Taking the "Public" Out of Public Cloud:
Getting Started with Private Endpoints

Microsoft Data Platform Group
Birmingham

Introduction

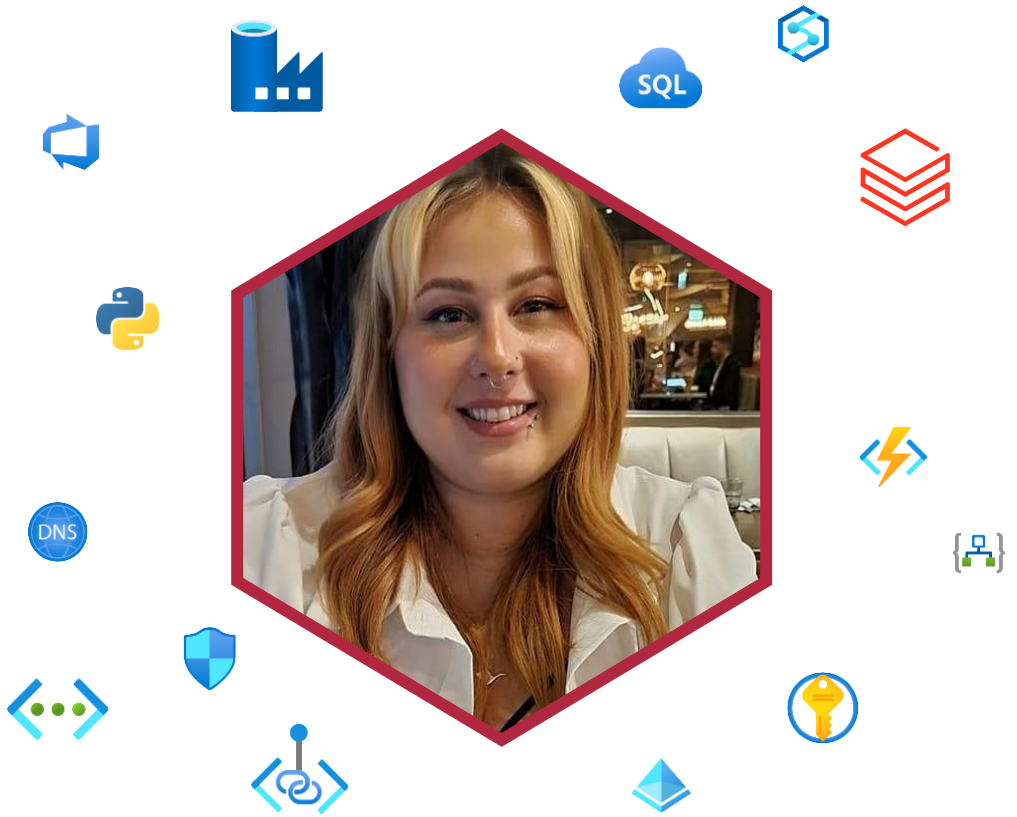
Introduction

Grace O'Halloran (grace-o-halloran)

@graceaohalloran

grace@advancinganalytics.co.uk

www.thinkingacloud.co.uk



What to expect

What to expect

1

Intro to Private Endpoints

- What is an endpoint
- Public vs Private Endpoints
- Why Private Endpoints are more secure

5 mins

2

7 Steps to Success: Deploying and configuring Private Endpoints

- 7 steps to successfully deploy and configure a Private Endpoint
  - DNS
- Demo

30 mins

3

Common mistakes to avoid

- Using “select networks”
- Non-centralized Private DNS Zones

10 mins

Why is this important?

What is an endpoint?

What is an endpoint?

An IP endpoint refers to a unique network address that identifies a specific device or application on a network.

It is composed of an IP address and a port number.

The combination of the IP address and the port number creates a unique endpoint that can be used for communication and data transfer between devices over a network.

Public vs Private Endpoints

What is an endpoint?

When talking about endpoints of Azure services, they fall into two categories:

Public Endpoints

Public IP Addresses

Private Endpoints

Private IP Addresses

Why is it more secure?

Why is it more secure?

Public Endpoint

- Location information is publicly available; the IP address is resolvable from the public internet.
- By default, anyone on the public internet has access.

Public Endpoint with Selected Networks enabled

- Location information is publicly available; the IP address is resolvable from the public internet.
- Restricted access to selected networks and IP addresses.

Private Endpoint

- Location information is **not** publicly available; the IP address is **not** resolvable from the public internet.
- Can only access from **within** the private network.

7 Steps to Success!

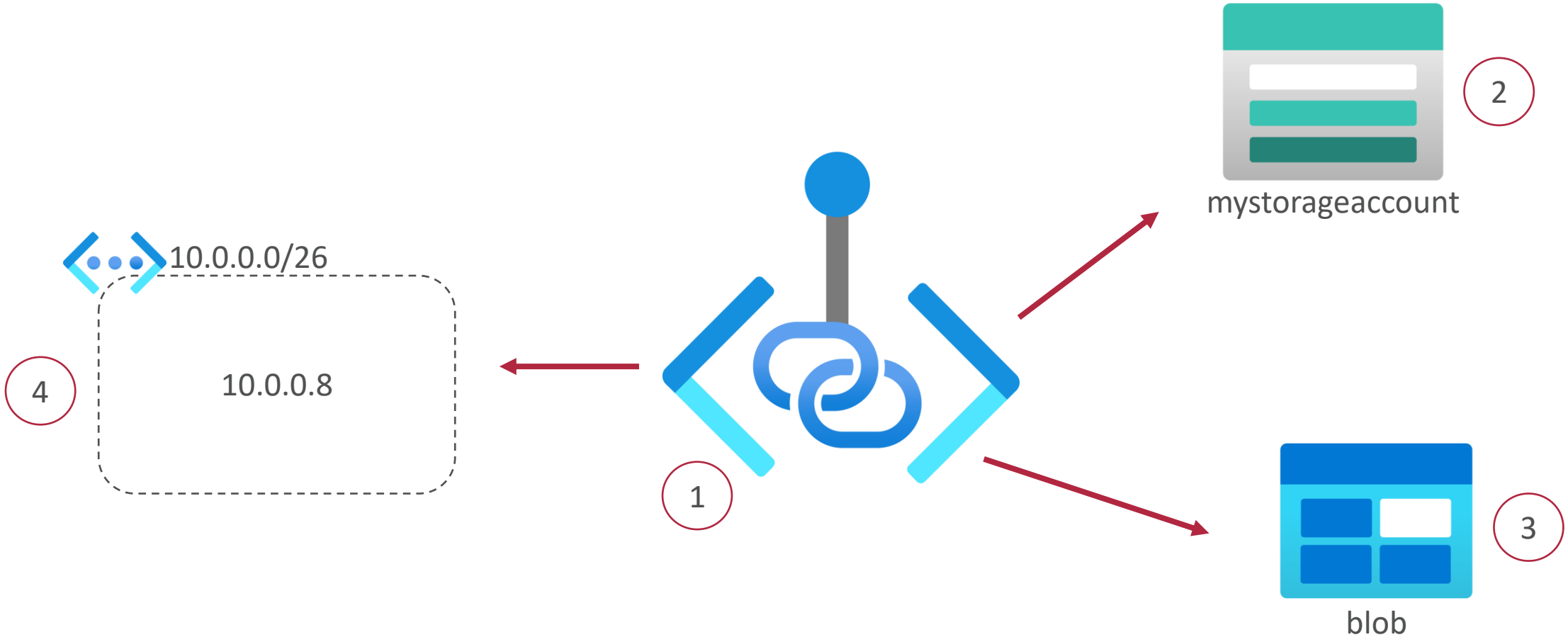
7 Steps to Success

1. Private Endpoint Resource
2. Coupled Azure Resource
3. Target Sub-resource
4. Virtual Network (IP Address)
5. Private DNS Zone Resource
6. A Record
7. Virtual Network Link

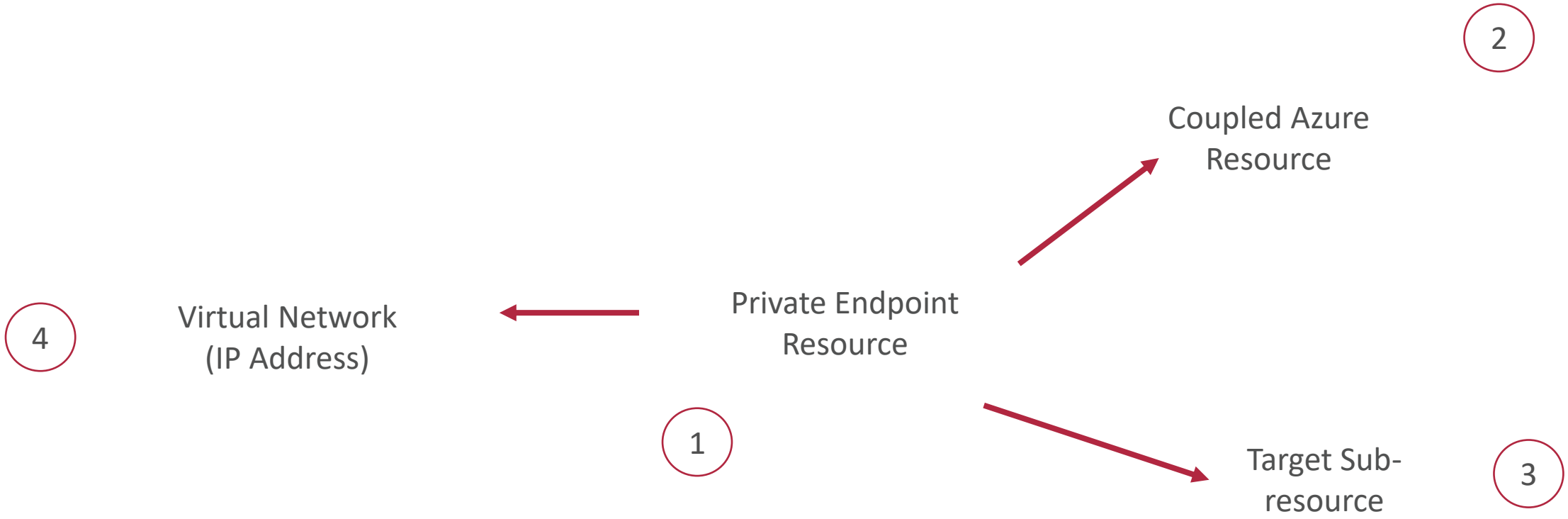
Steps 1 – 4: Private Endpoints

Private Endpoint

Steps 1 – 4: Private Endpoint

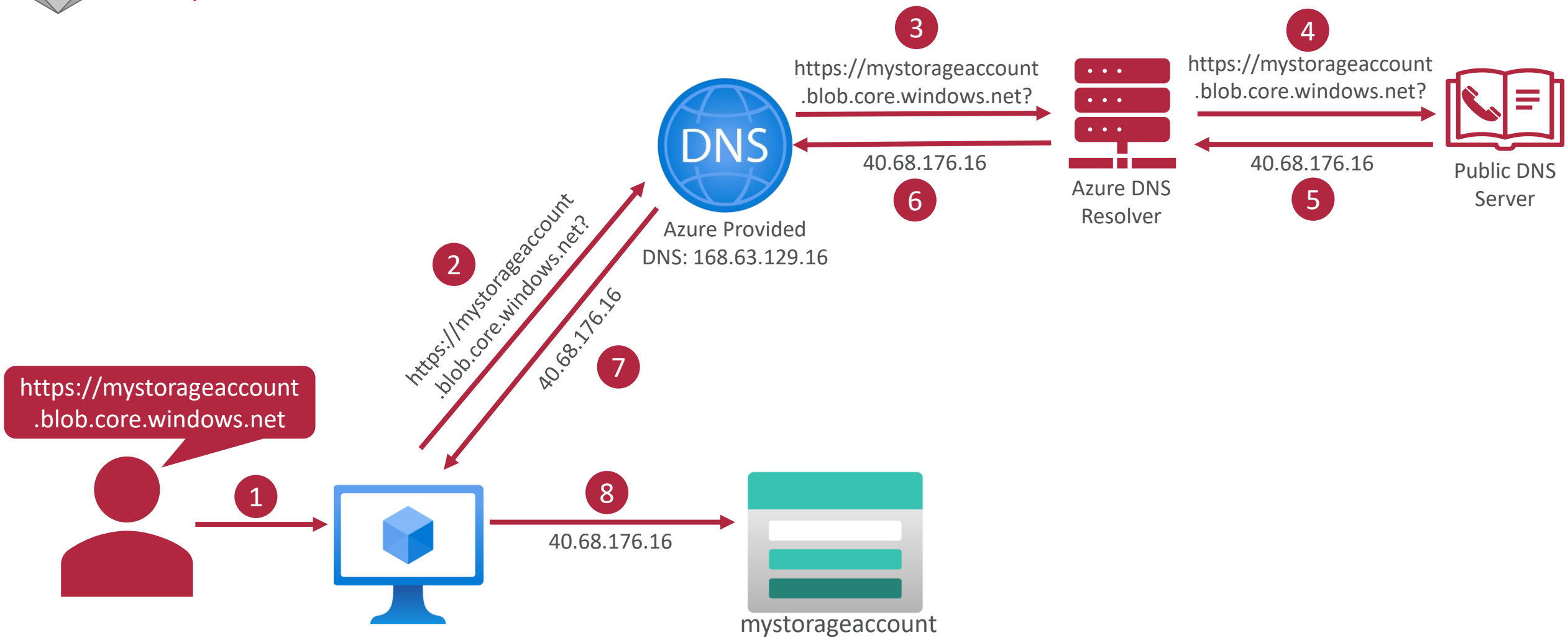


Steps 1 – 4: Private Endpoint



Private DNS Zone

Steps 5 – 7: Private DNS Zone

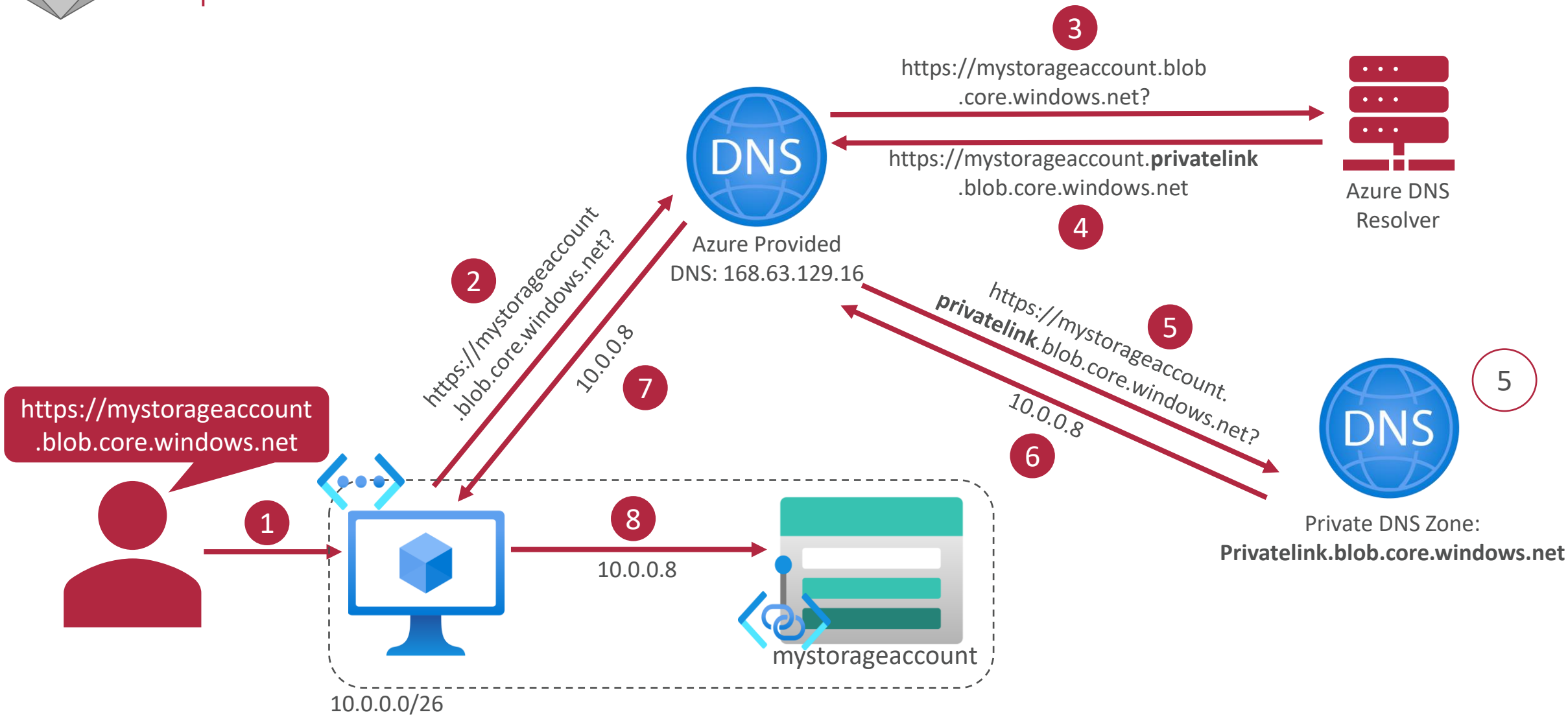


Steps 5 – 7: Private DNS Zone

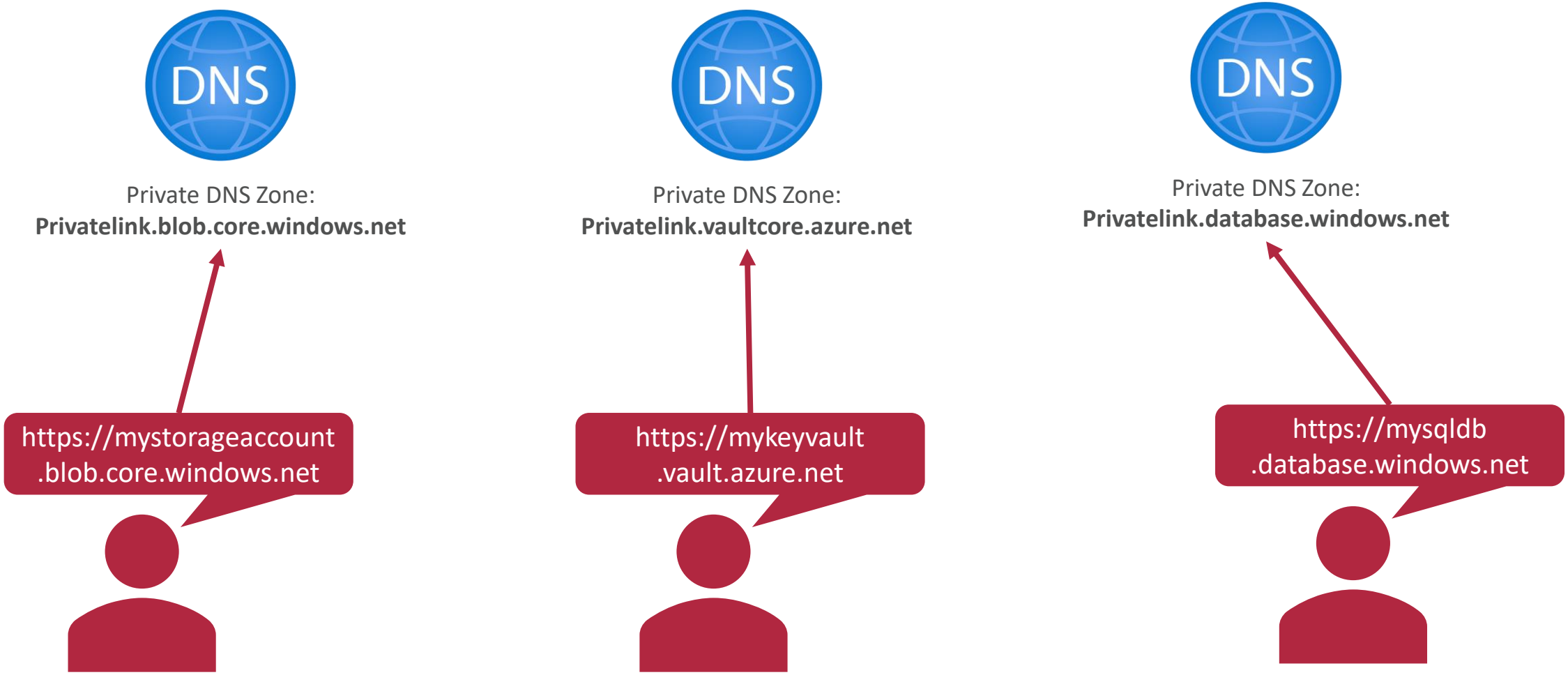
Azure Private DNS Zones:

- Azure Resource;
- Global resource, expected to be centralised;
- Private phonebook – not resolvable from the internet.

Steps 5 – 7: Private DNS Zone



Steps 5 – 7: Private DNS Zone



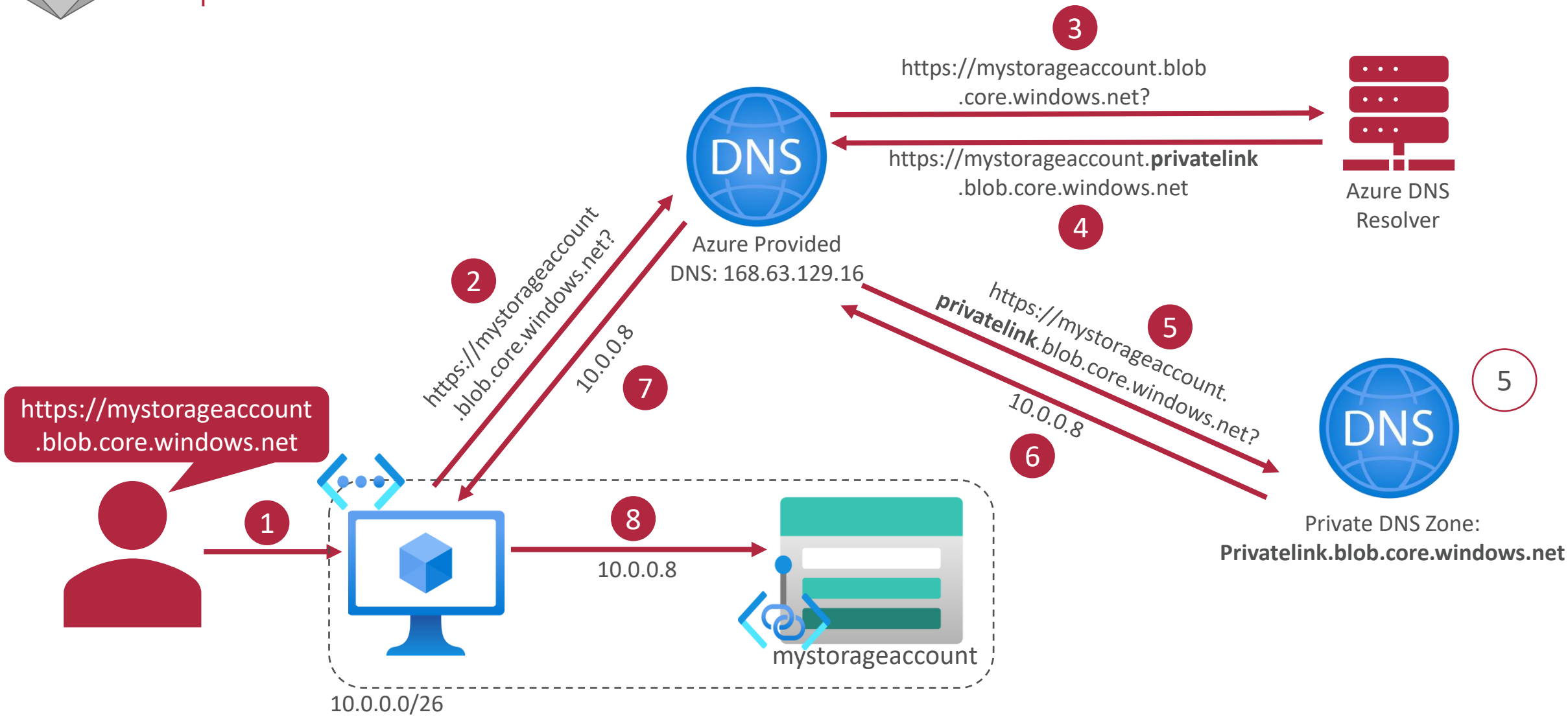
Steps 5 – 7: Private DNS Zone

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns

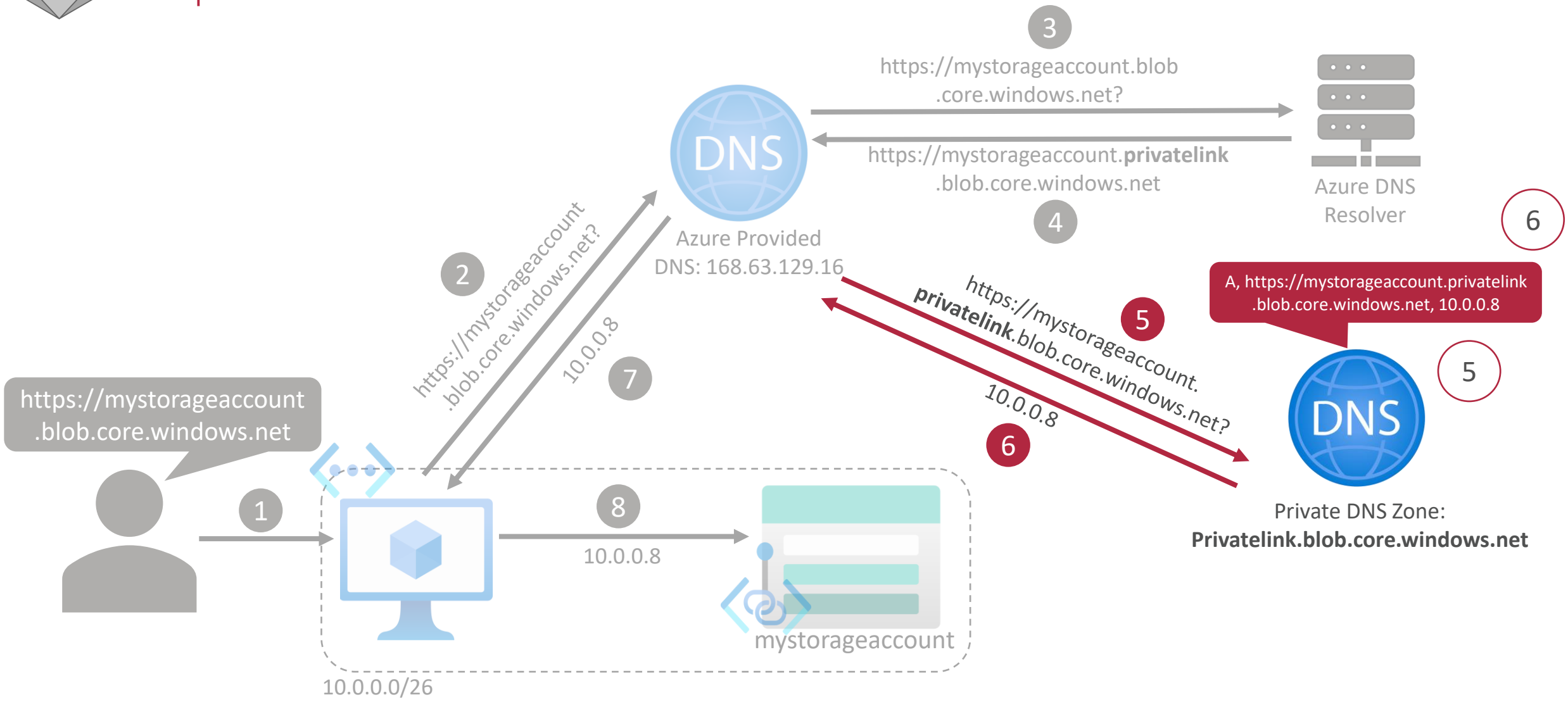
For Azure services, use the recommended zone names as described in the following table:

Private link resource type / Subresource	Private DNS zone name	Public DNS zone forwarders
Azure Automation / (Microsoft.Automation/automationAccounts) / Webhook, DSCAndHybridWorker	privatelink.azure-automation.net	azure-automation.net
Azure SQL Database (Microsoft.Sql/servers) / sqlServer	privatelink.database.windows.net	database.windows.net
Azure SQL Managed Instance (Microsoft.Sql/managedInstances)	privatelink.{dnsPrefix}.database.windows.net	{instanceName}.{dnsPrefix}.database.windows.net
Azure Synapse Analytics (Microsoft.Synapse/workspaces) / Sql	privatelink.sql.azuresynapse.net	sql.azuresynapse.net
Azure Synapse Analytics (Microsoft.Synapse/workspaces) / SqlOnDemand	privatelink.sql.azuresynapse.net	{workspaceName}-ondemand.sql.azuresynapse.net
Azure Synapse Analytics (Microsoft.Synapse/workspaces) / Dev	privatelink.dev.azuresynapse.net	dev.azuresynapse.net
Azure Synapse Studio (Microsoft.Synapse/privateLinkHubs) / Web	privatelink.azuresynapse.net	azuresynapse.net
Storage account (Microsoft.Storage/storageAccounts) / Blob (blob, blob_secondary)	privatelink.blob.core.windows.net	blob.core.windows.net
Storage account	privatelink.table.core.windows.net	table.core.windows.net

Steps 5 – 7: Private DNS Zone



Steps 5 – 7: Private DNS Zone



A Record

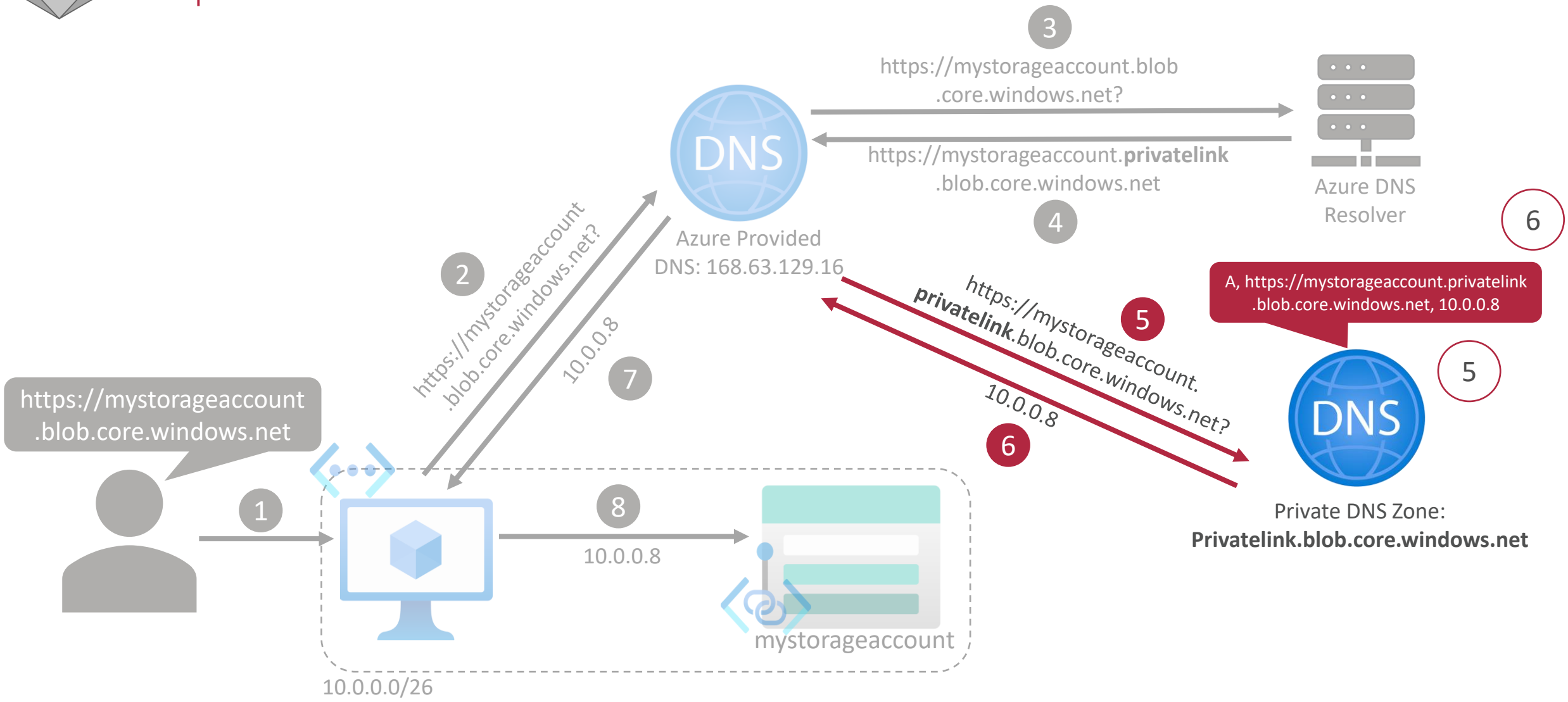
Steps 5 – 7: A Record

DNS Records are the **instructions** that live in the DNS Servers (the phonebook) on **how to handle DNS queries** for a particular **domain**.

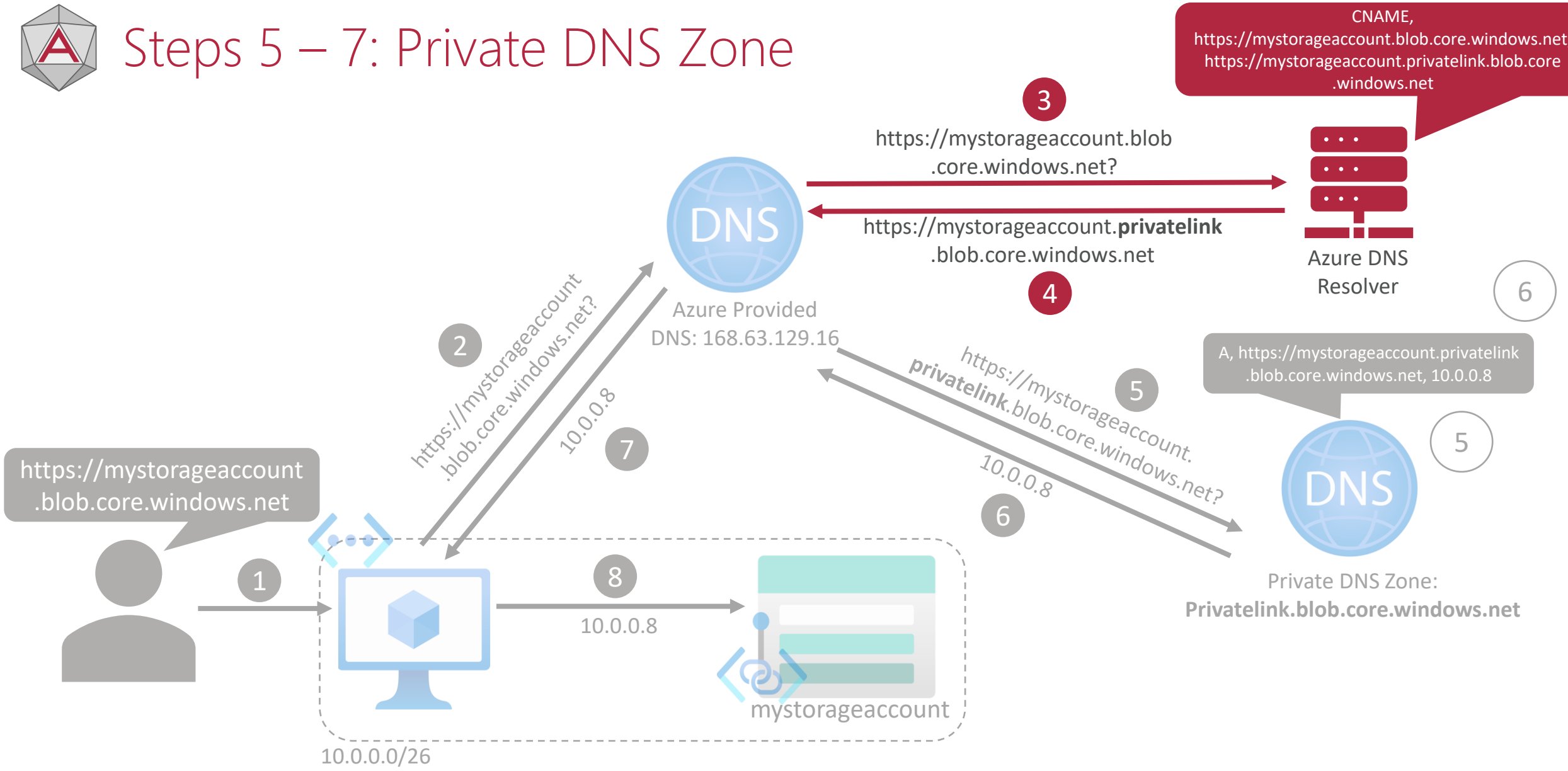
There are lots of types of DNS Records.

A Records contain a domain's associated **IP Addresses**.

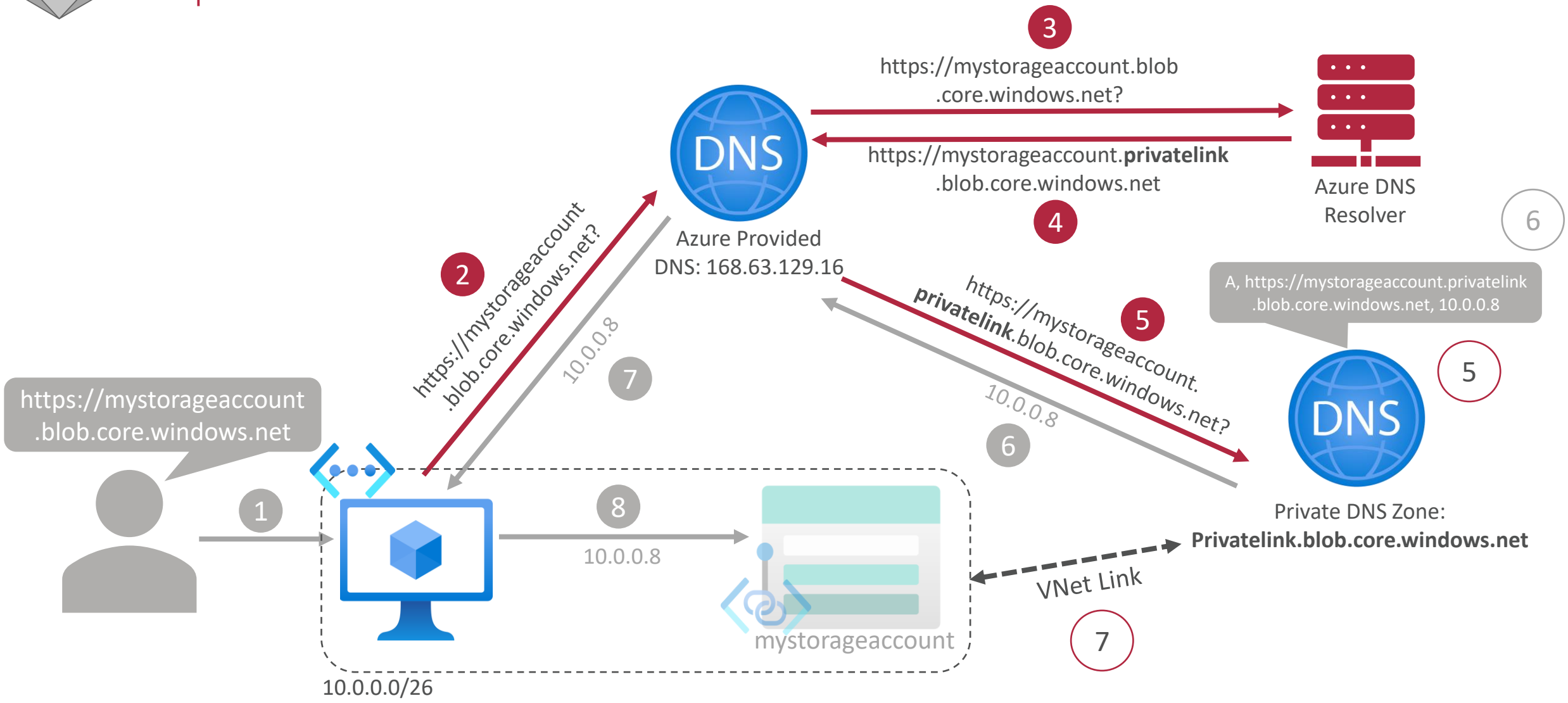
Steps 5 – 7: Private DNS Zone



Steps 5 – 7: Private DNS Zone



Steps 5 – 7: Private DNS Zone



VNet Link

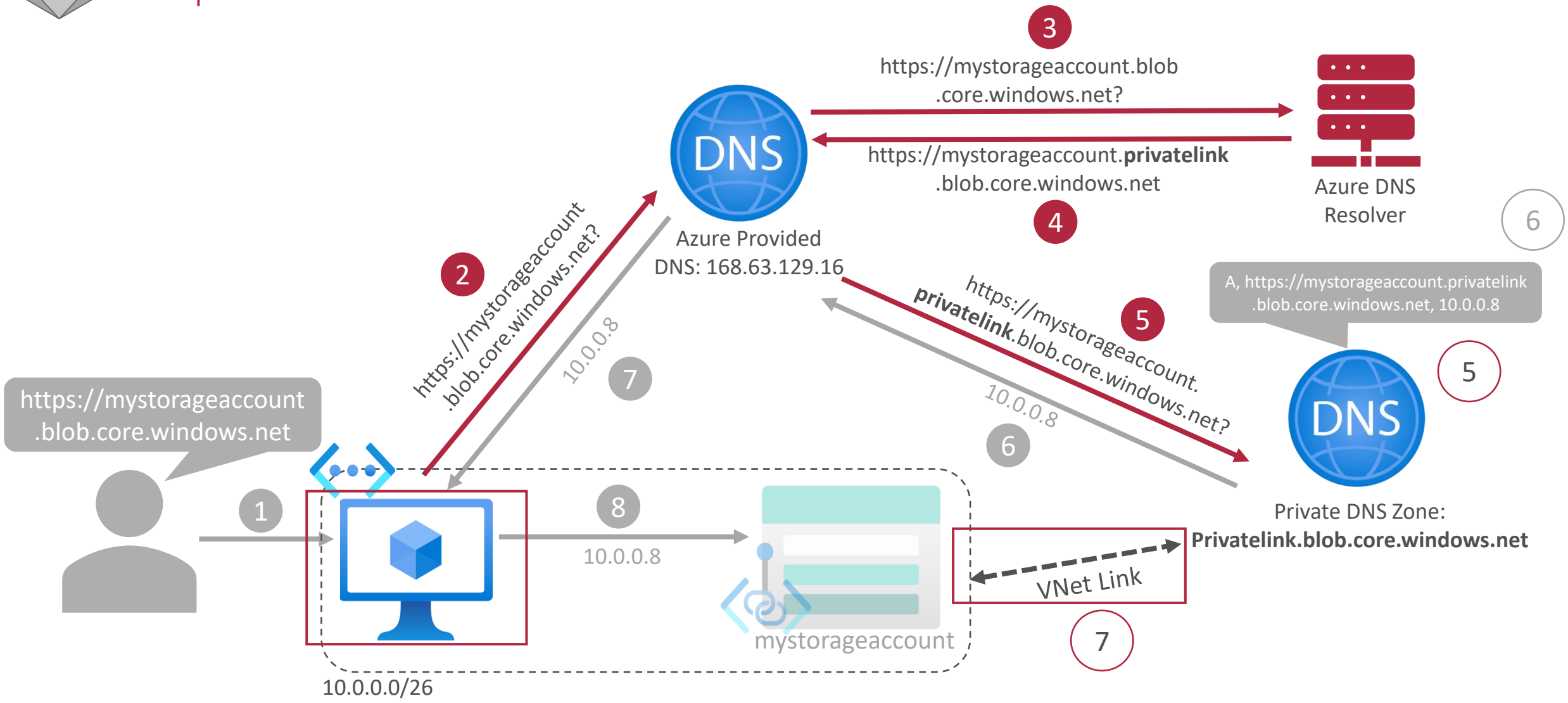
Steps 5 – 7: VNet Link

By default, **VNets are not aware of Private DNS Zones**, so any client (e.g. a VM) inside the VNet cannot use the zones to look up IP addresses.

We have to **explicitly connect** VNets to Private DNS Zones. This is called a **VNet Link**.

Once a VNet is linked to a Private DNS Zone, any client within that VNet can successfully **send DNS queries** to that zone.

Steps 5 – 7: Private DNS Zone



7 Steps to Success

1. Private Endpoint Resource
2. Coupled Azure Resource
3. Target Sub-resource
4. Virtual Network (IP Address)
5. Private DNS Zone Resource
6. A Record
7. Virtual Network Link

Demo: Setting up a private endpoint

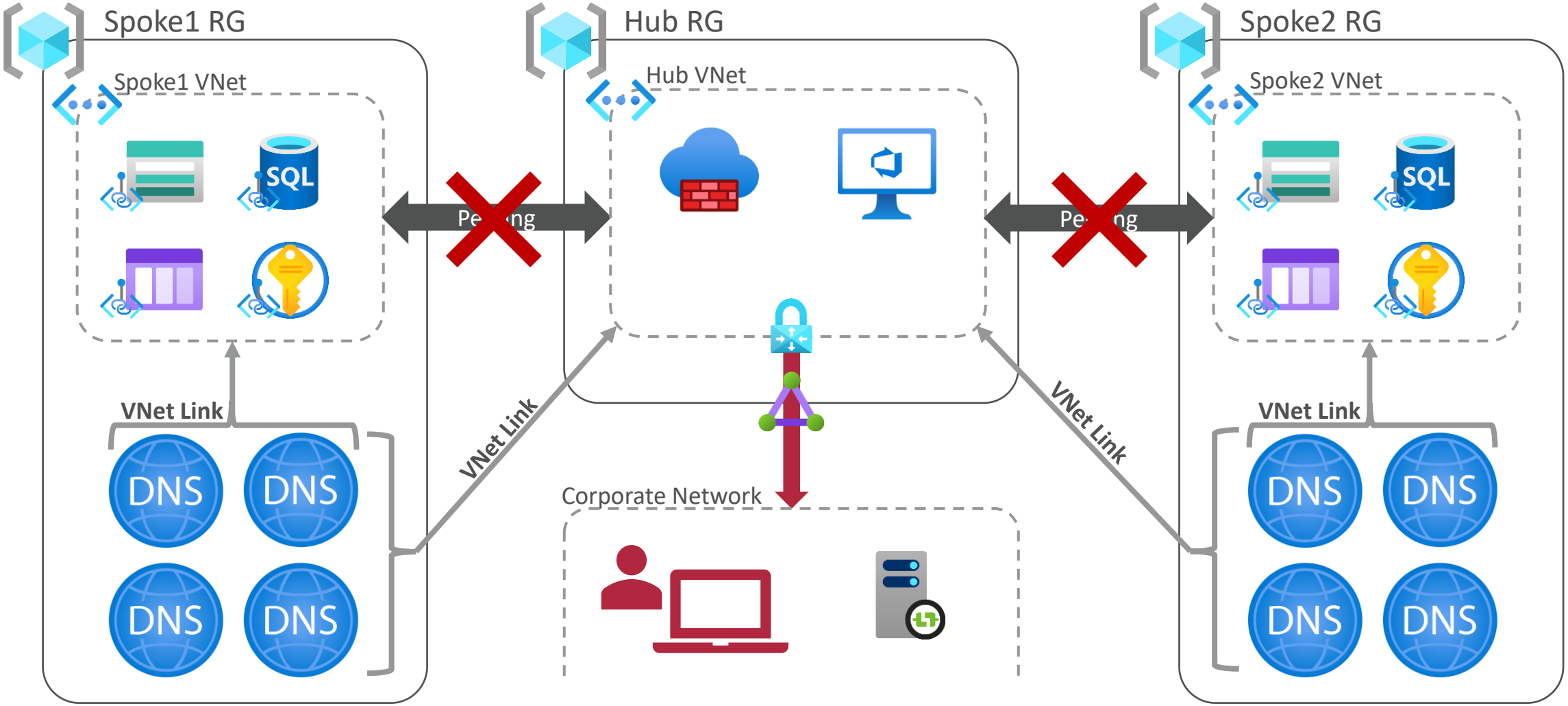
Common mistakes

Common Mistakes

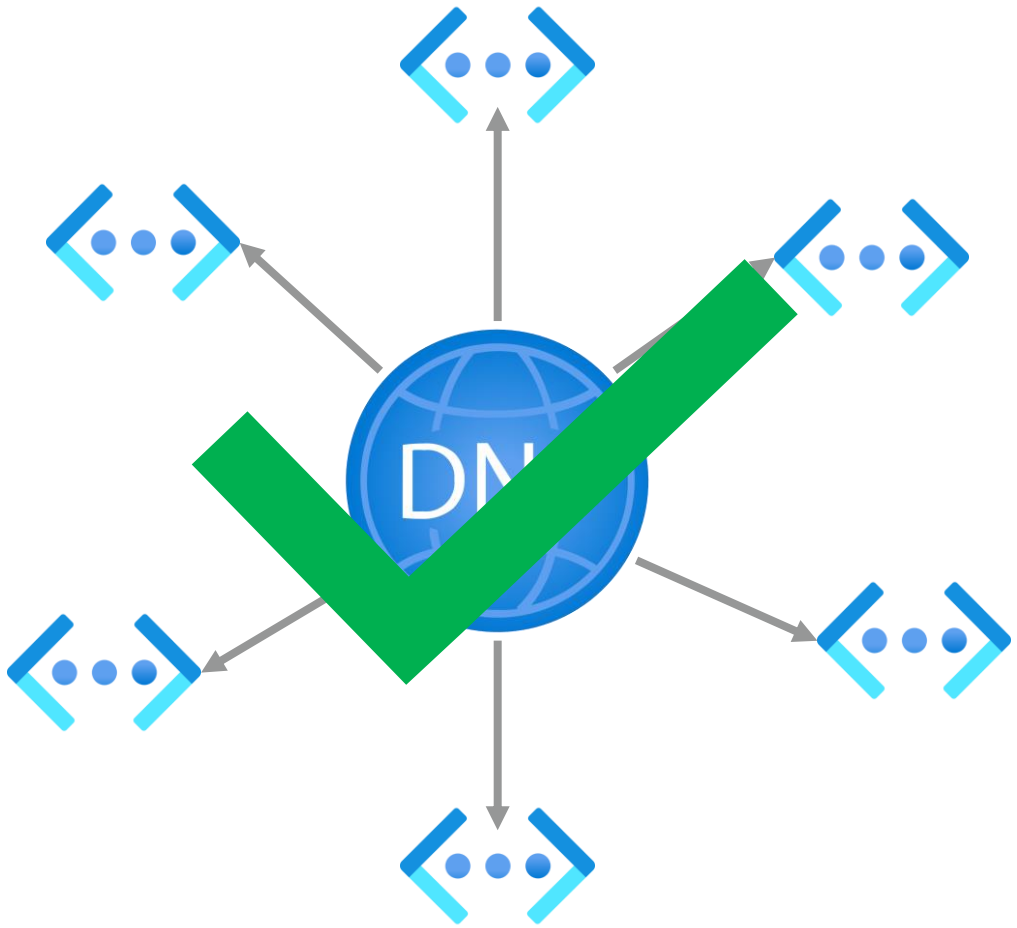
1. Non-centralised Private DNS Zones

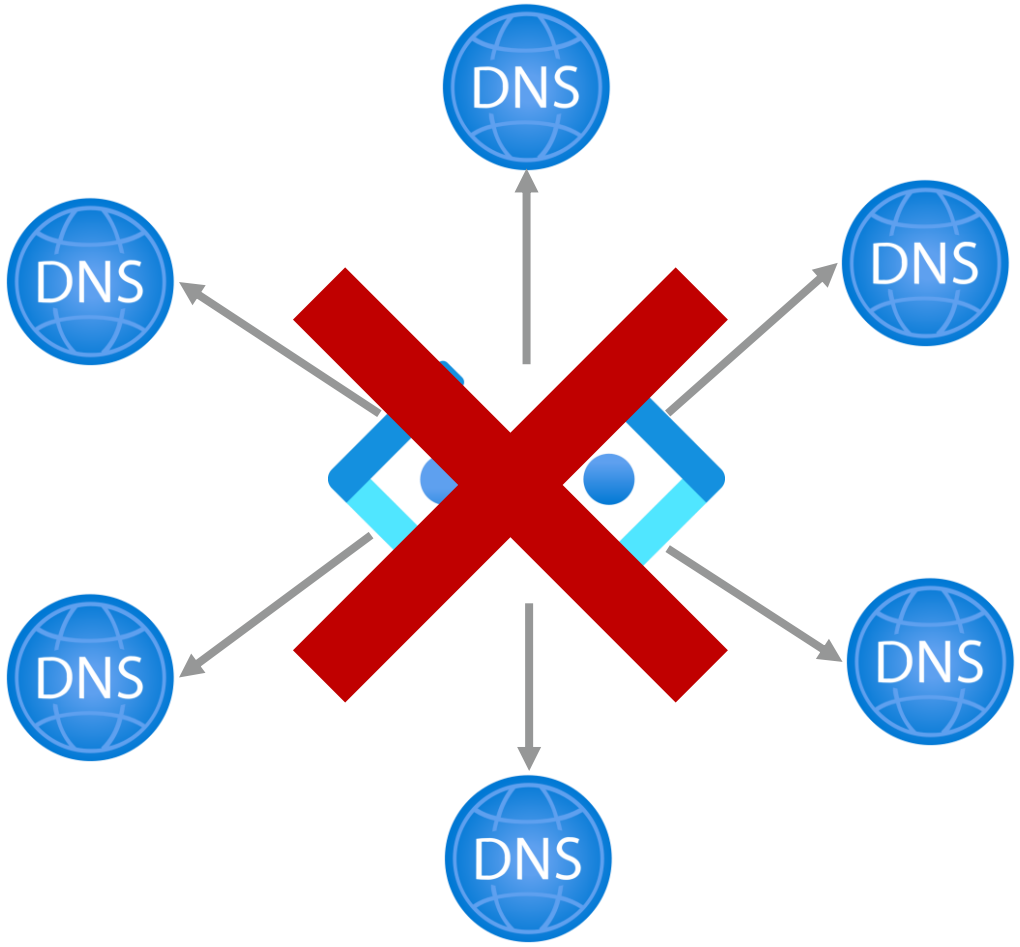
2. Using the “Selected Networks” option instead of “Disable all public access”

1. Non-centralised Private DNS Zones

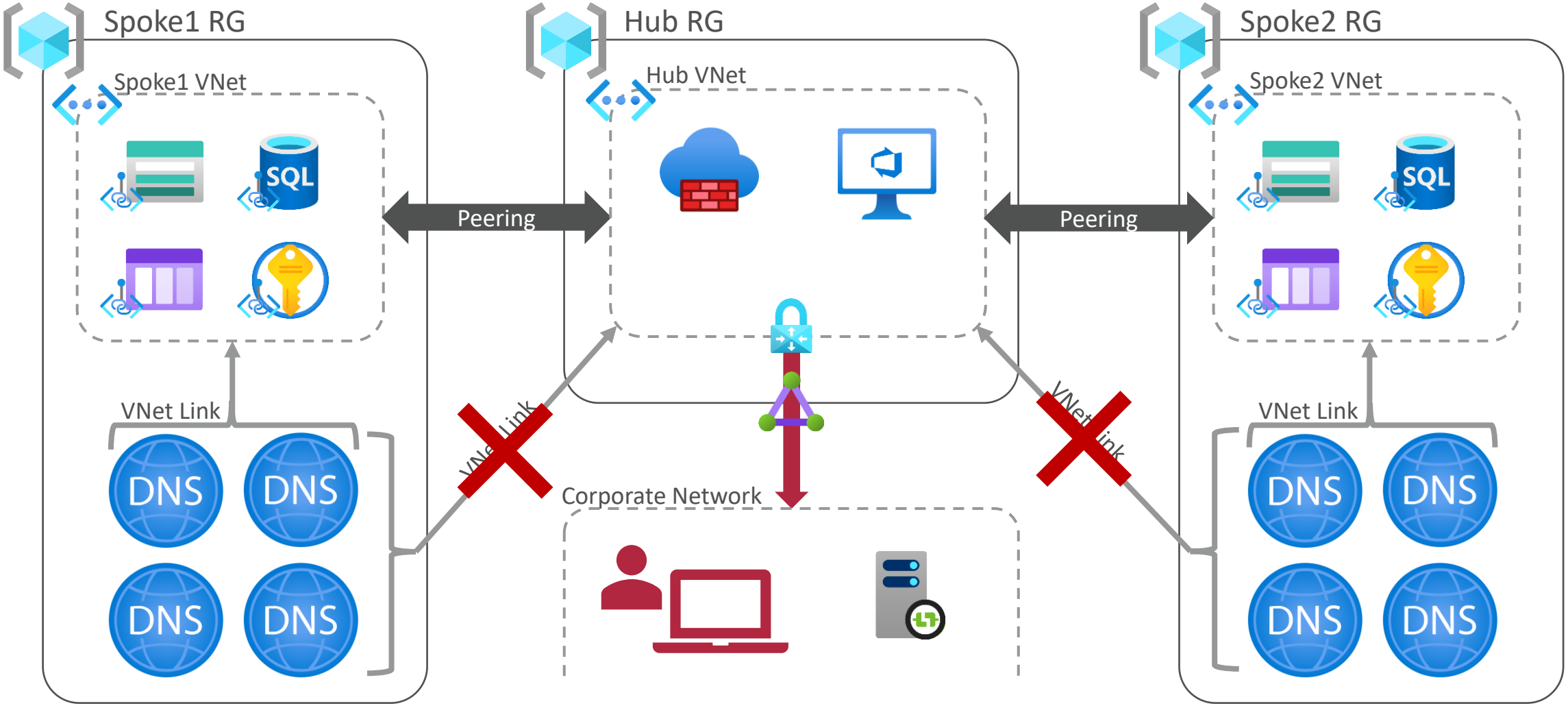


1. Non-centralised Private DNS Zones

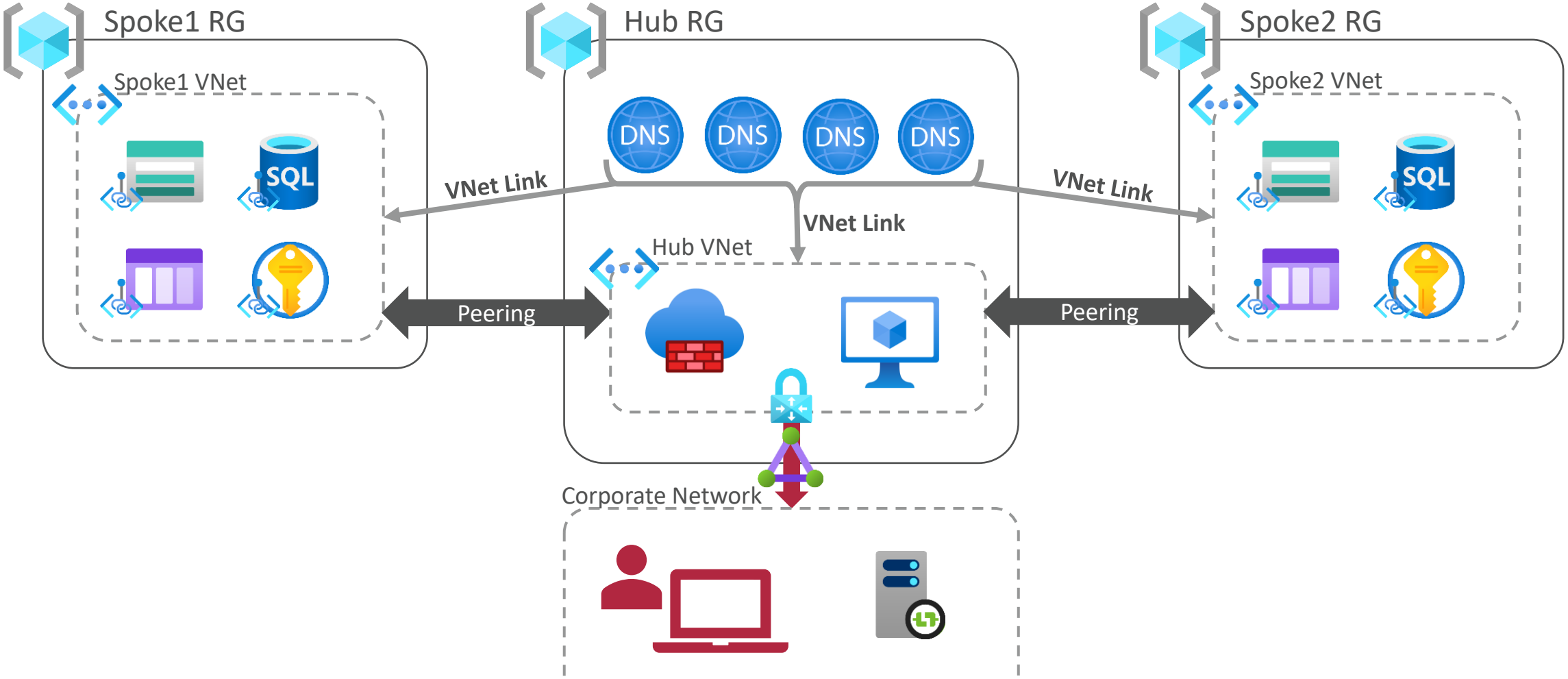




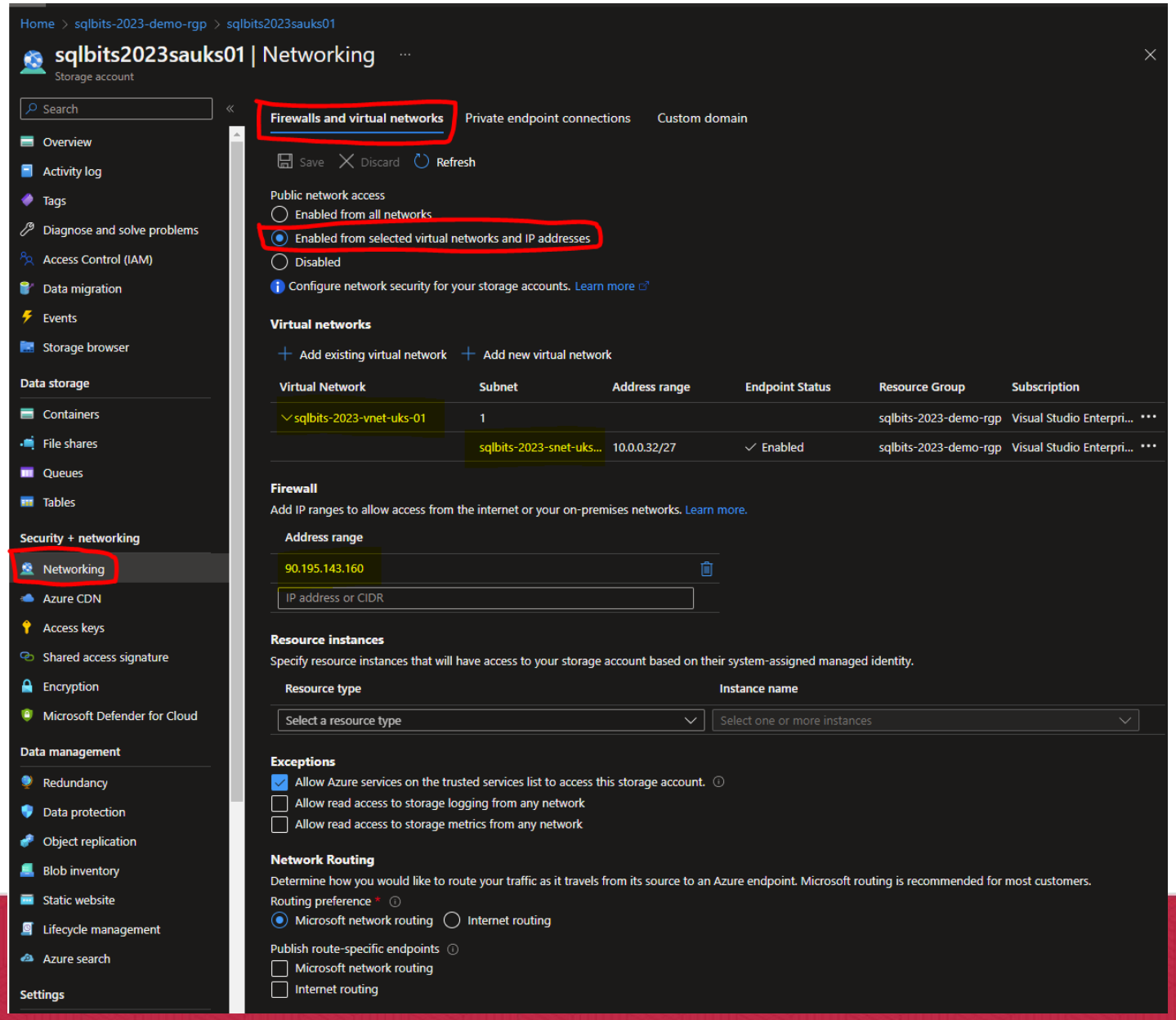
1. Non-centralised Private DNS Zones



1. Non-centralised Private DNS Zones

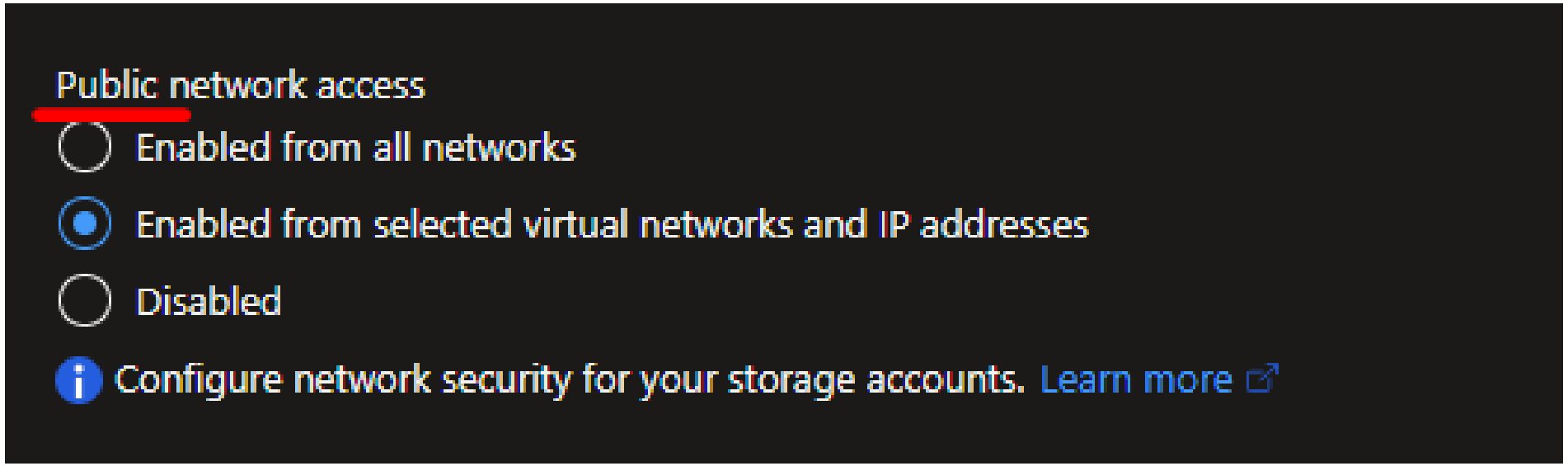


2. Using “Selected Networks” option

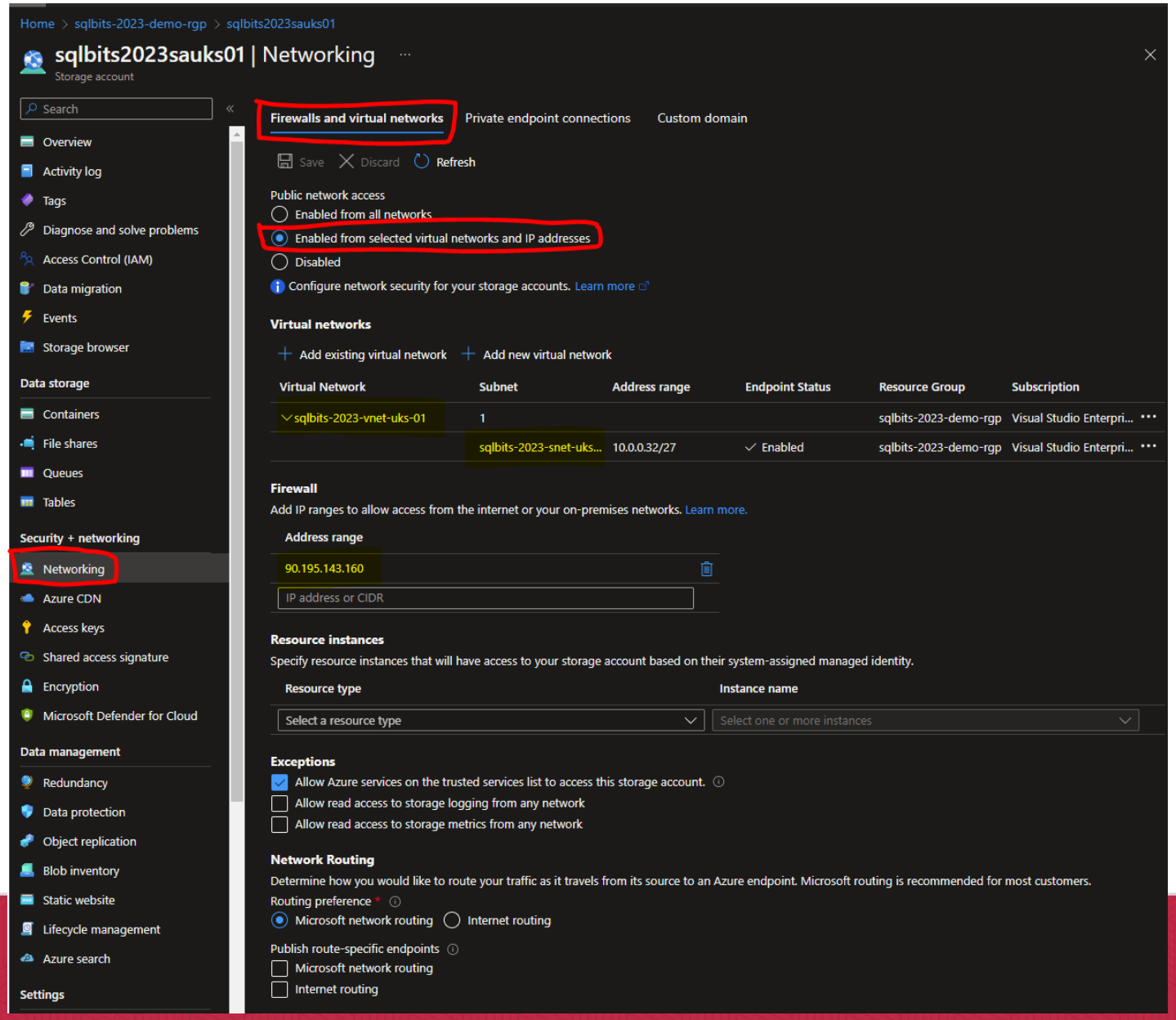


ADVANCING ANALYTICS

2. Using “Selected Networks” option



2. Using “Selected Networks” option



ADVANCING ANALYTICS

Thank you!
Any Questions?

 Grace O'Halloran (grace-o-halloran)

 @graceaohalloran

 grace@advancinganalytics.co.uk

 www.thinkingacloud.co.uk