DAYANANDA SAGAR UNIVERSITY
DEPARTMENT OF CST

AWS WEB SERVICES

MODULE-2
NETWORKING SERVICES

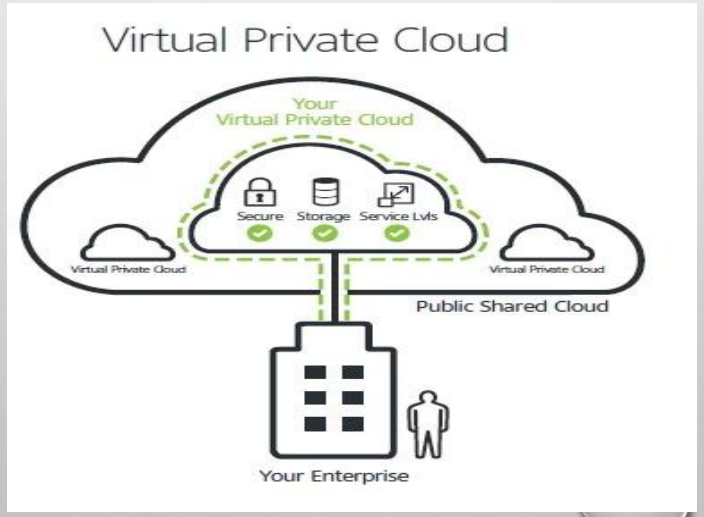
Module 2

Amazon VPC, Amazon Route 53

AMAZON VPC

WHAT IS AMAZON VPC ?

AMAZON VPC ENABLES YOU TO CONNECT YOUR ON-PREMISES RESOURCES TO AWS INFRASTRUCTURE THROUGH A VIRTUAL PRIVATE NETWORK. THIS VIRTUAL NETWORK CLOSELY RESEMBLES A TRADITIONAL NETWORK THAT YOU'D OPERATE IN YOUR DATA CENTER BUT ENABLES YOU TO LEVERAGE THE SCALABLE INFRASTRUCTURE IN AWS.



WHY VPC ?

- AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC) PROVIDES A LOGICALLY ISOLATED AREA OF THE AWS CLOUD WHERE YOU CAN LAUNCH AWS RESOURCES IN A VIRTUAL NETWORK THAT YOU DEFINE.

- YOU HAVE COMPLETE CONTROL OVER YOUR VIRTUAL NETWORKING ENVIRONMENT, INCLUDING A SELECTION OF YOUR IP ADDRESS RANGE, THE CREATION OF SUBNETS, AND CONFIGURATION OF ROUTE TABLES AND NETWORK GATEWAYS.

- YOU CAN EASILY CUSTOMIZE THE NETWORK CONFIGURATION FOR YOUR AMAZON VIRTUAL PRIVATE CLOUD. FOR EXAMPLE, YOU CAN CREATE A PUBLIC-FACING SUBNET FOR WEB SERVERS THAT CAN ACCESS TO THE INTERNET AND CAN ALSO PLACE YOUR BACKEND SYSTEM SUCH AS DATABASES OR APPLICATION SERVERS TO A PRIVATE-FACING SUBNET.

- YOU CAN PROVIDE MULTIPLE LAYERS OF SECURITY, INCLUDING SECURITY GROUPS AND NETWORK ACCESS CONTROL LISTS, TO HELP CONTROL ACCESS TO AMAZON EC2 INSTANCES IN EACH SUBNET.

WHY A VPC?

Privacy

Security

Prevents loss of Proprietary Data

The 3 most essential benefits you get from a **Virtual Private Cloud** are privacy, security and prevention from loss of proprietary data.

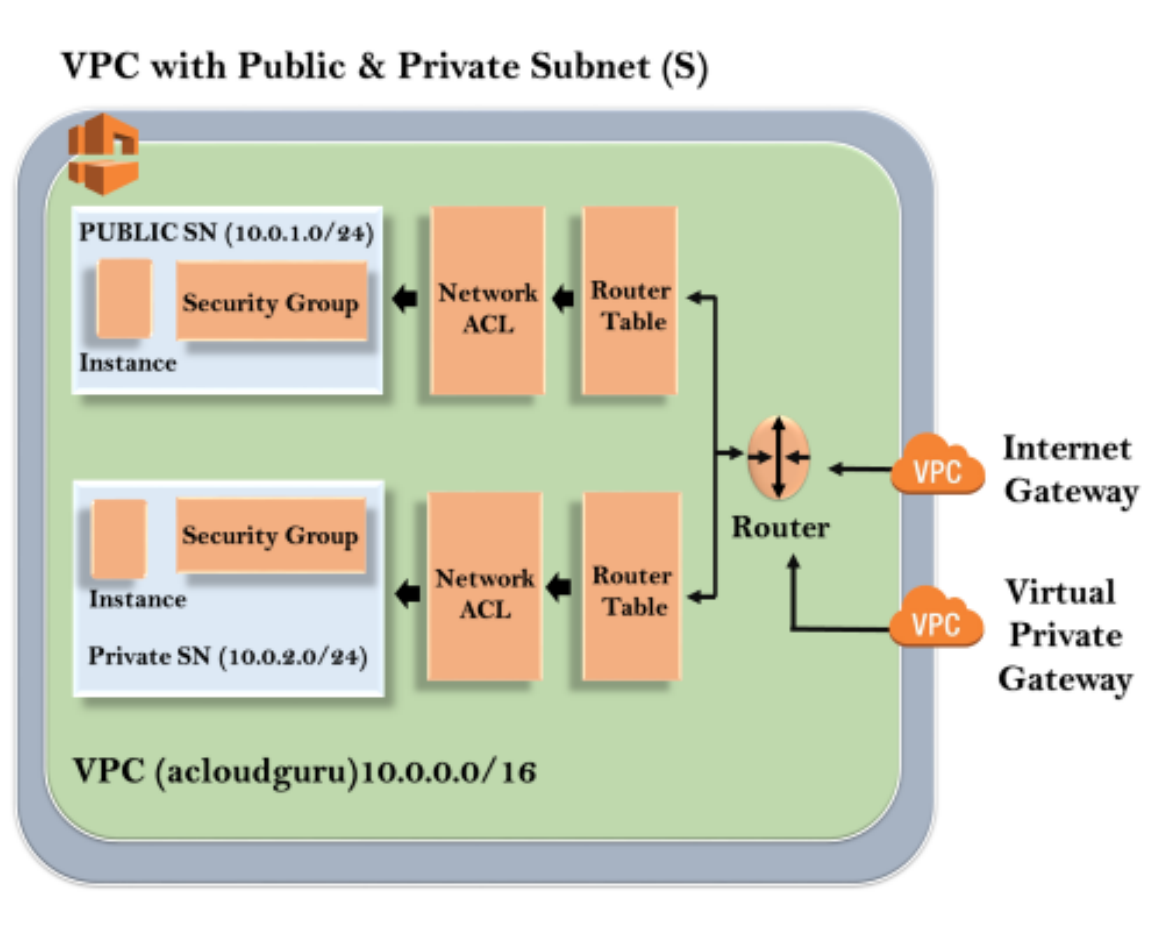
DIFFERENCE BETWEEN PRIVATE CLOUD AND VIRTUAL PRIVATE CLOUD

- A **PRIVATE CLOUD** IS SINGLE-TENANT A SERVICE EXCLUSIVELY OFFERED TO ONE ORGANIZATION.

- A **VIRTUAL PRIVATE CLOUD** IS A PRIVATE CLOUD WITHIN A PUBLIC CLOUD.

- WHILE THEY SOUND SIMILAR, IT'S IMPORTANT TO NOTE THAT THE TERMS 'PRIVATE CLOUD' AND 'VIRTUAL PRIVATE CLOUD' ARE NOT THE SAME.
- A PRIVATE CLOUD RUNS ON DEDICATED INFRASTRUCTURE WHICH MAY RESIDE ON-PREMISES IN A DEDICATED OFF-PREMISES DATA CENTRE – OR WITHIN A MANAGED CLOUD VENDOR. ADVANTAGES OF A PRIVATE CLOUD INCLUDE CONTROL AND EXCLUSIVITY. THERE ARE NO NEIGHBOURS TO SHARE HOSTED RESOURCES WITH.

ARCHITECTURE OF VPC

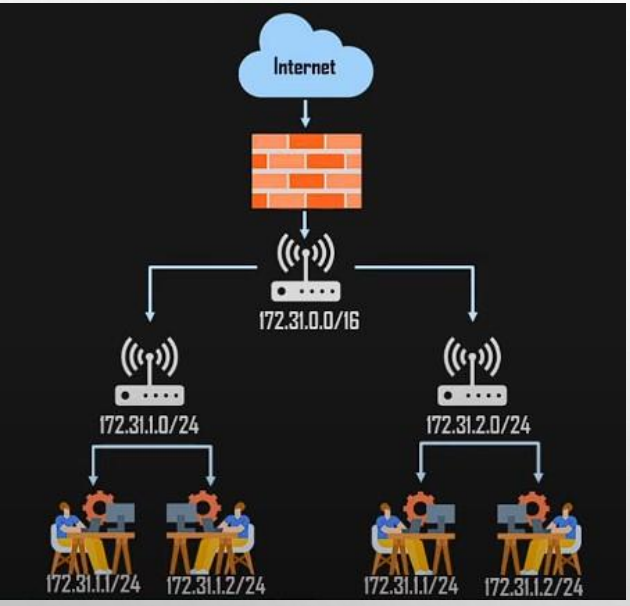


- THE OUTER LINE REPRESENTS THE REGION, AND THE REGION IS US-EAST-1. INSIDE THE REGION, WE HAVE VPC, AND OUTSIDE THE VPC, WE HAVE INTERNET GATEWAY AND VIRTUAL PRIVATE GATEWAY.
- INTERNET GATEWAY AND VIRTUAL PRIVATE GATEWAY ARE THE WAYS OF CONNECTING TO THE VPC. BOTH THESE CONNECTIONS GO TO THE ROUTER IN A VPC AND THEN ROUTER DIRECTS THE TRAFFIC TO THE ROUTE TABLE.
- ROUTE TABLE WILL THEN DIRECT THE TRAFFIC TO NETWORK ACL. NETWORK ACL IS THE FIREWALL OR MUCH LIKE SECURITY GROUPS.
- NETWORK ACL ARE STATE LIST WHICH ALLOWS AS WELL AS DENY THE ROLES. YOU CAN ALSO BLOCK THE IP ADDRESS ON YOUR NETWORK ACL.

- NOW, MOVE OVER TO THE SECURITY GROUP THAT ACCESSES ANOTHER LINE AGAINST THE EC2 INSTANCE. IT HAS TWO SUBNETS, I.E., PUBLIC AND PRIVATE SUBNET. IN PUBLIC SUBNET, THE INTERNET IS ACCESSIBLE BY AN EC2 INSTANCE, BUT IN PRIVATE SUBNET, AN EC2 INSTANCE CANNOT ACCESS THE INTERNET ON THEIR OWN. WE CAN CONNECT THE INSTANCES. TO CONNECT AN INSTANCE, MOVE OVER TO THE PUBLIC SUBNET AND THEN IT SSH TO THE PRIVATE SUBNET. THIS IS KNOWN AS JUMP BOXES. IN THIS WAY, WE CAN CONNECT AN INSTANCE IN PUBLIC SUBNET TO AN INSTANCE IN PRIVATE SUBNET.

COMPONETS OF VPC

1. SUBNET



- A SUBNET IS A LOGICAL DIVISION OF A LARGER NETWORK.
- IT IS A SMALLER PORTION OF THE NETWORK THAT TYPICALLY INCLUDES ALL THE MACHINES IN A CERTAIN AREA.
- WE CAN ADD AS MANY AS SUBNETS WE NEED IN ONE AVAILABILITY ZONE. EACH SUBNET MUST RESIDE ENTIRELY WITHIN ONE AVAILABILITY ZONE.
- THE PUBLIC SUBNETS WILL BE ATTACHED TO INTERNET GATEWAY WHICH ENABLES INTERNET ACCESS.
- THE PRIVATE SUBNETS WILL NOT HAVE INTERNET ACCESS.
- EACH AND EVERY SUBNET WHICH IS PRESENTED IN VPC MUST BE ASSOCIATED WITH THE ROUTING TABLE.

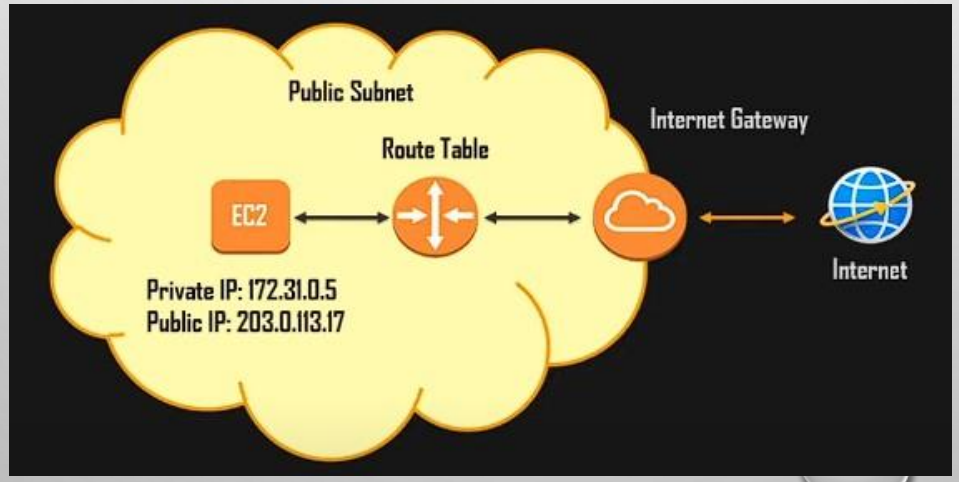
COMPONETS OF VPC

2. INTERNET GATEWAY

•THE INTERNET GATEWAY IS A VPC THAT HELPS INSTANCES TO COMMUNICATE OVER THE INTERNET USING TARGET PROVIDED IN THE ROUTE TABLE.

•WITH THE HELP OF IGW (INTERNET GATEWAY), THE RESOURCES PRESENT (E.G: EC2) IN THE VPC WILL ENABLE TO ACCESS THE INTERNET.

•ONE VPC CAN'T HAVE MORE THAN ONE IGW



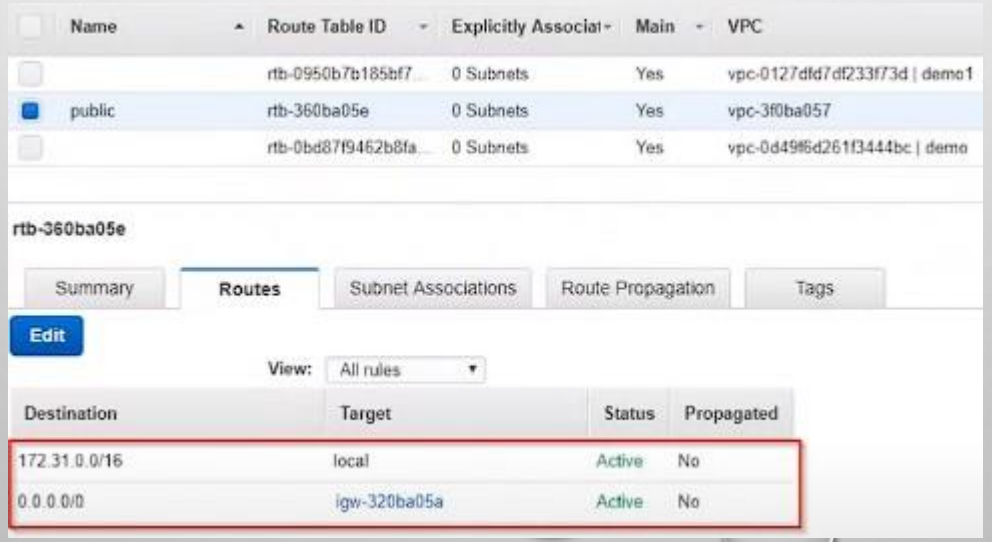
COMPONETS OF VPC

3. ROUTE TABLE

•ROUTE TABLE CONTAINS A SET OF RULES, CALLED ROUTE WHICH HELPS US TO ROUTE THE NETWORK TRAFFIC.

•A SINGLE VPC CAN HAVE AS MANY AS ROUTE TABLES IT REQUIRES.

•IF THE DEPENDENCIES ARE ATTACHED TO THE ROUTE TABLE THEN THEY CAN'T BE DELETED.

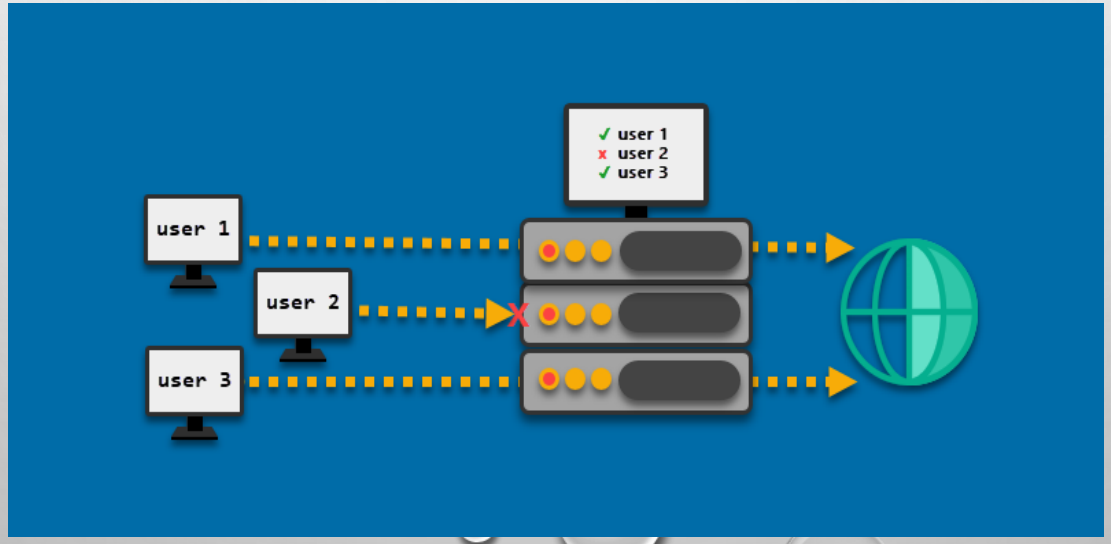


COMPONETS OF VPC

4. NETWORK ACCESS CONTROL

•THE NACL SECURITY LAYER FOR VPC SERVES AS A FIREWALL TO MANAGE TRAFFIC ENTERING AND LEAVING ONE OR MORE SUBNETS.

•THE NACL FOR THE DEFAULT VPC IS ACTIVE AND CONNECTED TO THE DEFAULT SUBNETS.



COMPONETS OF VPC

5. CLASSLESS INTER-DOMAIN ROUTING (CIDR)

•A TECHNIQUE FOR ALLOCATING IP ADDRESSES AND FOR IP ROUTING IS CALLED CLASSLESS INTER-DOMAIN ROUTING (CIDR), AND ITS RANGE IS 0-32.

•WHEN SETTING UP A VPC, WE MUST SPECIFY A SET OF IPV4 ADDRESSES USING CLASSLESS INTER-DOMAIN ROUTING (CIDR), FOR (EXAMPLE:10.0.0.0/16 FOR OUR VPC, THIS WILL SERVE AS THE MAIN CIDR BLOCK).

BENEFITS OF VPC

1. AMAZON PRIVATE CLOUD OFFERS ADVANCED SECURITY FEATURES INCLUDING SECURITY GROUPS AND NETWORK ACCESS CONTROLS
2. AWS VIRTUAL PRIVATE CLOUD IS EASY TO DEPLOY AND MANAGE VIA THE AWS MANAGEMENT CONSOLE
3. ABILITY TO SIMPLIFY WORKLOAD CLOUD MIGRATION WITH VMWARE (VIRTUAL MACHINES) CLOUD ON AWS
4. CUSTOMIZABLE IN ALLOWING USERS TO SELECT THEIR OWN IP ADDRESS RANGES AND CREATE SUBNET AS WELL AS CONFIGURE ROUTE TABLES AND NETWORK GATEWAYS. AWS ALSO ACCOMMODATES DNS (DOMAIN NAME SYSTEMS) VIA A DNS SERVER
5. AMAZON PRIVATE CLOUD IS CHARGED ON AN HOURLY BASIS

USE CASES OF VPC

1. USING VPC, YOU CAN HOST A PUBLIC-FACING WEBSITE, A SINGLE-TIER BASIC WEB APPLICATION, OR JUST A PLAIN OLD WEBSITE.
2. THE CONNECTIVITY BETWEEN OUR WEB SERVERS, APPLICATION SERVERS, AND DATABASE CAN BE LIMITED BY VPC WITH THE HELP OF VPC PEERING.
3. BY MANAGING THE INBOUND AND OUTBOUND CONNECTIONS, WE CAN RESTRICT THE INCOMING AND OUTCOMING SECURITY OF OUR APPLICATION.

WHAT IS AMAZON ROUTE 53 ?

AWS ROUTE 53 IS A HIGHLY AVAILABLE AND SCALABLE DNS WEB SERVICE. IT GIVES BUSINESSES AND DEVELOPERS A COST-EFFECTIVE WAY TO ROUTE END USERS TO INTERNET APPLICATIONS BY TRANSLATING THE DOMAIN NAMES INTO IP ADDRESSES

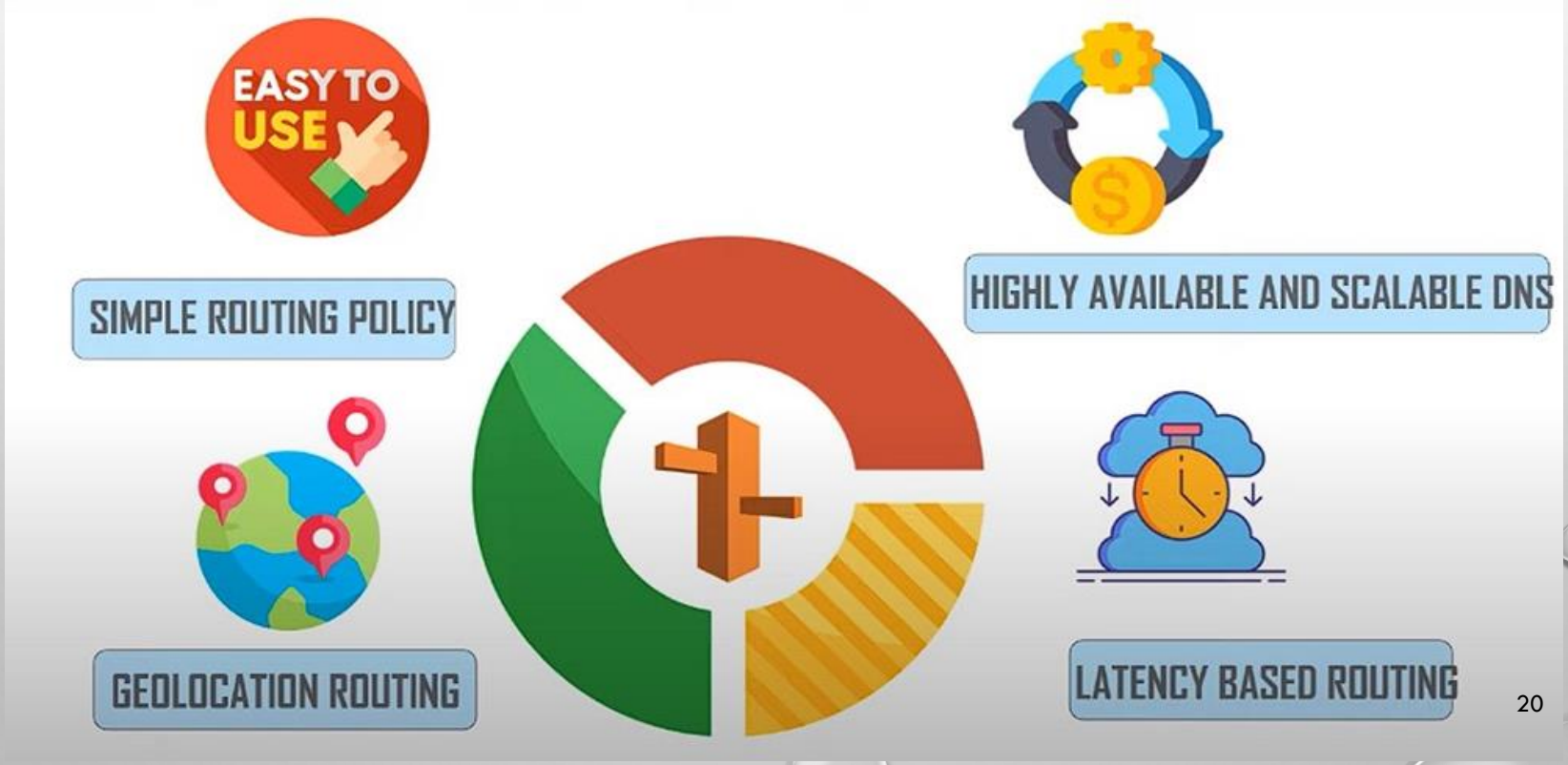
IN SIMPLER TERMS...

Suppose you type out the address of the webpage/website you need

Route 53 asks you to register the domain of the website.

Once the domain is registered Route 53 translates the domain name into an IP address and maps the activity.

WHY DO WE USE AMAZON ROUTE 53 ?

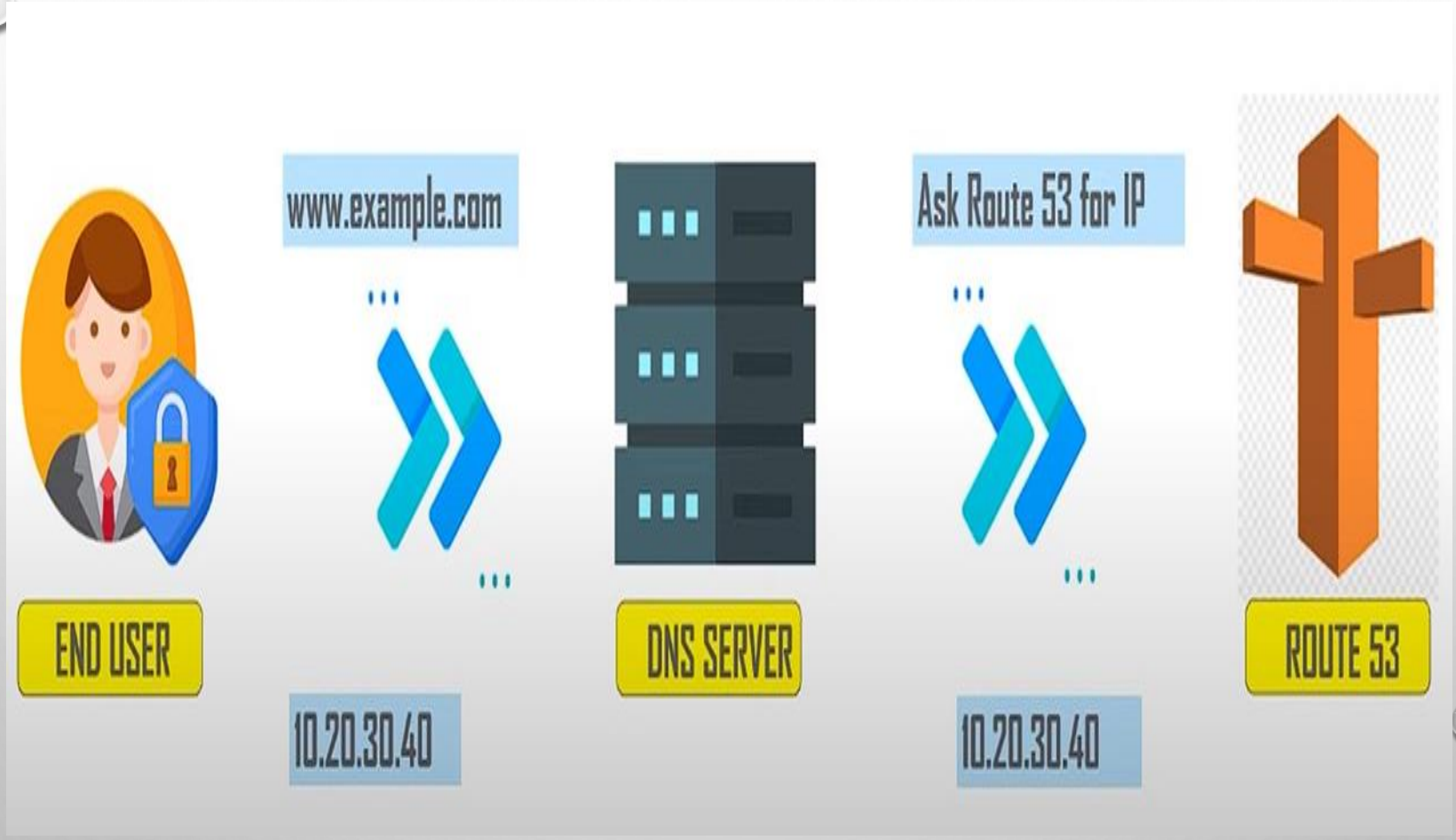


WORKING OF ROUTE 53

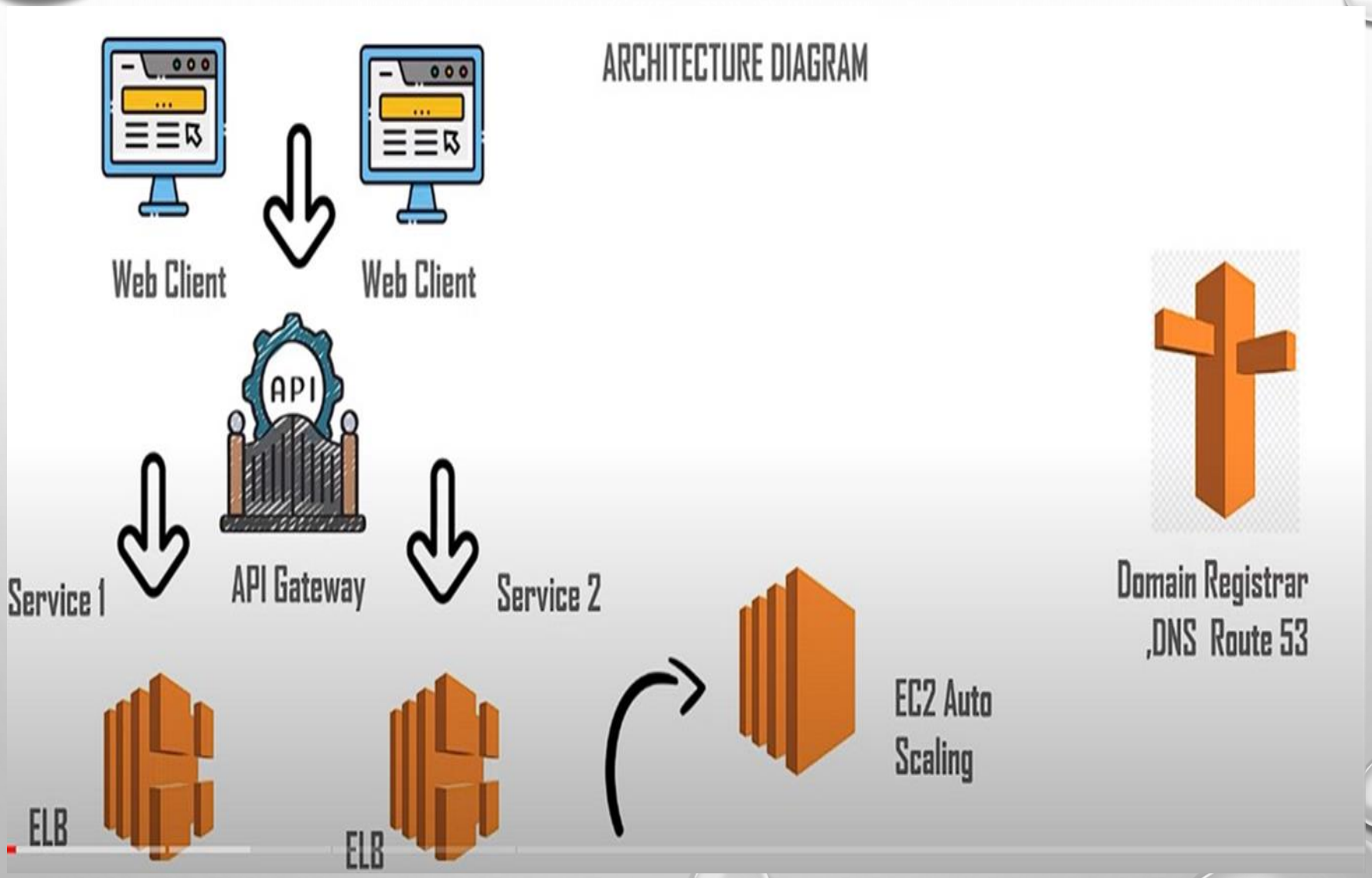
THE GLOBAL INFRASTRUCTURE CALLED THE DOMAIN NAME SYSTEM (DNS) TRANSLATES HUMAN-READABLE HOSTNAMES INTO NUMERICAL IP ADDRESSES. IP ADDRESSES ON THE CLOUD CAN CHANGE FREQUENTLY, AS SERVICES MOVE BETWEEN DATA CENTERS AND PHYSICAL MACHINES. THIS MEANS THE TRANSLATION AND COMMUNICATION PROCESS IS COMPLEX.

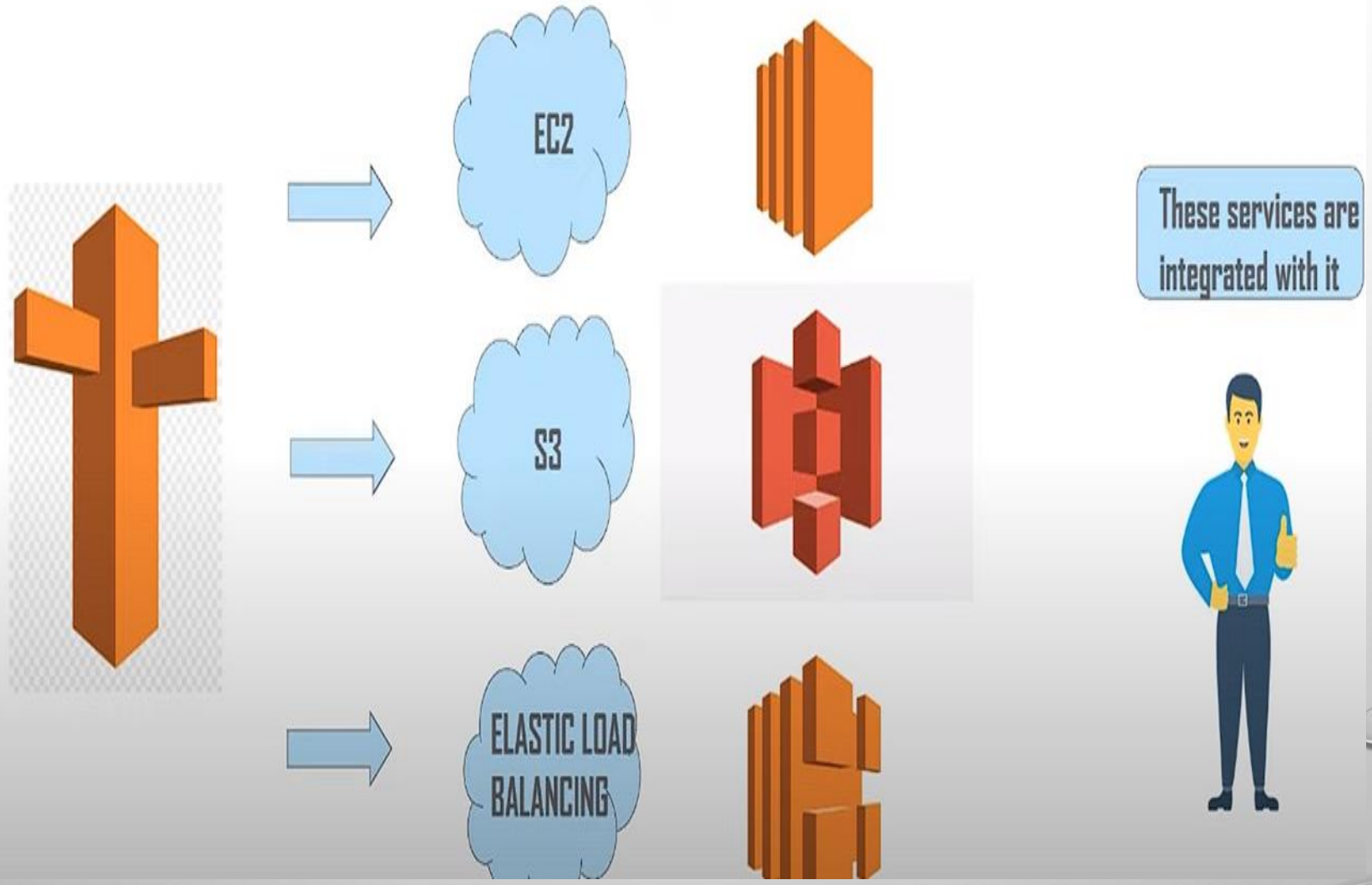
ORGANIZATIONS THAT RUN MACHINES IN THE CLOUD USING AMAZON WEB SERVICES (AWS) NEED AN AWS DNS SOLUTION—A WAY TO CORRECTLY TRANSLATE USER REQUESTS INTO AMAZON IP ADDRESSES WHILE ADAPTING TO CLOUD CHANGES AND QUICKLY PROPAGATING THEM TO DNS CLIENTS.

AWS ROUTE 53 IS AMAZON'S OFFICIAL DNS SOLUTION.


www.example.com
Ask Route 53 for IP
END USER
DNS SERVER
ROUTE 53
10.20.30.40
10.20.30.40

1. A USER ACCESSES AN ADDRESS MANAGED BY ROUTE 53, WWW.WEBSITE.COM, WHICH LEADS TO AN AWS-HOSTED MACHINE.
2. TYPICALLY MANAGED BY THE LOCAL NETWORK OR ISP, THE USER'S DNS RESOLVER RECEIVES THE REQUEST FOR WWW.WEBSITE.COM ROUTED BY AWS ROUTE 53 AND FORWARDS IT TO A DNS ROOT SERVER.
3. THE DNS RESOLVER FORWARDS THE TLD NAME SERVERS FOR ".COM" DOMAINS THE USER REQUESTS.
4. THE RESOLVER ACQUIRES THE FOUR AUTHORITATIVE AMAZON ROUTE 53 NAME SERVERS THAT HOST THE DOMAIN'S DNS ZONE.
5. THE DNS RESOLVER SELECTS ONE OF THE FOUR AWS ROUTE 53 SERVERS, AND REQUESTS DETAILS FOR WWW.WEBSITE.COM.
6. THE ROUTE 53 NAME SERVER SEARCHES THE DNS ZONE FOR THE WWW.WEBSITE.COM IP ADDRESS AND OTHER RELEVANT INFORMATION AND RETURNS IT TO THE DNS RESOLVER.
7. AS SPECIFIED BY THE TIME TO LIVE (TTL) PARAMETER, THE DNS RESOLVER CACHES THE IP ADDRESS LOCALLY, AND OF COURSE RETURNS IT TO THE USER'S WEB BROWSER.
8. THE BROWSER USES THE IP ADDRESS THE RESOLVER PROVIDES TO CONTACT AMAZON-HOSTED SERVICES SUCH AS THE WEB SERVER.
9. THE USER'S WEB BROWSER DISPLAYS THE WEBSITE.


ARCHITECTURE DIAGRAM
Web Client
Web Client
API
Service 1
API Gateway
Service 2
Domain Registrar
,DNS Route 53
ELB
ELB
EC2 Auto
Scaling


EC2
S3
ELASTIC LOAD BALANCING
These services are integrated with it

FEATURES OF AWS ROUTE 53

1. ROUTE 53 RESOLVER :

AWS ROUTE 53 RESOLVER IS A SERVICE THAT HELPS YOU RESOLVE DOMAIN NAMES WITHIN YOUR AMAZON VIRTUAL PRIVATE CLOUD (VPC) OR ON-PREMISES NETWORK. IT ENABLES DNS RESOLUTION FOR YOUR RESOURCES, ALLOWING YOU TO ROUTE TRAFFIC BOTH WITHIN YOUR VPC AND TO EXTERNAL RESOURCES, LIKE THE INTERNET.

2. APPLICATION RECOVERY RESOLVER :

THIS IS A FEATURE WITHIN ROUTE 53 RESOLVER THAT HELPS IMPROVE THE AVAILABILITY OF YOUR APPLICATIONS. IT AUTOMATICALLY DETECTS WHEN YOUR DNS RESOLVERS ARE EXPERIENCING ISSUES AND REROUTES DNS TRAFFIC TO HEALTHY RESOLVERS, ENSURING YOUR APPLICATIONS REMAIN ACCESSIBLE AND RELIABLE.

3. TRAFFIC FLOW :

TRAFFIC FLOW IS A FEATURE IN AWS ROUTE 53 THAT ALLOWS YOU TO CONTROL AND MANAGE THE ROUTING OF YOUR DNS TRAFFIC. IT ENABLES ADVANCED TRAFFIC MANAGEMENT BY LETTING YOU CREATE ROUTING POLICIES, SET UP FAILOVER CONFIGURATIONS, AND IMPLEMENT WEIGHTED ROUTING TO DISTRIBUTE TRAFFIC ACROSS MULTIPLE RESOURCES FOR HIGH AVAILABILITY AND LOAD BALANCING.

4. GEO DNS :

GEO DNS, ALSO KNOWN AS GEOLOCATION-BASED DNS, IS A FEATURE THAT ALLOWS YOU TO ROUTE DNS REQUESTS BASED ON THE GEOGRAPHICAL LOCATION OF THE REQUESTING CLIENT. THIS HELPS OPTIMIZE THE USER EXPERIENCE BY DIRECTING USERS TO THE NEAREST OR MOST APPROPRIATE SERVER OR CONTENT DELIVERY NETWORK (CDN) BASED ON THEIR GEOGRAPHIC LOCATION.

5. HEALTH CHECK AND MONITORING :

ROUTE 53 PROVIDES HEALTH CHECKS AND MONITORING CAPABILITIES THAT ALLOW YOU TO ENSURE THE AVAILABILITY AND PERFORMANCE OF YOUR APPLICATIONS AND RESOURCES. YOU CAN SET UP HEALTH CHECKS TO MONITOR THE HEALTH OF ENDPOINTS SUCH AS WEB SERVERS, AND ROUTE 53 CAN AUTOMATICALLY ROUTE TRAFFIC AWAY FROM UNHEALTHY ENDPOINTS.

6. DOMAIN REGISTRATION :

AWS ROUTE 53 OFFERS DOMAIN REGISTRATION SERVICES, ALLOWING YOU TO REGISTER AND MANAGE DOMAIN NAMES (E.G., EXAMPLE.COM). IT SIMPLIFIES THE PROCESS OF BUYING AND MANAGING DOMAIN NAMES, INCLUDING FEATURES LIKE AUTOMATIC RENEWALS, DNS MANAGEMENT, AND INTEGRATION WITH OTHER AWS SERVICES FOR EASY SETUP OF YOUR WEBSITES AND APPLICATIONS.

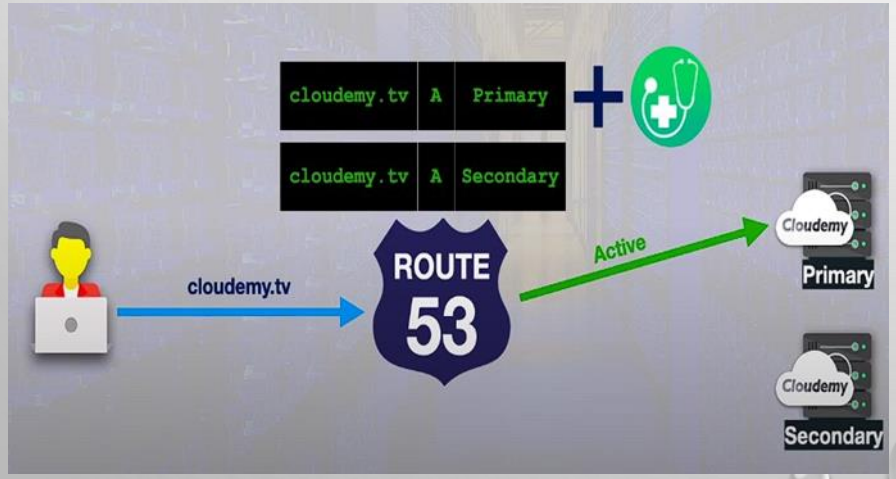
TYPES OF ROUTING POLICIES

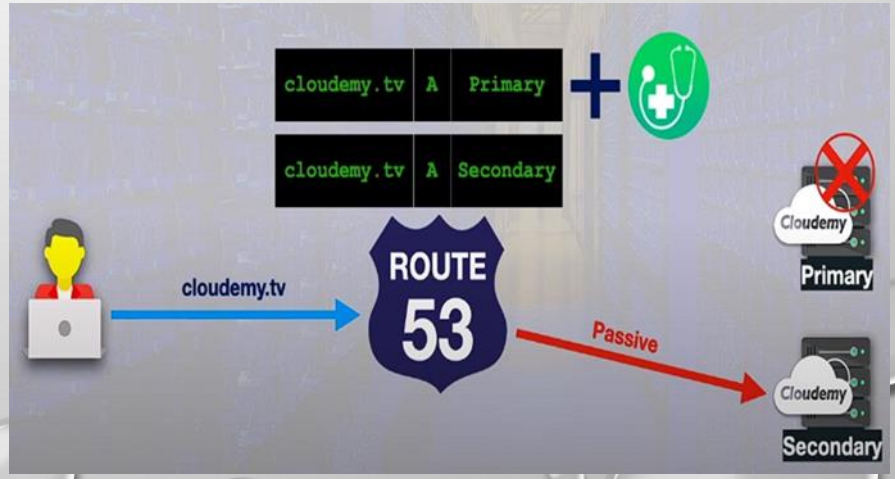
1. SIMPLE ROUTING POLICY

USED FOR A SINGLE RESOURCE THAT PERFORMS A GIVEN FUNCTION FOR YOUR DOMAIN. LIKE THE WEB SERVER THAT SERVES CONTENT FOR YOUR WEBSITE

2. FAILOVER ROUTING POLICY

THIS POLICY COMES INTO USE WHEN YOU WANT TO CONFIGURE THE ACTIVE- PASSIVE FAILOVER. FAILOVER OCCURS WHEN SYSTEM AUTOMATICALLY TRANSFERS CONTROL TO ANOTHER SYSTEM



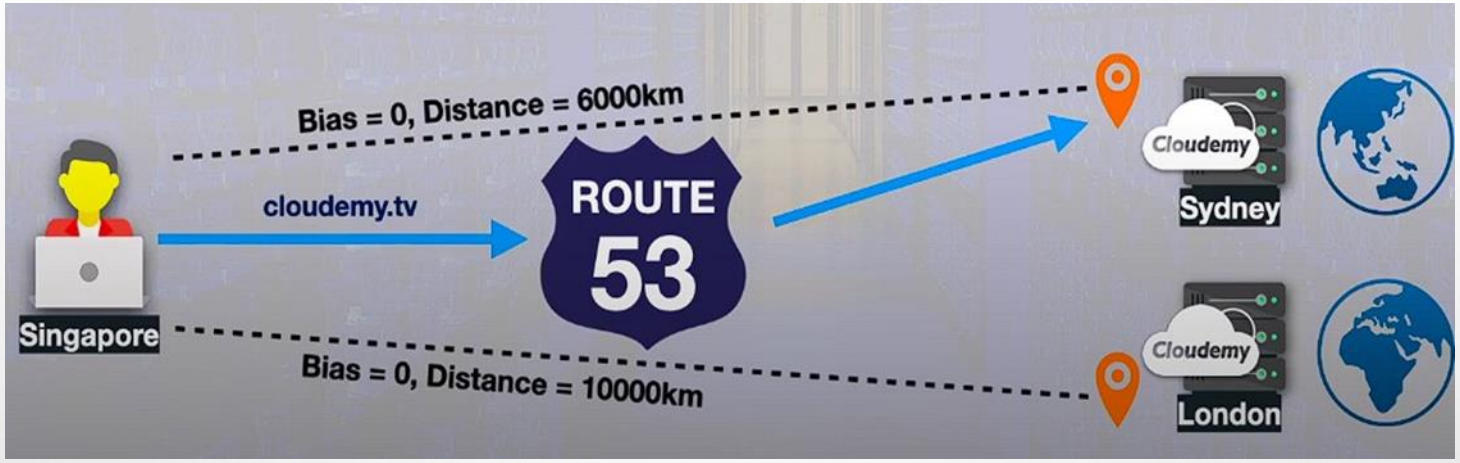


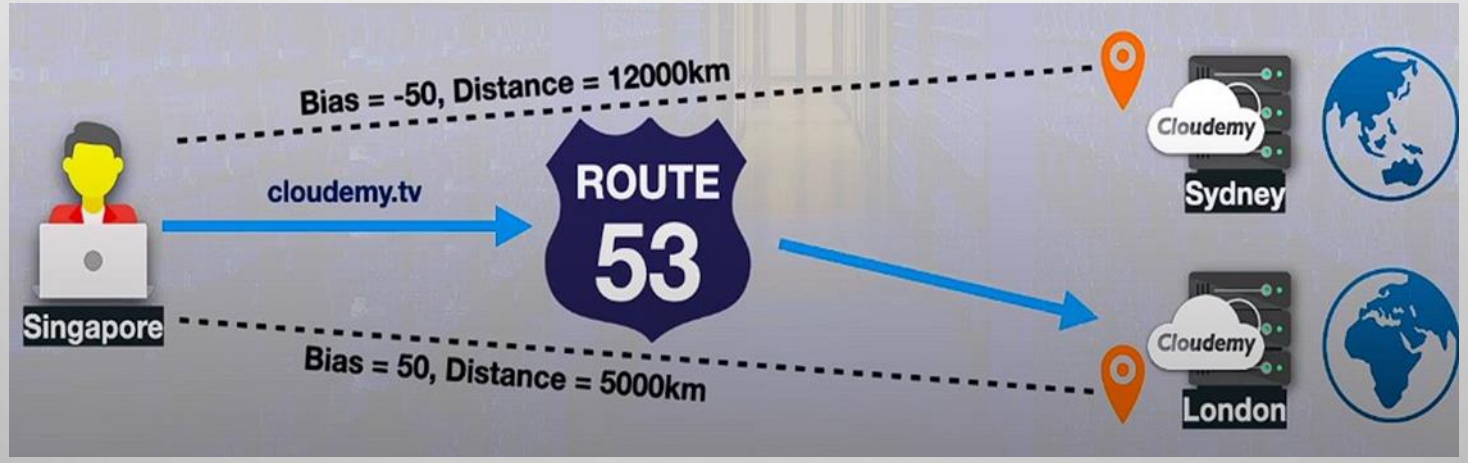
3. GEO LOCATION ROUTING POLICY

GEOLOCATION ROUTING POLICY IS GENERALLY USED WHEN YOU WANT TO ROUTE TRAFFIC BASED ON THE LOCATION OF YOUR USERS. IT CAN BE FROM A PARTICULAR LOCATION OR GLOBAL.

4. GEO PROXIMITY ROUTING POLICY

USE THIS WHEN YOU WANT TO ROUTE TRAFFIC BASED ON THE LOCATION OF YOUR RESOURCES AND OPTIONALLY SHIFT TRAFFIC FROM RESOURCES IN ONE LOCATION TO RESOURCES IN ANOTHER.


Bias = 0, Distance = 6000km
cloudemy.tv
ROUTE
53
Singapore
Bias = 0, Distance = 10000km
Cloudemy
Sydney
Cloudemy
London


Bias = -50, Distance = 12000km
cloudemy.tv
ROUTE
53
Singapore
Bias = 50, Distance = 5000km
Cloudemy
Sydney
Cloudemy
London

5. LATENCY ROUTING POLICY

USE THIS POLICY WHEN YOU HAVE RESOURCES IN MULTIPLE AWS REGIONS AND YOU WANT TO ROUTE TRAFFIC TO THE REGION THAT PROVIDES THE BEST LATENCY AND LESS ROUND TRIP TIME.

BENEFITS OF AWS ROUTE 53

- HIGHLY AVAILABLE AND RELIABLE
- FLEXIBLE
- SIMPLE
- FAST
- COST-EFFECTIVE
- DESIGNED TO INTEGRATE WITH OTHER AWS SERVICES
- SECURE
- SCALABLE

USE CASES OF AWS ROUTE 53

- **WEBSITE HOSTING**

  ROUTE 53 CAN BE USED TO ROUTE TRAFFIC TO YOUR WEB SERVERS OR HOSTING RESOURCES, ENSURING THAT YOUR WEBSITE IS ACCESSIBLE USING YOUR DOMAIN NAME.

- **LOAD BALANCING**

  YOU CAN USE ROUTE 53 TO DISTRIBUTE INCOMING TRAFFIC ACROSS MULTIPLE AWS RESOURCES, SUCH AS EC2 INSTANCES, ELASTIC LOAD BALANCERS (ELB), OR AWS GLOBAL ACCELERATOR, TO ACHIEVE LOAD BALANCING AND HIGH AVAILABILITY.

- **FAILOVER AND DISASTER RECOVERY**
  IMPLEMENT FAILOVER CONFIGURATIONS USING ROUTE 53 TO AUTOMATICALLY DIRECT TRAFFIC TO A BACKUP OR SECONDARY SITE OR RESOURCE IN CASE THE PRIMARY SITE BECOMES UNAVAILABLE DUE TO ISSUES LIKE SERVER FAILURE OR REGIONAL OUTAGES.

- **CONTENT DELIVERY**
  ROUTE 53 CAN ROUTE TRAFFIC TO CONTENT DELIVERY NETWORKS (CDNS) LIKE AMAZON CLOUDFRONT, IMPROVING THE DELIVERY OF STATIC AND DYNAMIC CONTENT TO END USERS WORLDWIDE.

- **GEOLOCATION-BASED ROUTING**
  CUSTOMIZE THE USER EXPERIENCE BY ROUTING TRAFFIC TO SPECIFIC RESOURCES BASED ON THE GEOGRAPHIC LOCATION OF THE USER. THIS IS USEFUL FOR SERVING REGION-SPECIFIC CONTENT OR APPLICATIONS.