AZ:303 Assessment – See configure Network Access to the Storage Account – Lesson 2.4 - Restrict Access to Selected Networks

[Configure Azure Storage firewalls and virtual networks](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal)

## Grant access from a virtual network

You can configure storage accounts to allow access only from specific subnets. The allowed subnets may belong to a VNet in the same subscription, or those in a different subscription, including subscriptions belonging to a different Azure Active Directory tenant.

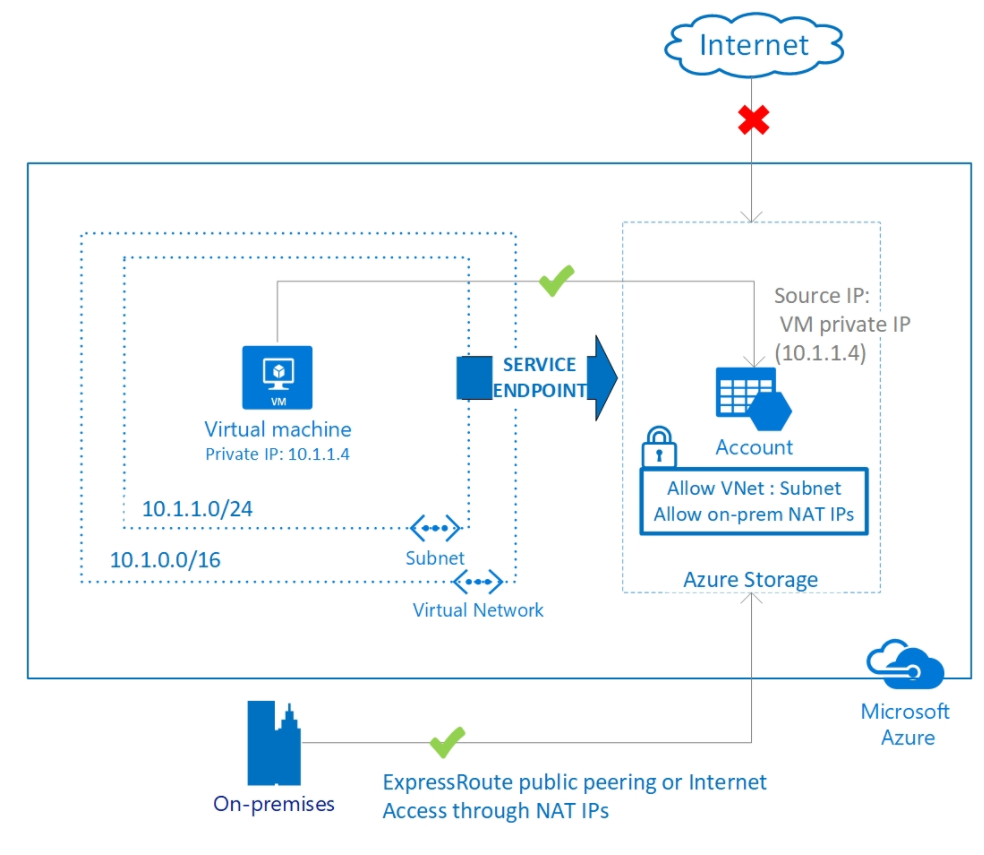
Enable a [Service endpoint](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview) for Azure Storage within the VNet. The service endpoint routes traffic from the VNet through an optimal path to the Azure Storage service. The identities of the subnet and the virtual network are also transmitted with each request. Administrators can then configure network rules for the storage account that allow requests to be received from specific subnets in a VNet. Clients granted access via these network rules must continue to meet the authorization requirements of the storage account to access the data.

**Secure Azure services to virtual networks**

* A virtual network service endpoint provides the identity of your virtual network to the Azure service. Once you enable service endpoints in your virtual network, you can add a virtual network rule to secure the Azure service resources to your virtual network.
* Today, Azure service traffic from a virtual network uses public IP addresses as source IP addresses. With service endpoints, service traffic switches to use virtual network private addresses as the source IP addresses when accessing the Azure service from a virtual network. This switch allows you to access the services without the need for reserved, public IP addresses used in IP firewalls.

**Note**

With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch. Please ensure Azure service firewall rules allow for this switch before setting up service endpoints. You may also experience temporary interruption to service traffic from this subnet while configuring service endpoints.



You can modify the storage after creation in Firewalls and virtual networks to allow access only from selected networks. (Lesson 2.4). Then add existing virtual network. Make sure that service endpoints are enabled).