

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	3
2. Network diagram	4
3. Fontys Server - NetLab	5
3.2 Terraform control	5
4.1 Service: EC2	6
4.1.1 Web Server	6
4.1.2 Database	6
4.1.3 Nat1	7
4.2 Service: VPC	8
4.2.3 Subnets	8
4.2.4 Route tables	9
4.2.5 Internet gateways	10
5. Process diagram	11

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.

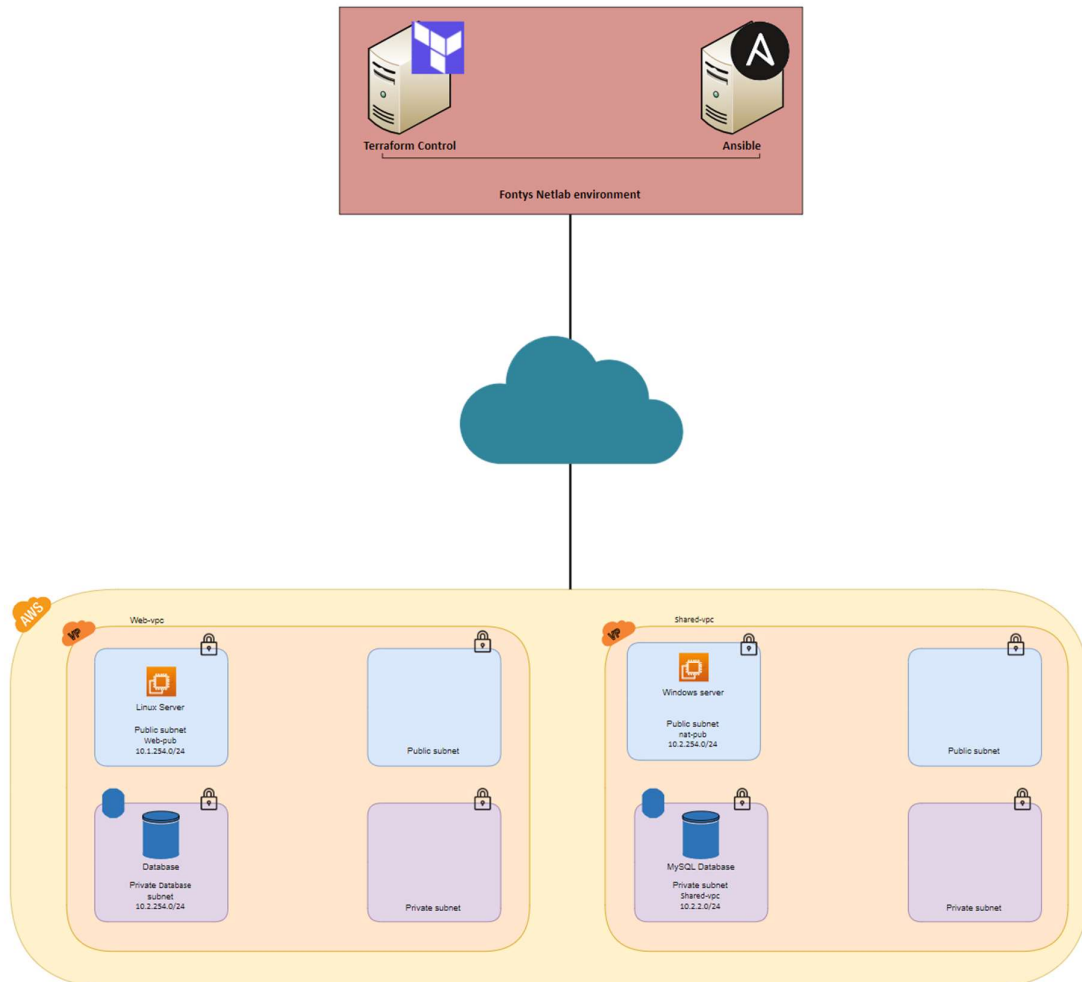


Figure 1: First version of the cloud environment

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 Terraform 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 Terraform 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

Instance ID i-08b9272c61313c329 (Web Server)	Public IPv4 address 18.203.77.124 open address	Private IPv4 addresses 10.1.254.10
IPv6 address -	Instance state Stopped	Public IPv4 DNS -
Hostname type IP name: ip-10-1-254-10.eu-west-1.compute.internal	Private IP DNS name (IPv4 only) ip-10-1-254-10.eu-west-1.compute.internal	Elastic IP addresses 18.203.77.124 [Public IP]
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address -	VPC ID vpc-0932b08efe907f418 (web-vpc)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0a902054125f6eedef (web-pub)	


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





Instance ID i-0fe75e3de7858b670 (Database)	Public IPv4 address -	Private IPv4 addresses 10.2.2.41
IPv6 address -	Instance state Stopped	Public IPv4 DNS -
Hostname type IP name: ip-10-2-2-41.eu-west-1.compute.internal	Private IP DNS name (IPv4 only) ip-10-2-2-41.eu-west-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address -	VPC ID vpc-020580ce3fdc8022e (shared-vpc)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-059072b8e117bf3e0 (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)
IPv6 address
–
Hostname type
IP name: ip-10-2-254-254.eu-west-1.compute.internal
Answer private resource DNS name
–
Auto-assigned IP address
–
IAM Role
–

Public IPv4 address
 18.203.241.46 open address 
Instance state
 Stopped
Private IP DNS name (IPv4 only)
 ip-10-2-254-254.eu-west-1.compute.internal
Instance type
t2.micro
VPC ID
 vpc-020580ce3fdc8022e (shared-vpc) 
Subnet ID
 subnet-03eecd55aa554d4ce (nat-pub) 

Private IPv4 addresses
 10.2.254.254
Public IPv4 DNS
–
Elastic IP addresses
 18.203.241.46 [Public IP]
AWS Compute Optimizer finding
 Opt-in to AWS Compute Optimizer for recommendations. Learn more 
Auto Scaling Group name
–

4.2 Service: VPC

4.2.1 web-vpc

VPC ID vpc-0932b08efe907f418	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0396dc0aa44e0ab72	Main route table rtb-08f765267f3bdbd7f	Main network ACL acl-044df0fc8f1f31bf
Default VPC No	IPv4 CIDR 10.1.0.0/16	IPv6 pool -	IPv6 CIDR -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 246259195818	

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.

VPC ID vpc-020580ce3fdc8022e	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0396dc0aa44e0ab72	Main route table rtb-0a69c963b532e7a12	Main network ACL acl-00a248c4daa36b869
Default VPC No	IPv4 CIDR 10.2.0.0/16	IPv6 pool -	IPv6 CIDR -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 246259195818	

4.2.3 Subnets

Web-pub3

Subnet ID subnet-013e2299b60d2d873	Subnet ARN arn:aws:ec2:eu-west-1:246259195818:subnet/subnet-013e2299b60d2d873	State Available	IPv4 CIDR 10.1.252.0/24
Available IPv4 addresses 251	IPv6 CIDR -	Availability Zone eu-west-1c	Availability Zone ID euw1-az2
VPC vpc-0932b08efe907f418 web-vpc	Route table rtb-08f765267f3bdbd7f	Network ACL acl-044df0fc8f1f31bf	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-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

Subnet ID subnet-059072b8e117bf3e0	Subnet ARN arn:aws:ec2:eu-west-1:246259195818:subnet/subnet-059072b8e117bf3e0	State Available	IPv4 CIDR 10.2.2.0/24
Available IPv4 addresses 250	IPv6 CIDR -	Availability Zone eu-west-1a	Availability Zone euw1-az3
VPC vpc-020580ce3fdc8022e shared-vpc	Route table rtb-0a69c963b532e7a12	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-owne -
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			

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

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

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

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

web-pub

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

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.

<div>Route table ID</div> <div>rtb-08f765267f3bdbd7f</div>	<div>Main</div> <div>Yes</div>	<div>Explicit subnet associations</div> <div>-</div>	<div>Edge associations</div> <div>-</div>
<div>VPC</div> <div>vpc-0932b08efe907f418 web-vpc</div>	<div>Owner ID</div> <div>246259195818</div>		
<div>Route table ID</div> <div>rtb-0a69c963b532e7a12</div>	<div>Main</div> <div>Yes</div>	<div>Explicit subnet associations</div> <div>-</div>	<div>Edge associations</div> <div>-</div>
<div>VPC</div> <div>vpc-020580ce3fdc8022e shared-vpc</div>	<div>Owner ID</div> <div>246259195818</div>		
<div>Route table ID</div> <div>rtb-00c3d792f9c8884f5</div>	<div>Main</div> <div>No</div>	<div>Explicit subnet associations</div> <div>subnet-0a902054125f6eedf / web-pub</div>	<div>Edge associations</div> <div>-</div>
<div>VPC</div> <div>vpc-0932b08efe907f418 web-vpc</div>	<div>Owner ID</div> <div>246259195818</div>		
<div>Route table ID</div> <div>rtb-0e73f8ddd079b5d55</div>	<div>Main</div> <div>No</div>	<div>Explicit subnet associations</div> <div>subnet-03eecd55aa554d4ce / nat-pub</div>	<div>Edge associations</div> <div>-</div>
<div>VPC</div> <div>vpc-020580ce3fdc8022e shared-vpc</div>	<div>Owner ID</div> <div>246259195818</div>		

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)

