
VPC
Virtual Private Cloud

A CLOUD GURU

What Is a VPC?

Think of a VPC as a virtual data center in the cloud.

- Logically isolated part of AWS Cloud where you can define your own network.
- Complete control of virtual network, including your own IP address range, subnets, route tables, and network gateways.

Fully Customizable Network

You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Web

Public-facing subnet.

Application

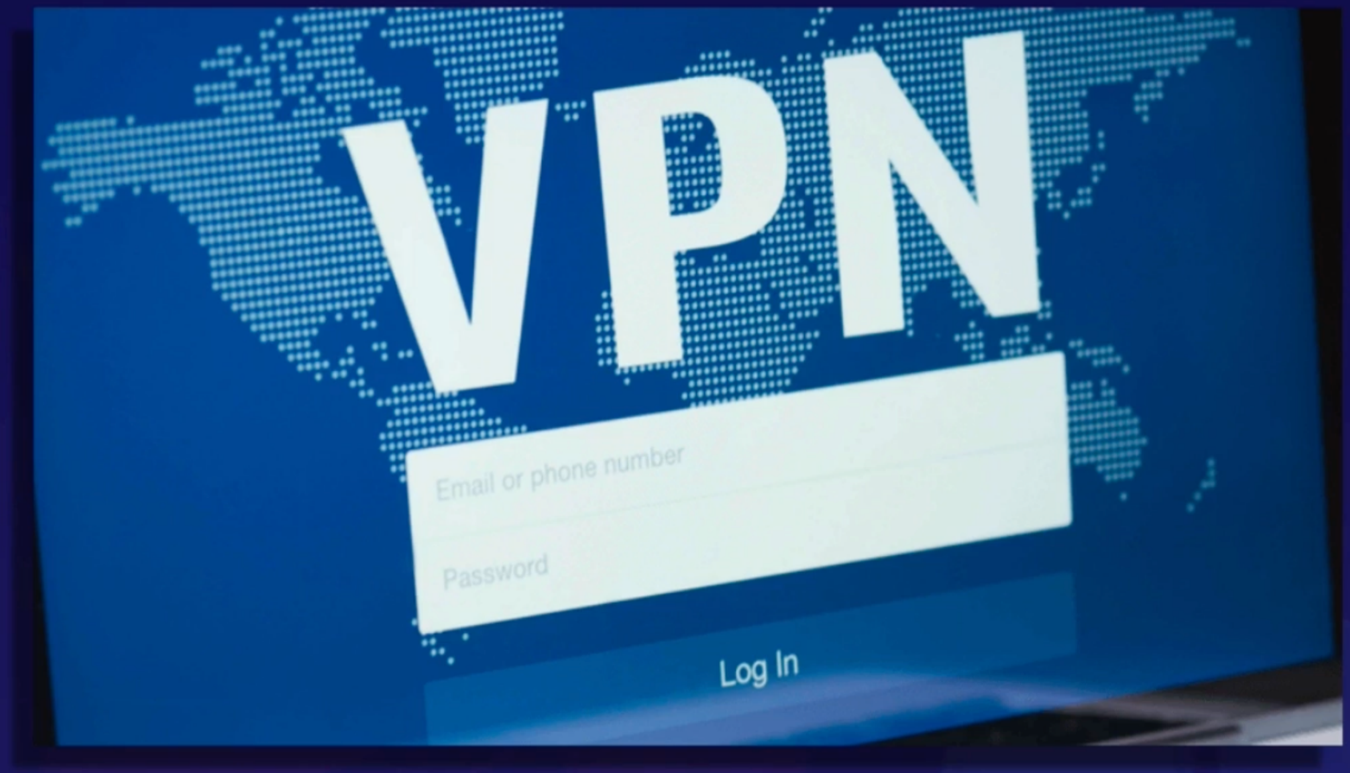
Private subnet. Can only speak to web tier and database tier.

Database

Private subnet. Can only speak to application tier.

VPNs

Additionally, you can create a **hardware Virtual Private Network (VPN)** connection between your corporate data center and your VPC and leverage the AWS Cloud as an extension of your corporate data center.



VPC Features

What can we do with a VPC?

Launch Instances
Launch instances into a subnet of your choosing.

Internet Gateway
Create internet gateway and attach it to our VPC.

Custom IP Addresses
Assign custom IP address ranges in each subnet.

More Control
Much better security control over your AWS resources.

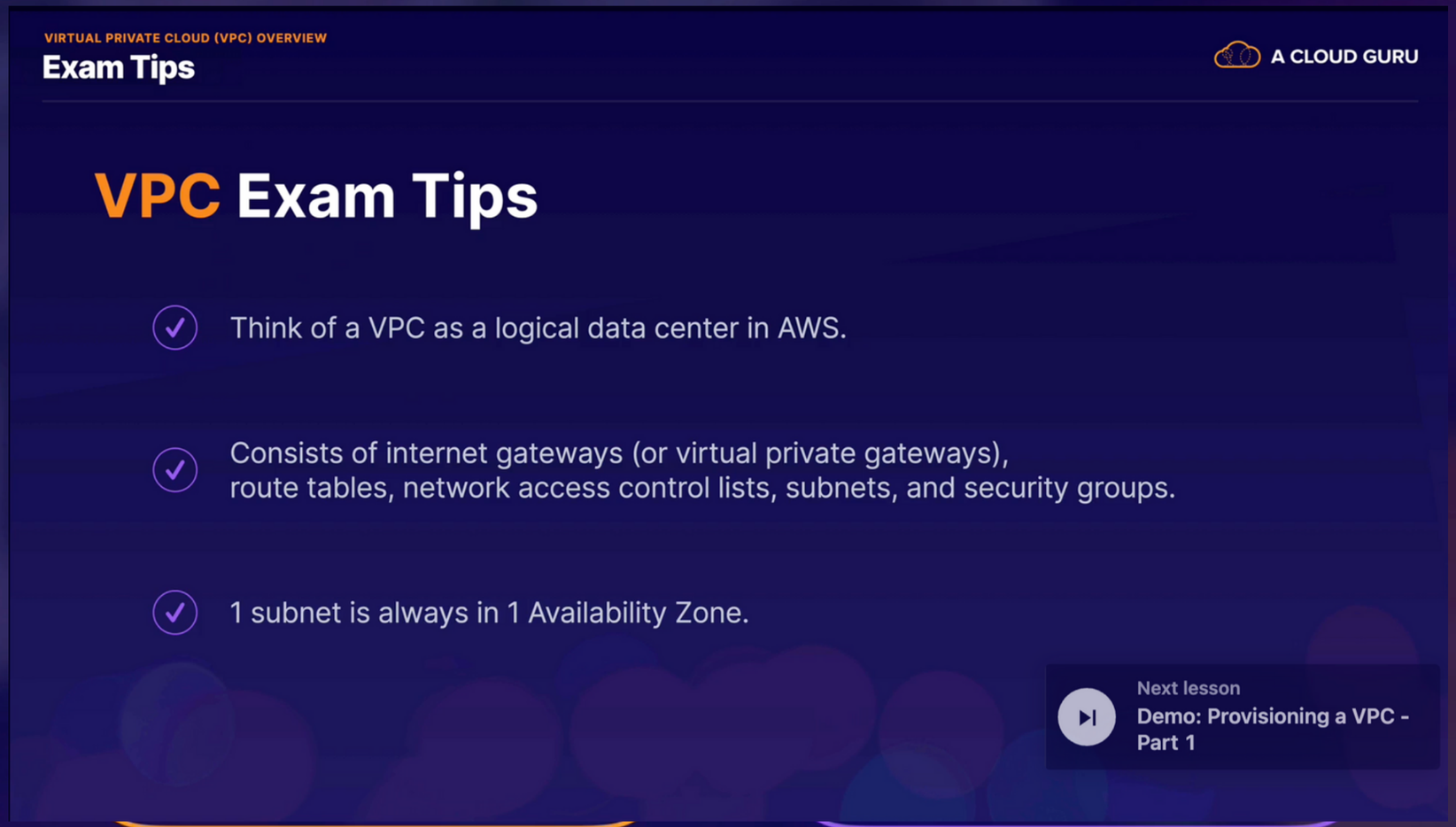
Route Tables
Configure route tables between subnets.

Access Control Lists
Subnet network access control lists.

BONUS TIP

You can use network access control lists (**NACLs**) to block specific IP addresses.

Comparing VPCs



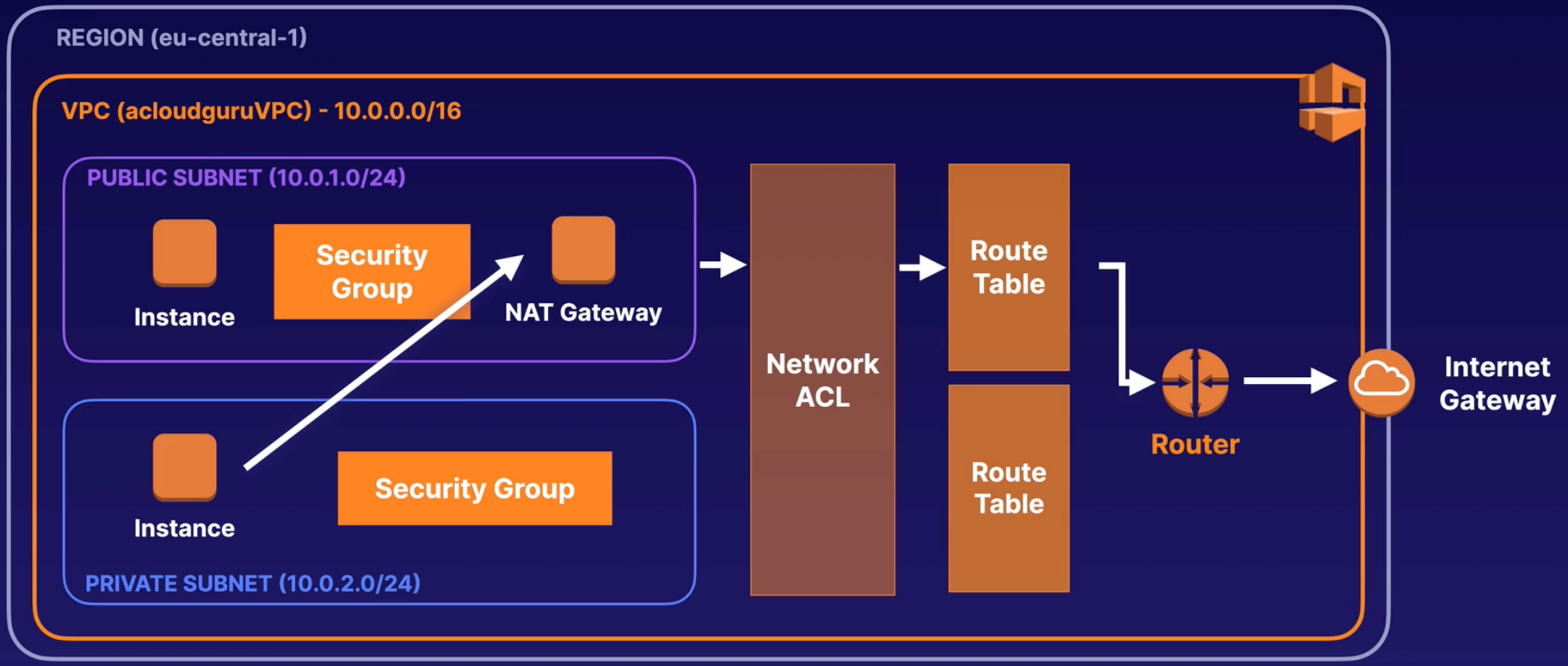
What Is a NAT Gateway?

NAT Gateways

You can use a network address translation (NAT) gateway to **enable instances in a private subnet** to connect to the internet or other AWS services while preventing the internet from initiating a connection with those instances.

Network Diagram

VPC with Public and Private Subnet(s)



5 Facts to Remember about NAT Gateways

- Redundant inside the Availability Zone
- Starts at 5 Gbps and scales currently to 45 Gbps
- No need to patch
- Not associated with security groups
- Automatically assigned a public IP address

What Is a Network ACL?

Network ACLs

The first line of defense

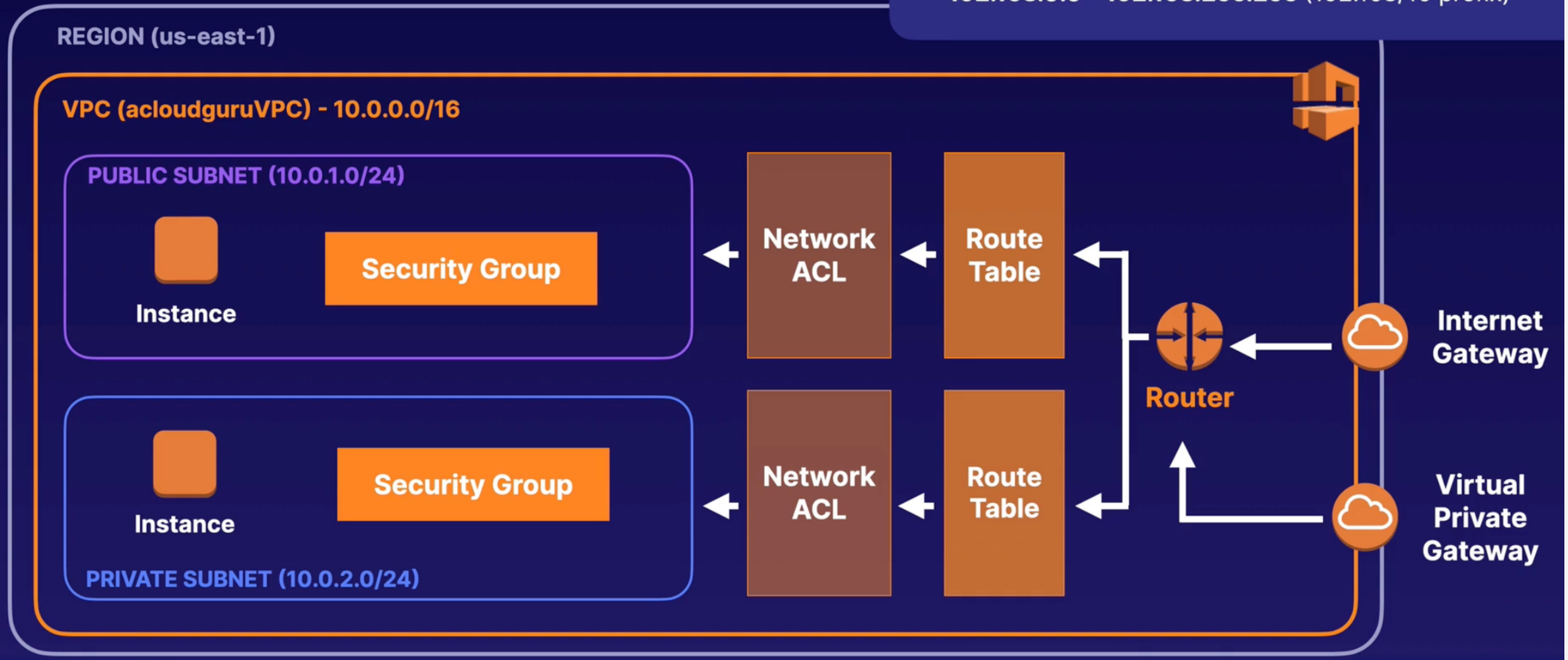
- A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

- You might set up network ACLs with rules similar to your security groups in order to add another layer of security to your VPC.

Network Diagram

VPC with Public and Private Subnet(s)

- **10.0.0.0 – 10.255.255.255** (10/8 prefix)
- **172.16.0.0 – 172.31.255.255** (172.16/12 prefix)
- **192.168.0.0 – 192.168.255.255** (192.168/16 prefix)



Overview of Network ACLs

- **Default Network ACLs:** Your VPC automatically comes with a default network ACL, and by default it allows all outbound and inbound traffic.
- **Custom Network ACLs:** You can create custom network ACLs. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- **Subnet Associations:** Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.
- **Block IP Addresses:** Block IP addresses using network ACLs, not security groups.

Network ACLs Tips

Network ACLs

- You can associate a network ACL with multiple subnets; however, a subnet can be associated with **only 1 network ACL** at a time. When you associate a network ACL with a subnet, the previous association is **removed**.
- Network ACLs contain a **numbered list of rules** that are evaluated in order, starting with the **lowest** numbered rule.
- Network ACLs have **separate** inbound and outbound rules, and each rule can either **allow or deny traffic**.
- Network ACLs are **stateless**; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).