

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



@ADVANCINGANALYTICS



@ADVANALYTICSUK



/ADVANCING ANALYTICS



www.advancinganalytics.co.uk

Introduction



@ADVANCINGANALYTICS



@ADVANALYTICSUK



/ADVANCING ANALYTICS



Introduction

in Grace O'Halloran (grace-o-halloran)

 @graceaohalloran

 grace@advancinganalytics.co.uk

 www.thinkingacloud.co.uk

 [https://github.com/gracedev94/
GraceOH-CommunityContent](https://github.com/gracedev94/GraceOH-CommunityContent)



**ADVANCING
ANALYTICS**



www.advancinganalytics.co.uk

What to expect



@ADVANCINGANALYTICS



@ADVANALYTICSUK



/ADVANCING ANALYTICS



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
- Demo

35
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?

Public Endpoints



Public IP Addresses

Private Endpoints



Private IP Addresses



Why is it more secure?





Why is it more secure?

Public Endpoint	Public Endpoint with Selected Networks enabled	Private Endpoint
<ul style="list-style-type: none">• Location information is publicly available; the IP address is resolvable from the public internet.• By default, anyone on the public internet has access.	<ul style="list-style-type: none">• Location information is publicly available; the IP address is resolvable from the public internet.• Restricted access to selected networks and IP addresses.	<ul style="list-style-type: none">• Location information is not publicly available; the IP address is not resolvable from the public internet.• Can only access from within the private network.

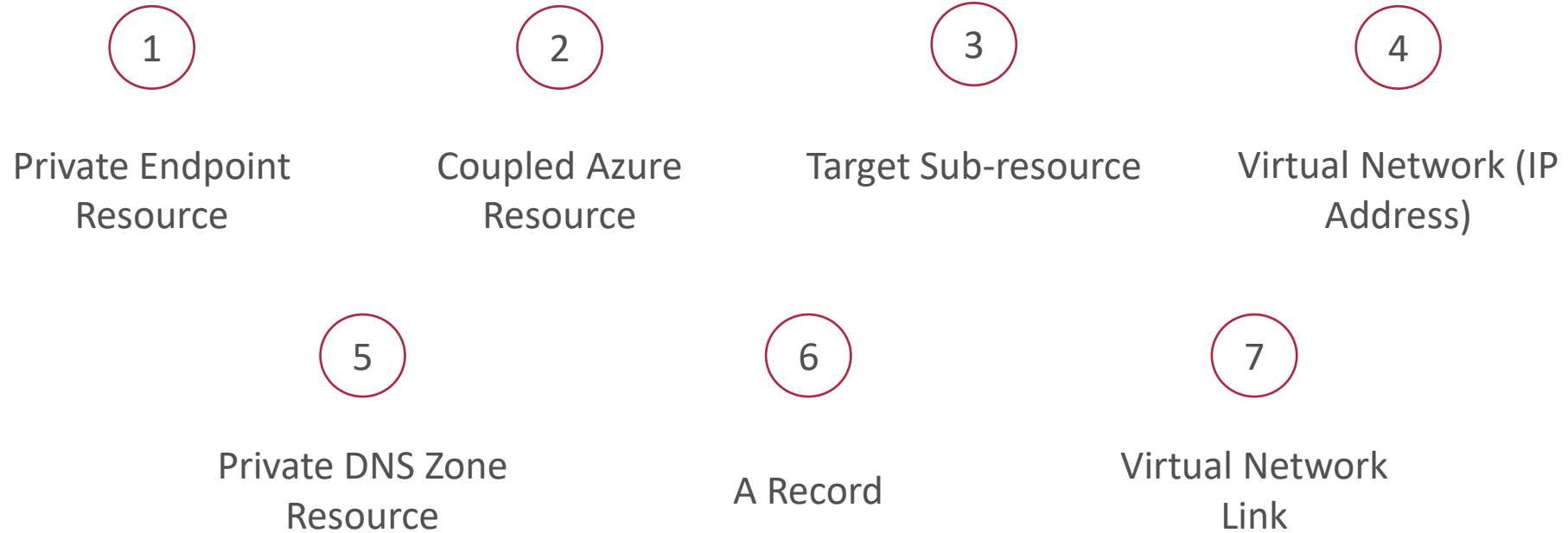


7 Steps to Success!





7 Steps to Success





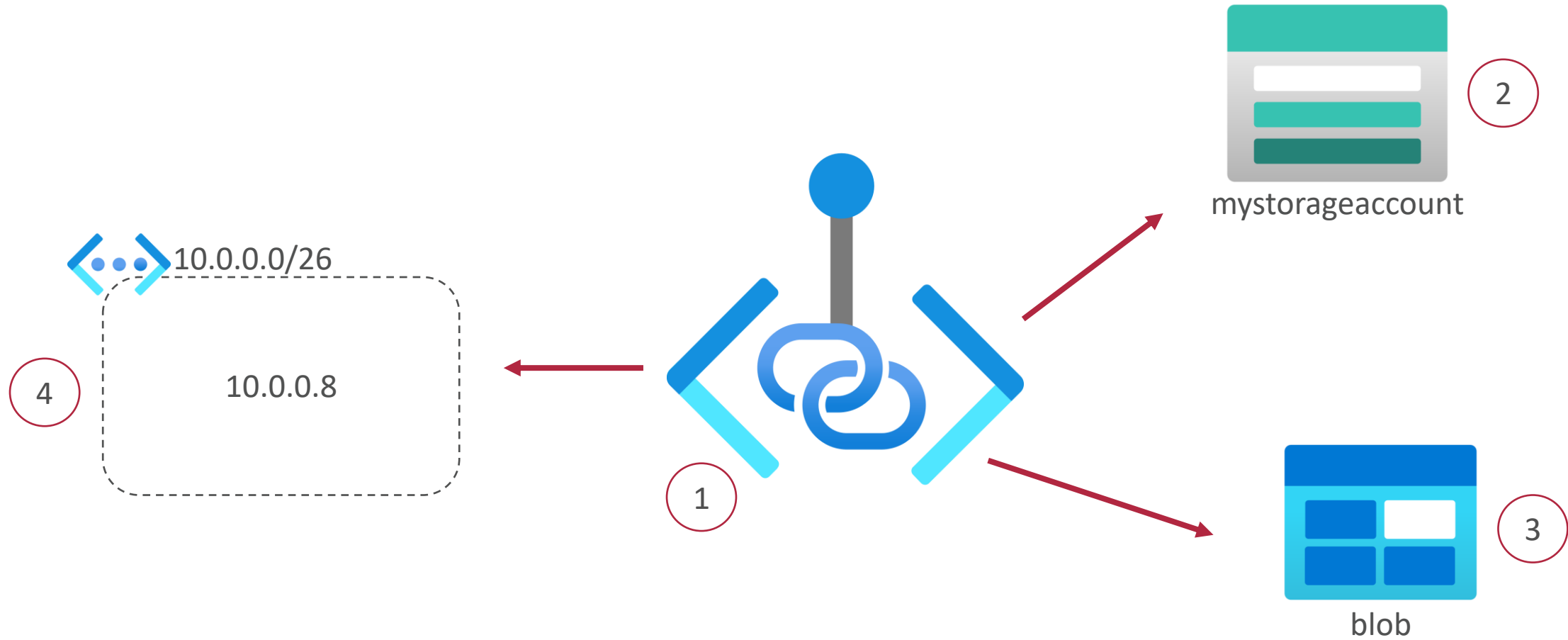
Steps 1 – 4: Private Endpoints

1

Private Endpoint

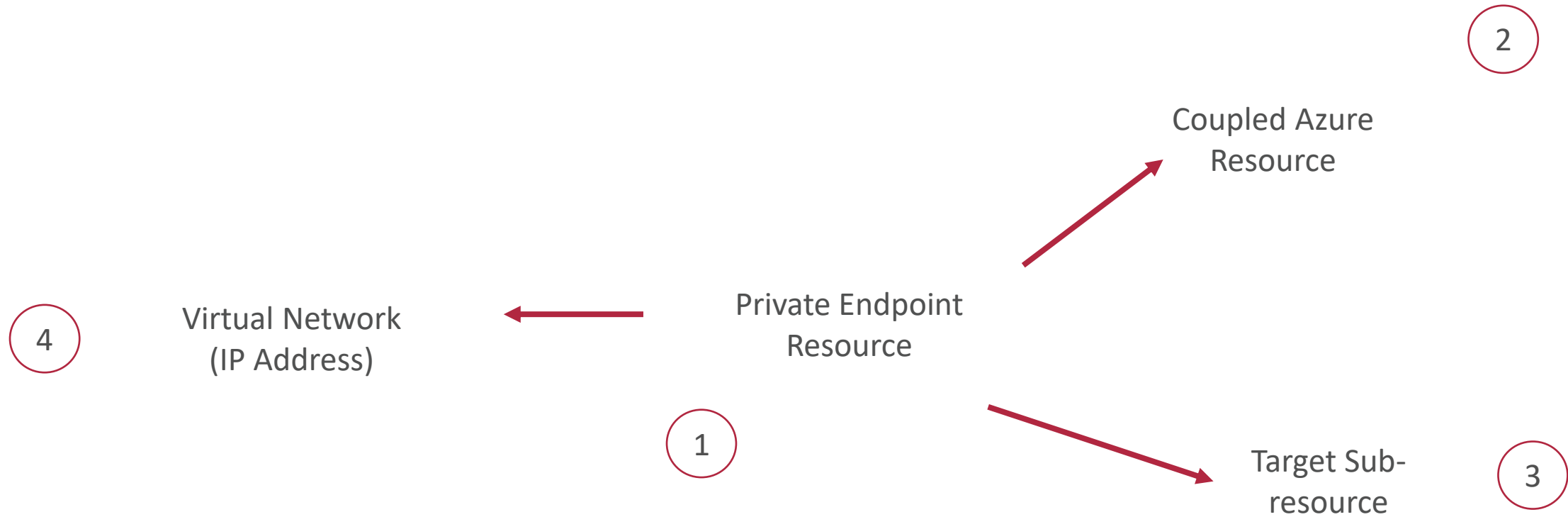


Steps 1 – 4: Private Endpoint





Steps 1 – 4: Private Endpoint





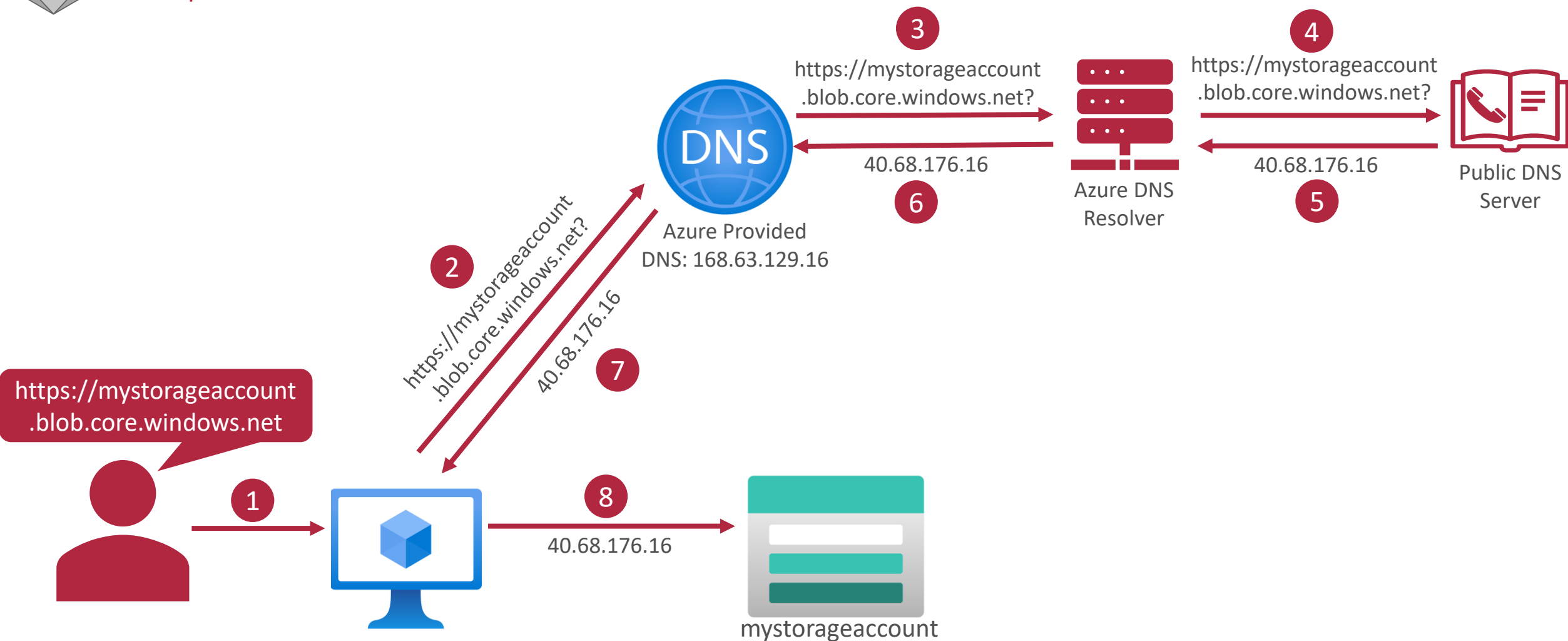
Steps 5 – 7: Private DNS Zone

5

Private DNS Zone



Steps 5 – 7: Private DNS Zone





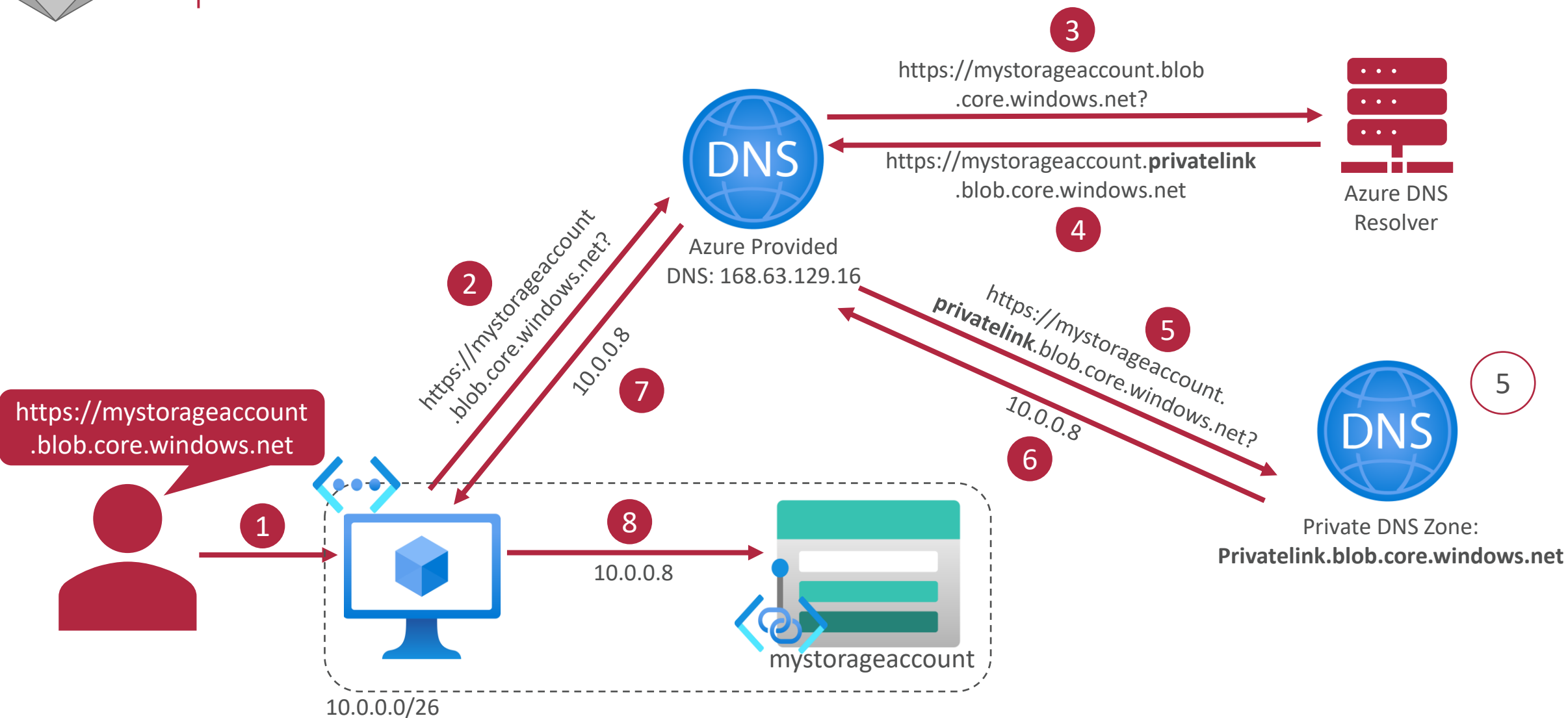
Steps 5 – 7: Private DNS Zone

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



Private DNS Zone:
Privatelink.blob.core.windows.net

[https://mystorageaccount
.blob.core.windows.net](https://mystorageaccount.blob.core.windows.net)



Private DNS Zone:
Privatelink.vaultcore.azure.net

[https://mykeyvault
.vault.azure.net](https://mykeyvault.vault.azure.net)



Private DNS Zone:
Privatelink.database.windows.net

[https://mysqldb
.database.windows.net](https://mysqldb.database.windows.net)





Steps 5 – 7: Private DNS Zone

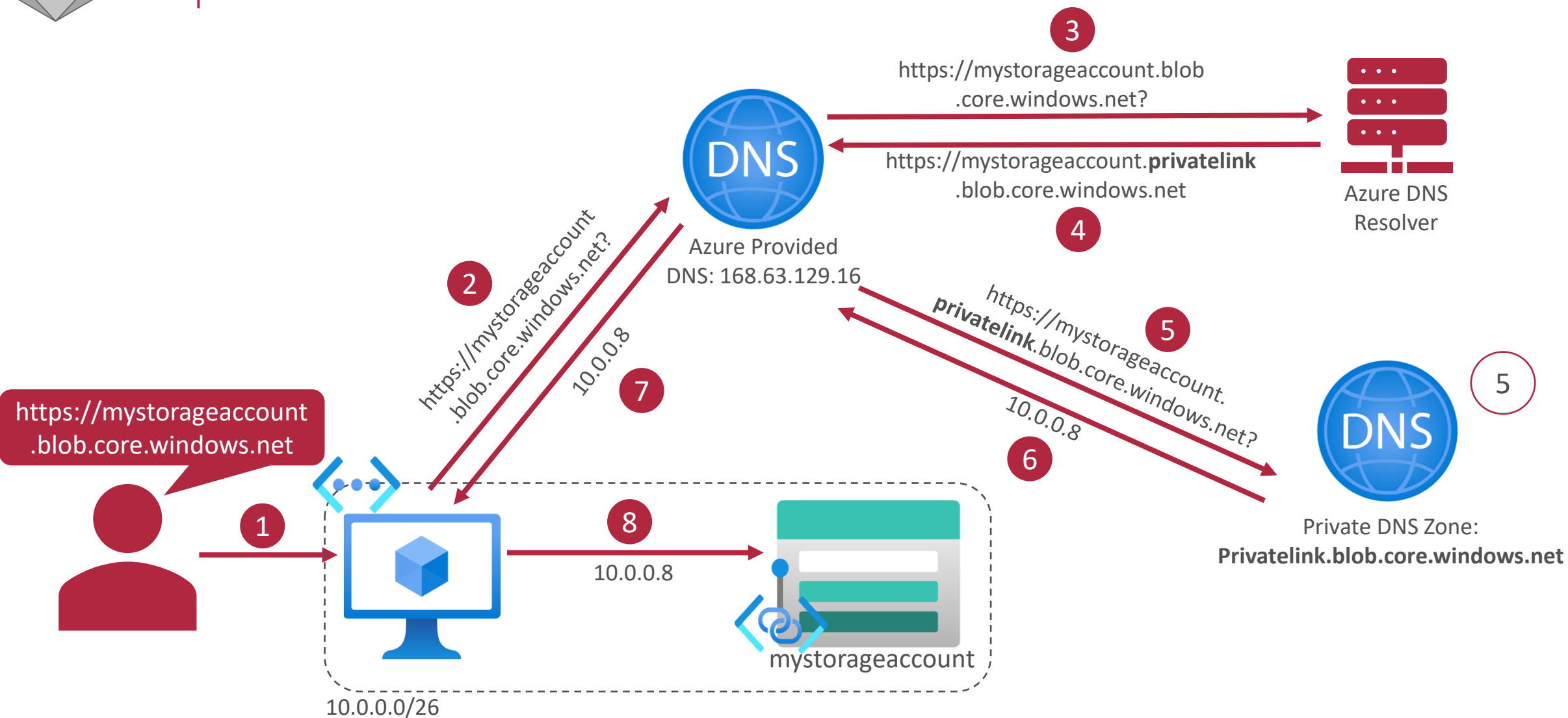
<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns>

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 (Microsoft.Storage/storageAccounts) / Table	privatelink.table.core.windows.net	table.core.windows.net

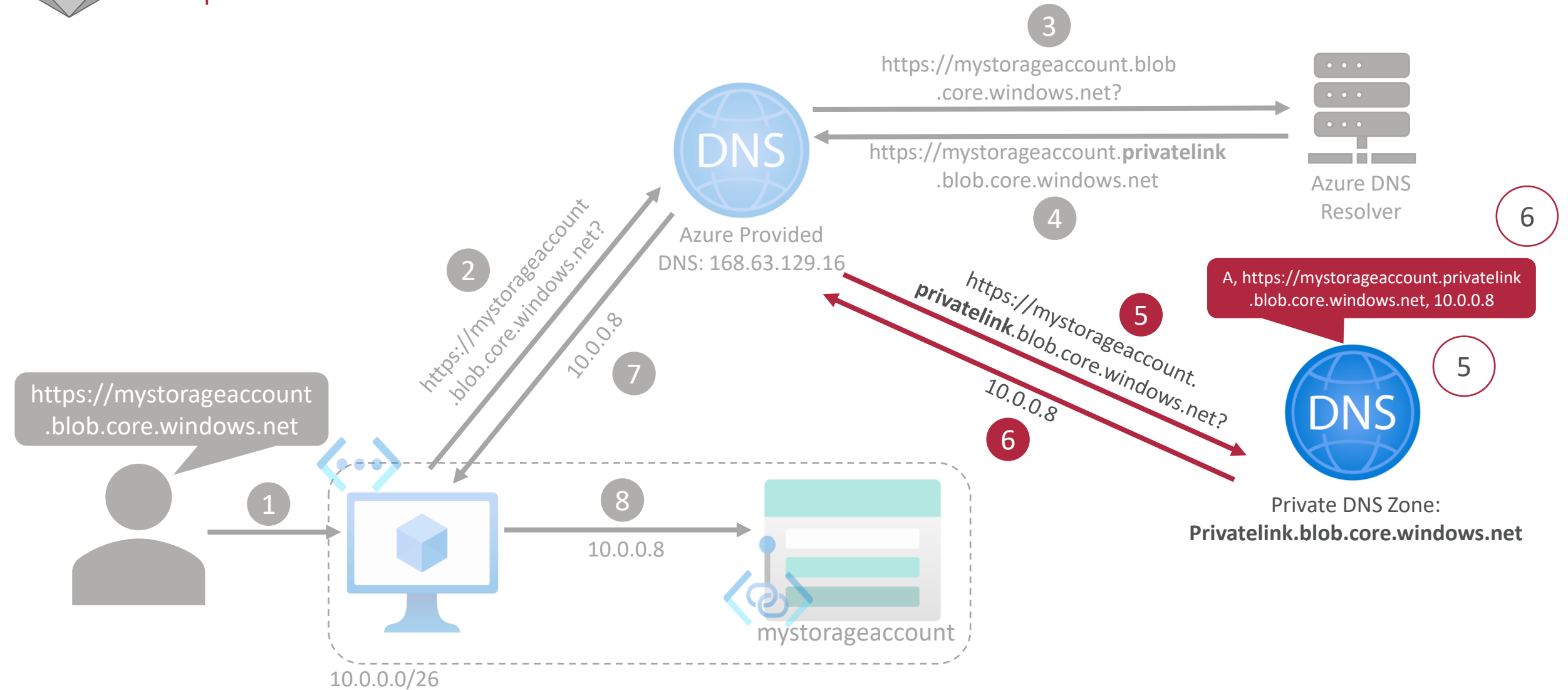


Steps 5 – 7: Private DNS Zone





Steps 5 – 7: Private DNS Zone





Steps 5 – 7: A Record

6

A Record



Steps 5 – 7: A Record

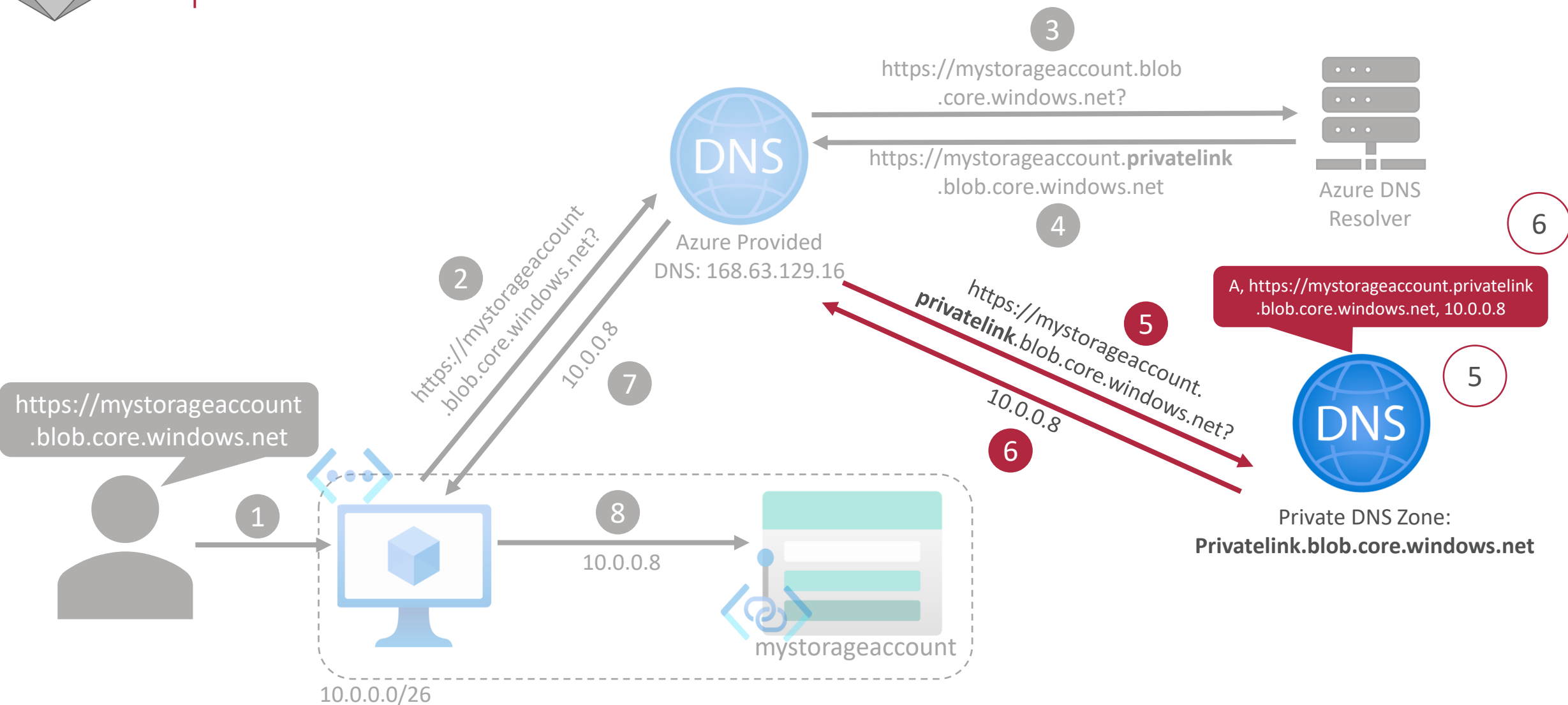
DNS Records are the **instructions** that live in the DNS Servers (the phonebook) on **how to handle DNS queries** for a particular **domain**.

There are lots of types of DNS Records.

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

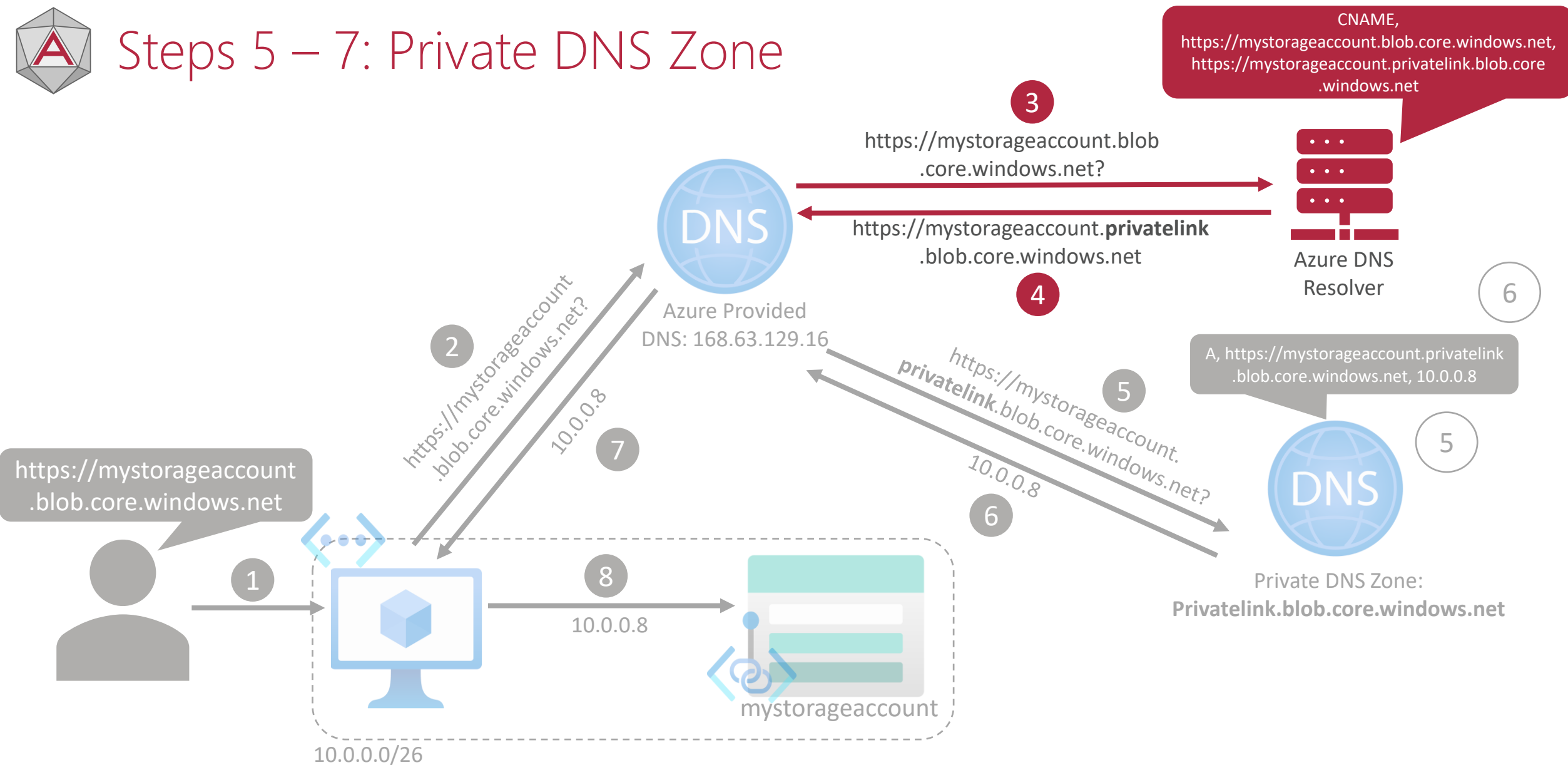


Steps 5 – 7: Private DNS Zone



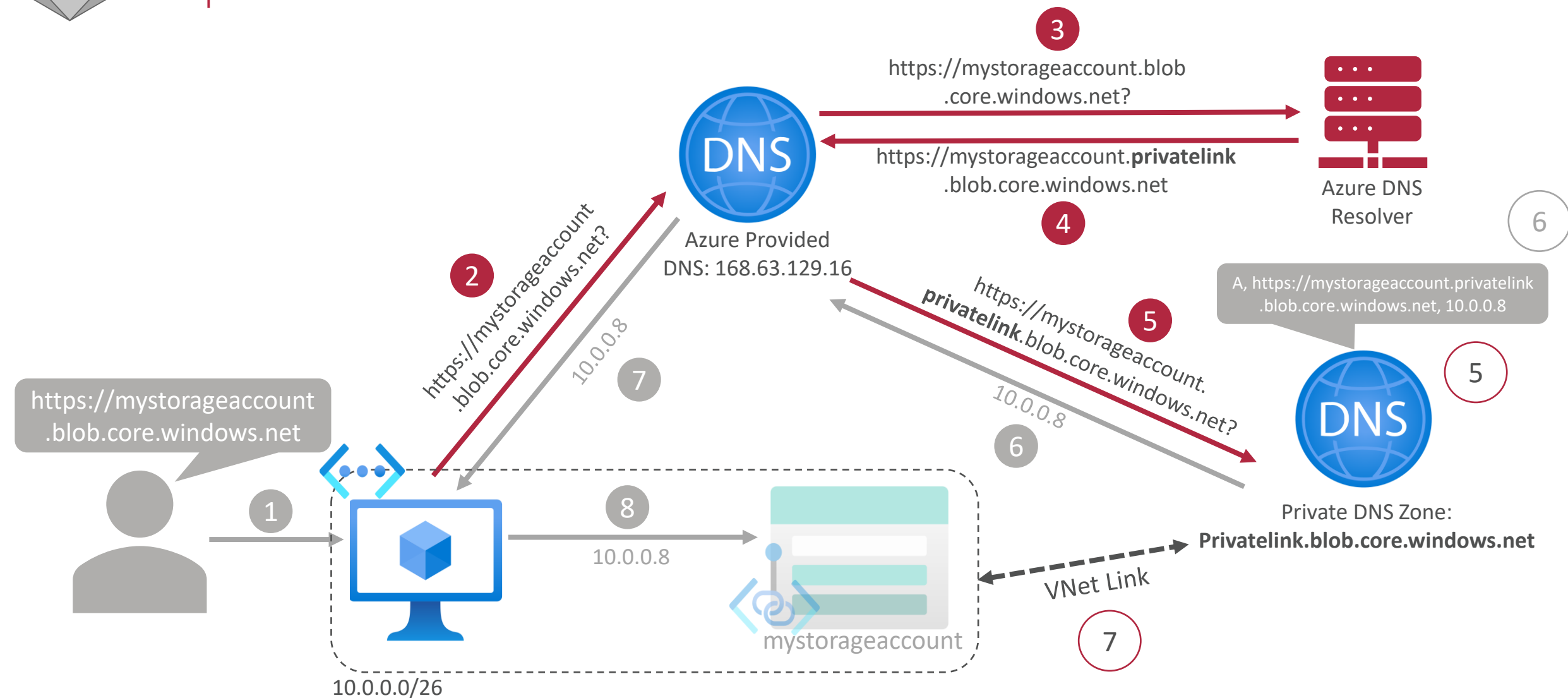


Steps 5 – 7: Private DNS Zone





Steps 5 – 7: Private DNS Zone





Steps 5 – 7: VNet Link

7

VNet Link



Steps 5 – 7: VNet Link

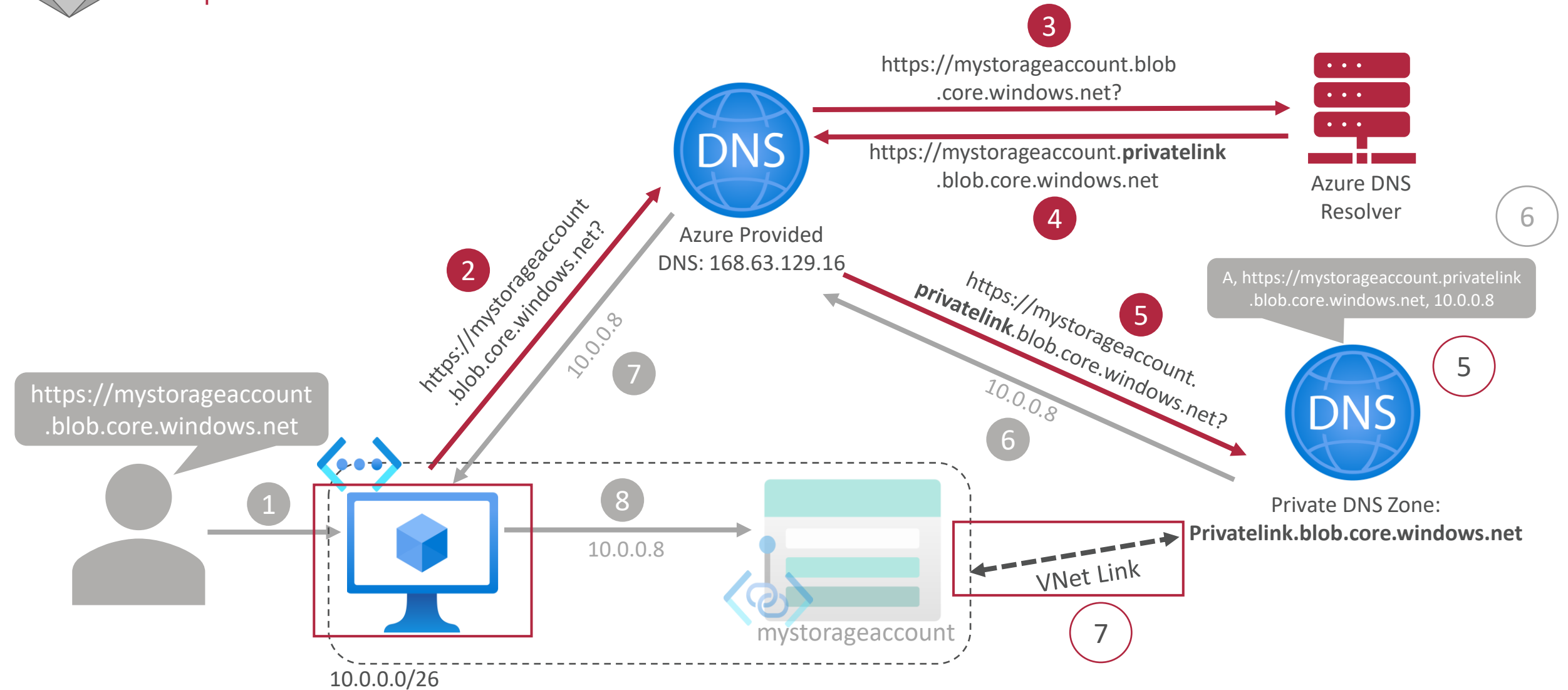
By default, **VNets are not aware of Private DNS Zones**, so any client (e.g. a VM) inside the VNet cannot use the zones to look up IP addresses.

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

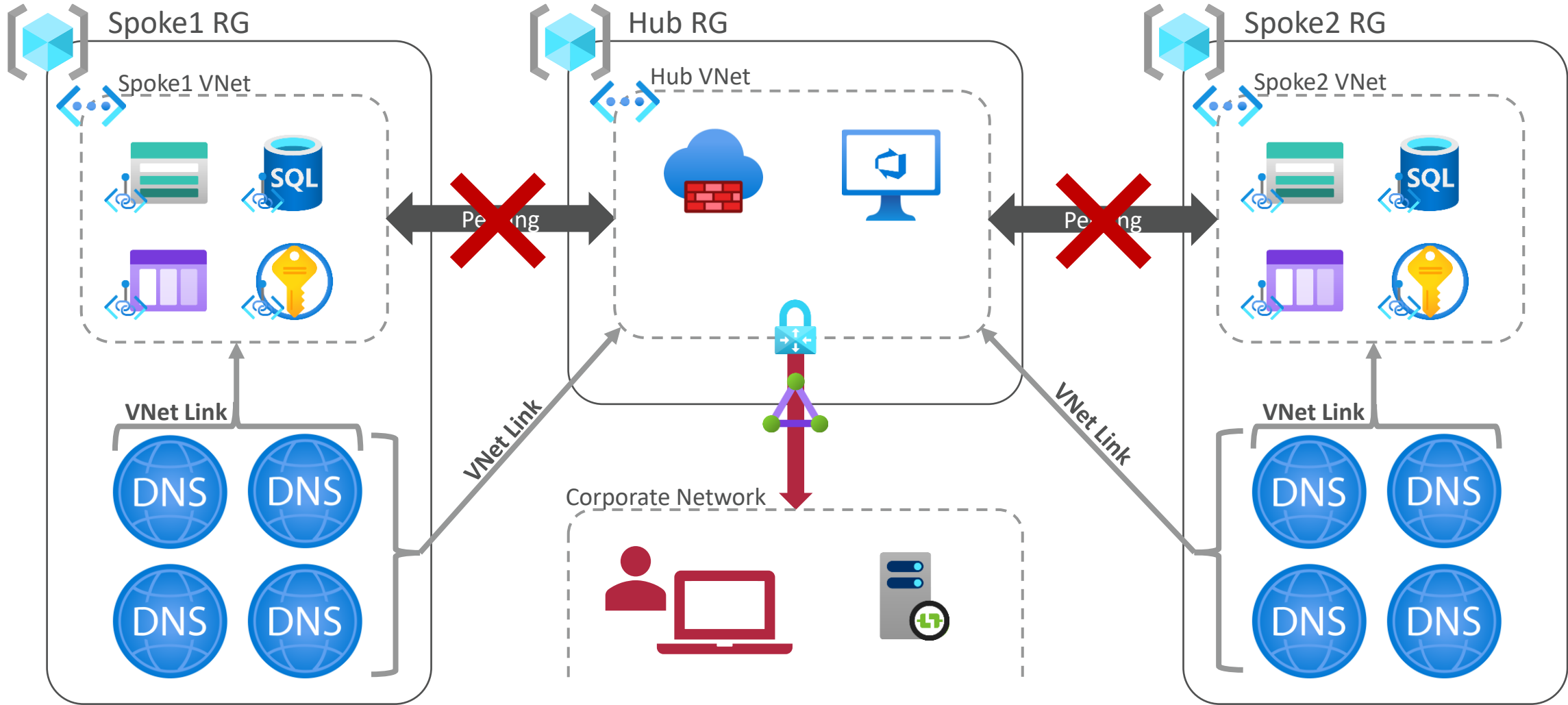
Non-centralised Private
DNS Zones

2

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

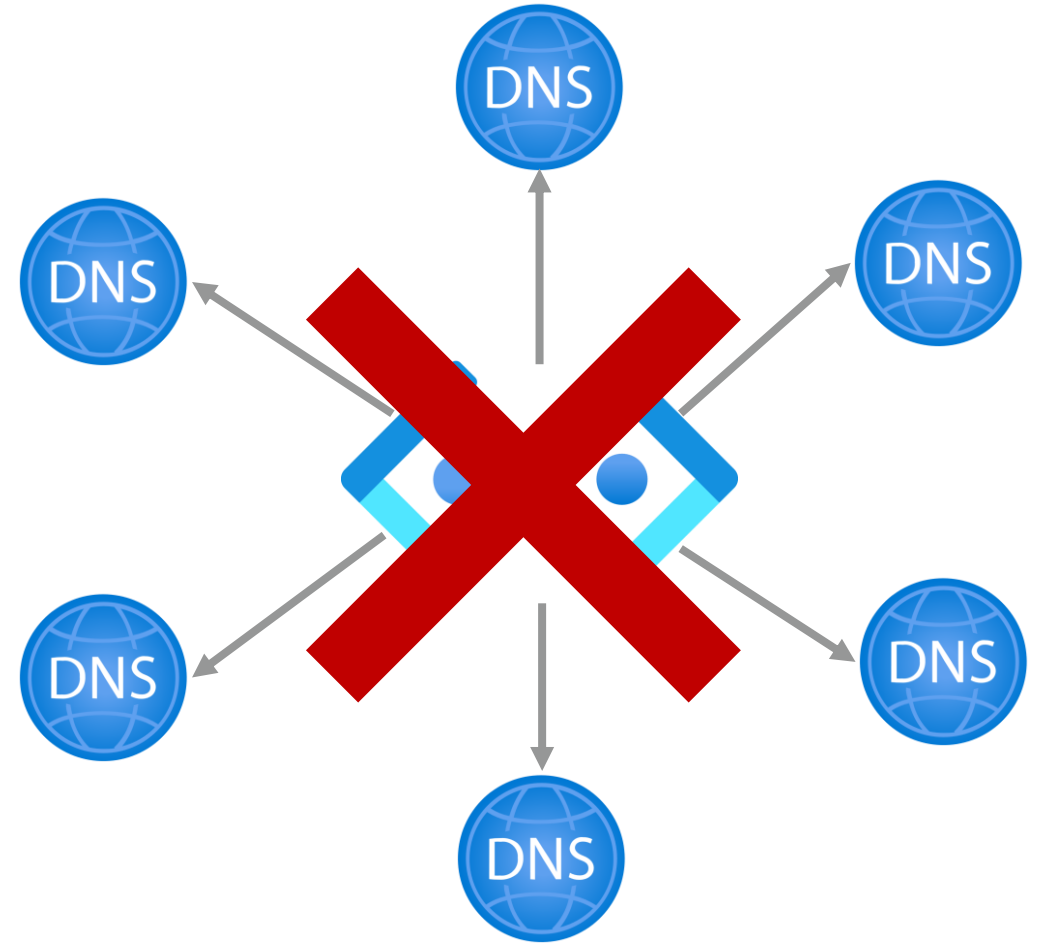
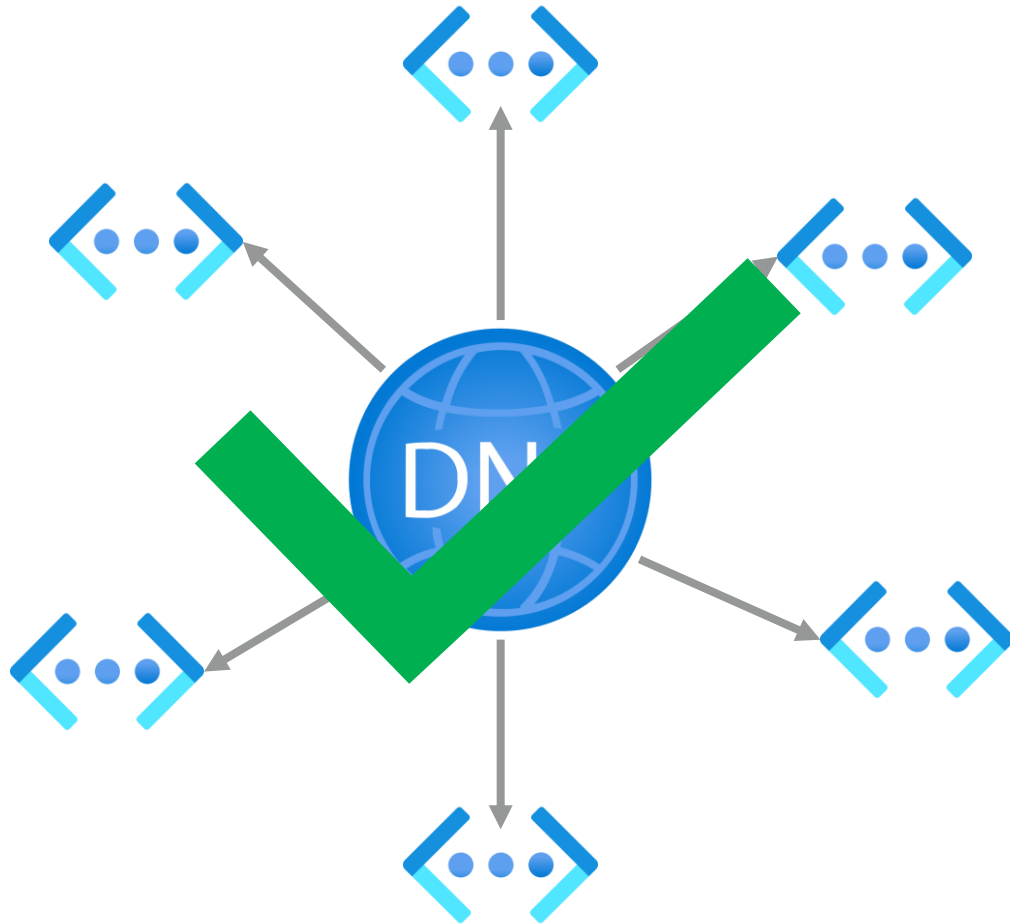


1. Non-centralised Private DNS Zones



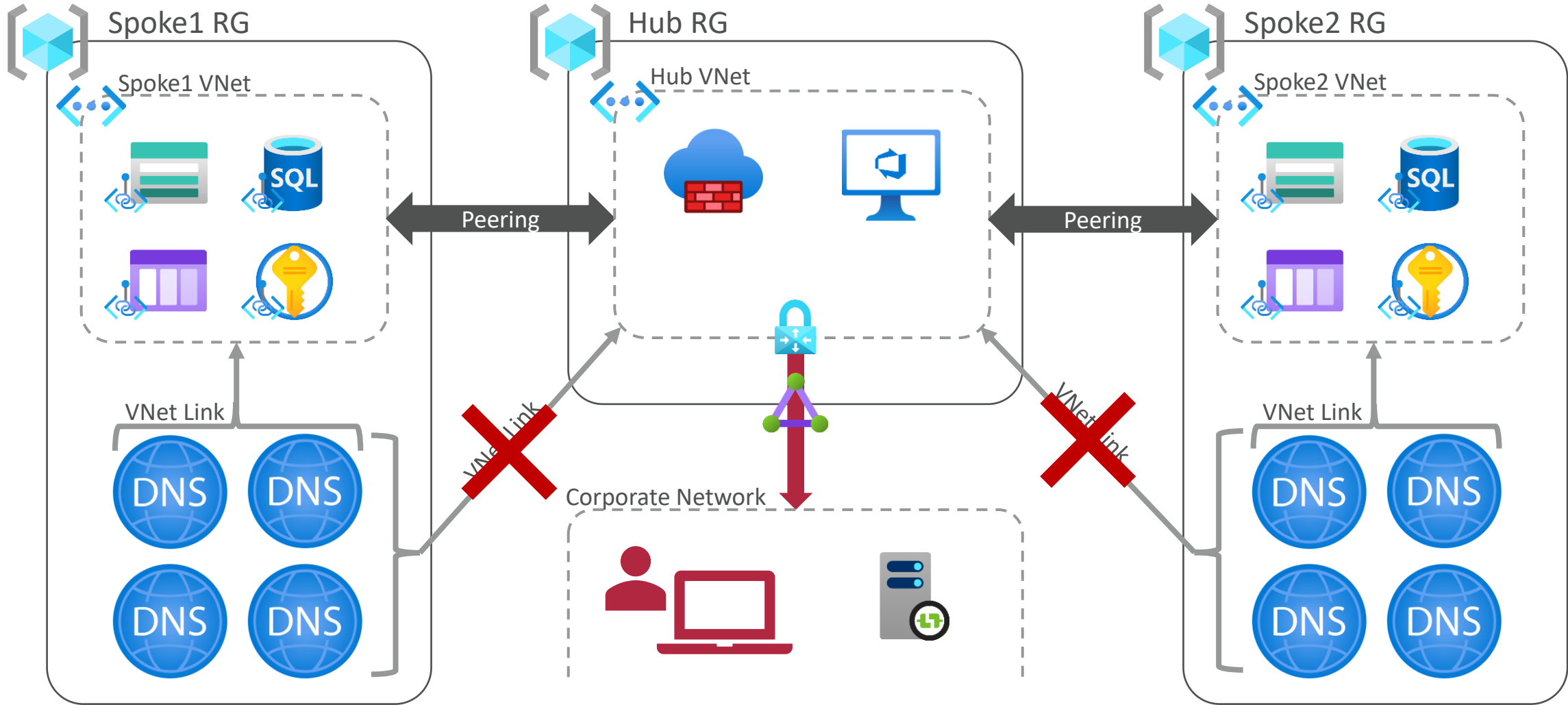


1. Non-centralised Private DNS Zones



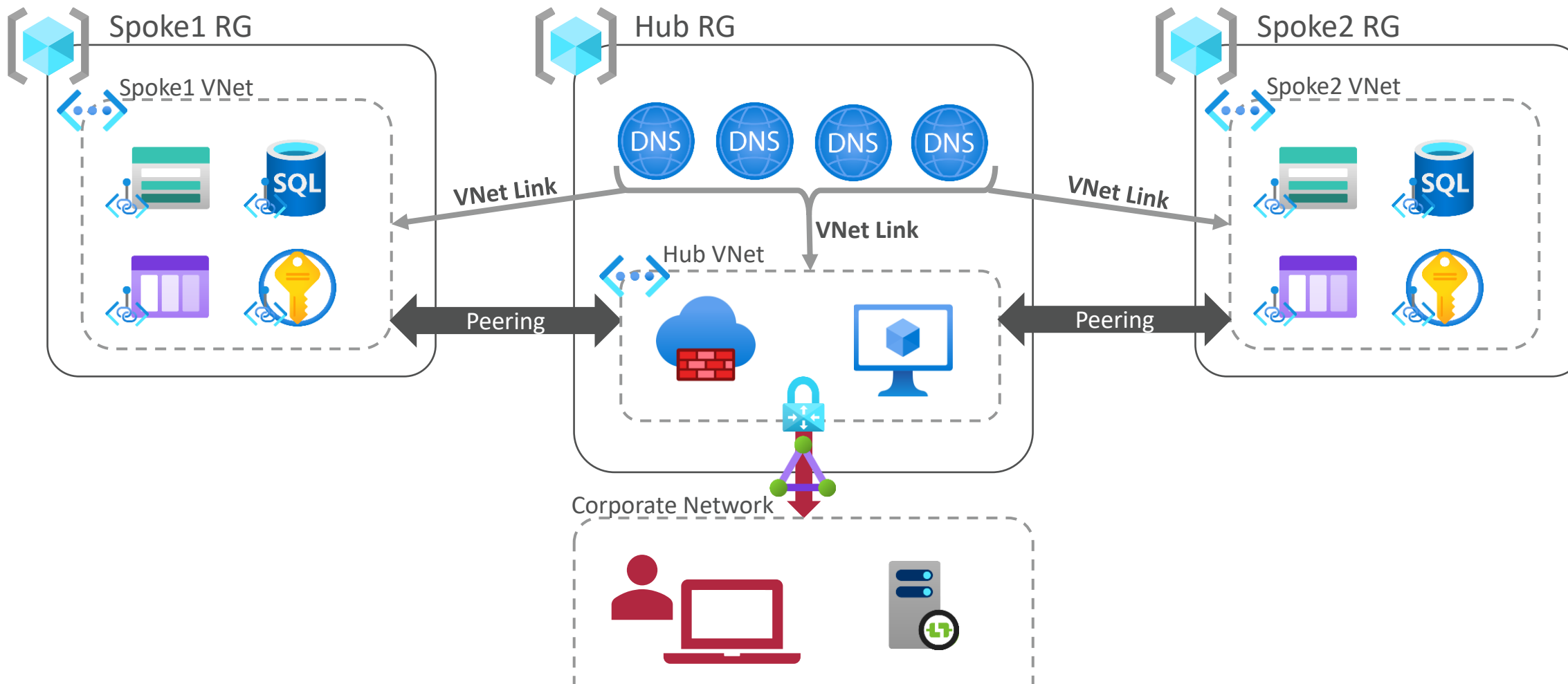


1. Non-centralised Private DNS Zones





1. Non-centralised Private DNS Zones





2. Using "Selected Networks" option

Home > sqlbits-2023-demo-rgp > sqlbits2023sauks01

sqlbits2023sauks01 | Networking

Storage account

Search

Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser

Data storage
Containers
File shares
Queues
Tables

Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud

Data management
Redundancy
Data protection
Object replication
Blob inventory
Static website
Lifecycle management
Azure search

Settings

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh

Public network access

☐ Enabled from all networks

☒ Enabled from selected virtual networks and IP addresses

☐ Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
sqlbits-2023-vnet-uks-01	1			sqlbits-2023-demo-rgp	Visual Studio Enterpri...
	sqlbits-2023-snet-uks...	10.0.0.32/27	✓ Enabled	sqlbits-2023-demo-rgp	Visual Studio Enterpri...

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

Address range

90.195.143.160

IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
Select a resource type	Select one or more instances

Exceptions

☒ Allow Azure services on the trusted services list to access this storage account.

☐ Allow read access to storage logging from any network

☐ Allow read access to storage metrics from any network

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference *

☒ Microsoft network routing ☐ Internet routing

Publish route-specific endpoints



☐ Microsoft network routing

☐ Internet routing



2. Using "Selected Networks" option

Public network access

- ☐ Enabled from all networks
- ☒ Enabled from selected virtual networks and IP addresses
- ☐ Disabled
-  Configure network security for your storage accounts. [Learn more](#) 



2. Using "Selected Networks" option

Home > sqlbits-2023-demo-rgp > sqlbits2023sauks01

sqlbits2023sauks01 | Networking

Storage account

Search

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser
- Data storage
 - Containers
 - File shares
 - Queues
 - Tables
- Security + networking
 - Networking**
 - Azure CDN
 - Access keys
 - Shared access signature
 - Encryption
 - Microsoft Defender for Cloud
- Data management
 - Redundancy
 - Data protection
 - Object replication
 - Blob inventory
 - Static website
 - Lifecycle management
 - Azure search
- Settings

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh

Public network access

- ☐ Enabled from all networks
- ☒ Enabled from selected virtual networks and IP addresses
- ☐ Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
sqlbits-2023-vnet-uks-01	1			sqlbits-2023-demo-rgp	Visual Studio Enterpri...
	sqlbits-2023-snet-uks...	10.0.0.32/27	✓ Enabled	sqlbits-2023-demo-rgp	Visual Studio Enterpri...

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

Address range

90.195.143.160

IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
Select a resource type	Select one or more instances

Exceptions

- ☒ Allow Azure services on the trusted services list to access this storage account.
- ☐ Allow read access to storage logging from any network
- ☐ Allow read access to storage metrics from any network

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference *

- ☒ Microsoft network routing
- ☐ Internet routing

Publish route-specific endpoints

- ☐ Microsoft network routing
- ☐ Internet routing



Resources

Blog post:

- [https://www.thinkingacloud.co.uk/p/7-steps-to-successfully-deploy-an-azure-private-endpoint /](https://www.thinkingacloud.co.uk/p/7-steps-to-successfully-deploy-an-azure-private-endpoint/)



Azure Private DNS Zone names:

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



Thank you!

Any Questions?



Blog



GitHub

in Grace O'Halloran (grace-o-halloran)

 @graceaohalloran

 grace@advancinganalytics.co.uk

 <https://www.thinkingacloud.co.uk>

 [https://github.com/gracedev94/
GraceOH-CommunityContent](https://github.com/gracedev94/GraceOH-CommunityContent)