



AZ-700

## Module 01

# Introduction to Azure Virtual Networks



# AZ-700 Agenda

Module 01: Introduction to Azure Virtual Networks 

Module 02: Designing and Implementing Hybrid Networking

Module 03: Designing and Implementing Azure ExpressRoute

Module 04: Load balance non-HTTP(S) traffic in Azure

Module 05: Load balance HTTP(S) traffic in Azure

Module 06: Design and Implement Network Security

Module 07: Design and Implement private access to Azure Services

Module 08: Design and Implement Network Monitoring

# Module Overview

- Explore Azure Virtual Networks
- Configure Public IP addresses
- Design name resolution for your Virtual Network
- Enable Cross-VNet connectivity with peering
- Implement virtual network traffic routing
- Configure internet access with Azure Virtual NAT

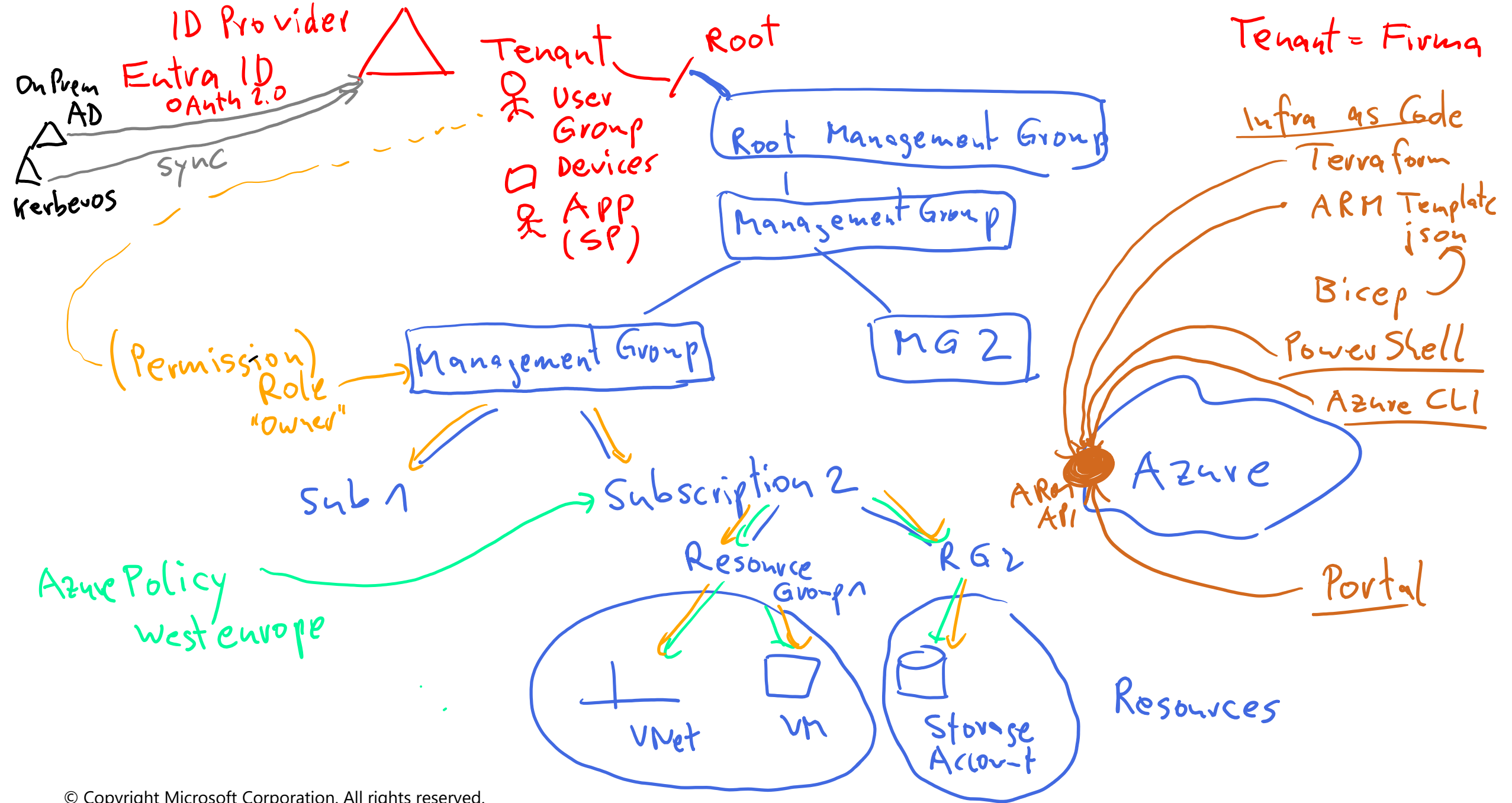
DNS

route add /p --- --

# Explore Azure Virtual Networks







# Capabilities of Azure Virtual Networks

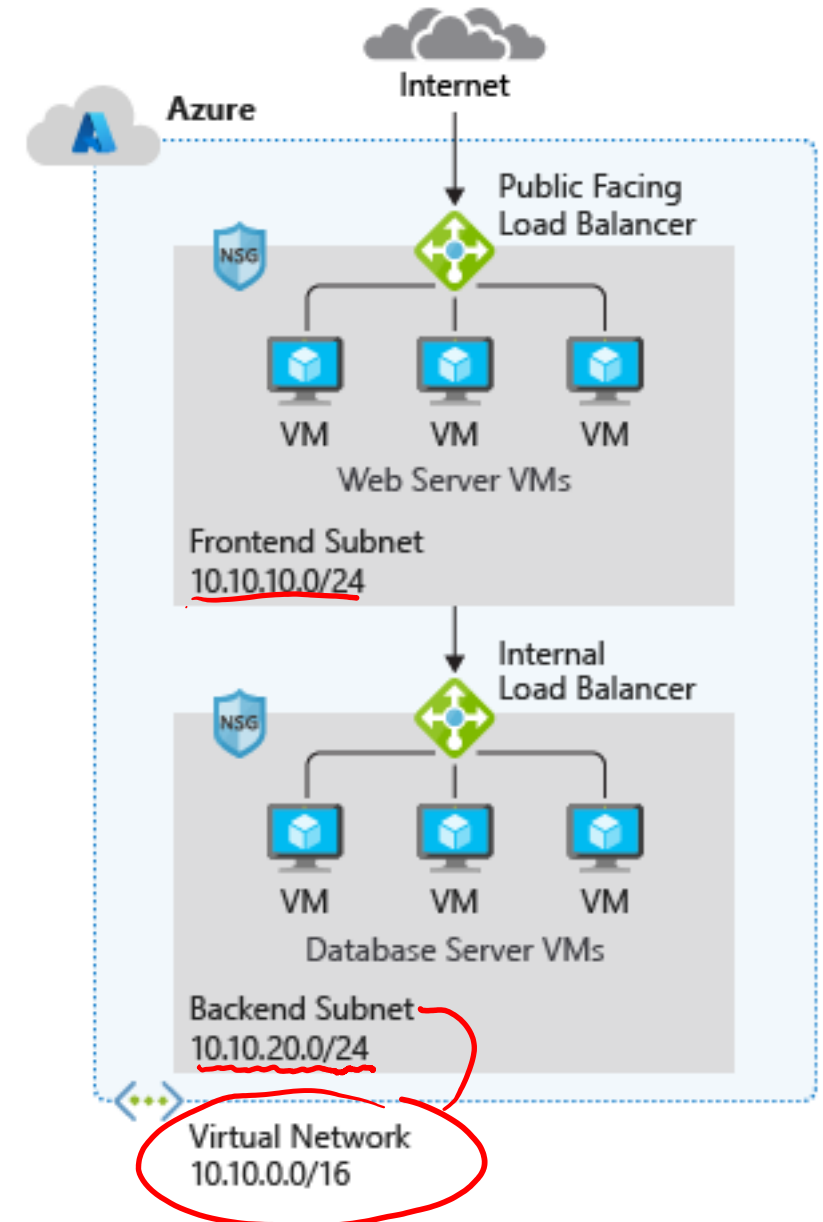
SDN

~~DHCP~~

- Communication with the Internet
- Communication between Azure resources
- Communication between on-premises resources
- Filtering network traffic
- Routing network traffic

IP

IP v 6



# Virtual Network address space

private

## RFC 1918

10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

### Azure reserves 5 IP addresses

- x.x.x.0: Network address
- x.x.x.1: Reserved by Azure for the default gateway
- x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
- x.x.x.255: Network broadcast address

### Unavailable address ranges:

- 224.0.0.0/4 (Multicast)
- 255.255.255.255/32 (Broadcast)
- 127.0.0.0/8 (Loopback)
- 169.254.0.0/16 (Link-local)
- 168.63.129.16/32 (Internal DNS)

100.64.0.0/10

Logical representation  
of your own network

Create a dedicated  
private cloud-only  
virtual network

Securely extend  
your datacenter with  
virtual networks

Enable hybrid  
cloud scenarios



# Subnets

+

 Subnet

+

 Gateway subnet

↺

 Refresh

👤

 Manage users

🗑

 Delete

🔍

 Search subnets

A virtual network can be segmented into one or more subnets

Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

Each subnet must have a unique address range – cannot overlap with other subnets in the virtual network in the subscription

# Private IP Addresses allocation

Private IP Addresses	IP address association
Virtual Machine	NIC
Internal Load Balancer	Front-end configuration
Application Gateway	Front-end configuration

**Dynamic (default).** Azure assigns the next available unassigned or unreserved IP address in the subnet's address range

~~DHCP~~

**Static.** You select and assign any unassigned or unreserved IP address in the subnet's address range

# Understand Regions and Subscriptions

**Regions:** VNet is scoped to a single region/location; however, multiple virtual networks from different regions can be connected using Virtual Network Peering.



# Create a Virtual Network

Create new virtual networks at any time

Add virtual networks when you create a virtual machine

Need to define the address space, and at least one subnet

Ensure non-overlapping address spaces

## Create virtual network

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

### Project details

Subscription \*

Visual Studio Enterprise

Resource group \*

Lab04

Create new

### Instance details

Name \*

VNet2

Region \*

(US) East US 2

# Configure Public IP addresses



# Public IP Addresses

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes (non-AZ only)	Yes
Application Gateway	Front-end configuration	Yes (V1 only)	Yes (V2 only)
Azure Firewall	Front-end configuration	No	Yes
NAT gateway	Gateway IP configuration	No	Yes

A public IP address resource can be associated with resources such as virtual machine network interfaces, internet-facing load balancers, VPN gateways, and Application Gateways

# Choose the appropriate **SKU** for a public IP

NSG — Subnet  
NIC

## Basic SKU

- Assigned with the static or dynamic allocation method
- Open by default. NSGs are recommended but optional
- Assigned to network interfaces, VPN gateway, public load balancers, or Application Gateways
- Don't support availability zone scenarios

## Standard SKU

- Always use static allocation method
- Secure by default and closed to inbound traffic
- Allow inbound traffic with NSG
- Assigned to network interfaces, standard public load balancers, or Application Gateways
- Can be zone-redundant, zonal, or no-zone

# Creating Public IP Addresses

Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Regional vs Global

Dynamic vs Static

Range of contiguous addresses available as a prefix

IP Version \* ⓘ

☒ IPv4 ☐ IPv6 ☐ Both

SKU \* ⓘ

☒ Standard ☐ Basic

Tier

☒ Regional ☐ Global

IPv4 IP Address Configuration

Name \*

IP address assignment

☐ Dynamic ☒ Static

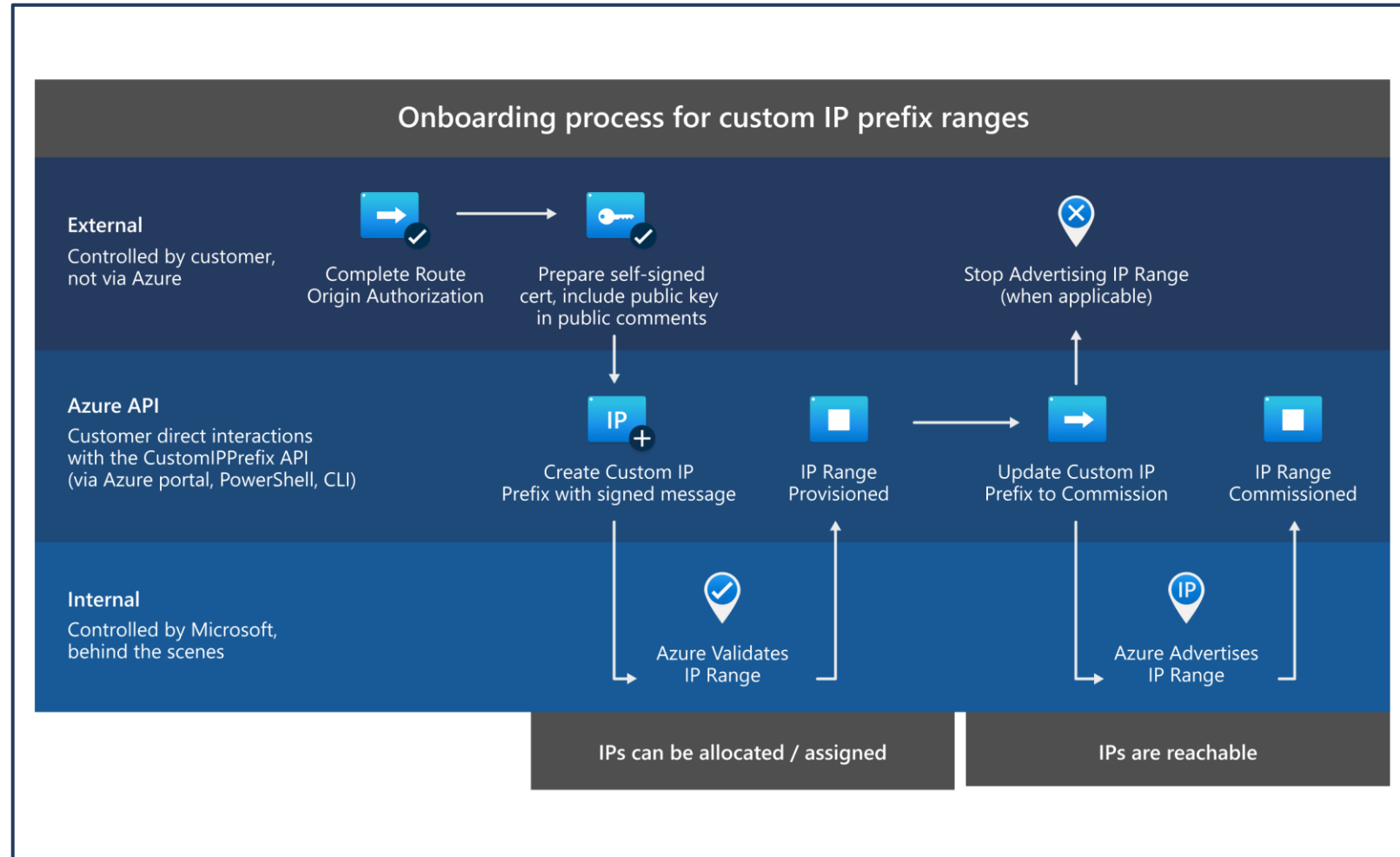


# Custom IP address prefix (Bring your own IP)

Retain IP ranges (BYOIP) to maintain established reputation and continue to pass through externally controlled allowlists.

Three phase process to bring an IP prefix to Azure:

- Validation
- Provision
- Commission



# Design Name Resolution for Azure Virtual Network



# Public DNS

Denic  
Nicat

Public DNS services resolve names and IP addresses for resources and services accessible over the internet such as web servers. Azure DNS is a hosting service for DNS domain that provides name resolution by using Microsoft Azure infrastructure

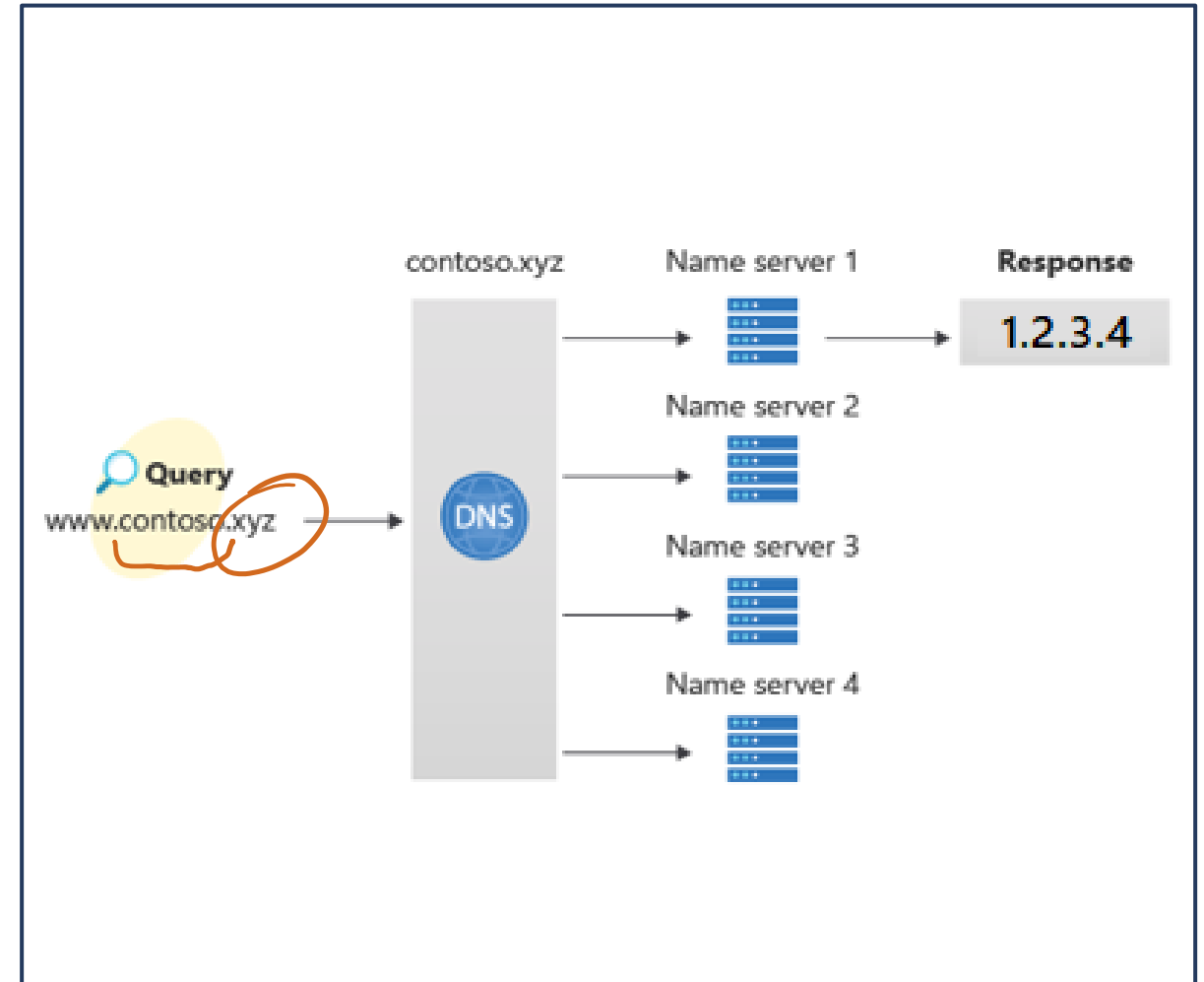
In Azure DNS, you can create address records manually within relevant zones. The records most frequently used will be:

- Host records: A/AAAA (IPv4/IPv6)
- Alias records: CNAME

32 Bit 128 Bit

Vint Cerf  
1969

TCP/IP



# Azure DNS Zones

A DNS zone hosts the DNS records for a domain

The same zone name can be reused in a different resource group or a different Azure subscription

Where multiple zones share the same name, each instance is assigned different name server addresses

Root/Parent domain is registered at the registrar and pointed to Azure NS

## Create DNS zone *public*

Basics Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more.](#)

Project details

Subscription \* MSDN Platforms Subscription

Resource group \* rg-dns [Create new](#)

Instance details

Name \* azureadmininc.org

Resource group location ⓘ East US

Review + create

Previous

Next : Tags >

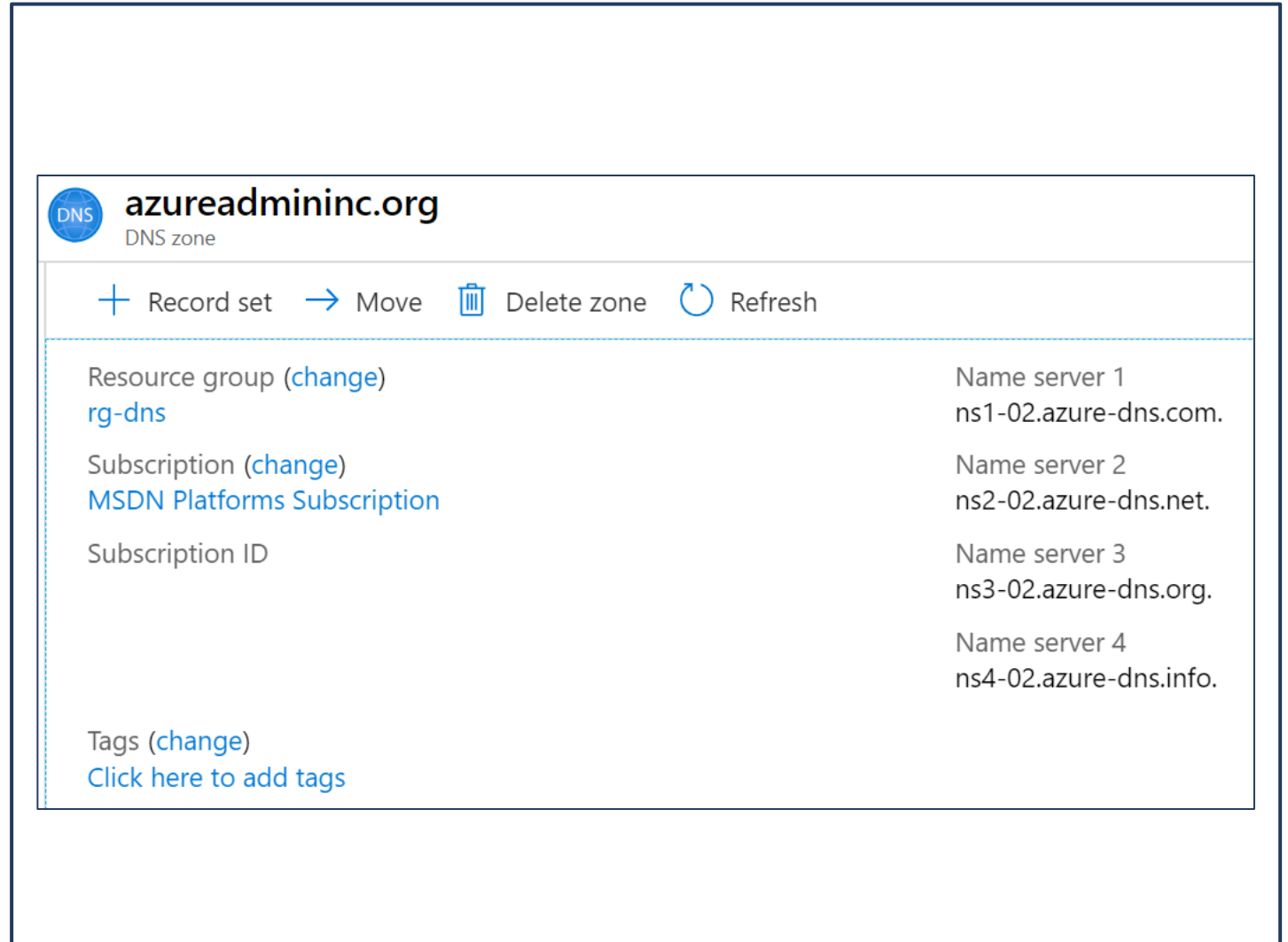
[Download a template for automation](#)

# DNS Delegation

When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four

Once the DNS zone is created, update the parent registrar

For child zones, register the NS records in the parent domain



The screenshot displays the Azure portal interface for a DNS zone named **azureadmininc.org**. The interface includes a header with the DNS icon and the zone name, followed by a toolbar with actions: **+ Record set**, **→ Move**, **🗑️ Delete zone**, and **🔄 Refresh**. The main content area is divided into two columns. The left column lists configuration details: **Resource group** (with a [change](#) link) set to **rg-dns**, **Subscription** (with a [change](#) link) set to **MSDN Platforms Subscription**, and **Subscription ID**. The right column lists the four required name servers: **Name server 1** (**ns1-02.azure-dns.com.**), **Name server 2** (**ns2-02.azure-dns.net.**), **Name server 3** (**ns3-02.azure-dns.org.**), and **Name server 4** (**ns4-02.azure-dns.info.**). At the bottom left, there is a **Tags** section (with a [change](#) link) and a [Click here to add tags](#) link.

azureadmininc.org DNS zone	
<b>+ Record set</b> <b>→ Move</b> <b>🗑️ Delete zone</b> <b>🔄 Refresh</b>	
Resource group ( <a href="#">change</a> ) rg-dns	Name server 1 ns1-02.azure-dns.com.
Subscription ( <a href="#">change</a> ) MSDN Platforms Subscription	Name server 2 ns2-02.azure-dns.net.
Subscription ID	Name server 3 ns3-02.azure-dns.org.
	Name server 4 ns4-02.azure-dns.info.
Tags ( <a href="#">change</a> ) <a href="#">Click here to add tags</a>	

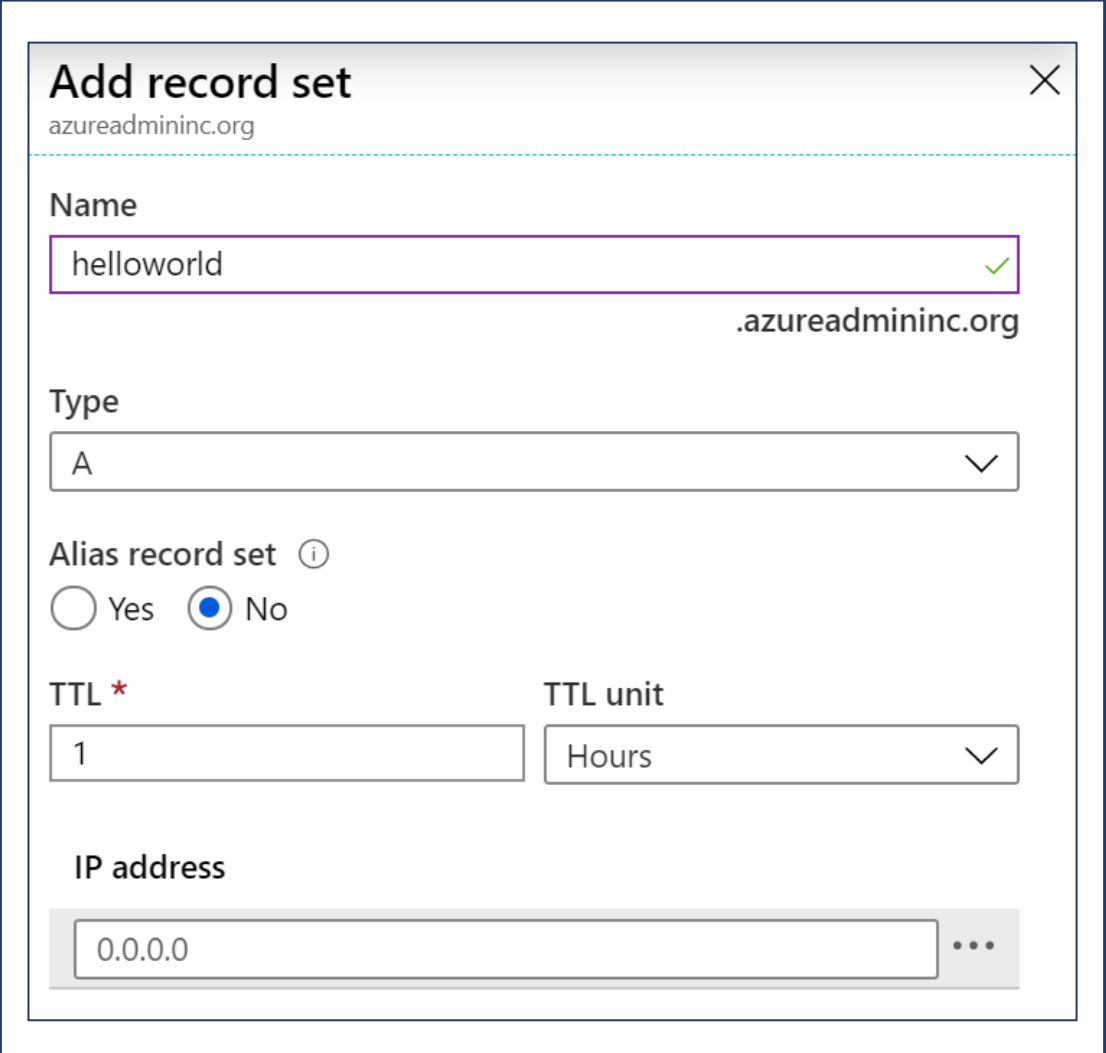
# DNS Record Sets

A record set is a collection of records in a zone that have the same name and are the same type

Azure DNS supports all common DNS record types: A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV, and TXT ?

A record set cannot contain two identical records

Changing the drop-down Type, changes the information required



The screenshot shows the 'Add record set' dialog box for the domain 'azureadmininc.org'. The dialog has a title bar with a close button. The main content area includes:

- Name:** A text input field containing 'helloworld' with a green checkmark icon on the right.
- Type:** A dropdown menu currently showing 'A'.
- Alias record set:** A section with an information icon and two radio buttons: 'Yes' (unselected) and 'No' (selected).
- TTL:** A text input field containing '1'.
- TTL unit:** A dropdown menu currently showing 'Hours'.
- IP address:** A text input field containing '0.0.0.0' with a three-dot menu icon on the right.

# DNS for Private Domains

Use your own custom domain names

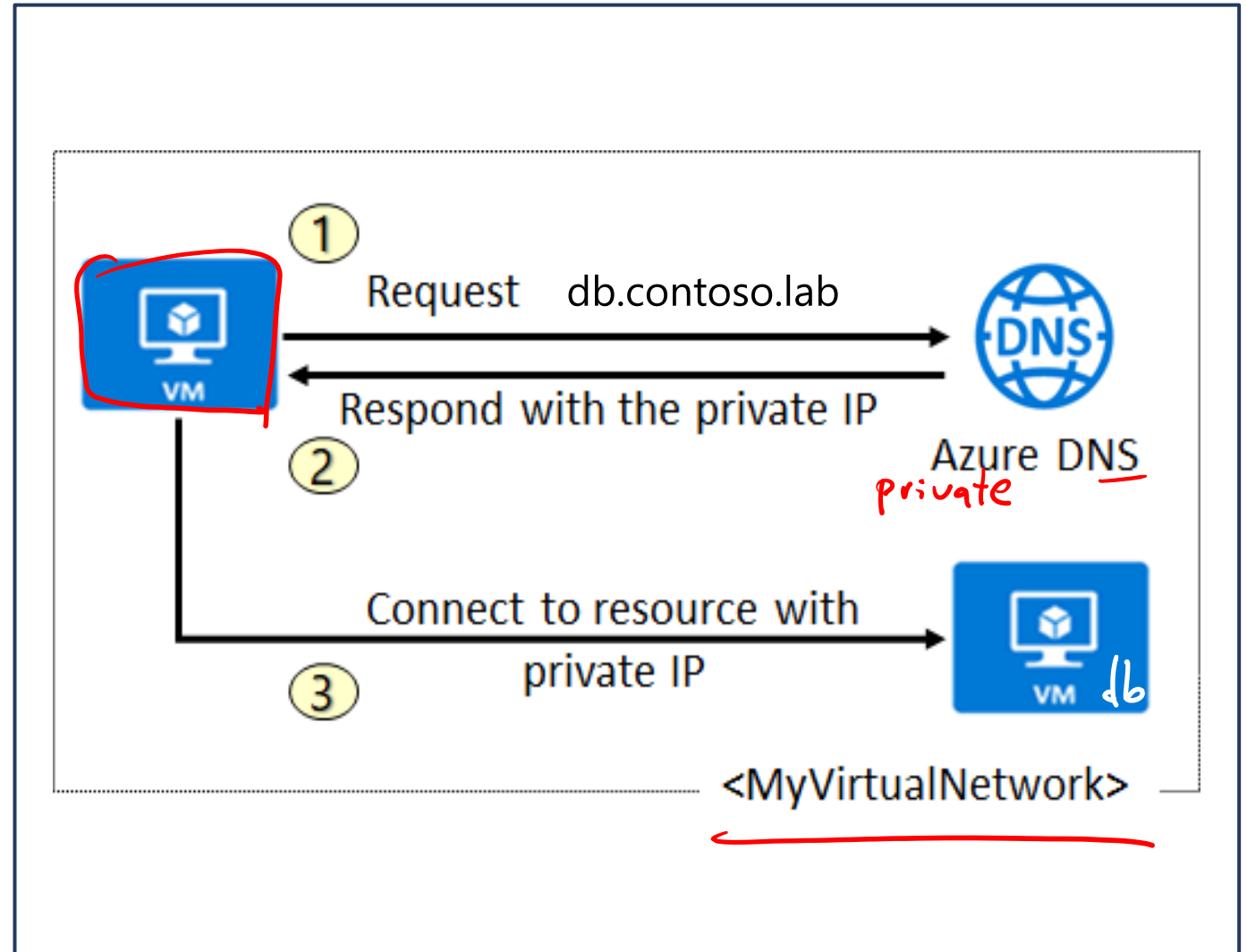
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

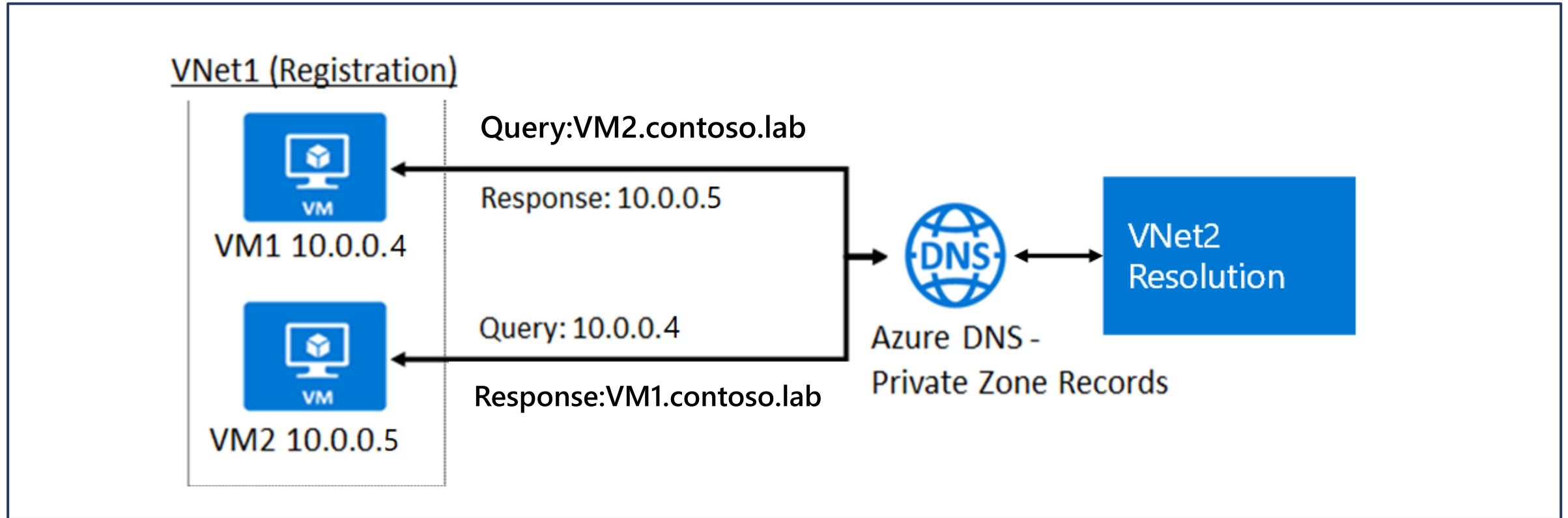
Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



# Private Zone Scenarios



DNS queries across the linked virtual networks are resolved

DNS resolution in VNet1 is private and not accessible from the Internet



# Significance of IP address 168.63.129.16

Enables the VM Agent to communicate with the Azure platform to signal that it is in a "Ready" state

Enables communication with the DNS virtual server to provide filtered name resolution to the resources (such as VM) that do not have a custom DNS server.

Enables health probes from Azure load balancer to determine the health state of VMs

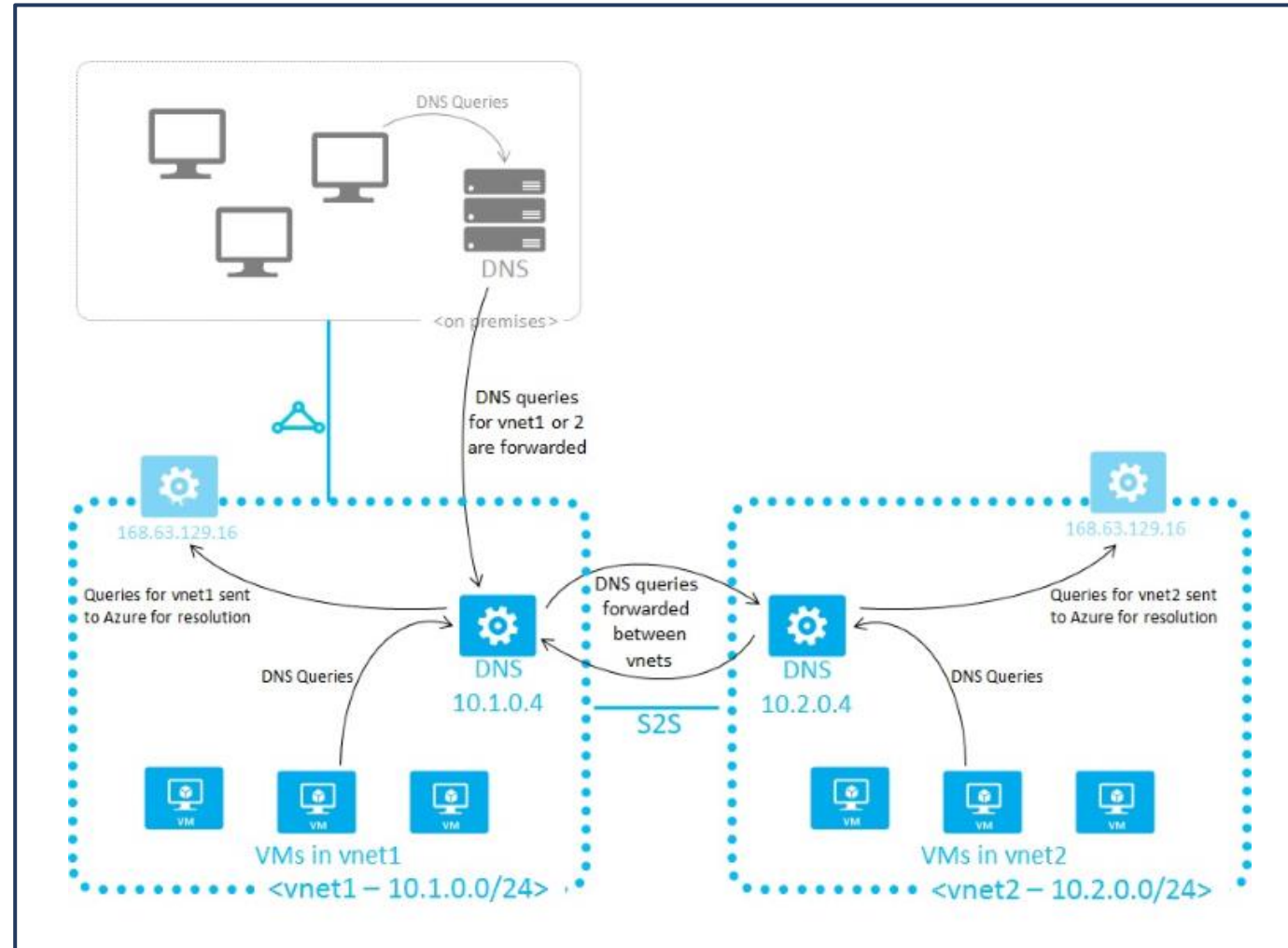
Enables the VM to obtain a dynamic IP address from the DHCP service in Azure

Enables Guest Agent heartbeat messages for the PaaS role

# Configure DNS settings inside a VNet

## Provide your own DNS solution:

- Provide appropriate host name resolution.
- Provide appropriate recursive resolution to allow resolution of external domain names.
- Be accessible (TCP and UDP on port 53) - NSG rules must allow access to your DNS listeners endpoint.
- Be secured against access from the internet, to mitigate threats posed by external agents.





# Enable Cross-VNet Connectivity with Peering

# Learning Objectives - Enable Cross-VNet Connectivity with Peering

- VNet Peering
- Gateway Transit and Connectivity
- Service Chaining
- Configure VNet Peering
- Demonstration
- Learning Recap

# VNet Peering

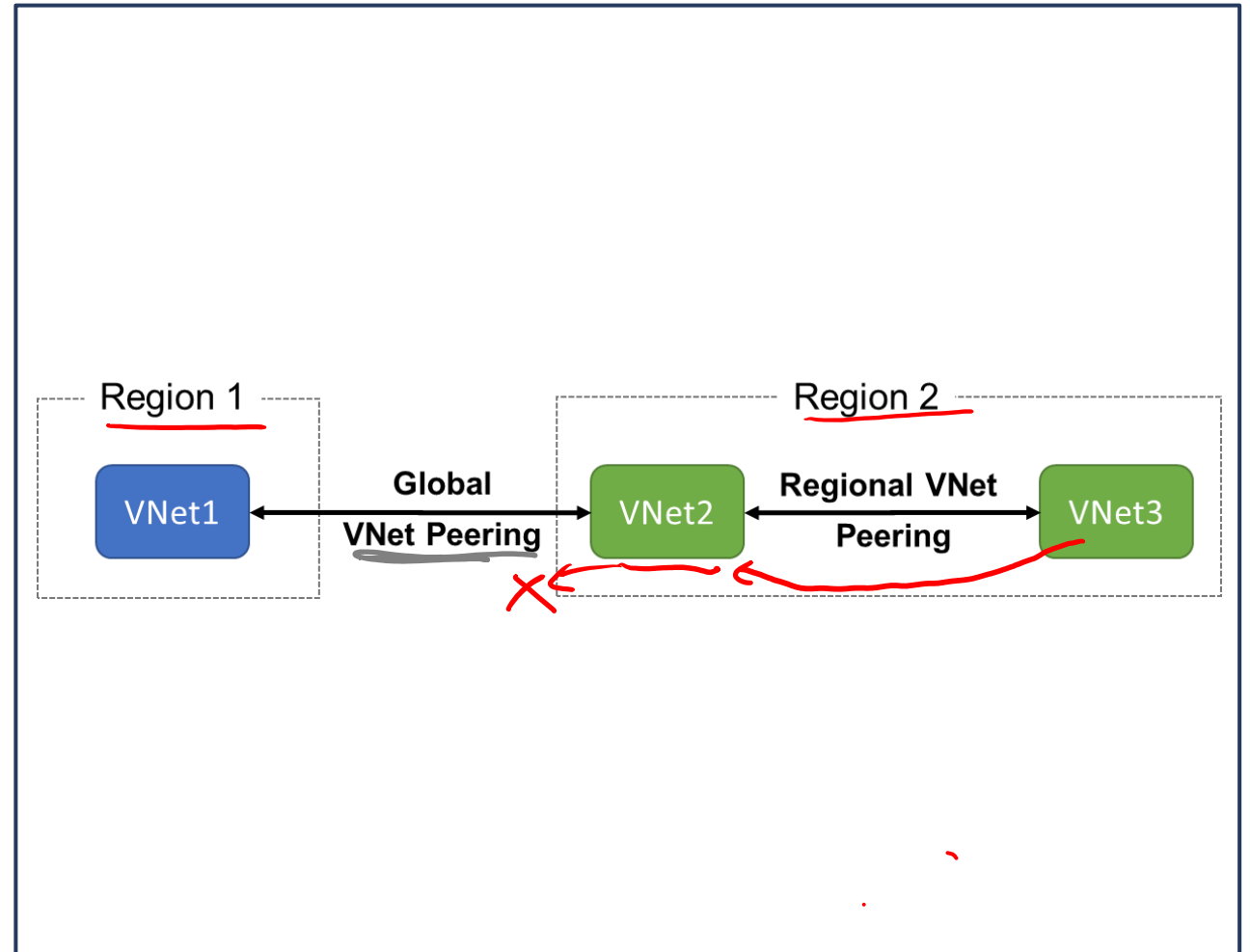
VNet peering connects two Azure virtual networks

Two types of peering: Regional and Global

Peered networks use the Azure backbone for privacy and isolation

You can peer across subscriptions and tenants

VNet peering is not transitive

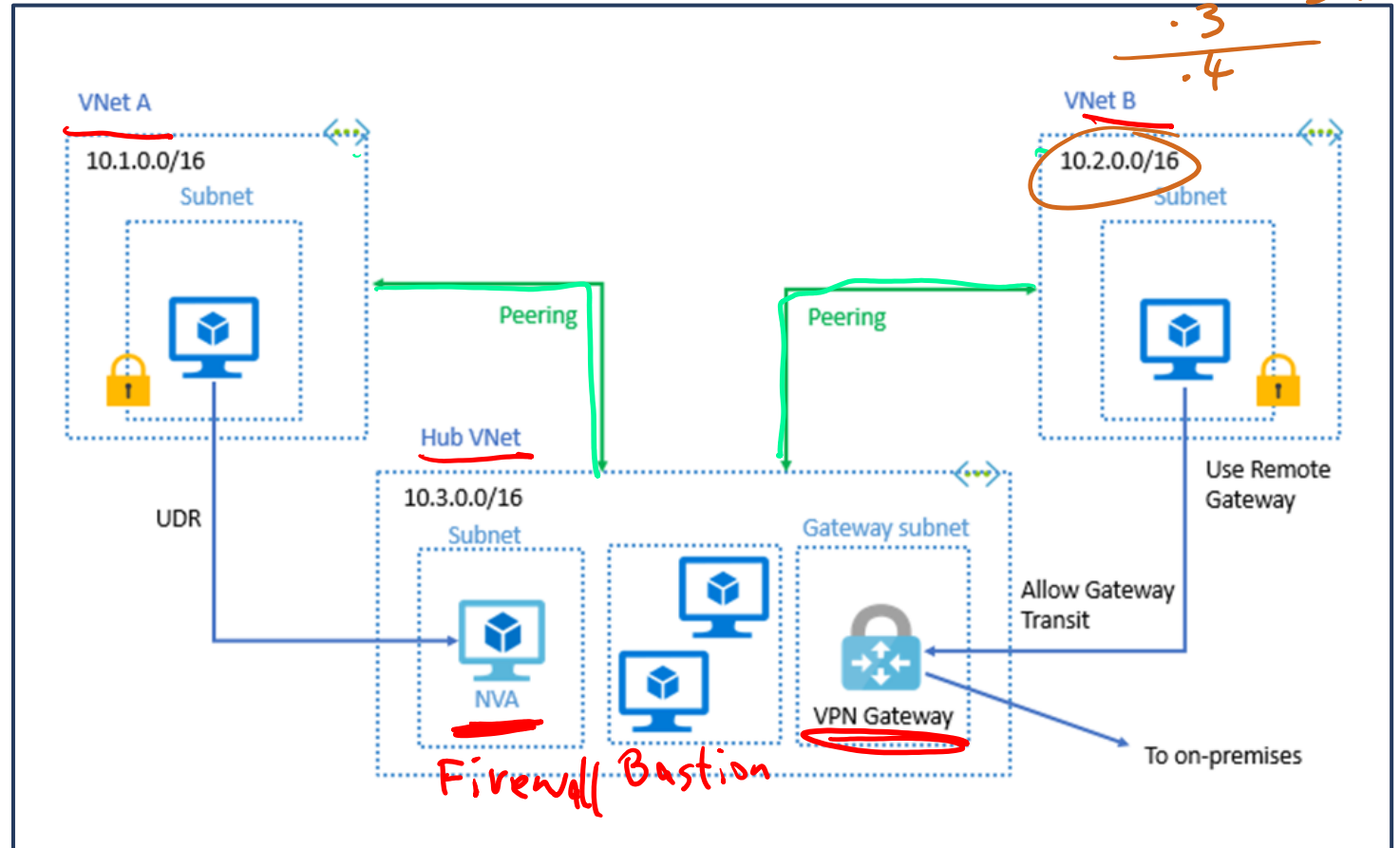


# Implementing VNet Peering

Gateway transit allows peered virtual networks to share the gateway and get access to resources

No VPN gateway is required in the peered virtual network

Default VNet peering provides full connectivity



IP address spaces of connected networks can't overlap

# Configure VNet Peering

Allow virtual network access settings

Configure forwarded traffic settings

This virtual network

Peering link name \*

Traffic to remote virtual network ⓘ

- ☒ Allow (default)
- ☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- ☒ Allow (default)
- ☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

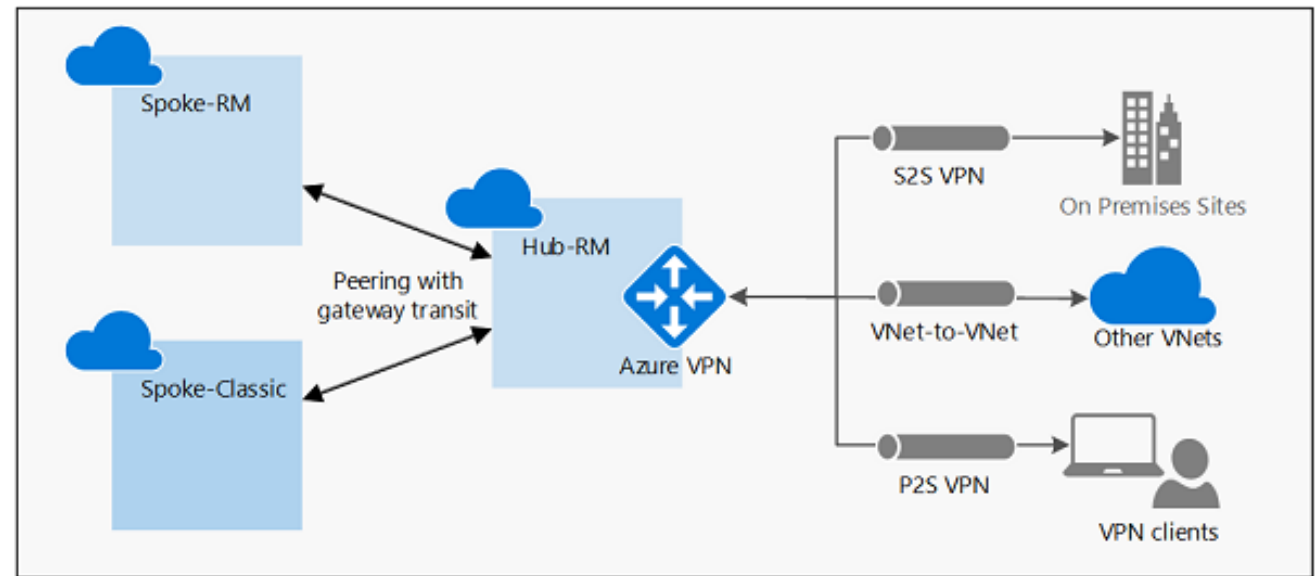
- ☐ Use this virtual network's gateway or Route Server
- ☐ Use the remote virtual network's gateway or Route Server
- ☒ None (default)

Remote virtual network

Peering link name \*

# Configure VNet peering – Gateway Transit

Gateway transit allows spoke virtual networks to share the VPN gateway in the hub



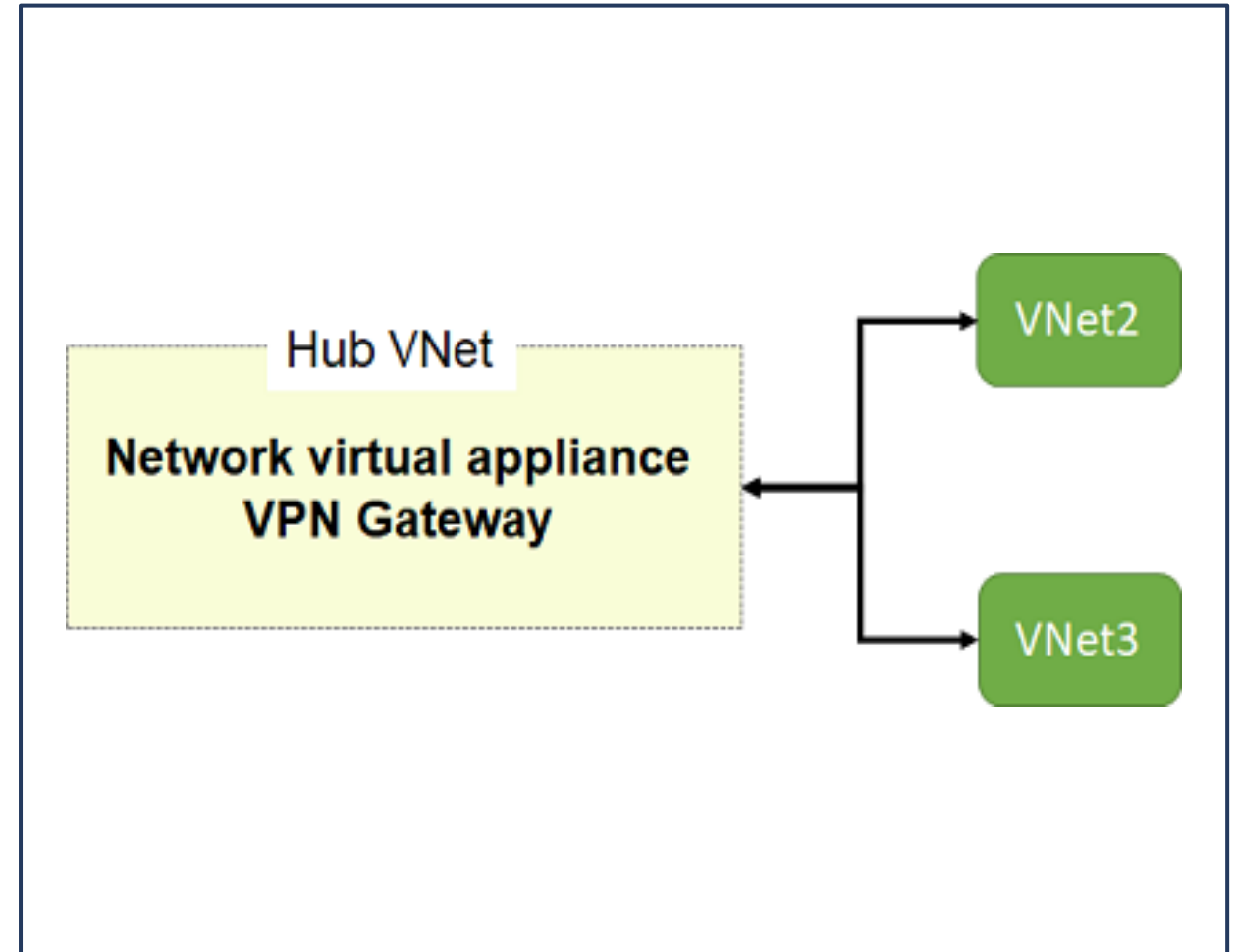


# Service Chaining

Leverage user-defined routes and service chaining to implement custom routing

Implement a VNet hub with a network virtual appliance or a VPN gateway

Service chaining enables 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



# Implement virtual network traffic routing



# Learning Objectives - Implement Virtual Network Traffic Routing

- Virtual network traffic routing
- Configure User-defined routes (UDRs)
- Configure forced tunneling
- Configure Azure Route Server
- Diagnose a routing problem
- Demonstration
- Learning Recap

# Virtual network traffic routing

System routes

Default routes

Custom routes

BGP

myVMNic1 - Effective routes

Network interface

Search (Ctrl+/) <<

Download Refresh

Showing only top 200 records, click Download above to see all.

Scope: Network interface (myVMNic1)

Associated route table: -

Effective routes

Source	↑↓	State	↑↓	Address Prefixes	↑↓	Next Hop Type	↑↓	Next Hop Type IP Address	↑↓	User Defined Route Name
Default		Active		10.1.1.0/24		Virtual network		-		-
Default		Active		0.0.0.0/0		Internet		-		-
Default		Active		10.0.0.0/8		None		-		-
Default		Active		100.64.0.0/10		None		-		-
Default		Active		192.168.0.0/16		None		-		-

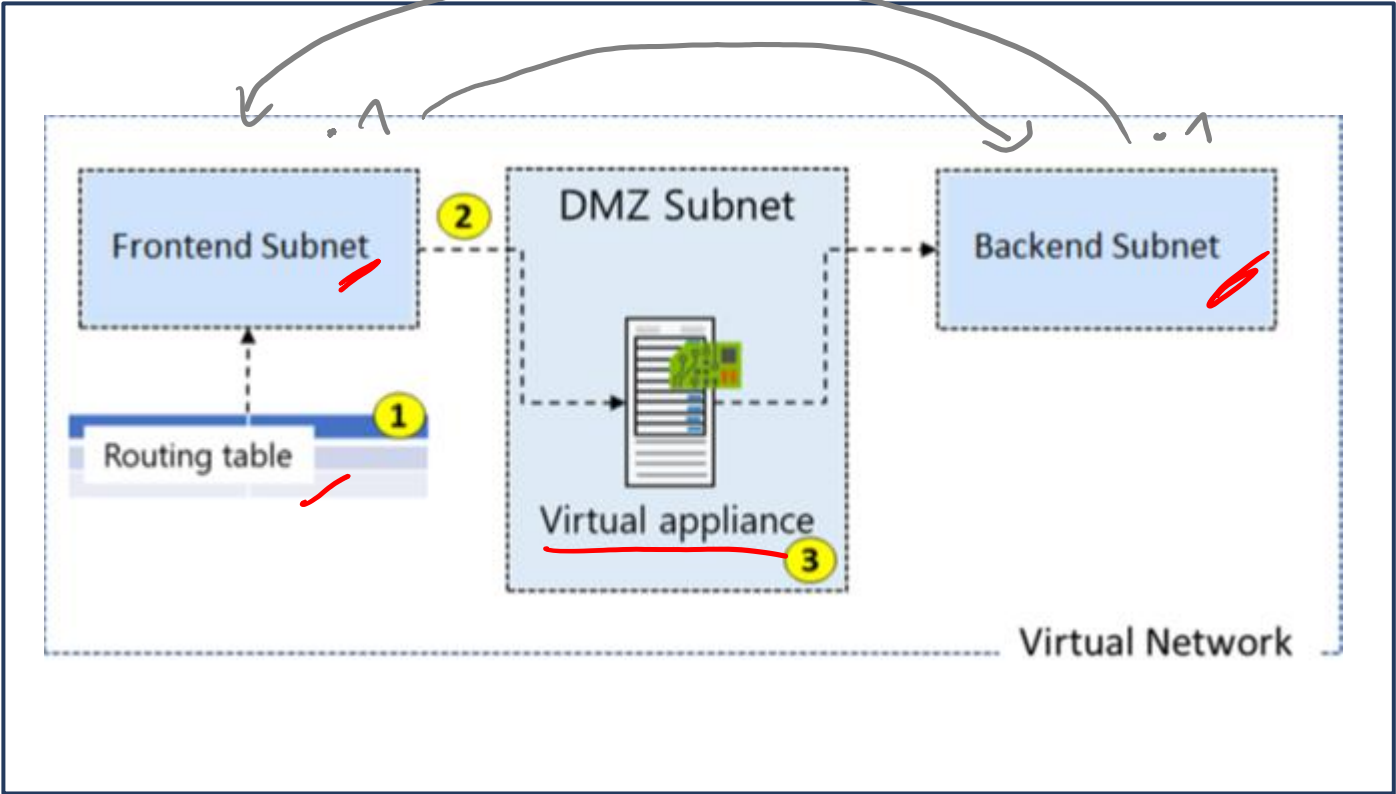
Settings

- IP configurations
- DNS servers
- Network security group
- Properties
- Locks
- Export template

Support + troubleshooting

- Effective security rules
- Effective routes**
- New support request

# Configure User-defined routes



### Create Route table

Subscription \* ⓘ  
Visual Studio Enterprise

Resource group \* ⓘ  
(New) myRGWest  
[Create new](#)

#### Instance details

Region \* ⓘ  
West US

Name \* ⓘ  
myRouteTablePublic

Propagate gateway routes \* ⓘ  
☒ Yes  
☐ No

# Create a Custom Route and associate route table to subnet

Add route

myRouteTablePublic

Route name \*

ToPrivateSubnet

Address prefix \* ⓘ

10.0.1.0/24

Next hop type ⓘ

Virtual network gateway

Virtual network gateway

Virtual network

Internet

Virtual appliance

None

Add subnet

VNet1

Name \*

Public

Address range (CIDR block) \* ⓘ

10.0.1.0/24

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

NAT gateway ⓘ

None

☐ Add IPv6 address space

Network security group

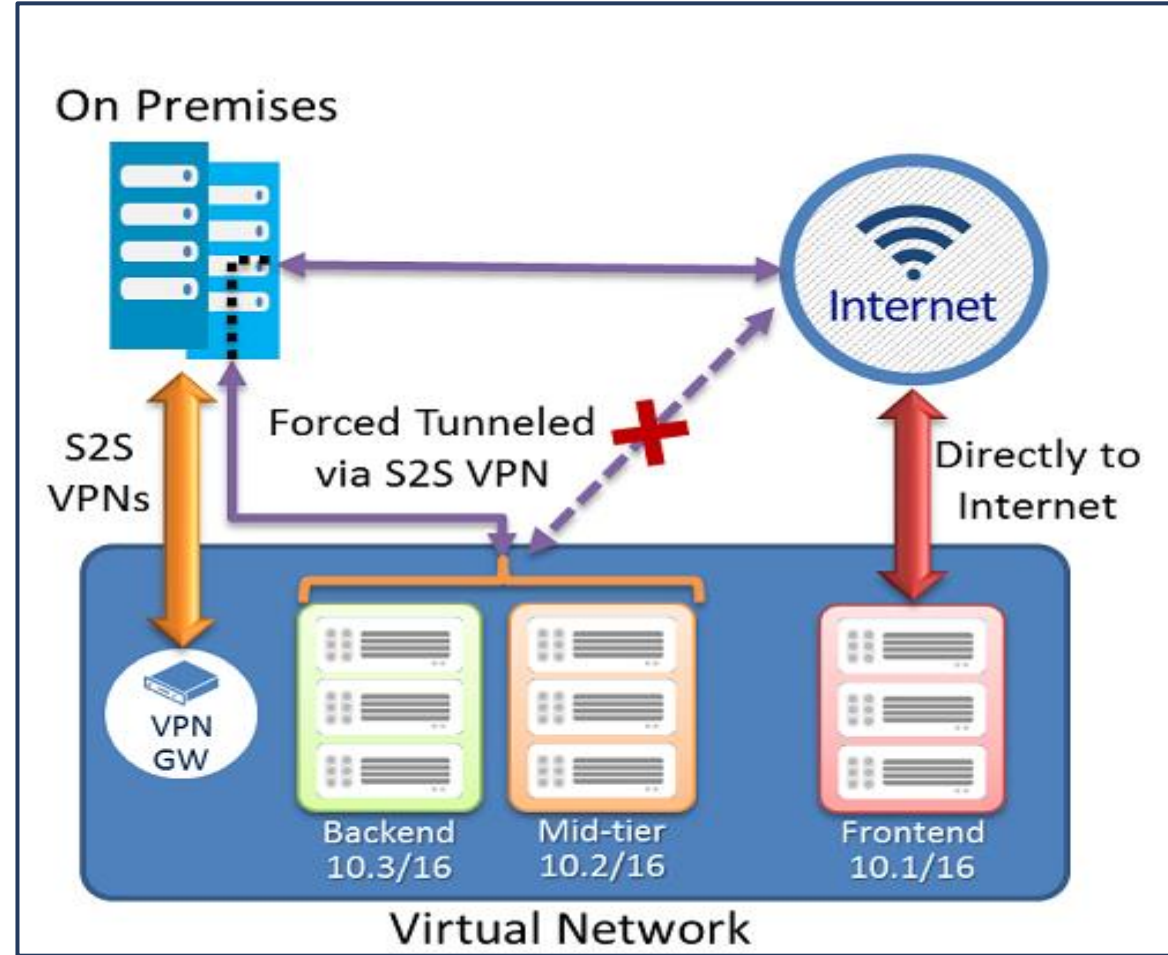
None

Route table

myRouteTablePublic

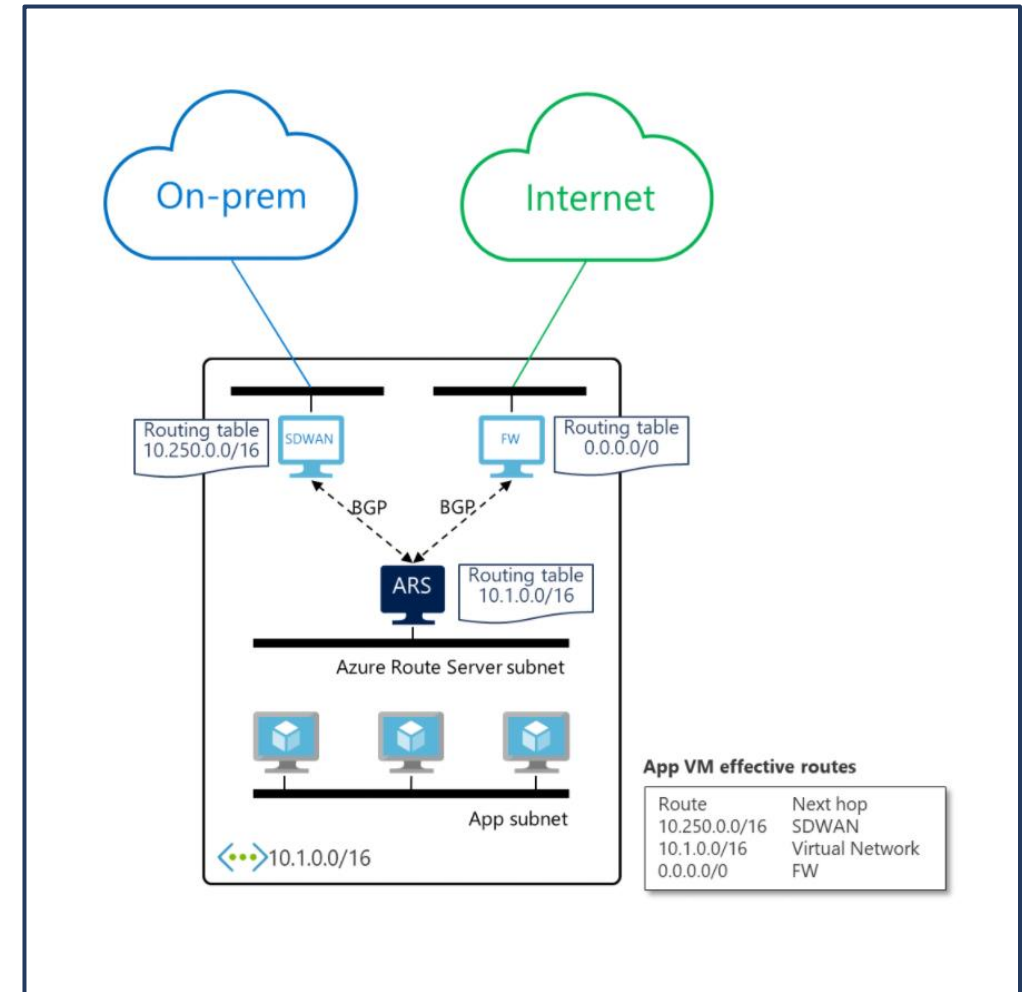
# Configure forced tunneling

- Create a routing table.
- Add a user-defined default route to the VPN Gateway.
- Associate the routing table to the appropriate VNet subnet(s).
- Forced tunneling must be associated with a VNet that has a route-based VPN gateway.
- You must set a default site connection among the cross-premises local sites connected to the virtual network.
- The on-premises VPN device must be configured using 0.0.0.0/0 as traffic selectors.



# Configure Azure Route Server

- Fully managed service that simplifies dynamic routing between NVA and the VNet
- NVA needs to support BGP
- You no longer need to manually update the routing table on your NVA whenever your virtual network addresses are updated.
- You no longer need to update User-Defined Routes manually whenever your NVA announces new routes or withdraw old ones.
- Needs a RouteServerSubnet





# Diagnose a routing problem

View effective routes in the Azure portal, PowerShell or CLI

Use Azure Network Watcher to troubleshoot

## **Resolve Issues:**

- Add a custom route to override a default route.
- Change or remove a custom route that causes traffic to be routed to an undesired location.
- Ensure that the route table is associated to the correct subnet (the one that contains the network interface).
- Ensure that devices such as Azure VPN gateway or network virtual appliances you've deployed are operating as intended.

# Configure internet access with Azure Virtual NAT



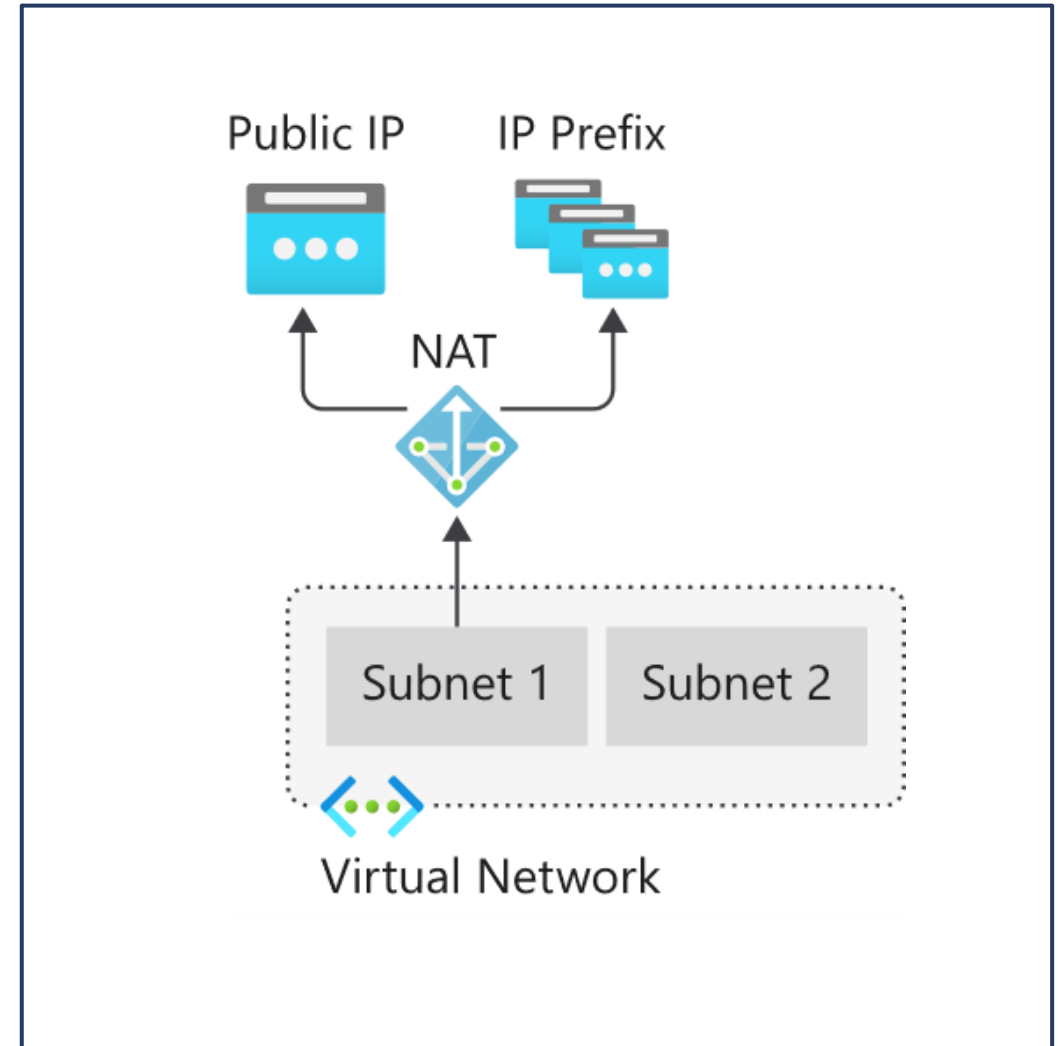
# Azure Virtual Network NAT

Virtual Network NAT (network address translation) simplifies outbound-only Internet connectivity for virtual networks

Is a fully managed and highly resilient service that supports dynamic workloads by scaling NAT

When configured on a subnet, all outbound connectivity uses your specified static public IP addresses

Outbound connectivity is possible without a load balancer or public IP addresses directly attached to virtual machines

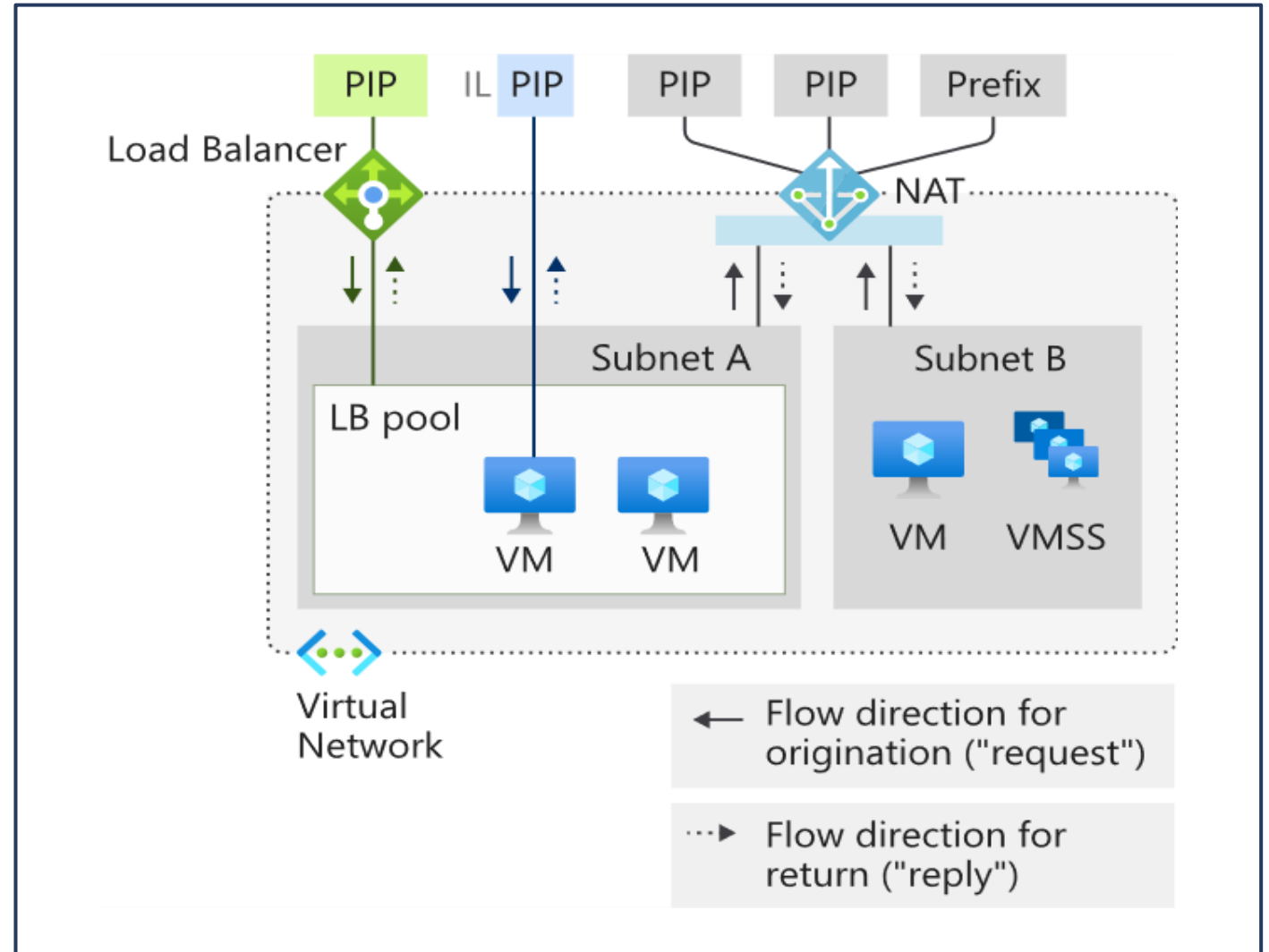


# Coexistence of inbound and outbound

NAT and compatible Standard SKU features are aware of the direction the flow was started.

Inbound and outbound scenarios can coexist.

These scenarios will receive the correct network address translations because these features are aware of the flow direction.



# How to deploy NAT

## NAT gateway resource:

1. Create regional or zonal (zone-isolated) NAT gateway resource
2. Assign IP addresses
3. If necessary, modify TCP idle timeout

## Virtual network:

- Configure virtual network subnet to use a NAT gateway.
- User-defined routes are not necessary.

**Basics** Outbound IP Subnet Tags Review + create

Azure NAT gateway can be used to translate outbound flows from a virtual network to the public internet.  
[Learn more about NAT gateways.](#)

**Project details**

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*

[Create new](#)

**Instance details**

NAT gateway name \*

Region \*

Availability zone ⓘ

Idle timeout (minutes) \* ⓘ

4-120

# Lab:

## Design and implement a Virtual Network in Azure



# Lab

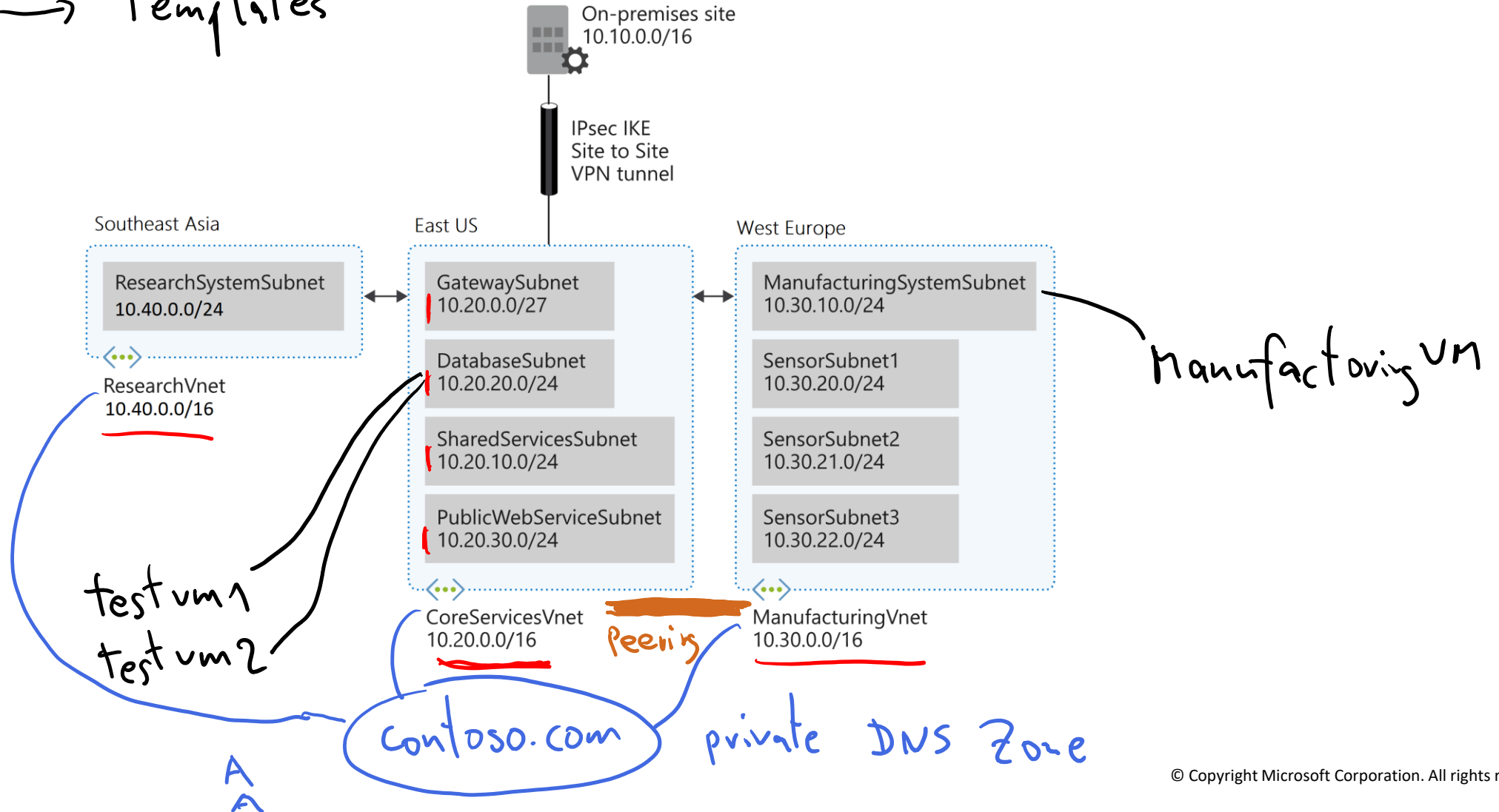
VNet → Portal

vm → Templates

Power Shell

Resolve-DNS Name

Test-NetConnection



# End of presentation

