Passing the AWS Cloud Practitioner exam

Study Group #3: EC2 & VPC

Presented By:
Christophe Limpalair,
Linux Academy

Linux Academy

Homework Quiz

7) How would a system administrator add an additional layer of login security to a user's AWS Management Console?

A) **Use AWS Cloud Directory**

B) **Audit AWS Identity and Access Management (IAM) roles**

C) **Enable Multi-Factor Authentication**

D) **Enable AWS CloudTrail**

Homework Quiz

7) How would a system administrator add an additional layer of login security to a user's AWS Management Console?

A) **Use AWS Cloud Directory**

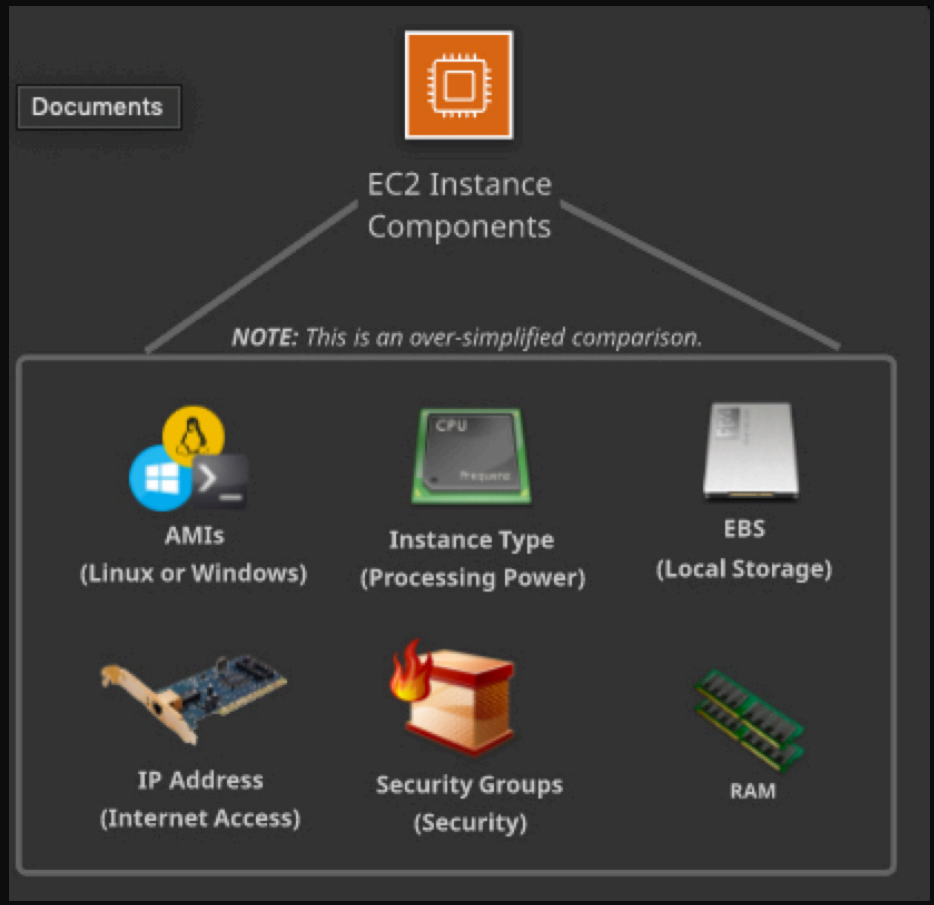
B) **Audit AWS Identity and Access Management (IAM) roles**

C) **Enable Multi-Factor Authentication**

D) **Enable AWS CloudTrail**

Elastic Cloud Compute (EC2) Instances

- Virtual computer / server
- Use cases:
  - Web servers & applications
  - Customer-managed databases
  - Workloads that require compute power
- Purchase options:
  - On-Demand (pay as you go)
  - Reserved Instances
  - Spot Instances



EC2 Reserved Instances

- Options:
  - Standard RI
    - Up to 75% off On-Demand price
  - Convertible RI
    - Up to 54% off On-Demand price
    - Can be exchanged for equal or greater value instances
  - Scheduled RI
    - RIs needed only for a specific schedule
- Other benefits:
  - 1 or 3 year commitments
  - Capacity & cost-savings can be shared across accounts with consolidated billing
  - Can be assigned to 1 AZ or multiple AZs in a region

EC2 Spot Instances

- For workloads that can be interrupted
- Up to 90% off On-Demand prices
- Use cases:
  - Containerized workloads
  - Big data workloads
  - Test or development workloads

Pop Quiz

You are running 10 m4.large instances and plan to keep those running for at least a year. However, you may need to increase the instance size after about 4 months. What can you purchase to reduce costs yet remain flexible?

A) Flexible Reserved Instances

B) Upgradable Reserved Instances

C) Standard Reserved Instances

D) Convertible Reserved Instances

Pop Quiz

You are running 10 m4.large instances and plan to keep those running for at least a year. However, you may need to increase the instance size after about 4 months. What can you purchase to reduce costs yet remain flexible?

A) Flexible Reserved Instances

B) Upgradable Reserved Instances

C) Standard Reserved Instances

D) Convertible Reserved Instances

Pop Quiz

You are running a workload on AWS that can be interrupted but that needs to work at massive scale. Which instance type would be the best option for this workload in order to minimize cost?

A) Convertible Reserved Instances

B) Spot Instances

C) On-Demand Instances

D) Scheduled Reserved Instances

Pop Quiz

You are running a workload on AWS that can be interrupted but that needs to work at massive scale. Which instance type would be the best option for this workload in order to minimize cost?

A) Convertible Reserved Instances

B) Spot Instances

C) On-Demand Instances

D) Scheduled Reserved Instances

Virtual Private Cloud (VPC)

A VPC is a private section of AWS where you can place AWS resources (like EC2 instances and databases). You have full control over who can access those resources.

Important concepts:

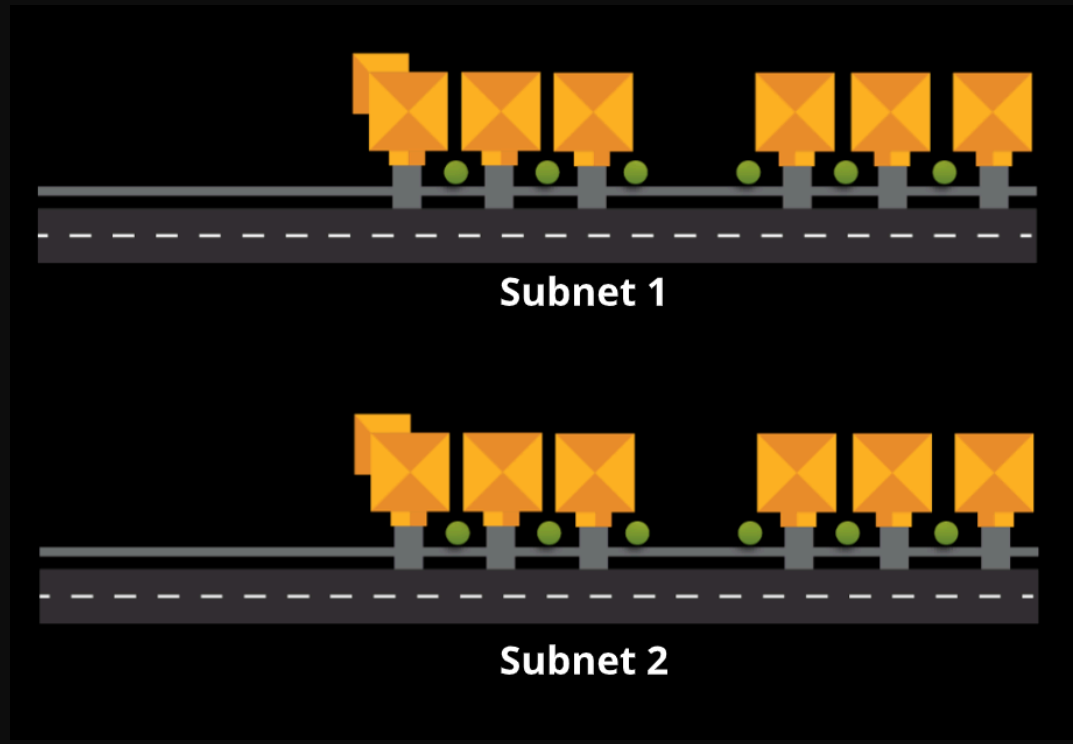
- Subnets
- Gateways (Internet, NAT, Virtual)
- VPC Security (NACLs, Security Groups, Flow Logs)

VPC Subnets

Subnets are subsections of a network (“subnetwork”)

After creating a VPC, you structure that VPC with subnets:

- Public subnets (accessible from the internet)
- Private subnets
- Subnets can go across Availability Zones in the same region
    - Increases High Availability
    - Creates Fault Tolerance



What makes Subnets public?

Internet Gateways (IGW):

IGWs are a combination of hardware and software that provides your private networks with a route to the open internet.

A subnet with a route (through a *route table*) to an Internet Gateway becomes a public subnet.

VPC Subnets

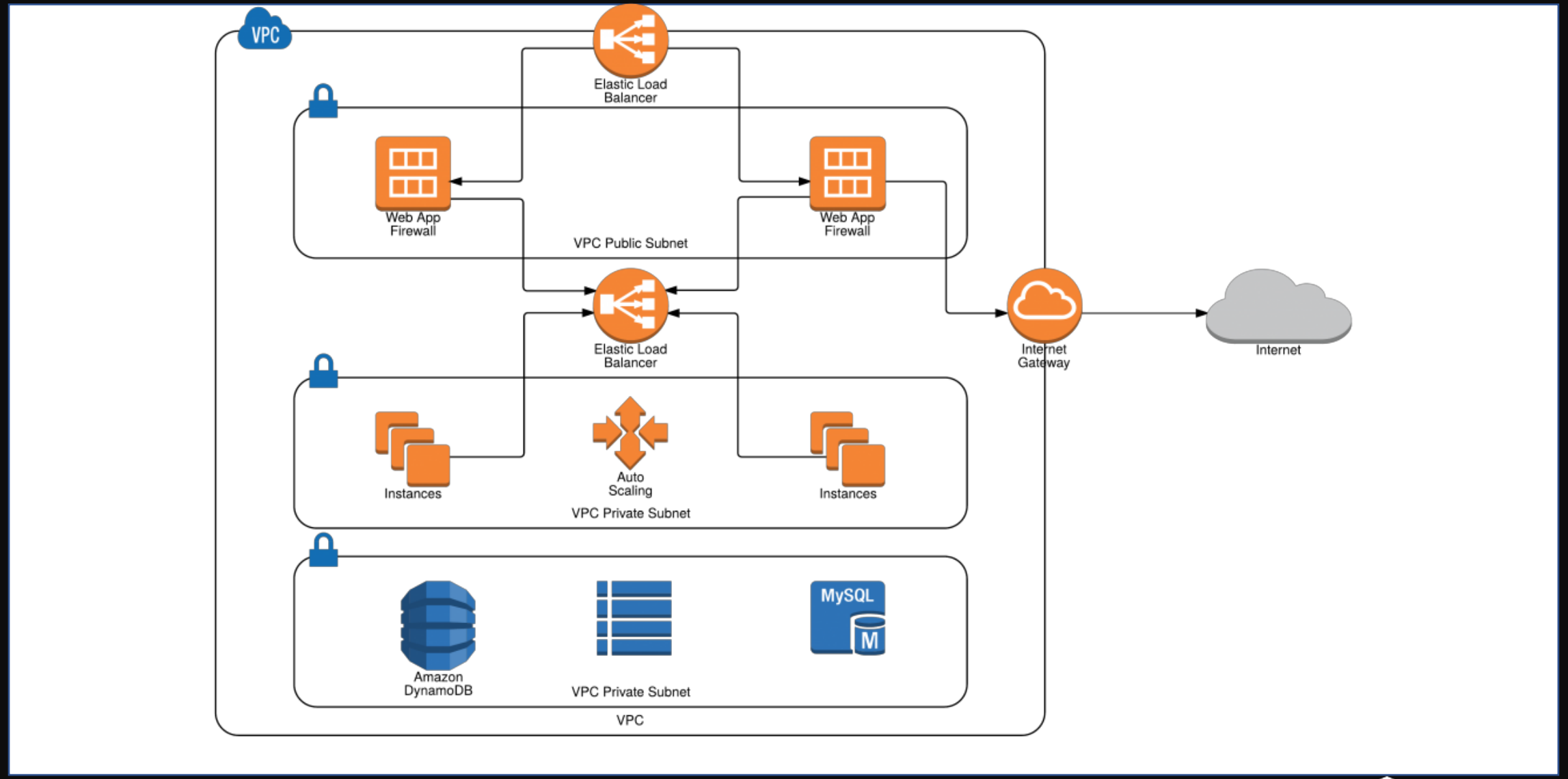
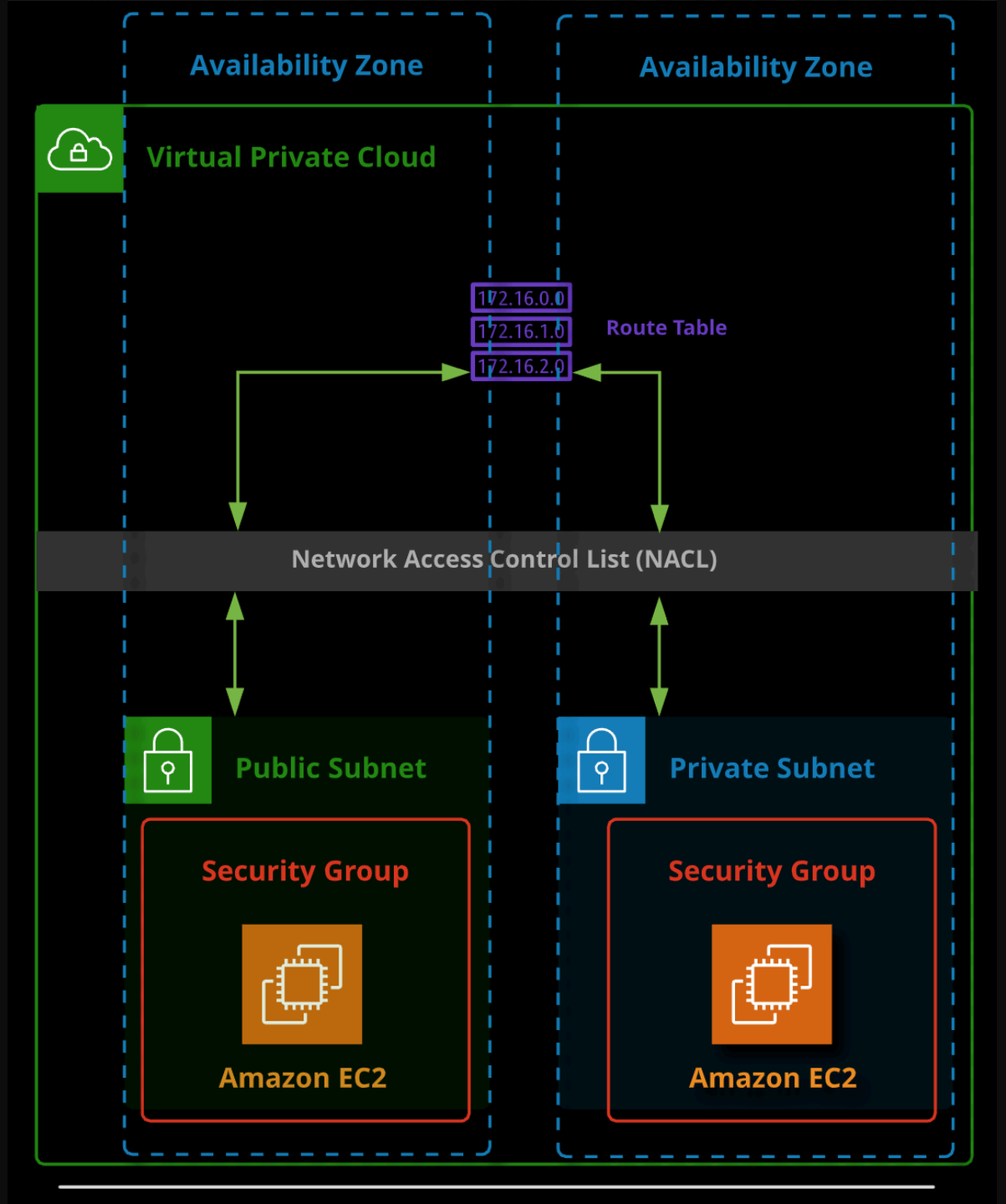


Photo credit: https://aws.amazon.com/

VPC Subnets



Virtual Private Gateways & Customer Gateways

Internet Gateways are different from Virtual Private Gateways, Customer Gateways, and NAT Gateways

Virtual Private Gateways:

- Used to create a connection between an on-premises network and your VPC
- Combined with a Customer Gateway, creates a Site-to-Site VPN connection
- Can be used with AWS Direct Connect (bypasses ISPs)

Virtual Private Gateways & Customer Gateways

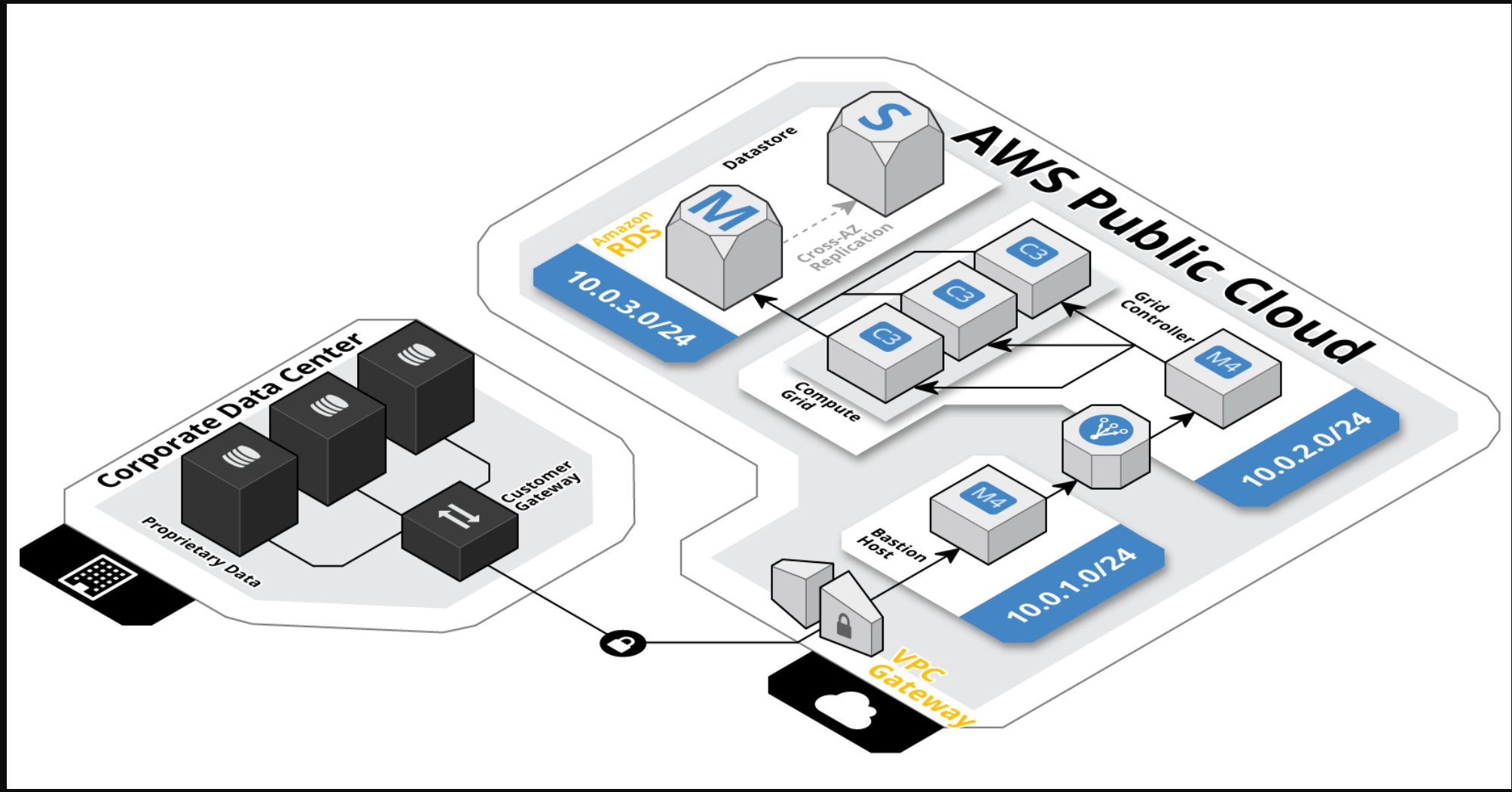


Image credit: https://cloudcraft.co/

NAT Gateways

NAT Gateways make it possible for instances in private subnets to reach out to the open internet (but prevent the open internet from making connections with those instances)

Use cases:

- Install/Update/Upgrade software
- Enables private resources to access other AWS resources outside of your VPC (could be done with VPC endpoints too)

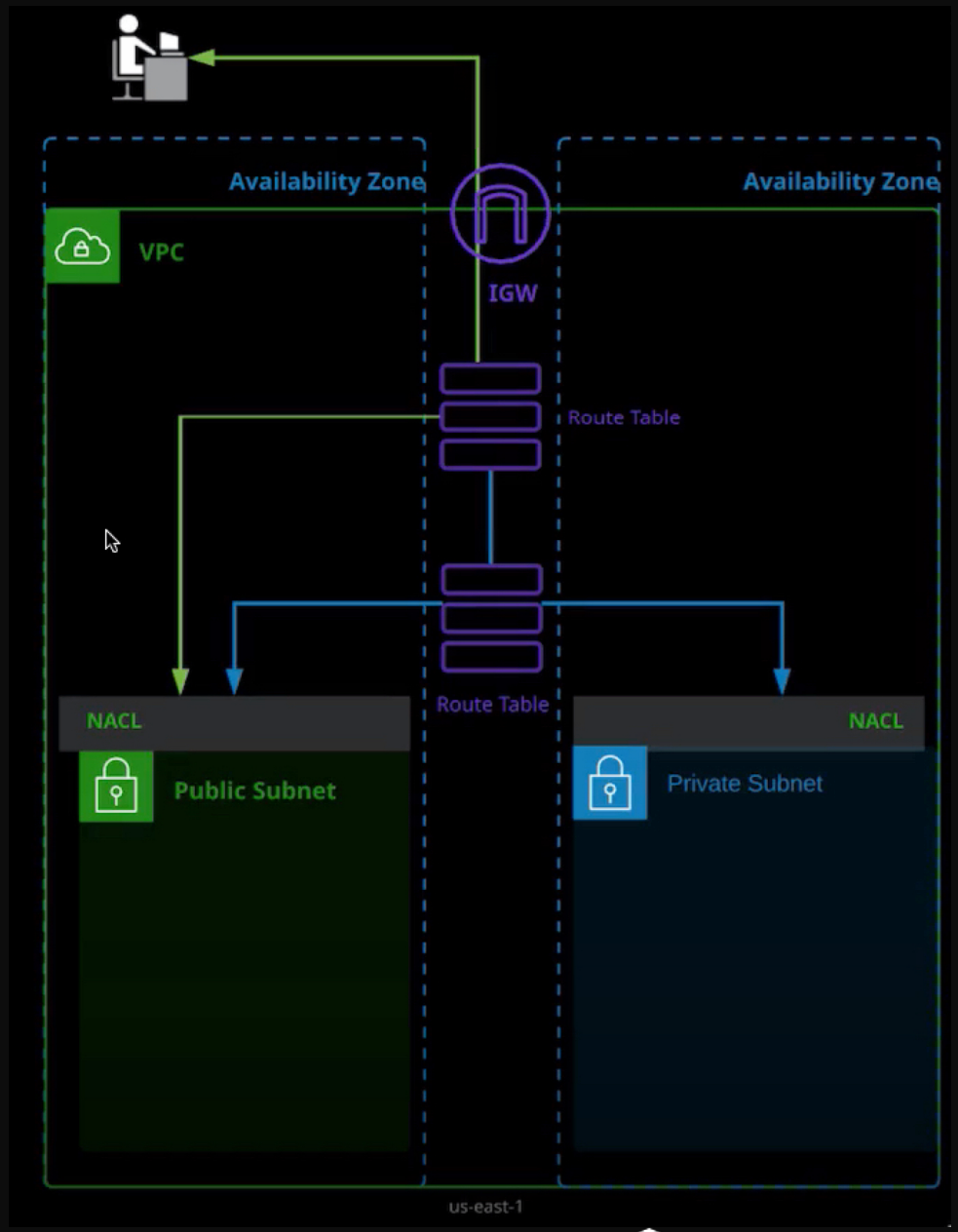
VPC Security

These act as firewalls and a security layer, giving you complete control over what traffic is allowed in and out of your VPC and within your VPC.

- Network Access Control Lists (NACLs)
- Security Groups (SGs)

This allows you to capture information about IP traffic flowing between your network interfaces

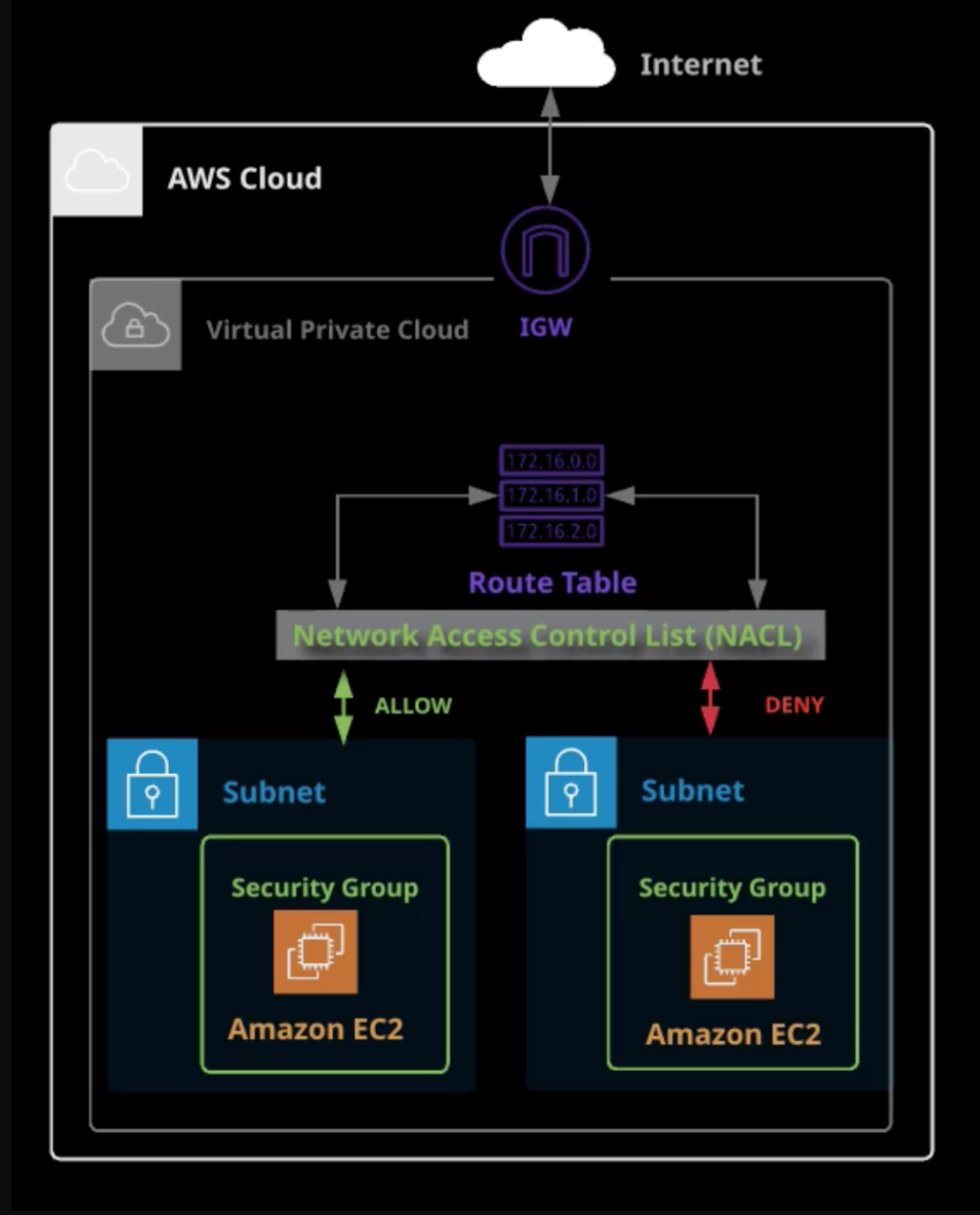
- Flow Logs (can publish to CloudWatch and S3)



VPC Security - NACLs

NACLs details:

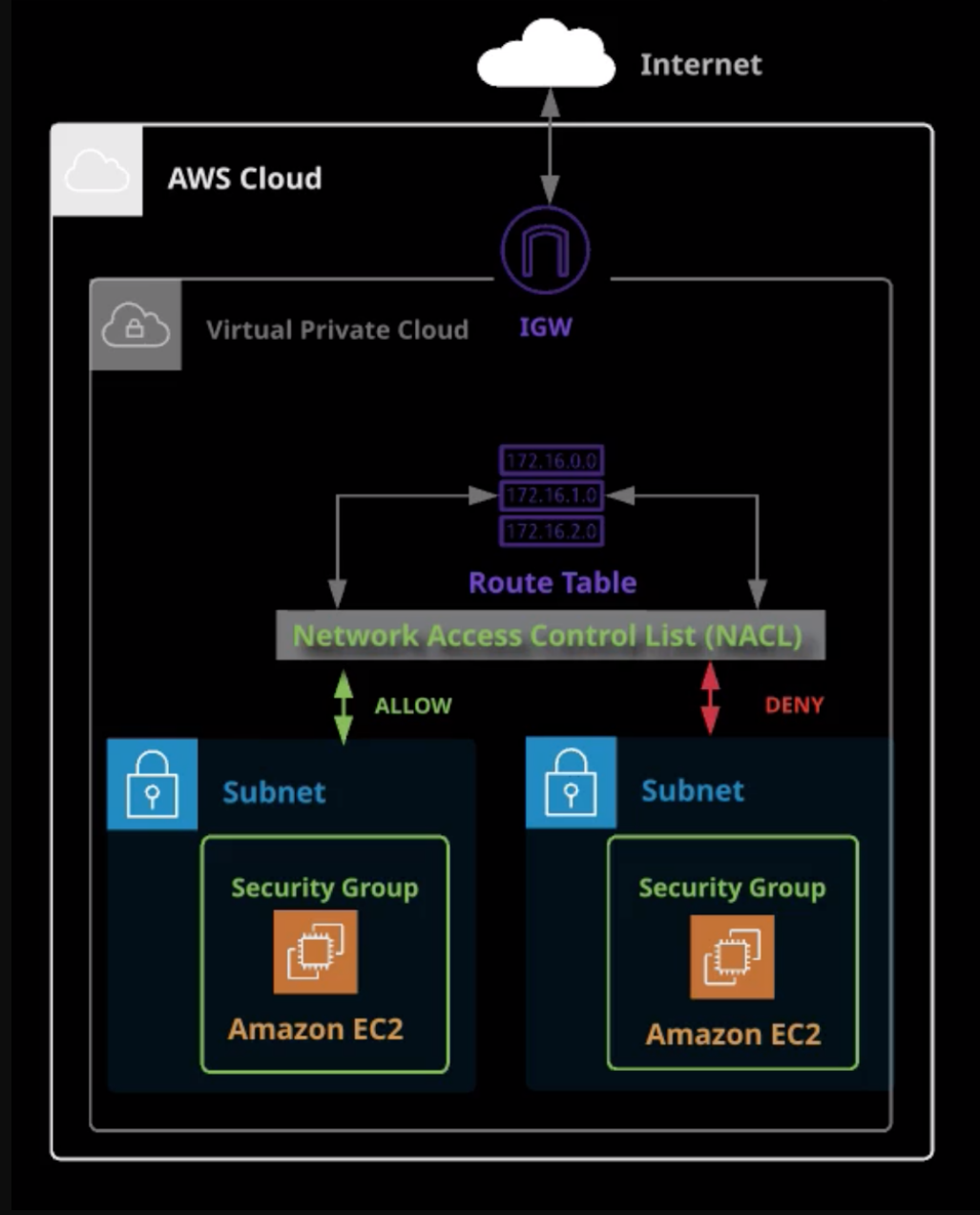
- At the subnet level
- Has inbound and outbound rules
- Stateless: traffic allowed one way has to also be allowed the other way



VPC Security – SGs

SGs details:

- At the instance level (gets evaluated after NACL)
- Everything is denied by default, you can only specify *allow* rules
- Stateful: traffic allowed one way is also allowed the other way



VPC Security – NACL vs SG

Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, an additional layer of defense if the security group rules are too permissive)

Image credit: https://aws.amazon.com

VPC Recap

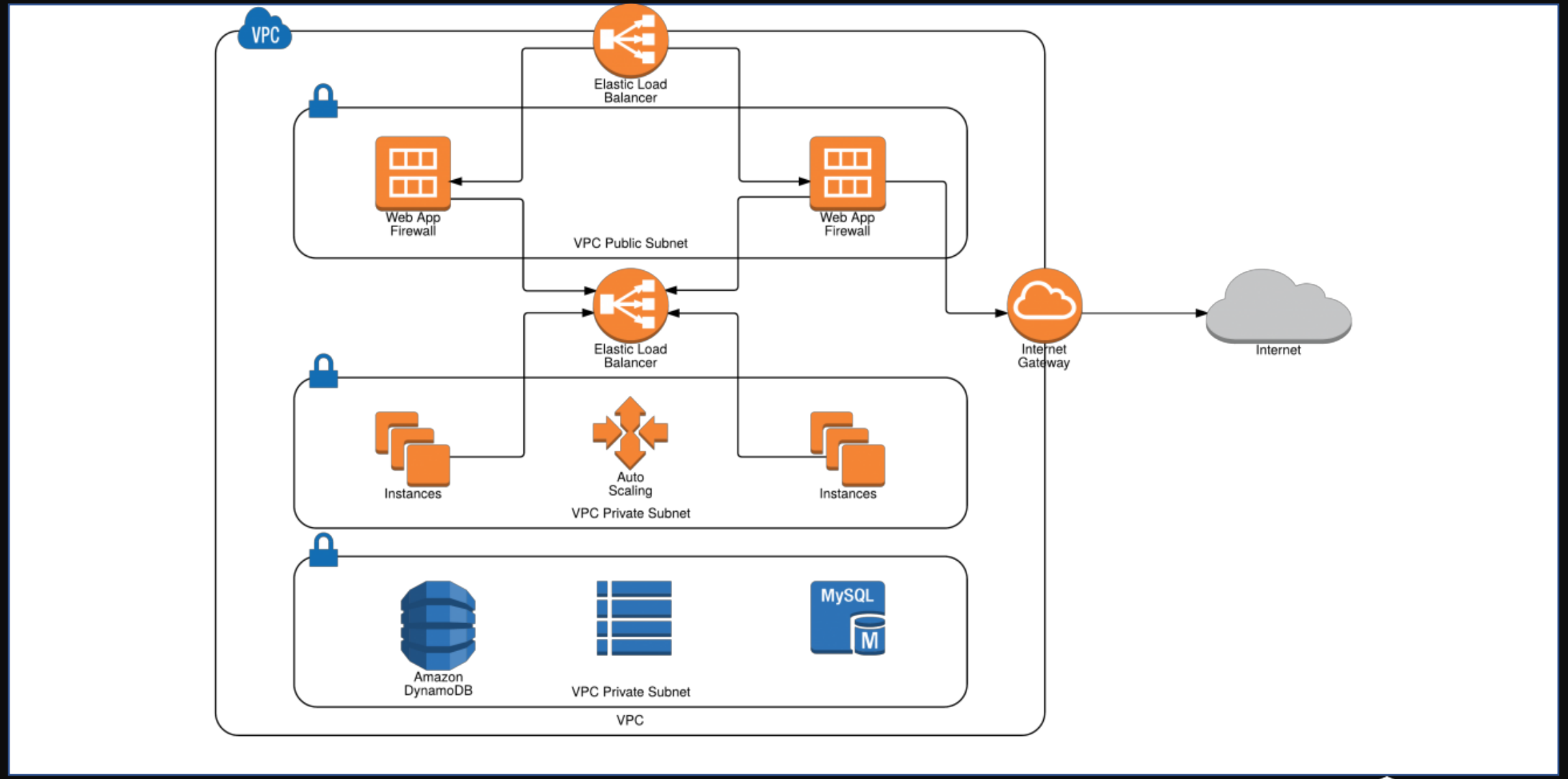


Photo credit: https://aws.amazon.com/

Pop Quiz

You've configured a VPC with public and private subnets, but your engineers are complaining that certain software packages are outdated and they're unable to connect to the internet in order to download updates. Which of these could be causing this issue? (Select 2)

A) Your private subnets aren't routing traffic through an Internet Gateway

B) You added deny rules in the Security Group blocking downloads

C) You added deny rules in the NACL blocking downloads

D) Your private subnets aren't routing traffic through a NAT Gateway

Pop Quiz

You've configured a VPC with public and private subnets, but your engineers are complaining that certain software packages are outdated and they're unable to connect to the internet in order to download updates. Which of these could be causing this issue? (Select 2)

A) Your private subnets aren't routing traffic through an Internet Gateway

B) You added deny rules in the Security Group blocking downloads

C) You added deny rules in the NACL blocking downloads

D) Your private subnets aren't routing traffic through a NAT Gateway

Pop Quiz

You have on-premises resources that need to communicate with your AWS VPC resources, and so you need to create a connection. Which of the following can help you accomplish this? (Select 2)

A) VPC Endpoint

B) Gateway endpoint

C) Virtual Private Gateway

D) NAT Gateway

E) AWS Direct Connect

Pop Quiz

You have on-premises resources that need to communicate with your AWS VPC resources, and so you need to create a connection. Which of the following can help you accomplish this? (Select 2)

A) VPC Endpoint

B) Gateway endpoint

C) Virtual Private Gateway

D) NAT Gateway

E) AWS Direct Connect

Homework

Review key terms & additional information

- ✓ **Download presentation slides and review**
- ✓ **Download sample AWS exam questions and answer:**
  - ✓ **#1, #3, #4**
- ✓ **VPC Hands-On Lab:** https://linuxacademy.com/hands-on-lab/934b78e6-5327-4ed3-a369-1b60b382722f/
- ✓ **EC2 Hands-On Lab:** https://linuxacademy.com/hands-on-lab/e898d77e-2a8d-4e79-b3d3-fd9b27f14649/

Read up on the following:

- ✓ **S3 -** https://aws.amazon.com/s3/
- ✓ **AWS Databases -** https://aws.amazon.com/products/databases/
- ✓ **AWS ElastiCache -** https://aws.amazon.com/elasticache/

Additional Info

Next meeting – August 28th:

S3 and Databases

Links / Resources / Info
https://github.com/Ellopunk/Cloud_Practitioner

Linux Academy Community
https://linuxacademy.com/join/community

Linux Academy Slack Channel
https://linuxacademy-community-slack.herokuapp.com/

Thank you

If you found this helpful, please invite your colleagues!

Linux Academy