Case Study

Group: RDEnvi

Robertas Asvicas

Dmitry Lvov

Contents

[Project definition 3](#_Toc55857907)

[Infrastructure Diagram 3](#_Toc55857908)

[Infrastructure Components 4](#_Toc55857909)

[VPC 4](#_Toc55857910)

[Subnets 4](#_Toc55857911)

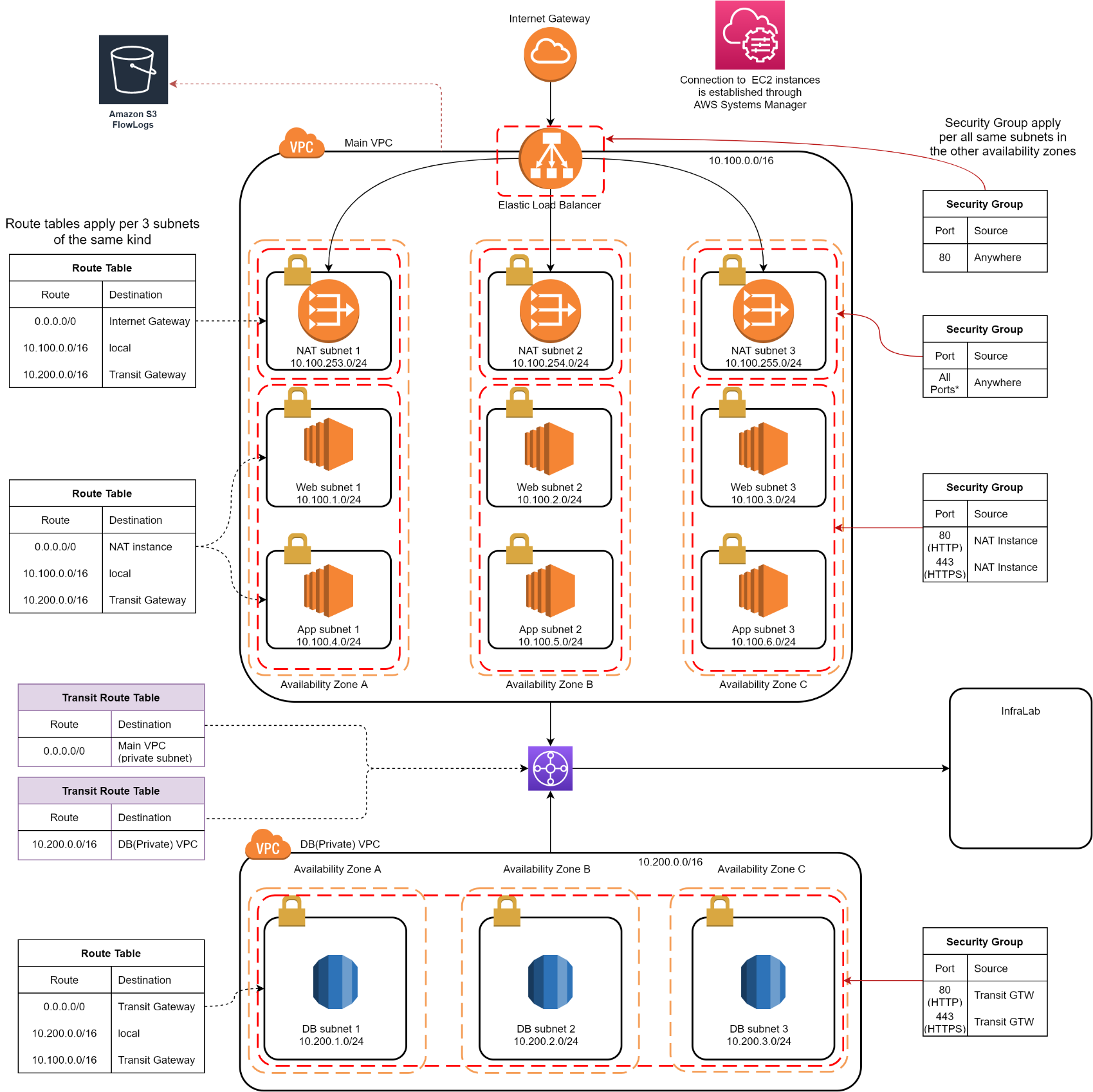
[NAT subnets: 4](#_Toc55857912)

[Web/App subnets 4](#_Toc55857913)

[Database subnets: 4](#_Toc55857914)

# Project definition

Our main goal in this project was to create suitable infrastructure for software students to host websites, applications. Infrastructure was supposed to be automated, scalable, and secure. We were using Amazon Web Services (further as AWS) for infrastructure creation, Ansible and Terraform for automation and different techniques for security implementations.

Infrastructure Diagram

Infrastructure Components

## VPC

Infrastructure is made out of 2 VPCs:

|  |  |
| --- | --- |
| Main VPC | Private VPC |
| CIDR block: 10.100.0.0/16 | CIDR block: 10.200.0.0/16 |
| Used to host everything BUT databases | Used to host ONLY databases |
| Has 3 Availability Zones | Has 3 Availability Zones |
| Has Internet Access | No Internet Access (only through Transit Gateway) |
| NAT subnets can be accessed from WAN | Can NOT be accessed from WAN |
|  |  |

## Subnets

There are 4 types of subnets in our infrastructure:

* NAT subnets
* Web subnets
* App subnets
* Database subnets

### NAT subnets:

Is hosting **NAT** **instances** which serve as a **middleman** between **Private** **subnet** and **Internet**. **Route Table** is configured that NAT subnet instances see Internet Gateway (further as IGW) – route to the Internet, Transit Gateway (further as TGW) – route to Database and local VPC Instances. Has its own **Security Group**, which allows all traffic Inbound into NAT subnet to all ports. **IP** addresses **range** varies **from 10.100.253.0/24 to 10.100.255.0/24**. Is deployed in all **3 Availability Zones** (further as AZ).

Web/App subnets:

Web and App subnets have **same configuration**. Are hosting **websites** (Apache, Nginx, Flask, etc.). **Route Table** is configured that it sees TGW – route to DB, NAT instance – route to IGW and local VPC instances. Has its own **Security Group**, which allows port **80** and port **443** (HTTP and HTTPS) traffic from NAT instances. **IP** addresses **range** varies **from 10.100.1.0/24 to 10.100.6.0/24.** Is deployed in all **3** **AZ**s.

### Database subnets:

Database subnets are hosting **database instances**. **Route Table** is configure that it sees TGW (route to Main VPC and IGW) and local VPC instances. Has its own **Security Group**, which allows port **80** and port **443** traffic **from** **TGW**. **IP addresses** range varies **from 10.200.1.0/24 to 10.200.3.0/24**. Is deployed in all **3 AZ**s.