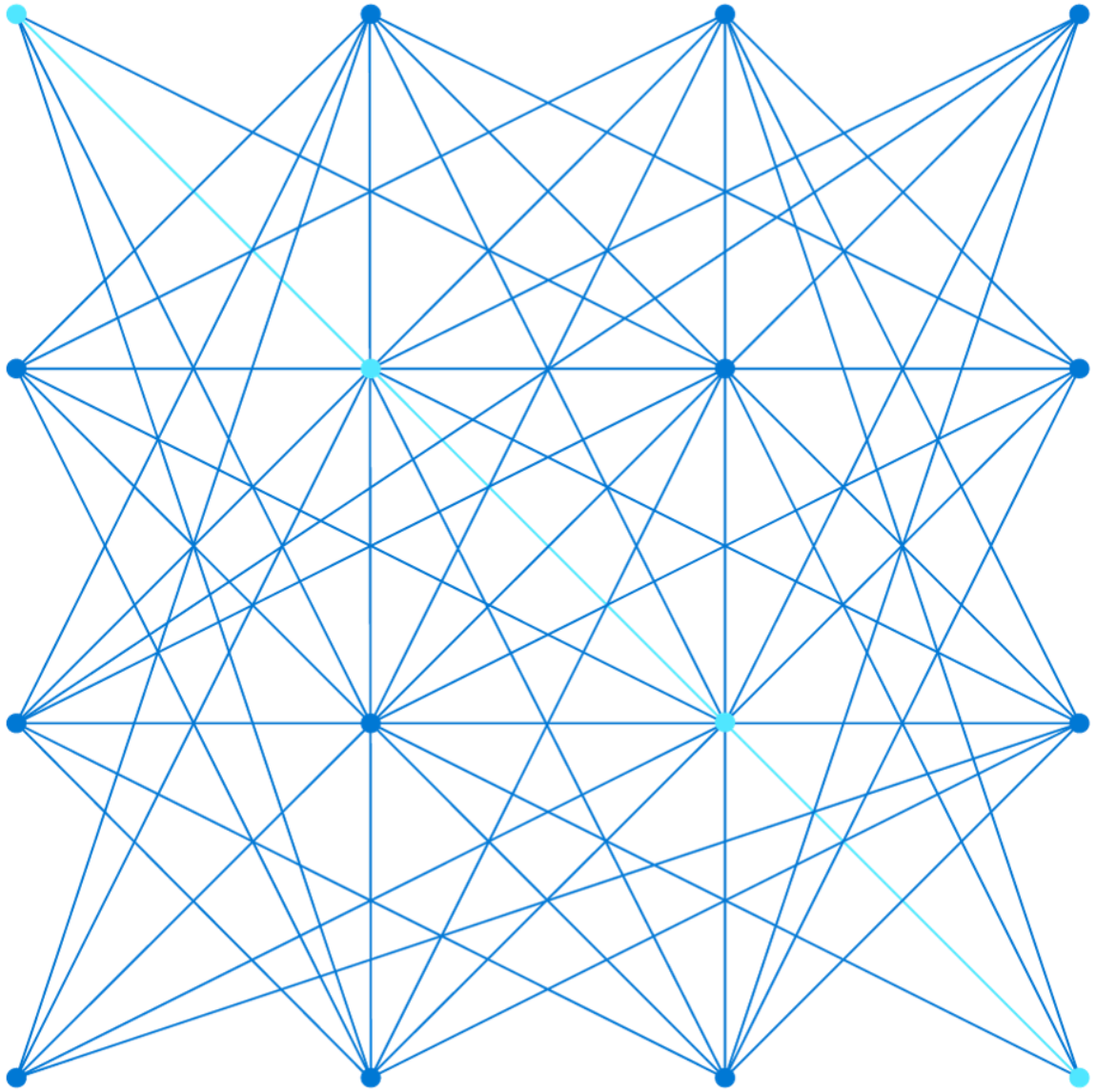
Microsoft Azure

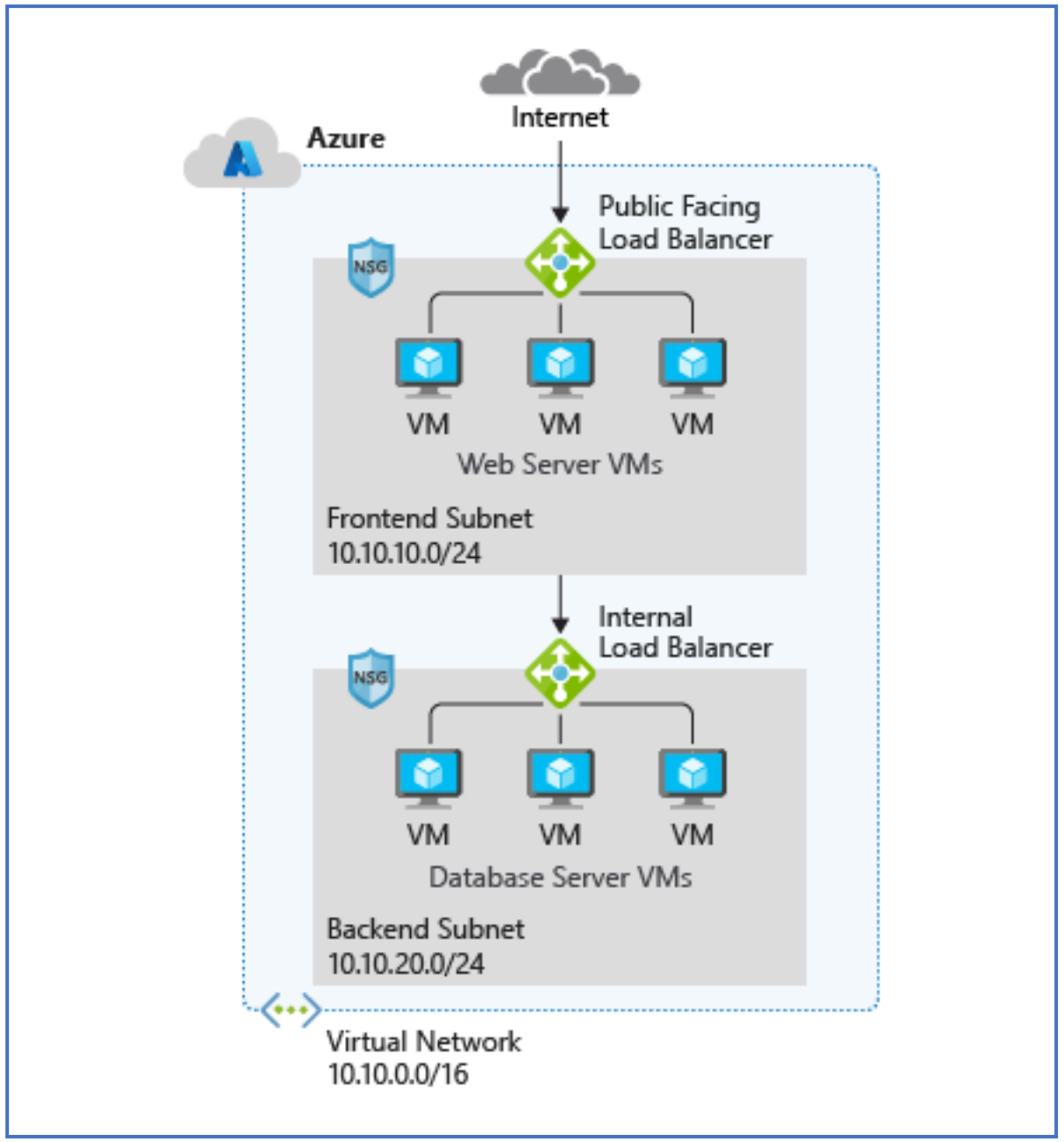
Introduction to Azure Virtual Networks



Lesson: Explore Azure Virtual Networks

Capabilities of Azure Virtual Networks

- Communication with the Internet
- Communication between Azure resources
- Communication between on-premises resources
- Filtering network traffic
- Routing network traffic



Virtual Network address space

RFC 1918
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Azure reserves 5 IP addresses

- x.x.x.0: Network address
- x.x.x.1: Reserved by Azure for the default gateway
- x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
- x.x.x.255: Network broadcast address

Unavailable address ranges:

- 224.0.0.0/4 (Multicast)
- 255.255.255.255/32 (Broadcast)
- 127.0.0.0/8 (Loopback)
- 169.254.0.0/16 (Link-local)
- 168.63.129.16/32 (Internal DNS)

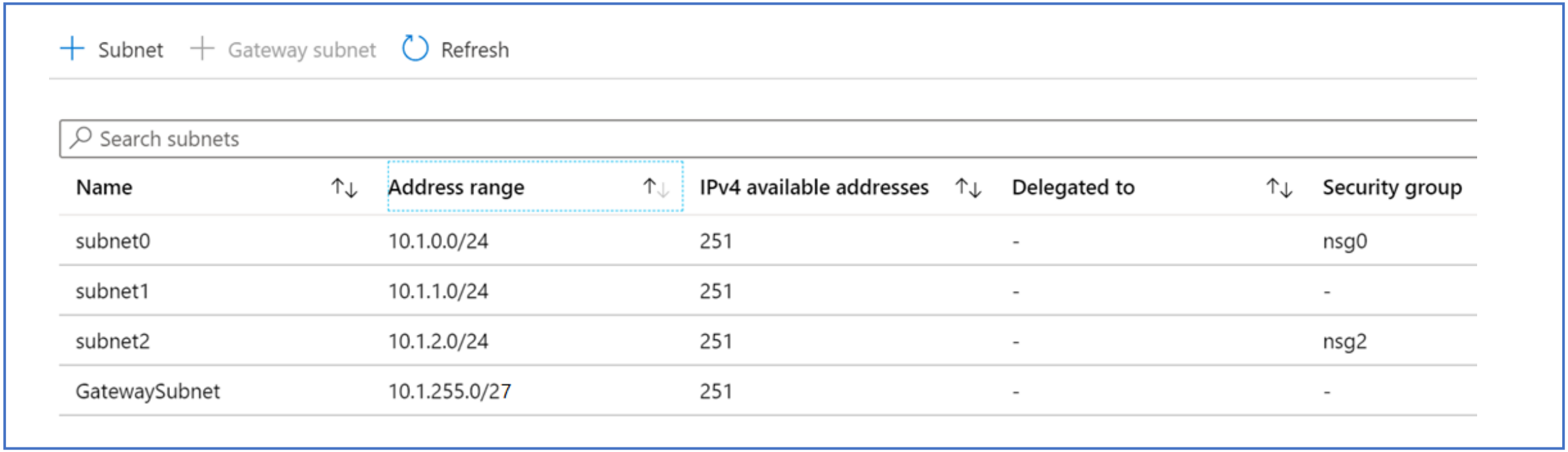
Logical representation of your own network

Create a dedicated private cloud-only virtual network

Securely extend your datacenter with virtual networks

Enable hybrid cloud scenarios

Subnets



A virtual network can be segmented into one or more subnets

Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

Each subnet must have a unique address range – cannot overlap with other subnets in the virtual network in the subscription

CIDR notation

CIDR	Subnet mask (decimal)	Subnet mask (binary)	Available addresses	
/0	0.0.0.0	00000000.00000000.00000000.00000000	4.294.967.296	2^{32}
/1	128.0.0.0	10000000.00000000.00000000.00000000	2.147.483.648	2^{31}
/2	192.0.0.0	11000000.00000000.00000000.00000000	1.073.741.824	2^{30}
/3	224.0.0.0	11100000.00000000.00000000.00000000	536.870.912	2^{29}
/4	240.0.0.0	11110000.00000000.00000000.00000000	268.435.456	2^{28}
/5	248.0.0.0	11111000.00000000.00000000.00000000	134.217.728	2^{27}
/6	252.0.0.0	11111100.00000000.00000000.00000000	67.108.864	2^{26}
/7	254.0.0.0	11111110.00000000.00000000.00000000	33.554.432	2^{25}
/8	255.0.0.0	11111111.00000000.00000000.00000000	16.777.216	2^{24}
/9	255.128.0.0	11111111.10000000.00000000.00000000	8.388.608	2^{23}
/10	255.192.0.0	11111111.11000000.00000000.00000000	4.194.304	2^{22}
/11	255.224.0.0	11111111.11100000.00000000.00000000	2.097.152	2^{21}
/12	255.240.0.0	11111111.11110000.00000000.00000000	1.048.576	2^{20}
/13	255.248.0.0	11111111.11111000.00000000.00000000	524.288	2^{19}
/14	255.252.0.0	11111111.11111100.00000000.00000000	262.144	2^{18}
/15	255.254.0.0	11111111.11111110.00000000.00000000	131.072	2^{17}
/16	255.255.0.0	11111111.11111111.00000000.00000000	65.536	2^{16}
/17	255.255.128.0	11111111.11111111.10000000.00000000	32.768	2^{15}
/18	255.255.192.0	11111111.11111111.11000000.00000000	16.384	2^{14}
/19	255.255.224.0	11111111.11111111.11100000.00000000	8.192	2^{13}
/20	255.255.240.0	11111111.11111111.11110000.00000000	4.096	2^{12}
/21	255.255.248.0	11111111.11111111.11111000.00000000	2.048	2^{11}
/22	255.255.252.0	11111111.11111111.11111100.00000000	1.024	2^{10}
/23	255.255.254.0	11111111.11111111.11111110.00000000	512	2^{9}
/24	255.255.255.0	11111111.11111111.11111111.00000000	256	2^{8}
/25	255.255.255.128	11111111.11111111.11111111.10000000	128	2^{7}
/26	255.255.255.192	11111111.11111111.11111111.11000000	64	2^{6}
/27	255.255.255.224	11111111.11111111.11111111.11100000	32	2^{5}
/28	255.255.255.240	11111111.11111111.11111111.11110000	16	2^{4}
/29	255.255.255.248	11111111.11111111.11111111.11111000	8	2^{3}
/30	255.255.255.252	11111111.11111111.11111111.11111100	4	2^{2}
/31	255.255.255.254	11111111.11111111.11111111.11111110	2	2^{1}
/32	255.255.255.255	11111111.11111111.11111111.11111111	1	2^{0}

Example:

IP Adress: 10.168.178.x

Subnet mask: 255.255.255.0 ≙ 11111111 11111111 11111111 00000000 (binary), 24 bits are fix -> definition of the subnet; 8 bits are variable -> definition of possible IP addresses)

Possible IP range for this network: 10.168.178.0 – 10.168.178.255 (256 IP addresses)

CIDR notation: 10.168.178.0/24

More examples:
10.168.178.0/25 -> 10.168.178.0 – 10.168.178.127 (128 IP addresses)
10.168.178.128/25 -> 10.168.178.128 – 10.178.168.256 (128 IP addresses)
10.168.178.0/26 -> 10.168.178.0 – 10.168.178.63 (64 IP addresses)
10.168.0.0/16 -> 10.168.0.0 – 10.168.255.255 (65.536 IP addresses)
10.0.0.0/8 -> 10.0.0.0 – 10.255.255.255 (16.777.216 IP addresses)
….

Understand Regions and Subscriptions

Regions: VNet is scoped to a single region/location; however, multiple virtual networks from different regions can be connected using Virtual Network Peering.

Public IP Addresses

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	Yes*
Application Gateway	Front-end configuration	Yes	Yes*
Azure Firewall	Front-end configuration	Yes (V1 only)	Yes (V2 only)
NAT gateway	Gateway IP configuration	No	Yes

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

*Static IP addresses only available on certain SKUs.

Lesson: Enable Cross-VNet Connectivity with Peering

VNet Peering

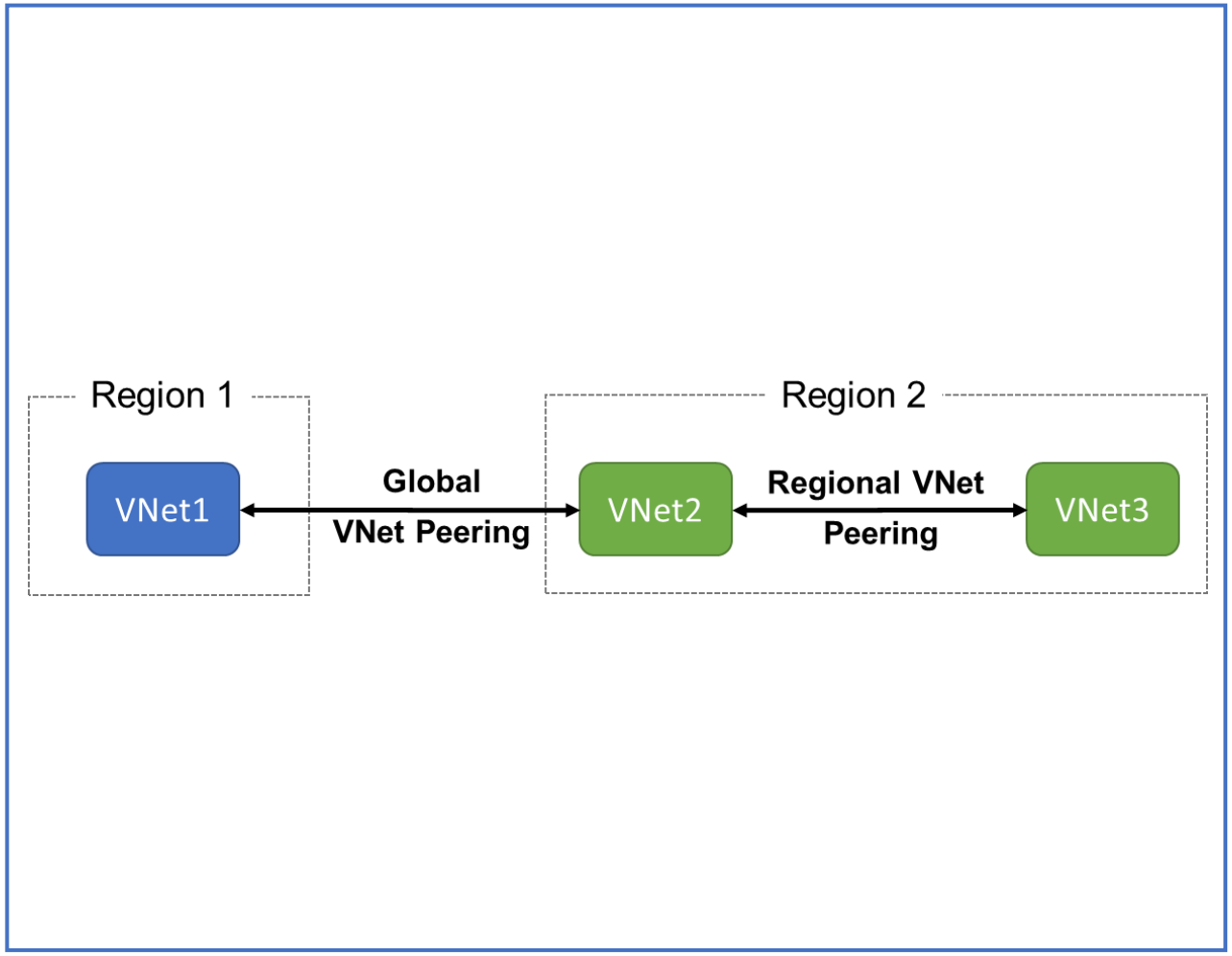
VNet peering connects two Azure virtual networks

Two types of peering: Regional and Global

Peered networks use the Azure backbone for privacy and isolation

You can peer across subscriptions and tenants

VNet peering is not transitive

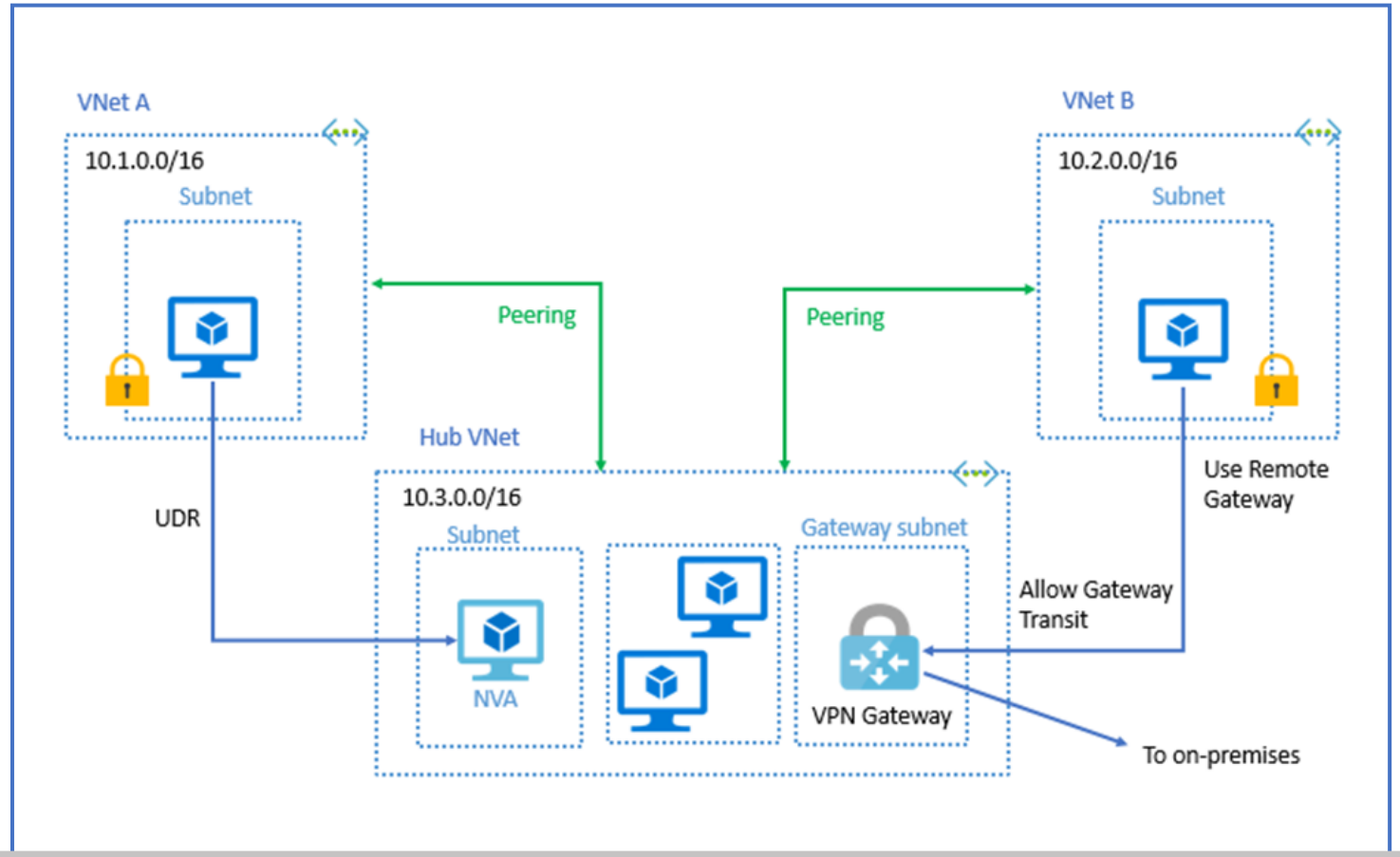


Implementing VNet Peering

Gateway transit allows peered virtual networks to share the gateway and get access to resources

No VPN gateway is required in the peered virtual network

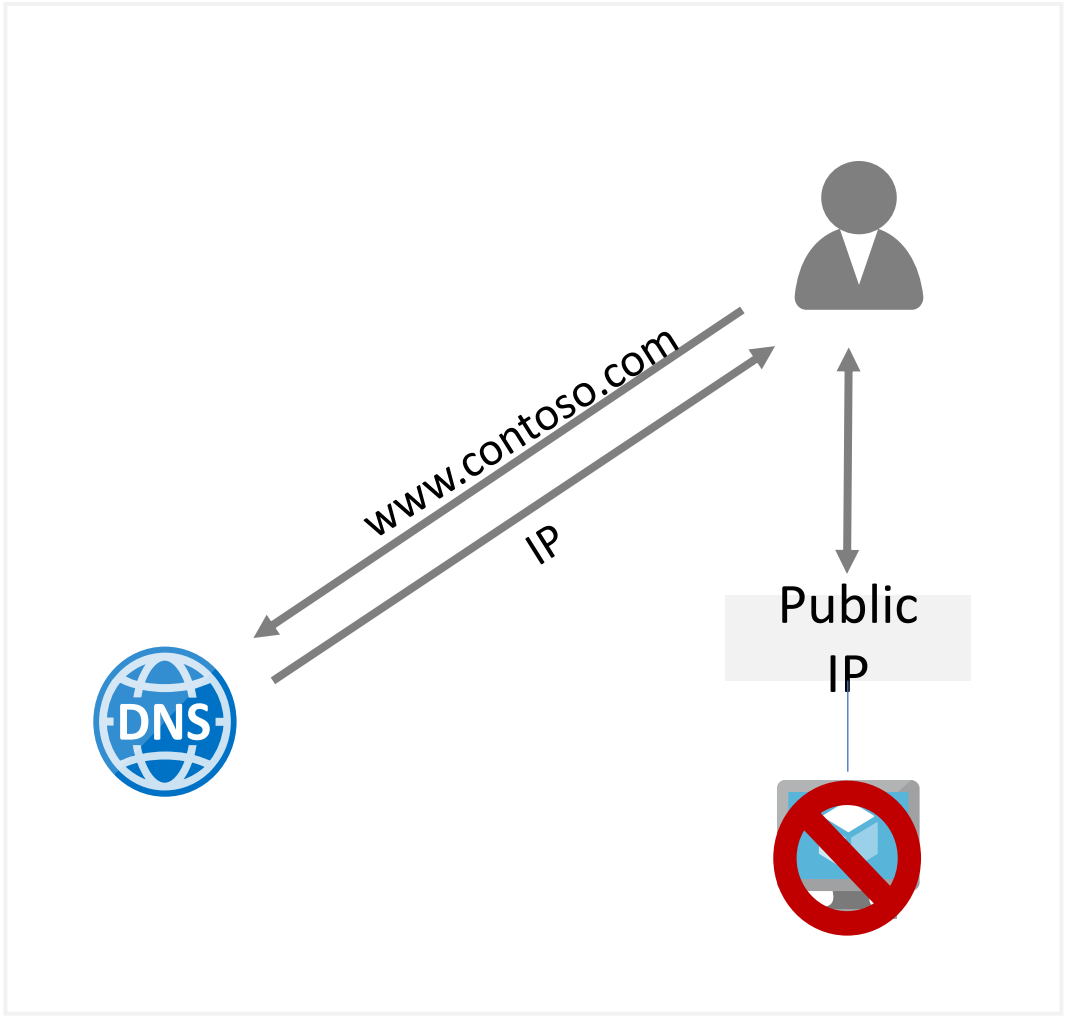
Default VNet peering provides full connectivity

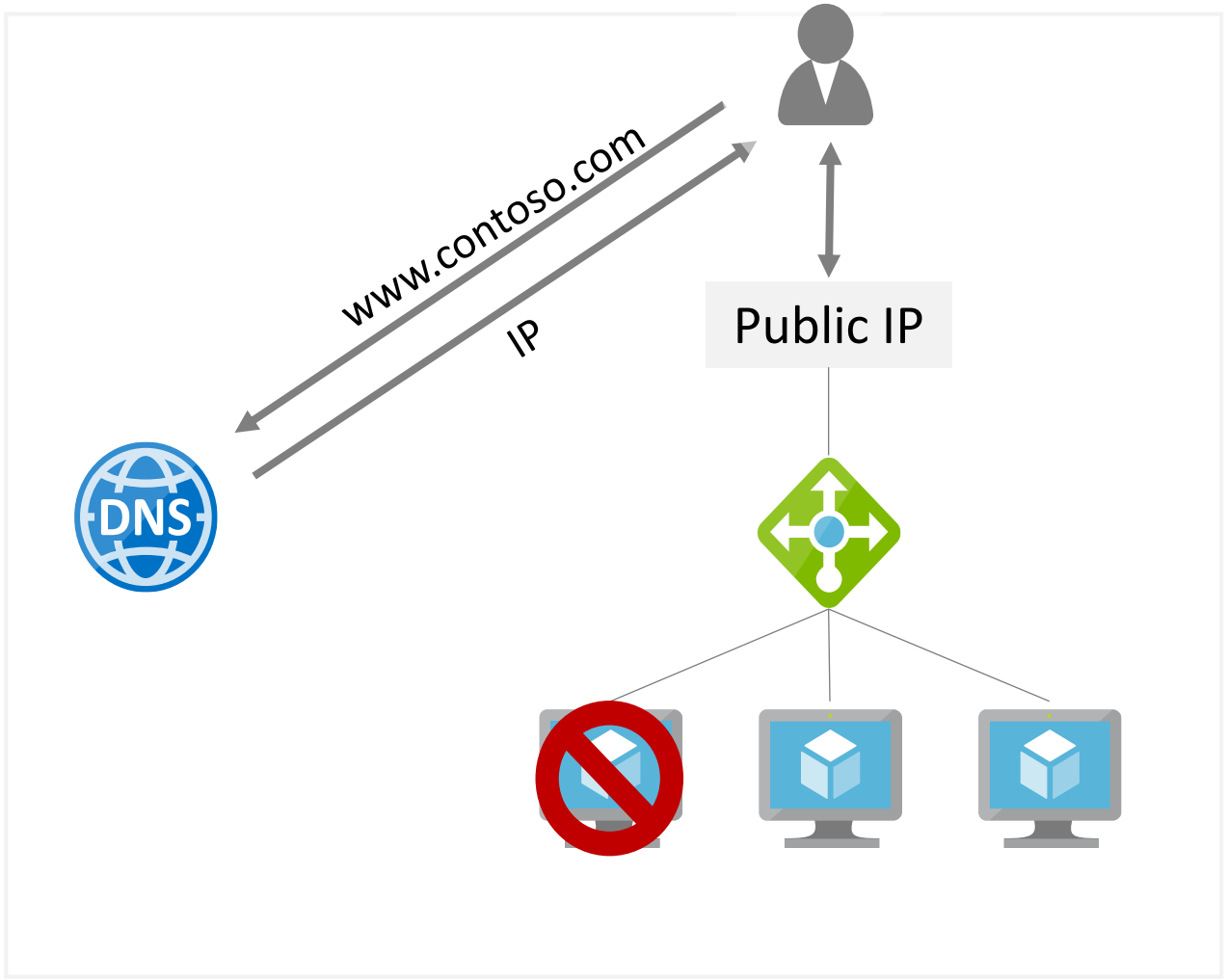


✓ IP address spaces of connected networks can't overlap

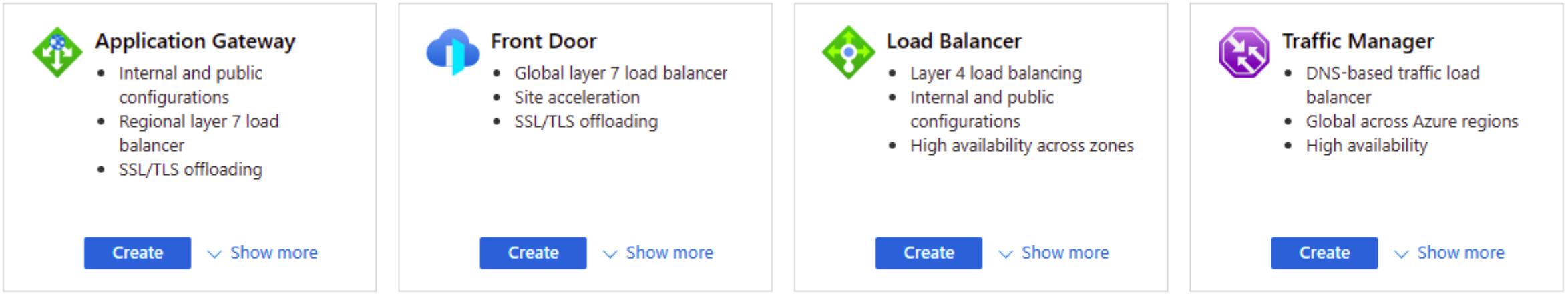
Lesson: Load balancing options in the Azure portal

What is a Load balancer



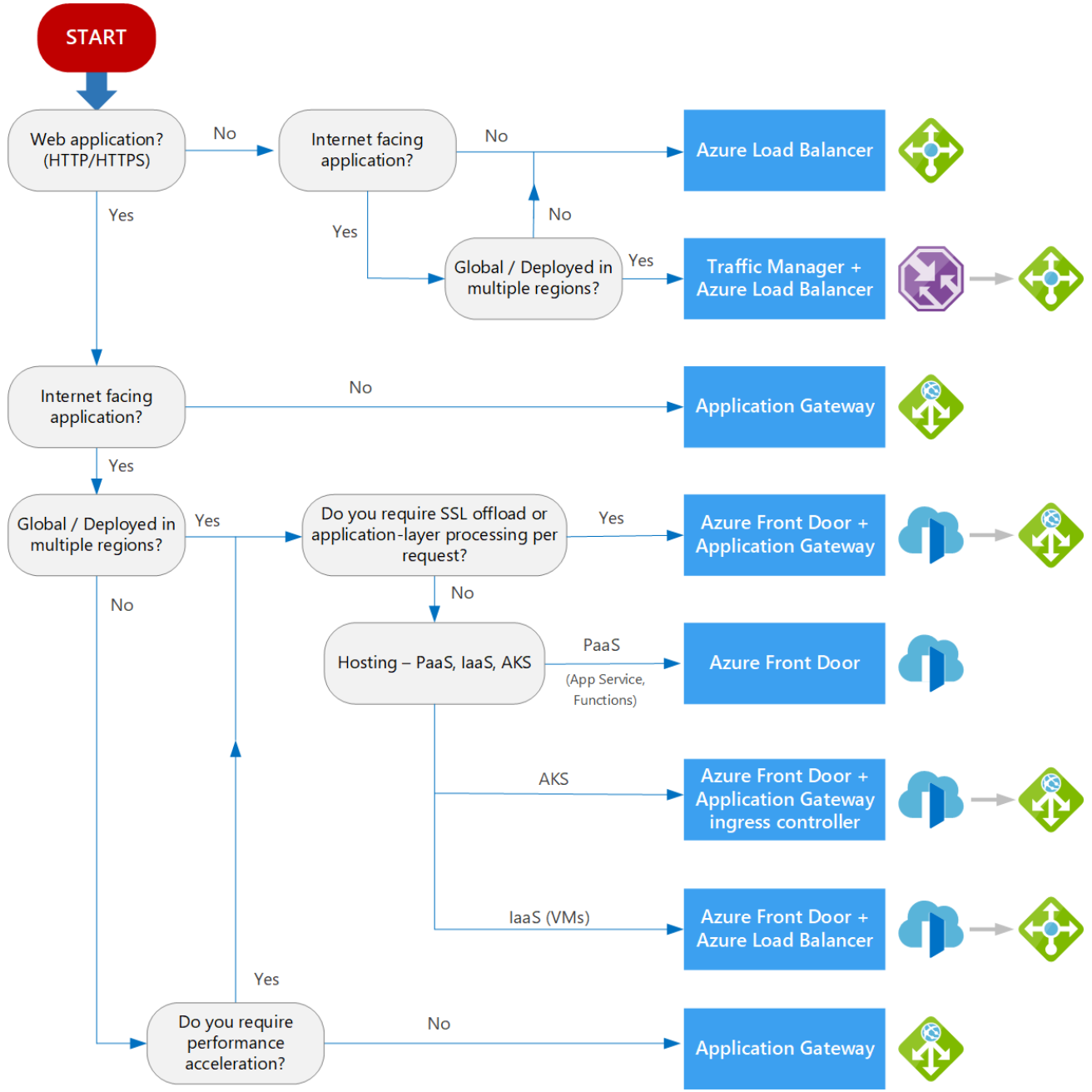


Load balancing options for Azure



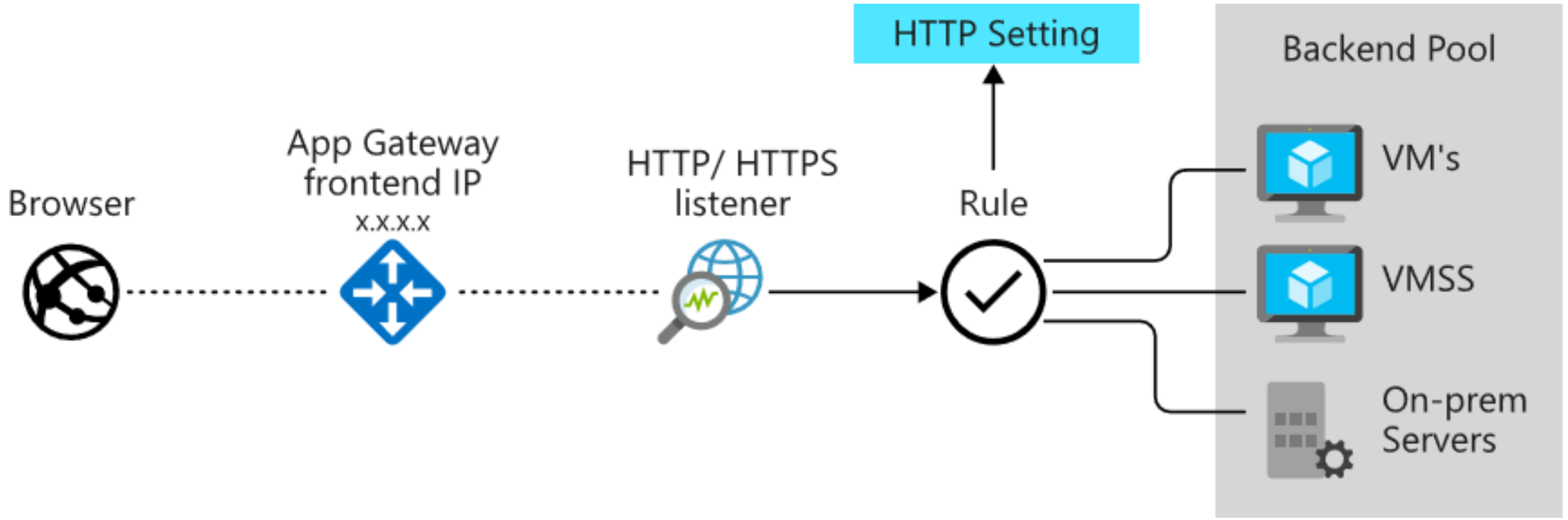
Choosing a load balancing option

- Type of traffic
- Scope
- Availability
- Cost
- Features and limitations



Lesson: Azure Application Gateway

Application Gateway features



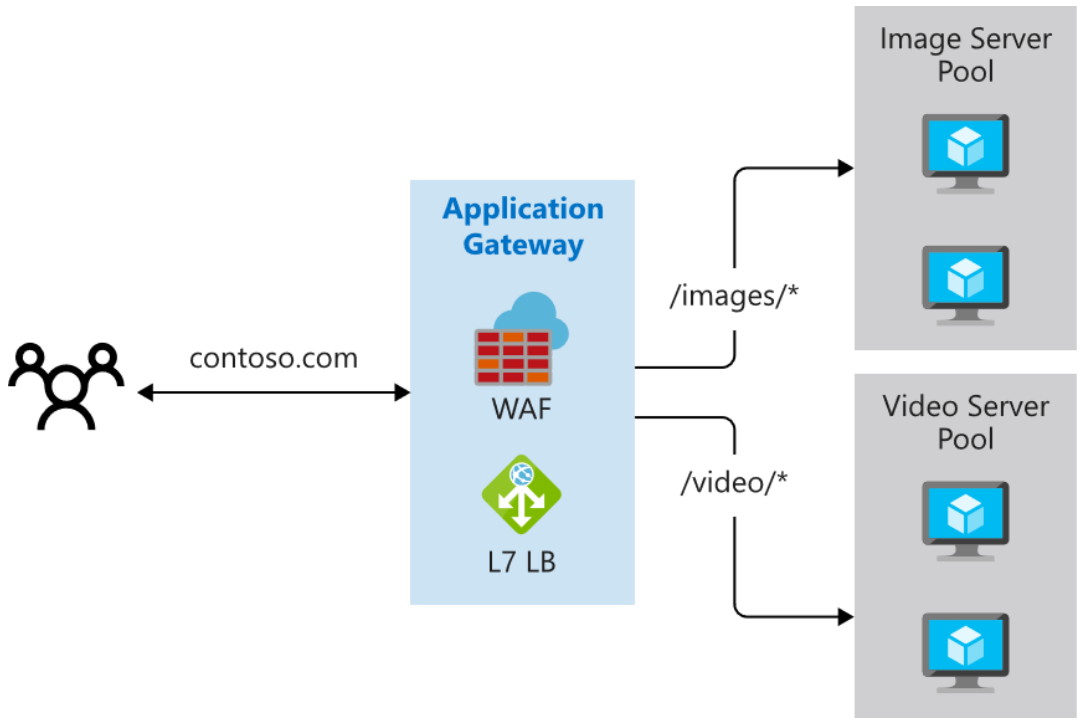
Manages web app requests

Routes traffic to a pool of web servers based on the URL of a request

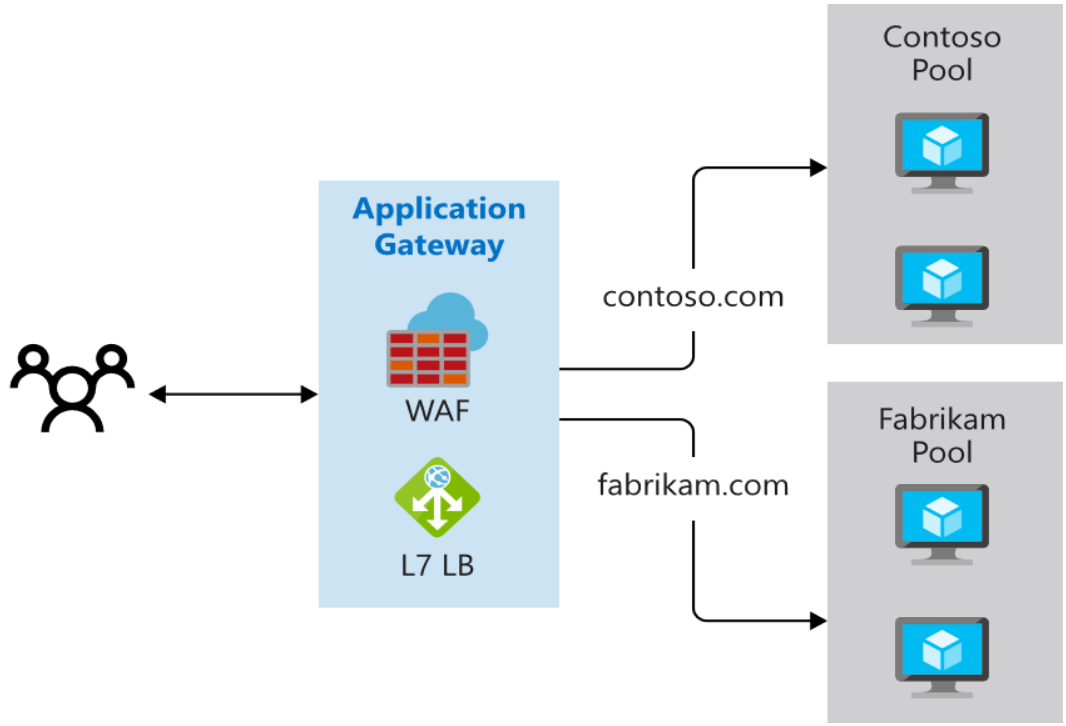
The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

Determine Application Gateway Routing

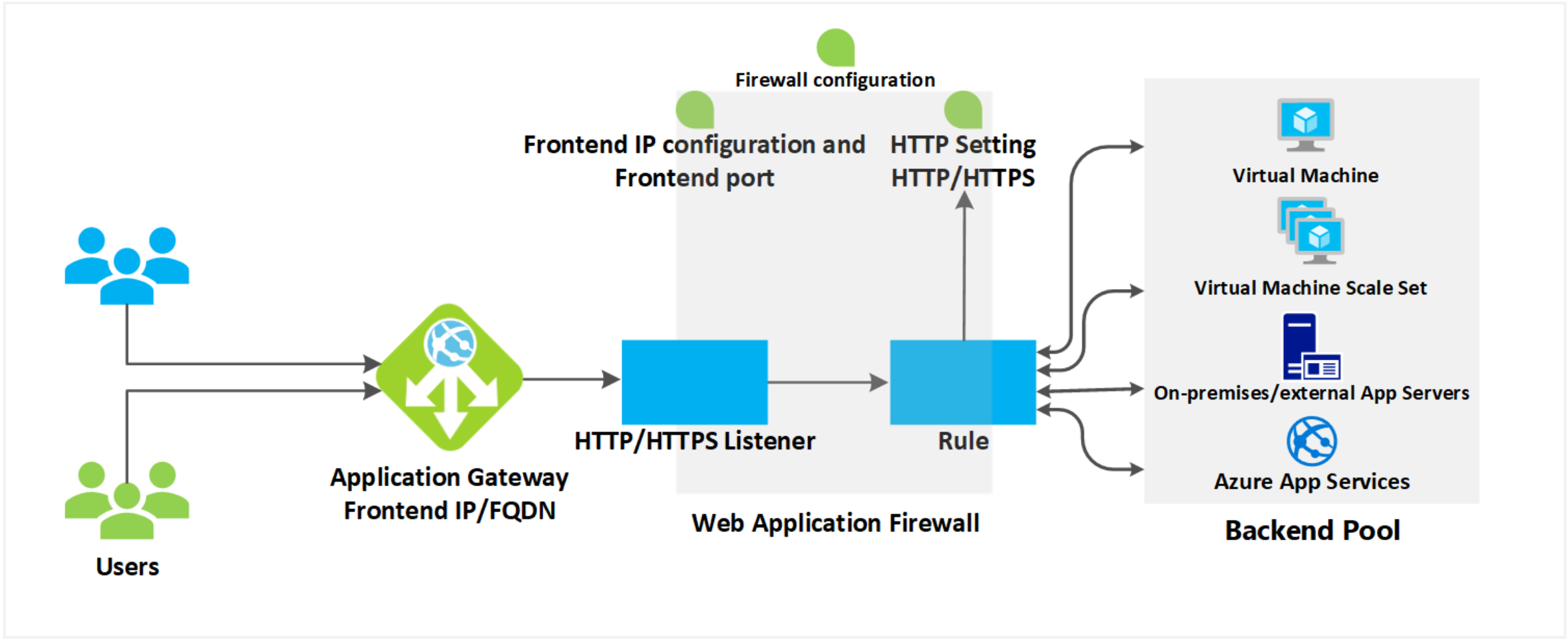
Path-based routing



Multiple-site routing



Application Gateway configuration planning



Lesson: Azure ExpressRoute

ExpressRoute Capabilities

Layer 3 connectivity with redundancy

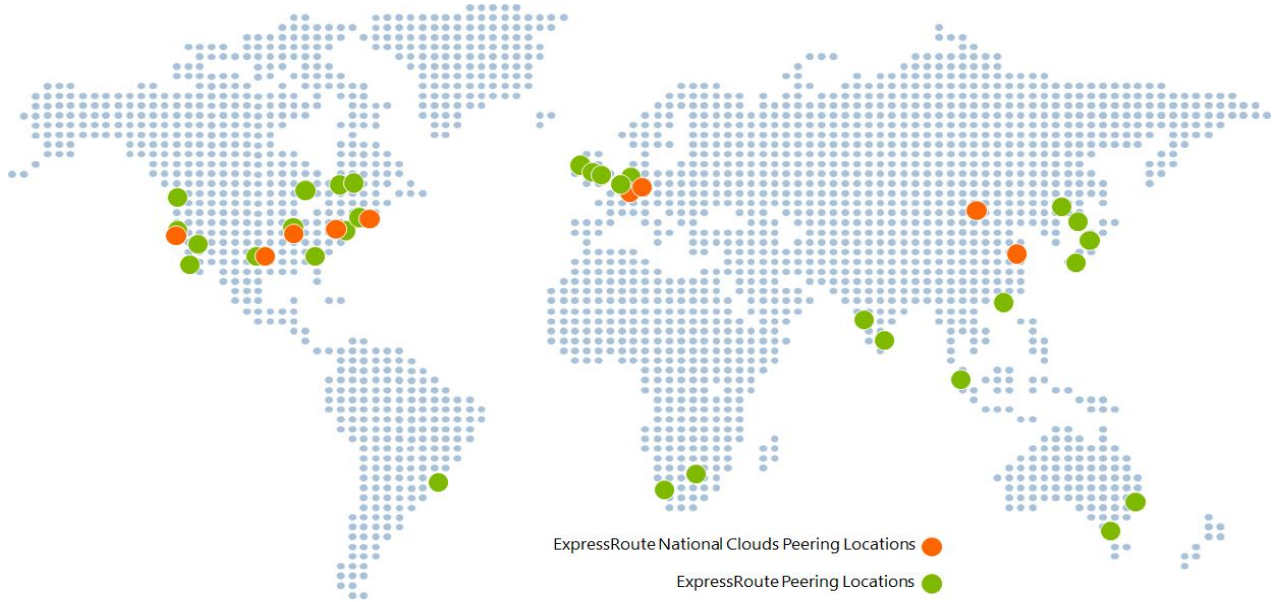
Connectivity to all regions within a geography

Global connectivity with ExpressRoute premium add-on

Across on-premises connectivity with ExpressRoute Global Reach

Bandwidth options – 50 Mbps to 100 Gbps

Billing models – Unlimited, metered, premium



Choose a peering location

Choose the right ExpressRoute Circuit and billing model

Choose Metered or unlimited data plan

Choose Bandwidth

You can increase gateway size but not decrease without service outage

Pricing varies by region and zone

Unlimited data. Billing is based on a monthly fee; all inbound and outbound data transfer is included free of charge.

Metered data. Billing is based on a monthly fee; all inbound data transfer is free of charge. Outbound data transfer is charged per GB of data transfer. Data transfer rates vary by region.

ExpressRoute premium add-on. ExpressRoute premium is an add-on to the ExpressRoute circuit.

Understand use cases for Azure ExpressRoute

Faster and Reliable connection to Azure services

Built in redundant circuits

Storage, backup, and Recovery

Border Gateway Protocol (BGP)

Extends Data center capabilities

Integrates with existing Multiprotocol Label Switching (MPLS)

Predictable, reliable, and high-throughput connections

SLA

Private connection to Microsoft cloud

Design considerations for ExpressRoute deployments

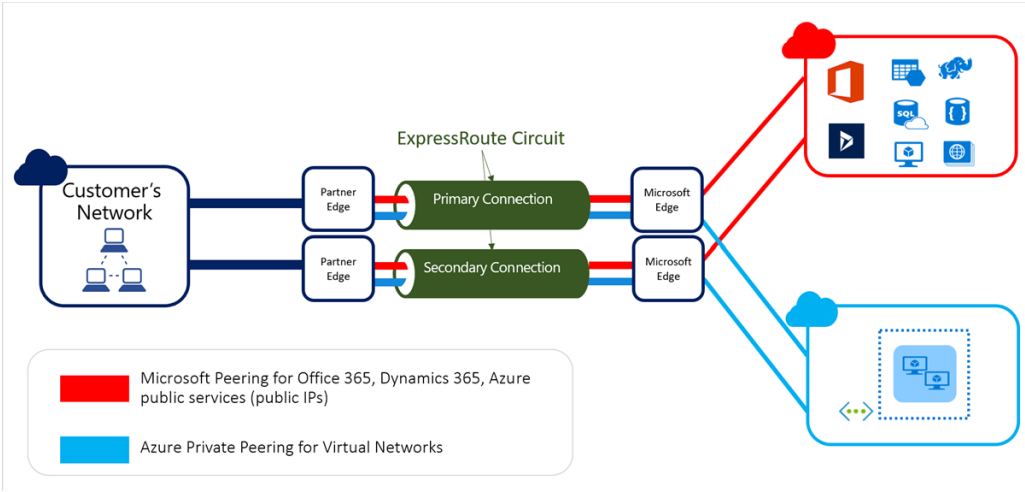
ExpressRoute using a Service Provider	ExpressRoute Direct
Uses service providers to enable fast onboarding and connectivity into existing infrastructure	Requires 100 Gbps/10 Gbps infrastructure and full management of all layers
Integrates with hundreds of providers including Ethernet and MPLS	Direct/Dedicated capacity for regulated industries and massive data ingestion
Circuits SKUs from 50 Mbps to 10 Gbps	Customer may select a combination of the following circuit SKUs on 100-Gbps ExpressRoute Direct: (5 Gbps, 10 Gbps, 40 Gbps, 100 Gbps) Customer may select a combination of the following circuit SKUs on 10-Gbps ExpressRoute Direct: (1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps)
Optimized for single tenant	Optimized for single tenant with multiple business units and multiple work environments

Design considerations for ExpressRoute deployments – continued

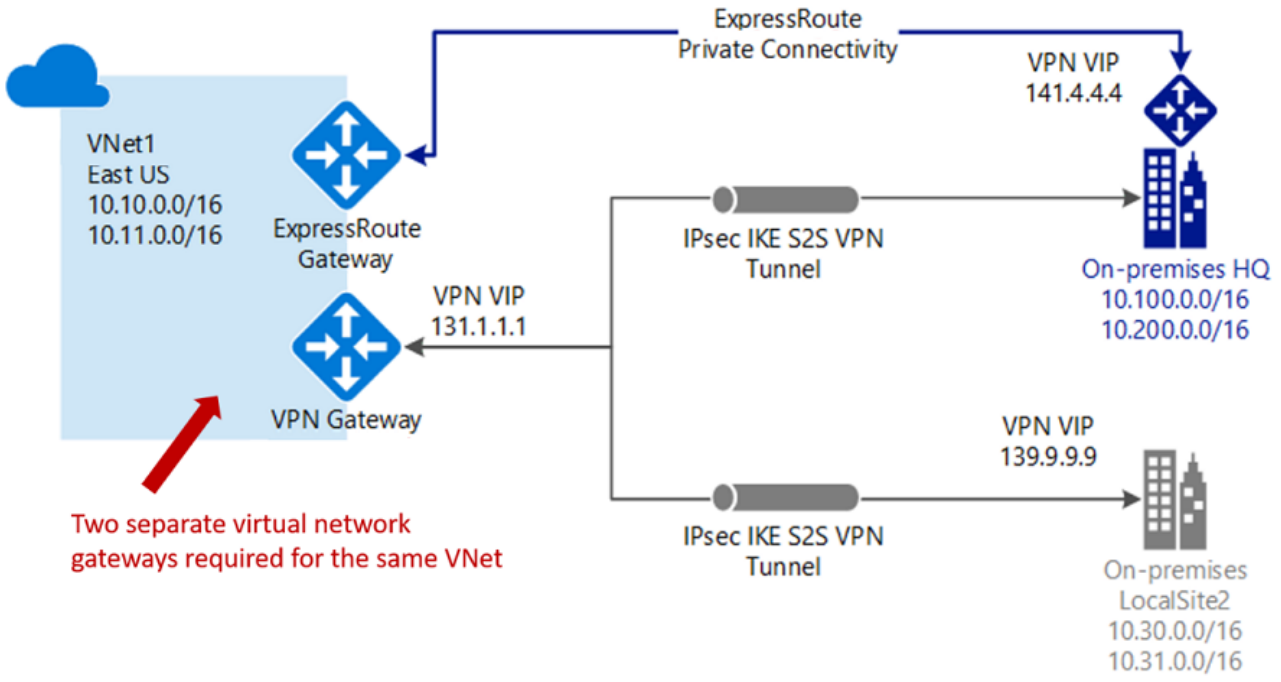
Recommend a route advertisement configuration

BGP community values associated with services accessible through Microsoft peering is available in the ExpressRoute routing requirements page.

Make a list of BGP community values you want to use in the route filter



Coexisting Site-to-Site and ExpressRoute



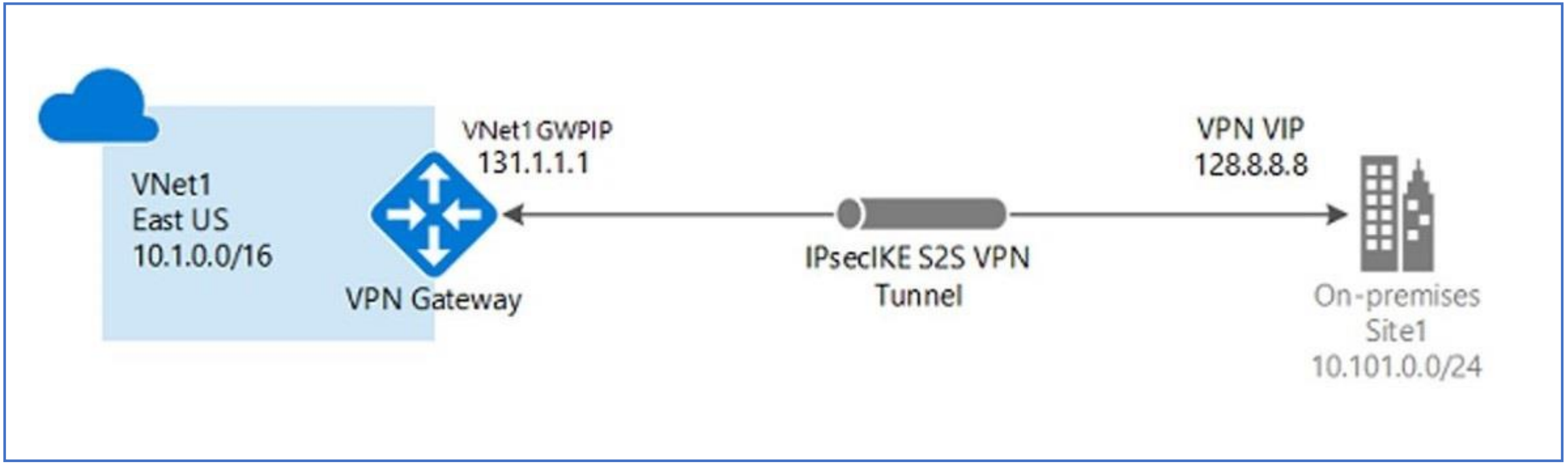
Use S2S VPN as a secure failover path for ExpressRoute

Use S2S VPNs to connect to sites that are not connected with ExpressRoute

Notice two VNet gateways for the same virtual network

Lesson: Design an Azure VPN gateway

Plan a VPN Gateway



Site-to-site connections **connect on-premises datacenters to Azure virtual networks**

VNet-to-VNet **connections connect Azure virtual networks (custom)**

Point-to-site (User VPN) connections **connect individual devices to Azure virtual networks**

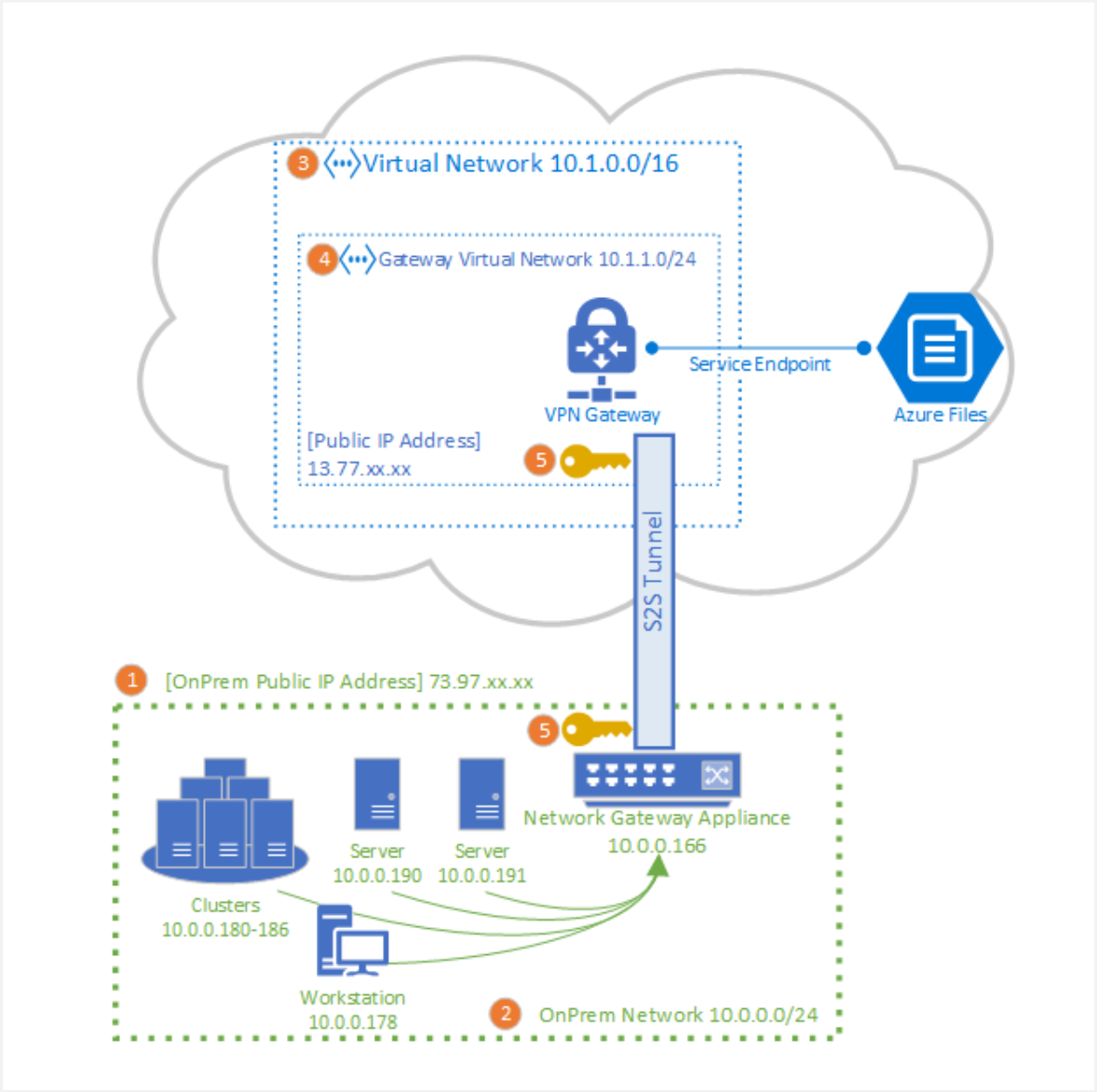
Configure the On-premises VPN Device

Remember the shared key for the Azure connection (next step)

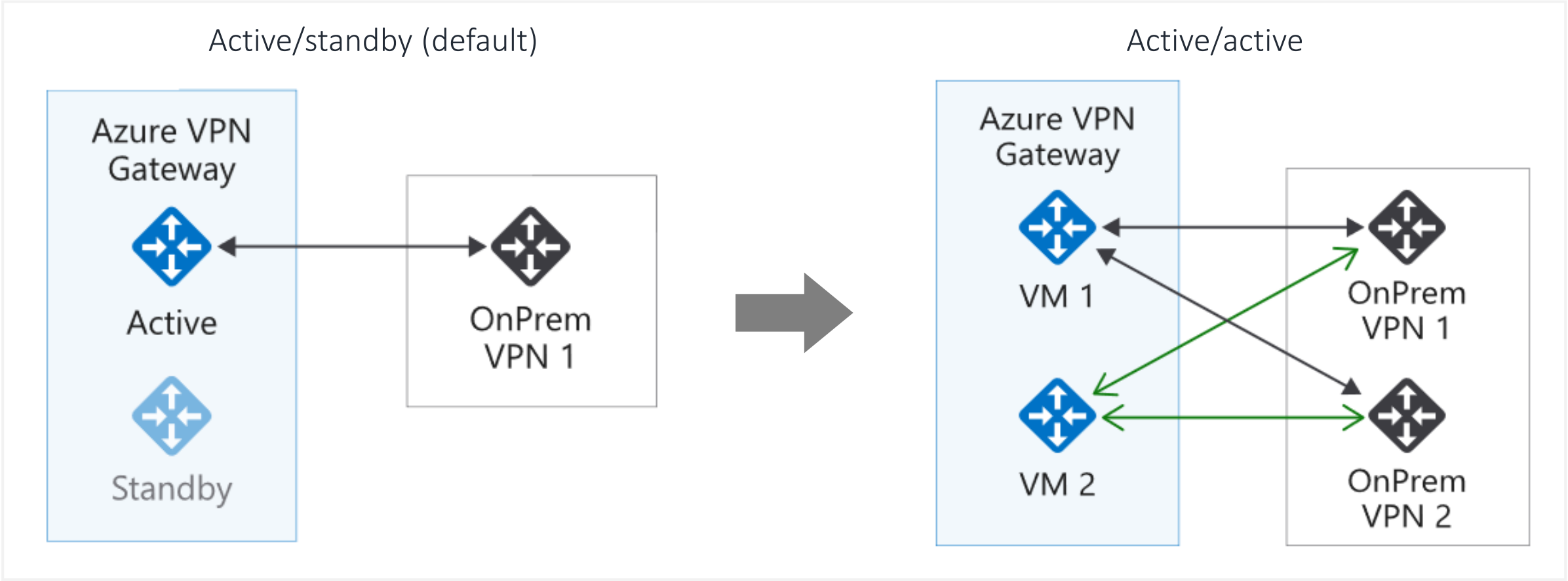
Consult the list of supported VPN devices (Cisco, Juniper, Ubiquiti, Barracuda Networks)

Specify the public IP address (previous step)

A VPN device configuration script may be available



High availability options for VPN connections



VPN gateways are deployed as two instances

Enable active/active mode for higher availability

End of presentation