- Azure Networking vNext -
How to build modern connectivity for IaaS, PaaS and SaaS

Eric Berg – Microsoft MVP
Vice President @ CGI

AZURE
BOOTCAMP SWITZERLAND

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

Experts Live Germany

MOUNTAIN IT
www.ericberg.de

MVP Microsoft® Most Valuable Professional

GEEKZEUGS HOME OF
GEEKSPRECH Podcast
GEEKSCHAU Webcast
GEEKTREFF Community

Azure Meetup THÜRINGEN

AZURE BOOTCAMP SWITZERLAND

Agenda

Networking Overview

Networking Recap

Connectivity

Integration

DNS

Build it

Q&A

Networking Overview

AZURE
BOOTCAMP SWITZERLAND

High Level Azure Services

Management

- Azure Monitor
- Log Analytics
- Azure Policy
- Azure Blueprints
- Azure Backup
- Site Recovery
- Azure Migrate
- Databox Family
- Cost Management

Platform as a Services (PaaS)

Compute/Containers

- Functions
- Kubernetes Service
- Container Instance
- Service Fabric

Web/Mobile

- Web Apps
- Logic Apps
- API Apps
- Mobile Apps
- Notification Hubs
- SignalR Service

DevOps/Developer

- Azure DevOps
- Lab Services
- Application Insights
- SDK

Integration

- API Management
- Logic Apps
- Service Bus
- Event Grid

Media/CDN

- Media Services
- Content Protection
- Video Indexer
- Content Delivery Network

IoT

- IoT Hub
- IoT Central
- Time Series Insights
- Azure Digital Twins
- IoT Edge

AI

- Cognitive Services
- Machine Learning Studio
- Machine Learning Service
- Bot Services
- Azure Search

Analytics

- SQL Data Warehouse
- Azure Databricks
- Apache Spark
- Stream Analytics
- Data Lake Storage Gen2

Data Services

- SQL Database
- SQL Data Warehouse
- Database for MySQL
- Cosmos DB
- Database for PostgreSQL
- Data Factory
- Database for MariaDB
- Azure Cache for Redis
- Database Migration Service
- Table Storage

Security

- Security Center
- Azure AD
- Azure AD for Domain Services
- Azure AD B2C
- DDoS Protection
- Key Vault
- Multi-Factor Authentication
- Azure ATP
- Role- based access control

Infrastructure as a Services (IaaS)

Compute

- Virtual Machine Scale Sets
- Linux Virtual Machine

Storage

- Disk Storage
- Managed Disks

Networking

- Virtual Network
- VPN Gateway
- Express Route
- Load Balancer
- Azure Firewall
- Virtual WAN
- Network Watcher

Azure Datacenter Infrastructure

60+ Azure regions

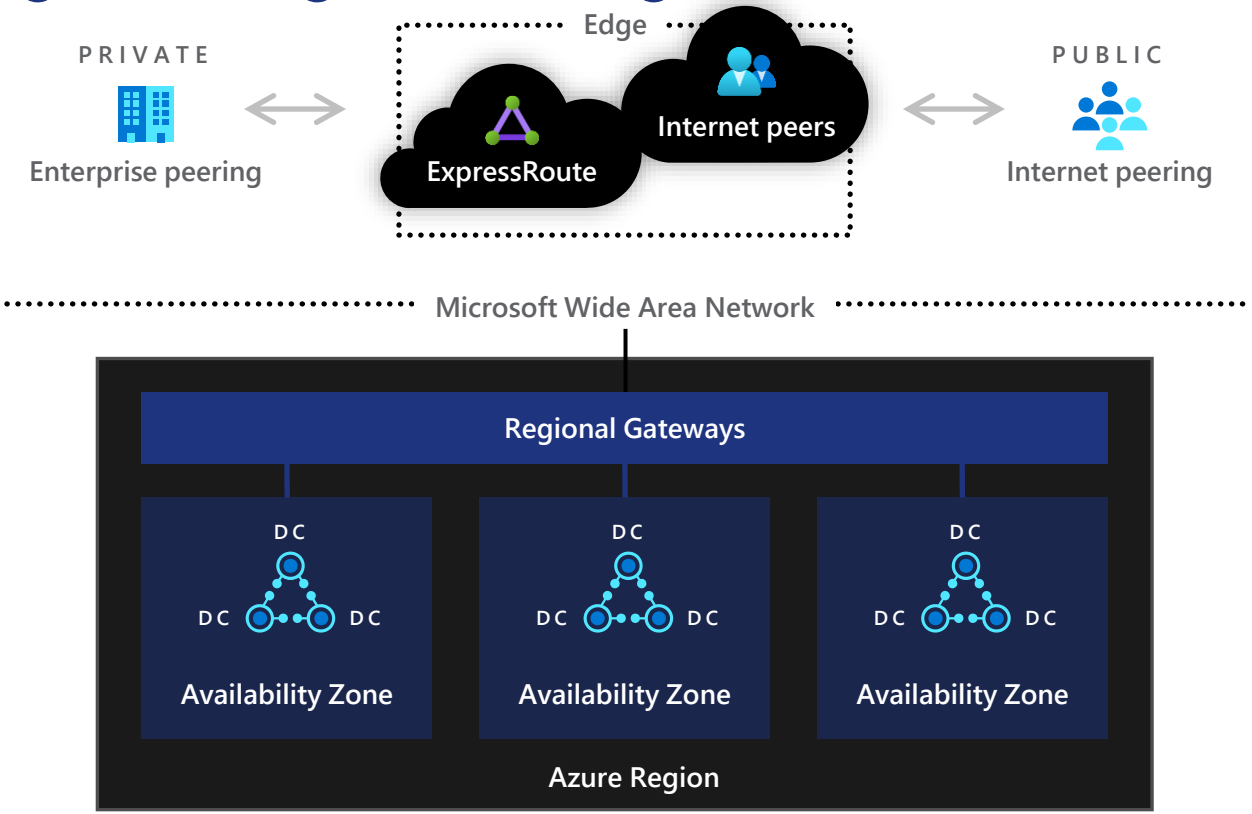
165k+ miles of fiber + subsea cables

185+ edge sites

500+ network partners

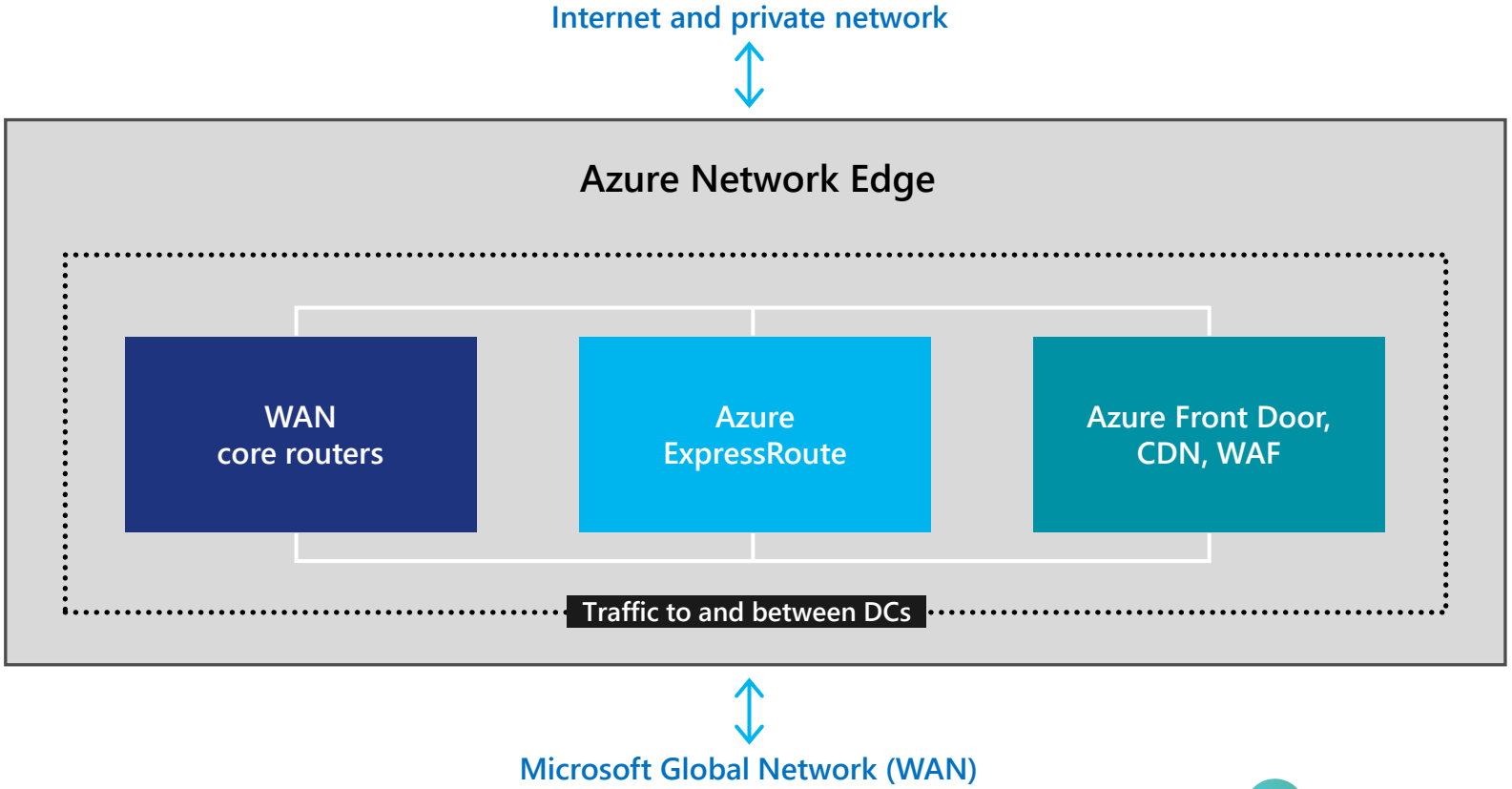
20k+ peering connections

Connecting Azure regions to the global network



AZURE
BOOTCAMP SWITZERLAND

The Azure Network Edge



AZURE
BOOTCAMP SWITZERLAND

Networking Recap

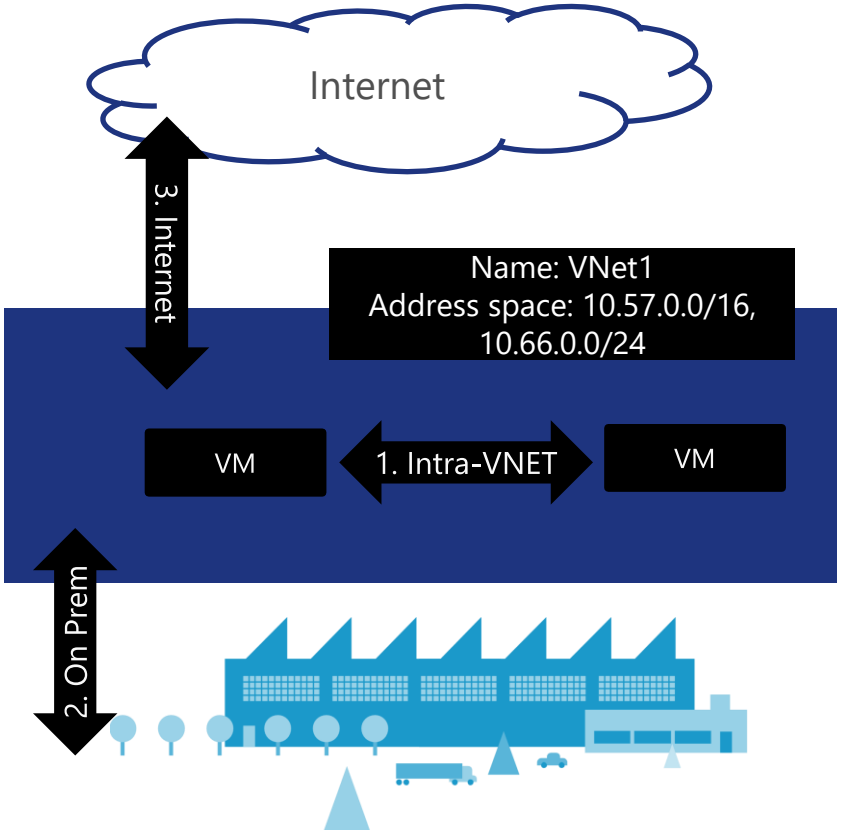
AZURE
BOOTCAMP SWITZERLAND

Virtual Network

Isolated, logical network that provides connectivity for Azure Resources

User-defined address space (can be one or more IP ranges, not necessarily RFC1918)

- Connectivity for VMs in the same VNET
- Connectivity to external networks/on-prem DC's
- Internet connectivity

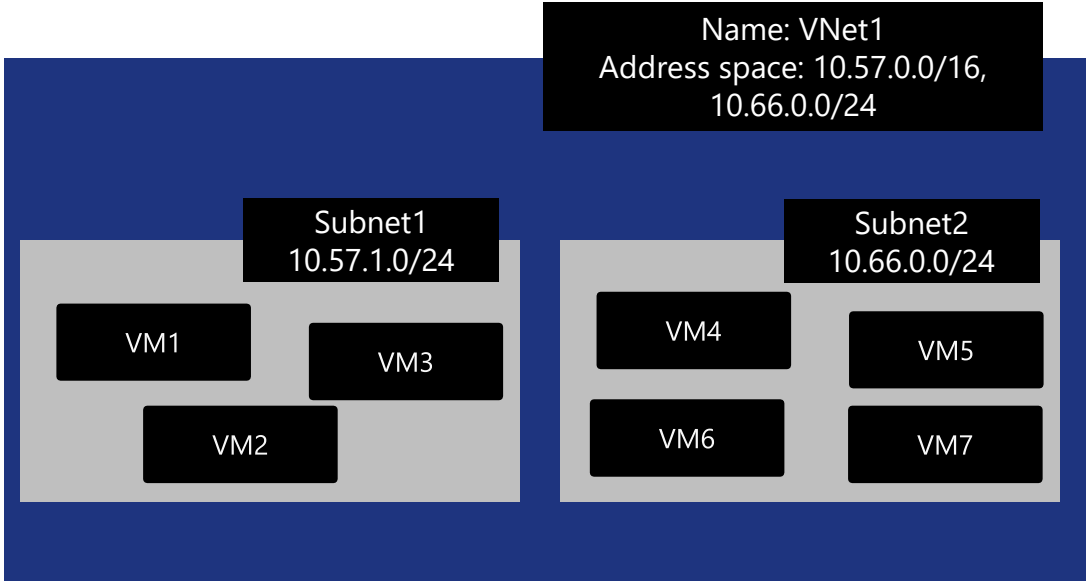


Subnet

Provides full layer-3 semantics and partial layer-2 semantics (DHCP, ARP, no broadcast / multicast)

Subnets can span only one range of contigous IP addresses

VMs can be deployed only to subnets (not VNETs)

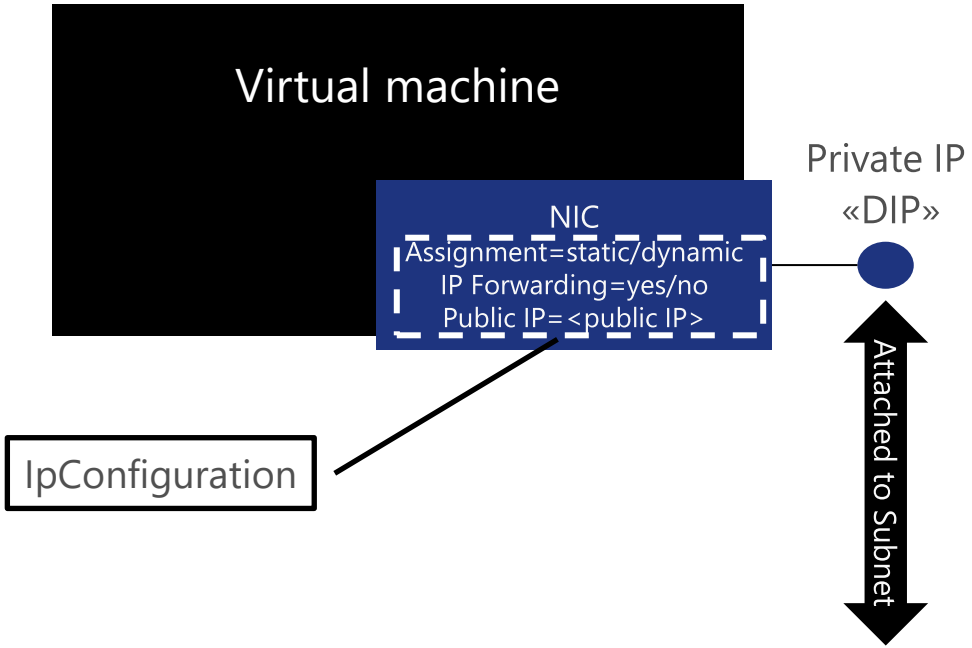


Network Interface

Virtual NIC that connects a VM to a Subnet

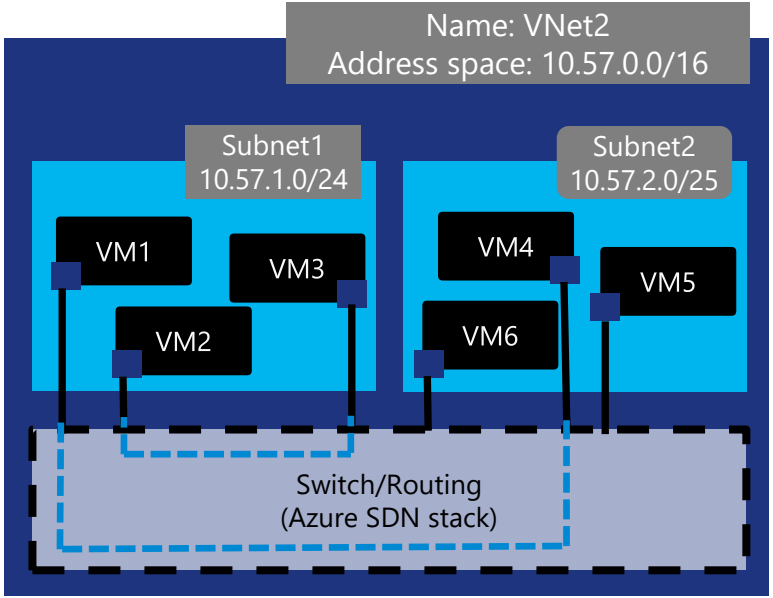
One private IP address (private == included in the subnet's IP range, not necessarily RFC1918)

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

AZURE
BOOTCAMP SWITZERLAND

Connectivity

AZURE
BOOTCAMP SWITZERLAND

Connecting *to* Azure

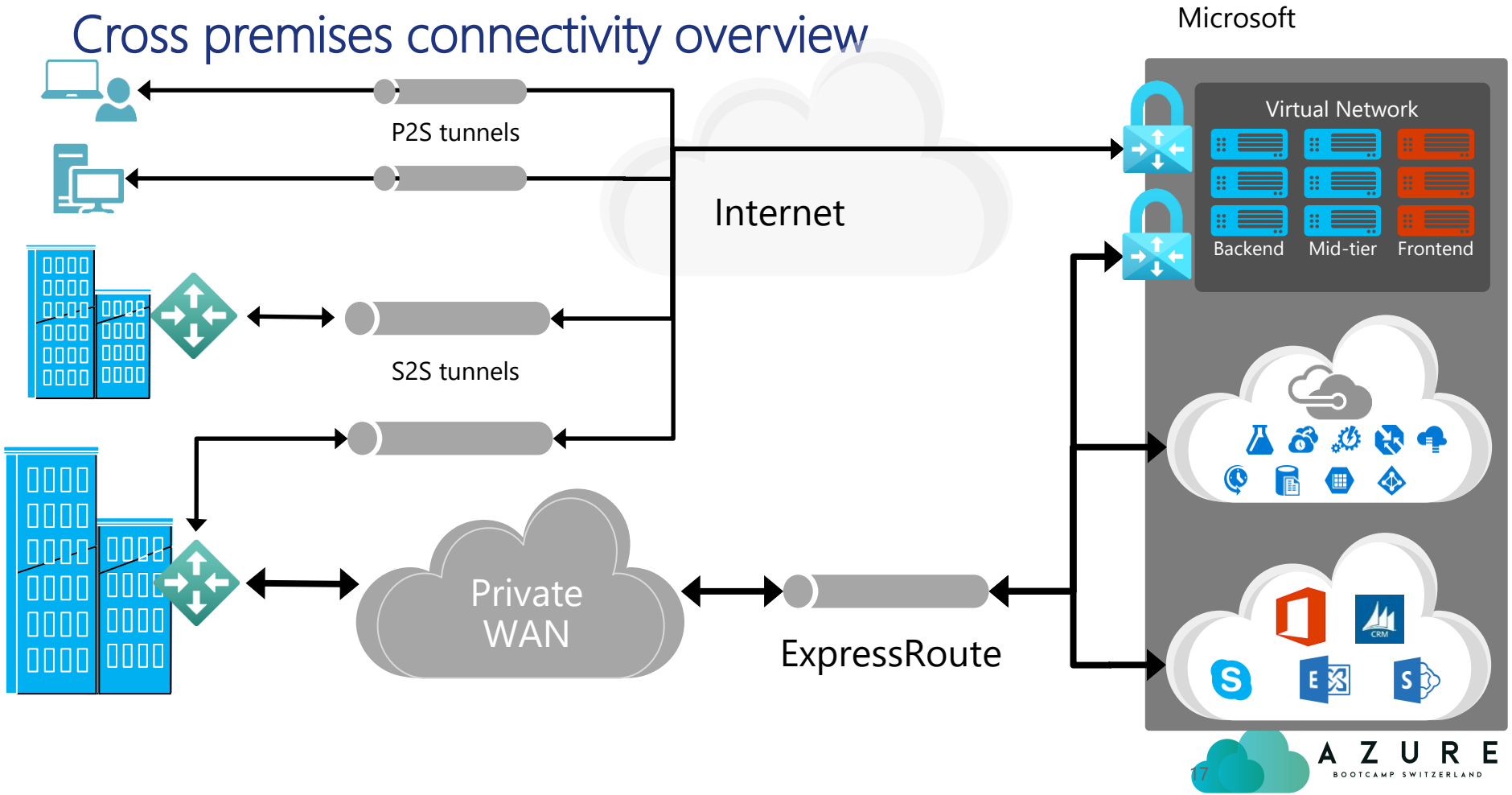
Cloud		Customer	Characteristics
	Internet Connectivity		• Internet facing with public IP addresses in Azure • VPN connectivity with virtual appliances (Marketplace)
	Remote access point-to-site connectivity		• Remote Access to VNet/On-prem • Connect from anywhere • Mac, Linux, Windows • Radius/AD authentication
	Site-to-site VPN connectivity		• High throughput, secure cross-premises connectivity • BGP, active-active for high availability & transit routing
	ExpressRoute private connectivity		• Private connectivity to Microsoft services • Mission critical workloads

AZURE
BOOTCAMP SWITZERLAND

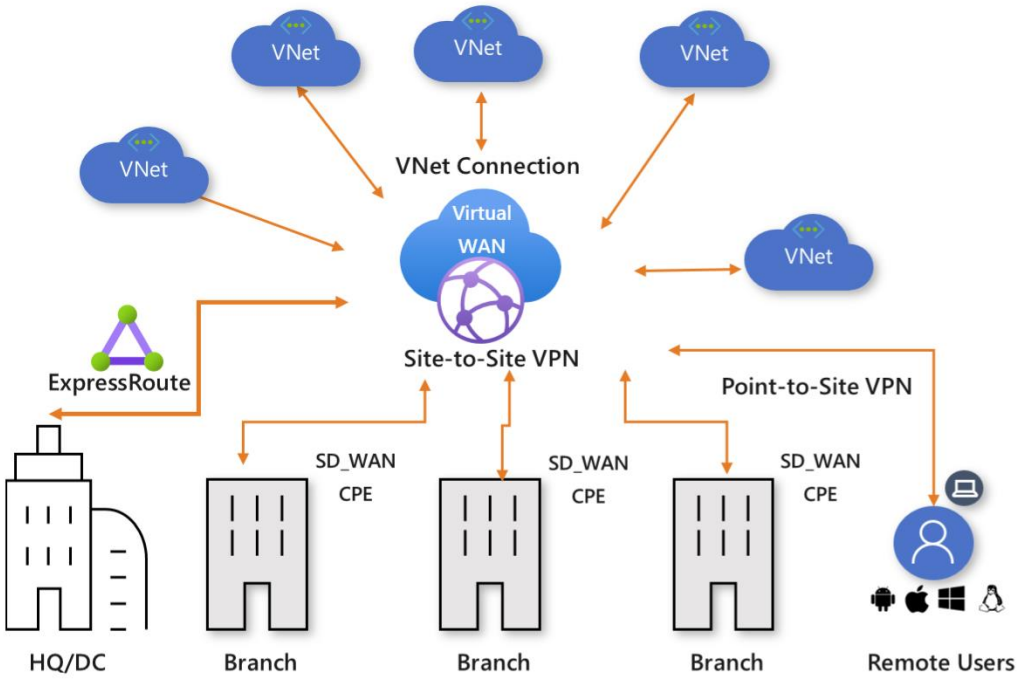
Connecting *in* Azure

Cloud		Cloud	Characteristics
	VNet Peering		• Same-/cross-region direct, private VM-to-VM connectivity • NSG & UDR across VNets • GatewayTransit for hub-and-spoke
	VNet-to-VNet via Gateways		• Transitive routing via BGP and VPN gateways • Secure connectivity via IPsec/IKE across Azure WAN links
	VNet-to-VNet via ExpressRoute circuit		• Traverse (“hairpin”) through ExpressRoute circuit & gateways • Traffic is not encrypted

Cross premises connectivity overview

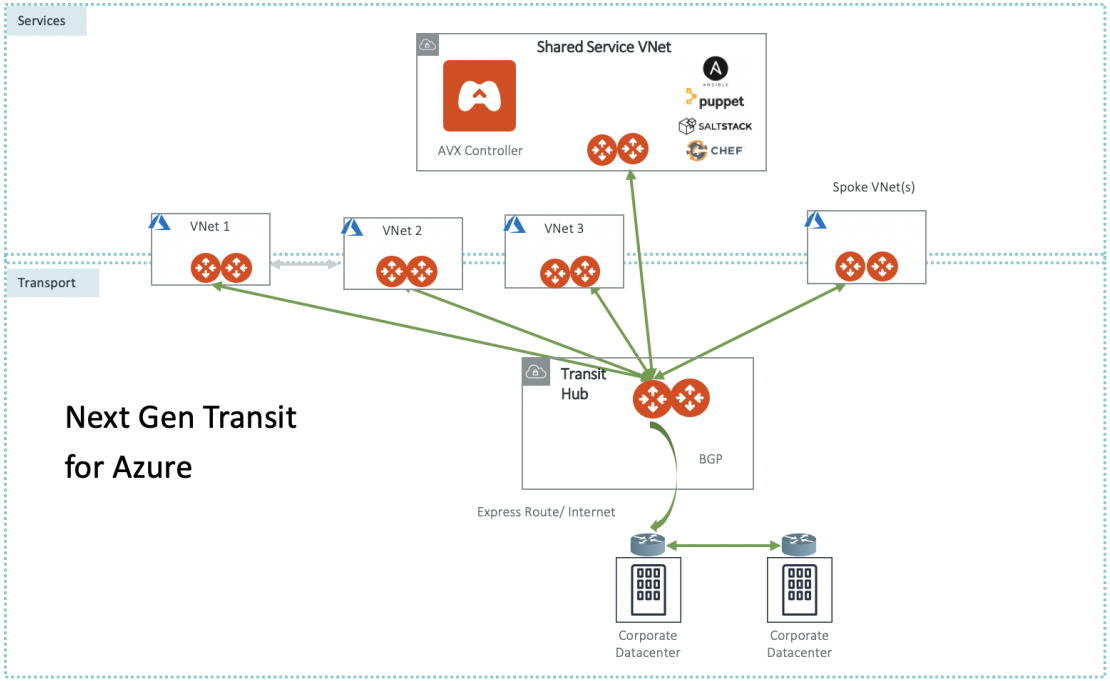


Azure Virtual WAN



AZURE
BOOTCAMP SWITZERLAND

NextGen Cloud Networking



AZURE
BOOTCAMP SWITZERLAND

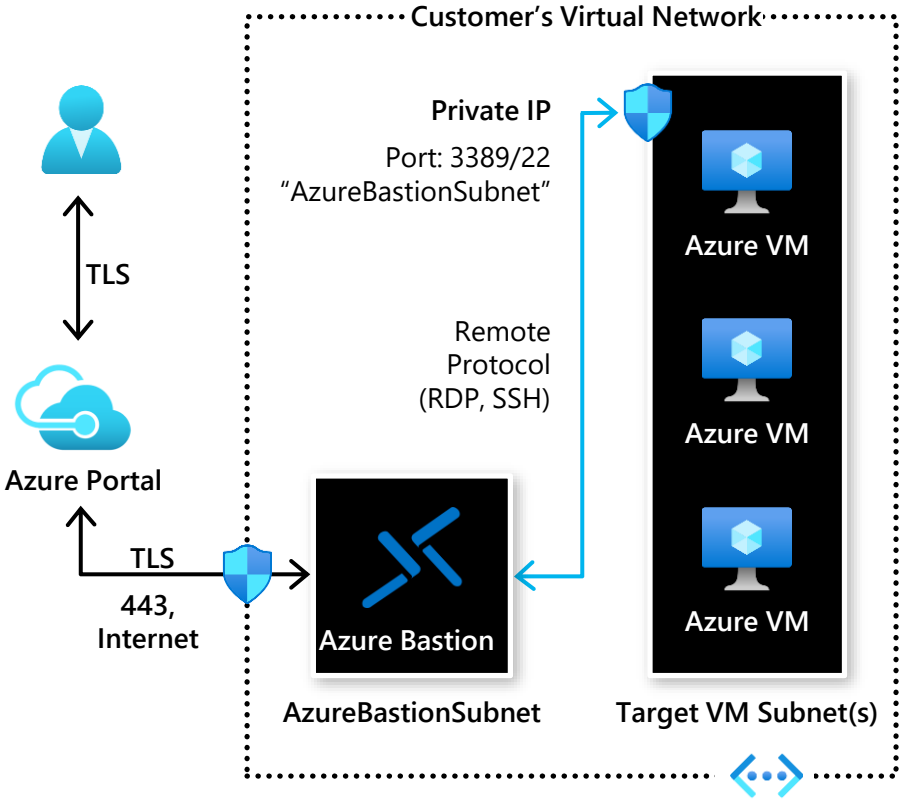
Azure Bastion

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

Management

- Azure Monitor
- Log Analytics
- Azure Policy
- Azure Blueprints
- Azure Backup
- Site Recovery
- Azure Migrate
- Databox Family
- Cost Management

Platform as a Services (PaaS)

Compute/Containers

- Functions
- Kubernetes Service
- Container Instance
- Service Fabric

Web/Mobile

- Web Apps
- Logic Apps
- API Apps
- Mobile Apps
- Notification Hubs
- SignalR Service

DevOps/Developer

- Azure DevOps
- Lab Services
- Application Insights
- SDK

Integration

- API Management
- Logic Apps
- Service Bus
- Event Grid

Media/CDN

- Media Services
- Content Protection
- Video Indexer
- Content Delivery Network

IoT

- IoT Hub
- IoT Central
- Time Series Insights
- Azure Digital Twins
- IoT Edge

AI

- Cognitive Services
- Machine Learning Studio
- Machine Learning Service
- Bot Services
- Azure Search

Analytics

- SQL Data Warehouse
- Azure Databricks
- Apache Spark
- Stream Analytics
- Data Lake Storage Gen2

Data Services

- SQL Database
- SQL Data Warehouse
- Database for MySQL
- Cosmos DB
- Database for PostgreSQL
- Data Factory
- Database for MariaDB
- Azure Cache for Redis
- Database Migration Service
- Table Storage

Security

- Security Center
- Azure AD
- Azure AD for Domain Services
- Azure AD B2C
- DDoS Protection
- Key Vault
- Multi-Factor Authentication
- Azure ATP
- Role- based access control

Infrastructure as a Services (IaaS)

Compute

- Virtual Machine Scale Sets
- Linux Virtual Machine

Storage

- Disk Storage
- Managed Disks

Networking

- Virtual Network
- VPN Gateway
- Express Route
- Load Balancer
- Azure Firewall
- Virtual WAN
- Network Watcher

Azure Datacenter Infrastructure

High Level Azure Services

Management

- Azure Monitor
- Log Analytics
- Azure Policy
- Azure Blueprints
- Azure Backup
- Site Recovery
- Azure Migrate
- Databox Family
- Cost Management

Platform as a Services (PaaS)

Compute/Containers

- Functions
- Kubernetes Service
- Container Instance
- Service Fabric

Web/Mobile

- Web Apps
- Logic Apps
- API Apps
- Mobile Apps
- Notification Hubs
- SignalR Service

DevOps/Developer

- Azure DevOps
- Lab Services
- Application Insights
- SDK

Integration

- API Management
- Logic Apps
- Service Bus
- Event Grid

Media/CDN

- Media Services
- Content Protection
- Video Indexer
- Content Delivery Network

IoT

- IoT Hub
- IoT Central
- Time Series Insights
- Azure Digital Twins
- IoT Edge

AI

- Cognitive Services
- Machine Learning Studio
- Machine Learning Service
- Bot Services
- Azure Search

Analytics

- SQL Data Warehouse
- Azure Databricks
- Apache Spark
- Stream Analytics
- Data Lake Storage Gen2

Data Services

- SQL Database
- SQL Data Warehouse
- Database for MySQL
- Cosmos DB
- Database for PostgreSQL
- Data Factory
- Database for MariaDB
- Azure Cache for Redis
- Database Migration Service
- Table Storage

Security

- Security Center
- Azure AD
- Azure AD for Domain Services
- Azure AD B2C
- DDoS Protection
- Key Vault
- Multi-Factor Authentication
- Azure ATP
- Role- based access control

Infrastructure as a Services (IaaS)

Compute

- Virtual Machine Scale Sets
- Linux Virtual Machine

Storage

- Disk Storage
- Managed Disks

Networking

- Virtual Network
- VPN Gateway
- Express Route
- Load Balancer
- Azure Firewall
- Virtual WAN
- Network Watcher

Azure Datacenter Infrastructure

High Level Azure Services

Management

- Azure Monitor
- Log Analytics
- Azure Policy
- Azure Blueprints
- Azure Backup
- Site Recovery
- Azure Migrate
- Databox Family
- Cost Management

Platform as a Services (PaaS)

Compute/Containers

- Functions
- Kubernetes Service
- Container Instance
- Service Fabric

Web/Mobile

- Web Apps
- Logic Apps
- API Apps
- Mobile Apps
- Notification Hubs
- SignalR Service

DevOps/Developer

- Azure DevOps
- Lab Services
- Application Insights
- SDK

Integration

- API Management
- Logic Apps
- Service Bus
- Event Grid

Media/CDN

- Media Services
- Content Protection
- Video Indexer
- Content Delivery Network

IoT

- IoT Hub
- IoT Central
- Time Series Insights
- Azure Digital Twins
- IoT Edge

AI

- Cognitive Services
- Machine Learning Studio
- Machine Learning Service
- Bot Services
- Azure Search

Analytics

- SQL Data Warehouse
- Azure Databricks
- Apache Spark
- Stream Analytics
- Data Lake Storage Gen2

Data Services

- SQL Database
- SQL Data Warehouse
- Database for MySQL
- Cosmos DB
- Database for PostgreSQL
- Data Factory
- Database for MariaDB
- Azure Cache for Redis
- Database Migration Service
- Table Storage

Security

- Security Center
- Azure AD
- Azure AD for Domain Services
- Azure AD B2C
- DDoS Protection
- Key Vault
- Multi-Factor Authentication
- Azure ATP
- Role- based access control

Infrastructure as a Services (IaaS)

Compute

- Virtual Machine Scale Sets
- Linux Virtual Machine

Storage

- Disk Storage
- Managed Disks

Networking

- Virtual Network
- VPN Gateway
- Express Route
- Load Balancer
- Azure Firewall
- Virtual WAN
- Network Watcher

Azure Datacenter Infrastructure

Azure Load Balancer

AZURE
BOOTCAMP SWITZERLAND

Azure Load Balancer

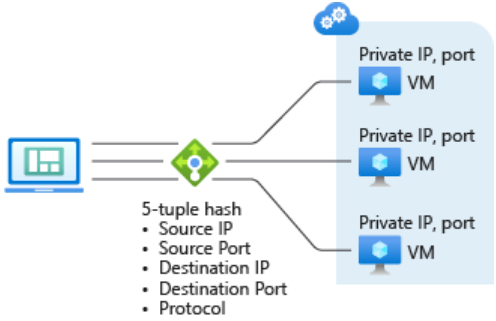
Allows you to scale your applications and create **high availability** and **resiliency** for your services and applications

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.



AZURE
BOOTCAMP SWITZERLAND

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

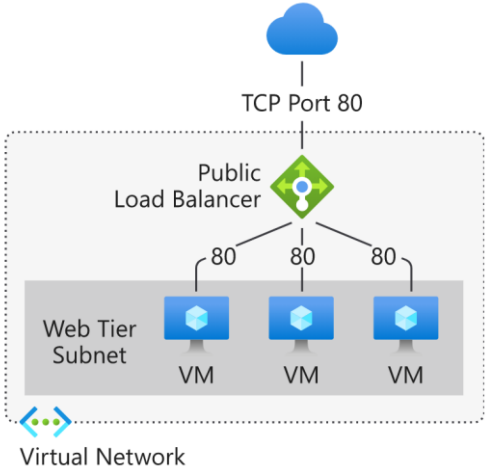
- Instantly reconfigures itself as you scale instance up or down

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



AZURE
BOOTCAMP SWITZERLAND

Internal Load Balancer

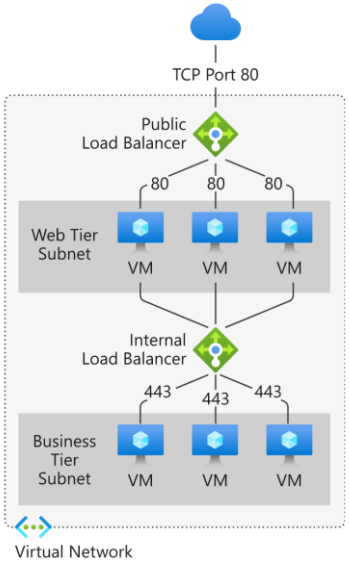
An internal Load Balancer directs traffic only to resources inside a virtual network or that use a VPN to access Azure infrastructure

Within a virtual network

Cross-premises virtual network

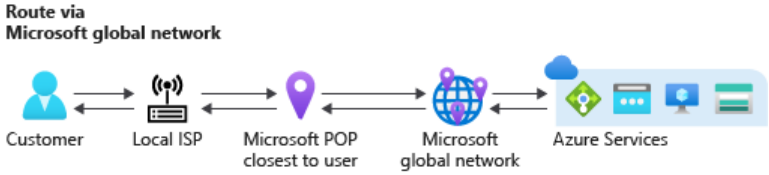
Multi-tier applications

Line-of-business applications

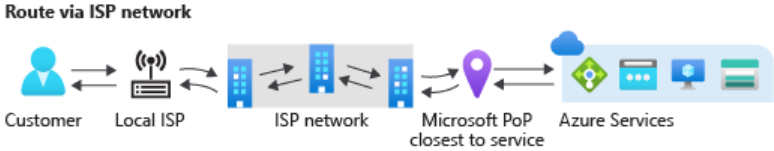


Routing Preference

Routing via Microsoft-Network



Routing via Internet



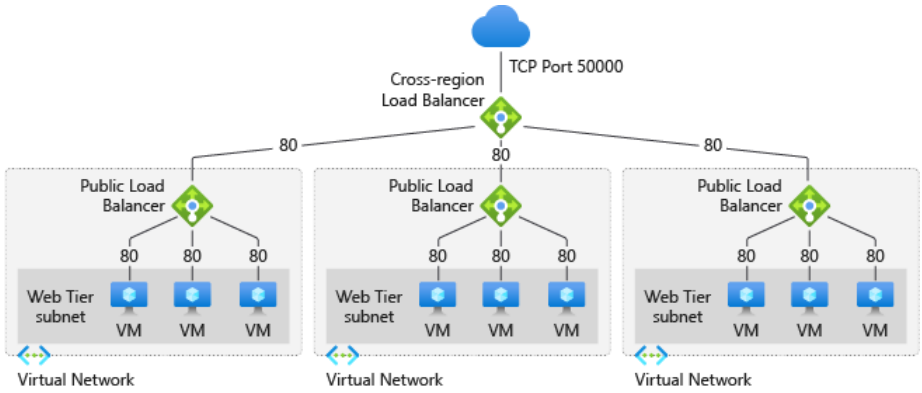
Cross-Region Load Balancer

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

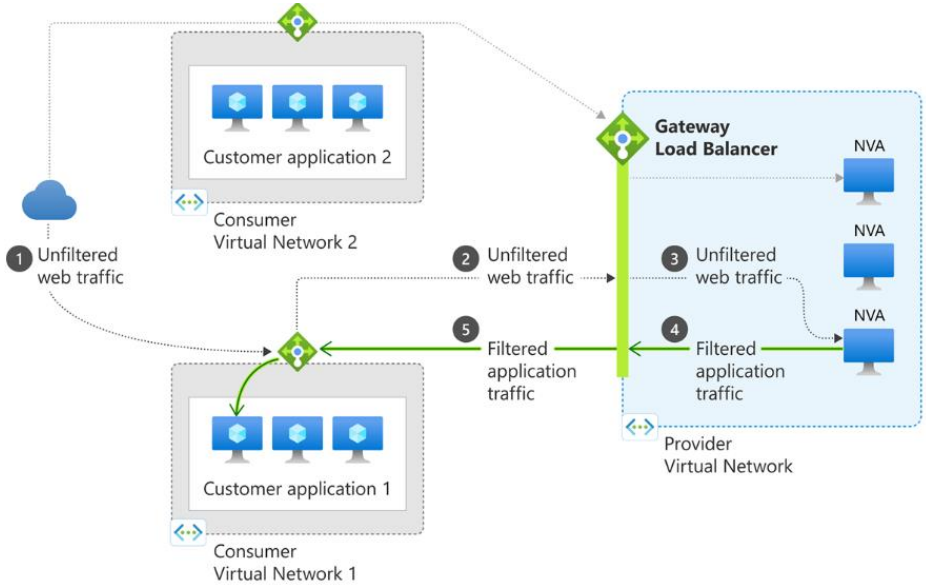


Gateway Load Balancer

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

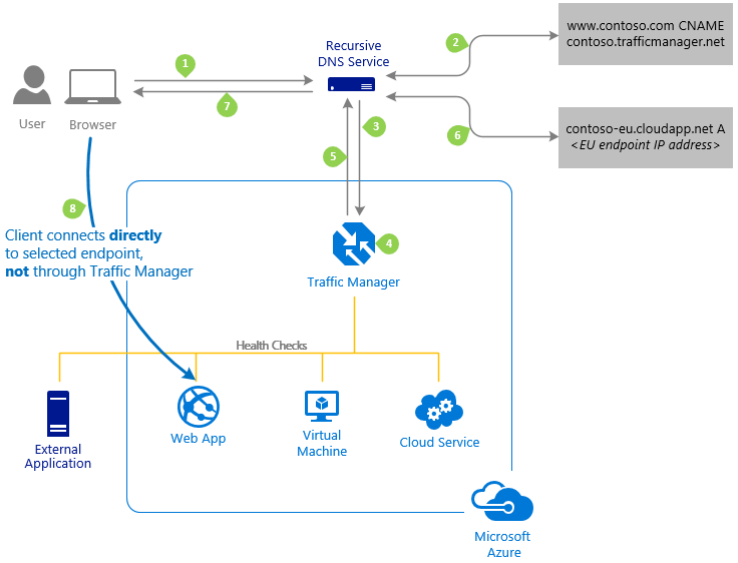
Azure Traffic Manager (TM)
Azure Front Door (AFD)

AZURE
BOOTCAMP SWITZERLAND

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

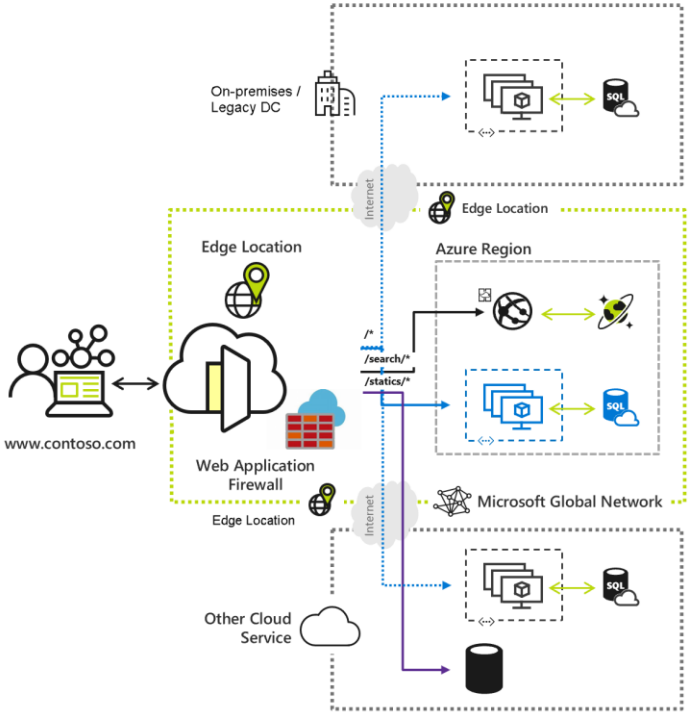
- Global DNS load balancing
- Automatic failover when an endpoint goes down
- Combine with hybrid applications
  Supports external, non-Azure endpoints so that it can be used with hybrid cloud and on-premises deployments
- Distribute traffic for complex deployments
  Use nested Traffic Manager profiles 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

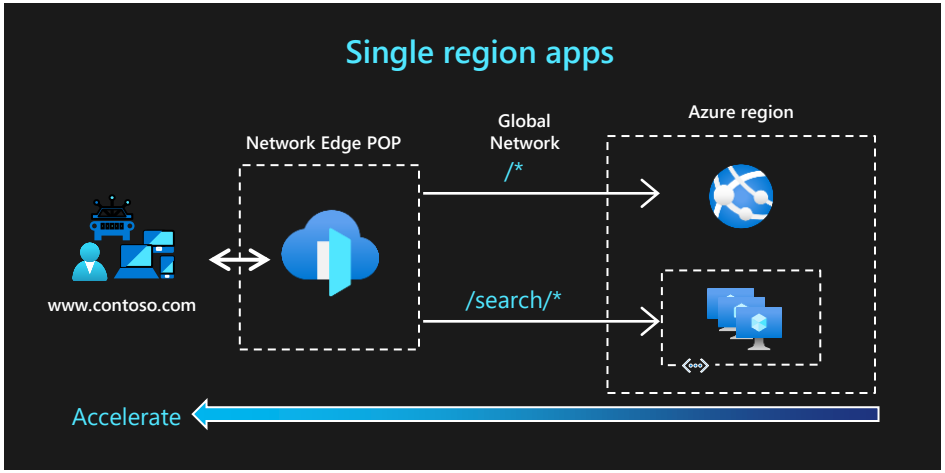
Improve HTTP performance and reduce page load times

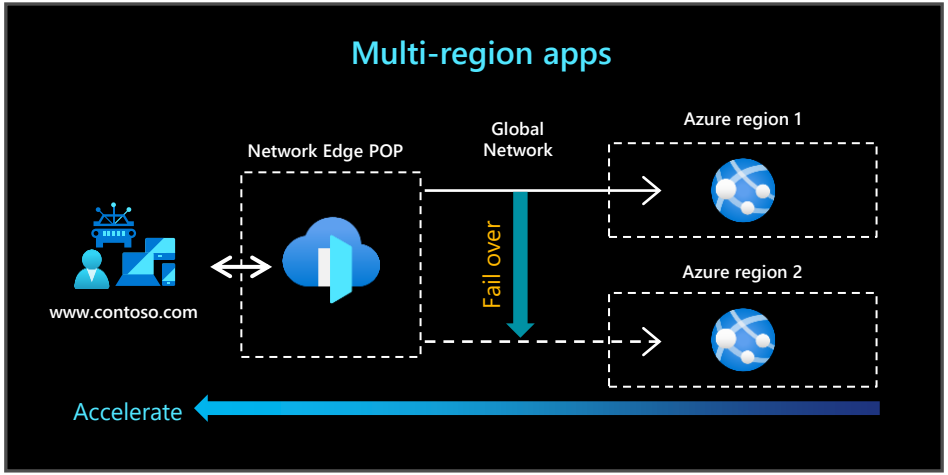
Load balancing at the Edge and fast-failover

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

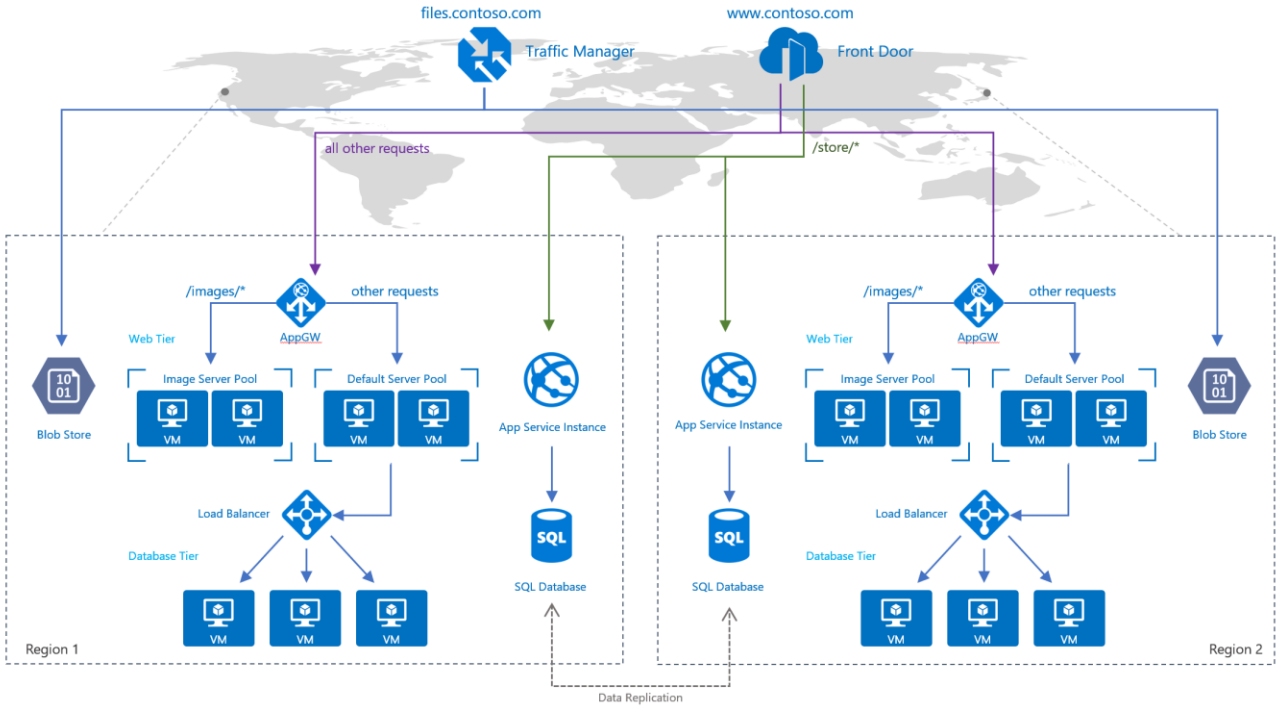




Traffic Manager or Front Door?

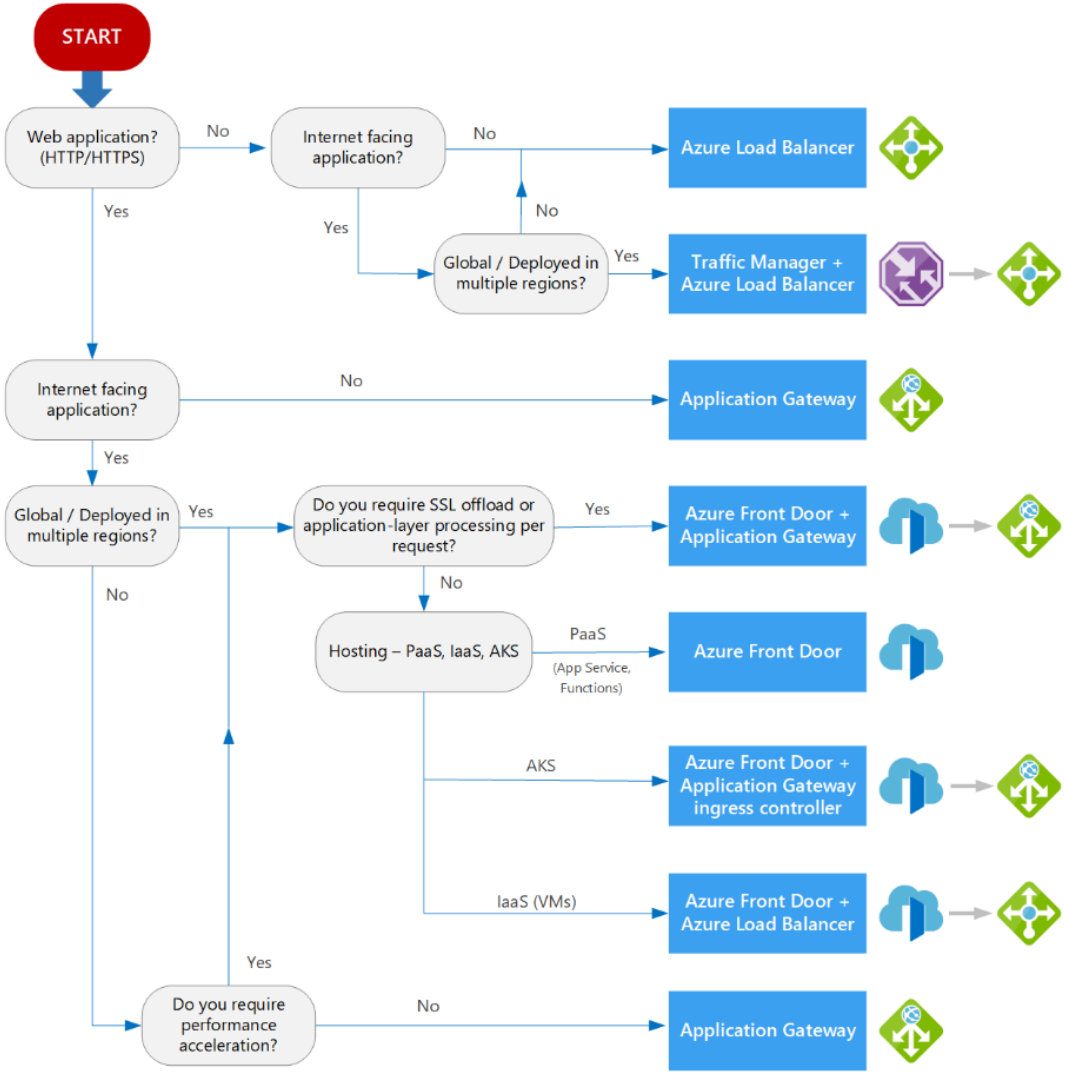
Traffic Manager	Front Door
Any protocol: **Because Traffic Manager works at the DNS layer, you can route any type of network traffic; HTTP, TCP, UDP, etc.**	HTTP acceleration: **With Front Door traffic is proxied at the Edge of Microsoft's network. Because of this, HTTP(S) requests see latency and throughput improvements reducing latency for SSL negotiation and using hot connections from AFD to your application**
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**	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**
Billing format: **DNS-based billing scales with your users and for services with more users, plateaus to reduce cost at higher usage**	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?



AZURE
BOOTCAMP SWITZERLAND

What to use?



AZURE
BOOTCAMP SWITZERLAND

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

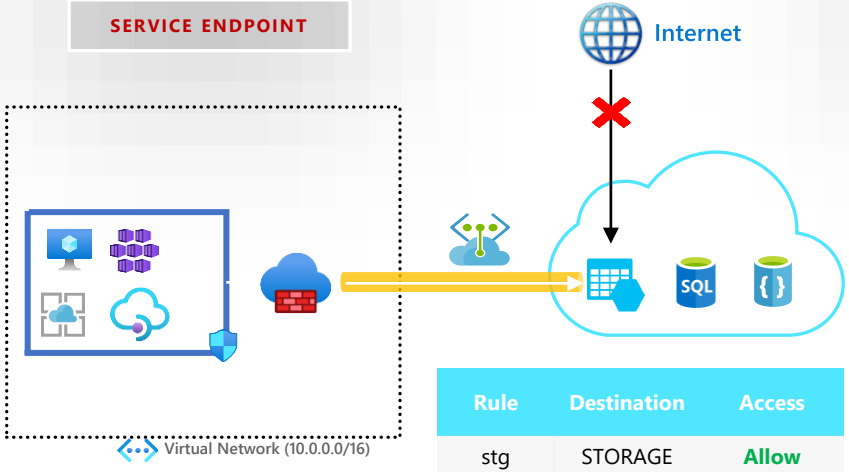
PaaS Services and Networking

Deploy a dedicated service	Use Service Endpoints	Utilize Private Links / Endpoints
Deploy customer specific service instance into own VNET – also for 3rd Party Integrate PaaS Services into VNET	Access to public endpoints via MS Backbone Private IP –> Public IP allowed	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)

AZURE
BOOTCAMP SWITZERLAND

Private PaaS

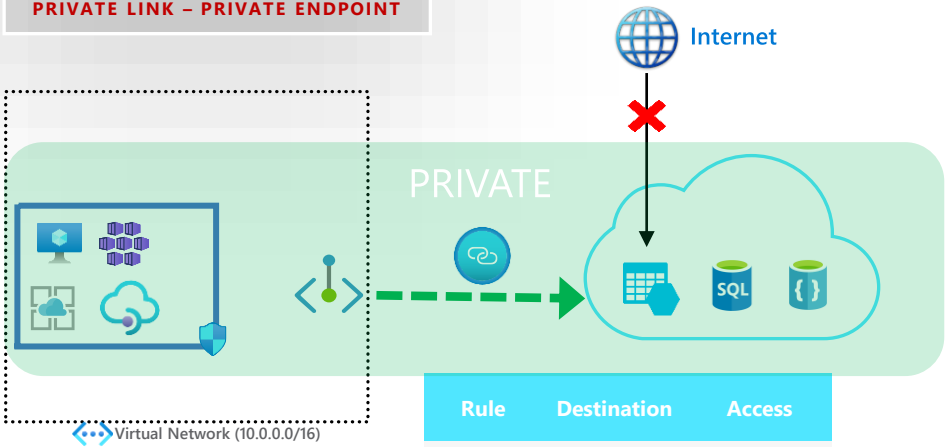
SERVICE ENDPOINT



Rule	Destination	Access
stg	STORAGE	Allow
vnet	VNET	Allow
internet	INTERNET	Deny

- 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

PRIVATE LINK – PRIVATE ENDPOINT

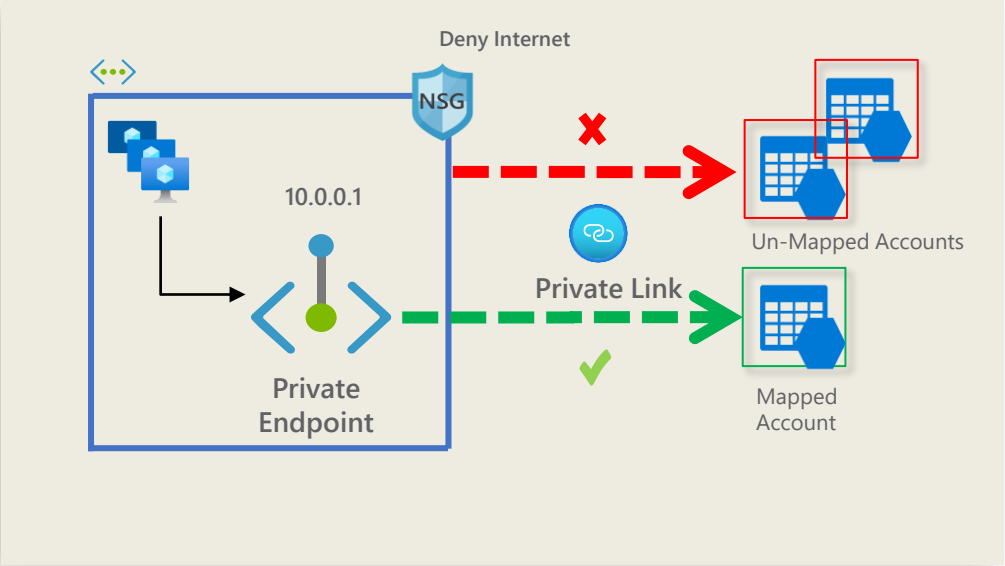


Rule	Destination	Access
vnet	VNET	Allow
internet	INTERNET	Deny

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

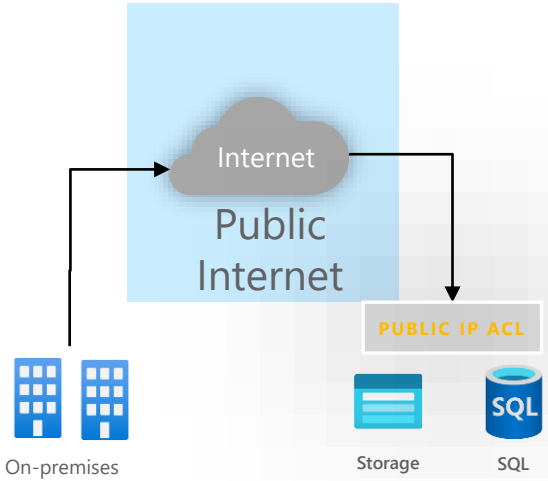
Data Exfiltration Protection

- 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



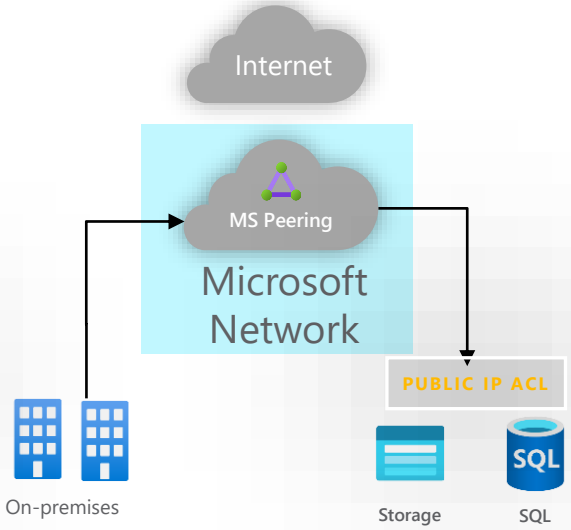
Secure connectivity from on-premises

Good



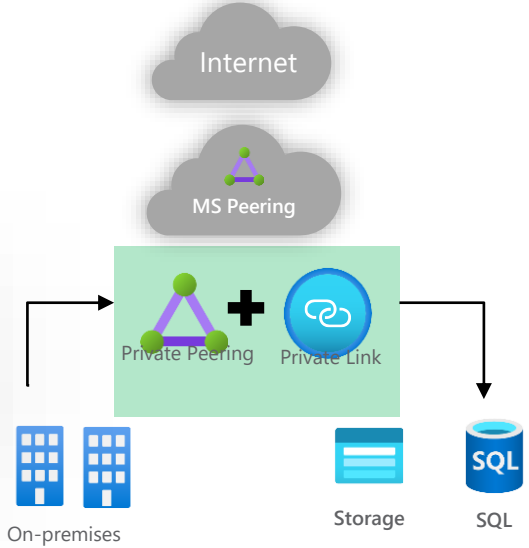
- Traffic traverses the Internet
- Secured using ACLs on Public Ips
- Corporate firewall open to Azure Public IPs

Better



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

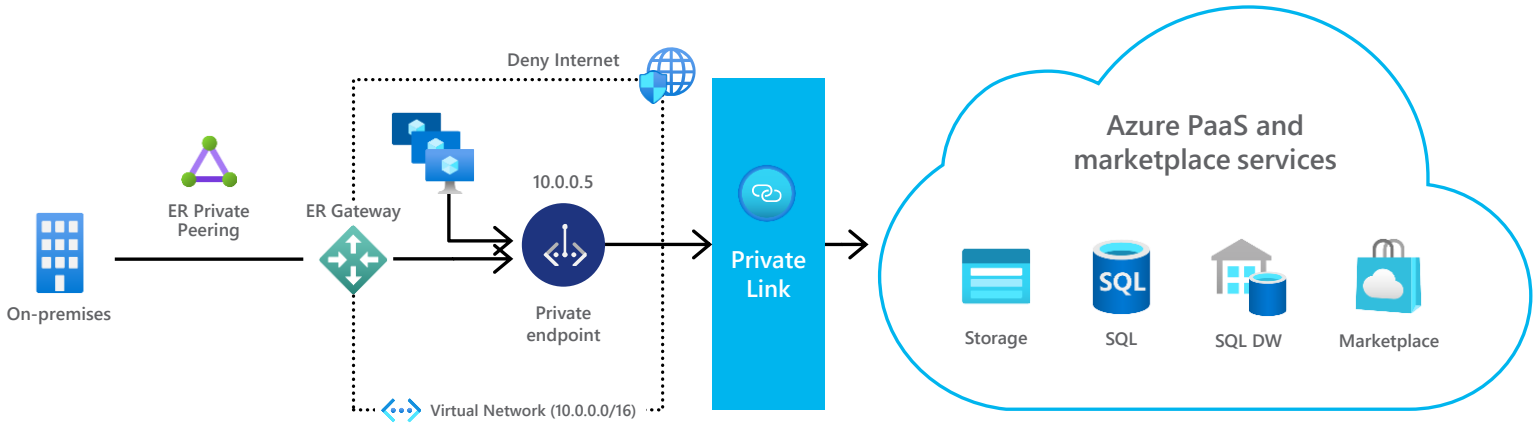
Best



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

AZURE BOOTCAMP SWITZERLAND

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

AZURE
BOOTCAMP SWITZERLAND

There is even more …

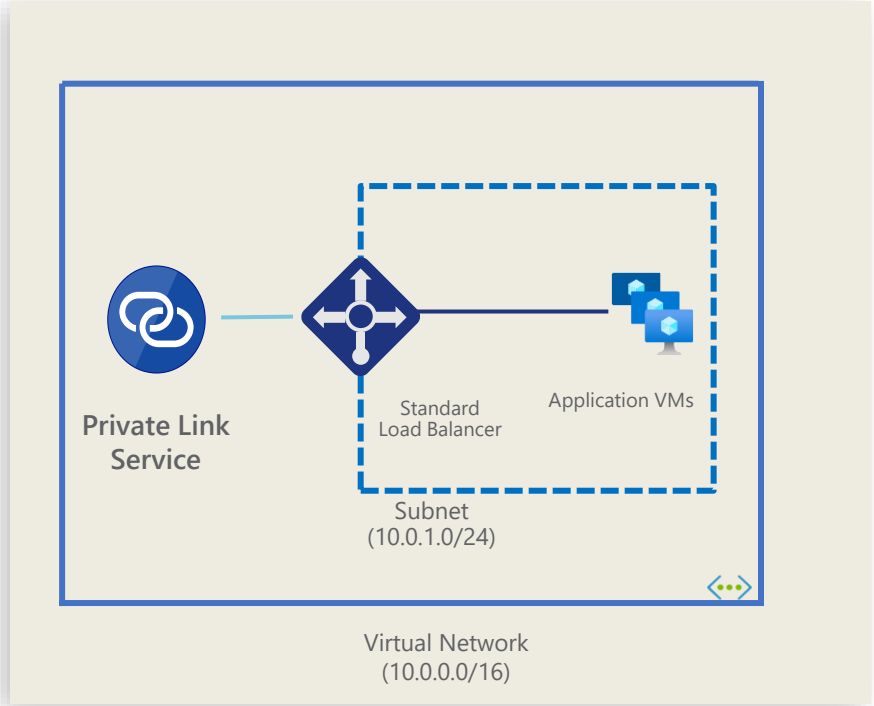
Your Own Private Link Service

- 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

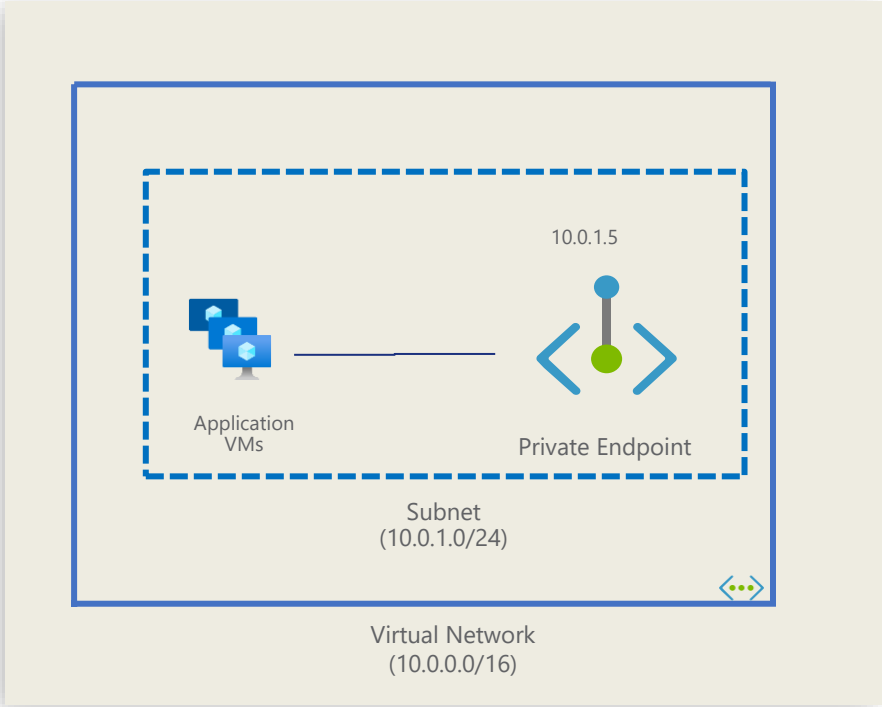
Create Private Link Service

- 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

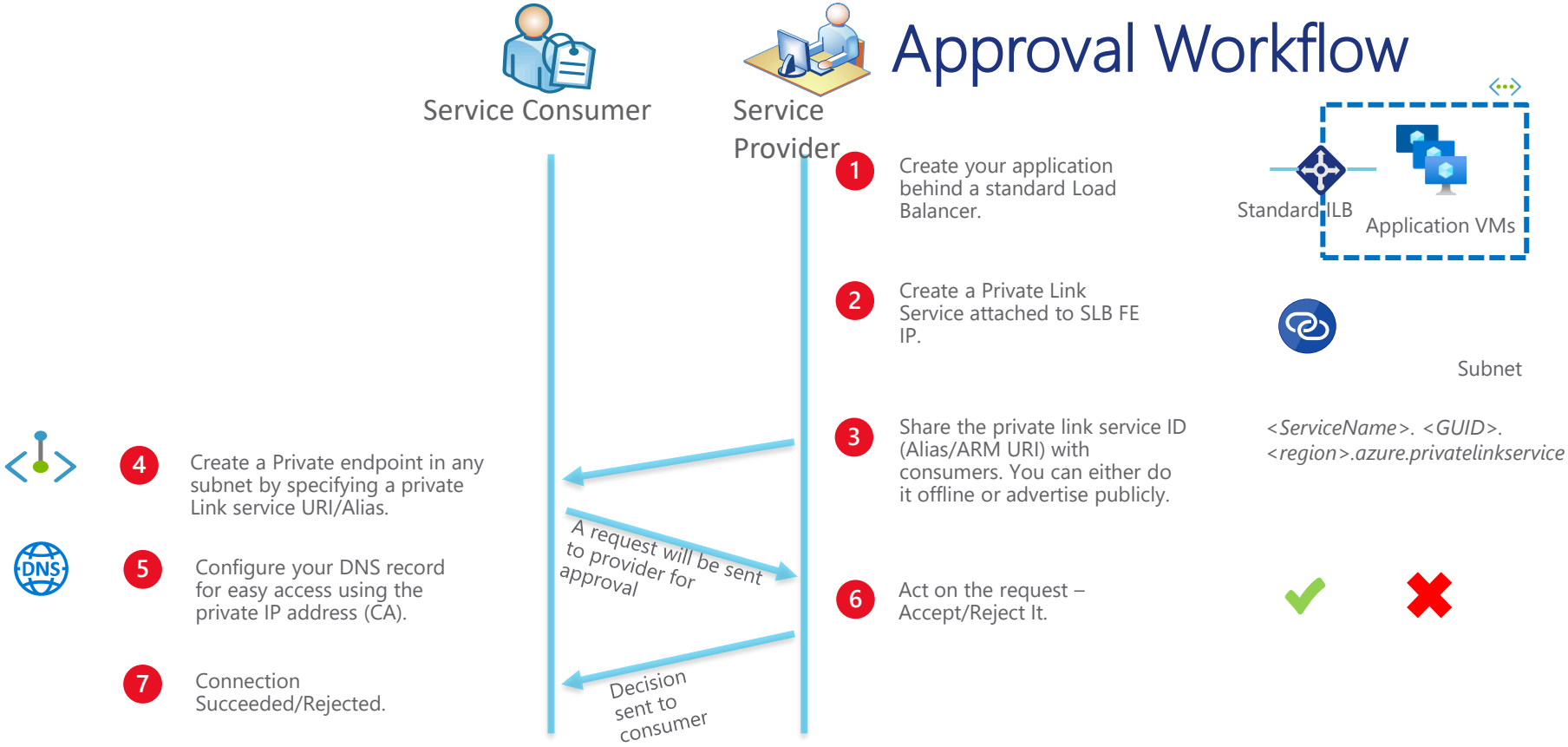


Consume Private Link Service

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

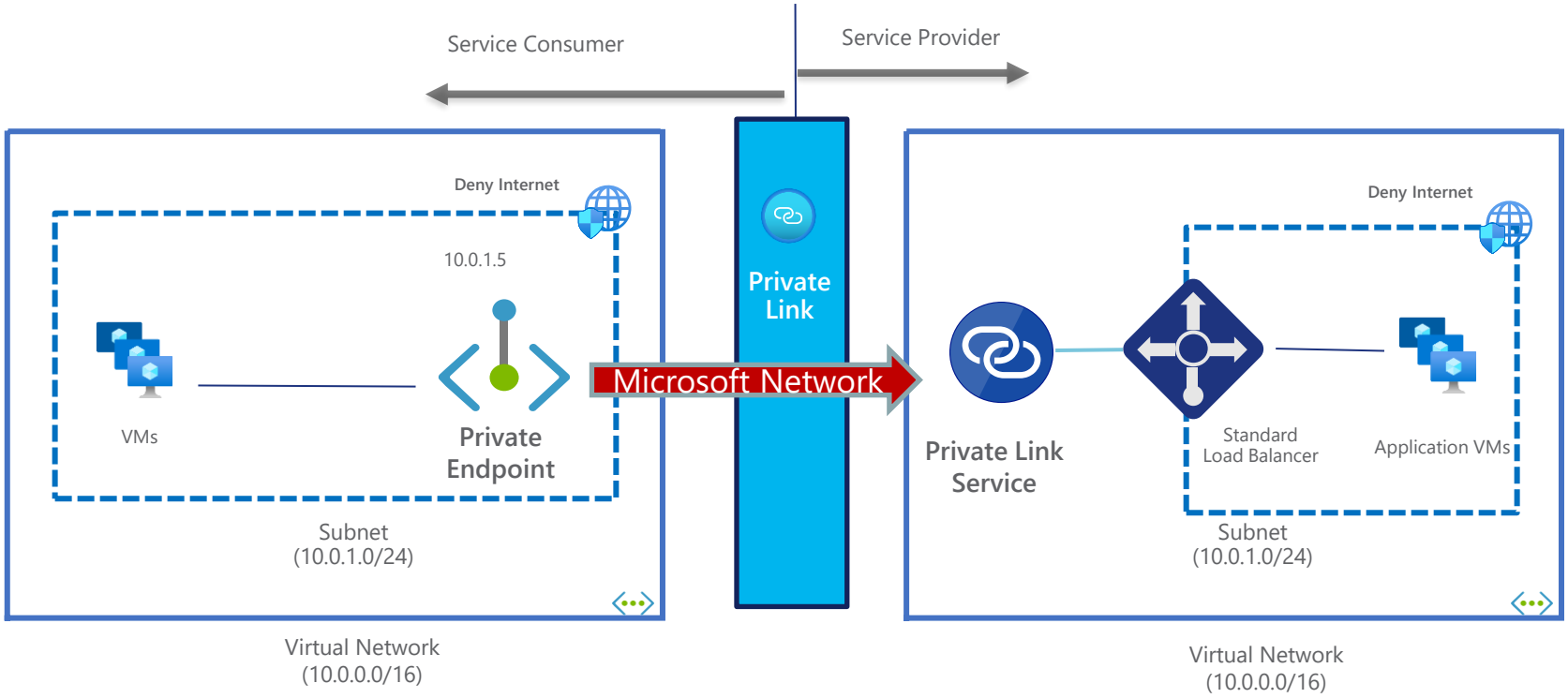


Approval Workflow



AZURE BOOTCAMP SWITZERLAND

Complete Picture



AZURE
BOOTCAMP SWITZERLAND

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

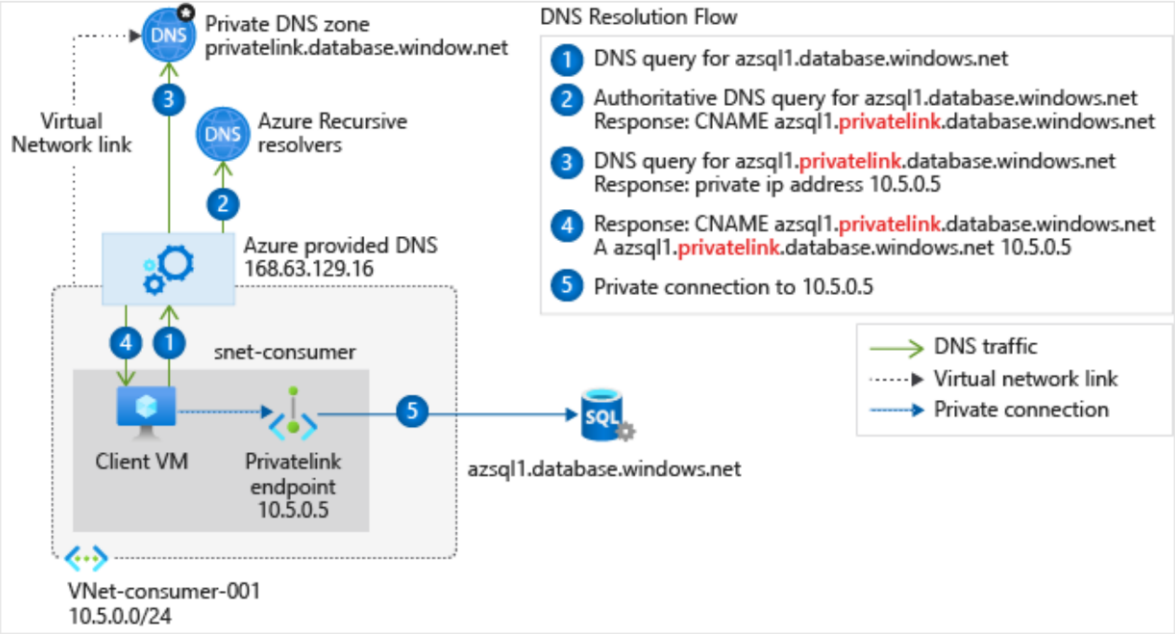
```
C:\Users\EricBerg>nslookup demostordus2021pep.blob.core.windows.net
Server:  unifi.localdomain
Address:  192.168.1.1

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
BOOTCAMP SWITZERLAND

Azure Private DNS

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



AZURE
BOOTCAMP SWITZERLAND

DEMO – Private Link / Endpoint

AZURE
BOOTCAMP SWITZERLAND

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 “DeployIfNotExisits” a DNS Zone Group to Private Endpoints

Solution will take care of everything

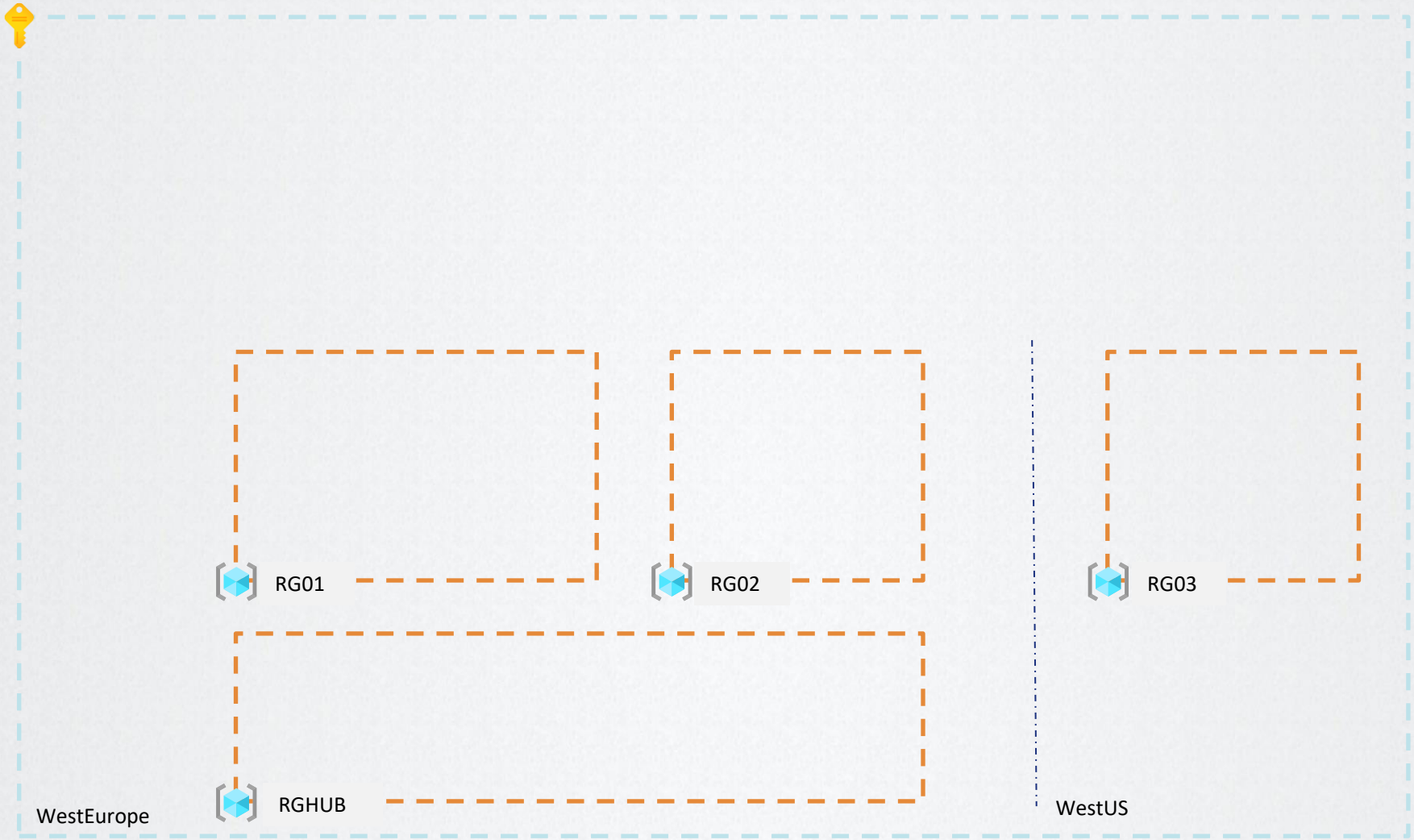
BUT

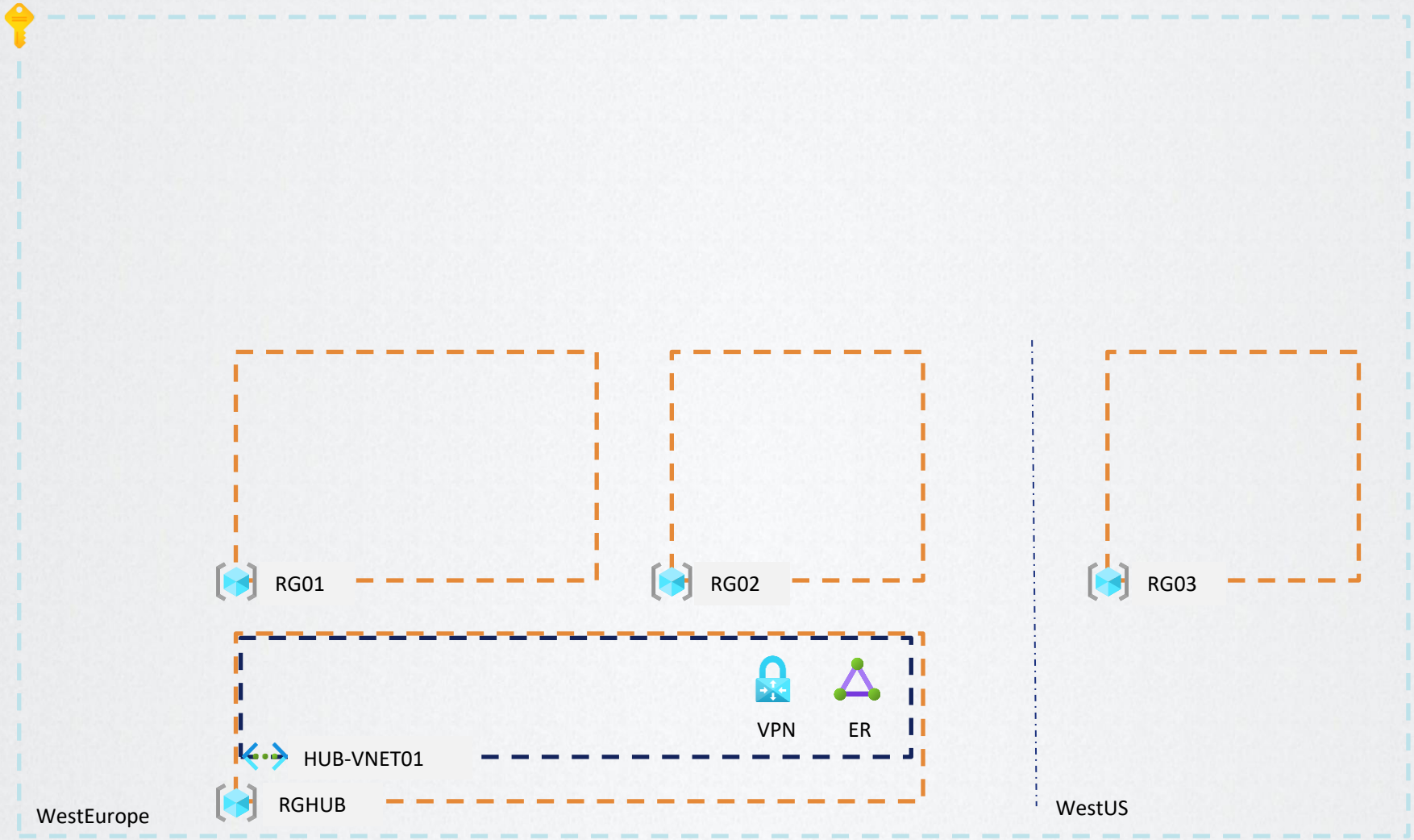
- bound to one tenant, as policy resides in one tenant
- Only one DNS Zone supported per policy

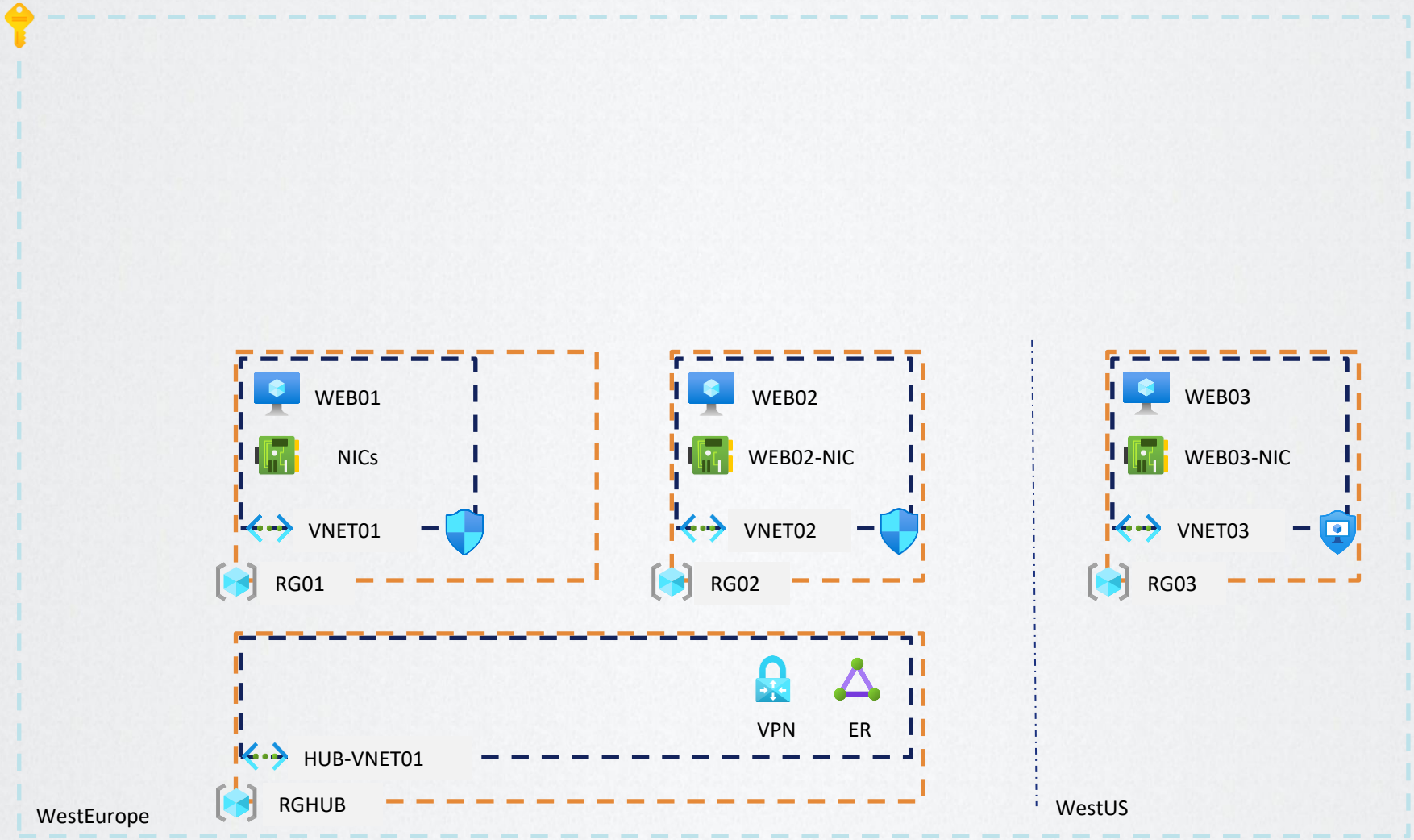
How are things built?

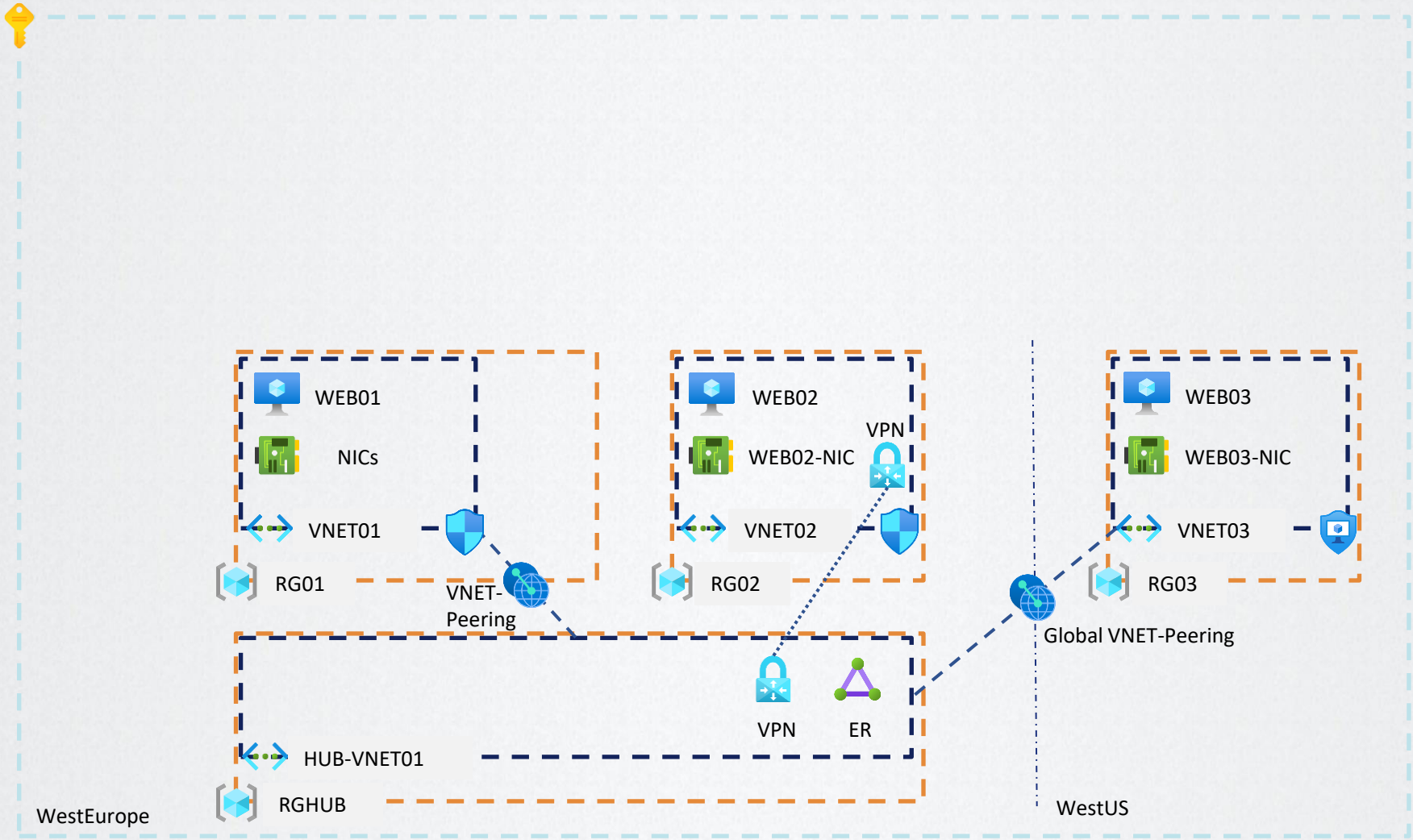
WestEurope

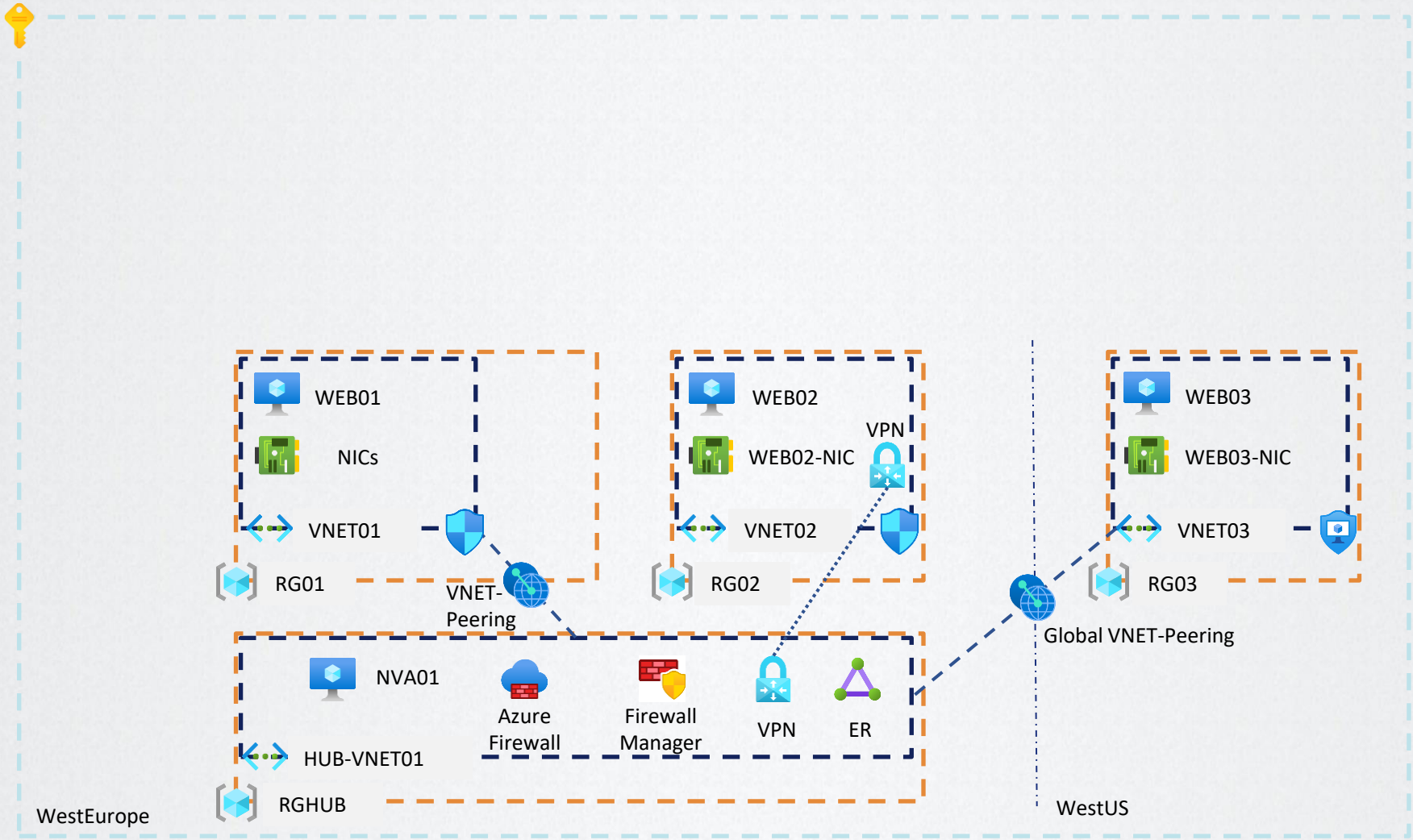
WestUS

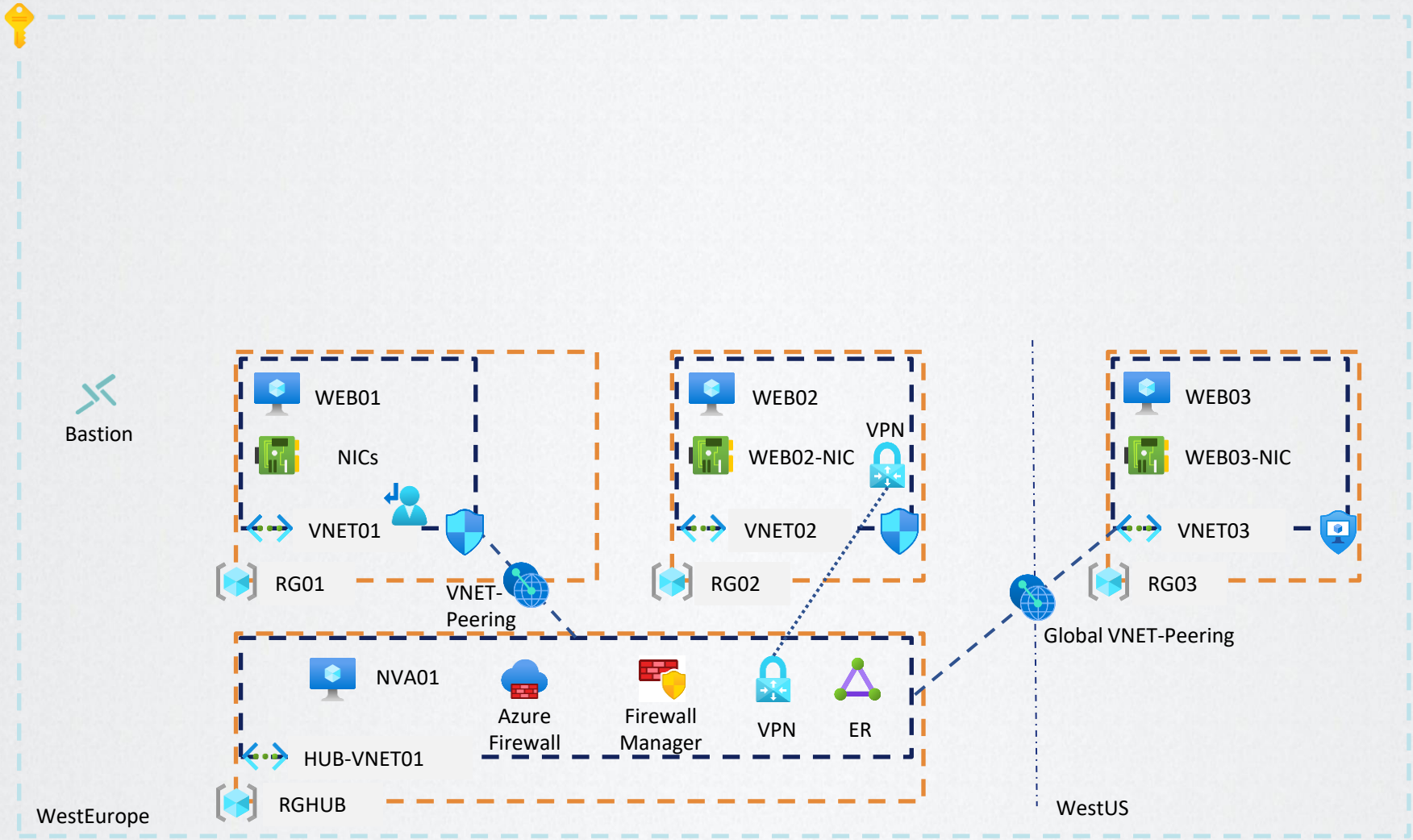

RG01
RG02
RG03
RGHUB
WestEurope
WestUS

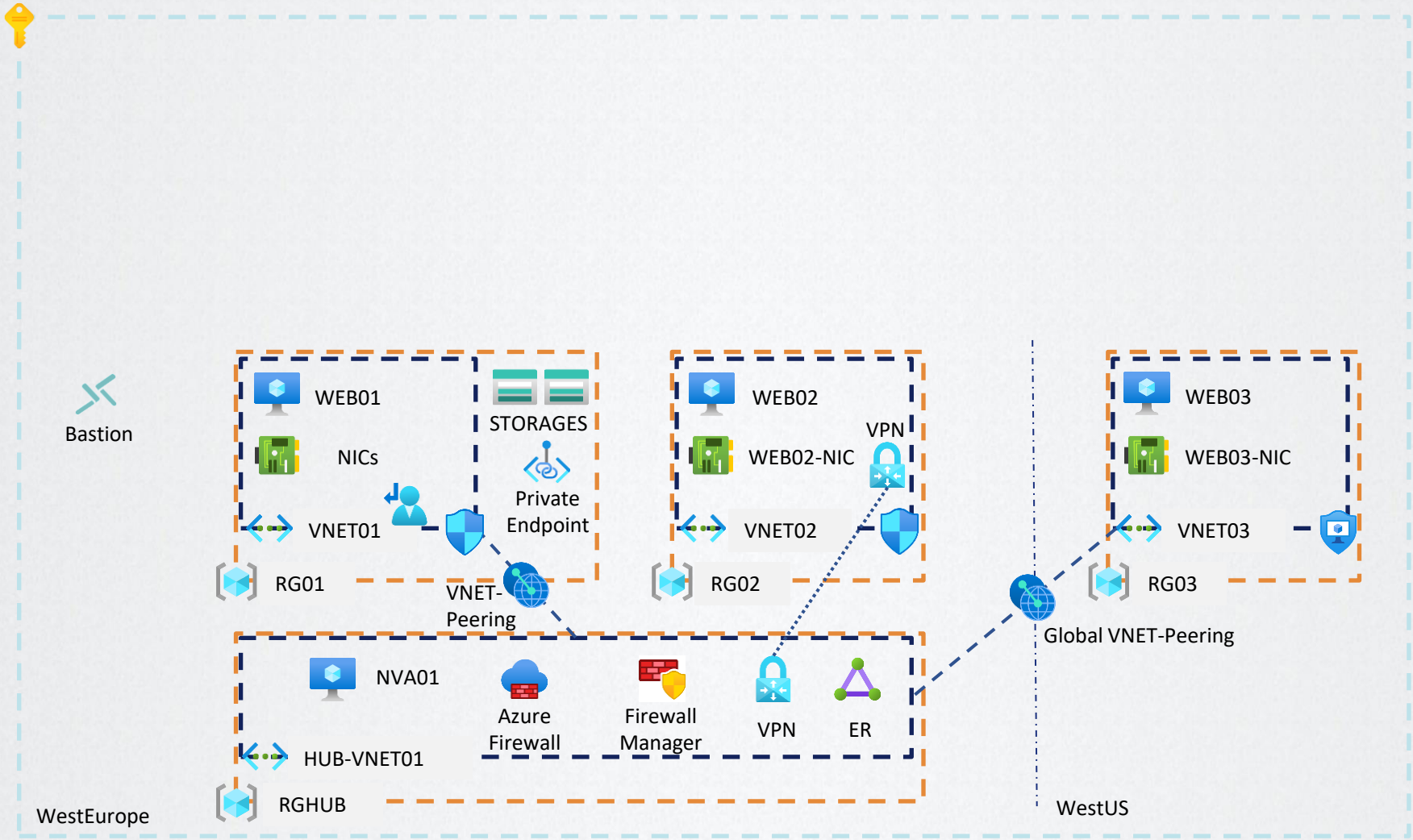

RG01
RG02
RG03
VPN
ER
HUB-VNET01
RGHUB
WestEurope
WestUS

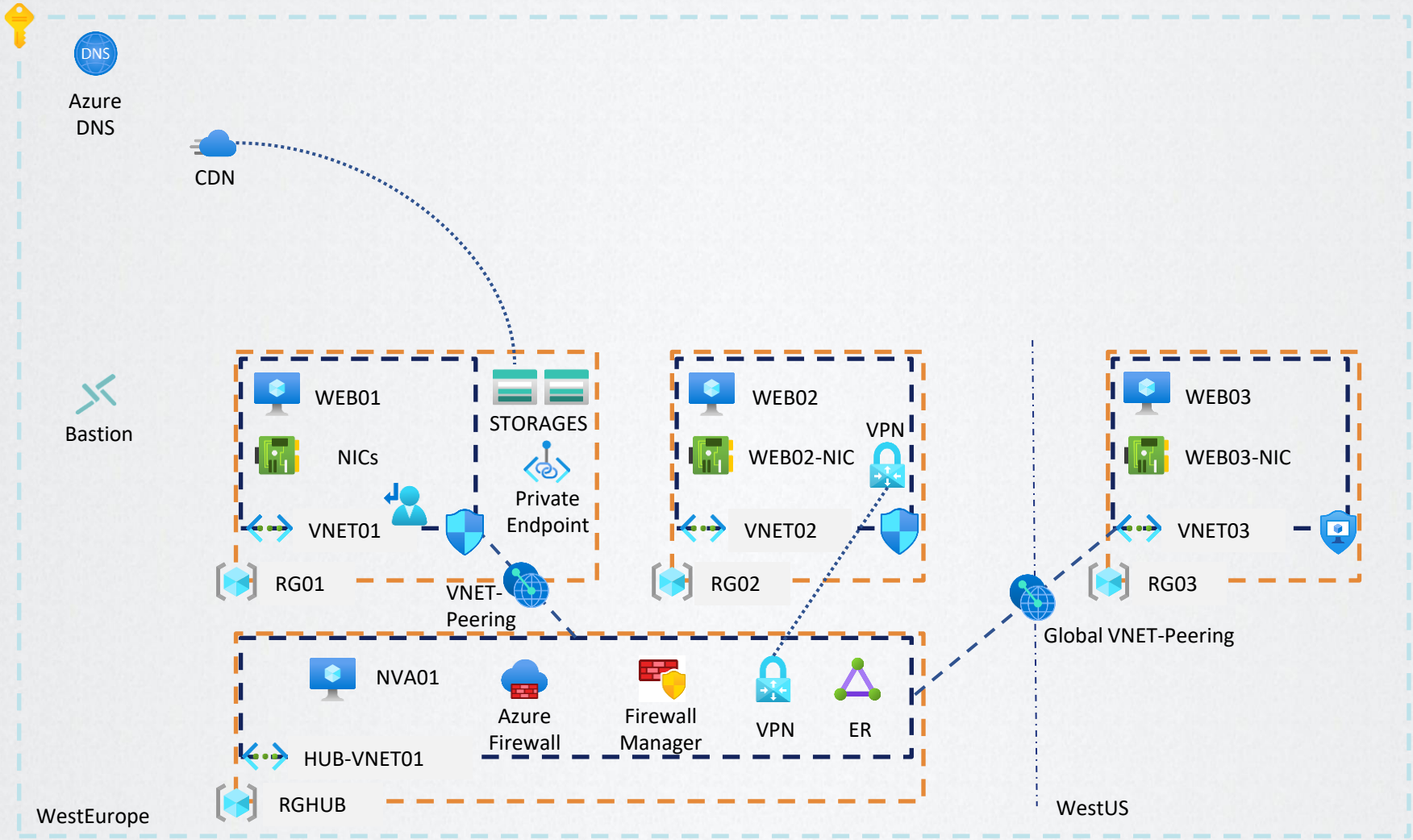

WEB01
NICs
VNET01
RG01
WEB02
WEB02-NIC
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
VPN
ER
HUB-VNET01
RGHUB
WestEurope
WestUS

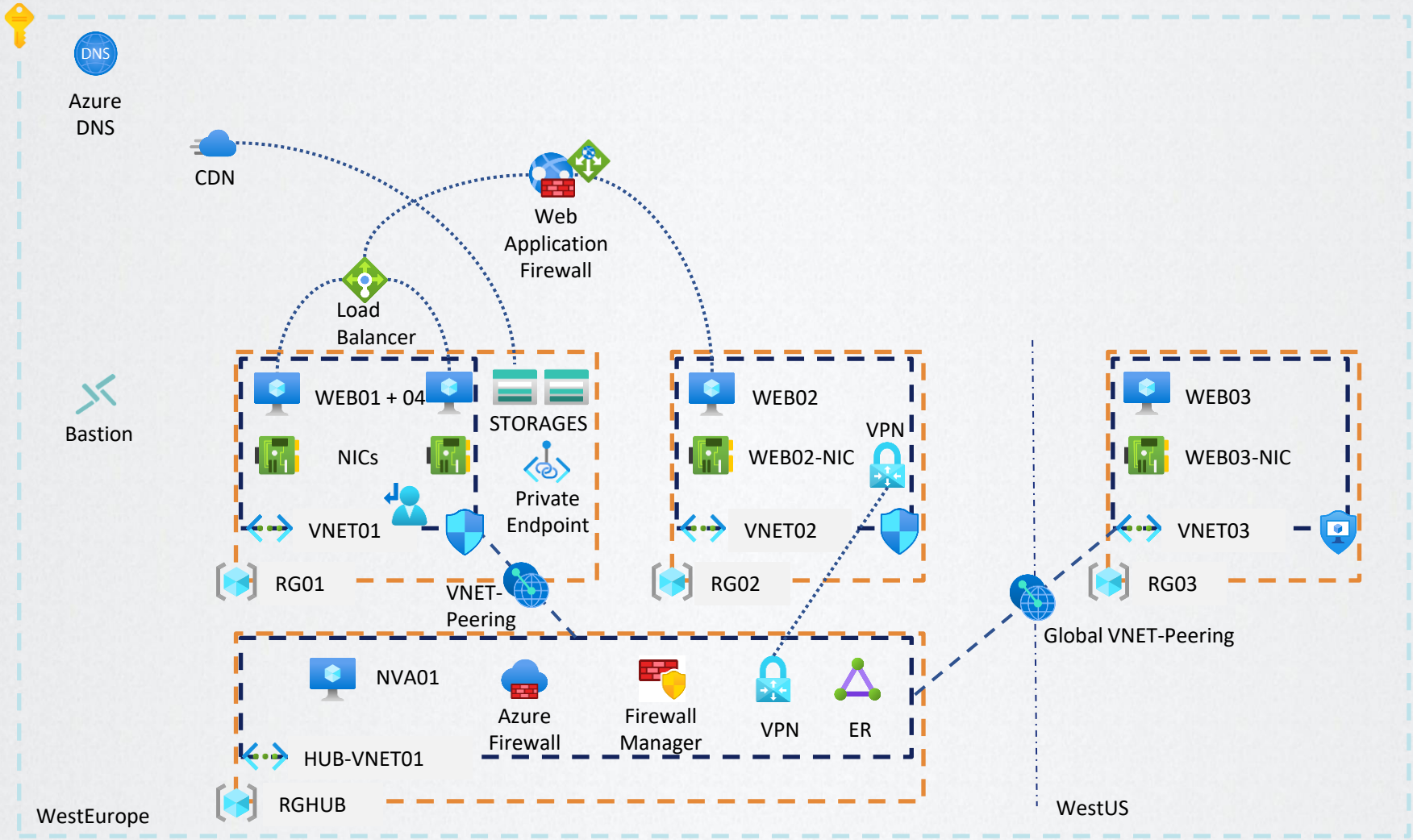

WEB01
NICs
VNET01
RG01
VNET-
Peering
WEB02
WEB02-NIC
VPN
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
VPN
ER
HUB-VNET01
RGHUB
WestEurope
WestUS

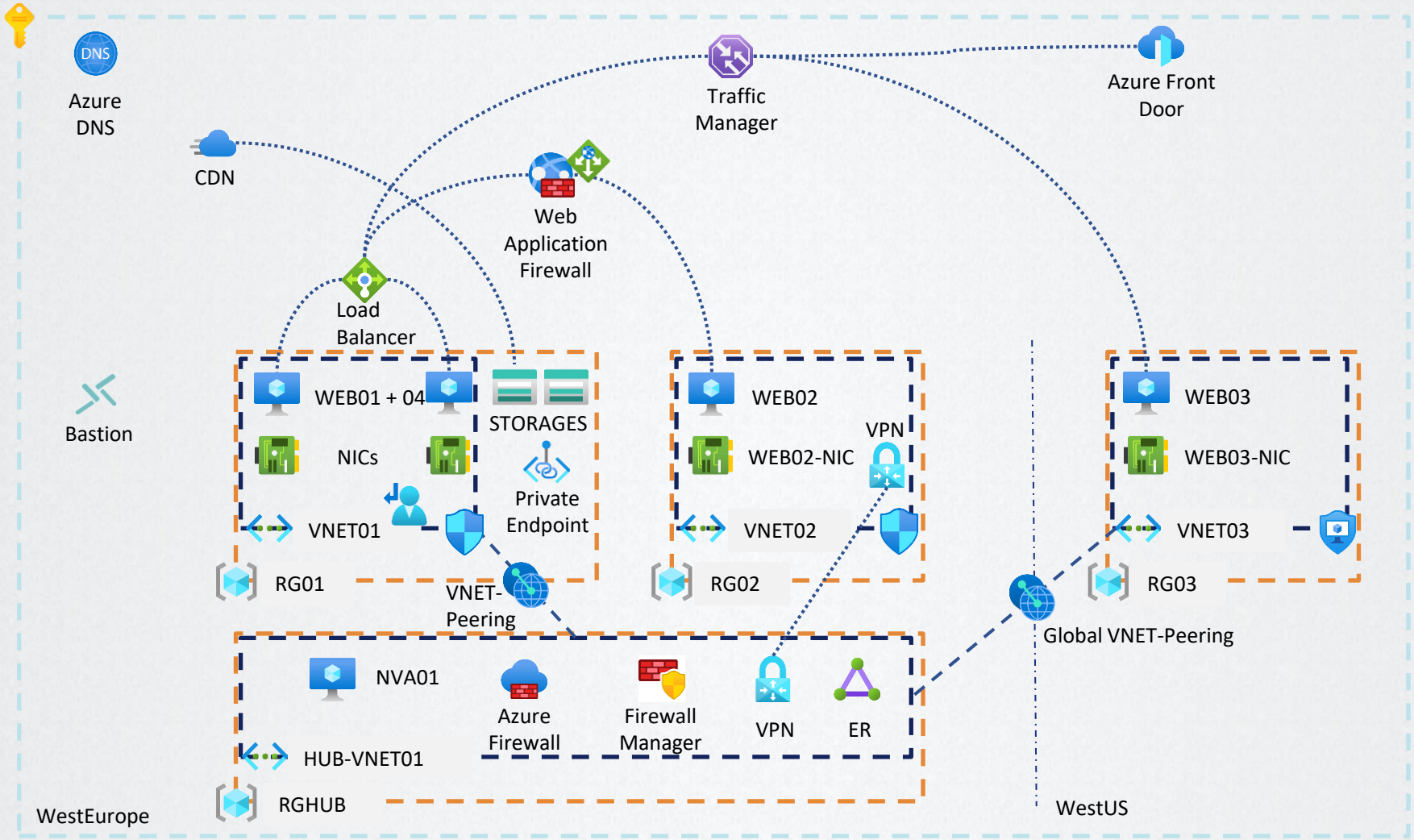

WEB01
NICs
VNET01
RG01
VNET-
Peering
WEB02
WEB02-NIC
VPN
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
NVA01
HUB-VNET01
RGHUB
Azure
Firewall
Firewall
Manager
VPN
ER
WestEurope
WestUS

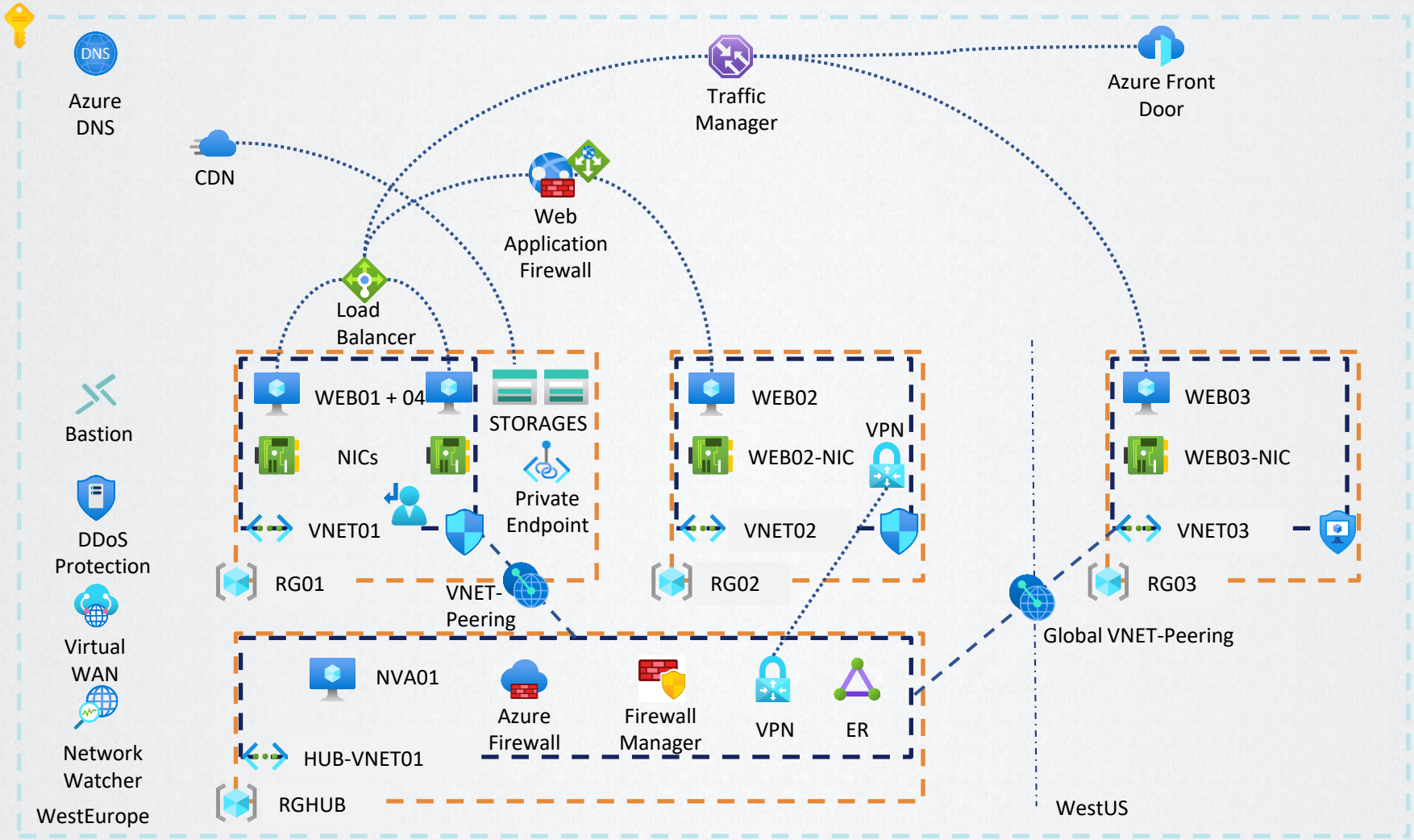

Bastion
WEB01
NICs
VNET01
RG01
VNET-
Peering
WEB02
WEB02-NIC
VPN
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
NVA01
HUB-VNET01
RGHUB
Azure
Firewall
Firewall
Manager
VPN
ER
WestEurope
WestUS

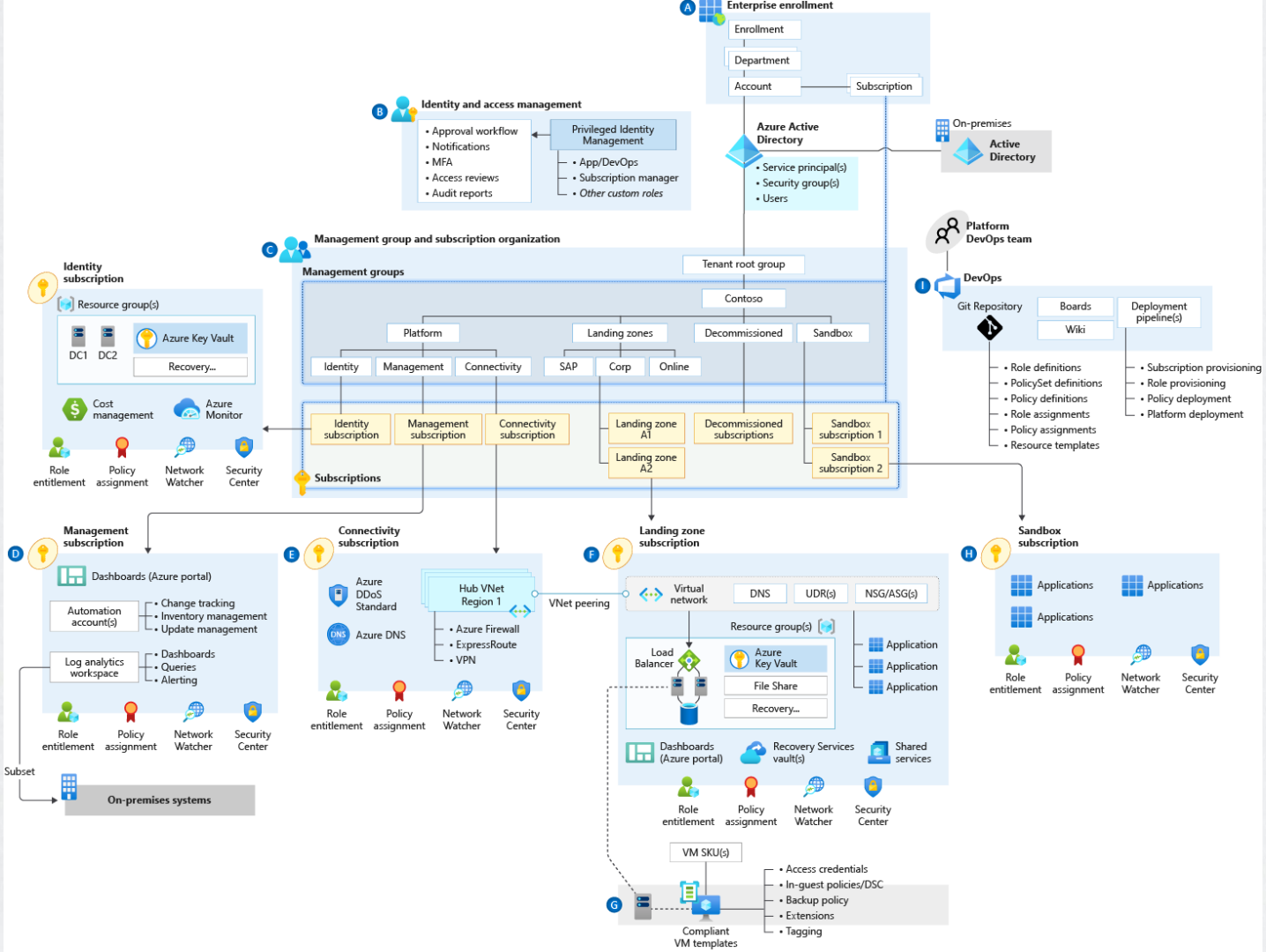

Bastion
WEB01
NICs
VNET01
RG01
STORAGES
Private Endpoint
VNET-Peering
WEB02
WEB02-NIC
VPN
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
NVA01
HUB-VNET01
RGHUB
Azure Firewall
Firewall Manager
VPN
ER
WestEurope
WestUS


Azure DNS
CDN
Bastion
WEB01
NICs
VNET01
RG01
STORAGES
Private Endpoint
VNET-Peering
WEB02
WEB02-NIC
VPN
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
NVA01
HUB-VNET01
RGHUB
Azure Firewall
Firewall Manager
VPN
ER
WestEurope
WestUS


Azure DNS
CDN
Web Application Firewall
Load Balancer
Bastion
WEB01 + 04
STORAGES
NICs
Private Endpoint
VNET01
RG01
VNET-Peering
WEB02
VPN
WEB02-NIC
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
NVA01
Azure Firewall
Firewall Manager
VPN
ER
HUB-VNET01
RGHUB
WestEurope
WestUS


Azure DNS
Traffic Manager
Azure Front Door
CDN
Web Application Firewall
Load Balancer
Bastion
WEB01 + 04
STORAGES
NICs
Private Endpoint
VNET01
RG01
VNET-Peering
WEB02
VPN
WEB02-NIC
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
NVA01
Azure Firewall
Firewall Manager
VPN
ER
HUB-VNET01
RGHUB
WestEurope
WestUS


Azure DNS
Traffic Manager
Azure Front Door
CDN
Web Application Firewall
Load Balancer
Bastion
DDoS Protection
Virtual WAN
Network Watcher
WestEurope
WEB01 + 04
STORAGES
NICs
Private Endpoint
VNET01
RG01
VNET-Peering
WEB02
VPN
WEB02-NIC
VNET02
RG02
WEB03
WEB03-NIC
VNET03
RG03
Global VNET-Peering
NVA01
Azure Firewall
Firewall Manager
VPN
ER
HUB-VNET01
RGHUB
WestUS


A
Enterprise enrollment
Enrollment
Department
Account
Subscription
B
Identity and access management
• Approval workflow
• Notifications
• MFA
• Access reviews
• Audit reports
Privileged Identity Management
• App/DevOps
• Subscription manager
• Other custom roles
Azure Active Directory
• Service principal(s)
• Security group(s)
• Users
On-premises
Active Directory
C
Management group and subscription organization
Management groups
Tenant root group
Contoso
Platform
Landing zones
Decommissioned
Sandbox
Identity
Management
Connectivity
SAP
Corp
Online
Identity subscription
Management subscription
Connectivity subscription
Landing zone A1
Landing zone A2
Decommissioned subscriptions
Sandbox subscription 1
Sandbox subscription 2
Subscriptions
Identity subscription
Resource group(s)
DC1
DC2
Azure Key Vault
Recovery...
Cost management
Azure Monitor
Role entitlement
Policy assignment
Network Watcher
Security Center
Platform DevOps team
I
DevOps
Git Repository
Boards
Wiki
Deployment pipeline(s)
• Role definitions
• PolicySet definitions
• Policy definitions
• Role assignments
• Policy assignments
• Resource templates
• Subscription provisioning
• Role provisioning
• Policy deployment
• Platform deployment
D
Management subscription
Dashboards (Azure portal)
Automation account(s)
• Change tracking
• Inventory management
• Update management
Log analytics workspace
• Dashboards
• Queries
• Alerting
Role entitlement
Policy assignment
Network Watcher
Security Center
Subset
On-premises systems
E
Connectivity subscription
Azure DDoS Standard
Azure DNS
Hub VNet Region 1
• Azure Firewall
• ExpressRoute
• VPN
VNet peering
Role entitlement
Policy assignment
Network Watcher
Security Center
F
Landing zone subscription
Virtual network
DNS
UDR(s)
NSG/ASG(s)
Resource group(s)
Load Balancer
Azure Key Vault
File Share
Recovery...
Application
Application
Application
Dashboards (Azure portal)
Recovery Services vault(s)
Shared services
Role entitlement
Policy assignment
Network Watcher
Security Center
G
VM SKU(s)
Compliant VM templates
• Access credentials
• In-guest policies/DSC
• Backup policy
• Extensions
• Tagging
H
Sandbox subscription
Applications
Applications
Applications
Role entitlement
Policy assignment
Network Watcher
Security Center

AZURE

BOOTCAMP SWITZERLAND

swisscom

AVENIQ

die Mobiliar

scopewyse

axpo

JOKER IT

GRABX

techtask

» Leading through the sea of clouds »

SPIE

baggenstos.

isolutions

digicomp

Want to dive deeper?!

Azure PaaS, but as private as possible…

Stephan Graber – 14:25

Azure Virtual Network Manager: The future of network management?

Marcel Zehner – 15:40

AZURE
BOOTCAMP SWITZERLAND