# Cloud DBAs new responsbilities - Network edition

Rune Ovlien Rakeie
Tietoevry



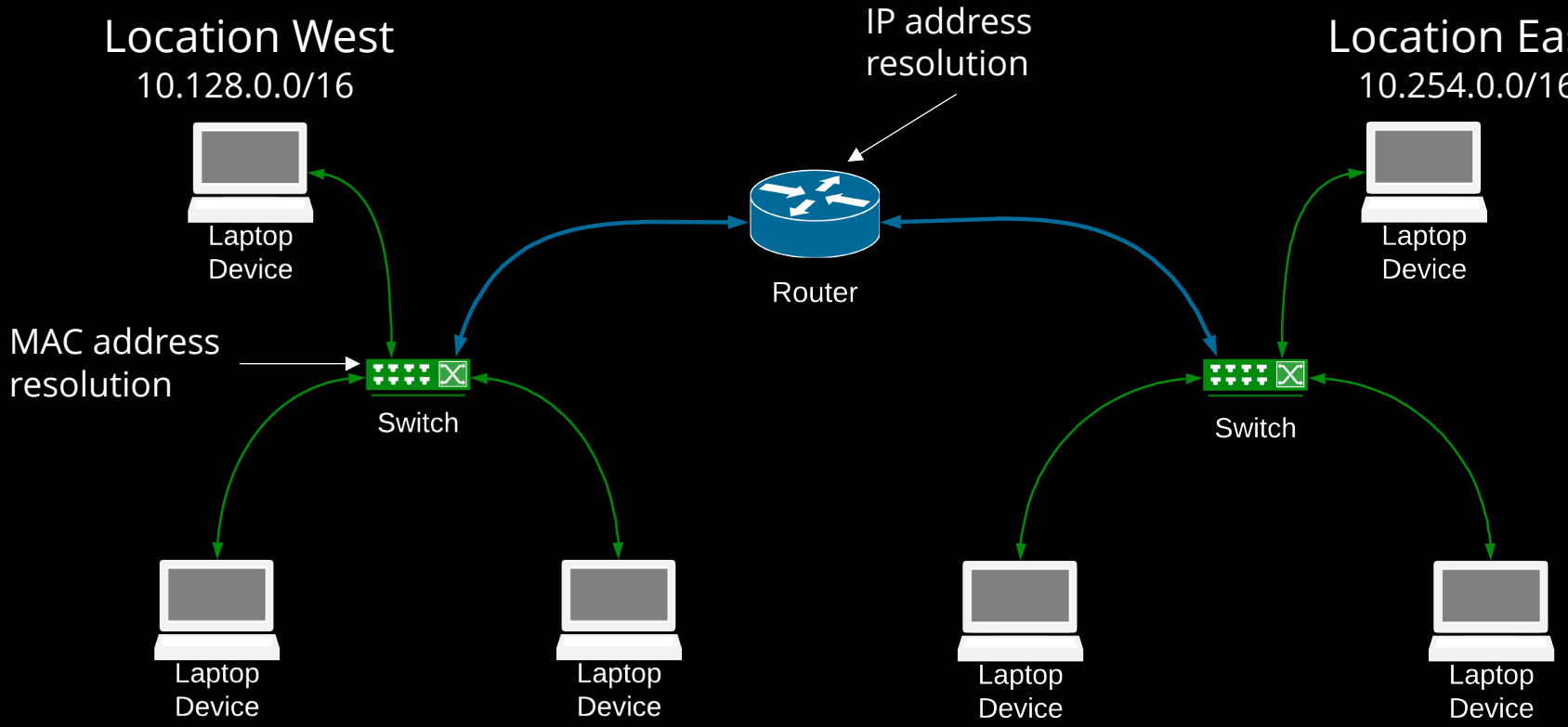

# AGENDA

- Networking 101
- Networking in Azure
- Securing database network traffic
- Hybrid scenarios

# Networking 101

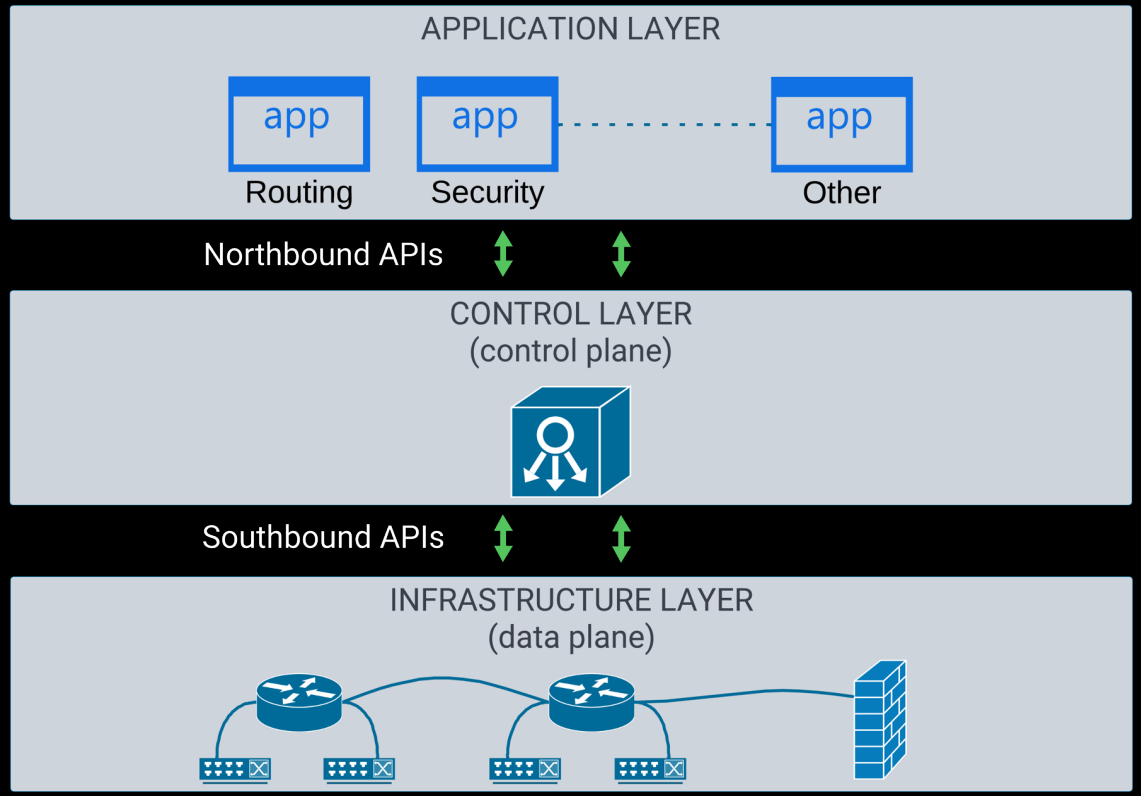


# Networking 101 (traditional)

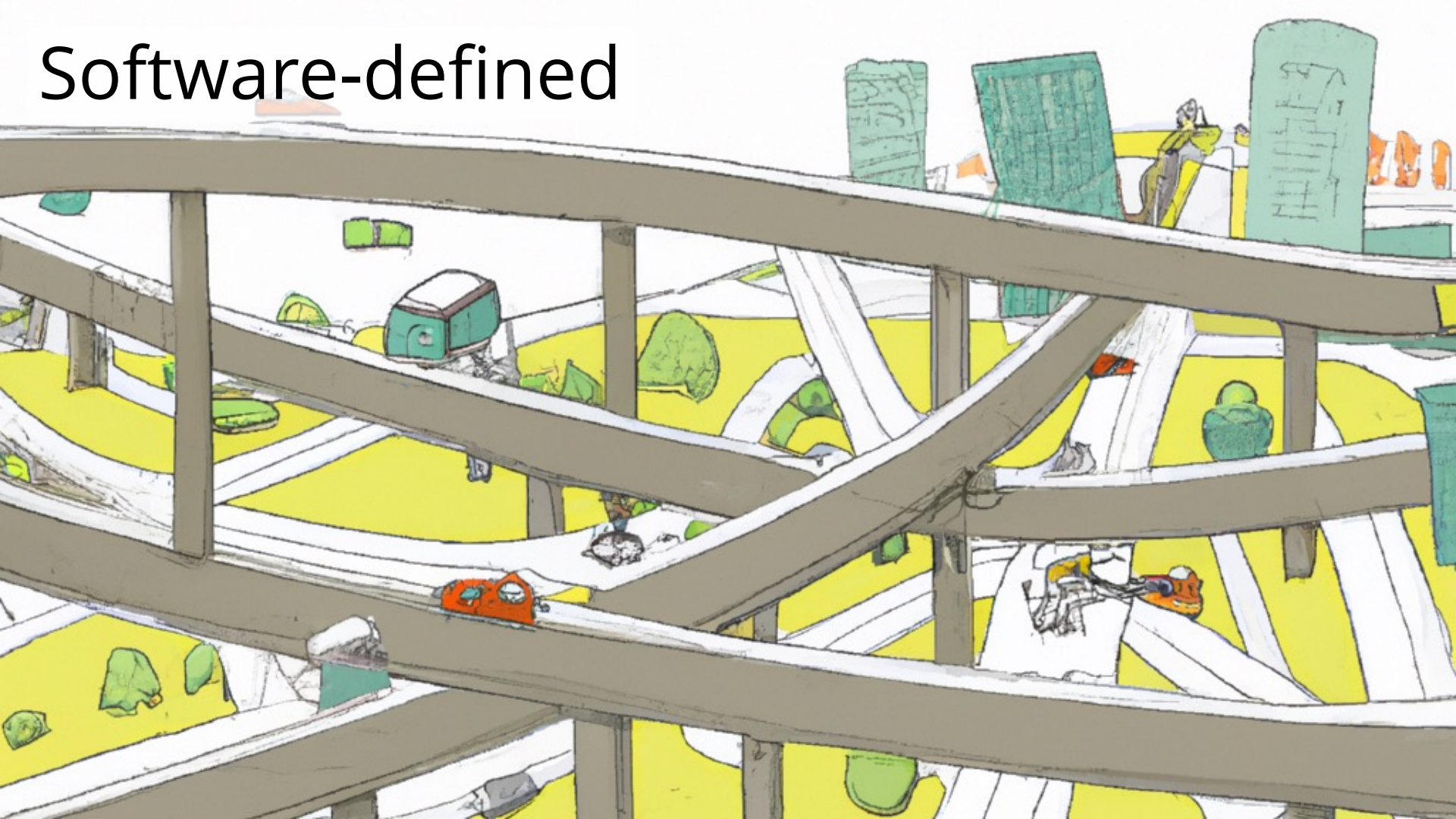



Traditional

# Networking 101 (SW Defined Networking)



# Software-defined



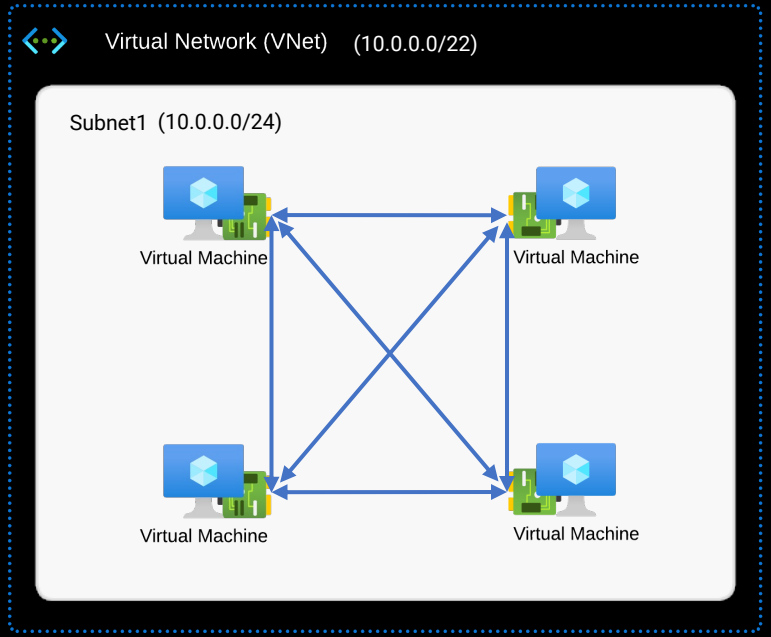
# Networking in Azure



# Networking in Azure

Subscription

Network mesh




- Multiple address spaces
- IPv6 support
  - with limitations
- Dual-stack (v4 + v6)

# NICs are routers 🤯

Routes are auto-updated



=



Needs configuration

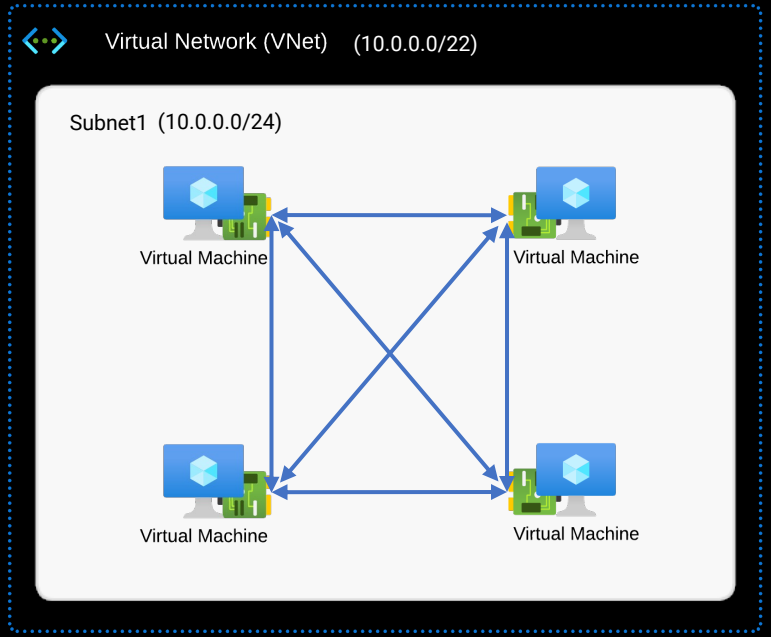
Azure NIC

On-prem router

# Networking in Azure

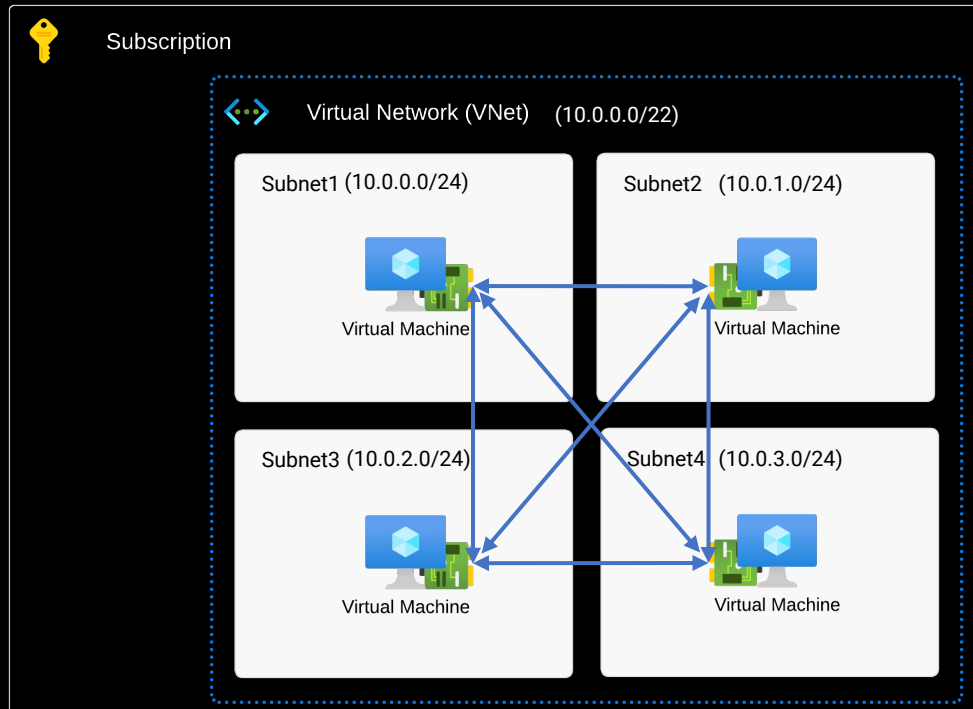
Subscription

Network mesh




- Multiple addresspaces
- IPv6 support
  - with limitations
- Dual-stack (v4 + v6)

# Azure subnets




Subnet

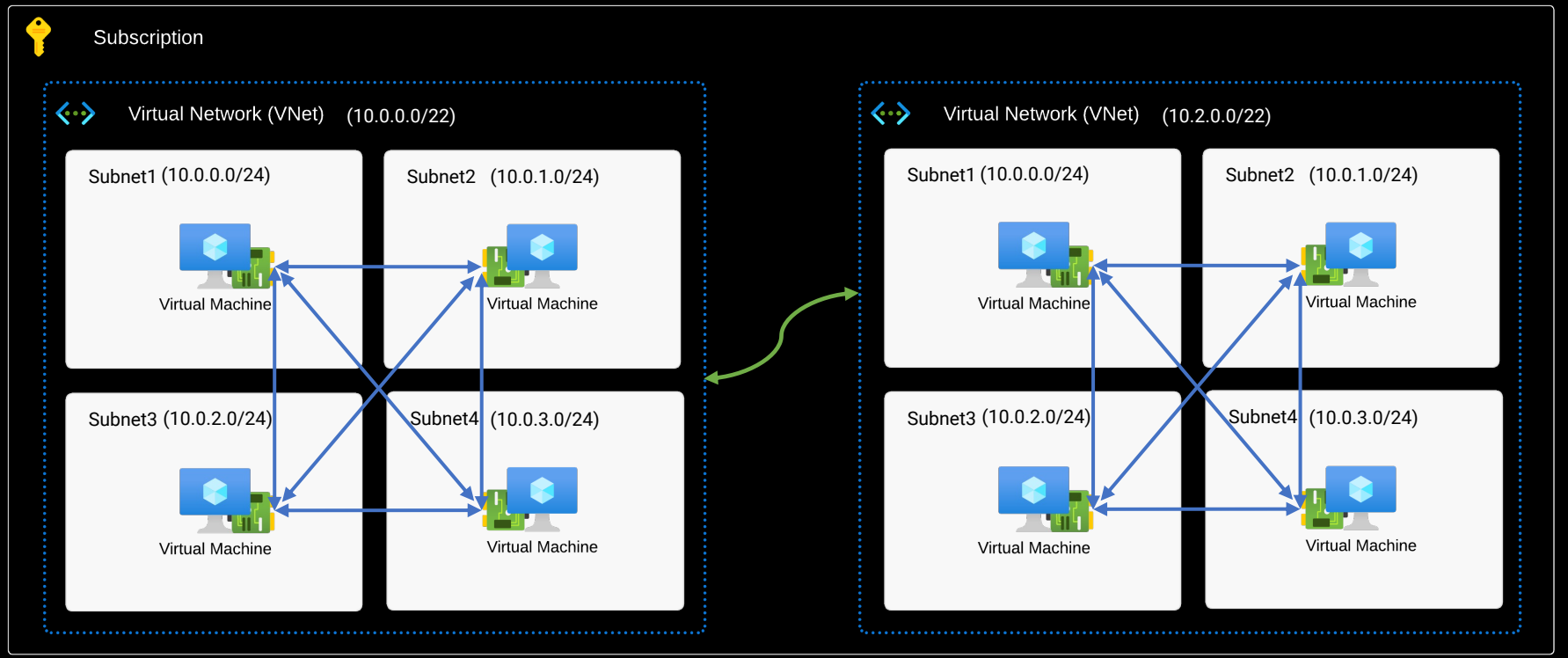
- Logical grouping of resources
- Share an IP address space
- Share routing policy (optional)

Route table (UDR)
(overrides learned routes)

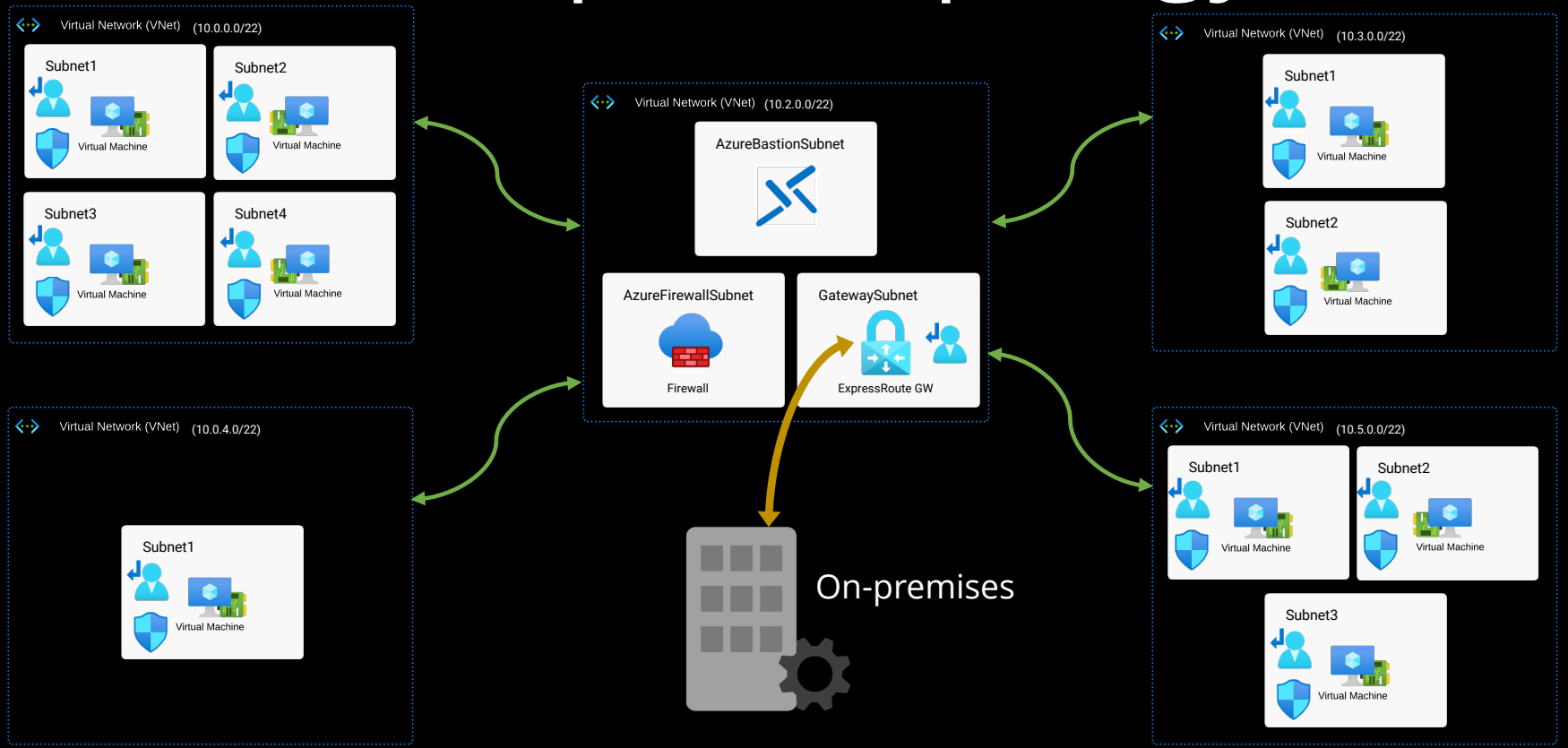
- Share traffic filtering (optional)

Network Security Group (NSG)

# VNet peering



# Hub and Spoke topology



# Route table (UDR)






Route table for every spoke

| Name | Address prefix | Next Hop type | Next Hop IP address |
|---|---|---|---|
| to-hub | 0.0.0.0/0 | Virtual appliance | 10.2.0.132 |

Route table for virtual network gateway

| Name | Address prefix | Next Hop type | Next Hop IP address |
|---|---|---|---|
| to-spoke-1 | 10.3.0.0/22 | Virtual appliance | 10.2.0.132 |
| to-spoke-2 | 10.4.0.0/22 | Virtual appliance | 10.2.0.132 |
| ... | ... | ... | ... |

# Network Security Group (NSG)



Filter in/outbound network traffic

- Subnet
- NIC

Integral part of Zero Trust

- “Assume breach” principle

For ease of maintenance

- Use Application Security Groups

SQL Konferenz 2023
powered by PASS Deutschland e.V.

PASS Microsoft Data Platform Community
DEUTSCHLAND e.V.

# Securing database network traffic for Azure SQL DB and MI



# Connecting to Azure SQL DB

~~Public endpoint~~

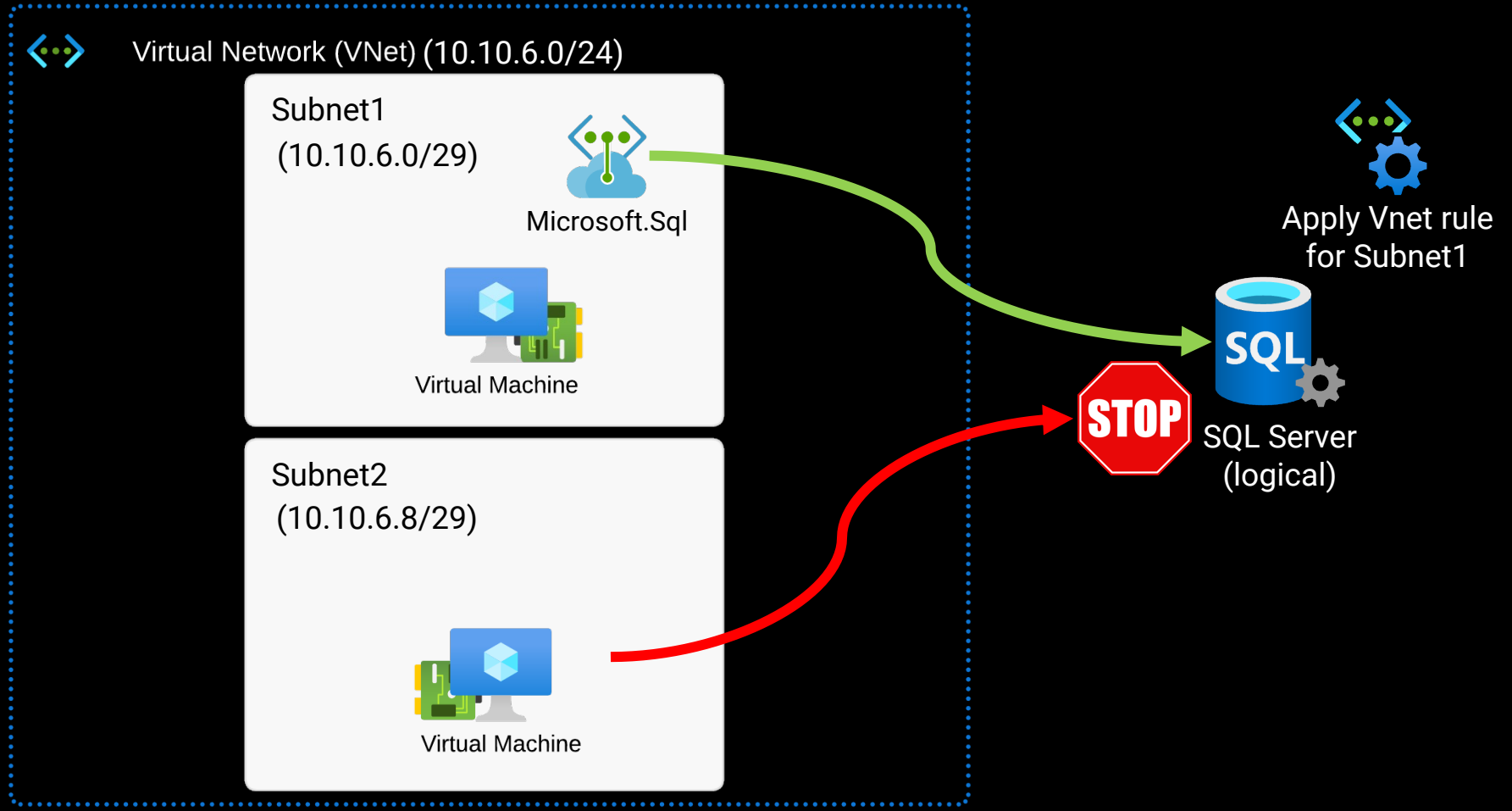
Service Endpoint (Azure SQL DB)

VNet-Local endpoint (Managed Instance)

Private endpoint

# Service endpoint (SQLDB)

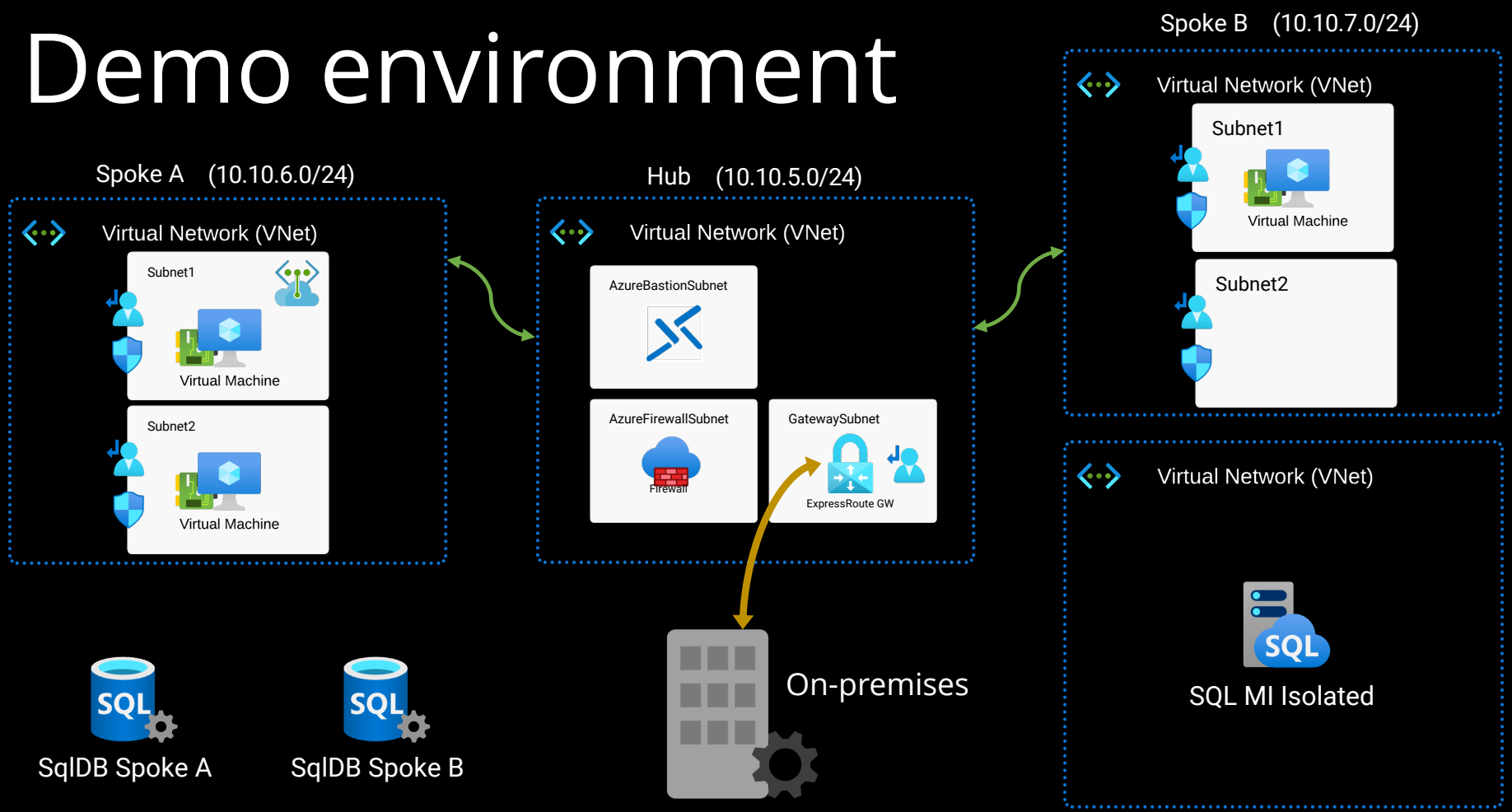
- Secure and direct connectivty
- Optimized route over Azure backbone
- Associated with subnet
- Approval on logical SQL Server

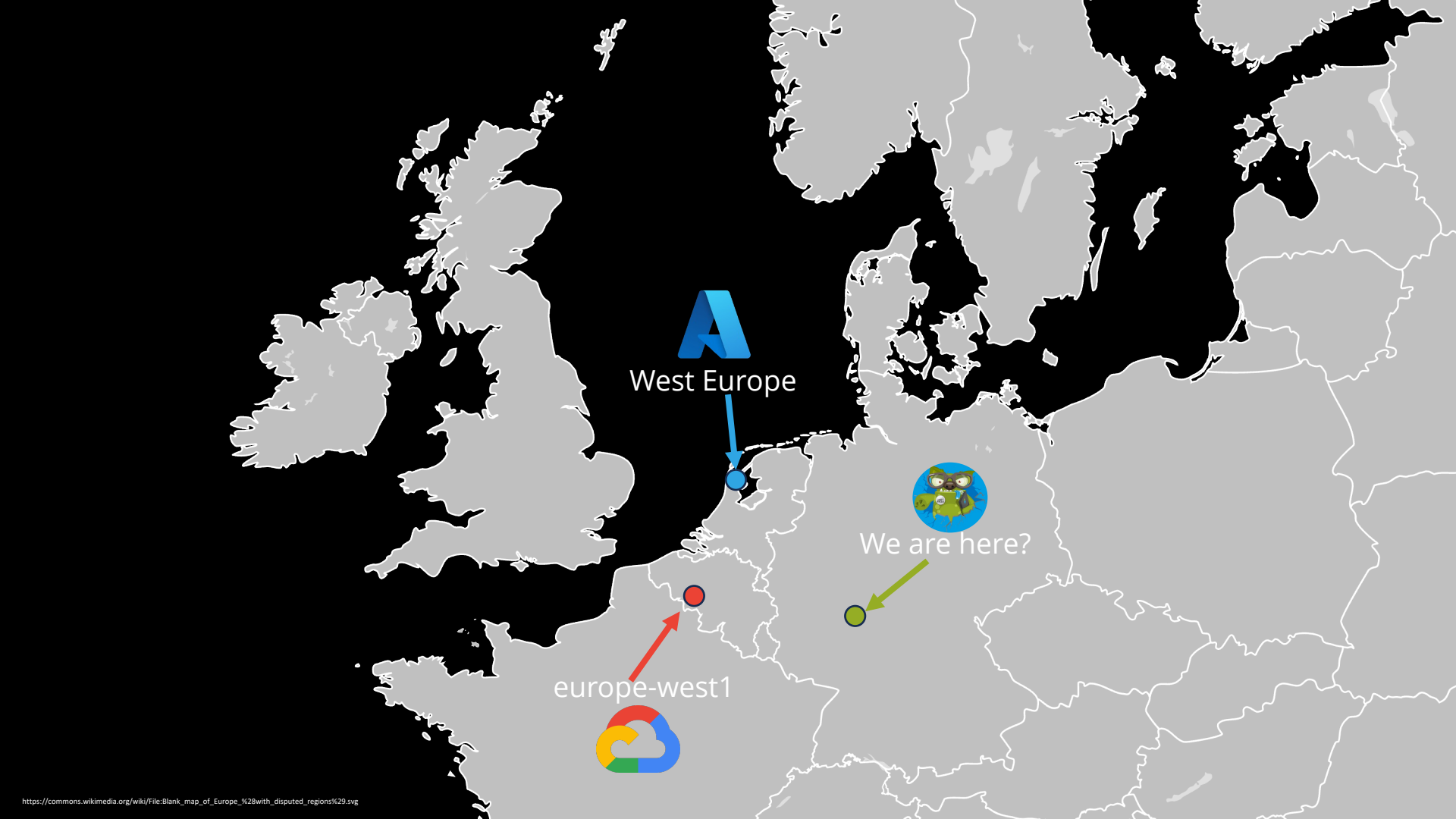

Virtual Network (VNet) (10.10.6.0/24)
Subnet1
(10.10.6.0/29)
Microsoft.Sql
Virtual Machine
Subnet2
(10.10.6.8/29)
Virtual Machine
Apply Vnet rule
for Subnet1
SQL
STOP
SQL Server
(logical)

# DEMO



# Demo environment




West Europe
We are here?
europe-west1
https://commons.wikimedia.org/wiki/File:Blank_map_of_Europe_%28with_disputed_regions%29.svg

# VNet-local endpoint (MI)

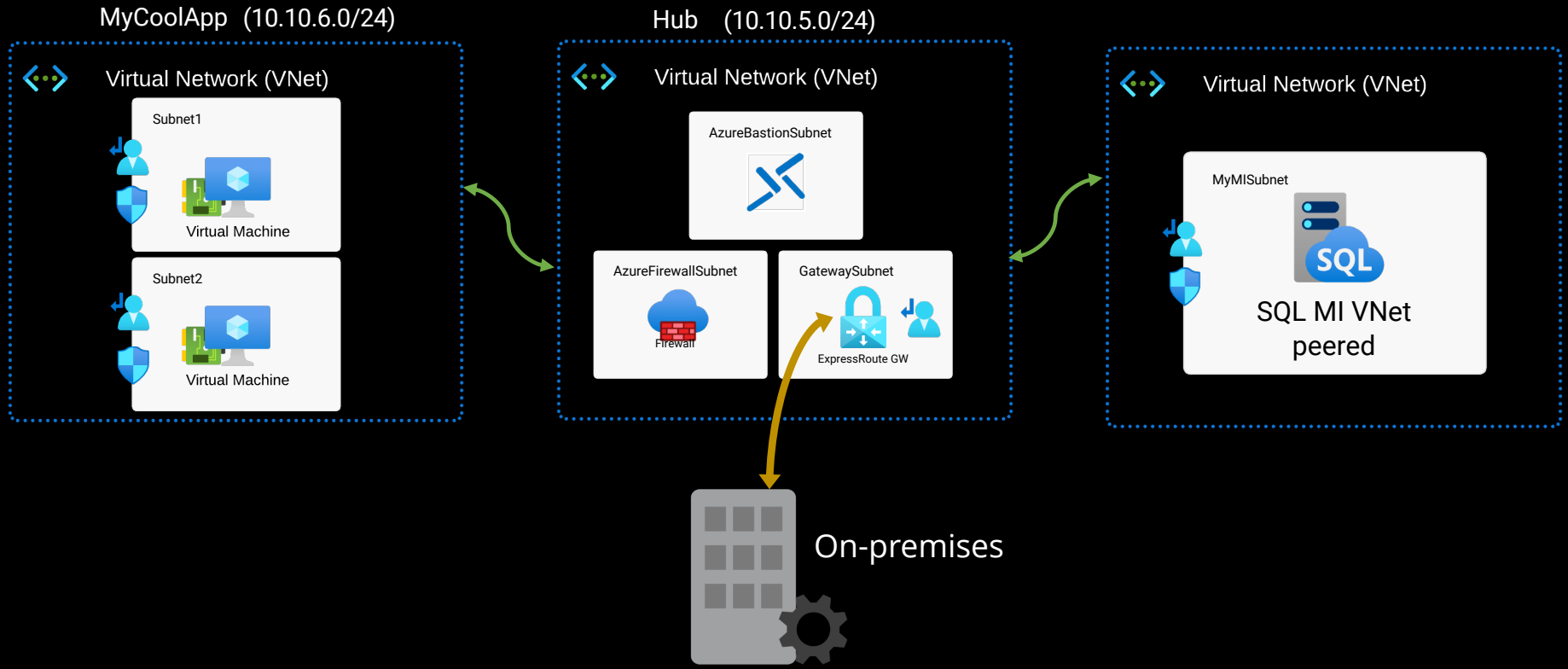
Endpoint local to MI VNet

Supports redirect connection type

When <> 1433 ports are required

Less secure but higher performance

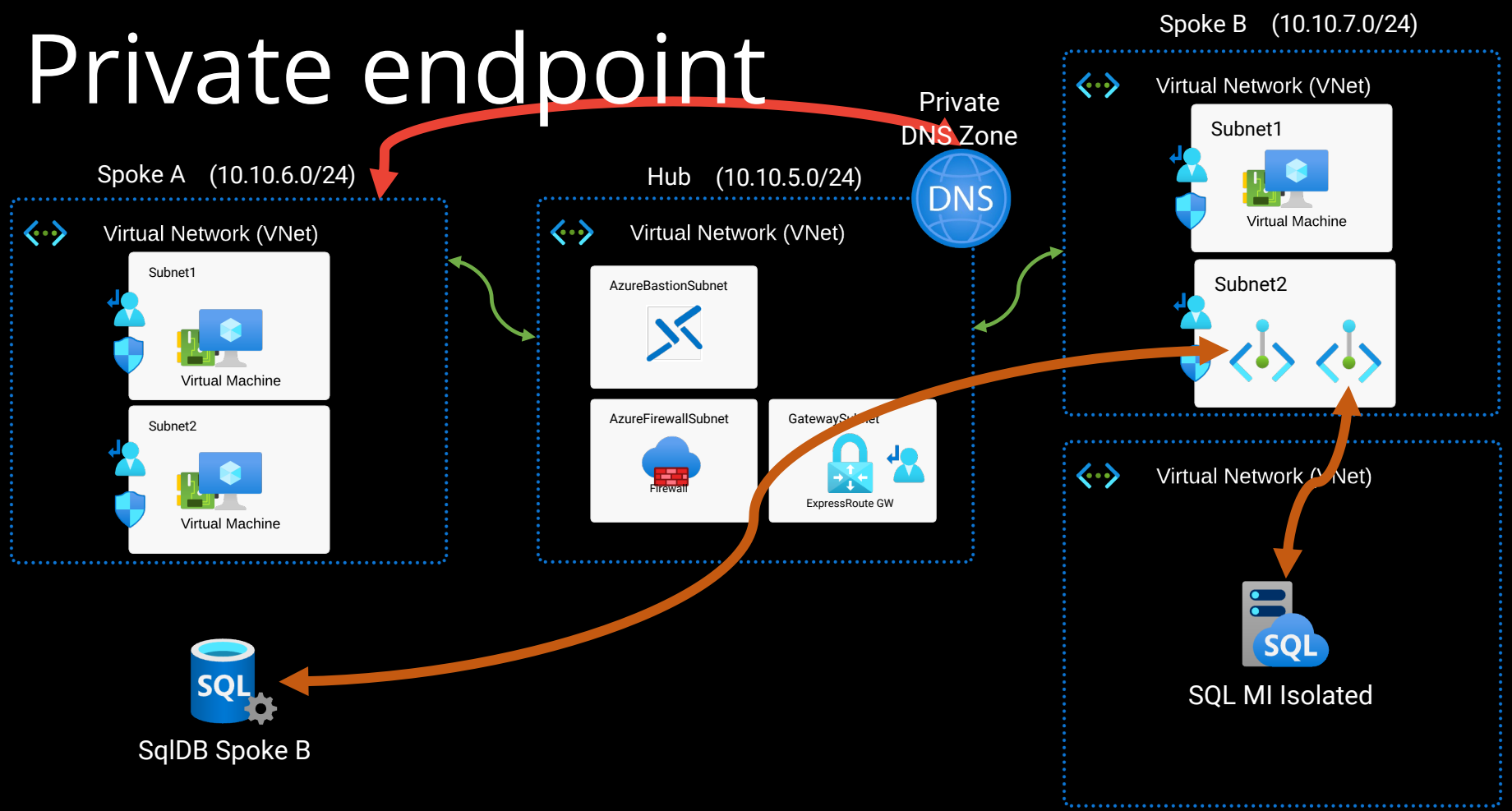
# VNet local


MyCoolApp (10.10.6.0/24)
Virtual Network (VNet)
Subnet1
Virtual Machine
Subnet2
Virtual Machine
Hub (10.10.5.0/24)
Virtual Network (VNet)
AzureBastionSubnet
AzureFirewallSubnet
Firewall
GatewaySubnet
ExpressRoute GW
Virtual Network (VNet)
MyMISubnet
SQL
SQL MI VNet peered
On-premises

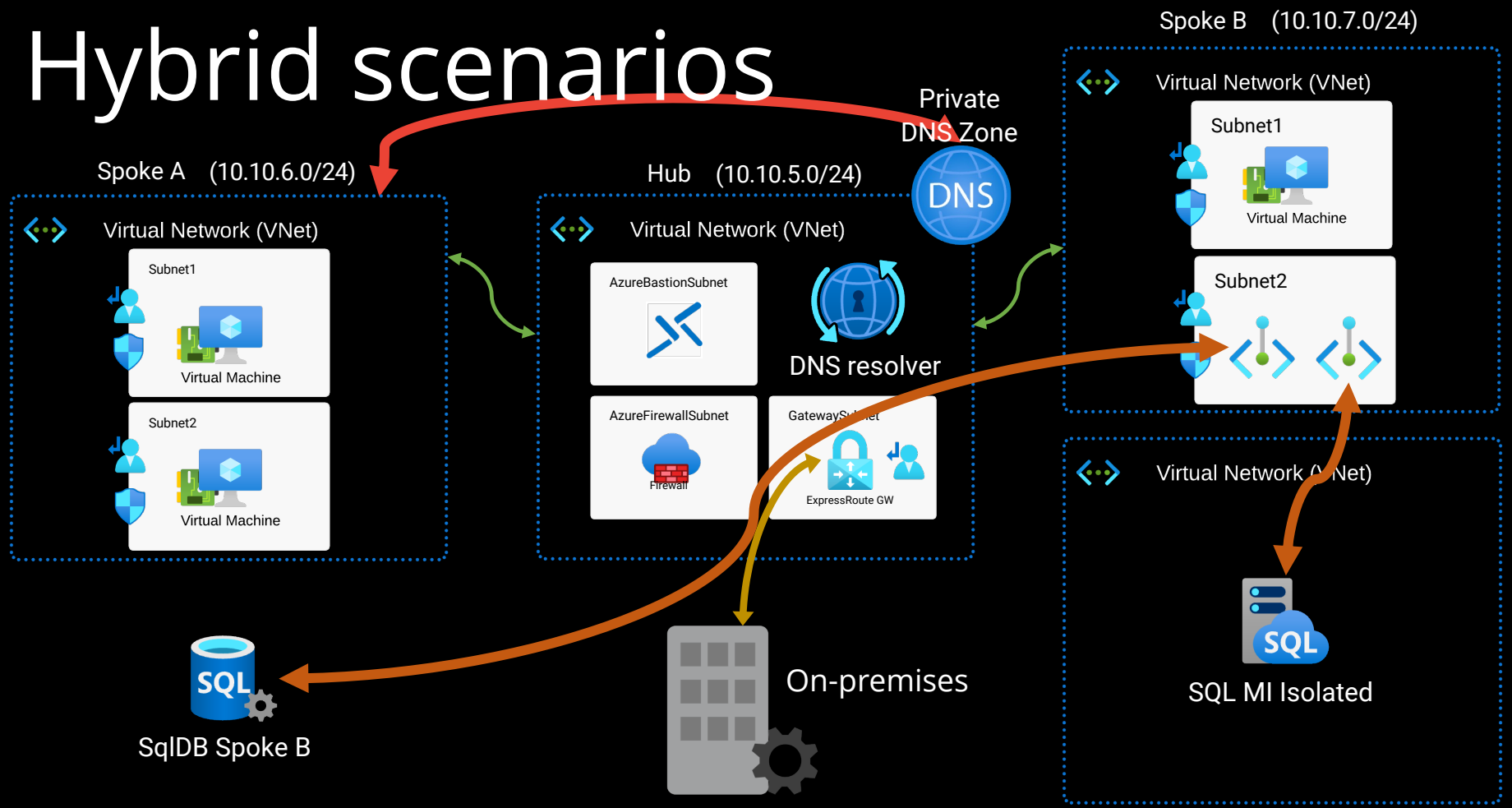
# Private endpoint

- Secure access to service in your VNet
- Is in essence a NIC
- Points to a Private Link service
- Only support proxy connection type (MI)

# Private endpoint



# Hybrid scenarios



# Resources

Scenarios with private endpoints to Azure SQL Managed Instance (microsoft.com)
(Zoran Rilak)

Zero Trust Model - Modern Security Architecture | Microsoft Security



# THANK YOU TO OUR SPONSORS

PASS Microsoft Data Platform Community DEUTSCHLAND e.V.

pmOne

SOLARWINDS

smart casual datadesign

Mainzer Datenfabrik

b.telligent
smart data. smart decisions.

HMS analytical software

ORAYLIS
turn your data into value

TIMEXTENDER

Microsoft

ITGAIN

SOLISYON
www.solisyon.de

GDS BUSINESS INTELLIGENCE GmbH



- Organizer of Data Saturday Oslo
- 25+ years experience with database technology and SQL Server specifically
- Developer, DBA, Solution Architect

---

- Single-track bicycling through the forests of southern Norway


# Rune Ovlien Rakeie

Principal Cloud Architect
Tietoevry

in • /runeovlienrakeie

• @datarune.online


Scan to eval






Thank you very much for your attention.

Vielen Dank für Eure Aufmerksamkeit.