Security implementation document

Group C

Distributed computing

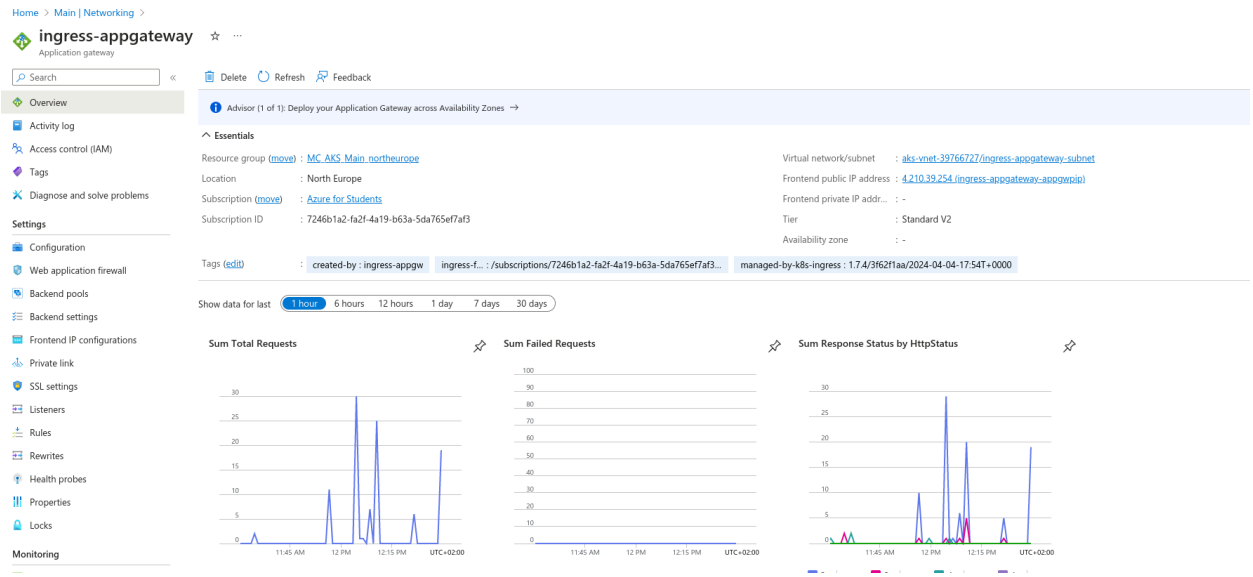
Evgeni,Stefan,Nikolay,Vlad,Naadir, Thomas, Renis

Introduction

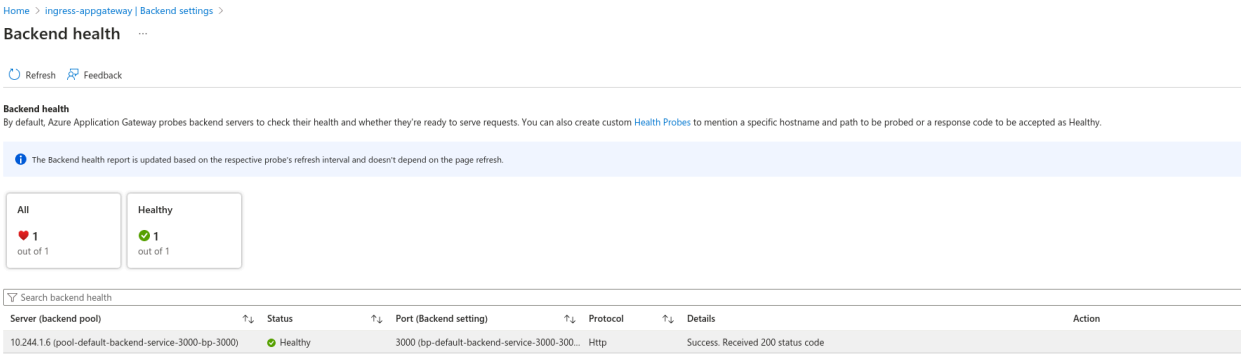
In this document we are going to explain how we managed to implement the researched security methods in our project and how our security works overall. In the security report we mentioned that we are going to implement different levels of security. Azure security, K8s security and Network Security.

Azure Security & monitoring

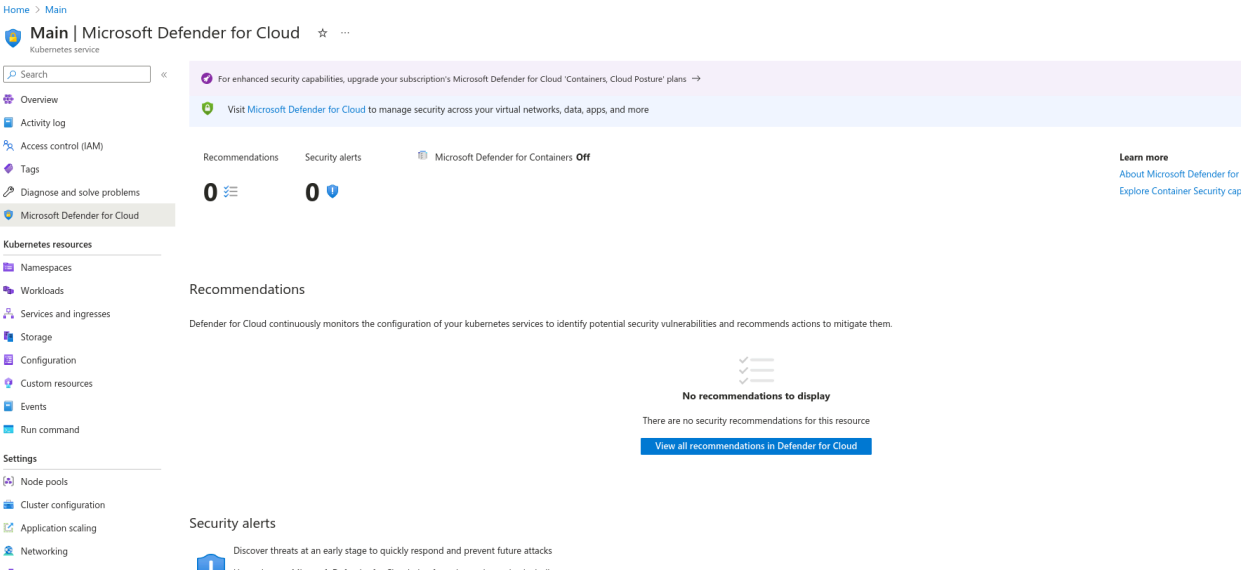
In terms of Azure security we implemented a couple of things. One of them is creating the application gateway and configuring it in a way that it prevents malicious traffic as well as DOS attacks.



In here we have also enabled some advanced monitoring options so that we have a bigger overview of the requests and the response time.
The Application gateway also provides us with a WAF and also gives us constant health checks.

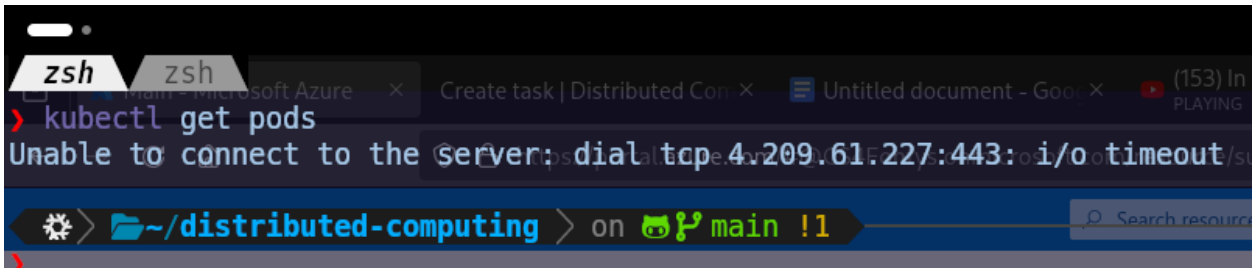


Also we enabled and followed the AKS recommendations so that we got 100% security checks in Azure.



Network security

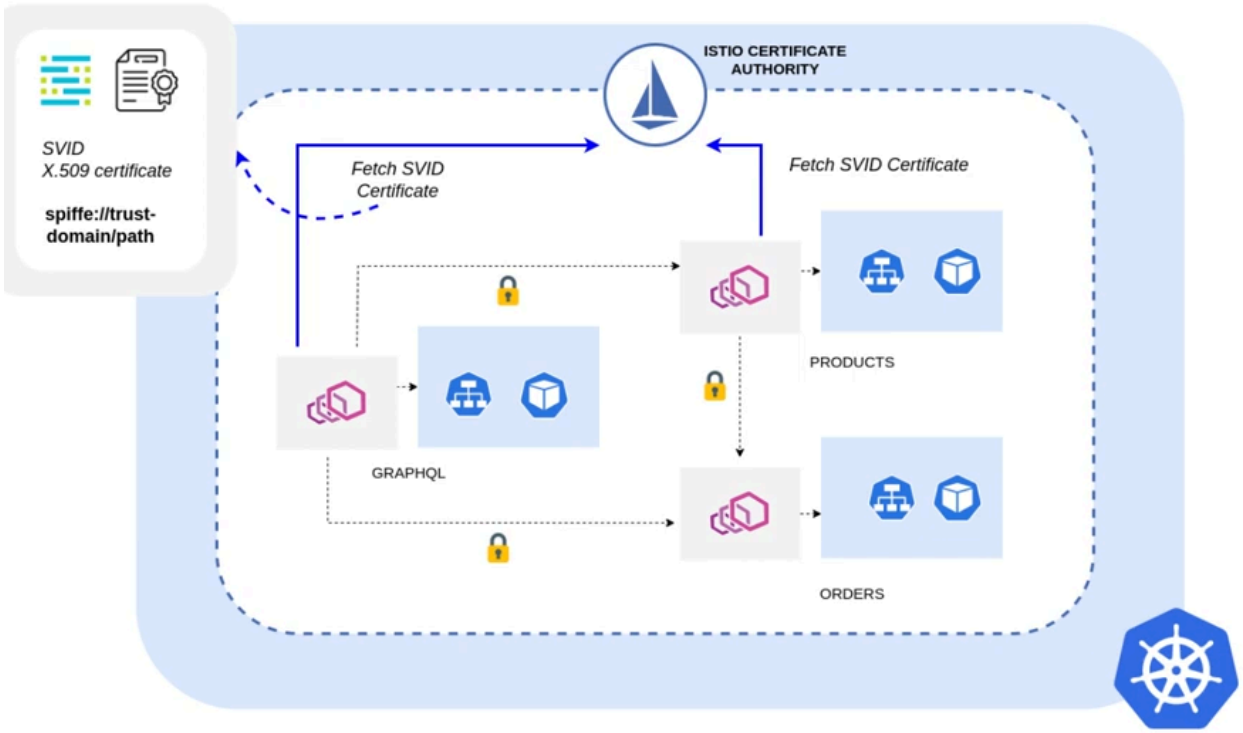
We have enforced strong security rules and policies for access. The K8s API is basically unreachable since we have made it accessible only for specific IPs by setting **Authorized IP ranges**.



This is what unauthorized IP gets when tries to access the AKS API.

K8s security/pod security

For K8s security we have enabled RBAC authentication for the cluster. That way processes are authenticated by Azure users that have the needed privileges. Since K8s takes care about fallen pods we don't have to worry about backups and ect. The nodes are placed in different V-nets for preventing chain attacks if one of the pods gets compromised.
In the research documents we have talked a lot about encrypted communication pods. For this we have used this K8s package called **Istio**.



This is a brief overview of how Istio mTLS security works. Istio is used as a proxy to check for authentication and as certificate authority , using Spiffe it manages to issue certificates and uses proxy containers to check for authenticated access.

Name	State	Reason
backend	Running	
istio-proxy	Running	

Other things that we included in the security part are secrets. We store information like Redis passwords,ports,certificates etc. as K8s secret objects. We extract them from there as values and use them in configuration files.