Microsoft

# AZ-800 Administer Windows Server Hybrid Core Infrastructure

# Agenda AZ-800

1 Deploy and manage identity infrastructure – Windows Server
2 Deploy and manage identity infrastructure – Hybrid

3 Administering Windows Server Hybrid Core Infrastructure – Windows Server
4 Administering Windows Server Hybrid Core Infrastructure – Hybrid

5 Manage virtualization and containers – Windows Server
6 Manage virtualization and containers – Hybrid

7 Implement and manage networking infrastructure – Windows Server
8 Implement and manage networking Infrastructure – Hybrid

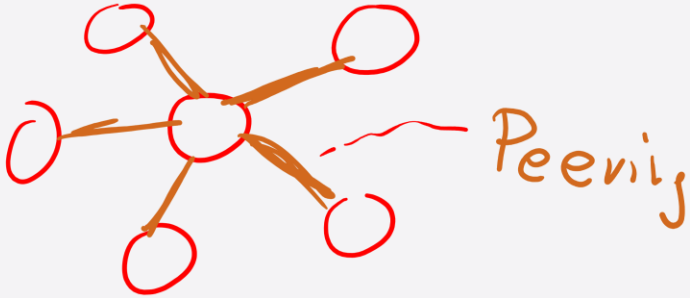
9 Configure storage and file services – Windows Server
10 Configure storage and file services – Hybrid

# Implement and manage an on-premises and hybrid networking Infrastructure *(Implementing hybrid networking infrastructure)*

- Implement hybrid network infrastructure
- Implement DNS for Windows Server IaaS VMs
- Implement Windows Server IaaS VM IP addressing and routing
- Lab 08 – Implementing Hybrid Networking Infrastructure

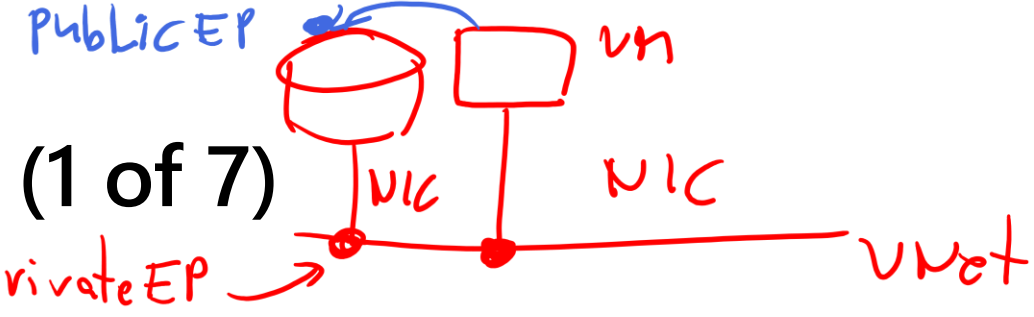
# Implement hybrid network infrastructure

# Learning Objectives – Hybrid network infrastructure




- Describe Azure network topologies
- Implement an Azure private virtual network (VPN)
- Create a route-based VPN gateway using the Azure portal
- Implement Azure ExpressRoute
- Implement an Azure wide area network (WAN)
- Implement DNS resolution in hybrid environments
- Learning recap

# Describe Azure network topologies (1 of 7)




VNet 10.0.0.0/16

## What is a virtual network?

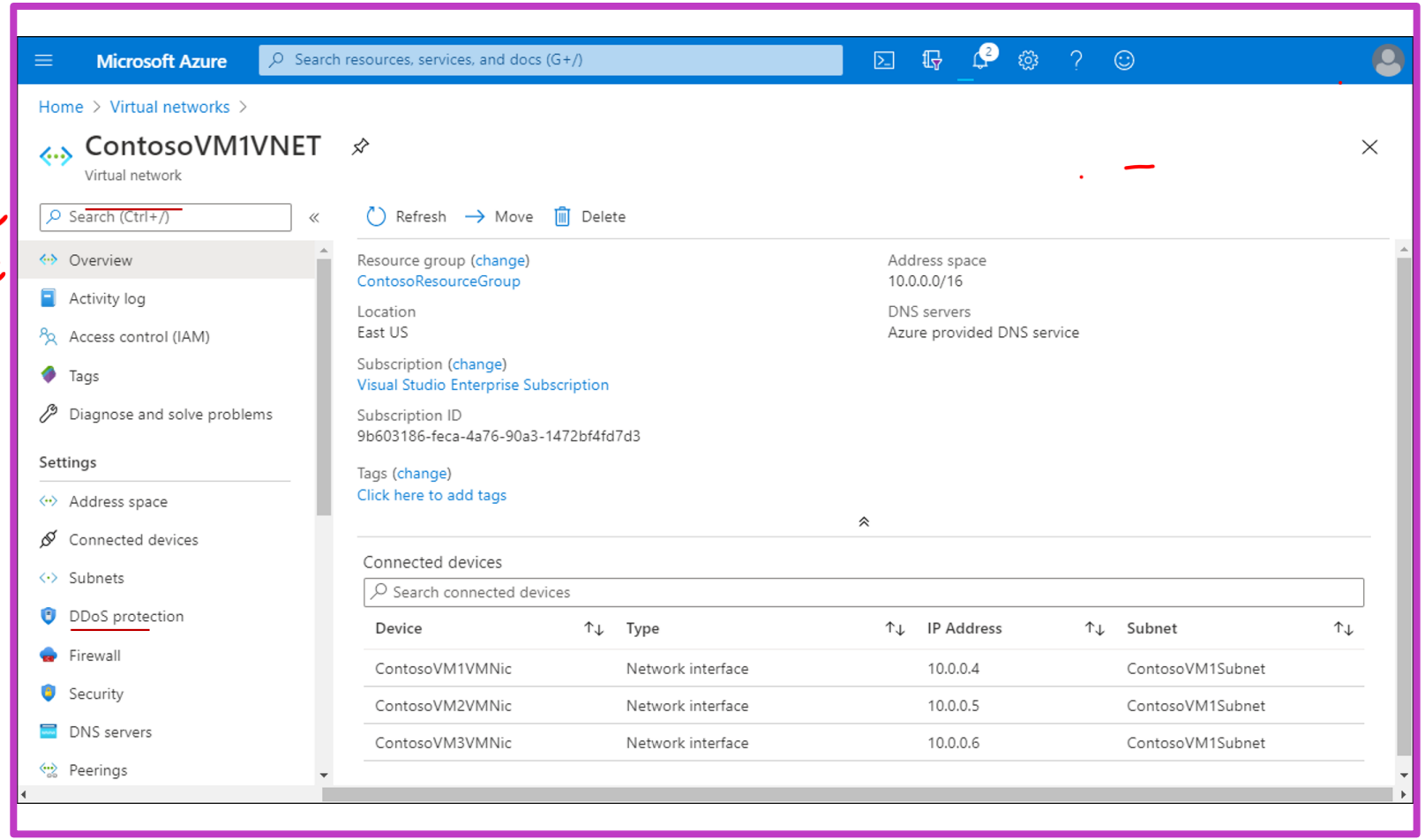
- Azure Virtual Network is the Fundamental building block for your private network in Azure.

## What is a Subnet?

10.0.0.0/24
10.0.1.0/24

- A subnet is subsection of a VNet. Subnet releases the IP address to Azure resources.
- Azure VMs, Appservices, Load balancers, Firewall, Bastion server and other Azure resources get the private IP address from the subnet.

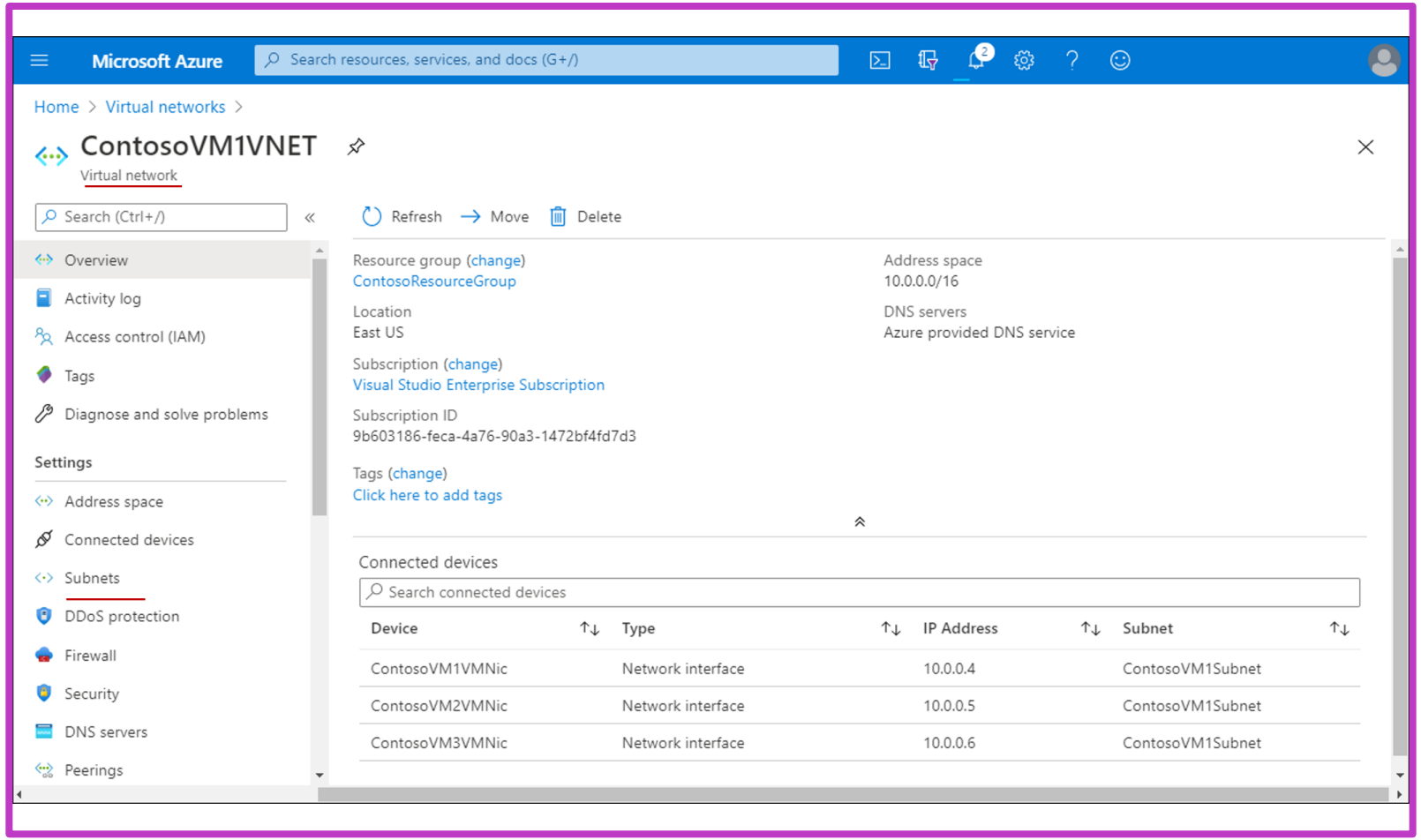
GatewaySubnet



# Describe Azure network topologies (2 of 7)

## What is a Network Interface?

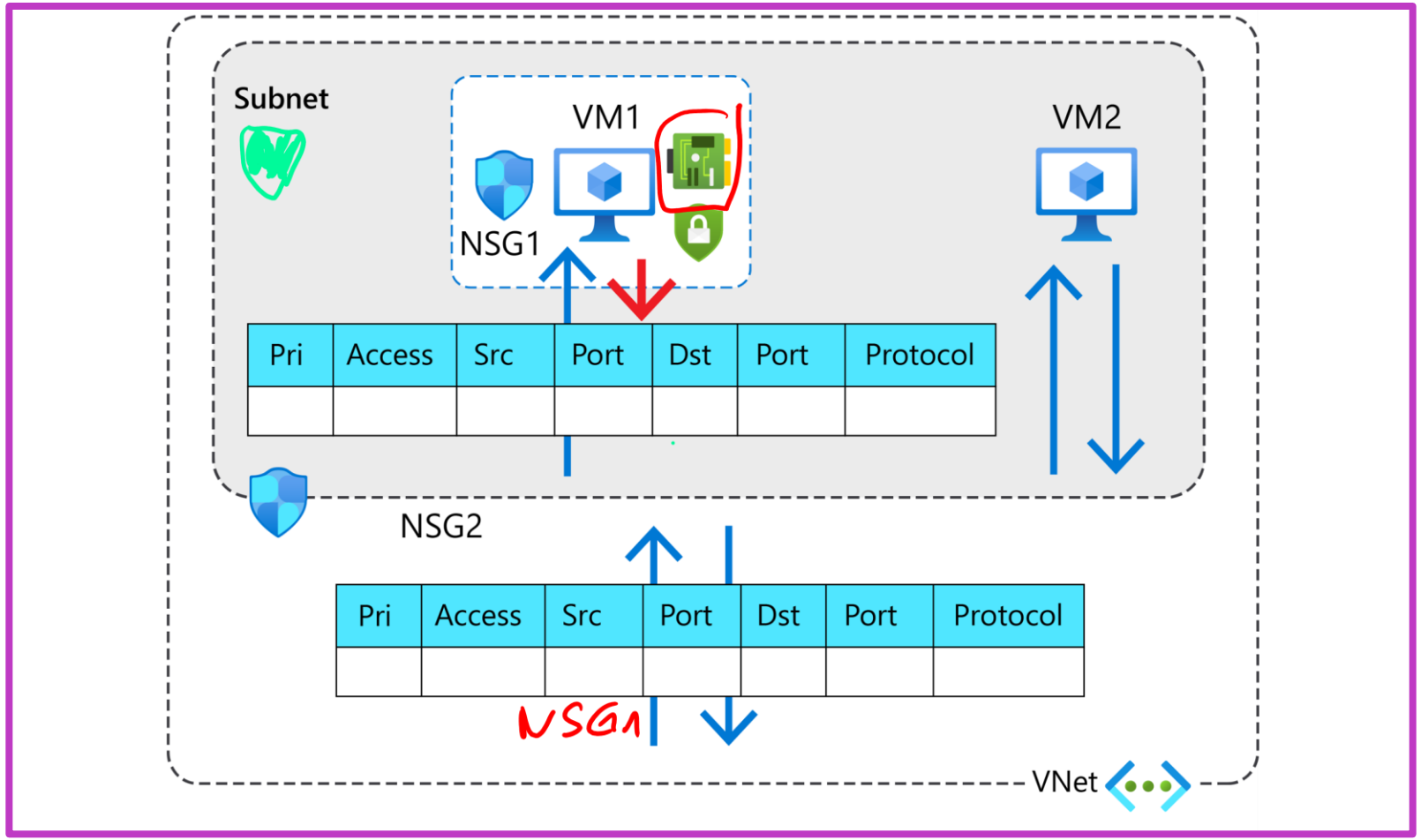
- A Network interface card enables an Azure VM to communicate with Internet, Azure, and on-premises resources.
- A virtual machine cannot exist with out a Network interface card (NIC).
- Even in the Shutdown state, the NIC is always attached to the VM.
- A VM can have multiple NIC cards within the same VNet.



# Describe Azure network topologies (3 of 7)

## What is a network security group?

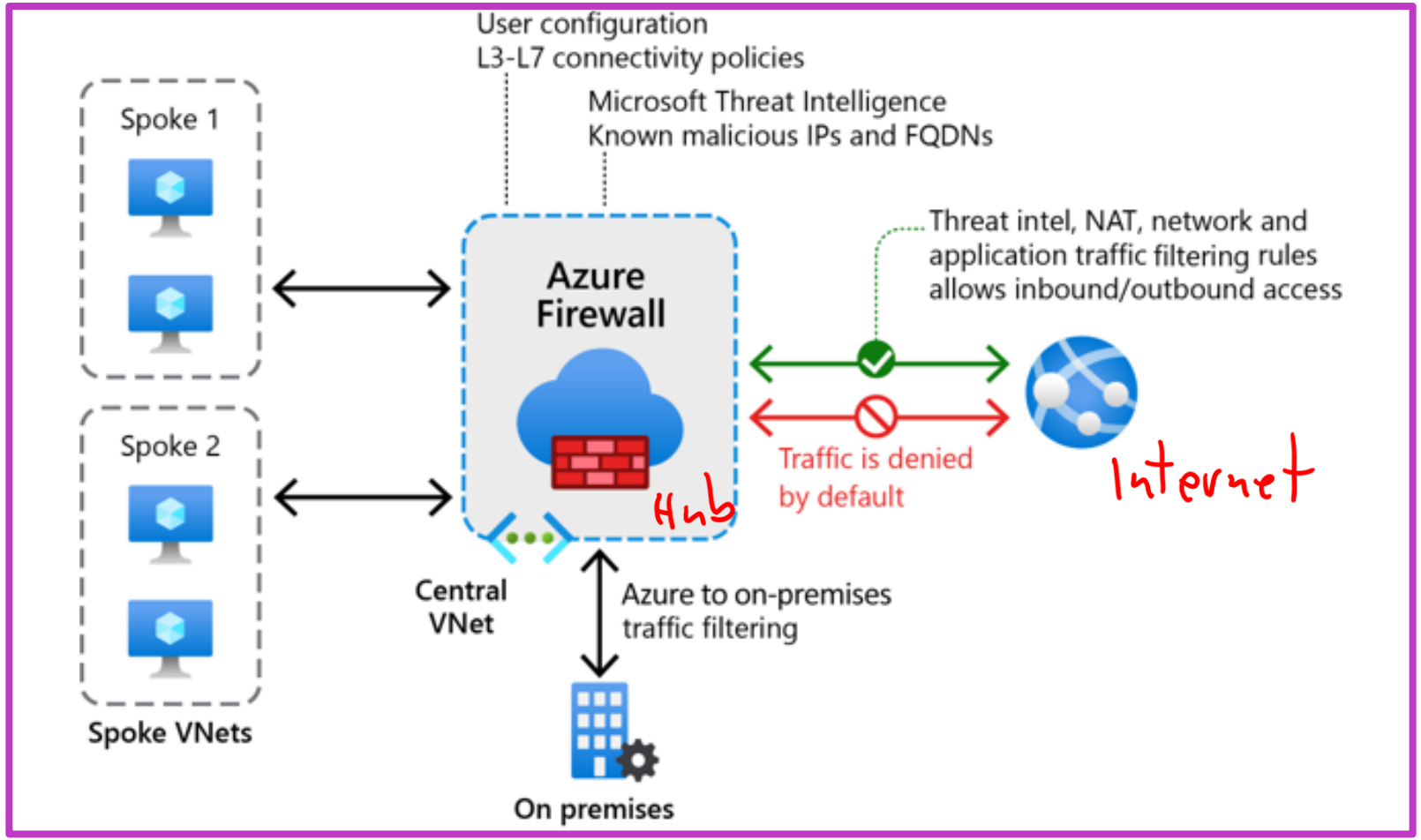
- A network security group (NSG) contains security rules that filters inbound and outbound network traffic.
- You can use NSGs to allow or deny network traffic. Rules are stateful.
- NSGs work with 5-tuple information (Source, destination, source port, destination port and protocol).
- NSGs can be assigned to VM NIC card or to a Subnet or both.
- NSG rules can be in between 100- 4096. The lower the number the higher the priority.



# Describe Azure network topologies (4 of 7)

## What is Azure Firewall?

- Azure Firewall is a cloud-native and intelligent network firewall security service.
- It is a fully stateful, firewall as a service, with built in High Availability.
- There are two types of Azure firewalls, standard and premium.
- Azure firewall provides Layer 3-7 filtering and threat intelligence.
- You can connect multiple VNets to Azure firewall.



# Describe Azure network topologies (5 of 7)

## What is Azure VPN Gateway?

- A VPN gateway is a specific type of VNet gateway that you can use to send encrypted traffic between two locations. For example: from Azure to on-premises, between VNets in Azure, or Azure to other cloud providers.
- A virtual Network Gateway is composed of two or more platform as a service (PaaS) VMs.
- VPN gateway requires one public IP and one Private IP. Public IP is provided by Azure, Private IP is assigned by its own dedicated subnet called “GatewaySubnet”.
- After VPN gateway deployment you can create IPsec/IKE VPN tunnel connections to other VNets/ on-premises/other cloud providers to encrypt the traffic.
- Only one VPN gateway is allowed per VNet but you can create multiple VPN connections to the same VNet.

# Describe Azure network topologies (6 of 7)

## What is Azure ExpressRoute?

- ExpressRoute is a dedicated private connection to Azure. The traffic is not routed though the internet.
- With ExpressRoute, you can extend your on-premises networks into the Microsoft cloud.
- By using ExpressRoute, you can establish connections to Microsoft cloud services, including Azure and Microsoft Office 365.
- ExpressRoute offers standard and premium versions and is mostly used for production traffic.

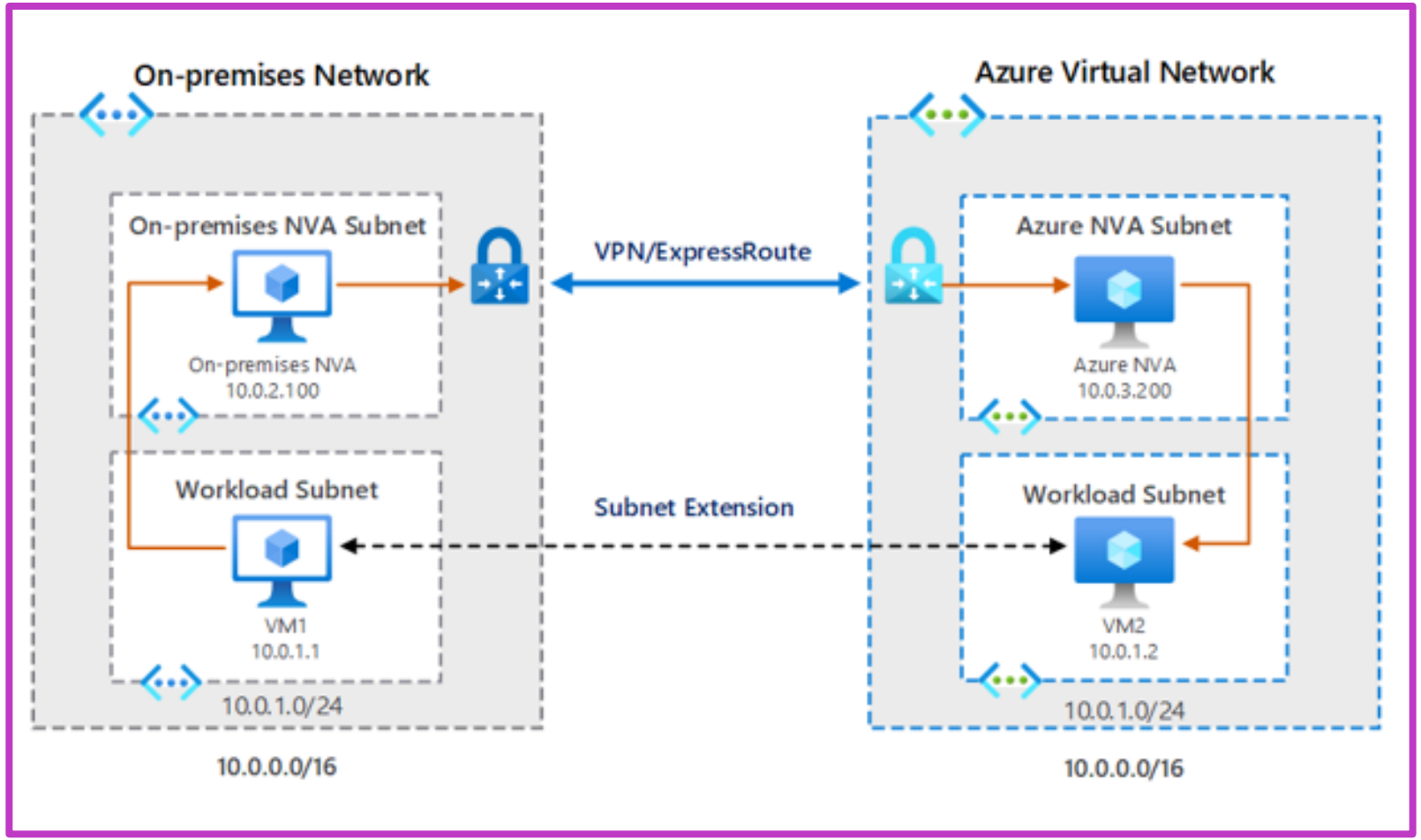
## What is Azure Virtual WAN?

- Azure Virtual WAN is a networking service that provides networking, security, and routing functionalities.
- It provides a single operational interface.
- It has a Hub and Spoke architecture.
- It enables global transit architecture.

# Describe Azure network topologies (7 of 7)

## Azure subnet extension

- Extending a subnet enables you to include Azure resources as part of your own local, on-premises subnets, which essentially makes these separate locations part of the same IP broadcast domain.
- You can extend an on-premises subnet to Azure using a layer-3 overlay network-based solution.



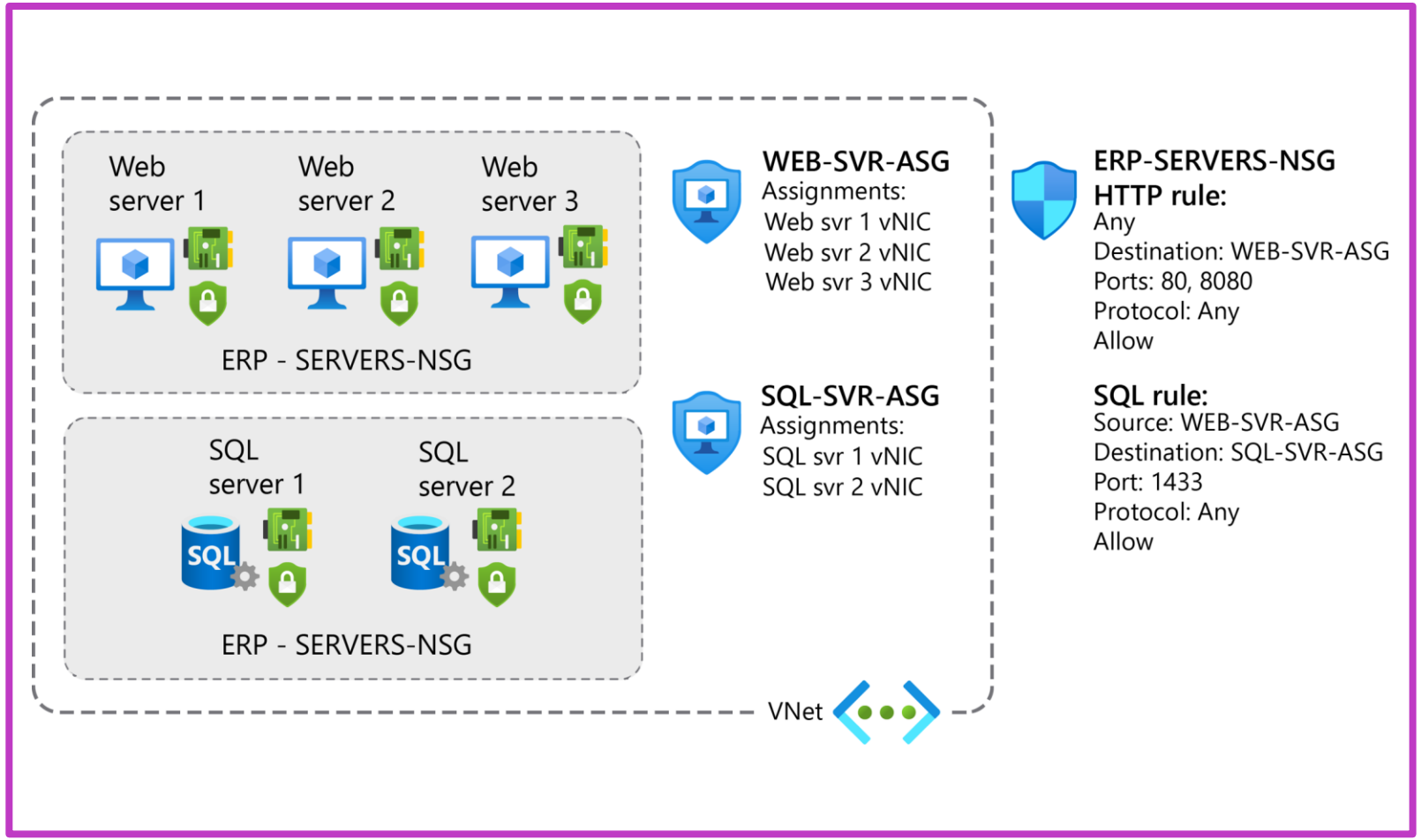
# Application security groups

**An application security group (ASG) enables you to group network interfaces together.**

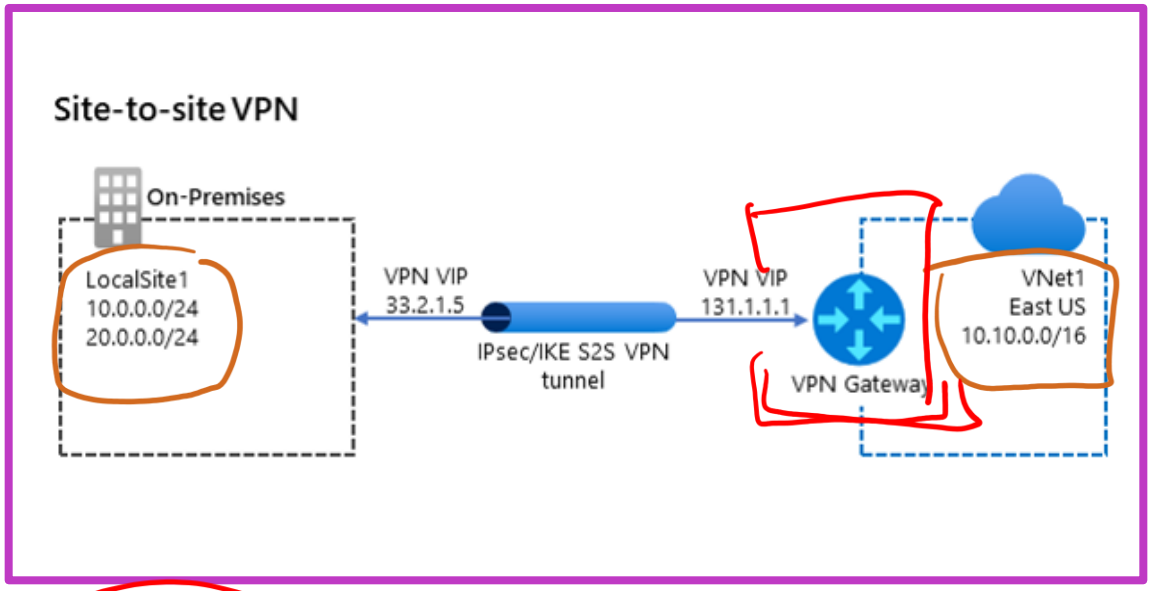
**ASG enables you to group network interfaces together. You can then use that ASG as a source or destination rule within an NSG.**

Without ASGs, you'd need to create a *separate rule for each* VM.

For example, Contoso has a number of front-end servers in a VNet. IT staff decide to implement NSGs and ASGs to secure the network resources.

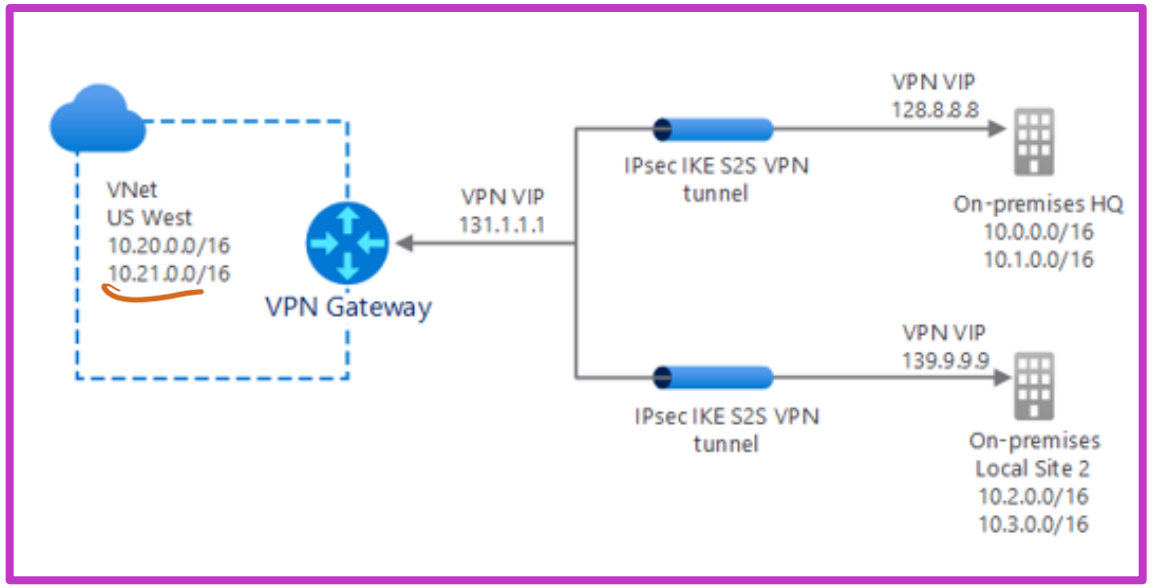


# Implement Azure VPN options (1 of 3)




## Site-to-site

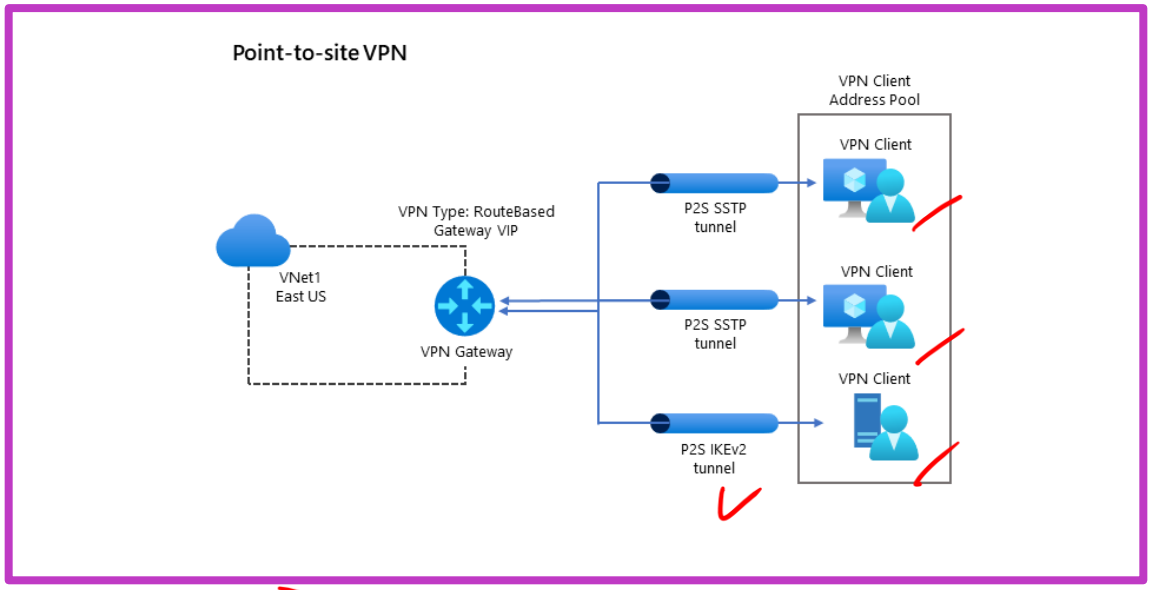
Site-to-Site VPN connecting on-premises to Azure




## Multi-site

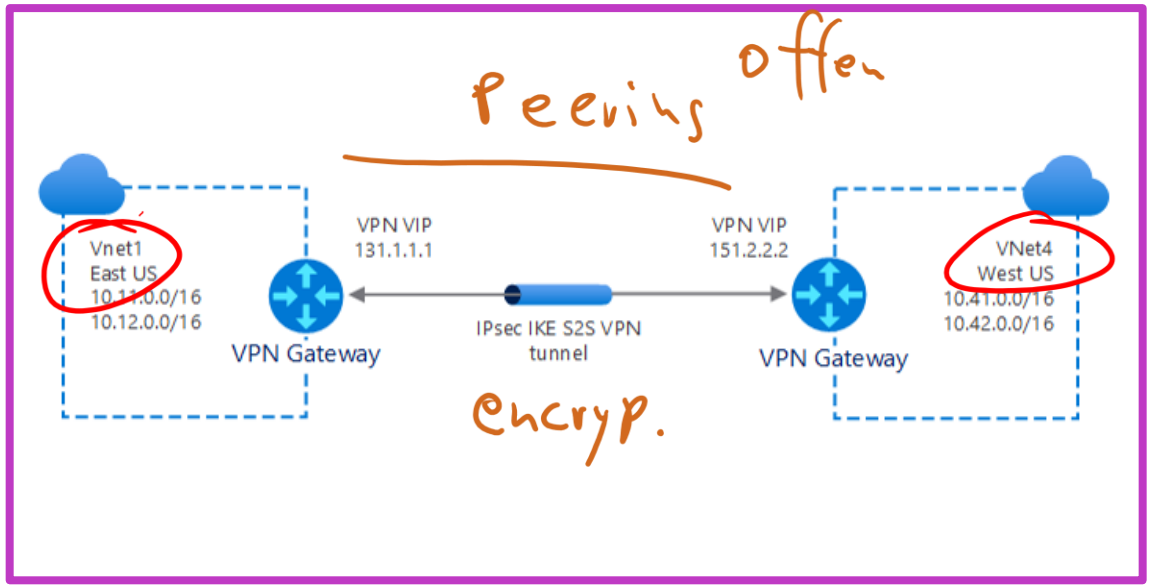
Multi-site VPN connecting multiple sites to Azure

# Implement Azure VPN options (2 of 3)




## Point-to-site

Point-to-Site VPN connecting single source to Azure




## VNet-to-VNet

VNet-VNet VPN connecting two VNets in Azure

# Implement Azure VPN options (3 of 3)

## Implement VPN gateway

- Policy-based
  - You must define sets of IP addresses that the gateway uses to determine packet destinations.
  - The gateway evaluates every packet against those sets of IP addresses to determine through which tunnel a packet is encrypted and routed.
- Route-based
  - Route-based gateways IP routing determines which one of your tunnel interfaces to send each packet.
  - They avoid the need to define which IP addresses are behind each tunnel.

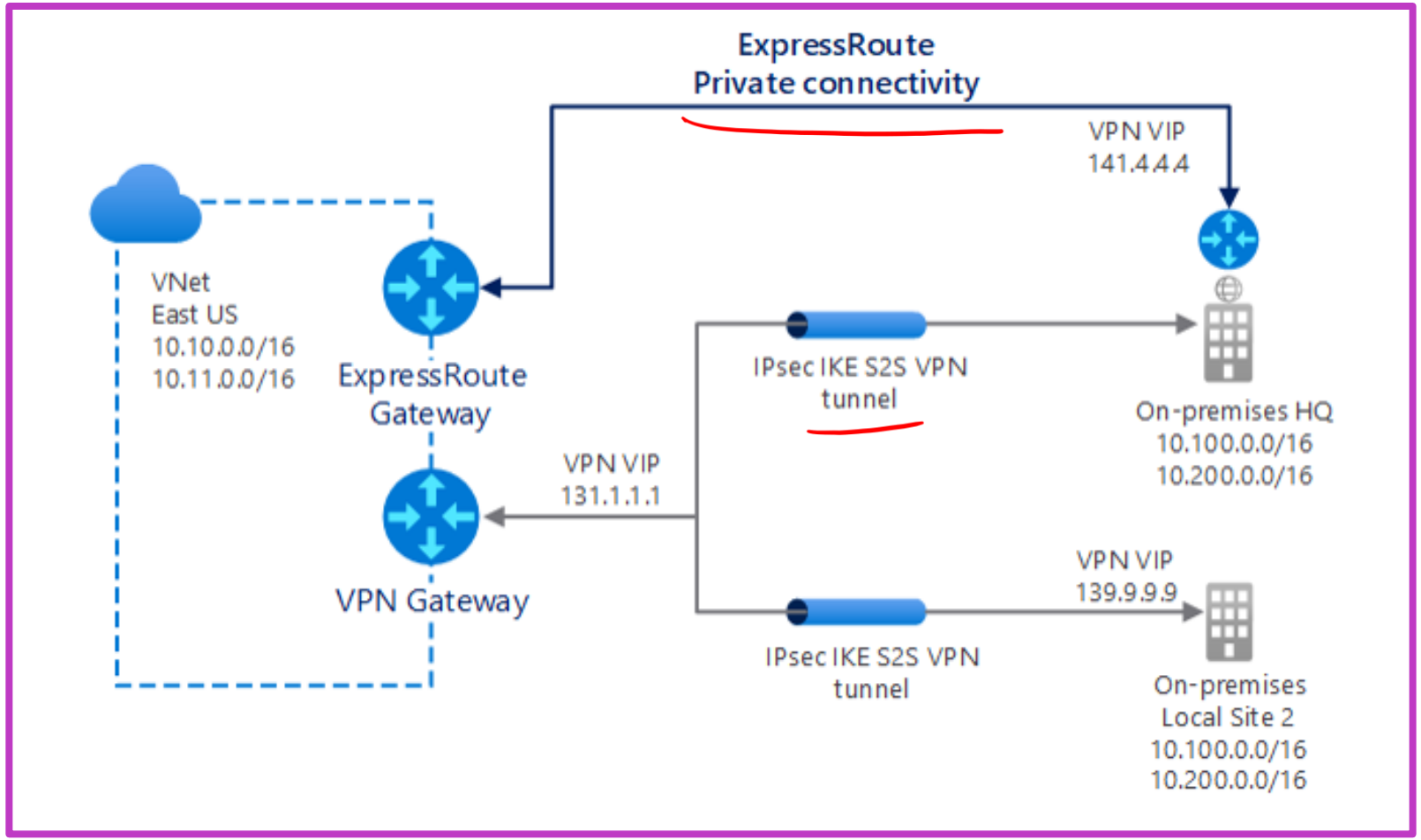
## Additional settings

- You must also define the following settings to implement VPN gateway
  - VPN or ExpressRoute. Choose the fundamental type of connection.
  - Gateway subnet address range. Specifies the private IP address range associated with the VPN gateway.
  - Public IP address. Specifies the public IP address object that gets associated with the VPN gateway.

# Implement Azure ExpressRoute (1 of 3)

## ExpressRoute connections

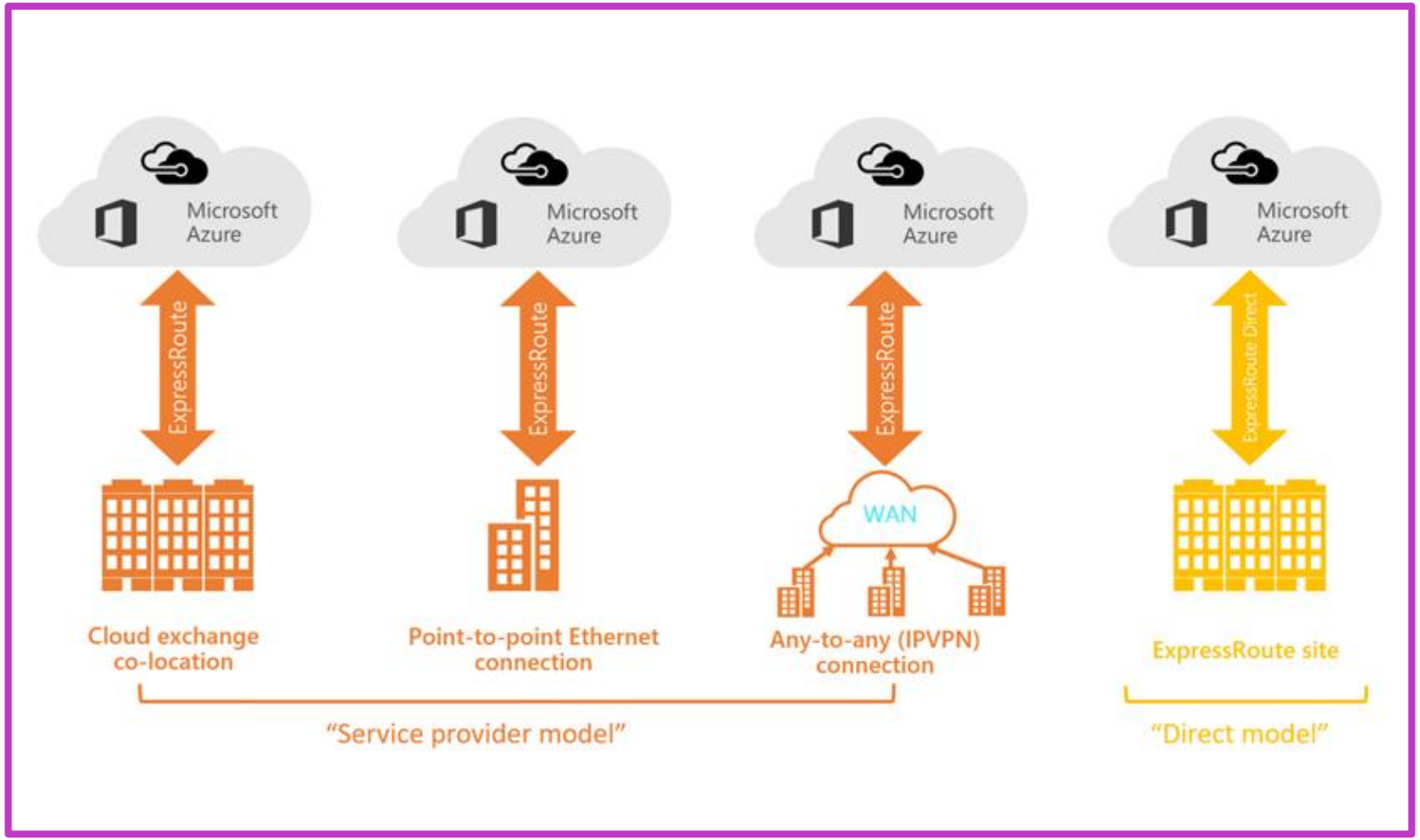
- You can use Azure ExpressRoute connections to facilitate a private connection from your on-premises networks to the Microsoft Cloud, or to other sites within your organization.
- You configure an ExpressRoute connection by using a VNet gateway.
- It's also possible to combine ExpressRoute and S2S connections.



# Implement Azure ExpressRoute (2 of 3)

**When implementing ExpressRoute, you can implement the following connection options:**

- CloudExchange co-location
- A P2P Ethernet connection
- An any-to-any (IPVPN) connection
- ExpressRoute Direct

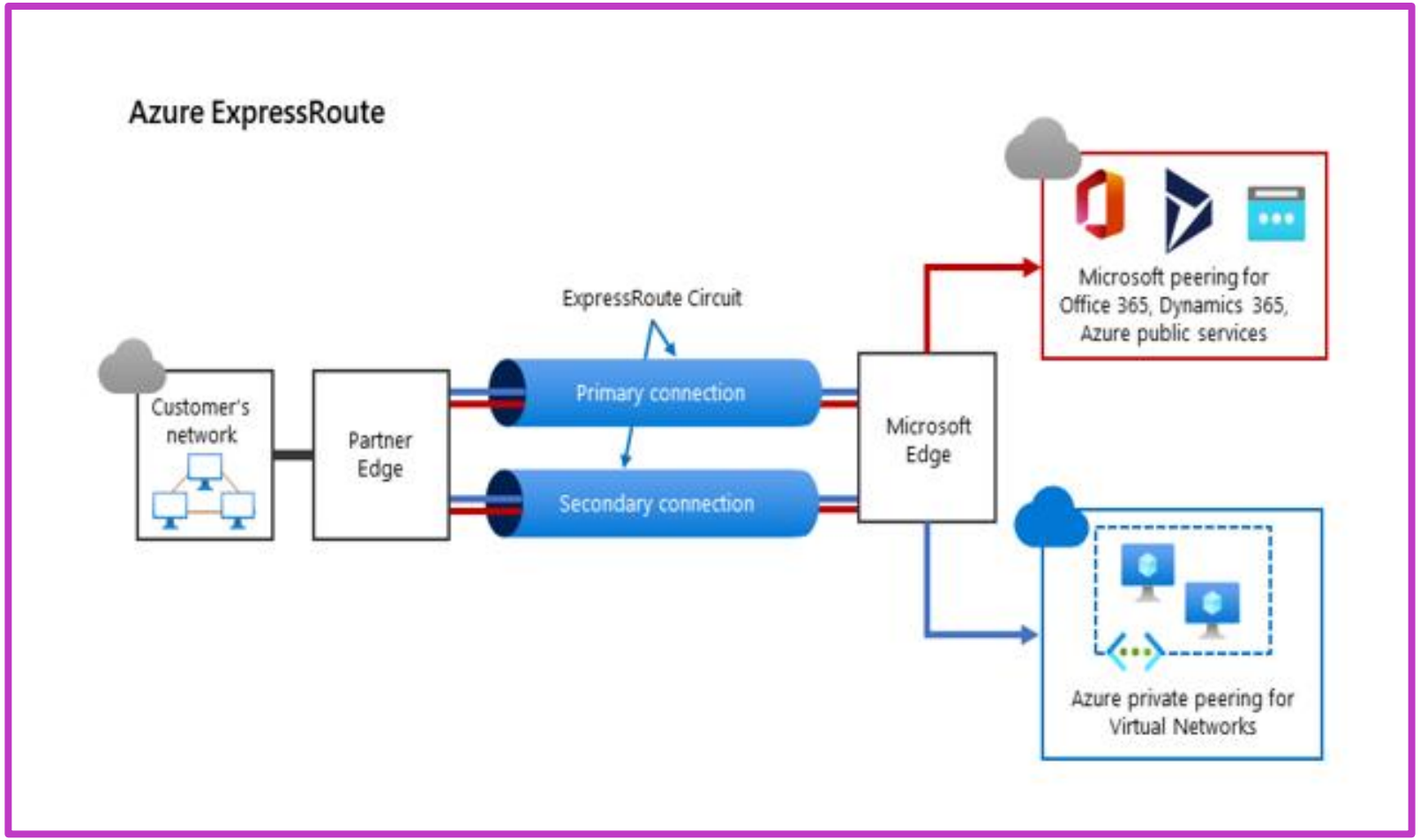


# Implement Azure ExpressRoute (3 of 3)

**To configure ExpressRoute, you must:**

- Create a circuit. (with the help of vendor)
- Create a peering connection
  - Configure private peering (Connects to Azure VNet)
  - Configure Microsoft peering

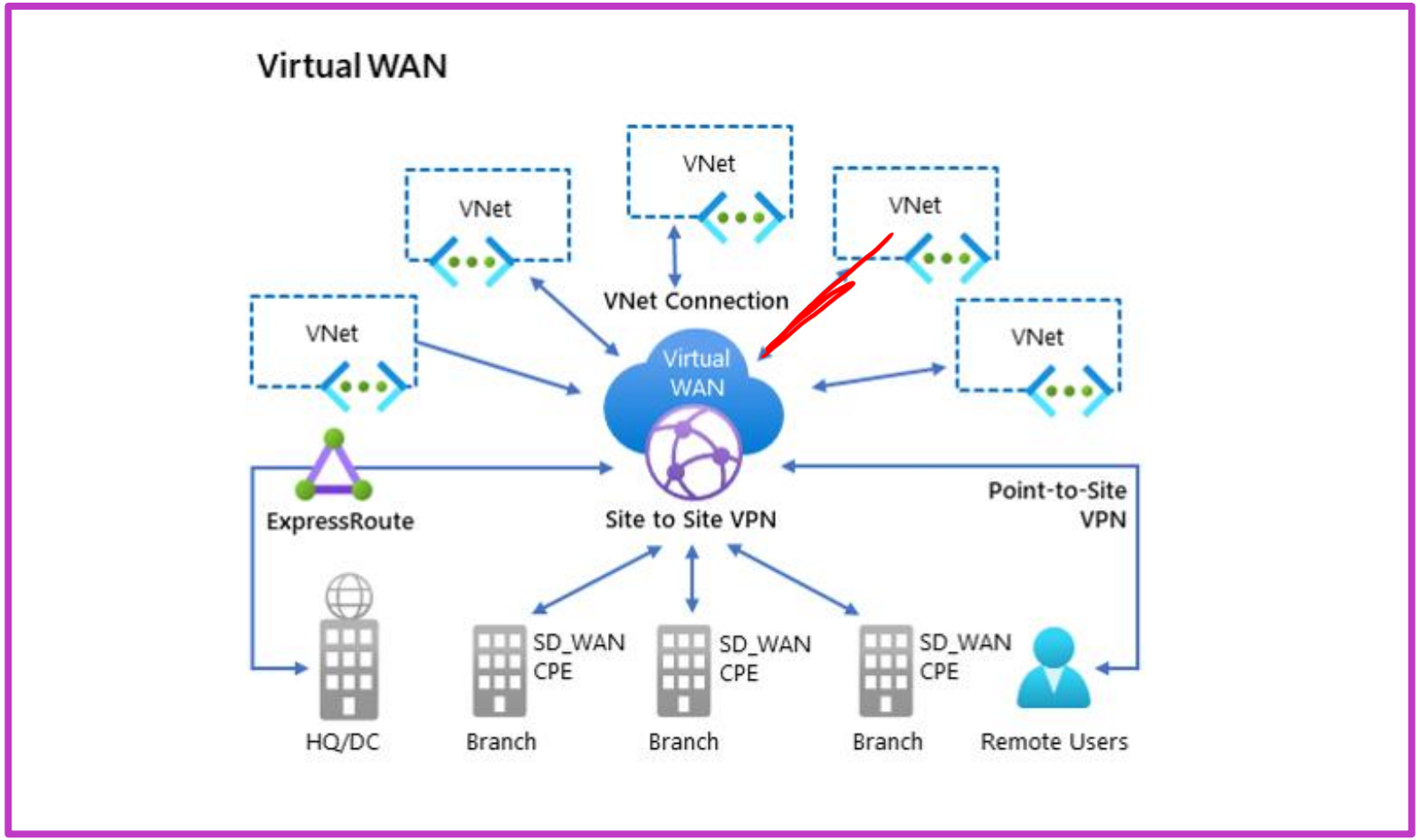
  (Connects to Microsoft SaaS applications)



# Configure Azure Virtual WAN

**To configure Azure WAN, create an S2S connection and complete the following high-level steps:**

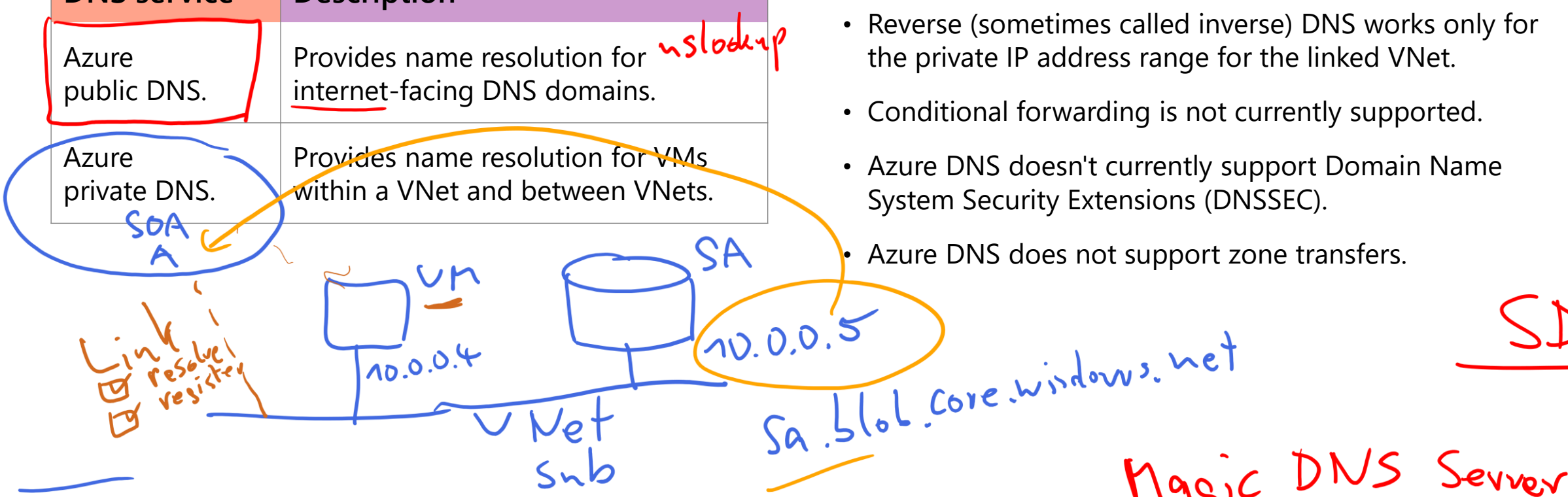
1. Create a virtual WAN.
2. Create a hub.
3. Create a site.
4. Connect a site to a hub.
5. Connect a VPN site to a hub.
6. Connect a VNet to a hub.
7. Download a configuration file.
8. Review your virtual WAN.



# Implement DNS in hybrid environments (1 of 2)

**There are two types of DNS services offered by Azure. Public DNS and Private DNS**

| DNS service | Description |
|---|---|
| Azure public DNS. | Provides name resolution for internet-facing DNS domains. |
| Azure private DNS. | Provides name resolution for VMs within a VNet and between VNets. |




**Limitations and considerations of Azure DNS:**

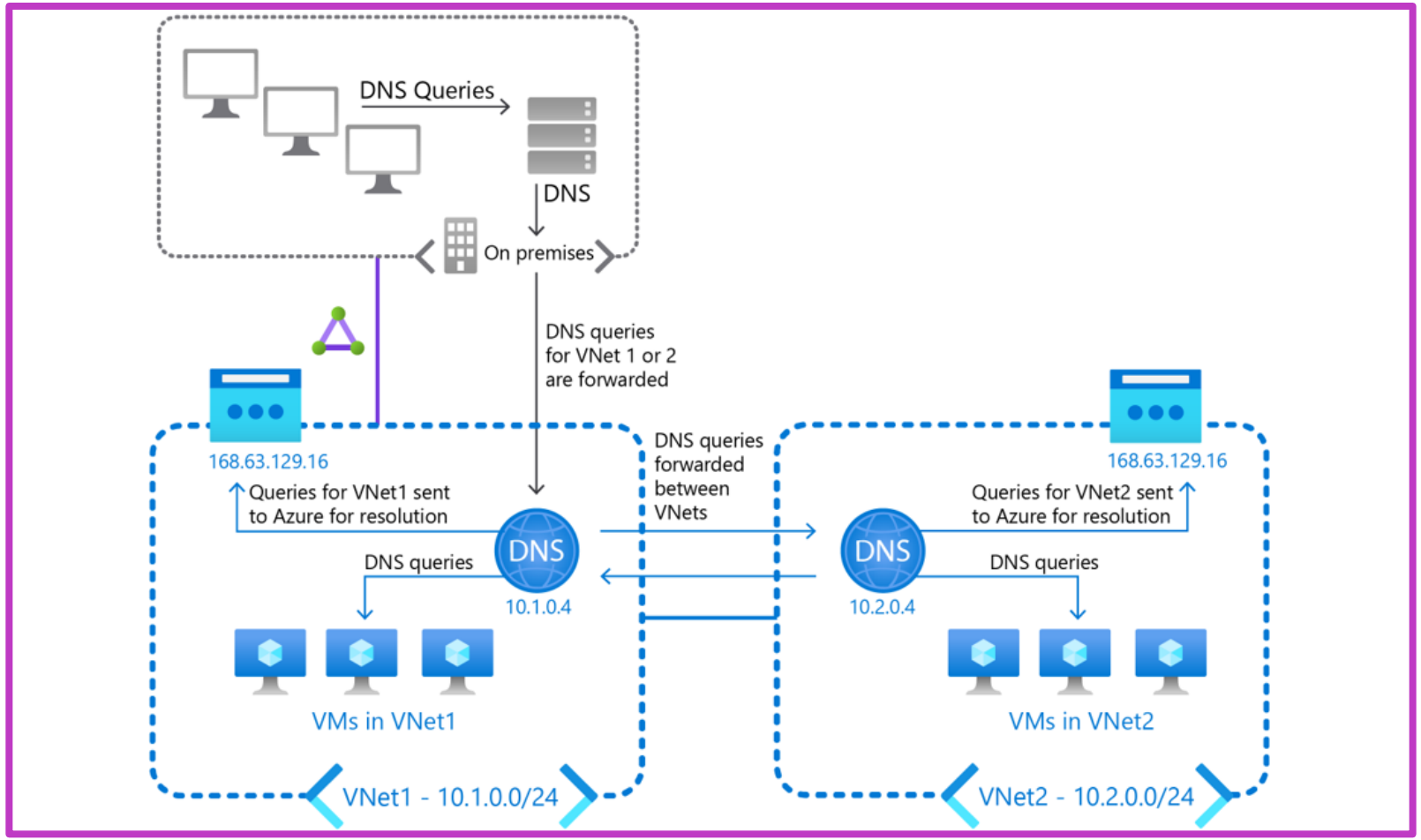
- You can only link a specific VNet to one private DNS zone.
- Reverse (sometimes called inverse) DNS works only for the private IP address range for the linked VNet.
- Conditional forwarding is not currently supported.
- Azure DNS doesn't currently support Domain Name System Security Extensions (DNSSEC).
- Azure DNS does not support zone transfers.

# Implement DNS in hybrid environments (2 of 2)

**On-premises DNS server can forward DNS lookups to Azure**

**You can use DNS forwarding to:**

- Enable DNS resolution between VNets.
- Enable your on-premises machines to resolve Azure-provided host names.



# Learning recap – Implement hybrid network infrastructure

## Module assessment

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

Implement hybrid network infrastructure

# Implement DNS for Windows Server IaaS VMs

# Learning Objectives – DNS for Windows Server IaaS VMs

- Describe Azure DNS
- Implement DNS in Azure
- Create and configure an Azure DNS zone
- Describe DNS options for Azure IaaS VMs
- Implement split-horizon DNS in Azure
- Troubleshoot DNS in Azure
- Learning recap

# Understand Azure DNS

## Azure DNS is an Azure service that provides name resolution for your Azure resources

## Azure DNS Service

- Azure public DNS
- Azure private DNS

## Features of Azure private DNS

- Automatic registration of VMs from a VNet that you link to a private zone
- Forward DNS resolution across VNets that you link to your private zone
- Reverse DNS lookup within the VNet scope

# Implement Azure DNS (1 of 2)

## Configure a public DNS zone

| | | |
|---|---|---|
| Create the public zone | Add records to the public zone | Test name resolution in the public zone |

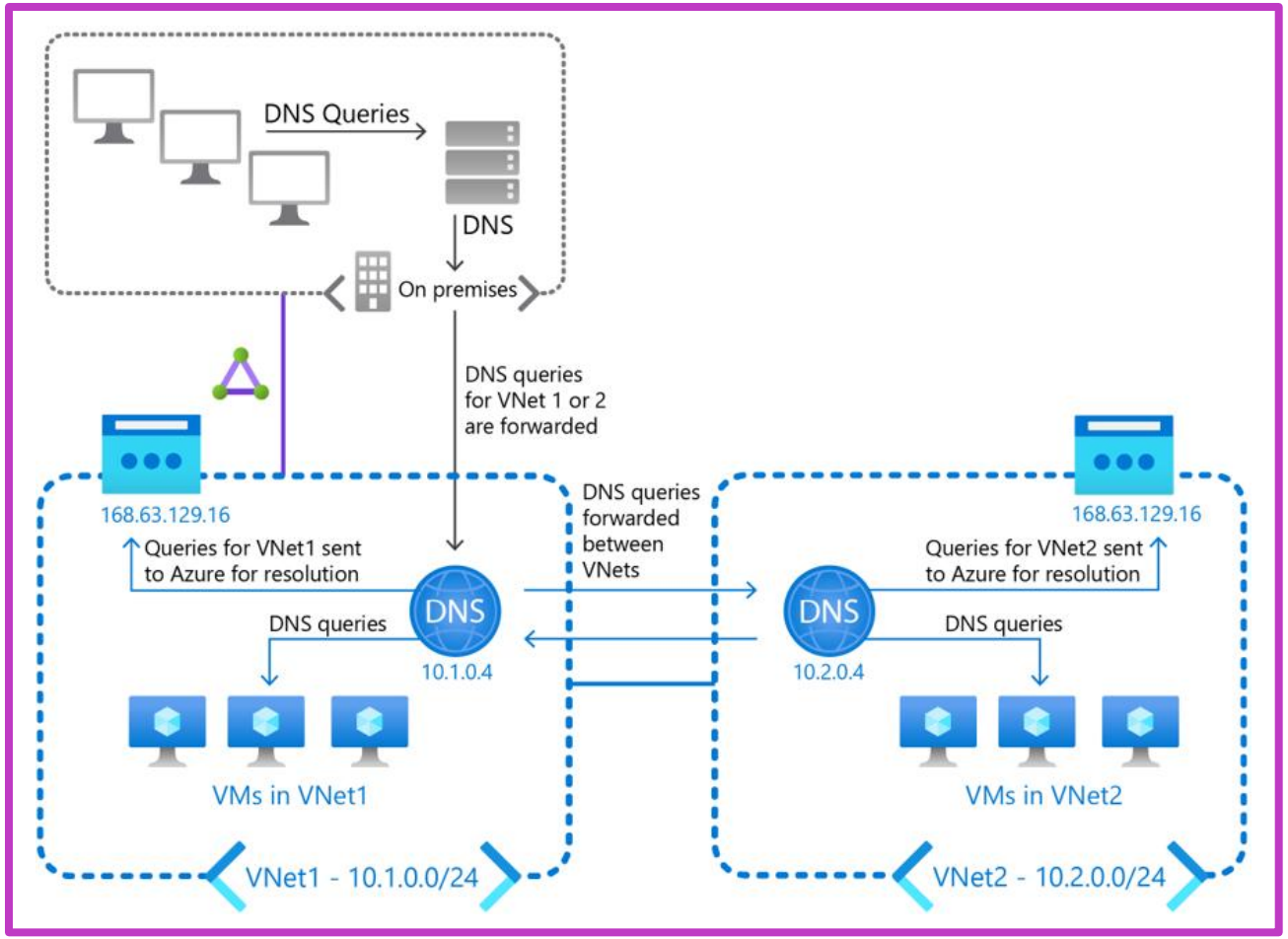
# Implement Azure DNS (2 of 2)

## Configure an Azure private DNS zone

| | | | |
|---|---|---|---|
| Create the private zone | Link VNets | Manage records | Test name resolution in the private zone |

# Implement DNS with Azure IaaS virtual machines

- Windows Server DNS servers that are attached to a VNet can forward DNS queries to the recursive resolvers in Azure.
- You can use DNS forwarding to:
  - Enable DNS resolution between VNets.
  - Enable your on-premises machines to resolve Azure-provided hostnames.
- To resolve a VM's host name, your DNS server VM must meet the following requirements:
  - It must reside in the same VNet as the VM.
  - It must be configured to forward host name queries to Azure.



# Implement split-horizon DNS in Azure

**The private zone for Contoso.com would contain the information in the following table.**

| Host | Record type | IP address |
|---|---|---|
| www | CNAME | Webserver1.<br>contoso.com |
| Relay | CNAME | Exchange1.<br>contoso.com |
| Webserver1 | A | 192.168.1.200 |
| Exchange1 | A | 192.168.1.201 |

**The public zone for Contoso.com would contain the information in the following table.**

| Host | Record type | IP address |
|---|---|---|
| www | A | 131.107.1.200 |
| Relay | A | 131.107.1.201 |
| | MX | Relay.contoso.com |

# Troubleshoot DNS (1 of 3)

**If you experience problems administering Azure DNS, review the following table for guidance on how to proceed.**

| Problem | What to check |
| --- | --- |
| You can't create a DNS zone | 1. Review Azure DNS audit logs.<br>2. Ensure each DNS zone name must be named uniquely.<br>3. If you receive the error, "You have reached or exceeded the maximum number of zones in subscription {subscription id}", use another Azure subscription or delete zones.<br>4. You can also contact Azure Support to increase your zone subscription limit. If you get the error The zone '{zone name}' is not available, try using a different zone name. |
| You can't create a DNS record | 1. Review Azure DNS audit logs.<br>2. Verify for duplicate records.<br>3. Verify that you are not attempting to create a record set at the zone root; if you are, use the @ character as a prefix. Ensure you do not have an alias (CNAME) conflict.<br>4. Check whether you have reached the limit on the record set number permitted in your DNS zone. If you have, then either delete some record sets or contact Azure Support to increase the limit. |
| You can't resolve a DNS record | 1. Verify that the queried records are correct.<br>2. Make sure that the records are correct in Azure DNS. Verify that the petitioned records can be resolved on the Azure DNS name servers. If you're using a local computer to perform the query, check the DNS name cache. If necessary, empty this cache and try again. |

# Troubleshoot DNS (2 of 3)

**The command-line tools and procedures for troubleshooting name resolution and configuration issues are described in the following table.**

| Tool | Description |
|---|---|
| NSLookup | Use to query DNS information. This tool is flexible and can provide valuable information about DNS server status. You also can use it to lookup resource records and validate their configuration. Additionally, you can test zone transfers, security options, and MX record resolution. |
| DNSCmd | Use to manage the DNS server role. This command-line tool is useful in scripting batch files to help automate routine DNS management tasks or to perform simple unattended setup and configuration of new DNS servers on your network. |
| IPConfig | Use to review IP configuration details that the computer uses. This command includes additional command-line options that you can use to troubleshoot and support DNS clients. |
| Monitoring on DNS server | Perform simple local queries and recursive queries from the Monitoring tab in the DNS Server Properties dialog box to test whether the server can communicate with upstream servers. You also can schedule these tests to occur at regular intervals. |

# Troubleshoot DNS (3 of 3)

**If you cannot connect to a remote host and suspect a name resolution problem, troubleshoot the name resolution by performing the following steps:**

1. Open an elevated command prompt, and then clear the DNS resolver cache by entering the following command at a command prompt: **`ipconfig /flushdns`**
2. Attempt to ping the remote host by its IP address. This helps identify whether the issue is related to name resolution. If the ping succeeds by using the IP address but fails by using its host name, then the problem is related to name resolution
3. Attempt to ping the remote host by using its host name. For example, at Contoso, you would enter the following command at a command prompt: **`Ping LON-DC1.contoso.com`**
4. At the command prompt, enter the following command, and then select Enter: **`NSLookup.exe -d2 LON-DC1.contoso.com. > filename.txt`**
5. Examine the contents of the filename.txt file to identify the failed stage in name resolution

# Learning recap – Implement DNS for Windows Server IaaS VMs

## Module assessment

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

Implement DNS for Windows Server IaaS VMs

# Implement Windows Server IaaS VM IP addressing and routing

# Learning Objectives – VM IP addressing and routing

- Implement an Azure VNET
- Implement IP address allocation in Azure
- Assign and manage IP addresses
- Configure a private IP address for an Azure VM
- Create a VM with a static IP address
- Implement IaaS VM IP routing
- Implement IPv6 for Windows Server IaaS VMs
- Learning recap

# Implement a virtual network

## Azure VNets

- By placing a VM on the same VNet as other VMs, you effectively provide direct IP connectivity among them within the same private IP address space.
- You can also connect different VNets together.
- It is possible to connect VNets in Azure to your on-premises networks.
- An Azure VNet constitutes a logical boundary defined by a private IP address space of your choice.

## Azure VM network interface

- A network interface is the interconnection between a VM and a VNet.
- You can create a VM with multiple network interfaces and add or remove network interfaces through the lifecycle of a VM.
- Multiple network interfaces allow a VM to connect to different subnets in the same VNet and send or receive traffic over the most appropriate interface.
- VMs with any number of network interfaces can exist in the same availability set, up to the number supported by the VM size.

# Implement IaaS VM IP addressing

## Private IP addressing

- You use private IP addresses to communicate between resources in Azure.
- You assign a static private IP address when you create the Azure VM or at any point after.
- There are two ways in which Azure assigns private IP addresses: Dynamic and Static.
- You can configure custom DNS settings for your VMs.
- You can assign private IP addresses to the front-end configuration of both internal load balancers and application gateways.
- You can assign either a dynamic or static IP to these resources as well.

## Public IP addressing

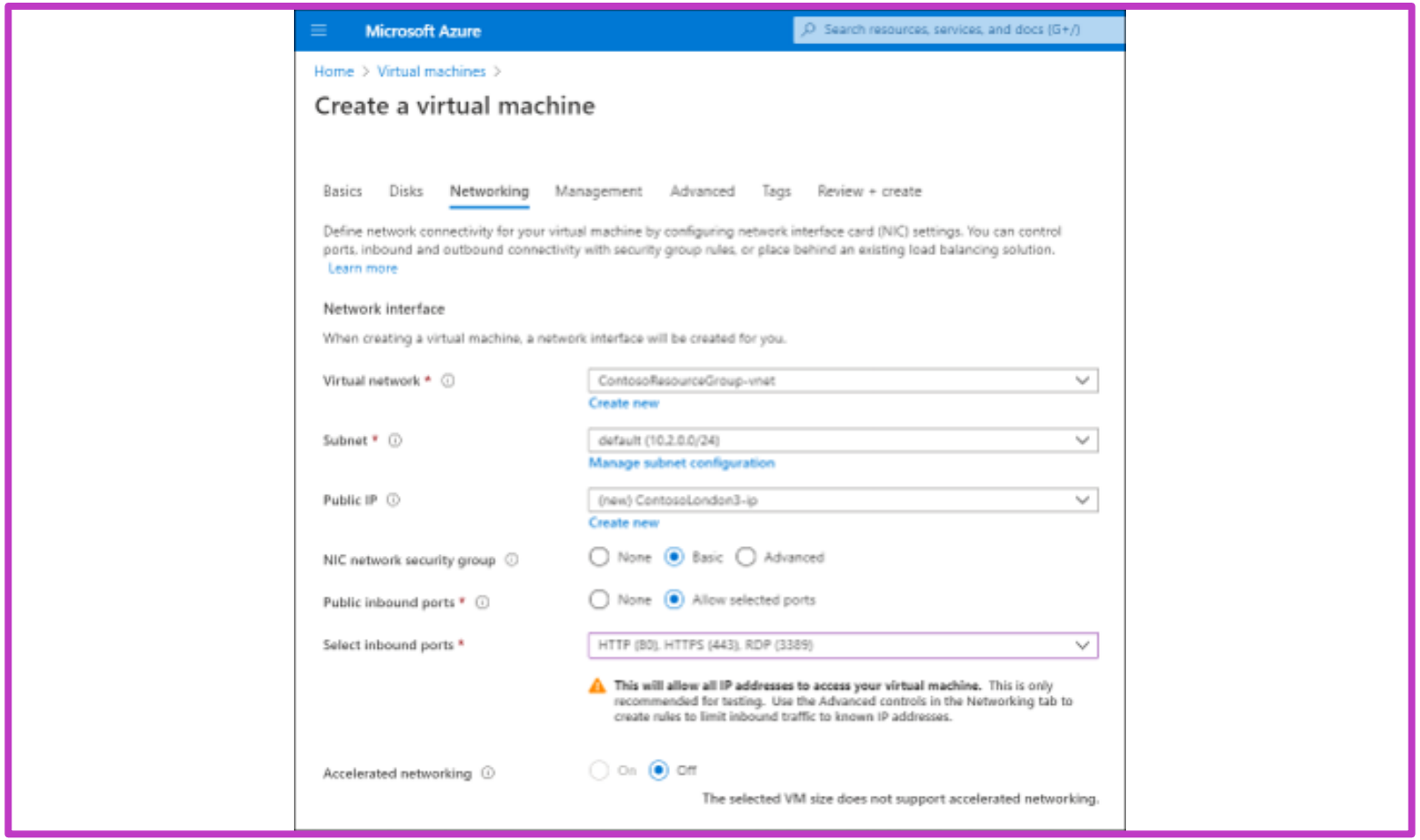
- You can assign a public IP address to the following:
  - VM network interfaces
  - Internet-facing load balancers
  - VPN gateways
  - Application gateways
  - Azure Firewall
- Public IP addresses are available in two stock keeping units (SKUs):
  - Basic
  - Standard

# Assign and Manage IP addresses (1 of 2)

## Assign an IP configuration during VM creation

You can review the following settings if you want to reconfigure the VM's network setting:

- IP configuration (NIC Private IP and link to NIC Public IP)
- Network Interface
- VNet/subnet
- NIC Public IP
- NIC Private IP
- Inbound port rules
- Outbound port rules
- Application security groups
- Load balancing

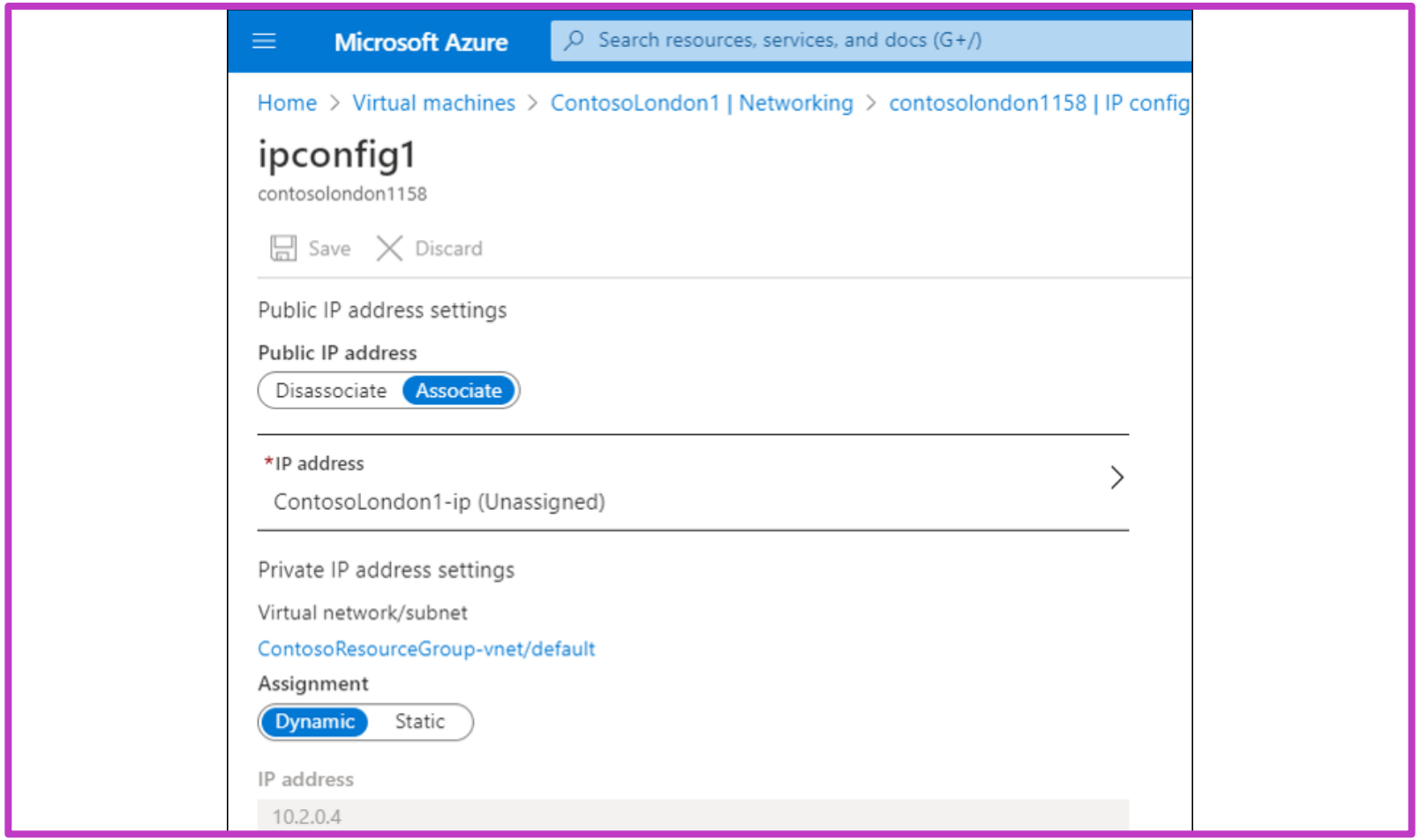


# Assign and Manage IP addresses (2 of 2)

## Manage VM IP addresses

Some steps to review or edit the private IP configuration for a VM:

1. Navigate to Virtual machines, and then select the appropriate VM
2. Select the appropriate network interface
3. Select IP configurations
4. Under the IP configurations table, select the listed entry
5. On the Choose public IP address page, select Create new
6. Enter a new name, choose the SKU and Assignment methods, and then select OK
7. Make any changes, and then select Save



# Demonstration – Configure a Private IP address for a virtual machine

Create a VNet

Create a VM for testing static private IP addresses

Retrieve private IP address information for a VM

Add a static private IP address to an existing VM

# Demonstration – Create a virtual machine with a static public IP address

Create and configure a new VM

Add a static public IP address

Review newly configured IP address and its associated VM

# Implement IaaS virtual machine IP routing

## System routes

- When you create a VNet, Azure automatically creates several default routes also called “system routes”
- Next hop type
  - Virtual network
  - Internet
  - None
- Azure creates additional default routes if you add specific Azure capabilities
- Next hop type
  - VNet peering
  - Virtual network gateway
  - VirtualNetworkServiceEndpoint

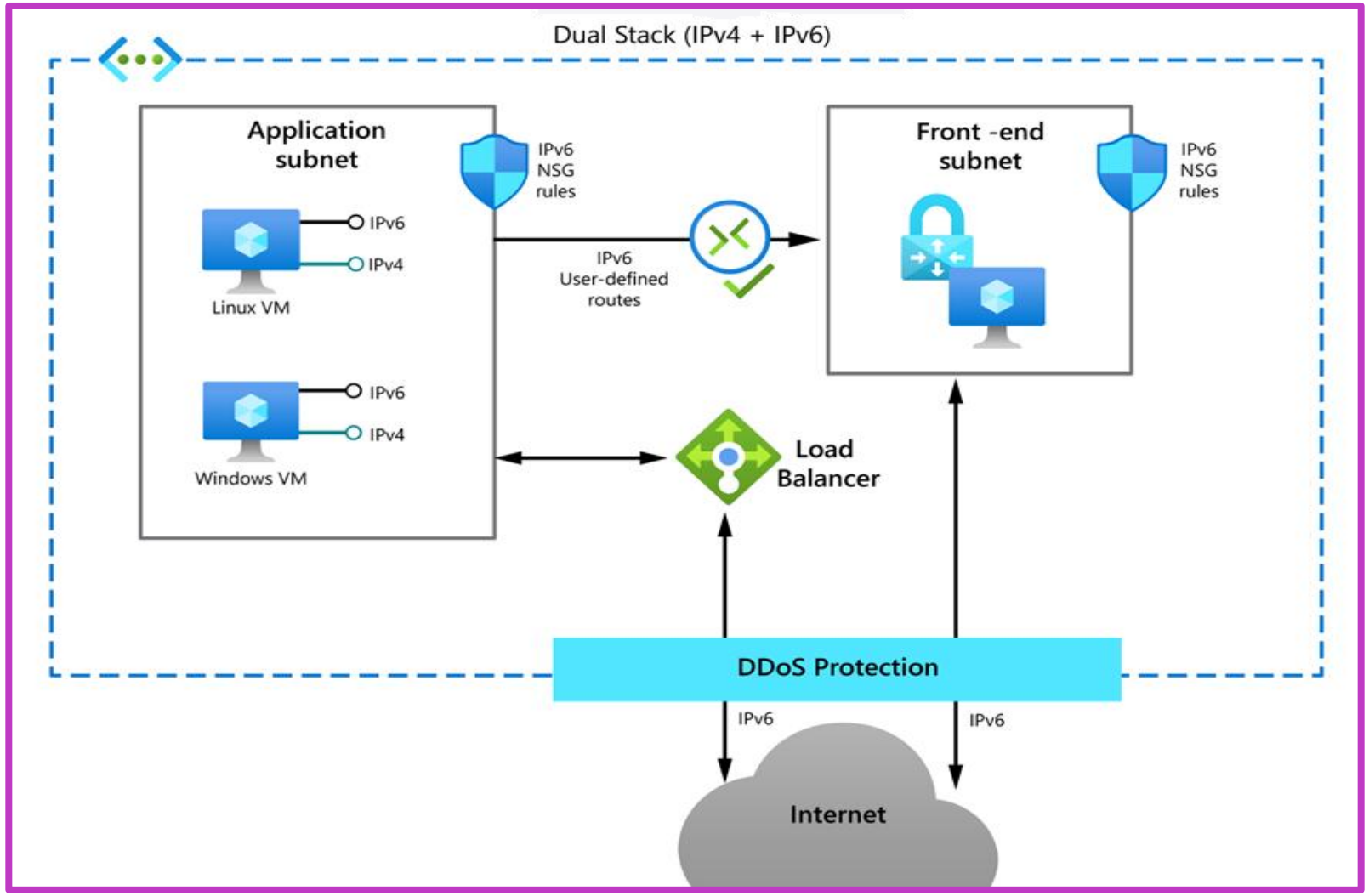
## Custom routes

- You can create either user-defined custom routes in Azure or generate custom routes by exchanging BGP routes with your on-premises network infrastructure and an Azure VNet gateway
- User-defined
  - You can create user-defined custom routes in Azure to override Azure's default system routes
- Next hop type
  - Virtual appliance
  - Virtual network gateway
  - None
  - VNet
  - Internet

# Implement IPv6 for Windows Server IaaS virtual machines (1 of 2)

### What is IPv6 for Azure VNet?

- You can use IPv6 for Azure VNet to host applications in Azure that require both IPv6 and IPv4 connectivity within a virtual network and to and from the internet.
- Azure's dual stack IPv4/IPv6 connectivity enables your hosted apps to communicate in both the IPv4 and IPv6 internet.

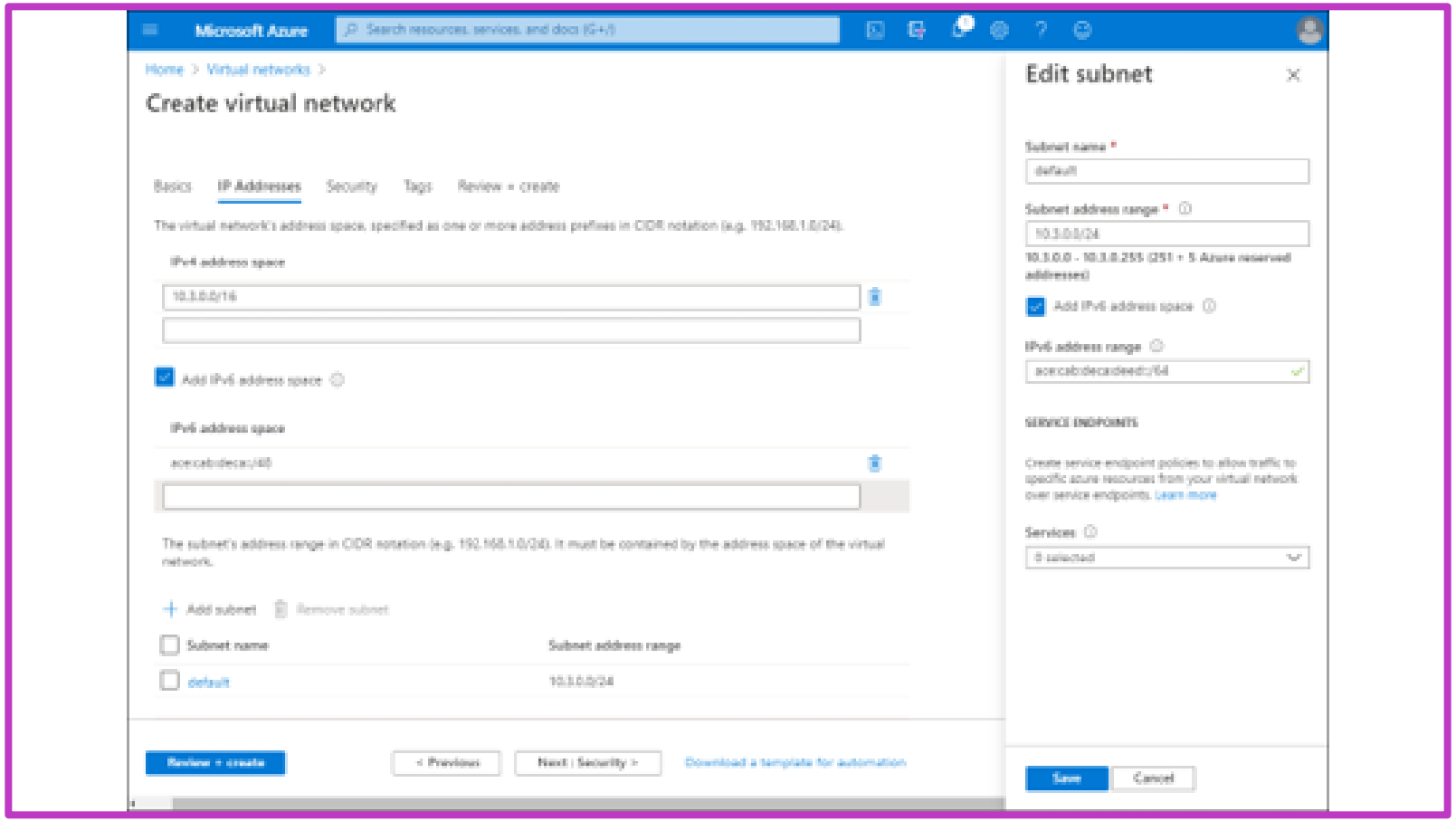


# Implement IPv6 for Windows Server IaaS virtual machines (2 of 2)

## Create a dual-stack VNet

Perform following procedure to create a dual-stack VNet:

- In the Azure portal, select Virtual networks, and then select Add.
- Enter the basic information on the Basics page, and then select Next: IP Addresses.
- On the IP Addresses page, select the Add IPv6 address space check box.
- Select the subnet that displays, and on the Edit subnet blade, select the Add IPv6 address space check box.
- Enter an IPv6 address, and then select Save.
- Select Review + Create, and then select Create.



# Learning recap – Implement Windows Server IaaS VM IP addressing and routing

## Module assessment

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

Implement Windows Server IaaS VM IP addressing and routing

# Lab 08 – Implement hybrid networking infrastructure

# Lab 08: Implementing hybrid networking infrastructure

## Lab scenario

You are tasked with building a test environment in Azure, consisting of Microsoft Azure virtual machines deployed into separate virtual networks configured in the hub and spoke topology. This testing must include implementing connectivity between spokes by using user-defined routes that force traffic to flow via the hub. You also need to implement DNS name resolution for Azure virtual machines between virtual networks by using Azure private DNS zones and evaluate the use of Azure DNS zones for external name resolution.

## Objectives

- Implement virtual network routing in Azure.
- Implement DNS name resolution in Azure.

# End of presentation