

AZ-700

Module 04

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

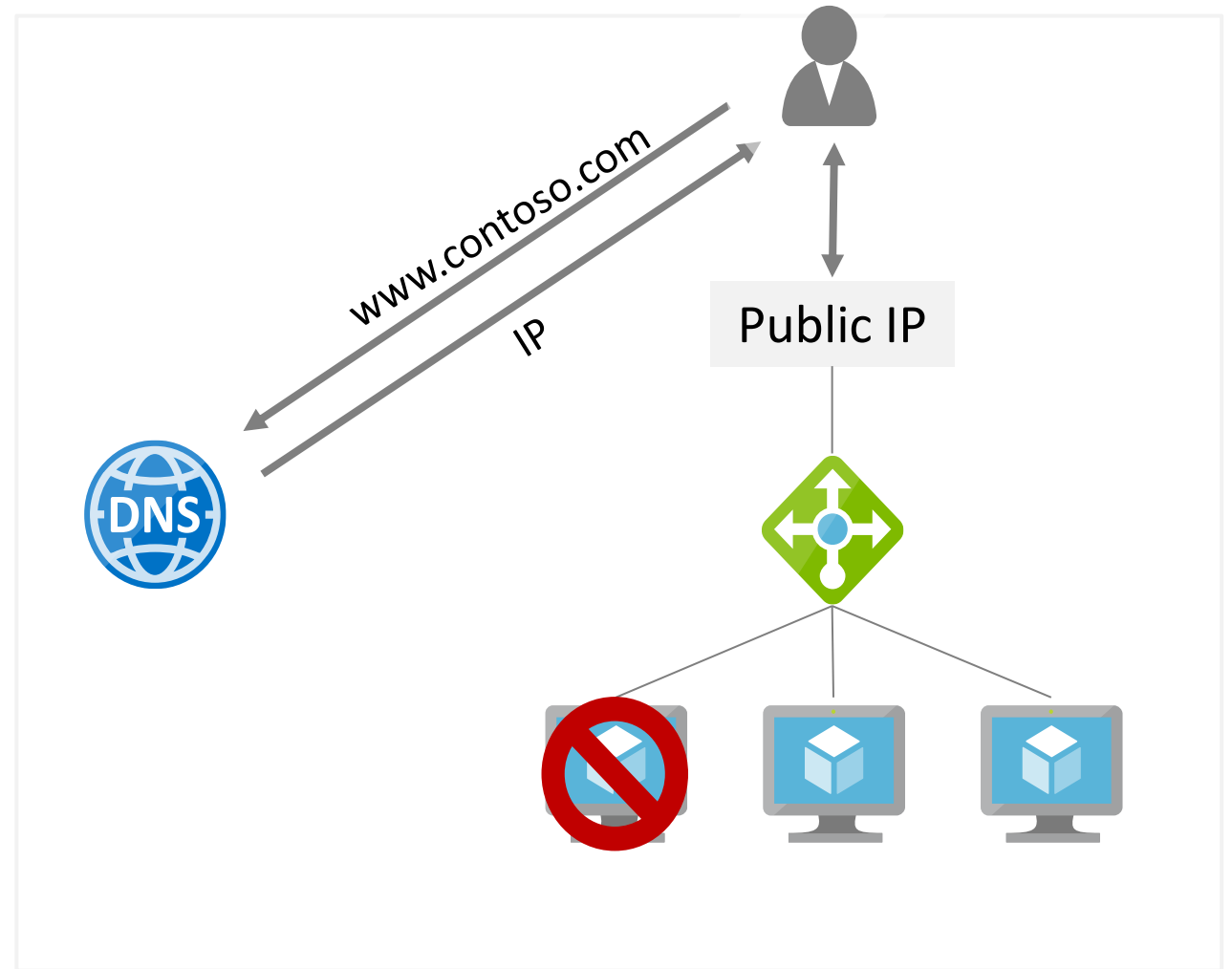
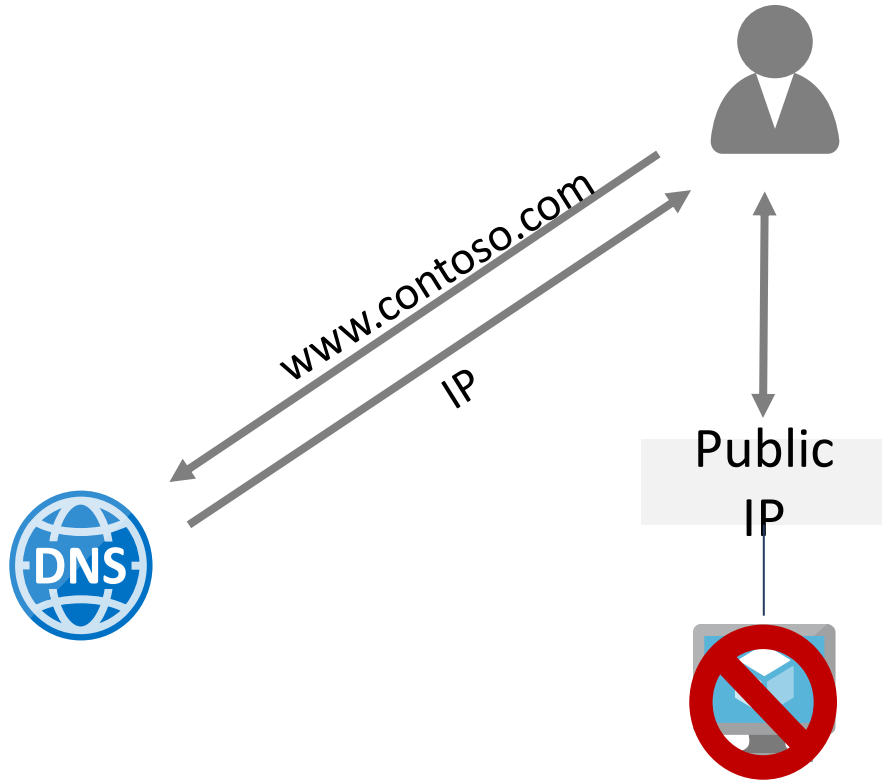
Module Overview

- Explore load balancing options in the Azure portal
- Design and implement Azure Load Balancer using the Azure portal
- 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



Application Gateway

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

Create

▼ Show more



Front Door

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

Create

▼ Show more



Load Balancer

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

Create

▼ Show more



Traffic Manager

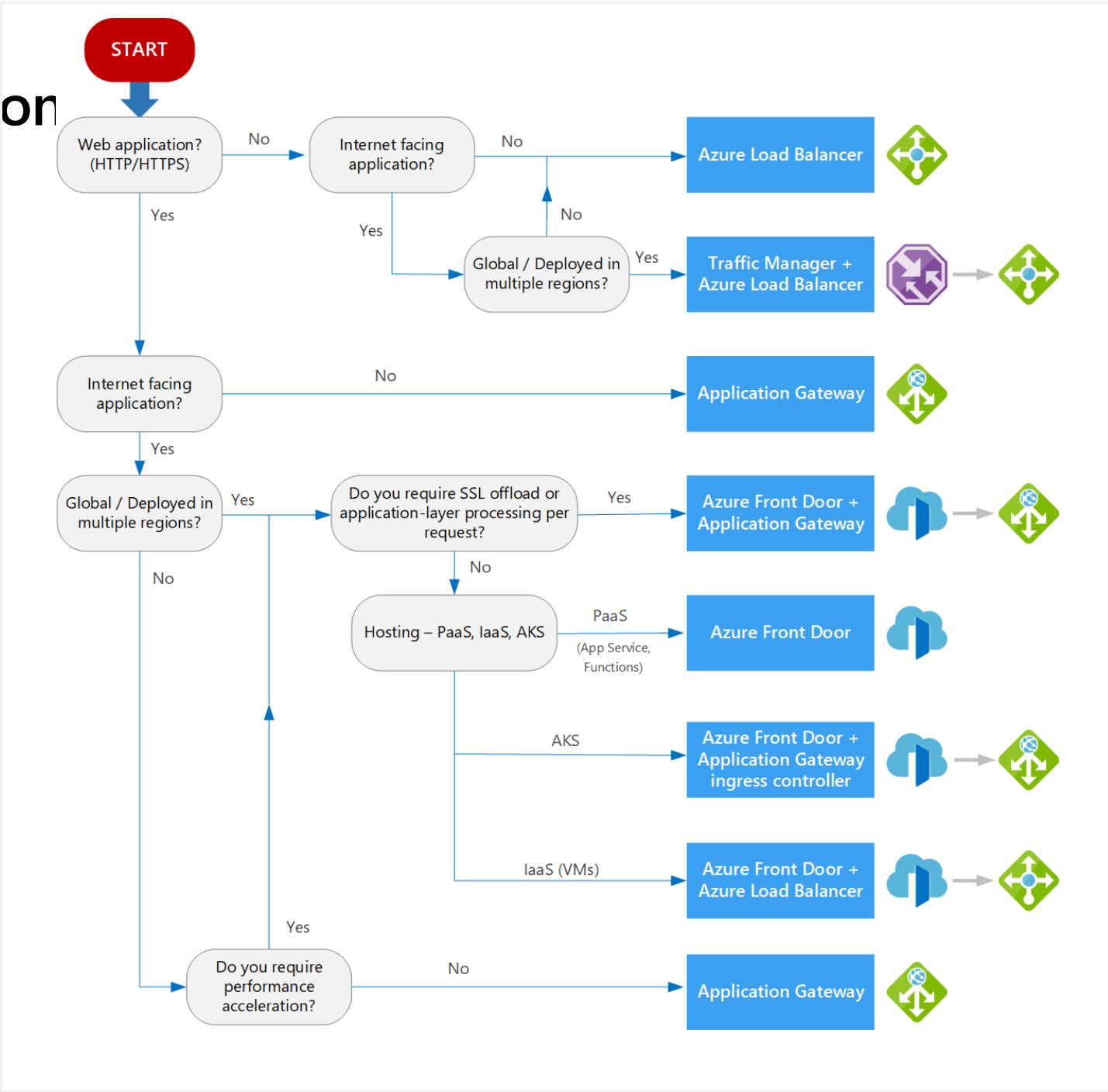
- DNS-based traffic load balancer
- Global across Azure regions
- High availability

Create

▼ Show more

Choosing a load balancing option

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



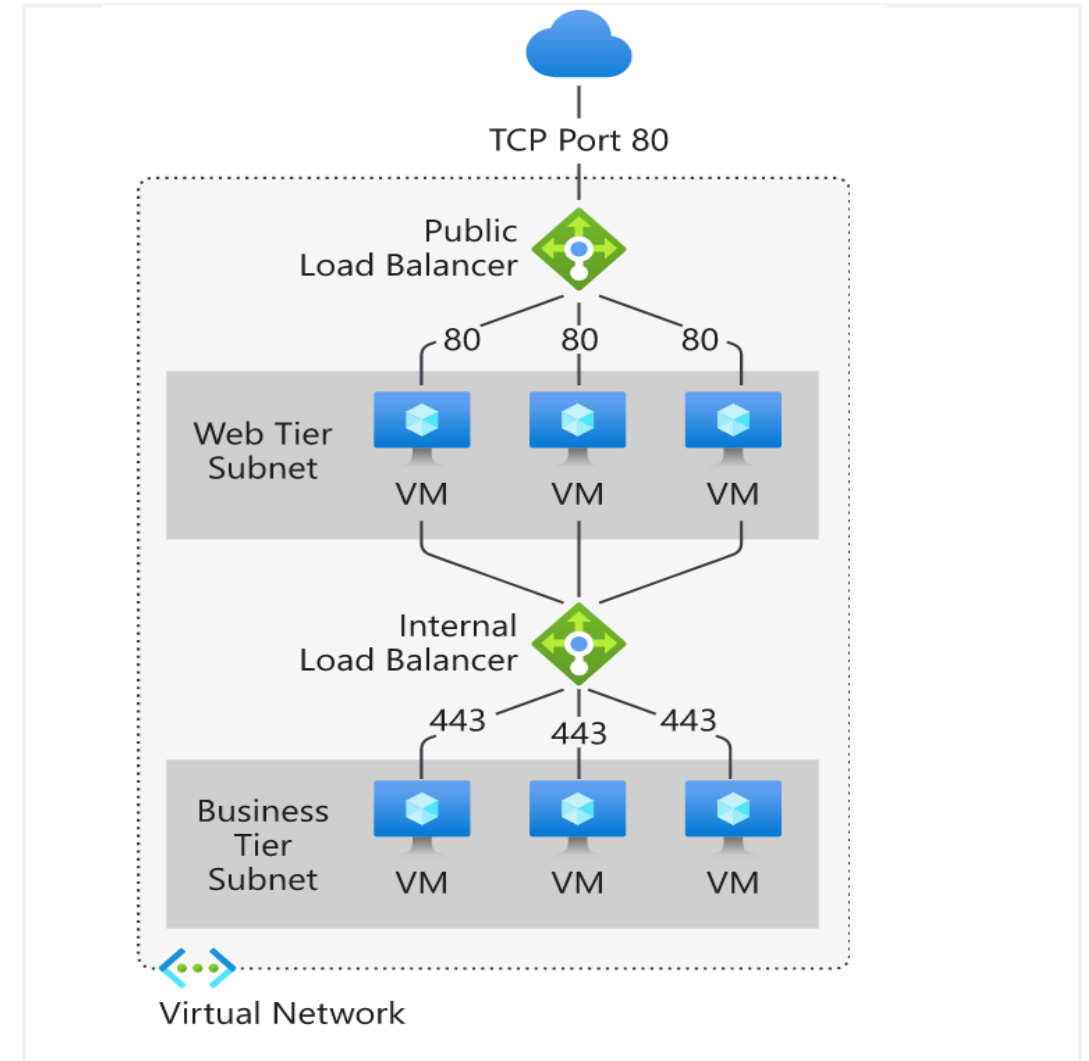
Design and implement Azure Load balancer



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

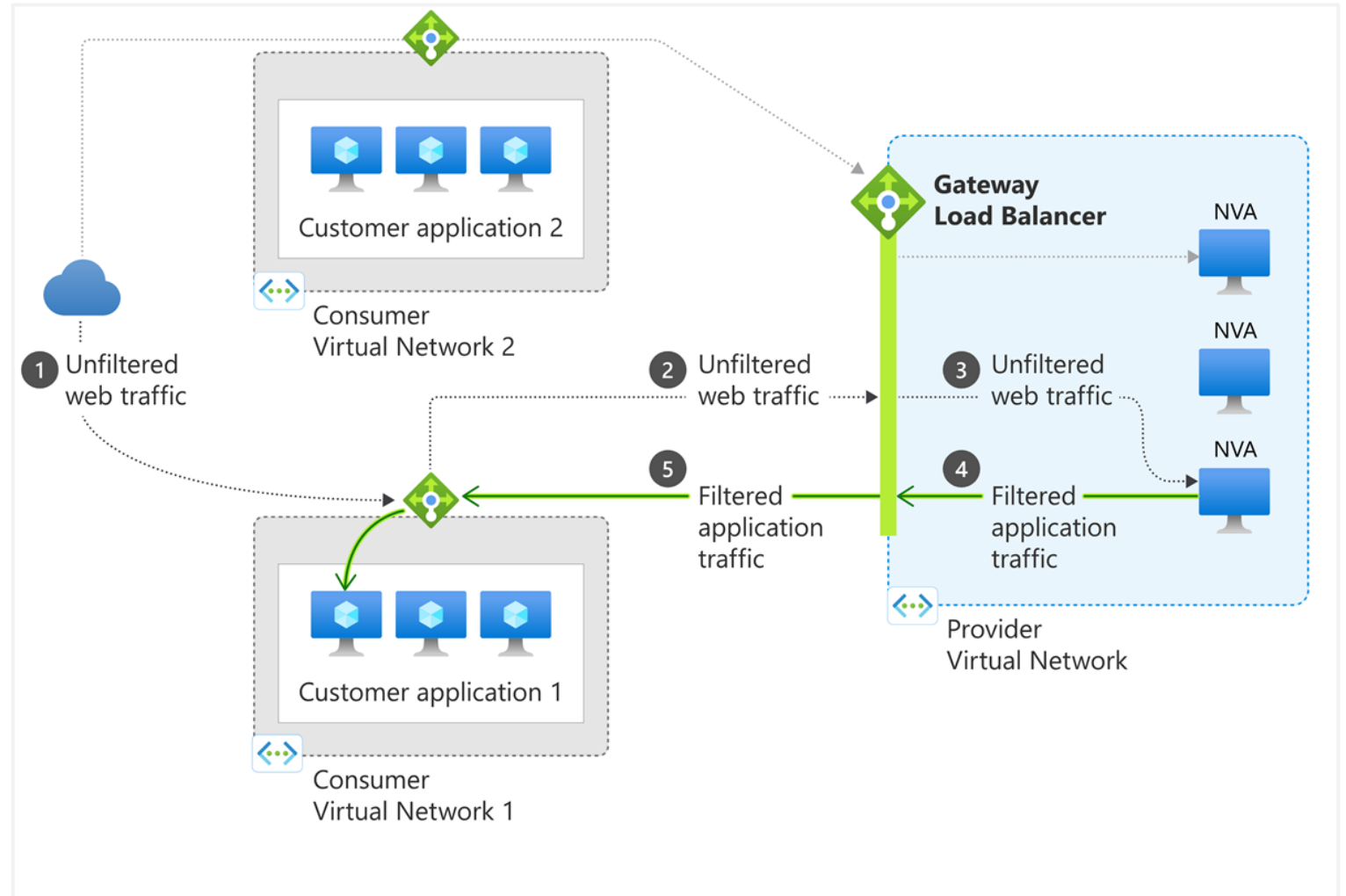


Gateway Load Balancer

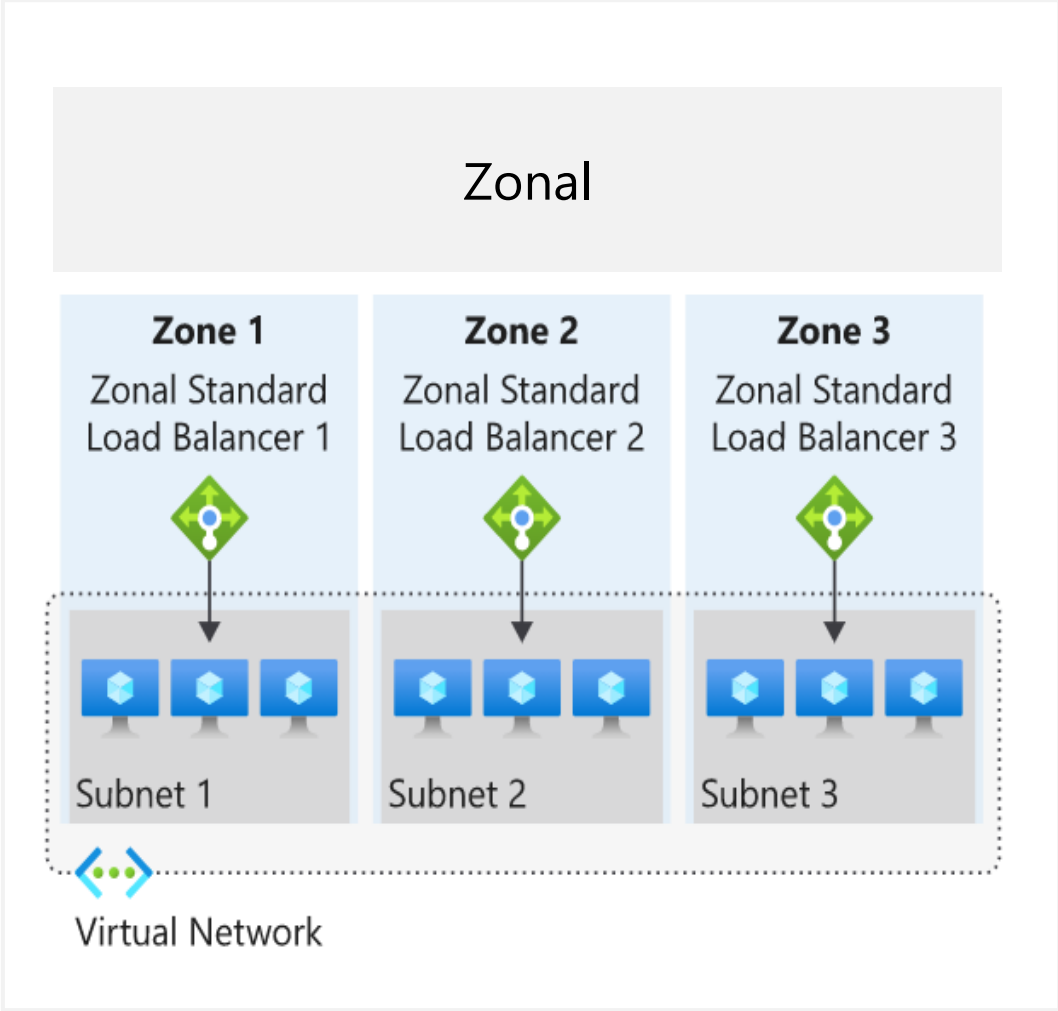
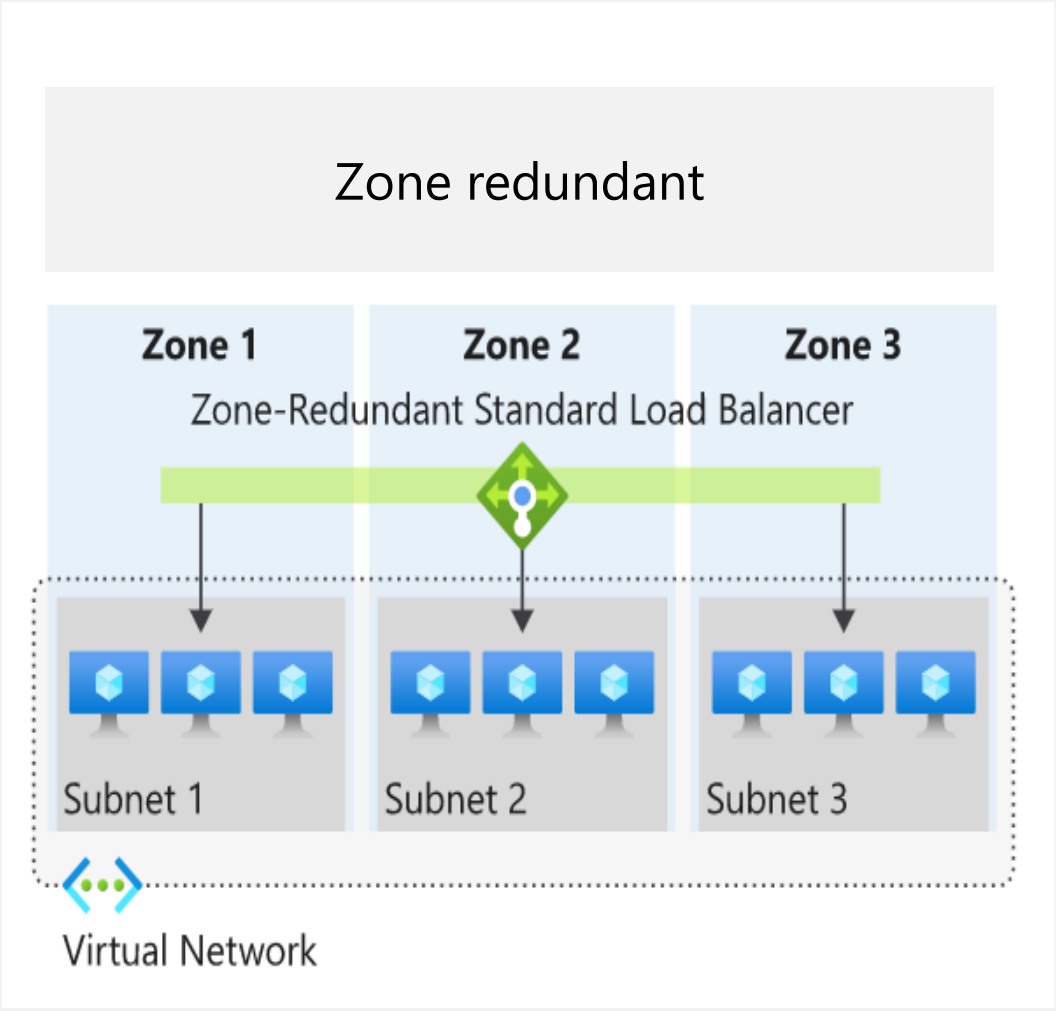
Gateway Load Balancer is a SKU of the Azure Load Balancer portfolio catered for high performance and high availability scenarios with third-party Network Virtual Appliances (NVAs)

Components to configure:

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



Azure Load balancer and availability zones



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

[Review + create](#) [< Previous](#) [Next : Tags >](#) [Download a template for automation](#)

Create Backend Pools

Add backend pool

Name *

cesbackendpool

Virtual network * ⓘ

Associated to ⓘ

Unassociated

Unassociated

Virtual machines

Virtual machine scale set

IP Version

| 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

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) ⓘ

0

4

Floating IP (direct server return) ⓘ

Disabled Enabled

Configure Session Persistence

Session persistence ⓘ

None

None

Client IP

Client IP and protocol

The diagram illustrates the flow of traffic from a Client to a Load balancer and then to three Virtual machines (VMs) within a Cloud service or virtual machines pool. The Client sends three connections (Connection 1, Connection 2, Connection 3) to the Internet. The Load balancer receives these connections and distributes them to the VMs based on session persistence settings. The Load balancer is labeled 'Load balancer' and the pool is labeled 'Cloud service or virtual machines'. The VMs are labeled 'Virtual machine 1', 'Virtual machine 2', and 'Virtual machine 3'. The connections are labeled 'DIP 1, local port', 'DIP 2, local port', and 'DIP 3, local port'.

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

i 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 ▼

Port * ⓘ

80

Path * ⓘ

/ ✓

Interval * ⓘ

5

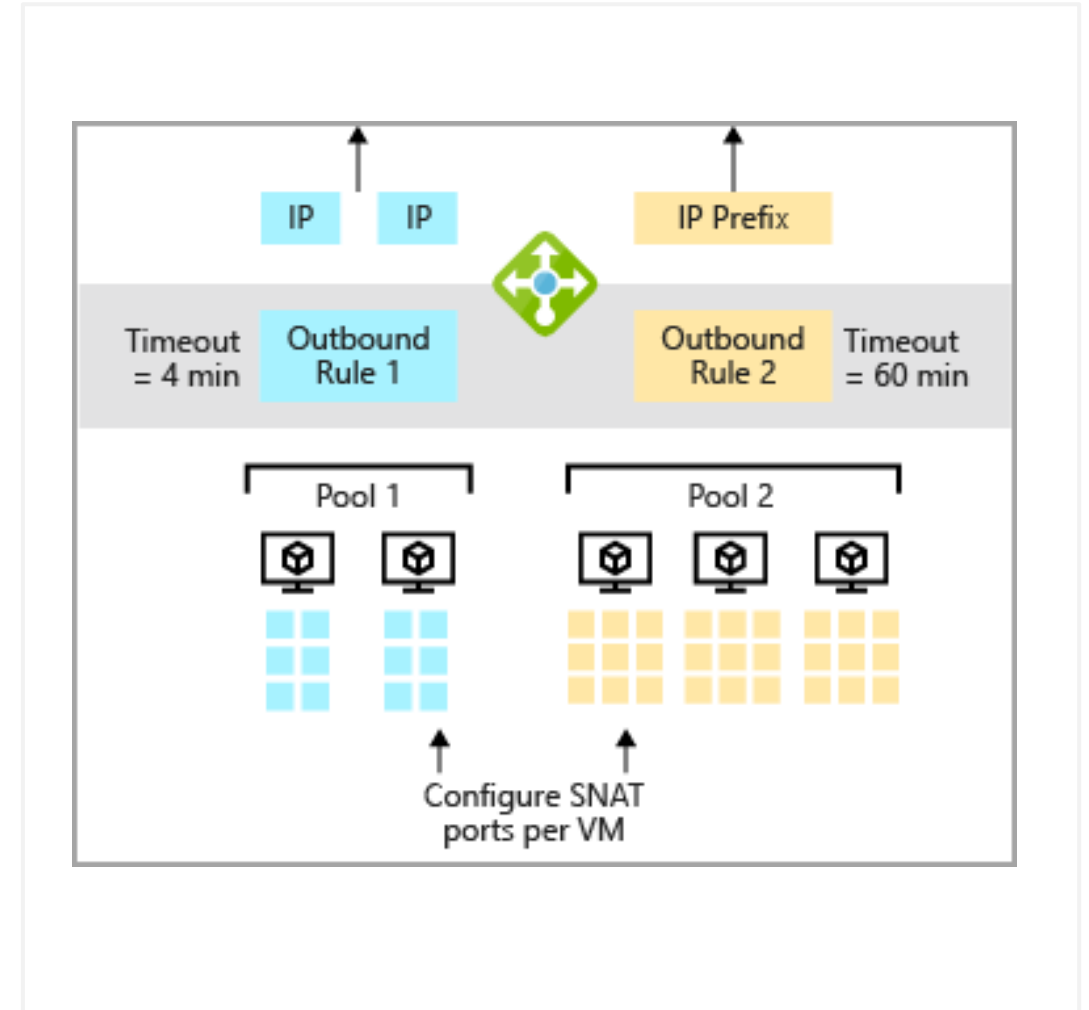
seconds

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

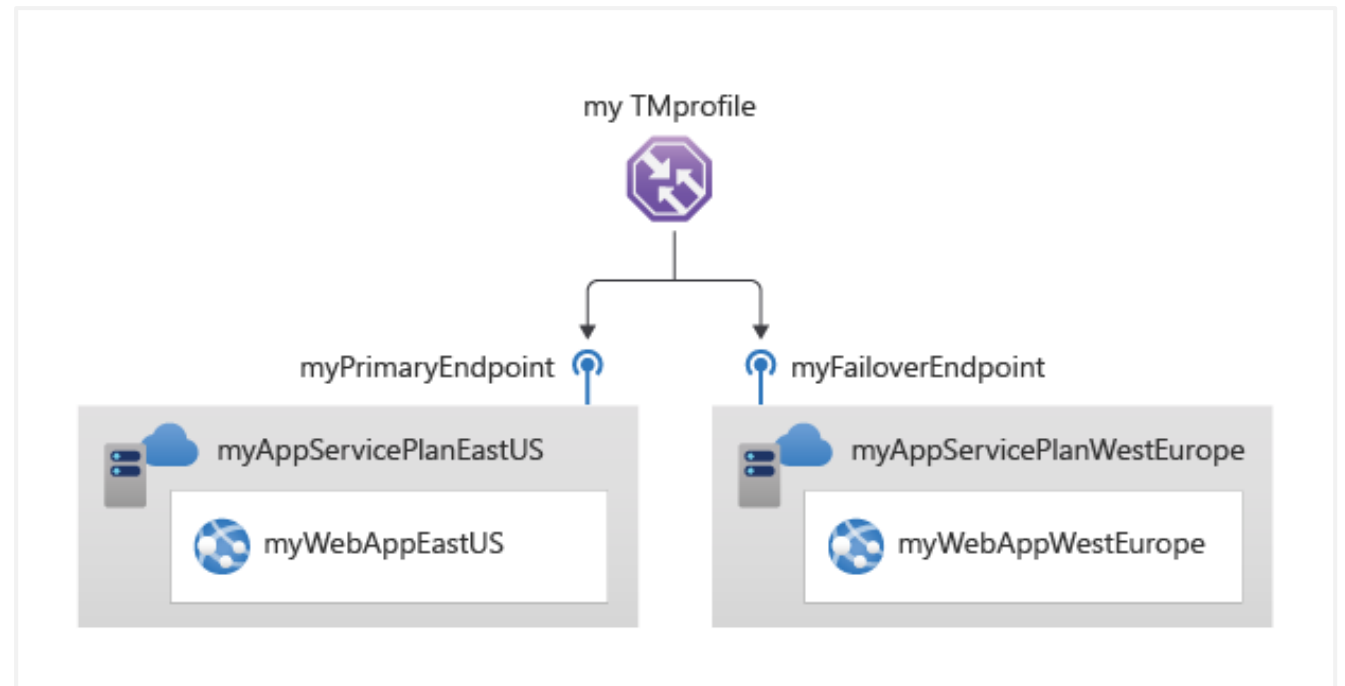
Increase application availability

Improve application performance

Service maintenance without downtime

Combine hybrid applications

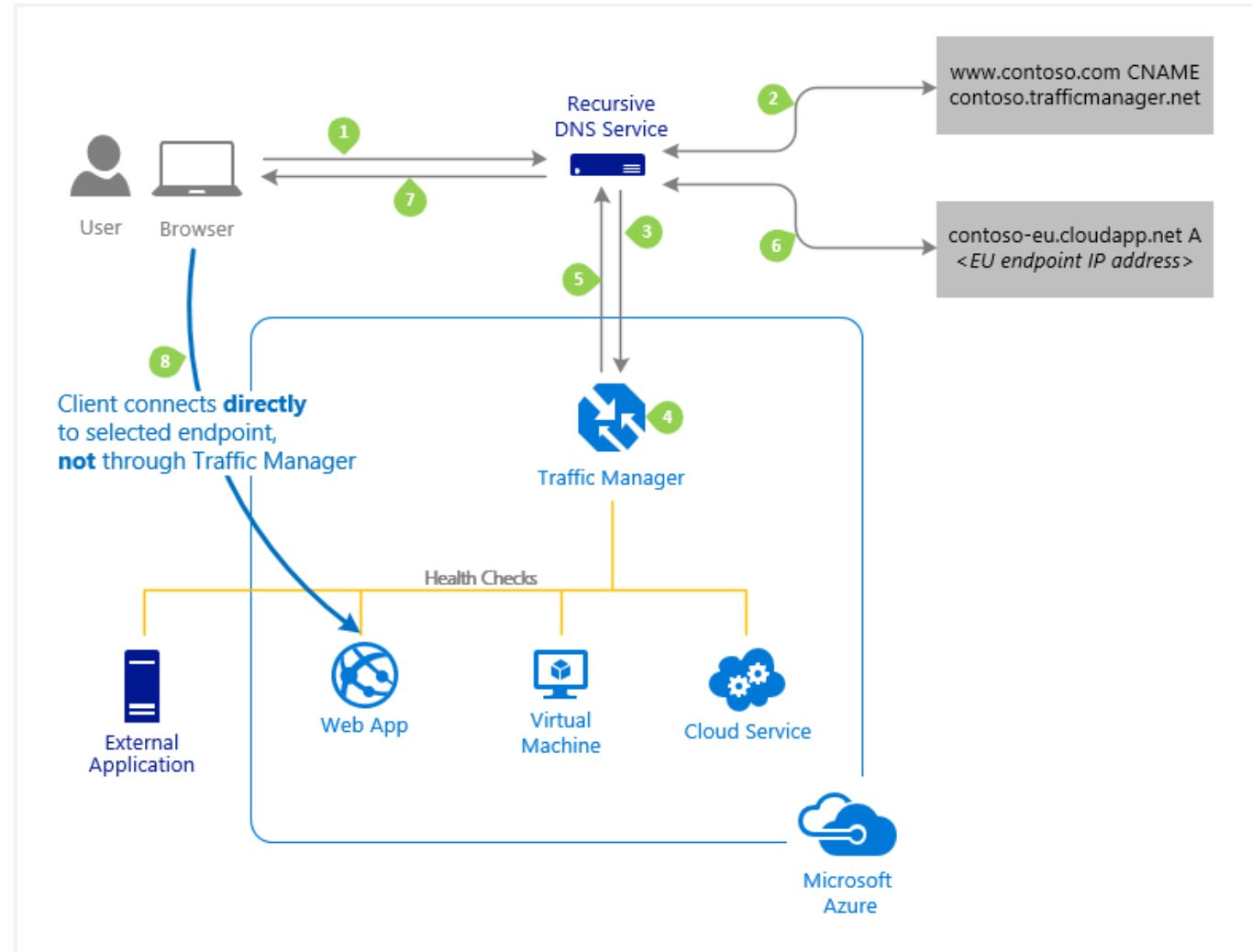
Distribute traffic for complex deployments



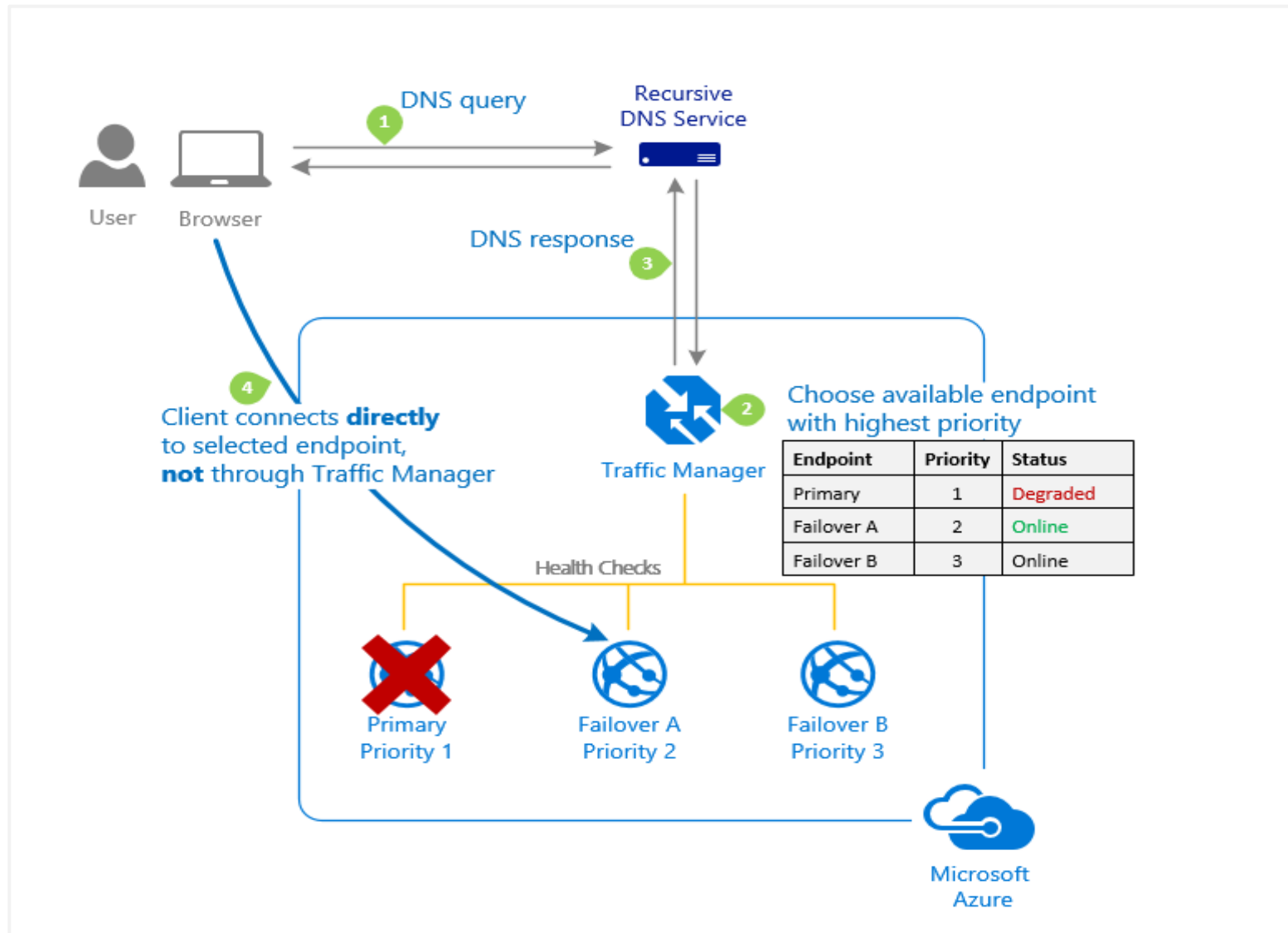
How Traffic manager works

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

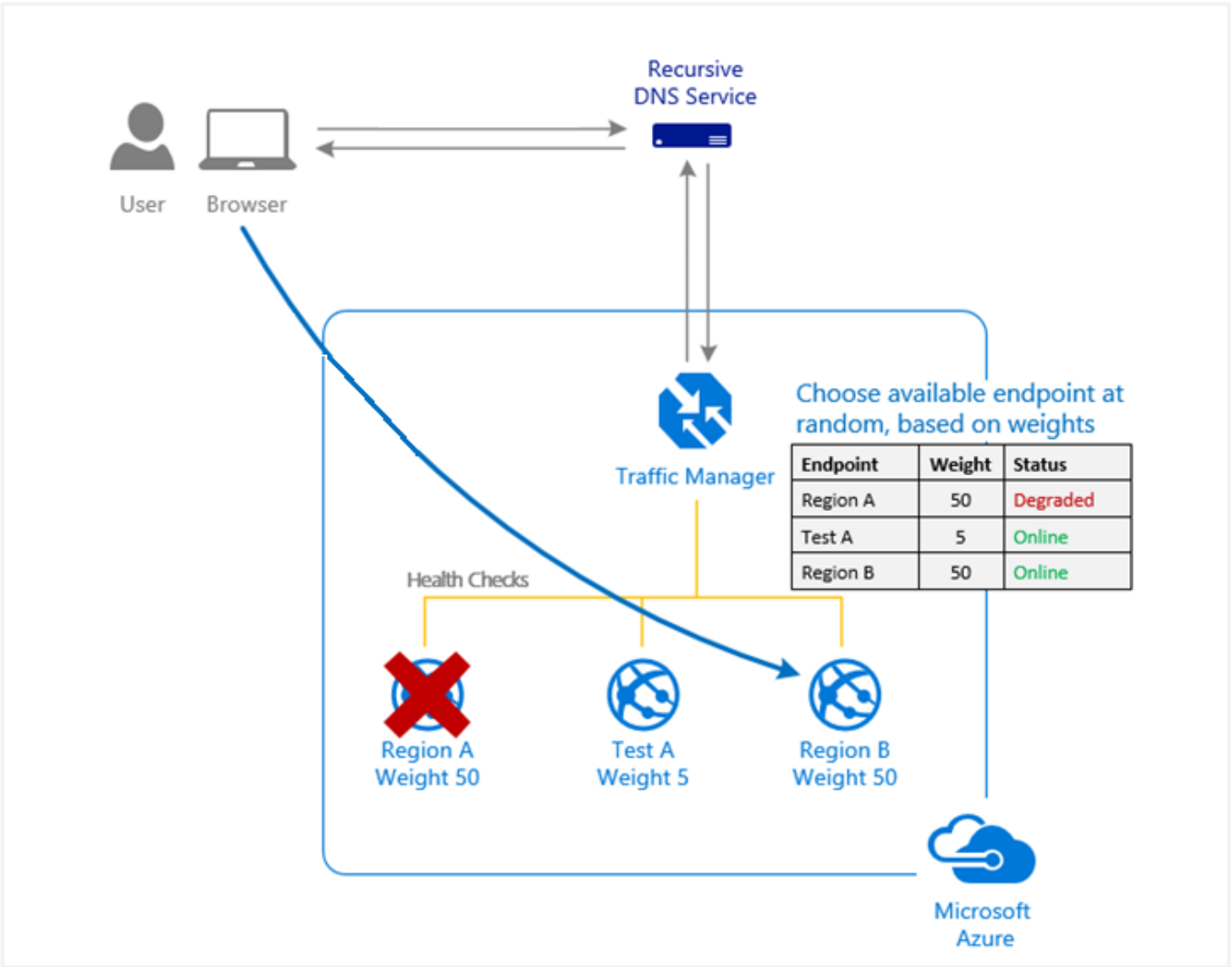
- The configured state of each endpoint
- The current health of each endpoint, as determined by the Traffic Manager health checks
- The chosen traffic-routing method
- Final connection is not going through Traffic Manager



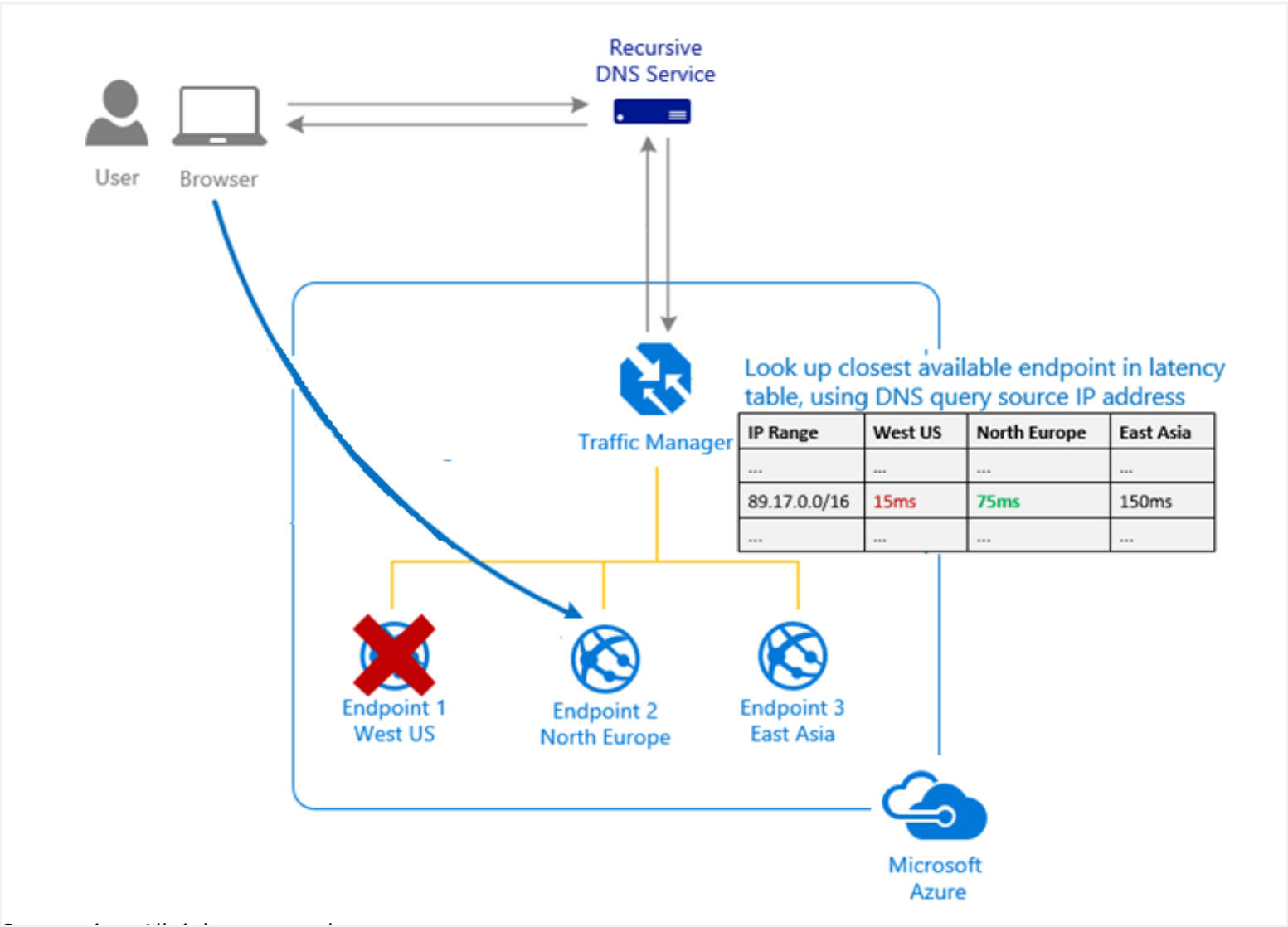
Traffic routing methods – Priority



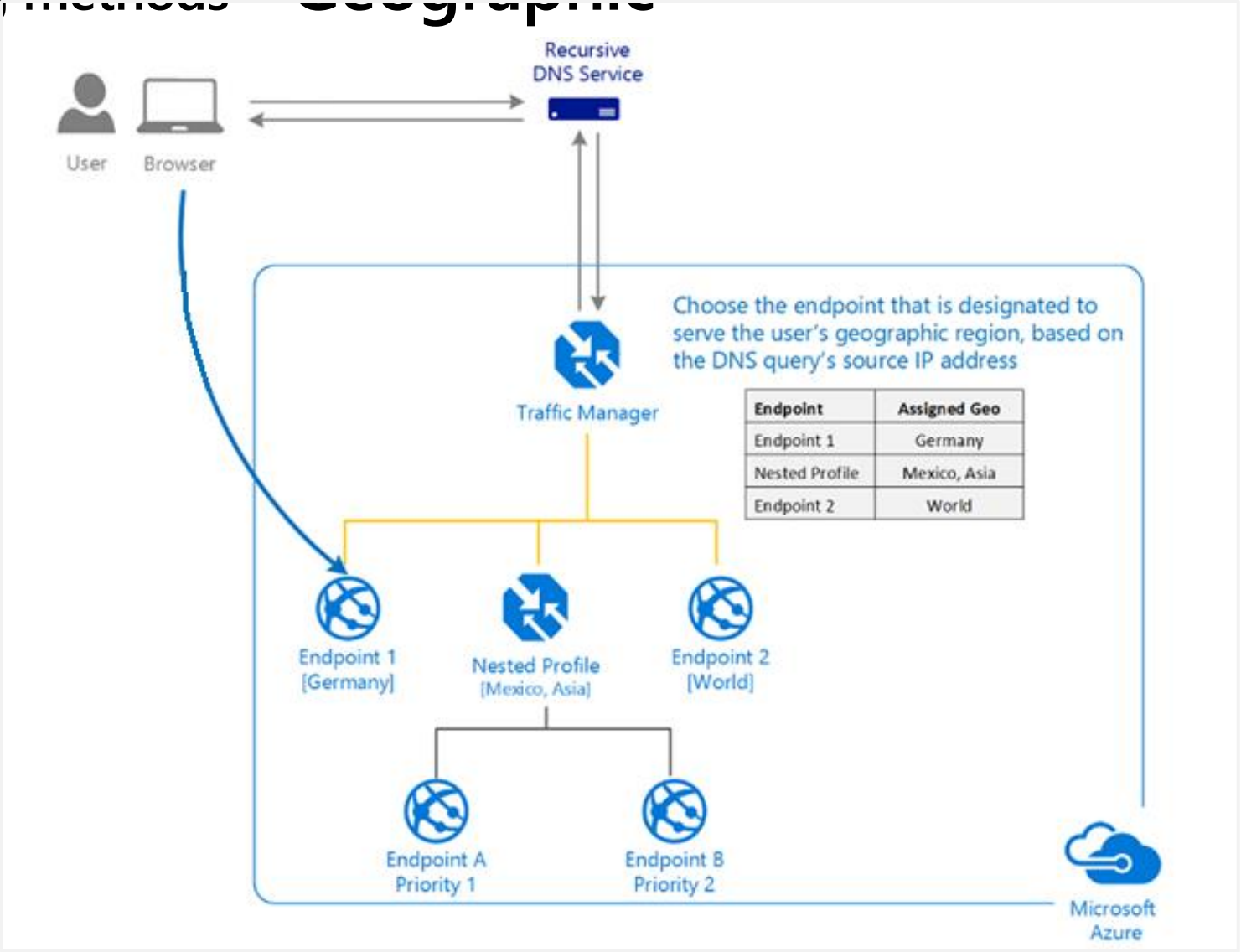
Traffic routing methods – Weighted



Traffic routing methods – Performance



Traffic routing methods - Geographic

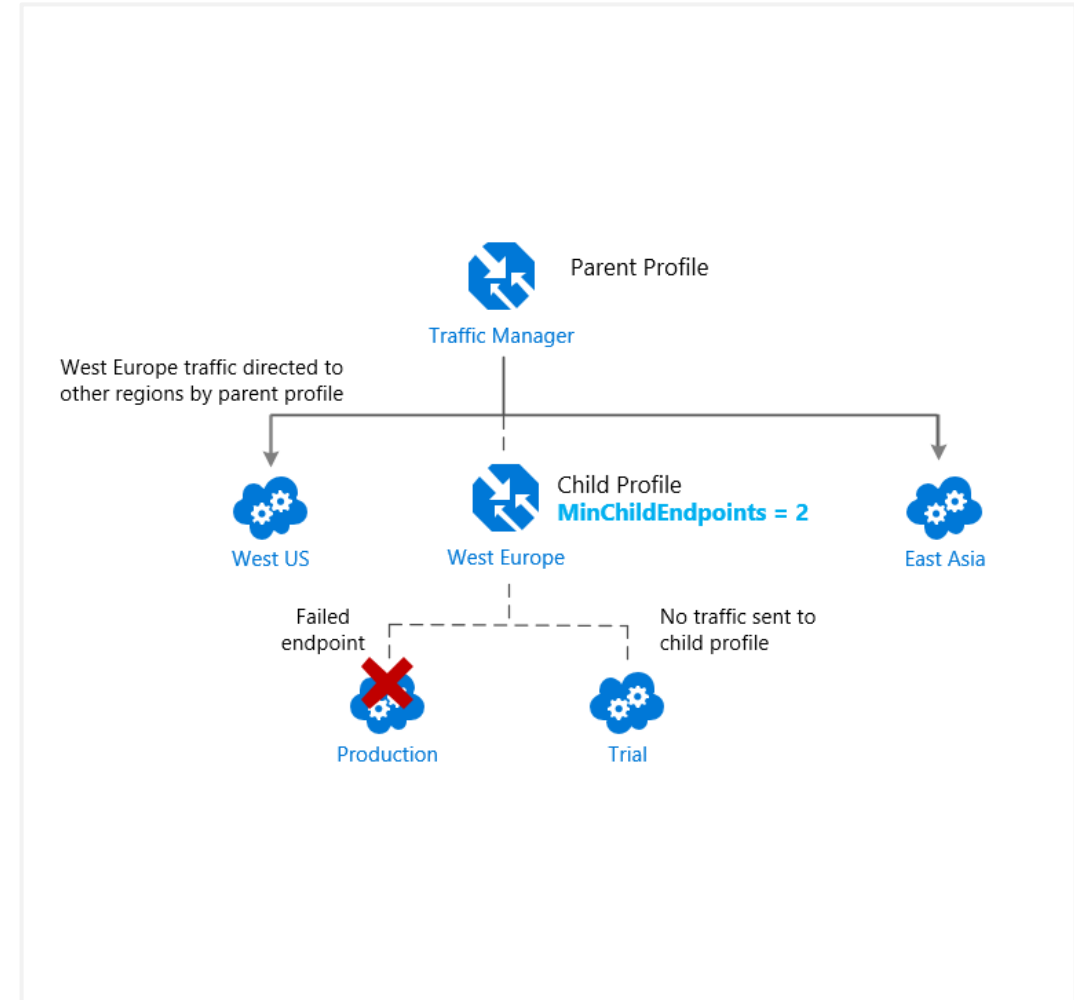


Traffic manager endpoints

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

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 ^
Performance
Weighted
Priority
Geographic
MultiValue
Subnet

Create

Automation options

© Copyright Microsoft Corporation. All rights reserved.

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

Contoso-TMprofile-SR | Configuration

Traffic Manager profile

Search (Ctrl+/)

Save Discard

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Real user measurements

Traffic view

Endpoints

Properties

Locks

Monitoring

Alerts

Metrics

Diagnostic settings

Logs

Automation

Tasks (preview)

Export template

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 * ⓘ

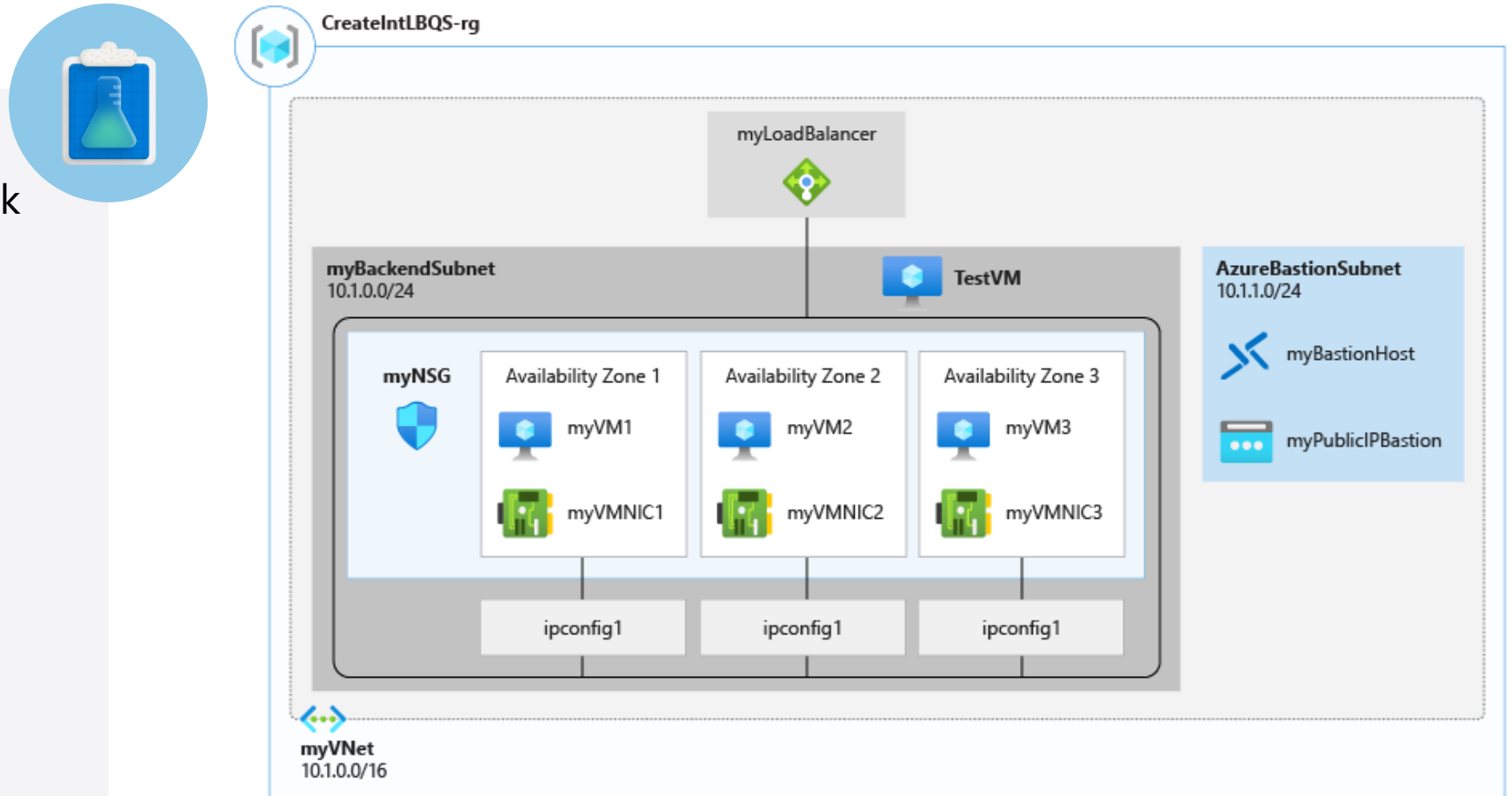
10 seconds

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



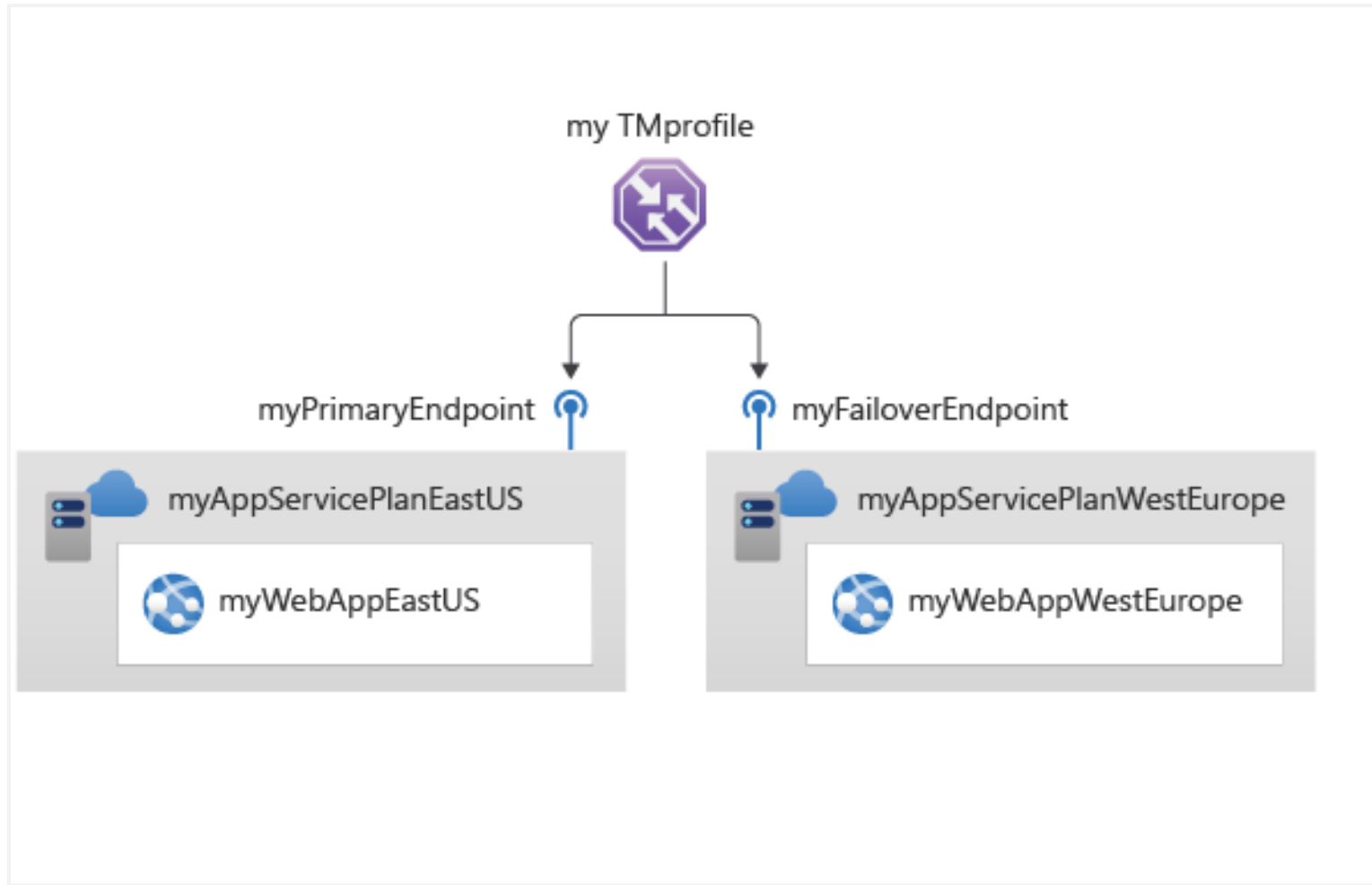
Exercise – Create a traffic manager profile using the Azure portal



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

