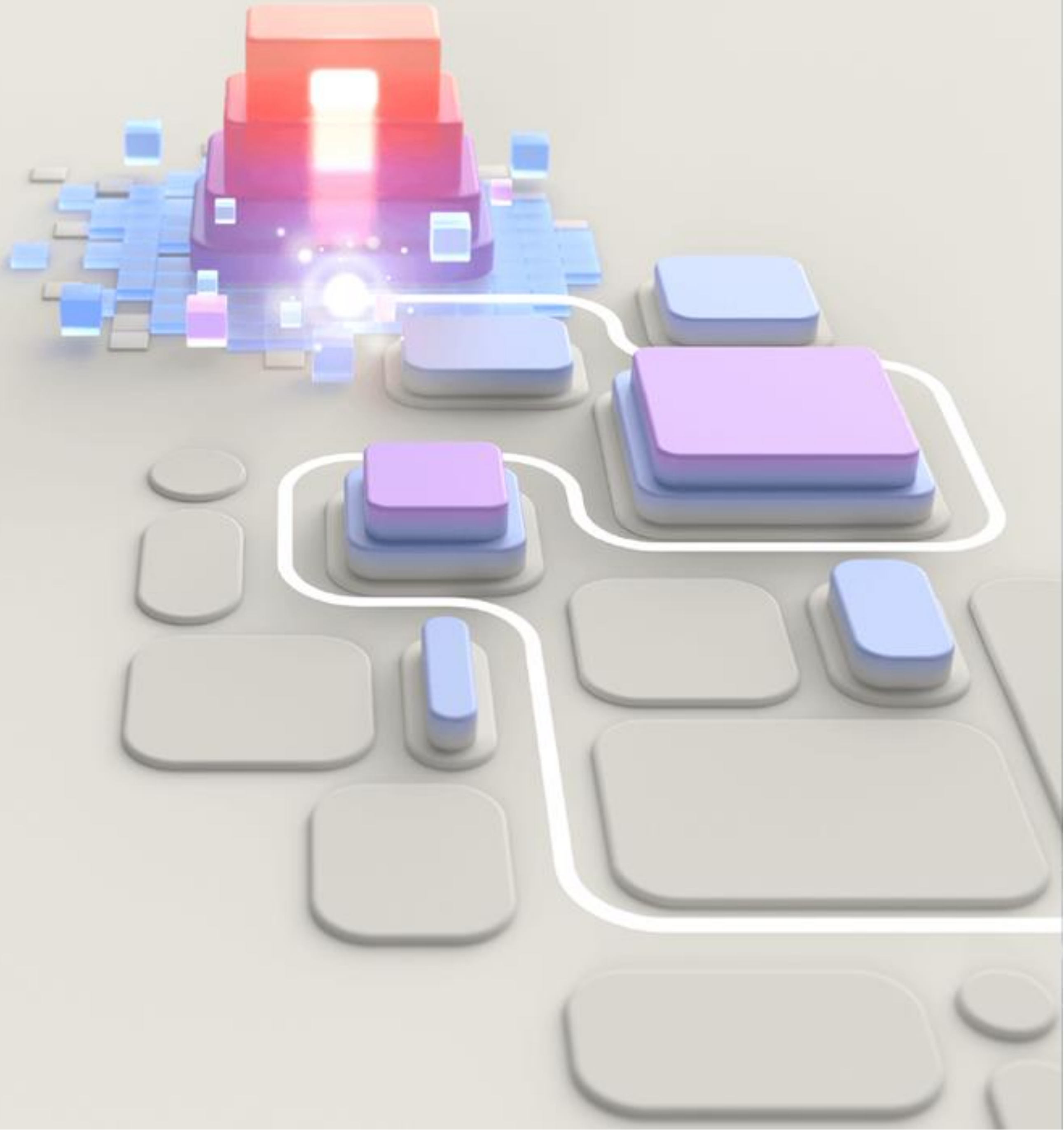
Microsoft

AZ-700

Load balancing HTTP(S) traffic in Azure



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 ←

App GW
↓
Regional

+ CDN

Front Door
Global

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

- Design Azure Application Gateway
- Configure Azure Application Gateway
- Exercise: Deploy Azure Application Gateway
- Design and configure Azure Front Door
- Exercise: Create a Front Door for highly available web application using the Azure portal

IaaS → PaaS

VM

Web Server

App Service

Tim Berners-Lee
CERN
404

Design Azure Application Gateway

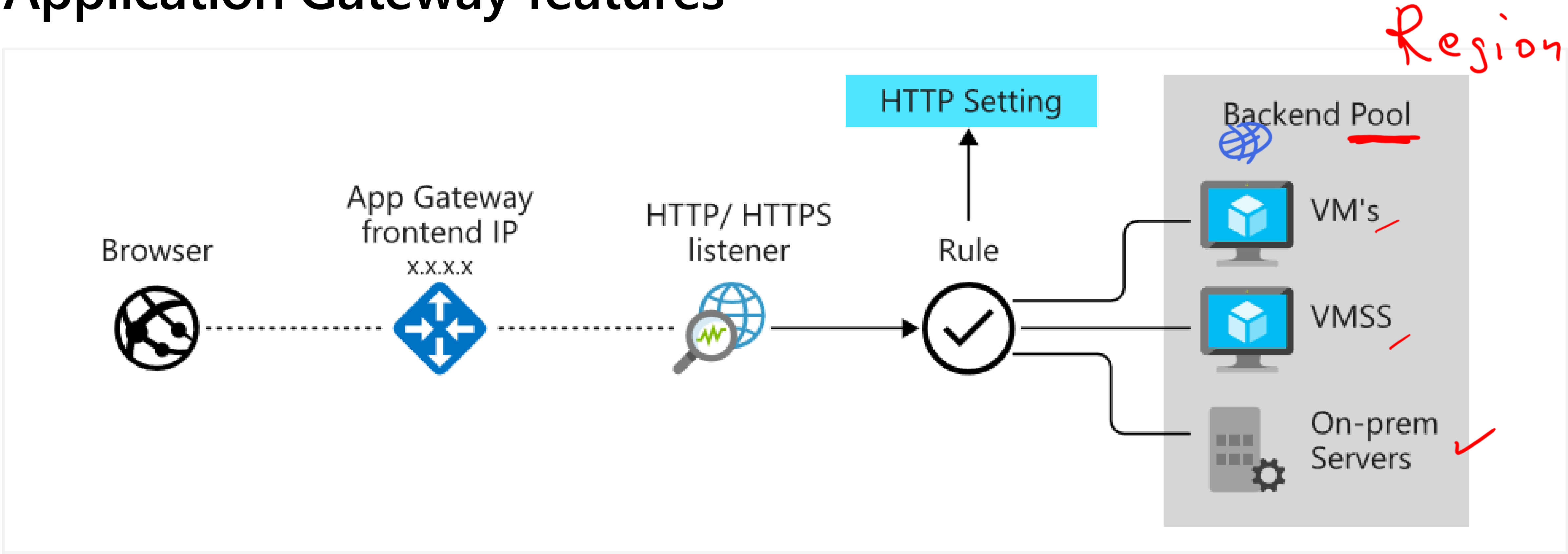
WAF OWASP

FrontDoo

Learning Objectives - Design Azure Application Gateway

- Application Gateway features
- Determine Application Gateway Routing
- Choosing an Azure App Gateway SKU
- Application Gateway configuration planning
- Learning Recap

Application Gateway features



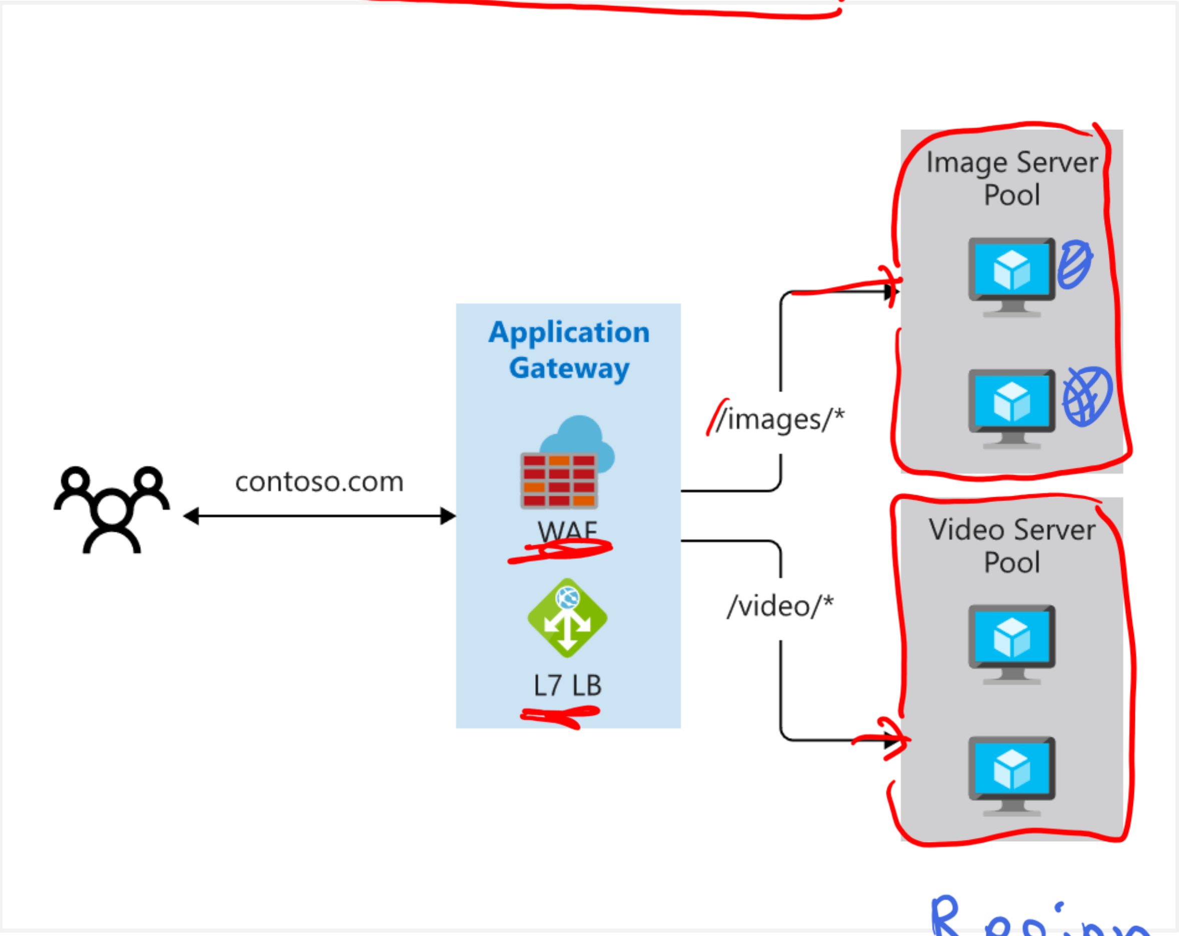
Manages web app requests

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

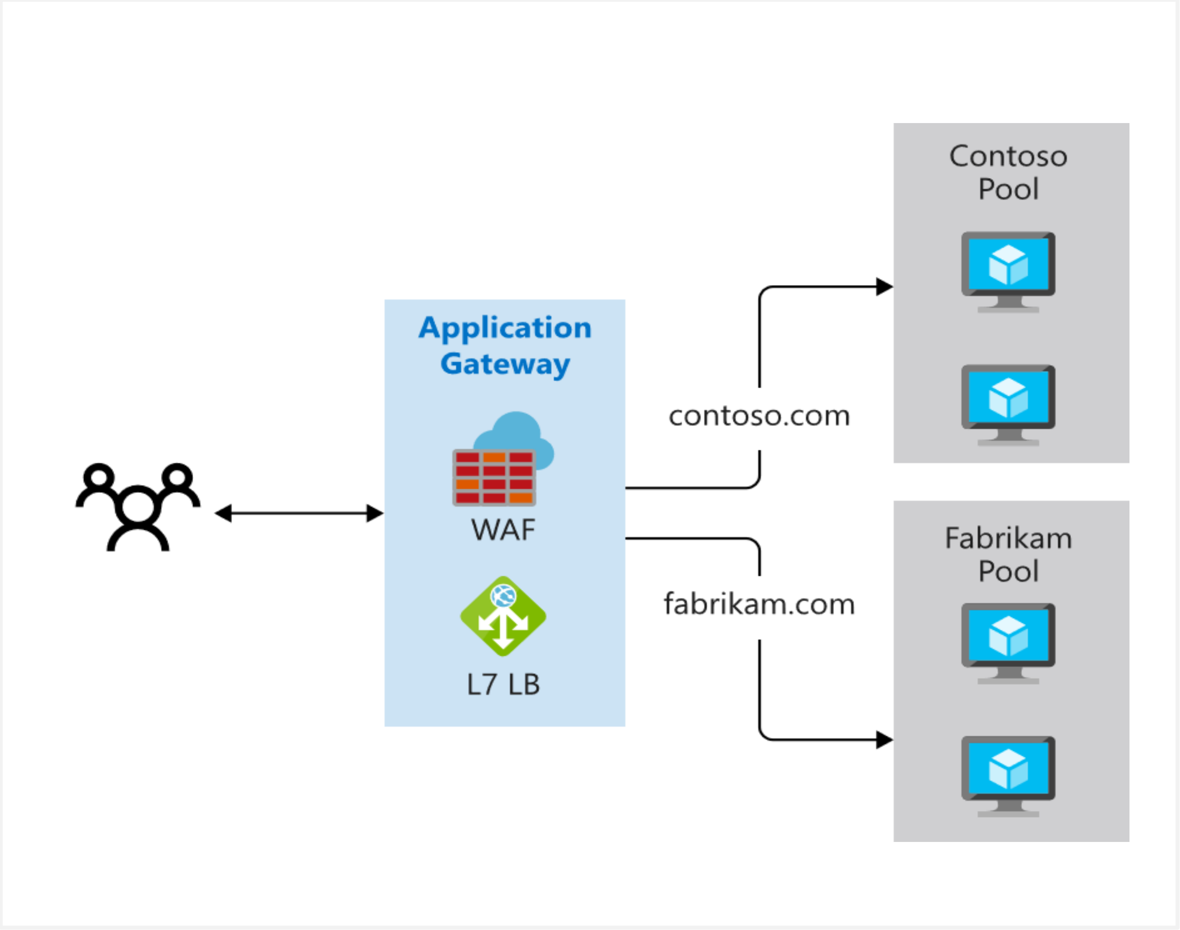
Determine Application Gateway Routing

Path-based routing



Region

Multiple-site routing



Choosing an Azure App Gateway SKU

SKU	Usage	SLA
Basic (Preview)	Designed for applications that have lower traffic and SLA requirements, and don't need advanced traffic management features.	99.9%
Standard_v2 SKU	Designed for running production workloads and high traffic. This SKU includes autoscaling.	99.95%

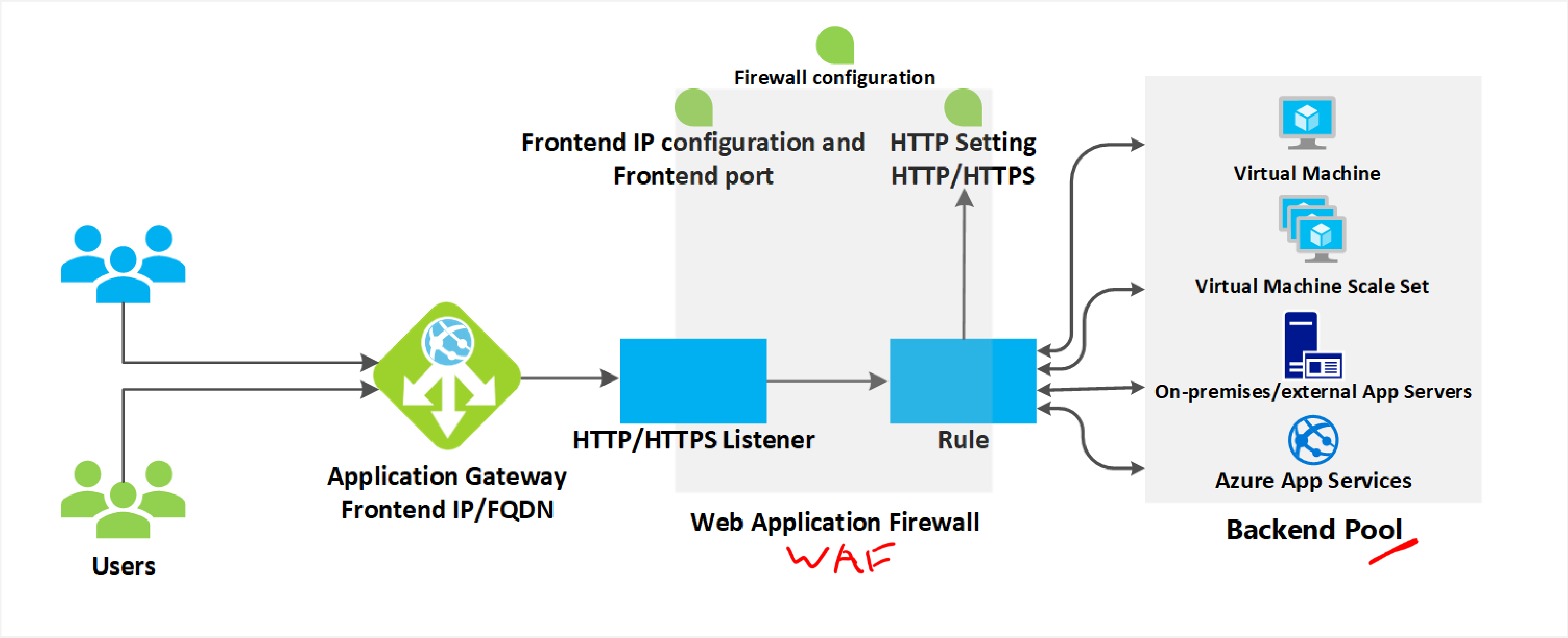
Both SKUs provide basic functionality – cookie affinity, path-based affinity, and public/private IP addresses.

Max connections per sec:

- Basic: 200
- Standard: 62,500

The older V1 SKU is being deprecated. A migration path is available.

Application Gateway configuration planning



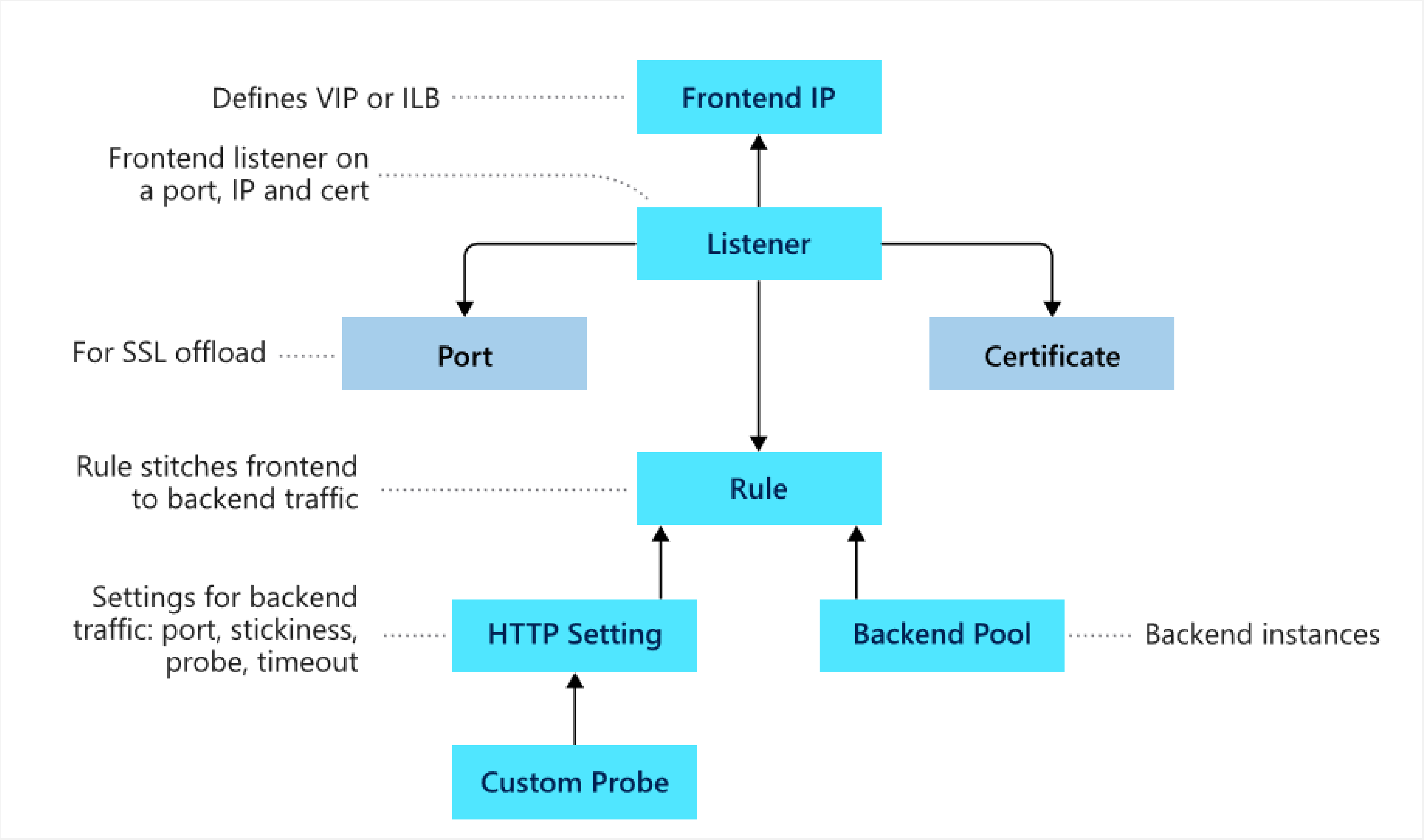
Configure Azure Application Gateway

Learning Objectives - Configure Azure Application Gateway

- Configure Application Gateway
- Configure Health Probes
- Configure Listeners
- Redirection Overview
- Application Gateway Request routing rules
- Associated back-end pool
- Configure URL-based routing
- Configure rewrite policies
- Demonstration
- Learning Recap

Configure Application Gateway

- Frontend IP
- Listeners
- Routing rules
- Backend pools
- Web application firewall (optional)
- Health probes

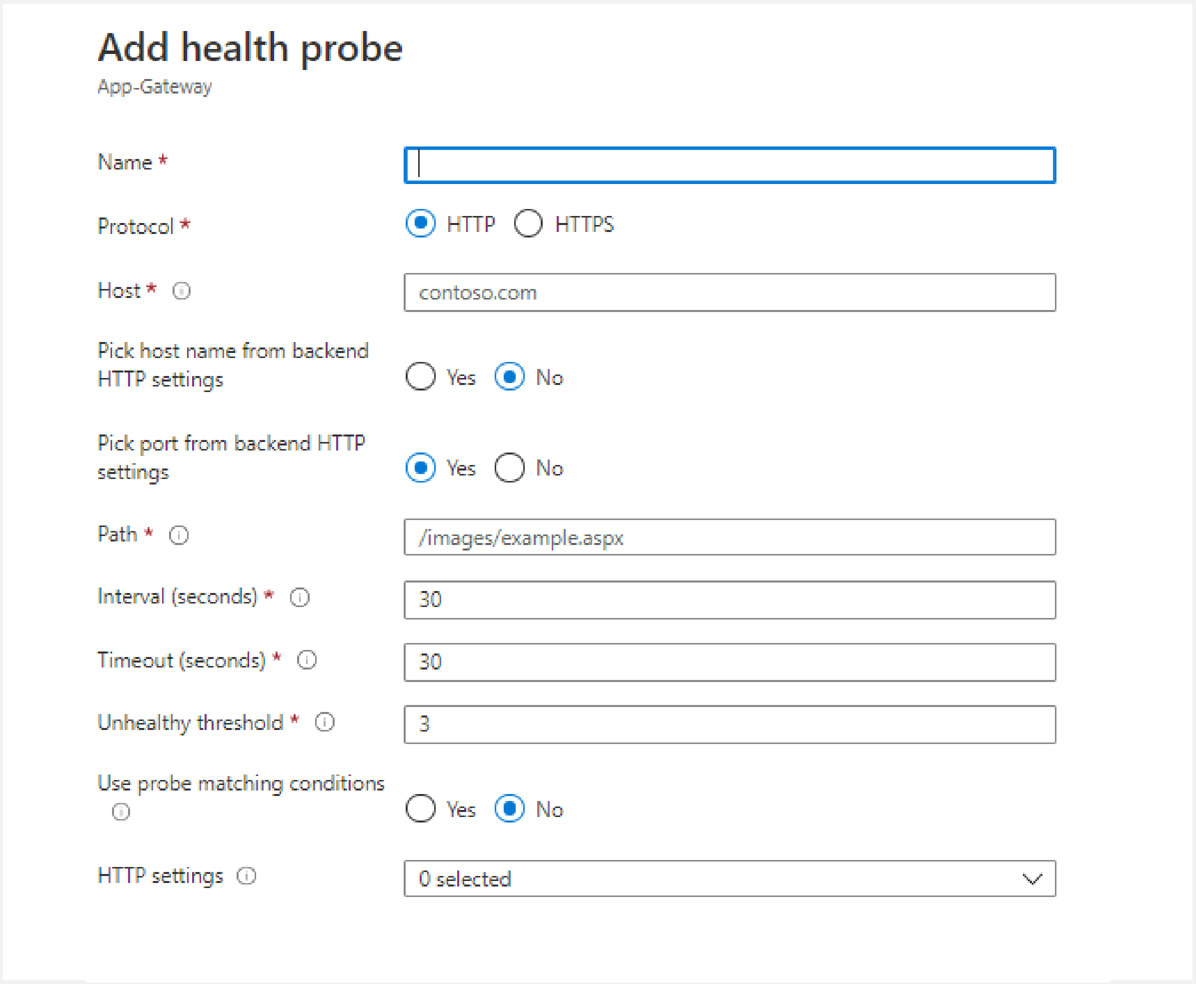

Defines VIP or ILB
Frontend IP
Frontend listener on a port, IP and cert
Listener
For SSL offload
Port
Certificate
Rule stitches frontend to backend traffic
Rule
Settings for backend traffic: port, stickiness, probe, timeout
HTTP Setting
Backend Pool
Backend instances
Custom Probe

Configure health probes

Default health probe

Custom health probe

Probe matching



Add health probe

App-Gateway

Name *

Protocol * ● HTTP ○ HTTPS

Host * ⓘ contoso.com

Pick host name from backend HTTP settings ○ Yes ● No

Pick port from backend HTTP settings ● Yes ○ No

Path * ⓘ /images/example.aspx

Interval (seconds) * ⓘ 30

Timeout (seconds) * ⓘ 30

Unhealthy threshold * ⓘ 3

Use probe matching conditions ⓘ ○ Yes ● No

HTTP settings ⓘ 0 selected

Configure listeners

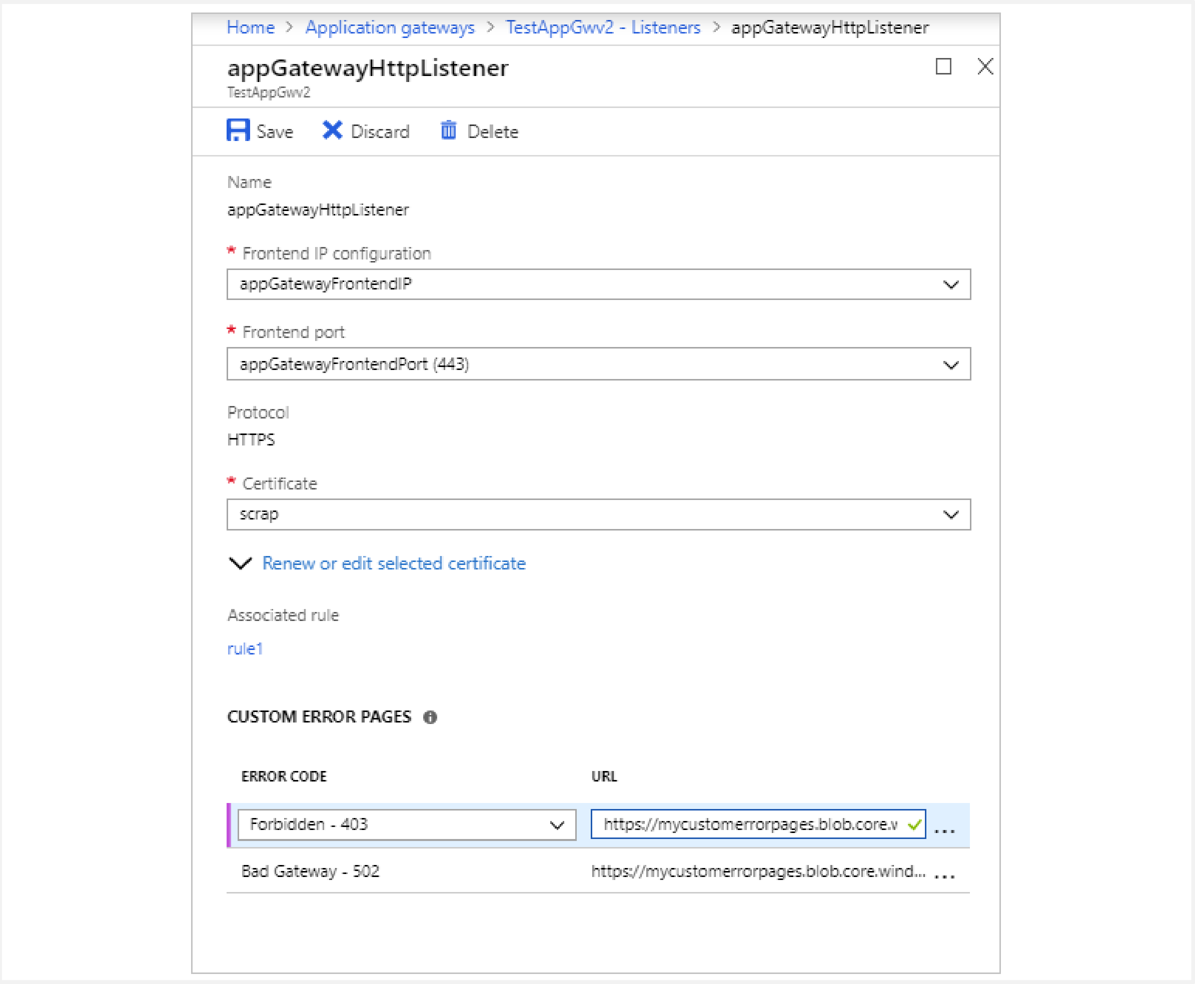
Basic or Multi Site

Order of Processing Listeners

Frontend IP address

Frontend Port

Protocol HTTP or HTTPS


Home > Application gateways > TestAppGwv2 - Listeners > appGatewayHttpListener
Save
Discard
Delete
Renew or edit selected certificate

appGatewayHttpListener
TestAppGwv2

Name
appGatewayHttpListener

* Frontend IP configuration
appGatewayFrontendIP

* Frontend port
appGatewayFrontendPort (443)

Protocol
HTTPS

* Certificate
scrap

Associated rule
rule1

CUSTOM ERROR PAGES

ERROR CODE	URL
Forbidden - 403	https://mycustomerrorpages.blob.core.v
Bad Gateway - 502	https://mycustomerrorpages.blob.core.wind...

Redirection overview

404

Global redirection: Redirects from one listener to another listener on the gateway. This enables HTTP to HTTPS redirection on a site

Path-based redirection: Enables HTTP to HTTPS redirection only on a specific site area, for example a shopping cart area denoted by /cart/*.

Redirect to external site: Requires a new redirect configuration object, which specifies the target listener or external site to which redirection is desired

The following types of redirection are supported:

- 301 Permanent Redirect
- 302 Found
- 303 See Other
- 307 Temporary Redirect

500

Application Gateway Request routing rules

Rule Types:

Basic
Path-based

Order of processing rules
For the v1 and v2 SKU, pattern matching of incoming requests is processed in the order that the paths are listed in the URL path map of the path-based rule.

Associated listener

Associate a listener to the rule so that the request-routing rule that's associated with the listener is evaluated to determine the back-end pool to route the request to.

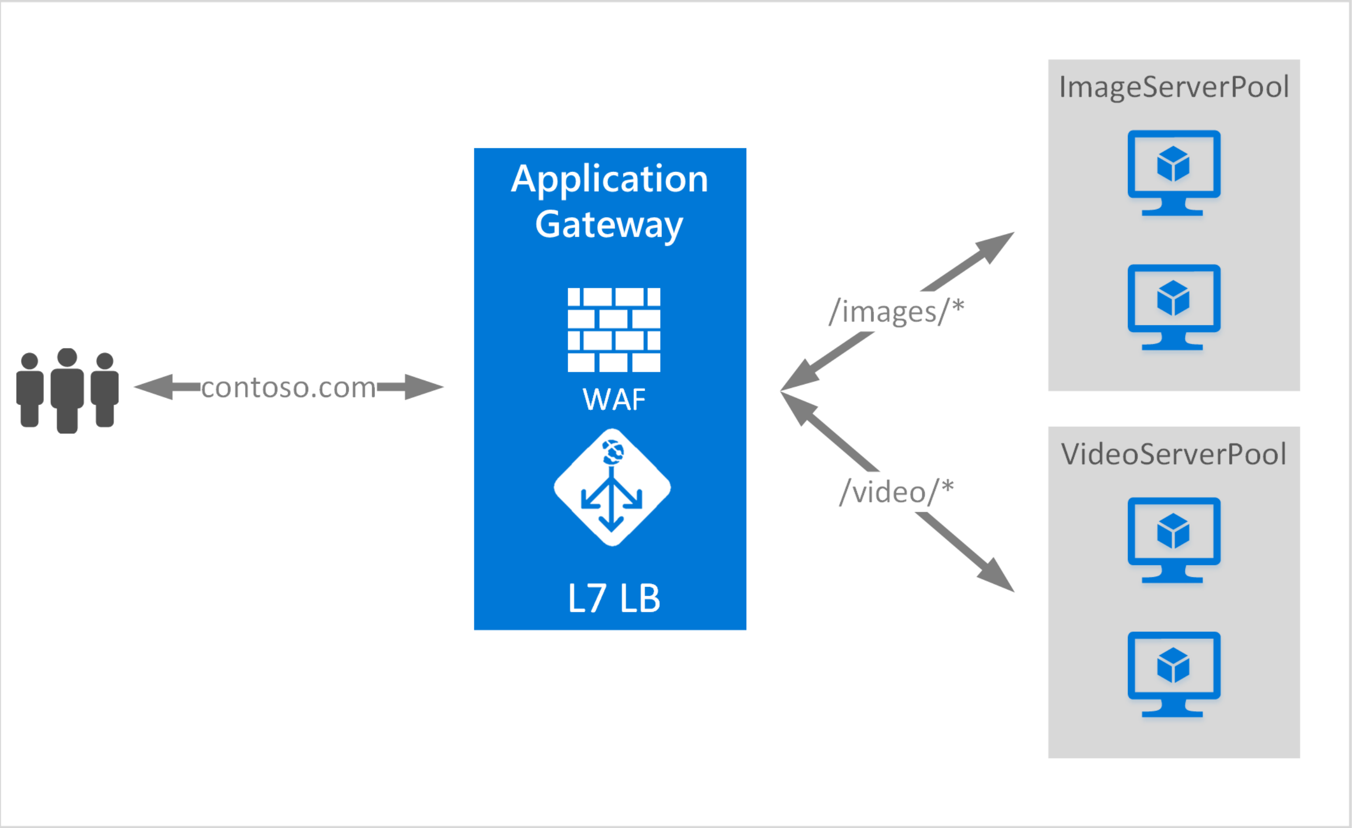
Associated back-end pool

basic rule: one back-end pool is allowed. All requests on the associated listener are forwarded to that back-end pool.

path-based rule: multiple back-end pools correspond to each URL path. Requests that match the URL path are forwarded to the corresponding back-end pool.

Configure URL Path-based routing

URL Path Based Routing allows you to route traffic to back-end server pools based on URL Paths of the request



Configure rewrite policies

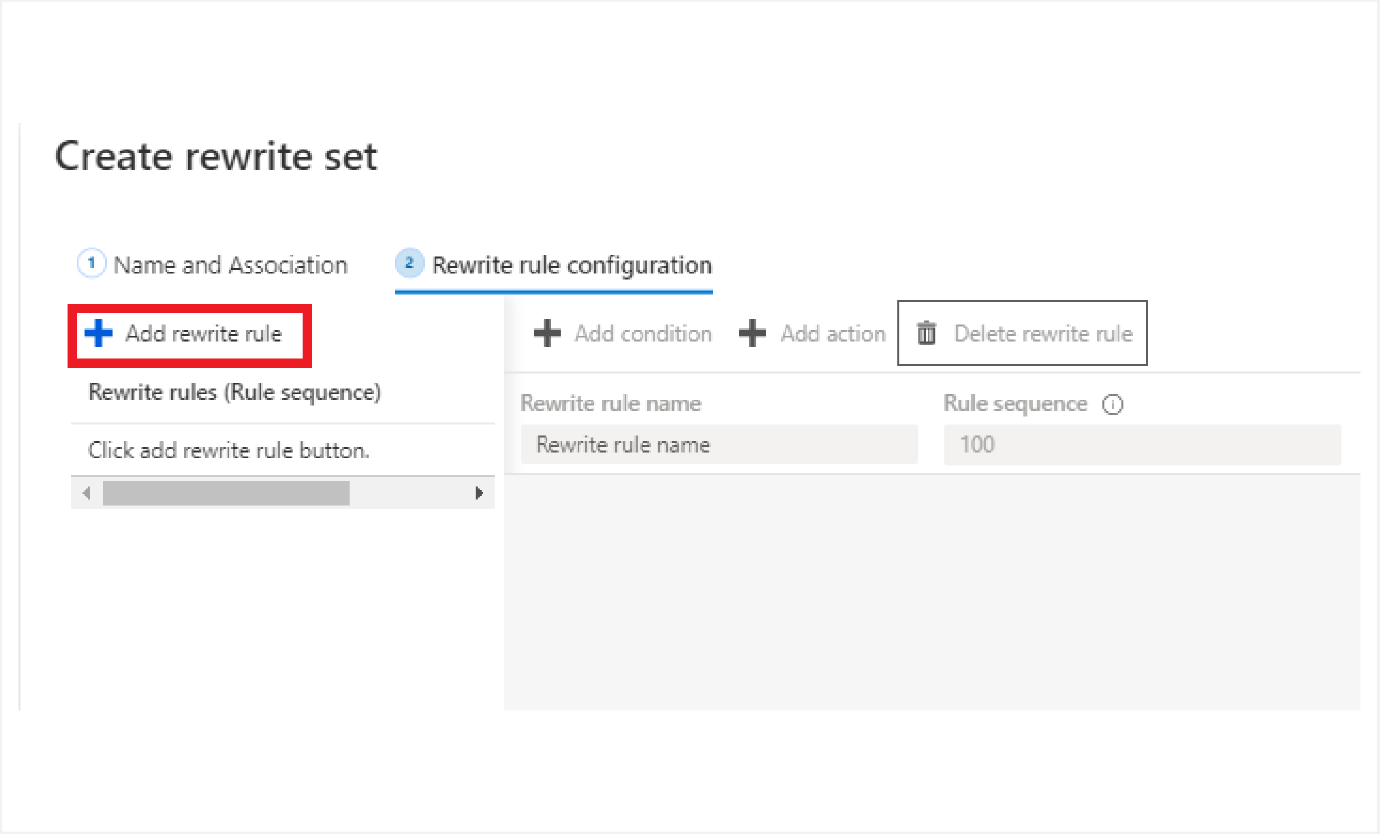
A rewrite rule set contains:

Request routing rule association

Rewrite Condition

Rewrite type

- Rewriting request headers
- Rewriting response headers
- Rewriting URL components:
  - **URL path**
  - **URL Query String**
  - **Re-evaluate path map**



Create rewrite set

Click add rewrite rule button.

Rewrite rule name: Rewrite rule name

Rule sequence: 100

Design and configure Azure Front Door

Learning Objectives - Design and Configure Azure Front Door

- What is Azure Front Door
- Azure Front Door Standard and Premium
- Create a Front Door in the Azure portal
- Configure routing and redirection rules
- Configure an origin (Backend)
- Configure health probes
- Secure Front Door with SSL and end-to-end SSL encryption
- Demo
- Learning Recap

What is Azure Front Door

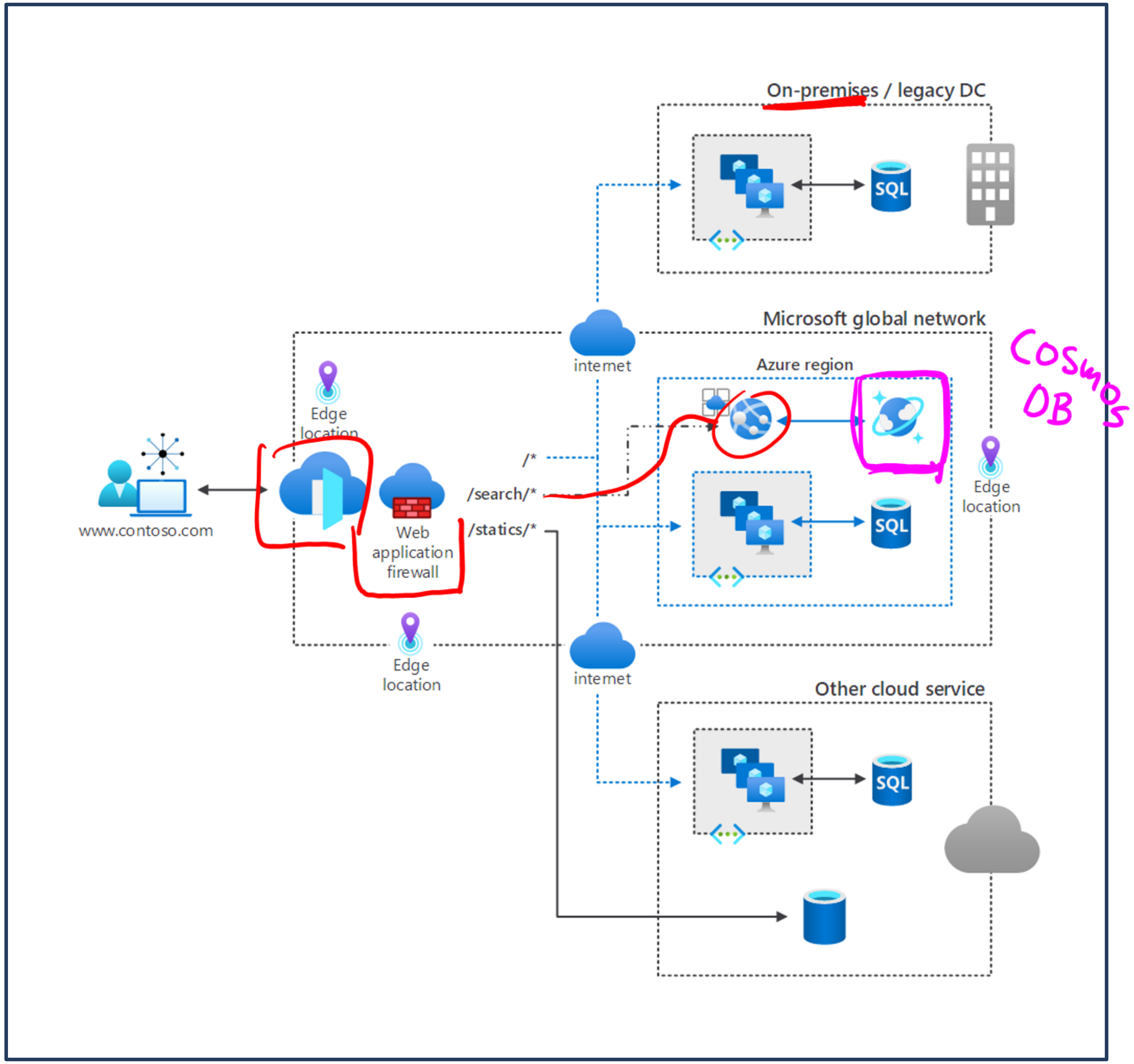
Global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications

Accelerated application performance by using split TCP-based anycast protocol

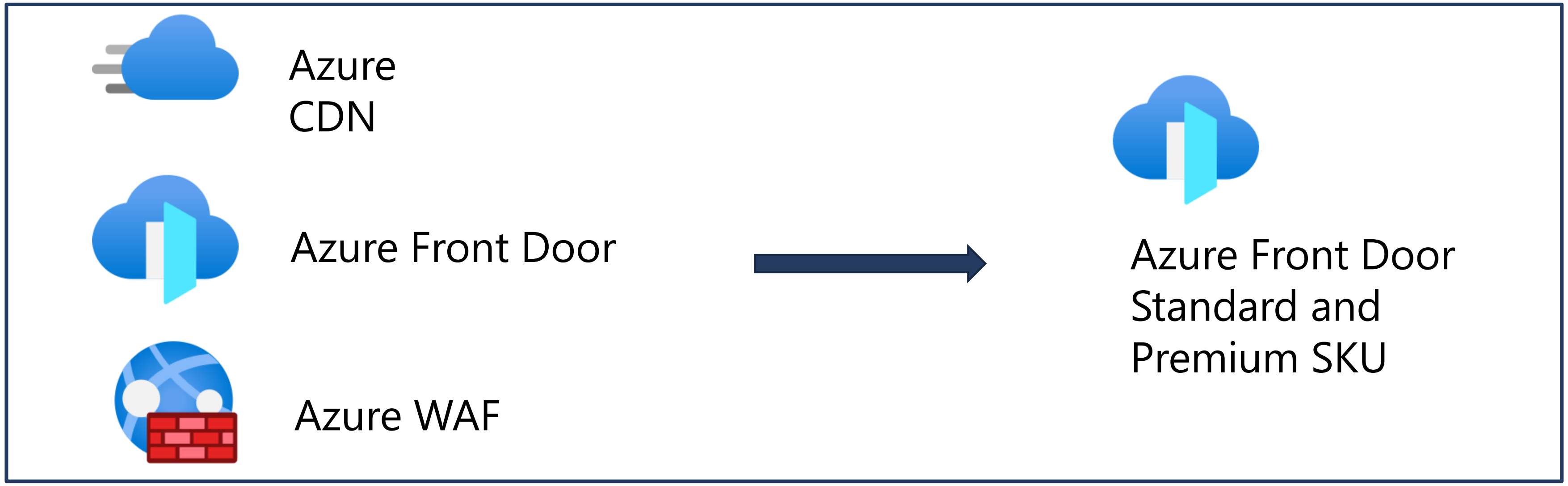
Intelligent health probe monitoring for backend resources

URL-path based routing for requests

Enables hosting of multiple websites for efficient application infrastructure



Azure Front Door Standard and Premium



Azure Front Door Standard SKU:

- Content delivery optimized
- Static and dynamic content acceleration
- Global load balancing
- SSL offload
- Domain and certificate management
- Enhanced traffic analytics
- Basic security capabilities

Azure Front Door Premium SKU builds on capabilities of Standard SKU, and adds:

- Extensive security capabilities across WAF
- Bot protection
- Private Link support ?
- Integration with Microsoft Threat Intelligence and security analytics.

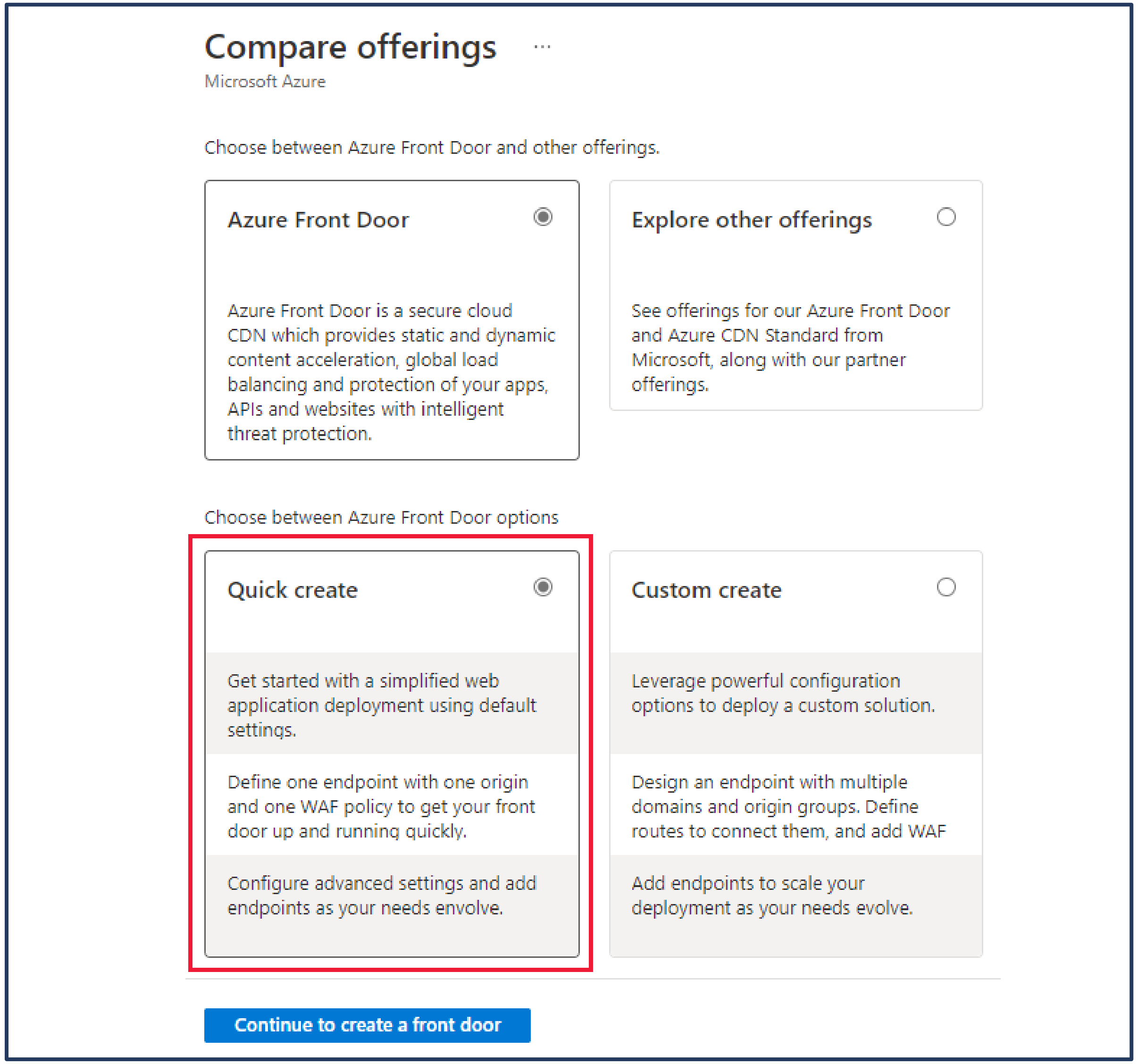
Create a Front Door in the Azure portal

Quick Create or Custom Create

Select between Standard and Premium tier

Globally unique endpoint name

Select Origin type, for example: App service or App Gateway



Compare offerings ···

Microsoft Azure

Choose between Azure Front Door and other offerings.

Azure Front Door ●

Azure Front Door is a secure cloud CDN which provides static and dynamic content acceleration, global load balancing and protection of your apps, APIs and websites with intelligent threat protection.

Explore other offerings ○

See offerings for our Azure Front Door and Azure CDN Standard from Microsoft, along with our partner offerings.

Choose between Azure Front Door options

Quick create ●

Get started with a simplified web application deployment using default settings.

Define one endpoint with one origin and one WAF policy to get your front door up and running quickly.

Configure advanced settings and add endpoints as your needs envolve.

Custom create ○

Leverage powerful configuration options to deploy a custom solution.

Design an endpoint with multiple domains and origin groups. Define routes to connect them, and add WAF

Add endpoints to scale your deployment as your needs evolve.

Configure routing and redirection rules

- Azure Front Door traffic routing takes place over multiple stages. First, traffic is routed from the client to the Front Door. Then, Front Door uses your configuration to determine the origin to send the traffic to.

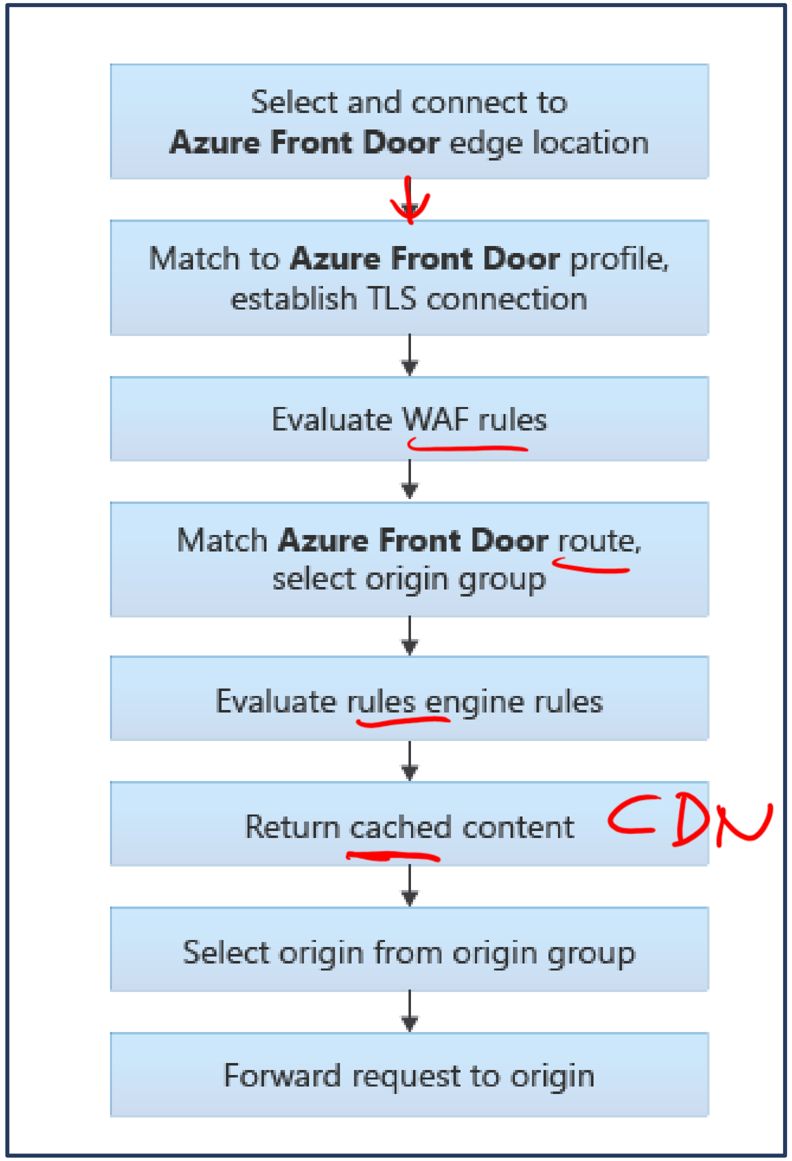
- The Front Door web application firewall, routing rules, rules engine, and caching configuration can all affect the routing process.

Incoming matches

- HTTP Protocols (HTTP/HTTPS)
- Hosts (for example, www.foo.com, *.bar.com) ←
- Paths (for example, /*, /users/*, /file.gif) ←

CDN
Static Content

Redis
SQL



Select and connect to **Azure Front Door** edge location

Match to **Azure Front Door** profile, establish TLS connection

Evaluate WAF rules

Match **Azure Front Door** route, select origin group

Evaluate rules engine rules

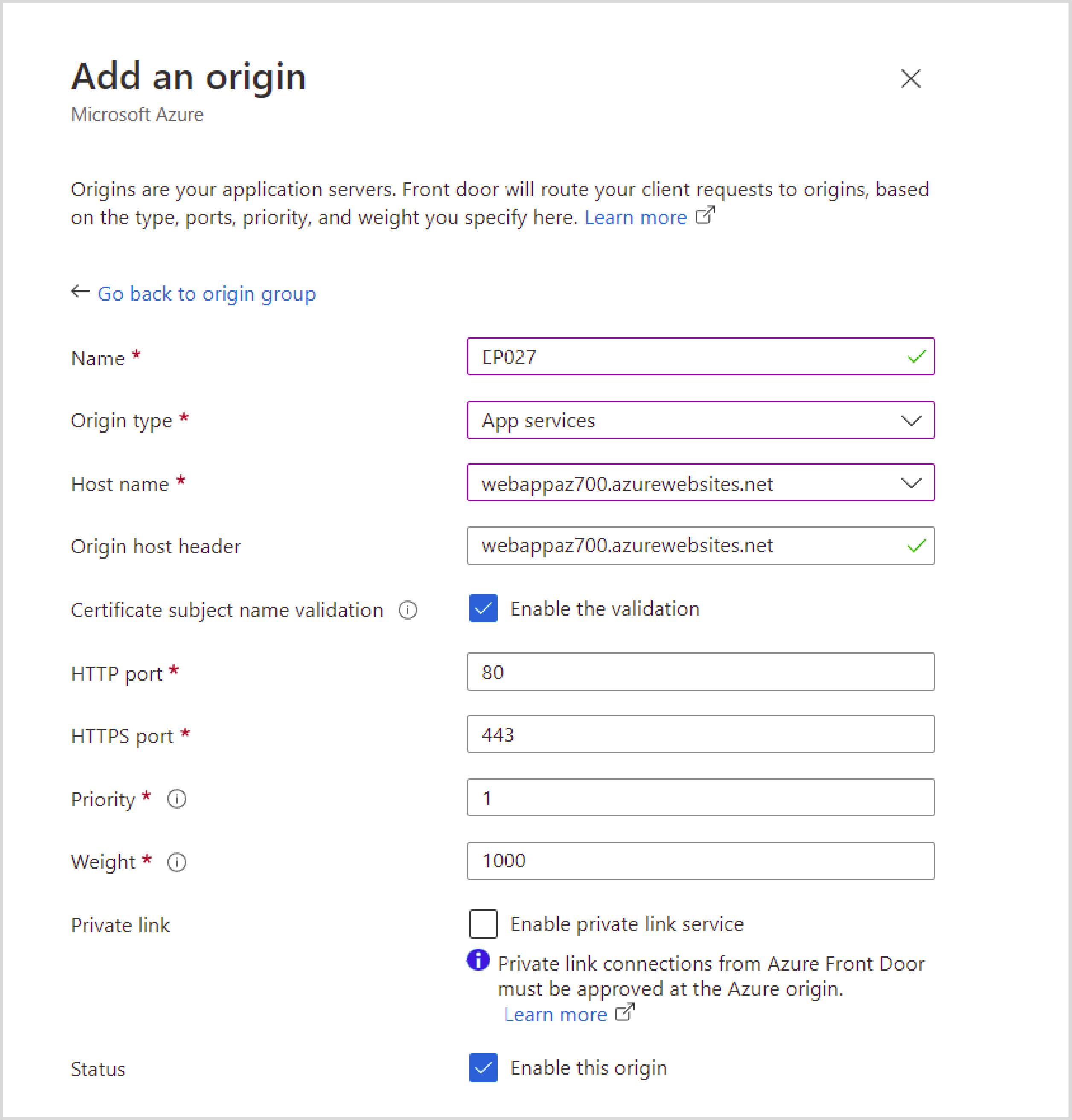
Return cached content CDN

Select origin from origin group

Forward request to origin

Configure an Origin (Backend)

- Origin type
- Host name
- Origin host header
- HTTP & HTTPS port



Add an origin

Microsoft Azure

Origins are your application servers. Front door will route your client requests to origins, based on the type, ports, priority, and weight you specify here. Learn more

← Go back to origin group

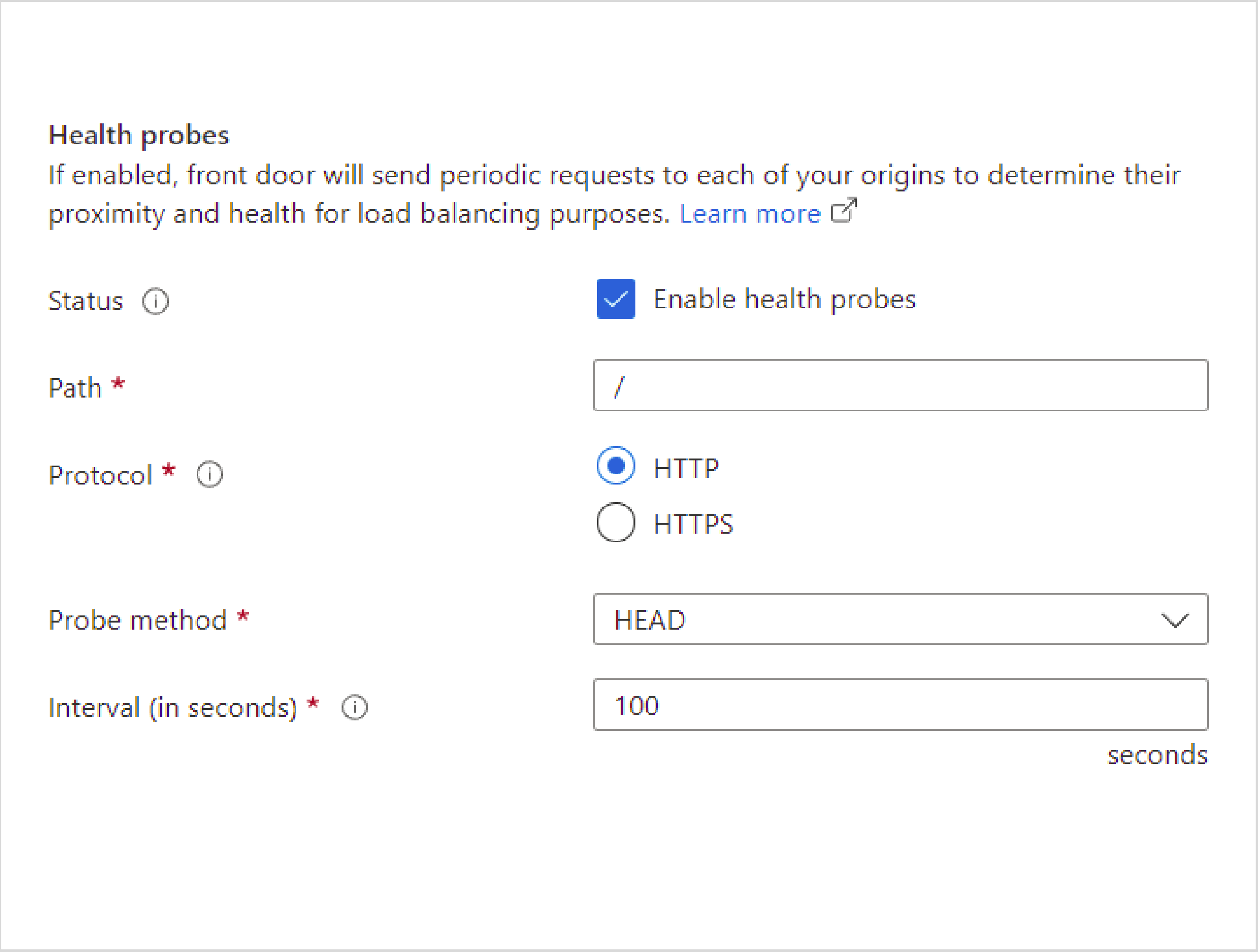
Name *	EP027 ✓
Origin type *	App services
Host name *	webappaz700.azurewebsites.net
Origin host header	webappaz700.azurewebsites.net ✓
Certificate subject name validation ⓘ	☑ Enable the validation
HTTP port *	80
HTTPS port *	443
Priority * ⓘ	1
Weight * ⓘ	1000
Private link	☐ Enable private link service Private link connections from Azure Front Door must be approved at the Azure origin. Learn more
Status	☑ Enable this origin

Configure health probes

Front Door supports the following HTTP methods for sending the health probes:

GET: The GET method means retrieve whatever information (in the form of an entity) is identified by the Request-URI.

HEAD: The HEAD method is identical to GET except that the server MUST NOT return a message-body in the response. For new Front Door profiles, by default, the probe method is set as HEAD.



Health probes

If enabled, front door will send periodic requests to each of your origins to determine their proximity and health for load balancing purposes. Learn more

Status ☑ Enable health probes

Path * /

Protocol * ● HTTP ○ HTTPS

Probe method * HEAD

Interval (in seconds) * 100 seconds

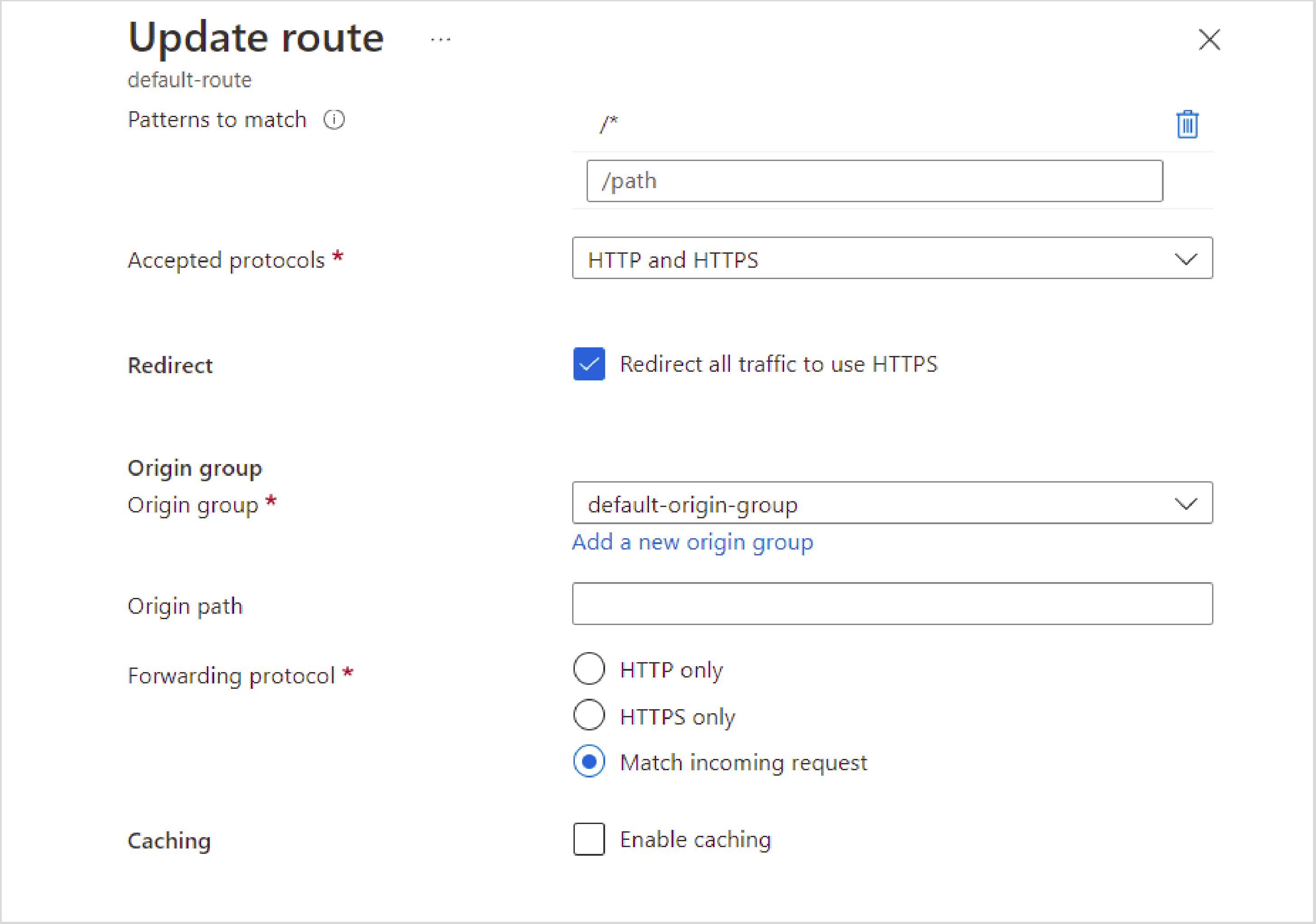
Secure Front Door with SSL and end-to-end SSL encryption

Create HTTP to HTTPS redirect rule

Create a routing rule for HTTP to HTTPS redirect

Add routing rule to handle the HTTPS traffic

On the Route Details section, set the Route Type to Forward.



Update route

default-route

Patterns to match: /*

/path

Accepted protocols *: HTTP and HTTPS

Redirect: ☑ Redirect all traffic to use HTTPS

Origin group

Origin group *: default-origin-group

Add a new origin group

Origin path:

Forwarding protocol *:
○ HTTP only
○ HTTPS only
● Match incoming request

Caching: □ Enable caching

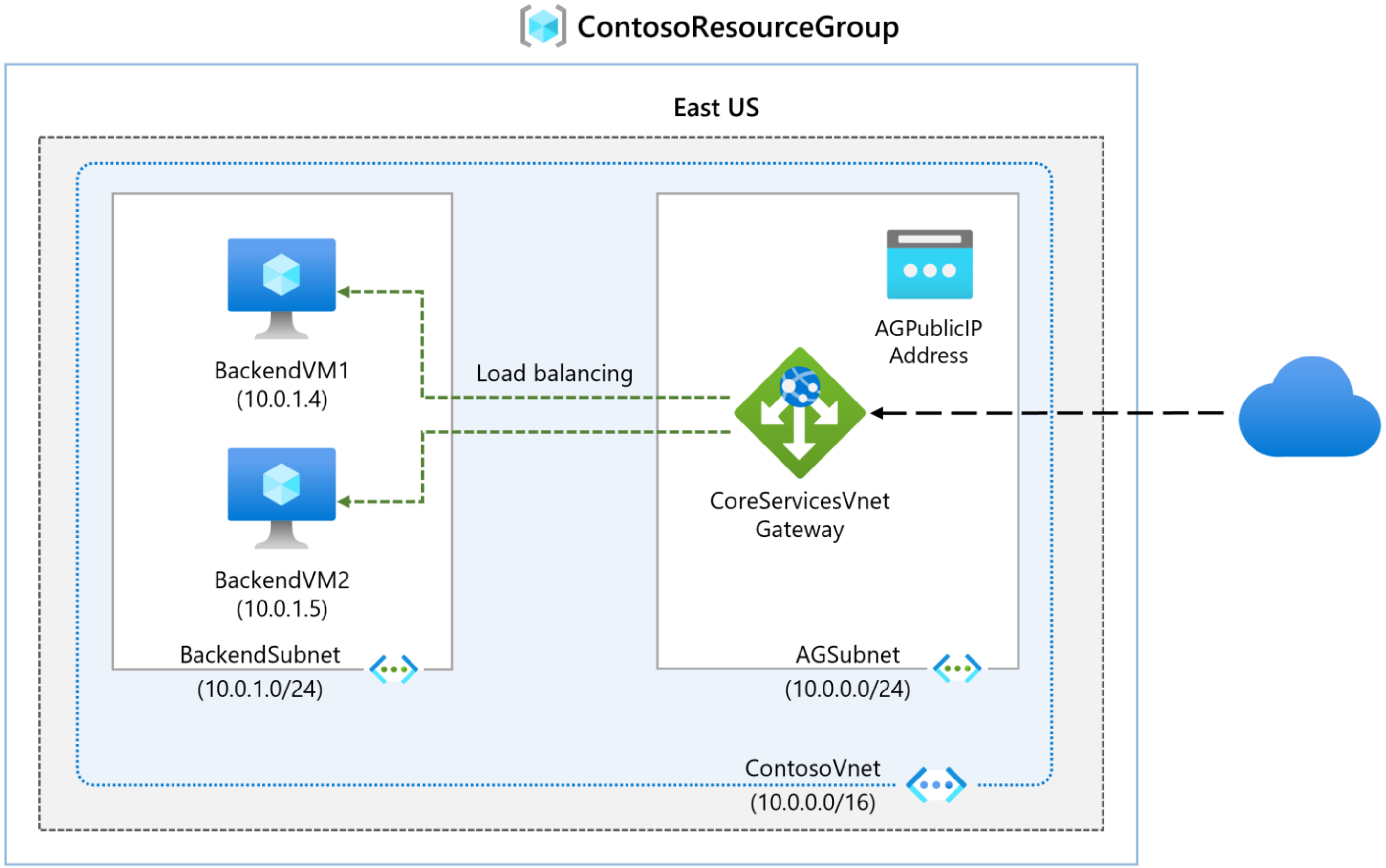
Lab 5:

Deploy Azure Application Gateway

Create a Front Door

Exercise – Deploy Azure Application Gateway

- Task 1: Create an application gateway
- Task 2: Add backend targets
- Task 3: Add backend servers to backend pool
- Task 4: Test the application gateway



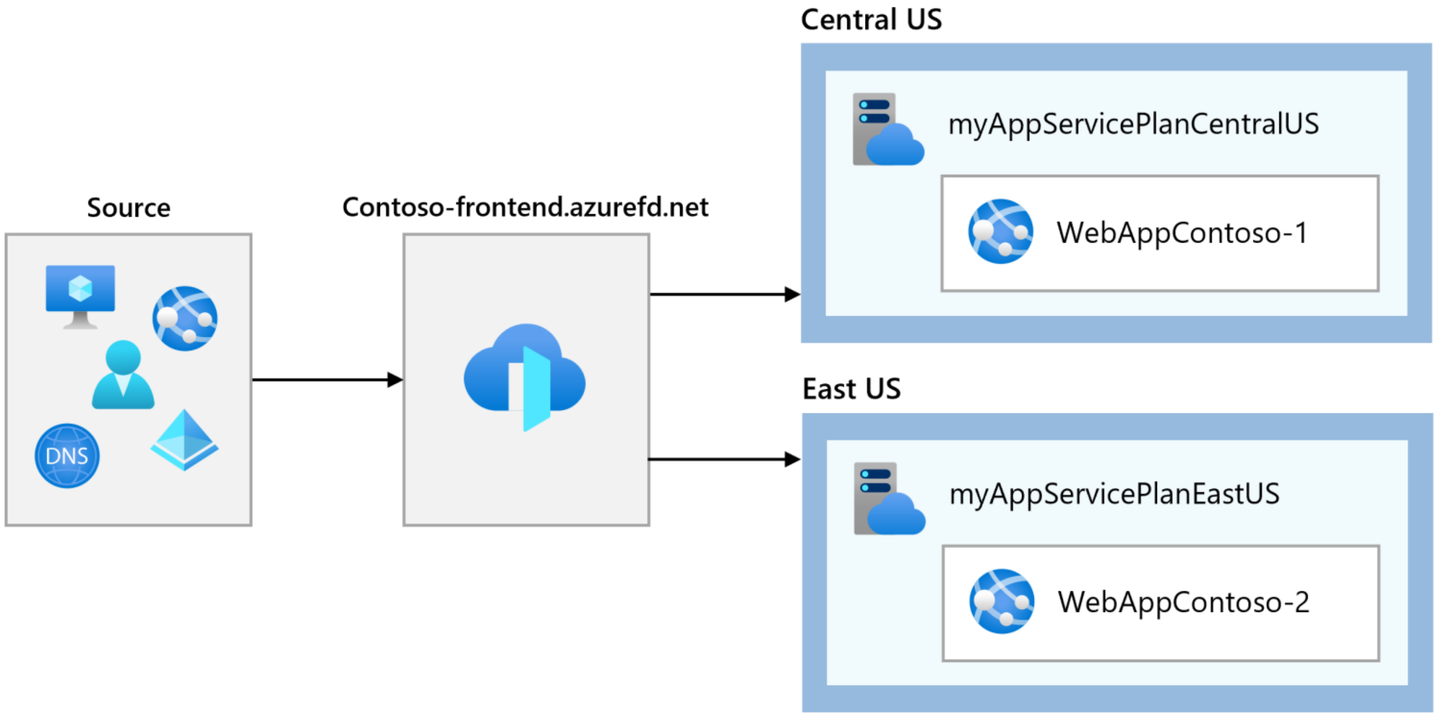
Exercise: Create a Front Door for a highly available web application

Task 1: Create two instances of a web app

Task 2: Create a Front Door for your application

Task 3: View Azure Front Door in action

Task 4: Clean up resources



End of presentation