VPC Virtual Private Cloud - REGION

- VPC needs CIDR block
- Largest /16, smallest /28 (5 addressed reserved)

Subnet - AVAILABILITY ZONE

```
- Smallest CIDR /28 (16 ip addrss) - default /20
- 5 ip reserved always
- Can only span single AZ
- Public - with route to IGW
- Private - without route to IGW
- VPN-Only - with route to VPG and without route to IGW
```

Route Tables

```
- Routes between Subnets
- One route table can be assigned to multiple Subnets, One subnet can have only one route table
- Each route table contains route to local traffic which you cannot delete.
- Each route has destination (CIDR) and target (IGW, NAT instance/Gateway, VPG, Peering)
```

DHCP option sets

```
- Configuration for hosts
- domain name, domain name servers (DNS entry), netios node type, ntp
- can be changed after VPC is greated
```

Security Group - Instance

```
- When multiple Security Groups are assigned to the instance - union is used.
- Exists on only within VPC
- Statefull
- Inbound and Outbound
- Applied immediately
- Applied to instance
- You can have multiple security groups associated to the instance
- Security groups are associated with network interfaces. Changing an
instance's security groups changes the security groups associated with the
primary network interface (eth0)
- You can assing specific security group to additional interface (Network
Interfaces)
- Rules are block by default
- Only Allow rules can be added
- Rule can have:
    - Protocol
    - Port Range
    - ICMP Type
    - Source or Destination (in or out):
        - IP Address (range, CIDR)
        - Another Security Group
    - Description
```

NACLs - Subnet

```
- Stateless (require in and out rules)
- Supports both deny and accept rules
- Rules are evaluated by number, lowest first, first rule that matches is
executed
- One subnet - one NACL
```

IGW

```
- Translates public addresses to private ones
- EC2 instances are only aware of their private addresses, IGW translates to
public ip
```

EIP - REGION

```
- Does not support Tagging
- Static public IP Adress
- Can be assinged to one instance at a time
- Cost only when not assigned
- Has to be released
- Can be attached to instance in different VPC
```

ENI - Availability Zone

```
- Elastic Network Interface
- One Public IP, One or more Private IP
- One instance can have multiple ENI
- Instance can have ENI from different subnets
- Number of ENIs you can attach varries by Instance Type
```

Endpoints

```
- Local enpoints inside VPC for S3 and DynamoDB
- You can specify Policies
- You can have multiple endpoints in VPC with different policies
- Needs to be added to route table (source service, destination endpoint)
```

Peering - REGION

```
- Connection between two VPC
- Can be created between two VPC with different AWS accounts (account id and
vpc id)
- Request/Accept
- Request Expires
- Non overlapting CIDRs
- One-to-one
- only within one region
- No transative routing
- only one Peering between two VPCs
```

NAT

```
Once you create instance or Gateway you have to add rule to Route table to
route traffic from subnet to NAT
### Gateway
    - you have to specify public subnet
    - uses EIP,
    - managed,
    - highly available
### Instance
    - Runs in public subnet
    - Needs source/destination check disabled
    - use NAT AMI
    - set security group
```

VPN (Virtual Private Gateway)

```
### VPG Virtual Private Gateway
    AWS side of VPN connection
    - one VPG per VPC
    - can be detached attached to other VPC
### CGW Customer Gateway
    Customer side of VPN connection
    - you can have multipe CGW for each VPG (multi to one)
- Can use dynamic routing if CGW supports BGP
- Can use static routing
- Uses IPsec
- VPN tunnel must be initiated from Customer side (CGW)
- VPN connections consist of two tunnels for HA
- CloudHub - VPN connection between branches over AWS - Requires BGP
```

VPC Flow Logs

```
- Set on a subnet
- Once created can't be changed, you have to create new one and delete old one
- It always shows primary IP address of the instance
- Logs are sent to CloudWatch Log group
```