

AZ-104

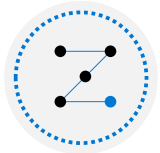
Administer Virtual Networking



About this course: Course Outline



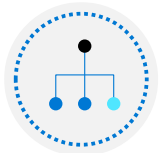
01: Administer Identity



02: Administer Governance and Compliance



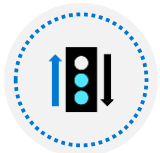
03: Administer Azure Resources



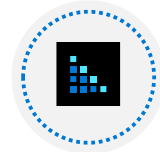
04: Administer Virtual Networking



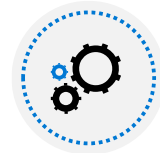
05: Administer Intersite Connectivity



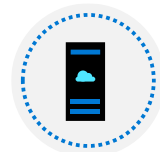
06: Administer Network Traffic Management



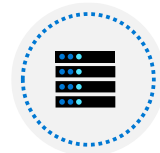
07: Administer Azure Storage



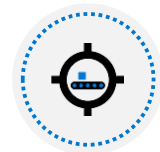
08: Administer Azure Virtual Machines



09: Administer PaaS Compute Options

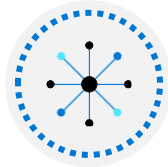


10: Administer Data Protection



11: Administer Monitoring

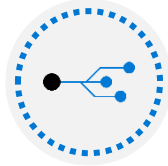
Administer Virtual Networking Introduction



Configure Virtual Networks

SDN

TCP / IPv4
IPv6



Configure Network Security Groups

NSG & FW

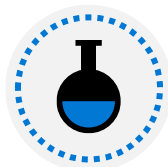
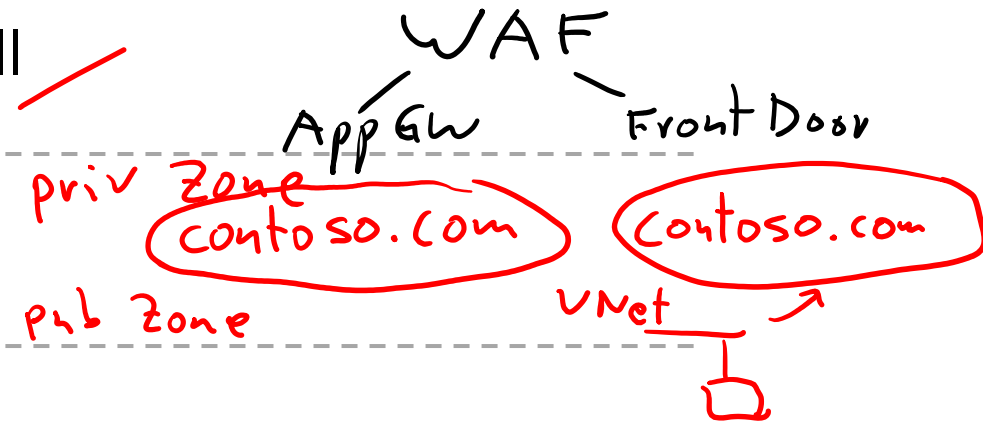


Configure Azure Firewall

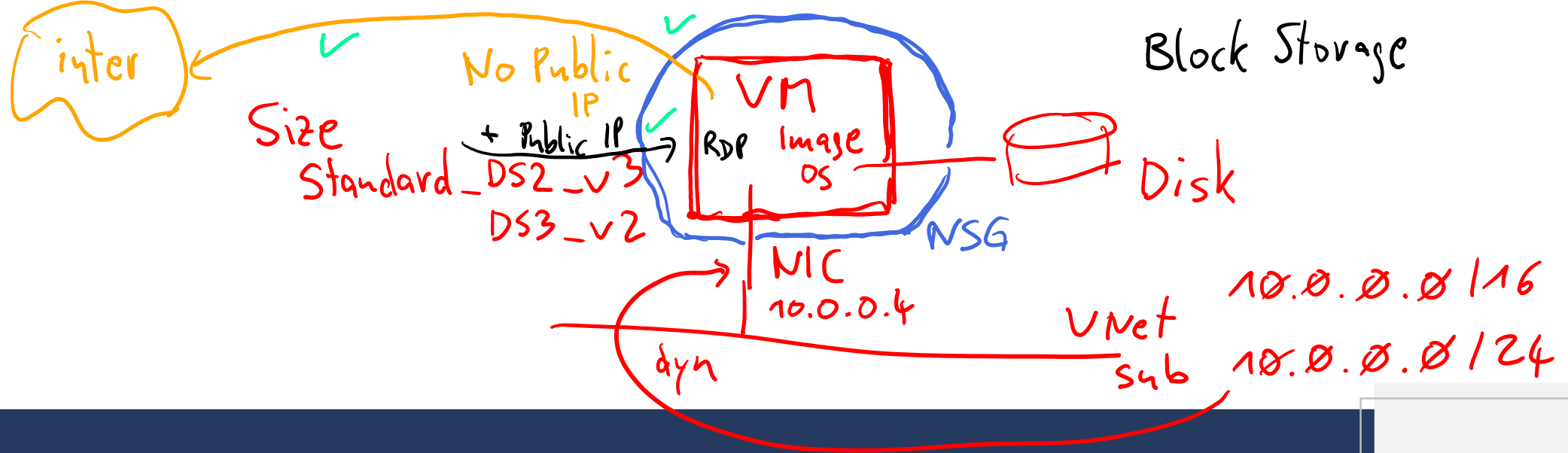


Configure Azure DNS

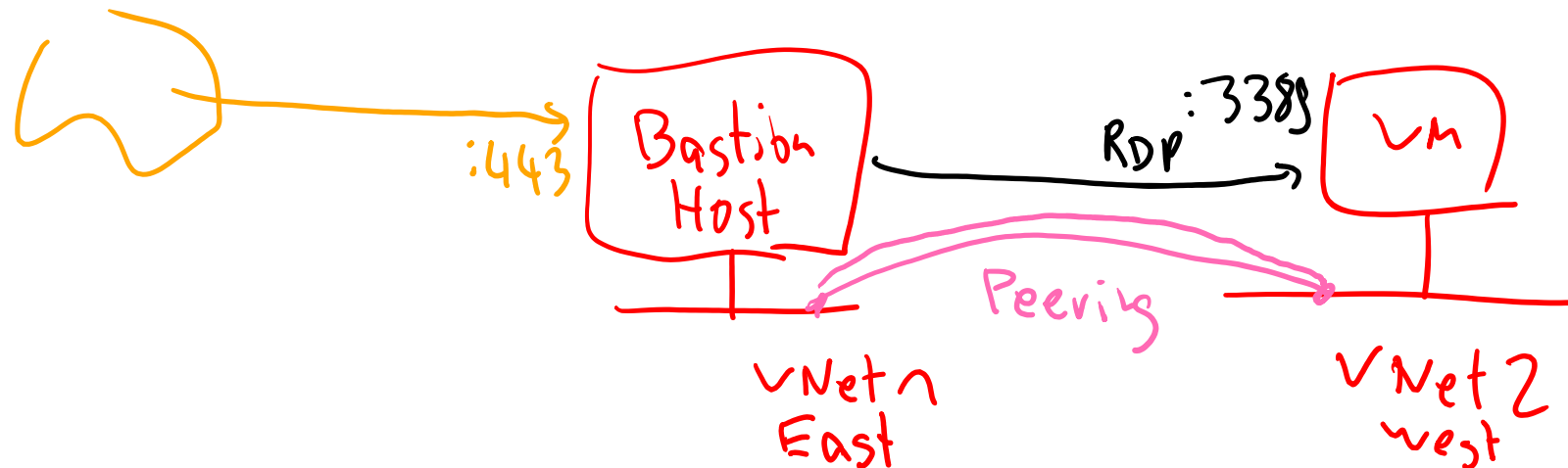
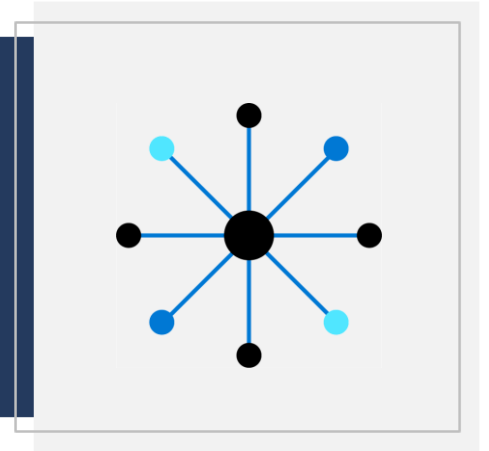
IANA



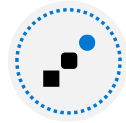
Lab 04 – Implement Virtual Networks



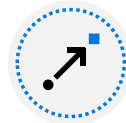
Configure Virtual Networks



Configure Virtual Networks Introduction



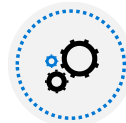
Plan Virtual Networks



Create Subnets



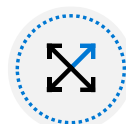
Create Virtual Networks



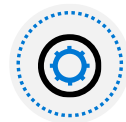
Plan IP Addressing



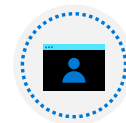
Create Public IP Addresses



Associate Public IP Addresses



Associate Private IP Addresses

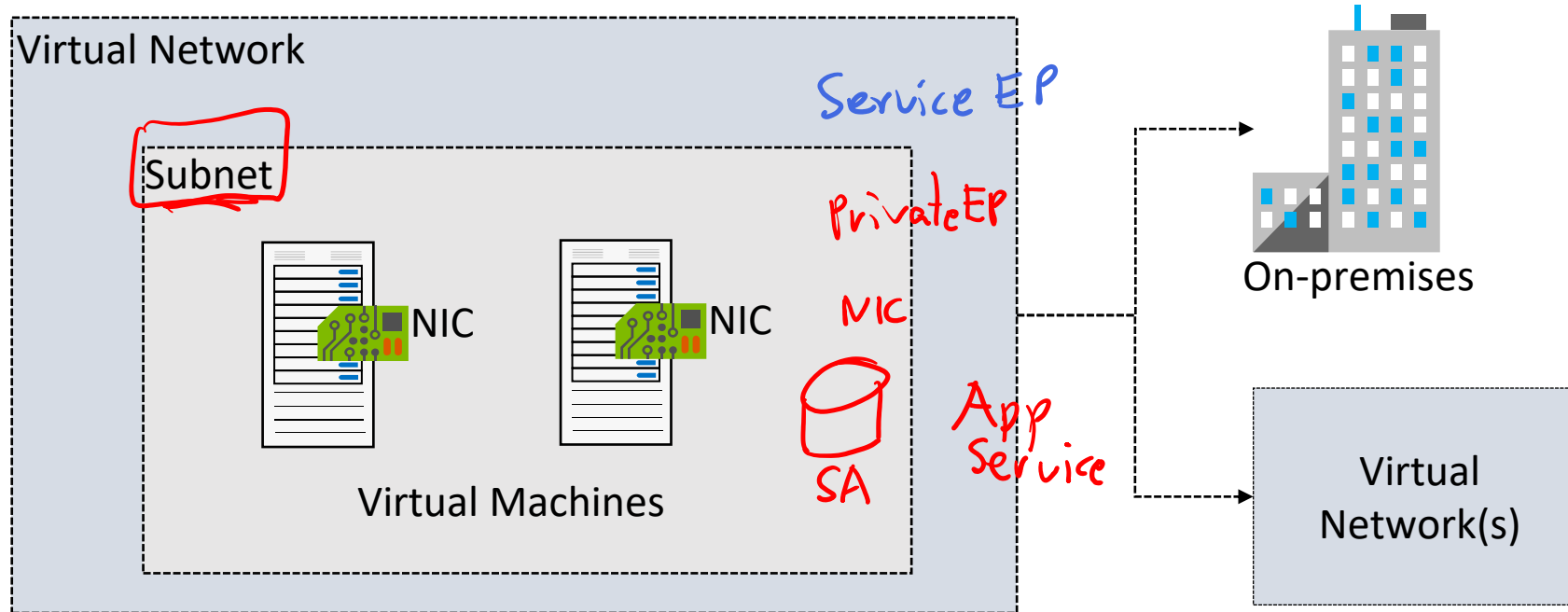


Demonstration – Virtual Networks



Summary and Resources

Plan Virtual Networks



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

Create Subnets

Scope 10.0.0.0/16
172.16.0.0/16

+ Subnet + Gateway subnet Refresh Manage users Delete				
Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/27	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

fix

fix

fix

Azure Firewall Subnet

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 vnet in the subscription

Create Virtual Networks

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

Be careful with 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 *

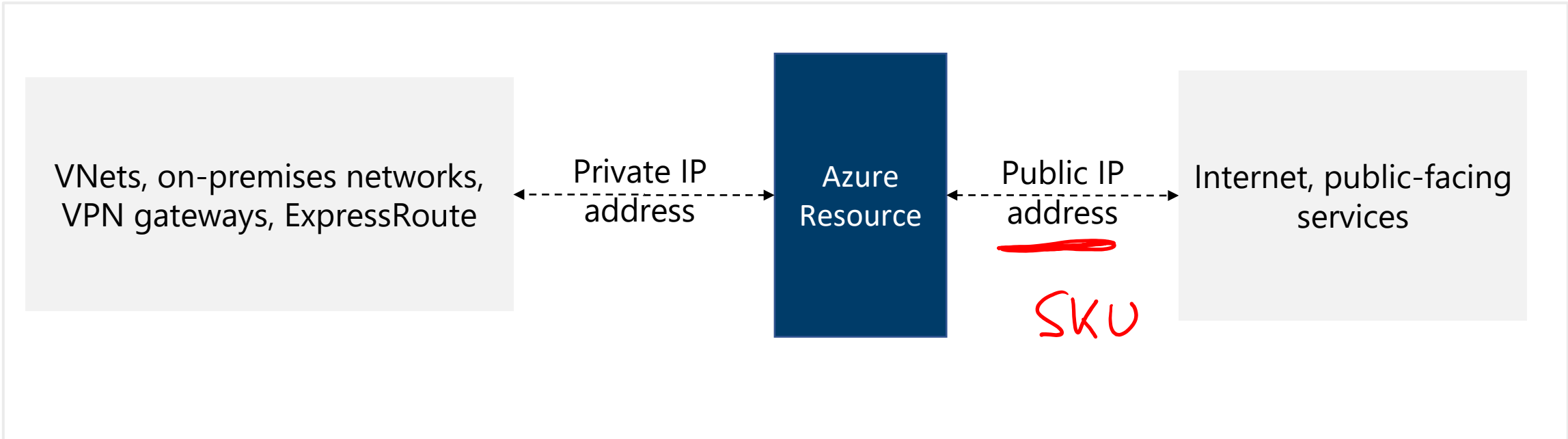
VNet2



Region *

(US) East US 2

Plan IP Addressing



Private IP addresses - used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure

Public IP addresses - used for communication with the Internet, including Azure public-facing services

New - Net Net Ip Address
~~Address~~

Create Public IP Addresses

Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Dynamic vs Static

Zone redundant (Standard SKU)

Range of contiguous addresses available as a prefix

Create public IP address

IP Version * ⓘ

☒ IPv4 ☐ IPv6 ☐ Both

SKU * ⓘ

☒ Basic ☐ Standard

IPv4 IP Address Configuration

Name *

My PiP

IP address assignment *

☒ Dynamic ☐ Static

Associate 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	Yes*
Application Gateway	Front-end configuration	Yes	Yes*

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

*Static IP addresses only available on certain SKUs.

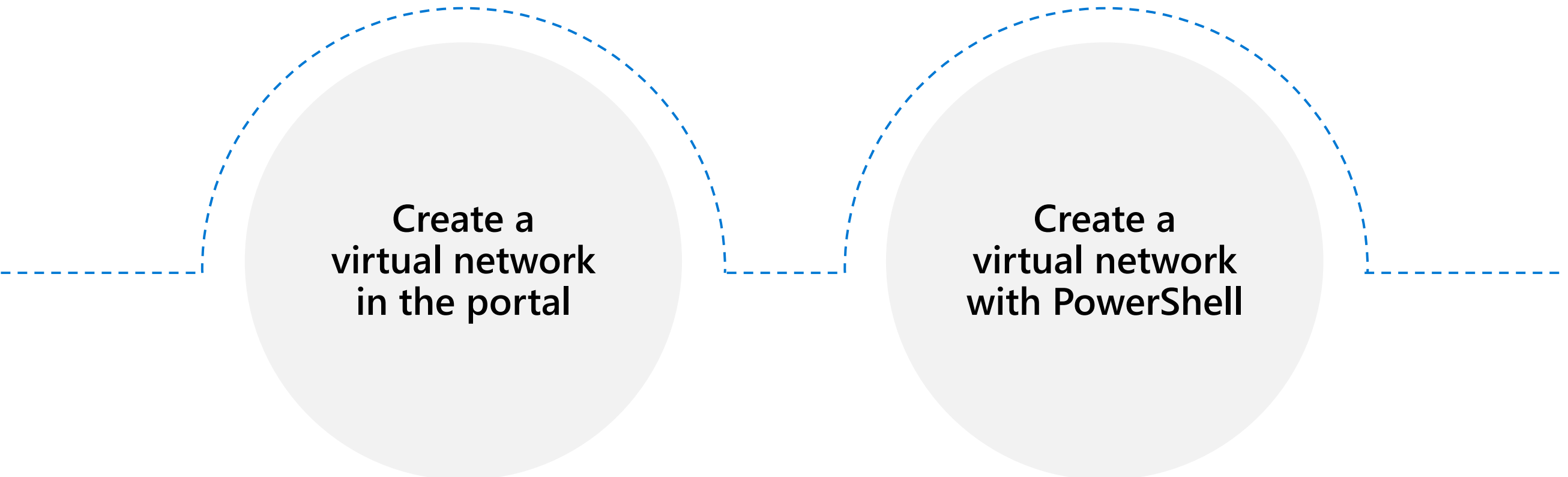
Associate Private IP Addresses

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	<u>NIC</u>	<u>Yes</u>	<u>Yes</u>
Internal Load Balancer	Front-end configuration	<u>Yes</u>	<u>Yes</u>
Application Gateway	Front-end configuration	<u>Yes</u>	<u>Yes</u>

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

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

Demonstration – Virtual Networks



The diagram consists of two light gray circles arranged horizontally. A dashed blue line starts from the left edge of the first circle, goes up and over its top, then down to the right edge of the first circle, across the gap between the circles, up and over the top of the second circle, and finally down to the right edge of the second circle. This line connects the two steps in a sequence.

**Create a
virtual network
in the portal**

**Create a
virtual network
with PowerShell**

Summary and Resources – Configure Virtual Networks

Knowledge Check



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

[Design an IP addressing schema for your Azure deployment \(Sandbox\)](#)

[Implement Windows Server IaaS VM IP addressing and routing](#)

A sandbox indicates a hands-on exercise.

Configure Network Security Groups



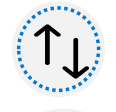
Configure Network Security Groups Introduction



Implement Network Security Groups (NSGs)



Determine NSG Rules



Determine NSG Effective Rules



Create NSG Rules



Implement Application Security Groups (ASGs)





Demonstration – NSGs



Summary and Resources

Implement Network Security Groups (NSGs)

 **nsg0**
Network security group

 Directory: Microsoft

Overview


Activity log


Access control (IAM)

Tags

Diagnose and solve problems

→ Move

 Delete

 Refresh

Resource group [\(change\)](#) : rg01

Location : East US

Subscription [\(change\)](#) :

Subscription ID :

Tags [\(change\)](#) : [Click here to add tags](#)

Custom security rules : 1 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

⌵

Limits network traffic
to resources in a
virtual network

Lists the security rules
that allow or deny
inbound or outbound
network traffic

Associated
to a subnet or a
network interface

Can be associated
multiple times

Determine NSG Rules

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	 RDP_Inbound	3389	Any	Any	Any	 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow
65500	DenyAllInBound	Any	Any	Any	Any	 Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

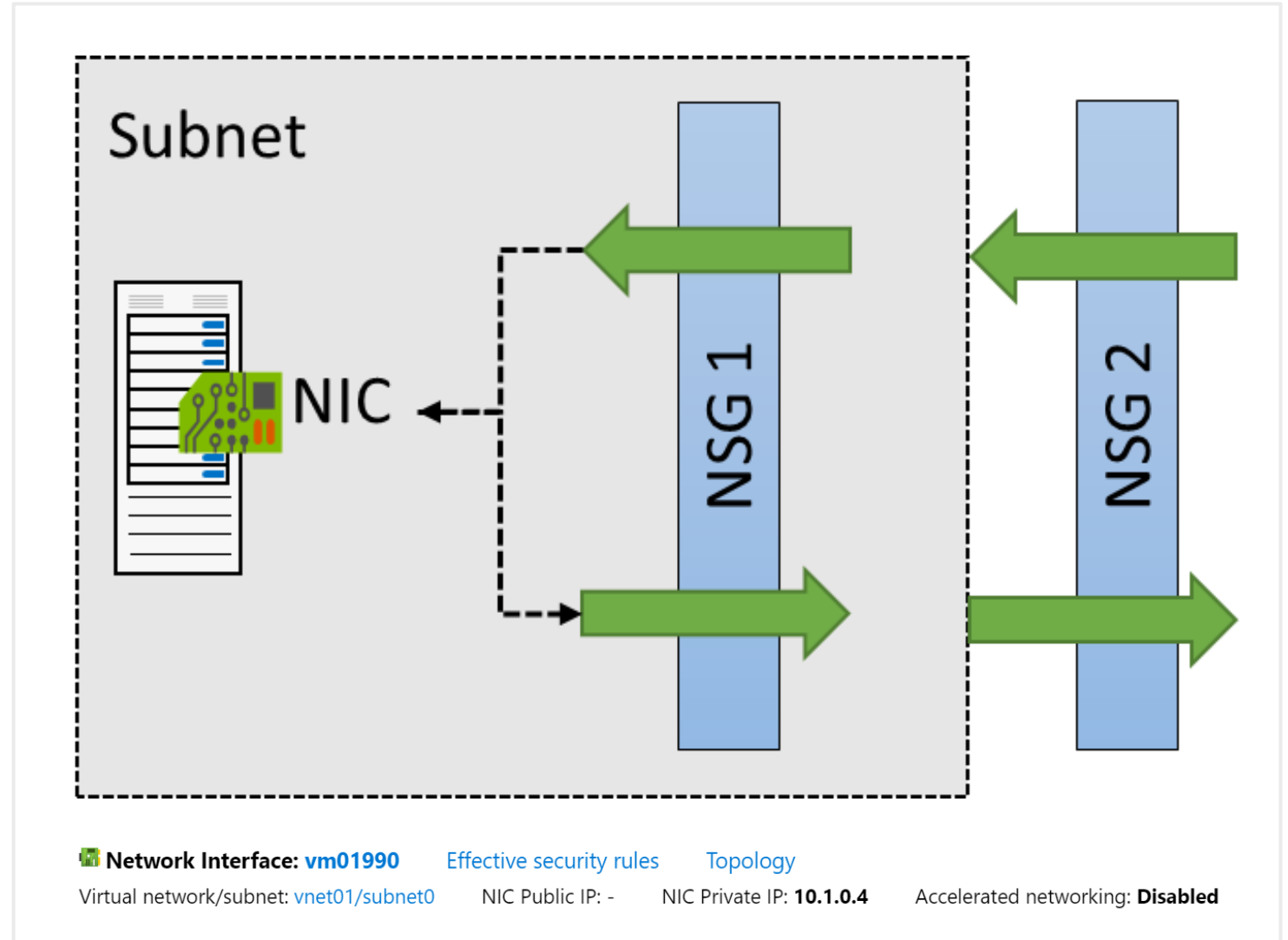
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

Determine NSG Effective Rules

NSGs are evaluated independently for the subnet and NIC

An “allow” rule must exist at both levels for traffic to be admitted

Use the Effective Rules link if you are not sure which security rules are being applied



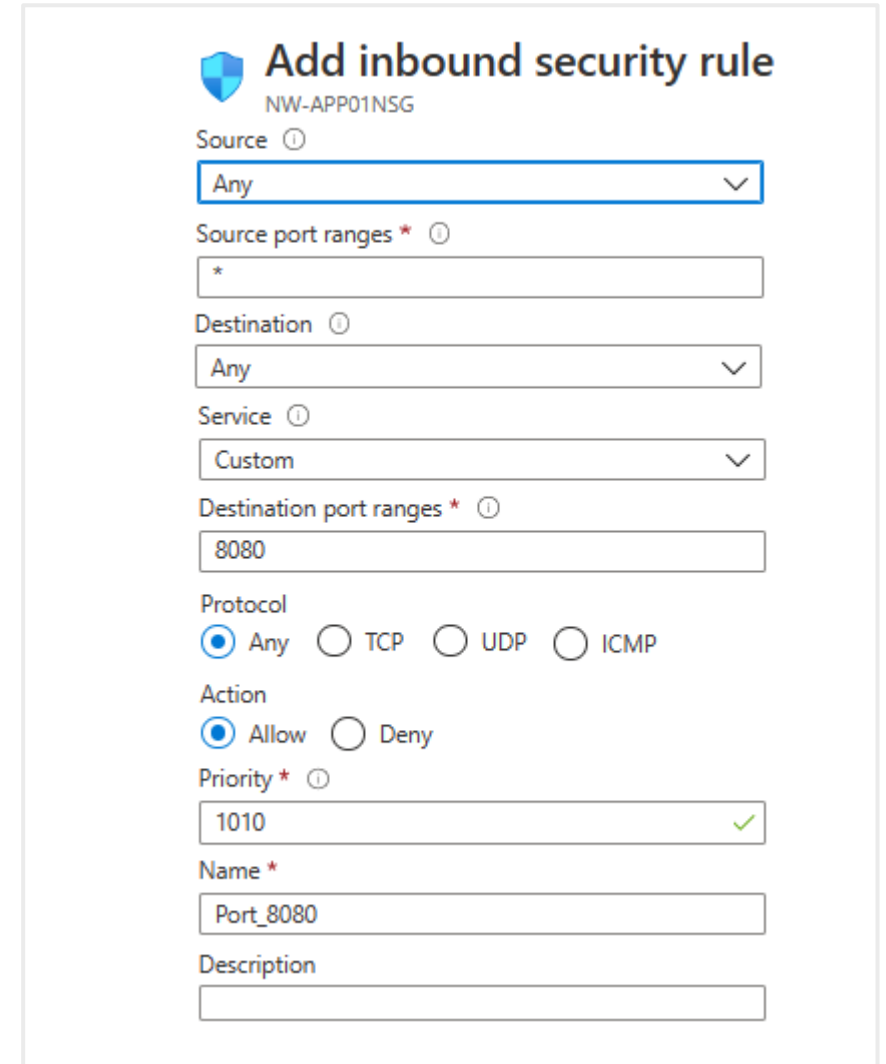
Create NSG rules

Source (Any, IP addresses, service tags, application security group)

Destination (Any, IP addresses, virtual network, application security group)

Service (HTTPS, SSH, RDP, DNS, POP3, custom, ...)

Priority – The lower the number, the higher the priority



The screenshot shows the 'Add inbound security rule' configuration page for a Network Security Group (NSG) named 'NW-APP01NSG'. The configuration is as follows:

- Source:** A dropdown menu set to 'Any'.
- Source port ranges:** A text input field containing an asterisk (*).
- Destination:** A dropdown menu set to 'Any'.
- Service:** A dropdown menu set to 'Custom'.
- Destination port ranges:** A text input field containing '8080'.
- Protocol:** Radio buttons for 'Any' (selected), 'TCP', 'UDP', and 'ICMP'.
- Action:** Radio buttons for 'Allow' (selected) and 'Deny'.
- Priority:** A text input field containing '1010', with a green checkmark icon to its right.
- Name:** A text input field containing 'Port_8080'.
- Description:** An empty text input field.

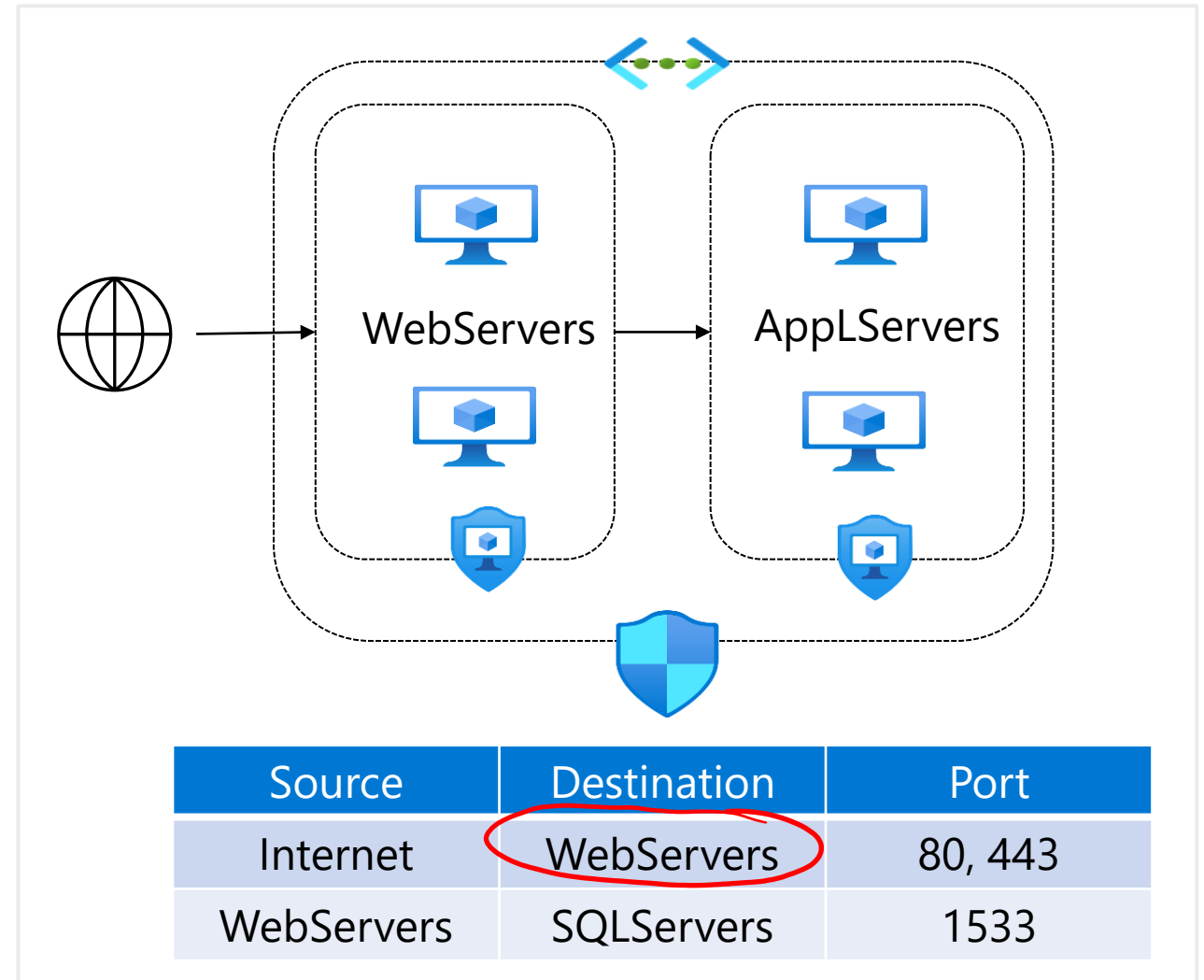
Implement Application Security Groups

Extends your application's structure

ASGs logically group virtual machines – web servers, application servers

Define rules to control the traffic flow

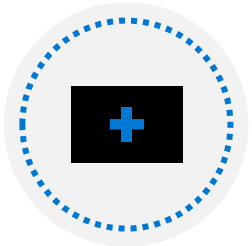
Wrap the ASG with an NSG for added security



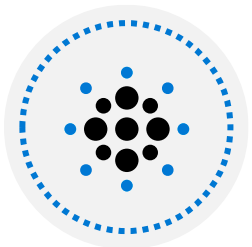
Demonstration – Network Security Groups



Access the NSGs blade



Add a new NSG



Explore inbound and outbound rules

Summary and Resources – Configure Network Security Groups

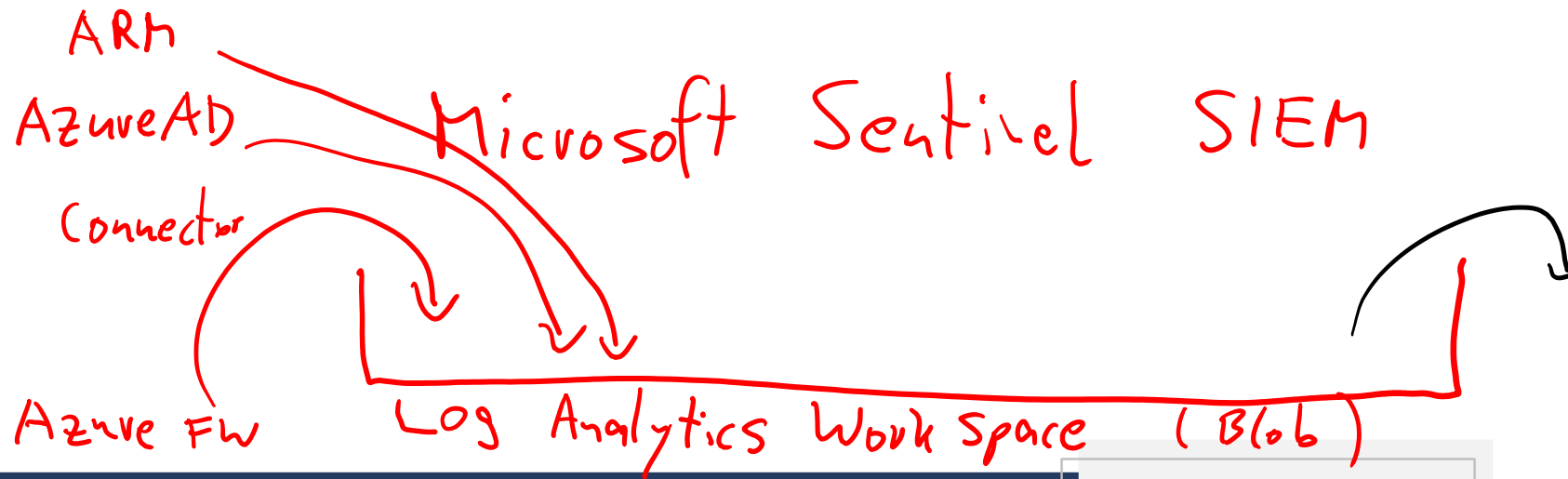
Knowledge Check



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

[Secure and isolate access to Azure resources by using network security groups and service endpoints \(Sandbox\)](#)

A sandbox indicates a hands-on exercise.



Lesson 03: Configure Azure Firewall



Azure Firewall Subnet

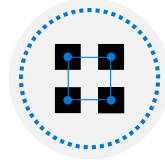
Configure Azure Firewall Introduction



Determine Azure Firewall Uses



Create Azure Firewalls



Create Azure Firewall Rules



Summary and Resources

Hub-Spoke-Topo

Determine Azure Firewall Uses

Stateful firewall as a service

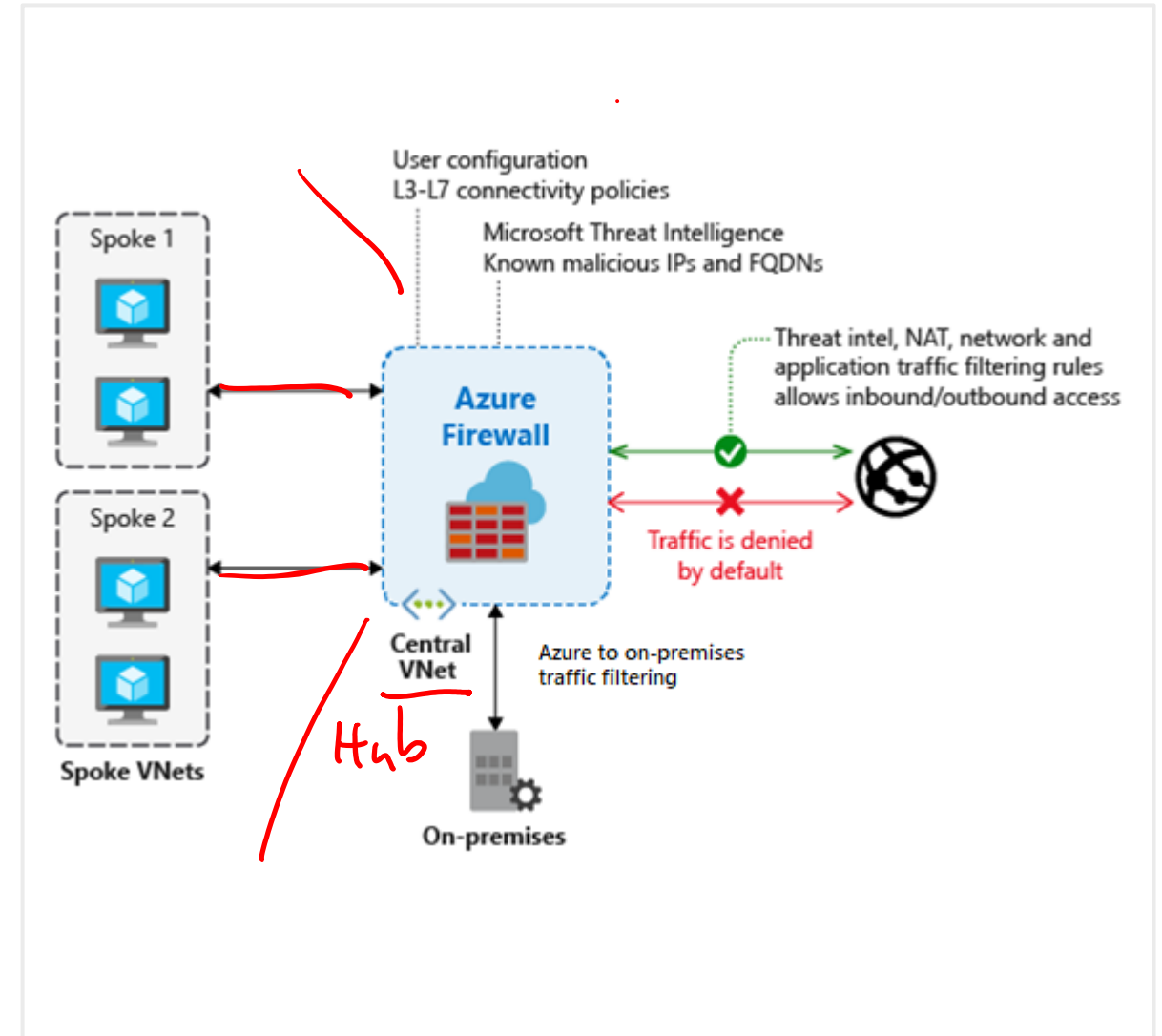
Built-in high availability with unrestricted cloud scalability

Create, enforce, and log application and network connectivity policies

Threat intelligence-based filtering

Fully integrated with Azure Monitor for logging and analytics

Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways

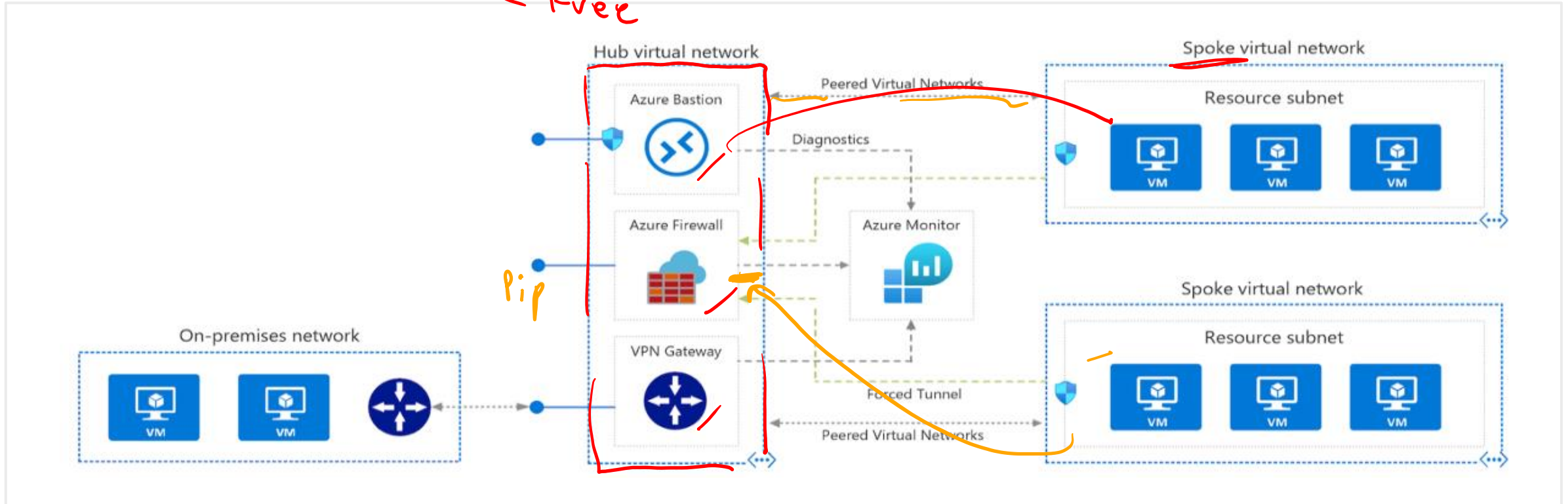


Create Azure Firewalls

Standard
Basic
Free

NVA
UDR

Network Virtual Appliance
User Defined Route



A Hub-Spoke network topology is recommended

Shared services are placed in the hub virtual network

Each environment is deployed to a spoke to maintain isolation

Create Azure Firewall Rules

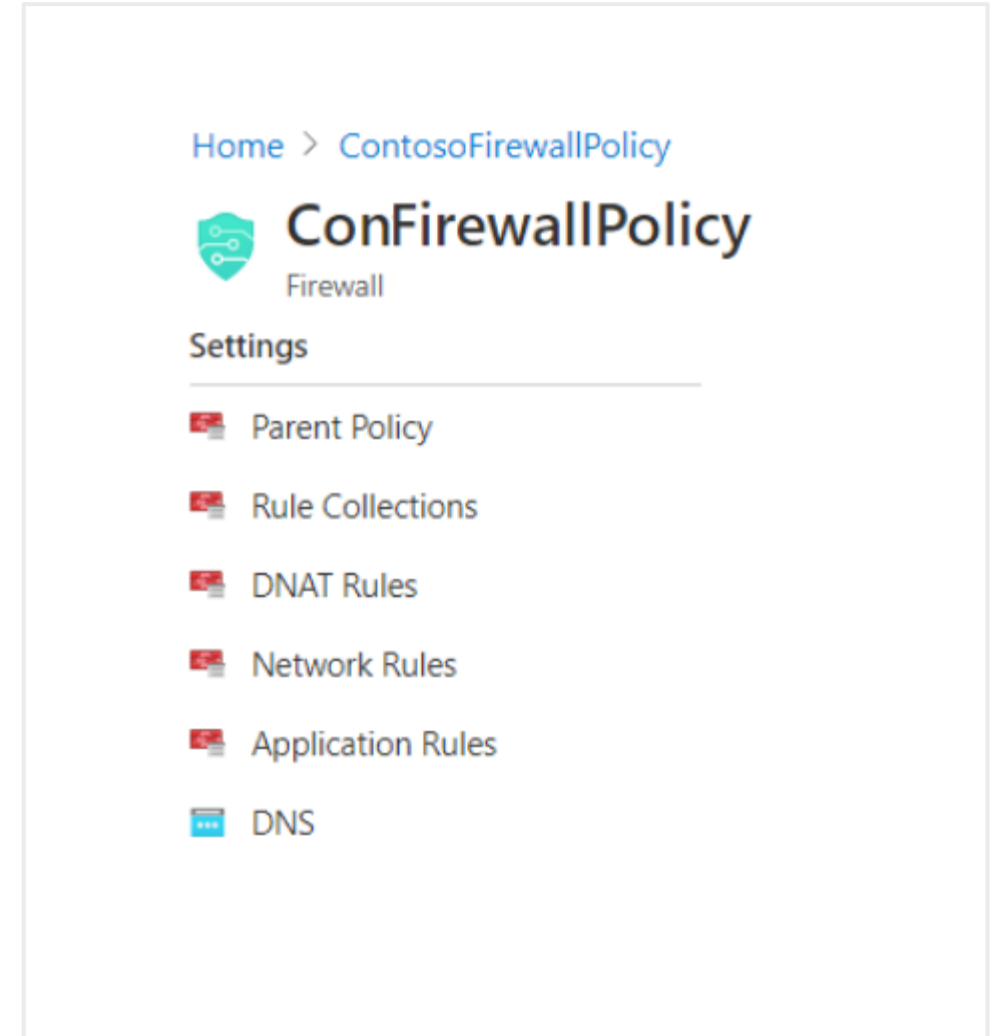
Azure Firewall Manager centralizes firewall management

Firewall policies container rules and settings to control access

NAT rules allow incoming connections

1.) **Network rules** contain source and destination addresses, protocols, and destination ports

2.) **Application rules provide** qualified domain names (FQDNs) that can be accessed from a subnet



Summary and Resources - Azure Firewall

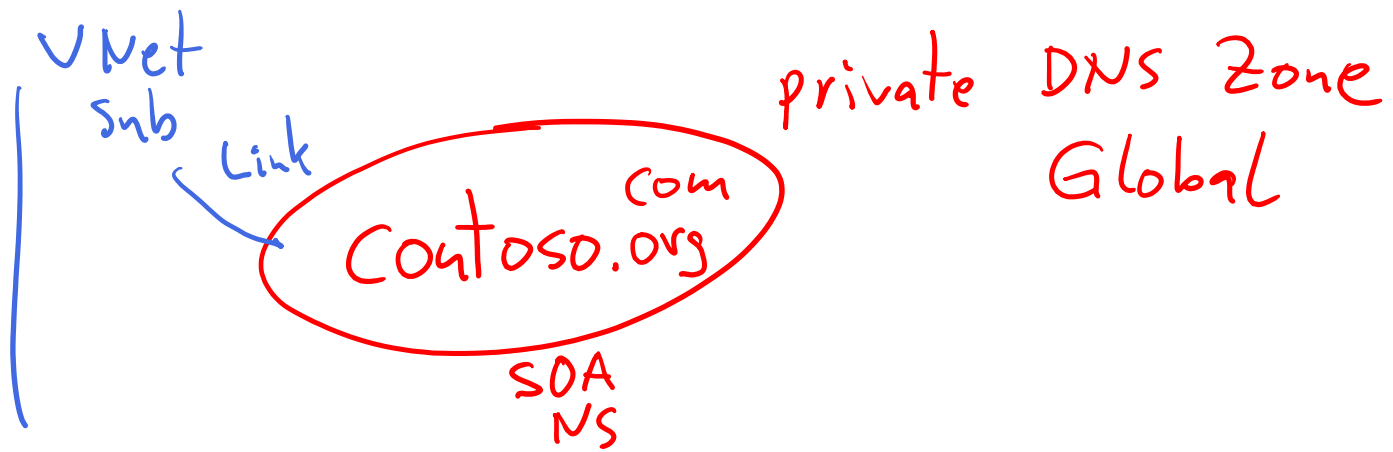
Knowledge Check



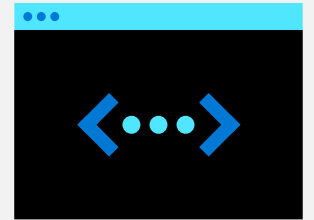
Microsoft Learn Modules (docs.microsoft.com/Learn)

[Introduction to Azure Firewall](#)

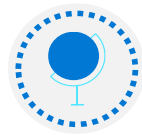
[Introduction to Azure Firewall Manager](#)



Configure Azure DNS



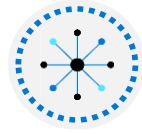
Configure Azure DNS Introduction



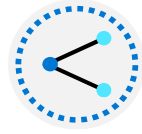
Identify Domains and Custom Domains



Verify Custom Domain Names (optional)



Create Azure DNS Zones



Delegate DNS Domains



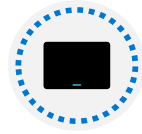
Add DNS Record Sets



Plan for Private DNS Zones



Determine Private Zone Scenarios



Demonstration – DNS Name Resolution



Summary and Resources

On Prem contoso.com

Identity Domains and Custom Domains

When you create an Azure subscription an Azure AD domain is created for you

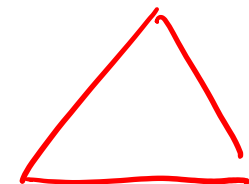
The domain has initial domain name in the form *domainname.onmicrosoft.com*

You can customize/change the name

After the custom name is added it must be verified – this demonstrates ownership of the domain

contoso.com

SOA
TXT



Tenant
onmicrosoft.com
contoso.com

TXT

A screenshot of the 'Create a directory' form in the Azure portal. The form is titled 'Create a directory' and 'Azure Active Directory'. It has tabs for 'Basics', 'Configuration', and 'Review + create'. The 'Configuration' tab is selected. Under 'Directory details', it says 'Configure your new directory'. The 'Organization name' field is 'Azure Administrator Incorporated'. The 'Initial domain name' field is 'azureadminincorg', and the full domain 'azureadminincorg.onmicrosoft.com' is shown below it. The 'Country/Region' is 'United States'. There are 'Review + create', '< Previous', and 'Next : Review + create >' buttons at the bottom.A screenshot of the 'Custom domain name' form in the Azure portal. The form is titled 'Custom domain name' and 'Azure Administrator Incorporated'. It has a 'Custom domain name' field with the value 'azureadminincorg' and a green checkmark. There is an 'Add domain' button at the bottom.

Create Azure DNS Zones

A DNS zone hosts the DNS records for a domain

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

BasicsTagsReview + 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 >

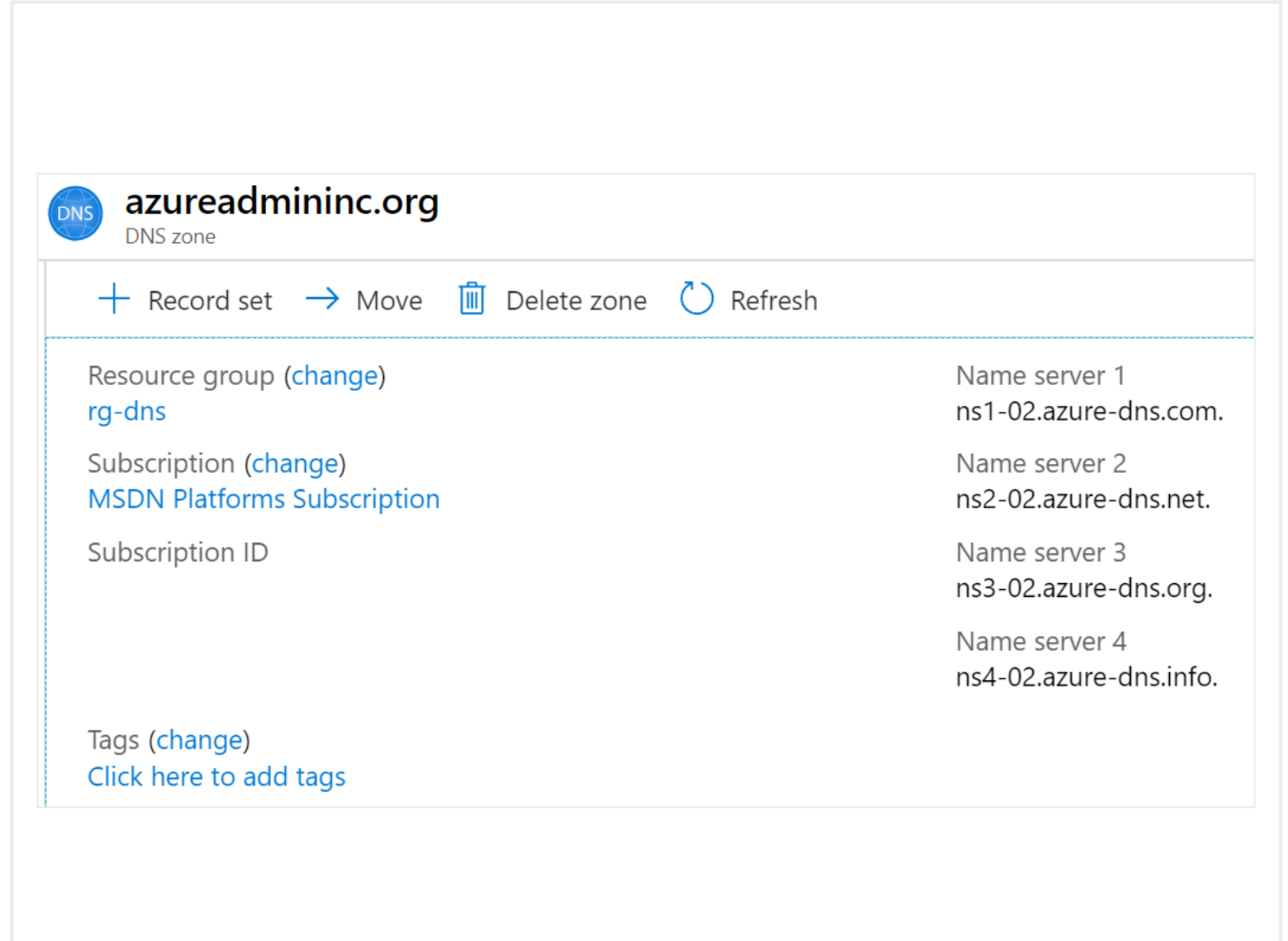
[Download a template for automation](#)

Delegate DNS Domains

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, and a toolbar with actions: **+ Record set**, **→ Move**, **🗑️ Delete zone**, and **🔄 Refresh**. The main content area is divided into two columns. The left column lists metadata: **Resource group** ([change](#)) **rg-dns**, **Subscription** ([change](#)) **MSDN Platforms Subscription**, **Subscription ID**, and **Tags** ([change](#)) with a [Click here to add tags](#) link. 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.**

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

Add DNS Record Sets

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

You can add up to 20 records to any record set

A record set cannot contain two identical records

Changing the drop-down Type, changes the information required

Add record set

azureadmininc.org

Name

helloworld

✓

.azureadmininc.org

Type

A

✓

Alias record set ⓘ

☐ Yes ☒ No

TTL *

1

TTL unit

Hours

✓

IP address

0.0.0.0

...

Plan for Private DNS Zones

Use your own custom domain names

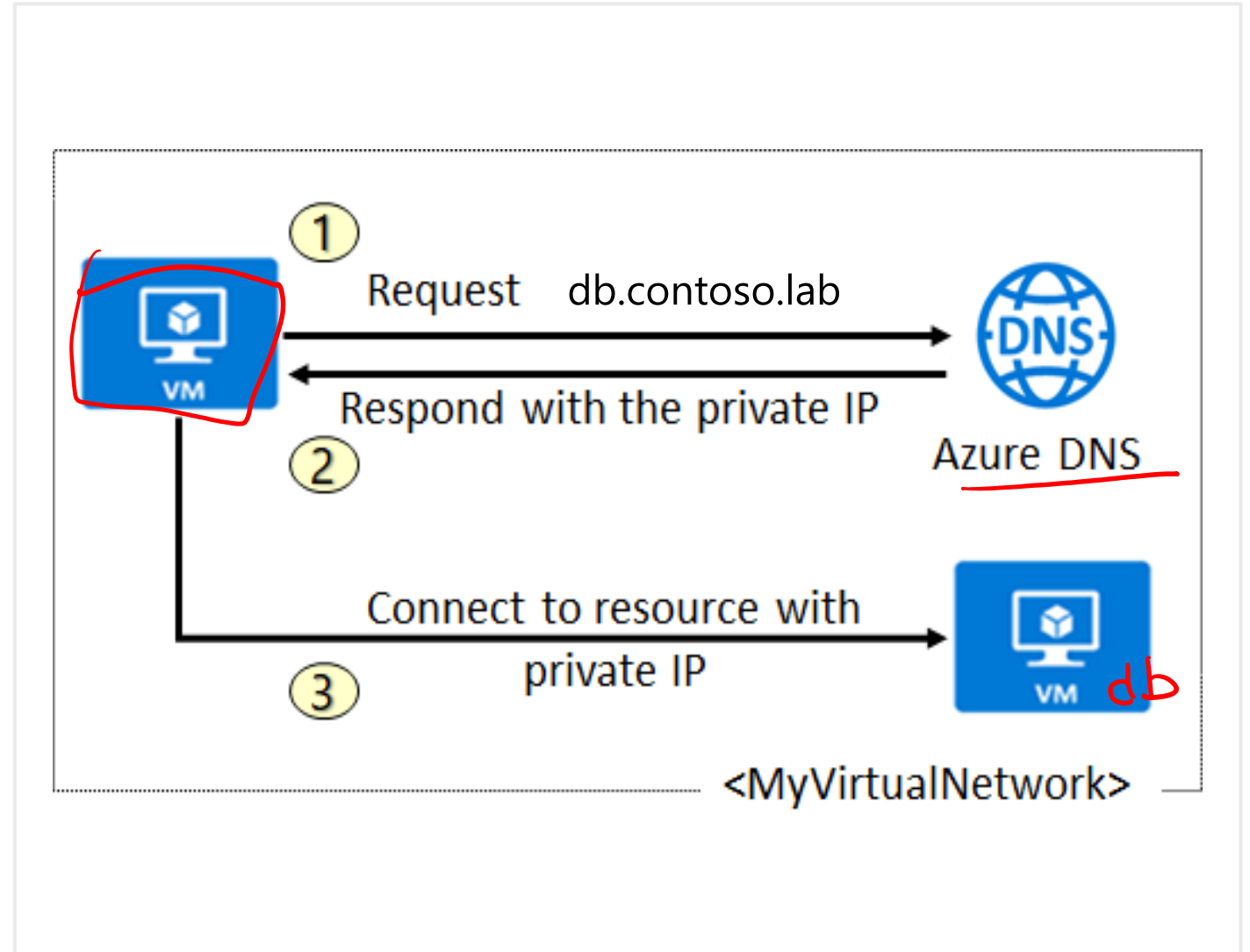
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

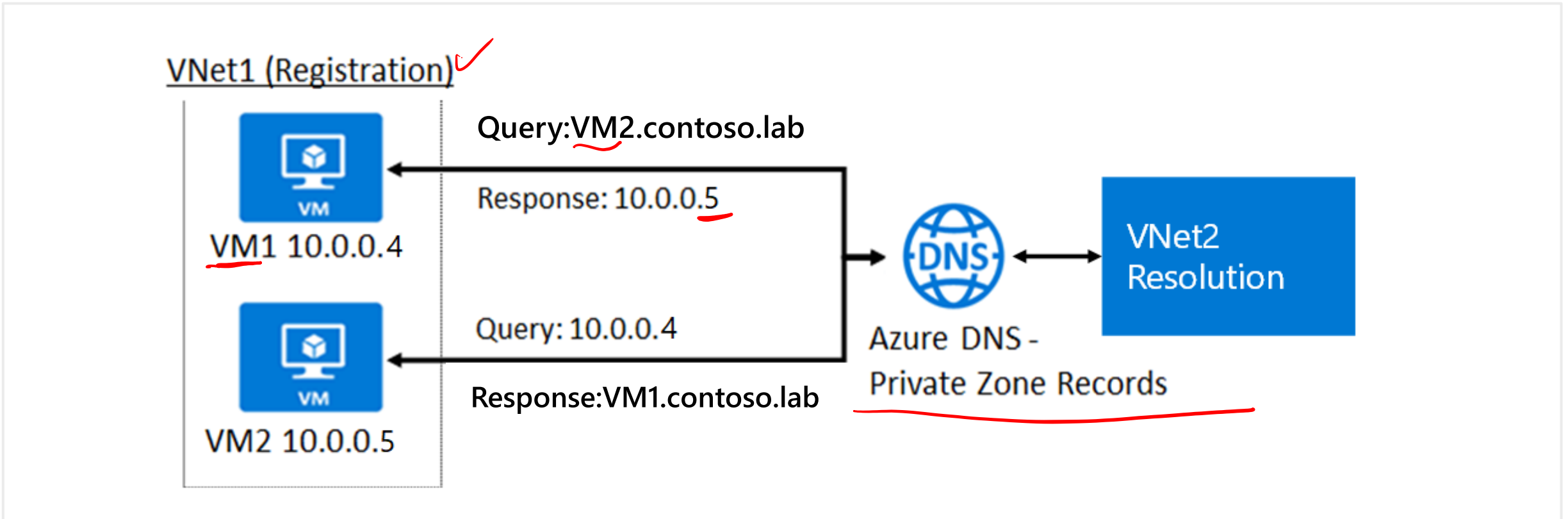
Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



Determine Private Zone Scenarios

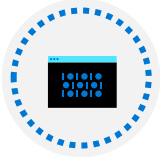


DNS resolution in VNet1 is private and not accessible from the Internet

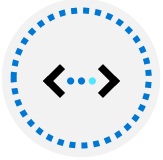
DNS queries across the virtual networks are resolved

Reverse DNS queries are scoped to the same virtual network

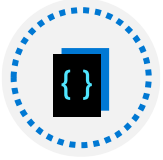
Demonstration - DNS



Create a DNS zone



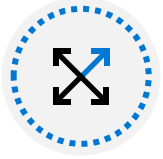
Add a DNS record set



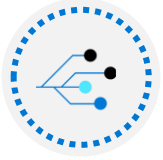
Use PowerShell to view DNS information



View your name servers



Test the resolution



Explore DNS metrics

Summary and Resources – Configure Azure DNS

Knowledge Check



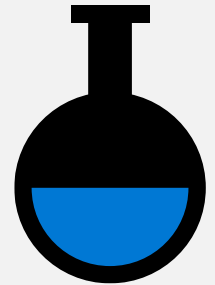
Microsoft Learn Modules (docs.microsoft.com/Learn)

[Host your domain on Azure DNS \(Sandbox\)](#)

[Implement DNS for Windows Server IaaS VMs](#)

A sandbox indicates a hands-on exercise.

Lab 04 – Implement Virtual Networks



Lab 04 – Implement Virtual Networking

Lab scenario

You plan to create a virtual network in Azure that will host a couple of Azure virtual machines. You will deploy them into different subnets of the virtual network. You also want to ensure that their private and public IP addresses will not change over time. To comply with Contoso security requirements, you need to protect public endpoints of Azure virtual machines accessible from Internet. Finally, you need to implement DNS name resolution for Azure virtual machines both within the virtual network and from Internet.

Objectives

Task 1:

Create and configure a virtual network

Task 2:

Deploy virtual machines into the virtual network

Task 3:

Configure private and public IP addresses of Azure VMs

Task 4:

Configure network security groups

Task 5:

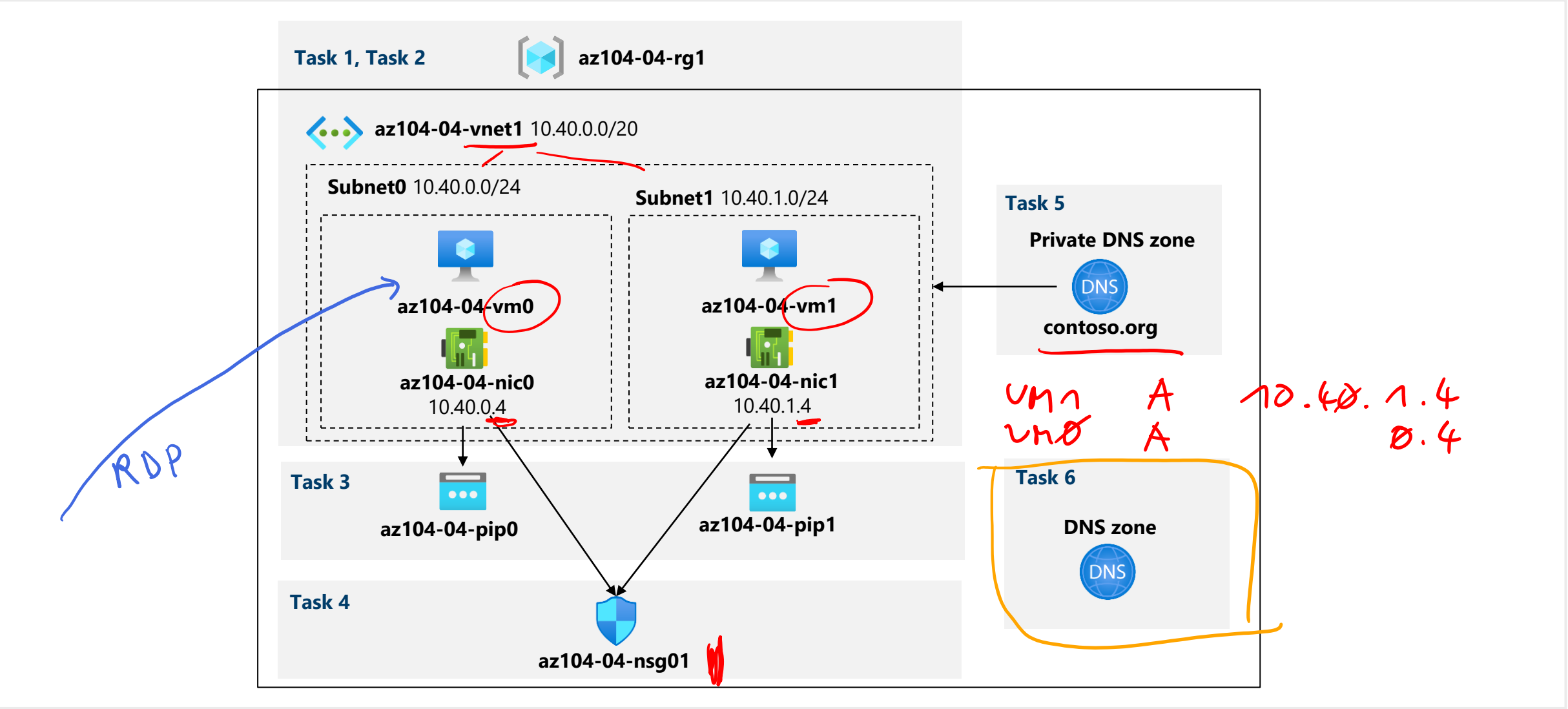
Configure Azure DNS for internal name resolution

Task 6:

Configure Azure DNS for external name resolution

Next slide for an architecture diagram 

Lab 04 – Architecture diagram



End of presentation

