

AZ-104

Administer Virtual Networking



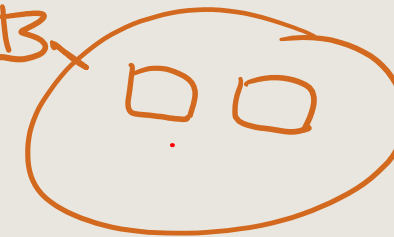
AZ-104 Agenda

Vint Cerf
1962

- 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

VMet
Peering

LB



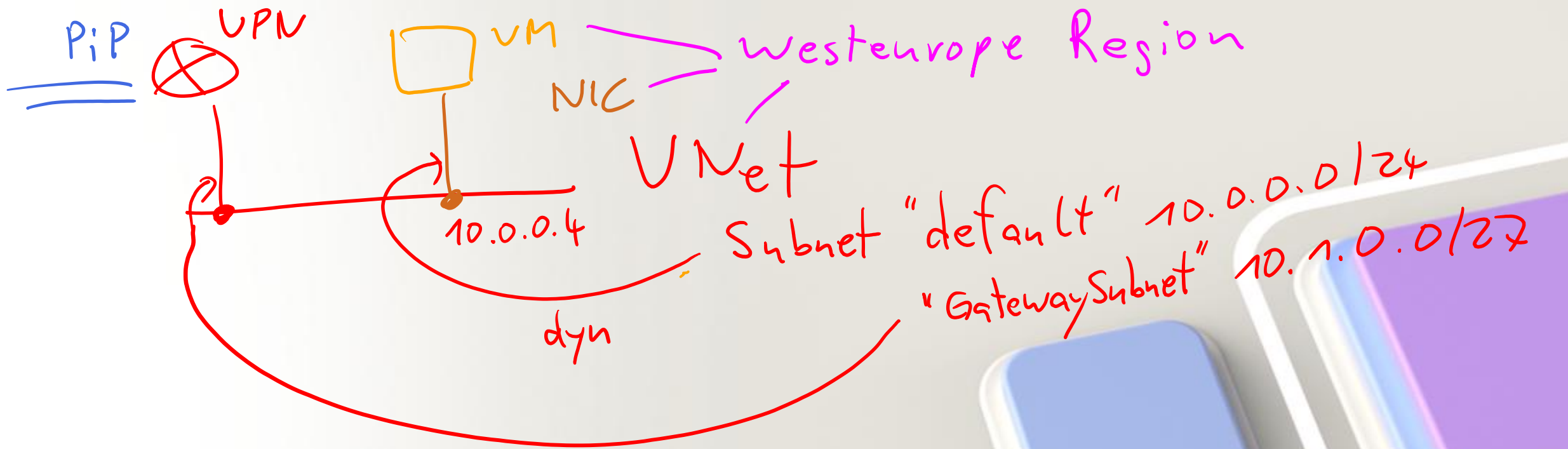
IP —
private
10 / 8
192.168 / 16
172.16 / 12

IP v 6 — public
private

Learning Objectives - Administer Virtual Networking

- Configure Virtual Networks
- Configure Network Security Groups
- Host your domain on Azure DNS
- Lab 04 – Implement Virtual Networks

NSG



Configure Virtual Networks

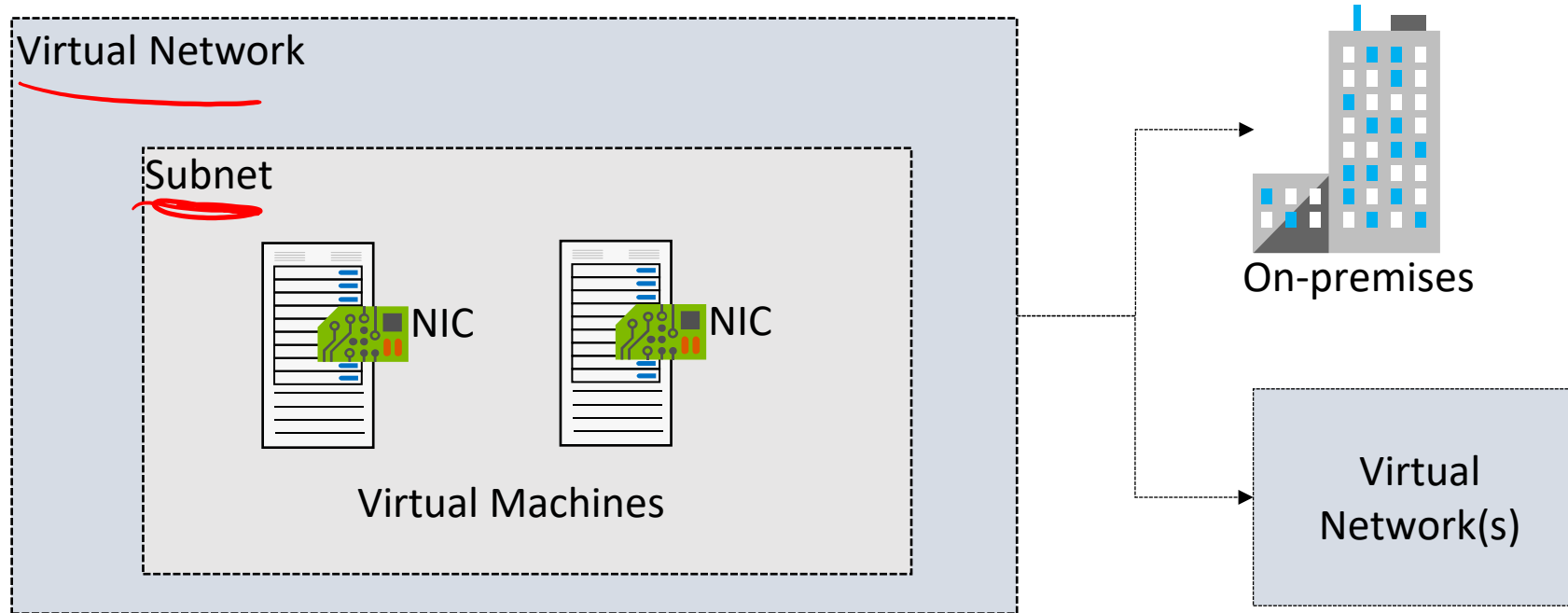
Learning Objectives - Configure Virtual Networks

- Plan Virtual Networks
- Create Virtual Networks
- Create Subnets
- Plan IP Addressing
- Create Public IP Addresses
- Associate Public IP Addresses
- Allocate or Assign Private IP Addresses
- Demonstration – Virtual Networks
- Learning Recap

Implement and manage virtual networking (15–20%): Configure and manage virtual networks in Azure

- Create and configure virtual networks and subnets
- Configure public IP addresses

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 Virtual Networks

- Create new virtual networks at any time
- Add virtual networks when you create a virtual machine
- Define the address space, and at least one subnet
- Check for 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

Create Subnets

<div><div><div><div></div></div><div>Subnet</div></div><div><div><div></div></div><div>Gateway subnet</div></div><div><div><div></div></div><div>Refresh</div></div><div><div><div></div></div><div>Manage users</div></div><div><div><div></div></div><div>Delete</div></div></div>				
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	10.0.30.0/26	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

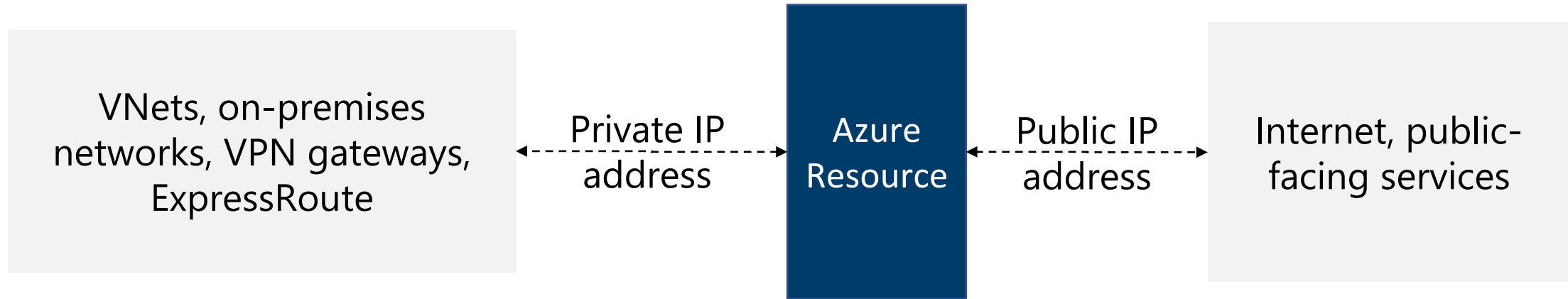
A virtual network can be segmented into one or more subnets

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

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

IPv4 or IPv6

Standard SKU – do you need to upgrade?

Regional vs Global

Microsoft network vs. Internet

Create public IP address ...

Basics DDoS Protection Tags Review + create

Configuration details

Name *

IP Version * ⓘ ☒ IPv4 ☐ IPv6

SKU * ⓘ ☒ Standard

Availability zone * ⓘ

Zone-redundant

▼

Tier * ⓘ ☒ Regional ☐ Global

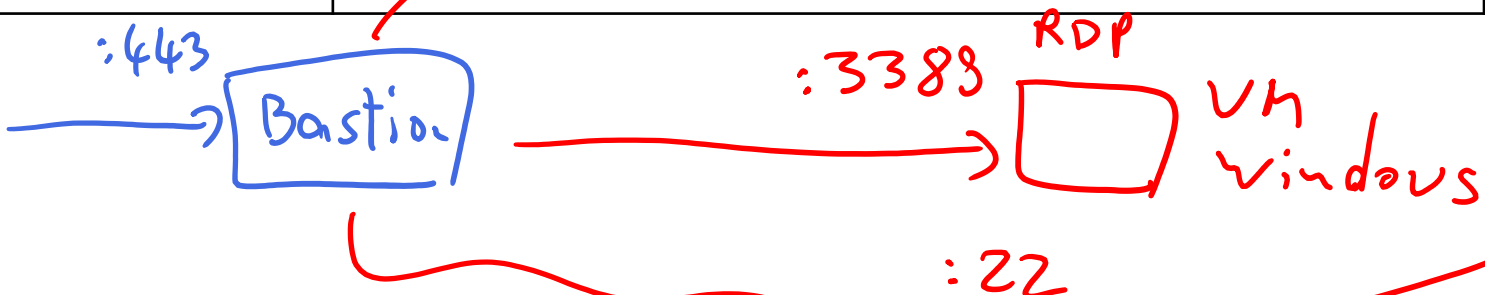
IP address assignment

IP address assignment * ⓘ ☐ Dynamic ☒ Static

Routing preference * ⓘ ☒ Microsoft network ☐ Internet

Associate Public IP Addresses

Top-level resource	IP address configuration
Virtual Machine	Network interface
Virtual Network Gateway (VPN), Virtual Network Gateway (ER), NAT Gateway	Gateway IP configuration
Public Load Balancer, Application Gateway, Azure Firewall, Route Server, API Management	Front-end configuration
Bastion Host	Public IP configuration



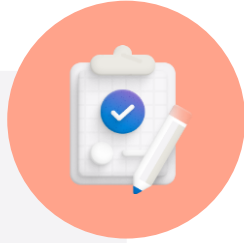
Allocate or Assign Private IP Addresses

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

Learning Recap – Virtual Networks



Check your
knowledge
questions and
additional
study

Reference modules

- [Introduction to Azure Virtual Networks](#)
- [Design an IP addressing schema for your Azure deployment](#)
- [Implement Windows Server IaaS VM IP addressing and routing](#)

Configure Network Security Groups (NSGs)




Learning Objectives – Network Security Groups


- Implement Network Security Groups
- Determine NSG Rules
- Determine NSG Effective Rules
- Create NSG Rules
- Implement Application Security Groups
- Demonstration – NSGs
- Learning Recap

Implement and manage virtual networking (15–20%): Configure secure access to virtual networks


- Create and configure network security groups (NSGs) and application security groups
- Evaluate effective security rules in NSGs


Implement Network Security Groups


 **nsg0**
Network security group


 Directory: Microsoft


→ 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

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

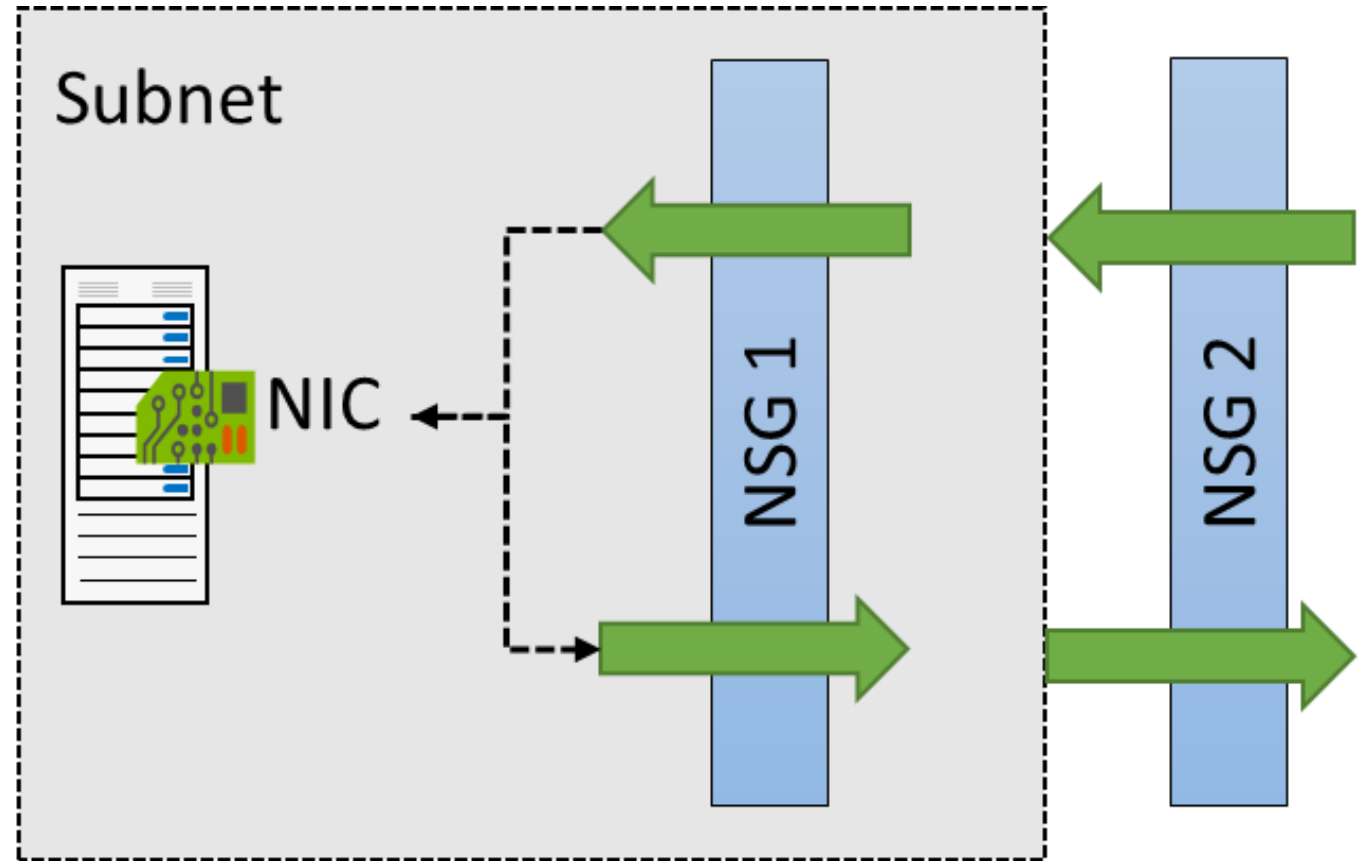
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

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



 Network Interface: **vm01990**

[Effective security rules](#)

[Topology](#)

Virtual network/subnet: **vnet01/subnet0**

NIC Public IP: -

NIC Private IP: **10.1.0.4**

Accelerated networking: **Disabled**

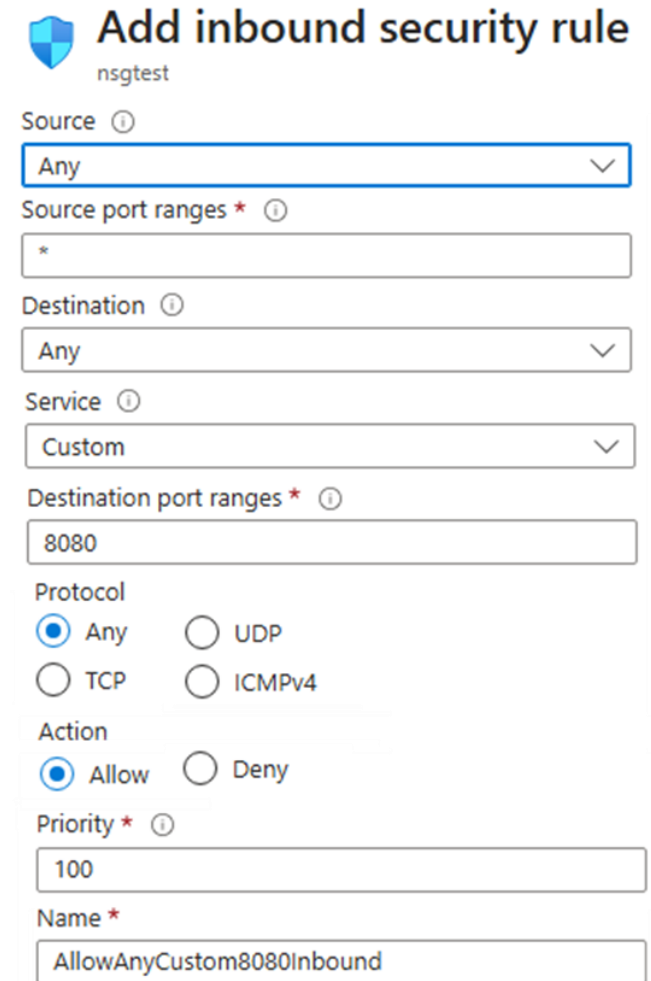
Create NSG rules

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

Destination (Any, IP addresses, service tag, and 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' form in the Azure portal. The form is titled 'Add inbound security rule' with a shield icon and the text 'nsgtest' below it. The form fields are as follows:

- Source**: A dropdown menu with 'Any' selected.
- Source port ranges**: A text input field with '*' entered.
- Destination**: A dropdown menu with 'Any' selected.
- Service**: A dropdown menu with 'Custom' selected.
- Destination port ranges**: A text input field with '8080' entered.
- Protocol**: Radio buttons for 'Any' (selected), 'UDP', 'TCP', and 'ICMPv4'.
- Action**: Radio buttons for 'Allow' (selected) and 'Deny'.
- Priority**: A text input field with '100' entered.
- Name**: A text input field with 'AllowAnyCustom8080Inbound' entered.

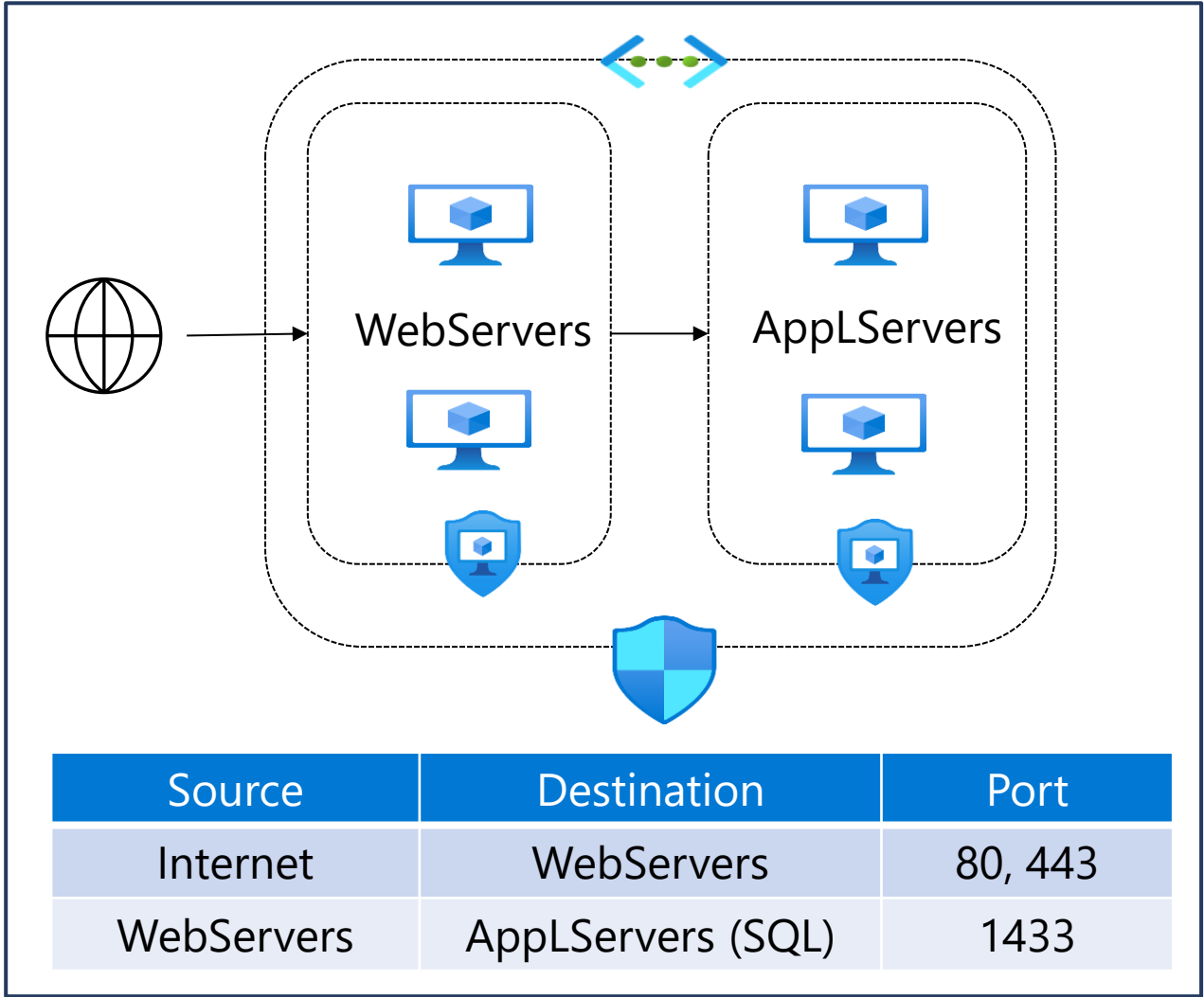
Implement Application Security Groups

Extends your application's structure

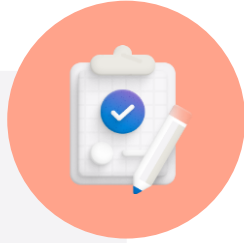
ASGs logically group virtual machines – web servers, application servers

Define rules to control the traffic flow

Wrap the ASG with an NSG for added security



Learning Recap – Network Security Groups



Check your
knowledge
questions and
additional
study

Reference modules

- [Configure network security groups](#)
- [Filter network traffic with a network security group using the Azure portal](#)
- [Secure and isolate access to Azure resources by using network security groups and service endpoints](#)

Host your domain on Azure DNS



Learning Objectives - Host your domain on Azure DNS

- What is Azure DNS?
- Configure Azure DNS to host your domain
- Verify delegation of domain name services
- Dynamically resolve resource name by using alias record
- Configure a private DNS zone
- Demonstration – DNS Name Resolution
- Learning Recap

Implement and manage virtual networking (15–20%): Configure name resolution and load balancing

- Configure Azure DNS

What is Azure DNS?

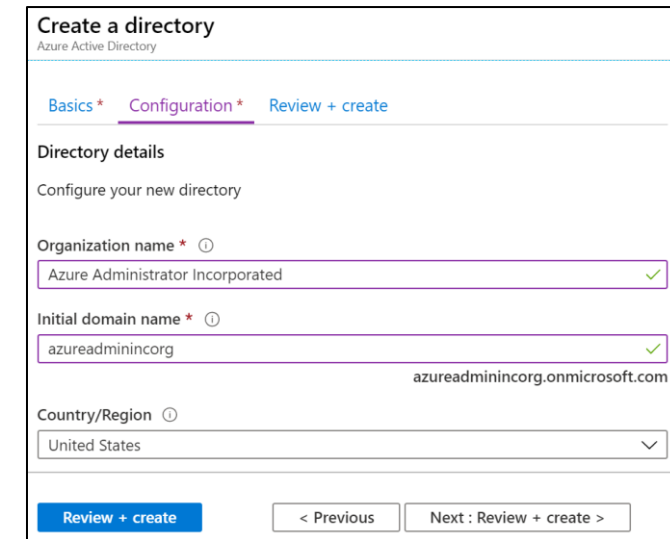
When you create a new tenant, a new default domain is created

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

Tenant

You can add a custom domain name

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



Create a directory
Azure Active Directory

Basics * Configuration * Review + create

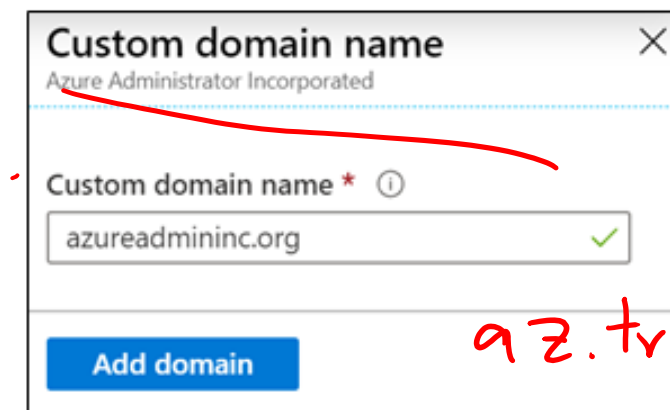
Directory details
Configure your new directory

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 X

Azure Administrator Incorporated

Custom domain name * ⓘ
azureadmininc.org ✓

Add domain

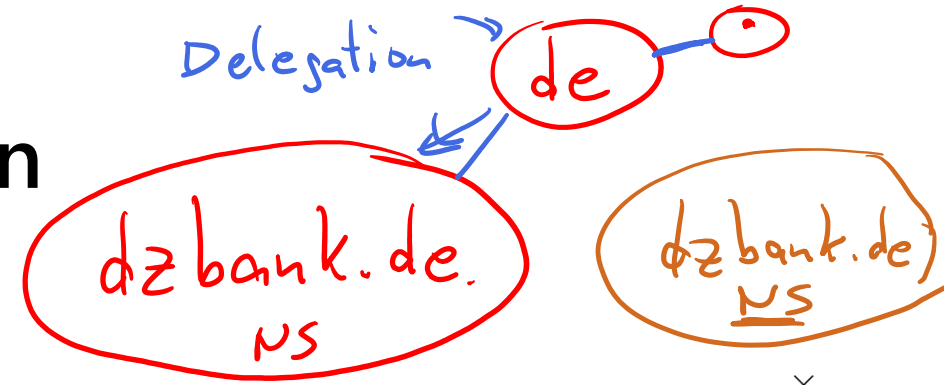
az.training

Configure Azure DNS to host your domain

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

[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](#)

Verify delegation of domain name services

- 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](#)

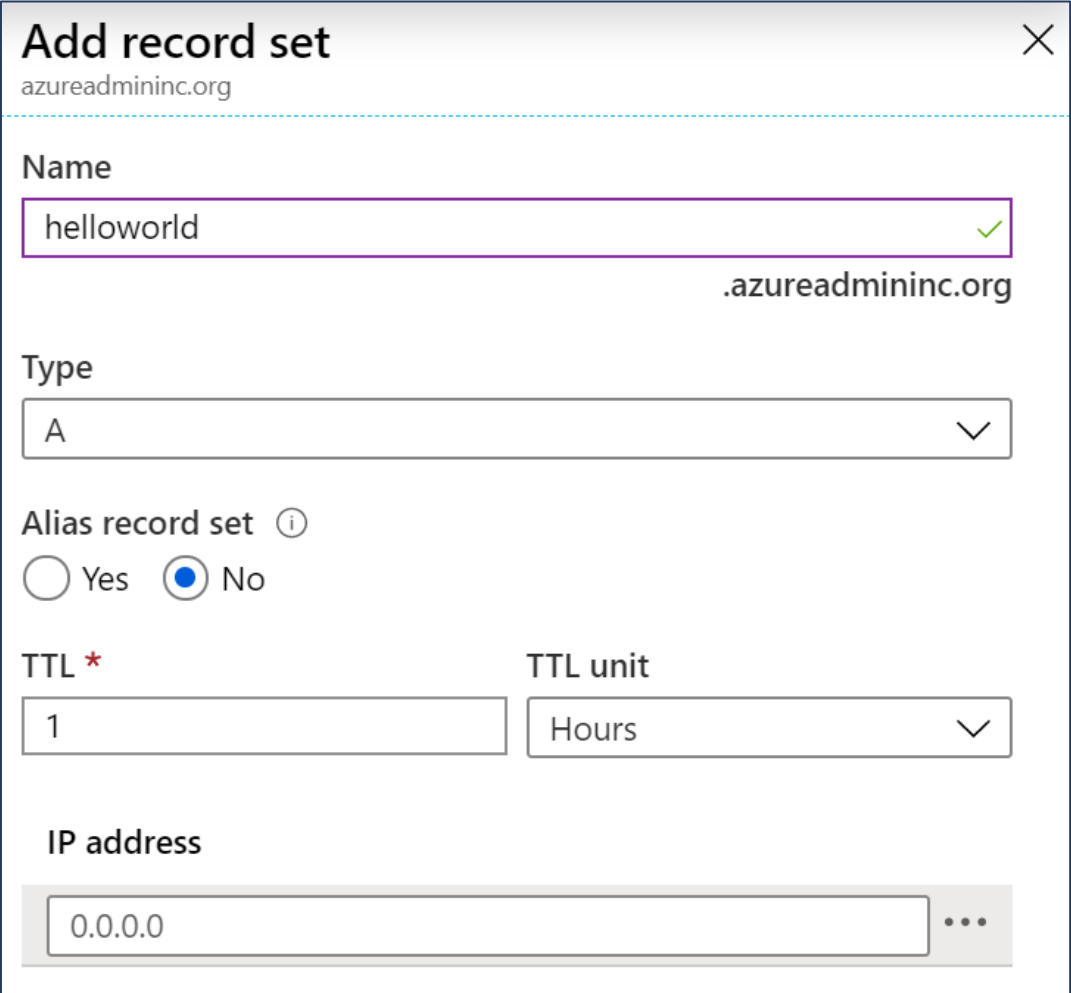
Dynamically resolve resource name by using alias record

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



The screenshot shows the 'Add record set' dialog box for the domain 'azureadmininc.org'. The 'Name' field contains 'helloworld' with a green checkmark, and the full name '.azureadmininc.org' is displayed to the right. The 'Type' dropdown is set to 'A'. The 'Alias record set' section has 'No' selected. The 'TTL' is set to '1' and the 'TTL unit' is 'Hours'. The 'IP address' field contains '0.0.0.0' with a three-dot menu icon to its right.

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 ...

Configure a private DNS zone

Use your own custom domain names

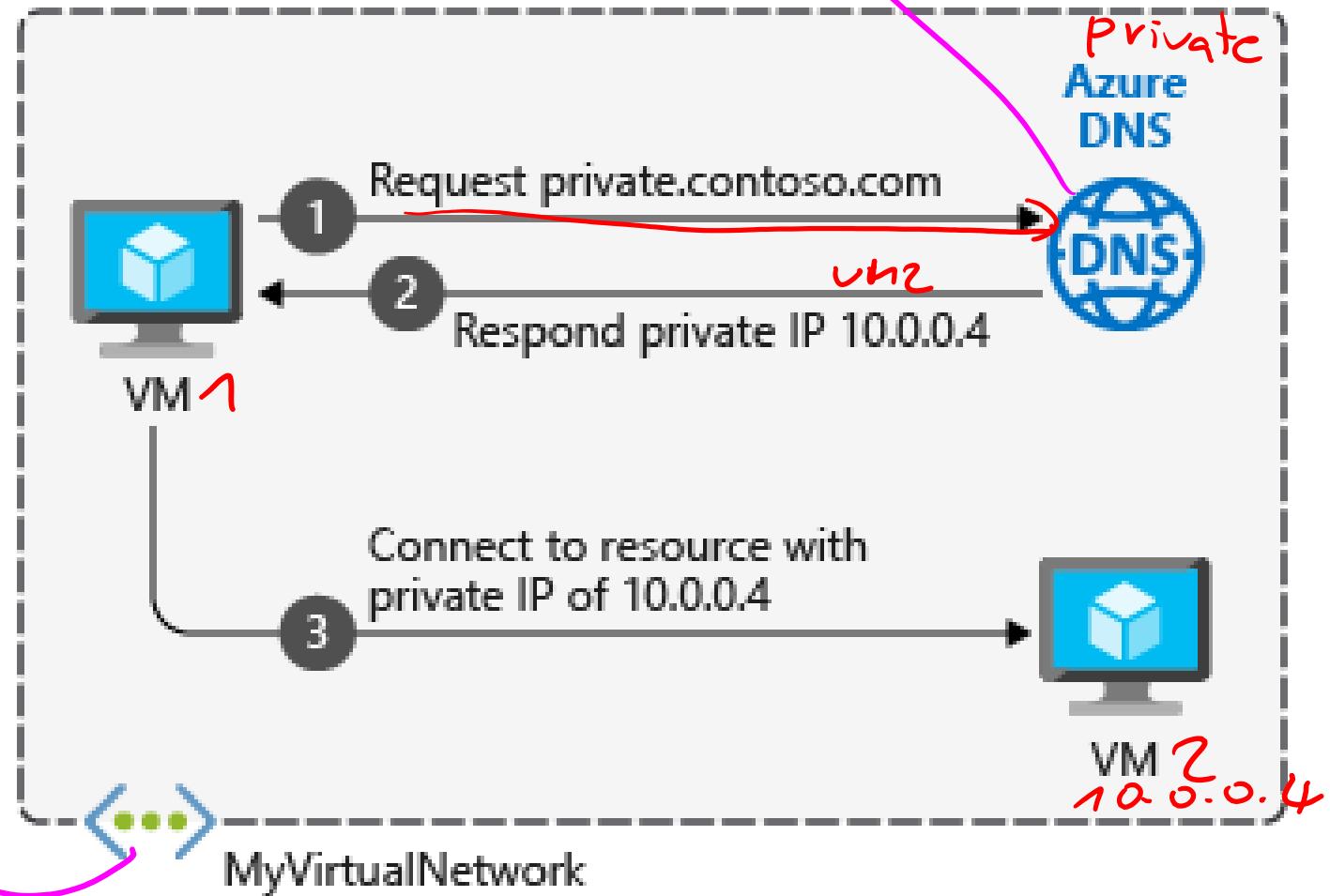
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

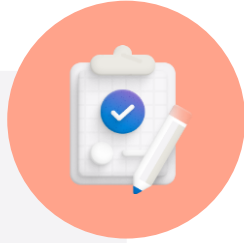
Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



Learning Recap – Host your domain on Azure DNS



Check your
knowledge
questions and
additional
study

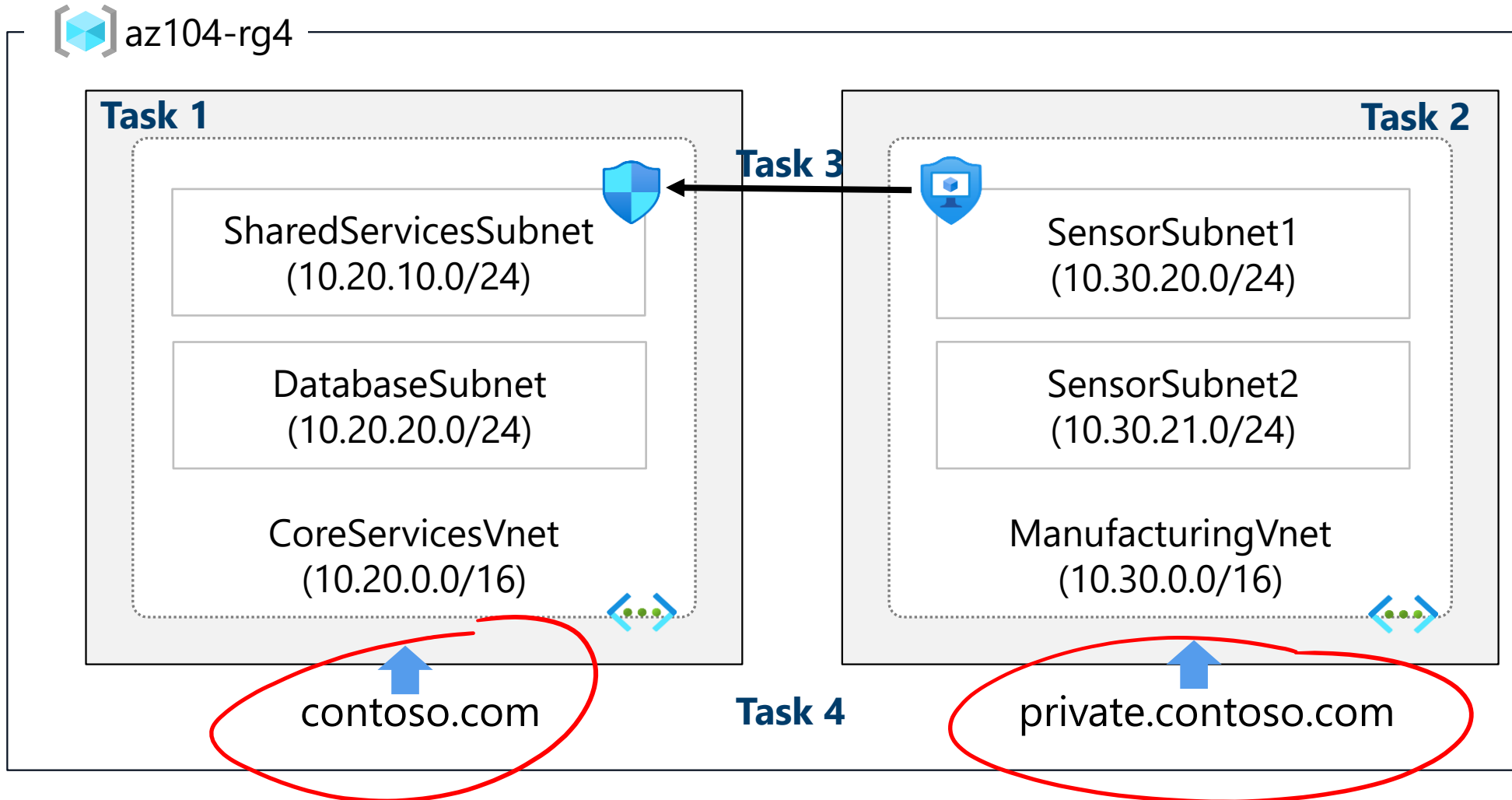
Reference modules

- [Introduction to Azure DNS](#)
- [Host your domain on Azure DNS](#)

Lab – Implement Virtual Networks



Lab 04 – Architecture diagram



End of presentation

