Cloud Computing

Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powerd by simplilearn

Cloud Computing

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Technologies: AZ:303

Powerd by simplilearn

Implement Virtual Networking

Learning Objectives

By the end of this lesson, you will be able to:

- Analyze Virtual Networks (VNet) and its concepts
- Communicate with the internet, Azure resources, and on-premise resources
- Filter and route network traffic
- Implement Virtual Network peering
- Differentiate between Virtual Network peering and VPN gateways

A Day in the Life of an Azure Architect

You are working in a company as a cloud architect that is planning to use a few azure resources after seeing recent growth in their business. However, they are skeptical about security when using the resources for their critical business functions.

- You are asked to advise a network solution that will allow Azure resources to securely connect with one another, the internet, and on-premise network.
- The company also wants to ensure the network security and is looking for a solution that will allow or deny network traffic to the virtual machine instances in a virtual network, based upon the network rules specified.

A Day in the Life of an Azure Architect

- Also, for the communication purpose the company is looking for a solution that will allow an Azure Virtual Machine to communicate with the internet, Azure resources, and on-premise resources.
- Last but not the least, keeping the data security in mind the company is looking for a solution that can be used to deliver encrypted traffic across the public Internet between an Azure virtual network and an on-premise location.

To achieve all of the above along with some additional features, we will be learning a few concepts in this lesson that will help you find a solution for the given scenario.

Implementing Virtual Network

Azure Networking Components

Azure networking offers a wide range of services and products.

Virtual Network

Provision private networks, optionally connect to on-premise data centers

Application Gateway

Build secure, scalable, and highly-available web front-end in Azure

Content Delivery Network

Ensure secure reliable content delivery with a broad global reach

Azure Networking Components

Load Balancer

Deliver highly available network performance to your application

VPN Gateway

Establish secure cross-premises connection

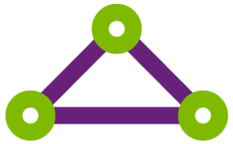
Traffic Manager

Route incoming traffic for high performance and availability

Azure Networking Components

Azure DNS

Host your DNS Domain in Azure



ExpressRoute

Dedicated private network fiber connection to Azure

Network Watcher

Network performance monitoring and diagnostics solution

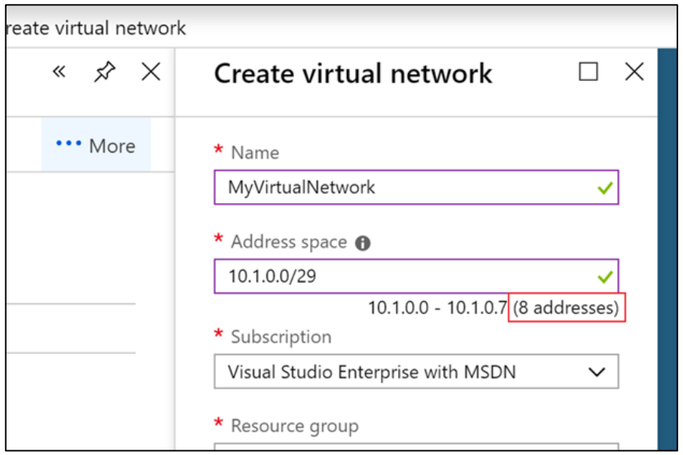
Virtual Network

Virtual Network (VNet) is a logical representation of user's own network in the cloud.

VNets are used to provide private connectivity between Azure Virtual Machines and other Azure services.

Virtual Network Concepts

The four concepts of Azure virtual network are:



Address space:

When creating a VNet, an user must specify a custom private IP address space using public and private (RFC 1918) addresses.

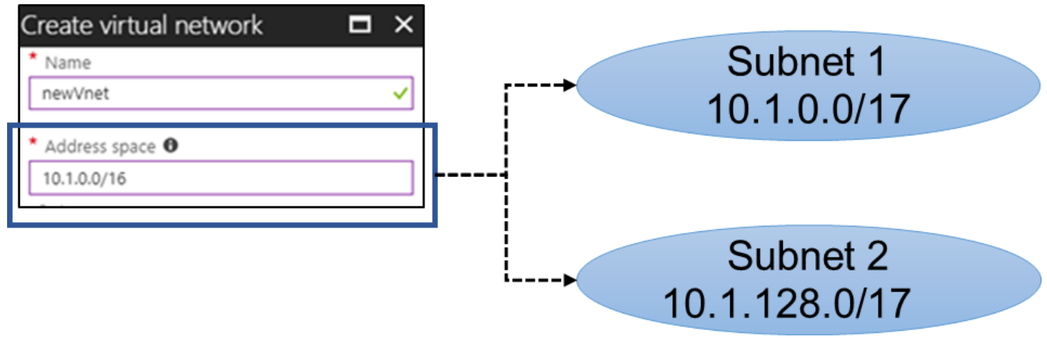
By default, Azure assigns resources in a virtual network a private IP.

Subscription:

VNet are scoped to a subscription.

Virtual Network Concepts

The four concepts of Azure virtual network are:



Subnets:

A virtual network can be divided into one or more sub-networks and these sub-networks are referred to as Subnets.

Regions:

While creating a VNet, a single region or location can be selected for deployment.

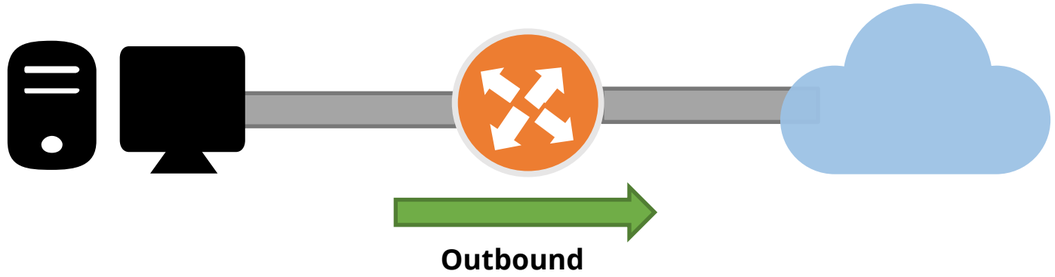
Virtual Network Best Practices

These are the best practices for a Virtual Network.

- Ensure non-overlapping address space
- Ensure that the entire VNet address space is not covered
- Configure a few larger VNets than many small ones, this prevents management overhead
- Secure VNets by assigning Network Security Groups to subnets

Communication with the Internet

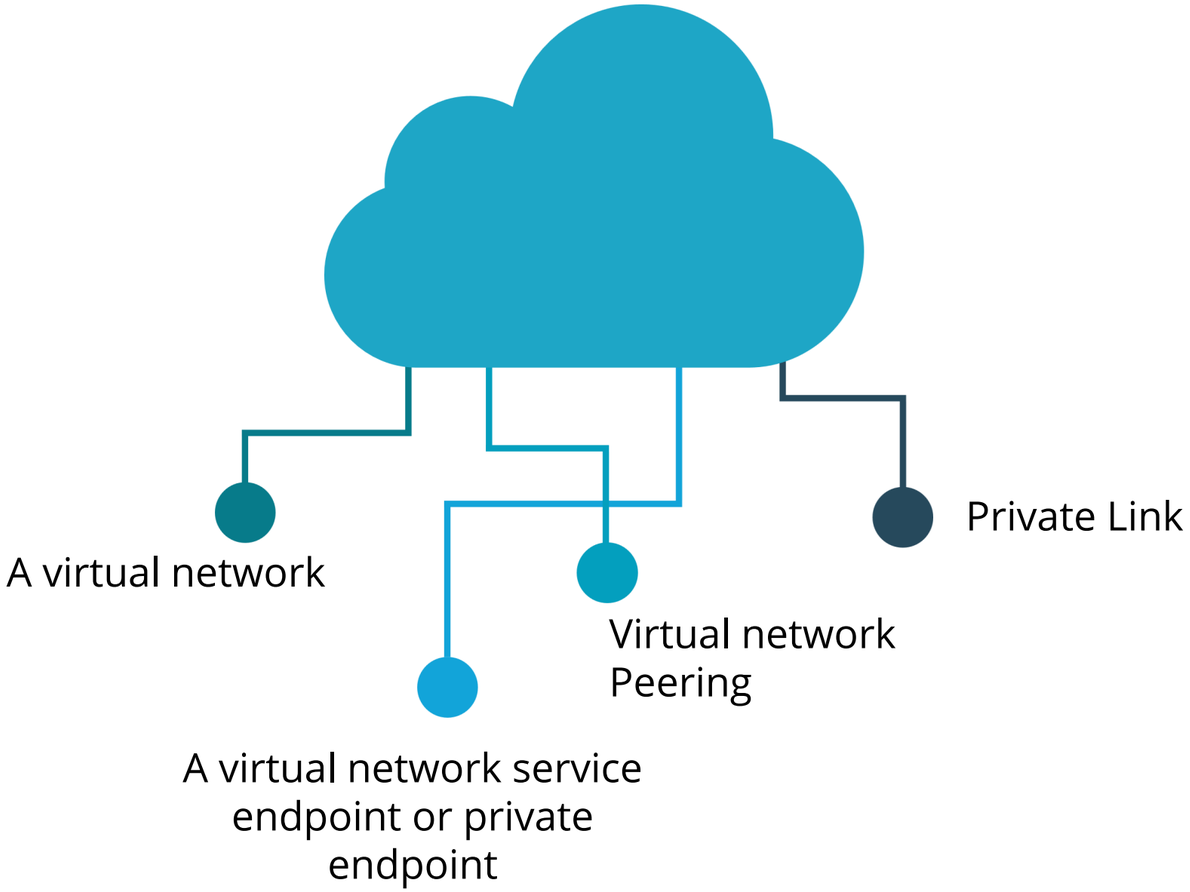
Outbound traffic is allowed by default, so a VNet can communicate outbound with the internet.



Inbound traffic can be provided by assigning a public IP addresses or a public load balancer.

Communication Between Azure Resources

There are different ways for Azure resources to communicate securely with each other:



Communication with On-Premise Resources

Connecting the on-premise computers and networks to a virtual network can be done in a variety of ways:

Point-to-site VPN:

Established between a virtual network and a single computer in your network.

Site-to-site VPN:

Established between users on-premise VPN device and an Azure VPN Gateway.

Azure ExpressRoute:

Established between your network and Azure through an ExpressRoute partner.

Filter Network Traffics

Network traffic can be filtered using:

Network Security groups (NSGs)

An NSG contains a list of security rules that allow or deny inbound or outbound network traffic. An NSG can be associated to a subnet or a network interface.

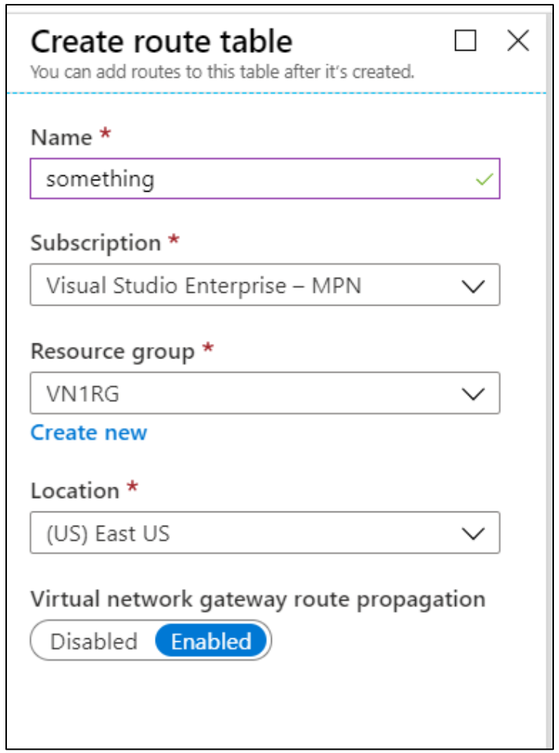
Network virtual appliances (NVA)

An NVA is a VM that performs a network functions, such as a firewall, WAN optimization, or any other network function.

Route Network Traffic

By default, Azure routes traffic between subnets, connected virtual networks, on-premise networks, and the Internet.

The following can be used to override the default rules:

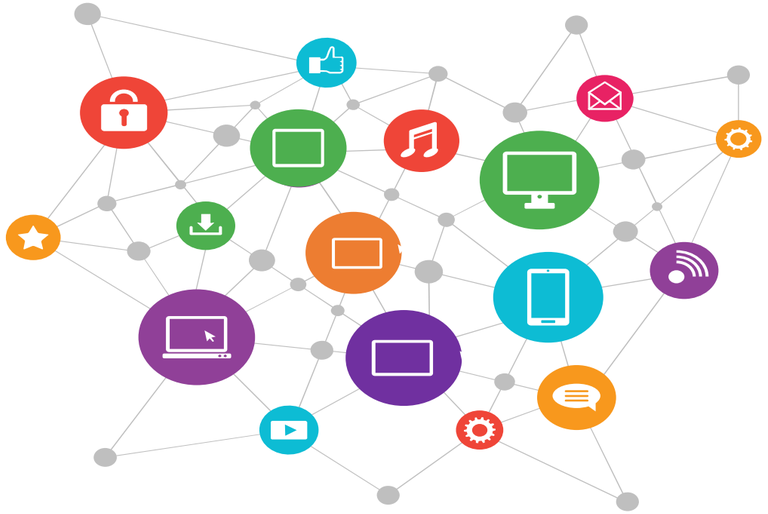


Route tables:

For each subnet, custom tables with routes can be created. This helps in monitoring where the traffic is routed.

Route Network Traffic

The following can be used to override the default rules:



Border Gateway Protocol routes:

on-premise BGP routes can be propagated to virtual networks if the virtual network is connected to the on-premise network using an Azure VPN Gateway or ExpressRoute connection.

Assisted Practice

Creating a VNet

Duration: 10 Min.

Problem Statement:

You've been assigned the task of creating a VNet that will allow Azure resources to securely connect with one another, the internet, and on-premise networks.

Assisted Practice: Guidelines

Steps to create a virtual network:

1. Go to the Azure Portal
2. Select Virtual network from Azure services
3. Create a virtual network

Assisted Practice

Creating a Subnet

Duration: 10 Min.

Problem Statement:

You are given a project to create a subnet to have a range of IP addresses in the VNet. You can divide a VNet into multiple subnets for organization and security.

Assisted Practice: Guidelines

Steps to create a subnet:

1. Go to the Azure Portal
2. Select Virtual network from Azure services
3. Create a subnet

Assisted Practice

Creating Network Security Group (NSG)

Duration: 10 Min.

Problem Statement:

You are given a project to create an NSG to activate a rule or access control list (ACL), which will allow or deny network traffic to your virtual machine instances in a virtual network.

Assisted Practice: Guidelines

Steps to create an NSG:

1. Go to the Azure portal
2. Create a resource
3. Enter Network security group in the Search Marketplace box
4. Create the Network security group

Assisted Practice

Creating Network Interface Card (NIC)

Duration: 10 Min.

Problem Statement:

You've been tasked with creating a network interface card (NIC) that will allow an Azure Virtual Machine to communicate with the internet, Azure resources, and on-premise resources.

Assisted Practice: Guidelines

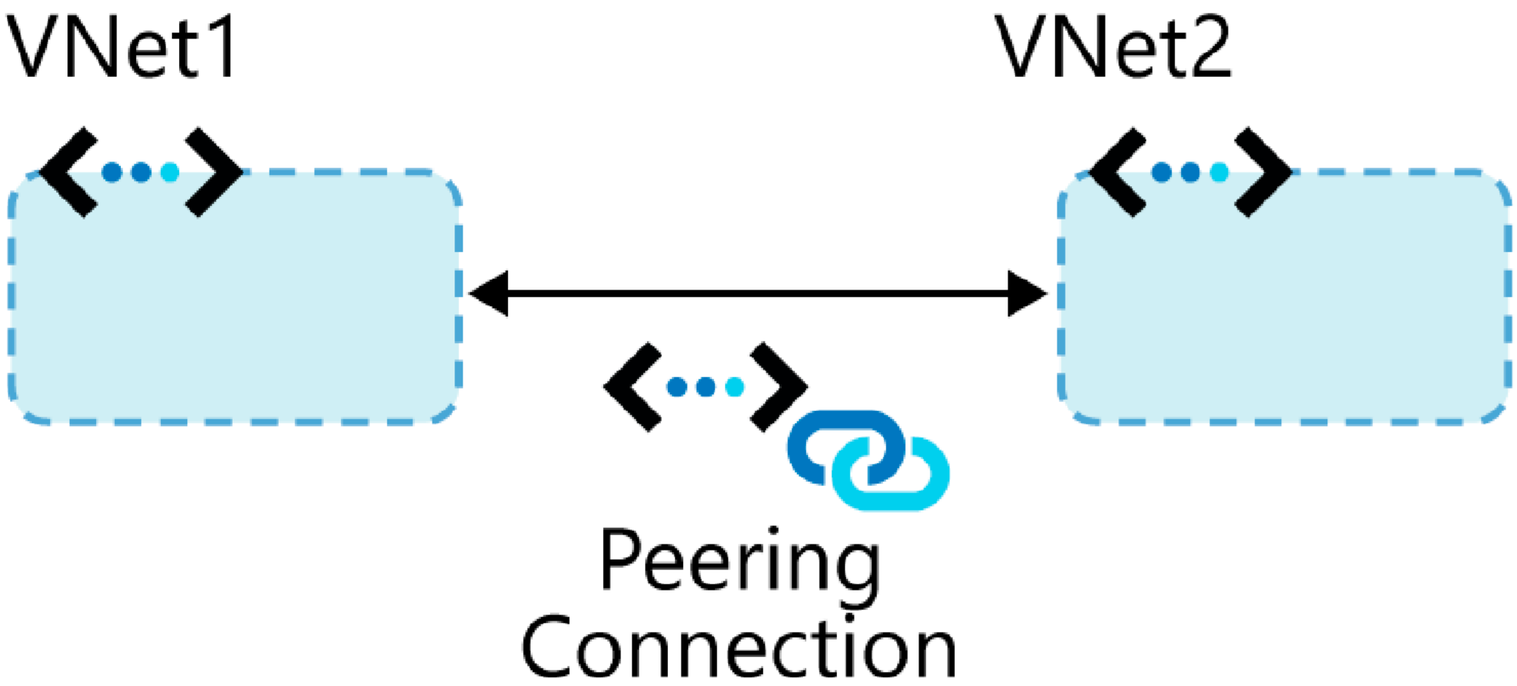
Steps to create an NIC:

1. Go to the Azure portal
2. Create a resource
3. Enter Network interface in the Search Marketplace box
4. Create the Network interface

Virtual Network Peering

Virtual Network Peering

Virtual Network (Vnet) Peering connects two Azure virtual networks.



Virtual Network Peering Types

These are the types of peering connection:

Virtual network peering

Connects virtual networks in the same azure region
E.g. Connecting two virtual networks in north Europe.

Global virtual network peering

Connects virtual networks present in different azure regions
E.g. Connecting a virtual network in north Europe and a virtual network in west europe.

Peering Considerations

When it comes to VNet Peering, keep the following in mind:

Reciprocal connections:

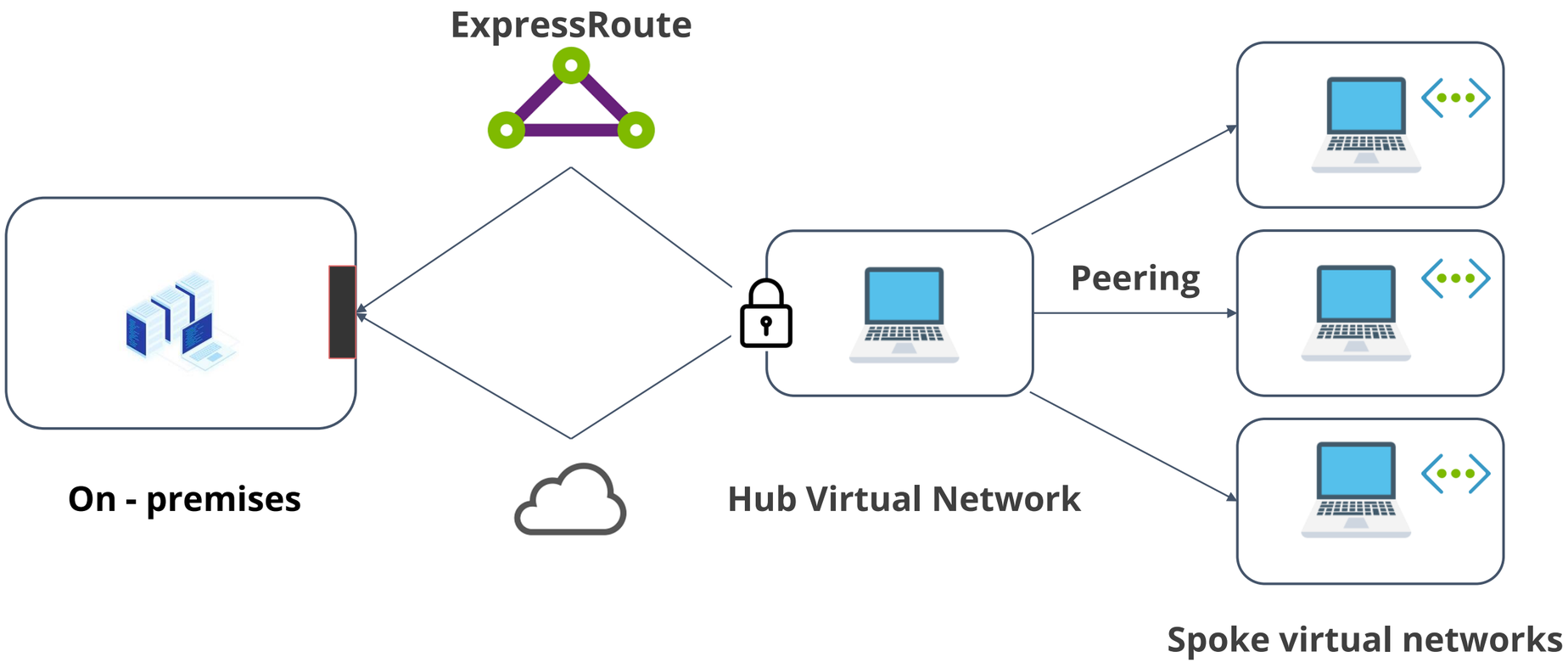
A user must establish a connection in each virtual network to link the networks while using virtual network peering.

Cross-subscription connections:

Virtual network peering can be done even when both virtual networks are in different subscriptions.

Transitivity

Peer-to-peer transitive routing is a concept used in azure to describe network traffic that is routed via an intermediary virtual network between two virtual networks.



Note: Virtual network peering is nontransitive.

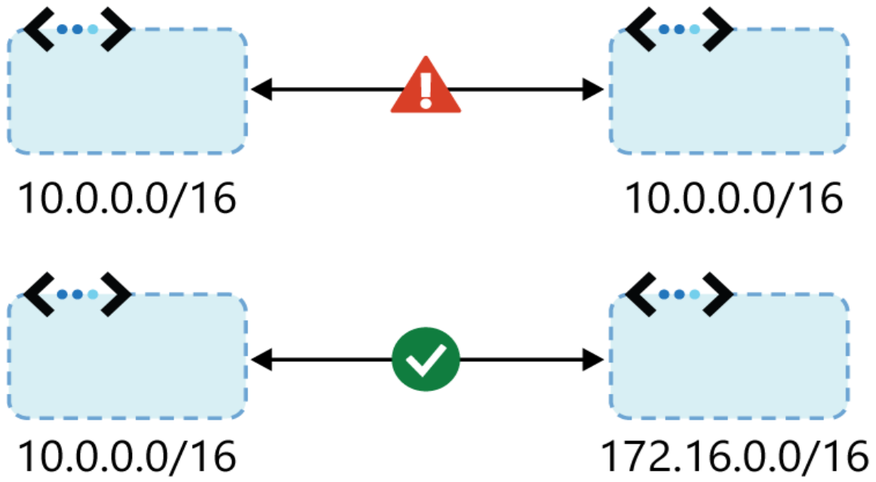
Gateway Transit

Benefits of Gateway Transit are:

- Facilitate cross-premise connectivity
- Enable the Allow gateway transit option in the hub
- Enable the Use remote gateway option on the spoke

Peering considerations

- IP address spaces should not overlap
- Peering is the recommended option



VNet Peering and VPN Gateways

VNet Peering

- Is direct (no interconnecting device)
- Has low-latency and high-bandwidth
- Is regional or global

VPN Gateway

- Serves as an interconnecting devices
- Introduces extra latency and limits bandwidth

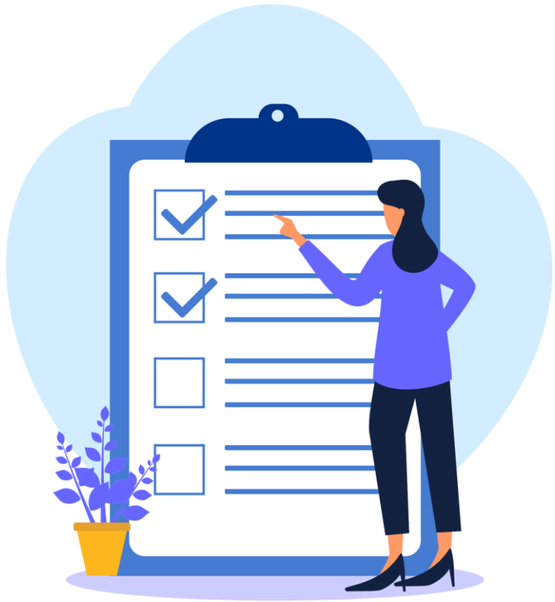
Gateway Transit

- Allows sharing a VPN or Express Route gateway across a peering
- Minimizes complexity and centralizes management

VNet Peering Vs VPN Gateways

Virtual Network peering and VPN gateways support connecting:

- Virtual networks in different regions
- Virtual networks in different Azure Active Directory tenants
- Virtual networks in different azure subscriptions
- Virtual networks that use a mix of azure deployment models

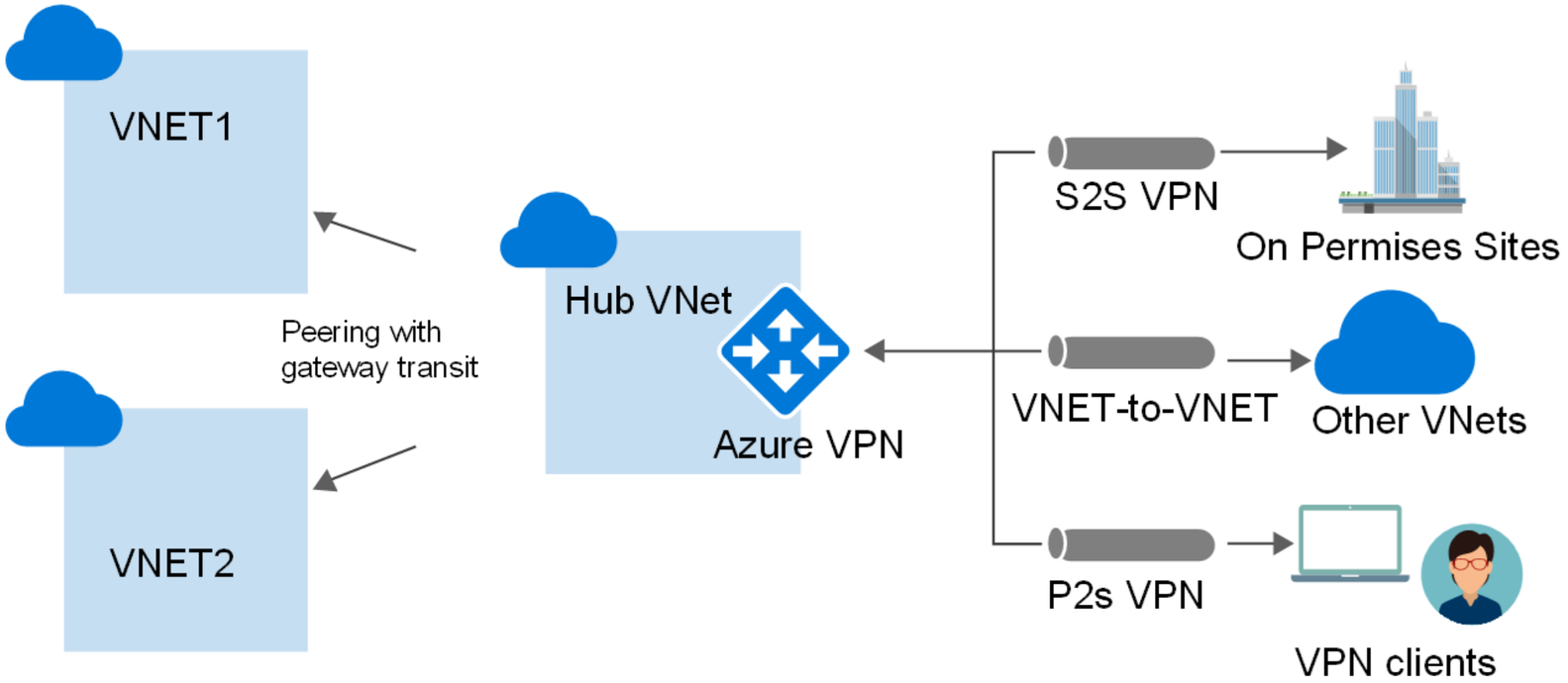


VNet Peering Vs VPN Gateways

Item	Virtual network peering	VPN Gateway
Limits	Up to 500 per VNet	One per VNet (per gateway limits are SKU dependent)
Pricing model	Ingress/Egress	Hourly + Egress
Encryption	Not included	IPsec/IKE
Bandwidth	No limits	SKU-dependent
Public endpoints	No	Yes
Transitivity	No	Yes (routing dependent)
Initial setup time	Fast	30 minutes
Typical scenarios	Data replication, database failover, and other scenarios needing frequent backups of large data	Encryption-specific scenarios that are not latency sensitive and do not need high throughout

Service Chaining

Service chaining allows you to direct traffic from one virtual network to a virtual appliance or virtual network gateway in a peered virtual network, through user-defined routes.



Assisted Practice

Creating a Public IP

Duration: 10 Min.

Problem Statement:

You've been assigned a project to build a public IP address that will allow Azure resources to communicate with the Internet and public Azure services.

Assisted Practice: Guidelines

Steps to create a Public IP:

1. Go to the Azure portal
2. Create a resource
3. Enter Public IP address in the Search Marketplace box
4. Create the Public IP address

Assisted Practice

Creating a VPN Gateway

Duration: 10 Min.

Problem Statement:

You've been given the task of creating a VPN Gateway that will deliver encrypted traffic across the public Internet between an Azure virtual network and an on-premise location.

Assisted Practice: Guidelines

Steps to create a VPN Gateway:

1. Go to the Azure portal
2. Create a resource
3. Create a virtual network
4. Create a subnet configuration
5. Create a gateway subnet
6. Create a VPN gateway

Key Takeaways

- Virtual Network (VNet's) is a logical representation of user's own network in the cloud.
- Network Traffic can be filtered using Network Security groups, Network Virtual Appliances.
- Azure routes traffic between subnets, connected virtual networks on-premise networks, and the Internet.
- Virtual Network (Vnet) Peering connects two azure virtual networks.

Implement VNet Peering

Duration: 25 Min.

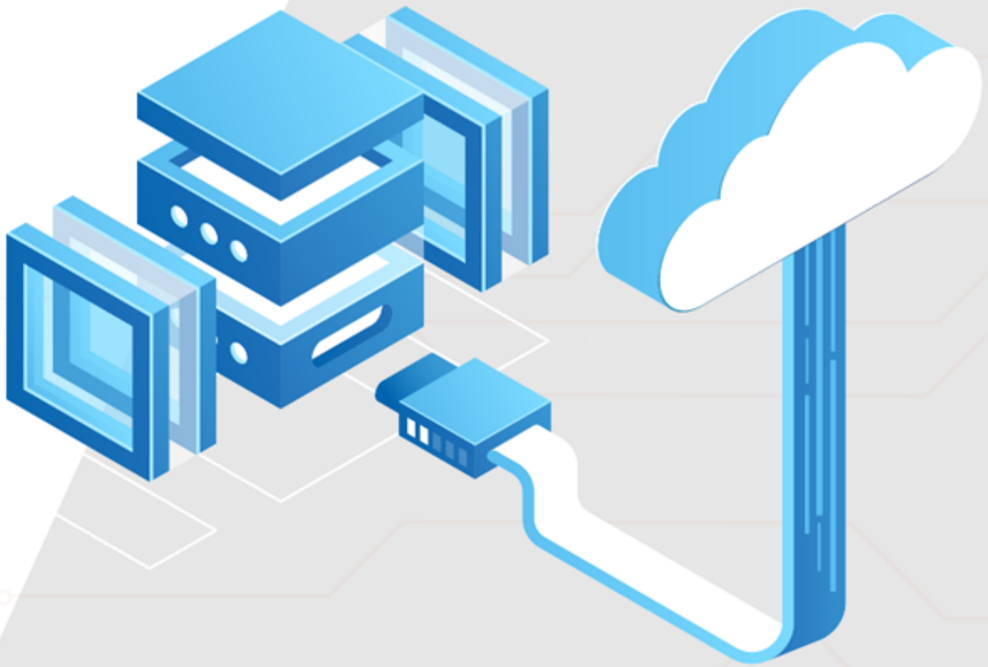
Project Agenda: To implement VNet Peering

Description: You have been given a project to create two virtual networks in the same region. Do ensure that the virtual networks have different address space. Once the virtual networks are created you need to create peering between these virtual networks so that resources in these VNets can interact with each other privately.

Perform the following:

Create two virtual networks in the same region and peer them both.

LESSON-END PROJECT



Thank you