Microsoft

AZ-700

Load balancing non-HTTP(S) traffic

AZ-700 Agenda

Module 01: Introduction to Azure Virtual Networks

Module 02: Designing and Implementing Hybrid Networking

Module 03: Designing and Implementing Azure ExpressRoute

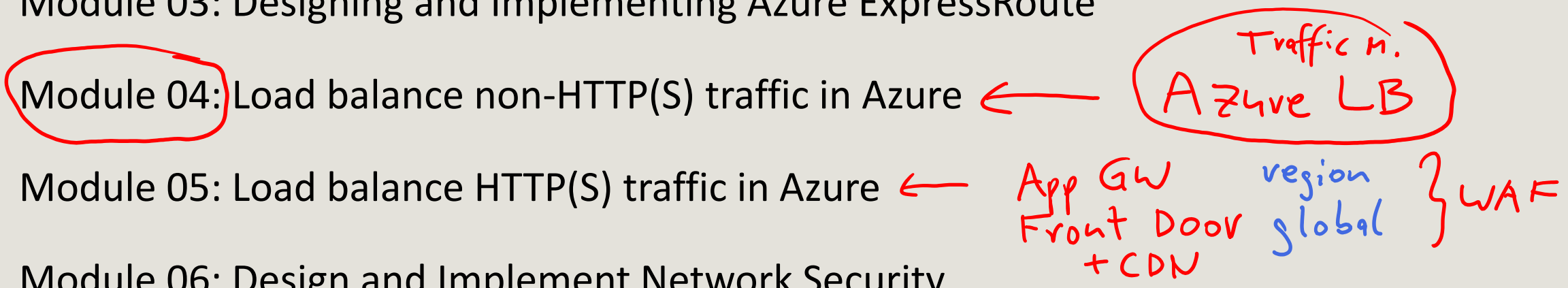
Module 04: Load balance non-HTTP(S) traffic in Azure

Module 05: Load balance HTTP(S) traffic in Azure

Module 06: Design and Implement Network Security

Module 07: Design and Implement private access to Azure Services

Module 08: Design and Implement Network Monitoring



Module Overview

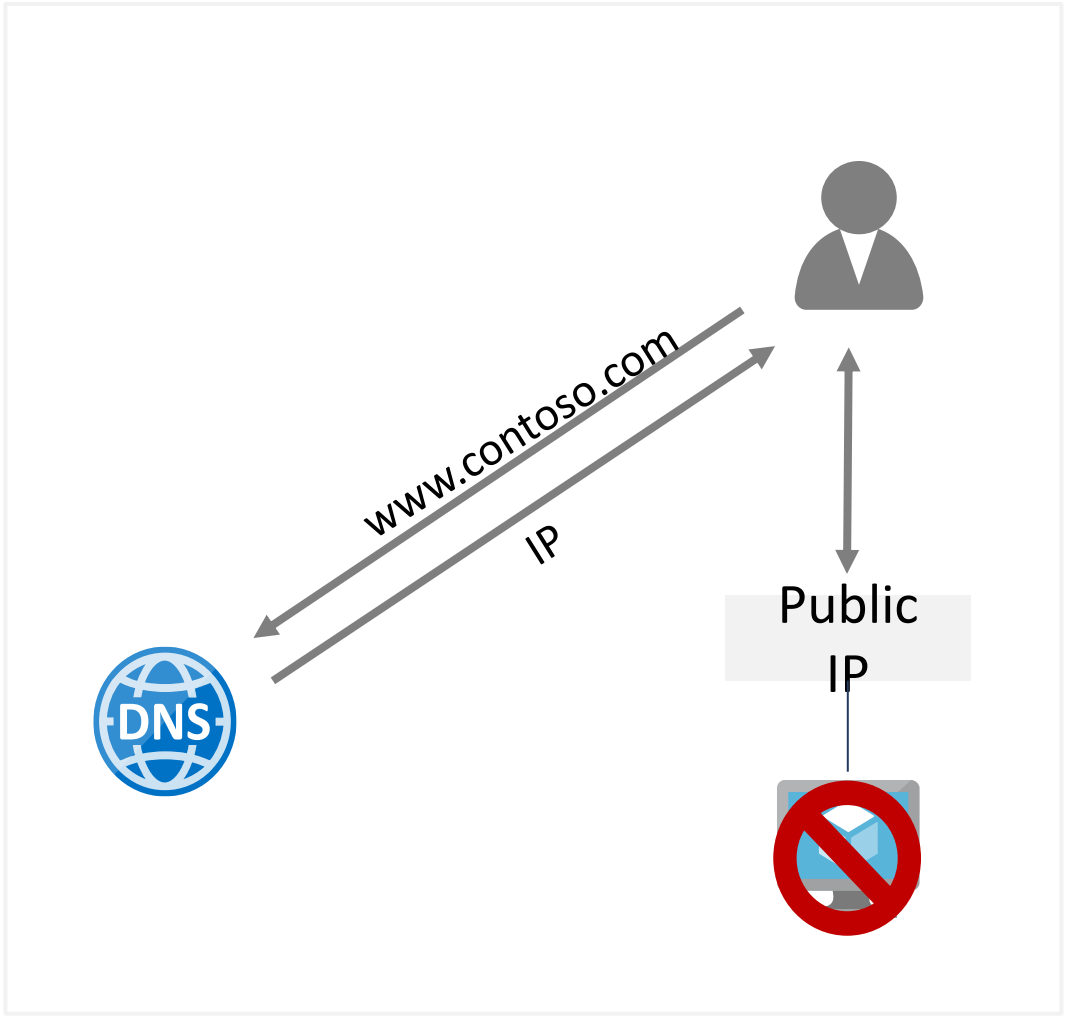
- Explore load balancing options in the Azure portal
- Design and implement Azure Load Balancer using the Azure portal
- Exercise – Create and configure an internal load balancer using the Azure portal
- Explore Azure Traffic Manager
- Exercise: Create a traffic manager profile using the Azure portal

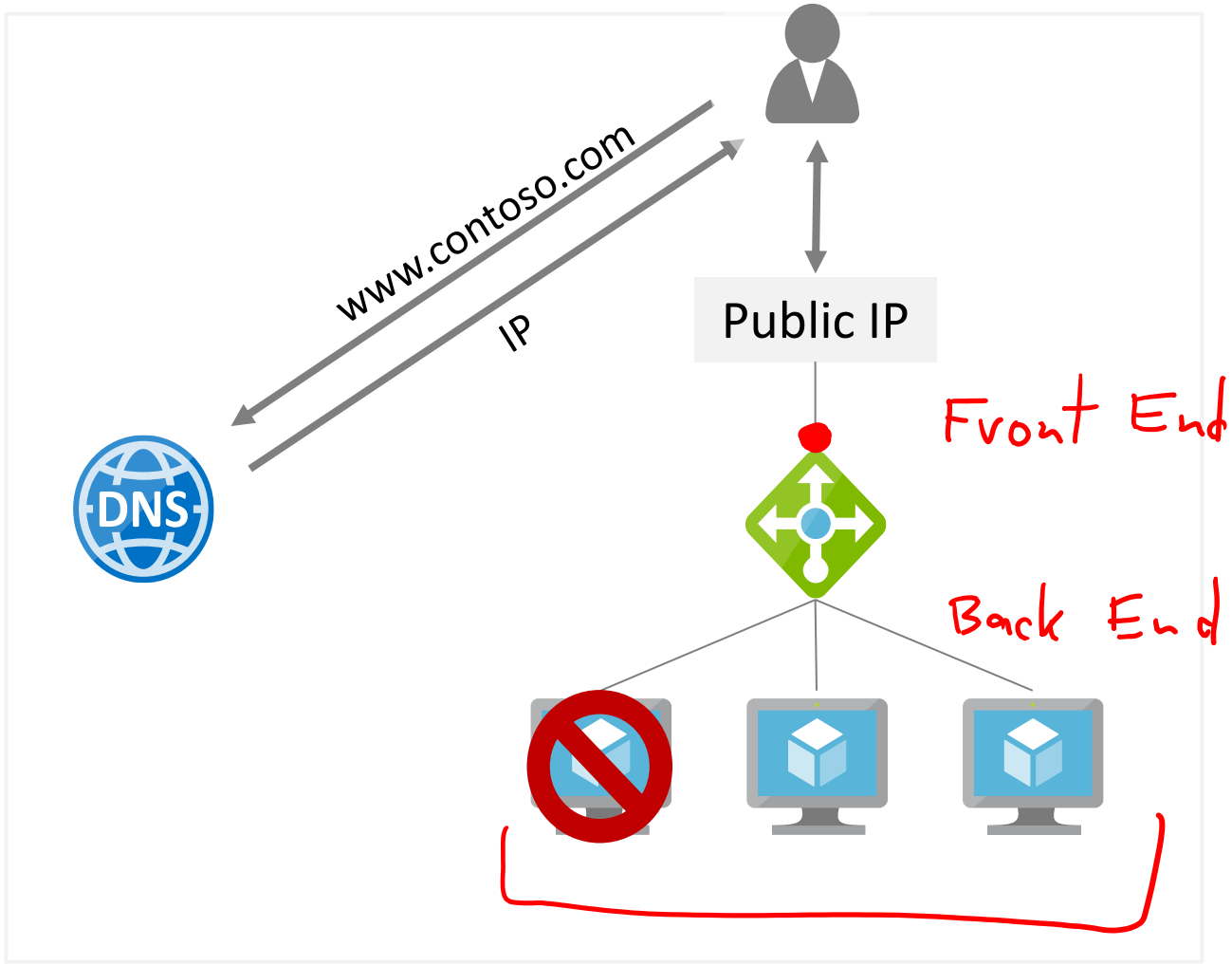
Explore load balancing options in the Azure portal

Learning Objectives – Load Balancing Options in the Azure Portal

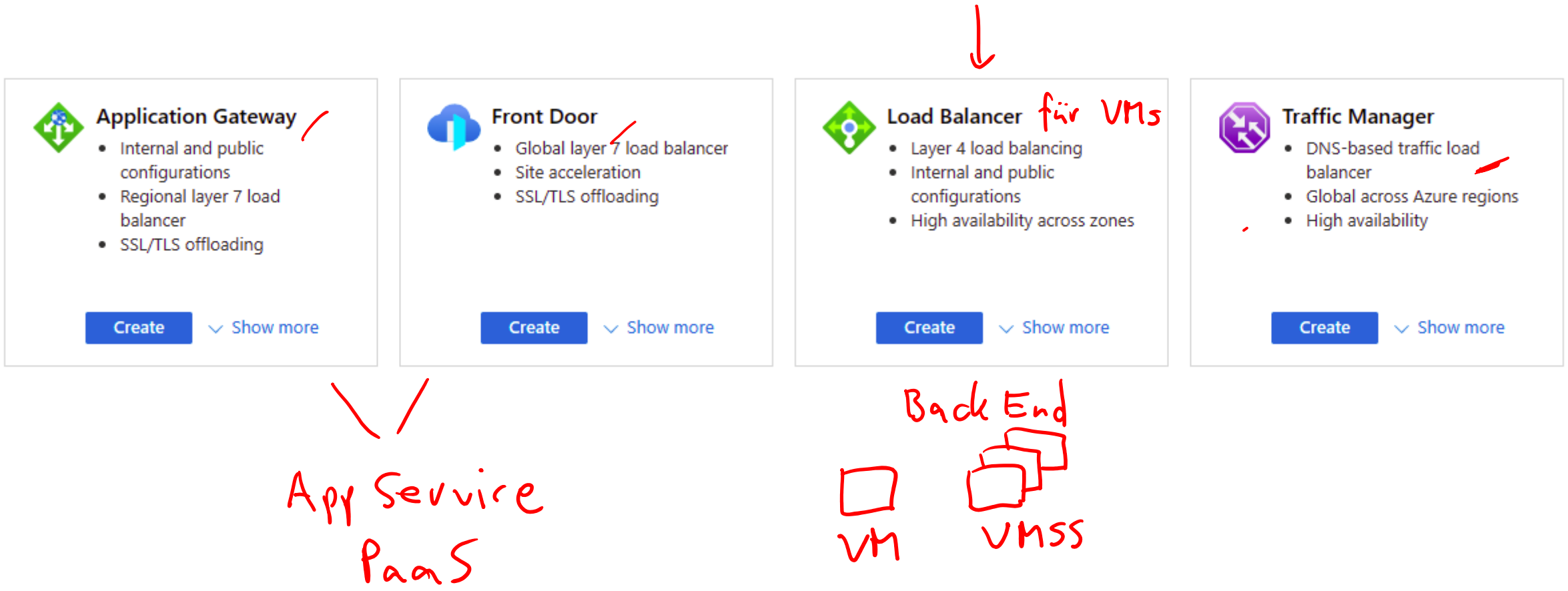
- What is a Load balancer
- Load balancing options for Azure
- Choosing a load balancing option
- Demonstration
- Learning Recap

What is a Load balancer



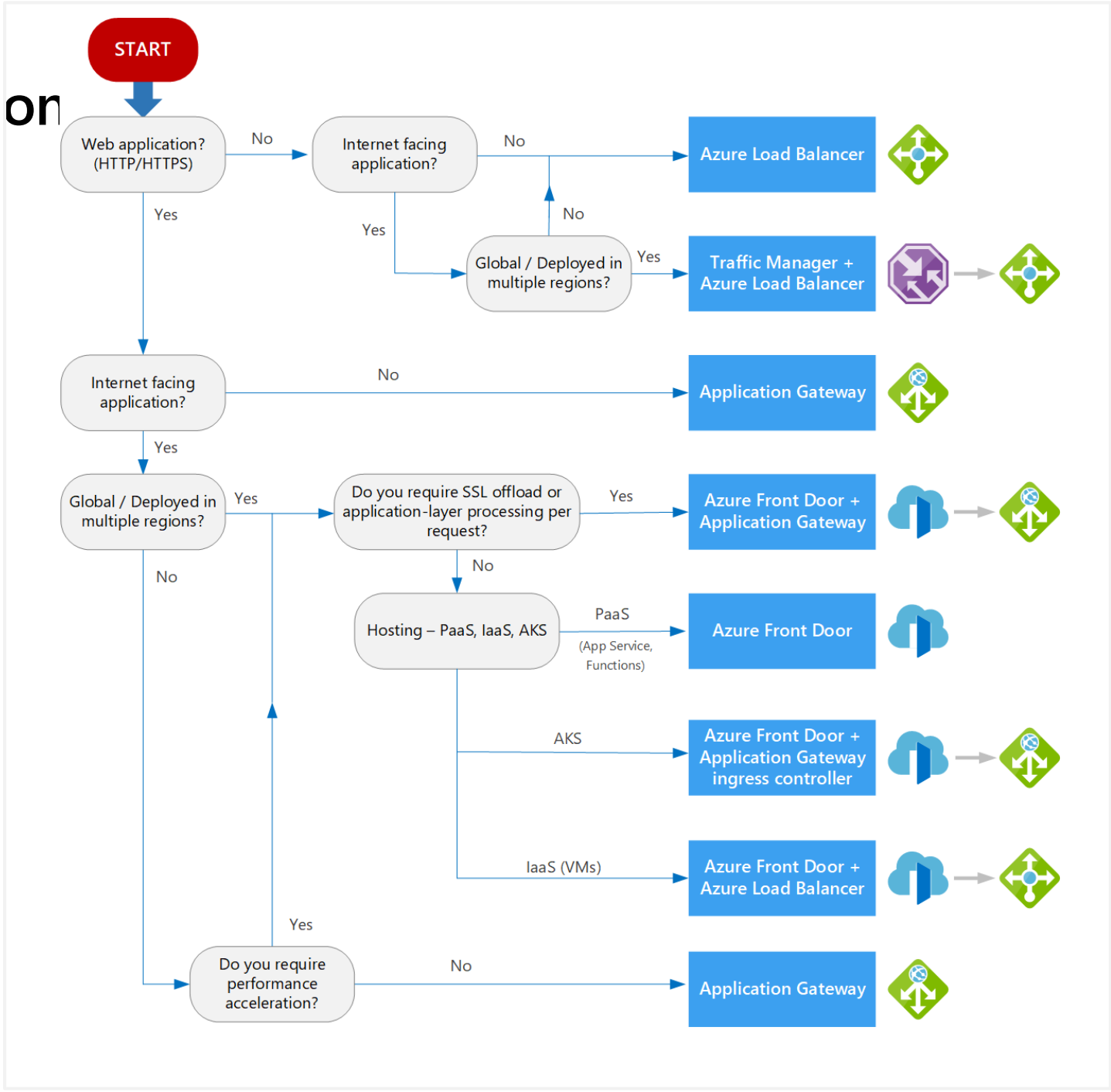


Load balancing options for Azure



Choosing a load balancing option

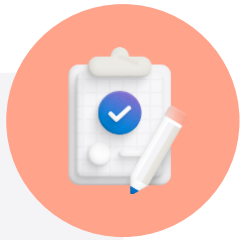
- Type of traffic
- Scope
- Availability
- Cost
- Features and limitations



Demonstration

- Create the virtual network
- Create load balancer
- Create backend servers and test virtual machine with IIS installed
- Test the load balancer

Learning Recap – Explore Load Balancing Options in the Azure Portal



Check your knowledge questions and additional study

- 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 an additional hands-on exercise.

Design and implement Azure Load balancer

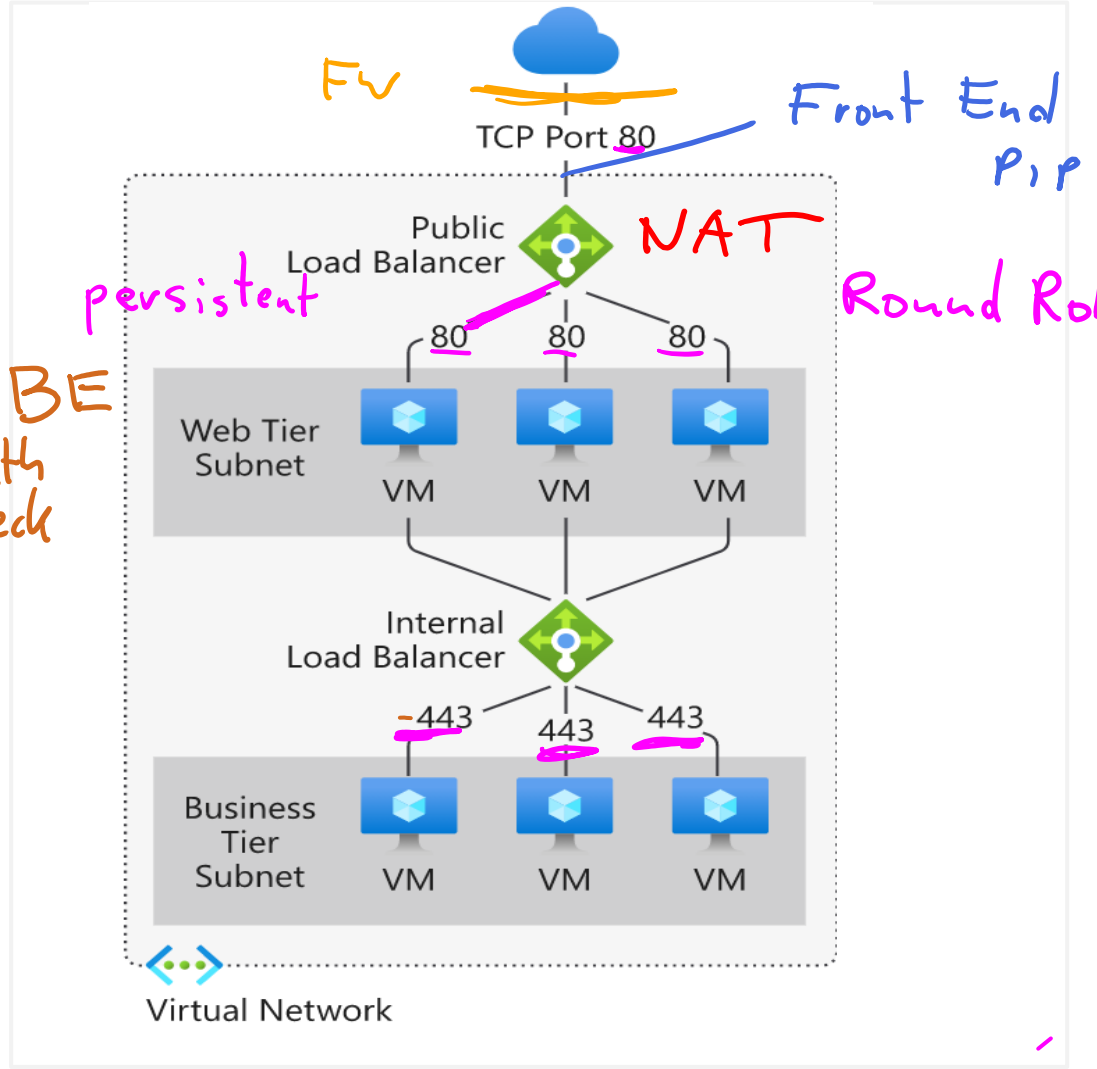
Learning Objectives – Azure Load Balancer

- Determine Load Balancer type
- Gateway Load Balancer
- Azure Load balancer and availability zones
- Determine Load Balancer SKUs
- Create Load balancer in the Azure portal
- Create Backend Pools
- Create Load Balancer Rules
- Configure Session Persistence
- Create Health Probes
- Configure outbound traffic with Standard load balancer
- Demonstration
- Learning Recap

Choosing a Load Balancer Type

A **public load balancer** is used to load balance internet traffic to VMs

An **internal load balancer** is used where private IPs are needed at the frontend only

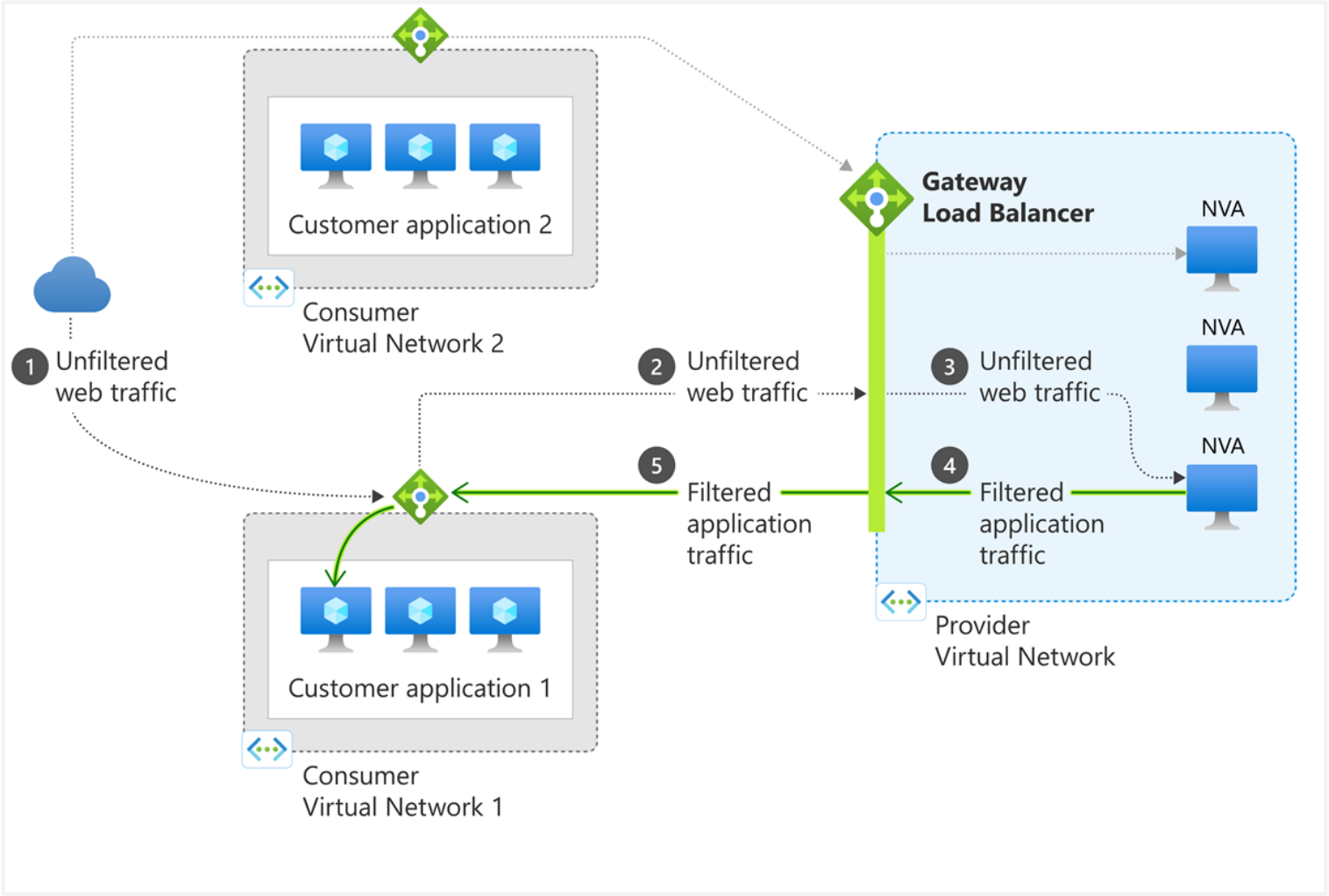


Gateway Load Balancer

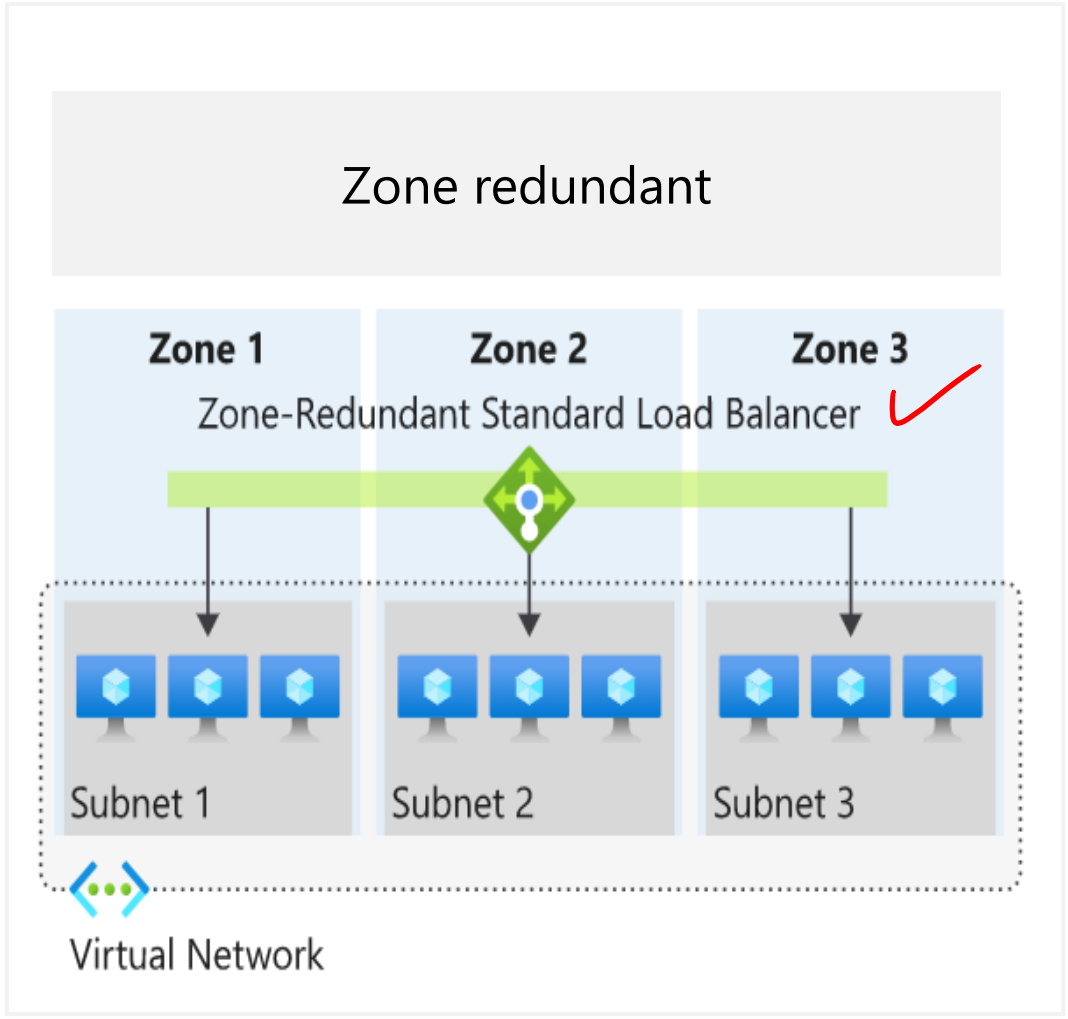
Gateway Load Balancer is a SKU of the Azure Load Balancer portfolio catered for high performance and high availability scenarios with third-party Network Virtual Appliances (NVAs)

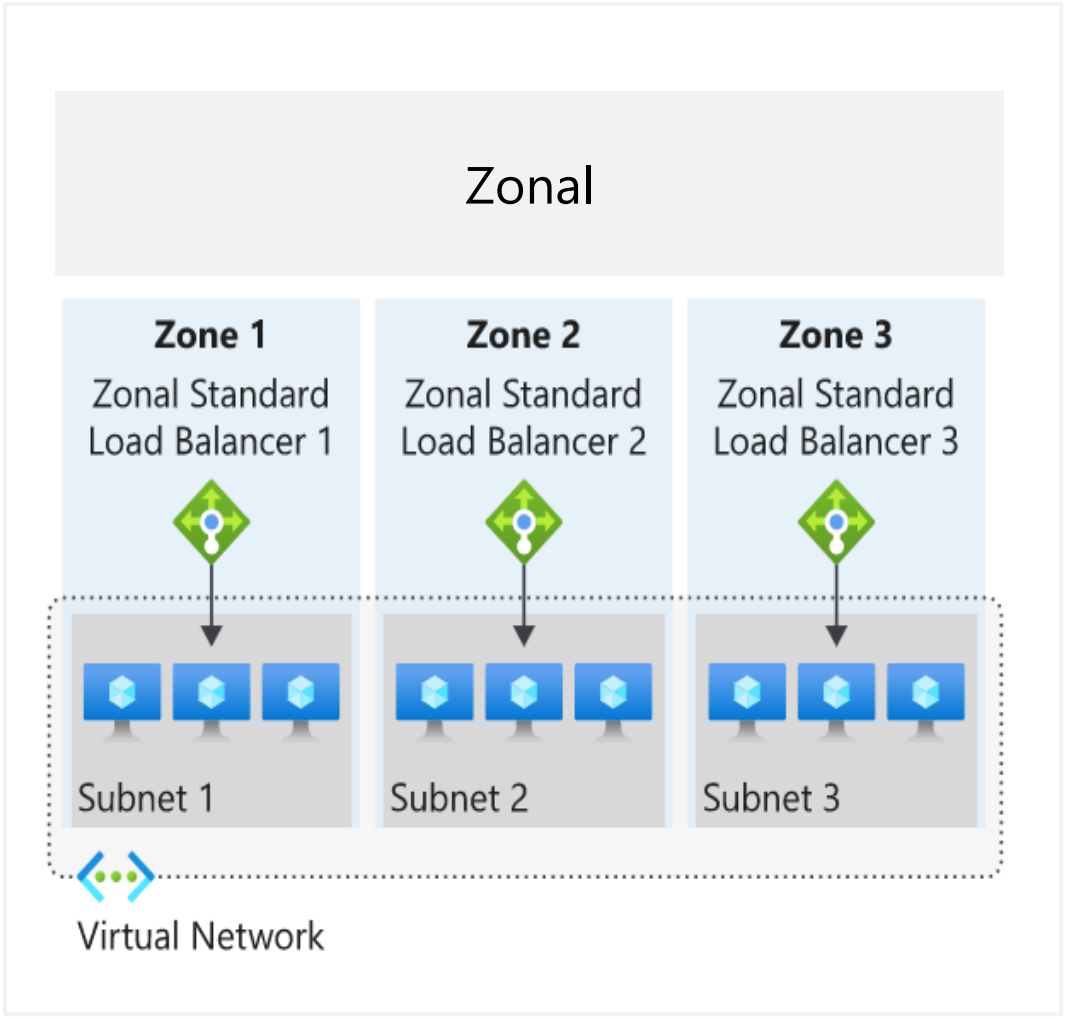
Components to configure:

- Frontend IP
- Load-balancing rules
- Backend pool(s)
- Tunnel interfaces
- Chain



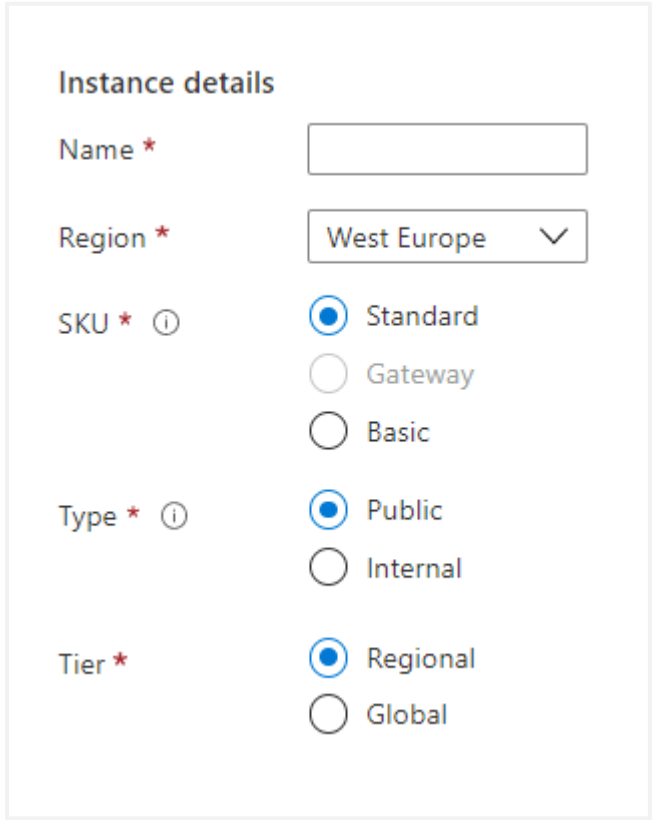
Azure Load balancer and availability zones





Determine Load Balancer SKUs

Feature	Basic SKU	Standard SKU
Backend pool size	Up to 300 IP Configurations	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	Open by default. NSG optional.	Closed to inbound flows unless allowed by an NSG. Internal traffic from the virtual network to the internal load balancer is allowed.
SLA	Not available	99.99%



Create Load balancer in the Azure portal

Subscription

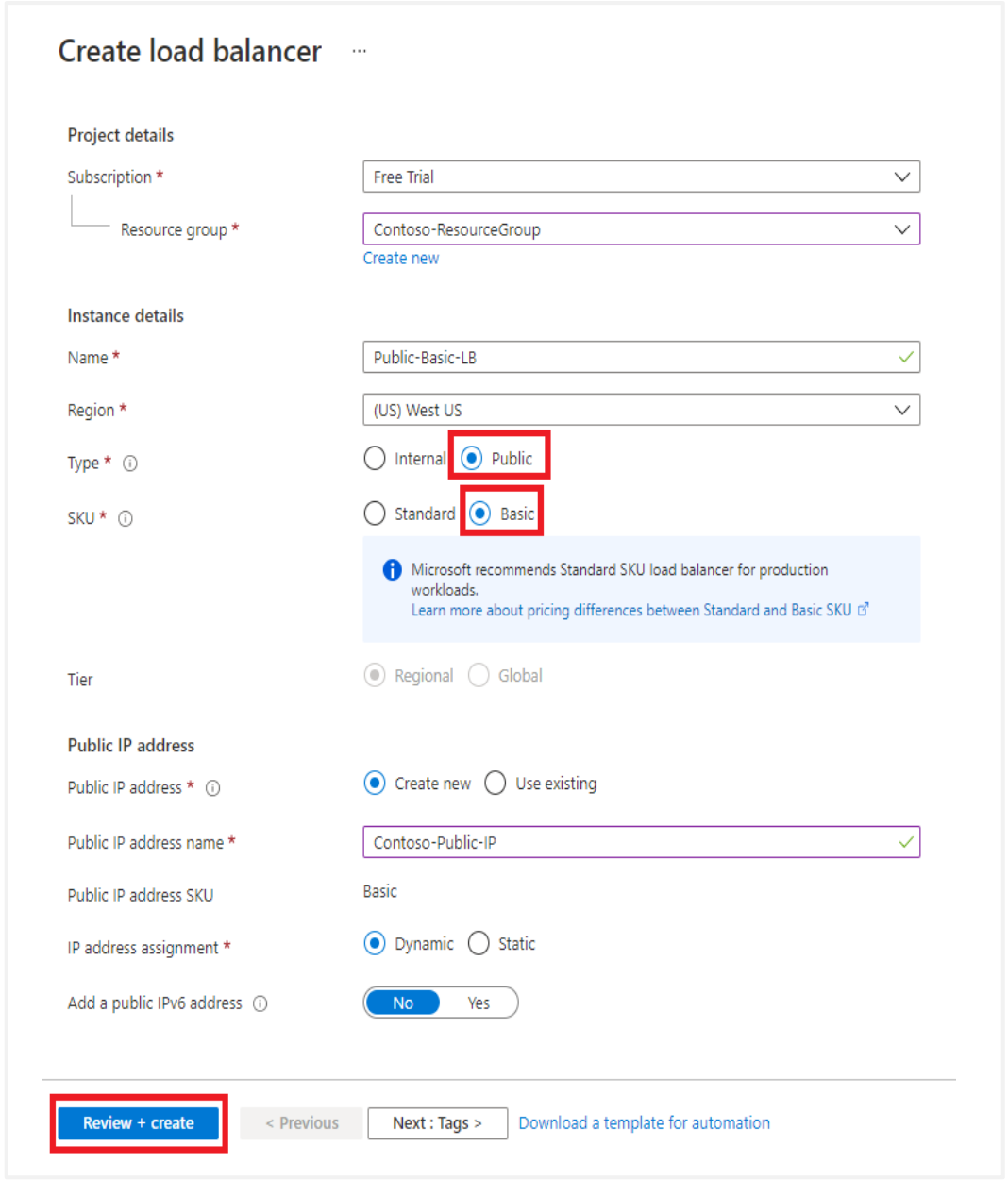
Name

Region

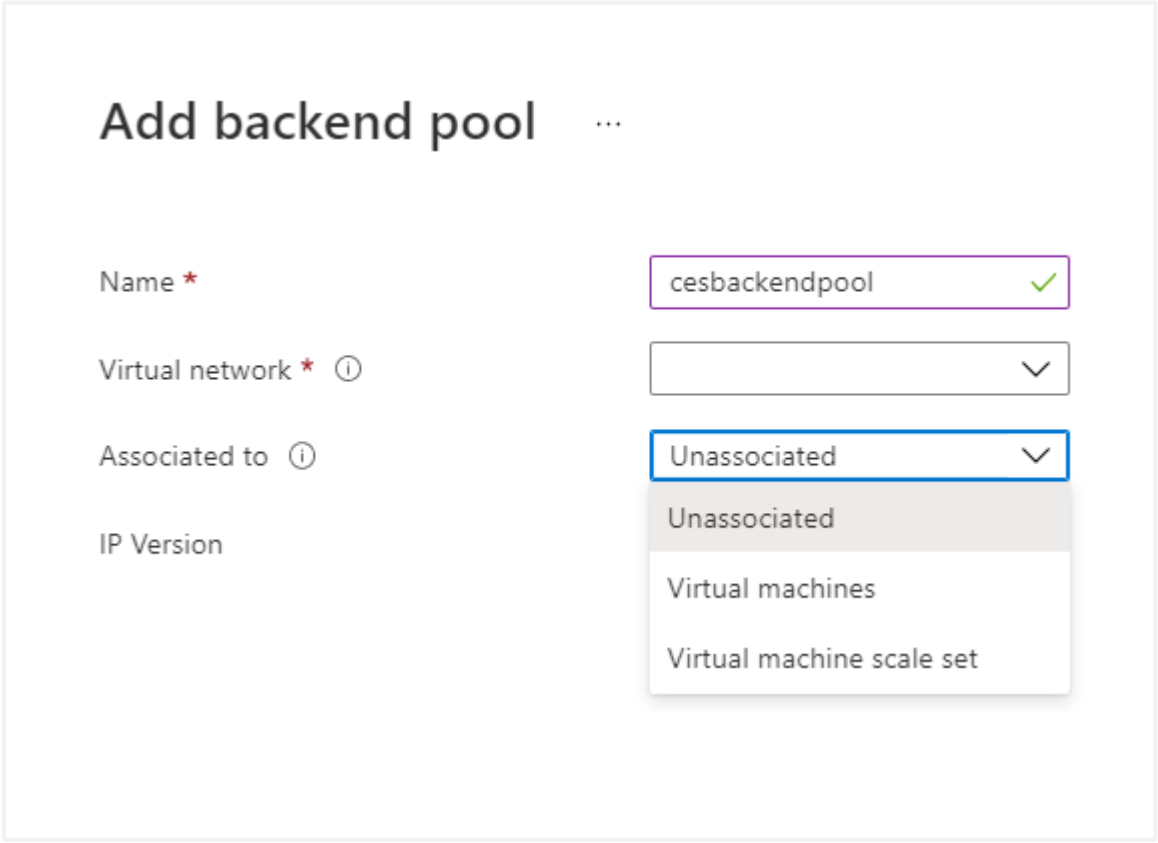
Type

SKU

Tier



Create Backend Pools



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

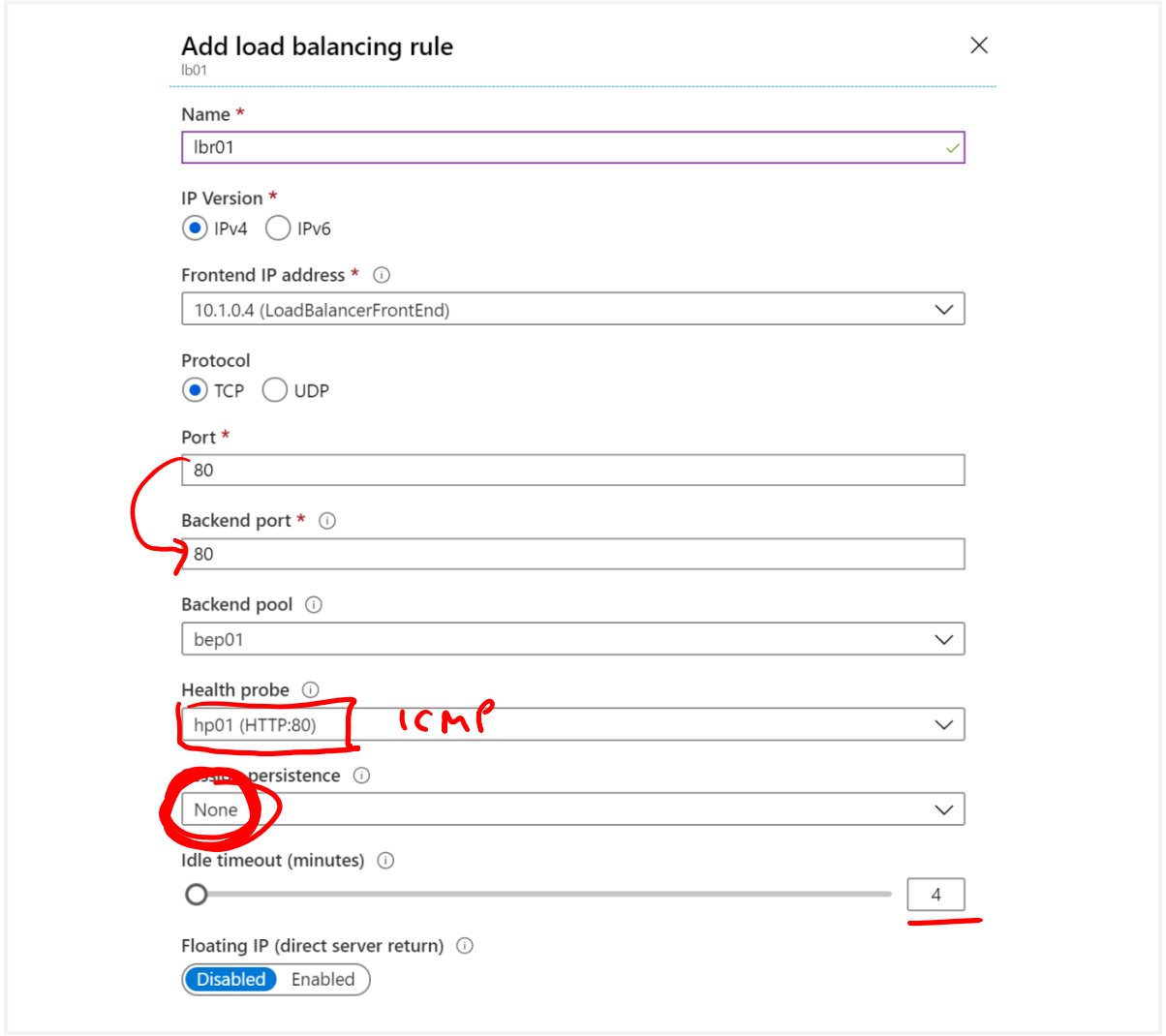
To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer

Create Load Balancer Rules

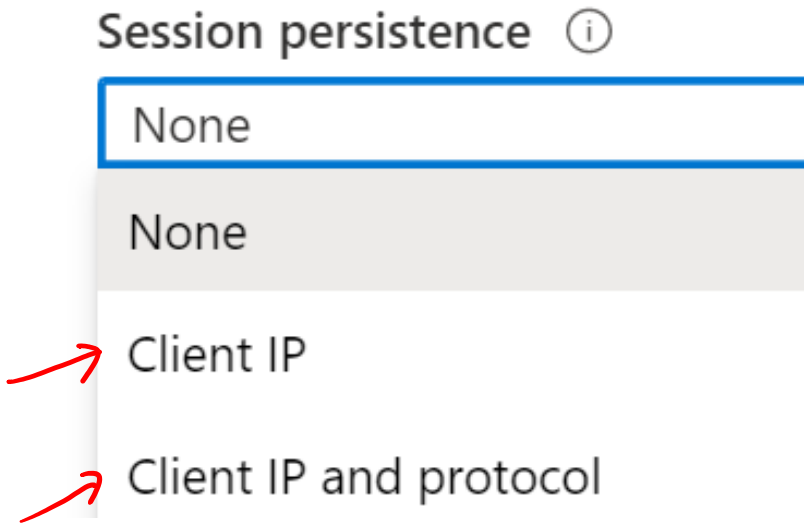
Maps a frontend IP and port combination to a set of backend pool and port combination

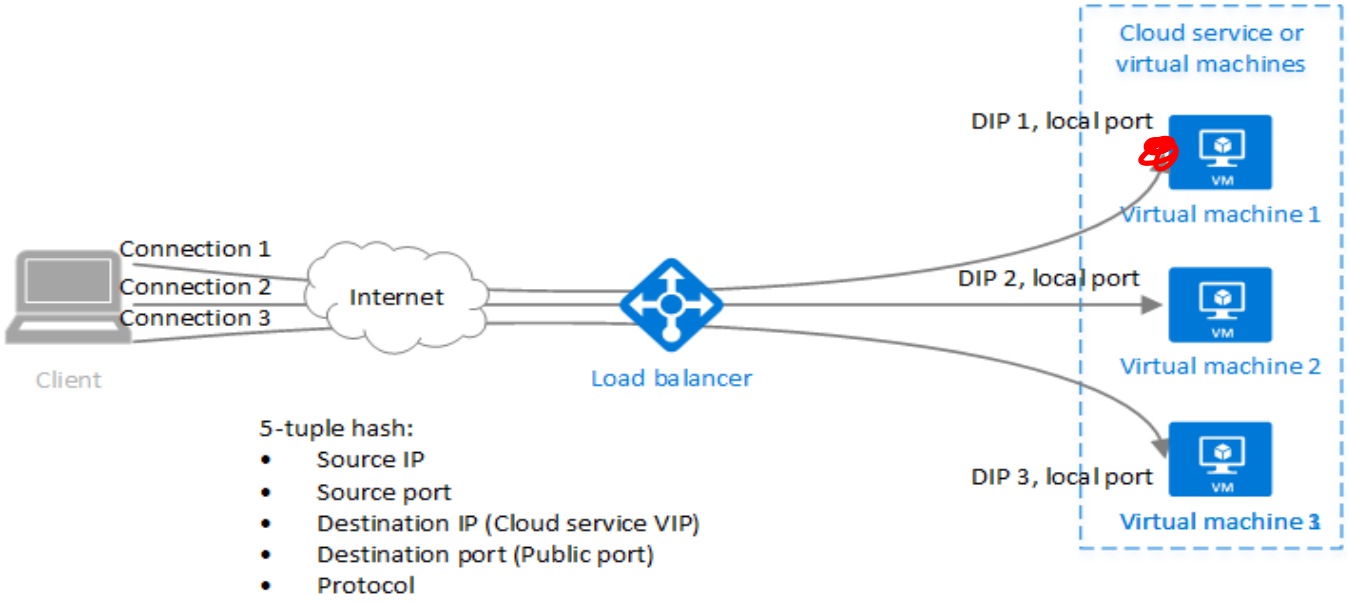
Rules can be used in combination with NAT rules

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



Configure Session Persistence





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

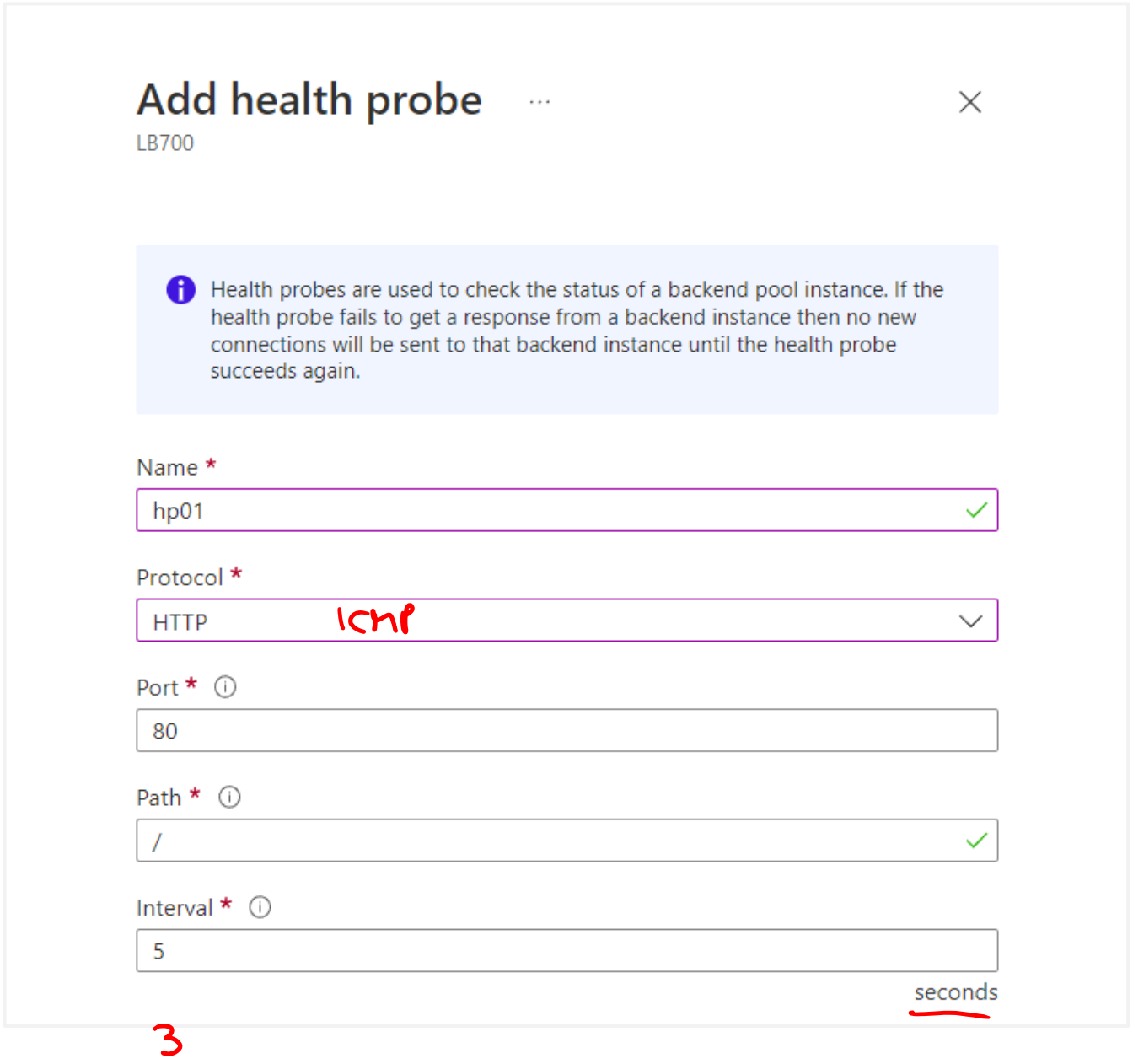
Create Health Probes

Allows the load balancer to monitor the status of an app

Dynamically adds or removes VMs from the load balancer rotation based on their response to health checks

HTTP custom probe

TCP custom probe tries to establish a successful TCP session

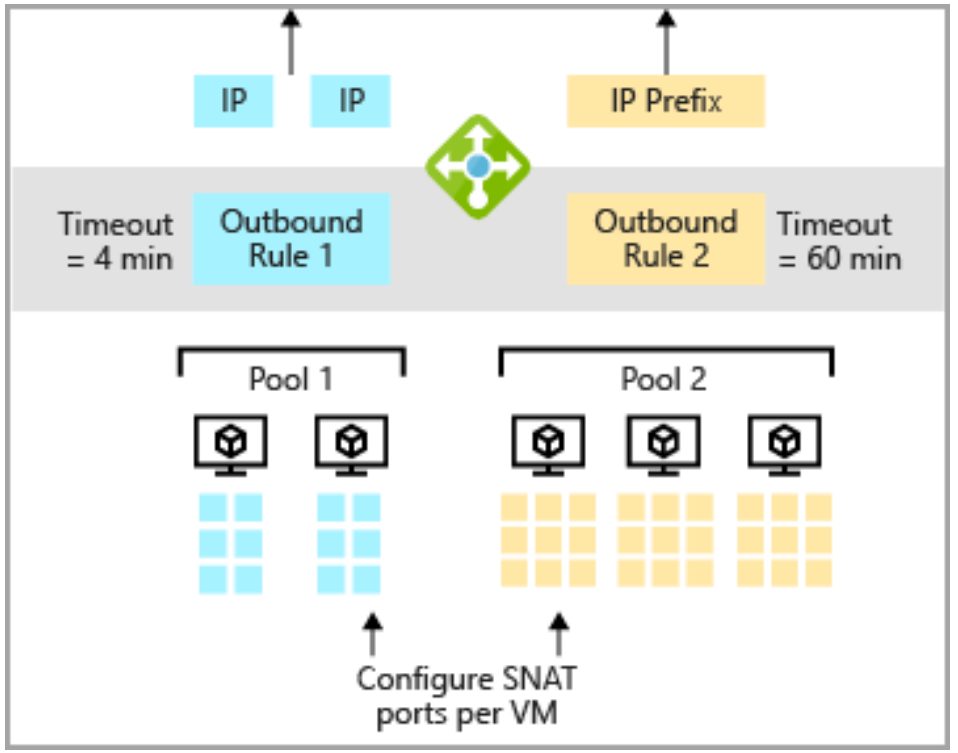


Configure outbound traffic with Standard load balancer

source network address translation (SNAT)

Outbound rules allow you to explicitly define SNAT

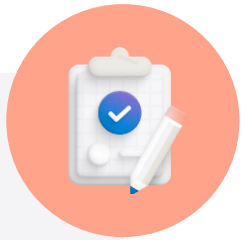
- IP masquerading
- Simplifying your allow lists
- Reduces the number of public IP resources for deployment.



Demonstration

- Create the virtual network
- Create public load balancer
- Create backend pool
- Create a health probe

Learning Recap –Azure Load Balancer



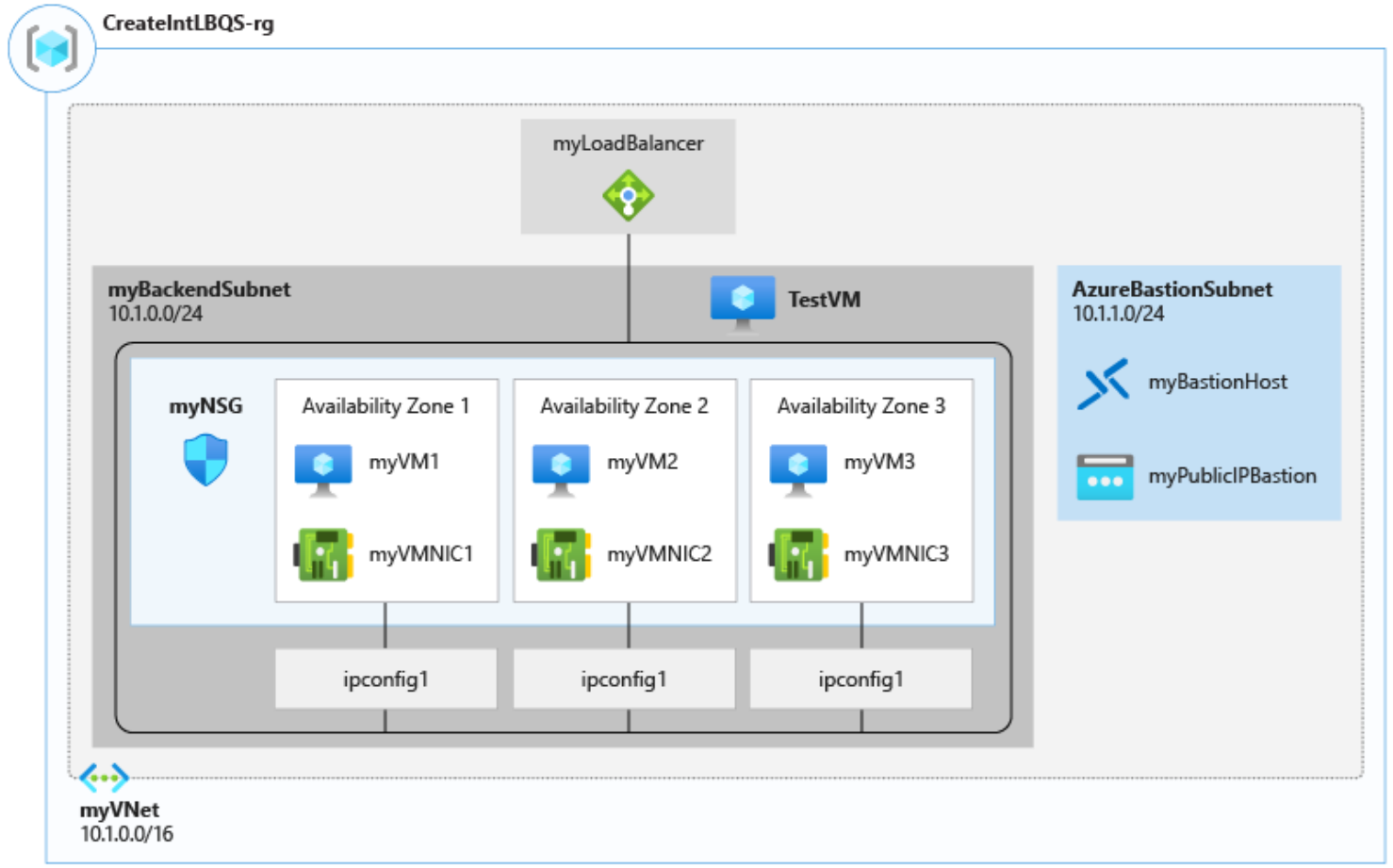
Check your knowledge questions and additional study

[What is Azure Load Balancer? – Azure Load Balancer | Microsoft Docs]

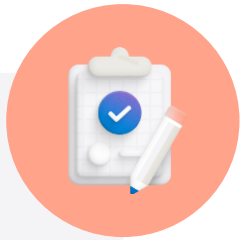
Exercise – Create and configure an internal load balancer using the Azure portal

Exercise - Create and configure an Azure load balancer

Task 1: Create the virtual network
Task 2: Create the load balancer
Task 3: Create load balancer resources
Task 4: Create backend servers
Task 5: Test the load balancer



Exercise Create and Configure an Internal Load Balancer Using the Azure Portal



Check your knowledge questions and additional study

[Quickstart: Create a public load balancer – Azure portal – Azure Load Balancer | Microsoft Docs]

Explore Azure Traffic Manager

Learning Objectives – Explore Azure Traffic Manager

- Use cases for Azure Traffic Manager
- How Traffic manager works
- Traffic routing methods
- Traffic manager endpoints
- Configuring traffic manager profiles
- Configure Endpoint monitoring
- Demonstration
- Learning Reap

Use cases for Azure Traffic Manager

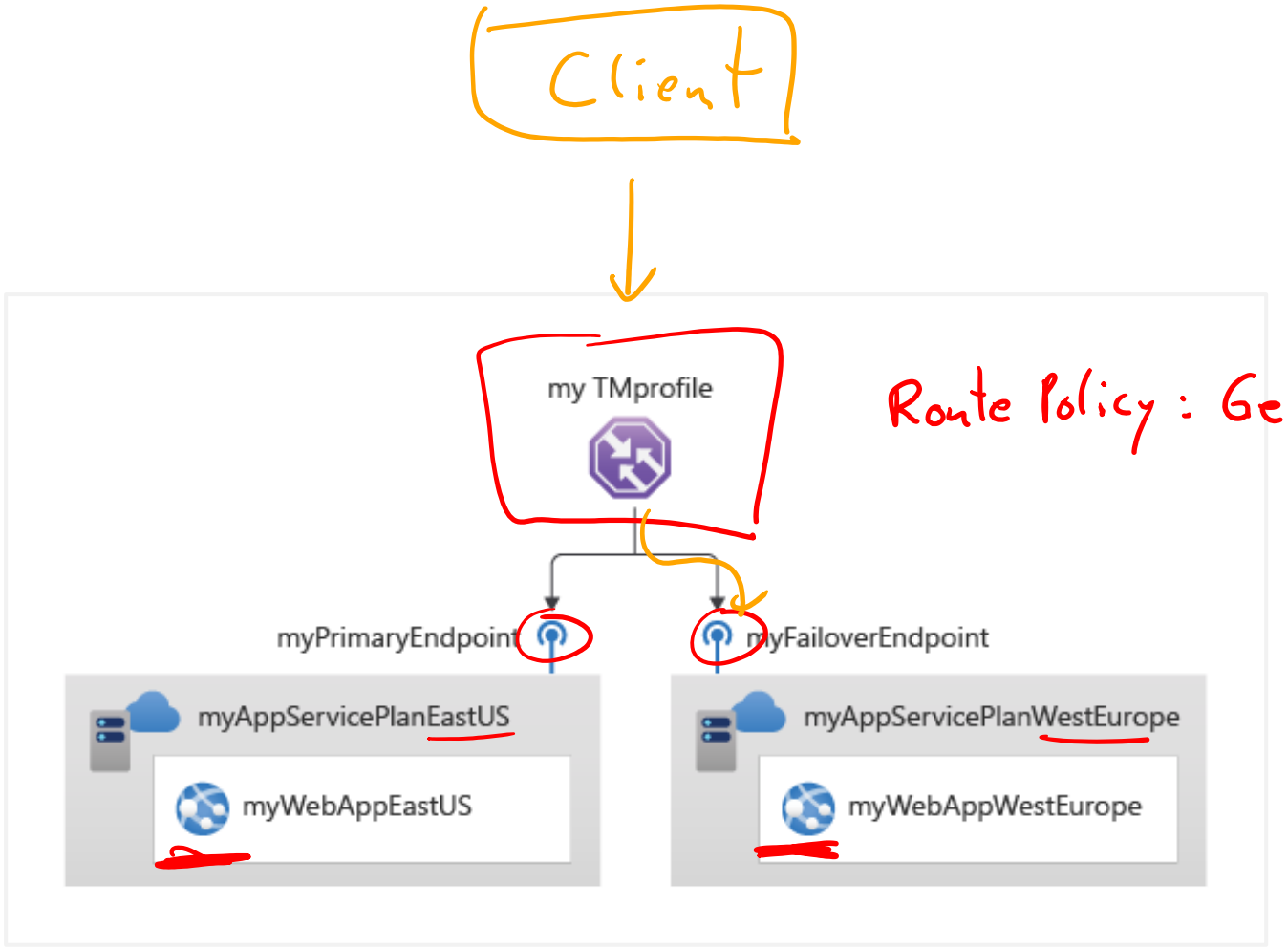
Increase application availability

Improve application performance

Service maintenance without downtime

Combine hybrid applications

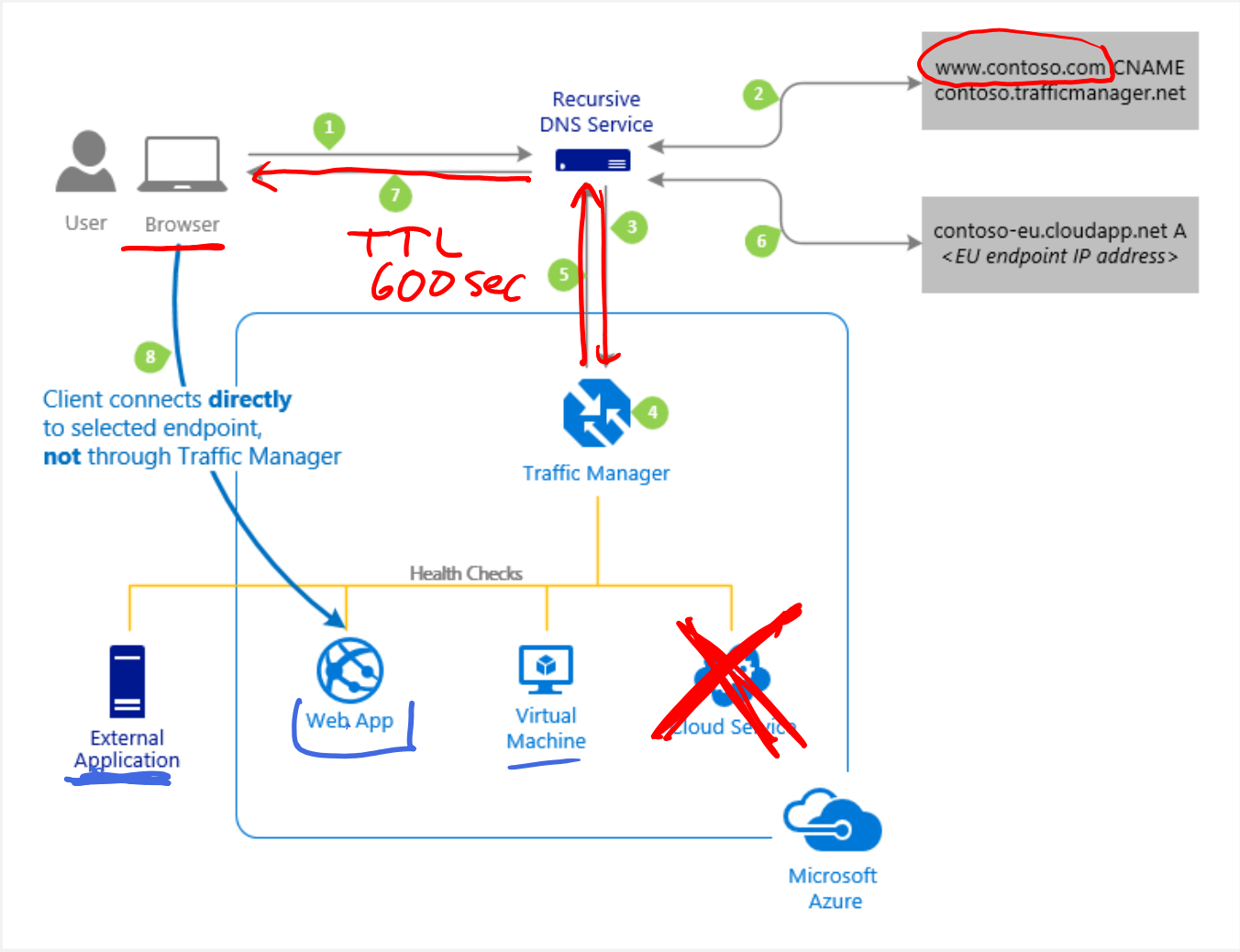
Distribute traffic for complex deployments



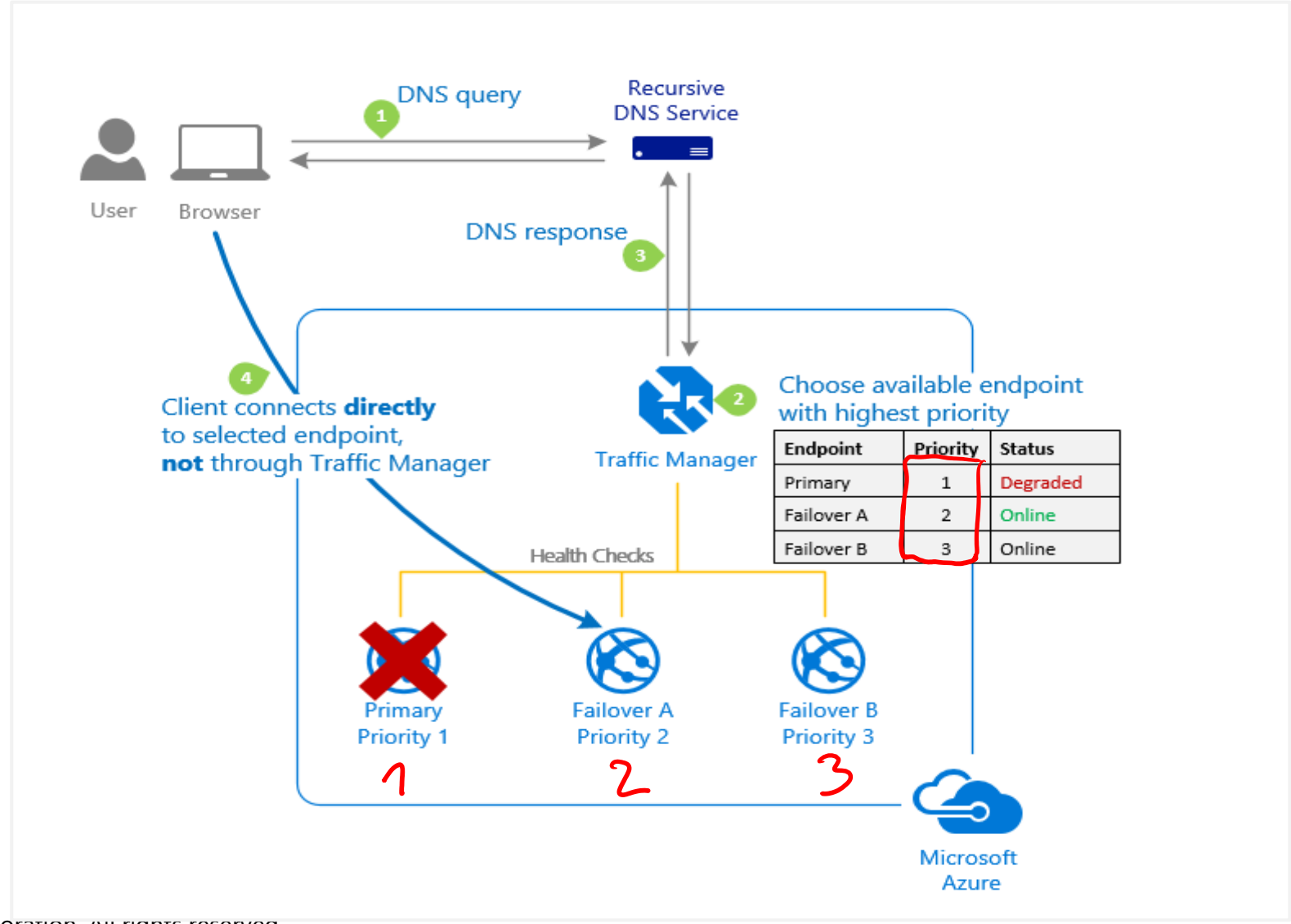
How Traffic manager works

The Traffic Manager name servers receive the request. They choose an endpoint based on:

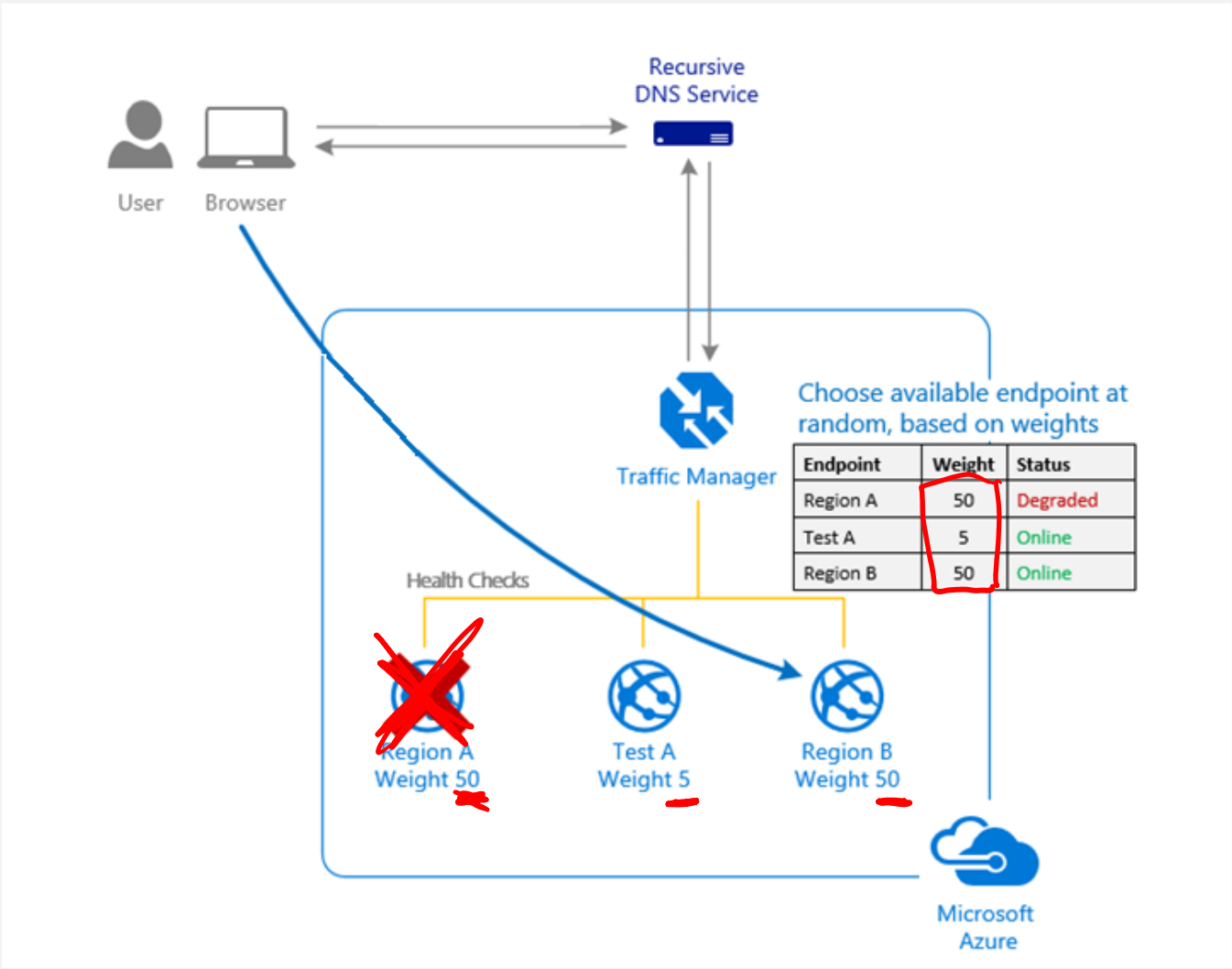
- The configured state of each endpoint
- The current health of each endpoint, as determined by the Traffic Manager health checks
- The chosen traffic-routing method
- Final connection is not going through Traffic Manager



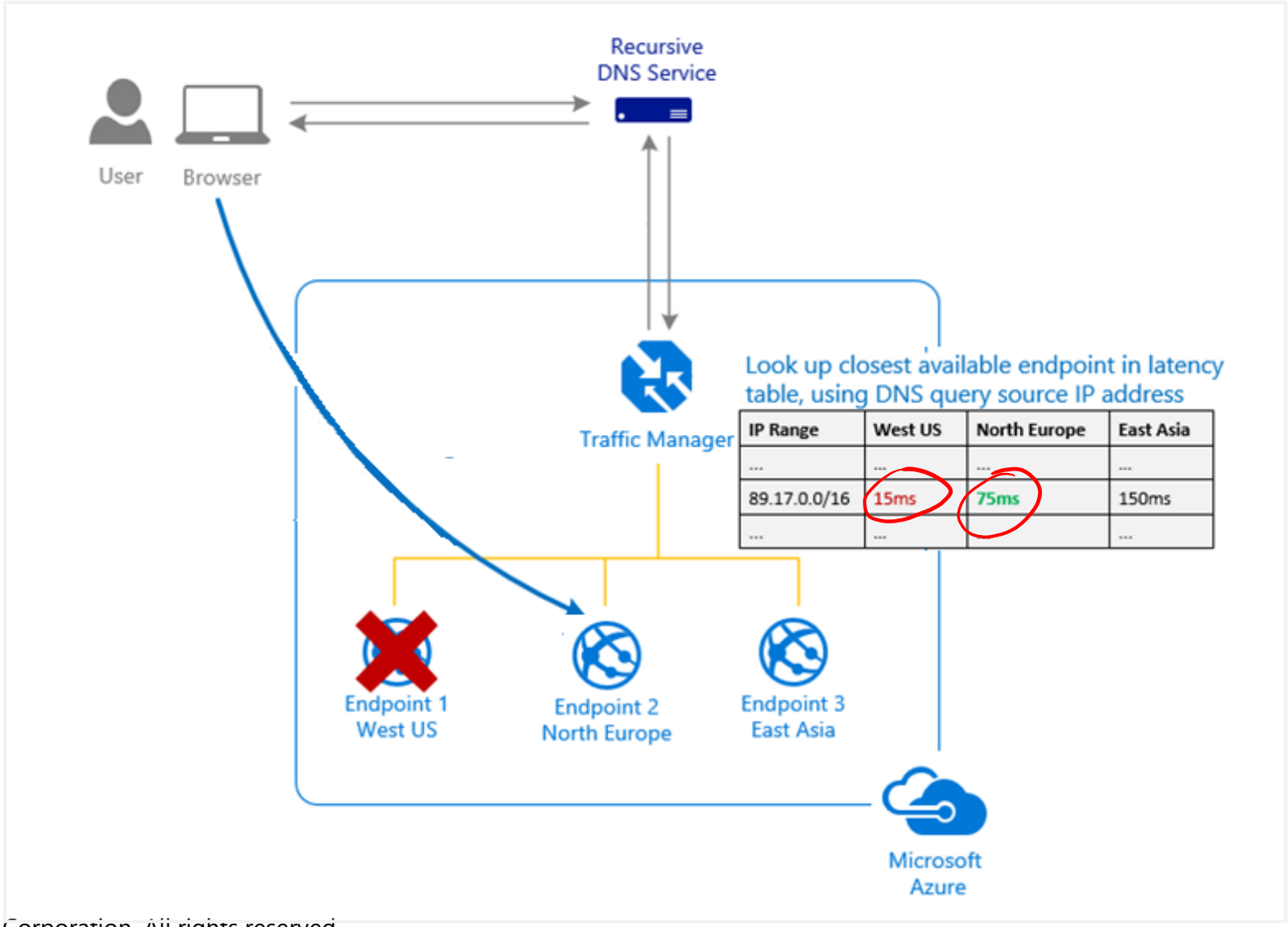
Traffic routing methods – Priority



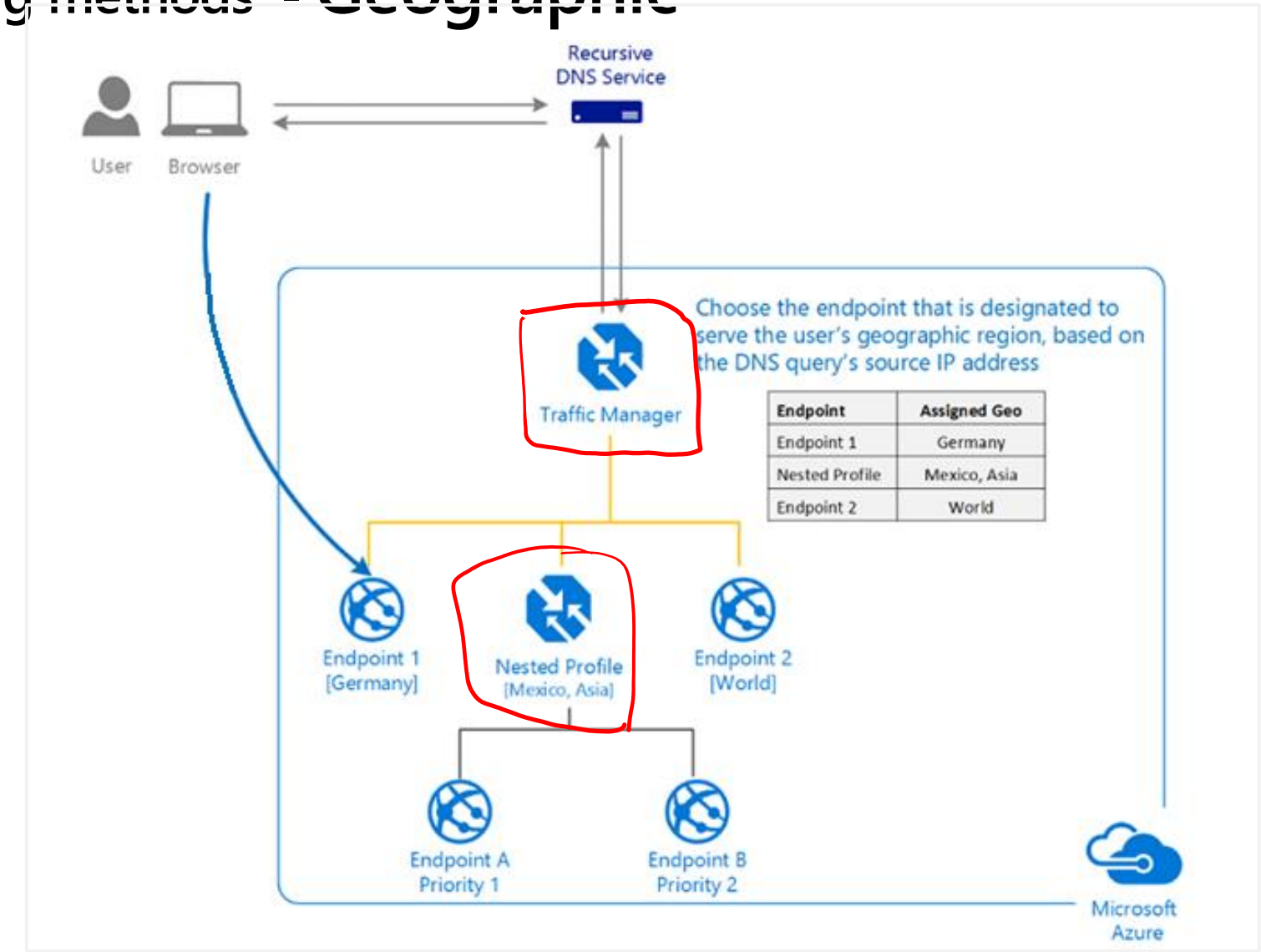
Traffic routing methods – Weighted



Traffic routing methods – Performance



Traffic routing methods - Geographic



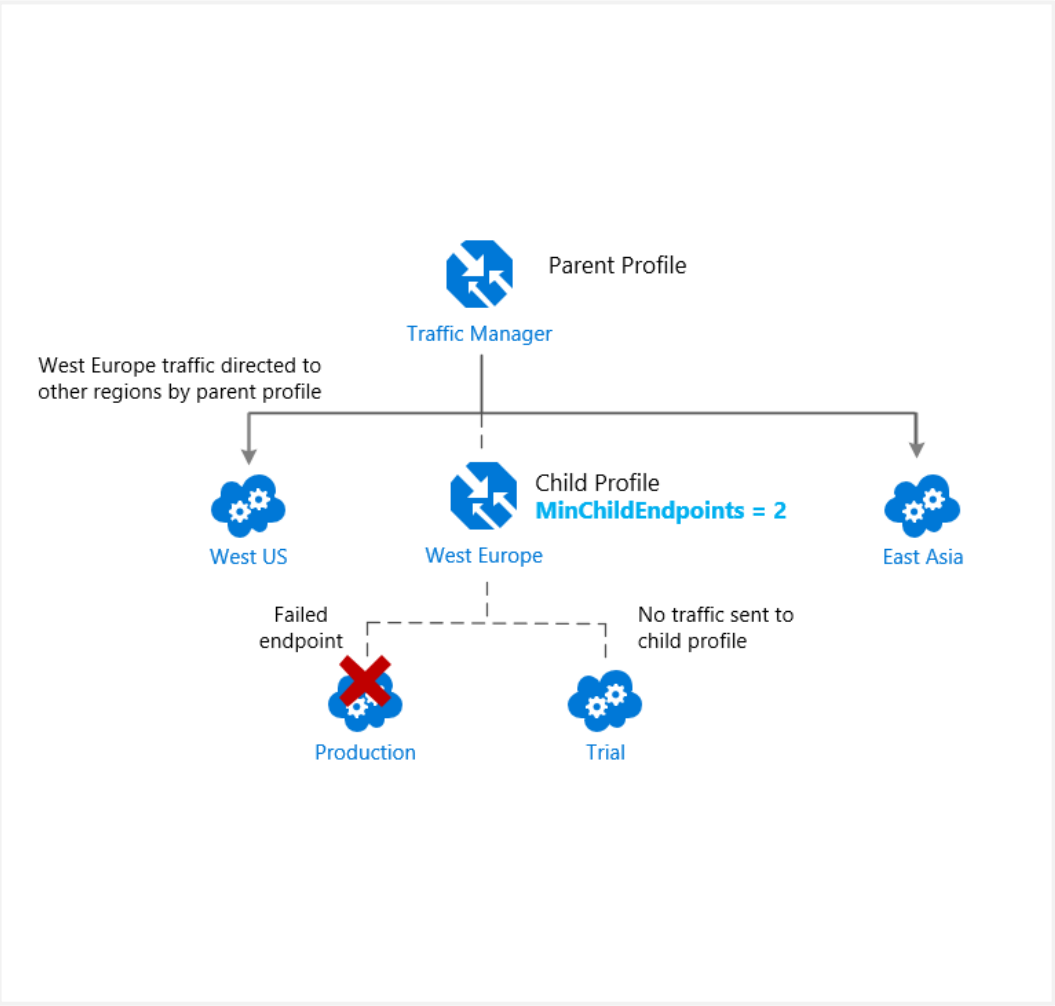
Traffic manager endpoints

Azure endpoints – load balance traffic to a cloud service, web app, or public IP address in the same subscription within Azure.

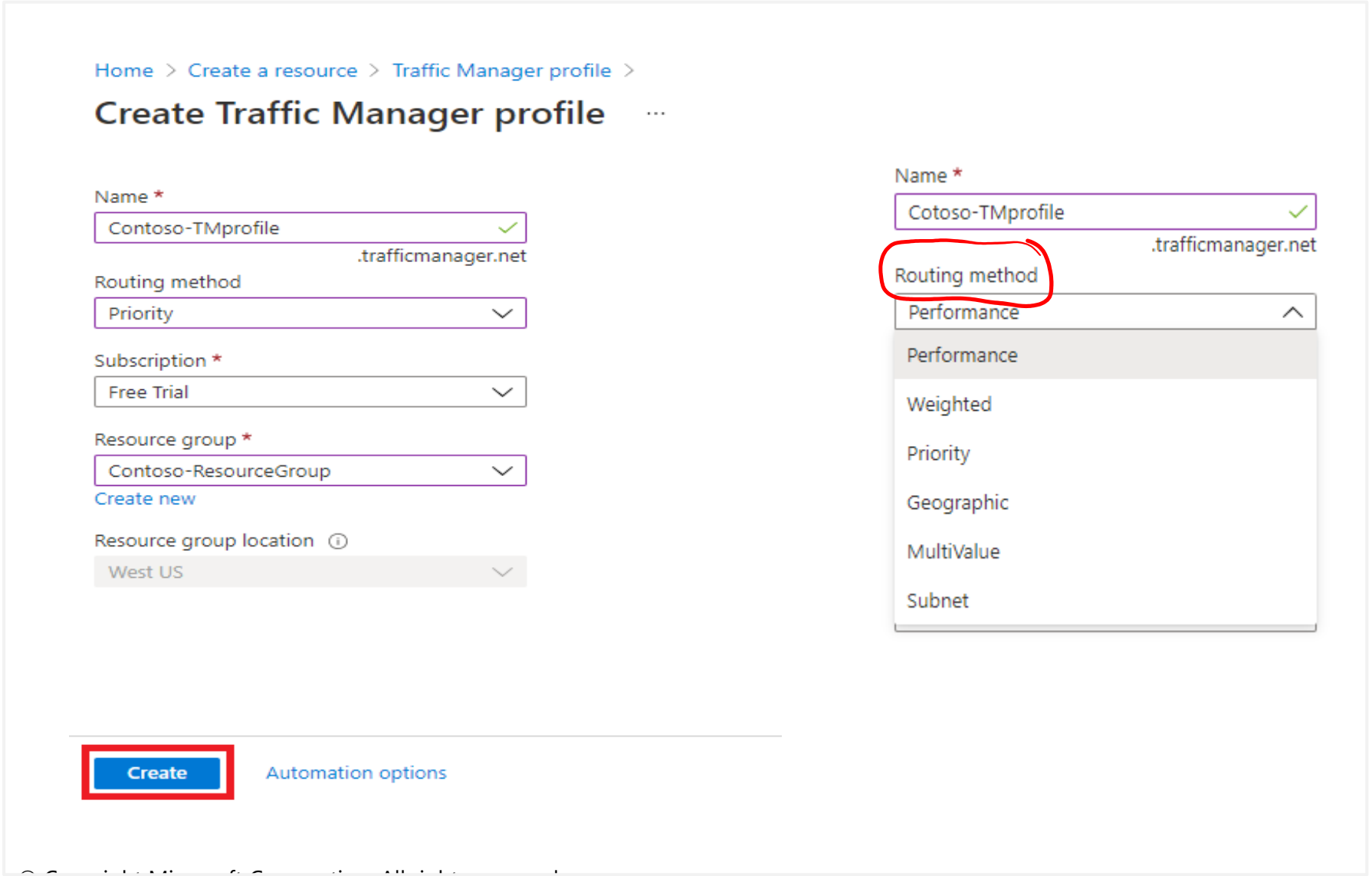
App Service

External endpoints - load balance traffic for IPv4/IPv6 addresses, FQDNs, or for services hosted outside Azure. These services can either be on-premises or with a hosting provider.

Nested endpoints - combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.



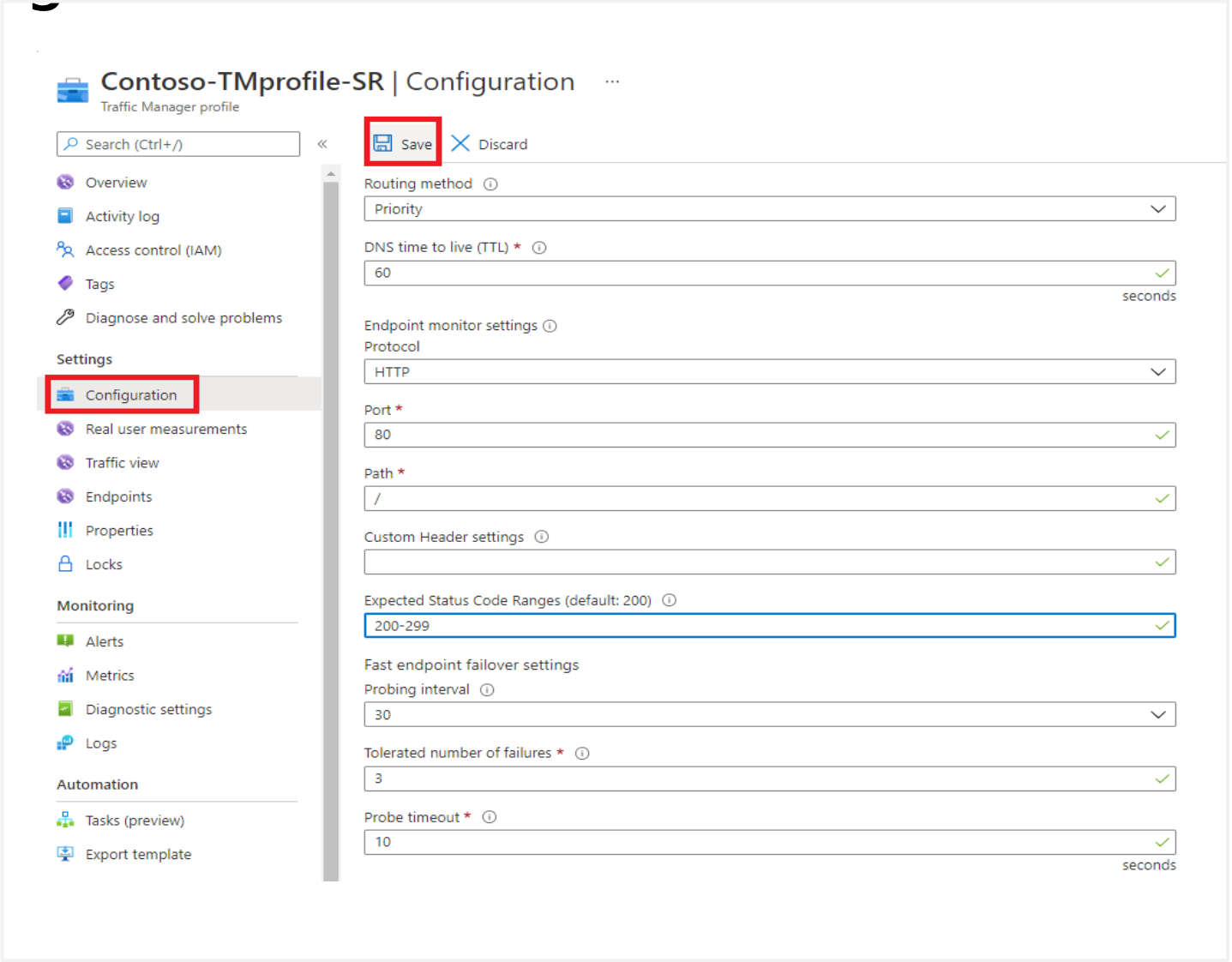
Configuring traffic manager profiles



Configure Endpoint monitoring

Open the **Configuration page** for the Traffic Manager profile

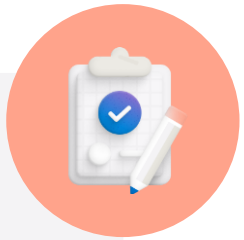
Select **Endpoint monitor settings** section, and specify the following settings:
Protocol
Port
Path
Custom header settings
Expected status code ranges
Probing interval
tolerated number of failures
probe timeout



Demonstration – Azure Traffic Manager

- Create a Traffic Manager profile
- Add Traffic Manager endpoints
- Test Traffic Manager profile

Learning Recap – Azure Traffic Manager



Check your knowledge questions and additional study

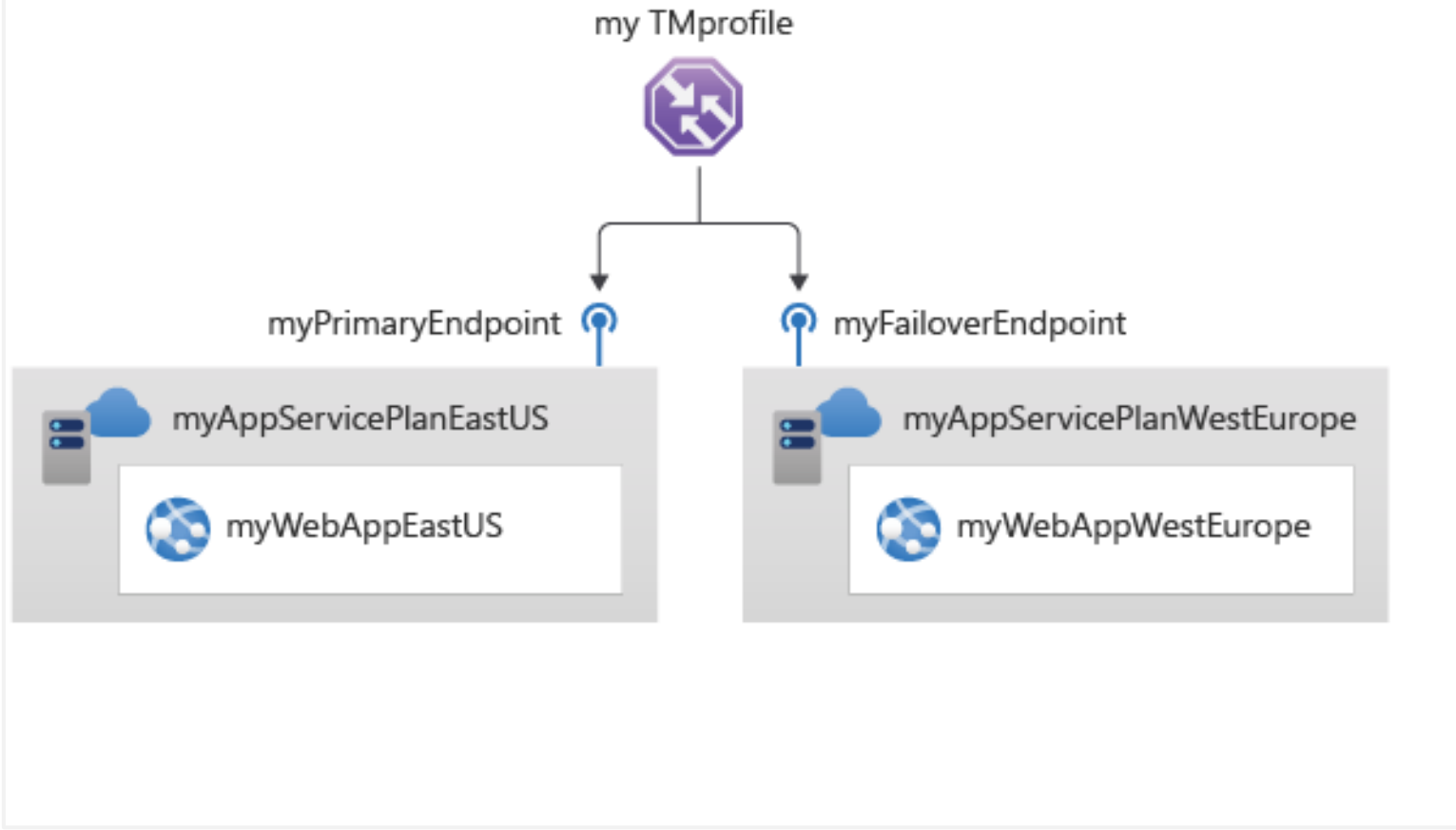
[Azure Traffic Manager | Microsoft Docs]

[Tutorial – Improve website response with Azure Traffic Manager | Microsoft Docs]

Exercise – Create a traffic manager profile using the Azure portal

Exercise- create a traffic manager profile using the Azure portal

Task 1: Create the web apps
Task 2: Create a Traffic Manager profile
Task 3: Add Traffic Manager endpoints
Task 4: Test the Traffic Manager profile



End of presentation