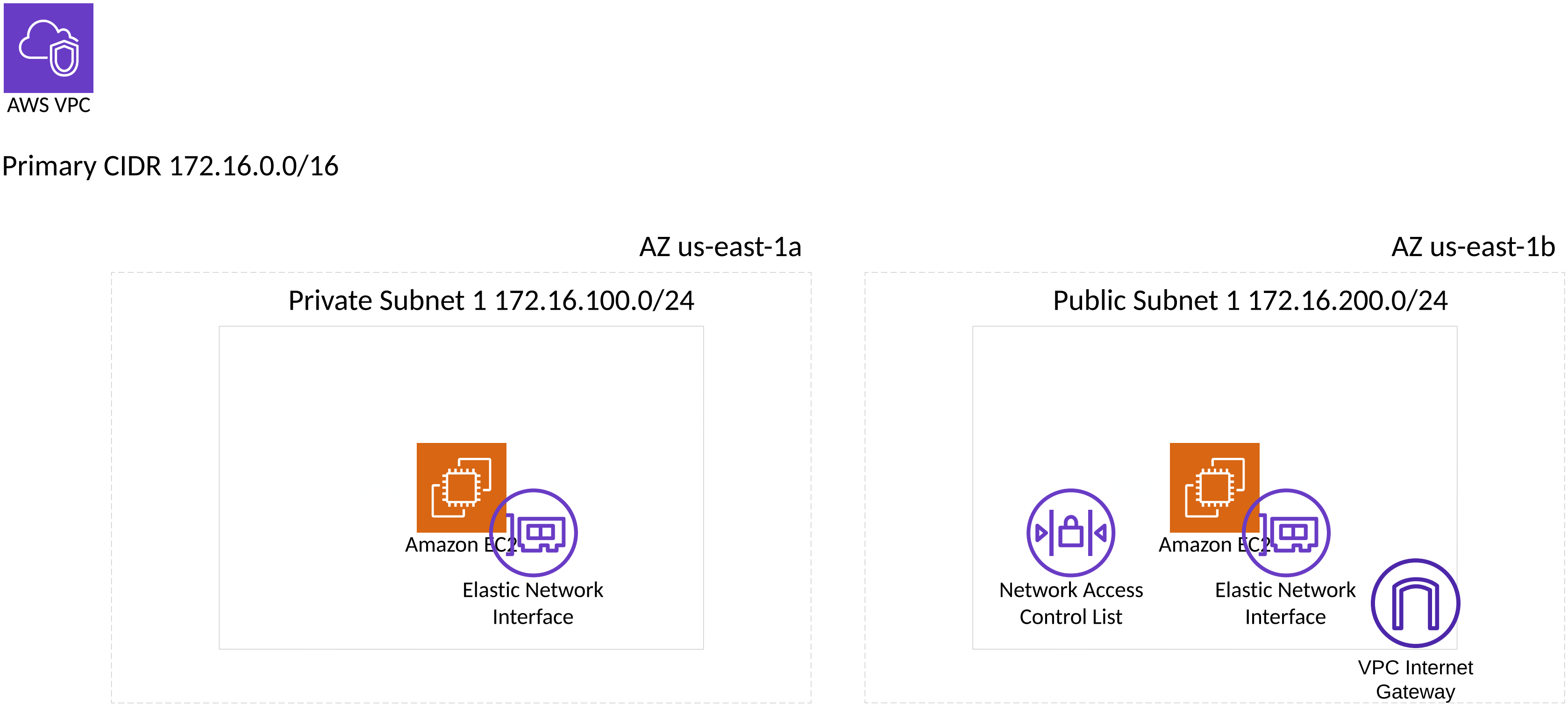
AWS VPC Architecture



Primary CIDR 172.16.0.0/16

AZ us-east-1a

Private Subnet 1 172.16.100.0/24

Amazon EC2
Elastic Network Interface

AZ us-east-1b

Public Subnet 1 172.16.200.0/24

Network Access Control List
Amazon EC2
Elastic Network Interface
VPC Internet Gateway

Security Group: Inbound and outbound rules to specify the traffic the security group allows. Functions as a firewall.
Every ENI has at least one security group associated with it.
Whitelisting: Deny all traffic that is not explicitly allowed by a rule.
NACL: Stateless, 1 per subnet, processed in ascending order of rule number. Inbound rules and outbound rules.
Subnets are within the primary CIDR and do not overlap (are not "out of bounds"). Subnets in different AZ's adds resiliency.