4 VPC

VPC Sizing and structure

Custom VPC's

VPC subnets

Subnets are what AWS services run from inside the VPC's and are used to add structure, functionality and resilience to your VPC's.

Subnets when created in AWS are private by default and can be made public through configuration.

- A subnet is a subnetwork of a VPC within a particular Availabilty Zone (if AZ fails, subnet fails and so all ressources in that subnet fail). 1 Subnet is in 1 Availability Zone (important for exam) and can never be in more than 1 AZ. But 1 AZ can have multiple subnets.
- The IPv4 CIDR block is a subset of the VPC CIDR block.
- The IPv4 CIDR block of the subnet can't overlap with a CIDR block of another subnet in the same VPC.
- IPv6 CIDR blocks are also supported if enabled on the VPC. Default is /64 subset of the /56 VPC block.
- Subnets can communicate with other subnets in the same VPC by default.

Subnet IP adressing

- Every subnet has 5 IP addresses reserved by AWS:
    - Network address (the first IP address of the subnet: x.x.x.0)
    - VPC router (the second IP address of the subnet: x.x.x.1 Network +1)
    - DNS server (the third IP address of the subnet: x.x.x.2 Network +2)
    - Reserved by AWS for future use (the fourth IP address of the subnet: x.x.x.3 Network +3)
    - Network broadcast address (the last IP address of the subnet: x.x.x.255)

VPC Routing, Internet Gateway and Bastion Hosts

- Every VPC has a VPC router that is highly available and managed by AWS. It runs in all the AZ that the VPC uses.
- A VPC has a Main route table and the optional subnet route table can be associated with the main route table. A subnet can only be associated with one route table at a time. But a route table can be associated with multiple subnets. The destination column in a route table is the CIDR block of the destination network. The target is the target for the traffic. The target can be:
    - Local: The subnet itself
    - Internet Gateway: The internet
    - Virtual Private Gateway: A VPN connection
    - Direct Connect Gateway: A Direct Connect connection
    - Peering Connection: A VPC peering connection
    - NAT Gateway: A NAT gateway
    - Egress Only Internet Gateway: An egress-only internet gateway

    - Gateway VPC Endpoint: A gateway VPC endpoint
    - Interface VPC Endpoint: An interface VPC endpoint
    - VPC Endpoint Service: An endpoint service
    - Prefix List: A prefix list

The priority of the route is determined by the most specific route. If there are multiple routes that match the same destination, the most specific route is used. For example if there is a route for 0.0.0.0/0 (all IP adresses) and a route for 127.31.0.0/16, the route for 127.31.12.25 will be the 127.31.0.0/16 as it is more specific. ==> Higher prefix values are more specific = higher priority (/32 is 1 IP address so it is the most specific)

Internet Gateway

- An Internet Gateway is a **regional resiliant** service that allows communication between instances in your VPC and the internet. ***Exam tip: You don't need an internet gateway per AZ as it is a regional service.***
- 1 to 1 relationship between a VPC and an Internet Gateway. A VPC can have 0 to 1 Internet Gateway and an Internet Gateway can be attached to 0 to 1 VPC.
- The internet gateway runs from within the AWS public zone and thus allows services in the VPC to communicate with the internet using public IP addresses.
- IGW is managed by AWS so AWS manages the performance

Using an Internet Gateway:

1. Create an Internet Gateway
2. Attach the Internet Gateway to the VPC
3. Create custom route table
4. Associate the route table with the subnet
5. Add a default route (0.0.0.0/0) that points all traffic to the Internet Gateway
6. Subnet allocate IPv4 (or IPv6) public IP addresses to instances (Nakijken want niet duidelijk)

IPv4 addressing

The service in the subnet is **never aware** of it's public IPv4 address. The Internet Gateway uses a record to translate the public IPv4 address to the private IPv4 address of the instance. **Exam tip:** Never be tricked to try to assign the public IPv4 address of an EC2 instance directly to the Operating System. The OS is never aware of the public IP address. **The public IP address is managed by the Internet Gateway.**

IPv6 addressing

IPv6 addresses are public by default and are assigned to the instance directly. The instance is aware of it's public IPv6 address. The Internet Gateway is just passing the traffic to the instance, it's not doing any translation.

Bastion Hosts and Jump Boxes

Bastion hosts are instances that sit in a public subnet inside a VPC and are used to manage incomming connections. And then they access the internal VPC ressources. Bastion hosts are used to secure the VPC

by not allowing direct access to the internal ressources. Bastion hosts are also used to monitor and log all the connections to the VPC.

Stateful and Stateless firewalls

In an application wether the traffic is inboud or outbound depends on the perspective of the firewall. If the firewall is protecting an API server:

- the traffic coming from the front-end is inbound traffic and the traffic going to the front-end is outbound traffic.
- But an update request from the API server to an update server is inbound traffic from the perspective of the API server and outbound traffic from the perspective of the update server.

Stateful and Stateless firewalls

1. Stateless firewalls don't keep track of the state of the connection:

- You have to specify the **rules for both the inbound and outbound** traffic. If you allow inbound traffic, you have to allow the outbound traffic as well.
- The request component is always to a well known port (inbound or outbound). The response component is often to an ephemeral port (outbound or inbound). That's why the response component often allows the full range of ephemeral ports. This is a security risk.

2. Stateful firewalls **keep track of the state** of the connection:

- You only have to specify the rules for the **inbound traffic**.
- The firewall will **automatically allow the response** traffic to go back out. The firewall keeps track of the state of the connection and allows the response traffic to go back out.

Network Access Control Lists (NACL's)

A network access control list (ACL) is an **optional layer of security** for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

NACL's:

- are stateless. Request and response seen as different traffic.
- only impacts data crossing subnet boundaries. Traffic within the subnet is not impacted by NACL's.
- can explicitly allow or deny traffic.
- IPs/CIDR, Port and protocol can be used to define the rules. No logical resources like security groups.
- can only by assigned to subnets, not to AWS resources.
- Use together with Security Groups to add explicity DENY rules (BAD IPs/Nets). Use SG groups to allow traffic.
- Each subnet can have zero or 1 NACL (default or Custom). Each NACL can be associated with multiple subnets.

Security Groups

Security groups are stateful firewalls: it detecs response traffic automatically.

- Response of allowed (outbound or inbound) request is allowed.
- There is no explicit DENY rule, only explicit ALLOW rules or implicit DENY. **Use with NACL's to add explicit DENY rules.** --> can't block bad actors(IPs) without explicit DENY. Use NACL's for that.
- Layer 7 layer so supports IP/CIDR, Port, Protocol and logical resources like EC2 instances. Including other security groups and itself.
- SG are attached to ENI's(Elastic Network Interfaces) and NOT to instances (even if the UI shows it this way). You actually **attach the SG to the primary ENI of the instance** but not the actual instance. (important for exam)

Network Address Translation (NAT) & NAT Gateway

NAT Gateway

A NAT Gateway is a managed service that allows instances in a private subnet to access the internet. Used for IP masquerading: use a single IP address to hide multiple private IP addresses.

The NAT gateway uses a translation table to translate the private IP addresses of multiple instances in the private subnet and changes source of packets to it's own (internal)source address. Normally a NAT Gateway has a public IP address but not in AWS, because nothing inside VPC has a public IP address. You have to use a VPC router and Internet Gateway to access the internet from a VPC. So the NAT Gateway has a default route in the VPC router that points to the Internet Gateway. The Internet Gateway changes the packet source address to the NAT Gateway public address.

- The NAT Gateway runs from a public subnet
- it uses Elastic IPs (static IPv4 Public)
- AZ resilient service (high availability in that AZ)
- For region resiliece - use NAT Gateway in each AZ and use a Route Table in each AZ with that NAT Gateway as the target. + 1 VPC router and 1 Internet Gateway (regional services)
- NAT Gateway is managed by AWS so AWS manages the performance, scaling(up to 45 Gbps), patching, etc.
- costs based on duration and data volume processed. Not free tier eligble.

Important for exam:

- 1 NAT Gateway per AZ. If you want region resilience, you need a NAT Gateway for every AZ you use in that region.
- NAT Gateway is only for **IPv4 traffic only** it doesn't work with IPv6 traffic. For IPv6 traffic you use an Internet Gateway directly (Egress Only IGW = outbound only). IPv6 addresses in AWS are publicly routable by default so you don't need NAT for IPv6.
- **NAT Gateways don't support Security Groups.** You have to use NACL's to control the traffic (always exam question)

NAT Instance

Network Address Translation is a process of giving a private resource outgoing only access to the internet.

A NAT instance is an EC2 instance that runs the NAT process. All maintenance, perfomance, scaling, etc. is managed by you. You can use this option if you want more customization and control over the NAT process

or also use the instance for other purposes: like a Bastion host or port forwarding. Or if you want to reduce costs during testing or development.

Important for exam

EC2 instance **filters the traffic** to handle only traffic with it's **own source or destination IP**. This will cause the NAT instance to malfuction because it won't handle other traffic. So you have to disable the feature `Source/Destination Checks` on that EC2 instance.