Technical design

Centralized Firewall

Semester 6 - Infrastructure

Fontys - Eindhoven

Version

Version	Date	Author(s)	Amendments	Status
1.0	11/14/2022	Group 1		In progress

Table of Contents

1. Introduction

This document describes in technical detail what the multi-cloud environment with the firewall solution will look like based on the requirements we received. The specifications are explained and also why certain choices were made for the design. It is highly recommended to read our project plan before reading this document, because we explain the global information and requirements in detail and this document will be easier to understand with more knowledge about the project.

2. Network diagram

This is the first version of the Sogeti multi-cloud environment which we created for the first sprint. The goal of this sprint is to show to the stakeholder that that we can roll out the environment with IaC and apply firewall rules for the different VPC's and subnets.

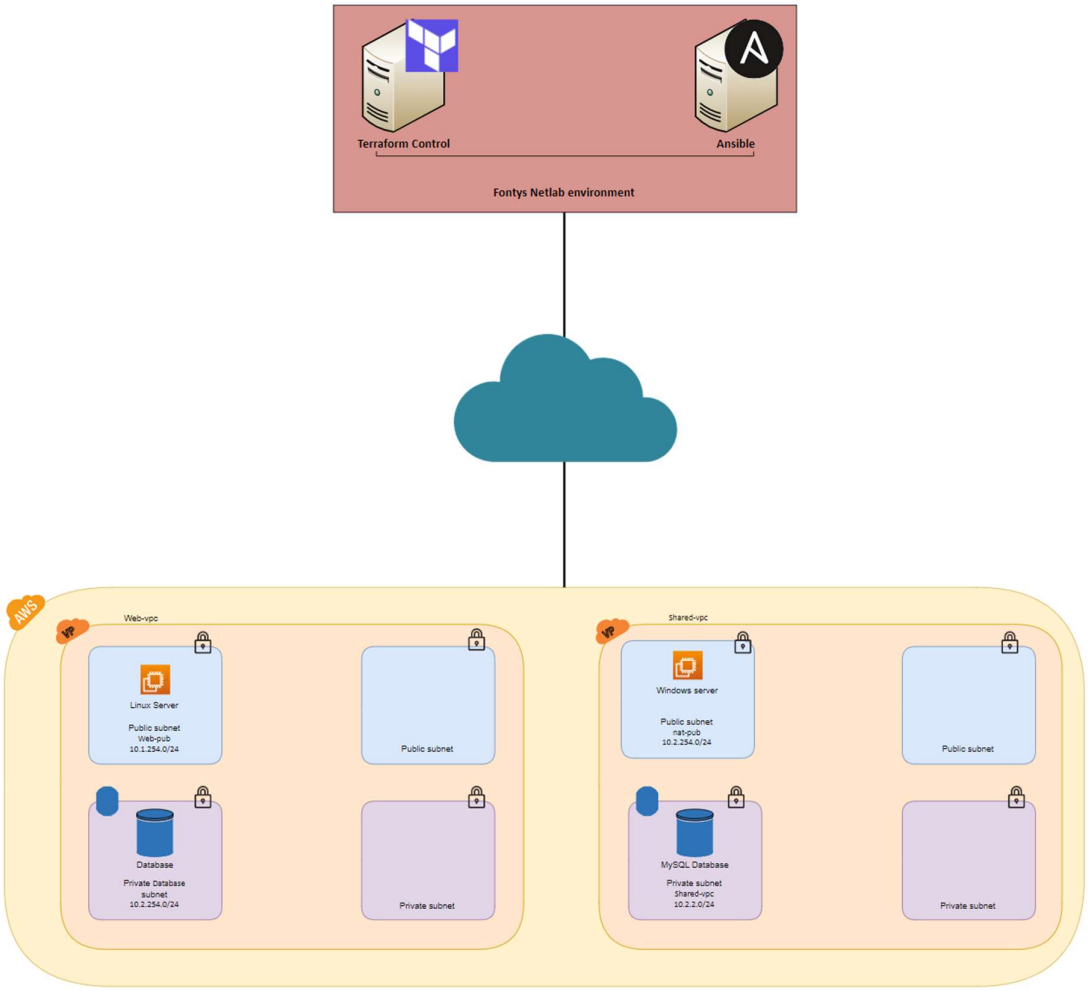


Figure 1: First version of the cloud environment

The environment works as following. On the diagram we have two environments: The first area is a virtual environment from Fontys University called the NetLab. In this area we host server with Ansible and Terrafrom installed on it. From our Terraform control server we are able to apply and roll out changes to the AWS environment. The second area depicts the Sogeti cloud environment. This is the production network of our project. In the future this will contain a firewall for the Sogeti clients to connect to. The first public subnet contains a webserver which is available for public.

3. Fontys Server - NetLab

3.2 Terraform control

This virtual machine is used to run the Ansible/Terraform scripts. It is a central point from where the administrator can run numerous different scripts for employing instances on the AWS environment. The AWS CLI is installed on it and is connected to a the groups IAM account (Luuk or Alex).

Hostname:	Terraform_control_vm
IP Address:	192.168.189.25/24
OS:	Ubuntu 20.04.5 LTS

Since we are using a test environment, the Terrafrom control server is installed for now in the NetLab, due the fact that we want to manage the cloud environment remotely. When the firewall solution is going to be used in real-time, the control server will probably be installed in a different on-premise environment to manage the cloud environment remotely. For future use it is recommended to place the Terraform server in an on-site environment. This is because of the security risks if anyone could access the server.

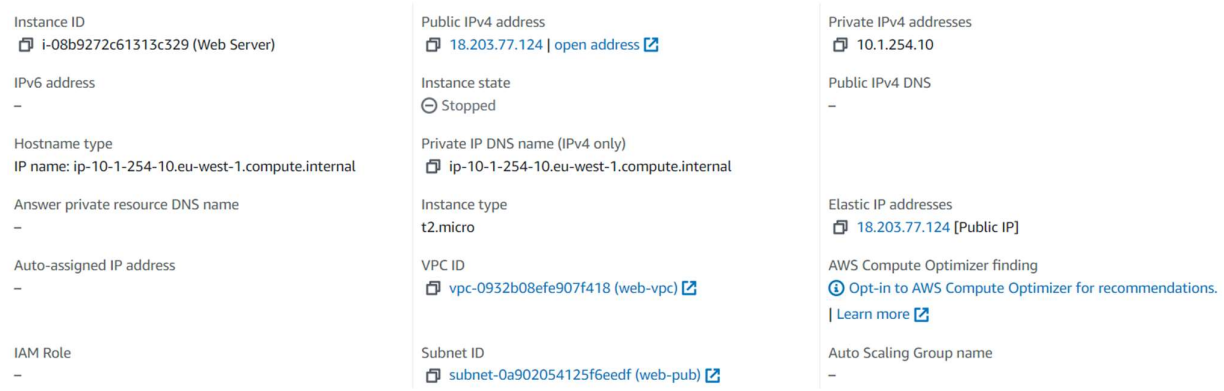
4. Amazon Web Services

We used the region Europe (Ireland) eu-west-1. This is due to a rule in the permissions on our AWS account and its not in our power to choose a region with better latency.

4.1 Service: EC2

This chapter contains and describes the different EC2 instances we use for our project. We use the different services to support the development of our cloud environment and test of the different resources are functioning as they should.

4.1.1 Web Server



This instance is for our public webserver. This EC2 instance helps us testing the AWS security rules. This compute instance is available in a public subnet so it should be accessible to public connections. In the future this instance could be removed.

4.1.2 Database

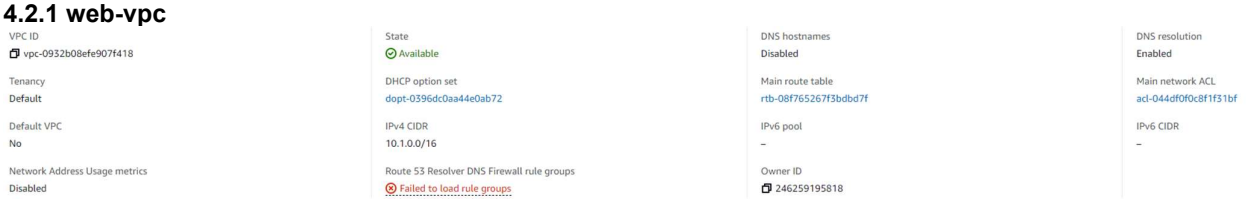
The database supports our webserver. At this moment the database is placed in a private subnet to show that this resource can only be accessed by the webserver. When the testing sprint is done, this resource can be removed from the environment.

4.1.3 Nat1

Instance ID i-0892e9a8cb47cc116 (Nat1)	Public IPv4 address 18.203.241.46 | open address	Private IPv4 addresses 10.2.254.254
IPv6 address –	Instance state Stopped	Public IPv4 DNS –
Hostname type IP name: ip-10-2-254-254.eu-west-1.compute.internal	Private IP DNS name (IPv4 only) ip-10-2-254-254.eu-west-1.compute.internal	
Answer private resource DNS name –	Instance type t2.micro	Elastic IP addresses 18.203.241.46 [Public IP]
Auto-assigned IP address –	VPC ID vpc-020580ce3fdc8022e (shared-vpc)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role –	Subnet ID subnet-03eecd55aa554d4ce (nat-pub)	Auto Scaling Group name –

4.2 Service: VPC

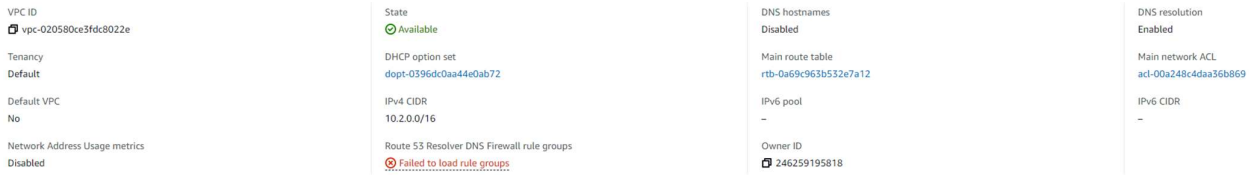
4.2.1 web-vpc



This is the VPC we use for the webserver. This VPC is accessible to the public to view the content on the webserver. The webserver VPC serves a demo purpose to show that we can control access between the VPCs

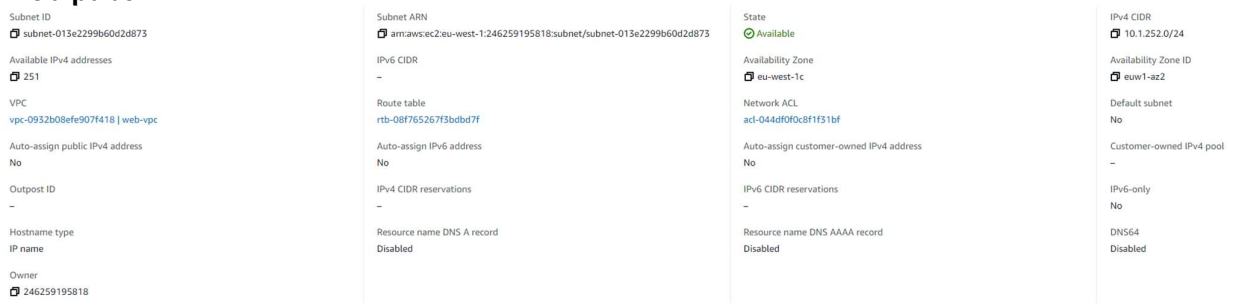
4.2.2 shared-vpc

The database is in a private VPC disconnected from the public VPC. The database is not accessible for public view on the internet, because of security reasons.



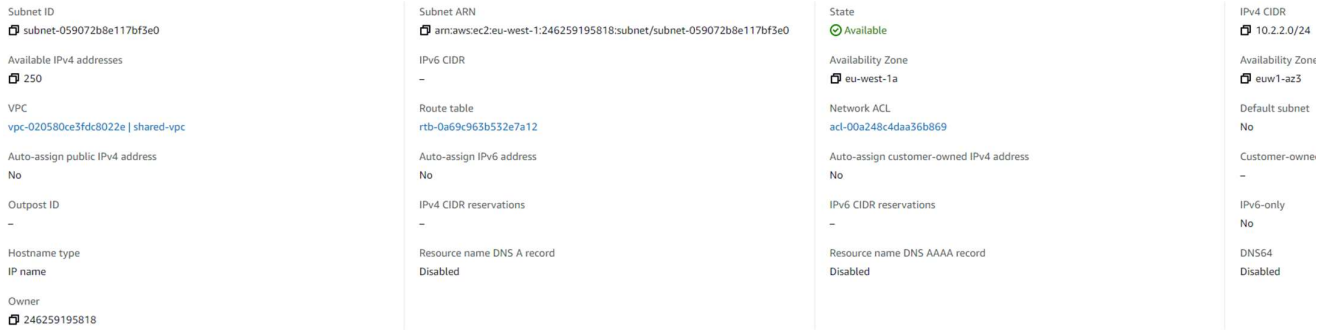
4.2.3 Subnets

Web-pub3



Web-pub3 is a public subnet which we used for testing our environment. The subnet is currently empty and could be removed in the future.

Database



This subnet is a private subnet in which contains our database. The subnet is set to private for security purposes. When the testing sprint is finished, this database subnet could be removed if we have no further need of RDS.

web-pub2

Subnet ID subnet-0db6f688af85b0f12	Subnet ARN arn:aws:ec2:eu-west-1:246259195818:subnet/subnet-0db6f688af85b0f12	State Available	IPv4 CIDR 10.1.253.0/24
Available IPv4 addresses 251	IPv6 CIDR –	Availability Zone eu-west-1b	Availability Zone ID euw1-az1
VPC vpc-0932b08efe907f418 | web-vpc	Route table rtb-08f765267f3bdbd7f	Network ACL acl-044df0f0c8f1f31bf	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool –
Outpost ID –	IPv4 CIDR reservations –	IPv6 CIDR reservations –	IPv6-only No
Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled	DNS64 Disabled
Owner 246259195818			

Web-pub2 is a public subnet which we used for testing our environment. The subnet is currently empty and could be removed in the future.

nat-pub

Subnet ID subnet-03eecd55aa554d4ce	Subnet ARN arn:aws:ec2:eu-west-1:246259195818:subnet/subnet-03eecd55aa554d4ce	State Available	IPv4 CIDR 10.2.254.0/24
Available IPv4 addresses 250	IPv6 CIDR –	Availability Zone eu-west-1a	Availability Zone ID euw1-az3
VPC vpc-020580ce3fdc8022e | shared-vpc	Route table rtb-0e73f8ddd079b5d55	Network ACL acl-00a248c4daa36b869	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool –
Outpost ID –	IPv4 CIDR reservations –	IPv6 CIDR reservations –	IPv6-only No
Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled	DNS64 Disabled
Owner 246259195818			

web-pub

Subnet ID subnet-0a902054125f6eedf	Subnet ARN arn:aws:ec2:eu-west-1:246259195818:subnet/subnet-0a902054125f6eedf	State Available	IPv4 CIDR 10.1.254.0/24
Available IPv4 addresses 250	IPv6 CIDR –	Availability Zone eu-west-1a	Availability Zone ID euw1-az3
VPC vpc-0932b08efe907f418 | web-vpc	Route table rtb-00c3d792f9c8884f5	Network ACL acl-044df0f0c8f1f31bf	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool –
Outpost ID –	IPv4 CIDR reservations –	IPv6 CIDR reservations –	IPv6-only No
Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled	DNS64 Disabled
Owner 246259195818			

4.2.4 Route tables

There are four route tables created for the public and private subnets. The tables specify how packets are forwarded between the subnets within the VPC.

Route table ID rtb-08f765267f3bdbd7f	Main Yes	Explicit subnet associations –	Edge associations –
VPC vpc-0932b08efe907f418 | web-vpc	Owner ID 246259195818		

Route table ID rtb-0a69c963b532e7a12	Main Yes	Explicit subnet associations –	Edge associations –
VPC vpc-020580ce3fdc8022e | shared-vpc	Owner ID 246259195818		
Route table ID rtb-00c3d792f9c8884f5	Main No	Explicit subnet associations subnet-0a902054125f6eedf / web-pub	Edge associations –
VPC vpc-0932b08efe907f418 | web-vpc	Owner ID 246259195818		
Route table ID rtb-0e73f8ddd079b5d55	Main No	Explicit subnet associations subnet-03eecd55aa554d4ce / nat-pub	Edge associations –
VPC vpc-020580ce3fdc8022e | shared-vpc	Owner ID 246259195818		

4.2.5 Internet gateways

A Internet Gateway is created for the public and private VPC's because these VPC's need to have internet access.

5. Process diagram

(Aleks will added here the information about the diagram)