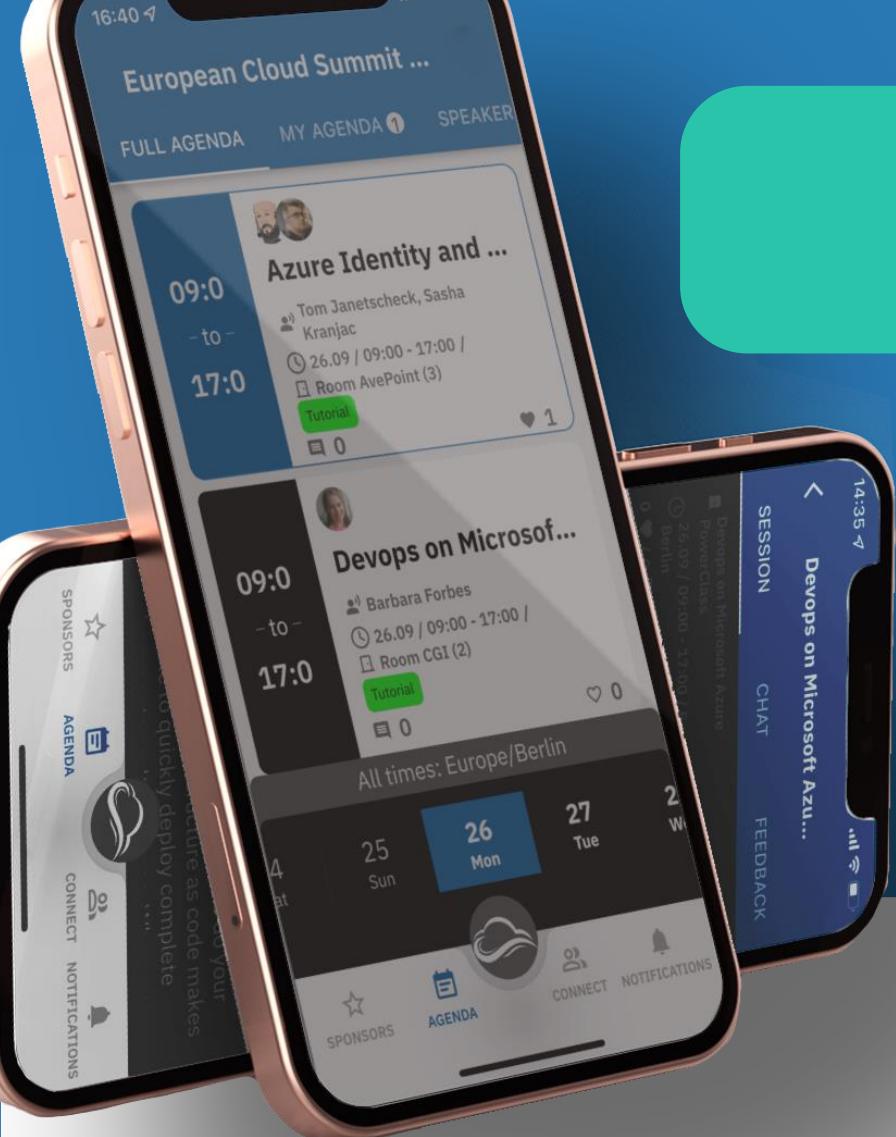


16:40 4G



European Cloud Summit ...
FULL AGENDA MY AGENDA 1 SPEAKER
Azure Identity and ...
09:0 - to - 17:0
Tom Janetscheck, Sasha Kranjac
26.09 / 09:00 - 17:00 / Room AvePoint (3)
Tutorial 1
Devops on Microsoft...
09:0 - to - 17:0
Barbara Forbes
26.09 / 09:00 - 17:00 / Room CGI (2)
Tutorial 0
All times: Europe/Berlin
25 Sun 26 Mon 27 Tue 28 Wed
SPONSORS AGENDA CONNECT NOTIFICATIONS
SPEAKERS AND SESSIONS
SESSION FEEDBACK BUSINESS NETWORKING AGENDA SPEAKERS AND SESSIONS
Did you know? You can use the app to scan other attendees' badges, and they will become your connections!
<https://csmmt.eu/app>

USE CLOUDSUMMIT APP!

SESSION FEEDBACK BUSINESS NETWORKING AGENDA SPEAKERS AND SESSIONS

DID YOU KNOW?

YOU CAN USE THE APP TO SCAN OTHER ATTENDEES' BADGES, AND THEY WILL BECOME YOUR CONNECTIONS!


<https://csmmt.eu/app>

- AZURE NETWORKING vNEXT - How to Build Modern Connectivity for IaaS, PaaS and SaaS

Eric Berg

Microsoft MVP – Azure & Cloud and Datacenter Management
Enterprise Cloud Architect @ CGI



EUROPEAN CLOUD SUMMIT

MAINZ, GERMANY 26 – 28 SEPTEMBER 2022



♥ DIAMOND AND PLATINUM SPONSORS ♥



Admin By Request
By FastTrack Software



AvePoint®



WEBCON®
LOW-CODE, BUT BETTER.



wasabi
hot cloud storage



nintex



Eric Berg



Vice President Expert @ CGI



Cloud, Datacenter and Management



Azure, AWS, GCP



info@ericberg.de



@ericberg_de | @GeekZeugs



www.ericberg.de | www.geekzeugs.de



MOUNTAIN IT
www.ericberg.de



Agenda

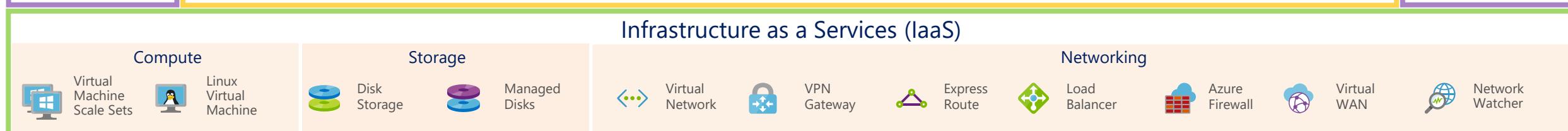
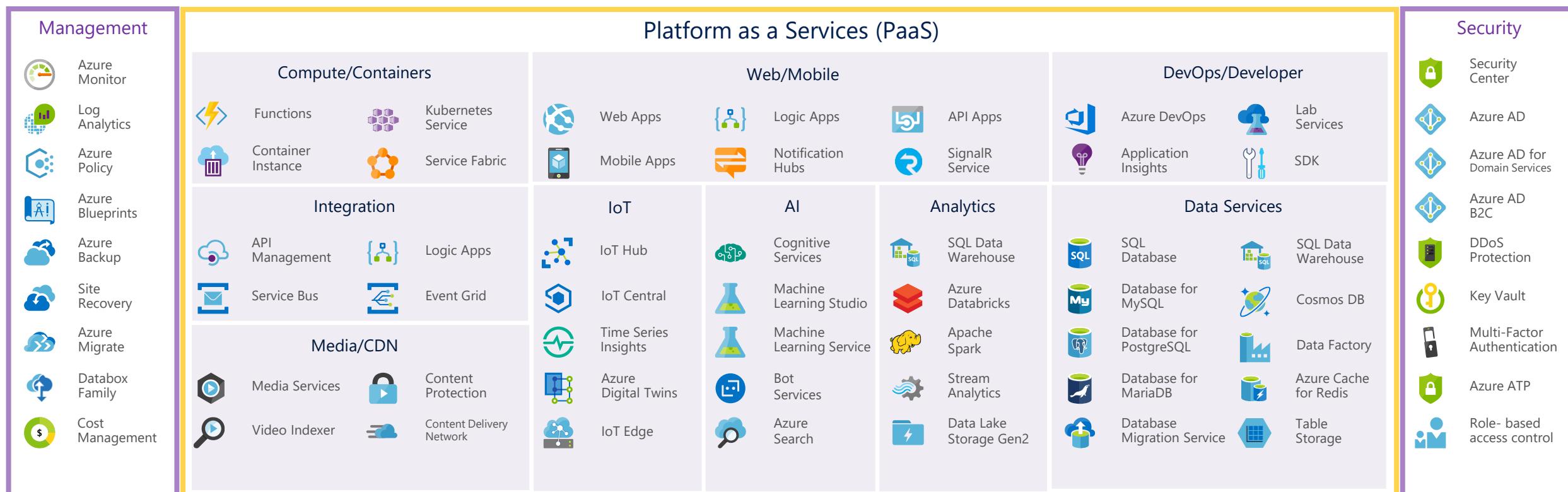


- Networking Overview
- Networking Recap
- Connectivity
- Integration
- DNS
- Build it
- Q&A



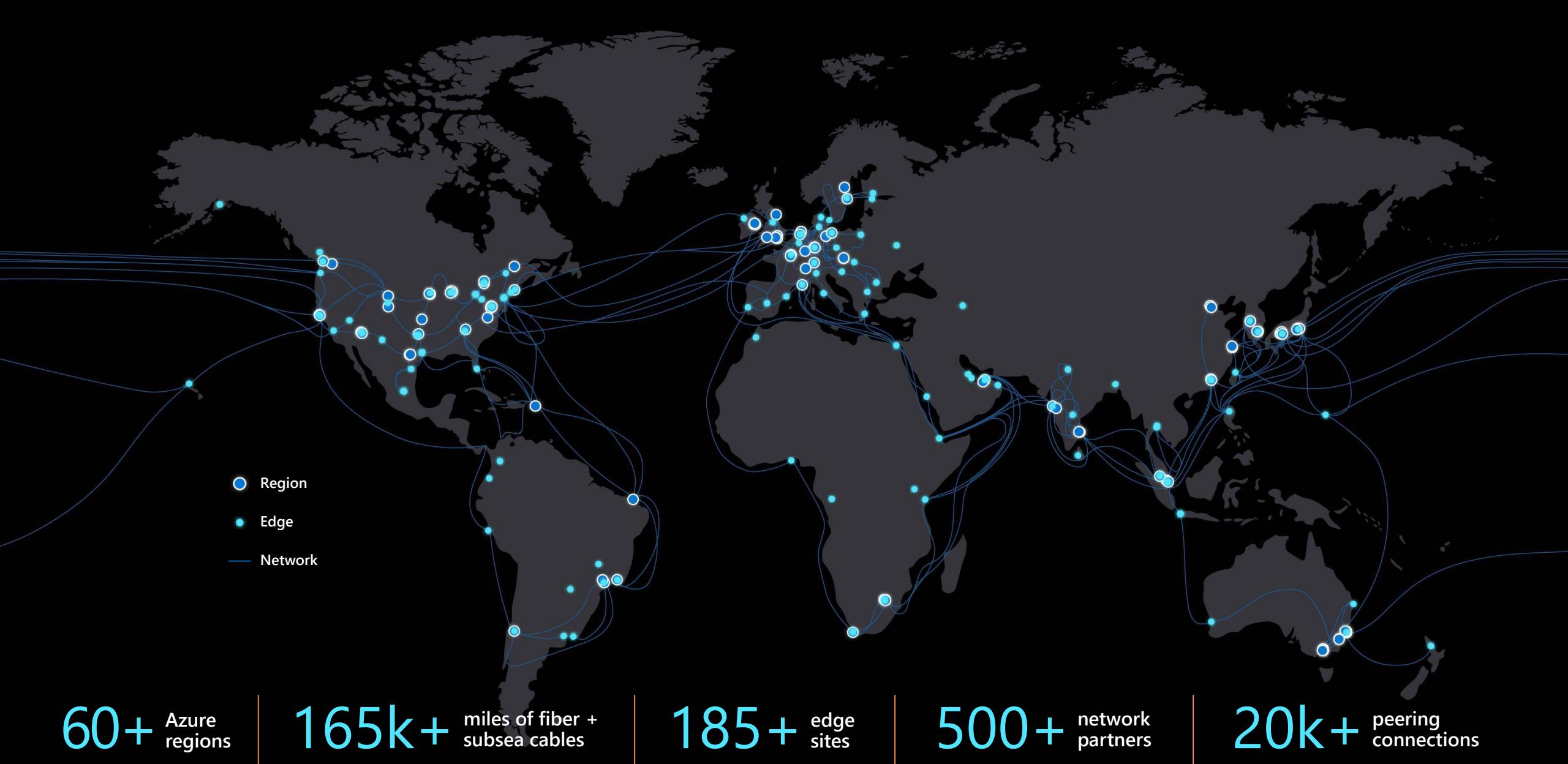
Networking Overview

High Level Azure Services

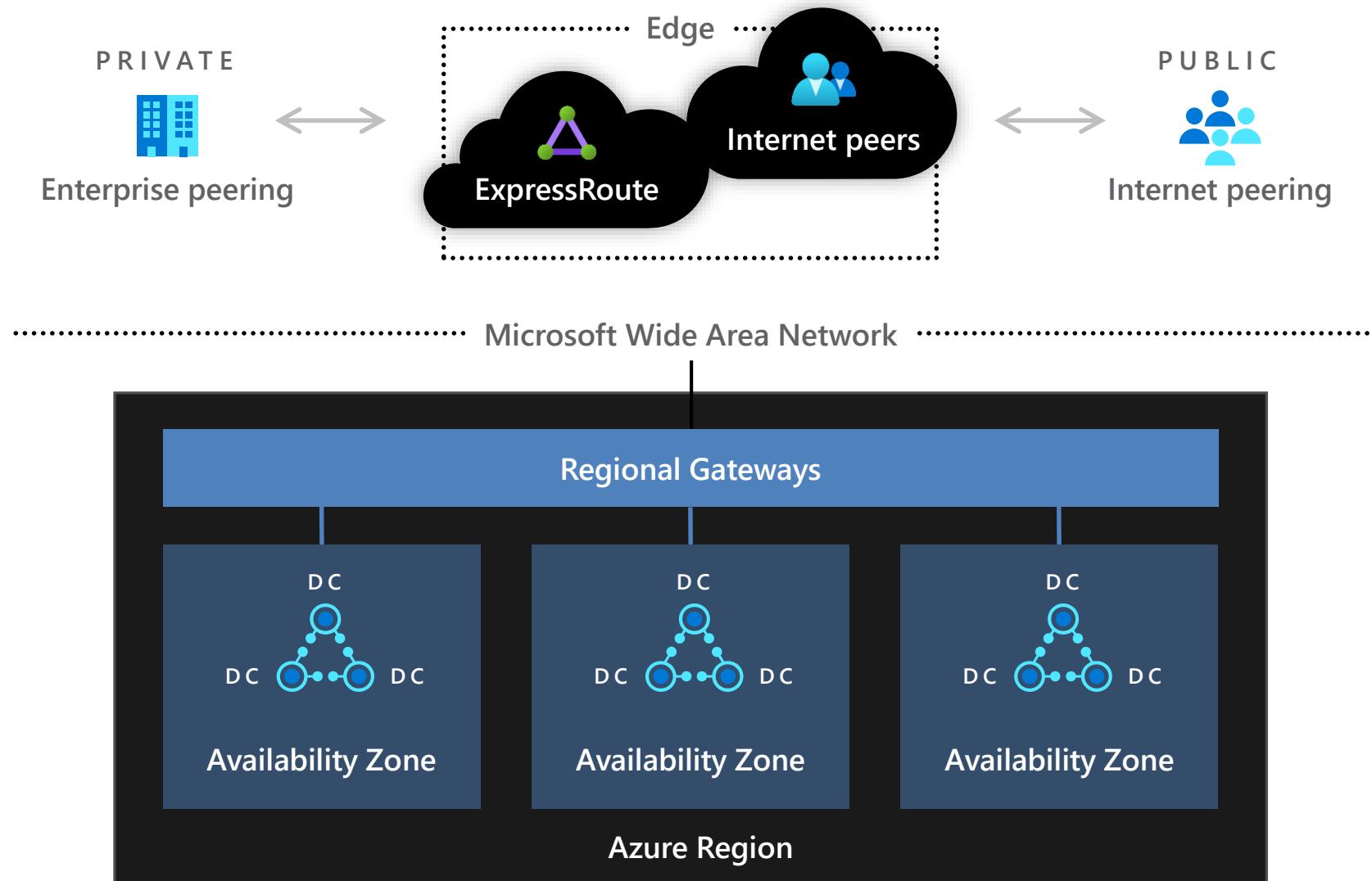


Azure Datacenter Infrastructure

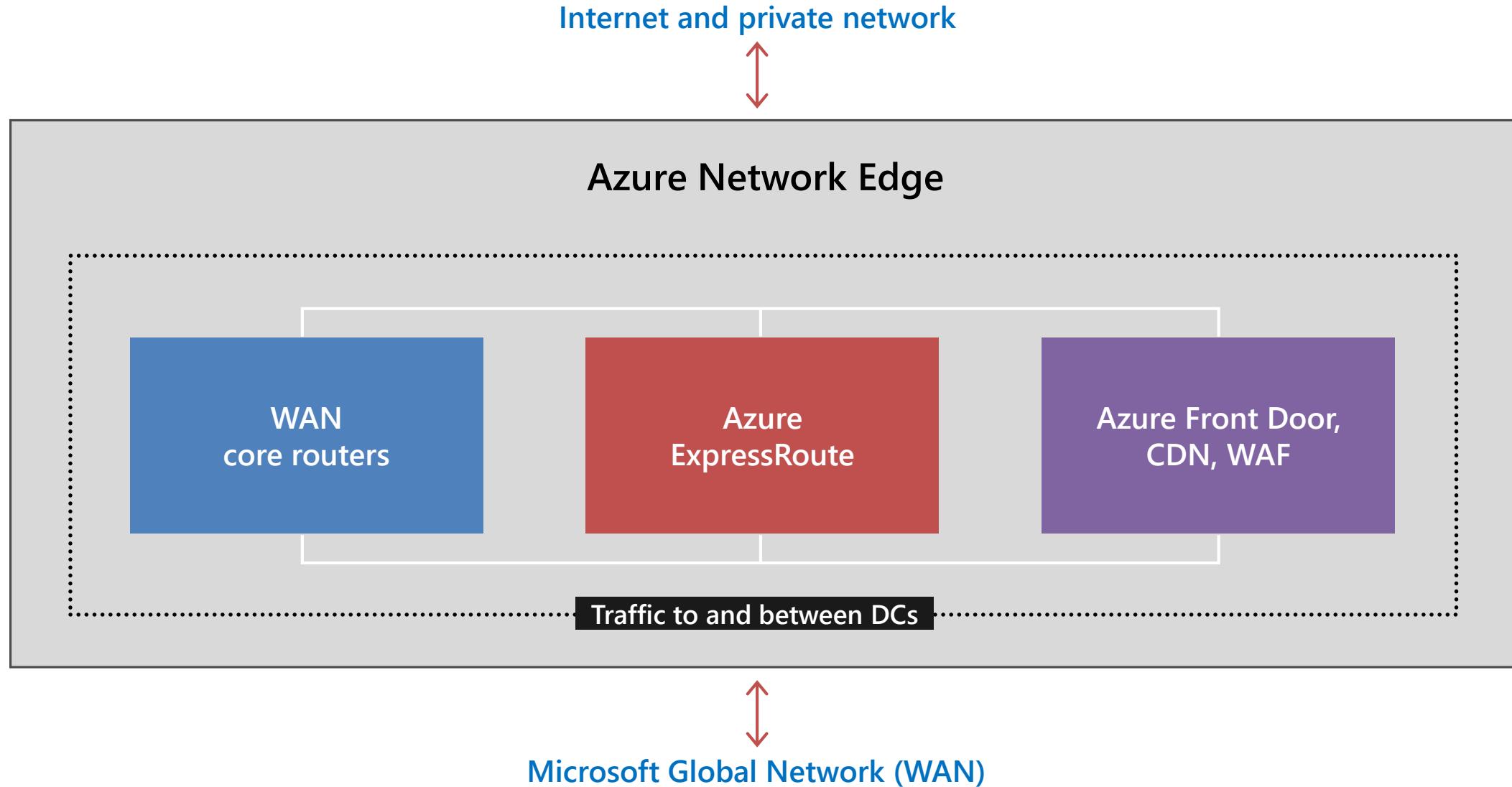




Connecting Azure regions to the global network



The Azure Network Edge

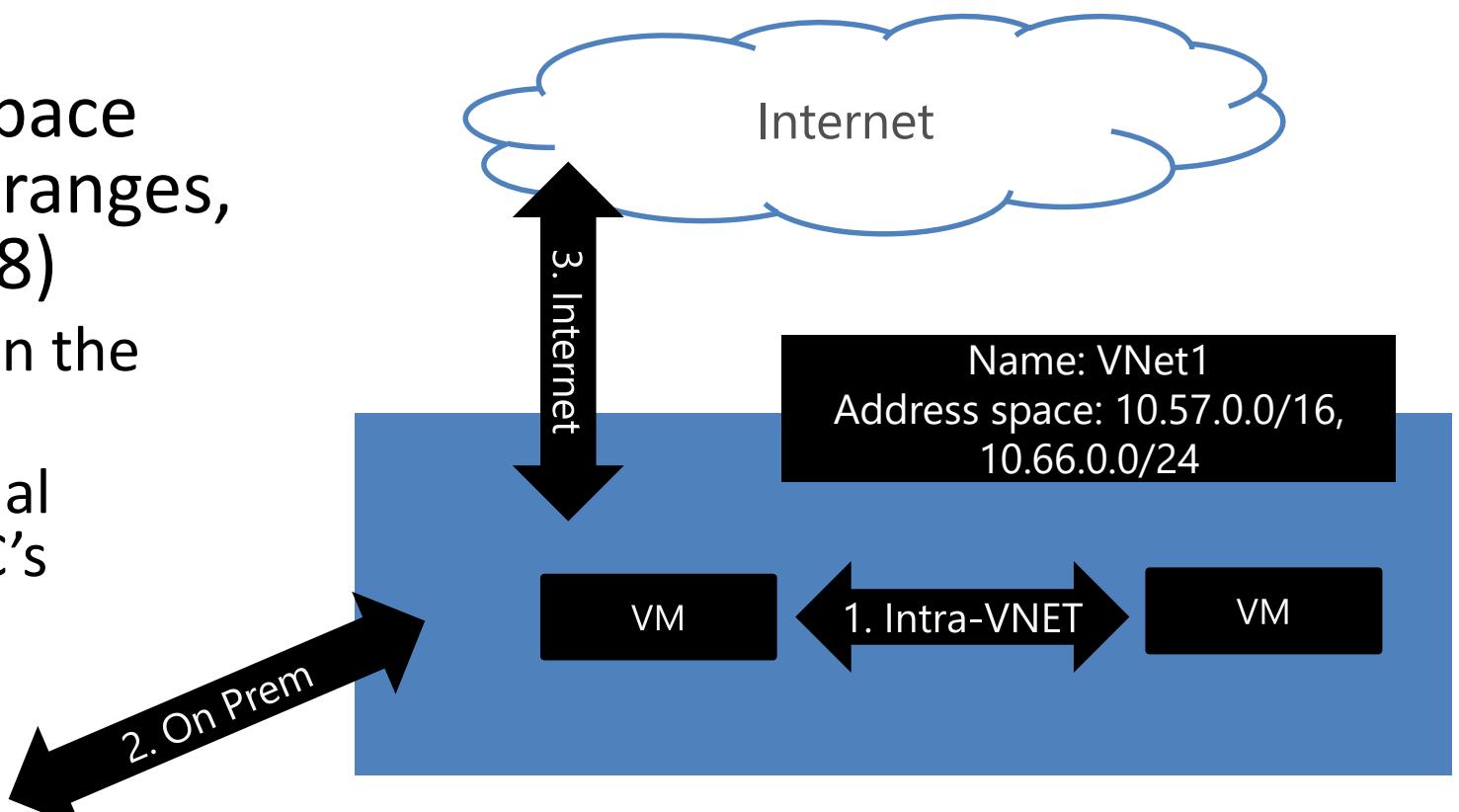
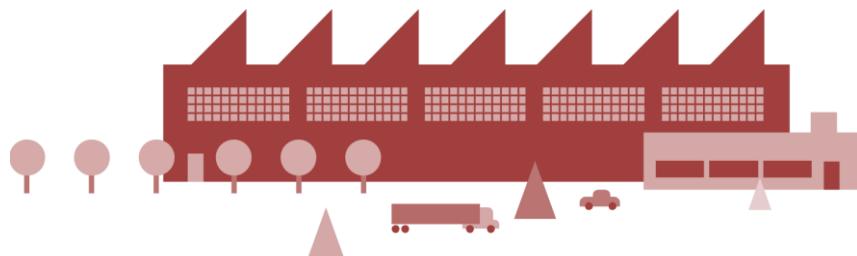




Networking Recap

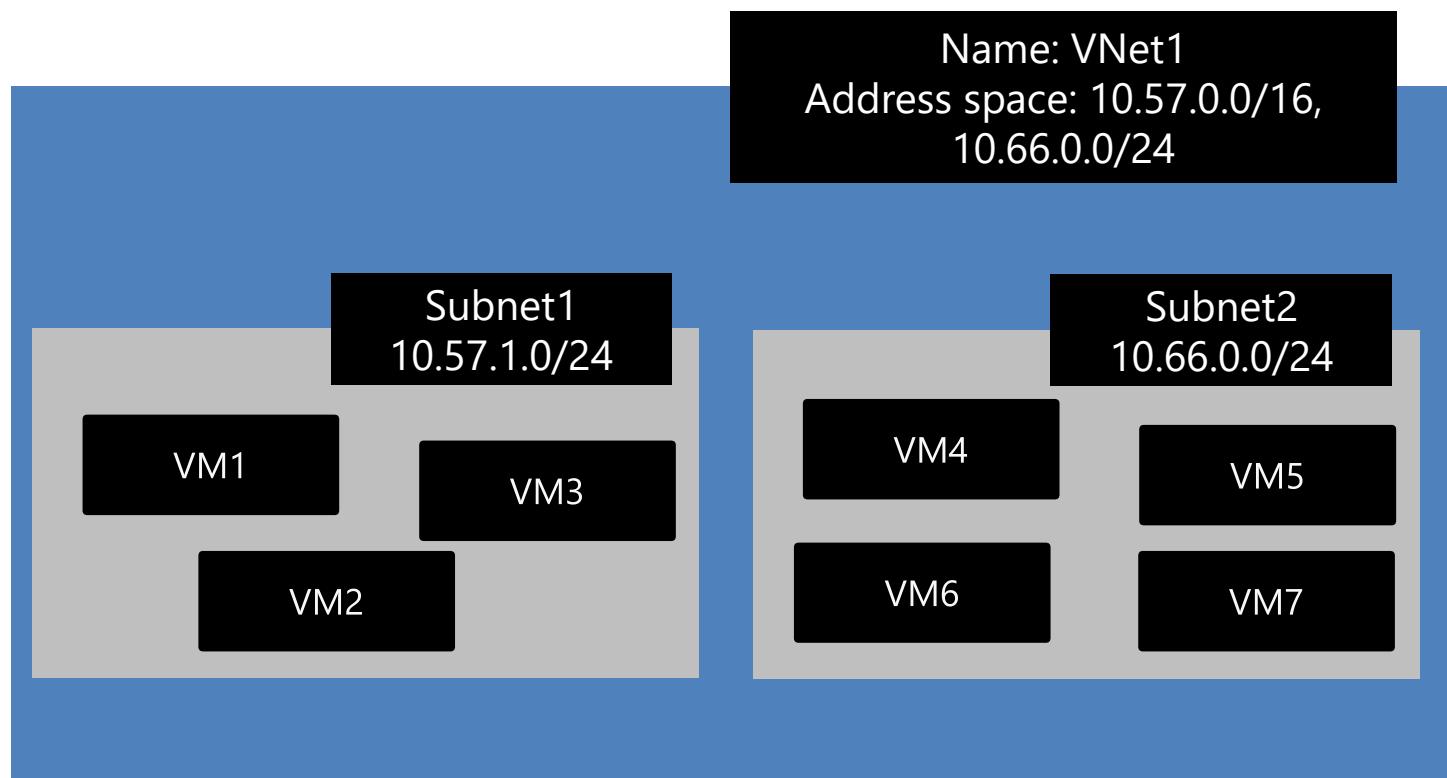
Virtual Network

- Isolated, logical network that provides connectivity for Azure Virtual Machines
- User-defined address space (can be one or more IP ranges, not necessarily RFC1918)
 1. Connectivity for VMs in the same VNET
 2. Connectivity to external networks/on-prem DC's
 3. Internet connectivity



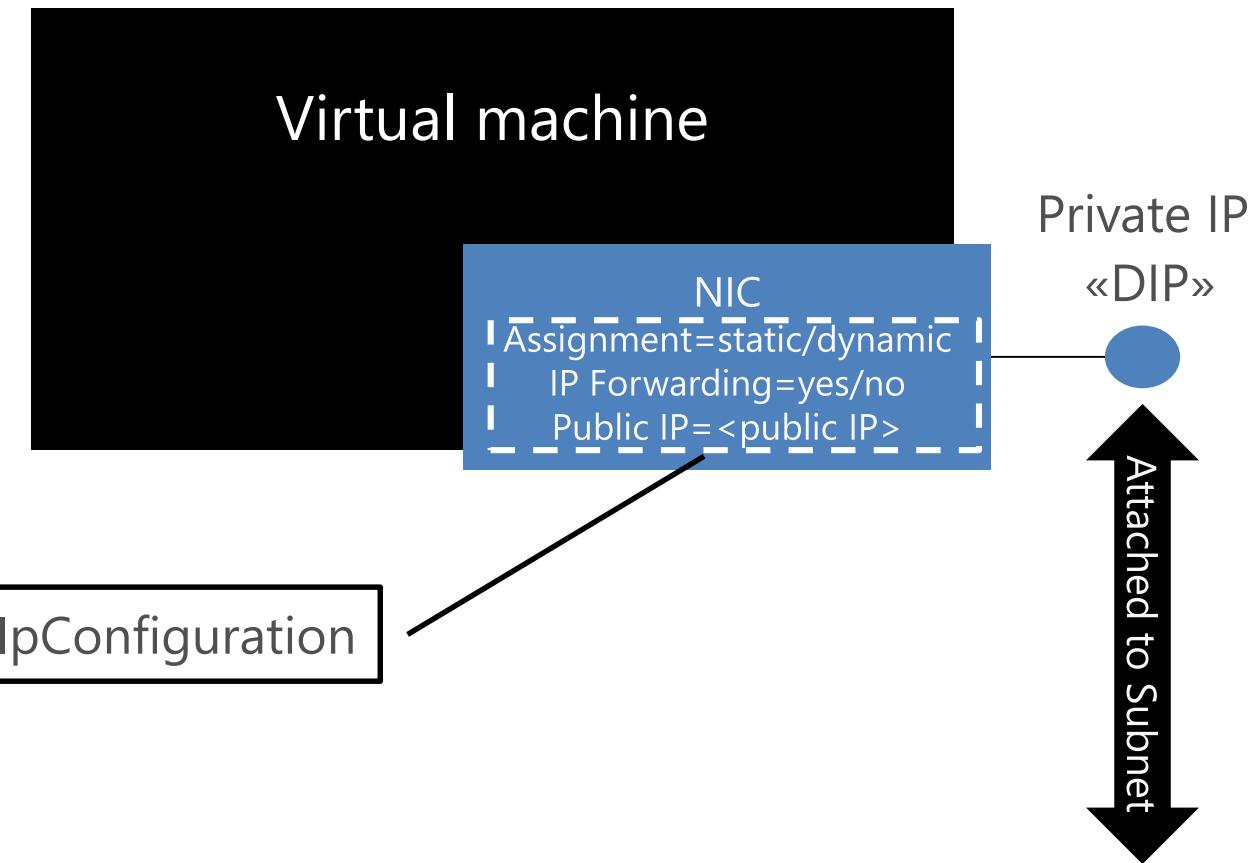
Subnet

- Provides full layer-3 semantics and partial layer-2 semantics (DHCP, ARP, no broadcast / multicast)
- Subnets can span only one range of contiguous IP addresses
- VMs can be deployed only to subnets (not VNETs)



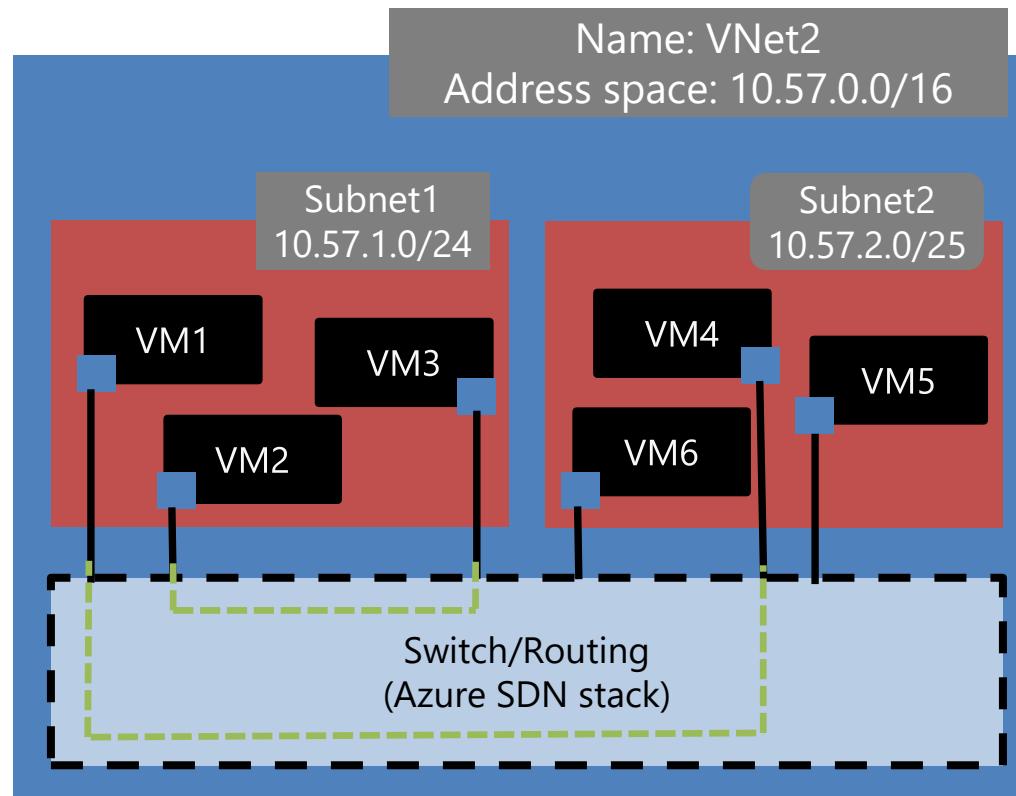
Network Interface

- Virtual NIC that connects a VM to a Subnet
- One private IP address (private == included in the subnet's IP range, not necessarily RFC1918)
- Private IP address always assigned via Azure DHCP



Switching/Routing in Azure VNETs

- A VNET provides a switching/routing functionality that allows VMs to talk to each other



Please note that, in an Azure VNet, packets can flow between two different subnets without explicitly traversing any layer-3 device. Azure's network virtualization stack effectively works as a layer-3 switch





Connectivity

Connecting to Azure

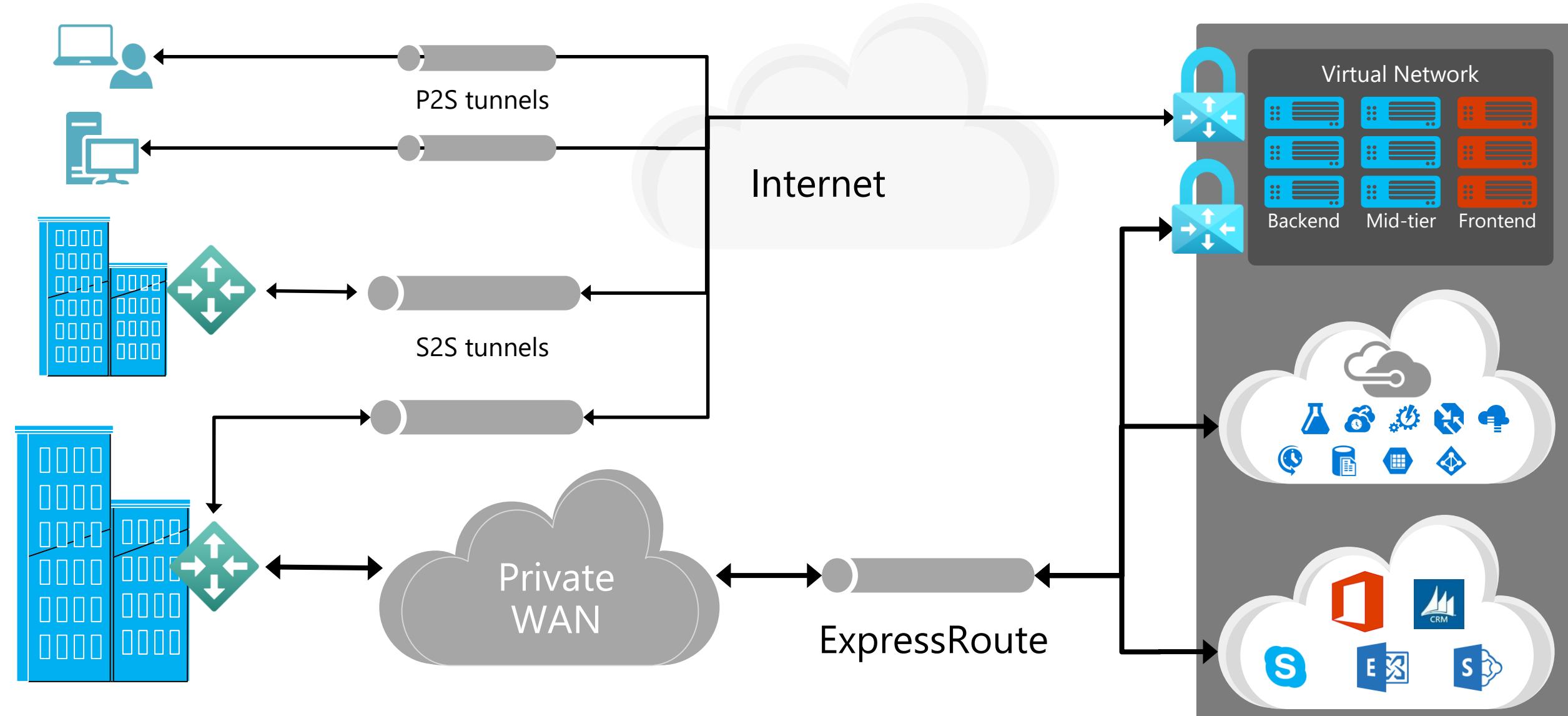
Cloud		Customer	Characteristics
	Internet Connectivity		<ul style="list-style-type: none">• Internet facing with public IP addresses in Azure• VPN connectivity with virtual appliances (Marketplace)
	Remote access point-to-site connectivity		<ul style="list-style-type: none">• Remote Access to VNet/On-prem• Connect from anywhere• Mac, Linux, Windows• Radius/AD authentication
	Site-to-site VPN connectivity		<ul style="list-style-type: none">• High throughput, secure cross-premises connectivity• BGP, active-active for high availability & transit routing
	ExpressRoute private connectivity		<ul style="list-style-type: none">• Private connectivity to Microsoft services• Mission critical workloads

Connecting in Azure

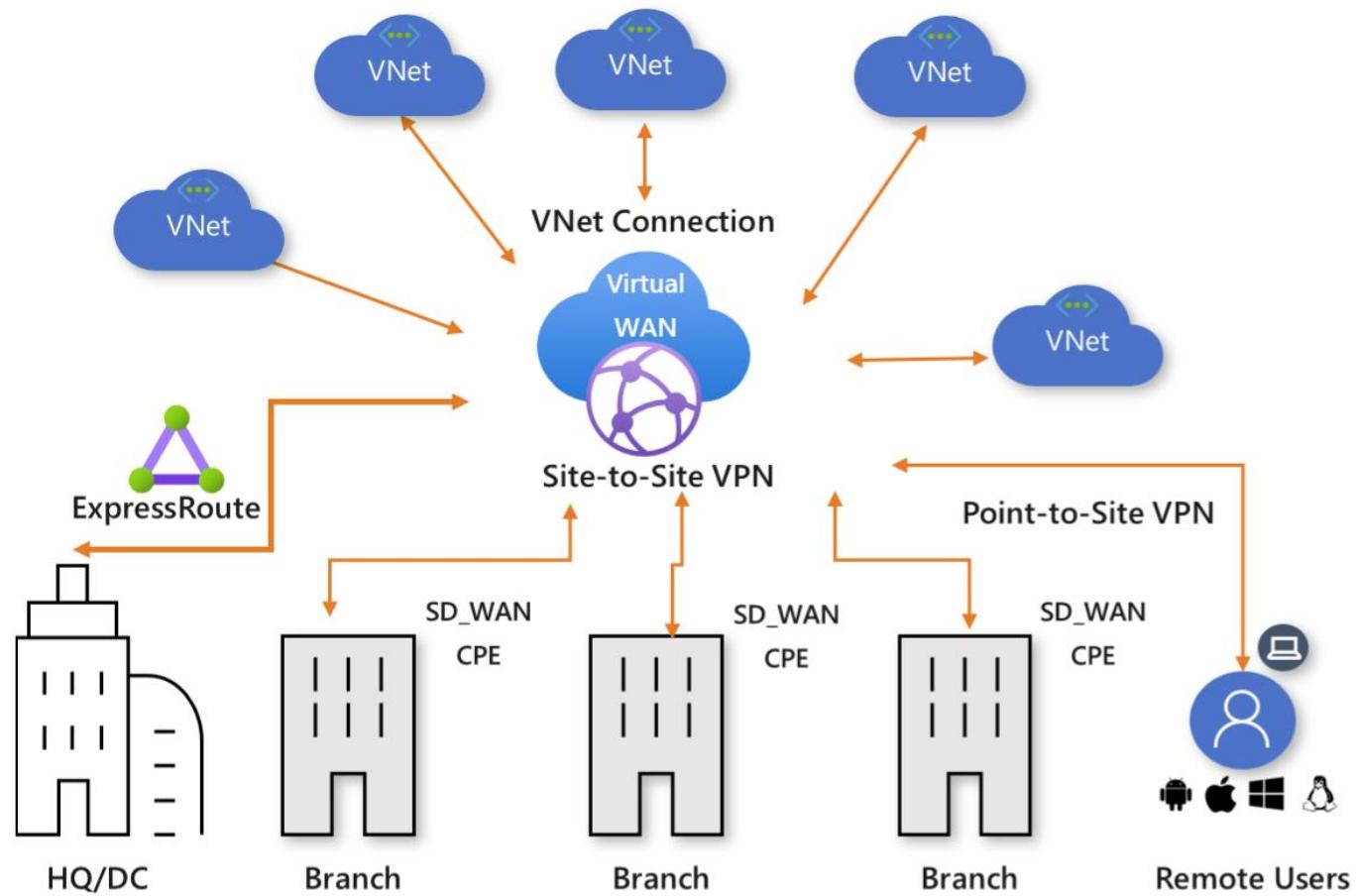
Cloud	Cloud	Characteristics
	VNet Peering	<ul style="list-style-type: none">• Same-/cross-region direct, private VM-to-VM connectivity• NSG & UDR across VNets• GatewayTransit for hub-and-spoke
	VNet-to-VNet via Gateways	<ul style="list-style-type: none">• Transitive routing via BGP and VPN gateways• Secure connectivity via IPsec/IKE across Azure WAN links
	VNet-to-VNet via ExpressRoute circuit	<ul style="list-style-type: none">• Traverse ("hairpin") through ExpressRoute circuit & gateways• Traffic is not encrypted

Cross premises connectivity overview

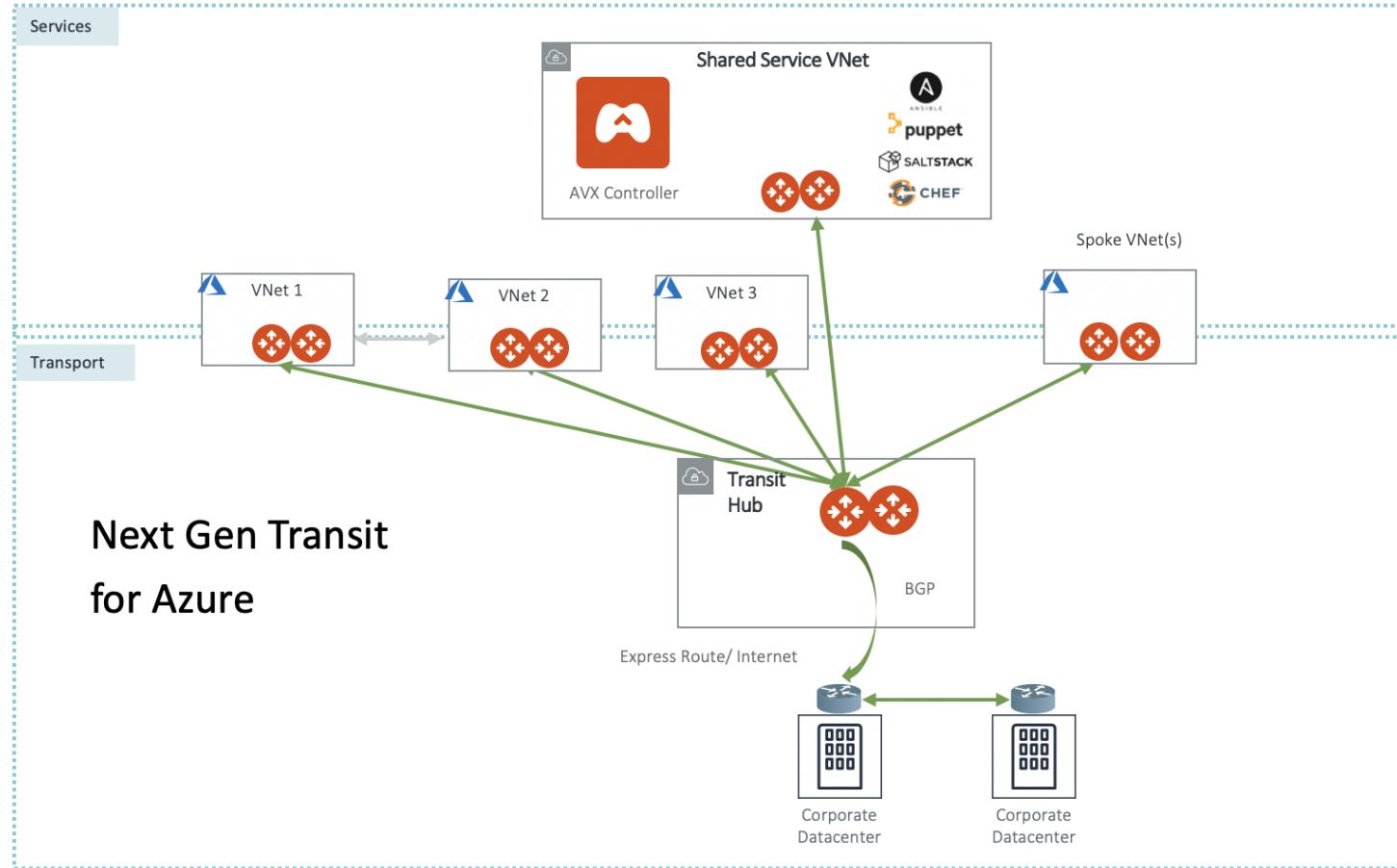
Microsoft



Azure Virtual WAN



NextGen Cloud Networking



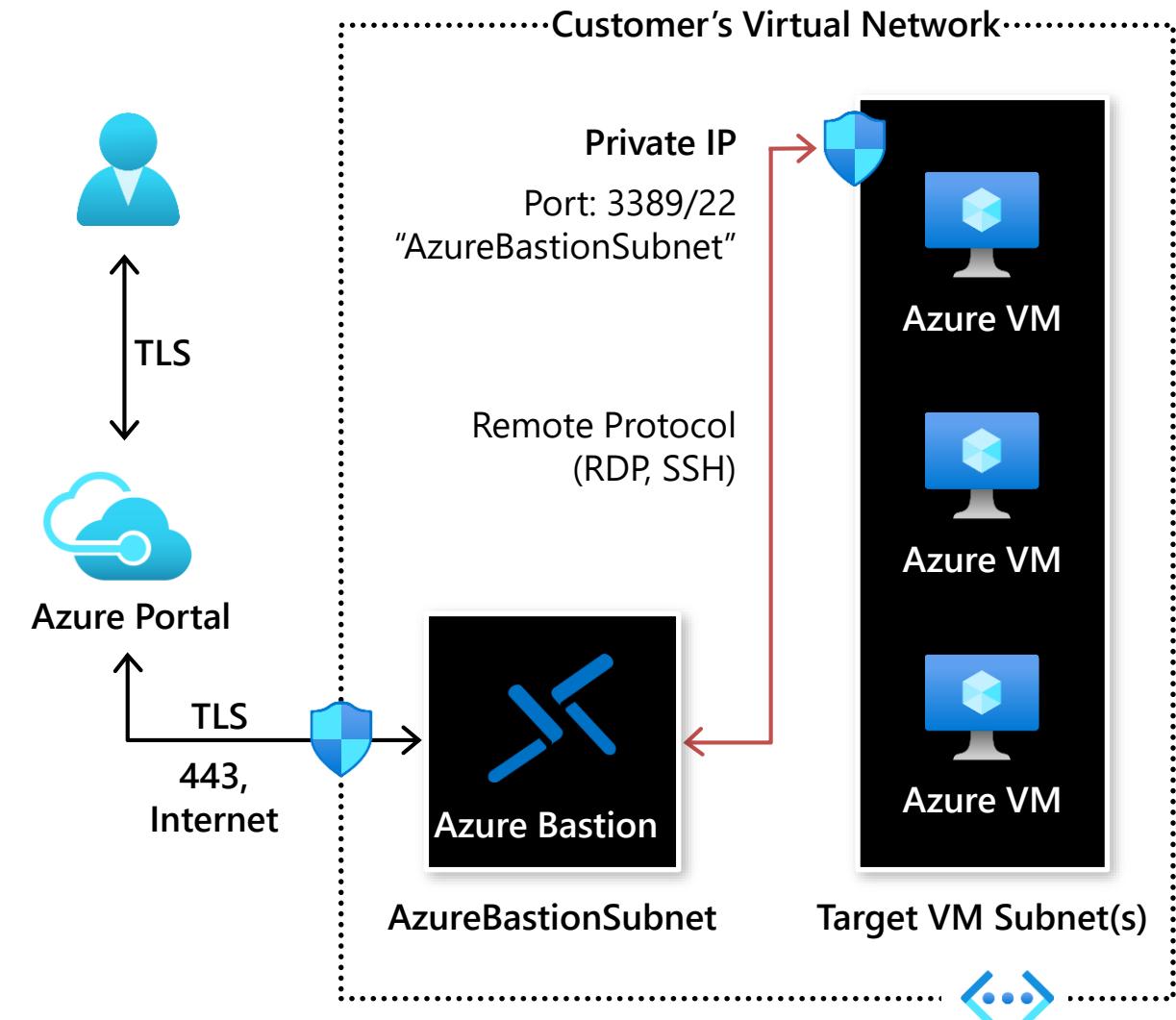
Azure Bastion

Secure and seamless RDP and SSH access to your virtual machines

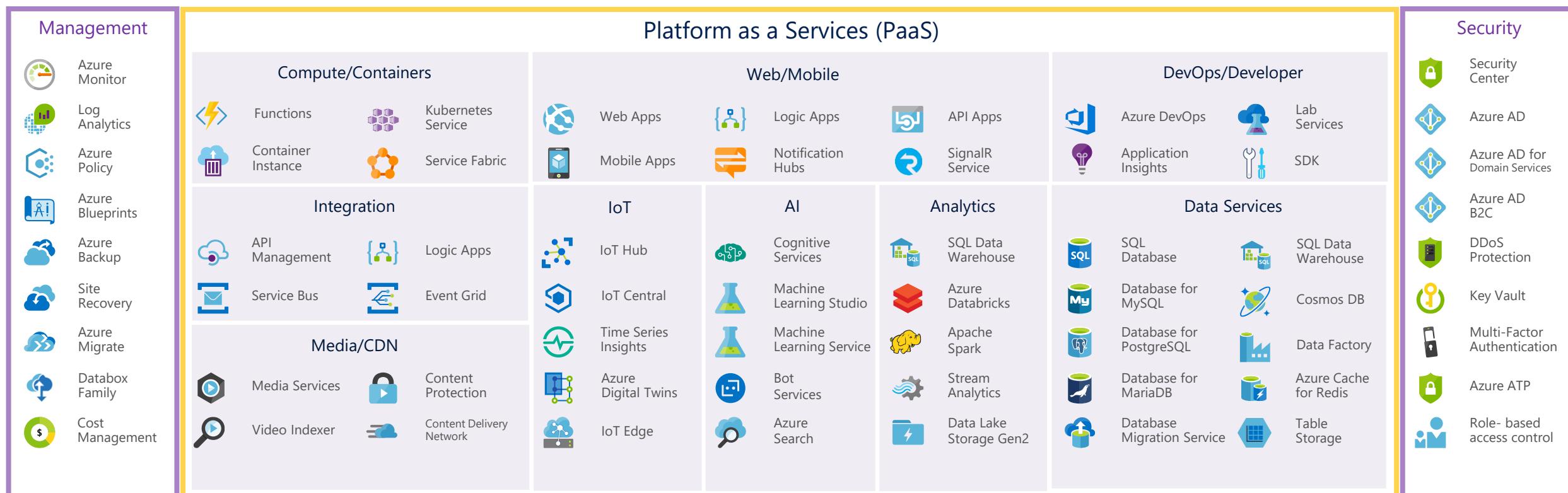
RDP/SSH to your workload using HTML5 standards-based web-browser, directly in Azure Portal

Resources can be accessed without public IP addresses

Supported Azure resources include VMs, VM Scale Sets, Dev-Test Labs



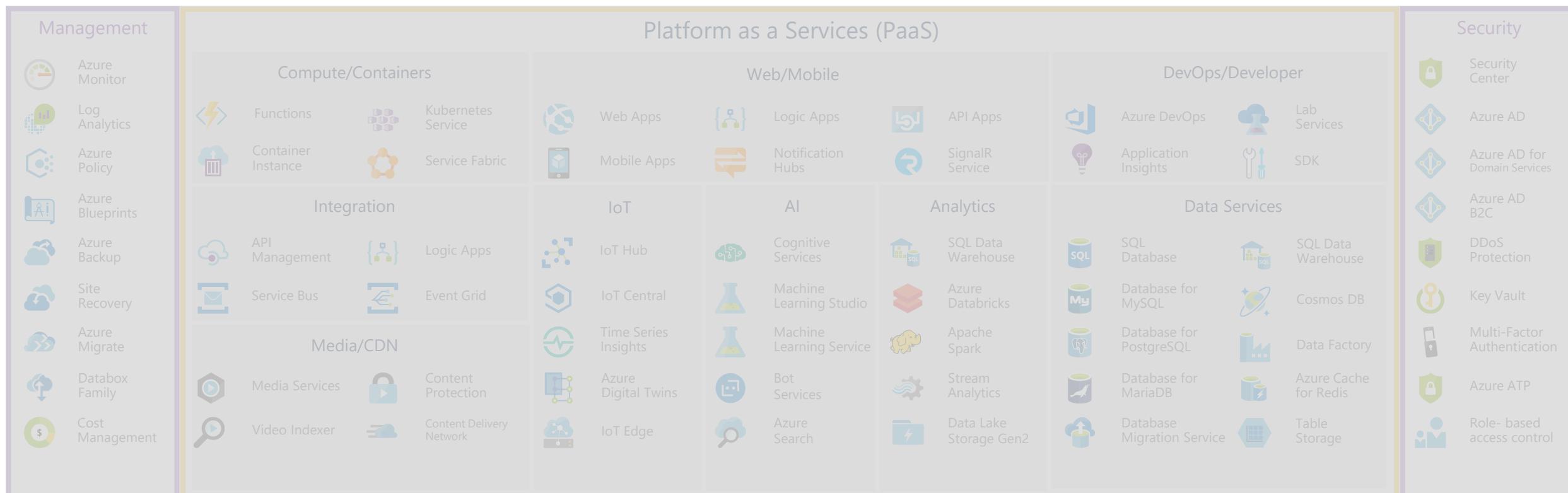
High Level Azure Services



Azure Datacenter Infrastructure



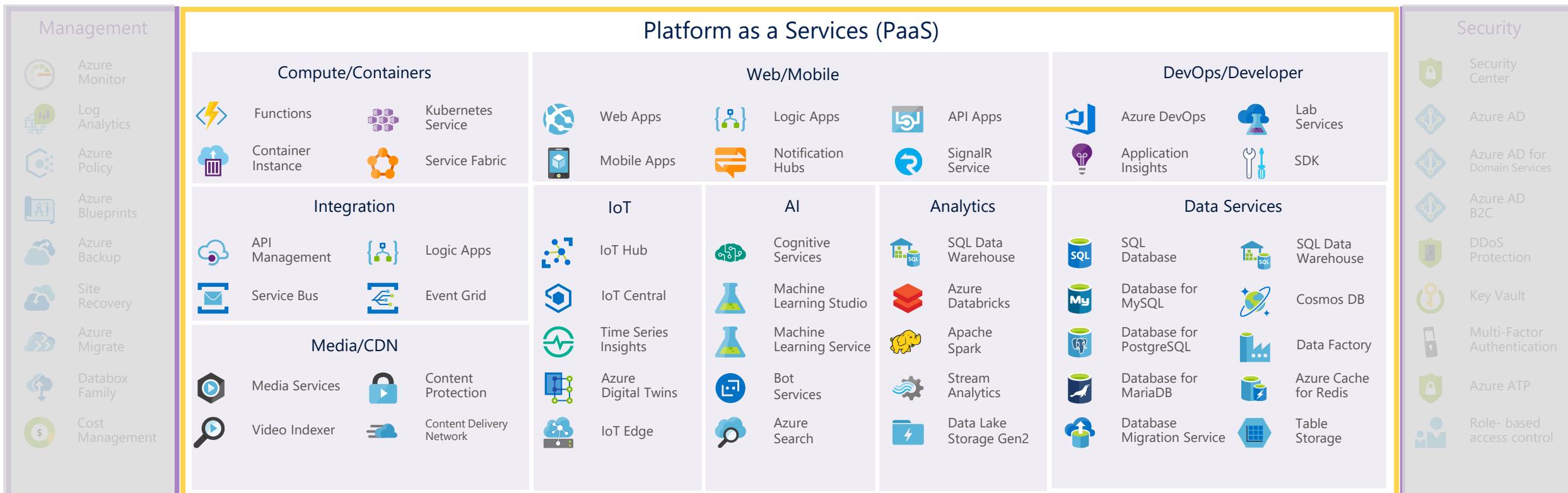
High Level Azure Services



Azure Datacenter Infrastructure



High Level Azure Services



Azure Datacenter Infrastructure





Azure Load Balancer

Azure Load Balancer

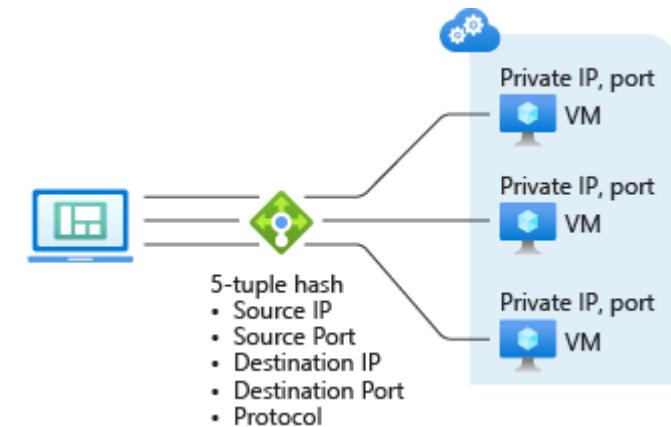
Allows you to scale your applications and create **high availability** and **resiliency** for your services and applications

Public

A public Load Balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the VM and vice versa.

Internal

An internal Load Balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.



Public Load Balancer

A public Load Balancer maps the **public IP address** and port number of incoming traffic to the **private IP address** and port number of the VM

Automatic reconfiguration

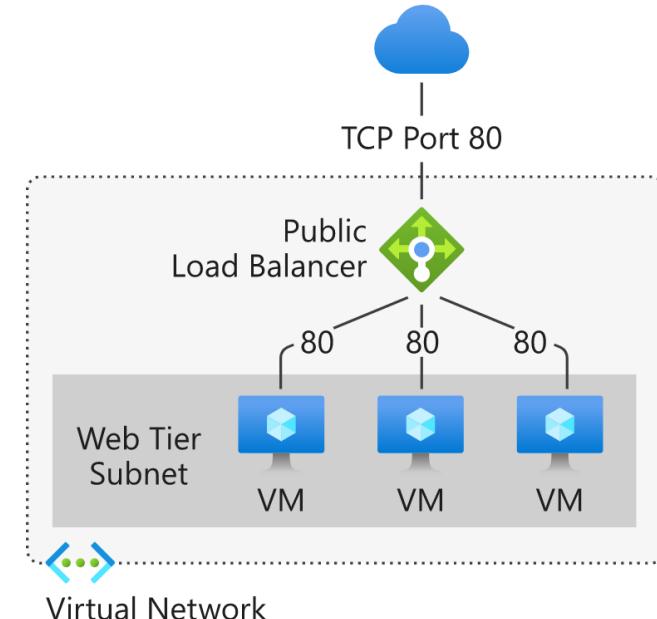
Instantly reconfigures itself as you scale instance up or down

Outbound connections (SNAT)

All outbound flows from private IP addresses inside your virtual network to public IP addresses on the internet can be translated to a frontend IP address of the Load Balancer

Default Distribution Mode

Azure Load Balancer distributes traffic evenly amongst multiple VM instance



Internal Load Balancer

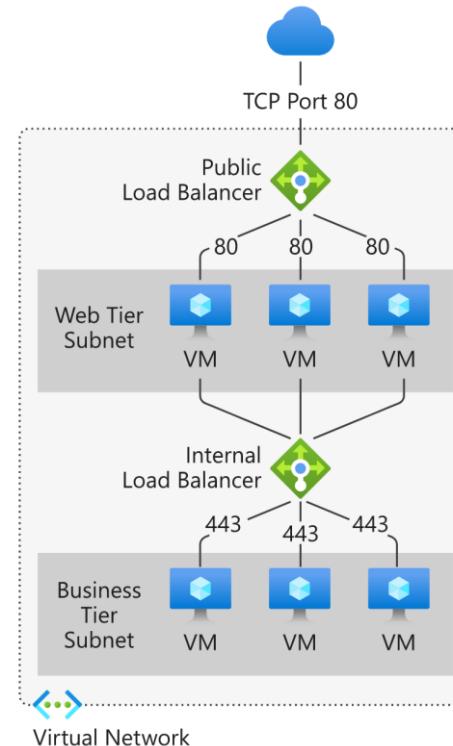
An internal Load Balancer directs traffic only to resources **inside a virtual network** or that use a VPN to access Azure infrastructure

Within a virtual network

Cross-premises virtual network

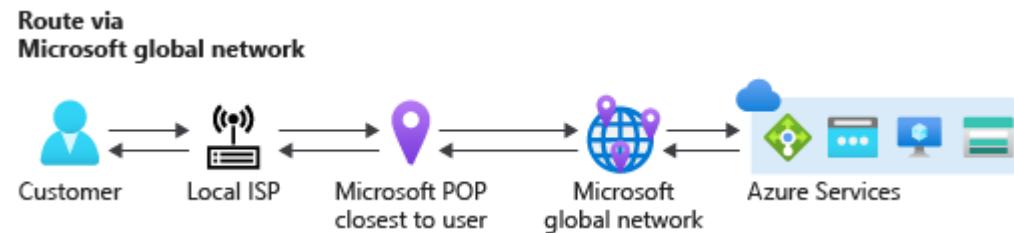
Multi-tier applications

Line-of-business applications

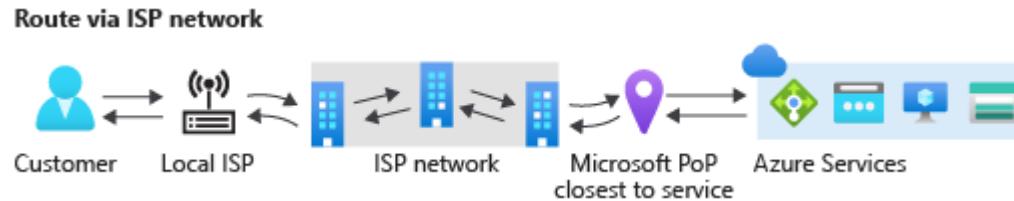


Routing Preference

Routing via Microsoft-Network



Routing via Internet



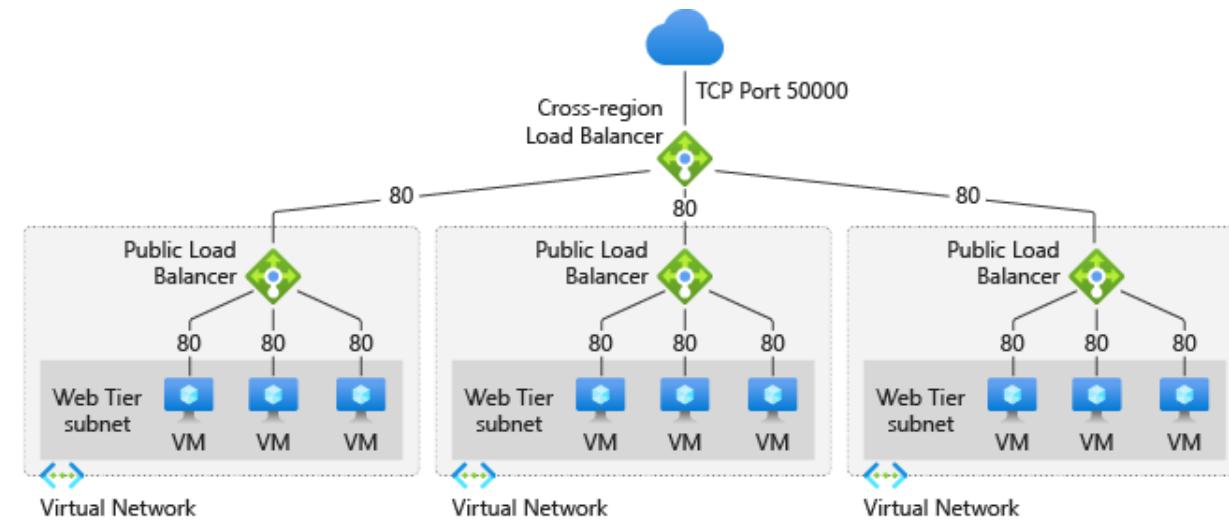
Cross-Region Load Balancer

Challenge with Load Balancers

- Bound to a VNET
- Bound to a region
- Global Deployments have different Frontend IPs
- Manual changes required in case of a disaster

Cross-Region Load Balancer

- Load Balancer of Load Balancers
- Backends are regional public LBs
- No private / internal LBs, no UDP

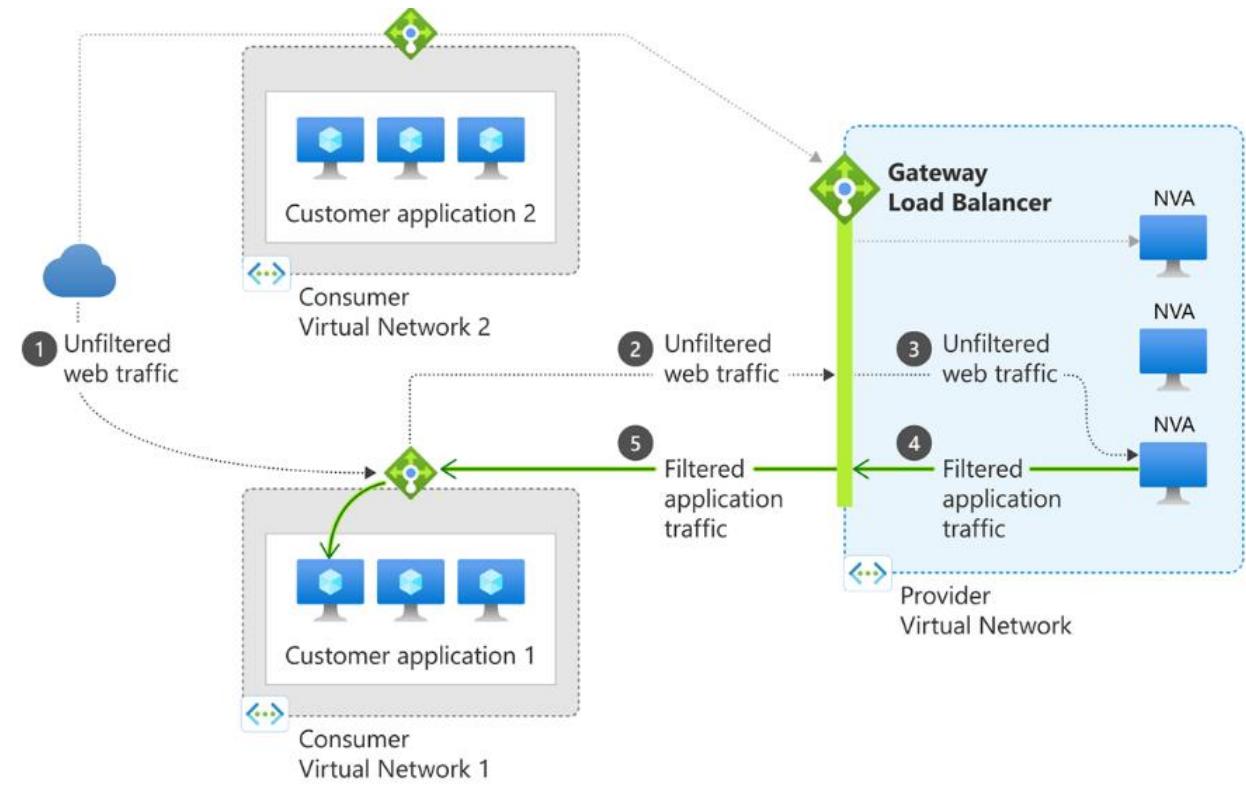


Gateway Load Balancer

Gateway Load Balancer allow to easily deploy, scale, and manage NVAs

Benefits

- integrate NVA transparently
- Easy add or remove - scaling
- Improve NVA availability
- Chain applications across regions and subscriptions





DEMO – LOAD BALANCERS



Azure Traffic Manager (TM) Azure Front Door (AFD)

Azure Traffic Manager

Azure Traffic Manager is a **DNS-based traffic load balancer** that enables you to distribute traffic optimally to services across global Azure regions

Global DNS load balancing

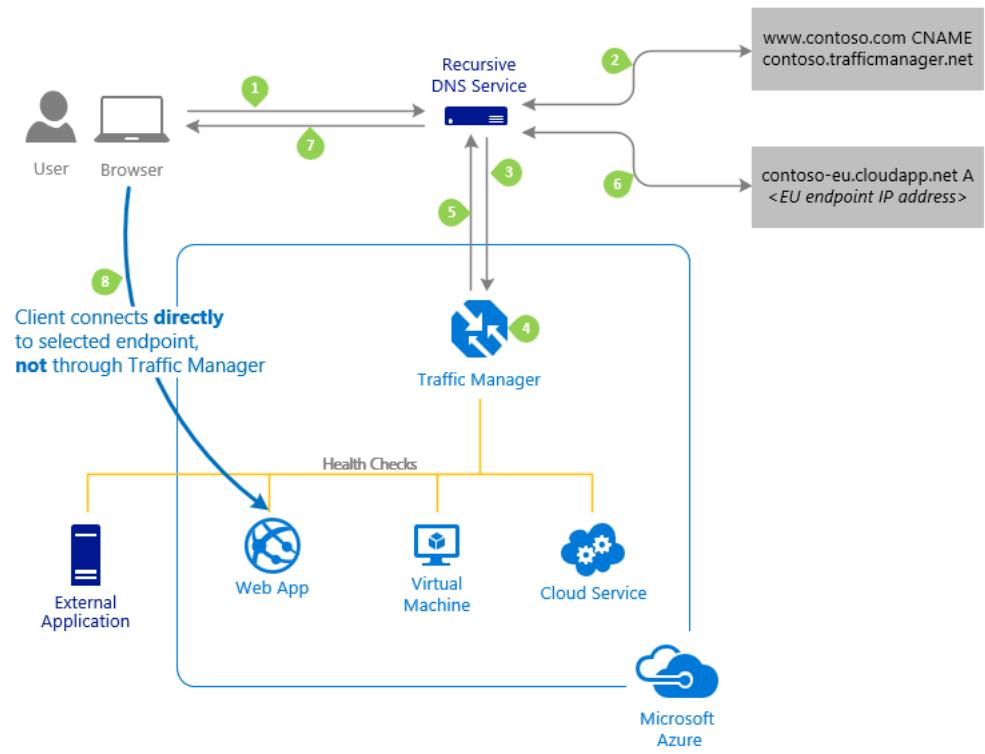
Automatic failover when an endpoint goes down

Combine with hybrid applications

Supports external, non-Azure endpoints so that it can be used with hybrid cloud and on-premises deployments

Distribute traffic for complex deployments

Use nested Traffic Manager profiles for sophisticated, flexible rules for complex deployments



Azure Front Door

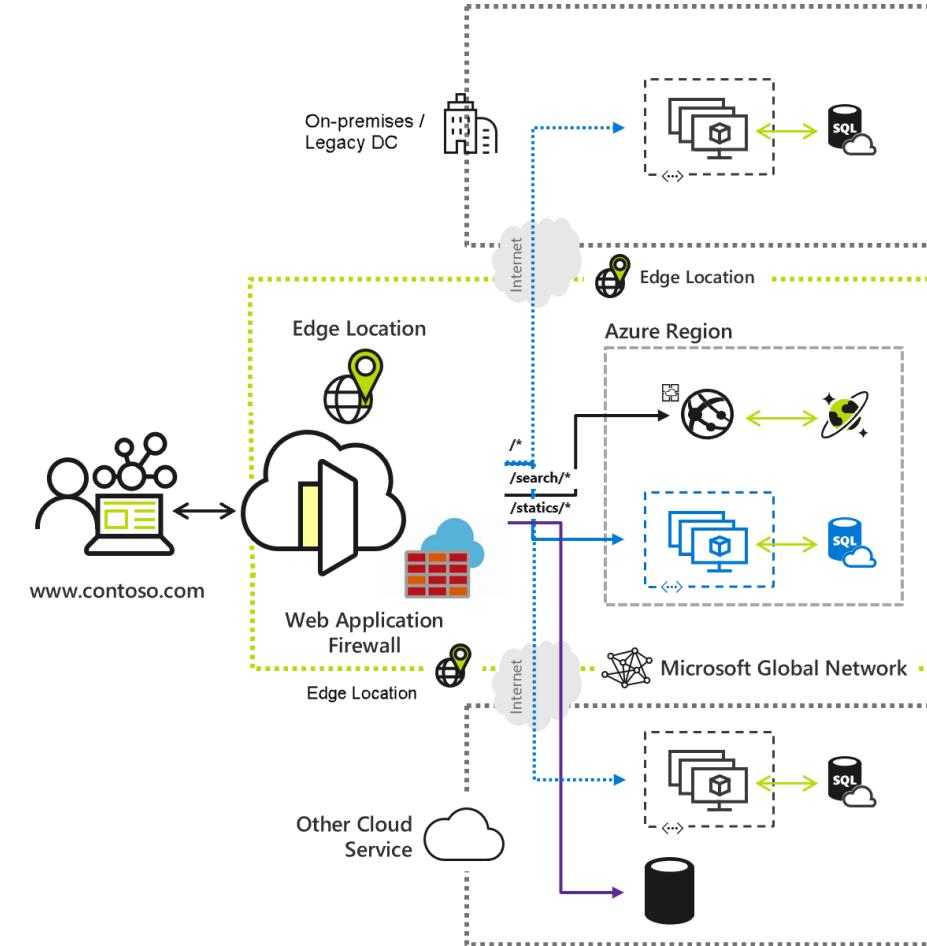
Azure Front Door Service provides a **scalable and secure entry point** for fast delivery of your global web applications

SSL offload and application acceleration

Global HTTP load balancing with instant failover

Application Firewall and DDoS protection

Centralized traffic orchestration view



Azure Front Door

Single or multi-region app and API acceleration

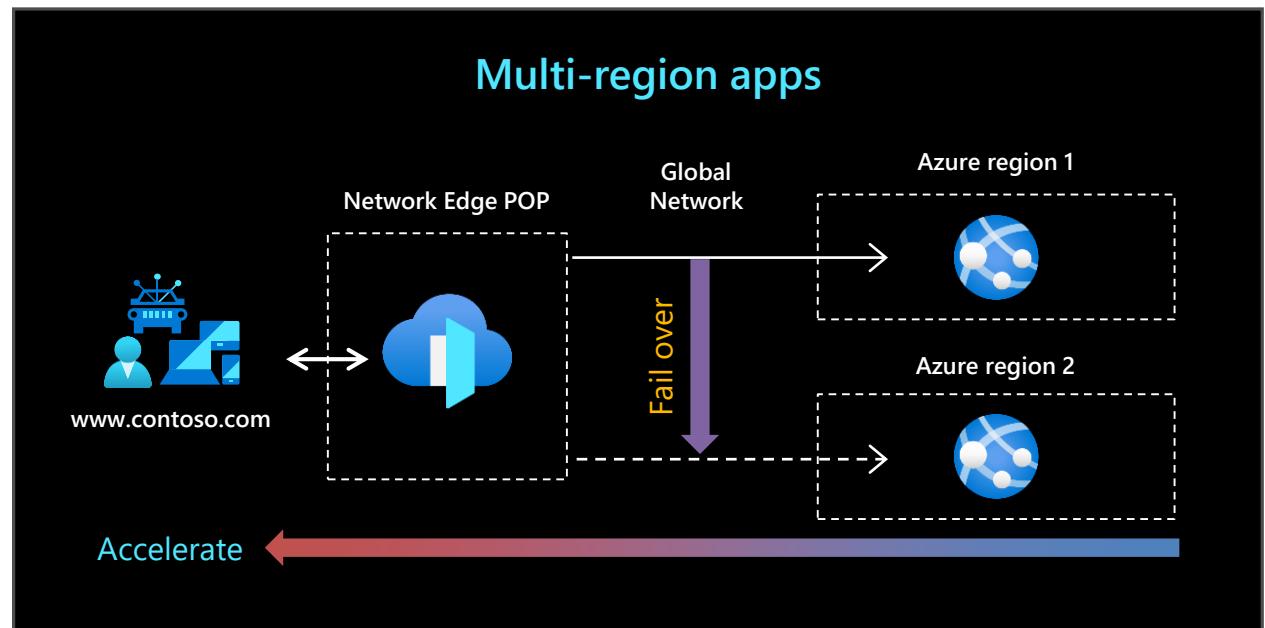
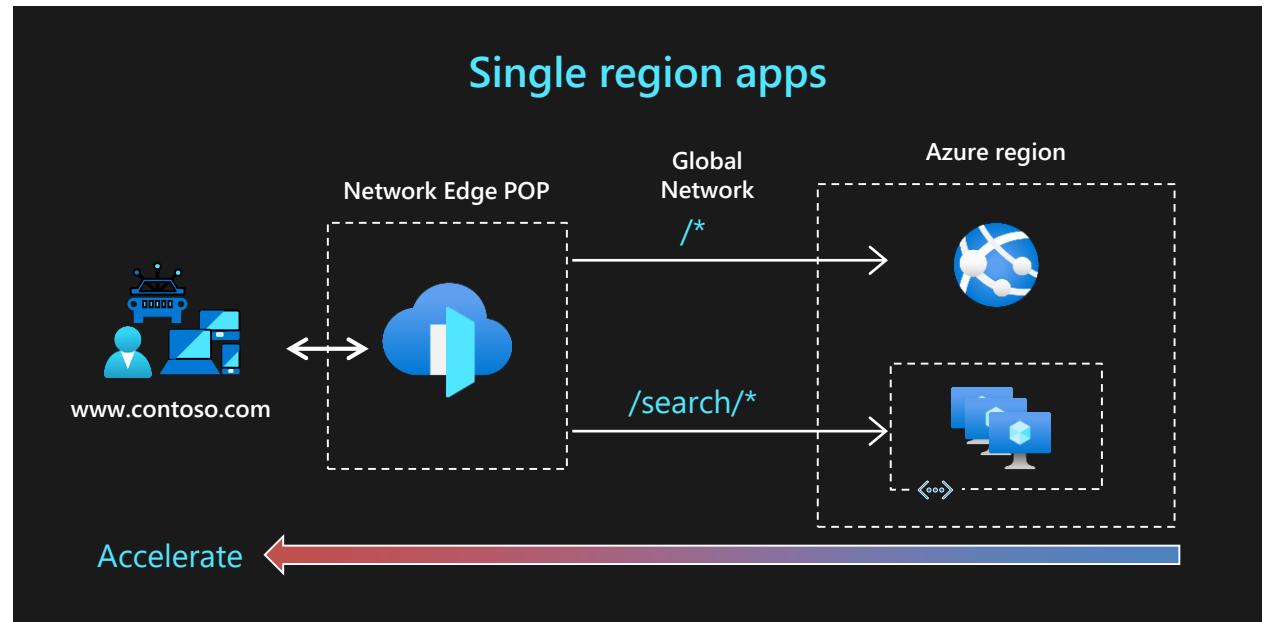
Improve HTTP performance and reduce page load times

Load balancing at the Edge and fast-failover

Build always-on application experiences that fail-fast (safely)

Integrated SSL, WAF and DDoS

Protect and scale your application to global users, devices, traffic and attacks



Traffic Manager or Front Door?

Traffic Manager

Any protocol: Because Traffic Manager works at the DNS layer, you can route any type of network traffic; HTTP, TCP, UDP, etc.

On-premise routing: With routing at a DNS layer, traffic always goes from point to point. Routing from your branch office to your on-premises datacenter can take a direct path; even on your own network using Traffic Manager

Billing format: DNS-based billing scales with your users and for services with more users, plateaus to reduce cost at higher usage

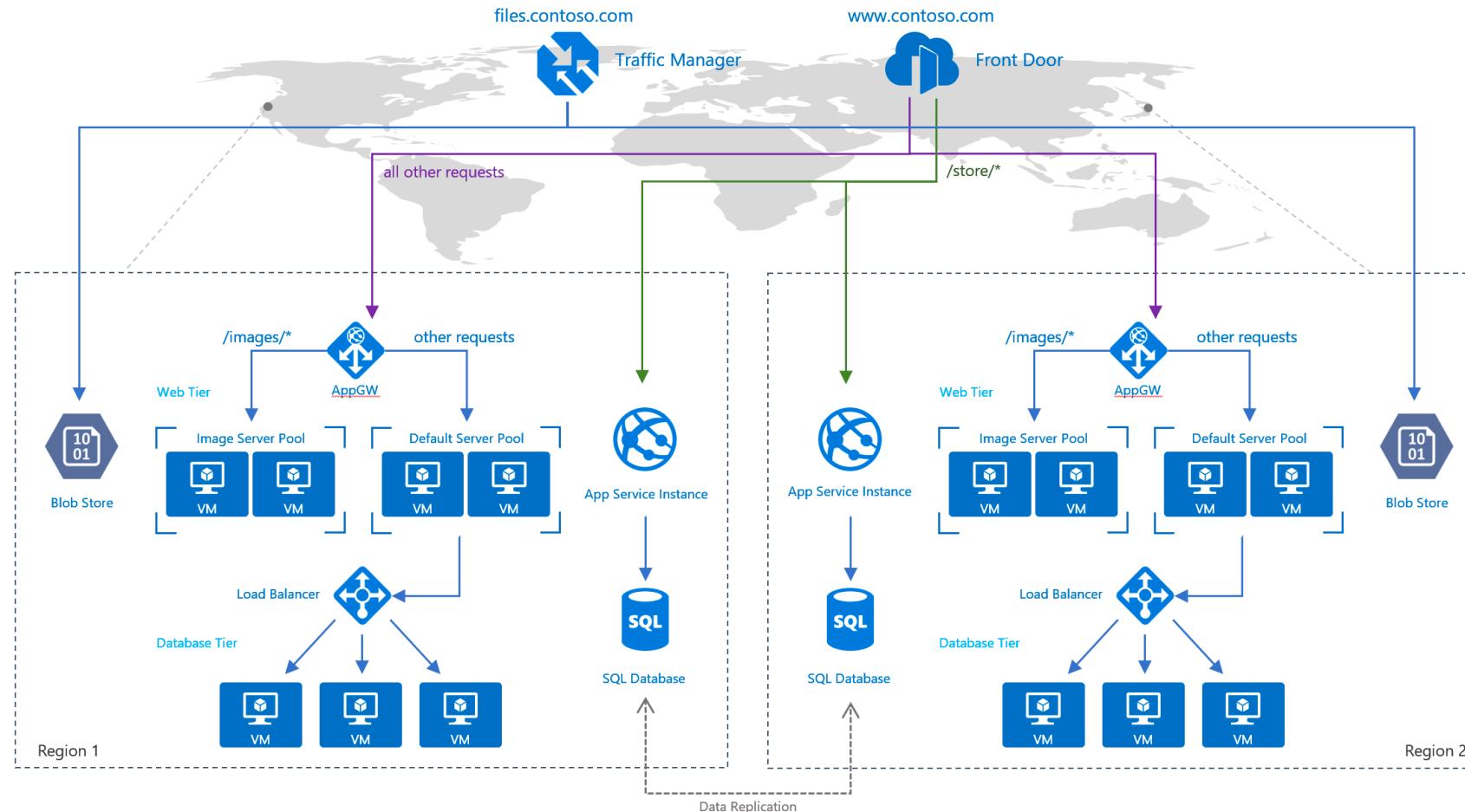
Front Door

HTTP acceleration: With Front Door traffic is proxied at the Edge of Microsoft's network. Because of this, HTTP(S) requests see latency and throughput improvements reducing latency for SSL negotiation and using hot connections from AFD to your application

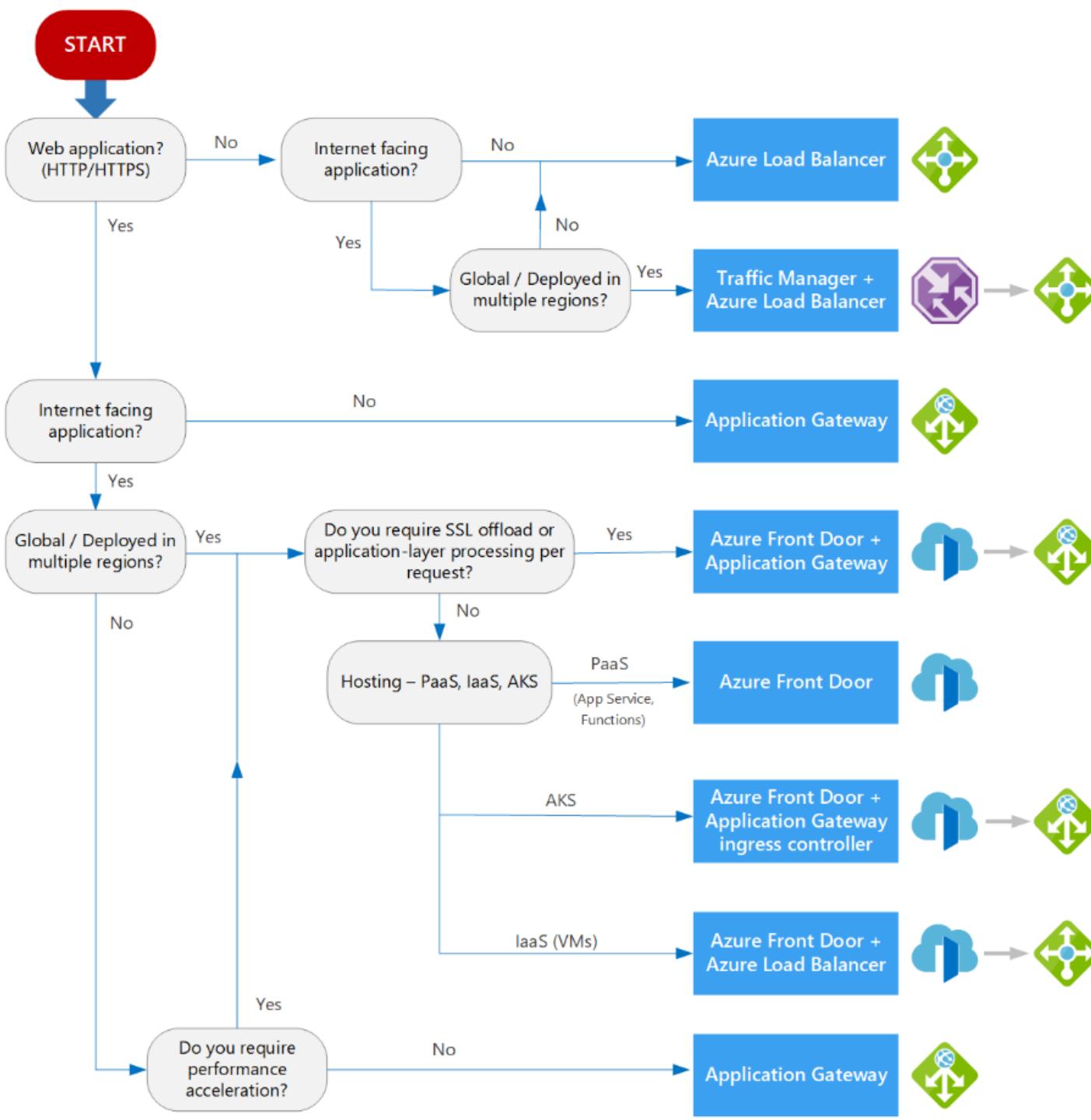
Independent scalability: Because Front Door works with the HTTP request, requests to different URL paths can be routed to different backend/regional service pools (microservices) based on rules and the health of each application microservice

Inline security: Front Door enables rules such as rate limiting and IP ACL-ing to let you protect your backends before traffic reaches your application

Traffic Manager or Front Door?



What to use?





DEMO – LOAD BALANCING



OK ...

... but that's only outside networks



Service Endpoints and Private Link

PaaS Services and Networking

- PaaS Services are designed to be accessed via public endpoints
- Two main challenges
 - Access “internal” data sources from PaaS (e.g. present SAP data in Azure WebApp)
 - Access PaaS Services from “internal” Systems (e.g. use Azure SQL DB with an app running in a VM with no Internet access)
- Ways to integrate PaaS into networks

PaaS Services and Networking

Deploy a dedicated service

Deploy customer specific service instance into own VNET – also for 3rd Party
Integrate PaaS Services into VNET

Use Service Endpoints

Access to public endpoints via MS Backbone
Private IP → Public IP allowed

Utilize Private Links / Endpoints

Private Endpoint (NIC) for your PaaS providing private IP addresses

PaaS → VNET
(VNET → PaaS)

VNET → PaaS

VNET → PaaS

App Service VNET Integration
Integration Service Environments
App Service Environment
Azure Kubernetes Service (AKS)
...

Azure Storage
Azure Databases
Azure KeyVault
Azure Cognitive Services
...

Azure Automation
Azure Data Factory
Azure IoT Hub
Azure Migrate
...

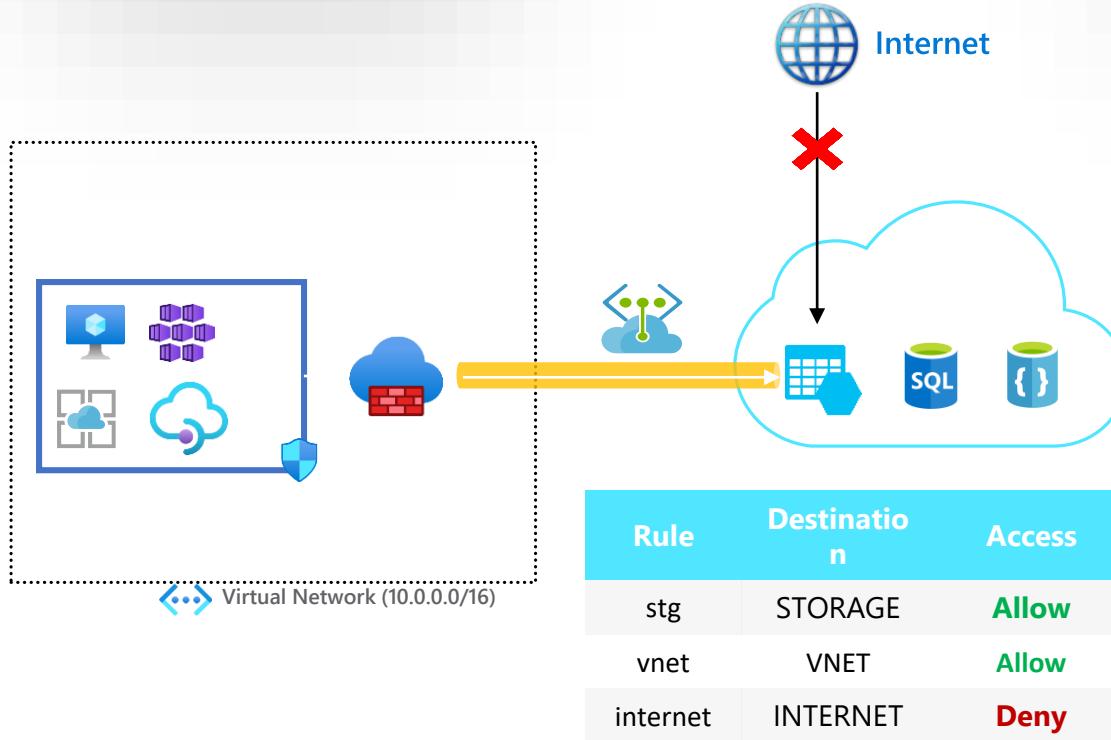
Azure NetApp Files
Dedicated HSM

Azure Container Registry (Preview)

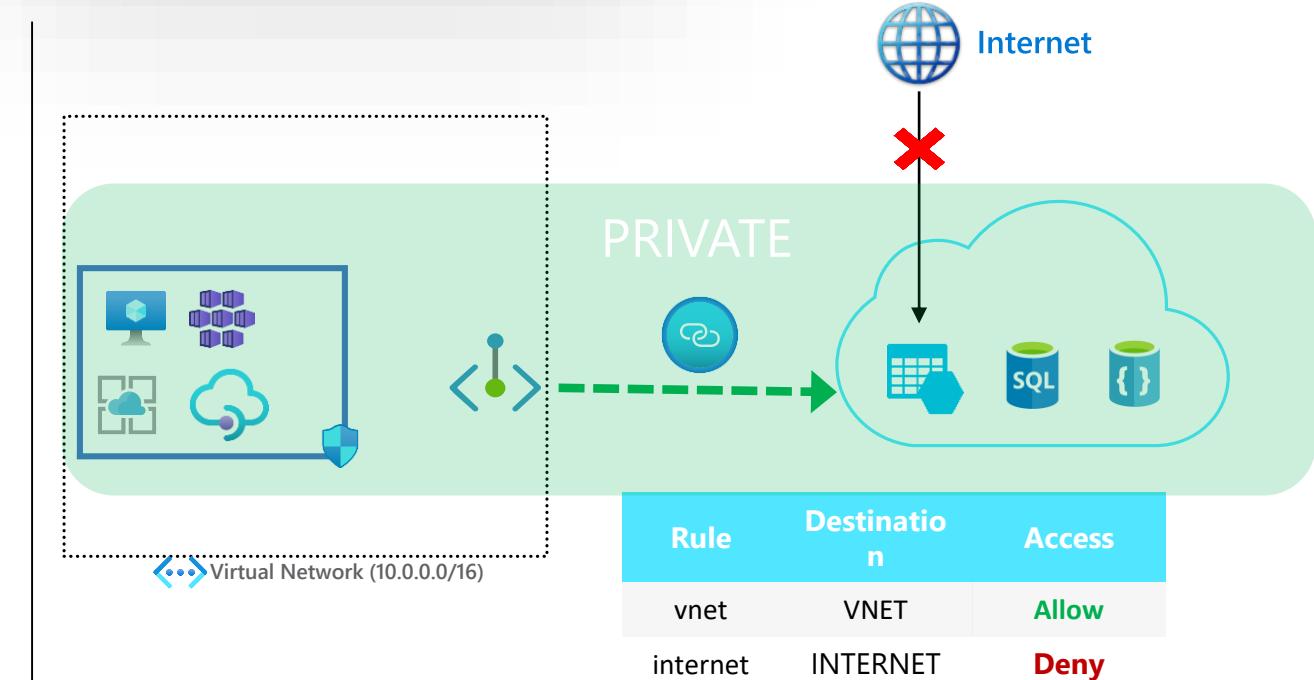
Azure Private Link Services (own)

Private PaaS

SERVICE ENDPOINT



PRIVATE LINK – PRIVATE ENDPOINT

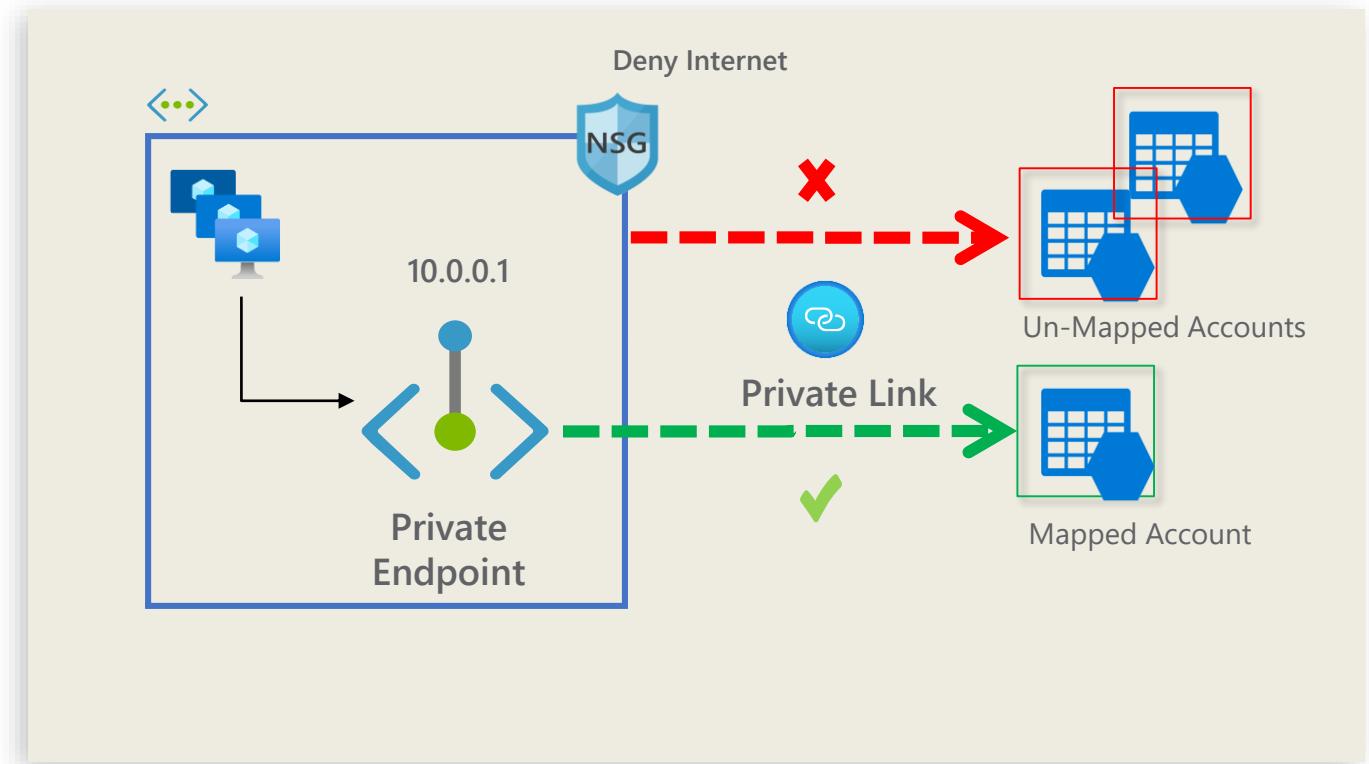


- VNet to PaaS service via the Microsoft backbone
- Destination is still a public IP address. NSG opened to Service Tags
- Need to pass NVA/Firewall for exfiltration protection

- VNet Paas via the Microsoft backbone
- PaaS resource mapped to Private IP Address. NSGs restricted to VNet space
- Built-in data exfiltration protection

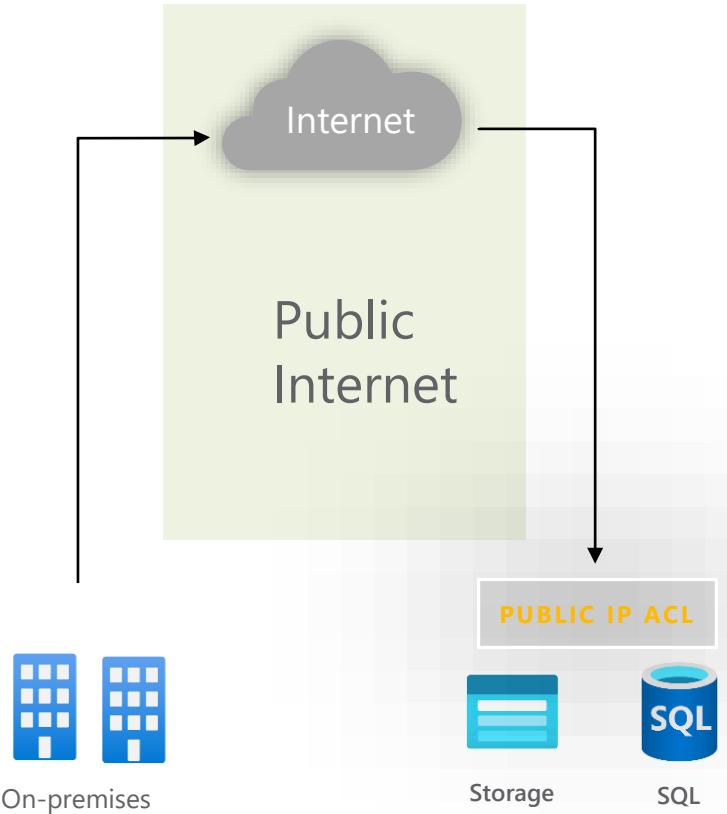
Data Exfiltration Protection

- Private Endpoint maps specific PaaS resource to an IP address, not the entire service
- Access only to mapped PaaS resource
- Data exfiltration protection is in-built



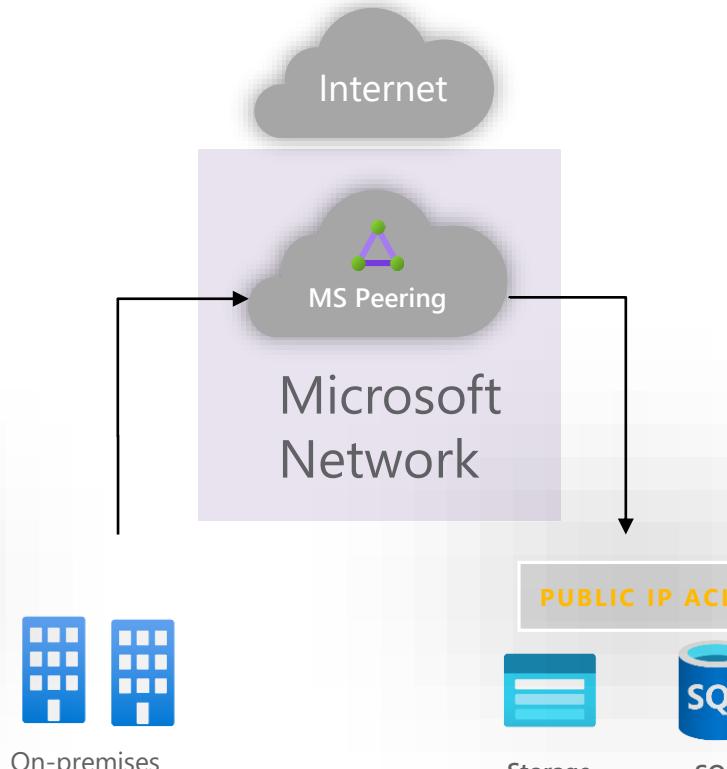
Secure connectivity from on-premises

Good



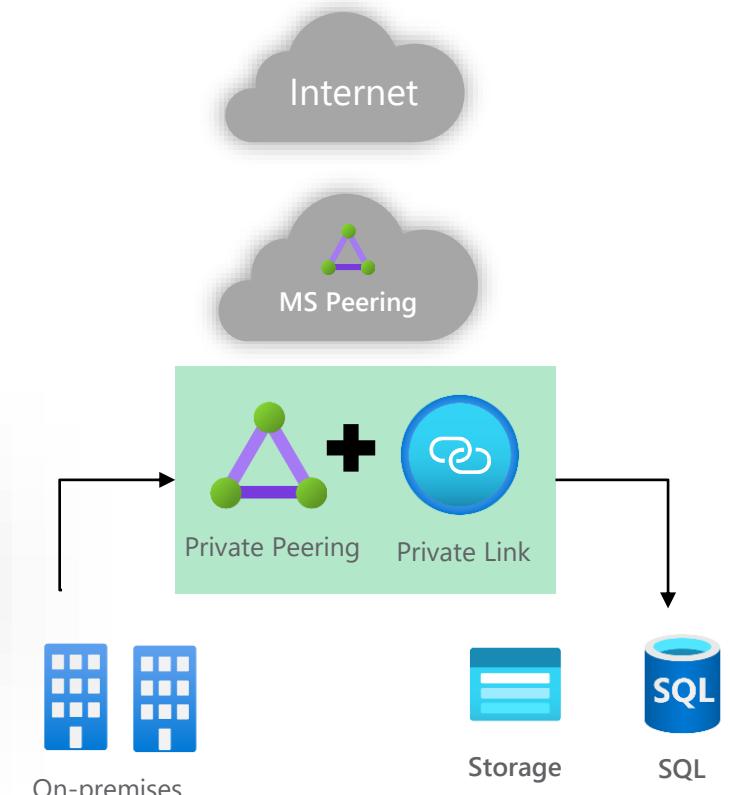
- Traffic traverses the Internet
- Secured using ACLs on Public IPs
- Corporate firewall open to Azure Public IPs

Better



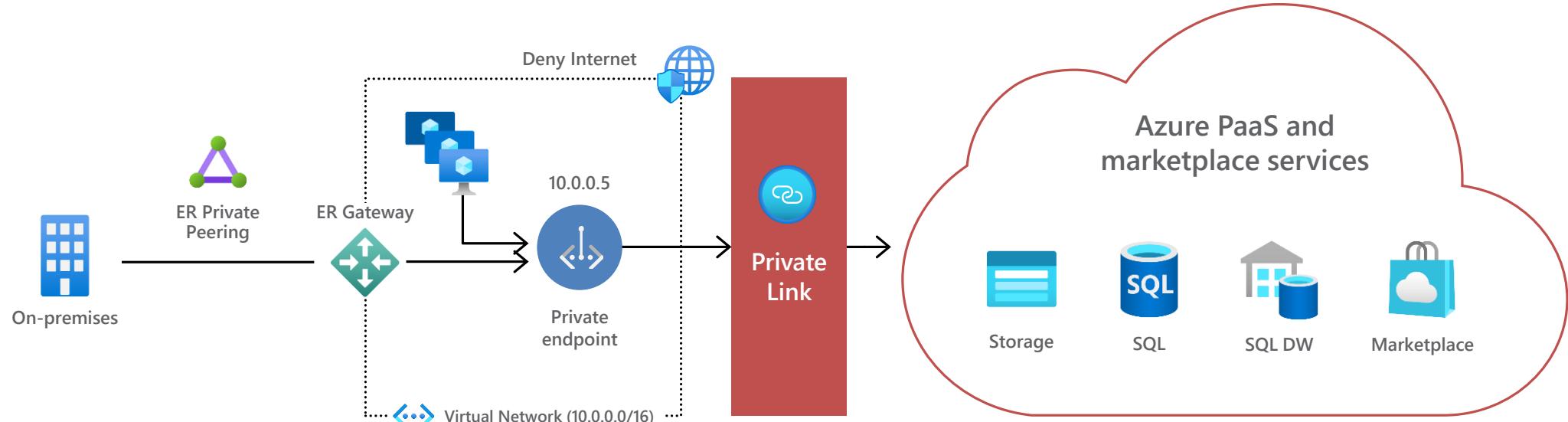
- Traffic stays within Microsoft and partner network
- MS Peering draws Microsoft Public IP traffic
- Corporate Firewall open to Azure Public IPs

Best



- Traffic is fully private traversing the Microsoft network
- No exposure of public IPs on either side
- Corporate Firewall open only to private

Azure Private Link



Private Link for Azure Storage, SQL DB and customer own service

Private access from Virtual Network resources, peered networks and on-premise networks

In-built Data Exfiltration Protection

Predictable private IP addresses for PaaS resources

Unified experience across PaaS, Customer Owned and marketplace Services



There is even more ...

Your Own Private Link Service

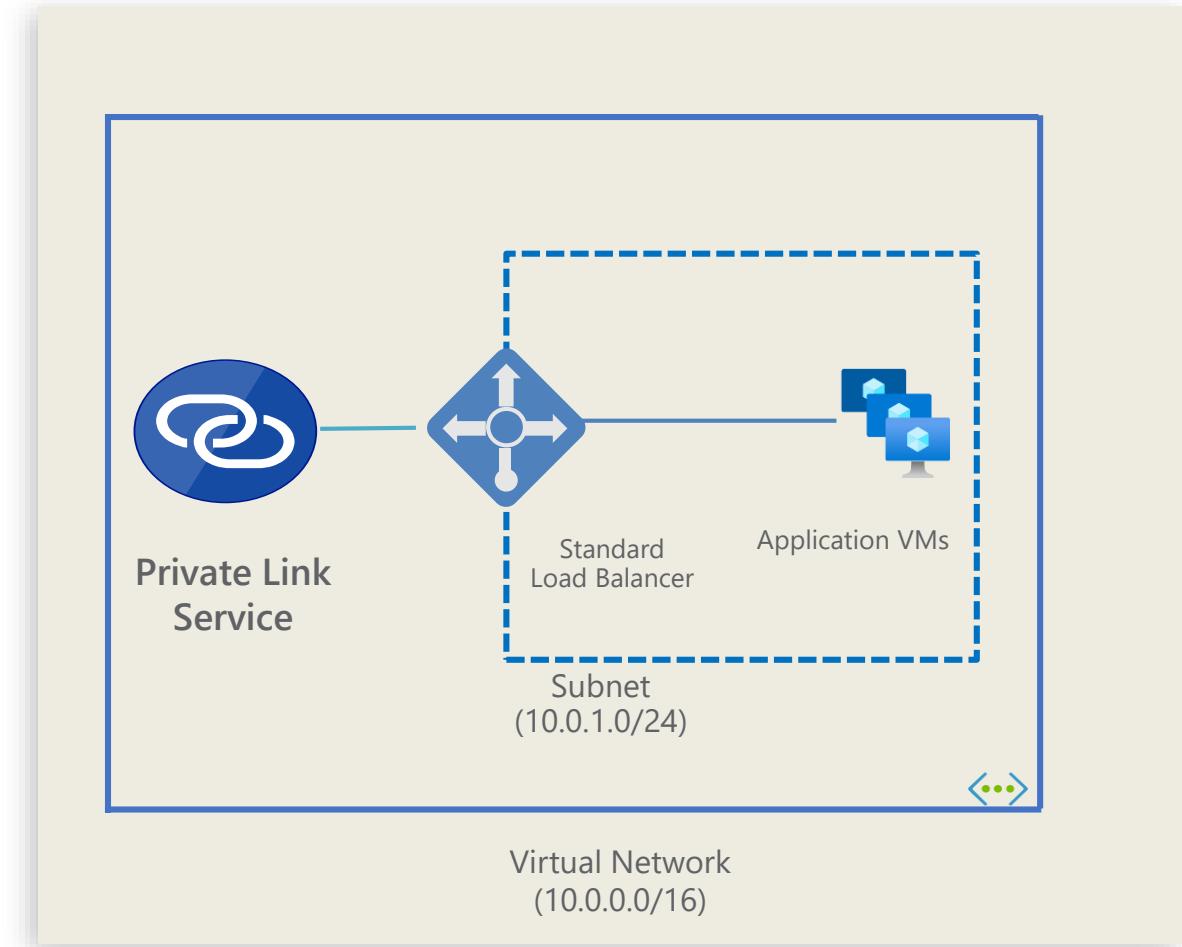
- Create or Convert your existing services into Private Link Service
- VNet-VNet Connectivity without worrying about overlapping IP Space
- No regional, tenant, subscription or RBAC restrictions
- Easily Scale and manage your service



Private Link
Service

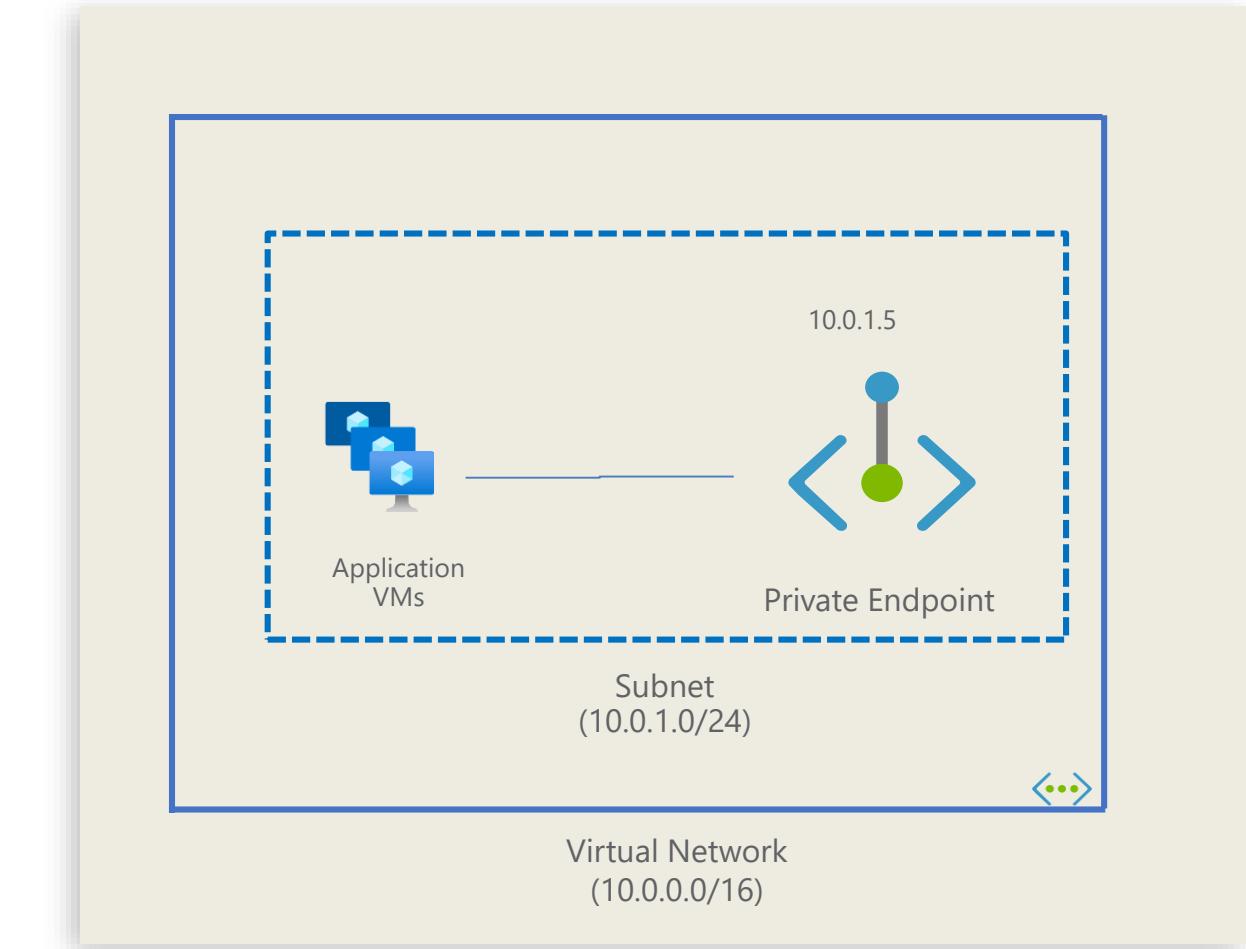
Create Private Link Service

- Application running behind Standard Load Balancer can be converted into Private Link service with one click of a button/one API call
- Private Link Service tied to Frontend IP configuration of Standard Load Balancer
- Frontend IP Configuration can be either Public or Private

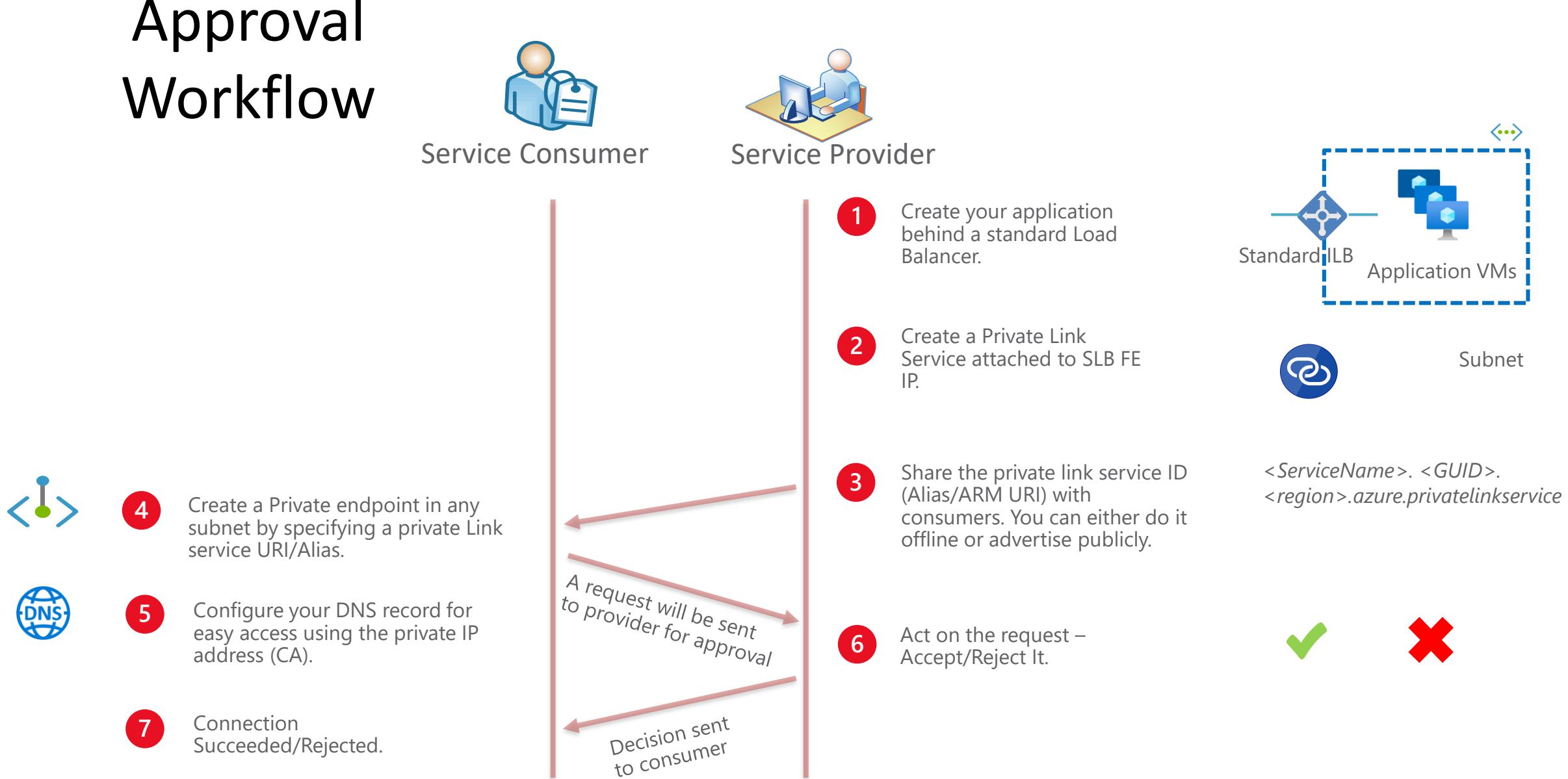


Consume Private Link Service

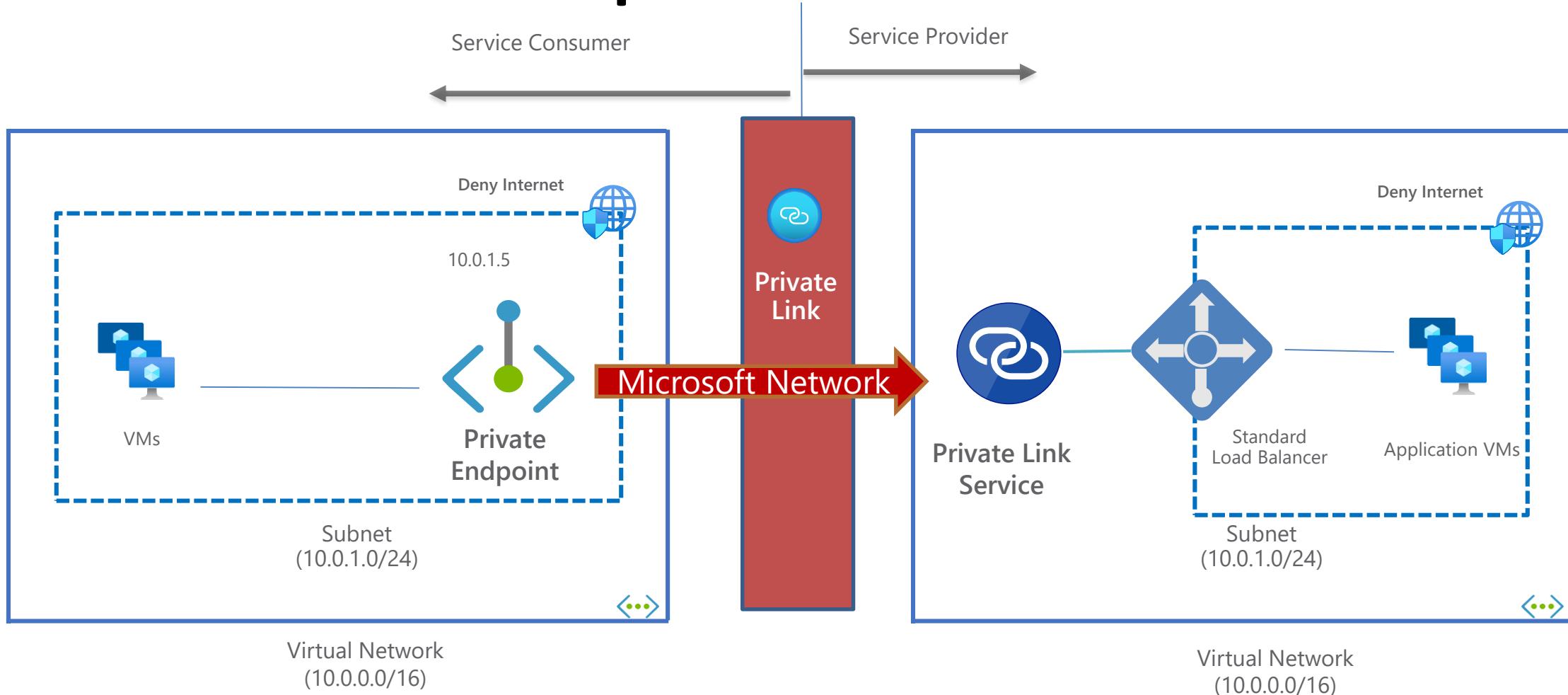
- Create a Private Endpoint in your VNet linking to Private Link Service.
- Multiple consumers can connect to same service. No RBAC restrictions.



Approval Workflow



Complete Picture





DNS for PaaS?!

What about DNS?

- Public DNS is “no longer working” when using Azure Private Endpoints!
- E.g. Storage Account:

- <https://demostordus2021.blob.core.windows.net>

```
C:\Users\EricBerg>nslookup demostordus2021.blob.core.windows.net
Server:  unifi.localdomain
Address: 192.168.1.1

Non-authoritative answer:
Name:      blob.ams07prdstr05a.store.core.windows.net
Address:   52.239.143.36
Aliases:   demostordus2021.blob.core.windows.net
```

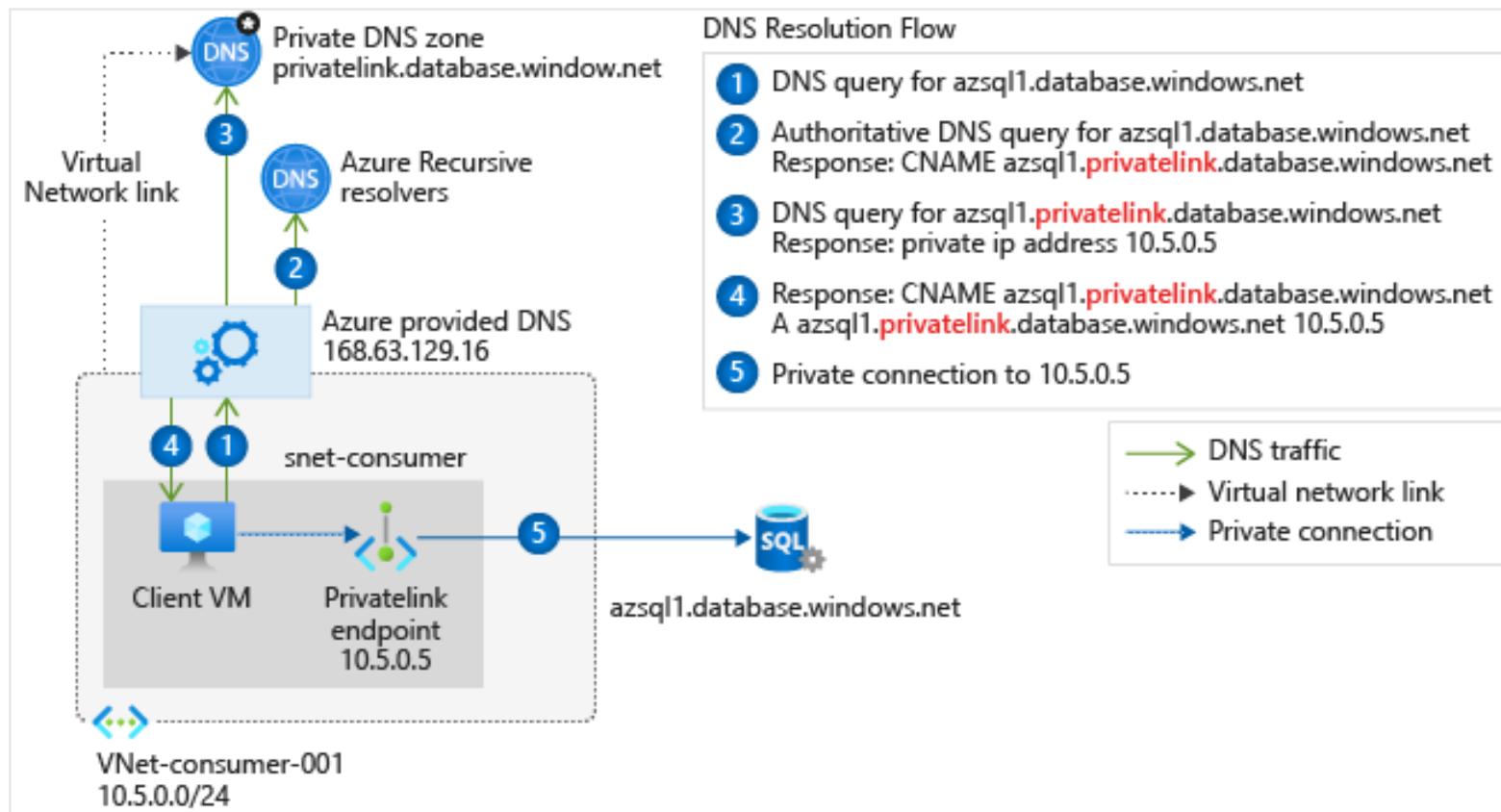
- <https://demostordus2021pep.blob.core.windows.net>

```
C:\Users\EricBerg>nslookup demostordus2021pep.blob.core.windows.net
Server:  unifi.localdomain
Address: 192.168.1.1

Non-authoritative answer:
Name:      blob.ams07prdstr02a.store.core.windows.net
Address:   20.150.37.228
Aliases:   demostordus2021pep.blob.core.windows.net
           demostordus2021pep.privatelink.blob.core.windows.net
```

Azure Private DNS

- Create Private DNS zones for your services (can be done at creation !!! ATTENTION)





DEMO – PRIVATE LINK / ENDPOINT

Azure Private DNS at Scale

- Consider Enterprise CAF Solution
 - Prepare central private DNS zones
 - Deny creation of Private DNS zones in spokes via policy
 - Create Azure Policy to “DeployIfNotExists” a DNS Zone Group to Private Endpoints
- Solution will take care of everything
- BUT
 - bound to one tenant, as policy resides in one tenant
 - Only one DNS Zone supported per policy



How things are built?



WestEurope

WestUS



RG01

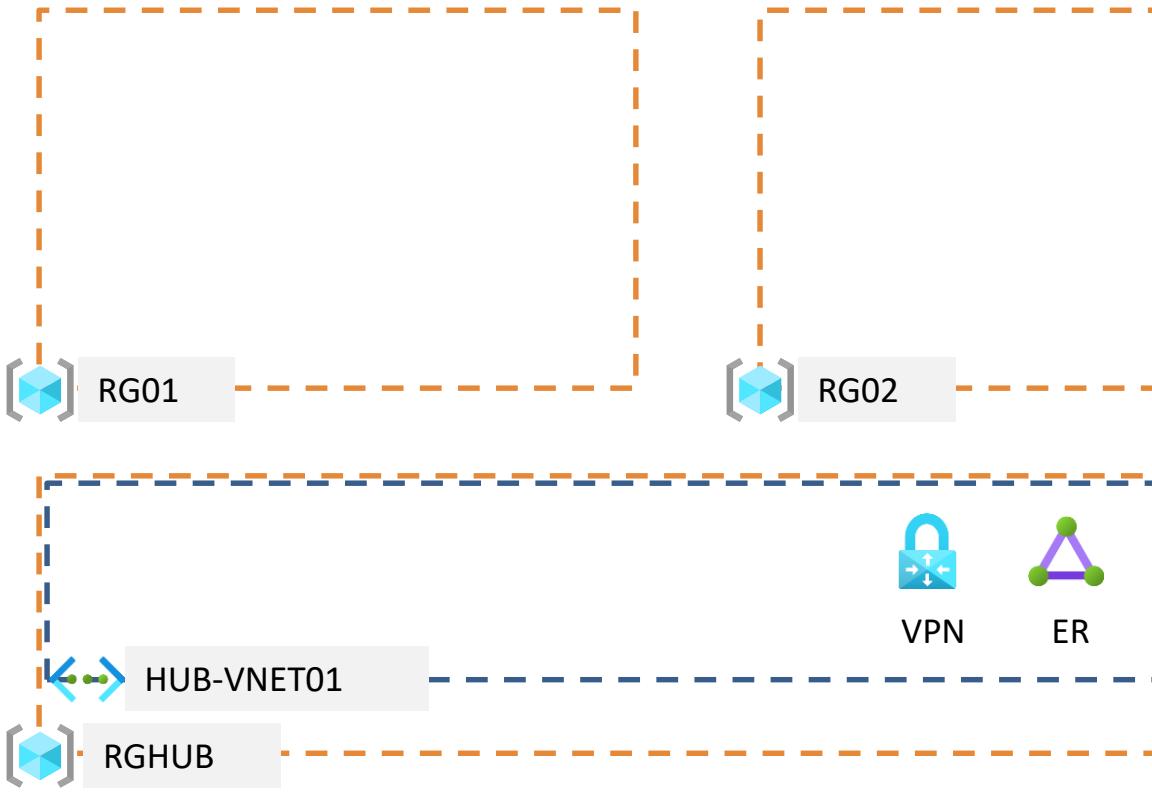
RG02

RG03

WestEurope

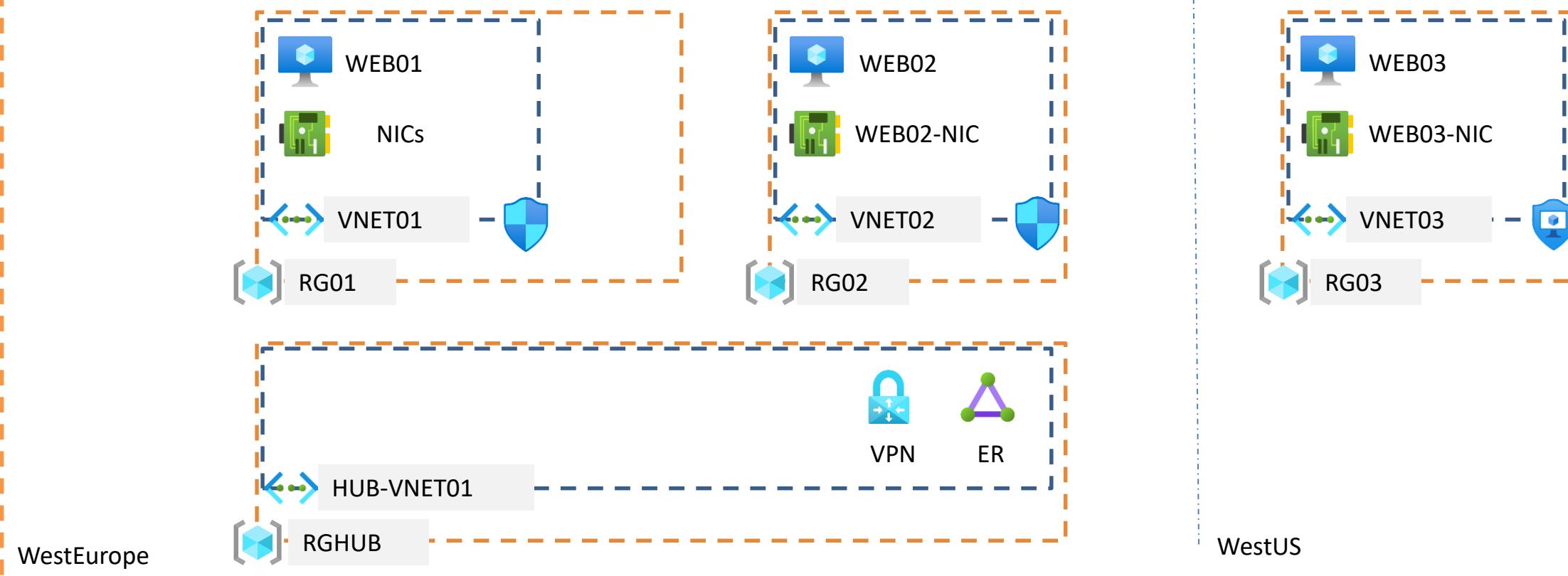
RGHUB

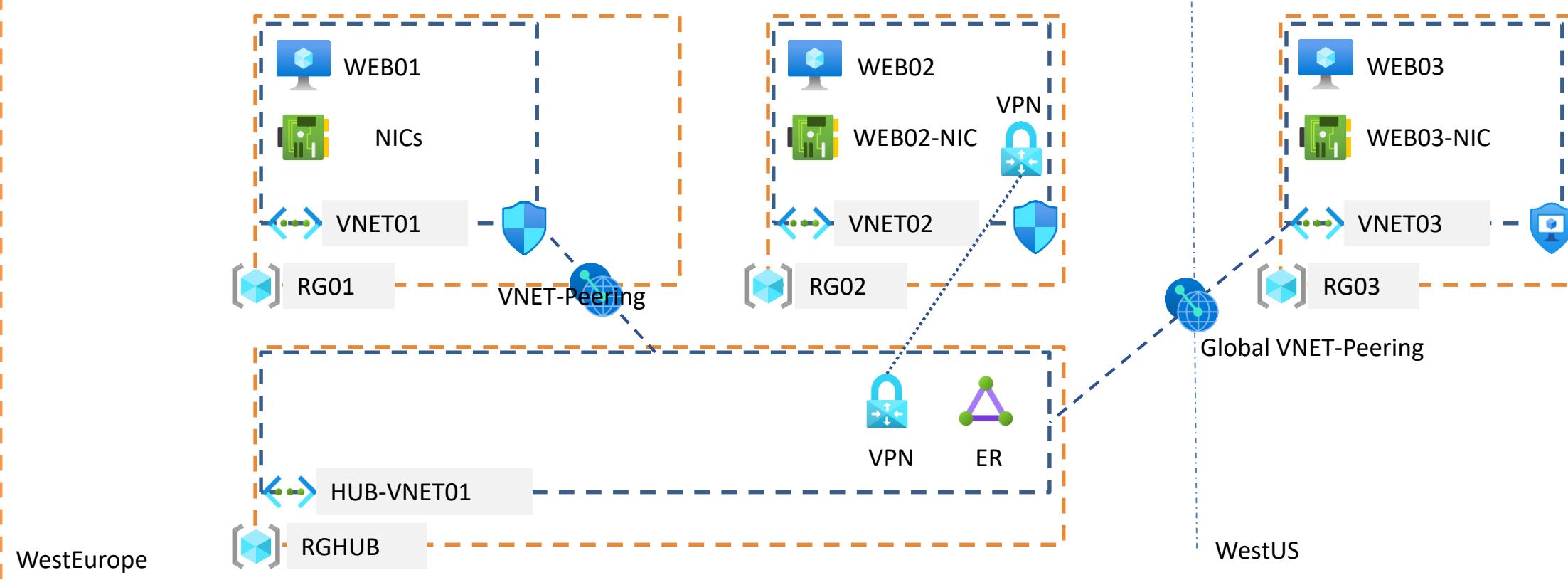
WestUS

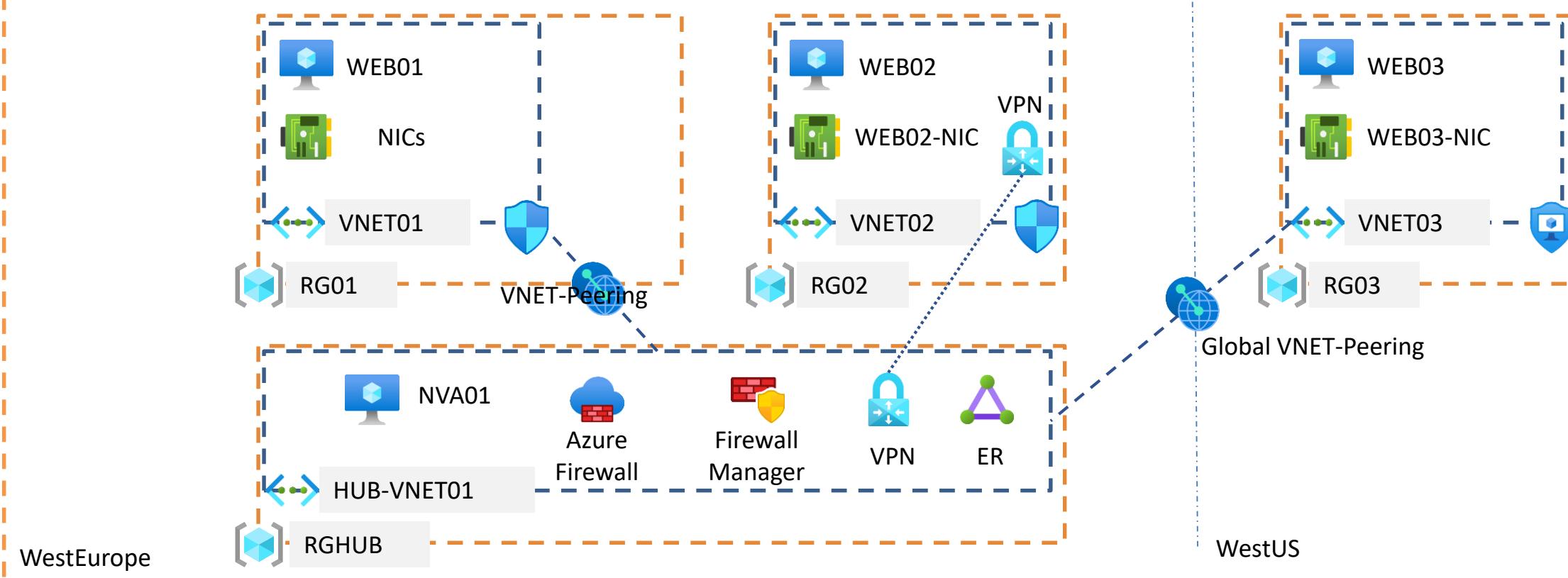


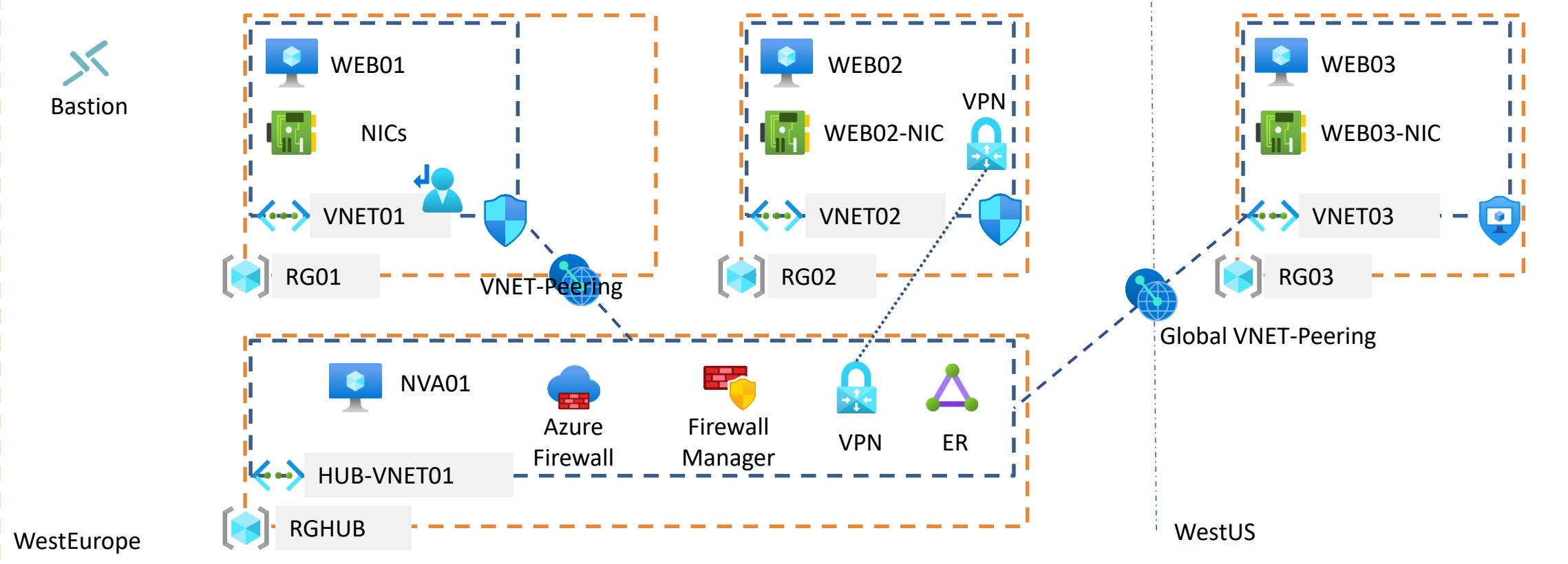
WestEurope

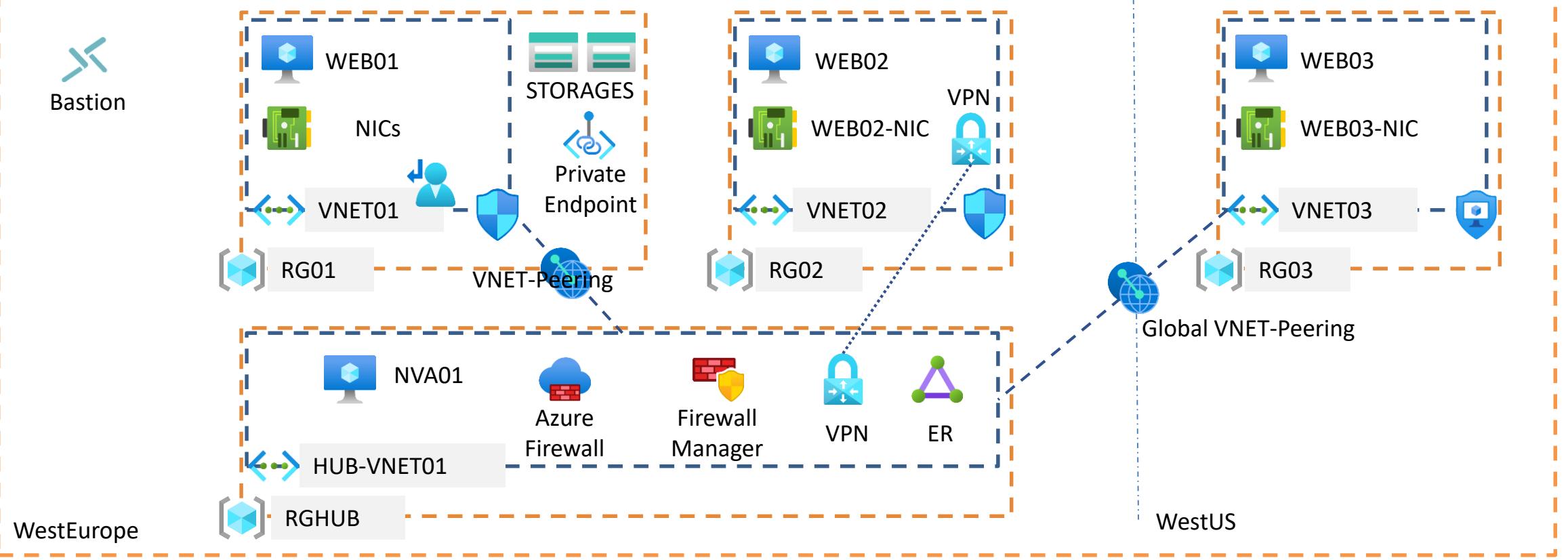
WestUS

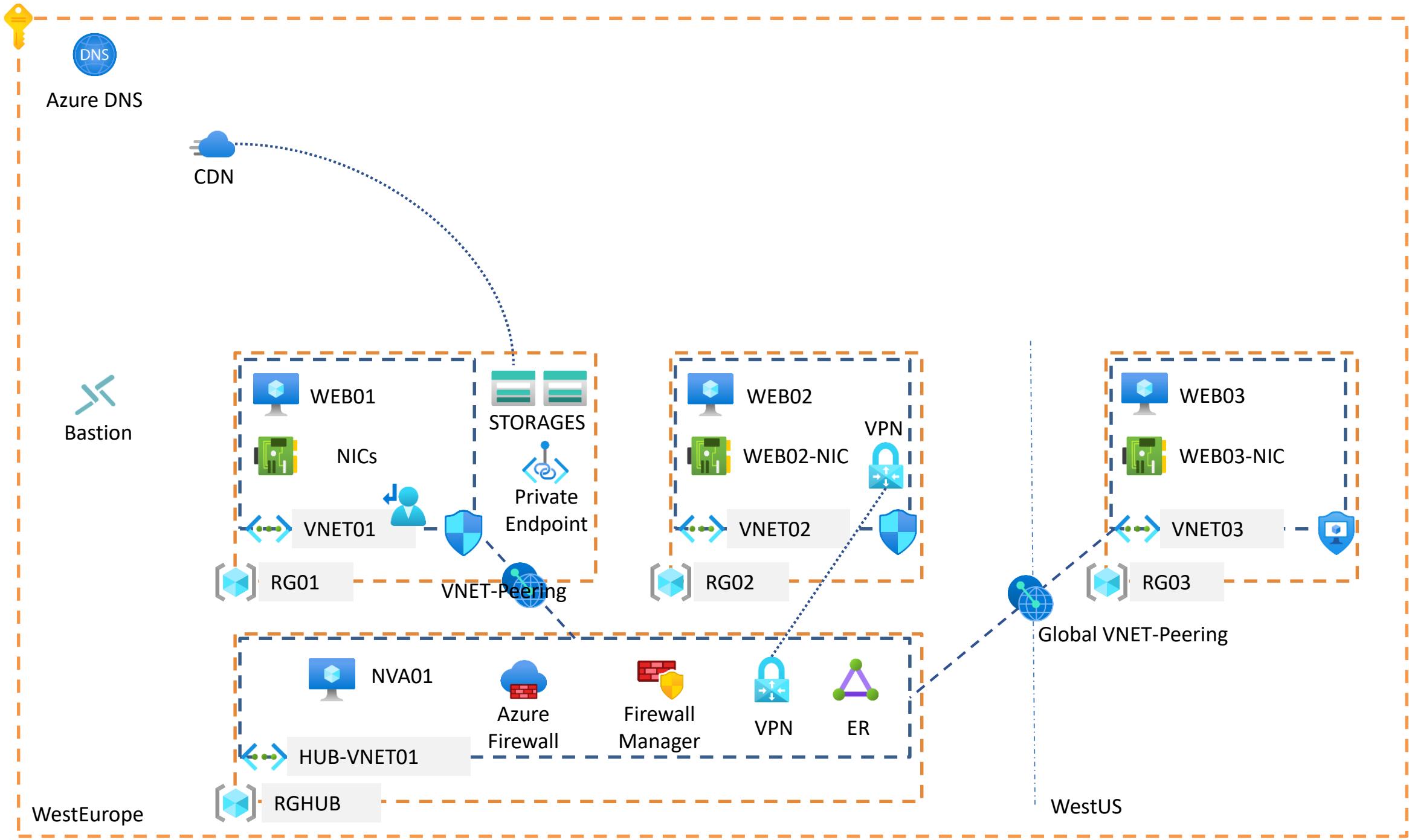


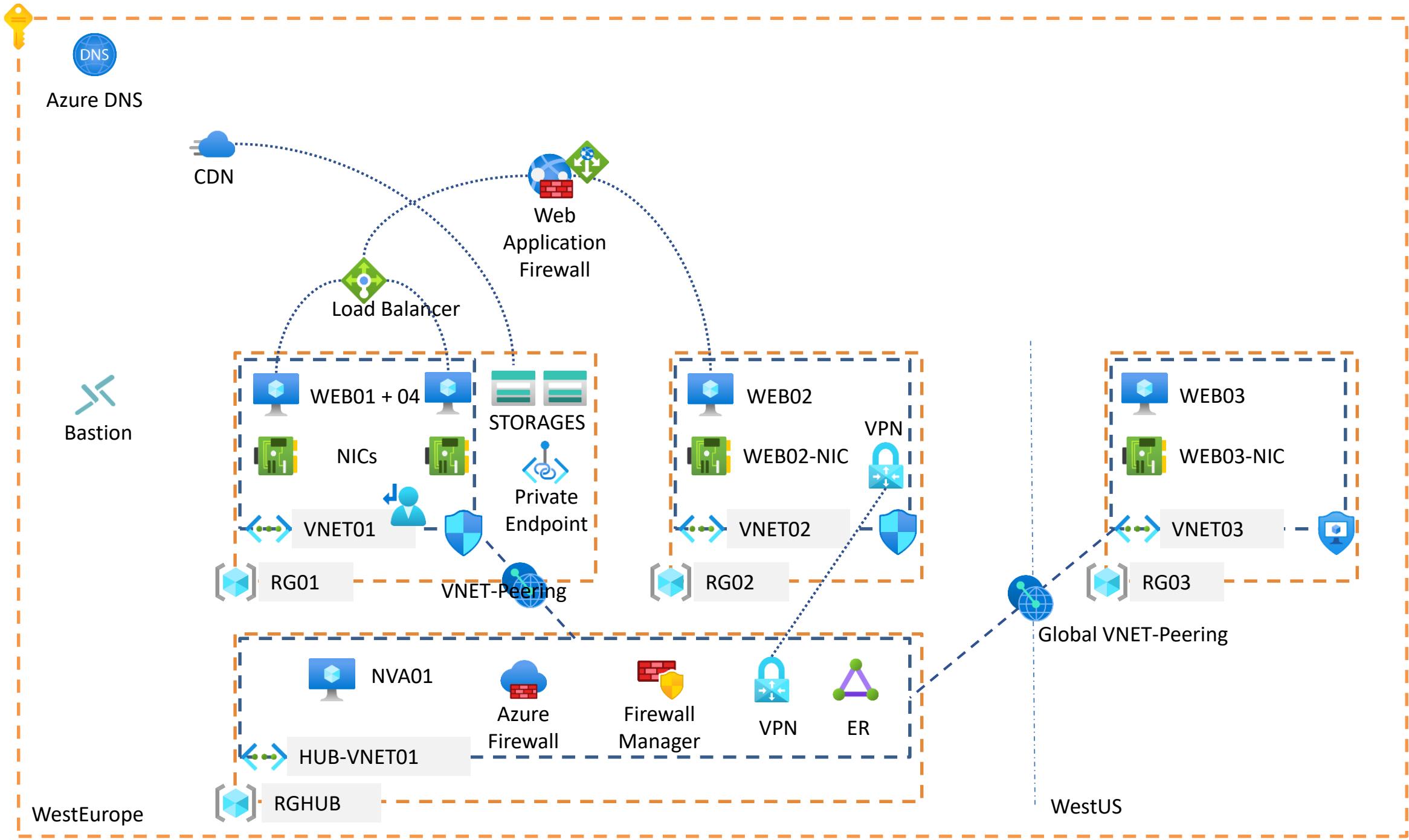


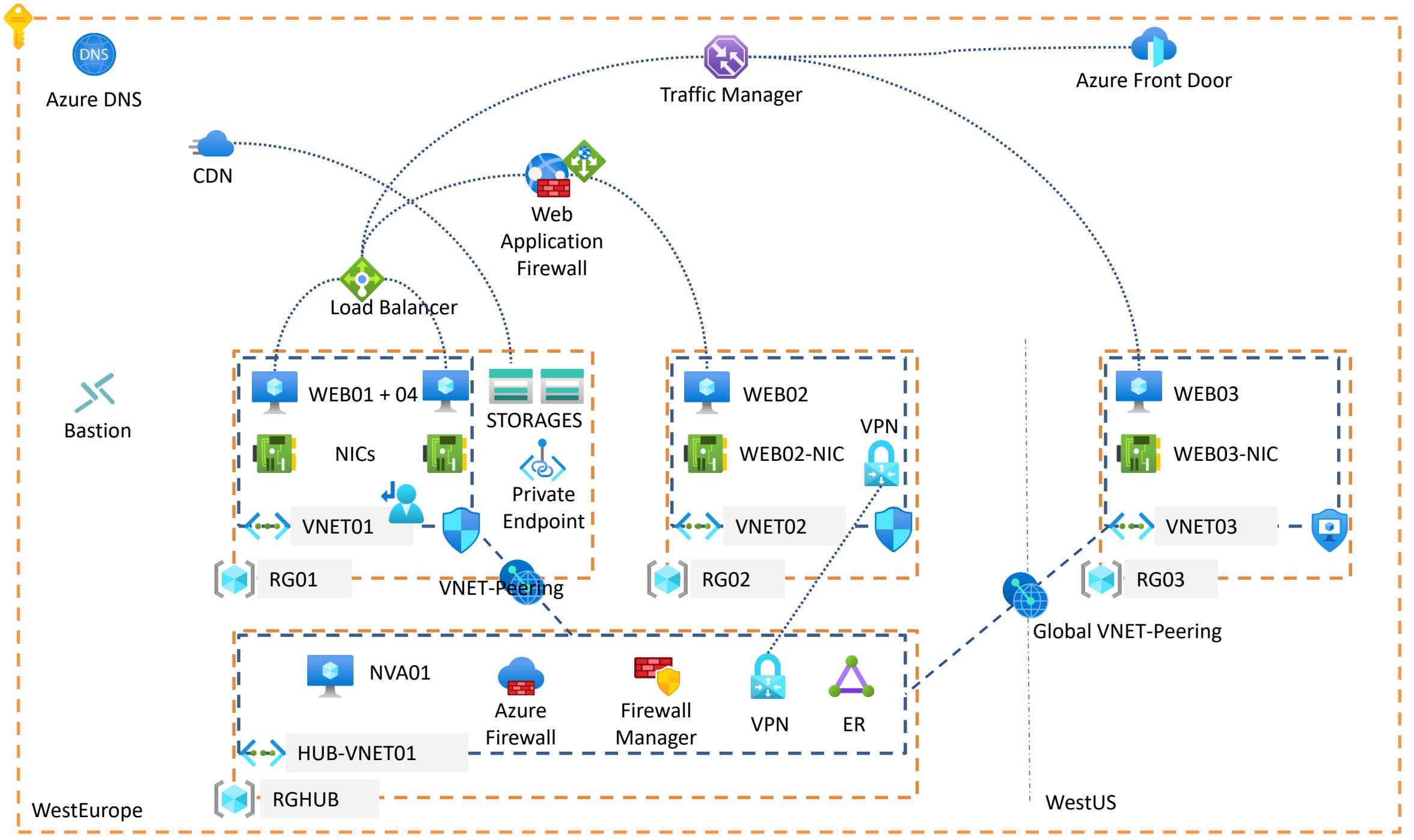


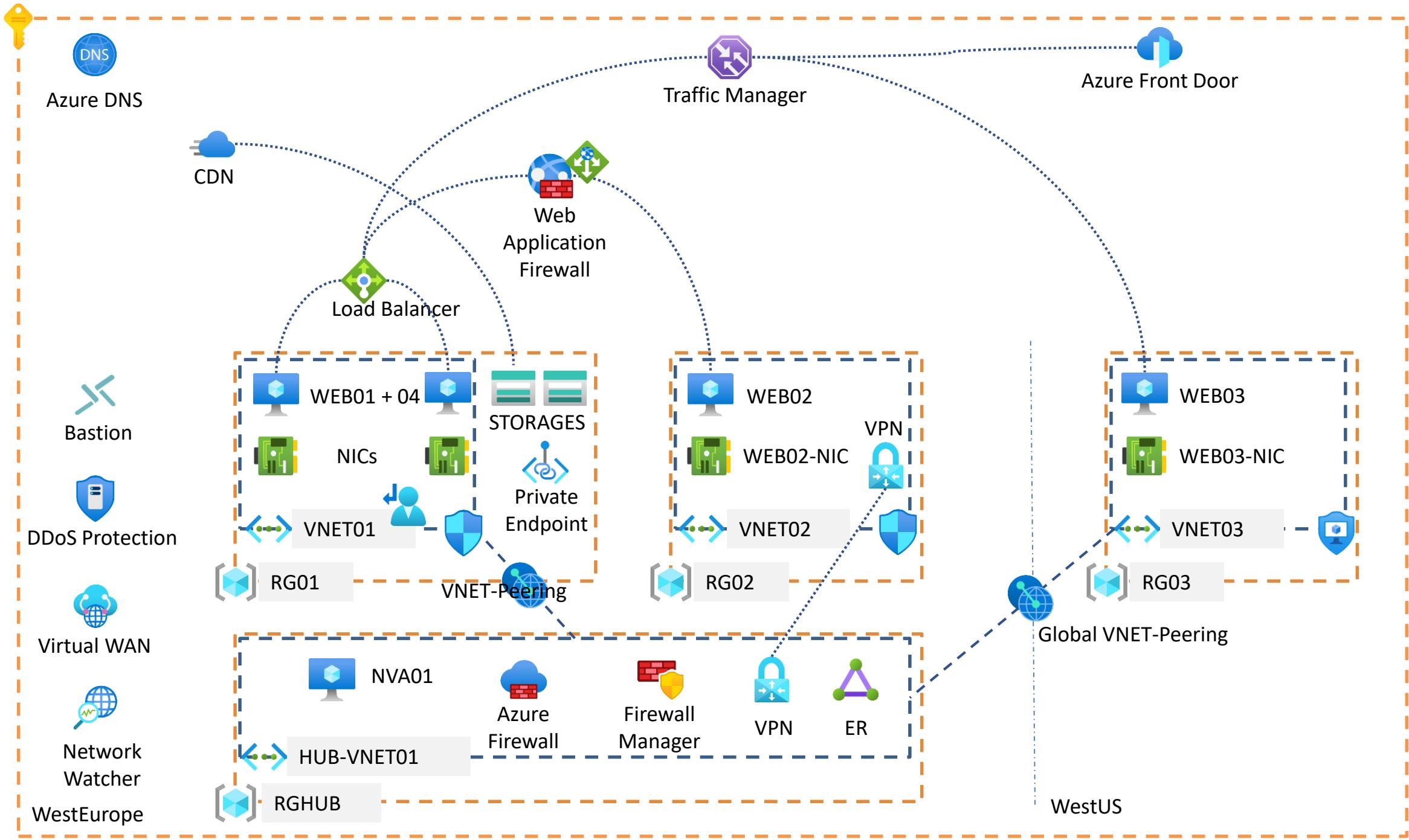


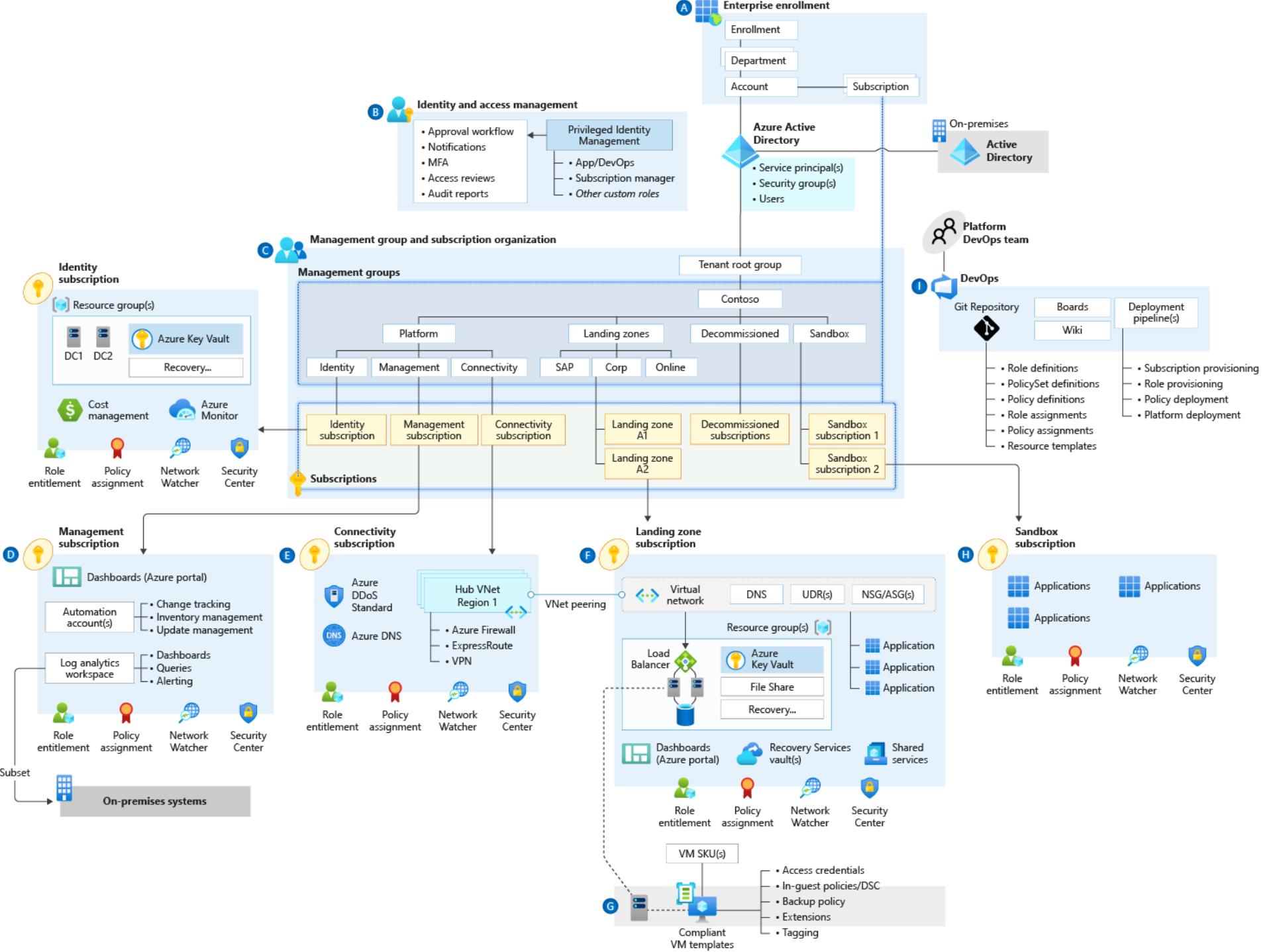














thank you

questions?



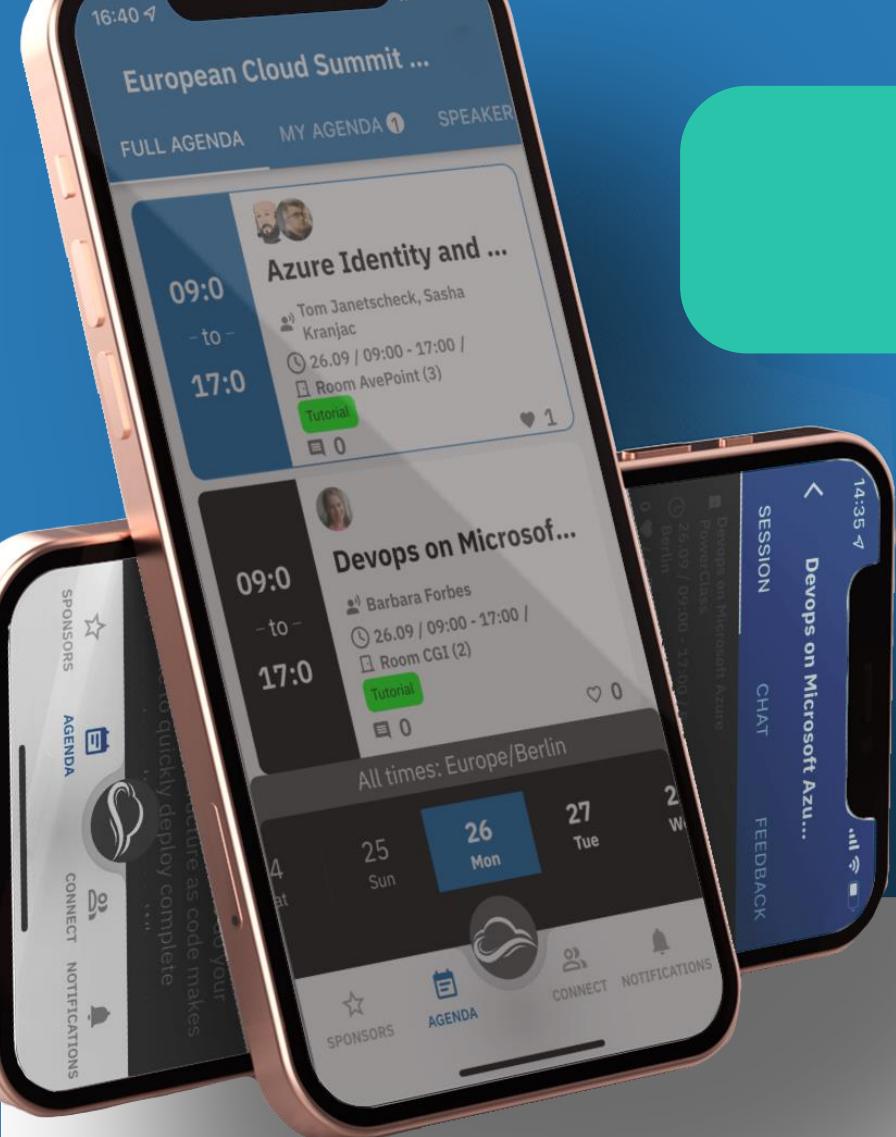
@ERICBERG_DE



WWW.ERICBERG.DE



16:40 4G



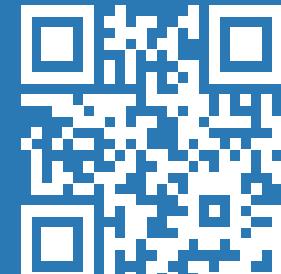
European Cloud Summit ...
FULL AGENDA MY AGENDA 1 SPEAKER
Azure Identity and ...
09:0 - to - 17:0
Tom Janetscheck, Sasha Kranjac
26.09 / 09:00 - 17:00 / Room AvePoint (3)
Tutorial 1
Devops on Microsoft...
09:0 - to - 17:0
Barbara Forbes
26.09 / 09:00 - 17:00 / Room CGI (2)
Tutorial 0
All times: Europe/Berlin
25 Sun 26 Mon 27 Tue 28 Wed
SPONSORS AGENDA CONNECT NOTIFICATIONS
SPEAKERS AND SESSIONS
SESSION FEEDBACK BUSINESS NETWORKING AGENDA SPEAKERS AND SESSIONS
Did you know? You can use the app to scan other attendees' badges, and they will become your connections!
<https://csmmt.eu/app>

USE CLOUDSUMMIT APP!

SESSION FEEDBACK BUSINESS NETWORKING AGENDA SPEAKERS AND SESSIONS

DID YOU KNOW?

YOU CAN USE THE APP TO SCAN OTHER ATTENDEES' BADGES, AND THEY WILL BECOME YOUR CONNECTIONS!


<https://csmmt.eu/app>