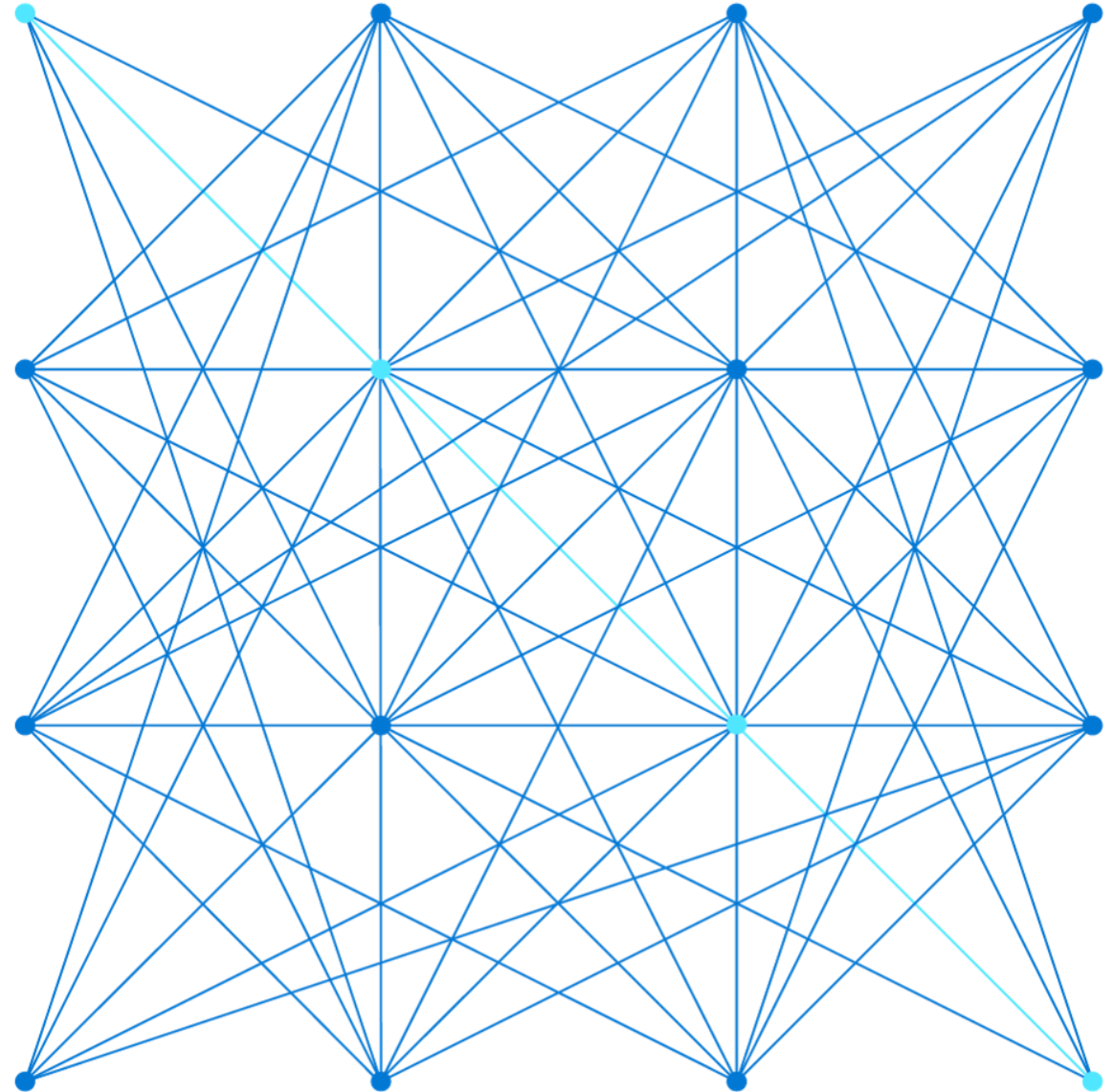# AZ-700

Load balancing
HTTP(S) traffic in Azure

Course 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

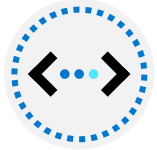Module 08: Design and Implement Network Monitoring

Module Overview

WAF

Regional

Design Azure Application Gateway

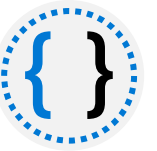Configure Azure Application Gateway

Exercice: deploy Azure Application Gateway

Global
+ CDN

Design and configure Azure Front Door

Exercise: create a Front Door for highly available web application using the Azure portal
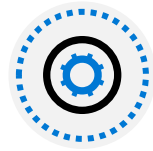
Design Azure Application Gateway

Design Azure Application Gateway overview
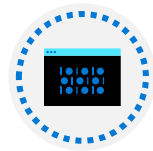
Application Gateway features

Determine Application Gateway Routing

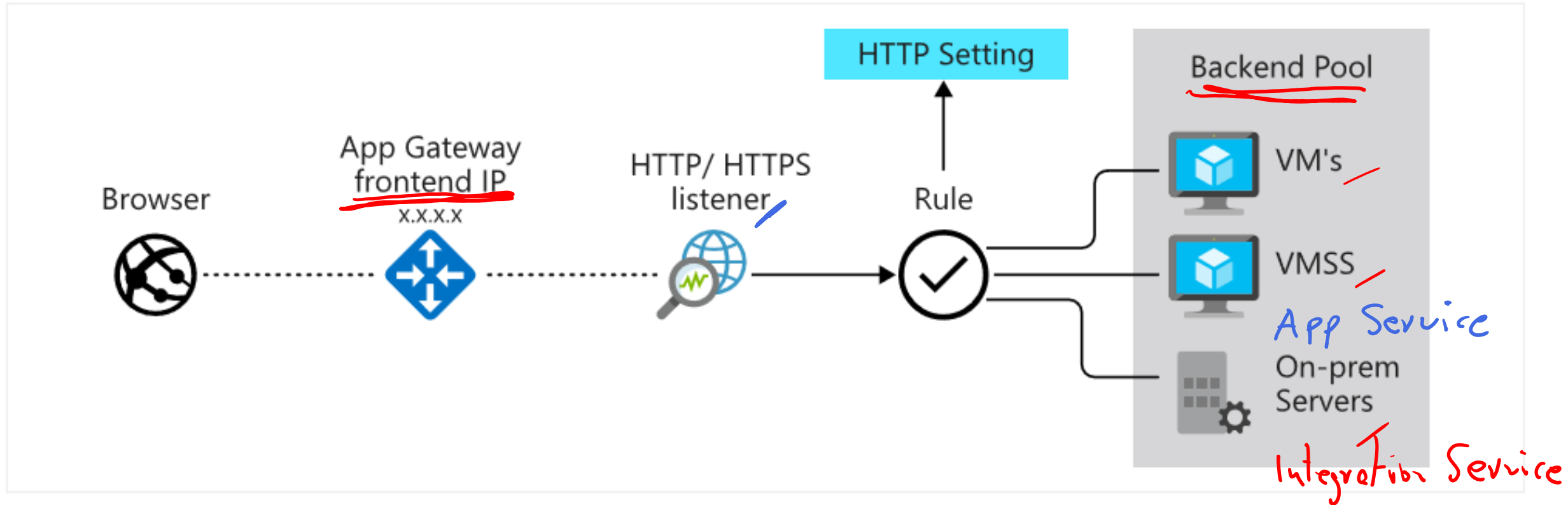Choosing an Azure App Gateway SKU

Application Gateway configuration planning

Review

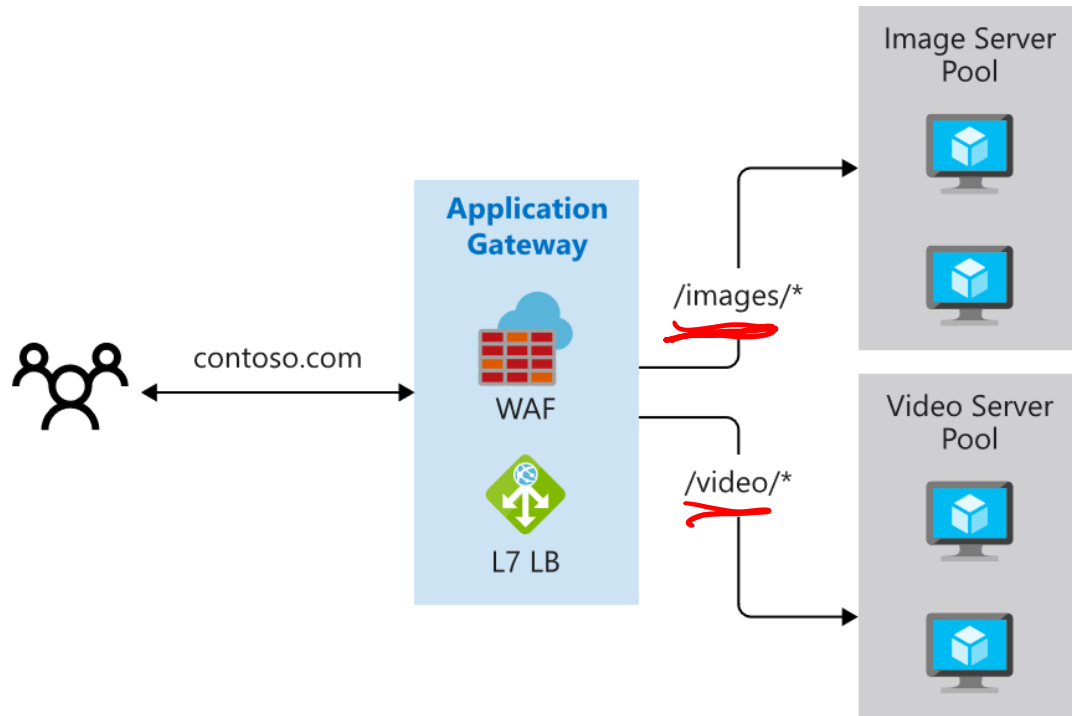# Application Gateway features

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

URL Rewriting

Path-based routing	Multiple-site routing

Path-based routing panel: Users connect via contoso.com to the Application Gateway (WAF, L7 LB). Requests matching /images/* route to the Image Server Pool, and requests matching /video/* route to the Video Server Pool.

Multiple-site routing panel: Users connect to the Application Gateway (WAF, L7 LB). Requests for contoso.com route to the Contoso Pool, and requests for fabrikam.com route to the Fabrikam Pool.
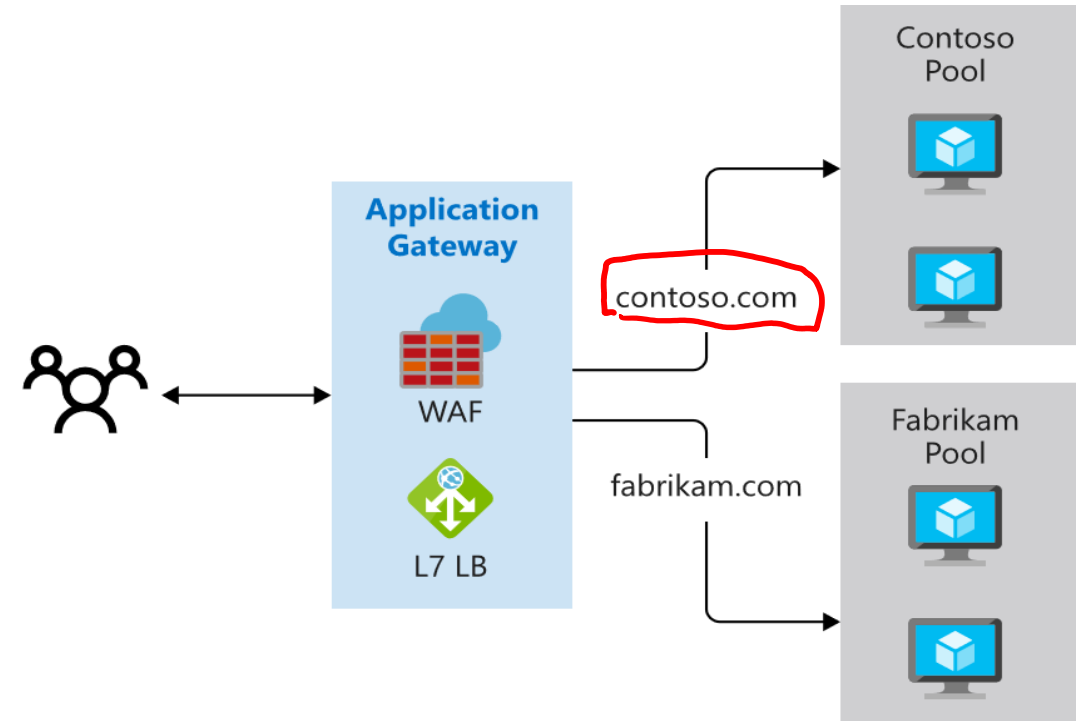
Choosing an Azure App Gateway SKU

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

Application Gateway configuration planning
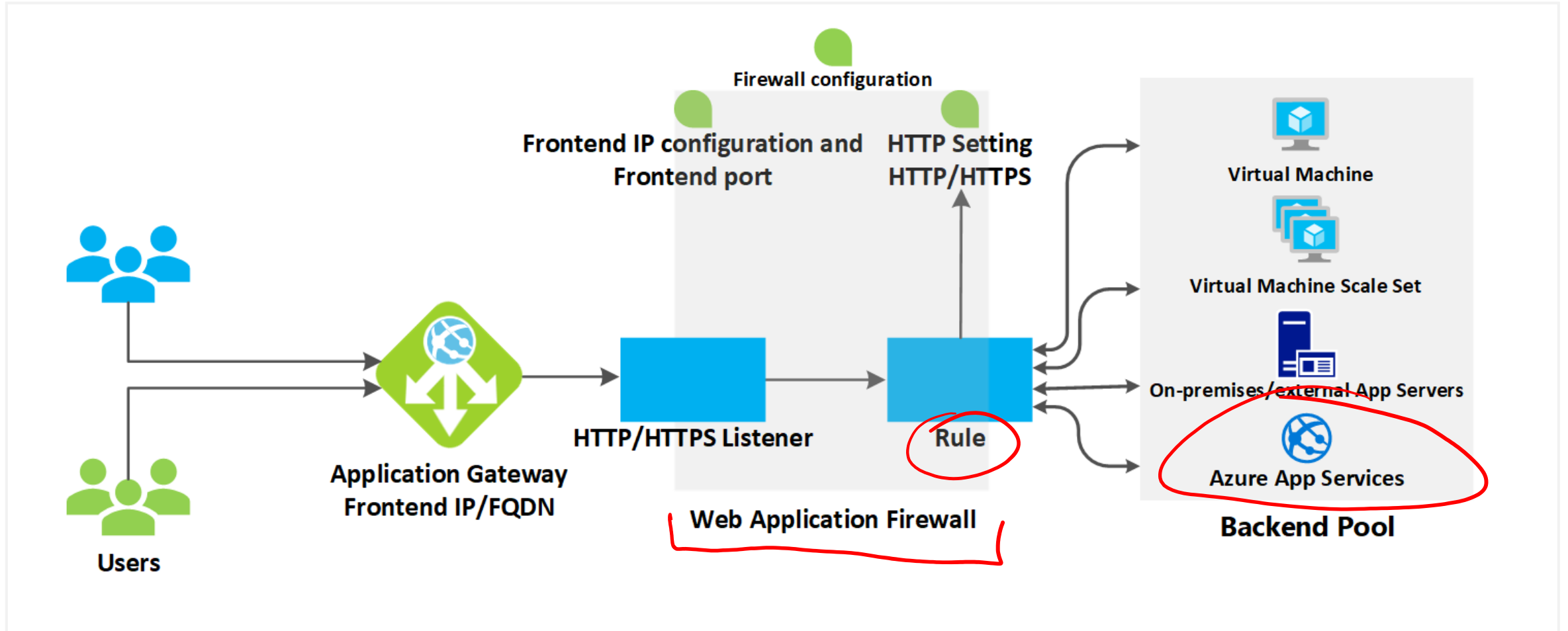
Summary – Design Azure Application Gateway

Check your knowledge	Microsoft Learn Modules (docs.microsoft.com/Learn)

[What is Azure Application Gateway | Microsoft Docs](#)

[Load balance your web service traffic with Application Gateway - Learn | Microsoft Docs](#)

Configure Azure Application Gateway

Configure Azure Application Gateway overview

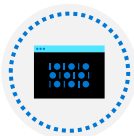Configure Application Gateway

Configure Health Probes

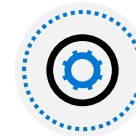Configure Listeners

Redirection Overview

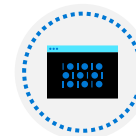Application Gateway Request routing rules

Associated back-end pool

Configure URL-based routing

Configure rewrite policies

Demonstration

Review

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
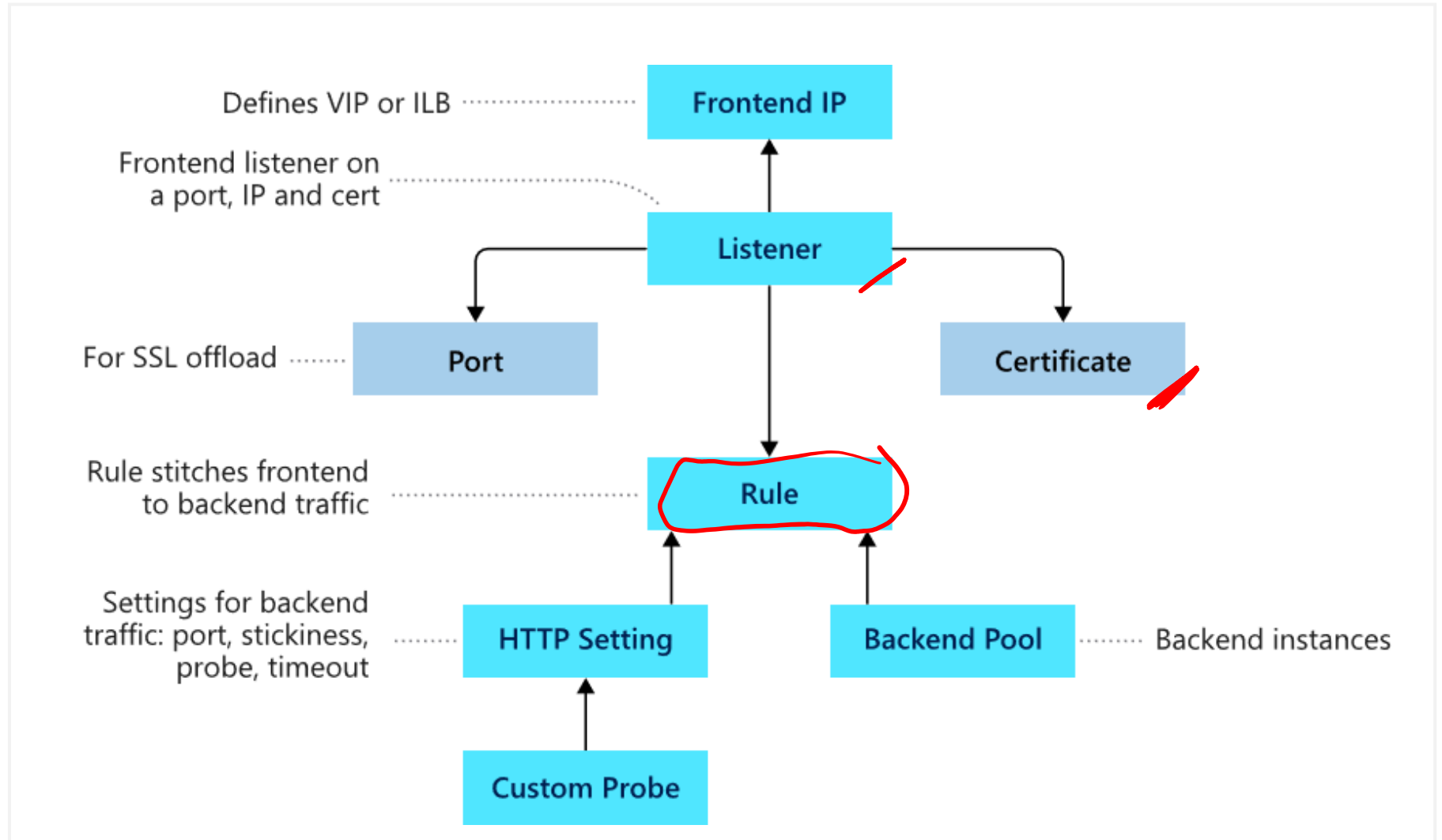
Custom Probe

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

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

contoso.com

Application Gateway

WAF

L7 LB

ImageServerPool

/images/*

VideoServerPool

/video/*
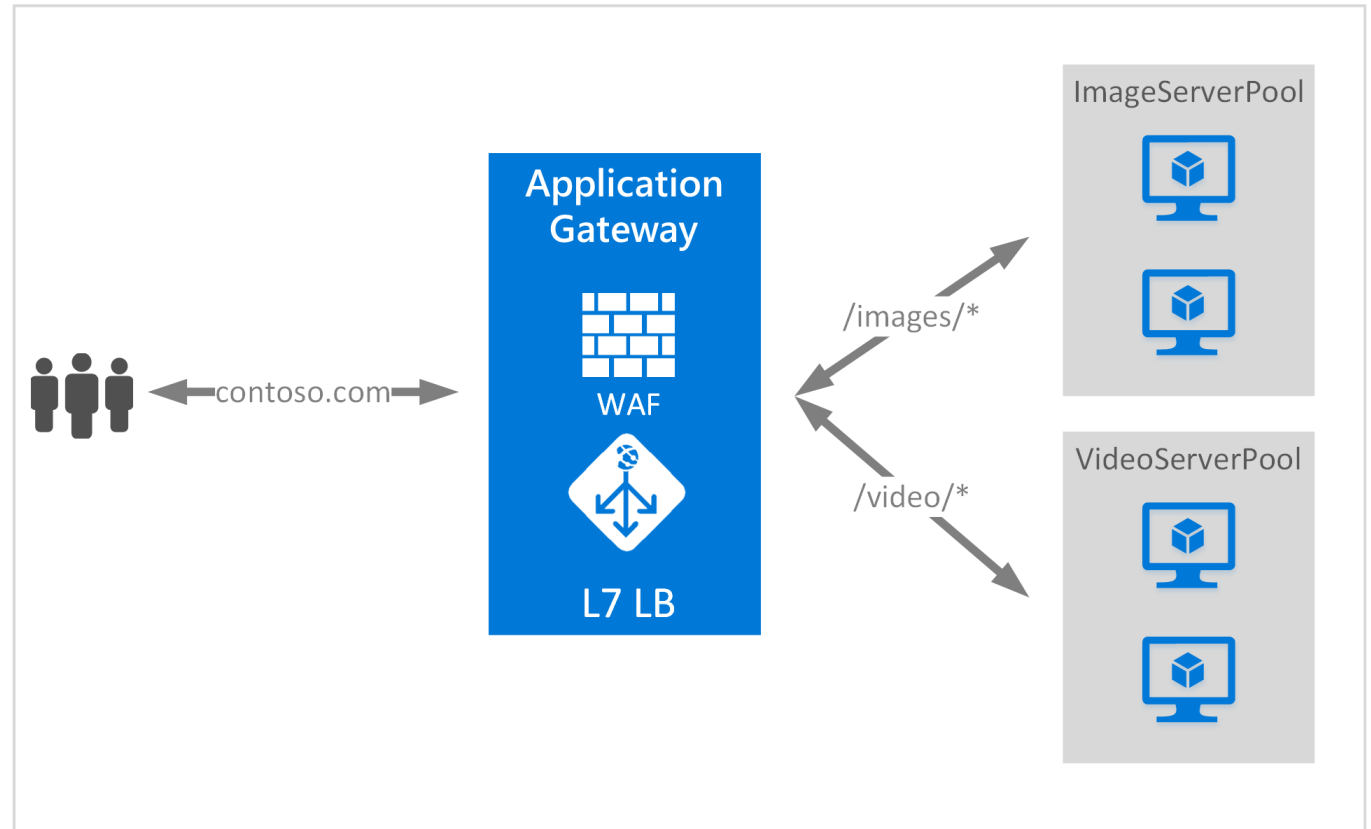
Configure rewrite policies

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

① Name and Association   ② Rewrite rule configuration

➕ Add rewrite rule   ➕ Add condition   ➕ Add action   🗑 Delete rewrite rule

Rewrite rules (Rule sequence)   Rewrite rule name   Rule sequence ⓘ

Click add rewrite rule button.   Rewrite rule name   100

Demo
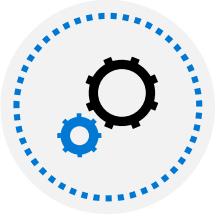
Create an application gateway

- -

Add backend targets

- -

Test the application gateway

Summary – Configure Azure Application Gateway

Check your knowledge	Microsoft Learn Modules (docs.microsoft.com/Learn)

[Azure Application Gateway documentation | Microsoft Docs](#)

- -

[What is Azure Application Gateway | Microsoft Docs](#)

- -
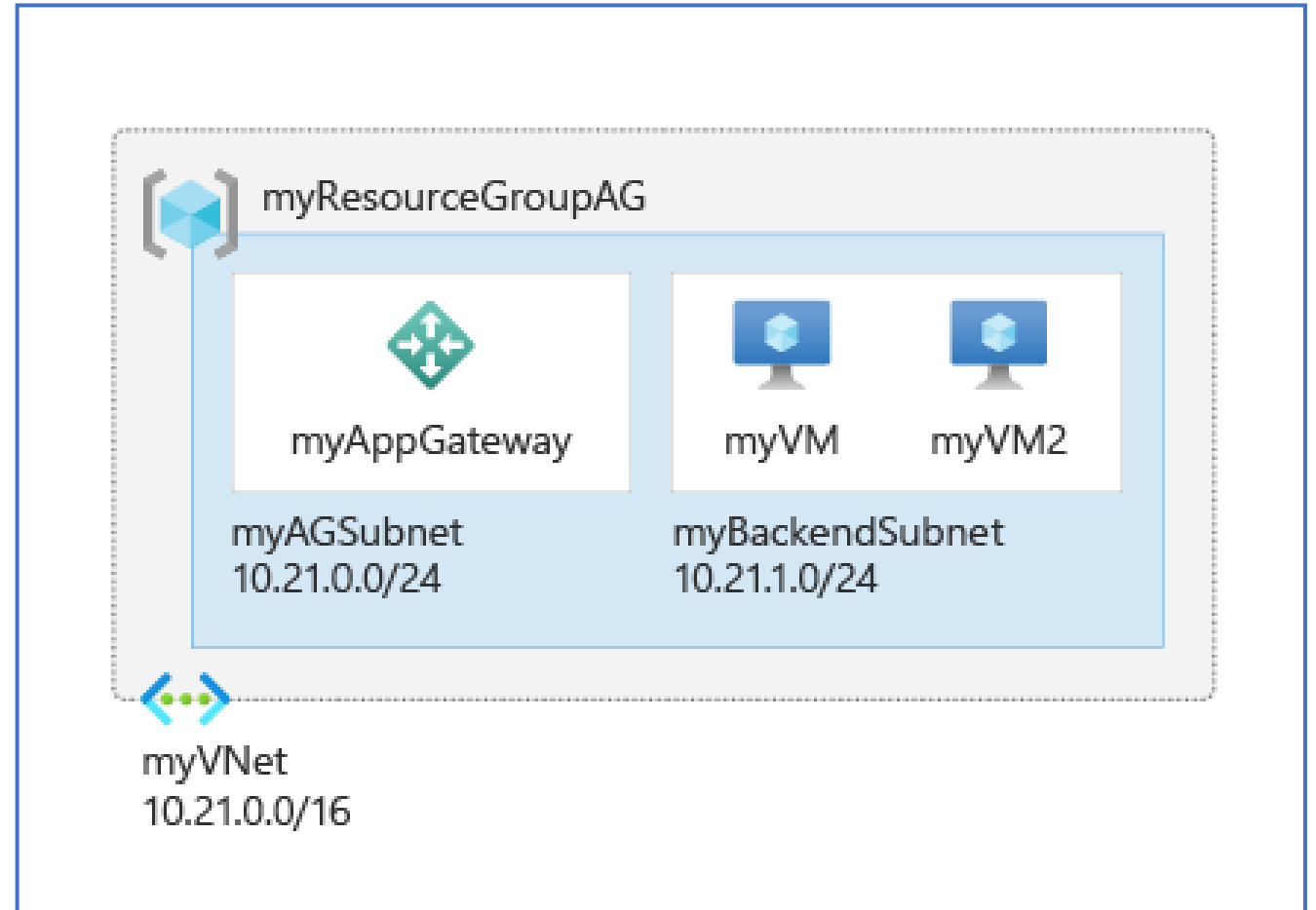
Exercise: deploy Azure Application Gateway

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

myResourceGroupAG

myAppGateway

myVM   myVM2

myAGSubnet
10.21.0.0/24

myBackendSubnet
10.21.1.0/24

myVNet
10.21.0.0/16

Summary – deploy Azure Application Gateway

Check your knowledge	Microsoft Learn Modules (docs.microsoft.com/Learn)

What is Azure Application Gateway | Microsoft Docs

- -

Quickstart: Direct web traffic using the portal - Azure Application Gateway | Microsoft Docs

Design and configure Azure Front Door

Design and configure Azure Front Door overview
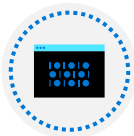
What is Azure Front Door

Azure Front Door Standard and Premium

Create a Front Door in the Azure portal

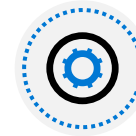Configure routing and redirection rules

Configure an origin (Backend)

Configure health probes

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

Demo

Review
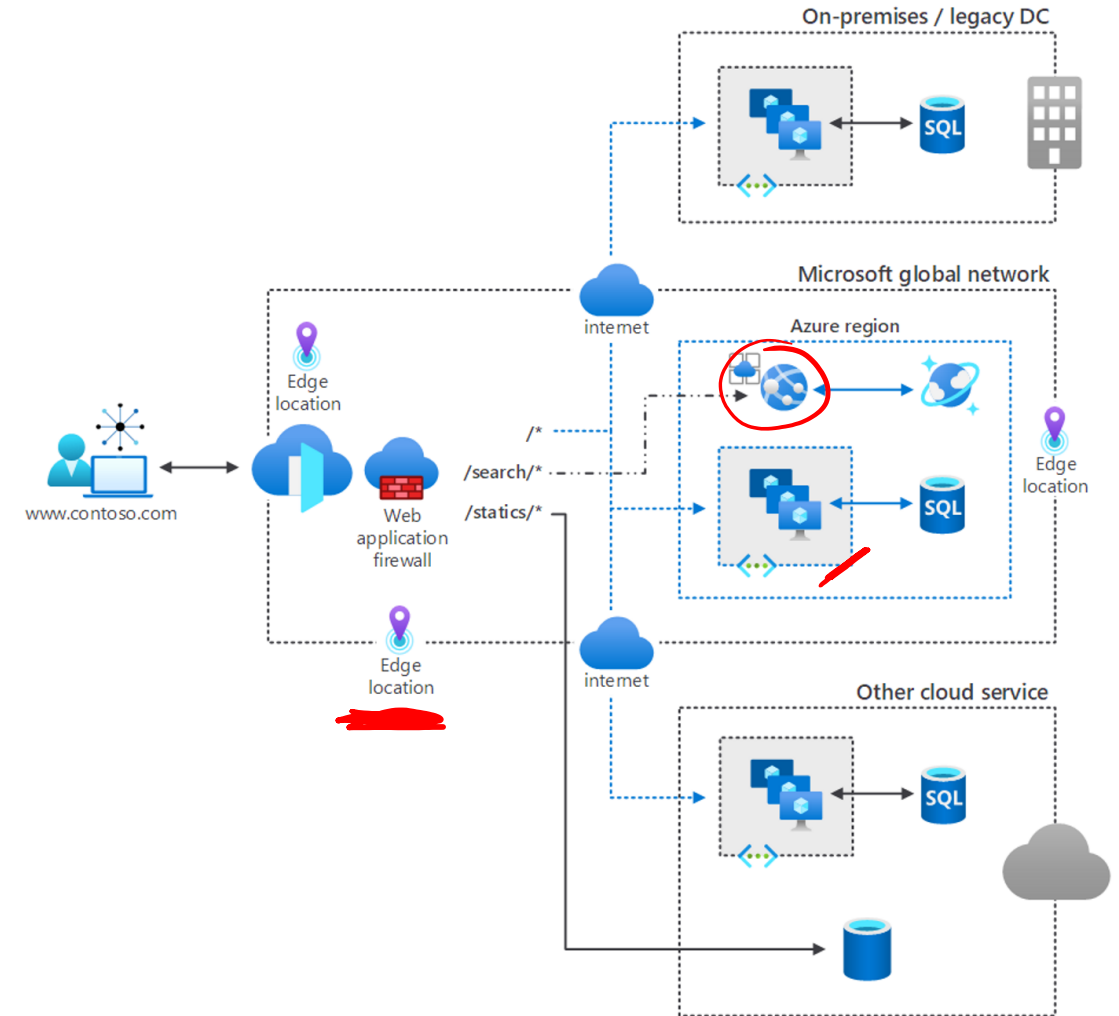
What is Azure Front Door

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

Akamai

Azure CDN

Azure Front Door

Azure WAF

→ Azure Front Door Standard and Premium SKU
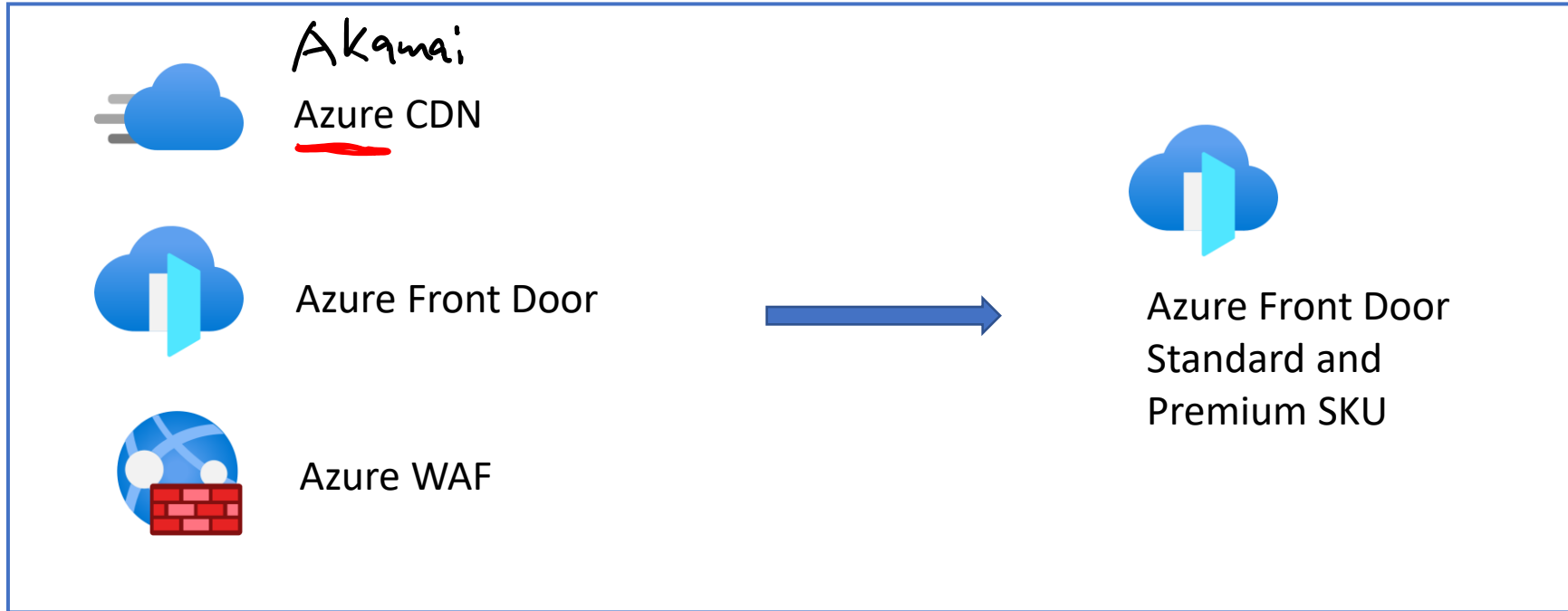
Azure Front Door Standard SKU is:
- Content delivery optimized
- Offering both static and dynamic content acceleration
- Global load balancing
- SSL offload
- Domain and certificate management
- Enhanced traffic analytics
- Basic security capabilities

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

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
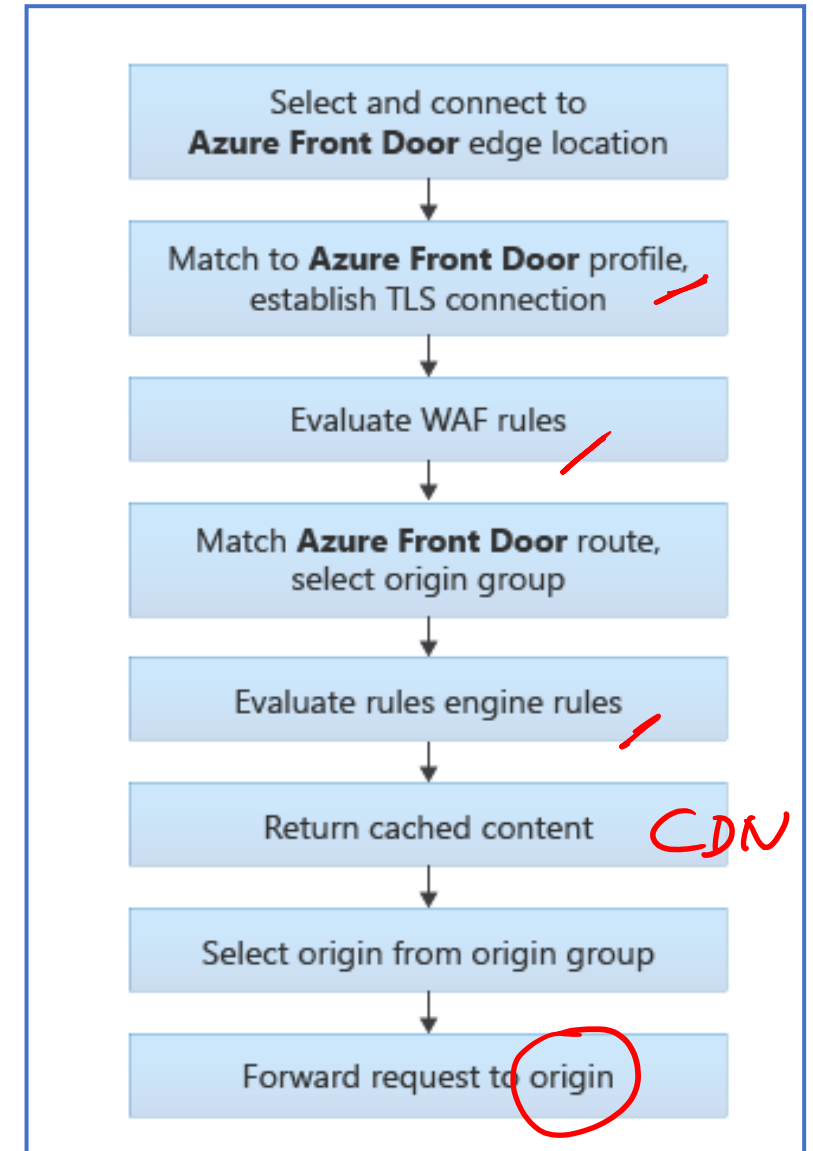
Configure an Origin (Backend)

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
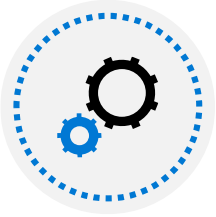   ○ HTTPS only
                             ● Match incoming request

Caching   ☐ Enable caching

Demonstration – deploy Azure Front Door

Create two instances of a web app

Create a Front Door for your application

View Azure Front Door in action

Summary – Design and Configure Azure Front Door

Check your knowledge	Microsoft Learn Modules (docs.microsoft.com/Learn)

Azure Front Door | Microsoft Docs

Tutorial: Scale and protect a web app by using Azure Front Door and Azure Web Application Firewall (WAF) | Microsoft Docs

---

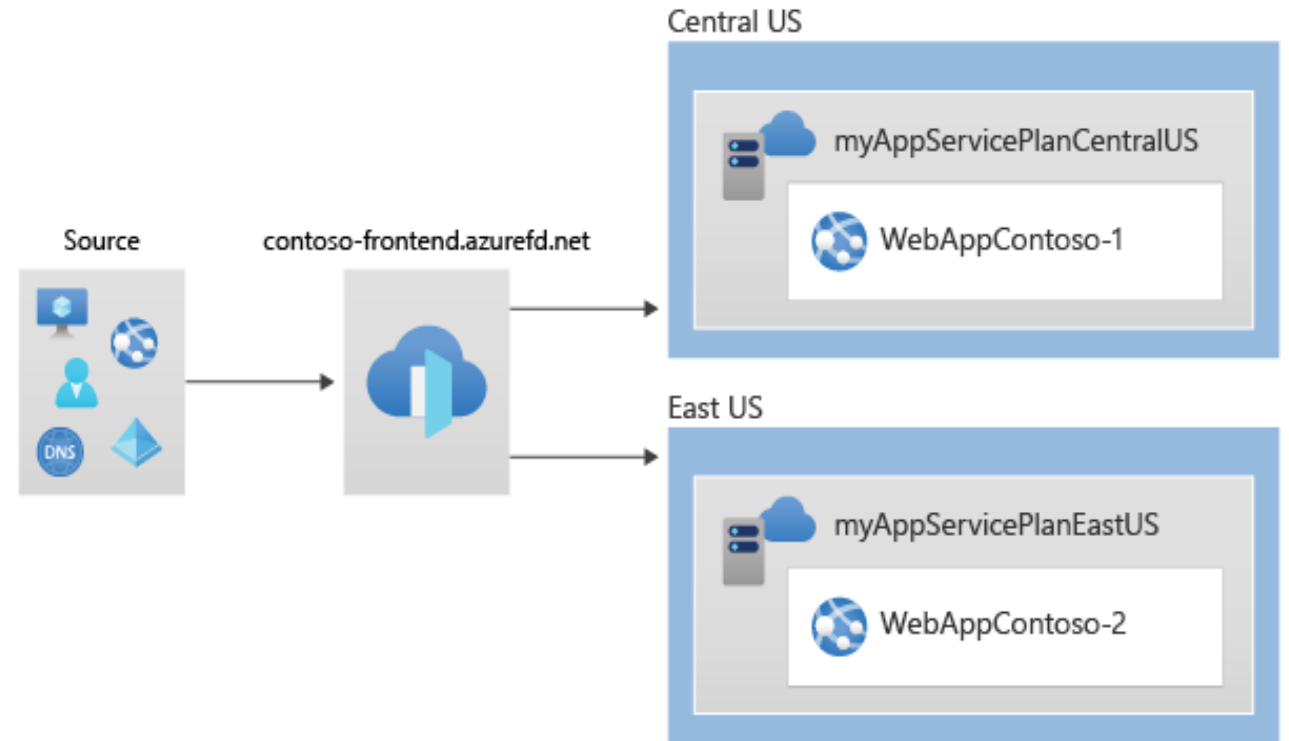# Exercise: create a Front Door for a highly available web application

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

Source

contoso-frontend.azurefd.net

Central US

myAppServicePlanCentralUS

WebAppContoso-1

East US

myAppServicePlanEastUS

WebAppContoso-2

Summary – deploy Front Door

Check your knowledge	Microsoft Learn Modules (docs.microsoft.com/Learn)
	[Quickstart: Set up high availability with Azure Front Door Service - Azure portal | Microsoft Docs](#)

End of presentation