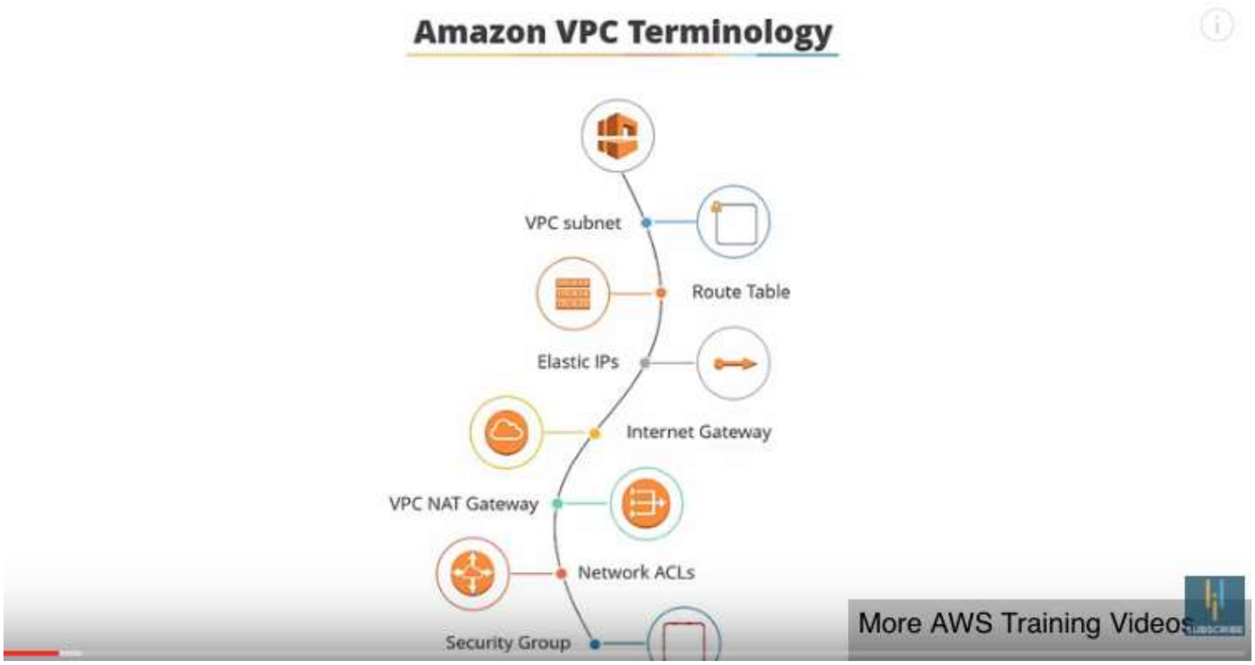
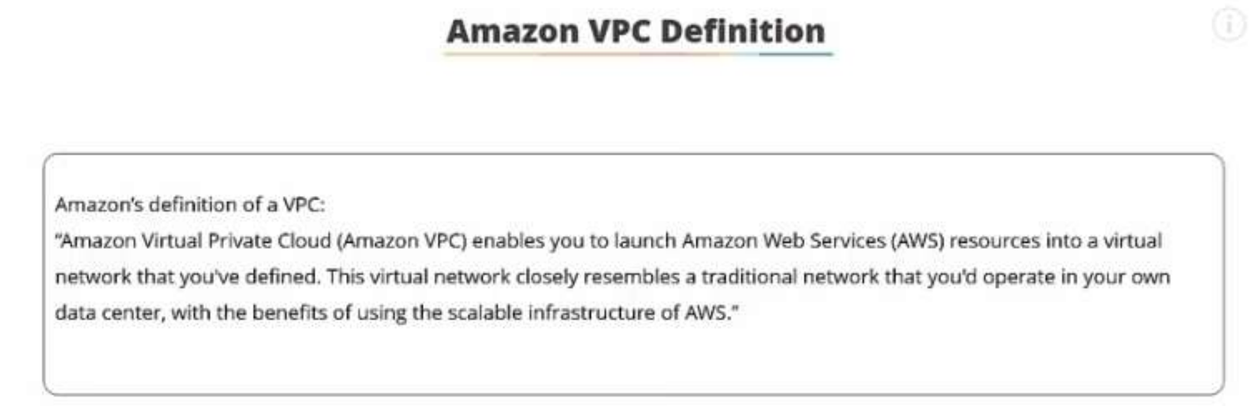
AWS’s Virtual Private Cloud (VPC) | Private IP Addresses, Public IP Addresses, Internet Gateways, Route Tables, NAT Gateways, Security Groups & Network ACLs

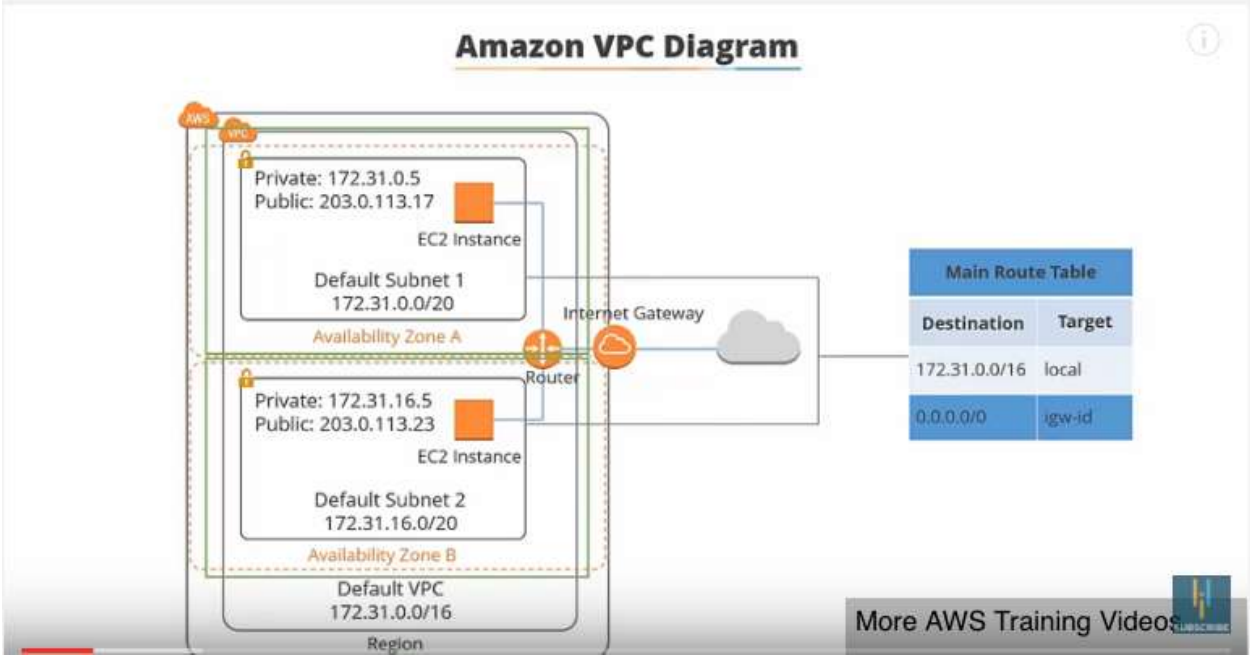


Amazon VPC Terminology



Amazon VPC Definition

Amazon's definition of a VPC:
"Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS."

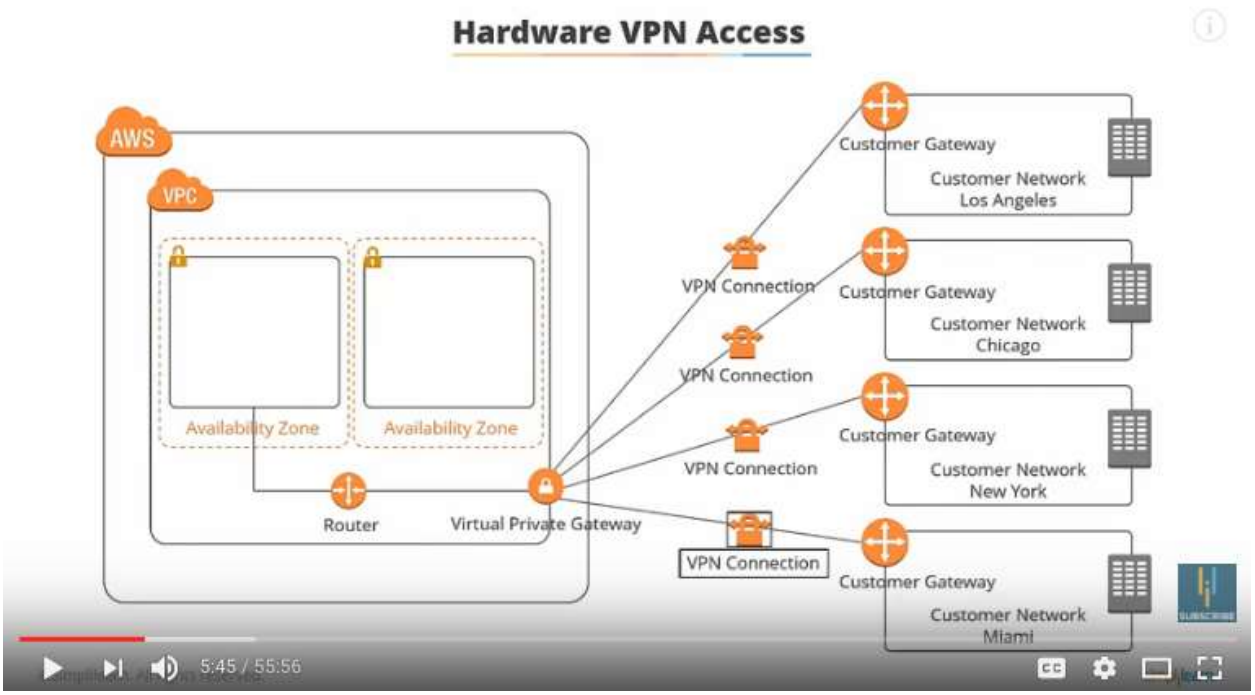


Main Route Table

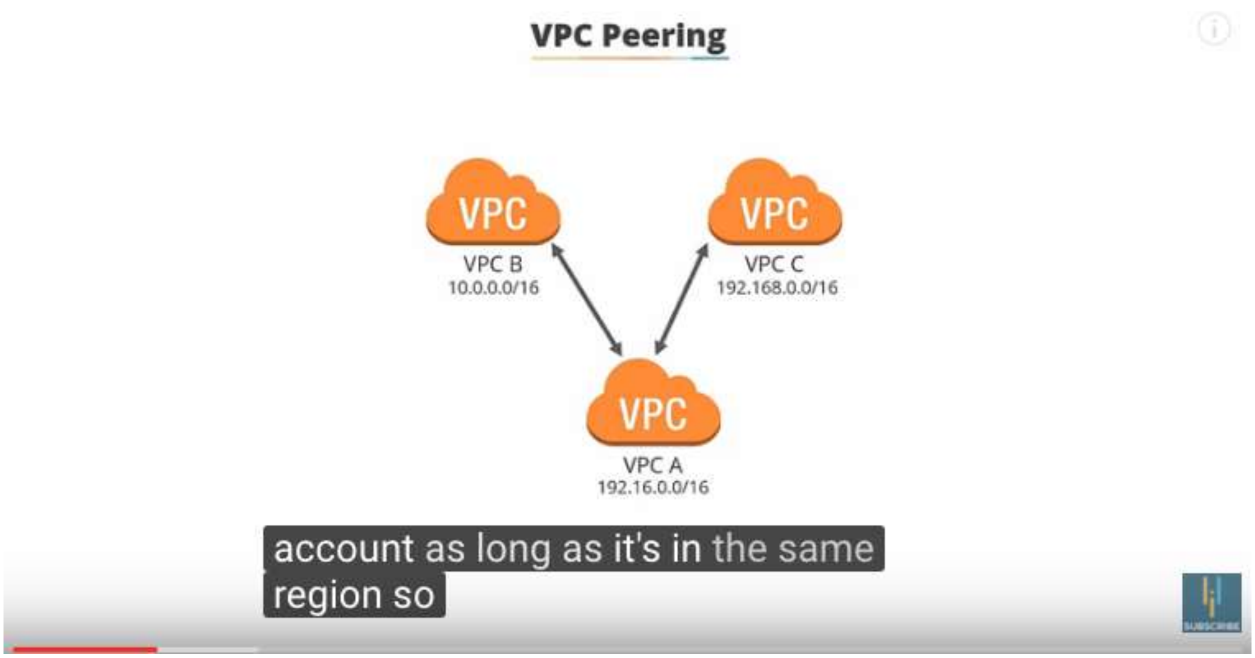
Destination	Target
172.31.0.0/16	local
0.0.0.0/0	igw-id

The default VPC contains over 65,000 private IPs… so why not use it? If you instead create a custom VPC, it is more secure and you can customize (define your own IP address range, create your own public and private subnets, tighten down security settings).

“By default, instances you launch into a VPC can’t communicate with your own network.” So you can connect your VPC to your own data center using **Hardware VPN Access**. “So that you can effectively extend your data center into the cloud and create a hybrid environment”.



To do this, you need a **Virtual Private Gateway**. On the left side (labelled ‘virtual private gateway’) is the **VPN concentrator** on the Amazon side. Then on your side, you need a **customer gateway**, which is either a physical device or a software applicate that sits on your side of the VPN connection. A VPN Tunnel comes up when traffic is generated from your side of the connection.



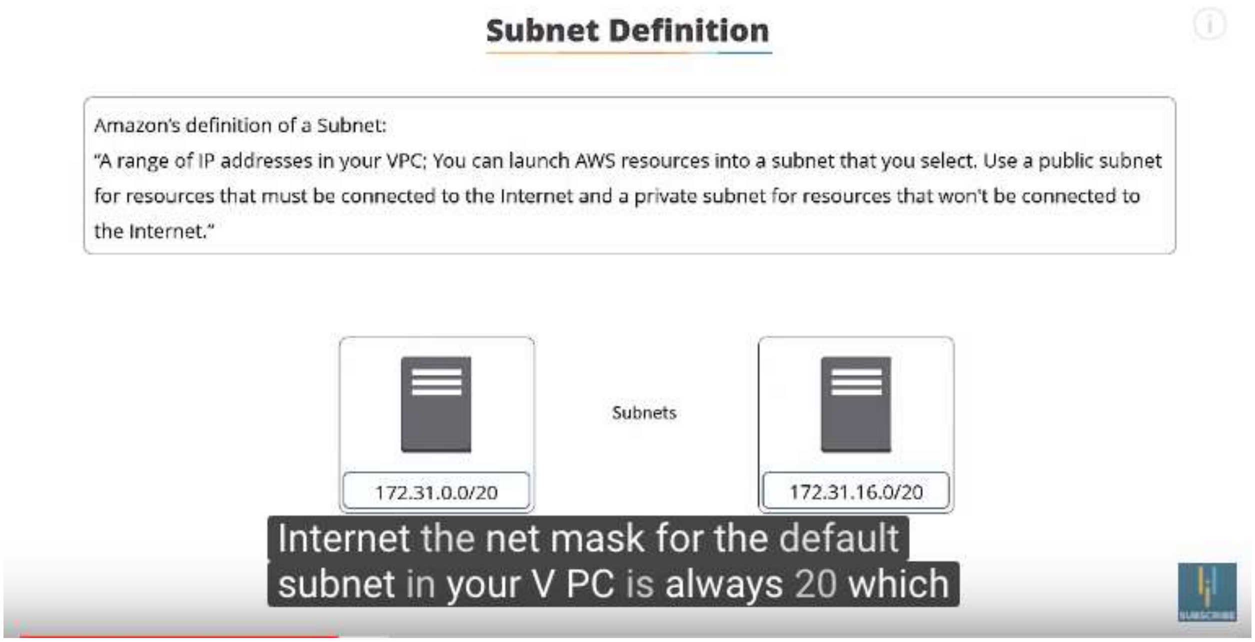
VPC Peering

account as long as it's in the same region so

Can be between your VPCs or other VPCs. VPC A wouldn’t be able to communicate with VPC B or C without a peering connection. Transitive peering does not work, meaning that VPCs need to be directly peered in order to be connected.

Also, VPCs with overlapping **CIDRS** cannot be peered. These are fine because they have different domain ranges, but if they didn’t there would be a problem.

If you delete the default VPC, you have to contact AWS support to get it back again!

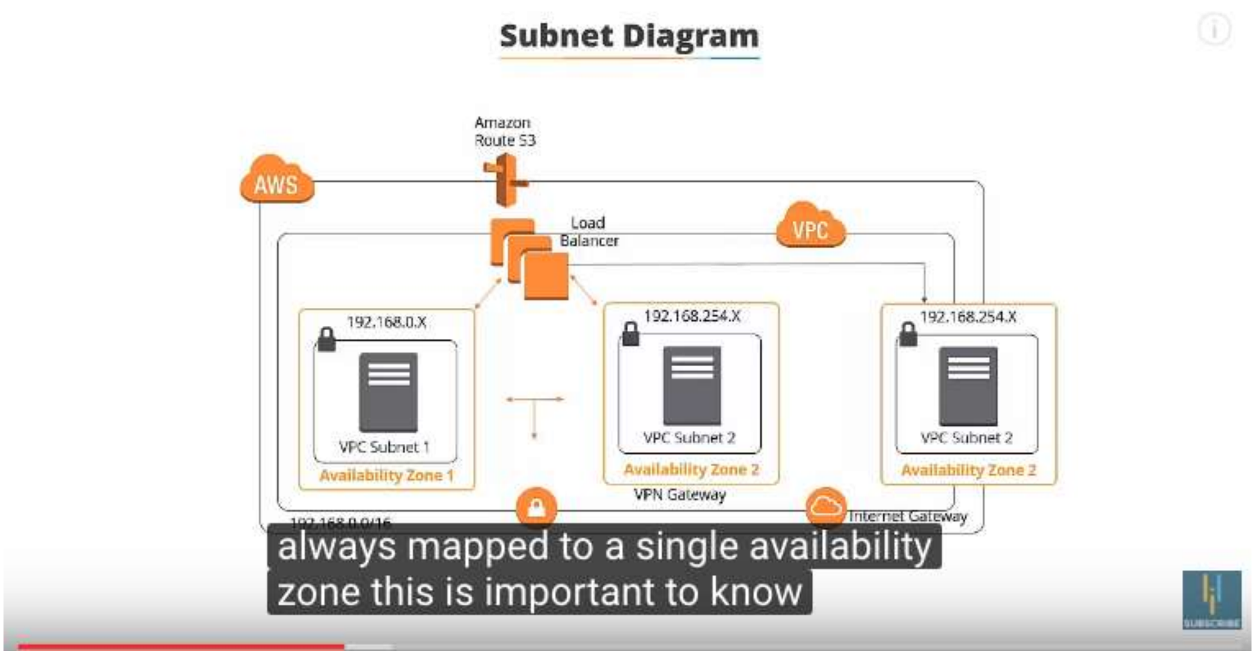


Subnet Definition

Amazon's definition of a Subnet:
"A range of IP addresses in your VPC; You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet and a private subnet for resources that won't be connected to the Internet."

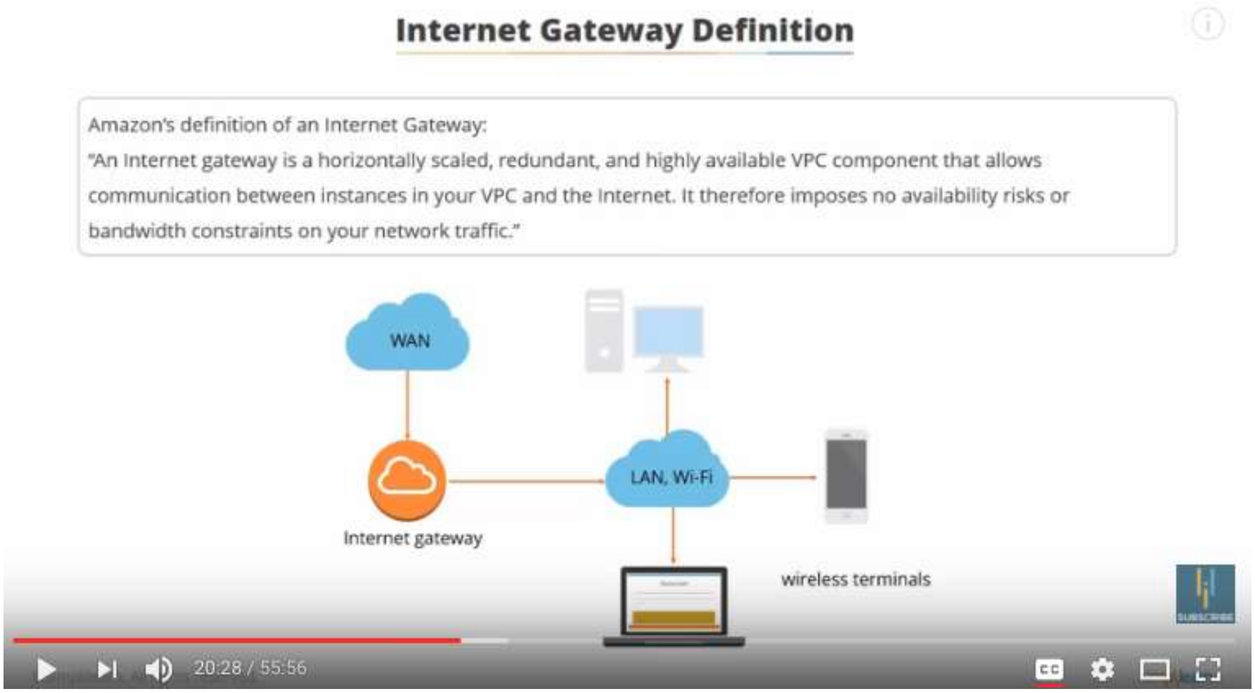
Internet the net mask for the default subnet in your V PC is always 20 which

Default Net Mask in 20 for Subnets. These preserve up to 4096 IP addresses per subnet. Subnets are always mapped to a single availability zone



Subnet Diagram

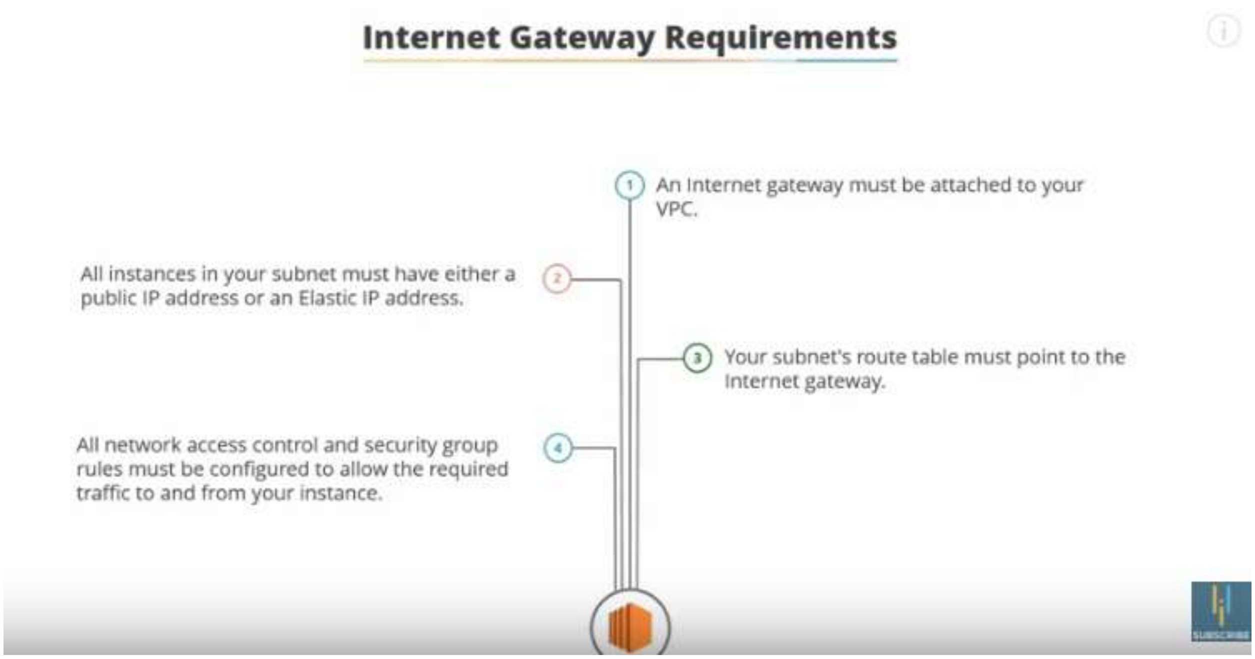
always mapped to a single availability zone this is important to know



Internet Gateway Definition

Amazon's definition of an Internet Gateway:

"An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic."



Internet Gateway Requirements

1. An Internet gateway must be attached to your VPC.

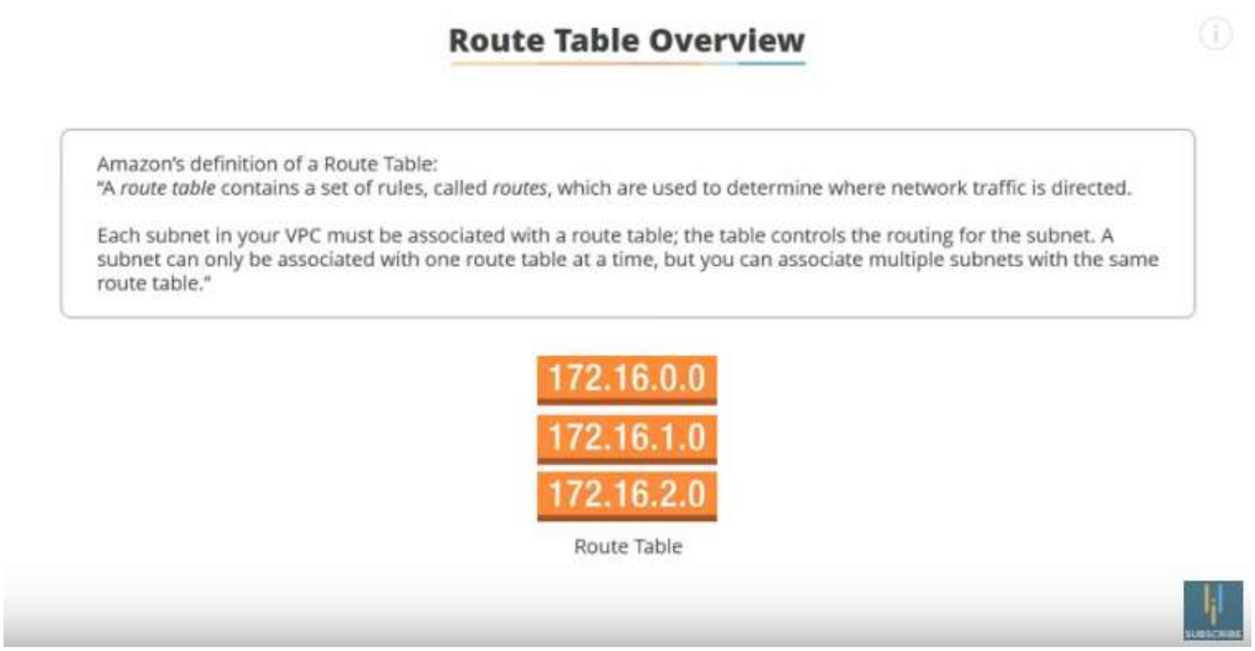
2. All instances in your subnet must have either a public IP address or an Elastic IP address.

3. Your subnet's route table must point to the Internet gateway.

4. All network access control and security group rules must be configured to allow the required traffic to and from your instance.

To attach your VPC to the internet, you need to attach an Internet Gateway, and you can only attach one internet gateway per VPC.

Before our instances can have access to the internet, we need to make sure that our subnet route tables point to the internet gateway.

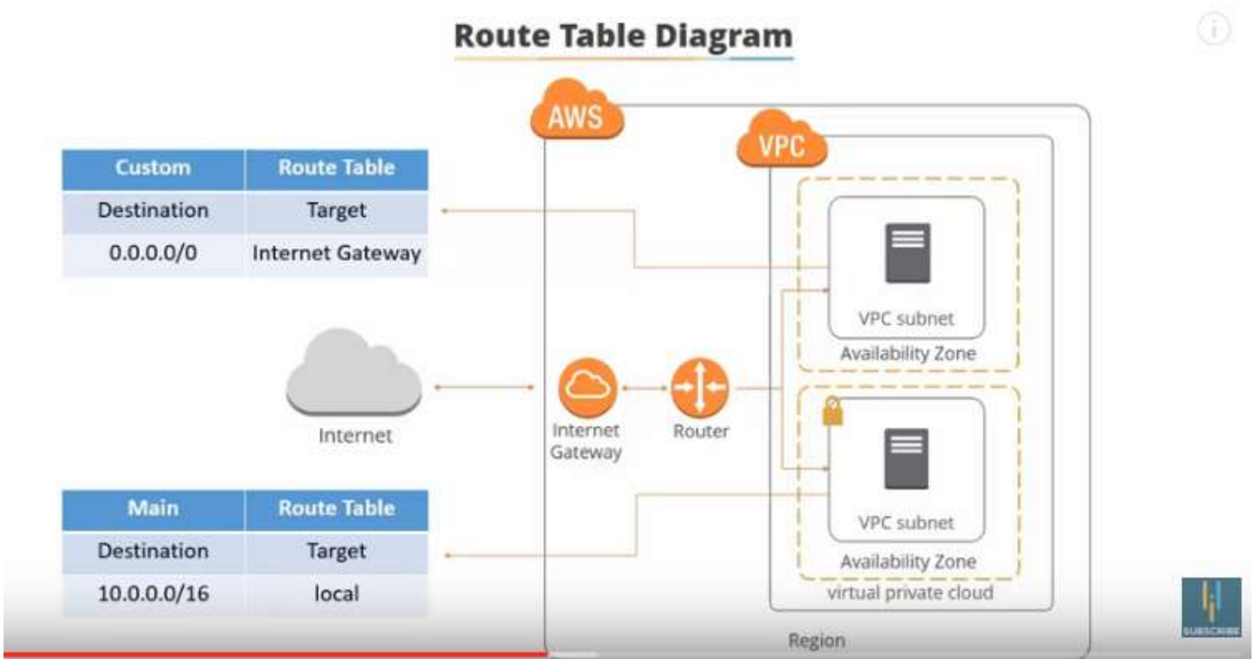


Route Table Overview

Amazon's definition of a Route Table:
"A *route table* contains a set of rules, called *routes*, which are used to determine where network traffic is directed.

Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table."

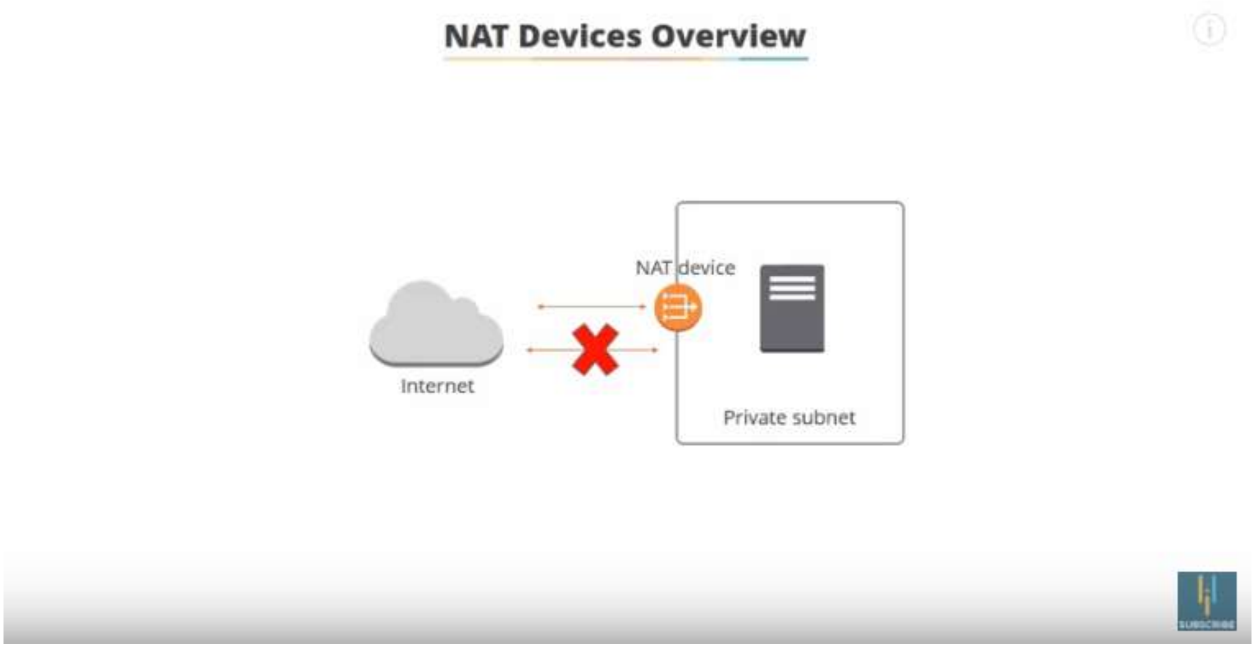
Every VPC has a default route table. It's good practice to create a new one to practice with customization.



Route Table Diagram

Custom	Route Table
Destination	Target
0.0.0.0/0	Internet Gateway

Main	Route Table
Destination	Target
10.0.0.0/16	local



NAT Devices Overview

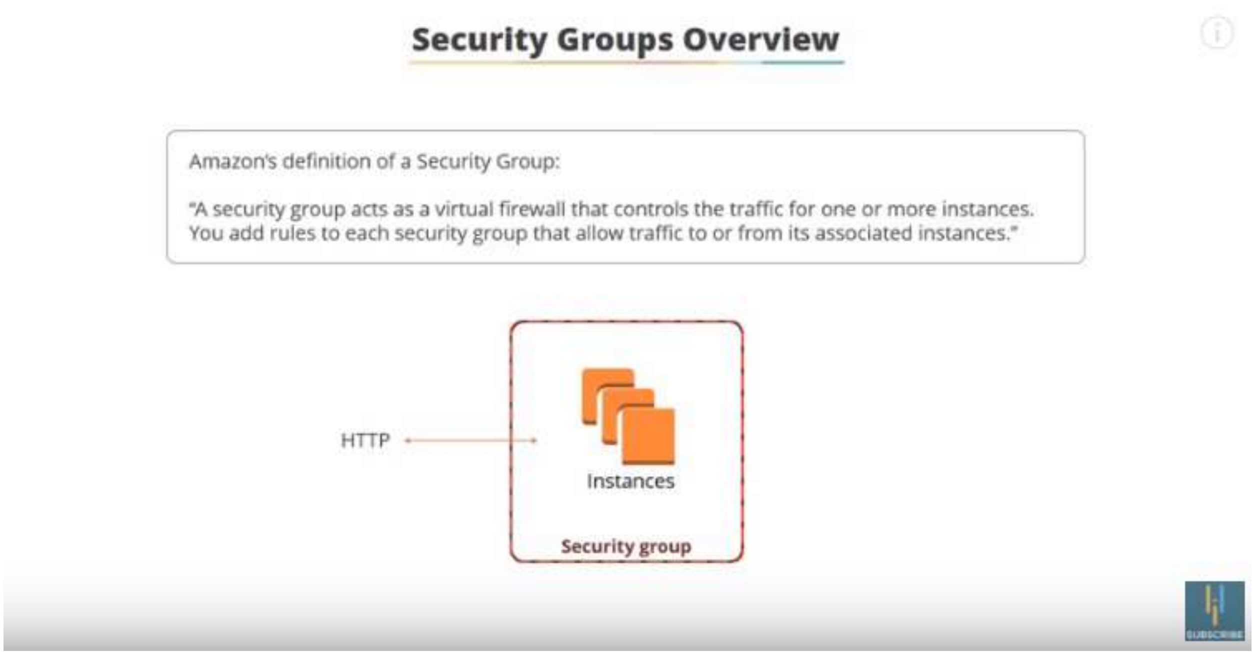
NAT devices [network address translation devices] allow you to give a private subnet to the internet, without allowing the internet to access that subnet.

A NAT device forwards traffic from your private subnet to the internet, or other AWS services, and then sends the response back to the instances. When traffic goes to the internet, the source IP address of your instance is replaced with the NAT device and when the internet traffic comes back again, then that device translates the address to your instance’s private IP address.

A NAT Gateway is recommended by AWS because it is a provided service that gives more bandwidth than NAT Instances. Each NAT Gateway is created in a specific availability zone and is implemented with redundancy.

A NAT Instance is launched from a NAT AMI [Amazon Machine Image] and runs as an instance in your VPC, so it’s something else you have to look after. Whereas, in a NAT Gateway, a fully managed service, you can basically install it and forget about it.

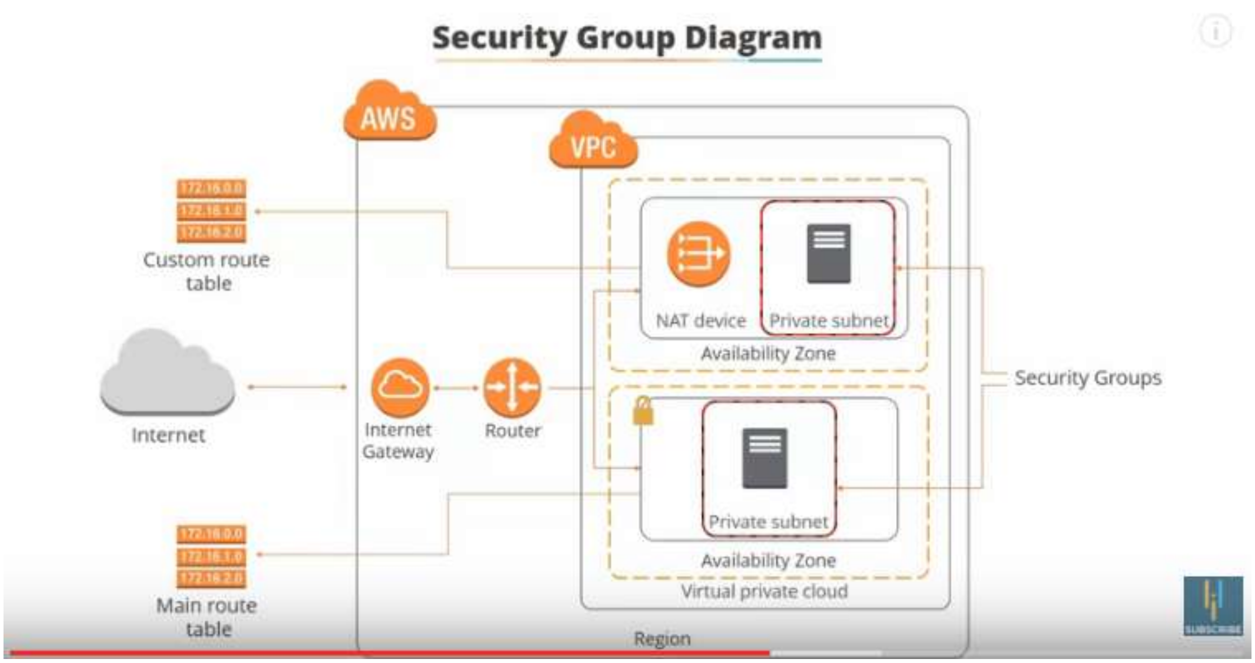
NAT Gateway must be launched into a public subnet because it needs internet connectivity.



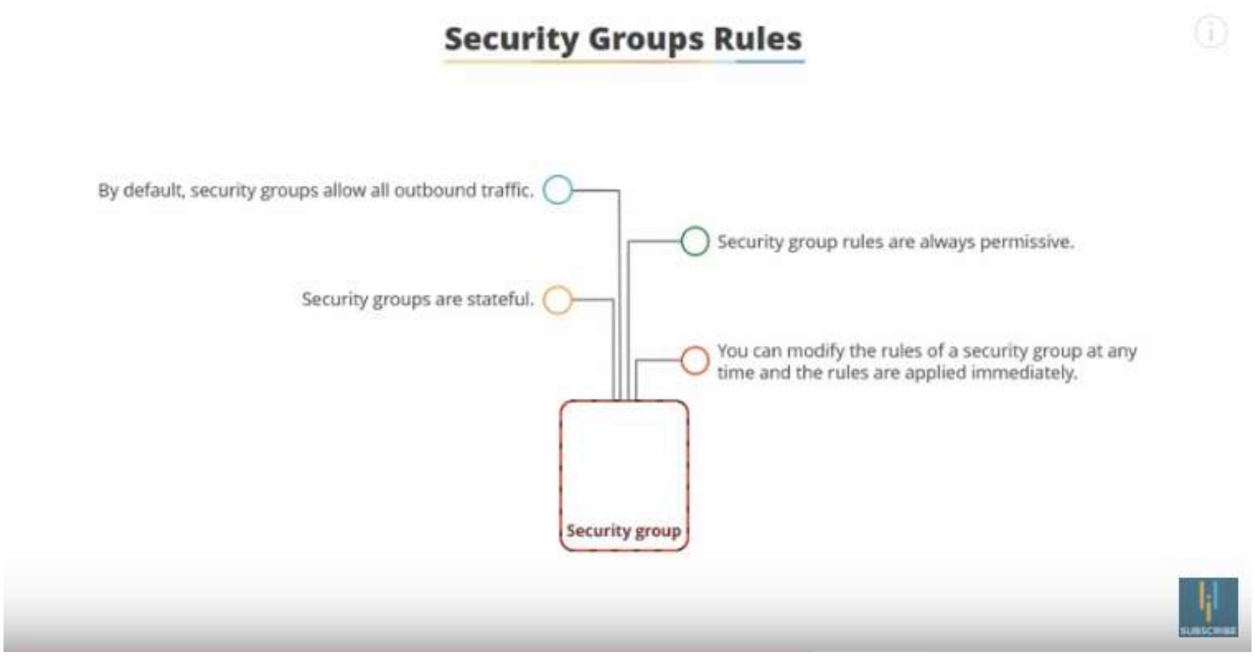
Security Groups Overview

Amazon's definition of a Security Group:

"A security group acts as a virtual firewall that controls the traffic for one or more instances. You add rules to each security group that allow traffic to or from its associated instances."



Security Group Diagram



Security Groups Rules

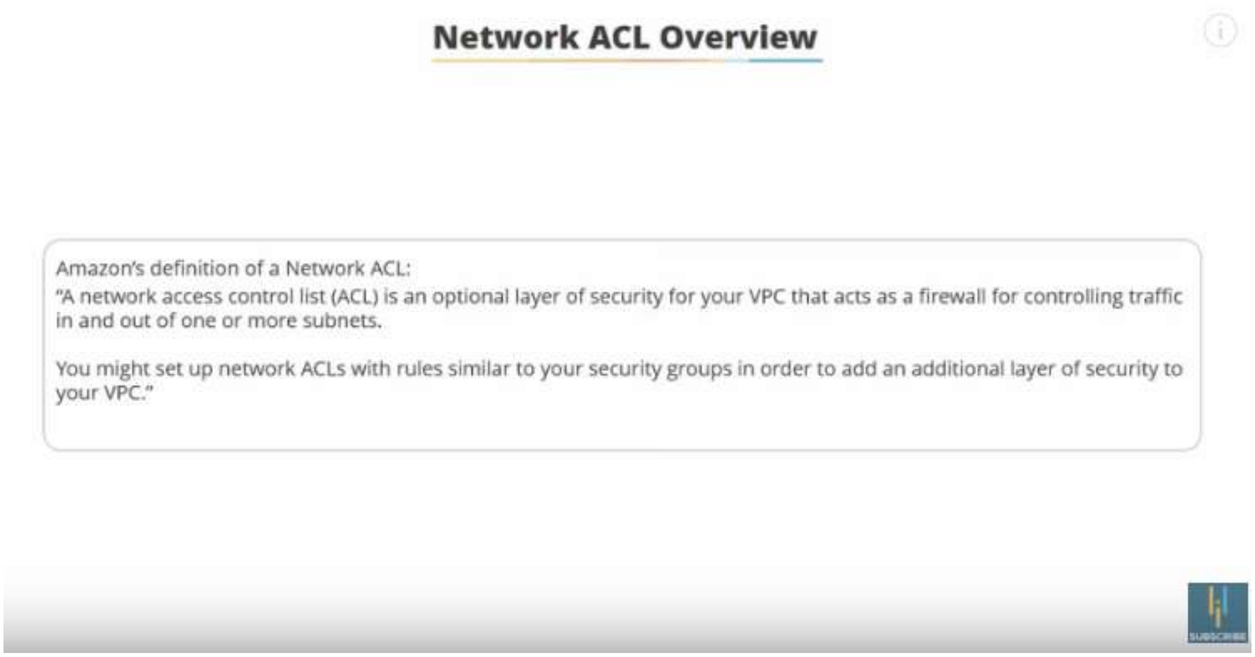
By default, security groups allow all outbound traffic.

Security group rules are always permissive.

Security groups are stateful.

You can modify the rules of a security group at any time and the rules are applied immediately.

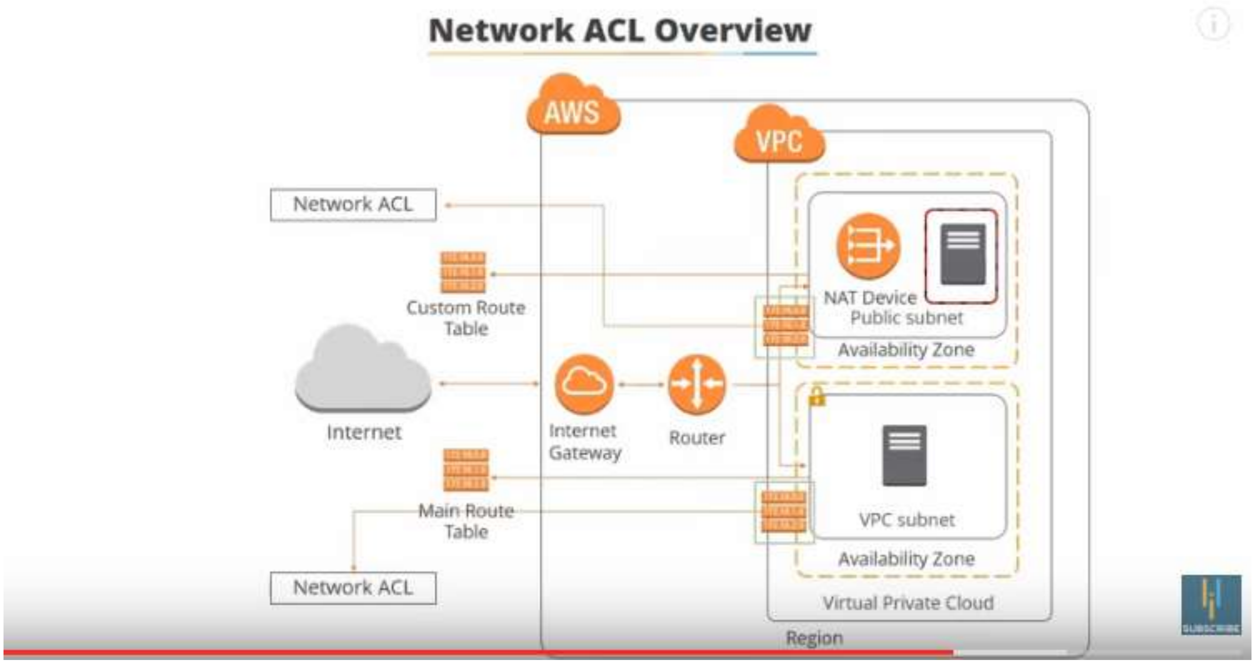
Now, for Network ACLs:



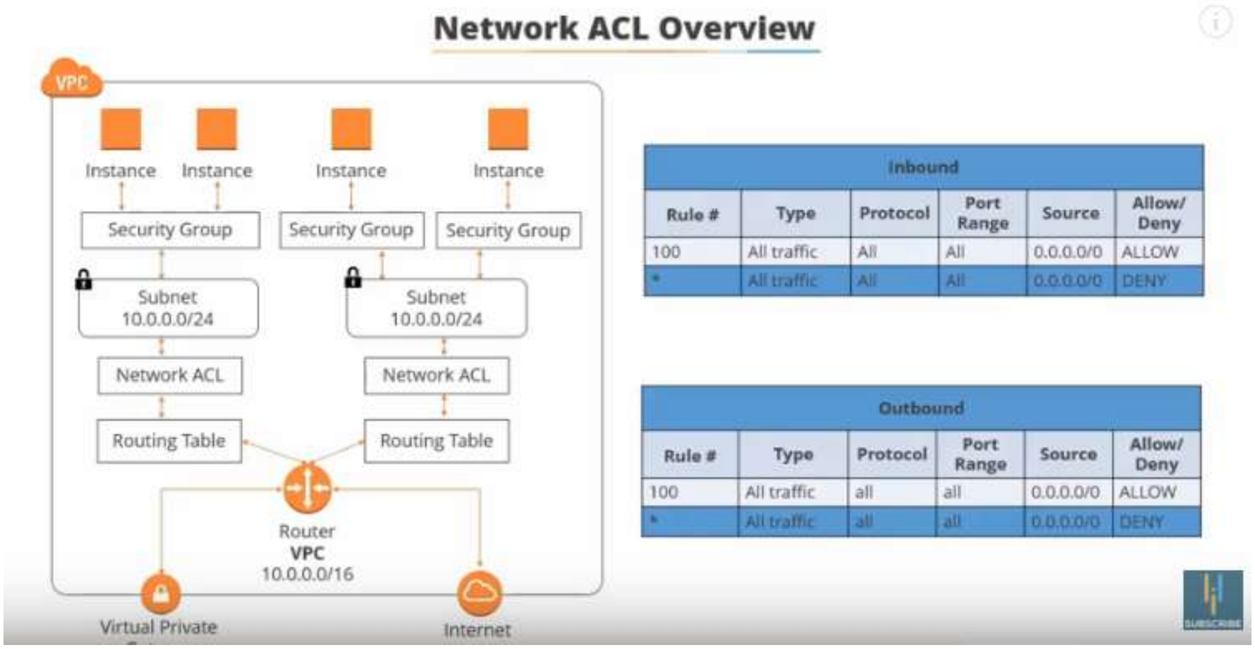
Network ACL Overview

Amazon's definition of a Network ACL:
"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."



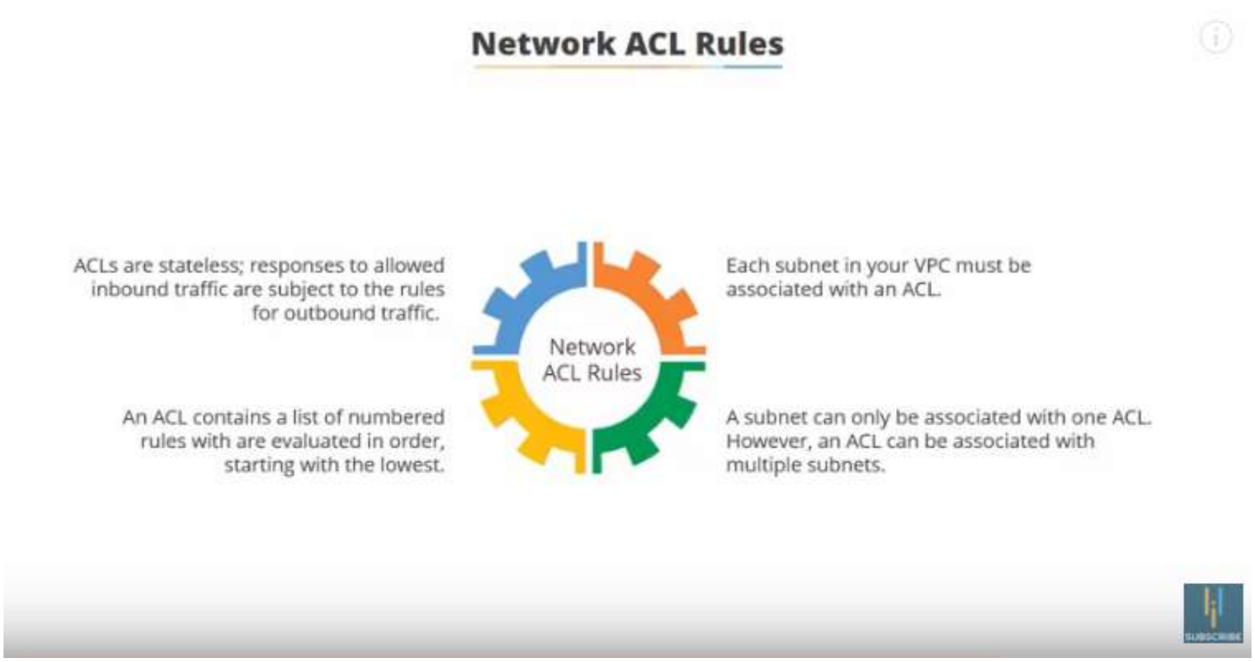
Network ACL Overview



Network ACL Overview

Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/ Deny
100	All traffic	All	All	0.0.0.0/0	ALLOW
*	All traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule #	Type	Protocol	Port Range	Source	Allow/ Deny
100	All traffic	all	all	0.0.0.0/0	ALLOW
*	All traffic	all	all	0.0.0.0/0	DENY



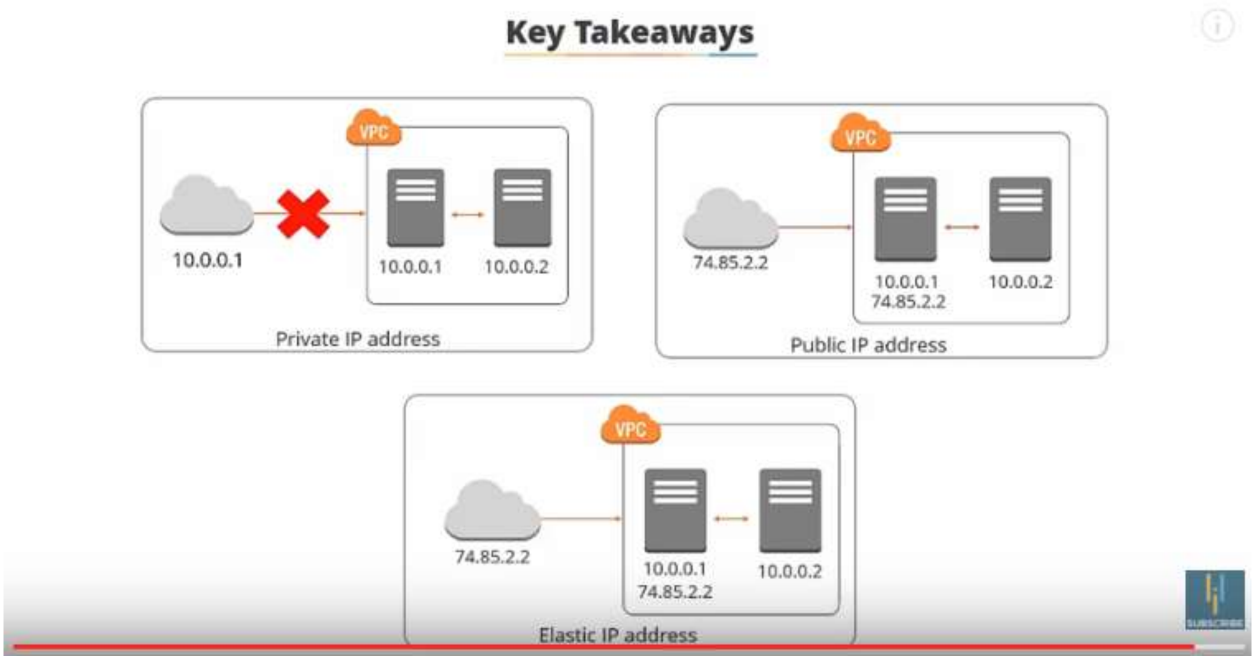
Network ACL Rules

ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic.

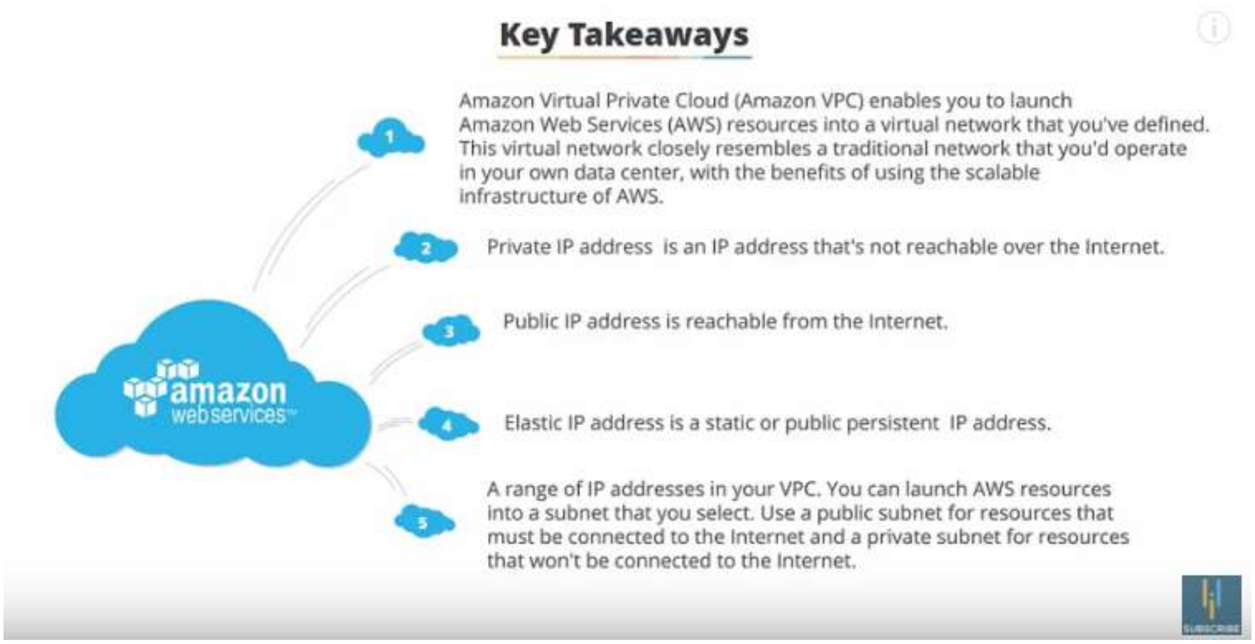
An ACL contains a list of numbered rules with are evaluated in order, starting with the lowest.

Each subnet in your VPC must be associated with an ACL.

A subnet can only be associated with one ACL. However, an ACL can be associated with multiple subnets.

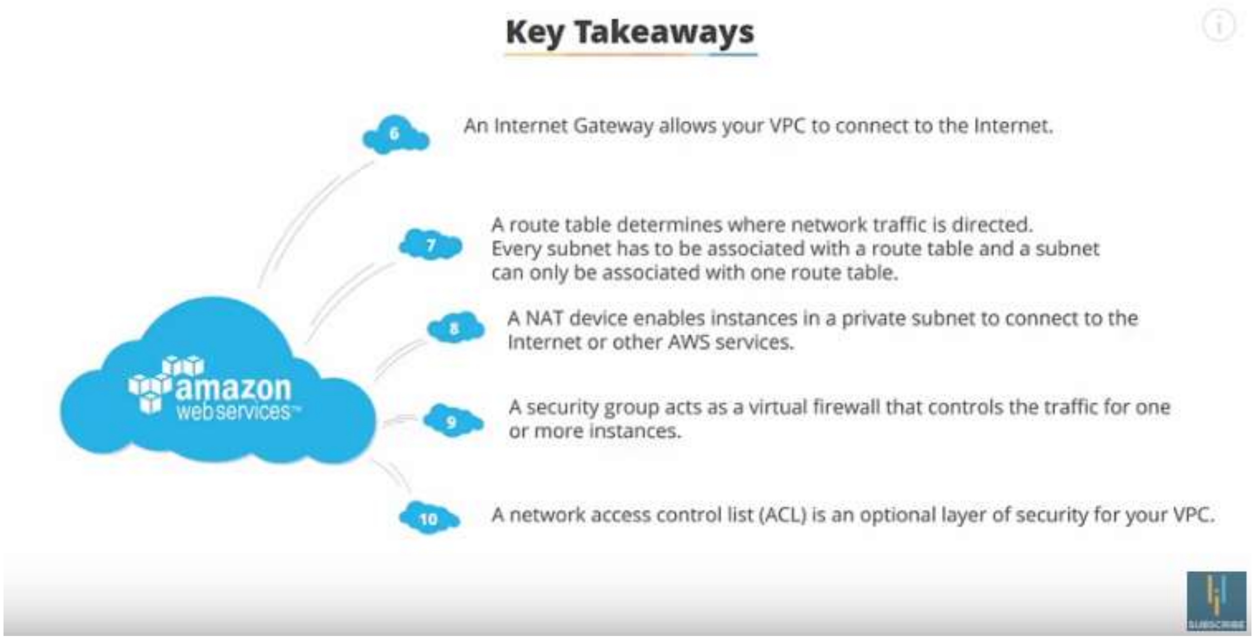


Key Takeaways



Key Takeaways

1. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
2. Private IP address is an IP address that's not reachable over the Internet.
3. Public IP address is reachable from the Internet.
4. Elastic IP address is a static or public persistent IP address.
5. A range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet and a private subnet for resources that won't be connected to the Internet.



Key Takeaways

6. An Internet Gateway allows your VPC to connect to the Internet.
7. A route table determines where network traffic is directed. Every subnet has to be associated with a route table and a subnet can only be associated with one route table.
8. A NAT device enables instances in a private subnet to connect to the Internet or other AWS services.
9. A security group acts as a virtual firewall that controls the traffic for one or more instances.
10. A network access control list (ACL) is an optional layer of security for your VPC.