

---

# AWS Certified Advanced Networking - Specialty

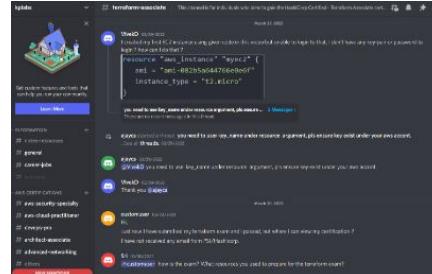
Instructed by Zeal Vora

# Our Community

You can join our **Discord community** for any queries / discussions. You can also connect with other students going through the same course in Discord (Optional)

Discord Link: <http://kplabs.in/chat>

Group Page: #advanced-networking



---

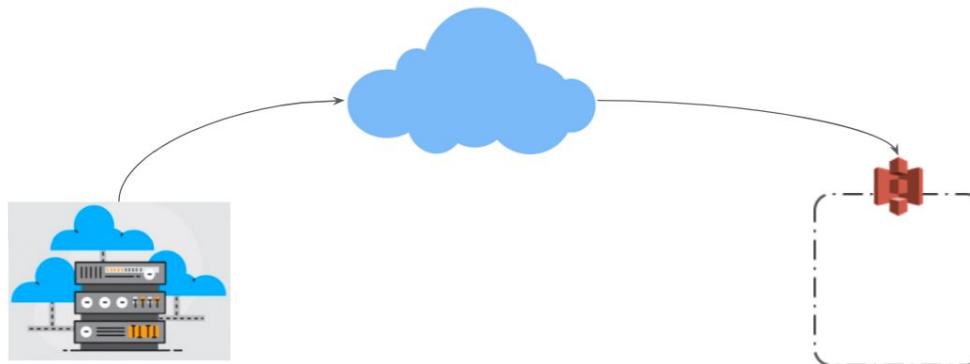
# VPC Endpoints

Private Communication is Better

---

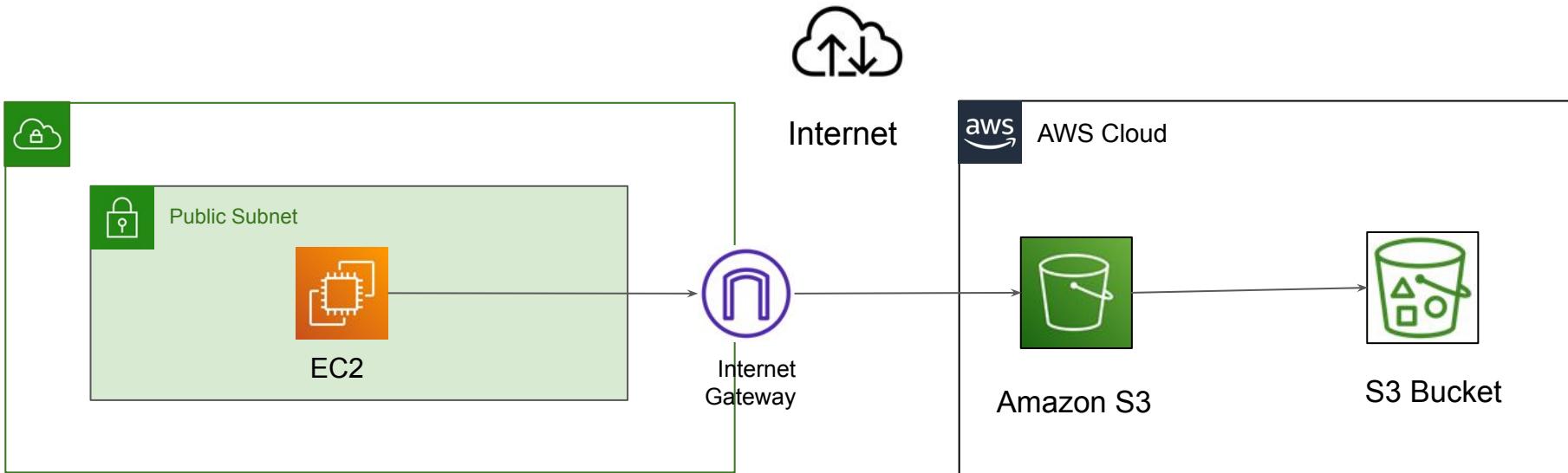
# Use-Case: EC2 and S3 Communication

For EC2 instances to be able to access public resources like S3, DynamoDB and others, the traffic needed to be passed via Internet Gateway.

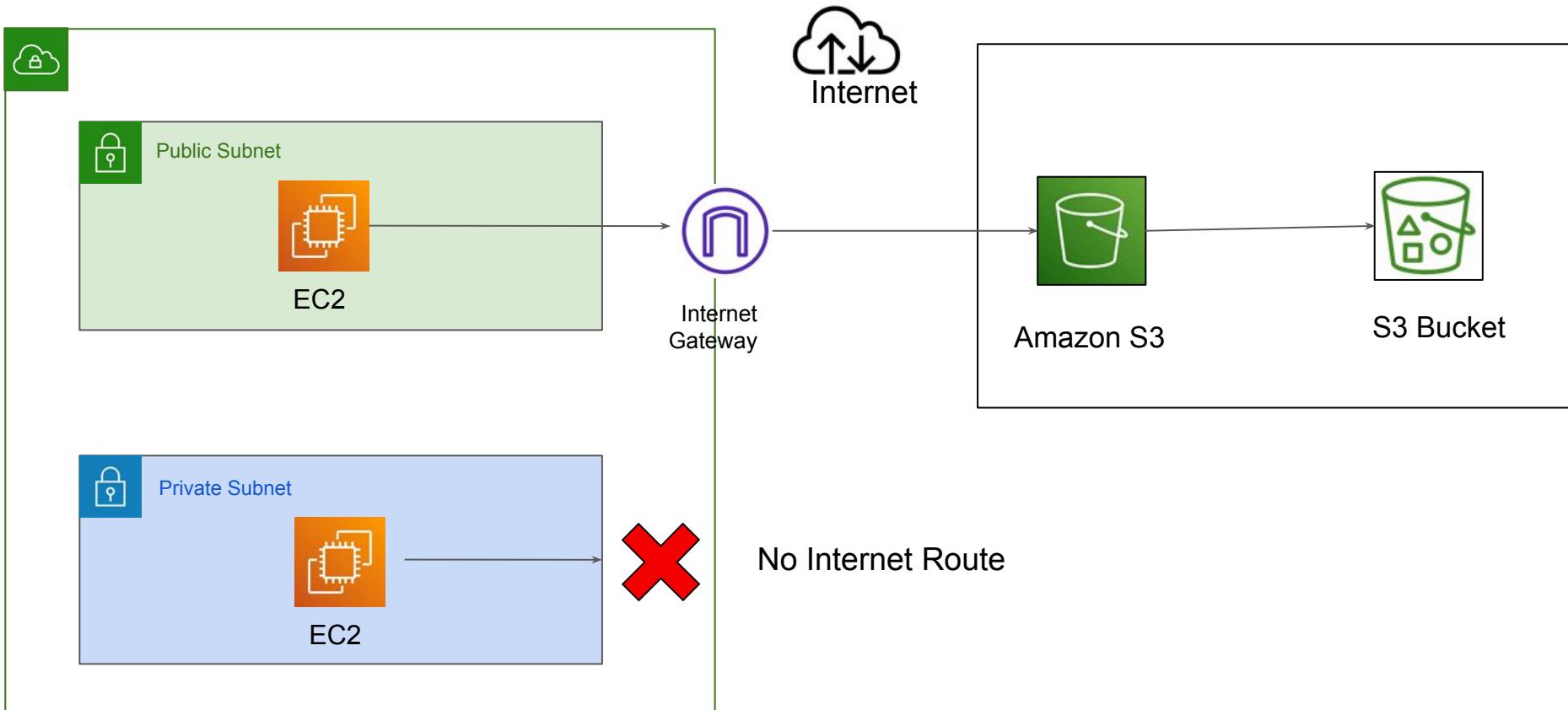


# Architectural Perspective

EC2 traffic towards S3 is routed to Internet Gateway



# Challenge with Private Workloads

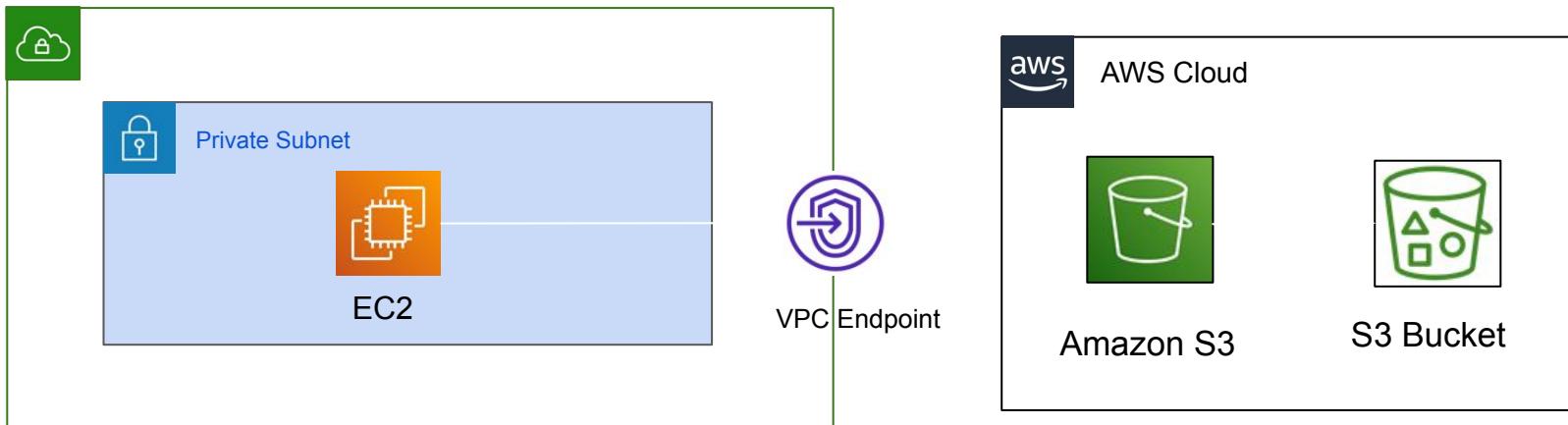


# Downsides of Using Public Internet

1. Data transfer cost of AWS
2. Higher Latency
3. Can bottleneck your internet gateway.
4. Security

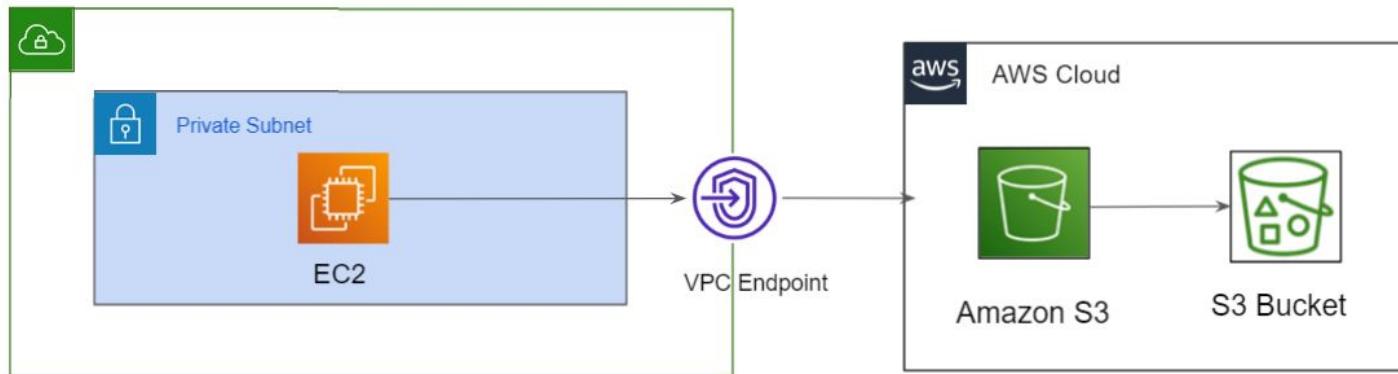
# Overview of VPC Endpoints

VPC Endpoints allows us to connect VPC to another AWS services OR other supported services over AWS private network.



# Overview of VPC Endpoints

VPC Endpoints allows us to connect VPC to another AWS services OR other supported services over AWS network.



# Revising Important Pointers

AWS PrivateLink is a technology that enables you to privately access services by using private IP addresses.

To use AWS PrivateLink, you can create a VPC endpoint for a service in your VPC.

VPC Endpoint allows us to connect VPC to another AWS services over AWS network.

Traffic between your VPC and the other service does not leave the Amazon network.

---

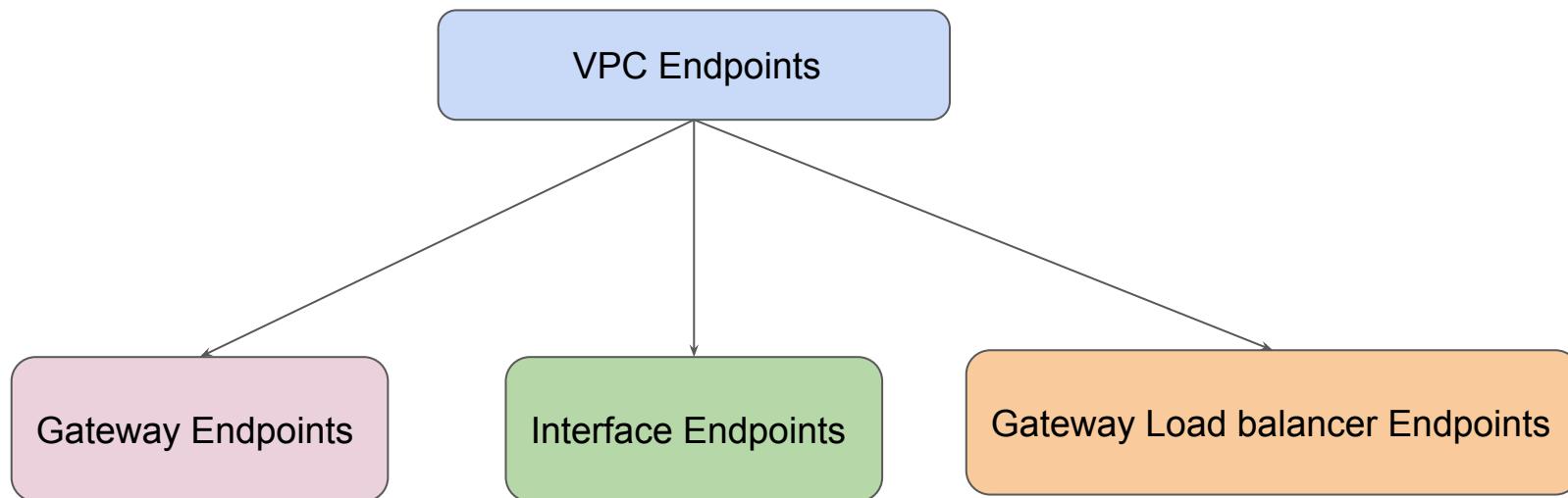
# Gateway VPC Endpoints

## Understanding Types

---

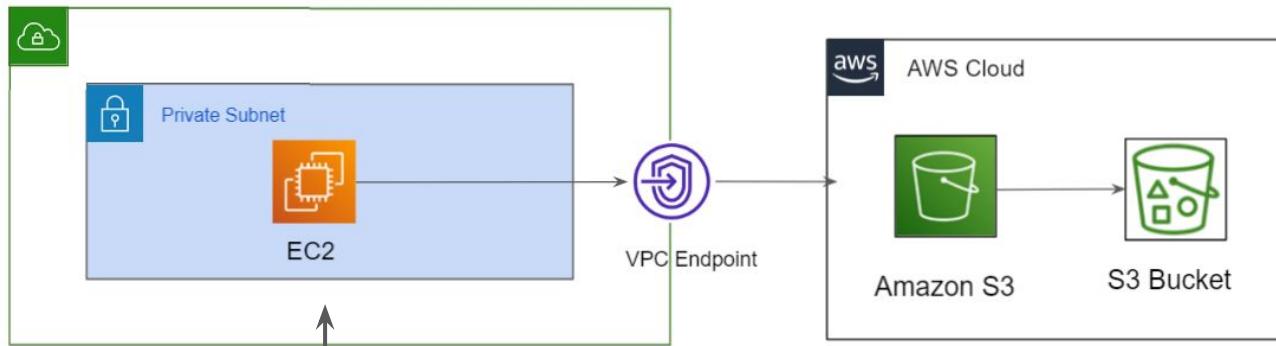
# VPC Endpoints Type

There are three primary types of VPC Endpoints available.



# Gateway VPC Endpoints

We specify the Gateway Endpoint as a route table target that is destined for supported AWS services.



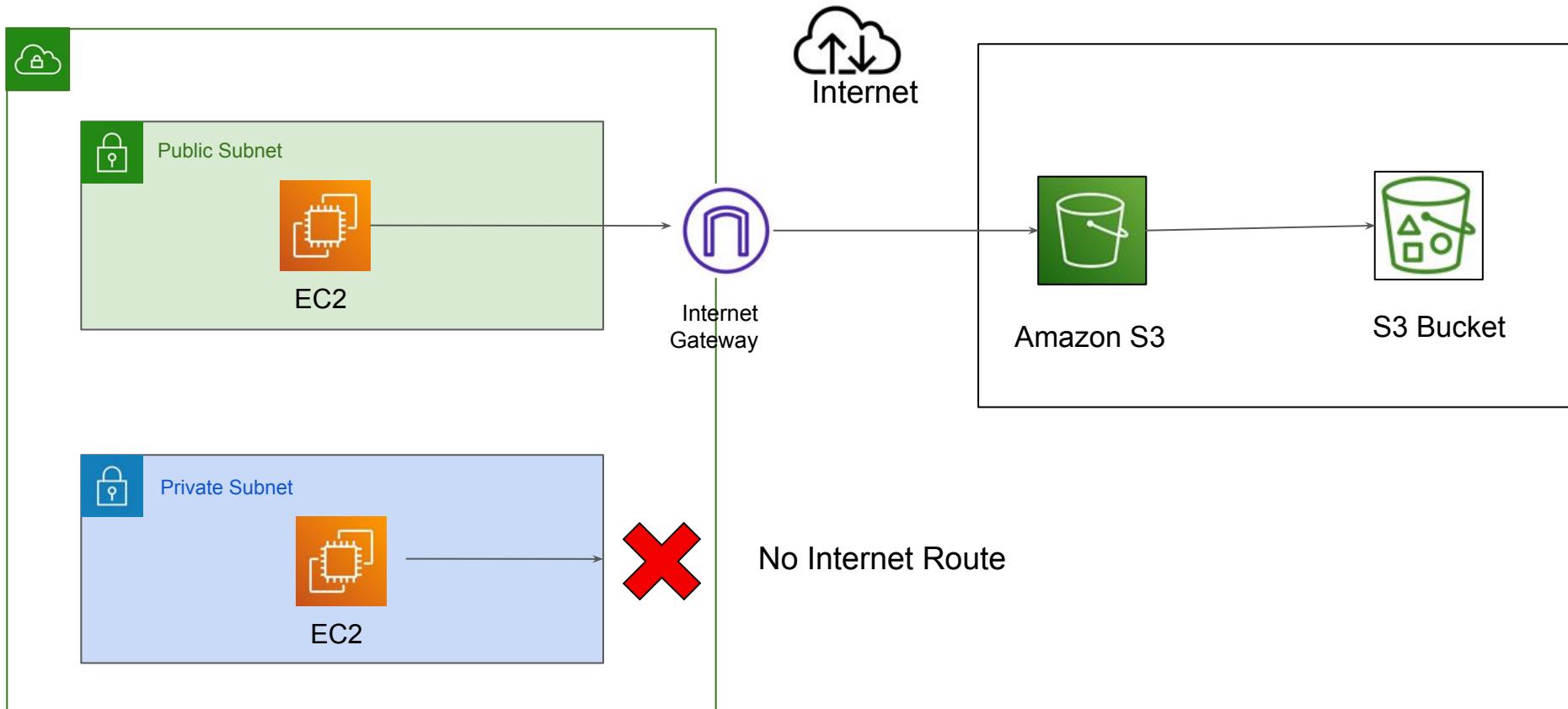
Destination	Target
172.31.0.0/16	local
54.231.0.0/17	vpce-11bb22cc

# Supported Services

A gateway endpoint is for the following supported AWS services:

1. Amazon S3
2. DynamoDB

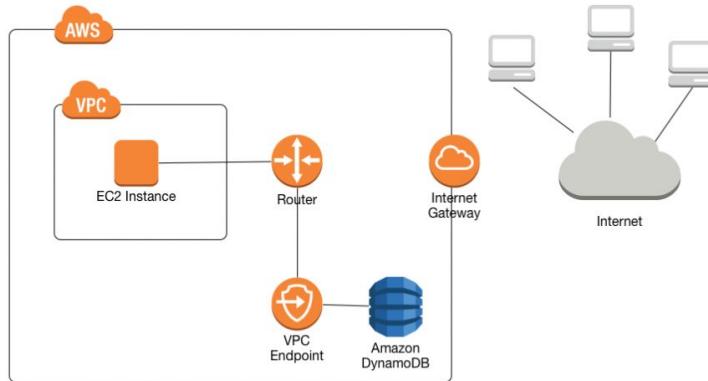
# Today's Architecture



# Downsides of Gateway Endpoints - 1

In Gateway endpoints approach, the VPC endpoint was created outside your VPC and traffic was routed via route table.

Thus, it is not possible to use it directly from VPN's or Direct connects and various others.



## Downsides of Gateway Endpoints - 2

Endpoints are supported within the same Region only. You cannot create an endpoint between a VPC and a service in a different Region.

Endpoints support IPv4 traffic only.

You must turn on DNS resolution in your VPC, or if you're using your own DNS server, ensure that DNS requests to the required service (such as Amazon S3) are resolved correctly to the IP addresses maintained by AWS.

---

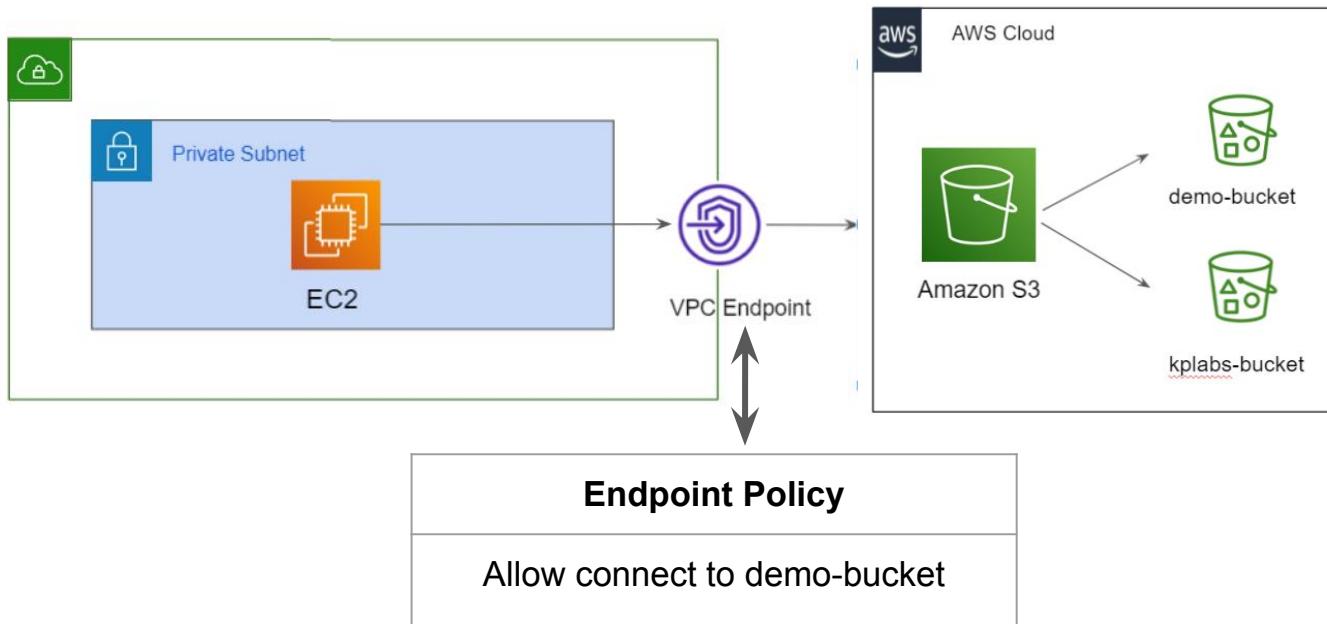
# VPC Endpoint Policies

Endpoint Based Access Control

---

# Overview of VPC Endpoint Policies

When you create a gateway endpoint, you can attach an endpoint policy to it that controls access to the service to which you are connecting.



# Default Policy

The default VPC Endpoint policy allows all the operations

The screenshot shows the AWS VPC Endpoint service in the AWS Management Console. At the top, there is a table listing a single VPC endpoint:

Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
vpce-09172dfa... (checkbox)	vpc-7582d50d	com.amazonaws.us-west-2.s3	Gateway	available	June 22, 2021 at 11:25:39 AM UTC+5...	

Below the table, the endpoint details are shown:

**Endpoint:** vpce-09172dfa... (checkbox)

Below the endpoint details, there are four tabs: Details, Route Tables, Policy, and Tags. The Policy tab is selected, indicated by a yellow background.

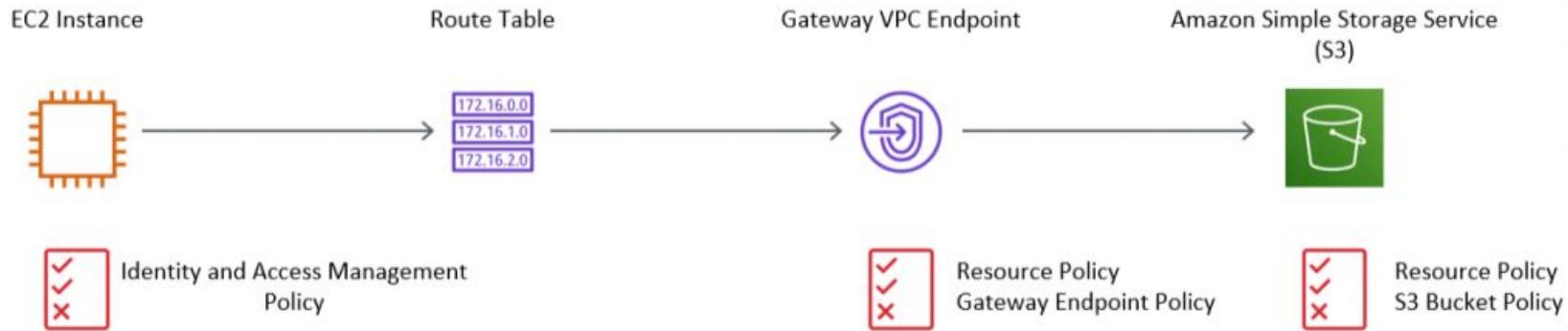
Under the Policy tab, there is a button labeled "Edit Policy".

Below the "Edit Policy" button, there is a note: "Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed."

A large gray box displays the JSON policy document:

```
{  
  "Statement": [  
    {  
      "Action": "*",  
      "Effect": "Allow",  
      "Resource": "*",  
      "Principal": "*"  
    }  
  ]  
}
```

# Policy Decision



---

# Interface Endpoints

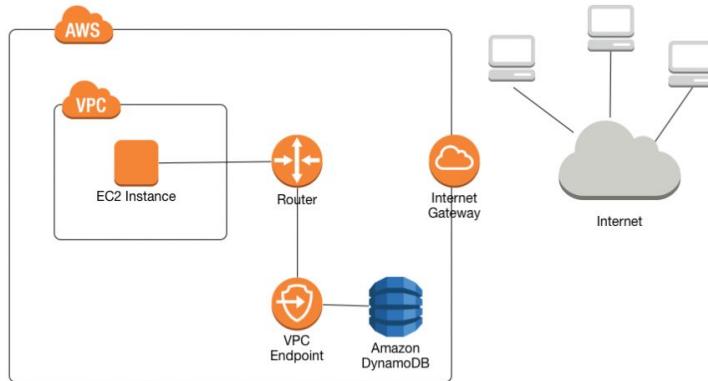
New Generation Endpoint

---

# Downsides of Gateway Endpoints - 1

In Gateway endpoints approach, the VPC endpoint was created outside your VPC and traffic was routed via route table.

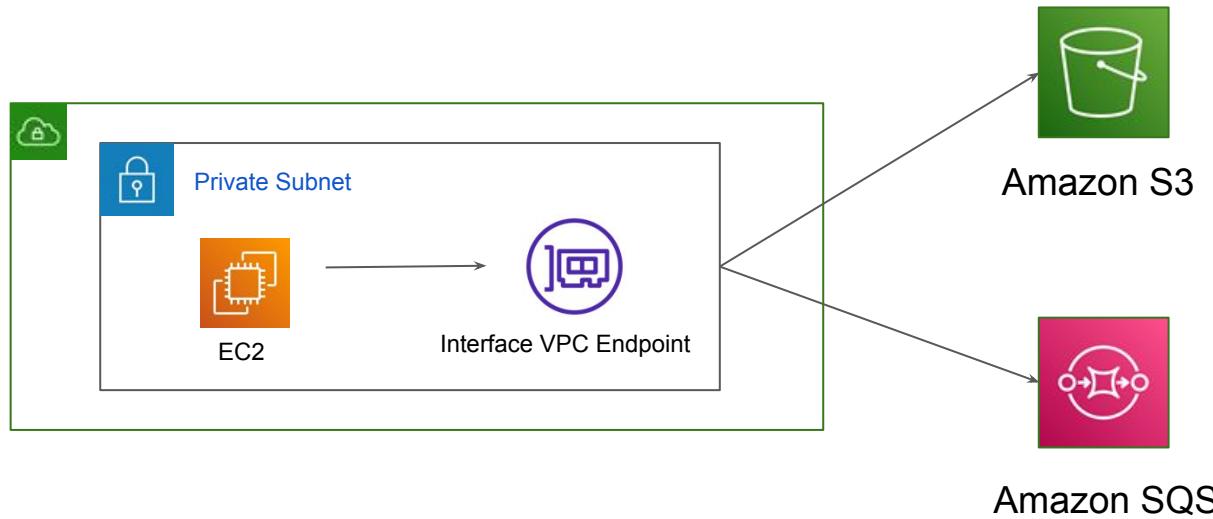
Thus, it is not possible to use it directly from VPN's or Direct connects and various others.



# Interface Endpoints

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet.

It serves as an entry point for traffic destined to a supported AWS service or a VPC endpoint service.



# Benefits of Interface Endpoint

1. Interface endpoints enable the use of security groups to restrict access to the endpoint.
2. VPN's and Direct Connect based connections are supported.
3. Interface endpoints supports lot of services unlike Gateway endpoints.

---

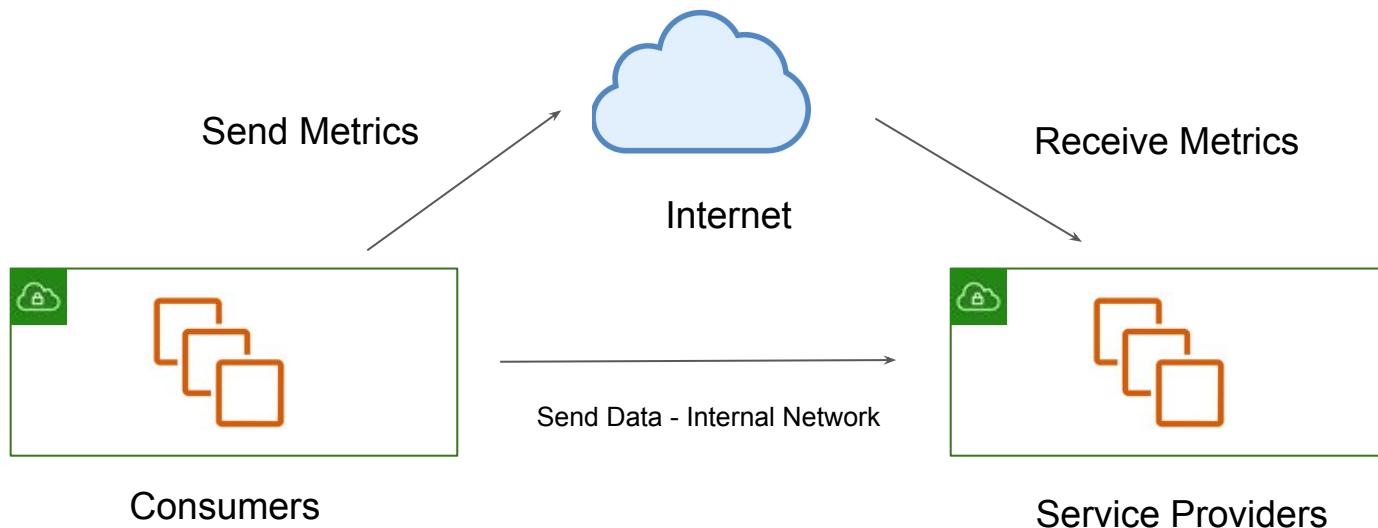
# VPC Endpoint Services

More Use-Cases Supported

---

# Sample Use-Case

There are many service providers like DataDog, New Relic for which we need to upload our server/application metrics through Internet.



# Dashboards using Metrics Collected

New Relic University > **SELECT** | Run New Relic University

**Calagator Demo App** Created by evose@newrelic.com Last edited 4/3/18

Search 2 attributes Add Dashboard Note Edit

Default 30m 60m 6h 1d 7d Custom

**Calagator Demo App**  
AN OPEN SOURCE CALENDAR AGGREGATOR

This demo app is built using the open source calagator project.

[Calagator on Github](#)

**Transaction Duration & Queing** Since 60 minutes ago

NAME	TRANS...	Avg D...	Avg Q...
Controller/Middleware/Rack/ActionDispatch::Static/call	971	0.01	0.07
Controller/calagator/site/index	319	0.56	0.1
Controller/calagator/events/search	313	5.78	0.1
Controller/Middleware/Rack/ActionDispatch::Routing::RouteSet/call	187	0.21	0.12
Controller/calagator/sources/new	20	0.17	0.04

**Frequent Transactions in the past 4 weeks** Since 4 weeks ago

Transactions

631 K Controller/Middleware/Rack/
210 K Controller/calagator/site/inde
197 K Controller/calagator/events/s
120 K Controller/Middleware/Rack/
29.4 K Controller/Middleware/Rack/
13 K Controller/calagator/sources/
10.3 K Controller/calagator/sources/

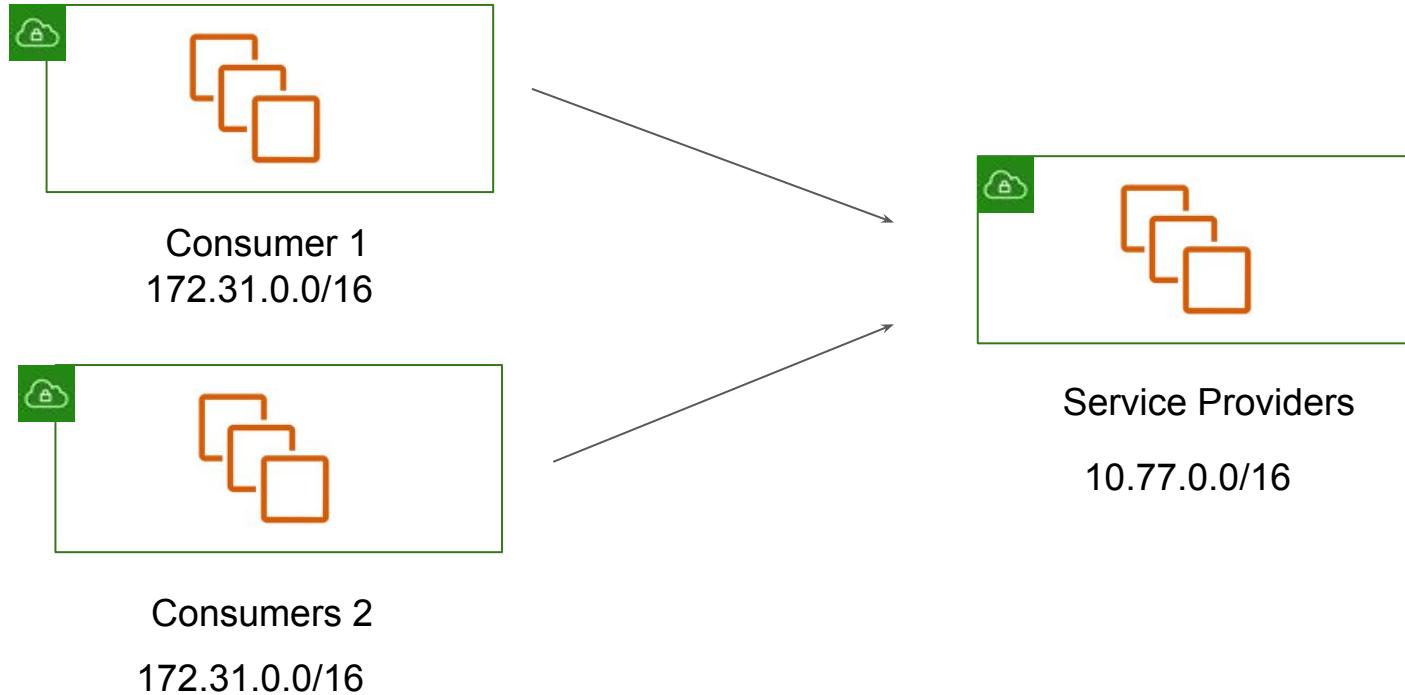
**NRU Calagator Demo - Apdex** Since 12 hours ago

**Apdex** Since 60 minutes ago

**Transaction Duration** Since 1 month ago

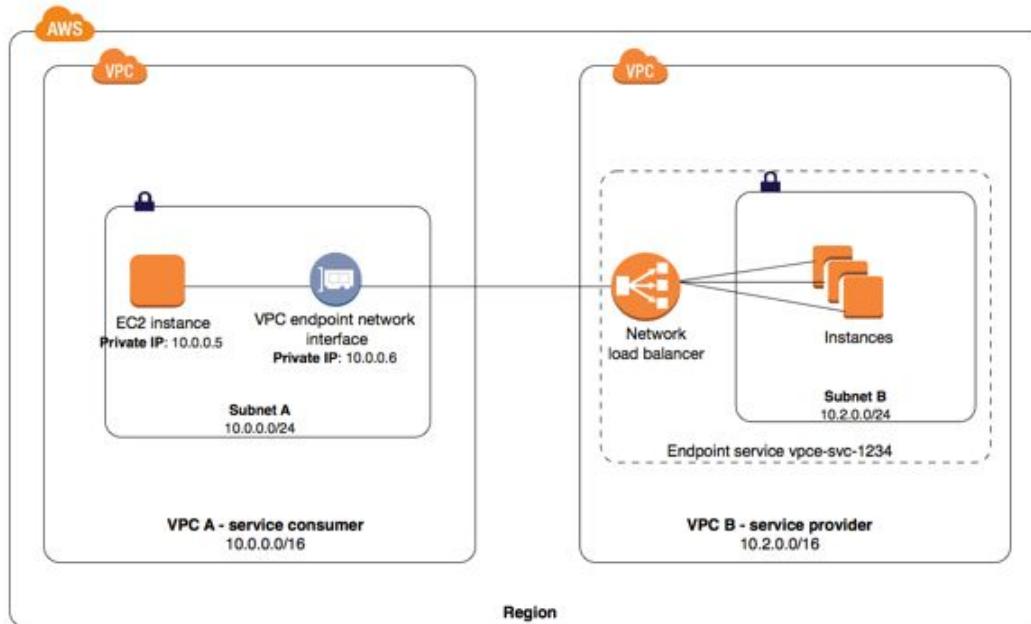
# Possible Approach - VPC Peering

VPC Peering Approach will have multiple challenges related to CIDR overlap between clients.



# Service VPC Endpoints

You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service)



---

# Intro to Amazon SQS

Message Queuing Service

---

# Use-Case: Restoring Image Application

Medium Corp is designing an application that will enhance and restore the images that users submit through the online portal.



# Current Architecture

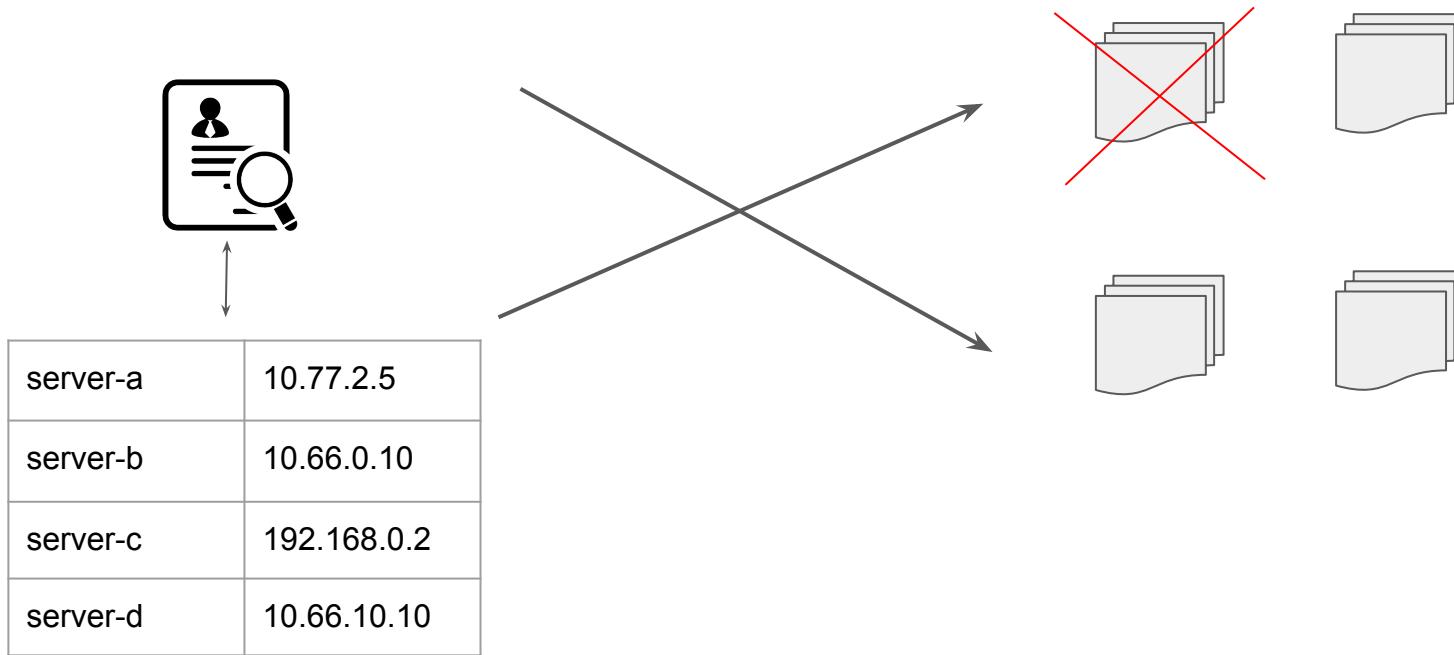
The overall architecture involves two components:

1. Image Gatherer - Takes the Images from the user via Upload button.
2. Imager Enhancer - Receives the Image from Image Gatherer.



# Challenges

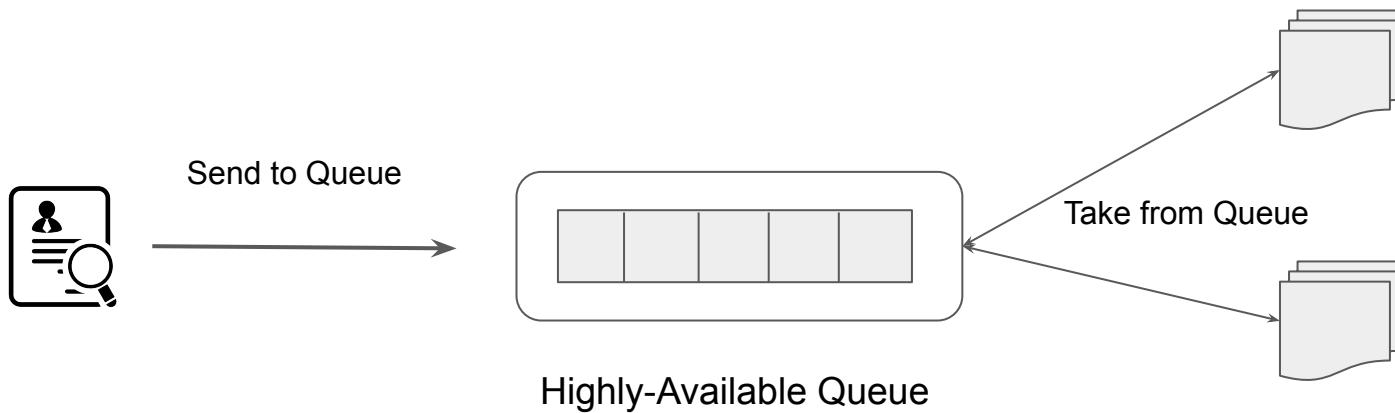
Due to popularity of the application and huge traffic spike, Medium Corp has decided to add more image enhancer servers.



# Better Architecture

One of the main function of message queue service is to take message from a Publisher and forward that to a consumer.

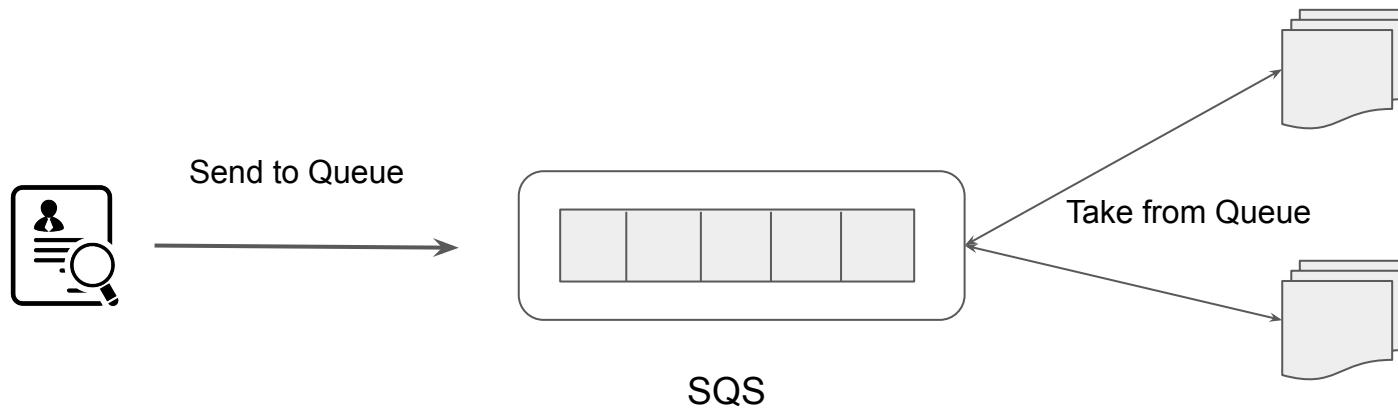
The queue stores these messages internally.



# Introduction to SQS

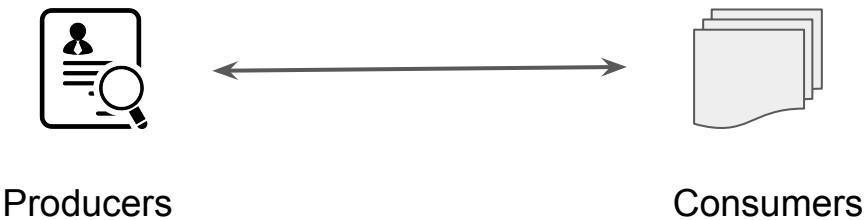
Amazon SQS is a fast reliable, scalable, and fully managed message queuing service.

Amazon SQS makes it simple and quiet cost effective to decouple the components of a specific application.



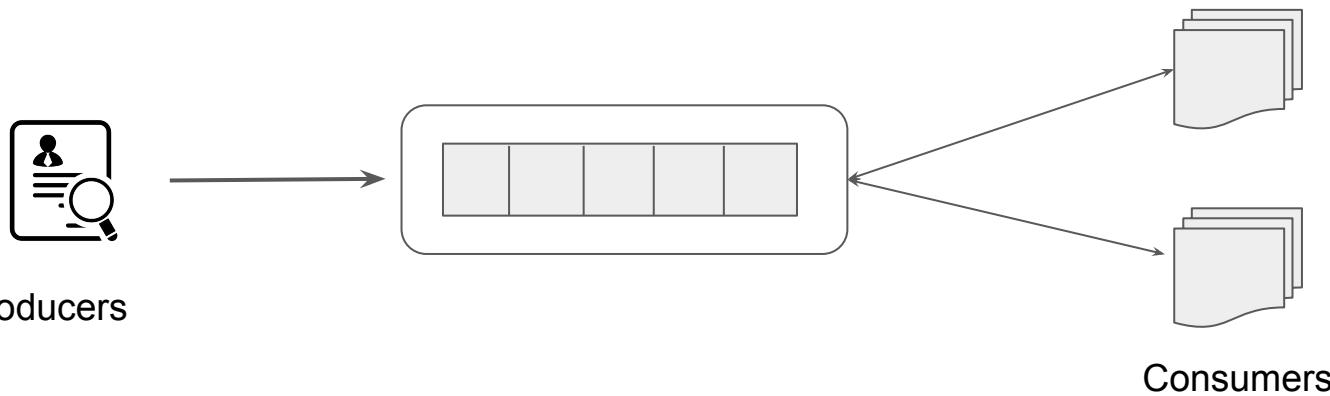
# Tightly Coupled Systems

Components of system architecture directly communicate with each other and have hard-dependency on each other.



# Loosely Coupled System

Components of system architecture that can process the information without being directly connected.



---

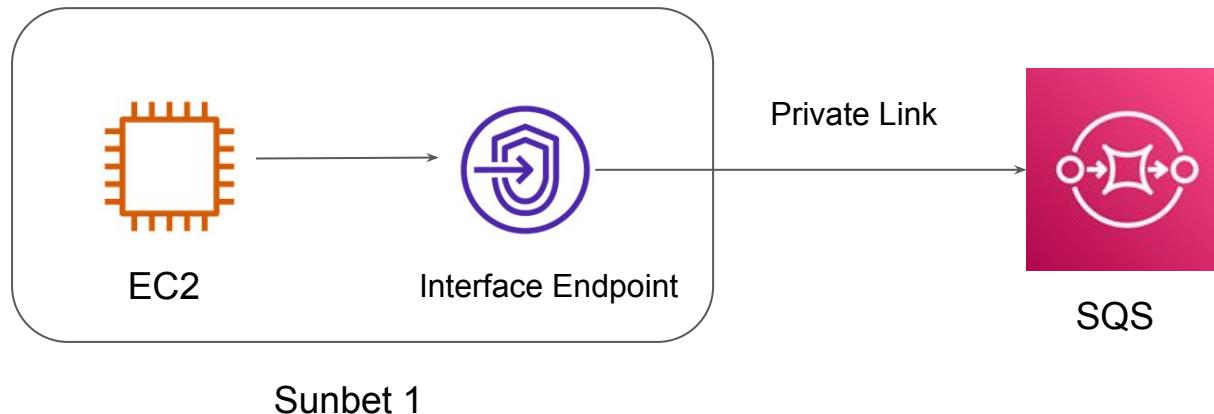
# SQS - VPC Endpoints

Send Messages Privately

---

# SQS Endpoints

AWS allows customers to access Amazon SQS from their VPC using VPC endpoints, without using public IPs, and without needing to traverse the public internet.



# Important Pointers - SQS Endpoints

You can use VPC only with HTTPS Amazon SQS endpoints.

When you configure Amazon SQS to send messages from Amazon VPC, you must enable private DNS and specify endpoints in the format `sqs.us-east-2.amazonaws.com`.

Private DNS doesn't support legacy endpoints such as `queue.amazonaws.com` or `us-east-2.queue.amazonaws.com`.

---

# Load Balancing in AWS

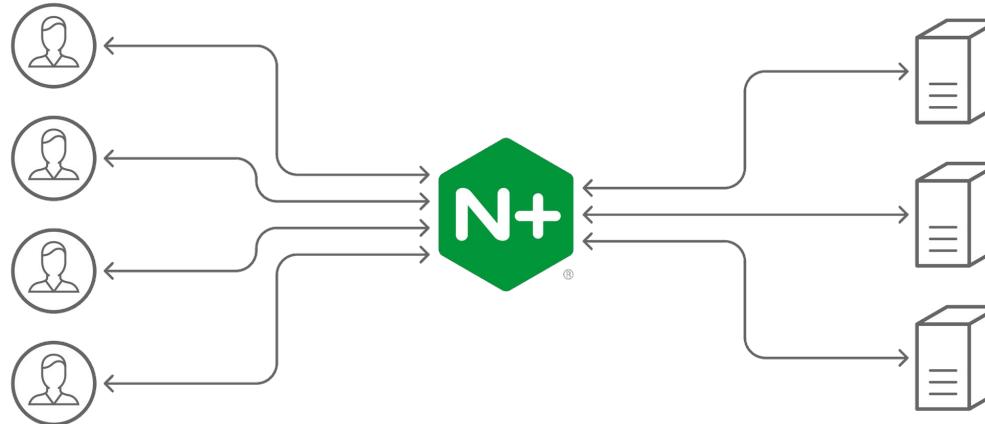
Let's Load Balance Traffic in AWS

---

# Basics of Load Balancing

There are multiple software and hardware based load balancing solutions available.

Some of the popular ones include Nginx, HA Proxy and others.



# Challenges with Maintaining Load Balancing Solution

If you are using a load balancing solution, various responsibilities falls to customer.

Some of these include:

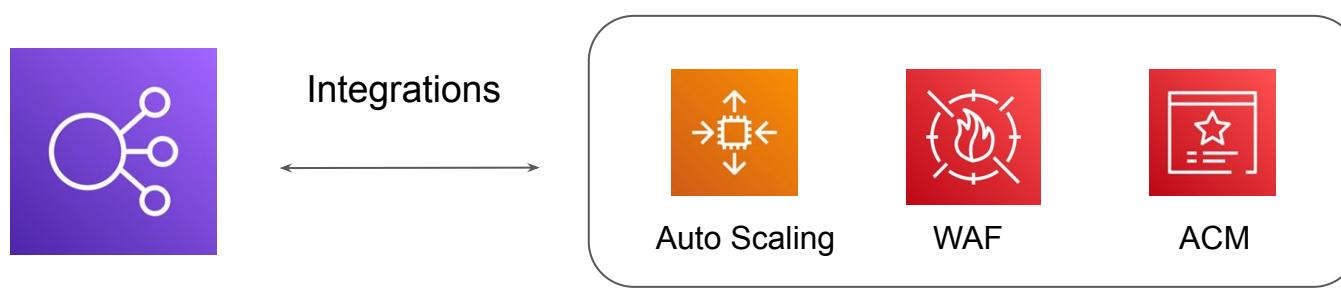
1. High-Availability of Load Balancers.
2. Security.
3. Performance.

# Basics of Elastic Load Balancing Service

AWS offers managed load balancing solutions for wide variety of use-cases.

These solutions are offered under the Elastic Load Balancing feature.

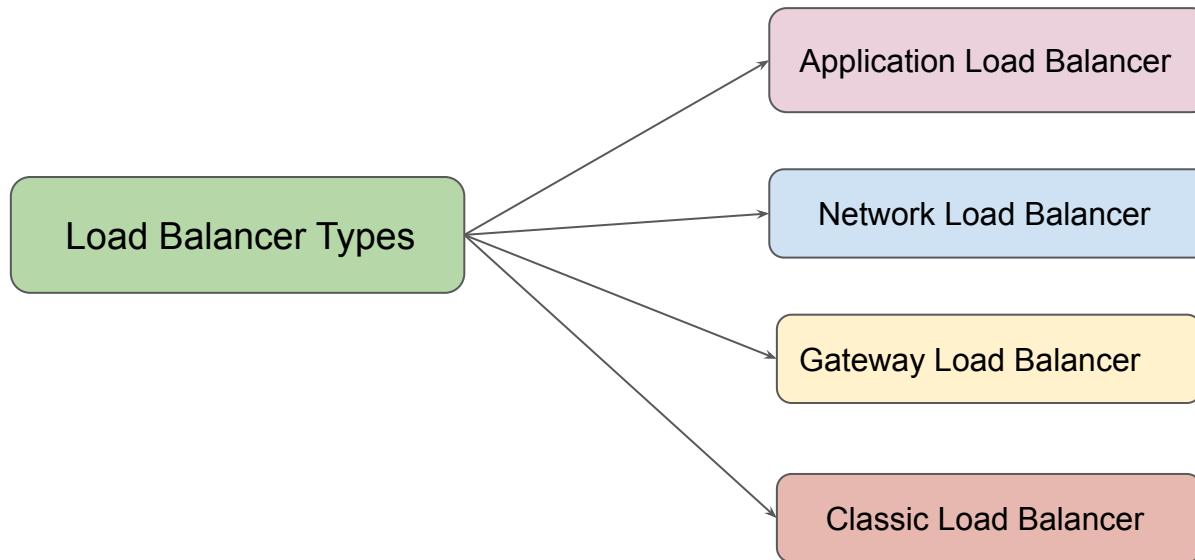
Tight integration with multiple AWS Services.



Elastic Load Balancing

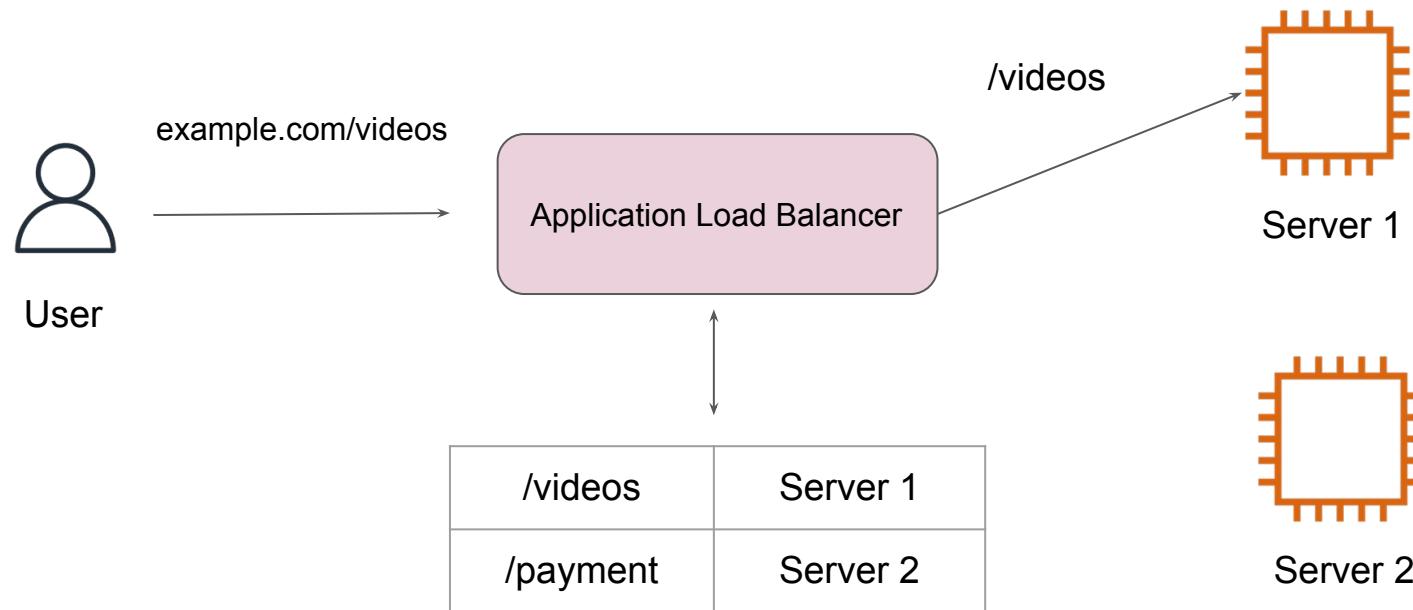
# Types of Load Balancers

There are 4 primary type of Load Balancer offerings available.



# Application Load Balancers

An Application Load Balancer makes routing decisions at the application layer (HTTP/HTTPS)

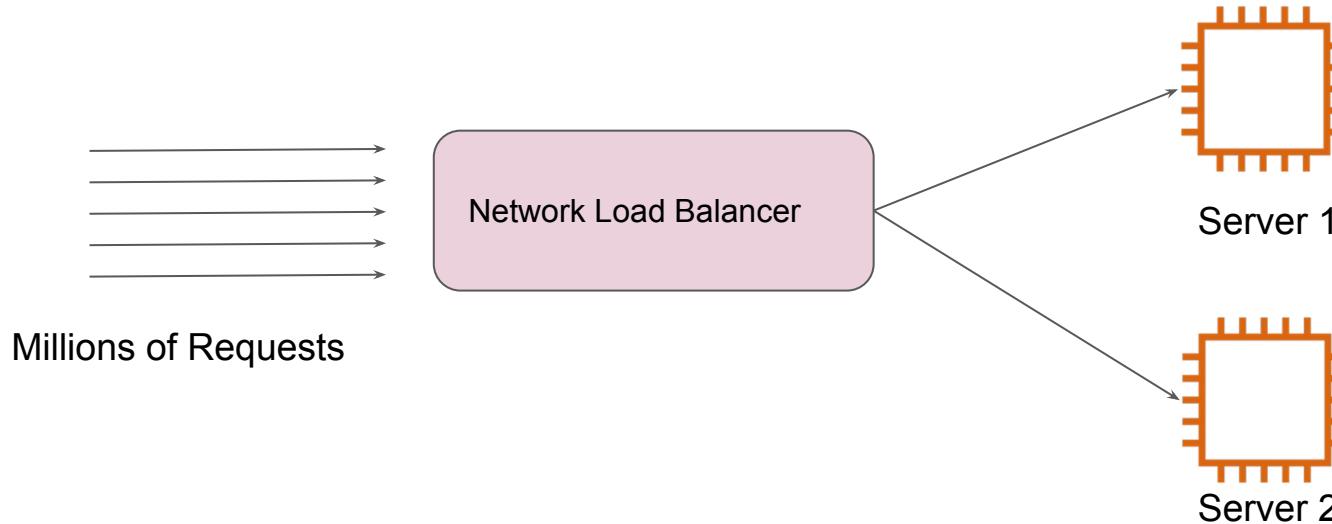


# Network Load Balancers

A Network Load Balancer makes routing decisions at the transport layer (TCP/UDP/SSL).

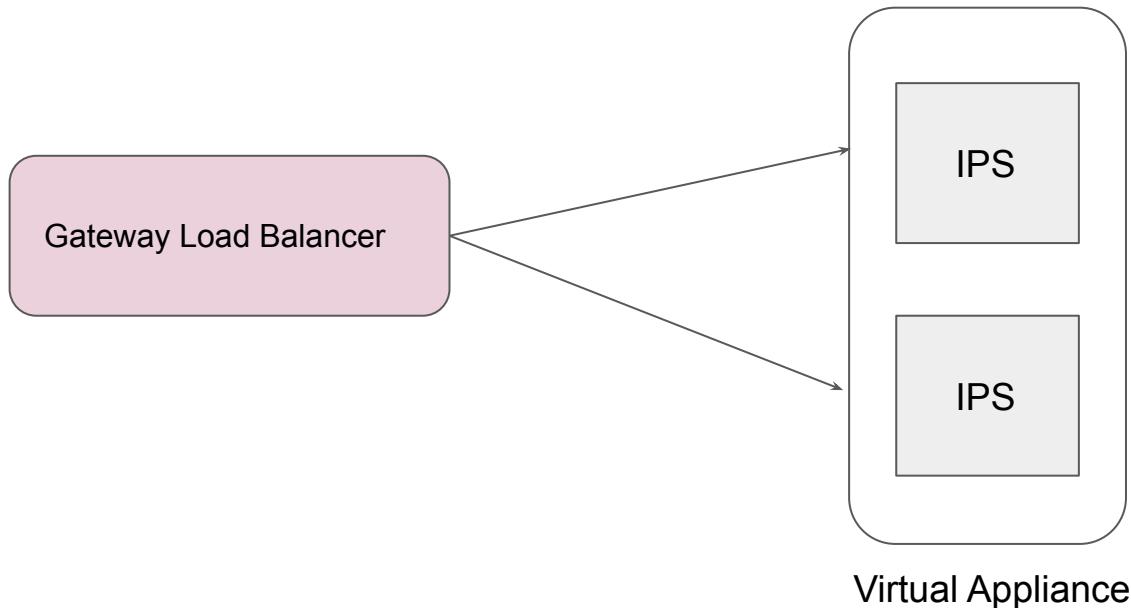
It can handle millions of requests per second.

Not all of the applications work on HTTP/HTTPS protocol.



# Gateway Load Balancers

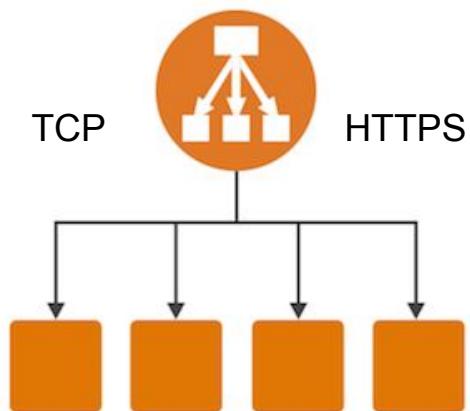
Gateway Load Balancers allow you to deploy, scale, and manage virtual appliances, such as firewalls, intrusion detection and prevention systems, and deep packet inspection systems



# Classic Load Balancers

A Classic Load Balancer makes routing decisions at either the transport layer (TCP/SSL) or the application layer (HTTP/HTTPS).

Previous Generation Load Balancer and not recommended.



# Summary Slide

Load Balancer	Important Notes
Application Load Balancer	Use when you have websites/applications at L7 (HTTP/HTTPS)
Network Load Balancers	<p>TCP and UDP based applications.</p> <p>Requirement to handle millions of requests per second.</p> <p>Ultra high performance.</p>
Gateway Load Balancer	<p>Use when you have virtual appliances:</p> <p>IDS/IPS Firewalls</p>

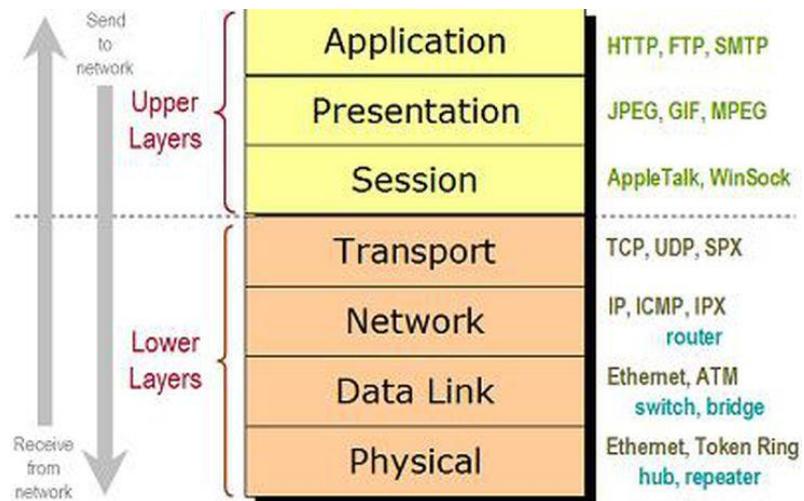
---

# OSI Model & Load Balancers

Revising Networking

# Basics of OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It



# Load Balancer & OSI Layers

Each load balancer operates at a specific layer.

You will only be able to perform operations on requests based on Layer the ELB supports.

Feature	Application Load Balancer	Network Load Balancer	Gateway Load Balancer	Classic Load Balancer
Load Balancer type	Layer 7	Layer 4	Layer 3 Gateway + Layer 4 Load Balancing	Layer 4/7

---

# Classic Load Balancers

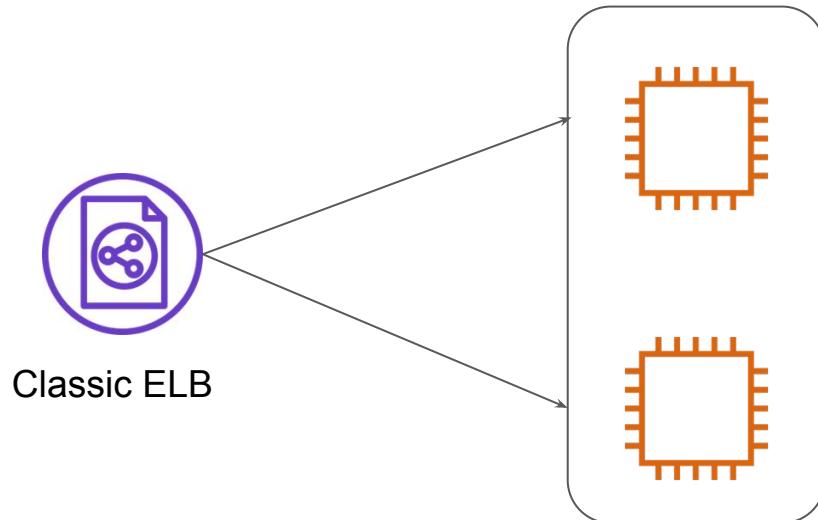
First generation Load Balancers

---

# Understanding Classic Load Balancers

These are older generation of load balancers.

Provides basic set of features for HTTP, HTTPS, TCP and SSL protocols.



# Limitation of Classic Load Balancers

- Does not support native HTTP/2 protocol.
- IP address as targets are not supported.
- Path based routing is not supported. (eg: /images should go to server 1 & /php to server 02)
- Many Many more .....

---

# Application Load Balancers

Next generation load balancers

---

# Basics of HTTP Headers

HTTP headers let the client and the server pass additional information with an HTTP request or response.

▶ GET http://demo-alb-137613815.us-east-1.elb.amazonaws.com/

---

Status	200 OK ⓘ
Version	HTTP/1.1
Transferred	196 B (35 B size)
Request Priority	Highest

---

▼ Response Headers (161 B)

- ⓘ Connection: keep-alive
- ⓘ Content-Length: 35
- ⓘ Content-Type: text/plain; charset=utf-8
- ⓘ Date: Thu, 21 Jul 2022 16:49:49 GMT
- ⓘ Server: awselb/2.0

---

▼ Request Headers (380 B)

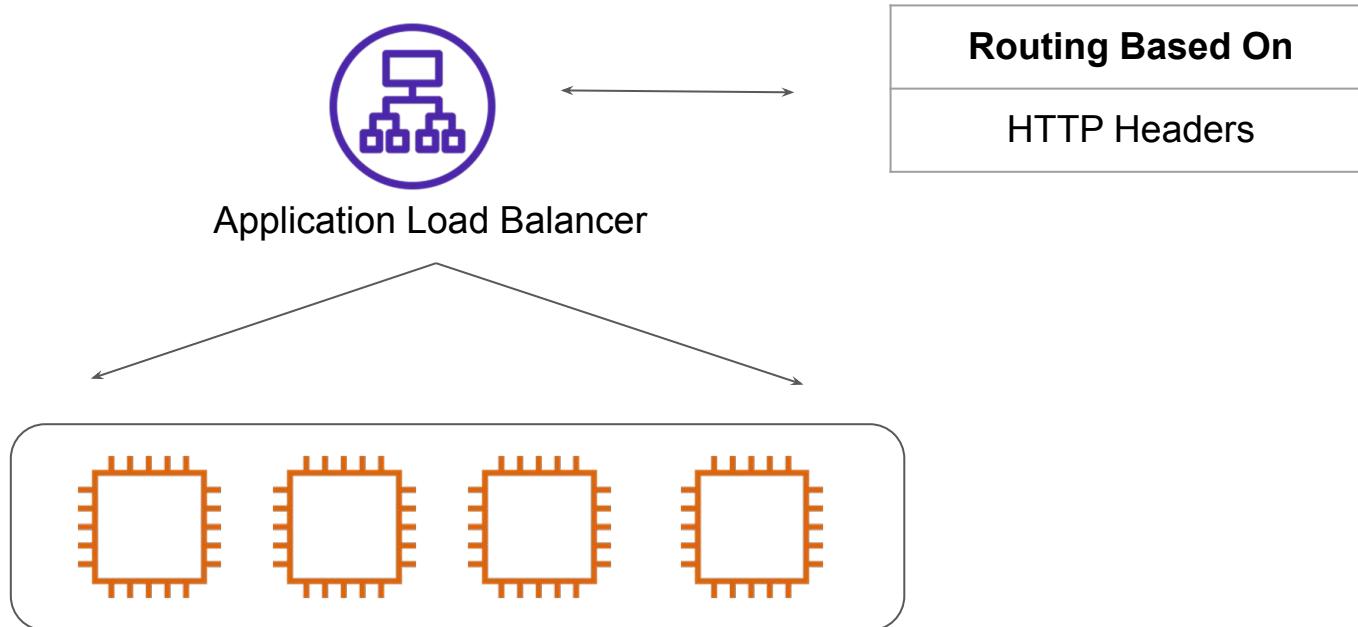
- ⓘ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8
- ⓘ Accept-Encoding: gzip, deflate
- ⓘ Accept-Language: en-US,en;q=0.5
- ⓘ Connection: keep-alive
- ⓘ Host: demo-alb-137613815.us-east-1.elb.amazonaws.com
- ⓘ Upgrade-Insecure-Requests: 1

---

ⓘ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

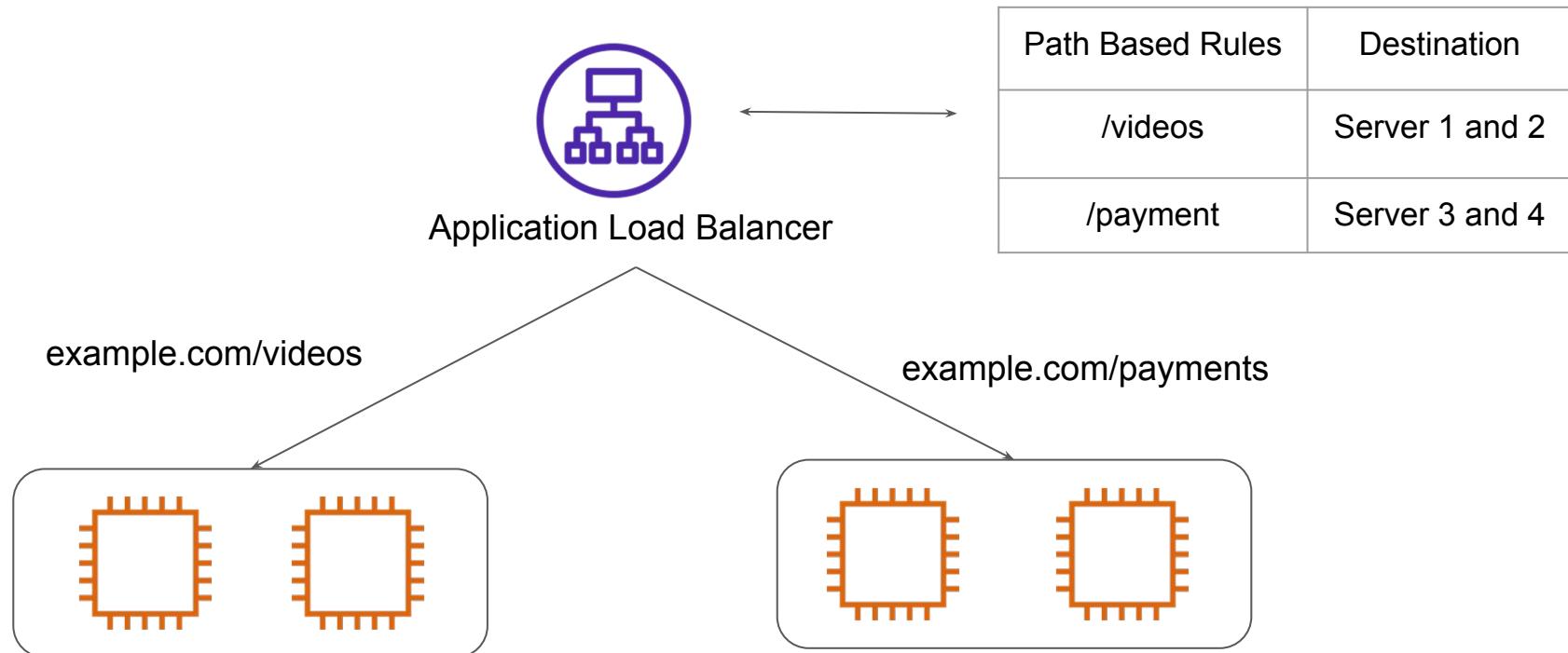
# Understanding ALB

Application Load Balancer functions at Application layer and support both HTTP & HTTPS



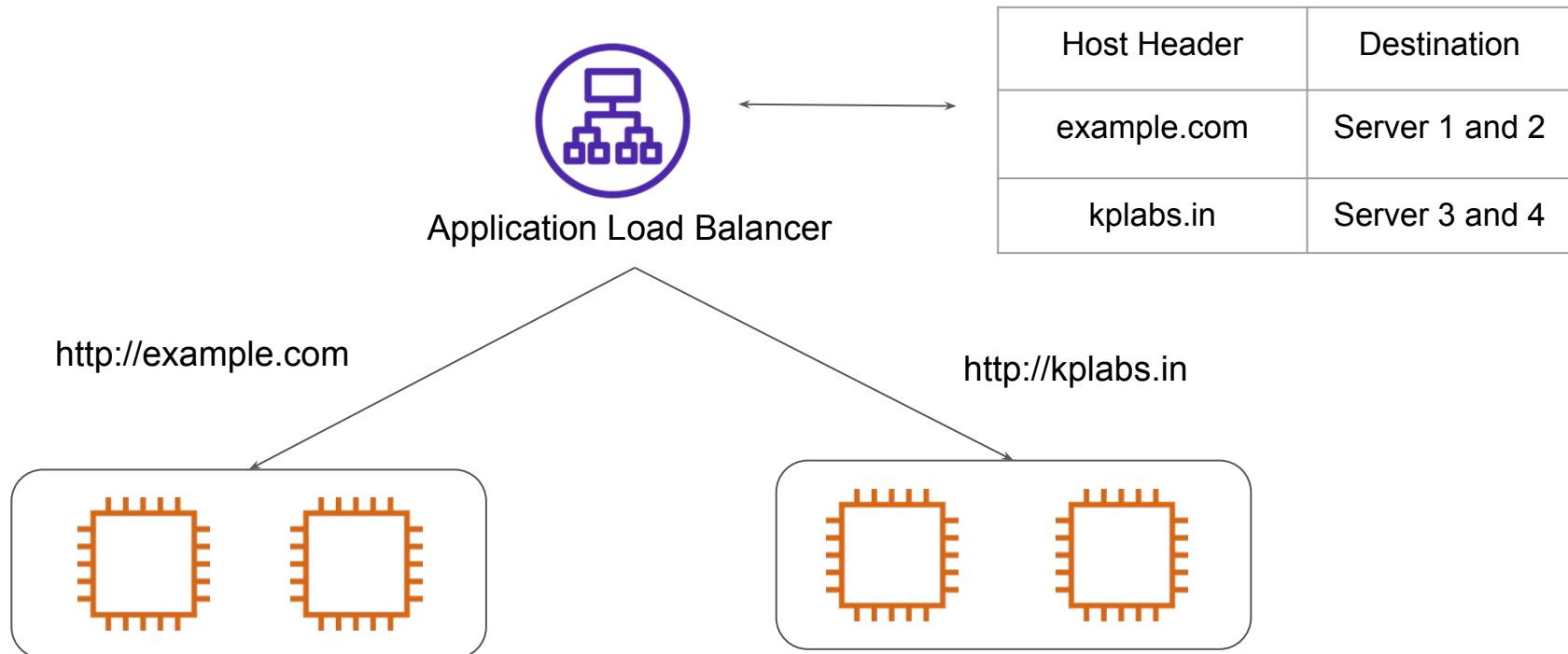
# Path Based Routing

The requests are routed based on the URI path.



# Routing Using Host Headers

The requests are routed based on the Host Header



---

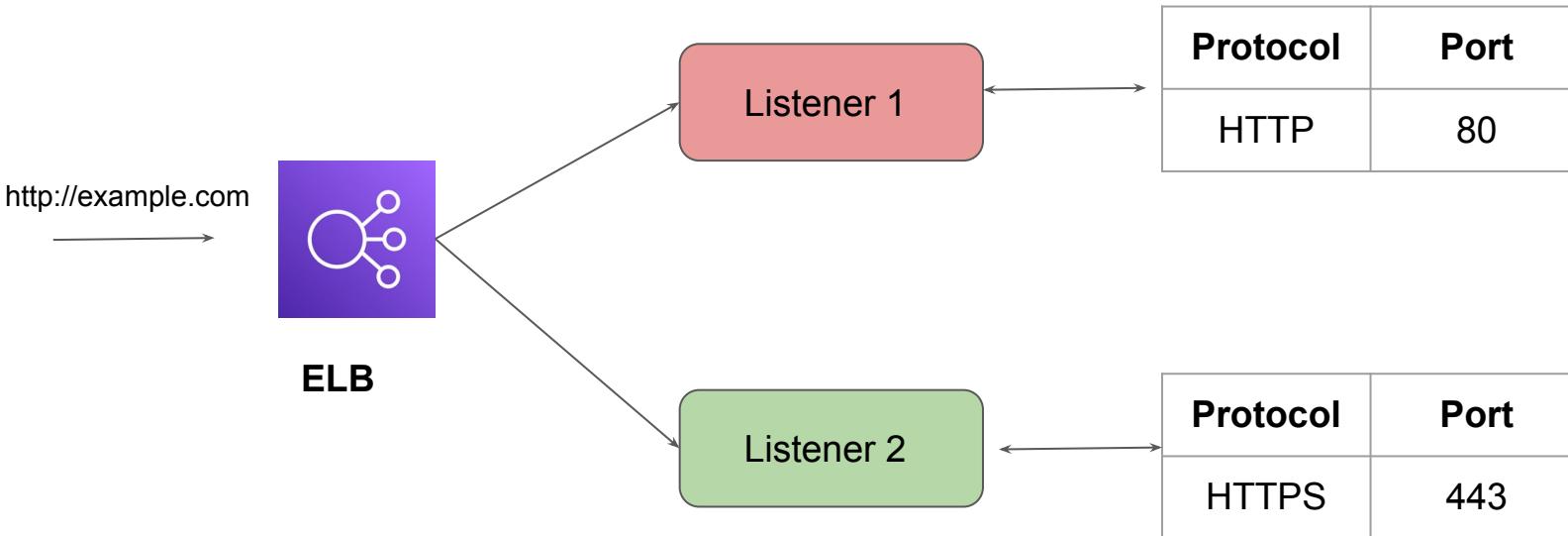
# Listener & Target Groups

Next generation load balancers

---

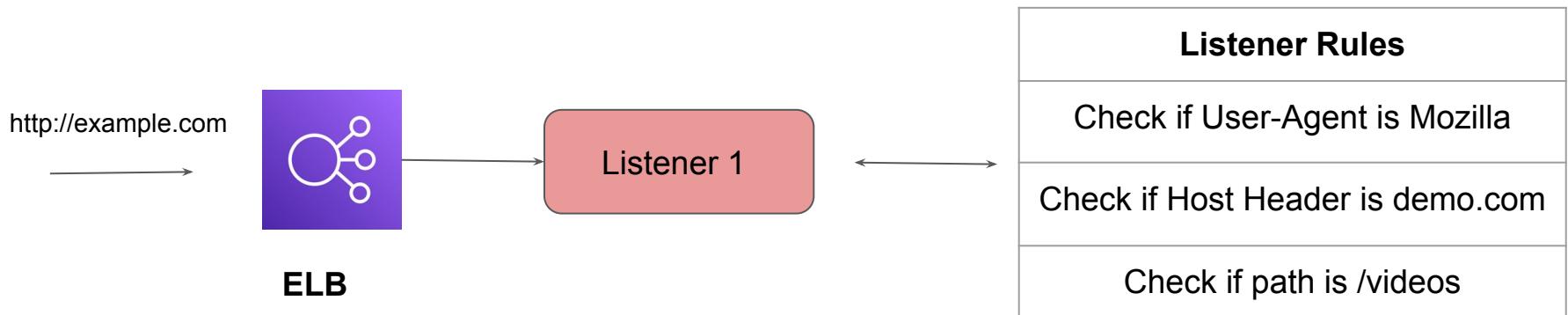
# Understanding Listeners

A **listener** is a process that checks for connection requests, using the protocol and port that you configure.



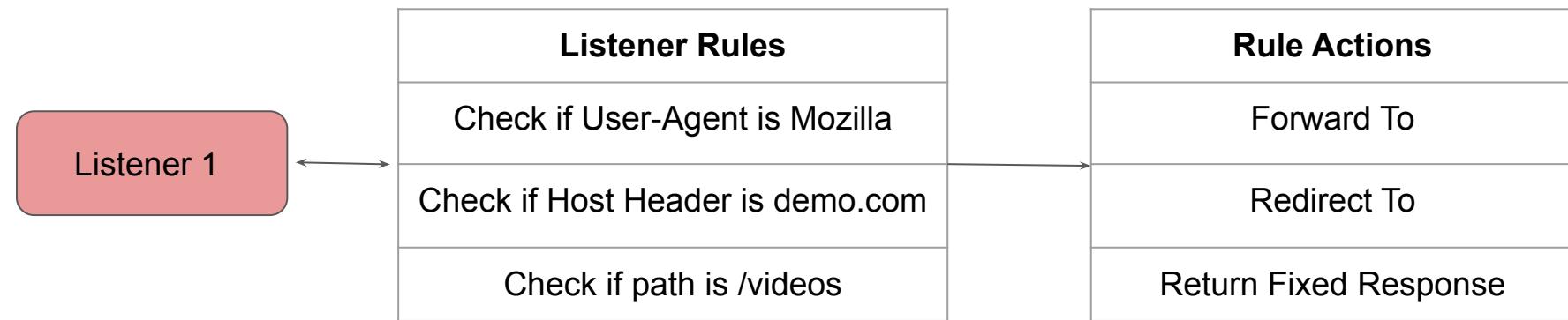
# Listener Rules

Each listener has a rule based on which an action is taken based on a request.



# Listener Rule Actions

If a request matches a specific rule, what action you want to perform on that request is determined in the Rule Actions.



## demo-alb | HTTP:80 (4 rules)

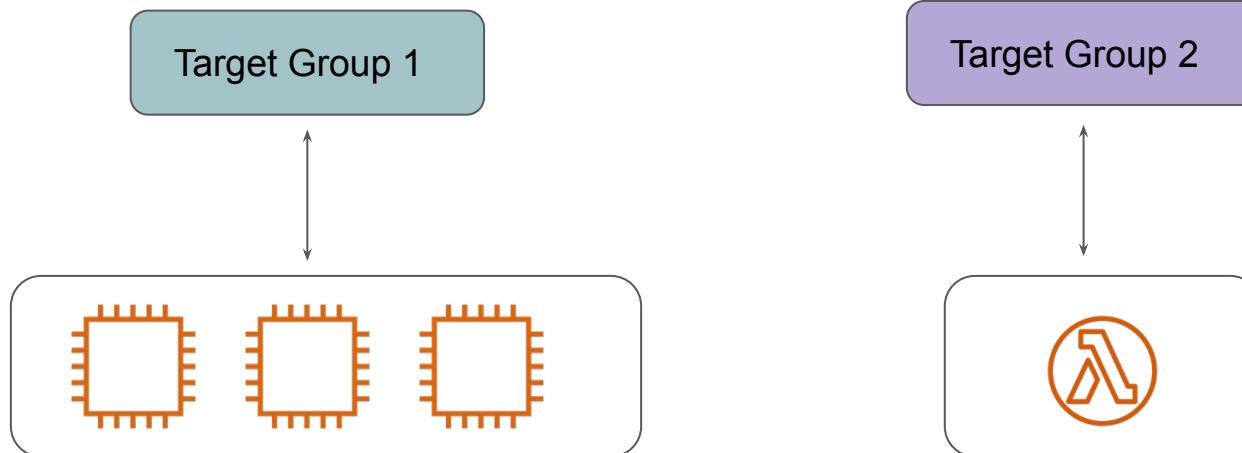
- ▶ Rule limits for condition values, wildcards, and total rules.

1 arn...93720 ▾	<b>IF</b> ✓ Http header User-Agent is *curl*	<b>THEN</b> <b>Return fixed response</b> 200 Content-Type: text/plain Response body: Hi curl! <a href="#">(less...)</a>
2 arn...c9bc6 ▾	<b>IF</b> ✓ Http header User-Agent is *Mozilla*	<b>THEN</b> <b>Return fixed response</b> 200 Content-Type: text/plain Response body: Hey Mozilla! You have great addons! <a href="#">(less...)</a>
3 arn...fdb85 ▾	<b>IF</b> ✓ Http header User-Agent is *wget*	<b>THEN</b> <b>Return fixed response</b> 200 Content-Type: text/plain Response body: Hi There wget! I detected you. <a href="#">(less...)</a>

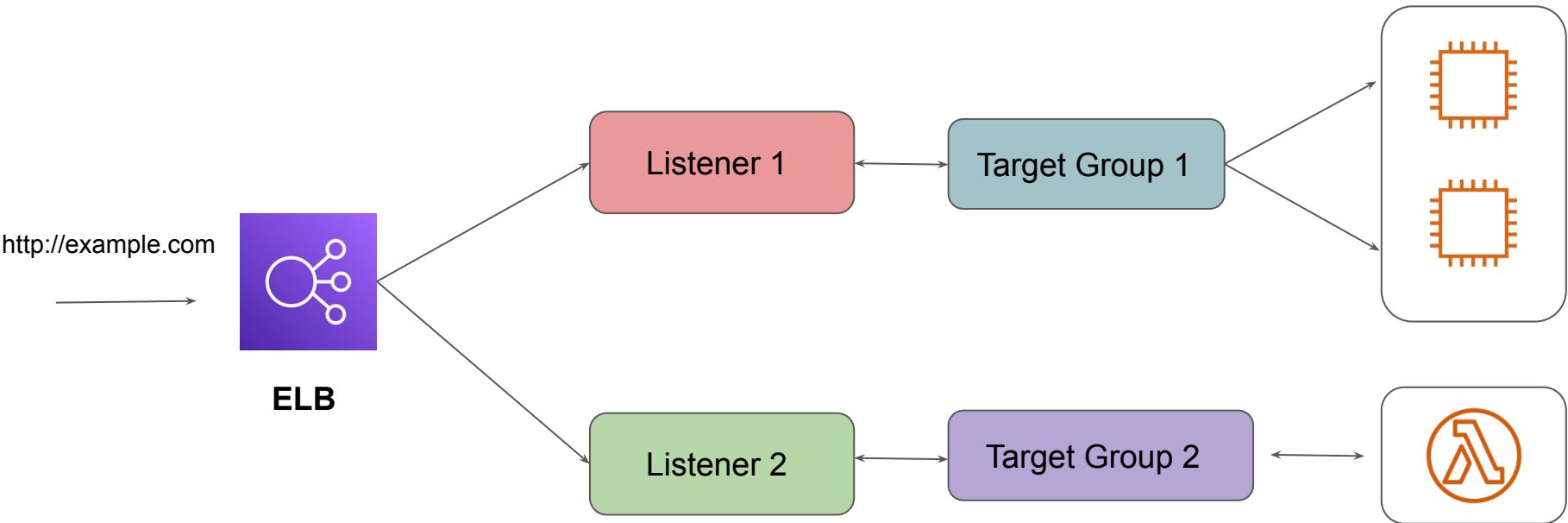
# Understanding Target Groups

Target group is used to route requests to one or more registered targets.

These targets can be EC2 instances, Lambda Functions, and others.



# Overall Workflow



---

# Network Load Balancers

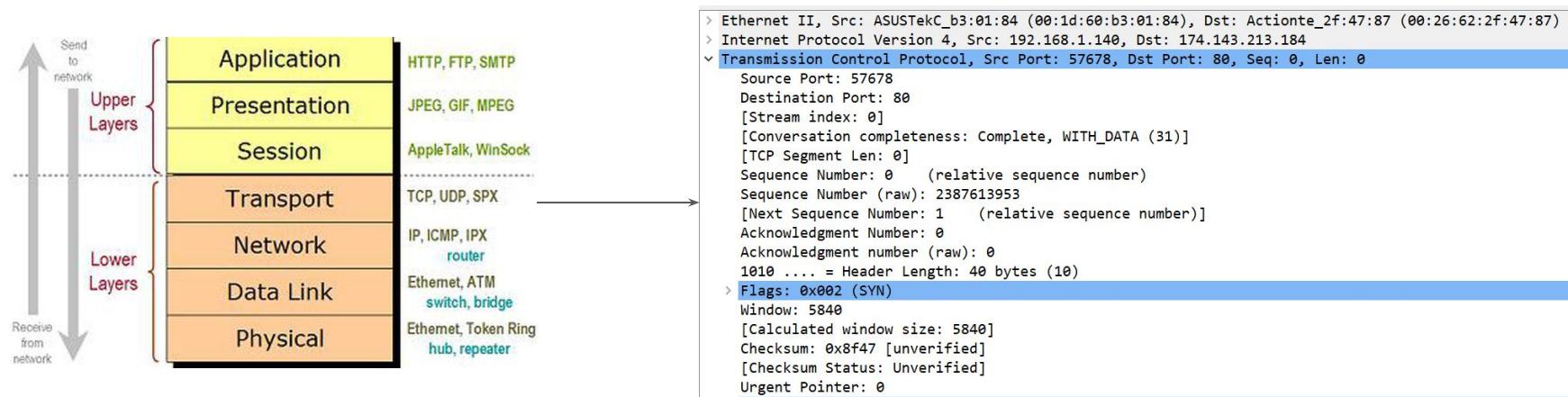
Next generation load balancers

---

# Understanding NLB

Network Load Balancer works on the fourth layer of the OSI model.

It can handle millions of requests per second.



# Basic Working

NLB primarily selects a target using a **flow hash algorithm** based on:

Protocol, Source IP address, Source port, Destination IP address, Destination port, and TCP sequence number.

Each individual TCP connection is routed to a single target for the life of the connection.

---

# Availability Zones and ELB nodes

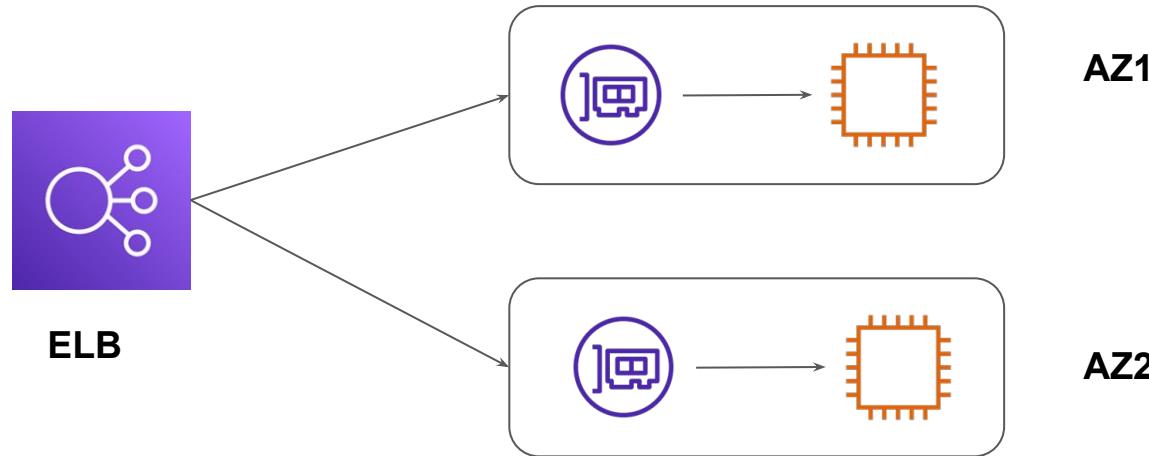
ELB Interfaces

---

# Availability Zones and ELB nodes

When you enable an Availability Zone for your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone.

If you register targets in an Availability Zone but do not enable the Availability Zone, these registered targets do not receive traffic.



# Recommendations

With an Application Load Balancer, it is a requirement that you enable at least two or more Availability Zones. If one Availability Zone becomes unavailable or has no healthy targets, the load balancer can route traffic to the healthy targets in another Availability Zone.

After you disable an Availability Zone, the targets in that Availability Zone remain registered with the load balancer. However, even though they remain registered, the load balancer does not route traffic to them.

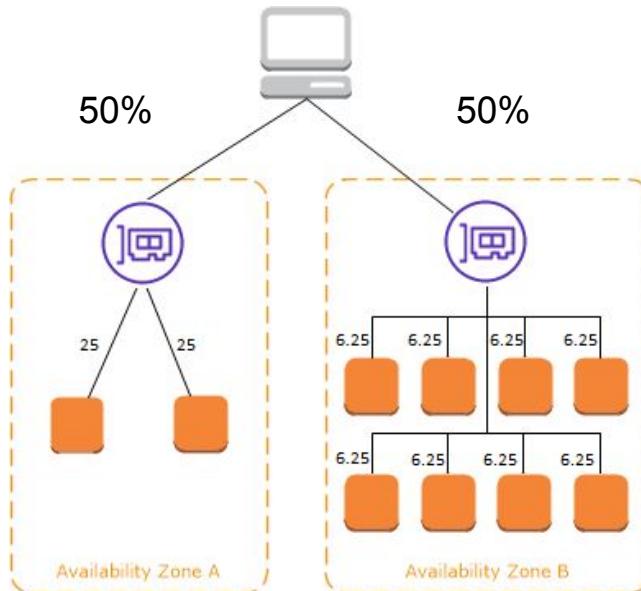
---

# Cross Zone Load Balancing

Interesting Learning

# Understanding the Challenge

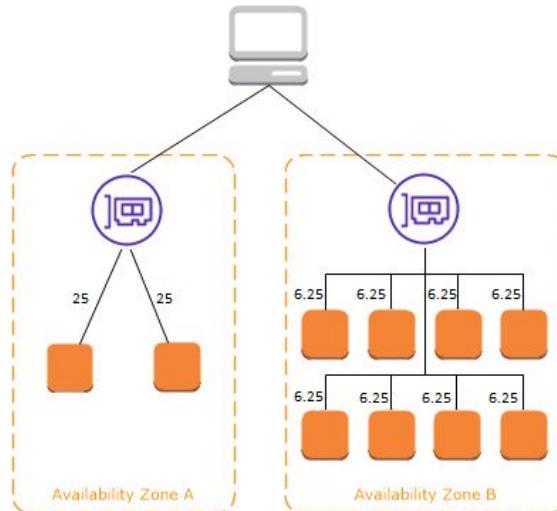
If Cross Zone Load Balancing is disabled, each load balancer node distributes traffic only across the registered targets in its Availability Zone.



# Cross Zone Load Balancing Disabled

Each of the two targets in Availability Zone A receives 25% of the traffic.

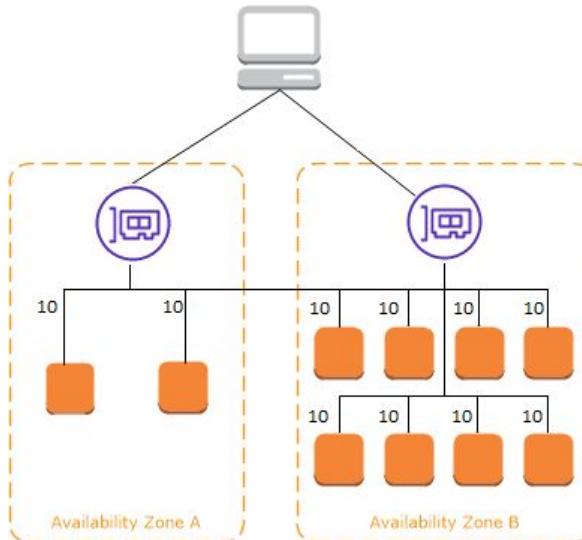
Each of the eight targets in Availability Zone B receives 6.25% of the traffic.



# Cross Zone Load Balancing

When cross-zone load balancing is enabled, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones.

If cross-zone load balancing is enabled, each of the 10 targets receives 10% of the traffic.



# Important Pointers

With Application Load Balancers, cross-zone load balancing is always enabled.

With Network Load Balancers and Gateway Load Balancers, cross-zone load balancing is disabled by default. After you create the load balancer, you can enable or disable cross-zone load balancing at any time.

---

# ELB Access Logs

Who is Visiting Us?

---

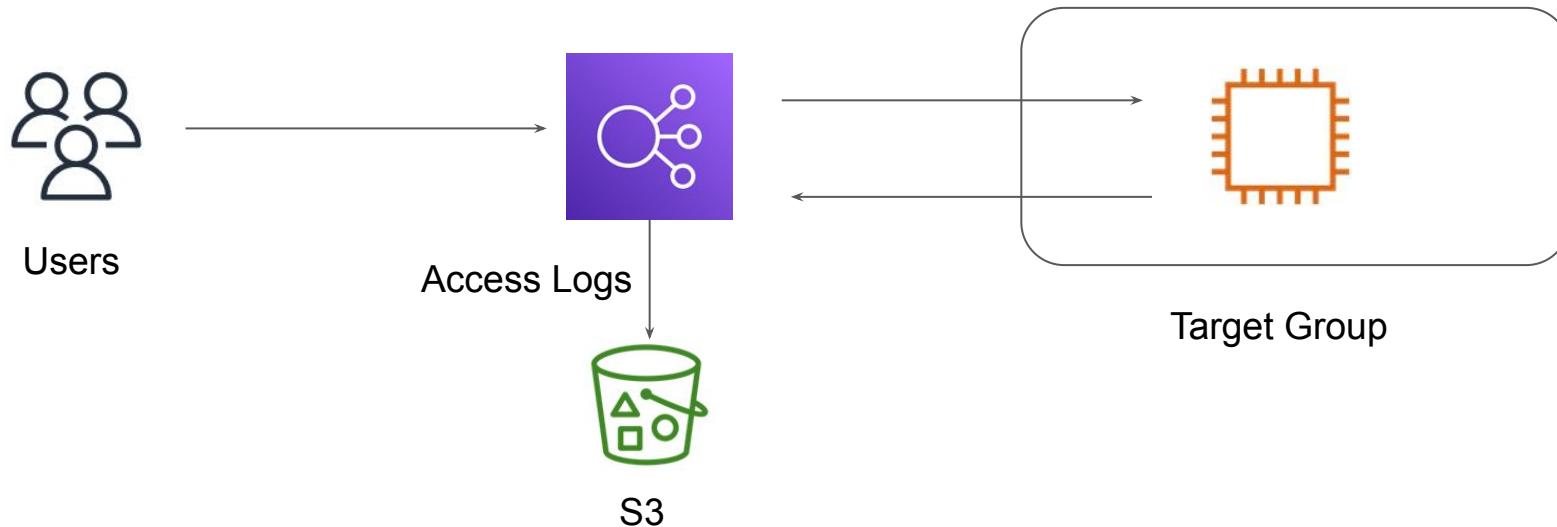
# Overview of Access Logs

An access log is a list of all the requests for individual files that people have requested from a Web site

```
[root@ip-172-26-7-135 nginx]# tail -f access.log
128.14.133.58 - - [03/Sep/2021:04:43:10 +0000] "GET / HTTP/1.1" 200 82 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" "-"
104.149.165.66 - - [03/Sep/2021:04:45:03 +0000] "HEAD /robots.txt HTTP/1.0" 404 0 "-" "-" "-"
92.118.160.57 - - [03/Sep/2021:05:02:42 +0000] "GET / HTTP/1.0" 200 82 "-" "NetSystemsResearch studies the availability of various services across the internet. Our website is netsystemsresearch.com" "-"
114.119.154.115 - - [03/Sep/2021:05:05:14 +0000] "GET /topic/blockchain/ HTTP/1.1" 404 153 "-" "Mozilla/5.0 (Linux; Android 7.0;) AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible; PetalBot;+https://webmaster.petalsearch.com/site/petalbot)" "-"
135.125.244.48 - - [03/Sep/2021:05:11:08 +0000] "POST / HTTP/1.1" 405 559 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"
135.125.244.48 - - [03/Sep/2021:05:11:08 +0000] "GET /.env HTTP/1.1" 404 555 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"
109.49.235.11 - - [03/Sep/2021:05:12:32 +0000] "GET / HTTP/1.1" 200 82 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" "-"
185.53.90.24 - - [03/Sep/2021:05:20:55 +0000] "GET http://icanhazip.com/ HTTP/1.1" 200 82 "-" "Go-http-client/1.1" "-"
114.119.154.11 - - [03/Sep/2021:05:28:51 +0000] "GET /topic/graphic-design/ HTTP/1.1" 404 153 "-" "Mozilla/5.0 (Linux; Android 7.0;) AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible; PetalBot;+https://webmaster.petalsearch.com/site/petalbot)" "-"
199.168.150.161 - - [03/Sep/2021:05:39:07 +0000] "GET / HTTP/1.1" 302 145 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" "-"
```

# ELB Access Logs

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer.



# Important Pointers for Access Logs - Part 1

Access logging is an optional feature of Elastic Load Balancing that is disabled by default

Elastic Load Balancing logs requests on a best-effort basis. AWS recommend that you use access logs to understand the nature of the requests, not as a complete accounting of all requests.

# Important Pointers for Access Logs - Part 2

The bucket and your load balancer must be in the same Region.

Bucket Policy should be designed so that AWS Account must be able to write to your bucket.

Elastic Load Balancing publishes a log file for each load balancer node every 5 minutes.

# Relax and Have a Meme Before Proceeding



**alcohol**  
@Mandac5

What is an extreme sport?



**allison**  
@amazaleax

Doing your homework while the  
teacher is collecting it

---

# Dualstack IP Address Type for ELBs

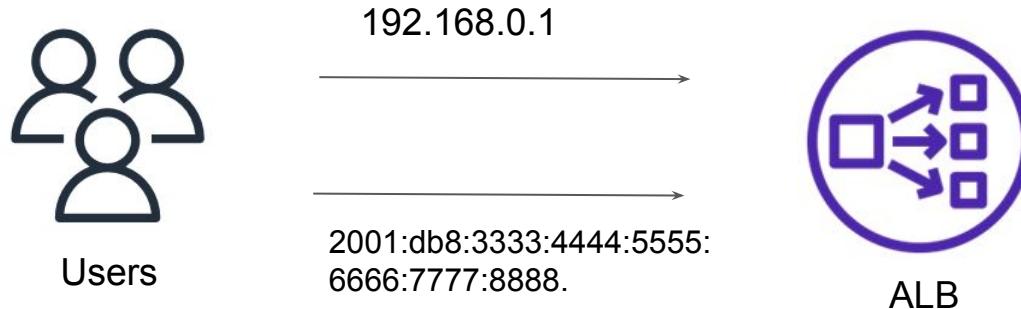
Enable IPv6 for ELBs

---

# IP Address Type Support

ELB Supports two address types:

- i) IPv4
- ii) Dualstack (includes both IPv4 and IPv6 addresses)



# Important Pointer

To use IPv6 addresses, the virtual private cloud (VPC) where you launch your ELB must have subnets with associated IPv6 CIDR blocks

IPv6 addresses can be associated only with internet-facing Application Load Balancers and Network Load Balancers.

Internal Application Load Balancers, Classic Load Balancers, and Network Load Balancers do not support IPv6 addresses.

---

# Sticky Sessions

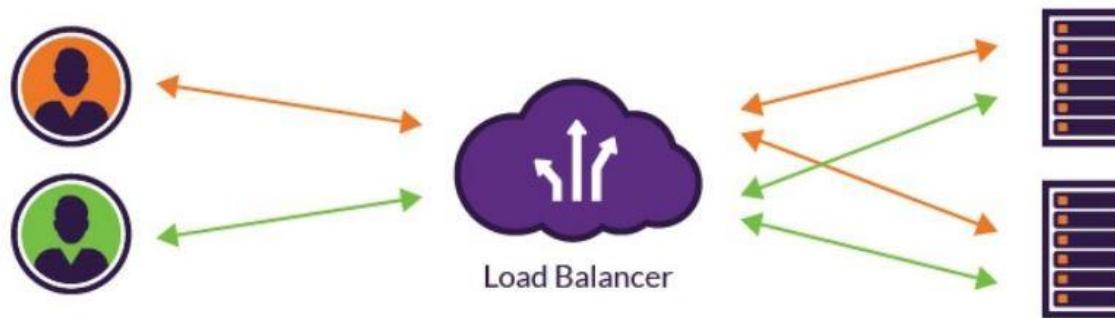
Direct Users to the Same Server

---

# Understanding the Challenge

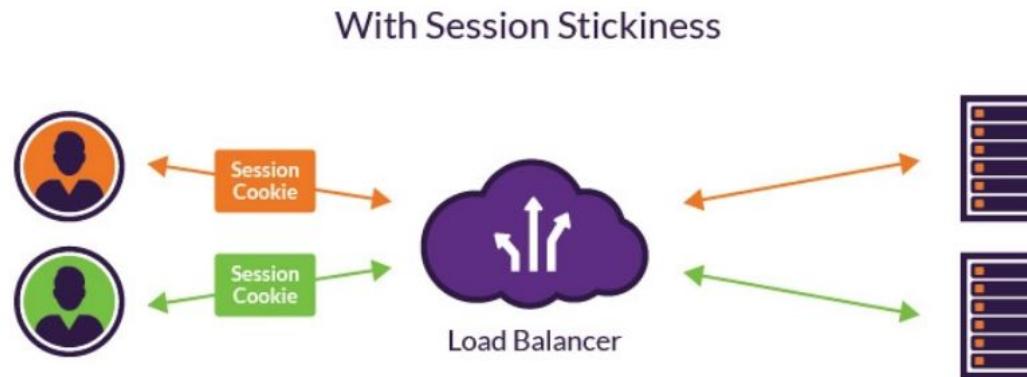
Generally the Load Balancers will distribute the traffic from the users to the backend servers via the round robin algorithm.

If subsequent requests are routed to different servers, your session state information is lost.



# Importance of Sticky Session

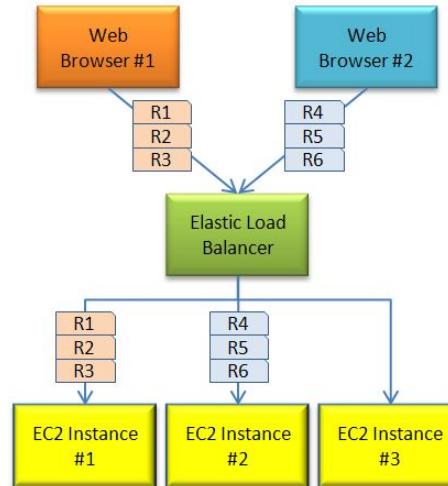
Sticky session refers to the feature of many commercial load balancing solution to route the requests for a particular session to the same physical machine that serviced the first request for that session.



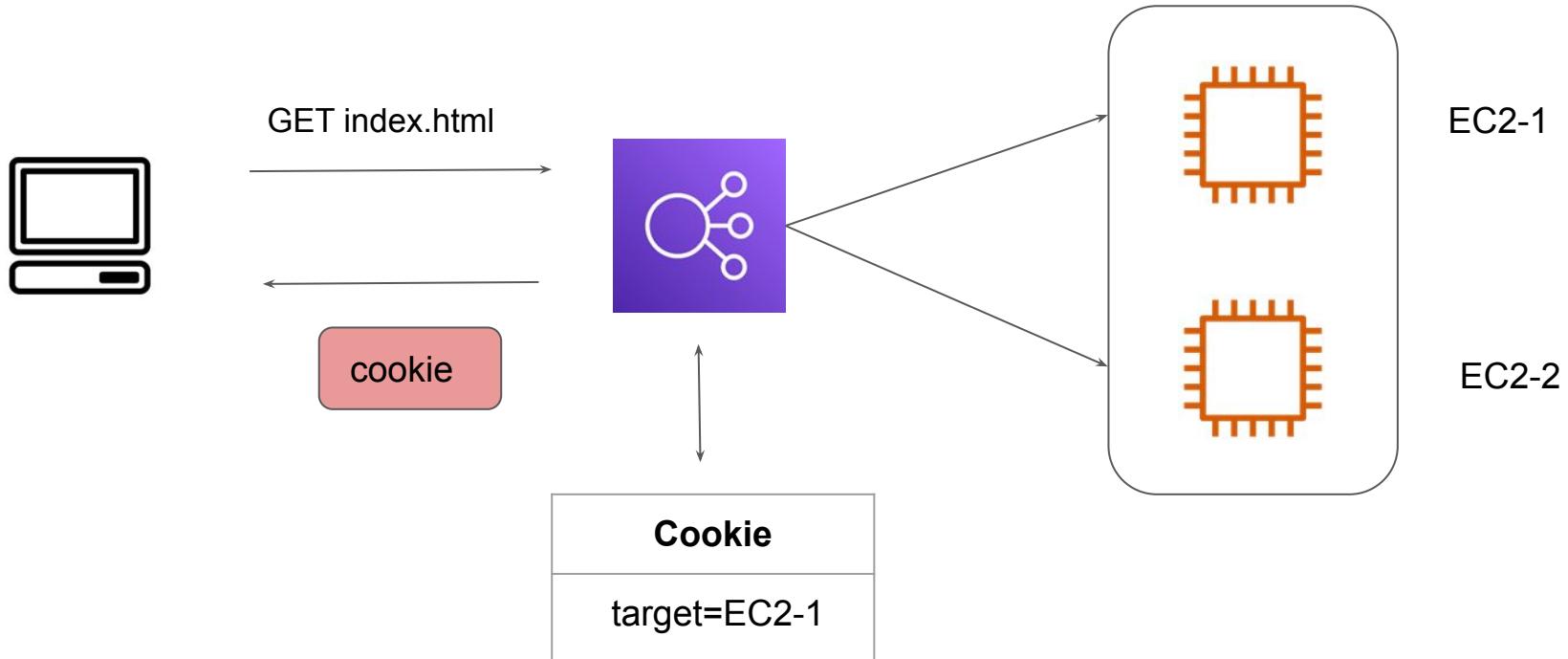
# Sticky Session and AWS Load Balancers

By default, an Application Load Balancer routes each request independently to a registered target based on the chosen load-balancing algorithm.

However, you can use the sticky session feature to enable the load balancer to bind a user's session to a specific target



# Overview of the Workflow



# Advantages of Sticky Sessions

When sticky sessions are used, the servers do not need to exchange the sessions data which can minimize the data transfers.

Sticky Sessions can also allow better utilization of your RAM Cache that leads to better responsiveness

# Disadvantage of Sticky Sessions

With sticky sessions, the overall balancing of traffic between servers can be affected.

A server can become overloaded if it accumulates too many sessions, or if specific sticky sessions require a high number of resources.

# Duration Based Stickiness

When a load balancer first receives a request from a client, it routes the request to a target (based on the chosen algorithm), and generates a cookie named AWSALB.

It encodes information about the selected target, and includes the cookie in the response to the client

In subsequent requests, the client should include the AWSALB cookie. When the load balancer receives a request from a client that contains the cookie, it detects it and routes the request to the same target

# Application Based Stickiness

The target is expected to set a custom application cookie.

When the ALB receives the custom application cookie from the target, it automatically generates a new encrypted application cookie to capture stickiness information.

The load balancer generated application cookie does not copy the attributes of the custom cookie set by the target. It has its own expiry of 7 days which is non-configurable

---

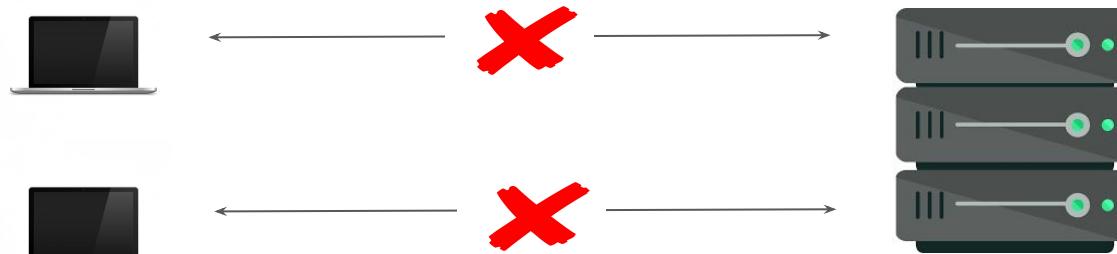
# Connection Draining in ELB

## Load Balancer Configurations

# Understanding the Challenge

In the process of using ELB, it might happen you might want to deregister the instance from load balancer to perform some updates or patching activities.

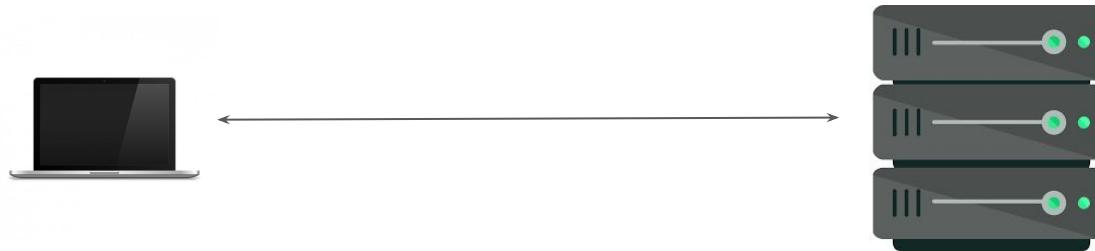
If we immediately deregister the EC2 instance, then all the existing connections would be blocked.



# Understanding Deregistration Delay

In order to handle this scenario, ELB has a feature called connection draining which allows the existing connections to complete before EC2 gets deregistered. This is a configurable value.

By default, ELB waits for 300 seconds before completing deregistration process.



---

# Capturing Client IP via ELB

ELB Networking!

---

# Capturing Client IP in ELB

Depending on type of ELB and Listeners, the approach in which Client IP is captured changes.



# Important Pointers to Remember

Sr No	Load Balancer Type	Description
1	Classic Load Balancer	<p>For HTTP based listeners, Client IP is forwarded by default to the servers.</p> <p>For TCP based listeners, Proxy Protocol needs to be enabled.</p>
2	Application Load Balancer	Client IP is passed with the request. Use X-Forwarded-For headers in application to capture the client address.
3	Network Load Balancer	<p>If target specified with instance-id, the source IP addresses of clients are preserved.</p> <p>If specified via IP address, Proxy Protocol needs to be enabled.</p>

---

# Selection of Cipher Suites

Cipher Suites for SSL/TLS Connection

---

# Understanding Cipher Suite Selection Option

AWS offers wide range of cipher suite options which can be selected by the customers.

These cipher suites can be selected for various services like:

- Elastic Load Balancing
- Amazon CloudFront
- Application Load Balancer

It is always recommended to make use of the most recent cipher suites.

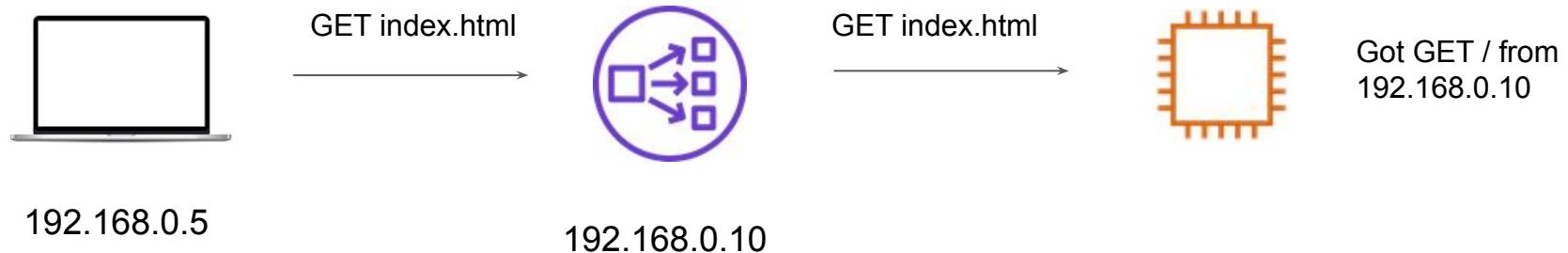
---

# X-Forwarded-For Header

## HTTP Headers

# Let's Understand the Challenge

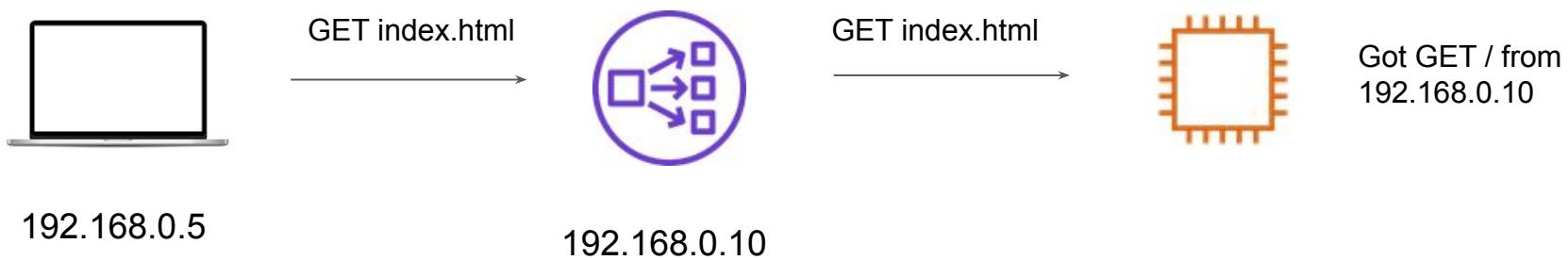
Whenever using a Reverse Proxy or Load Balancer, the client IP address remains hidden from the backend application.



# Sample Use-Case

There is a promotion ongoing and every IP address is required to make only 1 call to the app.

Since App is not receiving Client IP, it becomes difficult for it to implement the logic.



# Ideal Way of Doing Things

You might want to configure the Reverse Proxy / Load Balancer in a manner that it forwards the Client IP Address to the backend application servers.



# X-Forwarded-For Header

The X-Forwarded-For (XFF) HTTP header field is a common method for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.

Generic format is:      X-Forwarded-For: client, proxy1, proxy2

X-Forwarded-For: 203.0.113.195, 70.41.3.18, 150.172.238.178



---

# DHCP

Yay Protocols

---

# Understanding Basics

When client joins a network, it does not really have any IP address.

It sends a broadcast request all over the network asking for the IP address.

The DHCP server will offer an IP address that the newly joined client can use. There can be multiple DHCP servers offering different IP address.

The client will decide the IP it wants to have, and will send the DHCP request so that all the DHCP servers know which it would like to have.

The DHCP server will see if that address is still available and if yes, it will send DHCP ACK back to the client.

---

# DHCP Option Sets

Let's Control DHCP Features

---

# Revising the Basics

DHCP settings allows us to control multiple things, these include:

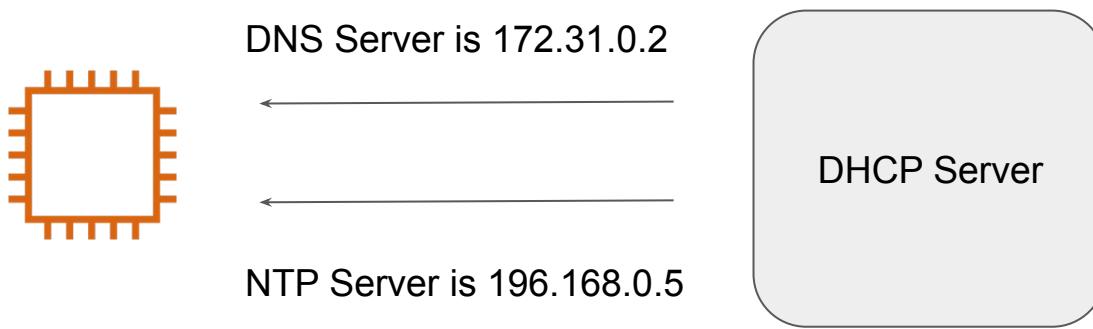
DNS Settings, Maximum Number of Users, IP Range and so on.

DHCP Server Setting	
<input checked="" type="checkbox"/> DHCP Server	<b>DHCP Reservation</b>
Start IP Address	192.168.1.100
Maximum Number of Users	50
IP Address Range	192.168.1.100 to 149
Client Lease Time	0 minutes (0 means one day)
Static DNS 1	0.0.0.0
Static DNS 2	0.0.0.0
Static DNS 3	0.0.0.0
WINS	0.0.0.0

# DHCP and AWS

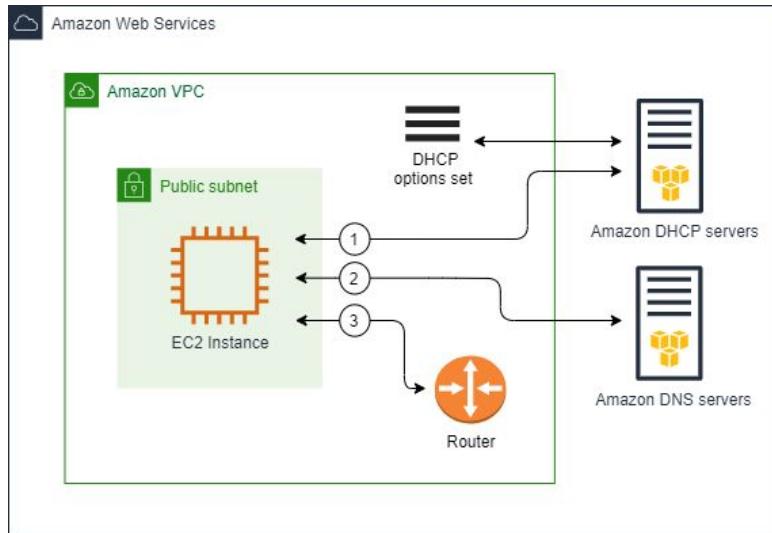
Network devices in your VPC makes use of DHCP.

EC2 instances in subnets can communicate with Amazon DHCP servers as needed to retrieve their IP address lease or other network configuration information (such as the IP address of an Amazon DNS server or the IP address of the router in your VPC).



# DHCP Option Sets

A DHCP option sets allows us to configure certain configuration associated with the Amazon DHCP server.



# Control using DHCP Option Sets

You can control the DNS servers, domain names, or Network Time Protocol (NTP) servers used by the devices in your VPC.

You can disable DNS resolution completely in your VPC.

**DHCP option**  
Specify at least one configuration parameter.

Domain name [Info](#)

Domain name servers [Info](#)  
  
Enter up to four IPv4 addresses and four IPv6 addresses, separated by commas.

NTP servers  
  
Enter up to four IPv4 addresses and four IPv6 addresses, separated by commas.

NetBIOS name servers  
  
Enter up to four IP addresses, separated by commas.

NetBIOS node type  
  
▼  
We recommend that you select point-to-point (2 - P-node). Broadcast and multicast are not currently supported.

---

# Encapsulation

Networking all the way :)

---

# Encapsulation the easy way

Recently I sent a letter via courier from Bangalore to Mumbai.

## Steps Involved:

- Write a message in piece of paper which you want to send.
- Encapsulate it in an envelope.
- Write the source and destination address on top of envelope.



# Understanding Encapsulation

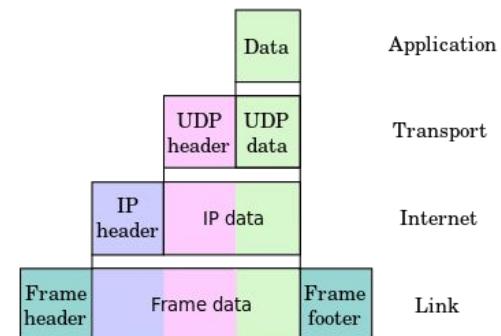
Application A (source 1) wants to send data to Application B (source 2)

Few questions:

Does it want reliable protocols like TCP ?

If TCP, what are the port number of source destination application ?

What is the IP address of destination server ?

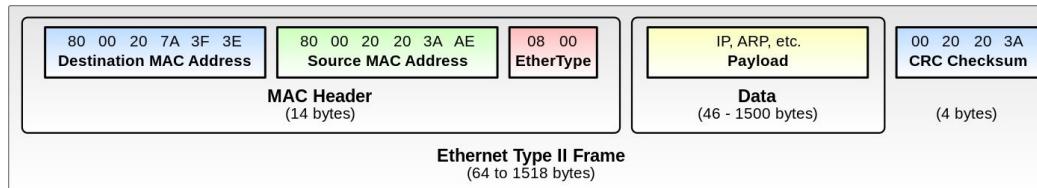


# Encapsulation also increases the size

Application A wants to send 10 bytes of data to Application B via TCP protocol.

Let's look into the overall overhead:

- Data : 10 bytes
- TCP header: 20 bytes
- IP header : 20 bytes
- Ethernet Header: 14 bytes



---

# TCP Protocol

Let's start protocols

# Let's understand in simple manner

Whenever we want to communicate with someone, we begin with maybe “Hello” over the phone or Hi over chats.

Same thing applies during the end of communication with “Bye”.

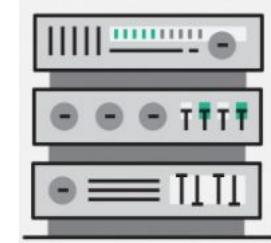
**Hello**



# TCP follows similar approach

In TCP protocol, there is a 3 way handshake that takes place before communication is established between two entities.

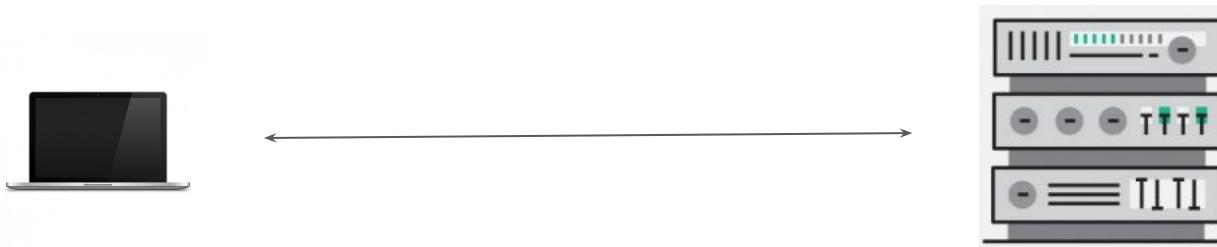
There is also a handshake which happens when communication is completed and connection needs to be closed.



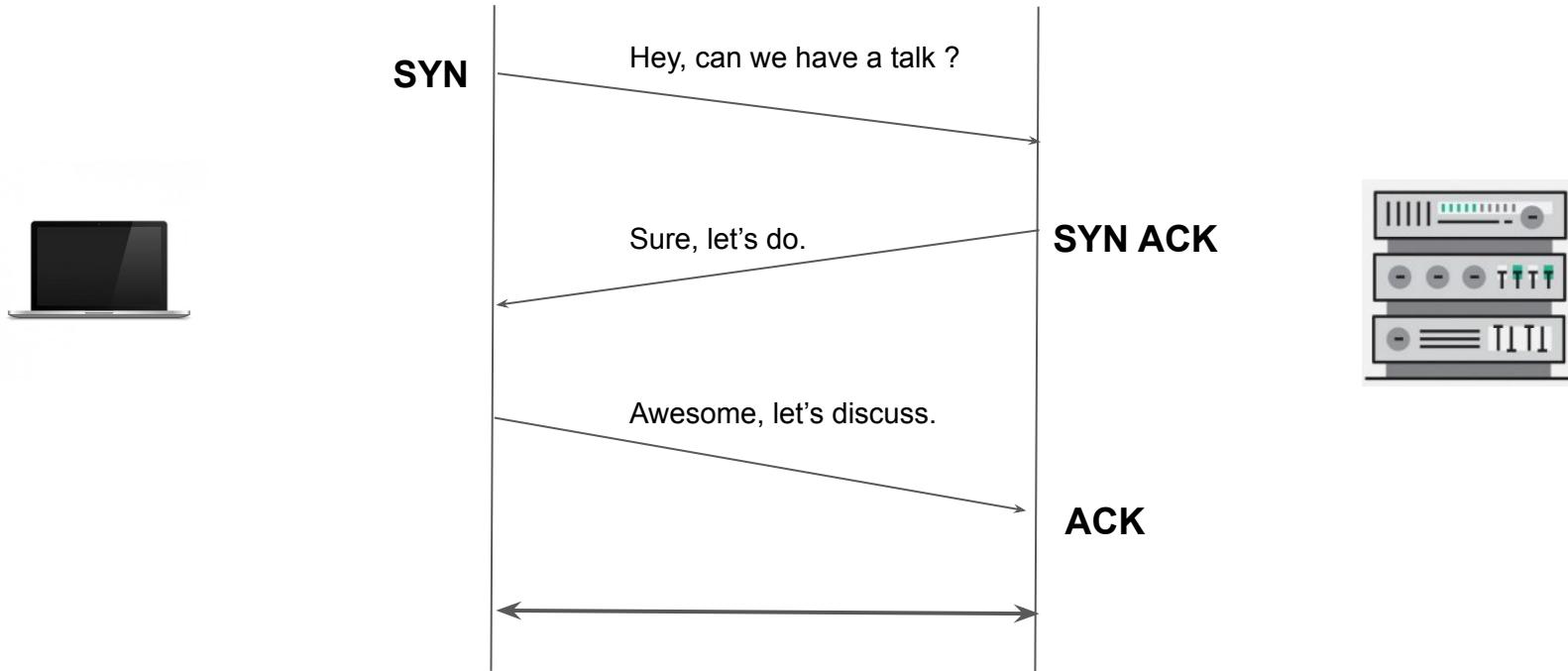
# Why TCP protocol at first place ?

TCP protocol allows two hosts to establish a connection and exchange streams of data.

TCP protocol is much more advanced, like it guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.



# TCP 3 way handshake



---

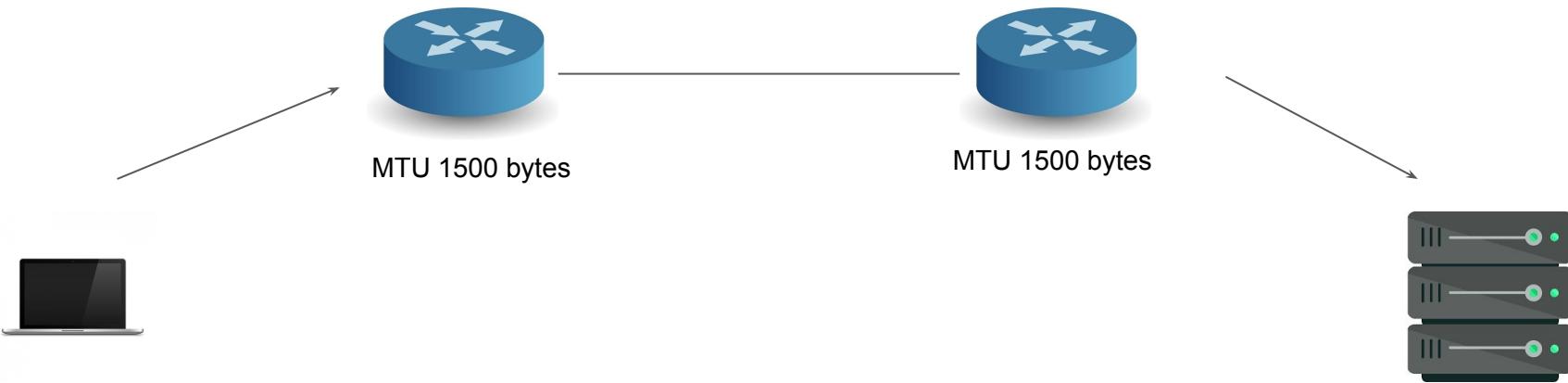
# MSS in TCP

Networking all the way :)

---

# Revising MTU

MTU is more related to maximum size of IP packet that can be sent over a single transaction over frame based networks like Internet.



# Understanding Maximum Segment Size

If the MTU is of 1500 bytes, it does not mean that we can send 1500 bytes of TCP data.

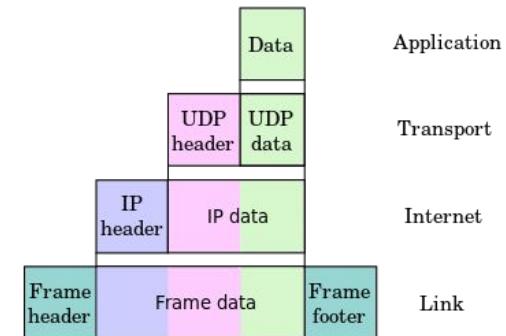
Remember the encapsulation process ?

MSS = Maximum data which can be sent in TCP protocol.

$MSS = MTU - \text{sizeof(TCPHDR)} - \text{sizeof(IPHDR)}$

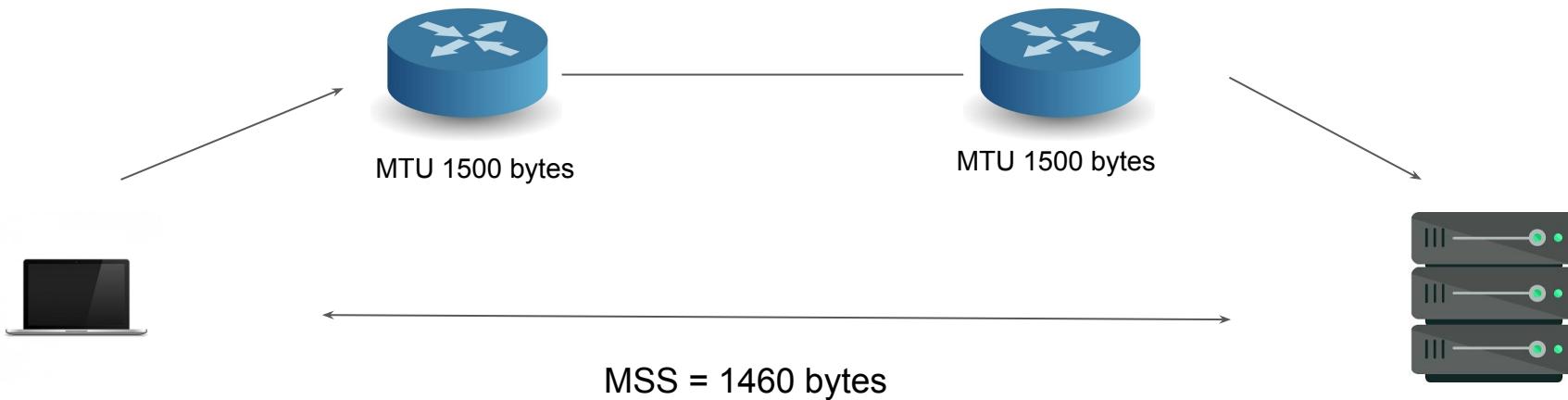
In generic scenario:

$MSS = MTU - 20 - 20 = MTU - 120$



# How is MSS calculated ?

During the TCP 3 way handshake, the MSS is defined by both the end of the communication regarding maximum value they can receive.



---

# IP Fragmentation

Networking all the way :)

---

# Understanding Maximum Segment Size

An IP packet that is larger than the MTU of the interface, is too large to be transmitted over that interface.

When the router receives a packet larger than MTU, there are two options:

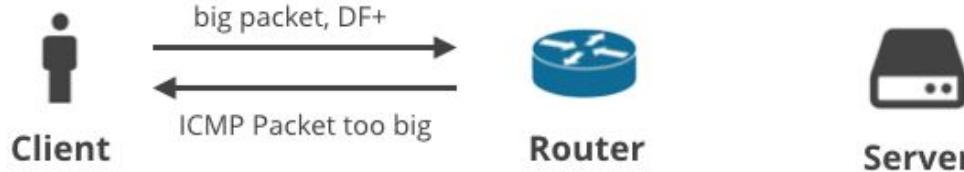
- i) Fragment the packet into smaller pieces and send it forward.
- ii) Discard the packet and send ICMP “packet too large” message.

# Understanding Maximum Segment Size

Case 1: Fragment the packet into smaller pieces and send it.



Case 2: Discard the packet and send ICMP “packet too large” message



---

# Numeric System

Maths again!

# Back to Olden times

Since the start of the days, we always have been looking into ways to keep track and count things for understanding.

Let's understand this with an example:

You are an early human and you want to keep track of the time it rained. So the day it did not rain, you write a symbol as I



# Number System for the Rescue

## Base 10 systems :

The number system that most of us are familiar with is the Base 10 number system, also called as the decimal. In decimal system, things are counted between 0 to 9

## Base 2 systems:

This is often called as binary system. This is the base of all the underlying computing systems. There are only two symbols: 0 and 1

192 equivalent to binary is 11000000

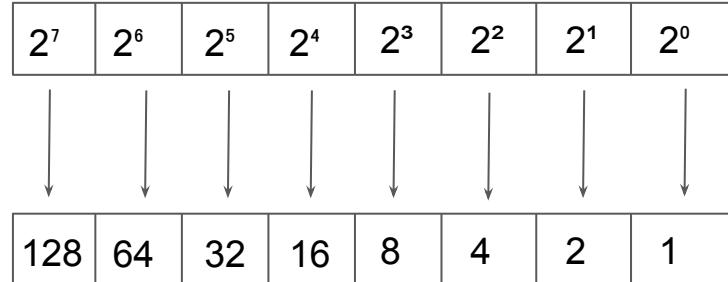
---

# Decimal to Binary

Maths again!

---

# Let's Convert



0	0	1	1	0	0	1	0
---	---	---	---	---	---	---	---

Represent 50

0	1	0	1	1	1	1	1
---	---	---	---	---	---	---	---

Represent 95

# IP addresses

IP Address : 172.31.32.50

Computer sees it as : 10101100.00011111.00100000.00110010

During the subnetting aspect, the knowledge of decimal and binary will prove to be important.



---

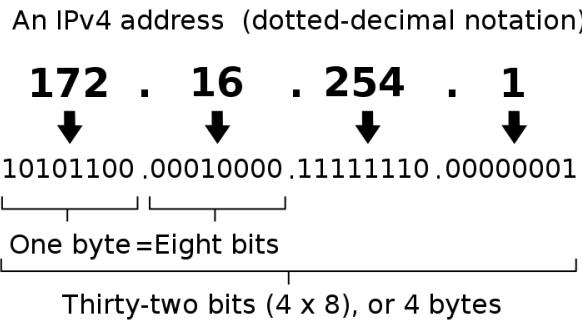
# IPV4 Addressing Scheme

IP Protocol

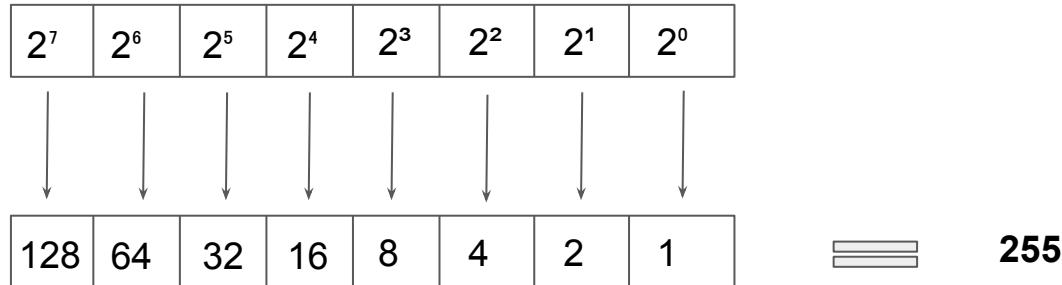
# Basic about IPV4 addressing scheme

An IPV4 protocol defines IP address as a 32-bit number

It is usually represented as dot-decimal notation consisting of four decimal numbers, each ranging from 0 to 255 separated by dots.



# Why maximum of 255 ?



1	1	1	1	1	1	1	1
---	---	---	---	---	---	---	---

---

# IPv6

It has begun!

---

# Let's start from beginning!

IPv4 has been our favourites (except the subnetting part!)

When IPv4 was designed, all these connected devices like mobile phones was basically like science fiction. Thus it does not address all the concerns of the modern age.

These limitations were addressed in IPv6 .

- IPv4 allows 4 billion IP addresses.
- IPV6 allows upto 340 trillion trillion addresses.

(340,282,366,920,938,463,463,374,607,431,768,211,456)

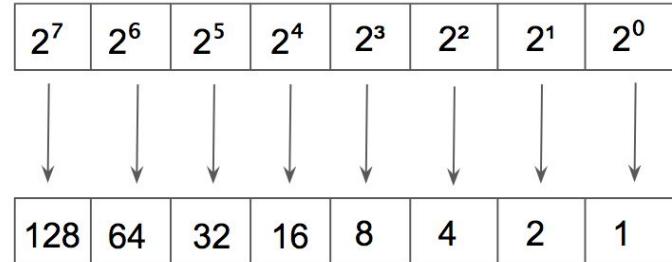
# IPv4

IPv4 address space is of 32 bits.

If we add just one bit to this (32+1), it will really make huge change.

Example:

If 32 bit has 2 million address, adding one extra bit will double the address space to 4 million

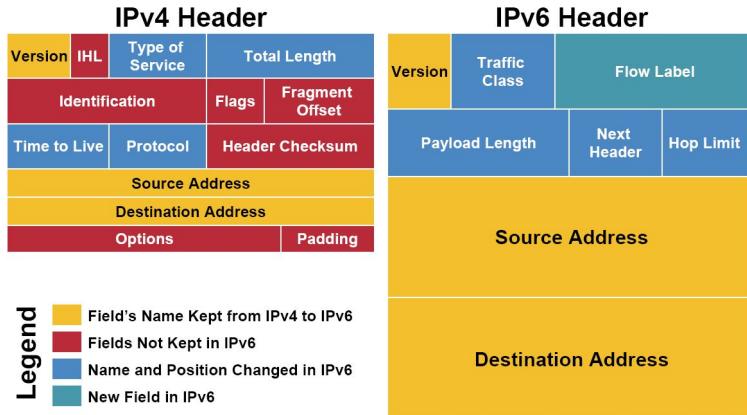


# IPv6

IPv6 address space is of 128 bits.

Because of the huge address space, NAT is no longer required for IPv6 generally.

IPv4 has lot of headers and even though header might not be in use, it still gets processed on every device which brings down the efficiency. IPv6 uses extension header approach.



# IPv6 Addressing

Here is 128 bit binary notation of IPv6 address

Sample IPv6 address: 2001:0db8:0000:0000:0000:0000:0000:0001

When an IPv6 address is written in hex notation, you have the flexibility to shorten the address considerably by reducing the number of zeros displayed.

2001:0db8:0000:0000:0000:0000:0001 --> 2001:db8::1

If you wonder how many 0's were there, you always know that there are 8 total blocks of numbers

# Changes with IPV6

With the introduction of IPv6, various commands and packages we use also changes:

ping → ping6

dhcp → dhcp6

icmp → icmpv6

More we will discuss in the relevant section.

---

# Egress-Only Internet Gateway

IPv6

---

# Understanding Egress-Only IGW

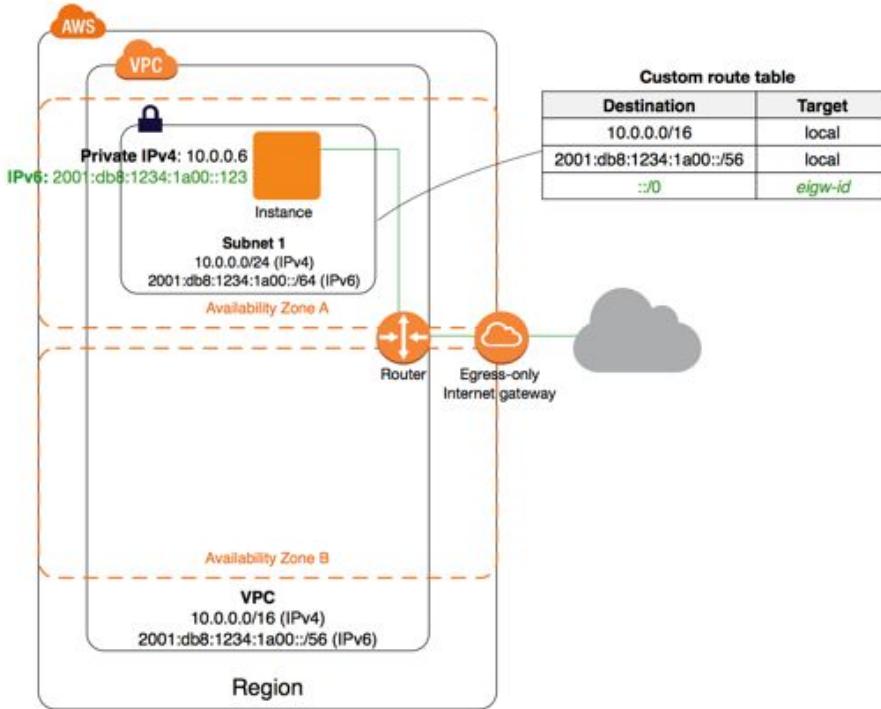
The IPv6 addresses which are assigned from AWS are public routable addresses.

Thus, instance in the public subnet can initiate connection to Internet via the Internet Gateway. Similarly resources from Internet can also initiate connection to the EC2 instance via it's public IPv4 or IPv6 addresses.

IPv6 addresses are globally unique, and are therefore public by default.

Egress-Only Gateway allows EC2 instance with IPv6 address to access internet directly but prevent resource from internet to directly initiate connection with the EC2 instance.

# Architecture for Egress-Only IGW



---

# IP Addr Reservation

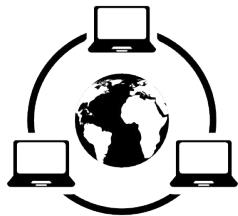
Networking again :)

# Introduction

By default, EC2 and VPC uses IPv4 addressing protocol.

Thus, when we create a VPC, we MUST assign a IPv4 CIDR block.

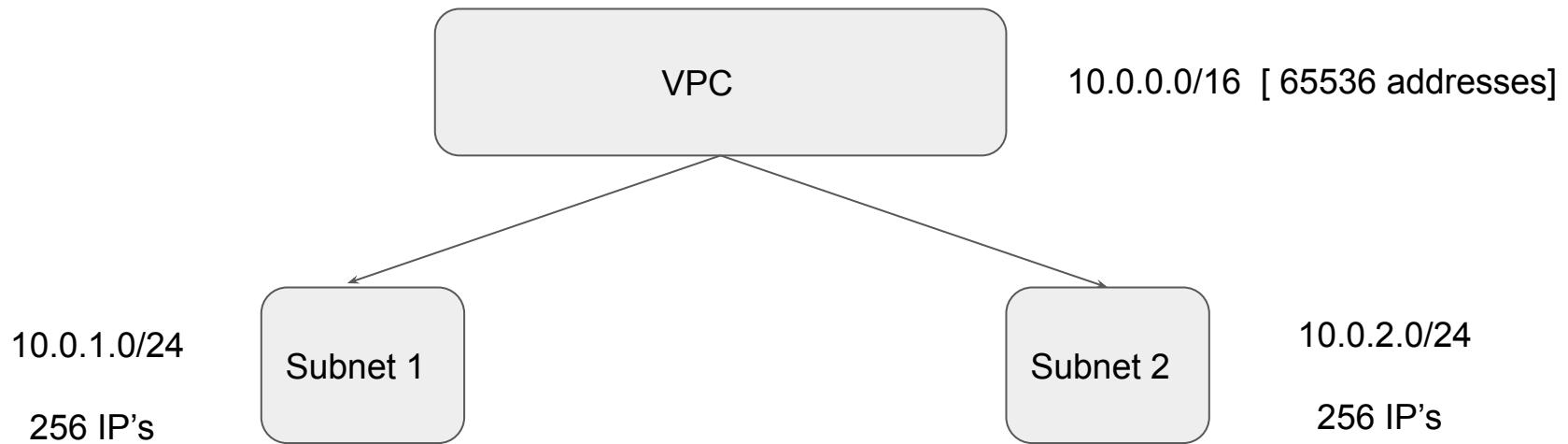
The IPv4 block must be between /16 to /28



# Let's do Subnet

When we specify /16, we can have maximum of 65,536 IP addresses.

When we specify /28, we can have maximum of 16 IP addresses.



# Reservation

The first four IP address and the last IP address in each subnet is not available for us to use and cannot be assigned to an instance.

Let's take an example:

For subnet block of 10.0.0.0/24, following five IP addresses are reserved:

- 10.0.0.0 - Network Address
- 10.0.0.1 - Reserved by AWS for VPC Router
- 10.0.0.2 - Reserved for AWS DNS.
- 10.0.0.3 - Reserved by AWS for future use.
- 10.0.0.255 - Network Broadcast. Since broadcast is not supported, this address is reserved.

# Important Pointers

- Understand minimum and maximum netmask [ /16 and /28 ]
- Know that 5 IP address in each subnet is reserved.
- IP address of subnet cannot overlap each other.



---

# Amazon Workspaces

## Virtual Remote Desktops

---

# Getting started

Amazon Workspaces is a managed, secure cloud desktop service.

Users can access the workspace from various clients like Chromebook, iPad, MAC, Windows and others.

We pay on the monthly or hourly basis for the workspace that we create.

---

# Network Requirement for Workspaces

Virtual Remote Desktops

---

# Important Pointers

Every workspace is provisioned with two network interfaces

The first NIC resides in customer VPC and second NIC is AWS Managed VPC.

This management VPC has one of the following CIDR:

- 172.31.0.0/16
- 192.168.0.0/16
- 192.19.0.0/16

The CIDR Is automatically chosen to not conflict with your VPC CIDR.

# Requirement for Workspaces

## 1. Virtual Private Cloud (VPC)

We need to have at-least two subnets for Workspace deployment because the directory services requires two subnets for Multi-AZ deployment.

## 2. Directory Service

Directory Service is required to authenticate the users and provide access to their workspaces. We can even use our own on-premise AD.

## 3. Security Group for Access Control

---

# Lambda@Edge

## Running Serverless at the Edge

---

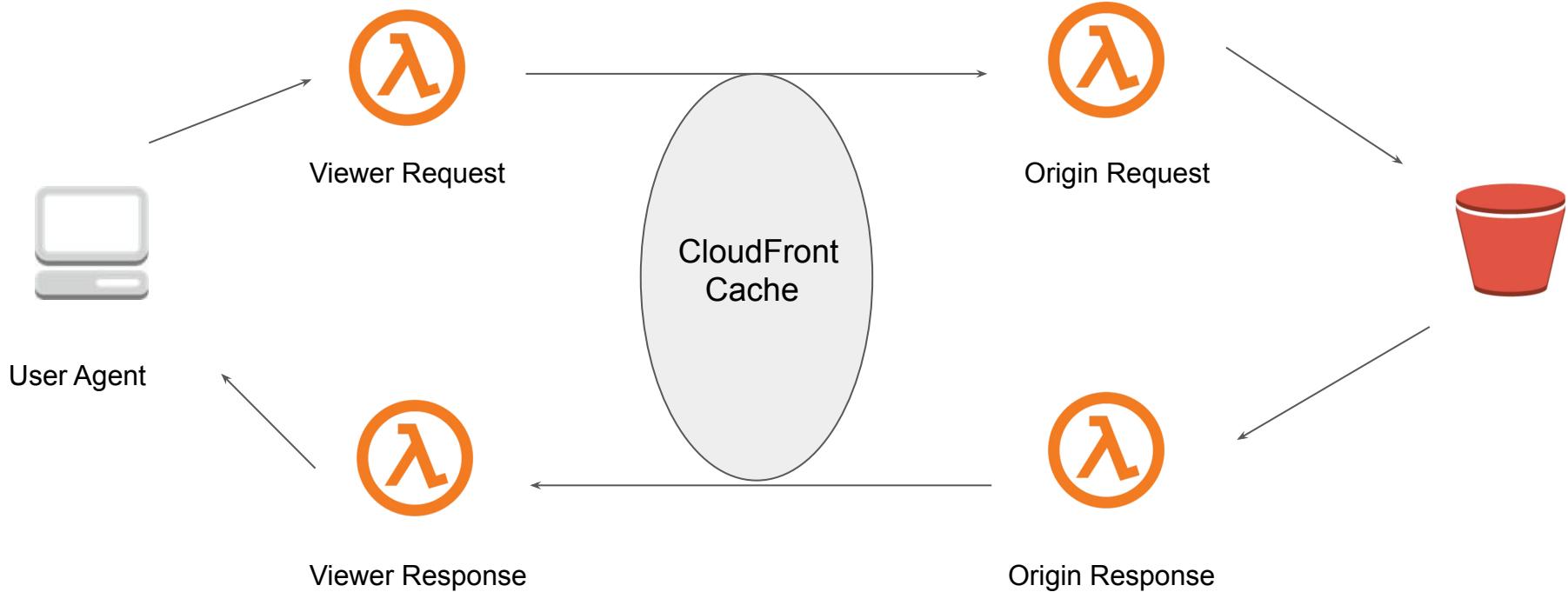
# Getting started

Lambda@Edge lets you run Lambda functions to customize content that CloudFront delivers.

You can use Lambda functions to change CloudFront requests and responses at the following points:

1. After CloudFront receives a request from a viewer ([viewer request](#))
2. Before CloudFront forwards the request to the origin ([origin request](#))
3. After CloudFront receives the response from the origin ([origin response](#))
4. Before CloudFront forwards the response to the viewer ([viewer response](#))

# Diagrammatic Representation



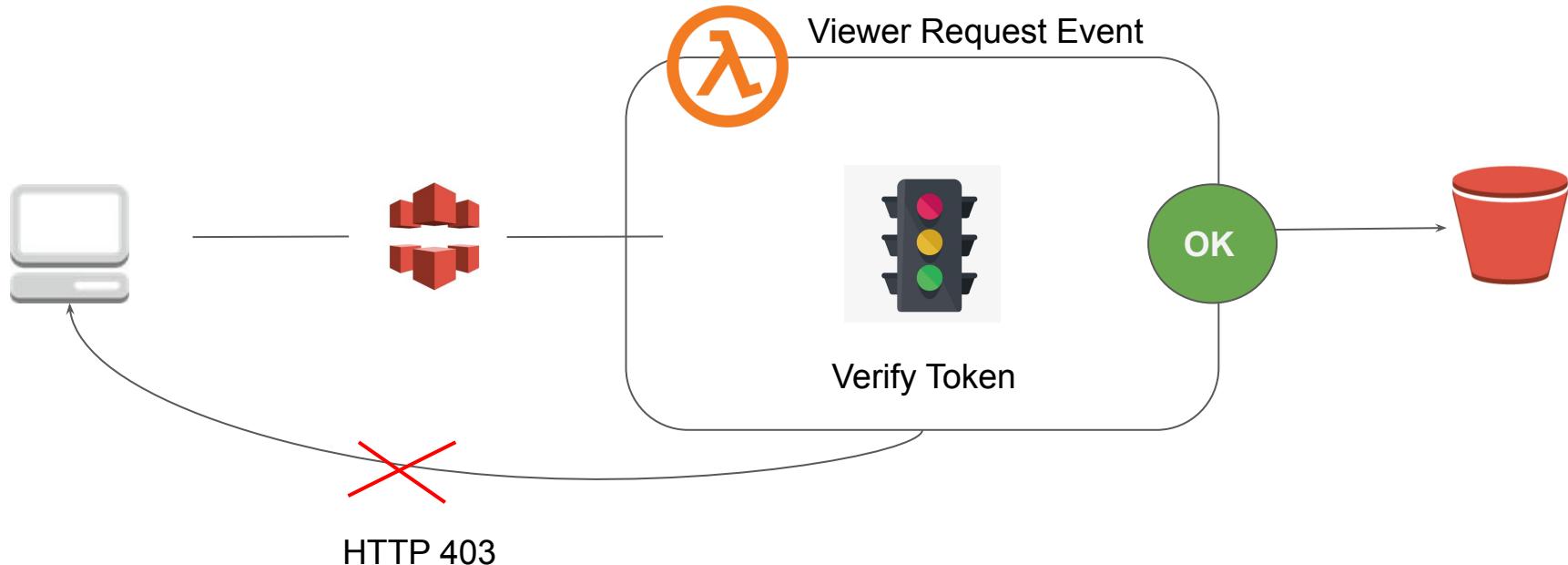
# Viewer Request

Viewer Request is executed on every request before CloudFront cache is checked.

There are various things that we can do at this stage, like:

- Modify URLs, cookies query strings etc.
- Perform Authentication and Authorization Checks.

# Viewer Request



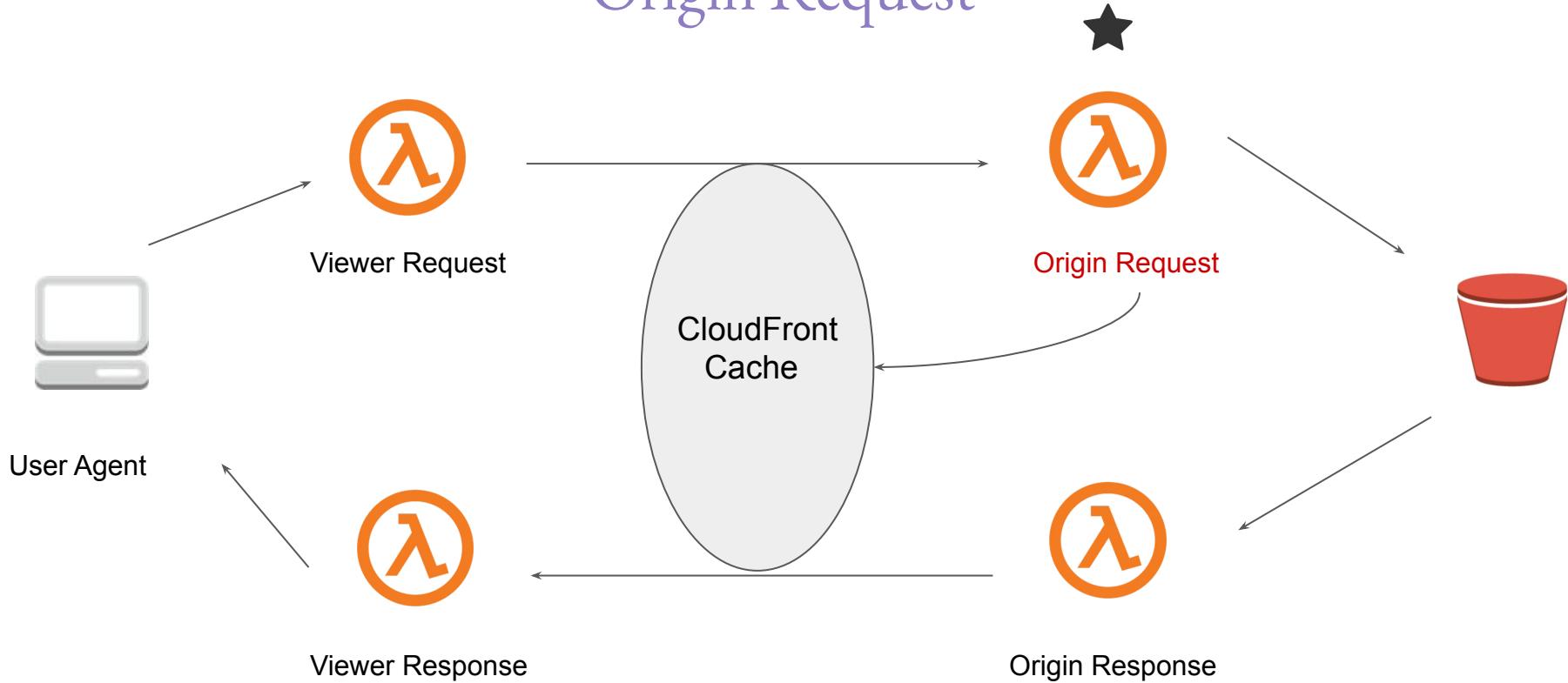
# Origin Request

Executed on cache miss, before a request is forwarded to the origin.

There are various things that we can do at this stage, like:

- Dynamically select origin based on the request headers

# Origin Request



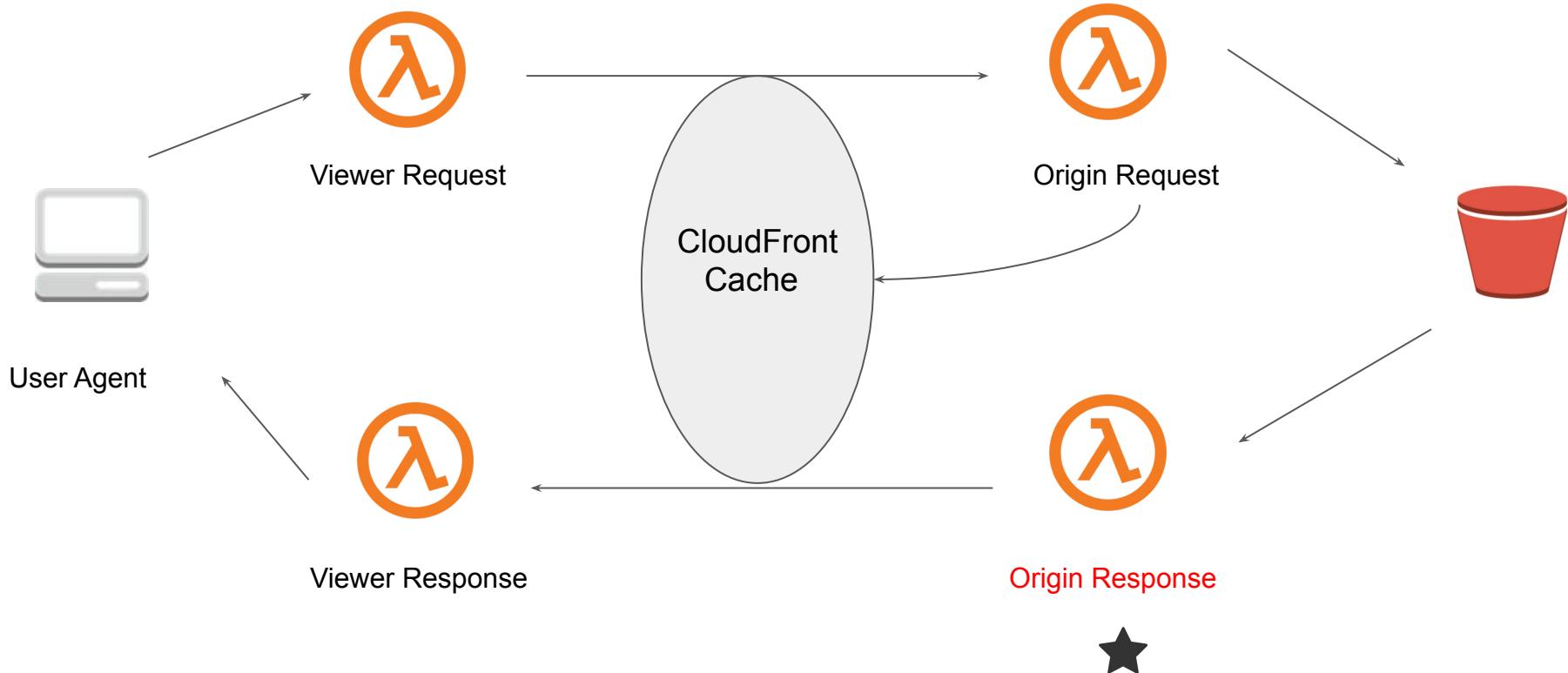
# Origin Response

Executed on a cache miss, after a response is received from the origin.

There are various things that we can do at this stage, like:

- Modify the response headers.
- Intercept and replace various 4XX and 5XX errors from the origin.

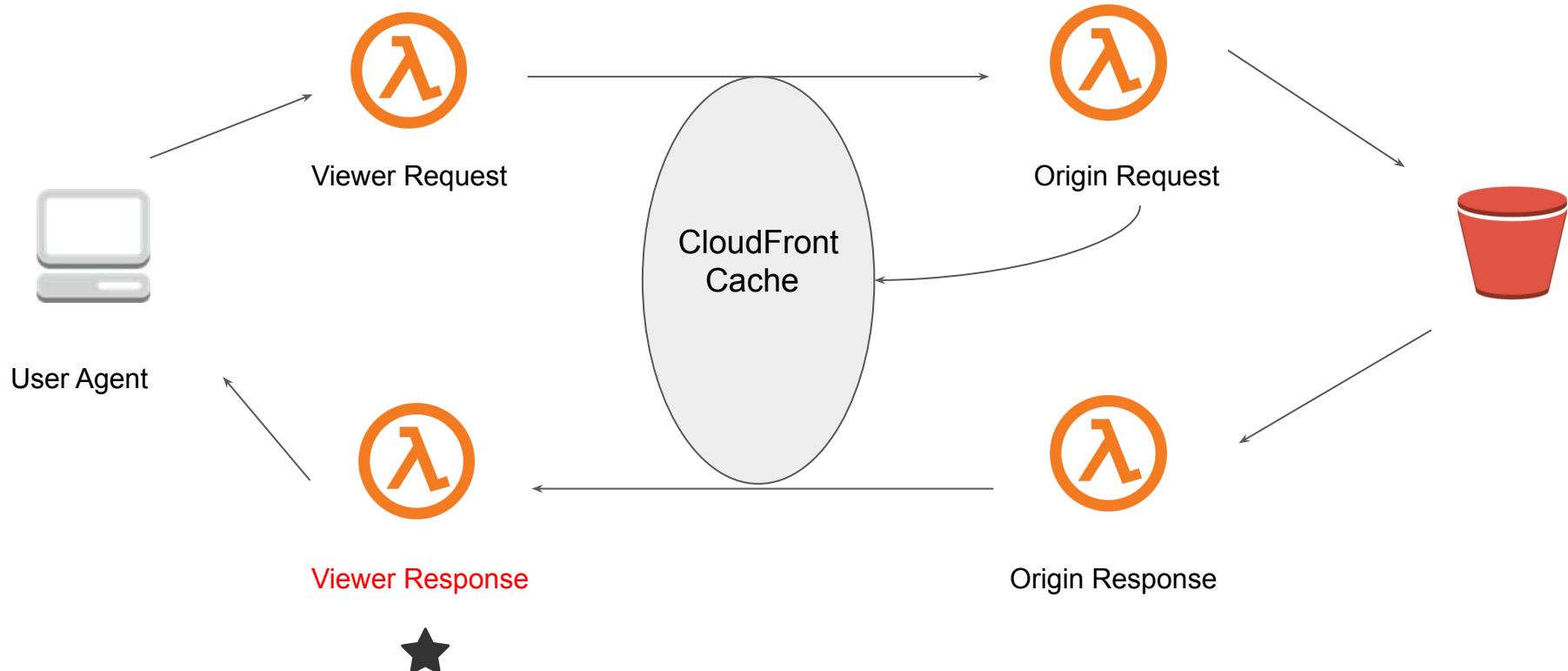
# Origin Response



# Viewer Response

Executed on all the responses received either from the origin or the cache.

Modifies the response headers before caching the response.



---

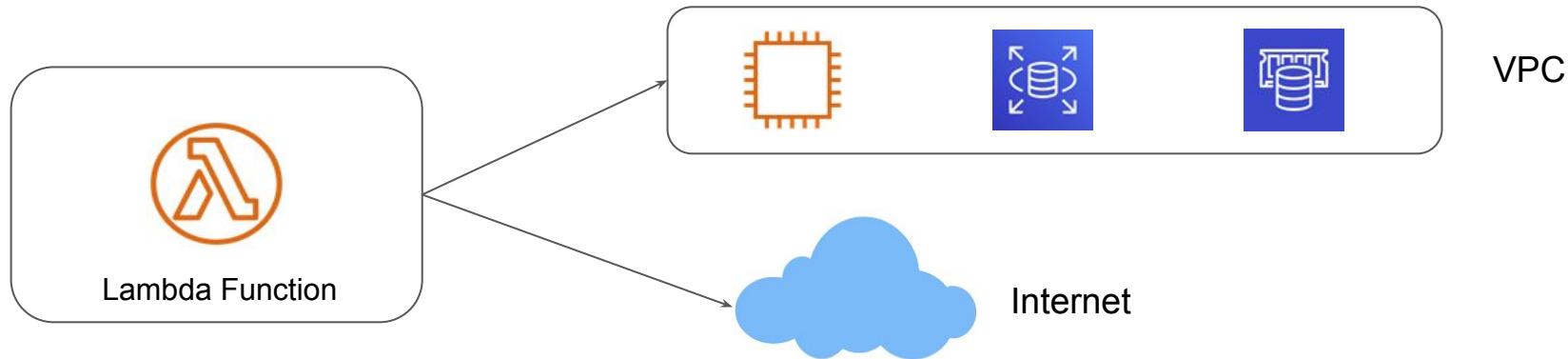
# Connectivity Features of Lambda

Networking Again!

# Connectivity Features

There can be scenarios where Lambda function needs to connect to EC2 instances, RDS databases which are running inside the VPC (private subnet)

Lambda can connect to both the resources inside the VPC and Public Resources.



# Lambda and VPC

By default, when your Lambda function is not configured to connect to your own VPCs, the function can access anything available on the public internet

However we can configure Lambda to connect to VPC by associate VPC and subnets with the function.



**Network**

Virtual Private Cloud (VPC) [Info](#)  
Choose a VPC for your function to access.

Default `Default` `172.31.0.0/16`

**Subnets**  
Select the VPC subnets for Lambda to use to set up your VPC configuration. Format: "subnet-id (cidr-block) | az name-tag".

`subnet-ffe20fb7 (172.31.32.0/20) | ap-southeast-1b X`

`subnet-979830ce (172.31.0.0/20) | ap-southeast-1c X`

# Important Point to Note

When launching in a specific subnet in VPC, make sure that NAT gateway is attached in-case if you need internet access to the Lambda function.

Lambda can also connect to AWS services like SQS via Private Link (VPC Endpoints)

If Lambda wants to connect to SQS to perform certain operations, appropriate IAM role will be needed.

If launched in VPC, you need to assign appropriate IAM role so that Lambda can perform certain operations like creating/deleting network interfaces.

---

# AppStream 2.0

Interesting Service

---

# Getting Started

AppStream 2.0 allows us to centrally manage our desktop application and securely deliver them to any computer.

## Sample Use-Case:

Software vendors can use AppStream 2.0 to deliver trials, demos, and training for their applications with no downloads or installations.

---

# Cross Origin Resource Sharing

Useful Topic for DevOps, Developers

---

# Getting Started

CORS is way to make use of additional HTTP headers to tell browser to let a web-application running on one origin (domain) have permission to access resource from different origin.

Example:

A frontend of JavaScript code for a web-application served from <http://domain-a.com> makes use of XMLHttpRequest to make a request for <http://api.domain-b.com/data.json>

---

# Multiprotocol Label Switching

MPLS



# Understanding the Challenge

When an internet router receives an IP packet, the packet contains no other information other than the destination IP address.

Thus, the router has to refer to complex routing tables to identify where to send the packet next.

This process is repeated at each hop along the way.



I need to reach 10.77.0.5



**Where do I send it next?**



# Overview of MPLS

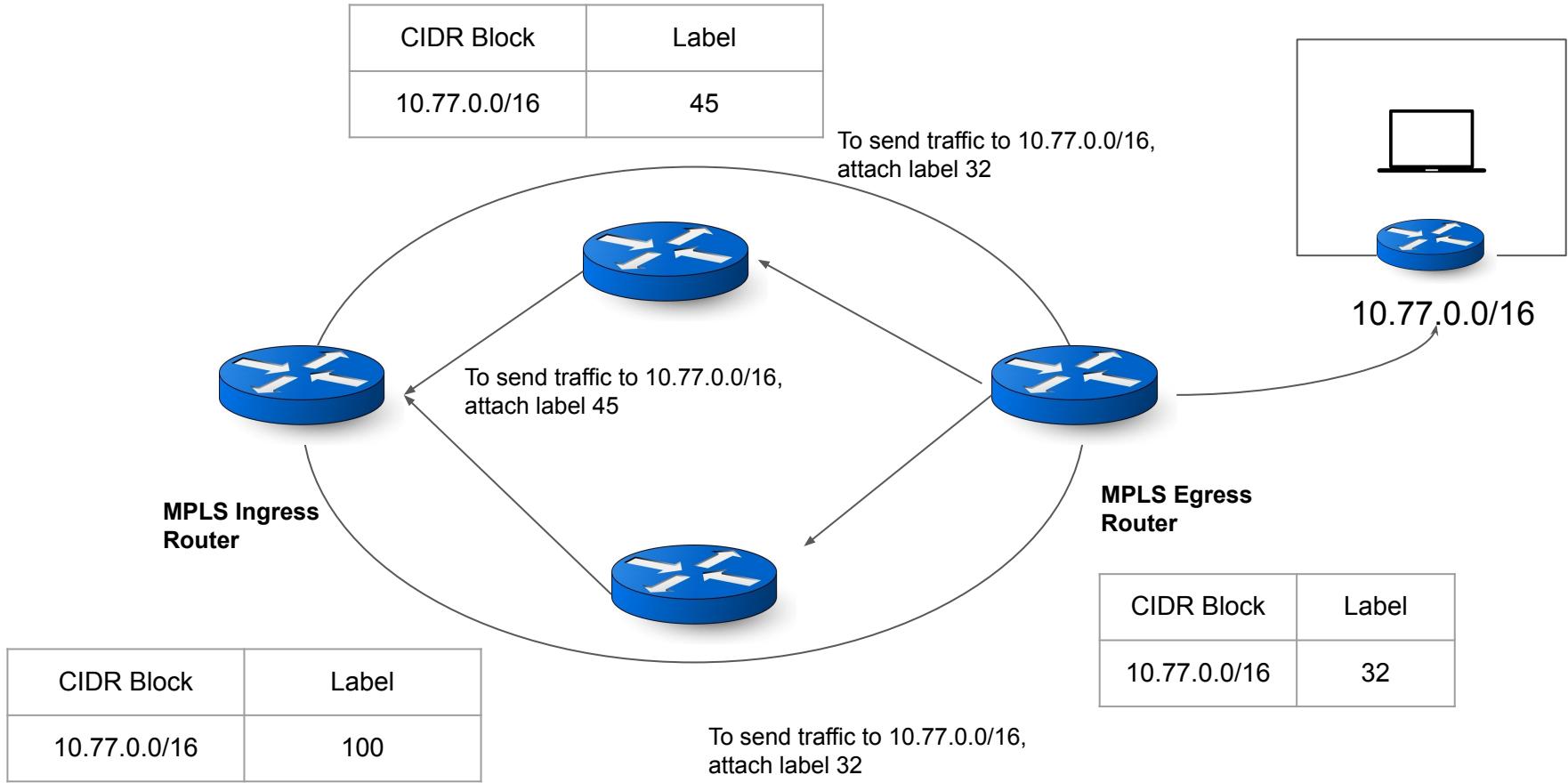
MPLS (Multi-Protocol Label Switching) addresses the problem of complex routing by establishing pre-determined, highly efficient routes (no IP based lookups)

In an MPLS network, packets of data are assigned labels, and all packet-forwarding decisions are made solely on the contents of these labels.

Two Important Benefits:

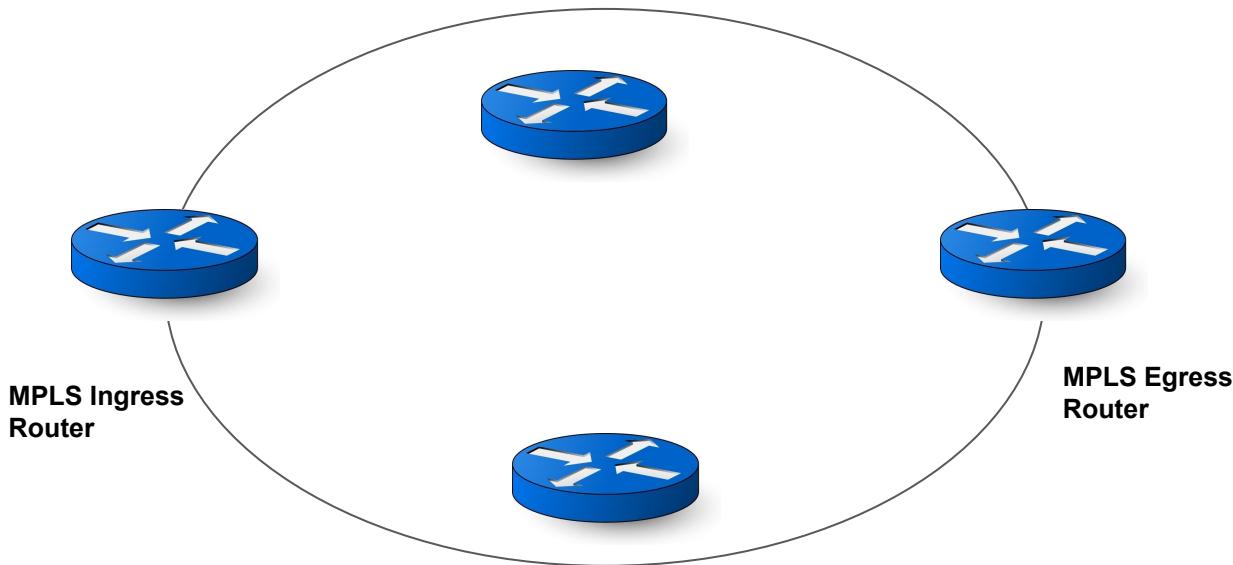
Multiple Protocol Supports: IP, IPX, and others.

Label based lookups - Increases speed



# Getting The Basics

MPLS (Multi-Protocol Label Switching) addresses the problem of complex routing by establishing pre-determined, highly efficient routes.



---

# VPC Peering

Let's Route

---

# VPC Peering

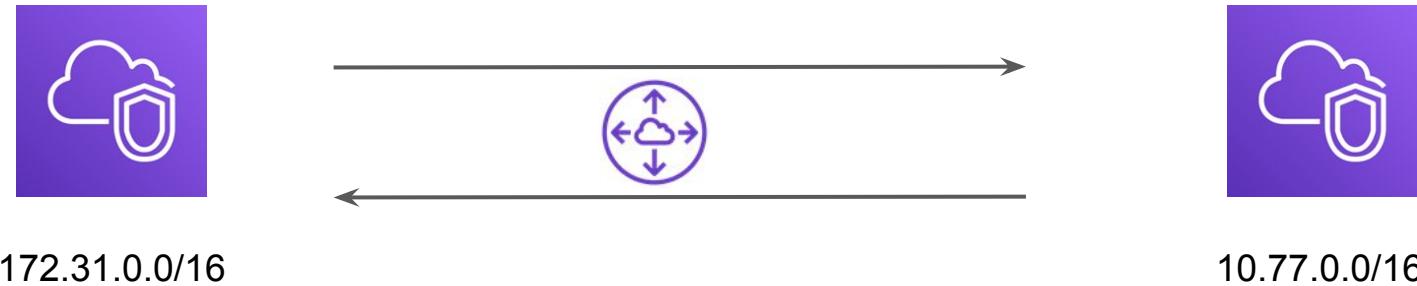
VPC peering is a network connection between two VPC that enables the communication between instances of both the VPC.



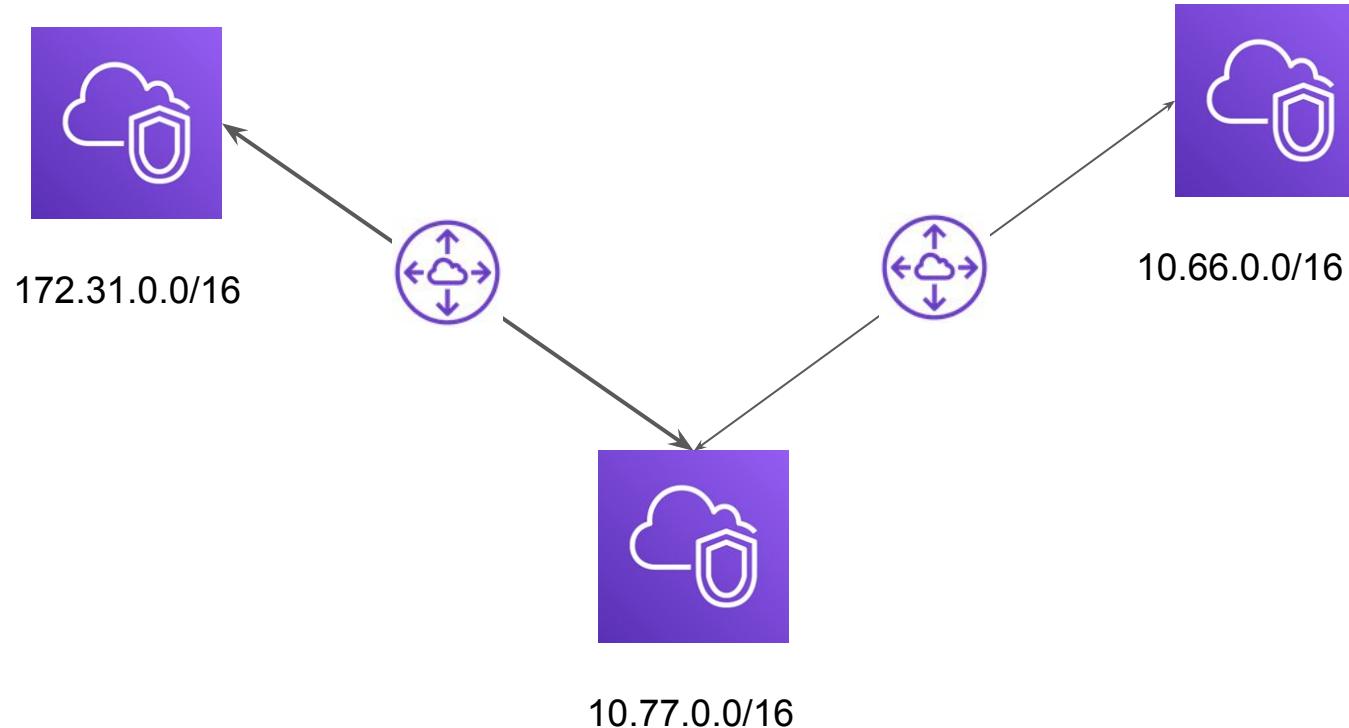
# Today's Architecture - 1

First VPC - 172.31.0.0/16

Secondary VPC - 10.77.0.0/16

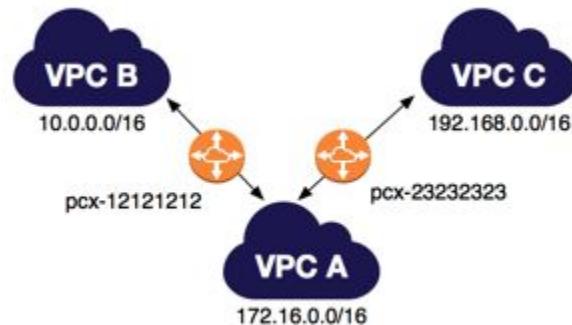


# Today's Architecture - 2



# Things to Remember

- VPC Peering is now possible between regions.
- VPC Peering does not act like a Transit VPC



# Unsupported VPC Peering Configurations - 1

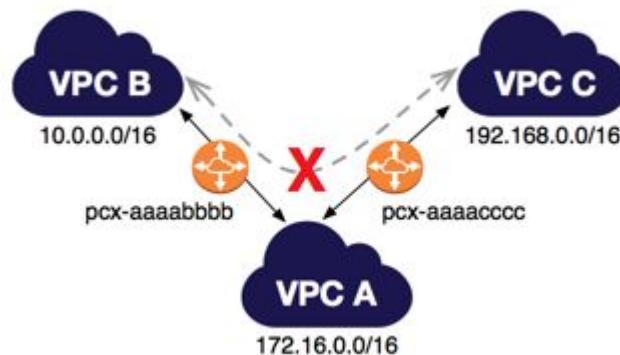
You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.



# Unsupported VPC Peering Configurations - 2

You have a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb), and between VPC A and VPC C (pcx-aaaacccc).

There is no VPC peering connection between VPC B and VPC C. You cannot route packets directly from VPC B to VPC C through VPC A.



---

# VPC Peering

Let's Route

---

# VPC Peering

VPC peering is a network connection between two VPC that enables the communication between instances of both the VPC.



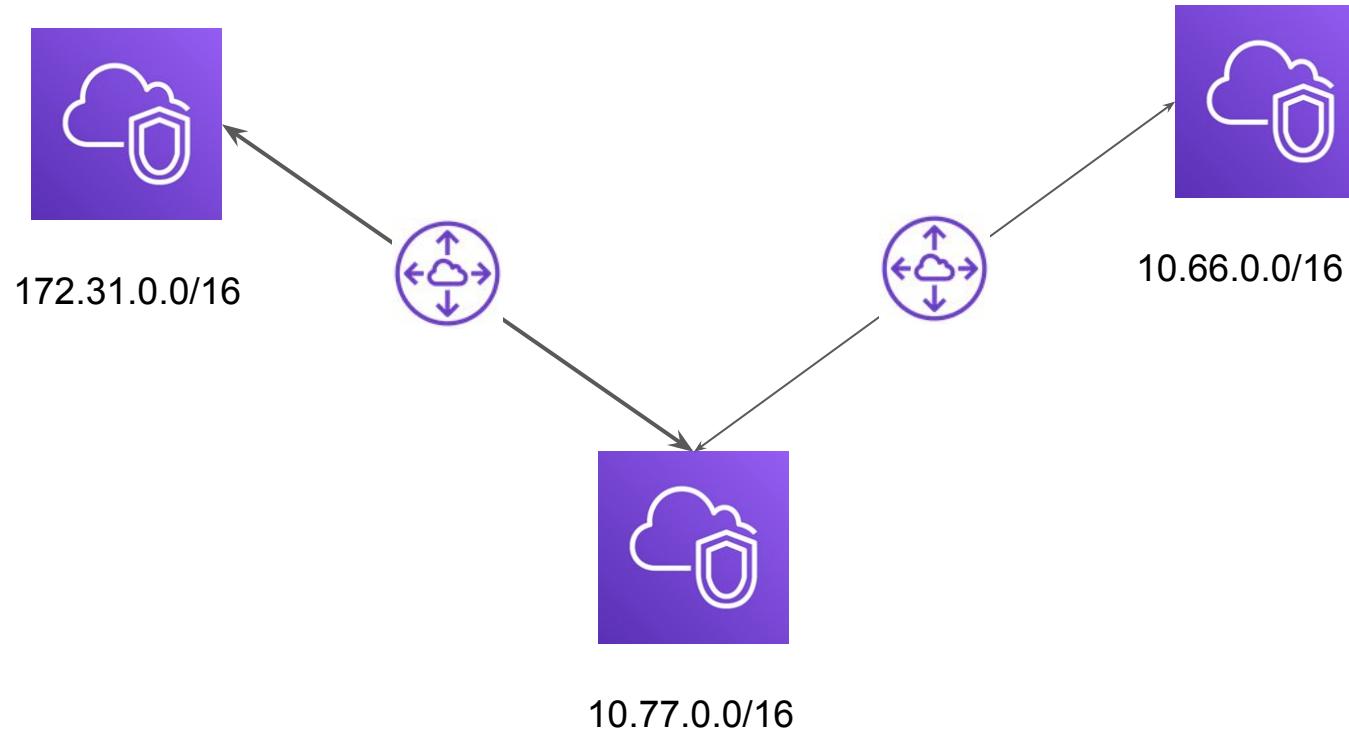
# Today's Architecture - 1

First VPC - 172.31.0.0/16

Secondary VPC - 10.77.0.0/16

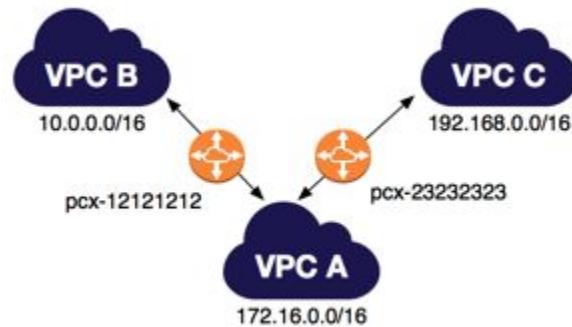


## Today's Architecture - 2



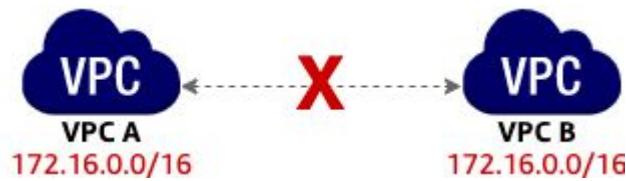
# Things to Remember

- VPC Peering is now possible between regions.
- VPC Peering does not act like a Transit VPC



# Unsupported VPC Peering Configurations - 1

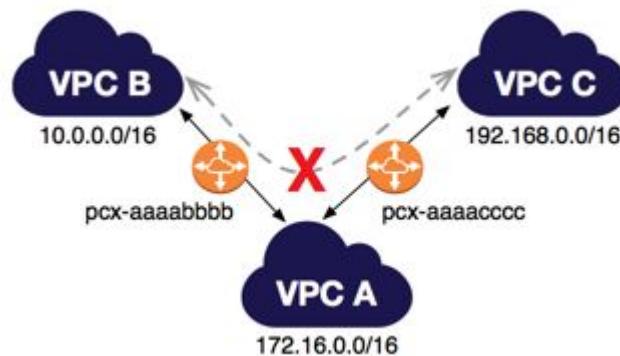
You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.



# Unsupported VPC Peering Configurations - 2

You have a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb), and between VPC A and VPC C (pcx-aaaacccc).

There is no VPC peering connection between VPC B and VPC C. You cannot route packets directly from VPC B to VPC C through VPC A.



---

# Resizing Considerations in VPC

Let's Resize

# Understanding the Basics

One of the important step in VPC creation is the decision of IPv4 CIDR block.

You can make use of Private CIDR Range along with Public Address block in VPC.

It is important to make use of Private Address block whenever possible.

Following three blocks of IP addresses are reserved for private use:

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)

# Understanding the Basics

AWS recommends using a larger CIDR block to avoid exhaustion of IPV4 addresses.

In-case if your CIDR block is exhausted, there are ways to add additional CIDR in VPC.

<b>Subnet Block</b>	<b>Total IP Addresses</b>
/16	65536
/17	32,768
/18	16,384
/19	8192
/24	256

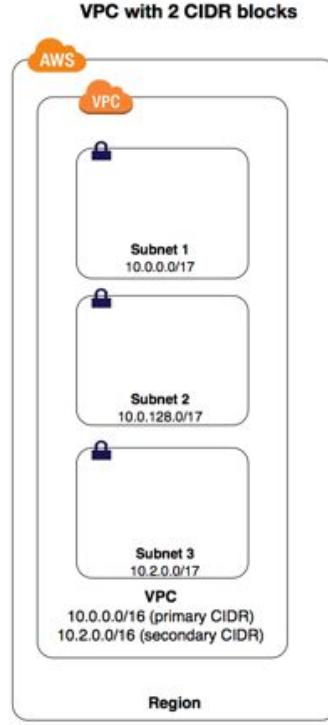
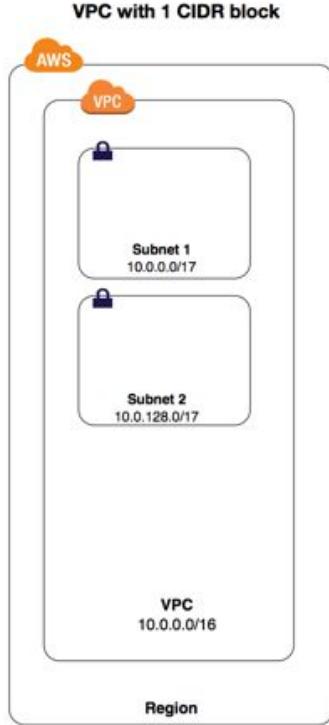
# Resize VPC Feature

Resize VPC Feature allows users to add five additional IPv4 CIDR ranges to your VPC.

This also allows expansion of VPC using IPv4 that have exhausted their addresses.

New VPC CIDR must not overlap with existing CIDR range or the CIDR range of peer VPC.

# Better Understood with Diagram



Main route table

Destination	Target
10.0.0.0/16	local

Main route table

Destination	Target
10.0.0.0/16	local
10.2.0.0/16	local

# Important Pointers

There is a default quota of 5 additional IPv4 blocks per VPC. This can be increased to maximum of 50 by raising a support request.

If the VPC peering connection is active, you can add CIDR blocks to a VPC provided they do not overlap with a CIDR block of the peer VPC.

There are restricted and permitted CIDR block associate that you need to consider before resize.

## Important Pointers - 2

We can add a single IPv6 CIDR block to the VPC. The CIDR block is a fixed prefix length of /56.

If you already have an IPV6 CIDR associated to the VPC, you cannot add another IPV6 address range

There are restricted and permitted CIDR block associate that you need to consider before resize.

In-case of errors related to “not enough addresses in subnet”, you can create new subnet with secondary IPv4 addresses and can additionally associate IPv6 block with range of /64

---

# Global Accelerator

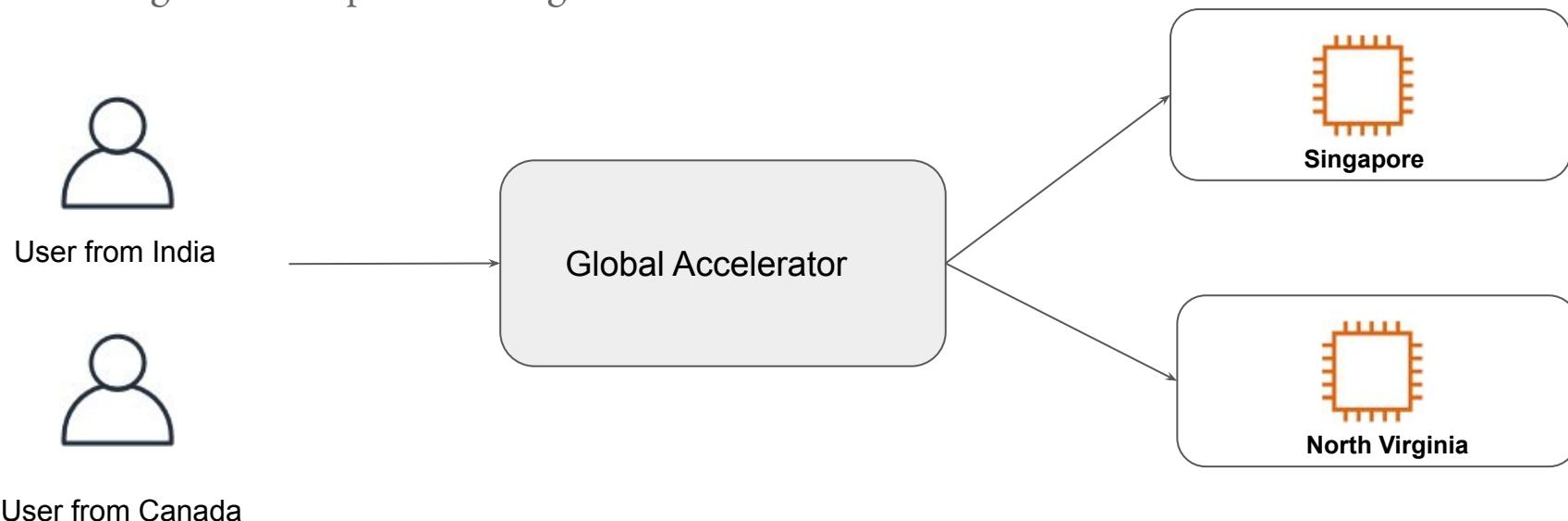
## Understanding The Basics

---

# Overview of Global Accelerator

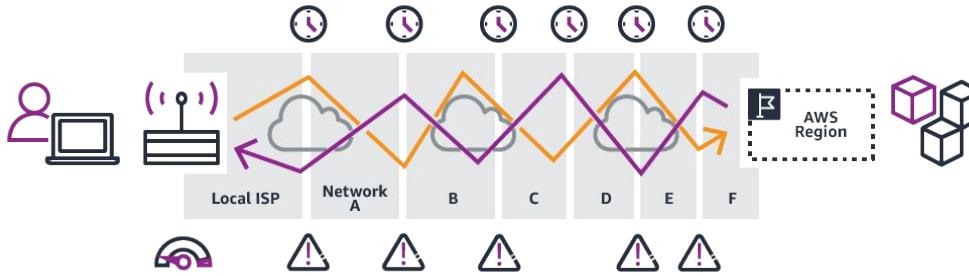
AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users.

It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Region

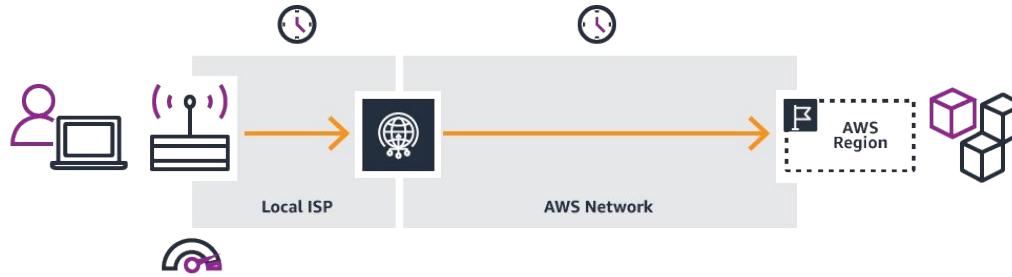


# Simplified Diagrammatic Difference

**Without  
Global Accelerator**



**After  
Global Accelerator**



# Working of Global Accelerator



---

# Traffic Mirroring

Capture Network Traffic

---

# Understanding the Challenge

Many organizations use various kind of wire data collection tools like Splunk stream to capture specific type network traffic to analyze for security threats.

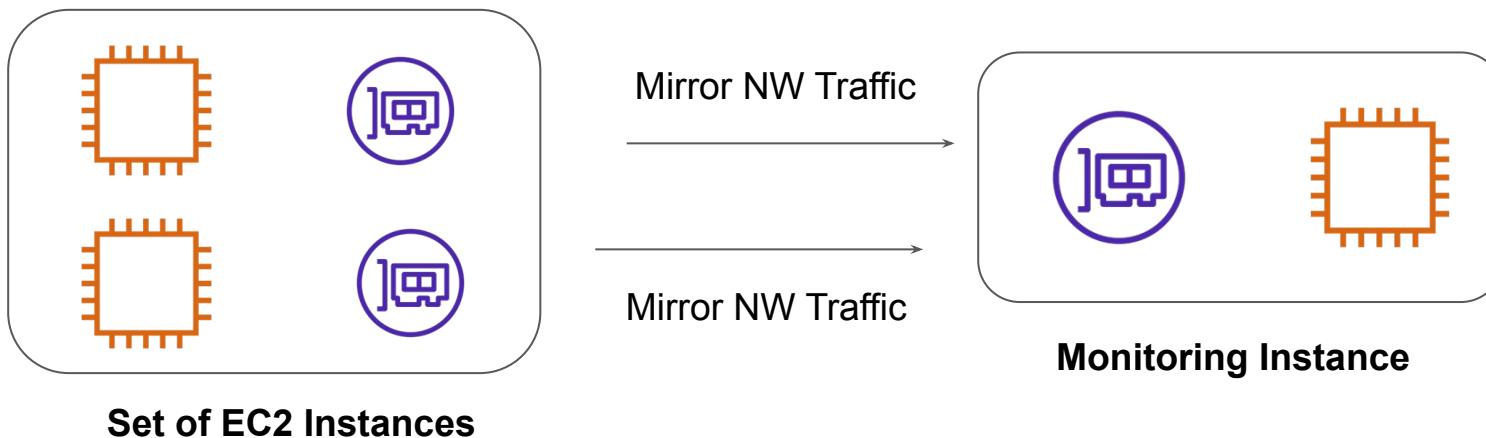
This used to impact the overall system performance.

```
3/30/17      { [-]
4:40:46.236 PM    bytes: 942
                  bytes_in: 249
                  bytes_out: 693
                  capture_bucket_date: 20170330
                  dest_ip: 10.141.32.197
                  dest_mac: 00:1B:17:00:01:30
                  dest_port: 8000
                  endtime: 2017-03-30T16:40:46.236839Z
                  file_server_id: steven
                  flow_id: cbfff4cc-1597-42dd-a2d7-f4172453d335
                  form_data: streamForwarderId=stream-nightly-currnightly.sv.splunk.com
                  http_comment: HTTP/1.1 200 OK
                  http_content_length: 345
                  http_content_type: application/json
                  http_method: GET
                  http_user_agent: SplunkStream/7.0.0
                  pcapsaved: T
                  protocol_stack: ip:tcp:http
                  server: Splunkd
                  site: stream-ui-test1.sv.splunk.com
```

# Basics of Feature

Traffic Mirroring is an Amazon VPC feature that you can use to copy network traffic from an elastic network interface.

You can then send the traffic to out-of-band security and monitoring appliances for:



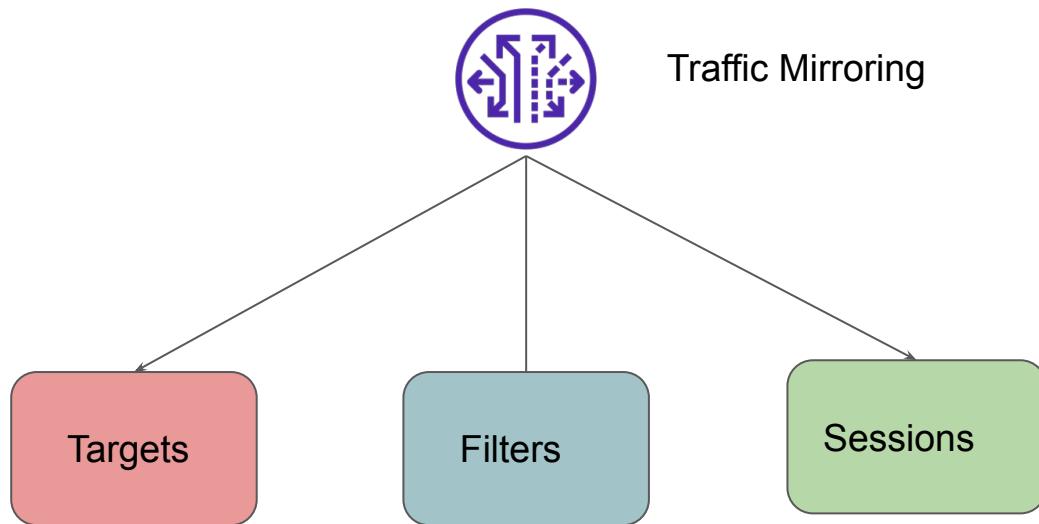
---

# Traffic Mirroring Concepts

Let's Capture Traffic!

# Important Concepts

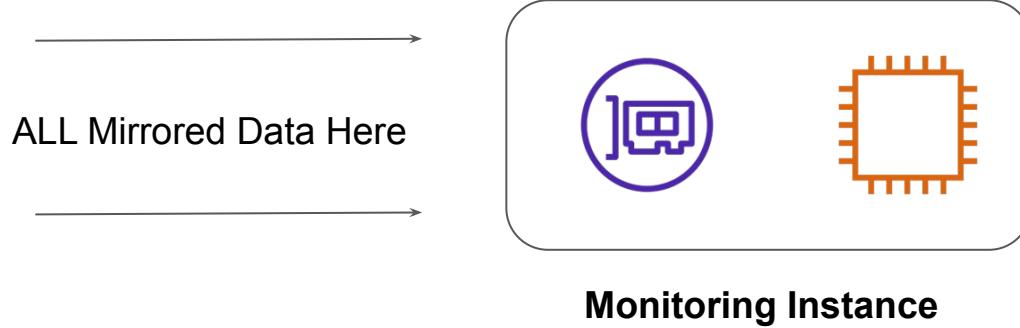
There are three important Traffic Mirroring Components



# Component 1 - Targets

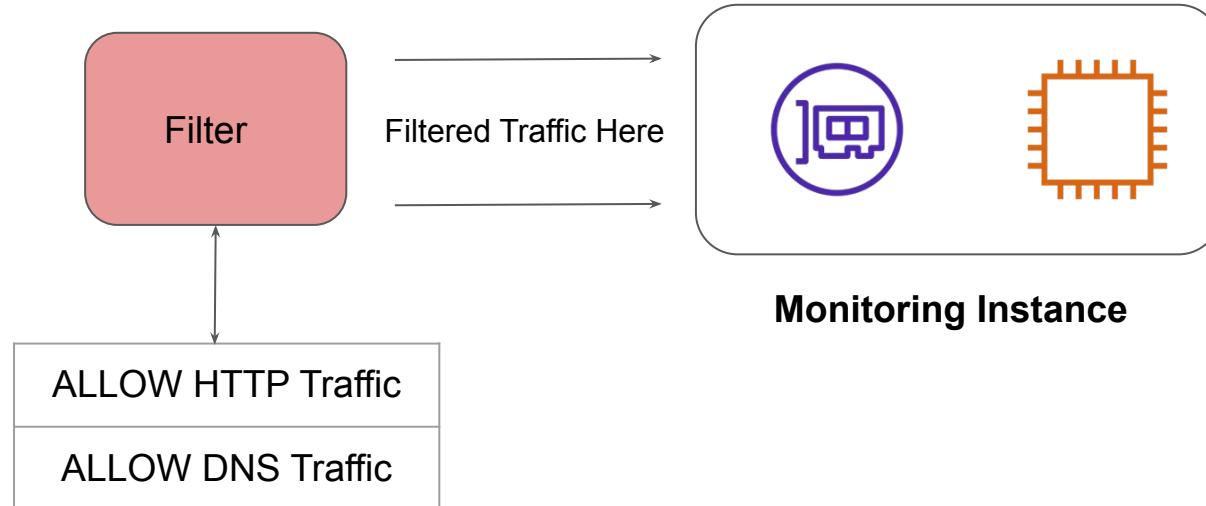
Targets is the destination for a traffic mirror session.

The traffic mirror target can be an elastic network interface, or a Load Balancer.



## Component 2 - Filters

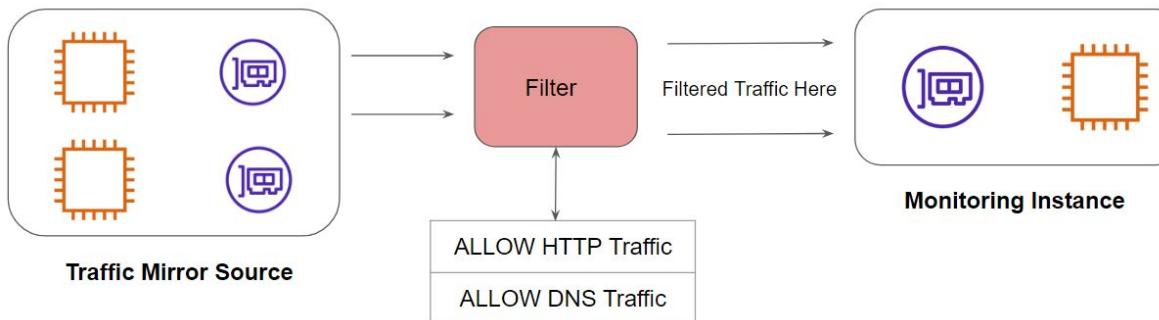
A traffic mirror filter is a set of inbound and outbound traffic rules that determine the traffic that is copied from the traffic mirror source and sent to the traffic mirror destination.



# Component 3 - Sessions

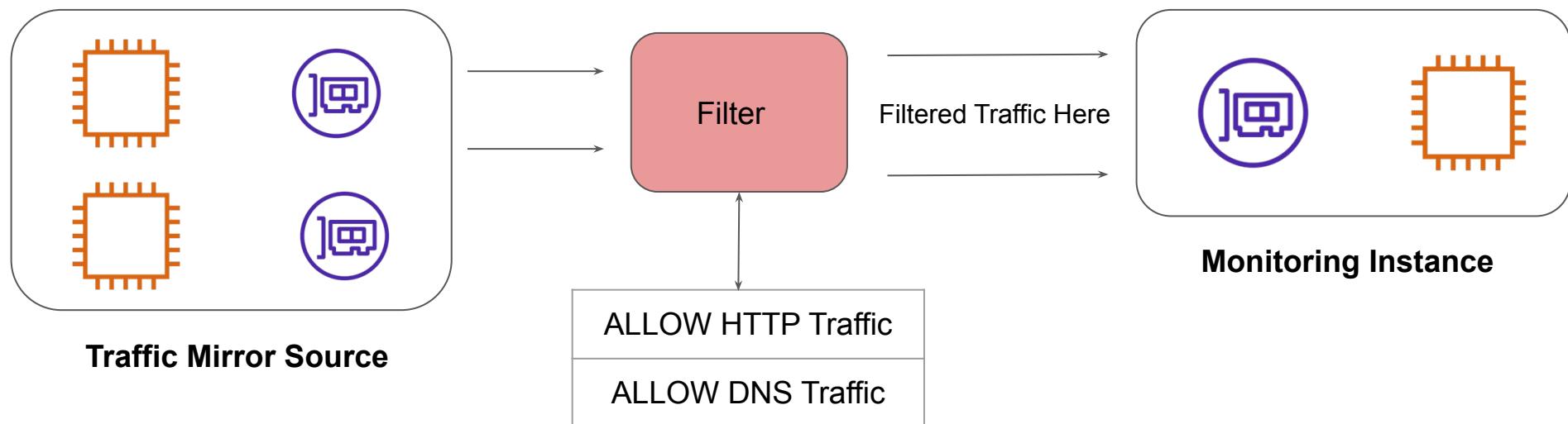
A traffic mirror session establishes a relationship between a traffic mirror source and a traffic mirror target. It contains the following:

- A traffic mirror source
- A traffic mirror target
- A traffic mirror filter



## Component 2 - Filters

A traffic mirror filter is a set of inbound and outbound traffic rules that determine the traffic that is copied from the traffic mirror source and sent to the traffic mirror destination.



---

# AWS Outposts

AWS in On-Premise

---

# Cloud is Servers Behind the Scenes

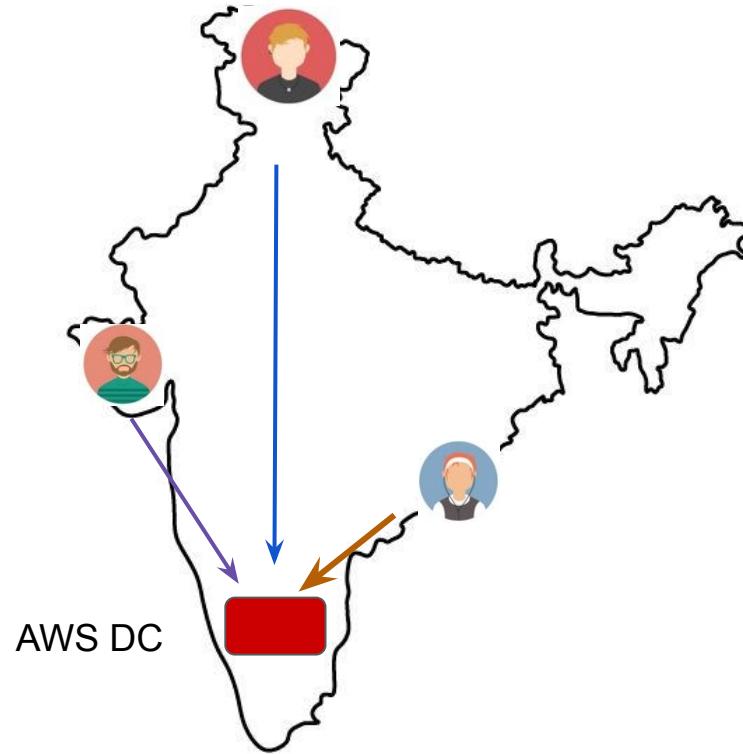
Cloud is basically set of Servers behind the scenes.

These servers reside in the AWS Datacenter.

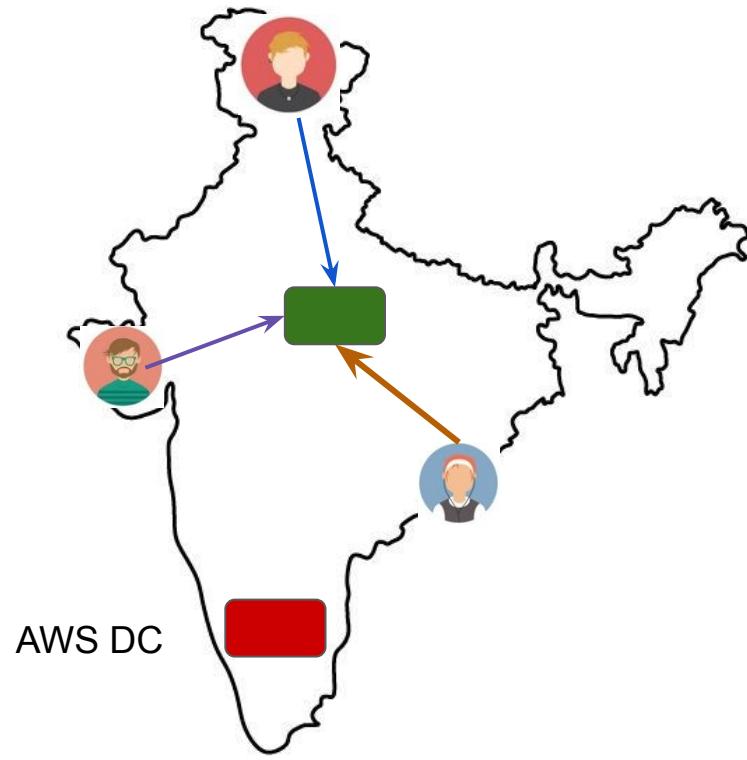
Everything from Power, Cooling, Internet Connectivity, Physical Security is managed by AWS.



# Challenge 1: Latency



# Possible Solution 1 - On-Premise Servers



# Challenges with Hybrid Architecture

1. Different set of API's to manage servers and services.
2. Automation is difficult.
3. Additional learning required.

# AWS Outposts

AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility.



AWS Side



Customer Side

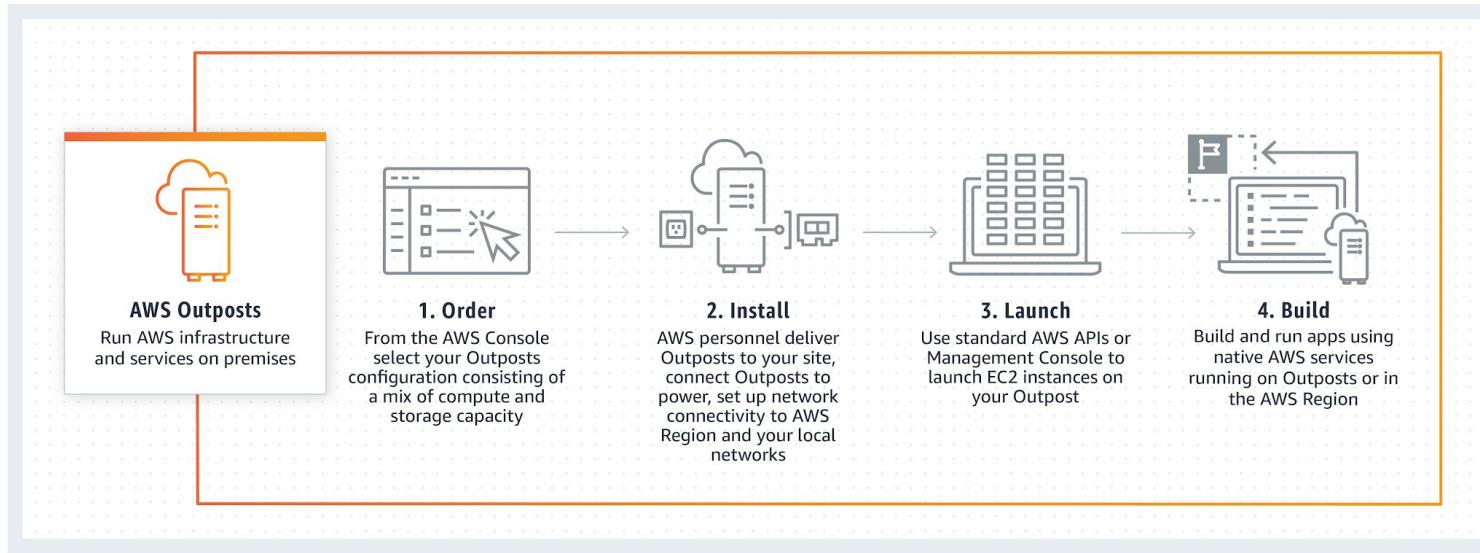
# Services that you can Run

With AWS Outposts, we can run wide variety of AWS services locally.

Some of these include:

- Amazon EC2
- Amazon EBS
- S3
- RDS
- EKS
- EMR

# Installation Step



# Use-Case for AWS Outposts

AWS Outposts can be used for wide-variety of use-cases.

Some of these include:

- Low-Latency Requirements
- Data Residency
- Local Data Processing

---

# IPAM in AWS

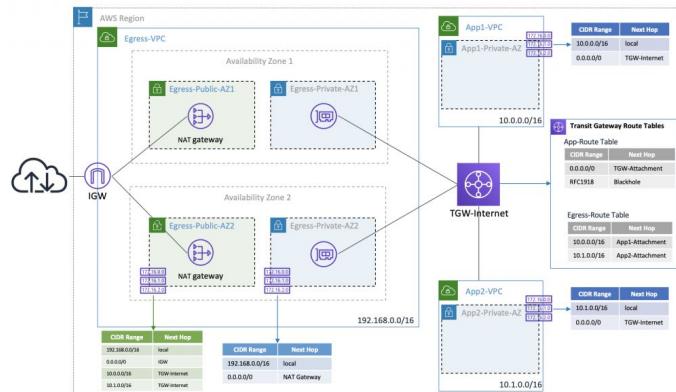
Track IP Addresses

---

# Understanding the Challenge

In the networks with fewer set of devices, network administrators use simple methods like maintaining spreadsheets to manage and keep track of IP Addresses.

However nowadays with 100s of AWS accounts, VPCs and others, the network has become more dynamic and traditional approach of tracking is not recommended.



# Basics of IPAM

IPAM allows network administrators to track and manage the network's IP space and also make sure the repository of assignable IP addresses stays up-to-date

The screenshot displays the IP Address Manager interface with three main sections:

- Top 10 DHCP Scopes by Utilization:** A table showing the utilization of DHCP scopes. The columns are SCOPE NAME, % IP SPACE USED, IPS AVAILABLE, and IPS USED.

SCOPE NAME	% IP SPACE USED	IPS AVAILABLE	IPS USED
192.168.0.0 / 24	59.38%	104	150
VoIP_Austin2	53.20%	95	108
VoIP_Austin1	50.25%	101	102
WiFi_Brno	50.00%	25	25
WiFi_Cork	49.02%	26	25
VoIP_Austin2	49.02%	26	25
Curitiba-Dev	48.44%	132	122
WiFi_Austin1	45.80%	71	60
WiFi_Austin2	44.78%	74	60
WiFi_Austin2	41.67%	70	50

- IP Address Conflicts:** A table showing IP address conflicts. The columns are IP ADDRESS, TYPE, SUBNET, TIME OF CONFLICT, ASSIGNED MAC, and CONFLICTING MAC.

IP ADDRESS	TYPE	SUBNET	TIME OF CONFLICT	ASSIGNED MAC	CONFLICTING MAC
10.199.22.2	UDT Node / Access Point	10.199.22.0	29 Jan 2017 7:38:08PM	D0-67-E5-2B-DF-7E	D0-80-C8-33-22-11
	UDT Node Port / SSID :			SE-Norte5520	SE-Norte5520
				Ic35 (Slot 1 Port: 35)	Ic35 (Slot 1 Port: 3)
10.1.1.10	UDT Node / Access Point	10.1.1.0 / 24	29 Jan 2017 7:32:18PM	00-12-FB-85-0A-E5	04-DB-56-B5-0A-E4
	UDT Node Port / SSID :			H3C	H3C
				Ethernet1/0/S	Ethernet1/0/R

- Last 25 IPAM Events:** A list of recent IPAM events. Each event includes a timestamp, source (SYSTEM), icon, message, and details.

TIME	SOURCE	ICON	MESSAGE	DETAILS
1/29/2017 1:38 AM	SYSTEM	⚠️	The IP address 10.199.22.2 is in conflict.	The following devices were detected on network with same IP address: - Dhcp Leases MAC: D0-67-E5-2B-DF-7E, MAC: D0-80-C8-33-22-11
1/29/2017 1:38 AM	SYSTEM	+	The conflict for IP Address: 10.199.22.2 is detected with MACs: D0-67-E5-2B-DF-7E, 00-80-C8-33-22-11.	
1/29/2017 1:32 AM	SYSTEM	+	The conflict for IP Address: 10.1.1.10 is detected with MACs: 00-12-FB-85-0A-E5, 04-DB-56-B5-0A-E4.	
1/29/2017 1:32 AM	SYSTEM	⚠️	The IP address 10.1.1.10 is in conflict.	The following devices were detected on network with same IP address: - Dhcp Leases MAC: 00-12-FB-85-0A-E5, MAC: 04-DB-56-B5-0A-E4
1/29/2017 1:27 AM	SYSTEM	+	The conflict for IP Address: 10.199.2.5 is detected with MACs: 00-10-18-AC-71-22, 78-FD-A4-C5-BA.	
1/29/2017 1:27 AM	SYSTEM	⚠️	The IP address 192.168.2.5 is in conflict.	The following devices were detected on network with same IP address:

# IPAM in AWS

Amazon VPC IP Address Manager (IPAM) is a VPC feature that makes it easier for you to plan, track, and monitor IP addresses for your AWS workloads.

The screenshot shows the 'Resources' page in the Amazon VPC IP Address Manager. At the top, there is a search bar labeled 'Input a CIDR' and a dropdown menu set to 'ipam-scope-076d6aca903a7c3b1'. Below the header is a table with the following columns: Resource ID, Compliance status, Overlap status, Resource name, and IP usage. The table lists seven resources, each with a checkbox, a copy icon, and a link to its details page. The resources are:

Resource ID	Compliance status	Overlap status	Resource name	IP usage
vpc-04101b332554fc1df	Unmanaged	Nonoverlapping	custom-vpc-mumbai	0%
vpc-05721a25e8f9484b2	Compliant	Overlapping	ipam-vpc	100%
vpc-095b1a4cf2da61207	Compliant	Overlapping	ipam-vpc-2	0%
vpc-09bc335f35d9624b0	Unmanaged	Overlapping	project-vpc	13%
vpc-48ae592e	Unmanaged	Overlapping	-	19%
vpc-77f6031c	Unmanaged	Overlapping	-	19%
vpc-a96ebcd4	Unmanaged	Overlapping	-	38%

# Benefits of IPAM in AWS

You can use IPAM to do the following:

- Monitor IP address space that's in use.
- View the history of IP address assignments in your organization
- Automatically allocate CIDRs to VPCs using specific business rules
- Enable cross-region/account sharing of your Bring Your Own IP (BYOIP) addresses

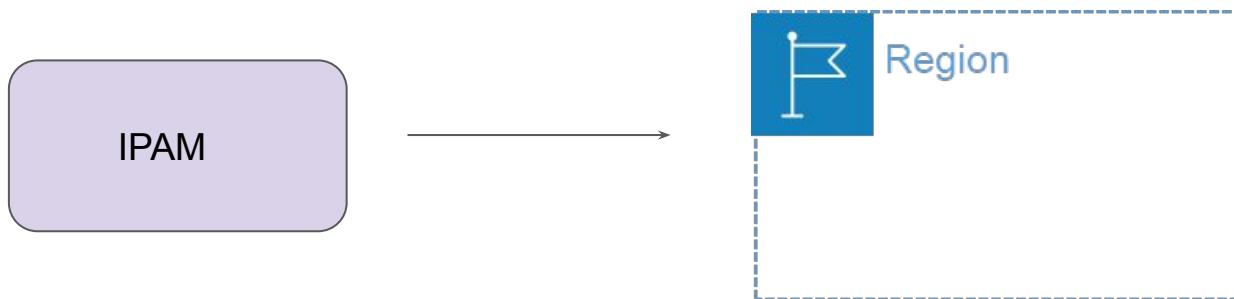
---

# IPAM Practical

## IP Address Manager

# Step 1 - Creating IPAM

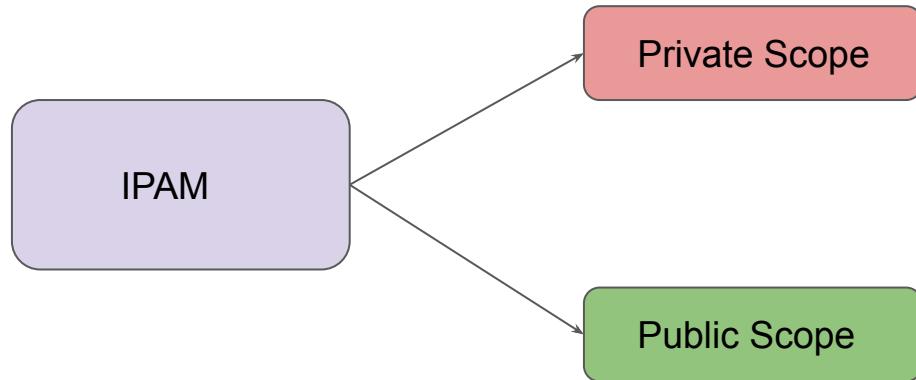
When you create the IPAM, you choose which AWS Region to create it in.



# Scopes in IPAM

When you create an IPAM, AWS VPC IPAM automatically creates two scopes for the IPAM.

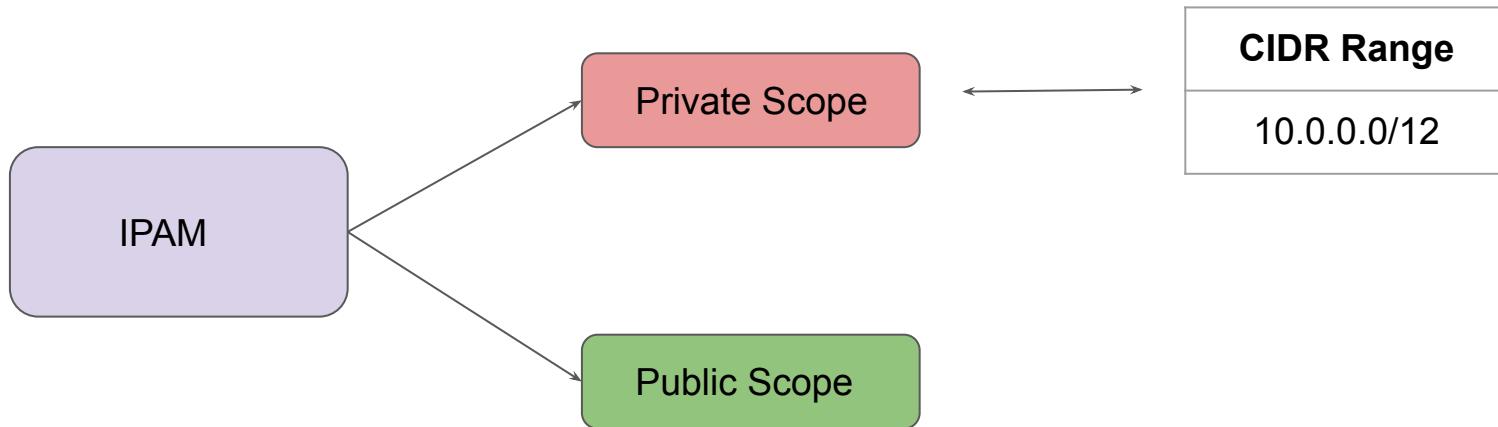
The **private scope** is intended for all private space. The **public scope** is intended for all public space.



# Pools in IPAM

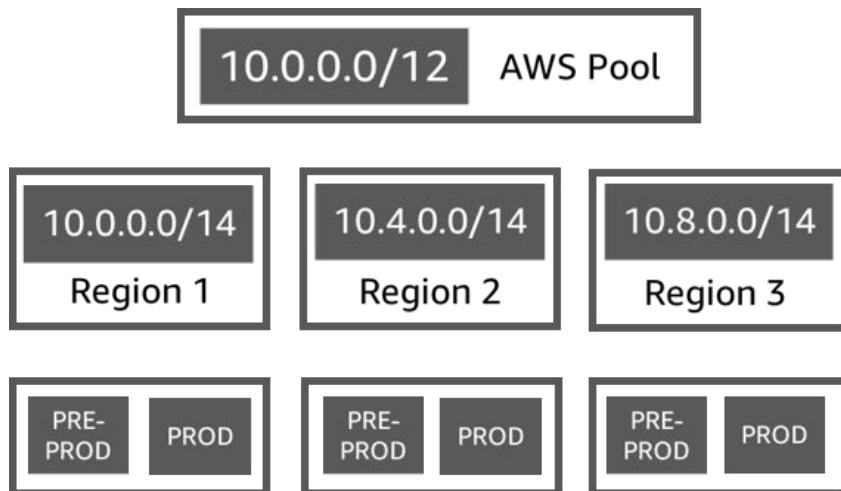
Pool is a collection of CIDR ranges.

A pool is associated with a scope.



# Sample Architecture - Pools

You can have multiple pools within a top-level pool.



---

# VPC Reachability Analyzer

Debugging Connectivity

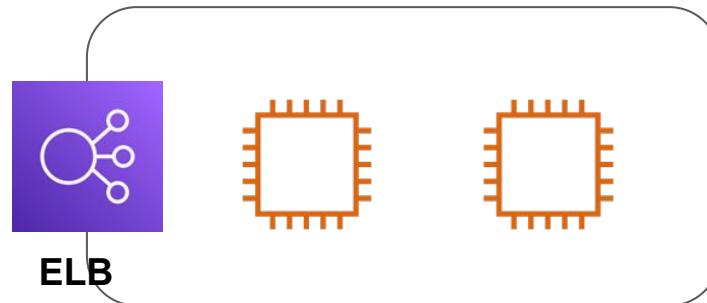
---

# Understanding with An Interview Question

- A user is not able to open a newly launched website.
- Organization is using ELB.
- Troubleshoot.

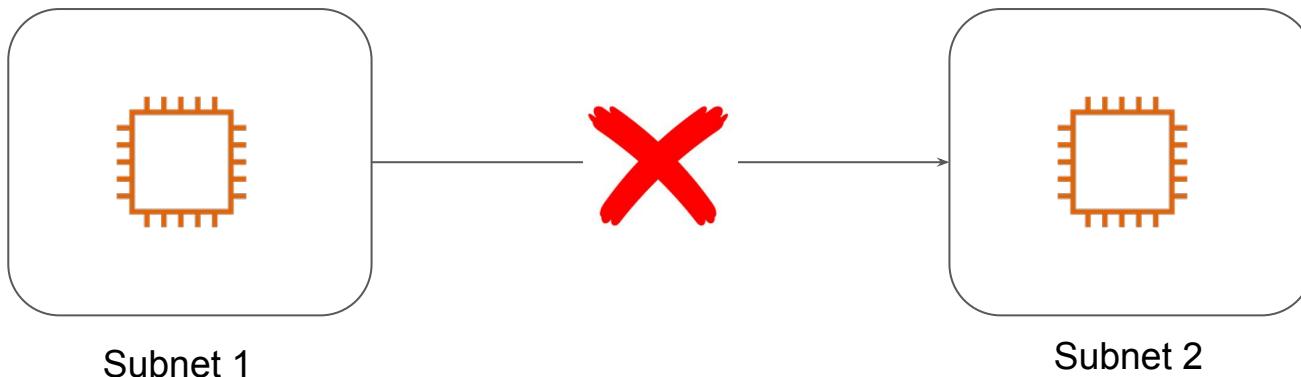


User



# VPC Reachability Analyzer

VPC Reachability Analyzer is a configuration analysis tool that enables you to perform connectivity testing between a source resource and a destination resource in your virtual private clouds (VPCs).



 Destination is not reachable. For more information, see the explanations below.

[Give us feedback](#)

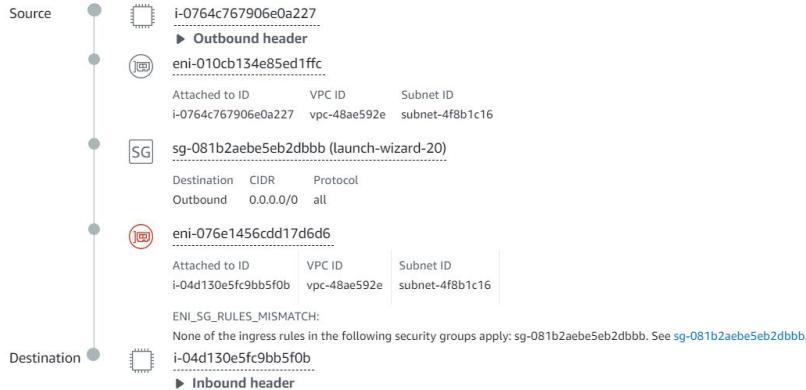
## Explanations

None of the ingress rules in the following security groups apply: sg-081b2aebe5eb2dbbb. See [sg-081b2aebe5eb2dbbb](#).

[► Details](#)

## Path details

 [View reverse path](#)



---

# Network Access Analyzer

Tune In with Compliance

---

# Understanding the Basics

Network Access Analyzer uses algorithms to analyze the network paths that a packet can take between resources in an AWS network.

It then produces findings whether the path conforms to the network requirement of organization.

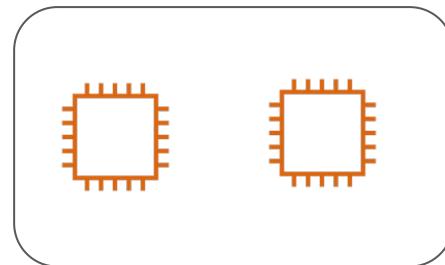
**Use-Case:** Only EC2 instances in App Subnet should be able to connect to DB Instances.



## Example 2 - Locate Instances With Internet Access

Military Corp is hosting EC2 instances that contains sensitive data.

These instances should NOT have a Internet Access.



---

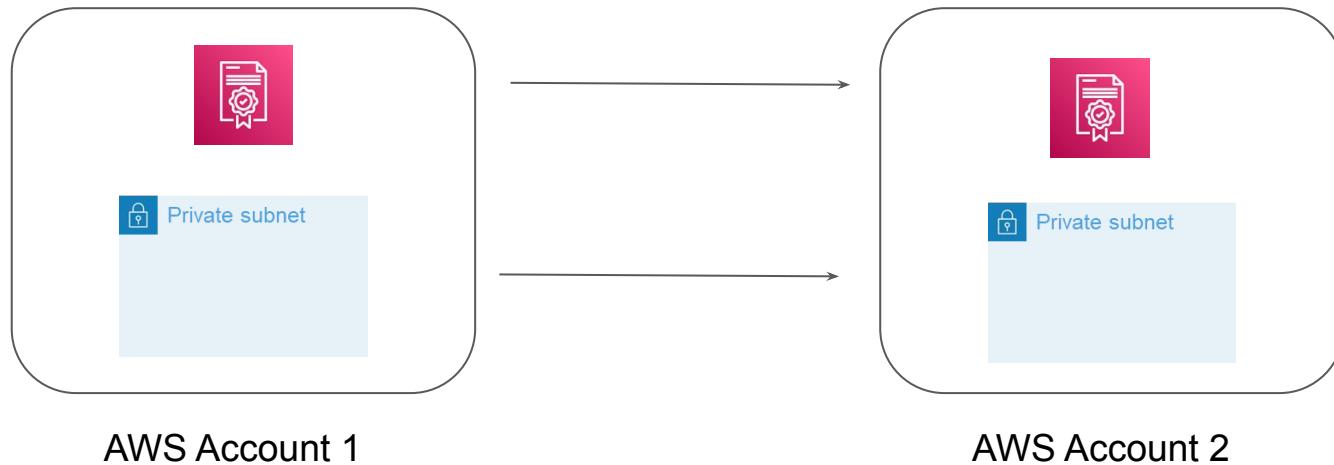
# AWS Resource Access Manager

Let's Share Resources

---

# Overview of Resource Access Manager

AWS Resource Access Manager (AWS RAM) helps you securely share the AWS resources that you create in one AWS account with other AWS accounts.



---

# VPC Sharing in AWS

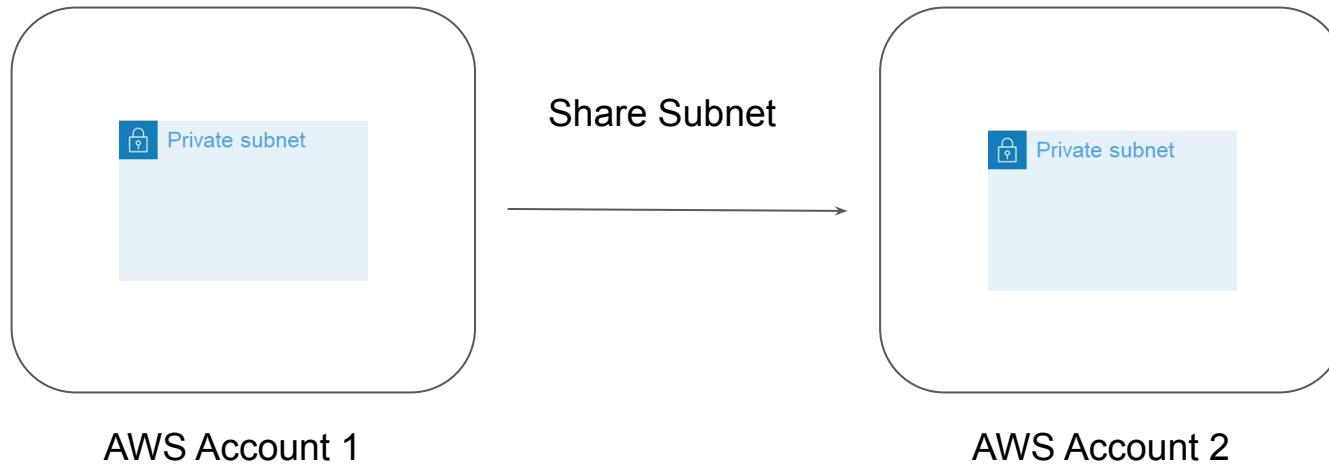
Let's Share Subnets

---

# Understanding the Basics

VPC sharing allows multiple AWS accounts to create their application resources, such as EC2 instances, RDS, and others into shared, centrally-managed virtual private clouds (VPCs).

In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations.



## Important Note

VPC owners are responsible for creating, managing, and deleting the resources associated with a shared VPC. These include subnets, route tables, network ACLs and others.

VPC owners cannot modify or delete resources created by participants, such as EC2 instances and security groups

Default subnets cannot be shared.

# Billing Considerations

In a shared VPC, each participant pays for their application resources including EC2 instances, RDS, Lambda functions and other resources.

Participants also pay for data transfer charges associated with inter-Availability Zone data transfer, data transfer over VPC peering connections.

VPC owners pay hourly charges across NAT gateways, virtual private gateways, transit gateways, and other VPC specific central resources.

# **Bring your own IP addresses**



# Basics of IP Reputation

IP reputation is a measure that helps evaluate the quality of an IP address and determine how legitimate its requests are

Bad IP Reputation generally corresponds to activities like sending spam emails, viruses etc that originate from the IP.

**LOCATION DATA**

North Bergen, United States

**OWNER DETAILS**

IP ADDRESS	161.35.125.167
⑦ FWD/REV DNS MATCH	Yes
HOSTNAME	fe.sati.com.py
⑦ DOMAIN	sati.com.py
⑦ NETWORK OWNER	digital ocean

**REPUTATION DETAILS**

⑦ SENDER IP REPUTATION	● Poor	Submit Sender IP Reputation Ticket
⑦ WEB REPUTATION	✗ Untrusted	Submit Web Reputation Ticket

**EMAIL VOLUME DATA**

	LAST DAY	LAST MONTH
⑦ EMAIL VOLUME	3.4	3.3
⑦ VOLUME CHANGE	-17.07%	
⑦ SPAM LEVEL	Critical	

**CONTENT DETAILS**

# Use-Case: Organization Migrating to Cloud

Organization's infrastructure is hosted in the on-premise datacenter.

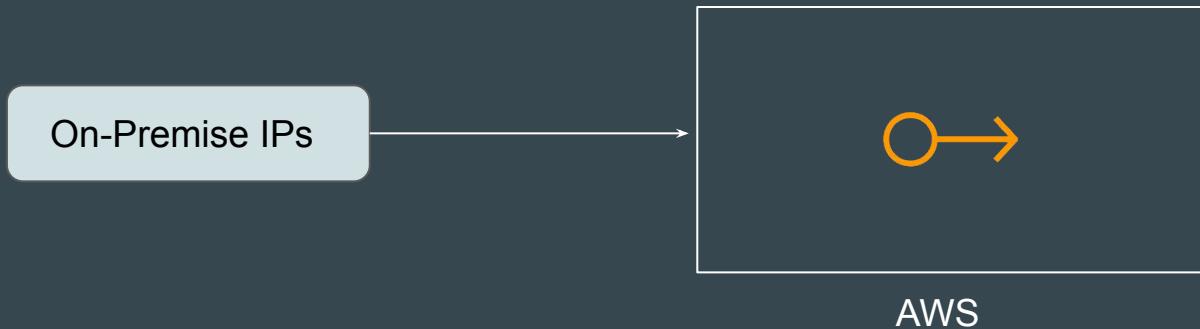
They have certain Public IPs from years with very good reputation.

They decide to migrate to Cloud and server receive IP with NOT as good reputation as their previous IPs.



# Introducing Bring Your Own IP

You can bring part or all of your publicly routable IPv4 or IPv6 address range from your on-premises network to your AWS account.



# Benefits of Bring Your Own IP

Benefits	Description
IP Reputation	Many customers consider the reputation of their IP addresses to be a strategic asset and want to use those IPs on AWS with their resources.
Customer whitelisting	BYOIP also enables customers to move workloads that rely on IP address whitelisting to AWS without the need to re-establish the whitelists with new IP addresses
Regulation and compliance	Many customers are required to use certain IPs because of regulation and compliance reasons. They too are unlocked by BYOIP.

# Important Requirements - Part 1

The address range must be registered with your regional internet registry (RIR) such as ARIN, RIPE, APNIC.

It must be registered to a business or institutional entity and cannot be registered to an individual person.

The most specific IPv4 address range that you can bring is /24.

The most specific IPv6 address range that you can bring is /48 for CIDRs that are publicly advertised, and /56 for CIDRs that are not publicly advertised.

## Important Requirements - Part 2

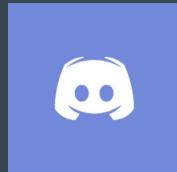
The addresses in the IP address range **must have a clean history**. AWS might investigate the reputation of the IP address and reserve the right to reject an IP address range if an IP has a poor reputation or is associated with malicious behavior.

## Points to Note

Customers can create Elastic IPs from the IPv4 space they bring to AWS and use them with EC2 instances, NAT Gateways, and Network Load Balancers.

# Join us in our Adventure

Be Awesome



[kplabs.in/chat](https://kplabs.in/chat)



[kplabs.in/linkedin](https://kplabs.in/linkedin)

---

# Web Application Firewall

Next generation firewalls

---

# Getting started

We all know about Firewalls and in some way might have worked as well.

Firewall works on the Layer 3 and Layer 4 of the OSI model.

Main aim of firewall: Block malicious and unauthorized traffic.

However what about malicious traffic like SQL Injection attacks, XSS and many more ?

# Introducing WAF

A Web Application Firewall is an application level firewall for HTTP applications.

It applies set of rules for the HTTP based conversations.

WAF generally are deployed to protect against attacks targeted towards application, specifically the ones defined in the OWASP Top 10 metrics.



# WAF Vendors

There are lot of ways in which you can implement WAF and various vendors as well.

Naxsi and Modsecurity are some of the famous open sources ones.

Signal Sciences, Akamai, AWS WAF are some of the commercial vendors that offer WAF related functionalities.



---

# AWS WAF

Protection against Layer 7 Attacks

---

# Understanding AWS WAF Concepts

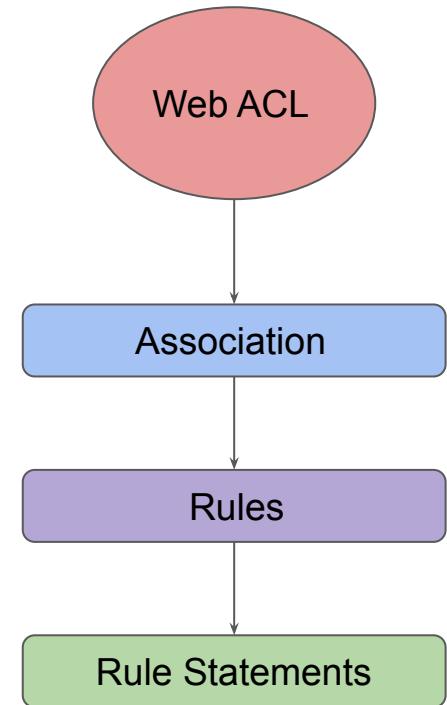
I live in a place A in Bangalore and want to meet my friend living in place B in Bangalore.

**Rule Statement:** If traffic is less on the roads?  
Are there any Uber / OLA available?

**Rules:** If traffic is less AND uber ola available then yes or no

**WebACL:** Container for all the things + default action.

**Association:** Zeal



# Rule Statements

Rule Statements define basic characteristics that would be analyzed within a web request.

These can be custom-defined or you can use ready-made ones from AWS and marketplace.

1. Block all the requests which are coming from out of India.
2. Block request which has a URI Path of /admin

You can even build custom condition based on:

Headers, HTTP Method, Query Strings, URI Path, Geo-Location, Body.

# Rules in WAF

We can combine multiple statements into rules to precisely target requests.

WAF provides two primary rule types: **Regular Rule & Rate-Based rule**

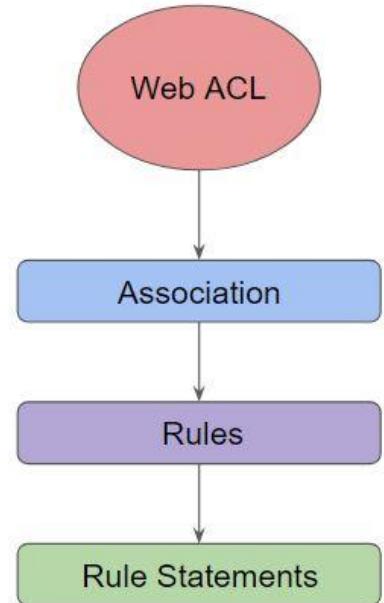
Let's look into sample regular rule:

1. If a request comes from 172.30.0.50
2. Request has SQL-like code

Rules with multiple statements can be AND, OR, NOT

**Rate-Based rule** = Regular Rule + Rate limiting feature

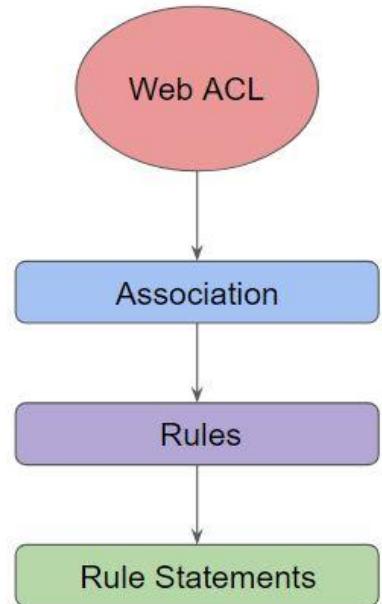
1. If a request comes from 172.30.0.50
2. If requests exceeds 1000 request in 10 minutes



# Web ACL in WAF

Web ACL is a centralized place that contains the rules, rule statements and associated configuration.

It is used to define the protection strategy.

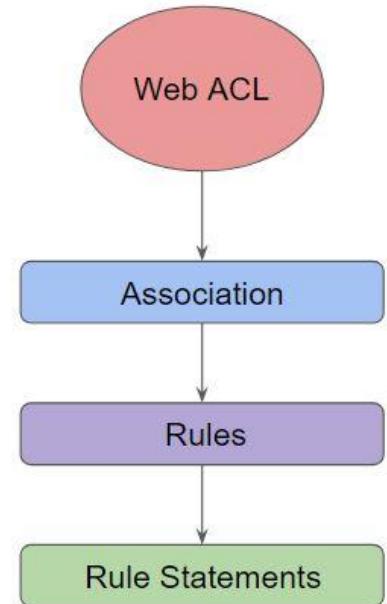


# Association in WAF

Association defines to which entity WAF is associated to.

WAF cannot be associated with EC2 instances directly.

**Support Association:** ALB and CloudFront, API Gateway



# Important Pointers

Rule Groups can be configured which has multiple rules that can be used across multiple Web ACLs.

Customers can decide to use ready-made AWS-Managed rules or even rules from AWS Marketplace.

Every Rule has a priority. If a request matches Priority 0 rule, none of the other rules will inspect the request

Pricing Aspect:

Web-ACL (\$5 per month), Rule (\$1 per month), Requests (\$0.60 / 1 million )

---

# HTTPS

## Secure Communication

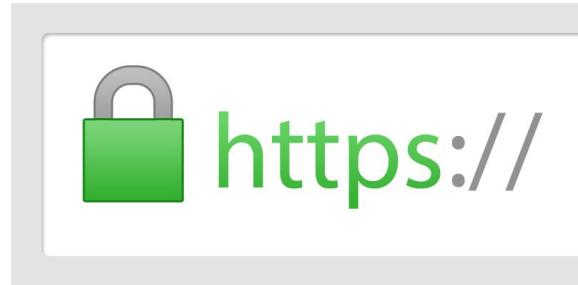
---

# Overview of HTTPS

HTTPS is an extension of HTTP.

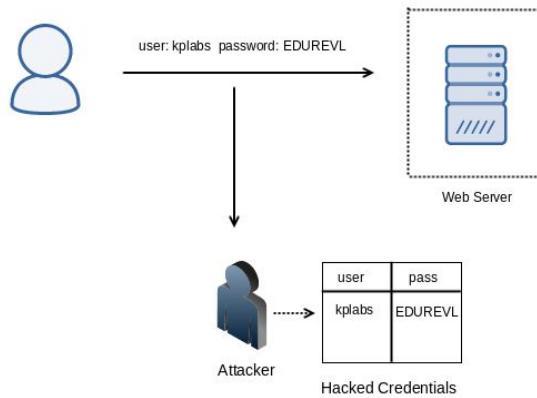
In HTTPS, the communication is encrypted using Transport Layer Security (TLS)

The protocol is therefore also often referred to as HTTP over TLS or HTTP over SSL.



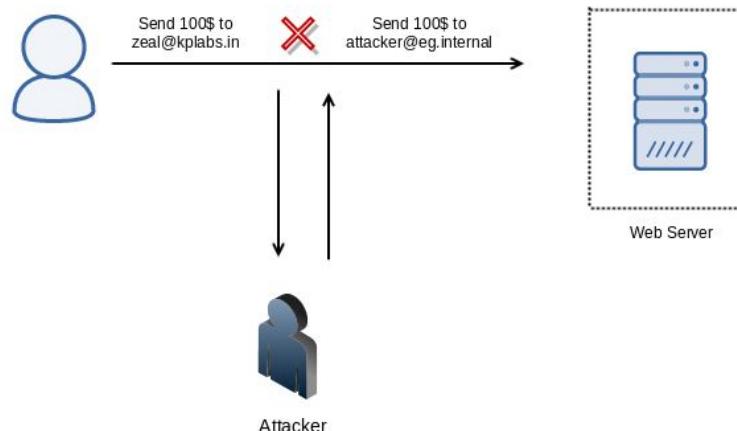
# Scenario 1: MITM Attacks

- User is sending their username and password in plaintext to a Web Server for authentication over a network.
- There is an Attacker sitting between them doing a MITM attack and storing all the credentials he finds over the network to a file:



## Scenario 2: MITM & Integrity Attacks

- Attacker changing the payment details while packets are in transit.



# Introduction to SSL/TLS

To avoid the previous two scenarios (and many more), various cryptographic standards were clubbed together to establish a secure communication over an untrusted network and they were known as SSL/TLS.

Protocol	Year
SSL 2.0	1995
SSL 3.0	1996
TLS 1.0	1999
TLS 1.1	2006
TLS 1.2	2008
TLS 1.3	2018

# Understanding it in easy way

Every website has a certificate (like a passport which is issued by a trusted entity).

Certificate has lot of details like domain name it is valid for, the public key, validity and others.

The screenshot shows a user interface for viewing a certificate's details. At the top, there are tabs for 'General' and 'Details', with 'Details' being the active tab. Below the tabs is a section titled 'Certificate Hierarchy' which displays a tree structure of certificate issuances:

- DST Root CA X3
  - Let's Encrypt Authority X3
    - zealvora.com

Below the hierarchy is a section titled 'Certificate Fields' containing a detailed list of certificate properties:

- zealvora.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info

At the bottom of the interface is a 'Field Value' section.

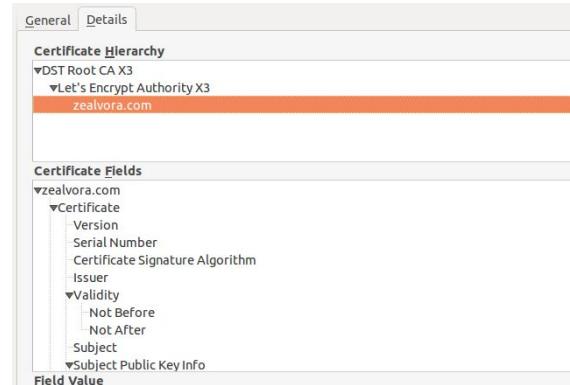
# Understanding it in easy way

Browser (clients) verifies if it trusts the certificate issuer.

It will verify all the details of the certificate.

It will take the public key and initiate a negotiation.

Asymmetric key encryption is used to generate a new temporary symmetric key which will be used for secure communication.



# Web Server Configuration

```
server {
    listen      80;
    server_name zealvora.com;
    return      301 https://$server_name$request_uri;
}

server {
    server_name zealvora.com;
    listen 443 default ssl;
    server_name zealvora.com;
    ssl_certificate /etc/letsencrypt/archive/zealvora.com/fullchain1.pem;
    ssl_certificate_key /etc/letsencrypt/archive/zealvora.com/privkey1.pem;

    location / {
        root /websites/zealvora/;
        include location-php;
        index index.php;
    }
    location ~ /.well-known {
        allow all;
    }
}
```

---

# AWS Certificate Manager

Certificates Again :)

# Earlier Approach

I have a website and I need to use HTTPS. There are two ways, self-signed certificate and the CA signed certificate.



Self Signed Certificate



CA Signed Certificate

# Generating Certificates

To generate a certificate for your domain, you will have to go to a Certificate Authority and after required level of validation, you would be issued a certificate.



User

Generate certificate for kplabs.in



Validated for 1 year.

cert

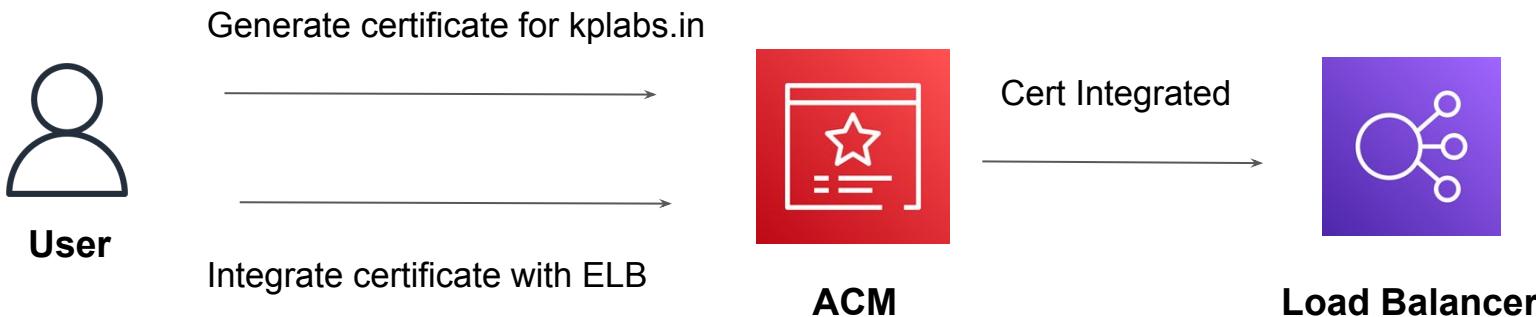
private key



**Certificate Authority**

# AWS Certificate Manager

AWS Certificate Manager (ACM) handles the complexity of creating, storing, and renewing public and private SSL/TLS X.509 certificates and keys that protect your AWS websites and applications.



# High-Level Flow Logs Format

version	- The VPC Flow Logs Version
account-id	- AWS Account ID
interface-id	- The network interface id
srcaddr	- The source address
destaddr	- Destination Address
src port	- Source Port
dest port	- Destination Port
protocol	- The protocol number
packets	- Number of packets transferred
bytes	- Number of bytes transferred
start	- Start time in unix seconds
end	- End time in unix seconds
action	- ACCEPT or REJECT
log status	- Logging status of flow log

2 7742829482 eni-4d788e3d 115.73.149.218 10.0.5.157 12053 23 6 2 88 1485439809 1485440090 REJECT OK

## Type of Traffic Not Logged

Flow logs do not capture all IP traffic. Some of these include:

- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
- Traffic generated by a Windows instance for Amazon Windows license activation.
- Traffic to and from 169.254.169.254 for instance metadata.
- DHCP traffic.

---

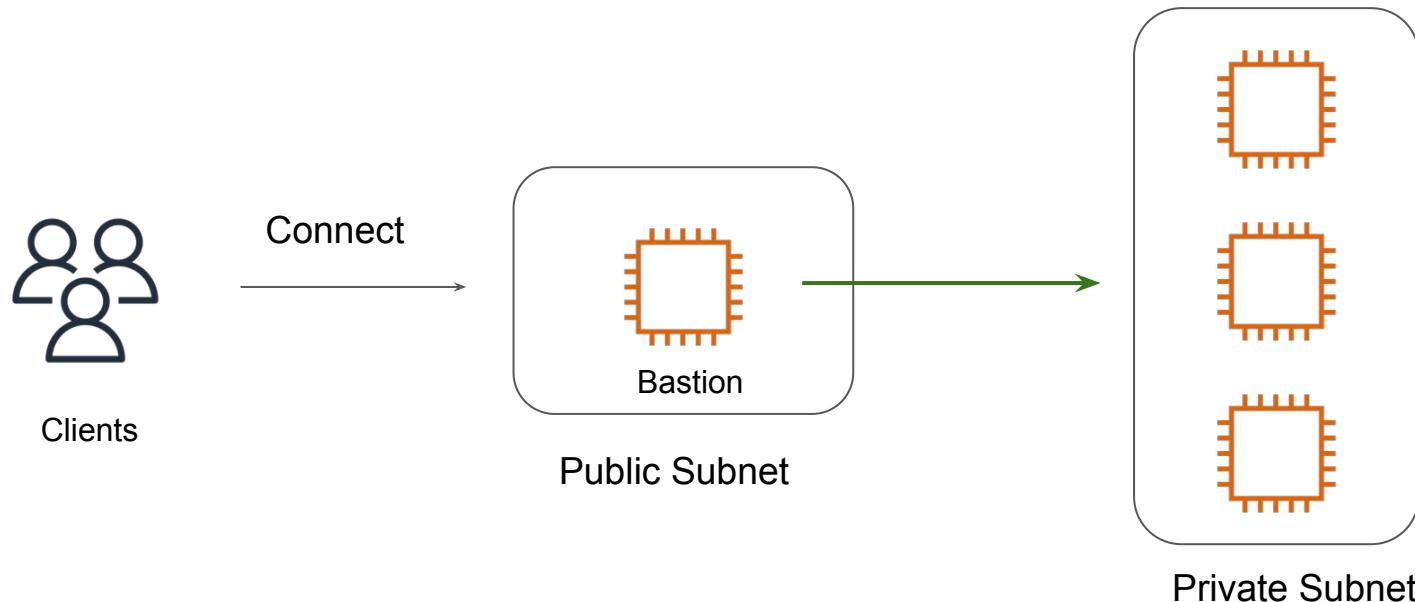
Bastion Host

Time to Defend

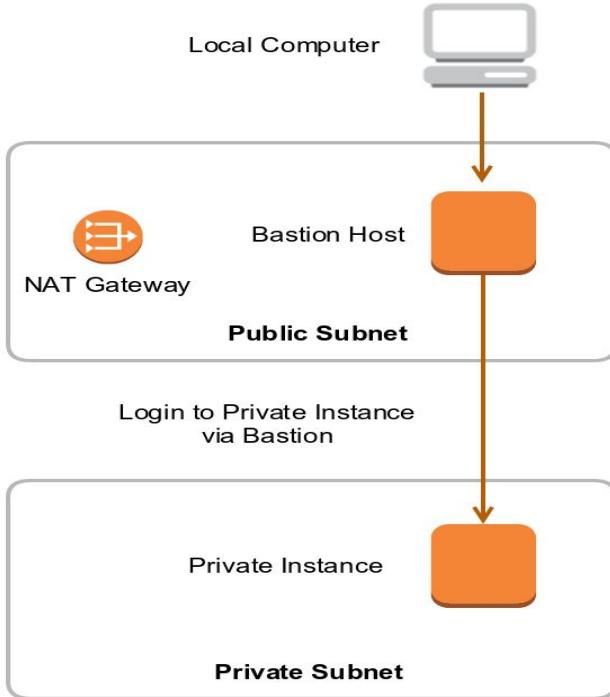
---

# Basics of Bastion Hosts

Bastion hosts also referred as jump box acts like a proxy server and allows the client machines to connect to the remote server in the private subnets.



# The Bastion Host



- Bastion Host → “Jump Box” from public to private subnet.
- User needs to have access for jump box and the private instance.

# The Security of Jump Box

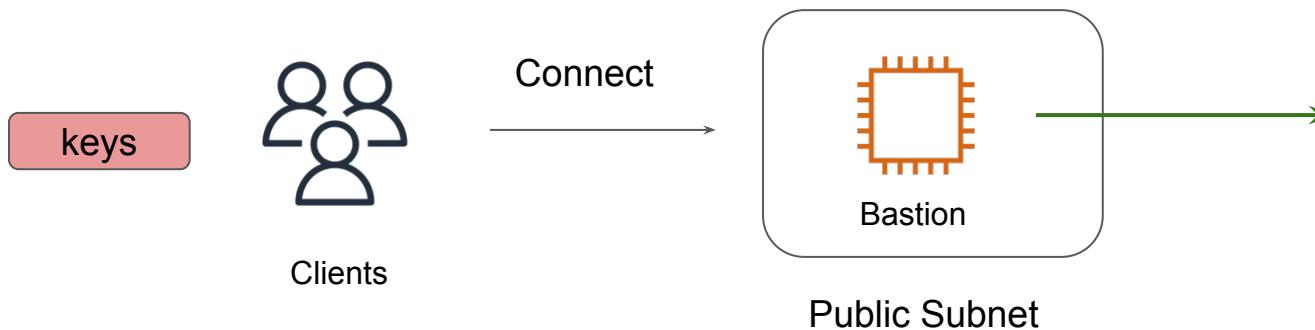
- All the unnecessary packages should be removed in the Bastion machine to minimize the attack surface area.
- Proper Server Hardening should be applied to the Bastion Host.
- Private Keys should never be stored on the bastion. We should use “Agent Forwarding” for Linux instances.

# Challenge with this Setup

Every user have private keys stored securely on their laptop.

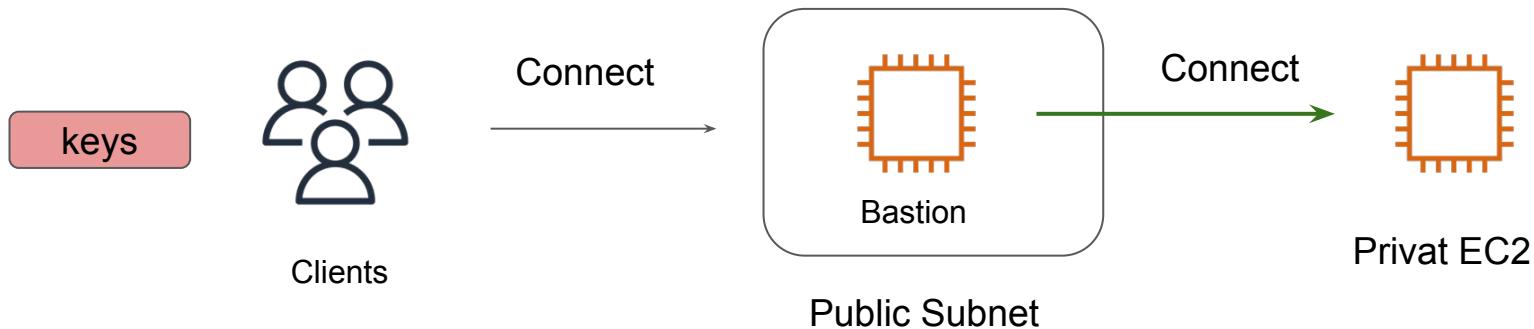
This private key can be used to connect to Bastion Host.

Once logged into Bastion, how will he login to private EC2 instance?



# SSH Agent Forwarding

SSH Agent forwarding allows users to use their local SSH keys to perform some operation on remote servers without keys being left from your workstation.



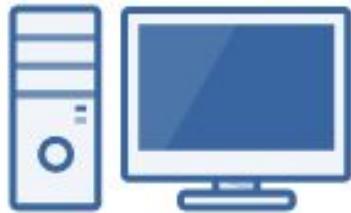
---

# Virtual Private Network

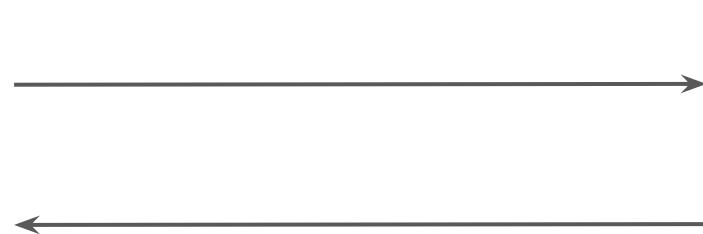
Let's Route

# VPN

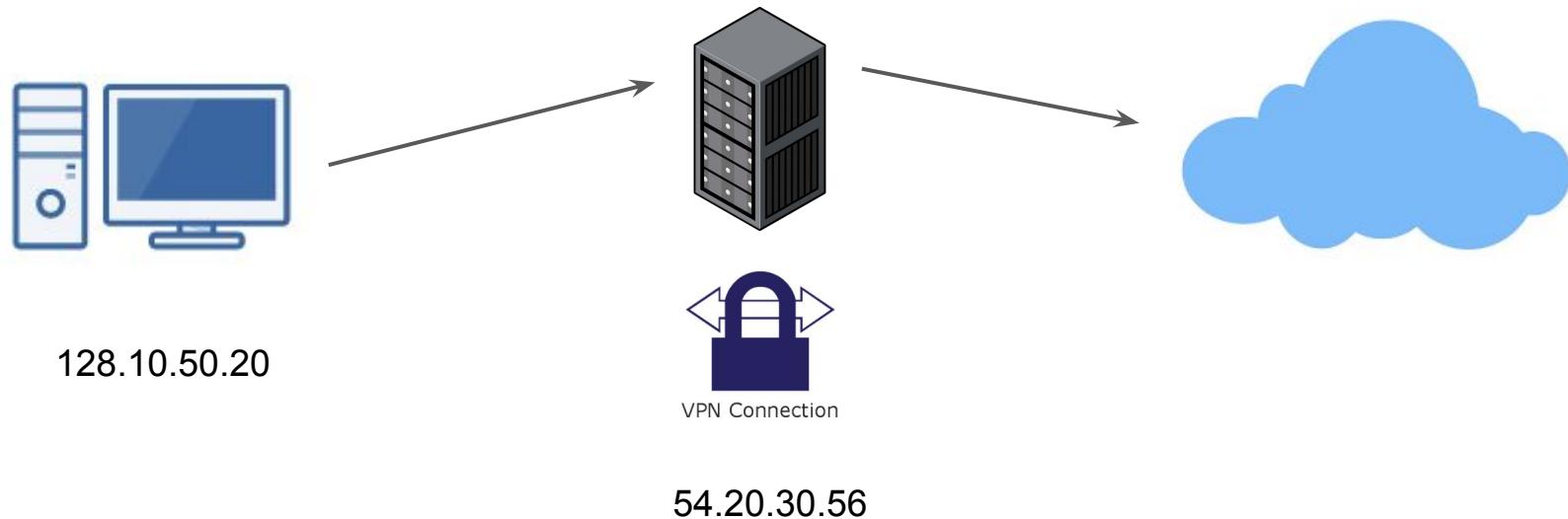
- VPN enables you to route traffic from yourself towards destination through itself.
- Something similar to Proxy.



128.10.50.20

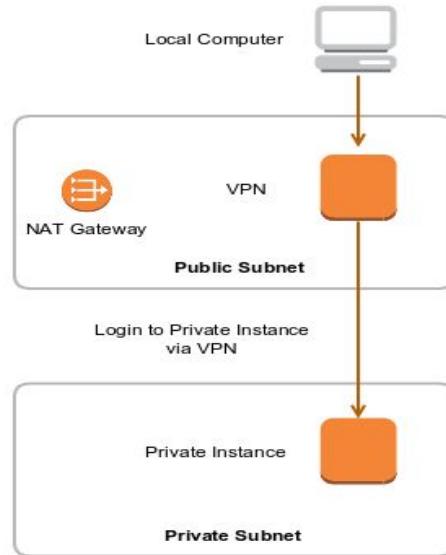


# Routing via VPN Server



# VPN use in Corporate Network

- In Corporate environments, VPN is used to connect to instances in Private Subnet.
- VPN Server resides in the Public Subnet and you route your traffic via VPN server to instances in Public Subnet.



---

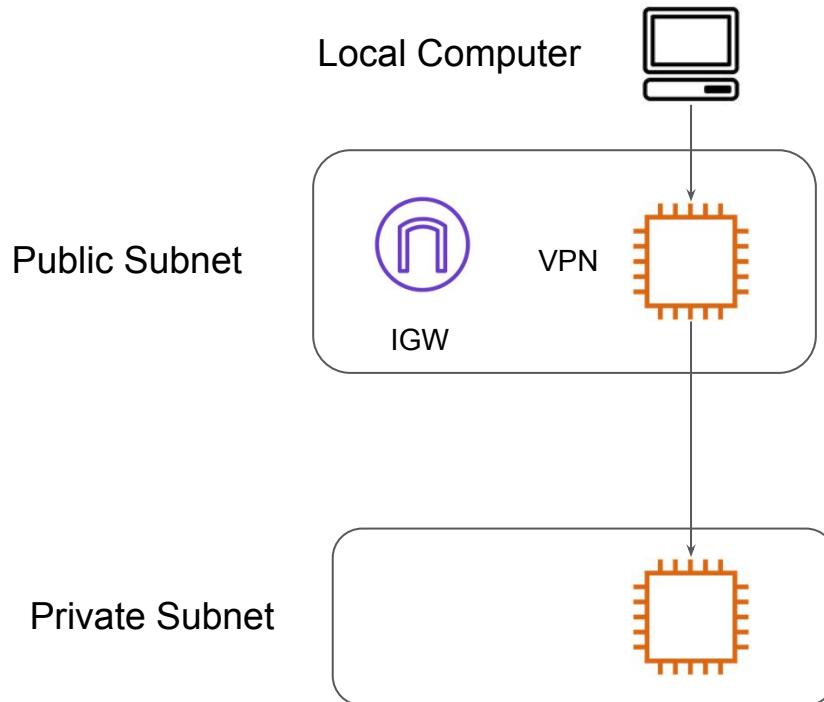
# AWS Client VPN

Creating our First VPN in AWS

---

# EC2 Based VPN Architecture

In this approach, you install VPN softwares like OpenVPN in the EC2 instance and use it to route traffic to private subnets.

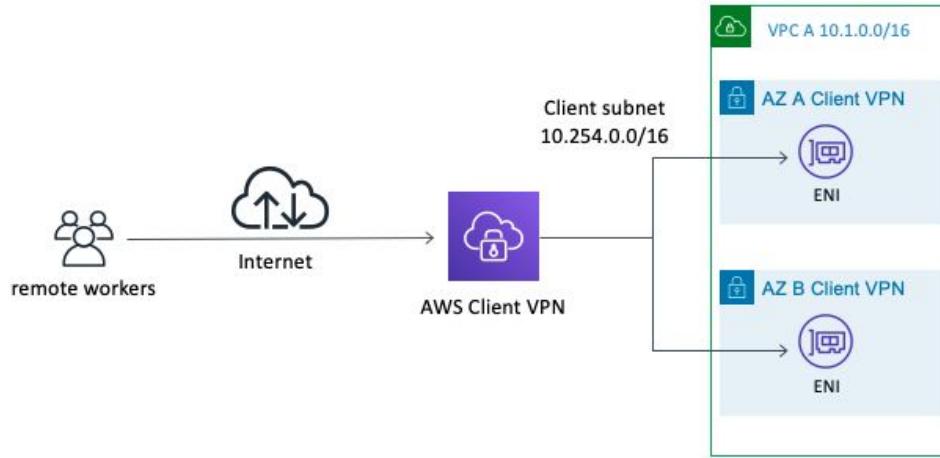


# Challenges with EC2 VPN Based Architectures

1. High-Availability (What if VPN EC2 goes down)
2. Patch Management.
3. Upgrade of VPN Software
4. Performance Optimization
5. VPN Server Configuration

# AWS Client VPN

AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources and resources in your on-premises network.



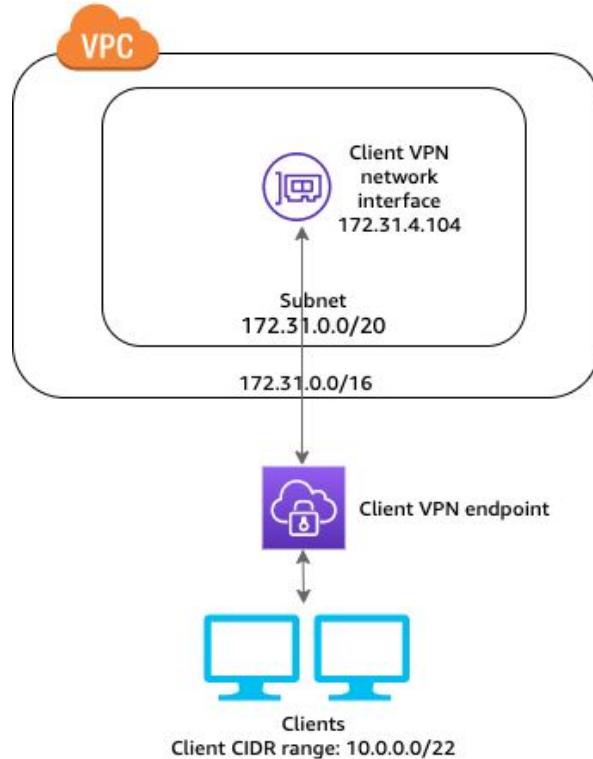
---

# ClientVPN Connectivity Architectures

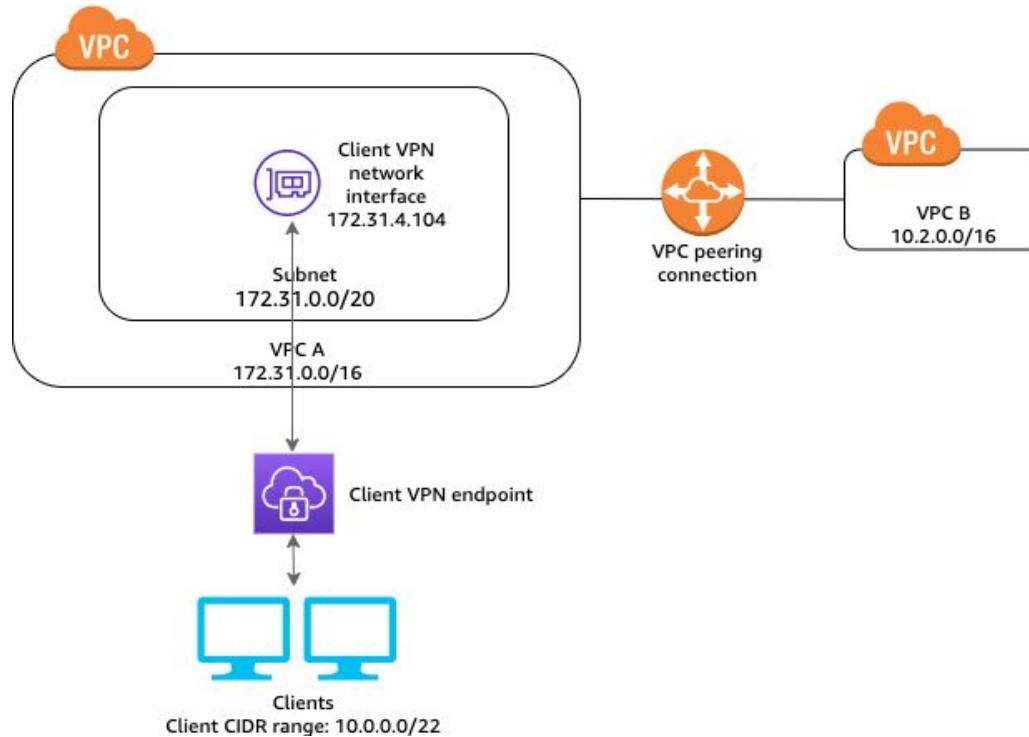
Connecting ClientVPN to Endpoints

---

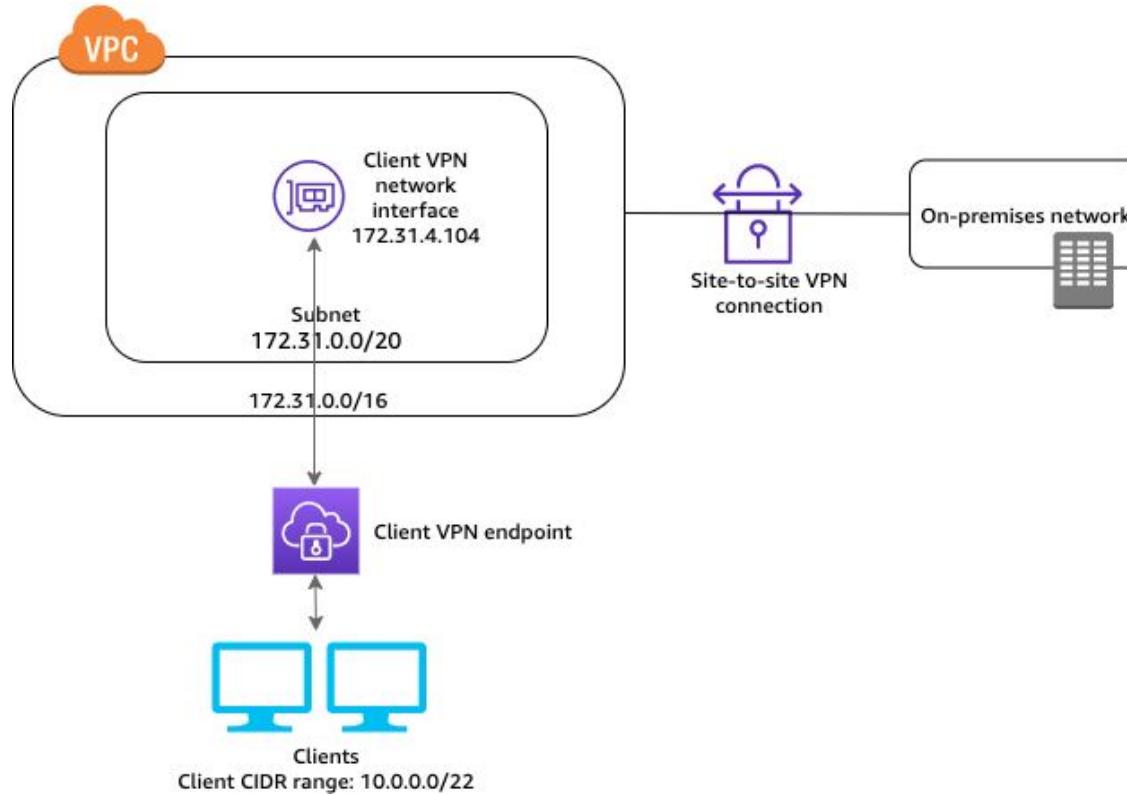
# 1 - Access to VPC



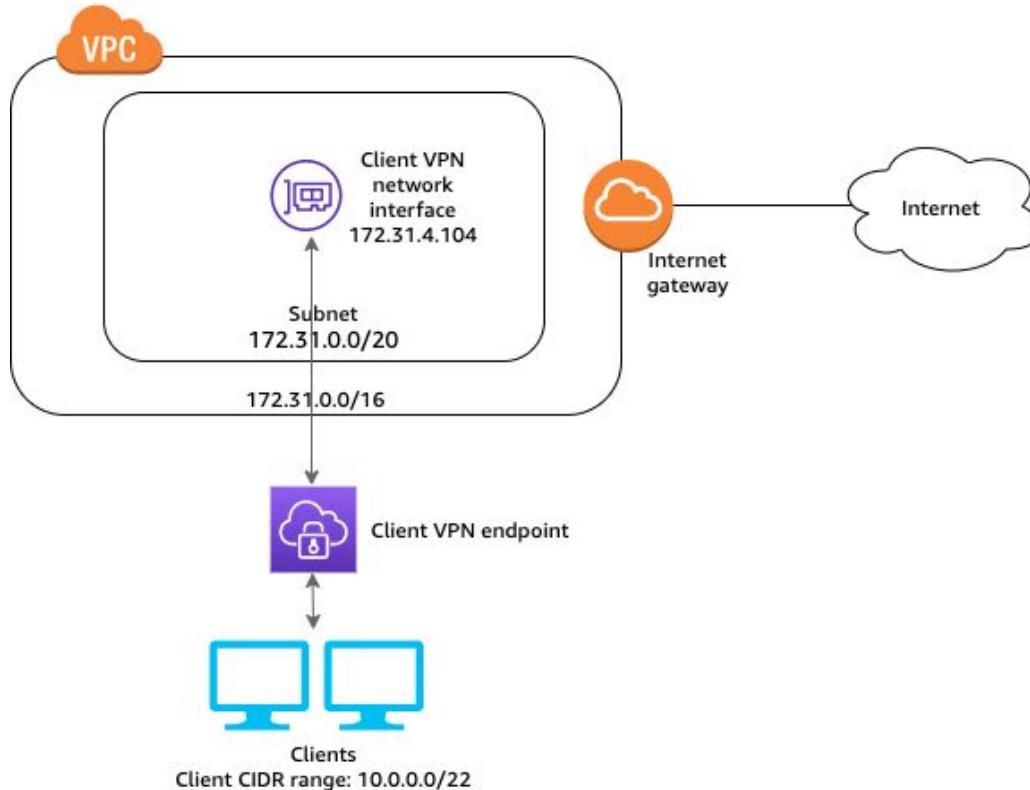
## 2- Access to Peered VPC



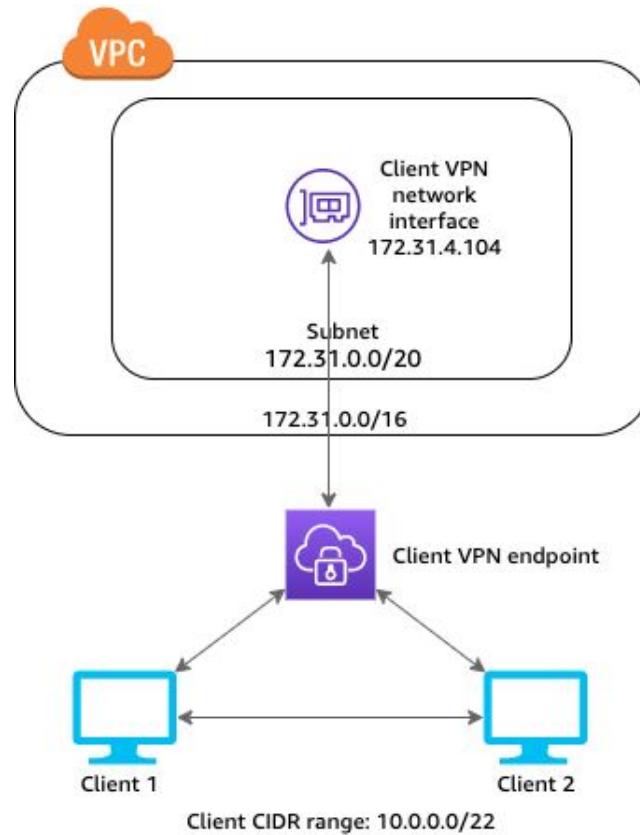
# 3 - Access to On-Premise Network



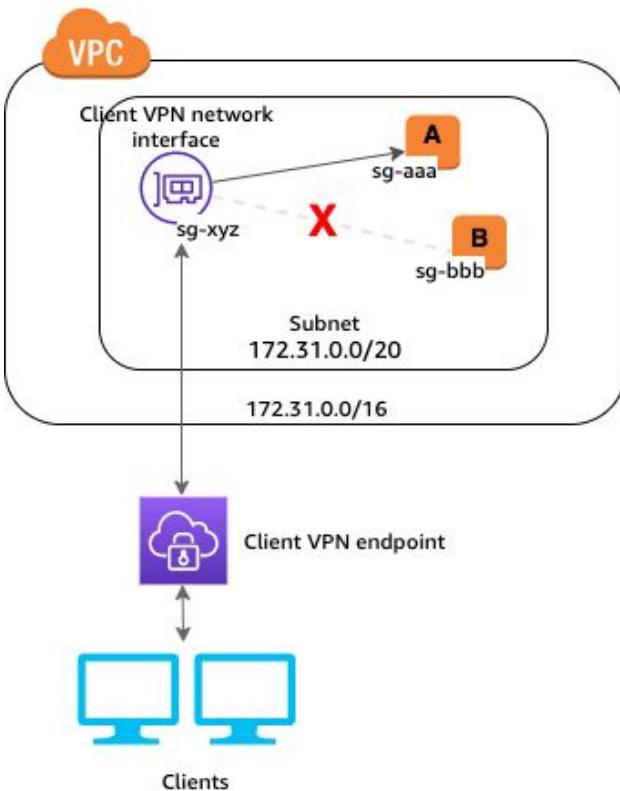
## 4 - Access to Internet



## 5 - Client to Client Access



## 6 - Restrict access using security groups



---

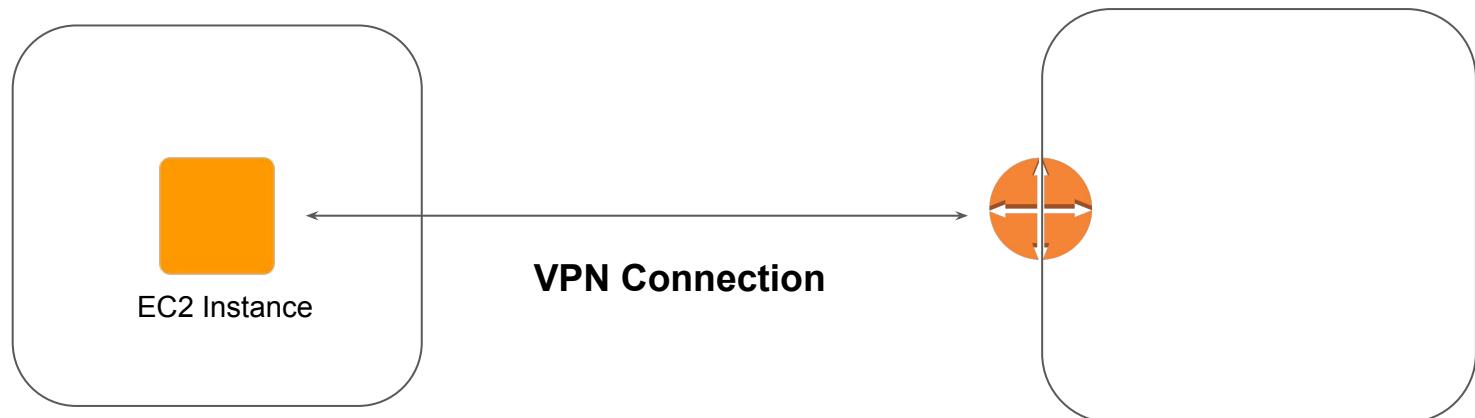
# Site to Site Tunnel

Let's Route

# Site to Site VPN

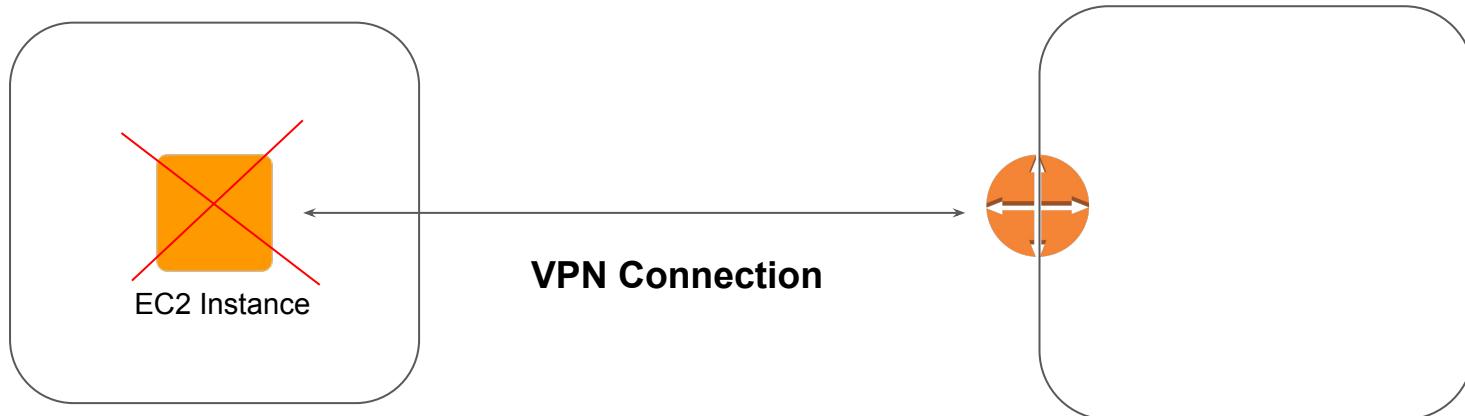
A Site to Site (S2S) VPN allows two networking domains to communicate securely between each other over an untrusted network like Internet.

The two sites can be AWS and on-premise data-center or even two different VPC's.

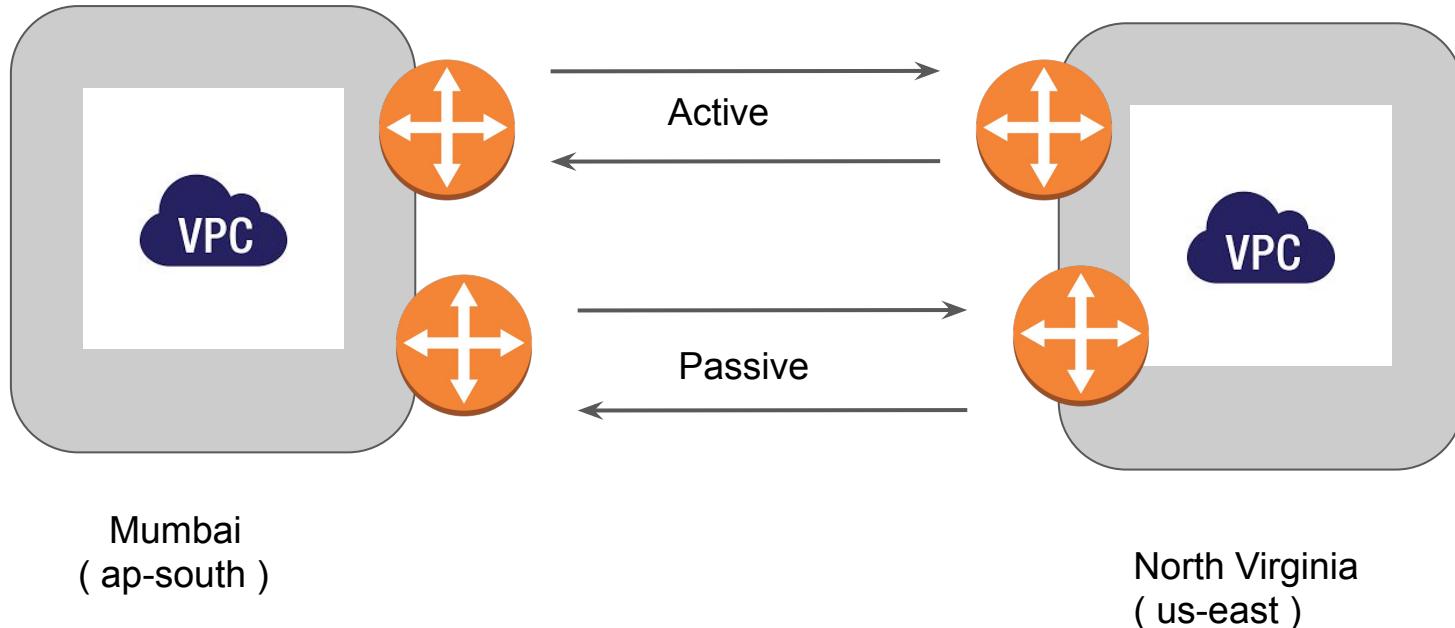


# Availability Challenges in S2S VPN

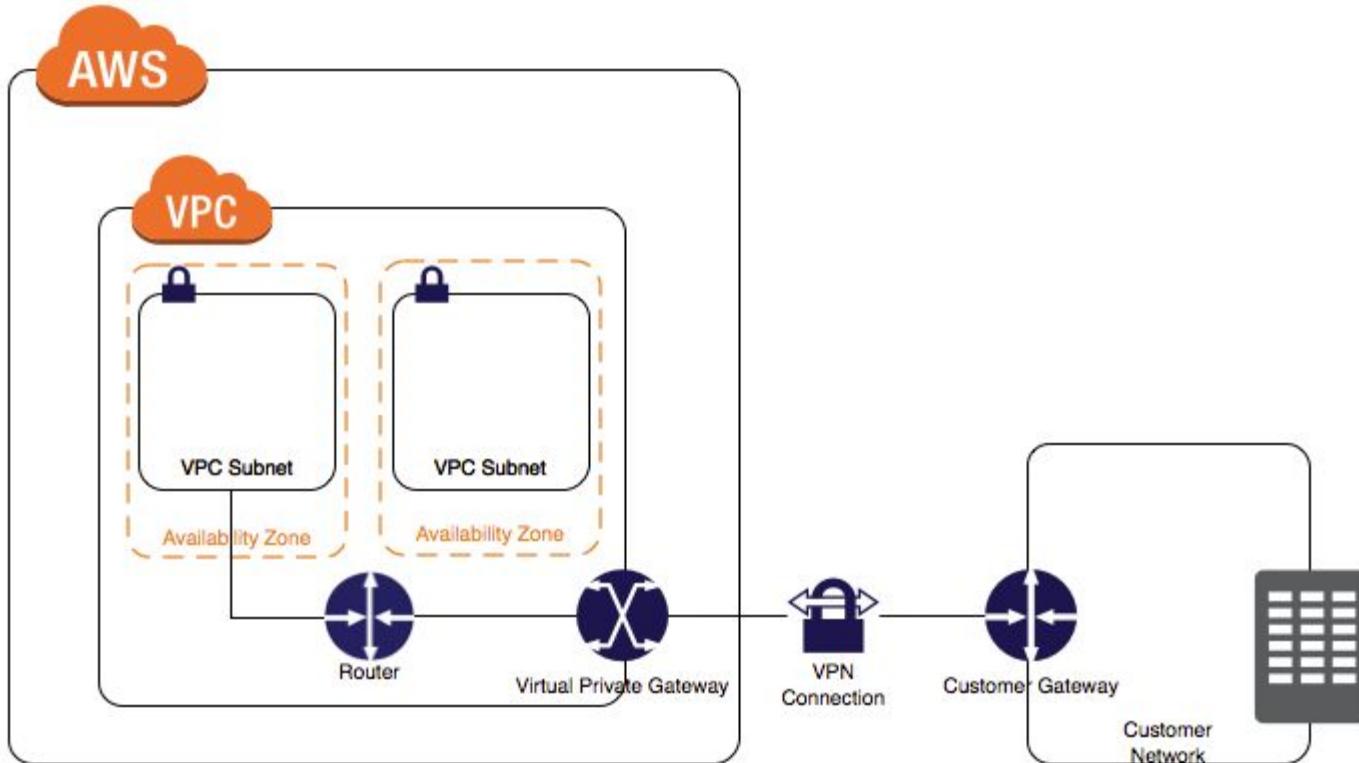
If you have a single tunnel endpoint and if one of the side goes down, then the entire tunnel breaks.



# High Availability in S2S VPN

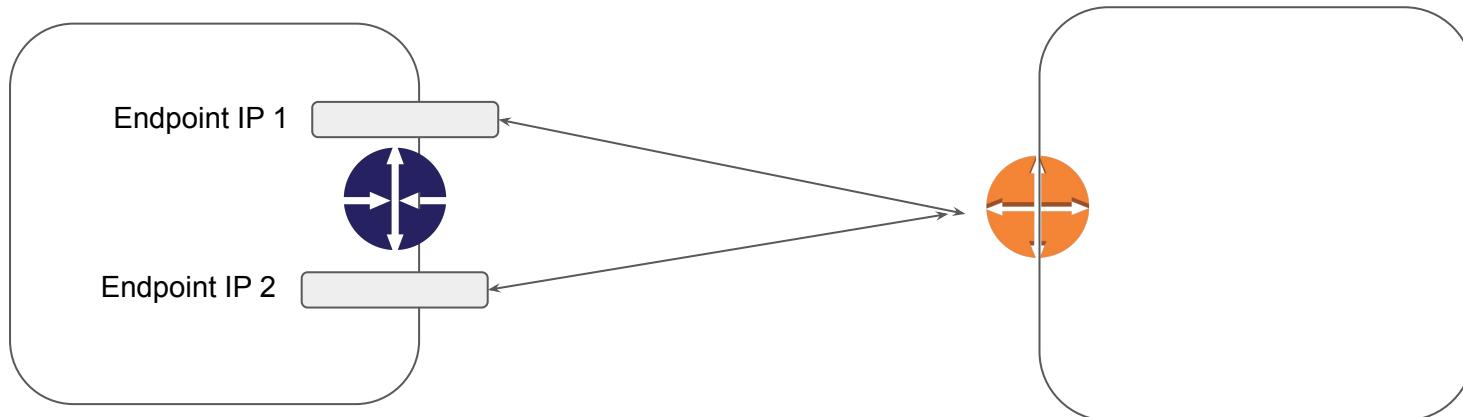


# Site to Site VPN



# Importance of VGW

- A Virtual Private Gateway (VGW) has built-in high-availability for VPN connection.
- AWS automatically creates 2 HA endpoints, each in a different AZ.



**VPN Connection = 2 VPN Tunnels**

# Importance of VGW

The screenshot shows a CloudWatch interface with a table of VPN connections and a detailed view of one connection.

**Table Headers:**

- Name
- VPN ID
- State
- Virtual Private Gateway
- Customer Gateway

**Table Data:**

Name	VPN ID	State	Virtual Private Gateway	Customer Gateway
ohio-mumbai	vpn-5cdf0a6b	available	vgw-7072fd40   ohio-mumbai	cgw-27058b17   ohio-mumbai

**VPN Connection Details:**

**VPN Connection:** vpn-5cdf0a6b

**Tunnel Details:**

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
18.216.150.193	169.254.59.32/30	UP	December 24, 2017 at 7:42:19 PM U...	-
18.220.211.76	169.254.57.128/30	DOWN	December 24, 2017 at 7:36:56 PM U...	-

# Relax and Have a Meme Before Proceeding

That stupid walk you do when  
someone's mopping a floor and you  
know you're gonna walk over it but you  
want them to see how sorry you are to  
be walking over it so you make  
yourself look like you're walking over  
hot lava.



It ain't much, but it's honest work

---

# VPN Performance

## Performance Aspects

# Getting Started

When we create an AWS VPN, AWS provides two different VPN endpoints.

Name	VPN ID	State	Virtual Private Gateway	Customer Gateway
ohio-mumbai	vpn-5cdf0a6b	available	vgw-7072fd40   ohio-mumbai	cgw-27058b17   ohio-mumbai

VPN Connection: vpn-5cdf0a6b

Details Tunnel Details Static Routes Tags

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
18.216.150.193	169.254.59.32/30	UP	December 24, 2017 at 7:42:19 PM U...	-
18.220.211.76	169.254.57.128/30	DOWN	December 24, 2017 at 7:36:56 PM U...	-

# Important Pointers

The VGW supports IPSec VPN's throughput of up to 1.25 Gbps.

To increase the bandwidth, you can forward the traffic to both the endpoints.

To support the above design, the Customer Gateway (CGW) should support Equal Cost Multipath (ECMP) to load balance traffic across both the links.

**Important:**

ECMP is not supported on latest AWS VPN (only classic VPN)

---

# NAT Gateway Performance

Multiple is better

---

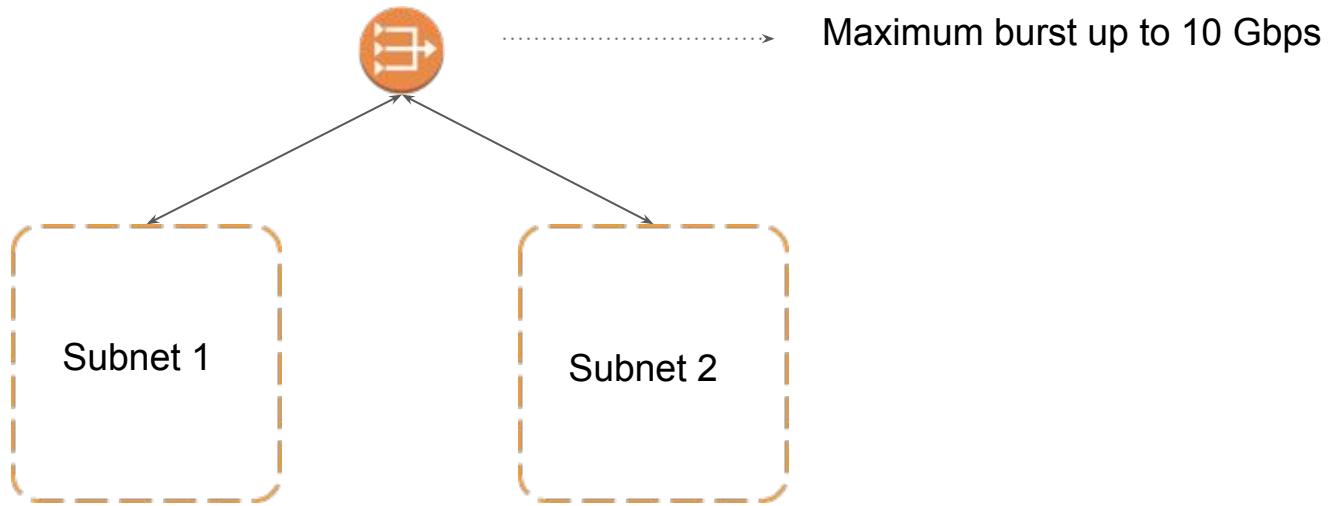
## Performance Aspect

NAT Gateway supports a burst of up to 10 Gbps of bandwidth.

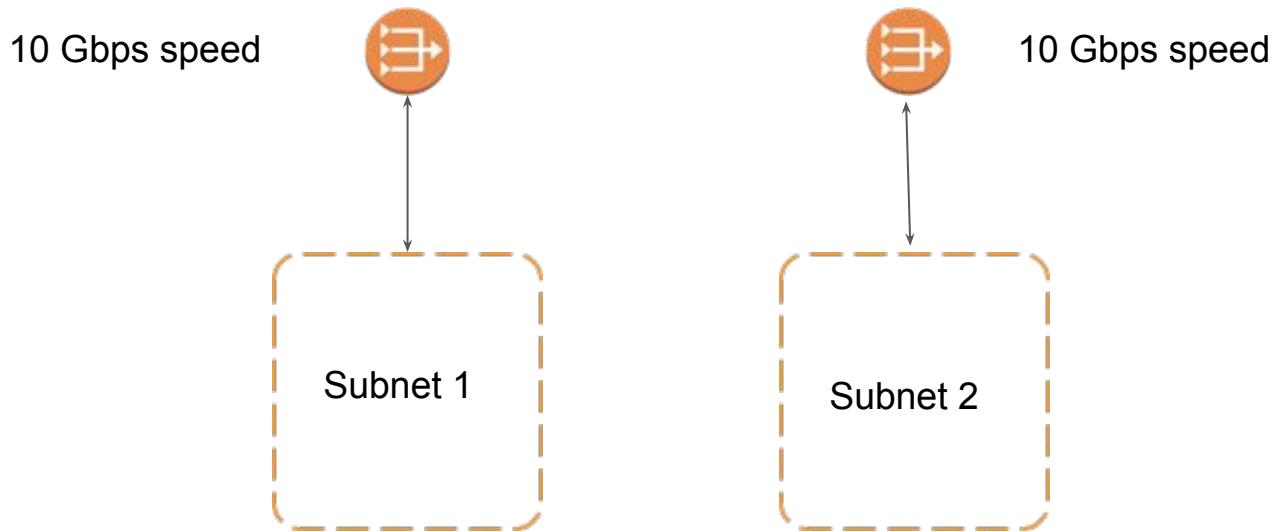
Thus all the instances within the private subnet need to have traffic less than that of 10 Gbps. If more than 10 Gbps, then the network will be the bottleneck.

Thus when we need more bandwidth, than the recommended design is to split the instance across multiple subnets and attach different NAT gateway to each of those subnets.

# Normal NAT Gateway based Architecture



# Multiple NAT Gateway Approach



---

# Static Routing

Traffic Path

---

# Real World Scenario

In one of my recent trip in scooty, I travelled 400 kms in a day from Coimbatore to Bangalore. One of the only support was the sign boards which tells which direction I should be going.



# Static Routing

[Static routing](#) is a form of routing which occurs when router uses manually-configured routes.

In many of the cases, these static routes are manually configured by the network administrator by manually adding it into the route table.



# Disadvantages

Static routing are more for small networks, when it comes to larger ones, these are not the ideal solution. Here are some of the disadvantages of static routes:

- i) **Human Error:** In case of manually configured, due to mistyping the route will remain down.
- ii) **Fault Tolerance:** If there is issue in network between two static device, traffic will not be re-routed. Thus network will remain unusable till that time.
- iii) **Administrative overhead:** Static routes must be configured at each router in the network. This configuration takes lot of time if there are many routers.

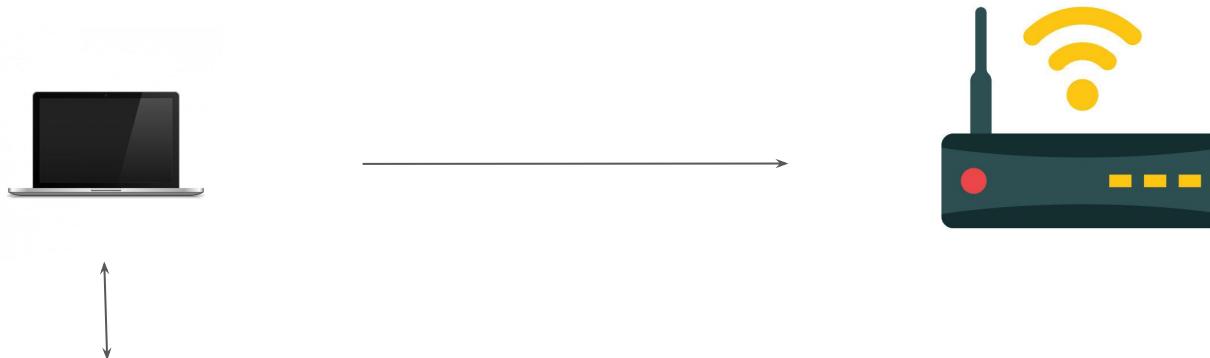
---

# Dynamic Routing

Changing Traffic Path

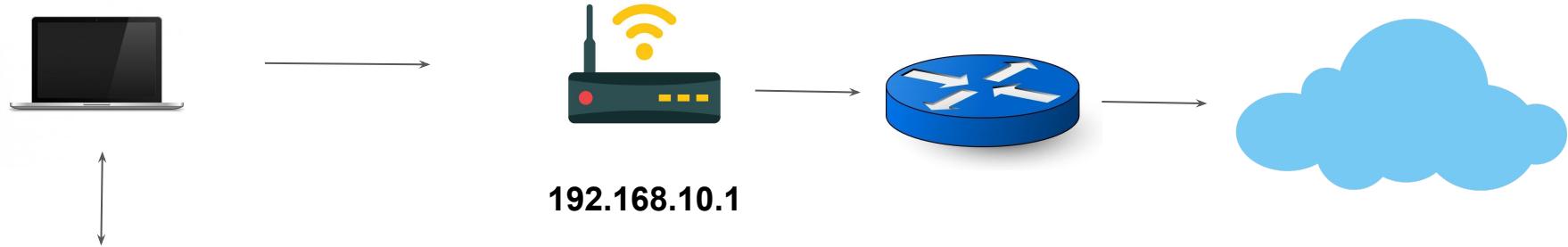
---

# Static Routing



192.168.0.1

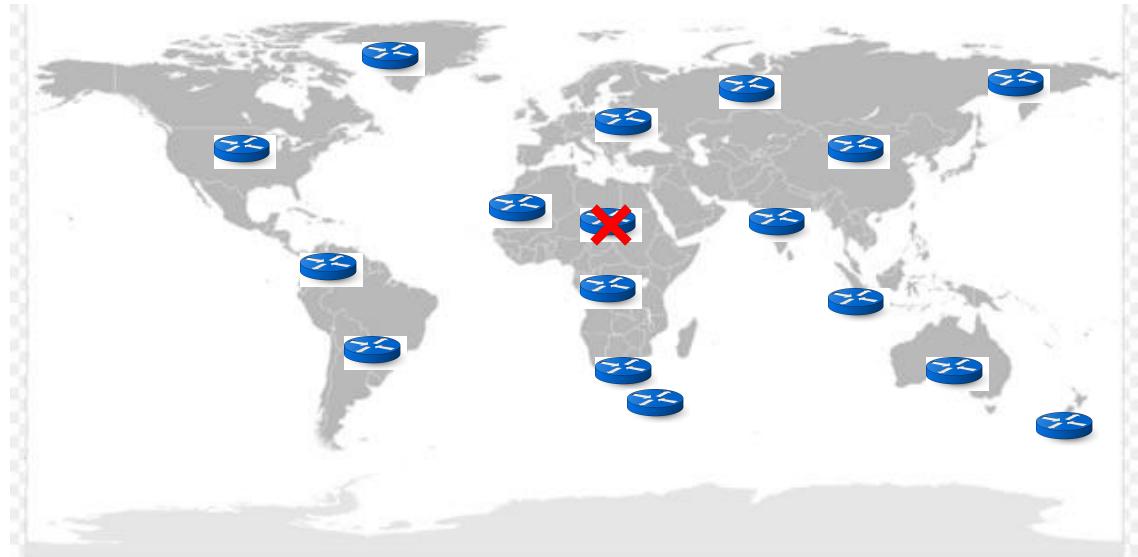
# Static Routing



Route	Destination
0.0.0.0	192.168.0.1

Route	Destination
0.0.0.0	116.25.0.1

# Dynamic Routing

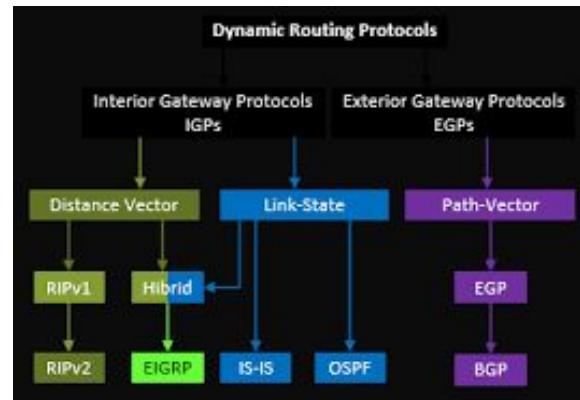


# Dynamic Routing Protocols

Dynamic Routing (also called as adaptive routing) can forward data via different route based on current conditions of communication networks.

There are several protocols that are used for dynamic routings like RIP, OSPF, BGP.

BGP is one of the protocols for external dynamic routing and thus is also called as “Routing Protocol for the Internet”



---

# Border Gateway Protocol

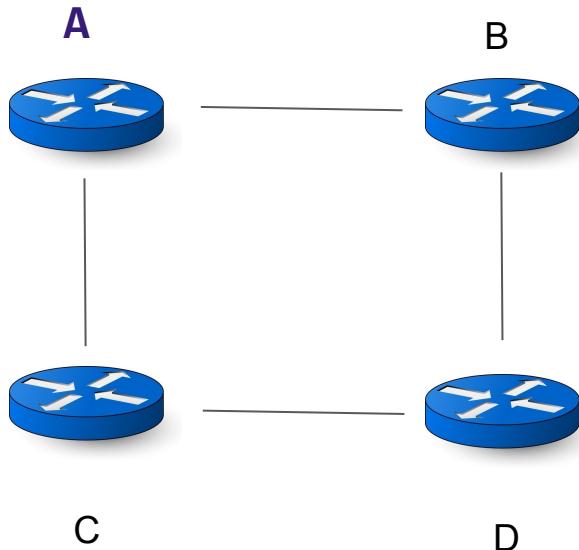
Exterior Routing

---

# Dynamic Routing

BGP is an exterior dynamic routing protocol which generally figures out on how the packet can further go out to the internet.

Router	Hop
B	1
C	1



Router	Hop
A	1
D	1
C	2 (via A)

Router	Hop
B	1
C	1
A	2 (via B)

---

# Autonomous System

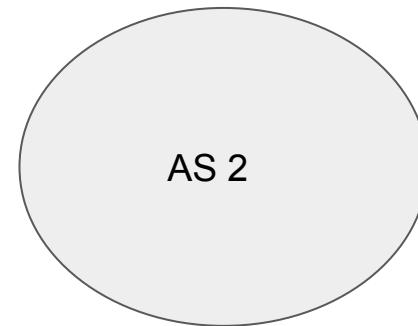
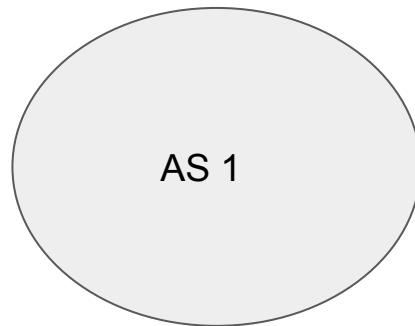
## Routing Arena

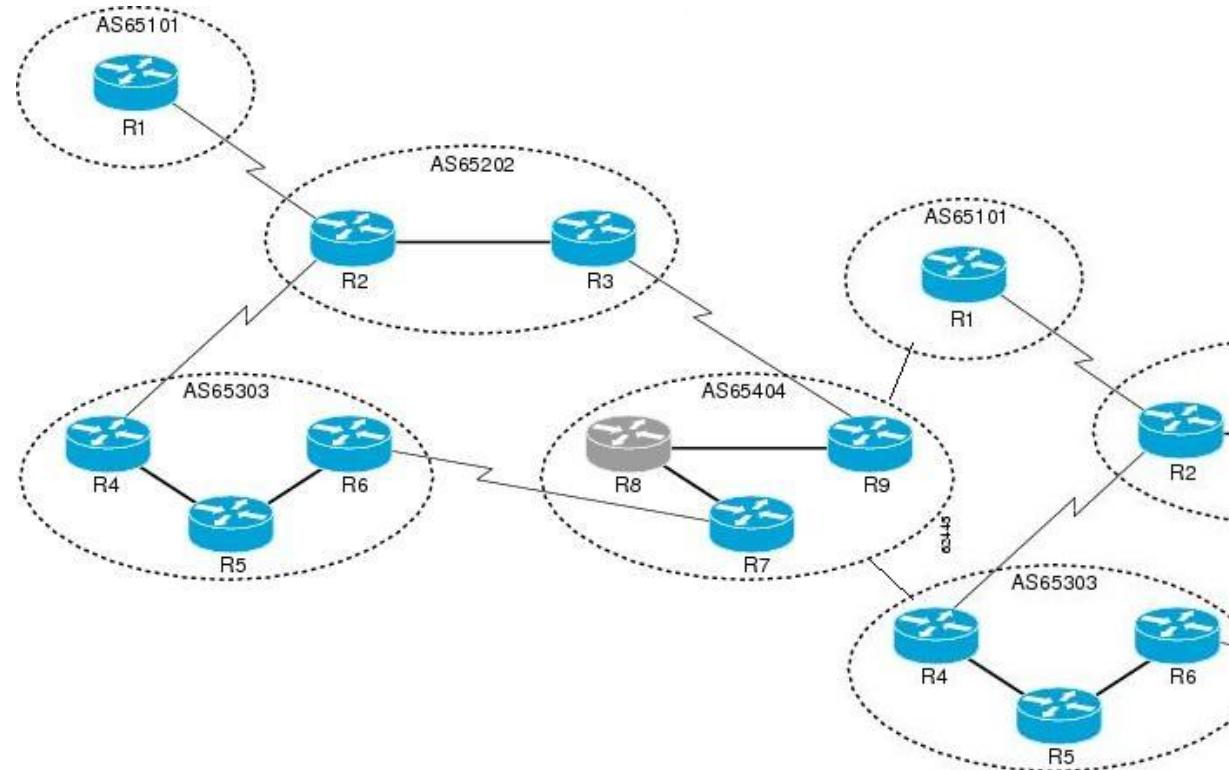
# Getting The Basics

An Autonomous System (AS) is a group of networks under a single administrative control.

This could be an Internet Service Provider (ISP) or a large Enterprise Organization.

Internet consist of a network of computer networks also referred as autonomous systems.

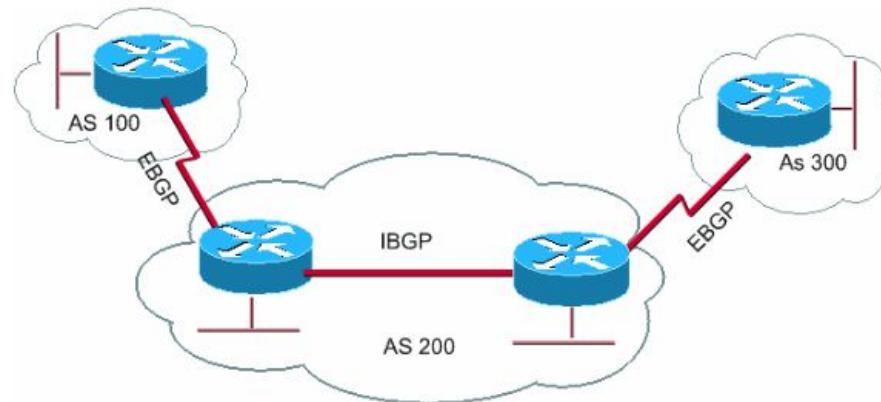




# IBGP and EBGP

If a BGP session is established between two neighbors in different autonomous systems, the session is external BGP (EBGP)

If the session is established between two neighbors in the same AS, the session is internal BGP (IBGP).

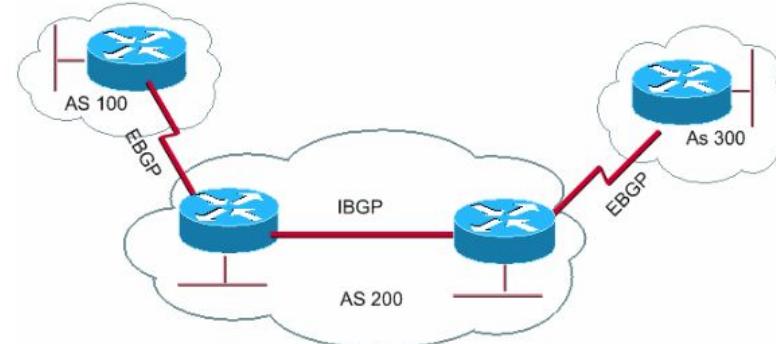


# ASN Numbers

An autonomous system number (ASN) is a unique number assigned to an autonomous system (AS) by the Internet Assigned Numbers Authority (IANA).

The Autonomous System Number (ASN) value 0 is reserved, and the largest ASN value 65,535, is also reserved (16 bit integers). The last ASN of the 32-bit numbers (4,294,967,295) are reserved and should not be used by operators.

The values, from 1 to 64,511, are available for use in Internet routing, and the values 64,512 to 65,534 is designated for private use.



# ASN Table

Number	Bits	Description	Reference
0	16	Reserved	RFC1930, RFC7607
1 - 23455	16	Public ASN's	
23456	16	Reserved for AS Pool Transition	RFC6793
23457 - 64495	16	Public ASN's	
64496 - 64511	16	Reserved for use in documentation/sample code	RFC5398
64512 - 65534	16	Reserved for private use	RFC1930, RFC6996
65535	16	Reserved	RFC7300
65536 - 65551	32	Reserved for use in documentation and sample code	RFC4893, RFC5398
65552 - 131071	32	Reserved	
131072 - 4199999999	32	Public 32-bit ASN's	
4200000000 - 4294967294	32	Reserved for private use	RFC6996
4294967295	32	Reserved	RFC7300

---

# BGP Path Selection Algorithms

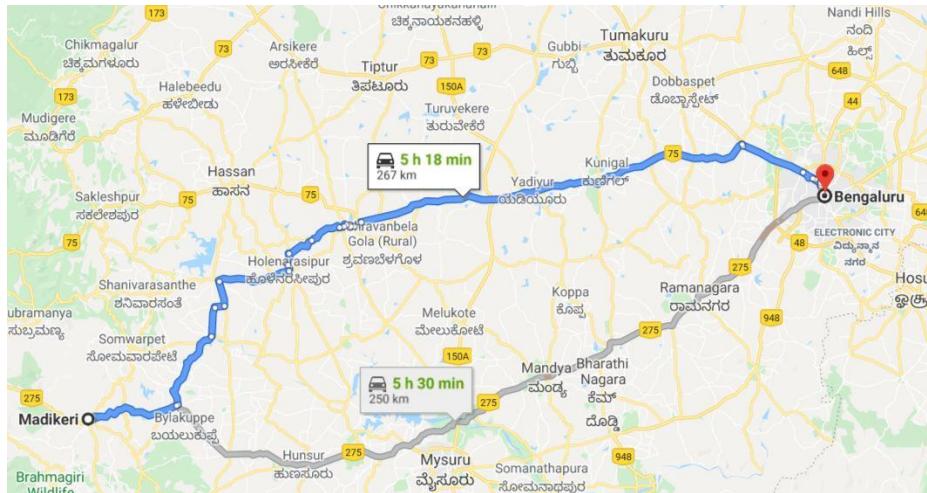
More BGP

---

# Simple Analogy - Google Map

When travelling from Point A to Point B, Google Maps shows the optimum route.

But if needed, you can also travel via different route depending on your preference and use-case.

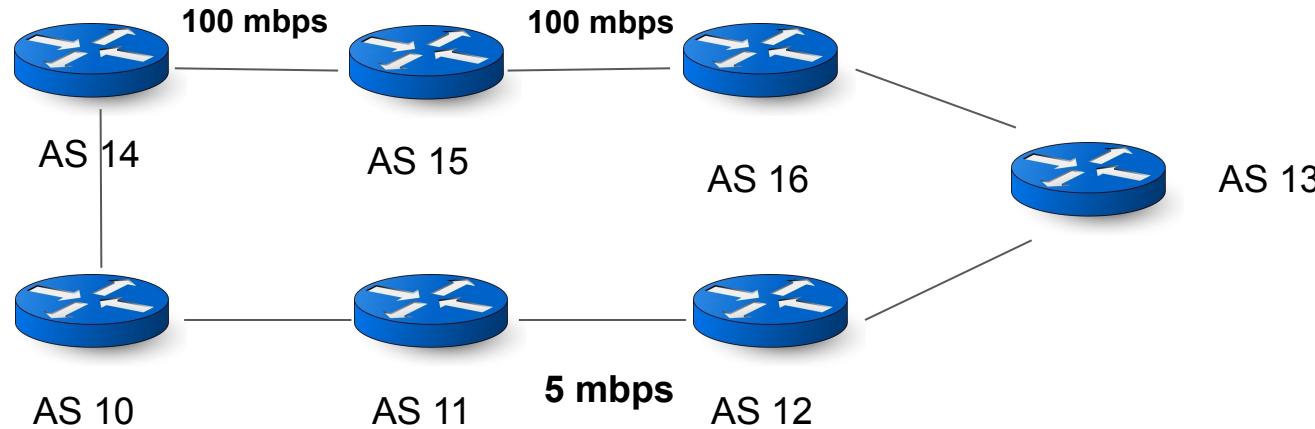


# Understanding the Challenge

- BGP prefers the shortest AS path to get to a destination.
- When we calculate distance between hops, it might not always be the best approach.

Let's assume AS 10 want sto connect to AS 13.

- 1 - AS 10 → AS 11 → AS 12 → AS 13
- 2 - AS 10 → AS 14 → AS 15 → AS16 → AS13

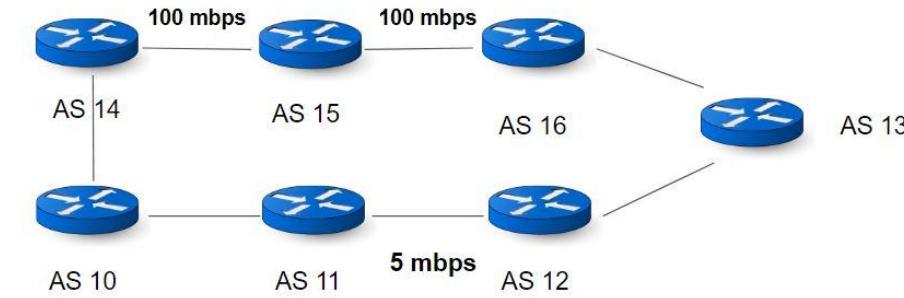


# AS\_Path Prepending

Since BGP prefers shorter AS path, we can influence this decision by adding own ASN number multiple times so the path becomes longer.

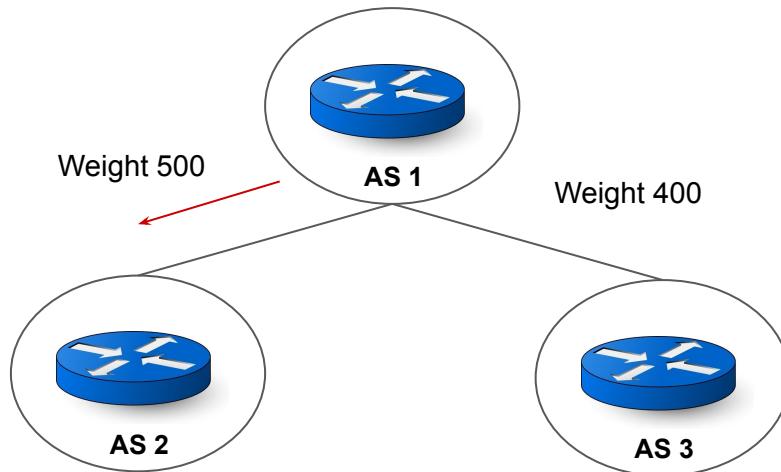
Router will assume that there are more AS in the path can will avoid the route.

- 1 - AS 10 → AS 10 → AS 10 → AS 10 → AS 11 → AS 12 → AS 13
- 2 - AS 10 → AS 14 → AS 15 → AS16 → AS13



# Weights

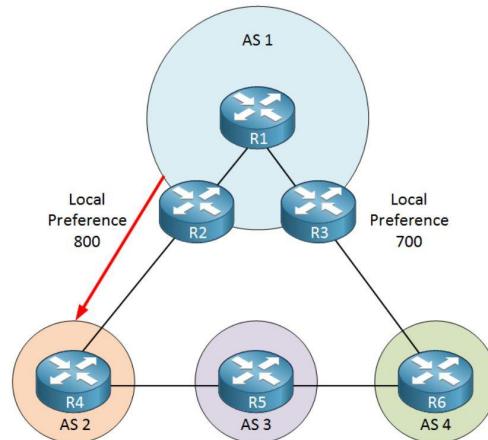
- Weight attribute assigns a weight based on which a specific path is preferred.
- It is a Cisco proprietary attribute, so you won't find it in other vendors.
- Local to the Router
- The path with the highest weight is preferred.



# LOCAL\_PREF

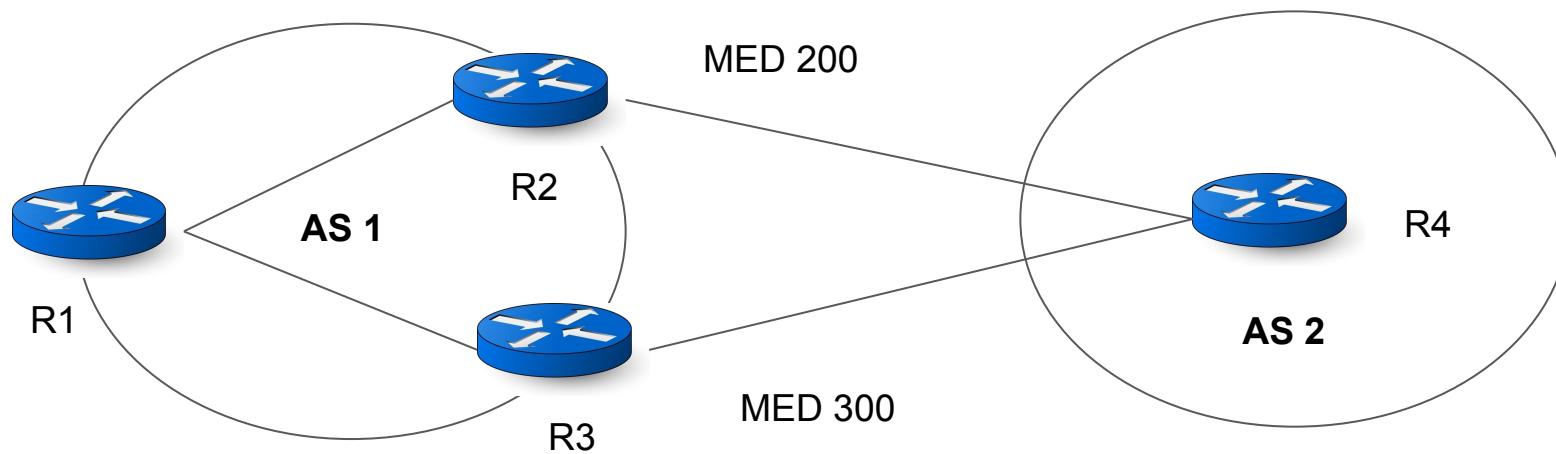
LOCAL\_PREF does a similar thing as that of the Weight attribute.

If set, local preference is exchanged between all internal BGP routers.



# MED Attribute

- MED Attribute determines how neighbors enters an Autonomous System.
- MED attribute is exchanged between autonomous systems.
- In the below example, R4 will prefer to enter AS1 via R2



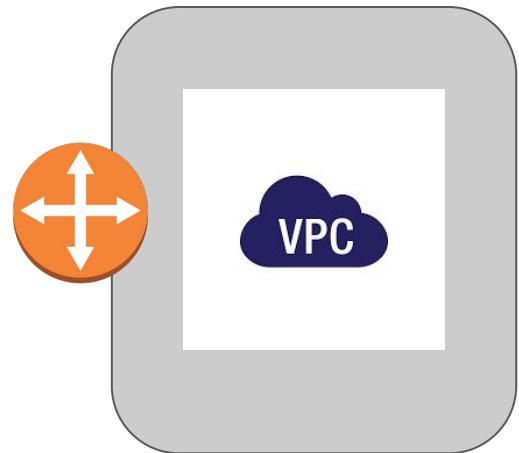
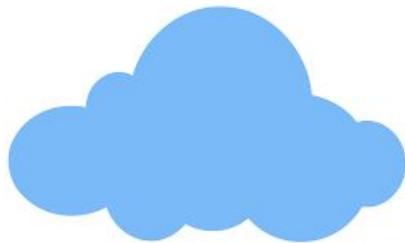
---

# Direct Connect

## Let's Route Centrally

---

# Customer to VPC

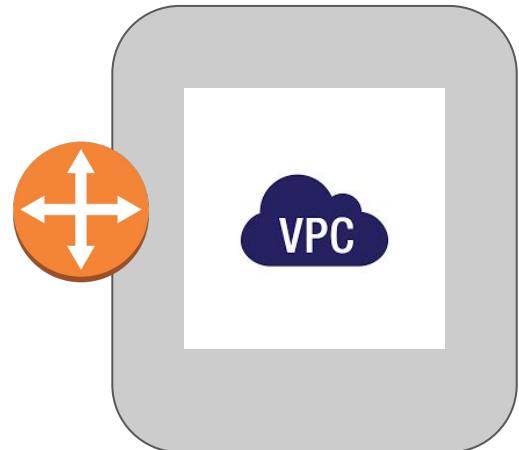


Packets travels via Hops



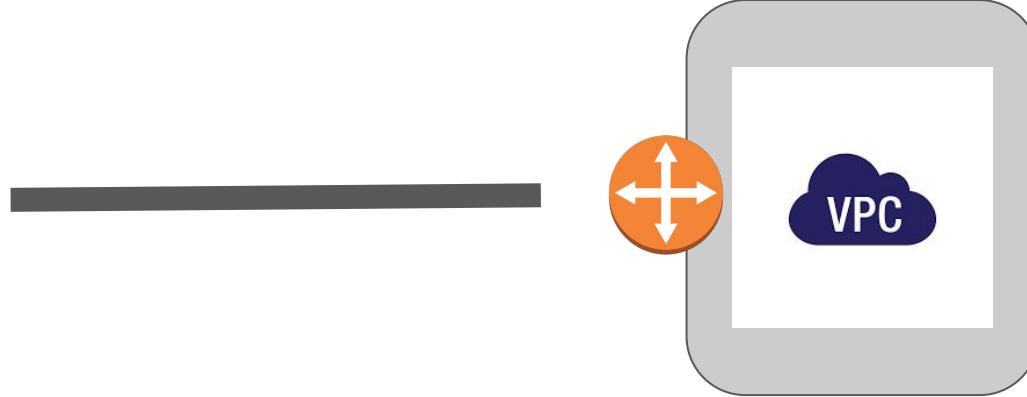
# Challenges

- Internet is a good option if amount of traffic is within a certain limit.
- There are always latencies which can also be involved.
- Many of the organization have hybrid architecture : DataCenter + AWS
- In such cases, latency can cause major challenges for the application



# Introducing DX

- In order to solve this challenge, AWS introduced Direct Connect.
- AWS Direct connect let's customer establish a dedicated direct network connection between the client's network and one of the direct connect locations.

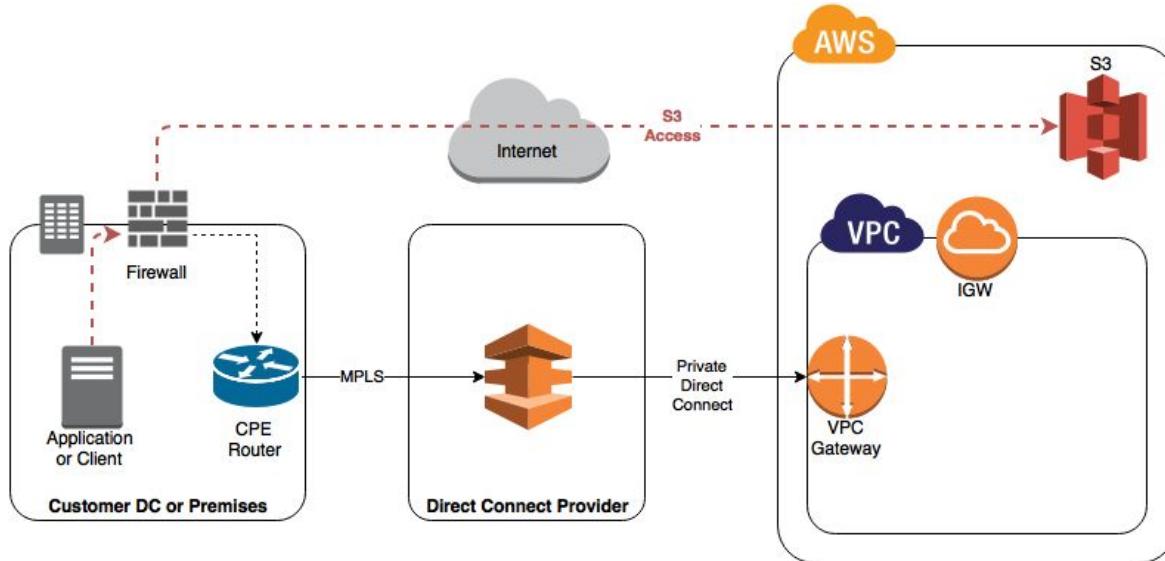


# Benefits of DX

Having direct connection between customer's datacenter to AWS, brings tremendous amount of benefits, some of them includes:

- i) Consistent Network Performance:
- ii) Reduces our bandwidth costs
- iii) Private connectivity to our AWS VPC

# Architecture of DX



---

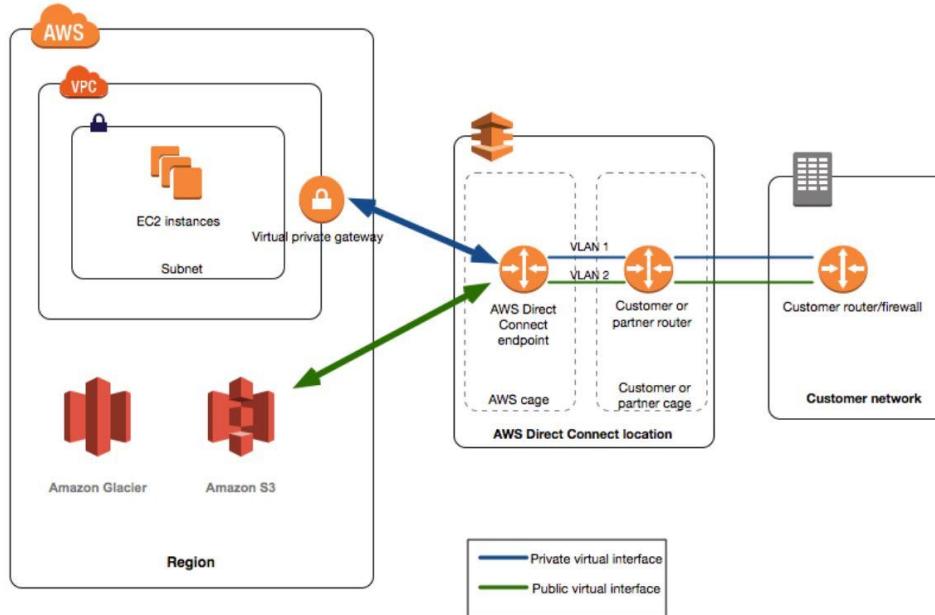
# Virtual Interfaces

Connecting to AWS via DX

---

# What after DX Line is Established?

The next primary step after Direct Connect is established is to configure the Virtual Interfaces.



# Virtual Interface Types

Depending on your requirement, appropriate Virtual Interface (VIF) can be created.

<b>Virtual Interface Type</b>	<b>Description</b>
Public Virtual Interface	Enables access to public AWS services like AWS S3, and others that are not in the VPC.
Private Virtual Interface	Enables access to your VPC
Transit Virtual Interface	Access one or more Amazon VPC Transit Gateways associated with Direct Connect gateways

# Steps 1 : Establish DX connection request

- Here we specify the connection name, location and the port speed.
- After we click on create, it will go for review to AWS and if approved, we get a LOA which we can download and give it to provider who will be establishing DX connection on your behalf.
- It takes upto 3 working days for the LOA to be approved.

**Connection settings**

Name  
A name to help you identify the connection.  
  
Name must contain no more than 100 characters. Valid characters are a-z, 0-9, and – (hyphen)

Location  
The location in which your connection is located.

Port speed  
Desired bandwidth for the new connection.  
 1Gbps  
 10Gbps

**Letter of Authorization and Connecting Facility Assignment**

Issue Date May 16, 2019	Requester By [Redacted]
Request By Amazon Data Services India, KK	Request To USA - Peptek TVP
Port By City Number Region 1 (12 - Global)	Port Type AWS Direct Connect (1x1)
Link Port / Router Port Number Link Router Port ID Serial: 0000	Link Type Single Mode Fiber

Please provide specific information regarding a requested port, with the Requesting Direct Connect customer number of the City or State, Router ID, and Port ID. A detailed description of the port is required for the creation of a connection. If you are requesting connectivity between the customer network above, this request is a reference or connection to the port indicated above. All changes to the physical connector are the responsibility of the customer. If you have any questions about this form, contact [aws-dc-support@amazon.com](mailto:aws-dc-support@amazon.com).

EXPIRATION NOTICE: The authorized connection by user is terminated after 180 days of the LOA/CPA issue date or the LOA/CPA will expire.

# Steps 2 : Create Virtual Interface

Create Virtual Interface based on your requirement.

Can be associated with Direct Connect Gateway or Virtual private Gateways.

**Create virtual interface**

You can create a private virtual interface to connect to your VPC. Or, you can create a public virtual interface to connect to AWS services that aren't in a VPC, such as Amazon S3 and Glacier. For private virtual interfaces, you need one private virtual interface for each VPC to connect from the AWS Direct Connect connection, or you can use a AWS Direct Connect gateway. [Learn more](#)

**Virtual interface type**

Type

**Private**  
A private virtual interface should be used to access an Amazon VPC using private IP addresses.

**Public**  
A public virtual interface can access all AWS public services using public IP addresses.

**Transit**  
A transit virtual interface is a VLAN that transports traffic from a Direct Connect gateway to one or more transit gateways.

# Step 3 - Download Router Configuration

After you have created the virtual interface for your AWS Direct Connect connection, you can download the router configuration file.

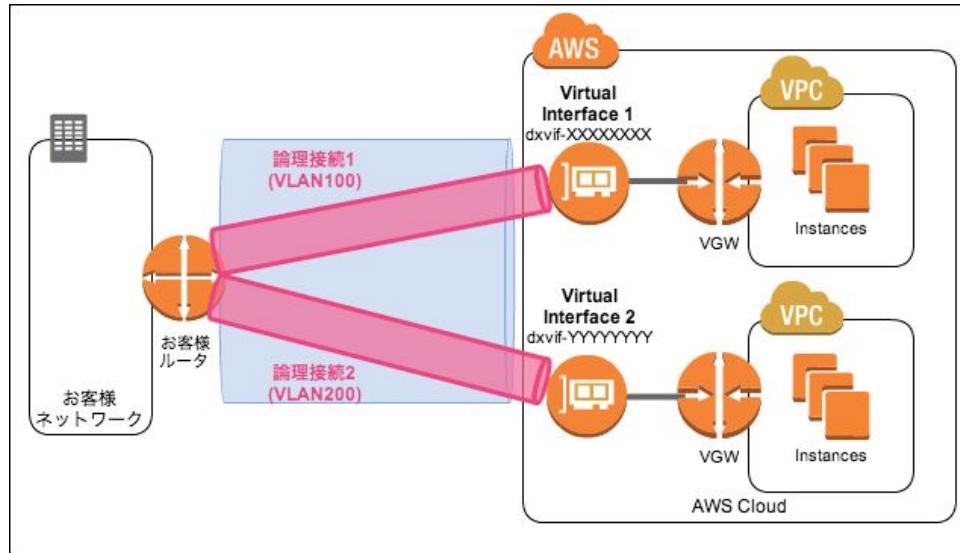
The file contains the necessary commands to configure your router for use with your private or public virtual interface



# Important Pointers

- By default 1Gbps and 10 Gbps connections are available, we can also have sub-1GB connection from direct connect partners which includes 50 mbps, 100 mbps, 200 mbps, 400 mbps, 500 mbps.
- Direct connect is not fault tolerant, so we need to either have secondary Direct Connect or use VPN as backup. Use BGP to automatic failover to backup connection.
- In US, direct connect will grant you access in all the US related region.

# Virtual Interfaces



---

# Physical Process for DX

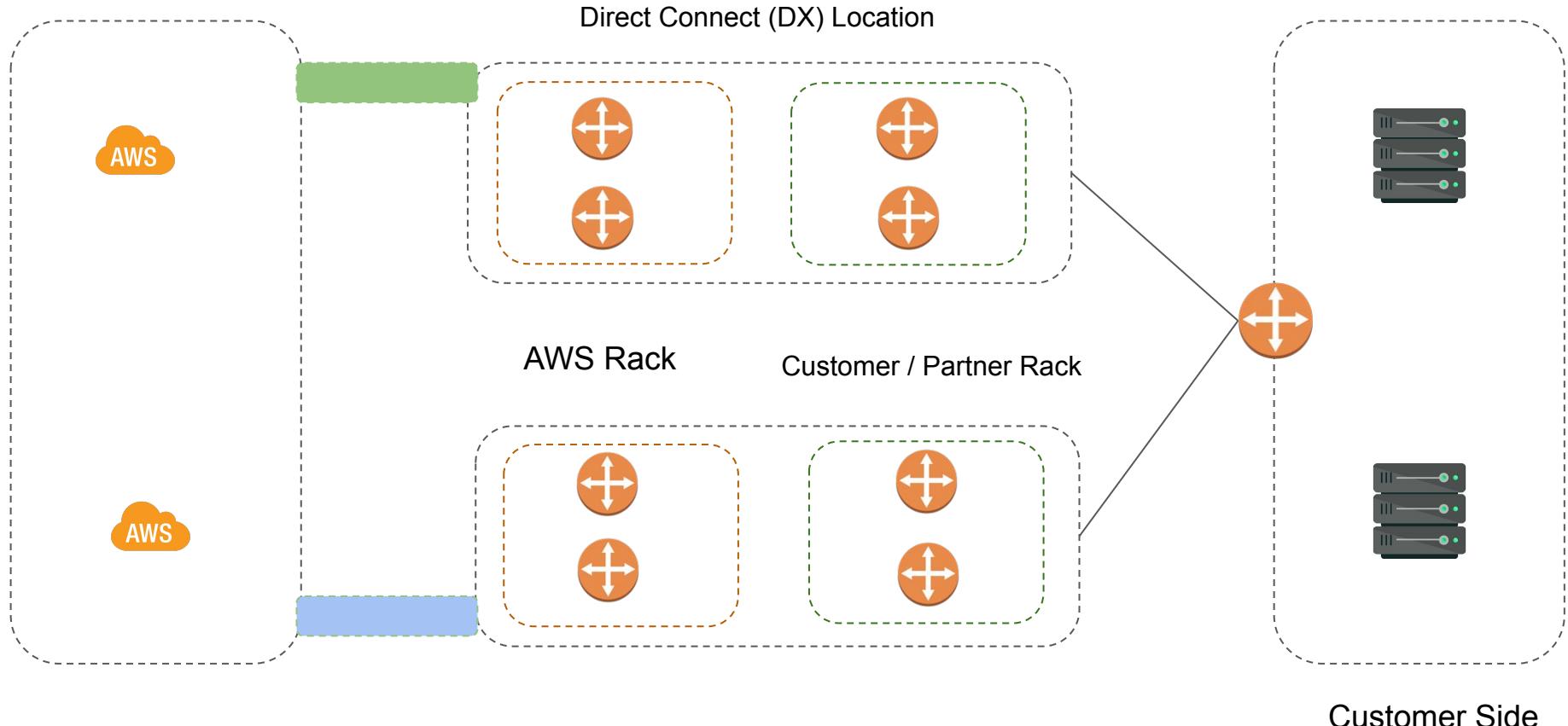
Customer to AWS

---

# Let's Begin

It is important for us to understand the physical process that happen when you might want to establish the DX connections.

Let's take an overview about the steps involved



# Let's Begin

- 1) We request a DX connection between AWS account and DX location.
- 2) AWS provides LOA document which contains the information about port and approval to connect to that port.
- 3) With the LOA, you or the partner can establish a cross-connect between your router port to AWS router port. This is a fiber port based on 802.1Q trunk..
- 4) When entire process is completed, we have a logical connection established where AWS provides port on a single DX router. The port is configured as 802.1Q trunk (so it can carry multiple VLAN)

## Letter of Authorization and Connecting Facility Assignment

**Issue Date**

March 16, 2012

**Requested By**

"CloudPack"

**Issued By\***

Amazon Data Services Japan, KK

**Issued To**

IBX - Equinix TY2

**Facility - Cage Number**

Equinix TY2 - [REDACTED]

**AWS Direct Connection ID**

dx-port-[REDACTED]

**Rack, Patch Panel, Port Number**

Rack: [REDACTED]

Patch Panel:[REDACTED]

Strands:[REDACTED]

**Cable Type**

Single Mode Fiber

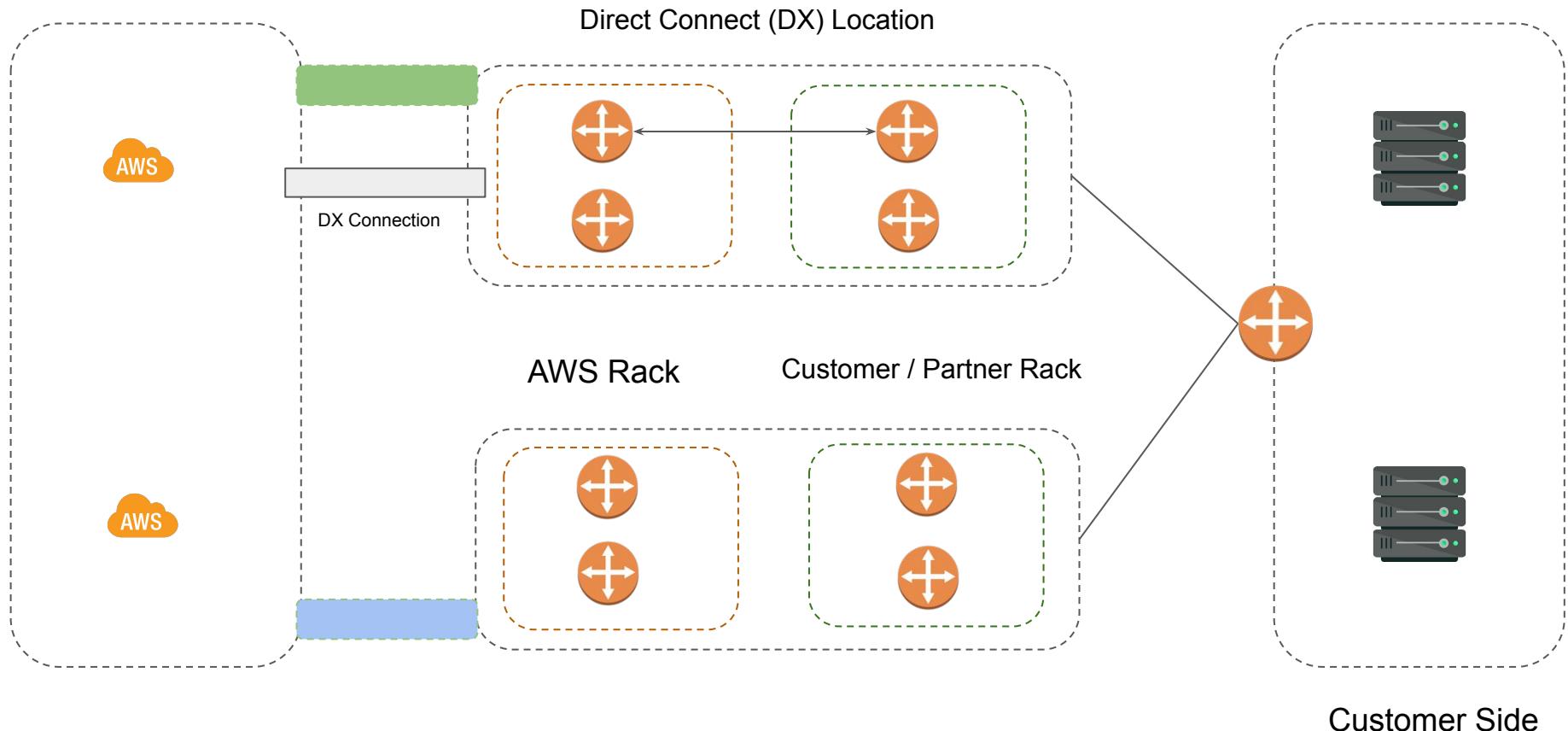
---

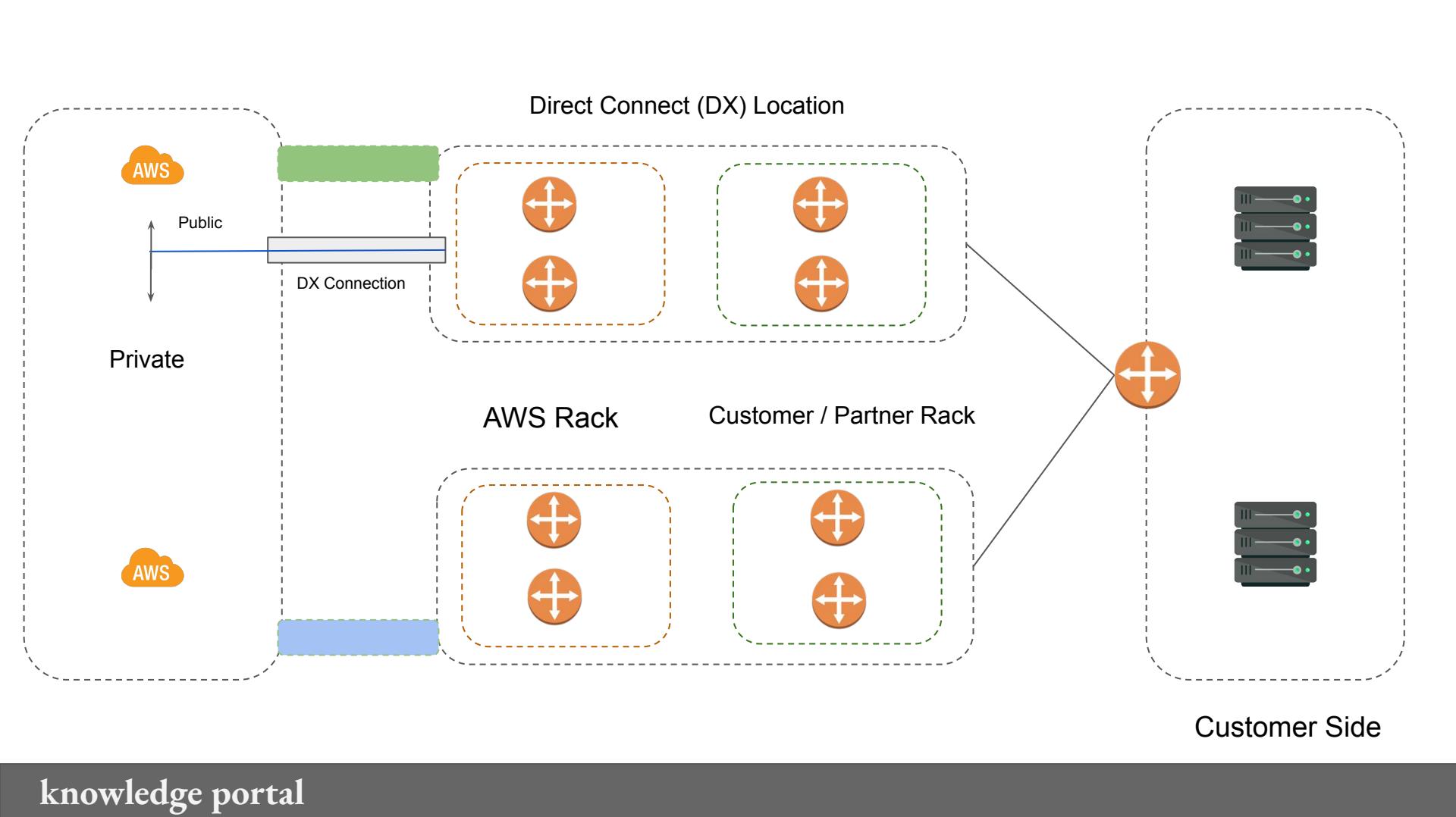
For location specific information on requesting a cross-connect, visit the "Requesting Cross-Connects at AWS Direct Connect locations" section of the Getting Started Guide:

<http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Colocation.html>

Please consider this letter as notification for connecting facility assignment for the purpose of establishing or augmenting connectivity between the parties identified above. This document authorizes a connection to the ports indicated above. All charges for the physical connection are the responsibility of "CloudPack". If you have any questions about this letter, contact [REDACTED]  
[REDACTED]

**EXPIRATION NOTICE** The authorized connectivity must be completed within 30 days of this LOA-CFA's issue date or this LOA-CFA will expire.





# Important Pointer

Connection between DX router and customer router is a single mode fiber and it needs to be a 1Gbps-1000Base-LX OR 10GBASE-LR



# Let's Revise

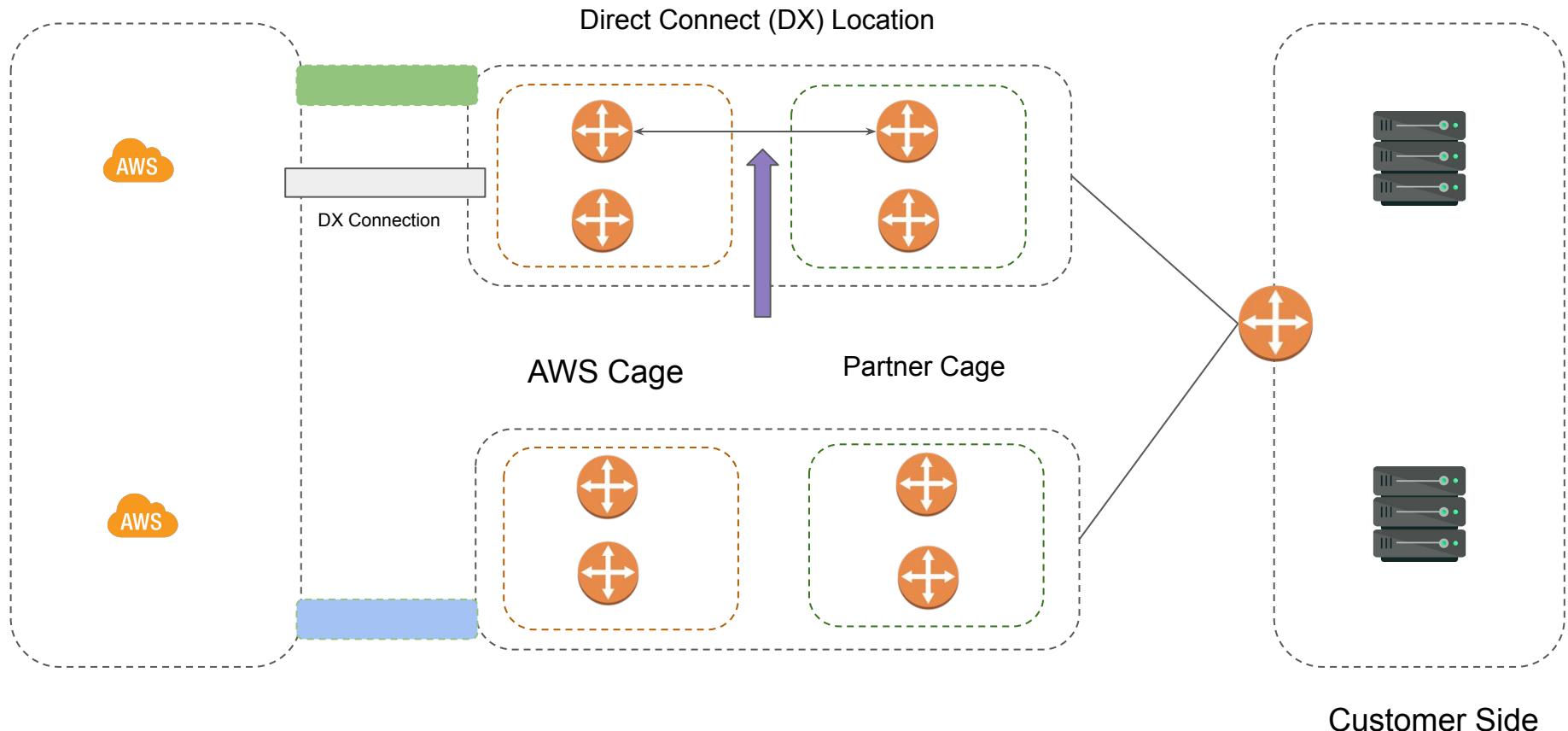
1	Select region in which you need DX connection	Customer Dependent
2	Order the connection - 1GBps or 10Gbps	AWS Dependent
3	Await for AWS to provide you LOA CFA	AWS Dependent
4	Arrange Cross Connect - Provide LOA & Customer Port details	Partner Dependent
5	Might have to arrange connectivity between DX location and customer side.	Partner Dependent (90 days)
6	Port Specific Configurations (Auto-Negotiation - off , port speed = static defined)	Customer Dependent
7	Interface creation & Configuration (Can download from AWS config / configure manually)	Customer Dependent

---

# Physical Process for DX

Via Partner!





# Important Pointers

Cross Connect is completely managed by the Partner and you don't have control over it.

The Cross Connect is between DX router & partner is shared between all of the customers of the partner.

While ordering with partner, instead of fully DX connection which provides multiple VLAN capability, we get a hosted connection. This connection is created by partner and shared into your account.

In hosted connection, only 1 VLAN is allowed. Thus only single public OR private interface.

# Hosted Connection Acceptance

AnyCompany Hosting	Demo Hosted Connection	Equinix SG2, Singapore	50Mbps	0	<span style="color: orange;">pending acceptance</span>
<b>Connection Name:</b>	Demo Hosted Connection	<b>Connection ID:</b>	dxcon-fh6ajycc		
<b>Type:</b>	Hosted Connection	<b>Port Speed:</b>	50Mbps		
<b>Location:</b>	Equinix SG2, Singapore	<b>VLAN Assigned:</b>	100		
<b>Provided By:</b>	AnyCompany Hosting	<b>Virtual Interfaces:</b>	0		
<b>State:</b>	<span style="color: orange;">pending acceptance</span>				

Before this connection can be active and used, you must accept it. If you accept, connectivity between your data center and AWS will be provided by partner.

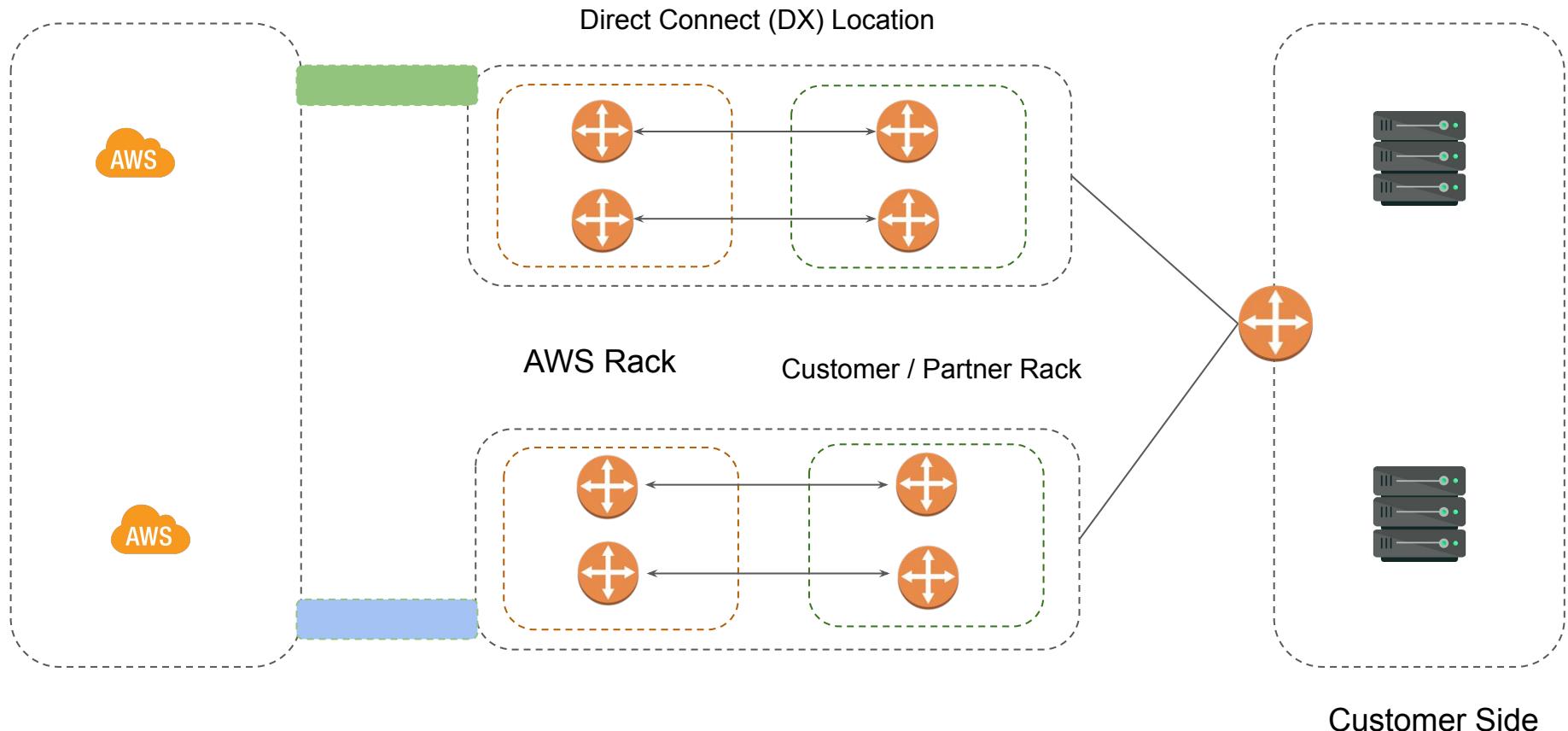
I understand that Direct Connect port charges apply once I click "Accept Connection".

**Accept Connection**   **Decline Connection**

---

# Dual DX Architecture

---



# Dual DX Architecture

- If going with the dual DX architecture, then essentially there would be multiple VIF
- You can run them in active/active or active/passive mode.

```
Network          Next Hop          Metric LocPrf Weight Path
*> 10.0.0.0/16    169.254.254.9      0    7224 i
*  10.0.0.0/16    169.254.254.13      0    7224 i

router bgp 65001
maximum-paths 2

Network          Next Hop          Metric LocPrf Weight Path
*> 10.0.0.0/16    169.254.254.9      0    7224 i
*m 10.0.0.0/16    169.254.254.13      0    7224 i
```

# Challenge with BGP MultiPath

VGW will receive the announcements from you for the Multi-Path.

It will assume that you want to run on active/active and it will also work based on that.

```
1: 172.16.0.0 /16 via 169.254.254.10 with AS_PATH: 65001 i
2: 172.16.0.0 /16 via 169.254.254.14 with AS_PATH: 65001 i
Choose: BGP Multipath
```

# Active-Passive Architecture of VIF

- Let's look into the Active / Passive Architecture.
- We can set priority based on local-preference option

```
router bgp 65001
  neighbor 169.254.254.9 route-map LOCALPREF-150 in
  neighbor 169.254.254.13 route-map LOCALPREF-200 in

  route-map LOCALPREF-200 permit 10
    set local-preference 200

  route-map LOCALPREF-150 permit 10
    set local-preference 150

      Network          Next Hop          Metric LocPrf Weight Path
      * 10.0.0.0/16    169.254.254.9    150   0    7224 i
      *> 10.0.0.0/16   169.254.254.13    200   0    7224 i
```

# Challenge with Active/Passive

- AWS will return traffic through both the path.
- This is something that we might not want to achieve.

```
1: 172.16.0.0 /16 via 169.254.254.10 with AS_PATH: 65001 i
2: 172.16.0.0 /16 via 169.254.254.14 with AS_PATH: 65001 i
Choose: BGP Multipath
```

# AS Path Prepending

Through AS Path Prepending, we make VGW believe that one of the path is longer than the other.

```
router bgp 65001
  neighbor 169.254.254.9 route-map PREPEND-X2 out
  neighbor 169.254.254.13 route-map PREPEND-X1 out

  route-map PREPEND-X1 permit 10
    set as-path prepend 65501

  route-map PREPEND-X2 permit 10
    set as-path prepend 65501 65501
```

# VGW Perspective - AS Prepending

```
1: 172.16.0.0 /16 via 169.254.254.10 with AS_PATH: 65001 65001 65001 i
2: 172.16.0.0 /16 via 169.254.254.14 with AS_PATH: 65001 65001 i
Choose: Path 2 (Shortest)
```

---

# Direct Connect Gateway

Direct connect all the way

---

# Gateway Types for Virtual Interface

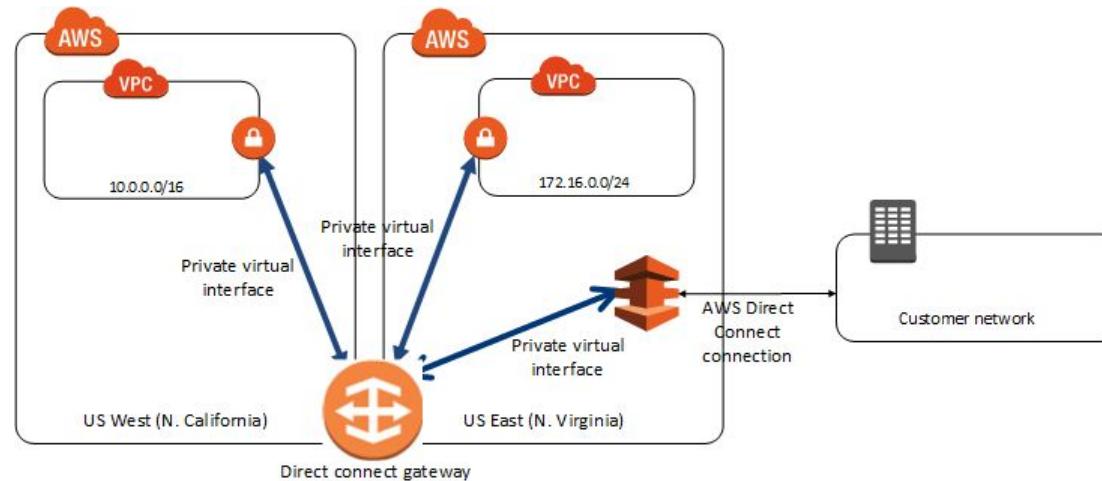
Following tables illustrates the supported gateway types for the Virtual Interfaces

<b>Gateway Types</b>	<b>Description</b>
Virtual Private Gateway	Allows connections to a single VPC in the same region
Direct Connect Gateway	Allows connections to multiple VPCs and regions

# Overview of DX Gateway

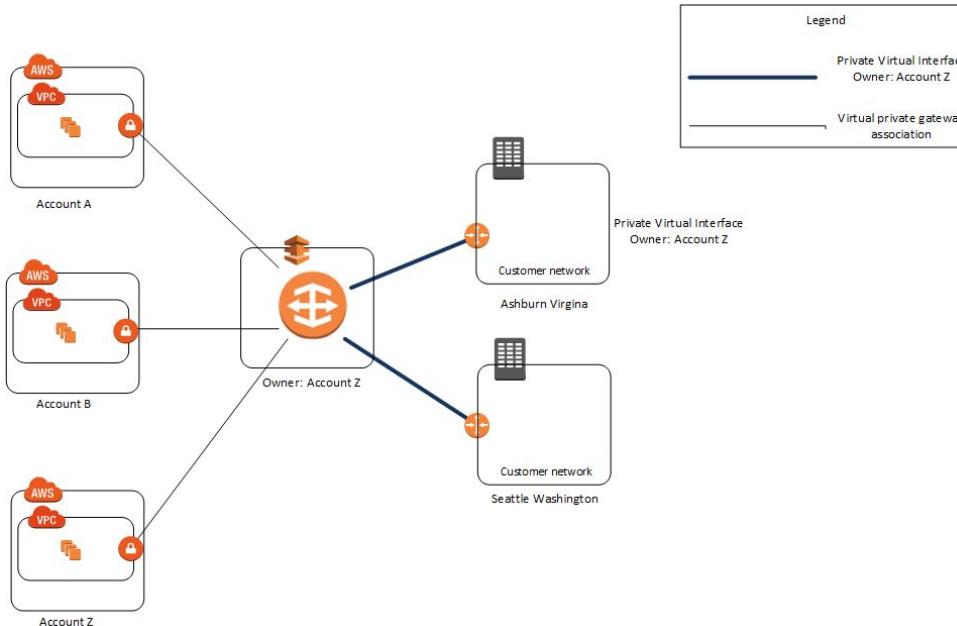
Direct Connect Gateway can be used to connect your direct connect connection over private VIF to one or more VPC's within the account that are located in same or multiple regions.

It allows us to combine private VIF's with multiple VGW's in local or in remote region.



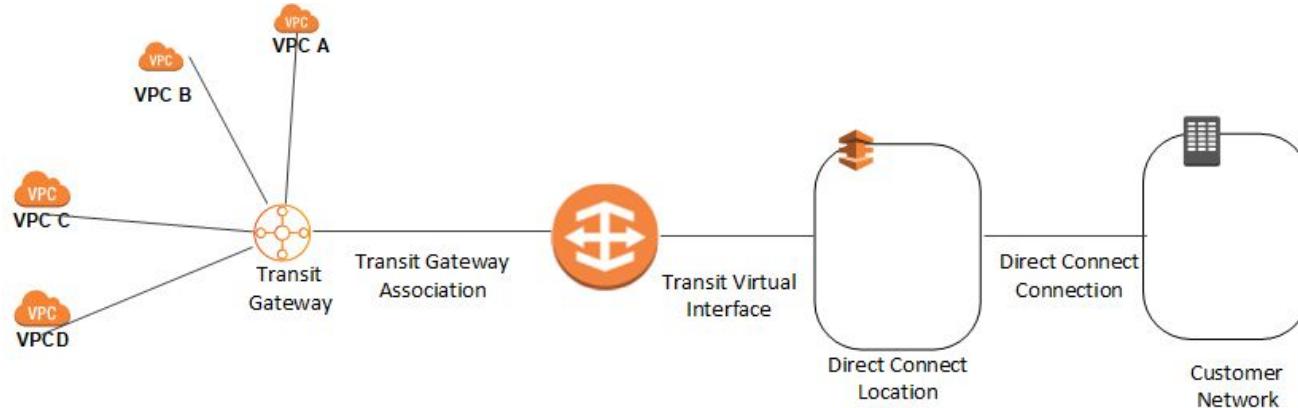
# Multiple Accounts

Multiple AWS accounts can also be integrated with DX Gateways.



# Transit Gateway Association

The following diagram illustrates how the Direct Connect gateway enables you to create a single connection to your Direct Connect connection that all of your VPCs can use.



---

## Direct Connect - High Availability

Allows us to have a better sleep.

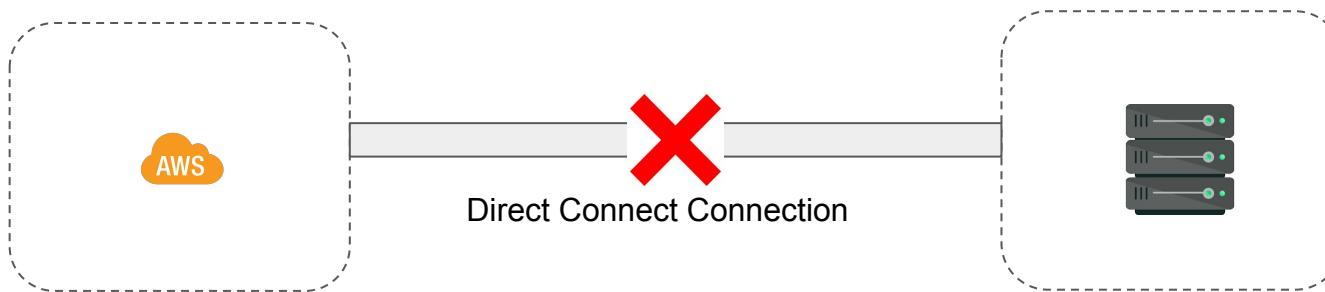
---

# Getting Started

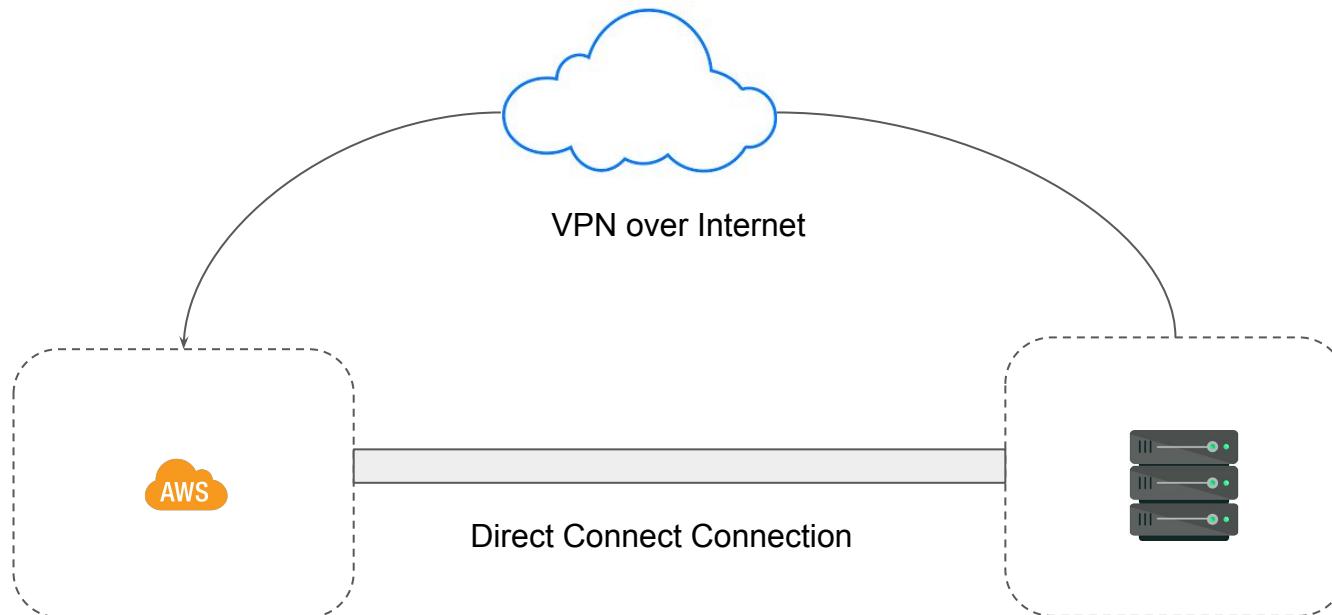
If you have a single DX connection, it is subjected to scenario of failover.

In-case if your DX connection breaks, your link will break completely.

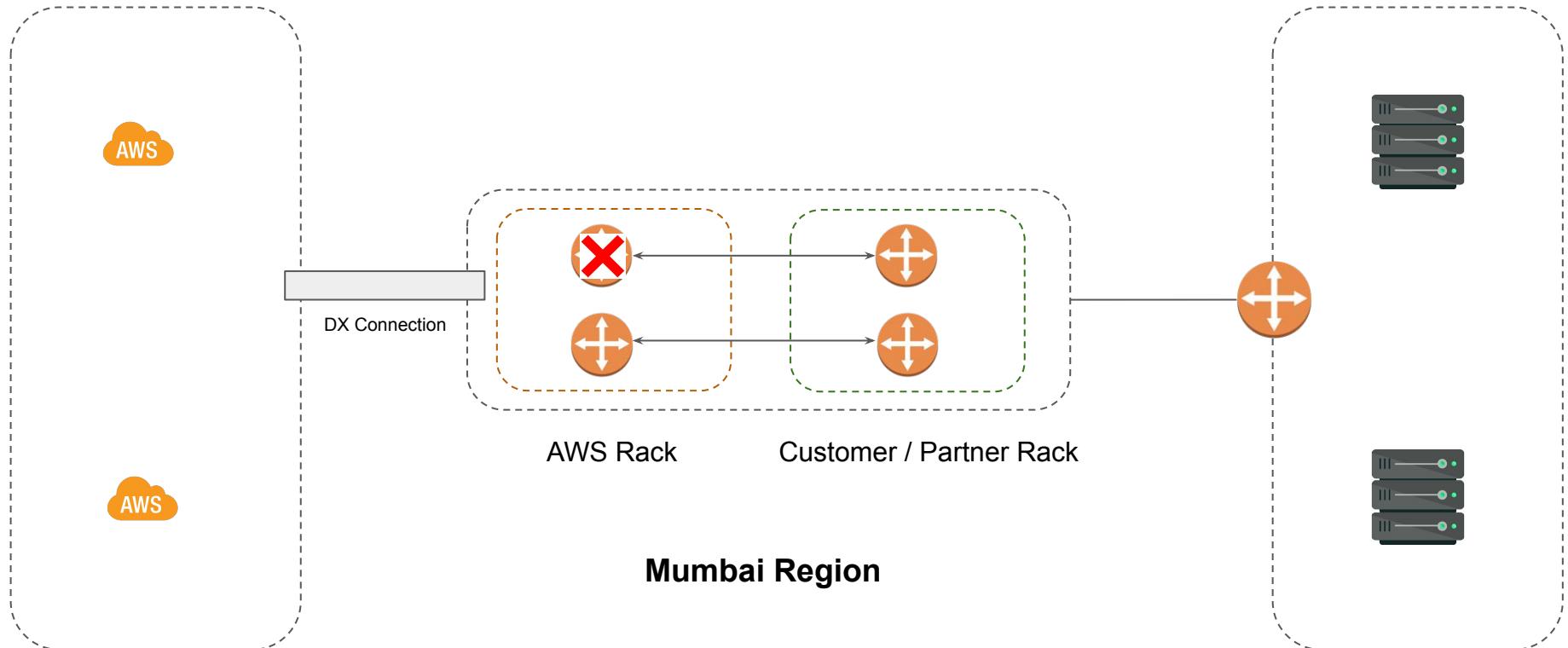
Hence it is recommended to have a backup connection of VPN over the Internet.



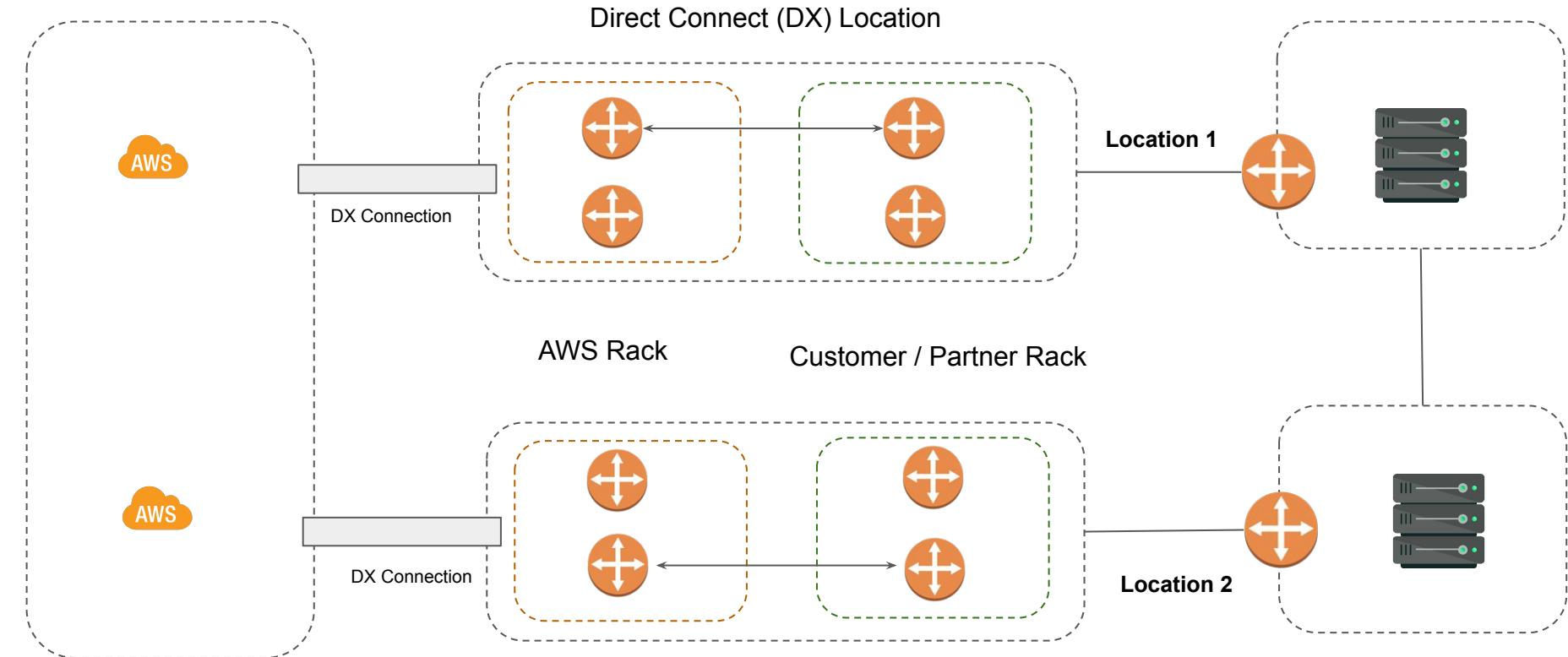
# Secondary Backup Connection



# Dual Connection - Single Location



# Dual Connection - Dual Location

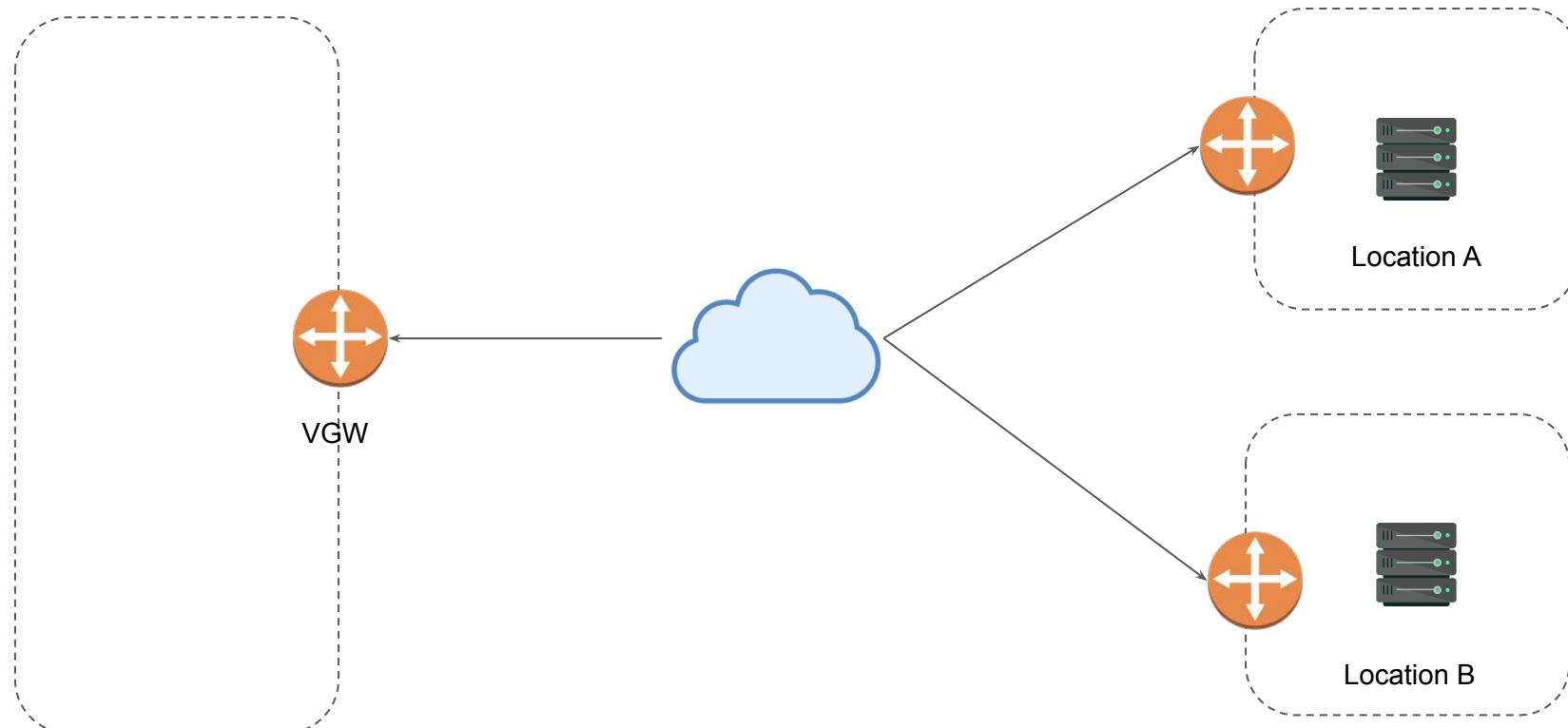


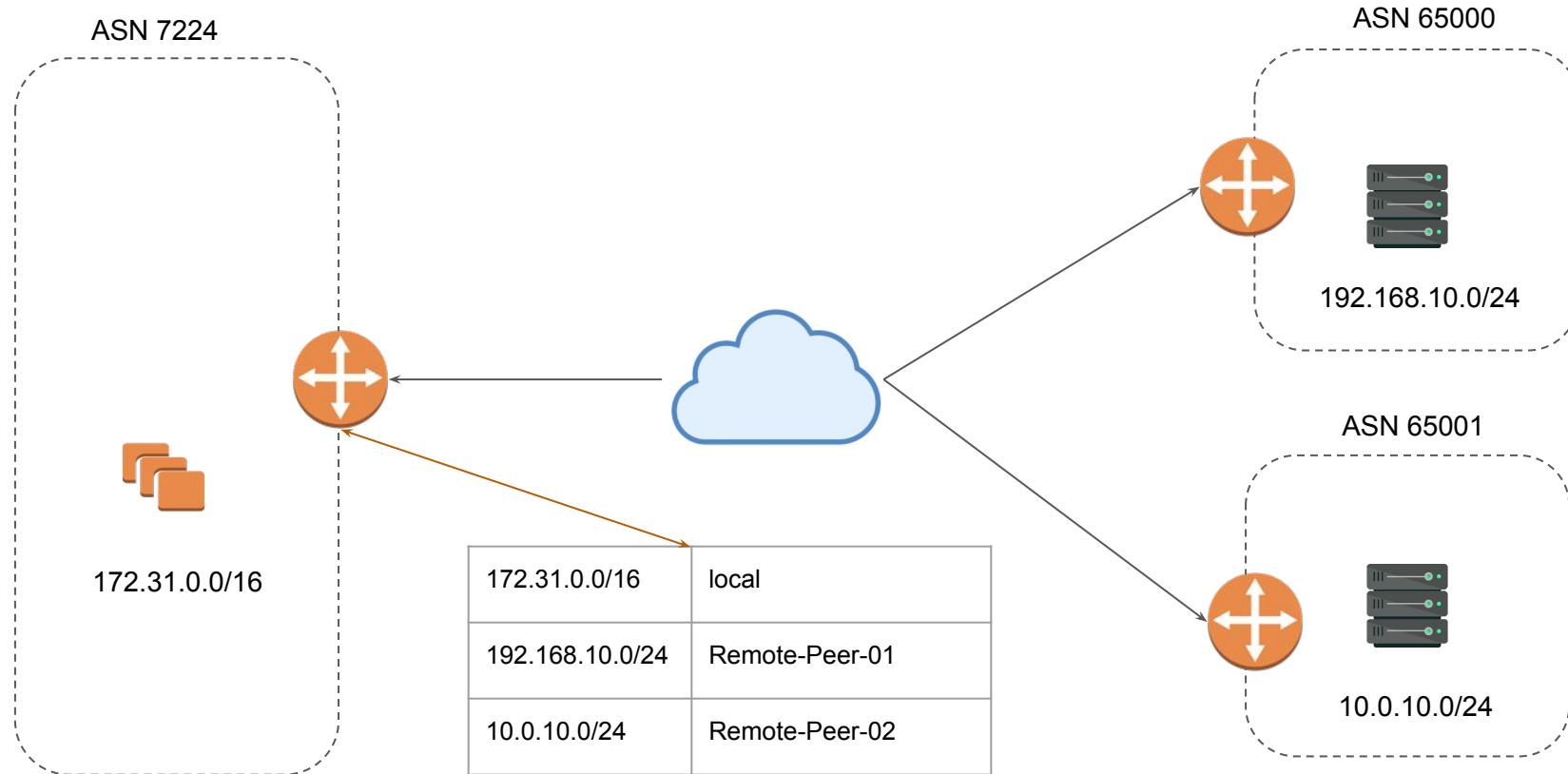
---

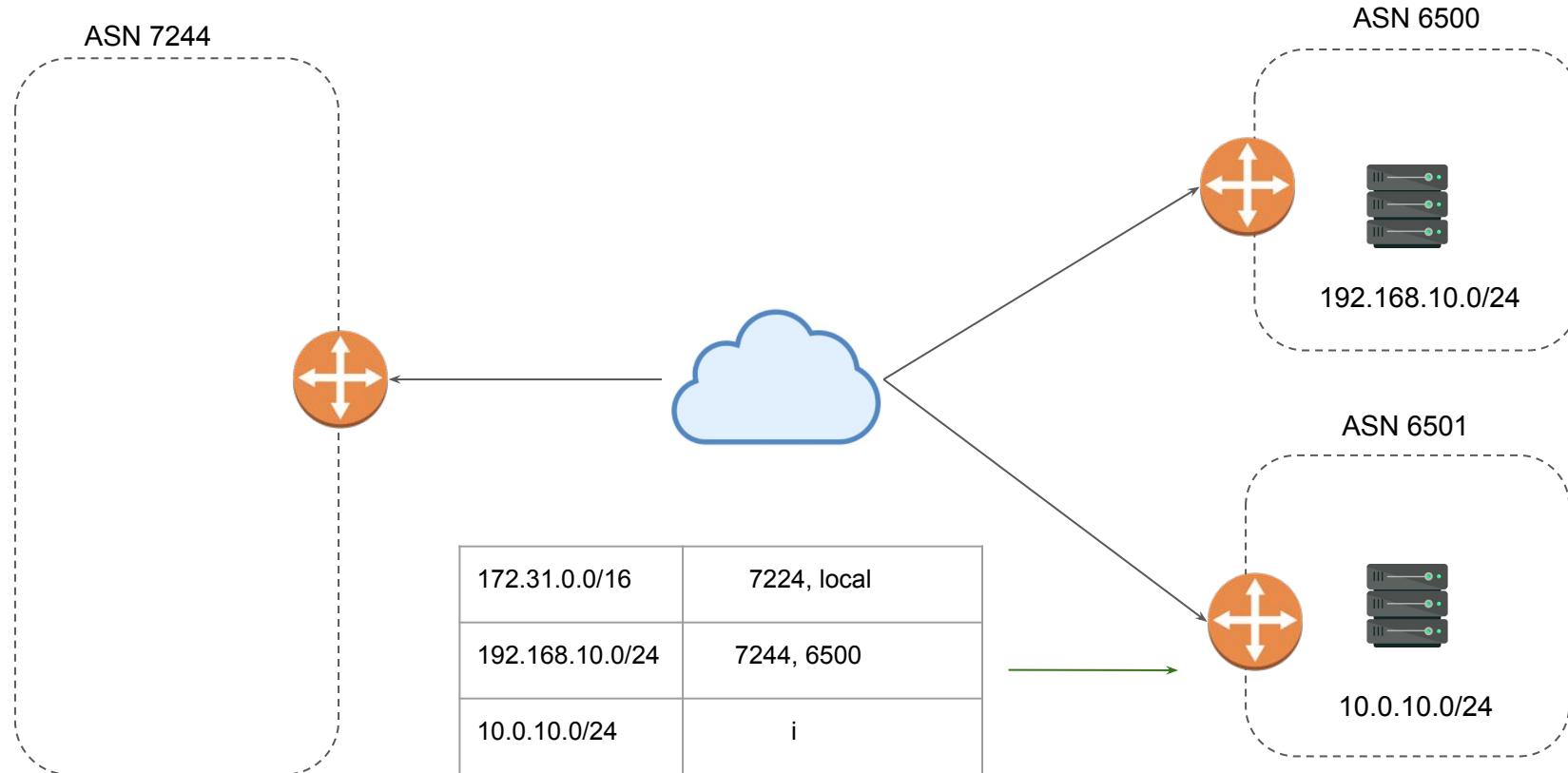
# AWS CloudHub

By product of VGW

---







# Important Pointers

In order for the architecture to work, it is necessary for the customer router to advertise the network prefixes that it has.

VGW will re-advertise those prefixes to all the endpoints connected.

Direct Connect is also supported in the design pattern of the CloudHub based architecture.

---

# BGP Communities

---

# Understanding BGP Community

A BGP community is bit of “extra information” that you can add to one or more prefixes which is advertised to BGP neighbors.

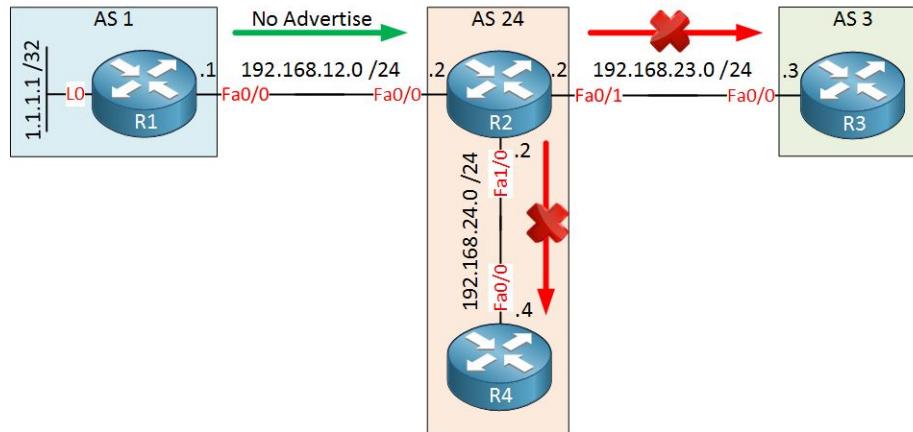
There are four well known BGP communities

- Internet: advertise the prefix to all BGP neighbors.
- No-Advertise: don’t advertise the prefix to any BGP neighbors.
- No-Export: don’t advertise the prefix to any eBGP neighbors.
- Local-AS: don’t advertise the prefix outside of the sub-AS

ISP generally instructs customer to tag prefixes with community so that it can be treated accordingly.

# No Advertise

When No Advertise is set, the router will not advertise your routes to it's neighbors.



# BGP Communities & DX

AWS Direct Connect supports a range of BGP community tags to help control the scope (regional or global) and route preference of traffic.

7224:9100—Local AWS Region

7224:9200—All AWS regions for a continent (for example, North America-wide)

7224:9300—Global (all public AWS Regions)

If you do not apply any community tags, prefixes are advertised to all public AWS regions (global) by default.

# Important Pointer

Let's assume you have a DX public VIF and you advertise your IP pool over the DX.

Community Tag Associated: Global

AWS will advertise it among all of its region.

Now if you want to use the public IP pool from Ohio region, then traffic will go from Ohio to Mumbai via AWS backbone network and delivered over public VIF.

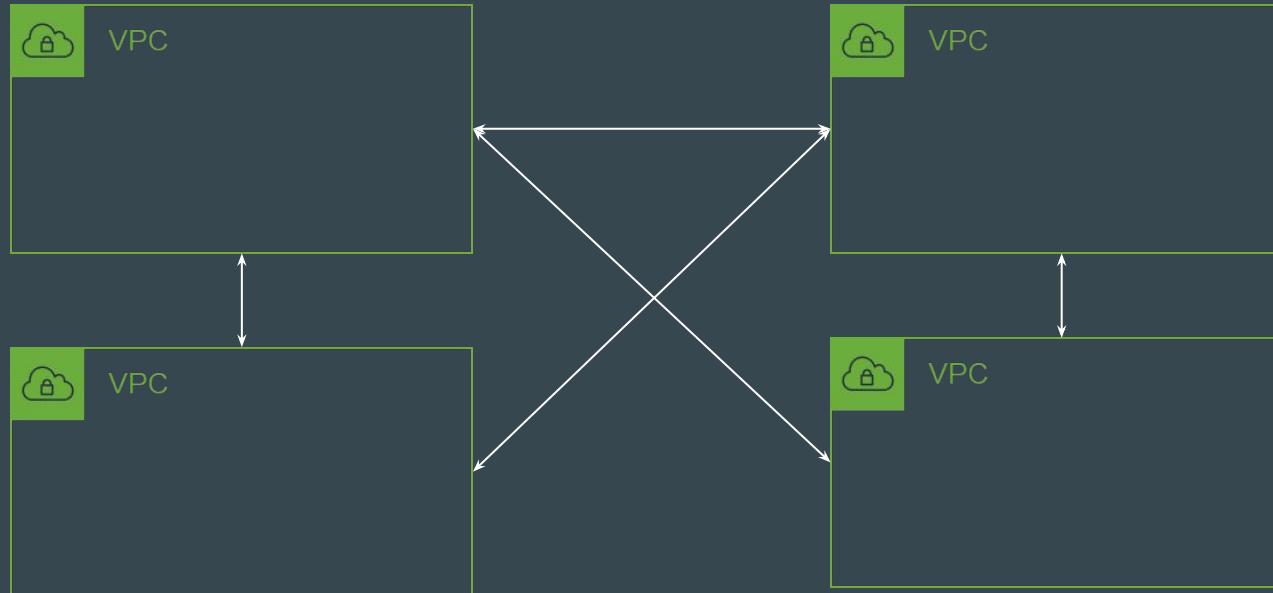
In case, you advertise that public IP Pool as Local AWS region, then, when accessed from Ohio for example, traffic will be routed over Internet

# **Transit Gateways**



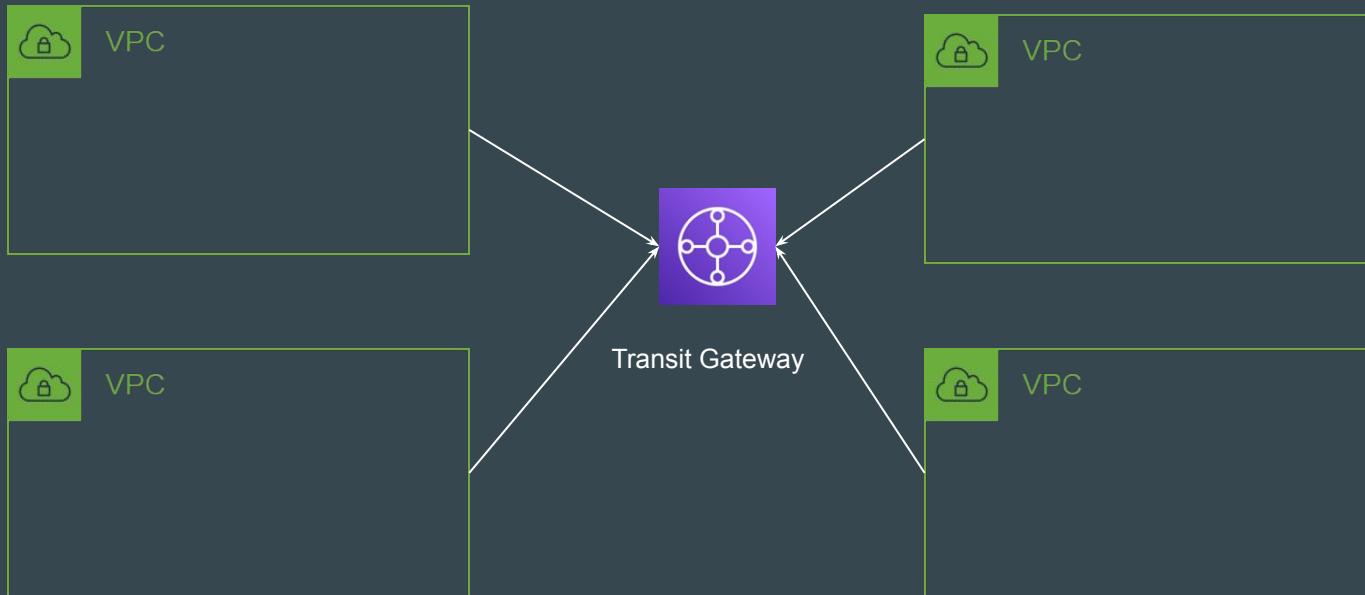
# Use-Case: Connecting 4 VPCs

More the Number of VPCs, more the number of peering connection you have to establish for inter-connectivity related use-case.

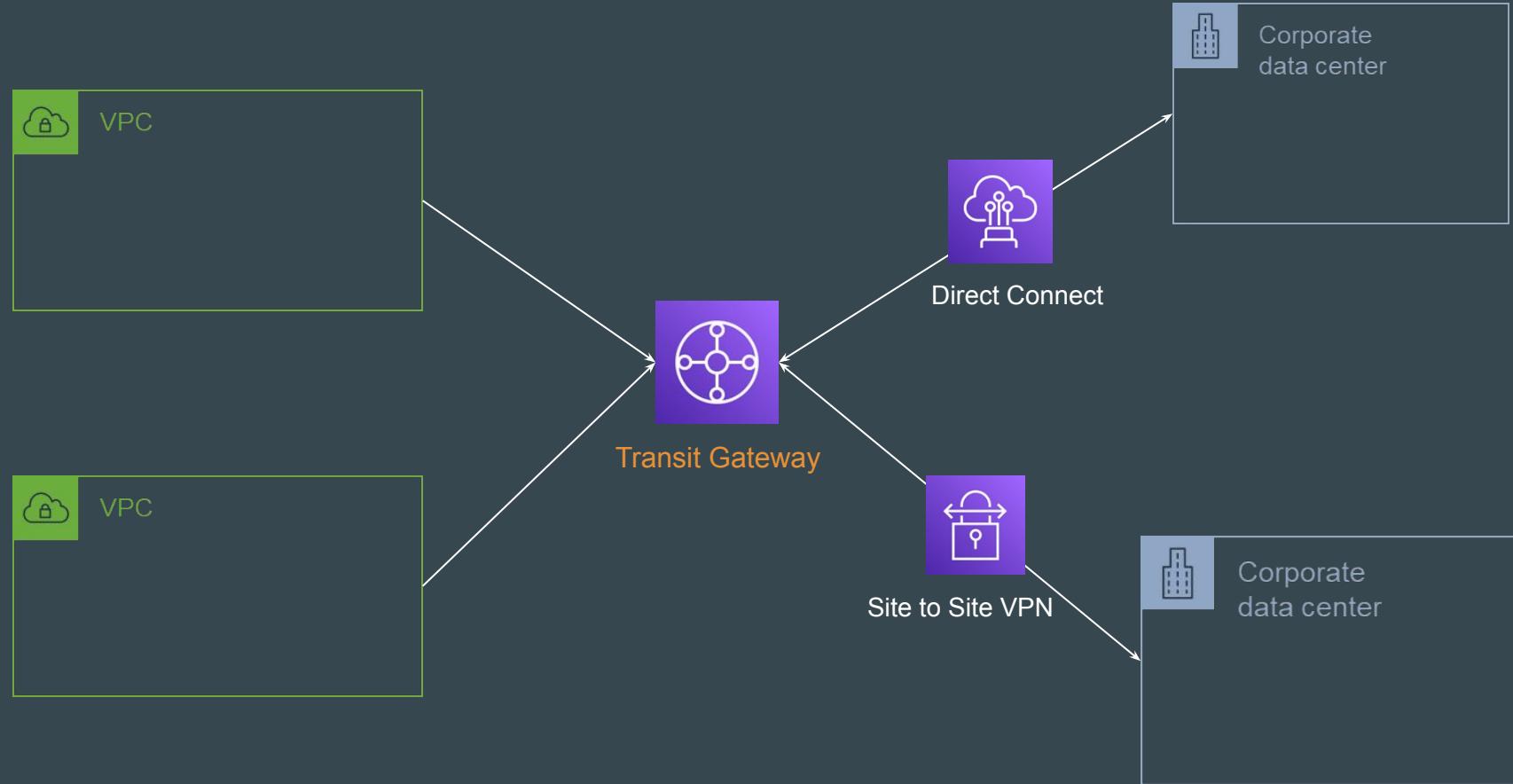


# Introducing Transit Gateway

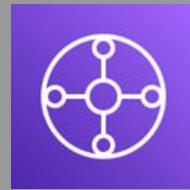
AWS Transit Gateway **connects** your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub



# Larger Setup



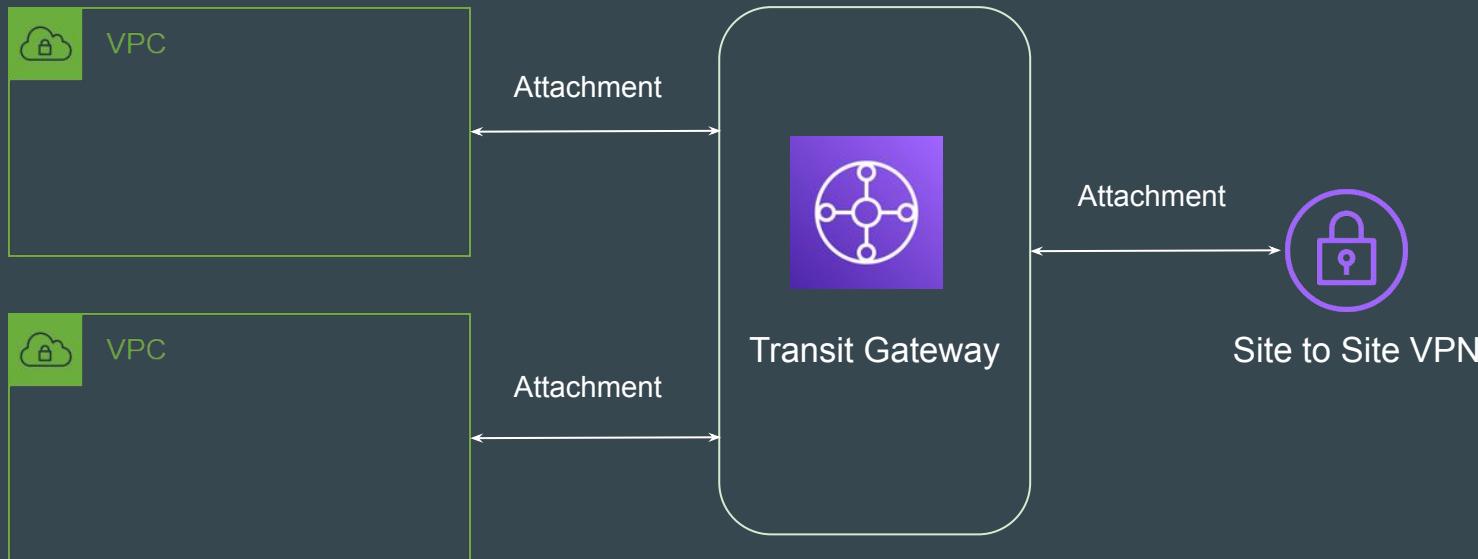
# Transit gateway concepts



# Concept 1 - Attachments

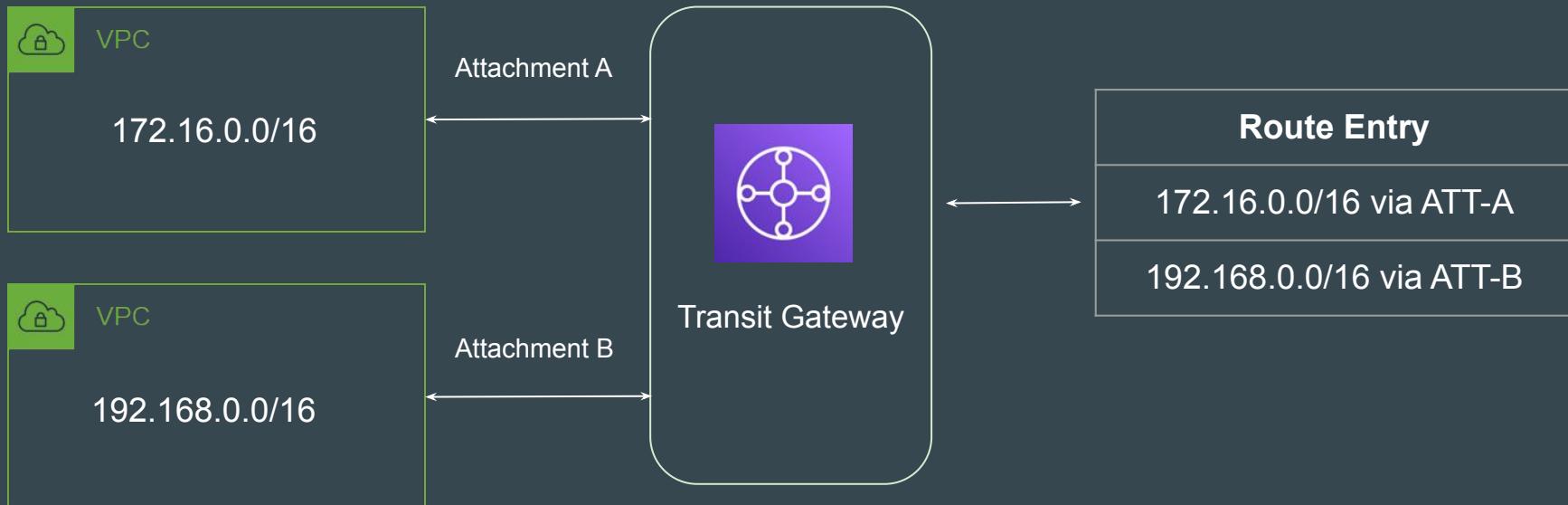
Multiple resources can be attached to Transit Gateway.

Some of the supported entities: VPCs, Direct Connect Gateway, VPN, SD-WAN



# Concept 2 - Route Table

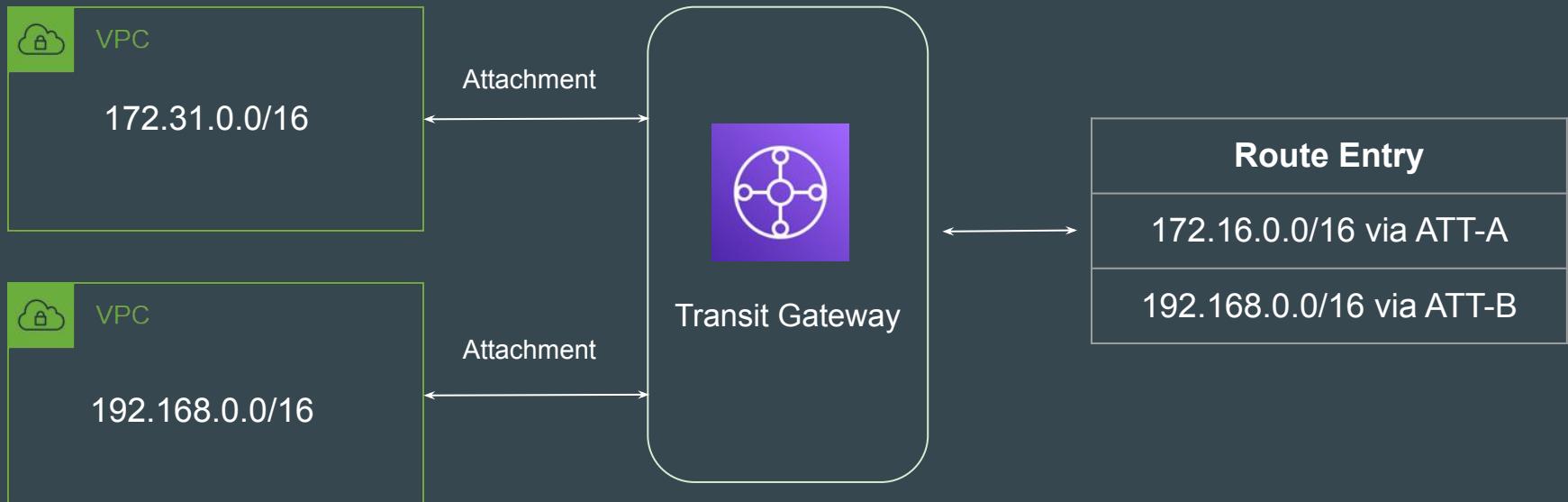
Defines how the traffic is routed between the connected resources.



# **Transit gateway Practical**



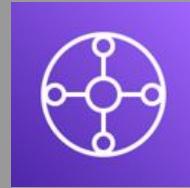
# Our Practical Setup



# Success Criteria

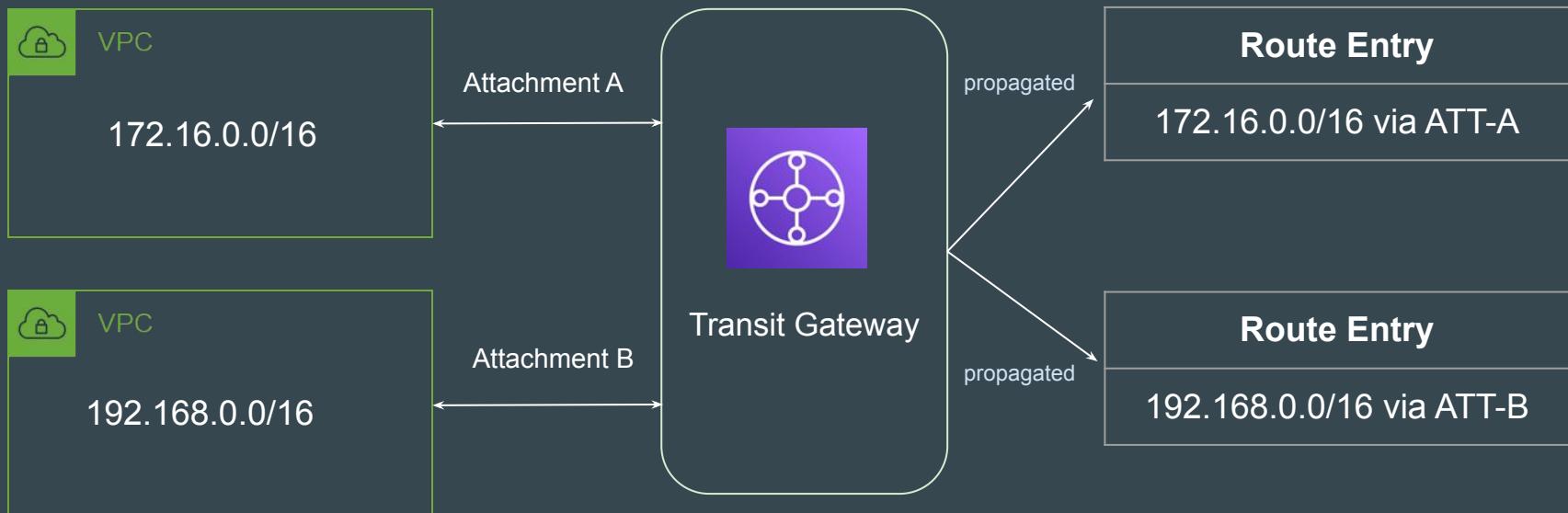
EC2 Instance from VPC-1 **should be able to communicate** to E2 Instance from VPC-2 through Transit Gateway.

# Routes in Transit Gateways



# Route Propagation

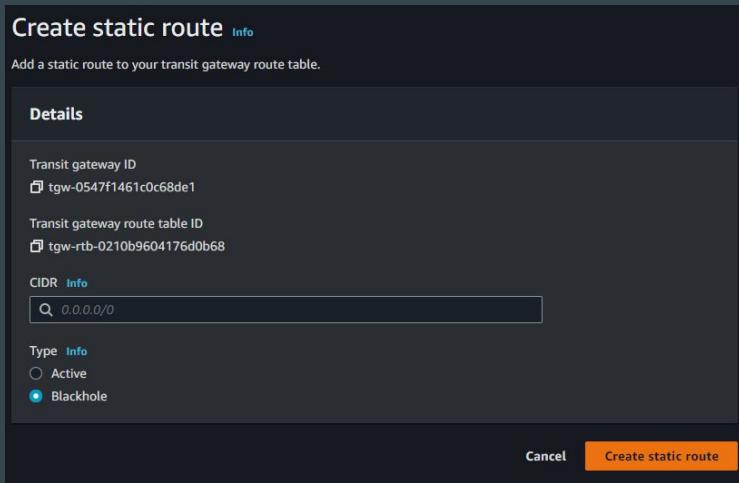
For a VPC attachment, the CIDR blocks of the VPC are propagated to the transit gateway route table.



# Static Routes

In addition to propagated routes, you can also add static routes.

Static routes allows more flexible routing policy with option to even **DROP** traffic.



# Route Evaluation Order

The most specific route for the destination address is given higher priority.

For routes with the same destination IP address but different targets, the route priority is as follows:

1. Static routes (for example, Site-to-Site VPN static routes)
2. Prefix list referenced routes
3. VPC propagated routes
4. Direct Connect gateway propagated routes
5. Transit Gateway Connect propagated routes
6. Site-to-Site VPN propagated routes

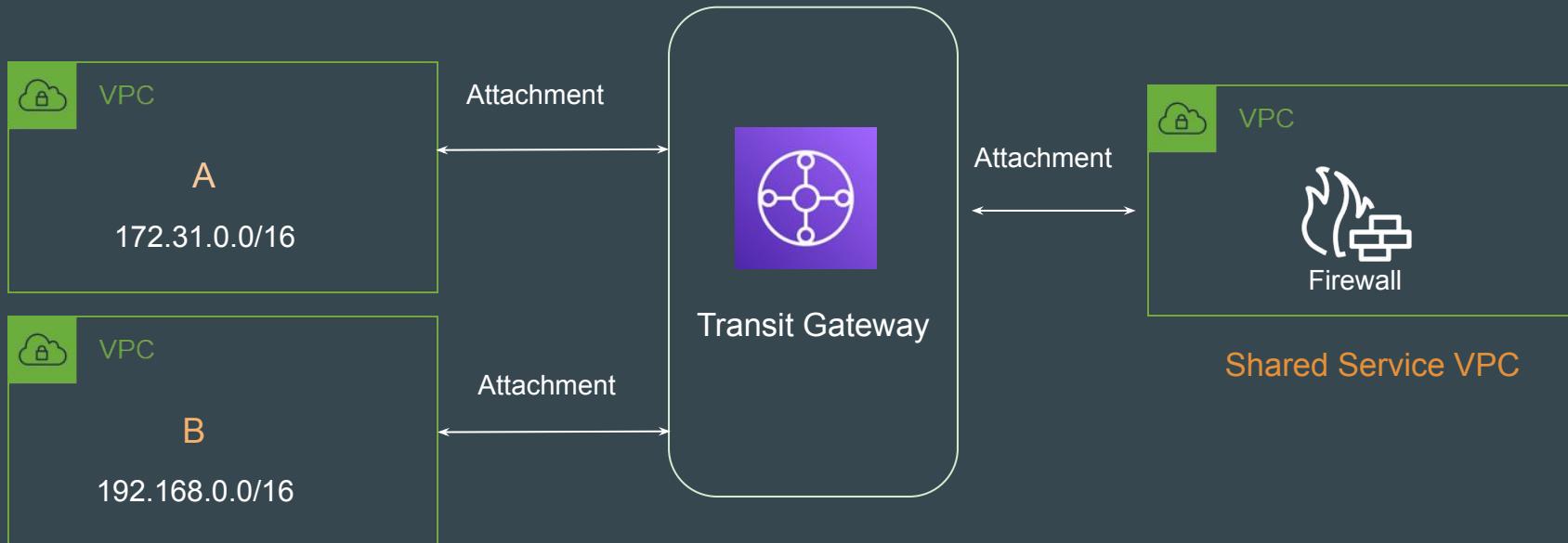
# Architecture Pattern - Appliance in Shared Service VPC

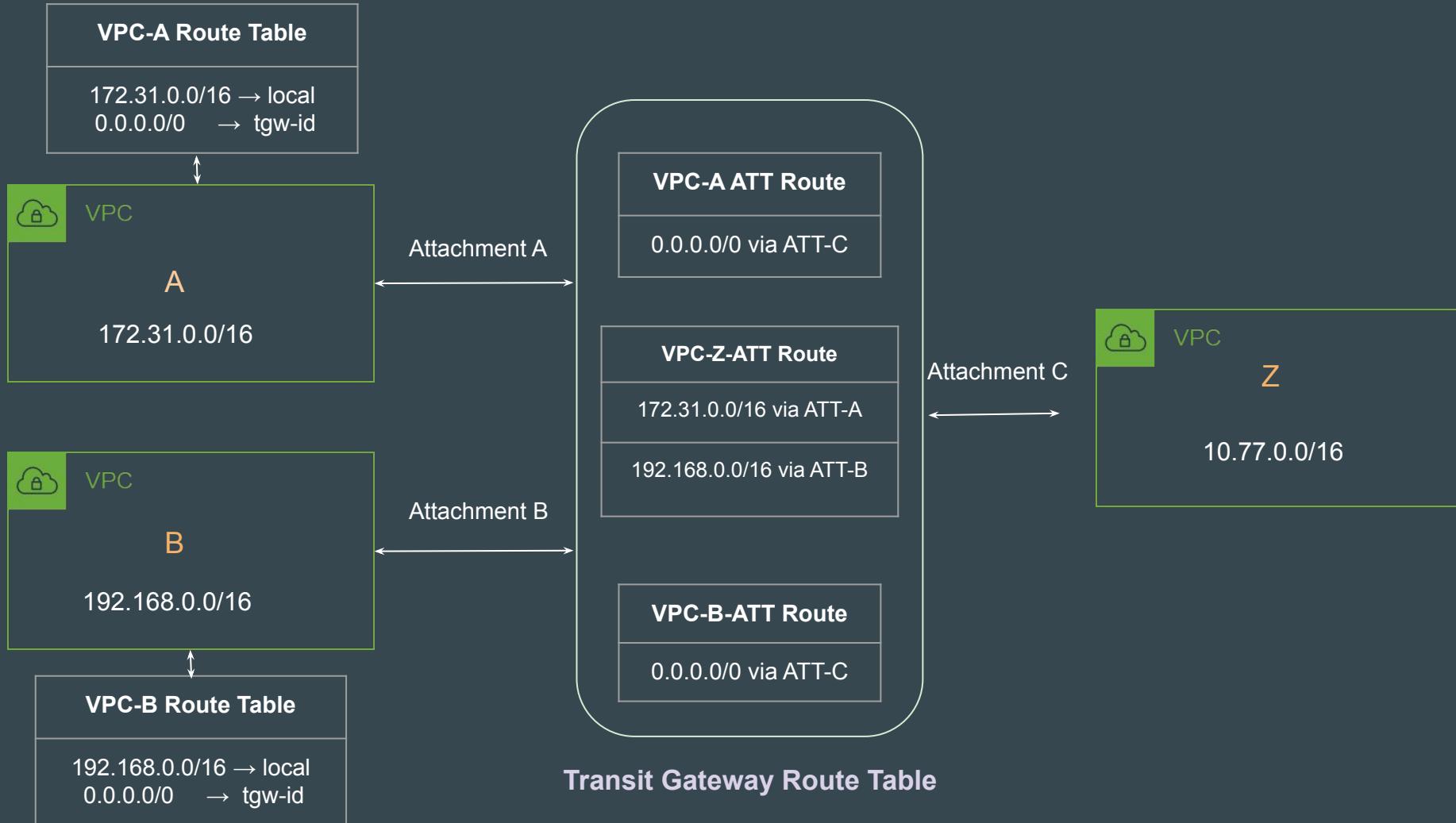


# Understanding the Use-Case

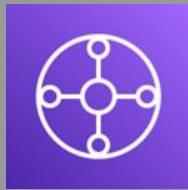
Many organizations have certain appliance like Proxy, Firewalls, IDS/IPS in a shared service VPC.

**Use-Case:** All traffic that's routed between transit gateway attachments should first be inspected by the appliance in the shared services VPC.





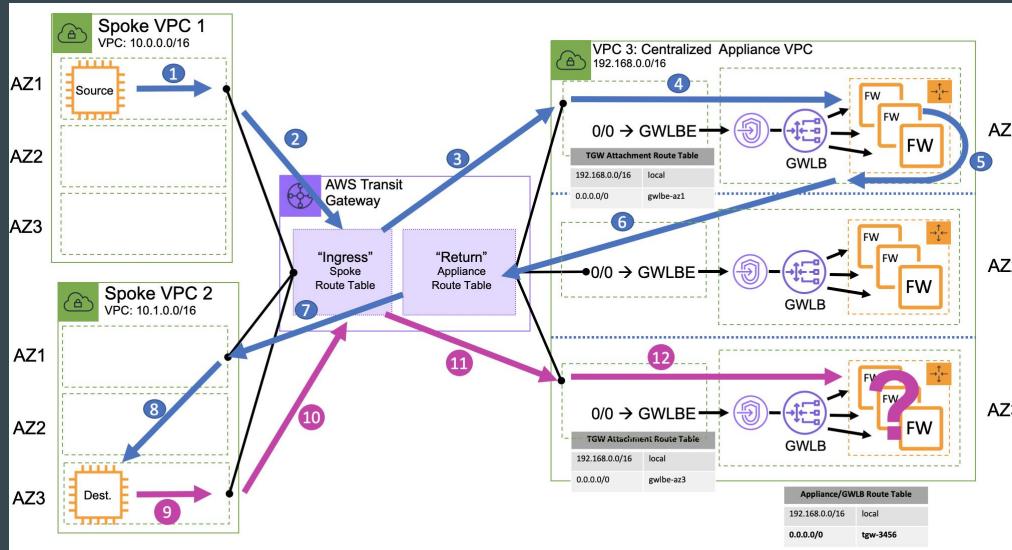
# **Appliance Mode - Transit Gateway**



# Understanding the Use-Case

By default, the AWS Transit Gateway applies a very specific routing algorithm that is optimized to maintain availability zone affinity.

Good for performance but can lead to challenges with centralized firewall (stateful).



# Workflow - Part 1

1. Source Traffic from Spoke VPC 1 destined towards Spoke VPC 2
2. Connection is initiated, the packet is directed to the AWS Transit Gateway attachment in the same availability zone
3. The Transit Gateway then forwards the packet to the centralized firewall VPC through the attachment in the same availability zone as long as one exists.
4. The centralized firewall VPC is configured to send traffic to a specific firewall endpoint and back to the AWS Transit Gateway.

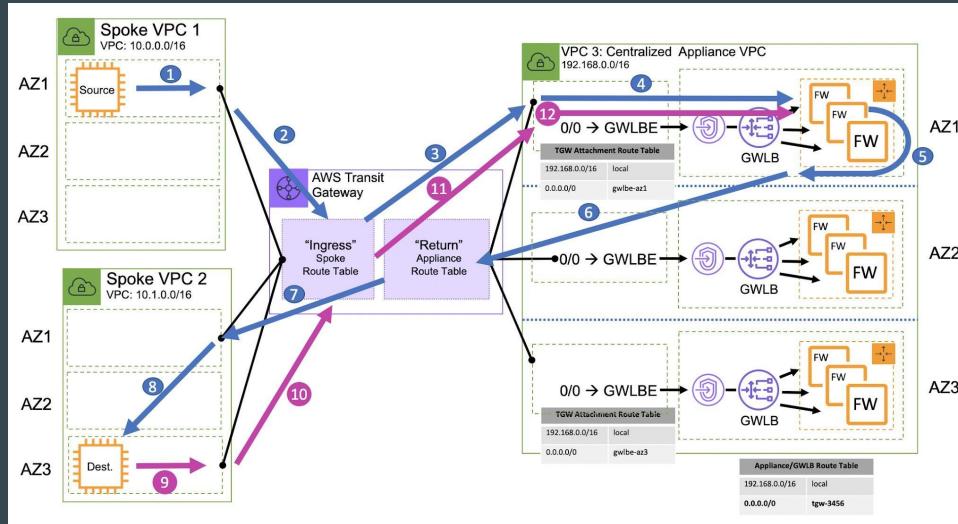
## Workflow - Part 2

5. The AWS Transit Gateway will then send the packet out the attachment in Spoke 2 VPC in Availability zone 1.
6. From there the packet will cross the availability zone boundary to its destination in availability zone 3.
7. When the destination initiates the reply back to the source it is directed to the AWS Transit Gateway attachment in availability zone 3 and is then forwarded to the centralized firewall VPC on the attachment in availability zone 3

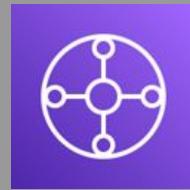
# Appliance Mode

When appliance mode is enabled, a transit gateway selects a single network interface in the appliance VPC, using a flow hash algorithm, to send traffic to for the life of the flow.

The transit gateway uses the same network interface for the return traffic.



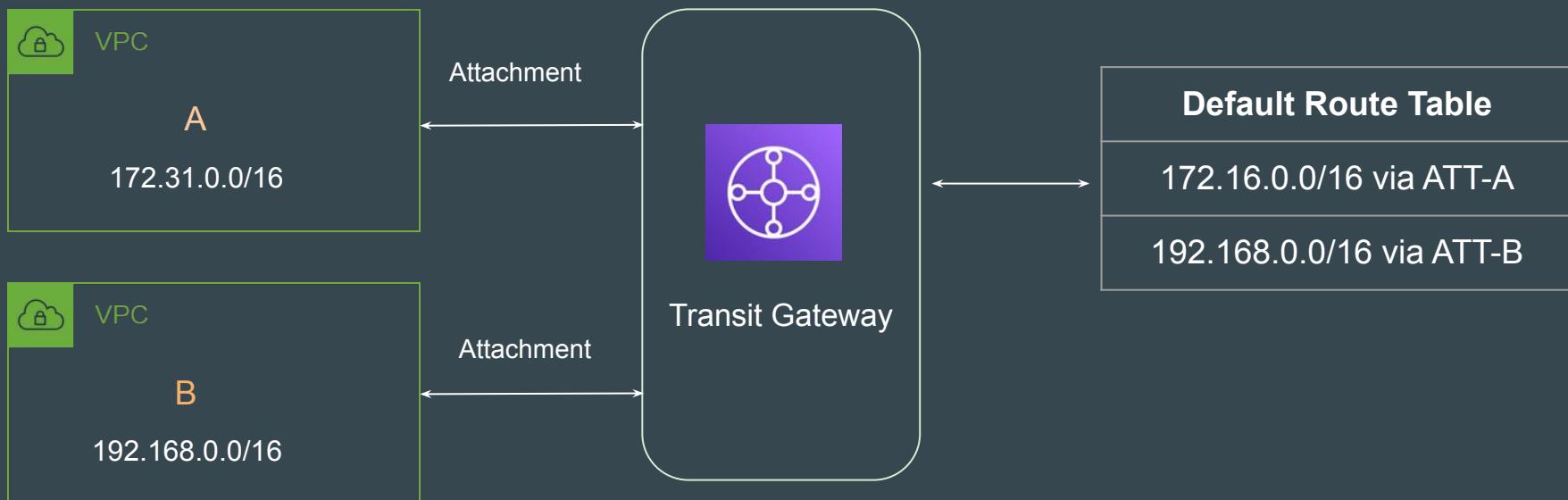
# Attachment Specific Routing



# Default Route Table

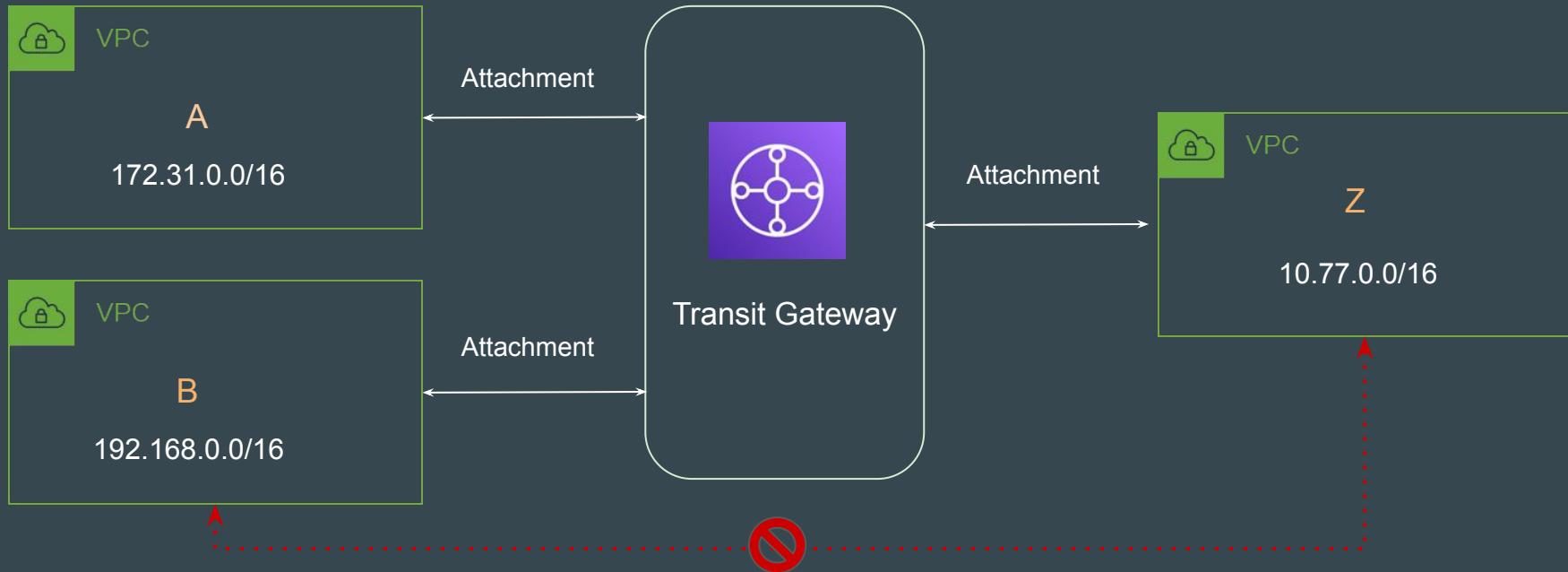
Your transit gateway automatically comes with a **default route table**.

By default, this route table is the **default association route table** and the **default propagation route table**.



# Understanding the Use-Case

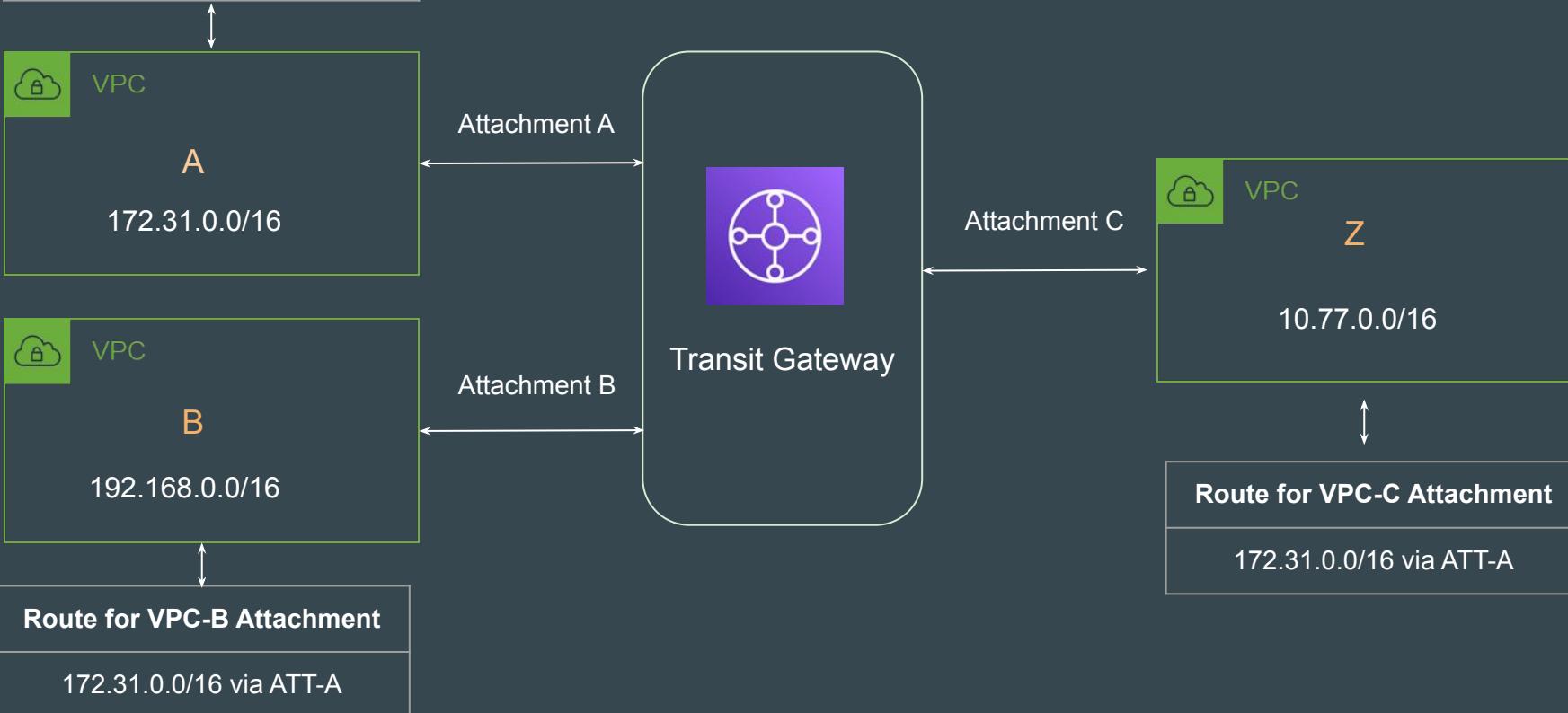
All communication should be allowed **EXCEPT** VPC-B to VPC-Z



### Route for VPC-A Attachment

10.77.0.0/16 via ATT-C

192.168.0.0/16 via ATT-B



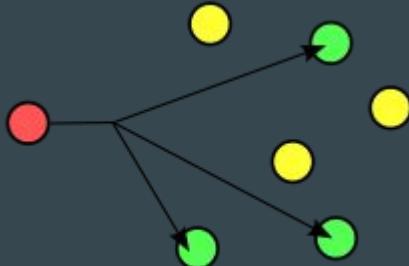
# Multicast on Transit Gateways



# Revising Multicast

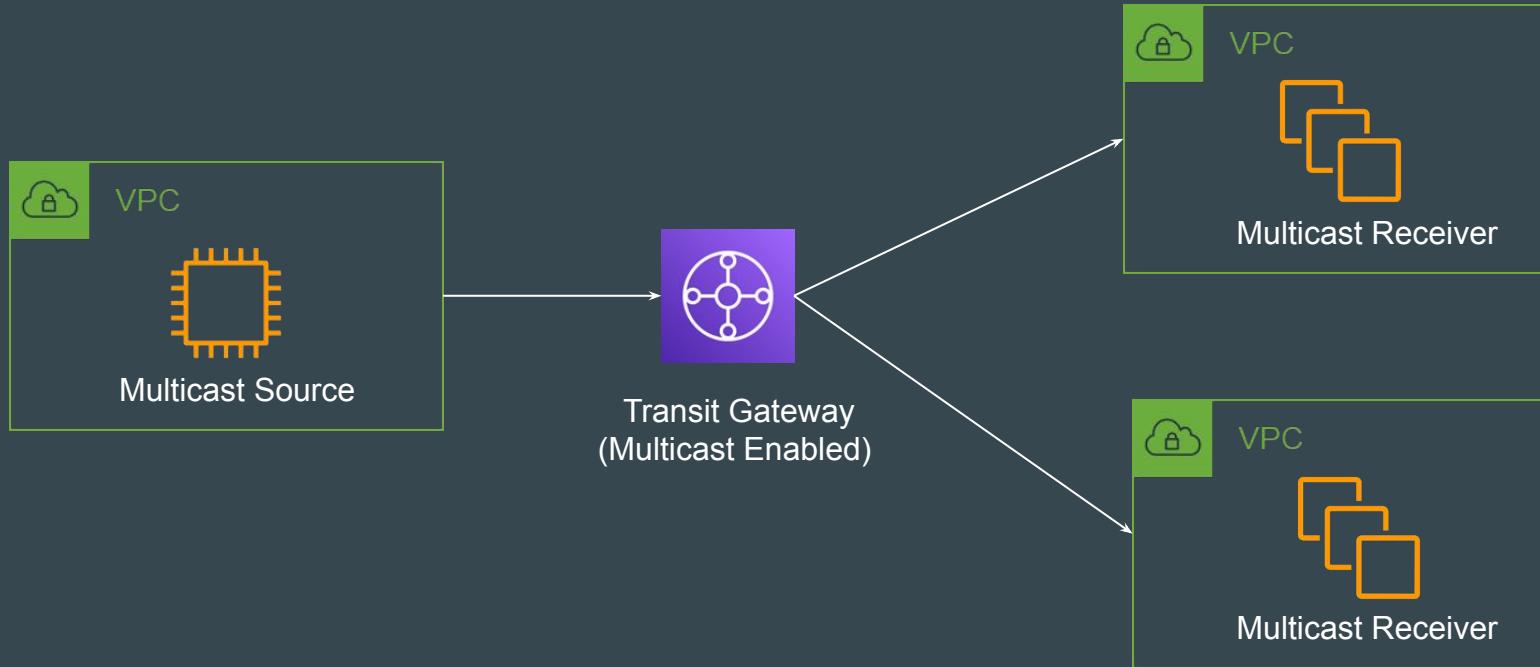
Multicast is a communication protocol used for delivering a single stream of data to multiple receiving computers simultaneously.

Multicast can be one-to-many or many-to-many distribution



# Transit Gateway and Multicast

Transit Gateway can act as a **multicast router** for instances sending traffic destined for multiple receiving instances.



# Multicast Concepts



# Enabling Multicast

To enable Multicast, you must select the “Multicast support” option while creating Transit Gateway.

**Details - optional**

Name tag  
Creates a tag with the key set to Name and the value set to the specified string.

Description [Info](#)  
Set the description of your transit gateway to help you identify it in the future.

**Configure the transit gateway**

Amazon side Autonomous System Number (ASN) [Info](#)

DNS support [Info](#)

VPN ECMP support [Info](#)

Default route table association [Info](#)

Default route table propagation [Info](#)

Multicast support [Info](#)

# Multicast Group

Identifies a set of hosts that will send and receive the same multicast traffic.

Multicast group membership is defined by individual elastic network interfaces attached to EC2 instances.

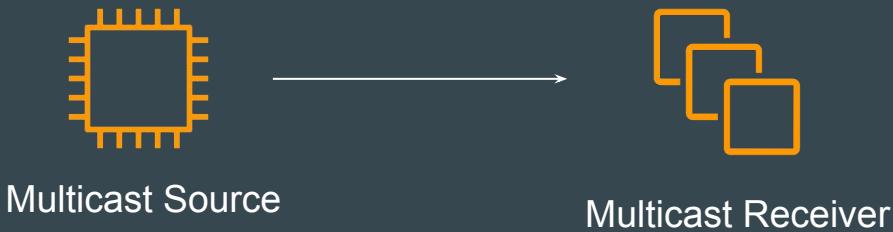
A multicast group is identified by a group IP address.

tgw-mcast-domain-01360bf189739310f / demo-multi-cast-domain														
Details		Associations		Groups		Sharing		Tags						
Groups (3)														
Filter groups								C Actions ▾ Add source						
□	Group IP address	▼	Network interface ID	▼	Member type	▼	Source type	▼	Subnet ID	▼	Attachment ID	▼	Resource type	
□	224.0.0.1		eni-04fe3deb2e9e58a20		Static	-			subnet-0c27e3766fd6...		tgw-attach-059b5d9a136...		VPC	
□	224.0.0.1		eni-08580ba813d2a9e...		Static	-			subnet-02e09c839a55...		tgw-attach-005f858d667...		VPC	
□	224.0.0.1		eni-0ef4022a4b17c2f9		-	Static			subnet-0f5bf06f894ac...		tgw-attach-0a717542c5d...		VPC	

# Multicast Source

The statically-added source sends multicast traffic and the members receive multicast traffic.

An elastic network interface associated with a supported EC2 instance that is statically configured to send multicast traffic.



# Multicast Group Member (Receiver)

An elastic network interface associated with a supported EC2 instance that receives multicast traffic.



# Multicast Domain

Allows segmentation of a multicast network into different domains, and makes the transit gateway act as multiple multicast routers.

You define multicast domain membership at the subnet level.

# Important Considerations

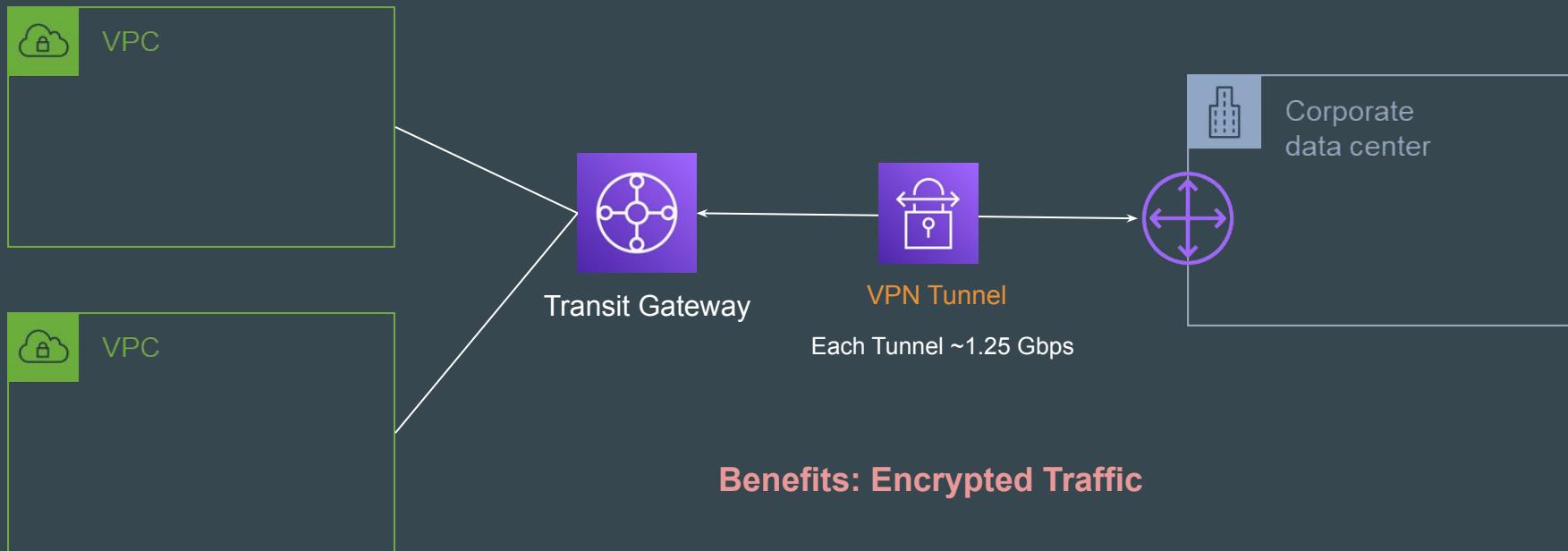
A non-Nitro instance cannot be a multicast sender.

# **Transit Gateway - VPN Attachments**



# AWS Transit Gateway + VPN

AWS Transit Gateway + VPN, using the **Transit Gateway VPN attachment**, provides the option of creating an IPsec VPN connection between your remote network and the Transit Gateway over the internet



## Points to Note

A single VPN tunnel has a maximum throughput of 1.25 Gbps

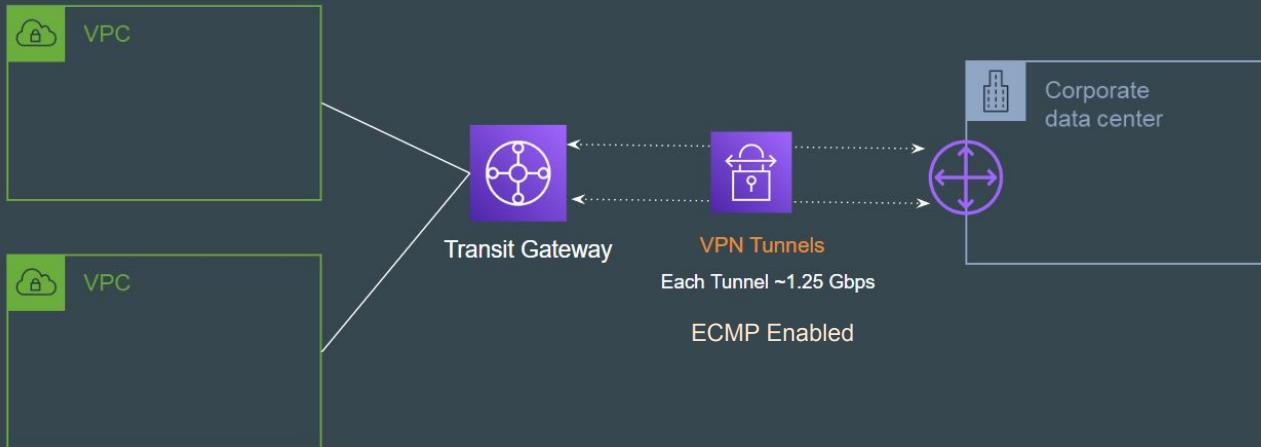
If you establish multiple VPN tunnels to an ECMP-enabled transit gateway, it can scale beyond the default maximum limit of 1.25 Gbps.

Equal-cost multi-path routing (ECMP) is a routing strategy where packet forwarding to a single destination can occur over multiple best paths with equal routing priority.

# Transit Gateway with Multiple VPN Connection

When you create your VPN, you must choose Dynamic for Routing options. Static routing does not support ECMP.

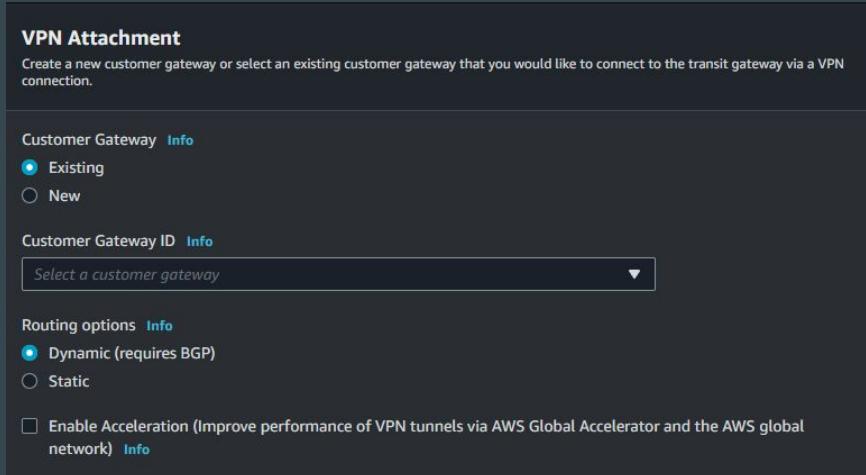
When you create your transit gateway, you must enable **VPN ECMP support**.



# VPN Attachment

To attach a VPN connection to your transit gateway, you must specify the customer gateway.

For static VPNs, we have to add the static routes to the transit gateway route table.



## ECMP with multiple VPN tunnels with a transit gateway

Ensure that your customer gateway is configured to perform ECMP for traffic going out to AWS for all VPN tunnels.

Confirm that your customer gateway is advertising the on-premises prefix to AWS with the same BGP AS PATH attribute.

For AWS to choose all the available ECMP paths, the AS Path and AS Number must match.

# Example Configuration

You plan to use ECMP with two VPN connections. The AS Number of your customer gateway is 65270. In this scenario, you configure your VPNs as follows:

## VPN-A

- Tunnel 1 – AS PATH: 65270 (while advertising the prefix)
- Tunnel 2 – AS PATH: 65270 (while advertising the prefix)

## VPN-B

- Tunnel 1 – AS PATH: 65270 (while advertising the prefix)
- Tunnel 2 – AS PATH: 65270 (while advertising the prefix)

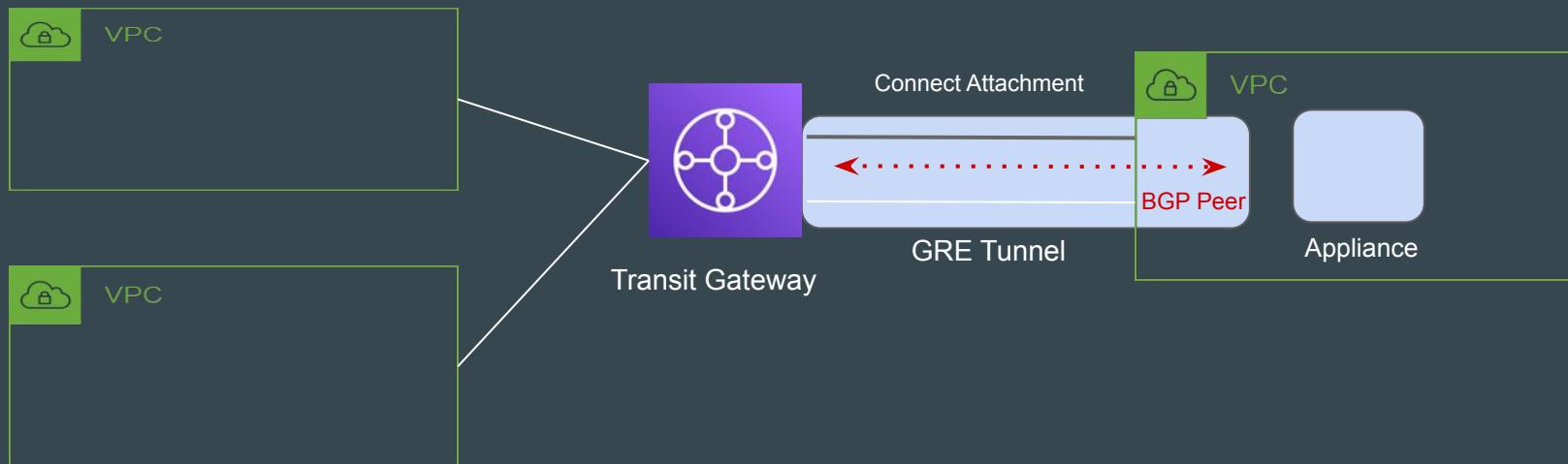
With a configuration similar to this information, AWS sends out traffic with ECMP on all four VPN tunnels.

# **Transit Gateway - Connect Attachments**



# Connect Attachment

A connect attachment allows you to establish connection between a transit gateway and the third-party appliances **using** Generic Routing Encapsulation (GRE) and Border Gateway Protocol (BGP).



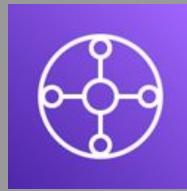
## Points to Note

Transit Gateway Connect allows you to establish connectivity both for on-premises SD-WAN infrastructure or SD-WAN appliances running in the cloud through **VPC attachment**, or **AWS Direct Connect attachment** as the underlying transport layer.

Up to 20 Gbps total bandwidth per Connect attachment

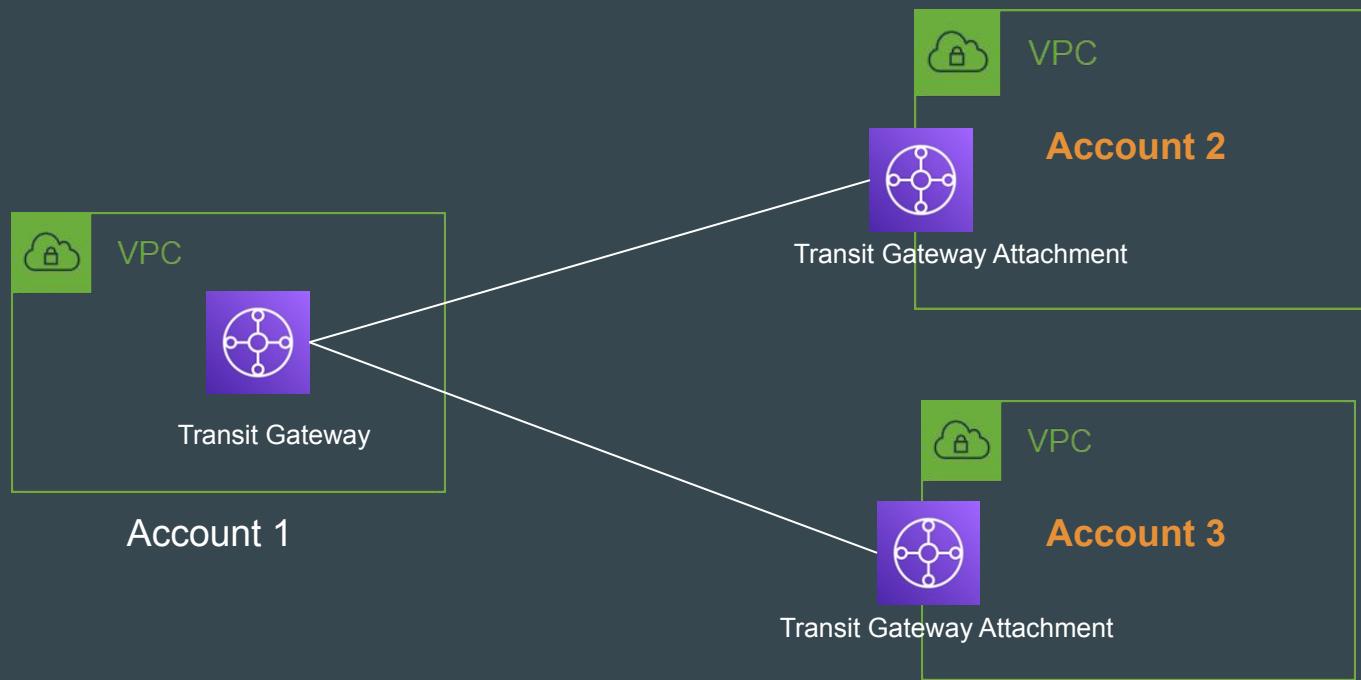
Static routes are not supported.

# Transit Gateway Sharing



# Base Architecture

Transit Gateway sharing allows VPCs across multiple accounts to use Transit gateway for inter-connectivity.



## Points to Note

An AWS Site-to-Site VPN attachment must be created in the same AWS account that owns the transit gateway.

When a transit gateway is shared with you, you cannot create, modify, or delete its transit gateway route tables, or its transit gateway route table propagations and associations.

---

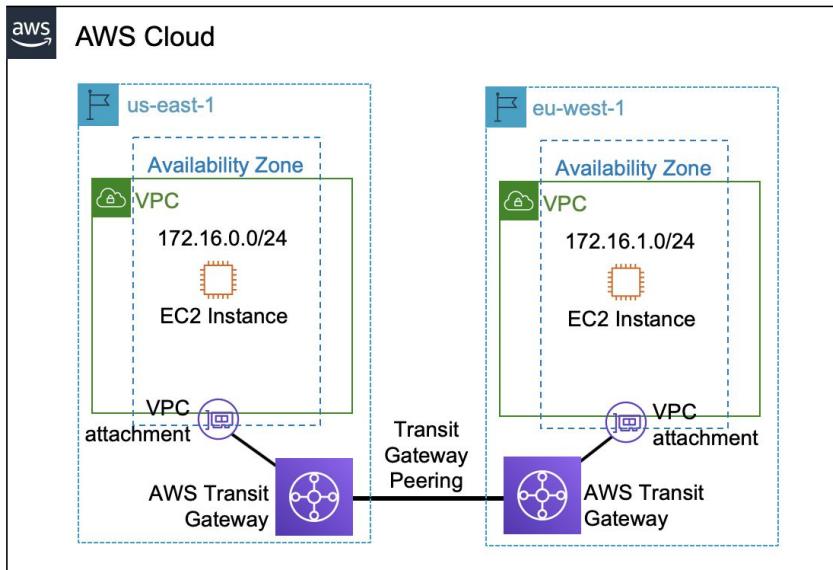
# Transit Gateway Peering

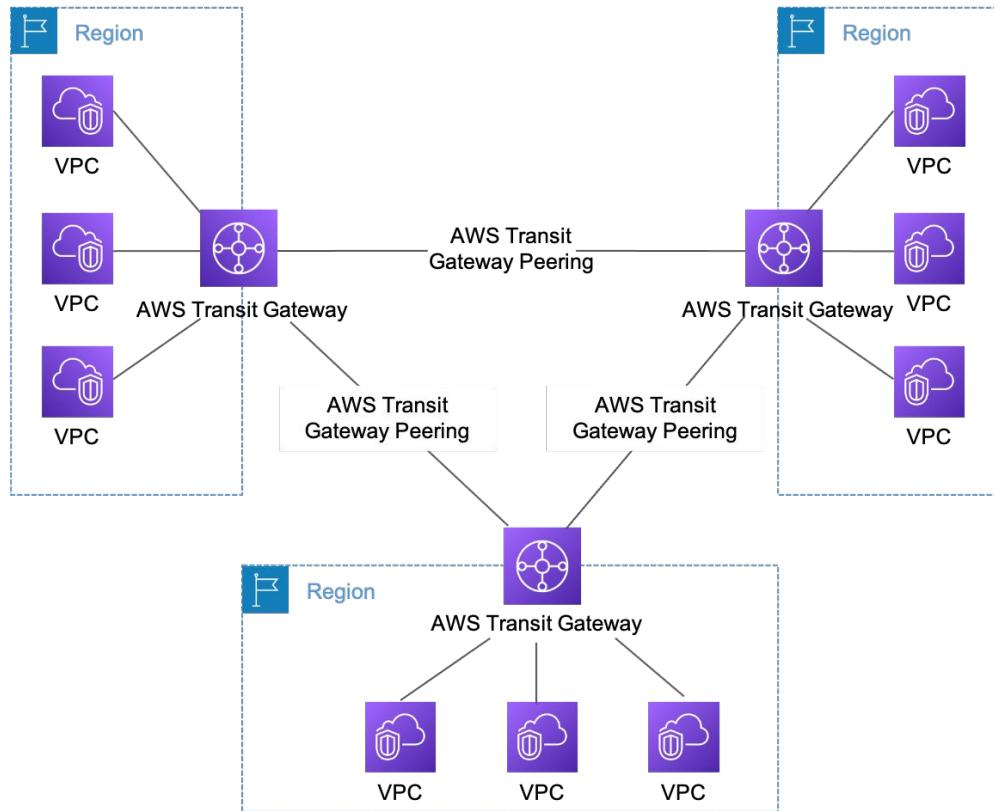
Let's Peer

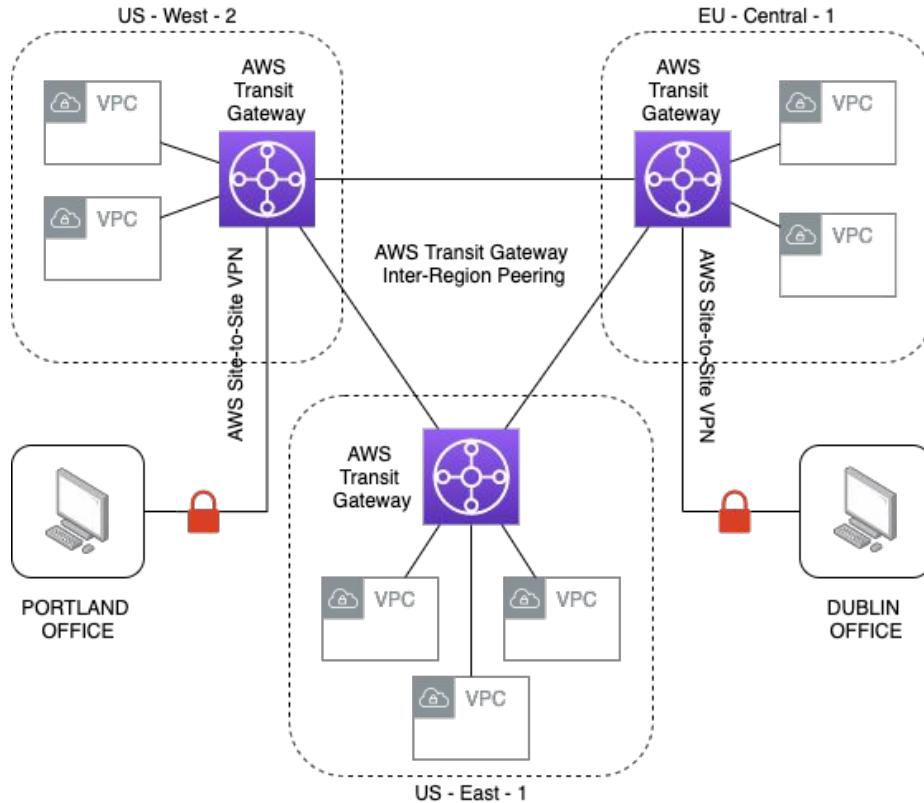
---

# Understanding TGW Peering Setup

Transit Gateway Peering allows us to peer two transit gateways and route traffic between them, which includes IPv4 and IPv6 traffic.







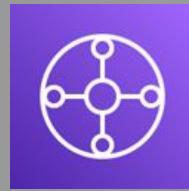
## Important Pointer

After you create a peering attachment request, the owner of the peer transit gateway (also referred to as the accepter transit gateway) must accept the request.

To route traffic between the transit gateways, add a static route to the transit gateway route table that points to the transit gateway peering attachment.

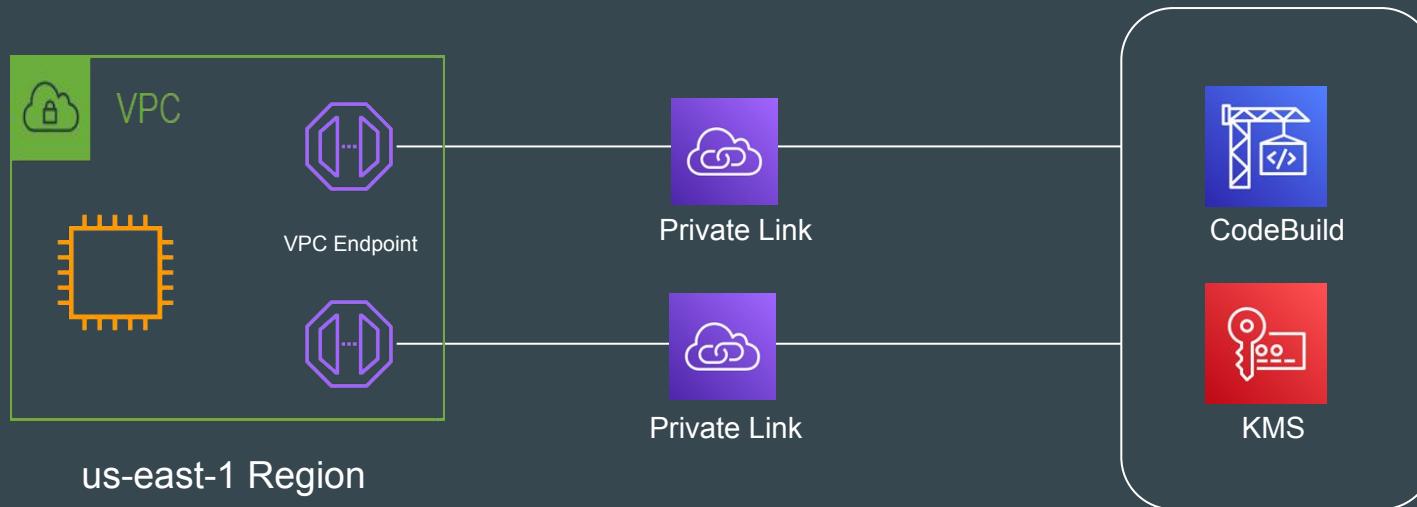
Transit gateway peering uses the same network infrastructure as VPC peering and is therefore encrypted.

# Centralized Access to VPC Endpoints



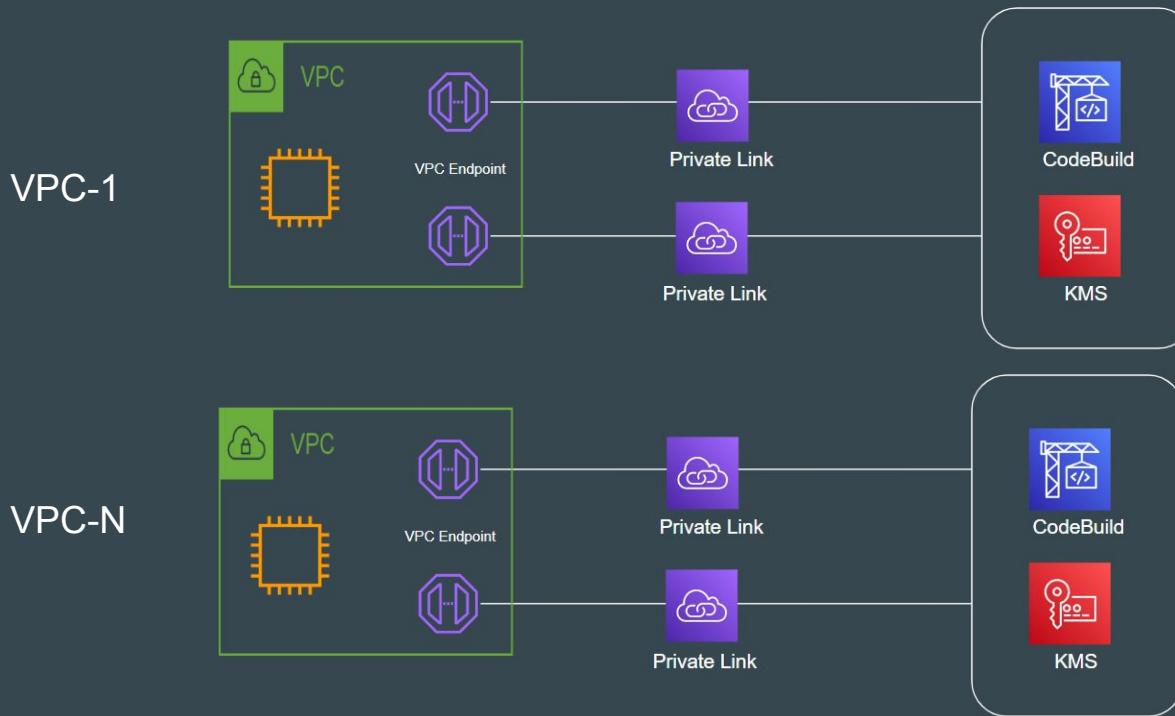
# Base Architecture

EC2 instance is using VPC Endpoints to connect with multiple AWS services.



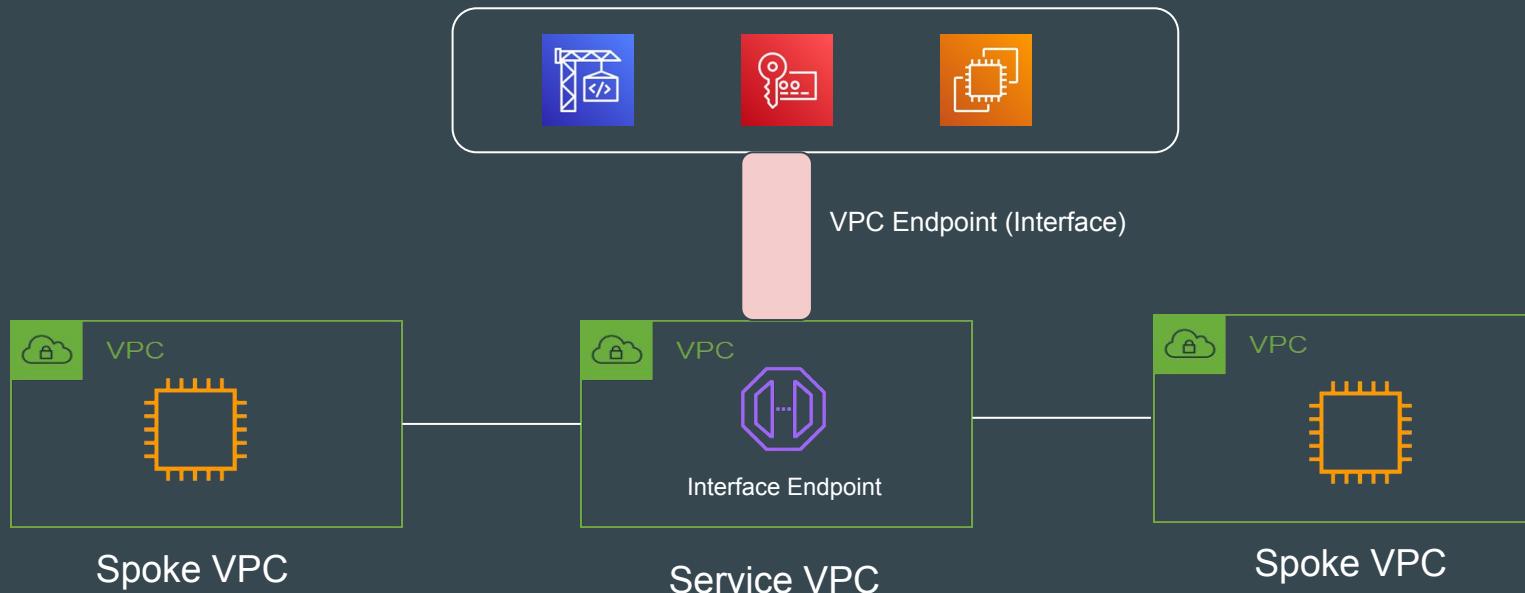
# Understanding the Challenge

More the number of VPCs → More the VPC Endpoints → Higher the Pricing.



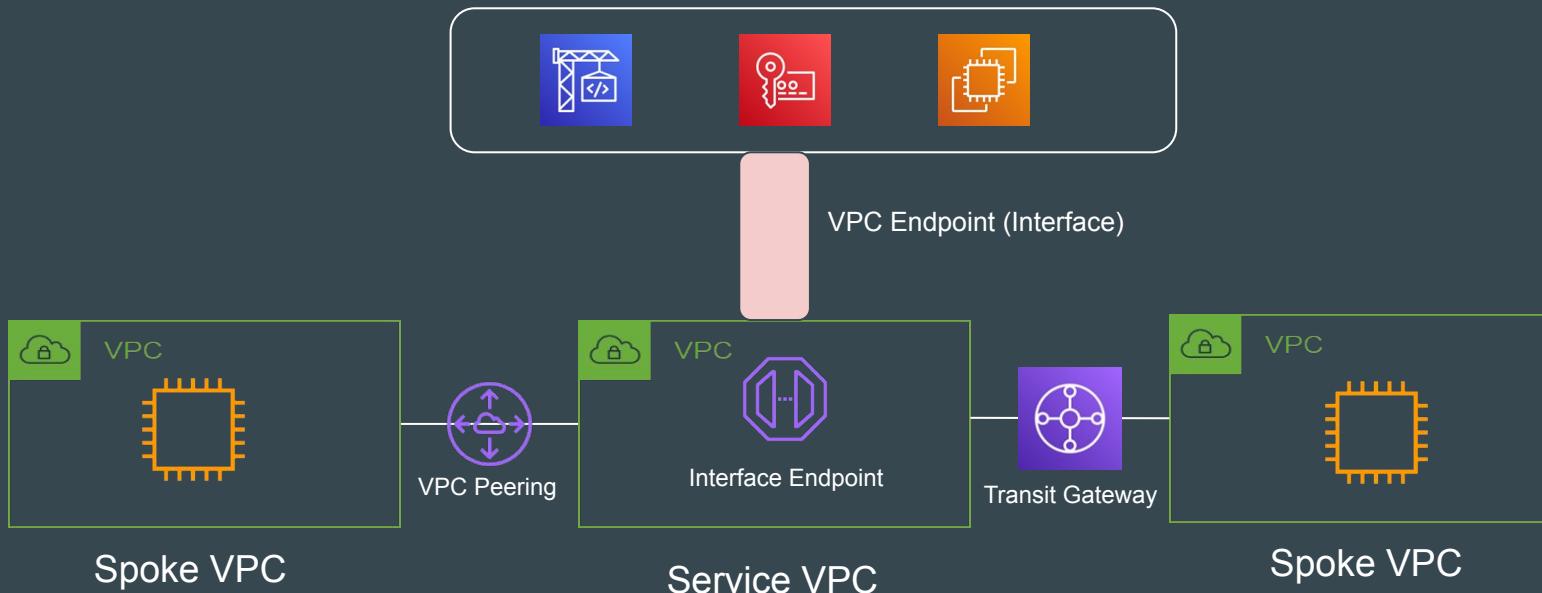
# Centralized Architecture

Following architecture allows centralized access to VPC interface endpoints to access AWS services across multiple VPCs



# Connectivity - Spoke to Service VPC

Connectivity between Spoke to Service VPC can be done using VPC Peering as well as Transit Gateways.



# Challenge with the DNS Resolution

We can enable the Private DNS for an interface endpoint and with that we can resolve the AWS service endpoint DNS from within the same VPC

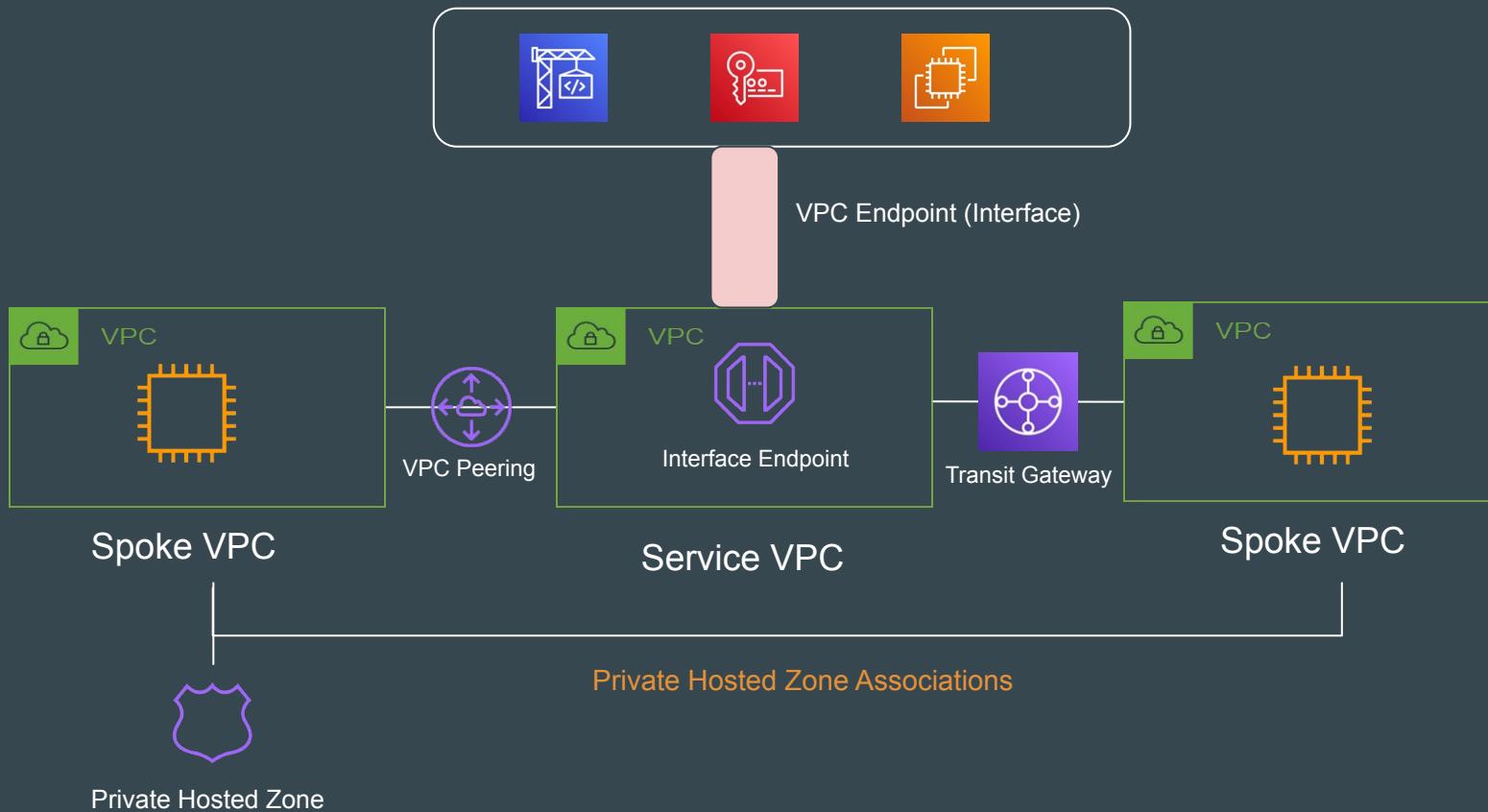
ec2.us-east-1.amazonaws.com → 10.77.0.15

However, the AWS service endpoint **does not resolve** from the peered VPCs.

# Suggested Solution

1. Disable Private DNS from VPC Endpoint.
2. Create a Private Hosted Zone with Full Service Endpoint URL.
3. Create Alias Record to the Regional VPC Endpoint.
4. Ensure PHZ is associated with appropriate VPC

# Final Architecture



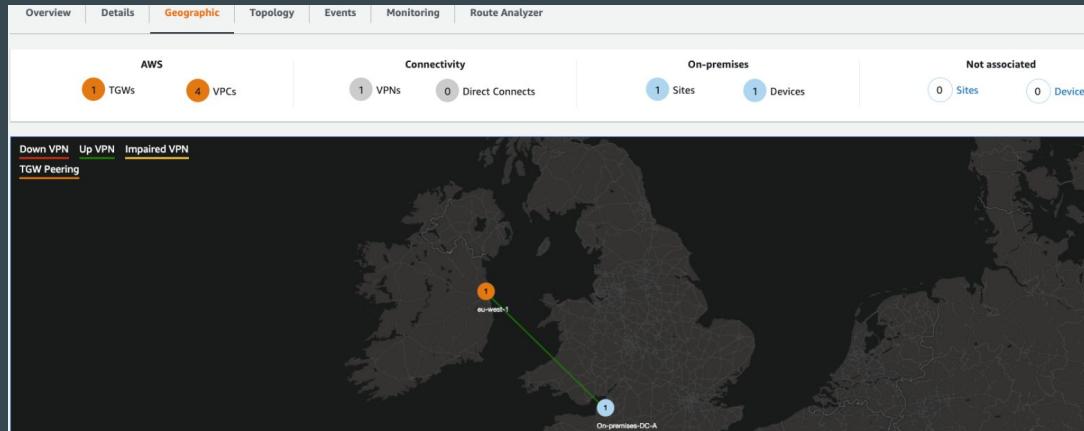
# Transit Gateway Network Manager



# Understanding the Basics

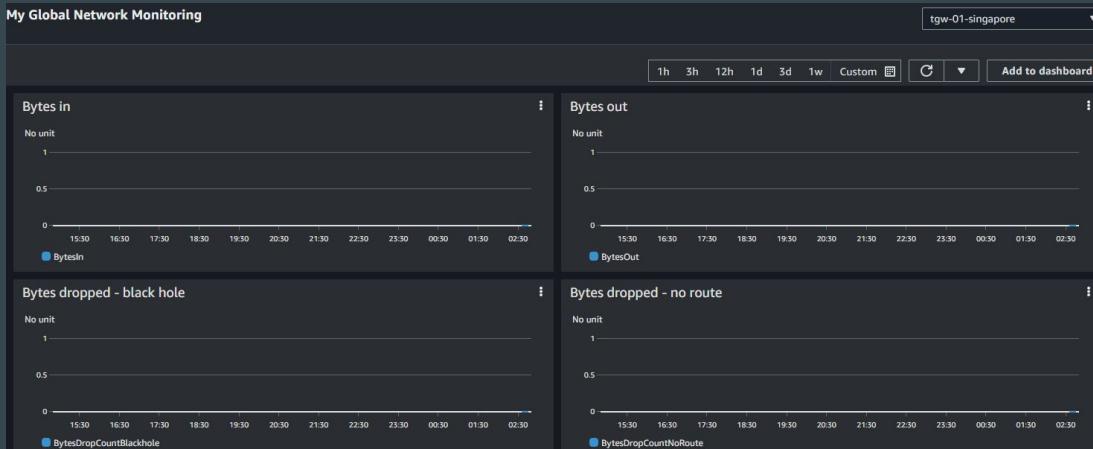
AWS Transit Gateway Network Manager provides a **single global view** of your private network.

This enables you to visualize your global network in a topology diagram and in a geographical map.



# Monitoring

From the console, you can review utilization metrics, such as bytes in/out, packets in/out, packets dropped and alerts for changes in the topology, routing or up/down connection status.



# Benefits of Transit Gateway Network Manager

Benefits	Description
Centralized Network Monitoring	Includes events and metrics to monitor the quality of your global network, both in AWS and on premises.
Global Network Visibility	Visualize and monitor your global network solely from the dashboard of the AWS Transit Gateway Network Manager
SD-WAN Integration	seamlessly integrates with SD-WAN solutions, from Cisco, Silver Peak, etc making it the unified interface to manage your global network across AWS and on-premises locations.

# Sample Use-Cases

Use-Case	Description
Quickly add on-premises locations	<p>AWS TGW's SD-WAN partners makes it very easy to add new on-premises locations to your network.</p> <p>You can connect new network locations remotely from your SD-WAN console and the AWS global network.</p>
Respond to connectivity problems	<p>Provides you with event notifications from a single interface (global view).</p> <p>You can identify and troubleshoot network problems faster than if you received the information from different tools.</p>

---

# Link Aggregation Groups

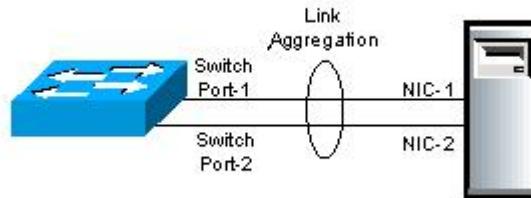
Direct Connect



# Getting Started

Link aggregation enables you to group Ethernet interfaces to form a single link layer interface, also known as a link aggregation group (LAG) or bundle.

There are various advantages which includes increasing network throughput beyond what a single connection could sustain, and also to provide redundancy in-case one of the link fails.



# DX and LAG

In DX perspective, LAG uses Link Aggregation Control Protocol (LACP) to aggregate multiple 1Gbps or 10 Gbps connection at single direct connect location, allowing customers to treat them as single managed connection.

Once we create LAG, we can associate existing connection with the LAG

# Important Pointer for DX and LAG

- All the connection in LAG must use the same bandwidth.
- Bandwidth of 1 Gbps and 10 Gbps are supported.
- You can have maximum of 4 connections in a LAG.
- All connection in LAG must terminate at same DX location and on the same AWS device.

# Important Pointer for LAG and DX

All the LAG's that we create must have an attribute which determines minimum number of connection in LAG that must be operational for the LAG itself to be operational.

Let's understand this with an example:

Total Connection for our LAG = 4

Minimum Number of Connection = 2

If two connection would fail, the overall status would be **Up**

If third connection fails, the overall status will be **Down** (even if single connection is still there)

---

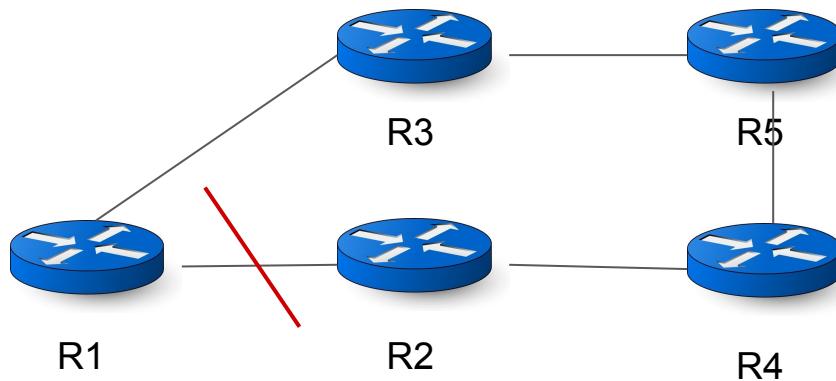
# Bidirectional Forwarding Detection

BFD

# Understanding the Challenge

Detecting a Link failure in time is one of the important aspects in production environments.

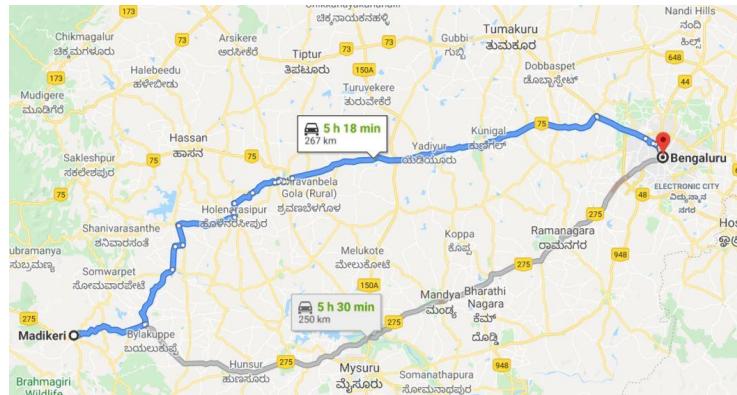
In the below diagram, let's assume packet from R1 needs to reach to R4.



# Simple Analogy - Google Map

When travelling from Point A to Point B, Google Maps shows the optimum route.

In order to detect the best route, Google Maps needs to quickly check the traffic and other congestion aspects (ongoing road repairs and others)



# Typical Solution

Various routing protocols like OSPF can select another path if they lose neighbor but it takes a while for them to realize that something is wrong.

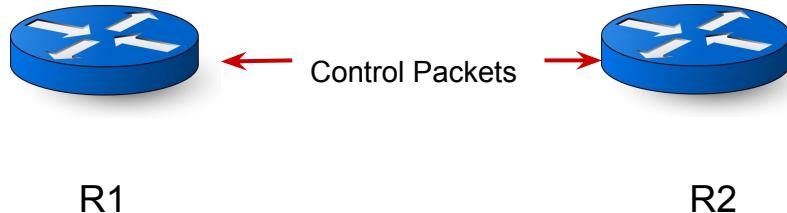
For example, OSPF can be tuned at a one-second interval level however these protocols are not designed for sub-second failure detection.



# Understanding BFD

The Bidirectional Forwarding Detection (BFD) protocol is a simple mechanism that detects failures in a network

One great benefit of BFD is that it can detect a link failure within milliseconds or even microseconds.

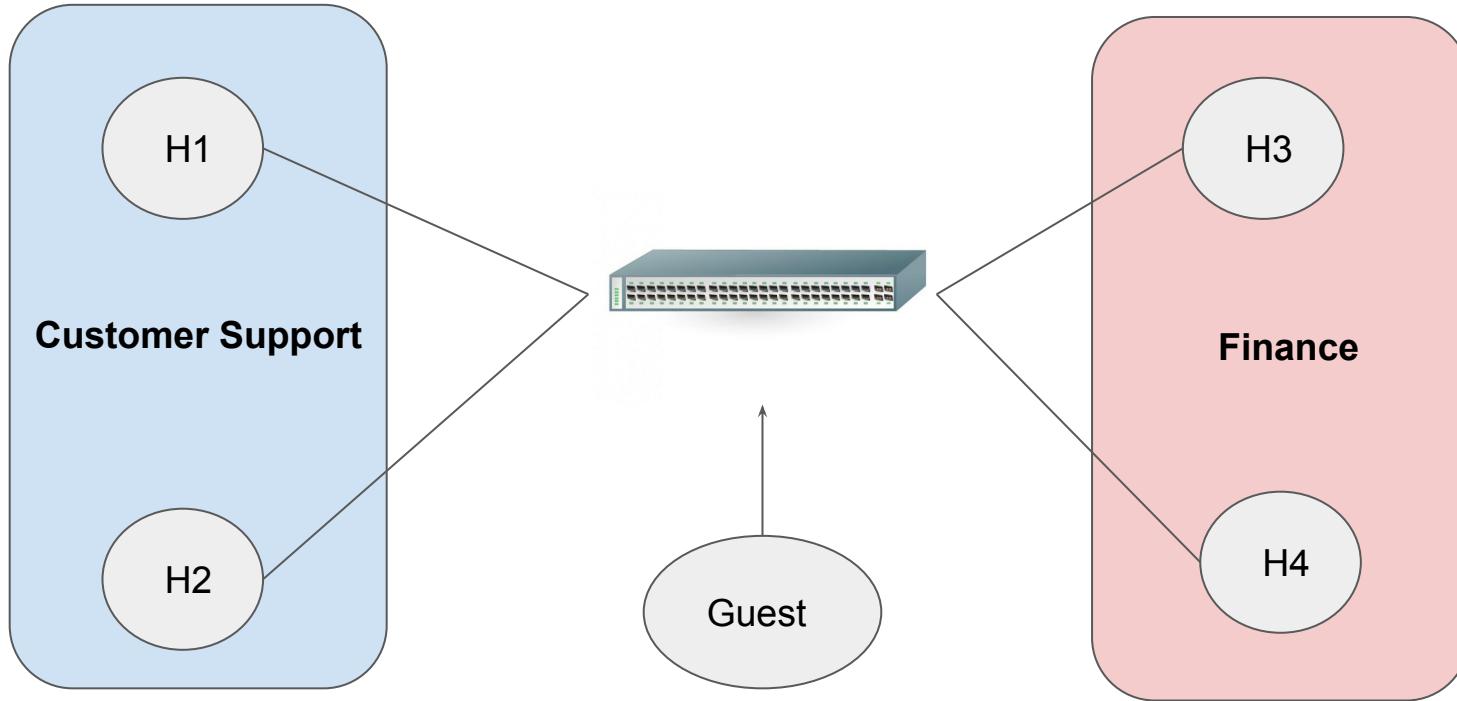


---

# Virtual Lans (VLANS)

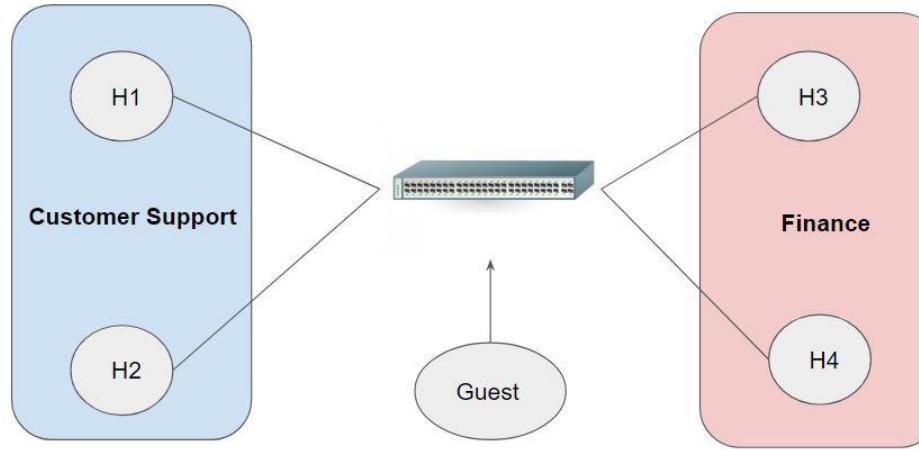
Let's Network

# Understanding Typical Setup



# Challenges with Traditional Approach

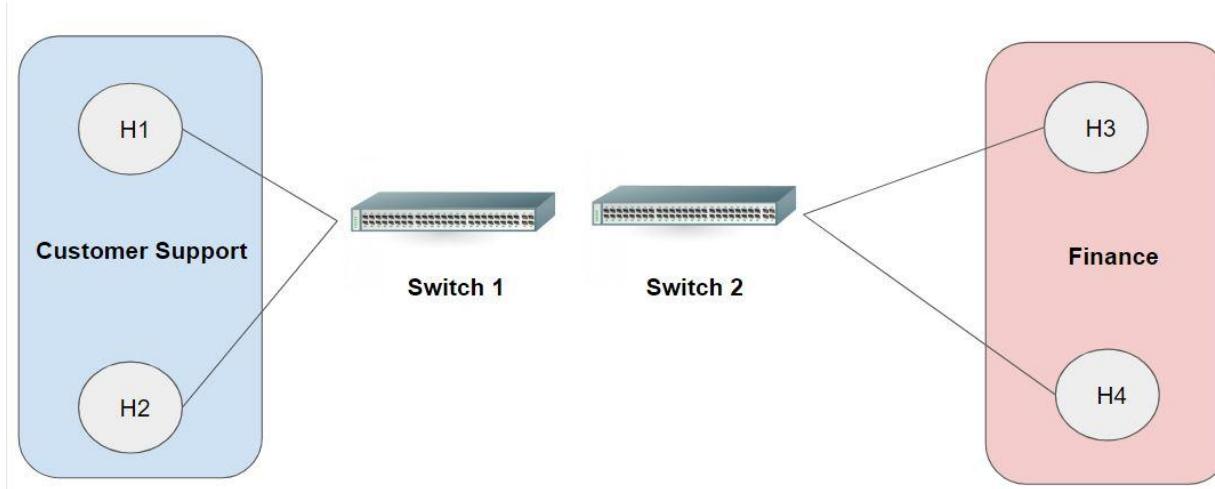
There can be a requirement where there is a need of isolation between different departments within the organization.



# Possible Solution

To isolate the host and communication, one possible way is to have different switches.

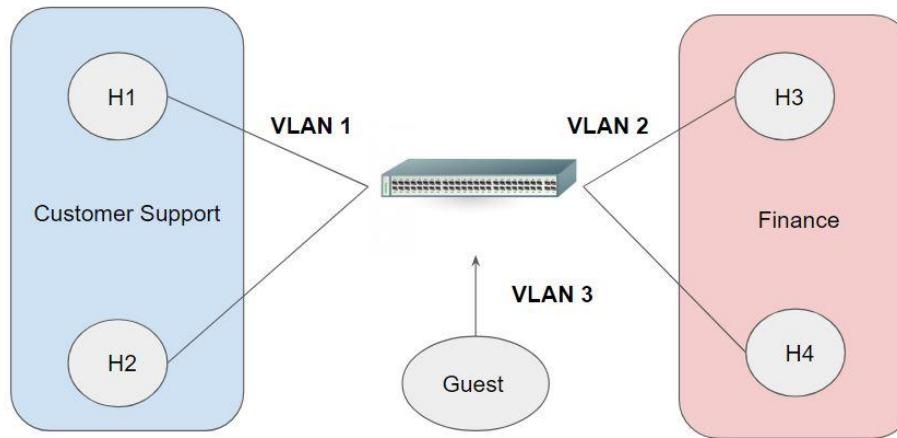
Hosts across switches by default will not be able to communicate with each other.



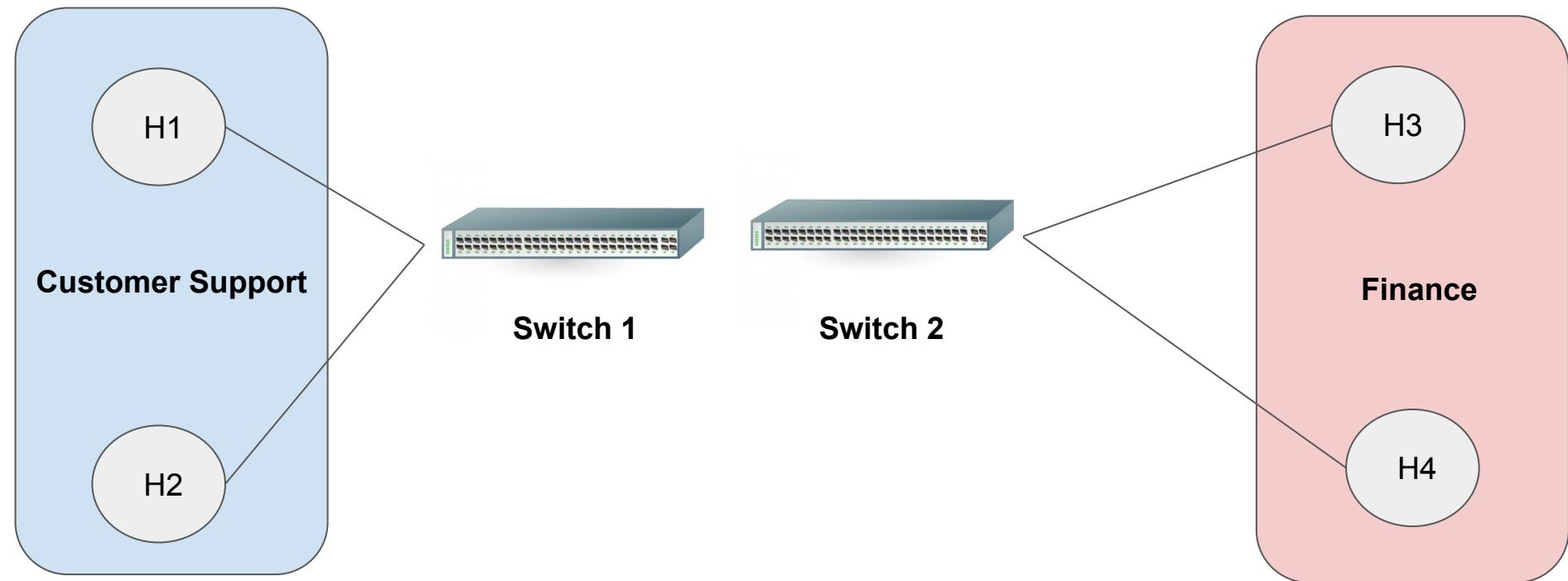
# Better Solution

With VLAN, we can have a single switch, and separate hosts into multiple separate networks and provide the required isolation (logical instead of physical)

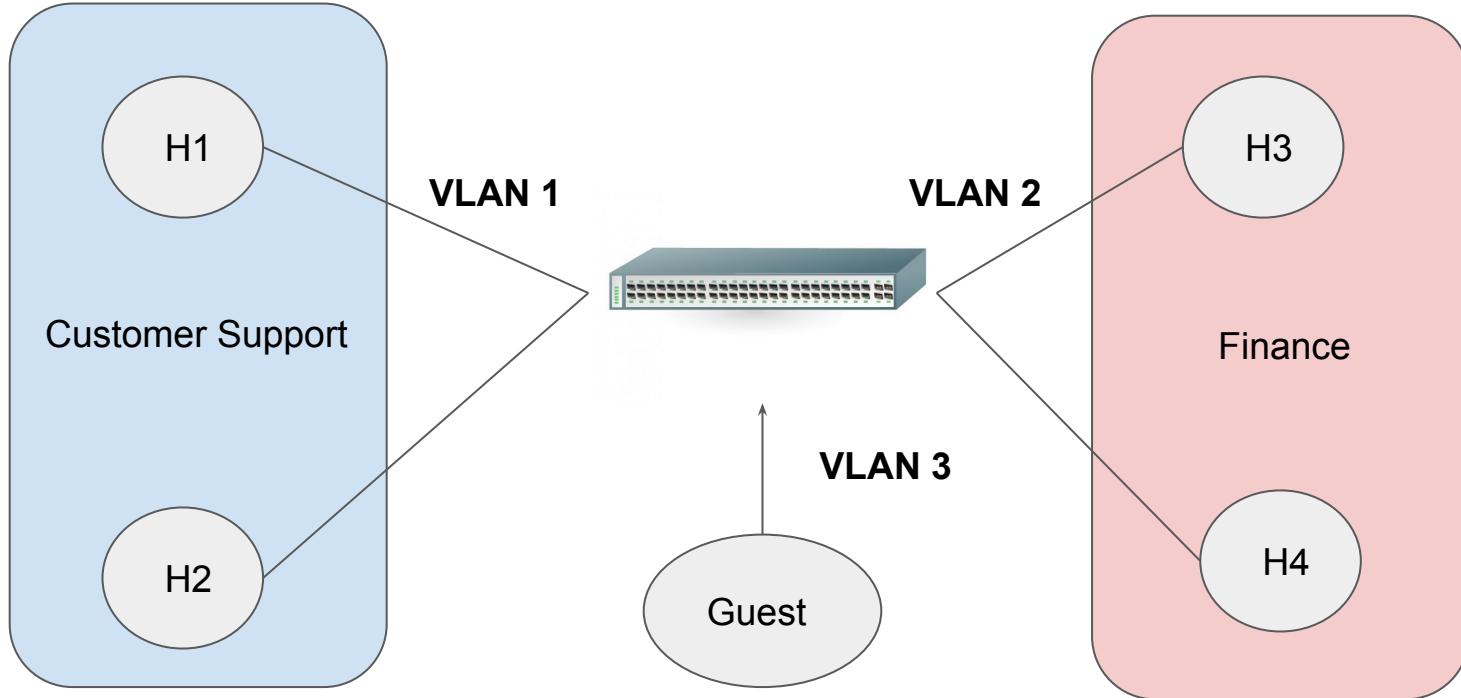
We can implement security controls on each of these network separately.



# Typical Solution



# VLAN Setup



---

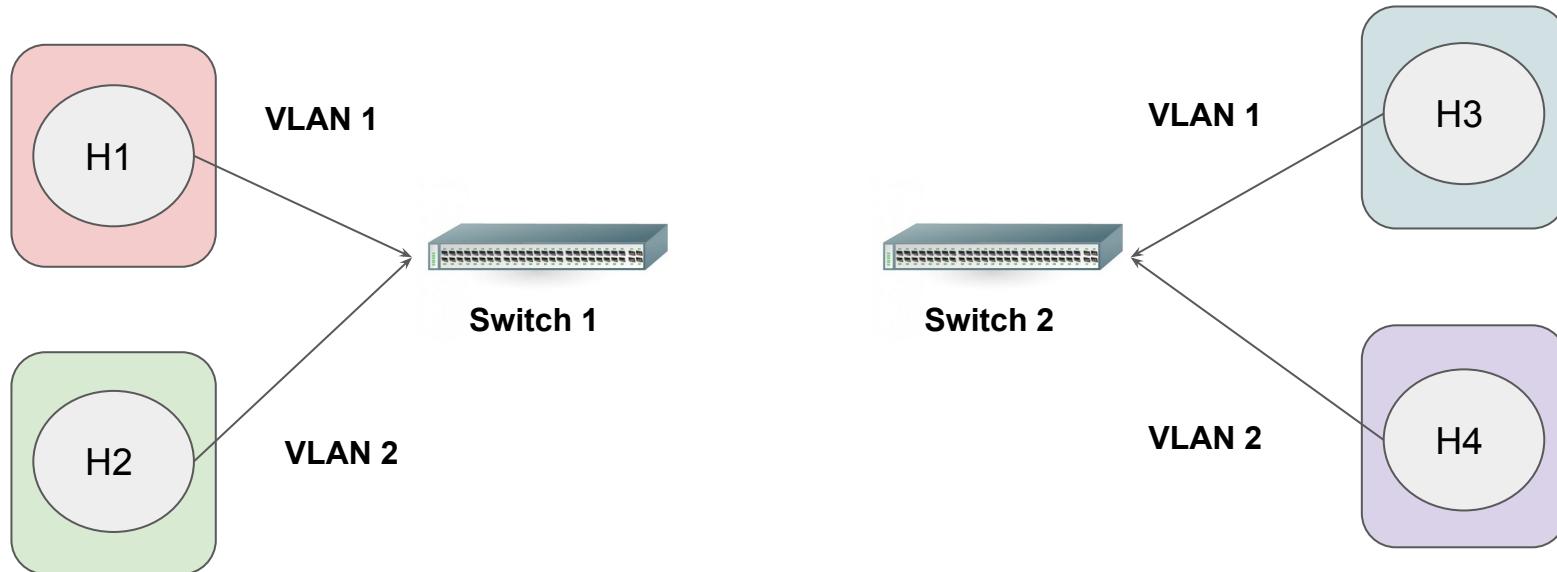
# VLAN Tagging

Virtual Lans are Awesome!

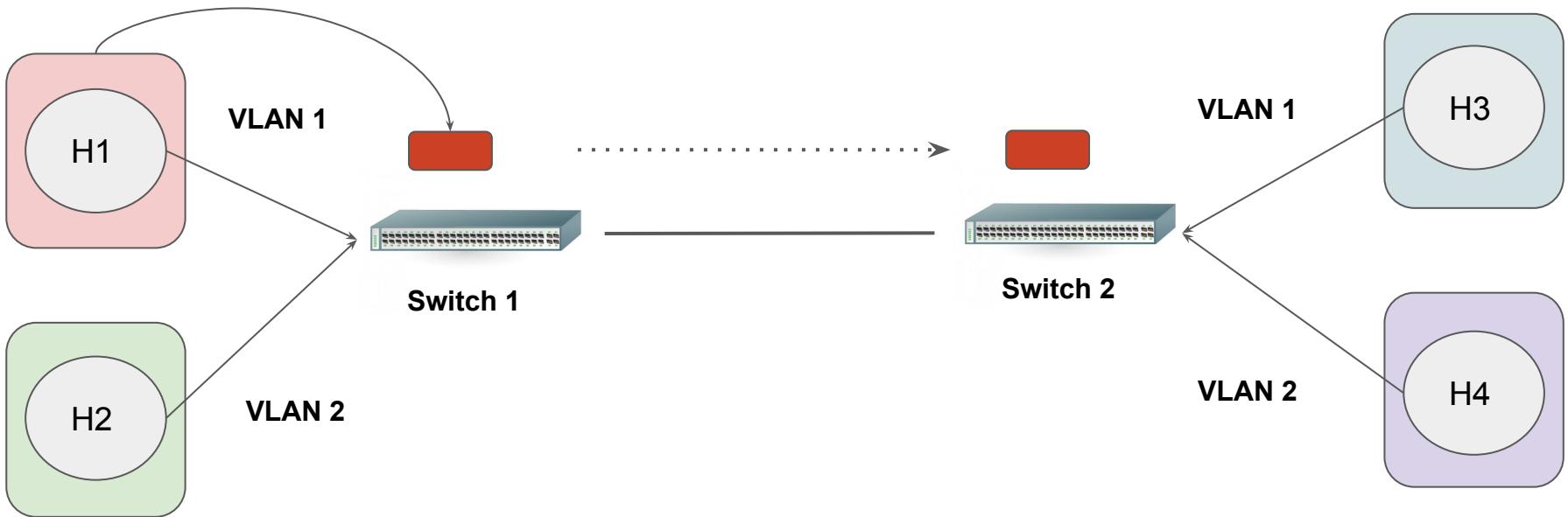
---

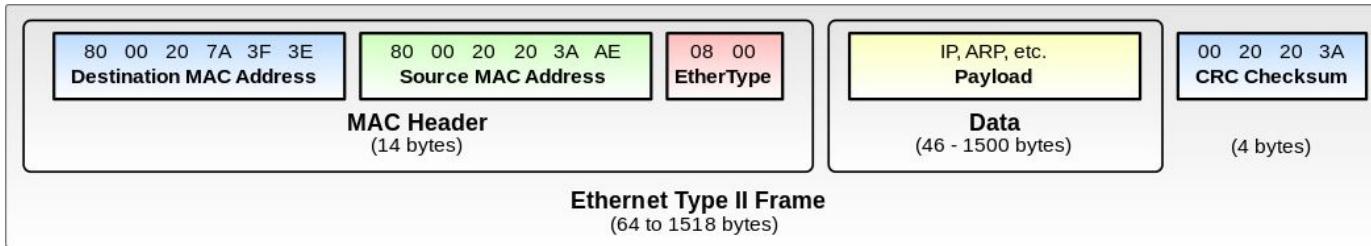
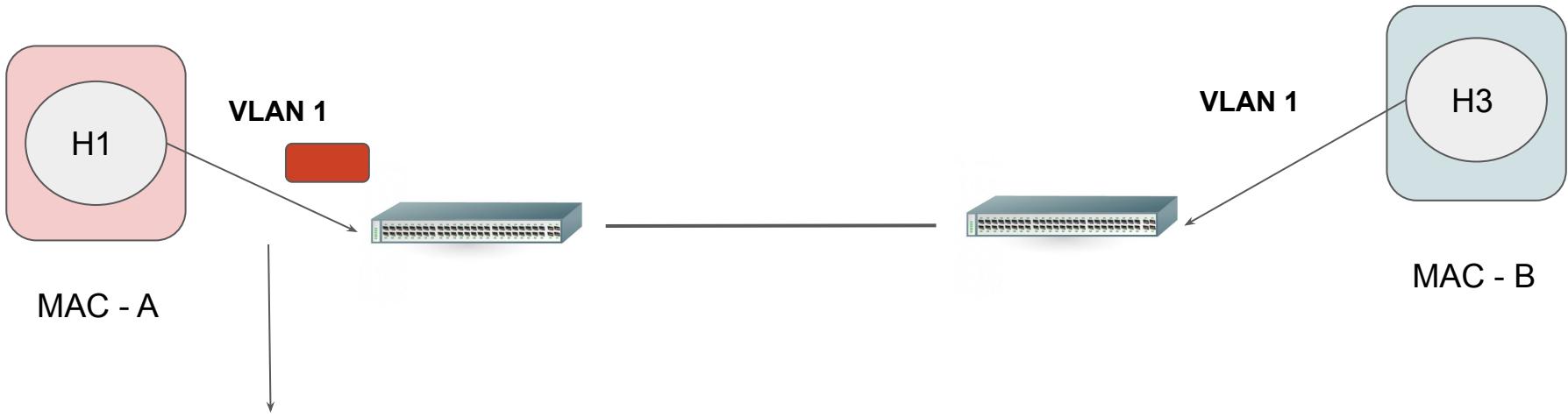
# Getting Started

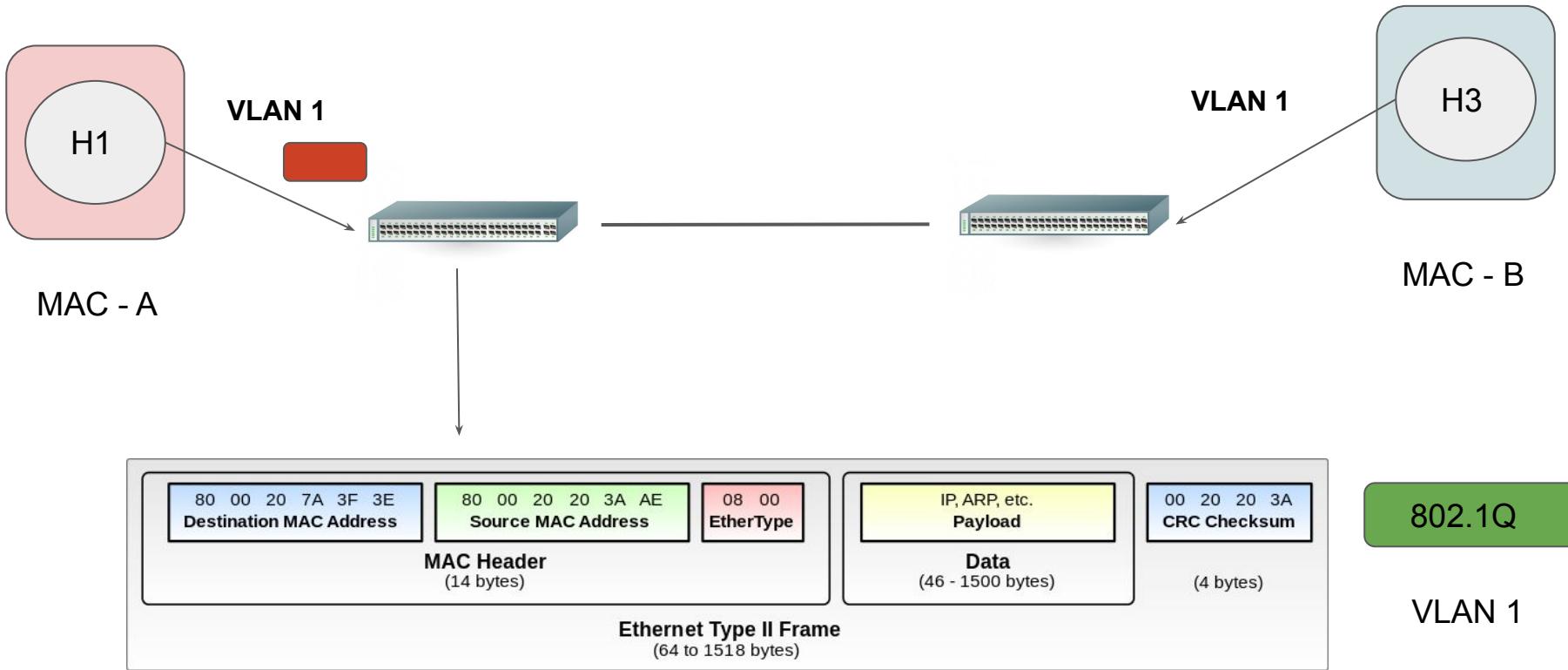
802.1Q is the networking standard that supports VLANs on an ethernet network.

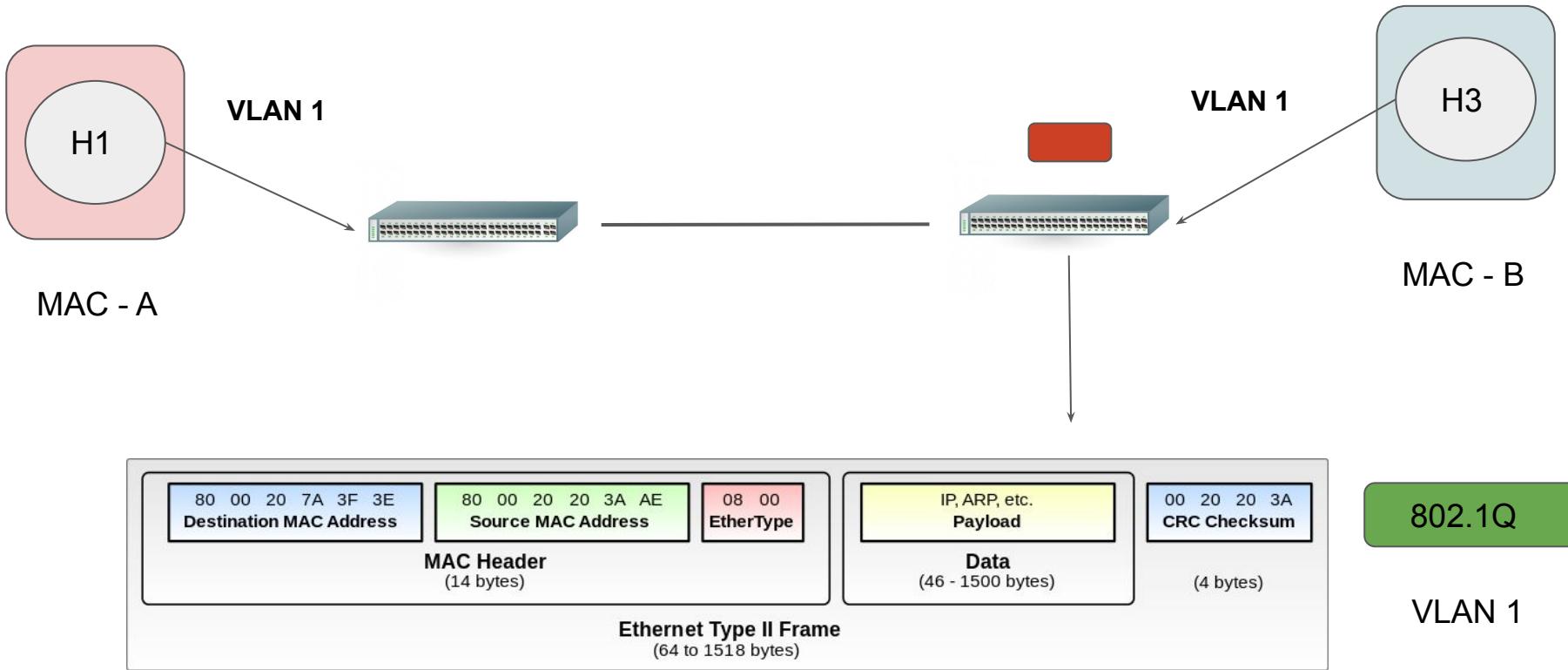


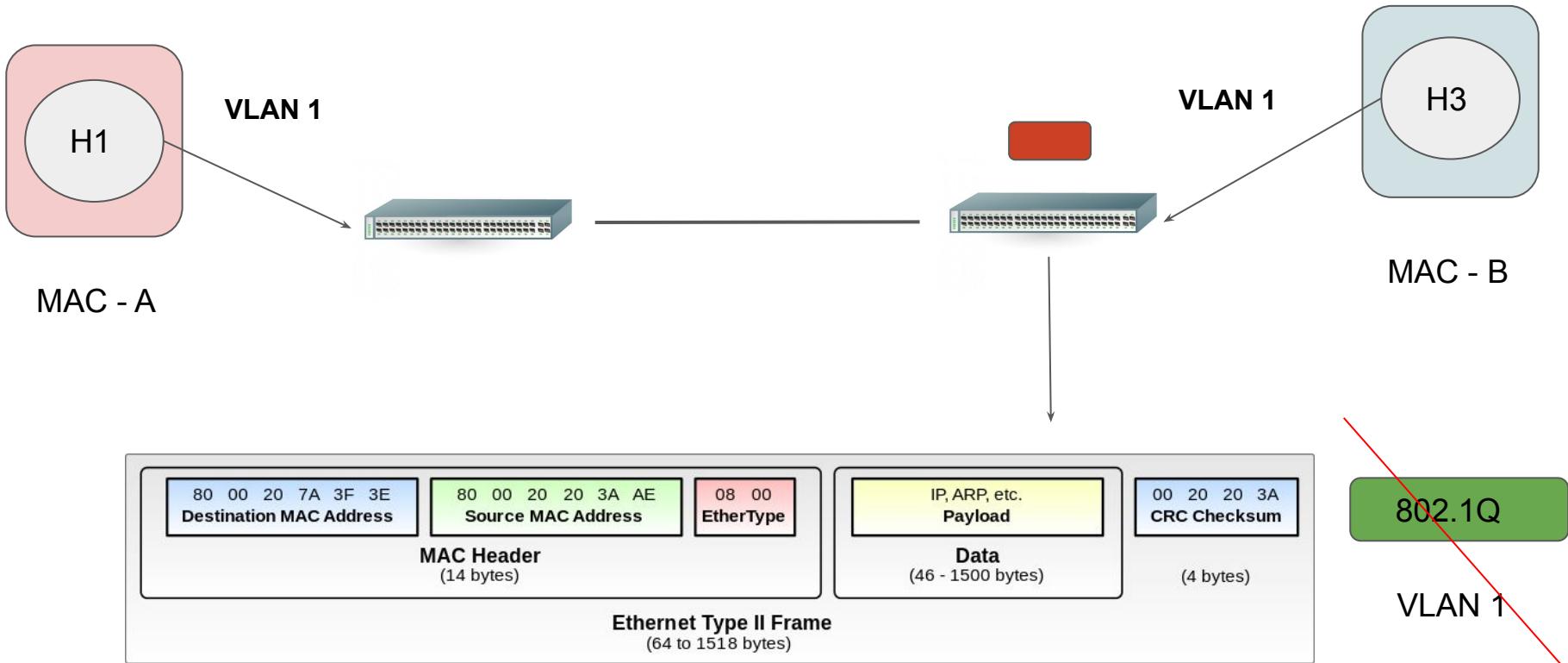
# Understanding the Challenge



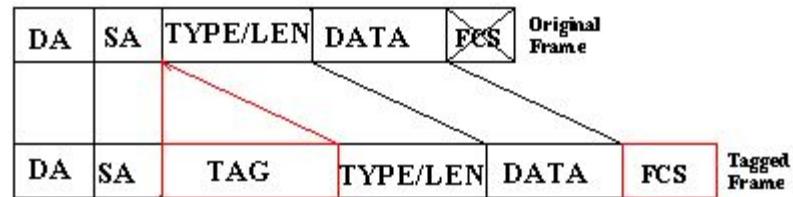




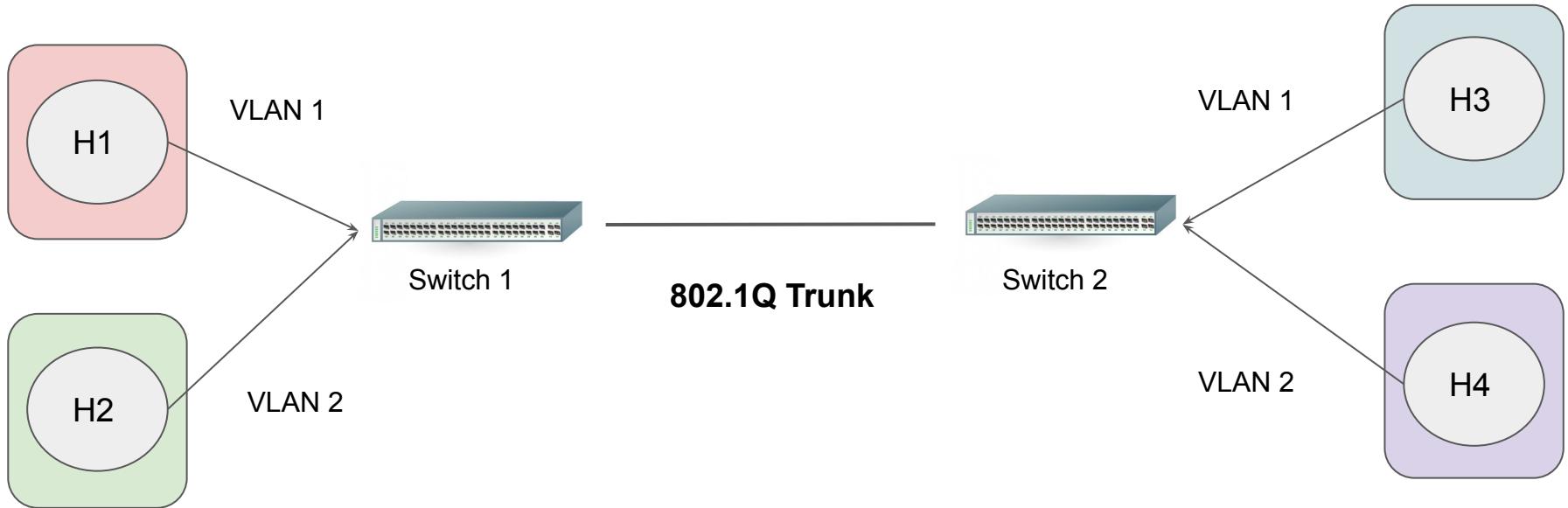




# Frame Format



# 802.1Q Trunk



---

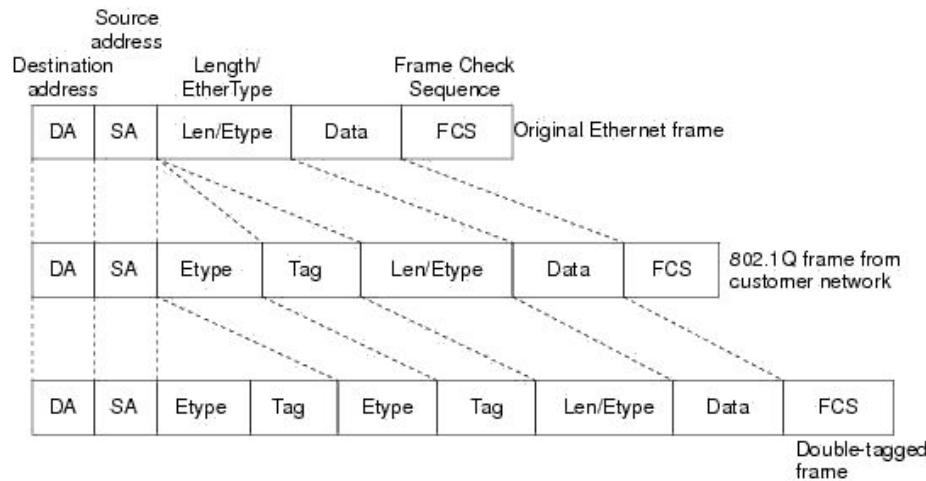
# Q-in-Q Tunneling

Tagging and Tagging

---

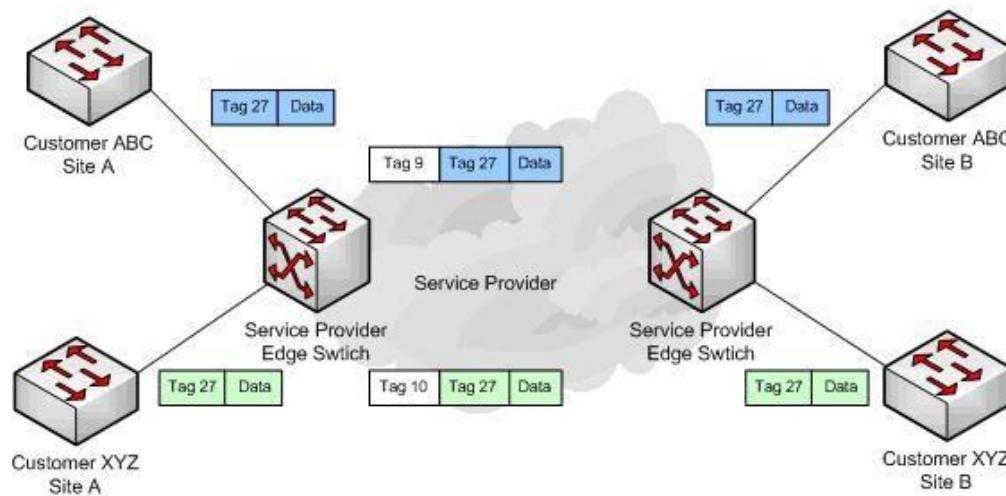
# Getting Started

The QinQ Support feature adds another layer of IEEE 802.1Q tag (called "metro tag" or "PE-VLAN") to the 802.1Q tagged packets that enter the network.



# Overview Use-Cases

It is helpful when there are multiple overlapping VLANs IDs between customers.



---

# Pre-Requisite with AWS VPN

Important Slide for Exam

---

# Overview of Pre-Requisites

Not all the customer gateway devices are supported to connect to VGW.

- Establish IKE Security Association using Pre-Shared Keys with protocol version 1 or 2.
- Establish IPsec Security Associations in Tunnel mode
- Utilize the AES 128-bit or 256-bit encryption function
- Utilize the SHA-1 or SHA-2 (256) hashing function
- Perform packet fragmentation prior to encryption
- Utilize Diffie-Hellman (DH) PPFS in "Group 2" mode, or one of the additional DH groups we support

# What if not ?

What happens if CGW does not meet the requirements ?

In cases where CGW does not meet the requirement, or if you need additional capabilities, then you can make use of EC2-based VPN termination endpoints.

---

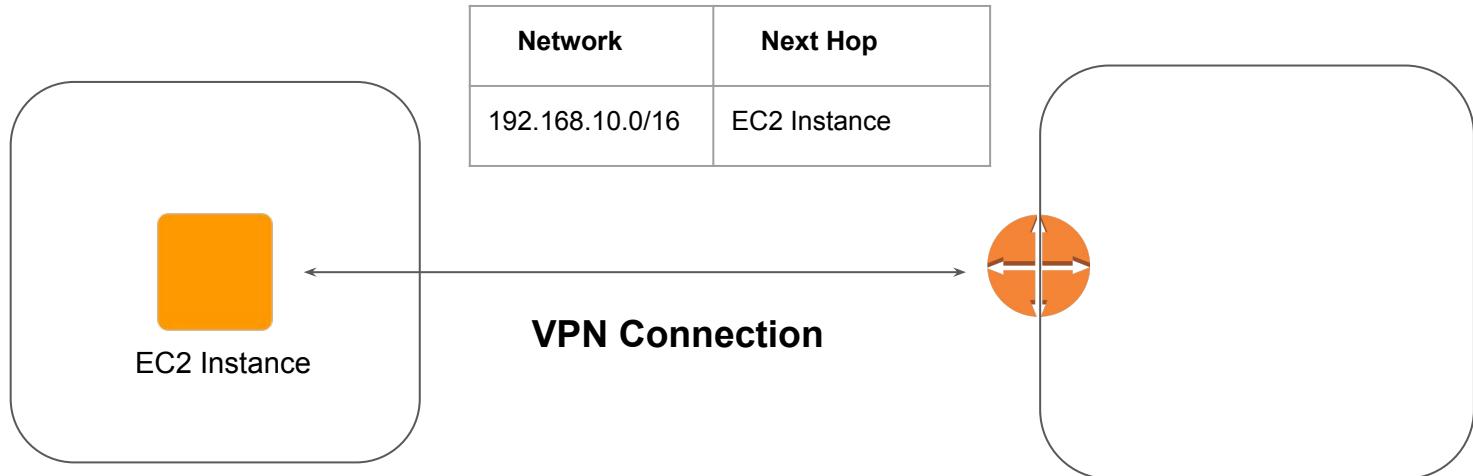
# High Availability for EC2 VPN

High Availability is a Key

---

# Getting Started

If we are using EC2 instance as a VPN termination endpoint, then the availability and redundancy is the responsibility of the customer.

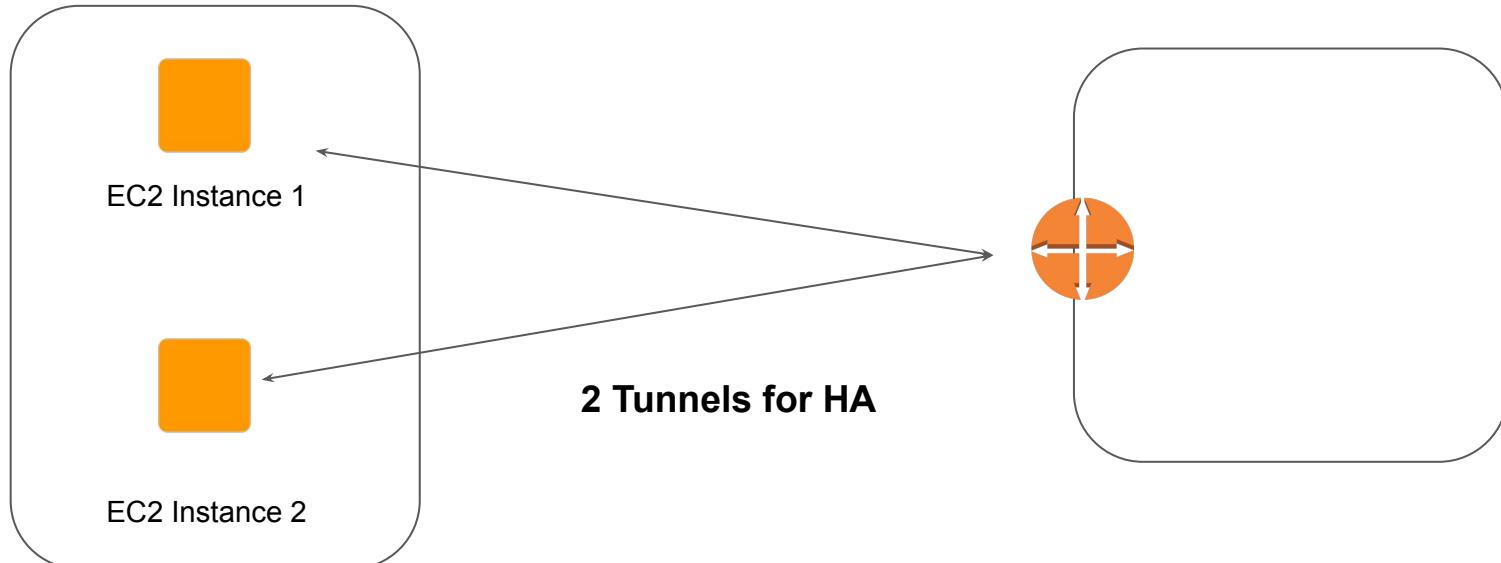


# Achieving High Availability

Network	Next Hop
192.168.10.0/16	EC2 Instance 1

→

Network	Next Hop
192.168.10.0/16	EC2 Instance 2



# Achieving High Availability

There needs to be a monitoring script which will do the failover when one VPN tunnel goes down.

This monitoring script will change the route table to point to standby VPN EC2 instance in-case primary one fails.

We can also make use of EC2 Auto-Recovery feature to restart EC2 instance in-case health-check fails.

---

# Troubleshooting VPN Instability Issues

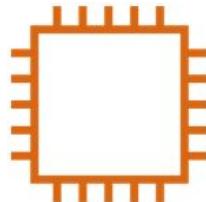
Let's Stabilize VPN

---

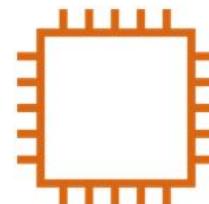
# Understanding Dead Peer Detection

When two peers communicate with IKE and IPSec, the situation may arise in which connectivity between the two goes down unexpectedly.

Dead Peer Detection (DPD) is a method of detecting a dead Internet Key Exchange (IKE) peer.



Hey Dude, are you alive?



Yes, Alive and Energetic

# DPD Configuration Options

Dead peer detection (DPD) timeout specifies the duration, in seconds, after which DPD timeout occurs. You can specify 30 or higher.

DPD timeout action specifies the action to take after dead peer detection (DPD) timeout occurs. You can specify the following:

DPD Timeout Action	Description
Clear	End the IKE session when DPD timeout occurs.
None	Take no action when DPD timeout occurs
Restart	Restart the IKE session when DPD timeout occurs

# Troubleshooting Step: DPD Settings

If a VPN peer doesn't respond to three successive DPDs, then the peer is considered dead and the tunnel is closed.

If your customer gateway device has DPD enabled, be sure that:

- It's configured to receive and respond to DPD messages.
- It isn't too busy to respond to DPD messages from AWS peers.
- It isn't rate limiting DPD messages due to IPS features enabled in the firewall.

## Troubleshooting Step 2: Idle Timeouts

Setting a default Idle Timeout for any IPSec VPN Connection enables administrator to define the maximum time for which the tunnel will stay connected even if no traffic passes through.

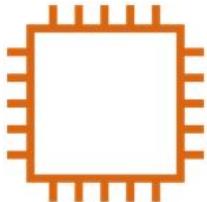
When there's no traffic through a VPN tunnel for the duration of your vendor-specific VPN idle time, the IPsec session terminates.

Be sure that there's constant bidirectional traffic between your local network and your VPC. If necessary, create a host that sends ICMP requests to an instance in your VPC every 5 seconds.

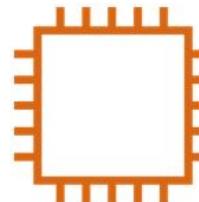
# Understanding Rekeying

Rekeying refers to the process of changing the session key—the encryption key of an ongoing communication—in order to limit the amount of data encrypted with the same key.

Make sure that inbound traffic to UDP ports 500 [IKE], 4500 [NAT-T], and IP 50 [ESP] on the customer gateway allow rekeys for the AWS endpoint.



Too much data encrypted with  
one key. Let's create new key.



---

# Placement Groups

Time to go fast

---

# Placement Groups

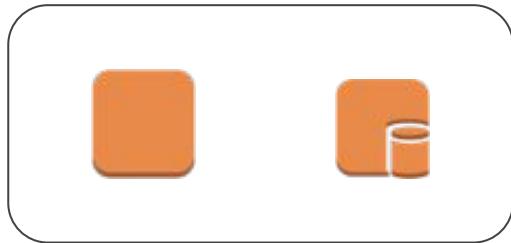
- Placement group are recommended for applications that require low latency, high network throughput.
- Placement groups can also be used to influence placement of a group of EC2 instances.



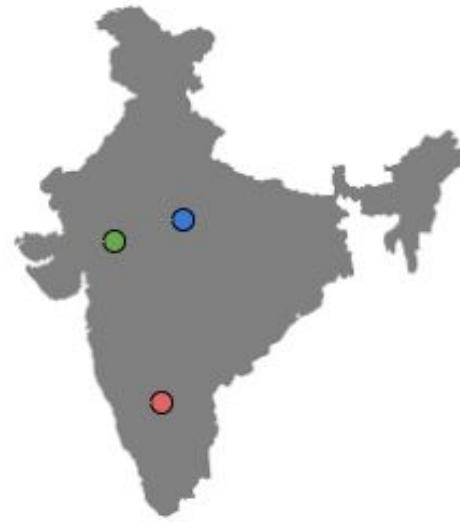
# Small Road vs Highway



# Let's understand GUI way



Placement Group

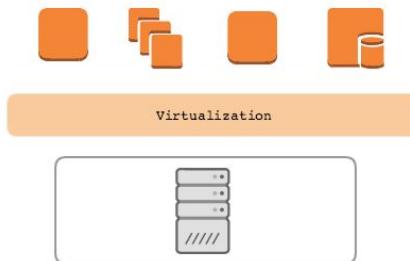


## Point 2 - Influencing Placement of EC2

- A single server can run multiple virtual machines.
- This can lead to issues if you are running a cluster of servers.

Example:

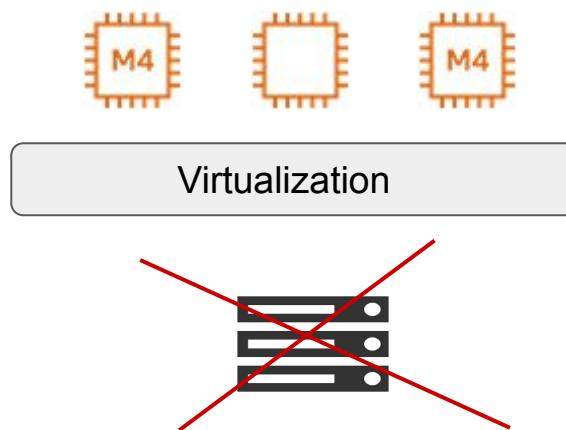
- Medium Corp is running a MySQL cluster consisting of two servers in single AZ. In the background, both the EC2 are part of the same underlying host.



# Example Use-Case

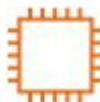
Medium Corp is running a MySQL cluster consisting of two servers in single AZ. The servers are of type m4.large.

In the background, both the EC2 are part of the same underlying host.

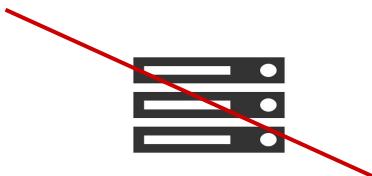


# Solution - Placement Group

With placement group, we can explicitly specify that two EC2 instance should not be part of the same server (same rack of servers)



Virtualization



Virtualization



# Racks in Data Center



# Types of Placement Groups

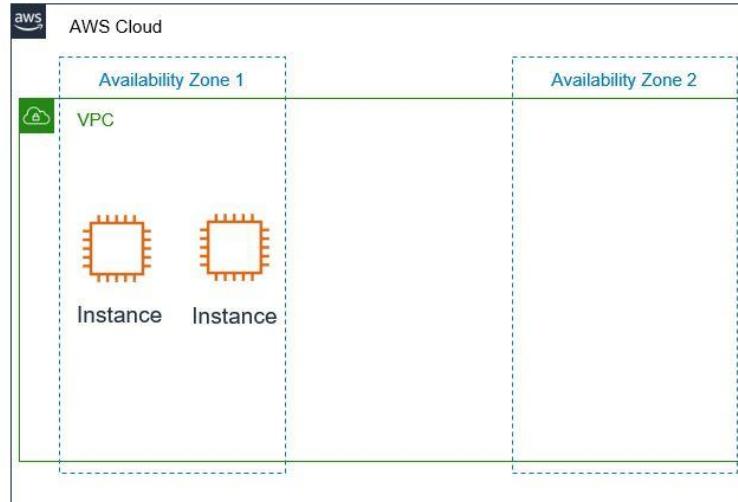
There are three types of placement groups available:

Sr No	Type	Description
1	Cluster	Packs instances close to each other in an Availability Zone.
2	Partition	Spreads instances in logical partition such that group of instances in one partition do not share underlying hardware.
3	Spread	Strictly places group of instances across distinct hardware to reduce failures.

# Cluster Placement Groups

Logical grouping of instances within a single Availability Zone.

Intended for applications that require low network latency and high network throughput.

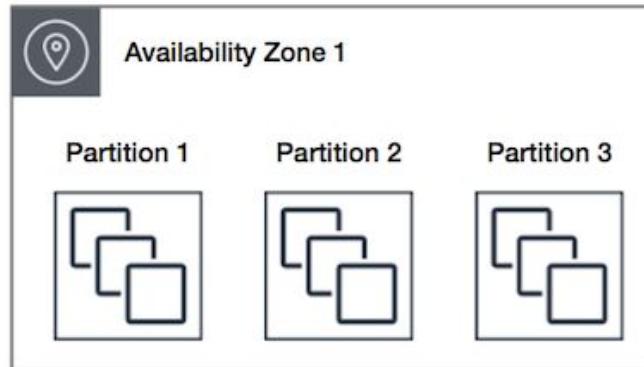


# Partition Placement Groups

AWS ensures that each partition within a placement group has its own set of racks.

In the below diagram, there are 3 partitions and each partition has multiple EC2 instances.

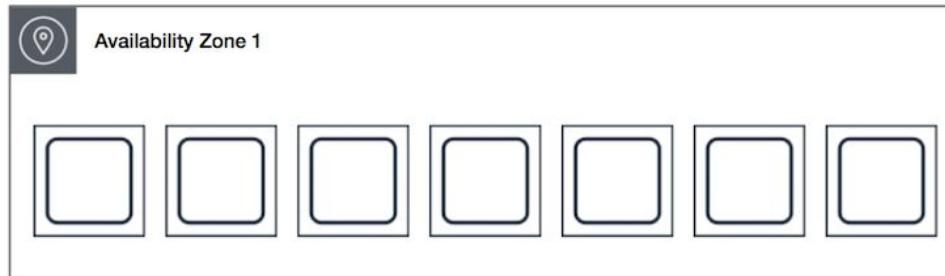
Each of these partitions resides in a different rack inside the Data center.



# Spread Placement Group

A spread placement group is a group of instances that are each placed on distinct racks, with each rack having its own network and power source.

In the following diagram, there are 7 EC2 instances and each instance is in a separate rack.



# Important Points - Cluster Placement Groups

- A cluster placement group can't span multiple Availability Zones.
- Only specific types of EC2 instances can be launched.
- Maximum network throughput traffic between two instance in placement group is limited by the slower of the two instance.
- Recommended to launch all instance together. Launching instance later can lead to capacity errors. In such-case, stop and start all instances in the placement group.

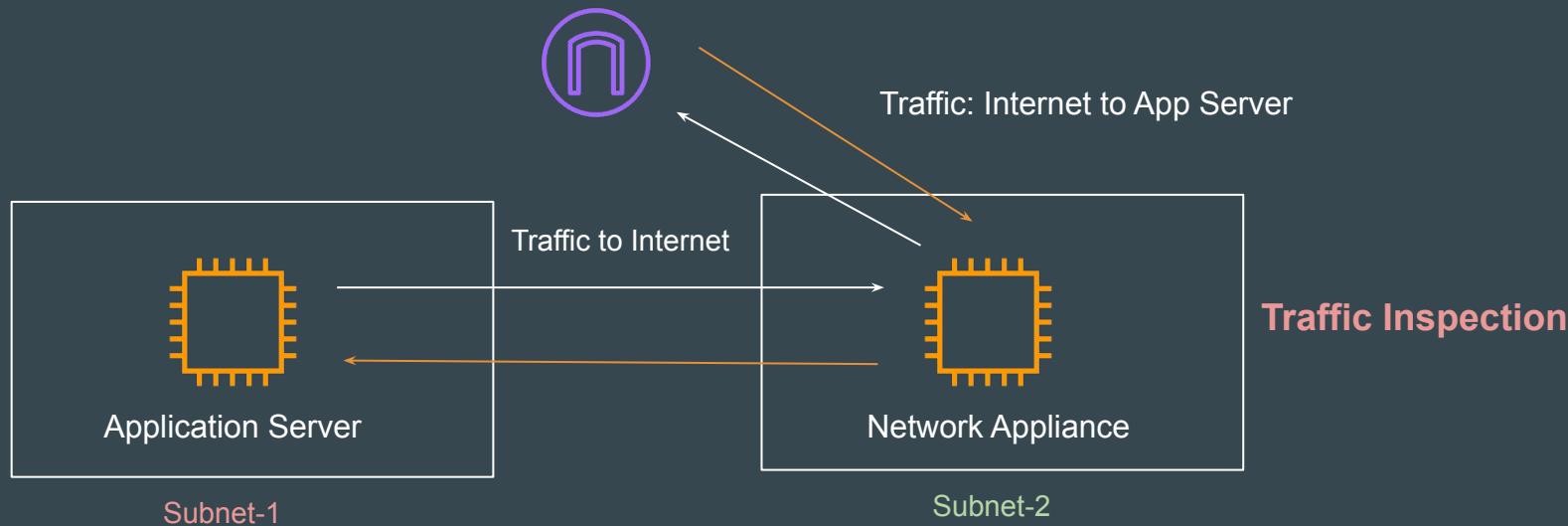
# Gateway Load Balancer



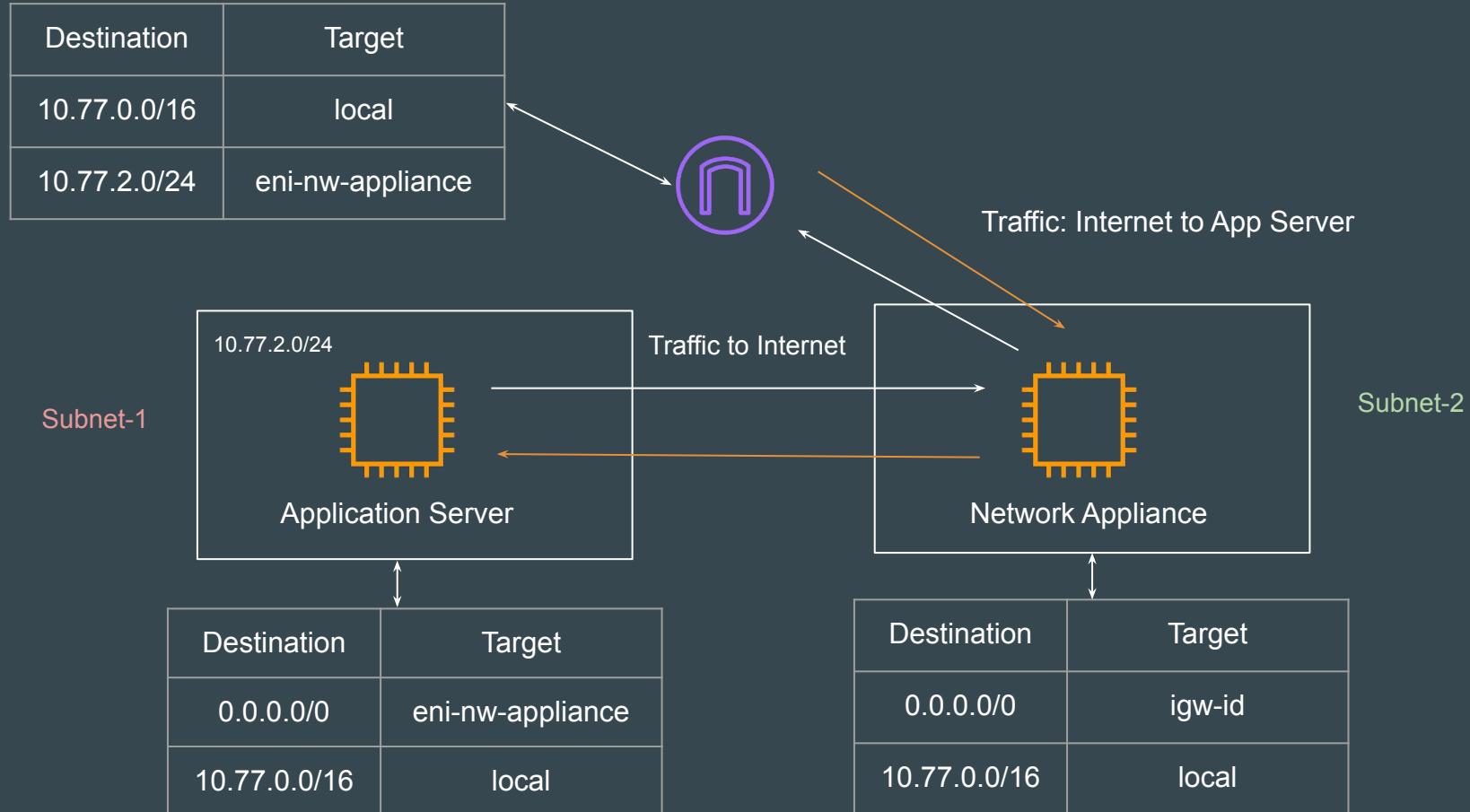
# Problem Statement

Traffic Inspection is one of the common use-cases in Enterprises.

Many providers offers virtual appliance related to IDS/IPS, Firewalls etc.



# The Architecture



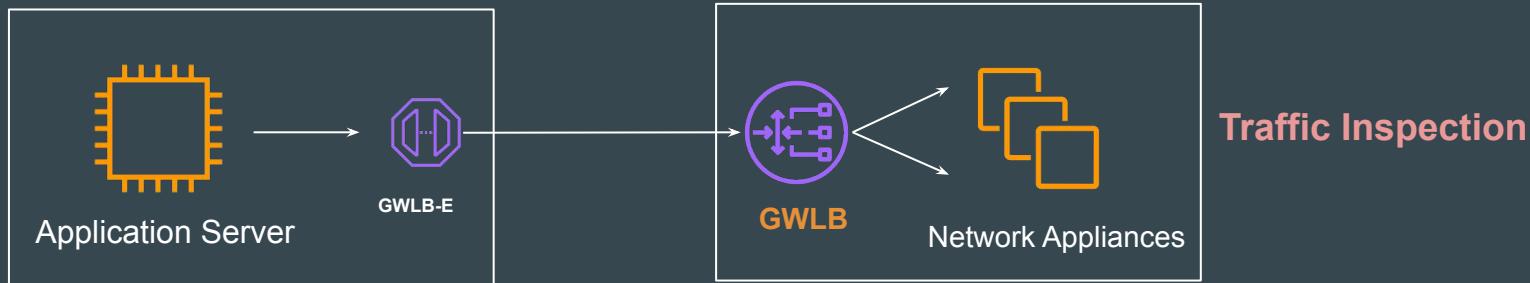
# Challenges with the Architecture

The routing is done at a ENI level of the Network Appliance.

**Issues:** High-Availability, Scaling

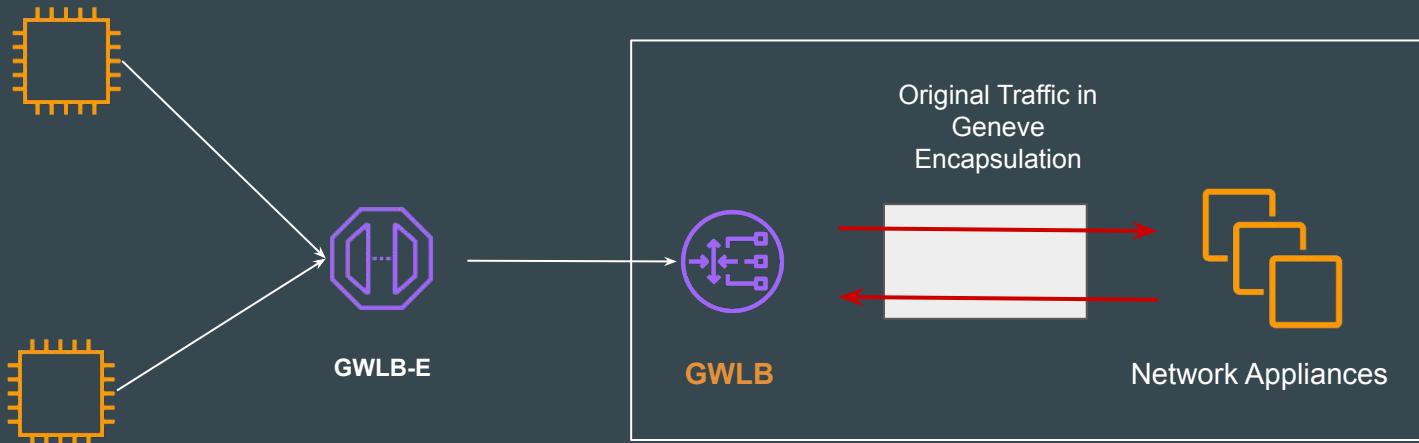
# Introducing GWLB

Gateway Load Balancers **enable you to deploy, scale, and manage** virtual appliances, such as firewalls, IDS/IPS , and deep packet inspection systems



# Points to Keep In Mind

In order to work with GWLB, appliances need to support **Geneve protocol** to exchange traffic with GWLB.



# **Packet Flow - GWLB and Appliance**



Packets Sent By Source

Src IP=A.B.C.D	Dst IP=E.F.G.H
Payload	

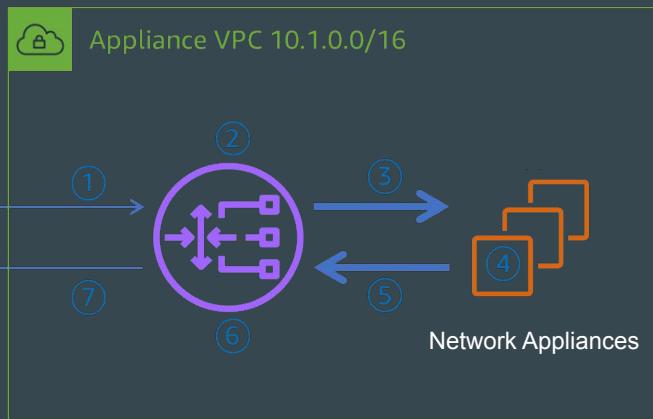


Packets Sent To Destination

Src IP=A.B.C.D	Dst IP=E.F.G.H
Payload	

## Step 2:

GWLB selects Appliance using 5-tuple  
Encaps packets in Geneve  
Forwards it to Appliance.



## Step 3: Packet Sent to Appliance

Outer Src IP = 10.1.4.10	Outer Dst IP = 10.1.2.5
GWLBE ENI ID	Attachment ID
Src IP=A.B.C.D	Dst IP=E.F.G.H
Payload	

## Step 4:

Appliance decaps the packet.  
Performs Inspection  
Sends the packet back to GWLB

Outer Src IP = 10.1.2.5	Outer Dst IP = 10.1.4.10
GWLBE ENI ID	Attachment ID
Src IP=A.B.C.D	Dst IP=E.F.G.H
Payload	

## Step 6:

GWLB decaps the packet

## Step 5: Packet Sent by Appliance

# The Workflow - Part 1

1. When GWLBE receives the packet from the source, it sends the packet to GWLB using the underlying PrivateLink technology. The packet stays on AWS network and reaches GWLB.
2. GWLB uses 5-tuple (Src IP, Dest IP, Src Port, Dest Port, Protocol) of the incoming packet and chooses a specific appliance as a target
3. GWLB then encapsulates original packet (shown in yellow color) using Geneve header and embeds the metadata in form of Type, Length, Value triplets, also known as TLVs

## The Workflow - Part 2

4. GWLB forwards encapsulated packet to the specific appliance. GWLB will stick that 5-tuple flow to that specific appliance in both directions of traffic for the life of that flow.
5. Appliance decaps the packets, performs inspection and send it back to GWLB
6. GWLB decaps the packets and sends it to appropriate GWLBE.

# Points to Note - Gateway Load Balancer



## Pointer - 1

A Gateway Load Balancer operates at the **third layer** of the Open Systems Interconnection (OSI) model, the network layer.

It listens for all IP packets across all ports and forwards traffic to the target group that's specified in the listener rule.

You cannot specify a protocol or port when you create a listener for a Gateway Load Balancer.

## Pointer - 2

The Gateway Load Balancer and its registered virtual appliance instances exchange application traffic using the **GENEVE protocol** on port 6081.

It maintains stickiness of flows to a specific target appliance using 5-tuple (for TCP/UDP flows) or 3-tuple (for non-TCP/UDP flows).

## Pointer - 3

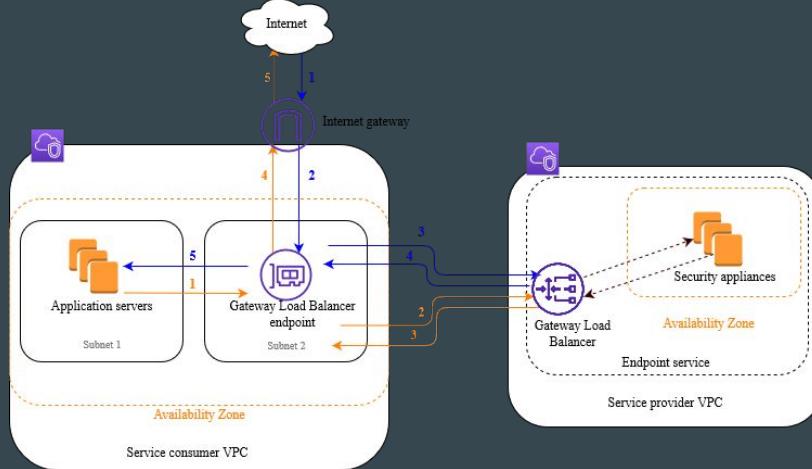
Gateway Load Balancers use Gateway Load Balancer endpoints to securely exchange traffic across VPC boundaries

A Gateway Load Balancer endpoint is a VPC endpoint that provides private connectivity between virtual appliances in the service provider VPC and application servers in the service consumer VPC.

## Pointer - 4

Traffic to and from a Gateway Load Balancer endpoint is configured using route tables.

You must create the Gateway Load Balancer endpoint and the application servers in different subnets



# Pointer - 5

Customer is responsible for choosing and qualifying software from appliance vendors

The appliance vendors listed as **Elastic Load Balancing Partners** have integrated and qualified their appliance software with AWS.

The screenshot shows the AWS Marketplace interface. At the top left, there's a navigation bar with 'SOLUTIONS' and a search bar containing 'Security Appliances'. Below the search bar, there are category links: 'Security Appliances', 'Network Analytics', 'Orchestration', and 'Systems Integration'. On the right side of the search bar, the 'CHASER' logo is displayed. The main content area features two partner profiles:

**Chaser Systems**

"The Gateway Load Balancer has allowed security-conscious customers to leverage Chaser's DiscrimiNAT Firewall, which protects against a range of Exfiltration and Command & Control TTPs, with auto scaling and high availability spec SREs would approve. Collaborating with AWS on this integration, we retained the developer experience, low latency and data in transit's processing private to the customer's VPC, as had come to be expected of our FQDN-filtering NAT solution."

- Dhruv Ahuja, Chief Engineer at Chaser Systems

[Partner Profile](#) | [Contact](#) | [AWS Marketplace](#)

**Check Point Software**

"AWS continues to deliver advanced cloud services to respond to customer needs and help organizations build secure cloud deployments. Gateway Load Balancer will simplify the design of cloud architectures and allow customers to use CloudGuard's advanced threat prevention technologies in an easier and more intuitive way."

- Itai Greenberg, VP Product Management at Check Point Software

[Partner Profile](#) | [Contact](#) | [AWS Marketplace](#)

## Miscellaneous

There is no security group that you can attach at GWLB level.

Supports Dual stack mode (IPv4 and IPv6)

Supports Health Check Protocol of HTTP, HTTPS, and TCP

---

# Content Delivery Network

CDN is Awesome

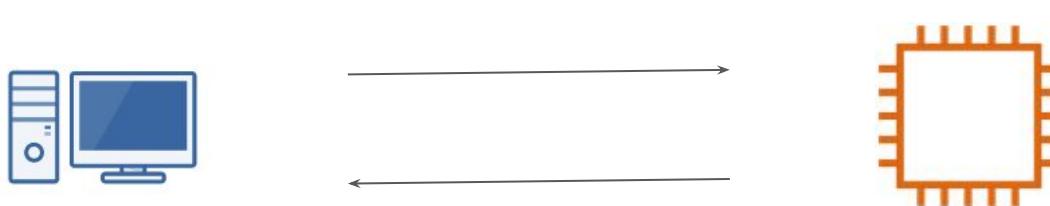
---

# Generic Scenario

Let's consider a typical scenario where everything is hosted in a single server.

On a smaller scale this seems to be an ideal approach.

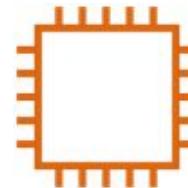
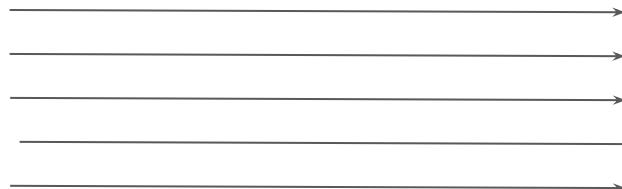
But when the traffic and popularity grows, there are a lot of challenges.



# Challenge 1 - Performance

With an increase in number of visitors, the performance can go down.

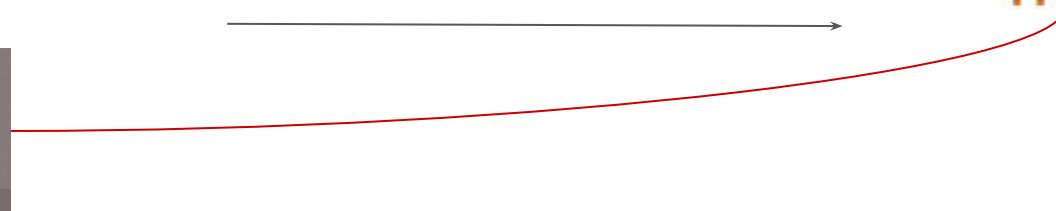
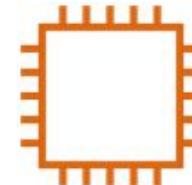
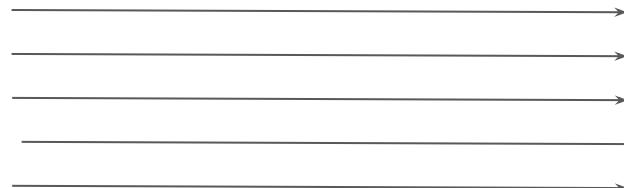
If website has 1 image and 1000 users are visiting it, then the same single image will need to be sent to 1000 users.



## Challenge 2 - Security

Attackers love the Internet.

A typical website and web-application face various type of attacks ranging from DOS, Web-Application attacks and so on.



# Typical Solution

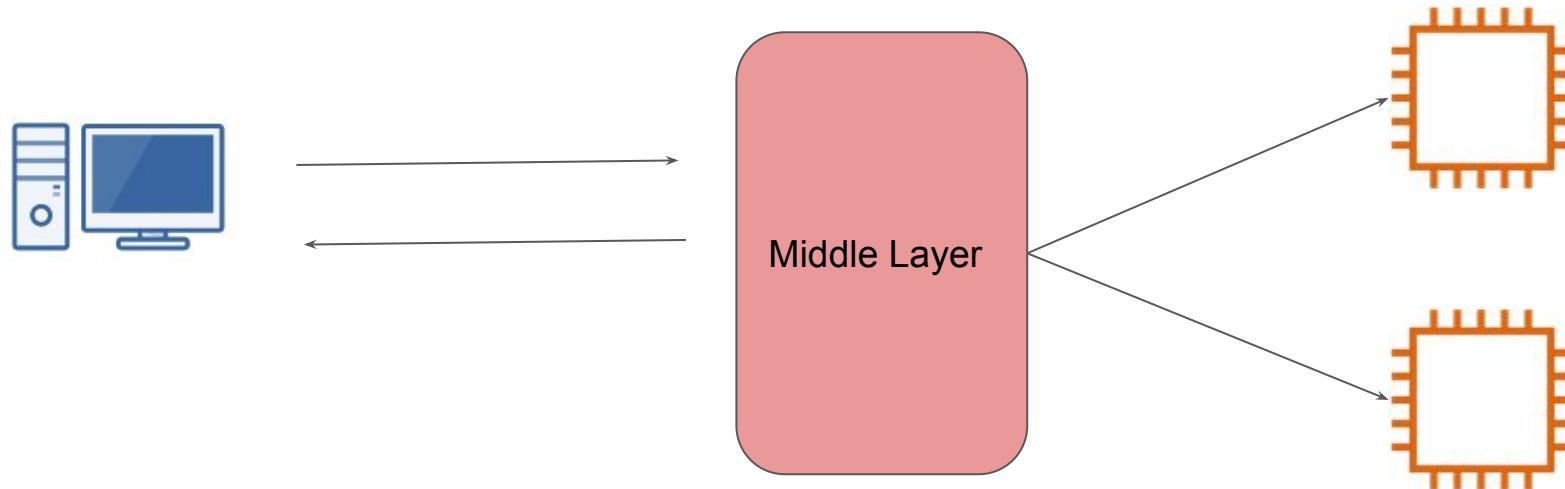
Some of the approaches to the challenges that we discussed:

1. Increase the size of server / increase number of servers for better performance.
2. Configure DDoS protection, Web-Application Firewall etc at the server level.

Doing these things on each server is a tedious task and it cannot scale very well.

# Better Architecture

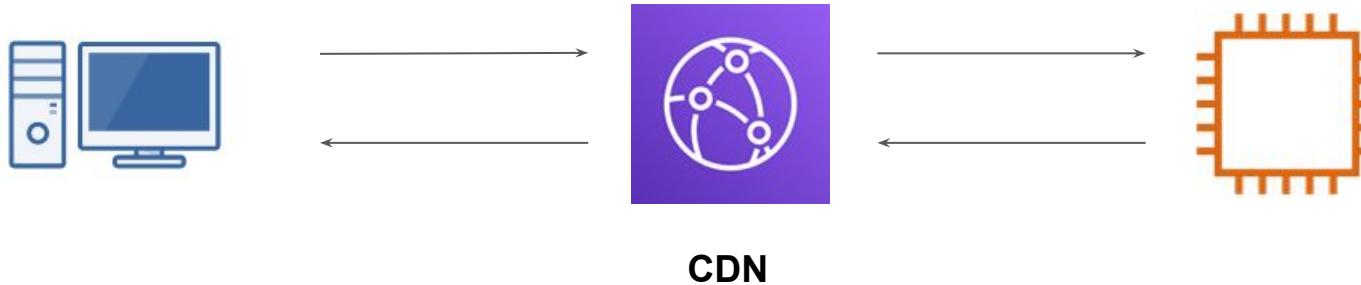
Better architecture would be to introduce a middle layer that has all functionalities related to protecting against attacks, caching of commonly requested objects for better performance.



# Content Delivery Network

A CDN acts as a proxy that receives the request and then forwards it to the backend systems.

Various CDN's also comes with features like DDoS Protection, WAF, Cachig and others.



---

# Deploying CloudFront Distribution

CDN is Awesome

---

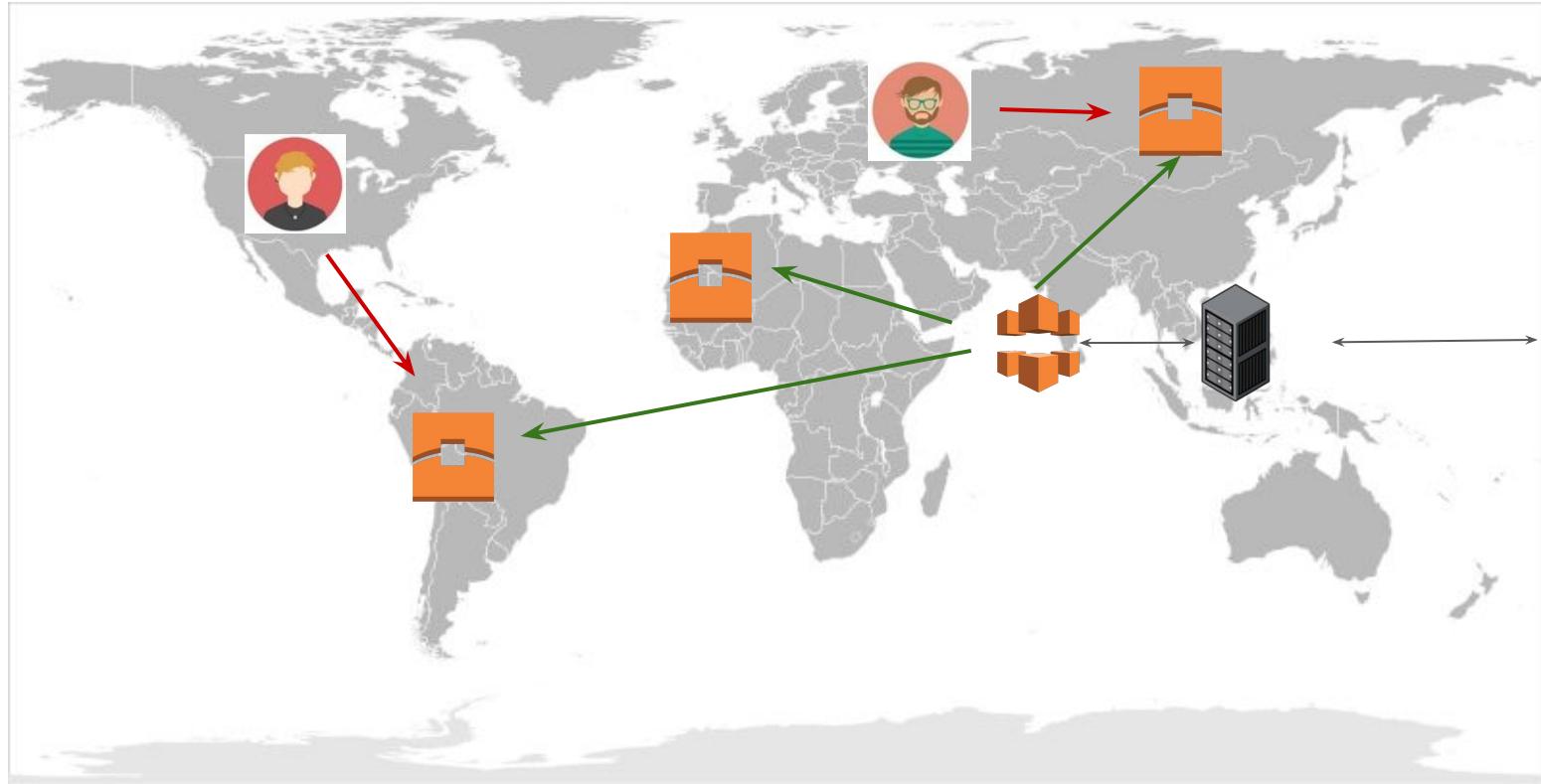
# Deploying CloudFront

## Steps Involved :-

1. Create a sample HTML Website
2. Create CloudFront Distribution
3. Connect CloudFront with Website Endpoint.



# Understanding CDN



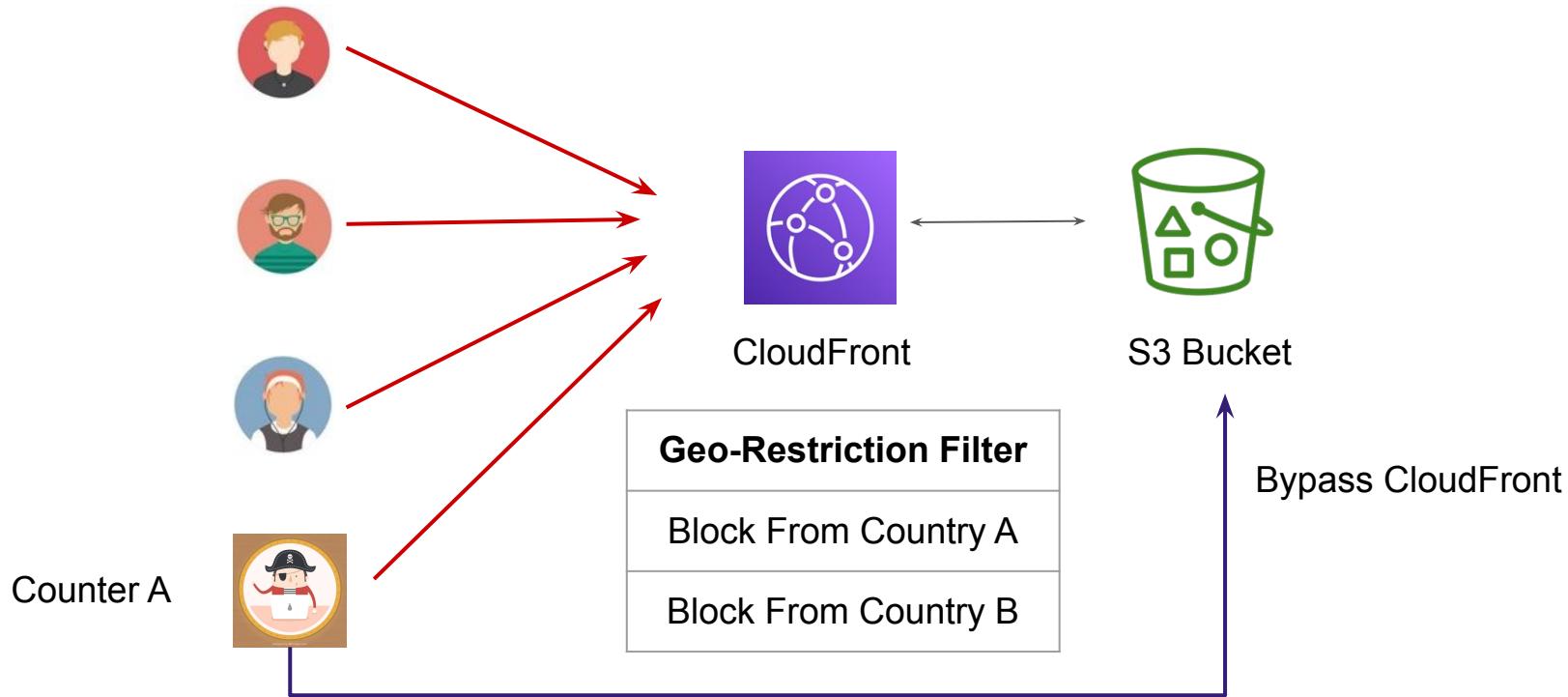
---

# Origin Access Identity

## CDN Security

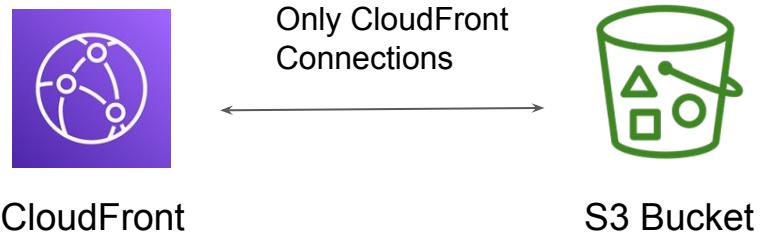
---

# Understanding the Challenge



# CloudFront Origin Access Identity

CloudFront Origin Access Identity ensures that only users coming through CloudFront distribution are able to access the contents of your S3 Buckets.



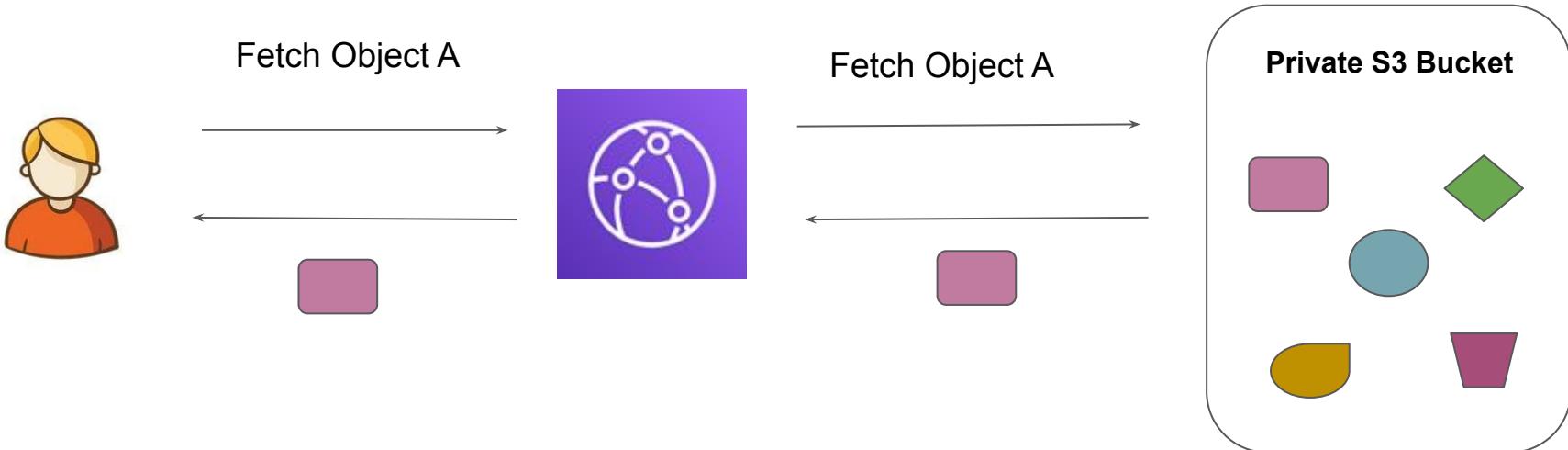
---

# CloudFront Signed URLs

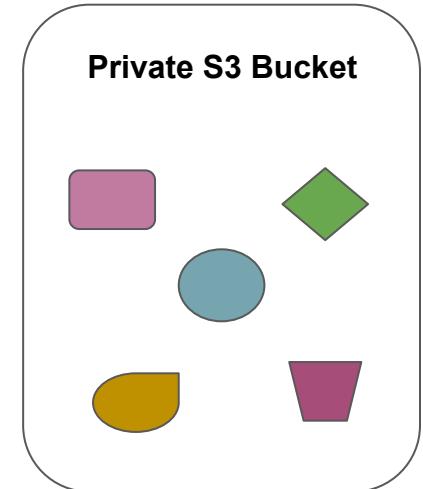
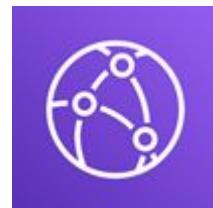
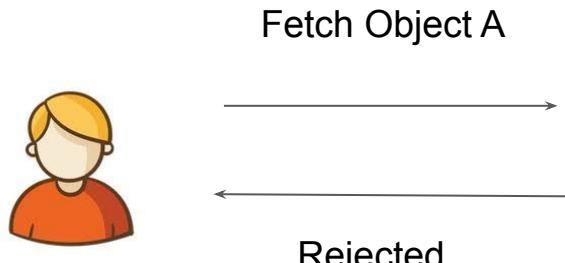
CDN is Awesome

---

# Generic Approach

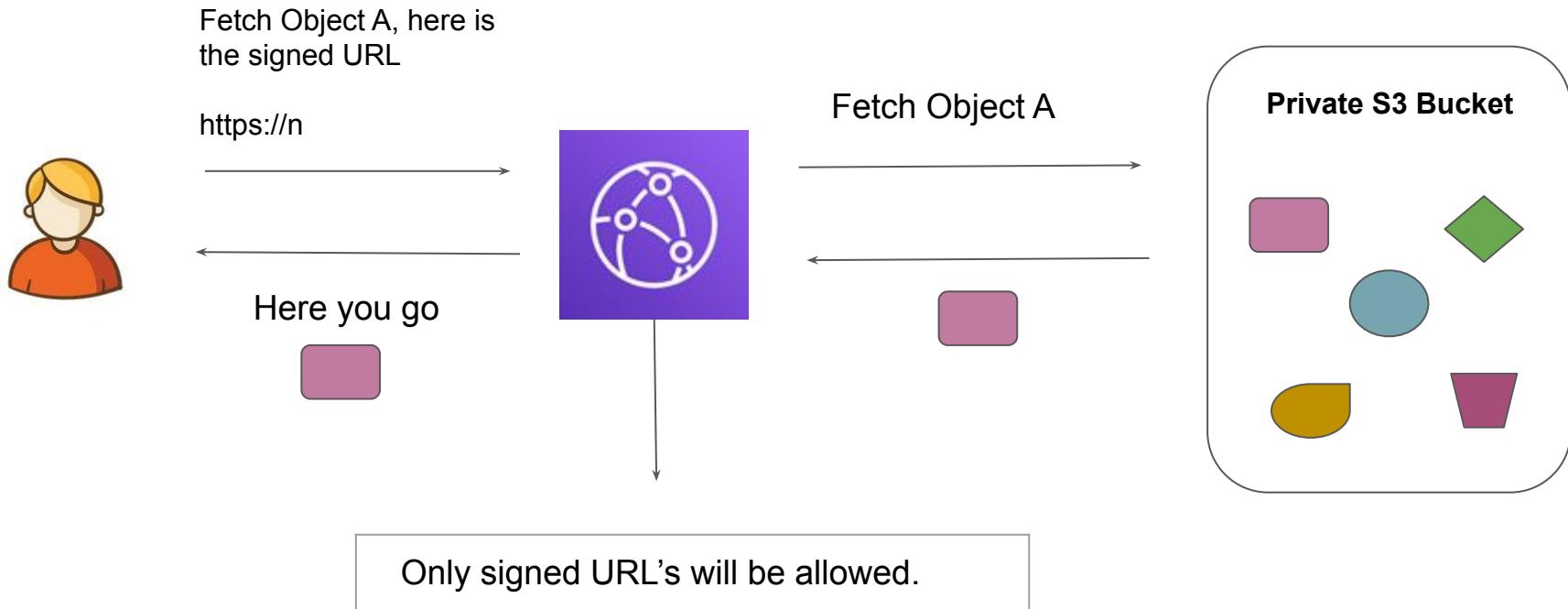


# Allow only special URLs



Only special URL's will be allowed.

# Architecture Overview of Signed URLs



# CloudFront Signed URLs

CloudFront Signed URLs mandates users to provide signed URLs or signed cookies to access the private content.

CloudFront signed URLs can be generated by the trusted signers assigned in your AWS account.

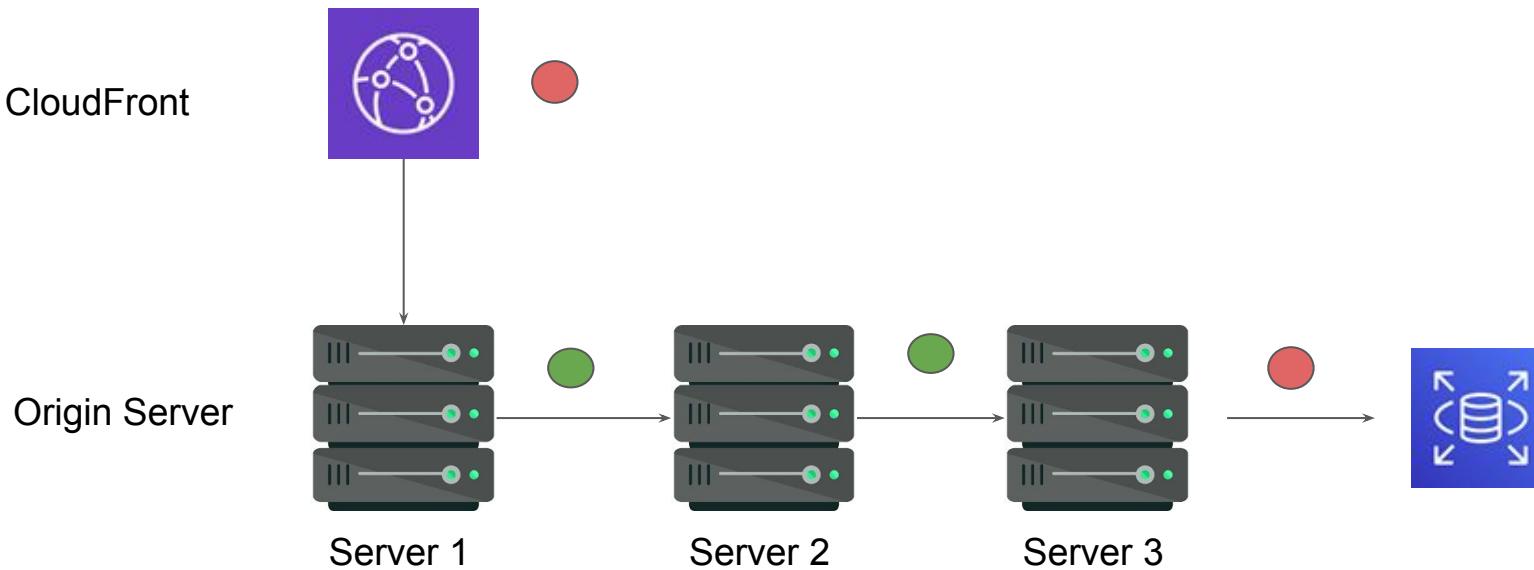
---

# Field Level Encryption - CloudFront

Cryptography Yet Again!

# Understanding The Challenge

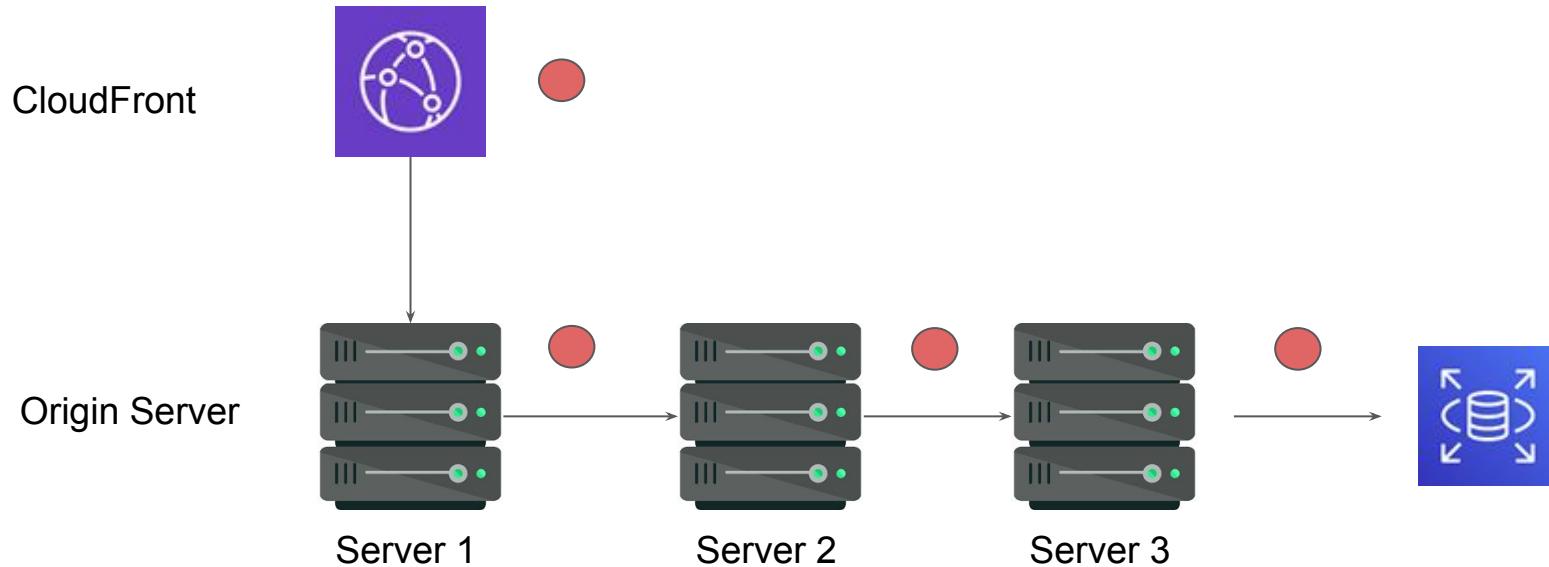
Sensitive Data when travelling via multi-tier architectures leads to security challenges.



# Possible Solution

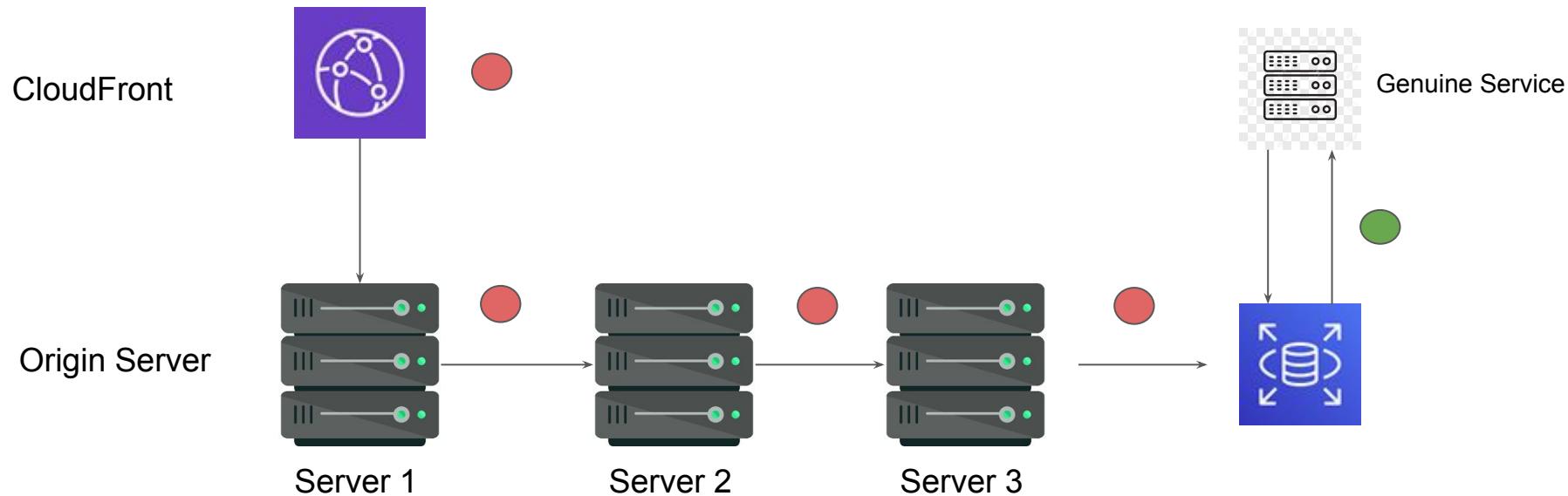
Encrypting Data end-to-end so that no intermediary service have access to it.

Only specific service which has genuine business need should be able to fetch and decrypt data.



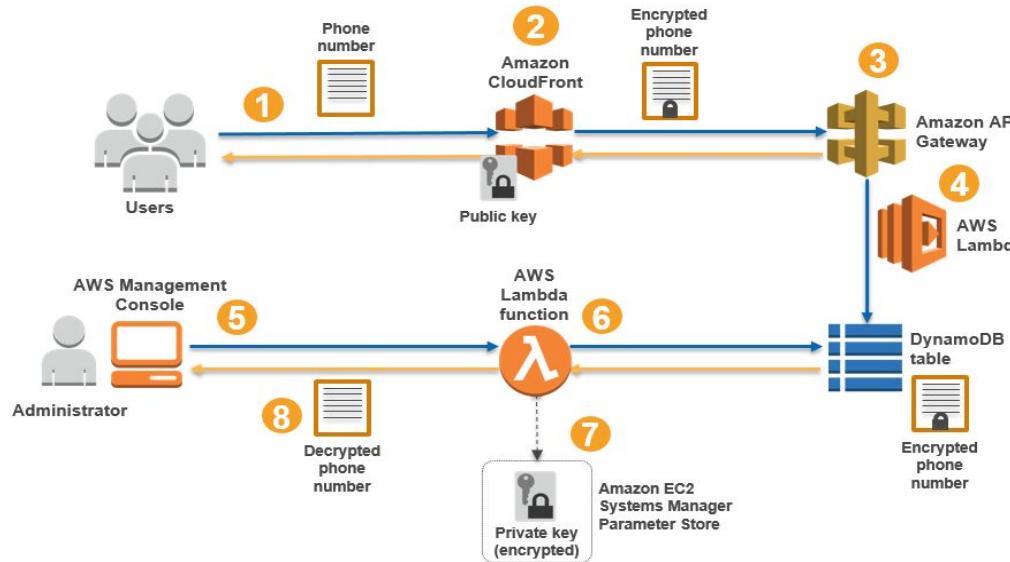
# Plain Text Data to Only Genuine Service

Only specific service which has genuine business need should be able to fetch and decrypt data.



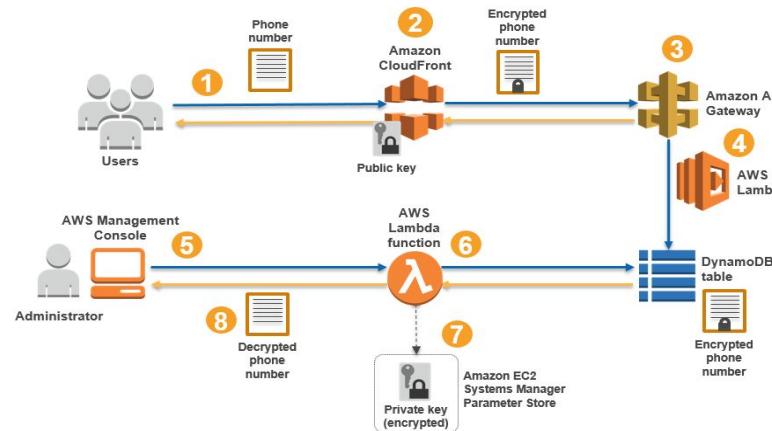
# Field Level Encryption

CloudFront field-level encryption encrypts the sensitive PII data before the request is forwarded to the origin.



# High Level Steps

1. Application sends POST request with PII data.
2. FLE intercepts POST request, encrypts the data with public key and forwards to origin.
3. Origin takes the data and processes it normally and stores to DynamoDB table.
4. Lambda Function stores the data in DynamoDB.
5. Admin uses Lambda function to retrieve encrypted data from DynamoDB.
6. Admin uses key-material stored in parameter store to decrypt sensitive data.
7. Decrypted Data is returned to the Administrator.



---

# Unified CloudWatch Agent

## Metrics and Logs

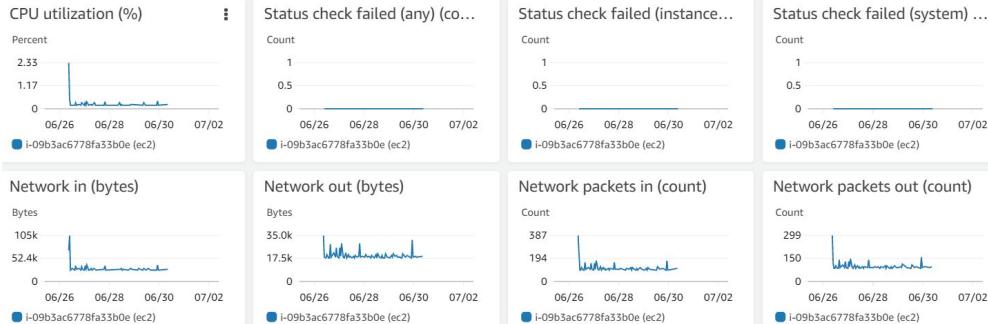
---

# Default CloudWatch Metrics

When we launch an EC2 instance in AWS, there are certain metrics that are captured by default.

Some of these include:

- CPU Utilization
- Network Related
- Disk Related

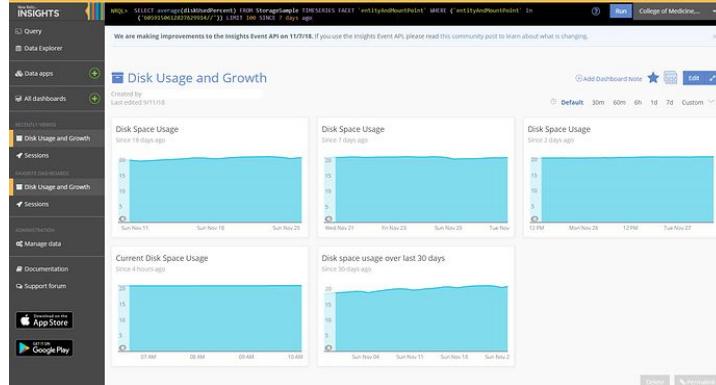


# Challenge 1 -More Metrics Are Needed

There are various important metrics that needs to be collected in addition to the default ones.

Some of these include:

- Memory Metrics
- Disk Usage Metrics
- Netstat related.

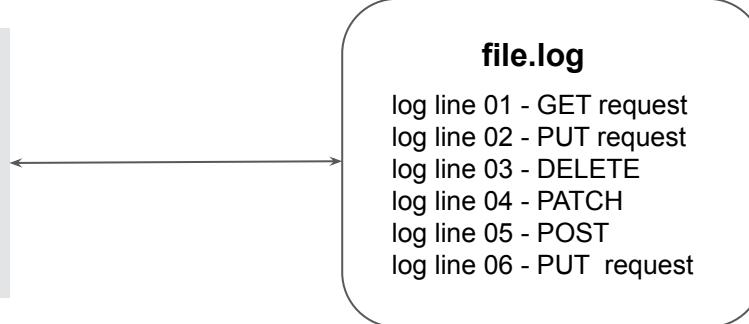


# Challenge 2 - Log Monitoring

A server can contain a lot of log files, from system logs to the application logs.

During debugging, it is important to have log files at hand.

This means in default case; you need to give access to the server to an individual who wants to debug.

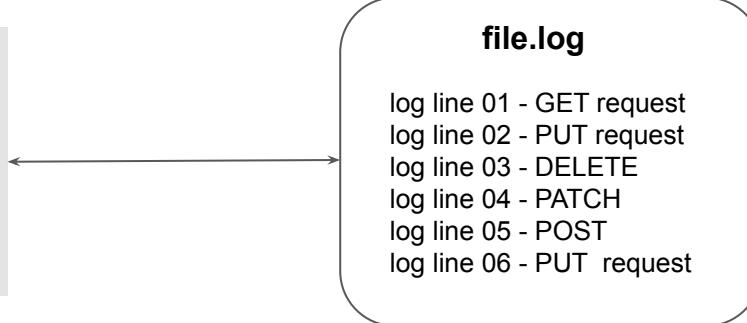
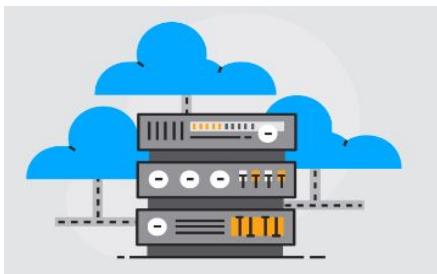


# Disadvantage of the Approach

Access must be given to the server to the developers.

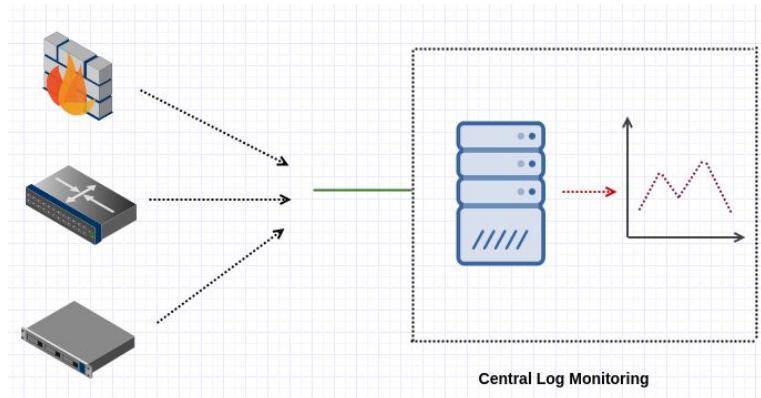
If the server gets terminated, the logs are lost.

No way to set up an alarm on certain conditions or create complex filters.



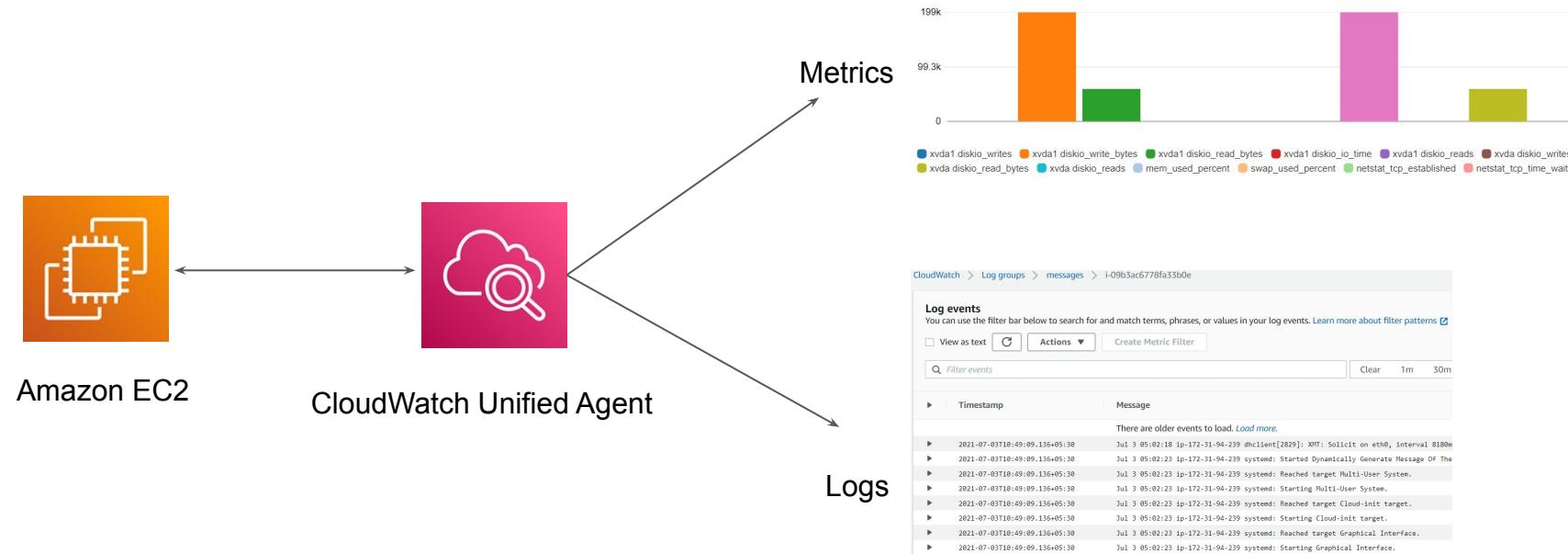
# Better Way

- We create a Central Log Server.
- We push the log files from individual systems to Central Log Server.



# Introducing Unified CloudWatch Agent

Unified CloudWatch Agent allows customers to capture both the internal system level metrics as well as logs collection.



# How-To Steps

1. Create a IAM Role with CloudWatchAgentServer policy.
2. Create EC2 using IAM Role.
3. Install CloudWatch Agent.
4. Run CloudWatch Agent Configuration Wizard
5. Start Unified CloudWatch Agent.

# Relax and Have a Meme Before Proceeding

When you're the only one who  
can pass the helicopter mission  
in GTA Vice City and your friend  
call you to pass it for him



---

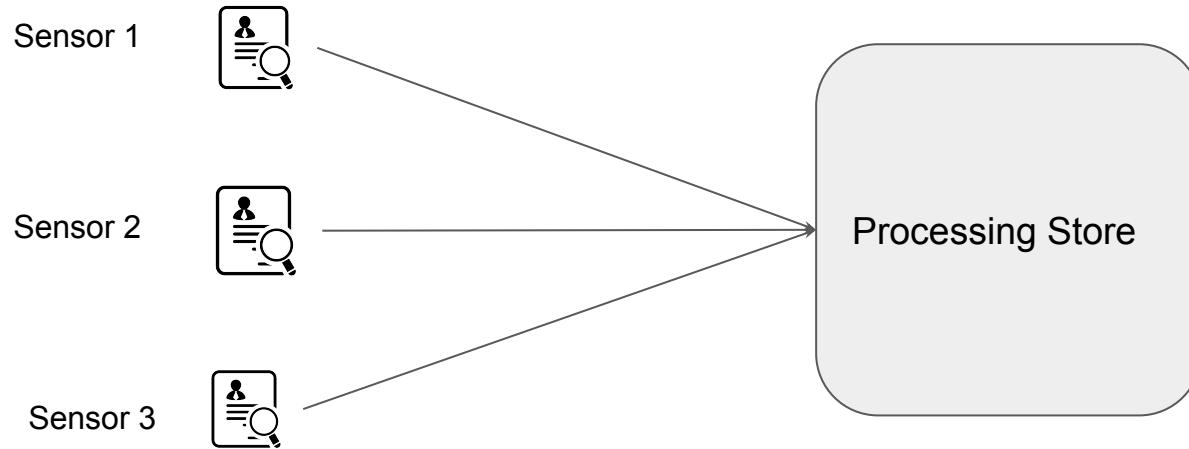
# Amazon Kinesis

## Streaming Data

---

# Basics of Streaming Data.

Streaming data is the continuous flow of data generated by various sources



# Examples of Streaming Data

A financial institution tracks changes in the stock market in real time and adjust it's portfolio accordingly.

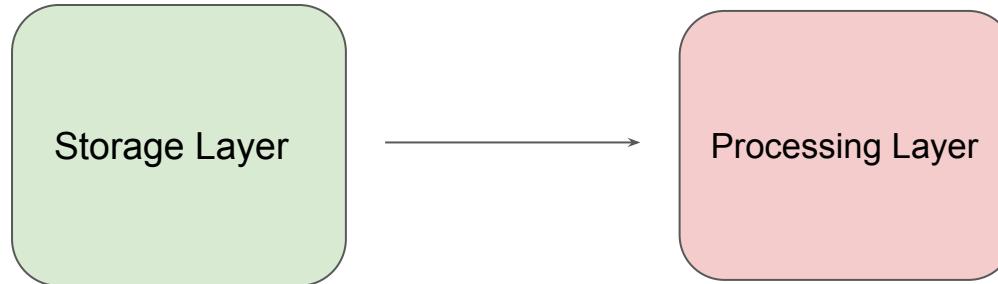
A media publisher streams billions of clickstream records from its online properties



# Challenges with Working of Streaming Data

Streaming data processing requires two layers: a storage layer and a processing layer.

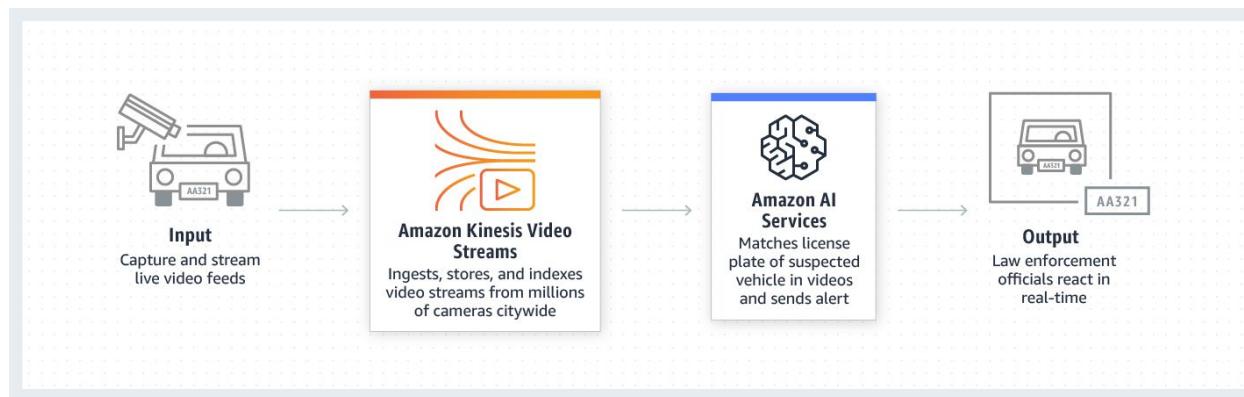
The storage layer needs to support record ordering and strong consistency, replayable reads and the processing layer is responsible for consuming data from the storage layer, running computation on that data and many other tasks.



# Basics of Amazon Kinesis

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information.

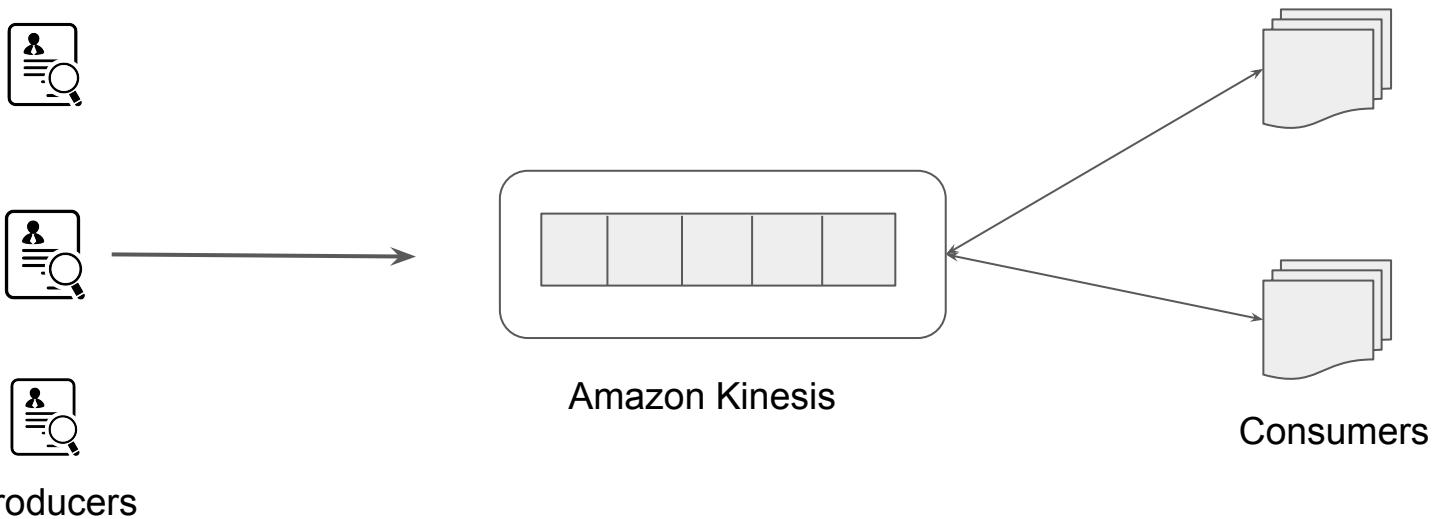
Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale



# 3 entities

There are 3 entities in this kind of use case:

Producer, Stream Store, Consumer



---

# Amazon Kinesis Services

Capabilities of Kinesis Set of Services

---

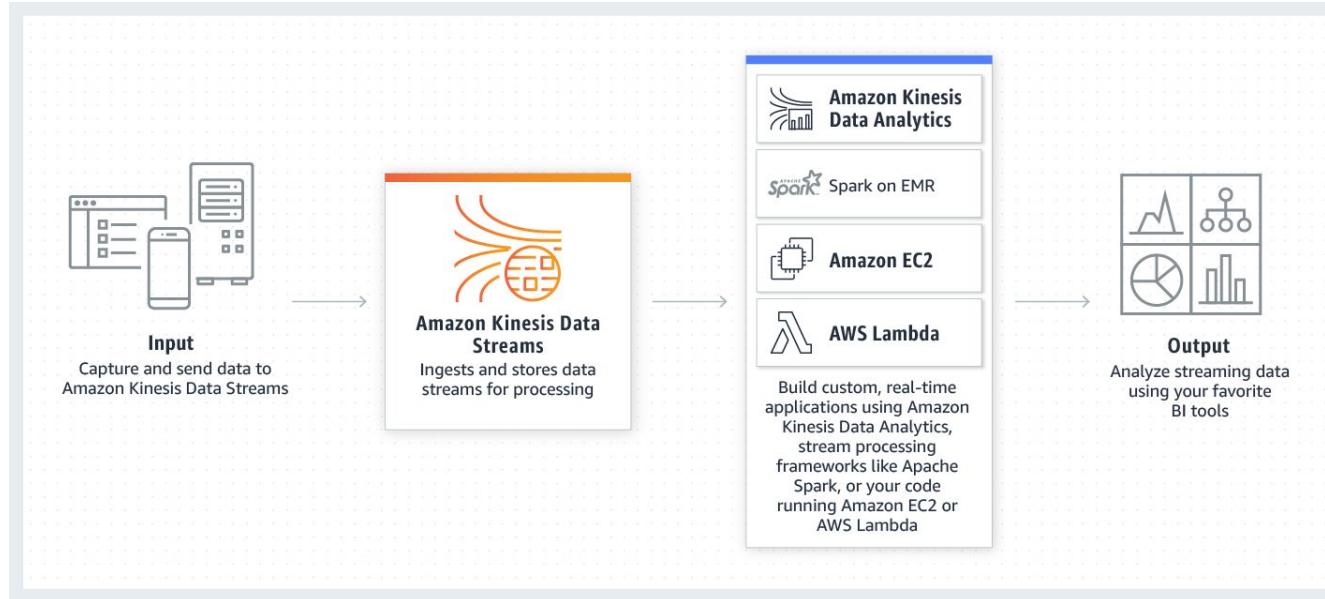
# Kinesis Offerings

Amazon Kinesis is a set of services which makes it easy to work with set of streaming data on AWS.

Sr No	Kinesis Services	Description
1	Kinesis Data Stream	Captures, processes and stores data streams in real-time
2	Kinesis Data Firehose	Primary to move data from point A to point B.
3	Kinesis Data Analytics	Analyze streaming data in real-time with SQL / Java code.
4	Kinesis Video Stream	Capture, processes and stores video streams.

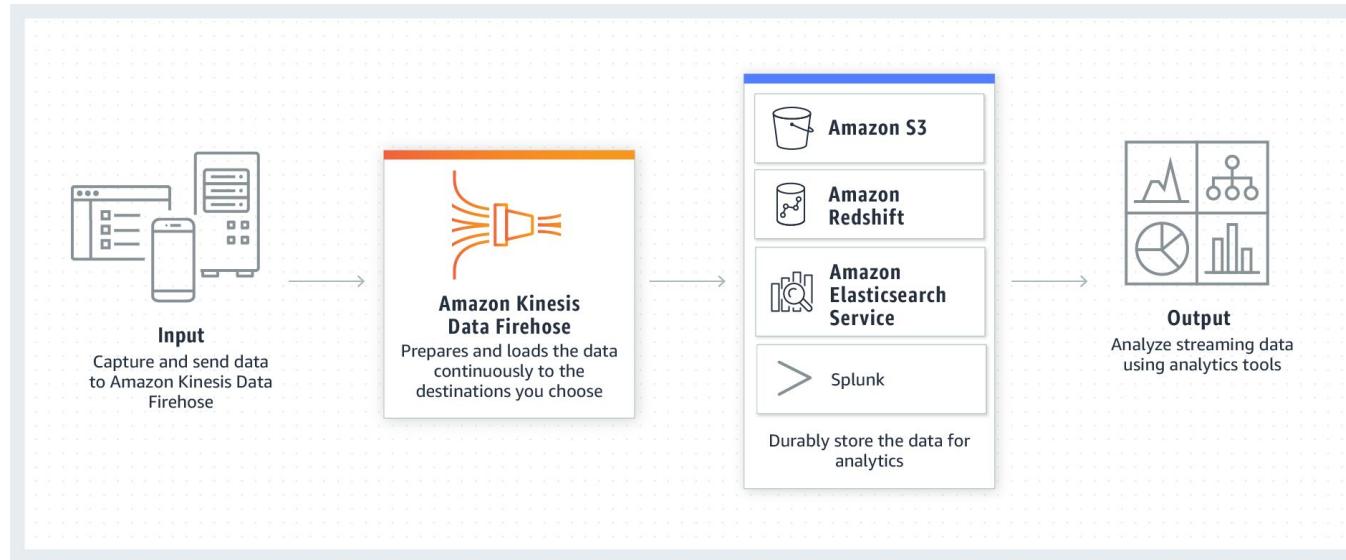
# Kinesis Data Stream

It allows us to capture, process and store data streams.



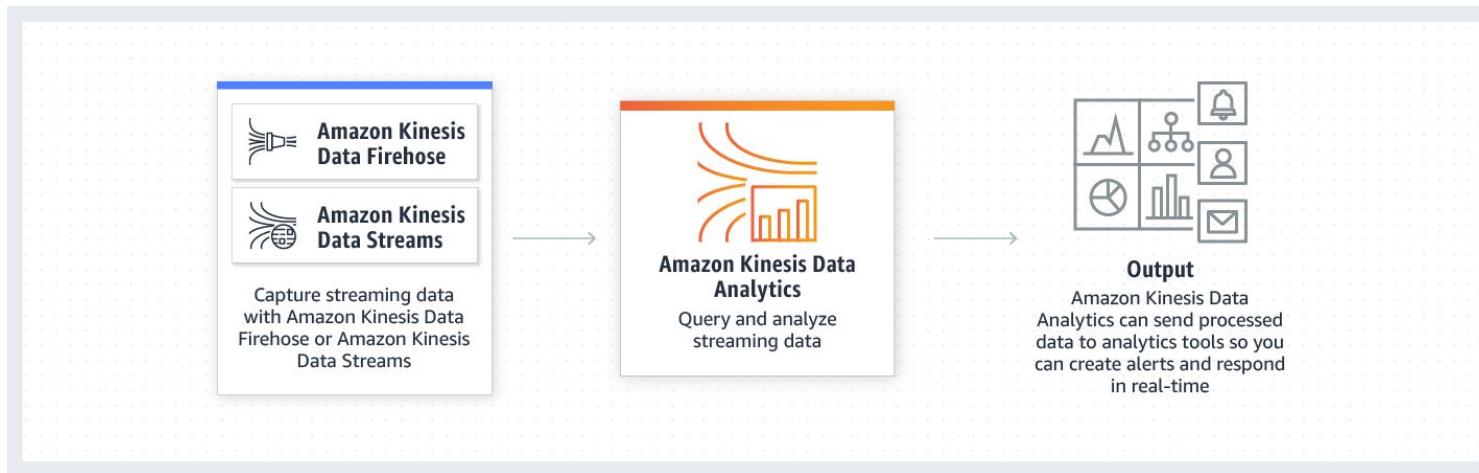
# Kinesis Firehose

Kinesis firehose delivers data from point A to point B.



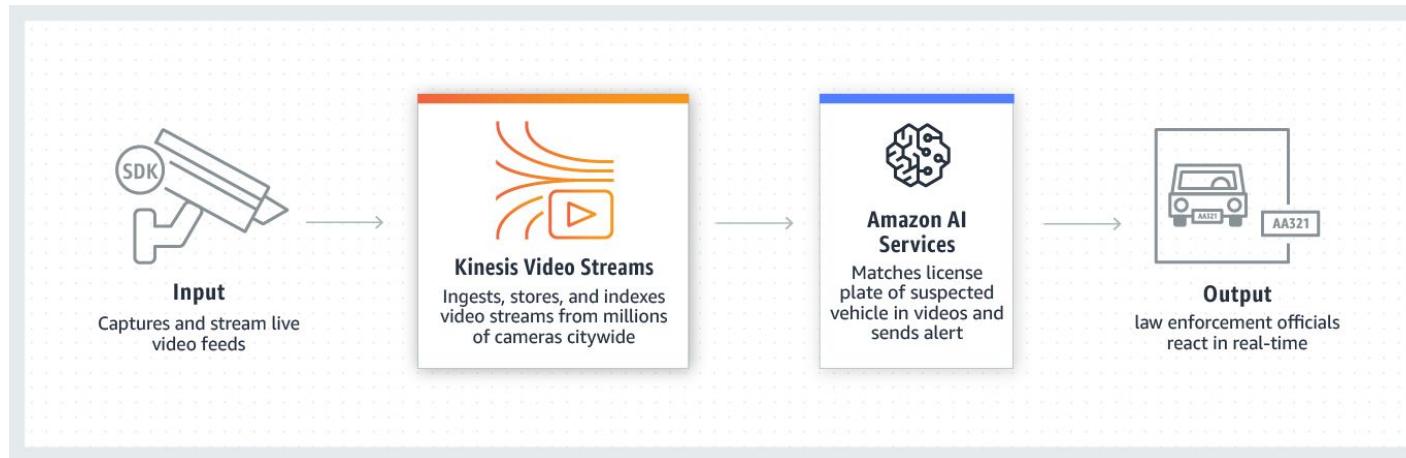
# Kinesis Data Analytics

Kinesis Data Analytics has ability to analyze data streams in real time.



# Kinesis Video Stream

Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS



---

# Direct Connect Billing

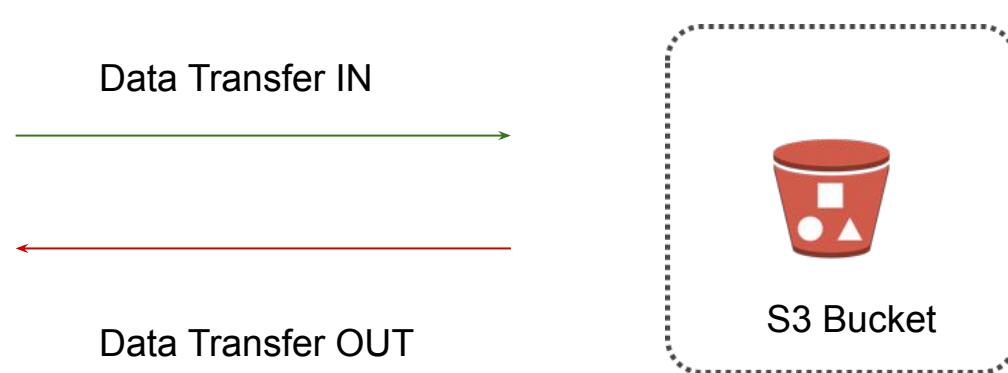
How you will be billed !

---

# Typical AWS Billing

In AWS the services are charged based on following factors:

- i) Typical service charge per hour / second
- ii) Network pricing
- iii) Resource charges



# Direct Connect Billing

In Direct Connect, the billing is calculated based on two factors:

- i) Pricing per port hour.
- ii) Data Transfer Charges (IN is free, OUT is charged)

Remember:

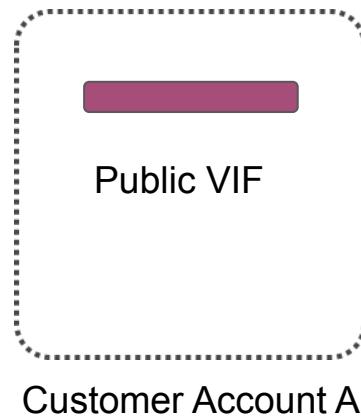
The account owner where the resource is IN, pays the price.

# Important Pointer

Virtual Interface can be hosted on external account as well.

In such case, the account on which the VIF interface is hosted, has to pay for the data transfer charges that occurs across that interface.

In US, there is a separate rate applied when you access the inter-region resources.



---

# Direct Connect Billing

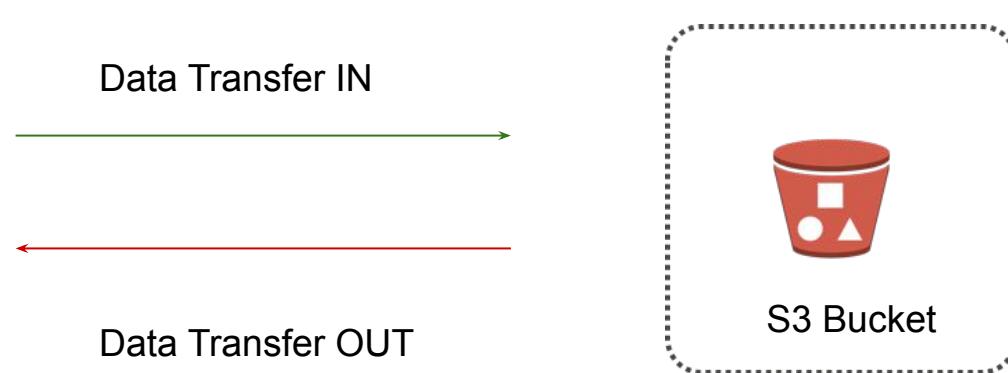
How you will be billed !

---

# Typical AWS Billing

In AWS the services are charged based on following factors:

- i) Typical service charge per hour / second
- ii) Network pricing
- iii) Resource charges



# Direct Connect Billing

In Direct Connect, the billing is calculated based on two factors:

- i) Pricing per port hour.
- ii) Data Transfer Charges (IN is free, OUT is charged)

Remember:

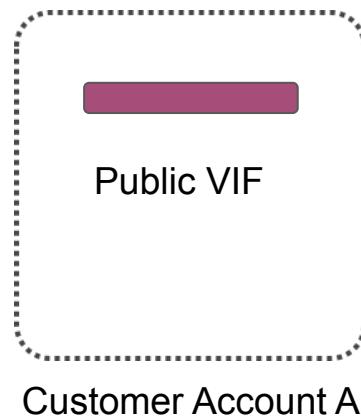
The account owner where the resource is IN, pays the price.

# Important Pointer

Virtual Interface can be hosted on external account as well.

In such case, the account on which the VIF interface is hosted, has to pay for the data transfer charges that occurs across that interface.

In US, there is a separate rate applied when you access the inter-region resources.



---

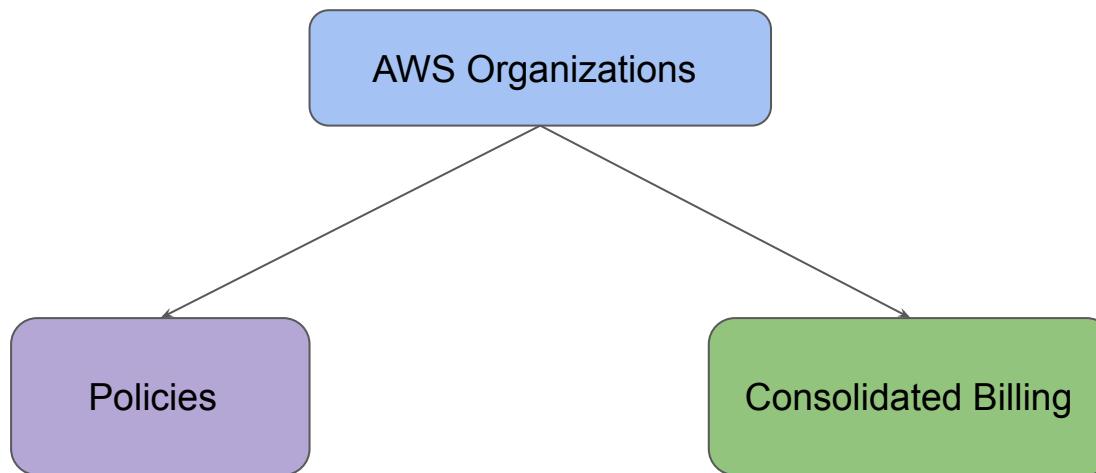
# AWS Organizations

Centralized Control

---

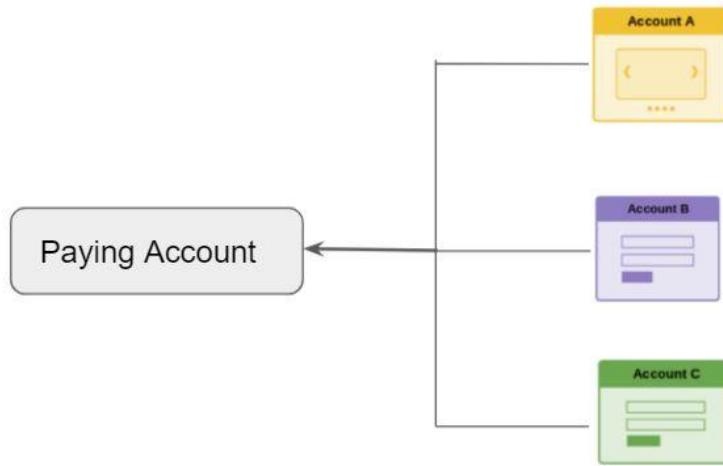
# Getting the basics right

AWS offers centralized policy-based management as well as the feature of consolidated billing for multiple AWS accounts through the feature of AWS Organizations.



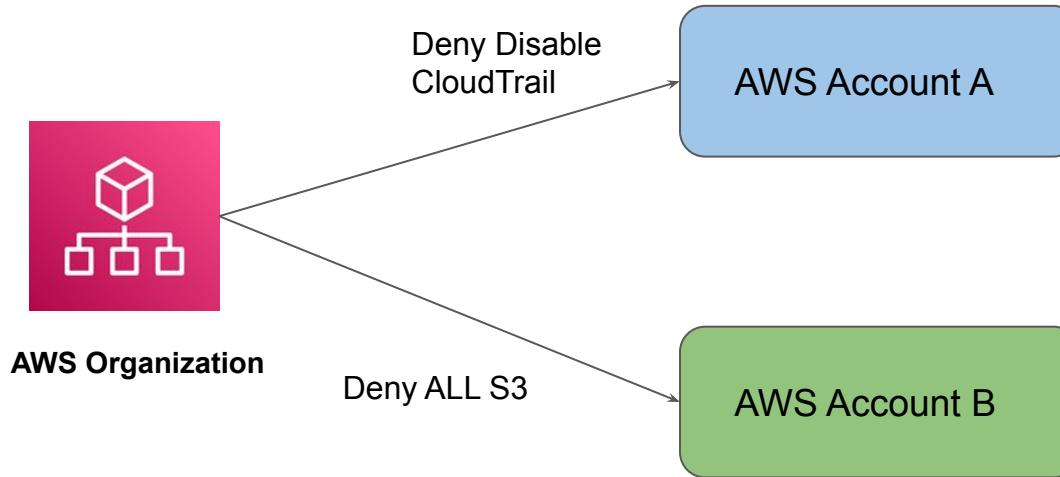
# Part 1 - Consolidated Billing

In consolidated billing, management account to access the billing information and pay for all member accounts.



## Part 2 - Policies

Policies in AWS Organizations enable you to apply additional types of management to the AWS accounts in your organizations.



---

# Firewall Manager

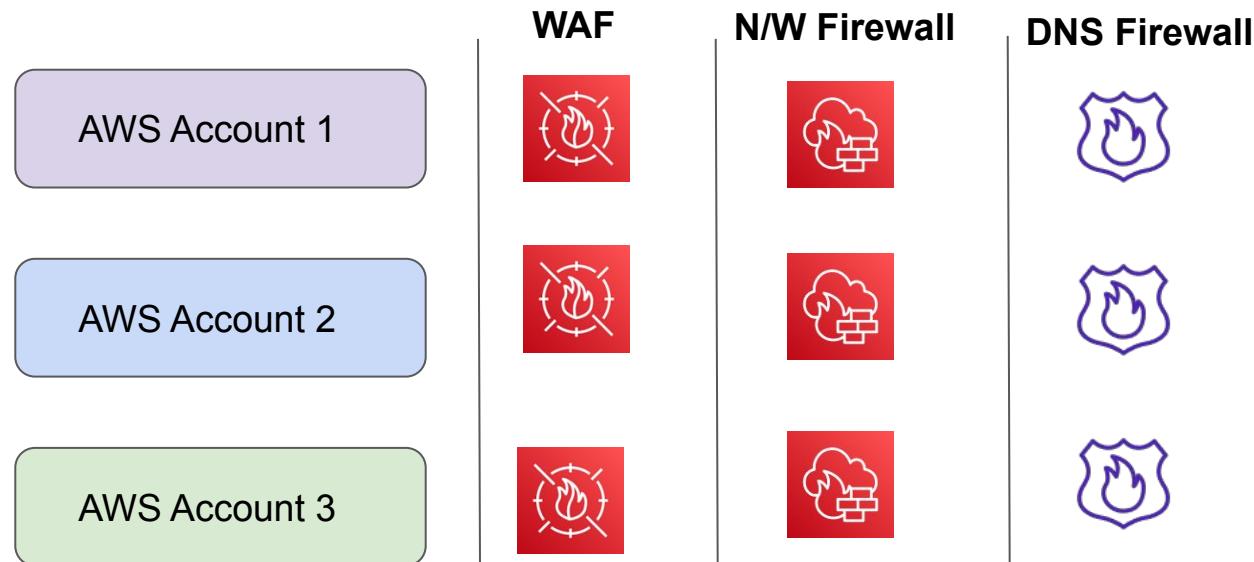
Centrally Manage Rules

---

# Understanding the Challenge

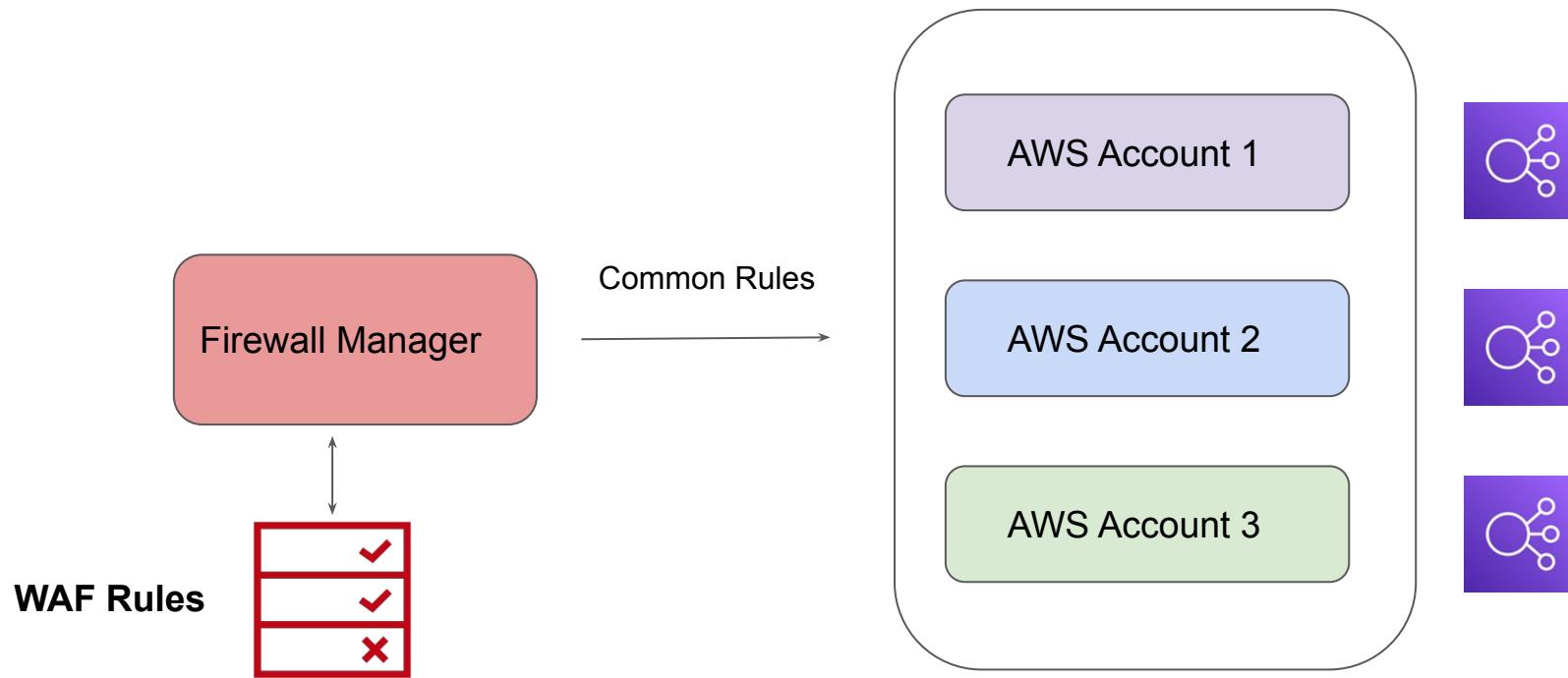
Most of the organizations are opting for Multi-Account based strategy for separation of environments (dev, stage, prod)

Security Team needs to create, maintain and update security services across all of the accounts.



# Understanding the Basics

AWS Firewall Manager is a security management service which allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations



# Supported Service

Firewall Manager supports wide variety of services, including:

- AWS WAF
- VPC Security Groups
- AWS Network Firewall
- Route53 DNS Firewall
- AWS Shield Advanced
- Palo Alto Cloud Next-generation firewalls

Important Prerequisite: AWS Organizations + AWS Config.

# Benefits of Firewall Manager

1. Simplify management of firewall rules across your accounts
2. Ensure compliance of existing and new applications
3. Easily deploy managed rules across accounts
4. Centrally deploy protections for your VPCs

---

# Infrastructure as Code

DevOps = Developers

---

# Understanding the Basics

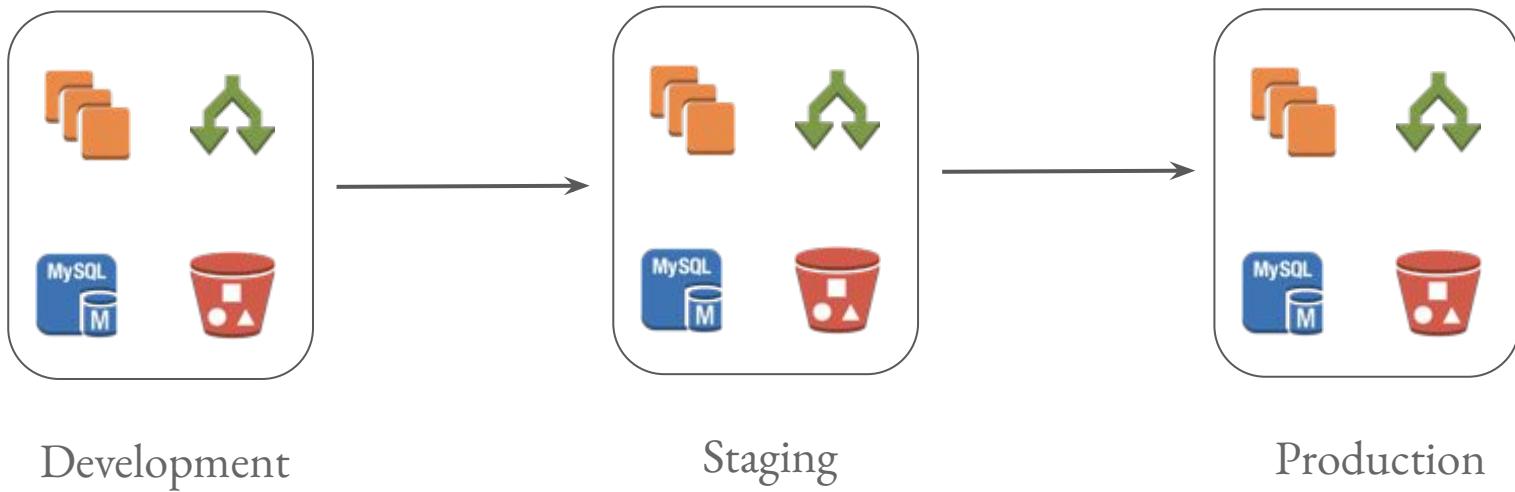
There are two ways in which you can build your infrastructure:

- Manually creating the infrastructure.
- Through Automation.

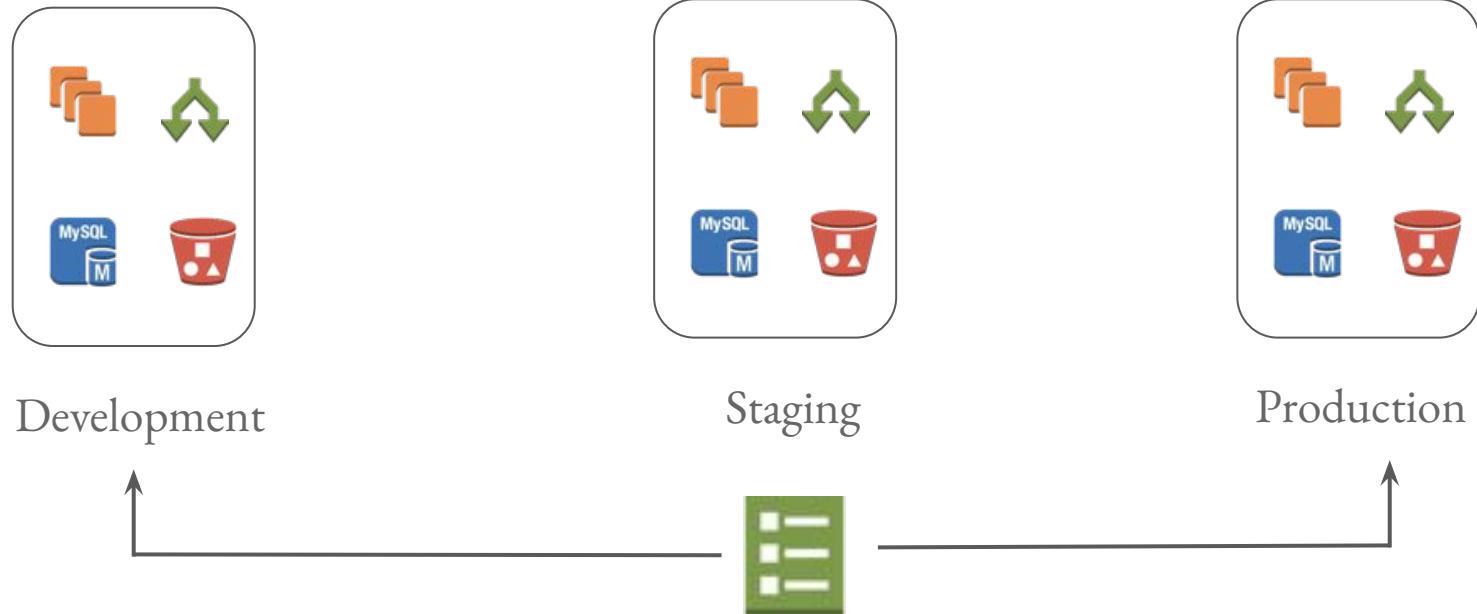
One of the major benefits of automation is the code usability.



# Example of single service



# Using IAAC



# Benefits of Infrastructure as a Code

There are several benefits of designing your infrastructure as code:

Reusable Code

Managing infrastructure via source control.

Enable collaboration



---

# CloudFormation - VPC

Let's Automate

---

# Getting started

We will look into a minimal template for deployment of VPC via CloudFormation.

# Simple VPC Template

```
1 AWSTemplateFormatVersion: "2010-09-09"
2 Description: VPC in North Virginia
3 Resources:
4   MyVPC:
5     Type: AWS::EC2::VPC
6     Properties:
7       CidrBlock: "10.77.0.0/16"
8       InstanceTenancy: default
9       Tags:
10      - Key: Name
11        Value: CFVPC
12      - Key: Environment
13        Value: Demo
14
```

# Getting started

**AWSTemplateFormatVersion** specifies the version of template being used.

Currently 2010-09-09 is the only valid value that can be associated.

All the resource you create goes inside the “**Resource**” section of the template.

---

# CloudFormation - Stack Dependencies

Deep Dive into CloudFormation

---

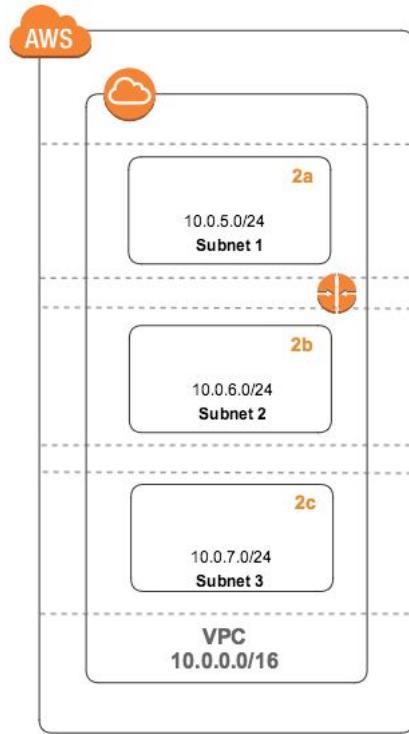
# Understanding Stack Dependencies

In the previous video we had created a simple VPC.

However having just a VPC is not of great use.

We need Subnets, Internet Gateways, NAT Gateways and others.

However while defining subnet, we need to provide the VPC ID.



Main Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-eb72s

# Dependencies Pointer

If the properties of resource A use a !Ref to resource B, the following rule apply:

- Resource B is created before resource A.
- Resource A is deleted before resource B.

---

# CloudFormation - DependsOn Attribute

Deep Dive into CloudFormation

---

# Dependencies Pointer

If the properties of resource A use a !Ref to resource B, the following rule apply:

- Resource B is created before resource A.
- Resource A is deleted before resource B.

# Let's Understand with Use-Case

## Sample Use-Case:

For Application 1, you need 3 resource to be created:

- EC2 Instance
- RDS
- S3 Bucket.

Note: Application inside EC2 instance won't get initialized if RDS Instance is not ready.

---

# CloudFormation - DependsOn Attribute

Deep Dive into CloudFormation

---

# Dependencies Pointer

If the properties of resource A use a !Ref to resource B, the following rule apply:

- Resource B is created before resource A.
- Resource A is deleted before resource B.

# Let's Understand with Use-Case

## Sample Use-Case:

For Application 1, you need 3 resource to be created:

- EC2 Instance
- RDS
- S3 Bucket.

Note: Application inside EC2 instance won't get initialized if RDS Instance is not ready.

---

# CloudFormation - Change Sets

Deep Dive into CloudFormation

---

# Understanding Change Sets

We normally edit the templates and do CloudFormation UpdateStack operation to activate the changes.

It is important to have an additional insight into the changes that CloudFormation is planning to perform when it updates a stack

This should then allow us to be able to preview the changes, verify that they are in line with their expectations, and proceed with the update.

# Change Sets

Change Sets allows us to submit the create a change set by submitting changes against the stack you want to update.

CloudFormation compares the stack to the new template and/or parameter values and produces a change set that you can review and then choose to apply

Changes (2)						
<input type="text"/> Search changes						
Action	Logical ID	Physical ID	Resource type	Replacement		
Add	MySubnet	-	AWS::EC2::Subnet	-		
Remove	MySubnet2c	subnet-03d07fda6b5a53761	AWS::EC2::Subnet	-		

---

# CloudFormation - Parameters

Deep Dive into CloudFormation

---

# Getting Started

Parameters in CloudFormation enable you to input custom values to your template each time you create or update a stack.

Let's understand with a use-case:

- We have created a CloudFormation template which will create an EC2 instance.
- Anyone within organization who wants to launch EC2 should use the template.

Problem:

- Template has a hard-coded value of m5.large and it needs constant modification.

# Defining Parameter in Template

In following example, we define an **InstanceTypeParameter**.

This allows users to specify the Amazon EC2 instance type for the stack to use when you create or update the stack.

## Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

### InstanceTypeParameter

Enter t2.micro, m1.small, or m1.large. Default is t2.micro.

t2.micro	▼
t2.micro	
m1.small	
m1.large	

---

# CloudFormation - StackSets

Need to learn the backend

# Getting Started

CloudFormation StackSets basically allows us to deploy stacks across multiple AWS account / AWS regions from single location.

## Simple Use-Case:

- AWS Config is recommended to be enabled in all regions.
- Before we had to maintain stack across each region.
- This can now be solved easily using Stack Sets

# Deployment Instruction

Two IAM Roles required:

1 for the Administrator Account of StackSets

1 for the Destination AWS Accounts.

Role Name for Admin Account: AWSCloudFormationStackSetAdministrationRole

Role Name for Dest Account: AWSCloudFormationStackSetExecutionRole

---

# Elastic Beanstalk

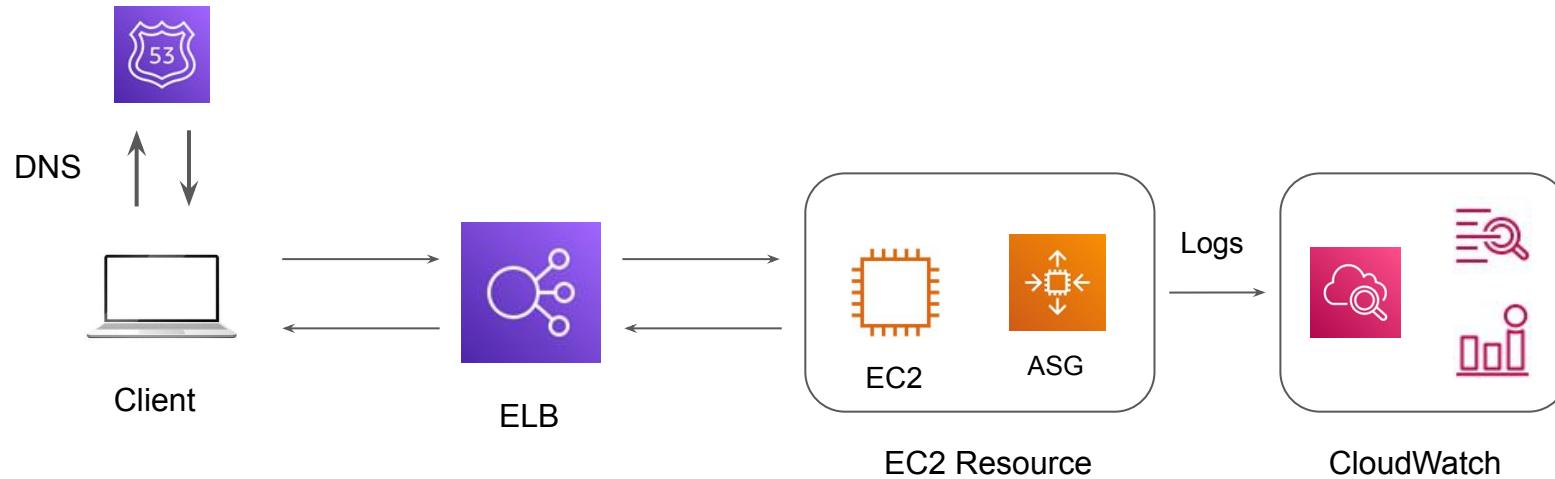
## Orchestration

---

# Traditional Deployment Approach

Use-Case: Deploy a simple Hello World application for production.

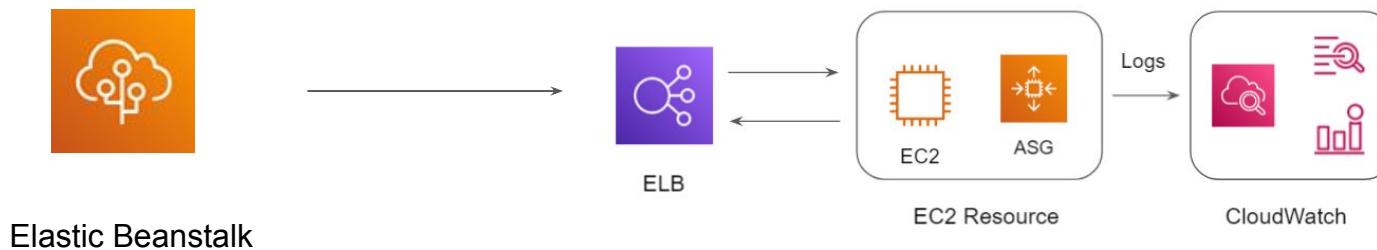
Resources to be created: AWS EC2, ELB, Auto-Scaling, Web-Server Configuration, and others.



# Elastic Beanstalk Deployment Approach

Use-Case: Deploy a simple Hello World application for production.

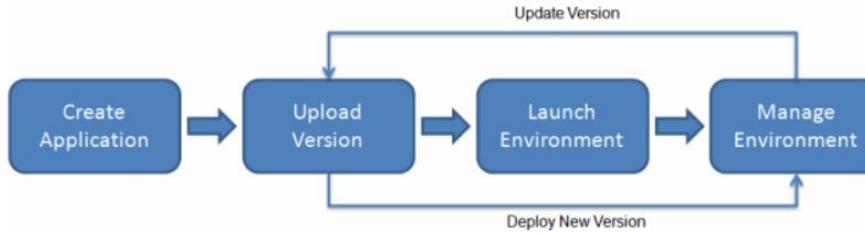
Create Elastic Beanstalk Environment



# Overview of Elastic Beanstalk

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services.

You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.



---

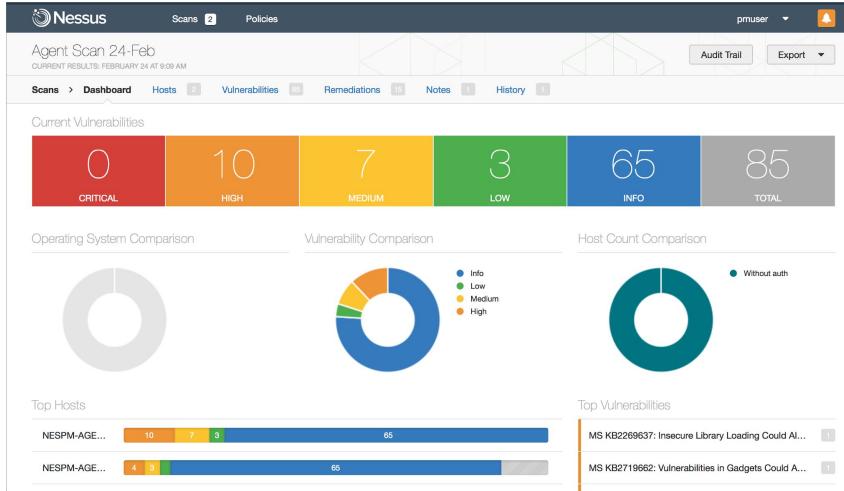
# Penetration Testing in AWS

Understand before you pentest

---

# Understanding Vulnerability Scanning

Vulnerability Scanning generally refers to scanning of a system to find known weakness.



# Understanding Penetration Testing

Penetration Tests often refers to running exploits against a given system with intention to compromise.



```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
      Is the server running on host "localhost" (::1) and accepting
      TCP/IP connections on port 5432?
could not connect to server: Connection refused
      Is the server running on host "localhost" (127.0.0.1) and accepting
      TCP/IP connections on port 5432?

          dBBBBBBBb  dBPP dBBBBBBP dBBBBBBb
          dB' dB' dB' dBPP    dBPP    dBPP BB
          dB' dB' dB' dBPP    dBPP    dBPP BB
          dB' dB' dB' dBPP    dBPP dBBBBBBP
          dB' dB' dB' dBPP    dBPP dBBBBBBP dB' BP
          dB' dB' dB' dBPP    dBPP dB' BP dBPP dBPP
          dB' dB' dB' dBPP    dBPP dB' BP dBPP dBPP
          dB' dB' dB' dBPP    dBPP dB' BP dBPP dBPP
          dB' dB' dB' dBPP    dBPP dB' BP dBPP dBPP

          To boldly go where no
          shell has gone before

      =[ metasploit v4.17.3-dev
+ -- --=[ 1795 exploits - 1019 auxiliary - 310 post
+ -- --=[ 538 payloads - 41 encoders - 10 nops
+ -- --=[ Free Metasploit Pro trial: http://r7.co/trymsp ]]

msf > [
```

# Getting Started

Earlier it was **mandatory** to submit an “AWS Vulnerability / Penetration Testing Request Form” to request the authorization for pentest to or from the AWS workloads.

AWS has now removed the clause and customers can go ahead and carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services.

# Allowed Services

Following are the supported services where prior approval is not needed.

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Do note that these lists are constantly updated by AWS.

# Additional Important Pointers

It is recommended to exclude following EC2 instance types to minimize potential disruption to your environment

- T3.nano
- T2.nano
- T1.micro
- M1.small

---

# CloudTrail

Let's Monitor Everything !

---

# Importance of Recording Everything

Installing video surveillance systems allows us to monitor activities round the clock and provides lots of benefits, some of these include:

1. Deterring Criminals
2. Helps in Investigation.
3. Regular monitoring of activities.
4. Insurance Benefits.



# Recording at AWS Level

It is **VERY** important for organizations to record the activities that happen within the Infrastructure as well as the servers.

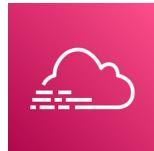
Example Auditor Question :-

Show me what did Anne did on 3rd of January 2017 between 10 AM to 2 PM.

User	Action	Time
James	Logged In	3:50 PM
Anne	Modified SG	7:30 PM
Susan	New EC2	11:00 PM

# Tools for Recording

Depending on the type of resource you use, the tools for recording might also change.



CloudTrail

Record AWS events



Record Linux events



---

# CloudTrail Event Types

Monitor Everything

---

# Type of Events

There are three types of events that can be logged in CloudTrail:

1. Management events
2. Data events
3. Insights events.

The screenshot shows the 'Events' configuration page. It includes a summary section for 'Events' with an 'Info' link and a note about additional charges. Below this, there's a 'Event type' section with a sub-instruction to choose the type of events to log. Three checkboxes are present: 'Management events' (checked), 'Data events' (unchecked), and 'Insights events' (unchecked). Each checkbox has a descriptive subtitle below it.

**Events** [Info](#)  
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

**Event type**  
Choose the type of events that you want to log.

**Management events**  
Capture management operations performed on your AWS resources.

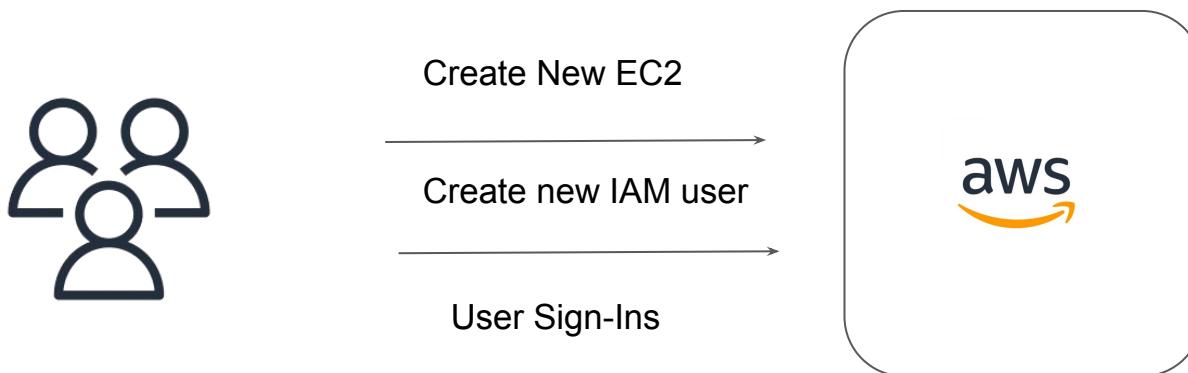
**Data events**  
Log the resource operations performed on or within a resource.

**Insights events**  
Identify unusual activity, errors, or user behavior in your account.

By default, trails log management events, but not data or Insights events.

# 1. Management Events

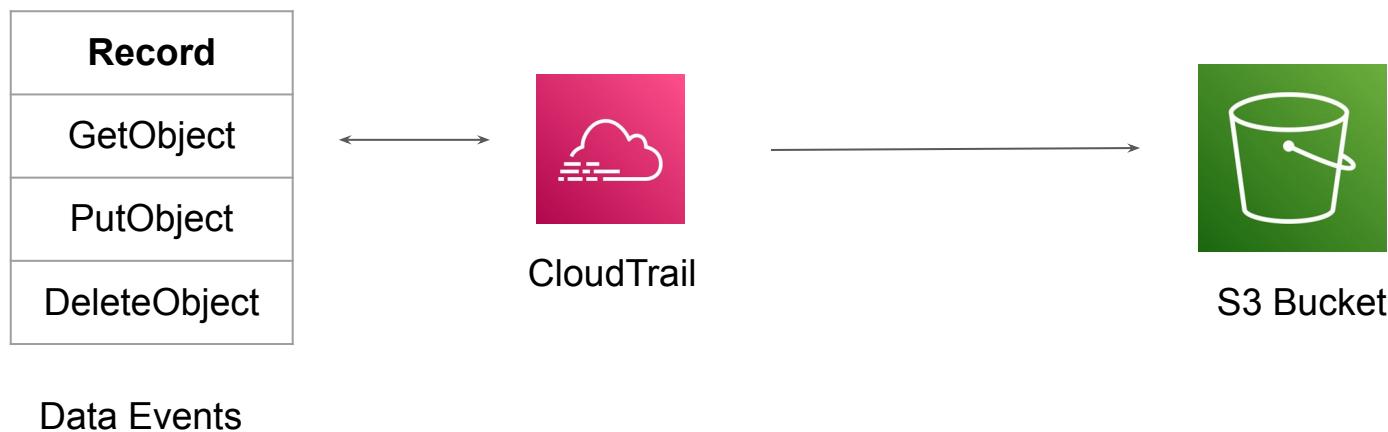
Management events provide information about management operations that are performed on resources in your AWS account.



## 2. Data Events

Data events provide information about the resource operations performed on or in a resource and are often high-volume activities.

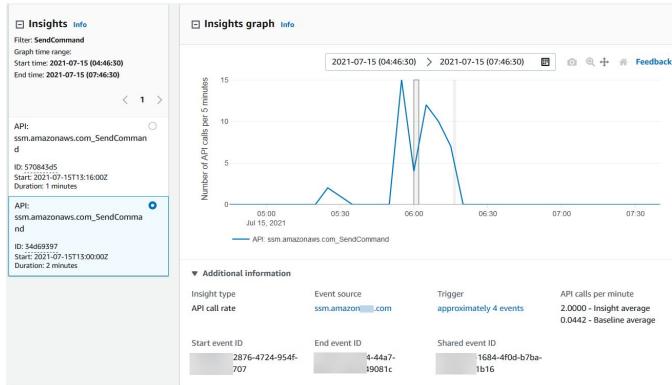
Following diagram shows type of events capture at S3 level when Data events is enabled.



### 3. Insights Events

Insight Events helps customers identify unusual operational activity in their AWS accounts such as spikes in resource provisioning, bursts of AWS Identity and Access Management (IAM) actions

Is designed to automatically analyze management events to establish a baseline for normal behavior, and then raise issues by generating Insights events when it detects unusual patterns.



---

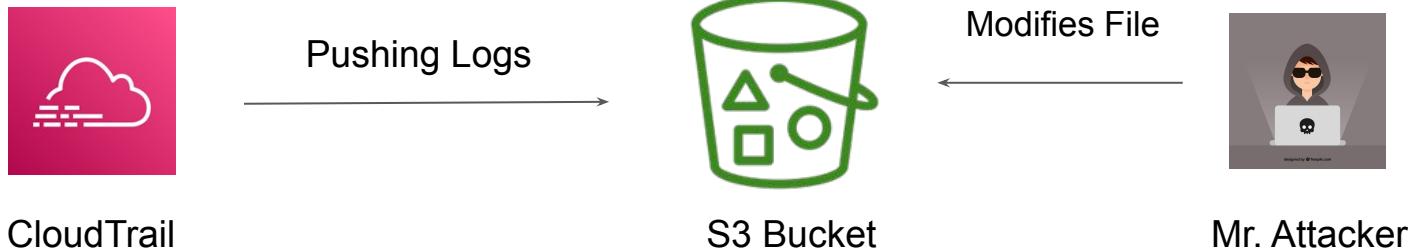
# CloudTrail - Log File Integrity Validation

Back to Security!

# Getting Started

CloudTrail log file integrity validation allows us to determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it.

This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing.



# Basic Working

When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers.

Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file.

# Relax and Have a Meme Before Proceeding

Do you have a special talent?

Me:



---

# AWS Config

## Overview of Infrastructure Changes

---

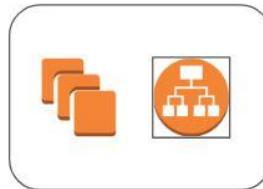
# AWS Config - High Level Overview

AWS Config is primarily used to record the resource configuration changes over time.

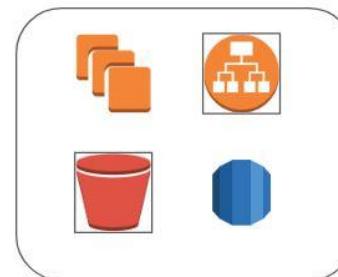
An EC2 instance was hosting website from past 90 days. Suddenly in last one week, there have been a lot of issues with the requests. What was changed?



Week 1



Week 2



Week 3

# Audit and Compliance

AWS Config comes with large set of rules that can continuously monitor your AWS environment and report the findings.

Noncompliant rules by noncompliant resource count	
Name	Compliance
RootAccountHardwareMFAEnabled-conformance-pack-zcx0hyuom	<span style="color: red;">⚠</span> 1 Noncompliant resource(s)
RootAccountMFAEnabled-conformance-pack-zcx0hyuom	<span style="color: red;">⚠</span> 1 Noncompliant resource(s)
IAMPasswordPolicy-conformance-pack-zcx0hyuom	<span style="color: red;">⚠</span> 1 Noncompliant resource(s)
approved-amis-by-id	<span style="color: red;">⚠</span> 1 Noncompliant resource(s)
cloudtrail-security-trail-enabled	<span style="color: red;">⚠</span> 1 Noncompliant resource(s)

[View all noncompliant rules](#)

# Conformance Packs

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed

The screenshot shows the 'Deploy conformance pack' wizard in the AWS Config console. The current step is 'Step 1 Specify template'. A search bar at the top contains the text 'S'. Below it is a dropdown menu showing a list of operational best practices:

- Operational Best Practices for Amazon S3
- Operational Best Practices for Asset Management
- Operational Best Practices for BCP and DR
- Operational Best Practices for BNM RMIT
- Operational Best Practices for CCN ENS Low
- Operational Best Practices for CCN ENS Medium
- Operational Best Practices for CIS AWS v1\_3 Level1
- Operational Best Practices for CIS AWS v1\_3 Level2
- Operational Best Practices for CIS
- Operational Best Practices for CMMC Level 1
- Operational Best Practices for CMMC Level 2
- Operational Best Practices for Compute Services
- Operational Best Practices for Data Resiliency
- Operational Best Practices for Amazon S3

To view the sample templates, see [Conformance Pack Sample Templates](#).

At the bottom right are 'Cancel' and 'Next' buttons.

# Pricing of AWS Config

You pay \$0.003 per configuration item recorded in your AWS account per AWS Region. A configuration item is recorded whenever a resource undergoes a configuration change or a relationship change.

Based on rule evaluation. A rule evaluation is recorded every time a resource is evaluated for compliance against an AWS Config rule.

You are charged per conformance pack evaluation in your AWS account per AWS Region based on the tier below.

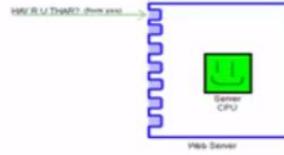
---

# Denial of Service

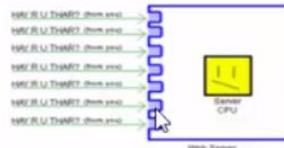
Attack difficult to mitigate

---

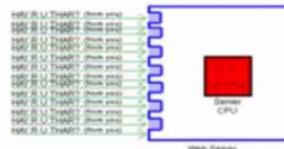
**normal service →**



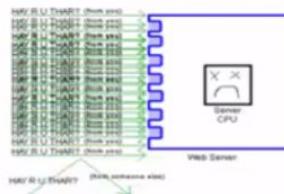
**high traffic →**



**single DOS →**



**LOL DDOS'D →**



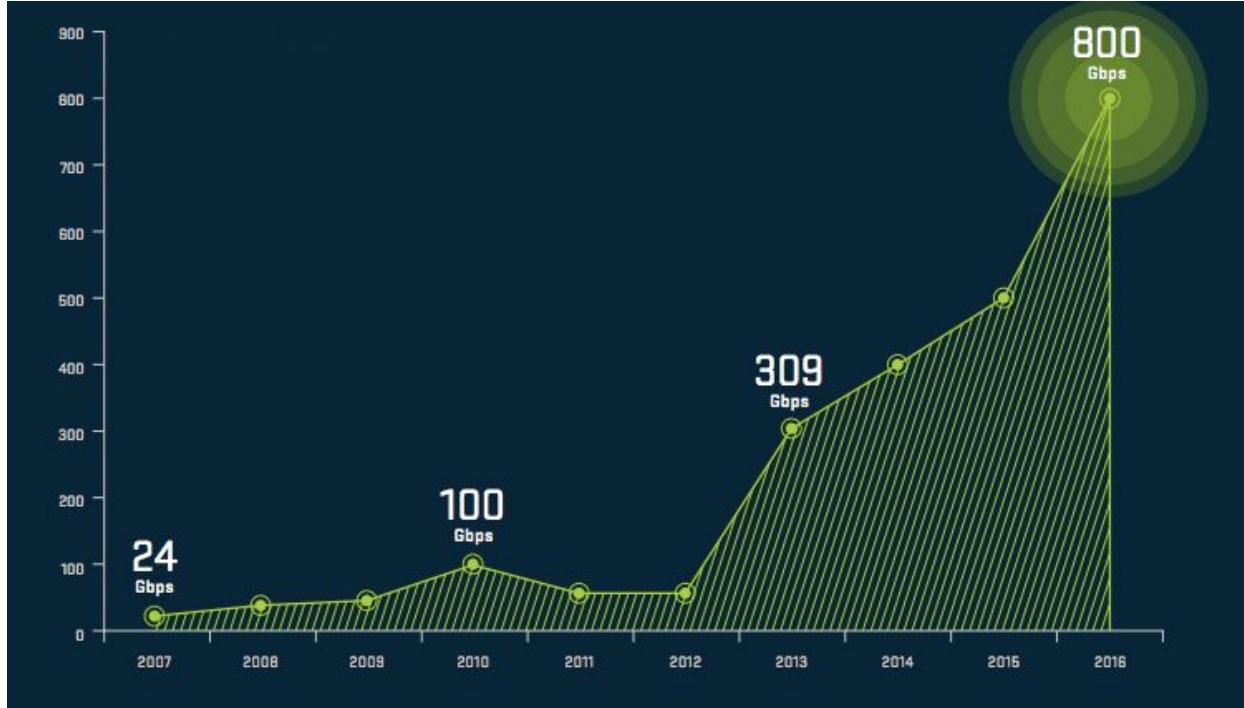
# DOS and DDoS are part and parcel of servers life

DOS and DDoS attacks are very common attack vectors used nowadays to bring down the servers or flood the network.

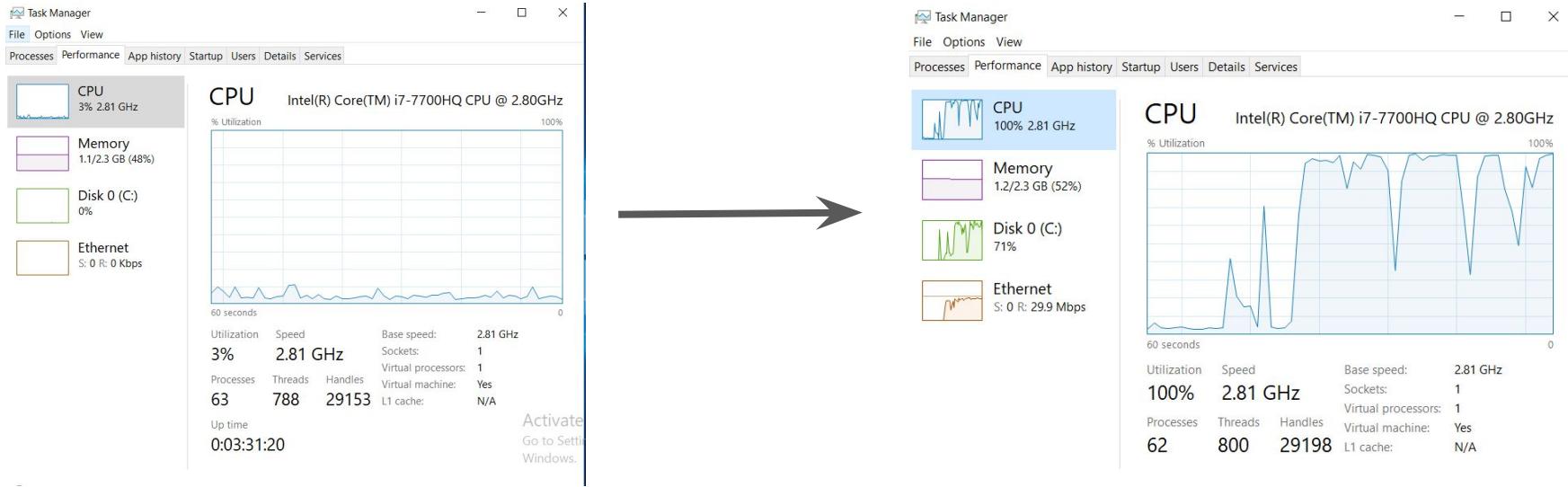
The reason why they are so successful is because of ease of ability to launch the attack and most of the protection mechanisms are based on expensive hardware.



# DDOS attacks are going really big!



# Before vs After (DOS Attack)



# DDOS Attacks Crush Twitter, Hobble Facebook

Posted Aug 6, 2009 by Michael Arrington (@arrington)



The image shows the Twitter homepage. At the top, there's a navigation bar with links for Home, Profile, Find People, Settings, Help, and Sign out. Below the navigation, a large message box contains the text: "We had network issues today related to a denial-of-service attack. Service now is restored for most people and we're investigating further." This message was posted 8 minutes ago from the web. At the bottom of the page, there's a Facebook logo and a link to their site. The footer contains links for About Us, Contact, Blog, Status, Goodies, API, Business, Help, Jobs, Terms, and Privacy.

## Crunchbase

<b>Facebook</b>	-
FOUNDED 2004	
<b>OVERVIEW</b> Facebook is an online social networking service that allows its users to connect with friends and family as well as make new connections. It provides its users with the ability to create a profile, update information, add images, send friend requests, and accept requests from other users. Its features include status update, photo tagging and sharing, and more. Facebook's profile structure includes ...	
LOCATION Menlo Park, California	
CATEGORIES Social Media, Social Network, Social	
WEBSITE <a href="http://www.facebook.com">http://www.facebook.com</a>	

---

# Mitigating DDOS

The stronghold for Fort

---

# Mitigating DDOS

- Be ready to scale as traffic surges.
- Minimize the attack surface area.
- Know what is normal and abnormal.
- Create a Plan for Attacks.



# Be Ready to Scale

## 1. Be Ready to Scale

- Your infrastructure should be designed to scale when the traffic increases.
- It not only helps in Business but also during DDOS Attacks.

Example :

Whenever CPU load is more than 70% in Application servers, automatically add one more Application server to meet the needs.

**AWS Services :** ELB, Auto Scaling

# Let's Minimizing is the Key

## 2. Minimize the attack surface area.

Decouple your infrastructure.

Example :

Application and Database should not be on the same server.

**AWS Services** : SQS, Elastic BeanStalk

# Normal and Abnormal

## 3. Know what is normal and abnormal

- Key metrics need to be defined to understand the behavior.

Example :

Website getting a huge surge in traffic in the middle of the night at 3 AM

**AWS Services** :- CloudWatch, SNS.

# Create a Plan

## 4. Create a Plan for Attacks.

For example :

- Check whether the Source IP Address is the same.
- Check from which country the increased traffic is coming from.
- Nature of the attack ( SYN Flood, Application Level )
- Can it be blocked with NACL or Security Group level.



It is recommended to have AWS Support. At-least Business Support.

# AWS Services for DDoS Attack Mitigation

Following are some of the key AWS services involved in DDoS attack mitigation

- **AWS Shield**
- **Amazon CloudFront**
- **Amazon Route53**
- AWS WAF
- Elastic Load Balancing
- VPC & Security Groups

---

# Network ACL

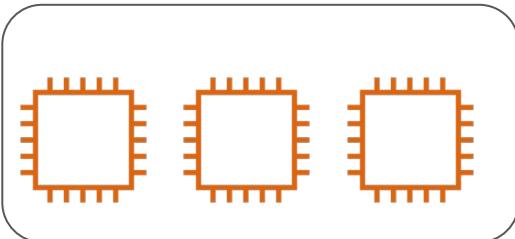
Multiple Layers for Defense

---

# Understanding the Basics

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.

- Security Group works at an EC2 instance level.
- Network ACL works at a Subnet Level.



**Security Group**

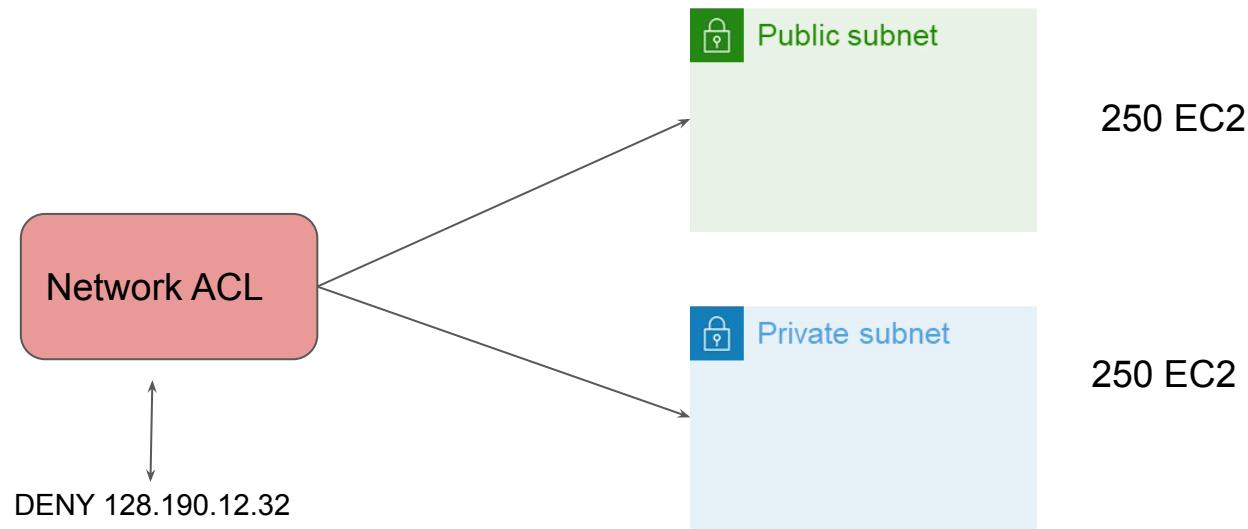


**Network ACL**

# Understanding with Use-Case

Company XYZ is getting **lot of attacks** from a random IP **128.190.12.32**. The company has more than 500 servers and Security team decided to block that IP in firewall for all the servers.

How to go ahead and achieve that goal ?



# Important Pointers

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.

Default NACL allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.

You can associate a network ACL with multiple subnets. However, a subnet can be associated with only one network ACL at a time.

---

# Network ACL - Rule Ordering

Setting Right Set of NACL Rules

---

# Basics of Rules

You can add or remove rules from the default network ACL

When you add or remove rules from a network ACL, the changes are automatically applied to the subnets that it's associated with.

The screenshot shows the AWS Network ACL management interface for a specific ACL named 'acl-1888e173'. The 'Inbound rules' tab is selected, showing two rules listed in a table. The table includes columns for Rule number, Type, Protocol, Port range, Source, and Allow/Deny status. The first rule, numbered 100, allows all traffic from 0.0.0.0/0. The second rule, marked with an asterisk (\*), denies all traffic from 0.0.0.0/0. A 'Filter inbound rules' search bar and a 'Edit inbound rules' button are also visible.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input type="checkbox"/> Deny

# Rule Ordering

Rules are evaluated starting with the lowest numbered rule.

As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that might contradict it.

Rule Number	Rule Contents
99	ALLOW from 10.77.0.5
100	DENY from ALL

# Important Pointers - Deciding Ports

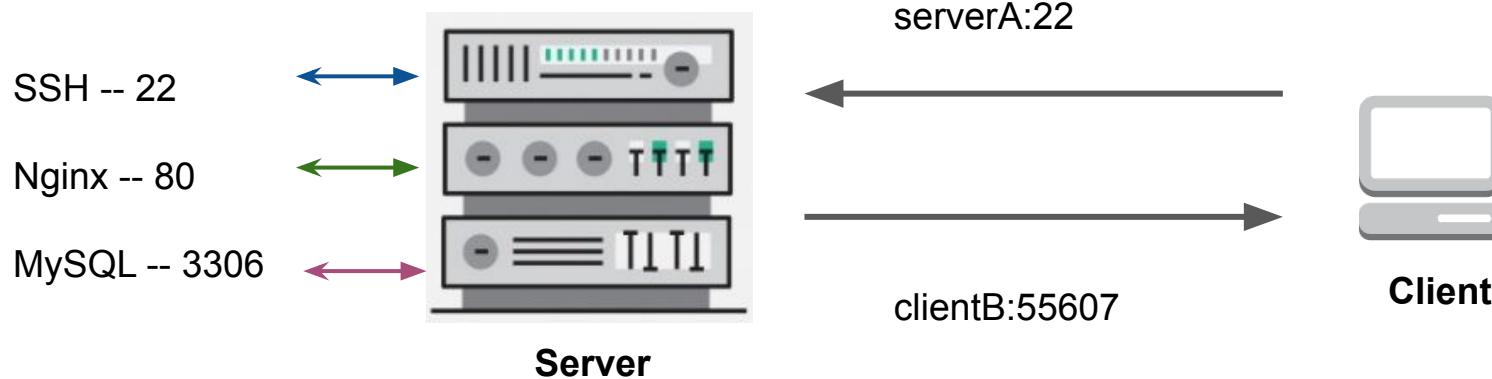
- Clients that initiates the request chooses ephemeral port range.
- Port 0 to 1023 are well known or reserved ports.
- This range varies depending on the Operating System.

**Example :-**

Many Linux kernels uses ports 32768-61000.

Request originating from the ELB uses 1024-65535

Windows XP uses 1025-5000 port range.



- Clients opens an **port 55607** from which it sends data to serverA port 22
- serverA has to respond back to the same IP (clientB ) & port ( 55607 ).

# TCP/IP Communication

```
fczv329@fcblr-l003:~/Documents$ cat handshake
19:46:27.378297 3c:a9:f4:a0:fa:e0 > 08:5b:0e:47:be:1e, ethertype IPv4 (0x0800), length 74: 172.20.1.55.55427 > 128.199.106.4.80: Flags [S], seq 3002048179, win 29200, options [mss 1460,sackOK,TS val 202385607 ecr 0,nop,wscale 7], length 0

19:46:27.798037 08:5b:0e:47:be:1e > 3c:a9:f4:a0:fa:e0, ethertype IPv4 (0x0800), length 74: 128.199.106.4.80 > 172.20.1.55.55427: Flags [S.], se
q 2402250441, ack 3002048180, win 14480, options [mss 1460,sackOK,TS val 2028995051 ecr 202385607,nop,wscale 8], length 0

19:46:27.798119 3c:a9:f4:a0:fa:e0 > 08:5b:0e:47:be:1e, ethertype IPv4 (0x0800), length 66: 172.20.1.55.55427 > 128.199.106.4.80: Flags [.], ack 1, win 229, options [nop,nop,TS val 202385712 ecr 2028995051], length 0
```

---

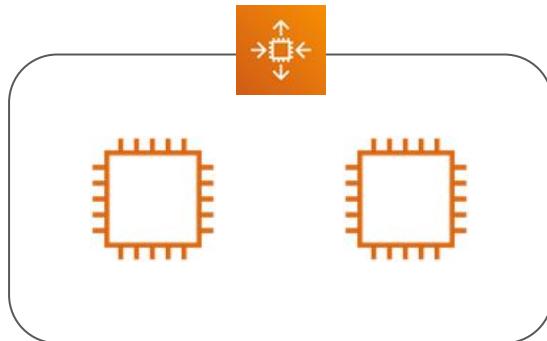
# Referencing Security Groups

Right Way

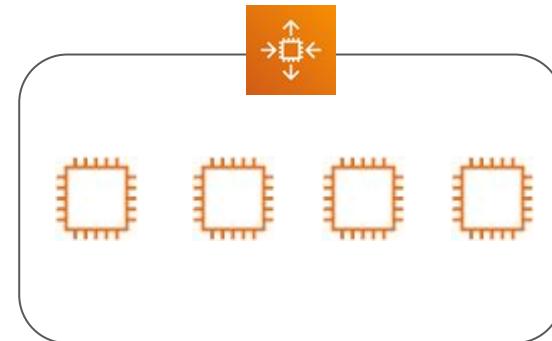
# Getting Started

In Security Group rules, along with IP addresses, we can also refer to the security group of the destination EC2 instances.

This is a good practice specifically when using EC2 instances in auto-scaling group.



Web Server Tier



Application Tier

# Solution

Create two security groups: 1st for Web Servers and 2nd for Application Servers.

Let's assume following are the security group id's assigned:

- i) Web Servers: sg-web
- ii) App Servers: sg-app

<b>SG Rule</b>	<b>Role</b>	<b>Allowed Rule</b>
1	Web Server Instances	Outbound Port 8080 to sg-app
2	App Instances	Inbound 8080 from sg-web

# Referencing SG Across VPC Peering

Security Group can be referenced across VPC Peering connections as well.

If there are two VPC's in a peering connection in the same region, then we can reference by security group id's from the peer VPC.

# Cross-Account SG Reference

To reference a security group in another AWS account, include the account number in **Source** or **Destination** field

other-aws-account-id/account-security-group-id

Example Rule:

123456789012/sg-1a2b3c4d

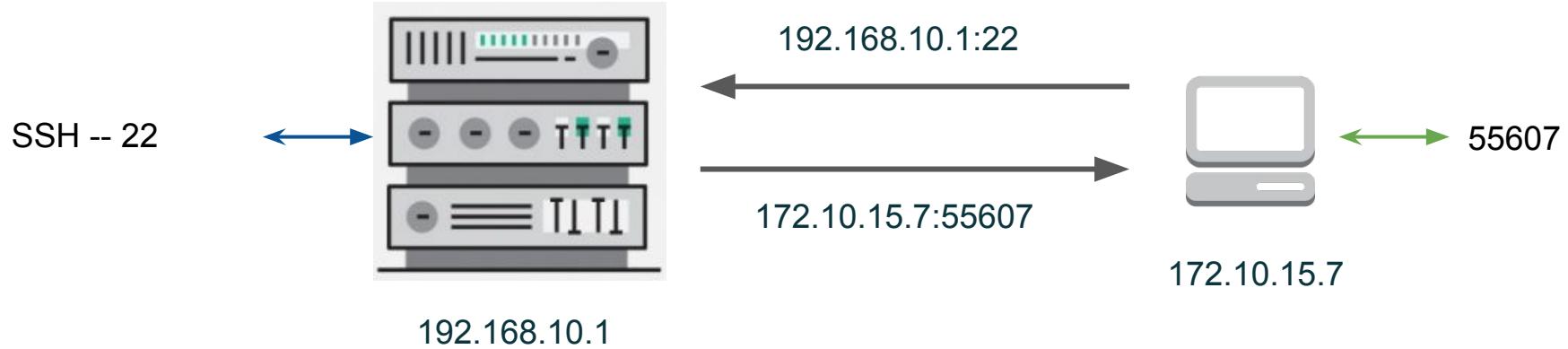
You cannot reference the security group of a peer VPC that's in a different region. Instead, use the CIDR block of the peer VPC.

---

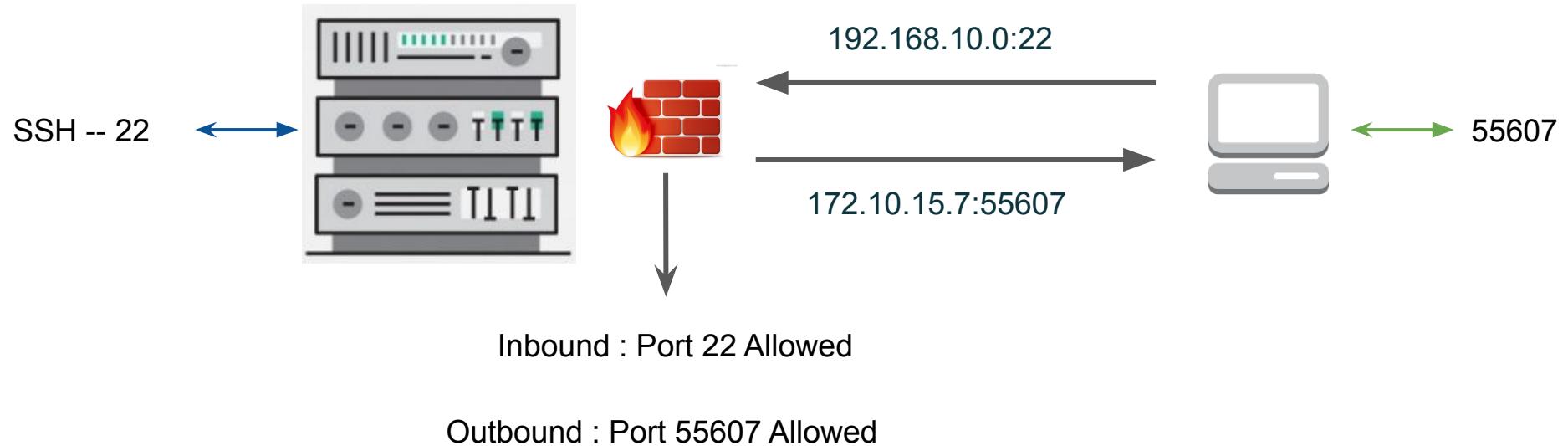
# Stateful vs Stateless Firewalls

2 types of Firewall

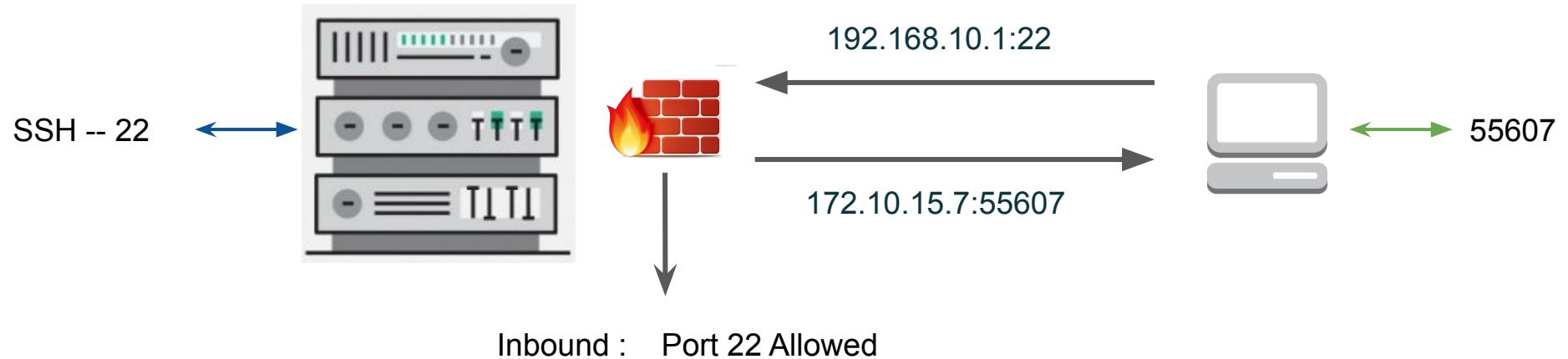
# Basic TCP/IP Communication



# When Stateless Firewall is Involved



# Stateful Firewall



# The Finale

There are 2 main types of Firewall :-

- Stateful Firewall
- Stateless Firewall

Stateful firewall maintains the connection state and knows which packets to allow Outbound even when outbound is restricted.

Stateless firewall does not maintain the connection state and for them each packet traversing inbound or outbound is a new separate packet.

---

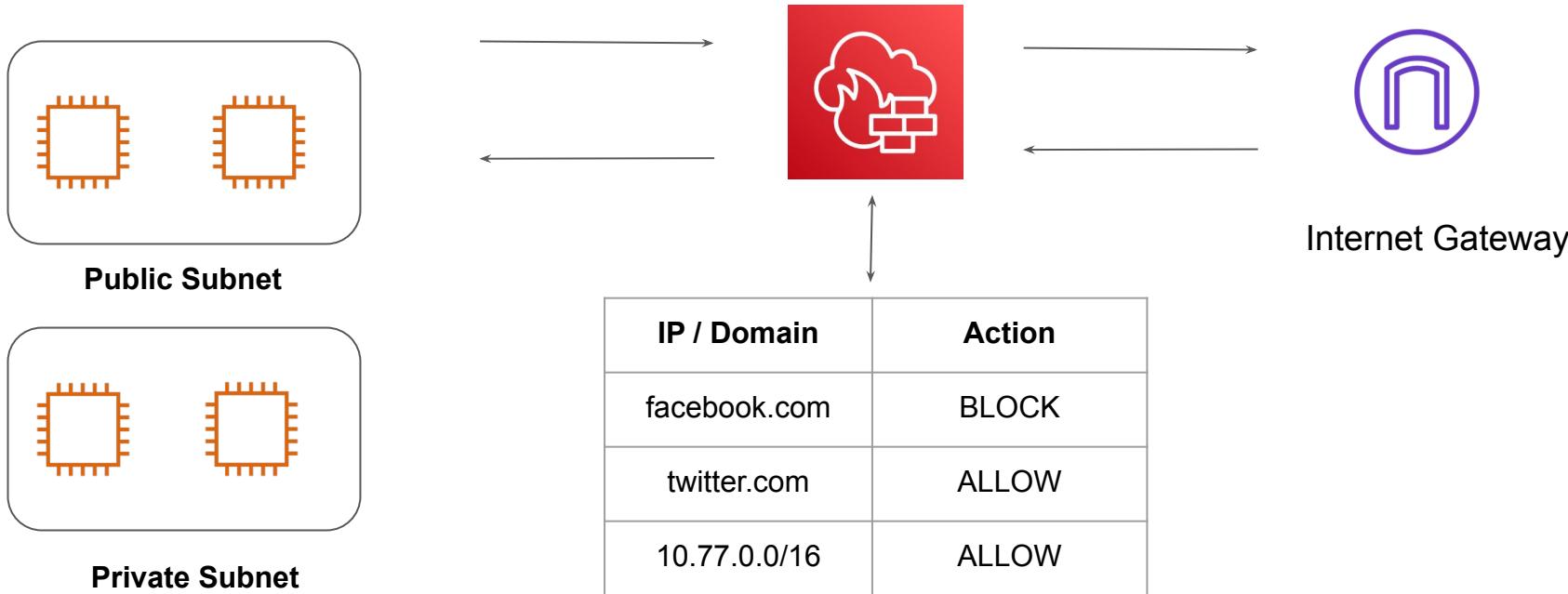
# AWS Network Firewall

Yet Another Firewall

---

# Basics of Network Firewall

AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC)



# Benefits of Network Firewall

You can use Network Firewall to monitor and protect your Amazon VPC traffic in a number of ways, including the following:

1. Pass traffic through only from known AWS service domains or IP address endpoints, such as Amazon S3.
2. Use custom lists of known bad domains to limit the types of domain names that your applications can access
3. Perform deep packet inspection on traffic entering or leaving your VPC

---

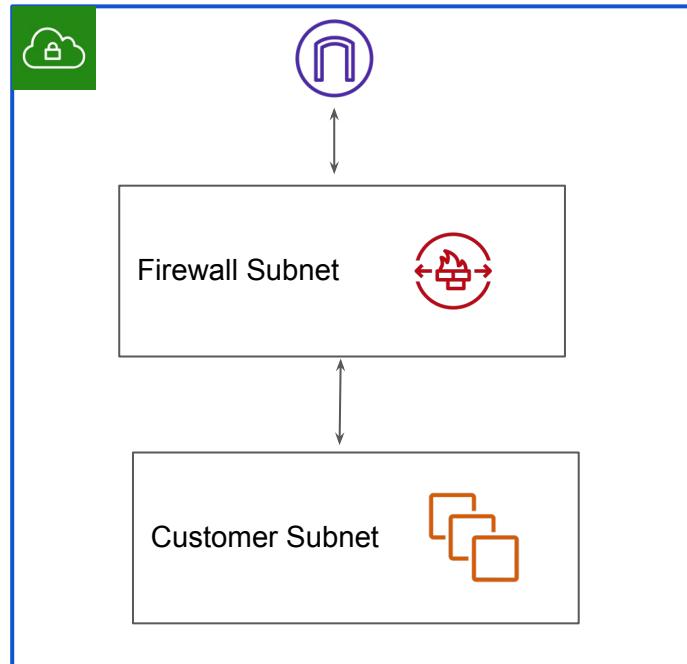
# Deploying Network Firewall

Let's Deploy Network Firewall

---

# Basic Deployment Architecture

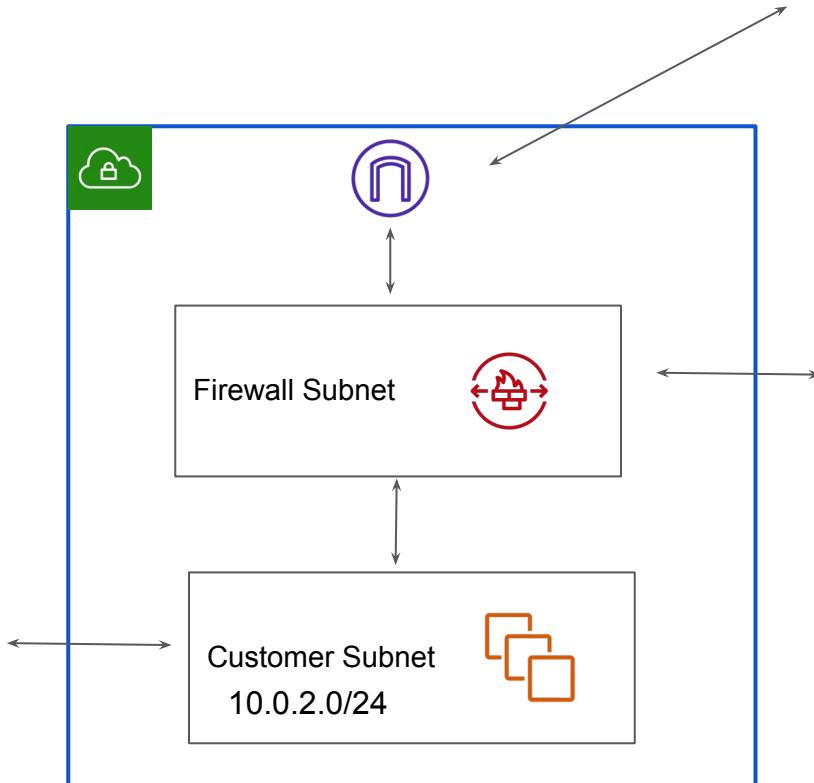
The Network firewall protects the subnets within your VPC by filtering traffic going between the subnets and locations outside of your VPC



# Route Table Entries

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	vpce-1234

**Customer Subnet**



Destination	Target
10.0.2.0/24	vpce-1234

**IGW**

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1234

**Firewall Subnet**

# Configuration Steps

Following are the 3 resource types that Network Firewall Manages.

<b>Resource Type</b>	<b>Description</b>
RuleGroup	Defines a set of rules to match against VPC traffic, and the actions to take when Network Firewall finds a match.
FirewallPolicy	Allows adding multiple rule groups and configure other settings.
Firewall	Provides traffic filtering logic for the subnets in a VPC.

---

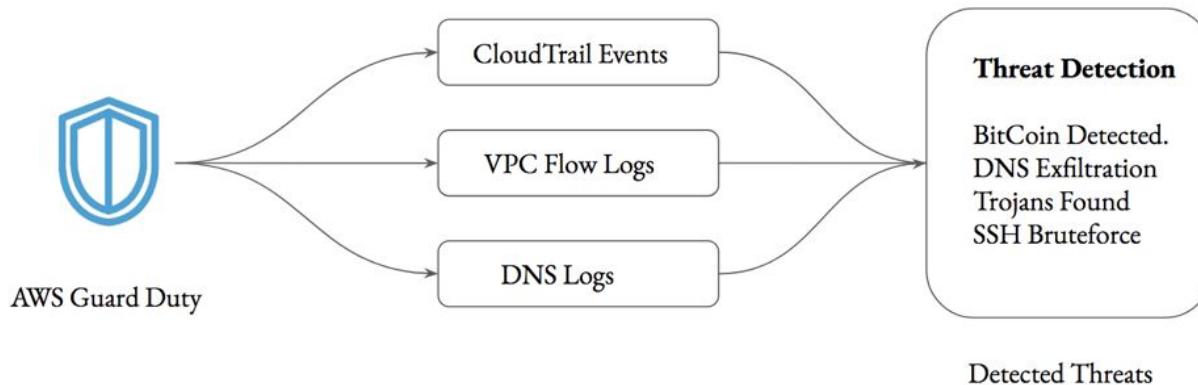
# AWS GuardDuty

Let's start Rolling !

---

# Understanding GuardDuty

AWS Guard Duty is a threat intelligence service by AWS which monitors for malicious behavior to help customers protect their AWS workloads.



# GuardDuty Findings

Findings 

Showing 67 of 67

9

47

11

Actions		Finding type	Resource	Last seen	Account	Co...
<input type="checkbox"/>	 [SAMPLE] UnauthorizedAccess:EC2/RDPBruteForce	Instance: i-99999999		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] Trojan:EC2/PhishingDomainRequest!DNS	Instance: i-99999999		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-99999999		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] Trojan:EC2/BlackholeTraffic!DNS	Instance: i-99999999		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-99999999		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] UnauthorizedAccess:EC2/TorIPCaller	Instance: i-99999999		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] UnauthorizedAccess:IAMUser/MaliciousIPCaller	AccessKey: GeneratedFindingAccess		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] Recon:EC2/Portscan	Instance: i-99999999		2 months ago	101586075...	1
<input type="checkbox"/>	 [SAMPLE] UnauthorizedAccess:EC2/MaliciousIPCaller.C...	Instance: i-99999999		2 months ago	101586075...	1

# Important Pointers

Guard Duty will only monitor the Route53 for DNS Logs.

Lot of organizations makes use of Active Directory DNS. The logs from these servers will not be monitored.

# Relax and Have a Meme Before Proceeding



---

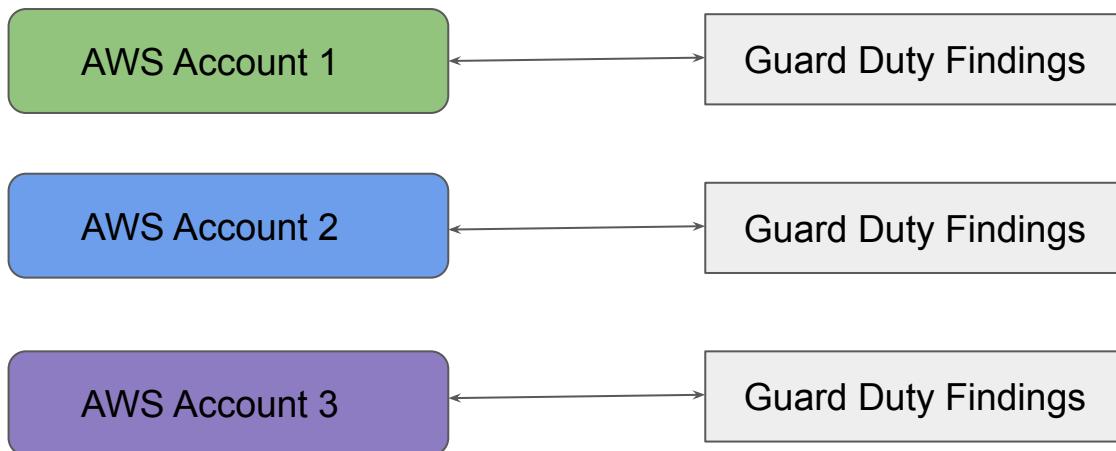
# Managing GuardDuty Findings Centrally

Multiple AWS Accounts

---

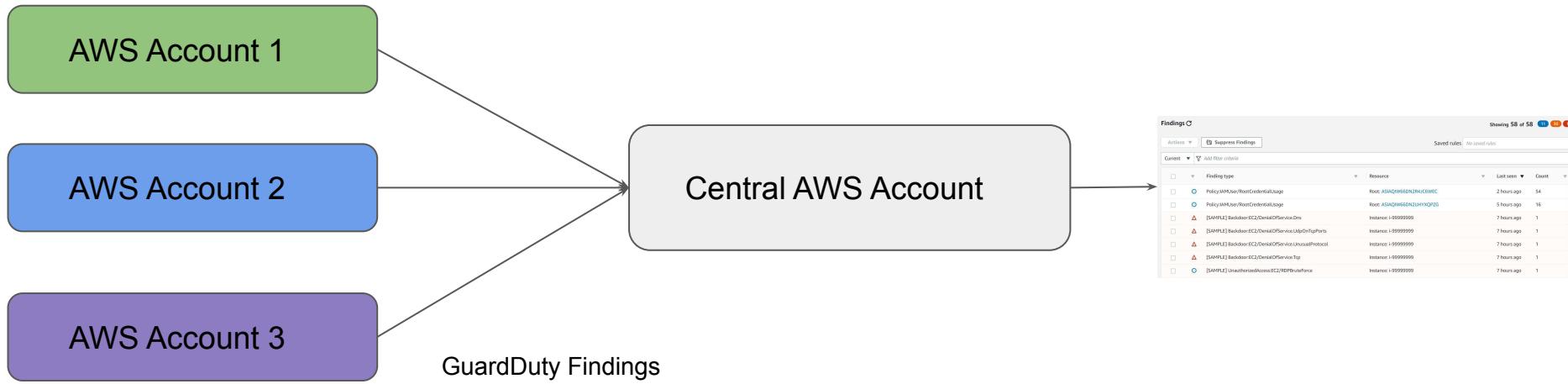
# Understanding the Challenge

- Enabling GuardDuty across all AWS account is recommended.
- Checking findings across individual account is troublesome.



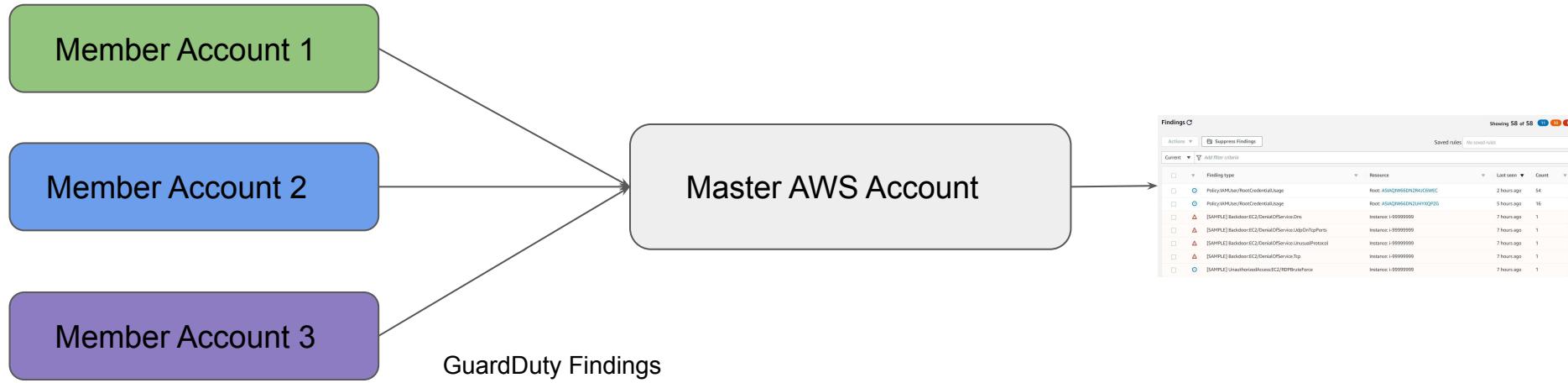
# Central Architecture

In this architecture, the Guard Duty findings from all the AWS Accounts will be sent to the Central AWS account.



# Right Terminology

In this architecture, the Guard Duty findings from all the AWS Accounts will be sent to the Central AWS account.



---

# Active Directory

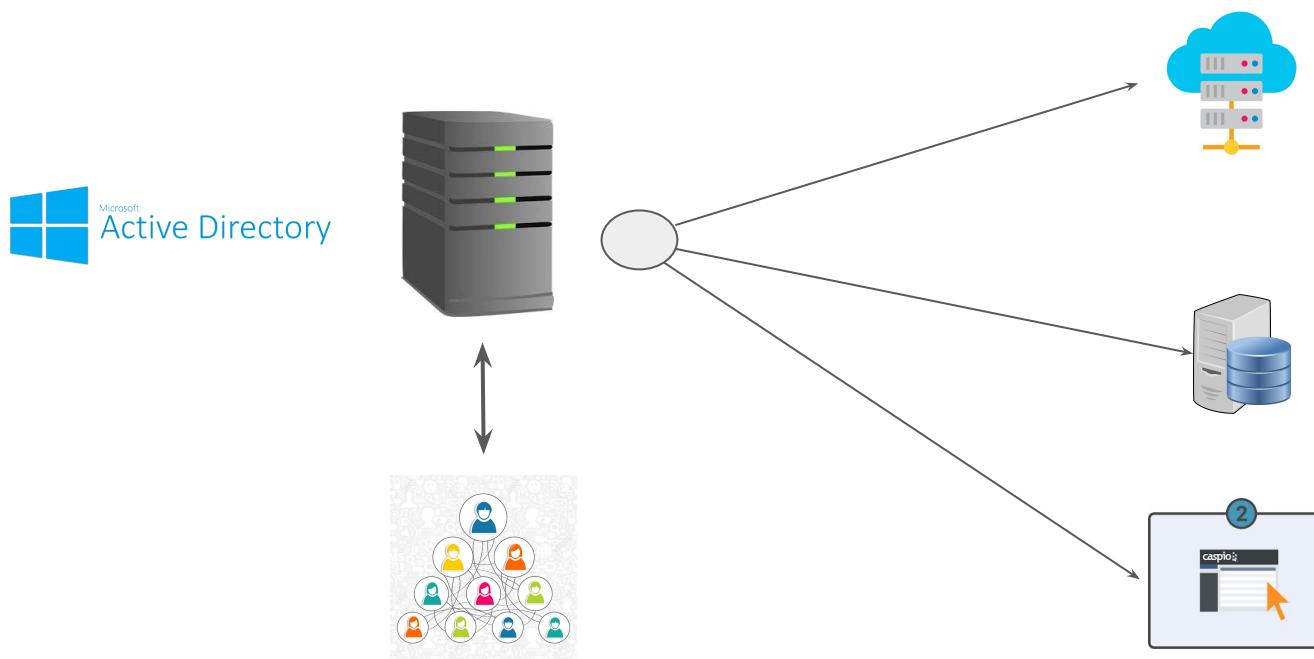
Directory Service

---

# Traditional Way



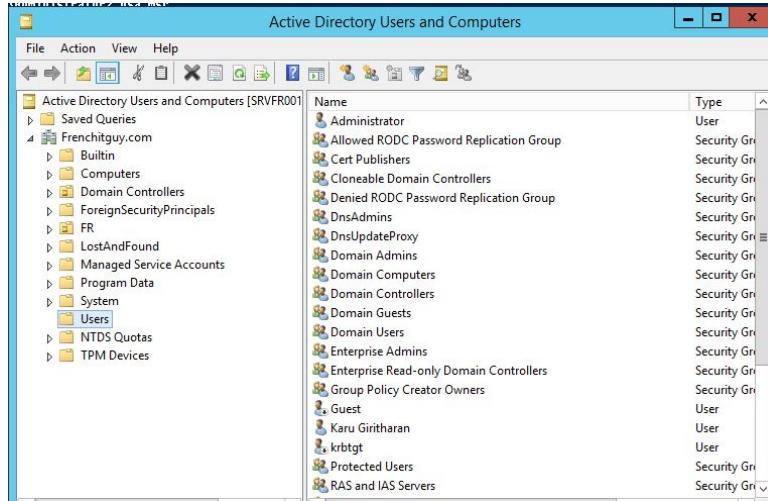
# Better Way



# Active Directory

Active Directory is one of the most popular directory service developed by Microsoft.

The server running the Active Directory service is called as the domain computer and it can authenticate and authorize the users and computers which are associated to it.



---

# AWS Directory Service

Directory on the Cloud

---

# Challenges with Active Directory

For those who have set up an AD knows, this can be a challenging and time-consuming process.

Some of the challenges involved can be:

- Provisioning the Infrastructure.
- Installing the directory software
- Getting replication setup between domain controllers for HA
- Monitoring / Patching and many more.



# Directory Service in the Cloud

AWS Directory Service is a managed service based on the cloud that allows us to create directories and let AWS experts handle and manage the other parts like high availability, monitoring, backups, recovery, and others.

There are three important components :

- Active Directory Service with Microsoft Active Directory
- Simple AD
- AD Connector

# Directory Service with Microsoft AD

AWS Directory Service for Microsoft Active Directory is powered by an actual Microsoft Windows Server Active Directory (AD) in the AWS Cloud.

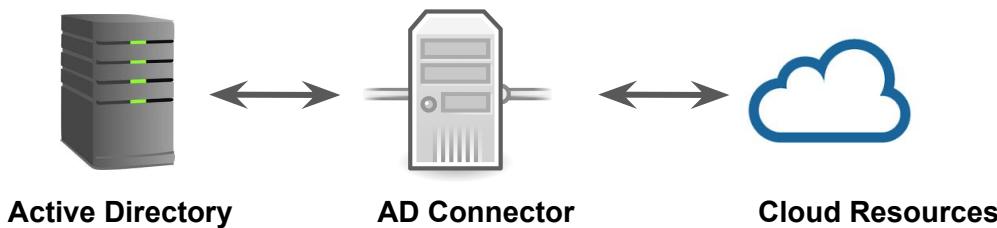
There are two types:

- Standard Edition -- For small and midsize ( up to 5000 users )
- Enterprise Edition -- For larger deployments.



# AD Connector

- It is a proxy service that provides easy way to connect applications in cloud to your existing on-premise Microsoft AD.
- When users log in to the applications, AD Connector forwards sign-in requests to your on-premises Active Directory domain controllers for authentication.



# Simple AD

- Simple AD is a Microsoft Active Directory–compatible directory from AWS Directory Service that is powered by Samba 4.
- Simple AD supports basic Active Directory features such as user accounts, group memberships, joining a Linux domain or Windows based EC2 instances, Kerberos-based SSO, and group policies. AWS provides monitoring, daily snapshots, and recovery as part of the service.
- Simple AD does not support trust relationships, DNS dynamic update, schema extensions, multi-factor authentication, communication over LDAPS, PowerShell AD cmdlets, or FSMO role transfer.

---

# Prefix Lists

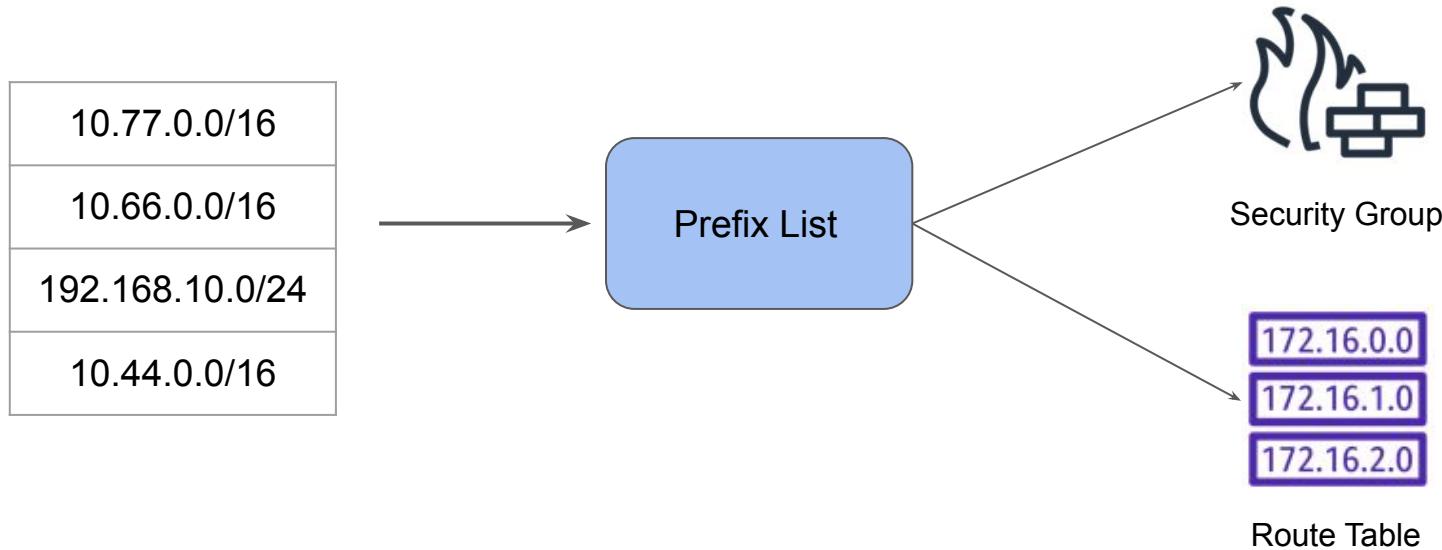
Centralizing IP Address Data

---

# Overview of Prefix Lists

A prefix list is a set of one or more CIDR blocks.

You can create a prefix list from the IP addresses that you frequently use, and reference them as a set in security group rules and routes instead of referencing them individually.



# Types of Prefix List

There are two types of prefix lists:

<b>Types of Prefix List</b>	<b>Description</b>
Customer-managed prefix lists	Sets of IP address ranges that you define and manage.
AWS-managed prefix lists	Sets of IP address ranges for AWS services.

# Important Pointers

A prefix list supports a single type of IP addressing only (IPv4 or IPv6). You cannot combine IPv4 and IPv6 CIDR blocks in a single prefix list.

A prefix list applies only to the Region where you created it.

When you reference a prefix list in a resource, the maximum number of entries for the prefix lists counts against the quota for the number of entries for the resource. For example, if you create a prefix list with 20 maximum entries and you reference that prefix list in a security group rule, this counts as 20 security group rules.

---

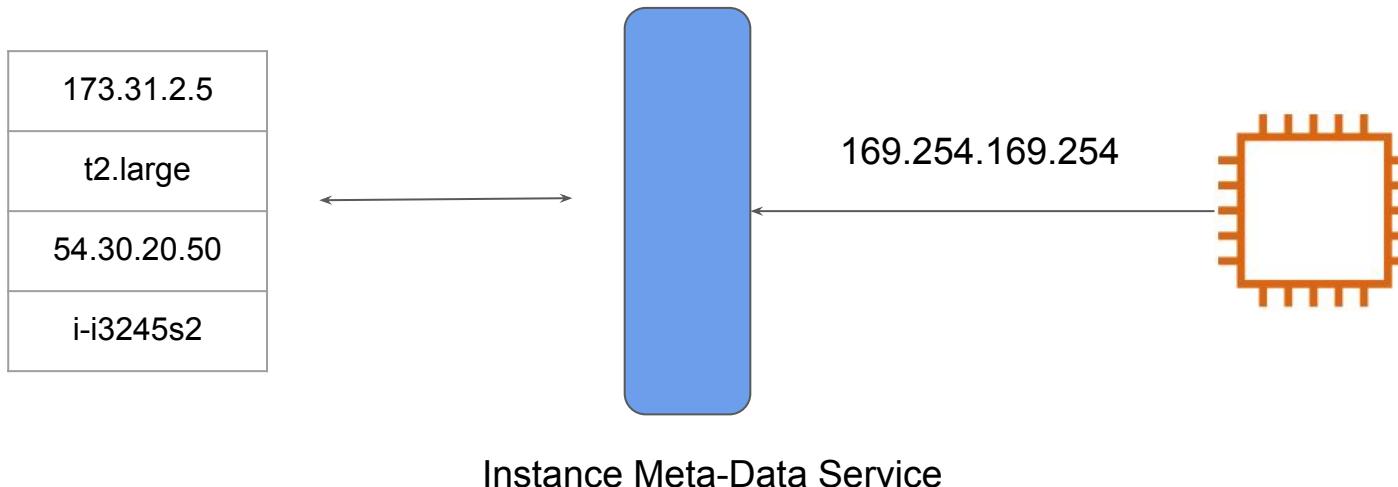
# EC2 Instance Metadata

Getting to know thy self

---

# Overview of Metadata Service

- Instance Metadata is basically data about your instance.
- This data can be accessed within the instance itself.



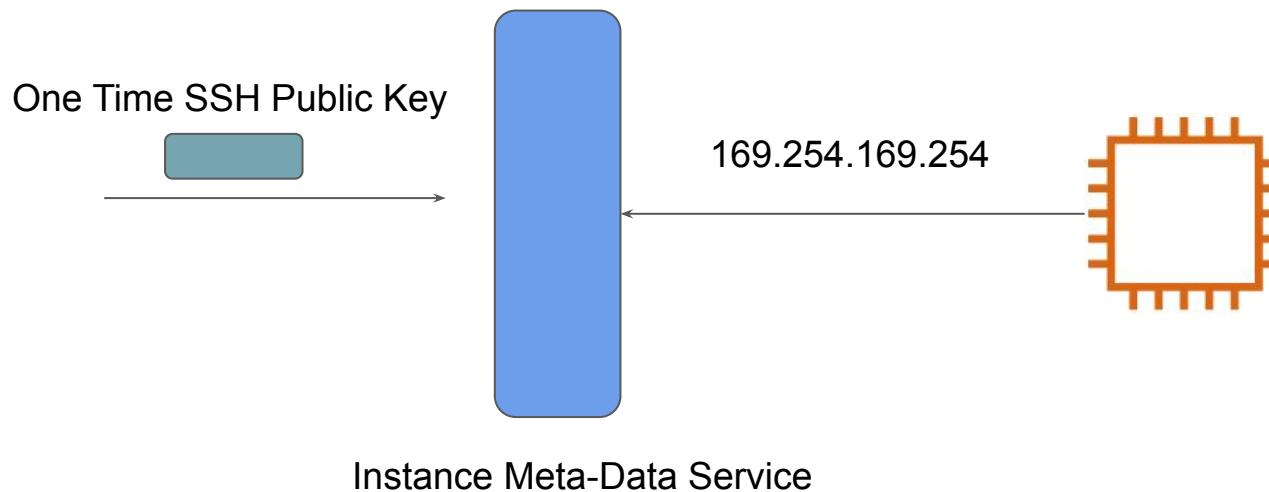
# Categories of Information

Information is divided into top level metadata items. Some of these include:

- ami-id
- hostname
- iam
- instance-type
- mac
- profile
- public-keys
- security-groups

# Data Pushed to Instance Meta-Data

AWS can push multiple things to the Instance Meta-Data that can subsequently be used by the EC2 instance.



---

# AWS KMS

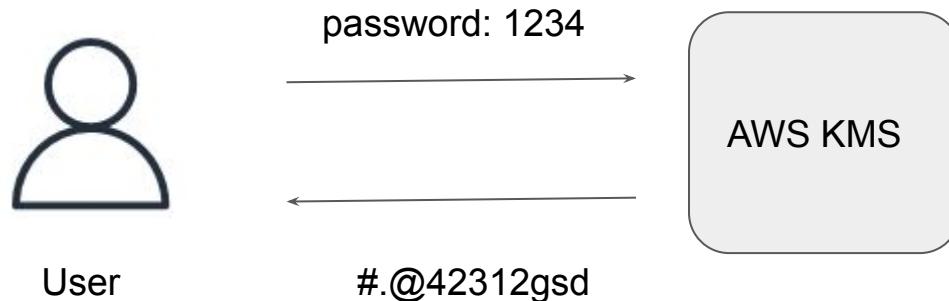
Do things the right way

---

# Basics of KMS

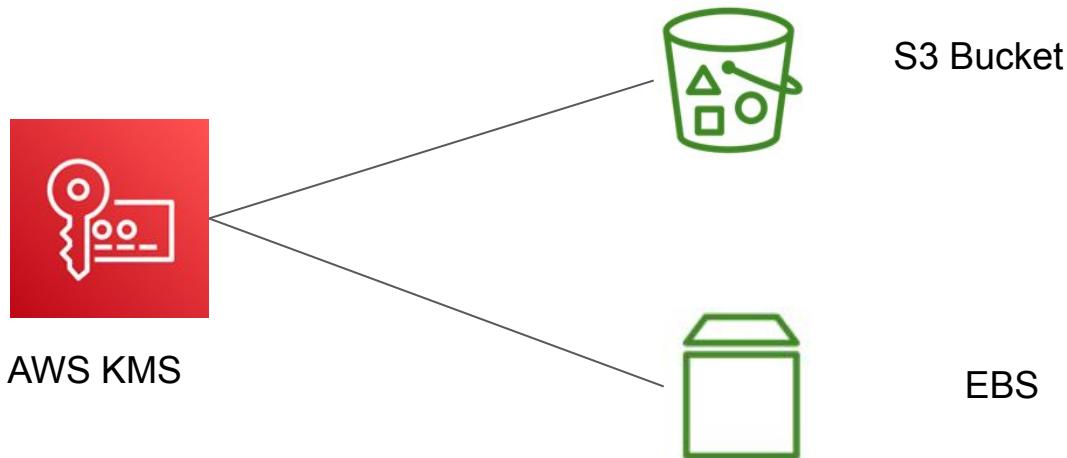
AWS KMS stands for AWS Key Management Service.

This service provides capability to encrypt and decrypt the data.



# Integration of KMS

AWS KMS also integrates with various AWS services like S3, DynamoDB, EBS and others.



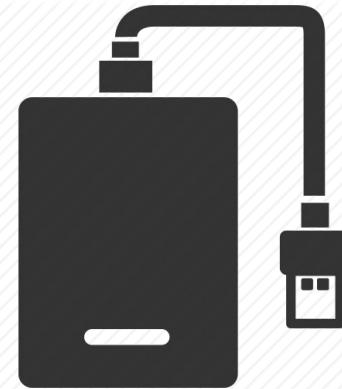
---

# S3 Encryption

S3 is Back

---

# What's the Need ?

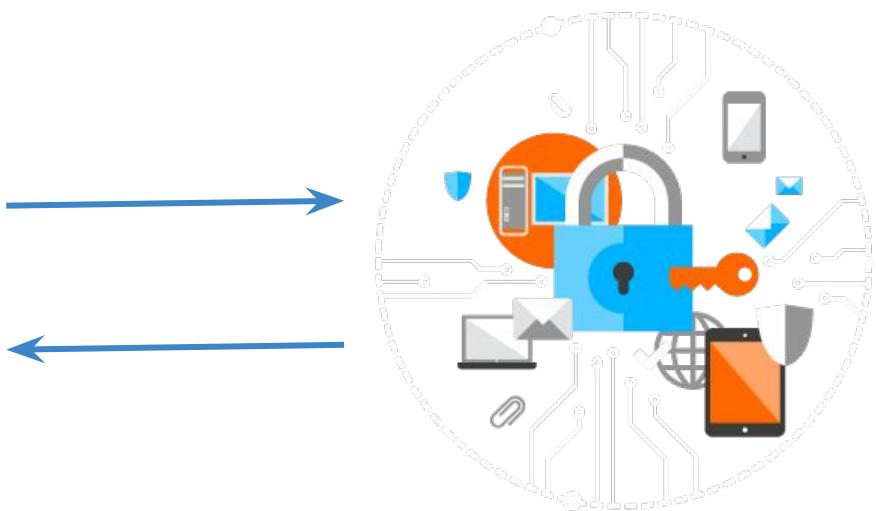


# Let's be Proactive

## Western Digital external HDs with hardware-based encryption

Aspiring to be a CISSP in 2017? Download the free planning kit!

WD introduced its new **My Book Essential** and **My Book for Mac** desktop external hard drives equipped with the new WD SmartWare software and hardware-based encryption.



# S3 also needs Encryption

AWS S3 offers multiple approaches to encrypt the data being stored in S3.

## i) Server Side Encryption

- Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.

## ii) Client Side Encryption

- Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

# Server Side Encryption

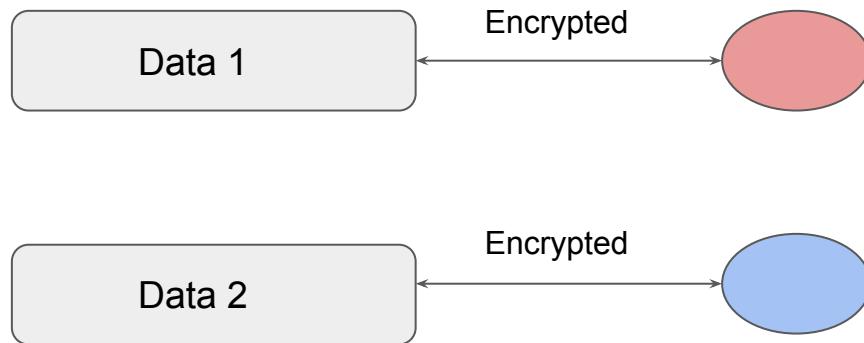
Within Server-Side encryption, there are three options that can be used depending on the use-case.

- Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)
- Server-Side Encryption with Customer-Provided Keys (SSE-C)

# SSE with Amazon S3-Managed Keys (SSE-S3)

## i) Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

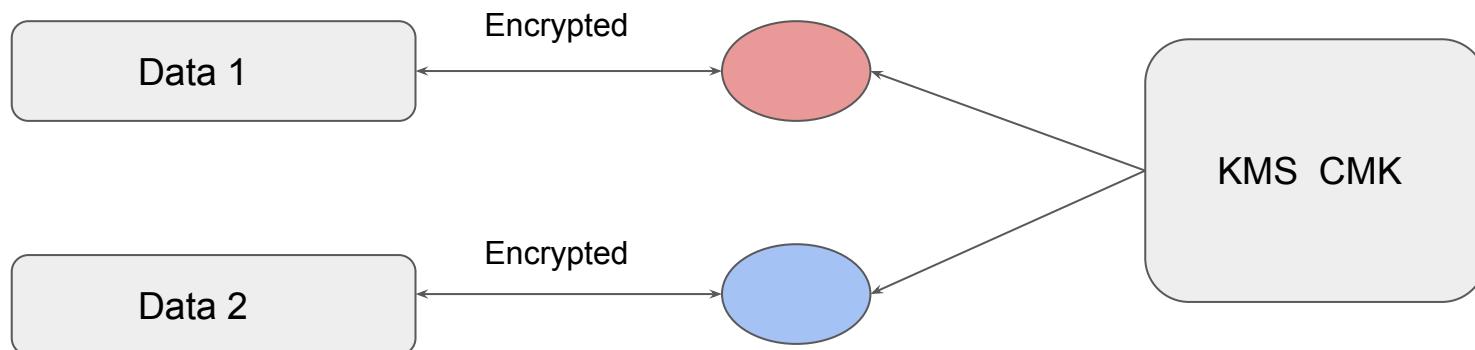
- In this approach, each object is encrypted with a unique key.
- Uses one of the strongest block ciphers to encrypt the data, AES 256.



# SSE with CMK (SSE-KMS)

## ii) Server-Side Encryption with CMKs Stored in AWS Key Management Service (SSE-KMS)

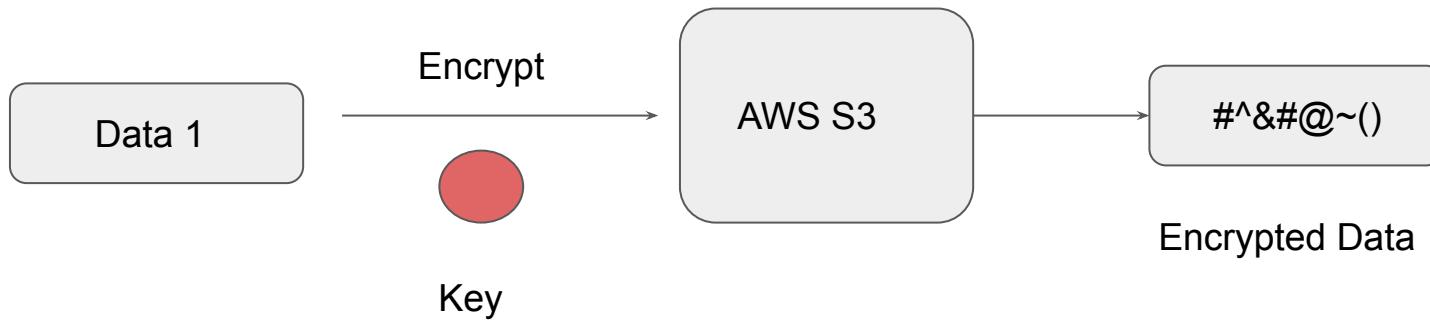
Encrypting data with own CMK allows customers to create, rotate, disable customer managed CMK's. We can also define access controls and enable auditing.



# SSE with Customer-Provided Keys (SSE-C)

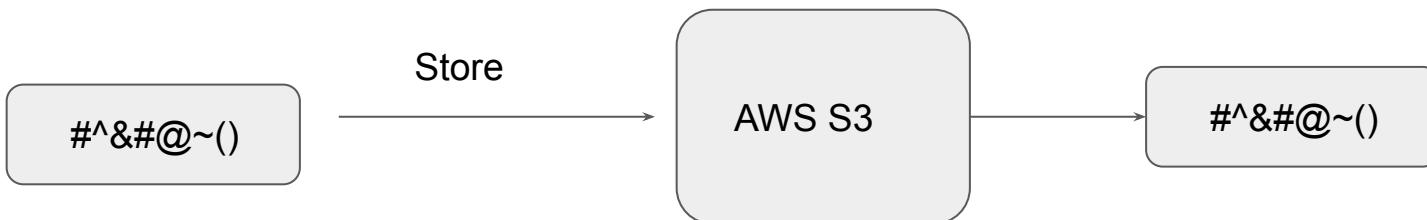
Allows customers to set their own encryption keys.

Encryption key needs to be provided as part of the request and S3 will manage both the encryption as well as the decryption options.



# Client Side Encryption

Client-side encryption is the act of encrypting data before sending it to Amazon S3.



# Relax and Have a Meme Before Proceeding

me: i'll do it at 6

time: 6:05

me: wow looks like i gotta wait til 7 now



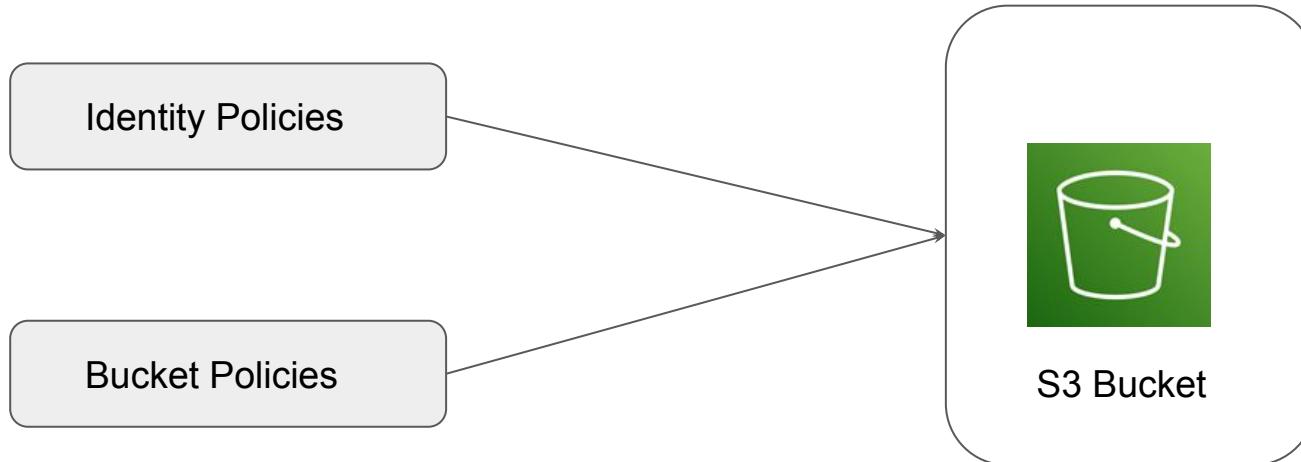
---

# S3 Bucket Policy

## Bucket Policies

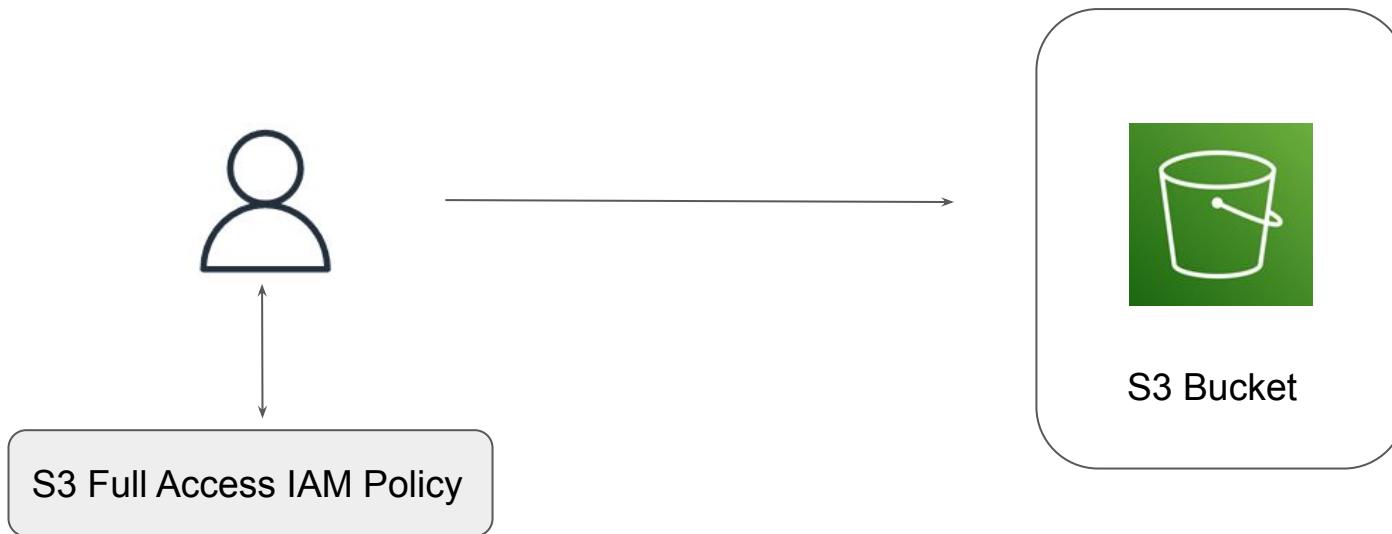
# Granting Permission for S3 Resource

There are two primary ways in which a permission to a S3 resource is granted.



# Use-Case 1: IAM User Needs Access to S3 Bucket

IAM User Named Bob needs Full Access to S3 Bucket.



# Wider Scope of S3 Bucket

Files within the S3 bucket can have scope beyond the IAM entity.

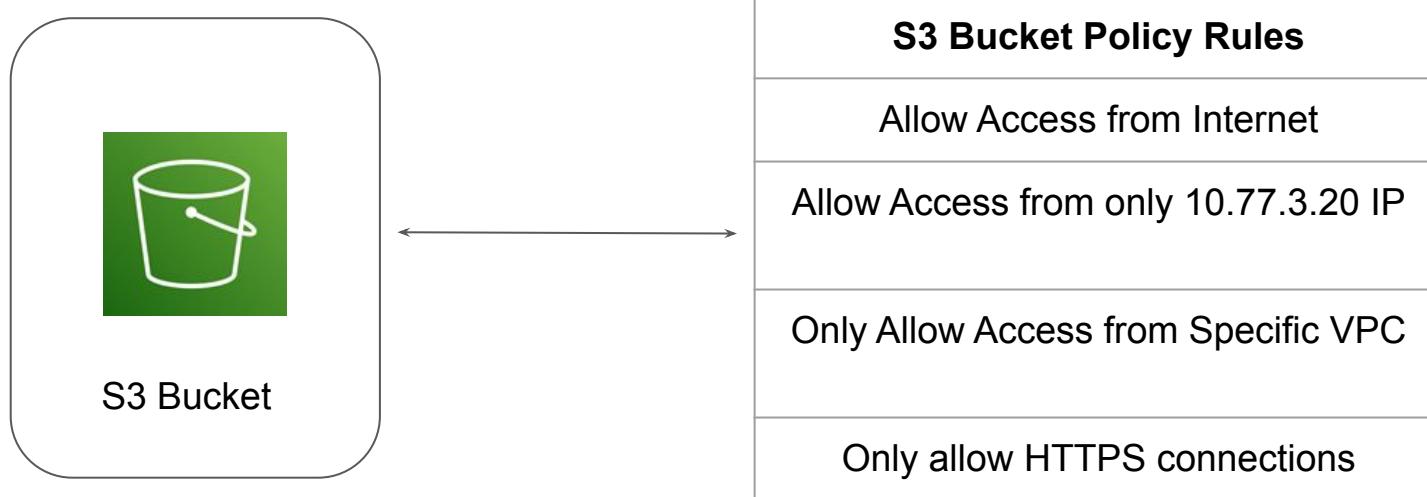
Organization can host entire websites in S3 Bucket.

S3 Buckets can even be used to host central files for download.



# S3 Bucket Policy

A bucket policy is a resource-based AWS IAM policy associated with the S3 Bucket to control access permissions for the bucket and the objects in it .



# Bucket Policy 1 - Public Access

The following example policy grants the s3:GetObject permission to any public anonymous users.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PublicRead",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": ["s3:GetObject"],  
            "Resource": ["arn:aws:s3:::demo-bucket/*"]  
        }  
    ]  
}
```

# Bucket Policy 2 - Only HTTPS

Only the HTTPS requests should be allowed. All HTTP requests should be blocked.

```
{  
    "Id": "ExamplePolicy",  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowSSLRequests",  
            "Action": "s3:GetObject",  
            "Effect": "Allow",  
            "Resource": [  
                "arn:aws:s3:::demo-bucket/*"  
            ],  
            "Condition": {  
                "Bool": {  
                    "aws:SecureTransport": "true"  
                }  
            },  
            "Principal": "*"  
        }  
    ]  
}
```

---

# Regaining Access to Locked S3 Bucket

Cloud Storage is Saviour

---

# Lockout of S3 Bucket

With a S3 Bucket policy that is configured incorrectly, all the IAM users can be locked out.

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is selected. Below the tabs, there's a section titled 'Objects' with a sub-instruction: 'Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)'.

Below this are several action buttons: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and Upload. There's also a search bar labeled 'Find objects by prefix' and a 'Show versions' toggle. At the bottom, there's a table header with columns: Name, Type, Last modified, Size, and Storage class.

A prominent error message box is displayed at the bottom left, containing a red circular icon with a white 'X', the text 'Insufficient permissions to list objects', and a explanatory note: 'After you or your AWS administrator have updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about [Identity and access management in Amazon S3](#)'.

# Bucket Policy - Restriction by IP

Only allow request from a specific IP Address.

```
{  
    "Version": "2012-10-17",  
    "Id": "S3PolicyId1",  
    "Statement": [  
        {  
            "Sid": "IPAllow",  
            "Effect": "Deny",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::demo-bucket",  
                "arn:aws:s3:::demo-bucket/*"  
            ],  
            "Condition": {"  
                "NotIpAddress": {"aws:SourceIp": "54.240.143.0/24"}  
            }  
        }  
    ]  
}
```

# Important Note

Wrong set of S3 Bucket policy will lead to you being locked out of S3 bucket.

In order to regain the control of S3 bucket, login with ROOT user and delete the Bucket Policy.

---

Trusted Advisor

Recommendations are always good

---

# What is Trusted Advisor ?

AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five major categories:

Cost Optimization



6 ✓ 3 ▲ 0 !

\$10.63

Potential monthly savings

Performance



10 ✓ 0 ▲

0 !

Security



11 ✓ 1 ▲

5 !

Fault Tolerance



13 ✓ 2 ▲

2 !

Service Limits



48 ✓ 0 ▲

0 !

# Trusted Advisor Check Categories

Categories	Description
Cost optimization	Recommendations that can potentially save you money.
Performance	Recommendations that can improve the speed and responsiveness of your applications.
Security	Recommendations for security settings that can make your AWS solution more secure.
Fault tolerance	Recommendations that help increase the resiliency of your AWS solution.
Service limits	Checks the usage for your account and whether your account approaches or exceeds the limit for AWS services and resources.

---

# Federation

Connecting Identities

---

# Understanding the Challenge

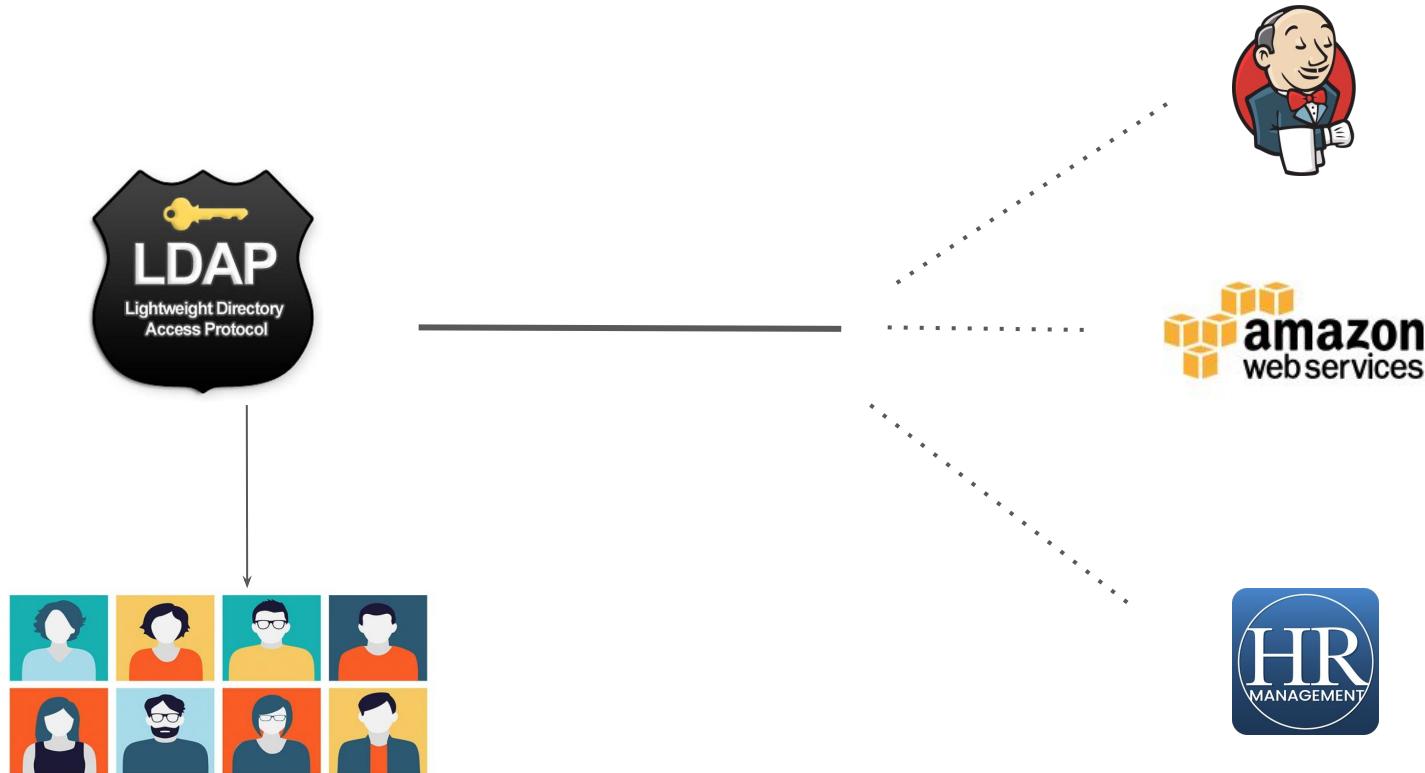
Let's assume there are 500 users within an organization. Your organization are using 3 services :-

- AWS ( Infrastructure )
- Jenkins ( CI / CD )
- HR Activator ( Payroll )



You have been assigned role to give users access to all 3 services.

# Storing Users Centrally



Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [pdc.e]

Saved Queries

enterprise.com

- Builtin
- CEO
- Computers
- Contractors
- Disabled Computers
- Disabled Users
- Districts
- Domain Controllers
- ForeignSecurityPrincipals
- Groups
- Inactive Users
- LostAndFound
- Managed Service Accounts
- Managers
- Microsoft Exchange Security Groups
- Production
- Program Data
- System
- TestOU
- Users
- Microsoft Exchange System Objects
- NTDS Quotas
- TPM Devices

Name Type Description

Ian Scur	User	
Cain Decker	User	
Elena Anderson	User	
Bill Jackson	User	Moved from: CN=Bill Jackson,OU=
Phill Jefferson	User	Moved from: CN=Phill Jefferson,OU=

Delegate Control...  
Move...  
Find...

New Computer  
All Tasks Contact  
Refresh Group  
Export List... InetOrgPerson  
View msExchDynamicDistributionList  
Arrange Icons msImaging-PSPs  
Line up Icons MSMQ Queue Alias  
Properties Organizational Unit  
Printer  
Help User  
Shared Folder

Create a new object...

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. The left pane displays a tree view of the directory structure under 'enterprise.com'. The right pane lists several users with their details: Name, Type, and a note indicating they were moved from other locations. A context menu is open over the user list, with the 'New' option selected. A secondary dropdown menu shows various object types: Computer, Contact, Group, InetOrgPerson, msExchDynamicDistributionList, msImaging-PSPs, MSMQ Queue Alias, Organizational Unit, Printer, User, and Shared Folder. The 'User' option is also highlighted in this secondary menu. At the bottom of the main pane, there is a text input field for 'Create a new object...'.

# Central Users

There are various solutions available which can store users centrally :-

- Microsoft Active Directory
- RedHat Identity Management / freeIPA



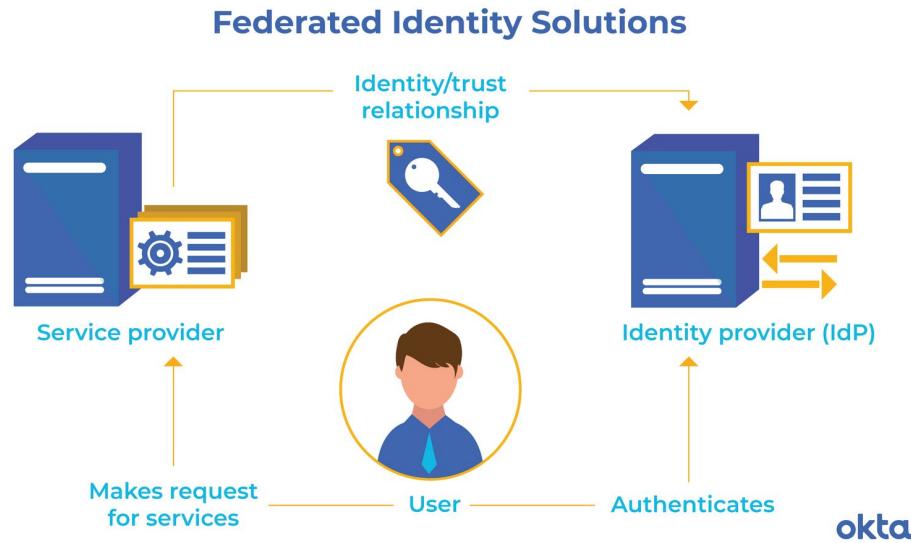
# Basics of Federation - AWS Perspective

Federation allows external identities ( Federated Users ) to have secure access in your AWS account without having to create any IAM users.

These external identities can come from :-

- Corporate Identity Provider ( AD, IPA )
- Web Identity Provider ( Facebook, Google, Amazon, Cognito or OpenID )

# Basic Workflow



# Understanding Identity Broker

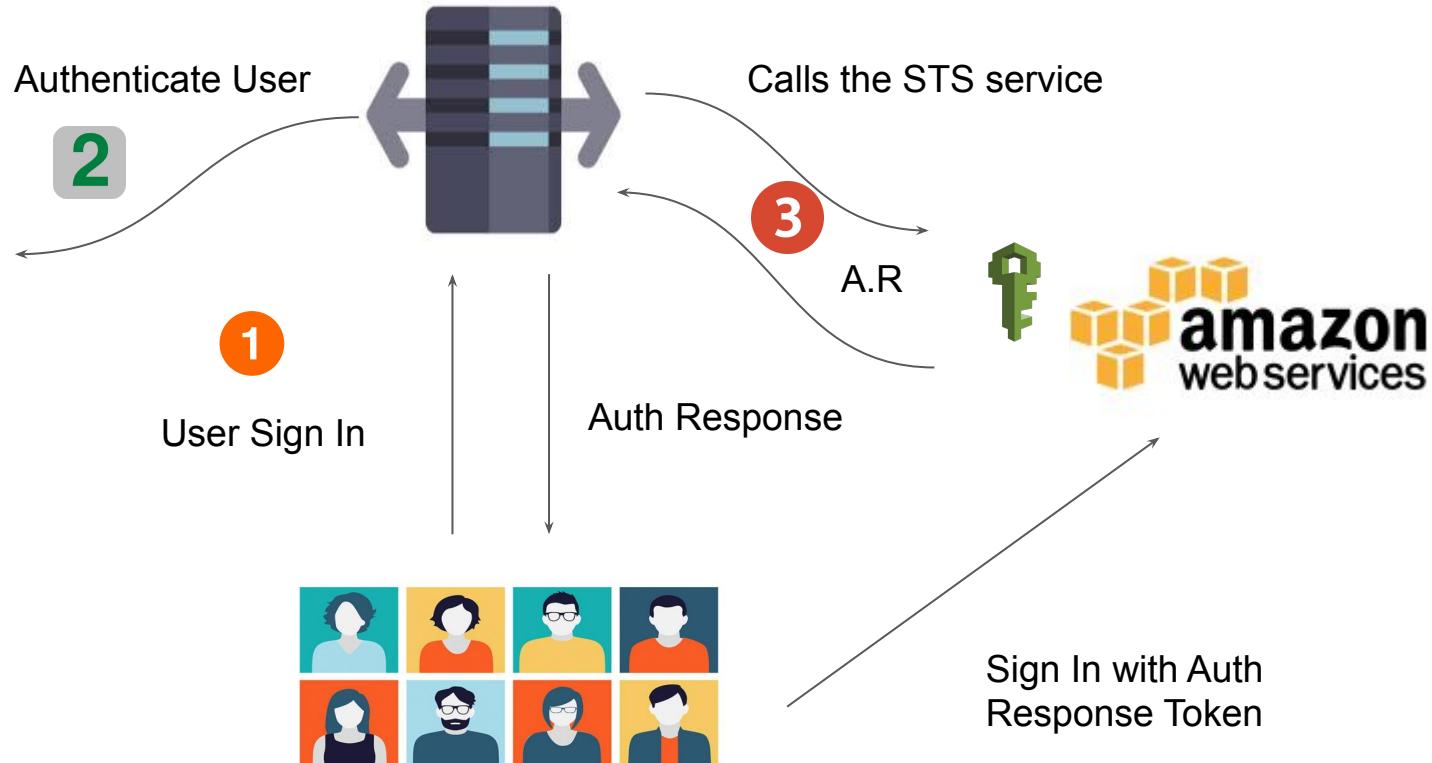
Identity Broker :-

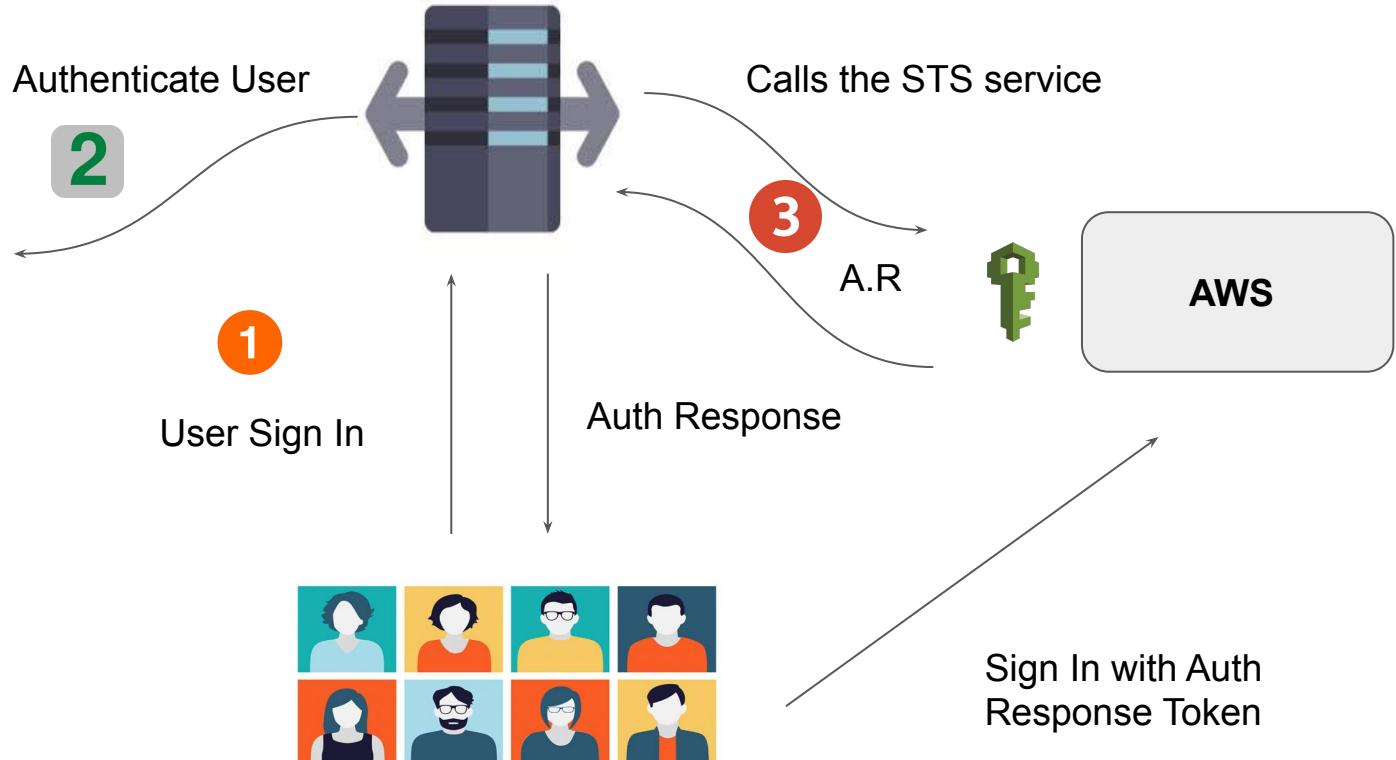
It is an intermediate service which connects multiple providers.

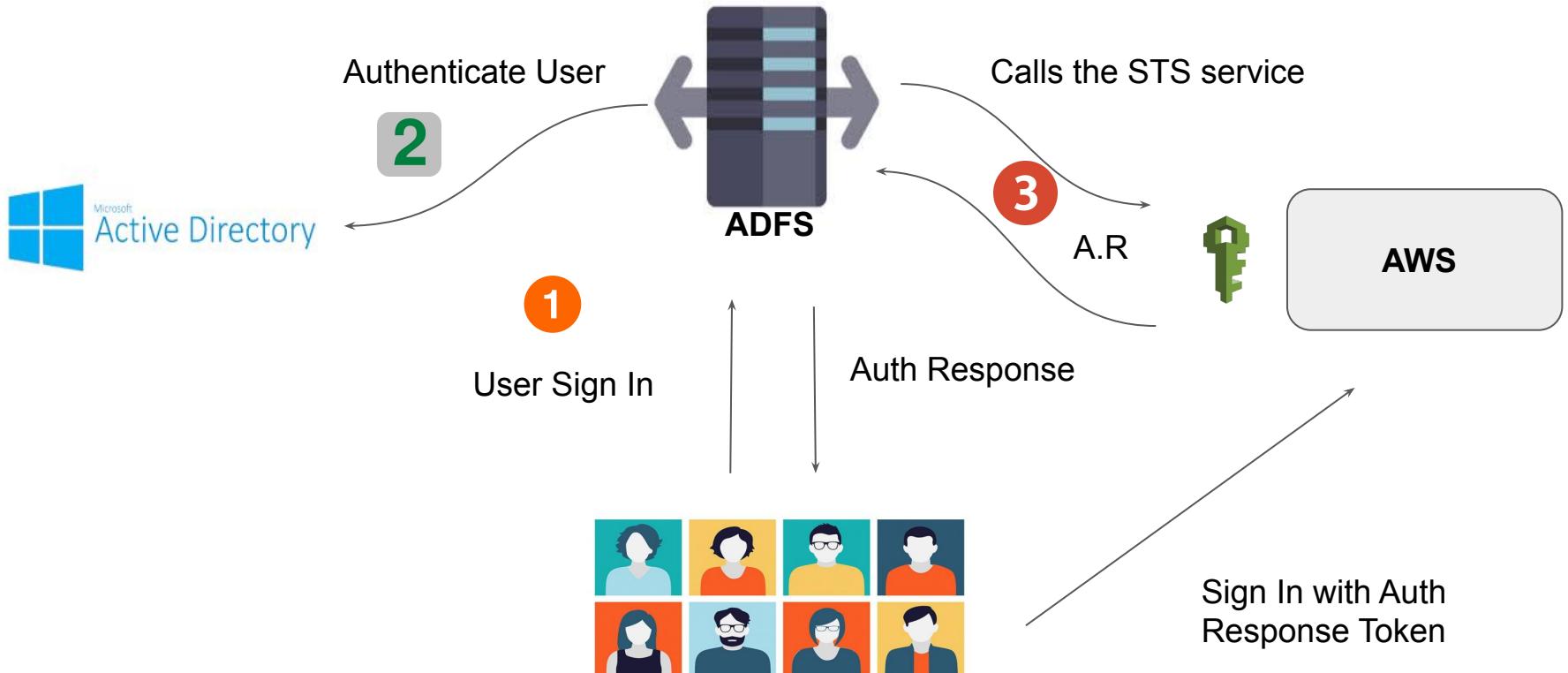




Microsoft  
Active Directory







## Steps to Remember

- User logs in with username & Password.
- This credentials are given to the Identity Broker.
- Identity Broker validates it against the AD.
- If credentials are valid, Broker will contact the STS token service.
- STS will share the following 4 things :-

Access Key + Secret Key + Token + Duration

- User can now use to login to AWS Console or CLI.

# Notations to Remember

**Identities** : Users

**Identity Broker** :

- It is a middleware that takes the users from point A & help connect them to point B.

**Identity Store** :-

- Place where users are present. Eg : AD, IPA, Facebook etc.

# Relax and Have a Meme Before Proceeding



Cole  
@its\_cmillz6

when you're sleeping and your alarm  
didn't ring yet but the amount of  
sleep you're getting is suspicious



---

# SAML

## Single Sign On

---

# Introduction to SAML

- SAML stands for Security Assertion Markup Language.
- It is a secure XML based communication mechanism for communicating identities across organizations.
- SAML eliminates the need to maintain multiple authentication credentials, such as passwords in multiple locations.

# Classic Way



# Challenges with classic way

- The administrator does not have direct visibility with the underlying database of the SAAS provider.
- If there are multiple SAAS providers, it is difficult to keep track of which user has access to which SAAS application.
- When the user leaves the organization, he needs to be removed from all the entities (Jenkins, AWS, HR app)

# Different Views

## Administrator's View

Have to login to different providers to manage and control the permissions of an individual user across the organization.

User forgetting username and passwords, MFA :(

## User's View

I have to remember passwords of all the applications in the organization.

It might be possible that even userID across apps is different, so have to remember that as well.

## SAAS Provider's View

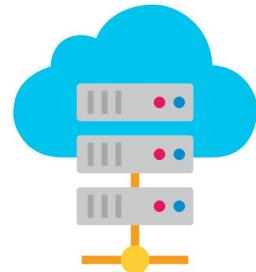
Have to maintain the user and password database of customers.

This is a big security liability.

# SAML



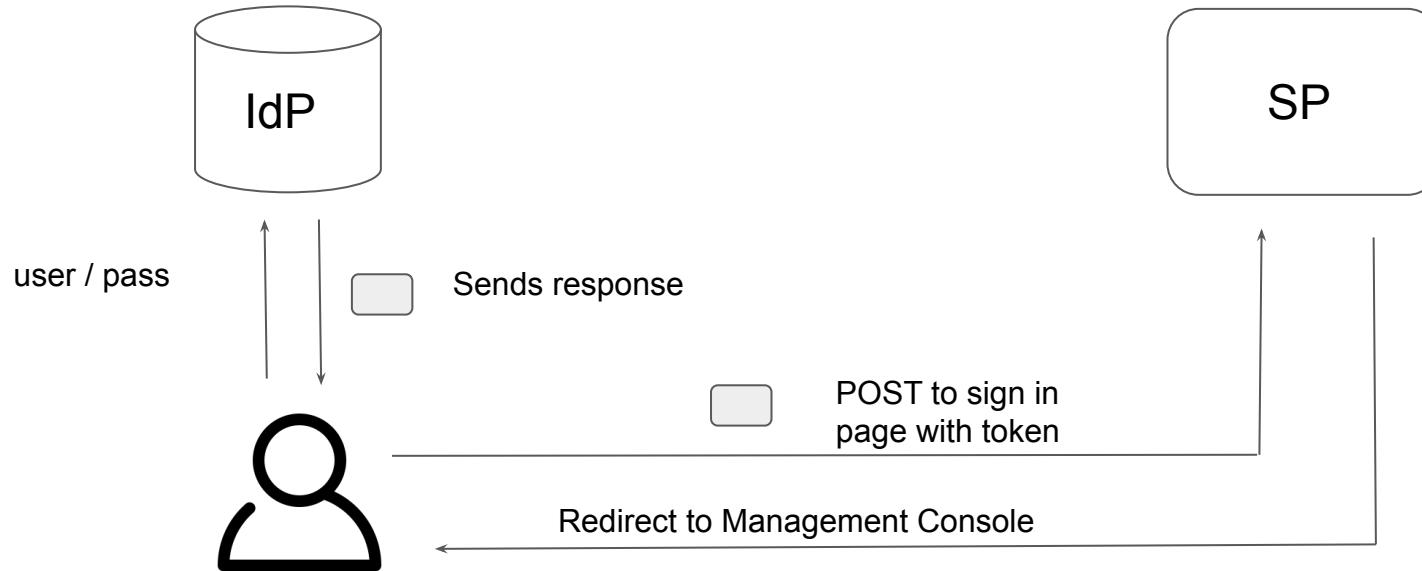
Identity Provider



Service Provider



# The SAML Way



# Introduction to SAML

- The flow gets initiated when user opens the IdP URL and enters the username and password and selects the appropriate application.
- IdP will validate the credentials and associated permissions and then user receives SAML assertion from the IdP as part of response.
- User does a POST of that SAML assertion to the SAAS sign in page and SP will validate those assertion.
- On validation, SP will construct relevant temporary credentials, and constructs sign in URL for the console and sends to the user.

---

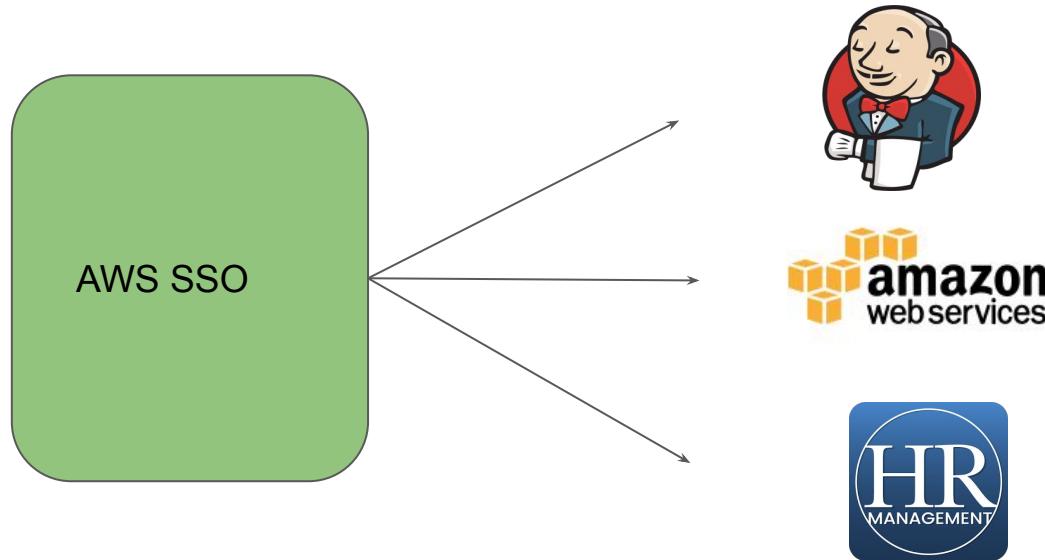
# AWS Single-Sign-On

## Centralized Architecture



# Overview of AWS SSO

AWS Single Sign-On (SSO) makes it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place.



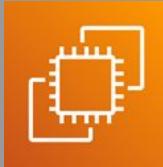
# SSO with AWS CLI

AWS CLI integrates with the SSO.

SSO users can authenticate via CLI, and they will be able to perform the CLI operations without having to add keys in their `~/.aws/credentials` file.

```
bash-4.2# aws sso login --profile Production-Account
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize this request, open the following URL:
https://device.sso.ap-southeast-1.amazonaws.com/
Then enter the code:
```

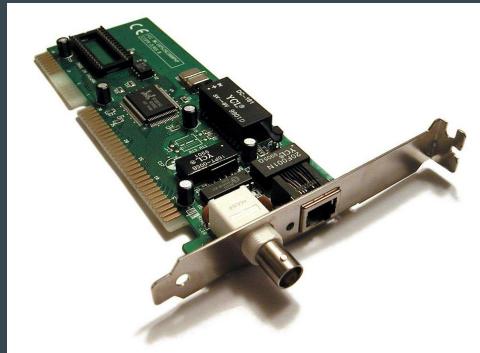
# Elastic Network Interface (ENI)



# Revising Basics of Network Interface

Network interface is a hardware component that connects a computer to a computer network

A virtual network interface (VIF) is an abstract virtualized representation of a computer network interface.



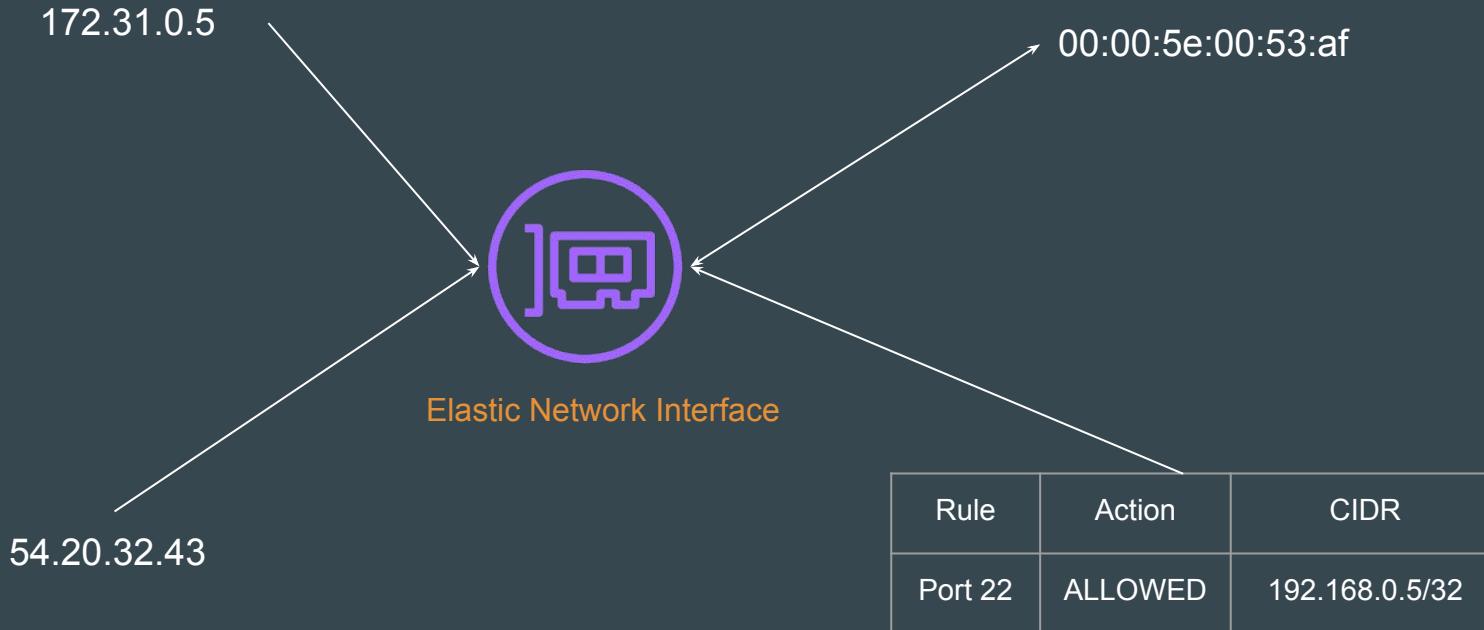
# Elastic network interfaces

An **elastic network interface** is a logical networking component in a VPC that represents a virtual network card.

Some of the following attributes include:

- A primary private IPv4 address
- One or more secondary private IPv4 addresses
- One Elastic IP address (IPv4) per private IPv4 address
- One or more security groups
- A MAC address
- A source/destination check flag

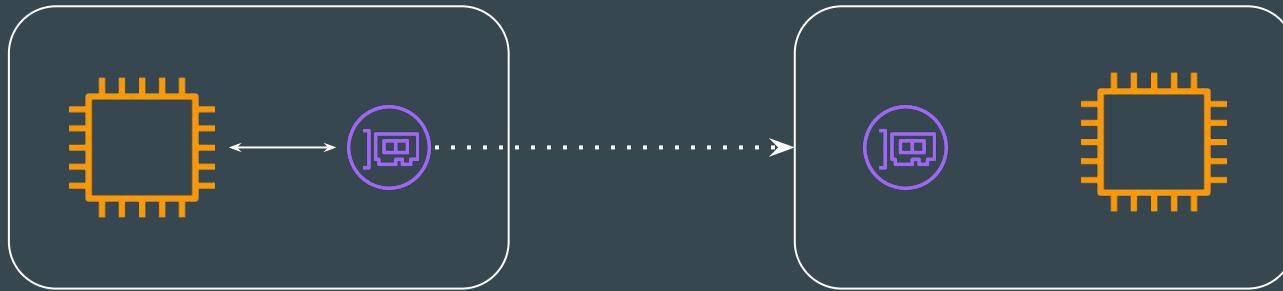
# Sample Attributes of ENI



# Portable NICs

You can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.

The **attributes of a network interface follow it as it's attached or detached from an instance and reattached to another instance.**



172.31.0.5

172.31.0.5

# Importance of Default NICs

Each instance has a **default network interface**, called the primary network interface. You cannot detach a primary network interface from an instance.

You can create and attach additional network interfaces.

The maximum number of network interfaces that you can use varies by instance type.

NICs are availability zone specific.

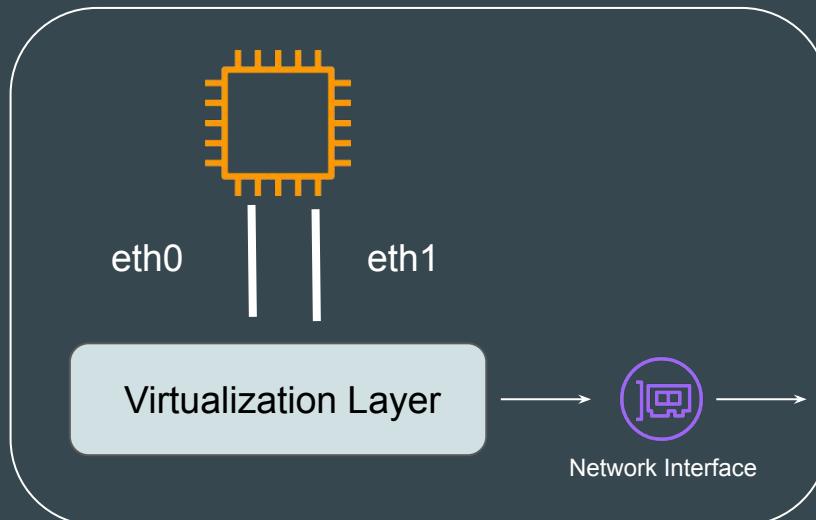
# Enhanced Networking



# Understanding the Basics

Every network interface card has a specific bandwidth.

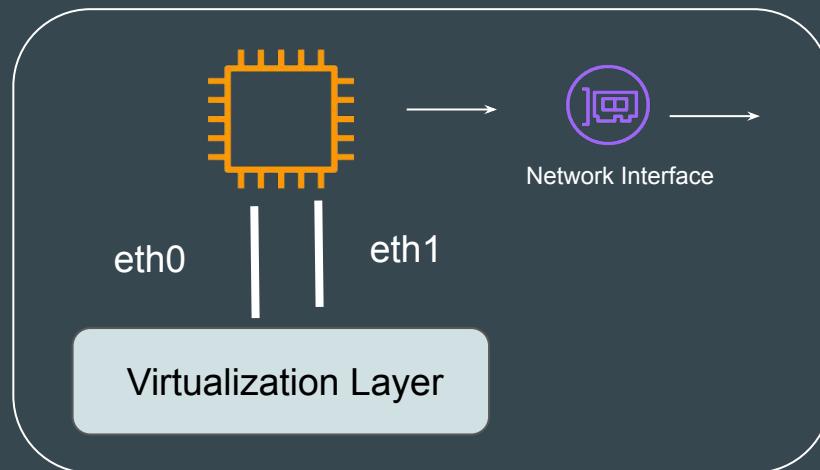
The networking bandwidth in-turn gets affected when we virtualization layer comes into picture.



# Basics of Enhanced Networking

Enhanced Networking uses single root I/O virtualization technique (SR-IOV) to provide high performance networking capabilities on supported instance types.

SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces.



# Mechanism to Enable Enhanced Networking

All current generation instance types support enhanced networking, except for T2 instances.

You can enable enhanced networking using one of the following mechanisms:

Approach	Description
Elastic Network Adapter (ENA)	Supports network speeds of up to 100 Gbps for supported instance types.
Intel 82599 Virtual Function (VF) interface (ixgbevf driver)	Supports network speeds of up to 10 Gbps for supported instance types.

# Instance and Supported Mechanism

Depending on the instance type, the supported mechanism to enable Enhanced Networking changes.

Instance type	EBS only	NVMe EBS	Instance store	Placement group	Enhanced networking
C4	Yes	No	No	Yes	Intel 82599 VF
C5	Yes	Yes	No	Yes	ENA
C5a	Yes	Yes	No	Yes	ENA
C5ad	No	Yes	NVMe *	Yes	ENA
C5d	No	Yes	NVMe *	Yes	ENA
C5n	Yes	Yes	No	Yes	ENA
C6a	Yes	Yes	No	Yes	ENA
C6g	Yes	Yes	No	Yes	ENA
C6gd	No	Yes	NVMe *	Yes	ENA
C6gn	Yes	Yes	No	Yes	ENA
C6i	Yes	Yes	No	Yes	ENA

# Verify if Module is Used in a Interface

ethtool -i eth0

```
[ec2-user@ip-172-31-19-108 ~]$ ethtool -i eth0
driver: ixgbevf
version: 5.10.157-139.675.amzn2.x86_64
firmware-version:
expansion-rom-version:
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: yes
```

Intel VF

```
[ec2-user@ip-172-31-40-246 ~]$ ethtool -i eth0
driver: ena
version: 2.8.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: yes
```

ENA

# EC2 Instance Network Bandwidth

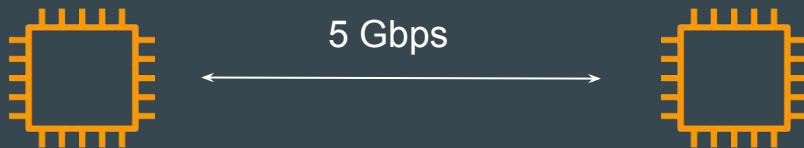


# Basics of Network Flow

Bandwidth for **single-flow** (5-tuple) traffic is limited to 5 Gbps when instances are not in the same cluster placement group

A 5-tuple uniquely identifies a UDP/TCP session

(SRC IP, SRC PORT, DST IP, DST PORT, PROTOCOL)



# Multi-Flow Traffic

We can increase the overall bandwidth if we have multi-flow traffic instead of single flow.



# Important Points - Multi-Flow

Bandwidth for aggregate multi-flow traffic available to an instance depends on the **destination of the traffic**.

Multi-Flow Traffic Destination	Description
Within the Region	Traffic can utilize the full network bandwidth available to the instance.
To other Regions, an internet gateway, Direct Connect, or local gateways (LGW)	Traffic can utilize up to 50% of the network bandwidth available to a current generation instance with a minimum of 32 vCPUs.  Bandwidth for a current generation instance with less than 32 vCPUs is limited to 5 Gbps.

# Available instance bandwidth

The available network bandwidth of an instance depends on the number of vCPUs that it has.

Instance type	Network performance
T2	Up to 1 Gbps
T3   T3a   T4g	Up to 5 Gbps †
m4.large	Moderate
m4.xlarge   m4.2xlarge   m4.4xlarge	High
m5.4xlarge and smaller   m5a.8xlarge and smaller   m5ad.8xlarge and smaller   m5d.4xlarge and smaller   m6g.4xlarge and smaller   m6gd.4xlarge and smaller	Up to 10 Gbps †
m4.10xlarge	10 Gbps
m5.8xlarge   m5a.12xlarge   m5ad.12xlarge   m5d.8xlarge   m5d.12xlarge   mac1.metal	10 Gbps
m5.12xlarge   m5a.16xlarge   m5ad.16xlarge   m6g.8xlarge   m6gd.8xlarge	12 Gbps
m6a.4xlarge and smaller   m6i.4xlarge and smaller   m6id.4xlarge and smaller	Up to 12.5 Gbps †

# Example

m5.16xlarge instance has 64 vCPUs and 20 Gbps network bandwidth

1. Traffic to another instance in the Region can utilize the full bandwidth available (20 Gbps)
2. Traffic to another instance in a different Region can utilize only 50% of the bandwidth available (10 Gbps).

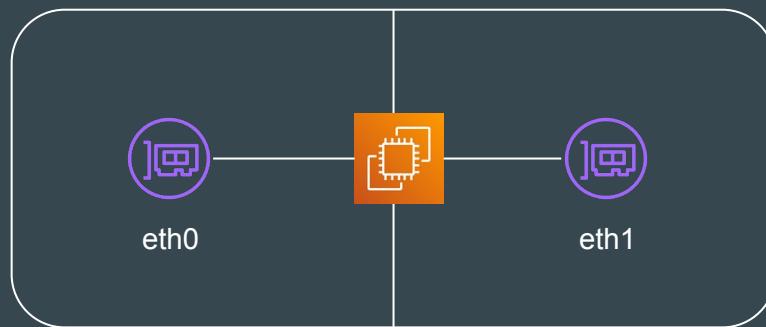
# Management Network



# EC2 Instance with Multiple NICs

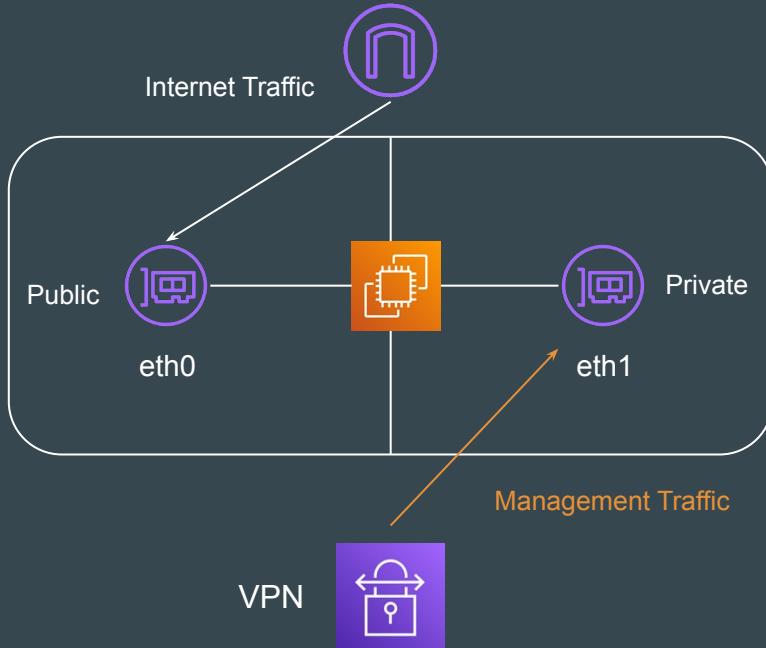
In generic scenario, for most of the organization, you have single NIC card attached to EC2 instance (eth0) and it is used both for public traffic as well as private traffic (via VPN)

An EC2 instance can have **multiple NIC cards** associated with them.



# Management Network

Management network means that one interface is dedicated for public traffic and second interface should be used for employees / management.



# Overall Architecture

The primary network interface on the instance (eth0) handles public traffic.

The secondary network interface on the instance (eth1) **handles backend management traffic**. It's connected to a separate subnet that has more restrictive access controls, and is located within the same Availability Zone (AZ) as the primary network interface.

---

# Quality of Service

## Networking Aspect

# Let's Begin

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies.

Let's understand this with an example:

- There are three people in the room who are sharing a Internet connection. The speed of Internet is 10 mbps. Person A is doing live gaming and hence utilizing most of the bandwidth. At the same time, person B has got a skype interview.

With QoS, it is possible to prioritize the network traffic where Skype traffic gets 1st priority and others traffic have secondary priority.

# QoS and AWS

Quality of Service (QoS) is not directly supported in AWS.

In AWS, there are chances that neighboring VM's can impact your network and CPU performance.

There are certain ways to mitigate this:

- You can run instance on your own dedicated hardware to avoid being affected by noisy neighbors.
- <https://aws.amazon.com/blogs/aws/new-amazon-ec2-bare-metal-instances-with-direct-access-to-hardware/>

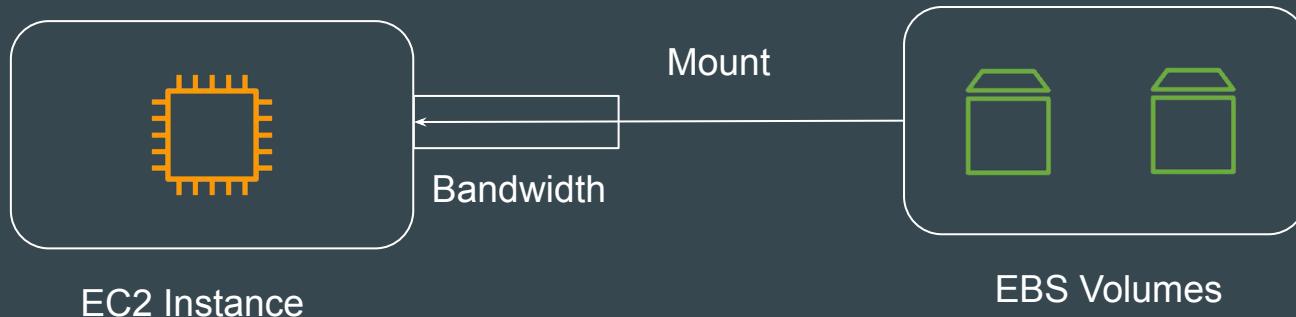
# EBS Optimized Instances



# Understanding the Basics

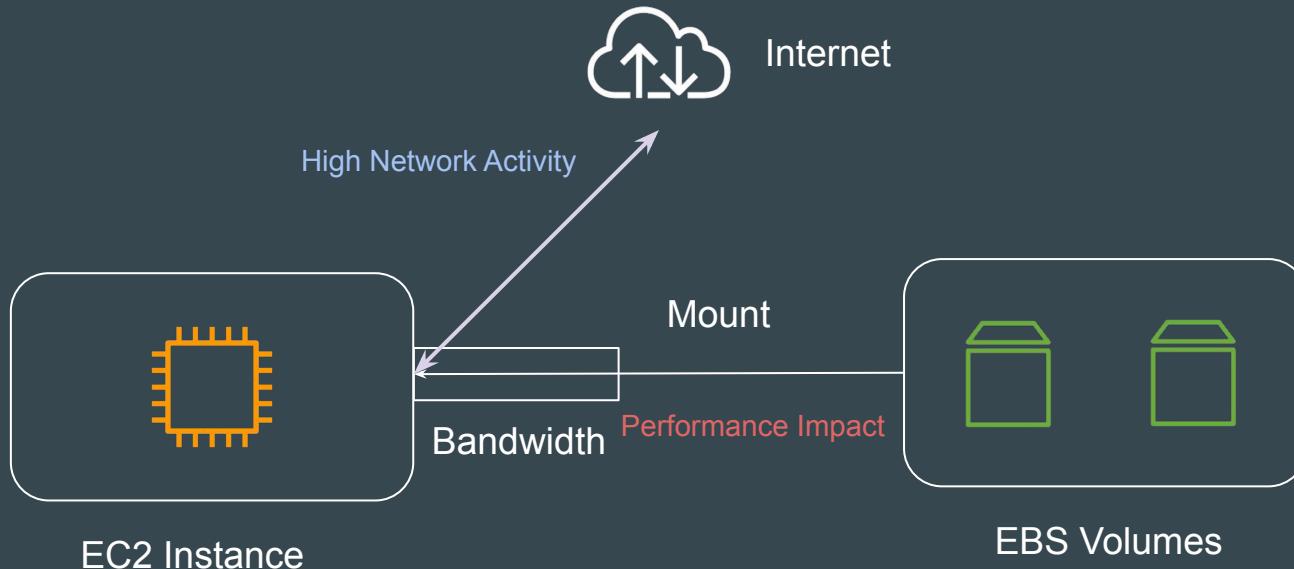
The available network bandwidth of an instance depends on the number of vCPUs that it has.

EBS volumes are mounted to the E2 instance via Network.



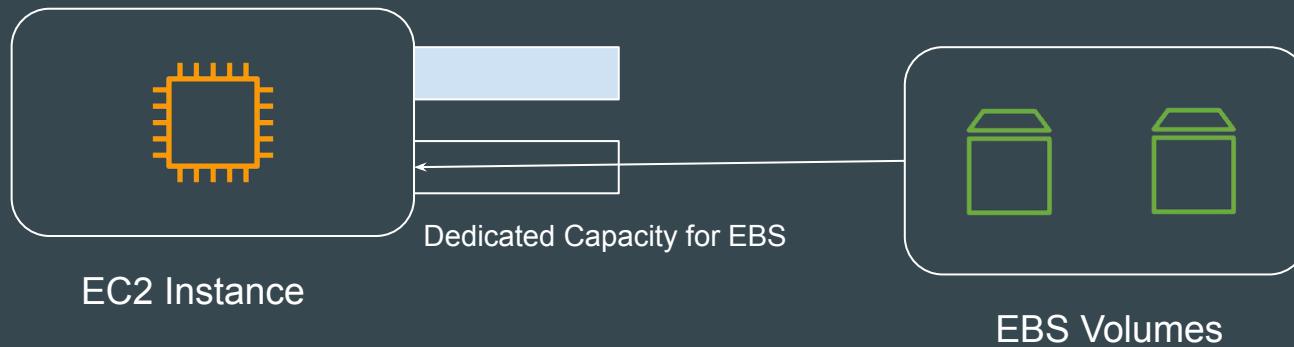
# Understanding the Challenge

If EC2 instance is using the available bandwidth and has high Network I/O, it can impact the overall performance at EBS level.



# EBS Optimized EC2 Instances

An Amazon EBS–optimized instance uses an optimized configuration stack and provides additional, **dedicated capacity** for Amazon EBS I/O.



# Supported Instance Types

Not ALL instance types support EBS Optimization.

Some instances types have EBS Optimization enabled by default.

For certain instance types, you have to explicitly enable EBS Optimization.



---

# Domain Name System (DNS)

The backbone of internet

---

# Attacks on DNS

## Biggest DDoS attack in history slows Internet, breaks record at 300 Gbps

Computerworld Mar 27, 2013 2:01 PM PT

RELATED TOPICS  
Cybercrime & Hacking  
Internet  
Cyberattacks



If you've had issues lately with your Internet being slow, it's because the Internet is undergoing the biggest DDoS attack in its history. If you can't reach Netflix, or are having difficulties accessing other sites, then it might be due to this huge online fight between [CyberBunker](#), a Dutch hosting company, and [Spamhaus](#), an anti-spam group. This Web war began when Spamhaus blacklisted the Dutch company as spammers. If the cyberattacks escalate, security experts [told](#) the New York Times that "people may not be able to reach basic Internet services, like e-mail and online banking."

Steve Linford, chief executive for Spamhaus, [told BBC](#) that the scale of this cyberattack has been "unprecedented. These attacks are peaking at 300 gb/s (gigabits per second). Normally when there are attacks against major banks, we're talking about 50 gb/s."

The attacks have been ongoing since [March 15](#) and are "[being investigated](#) by five different national cyber-police-forces

### MORE LIKE THIS

DDoS attack against Spamhaus later targeted Tier 1 providers

Update: Spamhaus hit by biggest-ever DDoS attacks

Spamhaus vs. CyberBunker: Sky falling on Internet in MAHOOOSIVE DNS DDoS FUD

on IDG Answers ↗  
How can a DDoS attack on a single company slow down the entire internet?

## Cable provider WOW says weekend attack on servers left Michigan customers without internet service

POSTED: 11:53 PM, Jul 12, 2015

UPDATED: 12:09 PM, Jul 13, 2015

Cable provider WOW says attack has left M...

TOP TEN AT 10PM

iZ.com CONNECTION PROBLEMS FOR MANY WOW! INTERNET CUSTOMERS IN SE MICHIGAN

# Let's understand the simple way



- Mr A - 9000000000
- Ms B - 8000000000
- Mr C - 8080XXXXXX

# DNS



Converts Domain Name to IP Address

google.com ⇒ 216.58.216.78

facebook.com ⇒ 173.252.120.6

yahoo.com ⇒ 98.139.183.24

---

# DNS Records

The backbone of internet

---

# DNS Records

DNS records are basically mapping files stored in the DNS server

Example:

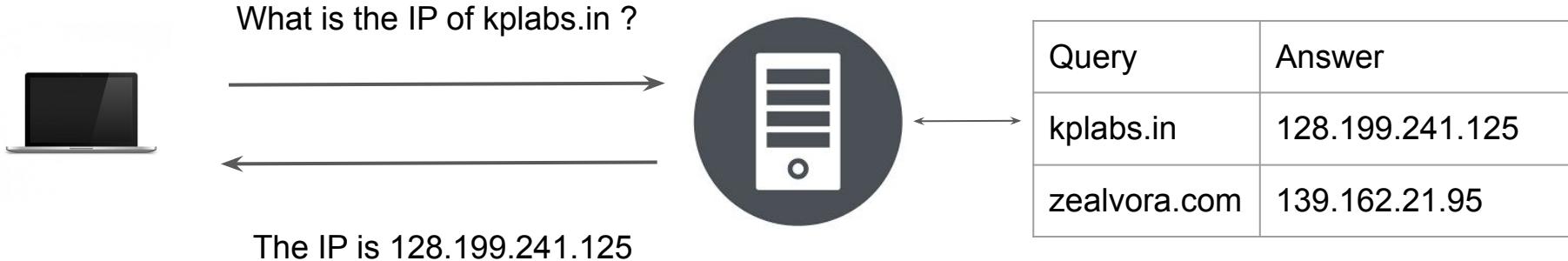
kplabs.in → 128.30.45.50

ipa.kplabs.in → 128.45.32.54

spacewalk.kplabs.in → 139.20.42.52



# Understanding how it works



# DNS Record Types

There are various types of DNS records, each one serves a specific purpose.

Types of DNS records :

A  
AAAA  
CNAME  
ALIAS  
MX

NS  
PTR  
SOA  
TXT  
SRV

---

# A, AAAA Records

The backbone of internet

---

# A Records

A which basically stands for “address” is one of the most basic types of DNS record and it points a domain to IPV4 address.

Example:

meooandmeooo.com → 192.168.10.20

blog.meooandmeooo.com → 128.30.45.50

# AAAA Records

AAAA records are similar to A records with difference of input being a IPV6 address.

Example:

ipv6ready.org → 2606:4100:3880:1250::100

# CNAME

CNAME records are used for pointing a domain name to another hostname.

Example:

blog.meooandmeooo.com → zealvora.com

---

# Route53

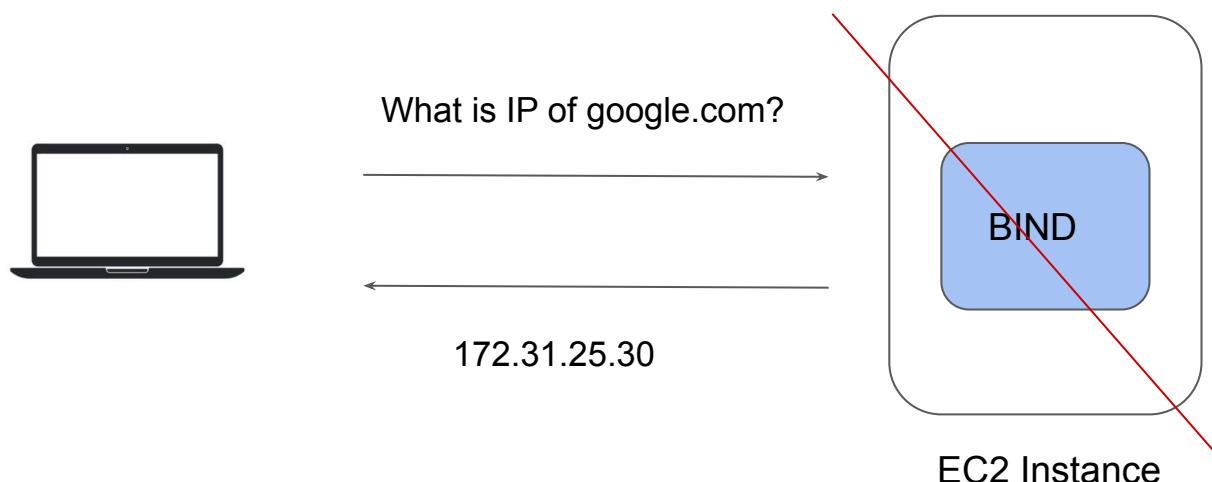
The DNS Server in AWS

---

# Overview of DNS Server

In order to get the DNS resolution, it is important to have a DNS Server running.

There are various softwares like Bind that provides features associated with DNS Resolutions.



# Managed vs Unmanaged

## Un-Managed Approach :

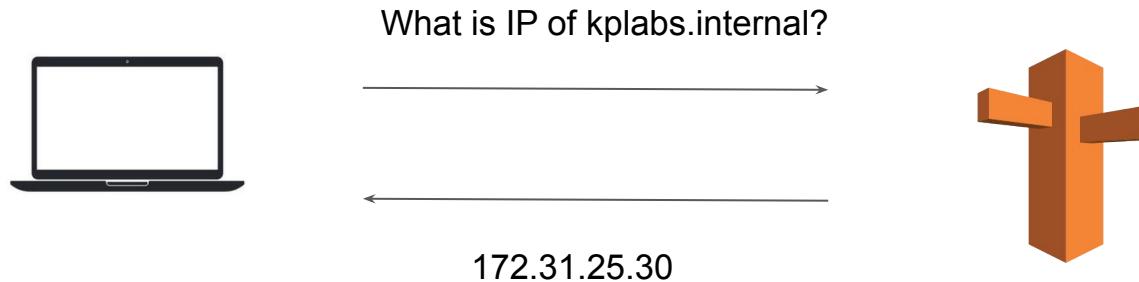
- Organization can configure and maintain their own DNS servers.
- Good for learning, not recommended on the longer term.

## Managed Approach:

- Let the service provider manage the DNS Servers for you.
- Sleep peacefully.

# Managed DNS Service

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service.



# Route53

Apart from standard DNS functionality, it provides great set of features like:

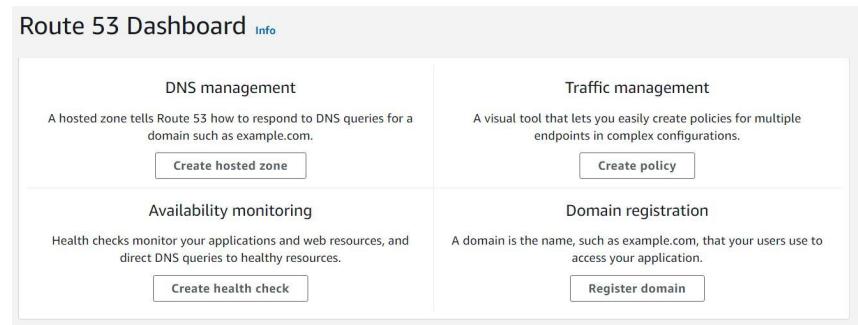
Launching private hosted zones.

Health Checks & Monitoring.

Routing capabilities.

Geo DNS

DNS Failover and many more



---

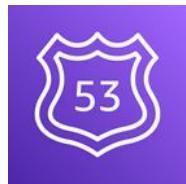
# Creating Route53 Records

Let's Implement DNS

---

# Overview of Hosted Zone

A hosted zone is a container for records, and records contain information about how you want to route traffic for a specific domain, such as example.com



Domain	Mapping
example.com	172.31.0.5
kplabs.example.com	192.168.2.0
demo.example.com	10.77.10.15

Hosted Zone

# Hosted Zone

example.com [Info](#)

[Delete zone](#) [Test record](#) [Configure query logging](#)

**Hosted zone details** [Edit hosted zone](#)

[Records \(4\)](#) [Hosted zone tags \(0\)](#)

**Records (4) [Info](#)**  
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

[Delete record](#) [Import zone file](#) [Create record](#)

[Type](#) [Routing policy](#) [Alias](#) [«](#) [1](#) [»](#) [⚙️](#)

<input type="checkbox"/>	Record name	Type	Routing policy	Differentiator	Value/Route traffic to
<input type="checkbox"/>	example.com	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
<input type="checkbox"/>	example.com	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
<input type="checkbox"/>	demo.example.com	A	Simple	-	10.77.10.15
<input type="checkbox"/>	kplabs.example.com	A	Simple	-	172.31.0.5

# Types of Hosted Zone

There are two types of Hosted Zones

Type	Description
Public Hosted Zone	Specifies how you want to route traffic on the Internet
Private Hosted Zone	Specifies how you want to route traffic in an Amazon VPC

# Understanding with Simple Analogy



Walkie Talkie  
Private Communication  
Private Hosted Zone



Mobile Phone  
Public Communication  
Public Hosted Zone

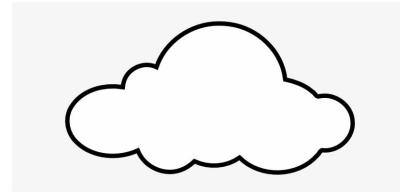
# Understanding Hosted Zones

Private Hosted Zone



Amazon VPC

Public Hosted Zone

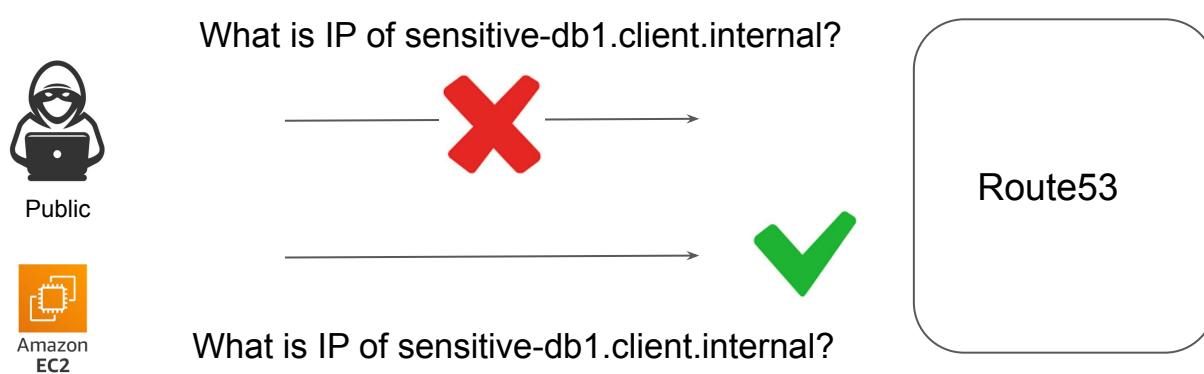


Internet

# Sample Use-Case

ABC organization is storing all the sensitive information like Credit card numbers in the database.

Applications connects to the database with the DNS of [sensitive-db1.client.internal](#) which internally routes to IP address 172.31.0.10



---

# CNAME Records

Name Based Records

---

# A Records

A which basically stands for “address” is one of the most basic types of DNS record and it points a domain to IPV4 address.

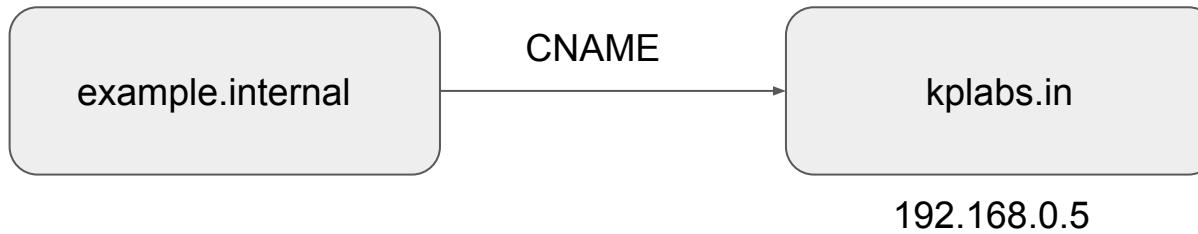
Domain	A Record
demo.kplabs.internal	192.168.10.20
blog.kplabs.internal	128.30.45.50

# CNAME Records

CNAME records are used for pointing a domain name to another hostname.

In below diagram, example.internal has CNAME to kplabs.in

When we resolve example.internal, the response will be 192.168.0.5



---

# MX Record

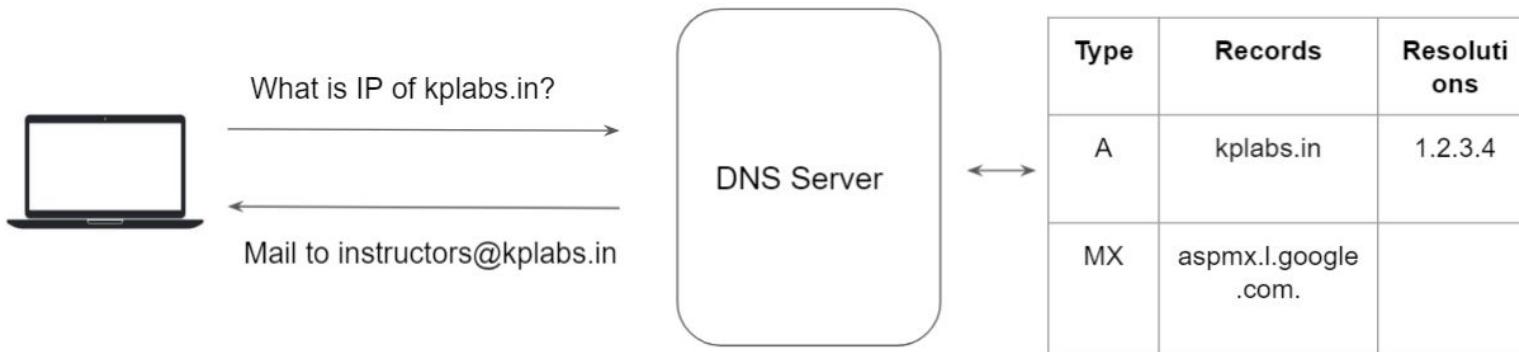
Mail Server Use-Case

---

# Overview of MX Records

A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name.

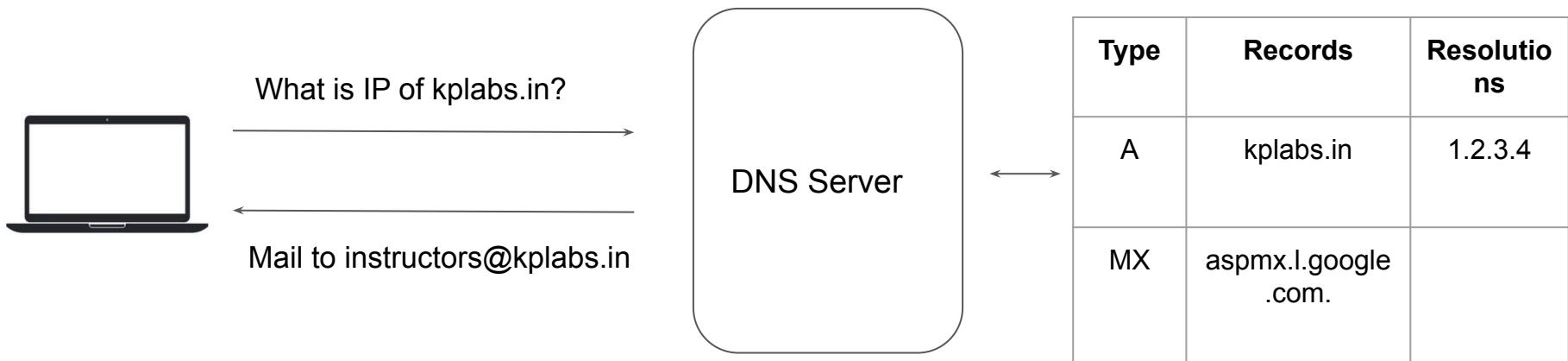
A single domain is used for multiple purpose, incl loading websites, sending emails and others.



# Overview of MX Records

A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name.

A single domain is used for multiple purpose, incl loading websites, sending emails and others.



# MX Record in More Detail

The characteristic payload information of an MX record is a Priority, and the domain name of a mail server .

The priority field identifies which mailserver should be preferred

Domain	Type	Priority	Host
kplabs.in.	MX	1	aspmx.l.google.com
kplabs.in.	MX	5	alt1.aspmx.l.google.com

---

# TXT Record

Text Information in DNS

---

# Overview of TXT Records

The DNS ‘text’ (TXT) record lets a domain administrator enter text into the Domain Name System (DNS) record.

Domain	Record Type	Value
txt.kplabs.in	TXT	This is an Awesome Domain!

# Use-Case 1: Prove Ownership of the Domain

I have a domain (kplabs.in) and I want to prove ownership of this domain to a 3rd Part.

3rd Part asks me to store following contents on verify.kplabs.in: “3rd Party Verification 123”

Domain	Type	Host
verify.kplabs.in	TXT	3rd Party Verification 123

---

# CNAME vs ALIAS

Understand the Use-Case

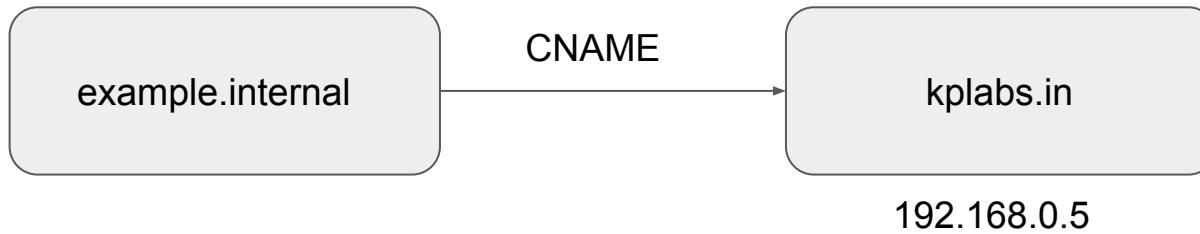
---

# CNAME Records

CNAME records are used for pointing a domain name to another hostname.

In below diagram, example.internal has CNAME to kplabs.in

When we resolve example.internal, the response will be 192.168.0.5

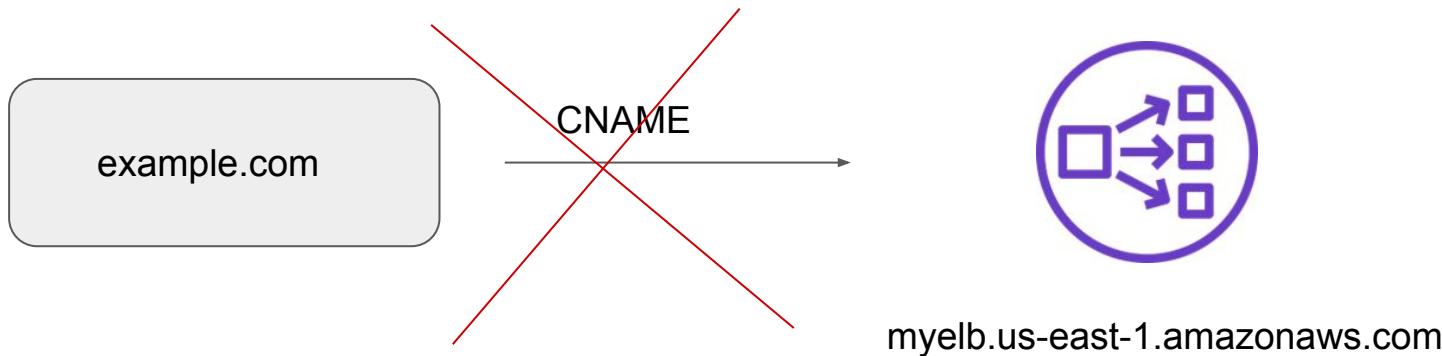


# Challenge with CNAME Record

There is one important drawback of CNAME Record.

It cannot be used with the ROOT domain.

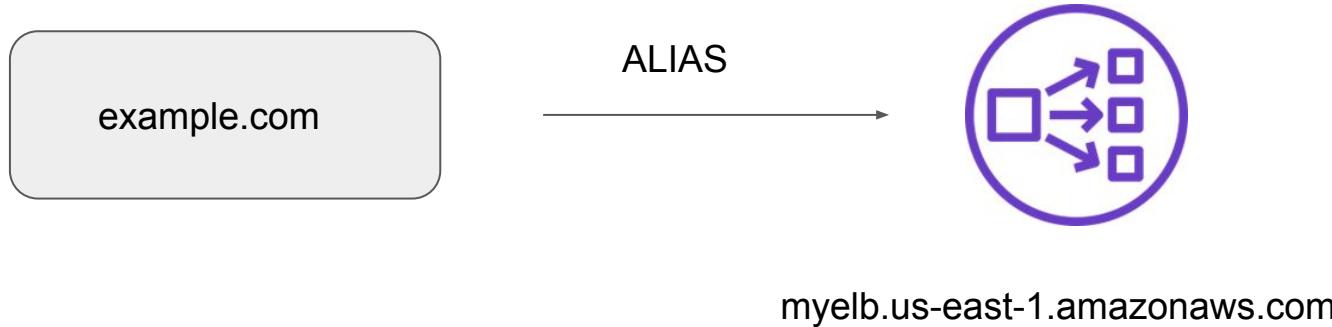
example.com CNAME acme.com << CANNOT WORK



# Use ALIAS Record

If we want ROOT domain to point to ELB, S3 Bucket, CloudFront distribution, it will not work with CNAME Records.

To resolve this drawback of CNAME record, we make use of ALIAS record which allows us to even point ROOT domain to DNS of AWS Services.



---

# Advance Route53 Features

Interesting Features of Route53

---

# Managed DNS Providers

Generally a managed DNS server supports basic functionality like :

- Domain Registration
- GUI for putting DNS records
- Mapping & Resolving various DNS Records.
- WHOIS Management

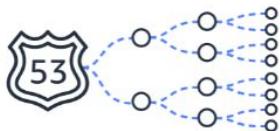
The screenshot shows a domain management interface. On the left, a sidebar with a green header titled 'Details' lists various management options: Contacts, Nameservers, DNS Records, URL Forwarding, Email Forwarding, NS Registration, and Account Transfer. To the right, under 'Domain Details', the domain name is listed as 'kplabs.in'. It shows the domain is locked ('Locked | Unlock'), has a transfer auth code ('Transfer Auth Code: Show Code'), and is hosted by 'name.com'. The nameservers listed are ns1.name.com, ns2.name.com, ns3.name.com, and ns4.name.com. Other details include automatic renewal being enabled and whois privacy being N/A.

**Domain Details**

**Domain name:** kplabs.in  
**Domain lock:** Locked | [Unlock](#)  
**Transfer Auth Code:** [Show Code](#)  
**Nameservers:** [Edit Nameservers](#)  
ns1.name.com, ns2.name.com, ns3.name.com, ns4.name.com  
**DNS hosted:** Yes [Update DNS records](#)  
**Registrar:** name.com  
**Website hosted:** No  
**Automatic Renewal:** Enabled   
**Whois Privacy:** N/A

# Route53 does a lot more

- Support of Public and Private Hosted Zones.
- Routing - Weighted, Latency, Geolocation, Round Robin
- Health Checks & Monitoring
- Route53 Endpoints
- DNS Firewall



Traffic Flow



Hosted Zone



Health Checks

---

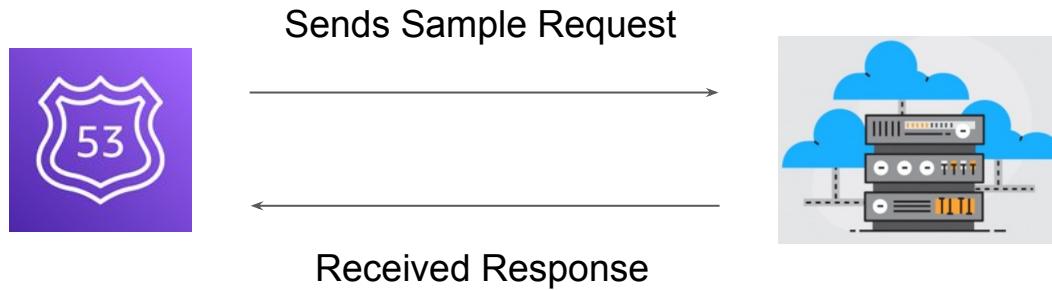
# Route53 Health Checks

Back to Monitoring!

---

# Overview of Health Checks

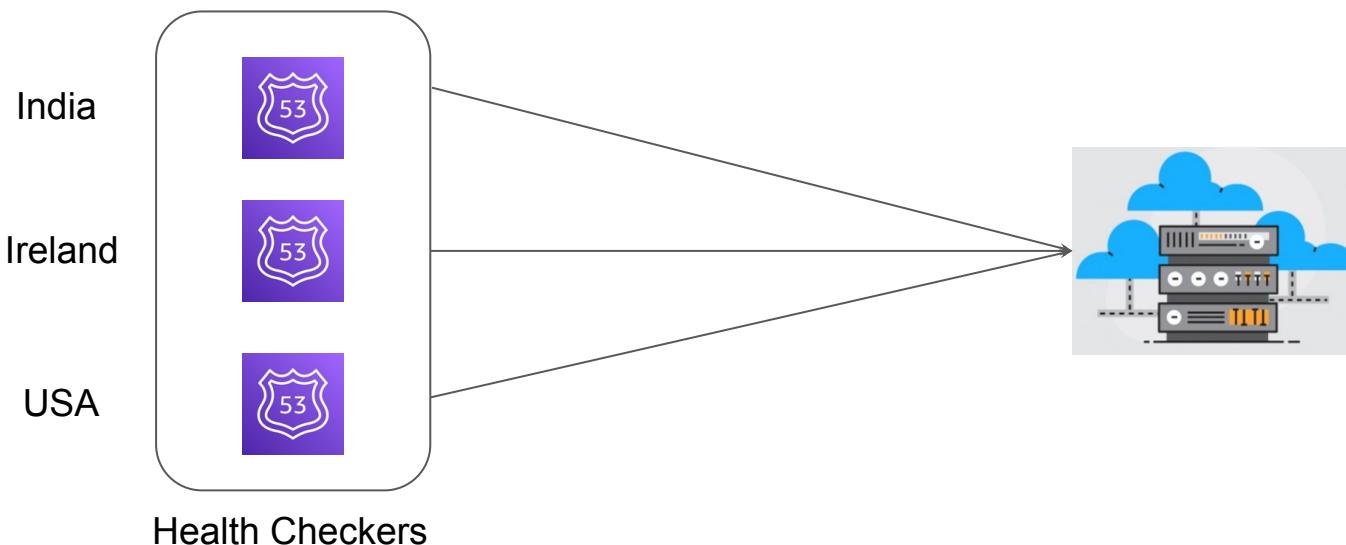
Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources



# Route53 Health Checkers

Route 53 has health checkers in locations around the world.

When you create a health check that monitors an endpoint, health checkers start to send requests to the endpoint that you specify to determine whether the endpoint is healthy.



---

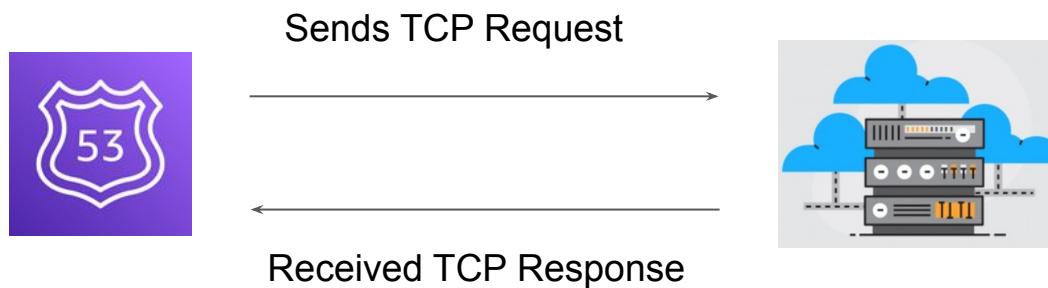
# Types of Health Checks

Back to Monitoring!

# Type of Health Checks

There are three primary type of Health Checks supported by Route53

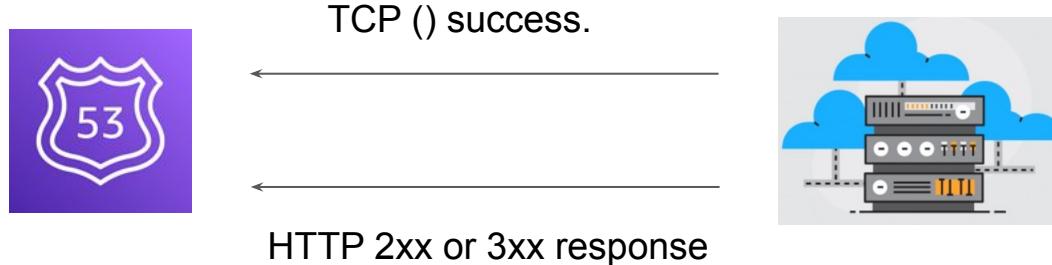
1. HTTP and HTTPS health checks
2. TCP health checks
3. HTTP and HTTPS health checks with string matching



# Type 1 - HTTP/HTTPS

Two important factors as part of this health check:

1. Route 53 must be able to establish a TCP connection with the endpoint within four seconds.
2. In addition, the endpoint must respond with an HTTP status code of 2xx or 3xx within two seconds after connecting.



## Type 2 - TCP

Route 53 must be able to establish a TCP connection with the endpoint within ten seconds.

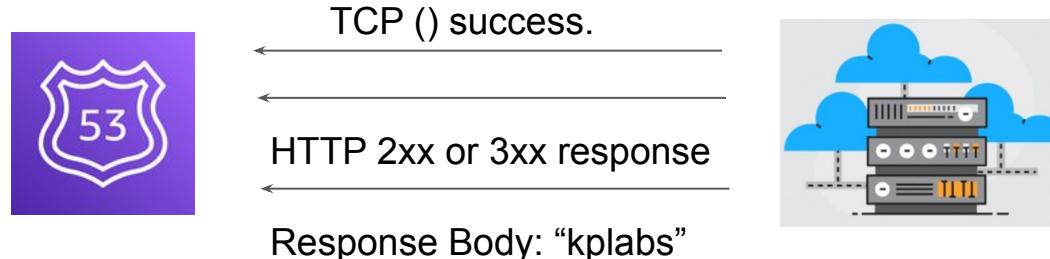


TCP () success.



## Type 3 - HTTP/HTTPS with string matching

1. Route 53 must be able to establish a TCP connection with the endpoint within four seconds.
2. In addition, the endpoint must respond with an HTTP status code of 2xx or 3xx within two seconds after connecting.
3. Must receive response body within next two seconds containing a specific string.
4. The string must appear entirely in the first 5,120 bytes of the response body or the endpoint fails the health check.



---

# Routing Policies

Great DNS Provider

---

# Routing Policies

Routing Policies determine how Amazon Route53 responds to the queries.

There are various supported routing policies available in Route53.

Each policy supports a specific use-case.

- Simple
- Weighted
- Latency
- Failover
- Geolocation
- Multi-value answer



# Simple Routing Policy

In simple routing, there is a plain one to one mapping between domain and host.

Example: blog.kplabs.internal A 128.199.241.125

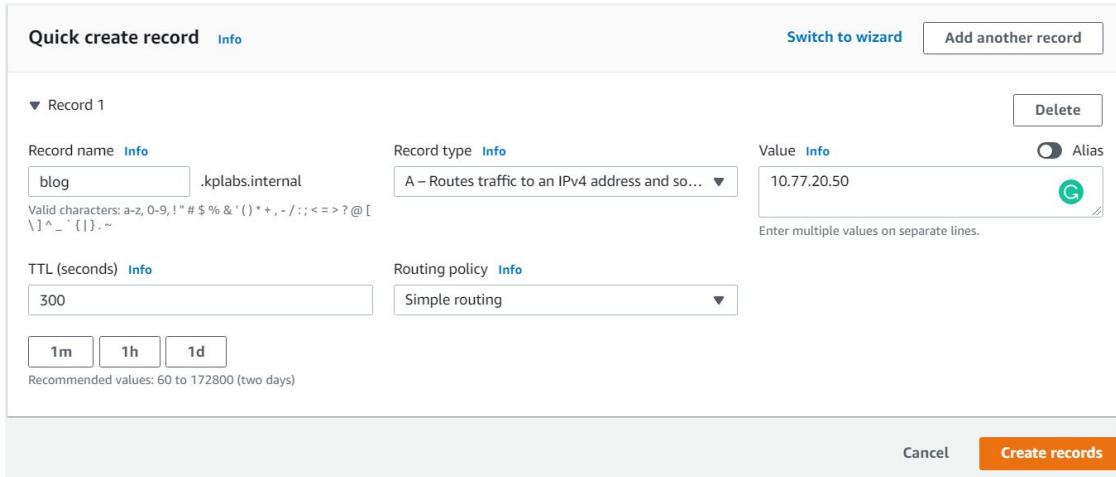
Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

▼ Record 1

Record name <a href="#">Info</a> blog.kplabs.internal	Record type <a href="#">Info</a> A – Routes traffic to an IPv4 address and so...	Value <a href="#">Info</a> 10.77.20.50 <small>Enter multiple values on separate lines.</small>
TTL (seconds) <a href="#">Info</a> 300	Routing policy <a href="#">Info</a> Simple routing	<input checked="" type="radio"/> Alias
<input type="button" value="1m"/> <input type="button" value="1h"/> <input type="button" value="1d"/>		

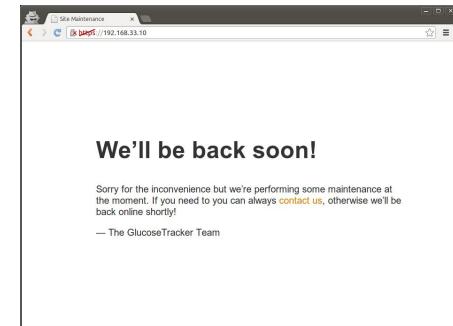
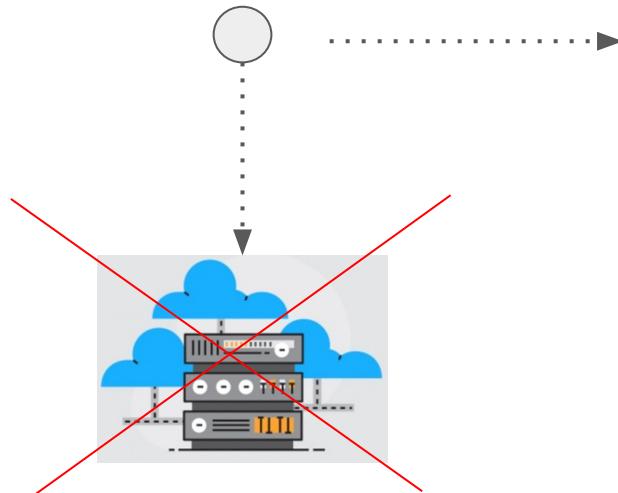
Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)



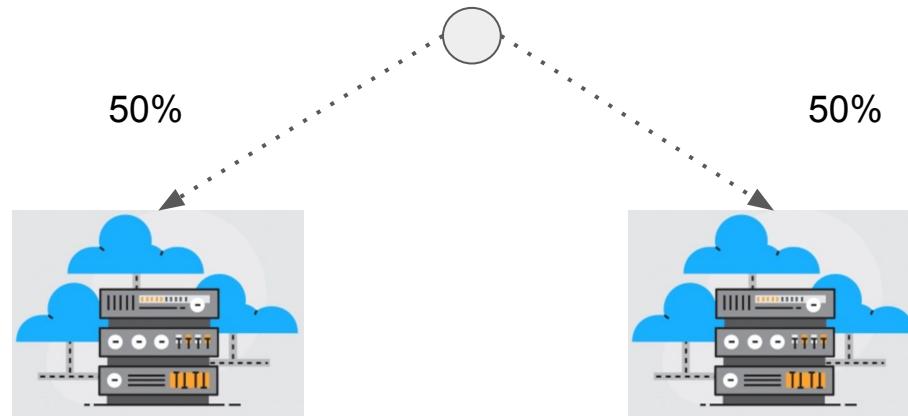
# Failover Routing

Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy.



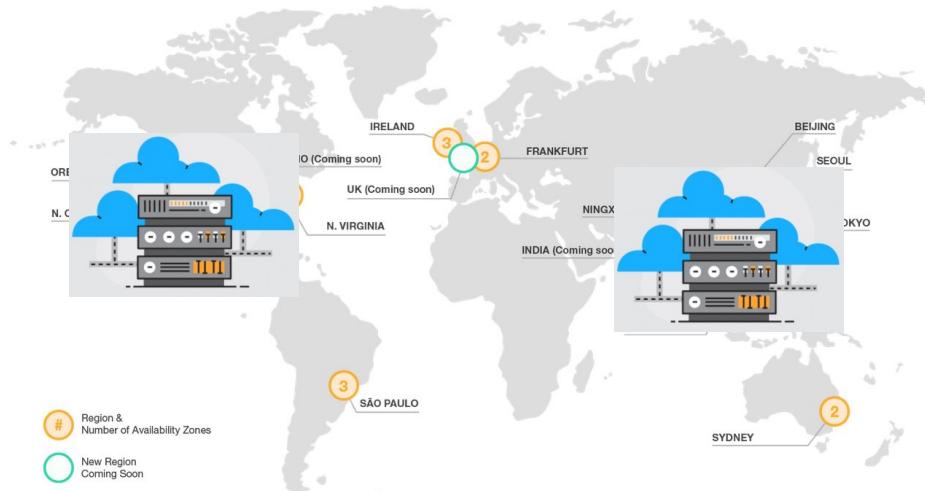
# Weighted Routing

Weighted routing helps us to route the traffic to multiple resources in a proportion that we specify from our end.



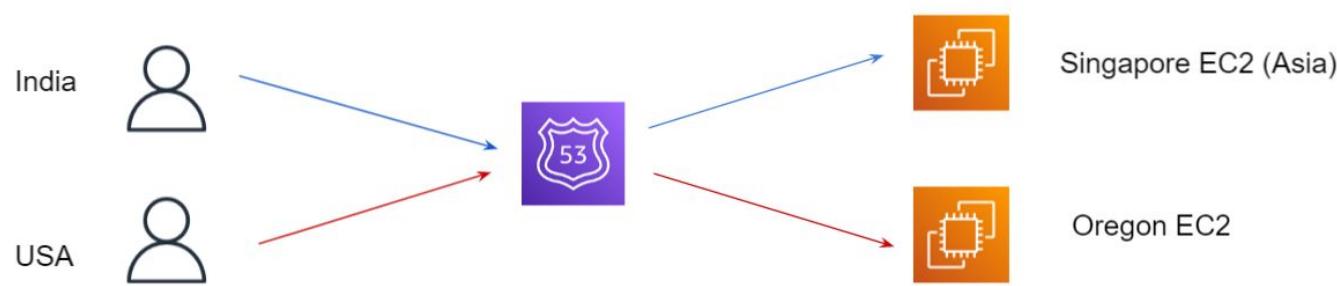
# Latency Based Routing

If your application is hosted in multiple AWS regions, we can improve the performance for the users by serving their request from AWS region that provides lowest latency.



# GeoLocation Routing

Geolocation routing allows us to choose different resources for different users based on different countries / continents.



# Join us in our Adventure

Be Awesome



[kplabs.in/twitter](http://kplabs.in/twitter)



[kplabs.in/linkedin](http://kplabs.in/linkedin)

[instructors@kplabs.in](mailto:instructors@kplabs.in)

---

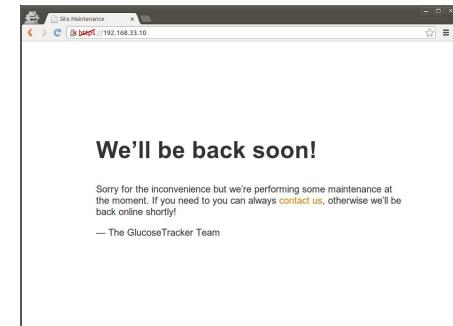
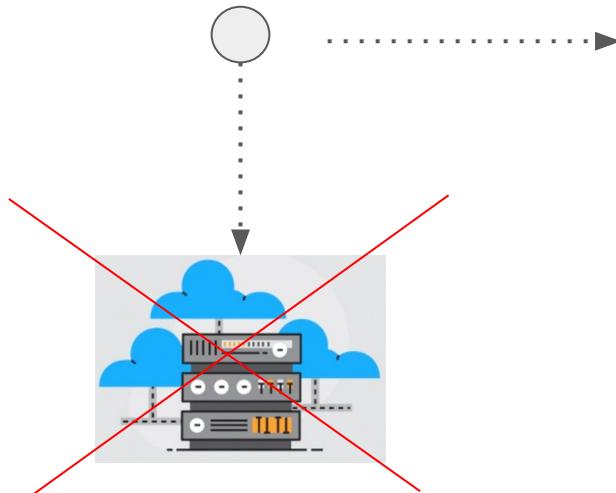
# Failover Routing Policy

Back to Monitoring!

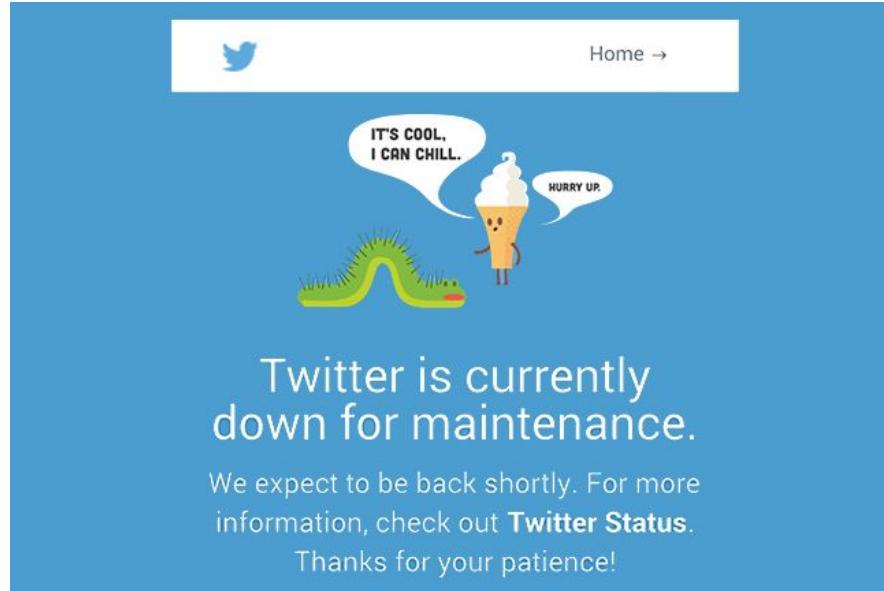
---

# Failover Routing

Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy.



# Maintenance Page



---

# Weighted Routing

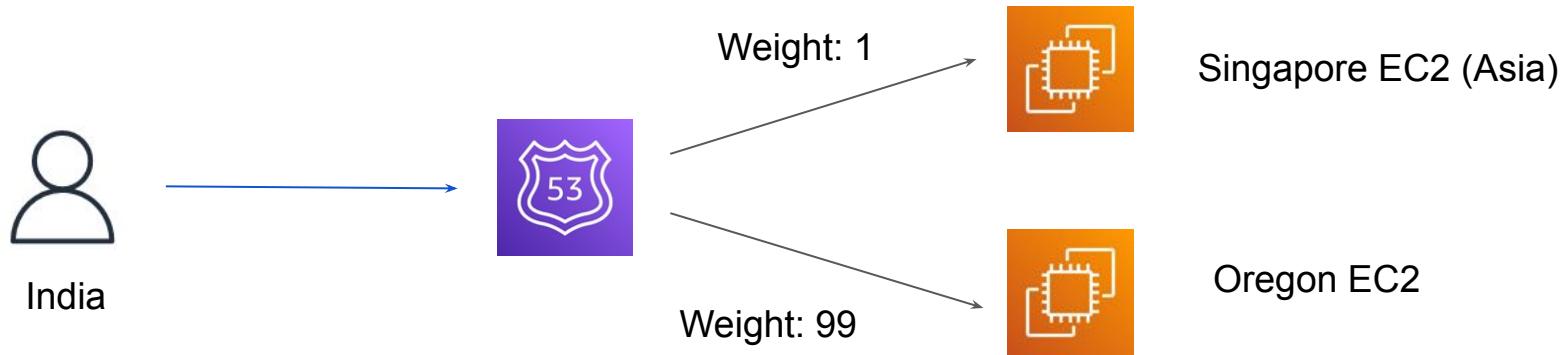
Route53 Routing Policy

---

# Overview of Weighted Routing Policy

**Weighted Routing** allows us to specify the proportion in which traffic should be routed to the underlying servers.

If we want to send small portion of traffic to a new website theme, you can specify the weight of 1 and 99. The resource with 1 gets 1% of the traffic and other gets 99% of traffic.



---

# Geolocation Routing

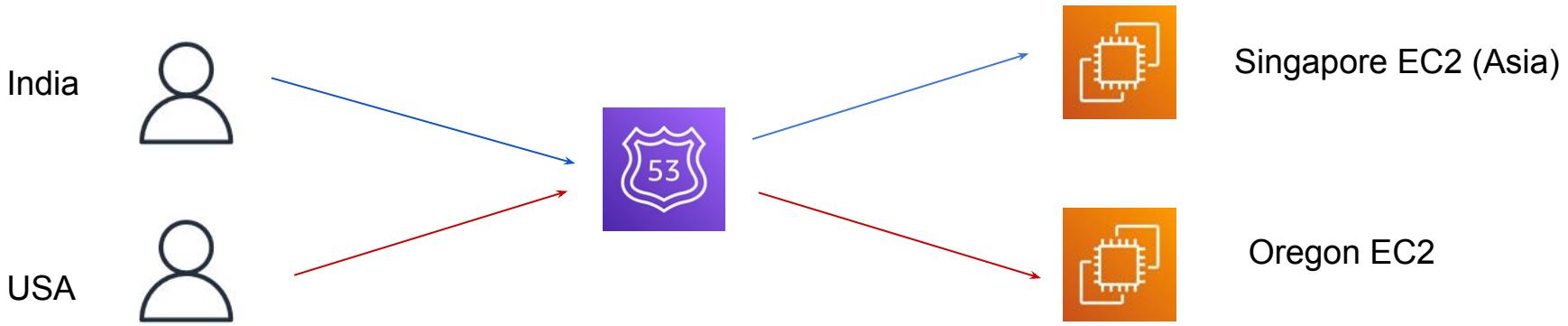
Route53 Routing Policy

---

# Overview of Geolocation Routing

**Geolocation Routing** allows us to choose resources based on the geographic location of the users

For example, you might want all queries from Asia to be routed to an ELB load balancer in the Singapore region.



# Important Caution

Geolocation Routing works by mapping database to IP address.

The **results are not always accurate** as some ISP might not have any geolocation data associated with them, and some ISP might move the IP block to different country without notification.

For such cases, Route 53 allows us to have a default resource block associated with the routing policy.

---

# Geolocation Routing

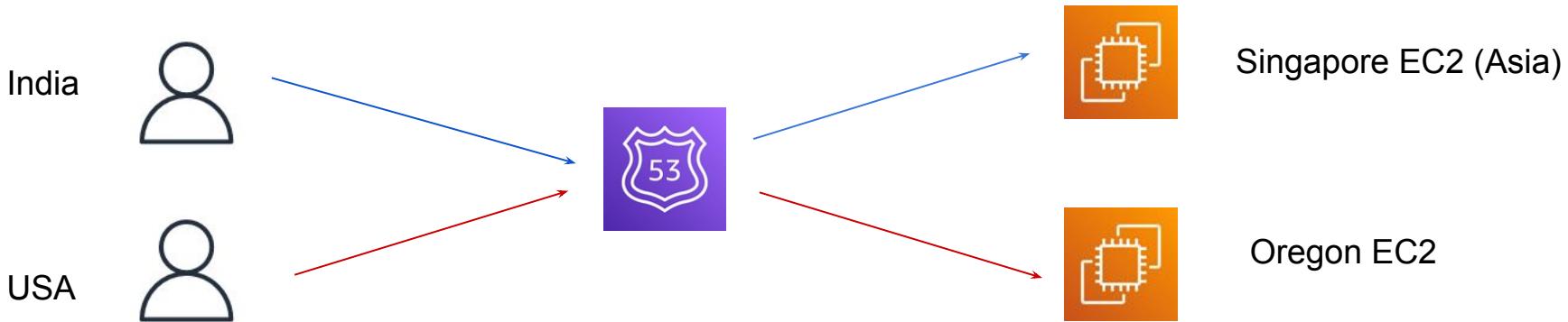
Route53 Routing Policy

---

# Overview of Geolocation Routing

**Geolocation Routing** allows us to choose resources based on the geographic location of the users

For example, you might want all queries from Asia to be routed to an ELB load balancer in the Singapore region.



# Important Caution

Geolocation Routing works by mapping database to IP address.

The **results are not always accurate** as some ISP might not have any geolocation data associated with them, and some ISP might move the IP block to different country without notification.

For such cases, Route 53 allows us to have a default resource block associated with the routing policy.

---

# Latency Routing

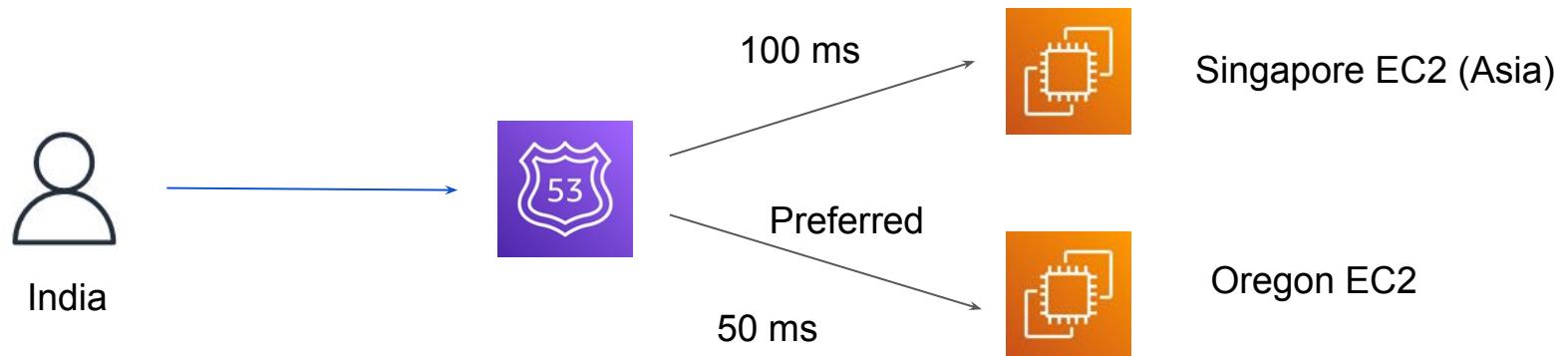
Route53 Routing Policy

---

# Overview of Latency Based Routing

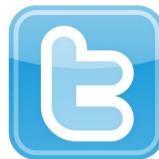
If your application is hosted in multiple AWS regions, we can improve the performance for the users by serving their request from AWS region that provides lowest latency.

A request that is routed to Singapore today might be routed to India tomorrow.



# Join us in our Adventure

Be Awesome



[kplabs.in/twitter](http://kplabs.in/twitter)



[kplabs.in/linkedin](http://kplabs.in/linkedin)

[instructors@kplabs.in](mailto:instructors@kplabs.in)

---

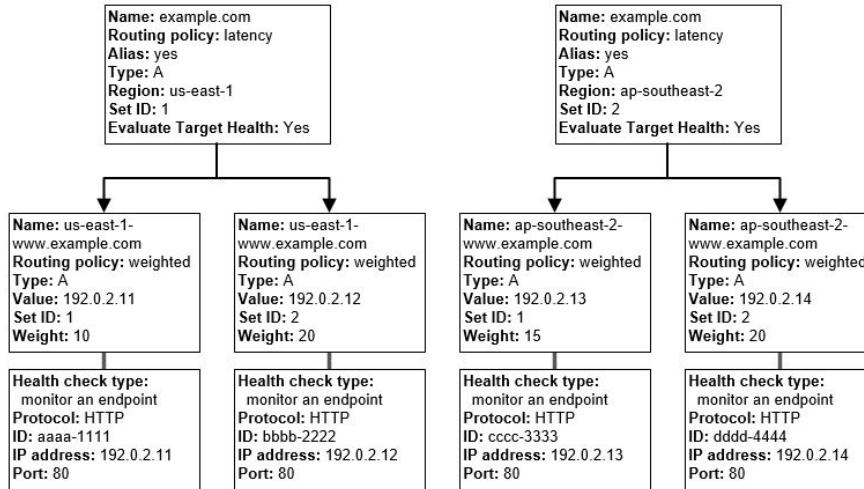
# Route53 Traffic Flow

Let's Route Traffic the Easier Way

---

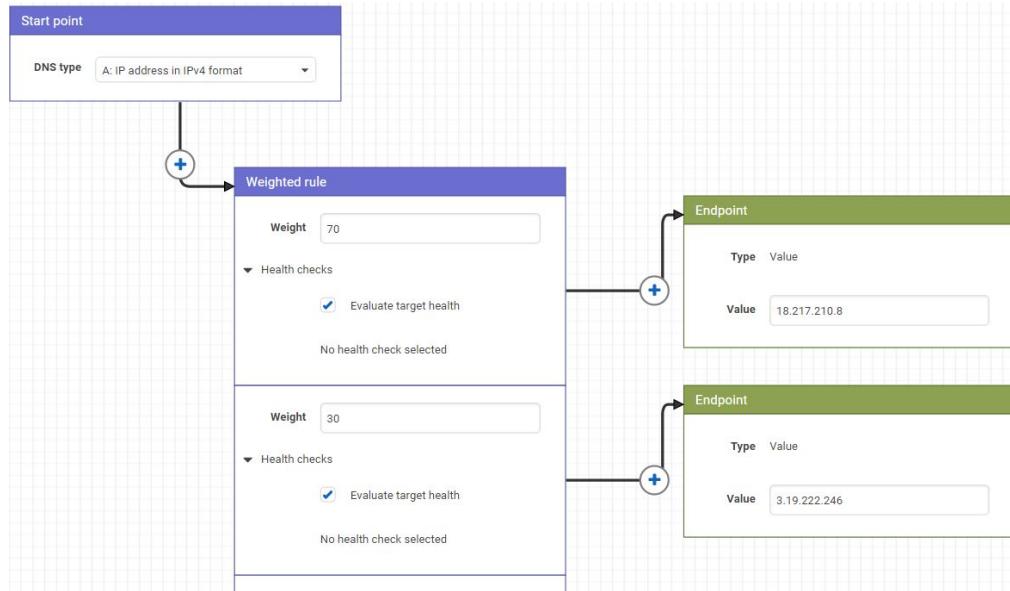
# Understanding the Challenge

When you create a complex tree records using alias records and a combination of Route 53 routing policies, such as latency, failover, and weighted, it becomes a little challenging when you create each record



# Overview of Traffic Flow

Traffic Flow providers users with a visual editor to configure the records.



# Important Pointers for Traffic Flow

You can create multiple versions of a traffic policy so you don't have to start all over when your configuration changes.

Certain Routing Policies like Geoproximity are only available in Traffic Flow.

There's a monthly charge for each traffic policy record (a little expensive)

---

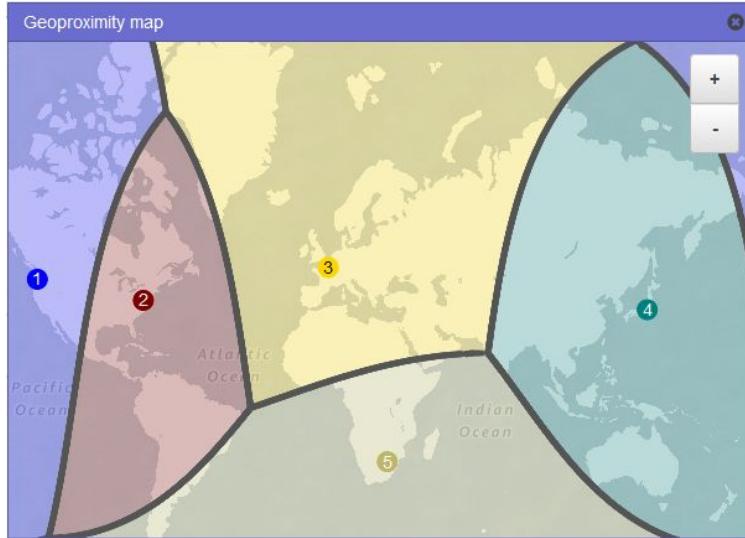
# Geoproximity Routing Policy

Route Traffic based on Physical Distance

---

# Overview of Geoproximity Routing

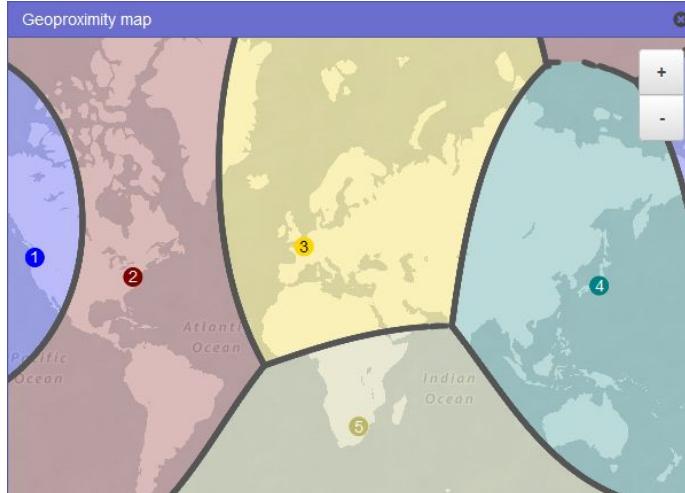
Geoproximity routing lets Amazon Route 53 route traffic based on the physical distance between your users and your resources.



# Understanding Bias

We can adjust the Bias value to route more traffic or less to a given resource in a Region.

To expand the size of the geographic region from which Route 53 routes traffic to a resource, specify a positive integer from 1 to 99 for the bias. Route 53 shrinks the size of adjacent regions.



---

# DNS Support in VPC

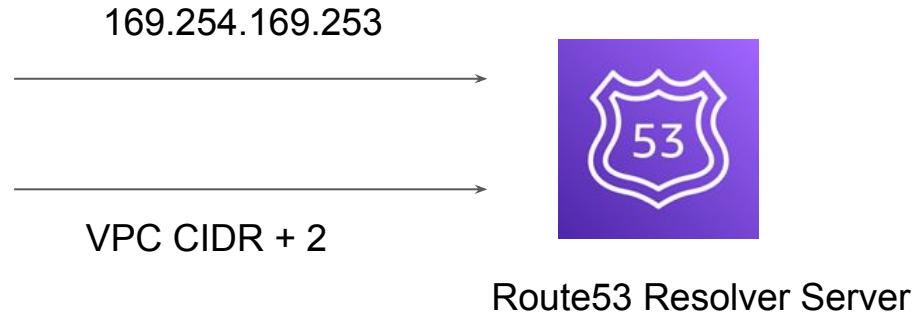
DNS Yet Again!

---

# Amazon DNS Server

The Amazon DNS server enables DNS for instances that need to communicate over the VPC's internet gateway.

The Amazon DNS server does not reside within a specific subnet or Availability Zone in a VPC. It's located at the address 169.254.169.253 (and the reserved IP address at the base of the VPC IPv4 network range, plus two). For 10.0.0.0/16, the IP is 10.0.0.2



# DNS attributes in your VPC

There are two primary attributes that determine the DNS Support provided for your VPC.

Attribute	Description
enableDnsHostnames	<p>Indicates whether instances with public IP addresses get corresponding public DNS hostnames.</p> <p>If this attribute is true, instances in the VPC get public DNS hostnames, but only if the enableDnsSupport attribute is also set to true.</p>
enableDnsSupport	<p>Indicates whether the DNS resolution is supported through Amazon Provided DNS server.</p> <p>If this attribute is false, the Amazon-provided DNS server that resolves public DNS hostnames to IP addresses is not enabled.</p>

# Case 1 - Both Attributes Are True

If both attributes are set to true, the following occurs:

- Instances with a public IP address receive corresponding public DNS hostnames.
- The Amazon-provided DNS server can resolve Amazon-provided private DNS hostnames.

## Case 2 - Both Attributes Are False

If both attributes are set to false, the following occurs:

- Instances with a public IP address do not receive corresponding public DNS hostnames.
- The Amazon-provided DNS server cannot resolve Amazon-provided private DNS hostnames.

---

# Reverse DNS

## Detailed DNS

---

# Forward DNS

In a forward DNS based scenario, an IP address is queried based on the provided domain name.

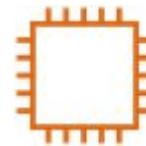


Client

What is IP of google.com?



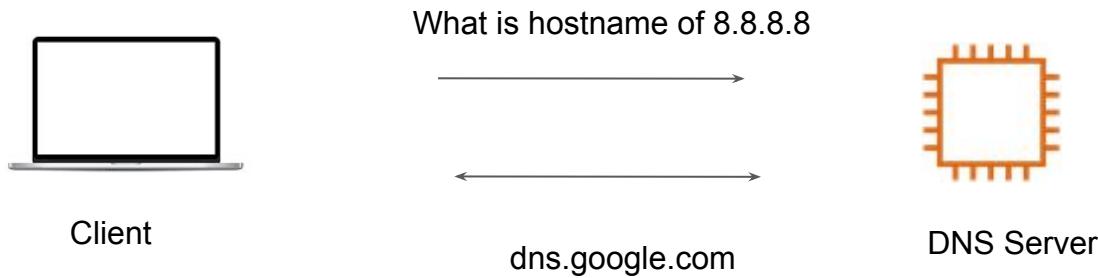
142.250.192.142



DNS Server

# Reverse DNS

Reverse DNS lookup or reverse DNS resolution (rDNS) is the querying technique of the Domain Name System (DNS) to determine the domain name associated with an IP address



# Why Reverse DNS?

Reverse DNS is important for a lot of use-cases.

Many of the email servers would reject emails from IP addresses that does not have a reverse DNS record set.

Many organizations use EC2 instances as part of their email server based architecture. For such cases it is important to have Reverse DNS setup.

---

# DNS Query Logging

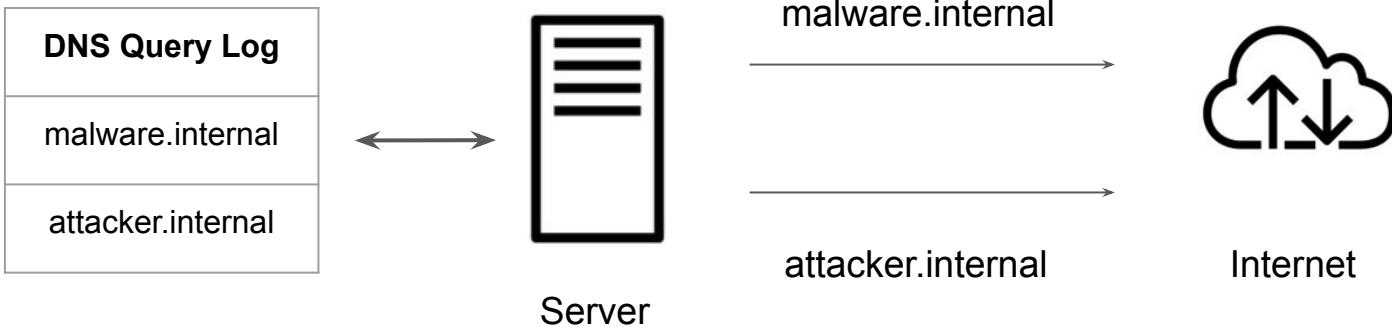
DNS Logs are Important

---

# DNS Logs Are Important

Each connection made to a domain by the client devices is recorded in the DNS logs.

Inspecting DNS traffic between client devices and your local recursive resolver could reveal a wealth of information for security and forensic analysis



# Route53 Query Logging

Query logs contain only the queries that DNS resolvers forward to Route 53.

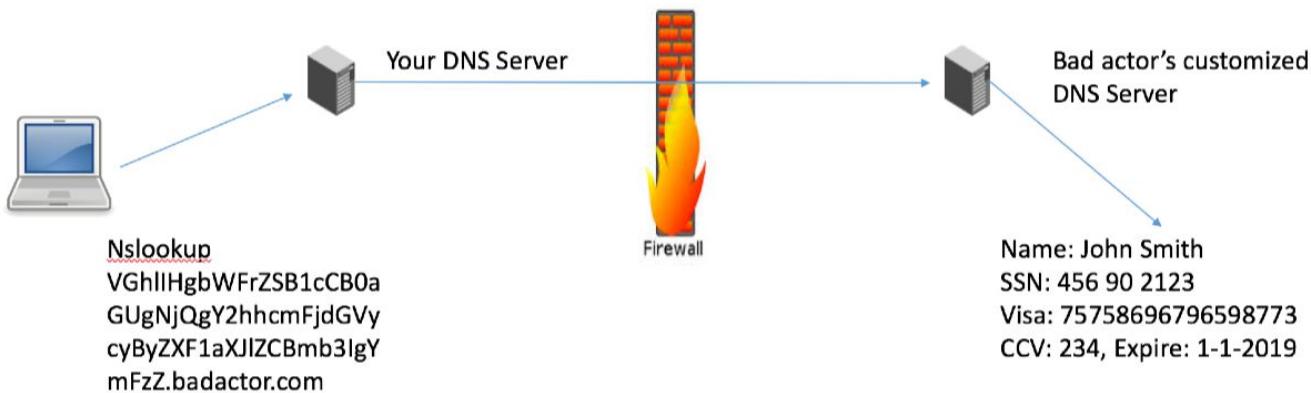
These log contain various information including:

Domain Requested, Timestamp of Request, DNS Record Type, and others.

```
2022-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP FRA6 192.168.1.1 -
2022-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP IAD12 192.168.3.1 192.168.222.0/24
2022-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP IAD12 192.168.3.1 192.168.111.0/24
2022-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP JFK5 192.168.1.2 -
```

# Security Attack via DNS

DNS Exfiltration is an unauthorized transfer of data via DNS queries routes to the attacker's server, providing them with a covert command and control channel, and data exfiltration path.



---

# Reusable Delegation Set

## Mastering DNS

---

# Understanding Delegation Set

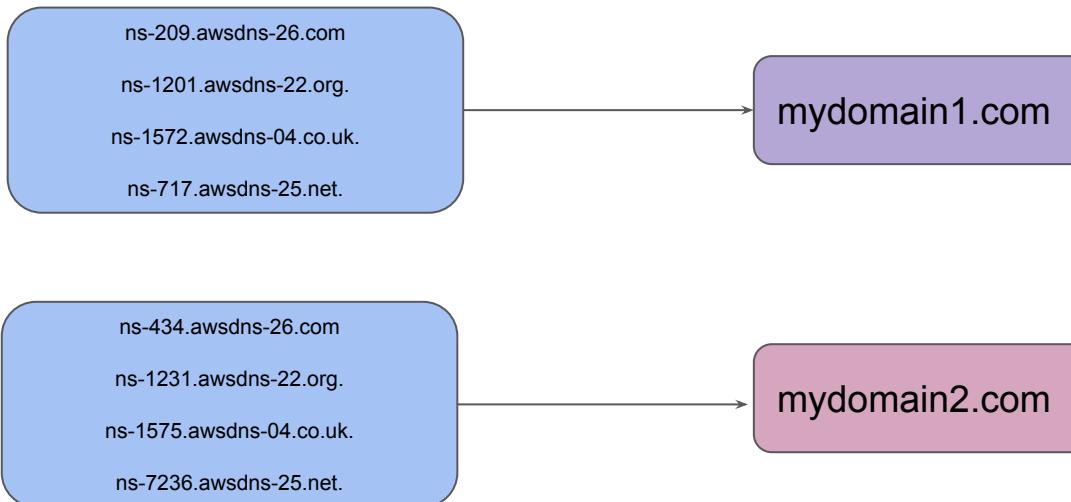
Each Amazon Route 53 hosted zone is associated with four name servers, known collectively as a delegation set.



# Challenge with Delegation Set

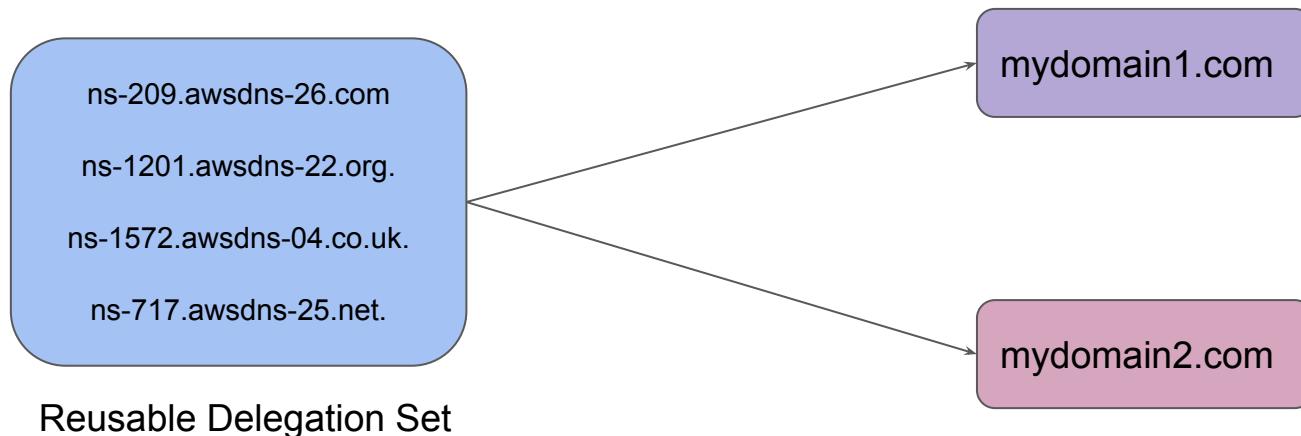
By default, Route 53 assigns a random selection of name servers to each new hosted zone.

For large scale domain migration, you will have to give unique set of name servers for each domain to the registrar.



# Reusable Delegation Set

Reusable Delegation allows customers to set a common name servers for all the hosted zones.



---

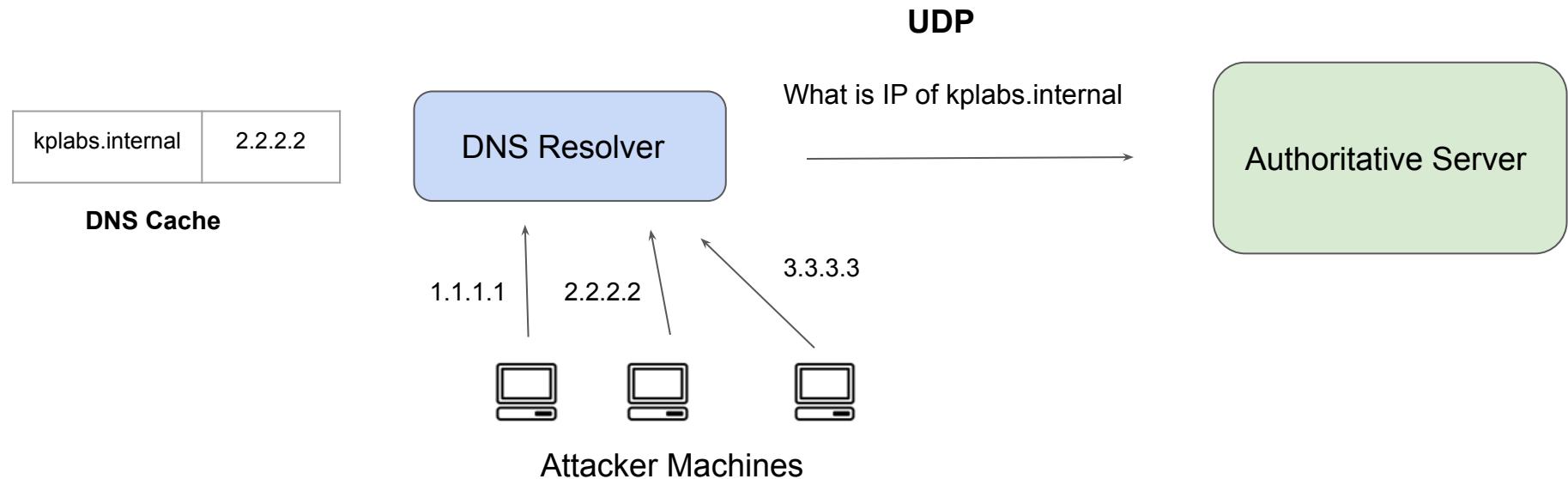
# DNS Cache Poisoning

Compromising DNS

---

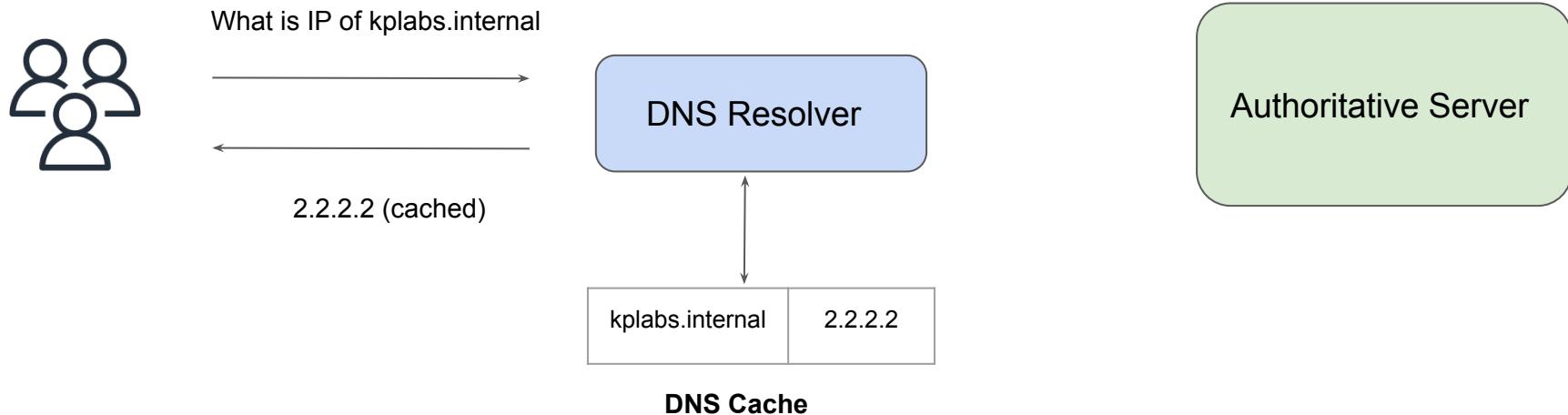
# Understanding DNS Cache Poisoning

DNS cache poisoning is a hacking attack in which false information is entered into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites



# Client and DNS Resolver

When the client queries the resolved, they would receive the Cached response.



## Important Note

In UDP, since there is no handshake that takes place, it is vulnerable to forging.

If a DNS resolver receives a forged response, it accepts and caches the data because there is no way to verify if the information is accurate and comes from a legitimate source.

---

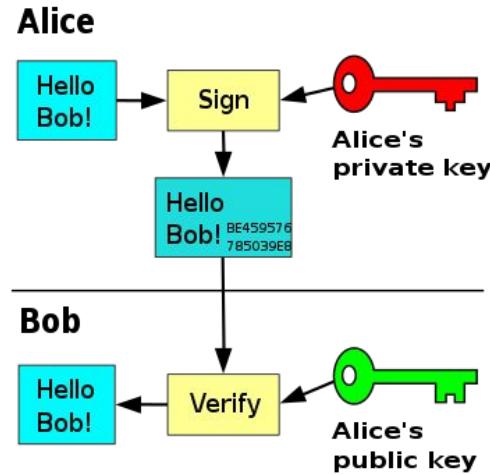
# DNSSEC

Securing DNS

---

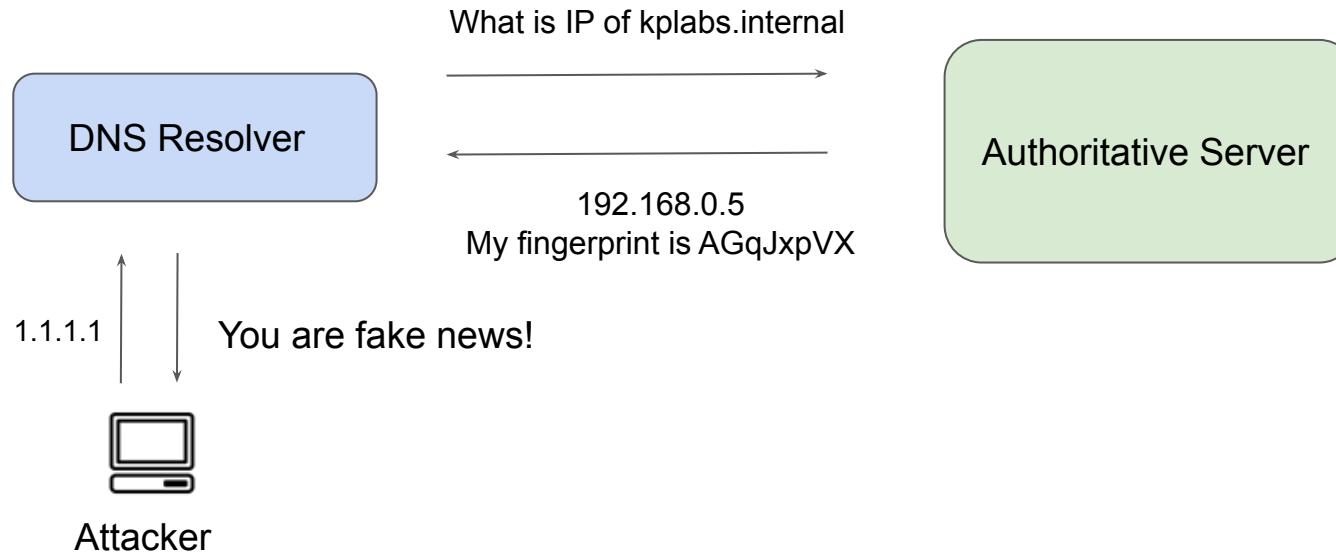
# Revising Digital Signatures

Digital signatures are used to ensure that one party cannot successfully dispute its authorship of a document or communication.



# Basics of DNSSEC

DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records.



# High-Level Pointers

It makes use of Asymmetric key encryption (public and private keys involved)

Public keys are published in the DNS.

Private keys are kept secure and used to digitally sign.

The DNS query response is validated using Public key.

# Disadvantages of DNSSEC

It adds complexity both on the client and server side.

Limited support from TLD and DNS servers

Increase in DNS Query Resolution Time

---

# Configuring DNSSEC in Route53

Let's Secure DNS

# Step 1 - Enable DNSSEC Signing & Create KSK

In this method, we perform two steps:

1. Enable DNSSEC Signing in Route53 Hosted Zone.
2. Generate KSK (Asymmetric Key) using KMS.

The screenshot shows the AWS Route53 Hosted Zone Details page for the domain `demo.zealvora.com`. The top navigation bar includes options like `Delete zone`, `Test record`, and `Configure query logging`. Below the navigation, there are tabs for `Records (3)`, `DNSSEC signing` (which is selected), and `Hosted zone tags (0)`. Under the `DNSSEC signing` tab, it displays the `DNSSEC signing` status as `Signing`. There are buttons for `View information to create DS record` and `Disable DNSSEC signing`. At the bottom, the `Key-signing keys (KSKs)` section lists one key named `demo` with a status of `Active` and a creation date of `July 10, 2022, 00:17 (UTC:+05:30)`.

## Step 2 - Provide Public Key to Registrar

Provide the public key from the key pair to your domain registrar, and specify the algorithm that was used to generate the key pair.

The domain registrar forwards the public key and the algorithm to the registry for the top-level domain (TLD).

Key type	Signing algorithm	Public key
<input checked="" type="checkbox"/> KSK	<input checked="" type="checkbox"/> ECDSAP256SHA256	<input checked="" type="checkbox"/> UzYMLi7W7miltVrv2B7mROLXuSD6Yiln70VT T0JNh6KbPKLoWUbc+DFAoRyu8jj++ZaLkc6uvcq/xY zTHLmNjA==

# Understanding the Working - Part 1

You submit a DNS query for example, by browsing to a website or by sending an email message.

The DNS resolver sends the original request to another DNS resolver.

The name server returns two values:

1. The record for the domain, such as example.com. Typically this contains the IP address of a host.
2. The signature for the record, which you created when you configured DNSSEC.

# Understanding the Working - Part 2

The DNS resolver uses the public key that you provided to the domain registrar to do two things:

1. Establish a chain of trust
2. Verify that the signed response from the DNS service provider is legitimate and hasn't been replaced with a bad response from an attacker.

If the response is authentic, the resolver returns the value to the client that submitted the request.

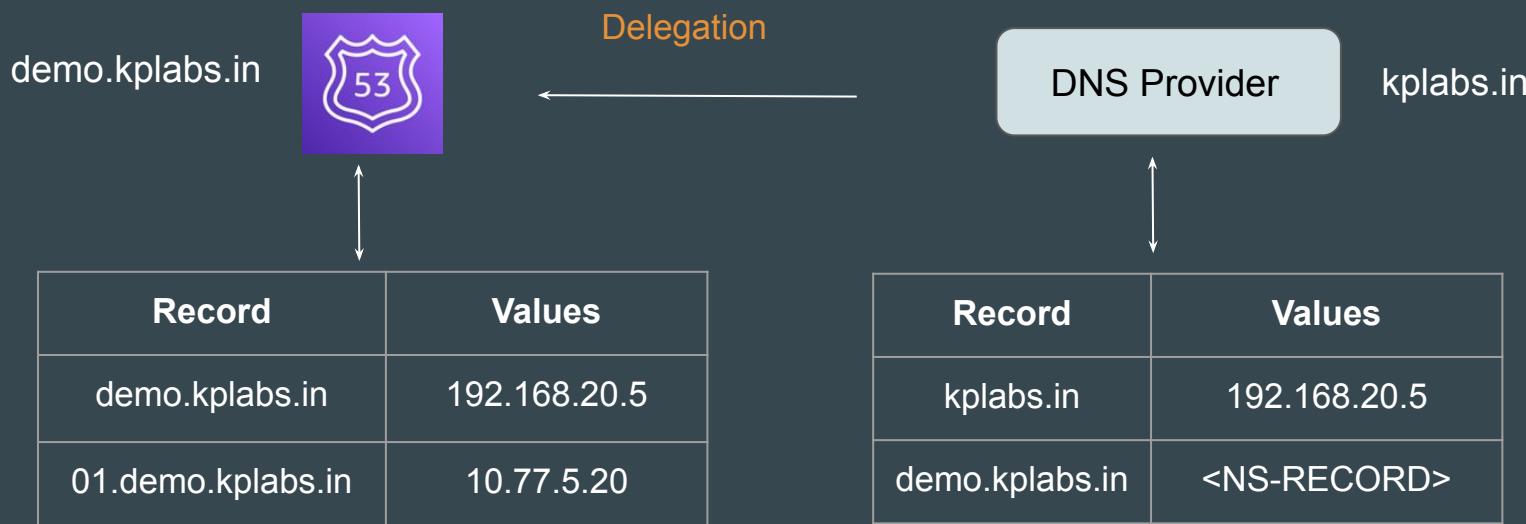
If the response can't be verified, the resolver returns an error to the user.

# Subdomain Delegation



# Delegating Subdomain

You can create a subdomain that uses Amazon Route 53 as the DNS service without migrating the parent domain from another DNS service.



# Primary Steps

1. Create a Hosted Zone in the Route53 associated with the sub-domain.
2. Add NS records for the subdomain to the zone file for the parent domain.

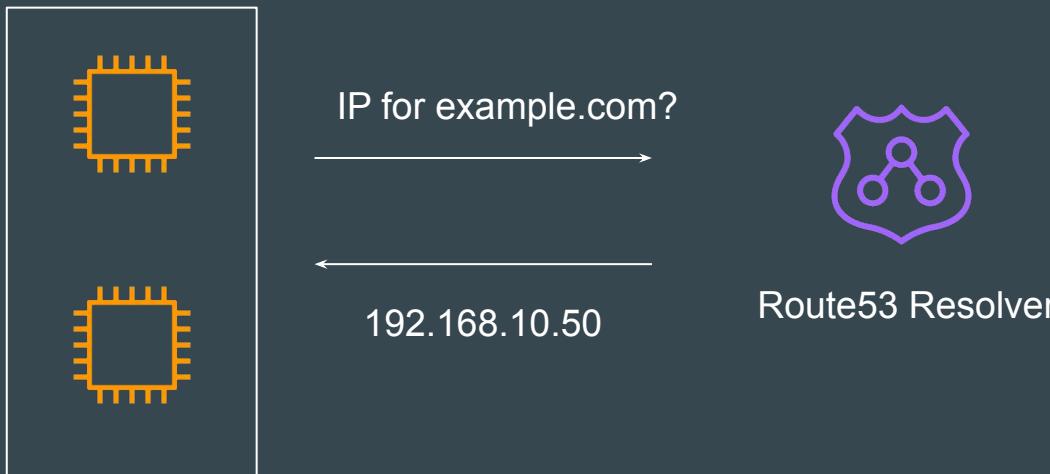
Depending on the TTL settings for the name servers for the parent domain, the propagation of your changes to DNS resolvers can take 48 hours or more.

# Route53 Resolver



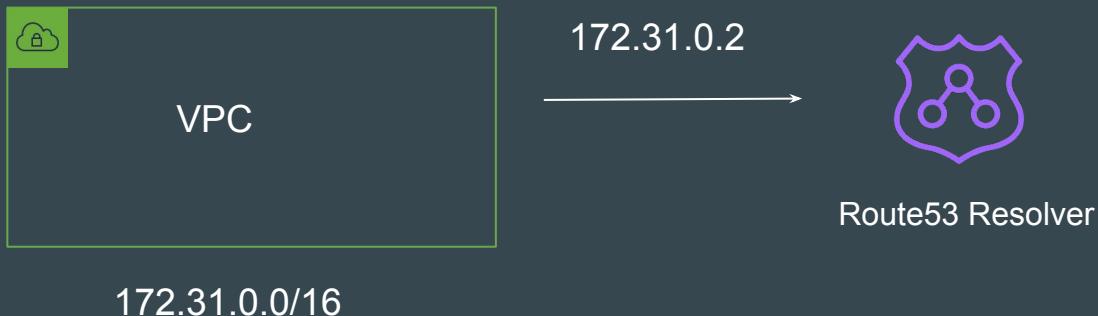
# Understanding the Basics

Amazon Route 53 Resolver **responds to DNS queries** from AWS resources for public records, Amazon VPC-specific DNS names, and Amazon Route 53 private hosted zones, and is available by default in all VPCs.



# Address of Route53 Resolver

An Amazon VPC connects to a Route 53 Resolver at a **VPC+2** IP address.



Contents of `/etc/resolv.conf` file of EC2 instance.

```
[ec2-user@ip-172-31-86-117 ~]$ cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search ec2.internal
options timeout:2 attempts:5
nameserver 172.31.0.2
```

# Query Resolution

A Route 53 Resolver automatically answers DNS queries for:

1. Local VPC domain names for EC2 instances (for example, ec2-192-0-2-44.compute-1.amazonaws.com).
2. Records in private hosted zones (for example, acme.example.com).
3. For public domain names, Route 53 Resolver performs recursive lookups against public name servers on the internet.

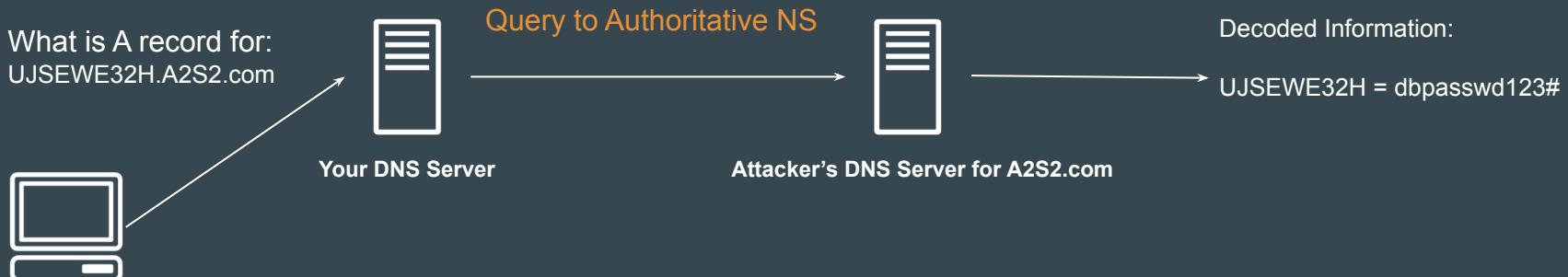
# Route 53 Resolver DNS Firewall



# DNS Exfiltration Attack

DNS data exfiltration is a way to exchange data between two computers without any direct connection.

The data is exchanged through DNS protocol on intermediate DNS servers.

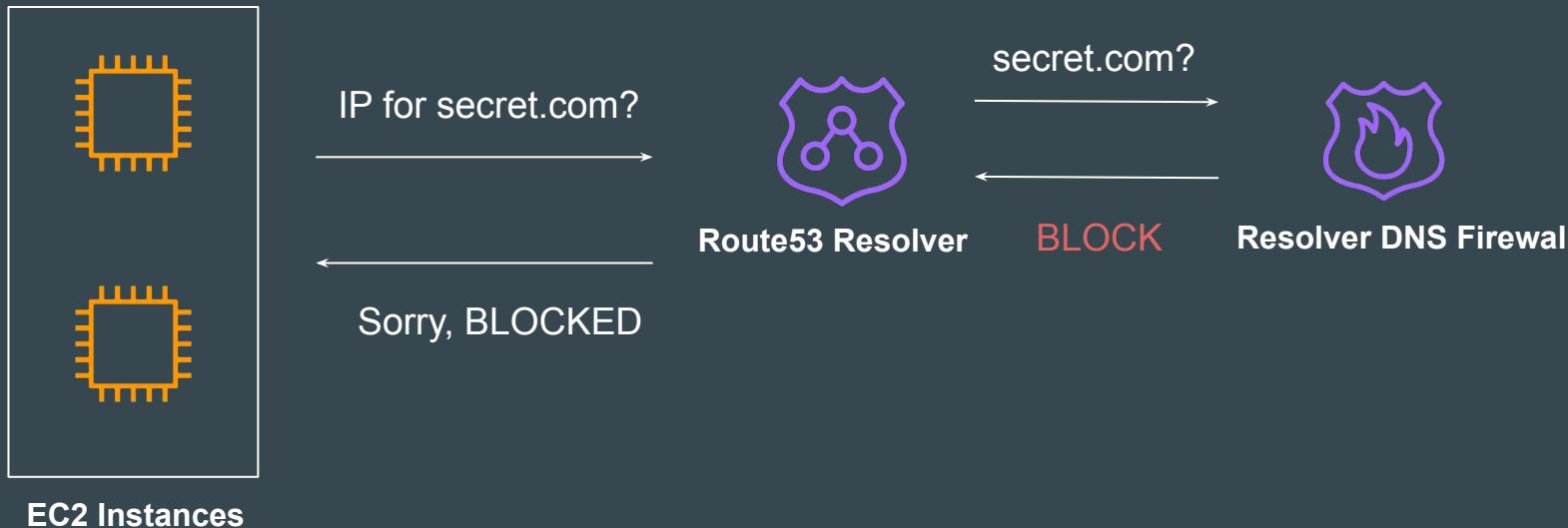


Encoded Stolen Information:

dbpasswd123# = UJSEWE32H

# Understanding the Basics

With Route 53 Resolver DNS Firewall, you can **filter and regulate outbound DNS traffic** for your virtual private cloud (VPC).



## Points to Note

You can deny access to the domains that you know to be bad and allow all other queries to pass through.

Alternately, you can deny access to all domains except for the ones that you explicitly trust.

You can use Firewall Manager to centrally configure and manage your DNS Firewall rule group associations for your VPCs across your accounts in AWS Organizations

A **primary use of DNS Firewall** protections is to help prevent DNS exfiltration of your data.

# AWS Managed Domain List

AWS Managed Domain Lists contain domain names that are associated with malicious activity or other potential threats.

AWS managed domain lists (3)		
These domain lists are in Region US East (N. Virginia).		
<input type="text"/> <input type="button" value="Search"/>		
Name	▲	ID
<input type="radio"/> AWSManagedDomainsAggregateThreatList		rslvr-fdl-15f4860b1ad54ead
<input type="radio"/> AWSManagedDomainsBotnetCommandAndControl		rslvr-fdl-aa970e9eb1ca4777
<input type="radio"/> AWSManagedDomainsMalwareDomainList		rslvr-fdl-2c46f2ecbfec4dcc

# Route53 Resolver Endpoints



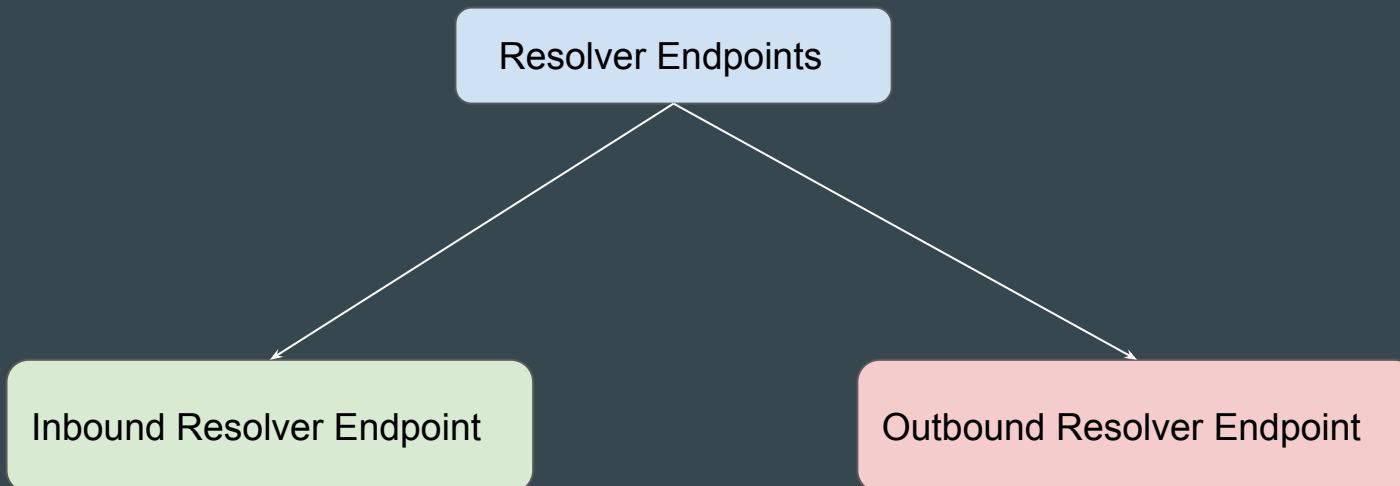
# Basics of Route53 Resolver Endpoints

AWS has released Route53 Resolver Endpoints that can allow resolution of private hosted zone domains from outside of the VPC.



# Types of Resolver Endpoints

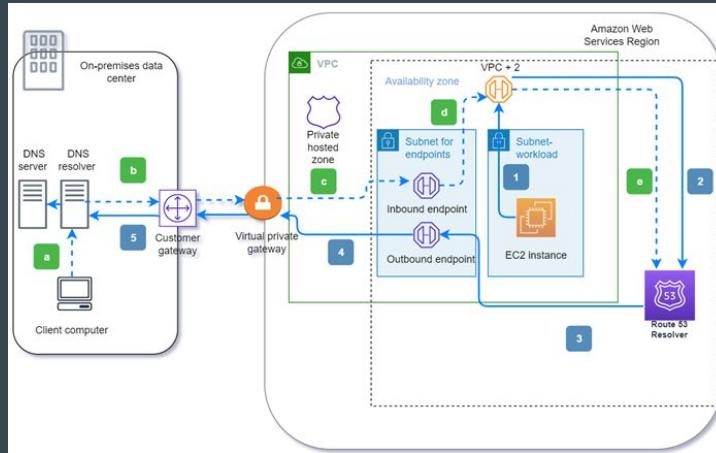
There are 2 primary types of Resolver Endpoints



# Understanding Resolver Endpoints

Inbound Resolver endpoints allow DNS queries to your VPC from your on-premises network or another VPC.

Outbound Resolver endpoints allow DNS queries from your VPC to your on-premises network or another VPC.

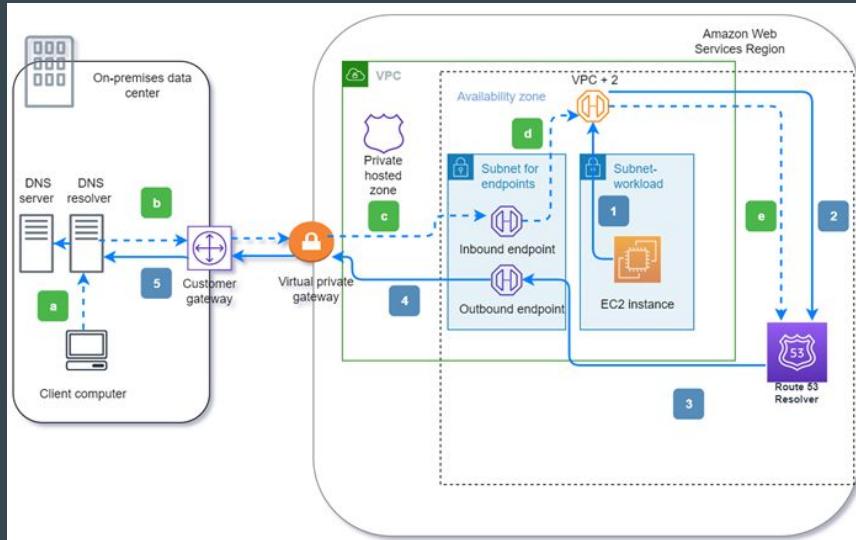


# Route53 Resolver - Inbound Endpoints



# Understanding Resolver Endpoints

Inbound Resolver endpoints allow DNS queries to your VPC from your on-premises network or another VPC.



# Inbound Endpoint Workflow - 1

1. A client in the on-premises data center needs to resolve a DNS query to an AWS resource for the domain dev.example.com. It sends the query to the on-premises DNS resolver.
2. The on-premises DNS resolver has a forwarding rule that points queries to dev.example.com to an inbound endpoint.
3. The query arrives at the inbound endpoint through a private connection, such as AWS Direct Connect or AWS Site-to-Site VPN, depicted as a virtual gateway.

## Inbound Endpoint Workflow - 2

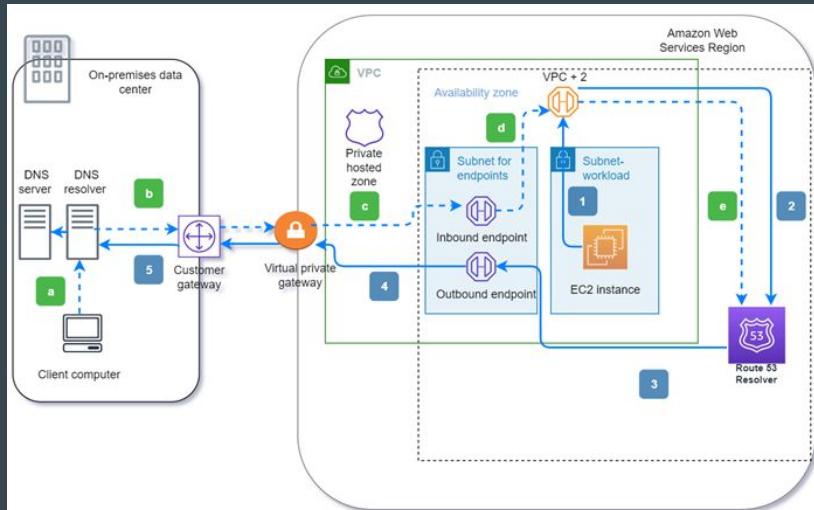
4. The inbound endpoint sends the query to Route 53 Resolver at the VPC +2.
5. Route 53 Resolver resolves the DNS query for dev.example.com and returns the answer to the client via the same path in reverse.

# Route53 Resolver - Outbound Endpoints



# Understanding Outbound Endpoints

Outbound Resolver endpoints allow DNS queries from your VPC to your on-premises network or another VPC.



# Outbound Endpoint Workflow - 1

1. An Amazon EC2 instance needs to resolve a DNS query to the domain internal.example.com. The authoritative DNS server is in the on-premises data center. This DNS query is sent to the VPC+2 in the VPC that connects to Route 53 Resolver.
2. A Route 53 Resolver forwarding rule is configured to forward queries to internal.example.com in the on-premises data center.
3. The query is forwarded to an outbound endpoint.

## Outbound Endpoint Workflow - 2

4. The outbound endpoint forwards the query to the on-premises DNS resolver through a private connection between AWS and the data center. The connection can be either AWS Direct Connect or AWS Site-to-Site VPN, depicted as a virtual private gateway.
5. The on-premises DNS resolver resolves the DNS query for internal.example.com and returns the answer to the Amazon EC2 instance via the same path in reverse.

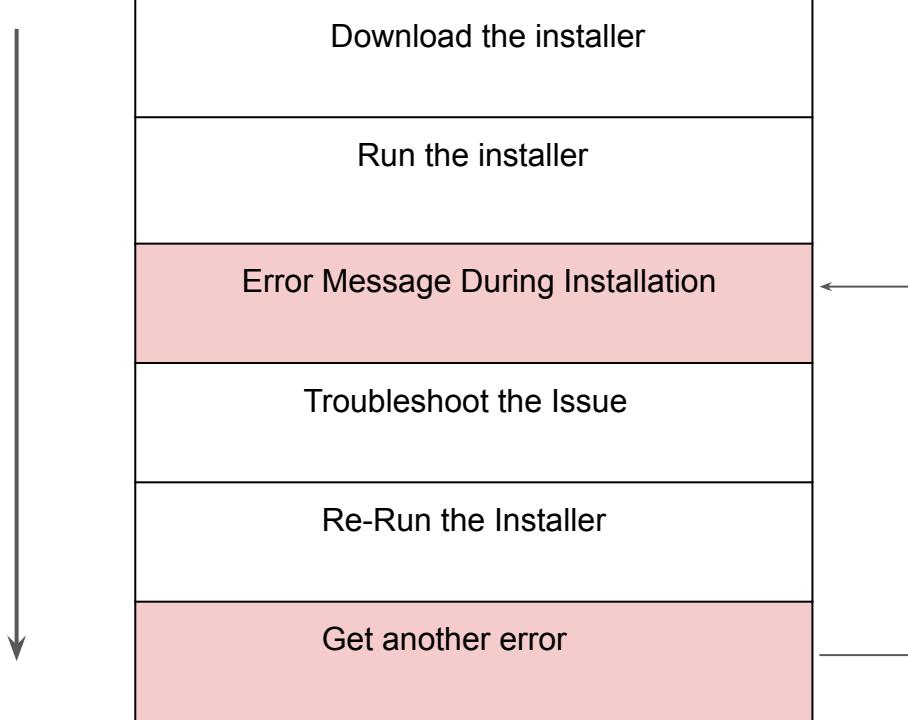
---

# Introduction to Docker

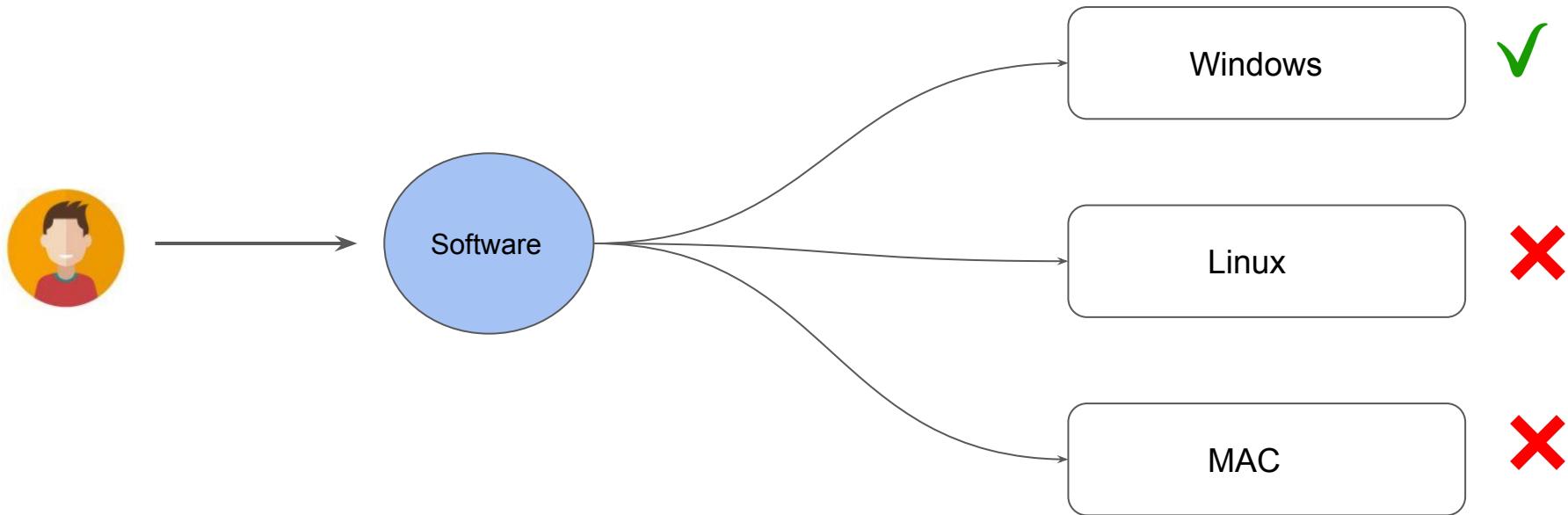
Build once, use anywhere

---

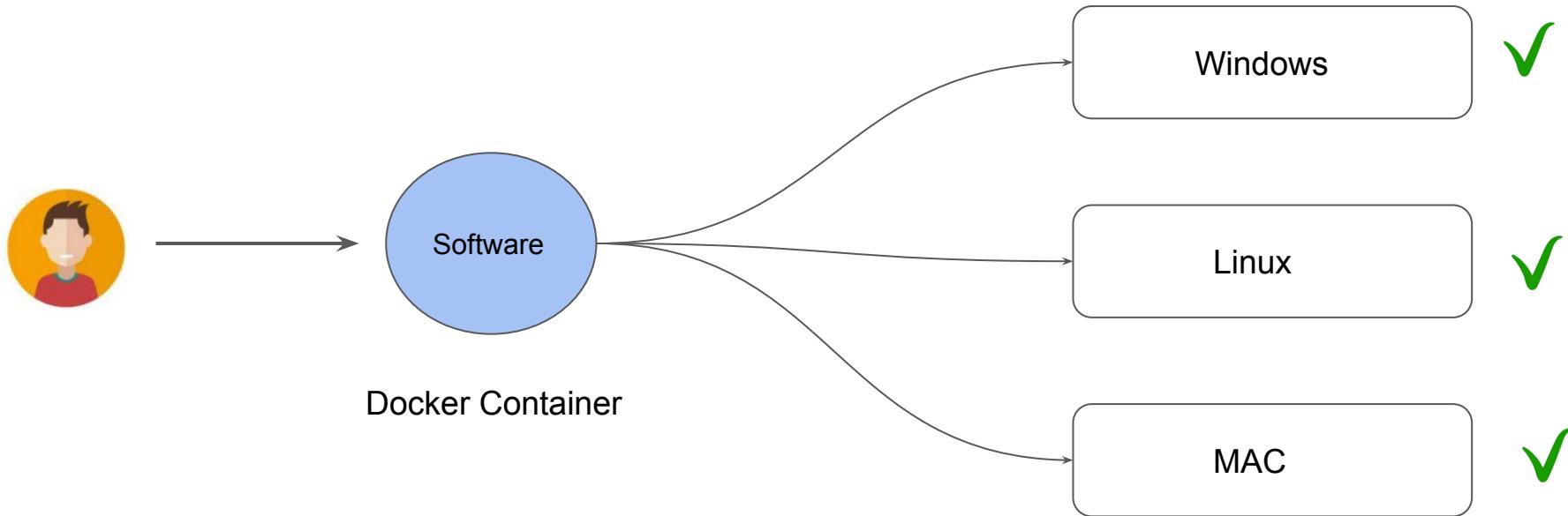
# Installation of Software Workflow



# What is Docker Trying to Achieve?



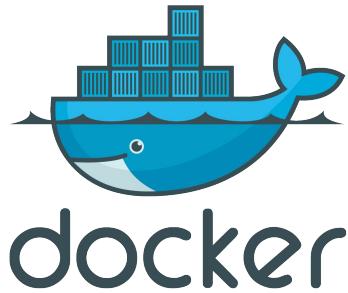
# What is Docker Trying to Achieve?



# Introduction

Docker is an open platform, once we build a docker container, we can run it anywhere, say it windows, linux, mac whether on laptop, data center or in cloud.

It follows the **build once, run anywhere** approach.

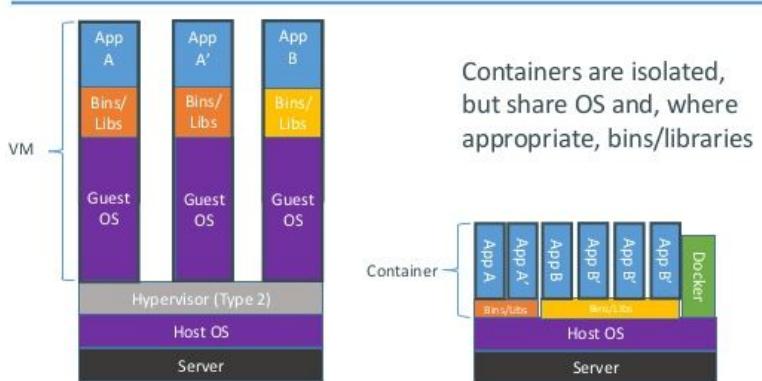


# Containers vs Virtual Machines

Virtual Machine contains entire Operating System.

Container uses the resource of the host operating system

## Containers vs. VMs



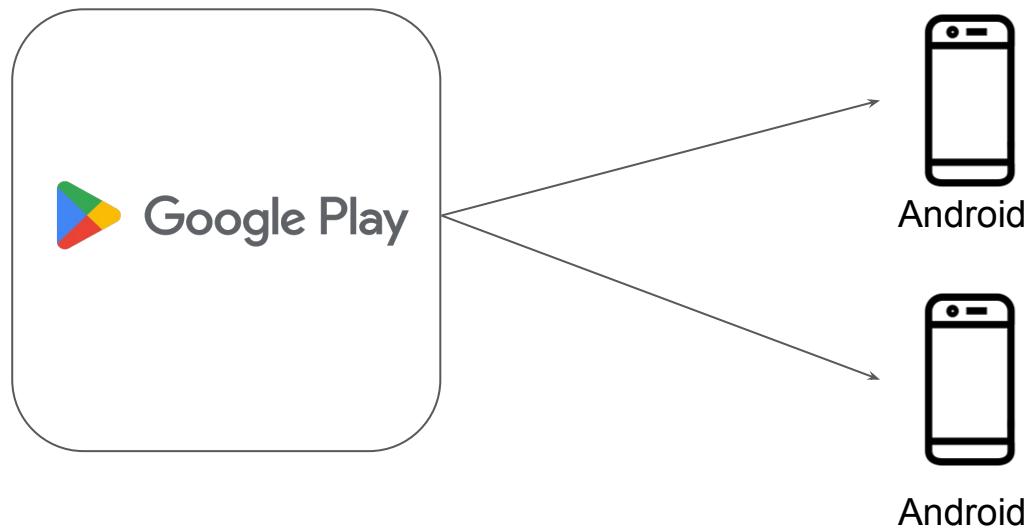
---

# Elastic Container Registry (ECR)

Storing Container Images

# Understanding with Analogy

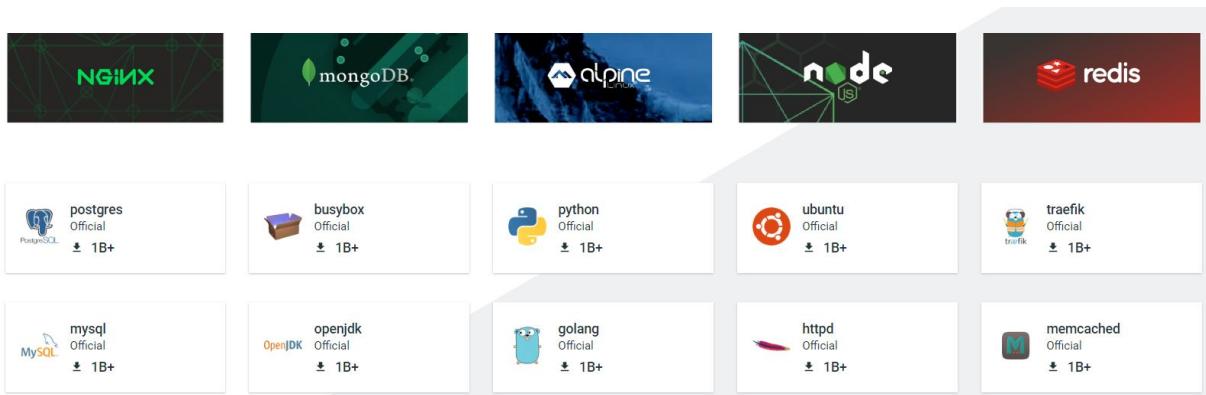
Google Play is an online store where people go to find their favorite apps, games, movies, TV shows, books, and more.



# Importance of Container Registry

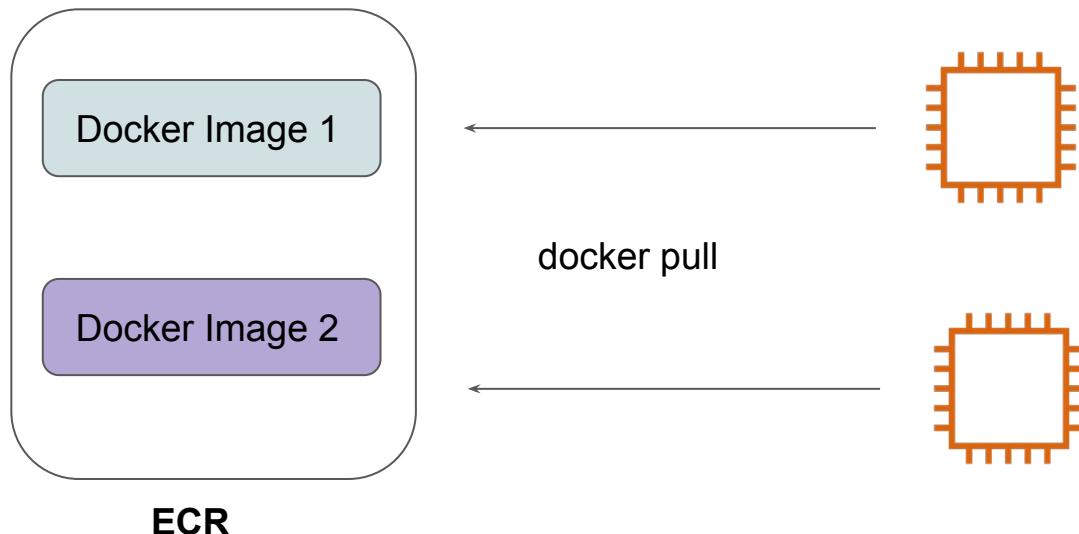
Container Registry is a single place for your team to manage Docker images.

Whenever you launch a Docker Container, the associated image is pulled from Registry.



# Basics of ECR

Amazon ECR is a fully managed container registry for storing Docker Images.



---

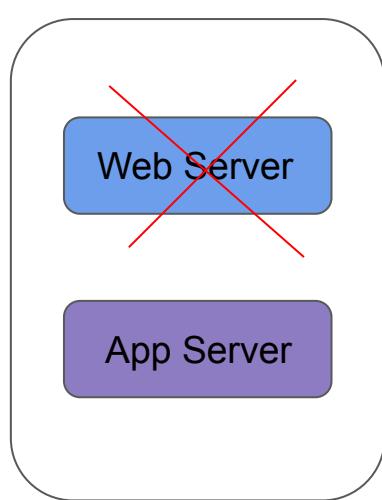
# Container Orchestration

Build once, use anywhere

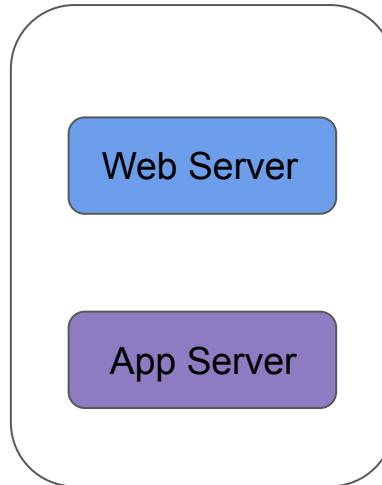
---

# Getting Started

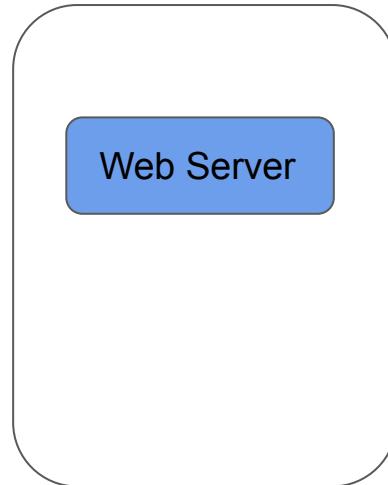
Container orchestration is all about managing the life cycles of containers, especially in large, dynamic environments.



VM 1

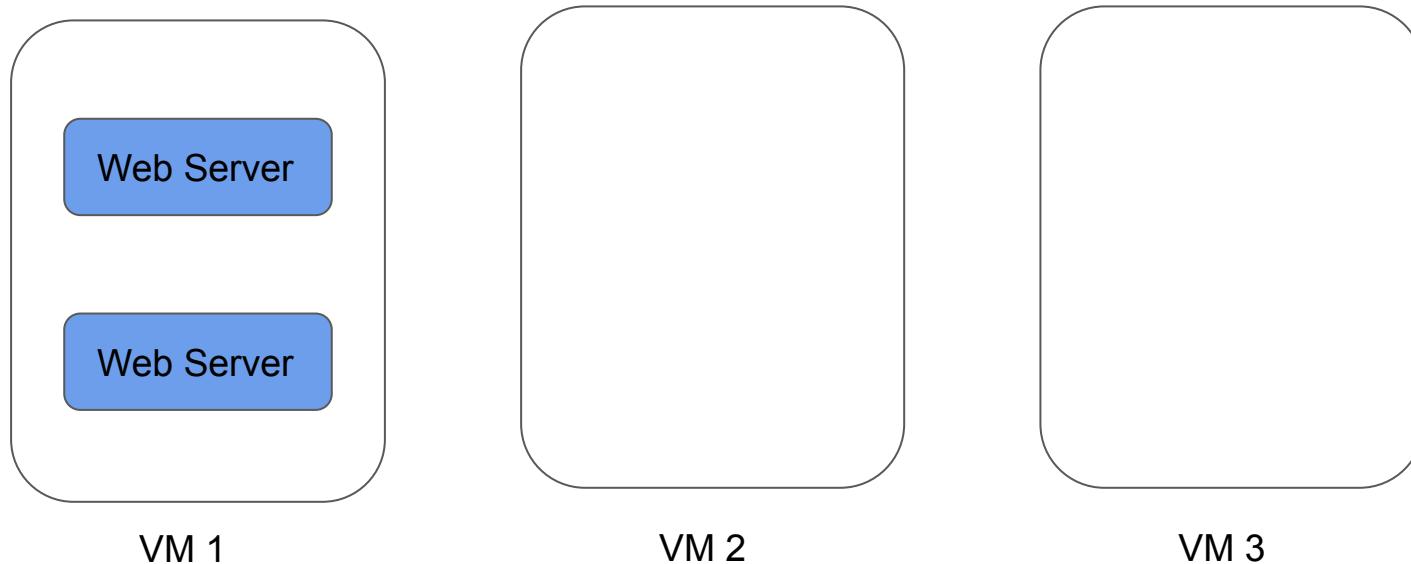


VM 2



VM 3

**Requirement:** Minimum of 2 web-server should be running all the time.



# Importance of Container Orchestration

Container Orchestration can be used to perform lot of tasks, some of them includes:

- Provisioning and deployment of containers
- Scaling up or removing containers to spread application load evenly
- Movement of containers from one host to another if there is a shortage of resources
- Load balancing of service discovery between containers
- Health monitoring of containers and hosts

# Container Orchestration Solutions

There are many container orchestration solutions which are available, some of the popular ones include:

- Docker Swarm
- Kubernetes
- Apache Mesos
- Elastic Container Service (AWS ECS)

There are also various container orchestration platforms available like EKS.

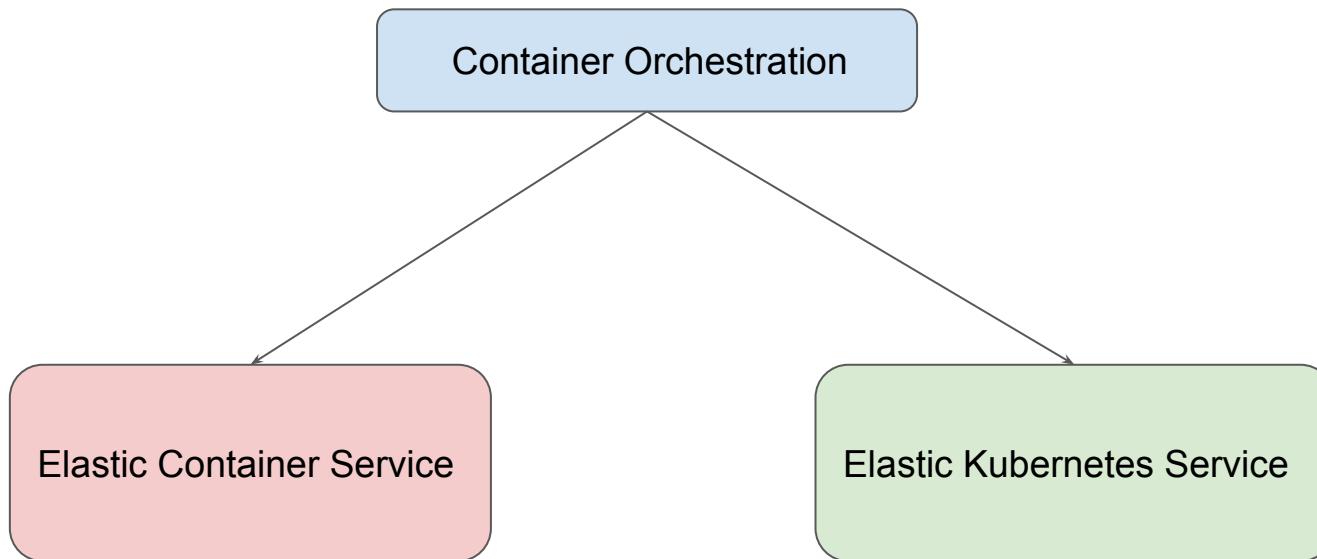
---

# Container Orchestration in AWS

## Choosing Right Orchestrator

# Container Orchestration in AWS

There are two primary services that are extensively used for container orchestration use-cases.



# Important Difference

<b>Pointers</b>	<b>AWS EKS</b>	<b>AWS ECS</b>
Open-Source	Yes	No
Complexity	More Complex	Less Complex
Community Support	More	Less

# Choosing Right Orchestrator

If you plan to work exclusively on AWS, you should choose ECS as it offers more in-depth AWS integration than Amazon EKS.

Organizations with limited expertise and insufficient resources to invest in learning Kubernetes can go with ECS.

If you plan to deploy containers across multiple platforms, you can choose EKS.

---

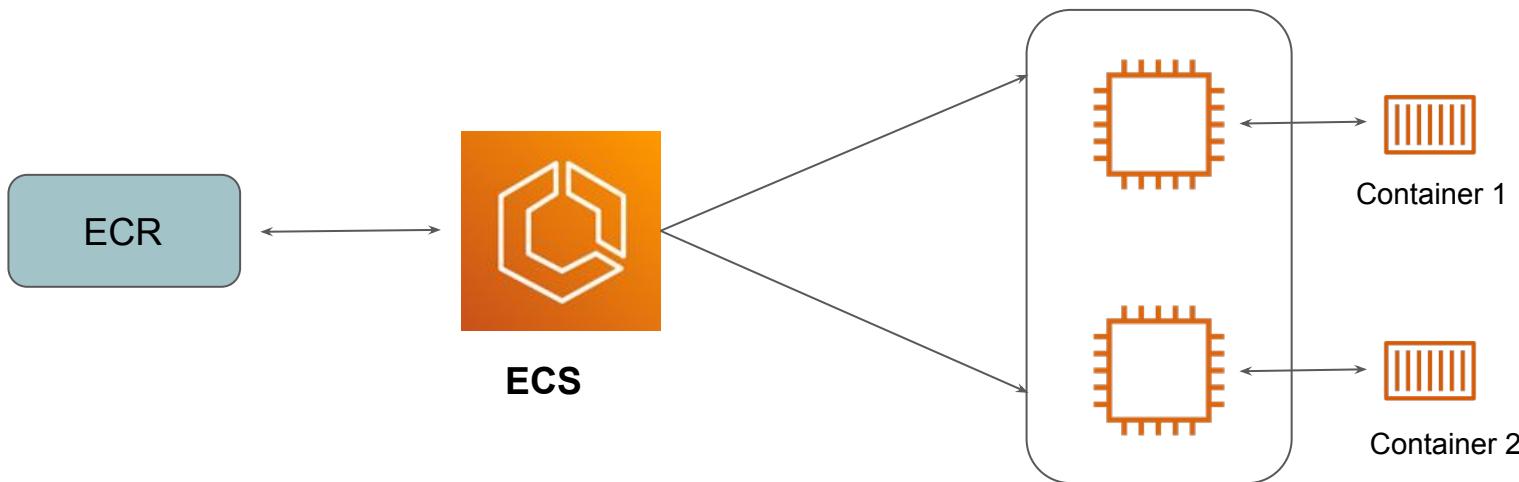
# Elastic Container Service (ECS)

Container Management

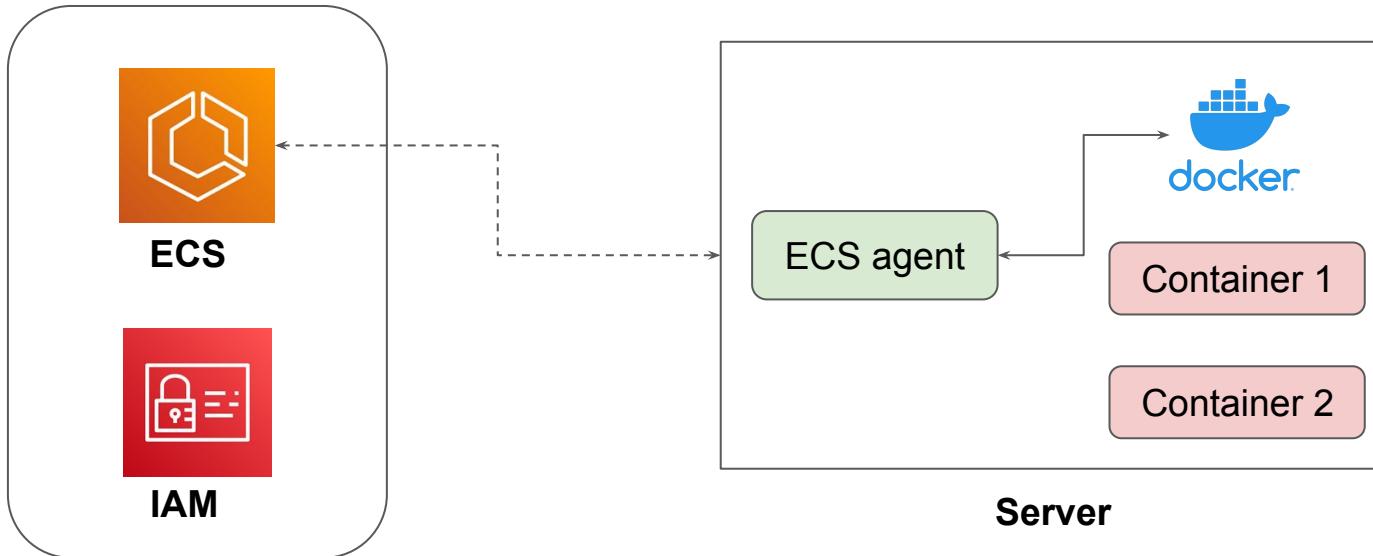
# Basics of Service

Amazon Elastic Container Service (Amazon ECS) is a highly scalable and fast container management service.

You can use it to run, stop, and manage containers on a cluster.



# High-Level Workflow



---

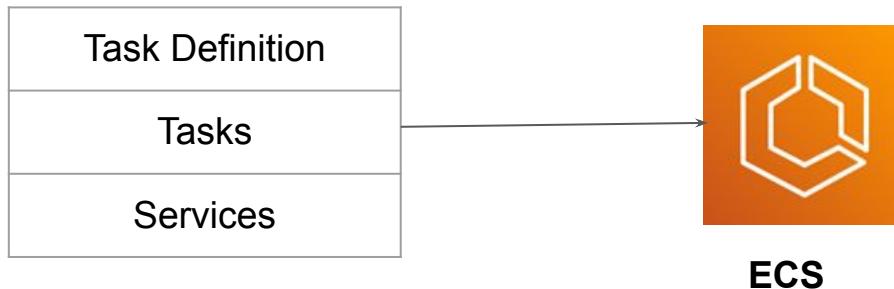
# Components of ECS

## Container Management

# Basic Components

There are three primary components of ECS Cluster:

Task Definition, Tasks and Service



# Component - Task Definition

A task definition is a text file that describes one or more containers that form your application.

It contains information like operating system, containers to use, ports to open, storage

**Container - 1** [Info](#)

[Essential container](#) [Remove](#)

**Container details**  
Specify a name, container image, and whether the container should be marked as essential. Each task definition must have at least one essential container.

Name	Image URI	Essential container
nginx	nginx:latest	Yes ▾

**Port mappings** [Info](#)  
Add port mappings to allow the container to access ports on the host to send or receive traffic. Any changes to port mappings configuration impacts the associated service connect settings.

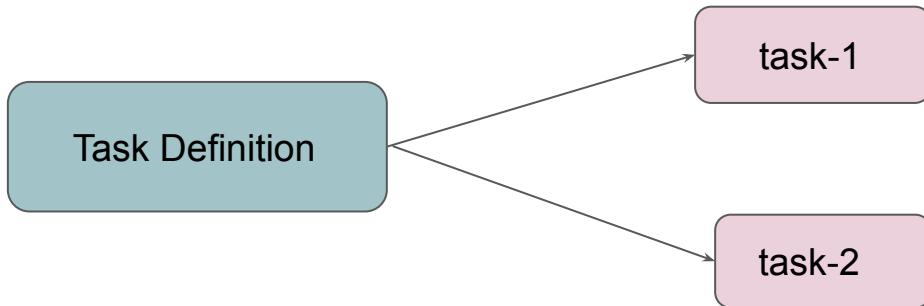
Host port	Container port	Protocol	
80	80	TCP ▾	<a href="#">Remove</a>

[Add more port mappings](#)

# Component - Task

A task is the instantiation of a task definition within a cluster.

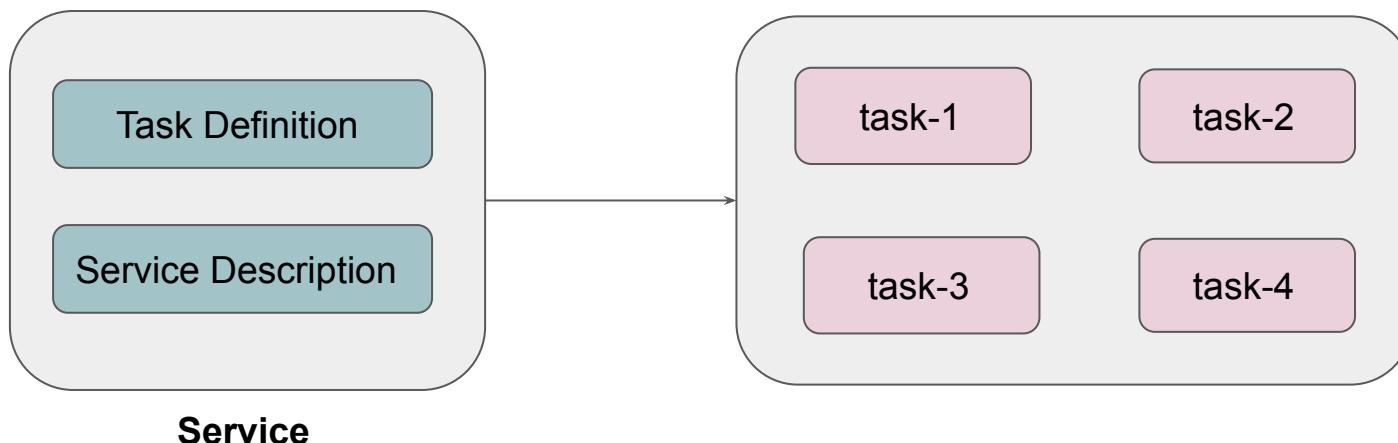
After you create a task definition for your application within Amazon ECS, you can specify the number of tasks to run on your cluster.



# Component - Service

Service to run and maintain your desired number of tasks simultaneously in an Amazon ECS cluster.

If any of your tasks fail or stop for any reason, the Amazon ECS service scheduler launches another instance based on your task definition



---

# Overview of Docker Networking

Build once, use anywhere

---

# Getting Started

Docker takes care of the networking aspects so that container can communicate with other containers and also with the Docker Host.

```
[root@docker-demo ~]# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.17.0.1 netmask 255.255.0.0 broadcast 0.0.0.0
        inet6 fe80::42:b6ff:fea6:f62b prefixlen 64 scopeid 0x20<link>
              ether 02:42:b6:a6:f6:2b txqueuelen 0 (Ethernet)
              RX packets 147774 bytes 42989090 (40.9 MiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 153893 bytes 273579092 (260.9 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 139.59.82.72 netmask 255.255.240.0 broadcast 139.59.95.255
        inet6 fe80::8838:79ff:feed:1335 prefixlen 64 scopeid 0x20<link>
              ether 8a:38:79:ed:13:35 txqueuelen 1000 (Ethernet)
              RX packets 822197 bytes 2191970977 (2.0 GiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 634774 bytes 44815091 (42.7 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

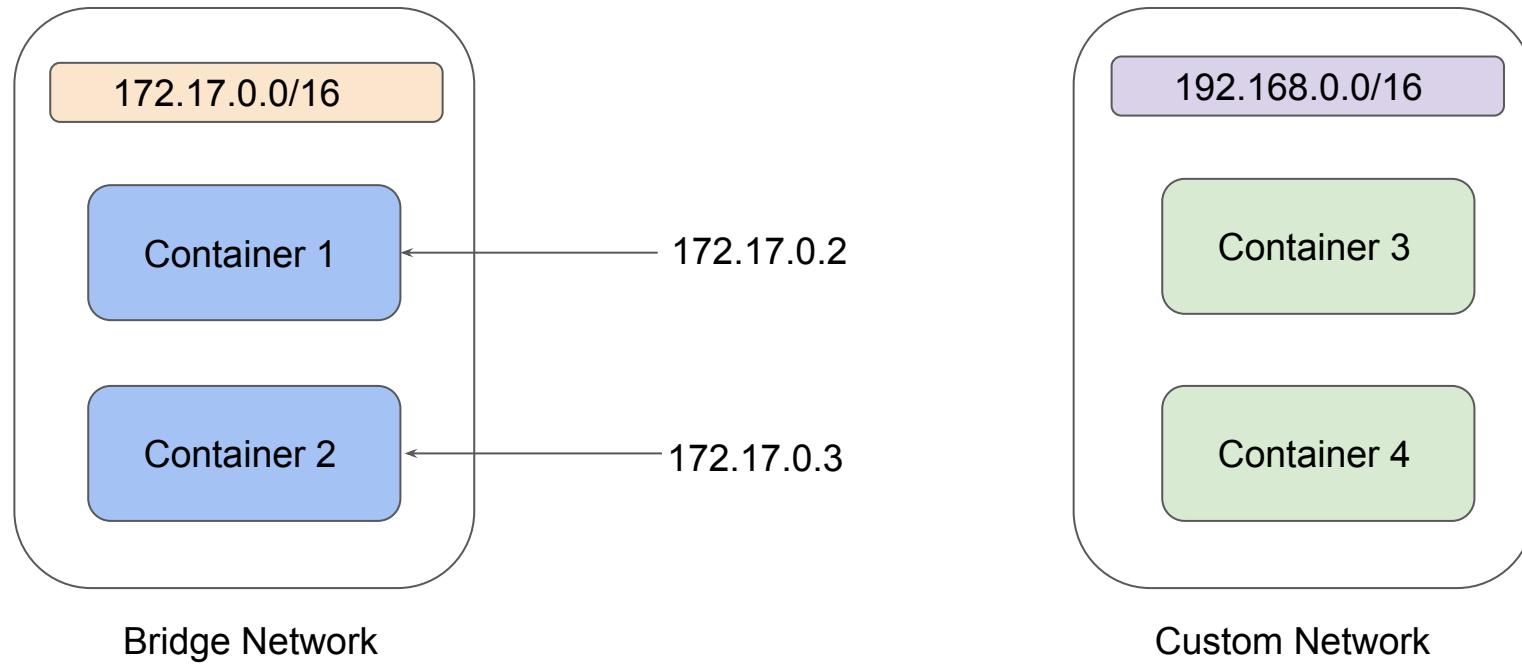
# Overview of Network Drivers

Docker networking subsystem is pluggable, using drivers.

There are several drivers available by default, and provides core networking functionality.

- bridge
- host
- overlay
- macvlan
- none

# Diagrammatic Representation



---

# ECS Networking

## Container Management

# Let's Network

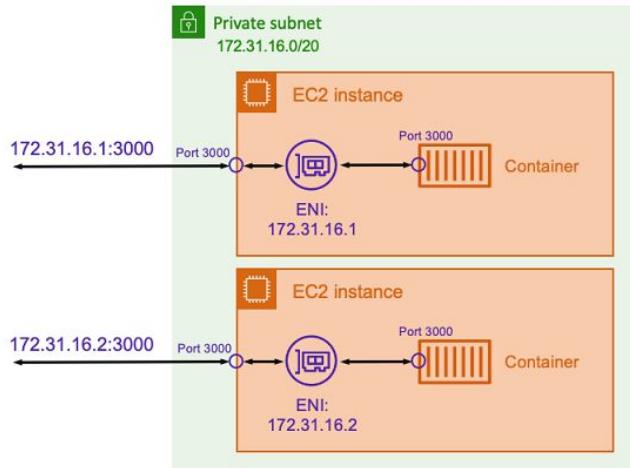
There are 3 primary networking mode that you can use in ECS

Network Mode	Description
Host Mode	The networking of the container is tied directly to the underlying host that's running the container.
Bridge Mode	The bridge network mode allows you to use a virtual network bridge to create a layer between the host and the networking of the container.
AWS VPC Mode	With the awsvpc network mode, Amazon ECS creates and manages an Elastic Network Interface (ENI) for each task and each task receives its own private IP address within the VPC.

# Host Mode (Not Recommended)

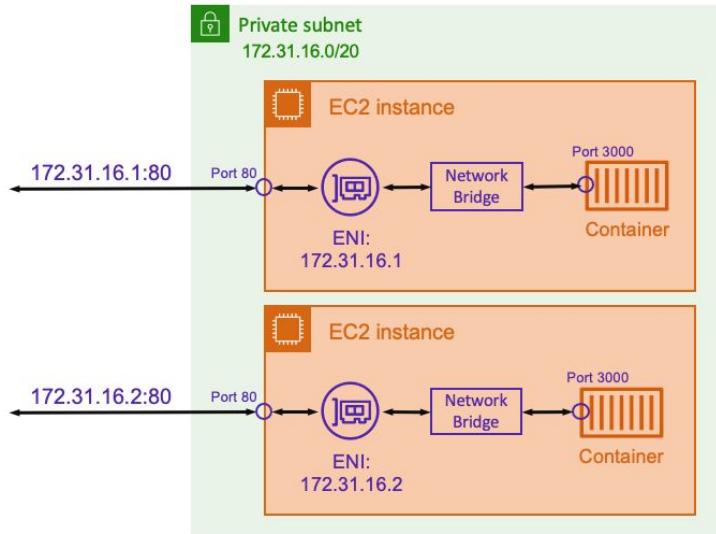
The networking of the container is tied directly to the underlying host that's running the container.

To connect to container: HOST IP + Port



# Bridge Mode

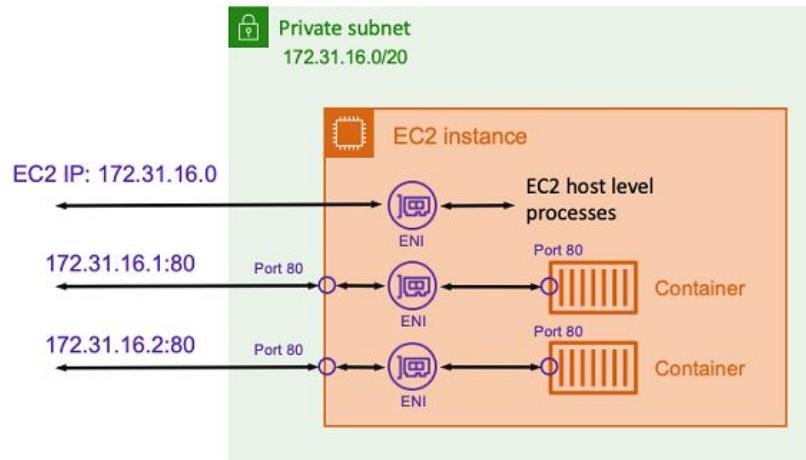
With bridge mode, you're using a virtual network bridge to create a layer between the host and the networking of the container.



# AWS VPC Mode

Amazon ECS creates and manages an Elastic Network Interface (ENI) for each task and each task receives its own private IP address within the VPC.

This ENI is separate from the underlying hosts ENI.



---

# Introduction to Kubernetes

Orchestrator Engine

---

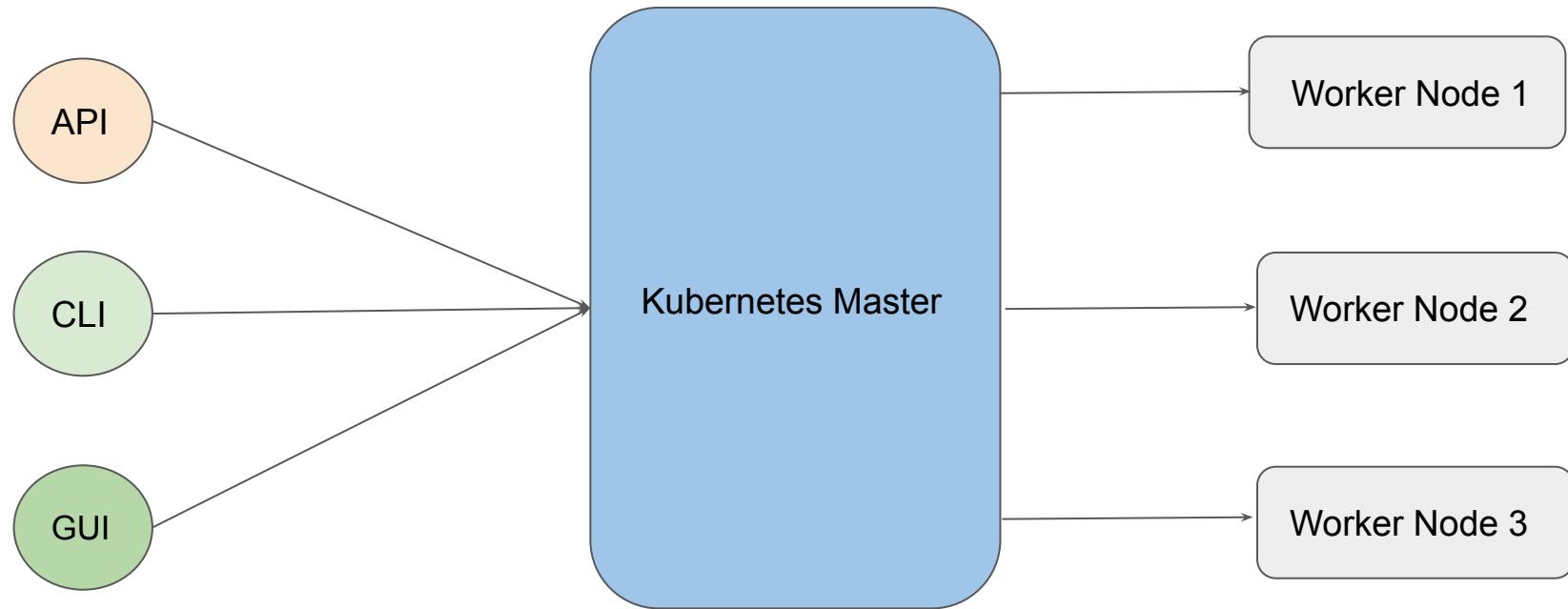
# Introduction to Kubernetes

Kubernetes (K8s) is an open-source container orchestration engine developed by Google.

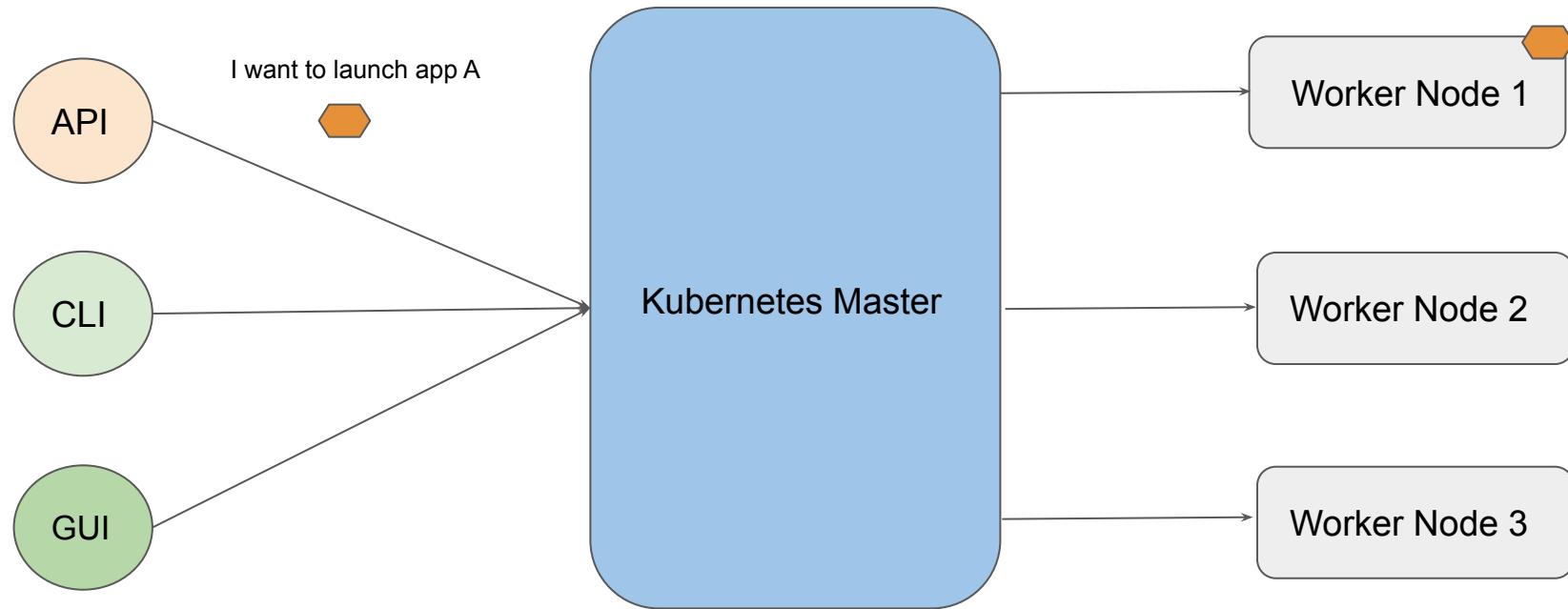
It was originally designed by Google, and is now maintained by the Cloud Native Computing Foundation.



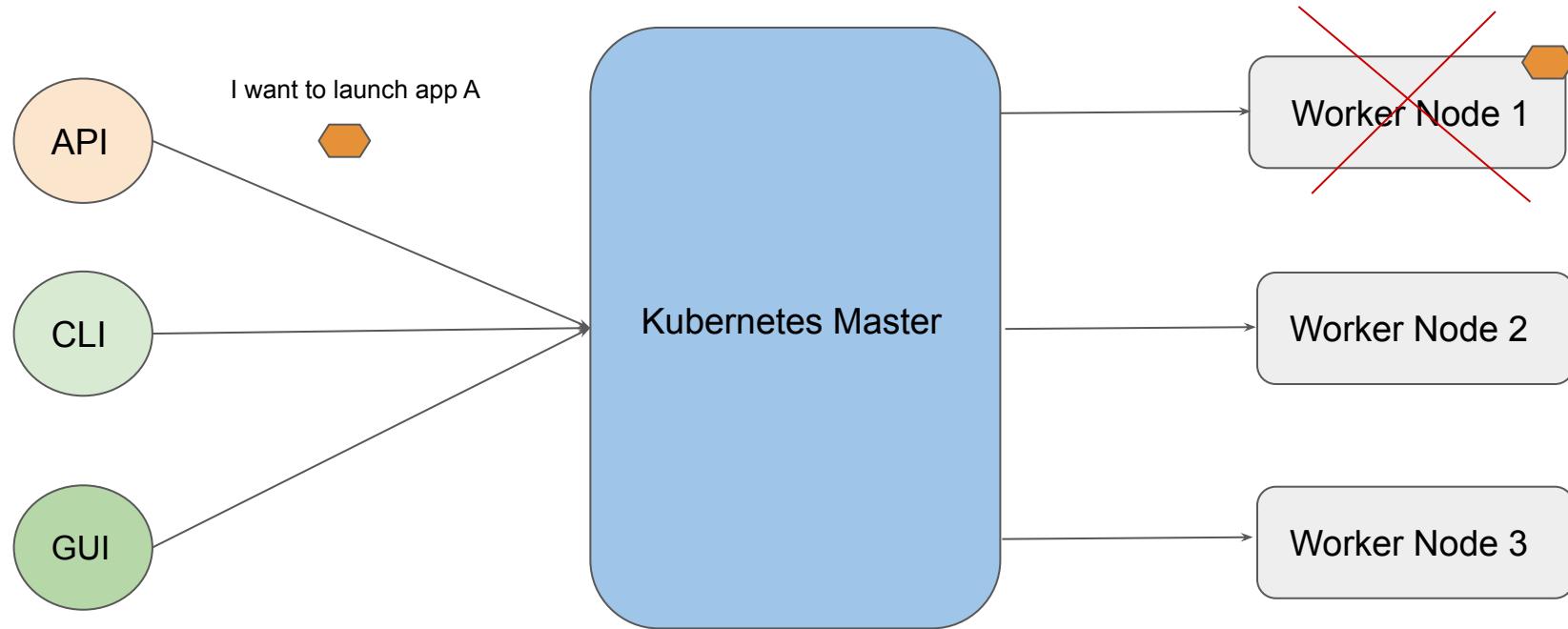
# Architecture of Kubernetes



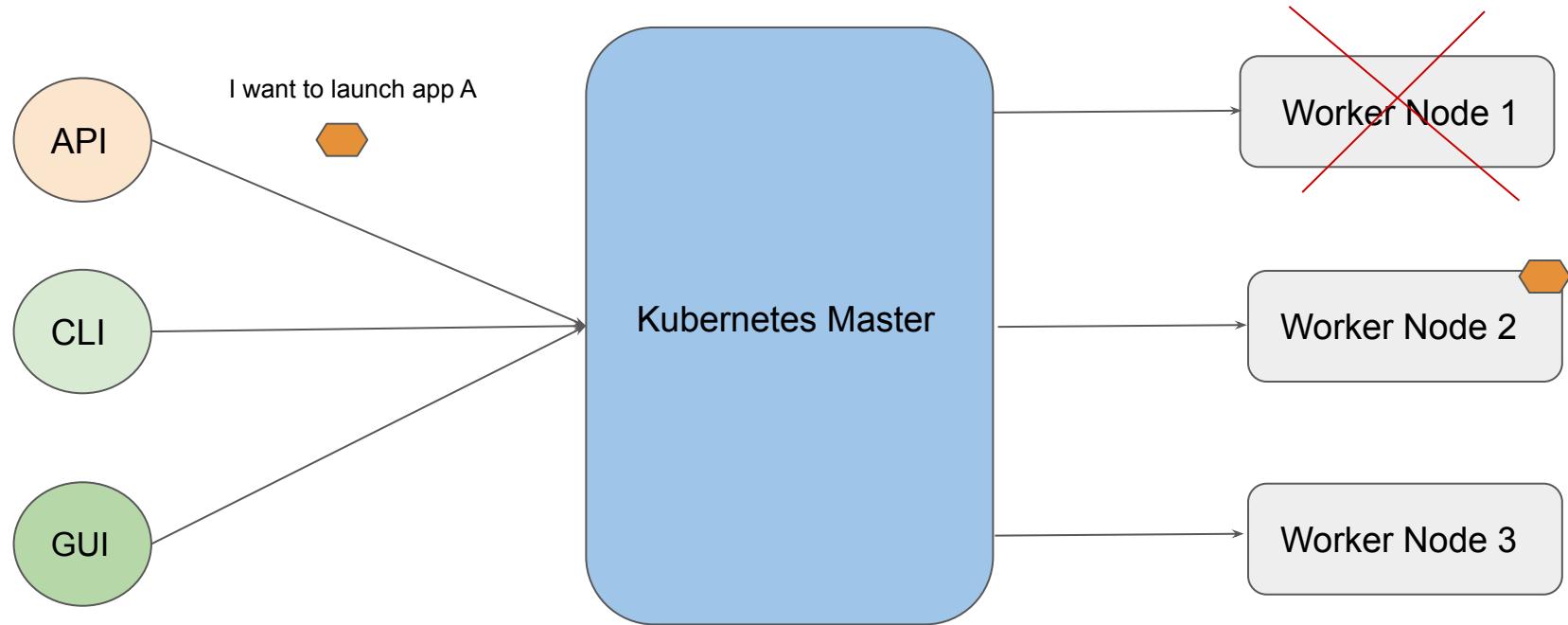
# Architecture of Kubernetes



# Architecture of Kubernetes



# Architecture of Kubernetes



---

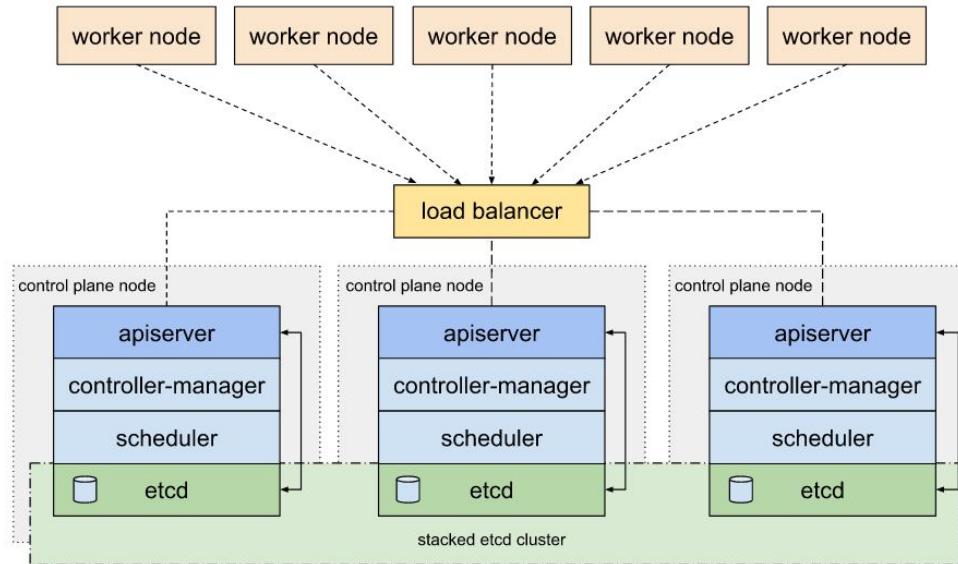
# Elastic Kubernetes Service

Managed Kubernetes in AWS

---

# Operating Kubernetes is Hard

Building and Maintaining entire Kubernetes cluster takes lot of time and resources.

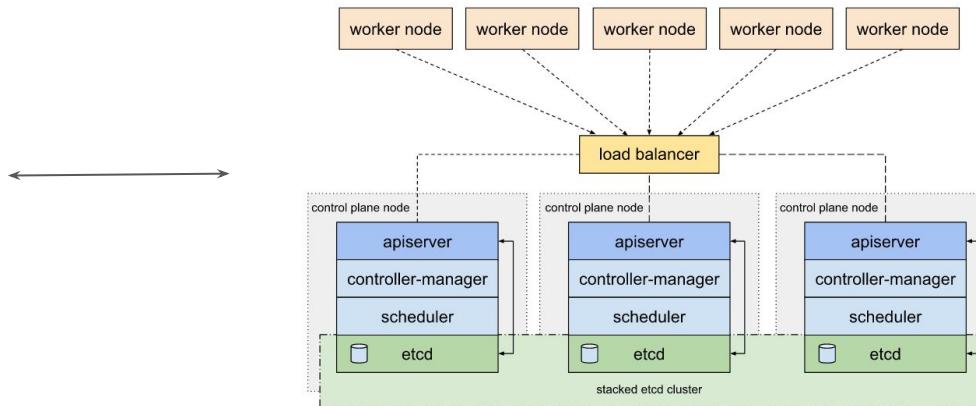


# Understanding the Basics

Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service that you can use to run Kubernetes on AWS.

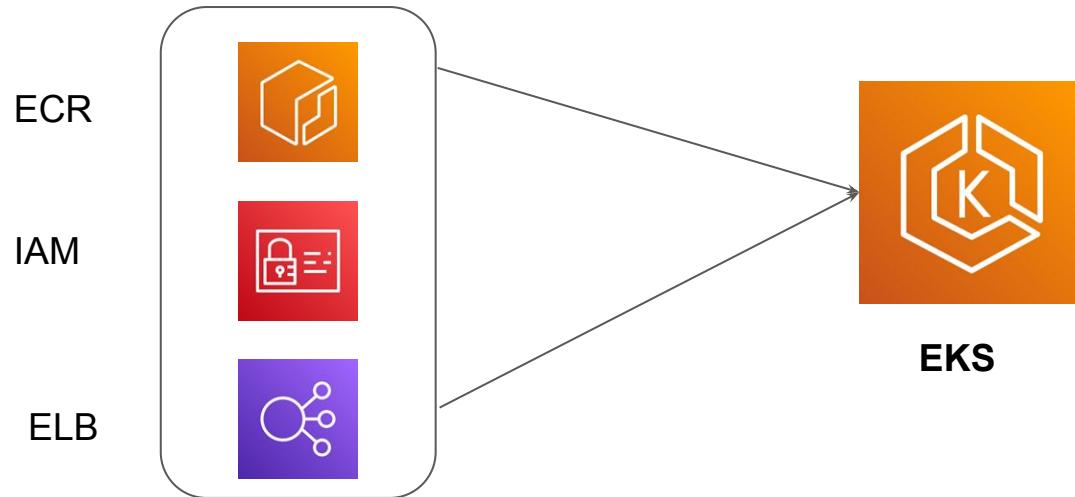


EKS



# Benefits of EKS

EKS provides tight integration with various other AWS services like ECR, IAM, ELB to provide end to end features for application deployments.



---

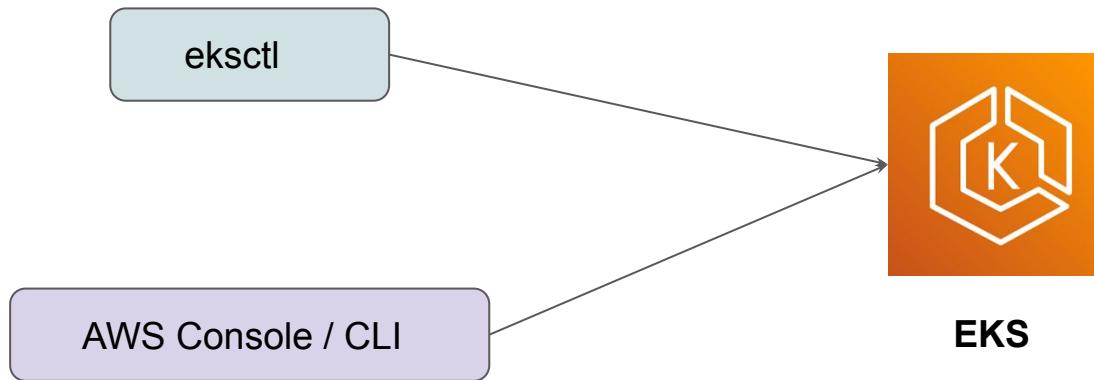
# EKS Practical Steps

Let's Create EKS Cluster

---

# Approaches to Create EKS Cluster

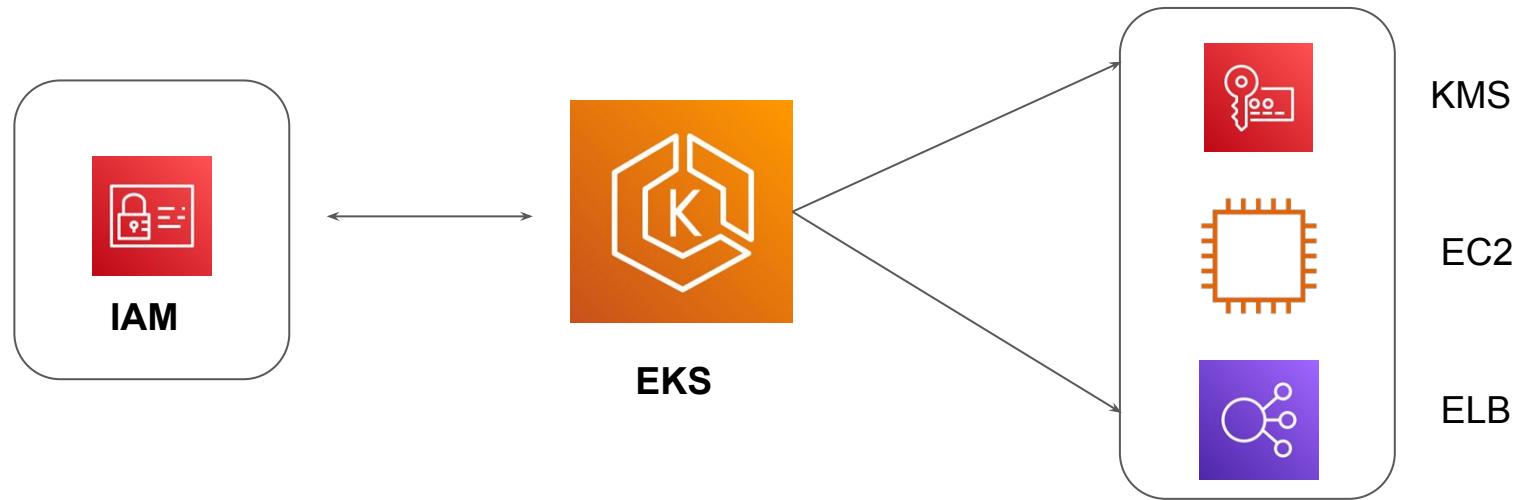
There are two primary ways to create EKS Cluster



# Step 1 - Build EKS Cluster

In this step, we build the base EKS Cluster.

Appropriate IAM Role needs to be associated so EKS can manage resource on your behalf.



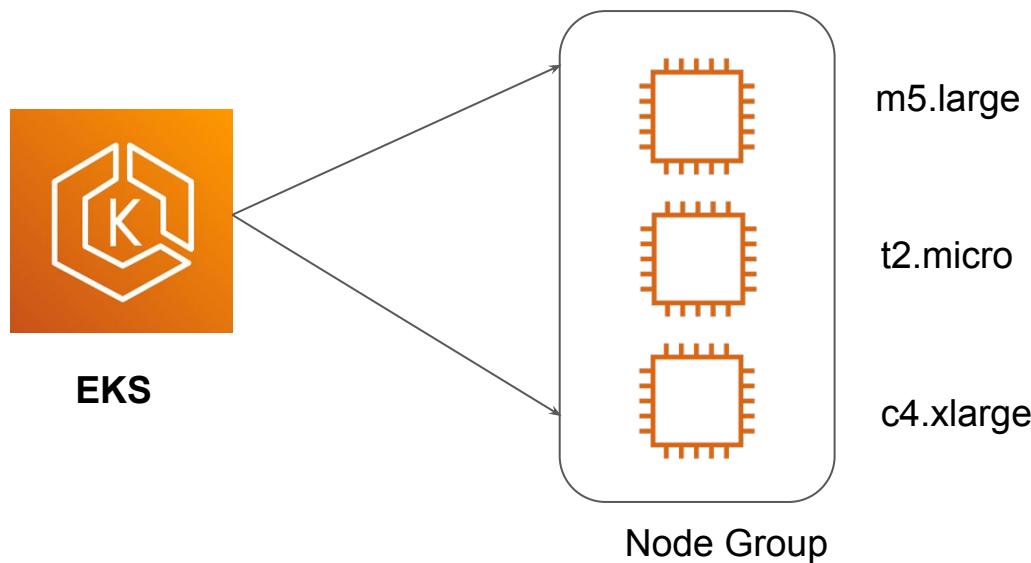
# Important Configuration - Building Cluster

Configs	Description
Kubernetes Version	Sets the K8s Version for your cluster.
Cluster Service Role	Allows EKS to manage resources.
VPC	VPC for cluster resources.
Cluster Endpoint Access	Public / Private Access to EKS Cluster.
Networking Add-Ons	To Configure appropriate networking in cluster.
Logging	Enable Logging for K8s Components.

## Step 2 - Create Node Group

A node group is a group of EC2 instances that supply compute capacity to your Amazon EKS cluster.

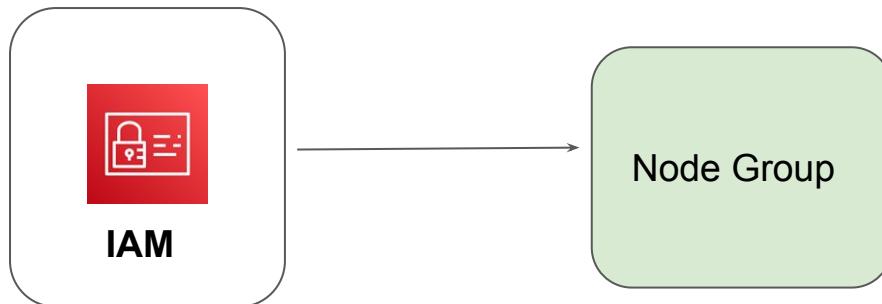
Configuration: AMI ID, Instance Type, Auto-Scaling Configuration, Disk Size.



# IAM Role for NodeGroup

An IAM Role needs to be associated with NodeGroup to ensure EC2 instance can perform following operations:

Fetch Images from ECR, Manage Network Interfaces, and others.



---

# EKS POD Networking

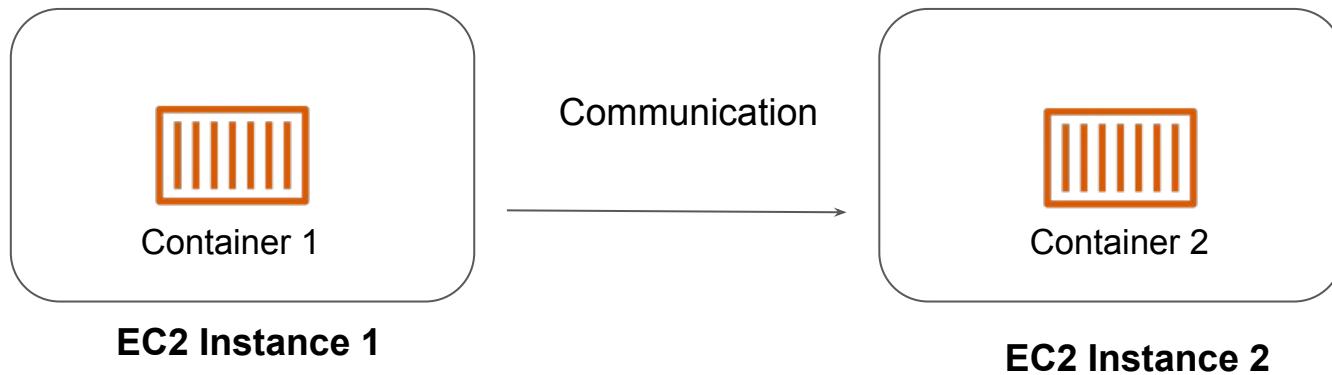
Communicate between Pods

---

# Understanding the Basics

In production environment, there is a necessity for PODS to be able to communicate to each other .

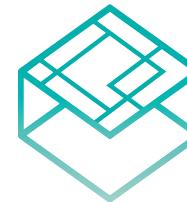
Appropriate networking needs to be setup to achieve this.



# Kubernetes Network Model

Important Requirements from Kubernetes side on how POD should communicate:

Every POD has its own IP address.
Container in one POD share the same network.
POD Communicate to other Pods without NAT



C N C F

# CNI Plugins

Container Network Interface consists of a specification and libraries for writing plugins to configure network interfaces in Linux containers, along with a number of supported plugins.

CNI concerns itself only with network connectivity of containers and removing allocated resources when the container is deleted

Popular Options: Calico, Weave



# Amazon VPC CNI plugin for Kubernetes

Amazon EKS supports native Amazon VPC networking using the [Amazon VPC Container Network Interface \(CNI\) plugin](#) for Kubernetes. This plugin:

1. Creates elastic network interfaces (network interfaces) and attaches them to your Amazon EC2 nodes.
2. Assigns a private IPv4 or IPv6 address from your VPC to each pod and service.

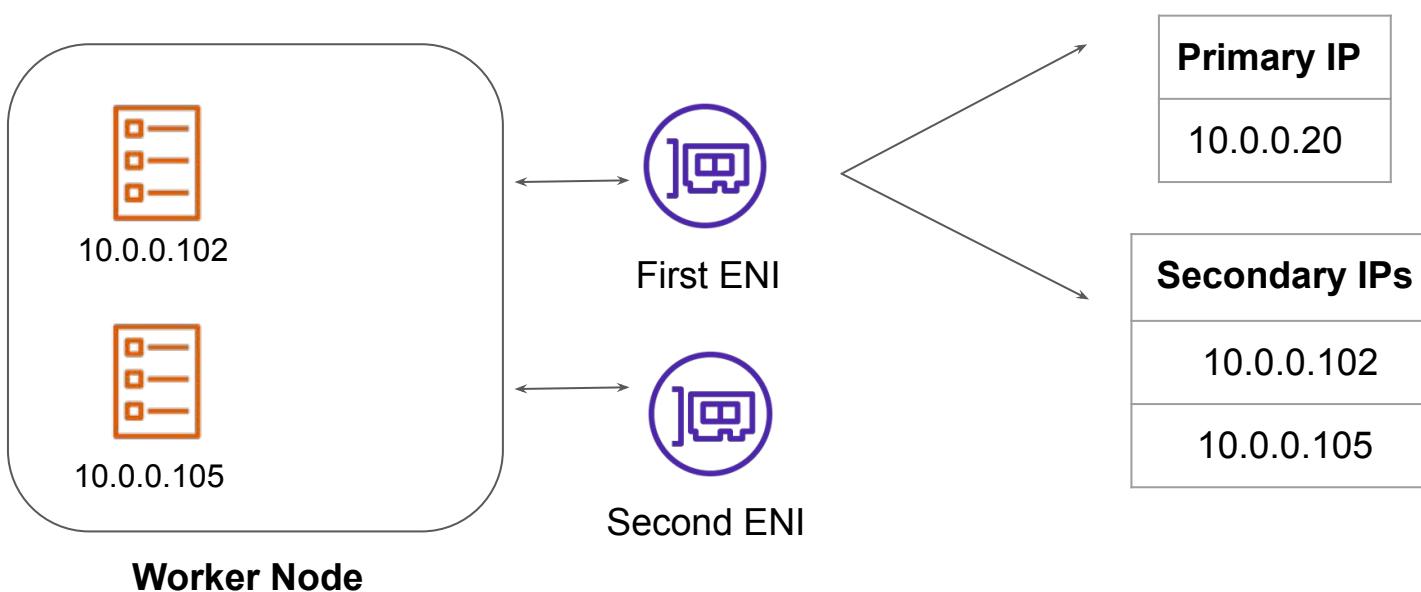
---

# VPC CNI Plugin

## Internal Working

# Basic Working

The Amazon VPC CNI plugin for Kubernetes is the networking plugin for pod networking in Amazon EKS clusters.



# Important Requirements

The plugin:

Requires AWS Identity and Access Management (IAM) permissions. If your cluster uses the IPv4 family, the permissions are specified in the AmazonEKS\_CNI\_Policy AWS managed policy.

# Important Requirements

The plugin:

Requires AWS Identity and Access Management (IAM) permissions. If your cluster uses the IPv4 family, the permissions are specified in the AmazonEKS\_CNI\_Policy AWS managed policy.

# Configuration Options

VPC CNI Plugin allows us to configure certain options to change the way plugin functions.

Some of the available options:

<b>Configuration Options</b>	<b>Description</b>
Custom Networking	Create Network Interface in a different subnet.
Security Group for PODS	Custom Set of Security group for PODS

# Horizontal POD Autoscaler



# Recommended Videos for EKS Networking

[https://www.youtube.com/watch?v=V8DidcYmNmU&ab\\_channel=AWSEvents](https://www.youtube.com/watch?v=V8DidcYmNmU&ab_channel=AWSEvents)