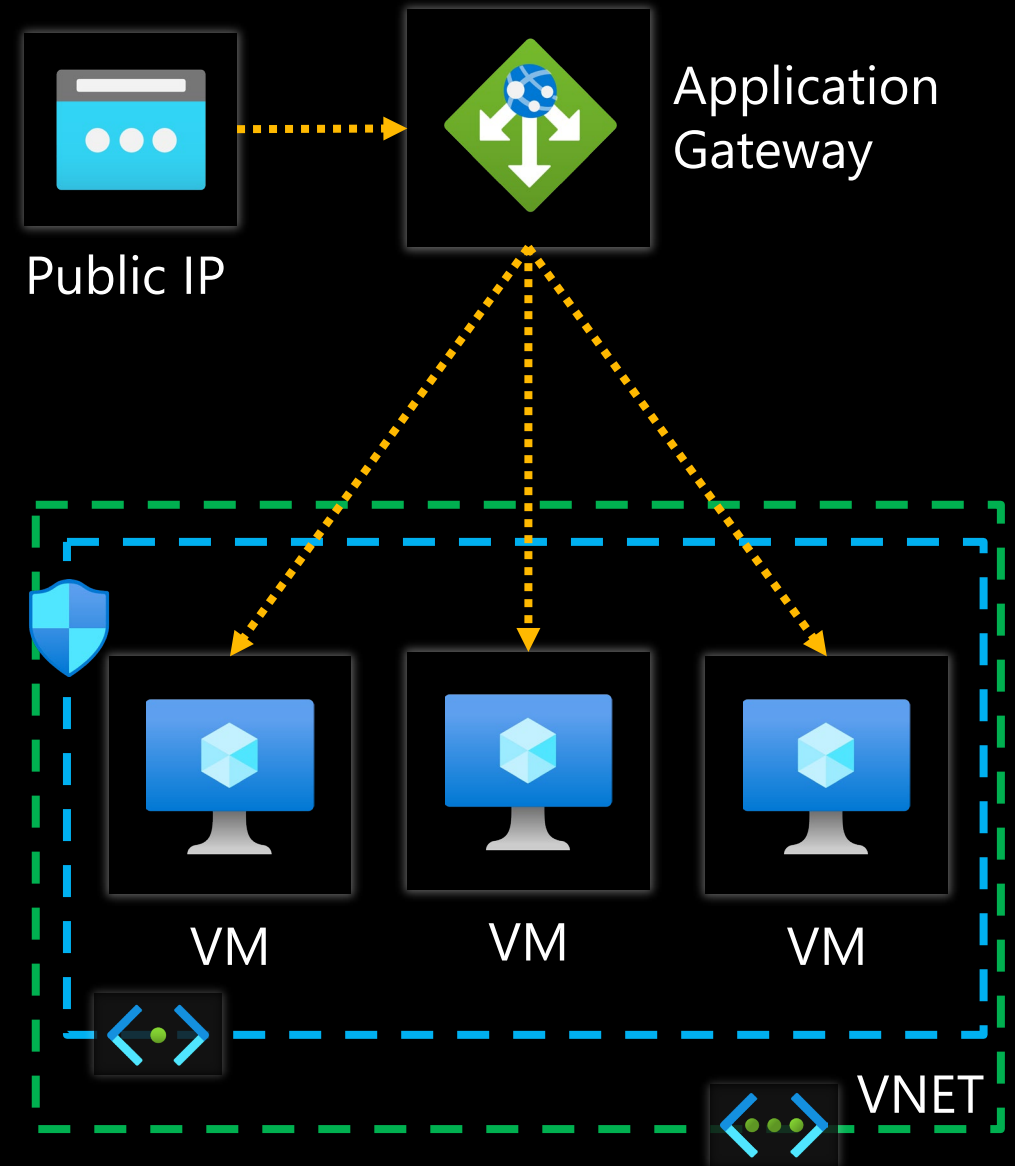


# Azure Application Gateway



# Azure Application Gateway

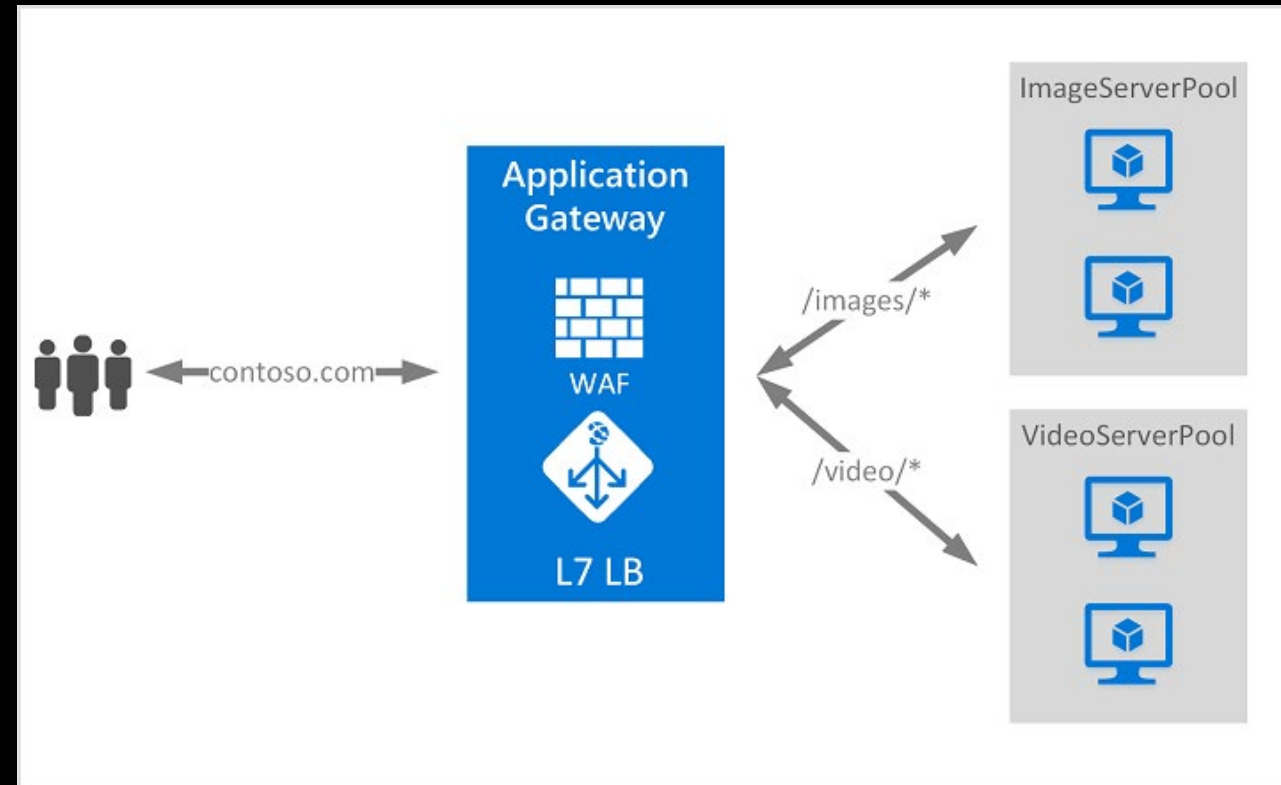
**Application** layer **Load Balancer**.

Routes network traffic to VMs, VMSS, App Service, AKS, Container Apps, Functions, etc.

Operates at **layer 7** in OSI model.

Can route traffic based on URL.

Supports **Web Application Firewall (WAF)**.



# Application Gateway features

**SSL/TLS termination:** TLS termination at the gateway and **end to end TLS encryption**.

Supports **autoscaling** based on traffic load.

Could span multiple **Availability Zones**.

**URL-based routing:** `contoso.com/app1`.

Could be used for **multiple applications**

**Redirection from HTTP to HTTPS** or to an external site.

**Session affinity:** keep a user session on the same server.

## Create SSL profile

appgateway

An SSL profile allows you to configure client authentication

SSL Profile Name \*

Client Authentication

SSL Policy

Upload your client certificate file. Any intermediate CA separately, the intermediate CA certificate and root CA certificate chain must contain exactly one root CA certificate

Upload a new certificate

Certificates

Additional client authentication configuration

☐ Verify client certificate issuer's DN ⓘ

Tier \* ⓘ  
Standard V2

Capacity type  
☒ Autoscale ☐ Manual

Minimum instance count \* ⓘ  
 1

Maximum instance count \* ⓘ  
 10

HTTP2 \*  
☒ Disabled ☐ Enabled

Backend protocol  
☒ HTTP ☐ HTTPS

Backend port \*  
 80

Additional settings

Cookie-based affinity ⓘ  
☐ Enable ☒ Disable

Connection draining ⓘ  
☐ Enable ☒ Disable

Request time-out (seconds) \* ⓘ  
 60

Override backend path ⓘ  
 /

# Application Gateway features







Could be exposed through **private or public** IP address.

Supports Private Link service (PLS).

## appgateway | Frontend IP configurations ☆ ...

Application gateway

### Settings

-  Configuration
-  Web application firewall
-  Backend pools
-  Backend settings
-  Frontend IP configurations
-  Private link

«

Type	Status	Name	IP address	Associated listeners
Public	Configured	frontend_ip_configuration	137.117.181.134 (pip-appgateway)	listener
Private	Not configured	-	-	-

# App Gateway features

Custom **error pages**.

Rewrite **HTTP headers and URL**.

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)

NewRewrite (100)

Rewrite rule name \*

NewRewrite

Rule sequence \* ⓘ

100

You can add conditions to trigger the fol

Do

Rewrite type \* ⓘ

Action type \* ⓘ

Header name \* ⓘ

Common header \*

Header value \* ⓘ

OK

Cancel

A-IM

Accept

Accept-Charset

Accept-Encoding

Accept-Language

Accept-Datetime

Access-Control-Request-Method

Access-Control-Request-Headers

Authorization

Cache-Control

Content-Length

Content-MD5

Content-Type

Cookie

listener ...

appgateway

Bad Gateway - 502

Enter Html file URL

Forbidden - 403

Enter Html file URL

Internal Server Error - 500 (Preview)

Enter Html file URL

Service Unavailable - 503 (Preview)

Enter Html file URL

Gateway timeout - 504 (Preview)

Enter Html file URL

Bad request - 400 (Preview)

Enter Html file URL

Method not allowed - 405 (Preview)

Enter Html file URL

Request timeout - 408 (Preview)

Enter Html file URL

# App Gateway health probes

appgateway

Application gateway

Backend health

☆

...

×

Search

Configuration

Web application firewall

Backend pools

Backend settings

Frontend IP configurations

Private link

SSL settings

Listeners

Rules

Rewrites

Health probes

Refresh

All

3 out of 3

Healthy

3 out of 3

Search backend health

Server (backend pool)	↑↓	Status	↑↓	Port (Backend ...)	↑↓	Protocol	↑↓	Details
10.0.1.4 (backend_address_po...		✓ Healthy		80 (http_setting)		Http		Success. Received 200 status code
10.0.1.8 (backend_address_po...		✓ Healthy		80 (http_setting)		Http		Success. Received 200 status code
10.0.1.9 (backend_address_po...		✓ Healthy		80 (http_setting)		Http		Success. Received 200 status code

# Application Gateway WAF

Protects web apps from common exploits and vulnerabilities without changing the code.

Protects against SQL injection, cross-site scripting, DDOS attacks, HTTP protocol violations, crawlers and scanners, Geo-filter traffic to allow or block certain countries/regions, etc.

The screenshot displays the Azure portal interface for configuring an Application Gateway Web Application Firewall (WAF). The top navigation bar shows the 'appgateway | Web application firewall' title. Below this, a search bar and action buttons (Save, Discard, Refresh) are visible. The left sidebar lists the following settings:

- Settings
- Configuration
- Web application firewall (selected)
- Backend pools
- Backend settings
- Frontend IP configurations

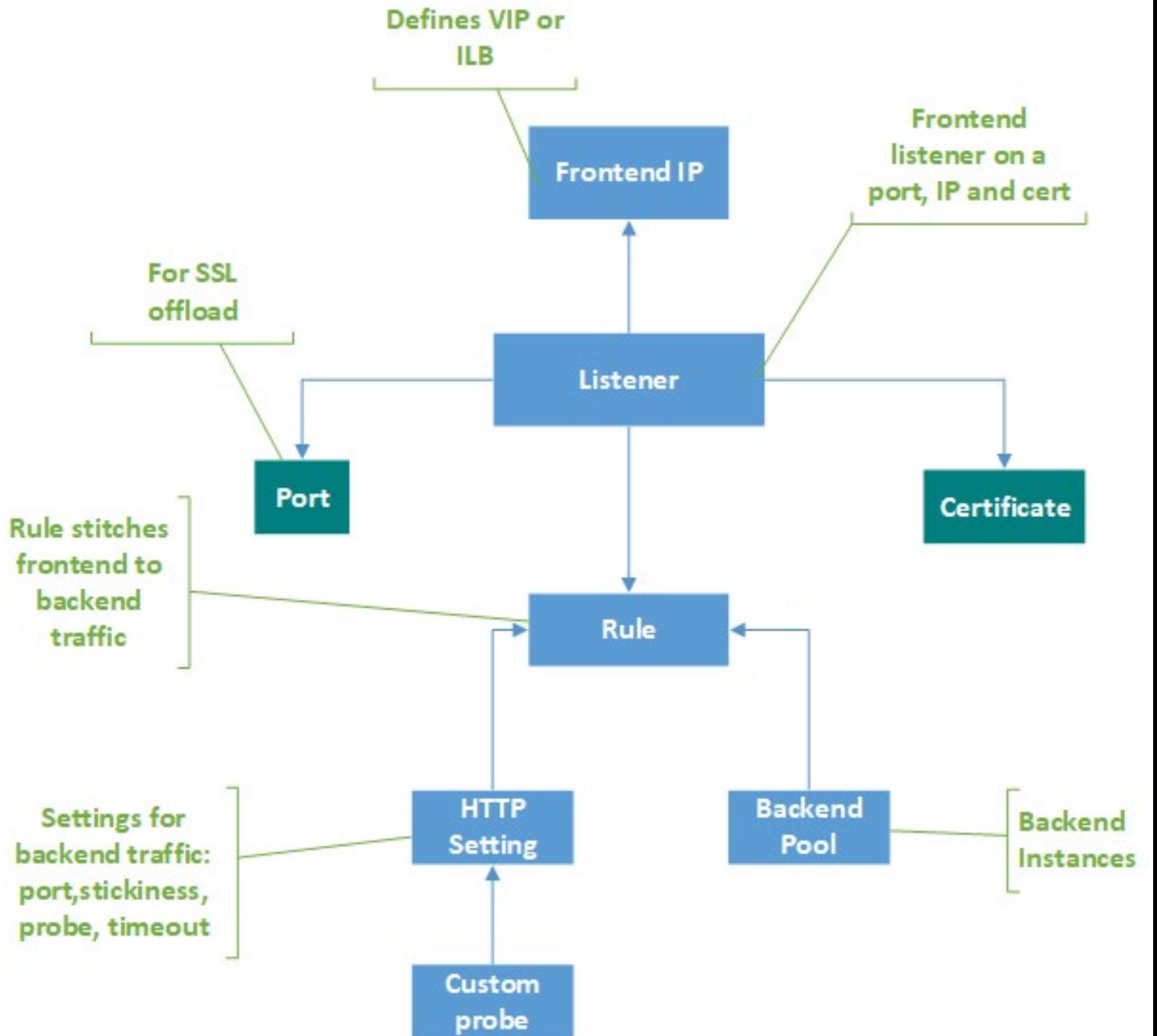
The main configuration area is titled 'Configure' and includes the following settings:

- Tier:** Standard V2 (selected), WAF V2
- WAF Policy:** (new) waf-policy (selected), with a 'Create new' link below it.

# App Gateway components

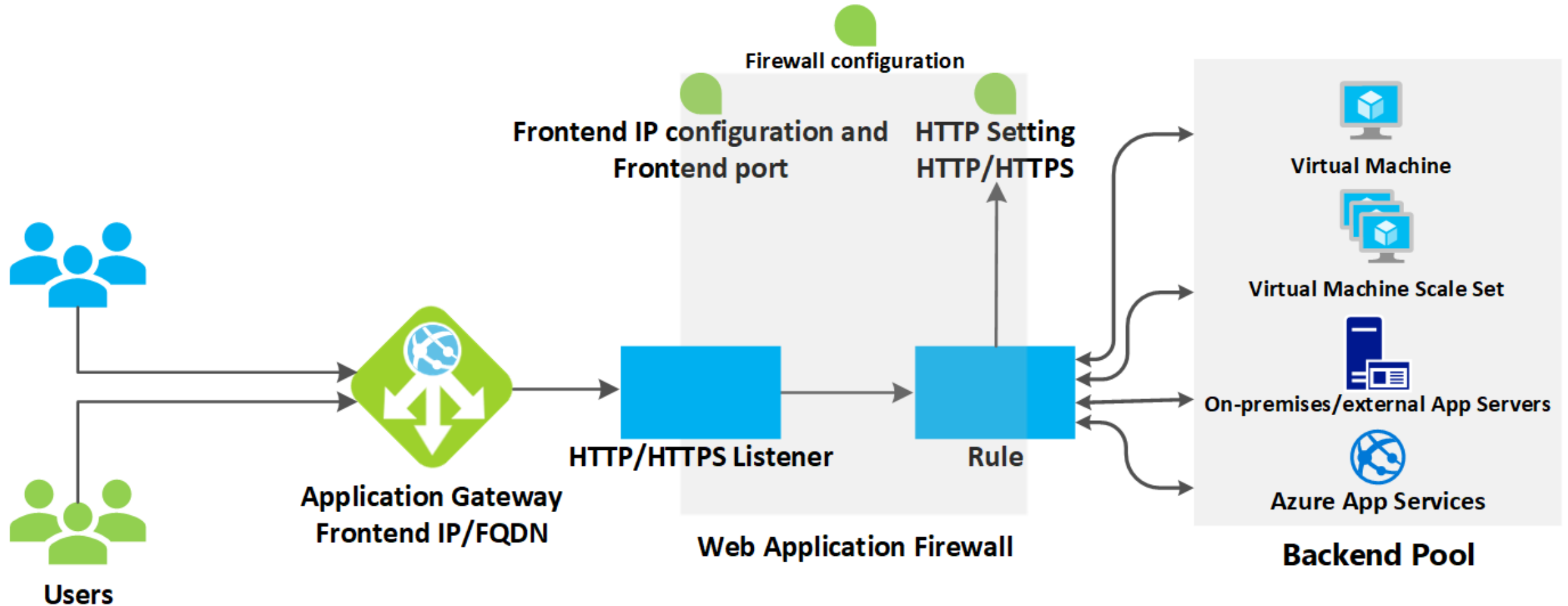
## Settings

- Configuration
- Web application firewall
- Backend pools
- Backend settings
- Frontend IP configurations
- Private link
- SSL settings
- Listeners
- Rules
- Rewrites
- Health probes





# App Gateway components



# Application Gateway important notes

Supports **only one public IP** address.

Could use **both an internal IP and an external IP**.

There are two versions: v1 and v2.

In v1, VIP can change if App Gateway restarted. In v2, **VIP and public IP are static**.

Must have its own **(dedicated) Subnet**. Multiple App Gateway can share the same Subnet.

Could be stopped and started using command line to reduce cost.

```
$ az network application-gateway stop -g MyResourceGroup -n MyAppGateway
```

Supports Key Vault to save TLS certificates.

# App Gateway for Kubernetes/AKS

## Application Gateway for Ingress Controller (AGIC)

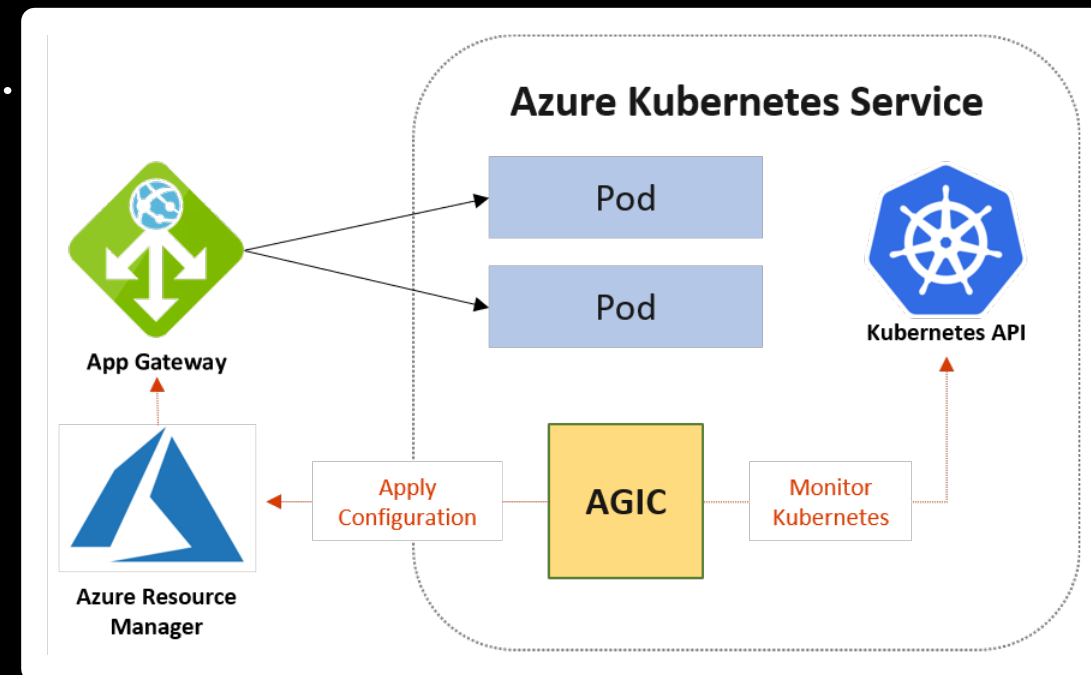
An ingress controller implementation for Azure Kubernetes Service (AKS) clusters.

Pods within an AKS cluster will receive network traffic through App Gateway.

[github.com/Azure/application-gateway-kubernetes-ingress](https://github.com/Azure/application-gateway-kubernetes-ingress)

## Application Gateway for Containers

An Ingress and API Gateway implementation for AKS.



# App Gateway pricing

	<b>Application Gateway</b>	<b>Web Application Firewall Application Gateway</b>
Fixed	<b>\$0.246</b> per gateway-hour <b>\$177</b> per month	<b>\$0.443</b> per gateway-hour <b>\$319</b> per month
Capacity Unit	<b>\$0.008</b> per capacity unit-hour <b>\$6</b> per month	<b>\$0.0144</b> per capacity unit-hour <b>\$10</b> per month

<b>Type</b>	<b>Example</b>	<b>Price</b>
Inbound	Data going into Azure data centers	Free
Outbound	Data going out of Azure data centers from app gateways	Charged at standard <a href="#">data transfer rates</a> .

# Azure Load Balancing solutions



## 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
- Global across Azure regions



## Traffic Manager

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

🔗

Load balancing

...

🔍 Search

🔗 Overview

Load Balancing Services

- 🔗 Application Gateway
- ☁️ Front Door and CDN profiles
- 🔗 Load Balancer
- 🌐 Traffic Manager

Help me choose

Service comparison

Tutorial

	<div>🔗</div> <div>Application Gateway</div> <div>Optimize delivery from application server farms while increasing application security with web application firewall.</div> <div>Create</div>	<div>☁️</div> <div>Front Door</div> <div>Scalable, security-enhanced delivery point for global, micro service-based web applications.</div> <div>Create</div>	<div>🔗</div> <div>Load Balancer</div> <div>Balance inbound and outbound connections and requests to your applications or server endpoints.</div> <div>Create</div>	<div>🌐</div> <div>Traffic Manager</div> <div>Distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.</div> <div>Create</div>
Supported protocols ⓘ	HTTP, HTTPS, HTTP2	HTTP, HTTPS, HTTP2	TCP, UDP	Any
Private load balancing ⓘ	✓		✓	
Global load balancing ⓘ		✓	✓	✓
Routing Policies ⓘ	Round robin	Latency, priority, round robin, weighted round robin	Hash Based	Geographical, latency, weighted, priority, subnet, multi-value
Supported environments ⓘ	Azure, non-Azure cloud, on prem	Azure, non-Azure cloud, on prem	Azure	Azure, non-Azure cloud, on prem
Connection draining ⓘ	✓			
Session affinity ⓘ	✓	✓	✓	
Host and path based load balancing ⓘ	✓	✓		
TLS offloading ⓘ	✓	✓		

# Azure Load Balancer solutions



## Application Gateway

Optimize delivery from application server farms while increasing application security with web application firewall.

[Create](#)

## Front Door

Scalable, security-enhanced delivery point for global, micro service-based web applications.

[Create](#)

## Load Balancer

Balance inbound and outbound connections and requests to your applications or server endpoints.

[Create](#)

## Traffic Manager

Distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

[Create](#)

Supported protocols ⓘ

HTTP, HTTPS, HTTP2

HTTP, HTTPS, HTTP2

TCP, UDP

Any

Private load balancing ⓘ



Global load balancing ⓘ



Routing Policies ⓘ

Round robin

Latency, priority, round robin, weighted round robin

Hash Based

Geographical, latency, weighted, priority, subnet, multi-value

Supported environments ⓘ

Azure, non-Azure cloud, on prem

Azure, non-Azure cloud, on prem

Azure

Azure, non-Azure cloud, on prem

Connection draining ⓘ



Session affinity ⓘ



Host and path based load balancing ⓘ



TLS offloading ⓘ



Site acceleration ⓘ



Security ⓘ

WAF, NSG

WAF

NSG

Caching and compression ⓘ

