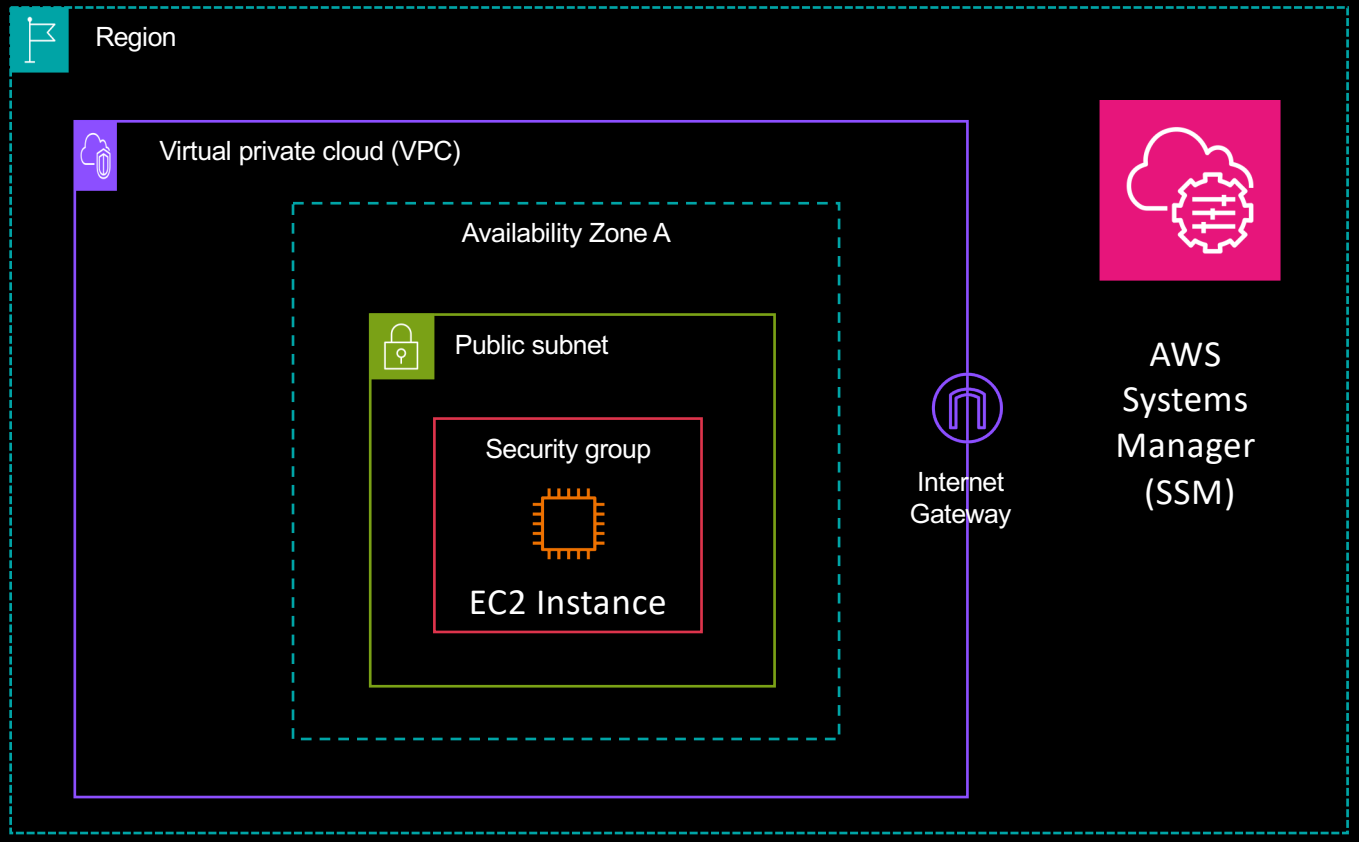
AWS Certified Cloud Practitioner

Module 03 - Networking with AWS

Virtual Private Cloud (VPC)

Instructor: Tim Platt, Cloud Solution Architect

What we've just accomplished in our AWS Account

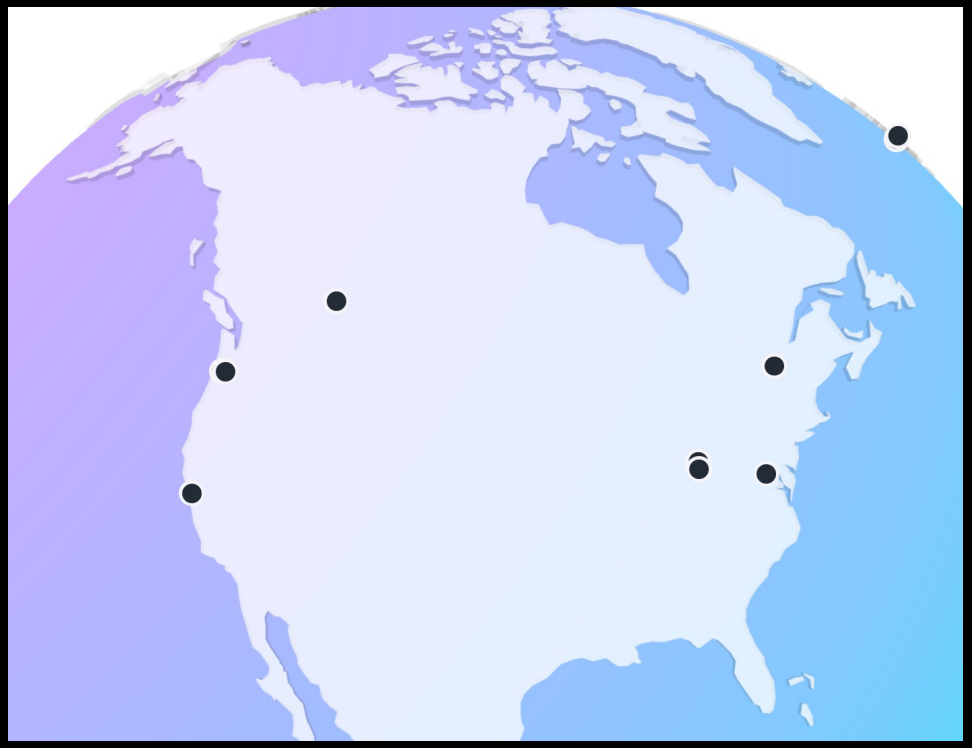


This is a simple setup that will work for our learning purposes.

But there are many more features of AWS VPC (Virtual networking) that need to be understood.

Let’s understand what a more complicated network setup might include

Regions and Availability Zones



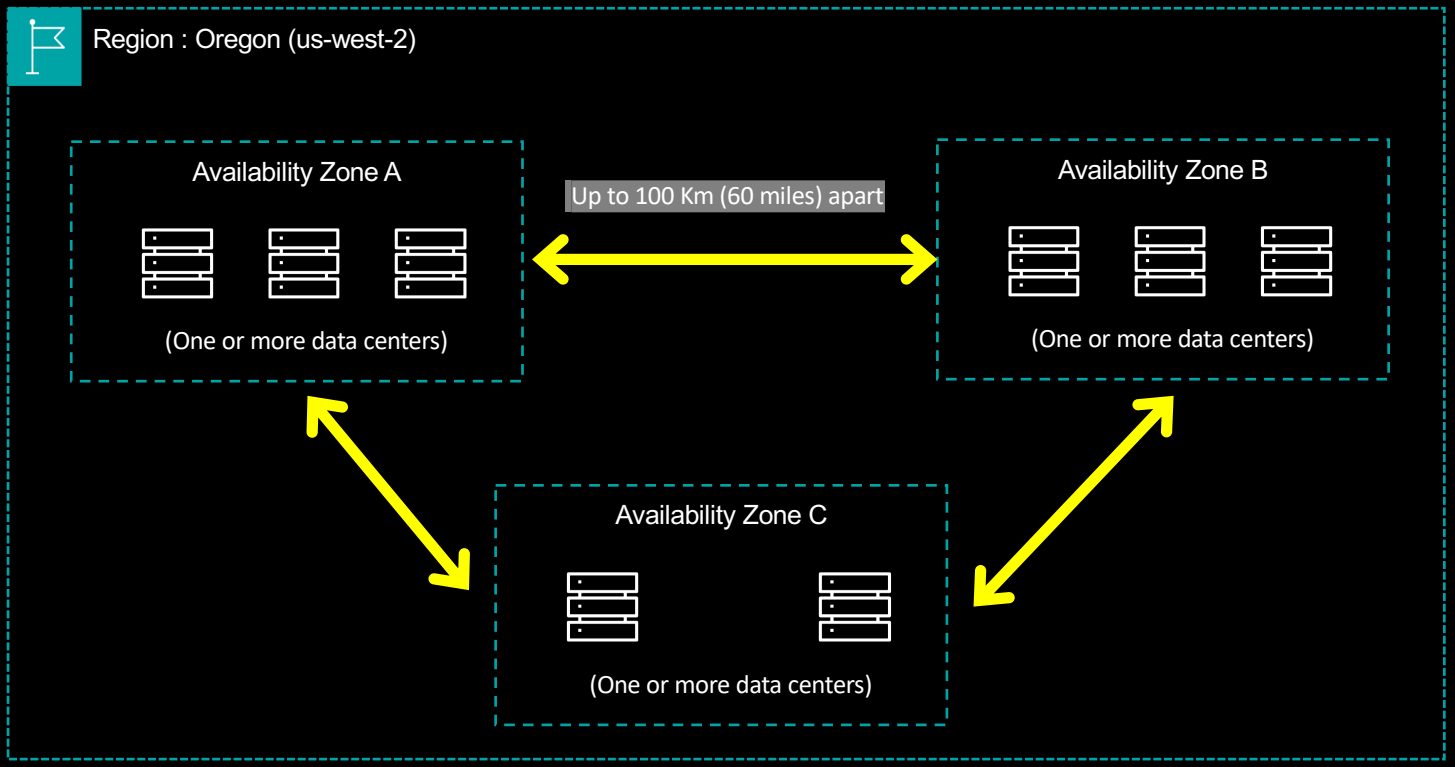
We can place our AWS Resources in REGIONS all around the globe

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Why?

- Get CLOSER to the customer
- Resilience against disasters
- Compliance needs – some data must reside within the US
- Cost differences in different regions (Example: Tokyo vs Ohio)

Regions are SUB-DIVIDED into Availability Zones (AZ)



Why? We can minimize Single Points of Failure for High Availability (HA)

Virtual Private Cloud (VPC)

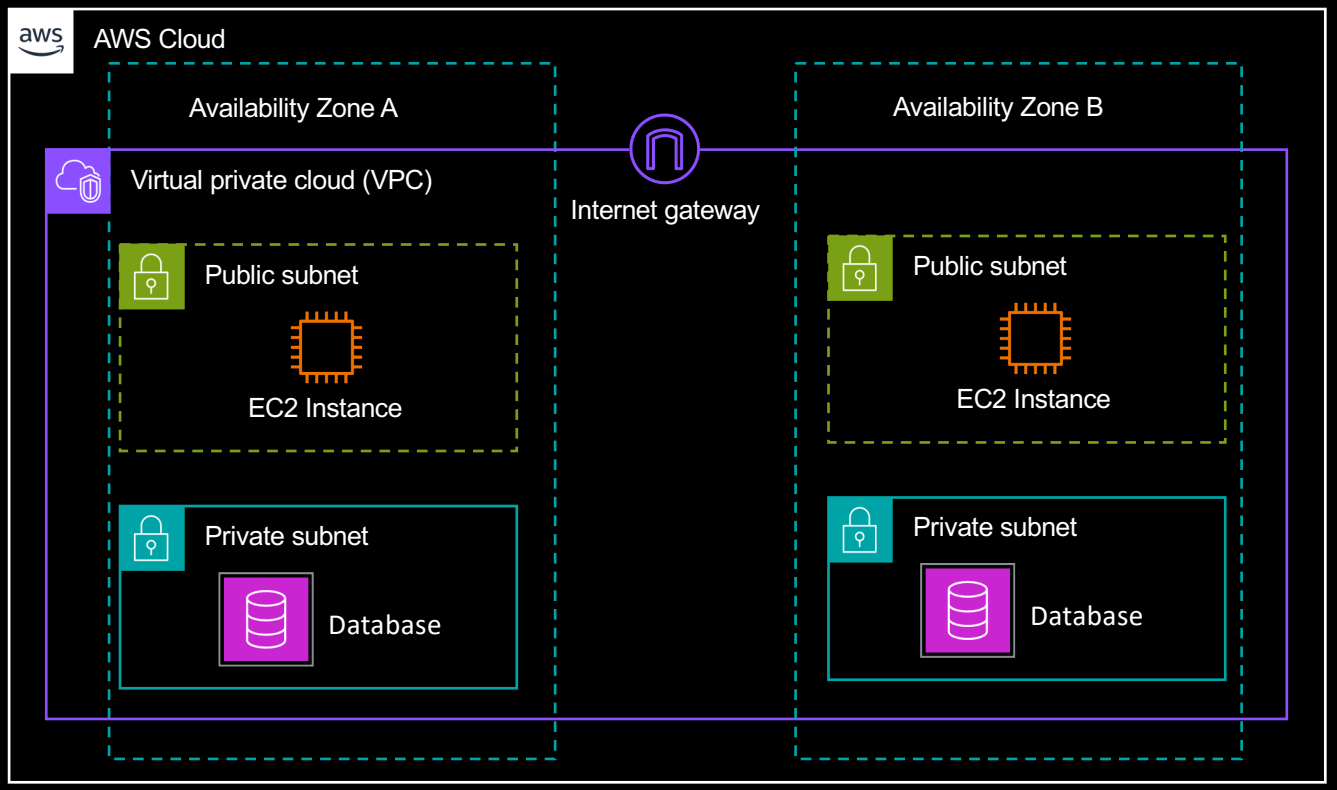
Network

A virtual network for your virtual servers in the cloud

Key Points

- A logically isolated section of the cloud where you can launch AWS resources
- Proper network design dictates having a layered or tiered network with “Defense in Depth” applying network level access controls
- Key sub-components:
  - Subnets (Public & Private)
  - Internet Gateway (IGW)
  - Route Table entries for the virtual router
  - Firewall rules – Network Access Control Lists (ACLs) and Security Groups
  - NAT Gateway (Network Address Translation)
- SUPERPOWER: Virtual equivalents of all the components needed to build a computer network: subnets, route tables, firewall rules, Domain Name System (DNS) name resolution, and more

A Best Practices based VPC



Key Points

- **Public Subnets** for Internet facing resources
- **Internet Gateway** facilitates Internet access (inbound and outbound)
- **Private Subnets** for things that should NEVER be accessible from the Internet
- More than one AZ (Notice the redundancy in the web servers and database nodes.

We are minimizing Single Points of Failure

Route Tables

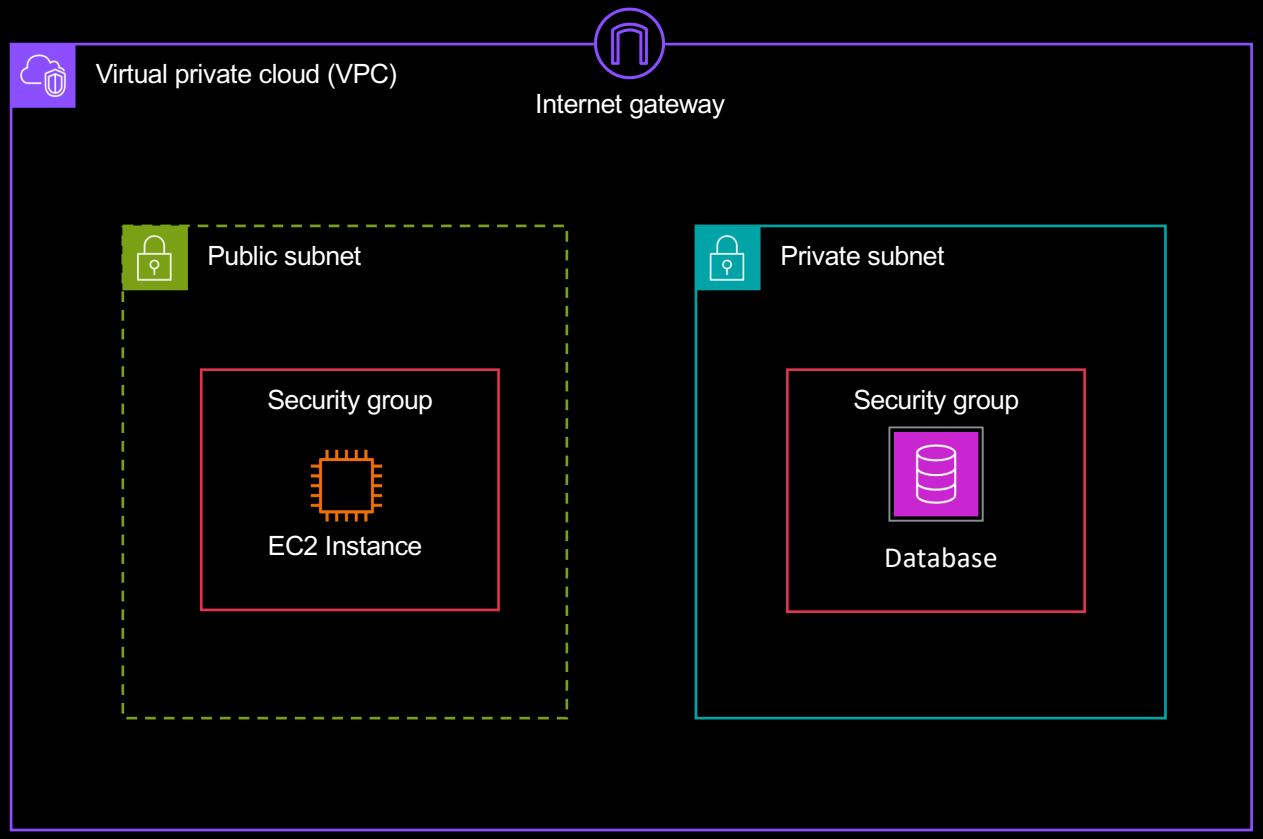
Destination	Target
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

Your Virtual Network (VPC) has a Virtual Router – you can't see it or access it, but you control the traffic routing rules.

A **route table** serves as the traffic controller for your virtual private cloud (VPC).

Each route table contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed.

What about Network Security? We have FIREWALLS

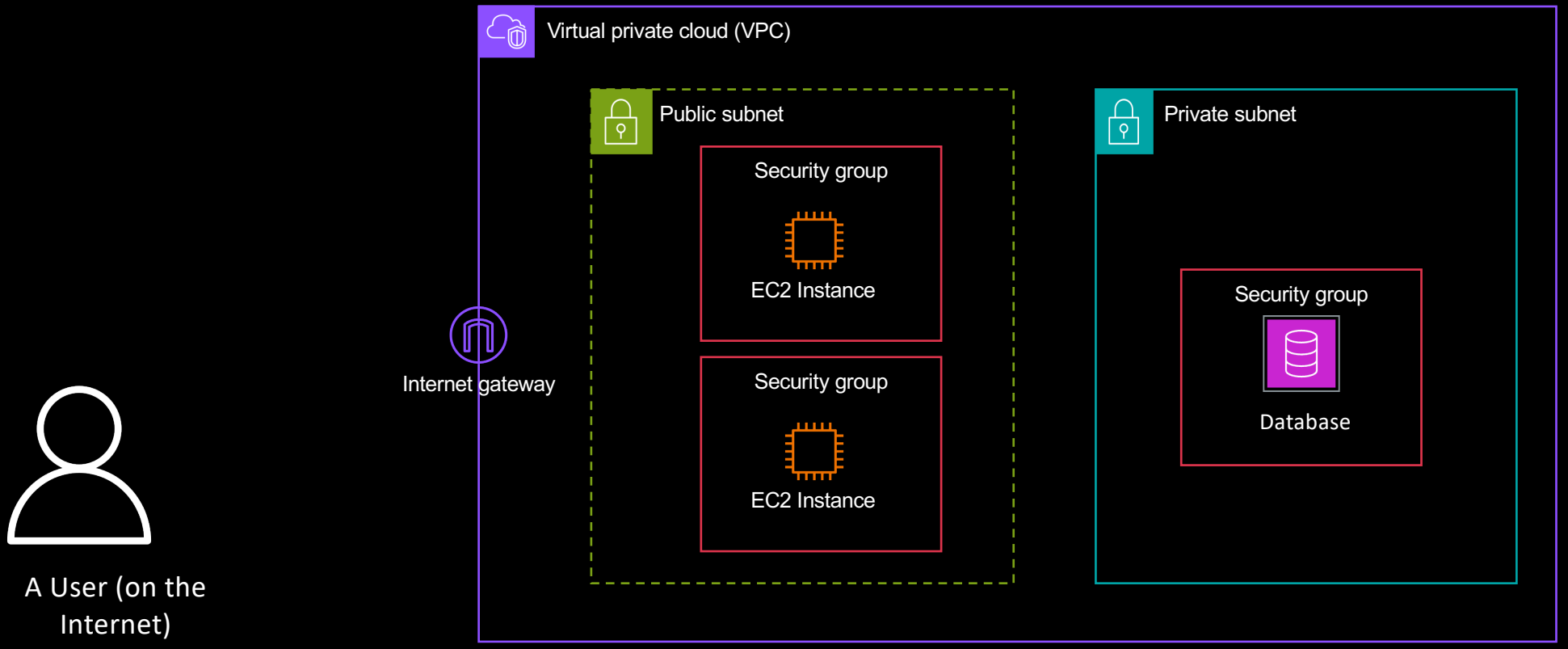


- Subnets have **Network Access Control Lists (ACLs)** that protect the entire subnet
- Within the subnet you have **Security Groups** that let you protect each instance with very specific rules

Why?

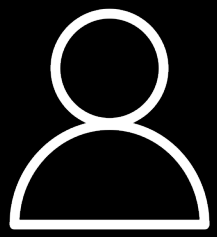
- We need to be able to precisely control inbound and outbound traffic
- Not just to the Internet, also within our own VPC
- That's "Defense in Depth"

Firewall Example

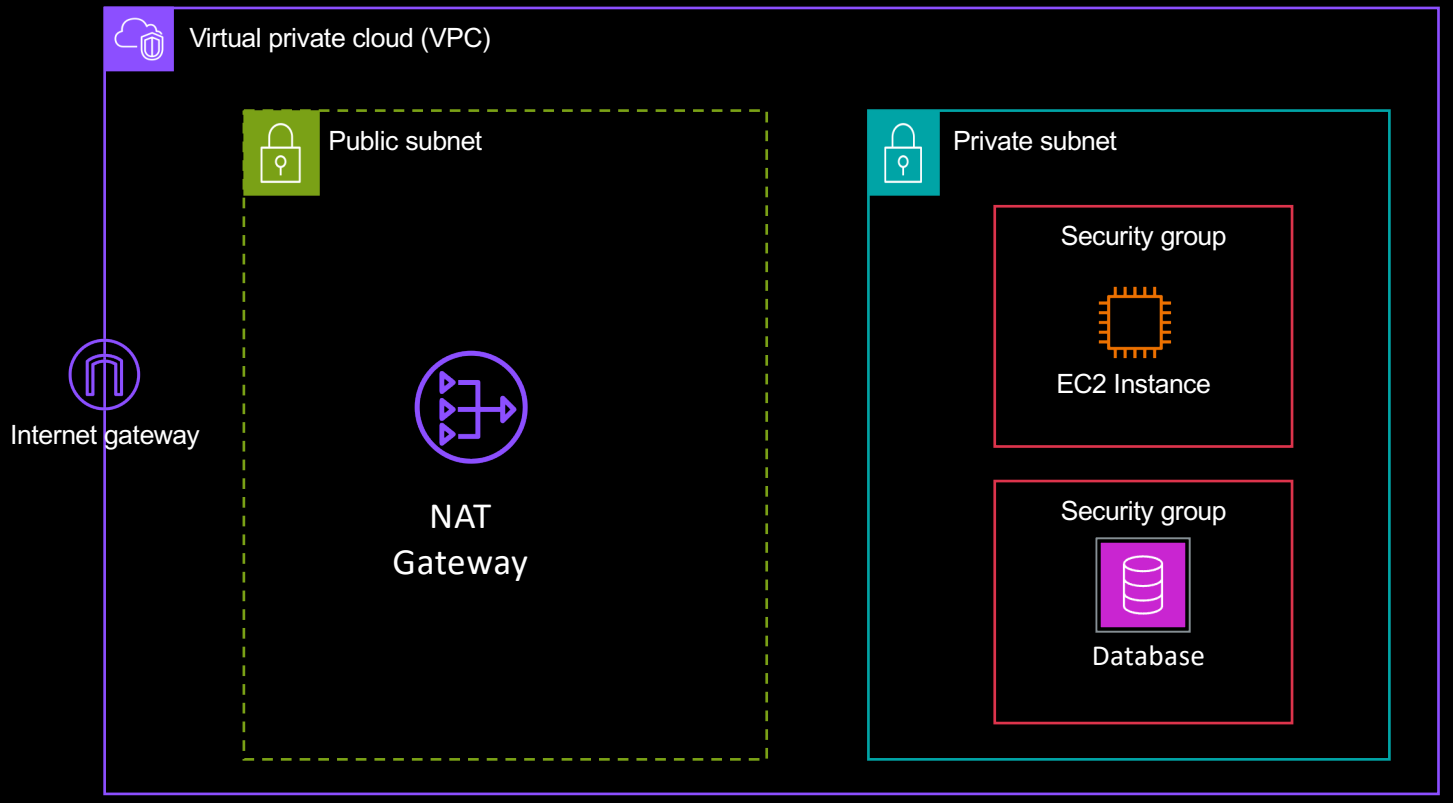


Network Address Translation (NAT) Gateway

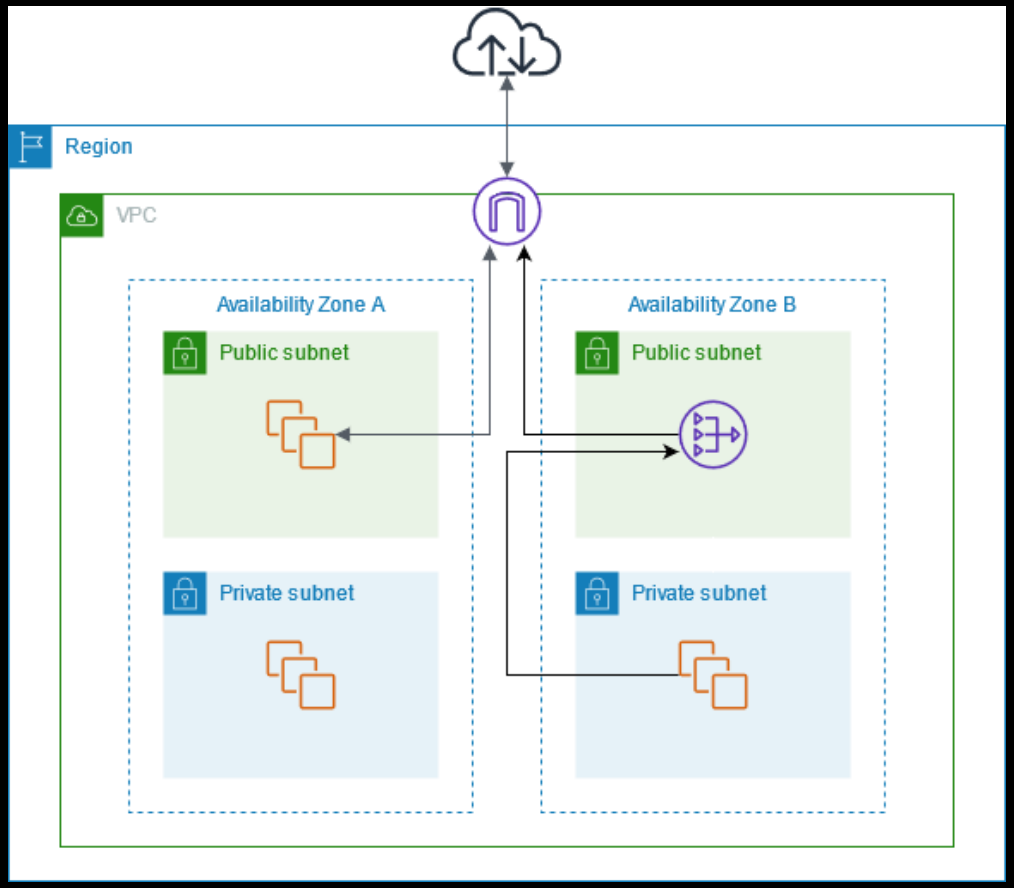
NAT gateway allows SAFE outbound access to the Internet for servers in the Private subnet



A User (on the Internet)



NAT gateway is a Network Address Translation (NAT) service



You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services can't initiate a connection with those instances.

In this scenario, the servers in the private subnet can initiate outbound connections to the Internet (to communicate with other clouds, or to download software, or to access web services)

NOTE: The arrows represent connections being opened. Understand NAT Gateway will NOT allow the Internet to initiate an inbound connection.

Route 53 – DNS (Domain Name System)

DNS

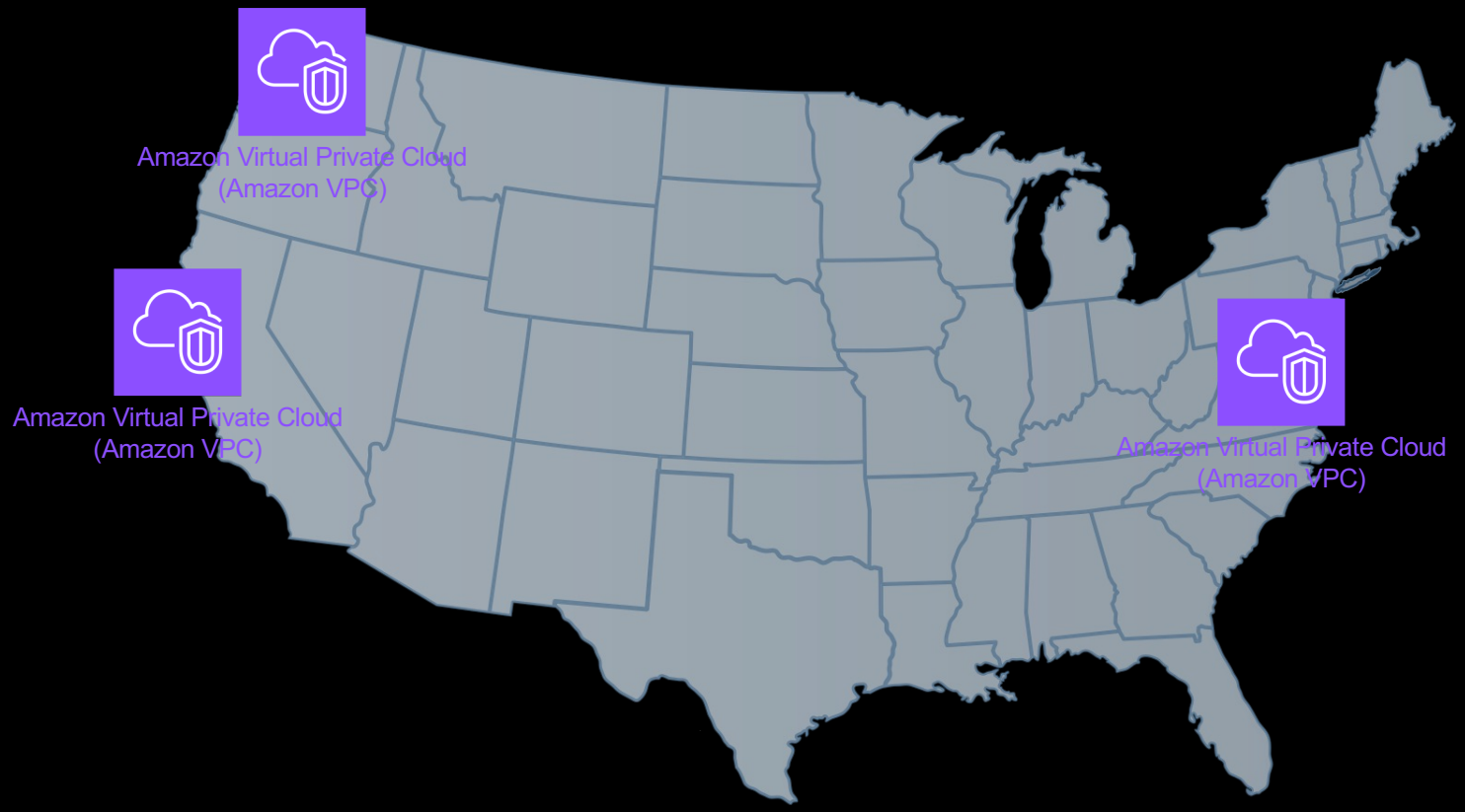
Manage custom DNS Names with powerful features

Key Points

- The DNS (Domain Name System) is what resolves friendly domain names (like www.amazon.com or www.awstrainer.com) to IP addresses
- Route 53 can be used to Register Domains but also to define the sets of Name records
- Hosted Zone - a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains.
  - Public Hosted Zone – Names are resolvable over the Internet
  - Private Hosted Zone – Names are resolvable only in your VPCs
- SUPERPOWER: Route 53 has lots of high performance features that simpler DNS services don't provide – like health checks, failover routing, and much more

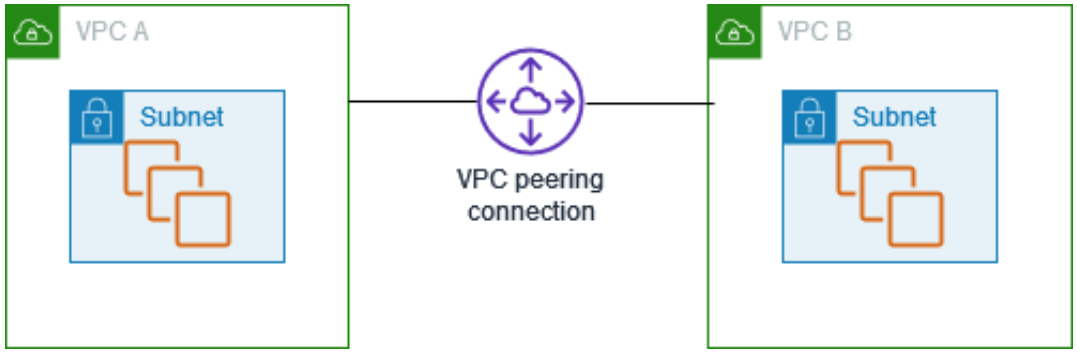
TIP: Route "53" gets its name from the network port used for DNS traffic – which is port 53.

How do we connect VPCs together?



NOTE: a VPC lives entirely within ONE region. If you use multiple regions, you will have multiple VPCs

VPC Peering – Simple connectivity between VPCs

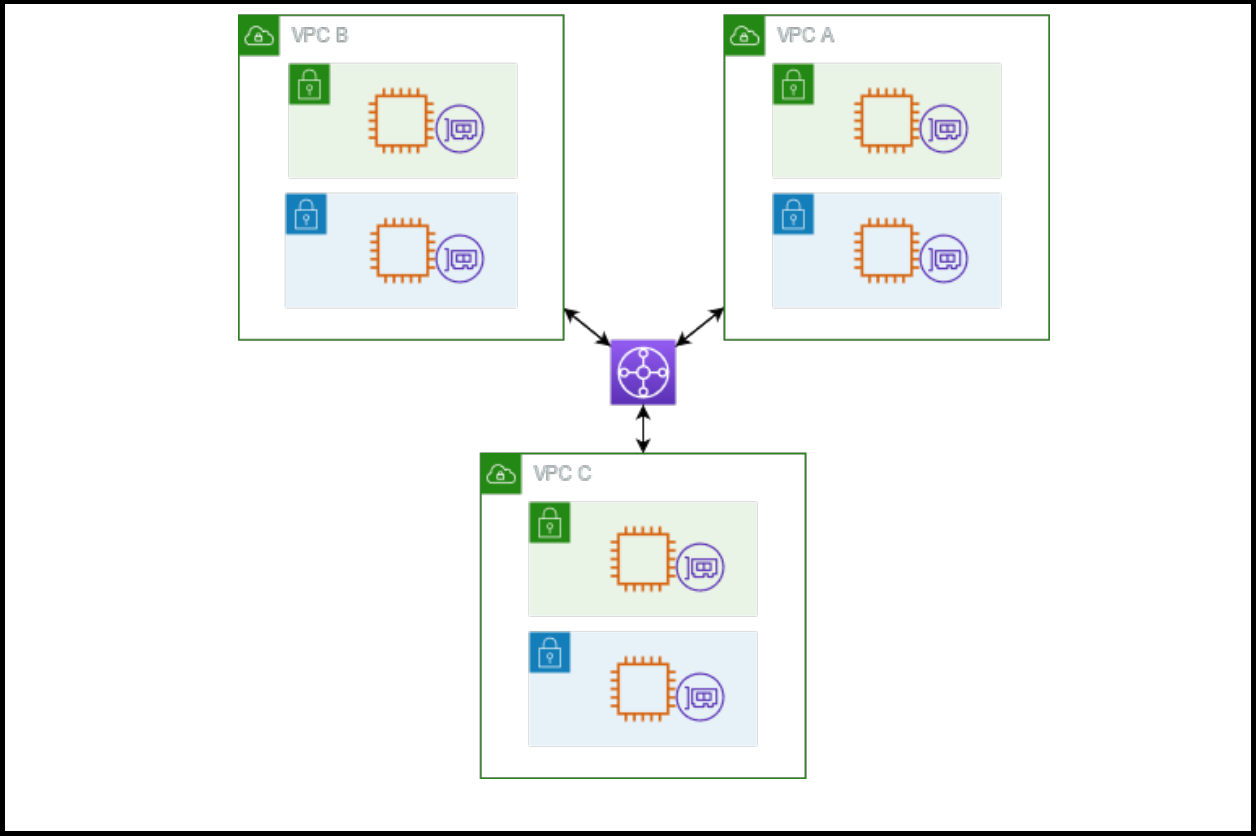


A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses.

The VPCs can be in same region, different regions, same account, or difference accounts.

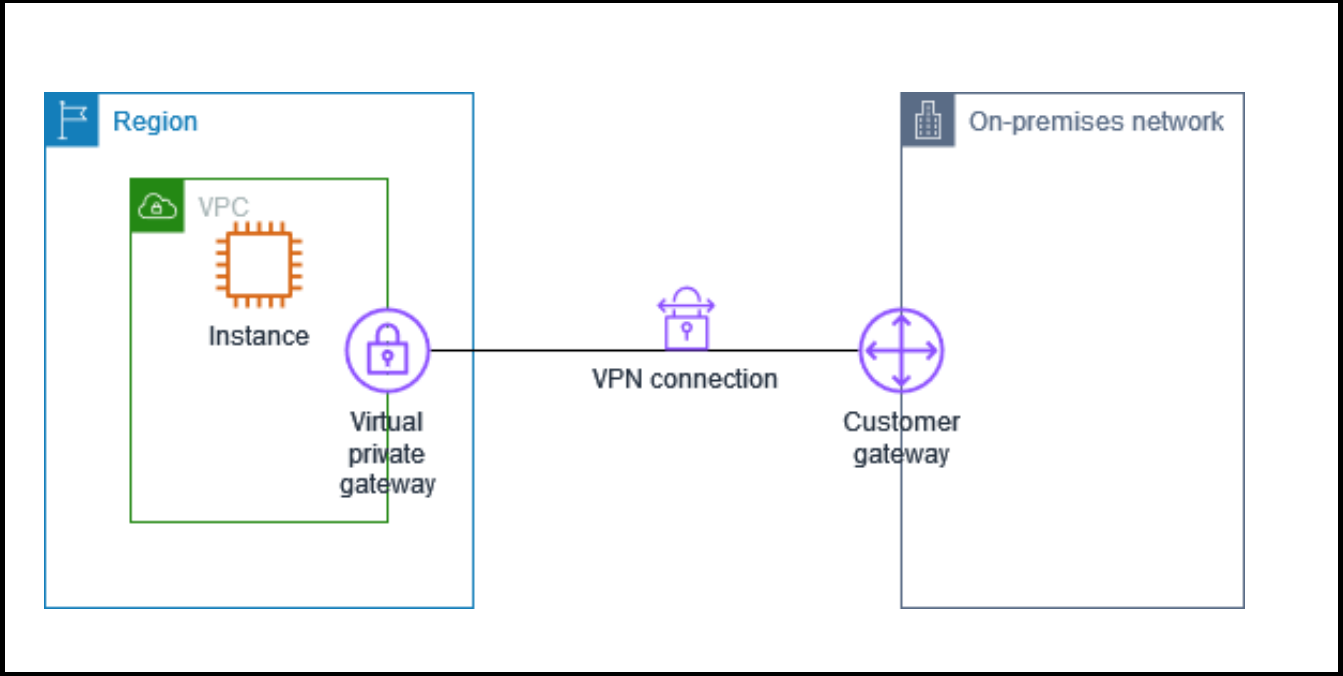
NOTE: VPC Peering is a non-transitive 1:1 connection between only two VPCs.

Transit Gateway – For large scale inter-connectivity



AWS Transit Gateway is a network transit hub used to interconnect multiple virtual private clouds (VPCs) and on-premises networks.

Hybrid connectivity - Site-to-Site Virtual Private Network (VPN)



NOTE: Virtual Private Gateway supports IPSec protocol only!

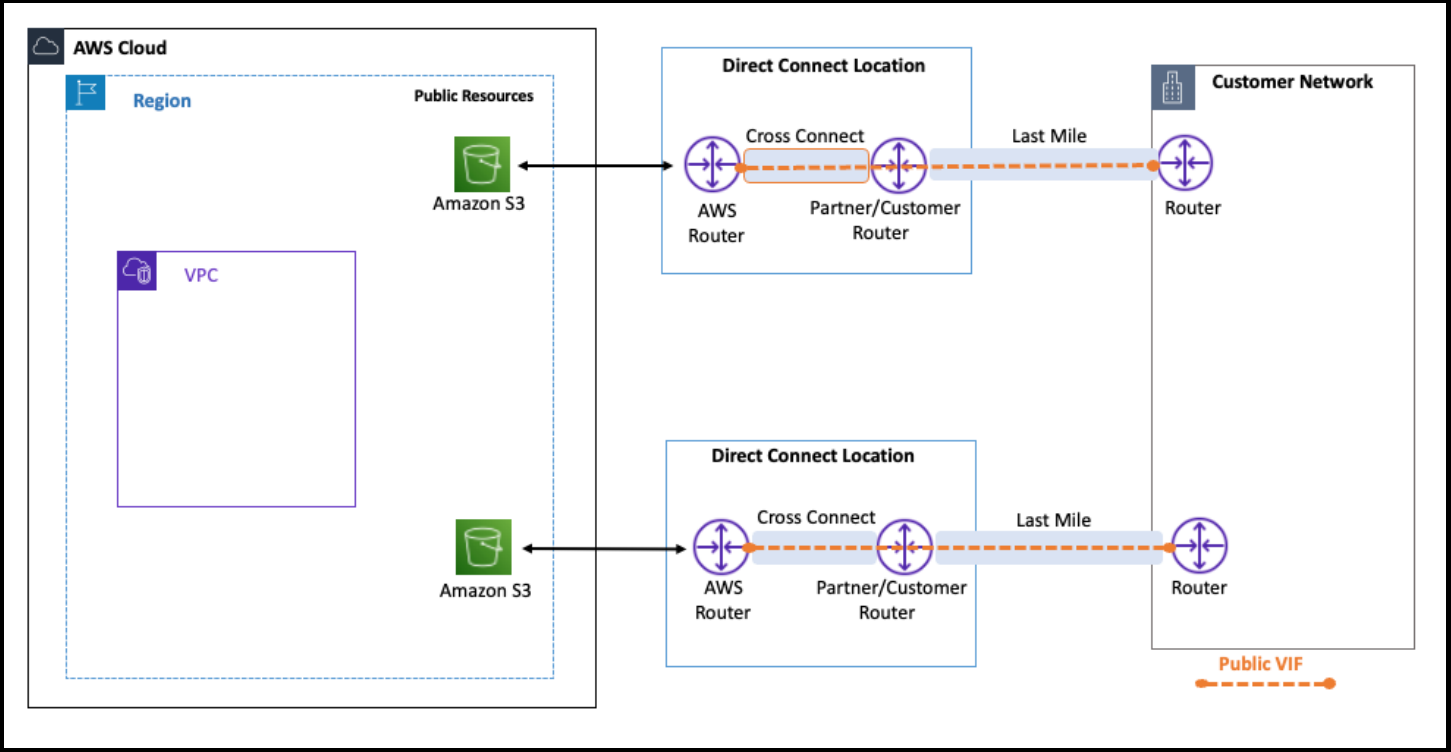
A Site-to-Site VPN is a way to connect two different locations securely over the Internet.

There are two devices (routers or equivalent) that maintain an encrypted tunnel so that traffic is secure.

The router or firewall on the customer side is known as a Customer Gateway

The virtual device on the AWS side is a Virtual Private Gateway (VGW)

Need more speed? Consider AWS Direct Connect instead



Direct Connect is a private fiber-optic connection that does NOT go over the Internet.

Up to 400 Gbps

(Compare to only 1.25 Gbps with site-to-site VPN)

Links (1 of 2)

- Regions & AZs: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
- CIDR.XYZ (figure out IP Address ranges): https://cidr.xyz/
- What is a VPC? https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- Security Groups: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html
- Network Access Control Lists: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
- Configure Route Tables: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

Links (2 of 2)

- NAT Gateways: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
- VPC Peering: https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html
- AWS Transit Gateway: https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html
- AWS Site-to-Site VPN: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html
- AWS Direct Connect: https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html