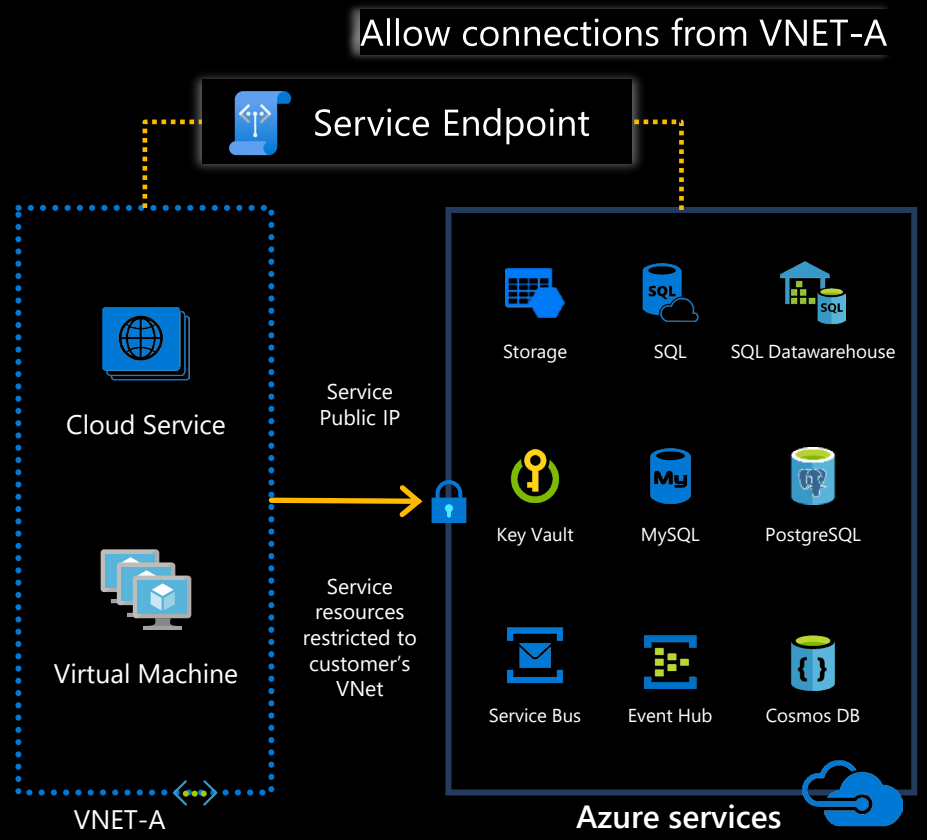
VNET Service Endpoint



VNET Service Endpoint

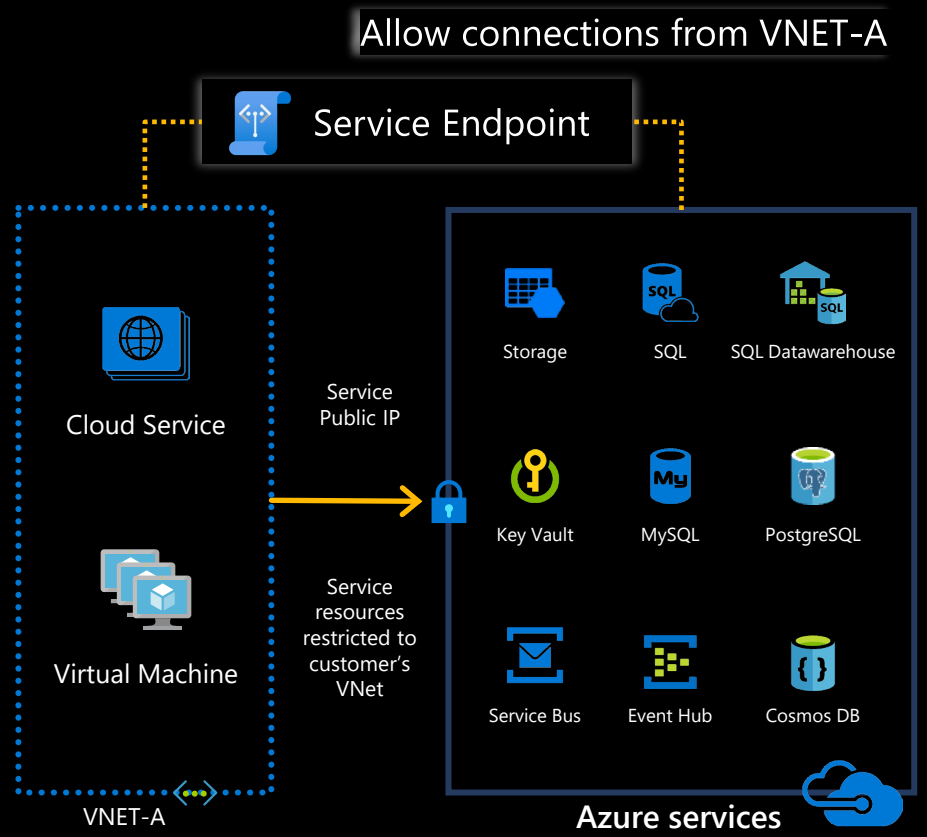
Provides private network access to Azure resources.

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

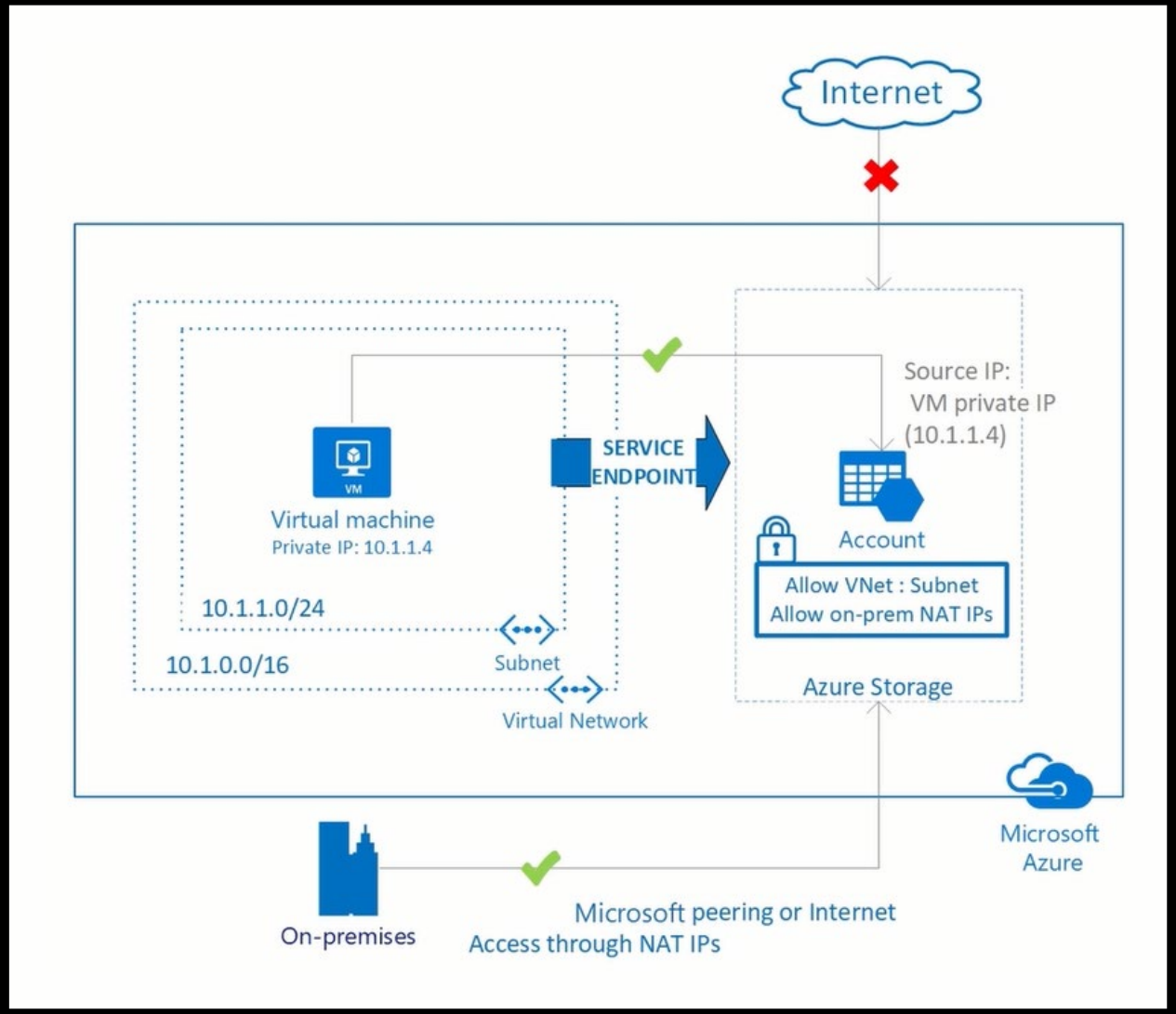
You want to limit access to your Azure services (like Storage Account, to only connections coming from your own Subnet.

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

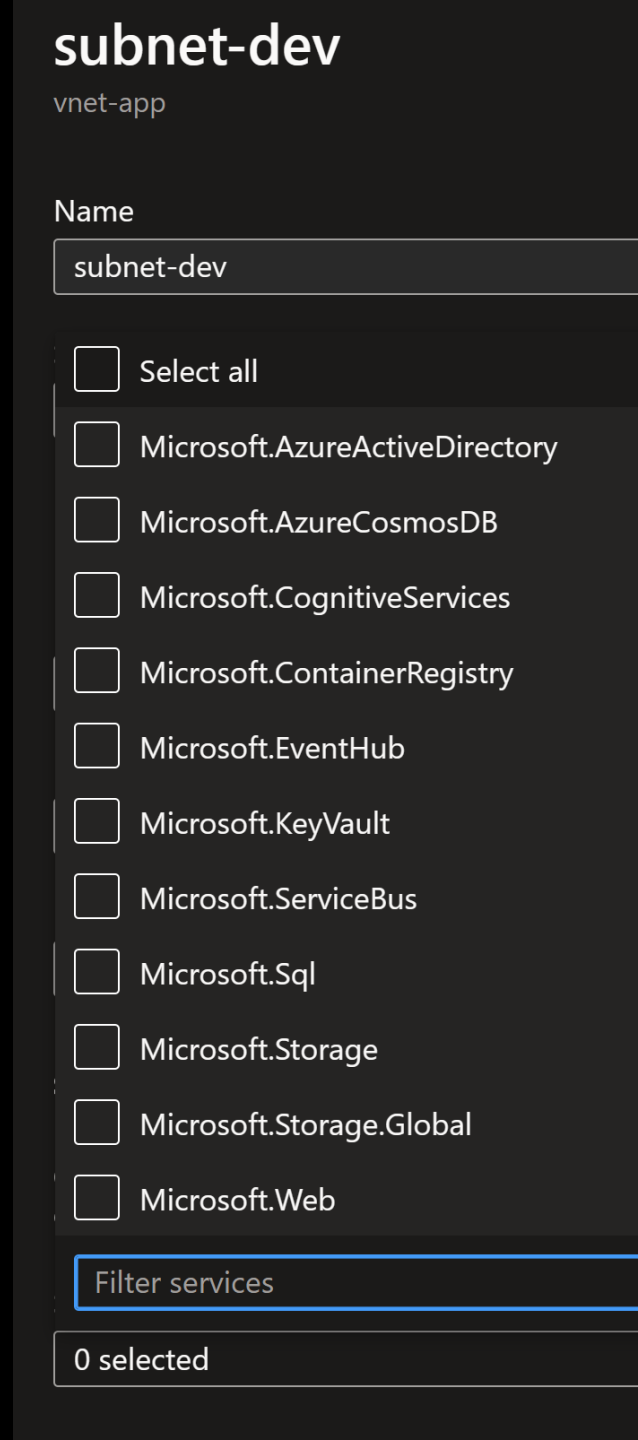
Azure CosmosDB, Azure Key Vault, Azure Service Bus

Azure Event Hubs, Azure Data Lake store Gen 1

Azure Cognitive Services

Azure Container Registry (Public Preview)

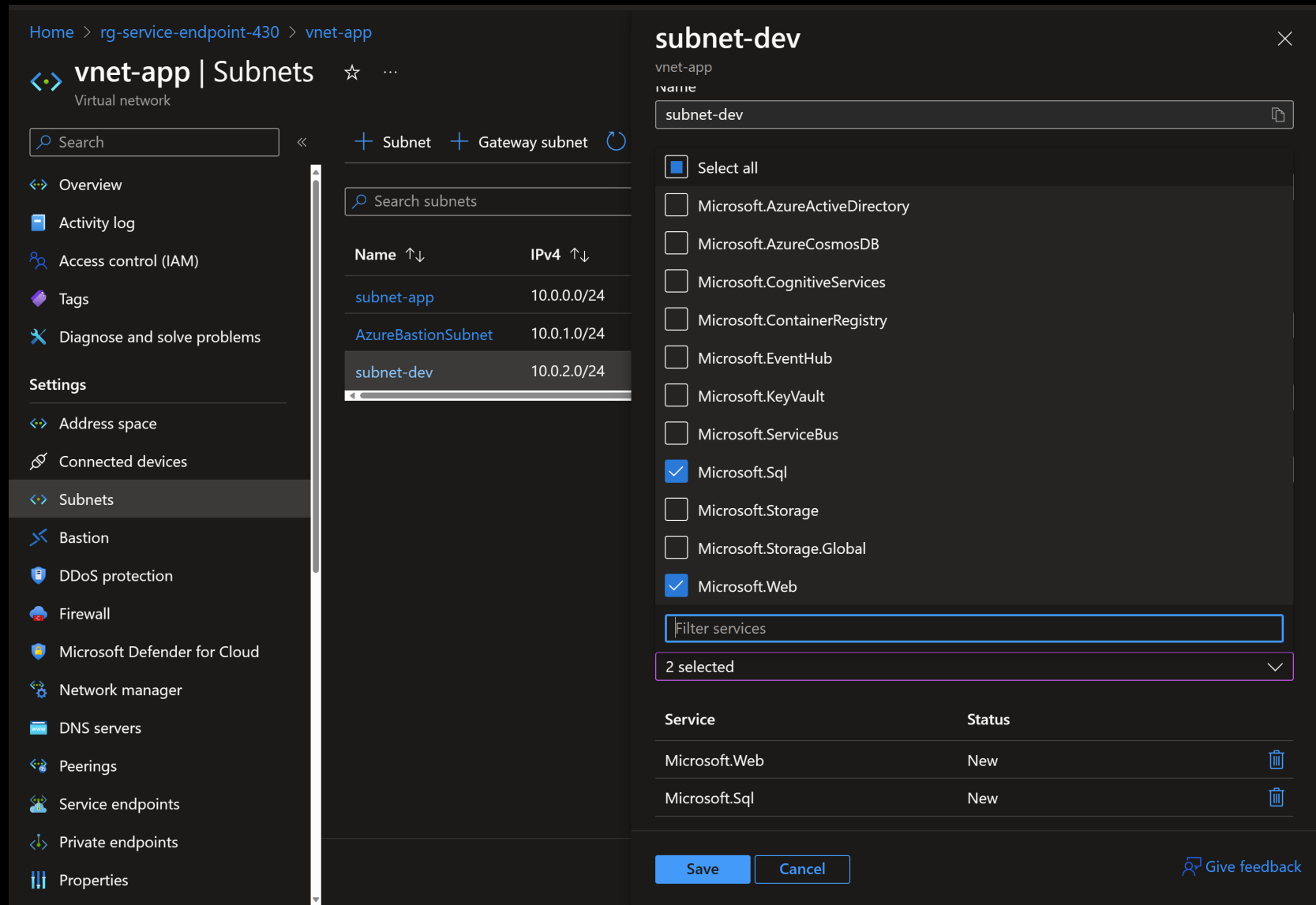
learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview



Enable Service Endpoint – step 1/2

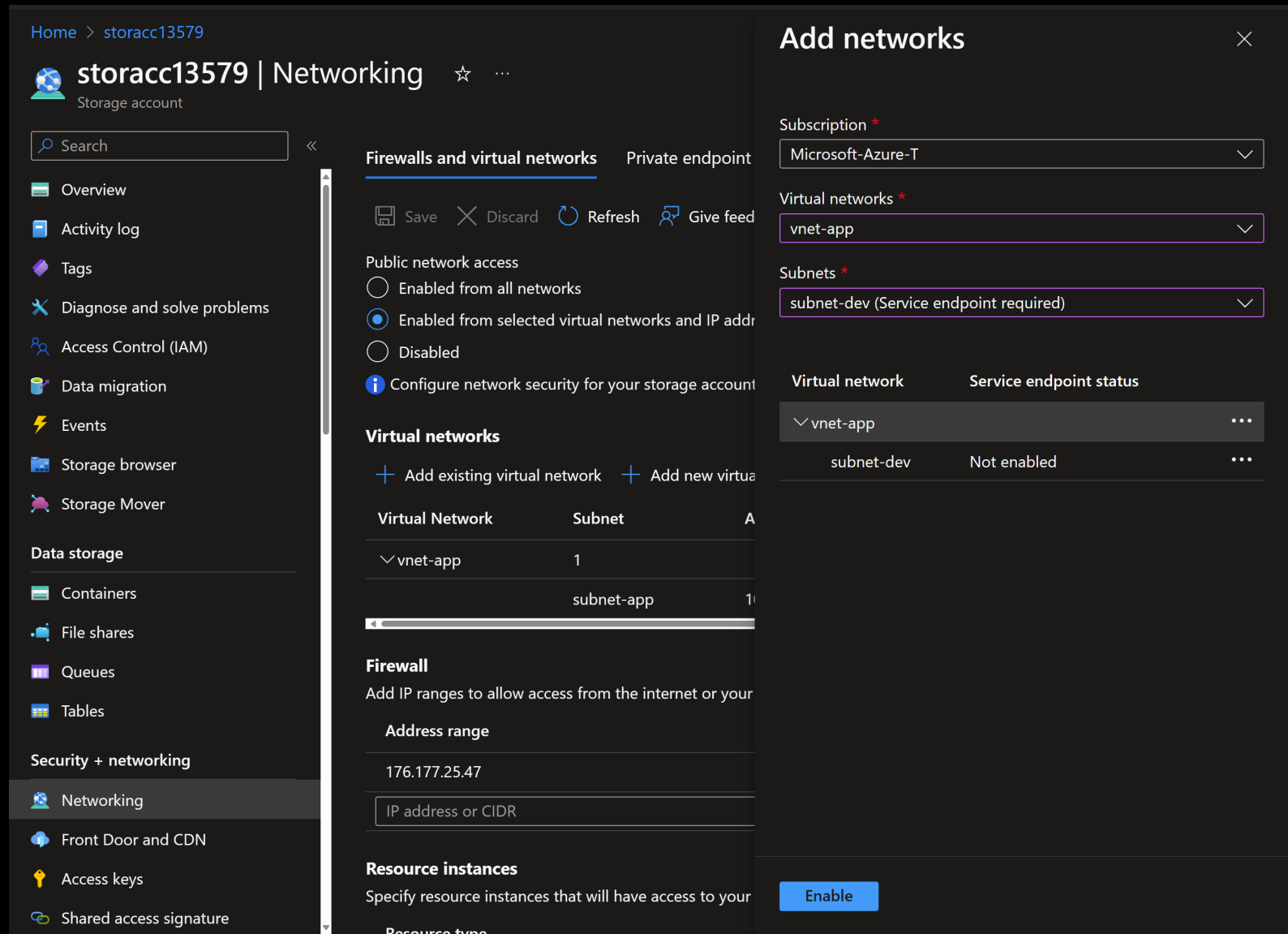
Configure Service Endpoint on the Subnet for a specific service type.

Can set multiple service types.

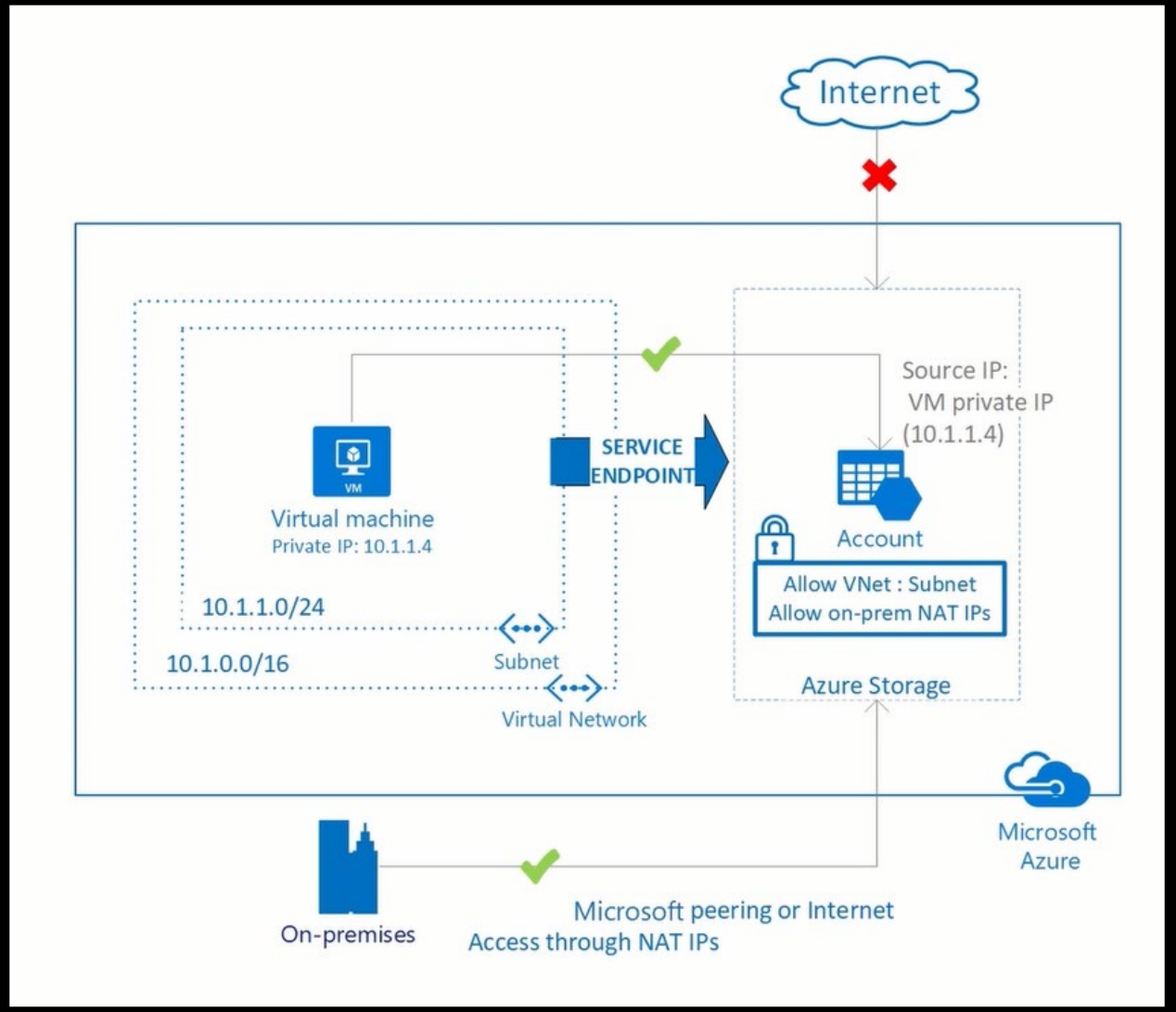


Enable Service Endpoint – step 2/2

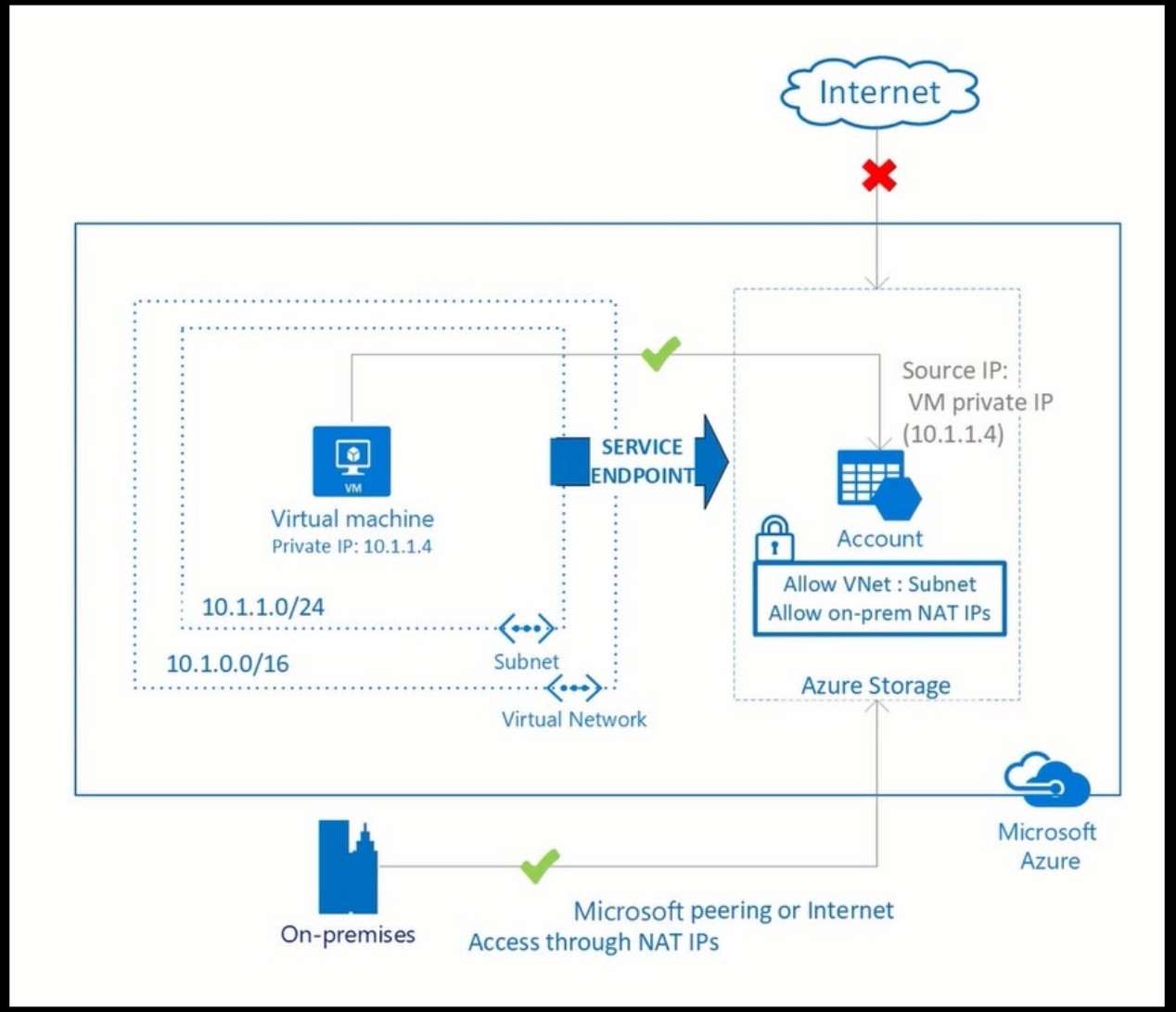
You configure your Storage Account to accept connections coming only from your Subnet.



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."