6️⃣

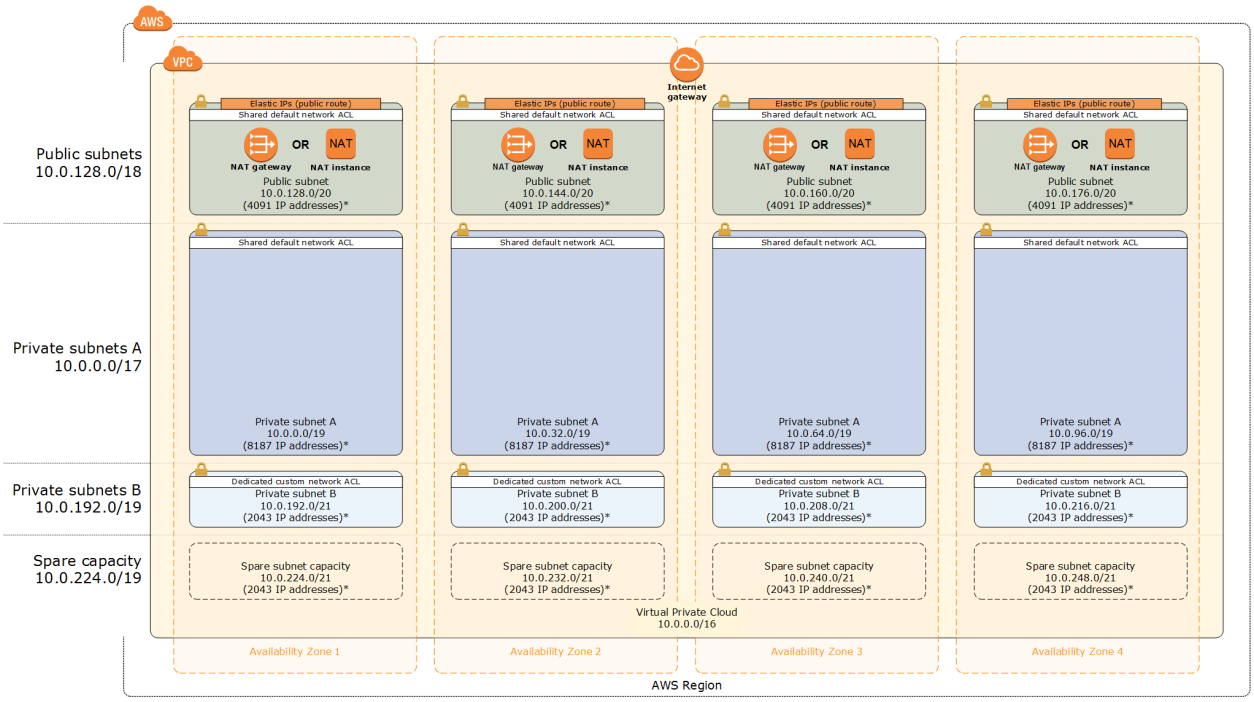
Lecture 6 - Networking in AWS: VPC, Route53 (1h)

- Q&A about the previous lesson (3-5m)

General

- IPv4 addresses - public and private
- Private addresses pools
  - 10.0.0.0 to 10.255.255.255 - number of addresses 16777216
  - 172.16.0.0 – 172.31.255.255 - number of addresses 1048576
  - 192.168.0.0 – 192.168.255.255 - number of addresses 65536
- CIDR blocks
  - https://cidr.xyz/

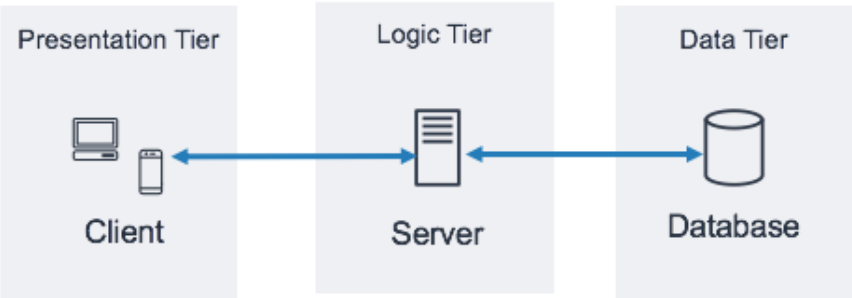
VPC



- VPC components
  - VPC → https://aws.amazon.com/vpc/faqs/
  - Subnets → https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html
  - Route tables → https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html
  - Gateways
    - Internet Gateway - provides access to the internet in a VPC
    - NAT https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
      - allows the internet access to the private subnet without sacrificing security
      - somehow like a one-way gateway
      - placed in a public subnets ⚠️
    - VPN (Virtual Private Gateway) → https://docs.aws.amazon.com/directconnect/latest/UserGuide/virtualgateways.html
    - Transit gateway → https://aws.amazon.com/transit-gateway
      - more like a multi-vpc multi-peering
    - Peering connections - connections between VPCs in different accounts/regions

        - IP CIDR blocks should not overlap VPC A = 10.0.0.0/16 + VPC 10.1.0.0/16
        - devices in a peered VPCs behave like they on the same network
      - Egress-only Internet Gateway (Applicable only for ipv6)
      - Direct Connect → https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html
    - VPC endpoints (AWS Privatelink) → https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html
      - allows to communicate with other AWS services bypassing the Internet (as if they were in the VPC)
      - good for security and compliance
    - VPC flow logs and format → https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
      - https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html
    - Not everything is allowed in VPC
      - broadcast is not supported
      - port scanning, any other pentesting activity (either with AWS permission)
- AZs → https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
    - are interconnected physical datacenters
    - randomized - its names are meaningful only for one setup
    - cross-az traffic is not free - consider this when placing your microservices
    - can be selected via subnets
- Firewalls
    - NACL → https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
      - is a subnet-level firewall
      - **stateless** - we have to define both inbound and outbound traffic
      - we have to allow the outbound at ephemeral ports → https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports

        - support deny rules
        - have rules priorities (lower-stronger, can do some logic on rules evaluation)
    - SG → https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html
        - EC2 Hypervisor level firewall (traffic is filter after NACL)
        - **stateful** - we have to only specify allowed inbound traffic
        - don't have deny rules - only allow
        - supports other SGs as an input (that's a bect practice actually)
- Bastion hosts → https://aws.amazon.com/quickstart/architecture/linux-bastion/
- Three-tier architecture
  → https://medium.com/the-andela-way/designing-a-three-tier-architecture-in-aws-e5c24671f124



- How to troubleshoot networks
    - check SGs
    - check NACLs
    - check Route tables
        - check NAT gateways/internet Gateways
        - check VPC peering (if any)
    - simulate the connection with Reachability analyzer
      https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html

Route53

- Fully Managed DNS service in AWS → https://aws.amazon.com/route53/faqs/
- Domain registration
- DNS records editing
- Has a health check capabilities
- 100% SLA
- Supports records types
  - NS - name of the nameservers
  - A - domain to ipv4 mapping
  - AAAA - domain to ipv6 mapping
  - TXT - text record to domain mapping
  - CNAME - domain to domain mapping
  - MX - mail records
  - Alias - AWS resource to domain mapping
  - (other)
- TTL - time to live (set lower to minimize the damage if any)
- Advanced routing policies → https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html
  - simple
  - weighted
  - latency-based
  - geoproximity
  - geolocation
  - multivalue
  - failover
- public and private hosted zones https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html
  - private - routable only insade some private corporate network
  - public - internet routable

- Not free - https://aws.amazon.com/route53/pricing/

Route53 use cases

- DNS records management
- disaster recovery - switching regions
- blue/green or red/black deployments, canary deployments
- to find some resources in a large cross-account environments

Homework

- Creating the first VPC with wizard and NAT
  - Launching a few EC2s in different subnets within VPC - private and public
  - Trying the internet connectivity from inside the private subnet with/without NAT
- Creating VPC without VPC wizard (NAT is optional)

Q&A session

- topic discussion
- sharing useful external resources and links