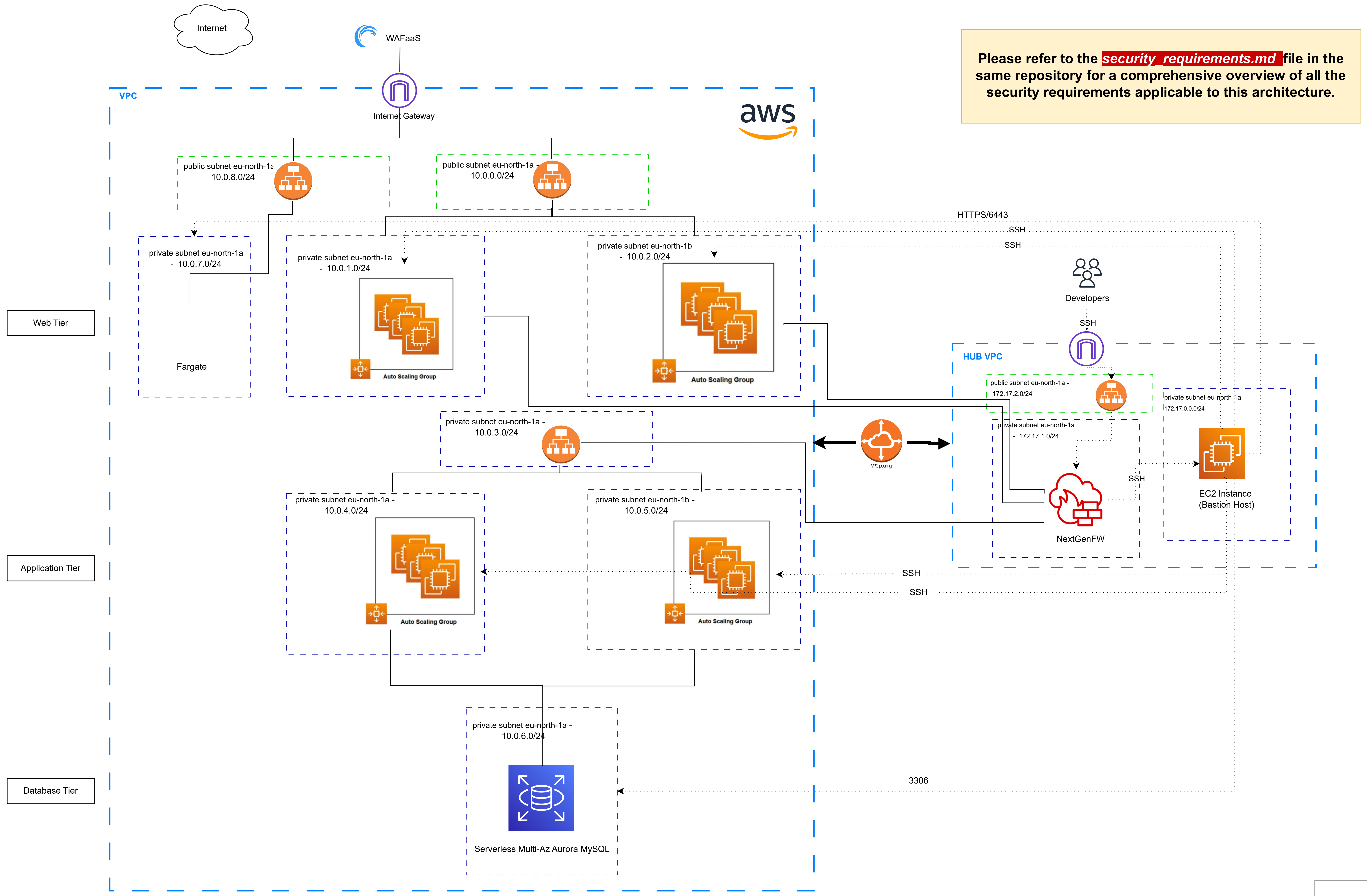

Please refer to the *security_requirements.md* file in the same repository for a comprehensive overview of all the security requirements applicable to this architecture.

Security group - A

TCP 443 2.22.60.0/24 10.0.0.0/24
TCP 443 23.15.12.0/24 10.0.0.0/24
TCP 443 2.16.37.0/24 10.0.0.0/24
TCP 443 184.51.33.0/24 10.0.0.0/24

TCP 443 2.22.60.0/24 10.0.8.0/24
TCP 443 23.15.12.0/24 10.0.8.0/24
TCP 443 2.16.37.0/24 10.0.8.0/24
TCP 443 184.51.33.0/24 10.0.8.0/24

Security group - B

TCP 443 10.0.0.0/24 10.0.1.0/24
TCP 443 10.0.0.0/24 10.0.2.0/24
SSH 172.17.0.0.0/24 10.0.1.0/24
SSH 172.17.0.0.0/24 10.0.2.0/24

Security group - C

TCP 443 172.17.1.0.0.0/24 10.0.3.0/24

Security group - D

TCP 443 10.0.3.0/24 10.0.4.0/24
TCP 443 10.0.3.0/24 10.0.5.0/24
SSH 172.17.0.0.0/24 10.0.4.0/24
SSH 172.17.0.0.0/24 10.0.5.0/24

Security group - E

TCP 443 10.0.4.0/24 10.0.6.0/24
TCP 443 10.0.5.0/24 10.0.6.0/24
TCP 330610.0.4.0/24 10.0.6.0/24
TCP 330610.0.5.0/24 10.0.6.0/24
TCP 3306 172.17.0.0.0/24 10.0.6.0/24

Security group - F

TCP 443 10.0.4.0/24 10.0.6.0/24
TCP 443 10.0.5.0/24 10.0.6.0/24
TCP 330610.0.4.0/24 10.0.6.0/24
TCP 330610.0.5.0/24 10.0.6.0/24
TCP 3306 172.17.0.0.0/24 10.0.6.0/24

Security group - G

TCP 443 172.17.0.0/24 10.0.7.0/24
TCP 6443 172.17.0.0/24 10.0.7.0/24
TCP 443 10.0.8.0/24 10.0.7.0/24

Context

- All communications are being established with VPC endpoints and private links.
- Public load balancer has been assigned the security group A to allow inbound connections from WAF IP addresses
- I have assumed the EKS serves a different purpose, such as a public API, and have therefore separated it.
- Developers should access and implement changes through the bastion host. In the diagram, it's represented as a single instance for simplicity, but it should be replicated to ensure high availability.