What is the best way to protect microservices?



# Sub-Questions

To answer my main question I split it up in smaller questions which I would research.

1. How can I ensure only my application can access the service?
2. How do I verify witch user sends an request to the service?
3. How do I make sure the data sent to the service is valid?

To answer these questions I used the dot framework. I started by doing Library research and after I learned some basic principles I started implementing the things I learned in my workshop fase.

# Library

To start my research I wanted to protect my services from other people. I could use an Ip whitelist but all of my services would need to have this whitelist and if an Ip changed it would need to be updated in all services. To make this easer I looked into an api gateway for my services. An api gateway takes all the responsibility for the protection of the other services. This way only the gateway has the Ip list and if an request comes from an invalid Ip it will return an error. To verify the users JWT can be used. A JTW is string containing a header, a body which are base64 encoded jsons and a RSA signature. Every request sent to the gateway has to be a JTW. In the gateway the JTW will be encoded and verified if the user has the permission to make the request. If he has permission the gateway will call the request from another service and return the information. If the data comes in it will be decoded so only valid data will make it true.

# Workshop

After I did my library research I started making a gateway for myself to try out the basic principles. I used the whitelist to make sure all the requests had to go true the gateway. This way I could verify if someone sent correct data by asking an other service first and then making the original request.

# Sources

<https://www.youtube.com/watch?v=SLc3cTlypwM>

<https://medium.com/microservices-learning/how-to-implement-security-for-microservices-89b140d3e555>