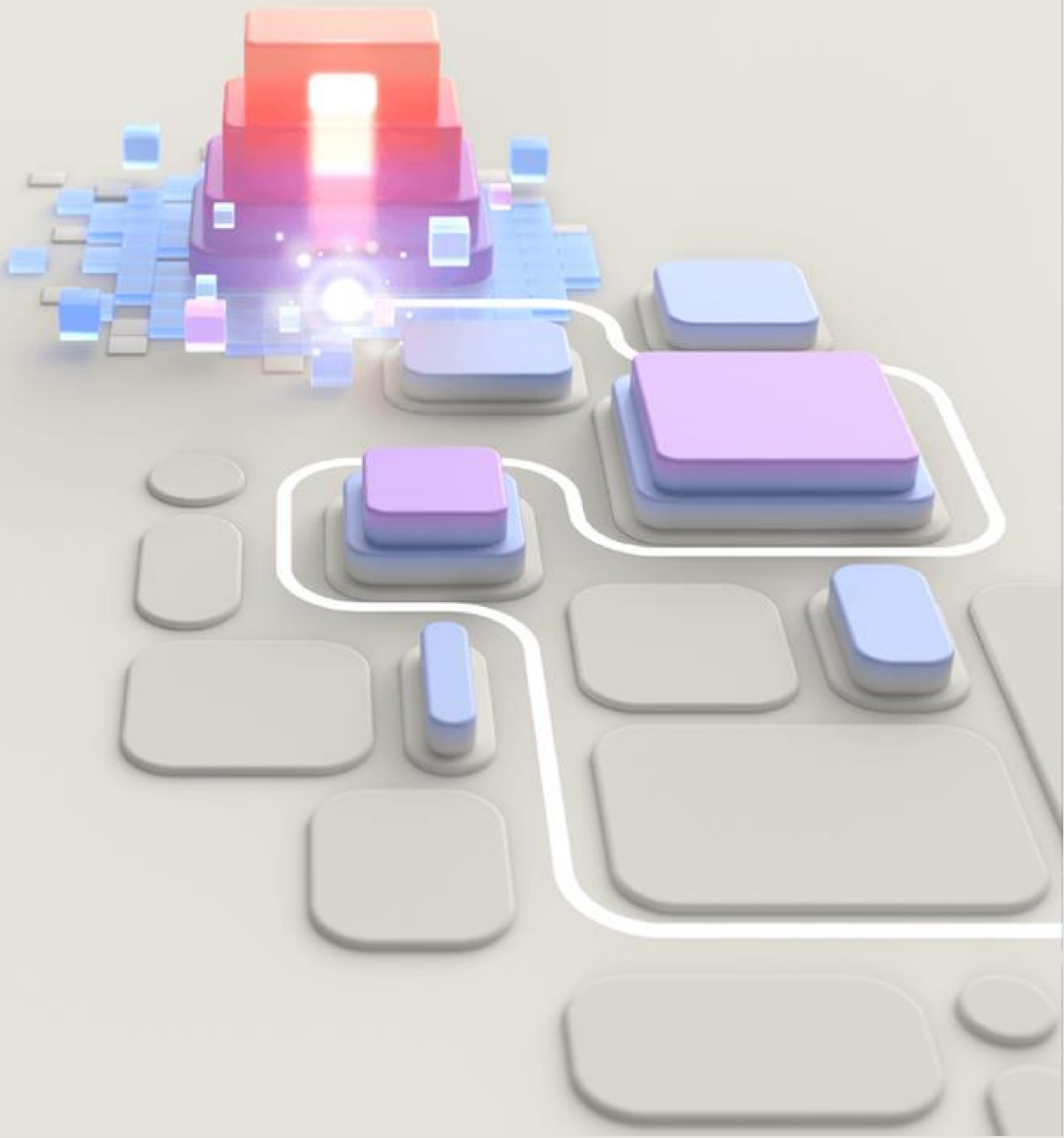
Microsoft

AZ-700

Module 04

Load balancing non-HTTP(S) traffic



AZ-700 Agenda

Tag 2

Guten Morgen!

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

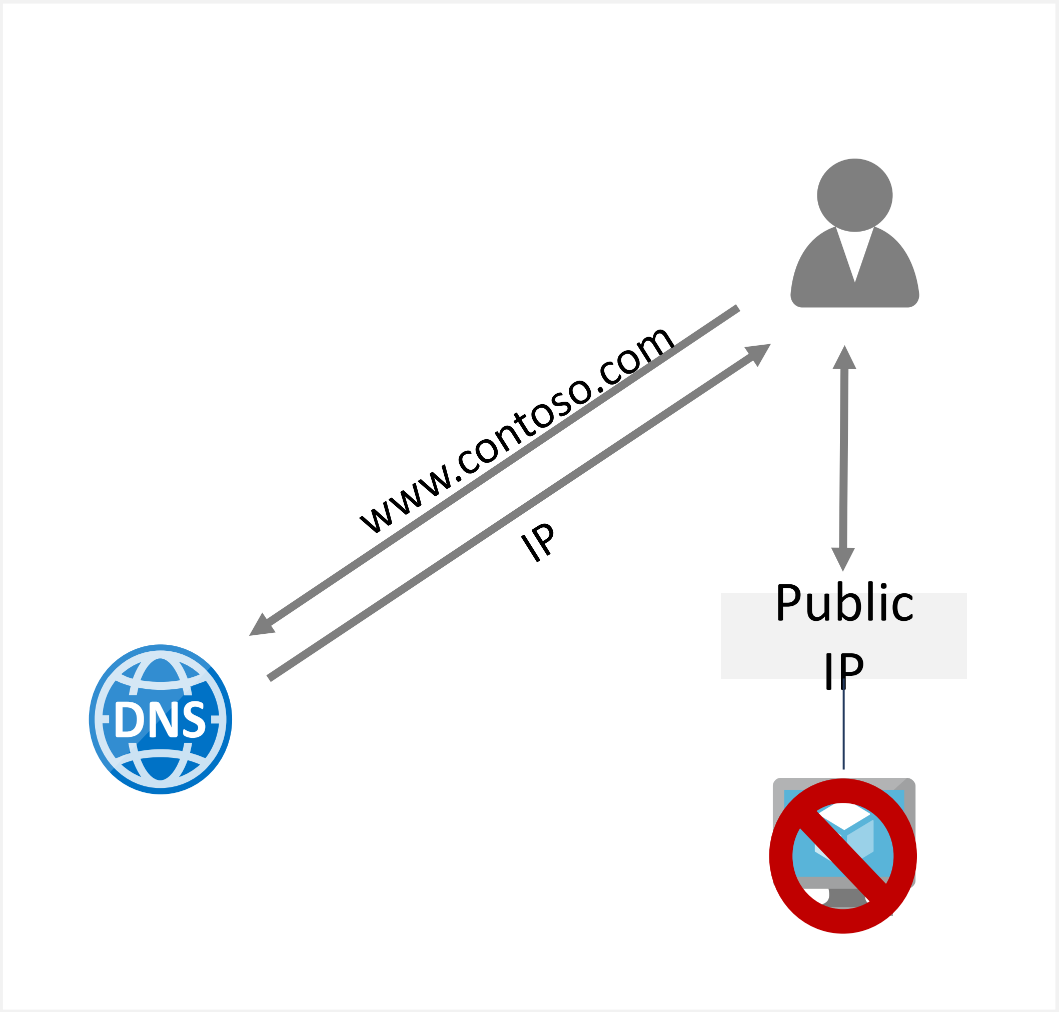
Module 08: Design and Implement Network Monitoring

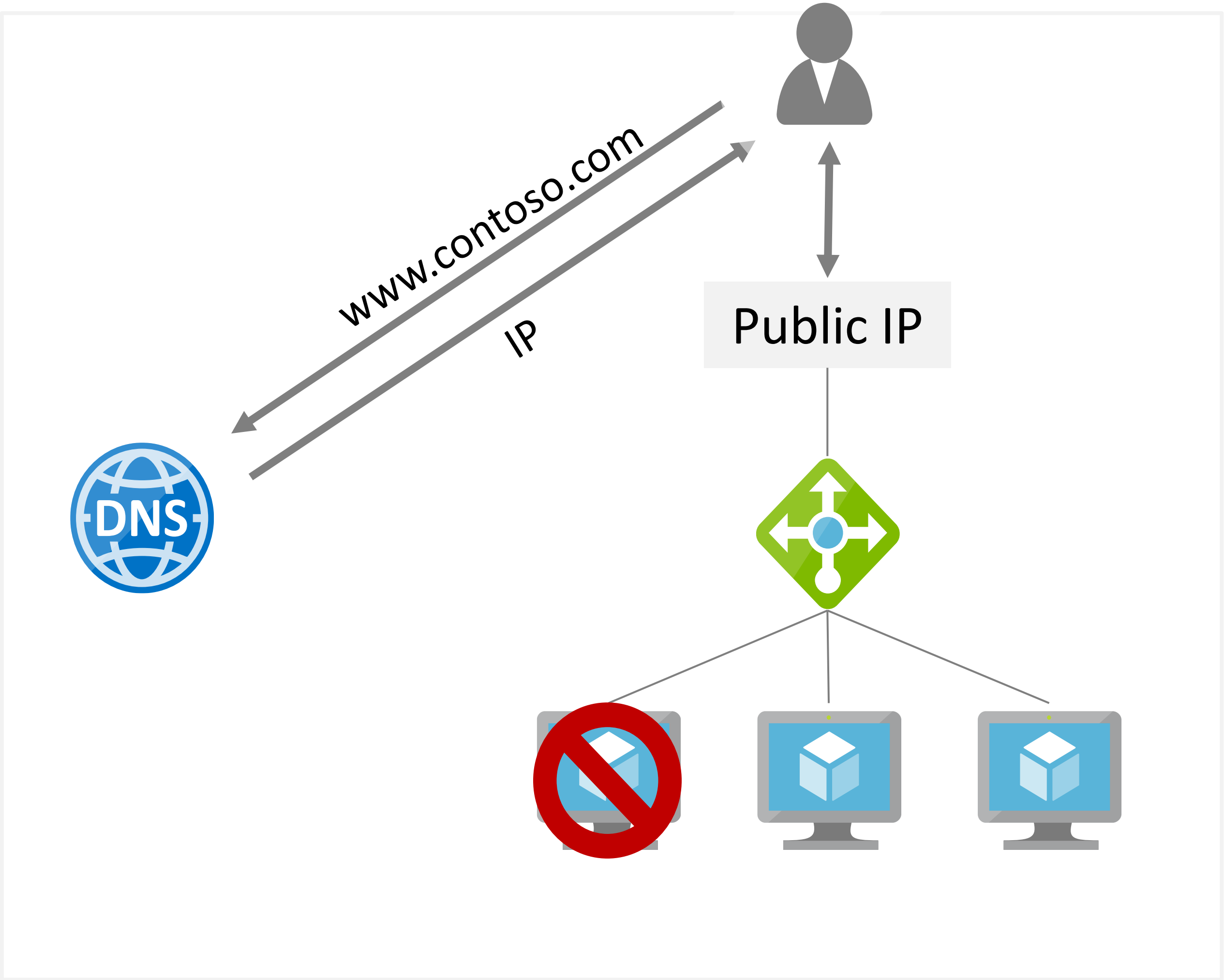
Module Overview

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

Explore load balancing options in the Azure portal

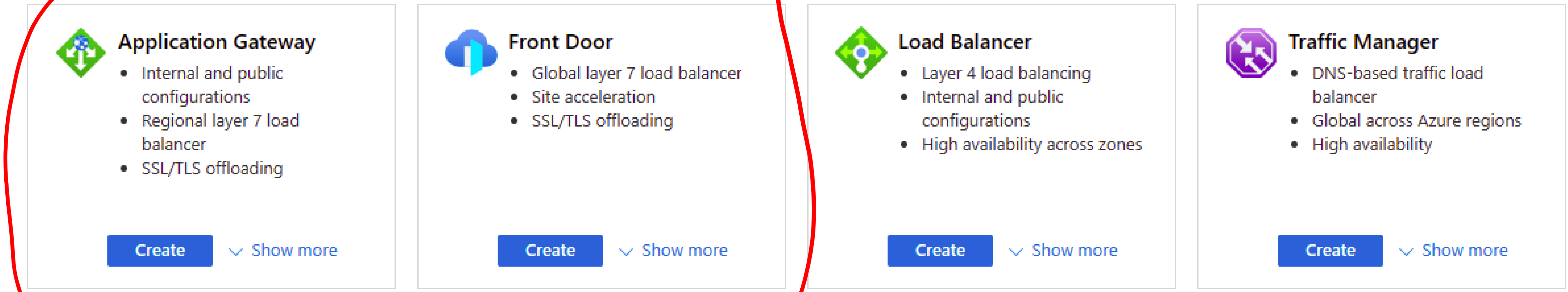
What is a Load balancer





Load balancing options for Azure

DNS



Application Gateway

- Internal and public configurations
- Regional layer 7 load balancer
- SSL/TLS offloading

Front Door

- Global layer 7 load balancer
- Site acceleration
- SSL/TLS offloading

Load Balancer

- Layer 4 load balancing
- Internal and public configurations
- High availability across zones

Traffic Manager

- DNS-based traffic load balancer
- Global across Azure regions
- High availability

Basic

Standard

Choosing a load balancing option

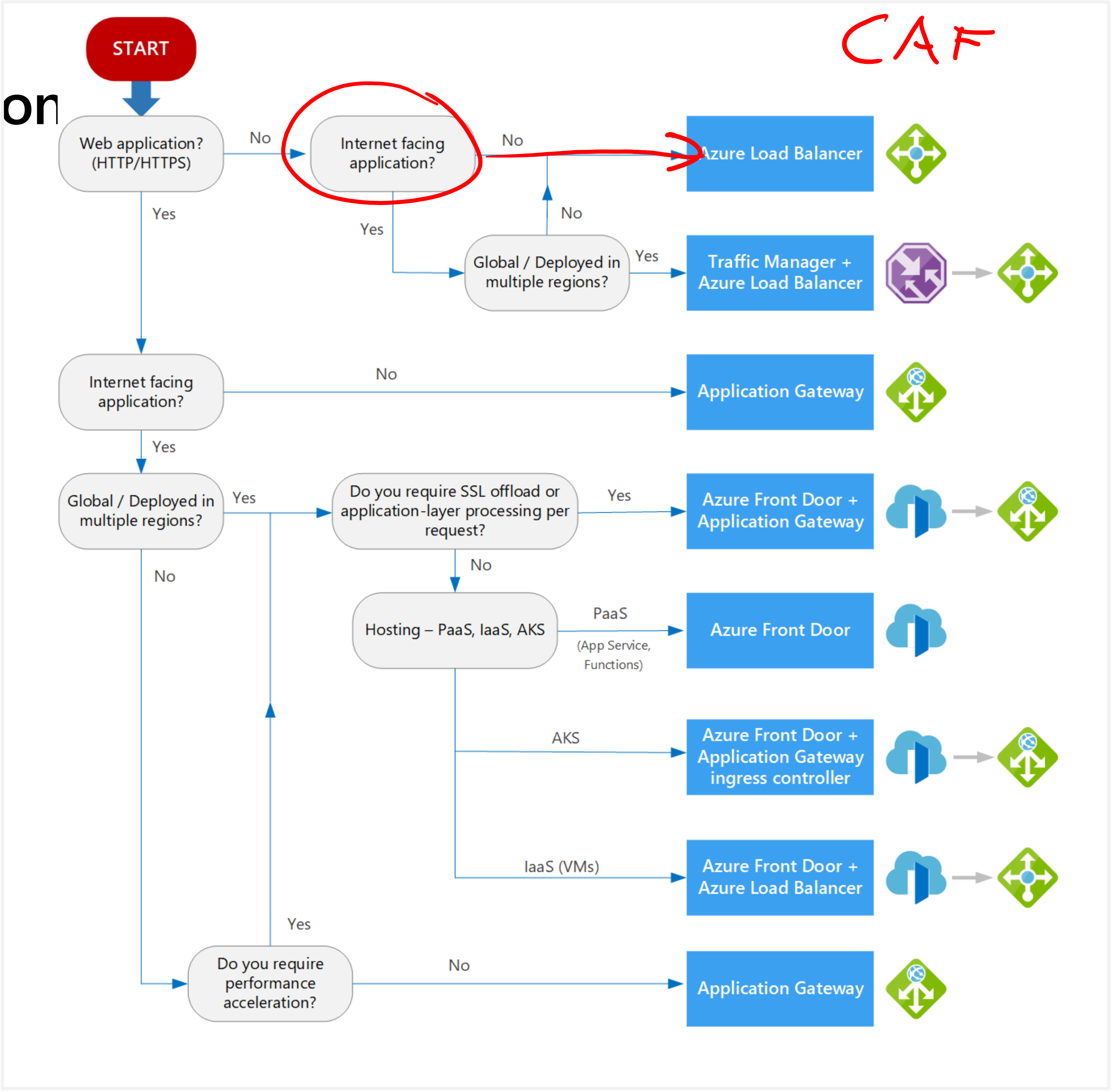
Type of traffic

Scope

Availability

Cost

Features and limitations



CAF

START

Web application? (HTTP/HTTPS)

No

Internet facing application?

No

Azure Load Balancer

Yes

No

Global / Deployed in multiple regions?

Yes

Traffic Manager + Azure Load Balancer

Yes

Internet facing application?

No

Application Gateway

Yes

Global / Deployed in multiple regions?

Yes

Do you require SSL offload or application-layer processing per request?

Yes

Azure Front Door + Application Gateway

No

Hosting – PaaS, IaaS, AKS

PaaS (App Service, Functions)

Azure Front Door

AKS

Azure Front Door + Application Gateway ingress controller

IaaS (VMs)

Azure Front Door + Azure Load Balancer

No

Yes

Do you require performance acceleration?

No

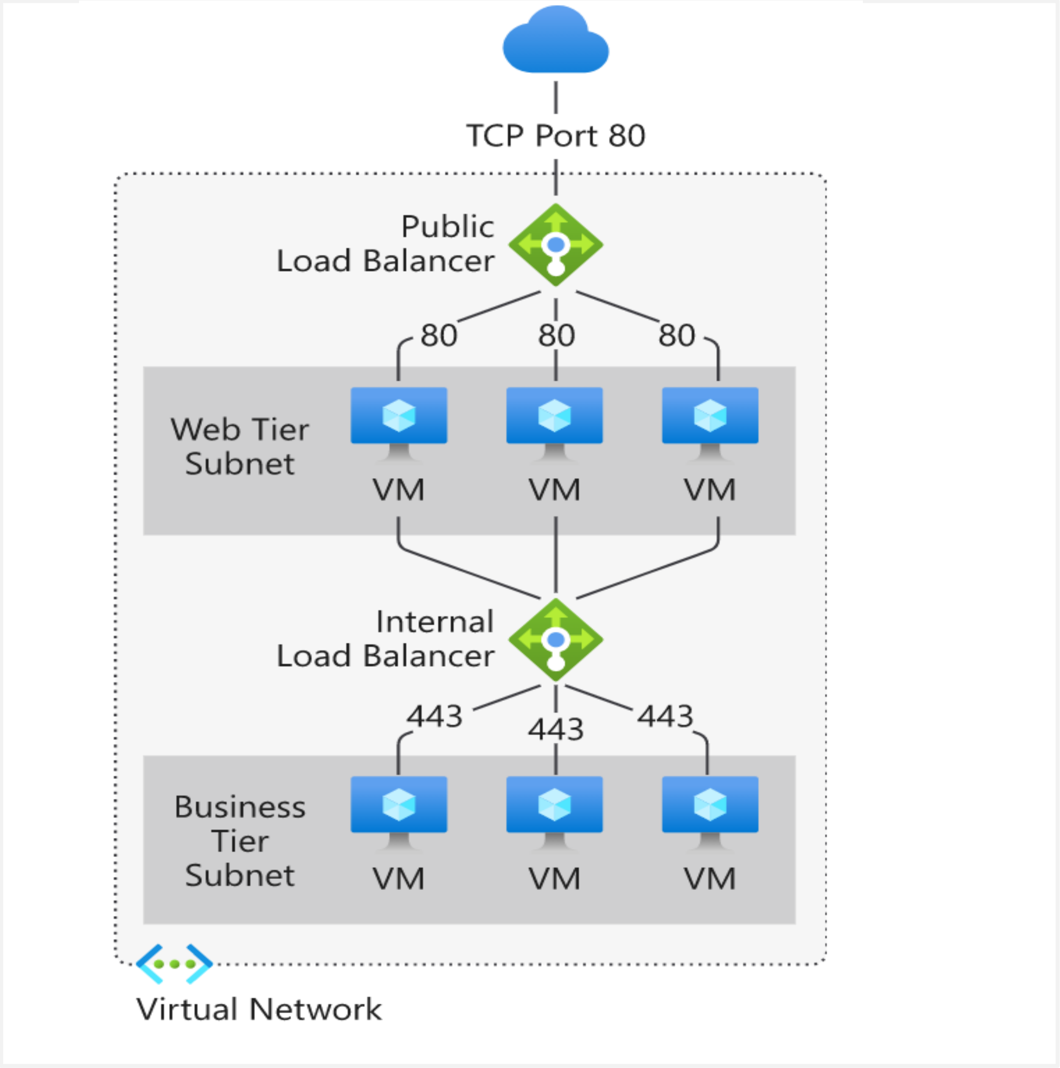
Application Gateway

Design and implement Azure Load balancer

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

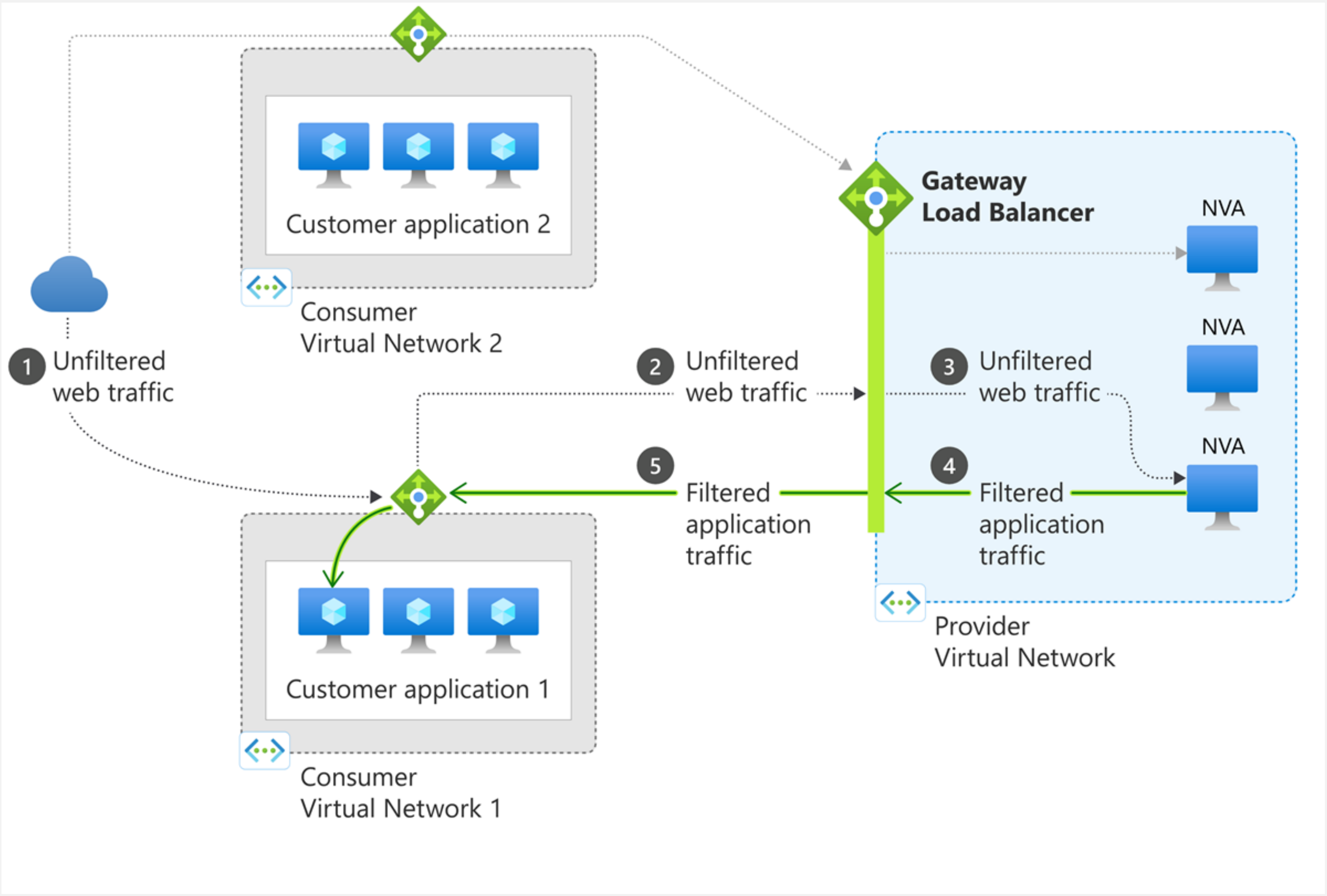


Gateway Load Balancer

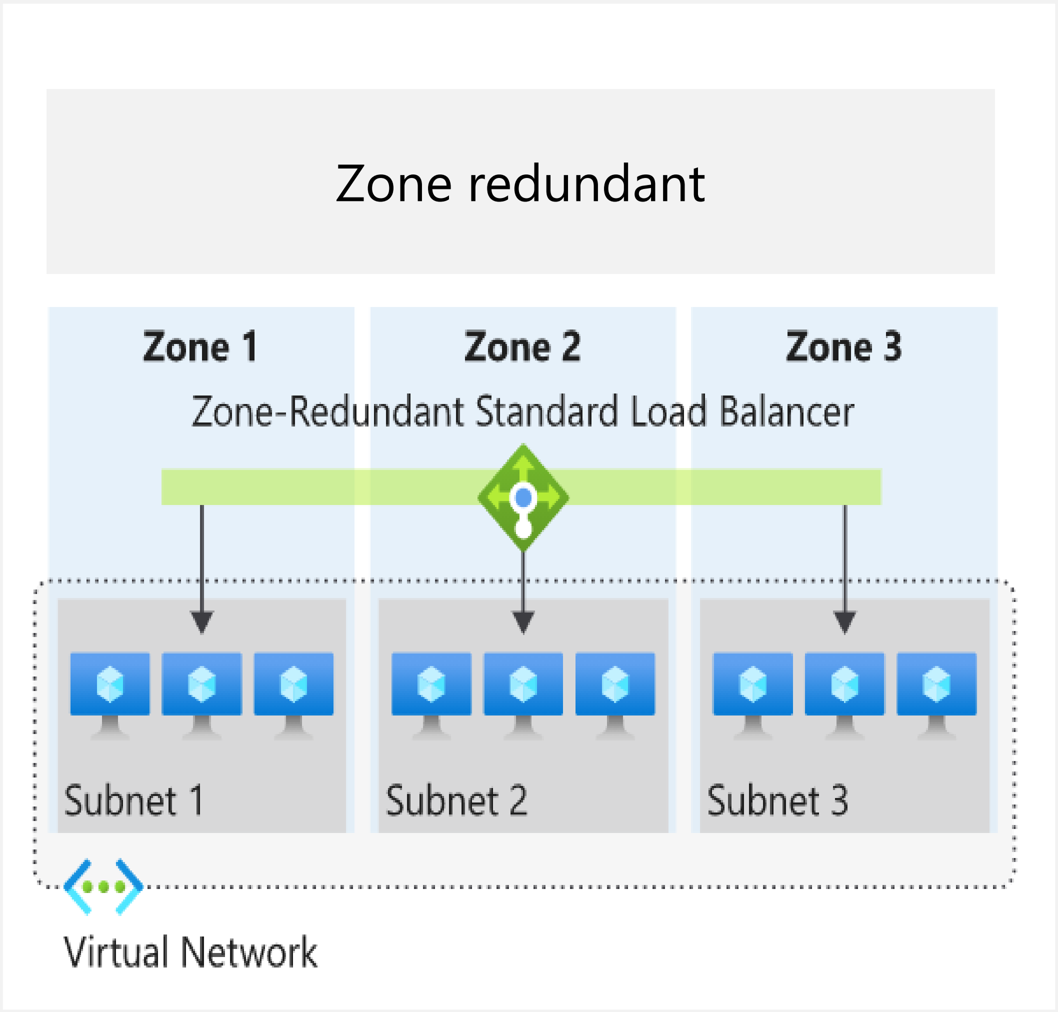
Gateway Load Balancer is a SKU of the Azure Load Balancer portfolio catered for high performance and high availability scenarios with third-party Network Virtual Appliances (NVAs)

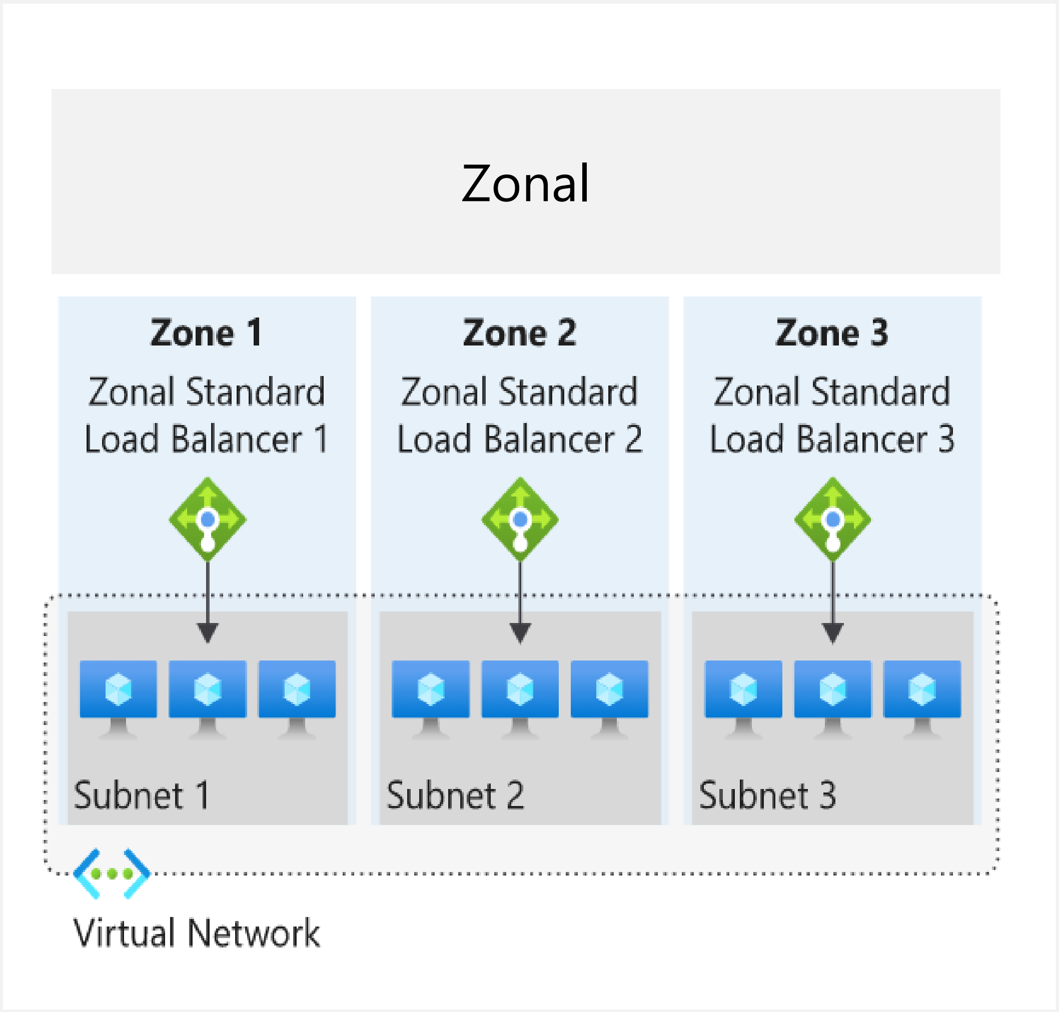
Components to configure:

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



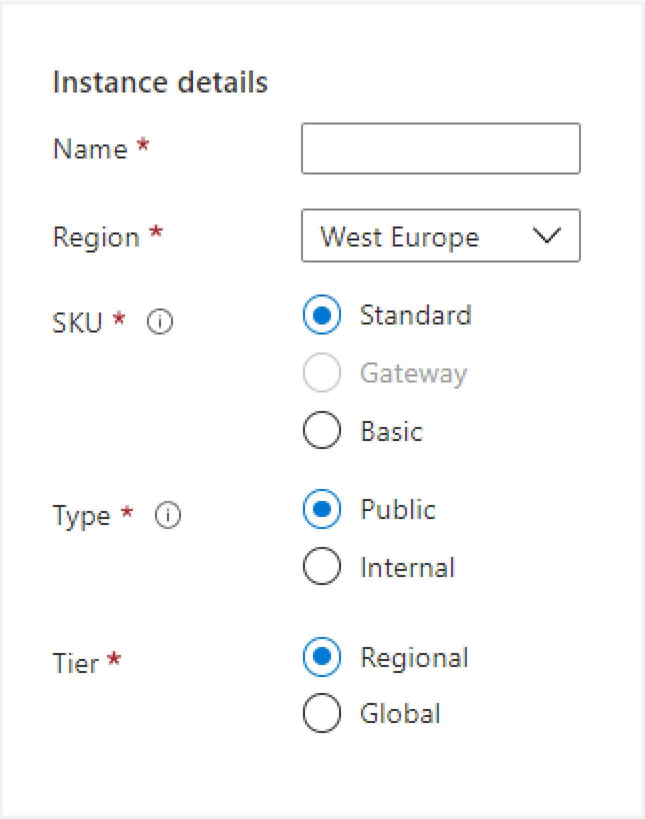
Azure Load balancer and availability zones




Zonal
Zone 1
Zonal Standard Load Balancer 1
Zone 2
Zonal Standard Load Balancer 2
Zone 3
Zonal Standard Load Balancer 3
Subnet 1
Subnet 2
Subnet 3
Virtual Network

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%

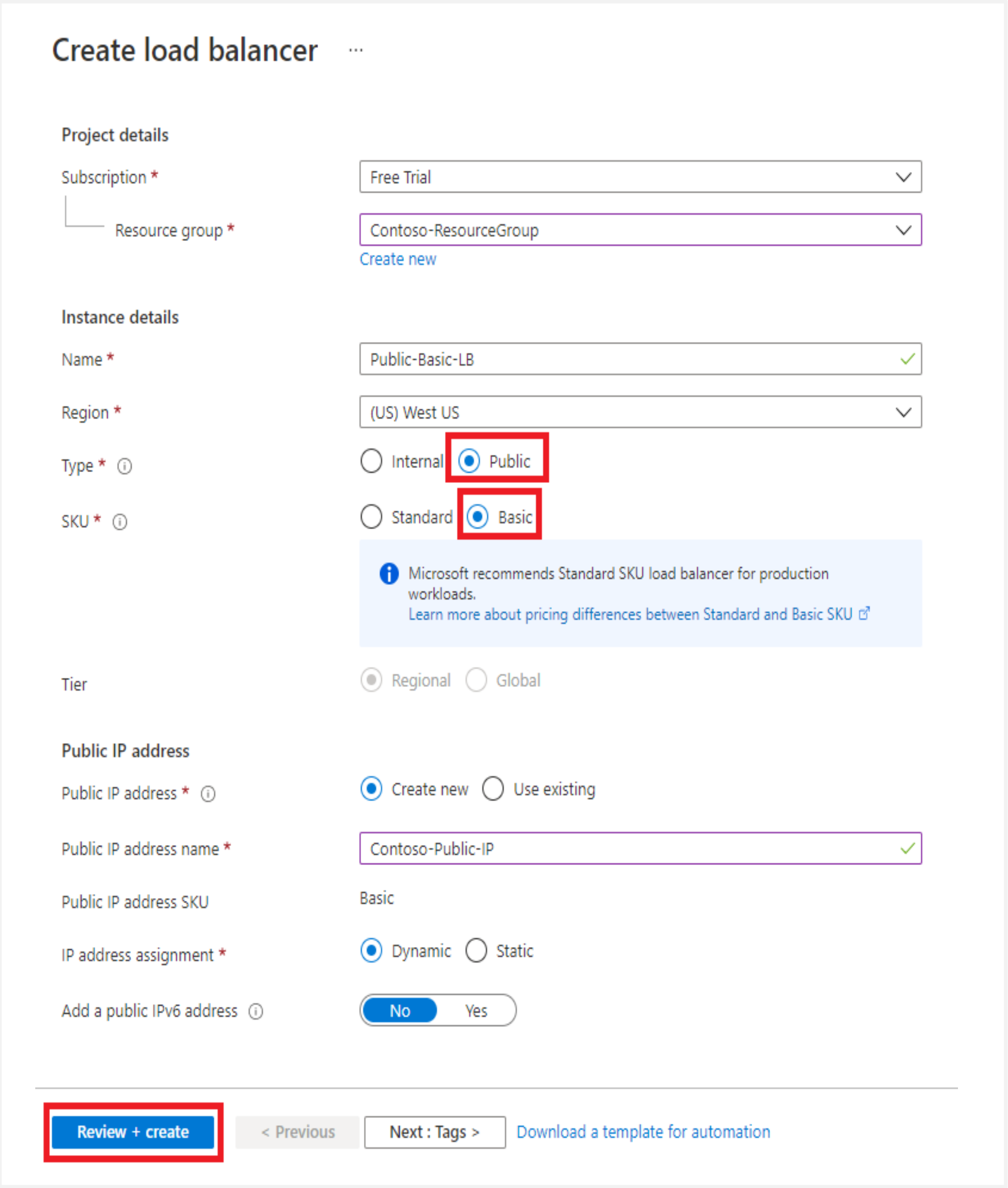


Instance details

Name *	
Region *	West Europe
SKU * ⓘ	● Standard ○ Gateway ○ Basic
Type * ⓘ	● Public ○ Internal
Tier *	● Regional ○ Global

Create Load balancer in the Azure portal

- Subscription
- Name
- Region
- Type
- SKU
- Tier



Create load balancer ···

Project details

Subscription *: Free Trial

Resource group *: Contoso-ResourceGroup

Create new

Instance details

Name *: Public-Basic-LB ✓

Region *: (US) West US

Type * ⓘ: ○ Internal ● Public

SKU * ⓘ: ○ Standard ● Basic

ⓘ Microsoft recommends Standard SKU load balancer for production workloads.
Learn more about pricing differences between Standard and Basic SKU

Tier: ● Regional ○ Global

Public IP address

Public IP address * ⓘ: ● Create new ○ Use existing

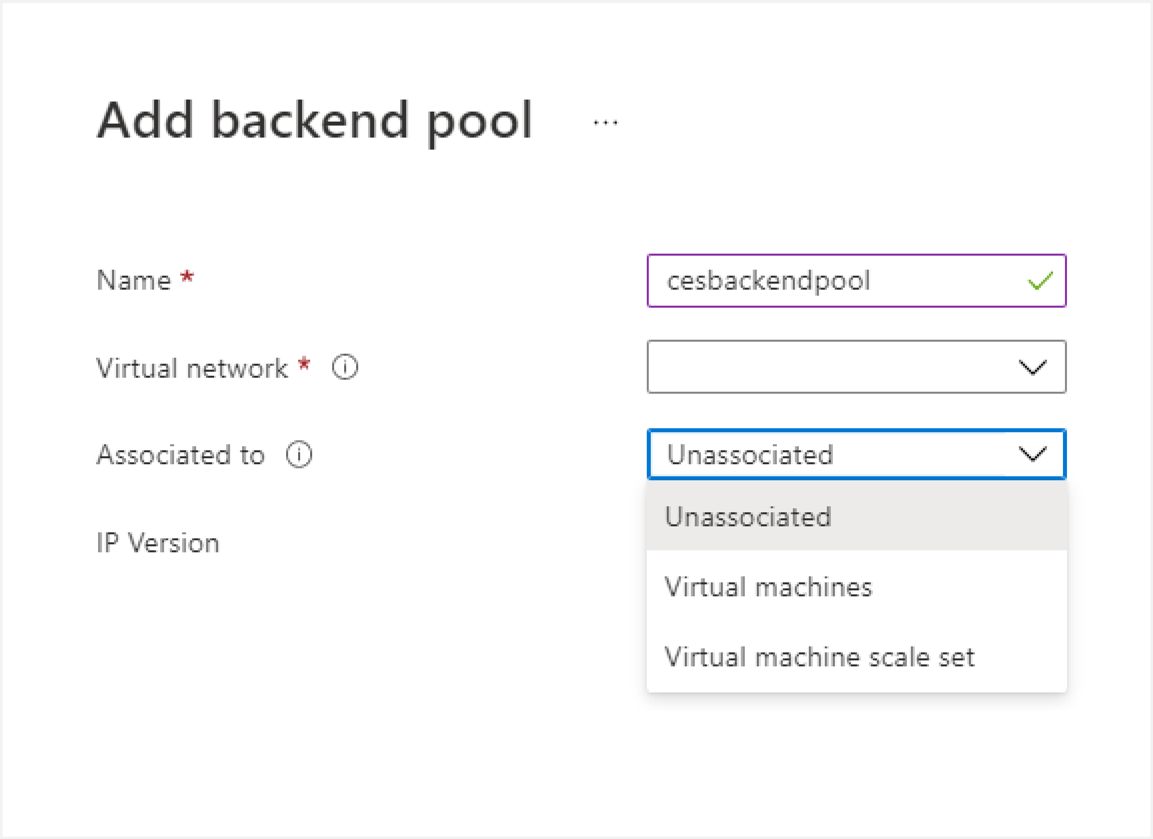
Public IP address name *: Contoso-Public-IP ✓

Public IP address SKU: Basic

IP address assignment *: ● Dynamic ○ Static

Add a public IPv6 address ⓘ: [✓ No] Yes

Create Backend Pools



Add backend pool ...

Name * cesbackendpool

Virtual network *

Associated to Unassociated

IP Version

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

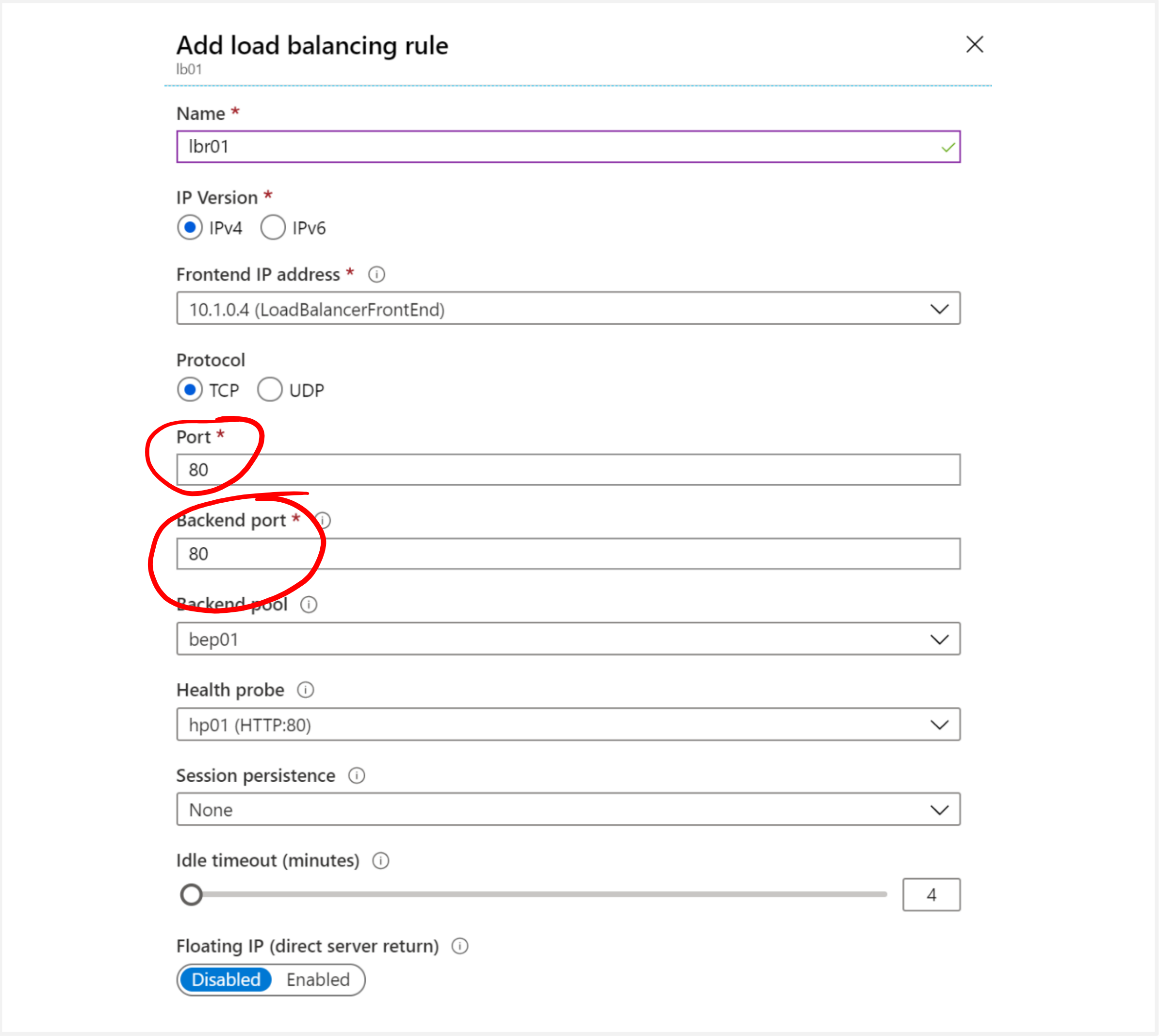
To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer

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



Add load balancing rule
lb01

Name * lbr01

IP Version * ● IPv4 ○ IPv6

Frontend IP address * 10.1.0.4 (LoadBalancerFrontEnd)

Protocol ● TCP ○ UDP

Port * 80

Backend port * 80

Backend pool bep01

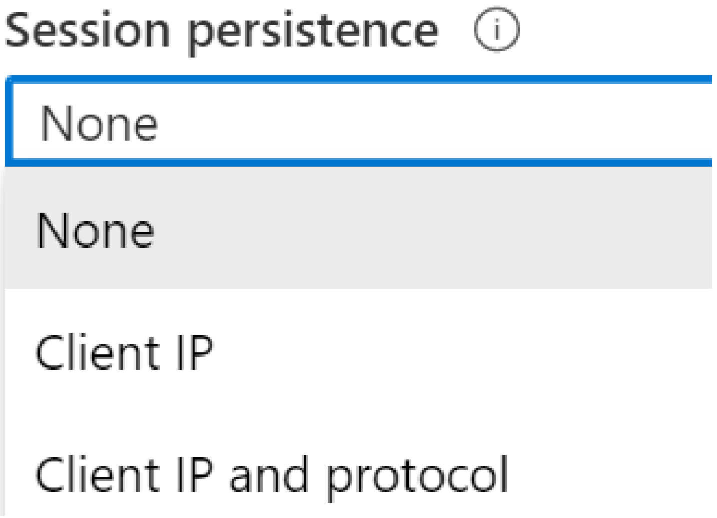
Health probe hp01 (HTTP:80)

Session persistence None

Idle timeout (minutes) 4

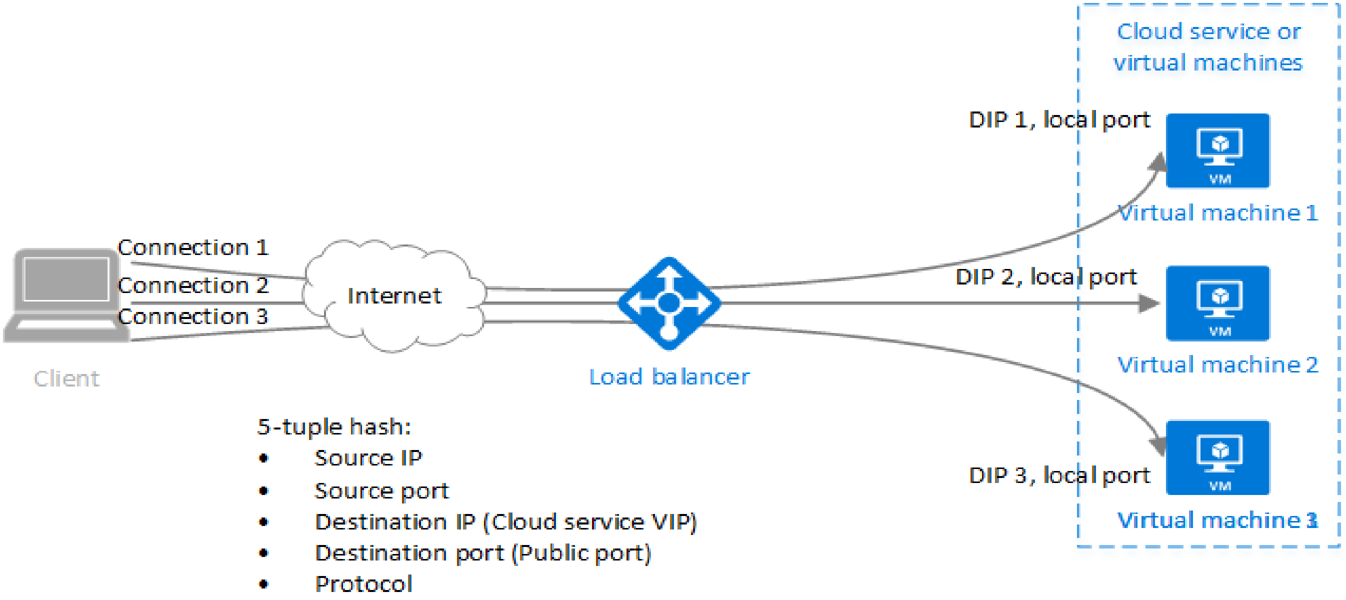
Floating IP (direct server return) [✓ Disabled] Enabled

Configure Session Persistence



Session persistence ⓘ

None



5-tuple hash:

- Source IP
- Source port
- Destination IP (Cloud service VIP)
- Destination port (Public port)
- 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

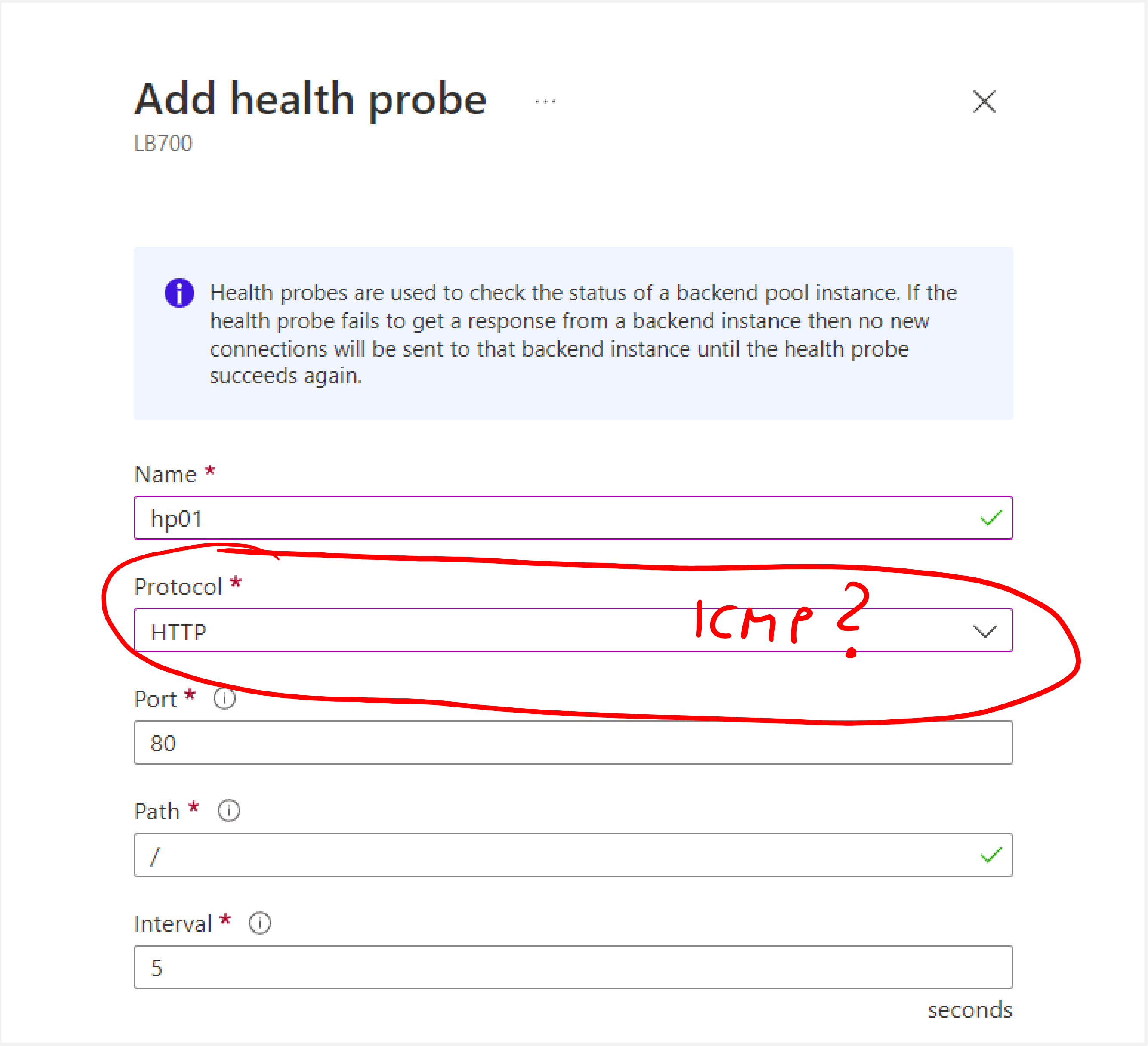
Create Health Probes

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



Add health probe

LB700

Health probes are used to check the status of a backend pool instance. If the health probe fails to get a response from a backend instance then no new connections will be sent to that backend instance until the health probe succeeds again.

Name * hp01

Protocol * HTTP

ICMP ?

Port * 80

Path * /

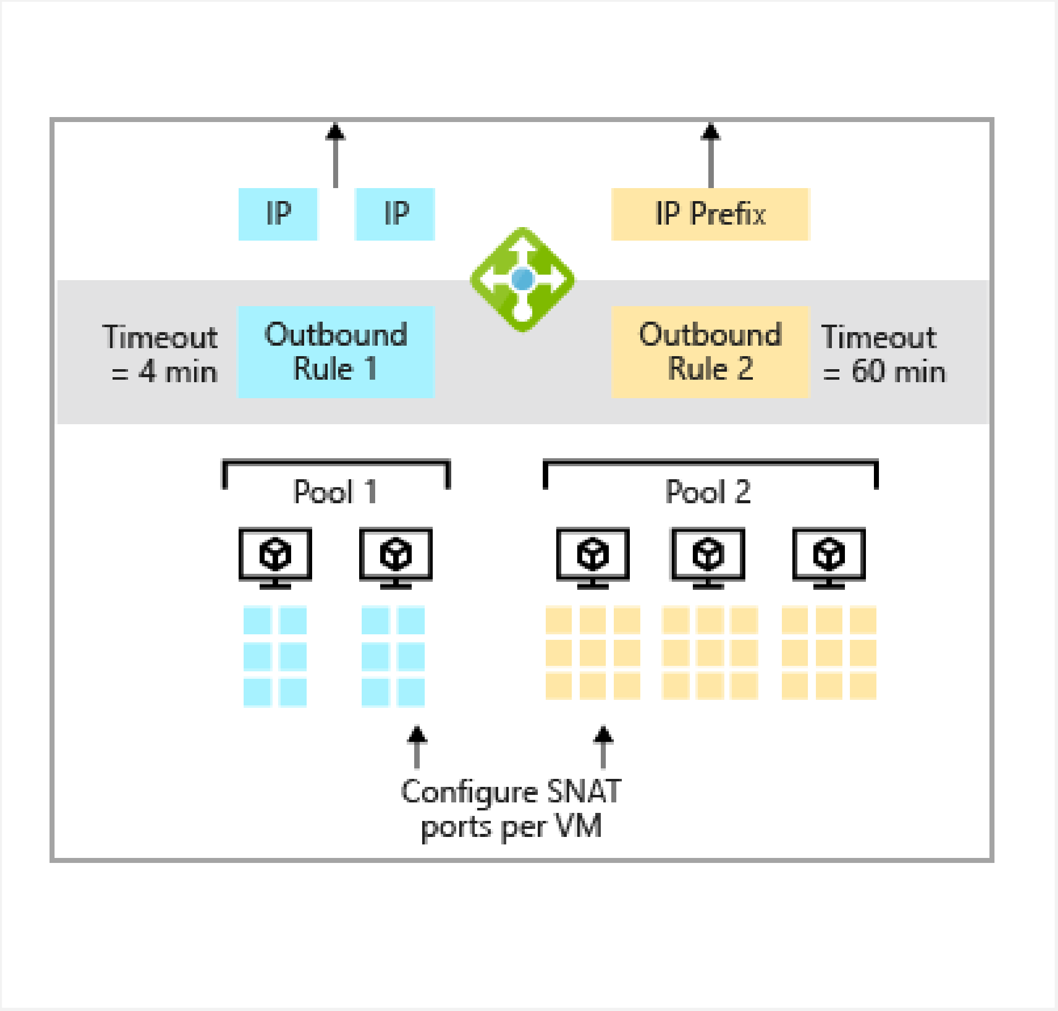
Interval * 5 seconds

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.



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

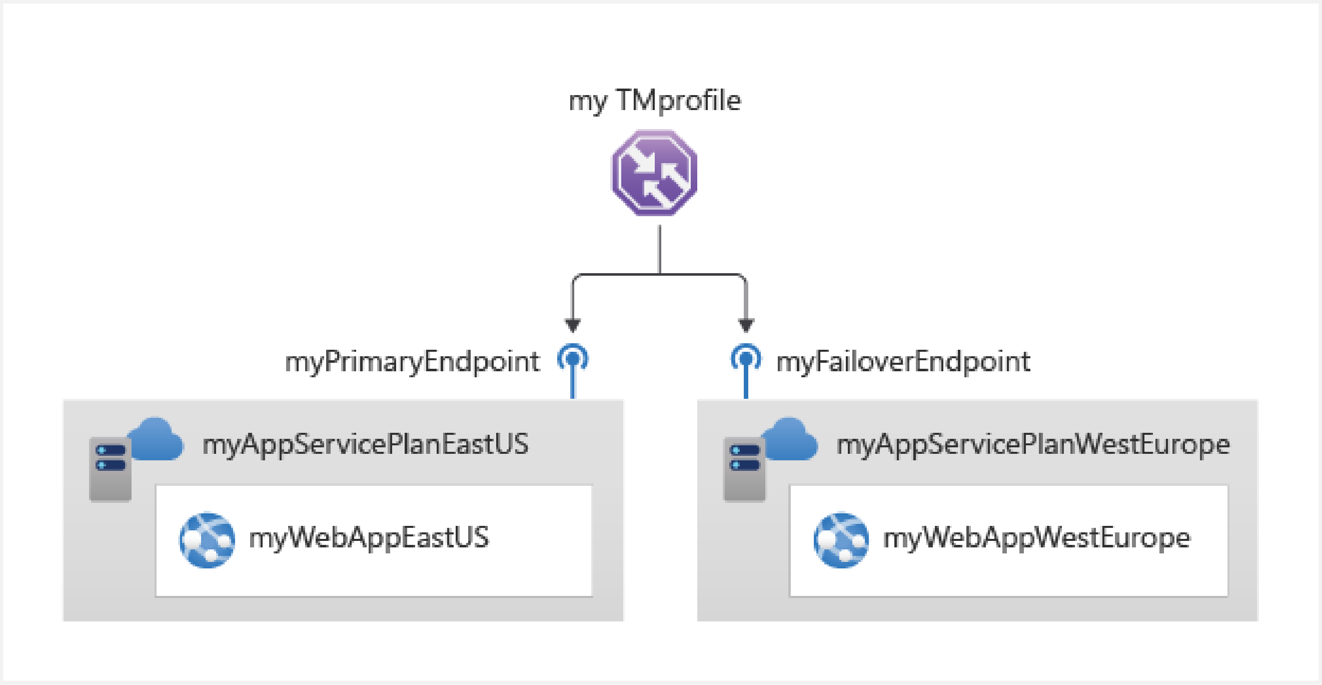
Increase application availability

Improve application performance

Service maintenance without downtime

Combine hybrid applications

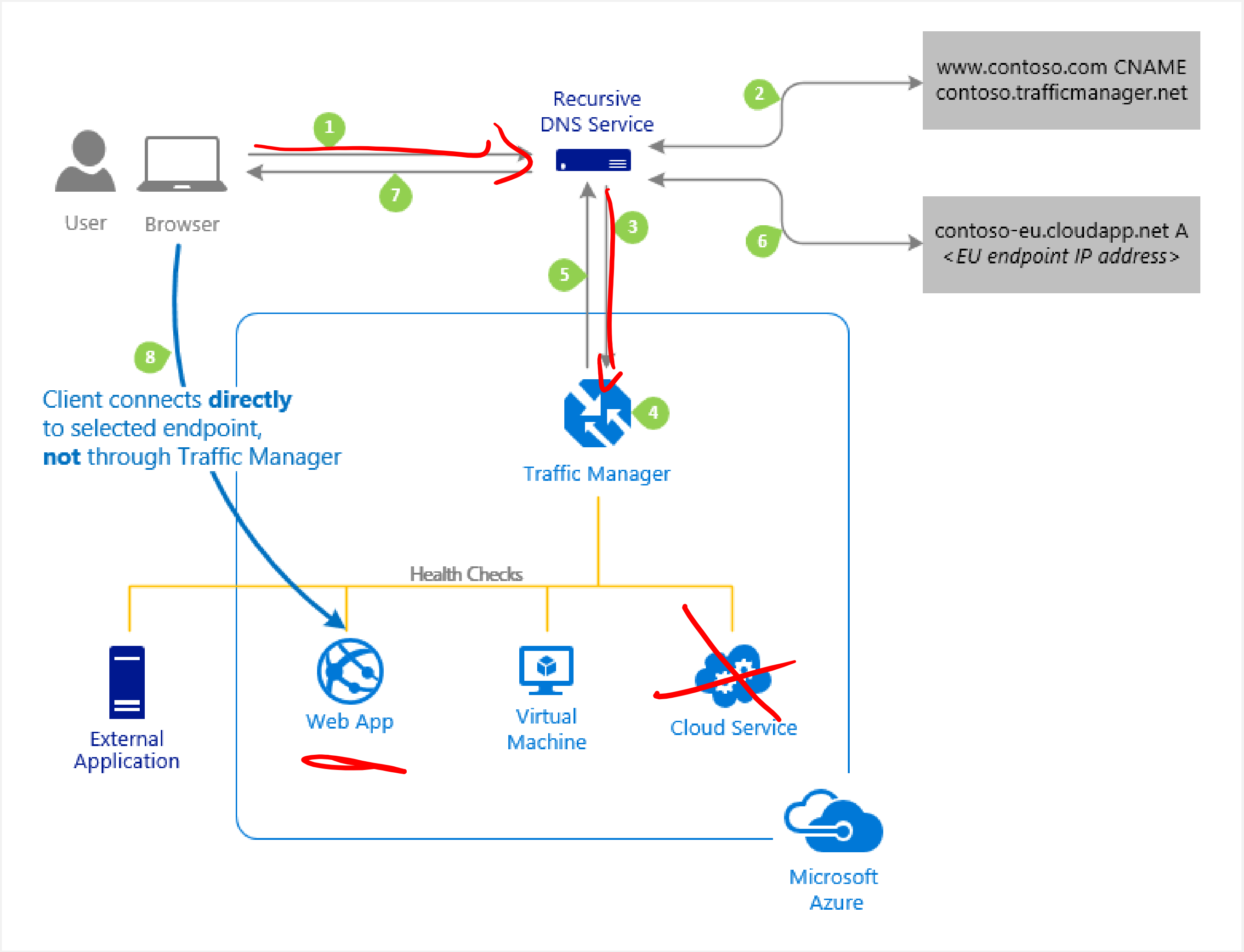
Distribute traffic for complex deployments



How Traffic manager works

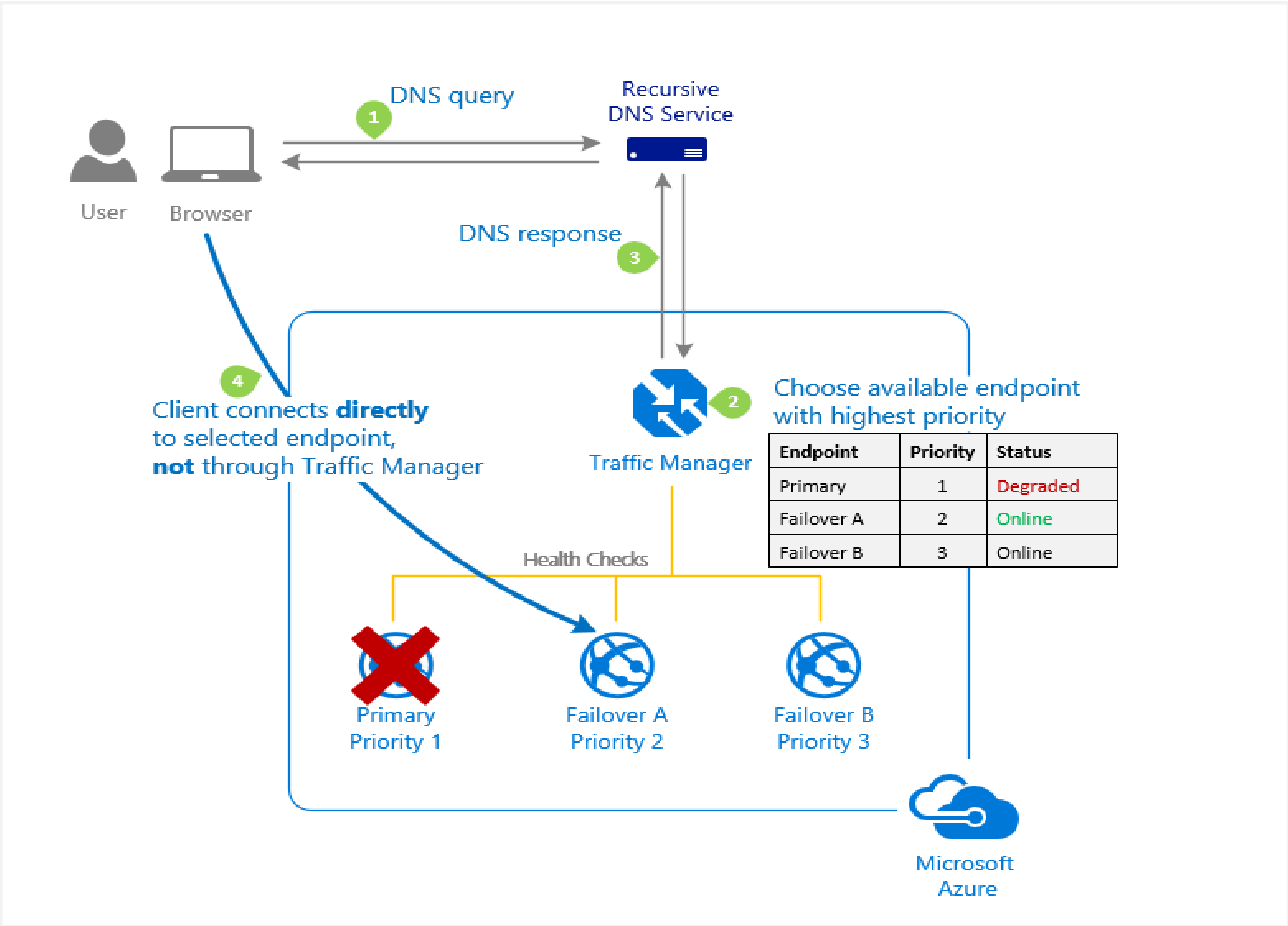
The Traffic Manager name servers receive the request. They choose an endpoint based on:

- 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



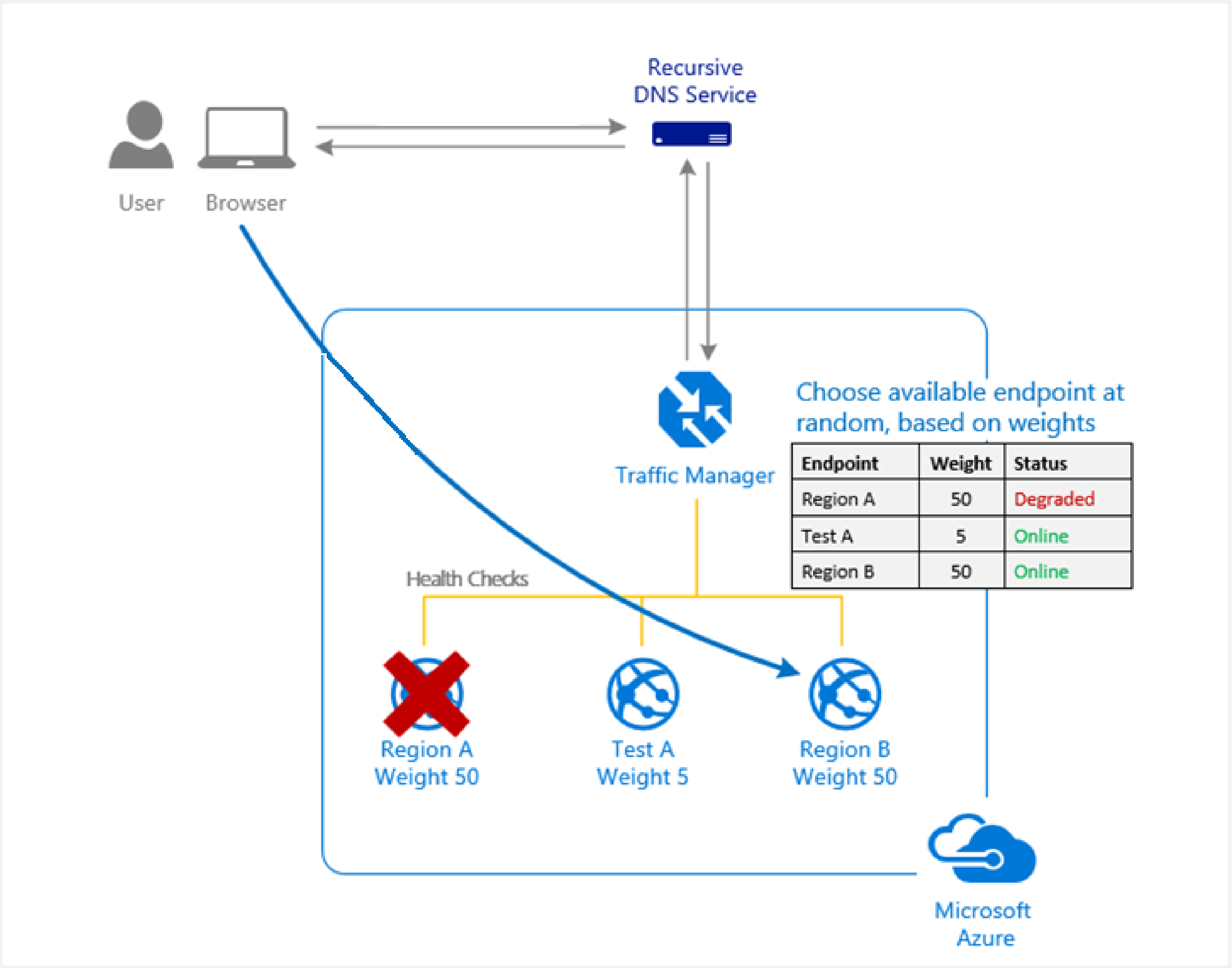
Recursive DNS Service
www.contoso.com CNAME contoso.trafficmanager.net
contoso-eu.cloudapp.net A <EU endpoint IP address>
User
Browser
1
2
3
4
5
6
7
8
Client connects **directly** to selected endpoint, **not** through Traffic Manager
Traffic Manager
Health Checks
External Application
Web App
Virtual Machine
Cloud Service
Microsoft Azure

Traffic routing methods – Priority



Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online

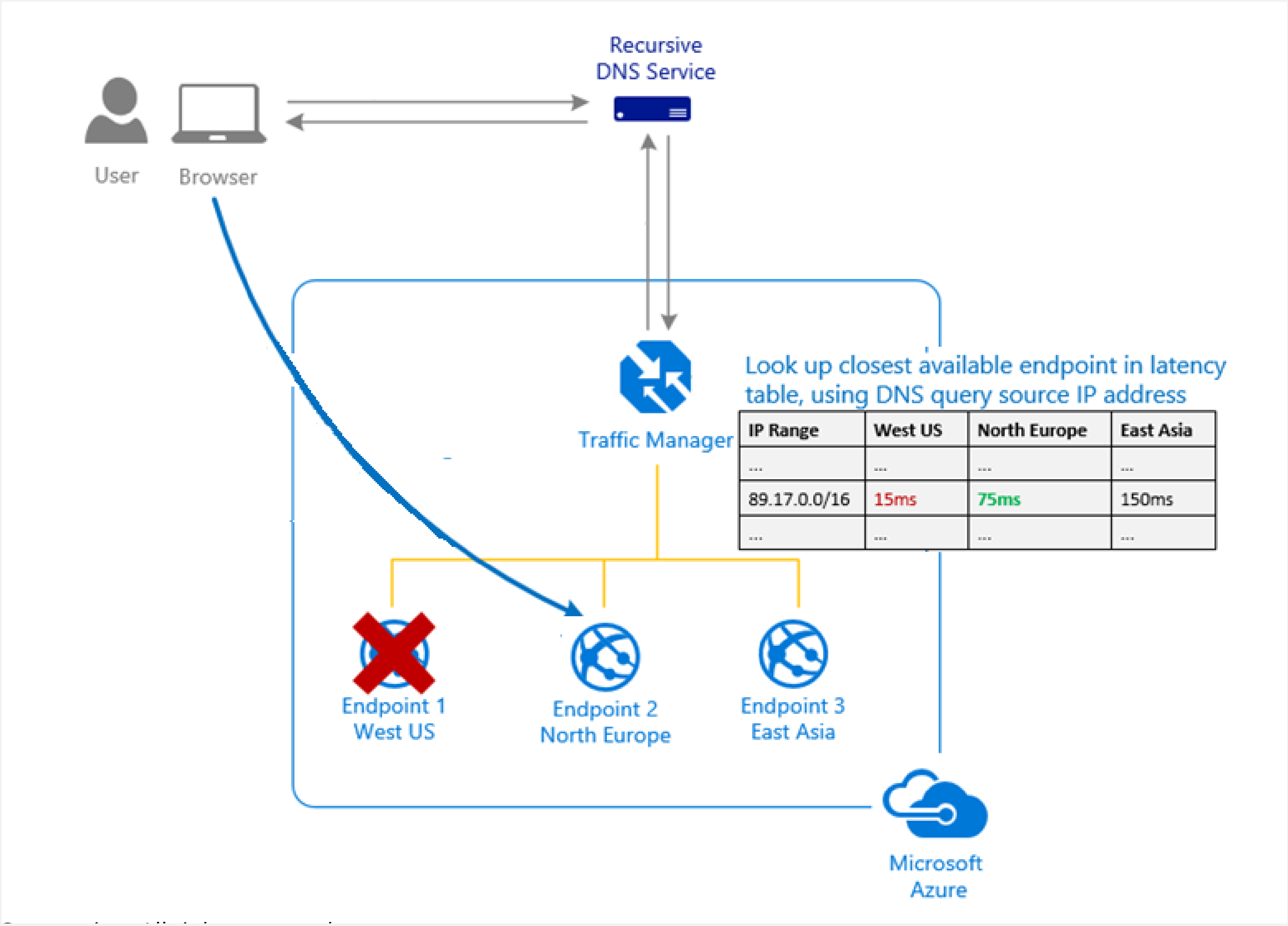
Traffic routing methods – Weighted



Choose available endpoint at random, based on weights

Endpoint	Weight	Status
Region A	50	Degraded
Test A	5	Online
Region B	50	Online

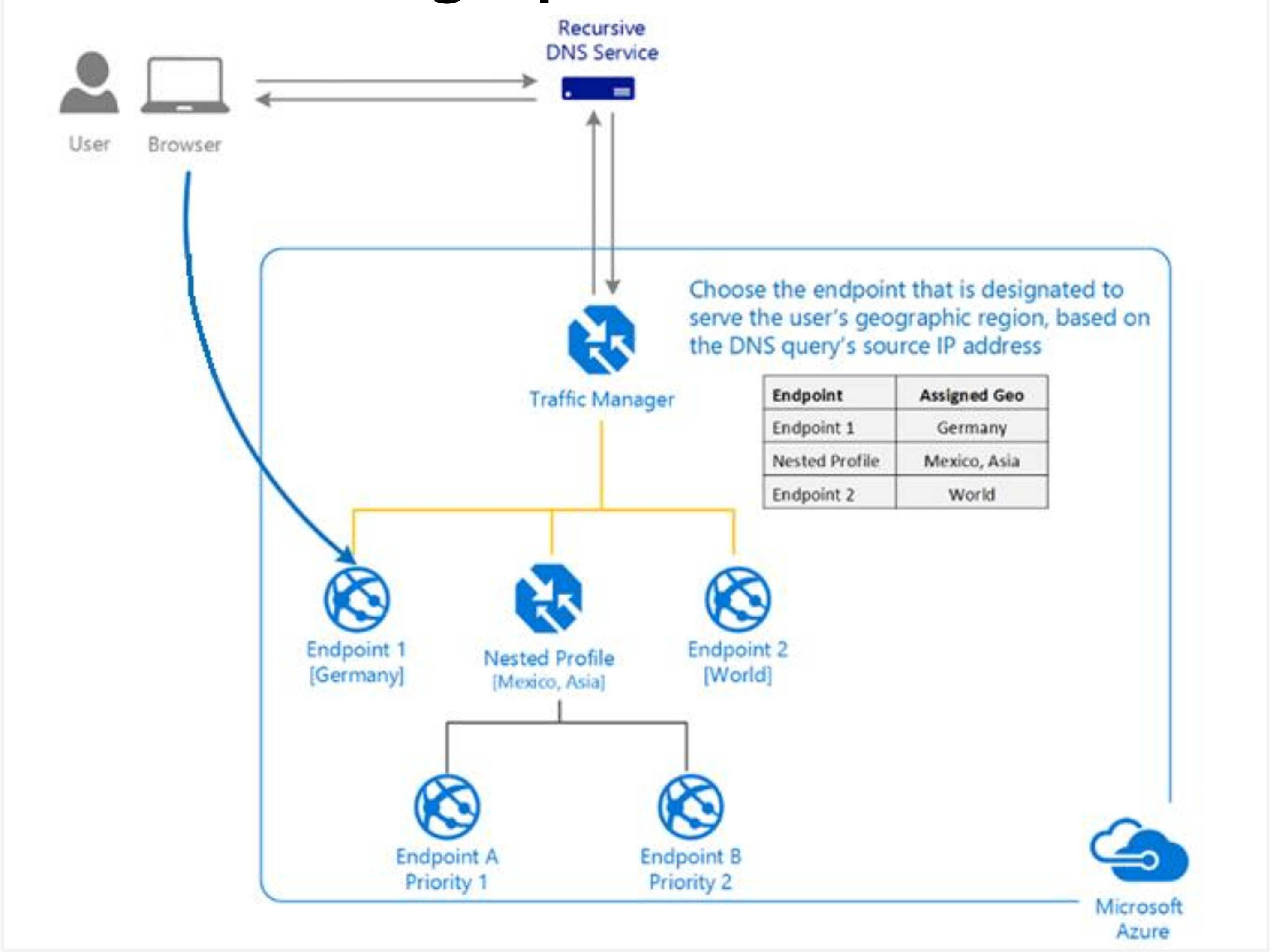
Traffic routing methods – Performance



Look up closest available endpoint in latency table, using DNS query source IP address

IP Range	West US	North Europe	East Asia
...	...	...	...
89.17.0.0/16	15ms	75ms	150ms
...	...	...	...

Traffic routing methods - Geographic



Choose the endpoint that is designated to serve the user's geographic region, based on the DNS query's source IP address

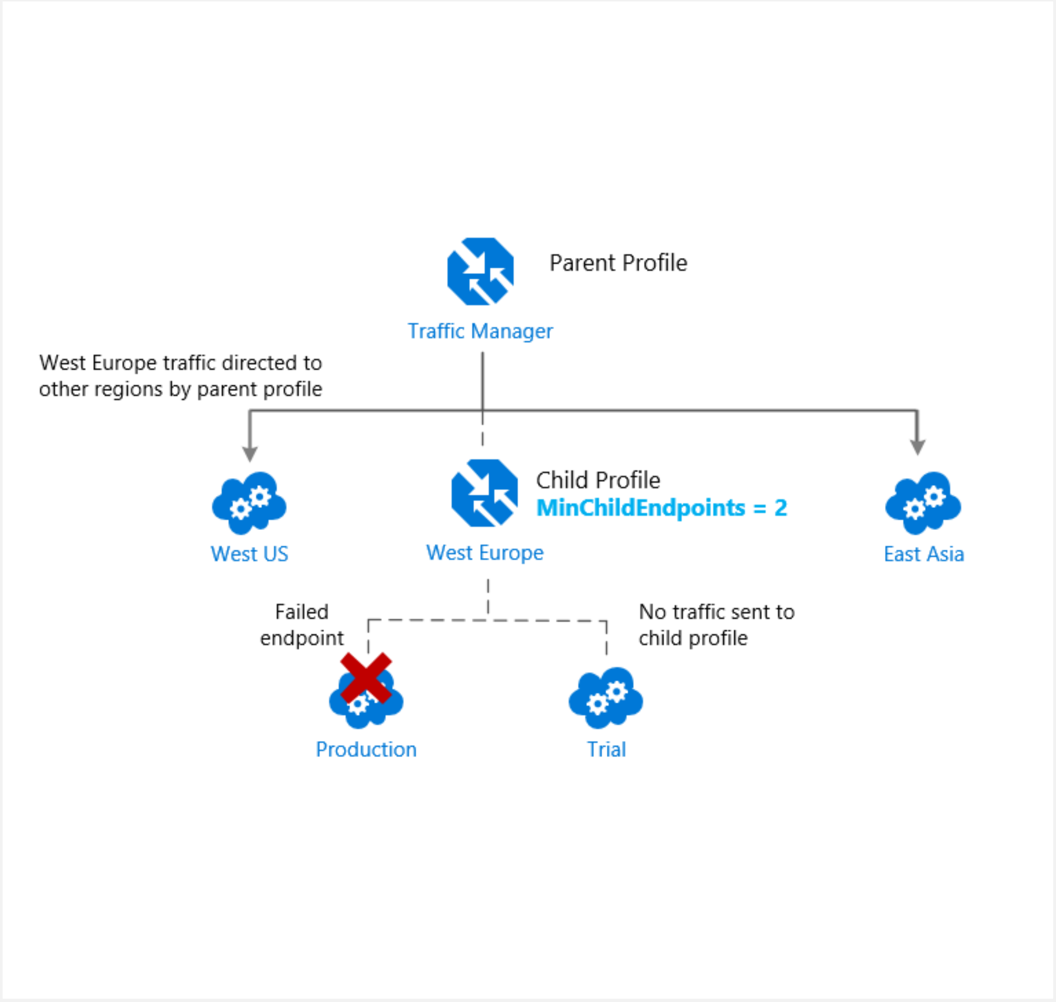
Endpoint	Assigned Geo
Endpoint 1	Germany
Nested Profile	Mexico, Asia
Endpoint 2	World

Traffic manager endpoints

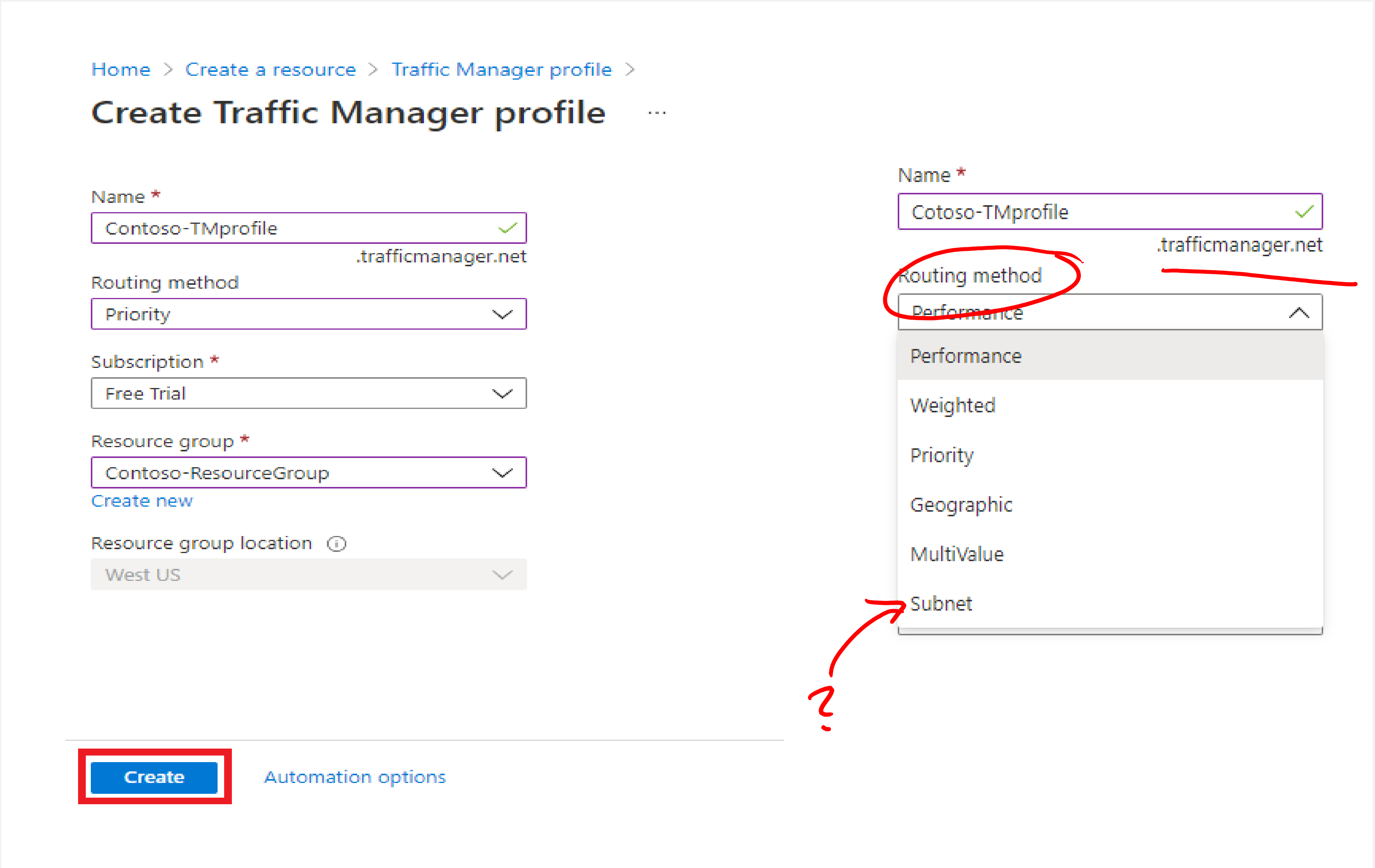
Azure endpoints – load balance traffic to a cloud service, web app, or public IP address in the same subscription within Azure.

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



Home > Create a resource > Traffic Manager profile >

Create Traffic Manager profile ...

Name * Contoso-TMprofile .trafficmanager.net

Routing method Priority

Subscription * Free Trial

Resource group * Contoso-ResourceGroup

Create new

Resource group location West US

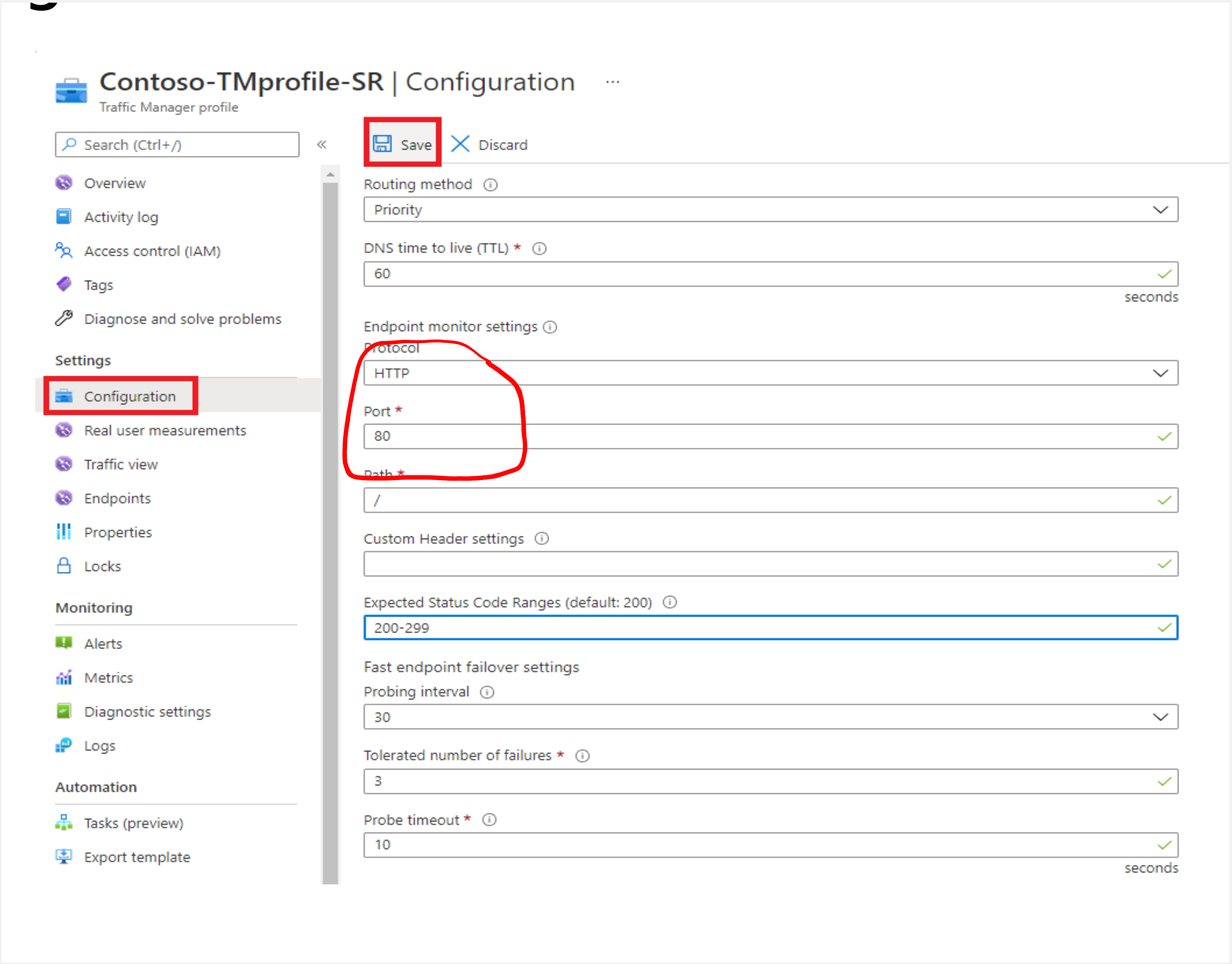
Name * Cotoso-TMprofile .trafficmanager.net

Routing method Performance

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

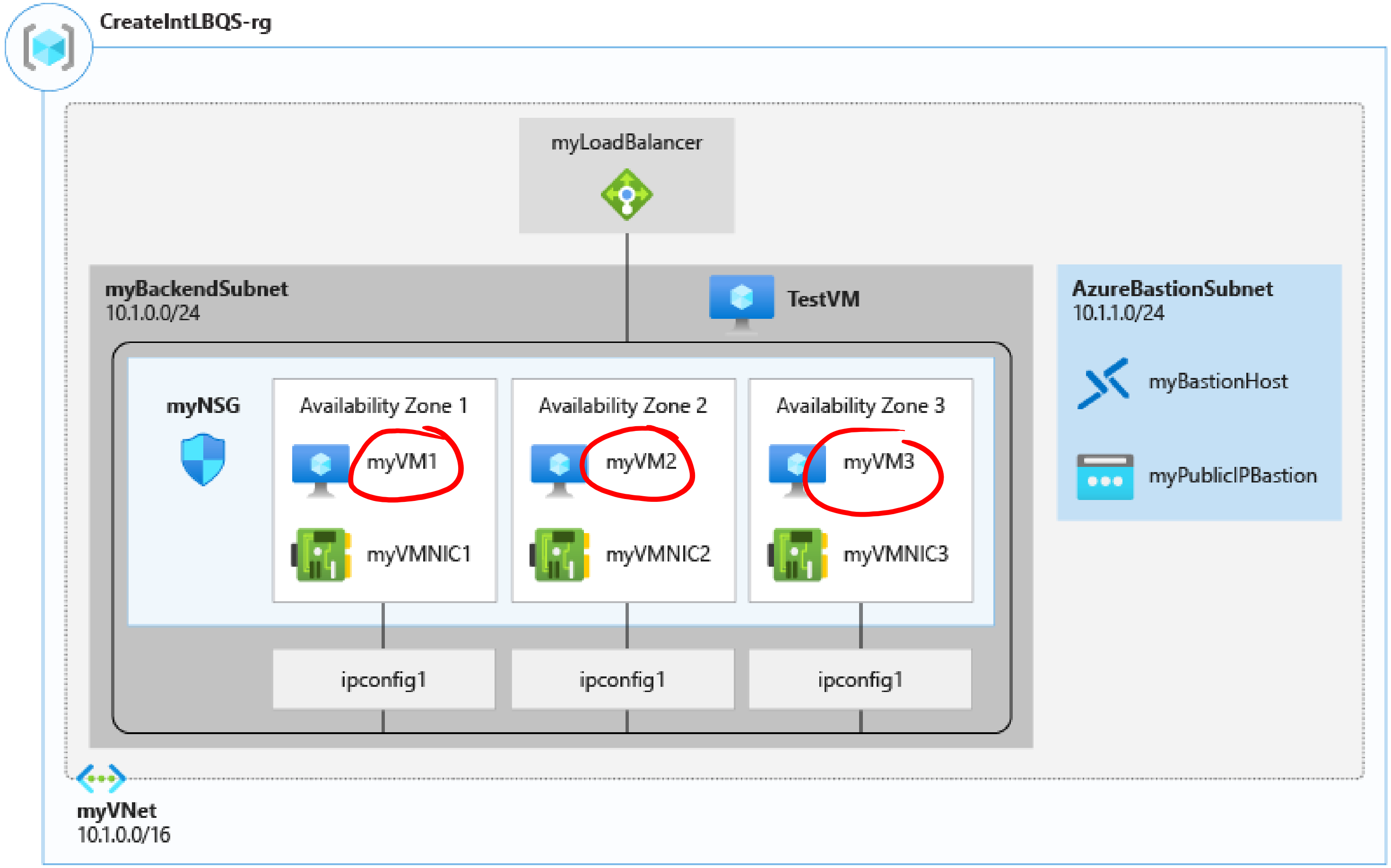


Routing method: Priority
DNS time to live (TTL) *: 60 seconds
Endpoint monitor settings
Protocol: HTTP
Port *: 80
Path *: /
Custom Header settings:
Expected Status Code Ranges (default: 200): 200-299
Fast endpoint failover settings
Probing interval: 30
Tolerated number of failures *: 3
Probe timeout *: 10 seconds

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

Exercise - Create and configure an Azure load balancer

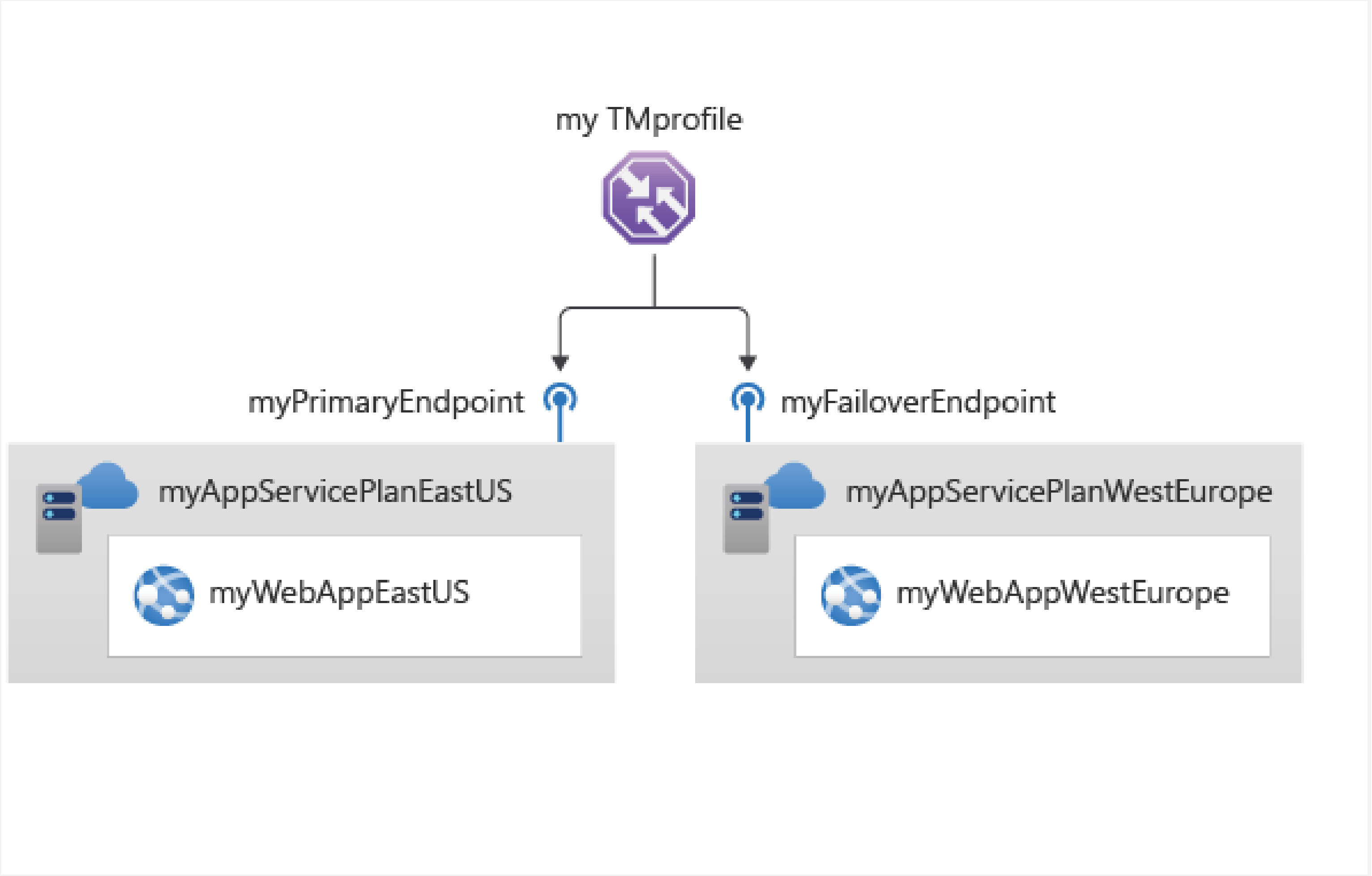
Task 1: Create the virtual network
Task 2: Create the load balancer
Task 3: Create load balancer resources
Task 4: Create backend servers
Task 5: Test the load balancer



Exercise – Create 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