Cloud Applications Architecture

Course 3 - Networking in the Cloud

Networking Concepts

IP Addresses

Public, private

Static, dynamic

IPv4, IPv6,

IP Addresses

IPv4

~4 billion addresses.

We are close to running out of (think of all the IoT devices).

Consists of 4 octets.

e.g. **10.120.70.1**

IPv6

many orders of magnitude more addresses

2001:0db8:85a3:0000:0000:8a2e:0370:7334

A device may have both.

IPv6 is usually optional in cloud.

IP Addresses

Public

Unique across the internet.

Not in the private/reserved ranges

Private

In one of the ranges:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

A device may have both.

Public is usually optional in cloud

IP Addresses

Static

The device is guaranteed to have the same IP address.

Great for servers.

Dynamic

The device is **not** guaranteed (and very **unlikely**) to have the same IP address.

Used in most cases.

Assigned by DHCP (dynamic host configuration protocol)

Routing

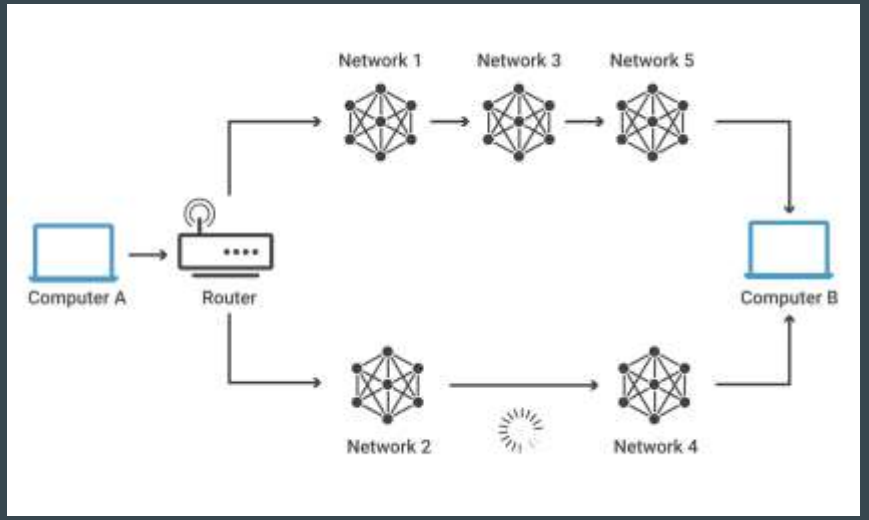
Selecting the path to reach the destination.

Protocols used by the internet:

- **IP**
- **BGP**
- **OSPF**
- **RIP**

Multiple delivery schemes:

- Unicast
- Broadcast
- Multicast, anycast, geocast



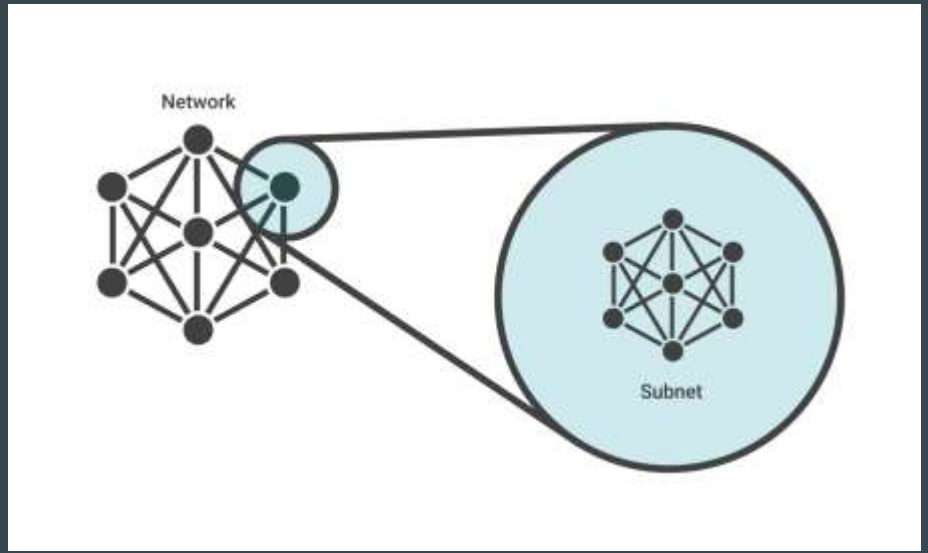
Subnets

A part (subnetwork) of a network.

Traffic can stay within one subnet

- better performance
- less congestion)

First part of a given IP address indicates the (sub)network. The other part indicates the device.



CIDR

Classless **I**nter-**D**omain **R**outing

Replaced classful networks in 1993 (classes A, B, C, D, E)

Example: 192.168.0.1**/24**

/24 tells us that the the first 24 bits indicate the network. So to find the network address, we apply the **network mask** 255.255.255.0 (bitwise AND).

The last 8 bits indicate the device within the network. (0 and 255 are reserved). This means that we can have 254 devices in this network.

CIDR - example

/27 -- 8 Subnets -- 30 Hosts/Subnet		
Network #	**IP Range**	**Broadcast**
.0	.1-.30	.31
.32	.33-.62	.63
.64	.65-.94	.95
.96	.97-.126	.127
.128	.129-.158	.159
.160	.161-.190	.191
.192	.193-.222	.223
.224	.225-.254	.255

	Addresses	**Hosts**	**Netmask**	**Amount of a Class C**
/30	4	2	255.255.255.252	1/64
/29	8	6	255.255.255.248	1/32
/28	16	14	255.255.255.240	1/16
/27	32	30	255.255.255.224	1/8
/26	64	62	255.255.255.192	1/4
/25	128	126	255.255.255.128	1/2
/24	256	254	255.255.255.0	1
/23	512	510	255.255.254.0	2
/22	1024	1022	255.255.252.0	4
/21	2048	2046	255.255.248.0	8
/20	4096	4094	255.255.240.0	16
/19	8192	8190	255.255.224.0	32
/18	16384	16382	255.255.192.0	64
/17	32768	32766	255.255.128.0	128
/16	65536	65534	255.255.0.0	256

NAT

Network **A**ddress **T**ranslation

Translate IP addresses

Used for:

- Overlapping networks (networks spanning the same private IPs)
- Accessing the public internet from devices without public IP addresses

Can also translate ports

Gateways

Allow reaching devices from different networks.

Networks usually have **default gateways** to which traffic is routed when the target is not found within the network.

VPN

Virtual **P**rivate **N**etwork

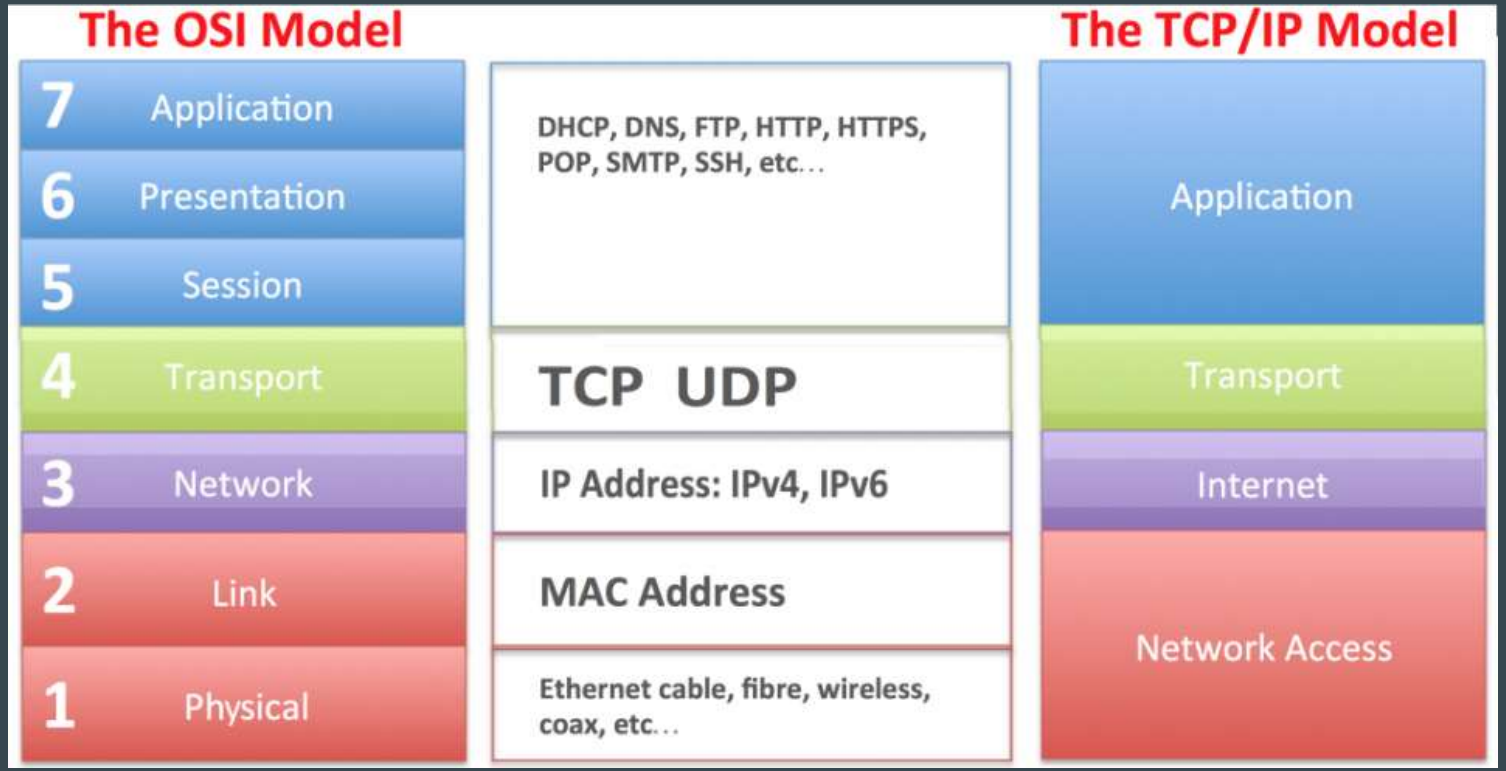
Connect securely to another network

Nowadays used to bypass censorship and watch movies from other regions

Initially designed for businesses

- Access the corporate network from outside (e.g. home, mobile)

Networking Models



OSI Model vs TCP/IP Model - Source

Cloud Networking

Context

Most relevant in the context of IaaS.

Constantly evolving.

- E.g. DigitalOcean released **VPCs** (virtual private cloud) in April 2020
- EC2 started without any custom networking support.

Highly dependant on the provider.

Common Terms

Virtual **P**rivate **C**loud (**VPC**)

- VPC on AWS, GCP, and DigitalOcean, vNet on Azure, etc.
- Logical (**isolated**) network slice where we can deploy resources.
- Works with **private IP addresses** given by a **CIDR**
- Can usually be split into **subnets**

Peering

- VPC peering usually
- Allows traffic between different networks
- It’s our responsibility to avoid/handle **IP overlaps**
- Can also be between on-premises and cloud

VPC Networking Components

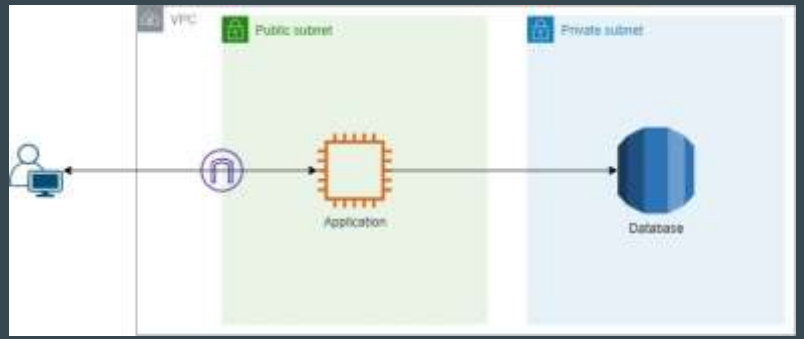
- Network interfaces
- Route tables
- Gateways: Internet, carrier, egress-only Internet
- NAT
- DNS

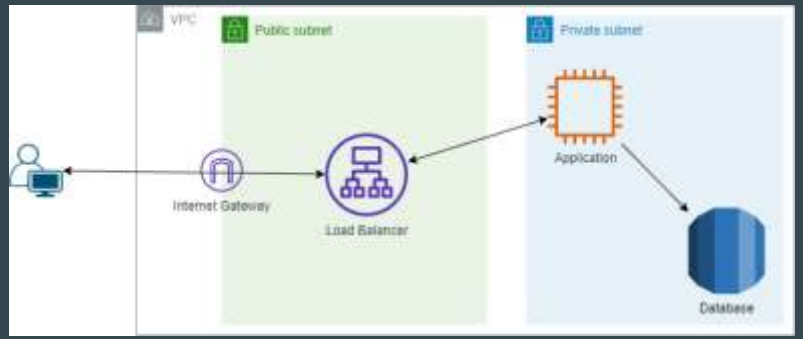
Secure by Design

Based on the least privilege principle and minimizing the attack surface.

Ideally, a service should be **accessible** (network-wise) only by the services that are intended to access it.

E.g. a dedicated database server should be accessible only by the application server/tier. Any other traffic shouldn't even be possible.





Common Vulnerabilities

Leaving the provider internal network to access managed services.

We cannot choose to deploy most managed services in a given network.

- They are reached via the public internet

Providers usually offer additional services/features designed to ensure private communication with the managed services.

Network Performance

Subnetting helps

Bigger VMs tend to have better (virtual) networking cards.

Some providers support clustering (running multiple VMs on the same rack)

Our designs should strive to leverage the provider infrastructure

- Packets should enter the provider network as soon as possible

Network Performance

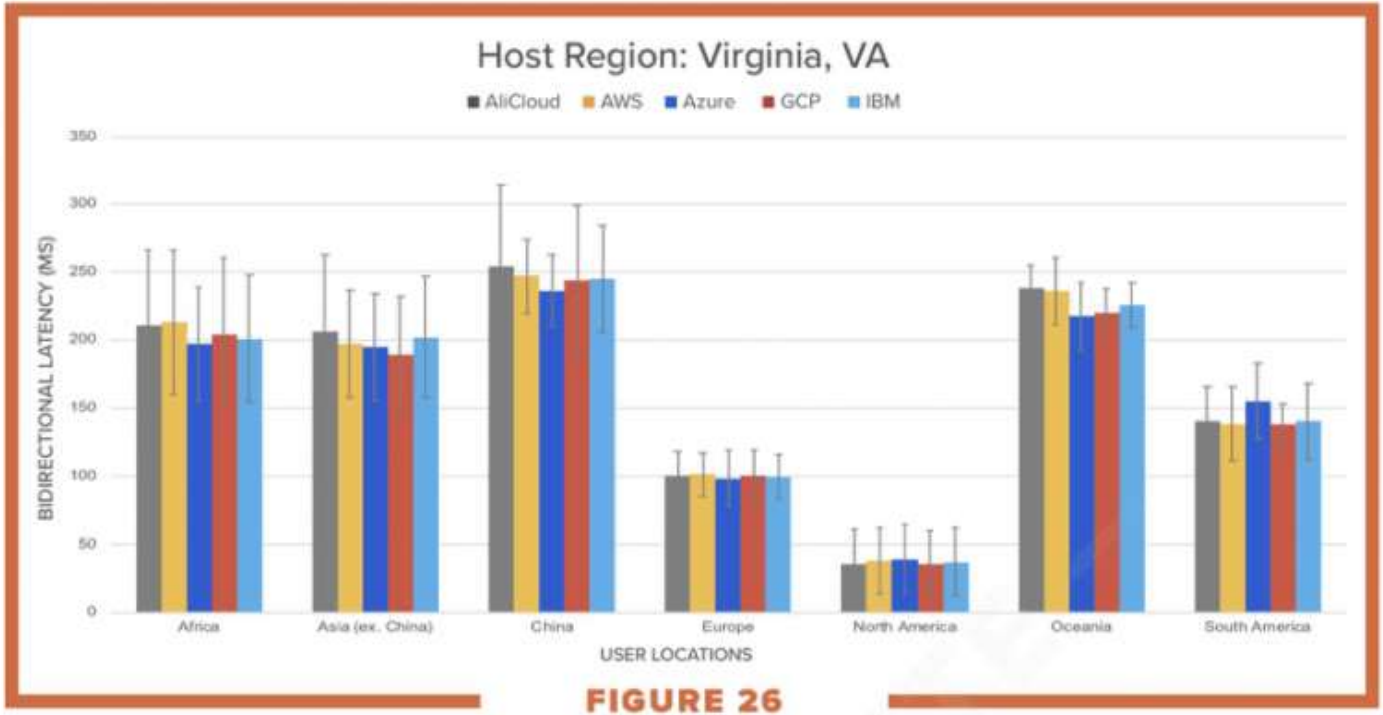


FIGURE 26

Bi-directional network latency between global user locations and the Virginia data centers (regions) of all five public cloud providers

source

Firewalls

Security groups in AWS, Network security groups in Azure, VPC firewall rules in GCP… similar names for the other providers.

Used to allow or explicitly deny inbound/outbound traffic.

Can be configured per protocol (e.g. TCP, UDP, ICMP - HTTP, SSH etc are based on these 3), port, and source (e.g. IP address).

Are attached to resources.

They are used to filter external (e.g. from the internet) and internal traffic (e.g. from other VMs).

Security Groups

Act as a virtual firewall for your instance to control inbound and outbound traffic

For each security group, you add *rules* that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic

AWS:
You can specify allow rules, but not deny rules.
You can specify separate rules for inbound and outbound traffic.
Security group rules enable you to filter traffic based on protocols and port numbers.

Network Access Lists (NACLs)

Are **stateless** (as opposed to firewalls which are usually stateful)

- I.e. both inbound and outbound must be allowed

Simpler, based on IP addresses

Usually support priority (lower = higher priority)

Security Groups vs NACLs

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 order, starting with the lowest numbered rule, 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 that it's associated with (therefore, it provides an additional layer of defense if the security group rules are too permissive)

DNS

Domain Name System

Translates domains to IP addresses

Cloud providers usually offer their own services

- E.g. Google’s Cloud DNS - one of the few services with 100% availability

Many companies have internal DNS

- Which might have to be migrated

More on DNS in course 5

Packet Mirroring

Some providers offer services for this

- E.g. Google Cloud

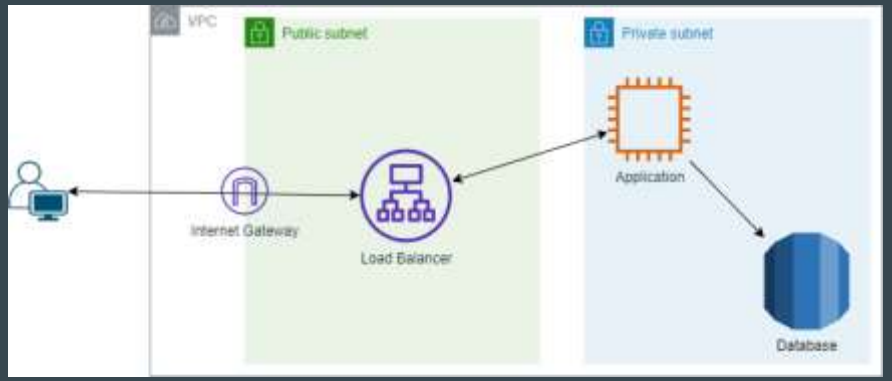
Can provide immense benefits for:

- Testing
- Recreating bugs
- Security analysis
- Anomaly detection

Does not impact traffic performance.

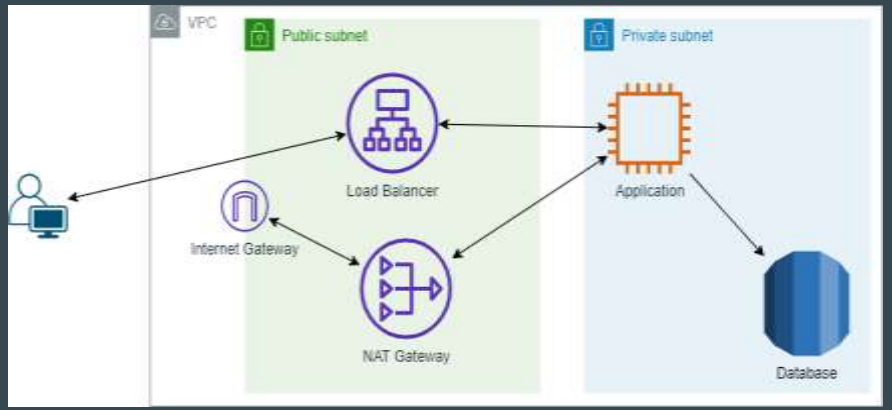
Accessing the Public Internet

Problem: the instance has to path to reach the internet (e.g. to download updates)



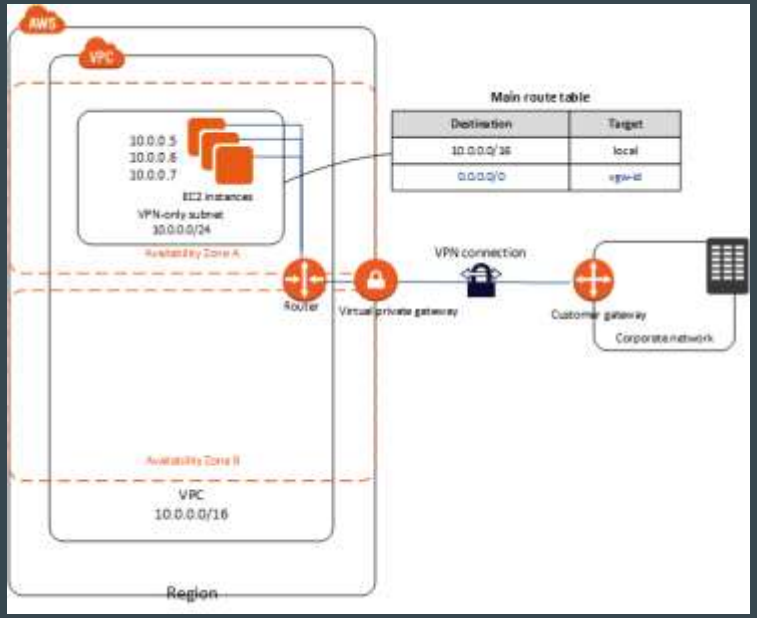
Solution: NAT

- Dedicated NAT services
  - E.g. NAT Gateway
- Configure a NAT instance

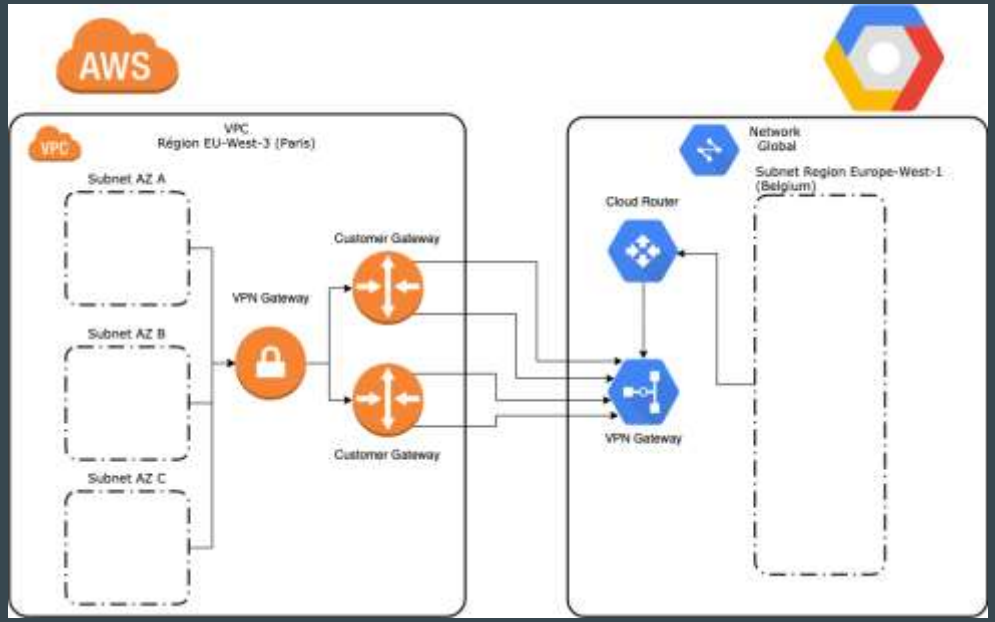


Connecting to the On-premises Systems (or other Clouds)

VPN Services



Example of VPN from On-Prem to AWS



Example of VPN from AWS to GCP

Direct Connection Services

When VPN is not enough (usually performance-wise).

Is a physical connection between customer network and cloud provider.

Highest performance achieved when connecting directly to the cloud infrastructure, but partners also offer this (enough in most cases) (e.g. Orange and Vodafone).

Network Architecture

Example of securely accessing public storage services from the corporate network