O'REILLY®

Azure Networking Fundamentals

Design and Implement Microsoft Azure Network Infrastructure

Reza Salehi

- Cloud Consultant and Trainer
- linkedin.com/in/rezasalehi2008
- @zaalion

COURSE

Microsoft Azure Fundamentals (AZ-900) Certification Course

★★★★★ 1 review

By Reza Salehi

Continue

TIME TO COMPLETE:
4h 37m

LEVEL:
Beginner

TOPICS:
Microsoft Azure

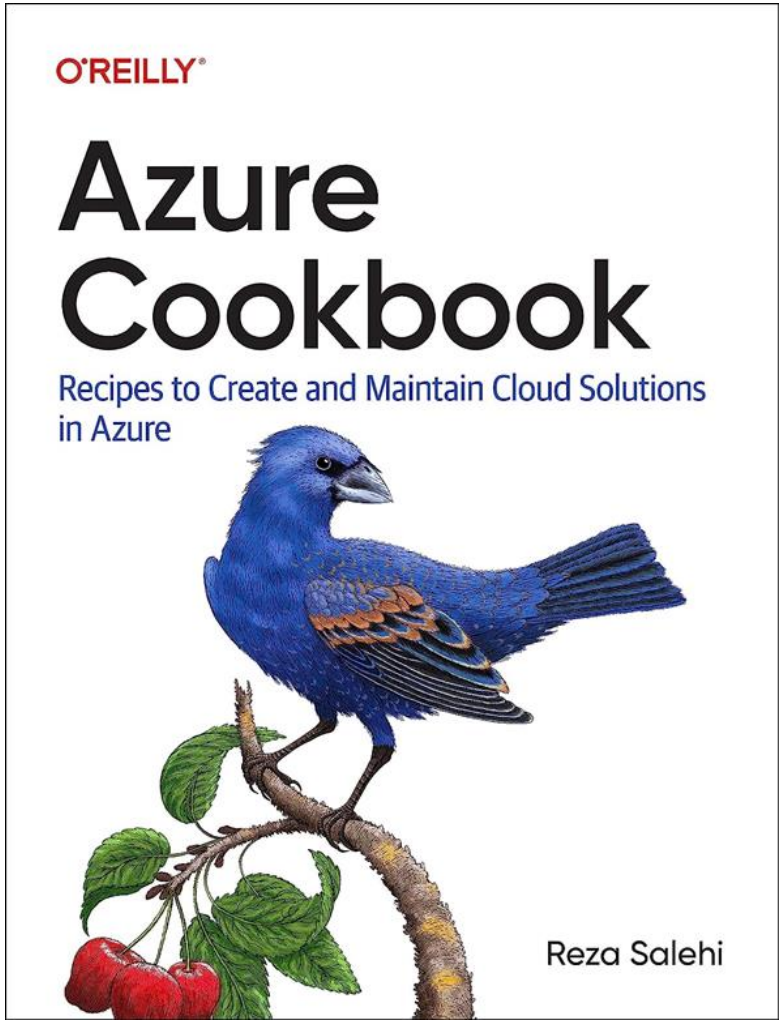
PUBLISHED BY:
O'Reilly Media, Inc.

PUBLICATION DATE:
October 2022

Preparing for certification?
Take Practice Exam >

https://learning.oreilly.com/videos/microsoft-azure-fundamentals/0636920797234/

- https://learning.oreilly.com/library/view/azure-cookbook/9781098135782/
- https://www.amazon.ca/Azure-Cookbook-Recipes-Maintain-Solutions/dp/1098135792/
- https://www.amazon.com/Azure-Cookbook-Recipes-Maintain-Solutions/dp/1098135792



Course schedule and learning objectives

- Introduction
- Basics of Computer Networking (address space, subnets, firewalls)
- Azure Virtual Networks (VNETs) and Virtual Subnets
- Deploying an Azure Virtual Machine to a VNET
- Public and Private IP addresses
- Routes and Route Tables
- Azure VNET Peering
- Common Azure VNET topologies
- Q&A
- Break

Course schedule and learning objectives

- Network Security Groups (NSGs)
- Azure Firewall, rules
- Azure service firewalls (Storage, Cosmos DB, SQL)
- Private Link and Private Endpoints
- Azure NAT Gateway
- Q&A

Networking Fundamentals

- Basic networking concepts (address space, CIDR, subnets, firewalls)

Poll: What IP address range does 10.0.1.64/26 specify?

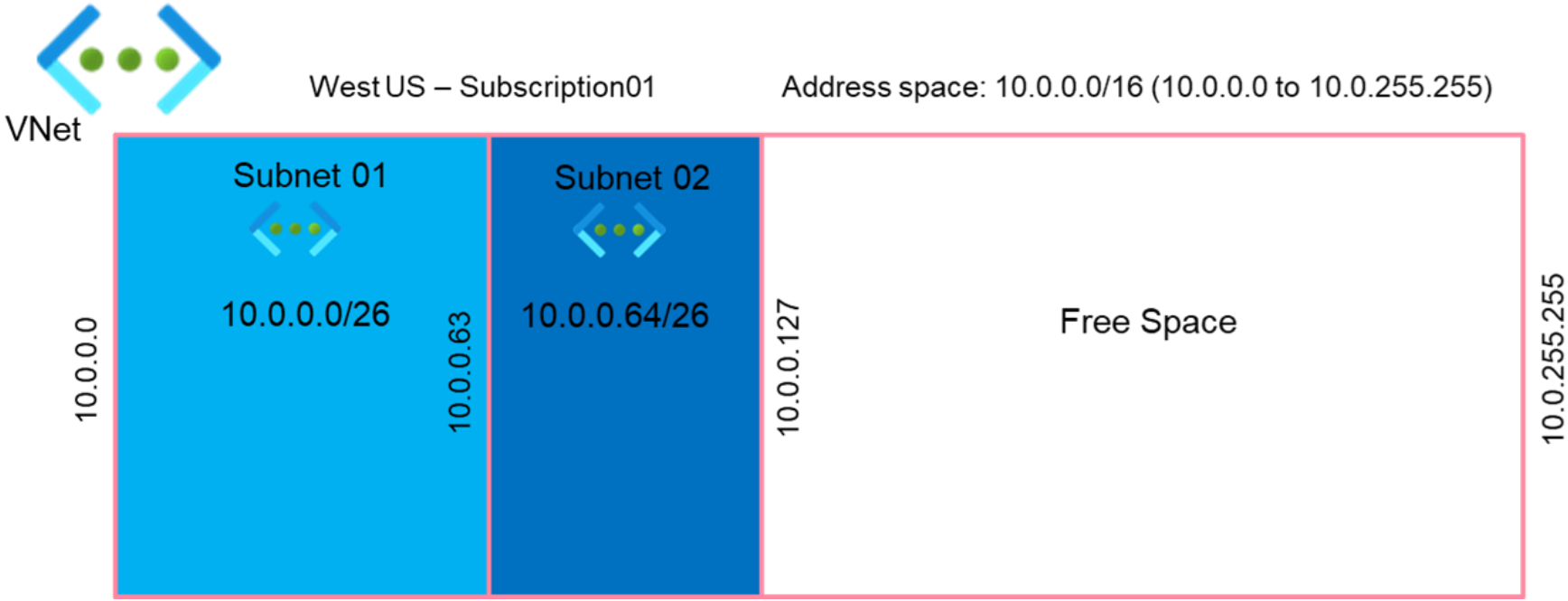
- 10.0.1.64 - 10.0.1.127
- 10.0.0.0 - 10.0.0.63
- 10.1.0.0 - 10.63.0.0
- 10.0.1.0 - 10.0.1.63

Address space, CIDR

- 10.0.0.0/24 → 10.0.0.0 - 10.0.0.255
- 10.0.0.0/26 → 10.0.0.0 - 10.0.0.63
- 10.0.0.0/32 → 10.0.0.0
- 10.0.100.0/32 → 10.0.100.0

https://www.ipaddressguide.com/cidr

Subnets


VNet
West US – Subscription01
Address space: 10.0.0.0/16 (10.0.0.0 to 10.0.255.255)
Subnet 01
10.0.0.0/26
Subnet 02
10.0.0.64/26
Free Space
10.0.0.0
10.0.0.63
10.0.0.127
10.0.255.255

Q&A

Azure Networking Fundamentals

- Azure Virtual Networks (VNETs) and Virtual Subnets [see 1]
- Deploying an Azure Virtual Machine to a VNET [see 1]
- Public and Private IP addresses [see 1]
- Routes and Route Tables [see 1]
- Azure VNET Peering [see 1]
- Common Azure VNET topologies (segmentation) [see 1]

Poll: What is the easiest method to connect two Azure VNets in the same region?

- Point-to-Site VPN
- Site-to-Site VPN
- VNet Peering
- Azure ExpressRoute

Azure Virtual Networks (VNETs) and Virtual Subnets

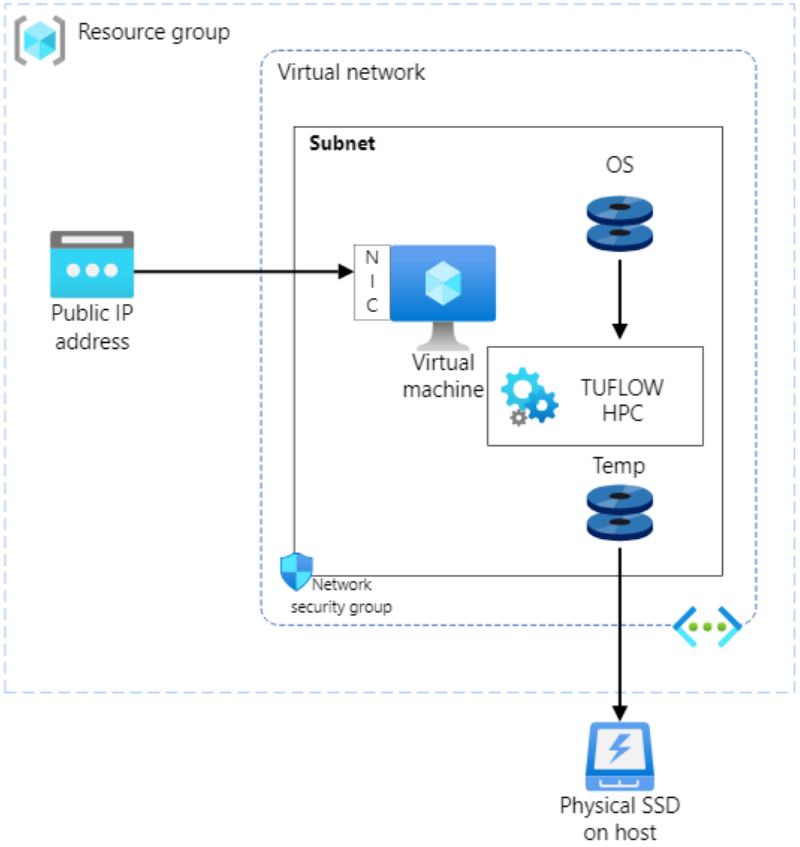
- Azure Virtual Network is a service that provides the fundamental building block for your private network in Azure.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Deploying an Azure Virtual Machine to a VNET

- An Azure Virtual Machine should be deployed to an Azure VNet
- The VM can get one (or more) private IP address

Azure Virtual Networks (VNETs) and Virtual Subnets



Microsoft Azure

Hands-on Demo

- Creating an Azure Virtual Network
- Deploying an Azure Virtual Machine to the above VNet

Public and Private IP addresses

- Public IP addresses allow Internet resources to communicate inbound to Azure resources.
  - Static
  - Dynamic
- The following resources can receive public IP addresses:
  - Virtual machine network interfaces
  - Virtual Machine Scale Sets
  - Public Load Balancers
  - Virtual Network Gateways (VPN/ER)
  - NAT gateways
  - Application Gateways
  - Azure Firewalls
  - Bastion Hosts
  - Route Servers
  - Api Management

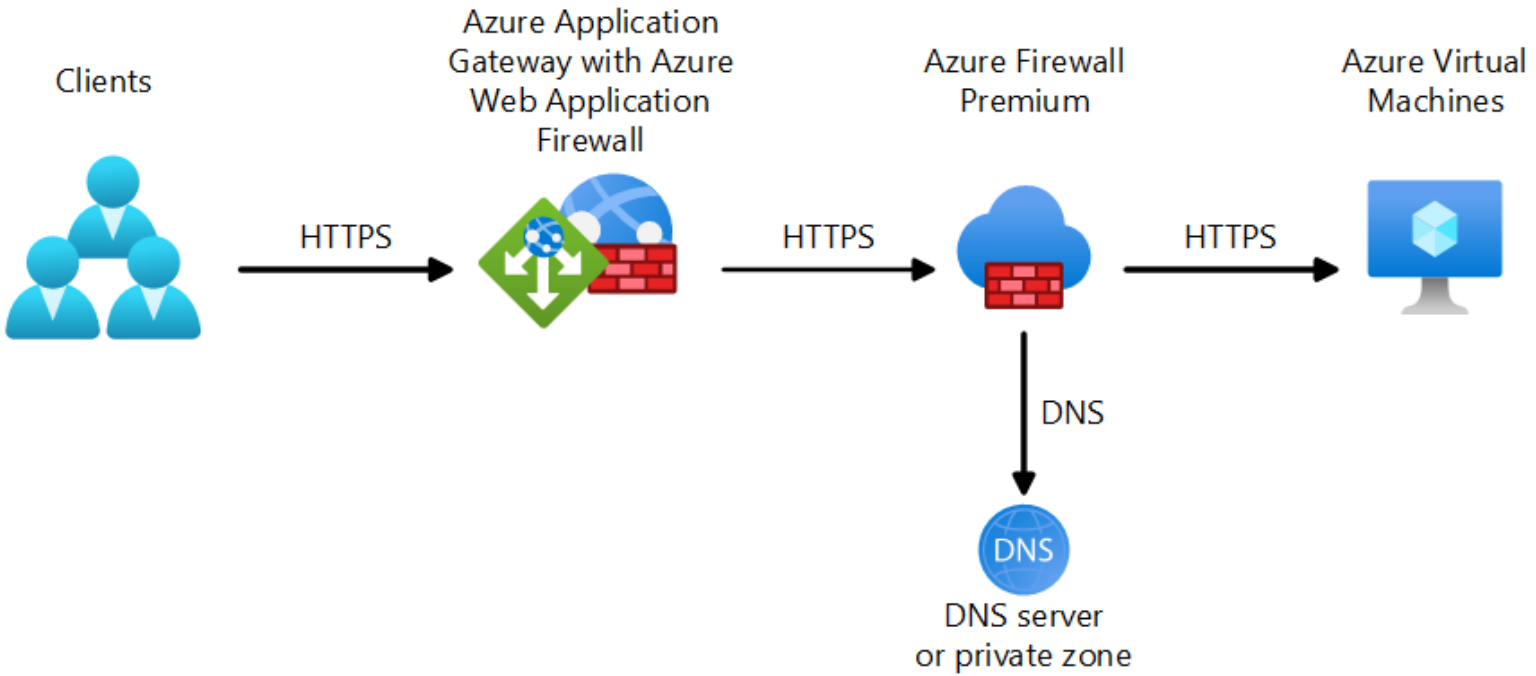
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses

Public and Private IP addresses: IP Prefix

- A public IP address prefix is a reserved range of public IP addresses in Azure.

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-address-prefix

Public and Private IP addresses



Microsoft Azure

Hands-on Demo

- Examining the VM private IP address
- Provisioning a new Public IP address
- Making our VM publicly accessible

Routes and Route Tables

- Azure automatically creates system routes and assigns the routes to subnets in a VNet.
- You can't create system routes, nor remove them, but you can override some system routes with custom (User-defined) routes.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Routes and Route Tables

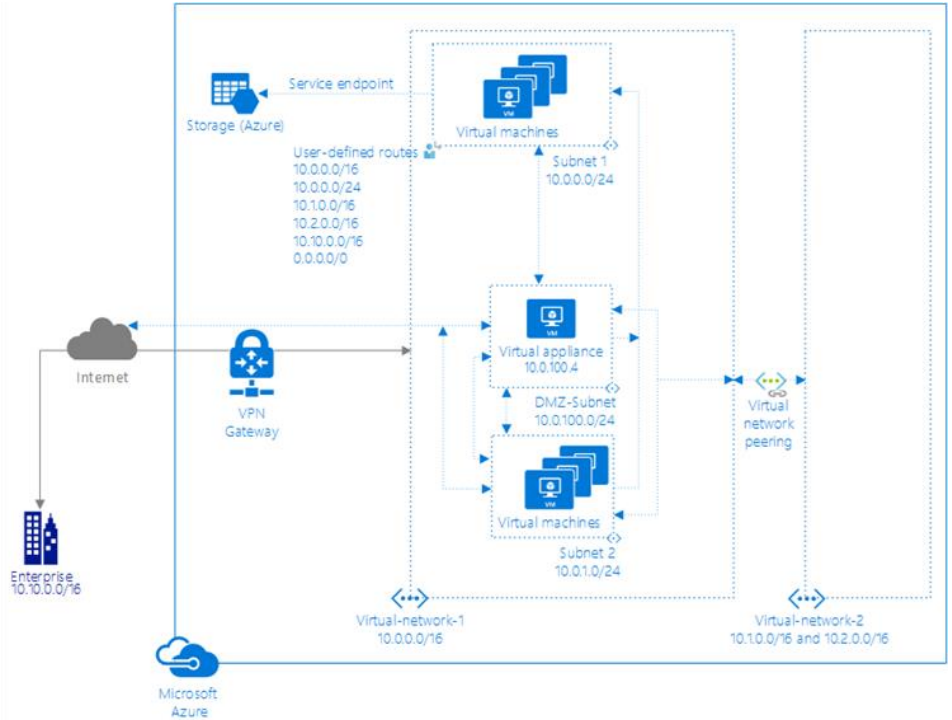
System routes

Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create system routes, nor can you remove system routes, but you can override some system routes with custom routes. Azure creates default system routes for each subnet, and adds more optional default routes to specific subnets, or every subnet, when you use specific Azure capabilities.

Default

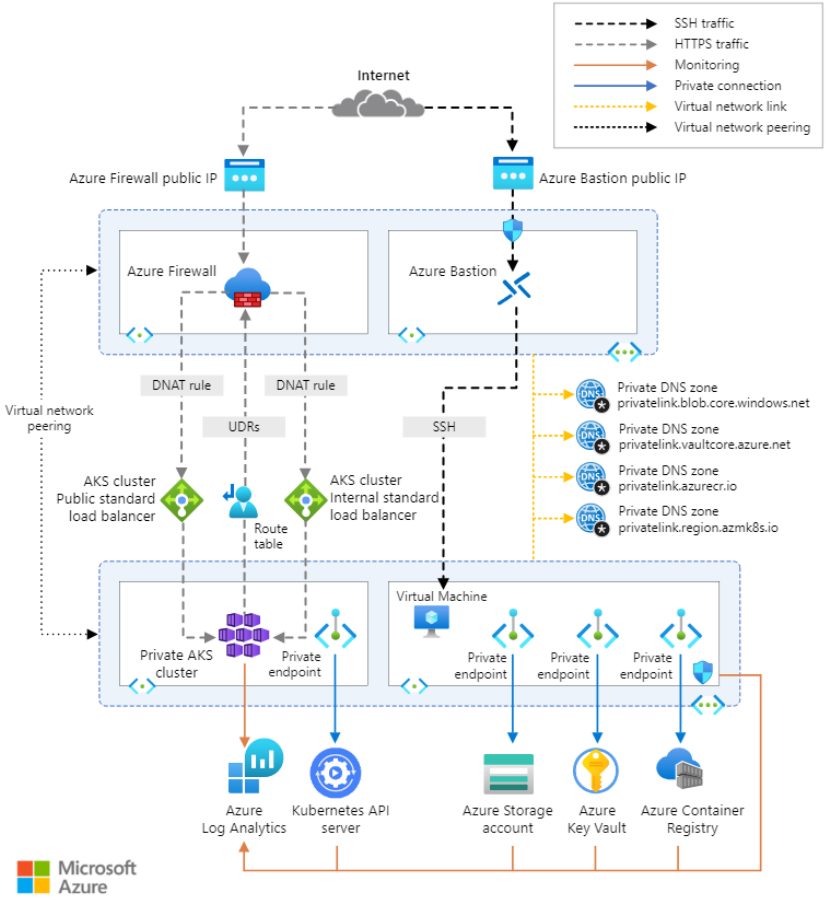
Each route contains an address prefix and next hop type. When traffic leaving a subnet is sent to an IP address within the address prefix of a route, the route that contains the prefix is the route Azure uses. Learn more about how Azure selects a route when multiple routes contain the same prefixes, or overlapping prefixes. Whenever a virtual network is created, Azure automatically creates the following default system routes for each subnet within the virtual network:

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	172.16.0.0/12	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None



https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Routes and Route Tables



Hands-on Demo

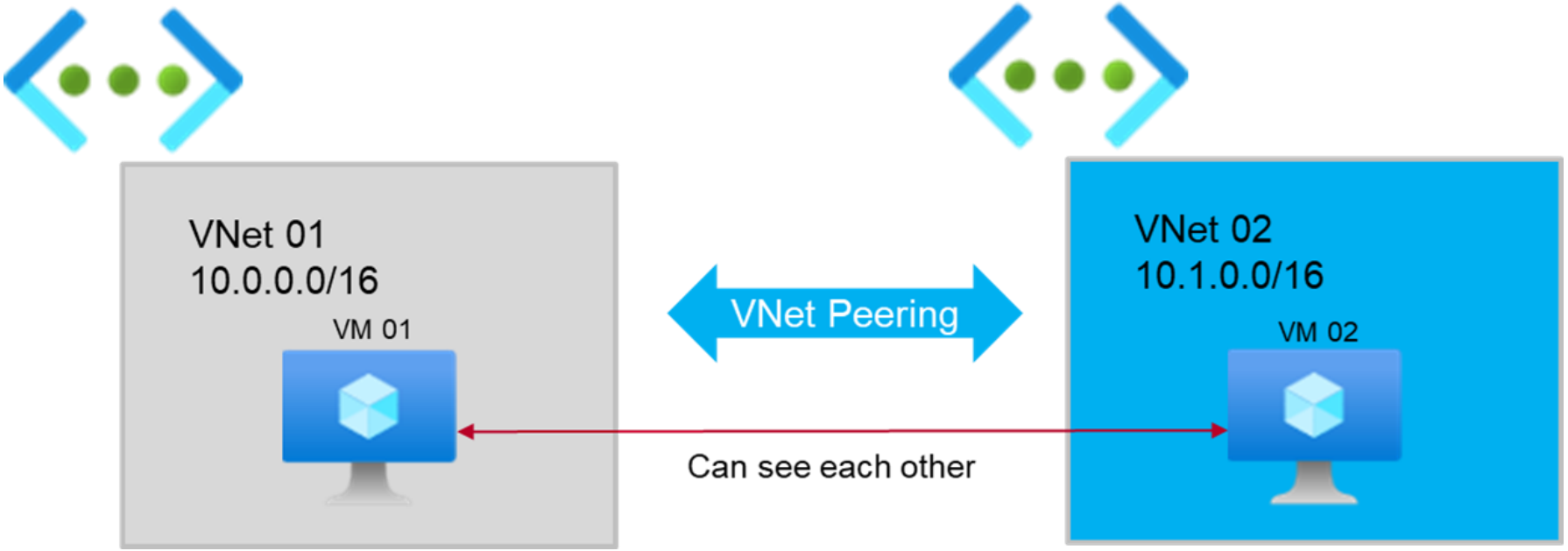
- Creating a Route Table and assign it to a subnet

Azure VNET Peering

- Virtual network peering enables you to connect two or more Virtual Networks in Azure.

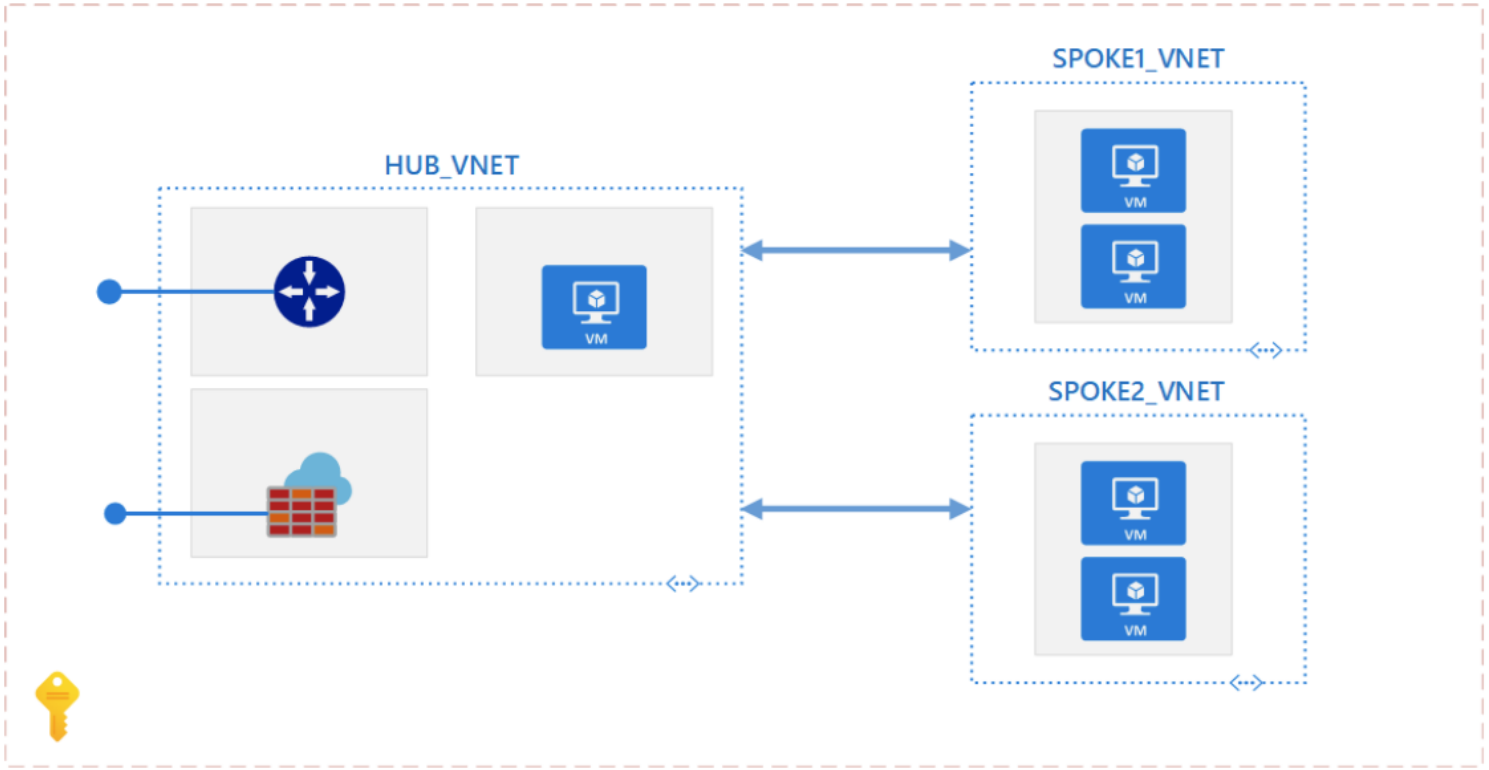
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

Azure VNET Peering



https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

Azure VNET Peering



https://learn.microsoft.com/en-us/azure/architecture/networking/prefixes/add-ip-space-peered-vnet

Hands-on Demo

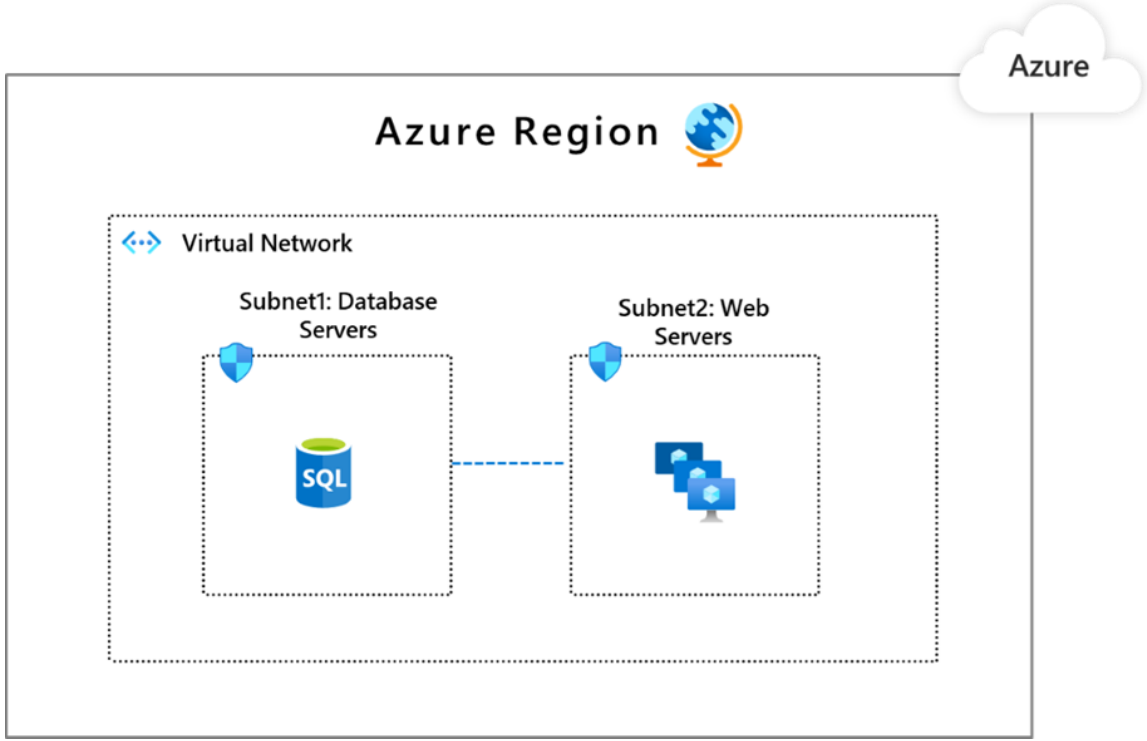
- Peering two Azure VNets

Common Azure VNET topologies (segmentation)

- Azure Network common topologies
  - Single VNet
  - Peered VNets
  - Hub/Spoke

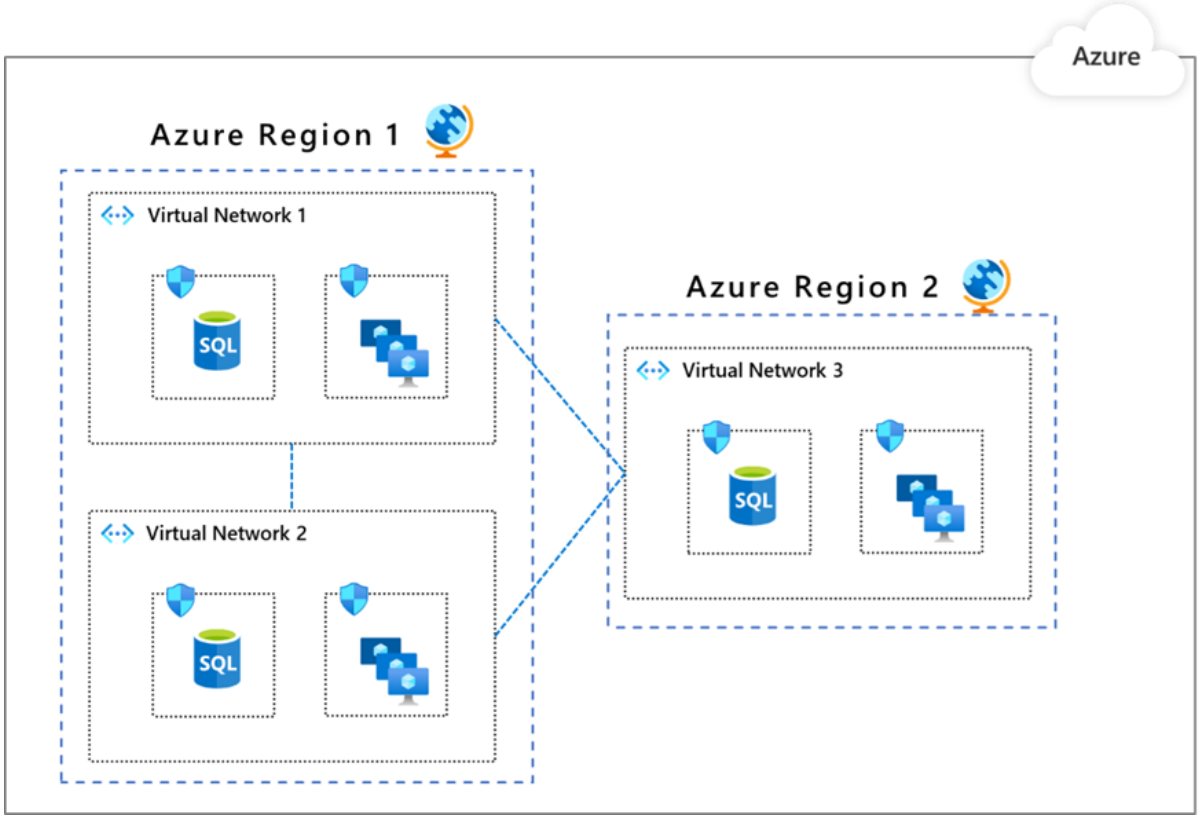
https://learn.microsoft.com/en-us/azure/well-architected/security/networking

Common Azure VNET topologies (segmentation)



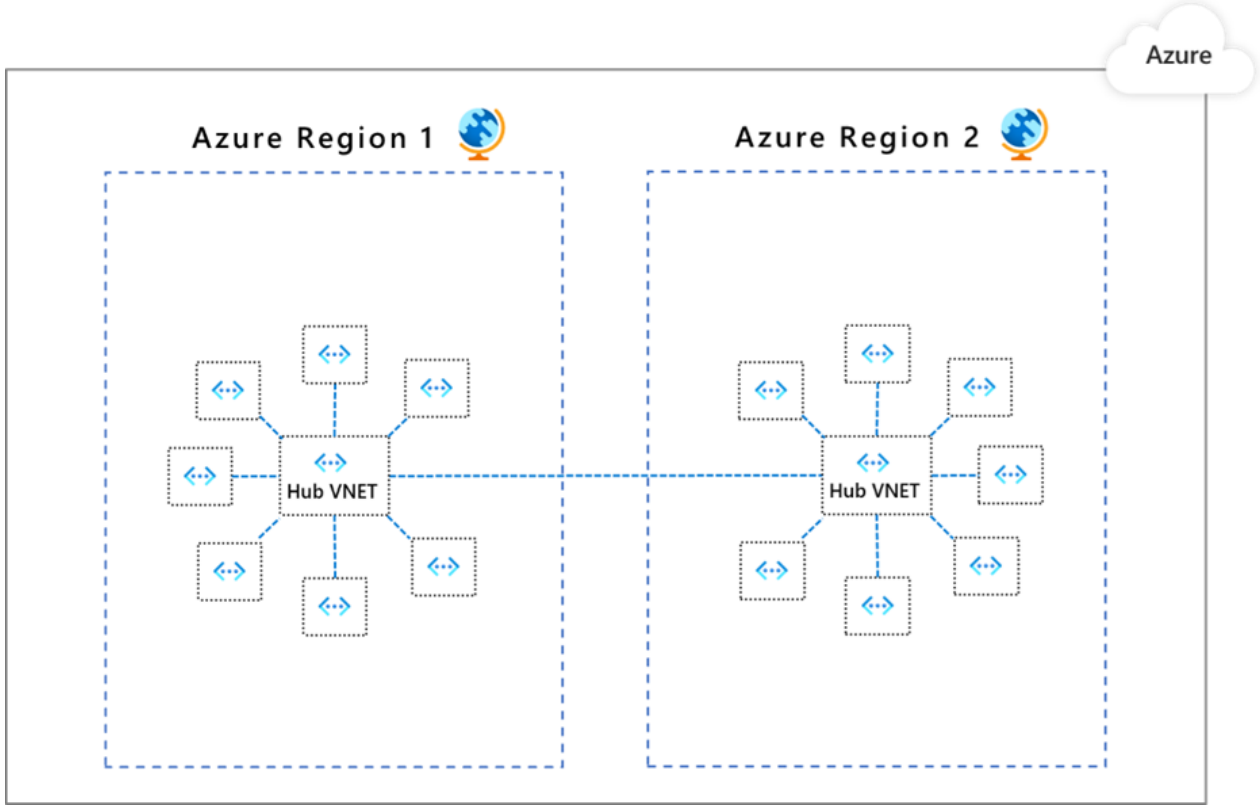
https://learn.microsoft.com/en-us/azure/well-architected/security/networking

Common Azure VNET topologies (segmentation)



https://learn.microsoft.com/en-us/azure/well-architected/security/networking

Common Azure VNET topologies (segmentation)



https://learn.microsoft.com/en-us/azure/well-architected/security/networking

Q&A

Break

Azure Networking Fundamentals

- Network Security Groups (NSGs) [see 1]
- Azure Firewall, rules [see 1 2]
- Azure service firewalls (Storage, Cosmos DB, SQL) [see 1 2 3]
- Private Link and Private Endpoints
- Azure NAT Gateway [see 1]

Poll: Which resource(s) can be used to secure both inbound and outbound traffic?

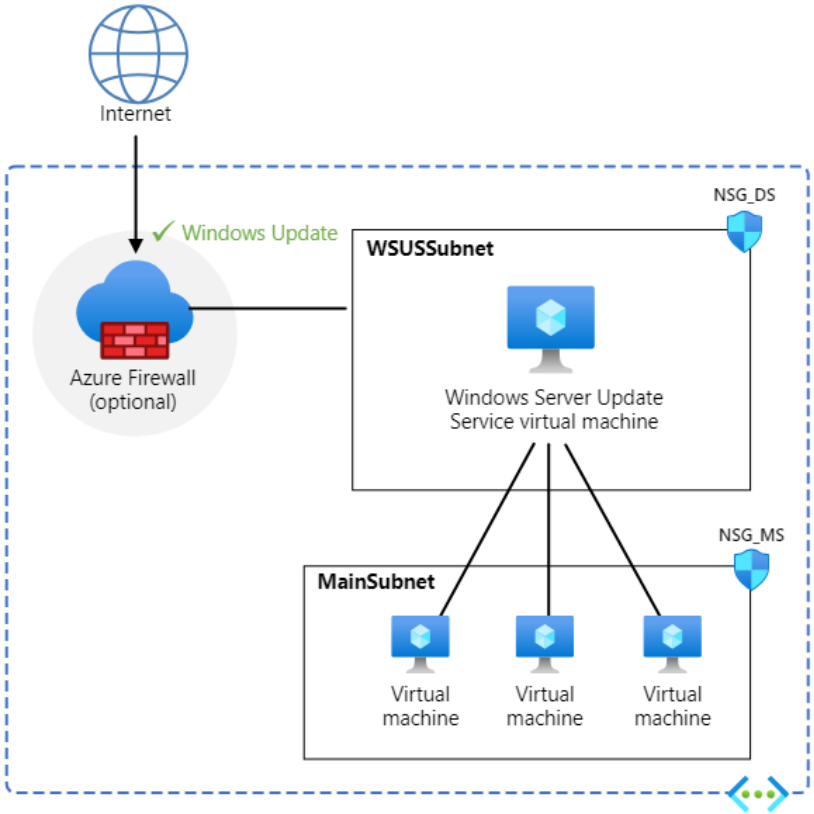
- NSG
- Azure Firewall
- NSG and Azure Firewall
- Web Application Firewall (WAF)

Network Security Groups (NSGs)

- Use an Azure network security group (NSG) to filter network traffic between Azure resources in an Azure virtual network.
- Security Rules
  - Inbound
  - Outbound
- Assign NSGs to
  - Subnets
  - NICs

https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Network Security Groups (NSGs)



Microsoft Azure

Hands-on Demo

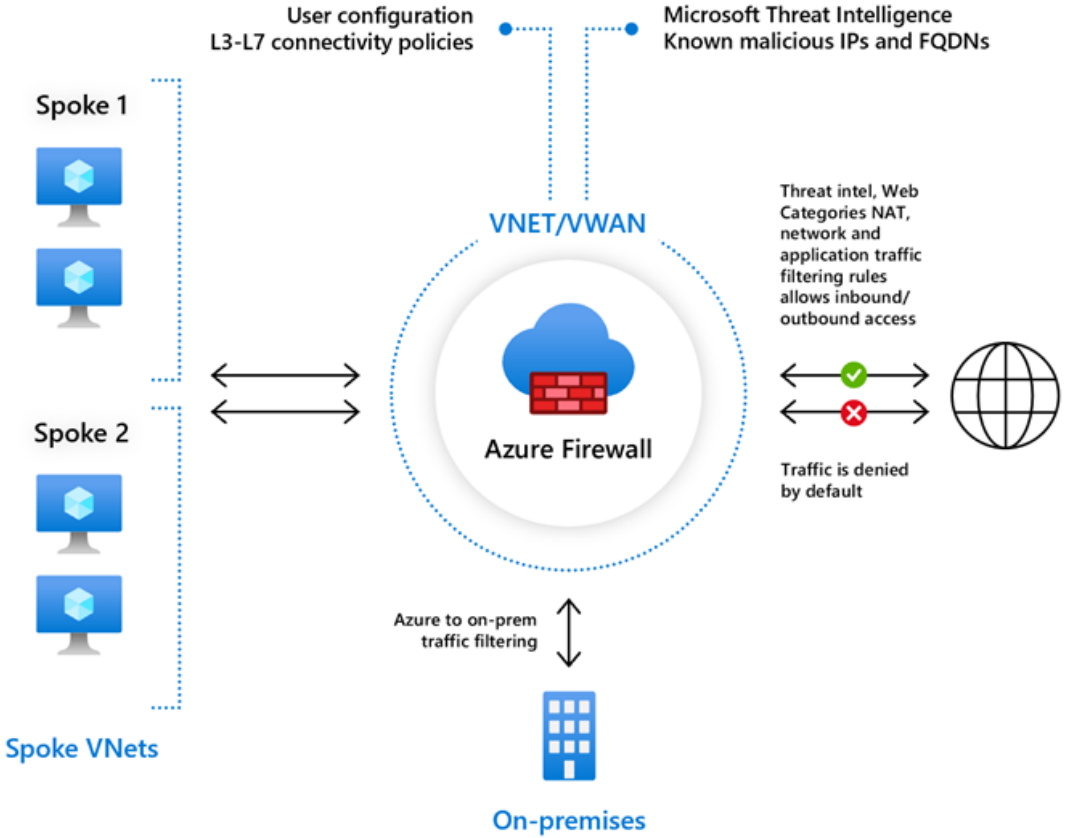
- Creating a Network Security Group (NSG)
- Protecting our VM using the NSG

Azure Firewall, rules

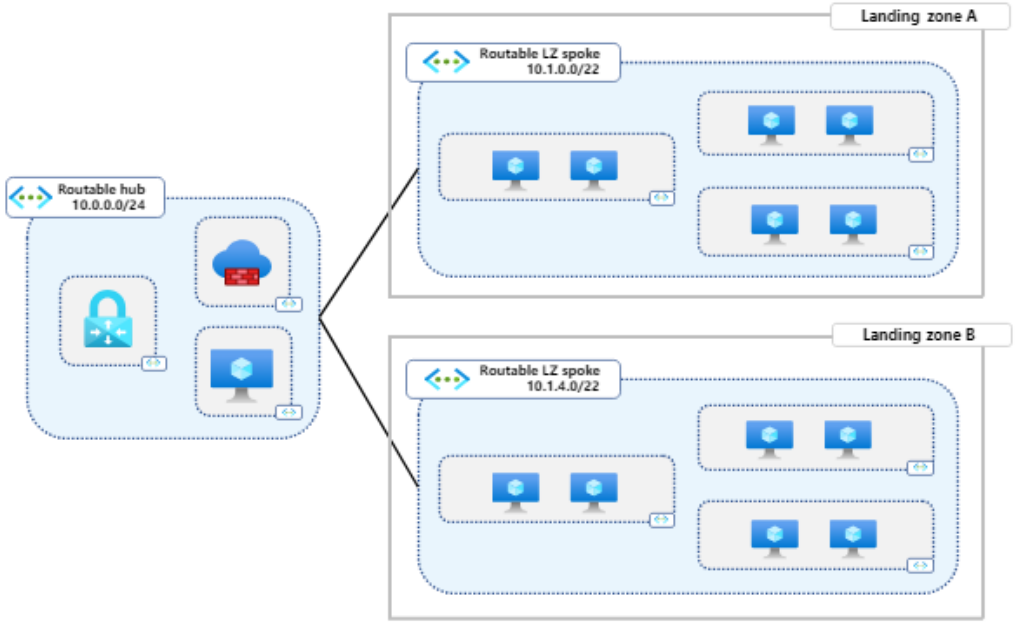
- Azure Firewall is a cloud-native firewall service that provides threat protection for cloud workloads running in Azure.
- Tiers
  - Basic
  - Standard
  - Premium
- Rules
  - DNAT
  - Network
  - Application

https://learn.microsoft.com/en-us/azure/firewall/overview
https://learn.microsoft.com/en-us/azure/firewall/rule-processing

Azure Firewall, rules



Azure Firewall, rules



Microsoft Azure

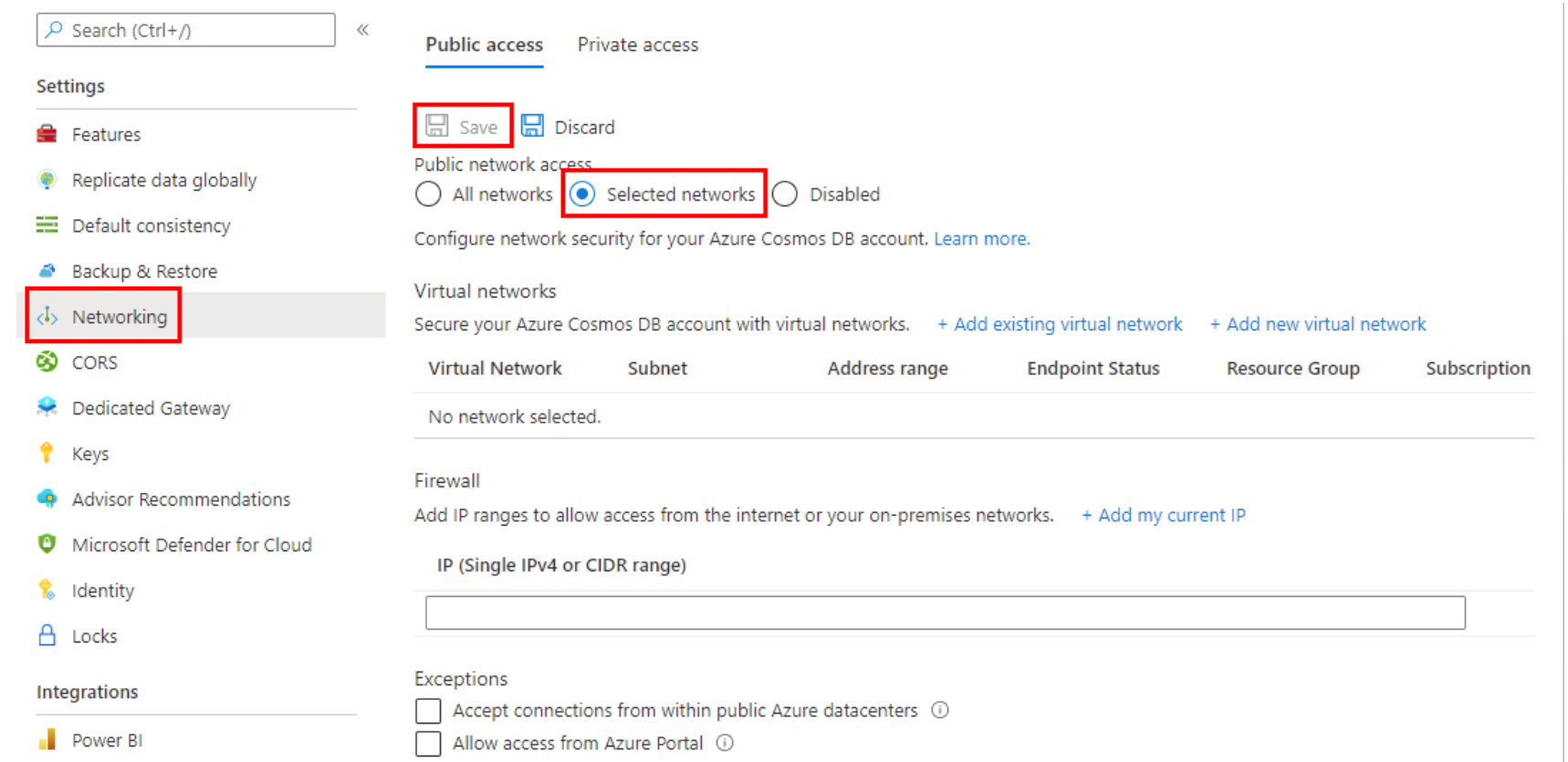
Hands-on Demo

- Provisioning an Azure Firewall resource

Azure service firewalls (Storage, Cosmos DB, SQL)

- Azure Storage, Cosmos DB, SQL and other resources provide a layered security model.
- This model enables you to control the level of access to your resource based on the client subset or IP address.

Azure service firewalls (Storage, Cosmos DB, SQL)



Hands-on Demo

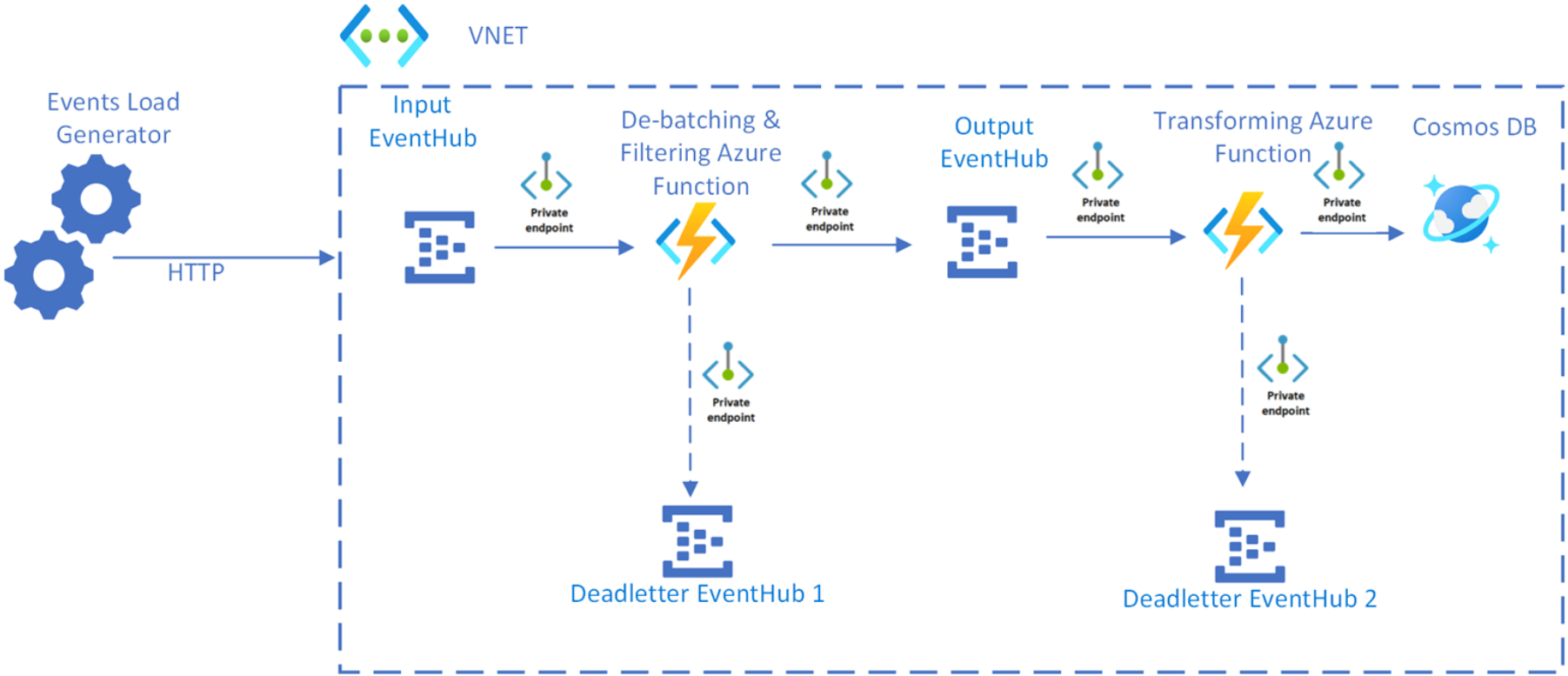
- Enabling service firewall for
  - Azure Storage Account
  - Azure SQL
  - Azure Cosmos DB
  - Azure Event Hubs

Private Link and Private Endpoints

- Azure Private Link enables you to access some Azure PaaS Services (e.g. , Azure Cosmos DB) over a private endpoint in your virtual network.
- The traffic does not go over public Internet
- Strongly recommended for Production workloads

https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

Private Link and Private Endpoints



Hands-on Demo

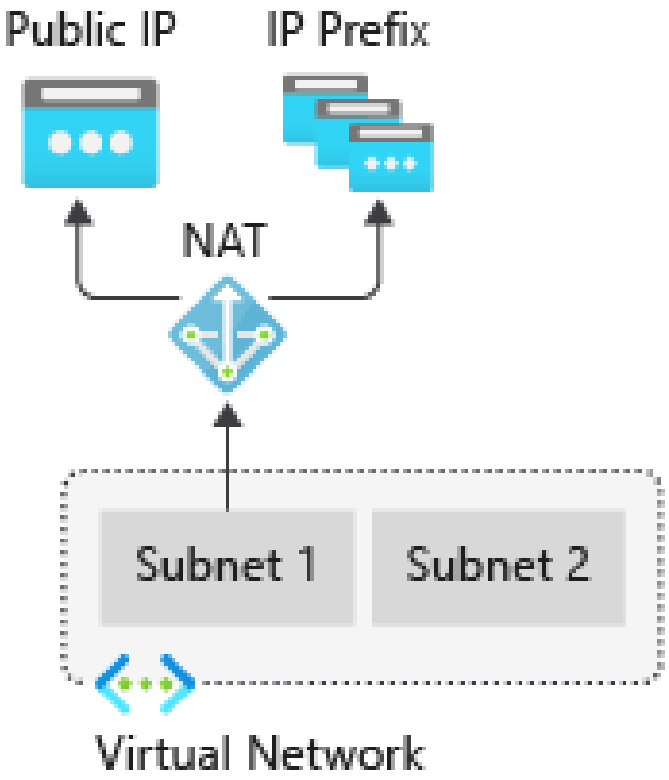
- Using Private Link with Azure Storage Account

Azure NAT Gateway

- Azure NAT Gateway is a fully managed Network Address Translation (NAT) service.
- Use Azure NAT Gateway to let all instances in a private VNets connect to the internet while remaining private.

https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview

Azure NAT Gateway



Hands-on Demo

- Using NAT Gateway to hide our VM IP address

Q&A

Takeaways

- O’Reilly Azure Cookbook
- Microsoft Azure Fundamentals (AZ-900) Certification Course
- Exam AZ-700: Designing and Implementing Microsoft Azure Networking Solutions


O'REILLY®