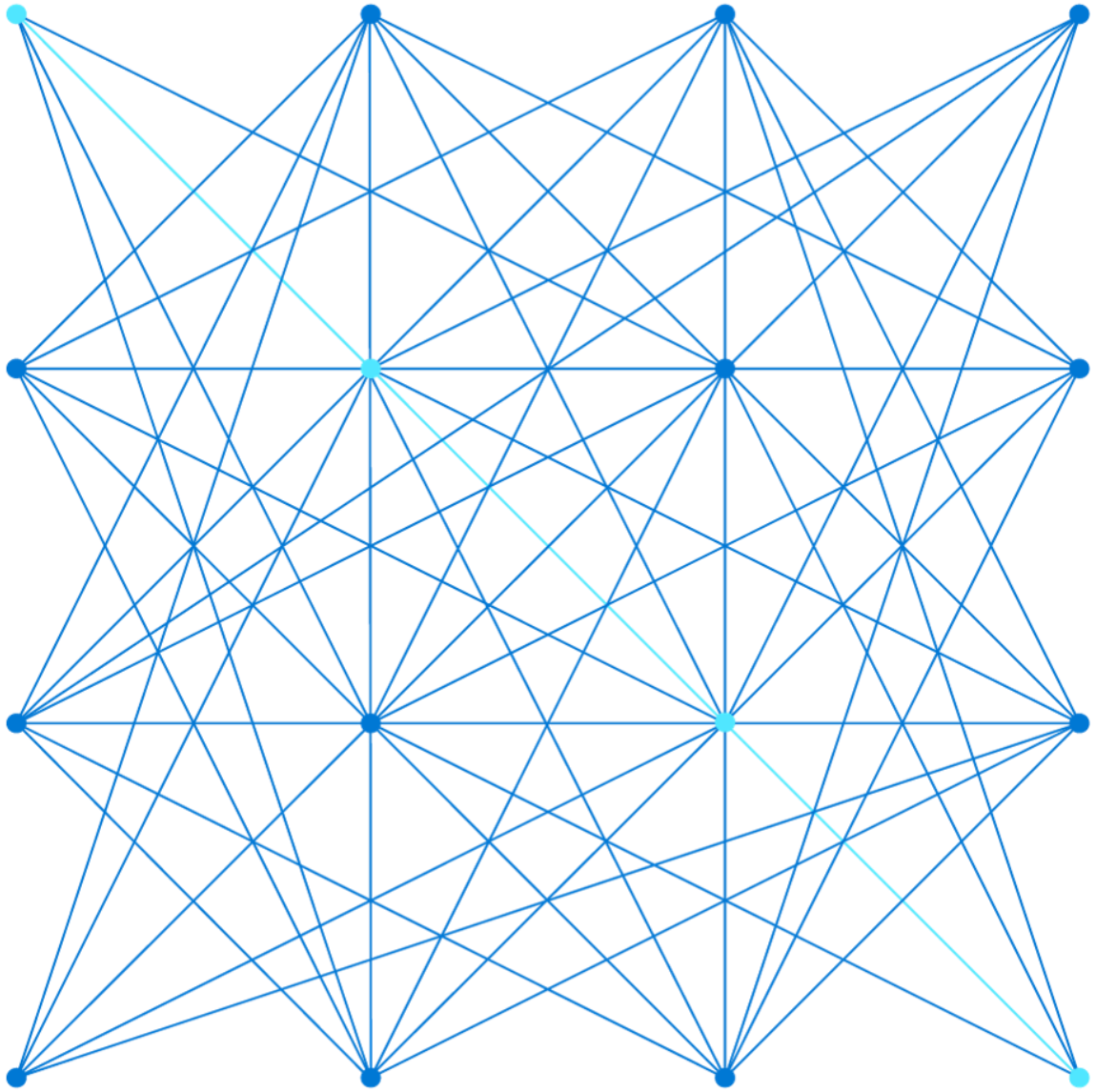
Microsoft Azure

AZ-700

Tag 3

Design and implement private access to Azure Services

Guten Morgen!



Course Agenda

Badges!

Labs!

Powershell!

Module 01: Introduction to Azure Virtual Networks

Module 02: Designing and Implementing Hybrid Networking

Module 03: Designing and Implementing Azure ExpressRoute

Module 04: Load balance non-HTTP(S) traffic in Azure

Module 05: Load balance HTTP(S) traffic in Azure

Module 06: Design and Implement Network Security FW WAF

Module 07: Design and Implement private access to Azure Services

Module 08: Design and Implement Network Monitoring

Test-NetConnection -Port 3389 | ping | Network Watcher

Design and implement private access to Azure Services

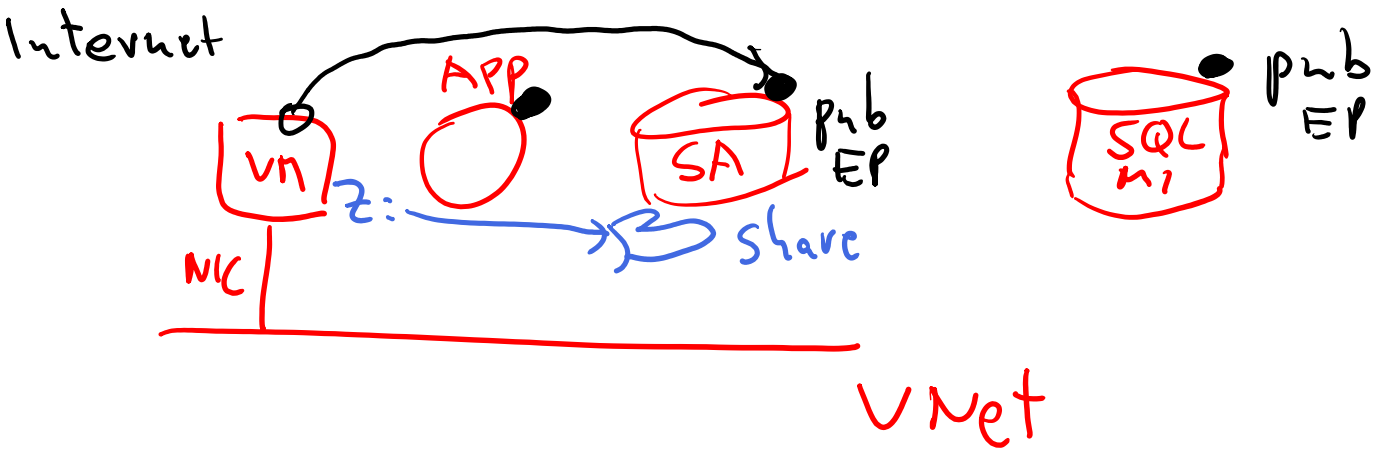
Explain Virtual Network Service Endpoints

Define Private Link Services and Private Endpoints

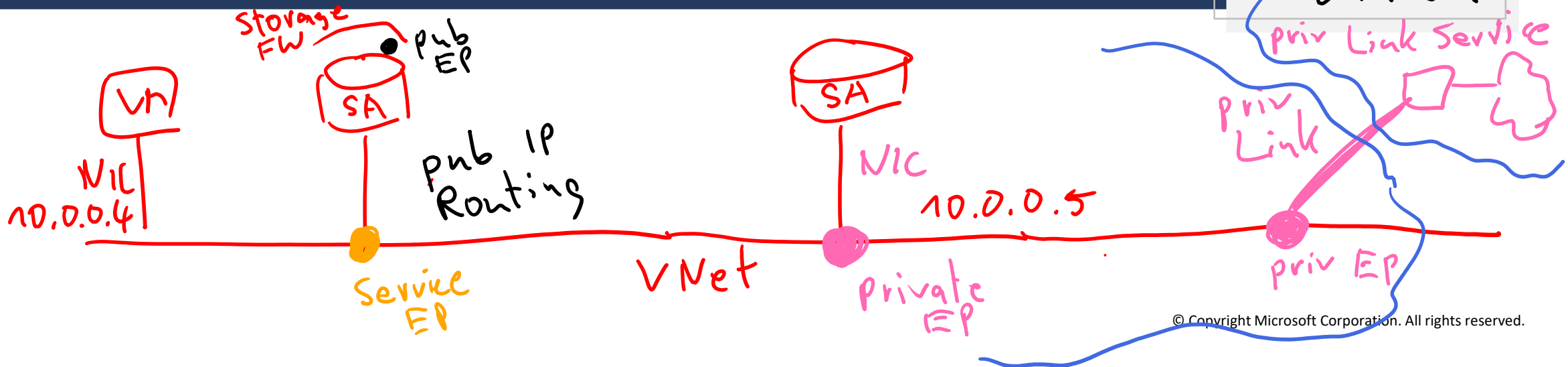
Integrate Private Endpoint with DNS

Exercise - Restrict network access to PaaS resources with virtual network service endpoints

Exercise - Create an Azure Private Endpoint using Azure PowerShell



Explain Virtual Network Service Endpoints



Explain Virtual Network Service Endpoints overview

What is a Service Endpoint?

Add Service Endpoints to a subnet

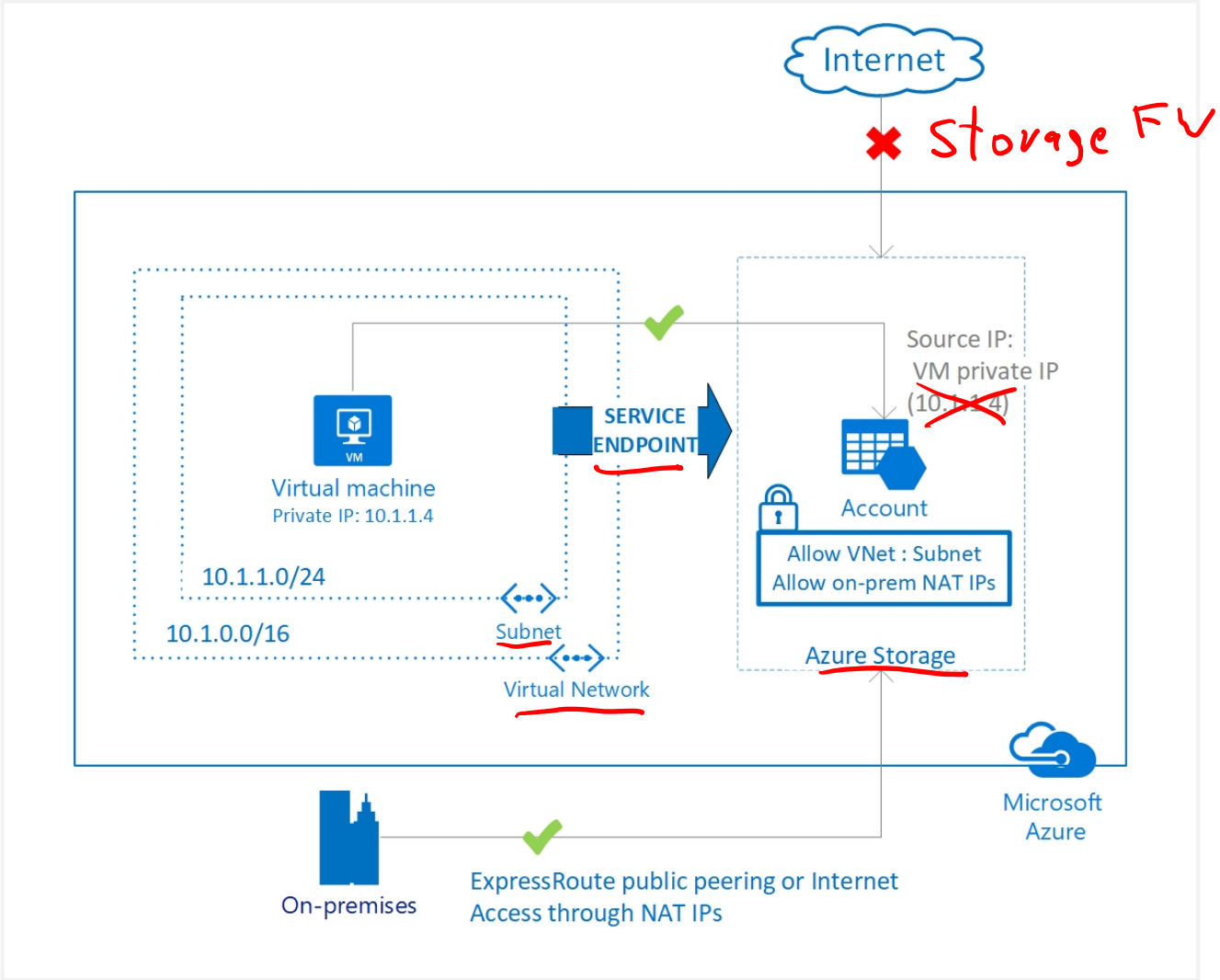
Demonstration

Review

What is Service Endpoint?

Secure and direct connectivity to Azure services over an optimized route over the Azure backbone network

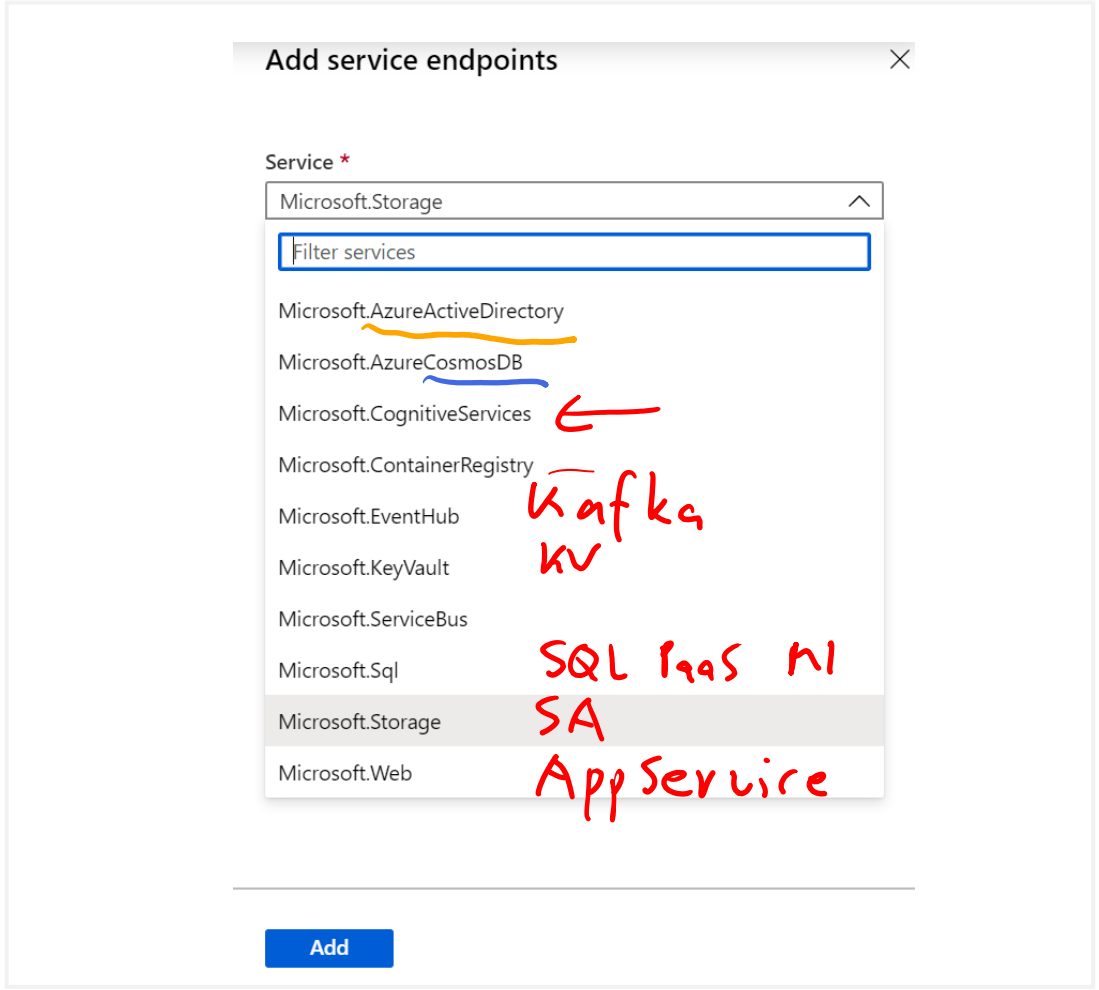
Optimal routing for Azure service traffic from your virtual network



Add Service Endpoints to a subnet

There are many services that support endpoints

Adding service endpoints can take up to 15 minutes to complete



Demonstration - Create a Service Endpoint service

1. Create a virtual network with one subnet
2. Add a subnet and enable a service endpoint
3. Create an Azure resource and allow network access to it from only a subnet
4. Deploy a virtual machine (VM) to each subnet
5. Confirm access to a resource from a subnet
6. Confirm access is denied to a resource from a subnet and the internet

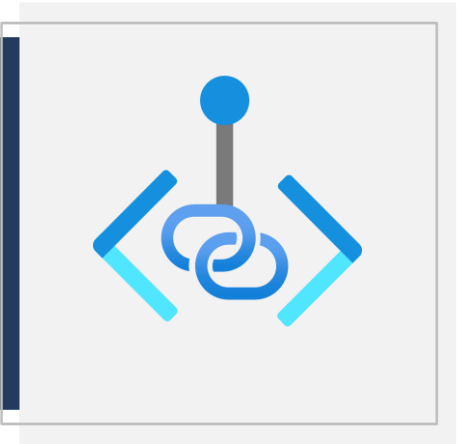
Summary – Explain virtual network Service endpoints

Check your knowledge

Microsoft Learn Modules (docs.microsoft.com/Learn)

Azure virtual network service endpoints | Microsoft Docs

Define Private Link Services and Private Endpoints



Define Private Link Services and Private Endpoints overview

What is Azure Private Link?

What is Azure Private endpoint?

What is Azure private Link service?

Private Link service workflow

Private endpoint properties

Demonstration

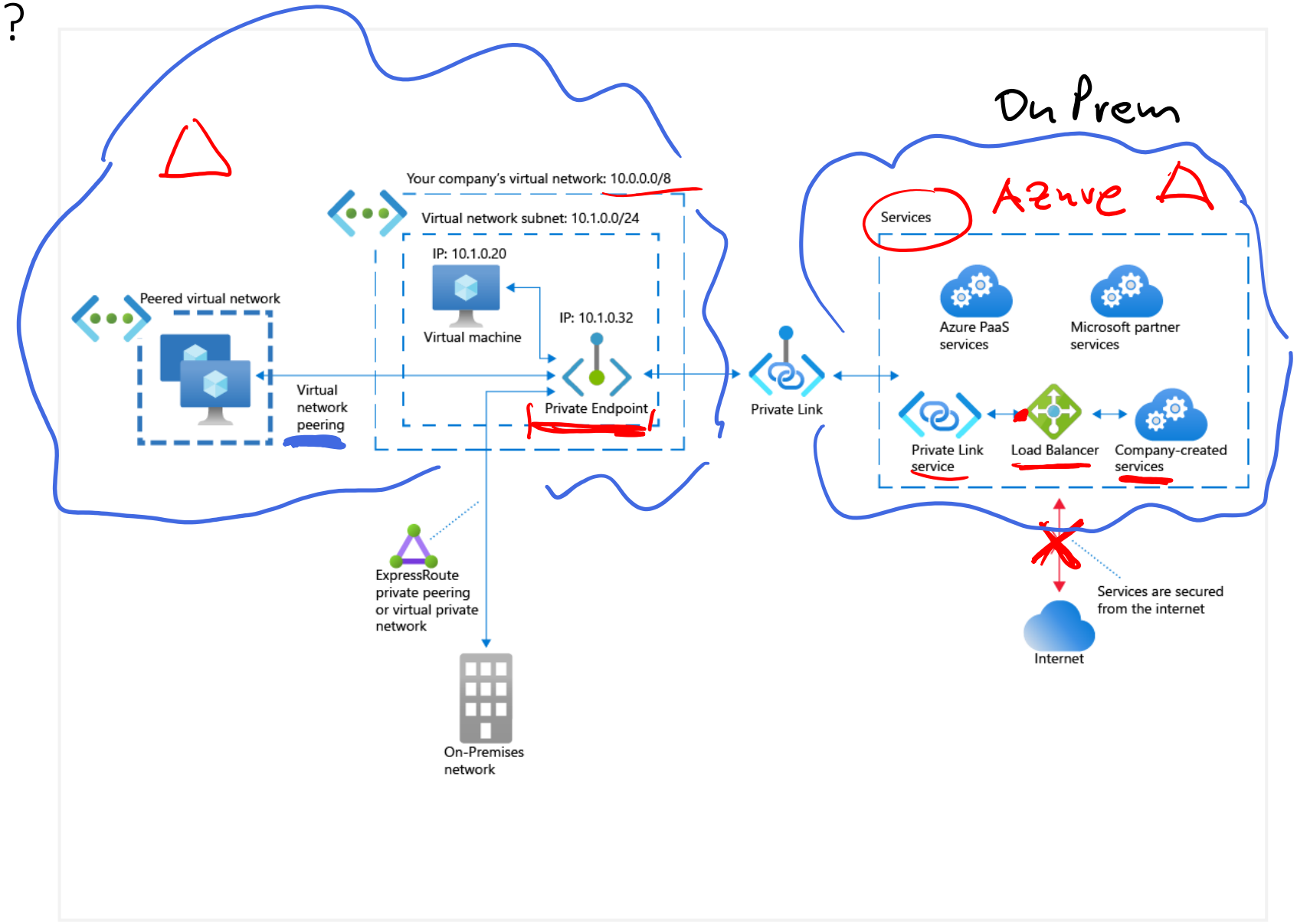
Review

What is Azure Private Link ?

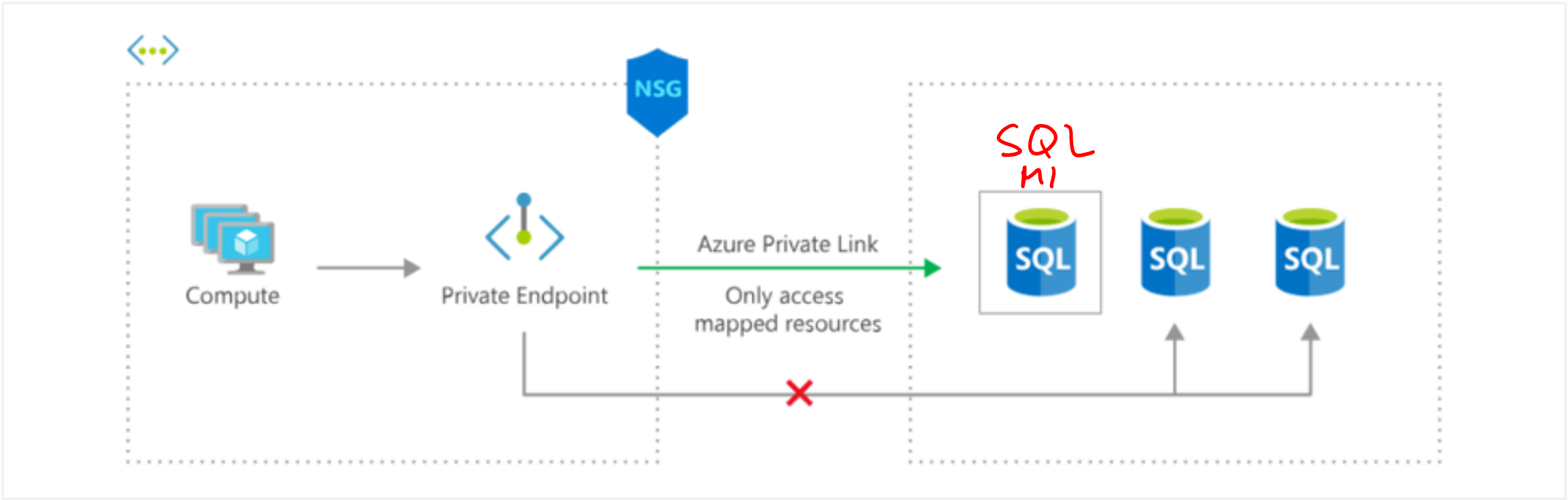
Integration with on-premises and peered networks

In the event of a security incident within your network, only the mapped resource would be accessible

Private connectivity to services on Azure. Traffic remains on the Microsoft network, with no public internet access



What is Azure Private Endpoint ?

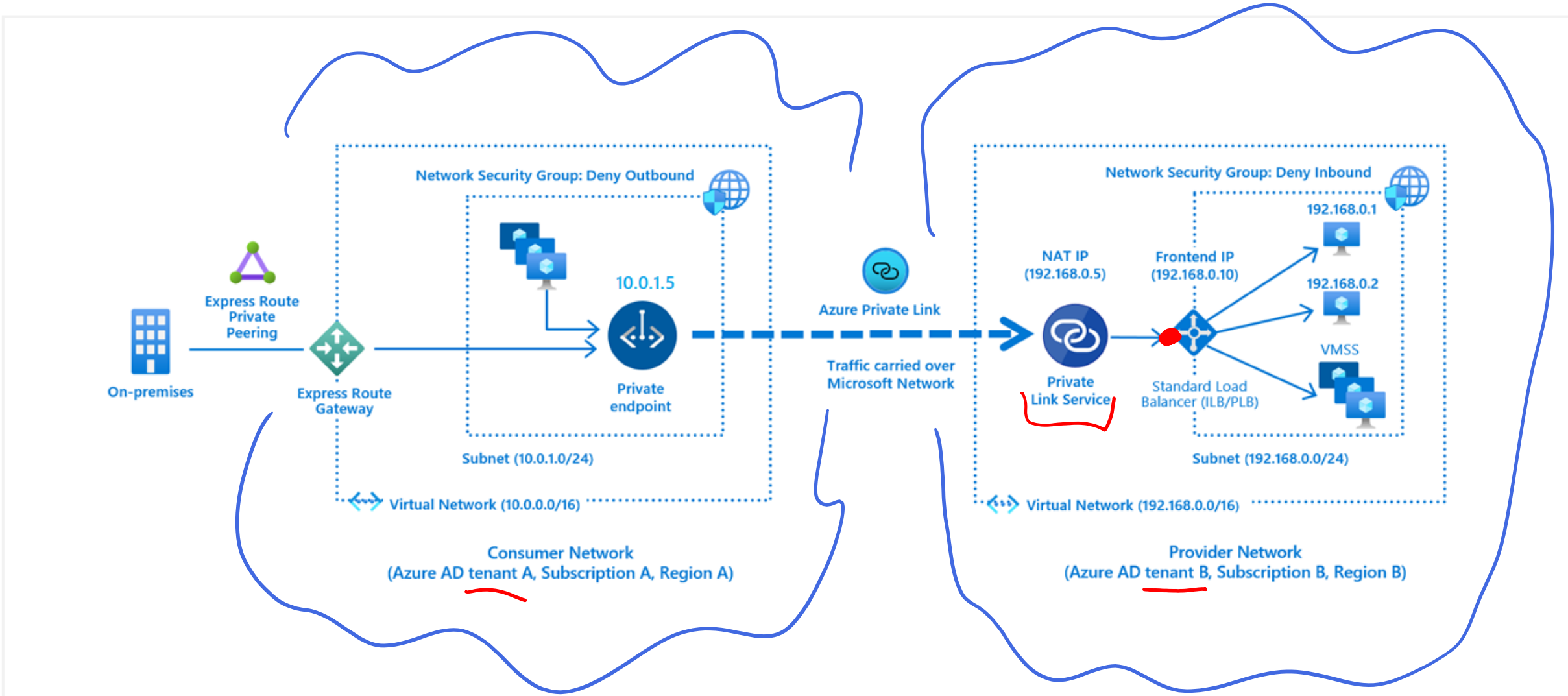


The Azure resource becomes, in a sense, a part of your virtual network.

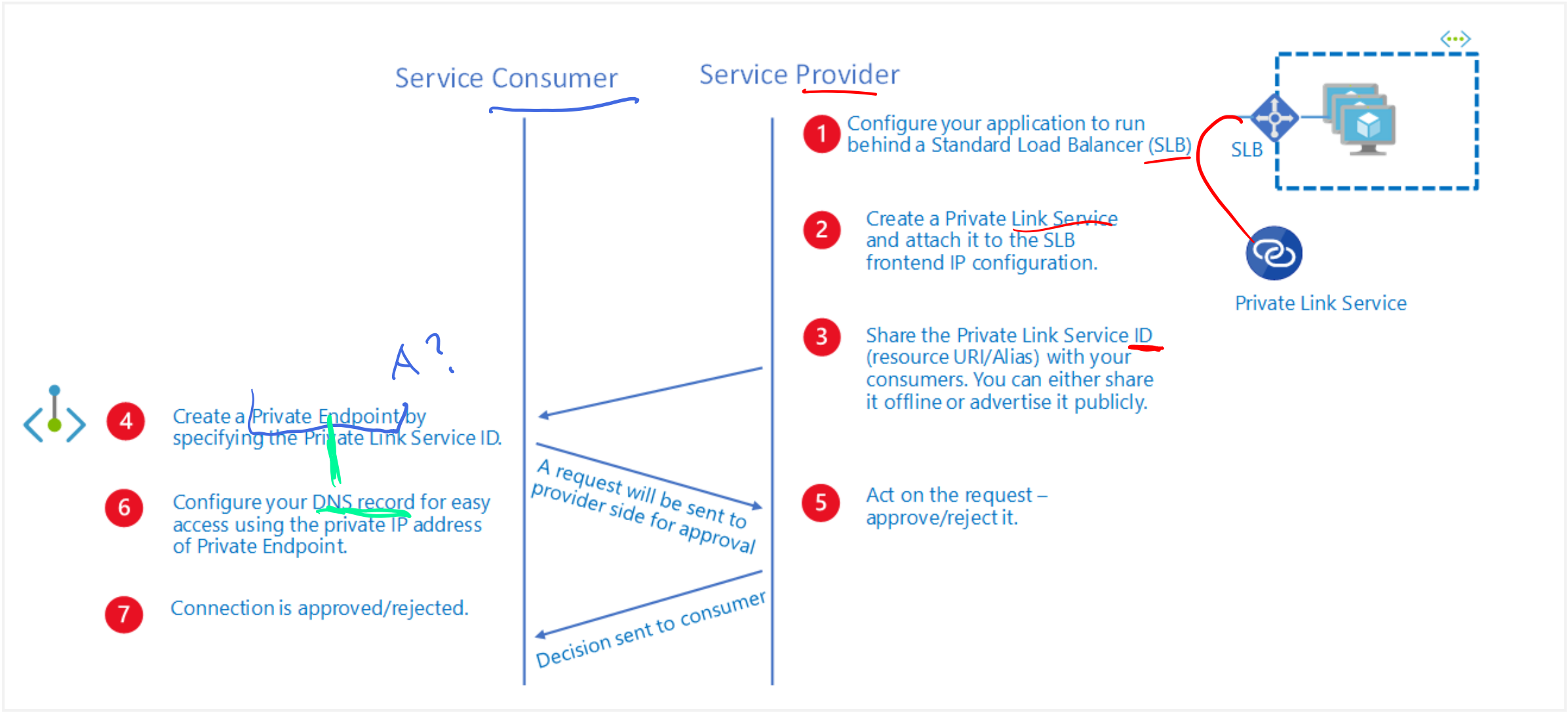
The connection to the resource now uses the Microsoft Azure backbone network instead of the public internet

Configure the Azure resource to no longer expose its public IP address, which eliminates that potential security risk.

What is Azure Private Link service?



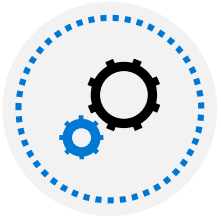
Private Link service workflow



Private Endpoint properties

Property	Description
Name	A unique name within the resource group.
Subnet	The subnet to deploy and allocate private IP addresses from a virtual network
Private Link Resource	The private link resource to connect using resource ID or alias, from the list of available types. A unique network identifier will be generated for all traffic sent to this resource.
Target subresource	The subresource to connect. Each private link resource type has different options to select based on preference.
Connection approval method	Automatic or manual. Based on Azure role-based access control (Azure RBAC) permissions, your private endpoint can be approved automatically. If you try to connect to a private link resource without Azure RBAC, use the manual method to allow the owner of the resource to approve the connection.
Request Message	You can specify a message for requested connections to be approved manually. This message can be used to identify a specific request.
Connection status	A read-only property that specifies if the private endpoint is active. Only private endpoints in an approved state can be used to send traffic. Additional states available: **Approved:** Connection was automatically or manually approved and is ready to be used. **Pending**: Connection was created manually and is pending approval by the private link resource owner. **Rejected**: Connection was rejected by the private link resource owner. **Disconnected:** Connection was removed by the private link resource owner. The private endpoint becomes informative and should be deleted for cleanup.

Demonstration – Create a Private Link service by using the Azure portal



Create a Private Link service that refers to your service

Give Private Link access to your service or resource deployed behind an Azure Standard Load Balancer

Users of your service have private access from their virtual network

Summary – Private Link and Private Endpoint

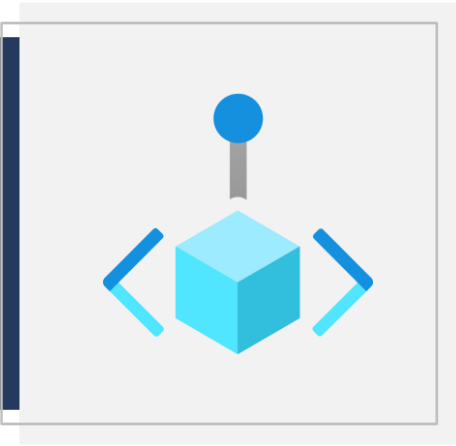
Check your knowledge

Microsoft Learn Modules (docs.microsoft.com/Learn)

What is Azure Private Link? | Microsoft Docs

What is an Azure Private Endpoint? | Microsoft Docs

Integrate Private Endpoint with DNS



Integrate Private endpoint with DNS overview

Azure Private Endpoint DNS configuration

Significance of IP address 168.63.129.16

Azure services Private DNS zone configuration examples

Virtual network workloads without custom DNS server

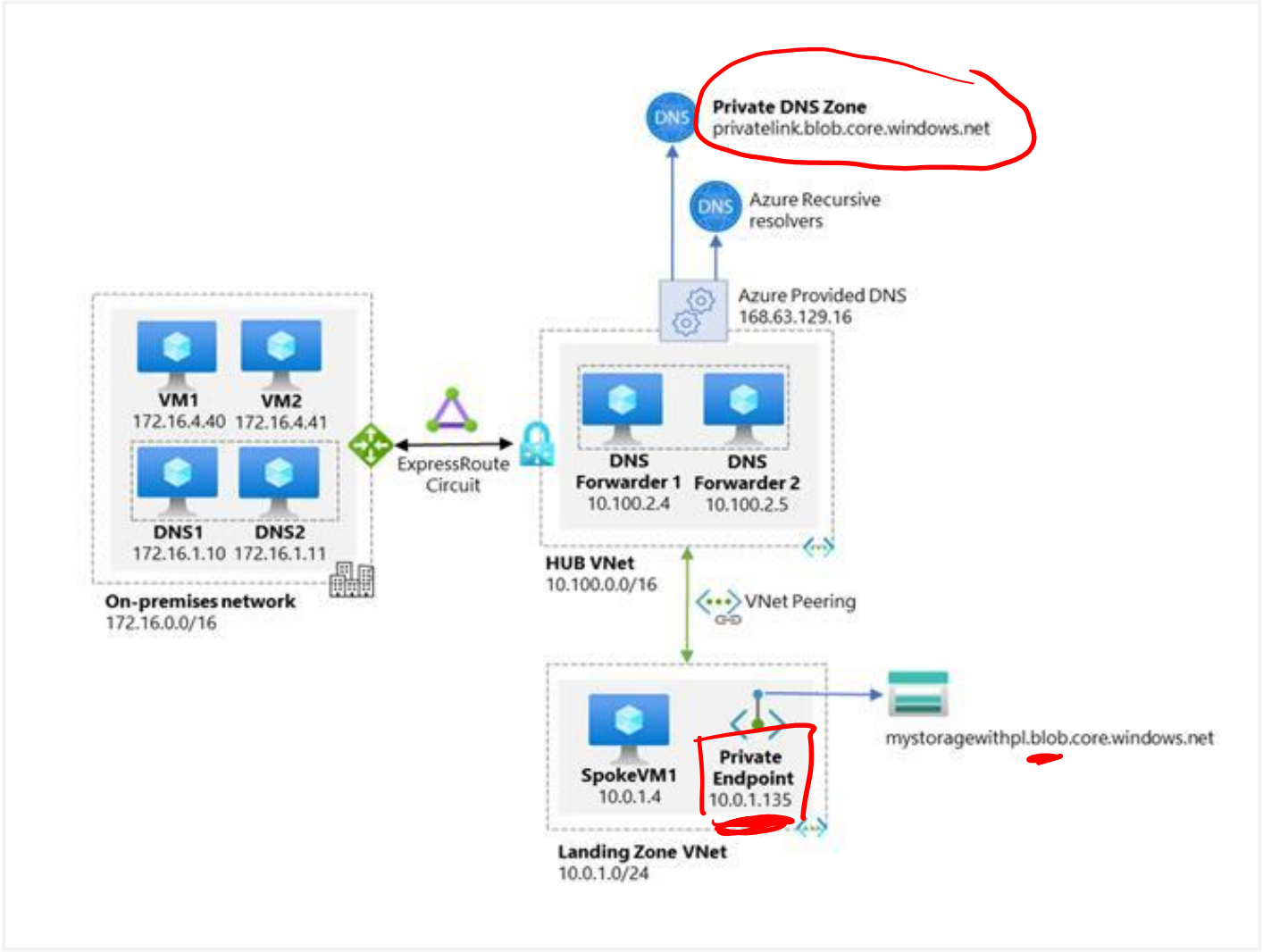
On-premises workloads using a DNS forwarder

Virtual network and on-premises workloads using a DNS forwarder

Review

Azure Private Endpoint DNS configuration

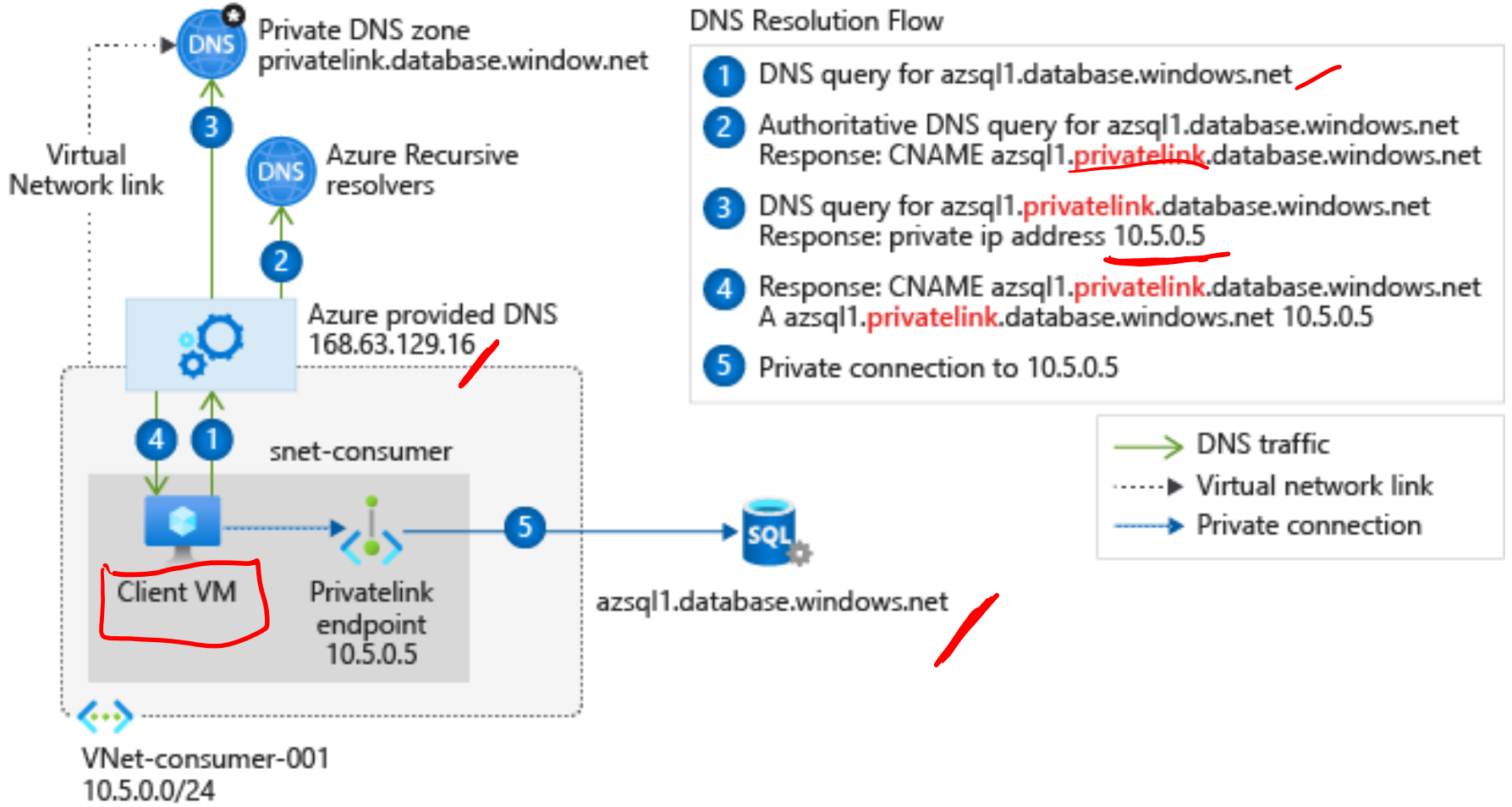
High-level architecture for enterprise environments with central DNS resolution and where name resolution for Private Endpoint resources is done via Azure Private DNS



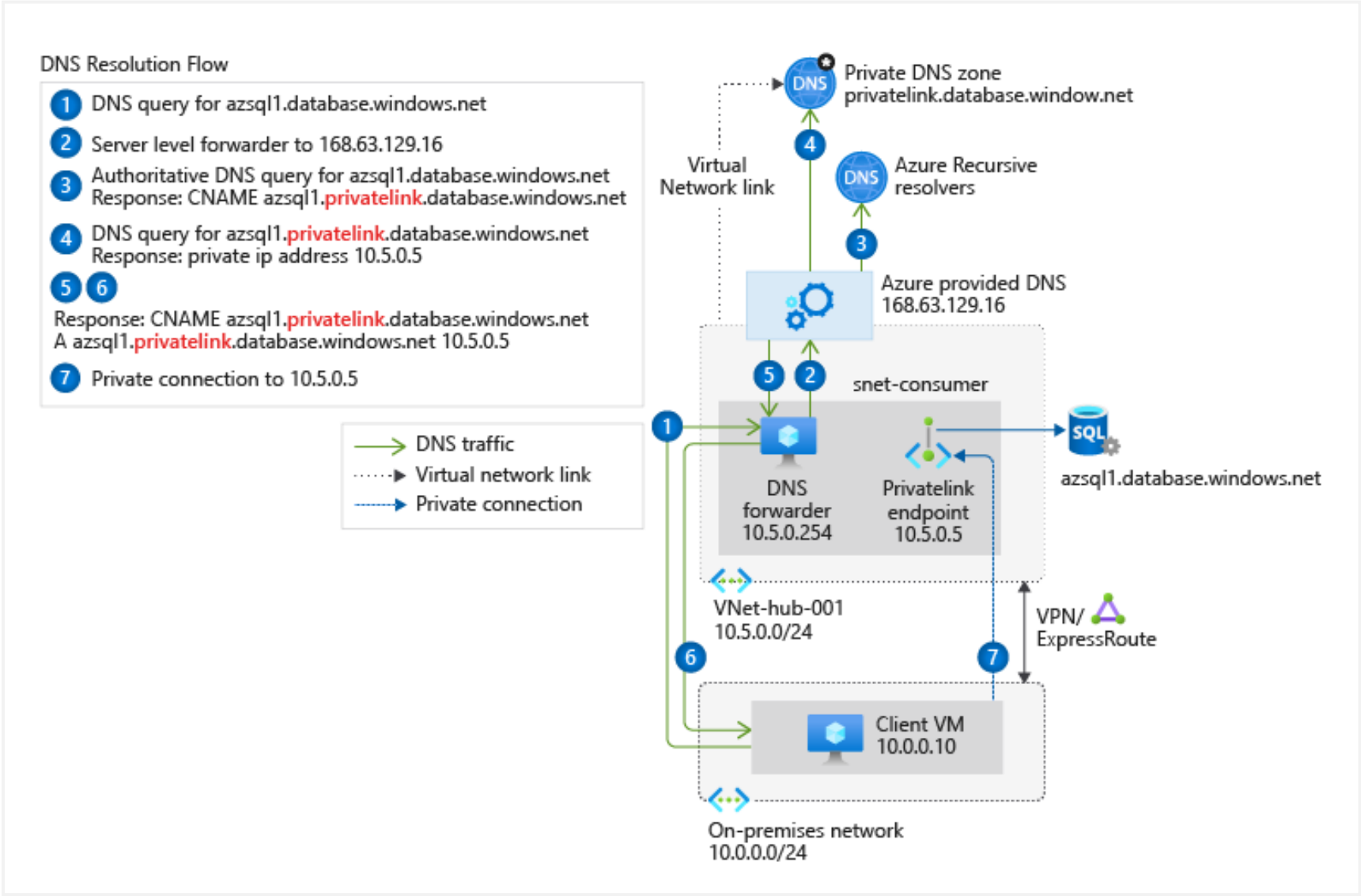
Azure services Private DNS zone configuration examples

Private Link resource type / Subresource	Private DNS zone name
Azure Automation / (Microsoft.Automation/automationAccounts) / Webhook, DSCAndHybridWorker	privatelink.Azure-automation.net
Azure SQL Database (Microsoft.Sql/servers) / sqlServer	privatelink.database.windows.net
Azure Synapse Analytics (Microsoft.Sql/servers) / sqlServer	privatelink.database.windows.net
Azure Synapse Analytics (Microsoft.Synapse/workspaces) / Sql	privatelink.sql.Azuresynapse.net
Storage account (Microsoft.Storage/storageAccounts) / Blob (blob, blob_secondary)	privatelink.[Service].core.windows.net

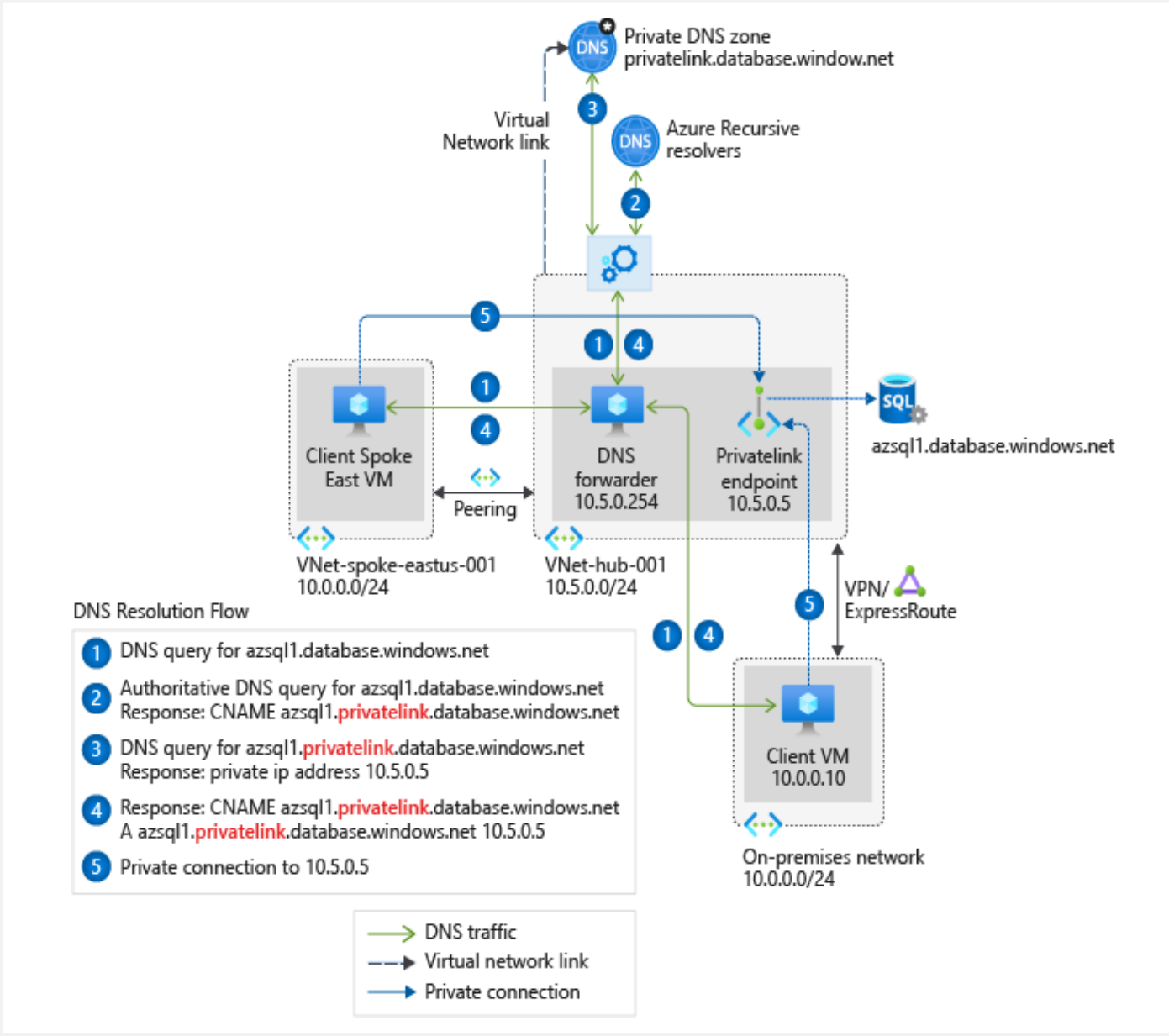
Virtual network workloads without custom DNS server



On-premises workloads using a DNS forwarder



Virtual network and on-premises workloads using a DNS forwarder



Summary – Integrate Private Endpoint with DNS

Check your knowledge

Microsoft Learn Modules (docs.microsoft.com/Learn)

Azure Private Endpoint DNS configuration | Microsoft Docs

Exercise - Restrict network access to PaaS resources with virtual network service endpoints

Restrict network access to PaaS resources with virtual network service endpoints

Task 1: Create a virtual network

Task 2: Enable a service endpoint

Task 3: Restrict network access for a subnet

Task 4: Add additional outbound rules

Task 5: Allow access for RDP connections

Task 6: Restrict network access to a resource

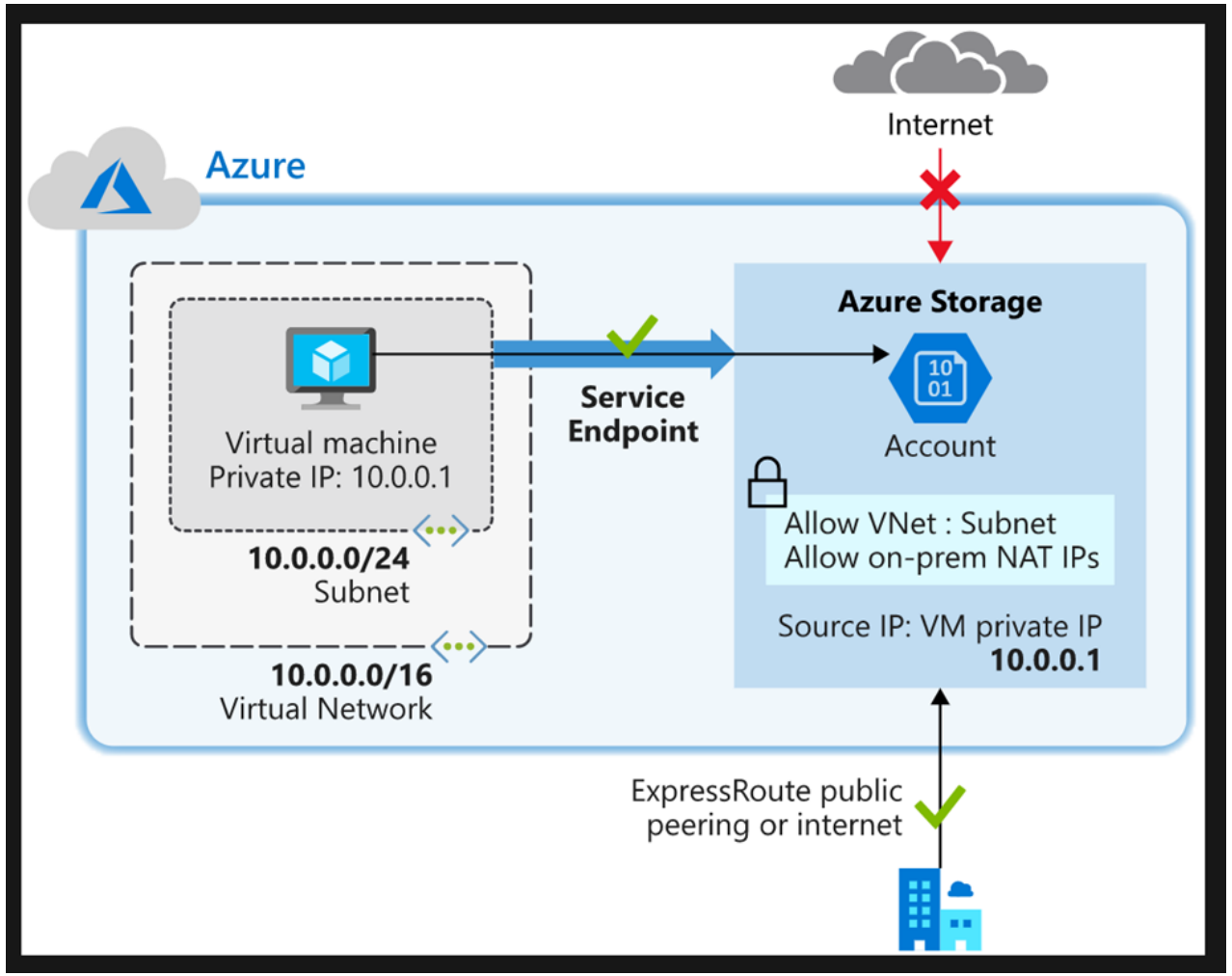
Task 7: Create a file share in the storage account

Task 8: Restrict network access to a subnet

Task 9: Create virtual machines

Task 10: Confirm access to storage account

Task 11: Clean up resources



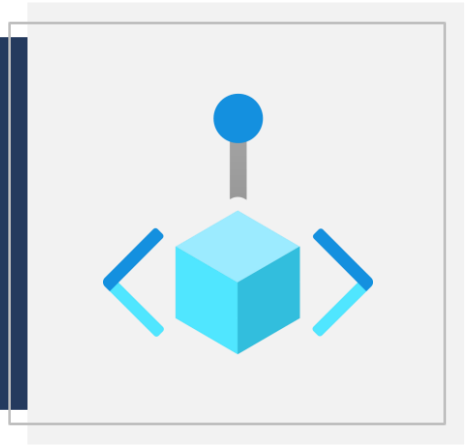
Summary – Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal

Check your knowledge

Microsoft Learn Modules (docs.microsoft.com/Learn)

Azure virtual network service endpoints | Microsoft Docs

Exercise - Create an Azure Private Endpoint using Azure PowerShell



Create an Azure Private Endpoint using Azure PowerShell

Task 1: Create a resource group

Task 2: Create a virtual network and bastion host

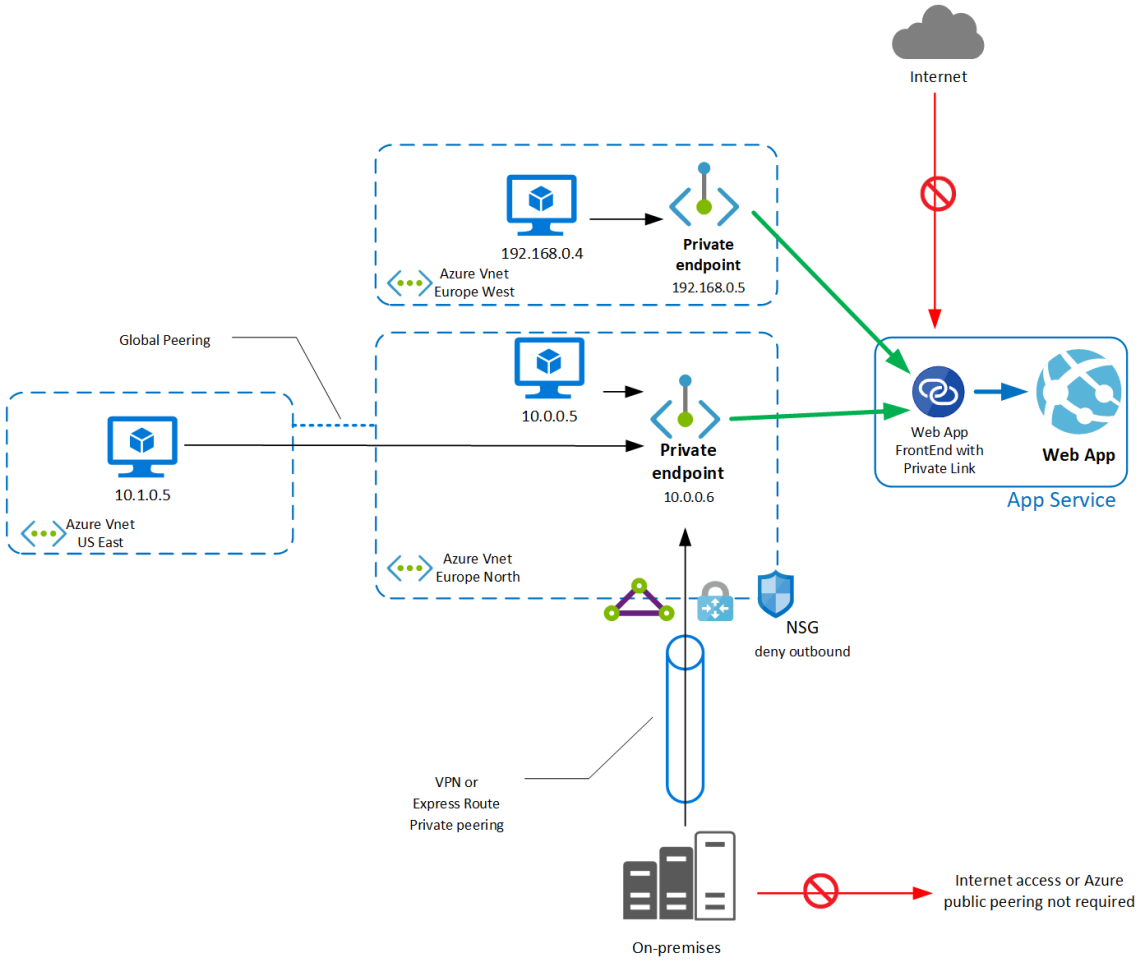
Task 3: Create a test virtual machine

Task 4: Create a Private Endpoint

Task 5: Configure the private DNS zone

Task 6: Test connectivity to the Private Endpoint

Task 7: Clean up resources



Summary – Exercise - Create an Azure Private Endpoint using Azure PowerShell

Check your knowledge	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Quickstart - Create a Private Endpoint using the Azure portal | Microsoft Docs

End of presentation