Microsoft

AZ-104

Administer
Network Traffic

AZ-104 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

Learning Objectives - Administer Network Traffic

- [Configure Azure Load Balancer](#)

- [Configure Application Gateway](#)

- [Configure Network Watcher](#)

- [Lab 06 – Implement Traffic Management](#)

Configure Azure Load Balancer

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 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		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

- 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

TCP Port 80

Public Load Balancer

Web Tier Subnet

80   80   80

VM   VM   VM
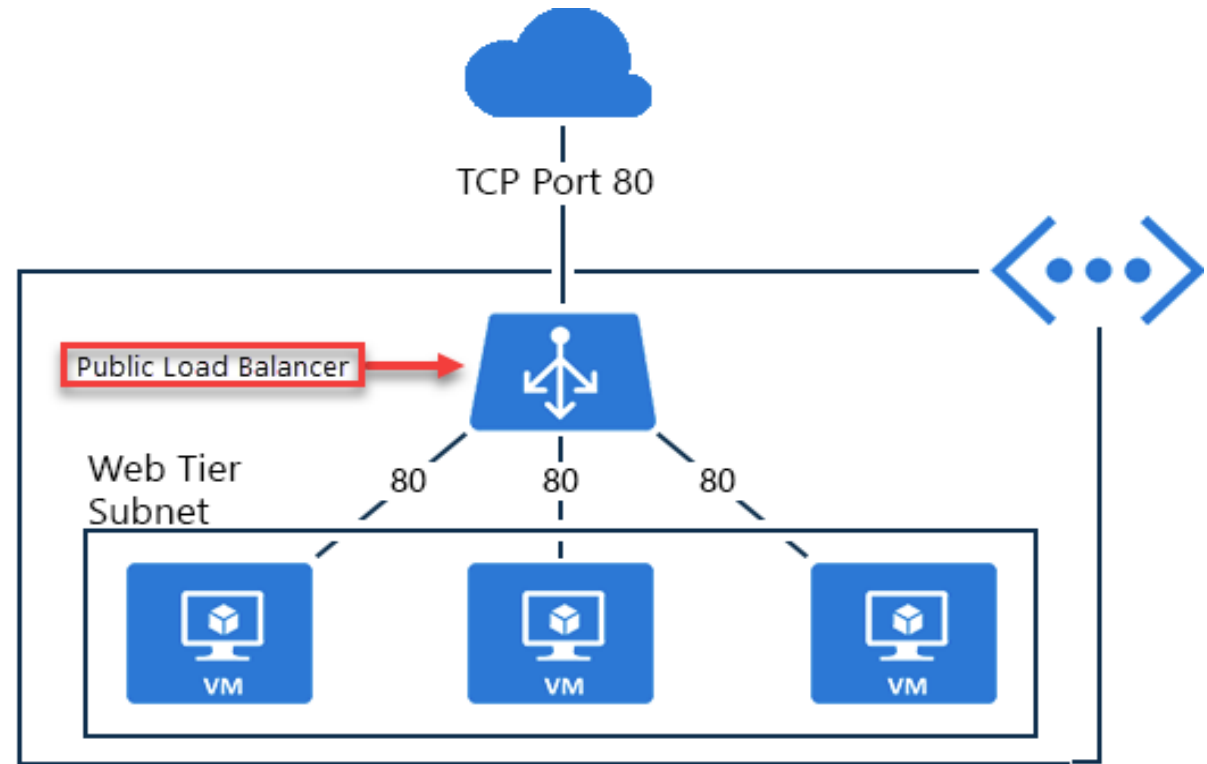
Implement an Internal Load Balancer

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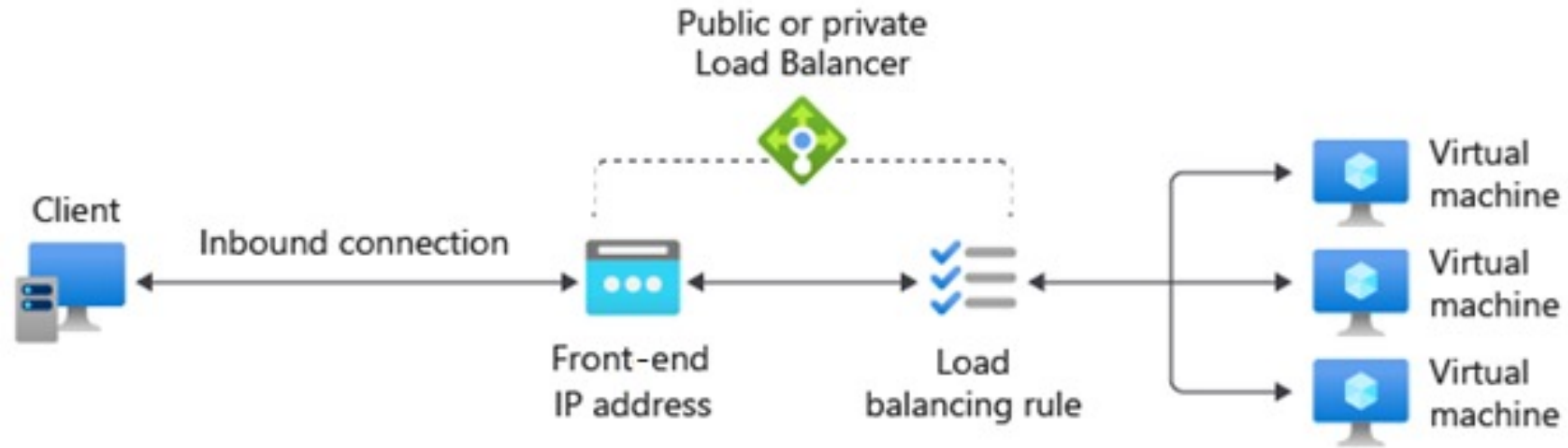
Enables load balancing within a virtual network, for cross-premises virtual networks, for multi-tier applications, and for line-of-business applications

Internal Load Balancer

Database Tier Subnet   1433   1433   1433
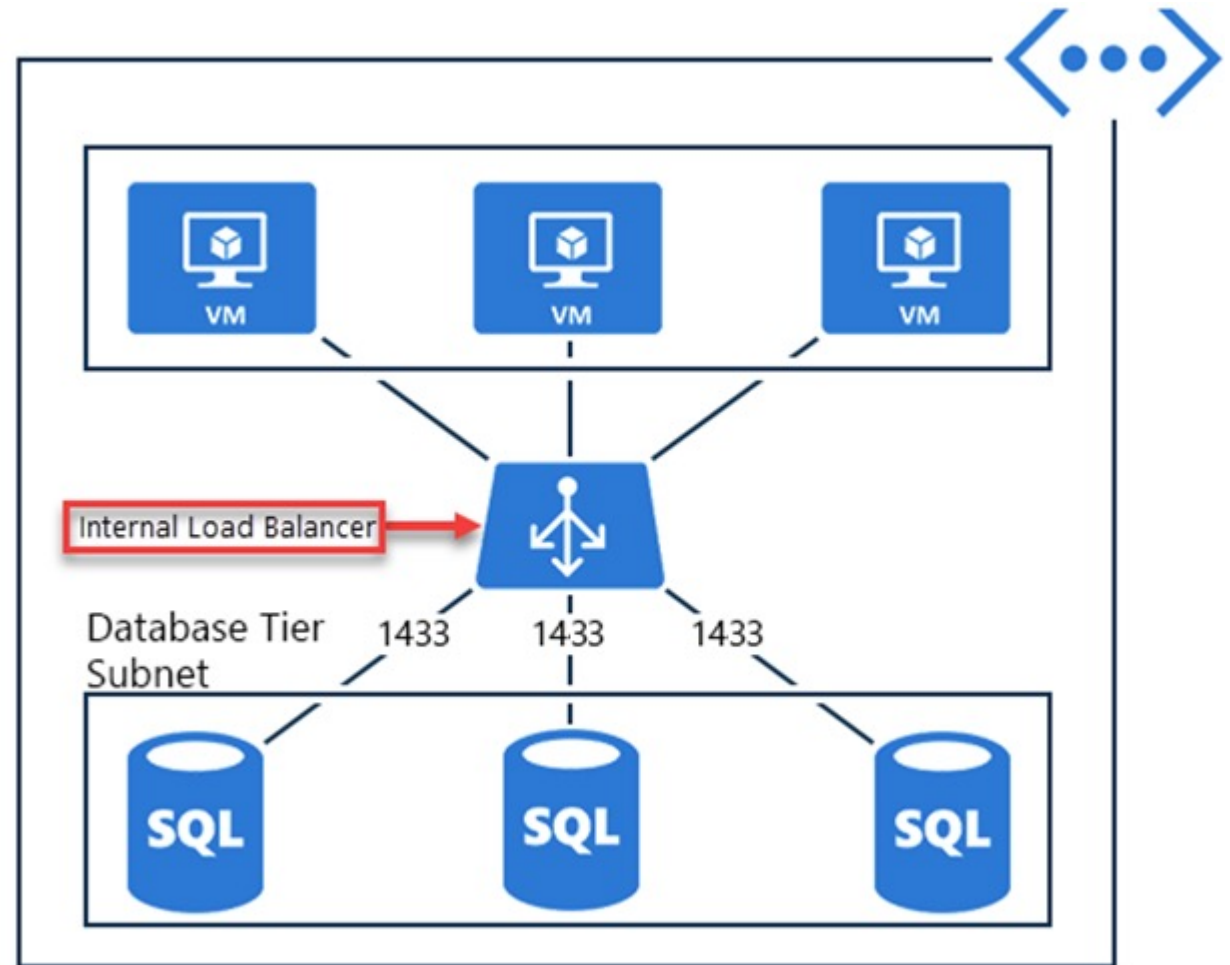
Determine Load Balancer SKUs

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

Public or private
Load Balancer

Client

Inbound connection

Front-end
IP address

Load
balancing rule

Virtual
machine

Virtual
machine

Virtual
machine

Maps a frontend IP and port combination to a set of backend pool and port combination
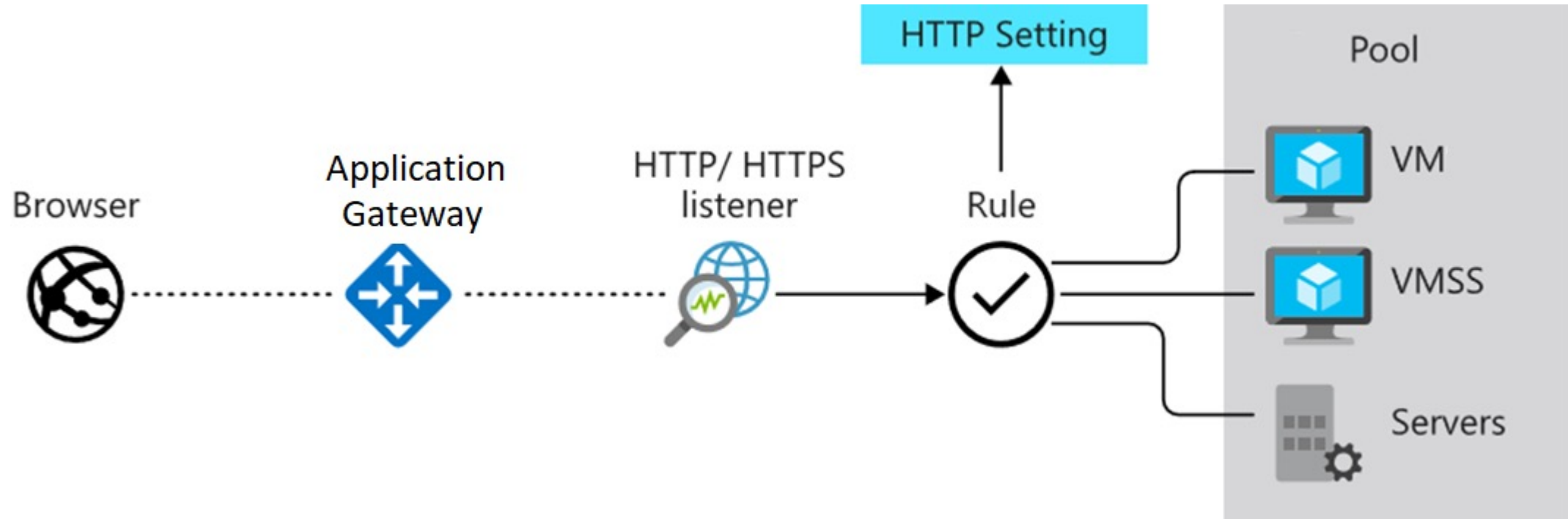
Rules can be combined with NAT rules

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

Configure Azure Application Gateway

Implement Application Gateway
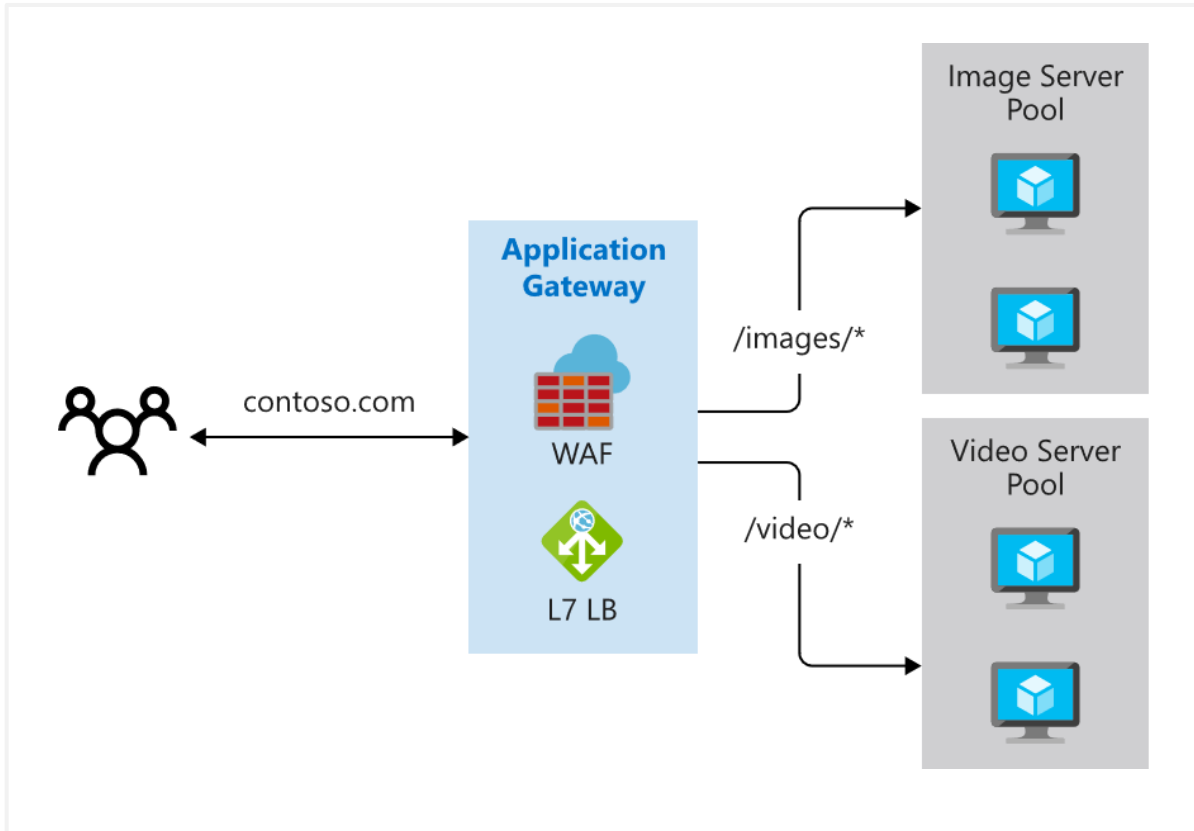

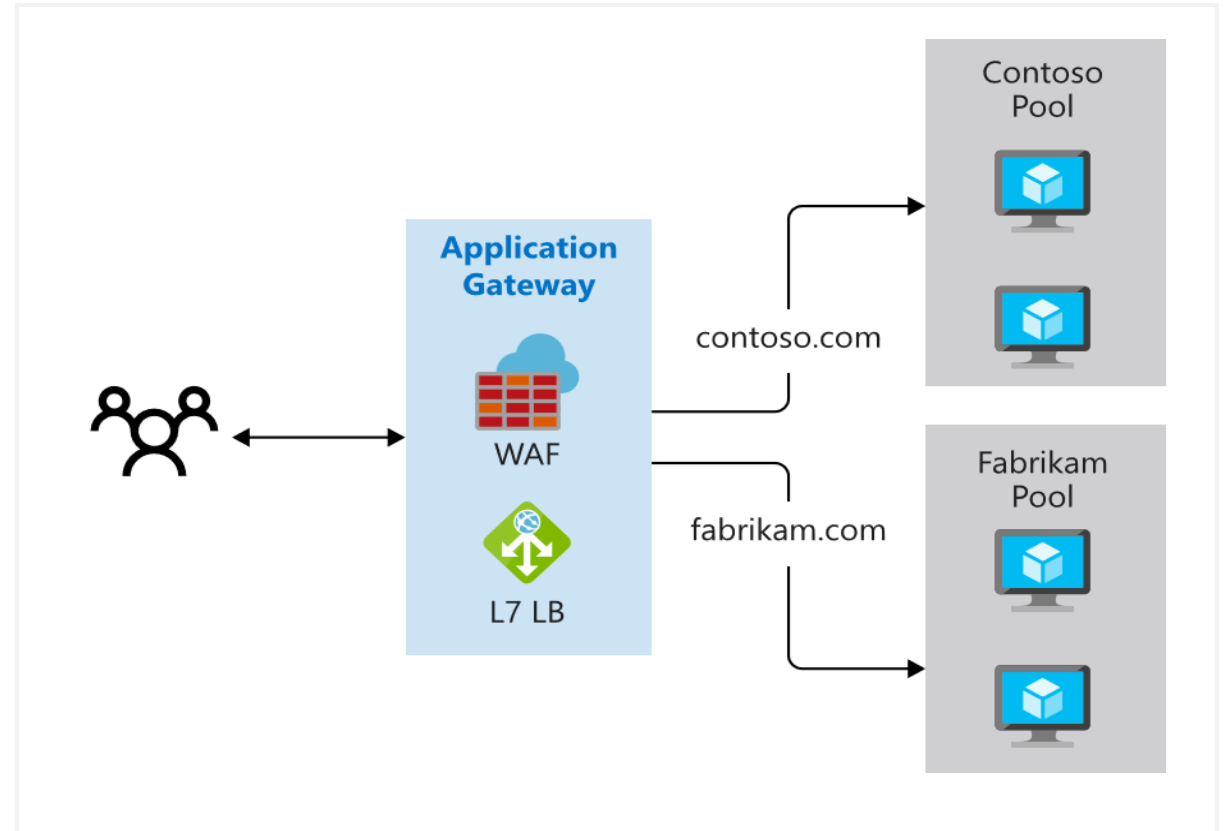|		
Manages web app requests	Routes traffic to a pool of web servers based on the URL of a request	The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

Determine Application Gateway Routing
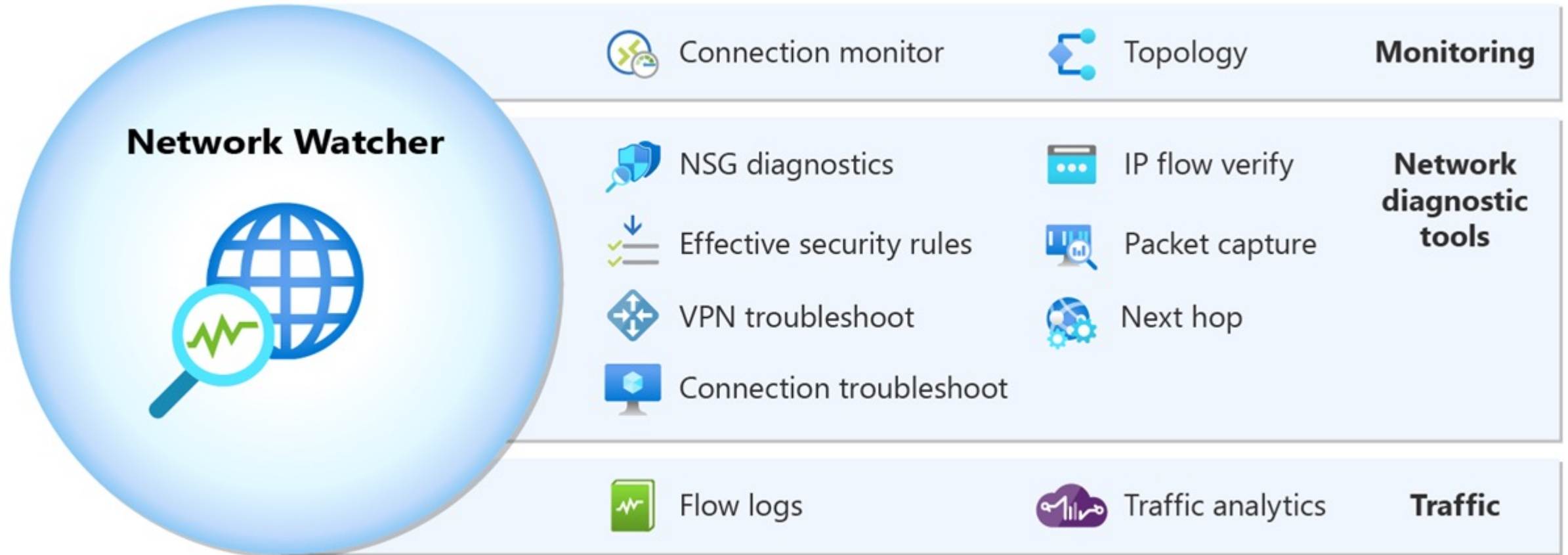
Path-based routing	Multiple-site routing

Configure Network Watcher

Describe Network Watcher Features

A regional service with various network diagnostics

Network Watcher

Connection monitor	Topology	**Monitoring**
NSG diagnostics	IP flow verify	**Network diagnostic tools**
Effective security rules	Packet capture	
VPN troubleshoot	Next hop	
Connection troubleshoot		
Flow logs	Traffic analytics	**Traffic**

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
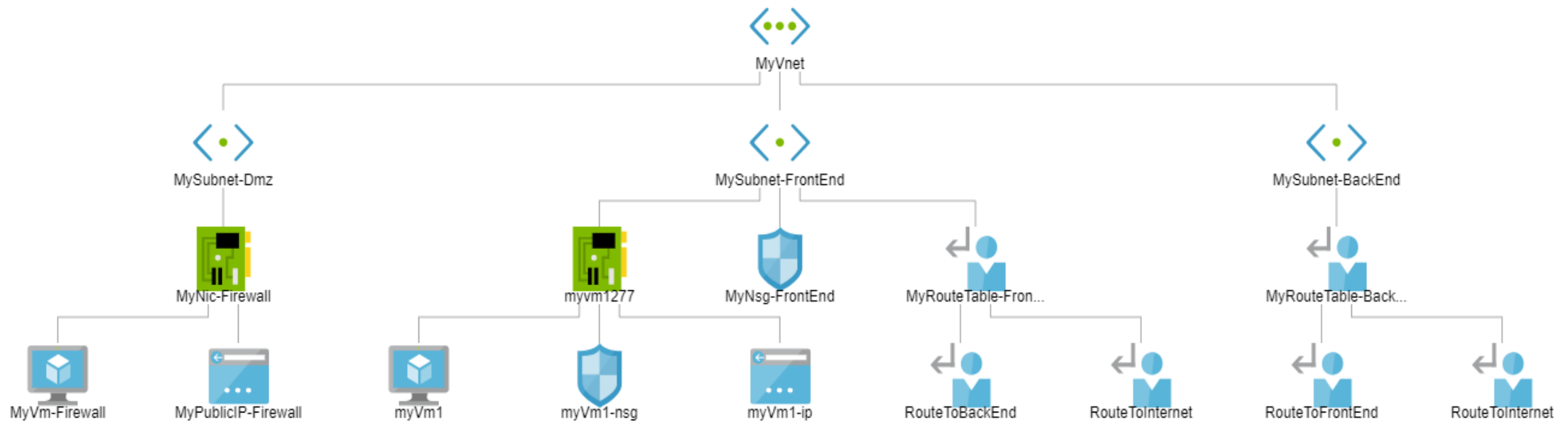
Next hop

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

Lab – Implement Traffic Management

Lab 06 – Implement traffic management

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
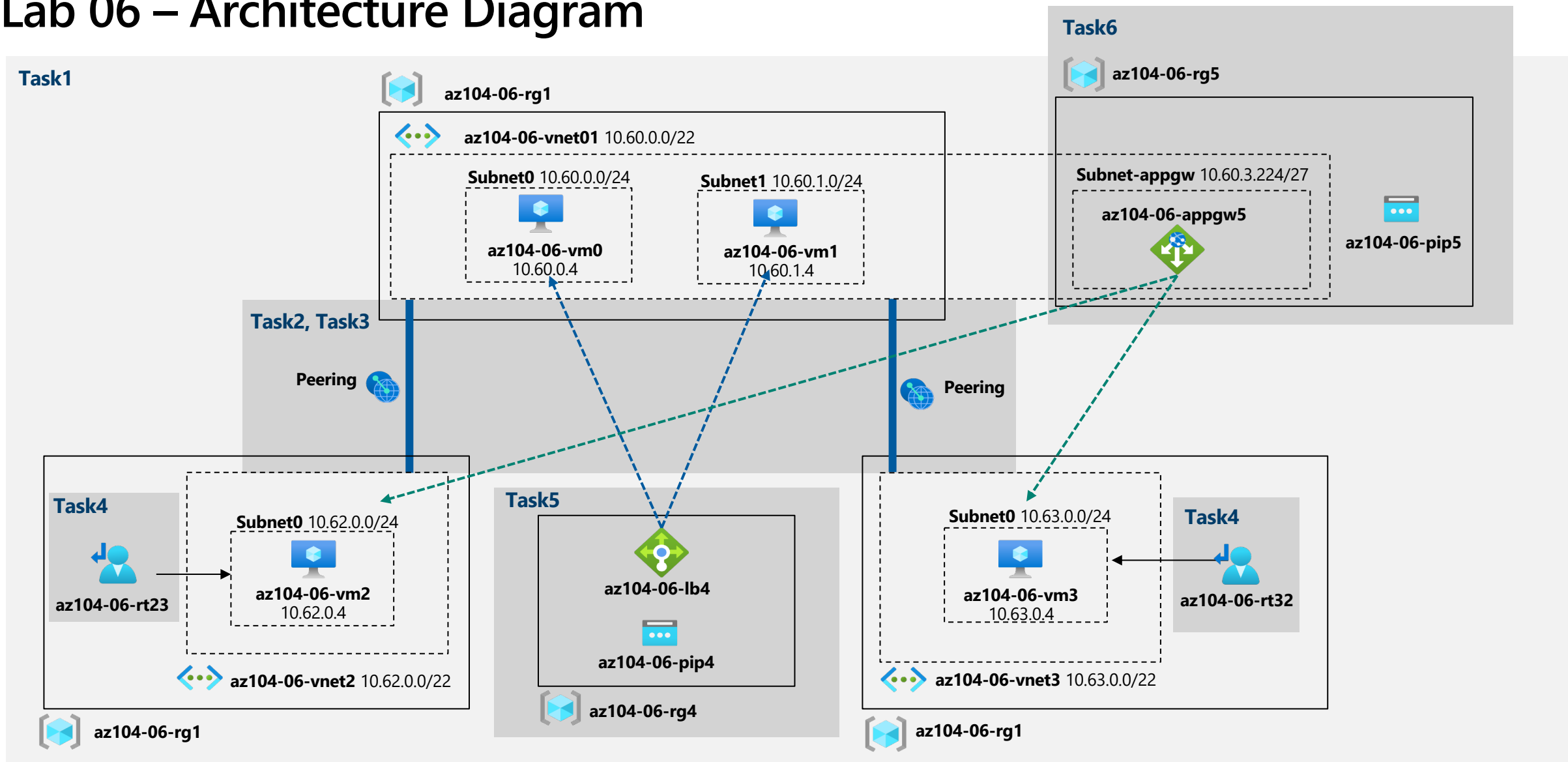
Task 4: Configure routing in the hub and spoke topology

Task 5: Implement Azure Load Balancer

Task 6: Implement Azure Application Gateway

Next slide for an architecture diagram →

Lab 06 – Architecture Diagram

Task1

az104-06-rg1

az104-06-vnet01 10.60.0.0/22

Subnet0 10.60.0.0/24

az104-06-vm0
10.60.0.4

Subnet1 10.60.1.0/24

az104-06-vm1
10.60.1.4

Task2, Task3

Peering

Peering

Task6

az104-06-rg5

Subnet-appgw 10.60.3.224/27

az104-06-appgw5

az104-06-pip5

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

az104-06-rg1

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

az104-06-rg1

Task4

az104-06-rt32

End of presentation