Microsoft

AZ-700

Module 05

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

Module 06: Design and Implement Network Security

Module 07: Design and Implement private access to Azure Services

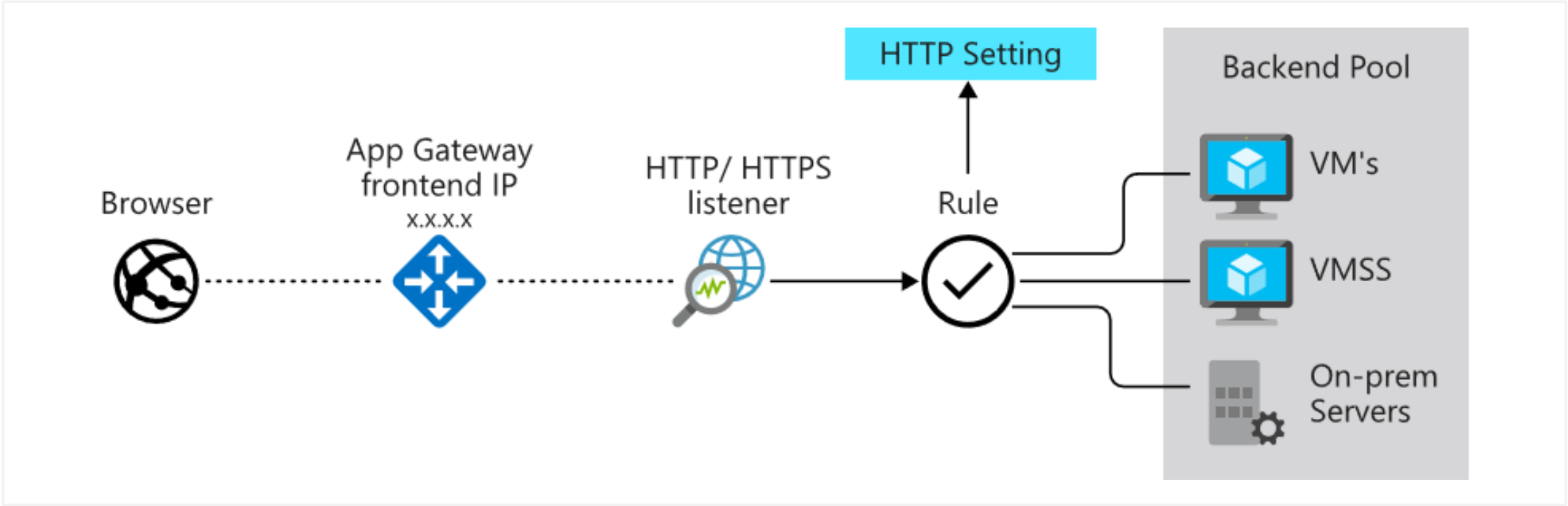
Module 08: Design and Implement Network Monitoring

Module Overview

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

Design Azure Application Gateway

Application Gateway features



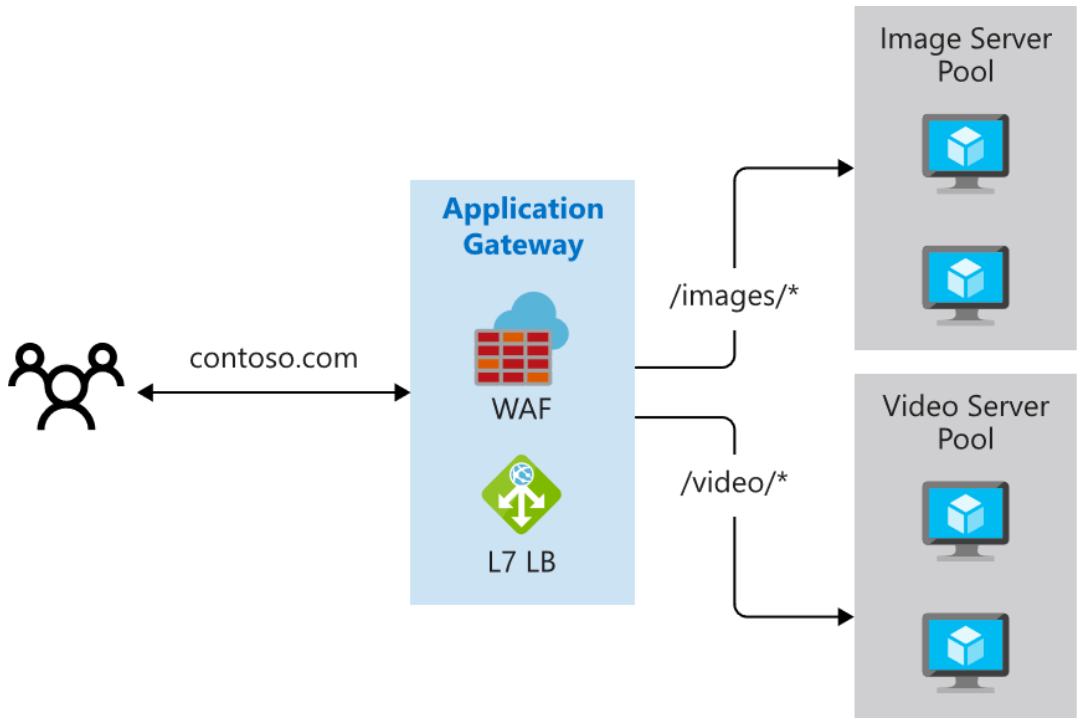
Manages web app requests

Routes traffic to a pool of web servers based on the URL of a request

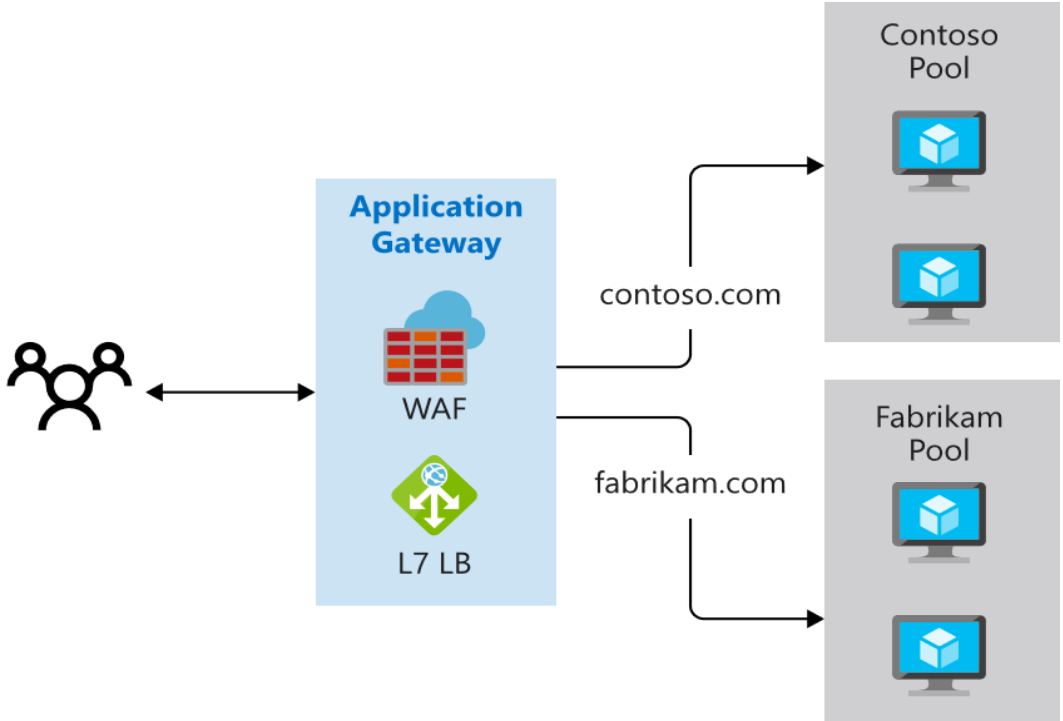
The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

Determine Application Gateway Routing

Path-based routing



Multiple-site routing



Choosing an Azure App Gateway SKU

Application Gateway Standard (V2) can be configured for **autoscaling** or **fixed size** deployments. The v2 SKU doesn't offer different instance sizes

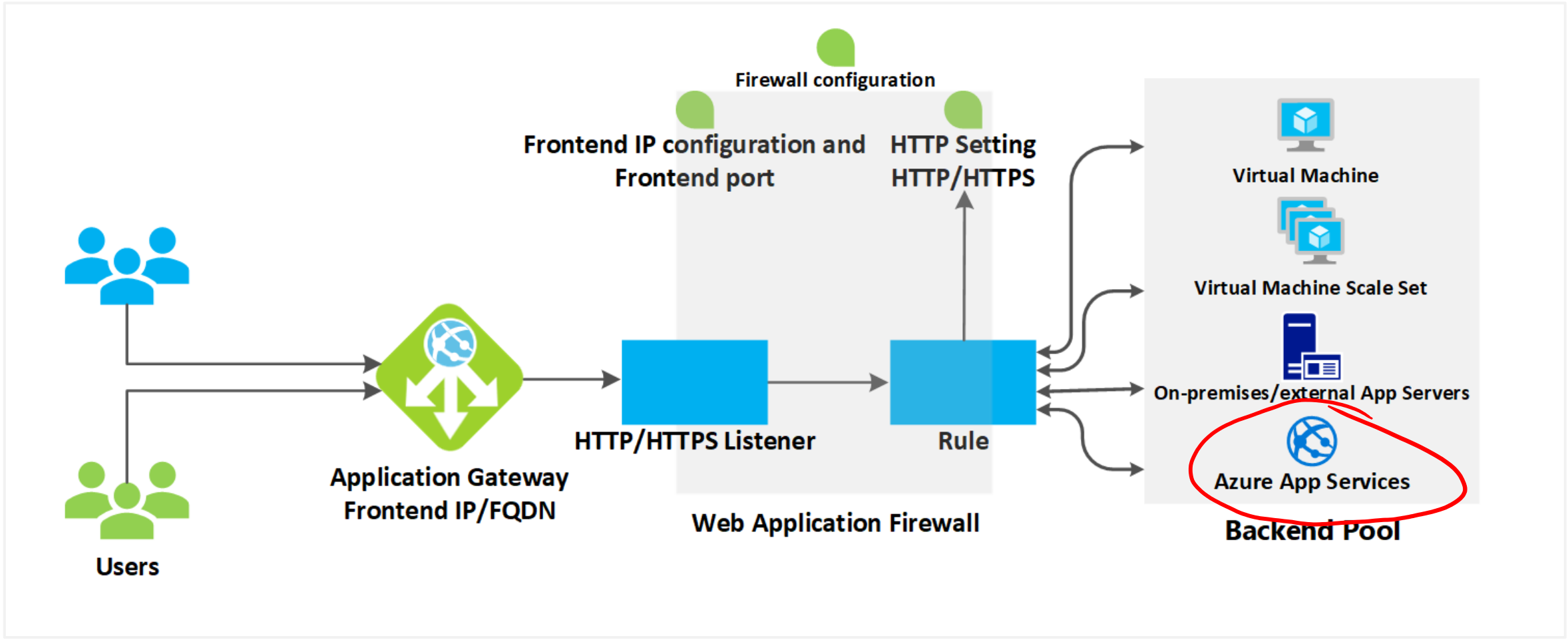
For a complete list of application gateway limits, see Application Gateway service limits

The Application Gateway Standard (V1) is offered in three sizes: **Small**, **Medium**, and **Large**. Small instance sizes are intended for development and testing scenarios.

Average back-end page response size	Small	Medium	Large
6 KB	7.5 Mbps	13 Mbps	50 Mbps
100 KB	35 Mbps	100 Mbps	200 Mbps

ed.

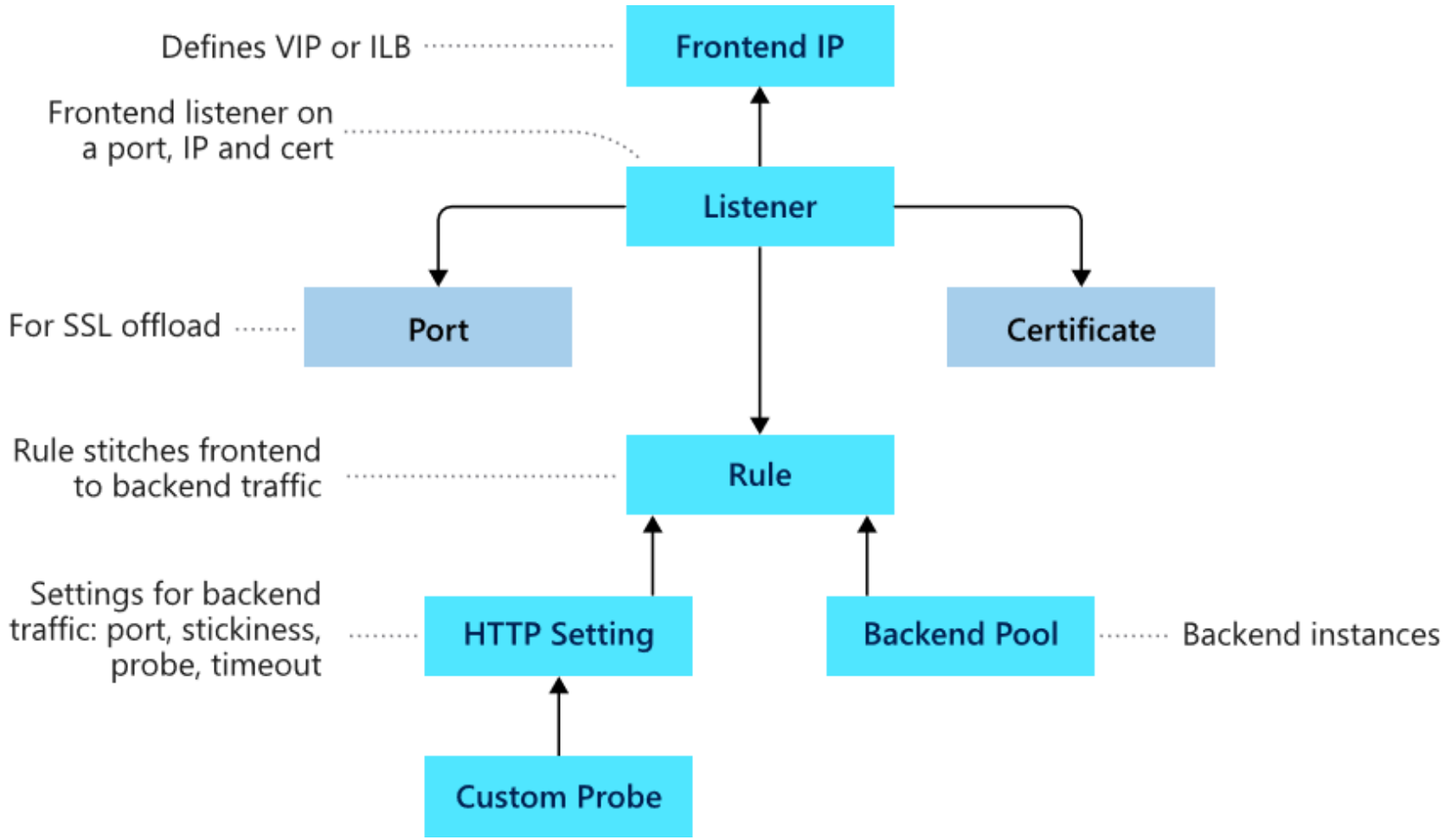
Application Gateway configuration planning



Configure Azure Application Gateway

Configure Application Gateway

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

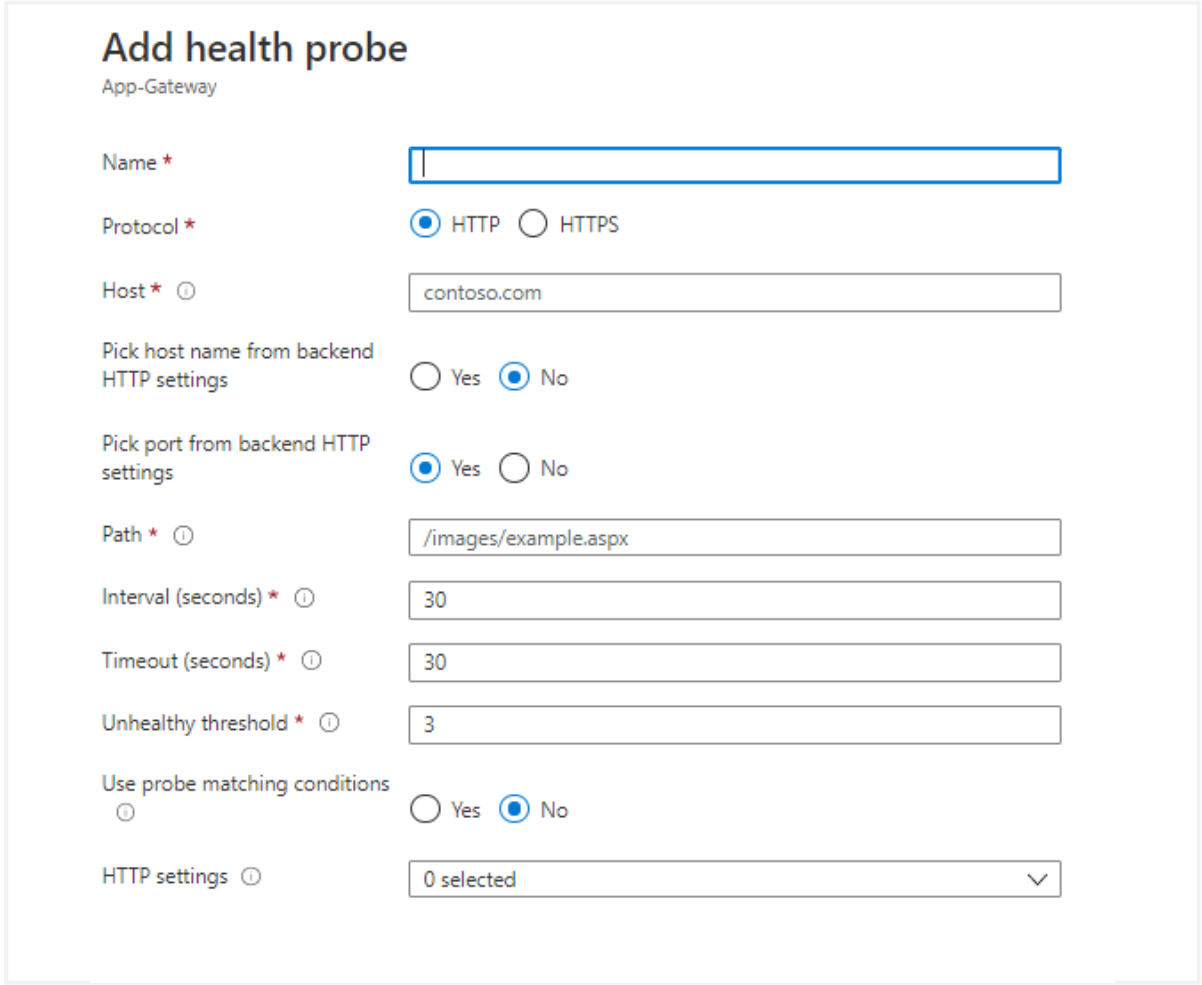


Configure health probes

Default health probe

Custom health probe

Probe matching



Configure listeners

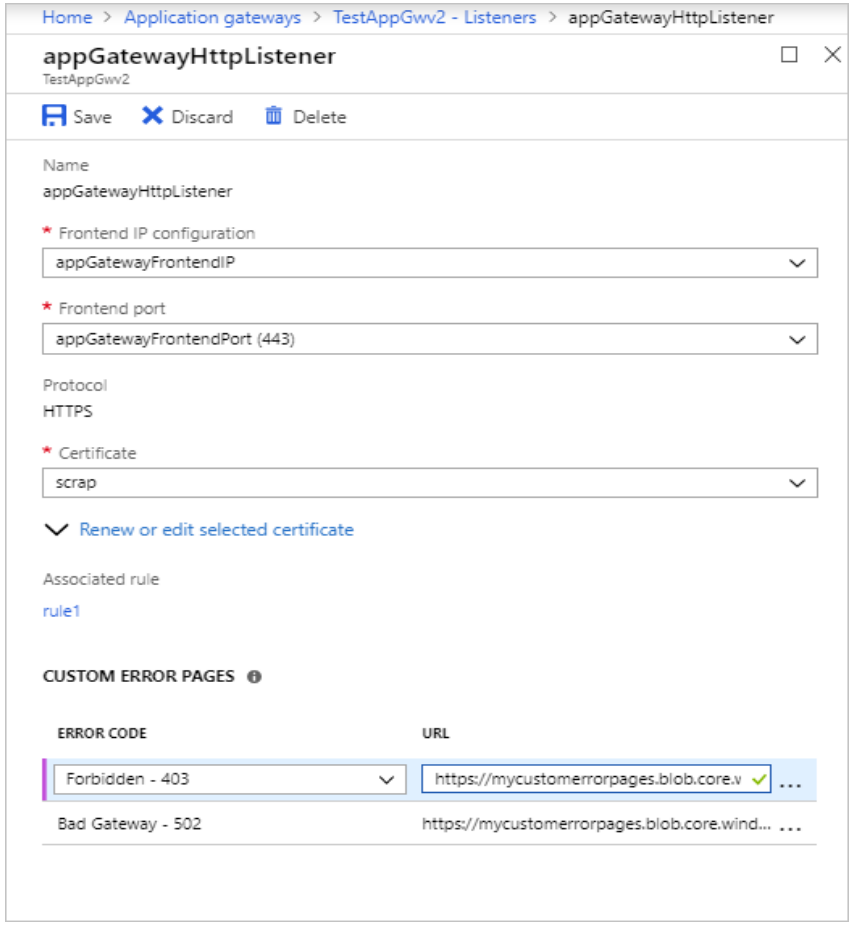
Basic or Multi Site

Order of Processing Listeners

Frontend IP address

Frontend Port

Protocol HTTP or HTTPS



Redirection overview

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

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.

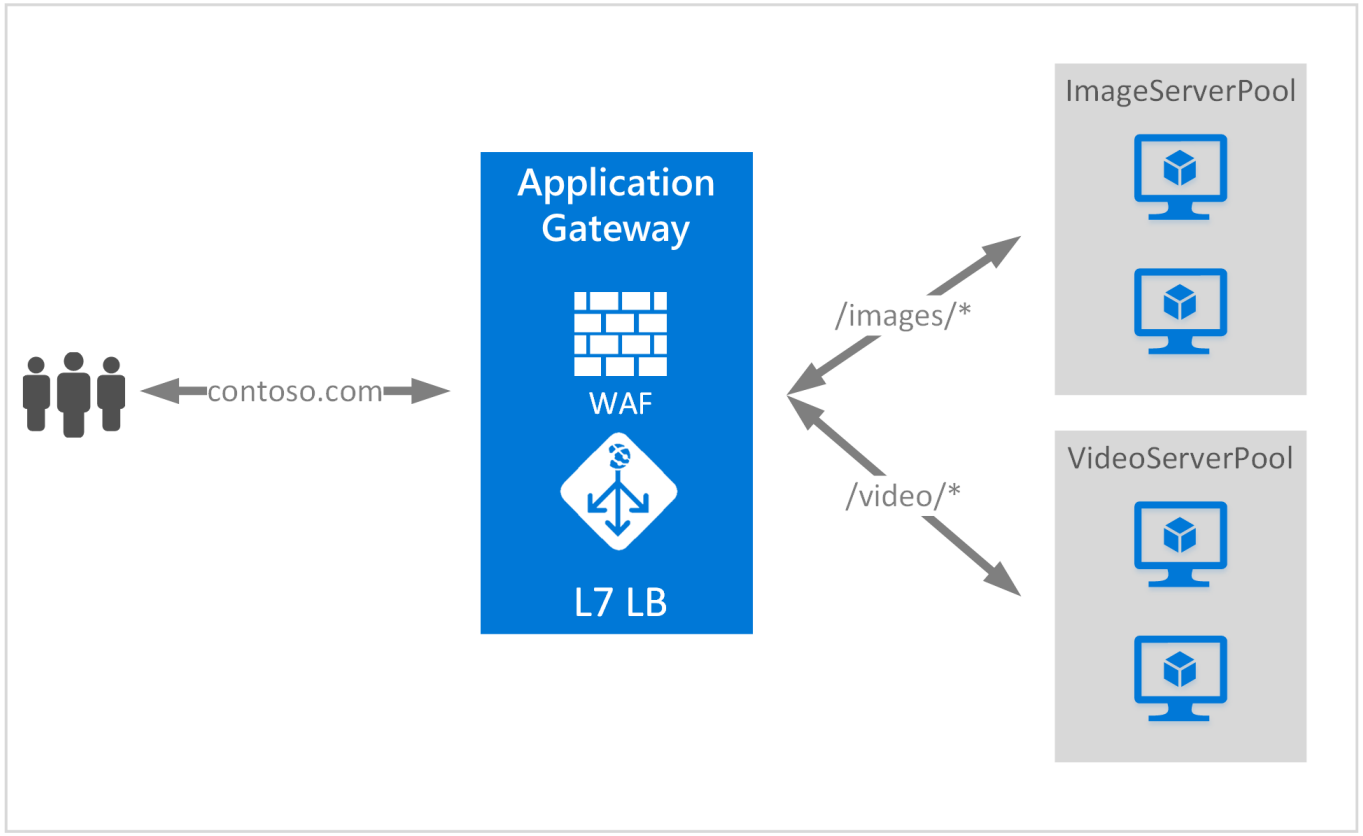
Associated back-end pool

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

path-based rule: add multiple back-end pools that correspond to each URL path. The requests that match the URL path that's entered 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

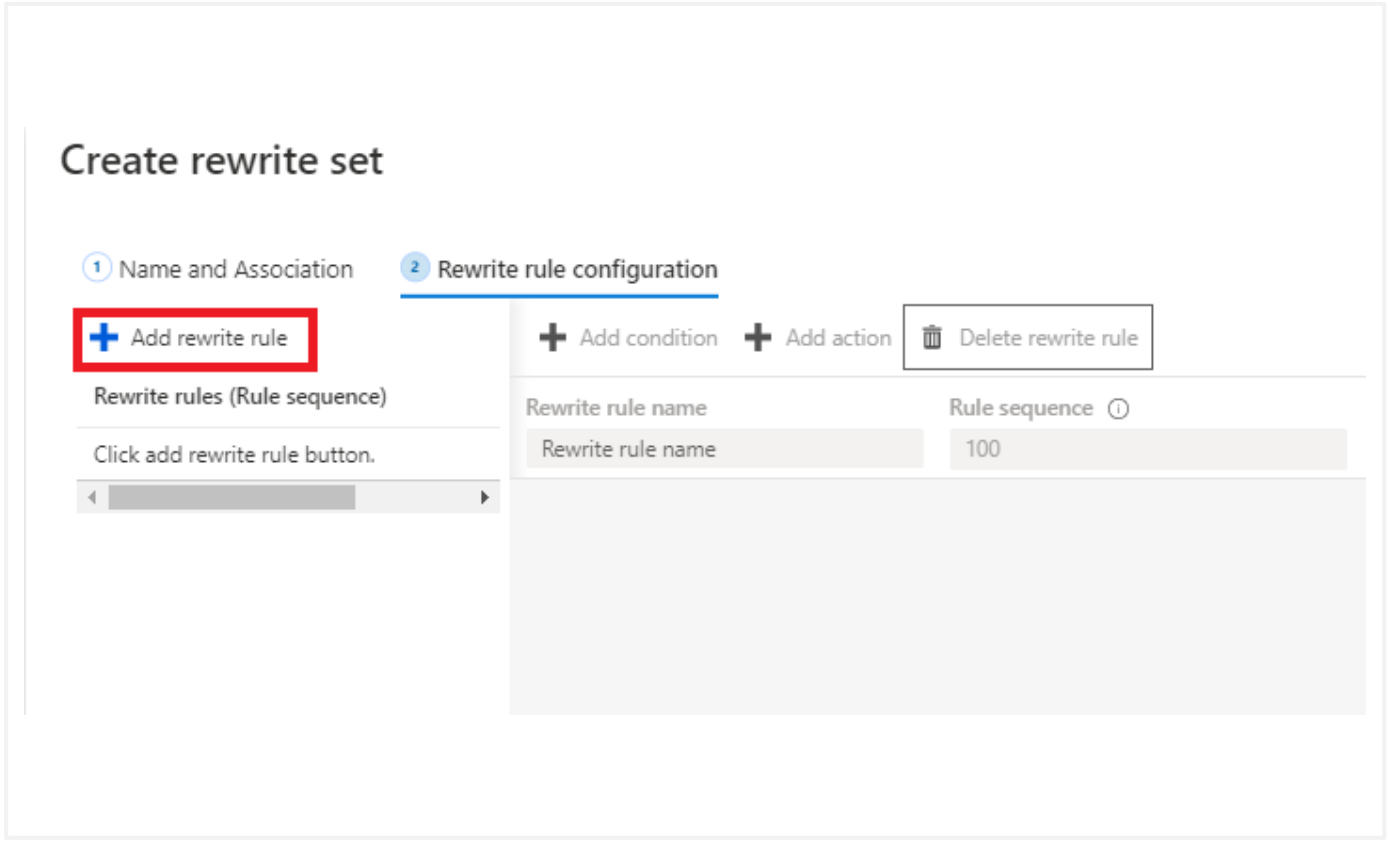
A rewrite rule set contains:

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**



Design and configure Azure Front Door

What is Azure Front Door

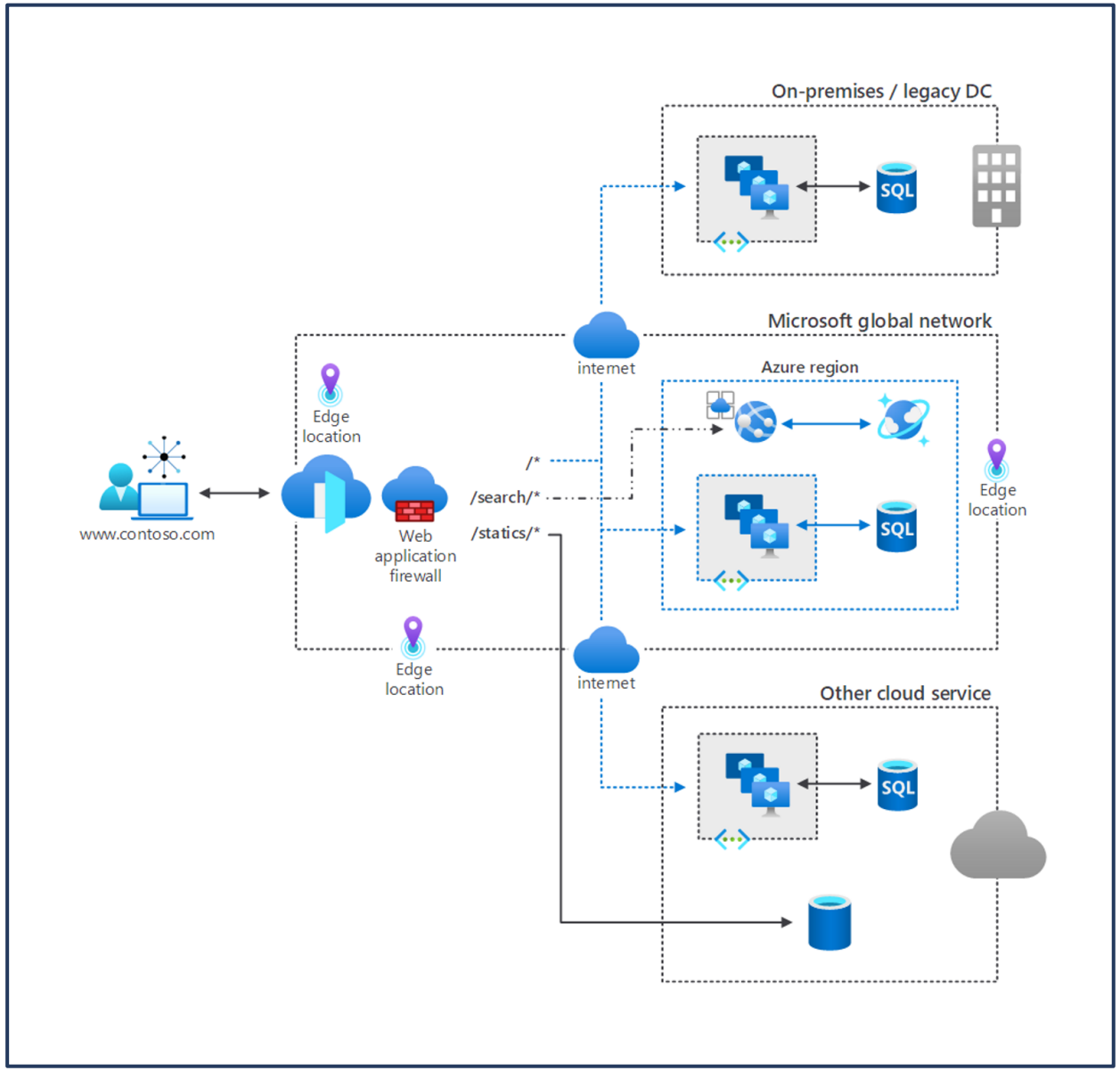
Global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications

Accelerated application performance by using split TCP-based anycast protocol

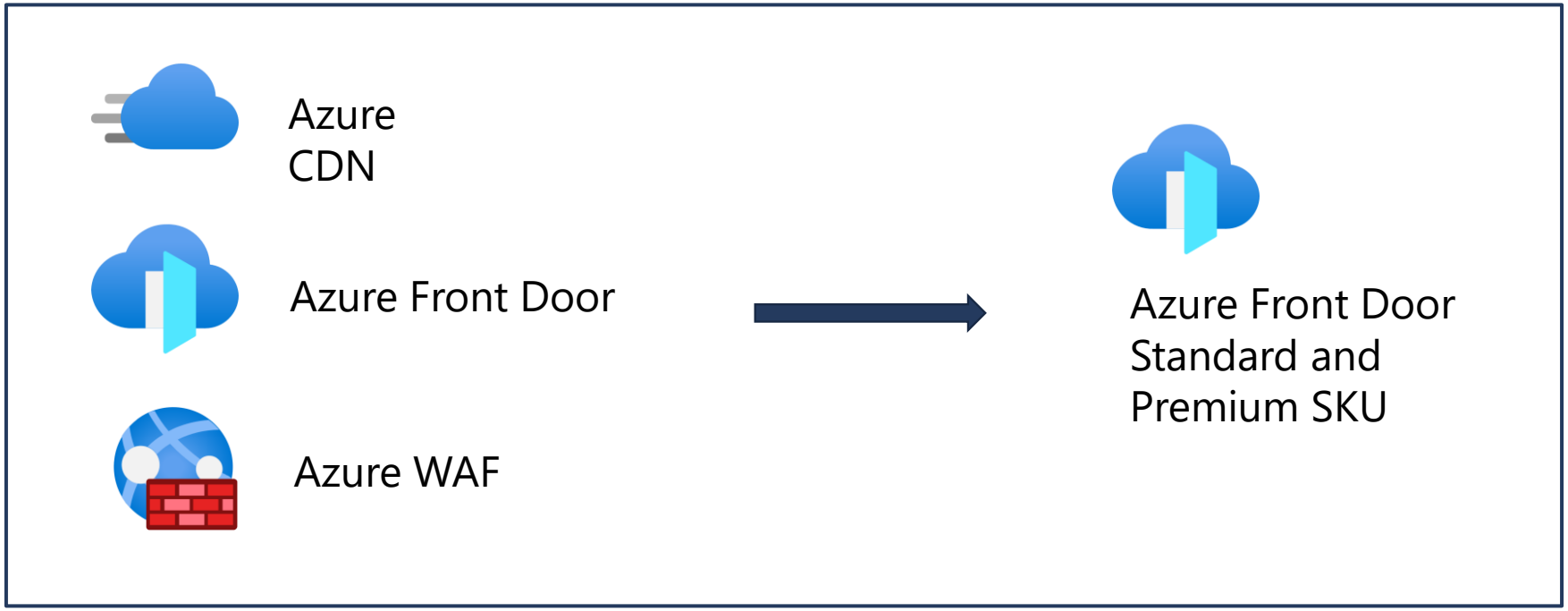
Intelligent health probe monitoring for backend resources

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 is:

- Content delivery optimized
- Offering both 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.

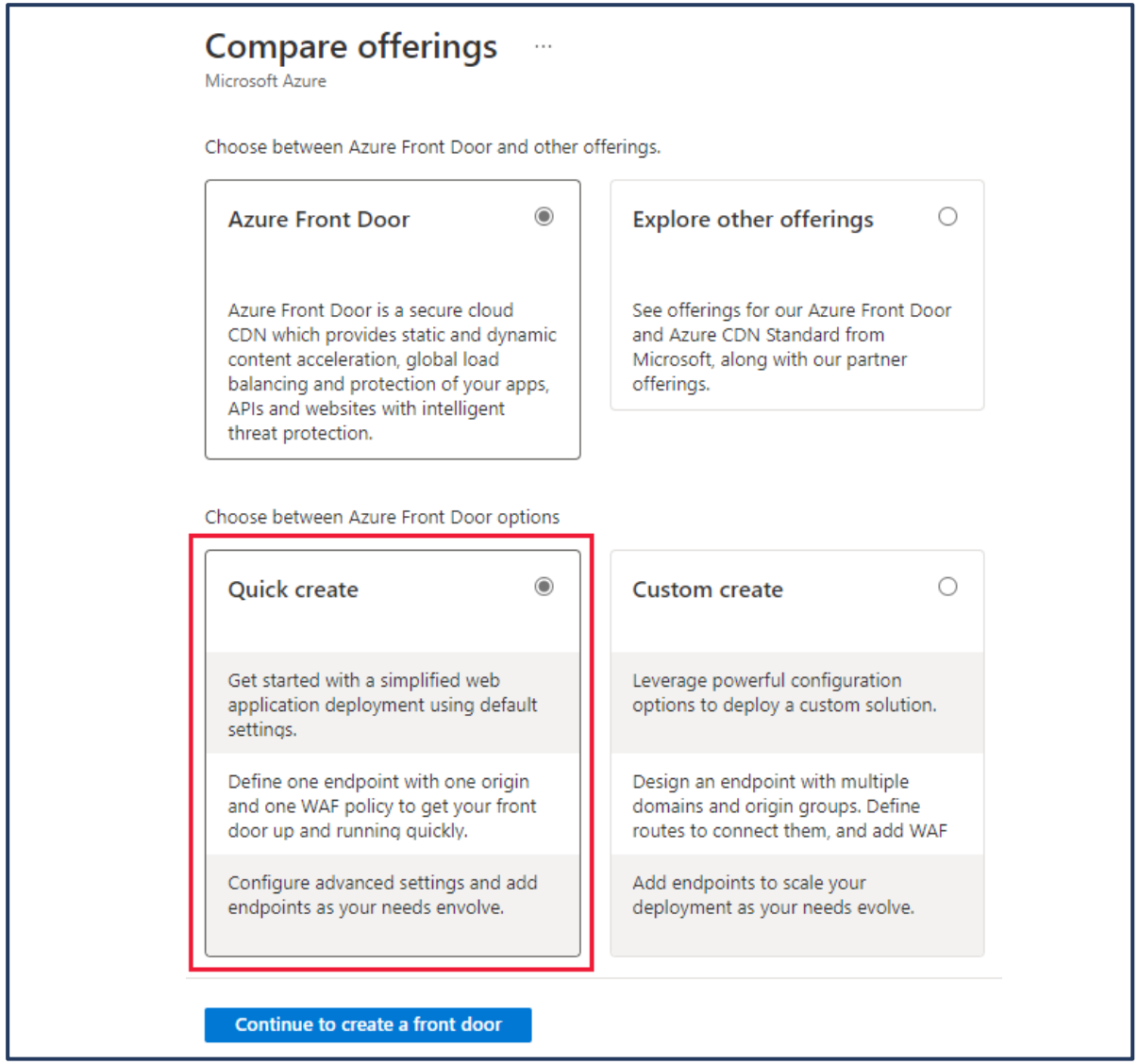
Create a Front Door in the Azure portal

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



Configure routing and redirection rules

Routing architecture overview

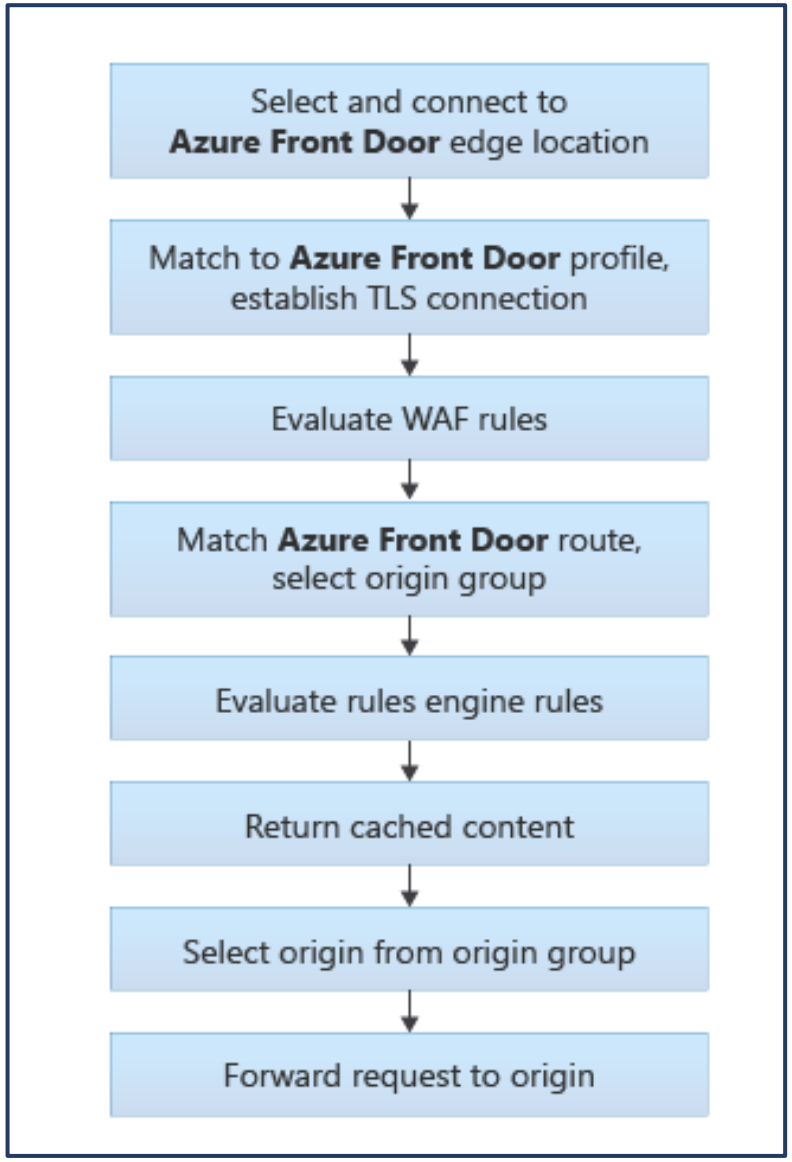
Front Door matches the incoming request to the left-hand side of the route. The right-hand side defines how Front Door processes the request

Incoming match (left-hand side)

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

Route data (right-hand side)

The decision of how to process the request, depends on whether caching is enabled or not for the specific route



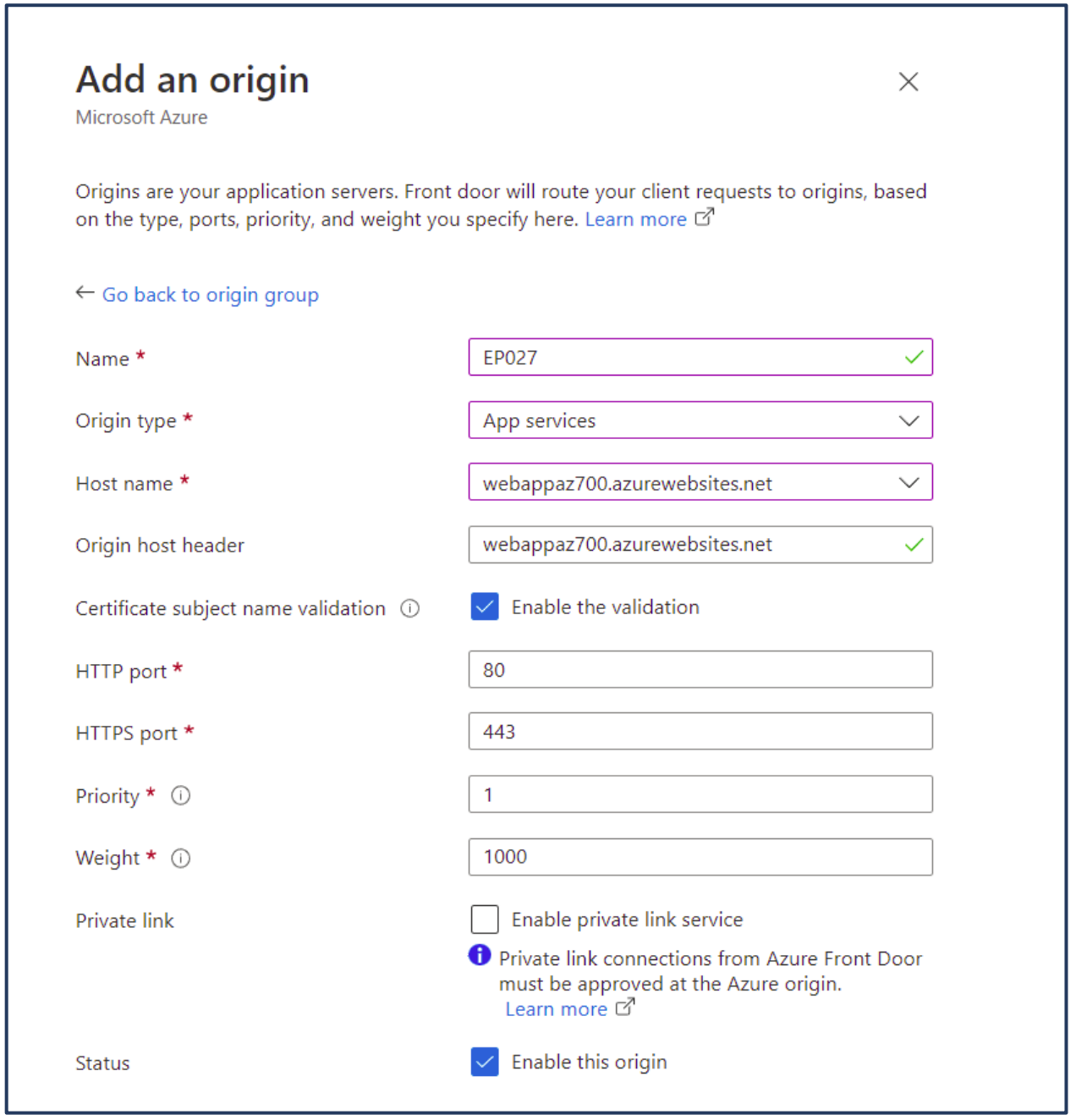
Configure an Origin (Backend)

Origin type

Host name

Origin host header

HTTP & HTTPS port

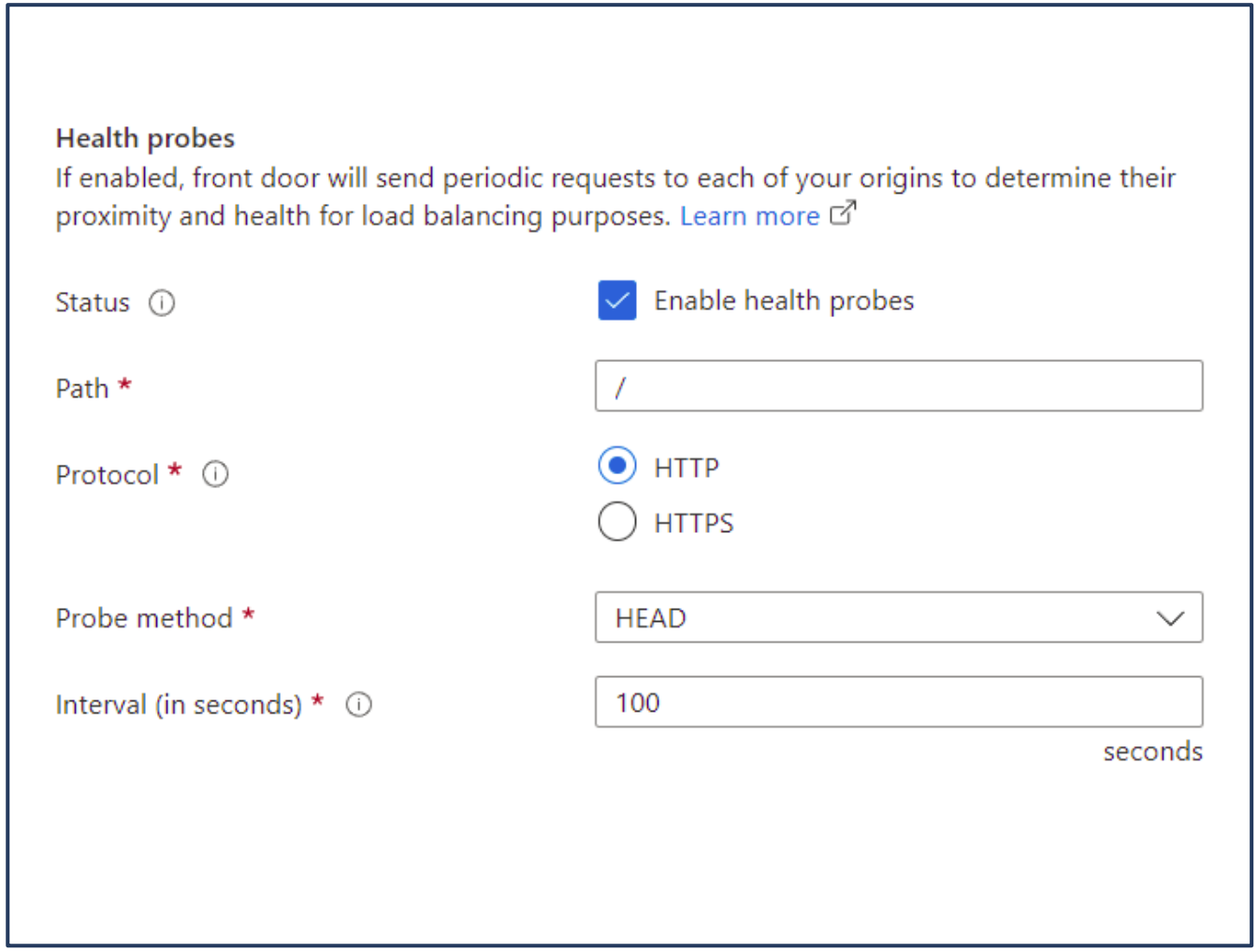


Configure health probes

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.



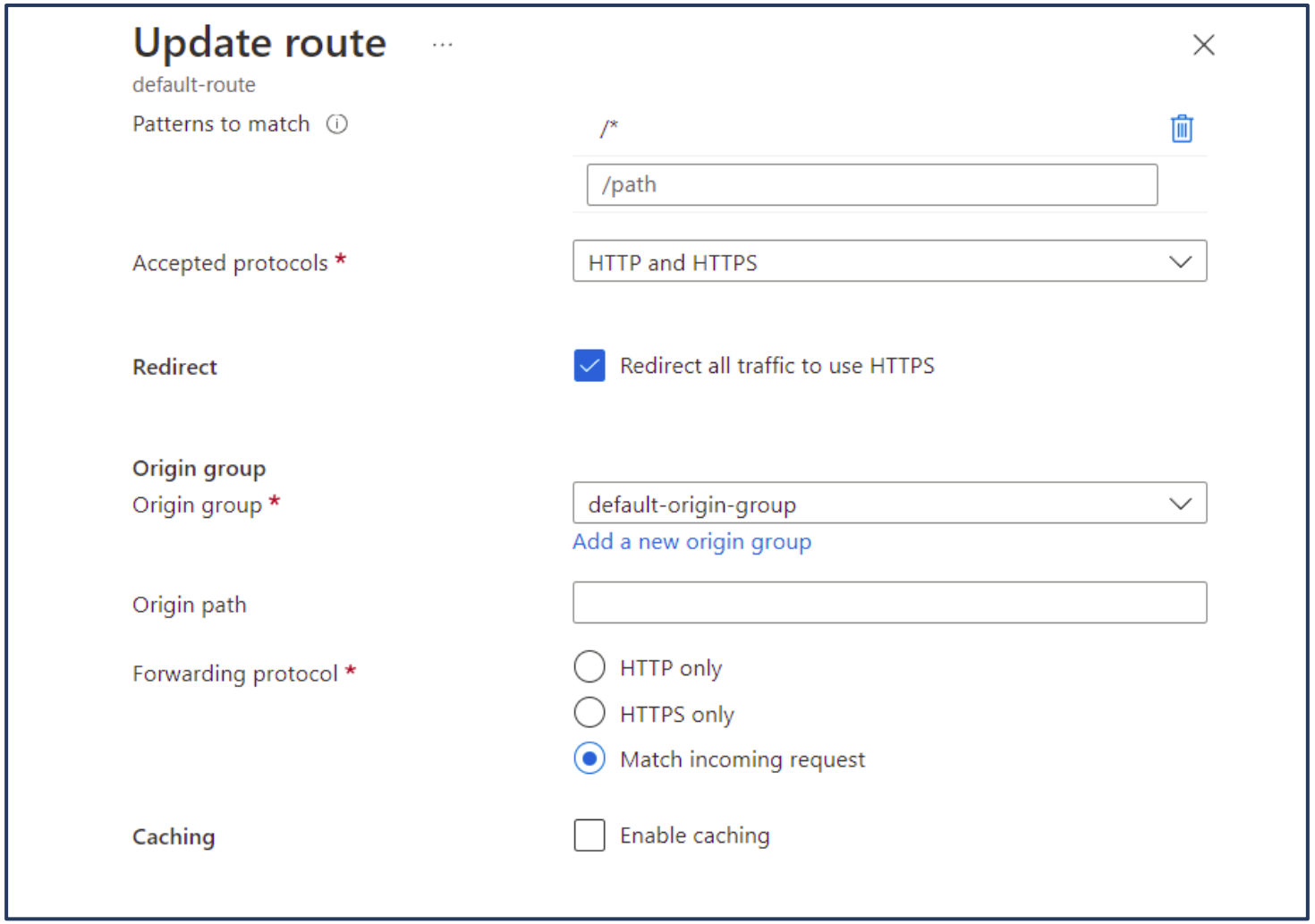
Secure Front Door with SSL and end-to-end SSL encryption

Create HTTP to HTTPS redirect rule

Create a routing rule for HTTP to HTTPS redirect

Add routing rule to handle the HTTPS traffic

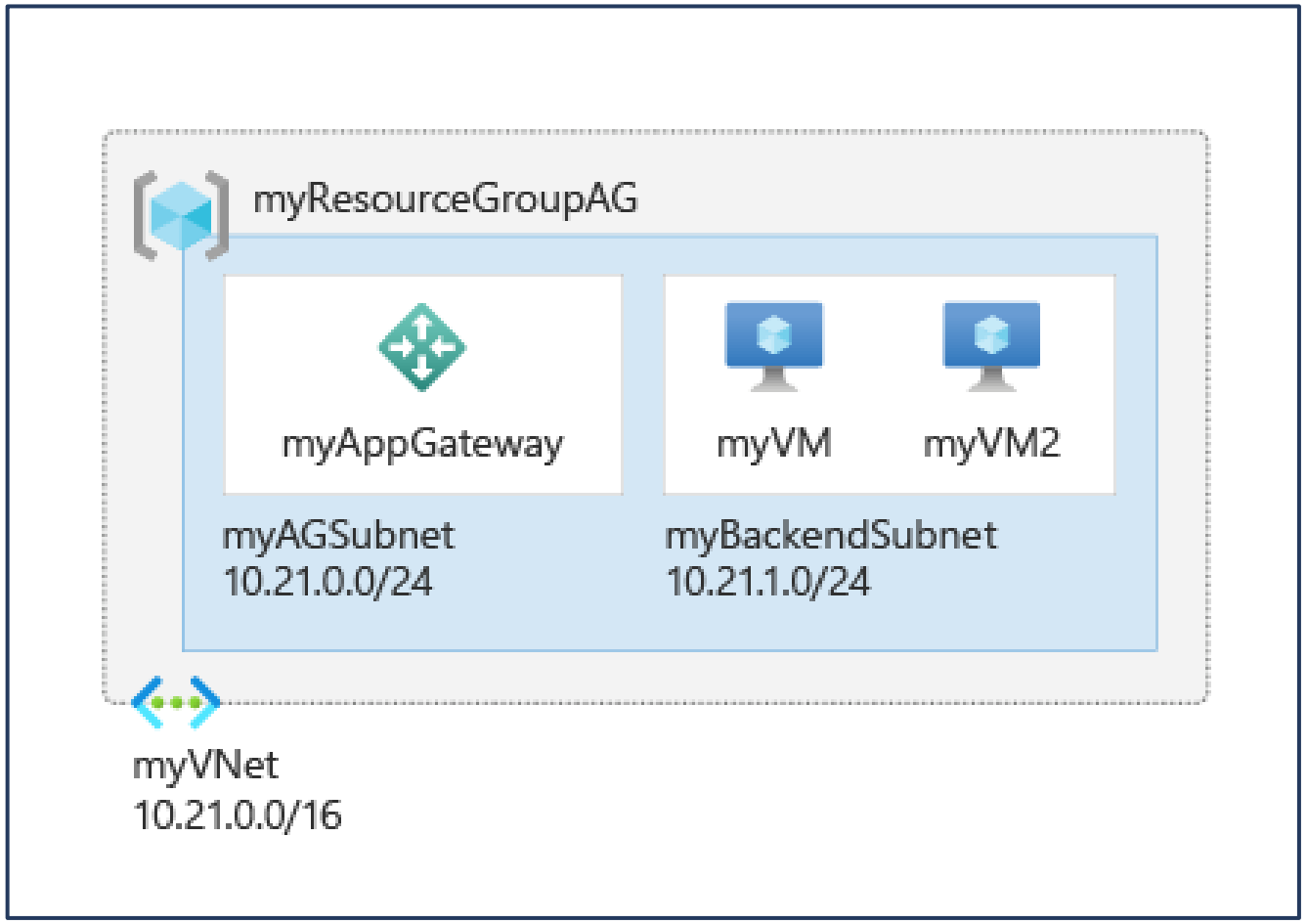
On the Route Details section, set the Route Type to Forward.



Exercise: Deploy Azure Application Gateway

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

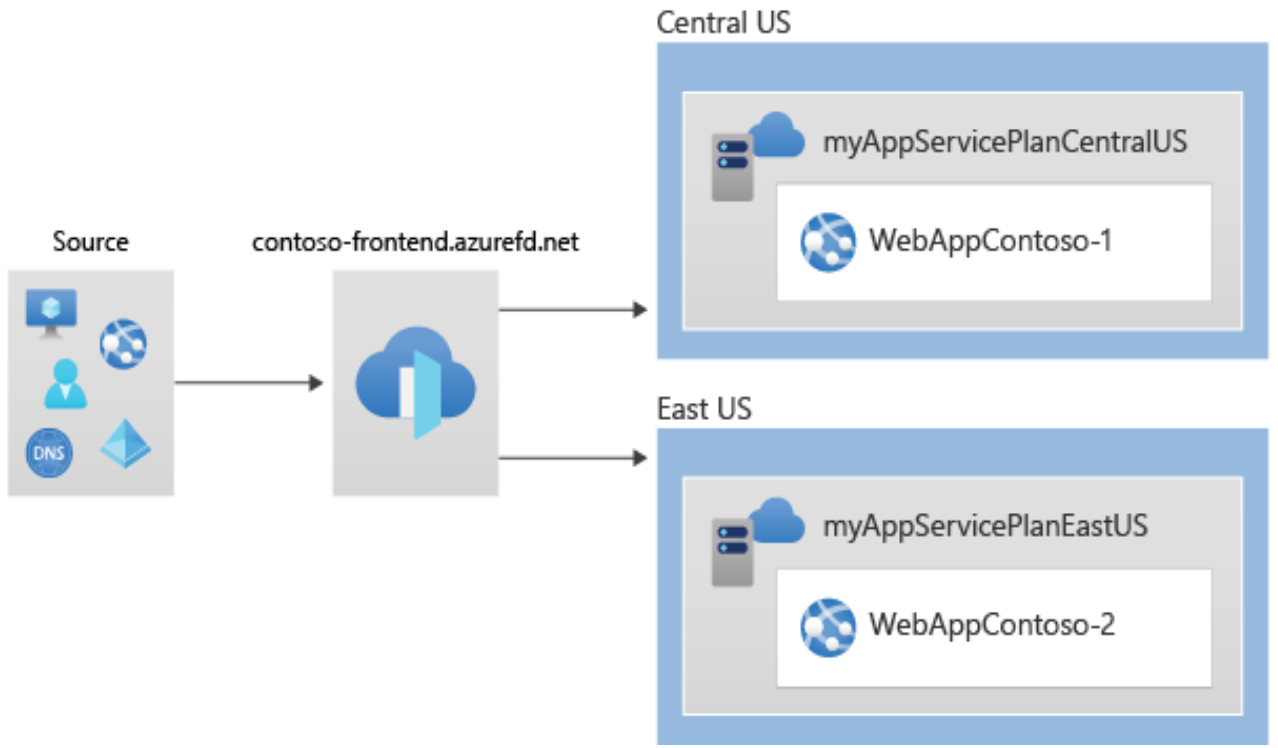
Exercise: create a Front Door for a highly available web application

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