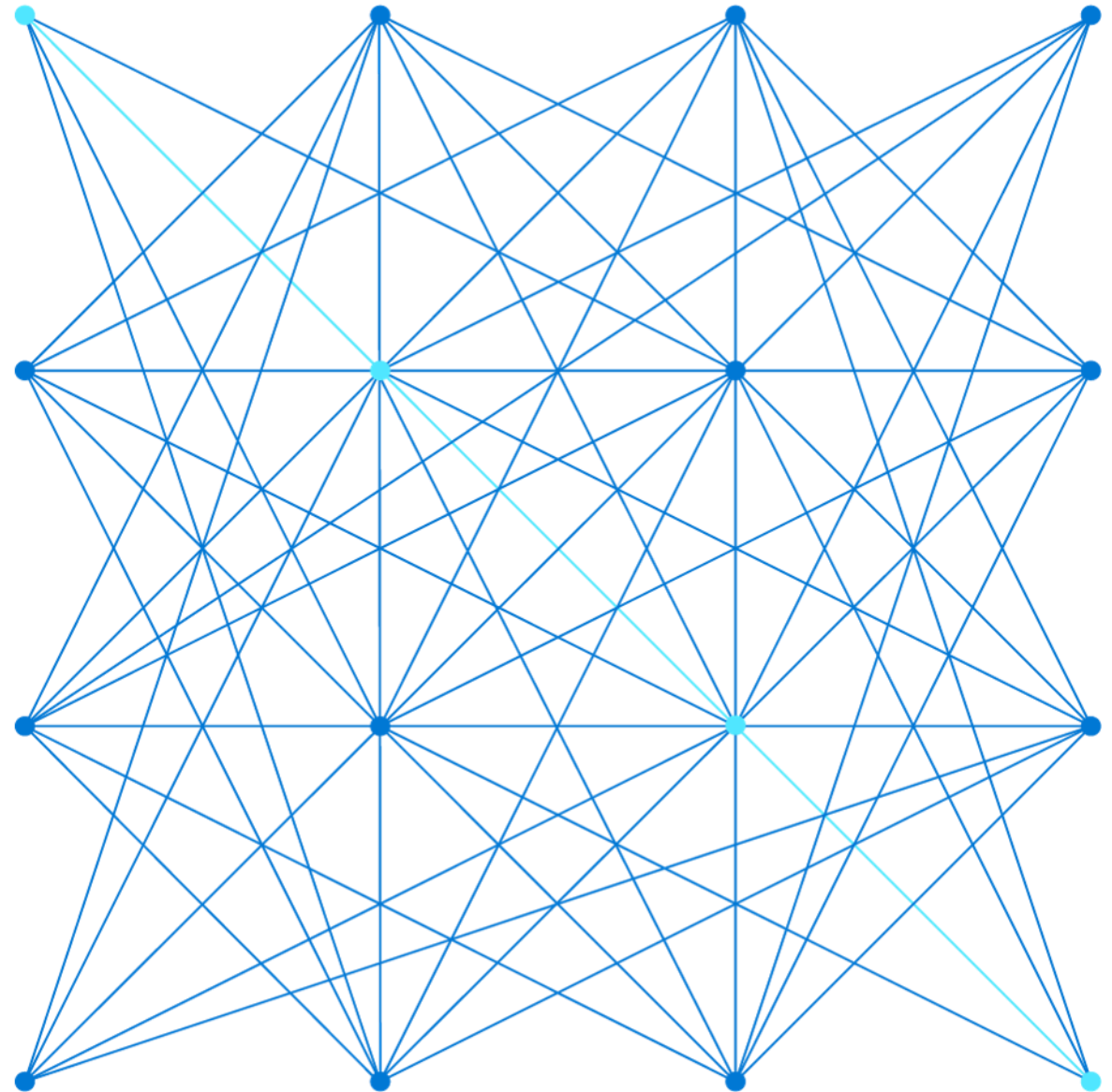


AZ-104

Tag 3

Administer Network Traffic

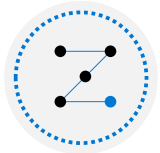
Guten Morgen!



About this course: Course Outline



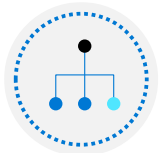
01: Administer Identity



02: Administer Governance and Compliance



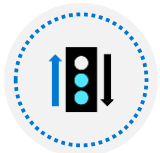
03: Administer Azure Resources



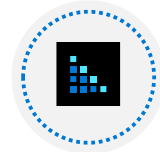
04: Administer Virtual Networking



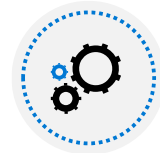
05: Administer Intersite Connectivity *Peering*



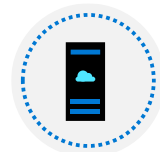
LB
VPN
06: Administer Network Traffic Management



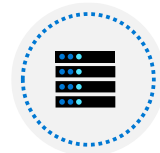
07: Administer Azure Storage



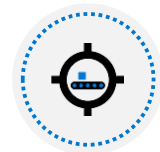
08: Administer Azure Virtual Machines



09: Administer PaaS Compute Options



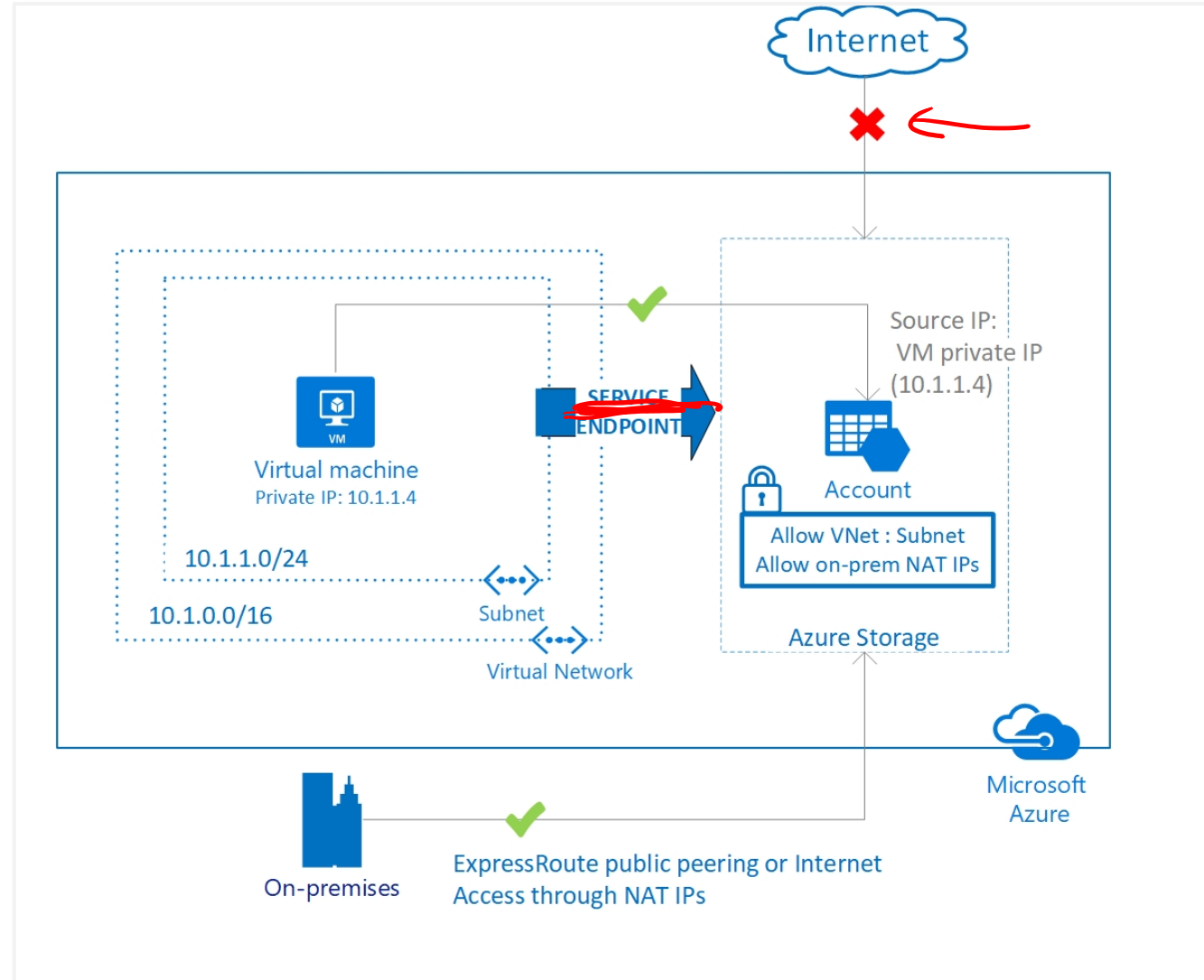
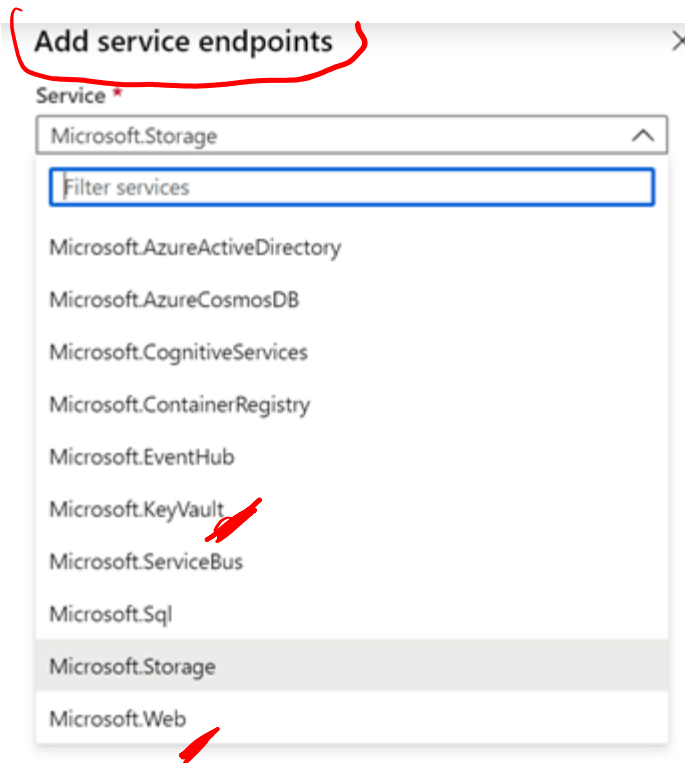
10: Administer Data Protection



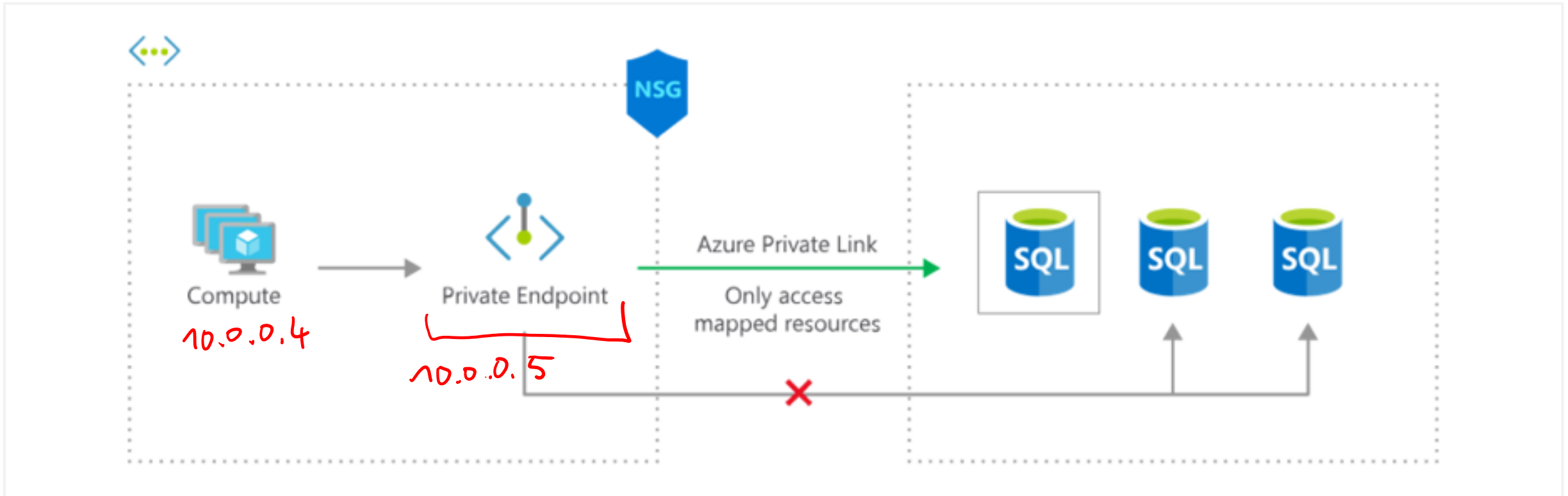
11: Administer Monitoring

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

Administer Network Traffic Introduction



[Configure Azure Load Balancer](#)



[Configure Application Gateway](#)

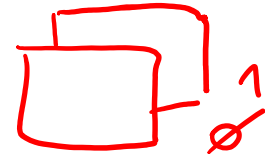


[Configure Network Watcher](#)



[Lab 06 – Implement Traffic Management](#)

UTC


VM Scale Set
VMSS

Configure Azure Load Balancer



Configure Azure Load Balancer Introduction



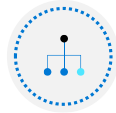
Choose a Load Balancer Solution



Implement a Public Load Balancer



Implement an Internal Load Balancer



Determine Load Balancer SKUs



Create Load Balancer Rules



Demonstration – Configure a load balancer



Summary and Resources

Choose a Load Balancer Solution

App Service

Anton Zeilinger

Entangled States

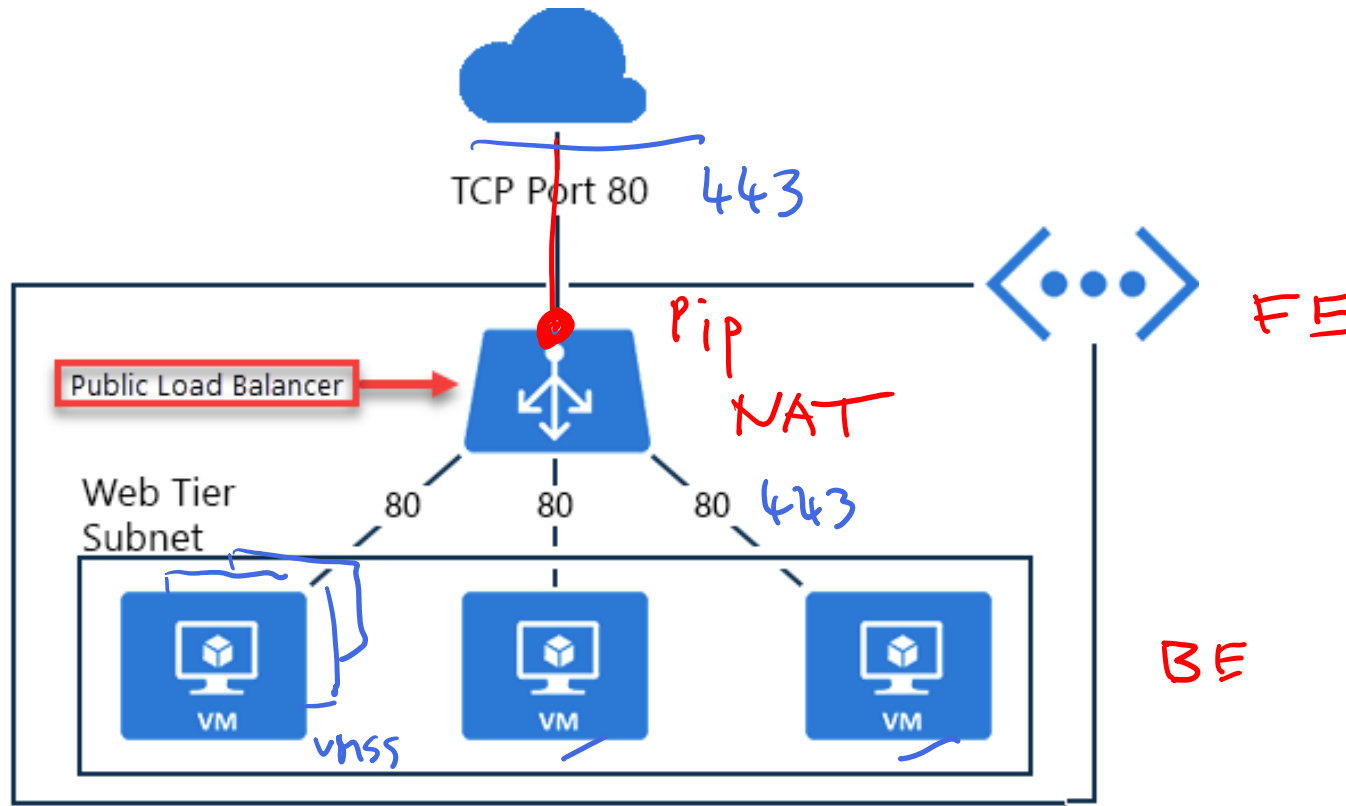
PaaS

PaaS

QC

Feature	Application Gateway	Front Door + CDN	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 (regional)	Yes		Yes	
Global	No	Yes		Yes DNS
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



SKU — Basic Free
Standard
Availability
SNAT
Mix

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

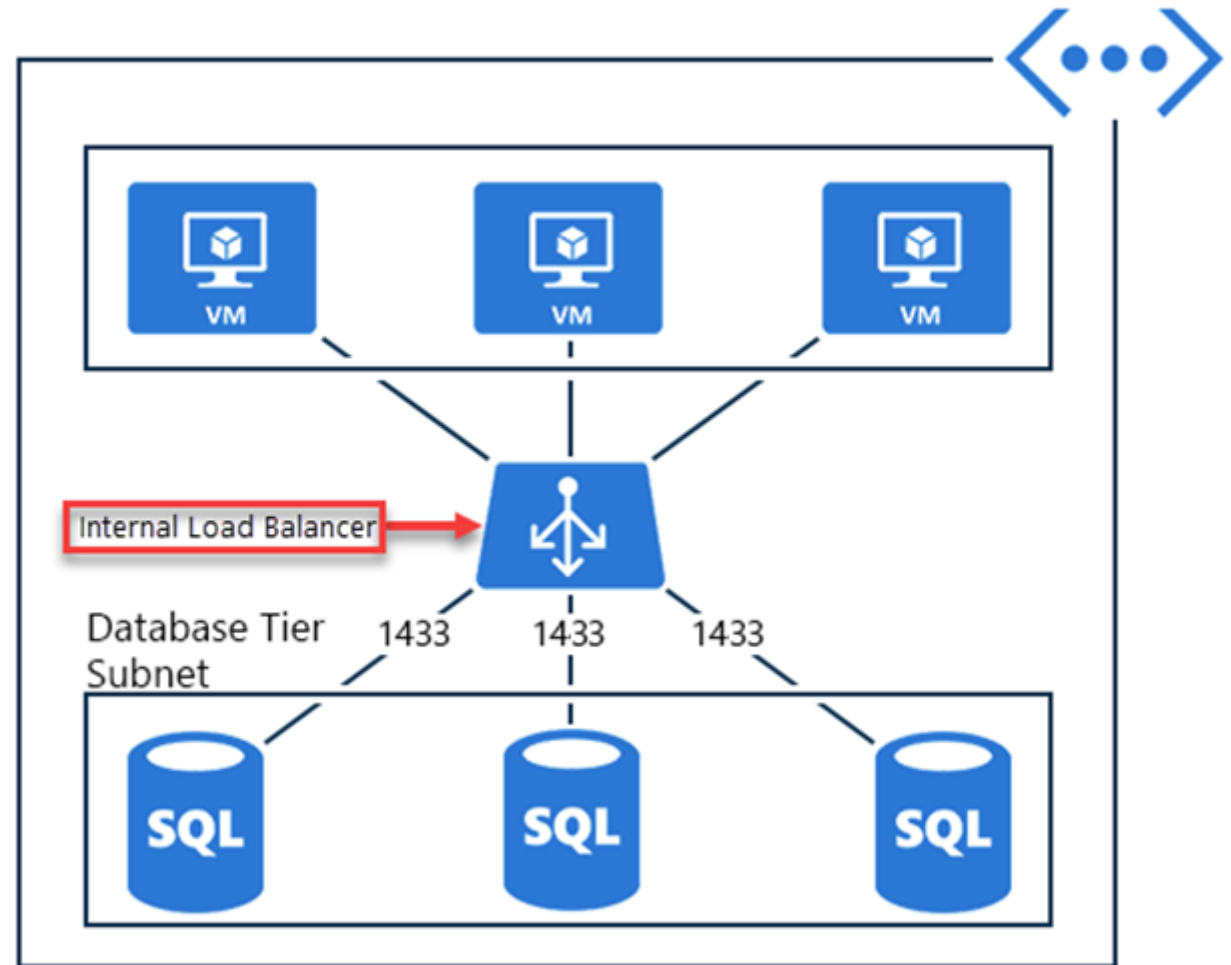
Apply load balancing rules to distribute traffic across VMs or services

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

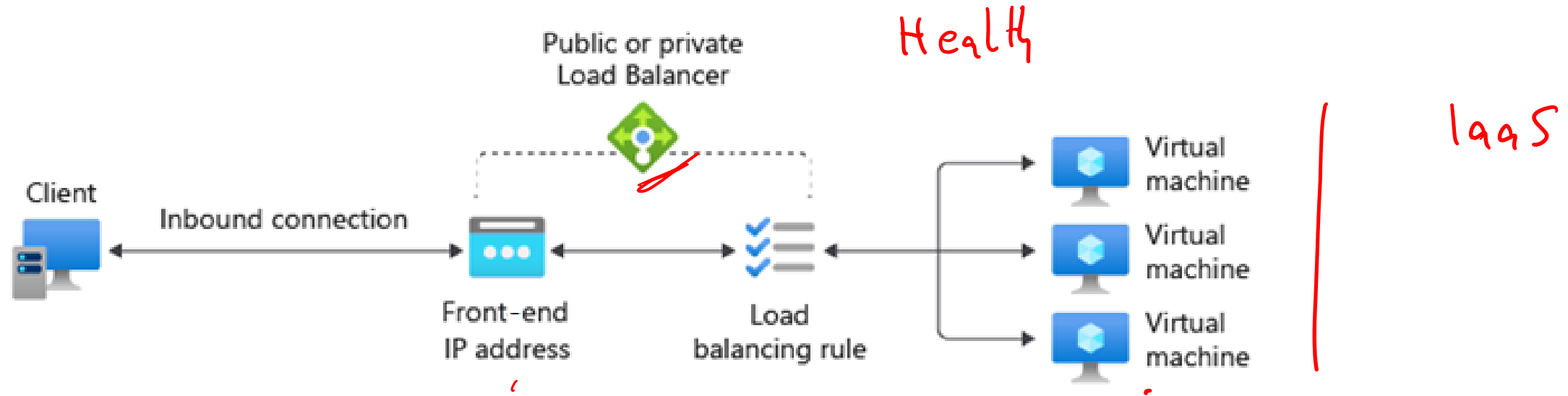
Enables load balancing within a virtual network, for cross-premises virtual networks, for multi-tier applications, and for line-of-business applications



Determine Load Balancer SKUs

Feature	Basic SKU	Standard SKU
Backend pool size	300 IP configurations, single availability set	Up to 5000 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	By default, open to the internet	Closed to inbound connections unless opened by NSGs
SLA	Not available	99.99%

Create load balancer rules

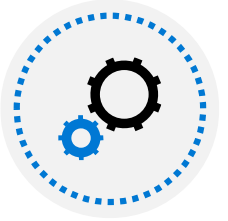


Maps a frontend IP and port combination to a set of backend pool and port combination

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

Demonstration – Configure a Load Balancer



Portal – Help me choose a load balancer



Configure a load balancer

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](#)

[Introduction to Azure Load Balancer](#)

A sandbox indicates a hands-on exercise.

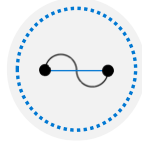
Configure Azure Application Gateway



Configure Azure Application Gateway Introduction



Implement Application Gateway



Determine Application Gateway Routing



Demonstration – Configure an Application Gateway

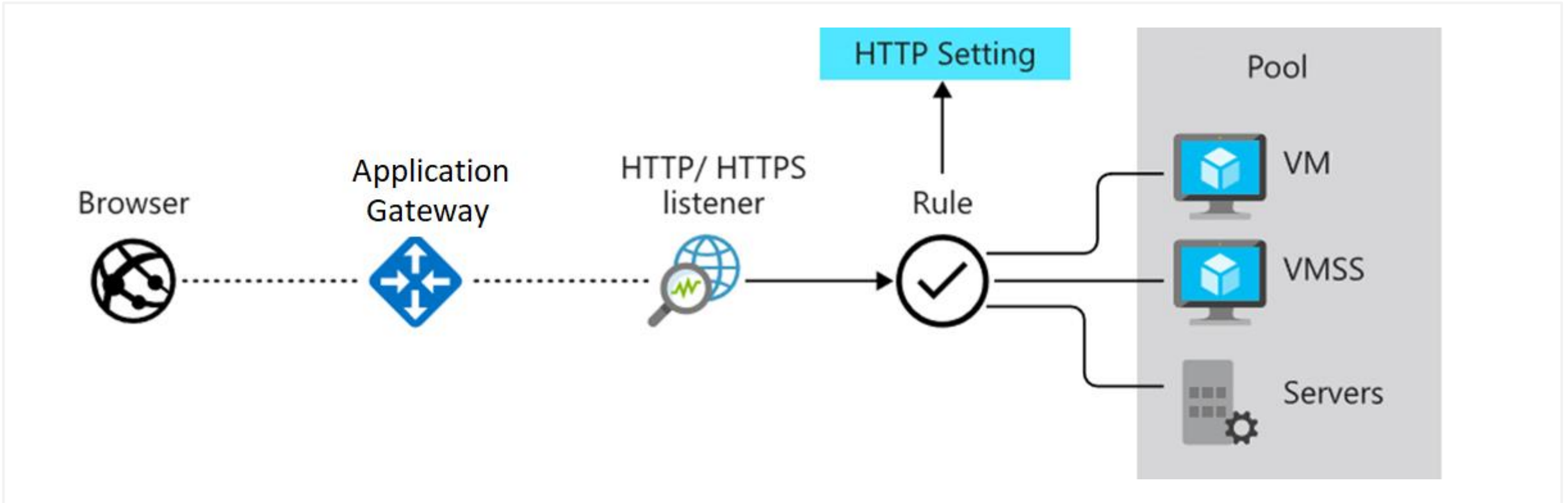


Setup Application Gateway Components



Summary and Resources

Implement Application Gateway



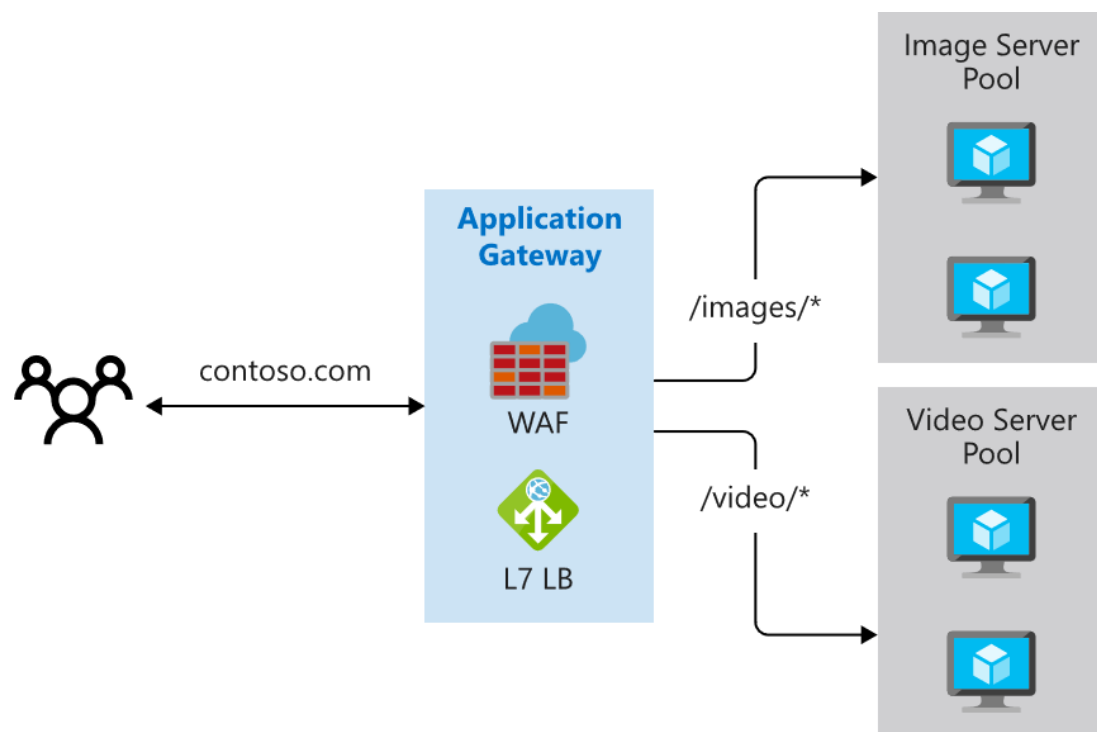
Manages web app requests

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

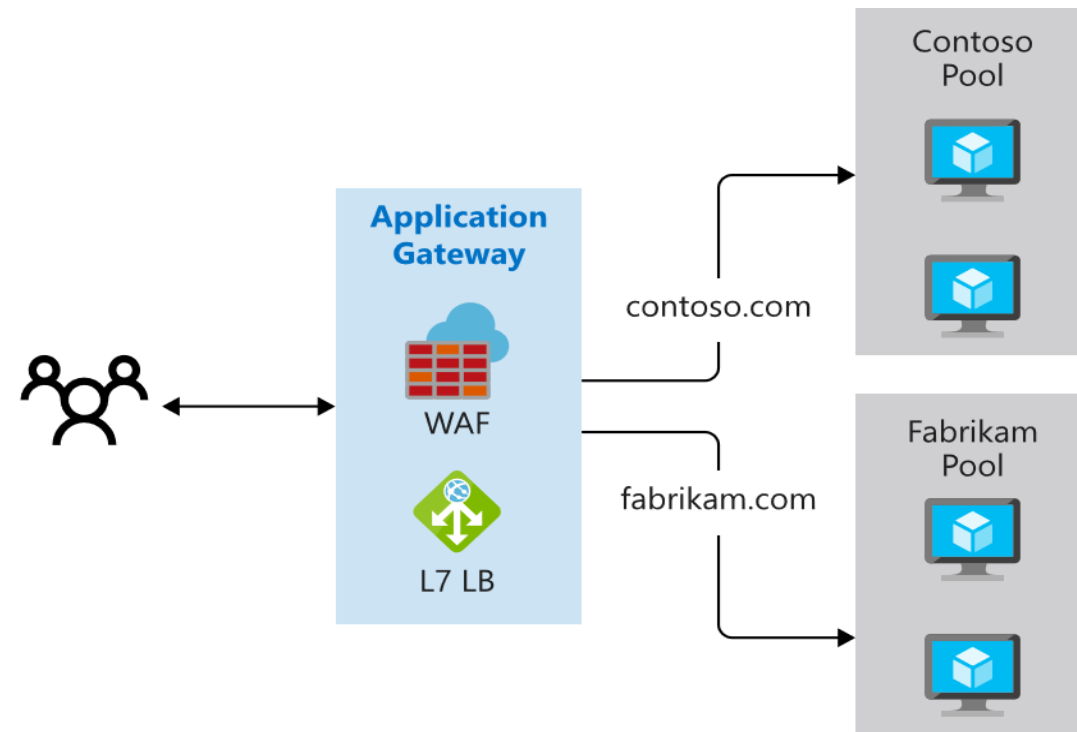
The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

Determine Application Gateway Routing

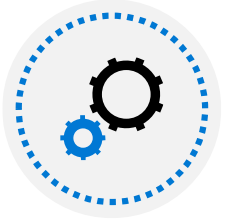
Path-based routing



Multiple-site routing



Demonstration – Configure an Azure Application Gateway



Configure the Azure Application Gateway



Compare to the Load Balancer

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

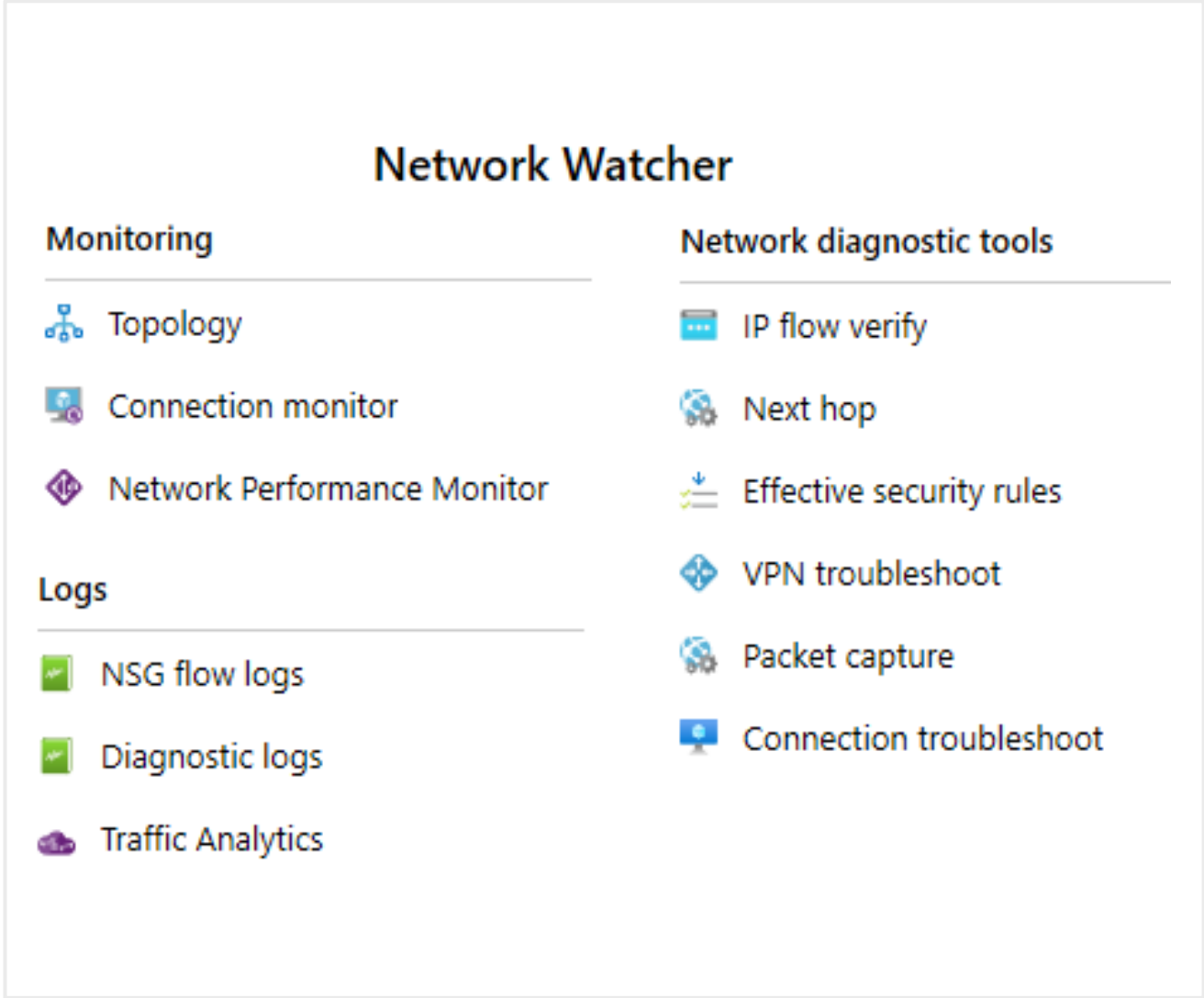
Next Hop determines if traffic is being correctly routed

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 *	Local port *
<input type="text" value="10.1.1.4"/>	<input type="text" value="3389"/>
Remote IP address *	Remote port *
<input type="text" value="13.24.35.46"/>	<input type="text" value="3389"/>

 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

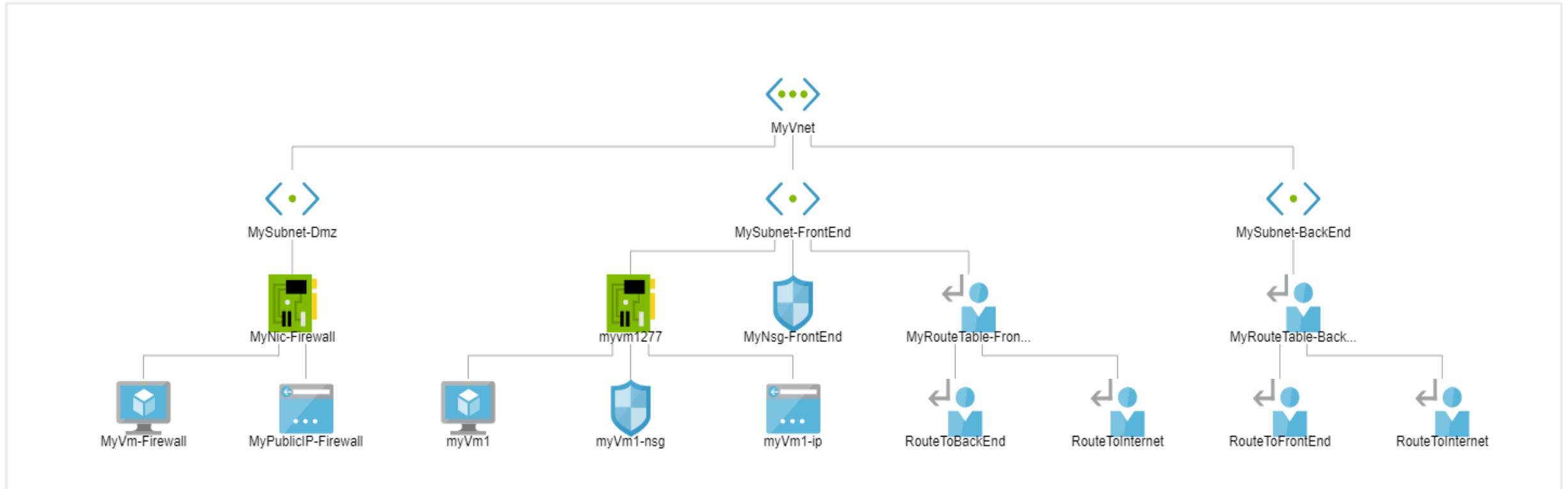
IP address

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 \(Sandbox\)](#)

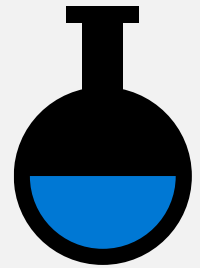
[Monitor the performance of virtual machines using Azure Monitor VM Insights \(Sandbox\)](#)

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

A sandbox indicates a hands-on exercise.

06

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:

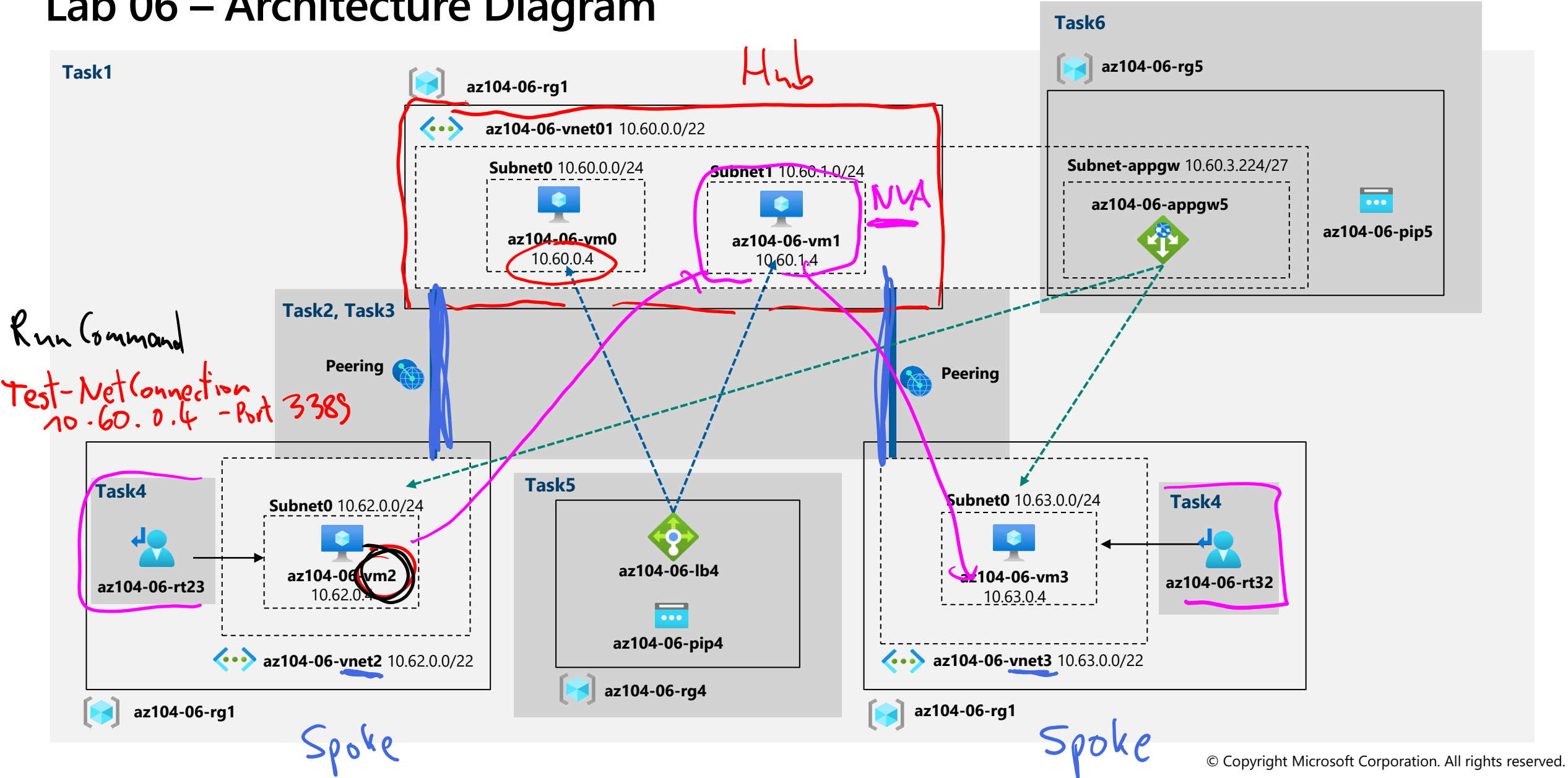
Implement Azure Load Balancer

Task 6:

Implement Azure Application Gateway

Next slide for an architecture diagram 

Lab 06 – Architecture Diagram



End of presentation

