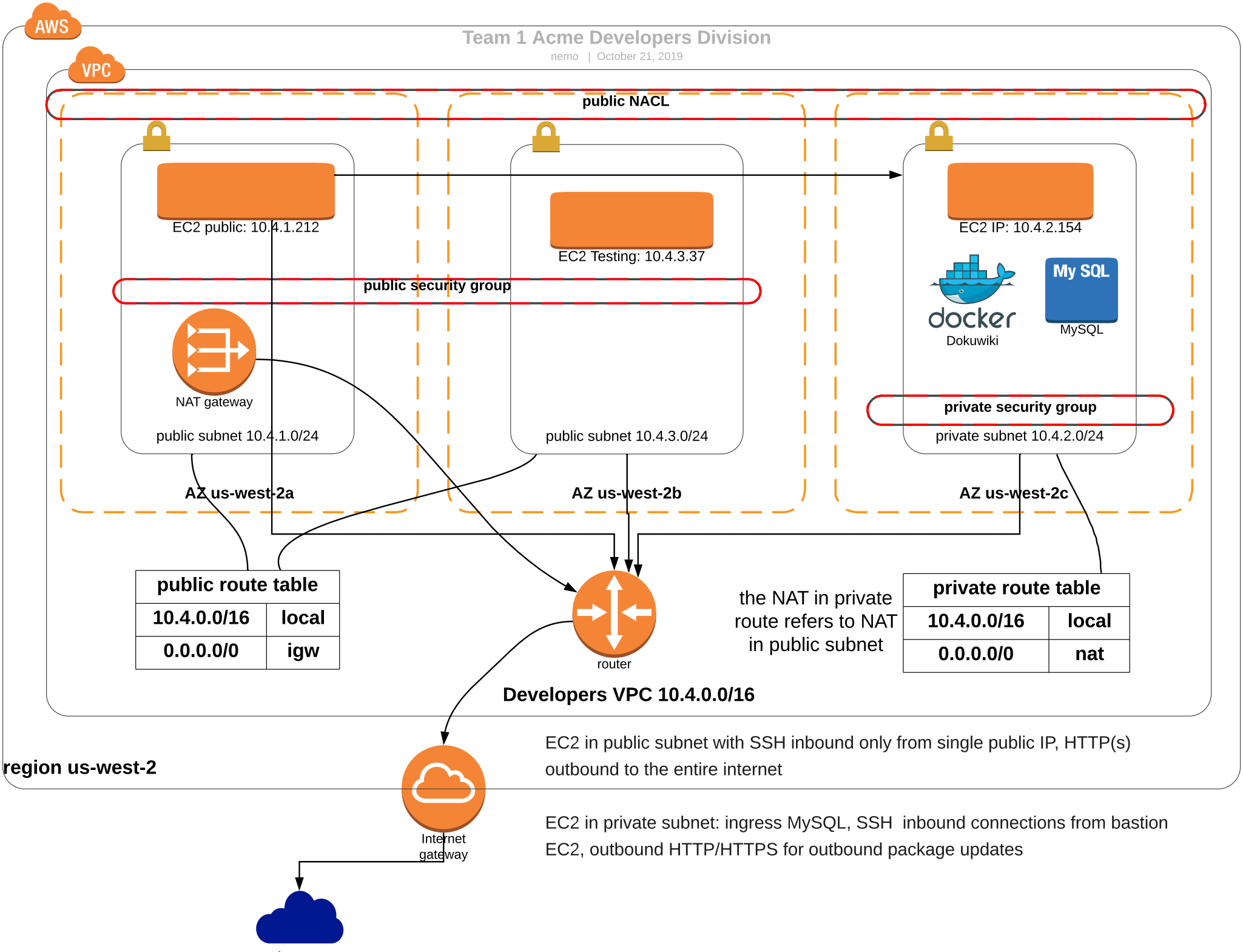

EC2 in public subnet with SSH inbound only from single public IP, HTTP(s) outbound to the entire internet

EC2 in private subnet: ingress MySQL, SSH inbound connections from bastion EC2, outbound HTTP/HTTPS for outbound package updates