Azure Networking – Native Tools vs. 3rd Party Management

Eric Berg – VP @ CGI | Microsoft MVP

AXXES

Arxus

codit

delaware

devoteam

DEXMACH
A CEGEKA COMPANY

Microsoft

ORDINA

inetum realdolmen
Positive digital flow

proximus

ZURE

Thank you partners!

Integration.team
Connecting anything, anytime, anywhere

NOEST

datarobots

JET BRAINS

U2U

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

Microsoft® MVP Most Valuable Professional

GEEKZEUGS HOME OF
GEEKSPRECH Podcast
GEEKSCHAU Webcast
GEEKTREFF Community

Azure Meetup THÜRINGEN

IT DEPENDS ...

THANK YOU!

QUESTIONS?

O.K. … let’s start over …

Disclaimer

No advertisement, recommendation, preferred solution, etc. of any mentioned 3rd Party Solution … just what I came across in the field!!!

Disclaimer 2

No … just joking

Agenda

- Networking Capabilities
- Networking Fundamentals
- Networking Recap
- 3rd Party Replacements
- How to decide?

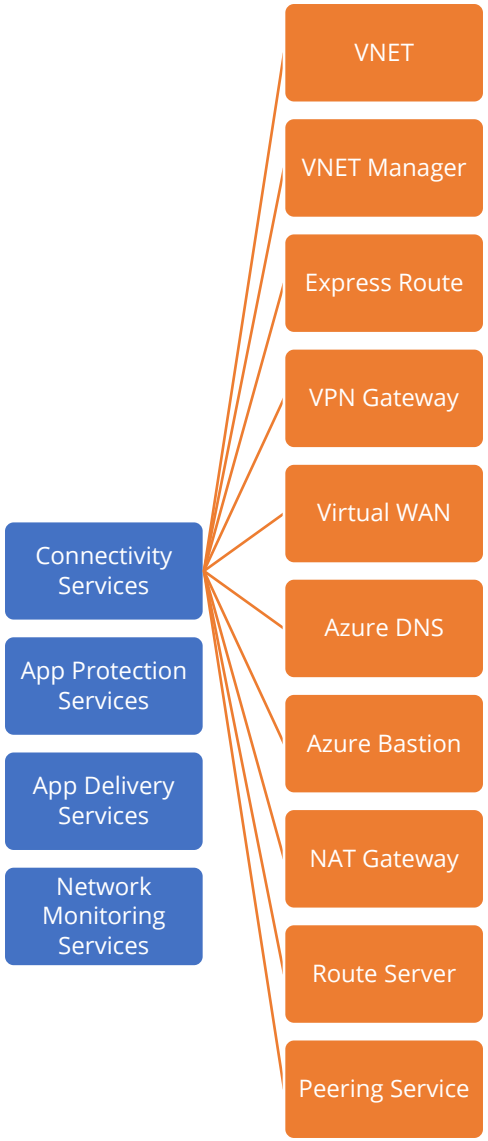
Networking Capabilities

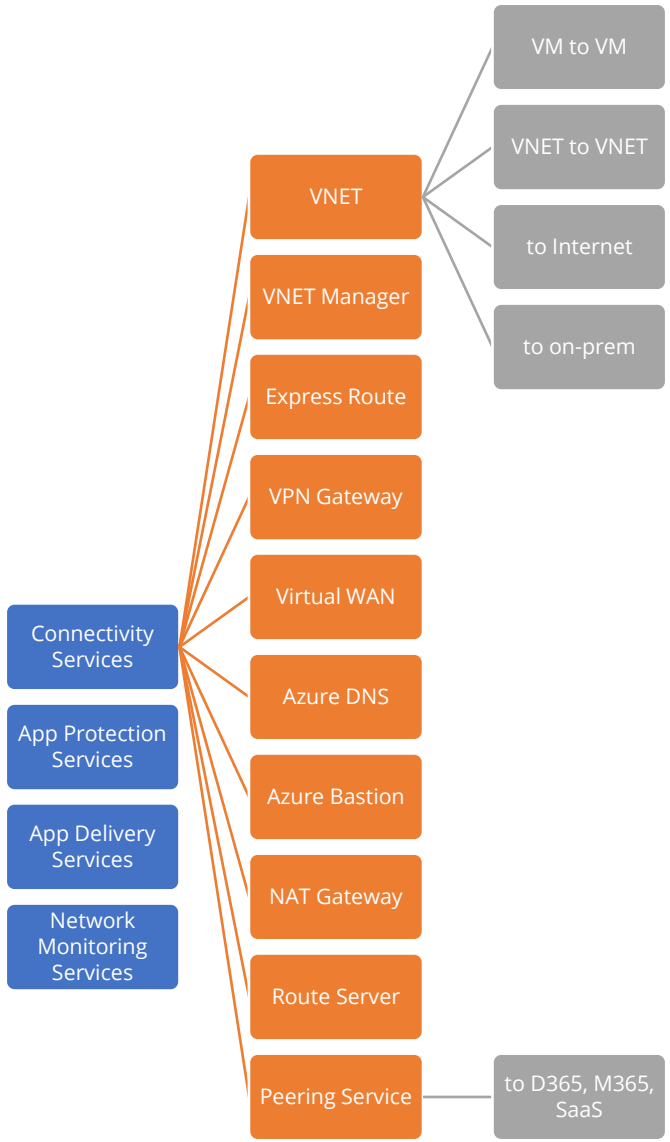
Connectivity Services

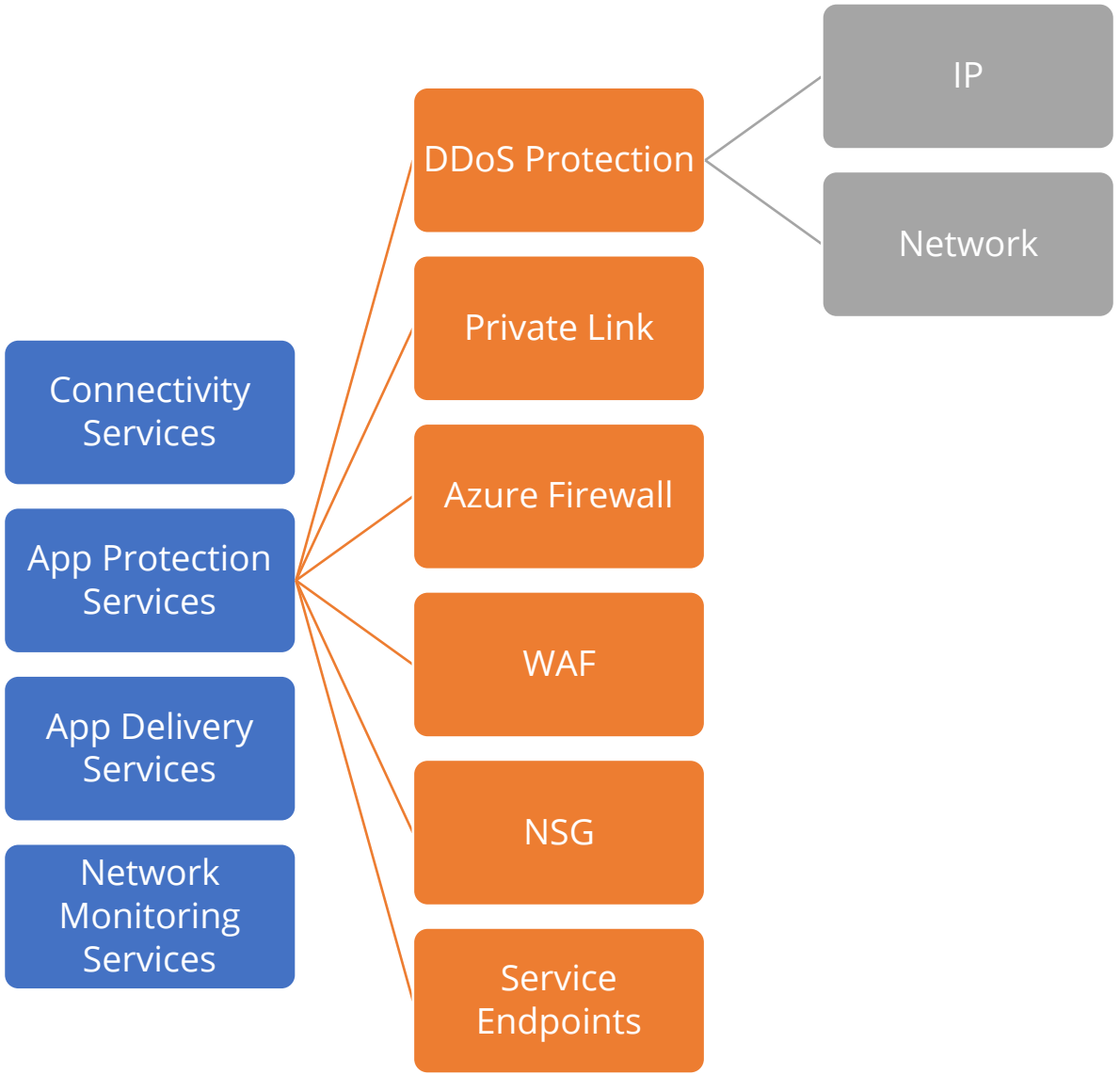
App Protection Services

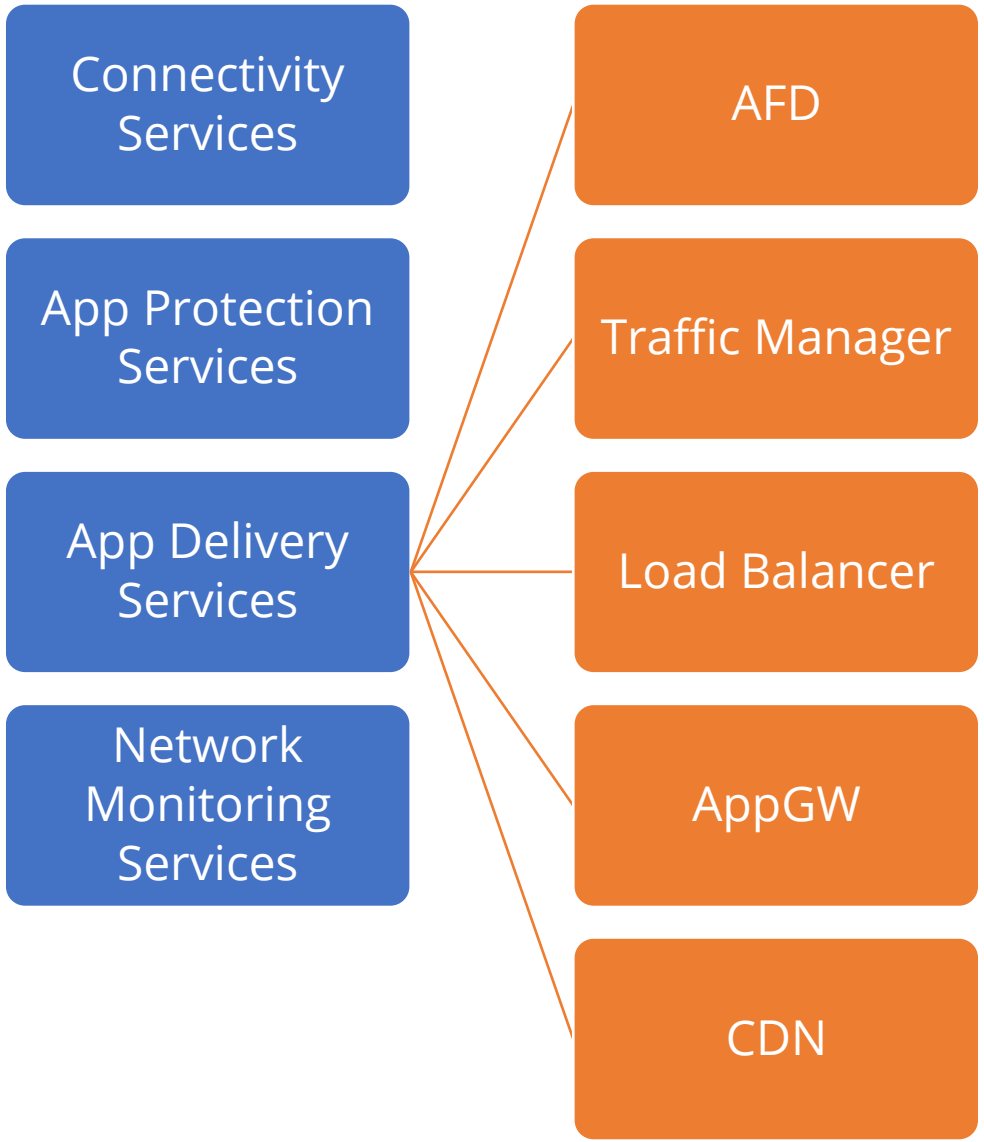
App Delivery Services

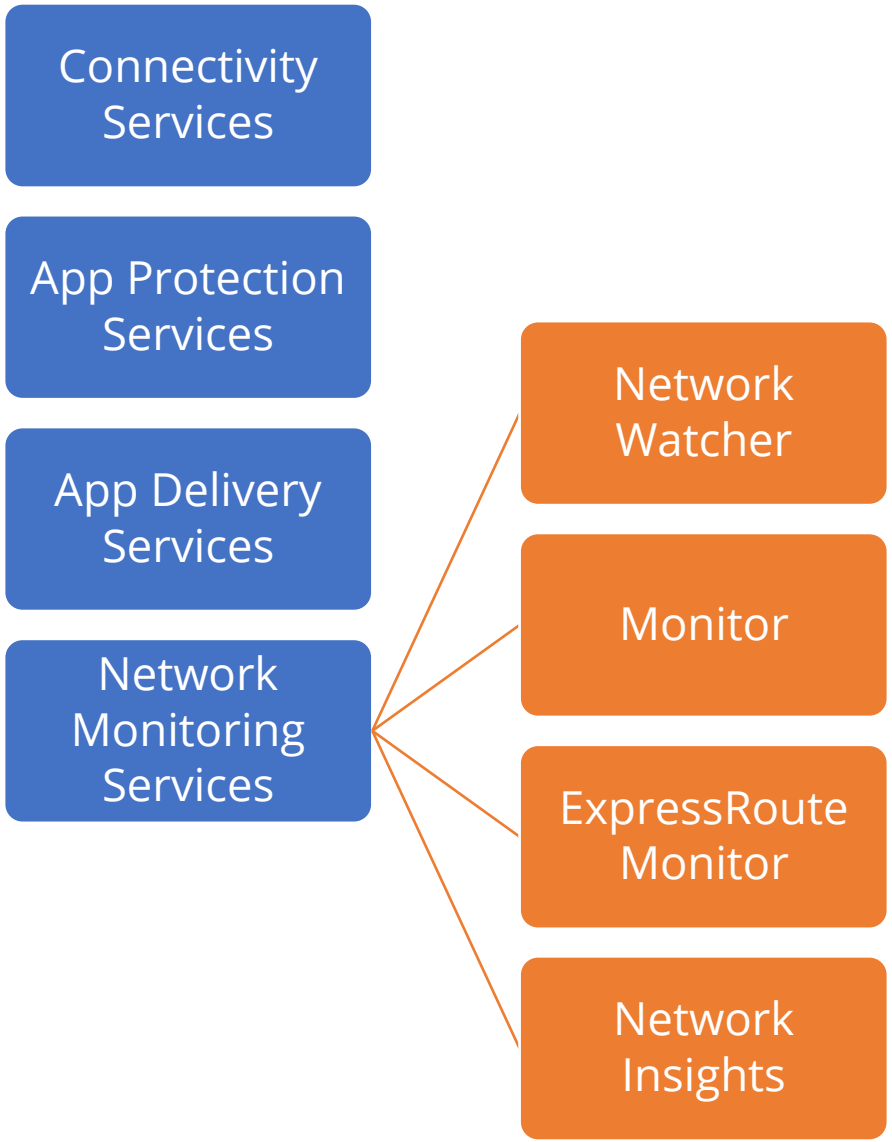
Network Monitoring Services

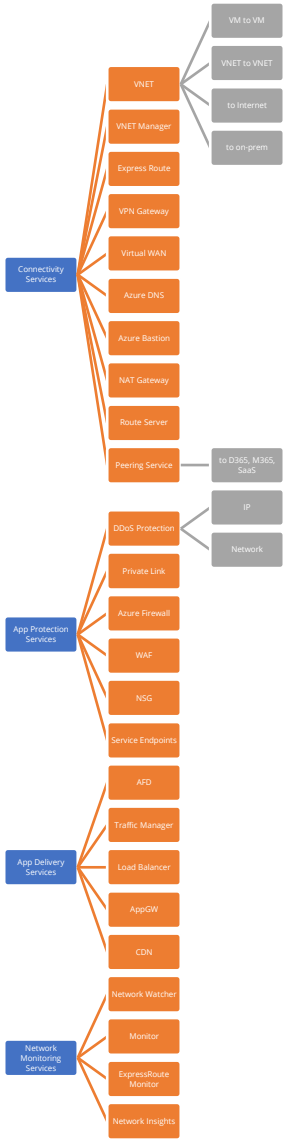

Connectivity Services
App Protection Services
App Delivery Services
Network Monitoring Services
VNET
VNET Manager
Express Route
VPN Gateway
Virtual WAN
Azure DNS
Azure Bastion
NAT Gateway
Route Server
Peering Service


Connectivity Services
App Protection Services
App Delivery Services
Network Monitoring Services
VNET
VNET Manager
Express Route
VPN Gateway
Virtual WAN
Azure DNS
Azure Bastion
NAT Gateway
Route Server
Peering Service
VM to VM
VNET to VNET
to Internet
to on-prem
to D365, M365, SaaS


Connectivity Services
App Protection Services
App Delivery Services
Network Monitoring Services
DDoS Protection
Private Link
Azure Firewall
WAF
NSG
Service Endpoints
IP
Network


Connectivity Services
App Protection Services
App Delivery Services
Network Monitoring Services
AFD
Traffic Manager
Load Balancer
AppGW
CDN


Connectivity Services
App Protection Services
App Delivery Services
Network Monitoring Services
Network Watcher
Monitor
ExpressRoute Monitor
Network Insights


Connectivity Services
VNET
VM to VM
VNET to VNET
to Internet
to on-prem
VNET Manager
Express Route
VPN Gateway
Virtual WAN
Azure DNS
Azure Bastion
NAT Gateway
Route Server
Peering Service
to D365, M365, SaaS
App Protection Services
DDoS Protection
IP
Network
Private Link
Azure Firewall
WAF
NSG
Service Endpoints
App Delivery Services
AFD
Traffic Manager
Load Balancer
AppGW
CDN
Network Monitoring Services
Network Watcher
Monitor
ExpressRoute Monitor
Network Insights

Networking Fundamentals

High Level Azure Services

Experts Live Europe

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

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

Media/CDN

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

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

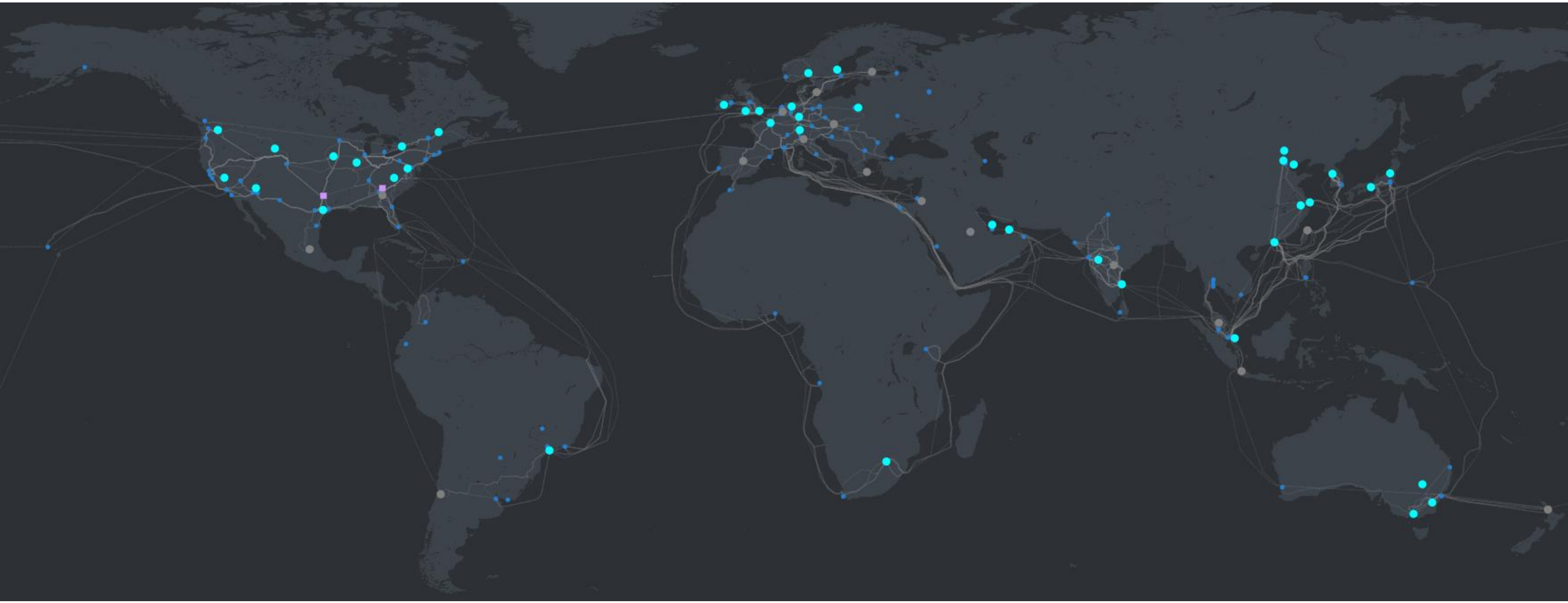
Storage

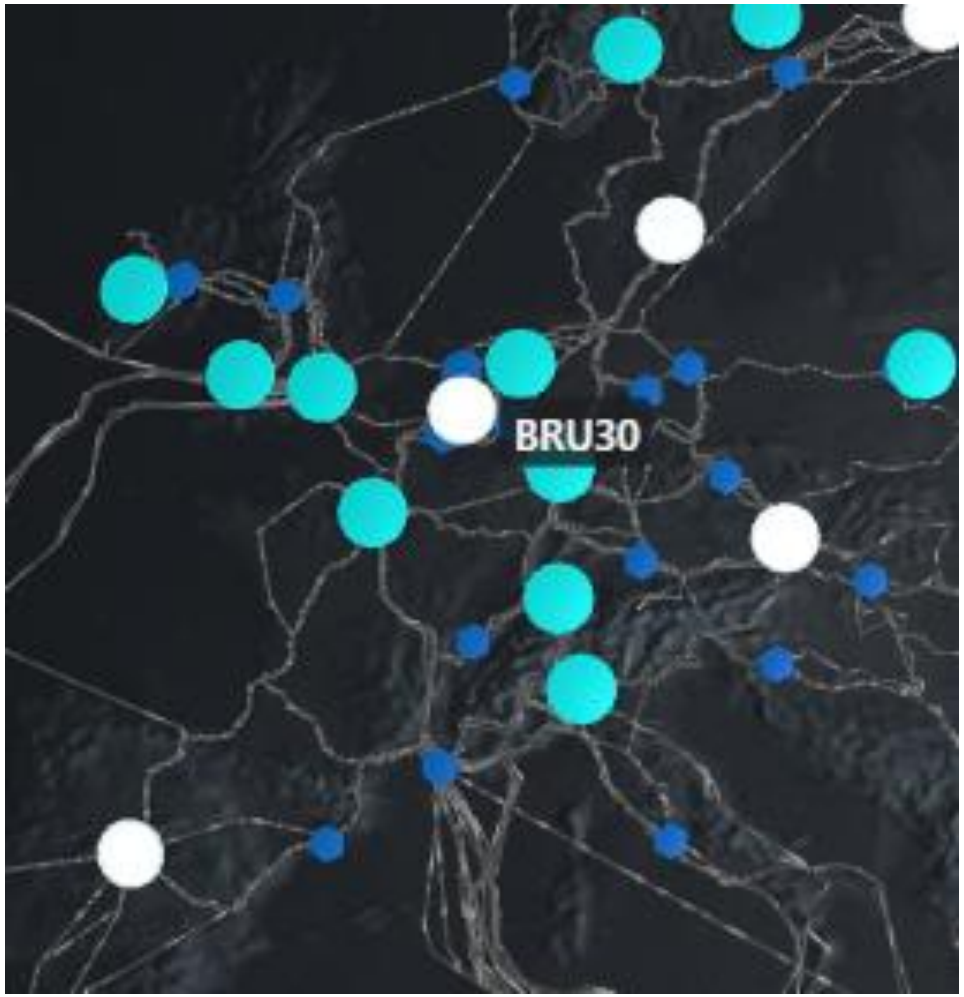
- Disk Storage
- Managed Disks

Networking

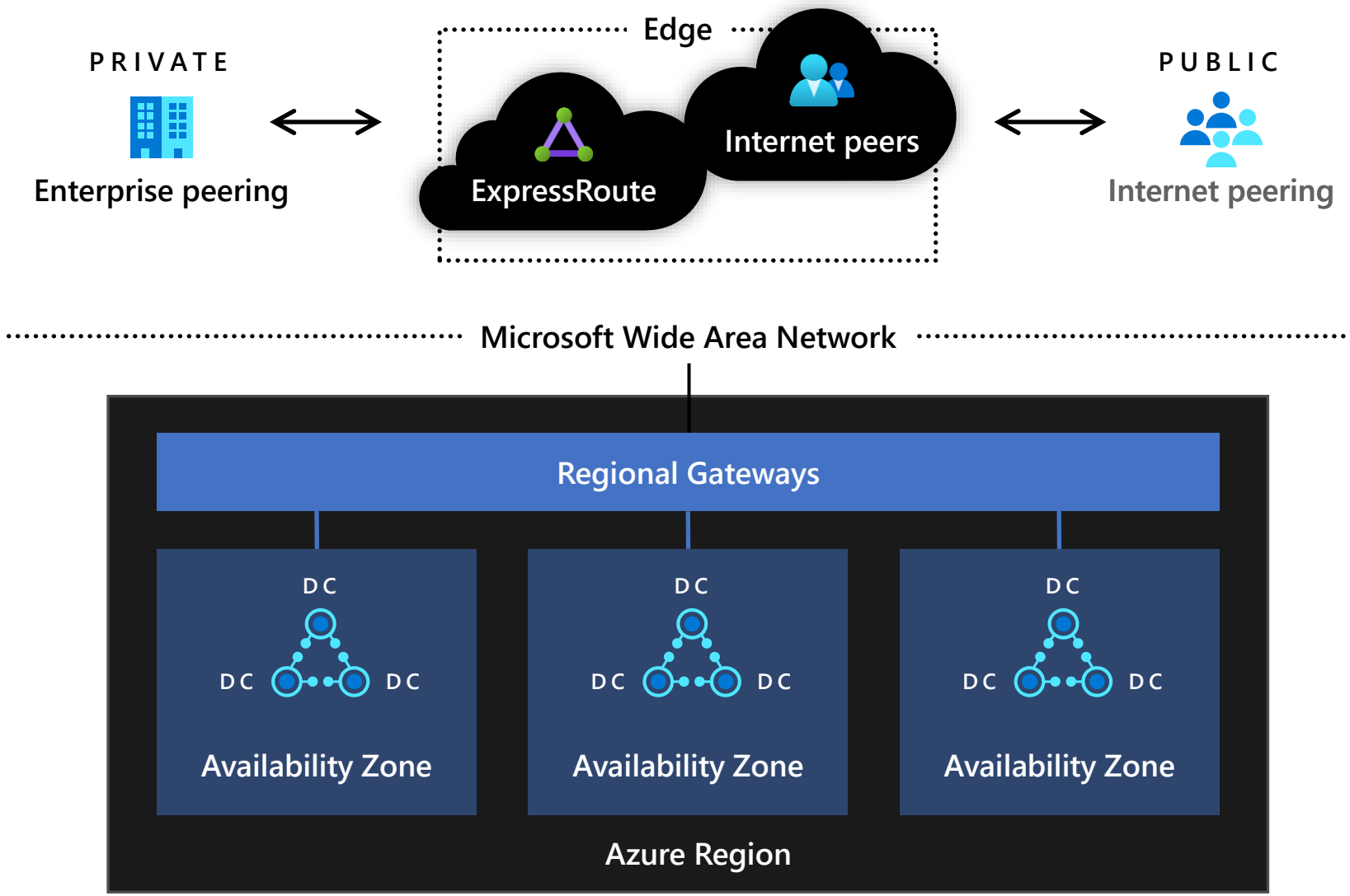
- Virtual Network
- VPN Gateway
- Express Route
- Load Balancer
- Azure Firewall
- Virtual WAN
- Network Watcher

Azure Datacenter Infrastructure

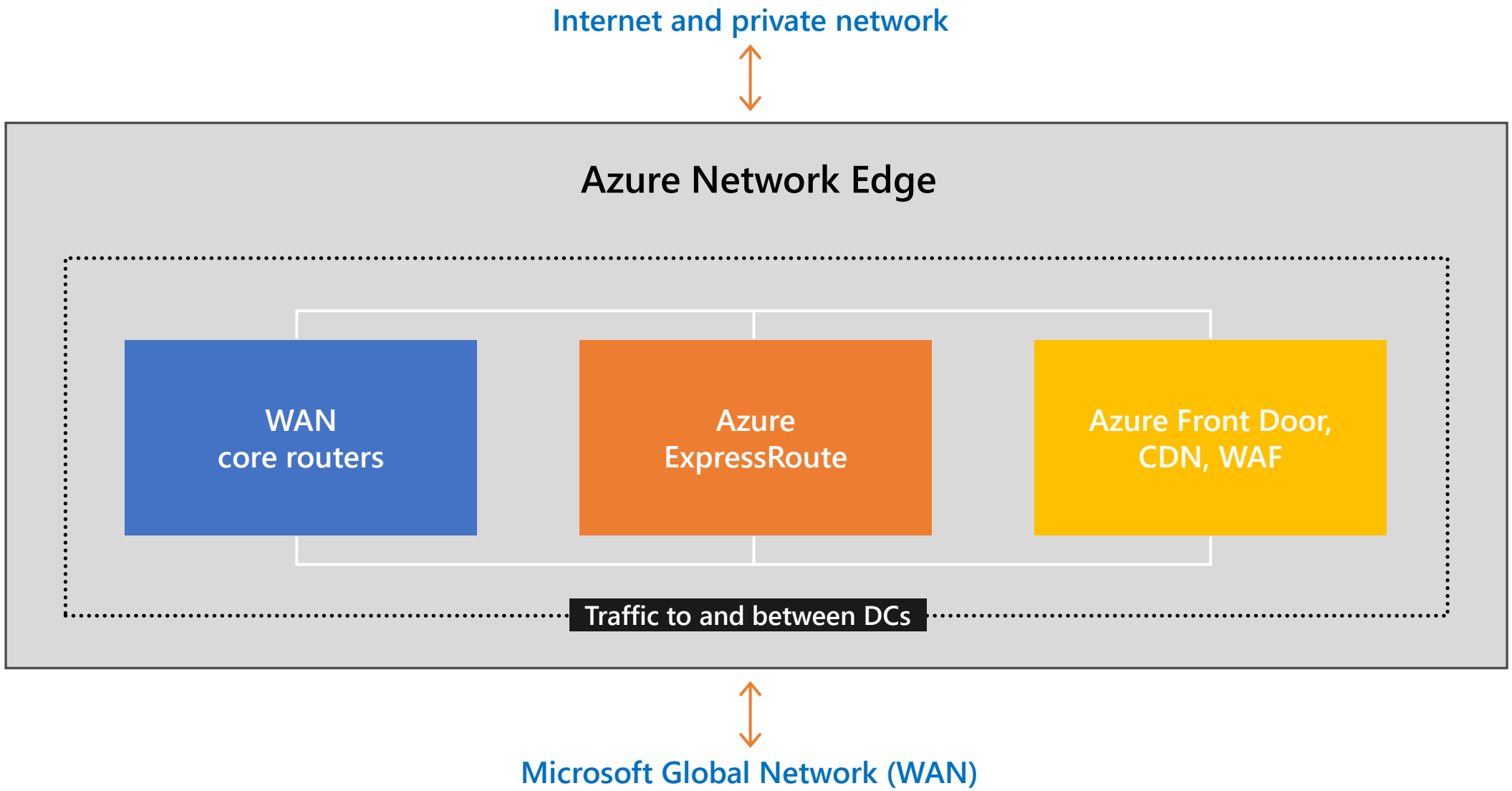



BRU30

Connecting Azure



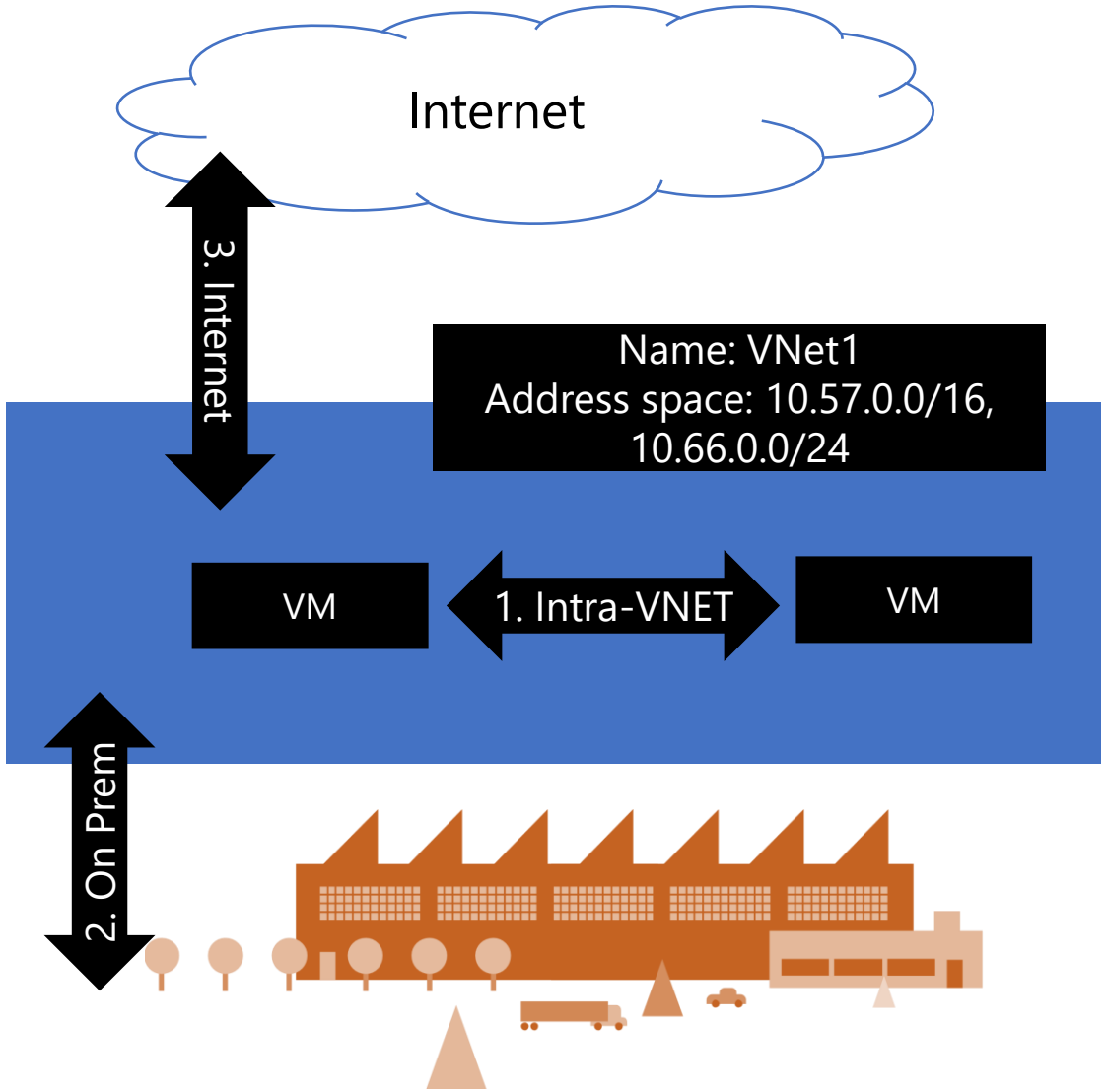
The Azure Network Edge



Networking Recap

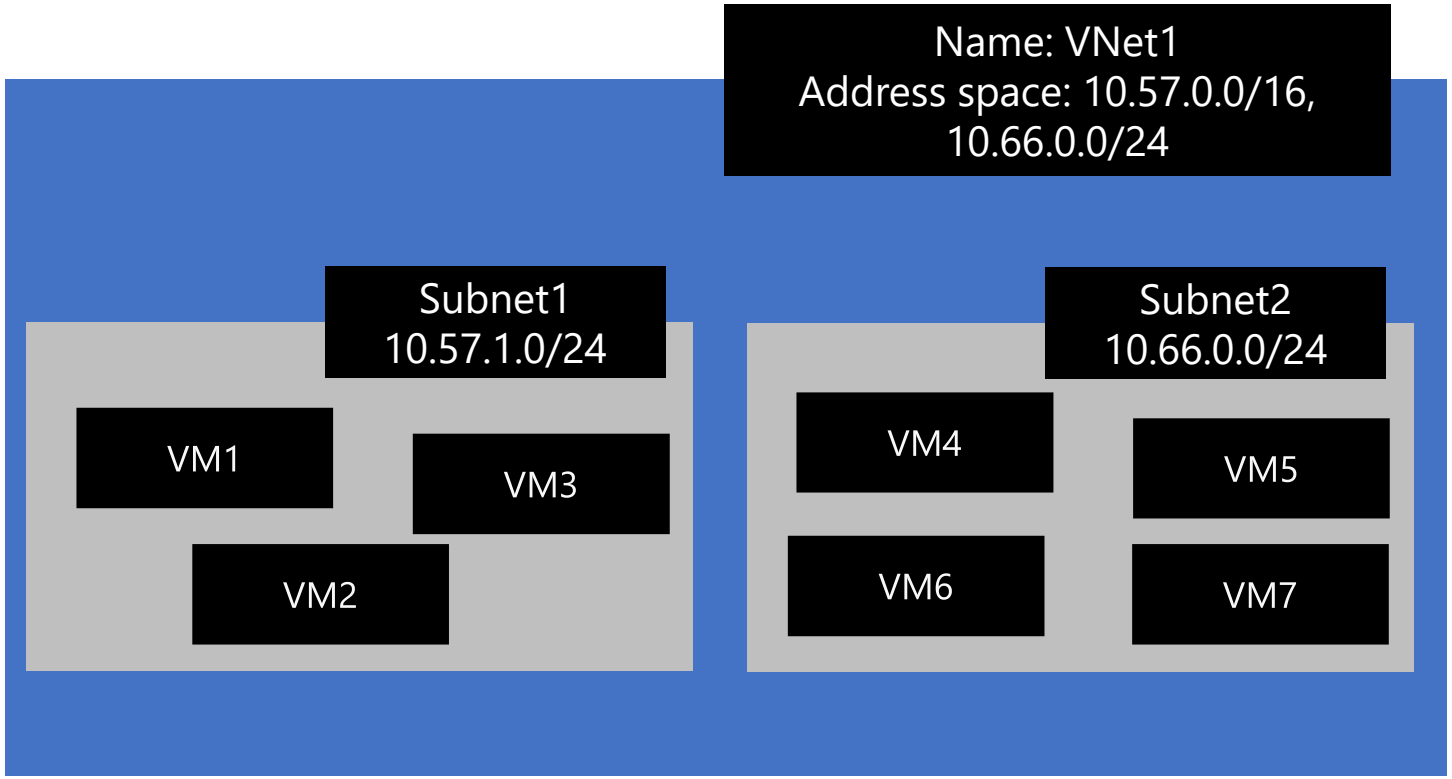
Virtual Network

- 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



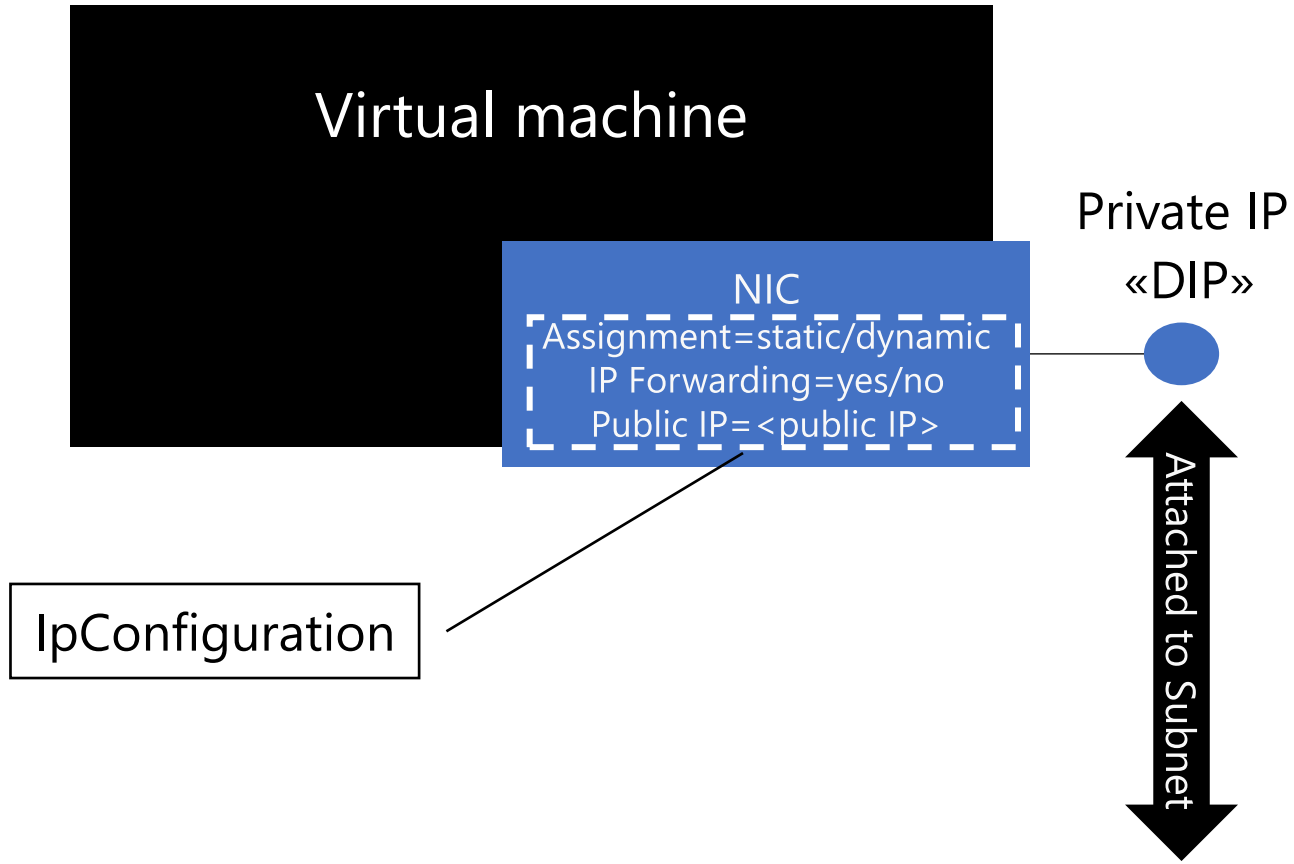
Subnet

- 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)



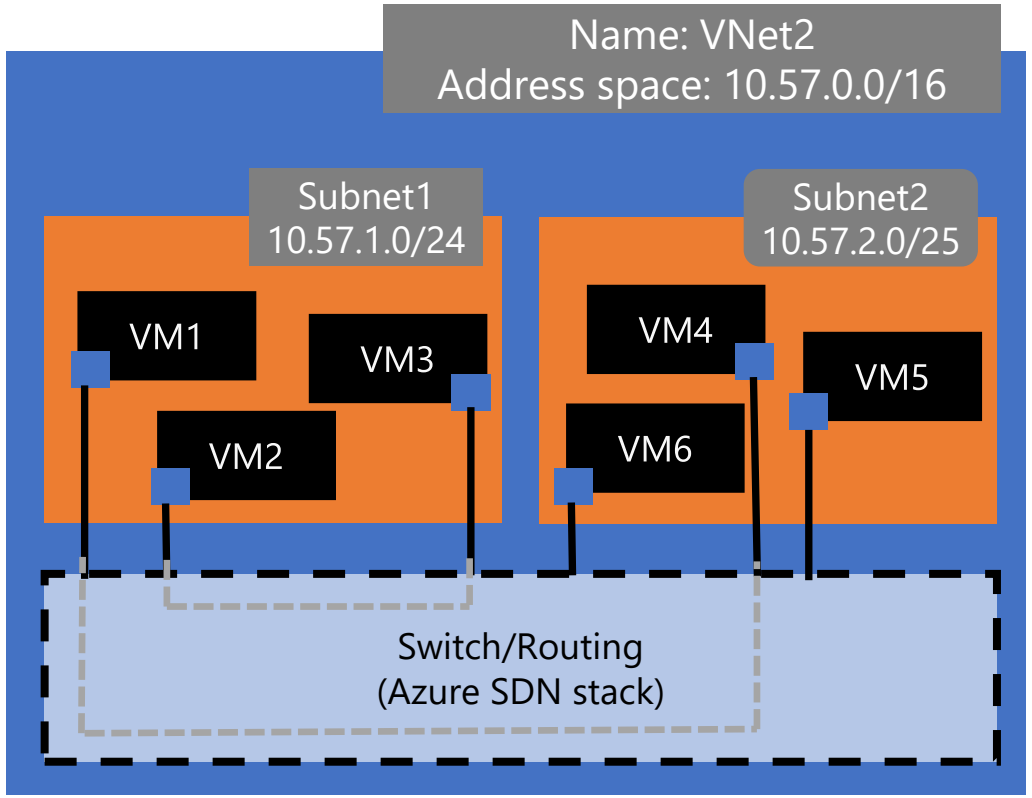
Network Interface

- 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

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

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

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

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

Media/CDN

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

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

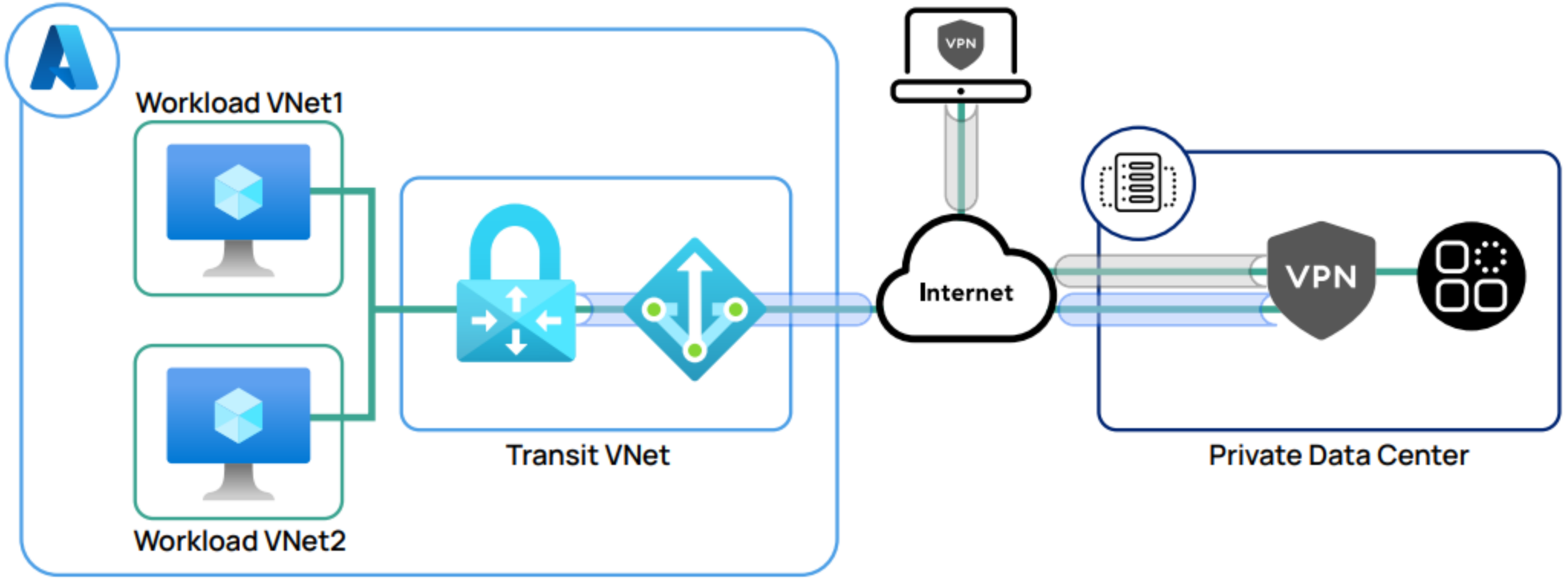
3rd Party Replacement(s)

Connectivity Services

- VNET
- VNET Manager
- Express Route
- VPN Gateway
- Virtual WAN
- Azure DNS
- Azure Bastion
- NAT Gateway
- Route Server
- Peering Service

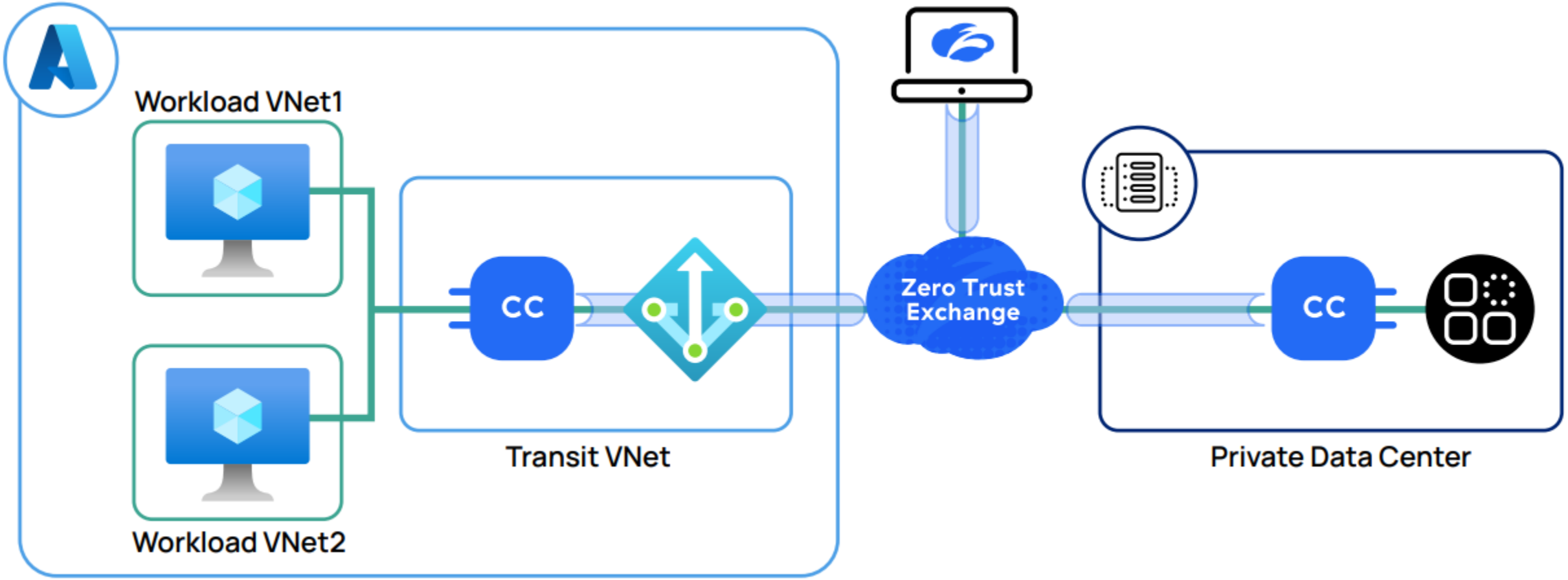
- None
- Management Console
- None … well …
- VPN / FW NVA
- SD-WAN but more complex
- Your DNS Server
- Any Secure Access Service
- Your NVA
- NVA but more complex
- None … well …

Example Zscaler



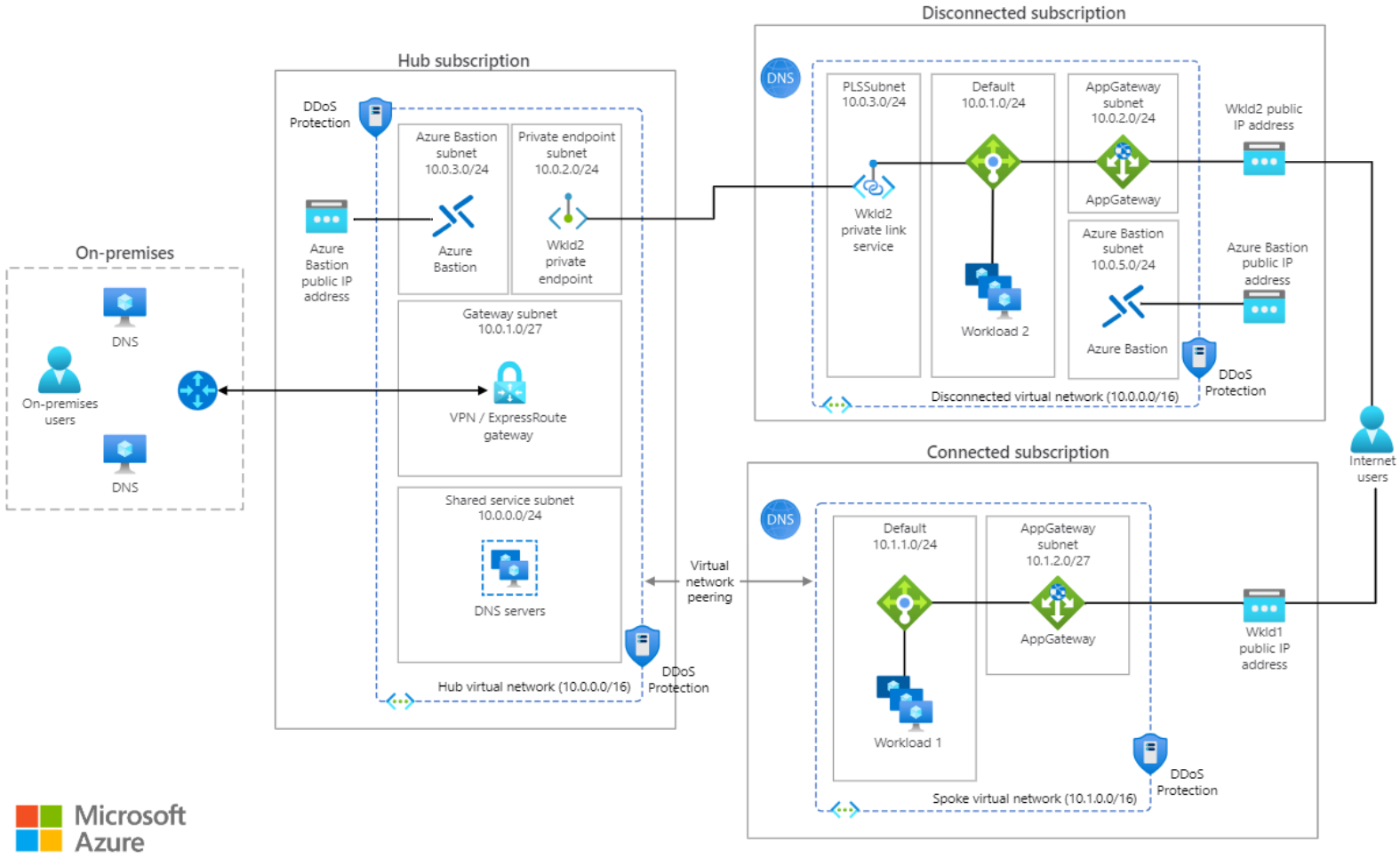
Source: Zero Trust for Private Apps in Miscrosoft Azure with ZPA (zscaler.com)

Example Zscaler

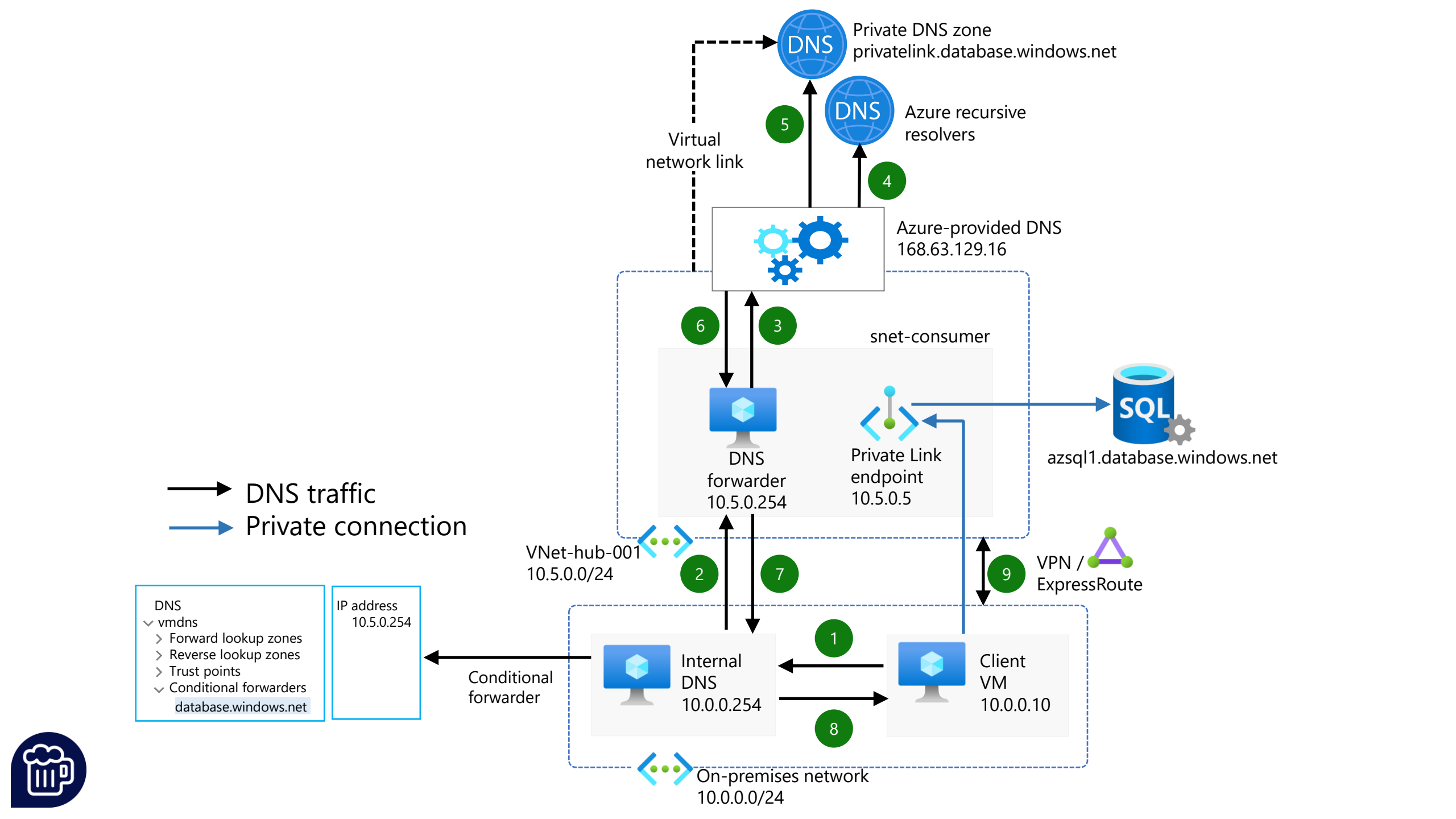


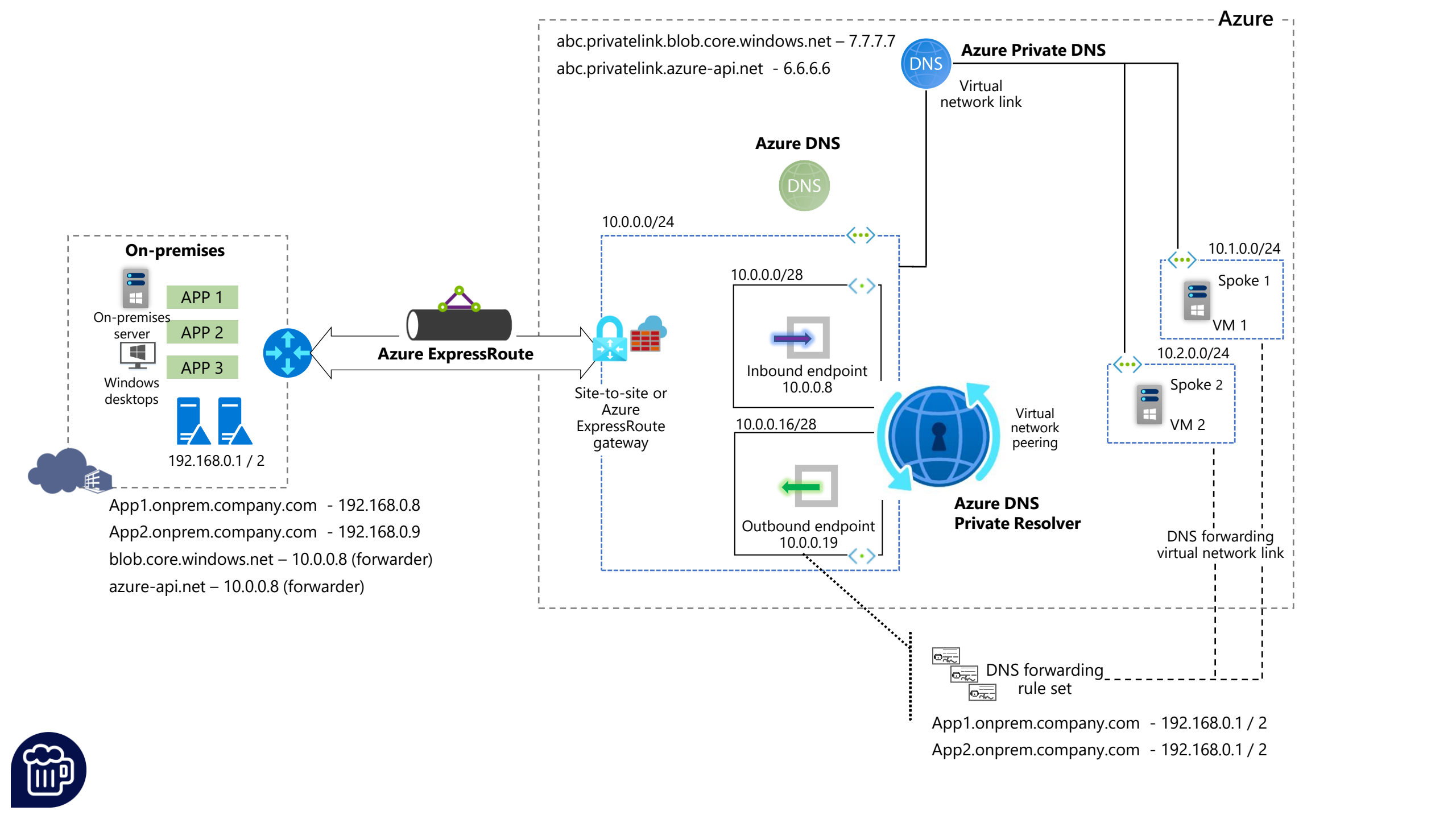
Source: Zero Trust for Private Apps in Miscrosoft Azure with ZPA (zscaler.com)

Example DNS



Source: [Design a hybrid Domain Name System solution with Azure - Azure Architecture Center]


Private DNS zone
privatelink.database.windows.net
Azure recursive
resolvers
Virtual
network link
Azure-provided DNS
168.63.129.16
snet-consumer
DNS
forwarder
10.5.0.254
Private Link
endpoint
10.5.0.5
azsql1.database.windows.net
DNS traffic
Private connection
VNet-hub-001
10.5.0.0/24
VPN /
ExpressRoute
DNS
vmdns
Forward lookup zones
Reverse lookup zones
Trust points
Conditional forwarders
database.windows.net
IP address
10.5.0.254
Conditional
forwarder
Internal
DNS
10.0.0.254
Client
VM
10.0.0.10
On-premises network
10.0.0.0/24


Azure
abc.privatelink.blob.core.windows.net – 7.7.7.7
abc.privatelink.azure-api.net - 6.6.6.6
Azure Private DNS
Virtual network link
Azure DNS
10.0.0.0/24
10.0.0.0/28
Inbound endpoint 10.0.0.8
10.0.0.16/28
Outbound endpoint 10.0.0.19
Azure DNS Private Resolver
Virtual network peering
10.1.0.0/24
Spoke 1
VM 1
10.2.0.0/24
Spoke 2
VM 2
DNS forwarding virtual network link
DNS forwarding rule set
App1.onprem.company.com - 192.168.0.1 / 2
App2.onprem.company.com - 192.168.0.1 / 2
On-premises
On-premises server
APP 1
APP 2
APP 3
Windows desktops
192.168.0.1 / 2
Azure ExpressRoute
Site-to-site or Azure ExpressRoute gateway
App1.onprem.company.com - 192.168.0.8
App2.onprem.company.com - 192.168.0.9
blob.core.windows.net – 10.0.0.8 (forwarder)
azure-api.net – 10.0.0.8 (forwarder)

App Protection Services

- DDoS Protection
- Private Link
- Azure Firewall
- WAF
- NSG
- Service Endpoints

- CloudFlare
- None
- Any NVA
- Any NVA
- None … well …
- None

Exa

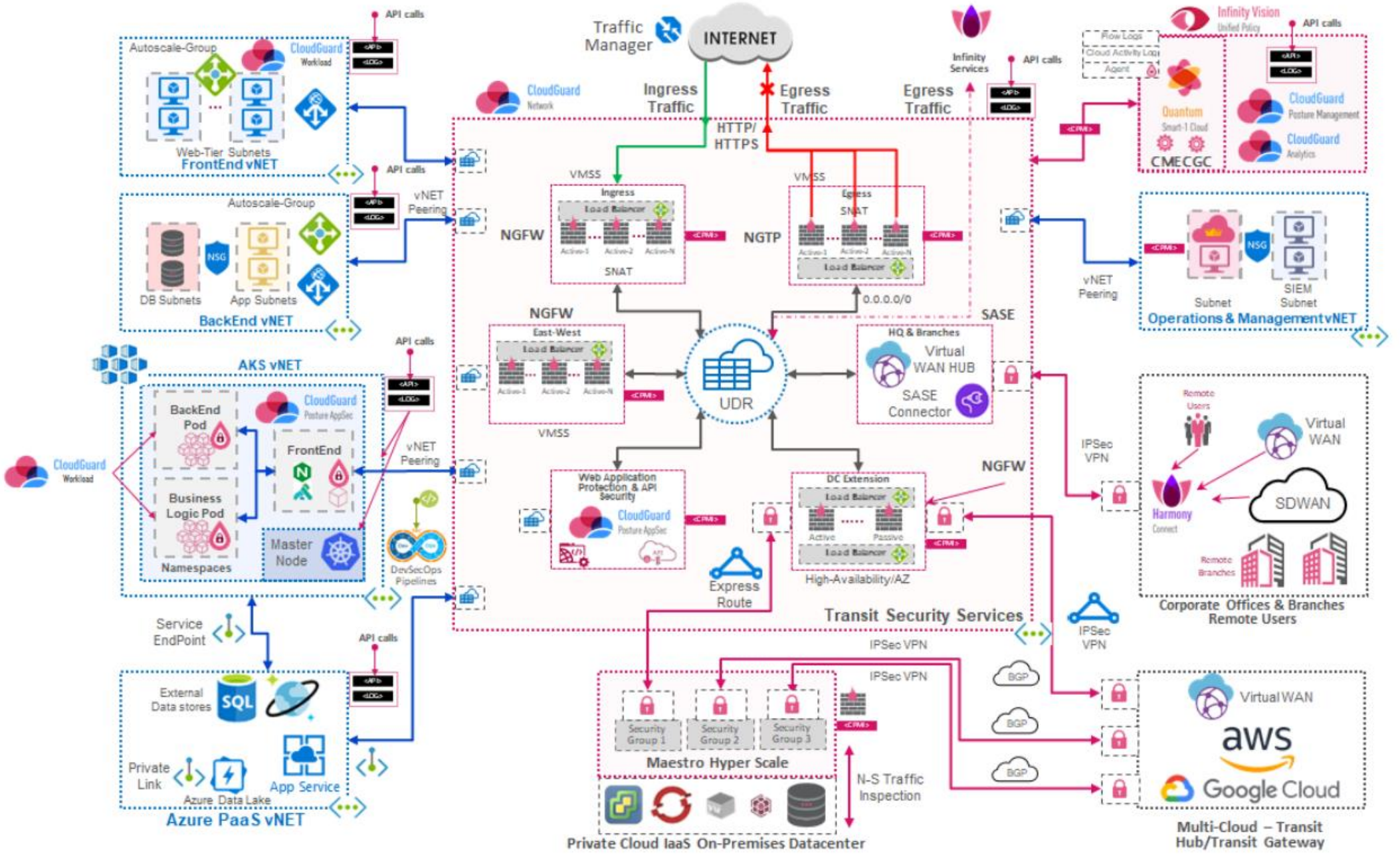


Figure 16: *Reference Architecture for Microsoft Azure*

App Delivery Services

- Azure Front Door
- Traffic Manager
- Load Balancer
- AppGW
- CDN
- Cloudflare
- F5 BIG-IP DNS
- KEMP
- NGINX
- Akamai

Example

FEATURES	AZURE	LOADMASTER
Basic and Standard Tier VM support	✗	✓
Network Level L4 load balancing	✓	✓
Multiple application access with single IP	Limited	✓
Pre-configured application templates	✗	✓
Web User Interface for ease of management	Limited	✓
High Availability & Clustering	Limited	✓
Hybrid Traffic Distribution	✓	✓ (with advanced traffic distribution)
Scheduling methods	Round Robin Only	L4/L7
Server Persistence	Limited	✓L4/L7(Advanced options)
SSL Termination/Offload	Limited	✓
Content Caching/Compression	✗	✓
Least Connection Scheduling	✗	✓

Source: Azure Load Ba r, Application Gateway -

Network Monitoring Services

- Network Watcher
- Monitor
- ExpressRoute Monitor
- Network Insights

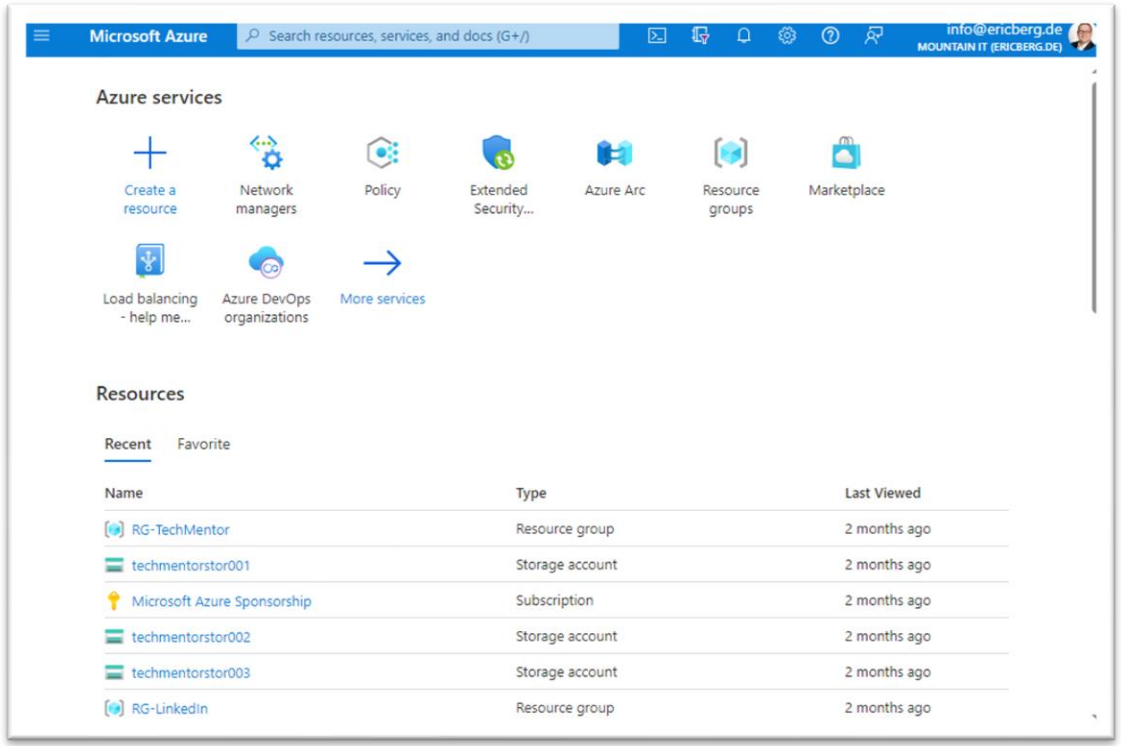
- 3rd Party Telemetry … but
- None at Azure Infra level
- None
- None at Azure Infra level

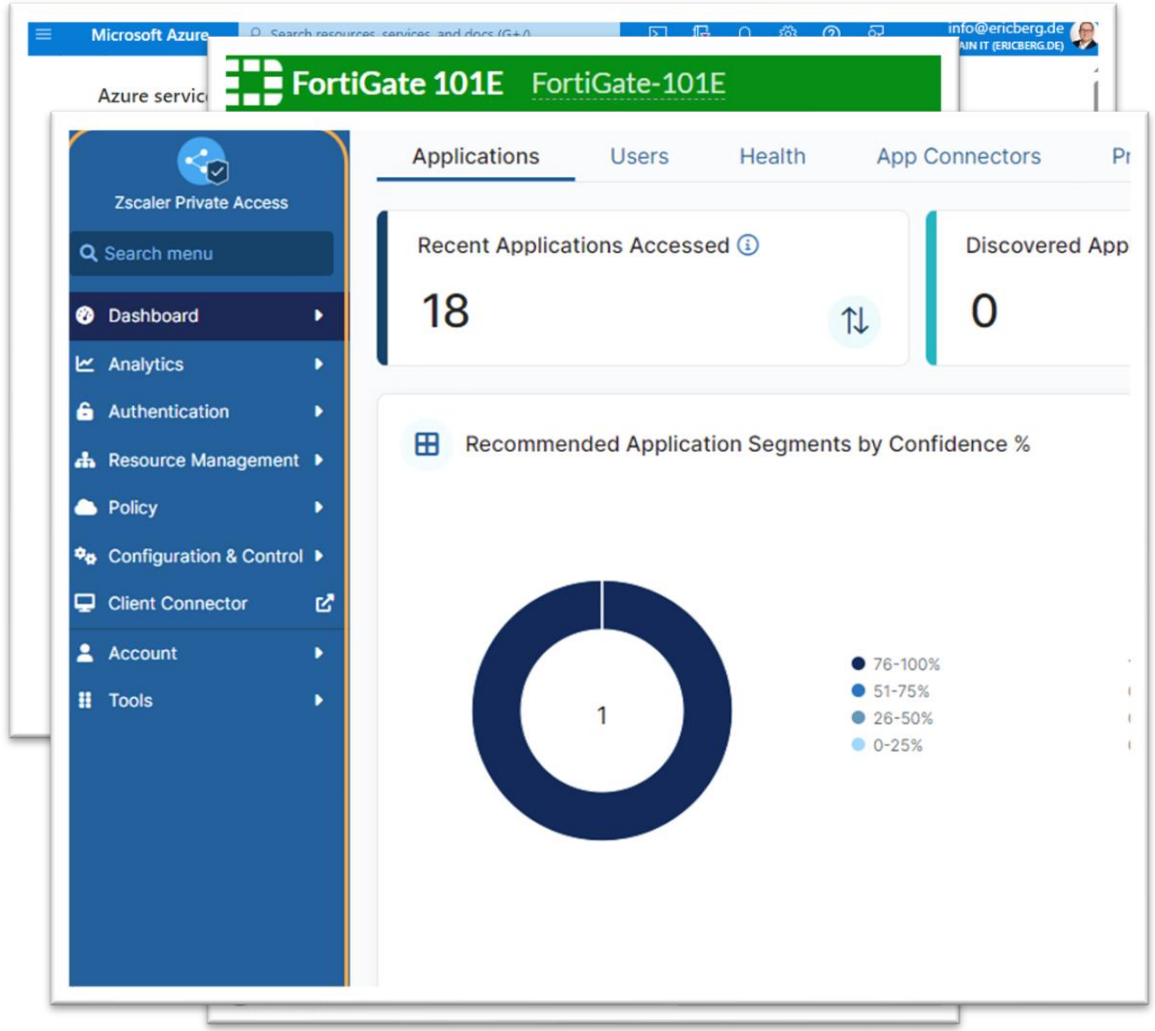
How to decide?!

Decision Criteria

- Cost considerations
- Scalability and Performance
- Security and Compliance
- Integration with Existing Infrastructure
- Ease of Use and Management
- Support and Maintenance
- Vendor Lock-in
- Regulatory Requirements

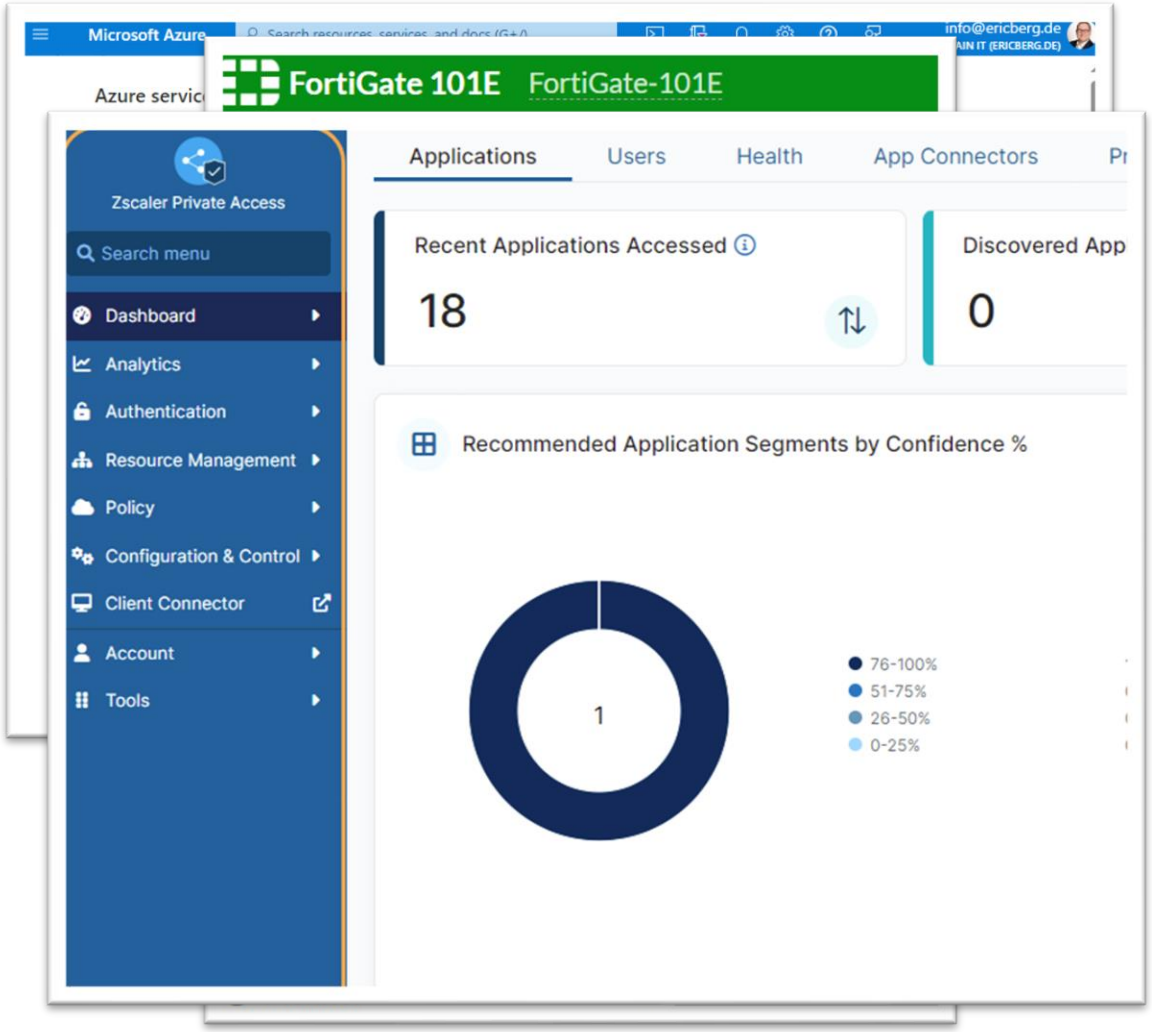
Think about the “Features”



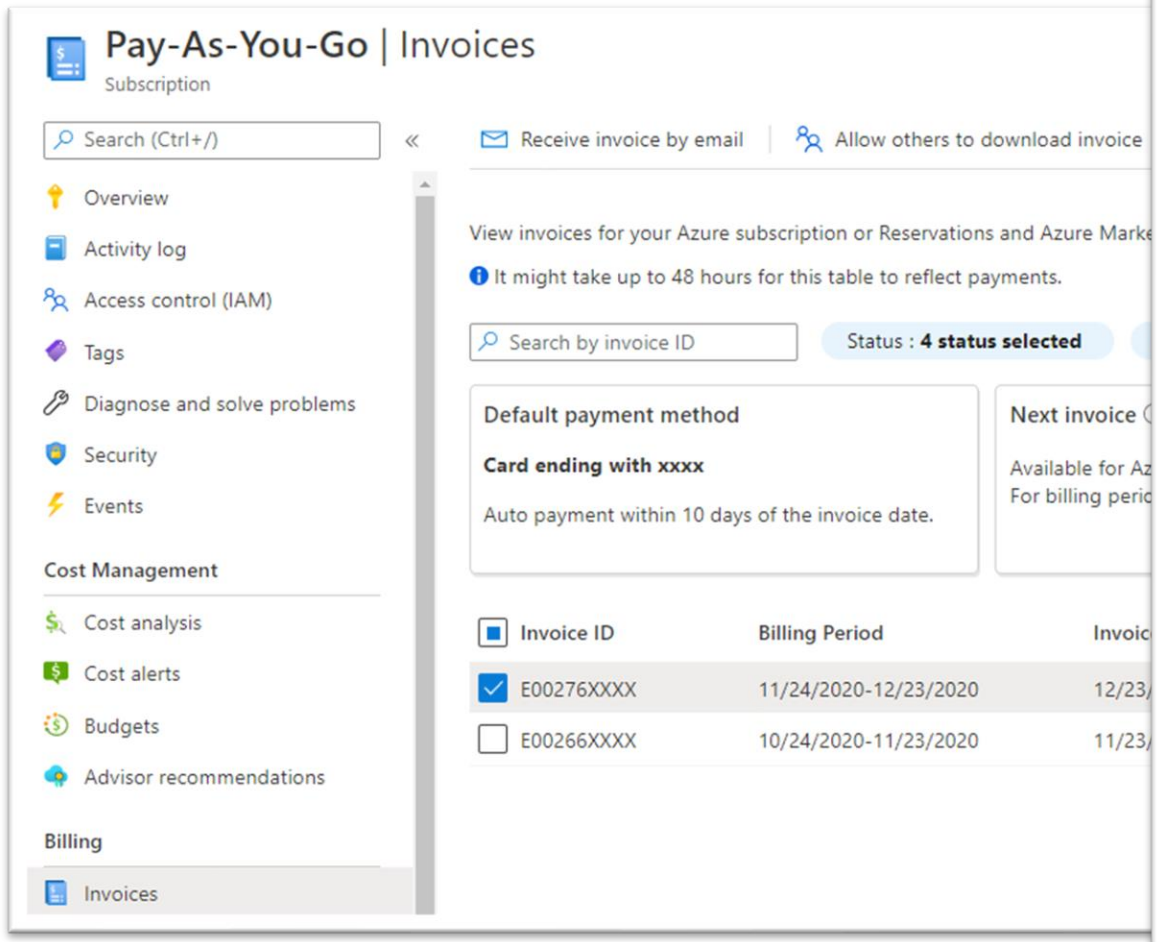


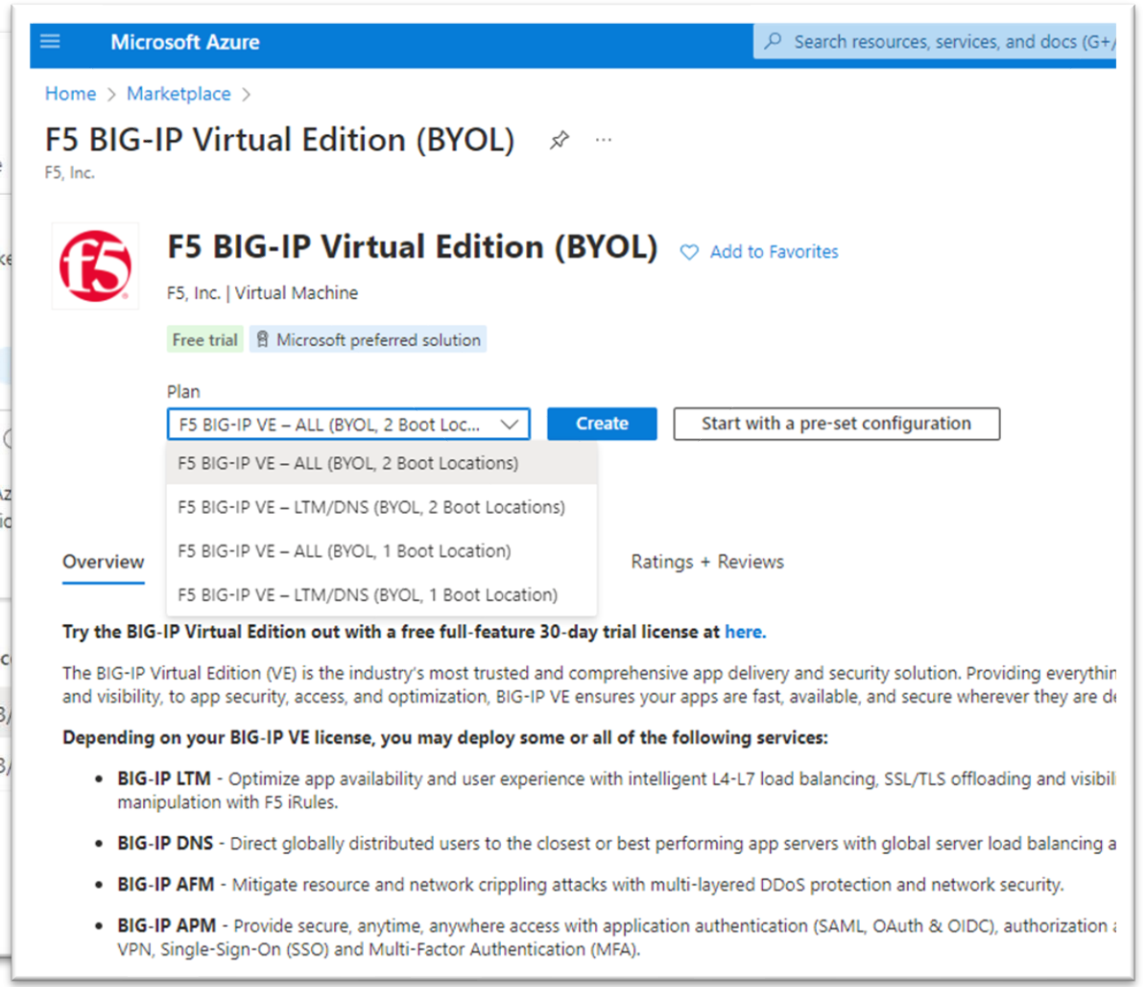
Think about the “Management”

```
# VNET SHI
resource "azurerm_virtual_network" "vnet_shi" {
  name                = "vnet-shi"
  location            = azurerm_resource_group.rg_shi_network.location
  resource_group_name = azurerm_resource_group.rg_shi_network.name
  address_space       = ["10.101.0.0/16", "fd00:101::/48"]
  #dns_servers         = ["10.101.0.4"]
  tags = local.tags_shi
}

# Subnet for SHI Service
resource "azurerm_subnet" "snet_shi_service" {
  name                 = "snet-shi-service"
  address_prefixes     = ["10.101.0.0/24", "fd00:101::/64"]
  virtual_network_name = azurerm_virtual_network.vnet_shi.name
  resource_group_name  = azurerm_virtual_network.vnet_shi.resource_group_name
}

# Route Table for SHI
resource "azurerm_route_table" "rt_shitofw" {
  name                          = "rt-SHItoFW"
  location                      = azurerm_resource_group.rg_shi_network.location
  resource_group_name           = azurerm_resource_group.rg_shi_network.name
  disable_bgp_route_propagation = false
  tags                          = local.tags_shi
}
```



Think about the “Cost”





Best Practices

- Hybrid Solutions: Combining Native & 3rd Party Tools
- Management & Integration
- Monitoring & Optimization
- Disaster Recovery & Redundancy
- Compliance & Governance

IT DEPENDS … BUT …

AXXES

Arxus

codit

delaware

devoteam

DEXMACH
A CEGEKA COMPANY

Microsoft

ORDINA

inetum realdolmen
Positive digital flow

proximus

ZURE

Thank you partners!

Integration.team
Connecting anything, anytime, anywhere

NOEST

datarobots

JET BRAINS

U2U

THANK YOU!

QUESTIONS?