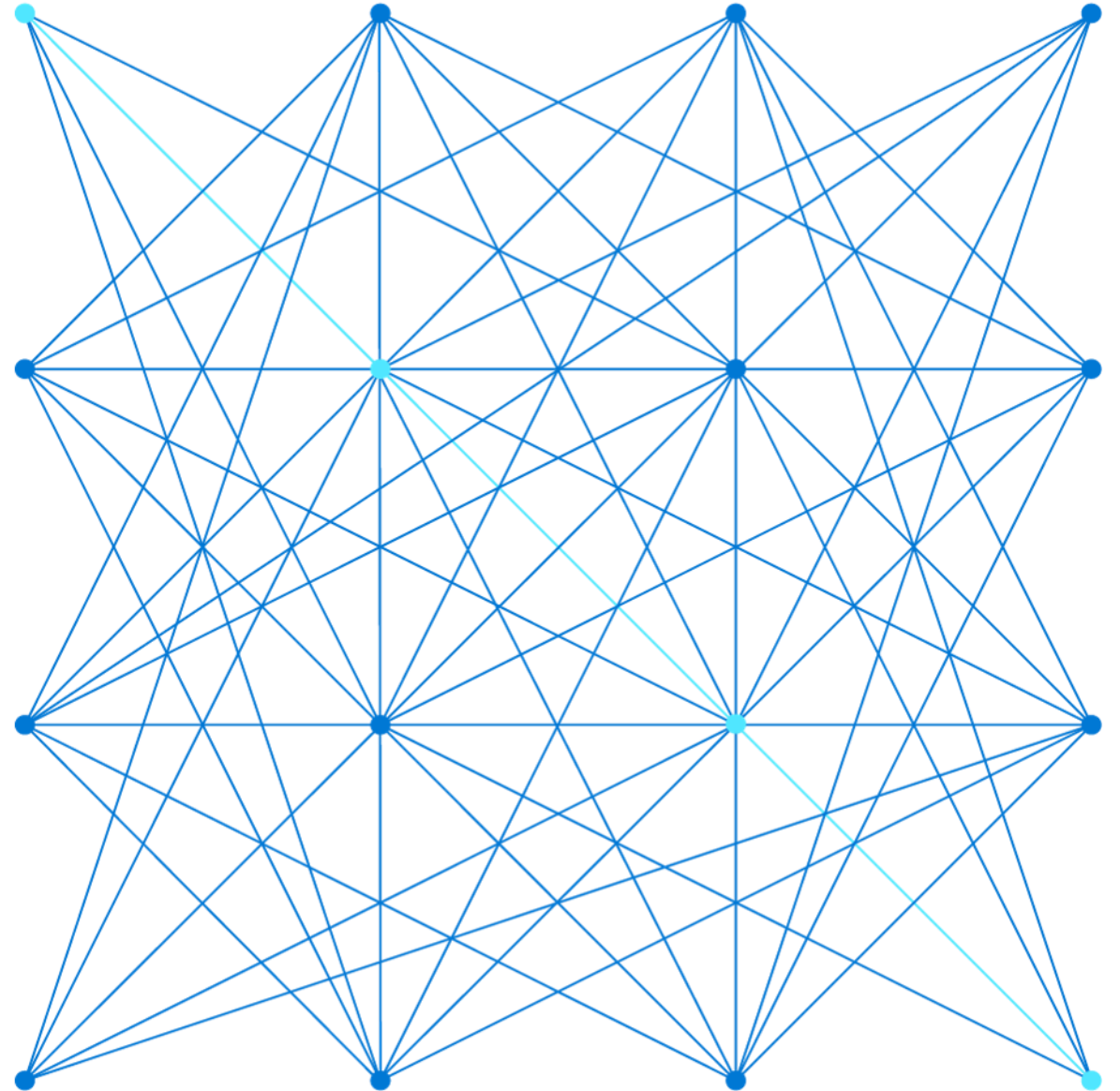


AZ-104

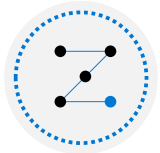
Administer Network Traffic



About this course: Course Outline



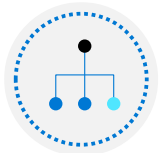
01: Administer Identity



02: Administer Governance and Compliance



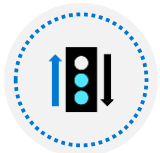
03: Administer Azure Resources



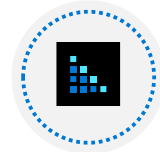
04: Administer Virtual Networking



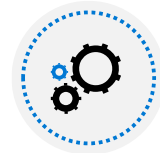
05: Administer Intersite Connectivity



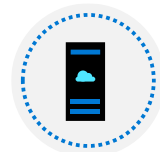
06: Administer Network Traffic Management



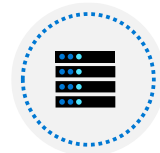
07: Administer Azure Storage



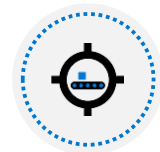
08: Administer Azure Virtual Machines



09: Administer PaaS Compute Options

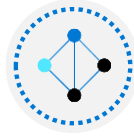


10: Administer Data Protection



11: Administer Monitoring

Administer Network Traffic Introduction



[Configure Network Routing and Endpoints](#)



[Configure Azure Load Balancer](#)



[Configure Application Gateway](#)

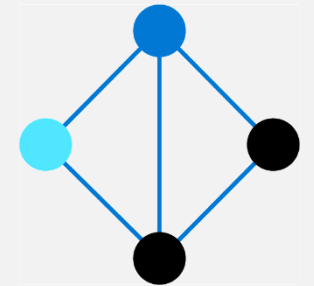


[Configure Network Watcher](#)

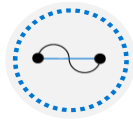


[Lab 06 – Implement Traffic Management](#)

Configure Network Routing and Endpoints



Configure Network Routing and Endpoints Introduction



Review System Routes

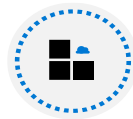


Identify User-Defined Routes

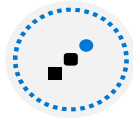


Demonstration – Custom Routing tables

- Examine a Routing Example



Determine Service Endpoint Uses



Identify Private Link Uses

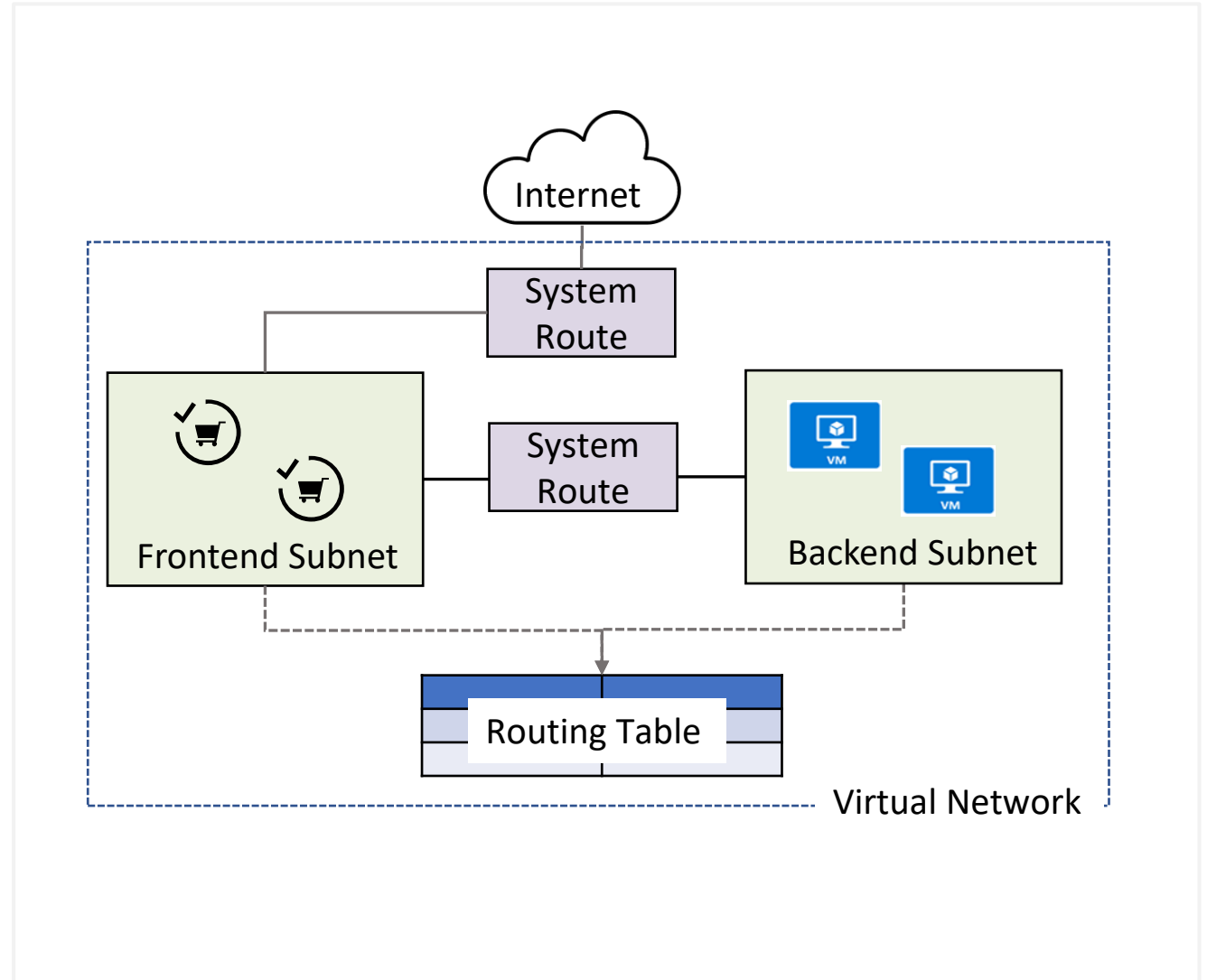


Summary and Resources

Review System Routes

System routes direct network traffic between virtual machines, on-premises networks, and the internet:

- Traffic between VMs in the same subnet
- Between VMs in different subnets in the same virtual network
- Data flow from VMs to the internet
- Communication between VMs using a VNet-to-VNet VPN
- Site-to-Site and ExpressRoute communication through the VPN gateway

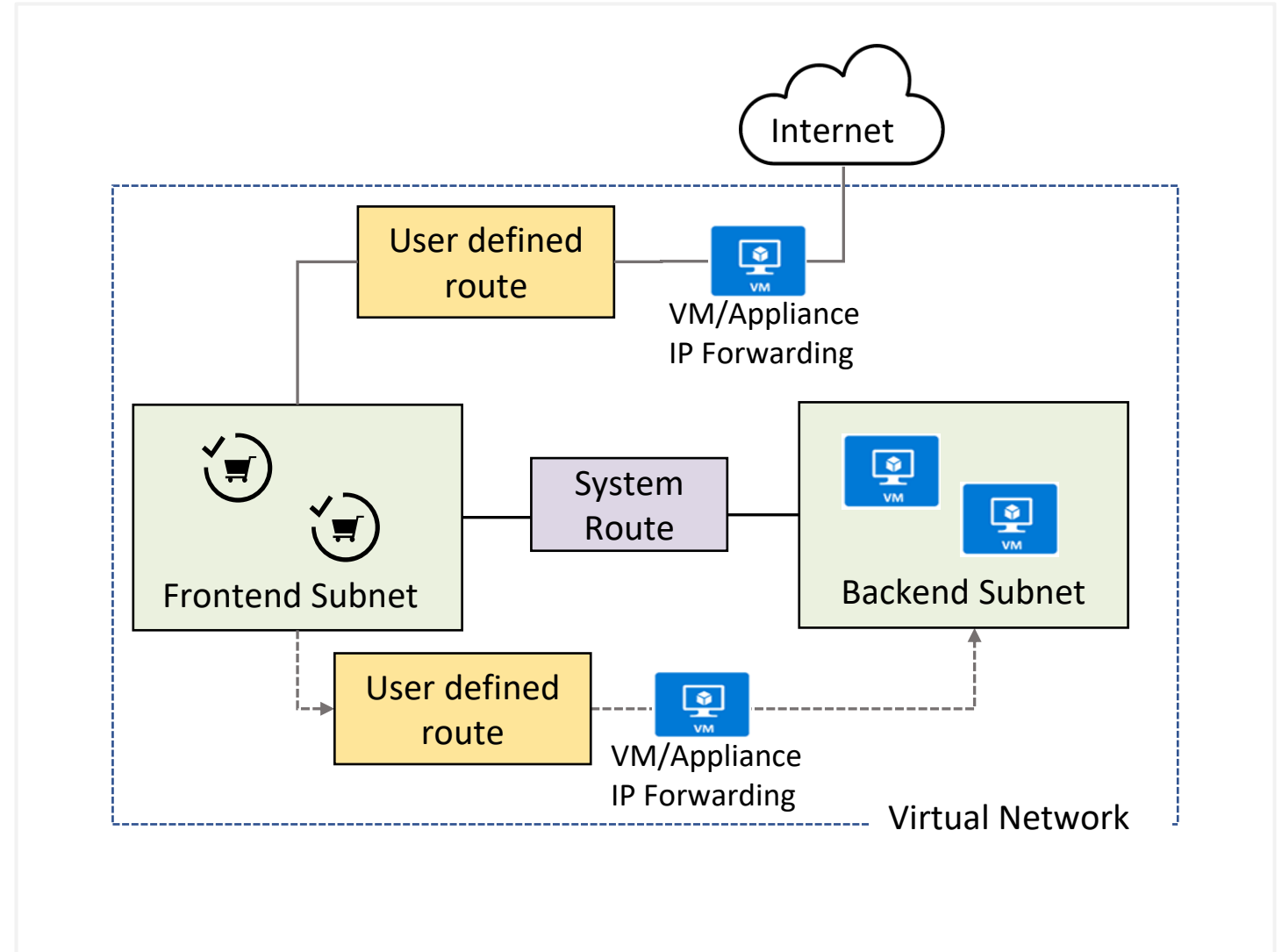


Identify User-Defined Routes

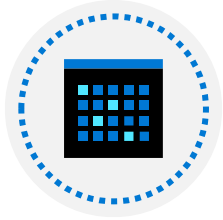
A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network

User-defined routes are custom routes that control network traffic by defining routes that specify the next hop of the traffic flow

The next hop can be a virtual network gateway, virtual network, internet, or virtual appliance



Demonstration – Custom Routing Tables



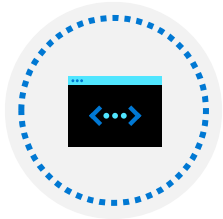
Create a route table



Add a route



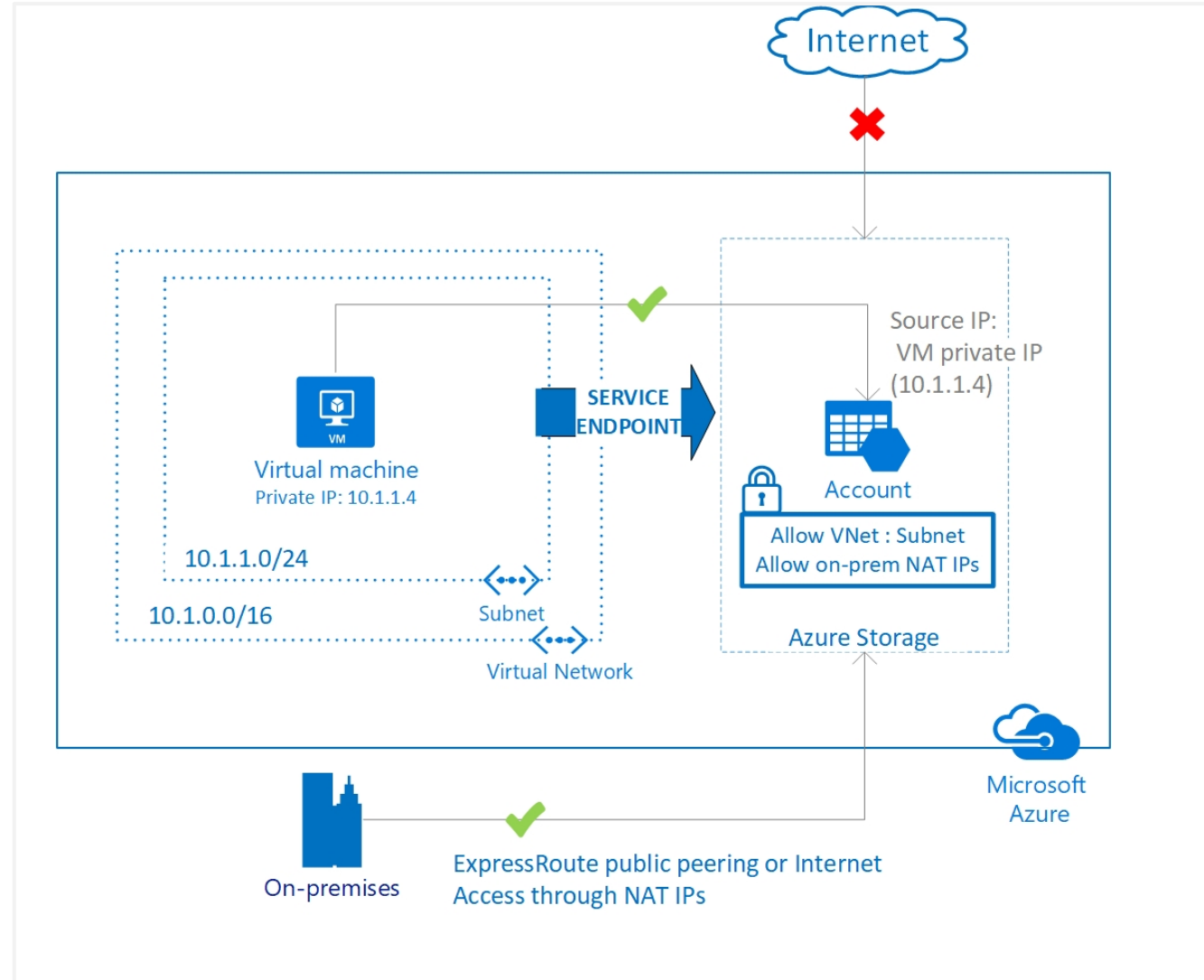
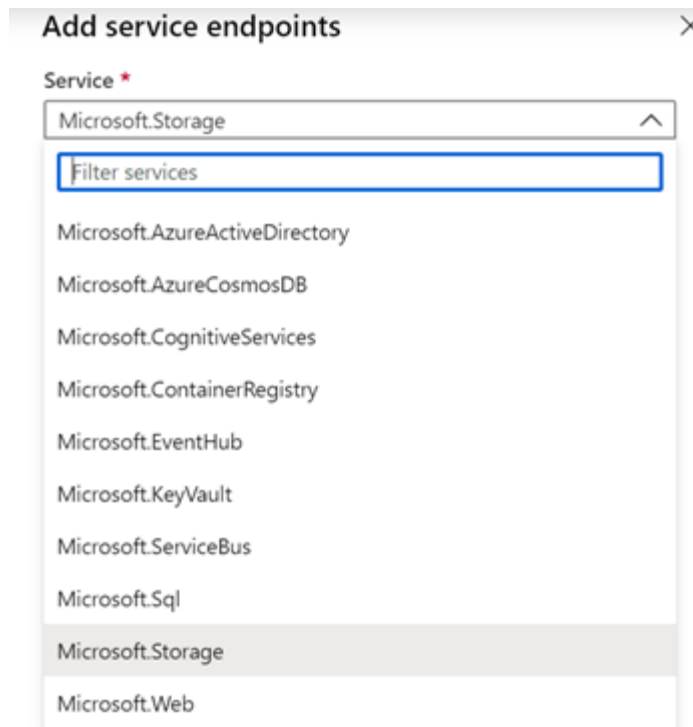
Associate a route table to a subnet



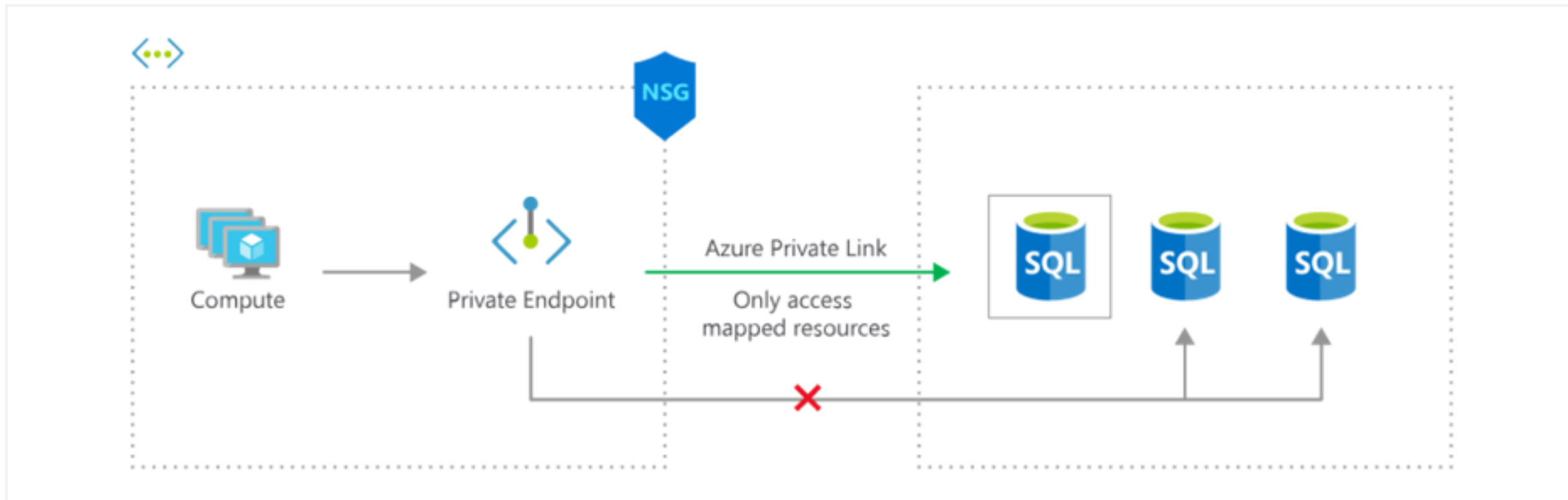
Use PowerShell to view your routing information (optional)

Determine Service Endpoint Uses

Endpoints limit network access to specific services -Adding service endpoints can take up to 15 minutes to complete



Identify Private Link Uses



Private connectivity to services on Azure. Traffic remains on the Microsoft network, with no public internet access

Integration with on-premises and peered networks

In the event of a security incident within your network, only the mapped resource would be accessible

Summary and Resources – Configure Network Routing and Endpoints

Knowledge Check Questions



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

[Manage and control traffic flow in your Azure deployment with routes \(Sandbox\)](#)

[Introduction to Azure Private Link](#)

A sandbox indicates a hands-on exercise.

Configure Azure Load Balancer



Configure Azure Load Balancer Introduction



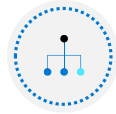
Choose a Load Balancer Solution



Implement a Public Load Balancer



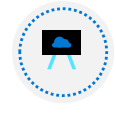
Implement an Internal Load Balancer



Determine Load Balancer SKUs



Create Backend Pools



Create Load Balancer Rules



Configure Session Persistence (optional)



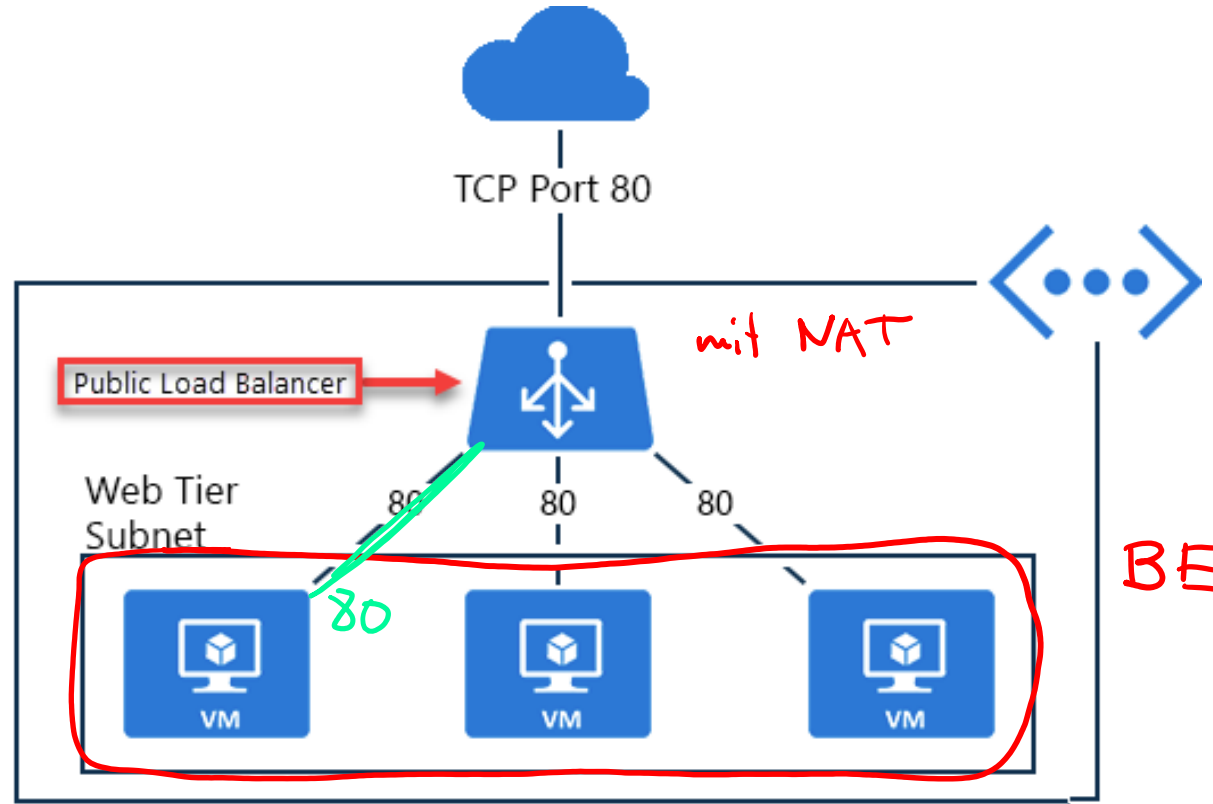
Summary and Resources

Choose a Load Balancer Solution

Feature	Application Gateway	Front Door	Load Balancer	Traffic Manager
Usage	Optimize delivery from application server farms while increasing application security with web application firewall.	Scalable, security-enhanced delivery point for global, micro service-based web applications.	Balance inbound and outbound connections and requests to your applications or server endpoints.	Distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.
Protocols	HTTP, HTTPS, HTTP2	HTTP, HTTPS, HTTP2	TCP, UDP	Any
Private	Yes		Yes	
Global		Yes		Yes
Env	Azure, non-Azure cloud, on premises	Azure, non-Azure cloud, on premises	Azure	Azure, non-Azure cloud, on premises
Security	WAF	WAF, NSG	NSG	

Implement a Public Load Balancer

Standard
Basic (free)



Maps public IP addresses and port number of incoming traffic to the VM's private IP address and port number, and vice versa

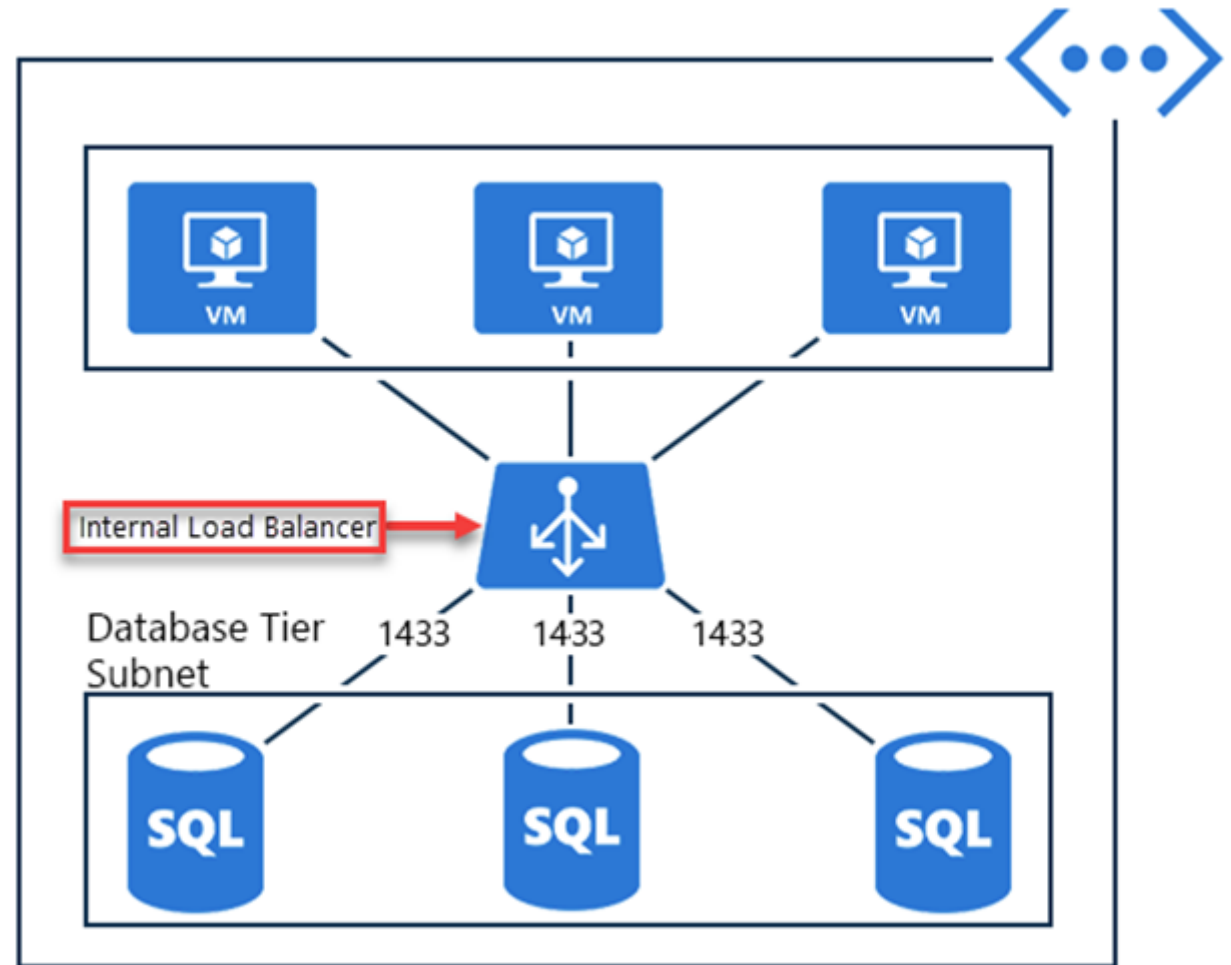
Apply load balancing rules to distribute traffic across VMs or services

Implement an Internal Load Balancer

Directs traffic only to resources inside a virtual network or that use a VPN to access Azure infrastructure

Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint

Enables load balancing within a virtual network, for cross-premises virtual networks, for multi-tier applications, and for line-of-business applications



Determine Load Balancer SKUs

Feature	Basic SKU	Standard SKU
Backend pool	Up to 300 instances	Up to 1000 instances
Health probes	TCP, HTTP	TCP, HTTP, HTTPS
Availability zones	Not available	Zone-redundant and zonal frontends for inbound and outbound traffic
Multiple frontends	Inbound only	Inbound and outbound
Secure by default	Open by default. NSG optional.	Closed to inbound flows unless allowed by a NSG. Internal traffic from the virtual network to the internal load balancer is allowed.
SLA	Not available	99.99%

Free

Instance details

Name *
lb01 ✓

Region *
(US) East US

Type * ⓘ
☒ Internal ☐ Public

SKU * ⓘ
☒ Basic ☐ Standard

Configure virtual network.

Virtual network * ⓘ
vnet01

Subnet *
subnet01 (10.1.0.0/24)
[Manage subnet configuration](#)

IP address assignment *
☐ Static ☒ Dynamic

Create Backend Pools

SETTINGS

Backend pools

Name

cesbackendpool

Associated to

Unassociated

Unassociated

Availability set

Single virtual machine

Virtual machine scale set

SKU	Backend pool endpoints
Basic SKU	VMs in a single availability set or VM scale set
Standard SKU	Any VM in a single virtual network, including a blend of VMs, availability sets, and VM scale sets

To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer

Create Load Balancer Rules

Maps a frontend IP and port combination to a set of backend pool and port combination

Rules can be combined with NAT rules

A NAT rule is explicitly attached to a VM (or network interface) to complete the path to the target

Add load balancing rule ✕

lbr01

Name *
lbr01 ✓

IP Version *
☒ IPv4 ☐ IPv6

Frontend IP address * ⓘ
10.1.0.4 (LoadBalancerFrontEnd) ▼

Protocol
☒ TCP ☐ UDP

Port *
80 443

Backend port * ⓘ
80 443

Backend pool ⓘ
bep01 ▼

Health probe ⓘ
hp01 (HTTP:80) ▼

Session persistence ⓘ
None ▼

Idle timeout (minutes) ⓘ
 4

Floating IP (direct server return) ⓘ
☒ Disabled ☐ Enabled

Configure Session Persistence (optional)

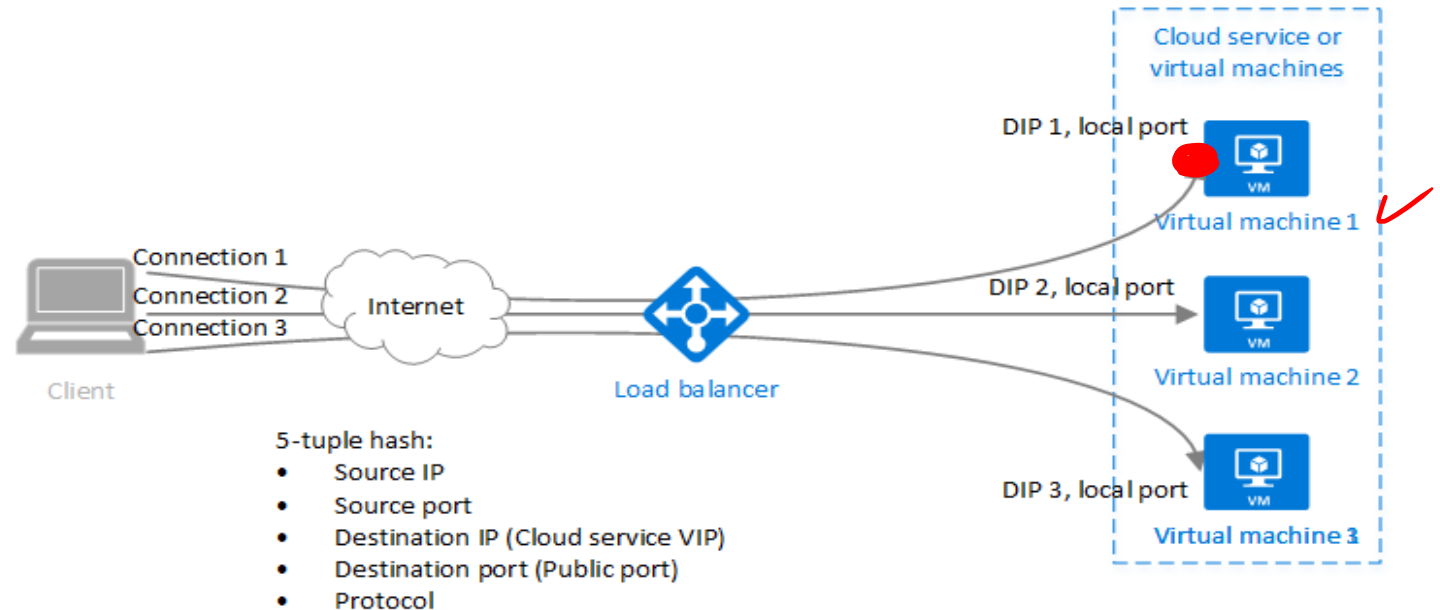
Session persistence ⓘ

None

None

Client IP

Client IP and protocol



Session persistence specifies how client traffic is handled

None (default) requests can be handled by any virtual machine

Client IP requests will be handled by the same virtual machine

Client IP and protocol specifies that successive requests from the same address and protocol will be handled by the same virtual machine

Summary and Resources – Configure Azure Load Balancer

Knowledge Check Questions



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

[Improve application scalability and resiliency by using Azure Load Balancer \(Sandbox\)](#)

[Load balance non-HTTP\(S\) traffic in Azure](#)

A sandbox indicates a hands-on exercise.

Configure Azure Application Gateway

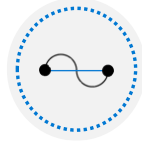
web



Configure Azure Application Gateway Introduction



Implement Application Gateway



Determine Application Gateway Routing

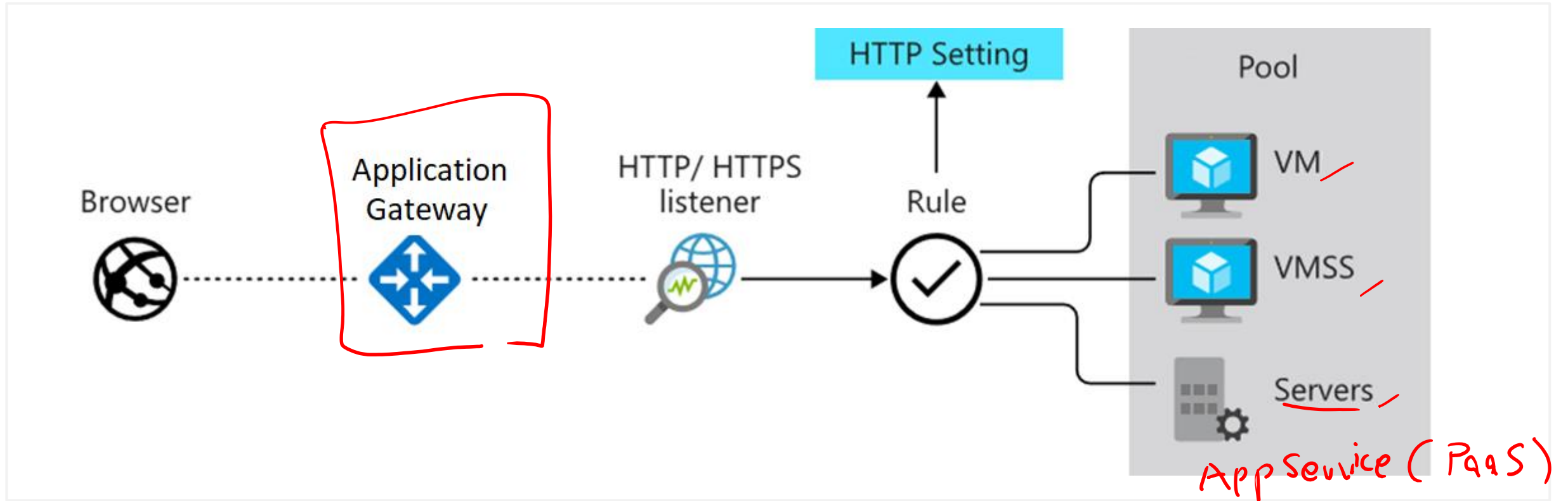


Setup Application Gateway Components (optional)



Summary and Resources

Implement Application Gateway



Manages web app requests

Routes traffic to a pool of web servers based on the URL of a request

The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

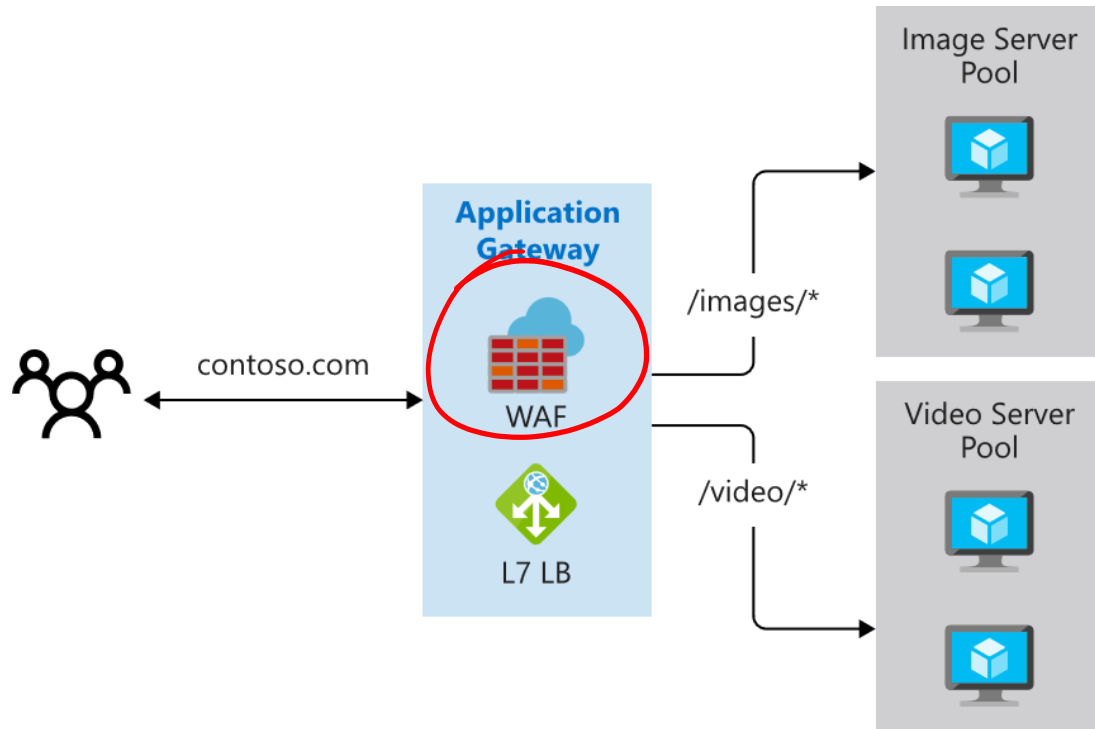
Determine Application Gateway Routing

Region

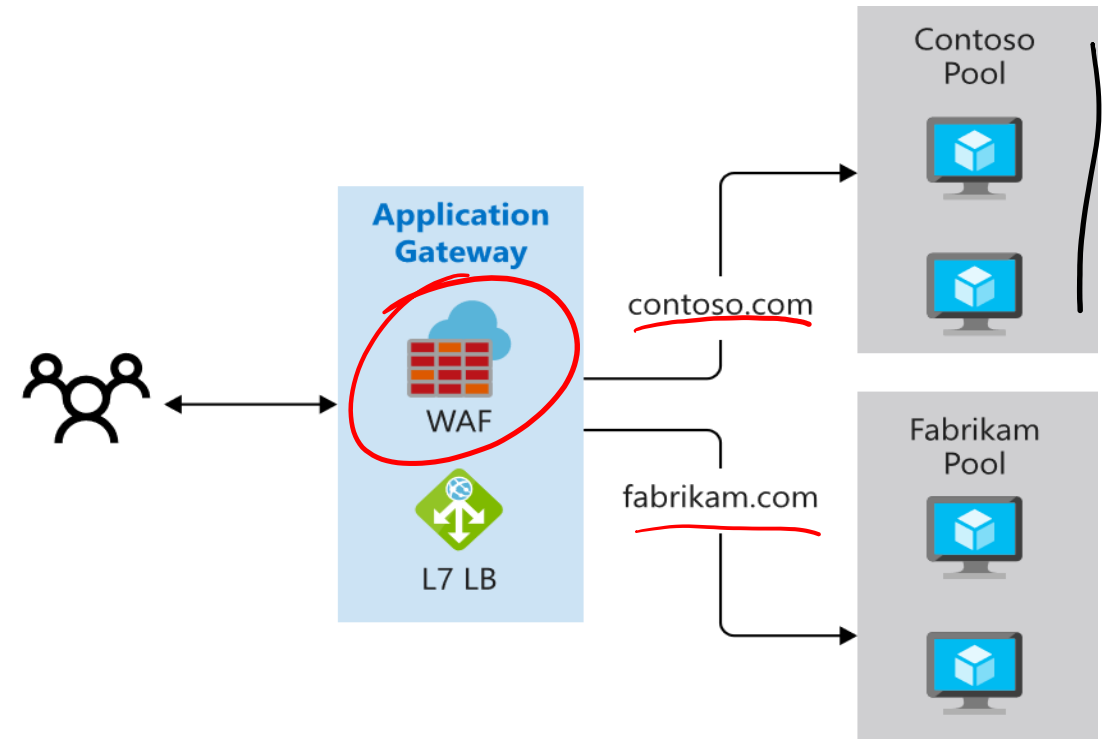
Front Door
+ CDN

Global

Path-based routing



Multiple-site routing



Setup Application Gateway Components (optional)

Frontend IP

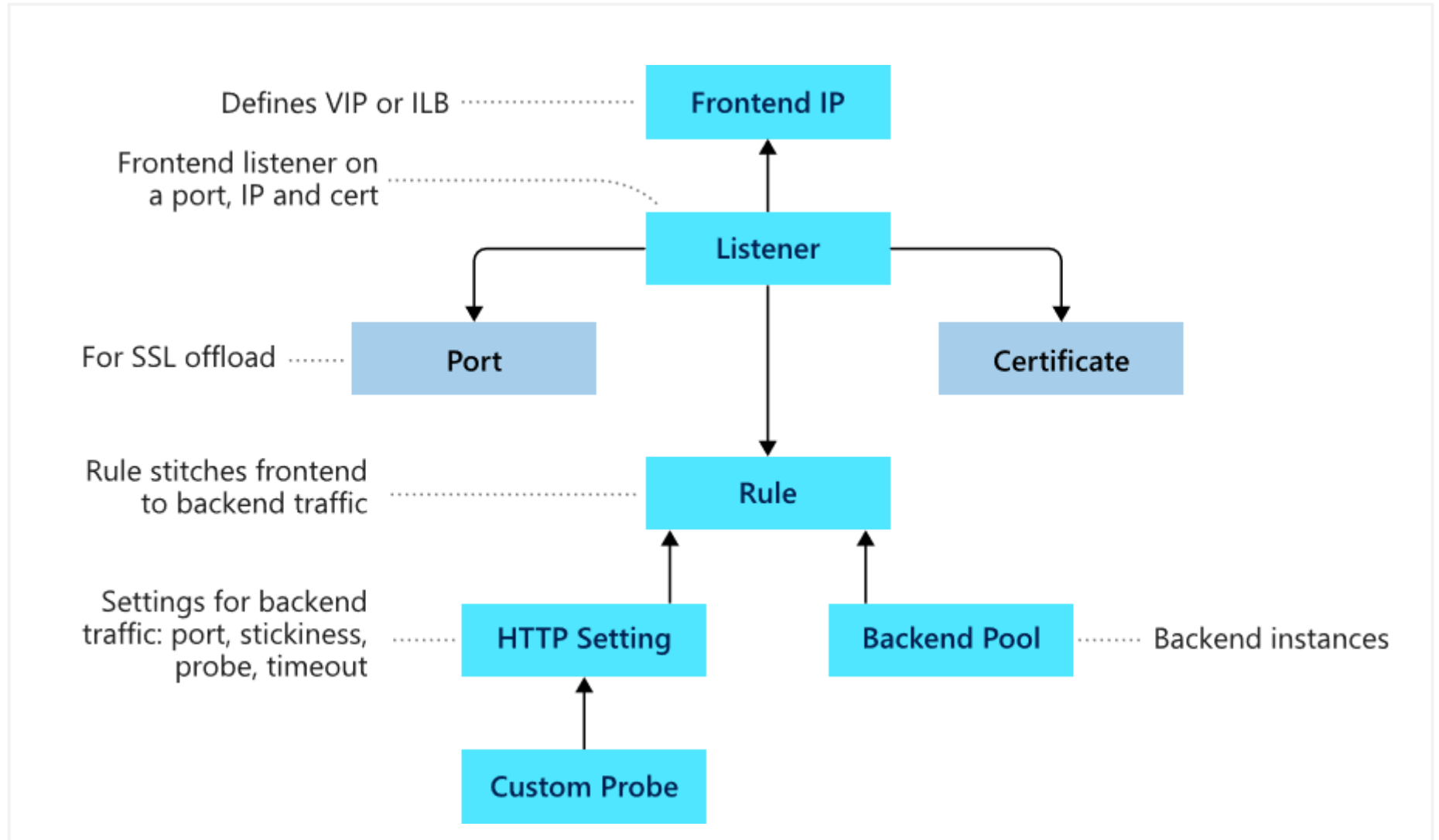
Listeners

Routing rules

Backend pools

Web application
firewall (optional)

Health probes



Summary and Resources – Configure Azure Application Gateway

Knowledge Check Questions



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

[Introduction to Azure Application Gateway](#)

[Load balance your web service traffic with Application Gateway](#)






[Load balance HTTP\(S\) traffic in Azure](#)

[Encrypt network traffic end to end with Azure Application Gateway](#)

Configure Network Watcher



Configure Network Watcher Introduction

-  Describe Network Watcher Features
-  Review IP Flow Verify Diagnostics
-  Review Next Hop Diagnostics
-  Visualize the Network Topology
-  Summary and Resources

Describe Network Watcher Features

A **regional service** that provides various network diagnostic and monitoring tools

IP Flow Verify diagnoses connectivity issues

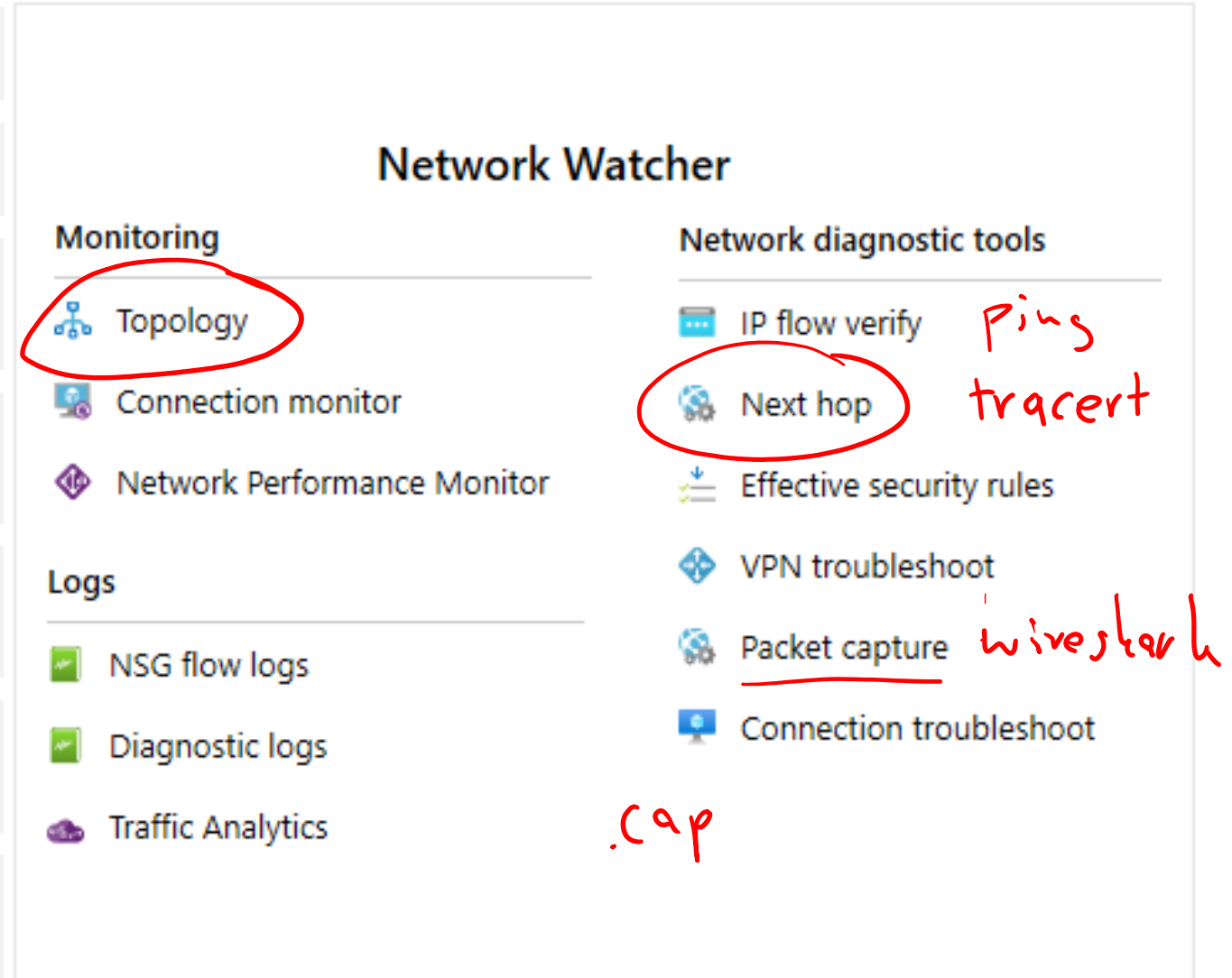
Next Hop determines if traffic is being correctly routed

VPN Diagnostics troubleshoots gateways and connections

NSG Flow Logs maps IP traffic through a network security group

Connection troubleshoot shows connectivity between source VM and destination

Topology generates a visual diagram of resources



Review IP Flow Verify Diagnostics

Checks if a packet is allowed or denied to or from a virtual machine

Network diagnostic tools

IP flow verify

Next hop

Effective security rules

VPN troubleshoot

Packet capture

Connection troubleshoot

Metrics

Usage + quotas

Logs

NSG flow logs

Diagnostic logs

Traffic Analytics

Packet details

Protocol

☒ TCP ☐ UDP

Direction

☒ Inbound ☐ Outbound

Local IP address * ⓘ

10.1.1.4

Local port * ⓘ

3389

Remote IP address * ⓘ

13.24.35.46

Remote port * ⓘ

3389

Check

✖ Access denied

Security rule

DenyAllInBound

Review Next Hop Diagnostics

Helps with determining whether traffic is being directed to the intended destination by showing the next hop

Subscription * ⓘ
MSDN Platforms Subscription

Resource group * ⓘ
Demo

Virtual machine * ⓘ
vm01

Network interface *
vm01165

Source IP address * ⓘ
10.1.1.4

Destination IP address * ⓘ
13.24.35.46

Next hop

Result

Next hop type

None

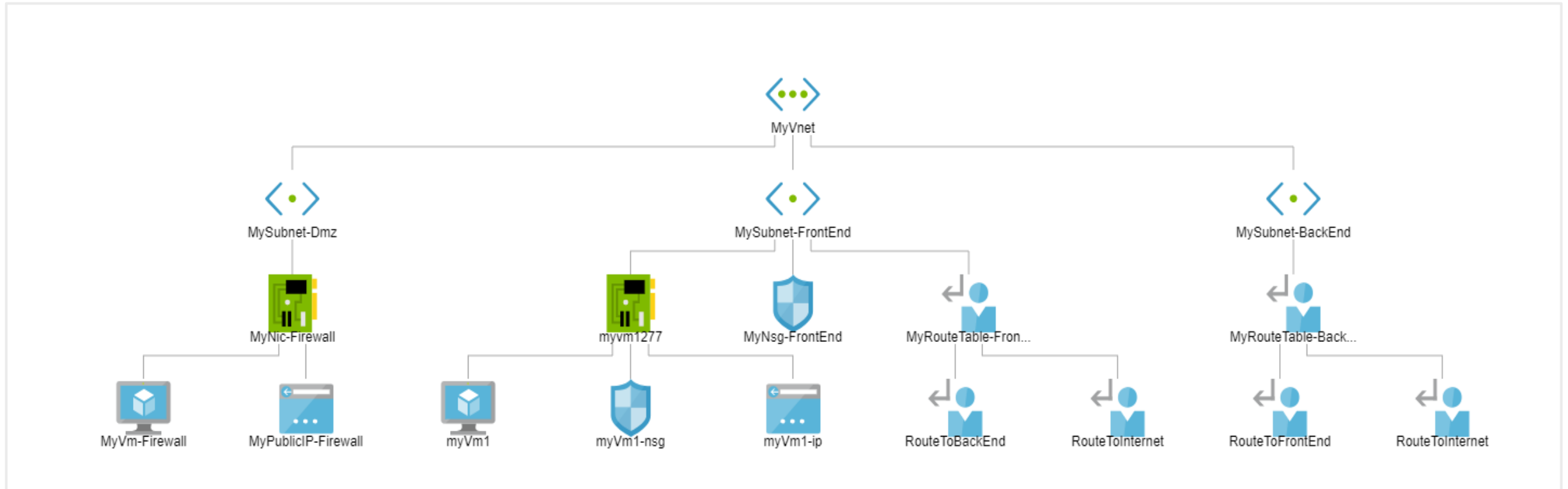
IP address

10.1.1.100

Route table ID

/subscriptions/2301e3a0-8420-...

Visualize the Network Topology



Provides a visual representation of your networking elements

View all the resources in a virtual network, resource to resource associations, and relationships between the resources

The Network Watcher instance in the same region as the virtual network

Summary and Resources – Configure Network Watcher

Knowledge Check Questions



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

[Introduction to Azure Network Watcher](#)

[Monitor and troubleshoot your end-to-end Azure network infrastructure by using network monitoring tools](#)

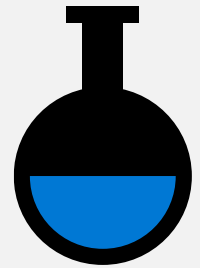
[Analyze your Azure infrastructure by using Azure Monitor logs \(Sandbox\)](#)

[Monitor the performance of virtual machines using Azure Monitor VM Insights \(Sandbox\)](#)

[Write your first query with Kusto Query Language](#)

A sandbox indicates a hands-on exercise.

Lab – Implement Traffic Management



Lab 06 – Implement traffic management

Scenario

You are tasked with implementing a hub spoke topology for network traffic. The topology should include an Azure Load Balancer and Azure Application Gateway.

Objectives

Task 1:

Provision the lab environment

Task 2:

Configure the hub and spoke network topology

Task 3:

Test transitivity of virtual network peering

Task 4:

Configure routing in the hub and spoke topology

Task 5:

Implement Azure Load Balancer

Task 6:

Implement Azure Application Gateway

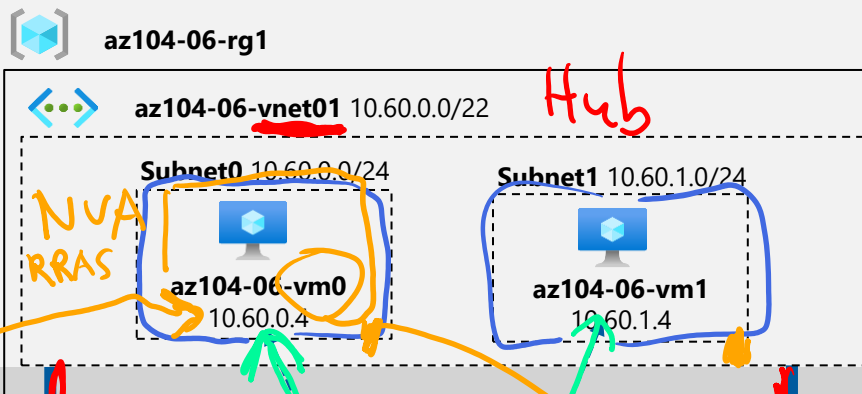
Next slide for an architecture diagram 

Lab 06 – Architecture Diagram

Network Watcher

Task1

VMs aus ARM Template



Task6

az104-06-rg5

Subnet-appgw 10.60.3.224/27

az104-06-appgw5

az104-06-pip5

App Service

Task2, Task3

Peering

Peering

Task4



az104-06-rt23

Subnet0 10.62.0.0/24



az104-06-vm2
10.62.0.4

az104-06-vnet2 10.62.0.0/22

Spoke

Task5

az104-06-lb4

az104-06-pip4

az104-06-rg4

Subnet0 10.63.0.0/24



az104-06-vm3
10.63.0.4

az104-06-vnet3 10.63.0.0/22

Spoke

Task4



az104-06-rt32

Test-Netconnection vm3 -port 3389

End of presentation

