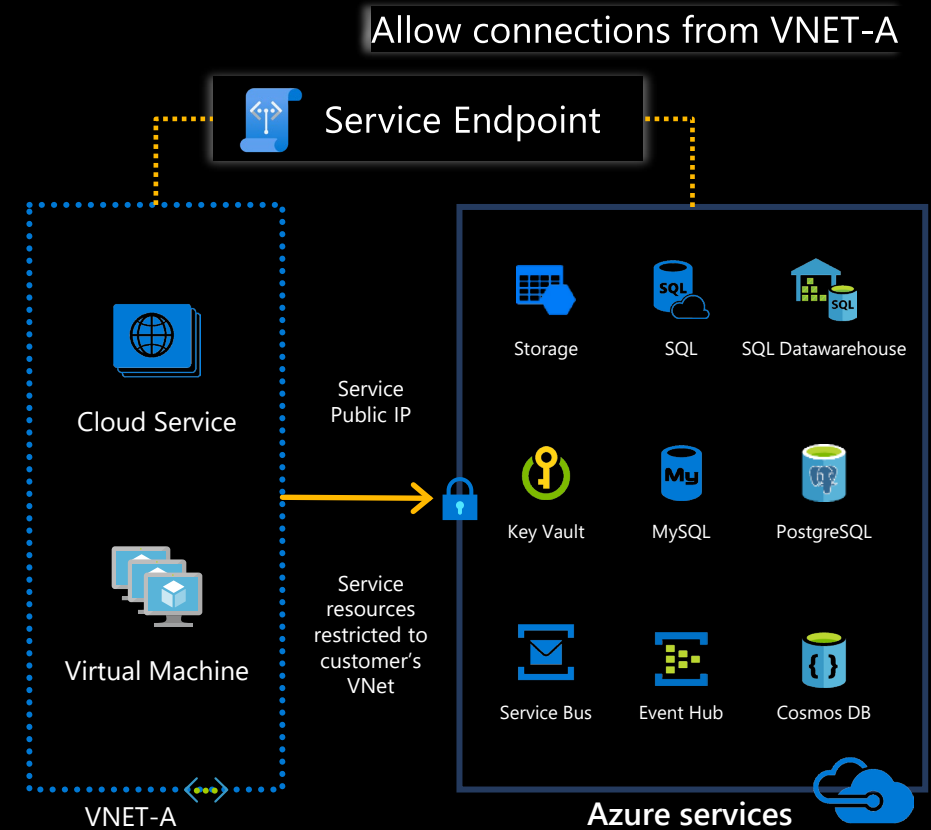


# VNET Service Endpoint



# VNET Service Endpoint

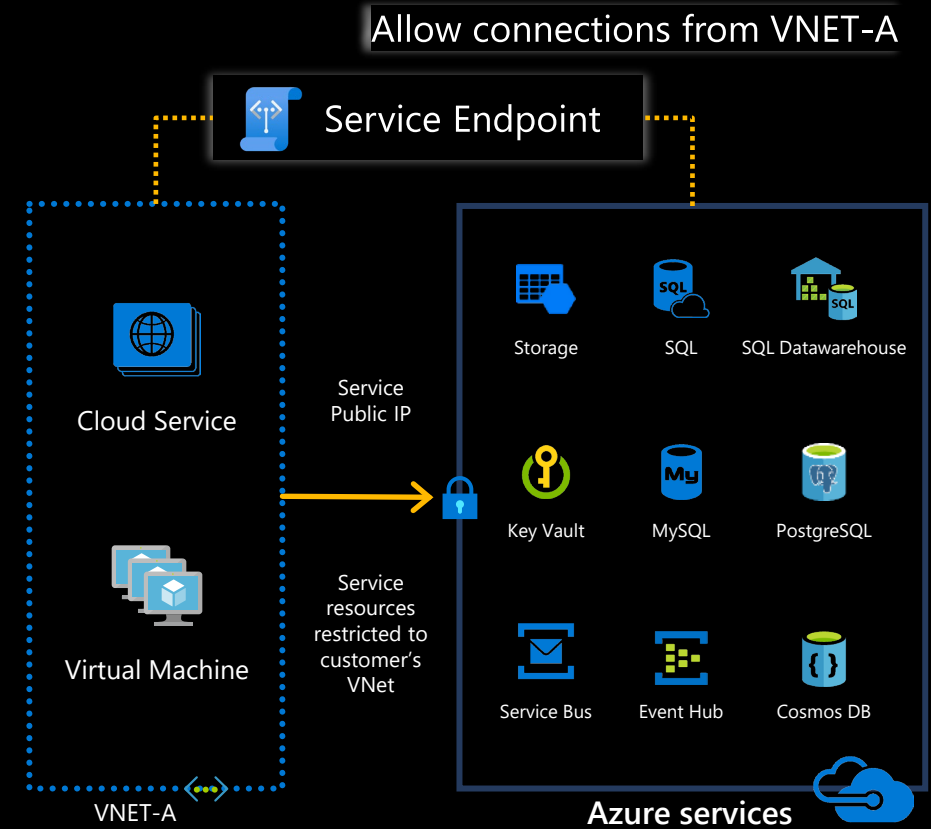
Provides **private network access** to Azure resources.

The compute resources connect to the **public IP** addresses of the Azure services.

Connects over an optimized route using **Azure backbone network**.

The compute resources on the private virtual network use their **private IP address as the source address** when connecting to the Azure service.

Works only for **outbound traffic**. No inbound.



# How does VNET Service Endpoint works

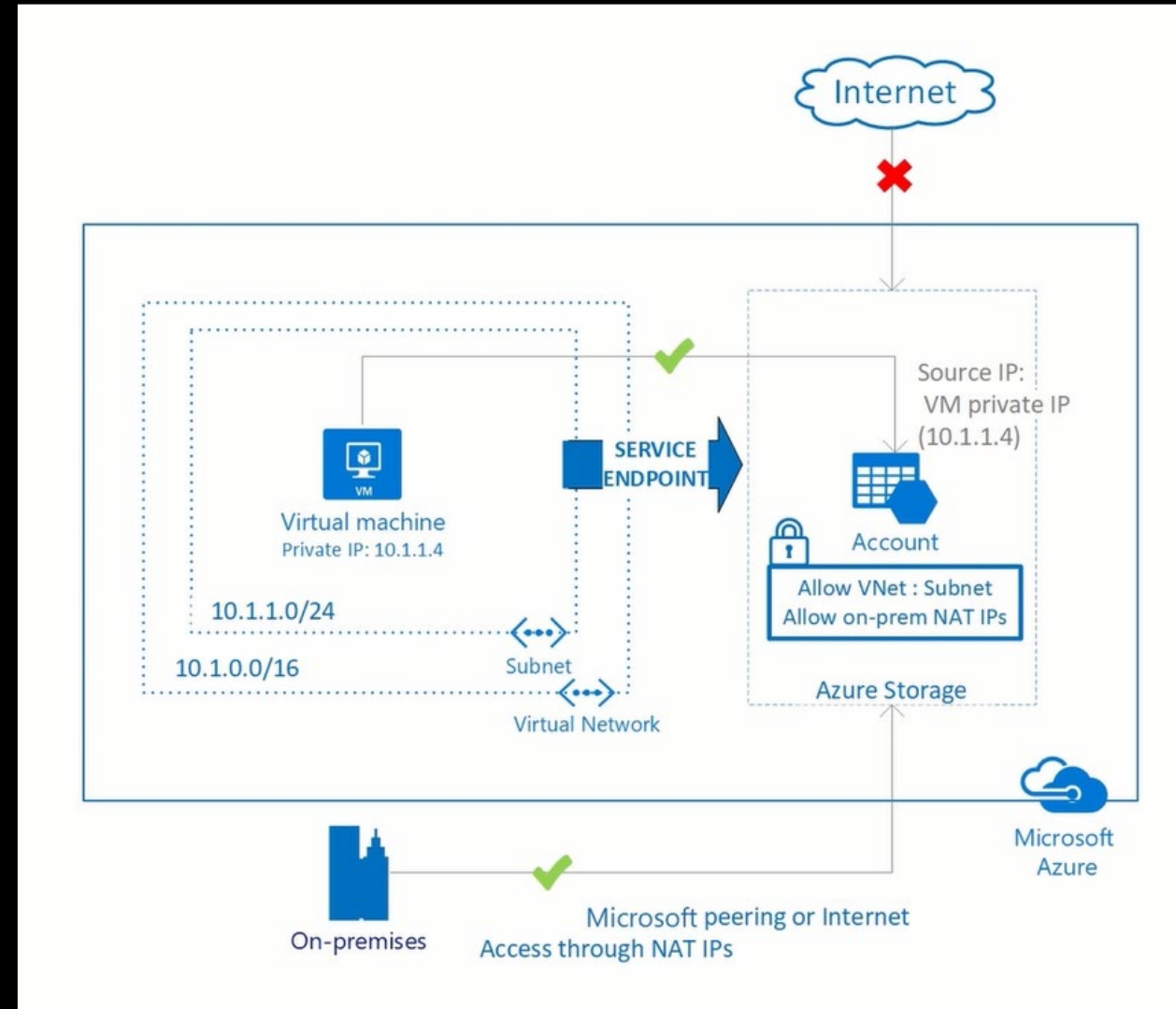
You want to **limit access to your Azure services** (like Storage Account, to only connections coming from your own Subnet.

You **configure your Subnet to use Service Endpoint** and specify the type of Azure service, like Storage Account.

You configure your Storage Account to **accept connections coming only from your Subnet**.

Azure can **identify the source of the connection** (tenant ID, subscription, resource group, VNET name, Subnet name).

Azure can then **allow or deny** the connections.



# Service Endpoint services

Azure storage, Azure App Service, Azure SQL database

Azure Synapse Analytics

Azure Database for PostgreSQL server

Azure database for MySQL server

Azure Database for MariaDB

Azure CosmosDB, Azure Key Vault, Azure Service Bus

Azure Event Hubs, Azure Data Lake store Gen 1

Azure Cognitive Services

Azure Container Registry (Public Preview)

[learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview)

subnet-dev

vnet-app

Name

subnet-dev

- ☐ Select all
- ☐ Microsoft.AzureActiveDirectory
- ☐ Microsoft.AzureCosmosDB
- ☐ Microsoft.CognitiveServices
- ☐ Microsoft.ContainerRegistry
- ☐ Microsoft.EventHub
- ☐ Microsoft.KeyVault
- ☐ Microsoft.ServiceBus
- ☐ Microsoft.Sql
- ☐ Microsoft.Storage
- ☐ Microsoft.Storage.Global
- ☐ Microsoft.Web

Filter services

0 selected

# Enable Service Endpoint – step 1/2

Configure Service Endpoint on the Subnet for a specific service type.

Can set multiple service types.

The screenshot shows the Azure portal interface for configuring a service endpoint on a subnet. The left sidebar contains navigation links for various network-related settings. The main pane displays the 'vnet-app | Subnets' view, where a table lists the subnets. The 'subnet-dev' subnet is selected, and a detailed configuration pane is open on the right. In this pane, a list of services is shown with checkboxes to enable or disable service endpoints. 'Microsoft.Sql' and 'Microsoft.Web' are checked. A summary bar indicates '2 selected'. Below this, a table shows the status of the selected services as 'New'. 'Save' and 'Cancel' buttons are at the bottom.

Home > rg-service-endpoint-430 > vnet-app

**vnet-app | Subnets** Virtual network

Search

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

**Settings**

Address space  
Connected devices  
**Subnets**  
Bastion  
DDoS protection  
Firewall  
Microsoft Defender for Cloud  
Network manager  
DNS servers  
Peerings  
Service endpoints  
Private endpoints  
Properties

+ Subnet + Gateway subnet

Search subnets

Name ↑↓	IPv4 ↑↓
subnet-app	10.0.0.0/24
AzureBastionSubnet	10.0.1.0/24
subnet-dev	10.0.2.0/24

**subnet-dev**

name  
subnet-dev

☐ Select all

- ☐ Microsoft.AzureActiveDirectory
- ☐ Microsoft.AzureCosmosDB
- ☐ Microsoft.CognitiveServices
- ☐ Microsoft.ContainerRegistry
- ☐ Microsoft.EventHub
- ☐ Microsoft.KeyVault
- ☐ Microsoft.ServiceBus
- ☒ Microsoft.Sql
- ☐ Microsoft.Storage
- ☐ Microsoft.Storage.Global
- ☒ Microsoft.Web

Filter services

2 selected

Service	Status
Microsoft.Web	New
Microsoft.Sql	New

Save Cancel

Give feedback

# Enable Service Endpoint – step 2/2

You configure your Storage Account to accept connections coming only from your Subnet.

The screenshot displays the Azure portal interface for a storage account named 'storacc13579'. The left-hand navigation pane includes sections for 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', 'Storage browser', 'Storage Mover', 'Data storage' (with sub-items like Containers, File shares, Queues, and Tables), and 'Security + networking' (with sub-items like Networking, Front Door and CDN, Access keys, and Shared access signature). The 'Networking' option is currently selected.

The main content area is titled 'storacc13579 | Networking' and features a search bar and a set of tabs: 'Firewalls and virtual networks' (active), 'Private endpoint', and 'Public endpoint'. Under the 'Firewalls and virtual networks' tab, there are controls for 'Public network access' (set to 'Enabled from selected virtual networks and IP addresses') and a link to 'Configure network security for your storage account'. Below this is a 'Virtual networks' section with a table listing the configured virtual networks.

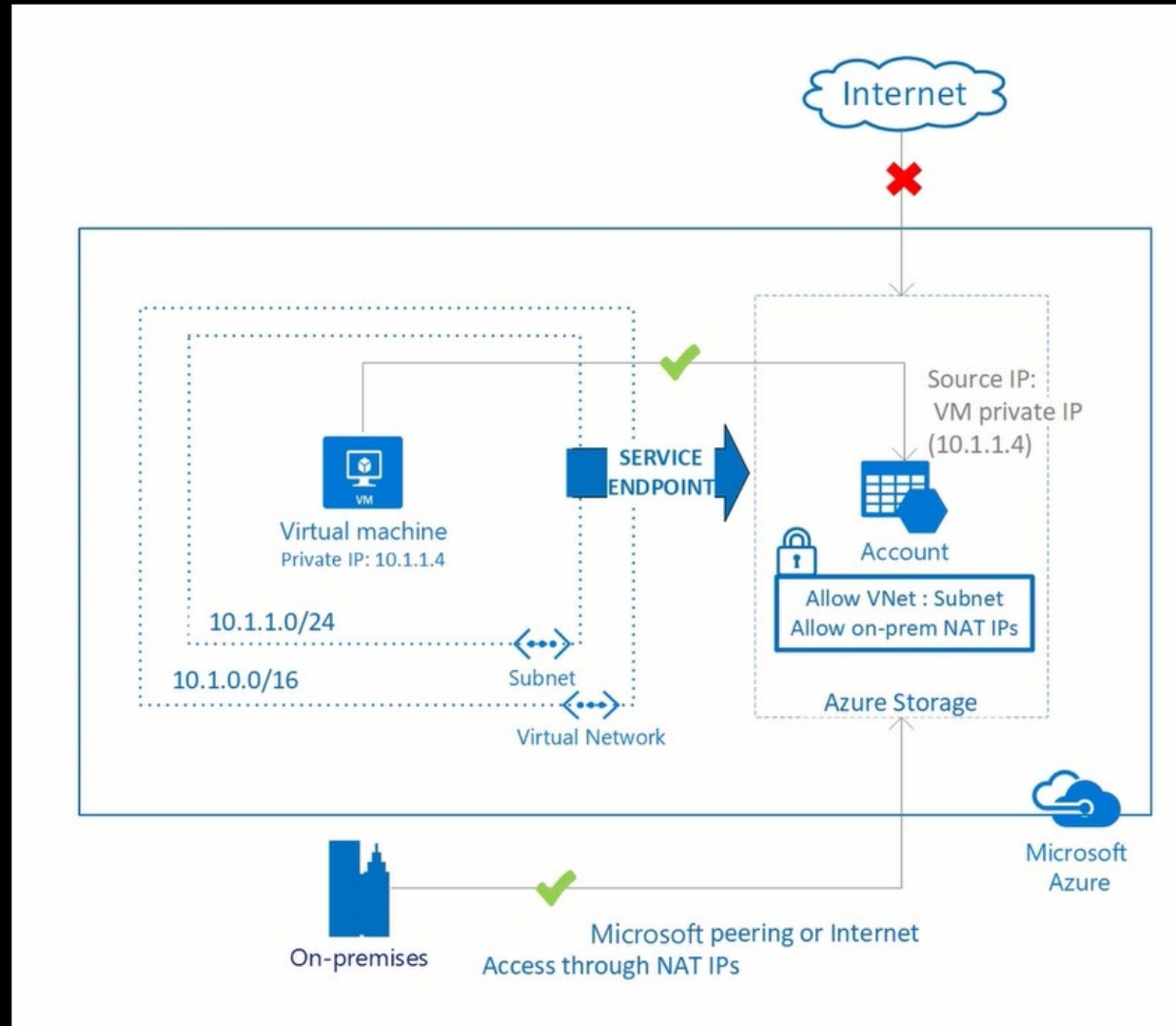
Virtual Network	Subnet	Address range
vnet-app	1	
	subnet-app	10.0.0.0/24

To the right of the main content area is a 'Add networks' panel. It contains dropdown menus for 'Subscription' (Microsoft-Azure-T), 'Virtual networks' (vnet-app), and 'Subnets' (subnet-dev (Service endpoint required)). Below these is a table showing the 'Service endpoint status' for the selected virtual network and subnet.

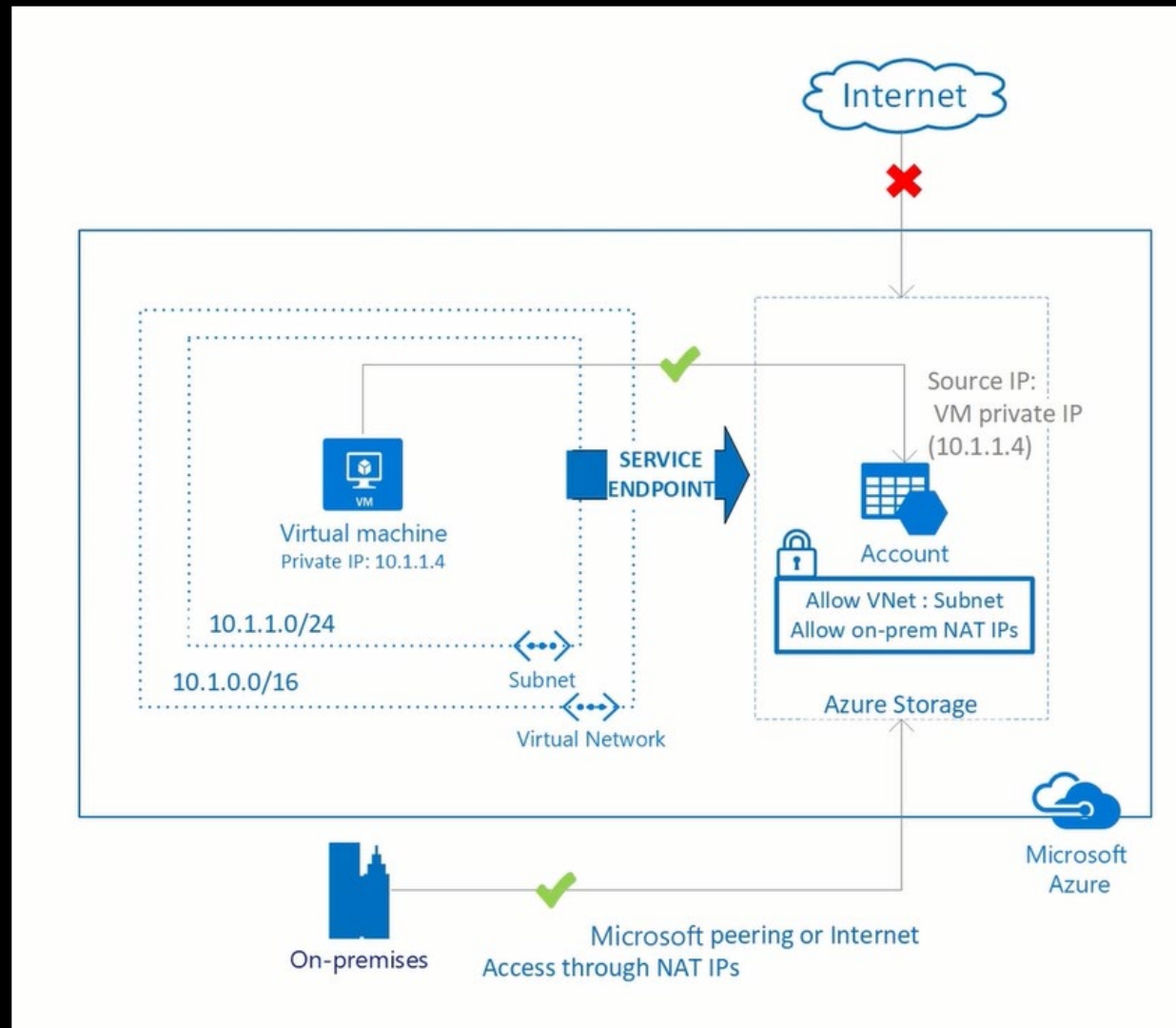
Virtual network	Service endpoint status
vnet-app	
subnet-dev	Not enabled

At the bottom of the 'Add networks' panel is an 'Enable' button. Below the 'Virtual networks' table, there is a 'Firewall' section with a text input for 'Address range' (containing '176.177.25.47') and a 'Resource instances' section with a text input for 'Resource type'.

# Service Endpoint for Storage Account



# Service Endpoint for App Service





# Service Endpoint vs Private Endpoint

PE traffic does not go over a public IP and has built **protection for exfiltration**.

**Future development is planned for PE**, not for SE.

PE has additional features such as access from peered and on-prem networks.

SE can be used in specific scenarios, but **additional security will have to be implemented** and maintained.

SE is free. PE pricing depends on inbound and outbound traffic.

PE is regional agnostic.

SE is regional specific and could provide global access for some services.

Microsoft says: "Microsoft **recommends use of Azure Private Link and private endpoints** for secure and private access to services hosted on the Azure platform."