Guide to secure Cloud-to-on-premise Communication

For AWS Event Reinvent Recap 2024

Slash
Sean
sean@slash.co

/slash

Hi, I am Sopeak

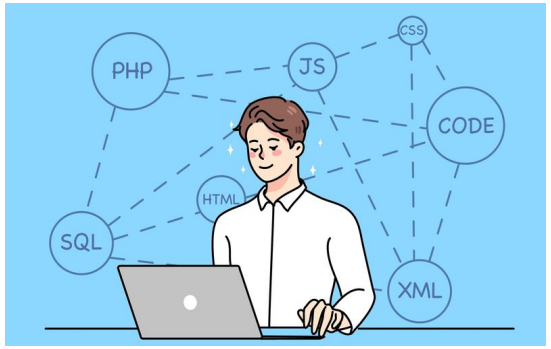
LinkedIn

Solutions Architect, Slash, in charge of technical research, solutioning and implementation strategy, Certified AWS SAA

With over a decade of experience in tackling technical challenges, project management, and fostering cohesive teams, he excels in solution-oriented approaches and software engineering in web, mobile, backend, DevOps in numerous languages and frameworks.

Specializing in enterprise client solutions and serving as a Tech Lead, Sean is dedicated to defining quality standards, fostering team culture, and spearheading hiring and training practices. His expertise extends to overseeing development teams and implementing DevSecOps strategies.

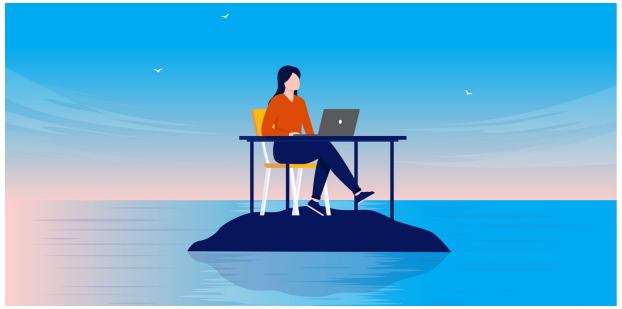
/slash



Ideas that Matter, Products that Scale, Change that Delivers.

From our digital solutions boutique to our venture-building agency, we harness the power of technology to create a positive legacy. We have been building meaningful digital products that people love and that the world needs since 2016.

/slash



We are Slash.

A boutique tech studio with its roots in software excellence, we value a strong relationship with clients who share the same vision.

Human-centered

Our foundation is people-centric. We deeply understand their needs, cultivate genuine relationships, and co-create solutions that enrich lives.

Growth-focused

Our commitment goes beyond product delivery; it marks the beginning of a journey. Fueled by a desire to learn, we constantly adapt and evolve to deliver optimal results.

Tech-savvy

Our expertise lies in best-in-class product design, software engineering, and agile practices. We enable continuous design and delivery, allowing businesses to deploy rapidly and scale securely.

/slash

Our quest today

On how we secure on-premise to cloud connection

Design the Architecture

High level walkthrough together on how we tackle the topic today

Understand components

Brief information about what are the components we are exploring today

Explore and learn

Explore the presentation today together!
There is no one way to learn and design this, but many possibilities.

EXPAND

Don’t stop! Keep expanding your knowledge through more research and practices!

/slash

Key takeaways

- *Some AWS Services for auto scaling, security, VPNs.*
- *Way of breaking down the architecture requirement and build it step by step.*
- *Explore and learn what each services can offer so you can use its to its potentials.*
- *There is always room for improvement and learning can be fun!*

0

Let’s begin

Start

/slash

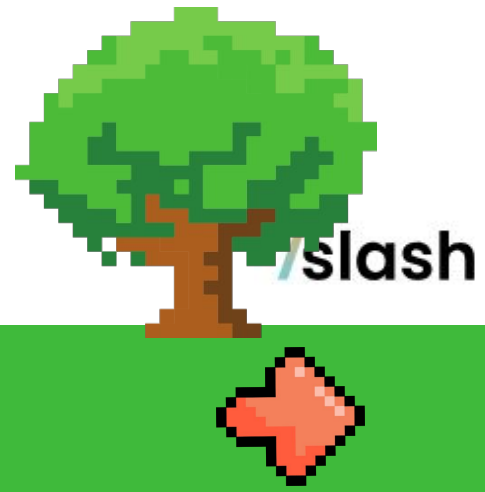
0

Imagine Mr. Sok work as a DevOp Engineer at insurance company.

0

Mr. Sok is tasked with deploying a web portal for Client to access company employee health insurance.

How can you help him?



200

First Quest:

Help Mr. Sok design the deployment solution for a web portal for employee health insurance.

START

/slash

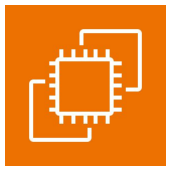
200

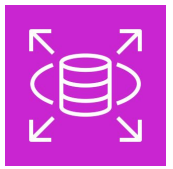
Design and deploy on AWS

What we need to do?

- Use the AWS account to deploy the infrastructure

Compute and Database


EC2


RDS

- **Assume the Web app is ready to on EC2**
  (We use Container, Lambda but for later)
- **Assume the Web app connect to PostgreSQL**

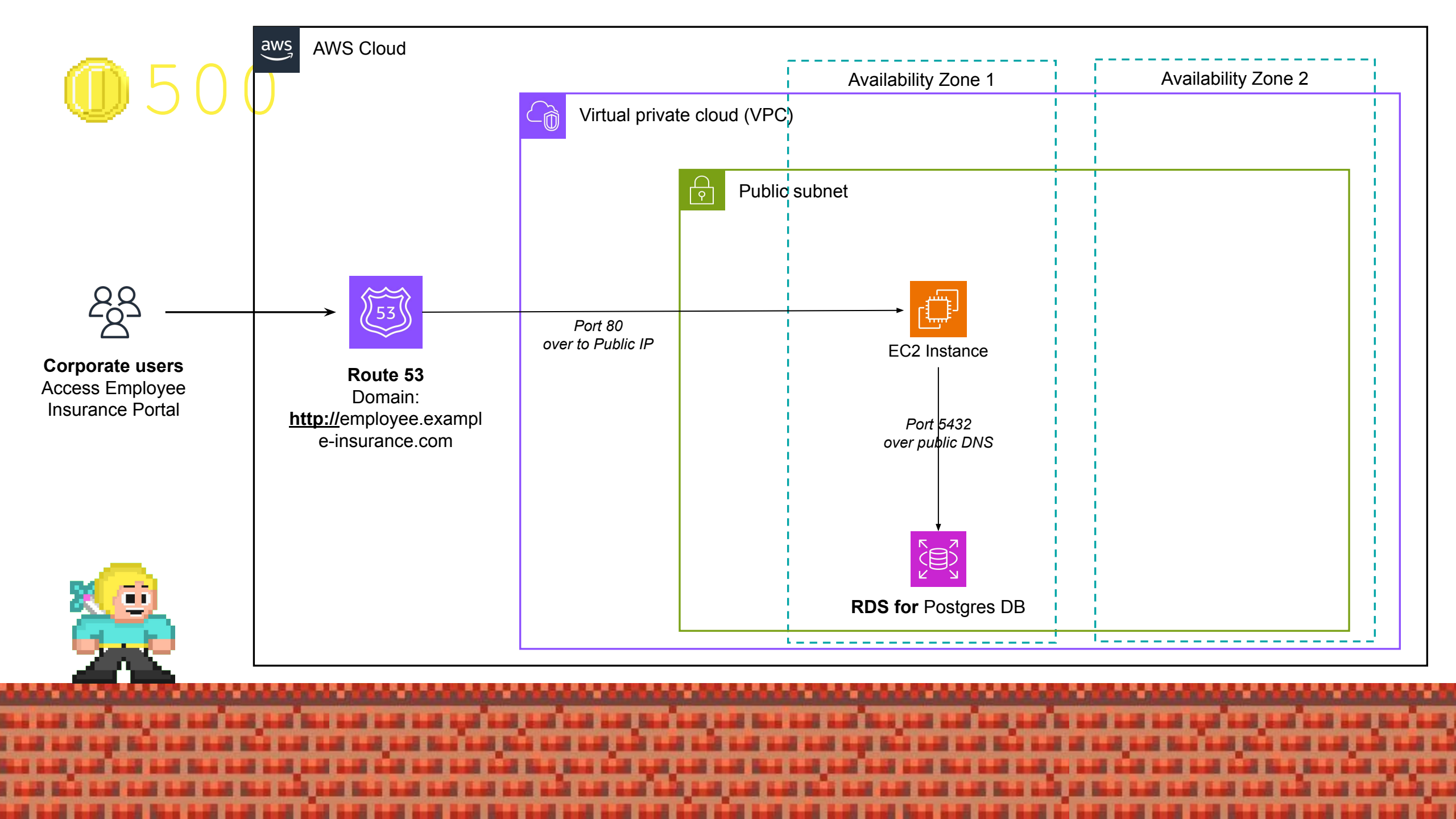
Public Access and Domain name


VPC

Route53

- Assume we will allow all public access to Web app and Connect to RDS thru Public Networking

- Assume we have domain name ready in Route 53


AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
Public subnet
Corporate users
Access Employee Insurance Portal
Route 53
Domain:
http://employee.example-insurance.com
Port 80
over to Public IP
EC2 Instance
Port 5432
over public DNS
RDS for Postgres DB

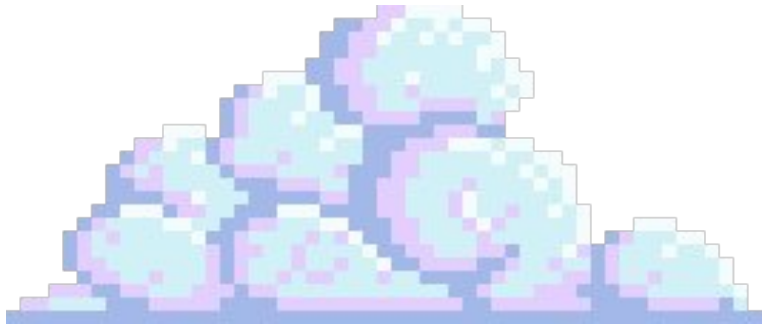
1500

/slash

Improve the security, limit access to Cambodia only, and handle large amount of incoming access?

/slash

1500



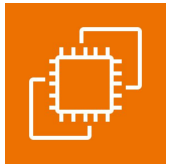
Next Quest:

Help Mr. Sok improve the security and scalability of the infrastructure.

START

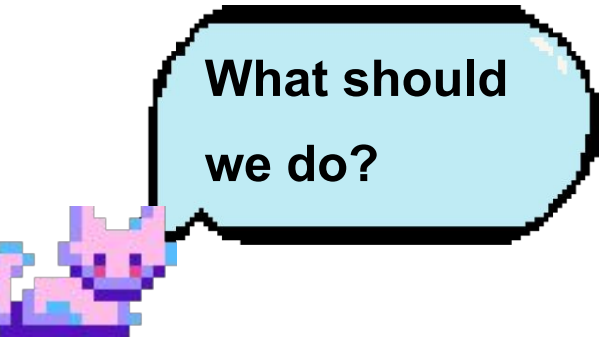
/slash

Limit Security Group Ports



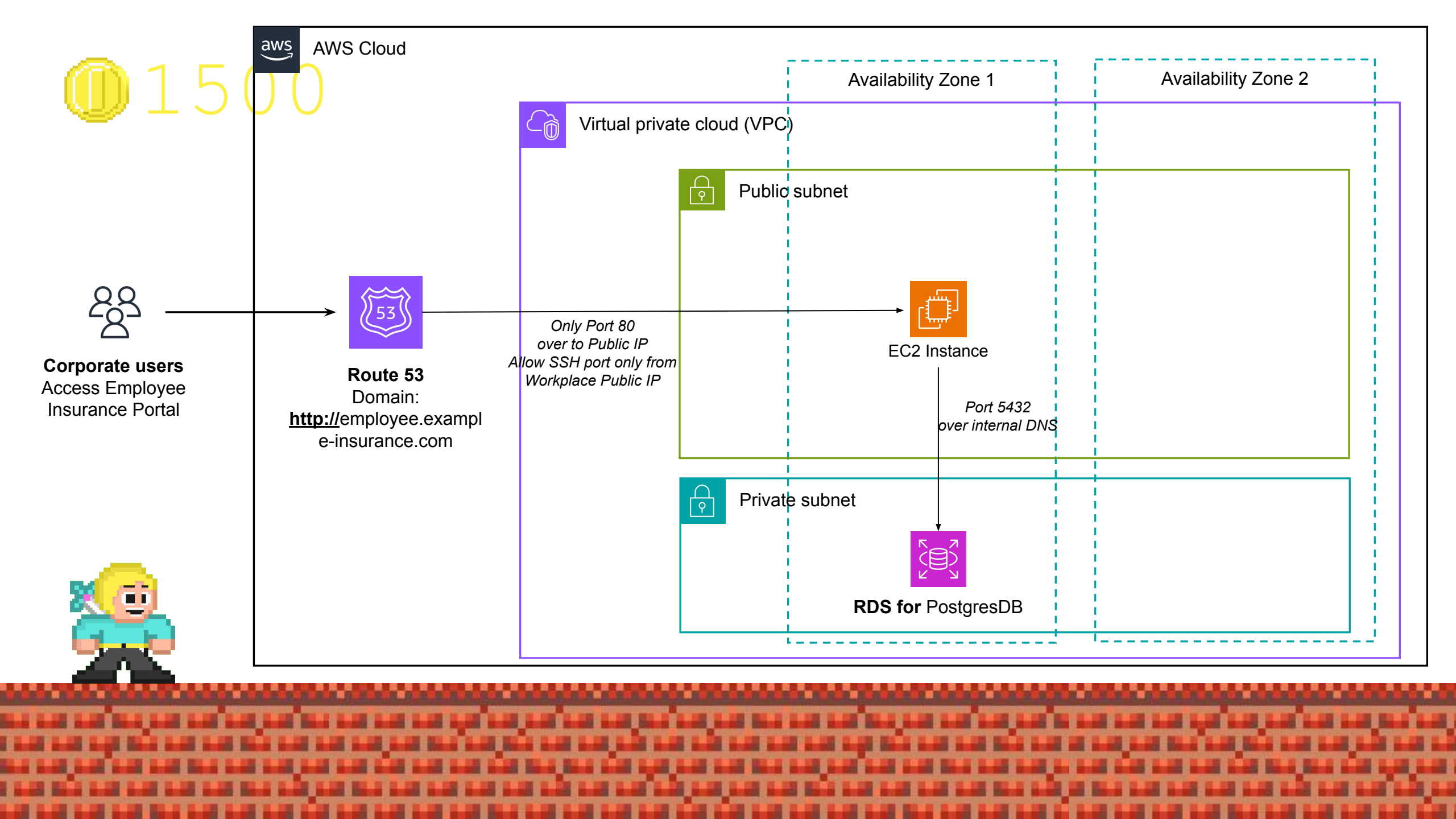
Make sure open on Port 80 on Security Group

Only allow SSH from company public IP



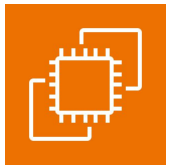
Move RDS to Private Subnet

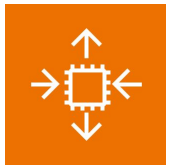
Database should only be accessed privately by Application


1500
aws
AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
Public subnet
Private subnet
Corporate users
Access Employee Insurance Portal
53
Route 53
Domain:
http://employee.example-insurance.com
Only Port 80
over to Public IP
Allow SSH port only from
Workplace Public IP
EC2 Instance
Port 5432
over internal DNS
RDS for PostgresDB

2500

Setup Auto Scaling for EC2

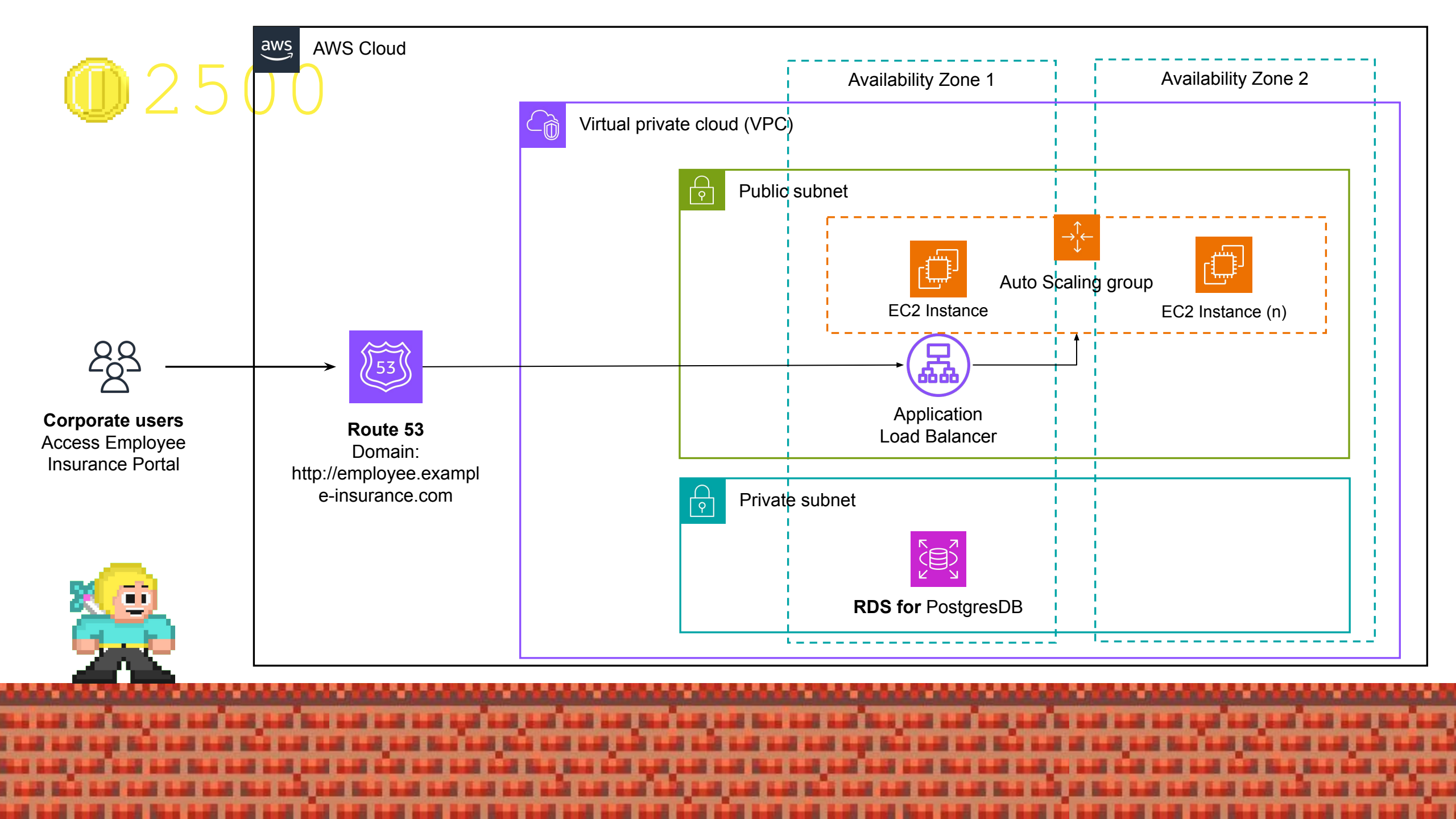

EC2


EC2
Auto scaling

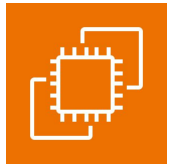

Application
Load Balancer

- **Scale server horizontally***
  (Assume Web app code is ready to work with multiple servers horizontally)
- **Use Application load balance to distribute requests to all instances**
- **Auto scaling rules - automatic scale in and out on demand**

/slash


2500
aws
AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
Public subnet
Auto Scaling group
EC2 Instance
EC2 Instance (n)
Application
Load Balancer
Private subnet
RDS for PostgresDB
53
Corporate users
Access Employee
Insurance Portal
Route 53
Domain:
http://employee.exampl
e-insurance.com

Configure HTTPs for application


EC2


VPC

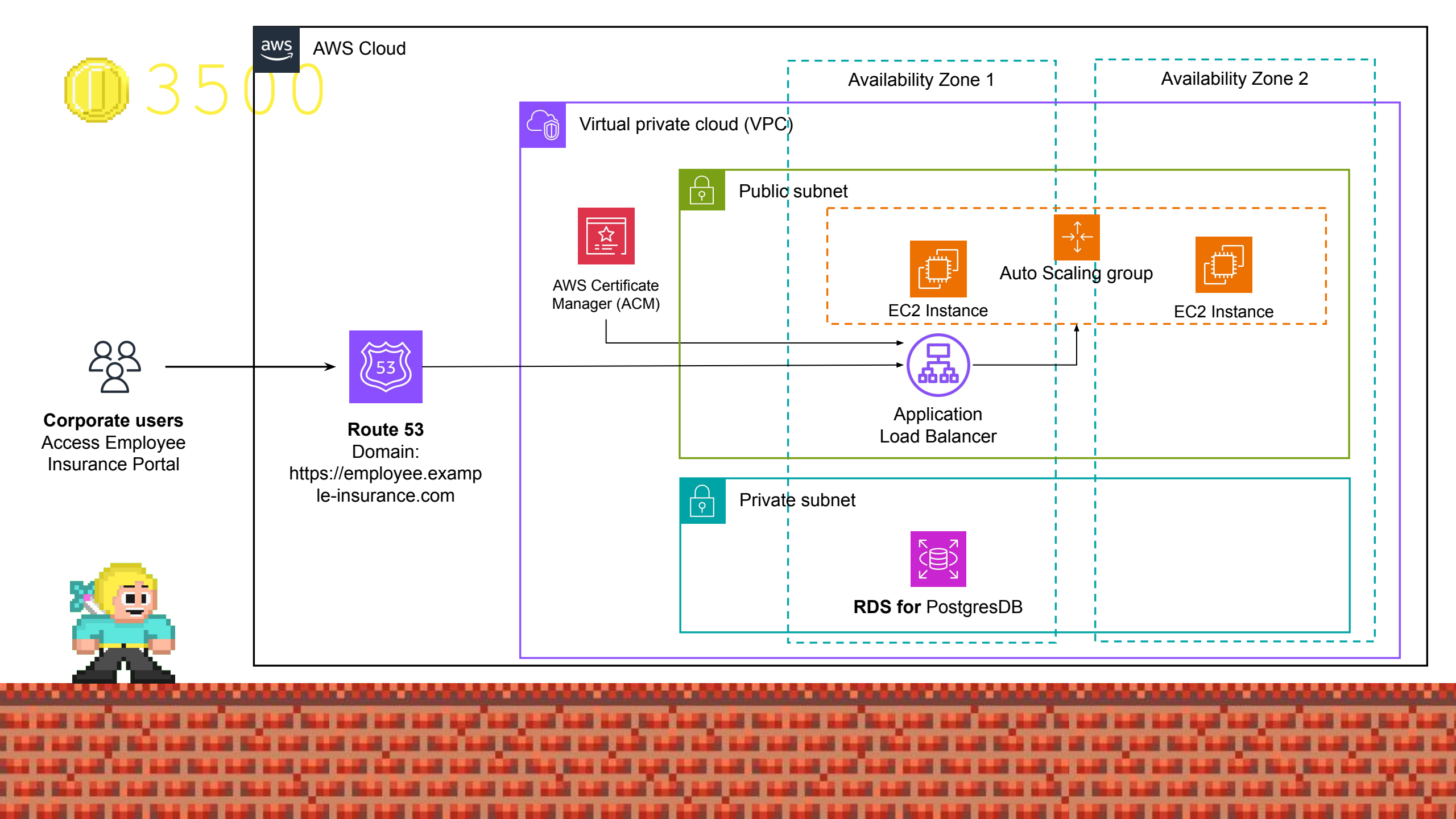

Use Https for Application Load Balancer and Configure Certificate


Application Load Balancer


AWS Certificate Manager (ACM)


Limit the Port of the EC2 instances to be accessible from only Load balancer

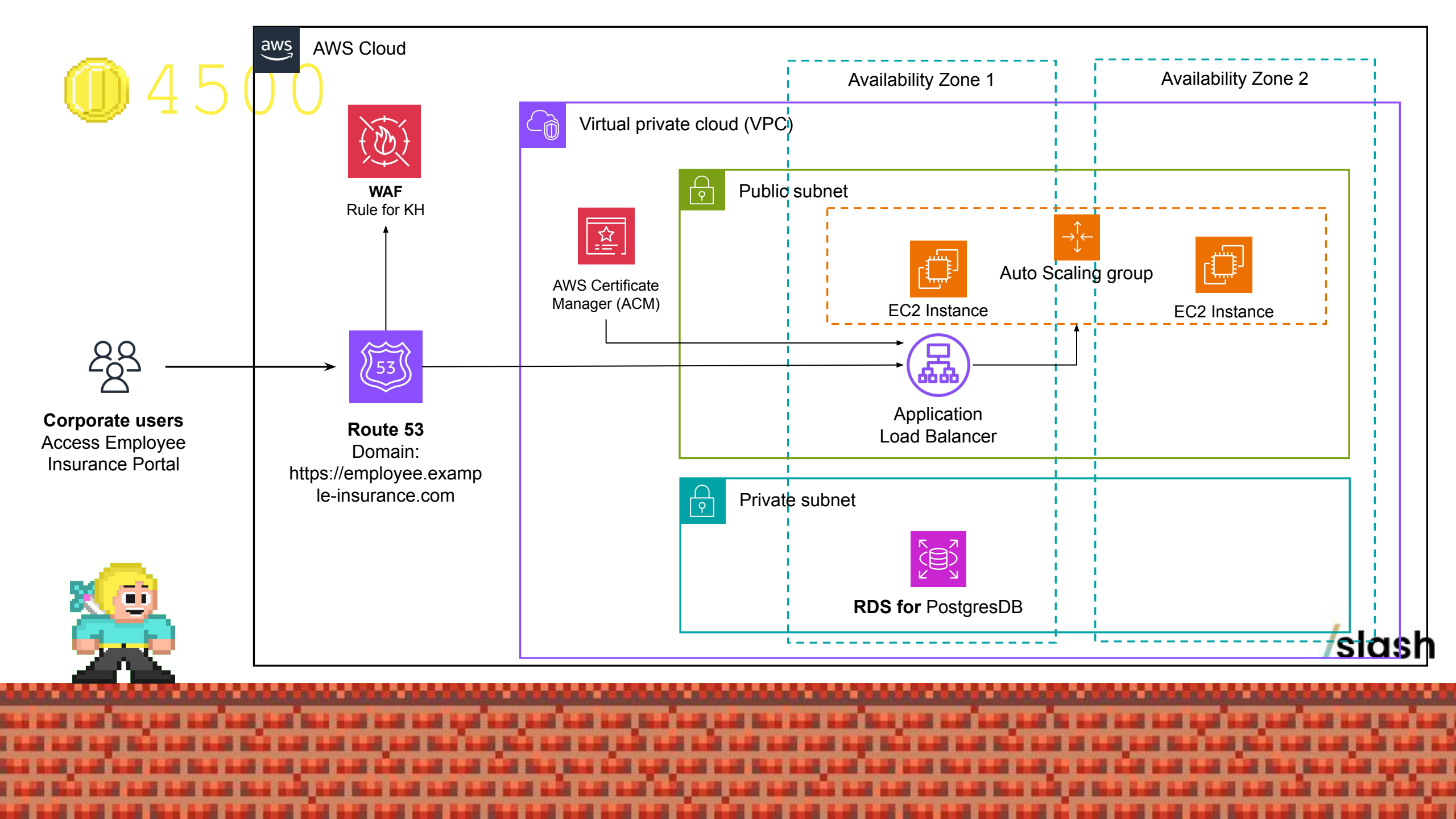
/slash


3500
aws
AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
Public subnet
AWS Certificate Manager (ACM)
Auto Scaling group
EC2 Instance
EC2 Instance
Application Load Balancer
Private subnet
RDS for PostgresDB
Corporate users
Access Employee Insurance Portal
Route 53
Domain:
https://employee.example-insurance.com

Configure WAF for Country Access

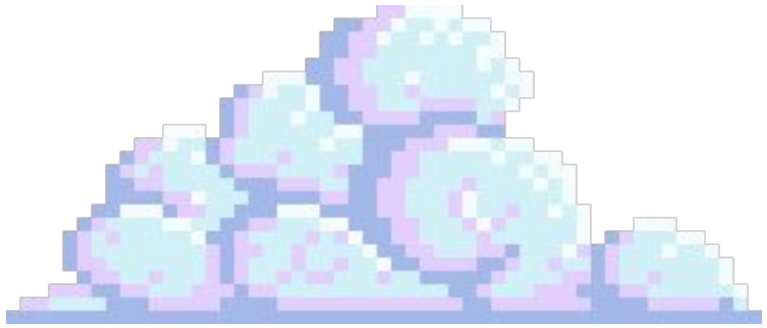
Configure WAF ACL rule for country, limit only from Cambodia

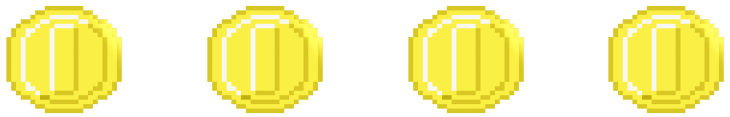
Use WAF for more use cases such as block/whitelist specific IP addresses, restrict access to Bot, block malicious SQL before traffic flowing to your Application server!

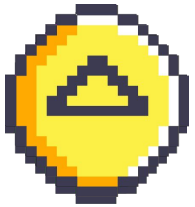

4500
AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
WAF
Rule for KH
Public subnet
AWS Certificate
Manager (ACM)
Auto Scaling group
EC2 Instance
EC2 Instance
Corporate users
Access Employee
Insurance Portal
Route 53
Domain:
https://employee.examp
le-insurance.com
Application
Load Balancer
Private subnet
RDS for PostgresDB
/slash


4500
"Secure connection to On-Premise"
Final boss...
/slash

4500







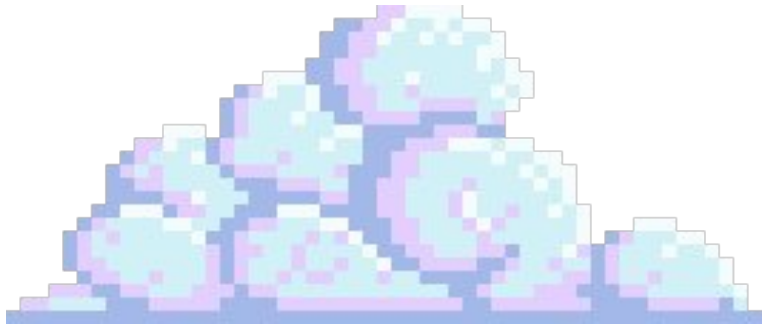
FINAL BOSS ALERTS!

New urgent task arises!

New feature is released to allow customer to make Online payment.

/slash

4500



FINAL BOSS ALERTS!

Due to compliance and security review, this new Online Payment API is deployed on On-Premise.

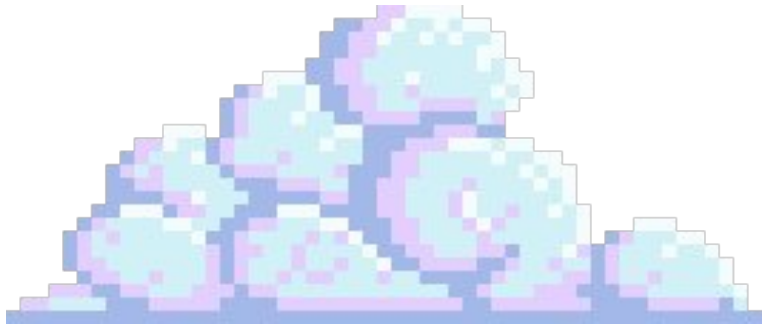
/slash

FINAL BOSS ALERTS!

And require the application to integrate securely to the On-Premise API!

/slash

4500



FINAL BOSS ALERTS!

Now help Mr. Sok implements the secure on-premise connection

you can do it

START

/slash

CIDRs, Devices / Softwares / Public IPs

- Cloud (VPC) CIDR / IPv4 range is not the same as On-Premise CIDR.
- Static Public IP available from On-Premise
- Physical / Software on your On-Premise side of VPN (e.g. Cisco, Fortigate, Palo etc..)

4500

Site-to-site VPNs

- To enable secure IPsec connectivity between On-premise and Cloud, we use Site-to-site VPN

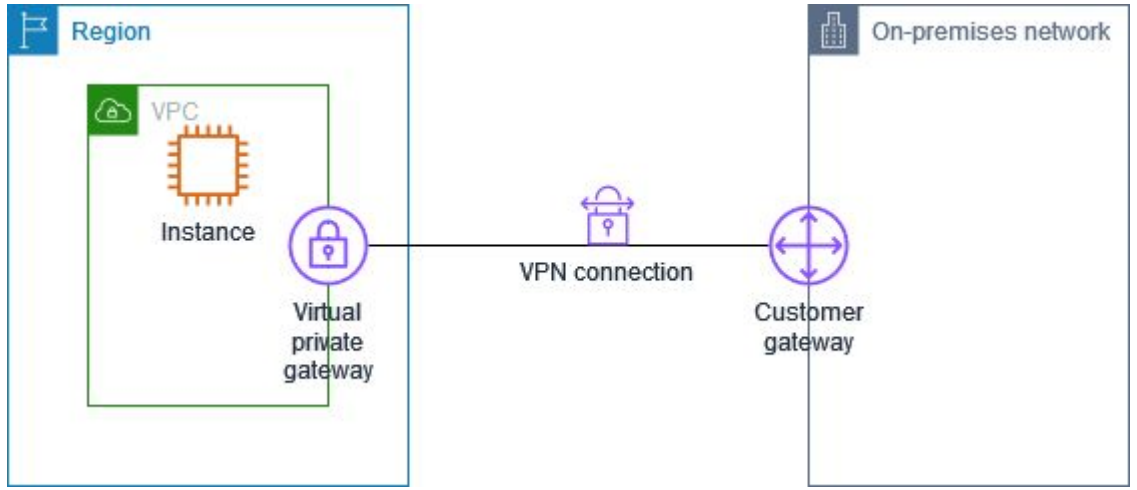
- There are many ways of setting site-to-site VPN as per different use cases

/slash

4500

Single Site-to-Site VPN connection

AWS Site-to-Site VPN

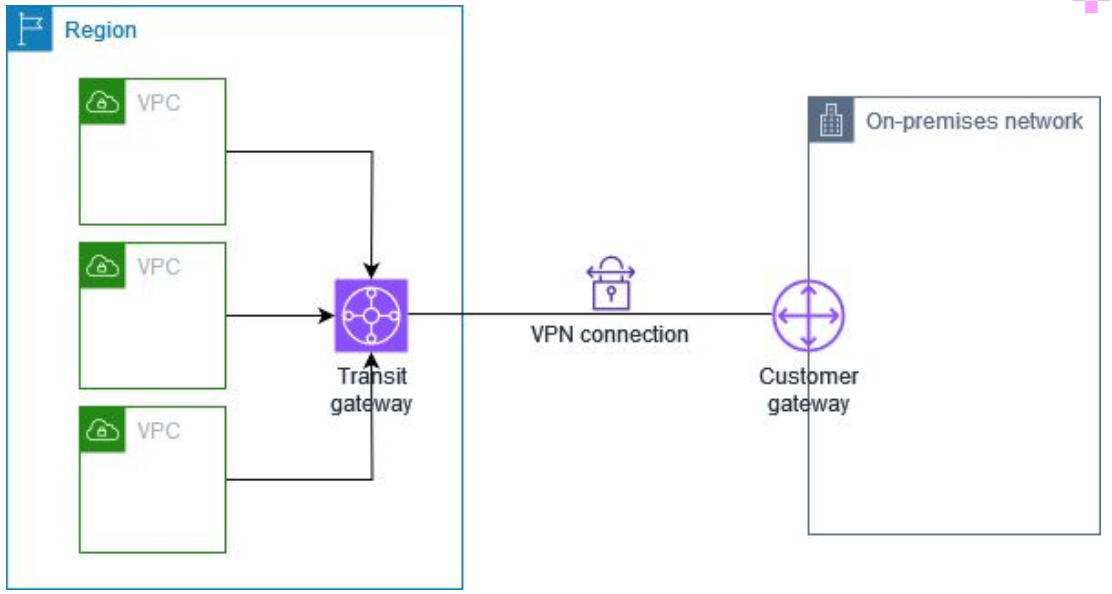


/slash

4500

Single Site-to-Site VPN connection with a transit gateway

AWS Site-to-Site VPN

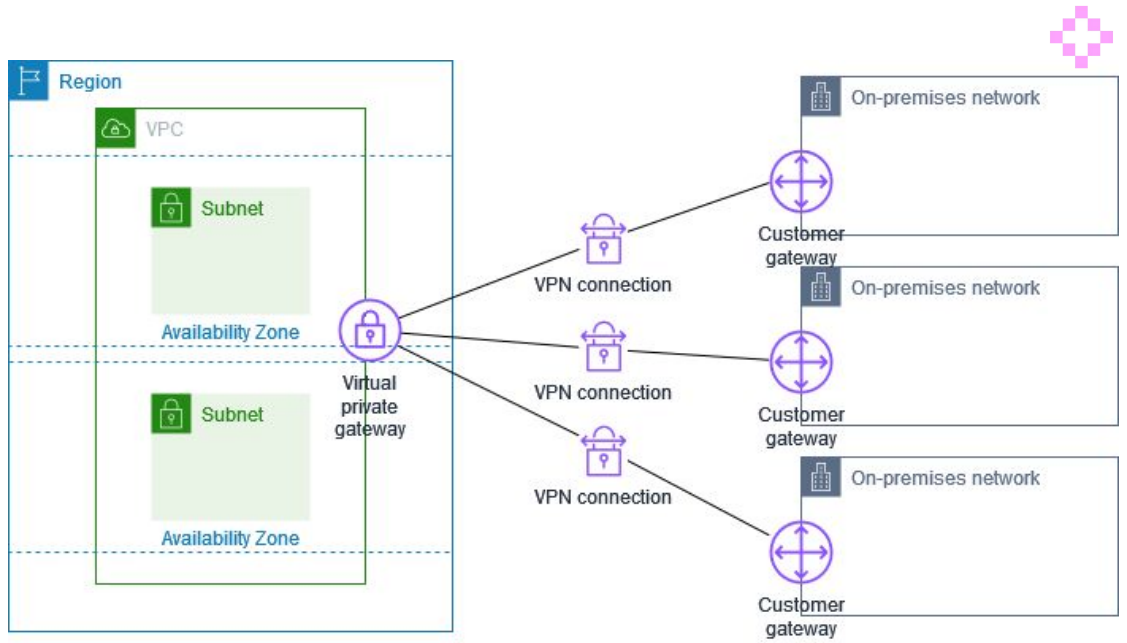


/slash

4500

Multiple Site-to-Site VPN connections

AWS Site-to-Site VPN

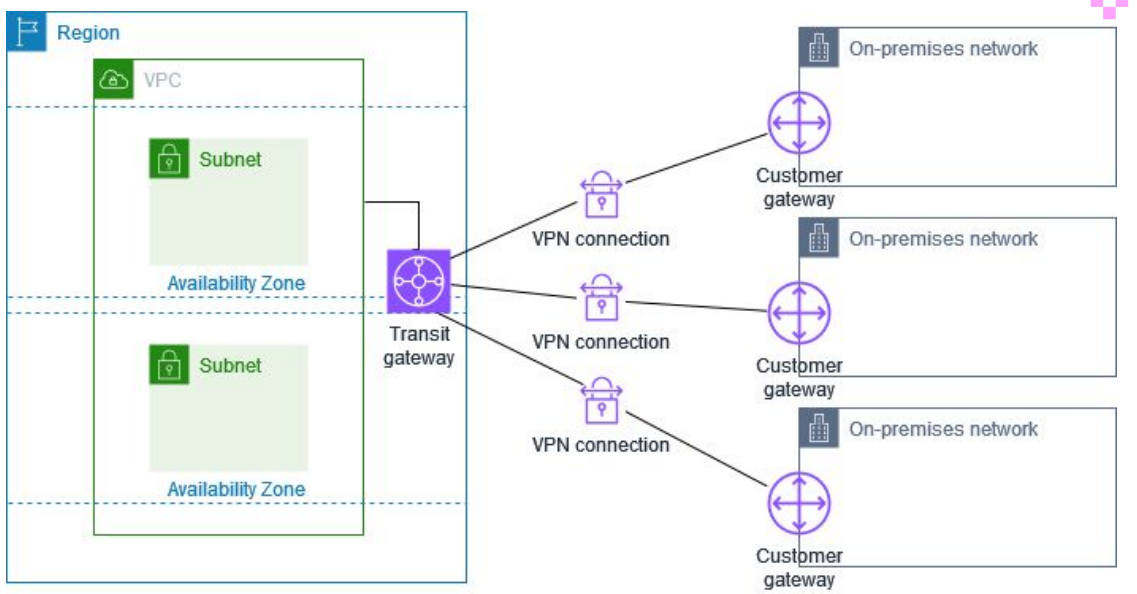


/slash

4500

Multiple Site-to-Site VPN connections with a transit gateway

AWS Site-to-Site VPN



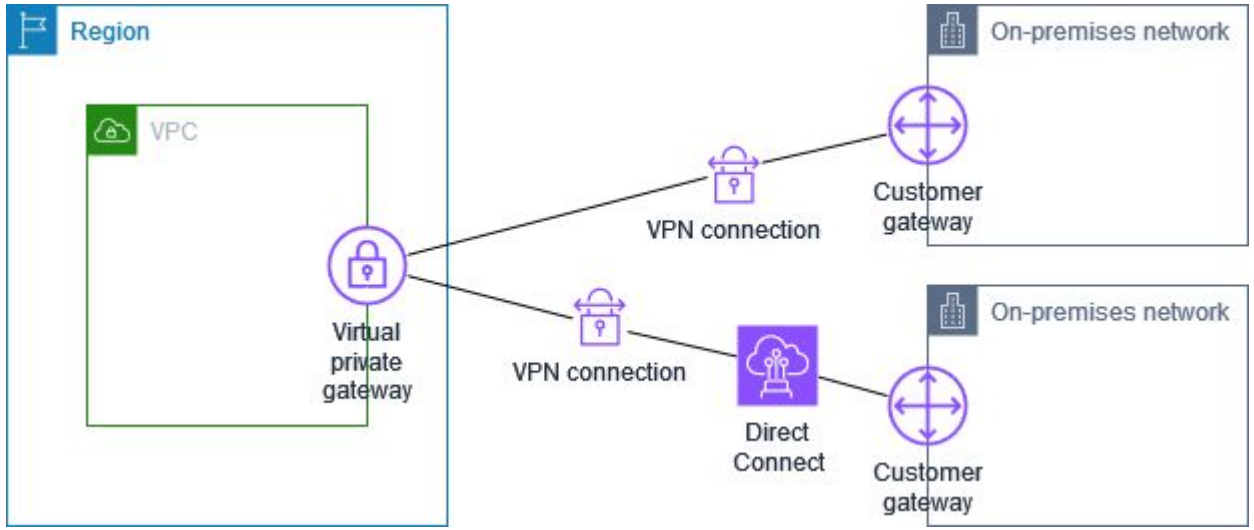
/slash

4500

Site-to-Site VPN connection with AWS Direct Connect

AWS Site-to-Site VPN

Hungry ><

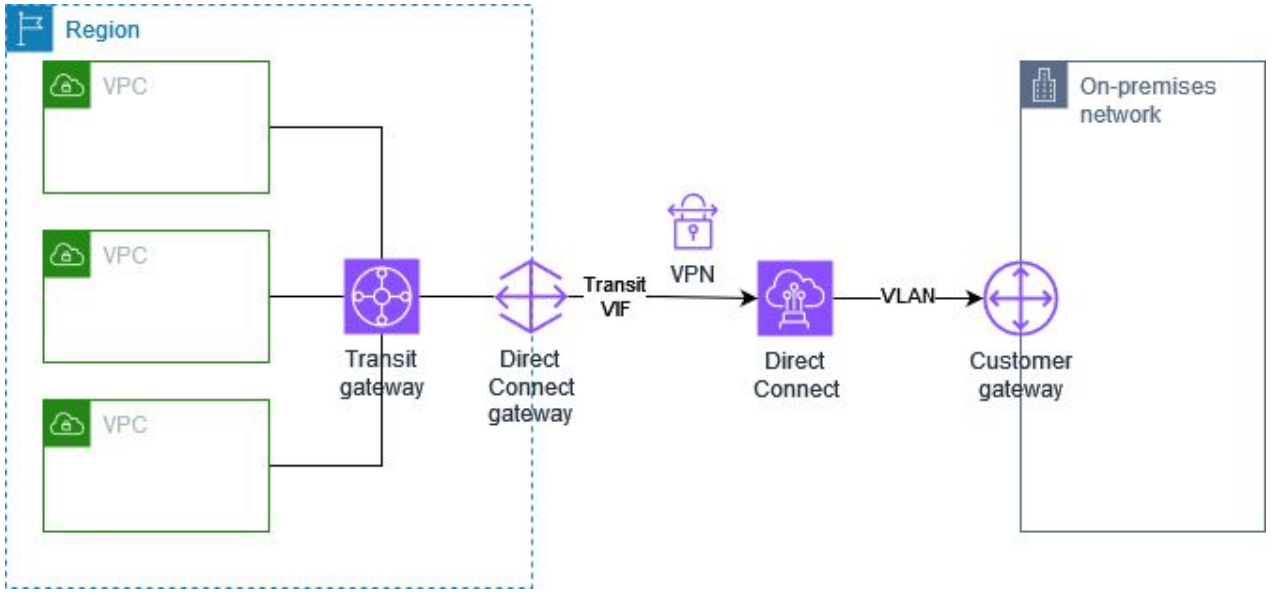


/slash

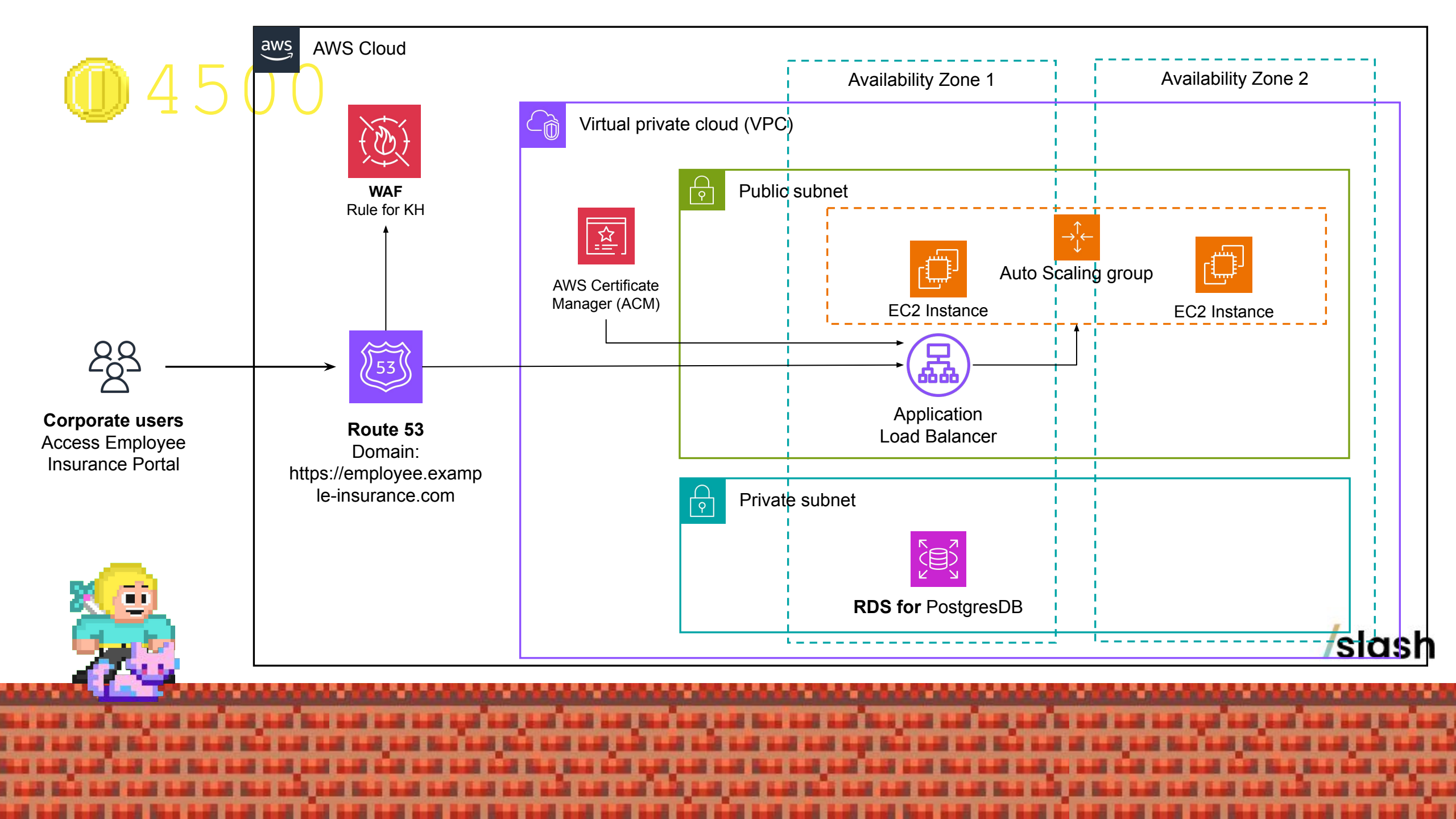
4500

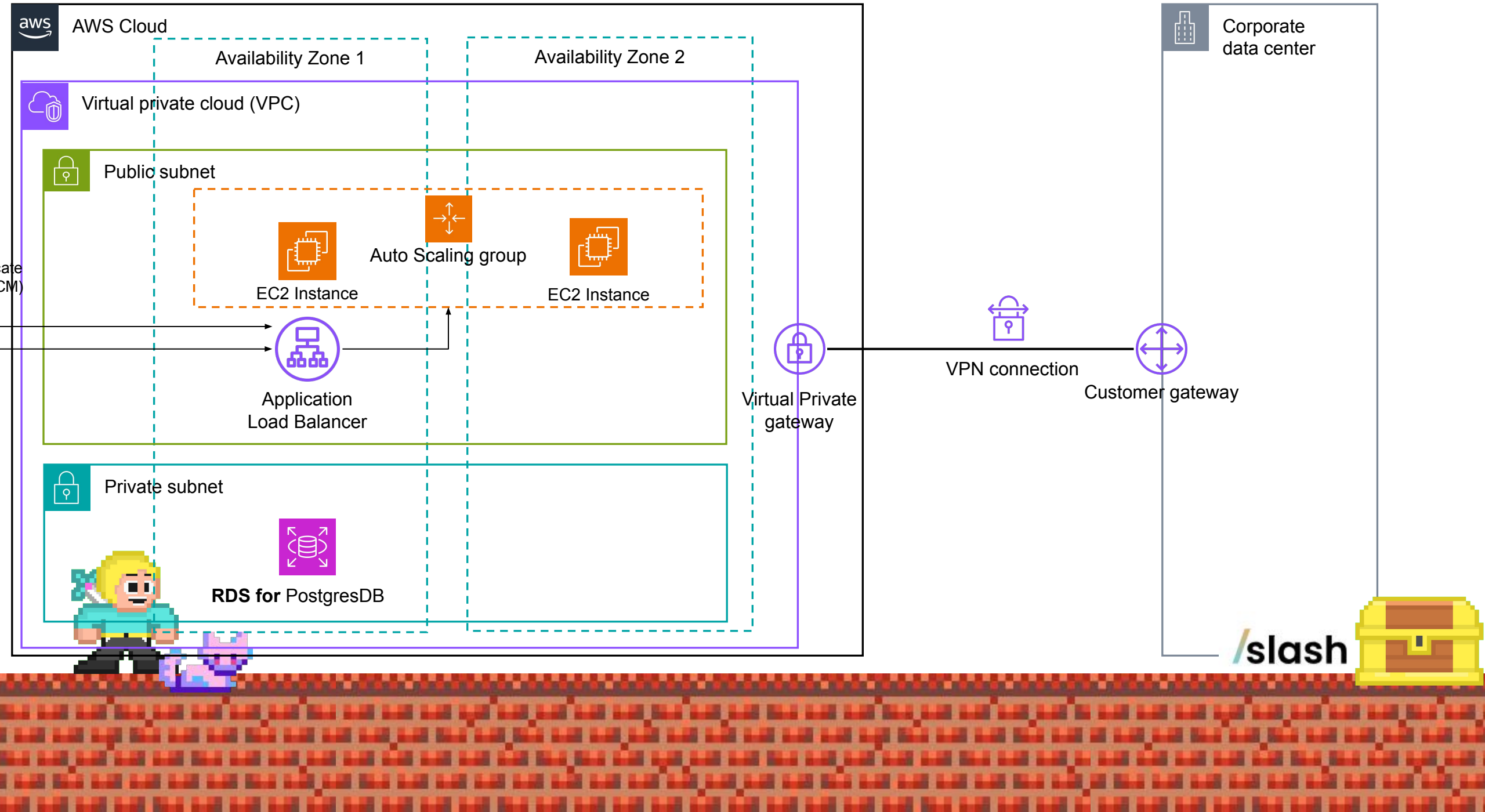
Private IP Site-to-Site VPN connection with AWS Direct Connect

AWS Site-to-Site VPN



/slash


4500
AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
WAF
Rule for KH
Public subnet
AWS Certificate
Manager (ACM)
Auto Scaling group
EC2 Instance
EC2 Instance
Corporate users
Access Employee
Insurance Portal
Route 53
Domain:
https://employee.examp
le-insurance.com
Application
Load Balancer
Private subnet
RDS for PostgresDB
slash


AWS Cloud
Availability Zone 1
Availability Zone 2
Virtual private cloud (VPC)
Public subnet
EC2 Instance
Auto Scaling group
EC2 Instance
Application
Load Balancer
Private subnet
RDS for PostgresDB
Virtual Private
gateway
VPN connection
Customer gateway
Corporate
data center
/slash

7000

Example of Steps to do Site-to-site VPNs

Below the iceberg:

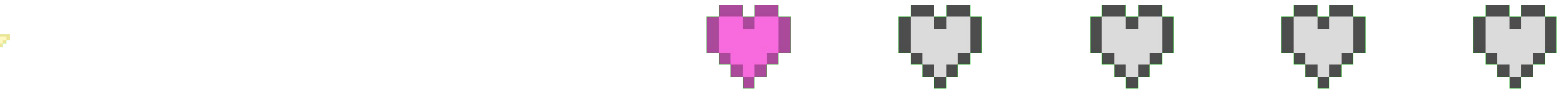
- **Create a customer gateway**
- **Create a target gateway on AWS side**

  (Virtual private gateway or Transit Gateway)
- **Configure Routing**

  (Route propagation / Add route to route table…)
- **Update Security Group**
- **Create VPN Connection**
- **Download Config file and Configure**

Customer Gateway Device

/slash



The end.

Thank you for your time!

**Slide use resources from Slides Carnival, AWS Documentation and Slash Presentation*

/slash