Azure
User group
Norway

Microsoft

Hub-Spoke VNETs in Azure.

Bastiaan Wassenaar – Oslo – 15.12.2022

Azure
User group Norway

Microsoft

Short introduction

Bastiaan Wassenaar
From The Netherlands → 2013 Norway (Bolstadøyri, Voss)

Working as an IT consultant ***(from home)***
Twitter: @BasWas
LinkedIn: /BasWas

MVP
Microsoft®
Most Valuable Professional

Before we start…

- Basic vnet knowledge
  - CIDR-range
  - Subnets
  - NSG’s
  - Basic peering knowledge

- If you think about doing this, team up! Especially with network engineers (if you’re not one).

Goal

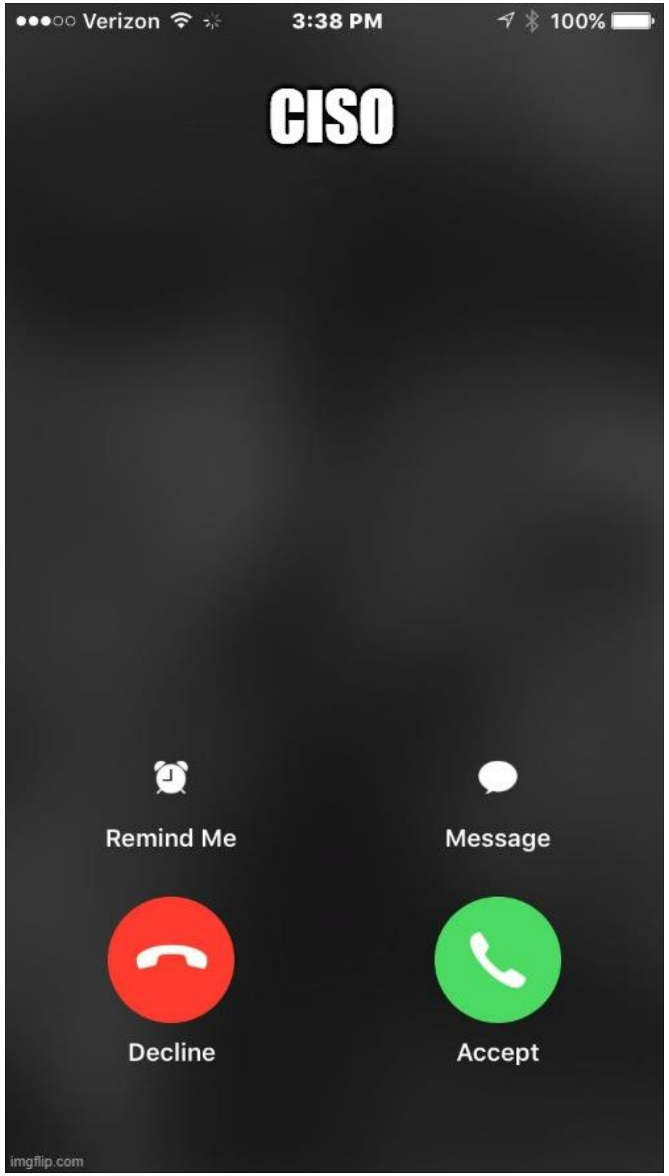
After this session you:

- Have a good basic understanding of the concept hub-spoke network.
- You understand where to start regarding your situation.
- Know where to look and learn further.

Agenda

- The history of vnets, service endpoints and private endpoints.
- Vnet peering (without hub-spoke)
- Hub-spoke building blocks
- Handling DNS

QUESTION:
WHY DO WE WANT THIS?
imgflip.com
memegenerator.net

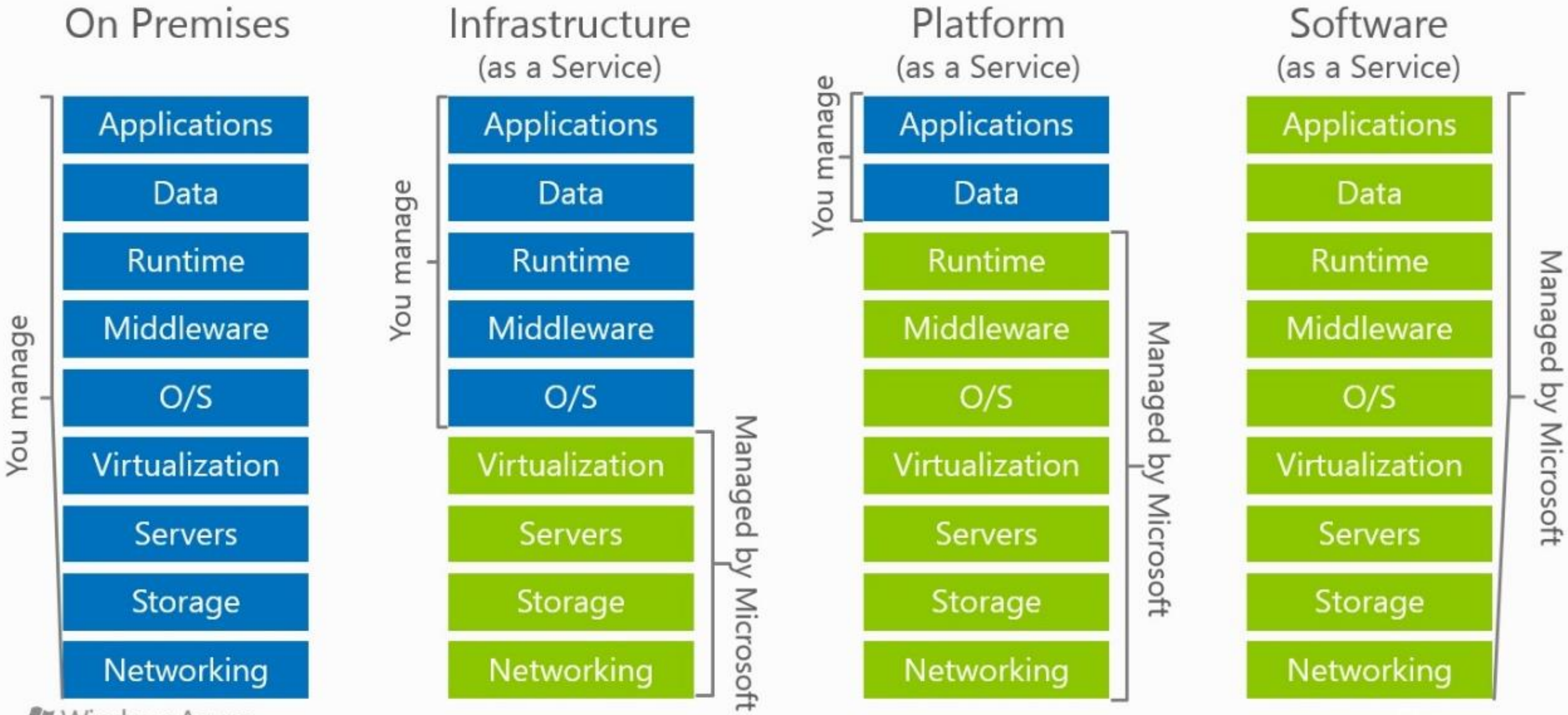

●●●○○ Verizon
3:38 PM
100%
CISO
Remind Me
Message
Decline
Accept
imgflip.com

But there are other reasons as well…

- Compliance related
- Connecting from on-premises networks
- Cross tenant connectivity

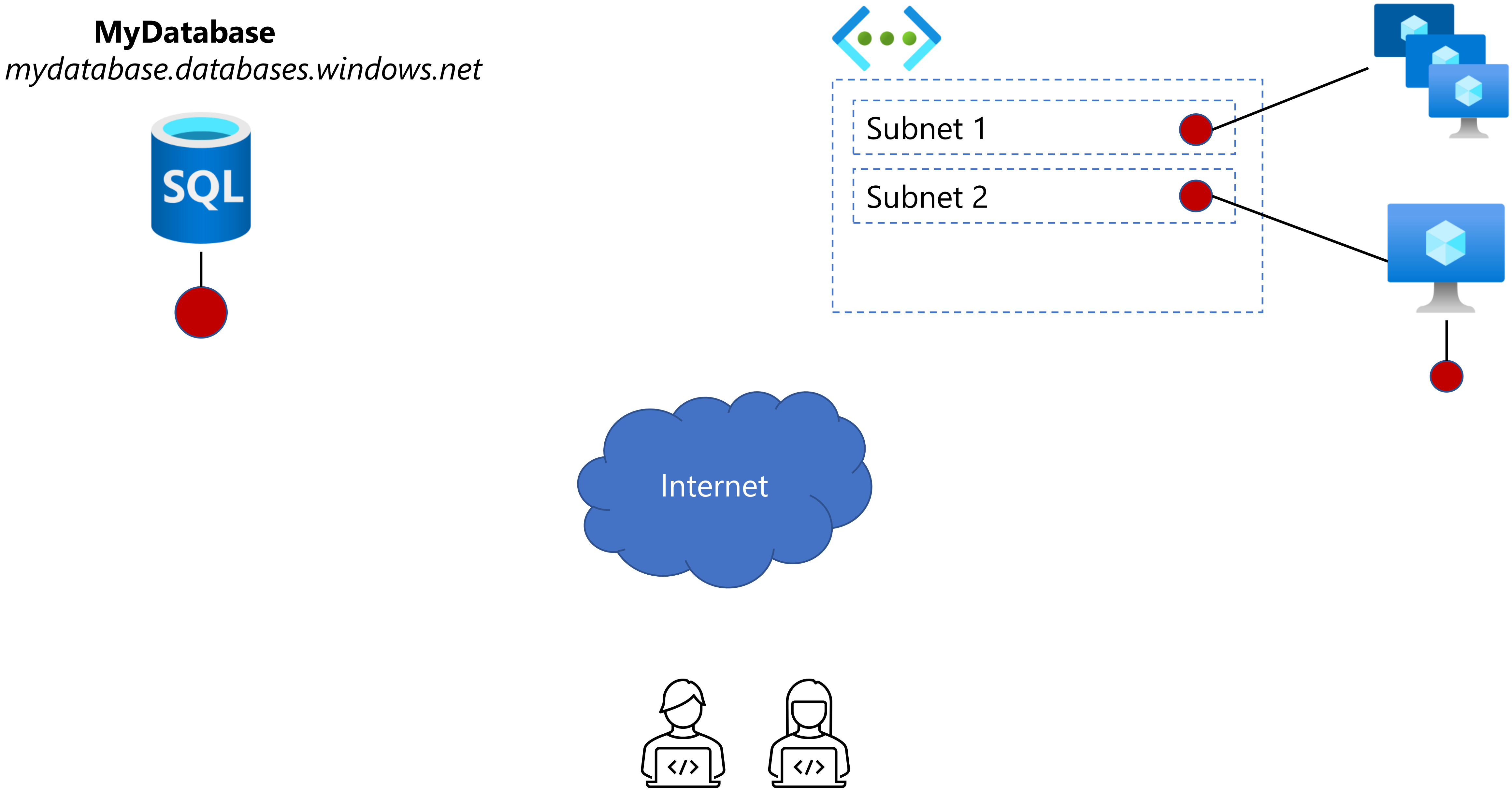
In the beginning. . .

Cloud Models



On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Windows Azure



MyDatabase

mydatabase.databases.windows.net

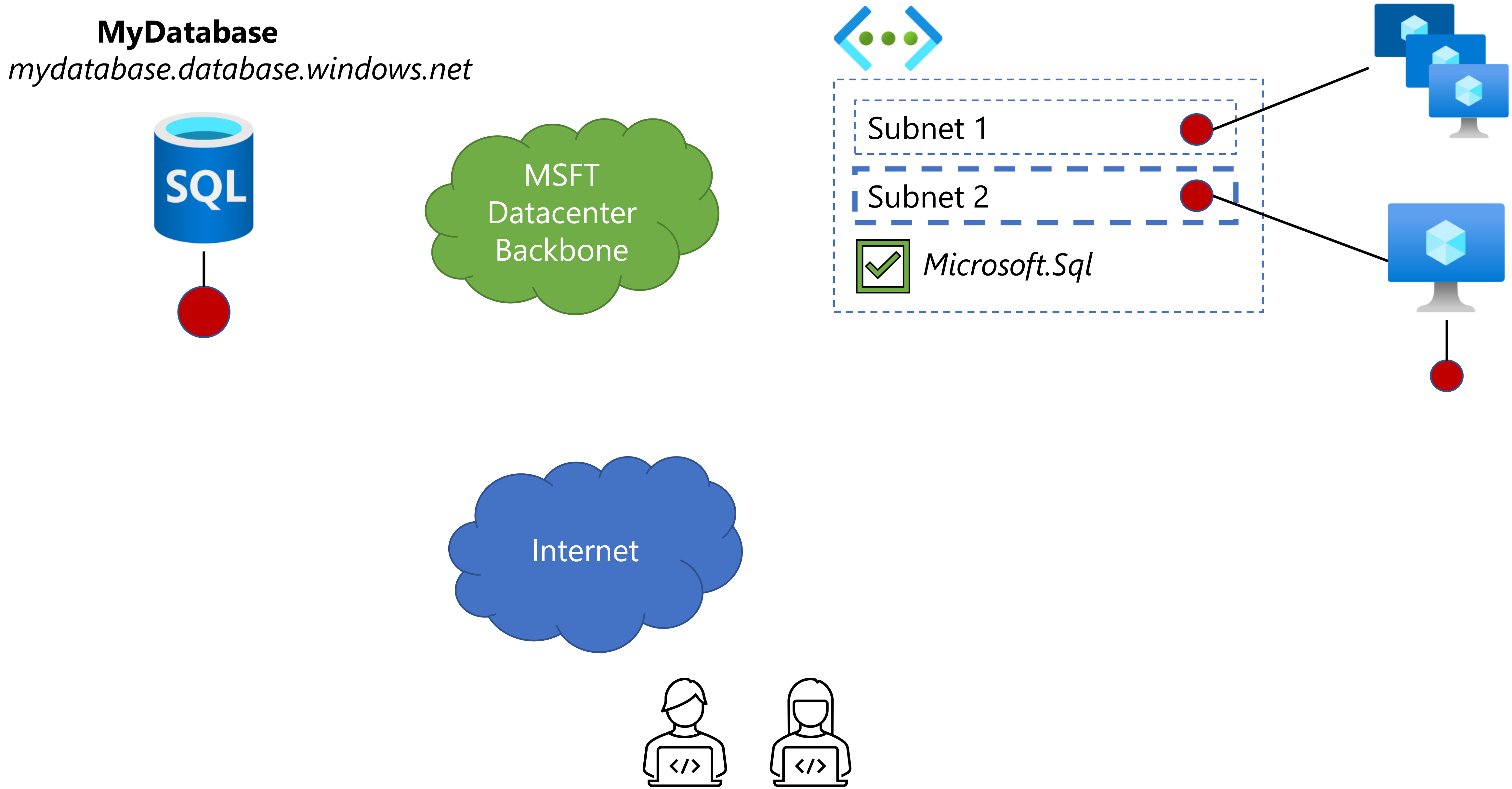
Subnet 1

Subnet 2

Internet

Cloud before *-endpoints

Service Endpoints



MyDatabase

mydatabase.database.windows.net

MSFT Datacenter Backbone

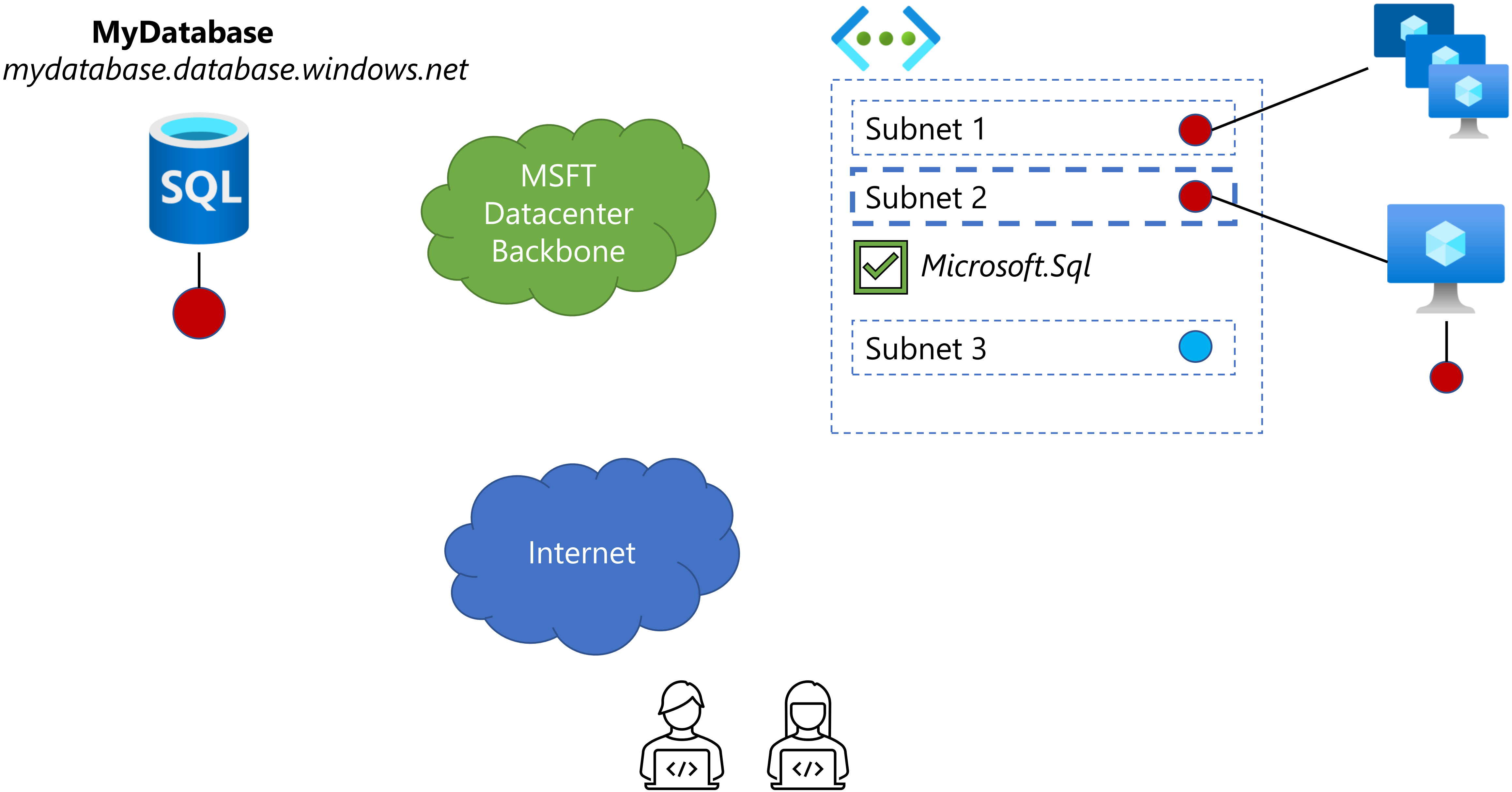
Subnet 1

Subnet 2

☑ *Microsoft.Sql*

Internet

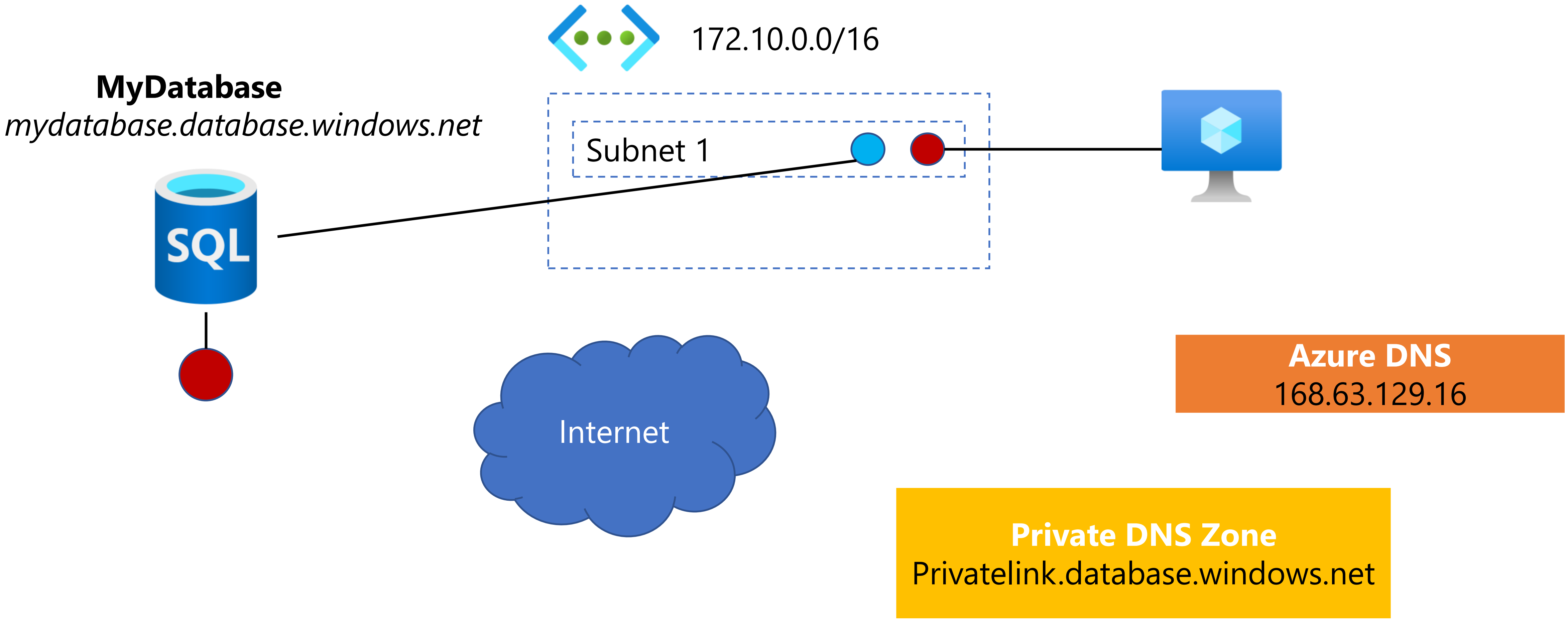
Private Endpoints



MyDatabase

mydatabase.database.windows.net

Private DNS Zones



MyDatabase

mydatabase.database.windows.net

172.10.0.0/16

Subnet 1

Internet

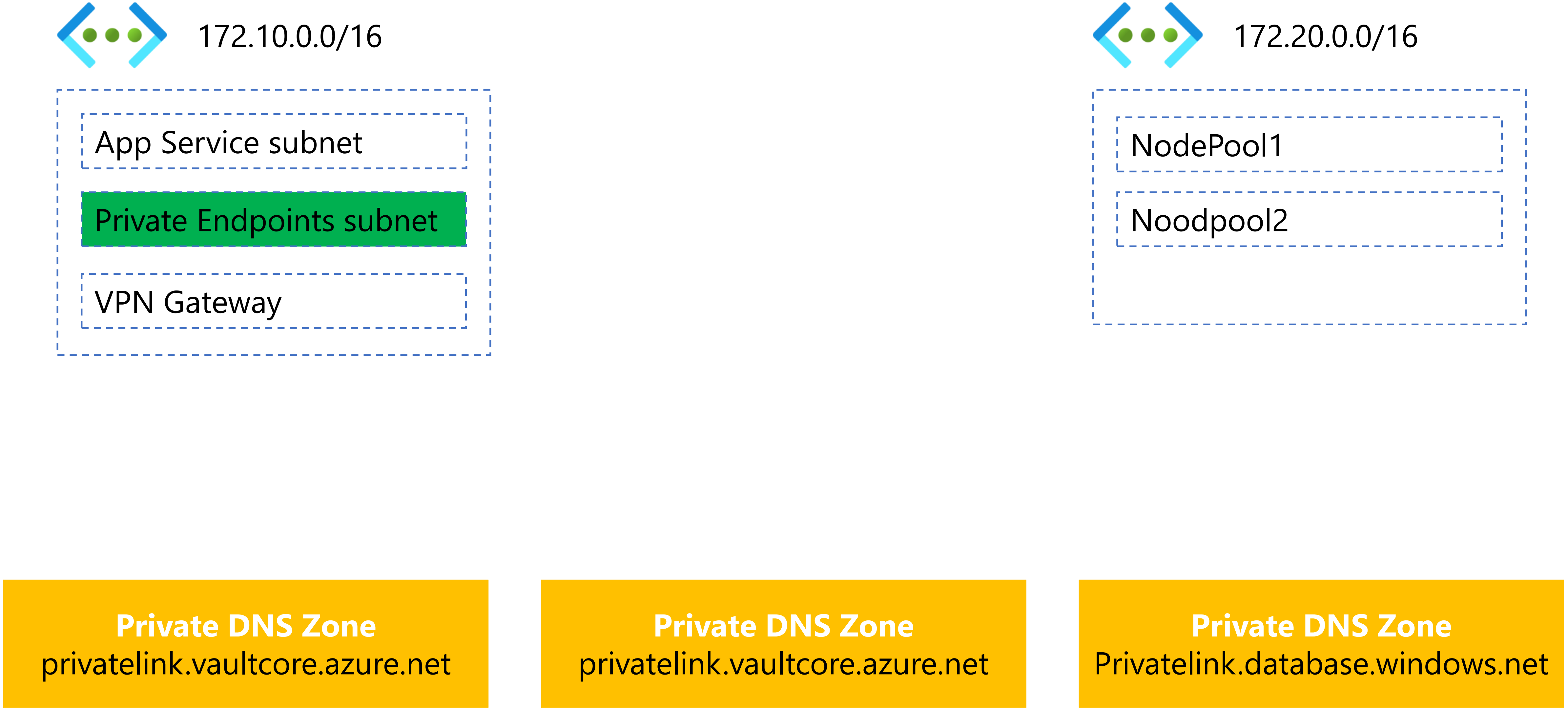
Azure DNS

168.63.129.16

Private DNS Zone

Privatelink.database.windows.net

VNET peering (without hub-spoke)



172.10.0.0/16

App Service subnet

Private Endpoints subnet

VPN Gateway

172.20.0.0/16

NodePool1

Noodpool2

Private DNS Zone
privatelink.vaultcore.azure.net

Private DNS Zone
privatelink.vaultcore.azure.net

Private DNS Zone
Privatelink.database.windows.net

VNET peering (without hub-spoke)

- 2 vnets, no worries
- 3-4 you can handle
- 5 or more gets complicated.

- Off course this all depends on your application / situation.

Hub-spoke building blocks

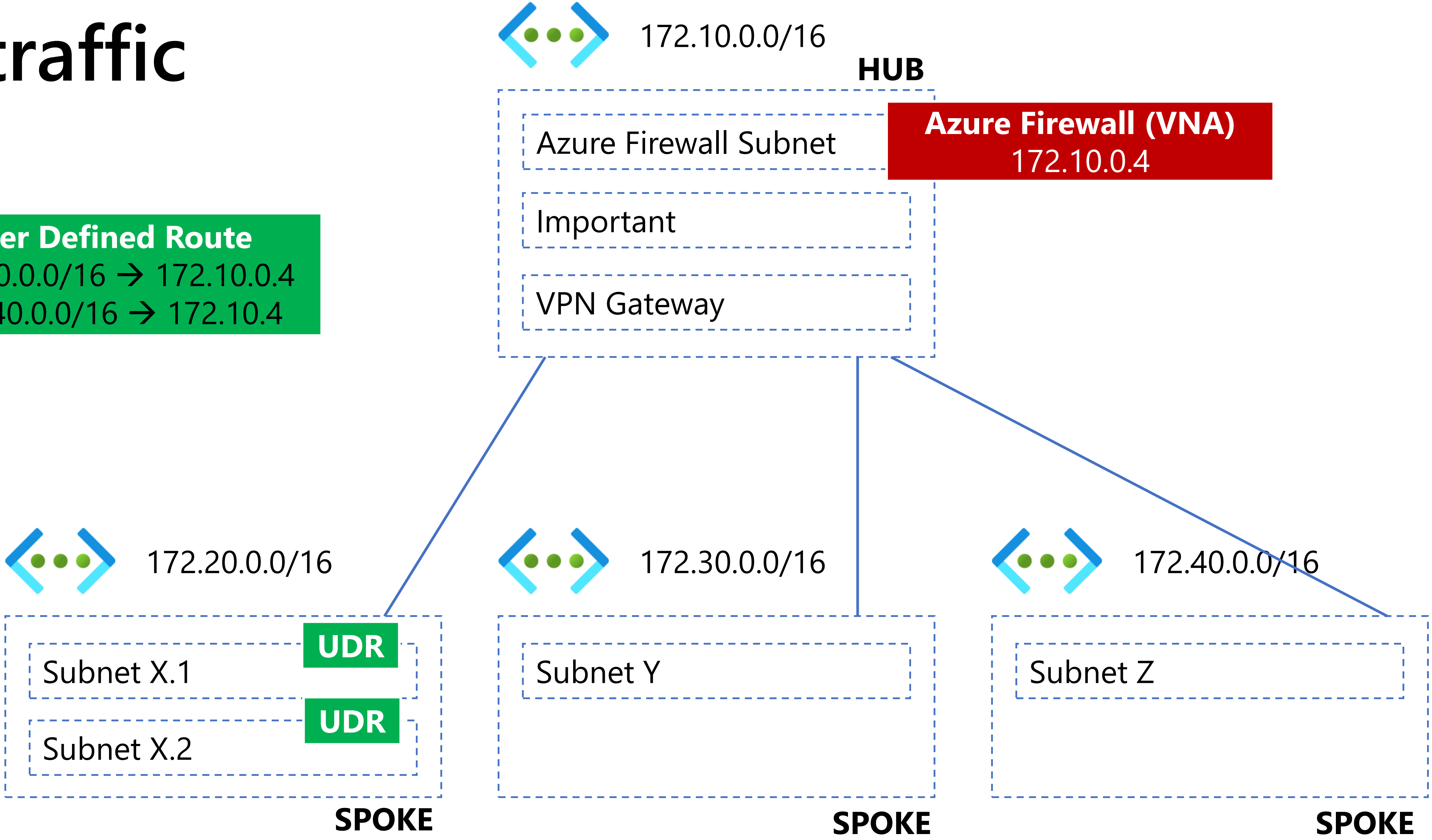
- VNA = Virtual Network Appliance (Azure Firewall, or vendor specific)
- UDR = User defined route (per subnet)
- Private DNS Zones
- Azure Policy / Landing Zones

Out of Scope today

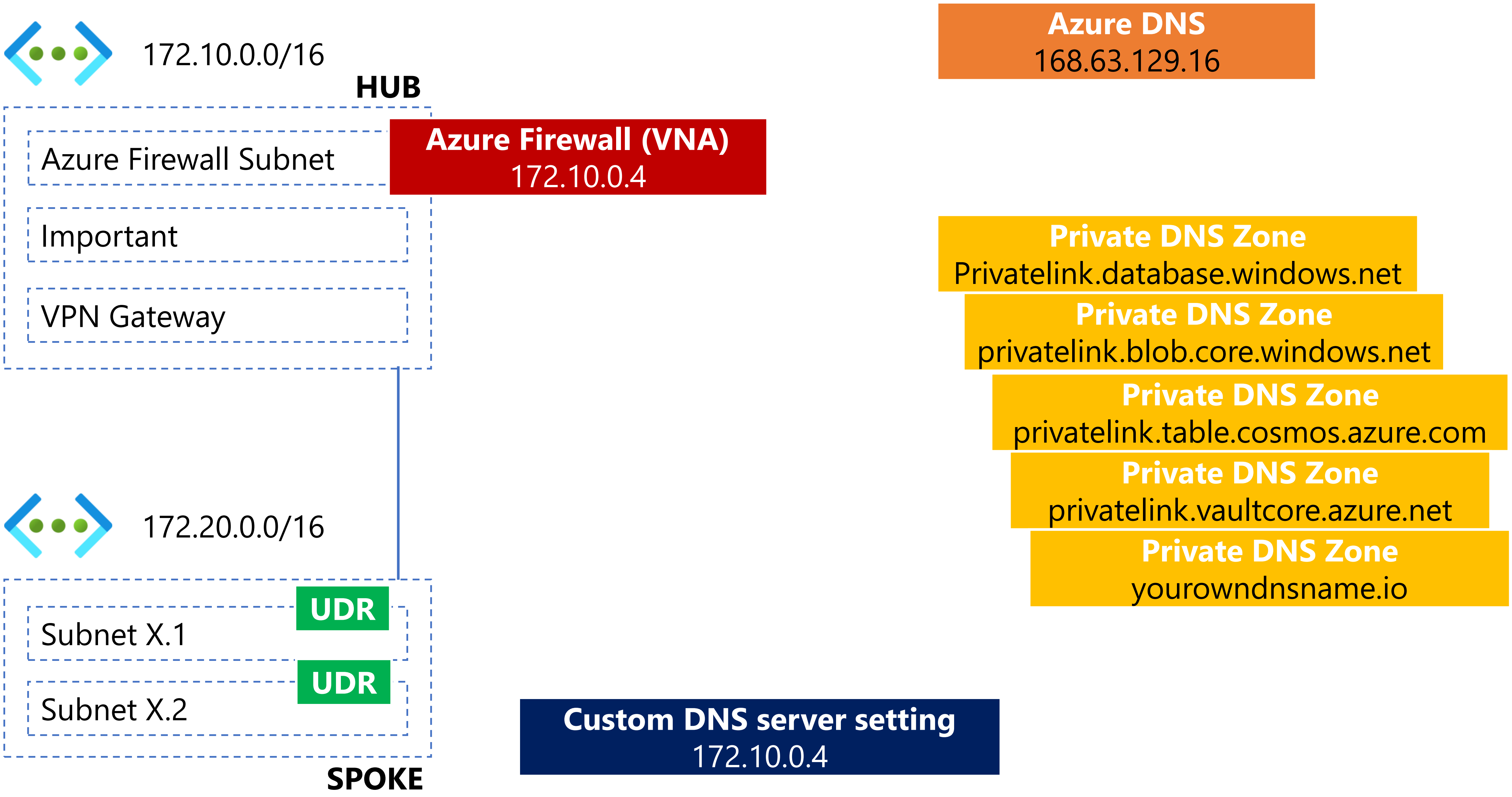
- On-prem connectivity and DNS (Azure DNS Private Resolver)
- Global virtual network peering

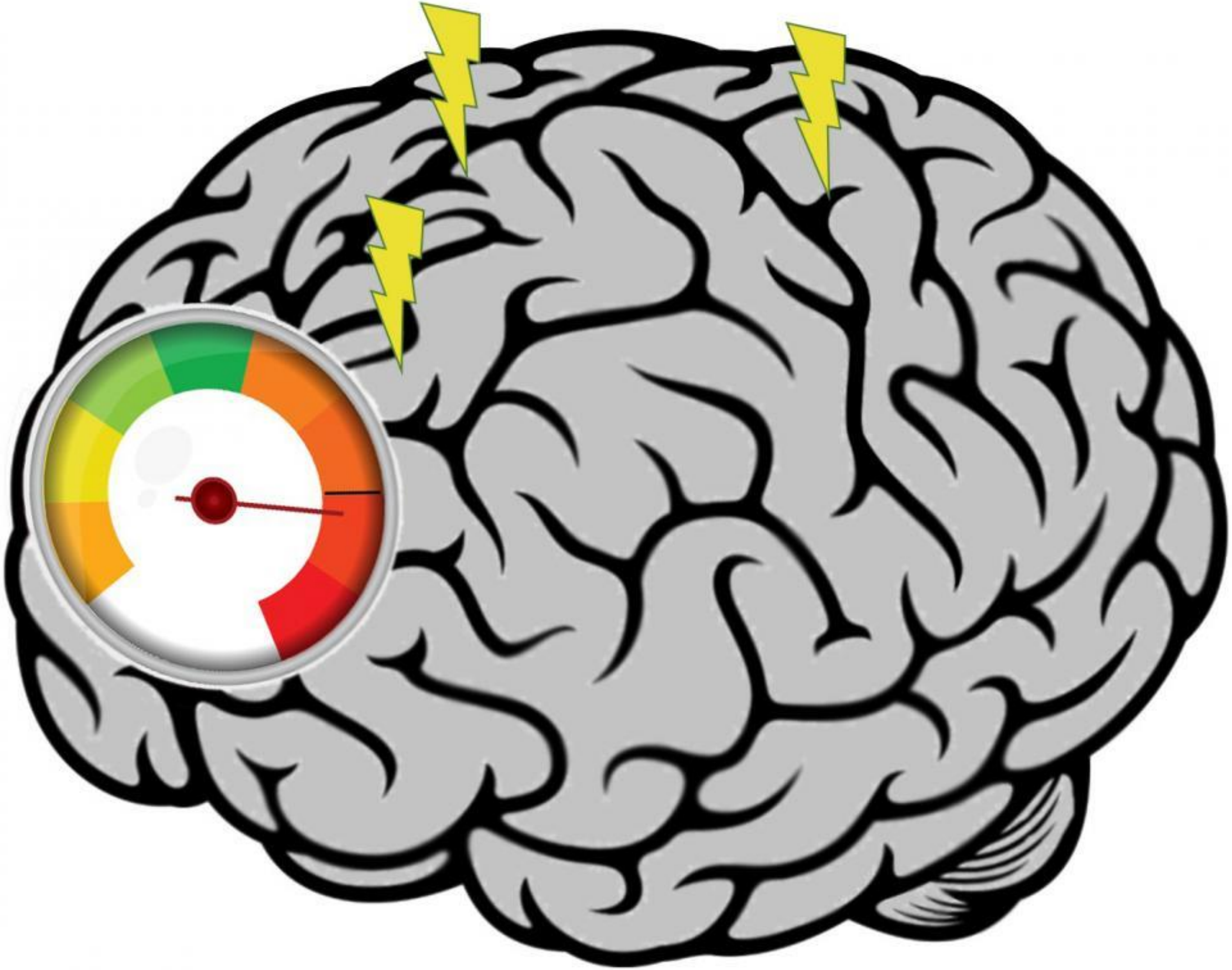
IP traffic

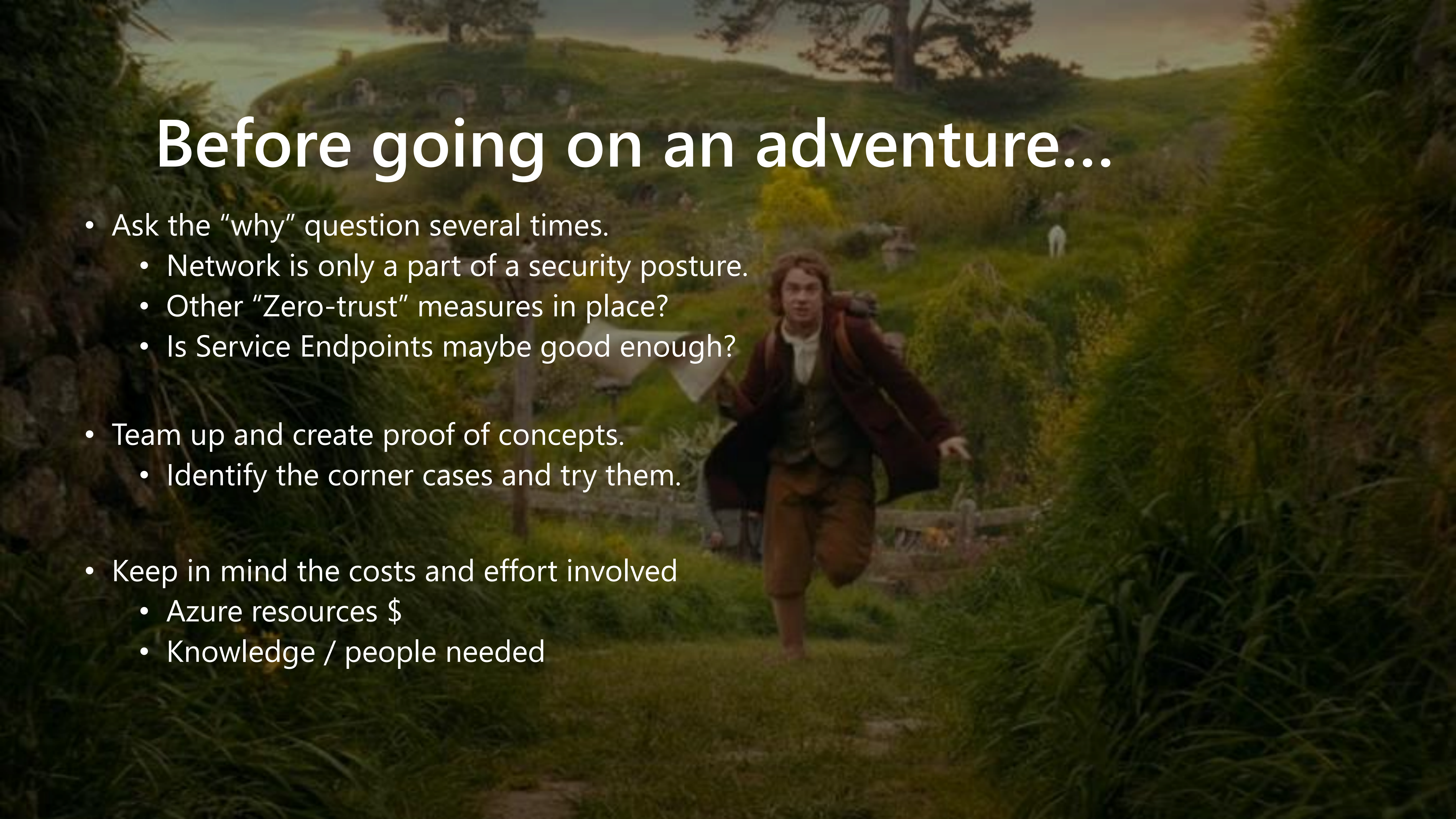
User Defined Route
172.30.0.0/16 → 172.10.0.4
172.40.0.0/16 → 172.10.4



DNS configuration







Before going on an adventure…

- Ask the “why” question several times.
  - Network is only a part of a security posture.
  - Other “Zero-trust” measures in place?
  - Is Service Endpoints maybe good enough?

- Team up and create proof of concepts.
  - Identify the corner cases and try them.

- Keep in mind the costs and effort involved
  - Azure resources $
  - Knowledge / people needed

Useful information

- John Savil’s Youtube channel
  - Complete Overview of Azure Virtual Network Peering - YouTube
  - Microsoft Azure Master Class Part 6 - Networking – YouTube
  - Understanding DNS in Azure - YouTube
  - Azure DNS Private Resolver Deep Dive - YouTube
- Microsoft Learn

Azure

User group

Norway

Thank you!

Microsoft