

# Cloud Infrastructure Operations

---

Day1 - Module3 클라우드 네트워킹

David Yoon | CEO  
david@2miles.co.kr



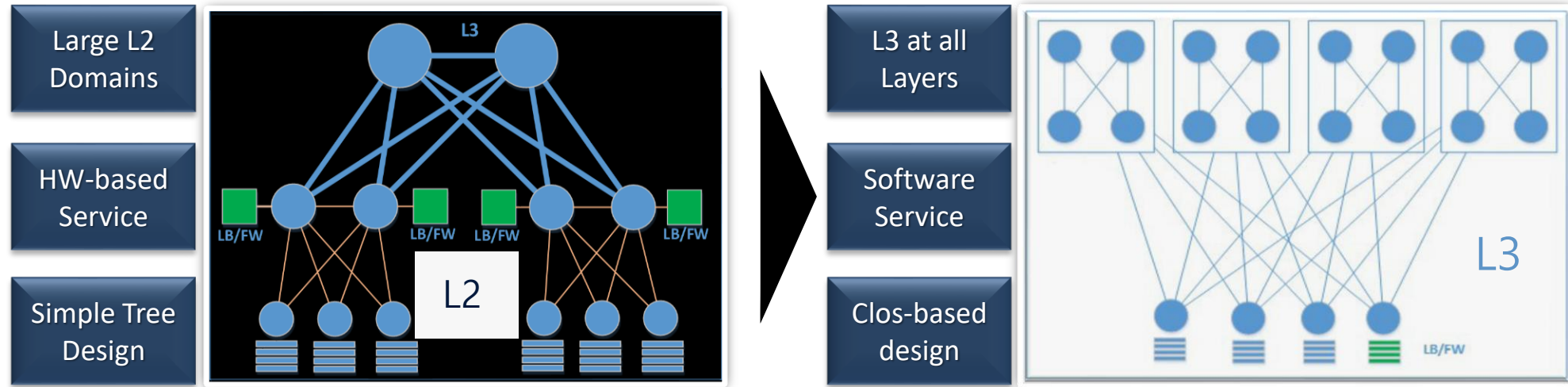


# Azure 네트워크

---



# 전통적인 네트워크 vs 하이퍼 스케일 네트워크



Diversity and manual provisioning

Agility



Automated provisioning, integrated process



Complex hardware and lack of automated operations

Efficiency



Simplify requirements, optimized design, and unify infrastructure



High complexity and human error

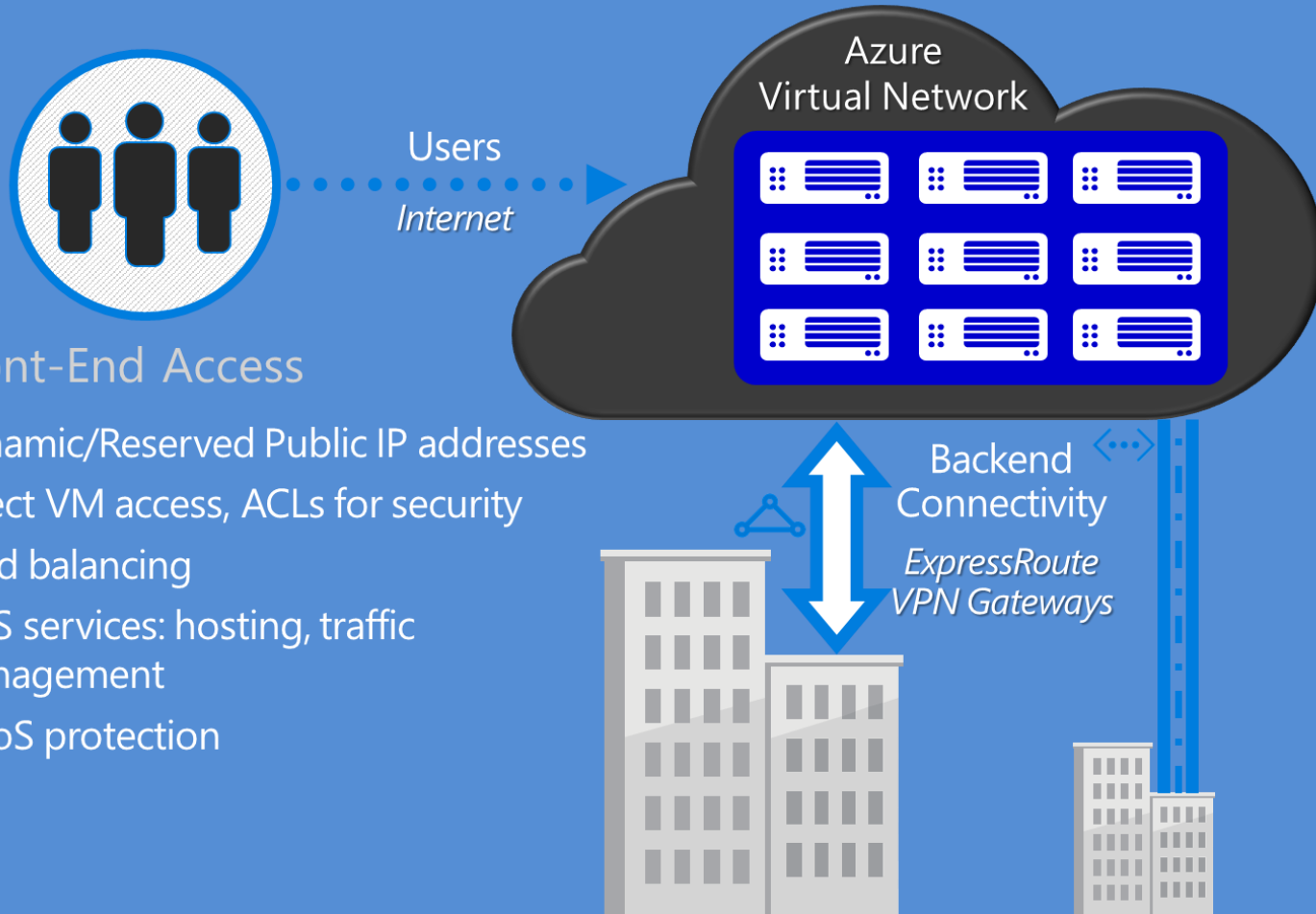
Availability



Resilient, automated monitoring and remediation, low human involvement

# Azure 네트워크 전체 구조

## The Big (Network) Picture



### Front-End Access

- Dynamic/Reserved Public IP addresses
- Direct VM access, ACLs for security
- Load balancing
- DNS services: hosting, traffic management
- DDoS protection

### Backend Connectivity

- Point-to-site for dev / test

- VPN Gateways for secure site-to-site connectivity

- ExpressRoute for private enterprise grade connectivity

# 가상 네트워크 - Virtual Network(VNET)

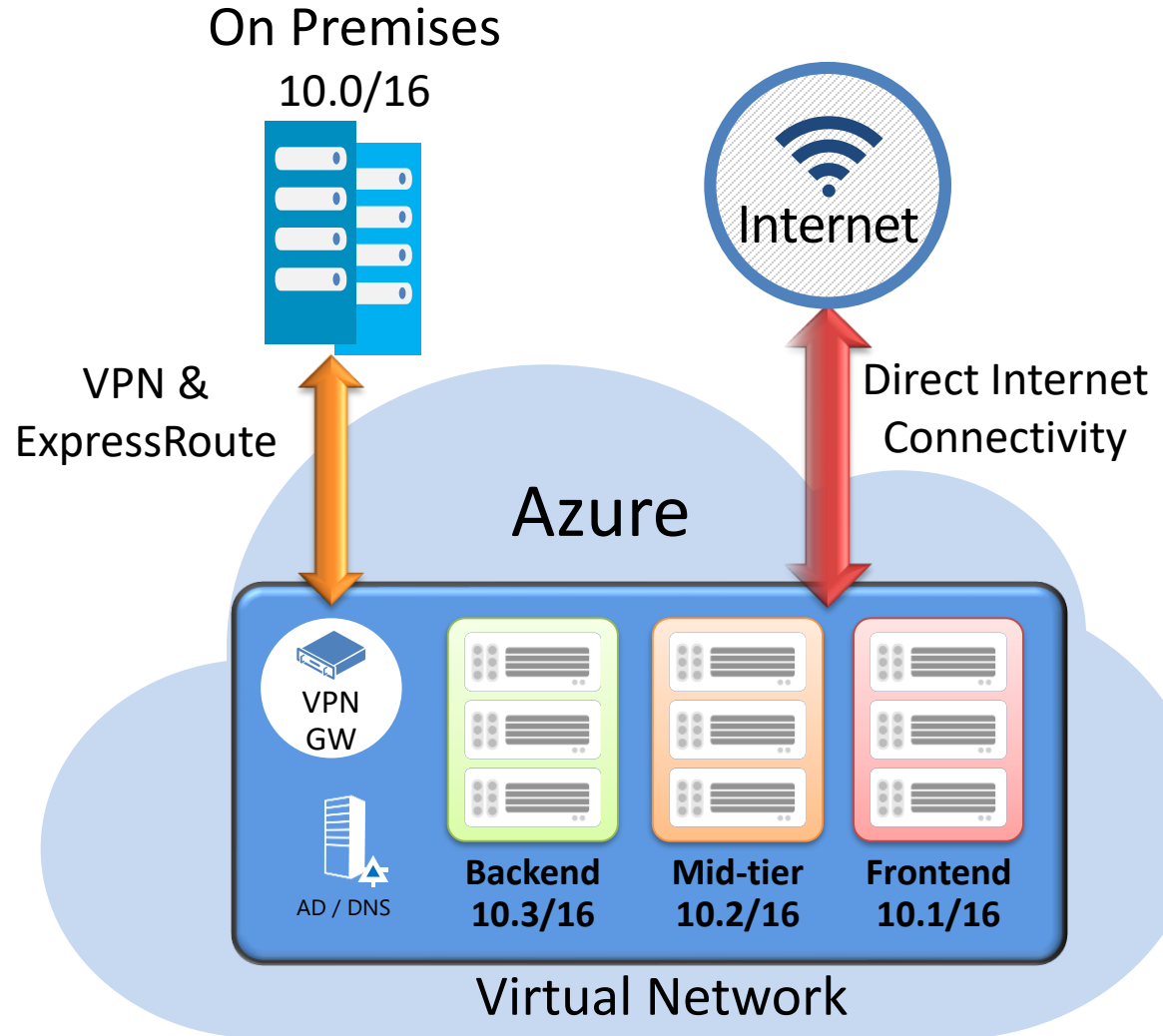


사용자 정의 가상 네트워크 설정

자체 DNS 사용 혹은 Azure DNS 사용

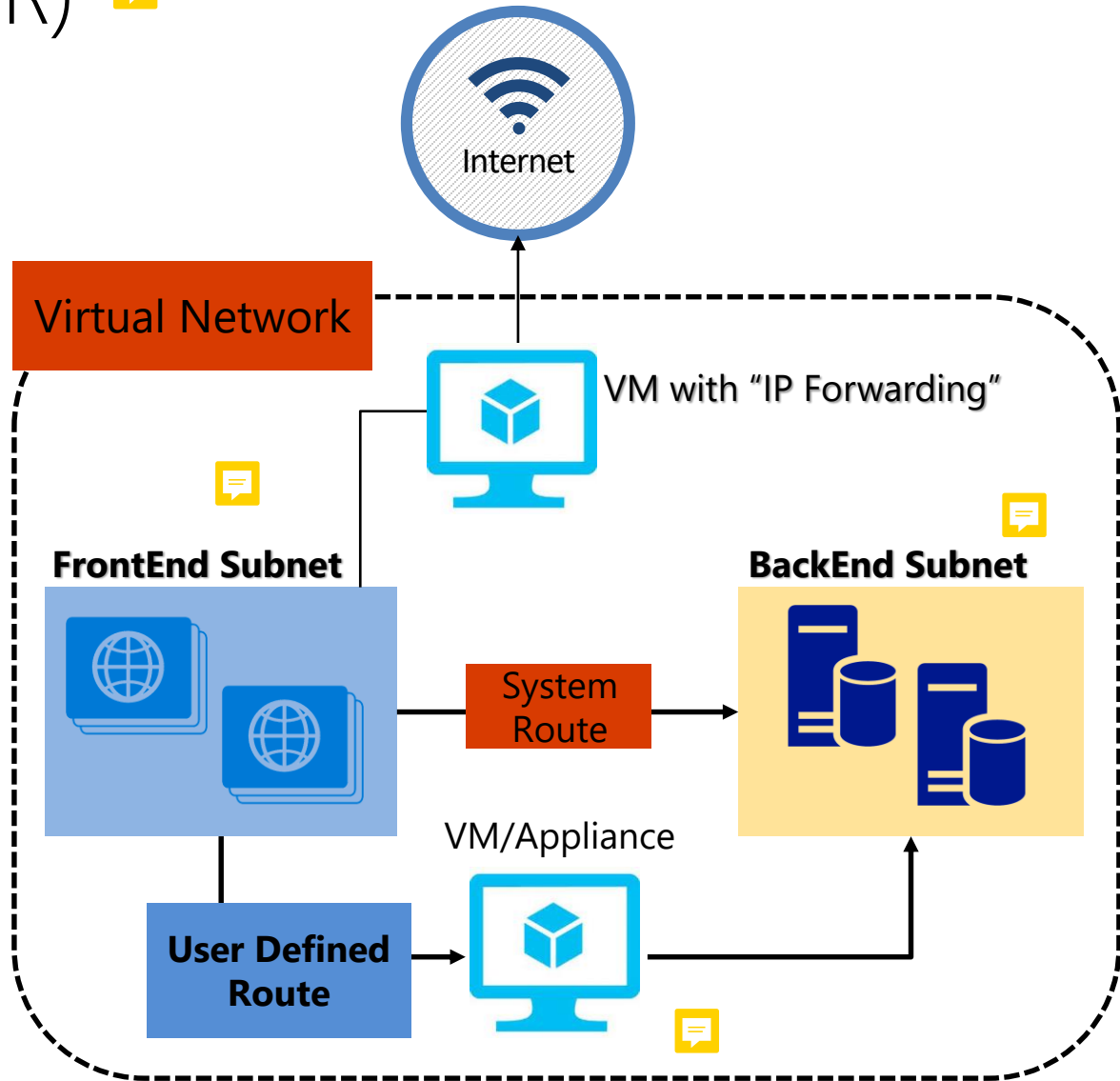
네트워크 보안 그룹(NSG)을 통한 보안 강화

사용자 정의 라우터(User Defined Route) 통한  
네트워크 흐름 제어



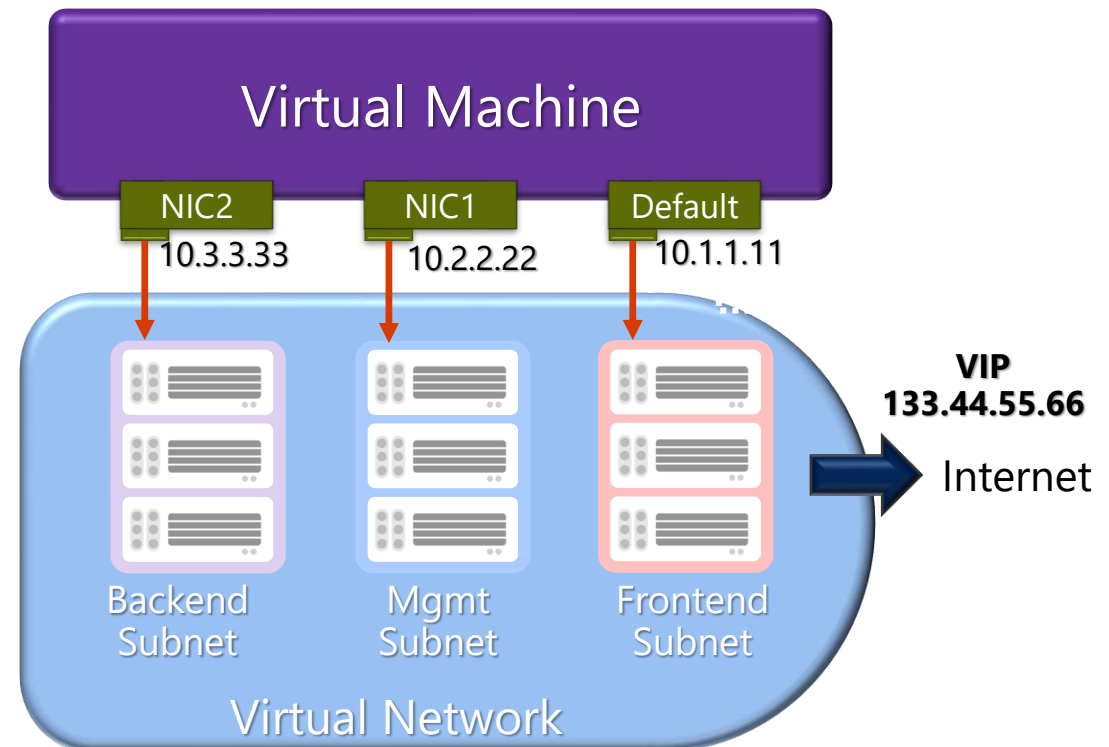
# 사용자 정의 라우터(UDR)

- Control traffic flow in your network with custom routes
- Attach route tables to subnets
- Specify next hop for any address prefix
- Set default route to force tunnel all traffic to on-premises or appliance



# Multiple NICs in Azure VMs

- Up to 16 NICs per VM
- NSG and Routes on all NICs
- Can separate frontend, backend, and management



# Azure Application Gateway



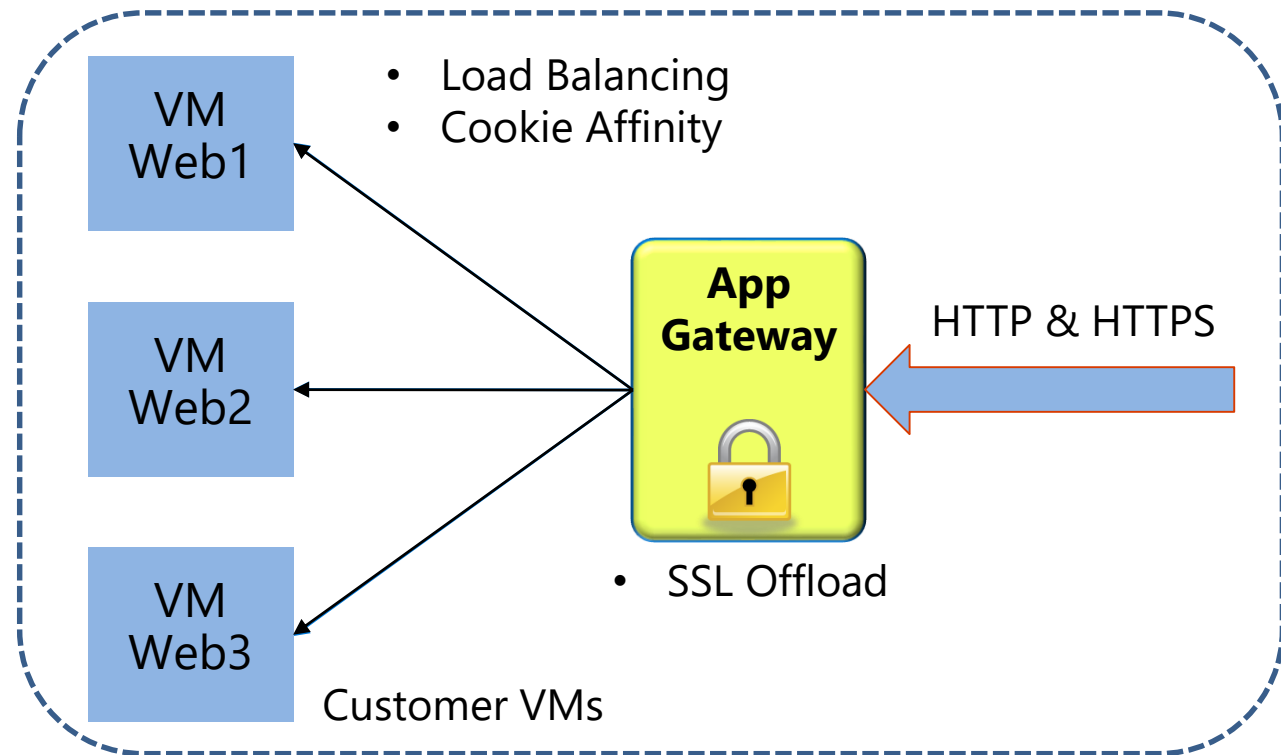
- Azure-managed, first-party virtual appliances
- HTTP routing based on app-level policies

Cookie affinity

- URL hash
- Weight (load)

- **SSL termination and caching**

- Centralize certificate management
- Scalable backend provisioning

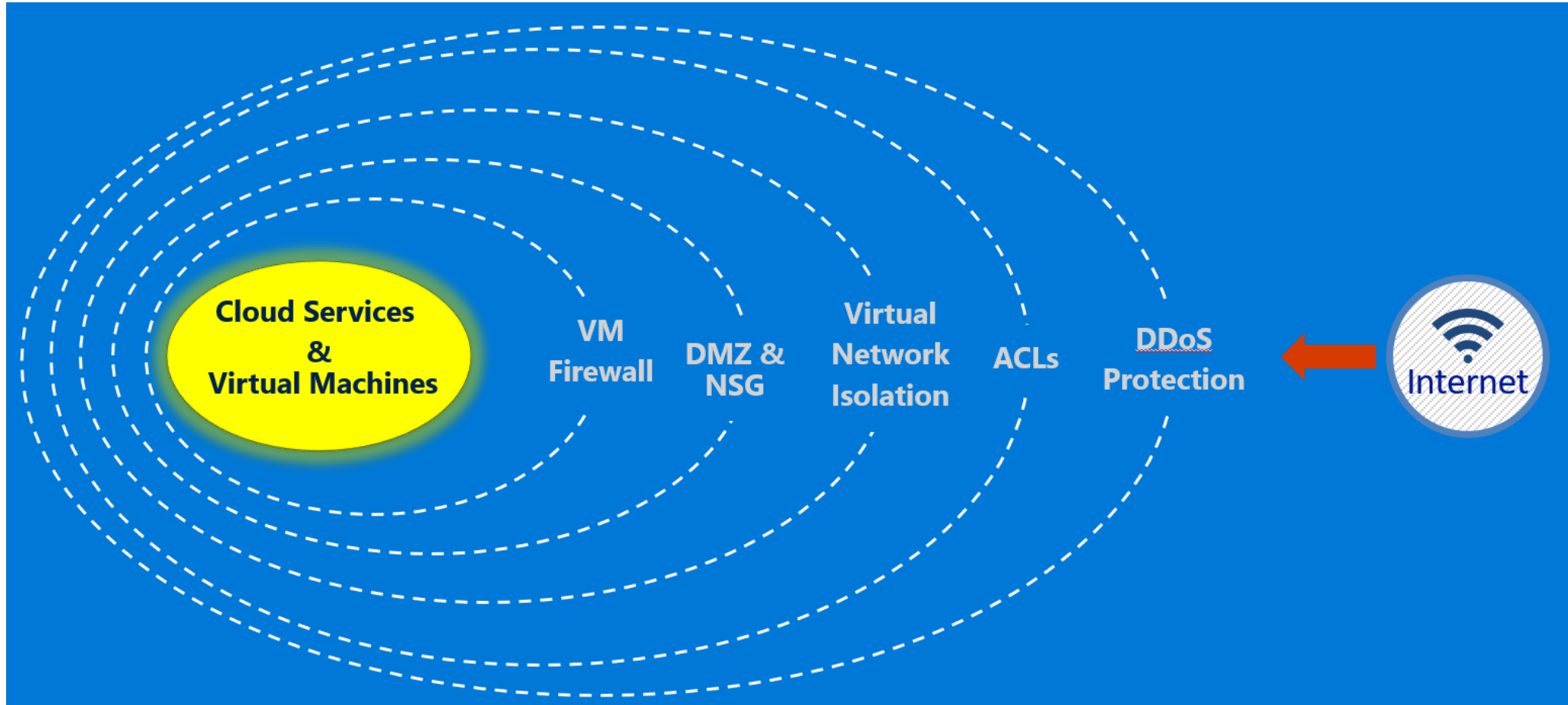




# 계층화된 보안 및 자원 보호



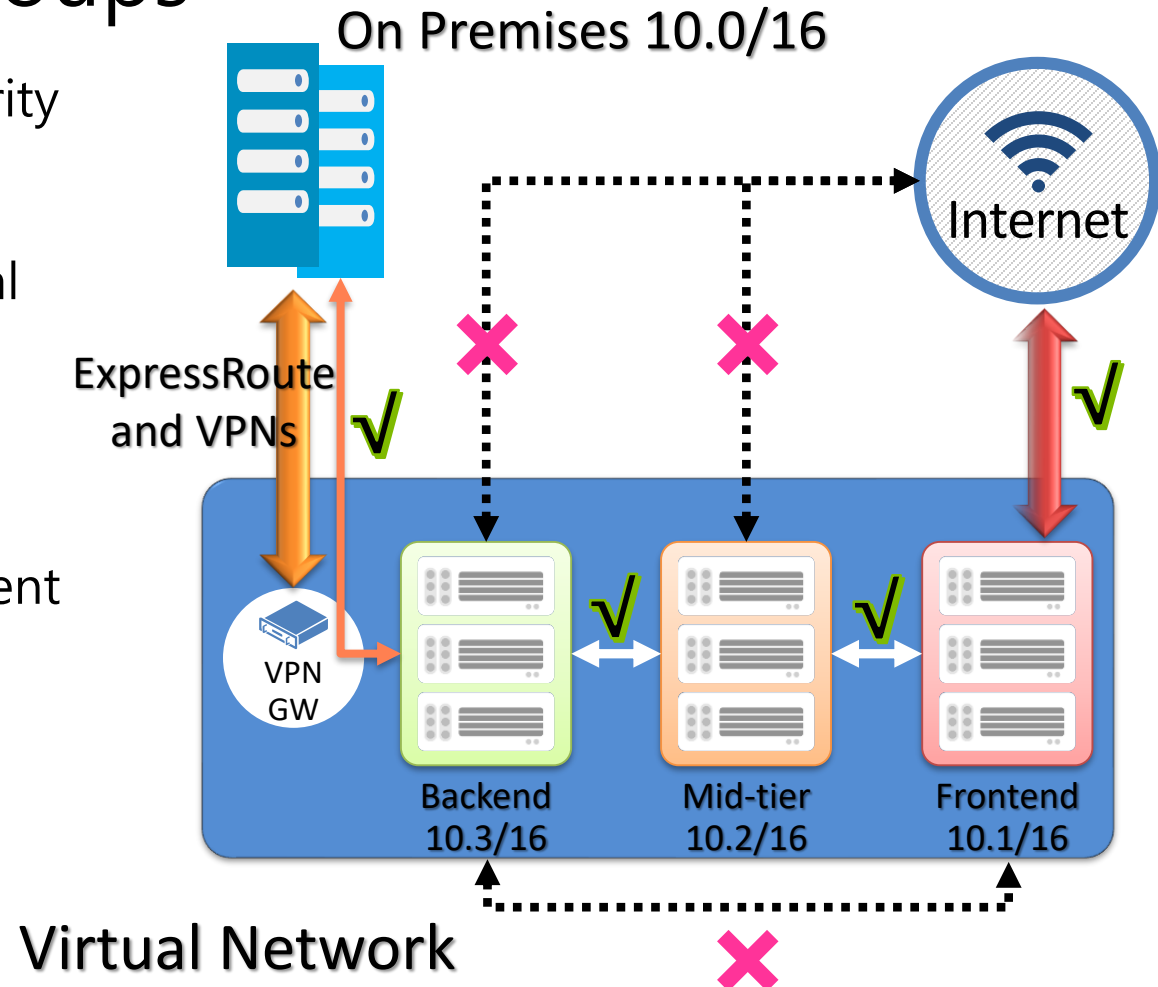
## Layered Security, Protection, and Isolation



# 네트워크 보안 그룹

## Network Security Groups

- Segment network to meet security needs
- 5 tuple ACLs on both directions
- Can protect Internet and internal traffic
- Enables DMZ subnets
- Associated to subnets/VMs and NICs
- ACLs can be updated independent of VMs





# Azure DNS & Traffic Manager

---



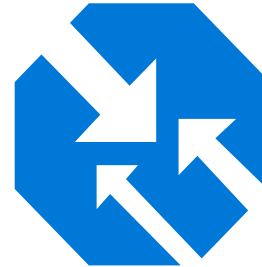
# 글로벌 부하 분산 서비스

## Azure DNS



DNS 서비스 제공 및 사용자 웹/도메인  
호스팅

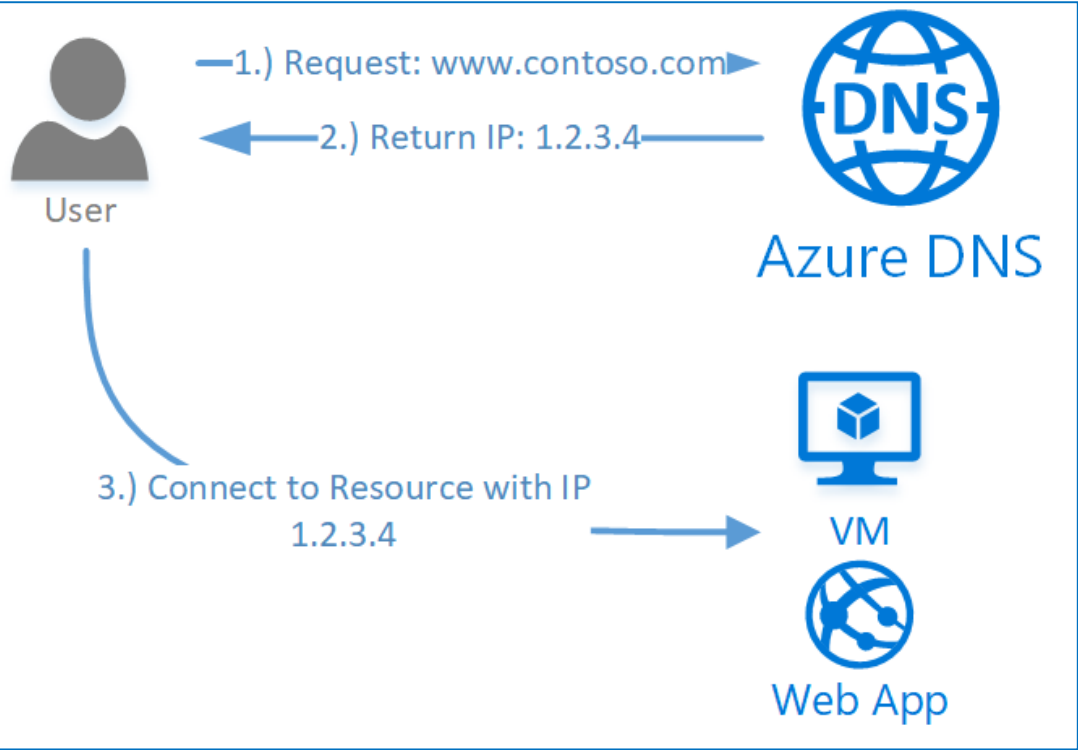
## Traffic Manager



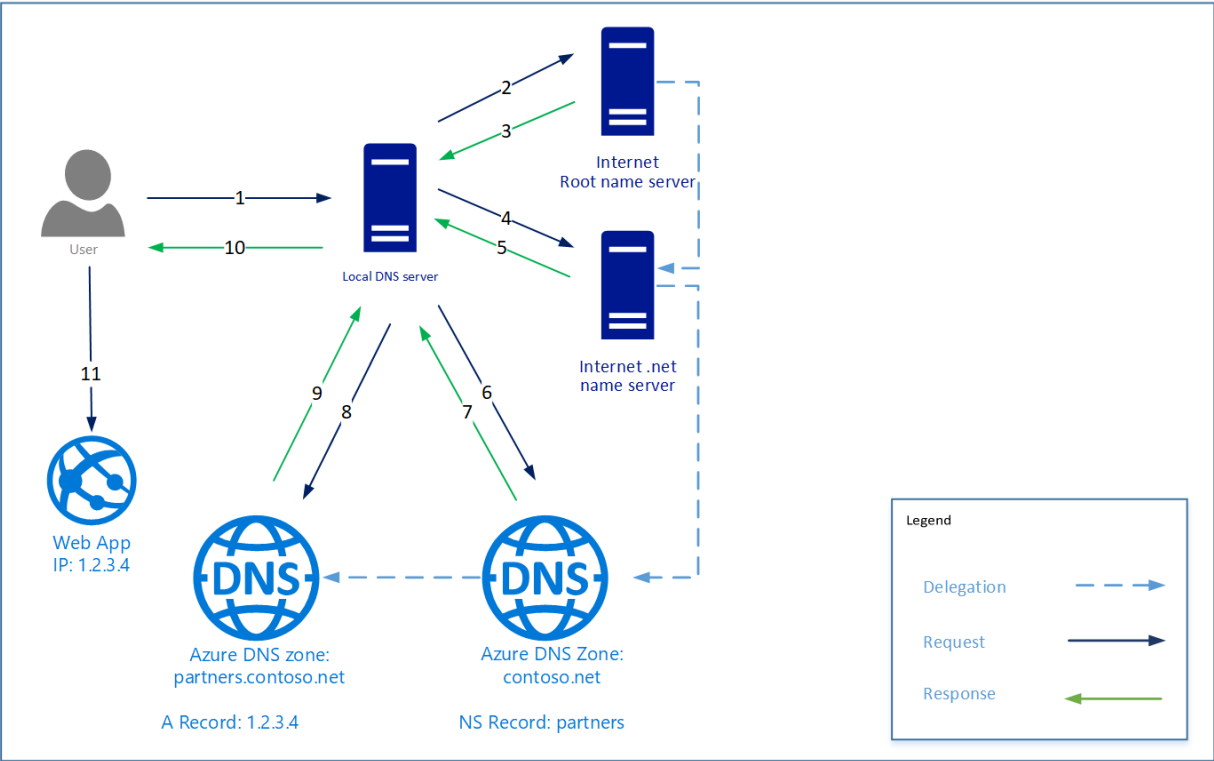
글로벌 부하 분산 서비스로 유연한 트래픽 관리  
정책을 통해 최고의 사용자 경험 제공

# Azure DNS 소개

## DNS 질의



## DNS 위임



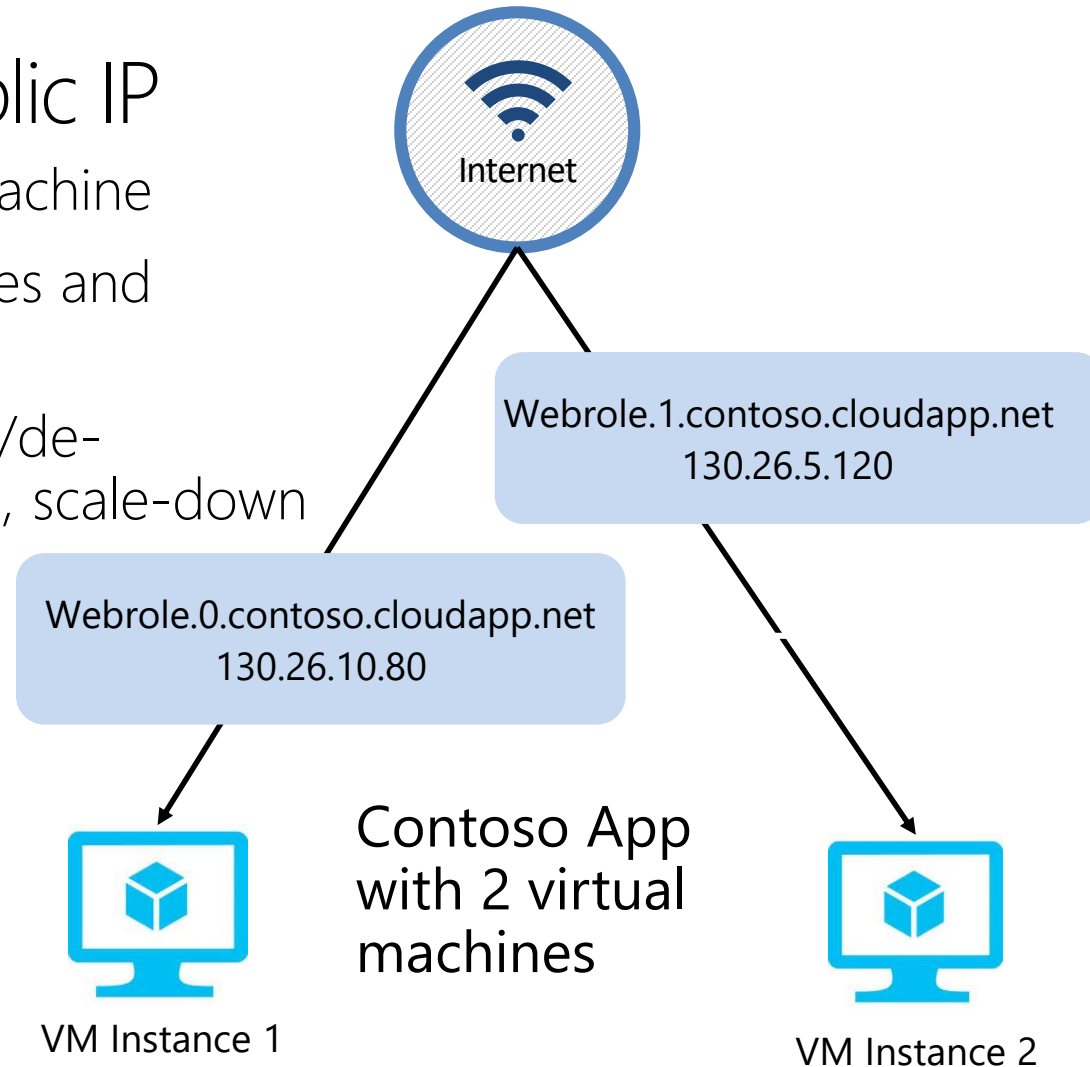
# 사용자 도메인 지정

## DNS Names for Public IP

FQDN access to a virtual machine

Available for virtual machines and web/worker roles

Automatic DNS registration/de-registration during scale-up, scale-down

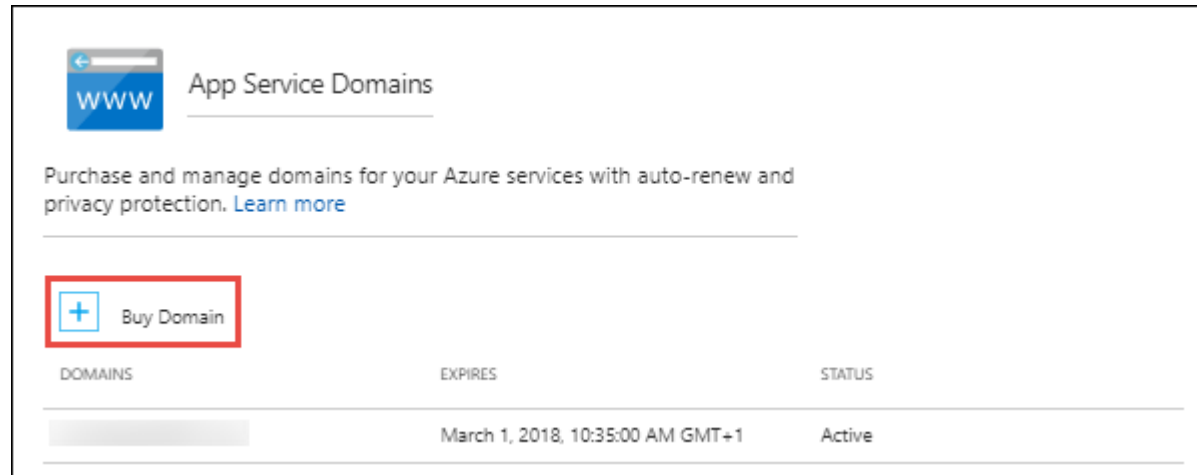
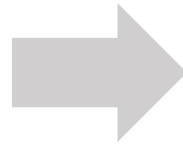
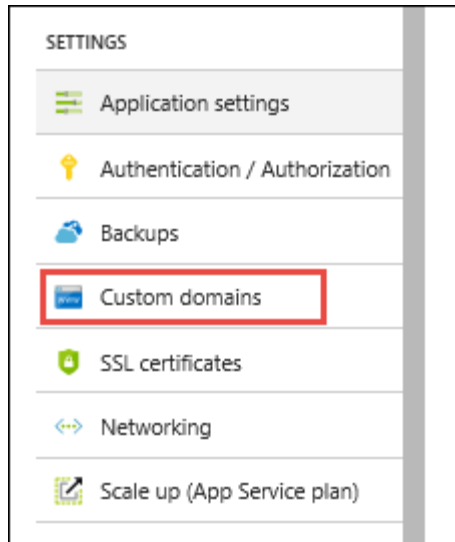


# Azure DNS

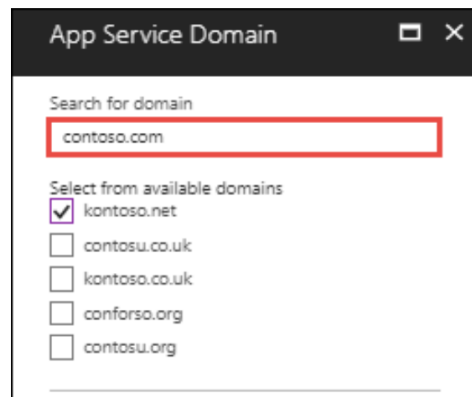
- Azure DNS는 Microsoft Azure 인프라를 사용하여 이름 확인을 제공하는 DNS 도메인에 대한 호스팅 서비스
- Azure에 도메인을 호스트하면 다른 Azure 서비스와 동일한 자격 증명, API, 도구 및 대금 청구를 사용하여 DNS 레코드를 관리
- Azure DNS를 사용하여 도메인 이름을 구매할 수 없음
- 사용지 지정 도메인은 연간 요금의 경우 App Service 도메인 또는 타사 도메인 이름 등록자를 사용하여 도메인 이름을 구매 후 Azure DNS에 도메인 위임
- Azure DNS에 도메인을 호스트하여 레코드 관리

# Azure 사용자 지정 도메인 등록

**App Services** 탭에서 앱의 이름을 클릭하고, **설정**을 선택한 다음, **사용자 지정 도메인**을 선택



**사용자 지정 도메인** 페이지에서 **도메인 구입**을 클릭

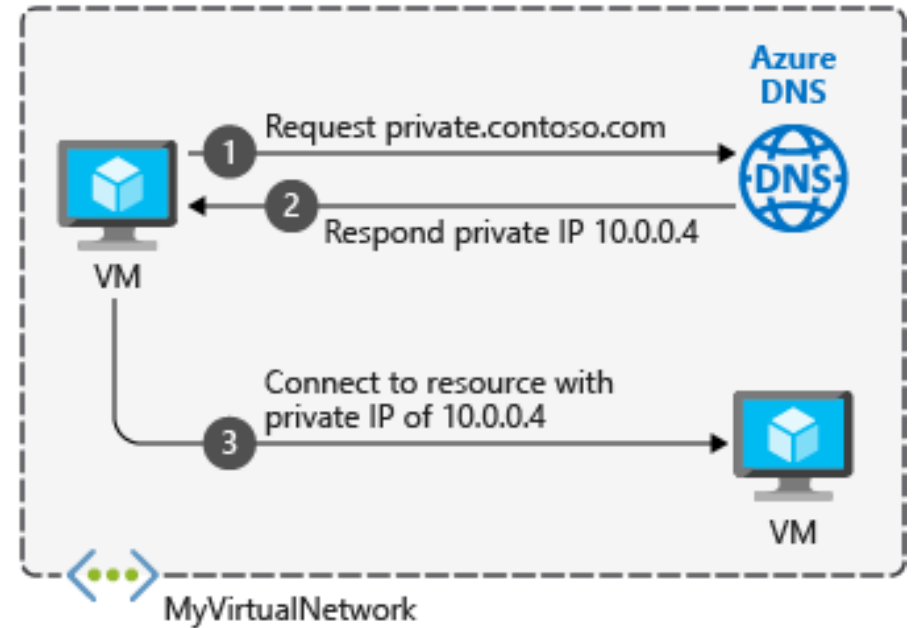


- **App Service** 도메인 페이지의 **도메인 검색** 상자에 구입할 도메인 이름을 입력하고 Enter를 입력
- 사용 가능한 도메인이 텍스트 상자 아래에 나타남
- 구입하려는 도메인을 하나 이상 선택 후 구매



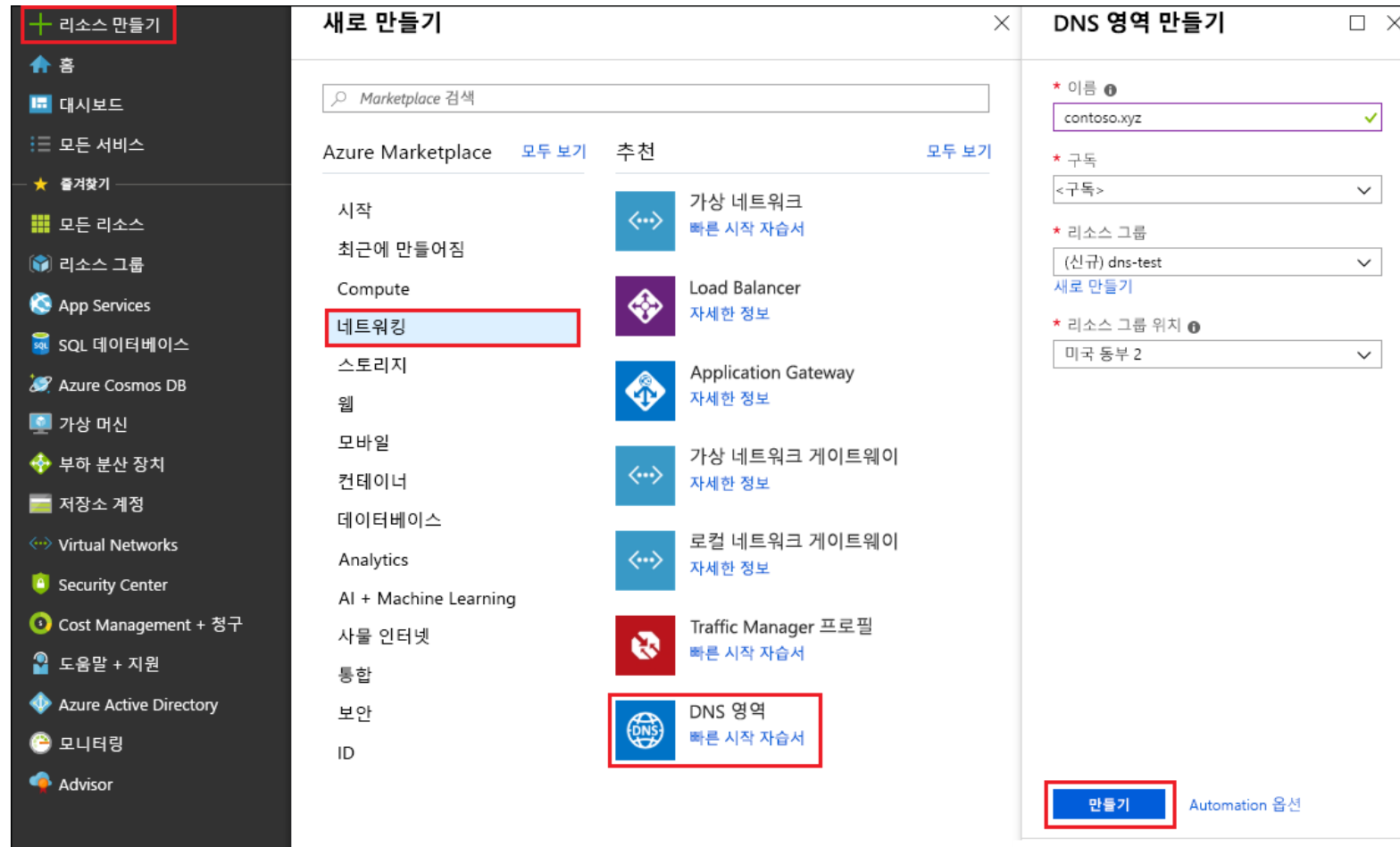
# Azure 프라이빗 DNS란?

- DNS(Domain Name System)는 서비스 이름을 해당 IP 주소로 변환(또는 확인)
- Azure DNS는 인터넷 연결 DNS 도메인 지원 외에 프라이빗 DNS 영역도 지원
- Azure 프라이빗 DNS는 사용자 지정 DNS 솔루션을 추가하지 않고도 가상 네트워크의 도메인 이름을 관리하고 확인할 수 있는 안정적이고 신뢰할 수 있는 DNS 서비스를 제공
- 프라이빗 DNS 영역을 사용하면 현재 Azure에서 제공하는 이름 대신 사용자 고유의 사용자 지정 도메인 이름(예, microsoft.com 등)을 사용할 수 있음
- 가상 네트워크에서 프라이빗 DNS 영역의 레코드를 확인하려면 가상 네트워크를 해당 영역과 연결해야 함, 연결된 가상 네트워크는 전체 액세스 권한을 가지며 프라이빗 영역에 게시된 모든 DNS 레코드를 확 가능
- 가상 네트워크 연결에 대한 자동 등록을 사용하도록 설정하면 해당 가상 네트워크의 가상 머신에 대한 DNS 레코드가 프라이빗 영역에 등록
- 자동 등록이 활성화된 경우 Azure DNS는 가상 머신이 생성되고, 해당 IP 주소를 변경하거나 삭제될 때마다 영역 레코드를 업데이트



# Azure Portal을 사용하여 Azure DNS 영역 및 레코드 만들기

공용 도메인에서 호스트 이름을 확인하기 위한 Azure DNS를 구성할 수 있음  
예를 들어 도메인 이름 등록 기관에서 *contoso.xyz* 도메인 이름을 구입한 경우, Azure DNS에서 *contoso.xyz* 도메인을 호스팅하고 [www.contoso.xyz](http://www.contoso.xyz) 를 웹 서버 또는 웹앱의 IP 주소로 확인하도록 구성



# DNS 레코드 만들기

DNS 영역 내에서 도메인에 대한 DNS 항목 또는 레코드를 만들 수 있음  
호스트 이름을 IPv4 주소로 확인하는 새 주소 레코드 또는 'A' 레코드를 만들

## 'A' 레코드를 만들려면

1. Azure Portal의 **모든 리소스**에서 **MyResourceGroup** 리소스 그룹의 **contoso.xyz** DNS 영역을 연다. 보다 쉽게 찾기 위해 **이름으로 필터링** 상자에 *contoso.xyz*를 입력

2. **DNS 영역** 페이지의 위쪽에서 **+ 레코드 집합**을 선택

3. **레코드 집합 추가** 페이지에서 다음 값을 입력하거나 선택

- **Name:** *www*를 입력합니다. 레코드 이름은 지정된 IP 주소로 확인하려는 호스트 이름
- **형식:** **A**를 선택합니다. 'A' 레코드가 가장 일반적이지만, 메일 서버('MX'), IP v6 주소('AAAA') 등에 대한 다른 레코드 형식도 있음
- **TTL:** *1*을 입력합니다. DNS 요청의 *Time-to-live*는 DNS 서버 및 클라이언트가 응답을 캐시할 수 있는 시간을 지정
- **TTL 단위:** **시간**을 선택. **TTL** 값에 대한 시간 단위
- **IP 주소:** 이 빠른 시작 예제의 경우 *10.10.10.10*을 입력.  
이 값은 레코드 이름이 확인하는 IP 주소.  
실제 시나리오에서는 웹 서버의 공용 IP 주소를 입력

# DNS 이름 확인

개요 페이지의 이름 서버 목록에서 이름 서버 이름 중 하나를 복사

contoso.xyz DNS zone

검색(Ctrl+/) << + 레코드 집합 → 이동 삭제 영역 새로 고침

개요  
활동 로그  
액세스 제어(IAM)  
태그  
문제 진단 및 해결

설정  
속성  
잠금  
Automation 스크립트

모니터링  
경고  
메트릭

지원 + 문제 해결  
새 지원 요청

리소스 그룹(변경) : dns-test  
구독(변경) : <구독>  
구독 ID : <구독 ID>  
태그(변경) : 태그를 추가하려면 여기를 클릭

이름 서버 1: ns1-08.azure-dns.com.  
이름 서버 2: ns2-08.azure-dns.net.  
이름 서버 3: ns3-08.azure-dns.org.  
이름 서버 4: ns4-08.azure-dns.info.

레코드 집합 검색

이름	형식	TTL	값
@	NS	172800	ns1-08.azure-dns.com. ns2-08.azure-dns.net. ns3-08.azure-dns.org. ns4-08.azure-dns.info.
@	SOA	3600	이메일: azuredns-hostmaster.micr... 호스트: ns1-08.azure-dns.com. 새로 고침: 3600 다시 시도: 300 만료: 2419200 최소 TTL: 300 일련 번호: 1
www	A	3600	10.10.10.10

C:\W> nslookup www.contoso.xyz ns1-08.azure-dns.com.

```
Administrator: Command Prompt

C:\WINDOWS\system32>nslookup www.contoso.xyz ns1-08.azure-dns.com
Server: UnKnown
Address: 40.90.4.8

Name: www.contoso.xyz
Address: 10.10.10.10

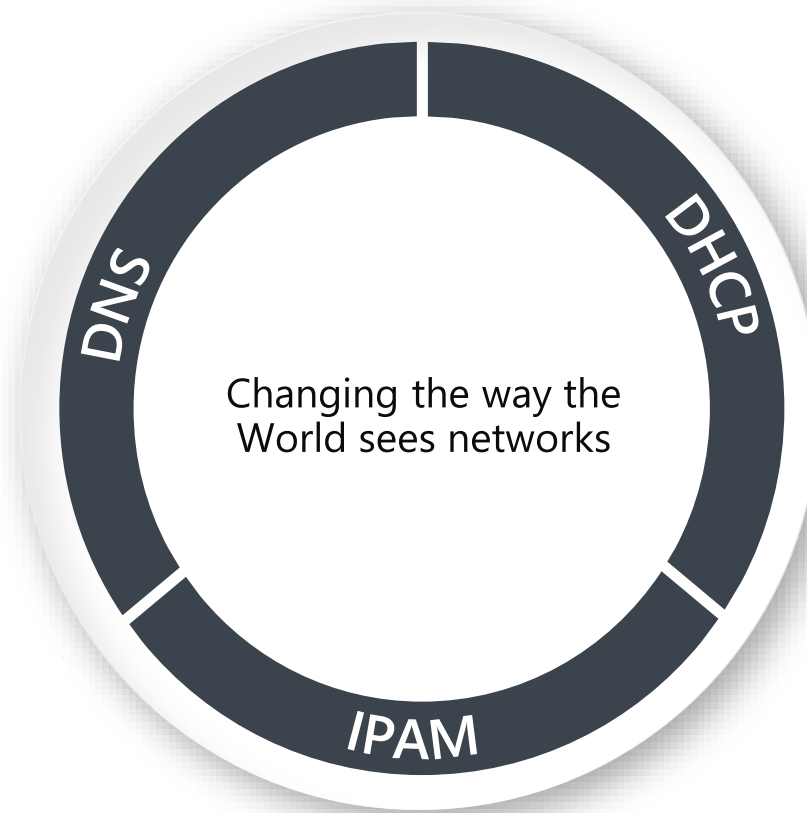
C:\WINDOWS\system32>
```

호스트 이름 **www.contoso.xyz**는 구성한 대로 **10.10.10.10**으로 확인

# Azure 파트너 DNS 관리 - Men & Mice Suite(MMS)

## DNS 관리

고가용성 및 안전하고 중앙 집중화된  
다양한 플랫폼을 지원하는 DNS  
관리솔루션



## DHCP 관리

하이브리드 운영 환경에서의 완벽한  
상호 운용성

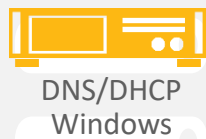
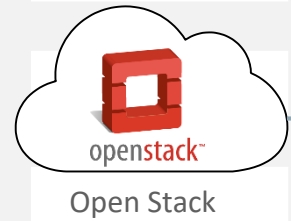
## IP 주소 관리

IP 자원 한눈에 보기 및  
엔터프라이즈 네트워크 통합  
운영 환경 지원

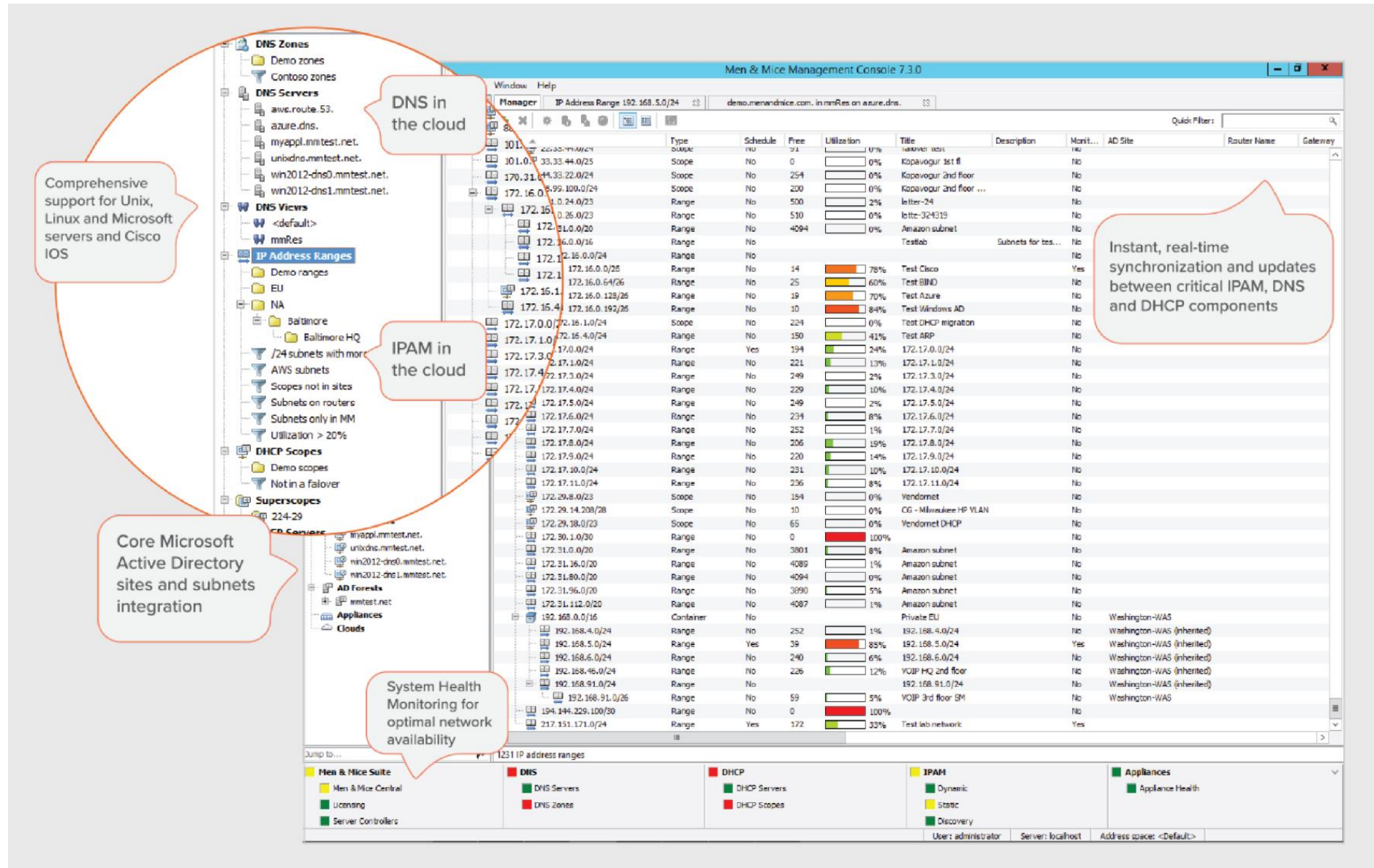
# MMS 기본 아키텍처

온-프레미스

퍼블릭 클라우드



# Men & Mice Suite 대시보드



# Traffic Manager

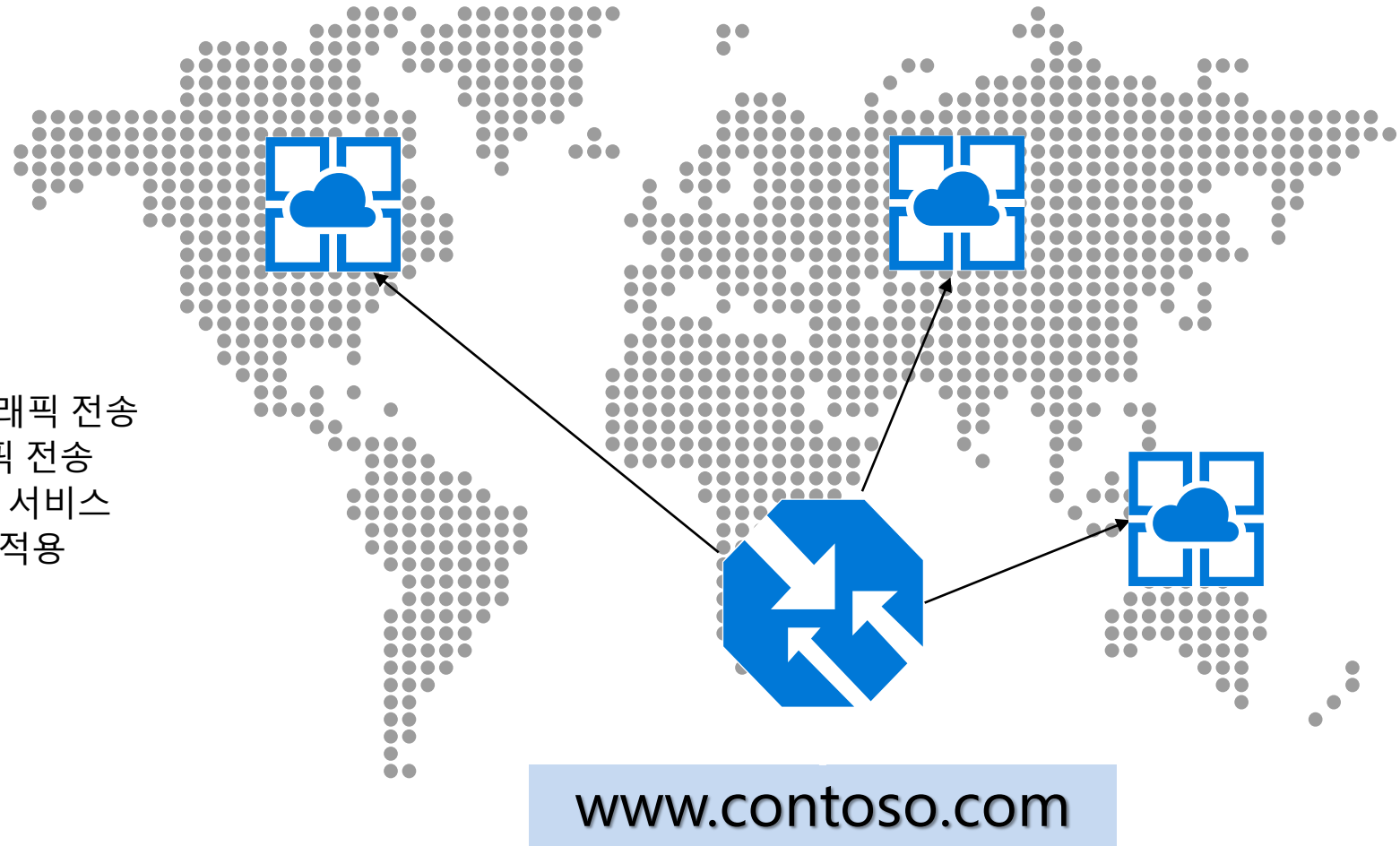
## Traffic 관리 정책

Latency – 가장 가까운 위치로 트래픽 전송

Round Robin – 순차적으로 트래픽 전송

Failover – Primary 사이트 장애 시 서비스

Nested – 유연한 멀티-레벨 정책 적용





# Azure 부하분산 서비스

---



# Internet IP Addresses & Load Balancing

## 공인 IP(Public IP)

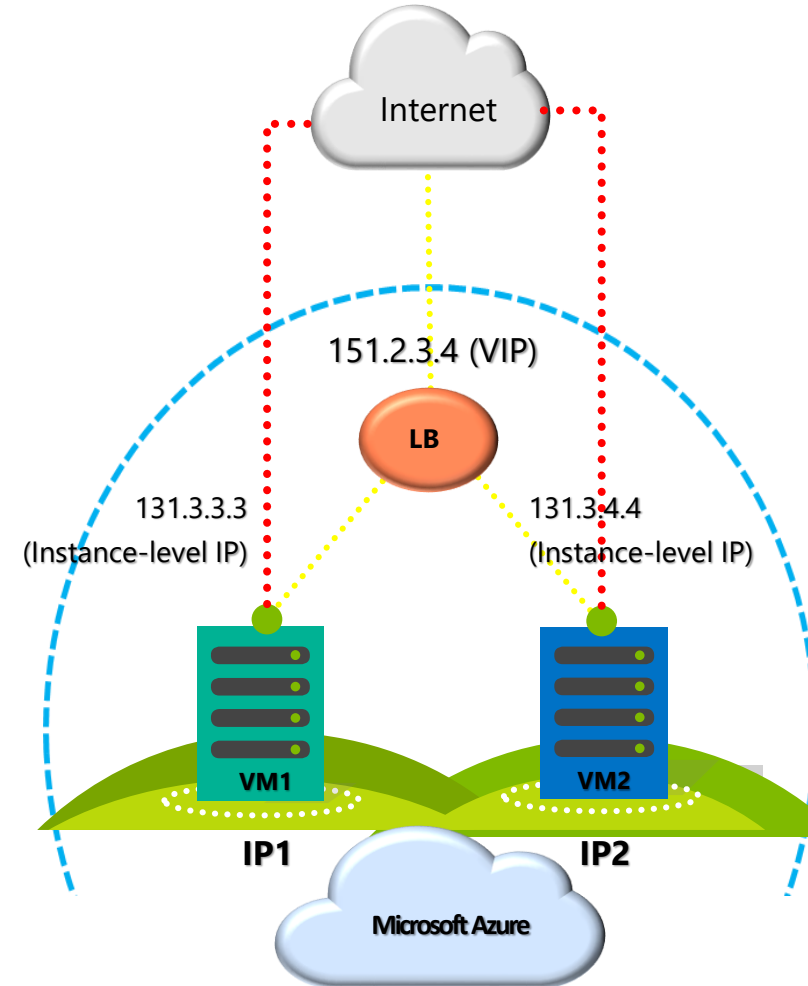
Can be used for instance (VM) level access or load balancing

## 가상 서버 IP (Instance Level IP)

Internet IP assigned exclusively to single VM  
Entire port range accessible by default  
Primarily for targeting a specific VM

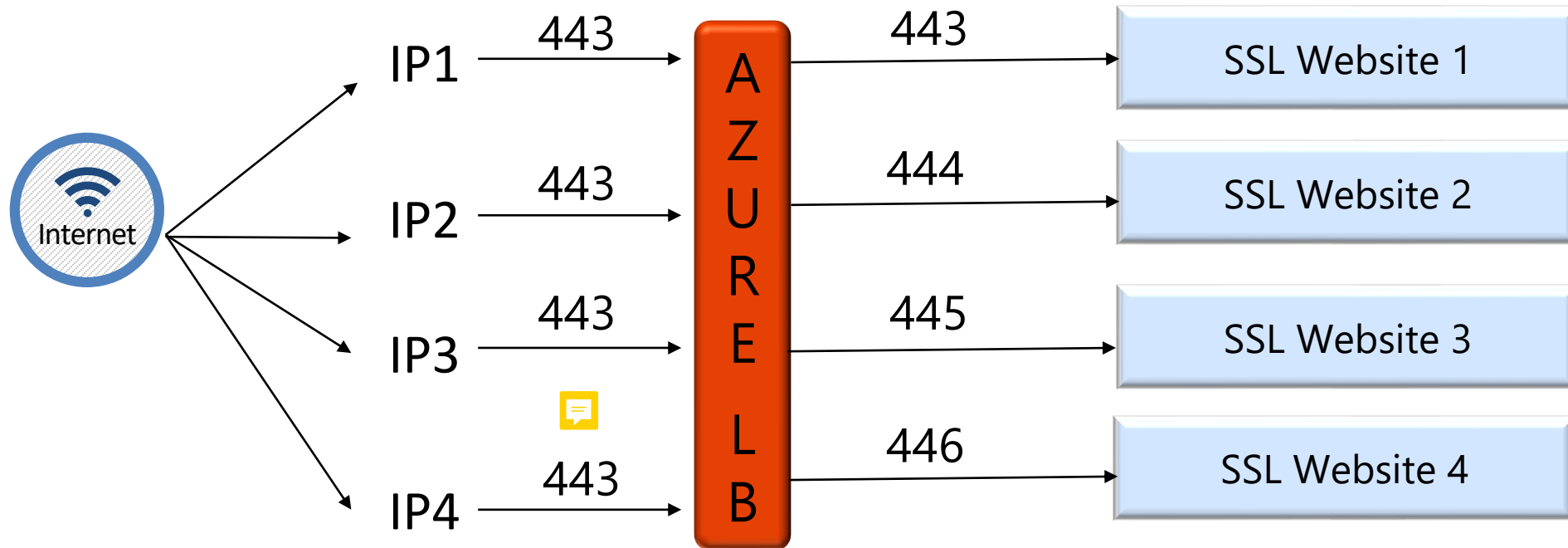
## 부하 분산용 IP (VIP)

Internet IP load balanced among one or more VM instances  
Allows port redirection  
Primarily for load balanced, highly available, or auto-scale scenarios



# Multiple Load-balanced IPs

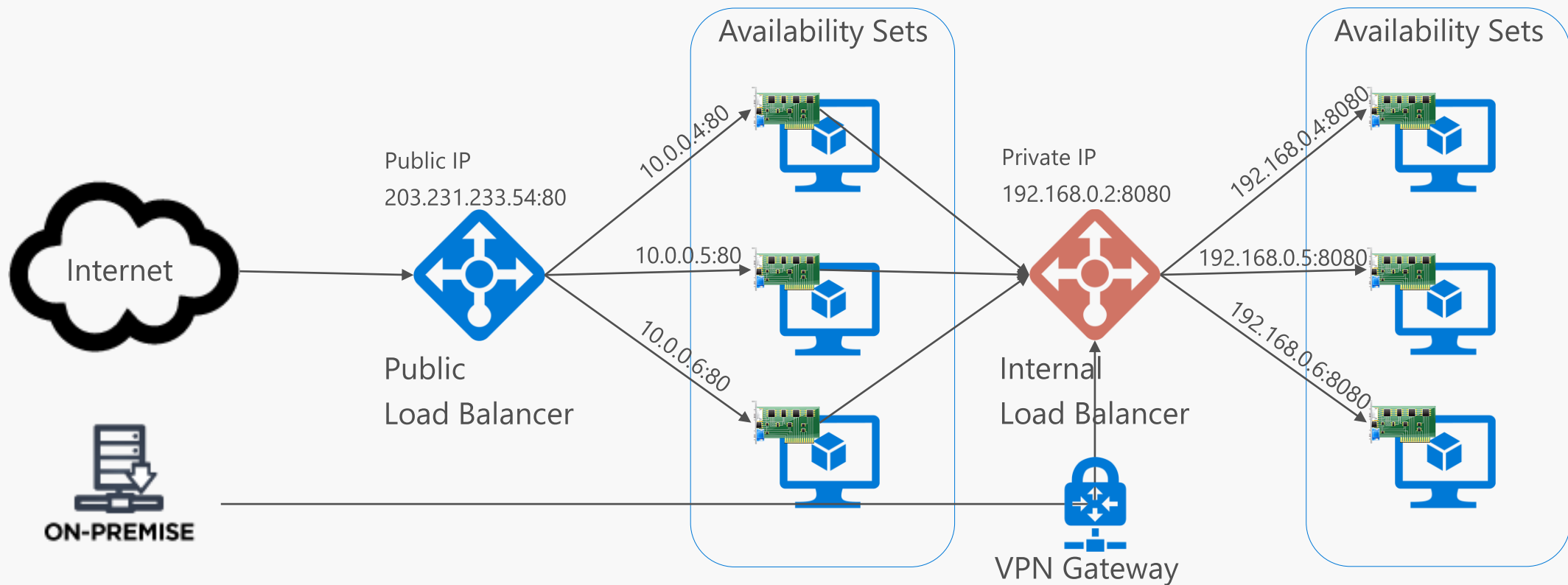
- Common use case: multiple SSL end points
- Across one or more VMs



# 부하 분산 장치




- Azure Load Balancer is a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy service instances in virtual machines defined in a load-balancer set.

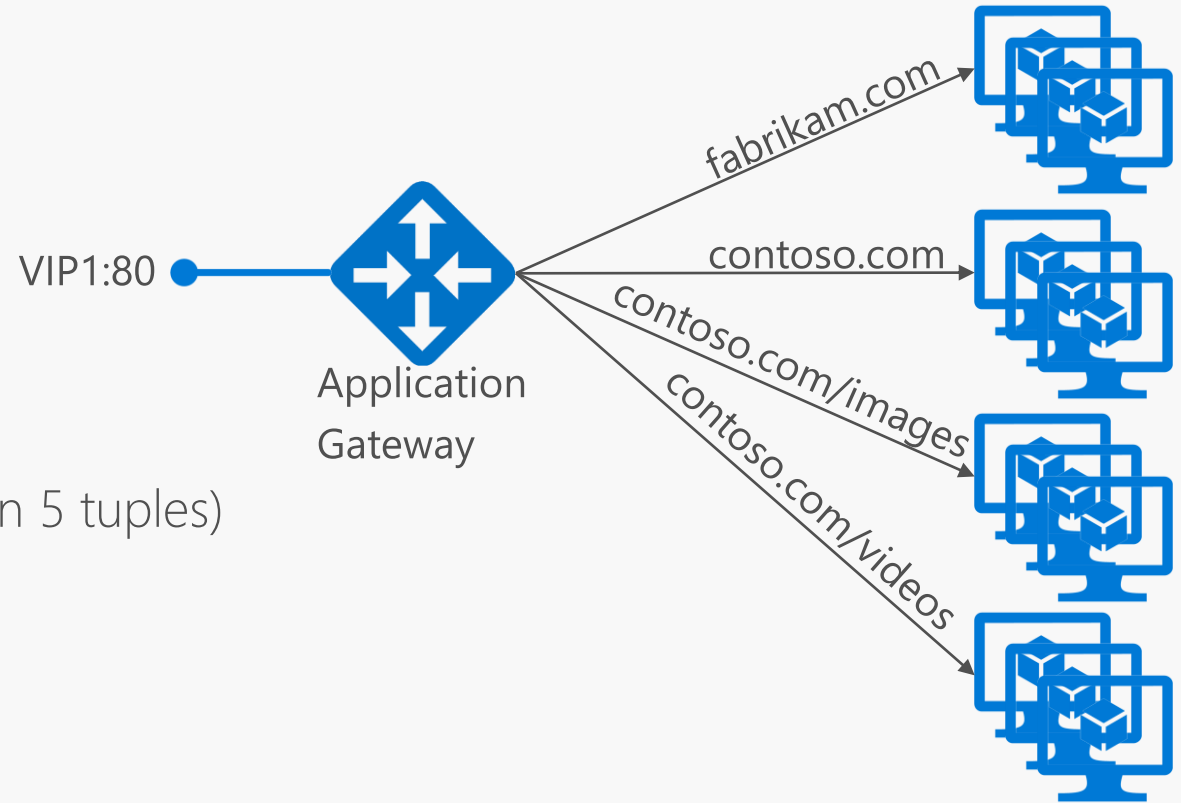


# 부하 분산 정책

- **Hash-based distribution** - By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers.
- **Port forwarding** - An endpoint listens on a public port and forwards traffic to an internal port.
- **Automatic reconfiguration** - Instantly reconfigures itself when you scale instances up or down.
- **Service monitoring** - When a probe fails to respond, Load Balancer stops sending new connections to the unhealthy instances.
- **Source NAT** - All outbound traffic to the Internet that originates from your service undergoes Source NAT (SNAT) by using the same VIP address as for incoming traffic.
- **Internal Load Balancer** - The infrastructure restricts the accessibility and creates a trust boundary between the load balanced virtual IP addresses to a Virtual Network and will never be exposed to a Internet endpoint directly.

# 어플리케이션 게이트웨이(L7 부하 분산)

- Support multiple VM Scale Sets
- Cross cluster
- Cross Geo
- SSL termination
- URL based routing 
- True round robin (as opposed to hash based on 5 tuples)
- Multi-site & SNI
- Session affinity based on cookie

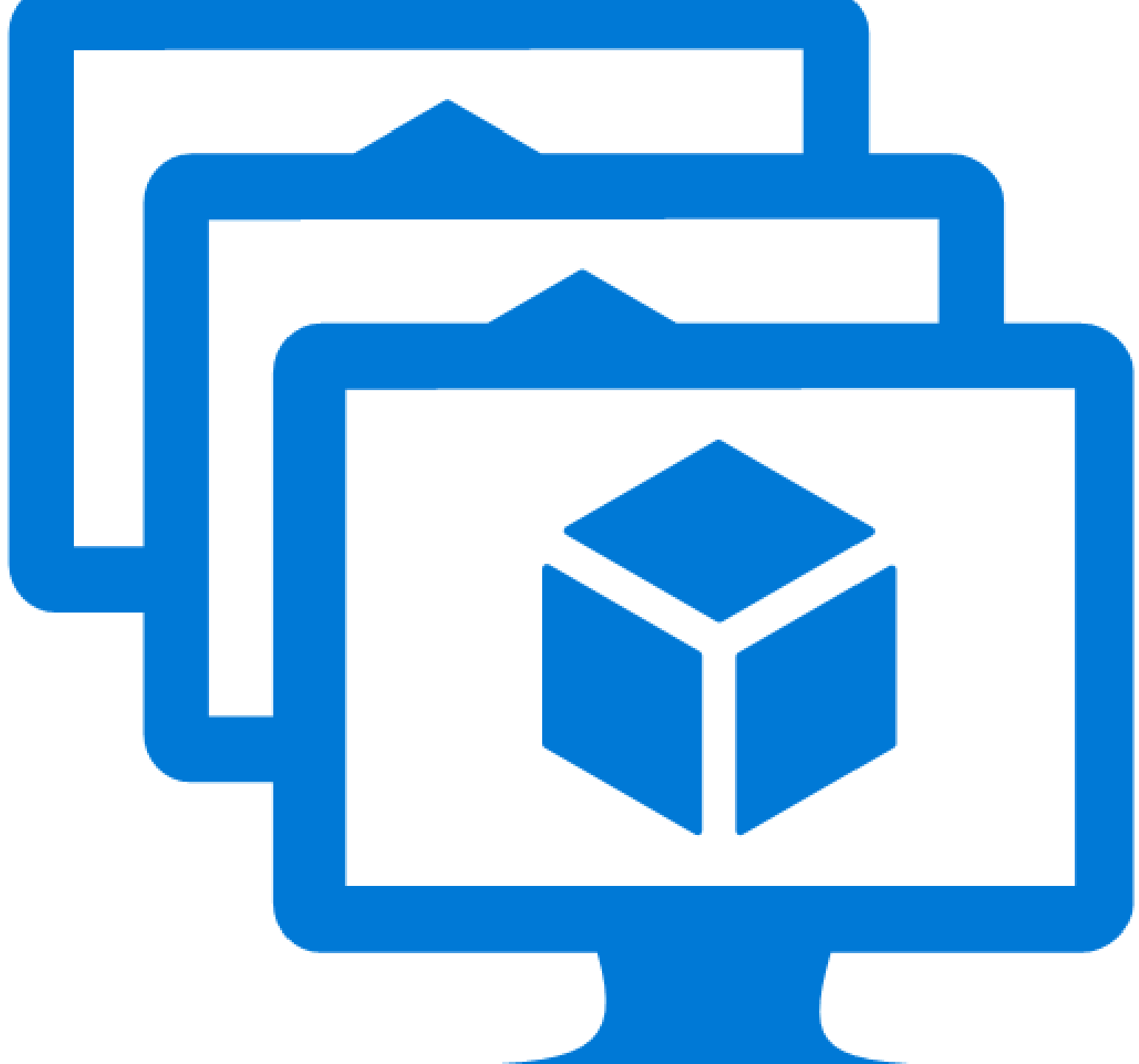


# 부하 분산 장치(L4) vs 어플리케이션 게이트웨이(L7)

Type	Azure Load Balancer	Application Gateway
Protocols	UDP/TCP	HTTP/ HTTPS
IP reservation	supported	not supported
Load balancing mode	5 tuple(source IP, source port, destination IP,destination port, protocol type	CookieBasedAffinity = false,rules = basic (Round-Robin)
Load balancing mode (source IP /sticky sessions)	2 tuple (source IP and destination IP), 3 tuple (source IP, destination IP and port). Can scale up or down based on the number of virtual machines	CookieBasedAffinity = true,rules = basic (Round-Robin) for new connections.
Health probes	Default: probe interval - 15 secs. Taken out of rotation: 2 Continuous failures. Supports user defined probes	Idle probe interval 30 secs. Taken out after 5 consecutive live traffic failures or a single probe failure in idle mode. Supports user defined probes
SSL offloading	not supported	supported

# Azure VPN & Express Route









---





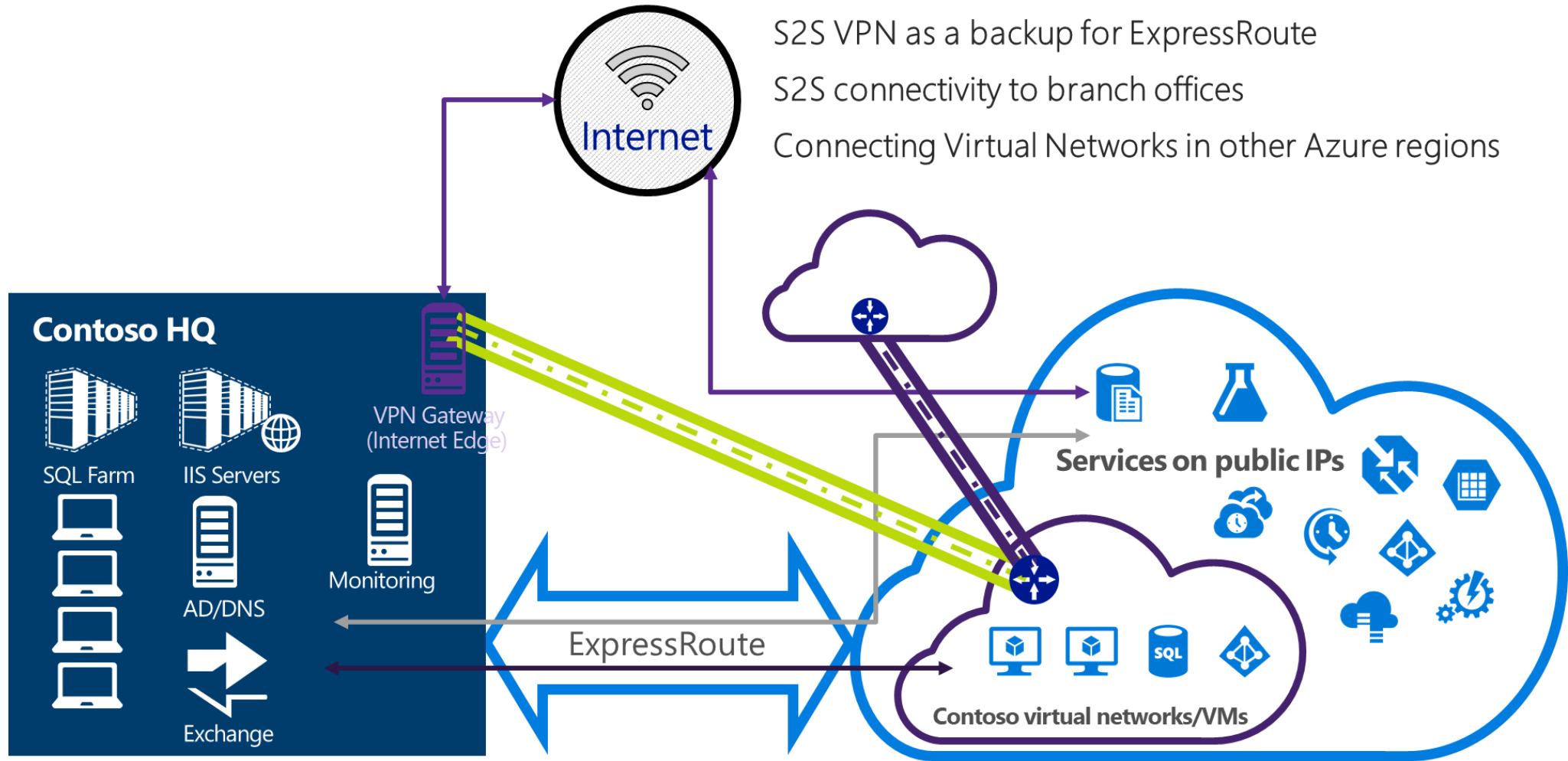
# 네트워크 연결 옵션

## Connectivity Options and Hybrid Offerings

Cloud		Customer	Segment and workloads
	Internet Connectivity		<ul style="list-style-type: none"><li>• <b>Consumers</b></li><li>• Access over public IP</li><li>• DNS resolution</li><li>• Connect from anywhere</li></ul>
	Secure point-to-site connectivity		<ul style="list-style-type: none"><li>• <b>Developers</b></li><li>• POC Efforts</li><li>• Small scale deployments</li><li>• Connect from anywhere</li></ul>
	Secure site-to-site VPN connectivity		<ul style="list-style-type: none"><li>• Connect to Azure compute</li></ul>
	ExpressRoute private connectivity		<ul style="list-style-type: none"><li>• <b>SMB &amp; Enterprises</b></li><li>• Mission critical workloads</li><li>• Backup/DR, media, HPC</li><li>• Connect to Microsoft services</li></ul>

# ExpressRoute 와 VPN 통합 연결

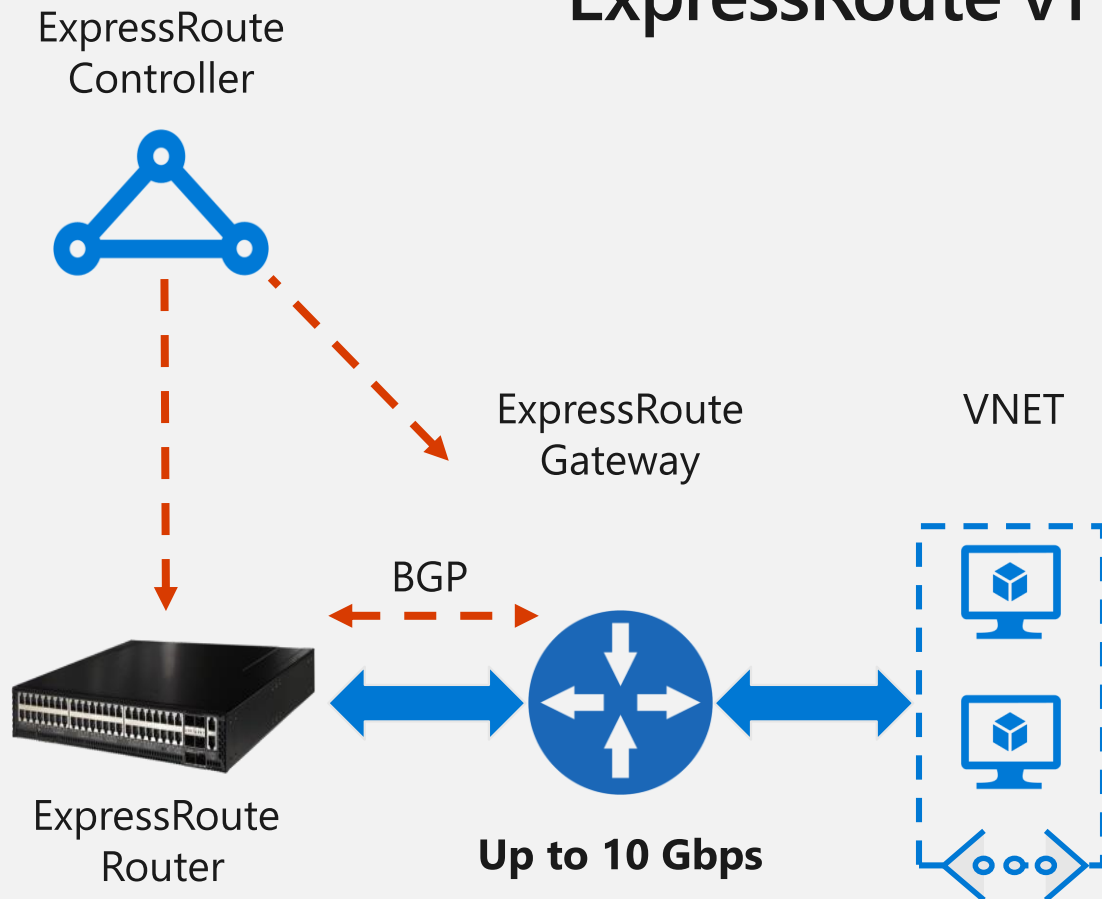
## ExpressRoute and S2S VPN Coexistence



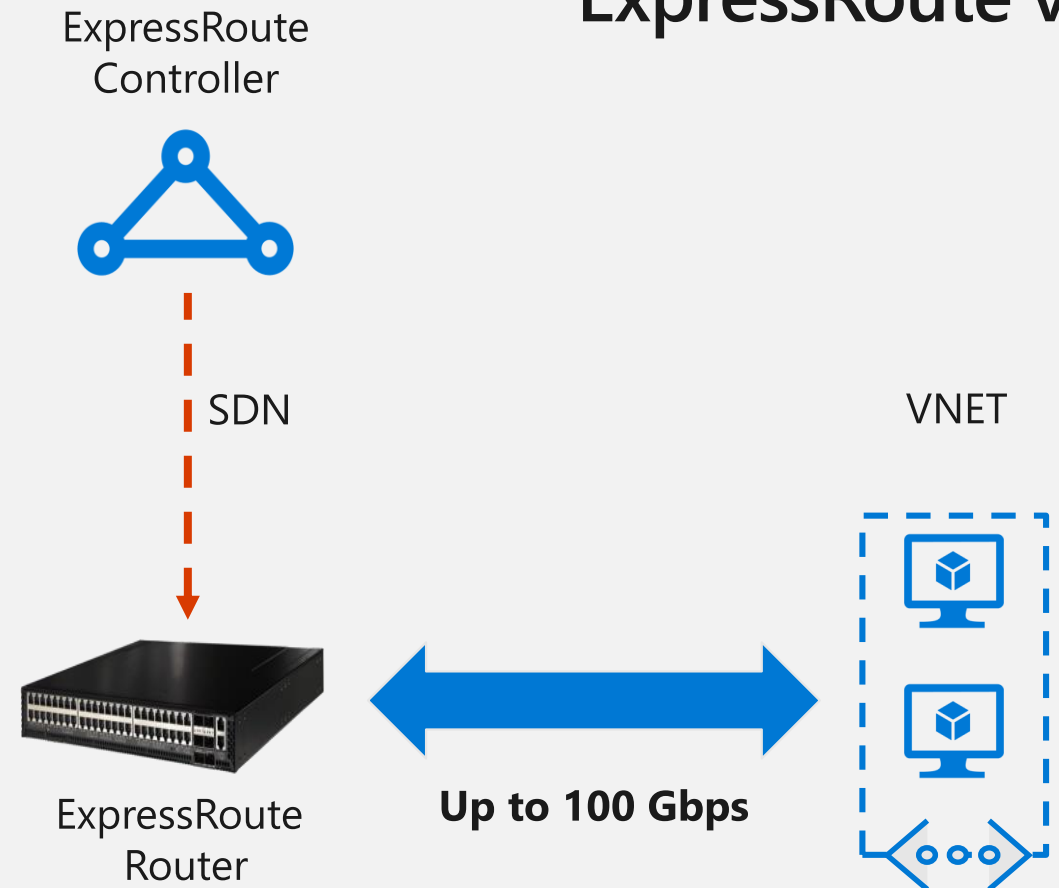
# Azure ExpressRoute

**10X** speed increase – now supporting **100 Gbps**  
Direct

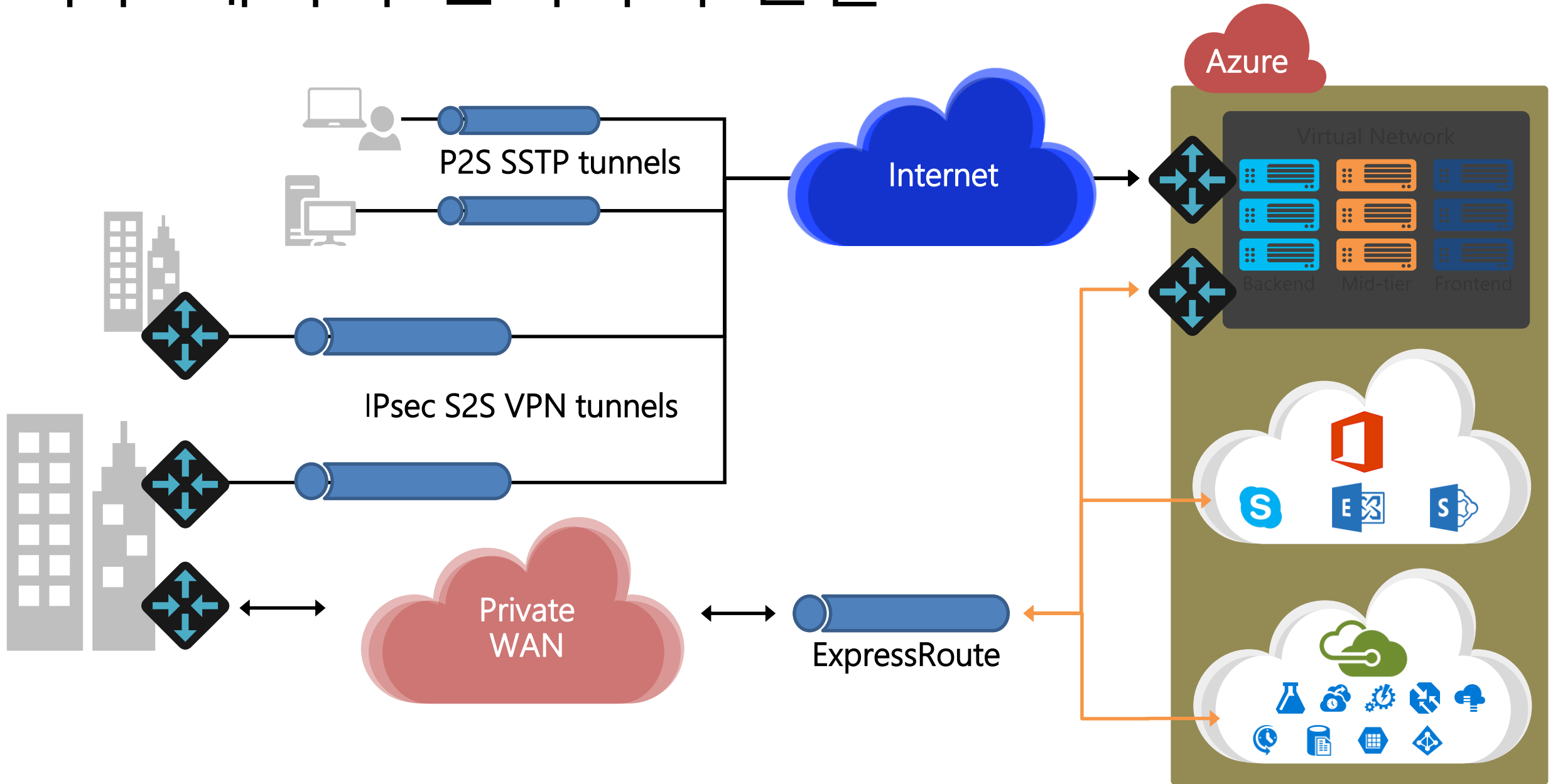
## ExpressRoute v1



## ExpressRoute v2



# 복수 데이터 센터와의 연결



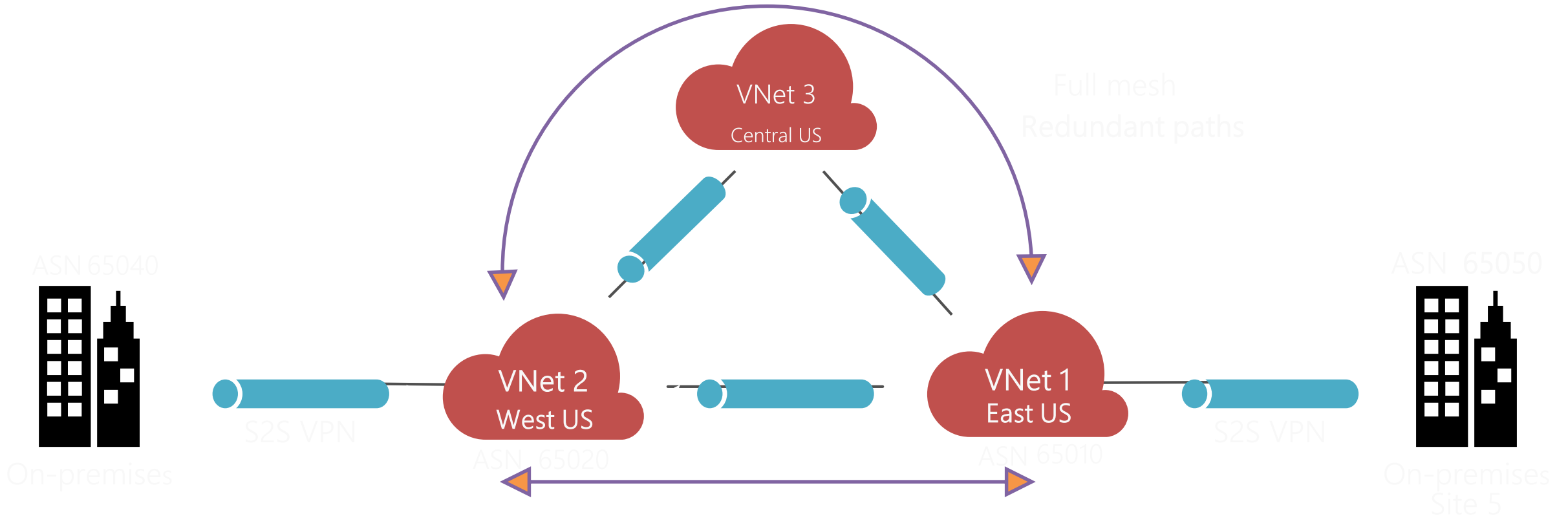
# 안전한 VPN 전송

## BGP for redundant paths and dynamic routing

- Automatic shortest path selection and failover

## Transit over Microsoft's Global Network

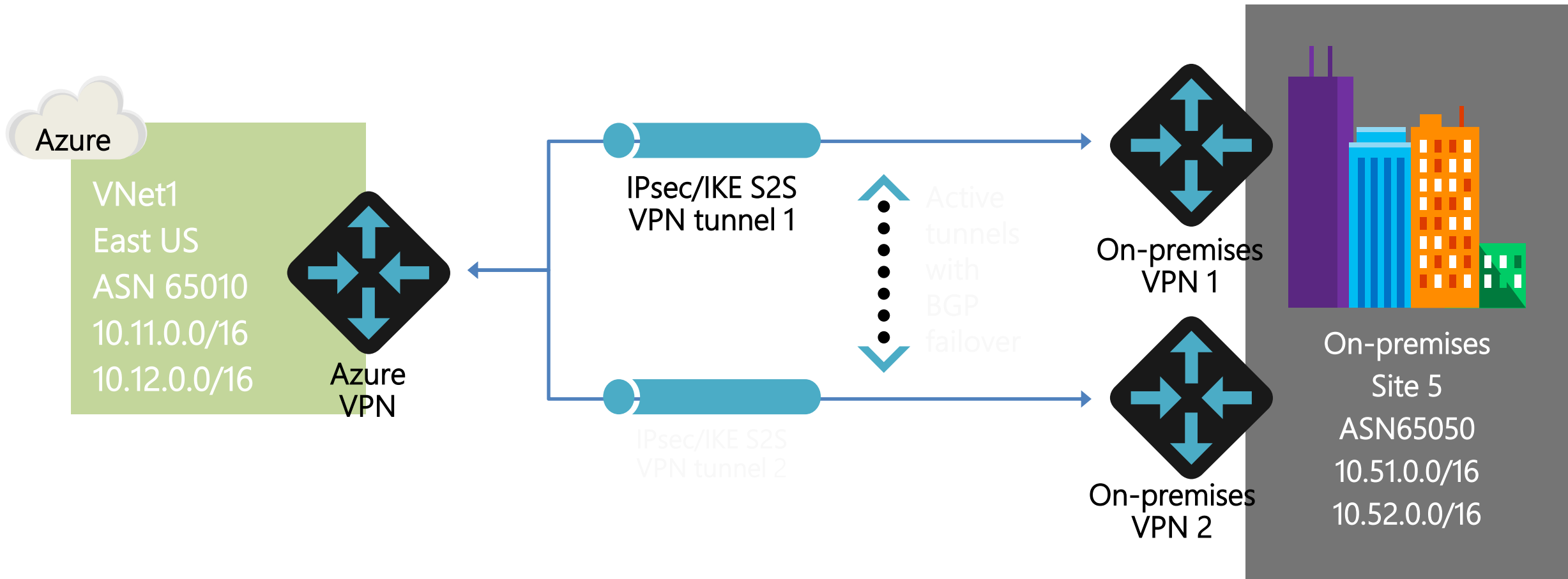
- Secure connectivity using Internet only for "last mile"



# 온-프레미스와의 연결

## Multiple tunnels/paths between VNets and on premises sites

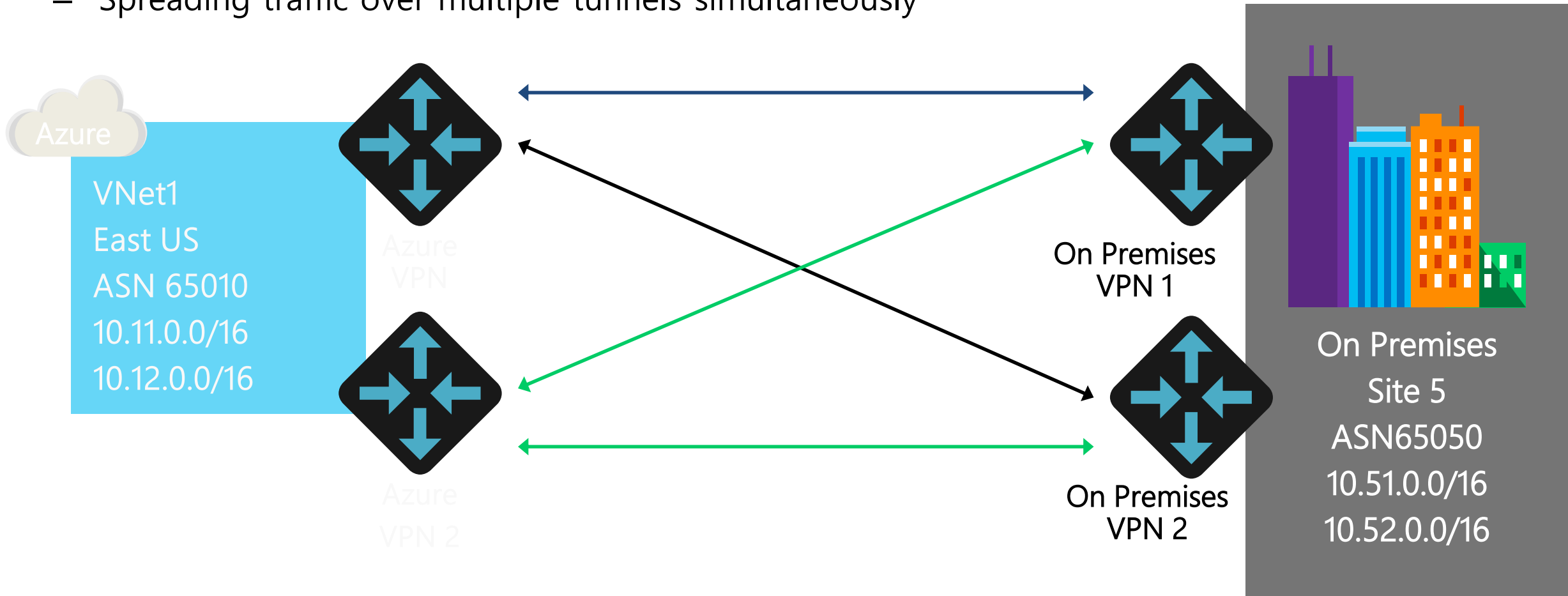
- Use BGP for reachability detection and path failover
- Support on-premises network with multiple ISPs and VPN devices



# Active-Active gateways 설정을 통한 가용성 확보

## Zero downtime during planned maintenance

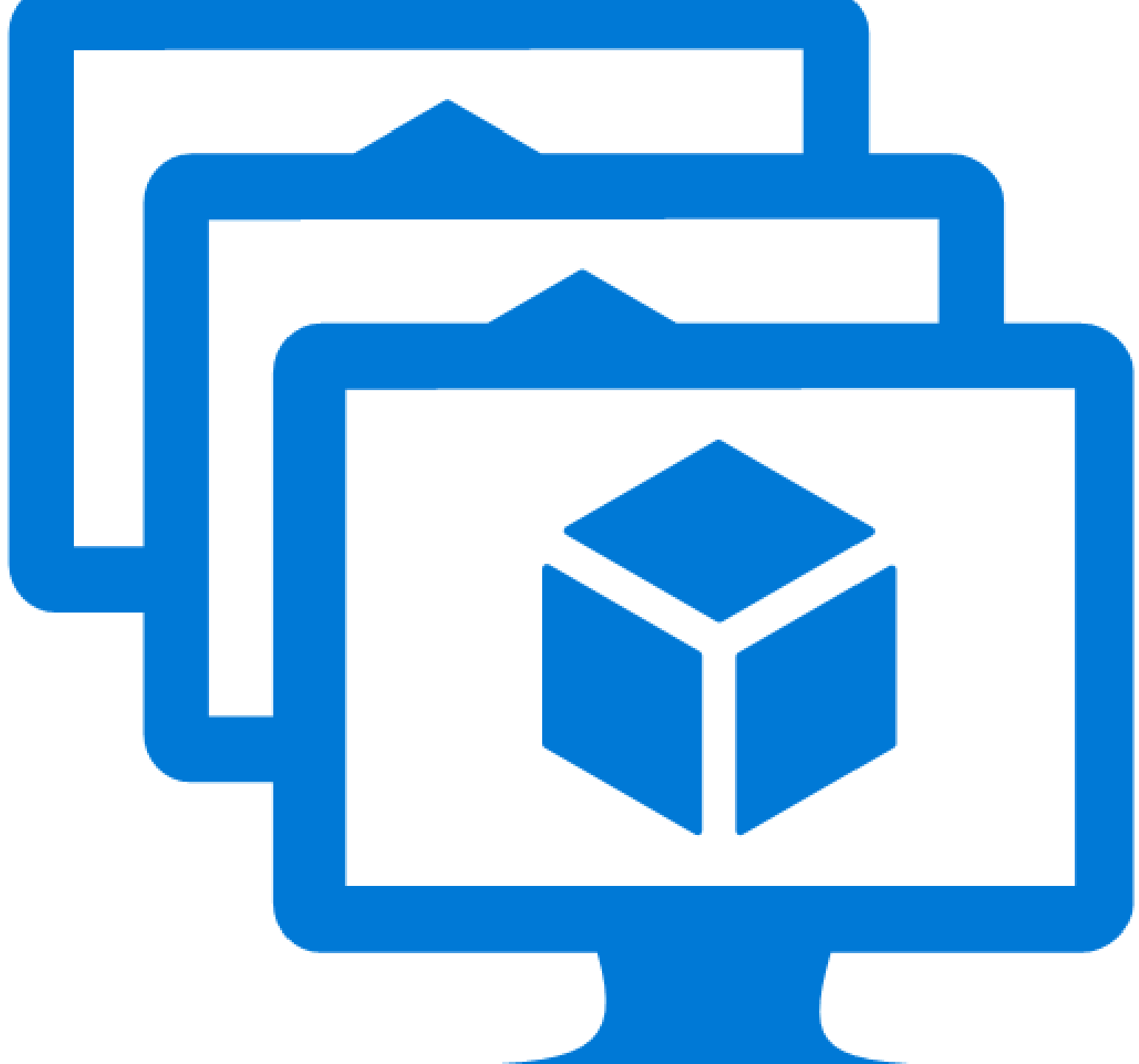
- From active-standby to active-active
- Support both cross-premises and VNet-to-VNet connectivity
- Spreading traffic over multiple tunnels simultaneously





# Azure CDN

---





# Why CDN? End users expect fast web experiences

73%

of mobile internet users say they've encountered a website too slow to load<sup>1</sup>

87%

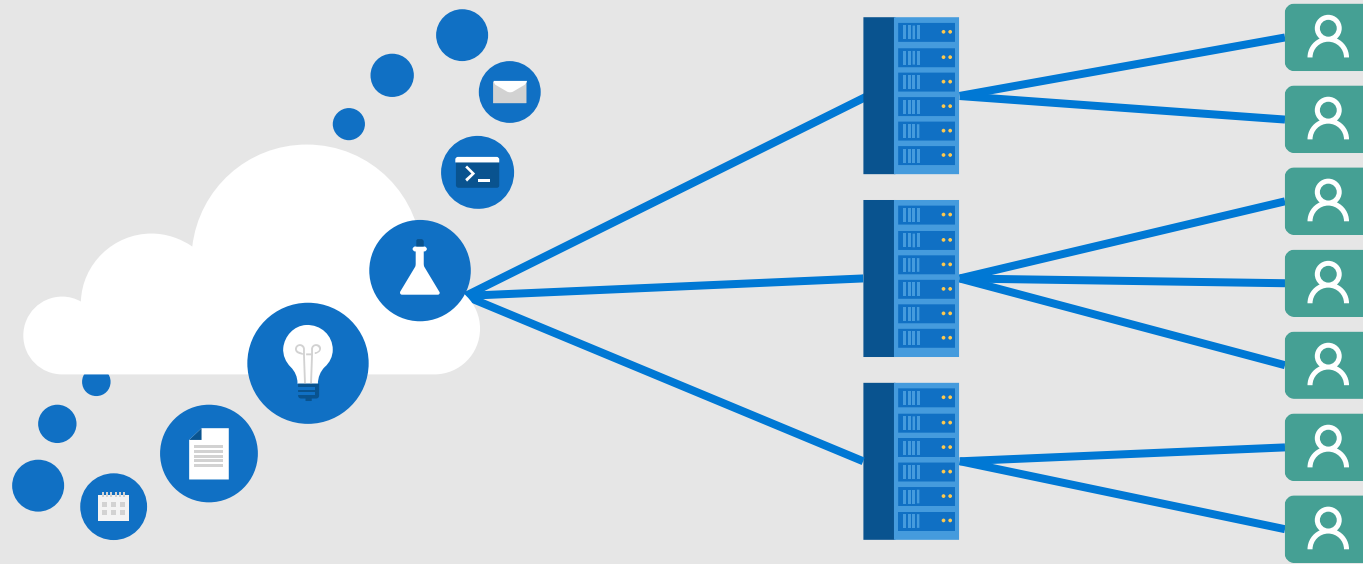
of viewers stop watching video if it takes more than 7 seconds to buffer<sup>2</sup>

87%

experience service degradation during security attacks.<sup>3</sup>

*"Google's search engine ranks pages based on load time, and Facebook will prioritize links that load quickly in its newsfeed." – **Section 10***

# CDN improves the customer experience



With traditional internet distribution, a single server sends your content to each end user. **A CDN delivers content through a network of servers closer to your end users.**

- ✓ Without a CDN, delivery of content suffers, yielding a poor customer experience due to routing complications, traffic and congestion, the explosion of devices, network types, and richer, more sophisticated content.
- ✓ Security threats start at the network layer, and attacks are increasing in scale, sophistication.
- ✓ Many customers may feel that CDN is not worth the extra effort. They want to avoid multi-year contracts and added complexity.

# Azure CDN Platform



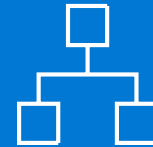
Domain  
Management



Origin Load  
Balancing



Caching and  
Streaming



Policy



Service  
Management



Optics and  
Self-Service



Locations



Performance



Network



Strengths



GA

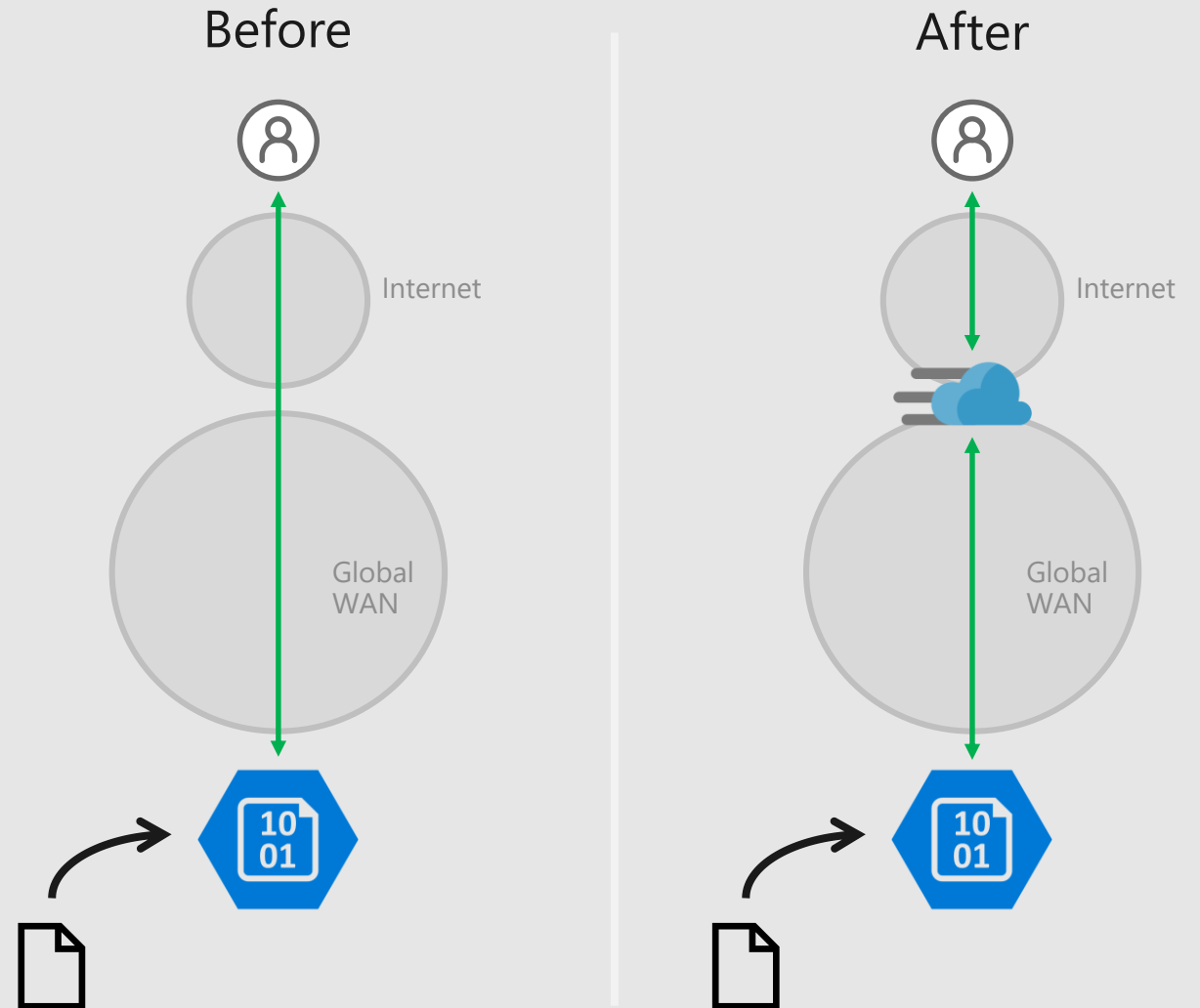
# Adding Azure CDN for your content

Scale out with CDN

Fast setup and support for custom domains, SSL certs

Portal and API managed

But what if I have live traffic to storage through my domain?



# 감사합니다

