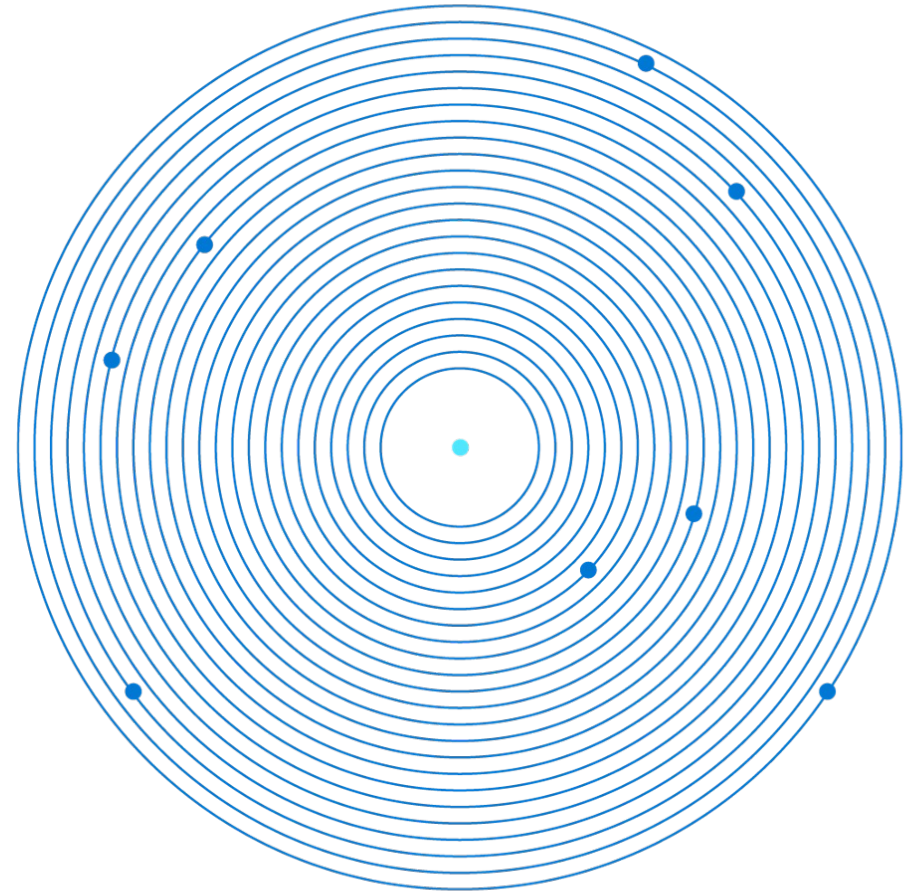


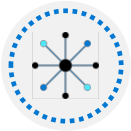
AZ-104T00A

Module 04:

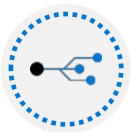
Virtual Networking



Module Overview



Lesson 01: Virtual Networks



Lesson 02: IP Addressing



Lesson 03: Network Security Groups



Lesson 04: Azure Firewall

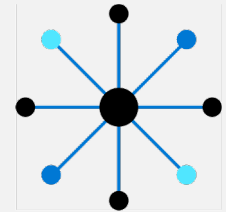


Lesson 05: Azure DNS

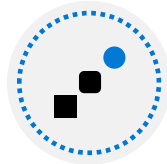


Lesson 06: Module 04 Lab and Review

Lesson 01: Virtual Networks



Virtual Networks Overview



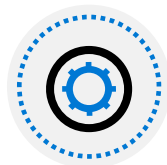
Azure Networking Components



Virtual Networks



Subnets



Implementing Virtual Networks



Demonstration – Creating Virtual Networks

Azure Networking Components

Adopting cloud solutions can save time and simplify operations

Azure requires the same types of networking functionality as on-premises infrastructure

Azure networking offers a wide range of services and products



Virtual Network

Microsoft

Create a logically isolated section in Microsoft Azure and securely connect it outward.



Load Balancer

Microsoft

A load balancer that distributes incoming traffic among backend virtual machine instances.



Application Gateway

Microsoft

Scalable layer-7 load balancer offering various traffic routing rules and SSL termination for backend



Traffic Manager profile

Microsoft

Create a Microsoft Azure Traffic Manager Profile that allows you to control the distribution of user



Virtual network gateway

Microsoft

The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN



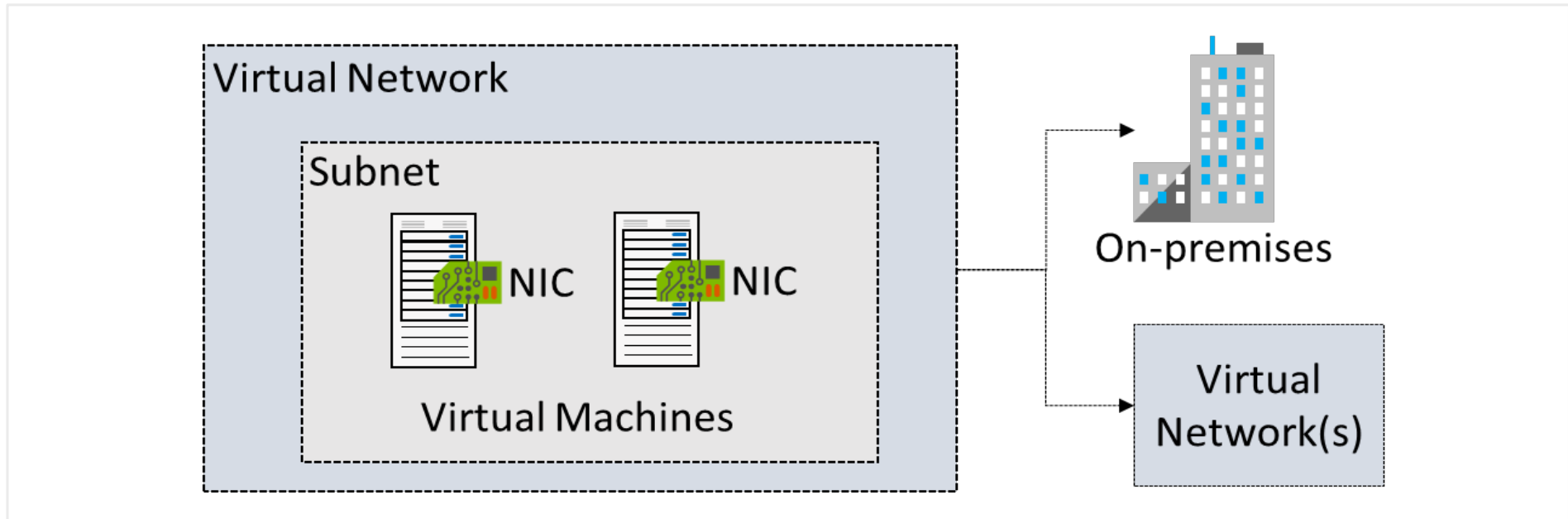
Virtual WAN

Microsoft

Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch



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

Subnets

Subnet

Gateway subnet

Refresh

Search subnets

Name	↑↓	Address range	↑↓	IPv4 available addresses	↑↓	Delegated to	↑↓	Security group
subnet0		10.1.0.0/24		251		-		nsg0
subnet1		10.1.1.0/24		251		-		-
subnet2		10.1.2.0/24		251		-		nsg2
GatewaySubnet		10.1.255.0/24		251		-		-

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

IPs that reserved on each subnet

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

Implementing 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

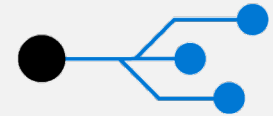


Region *

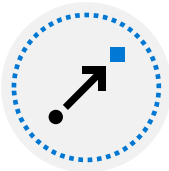
(US) East US 2



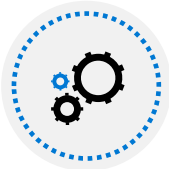
Lesson 02: IP Addressing



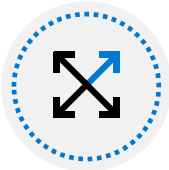
IP Addressing Overview



IP Addressing



Creating IP Addresses

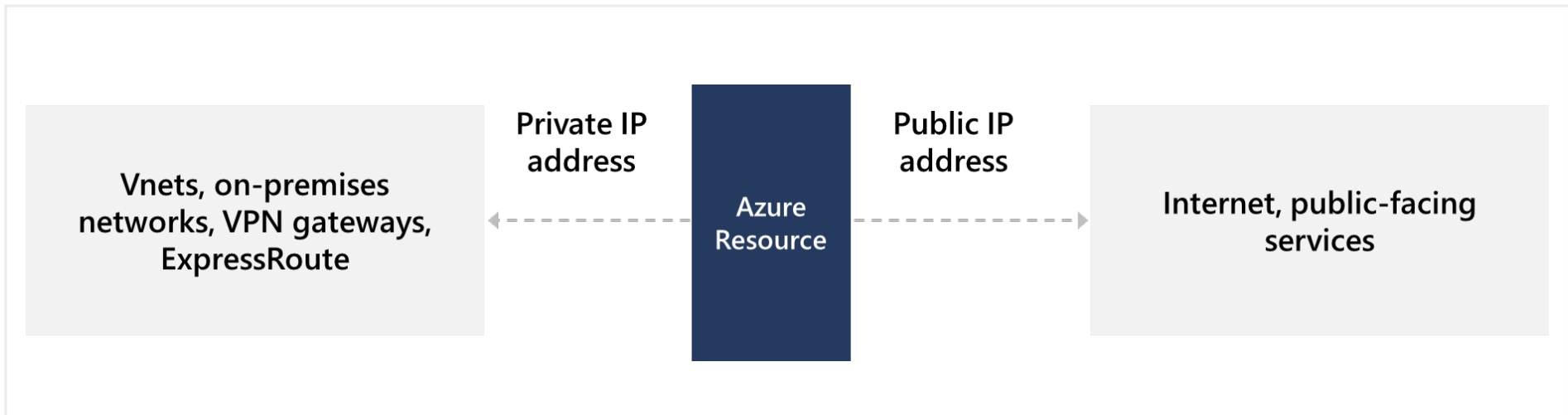


Public IP Addresses



Private IP Addresses

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

Creating Public IP Addresses

Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Available in Dynamic, Static or both
(depending on SKU):

Zone redundant

Not mixable or immutable

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 *

IP address assignment *

☒ Dynamic ☐ Static

Public IP SKUs

Basic SKU

- do not support Availability zones
- Availability zone settings is set to non by default

Standard SKU

- Public IP can be associated to a VM or a load balancer front end
- Availability zone settings is set to Zone-Redundant by default

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.

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

Lesson 03: Network Security Groups



Network Security Groups Overview



Network Security Groups (NSG)



NSG Rules



NSG Effective Rules



Creating NSG Rules



Demonstration – NSGs

Network Security Groups

The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'nsg0'. The top navigation bar shows the NSG name and its directory path. Below this, a search bar and action buttons (Move, Delete, Refresh) are visible. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area shows the NSG's properties: Resource group (rg01), Location (East US), Subscription, Subscription ID, and Tags. It also displays the number of custom security rules (1 inbound, 0 outbound) and the number of associated subnets and network interfaces (1 subnet, 0 interfaces).

nsg0
Network security group | Directory: Microsoft

Search (Ctrl+ /) « → Move 🗑 Delete ↻ Refresh

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

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

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

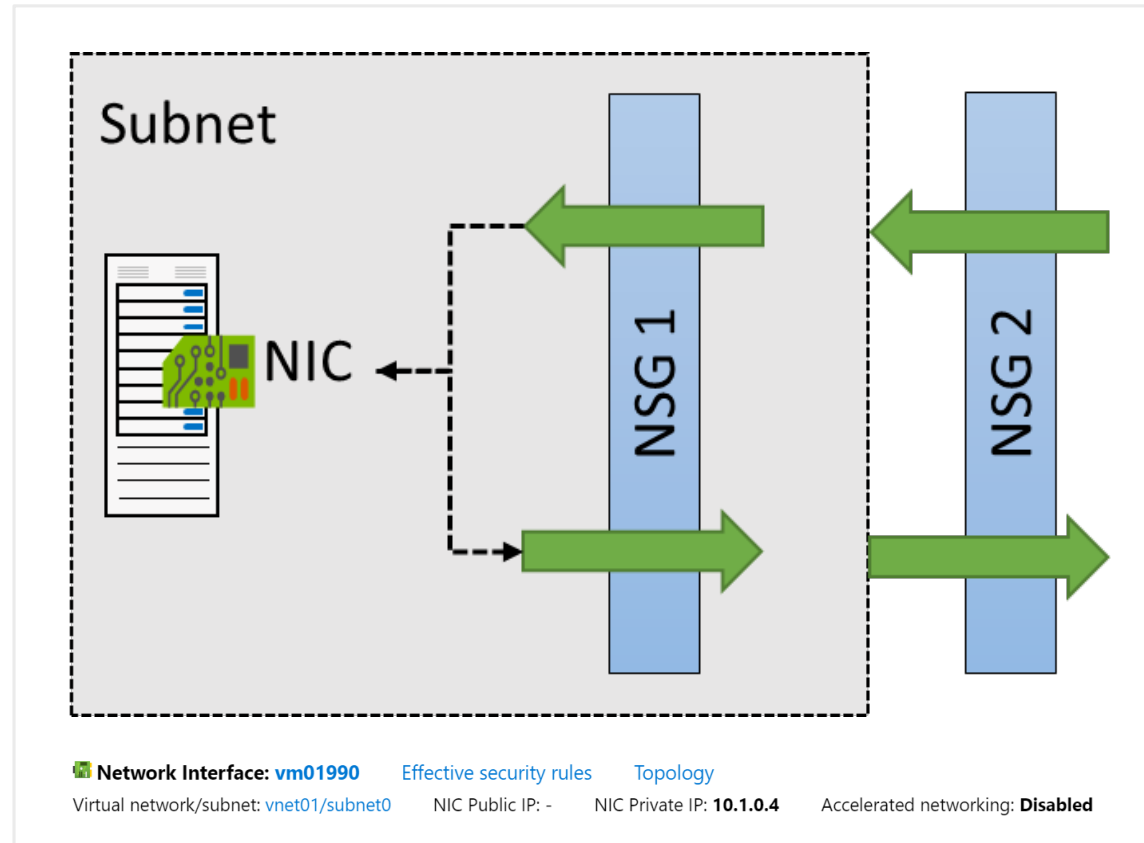
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

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



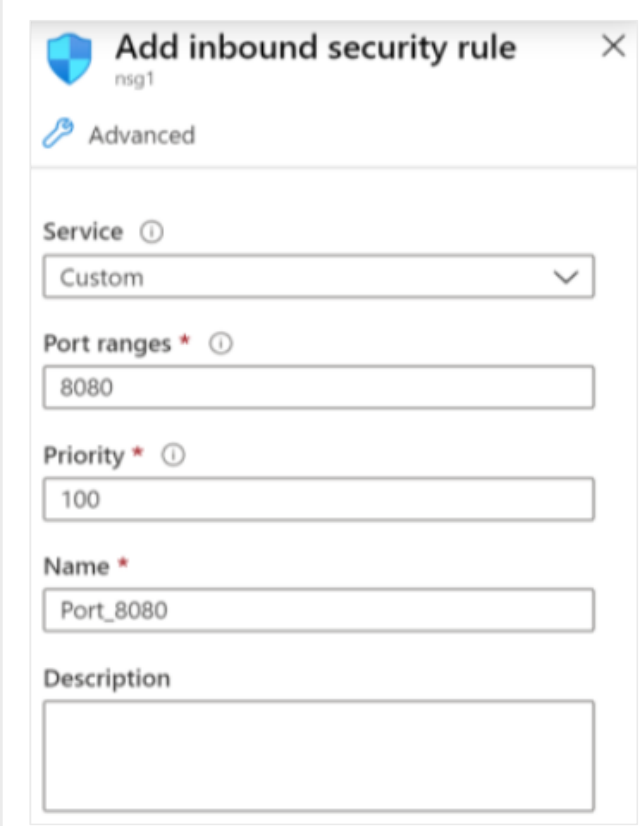
Creating NSG rules

Select from a large variety of services

Service – The destination protocol and port range for this rule

Port ranges – Single port or multiple ports

Priority – The lower the number, the higher the priority



The screenshot shows the 'Add inbound security rule' dialog box for a network security group named 'nsg1'. The 'Advanced' tab is selected. The 'Service' dropdown is set to 'Custom'. The 'Port ranges' field contains '8080'. The 'Priority' field contains '100'. The 'Name' field contains 'Port_8080'. The 'Description' field is empty.

Field	Value
Service	Custom
Port ranges	8080
Priority	100
Name	Port_8080
Description	

Lesson 04: Azure Firewall



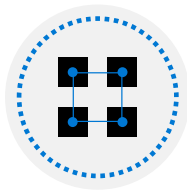
Azure Firewall Overview



Azure Firewall



Implementing Firewalls



Firewall Rules

Azure Firewall

Stateful firewall as a service

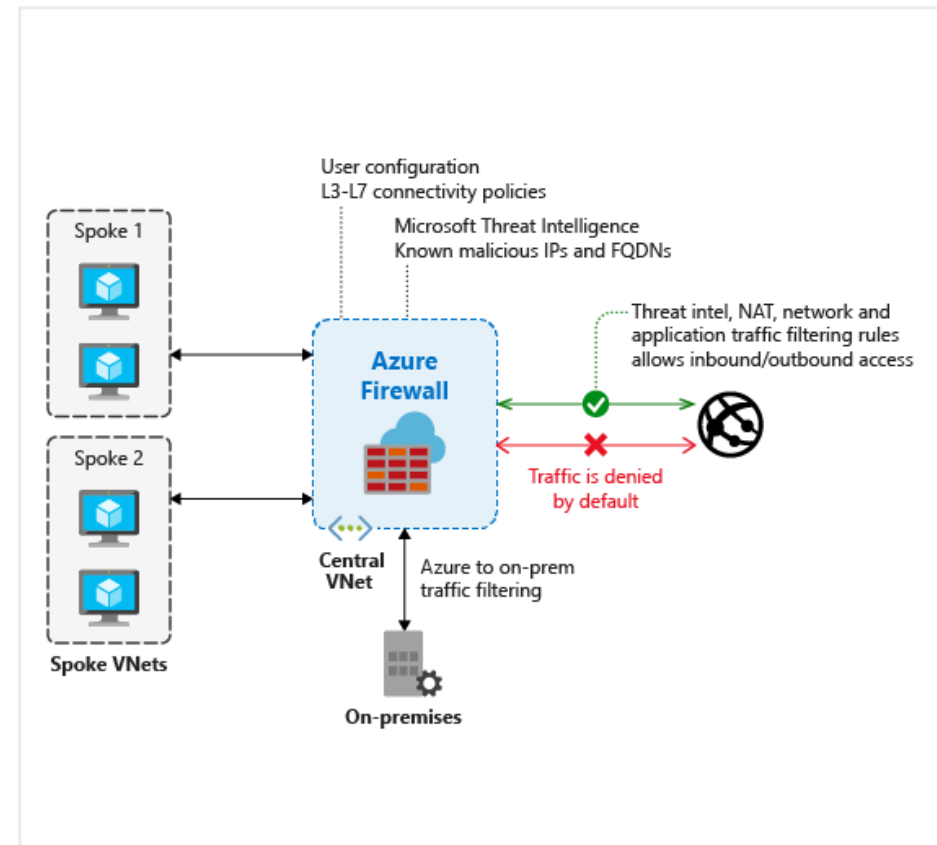
Built-in high availability with unrestricted cloud scalability

Create, enforce, and log application and network connectivity policies

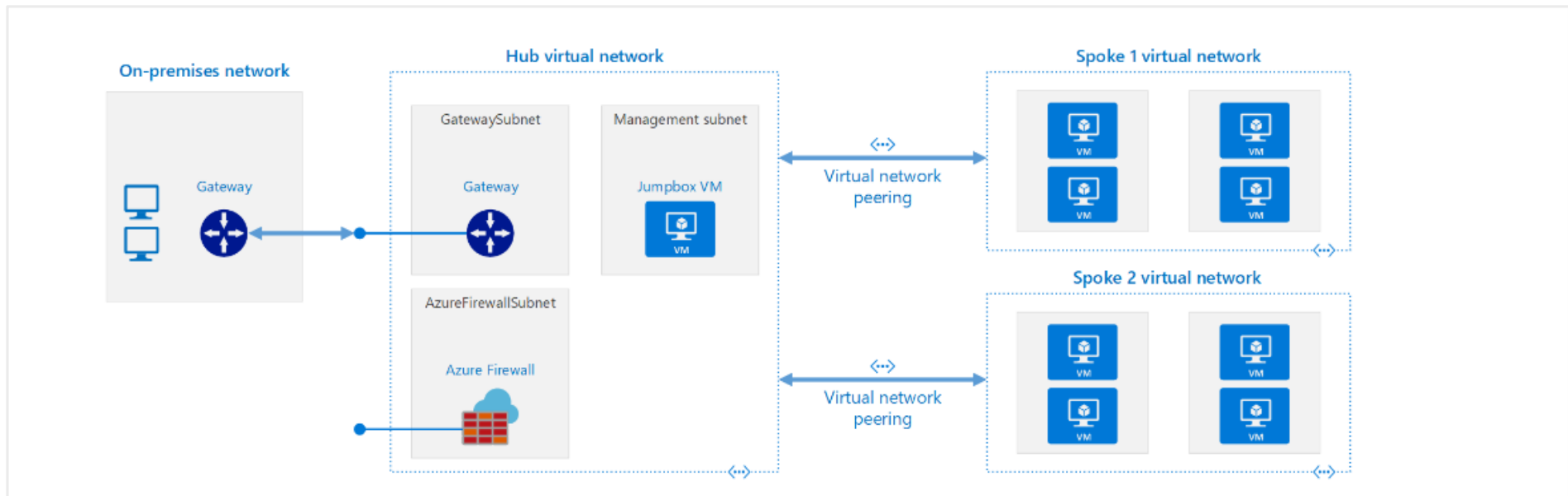
Threat intelligence-based filtering

Fully integrated with Azure Monitor for logging and analytics

Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways



Implementing Firewalls

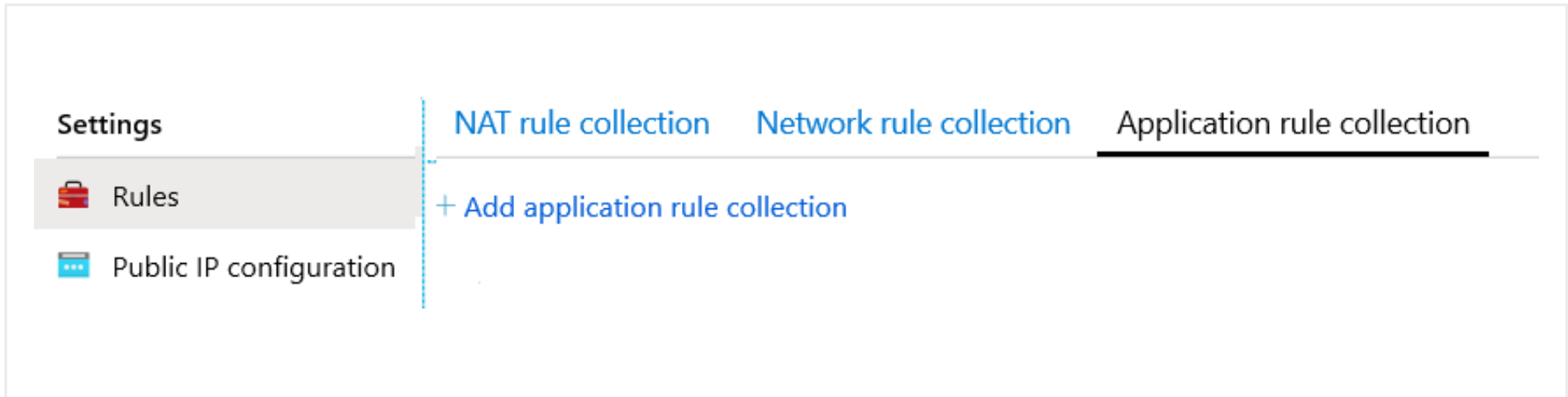


A Hub-Spoke network topology is recommended

Shared services are placed in the hub virtual network

Each environment is deployed to a spoke to maintain isolation

Firewall Rules

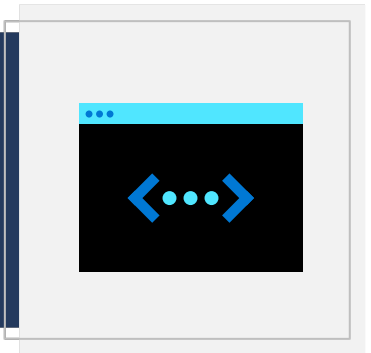


NAT rules. Configure DNAT rules to allow incoming connections

Network rules. Configure rules that contain source addresses, protocols, destination ports, and destination addresses

Application rules. Configure fully qualified domain names (FQDNs) that can be accessed from a subnet

Lesson 05: Azure DNS



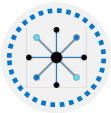
Azure DNS Overview



Domains and Custom Domains



Verifying Custom Domain Names



Azure DNS Zones



DNS Delegation



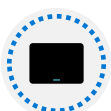
DNS Record Sets



DNS for Private Domains



Private Zones Scenarios



Demonstration – DNS Name Resolution

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 (next topic)

Create a directory
Azure Active Directory

Basics * Configuration * Review + create

Directory details
Configure your new directory

Organization name * ⓘ
Azure Administrator Incorporated ✓

Initial domain name * ⓘ
azureadminincorg ✓
azureadminincorg.onmicrosoft.com

Country/Region ⓘ
United States

Review + create < Previous Next : Review + create >



Custom domain name ✕
Azure Administrator Incorporated

Custom domain name * ⓘ
azureadmininc.org ✓

Add domain

Verify the Custom Domain Name



Verification demonstrates ownership of the domain name


Add a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone

Azure will query the DNS domain for the presence of the record

This could take several minutes or several hours

azureadmininc.org
Custom domain name


 Delete |  Got feedback?

 To use azureadmininc.org with your Azure AD, create a new TXT record with your domain name registrar using the info below.


Record type

☒ TXT ☐ MX


Alias or host name

@ 

Destination or points to address

MS=ms79094380 

TTL

3600 

[Share these settings via email](#)
Verification will not succeed until you have configured your domain with your registrar as described above.

Azure DNS Zones

A DNS zone hosts the DNS records for a domain

The name of the zone must be unique within the resource group

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](#)


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

 **azureadmininc.org**
DNS zone

 Record set

 Move

 Delete zone

 Refresh

Resource group ([change](#))
[rg-dns](#)

Subscription ([change](#))
[MSDN Platforms Subscription](#)

Subscription ID

Name server 1
ns1-02.azure-dns.com.

Name server 2
ns2-02.azure-dns.net.

Name server 3
ns3-02.azure-dns.org.

Name server 4
ns4-02.azure-dns.info.

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

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

DNS for Private Domains

Use your own custom domain names

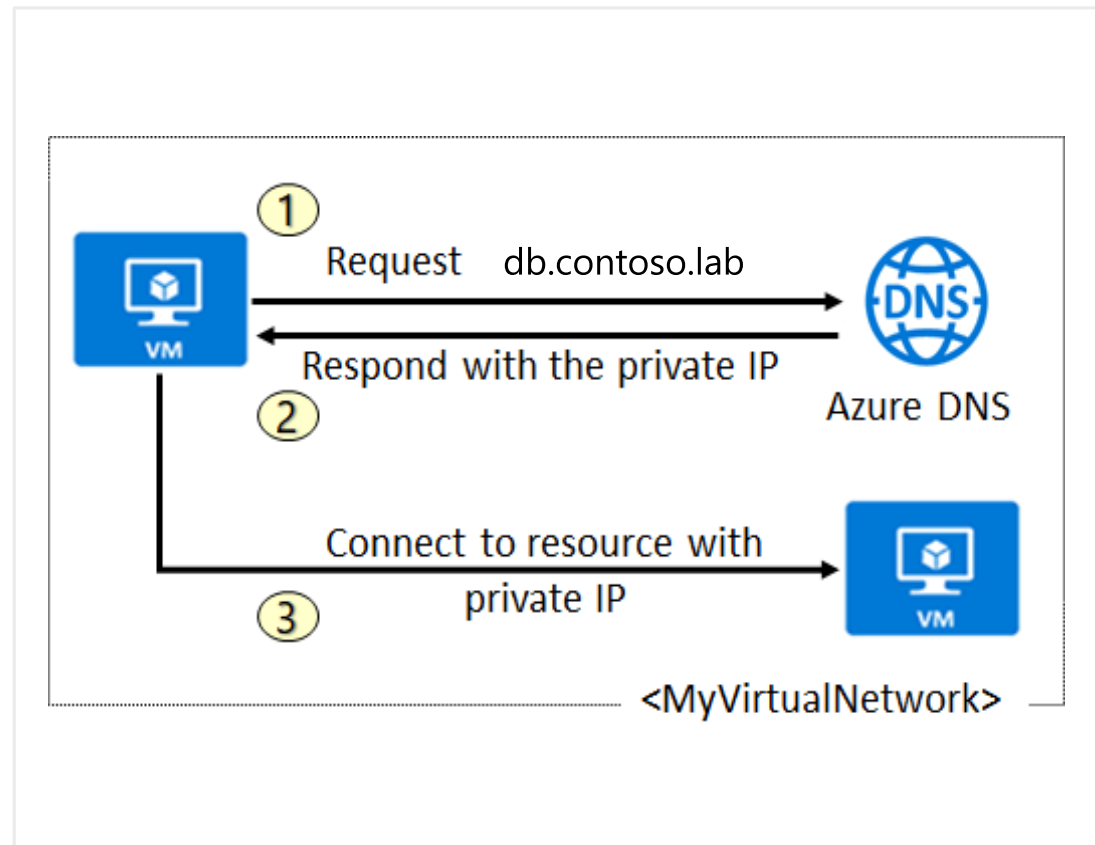
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

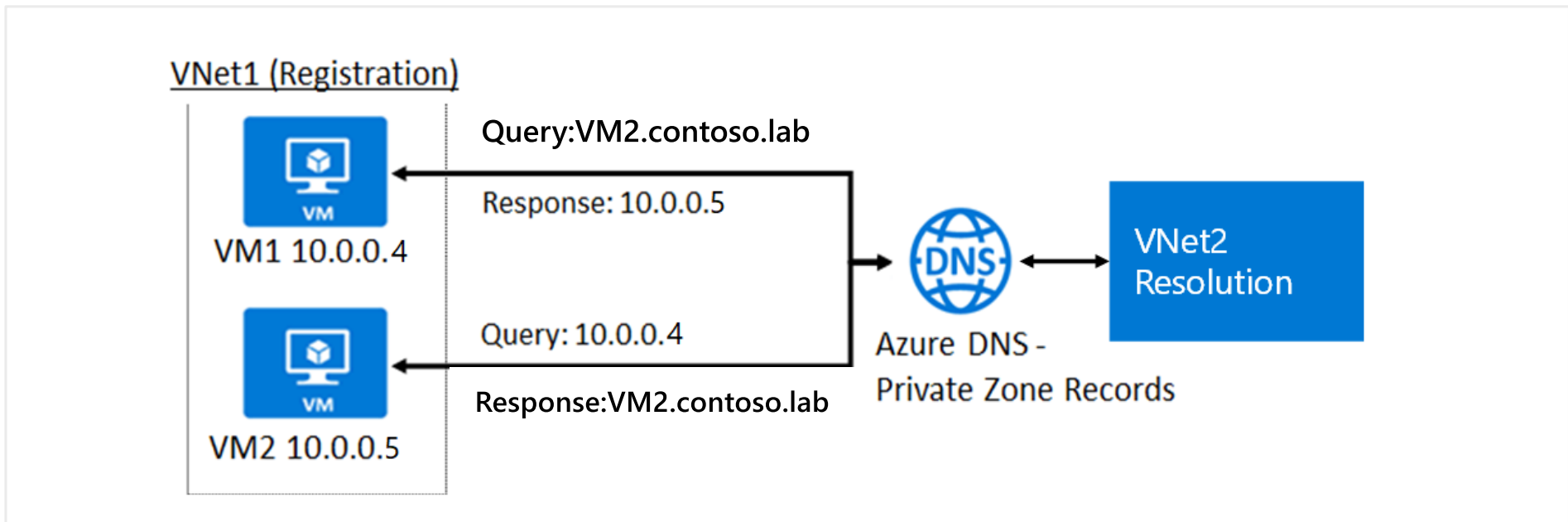
Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



Private Zone Scenarios

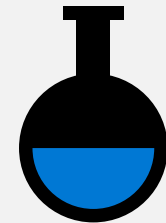


DNS resolution in VNet1 is private and not accessible from the Internet

DNS queries across the virtual networks are resolved

Reverse DNS queries are scoped to the same virtual network

Lesson 06: Module 04 Lab and Review



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:

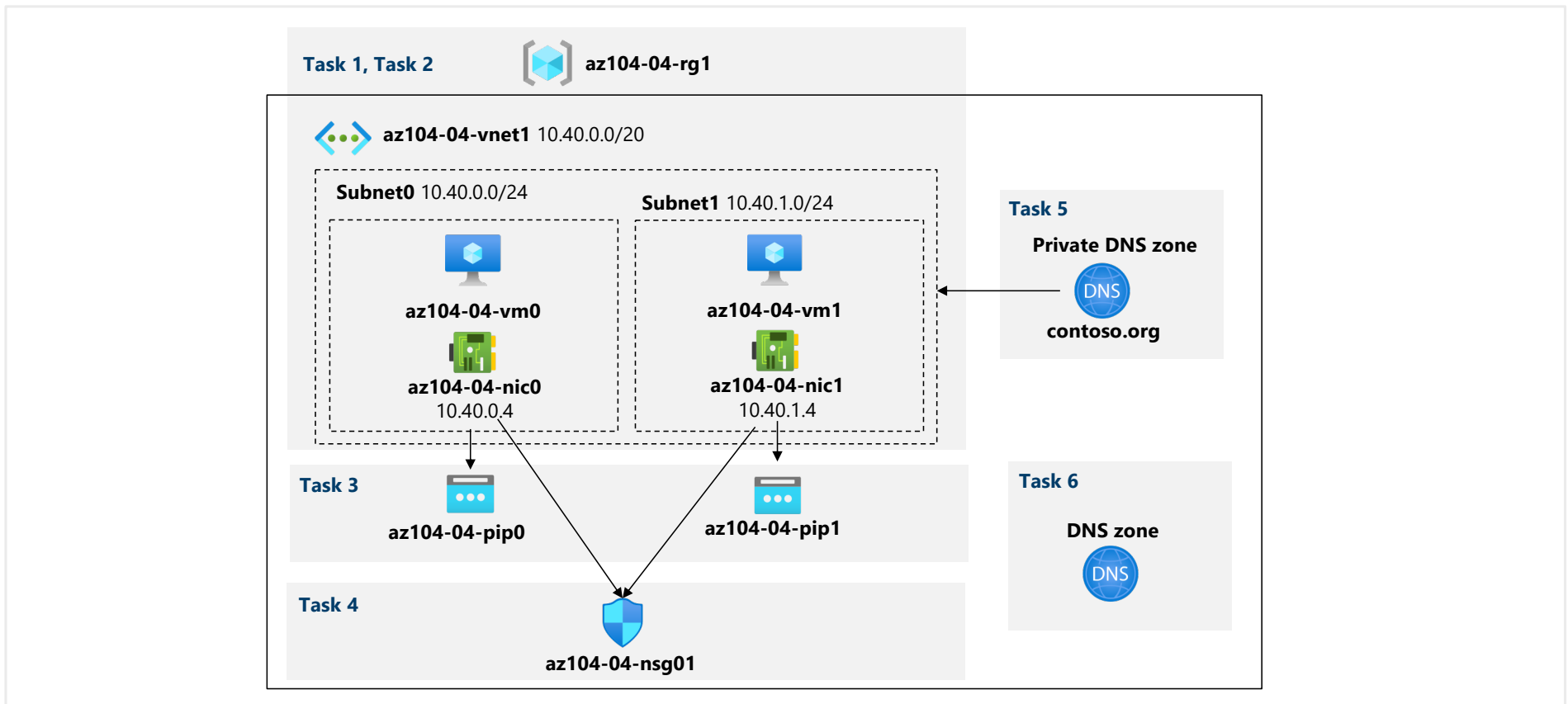
Configure Azure DNS for internal name resolution

Task 6:

Configure Azure DNS for external name resolution

Next slide for an architecture diagram 

Lab 04 – Architecture diagram



Module Review

Module Review Questions



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

Networking Fundamentals – Principals

Design an IP addressing schema for your Azure deployment

Secure and isolate access to Azure resources by using network security groups and service endpoints

End of presentation