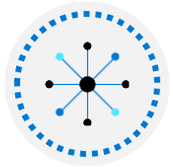
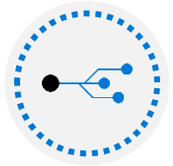
Microsoft Azure

AZ-104T00A Administer Virtual Networking

Administer Virtual Networking Introduction



Configure Virtual Networks



Configure Network Security Groups

Configure Azure Firewall

Configure Azure DNS

Lab 04 – Implement Virtual Networks

Configure Virtual Networks

Configure Virtual Networks Introduction


Plan Virtual Networks


Create Subnets

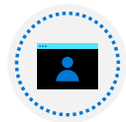

Create Virtual Networks


Plan IP Addressing


Create Public IP Addresses

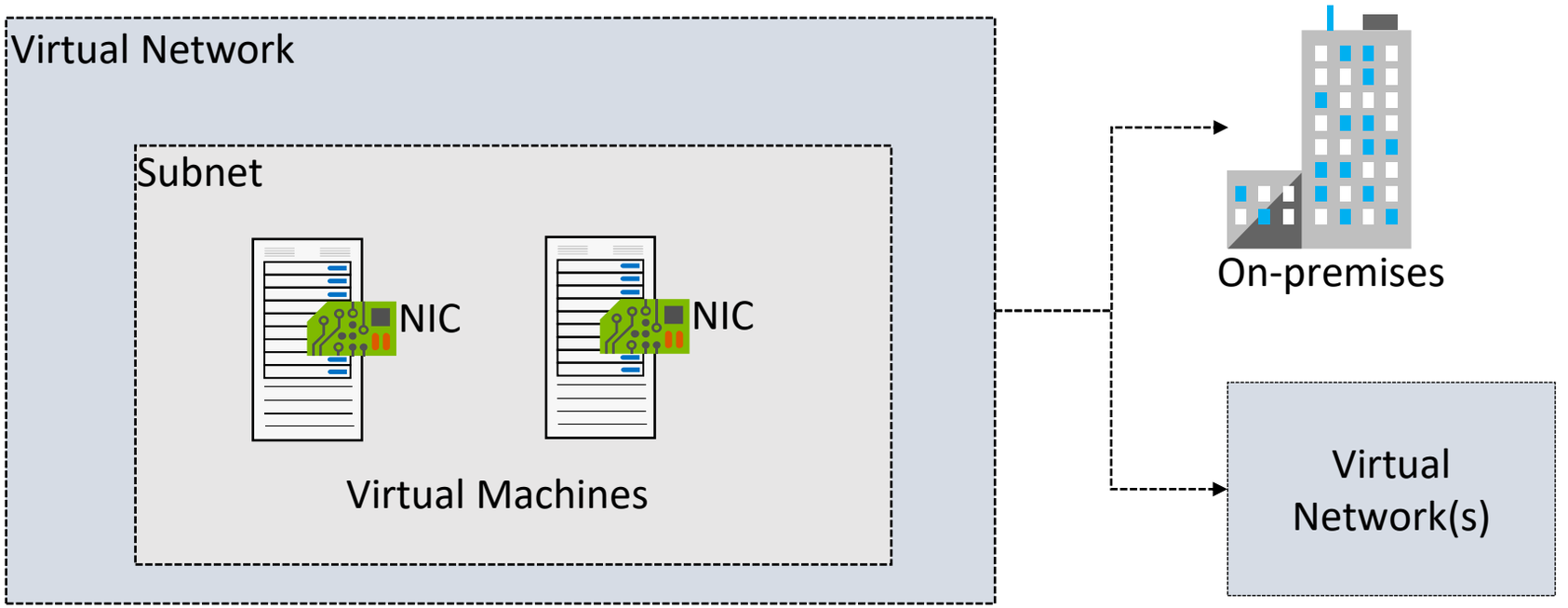

Associate Public IP Addresses


Associate Private IP Addresses


Demonstration – Virtual Networks


Summary and Resources

Plan Virtual Networks



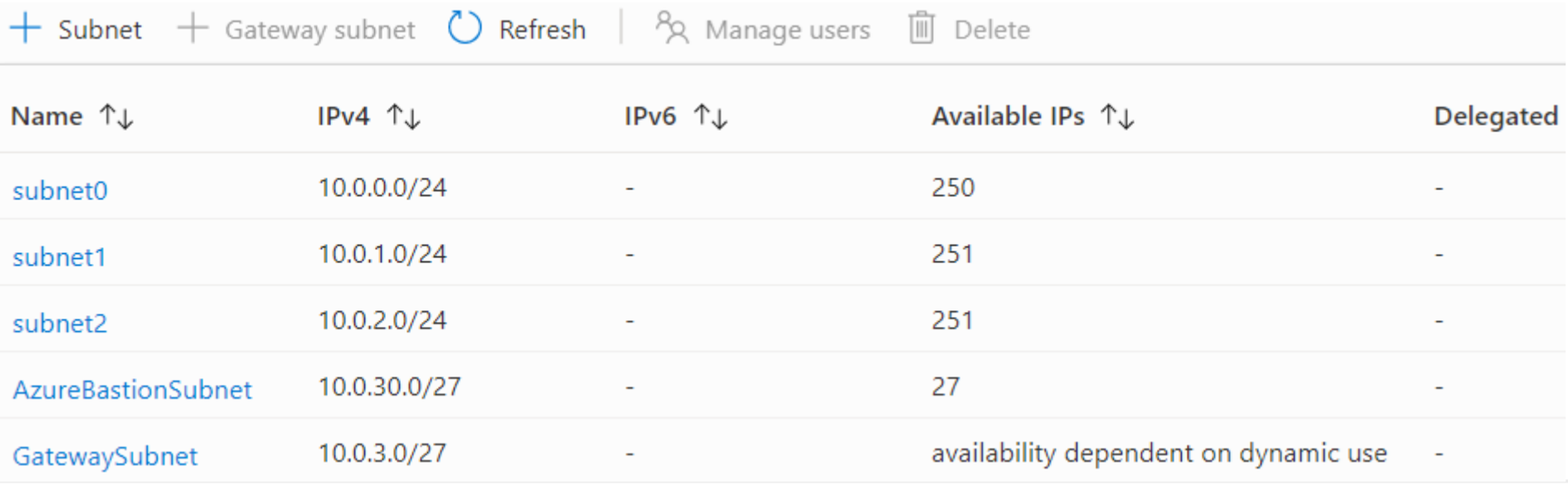
Logical representation of your own network

Create a dedicated private cloud-only virtual network

Securely extend your datacenter with virtual networks

Enable hybrid cloud scenarios

Create Subnets



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

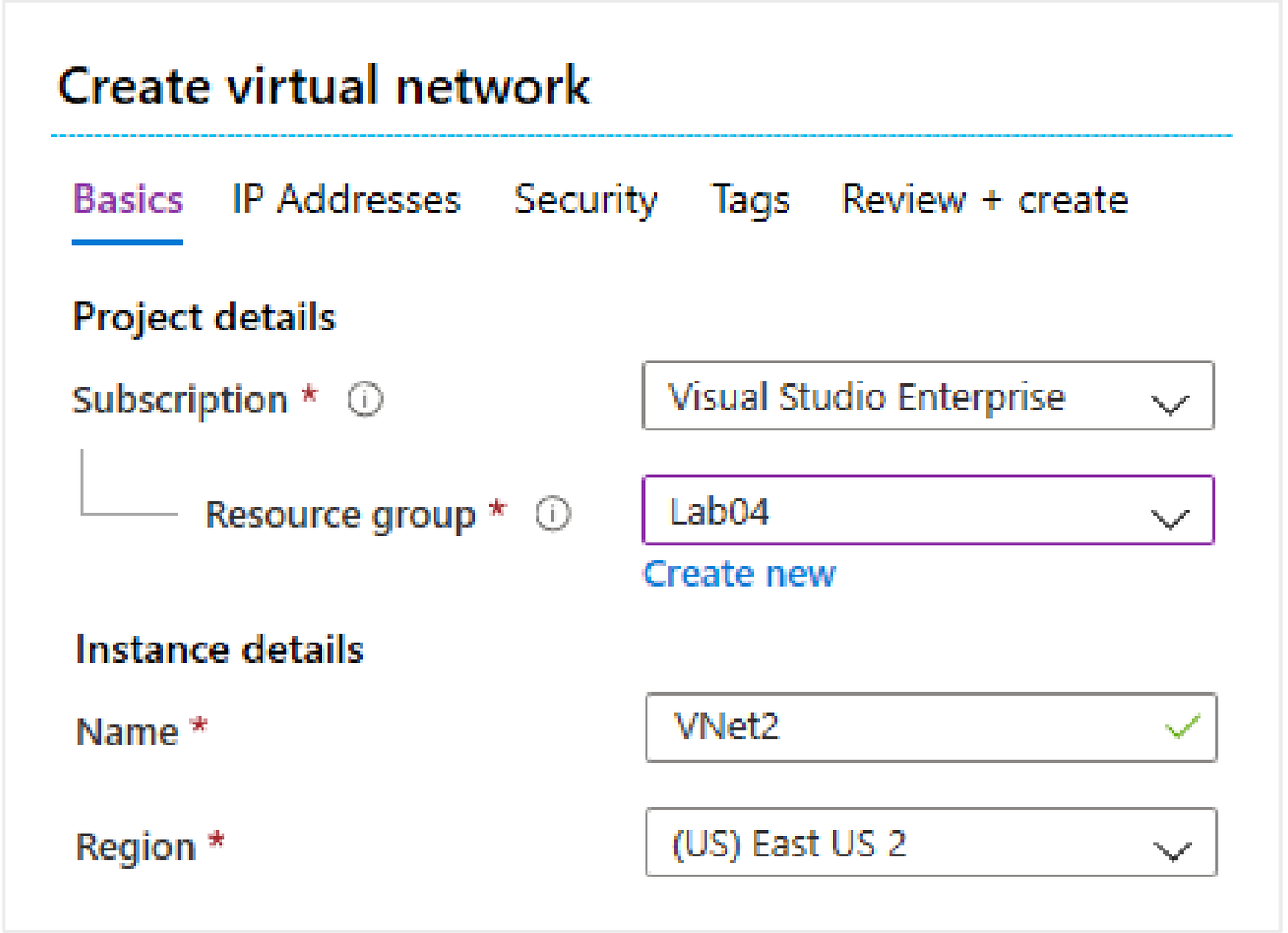
Create Virtual Networks

Create new virtual networks at any time

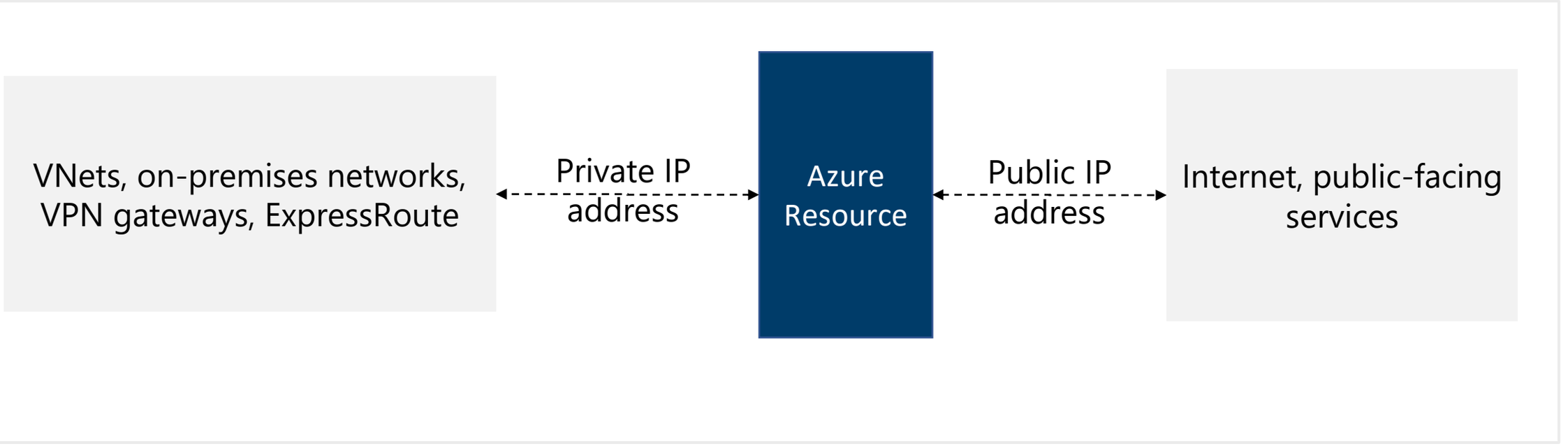
Add virtual networks when you create a virtual machine

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

Be careful with overlapping address spaces



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

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

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.

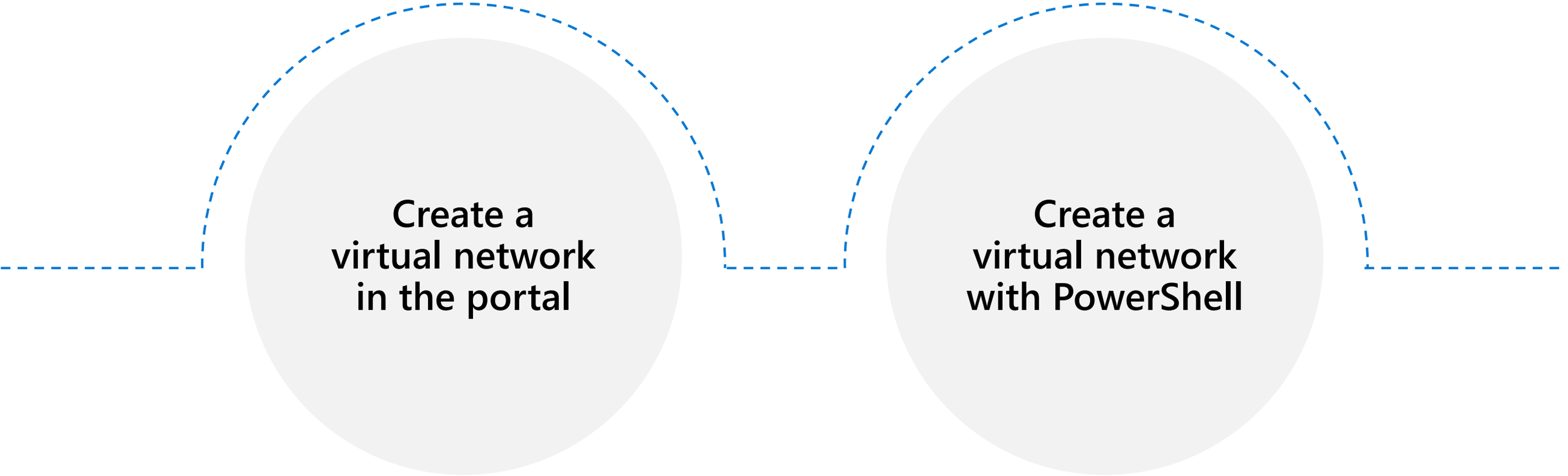
Associate Private IP Addresses

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

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



Summary and Resources – Configure Virtual Networks

Knowledge Check

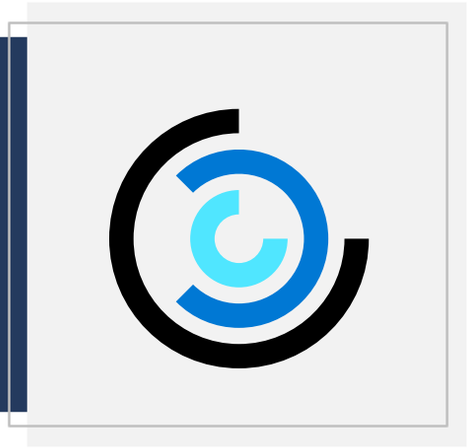
Microsoft Learn Modules (docs.microsoft.com/Learn)

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

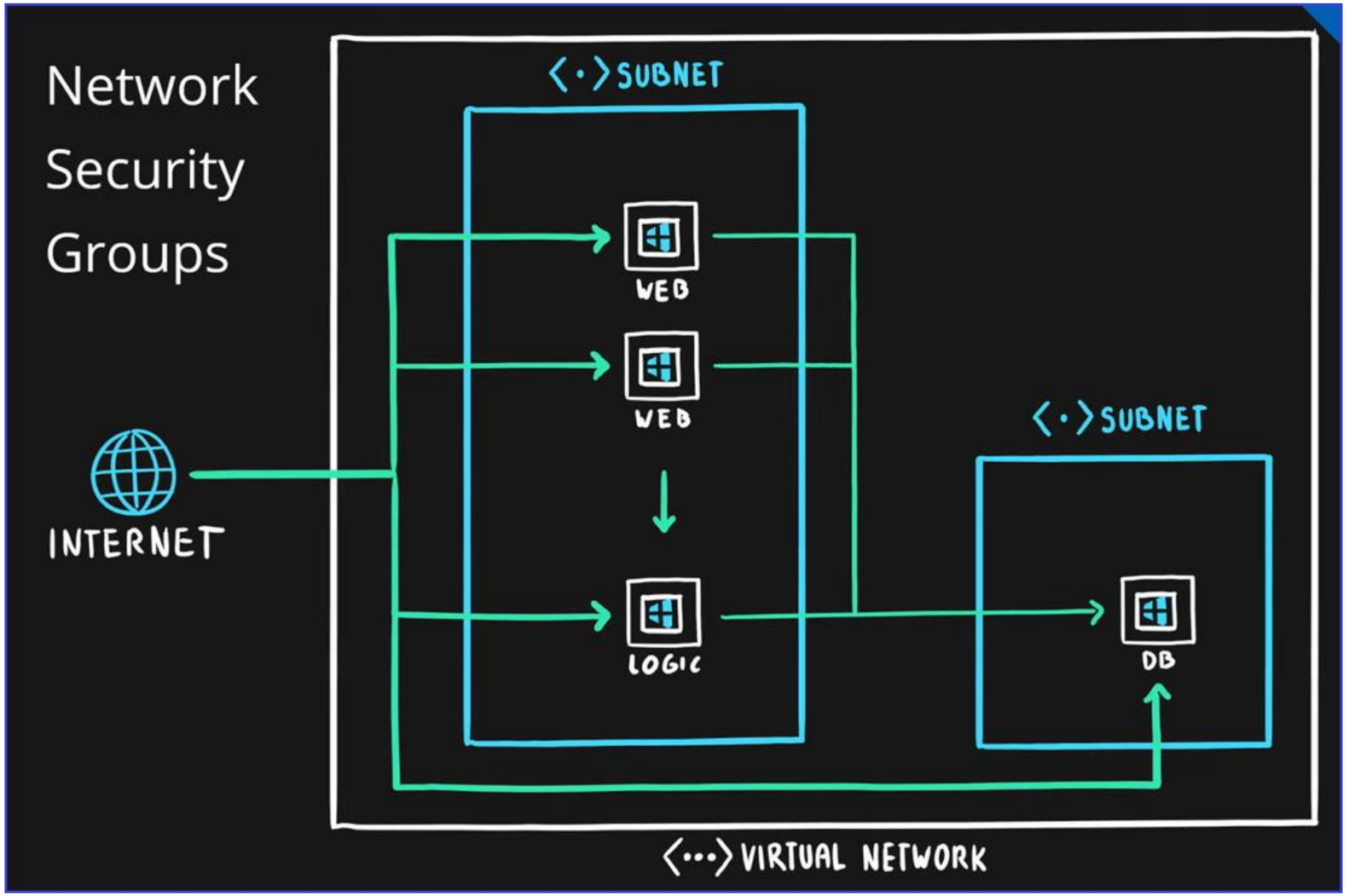
Create NSG Rules

Implement Application Security Groups (ASGs)

Demonstration – NSGs

Summary and Resources

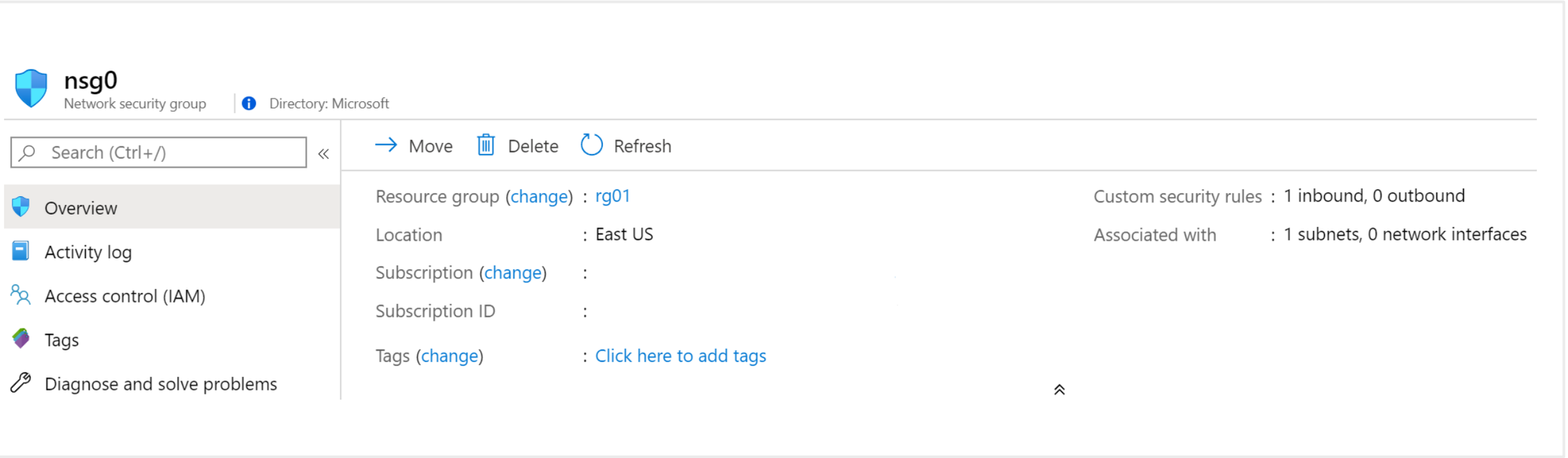
Implement Network Security Groups (NSGs)



NSG는 기본적으로
Internet에서 접속하는
모든 Traffic에 대하여
차단 및 허용하는 것이다

적용은 VM의 NIC 및 Subnet

Implement Network Security Groups (NSGs)



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

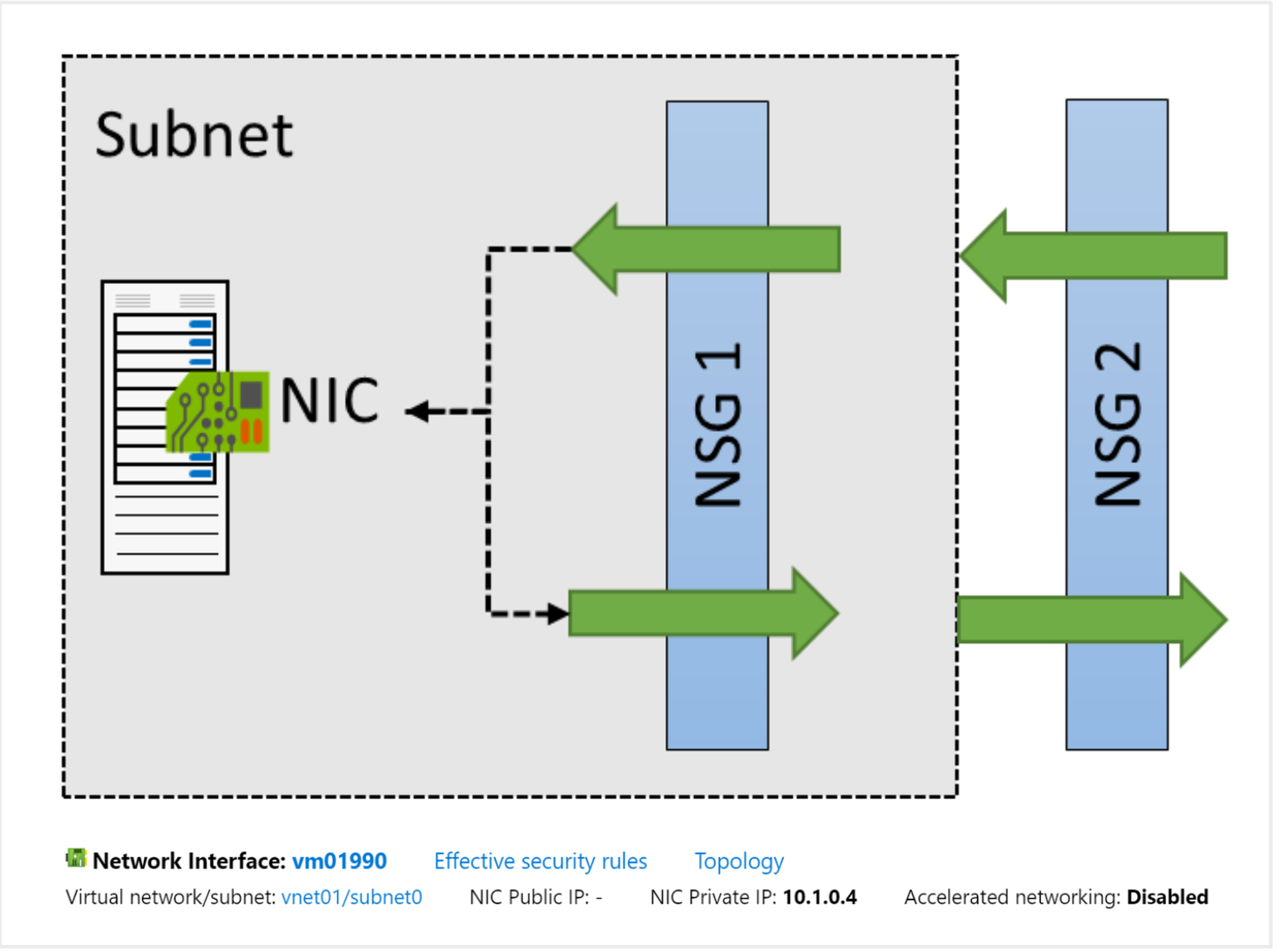
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

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



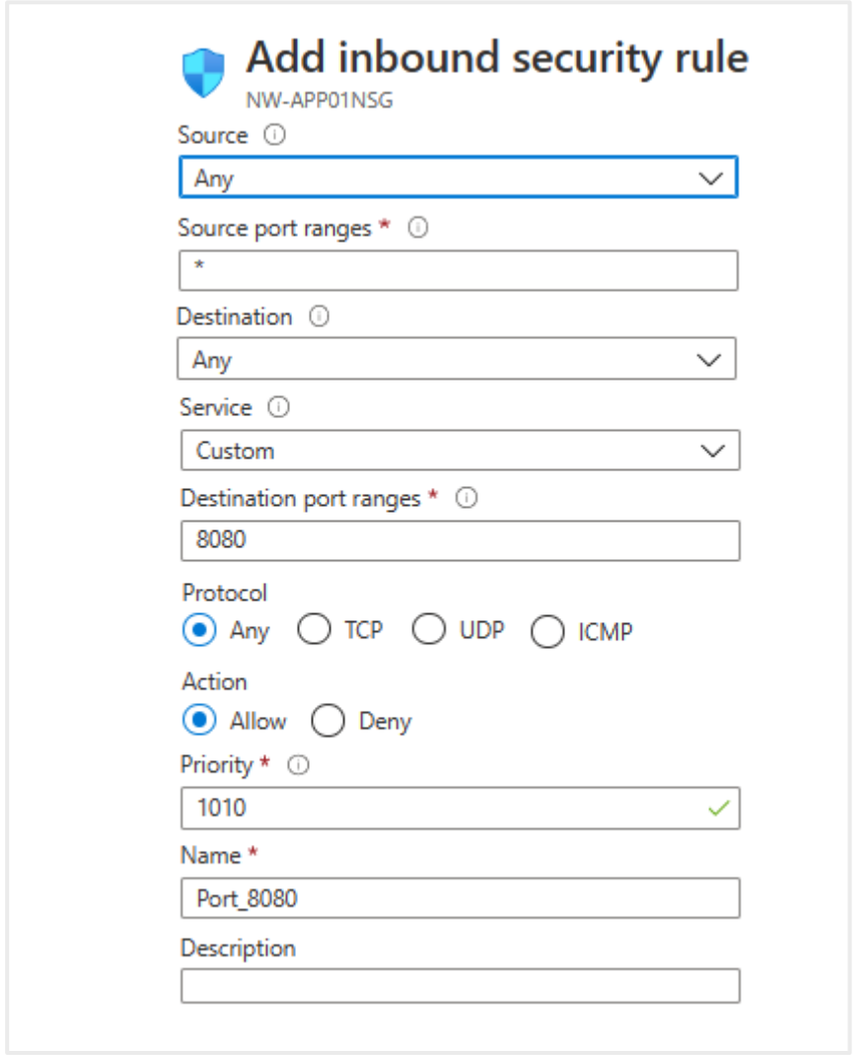
Create NSG rules

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

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

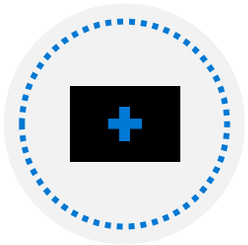
Service (HTTPS, SSH, RDP, DNS, POP3, custom, …)

Priority – The lower the number, the higher the priority

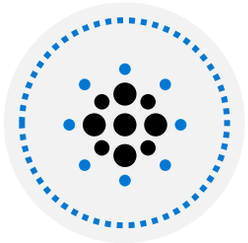


Demonstration – Network Security Groups

Access the NSGs blade



Add a new NSG



Explore inbound and outbound rules

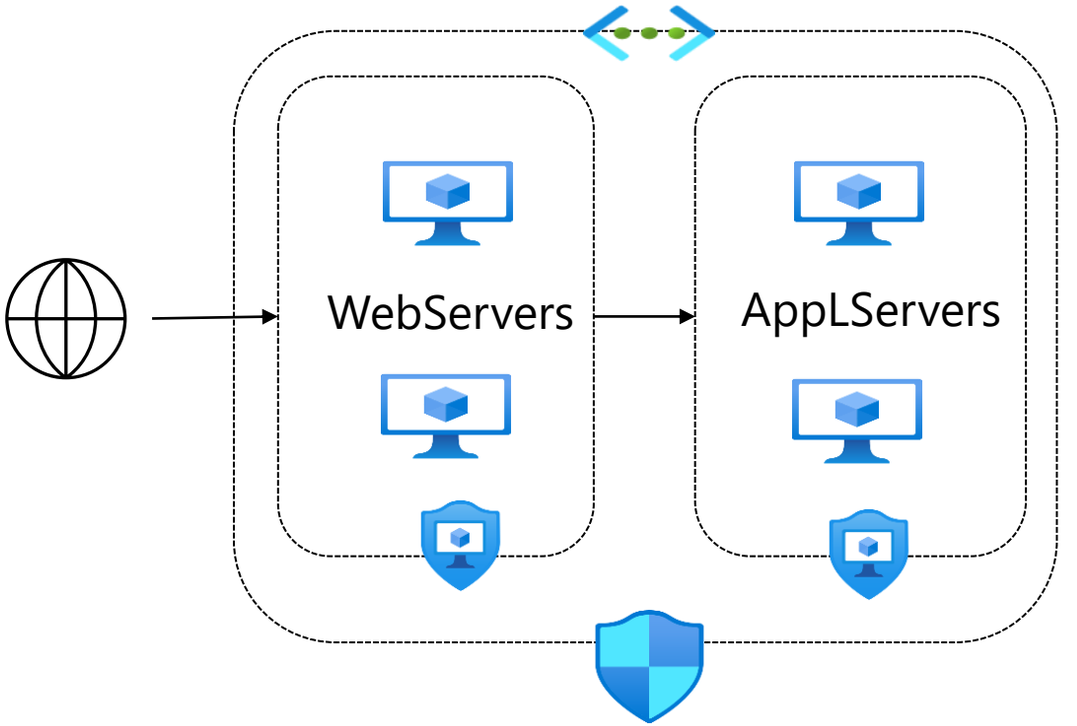
Implement Application Security Groups

Extends your application's structure

ASGs logically group virtual machines – web servers, application servers

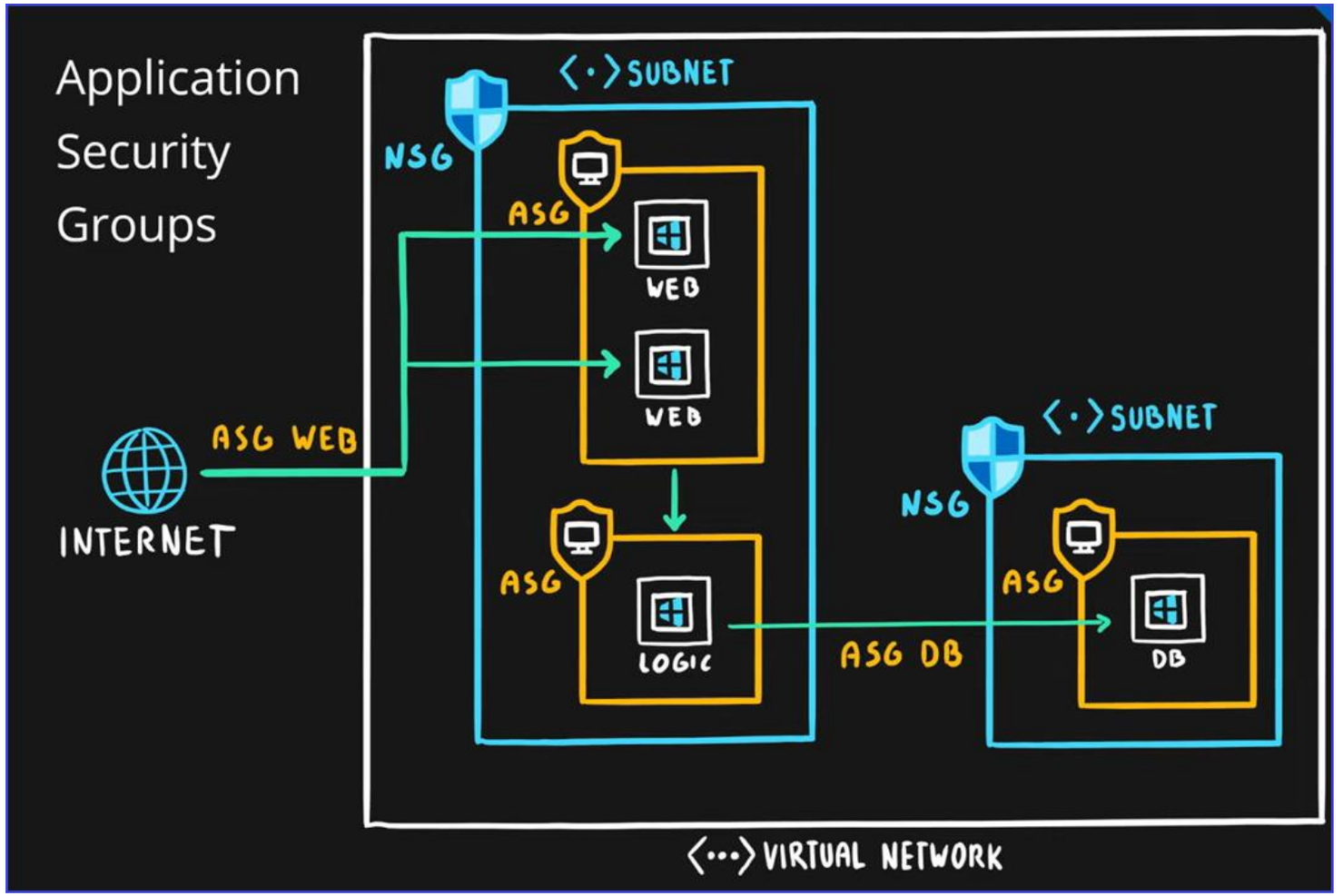
Define rules to control the traffic flow

Wrap the ASG with an NSG for added security

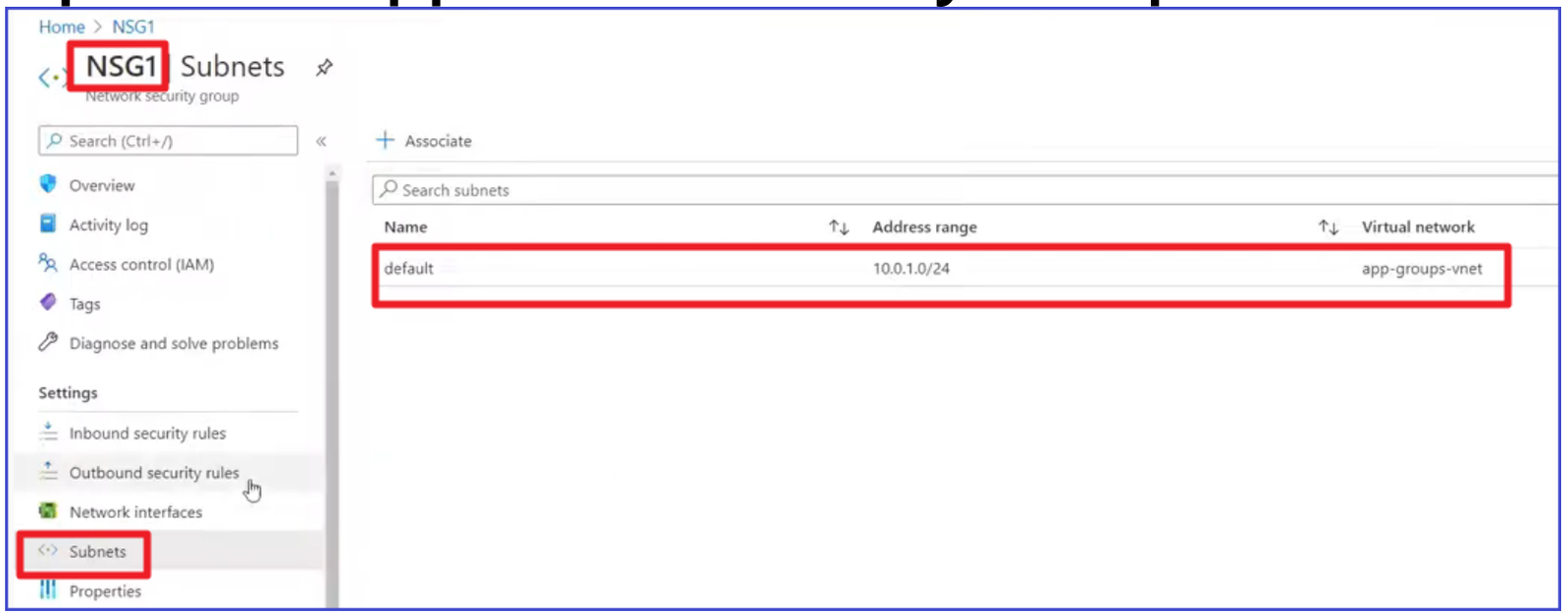


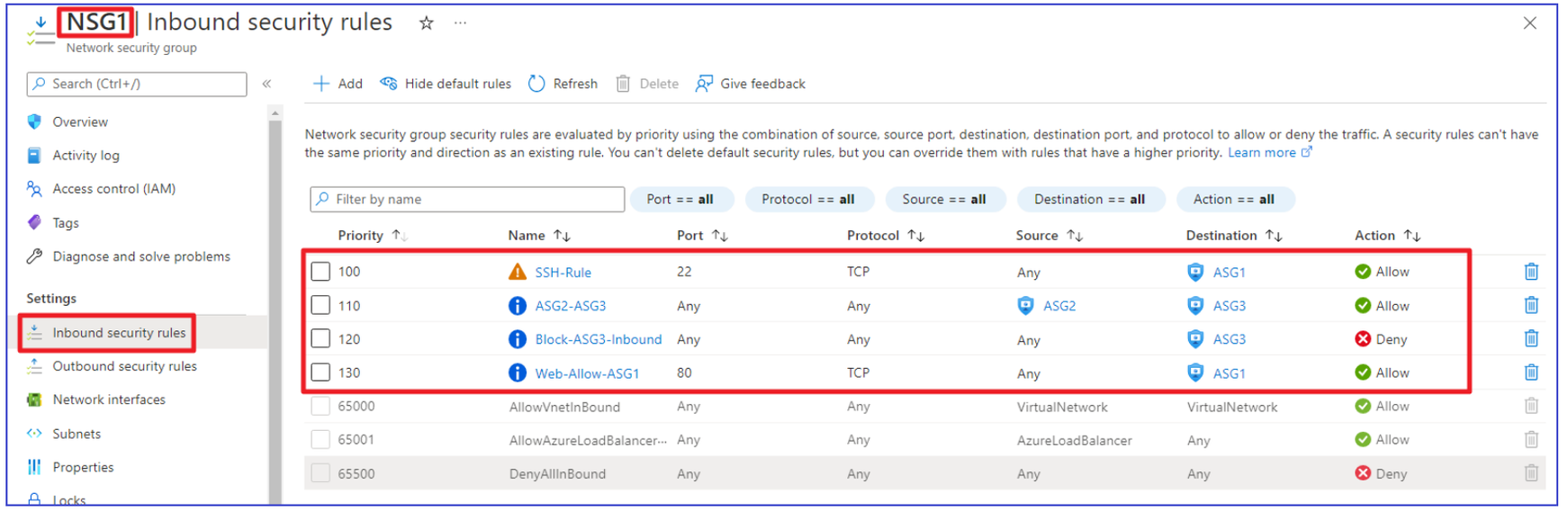
Source	Destination	Port
Internet	WebServers	80, 443
WebServers	SQLServers	1533

Implement Application Security Groups



Implement Application Security Groups





Implement Application Security Groups

- Vnet-HQ라는 Virtual Network을 기본으로 생성한다(subnet은 default)
- Linux VM 3개 준비한 후 nginx 설치하고 시작한다(NSG는 none으로 한다)

  (Virtual Network은 Vnet-HQ로 지정 / Win10에서 nginx web serve에 접속이 안되는지 확인한다)
- Application Security Group 3개 준비하여 각 VM에 적용한다-ASG1, ASG2, ASG3

  (각 VM의 networking에 가서 Application Security Groups에서 ASG1, ASG2, ASG3을 적용한다)
- Network Security Group(NSG1) 1개 준비하여 Subnet에 적용

  (Vnet-HQ의 default 서브넷에 연결한다 → 드디어 Vnet-HQ의 default에 NSG가 적용됨)
- NSG1에 Application Security Group들을 앞 그림과 같이 적용
  - 외부에서 VM1에 ssh로 접속한다(성공)
  - 외부에서 VM1의 web server에 접속한다(성공) / VM2와 VM3에 web server 접속을 실패
  - ssh로 접속한 VM1에서 VM3로 ping을 한다(실패)
  - VM1에서 VM2로 ping을 한다(성공)
  - VM1에서 ssh로 VM2로 접속한다(성공)
  - VM2에서 VM3로 ping을 한다(성공)

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)

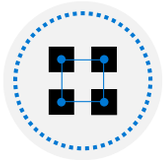
A *sandbox* indicates a hands-on exercise.

Lesson 03: Configure Azure Firewall

Configure Azure Firewall Introduction

Determine Azure Firewall Uses

Create Azure Firewalls



Create Azure Firewall Rules

Summary and Resources

Determine Azure Firewall Uses

Stateful firewall as a service

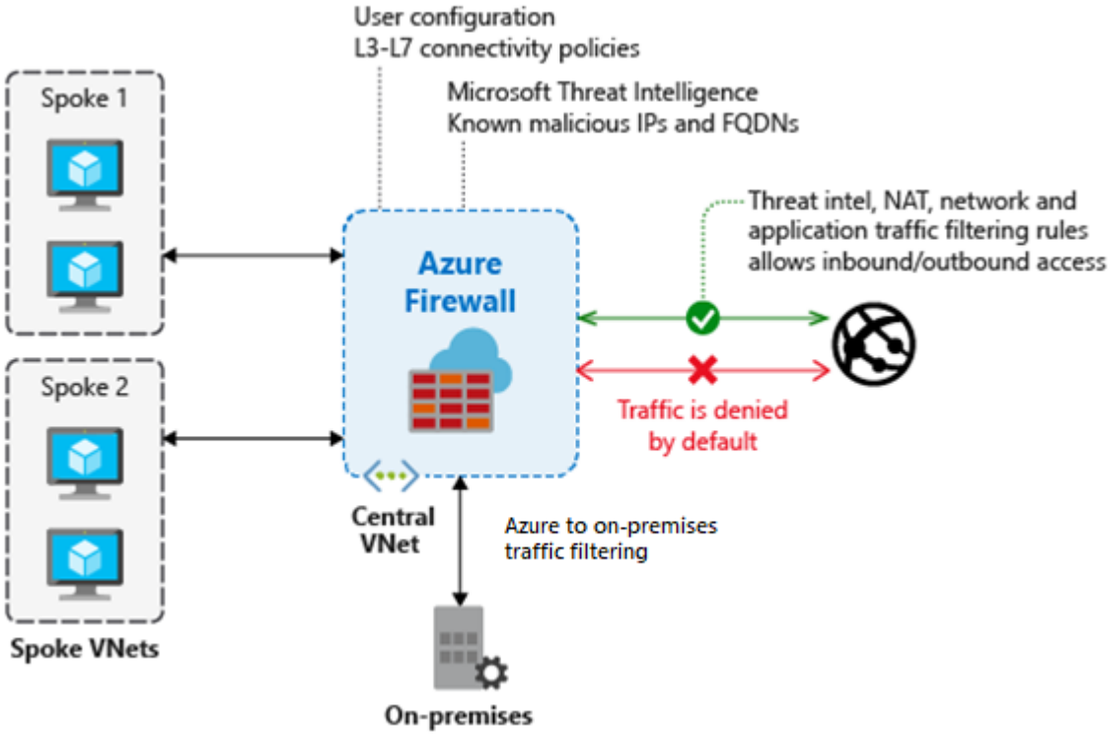
Built-in high availability with unrestricted cloud scalability

Create, enforce, and log application and network connectivity policies

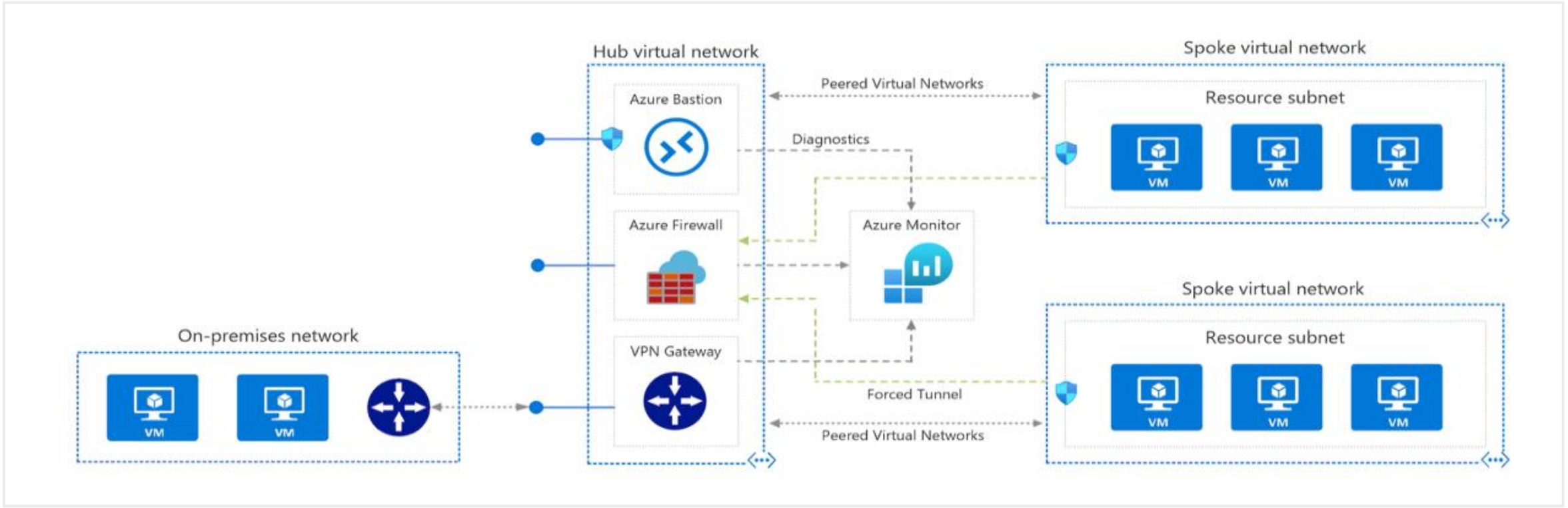
Threat intelligence-based filtering

Fully integrated with Azure Monitor for logging and analytics

Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways



Create Azure Firewalls



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

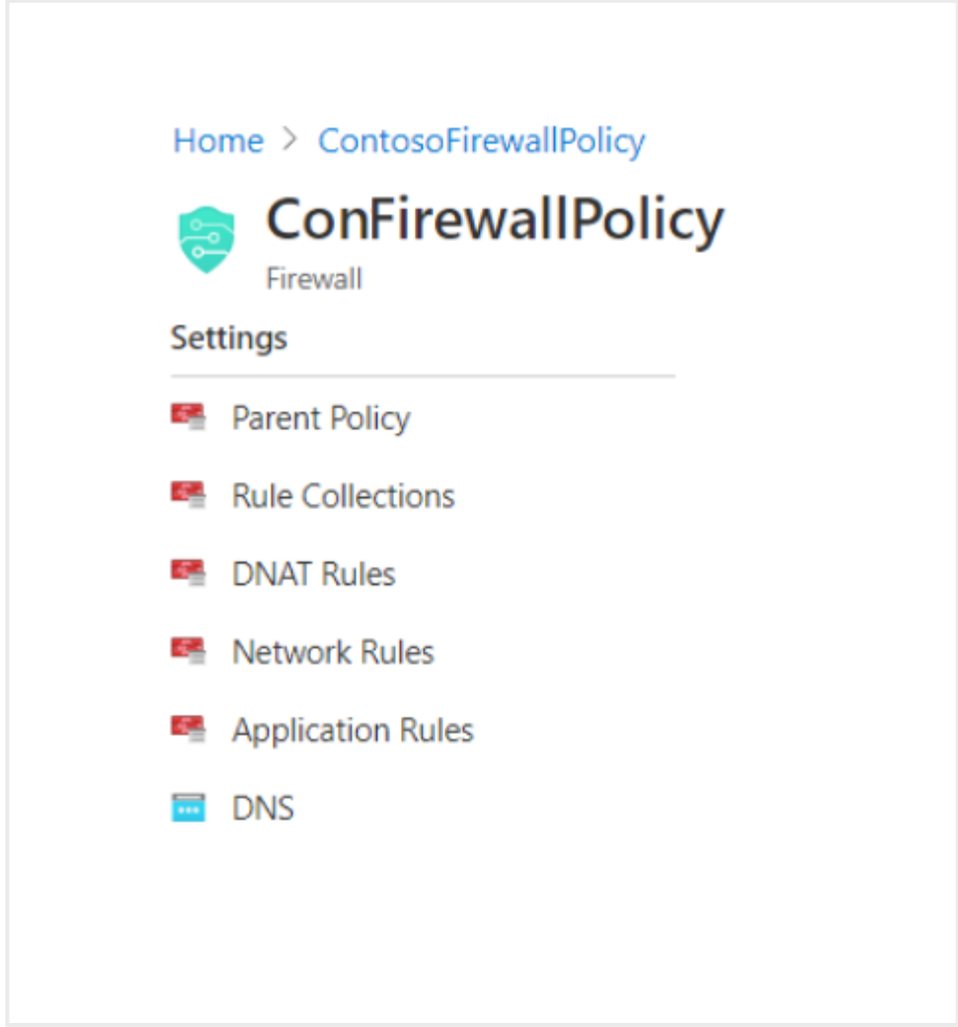
Azure Firewall Manager centralizes firewall management

Firewall policies container rules and settings to control access

NAT rules allow incoming connections

Network rules contain source and destination addresses, protocols, and destination ports

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



Summary and Resources - Azure Firewall

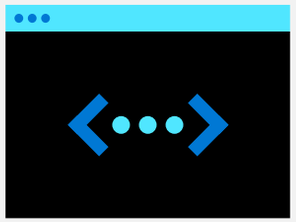
Knowledge Check

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

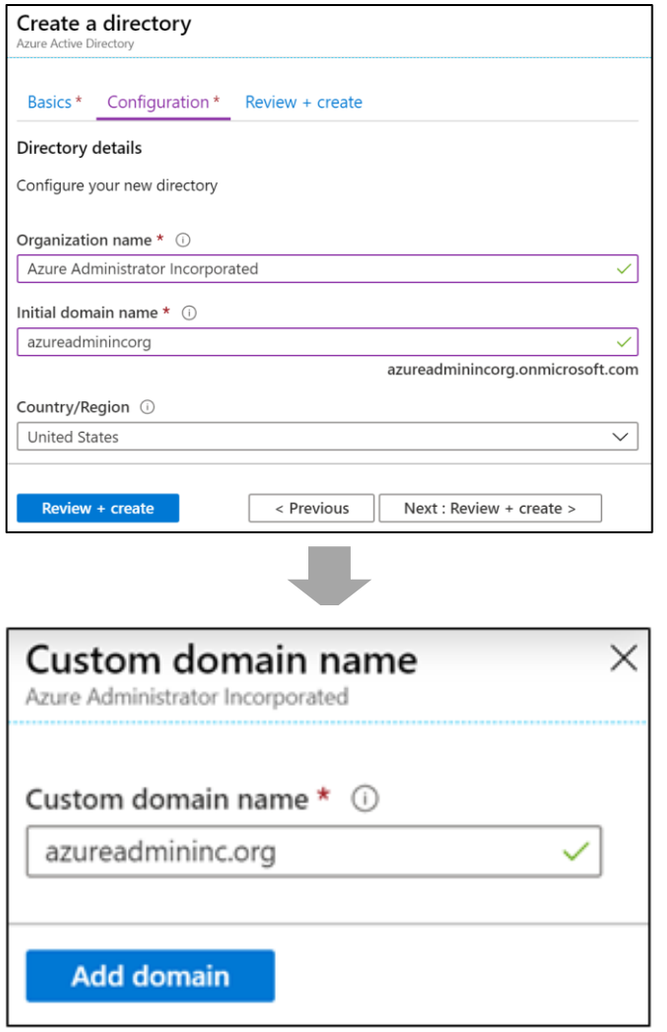
Identity Domains and Custom Domains

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

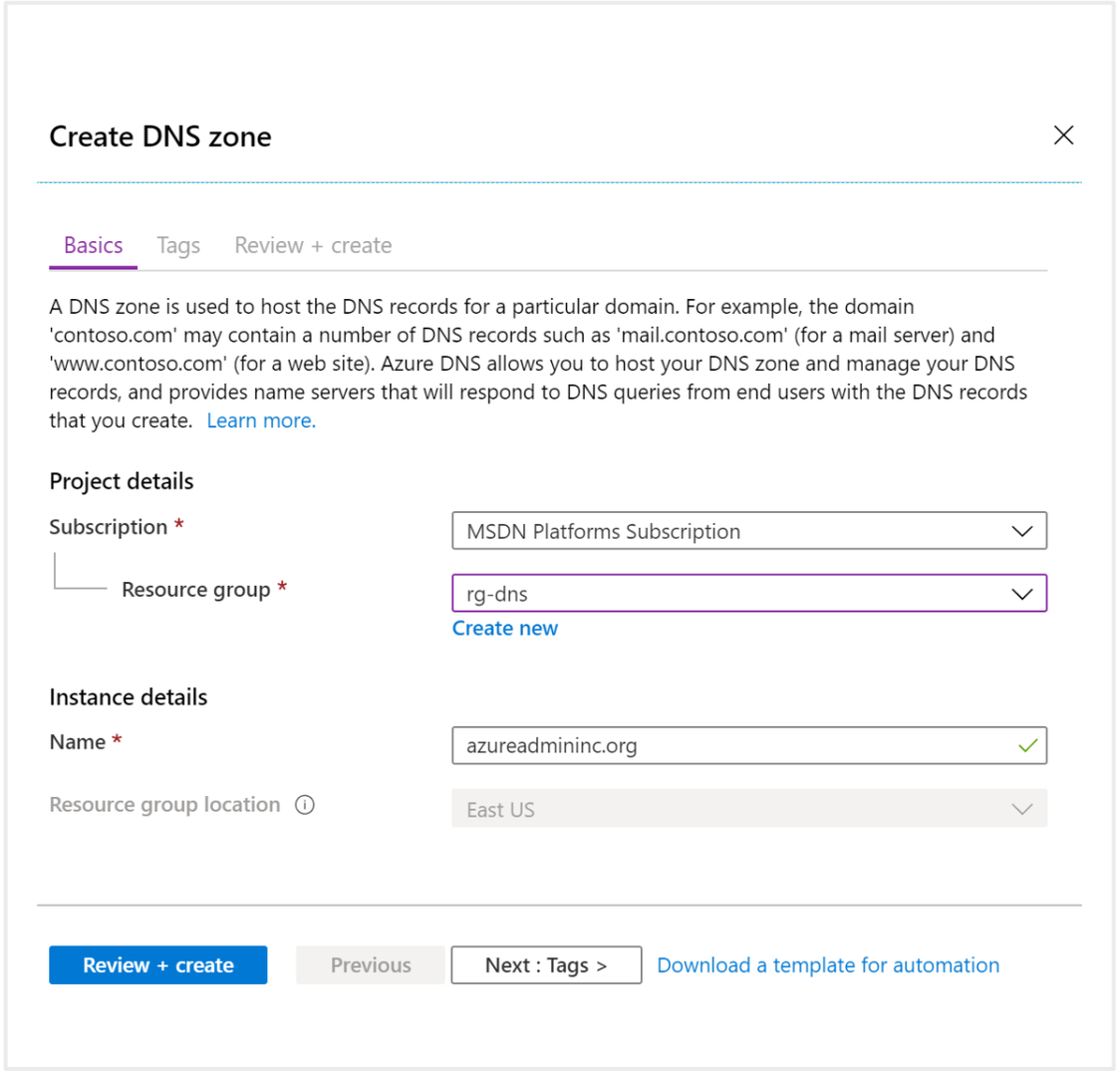


Create Azure DNS Zones

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

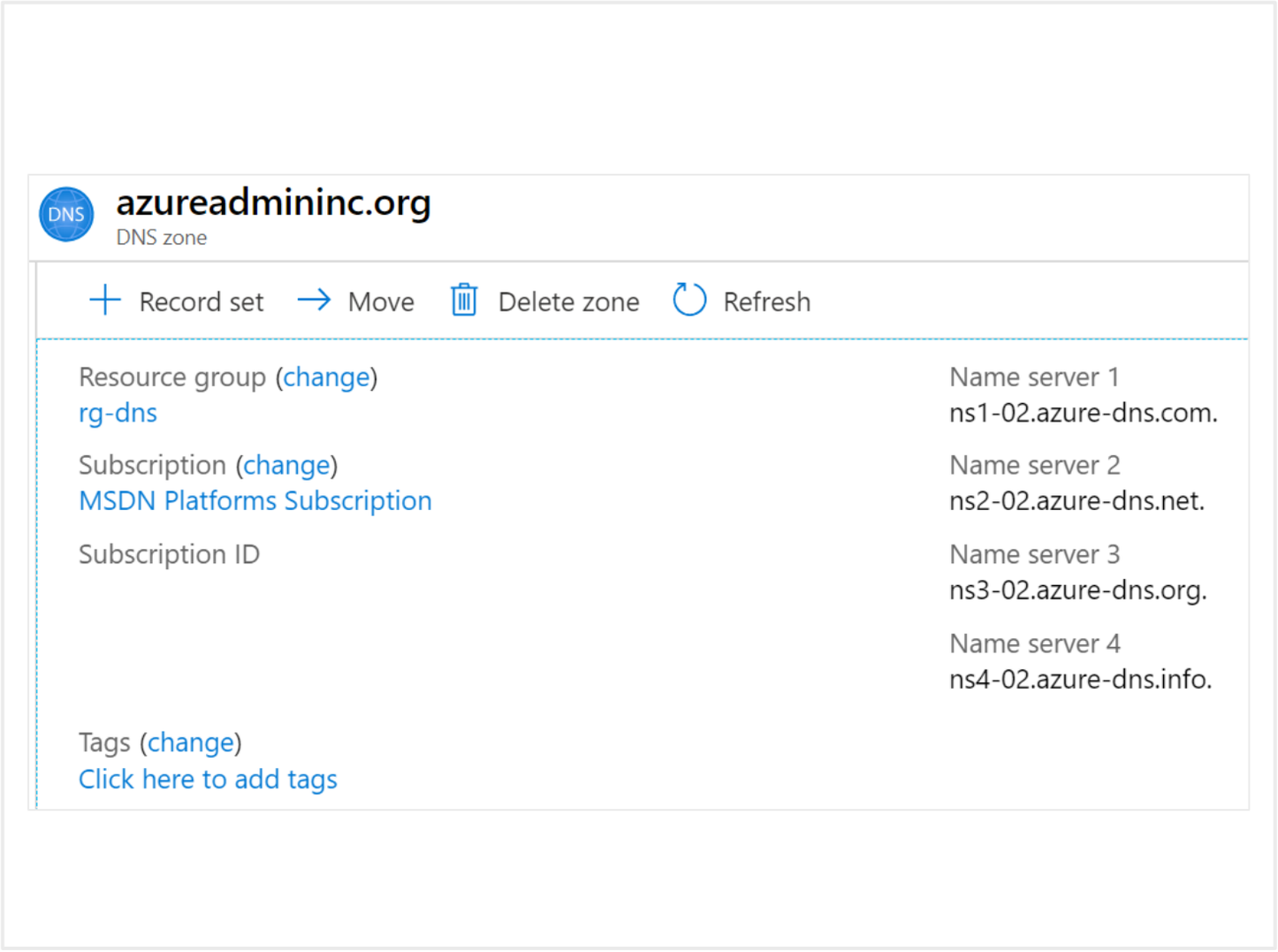


Delegate DNS Domains

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



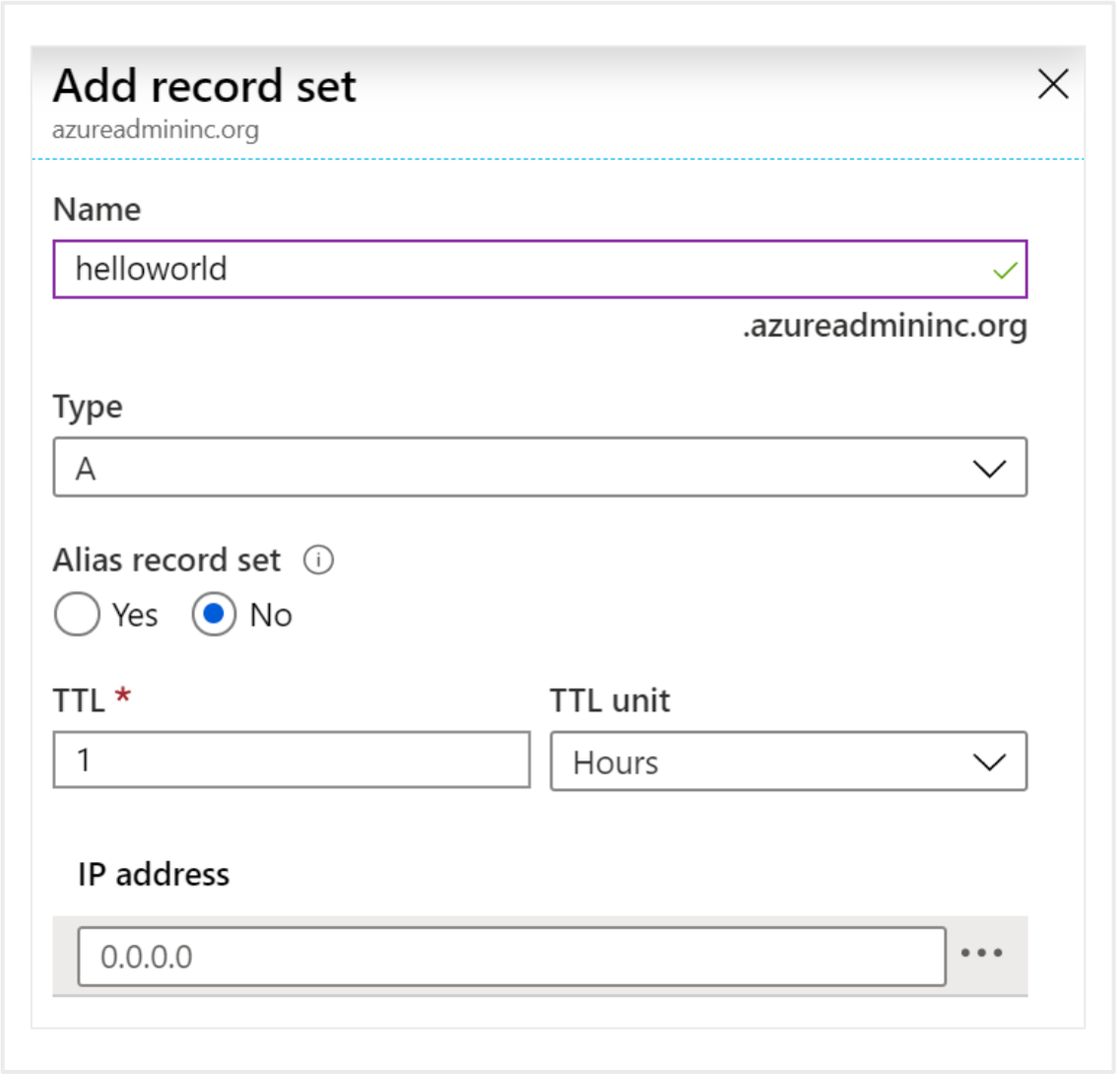
Add DNS Record Sets

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



Plan for Private DNS Zones

Use your own custom domain names

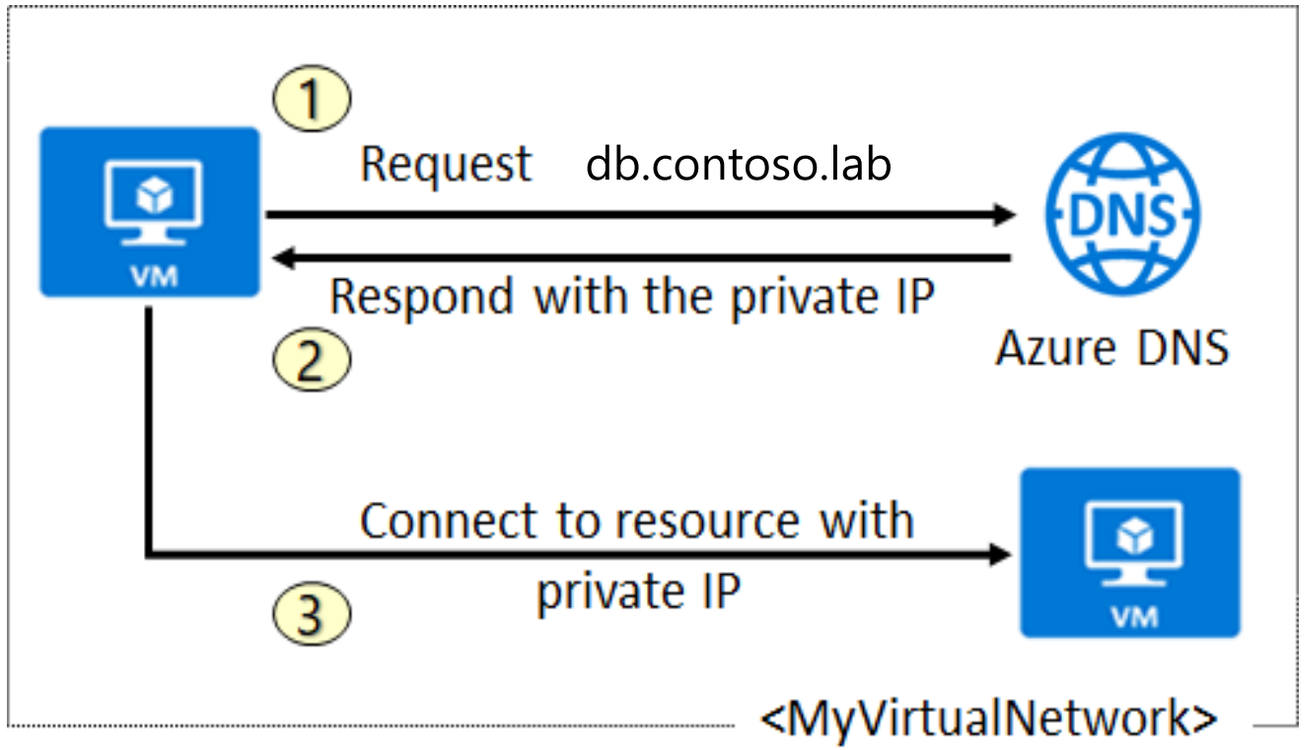
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

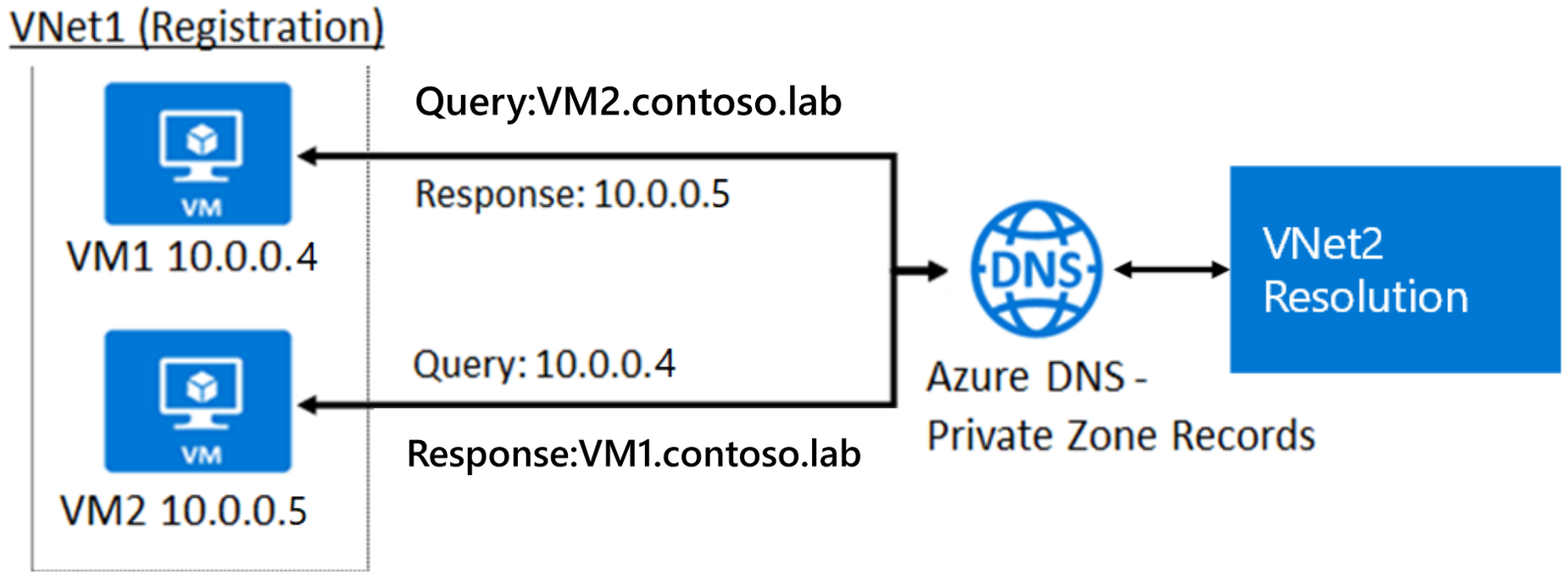
Removes the need for custom DNS solutions

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

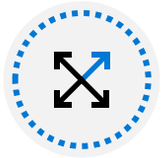
Demonstration - DNS

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

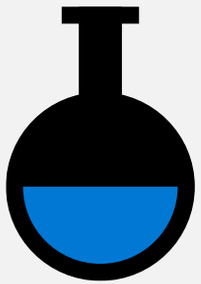
Microsoft Learn Modules (docs.microsoft.com/Learn)

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

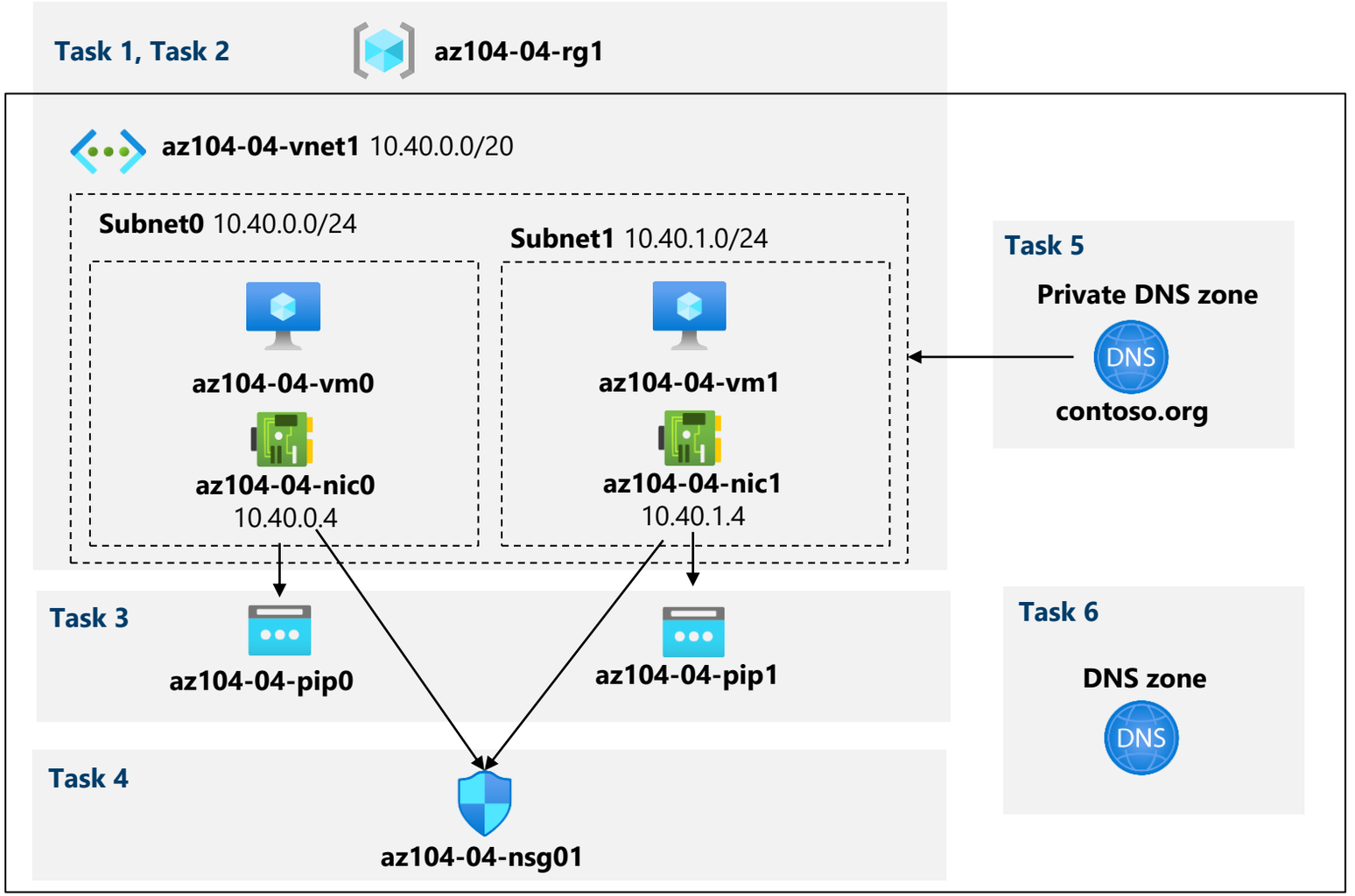
Task 4:
Configure network security groups

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