ALEF

Nginx Plus with App protect

NGINX plus with App Protect provides proxy load balancing and Web Application Firewall (WAF) features in a secure, agile and performance way. It can be deployed in the cloud, on-premise, and in a micro services environment. NGINX's WAF feature uses the same core WAF engine as F5 Advanced WAF.

USE case:

1. Overview

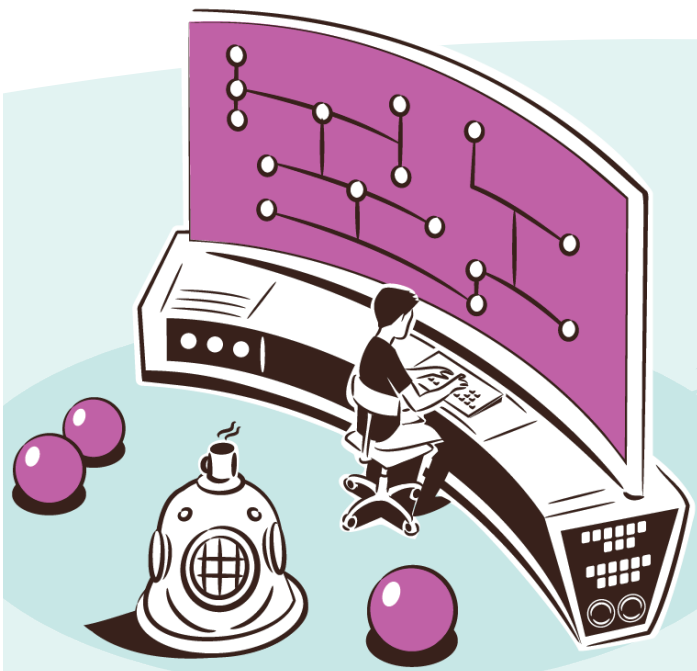
A major Slovak national IT system provides vital information to the better part of the country's population enabling them to manage their day-to-day life situations online.

The main monolithic application of the system was designed about 10 years ago and it has a typical service-oriented architecture with WAF. It is deployed on standard server hardware in an on-premise datacenter.

During the pandemic situation the development of a new web application became necessary.

The main priority requirements for the application were:

1. Dynamic scaling and rapid deployment
2. API-oriented
3. Secure



2. The challenge

Dynamic scaling and rapid deployment

To run the new agile web application would require the dynamic scaling of the hardware/network infrastructure. Additionally there were predictions that new features will be added and the traffic will increase.

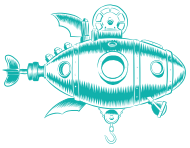
The existing on-premise (hardware based) datacenter was not designed to handle the infrastructure needs of a modern application with unpredictable traffic.

API oriented

Users can access the application via two interfaces. One is for business verified customers accessing the application through VPN and the second is for public access using HTTPS. Application should communicate through API.

Secure

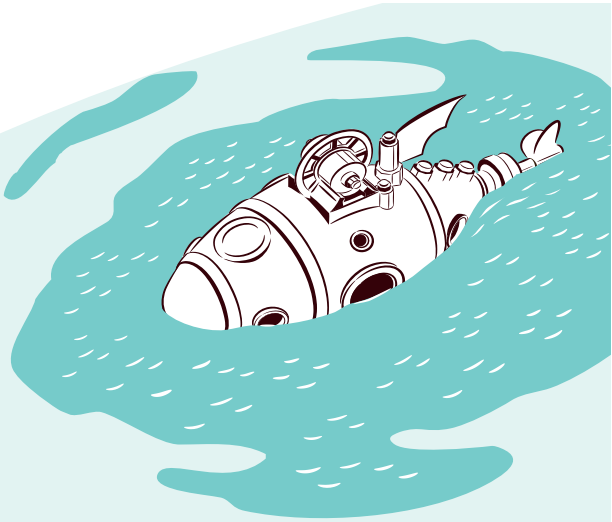
The main security requirement of the application was to have enabled WAF in enforcing mode for API calls. Traditional WAF solutions take time to configure the WAF policy manually or through learning. While in the learning phase the policy is initially not blocking traffic



Trust the Strong

ALEF DISTRIBUTION GR M.I.K.E. | A-office Building
Astronafton 1, 151 25 Amarousion | GREECE
gr-sales@alef.com | alef.com/gr

NGINX Part of F5



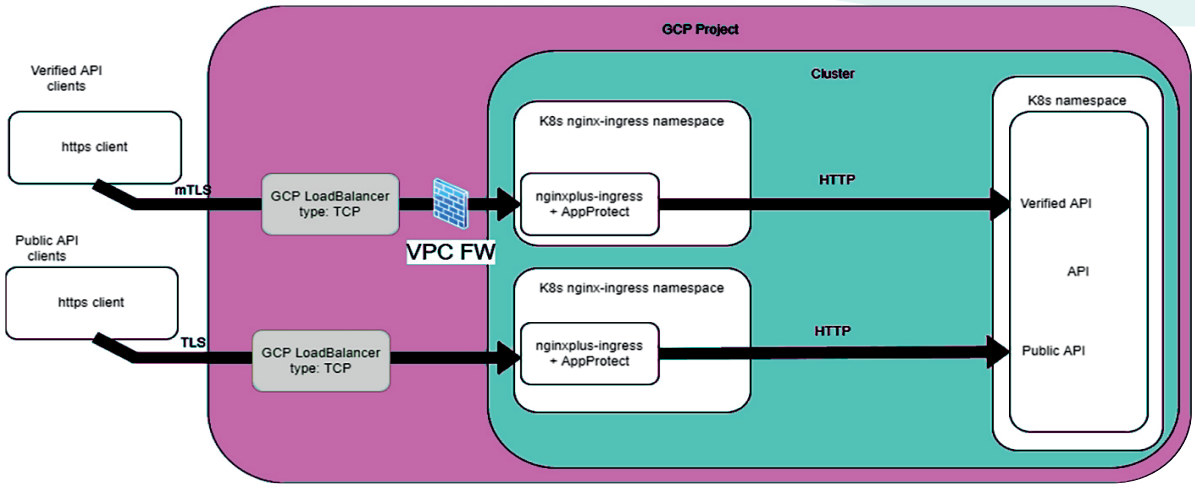
to interpret what is valid traffic. At the same time manual configuration consumes a lot of time to fine tune the policy. These steps must be repeated after each application update.

The company wanted to have a WAF policy to protect the API interface immediately and the application as well considering updates as well.

3. Solution

The company chose Google Cloud Platform (GCP) to host the new application. The application was developed in Kubernetes and has two separate API interfaces for verified and public customers.

The solution fits into the modern applications' CI/CD pipeline with better scalability and more flexible deployment compared to traditional deployments. Google Cloud has smooth integration with NGINX plus with App protect. Given the above-mentioned characteristics of the web application improved delivery time for new features. NGINX Plus with App protect was chosen as a secure load balancer with WAF in a Kubernetes Ingress Controller scenario as can be seen below:



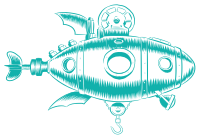
Besides NGINX plus advanced balancing options and logging, NGINX App protect enables to protect the new Application with WAF. NGINX App protect WAF API policy could be based on the swagger file or even link to the swagger file. Therefore, on each new release of the application, developers update the swagger file (description of the application calls) only and NGINX App protect secures and enforces the objects based on it.

4. The result

The company decided to run application in Google Cloud based on the heavier traffic expected for the application compared to the initial plan. Customers' web application is running in multiple microservice cloud containers.

NGINX plus supports the management and configuration of the instances via API. New features that are encapsulated as microservices can be launched in real time and without any server downtime through a dynamically configurable NGINX conf file and application swagger file that is automatically updated by API. This means that features can be rolled out quickly and instantly secure.

NGINX App protect is a secure WAF solution based on the same engine F5 uses in its Advanced WAF module with regular attack signature updates and additional security features like Threat Campaigns, BOT Defense and Layer 7 DoS protection.



Trust the Strong

ALEF DISTRIBUTION GR M.I.K.E. | A-office Building
Astronafton 1, 151 25 Amarousion | GREECE
gr-sales@alef.com | alef.com/gr

NGINX
Part of F5