 Microsoft Azure 인프라를 사용하여 DNS hosting, resolution 및 load balancing을 제공하는 클라우드 기반 도메인 네임 시스템 서비스입니다.

Ask **ChatGPT**

What is Azure DNS?

4가지 주요 구성 요소

- Azure 공용 DNS:** 인터넷에서 접근 가능한 DNS 도메인을 위한 호스팅 서비스로, 다른 Azure 서비스와 동일한 자격 증명, API, 도구 및 대금 청구를 사용하여 DNS 레코드를 관리. 이를 통해 웹사이트와 API 같은 공용 도메인을 전 세계에서 호스팅할 수 있음
- Azure 프라이빗 DNS:** 사용자 지정 DNS 솔루션 없이 가상 네트워크 내에서 도메인 이름 확인을 관리하며, 가상 머신과 같은 내부 도메인 이름과 리소스를 처리. 이 서비스는 **공개되어서는 안 되는 리소스**에 대한 안전한 DNS 확인을 제공
- Azure DNS Private Resolve:** VM 기반 DNS 서버를 배포하지 않고도 온-프레미스 환경에서 Azure DNS 프라이빗 영역을 쿼리하거나 그 반대로 쿼리할 수 있는 **하이브리드 클라우드 시나리오**를 지원하는 서비스
- Azure Traffic Manager:** DNS 기반 트래픽 로드 밸런서로 작동하여 공용 애플리케이션에 대한 트래픽을 전 세계 Azure 지역에 분산



<https://loth.io/posts/everything-you-need-to-know-about-azure-dns/>

Azure Traffic Manager

Azure Traffic Manager는 DNS(Domain Name System) 기반의 트래픽 부하 분산 장치입니다. 전 세계 Azure 지역에 분산된 공용 애플리케이션으로 들어오는 트래픽을 효율적으로 분산하는 역할을 합니다. 이를 통해 애플리케이션의 가용성과 응답성을 높일 수 있습니다.

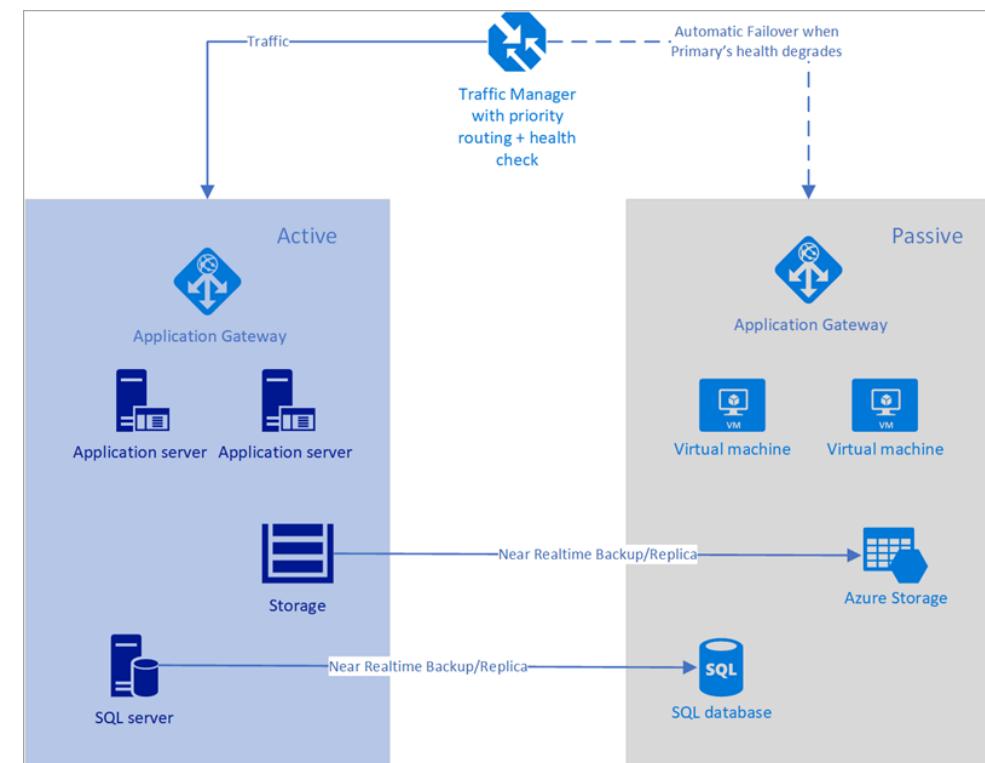
핵심 기능

- 애플리케이션 가용성 향상: 엔드포인트를 지속적으로 모니터링하고, 장애 발생 시 자동으로 트래픽을 다른 정상 엔드포인트로 보냄
- 애플리케이션 성능 개선: 클라이언트에서 가장 낮은 네트워크 대기 시간을 가진 엔드포인트로 트래픽을 보내 애플리케이션 응답성을 향상
- 무중단 서비스 유지 관리: 계획된 유지 보수 작업 시, 해당 엔드포인트의 트래픽을 다른 곳으로 보내 서비스 중단 없이 작업을 수행
- 하이브리드 애플리케이션 지원: Azure 외부의 온프레미스 또는 다른 클라우드 환경의 엔드포인트도 지원하므로 하이브리드 시나리오에 유용

주요 사용 시나리오

- 글로벌 고가용성
- 재해 복구
- 복잡한 배포의 확장성:

동작 원리



<https://learn.microsoft.com/en-us/azure/reliability/reliability-traffic-manager>

NSG

NSG(Network Security Group)는 Azure 가상 네트워크 내에서 네트워크 트래픽을 제어하는 보안 구성 요소입니다

Ask **ChatGPT**

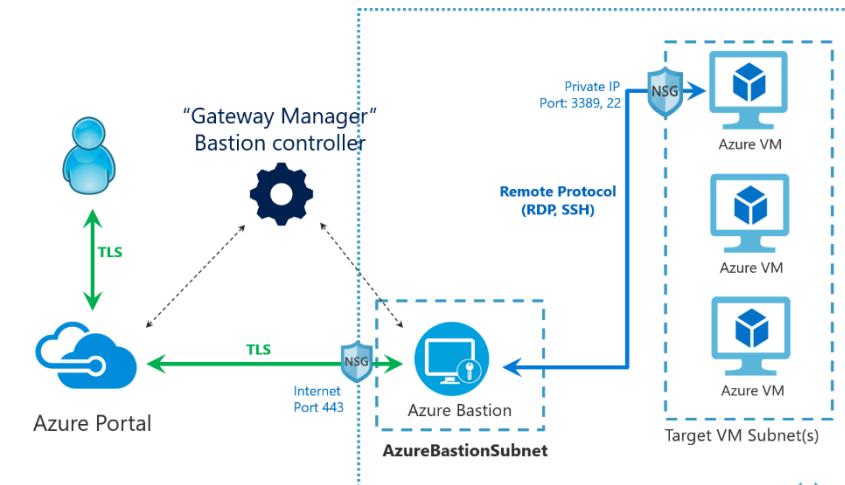
What is Azure NSG?

NSG란?

- NSG는 Azure 리소스와 주고받는 네트워크 트래픽을 필터링하고 제어하는 방화벽(Firewall) 역할을 수행
- 가상 네트워크 서브넷 및 네트워크 인터페이스에서 인바운드와 아웃바운드 트래픽을 모두 관리

Azure Firewall과의 차이는?

- Azure Firewall vs NSG의 핵심 차이는 동작 위치
 - Azure Firewall은 가상 네트워크 진입 시점에서 동작
 - NSG는 가상 머신 진입 시점에서 동작
 - 즉, Azure Firewall이 가장 앞단에서 방어하는 중앙집중식 방화벽이라면, NSG는 각 서브넷이나 VM 레벨의 분산형 방화벽

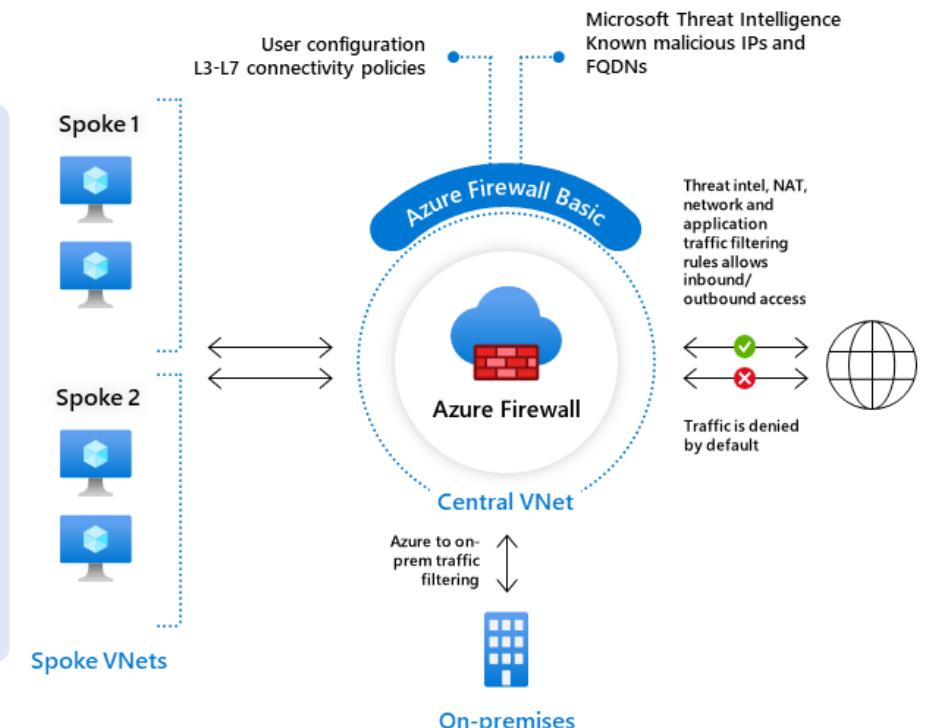


<https://learn.microsoft.com/en-us/azure/bastion/bastion-nsg>

Azure Firewall

Azure Firewall은 Azure 클라우드에서 제공하는 클라우드 네이티브 및 지능형 상태(stateful) 네트워크 방화벽 서비스입니다. Azure Virtual Network 리소스를 보호하기 위해 설계되었으며, 인바운드 및 아웃바운드 트래픽, 내부 네트워크 간 트래픽을 모두 검사하고 필터링합니다. 고가용성과 무제한 클라우드 확장성을 제공하여 대규모 환경에도 적합합니다.

- 완전 관리형 서비스로 중앙에서 정책을 만들어 적용하고 로그를 기록
- 위협 인텔리전스 기반 필터링 기능으로 알려진 악성 IP 및 도메인 차단
- TLS 암호화 트래픽 검사 지원으로 암호화된 연결 내 맬웨어 탐지 가능
- SKU는 기본, 스탠다드, 프리미엄이 있으며, Premium은 서명 기반 침입 탐지 및 고급 위협 방어 기능 포함
- Azure Firewall Manager를 통한 다중 방화벽 정책의 중앙 관리 가능
- 빠른 배포와 자동 크기 조정으로 클라우드 확장성 확보

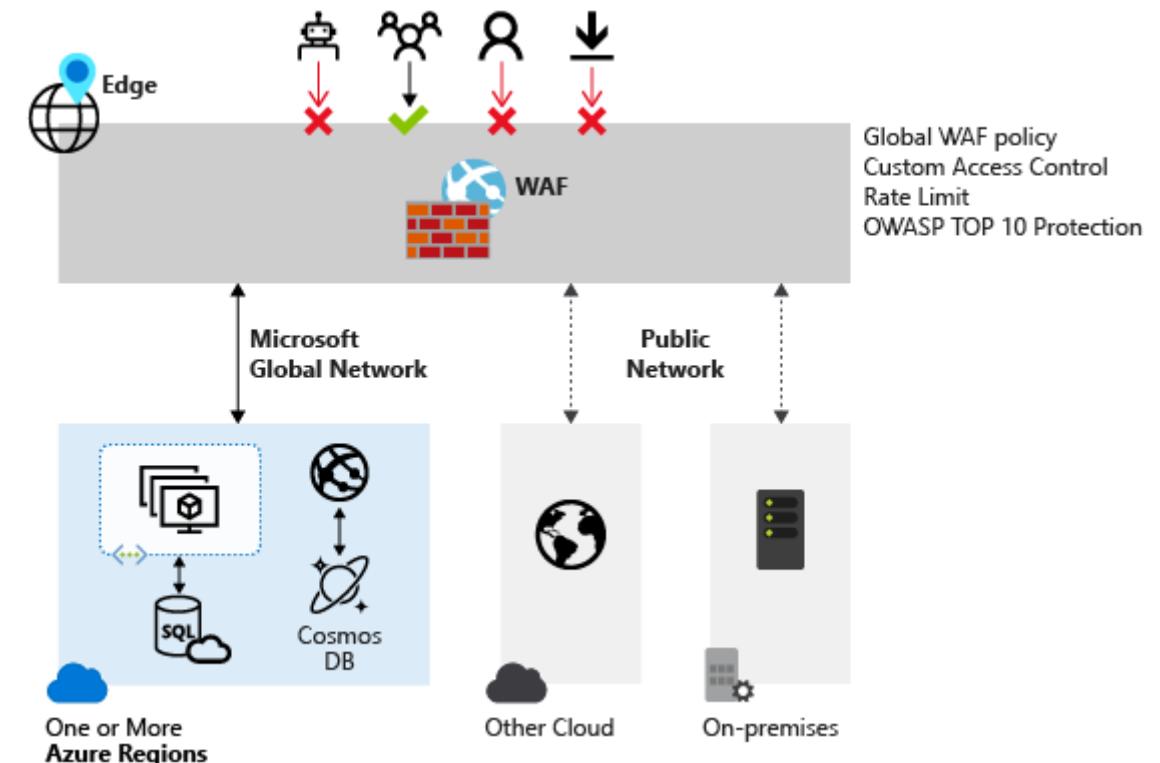


<https://learn.microsoft.com/en-us/azure/firewall/overview>

WAF

Azure Web Application Firewall(Azure WAF)은 웹 애플리케이션을 일반적인 악용과 취약성으로부터 중앙 집중식으로 보호하는 서비스입니다. 웹 애플리케이션이 흔히 노출되는 SQL 인젝션, 크로스 사이트 스크립팅(XSS) 같은 OWASP Top 10 취약점 공격을 탐지하고 차단합니다.

- 웹 애플리케이션에 대한 SQL 인젝션, XSS 등 공격 방어
- OWASP 핵심 규칙 집합 기반의 규칙 적용
- 사용자 정의 및 관리형 규칙 결합 가능
- 여러 웹사이트에 대한 정책 분리 및 맞춤형 보호
- DDoS 방어와 악성 봇 필터링 지원
- Azure Monitor 및 Microsoft Defender와 통합된 실시간 보안 모니터링
- Application Gateway나 Front Door에 옵션으로 붙여서 동작



<https://learn.microsoft.com/ko-kr/azure/web-application-firewall/overview>

Azure Firewall과 WAF의 차이는?

Azure Firewall은 가상 네트워크 차원의 종합 보안 솔루션이고, Azure WAF는 웹 애플리케이션 계층에서 웹 공격을 집중적으로 방어하는 서비스입니다.

구분	Azure Firewall	Azure WAF
주요 목적	네트워크 전체 트래픽 보호	웹 애플리케이션 HTTP/HTTPS 트래픽 보호
적용 계층	L3 ~ L7 (네트워크 및 애플리케이션)	L7 (웹 애플리케이션 계층)
방어 대상	IP, 포트, 프로토콜 기반 필터링	SQL 인젝션, XSS 등 웹 취약점 공격
통합 서비스	Azure Virtual Network 전체보호	Azure Application Gateway, Front Door
주요 기능	상태 저장 방화벽, 위협 인텔리전스, TLS 검사	OWASP 규칙 집합 기반 웹 공격 탐지, 맞춤형 규칙
적용 범위	모든 네트워크 트래픽	웹 서비스 트래픽 한정

[참고] 일상에서 접할 수 있는 VPN

VPN은 과거에는 회사 외부에서 회사 내부 네트워크를 안전하게 사용하기 위한 용도로 많이 사용되었으나, 현재는 접속이 제한된 서버에 우회 접속용으로 사용되고 있으며, 특히 중국 출장 시에 구글 검색 등을 위해서 사용하고 있습니다. 그러나 VPN 서비스를 사용하는 경우에는 많은 주의를 기울여야 합니다.

뉴스홈 | 최신기사

미국 프로그래머, 중국 회사에 일 대신시키다 발각

송고시간 | 2013-01-17 13:25

| 놀면서 자기 연봉 5분의 1만 지급…실적 우수 평가받아

(서울=연합뉴스) 류현성 기자=연간 수십만 달러 이상의 연봉을 받는 미국의 40대 소프트웨어 개발자가 중국의 한 회사에 자기 수입의 5분의 1을 주고 일을 대신하게 하고 자신은 매일 인터넷 서핑만 하다 발각됐다고 영국 텔레그래프 등 외신이 17일 보도했다.

이 같은 사실은 미국의 통신회사인 버라이즌 비즈니스의 한 컴퓨터 범죄 과학수사 요원이 올린 블로그를 통해 알려졌다.

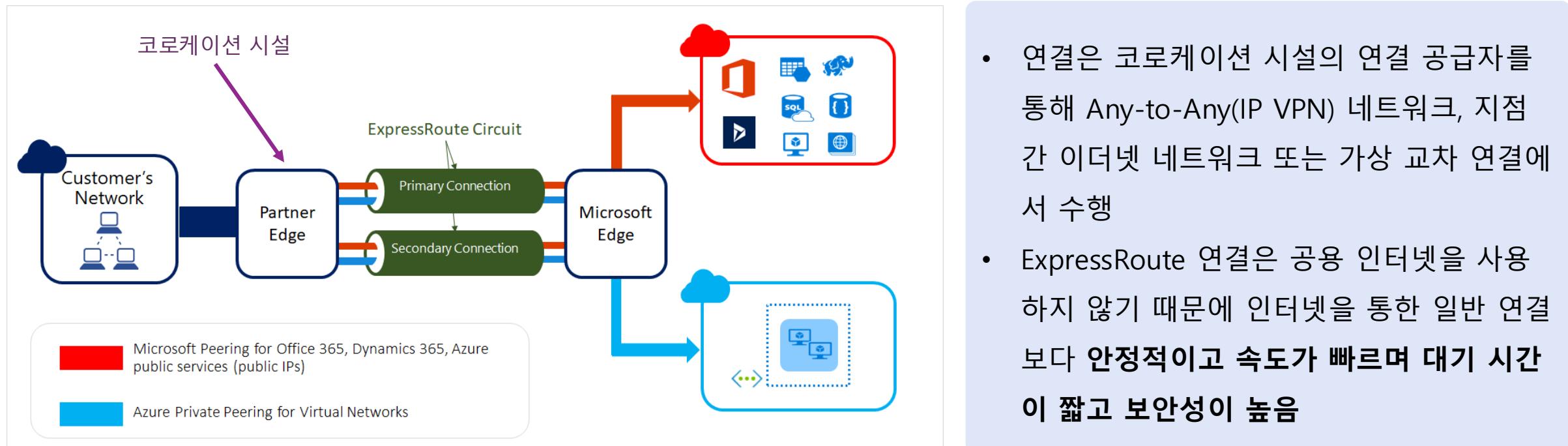
앤드루 벨런타인이라는 이 요원은 이름을 밝히지 않은 한 회사가 중국 선양(瀋陽)에서 누군가 자사 시스템에 들어오려고 시도하고 있다는 것을 인식하고 나서 해킹이 우려된다며 조사를 요청해 왔다고 이

<https://www.yna.co.kr/view/AKR20130117112500009>



Azure ExpressRoute

ExpressRoute를 사용하면 연결 공급자의 도움을 받아 프라이빗 연결을 통해 온-프레미스 네트워크를 Microsoft 클라우드로 확장할 수 있습니다. ExpressRoute를 사용하면 Microsoft Azure 및 Microsoft 365와 같은 Microsoft 클라우드 서비스에 대한 연결을 설정할 수 있습니다.



Private Links

Azure Private Link는 Microsoft Azure에서 제공하는 서비스로, 프라이빗 엔드포인트를 통해 Azure PaaS (Platform as a Service) 서비스, 고객 소유 서비스, 그리고 Microsoft 파트너 서비스에 안전하게 연결할 수 있도록 합니다. 이를 통해 데이터가 공용 인터넷을 통하지 않고 Azure의 가상 네트워크(VNet) 내에서 비공개로 전송되도록 합니다.

- **프라이빗 엔드포인트:** Azure VNet 내에서 특정 Azure 서비스에 연결하는 네트워크 인터페이스로, 해당 서비스와의 연결이 공용 인터넷을 거치지 않고 내부적으로 구성
- **보안 강화:** 데이터가 공용 인터넷을 통하지 않기 때문에 보안이 강화
- **네트워크 격리:** Azure 리소스를 프라이빗 VNet 내에서 격리하여 관리 가능
- **간편한 설정:** Azure Portal, CLI, PowerShell 등을 통해 쉽게 설정 가능

