Public Endpoint, Service Endpoint, Private Endpoint
Ja was denn nun?

Haiko Hertes, Azure Architect & Principal Consultant, Microsoft Azure MVP
10.10.2023

HERTES.NET
knowledge - experience - insights

E = M C²

MVP Microsoft® Most Valuable Professional

- Seit 2019 bei SoftwareOne
- Principal Consultant & Architect
- Azure Consulting Team
- Microsoft MVP, YouTuber, Blogger, Conference Speaker
- Familienvater, Offizier d.R., Holzwurm

www.hertes.net
about.me/haiko.hertes
twitter.com/HHertes
youtube.com/c/HaikoHertes

Haiko Hertes

Cloud Architect / Principal Consultant

software one

01

The issue

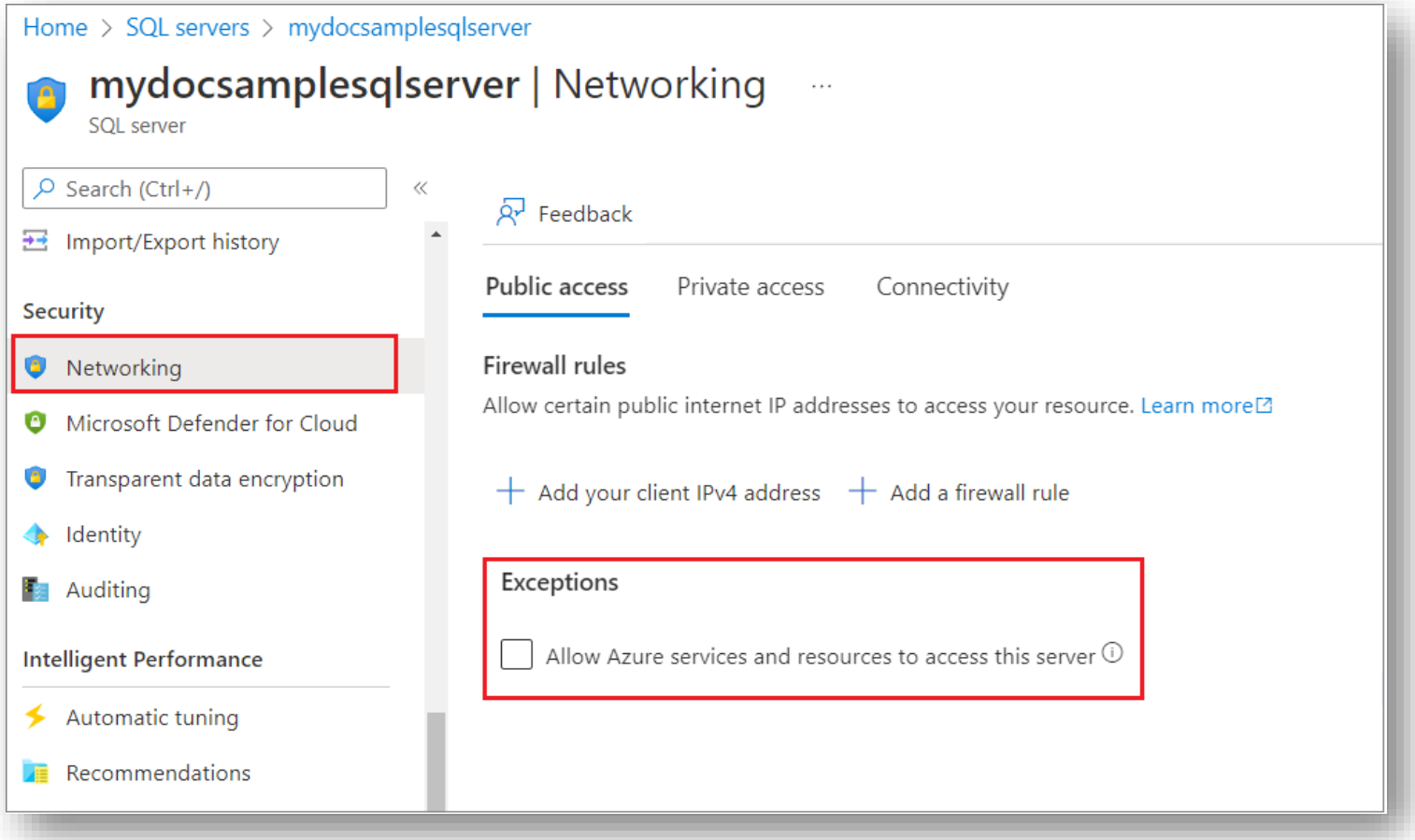
The issue

- **Azure SQL Database** (and so, Azure SQL Elastic Pool) as well as **Azure Synapse Analytics** uses a „**Public Endpoint**“ by default (*)
- This public endpoint will use the format *yourservername.database.windows.net*
- To allow access to the database, you need to
  - Allow access for Azure services and resources (ALL!)
  - Use IP addresses to whitelist source Ips
- The first option would allow access to a lot our sources, that might not be allowed to access the database
- Second option could be tricky when using dynamic IPs or a lot of sources

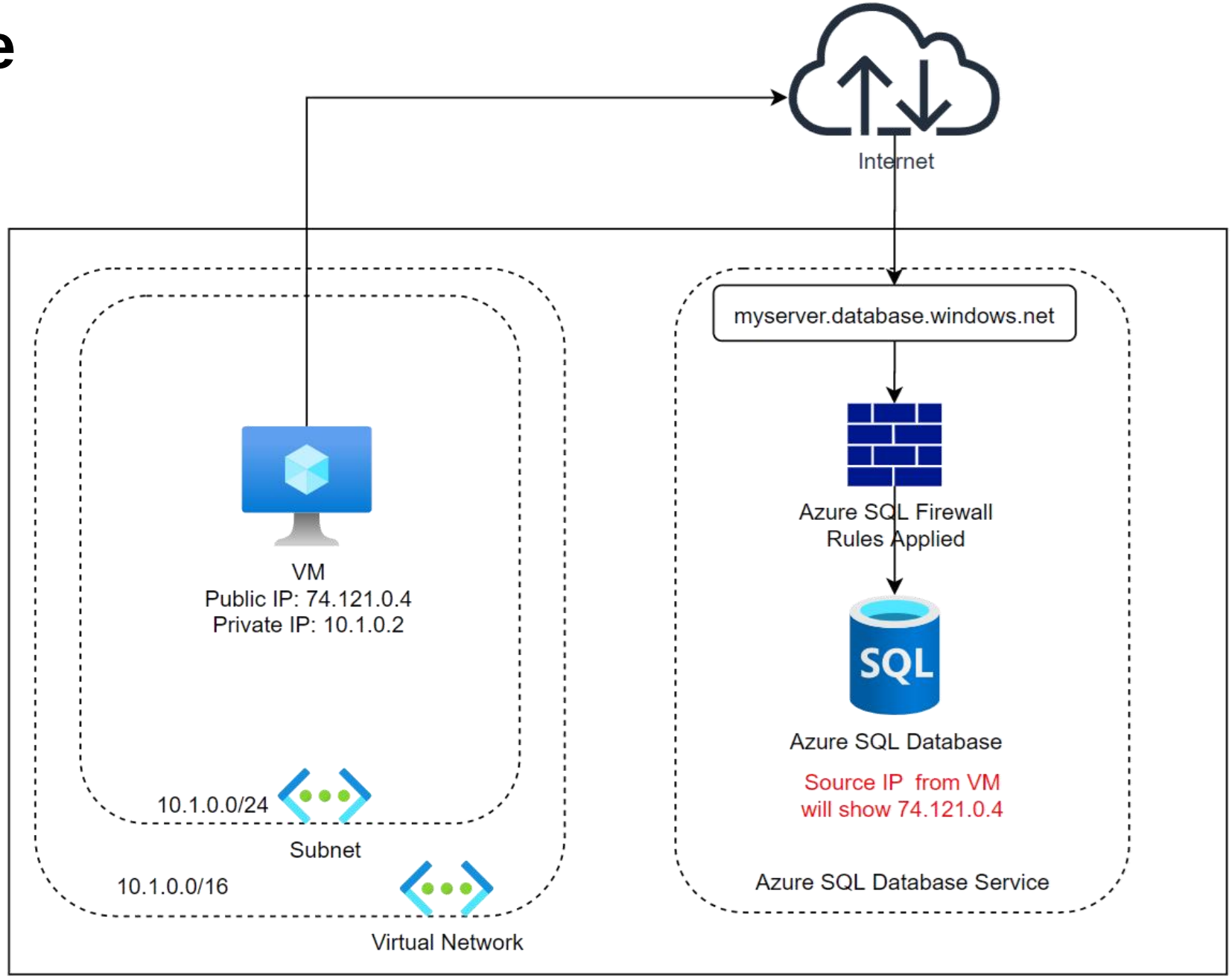
(*) This was changed recently – Public Endpoint must be enabled now first!

The issue

- Access to the Database is controlled trough a „firewall“
- You have no control over that firewall beside adding source IPs
- Even with that firewall, the service has still an endpoint that would be reachable from the internet somehow



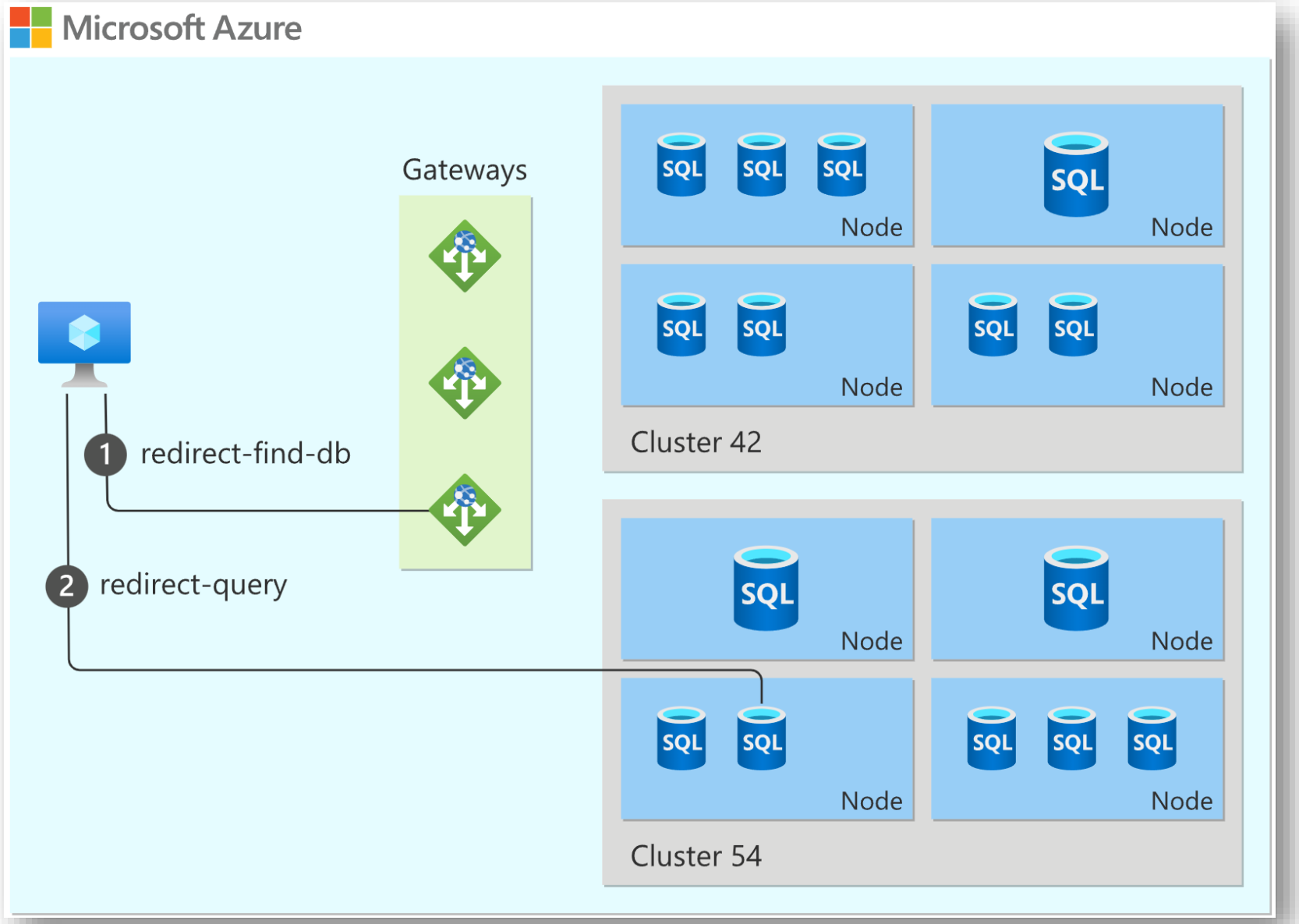
The issue


Internet
myserver.database.windows.net
Azure SQL Firewall
Rules Applied
SQL
Azure SQL Database
Source IP from VM
will show 74.121.0.4
Azure SQL Database Service
VM
Public IP: 74.121.0.4
Private IP: 10.1.0.2
10.1.0.0/24
Subnet
10.1.0.0/16
Virtual Network

The issue

Behind the scenes…

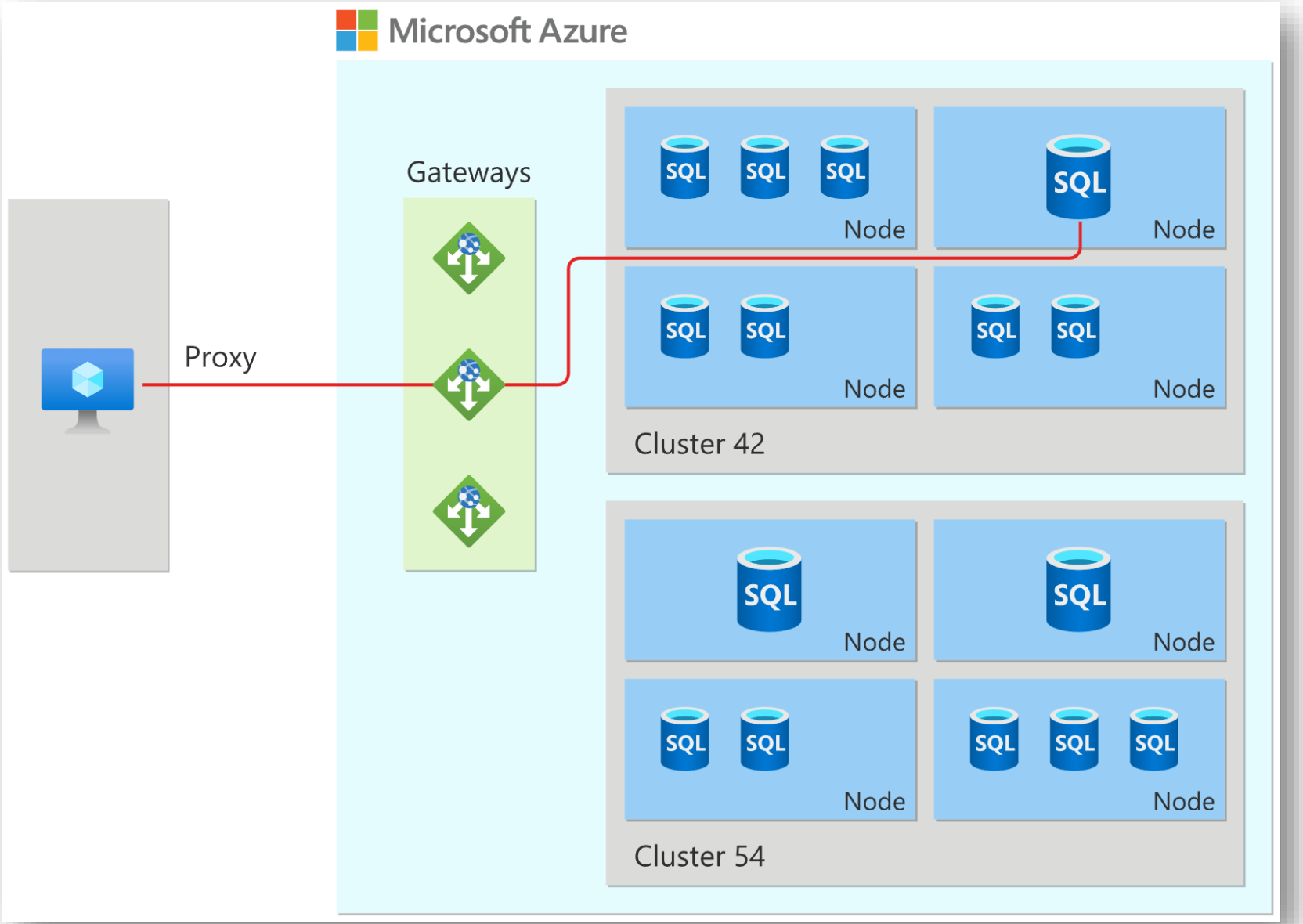
(Access from within Azure)



The issue

Behind the scenes…

(Access from outside)



The issue

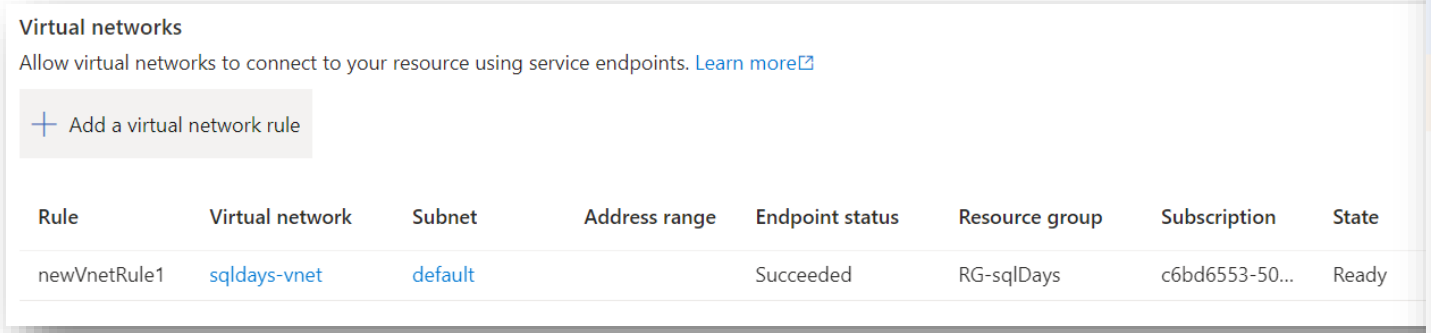
So we never could contact our database (server) directly!
Keep this in mind…

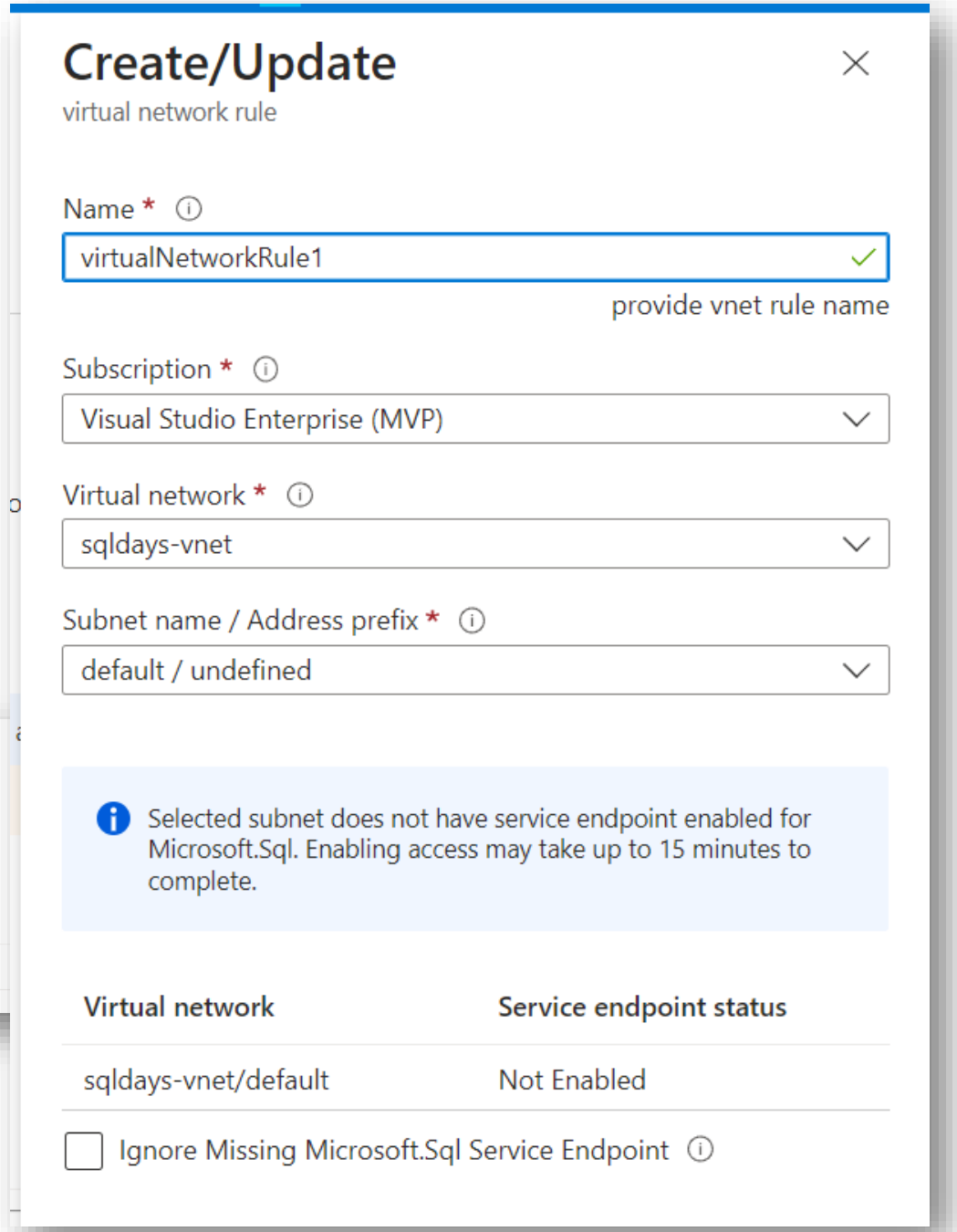
02

Service Endpoints

Service Endpoints

- Sometimes also called „VNet endpoints“
- They enable access from a given Subnet within a given Vnet
- Once the service endpoint is created on the Subnet / in the Vnet, you can use that Subnet within a „virtual network rule“

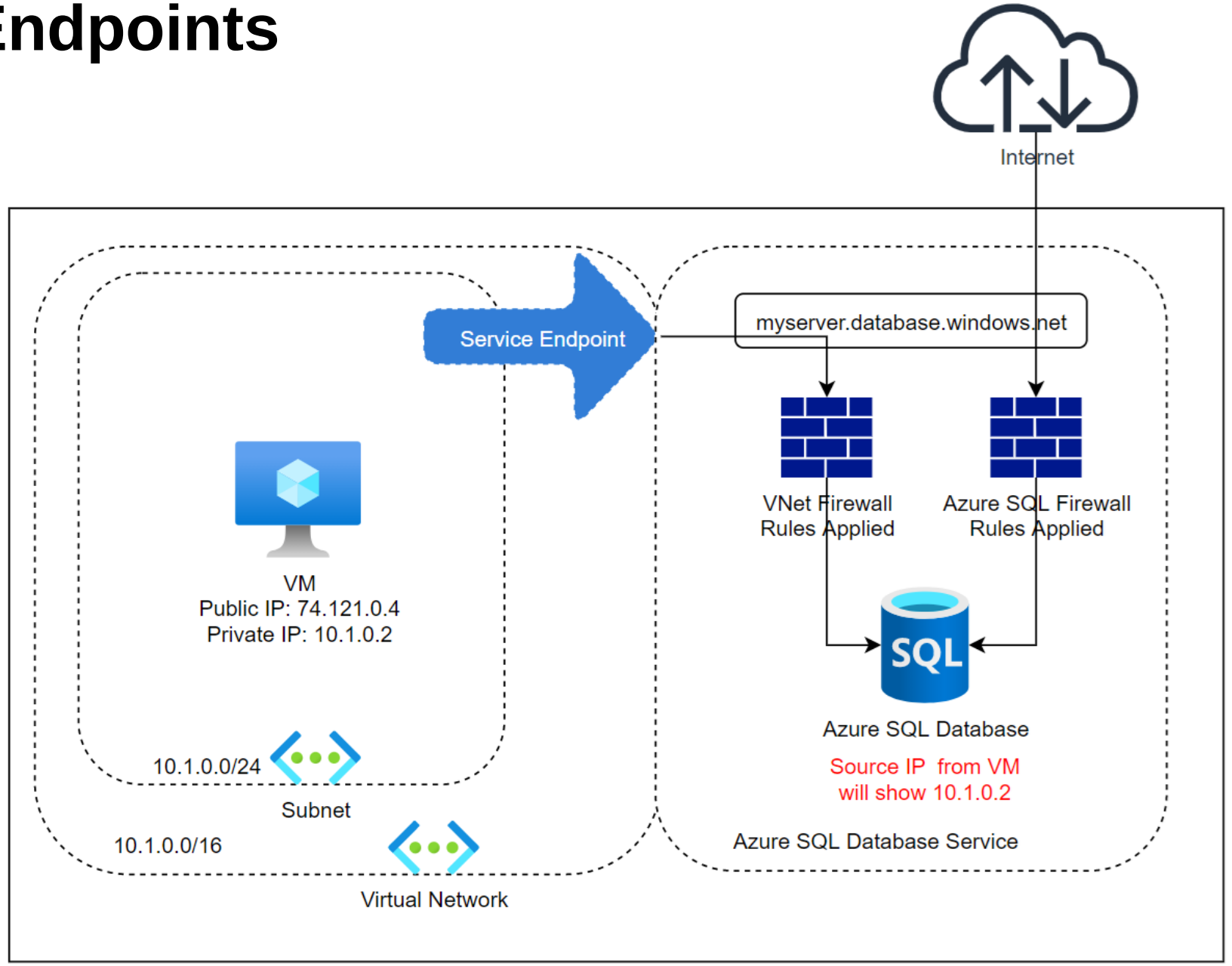




Service Endpoints

- Service Endpoints allow to shut down the Public Endpoint and still connect to the Database
- It also optimizes routing the traffic to the service
- It‘s easy to set up and has no additional costs
- But there is also some limitations:
- Service Endpoints could only be reached from the configured Azure Vnets – not from outside Azure (no VPN, no ExpressRoute, …)
  - You could add your on-prem public IP adress to solve this, but…

Service Endpoints



Service Endpoints

- Important: Although the Database will be reached through the private VNET it still uses it‘s public DNS name!
- You can not reach the database using either its public or any private IP address!
- The database will only be reachable by Service Endpoints for the configured Subnets – but you can add multiple Subnets to a database!

08

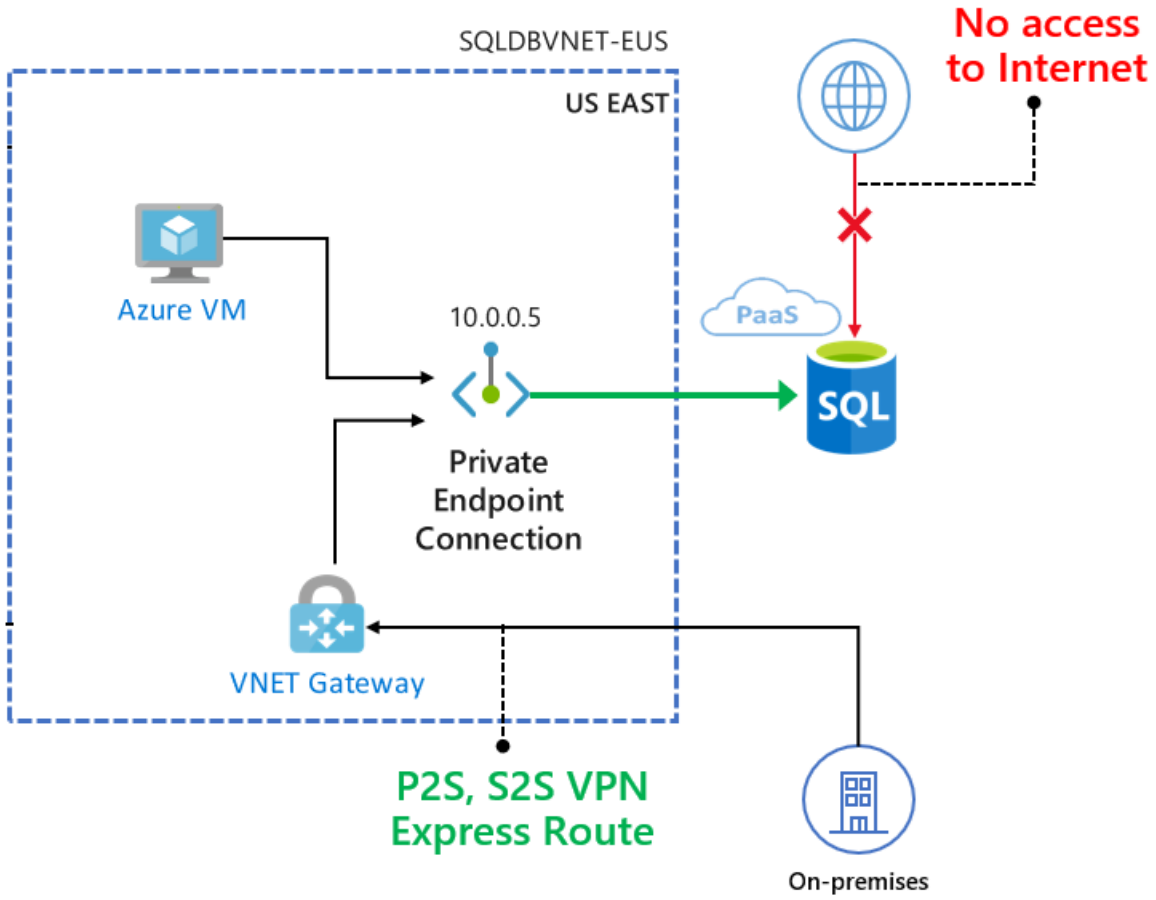
Private Endpoint / Private Link

Private Endpoints

- As Service Endpoints have some limitations and can‘t be reached from on-premises, Microsoft introduced Private Endpoints
- Azure SQL Database offers to use Private Endpoints, Azure SQL Managed Instance uses them by default
- Private Endpoints are not free – you need to pay for it and the traffic handled

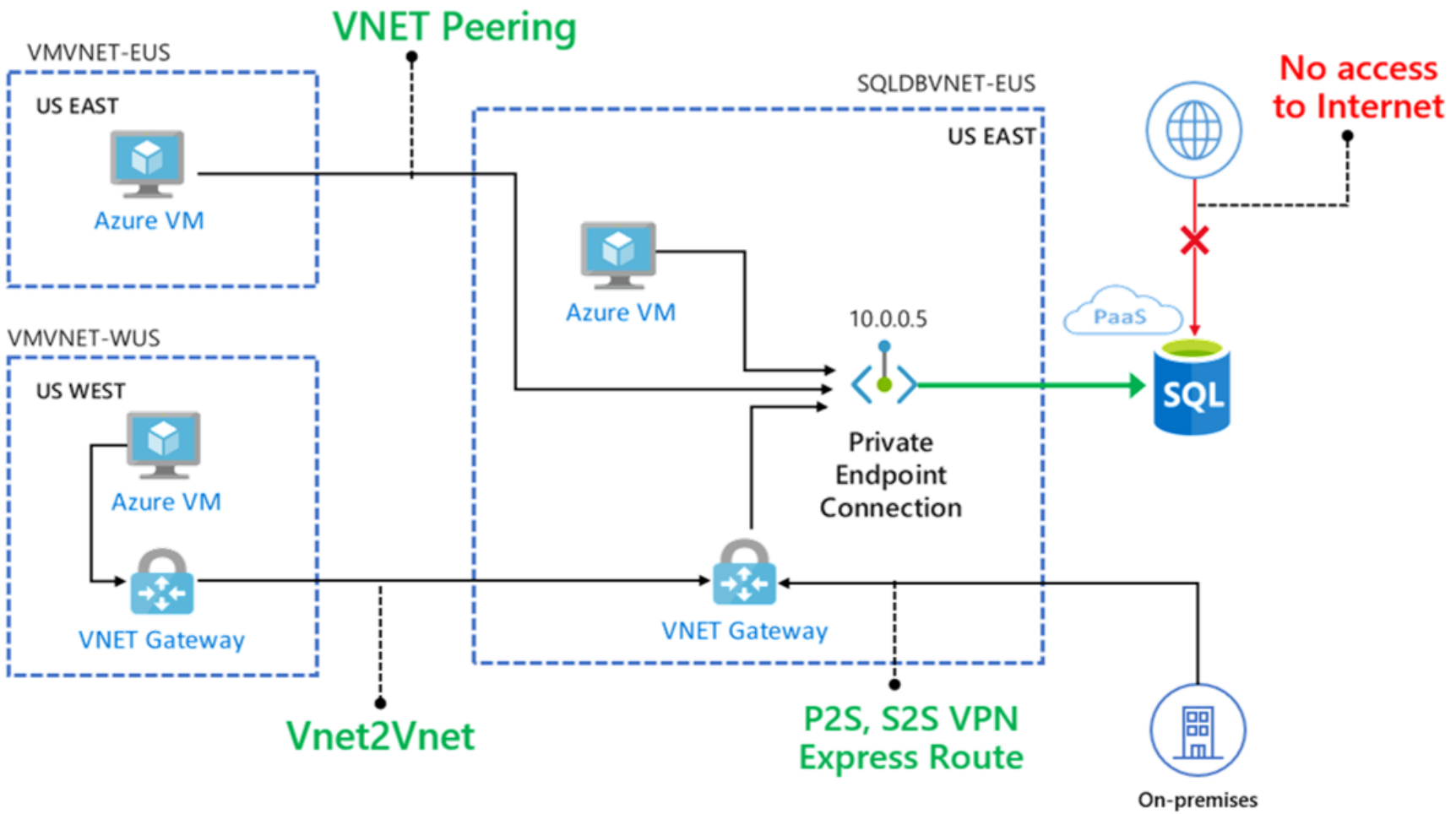
Private Endpoints

- A private endpoint is basically a NIC with an private IP address
- That NIC is connected to the PaaS service via Private Link



Private Endpoints

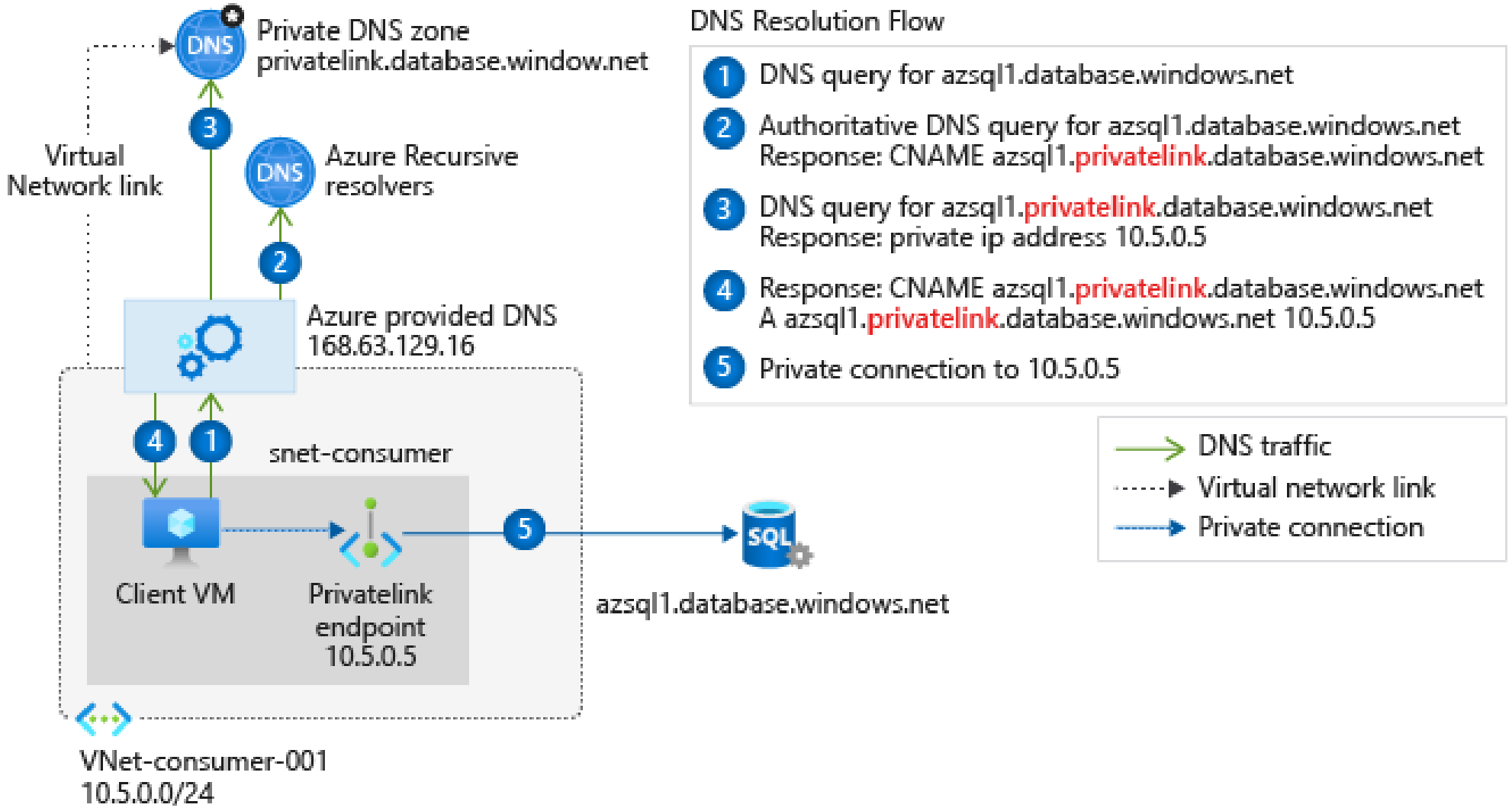
- Now with that private IP, the traffic can be routed into the service even across VNets, regions and also from on-premises:



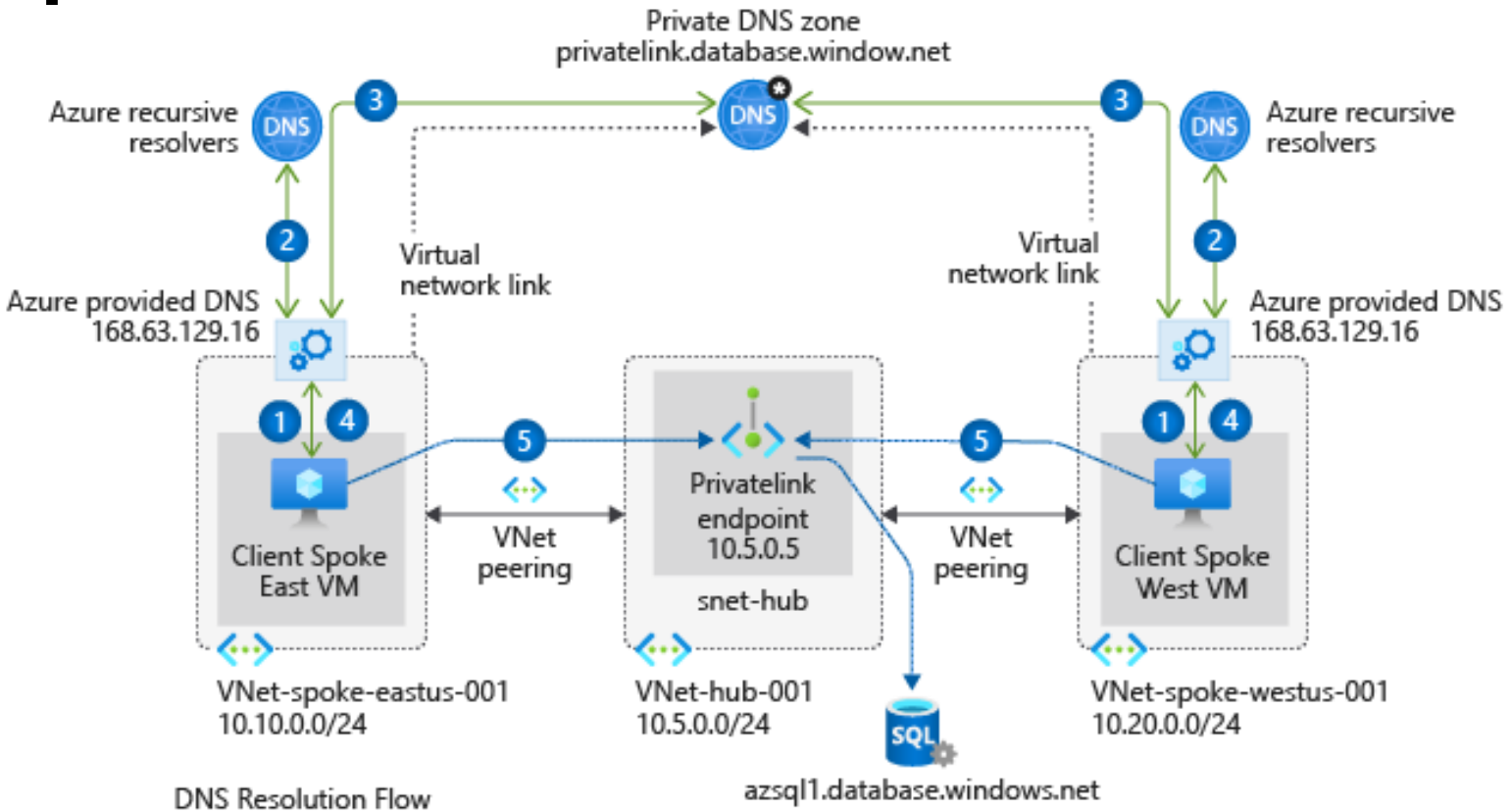
Private Endpoints

- But be aware that you still can‘t use the private IP adress directly when connecting to the service
- You need to use the public DNS name
- But this time, this DNS name needs to resolve into the private IP address
- There is 3 ways to achieve this:
  - Local hosts file
  - Azure Private DNS Zone
  - Custom DNS infrastructure
- When you don‘t use any custom DNS infrastructure at all, it‘s easy, otherwise a bit more complicated…

Private Endpoints & DNS



Private Endpoints & DNS



DNS Resolution Flow

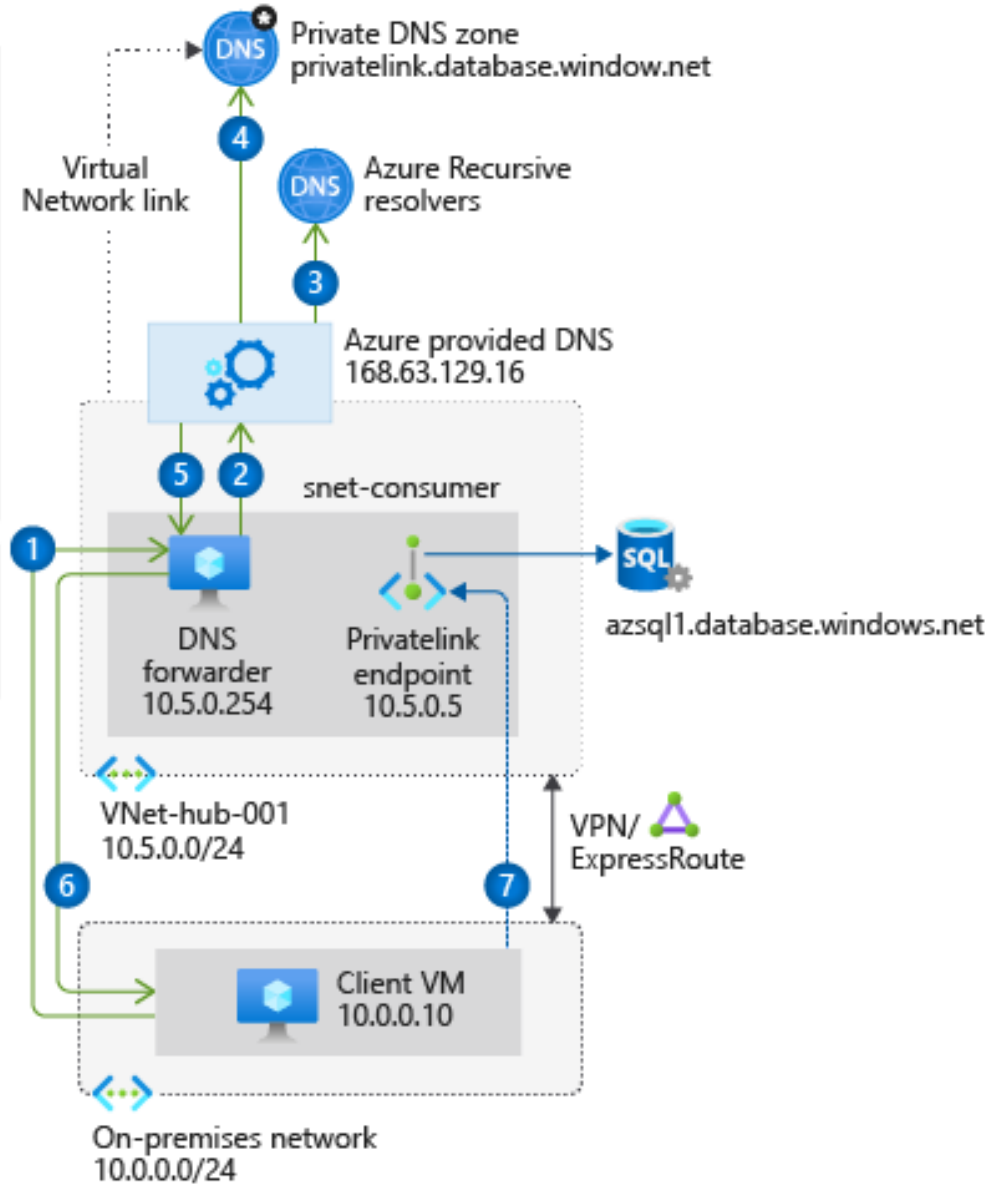
1. DNS query for azsql1.database.windows.net
2. Authoritative DNS query for azsql1.database.windows.net
   Response: CNAME azsql1.privatelink.database.windows.net
3. DNS query for azsql1.privatelink.database.windows.net
   Response: private ip address 10.5.0.5
4. Response: CNAME azsql1.privatelink.database.windows.net
   A azsql1.privatelink.database.windows.net 10.5.0.5
5. Private connection to 10.5.0.5

DNS traffic
Virtual network link
Private connection

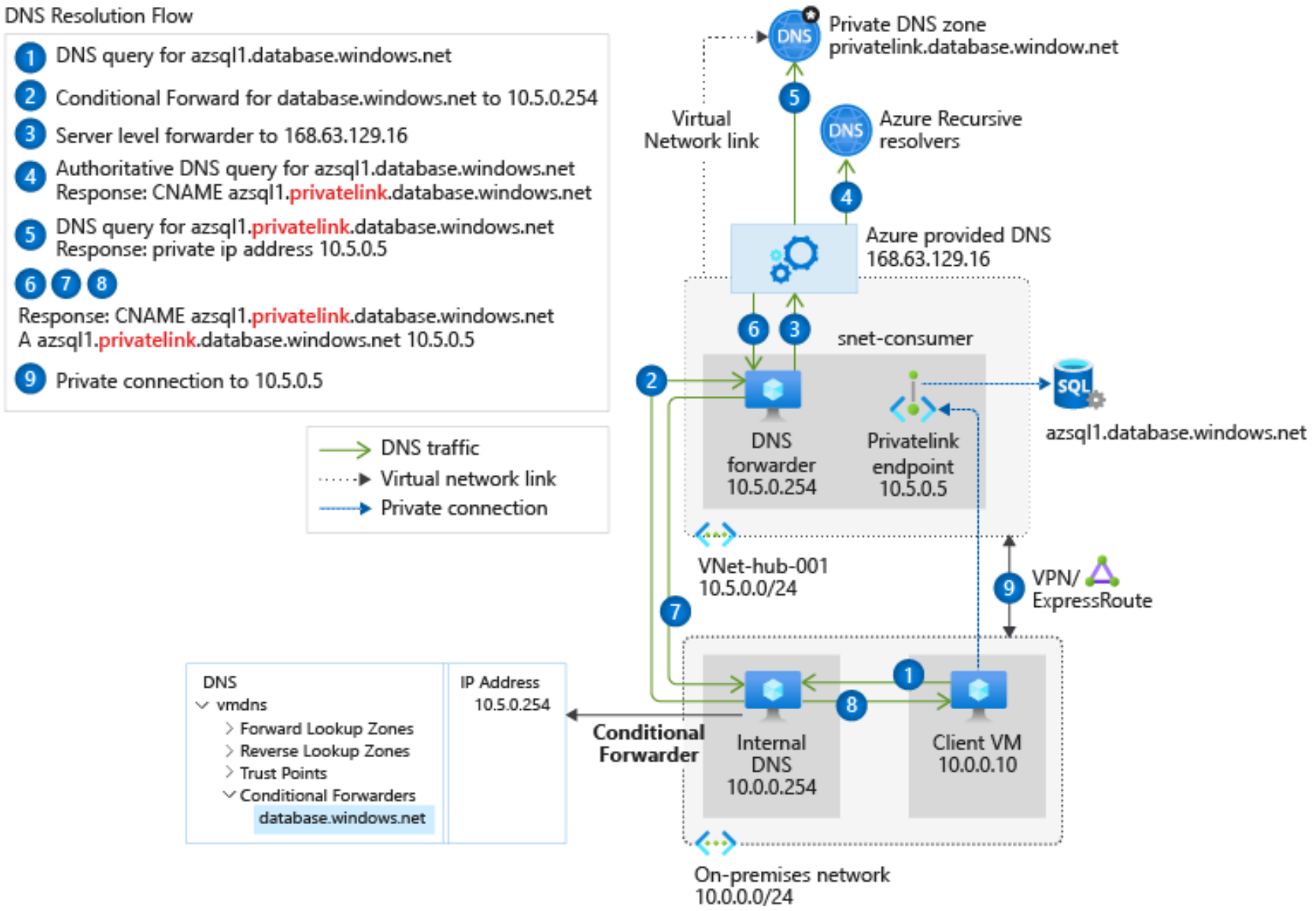
Private Endpoints & DNS

DNS Resolution Flow

1. DNS query for azsql1.database.windows.net
2. Server level forwarder to 168.63.129.16
3. Authoritative DNS query for azsql1.database.windows.net
   Response: CNAME azsql1.privatelink.database.windows.net
4. DNS query for azsql1.privatelink.database.windows.net
   Response: private ip address 10.5.0.5
5. 6. Response: CNAME azsql1.privatelink.database.windows.net
   A azsql1.privatelink.database.windows.net 10.5.0.5
7. Private connection to 10.5.0.5



Private Endpoints & DNS



07

Things to keep in mind

Things to keep in mind

- Any netowking change applies to the Azure SQL database server, not just a single database!
- Subnets to be allowed using Service Endpoints must be in the same region
- Private Endpoints require proper DNS resolution
- Private Endpoints are charged

Thank You!

Questions?

software one

Disclaimer

This publication contains proprietary information that is protected by copyright. SoftwareOne reserves all rights thereto.

SoftwareOne shall not be liable for possible errors in this document. Liability for damages directly and indirectly associated with the supply or use of this document is excluded as far as legally permissible.

The information presented herein is intended exclusively as a guide offered by SoftwareOne. The publisher's product use rights, agreement terms and conditions and other definitions prevail over the information provided herein. The content must not be copied, reproduced, passed to third parties or used for any other purposes without written permission of SoftwareOne