Microsoft Azure | SCK

Microsoft Azure

Advanced Networking

2020.12.

혁신을 위해 신뢰할 수 있는 인프라

온-디멘드 글로벌 규모	Microsoft 워크로드에 적합	Linux, 오픈 소스, Red Hat 지원	특수 목적의 인프라 지원
60+ 지역	Windows Server를 위한 최상의 하이브리드 클라우드 경험	~50% Linux를 실행하는 Azure VM	SAP
글로벌 네트워크 160개 이상의 에지 사이트와 20,000개 피어링 연결	가장 비용 효율적으로 Azure VM에서 SQL 실행	1.4x Linux의 성장률	vmware
150 VM 크기 옵션	하이브리드 환경을 위한 포괄적인 보호	Red Hat과 코로케이션 지원	ORACLE
			NetApp
			CRAY

가용성 영역

데이터센터 장애로부터 보호를 제공하는 Azure 네이티브 HA/DR 솔루션의 일부

데이터 상주로 포괄적인 복원력

동일한 데이터 상주 경계 내의 가용성 영역과 이중으로 구성된 지역은 고가용성, 재해 복구, 백업을 제공

전체 데이터센터 손실에 대해 보호

각 영역은 물리적으로 분리되어 있고 독립적인 전원, 네트워크, 냉각시스템을 갖춘 하나 이상의 데이터센터로 구성되어 있음. 응용 프로그램과 데이터는 영역-중복 서비스를 통해 복제됨

99.99% SLA로 미션-크리티컬 응용 프로그램 실행

지역 내에 개별 가용성 영역에서 두 대 이상의 VM이 실행되는 경우 업계 최고의 SLA로 고가용성이 지원됨

Azure는 93개 컴플라이언스 오퍼링을 지원

Azure는 업계에서 가장 깊고 포괄적인 컴플라이언스 범위를 제공

https://aka.ms/AzureCompliance

Global

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 22301:2012
- ISO/IEC 27701:2019
- ISO 9001:2015
- ISO 20000-1:2011
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CIS Benchmark
- CSA STAR Certification
- CSA STAR Attestation
- CSA STAR self-assessment
- WCAG 2.0 (ISO 40500:2012)

US Gov

- FedRAMP high
- EAR
- ITAR
- DoD DISA SRG Level 5
- DoD DISA SRG Level 4
- DoD DISA SRG Level 2
- DFARS
- DoE 10 CFR Part 810
- NIST SP 800-171
- NIST CSF
- Section 508 VPATs
- FIPS 140-2
- CJIS
- IRS 1075
- CNSSI 1253

Industry

- PCI DSS Level 1
- GLBA (US)
- FFIEC (US)
- Shared assessments (US)
- SEC 17a-4 (US)
- CFTC 1.31 (US)
- FINRA 4511 (US)
- SOX (US)
- 23 NYCRR 500 (US)
- OSFI (Canada)
- FCA + PRA (UK)
- APRA (Australia)
- FINMA (Switzerland)
- FSA (Denmark)
- RBI + IRDAI (India)
- MAS + ABS (Singapore)
- NBB + FSMA (Belgium)
- HDS (France)
- K-ISMS
- AFM + DNB (Netherlands)
- AMF + ACPR (France)
- KNF (Poland)
- European Banking Authority (EBA)
- FISC (Japan)
- HIPAA BAA (US)
- HITRUST certification
- GxP (FDA 21 CFR Part 11)
- MARS-E (US)
- NEN 7510:2011(Netherlands)
- FERPA (US)
- CDSA
- MPAA (US)
- FACT (UK)
- DPP (UK)
- TISAX (Germany)
- NERC
- GSMA

Regional

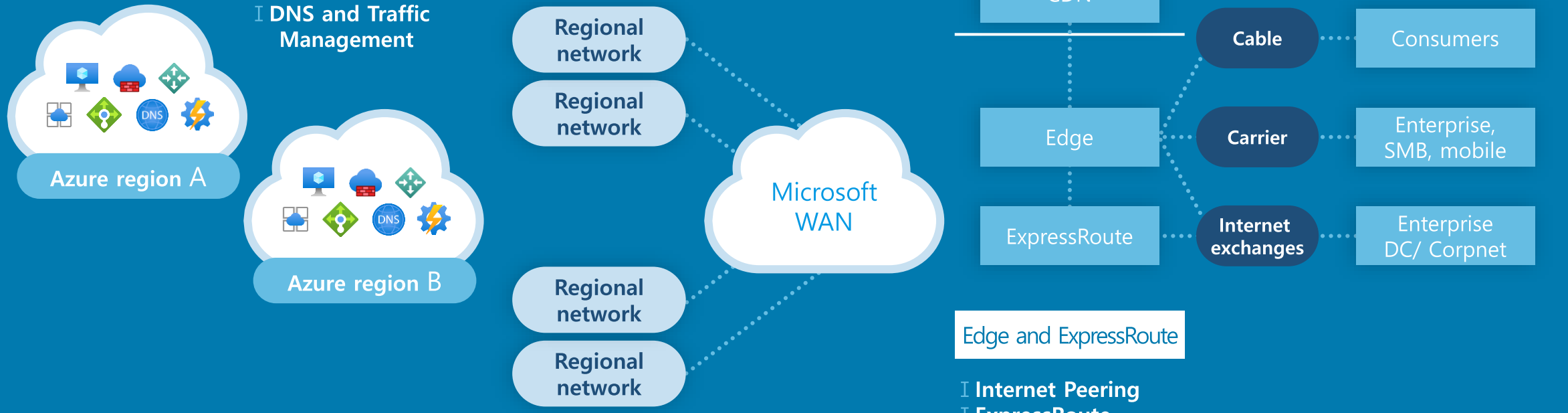
- Argentina PDPA
- Australia IRAP Unclassified
- Australia IRAP PROTECTED
- Canada Privacy Laws
- China GB 18030:2005
- China DJCP (MLPS) Level 3
- China TRUCS/CCCPPF
- EU EN 301 549
- EU ENISA IAF
- EU model clauses
- EU—US privacy shield
- GDPR
- Germany C5
- Germany IT-Grundschutz workbook
- India MeitY
- Japan CS mark gold
- Japan my number act
- Netherlands BIR 2012
- New Zealand Gov CIO Framework
- Singapore MTCS Level 3
- Spain ENS High
- Spain DPA
- UK cyber essentials plus
- UK G-Cloud
- UK PASF
- TruSight

Azure Networking 주요 서비스

Microsoft Azure Advanced Networking

Azure Networking 구성요소

하드웨어	서비스	리즌 간 구성요소	WAN 백본	CDN	Last mile
I SmartNIC/FPGA I SONiC	I Virtual Networks I Load Balancing I VPN Services I Firewall I DDoS Protection I DNS and Traffic Management	I DC Networks I Regional Networks I Optical Modules	I Software WAN I Subsea Cables I Terrestrial Fiber I National Clouds	I Acceleration for applications and content	I E2E monitoring (Network Watcher, Network Performance Monitoring)

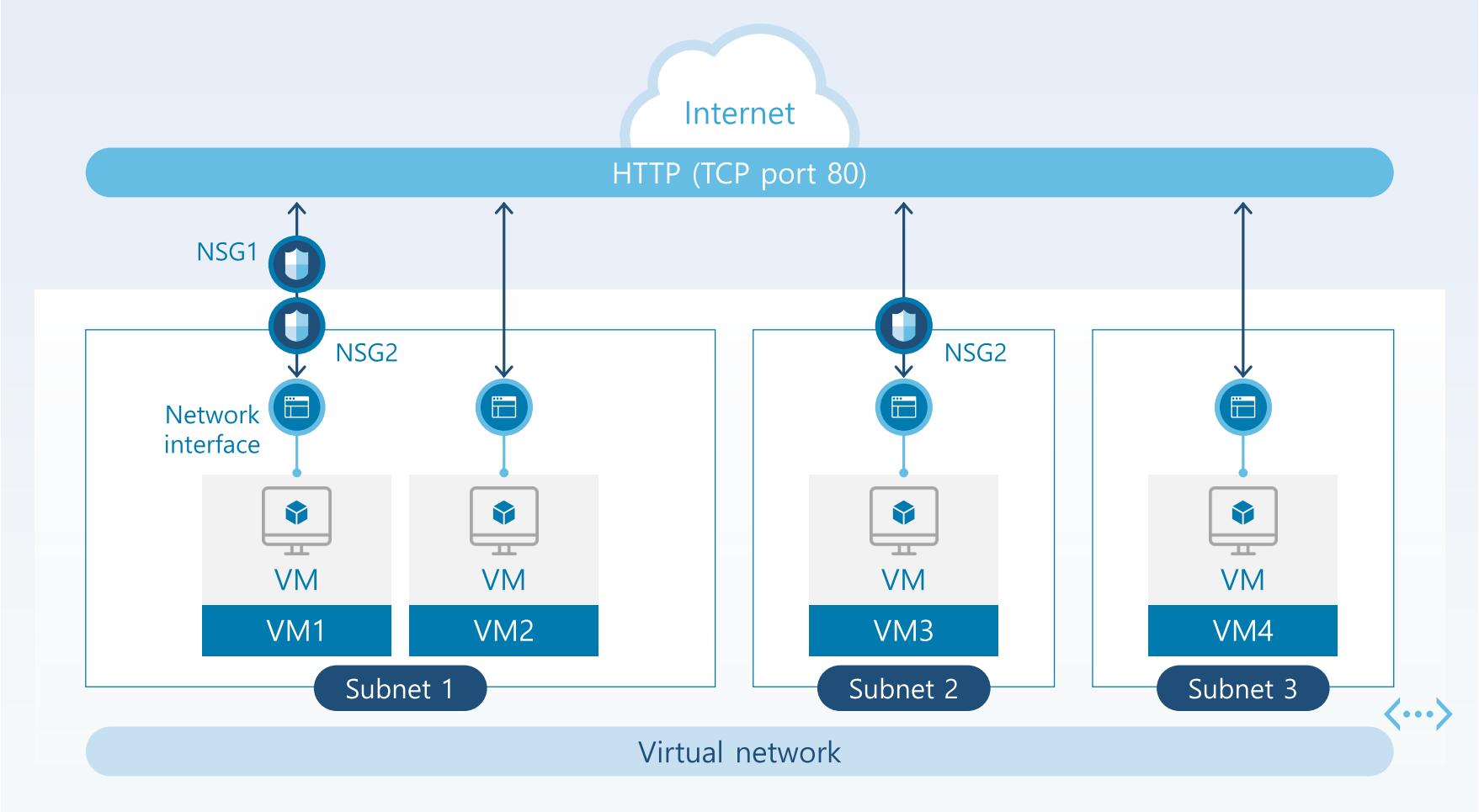


보안 관련
Network service

Microsoft Azure Advanced Networking

Network Security Group

네트워크 보안 그룹(NSG)은 여러 유형의 Azure 리소스에 대한 인바운드 및 아웃바운드 네트워크 트래픽을 허용 하거나 거부 하는 보안 규칙을 설정 하는 기능을 제공



Azure Firewall

Cloud native stateful Firewall as a service

중앙 거버넌스 제공

내장된 고가용성 및 자동 확장 제공
네트워크 및 애플리케이션 트래픽 필터링 제공
VNET 및 구독에 걸쳐 중앙화된 정책 제공

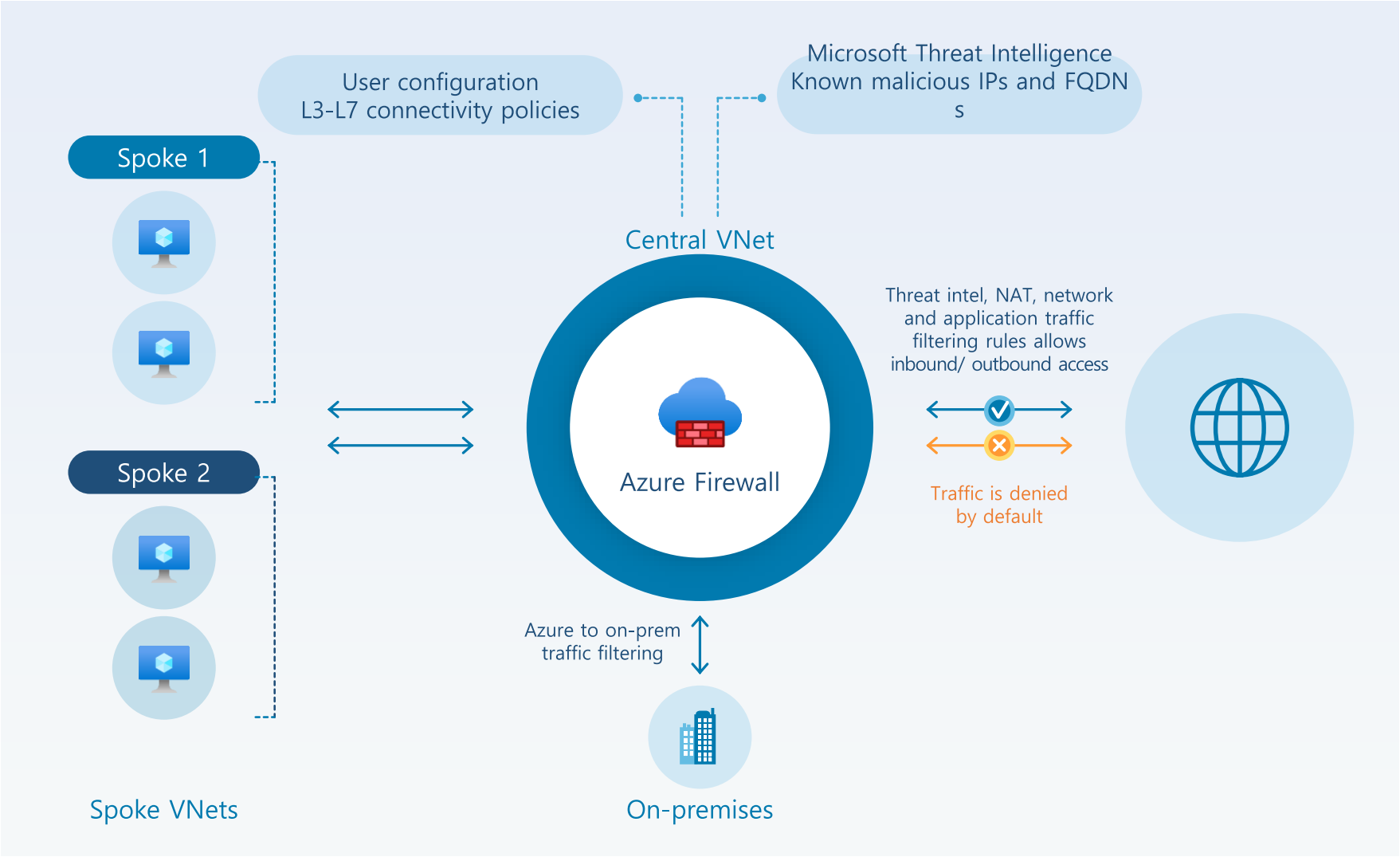
완벽한 VNET 보호

아웃 바운드, 인바운드, 스포크-스포크 및 하이브리드 연결 트래픽 필터링 (VPN 및 ExpressRoute)

중앙 집중식 로깅 기능 제공

로그를 스토리지 계정에 보관하고, 이벤트 허브로 이벤트를 스트리밍하거나, 선택한 Log Analytics 또는 SIEM (보안 통합 및 이벤트 관리) 시스템으로 보내는 기능 제공

Cloud Provider 중 유일한 FaaS 서비스



Azure Firewall

핵심 특징

애플리케이션 규칙

- FQDN Filtering
- FQDN Tags (e.g., Azure Backup, App Service Environment)
- 기본 인프라스트럭쳐 규칙 집합 제공

NAT 지원

- Default Source Network Address Translation (SNAT)
- Destination Network Address Translation (DNAT)

Threat Intel

- 알려진 IP 및 도메인에 대한 경고 및 거부

모니터링

- Azure monitor logging
- Azure monitor metrics

인바운드 및 하이브리드 연결에 대한 지원

- Network watcher 통합

Azure Firewall Manager

전 세계에 분산 된 소프트웨어 정의 경계에 대한 중앙 네트워크 보안 정책 및 경로 관리

중앙 배포 및 설정

- 여러 Azure Firewall 인스턴스 배포 및 구성
- 계층 적 정책으로 DevOps에 최적화

Automated routing

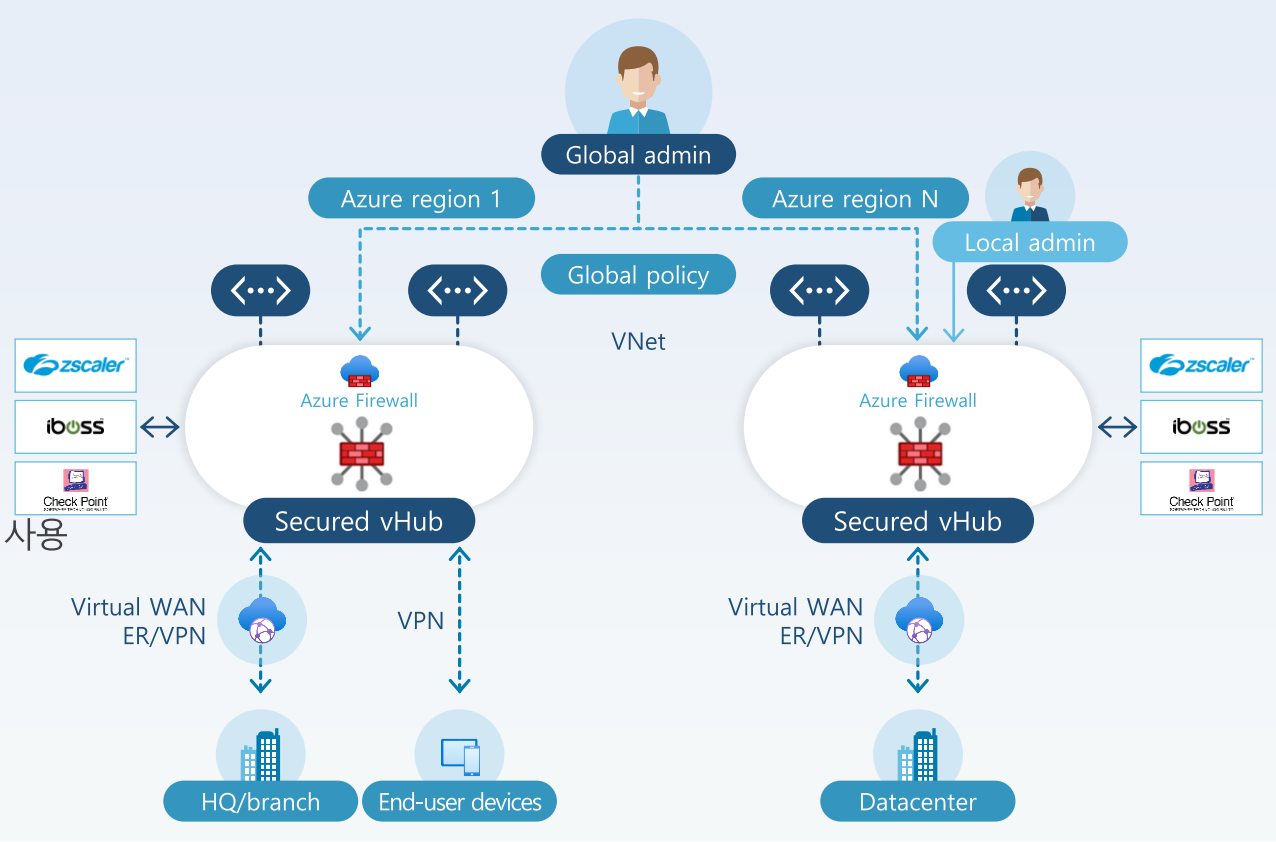
- 중앙 라우팅 구성을 사용하여 필터링 및
- 로깅을 위해 트래픽을 보안 허브로 쉽게 유도

Advanced security with 3rd party SECaaS

- 고급 인터넷 보안을 위해 동급 최고의 타사 보안 서비스 (SECaaS) 파트너 사용
- Private 트래픽을 위해 Azure Firewall과 결합

Virtual Network support, Split routing

- 가상 네트워크에서 Azure Firewall 지원
- 최적화 된 O365 및 Azure 공용 PaaS 액세스



주요
Network service

Microsoft Azure Advanced Networking

Azure Load Balancer

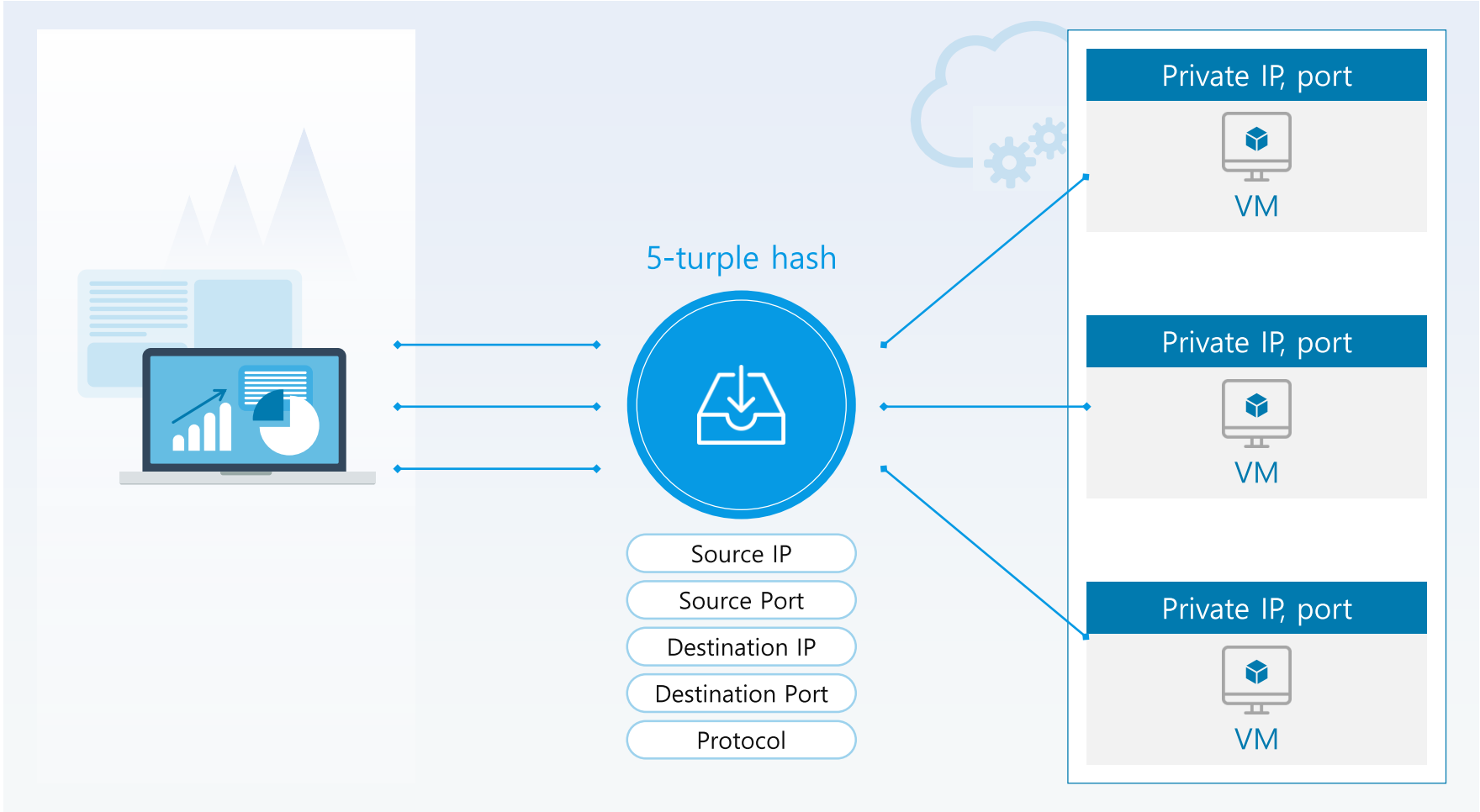
Layer 4 기반의 애플리케이션을 확장하고 서비스 및 애플리케이션에 대한 고가용성 및 복원성을 제공 하는 서비스

Public Load Balancer

들어오는 트래픽의 퍼블릭 IP 주소와 포트 번호를 VM의 프라이빗 IP 주소와 포트 번호에 매핑하고 그 반대의 경우도 동일한 서비스 제공

Internet Load Balancer

가상 네트워크 내부에 있거나 VPN을 사용하여 Azure 인프라에 액세스하는 리소스로만 트래픽을 보내는 기능



Public Load Balancer

Public Load Balancer 는 들어오는 트래픽의 공용 IP 주소와 포트 번호를 VM 의 사설 IP 주소 및 포트 번호에 매핑하는 기능을 제공하는 서비스

Automatic reconfiguration

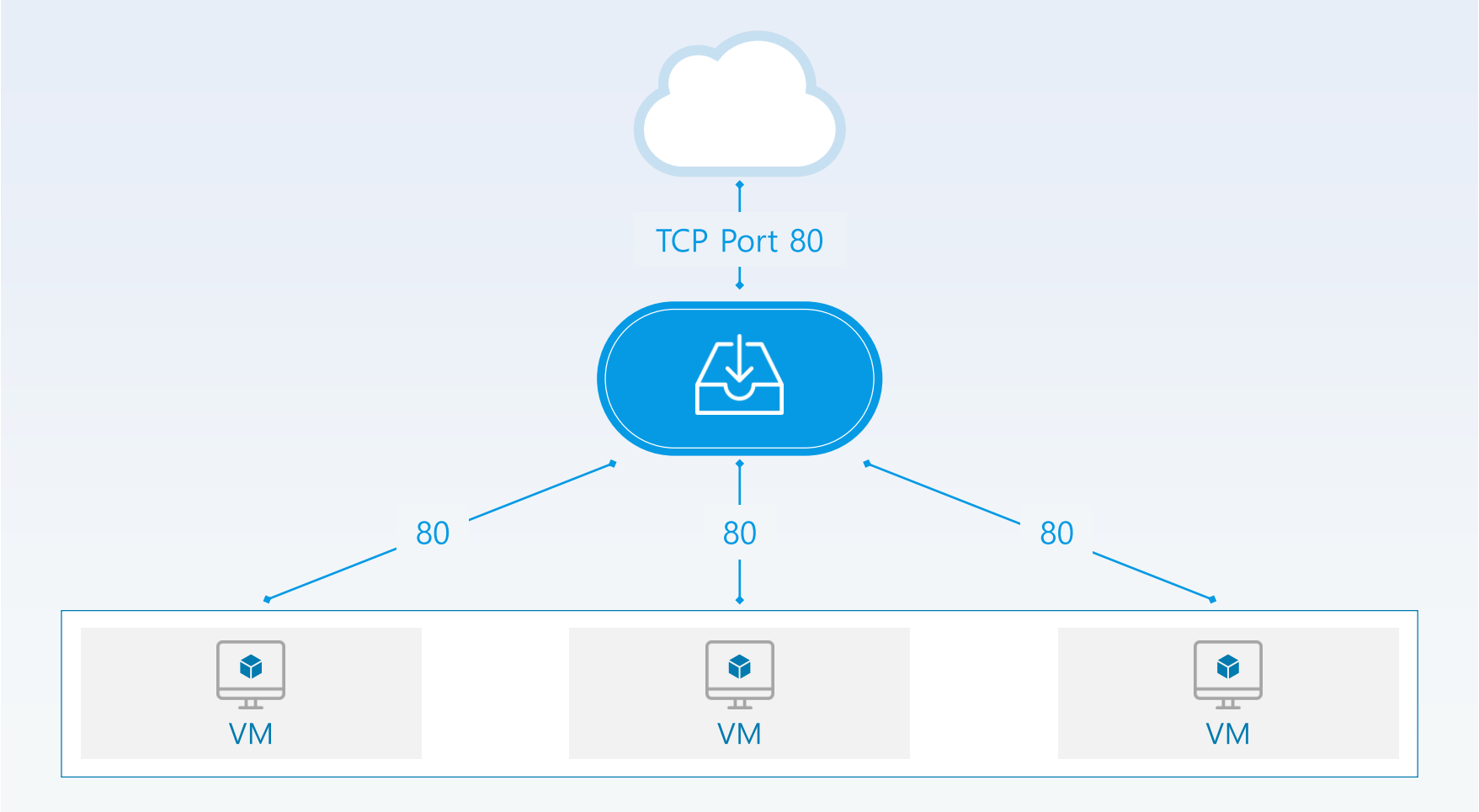
인스턴스를 확장하거나
축소 할 때 즉시 재구성

Outbound connections(SNAT)

가상 네트워크 내부의 개인 IP 주소에서 인터넷의 공용 IP 주소로의 모든 아웃바운드 흐름은 Load Balancer의 프런트 엔드 IP 주소로 변환 됨

Default Distribution Mode

Azure Load Balancer는 여러 VM 인스턴스 간에 트래픽을 균등하게 분산

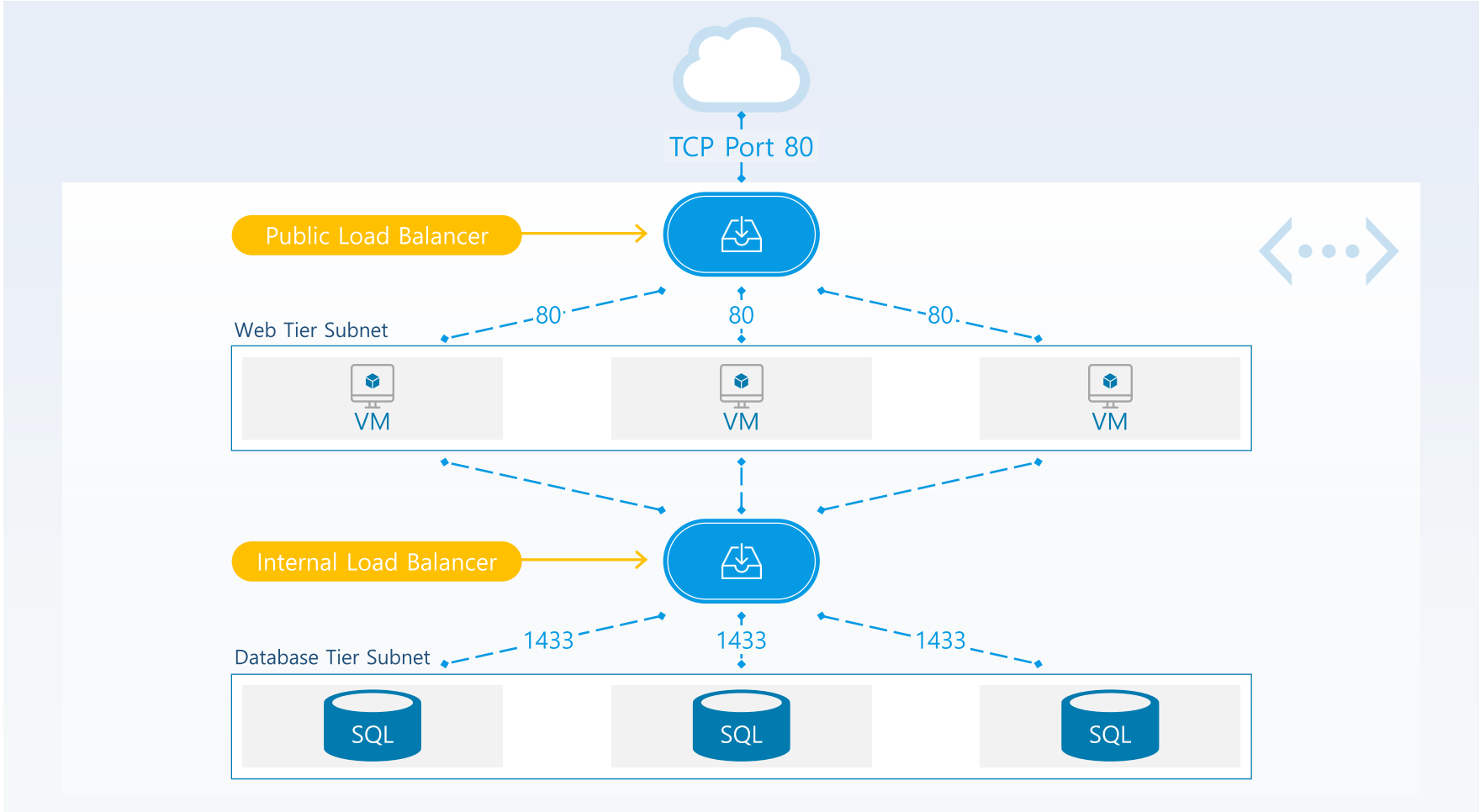


Internal Load Balancer

내부 Load Balancer는 가상 네트워크 내부의 리소스로만 트래픽을 전달하거나 VPN을 사용하여 Azure 인프라에 액세스

아래 케이스에 사용

- 가상 네트워크 내 running
- 크로스-프레미스 가상 네트워크
- 다 계층 애플리케이션
- LOB (기간 업무) 응용 프로그램

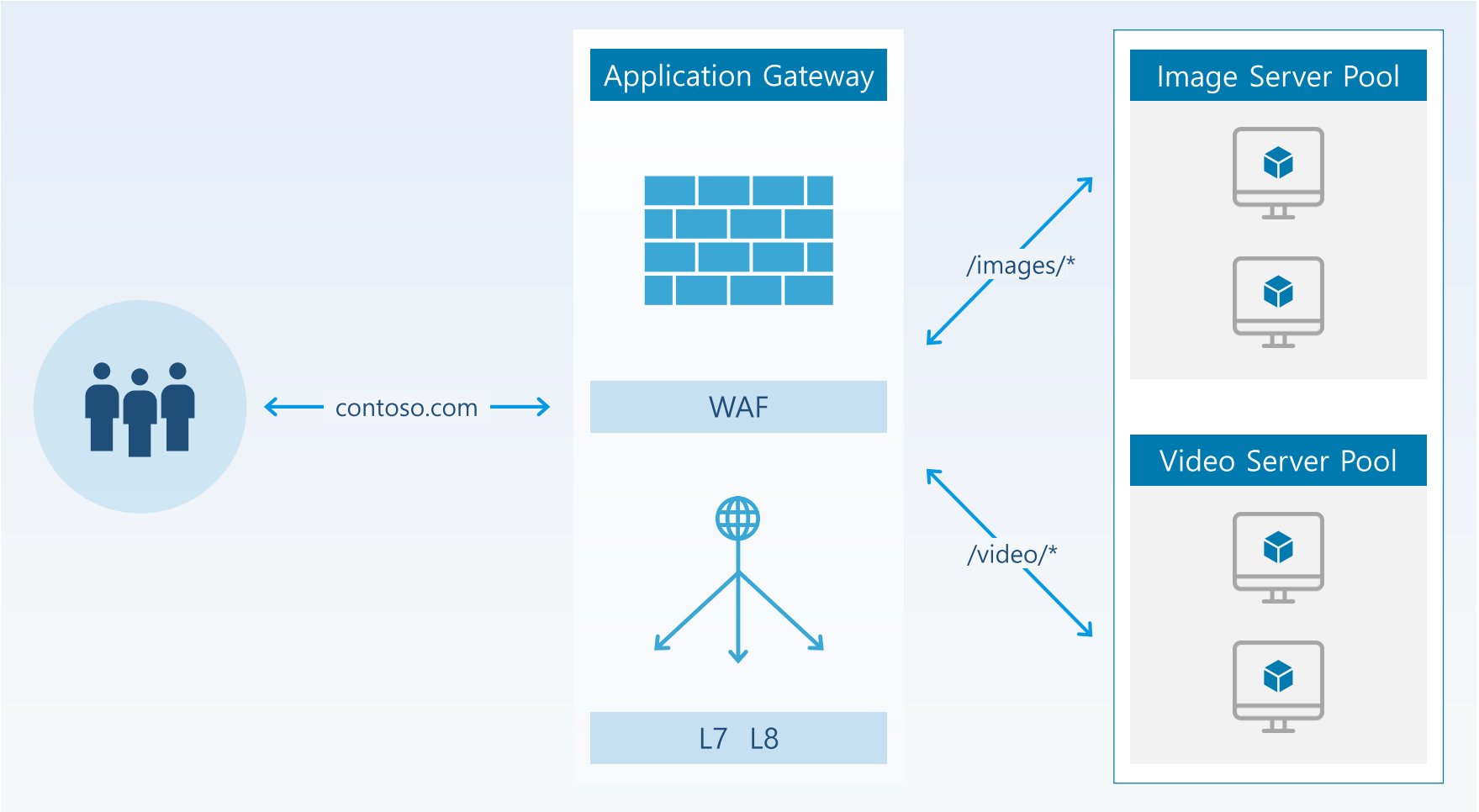


Azure Application Gateway(V2)

Azure Application Gateway는 웹 애플리케이션에 대한 트래픽을 관리 할 수 있는 웹 트래픽 부하 분산 장치(Layer 7 장치)

주요 기능

- Autoscaling
- Zone redundancy
- Static VIP
- Azure Kubernetes Service (AKS) Ingress controller
- Azure Key Vault integration
- Rewrite HTTP(S) headers
- URL-based routing
- Multiple-site hosting
- Traffic redirection
- Web Application Firewall (WAF)
- WAF custom rules
- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) termination
- End-to-end TLS encryption
- Session affinity
- Custom error pages
- WebSocket support
- HTTP/2 support
- Connection draining



Azure Traffic Manager

Azure Traffic Manager는 글로벌 Azure 지역의 서비스에 최적으로 트래픽을 분산 할 수 있는 DNS 기반 트래픽 부하 분산 장치

Global DNS load balancing

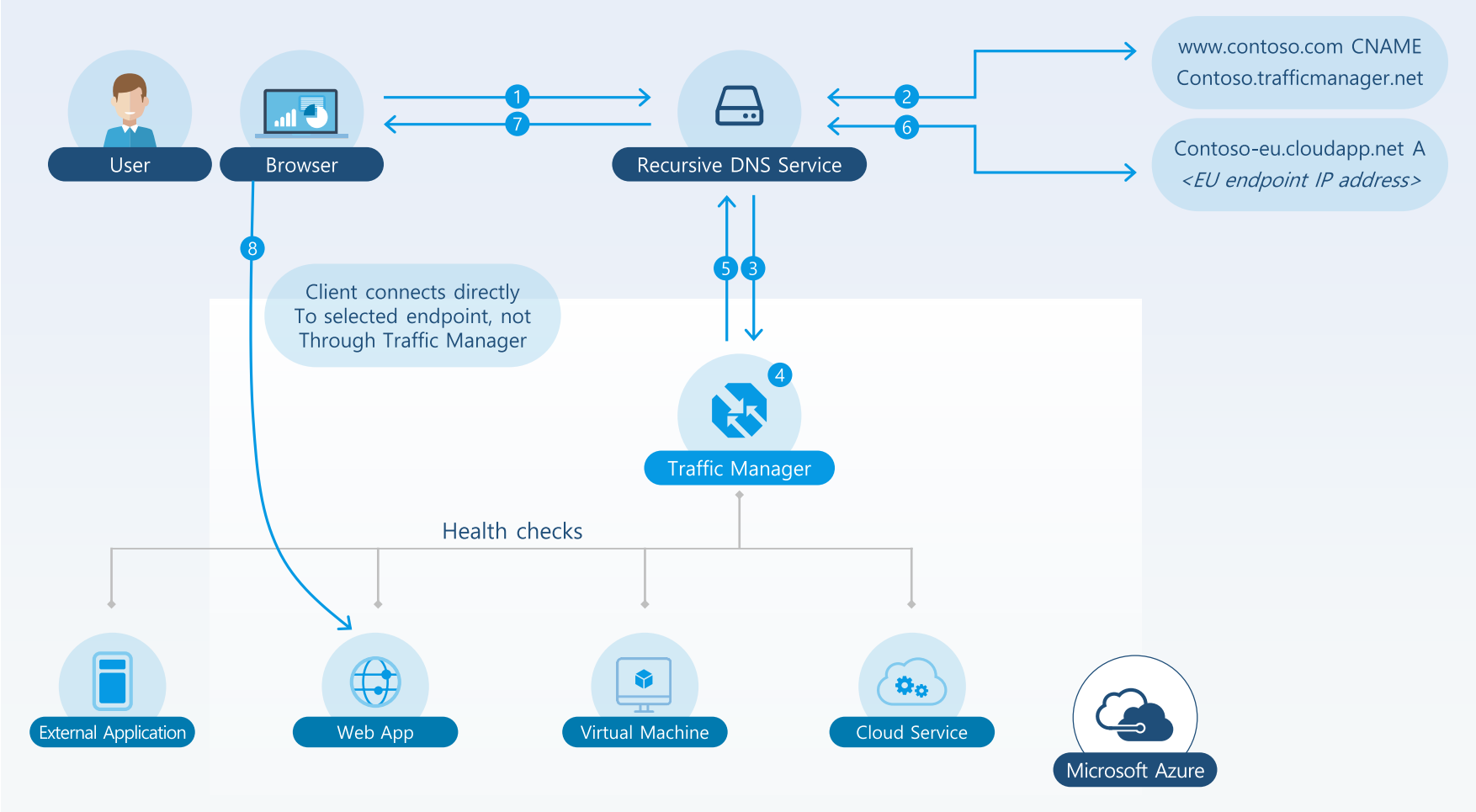
엔트포인트가 다운되었을 때 Automatic failover

하이브리드 애플리케이션 결합

외부의 비 Azure 끝점을 지원하므로 하이브리드 클라우드 및 온-프레미스 배포와 함께 사용할 수 있음

복잡한 배포를 위한 트래픽 분산

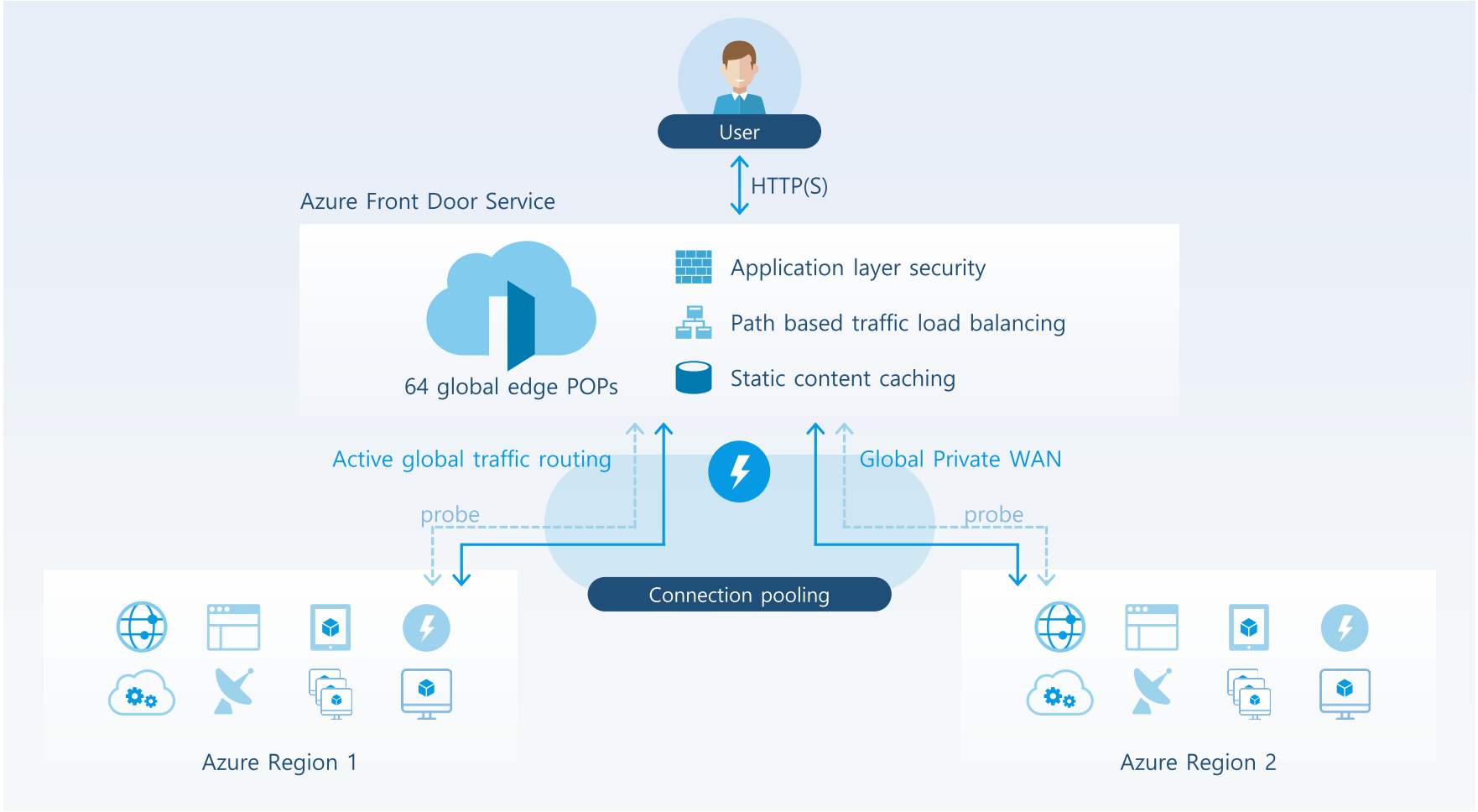
복잡한 배포를 위한 정교하고 유연한 규칙을 위해 중첩 된 Traffic Manager 프로필 사용



Azure Front Door

Azure Front Door Service는 글로벌 웹 애플리케이션의 빠른 제공을 위한 확장 가능하고 안전한 진입점을 제공

- SSL 오프로드 및 애플리케이션 가속화
- 즉각적인 장애 조치를 통한 글로벌 HTTP 부하 분산
- 애플리케이션 방화벽 및 DDoS 보호
- 중앙 집중식 트래픽 오케스트레이션 보기 제공



Traffic Manager 와 Front Door 의 차이점?

Traffic Manager	Front Door
Any protocol: Traffic Manager는 DNS 계층에서 작동하므로 모든 유형의 네트워크 트래픽을 라우팅 할 수 있습니다. HTTP, TCP, UDP 등	HTTP acceleration: Front Door를 사용하면 Microsoft 네트워크의 에지에서 트래픽이 프록시됩니다. 이로 인해 HTTP(S) 요청은 지연 시간 및 처리량이 향상되어 SSL 협상 지연 시간을 줄이고 AFD에서 애플리케이션으로의 핫 연결을 사용합니다.
On-premise routing: On-Premise 경로가 있는 경우에도 DNS 계층에서 라우팅 옵션을 사용할 수 있습니다.	Independent scalability: Front Door는 HTTP 요청과 함께 작동하므로 서로 다른 URL 경로에 대한 요청은 규칙 및 각 애플리케이션 마이크로 서비스의 상태에 따라 서로 다른 백엔드/지역 서비스 풀 (마이크로 서비스)로 라우팅 될 수 있습니다.
Billing format: DNS 기반 청구는 사용자와 더 많은 사용자가 있는 서비스에 대해 확장되며 사용량이 많을 때 비용을 줄이기 위해 정체됩니다.	Inline security: Front Door는 트래픽이 애플리케이션에 도달하기 전에 백엔드를 보호 할 수 있도록 속도 제한 및 IP ACL과 같은 규칙을 활성화합니다.

Azure Virtual WAN

관리되는 허브&스포크 아키텍처

I 공용(VPN) 및
사설(ExpressRoute) 연결

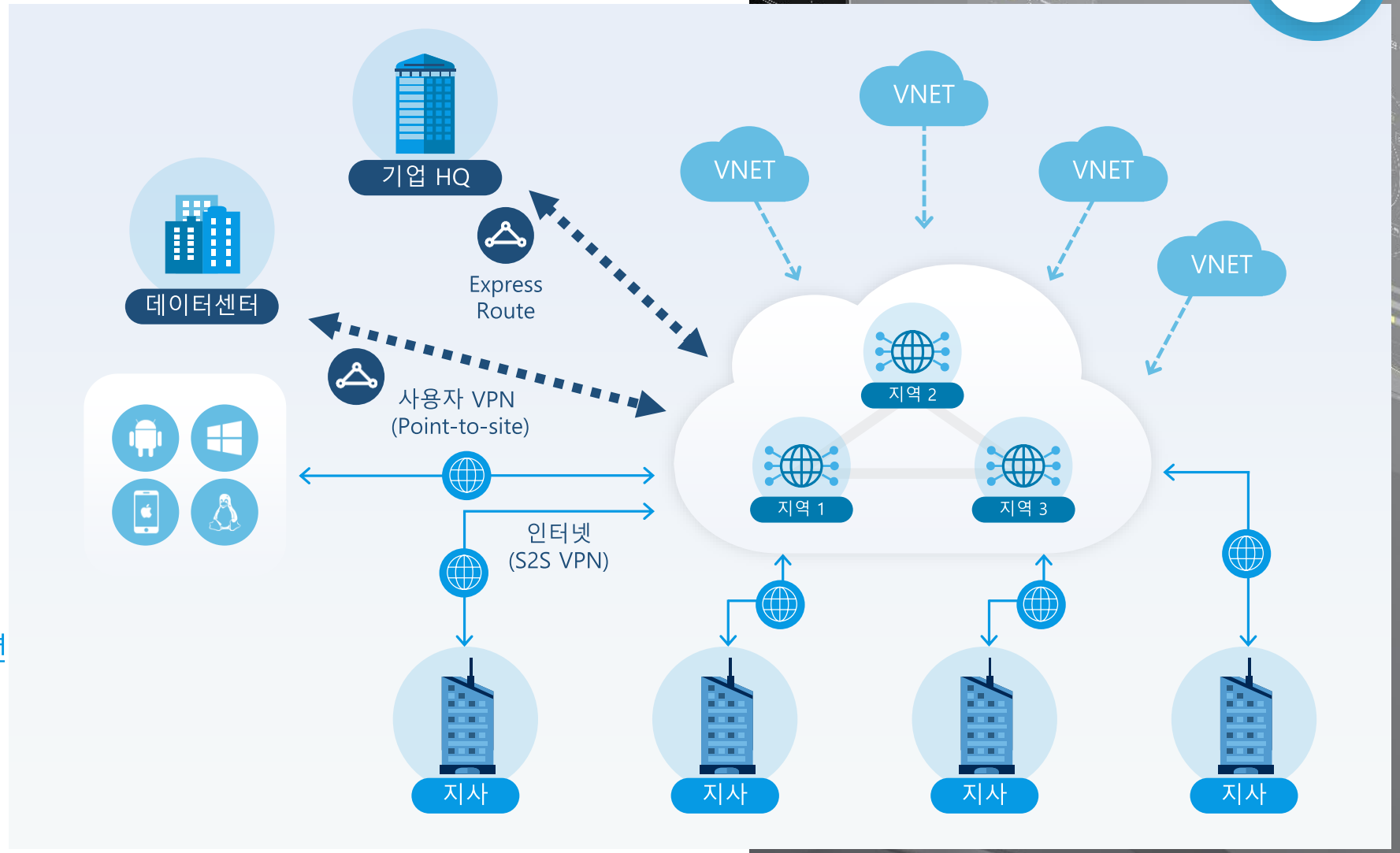
글로벌 규모

I 20Gbps S2S VPN + 20Gbps ER
+ 20Gps 사용자 VPN (P2S)
I 허브당 10K 사용자
I 허브 당 1000개 사이트

전송Transit 라우팅

클라우드 네트워크 오케스트레이션

I 자동화된 대규모 지사/
SDWAN CPE 연결



End-To-End Network service

Microsoft Azure Advanced Networking

Azure VPN Gateway

On-Premise 와 IPSec VPN 연결을 하기 위한 서비스

S2S

High throughput VPN – 10Gbps
- New Azure VPN gateways – VpnGw3/4/5
- Up to 10 Gbps aggregate
- Up to 10,000 P2S connections

IKEv1 + IKEv2 on VpnGw1-5
- IKEv1 on new VpnGw SKUs (1 ~ 5)
- Multiple IKEv1 S2S tunnels
- IKEv1 and IKEv2 on the same VPN gateway

VPN gateway packet capture
- With 5-tuple packet filter
- ETW or PCAP formats

Custom IKE traffic selectors

P2S

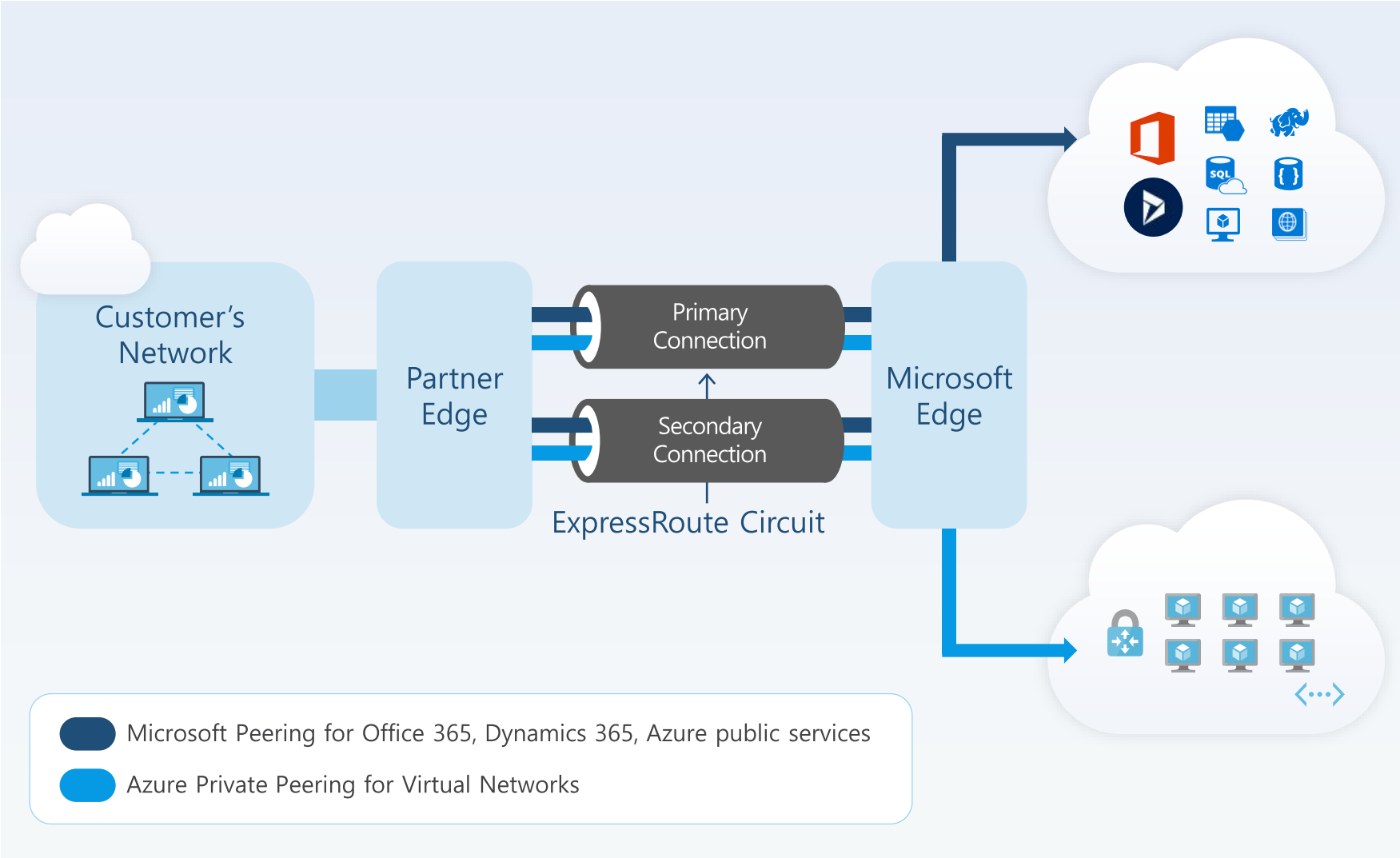
AAD auth + MFA PREVIEW

Azure VPN Client (Windows App)
- OpenVPN protocol
- Native AAD authentication with MFA
- Client-side Diagnostics, Logs, & Metrics

SKUs	Aggregate throughput	P2S connections	IKEv1/v2
VpnGw1	**650 Mbps**	**250**	**IKEv1+IKEv2**
VpnGw2	**1 Gbps**	**500**	**IKEv1+IKEv2**
VpnGw3	**2.5 Gbps**	**1000**	**IKEv1+IKEv2**
VpnGw4	**5 Gbps**	**5,000**	**IKEv1+IKEv2**
VpnGw5	**10 Gbps**	**10,000**	**IKEv1+IKEv2**

Express Route

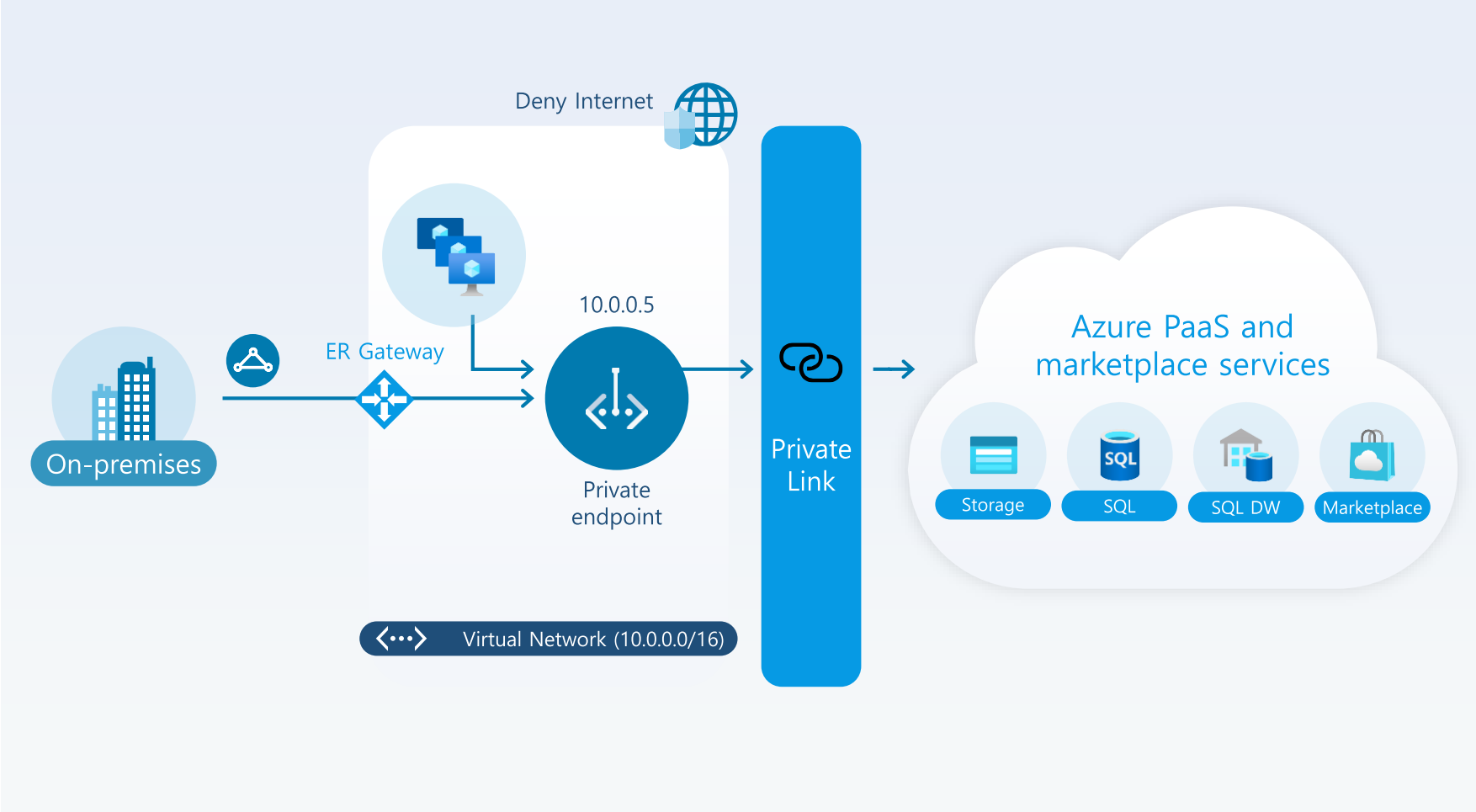
Azure DataCenter 와 Private 연결을 위한 전용선 서비스



Azure Private Link

Azure Storage, SQL DB 및 데이터 유출 보호를 위한 Private Link

- VNet, 피어링 된 VNet 및 온-프레미스에서 비공개 액세스
- 내장된 데이터 유출 방지
- PaaS 리소스에 대한 예측 가능한 프라이빗 IP 주소
- PaaS, 고객 소유 및 시장 서비스 전반에 걸친 통합 경험

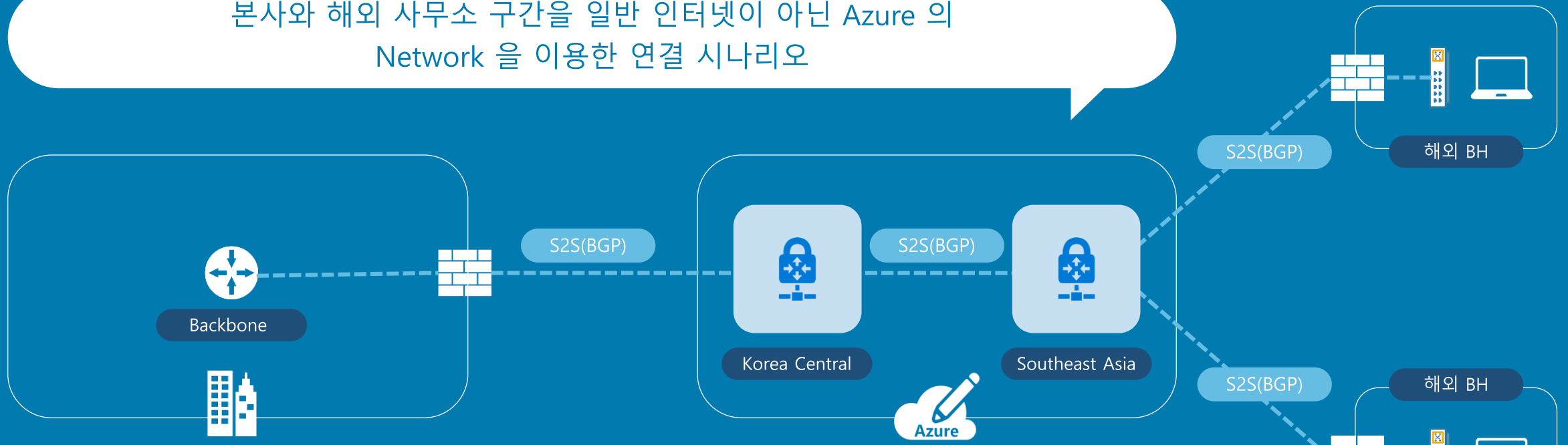


Advanced Network 시나리오

Microsoft Azure Advanced Networking

본사와 해외 지사간 S2S 연결 시나리오

본사와 해외 사무소 구간을 일반 인터넷이 아닌 Azure 의
Network 을 이용한 연결 시나리오



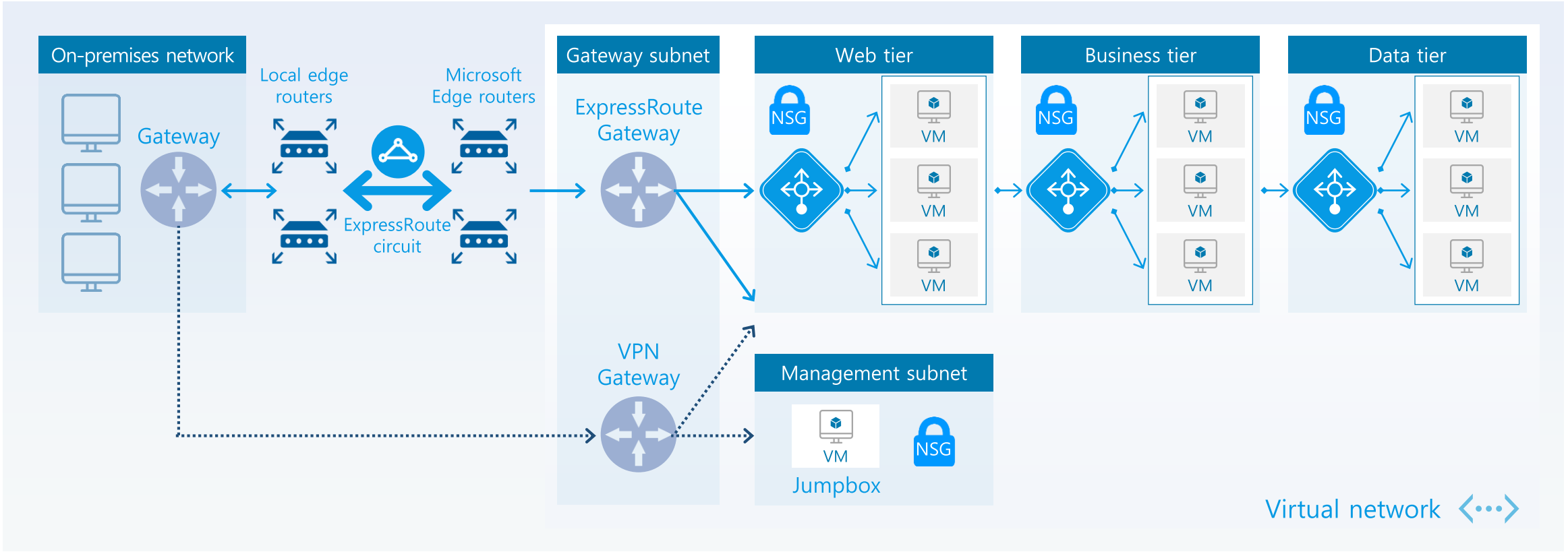
빠른 Azure Backbone 을 이용하여 본사와 해외지사 연결
On-Premise 장비에 대한 구성 변경 없이 S2S 연결만 이용하여 연결 하는 시나리오

본사와 Azure Datacenter 구간 사이의 전용선 연결

본사와 Azure Datacenter 구간을 전용선을 이용하여 연결
50M ~ 최대 10Gbps 의 연결 속도 제공

ER + VPN 을 이용한 고가용성 Hybrid 연결 시나리오

On-Premise 와 Azure Datacenter 사이에 ER 과 VPN 을 이용한 고가용성 시나리오

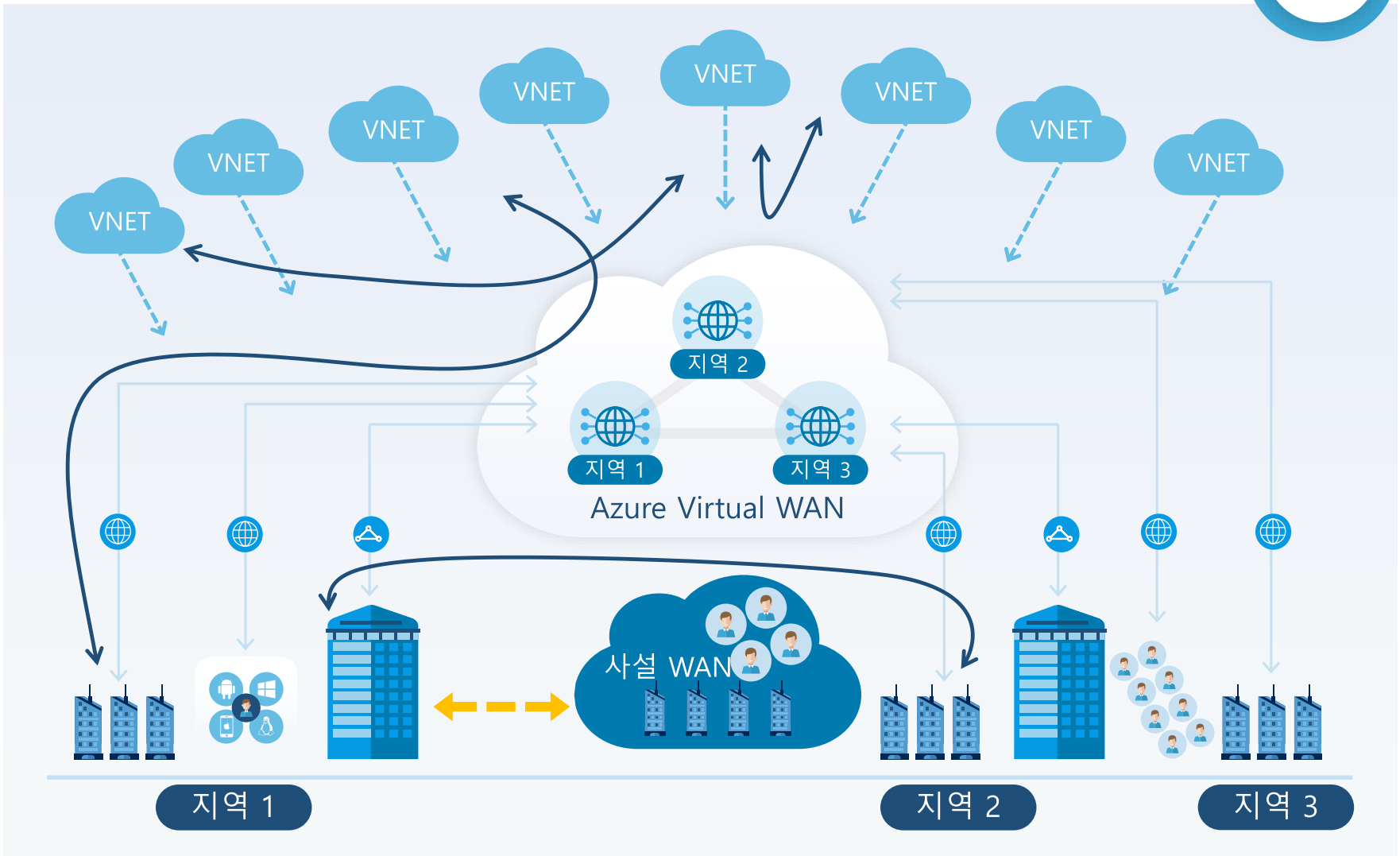


Azure Virtual WAN으로 글로벌 Branch 연결

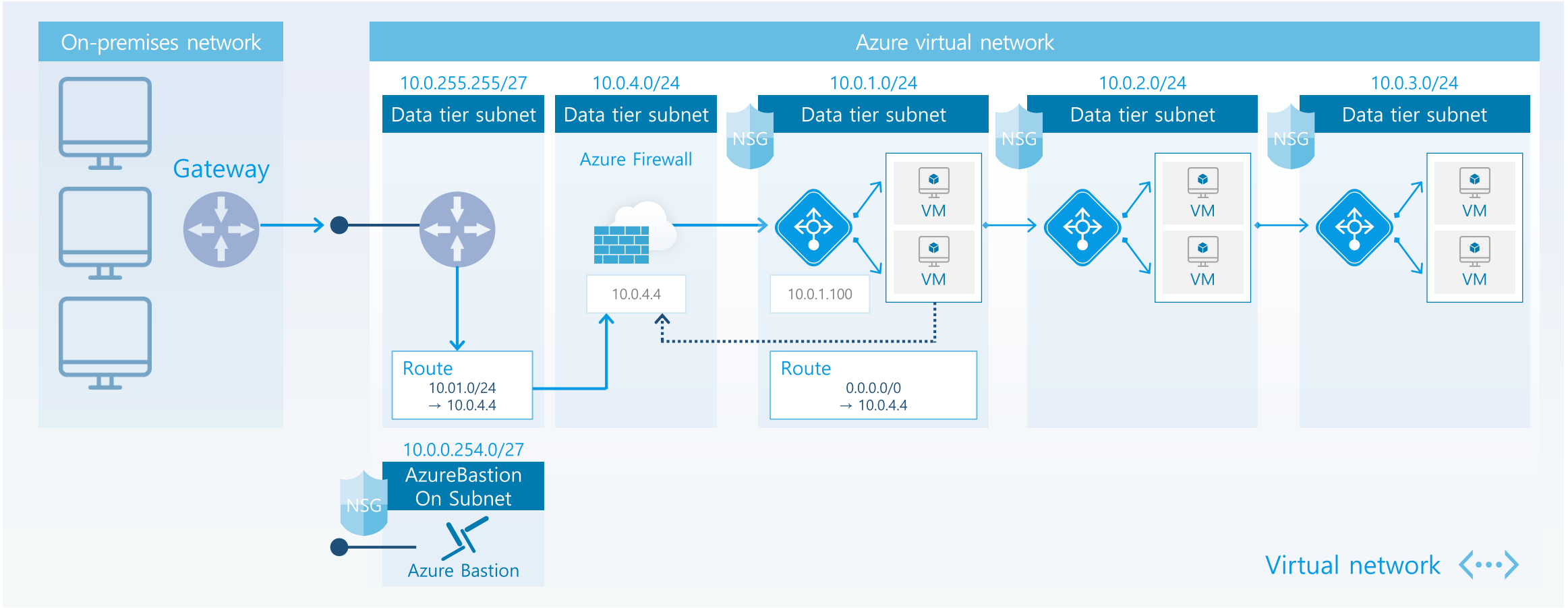
단순화된 네트워크, 손쉬운 사용, 운영비용 절감

Any-to-any 연결

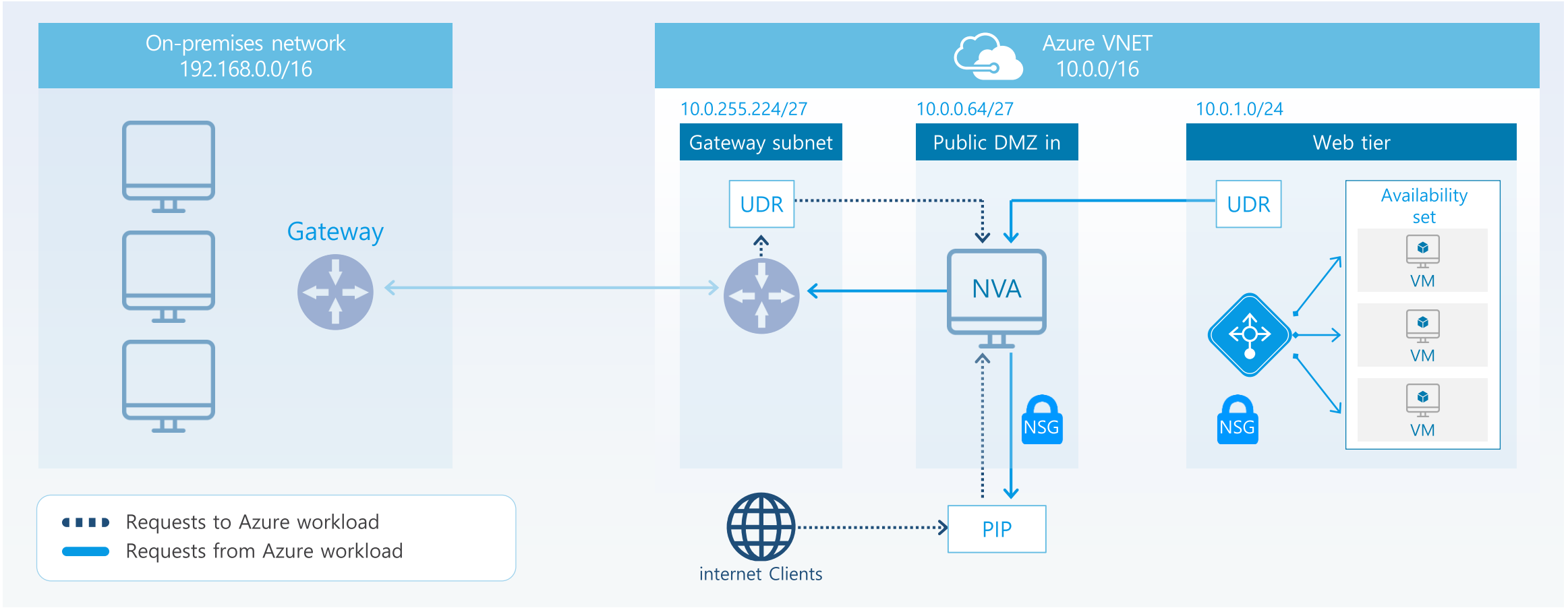
- 풀메시 허브
- 지사에서 Azure로
- 지사에서 지사로
- VPN <-> ER
- 사용자 VPN <-> 사이트
- VNET to VNET



Azure Firewall 을 이용한 DMZ 배포 시나리오



3rd Party MVA(Cisco, Juniper, Fortinet) 을 이용한 배포 시나리오



감사합니다

Microsoft Azure Advanced Networking

SCK