Network Infrastructure & Services:
Dublin Pharmaceutical Limited

Bruno Ferreira Borges de Sá
Student ID: 2020084

A Guided Technology Project
for the Higher Diploma in Science in Computing

CCT College Dublin
January 2020

ABSTRACT

This project and documentation are divided and organized in three main chapters: networking, virtualization and data collaboration.

On the first chapter, we will make a network design, establishing VLAN's, servers, gateways, DNS, among others, in order to meet the requirements that the company expects regarding their departments and inner and outside communications. For this, the application Cisco Packet Tracer is used to emulate not only the network design but the whole configuration while providing the possibility of testing it.

For virtualization chapter, we will be setting up NAT and internal Networks on virtual machines created on VirtualBox. One of these virtual machines are running Zentyal for requested network services such as security.

The data collaboration, where we make a connection between DPL and the external partner, is a topic where a different path was taken. The virtualization, network and security settings were made on Google Cloud instead of VirtualBox. Google Cloud, like Microsoft Azure or Amazon Cloud is a standard business solution for collaboration. The software on top though, Mongo and Ubuntu, are still using open source, as requested.

In Mongo the data can be inserted, edited and shared between DPL and their partner YAC. The connection between these two companies was done through an intranet portal made with JavaScript, specifically node.js. The code of the portal is created and operated with Vue framework.

Table of Contents

1 INTRODUCTION

Networking and database are the key to the modern world nowadays. They work side by side and we can see its importance on the most tempestuous times we have been through in the last hundred years: the coronavirus pandemic. Thankfully, technology has advanced enough since the last pandemic crisis. Without them, it would not be possible to share so much information and numbers about infections in regions and the virus itself. The same thing applies to the vaccine that is already on the way to a great part of the world. It has been a worldwide taskforce that without science and communication would not be possible for medicine and pharmaceutical industry to achieve such steps in such a small time (Klimec & Hanel, 2020).

It has been delightful to be able to investigate and try so many possibilities regarding network, database and intercommunication that are so easily relatable given the scenario. It is impossible not to think how essential technology is and how lost we would be without it, and yet, knowing that it involves not only big issues like COVID-19 but basically any company or service.

This project is also about the pharmaceutical sector, which needs new solutions to connect its intern departments between them and external communication technologies. Besides the networking reformulation there is database and web solutions proposed to integrate the whole picture in a functional and modern way.

The proposition consists in providing the best solution for the upcoming changes in DPL (Dublin Pharmaceutical Limited. The company has a solid basis being one of the most successful in the market for fifteen years. Therefore, as a natural step, they have decided expand their business. The changes include moving their physical site and a partnership of data collaboration with another pharmaceutical business.

In order to provide the company a new information and communications technologies this work proposes solutions that will better contemplate this transition, since the old model no longer fits the new additions. Therefore, we must re-design a new network structure and service solution for the company to help them increase the standards of quality service for customers and providers.

Our purpose is to leave the company an excellent and functional system that will not only efficient, safe and fail-safe but also designed to make the communication between staff, managers and departments easy and intuitive.

2 PROJECT OVERVIEW

Before beginning to design a network service, information was collected on how the company work and delivery their service and products and the processes that happen before, while and after. In addition, all the departments and employee's duties and inter communications needed to be deeply analyzed and traced so we can come up with a high-level service solution that will ensure the efficiency improvement.

Department	Number of employees
Research and Development (R&D)	300
Manufacturing	550
Sales and Marketing	150

Table 1

Keeping in mind how the company network and communication should be, we have studied and analyzed the current scenario. Only then we could have an idea of the depth of complexity this project demands. DPL has also requested us to use **only open-source software** for the design and implementation.

2.1 Network Infrastructure Design

Precisely, these are the tasks defined as part of network infrastructure solution. Through them we know what we want to achieve and will study the possibilities on how to get them done. One by one, we now are going to separate them by topics and tell and explain our decisions, its pros and cons and have a reflection on how they would apply given the scenario and limitations.

- Highly available and fault tolerant network design

- Secure inter-communications within internal divisions
- Communication between partner sites
- Segregated Wireless LAN solution for guest access
- VOIP solution
- Automated IPv4 address allocation
- Logical network subdivisions
- Access Control
- Name resolution services
- Secure local and remote management of networking devices
- Device Security best practices

2.2 Services of Proof Concept

After solving the whole network structure, we will then show the proof of concept, showing this system working. It was requested that the following implementations were applied in order to fill the company's demands regarding front-end and back-end web services.

• Detailed Inbound and Outbound security as specified in the project overview
• Automatic IPv4 address allocation
• Web Server services
• Custom intranet portal design
• Remote Access services
• Secure File Transfer capabilities
• Account management home directories

2.3 Project Relevance

DPL's upgrade on network infrastructure and service solution is an opportunity to converge many contents given on disciplines such as Network and Virtualization. The topics cover highly relevant issues for any IT student that aims to work with data, troubleshooting and networks or simply have a basic knowledge towards it.

This final asset also mixes subjects which are both challenging and pleasant because it gives a clearer idea of a real-world workplace. As mentioned before, any person that works or has any interest in technology knows how much IT has been important during the pandemic crisis the world has been through. These lessons and experiments with network and data gives us a great perspective on how things work. Although it doesn't compare to the proportion of a worldwide event, it has been very enriching being able to understand a small part of the network and data base environment.

3 PLANNING METHOD

When it comes planning, we built up the strategy that would more fit the project. The waterfall method was the chosen one to better achieve our goals. Although agile is a modern and dynamic method we decided to go with the traditional one. By far more reasons waterfall would fit us better. First the experience factor, agile is recommended when you have previously worked on a similar project before. Second because agile works better in a team where multiple areas are covered simultaneously, which is not the case. Third, waterfall would give us a better progress management especially working in a tight deadline.

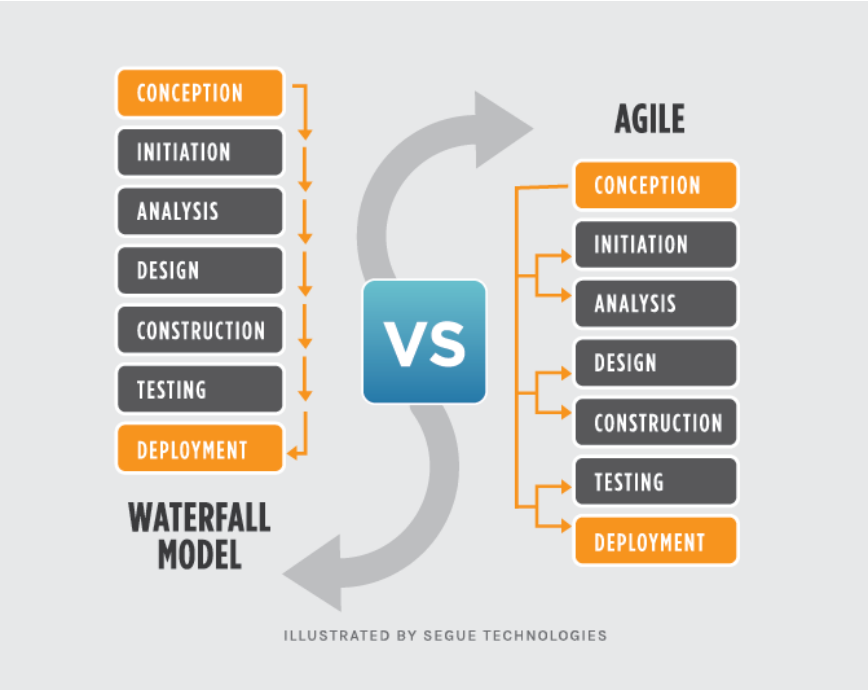
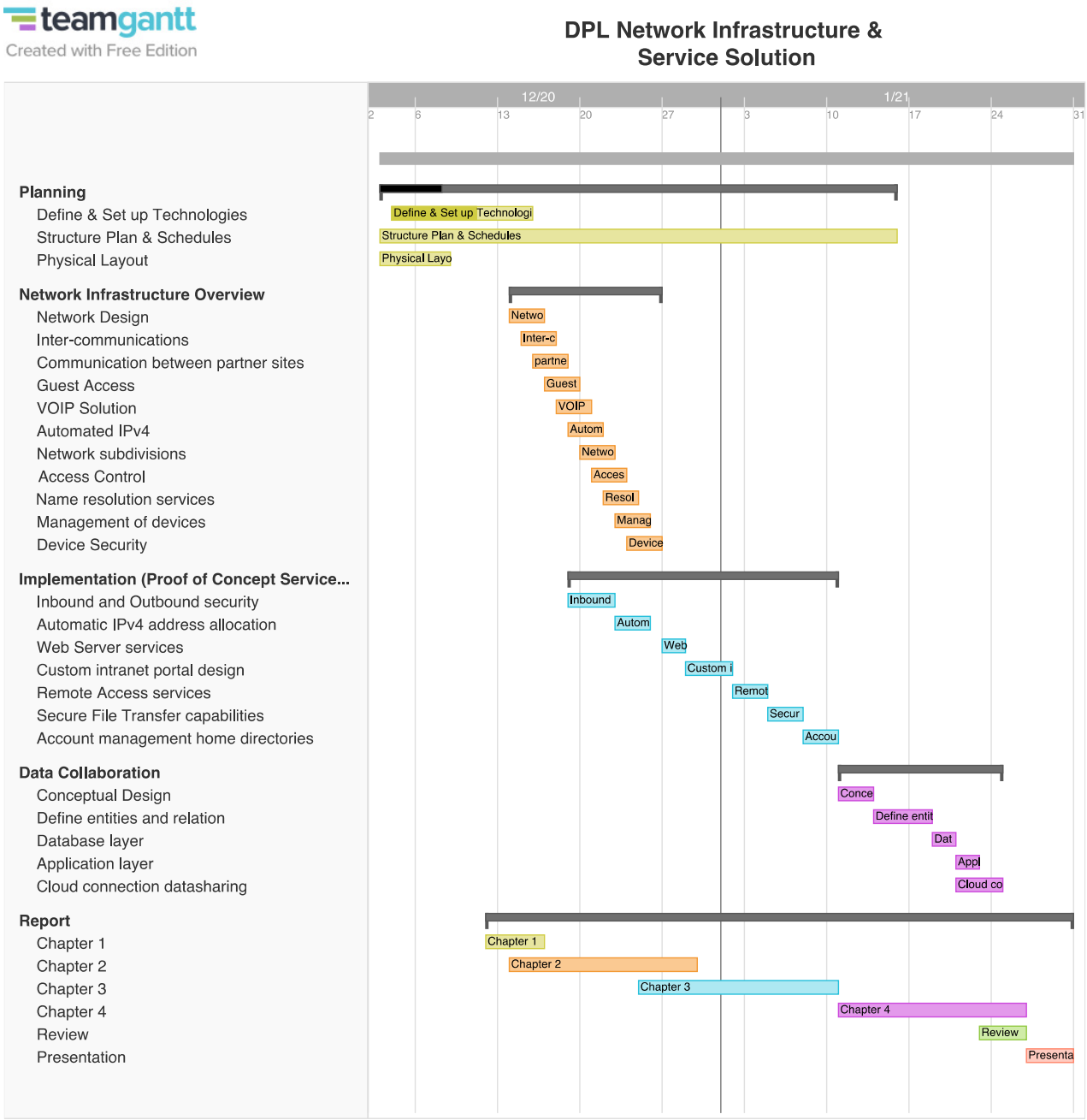


Figure 1: Waterfall vs. Agile. available at: https://www.seguetech.com/waterfall-vs-agile-methodology/

The process of making an overall plan showing specific goals against time were the reasons why it would suit our developing through prioritizing objectives and defining what tasks would depend on primary tasks to be accomplished (Lucidchart, 2017).

The chart that illustrates our planning is Gantt chart, provided by Team Gantt[1]. It features our schedules, timeline, sequence of tasks. Meanwhile the graphics like colors and categories helps us see the bigger picture as much as the singular works to be done.



[1] TeamGantt is an online project planning software that brings gantt charts online available at: https://www.teamgantt.com/

4 NETWORKING

Taking in consideration DPL requirements and limitations, some decisions were made regarding the software and methods adopted to deliver a decent solution and network implementation that will fulfill all the requirements proposed above. The following topics will cover them one by one providing explanation, troubleshooting and decision making for each one.

4.1 Highly available and fault tolerant network design

4.1.1 Technical considerations

The network design is based on some requirements. The first one is that all data center and external connections need to be high available (Data Center Knowledge, 2015). Solution is to setup redundant hardware infrastructure. It's common practice to operate at least 2 different data centers. As Caroll (n.d.) estates, each data center is equipped with the symmetric amount and setup of hardware and configuration. In order to guarantee a transparent failover, the software company Oracle (n.d.) recommends using planned downtime to switch services from one data center to the other and back. Especially the application configuration needs to be updated at all times. Examples are local user, passwords firewall configurations, web certificates, NAS mount points, storage access, job controls, backup, database access, etc. Special and ongoing care is necessary to achieve this service level. For business continuous management, such a redundant configuration is almost required, if a disaster should be handled in hours or up to one day. Each data center has to be sized being able to handle the standard load or according to the service level agreements, if no dynamic scaling as in a cloud is possible.

Moving on, all data center and external connections need to fulfil fault-tolerance. A fault tolerant service is protected against a single point of failures in such a way, that the central service is always up and reachable end-to-end to the clients like applications, servers or users. Best example is the time service client (ntpd), which builds average time based on two or more independent time sources and its own clock. Solution to fault tolerant service levels is to configure active/active network connections and to enforce stateless connections, that ensures

no loose data during an outage (Liu 2016, p. 4). Active/active also means to use two different providers of the same service, e.g., two different internet service providers, two different energy providers, using two different uninterruptable power supplies (UPS).

The most appropriate solution found is then to build two data centers with redundant, symmetric configuration based on established network infrastructure componentizes with a proven history of enterprise support and experience, based on data center best practices. Refer to the market analysis in the next sub chapter.

The core network has to be protected to the outside world with a protecting network layer and supported special hardened devices like intrusion detection, firewalls, protocol changes. Solution to this is to implement an Enterprise Edge zone, also called demilitarized zone (DMZ), where a complete network separation between enterprise and internet and service provider is guaranteed. All network traffic be it incoming or outgoing is analyzed, logged, configured and managed, no plain text data is transmitted, since everything is encrypted.

There are three different network types necessarily. First one are connections to other branches, then remote access for home office or third-party access, for support, data exchange, among others. And finally, some extra connections to redundant data centers. Solution to this is to build three separated networks in edge network: DMZ/Internet, WAN, Remote Access VPN). Also, outside connections need to be highly available and fault tolerant. In order to make it possible, the decision is connecting to two different internet service providers (ISP).

4.1.2 Market Research

Cisco was the technology and solution leader in building the global network infrastructure and leading enterprise partner since the late nineties. Market share research as of today shows competition though, but they still are the safe bet:

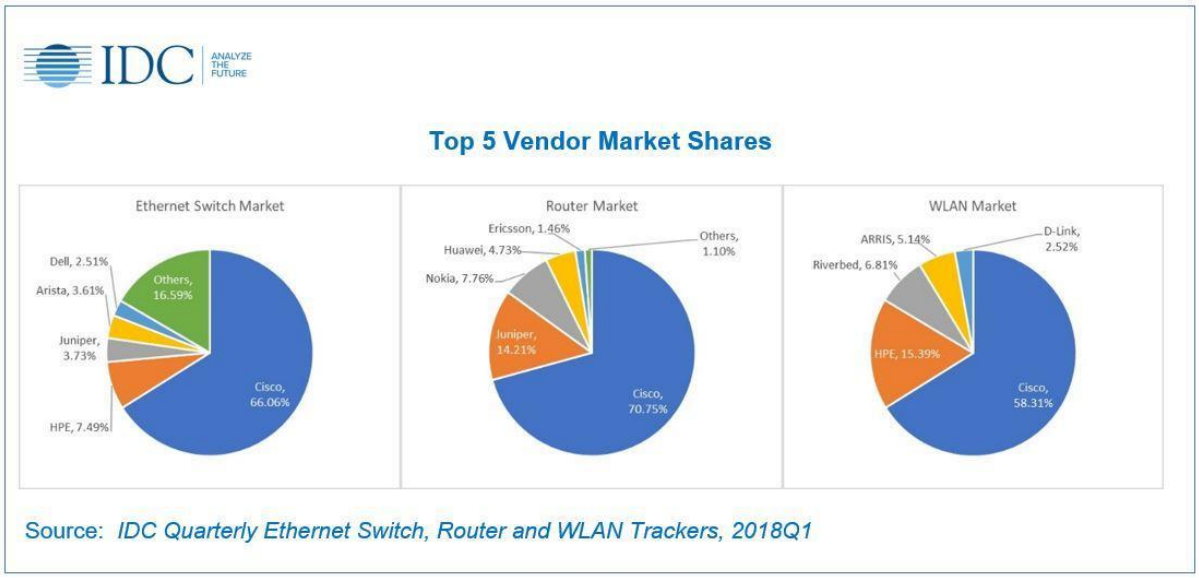


Figure 2: Cisco's market share in 2018. Available on: https://www.idc.com/getdoc.jsp?containerId=prUS46830820

Some identified Cisco's top competitors in the other markets it leads are: Avaya (enterprise voice systems) and Juniper Networks (network security). The researchers also cited some vendors that are making steady gains: Palo Alto Networks in network security; Arista Networks and Huawei in Ethernet switching; and Dell EMC in data center servers, where it's the No. 2 vendor. Financial health of Cisco is reflected with valuations on the stock market, where Cisco is listed on NASDAQ:

Figure 3: Cisco market share over the years. Available on Google.com

The conclusions regarding the financials parameters of Cisco are that marketing capitalization is big, therefore the company has enough margin to invest into research and development. Their Price/Earnings ratio is below twenty and positive, which resembles a quite healthy earning situation.

There are recurring concerns for Chinese companies, especially Huawei on how data security is guaranteed and if business relevant, confidential data is not shared with the Chinese government. Therefore, I would not recommend Huawei for DPL's strategic solution for network architecture.

Based on cisco's architecture principles and best practices and based on the technical requirements, the solution proposed is the following high level network architecture, Cisco based:

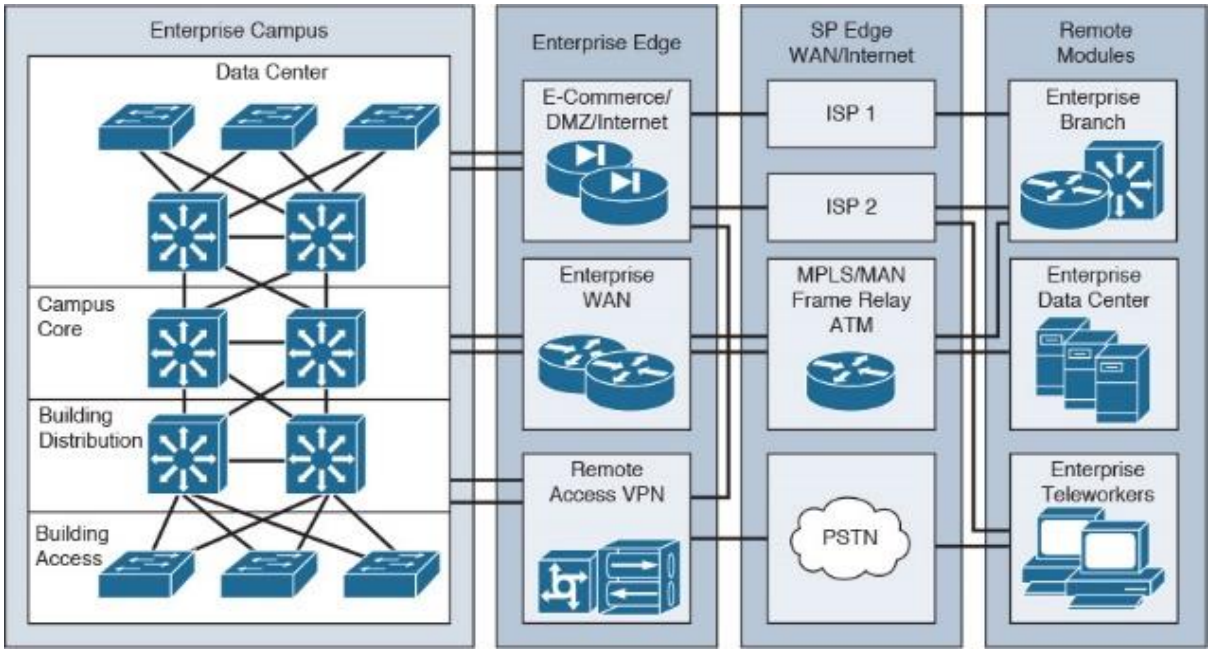


Figure 4: DMZ Demilitarized zone, ISP Internet service provider, VPN Virtual private network, PSTN Personal switched telephone network, ATM Asynchronous Transfer Mode, MPLS/MAN Multiprotocol Label Switching/Metropolitan Area Network, WAN Wide area network.

4.2 Network Design and Layout

4.2.1 Initial Step

Based on the technical and business considerations in previous chapters, DPL has decided to further use and extend their data center network to build a high available and fault tolerant architecture relying on Cisco technology for switches and routers. Further requirements from DPL have been listed below. In order to show the detailed network diagram and to provide the configuration steps as tested IOS (Cisco OS) commands, Cisco's network emulation software will be used, the packet tracer.

It is a big advantage for DPL to share the proposed layout with Cisco engineering in order to approve or consult on the considered solution (import/export as config file or as package). Cisco Packet Tracer is an emulation software is available for free.

In order to show features and functions, let's start with the default example t*cp_test_app.pkt* which reflects a simple scenario of a network ping between two servers in a data center connected to a switch and a router. The scenario is shown below and will be used to emulate the complete network design of DPL with additional requirements.

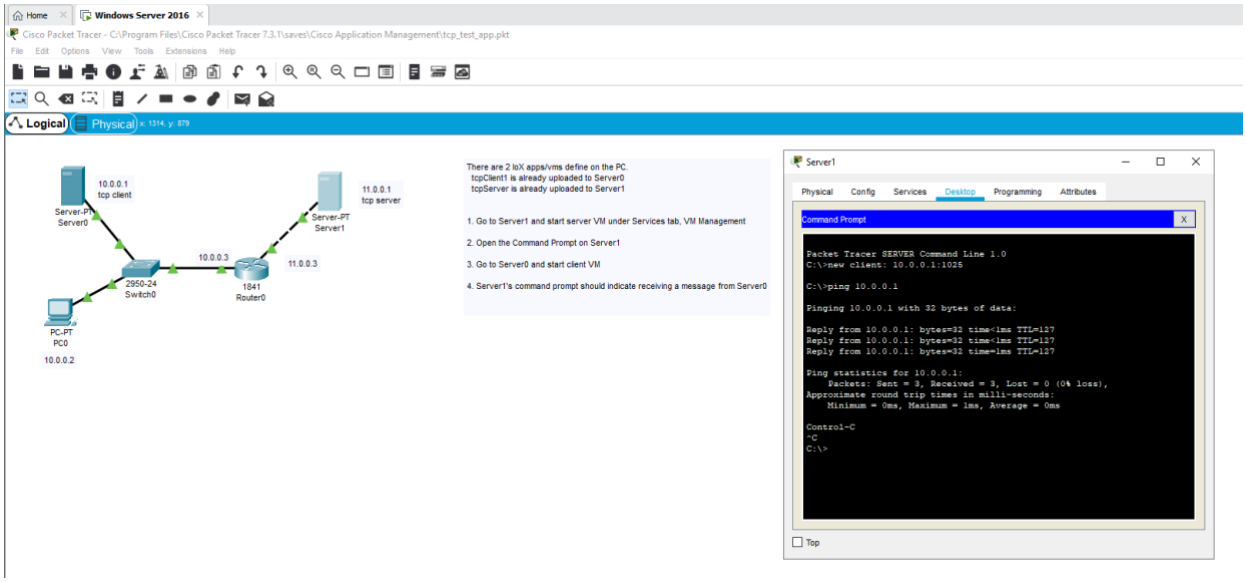


Figure 5: Ping emulation on Cisco Packet Tracer

4.2.2 Final Network Design

According to the requirements, which you can see technical considerations above and logical network subdivisions below, the final Cisco router configuration can be defined and configured in packet tracer:

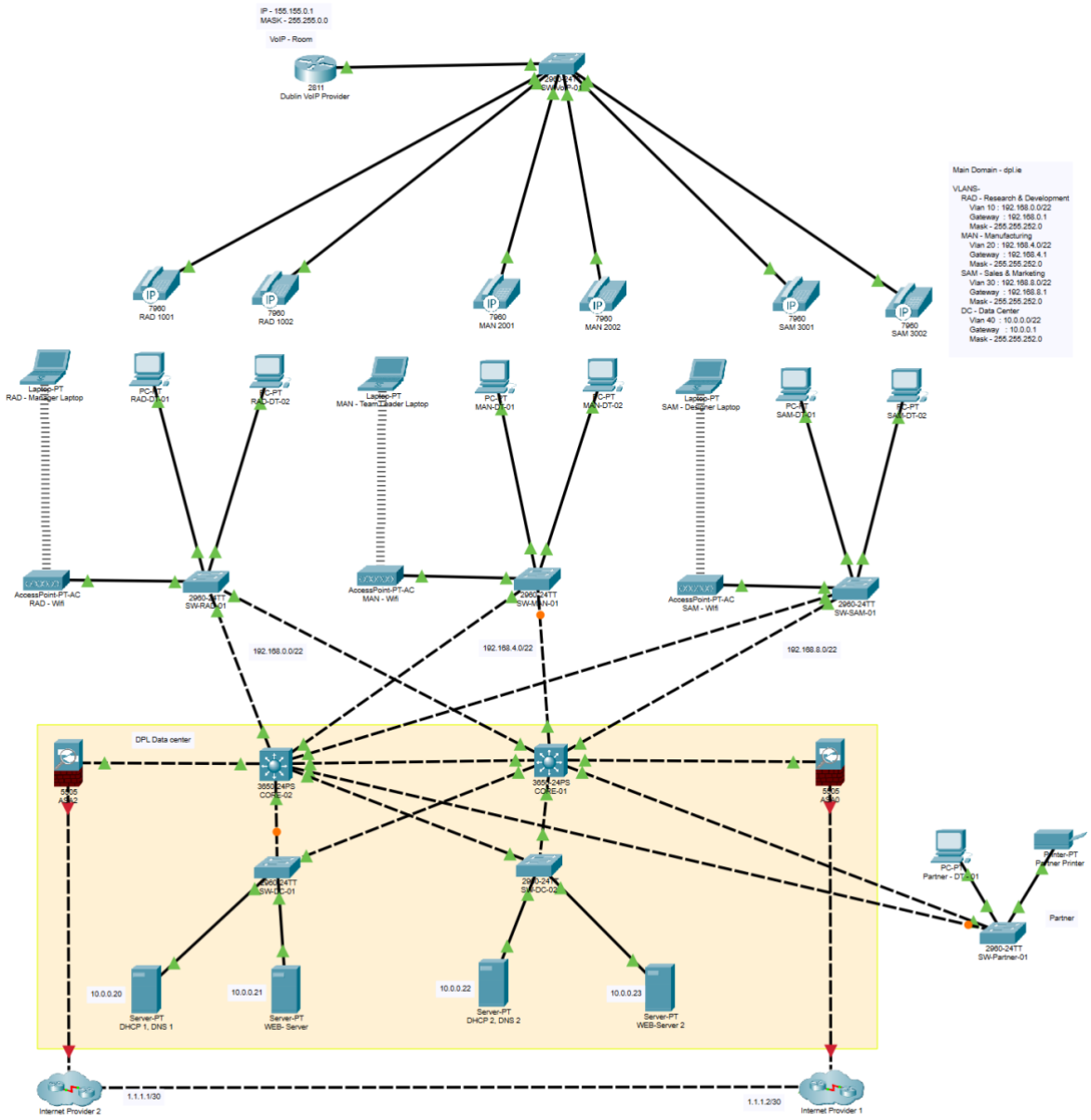


Figure: Final DPL Network Design

4.3 Secure inter-communications within internal divisions

Each division is separated by its own VLAN and each network device is isolated from a network broadcast. Ports on the routers are then assigned to each VLAN.

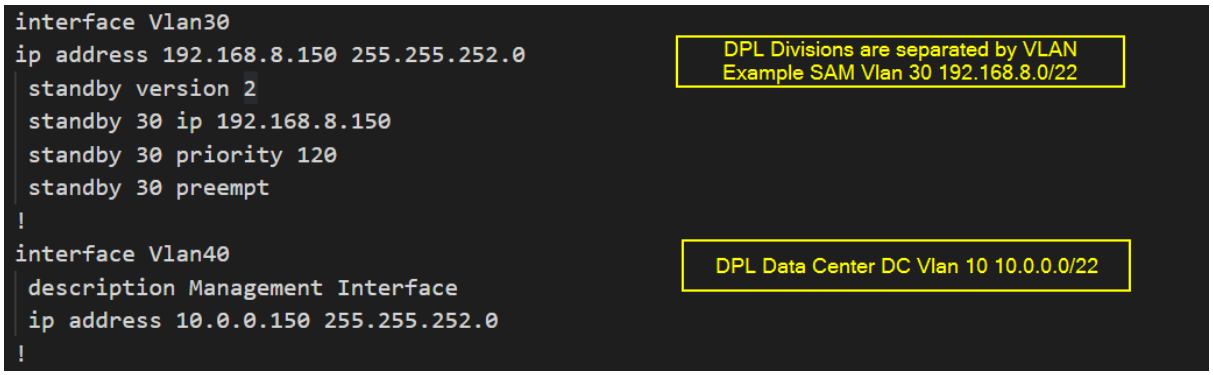


Figure 6: separated VLAN examples

These are some general guidelines in creating VLAN's. A VLAN creates a boundary between devices, so the goal is to plan the boundaries that will improve network functionality and security. As pointed by Reid (2007), the following instructions are how the VLAN's were built:

> **Grouping devices by traffic patterns -** Devices that communicate extensively between each other are good candidates to be grouped into a common VLAN. **Grouping devices for security -** It is often a good practice to put servers and key infrastructure in their own VLAN, isolating them from the general broadcast traffic and enabling greater protection. **Grouping devices by traffic types -** As discussed in this How To, VoIP quality is improved by isolating VoIP devices to their own VLAN. Other traffic types may also warrant their own VLAN. Traffic types include network management traffic, IP multicast traffic such as video, file and print services, email, Internet browsing, database access, shared network applications, and traffic generated by peer-to-peer applications. **Grouping devices geographically -** In a network with limited trunking, it may be beneficial to combine the devices in each location into their own VLAN. (Reid, D. 2007).

4.4 Communication between partner sites

The communication with partners follows Cisco's guidelines[2], which states that this type of connection needs to fulfill the following requirements:

- Transparent Access with automated authentication
- Security by encryption over public network
- Best practices by established industrial standards

The implementation is based on a layer 2 connection between Cisco switches. This communication can be extended securely within an IPsec tunnel over multiple layer 3 hops:

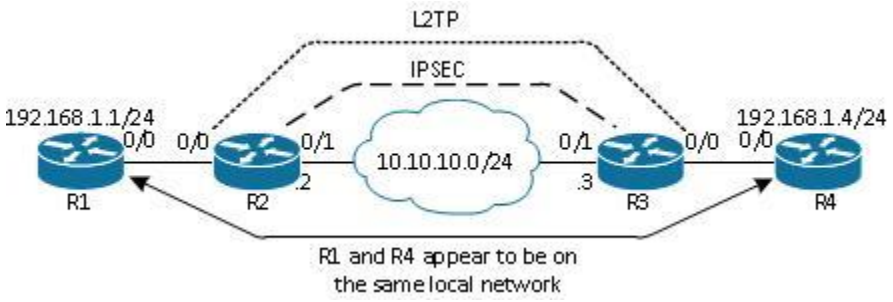


Figure 7: Network Topology

We will be using Adaptive Security Appliances (ASA) from Cisco to configure the enterprise firewall.

4.5 Segregated Wireless LAN solution for guest access

The first reason for a segregated wireless LAN solution is network speed. Both costumers or collaborators and the company will have their speed compromised if they share the same network. For sure DPL could separate a limited and specific amount of kbps for guest access

[2] Available from: https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116207-configure-l2tpv3-00.html

and if they have a really good provider this should not be a problem and the main priority, the company, won't have their performance interfered by bad network.

But performance is not the only reason, in fact, it is not even the main reason. Having a segregated LAN solution is also a security step. If guests are connected to the same network that fills the company's database, this makes a lot easier for a potential attack. Although there are many ways of avoiding that guests can have access to anything, like a limited usage, temporary login and password this is one more layer of security in order to preserve the company's integrity.

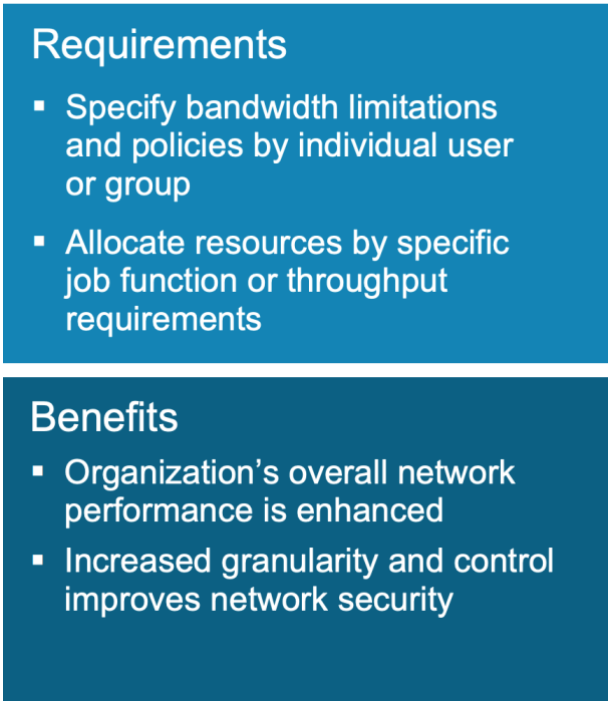


Figure 8: Guest Network Bandwidth Policy Controls. Available from: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/guest-access-solution/DeployingGuestAccess_051308.pdf

4.6 VOIP solution

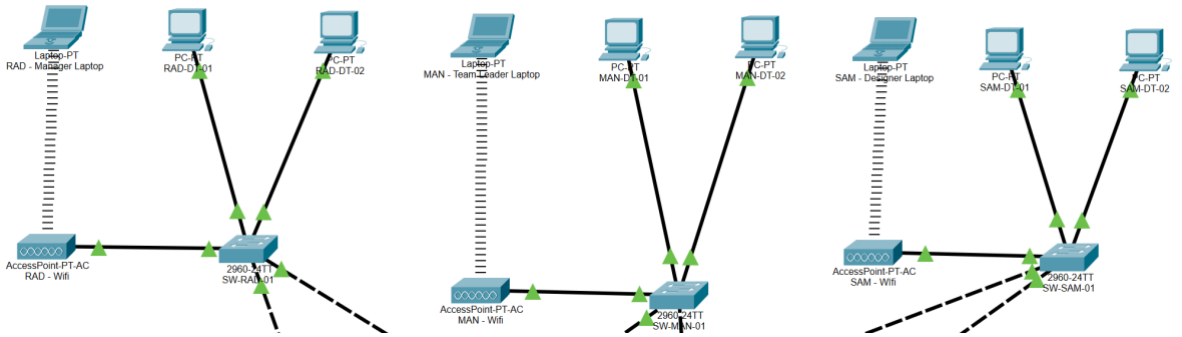


Figure 9: AccessPoint

When it comes to choosing a VoIP service some questions were taken into consideration regarding our application and how DPL would get the best of it according to the answers we came up with.

For instance, the first question was if we were providing the premise sharing the network with the departments VLANs or hiring a hosted service specifically for that. The answer is hiring a host because a managed (hosted) service provider reduces the company's resources and responsibilities while the premise option simply provide de voice network and DPL would administer its own network. A managed (hosted) service provider reduces your resources and responsibilities while the premise option simply provides the voice network and you administer your own network (Contact Centre World 2017).

In the picture below we can check how the implementation looks like. There is a specific provider for the phones and they do not connect or relate anyhow with the company's network.

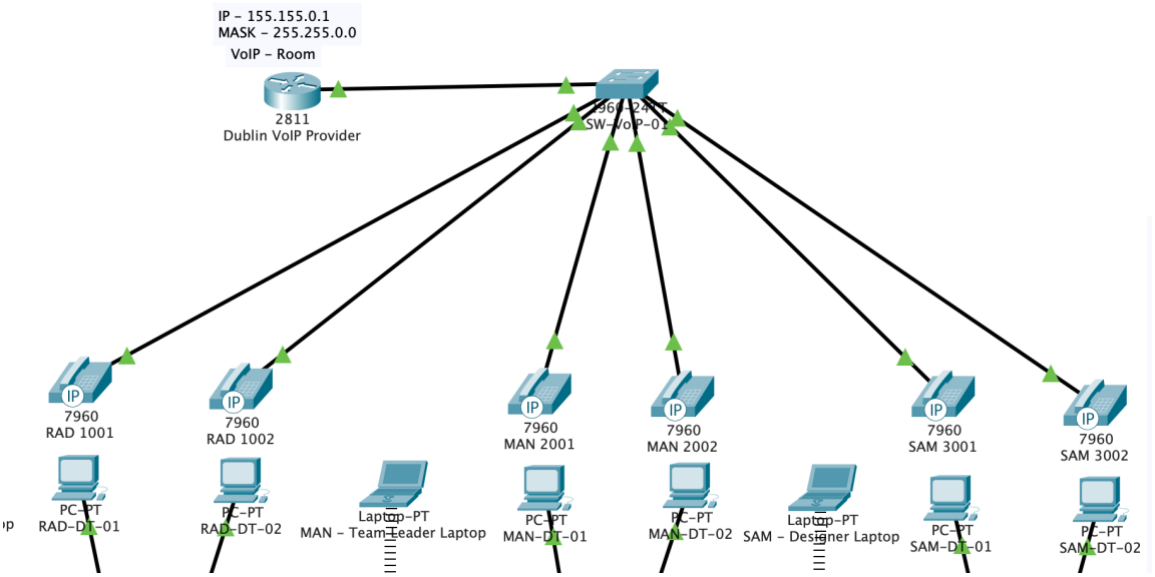


Figure 10: VoIP network design.

4.7 Automated IPv4 address allocation

For a long time, the Dynamic Host Configuration Protocol is able to provide fundamental network service for a client. Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. For Kerravala (2018), the ability to network devices quickly and easily is critical in a hyper-connected world, and although it has been around for decades, DHCP remains an essential method to ensure that devices are able to join networks and are configured correctly. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. Its usage can be explained by the following:

- Automation required
- Different network segments need different DHCP parameters

While the implementation successfully fulfills the requirements because of:

- One pool has to be declared for each VLAN
- The correct default gateway is configured for each VLAN
- The **IP helper-address <IP address>** configures DHCP request forwarding to the configured <IP address> DHCP server.

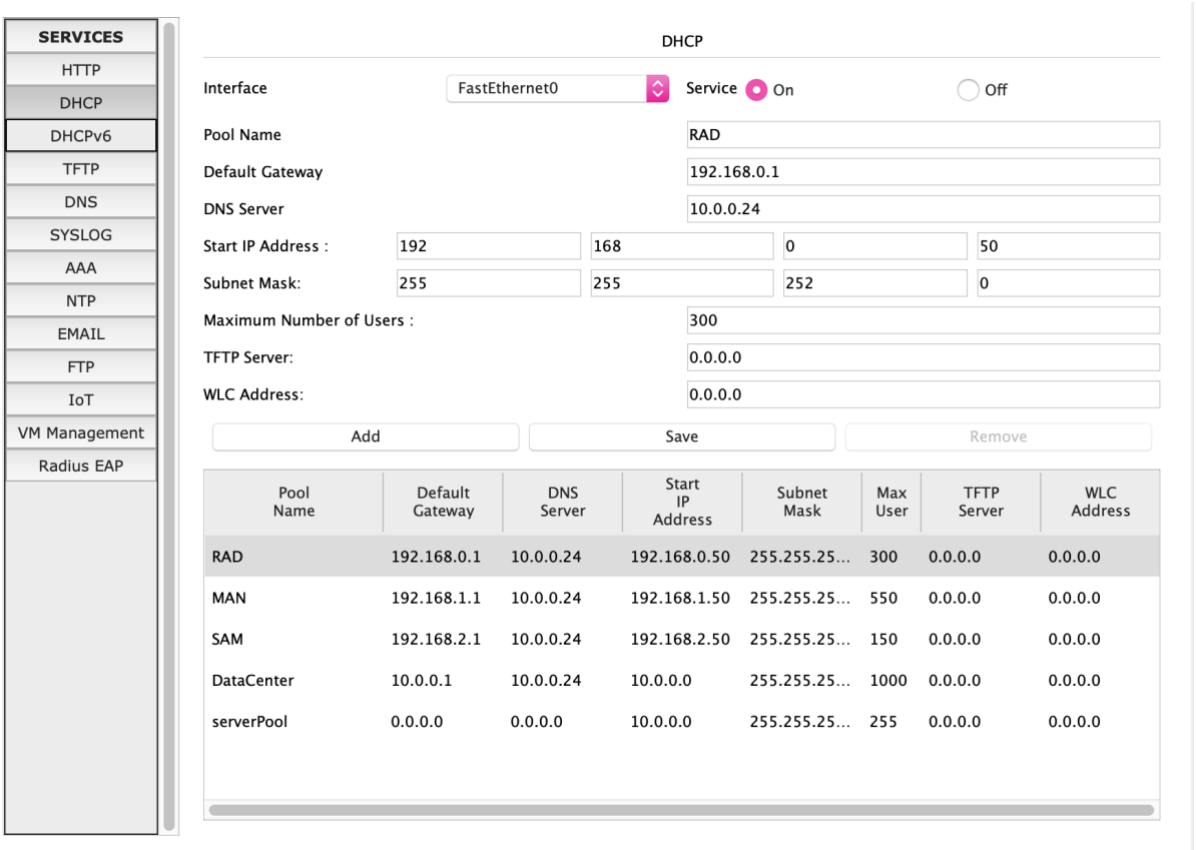
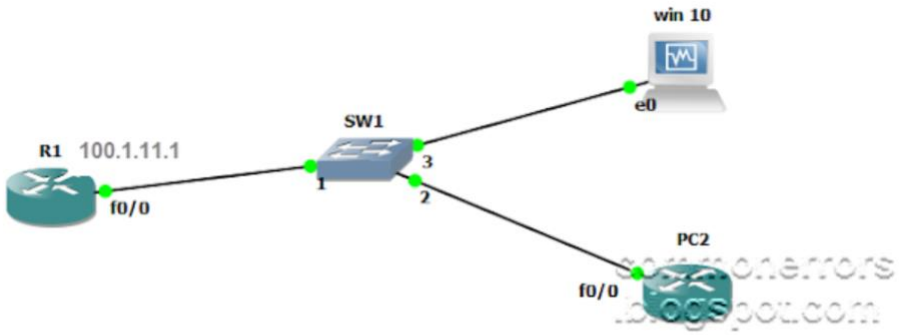


Figure 11: DHCP solution on Cisco Packet Tracer

IP address pools are declared on the DHCP management tab of the server like on the picture above. One pool has to be declared for each VLAN. Never forgetting to configure the right network settings and default gateway (Router0 FA 0/0.10 and FA 0.0.20 IP address) for each VLAN (Microsoft Docs, 2020).

The IOS commands look like this:



Following configuration are required for making the Router as DHCP server.

DHCP server (R1) Configuration:
R1#enable
R1#Configure t
R1 config)#ip dhcp pool ipranges
R1(dhcp-config)# network 100.1.11.0 255.255.255.0
R1(dhcp-config)#dns server 100.1.11.1
R1(dhcp-config)#default-router 100.1.11.1
R1(dhcp-config)#lease 10 (this command will set the IP lease for 10 day, view more Cisco Commands)

How to exclude the IP addresses from DHCP range

R1(dhcp-config)#ip dhcp excluded-addresses 100.1.11.20 100.1.11.31

Following are the configuration required on router which will act as DHCP client.

PC2 Configuration:
PC2#enable
PC2#Configure t
PC21#no ip routing
PC2#inf f0/0
PC2#ip address dhcp
PC2#no shutdown

Figure 12: DHCP lab in GNS3 | How to Configure DHCP on Cisco Router. Available from: http://commonerrors.blogspot.com/2015/08/dhcp-lab-in-gns3-how-to-configure-dhcp.html

4.8 Logical network subdivisions

A logical network division are relevant because the Research and Development department needs to be separated from Manufacturing and Sales departments. Besides, the user networks need to be separated from data center networks. Also, edge networks need to be separated from data center and internet.

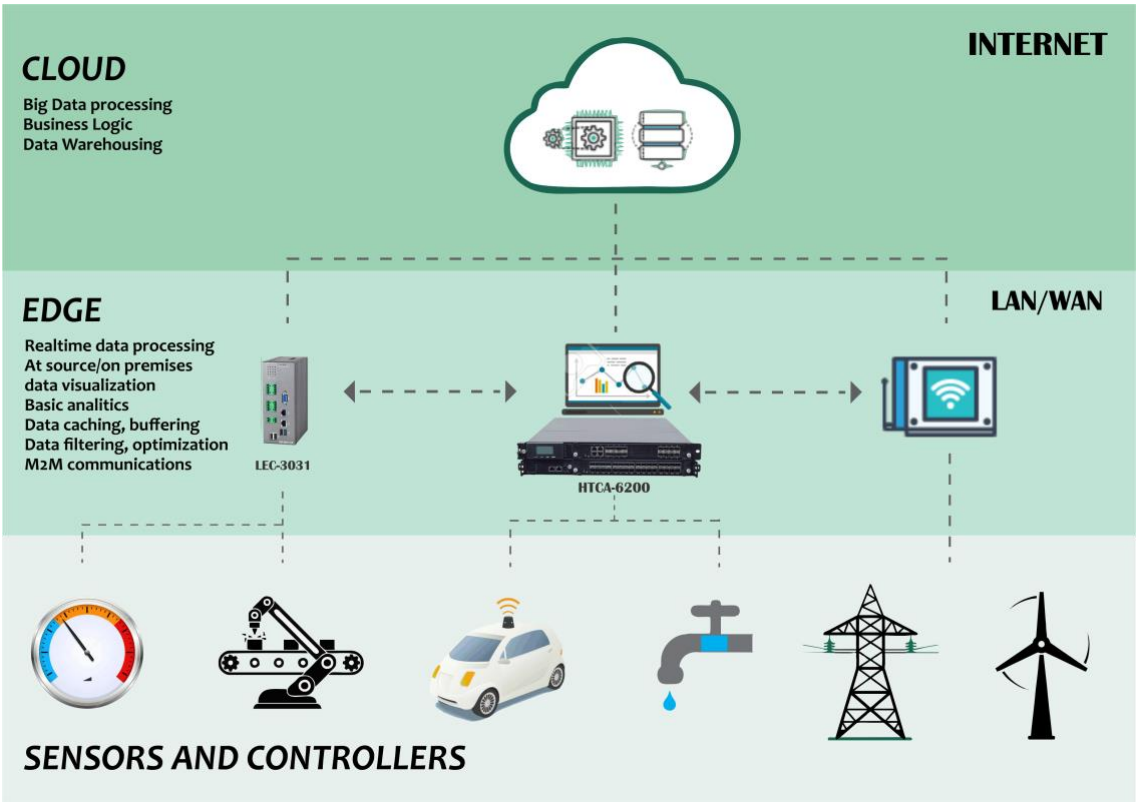


Figure 13: Edge networking works bringing computation and data storage as close to the point of request as possible in order to deliver low latency and save bandwidth. Available from: https://www.omnisci.com/technical-glossary/edge-network

For the three DPL divisions Research & Development (RAD), Manufacturing (MAN), Sales & Marketing (SAM) and Data Center (DC), we have used and configured in packet tracer the following networks:

	RAD	**MAN**	**SAM**	**DC**
Vlan	10	20	30	40
Network	192.168.0.0/22	192.168.4.0/22	192.168.4.0/22	10.0.0.0/22
Mask	255.255.252.0	255.255.252.0	255.255.252.0	255.255.252.0
Gateway	192.168.0.1	192.168.4.1	192.168.8.1	10.0.0.1

Table: Summary VLAN's and networks

Since we have three divisions, and 500 clients are expected for Sales and Marketing, the decision was for a 192.168.*.*/22 network with a number of usable of 1022 hosts. The math was done on an ip-subnet calculator[3].

IP Address:	192.168.0.0
Network Address:	192.168.0.0
Usable Host IP Range:	192.168.0.1 - 192.168.3.254
Broadcast Address:	192.168.3.255
Total Number of Hosts:	1,024
Number of Usable Hosts:	1,022
Subnet Mask:	255.255.252.0

Figure 14

The following subnets have been chosen for the three divisions SAM, MAN and RAD:

All 64 of the Possible /22 Networks for 192.168.*.*

Network Address	Usable Host Range	Broadcast Address:
192.168.0.0	192.168.0.1 - 192.168.3.254	192.168.3.255
192.168.4.0	192.168.4.1 - 192.168.7.254	192.168.7.255
192.168.8.0	192.168.8.1 - 192.168.11.254	192.168.11.255

Figure 15: Networks available

Following below, an example of the VLAN configuration using CLI. The running configuration can then be saved as startup configuration and exported into a txt file, where version control see github can be applied. The configuration has to be done in 'enable mode', and then starting with 'configuration terminal':

[3] Available from: https://www.calculator.net/ip-subnet-calculator.html?cclass=b&csubnet=22&cip=192.168.2.1&ctype=ipv4&printit=0&x=59&y=26

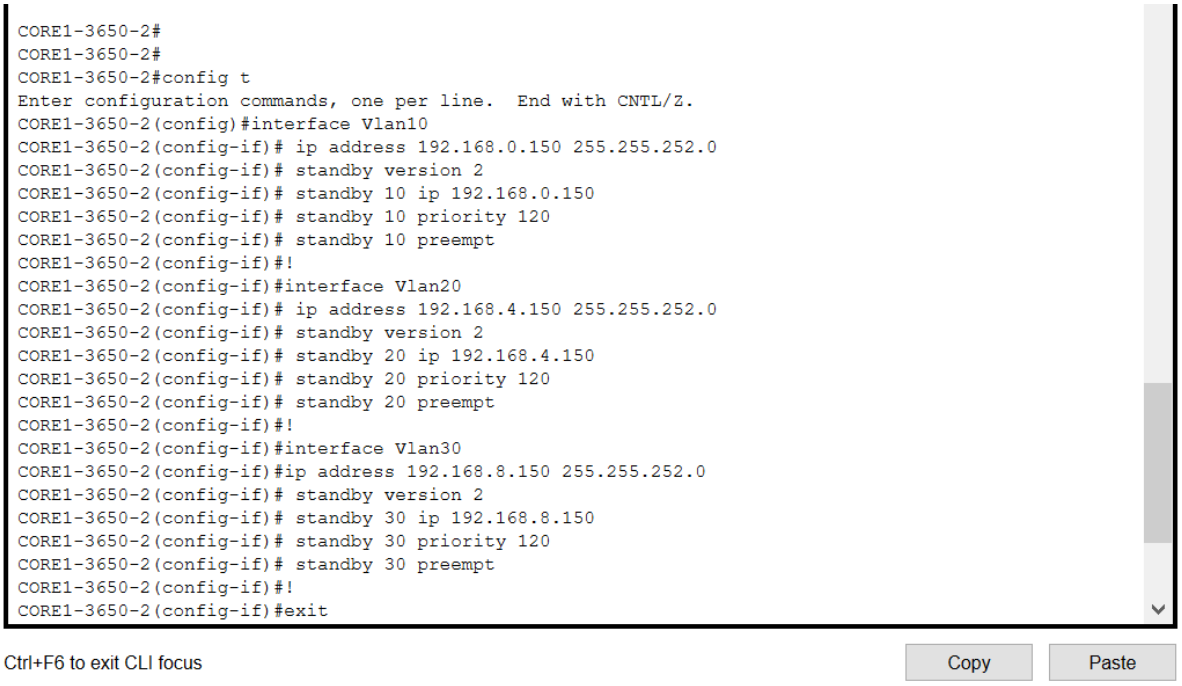


Figure 16: Packet Tracer's CLI.

4.9 Access Control

This section was implemented and configured using Access Lists. Access Lists define control on each port, service (www) and IP group-based. It also defines control on subnet level (allow RAD, deny SAM, deny MAN). These are the commands used on Cisco:

- access-list 10 deny tcp 192.168.1.0 0.0.0.252 host 10.0.0.21 eq www
- access-list 10 deny tcp 192.168.1.0 0.0.0.252 host 10.0.0.21 eq 443
- access-list 10 deny tcp 192.168.4.0 0.0.0.252 host 10.0.0.21 eq 443
- access-list 10 deny tcp 192.168.4.0 0.0.0.252 host 10.0.0.21 eq www
- access-list 10 permit ip any any

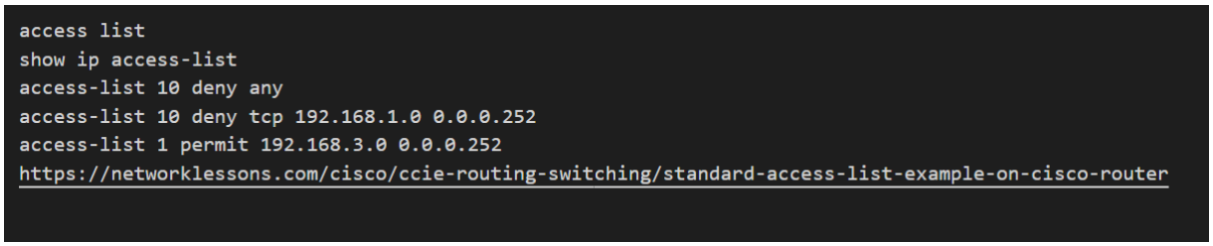


Figure 17

4.10 Name resolution services

Name resolution (DNS) service is highly required because of the translation of an IP into hostnames for IT administration. It also provides independence of IP changes on application levels, i.e. ssl certificates, aliases, webserver hostnames.

> The Domain Name System (DNS) protocol is an important part of the web's infrastructure, serving as the Internet's phone book: every time you visit a website, your computer performs a DNS lookup. Complex pages often require multiple DNS lookups before they start loading, so your computer may be performing hundreds of lookups a day (Google Developers, n.d.).

Therefore, the implementation fulfills the requirements for its high availability when a redundant DNS setup is configured. For the performance and disaster recovery a redundant DNS setup is configured. The load balancer on number two is required for high availability and performance.

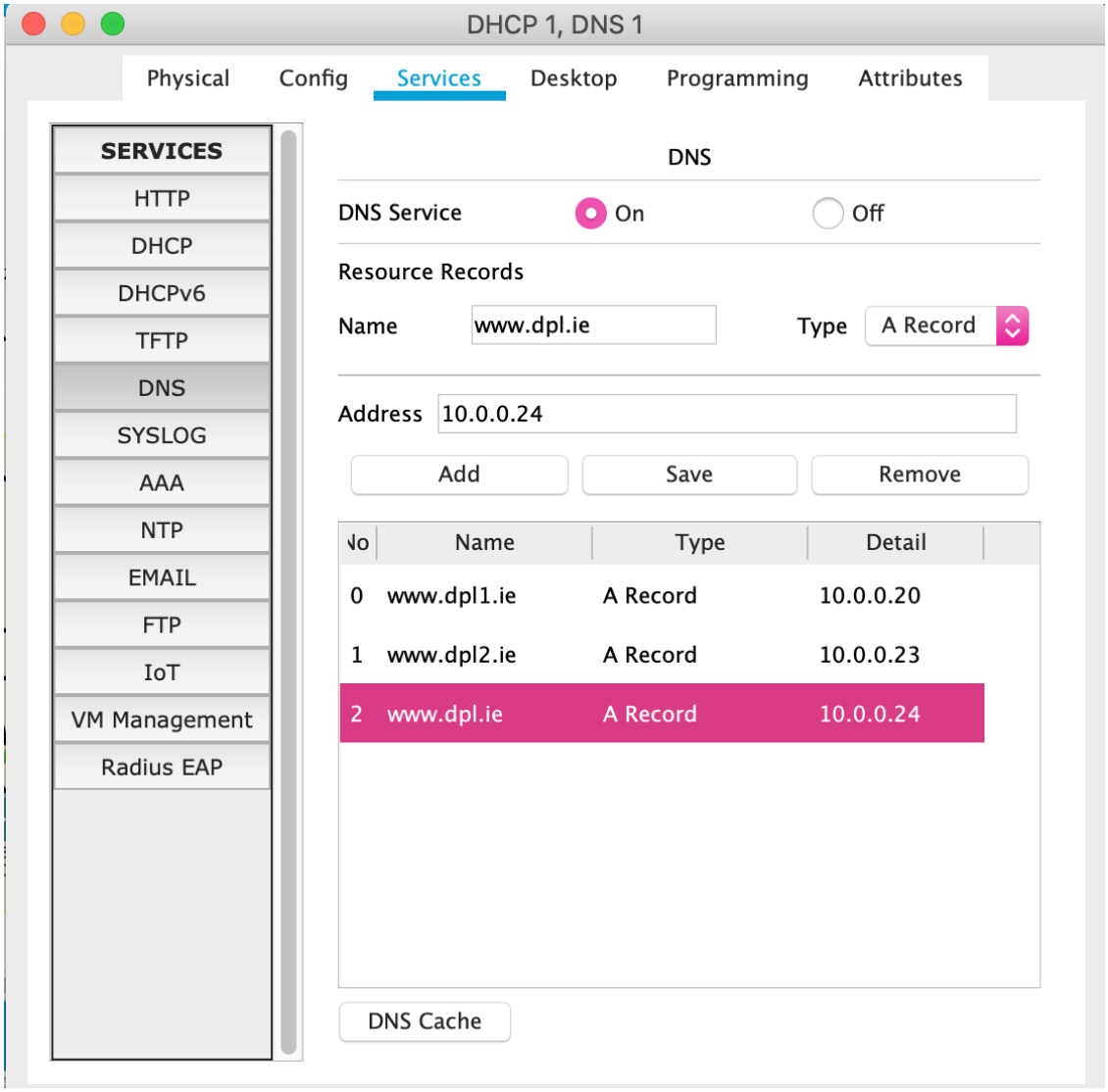


Figure 18: DNS configuration.

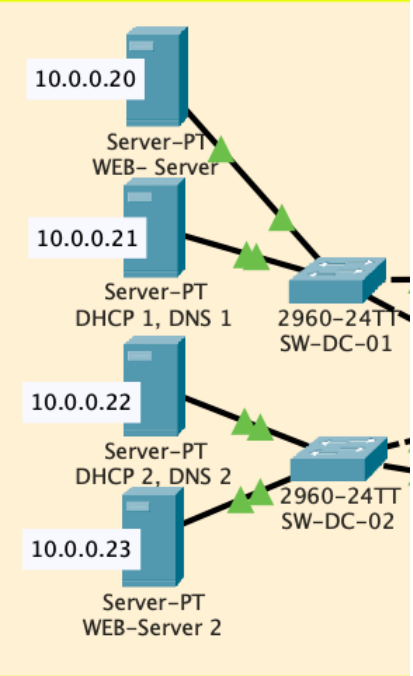


Figure 19: Double servers for redundancy.

4.11 Secure local and remote management of networking devices

All switches and routers need to be accessed with SSH. The SSH configuration starts with the correct SSH version, restrict authentication retries, automated inactivity logout, and no DNS should be done to avoid *dns-spoofing* (Hostinger 2017).

```
SW-RAD-01#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-RAD-01(config)#ip ssh version 2
SW-RAD-01(config)#ip ssh auth
SW-RAD-01(config)#ip ssh authentication-retries 4
SW-RAD-01(config)#ip ssh time-out 60
SW-RAD-01(config)#no ip domain-lookup
*Mar 01, 00:06:02.066: SYS-5-CONFIG_I: Configured from console by console
SW-RAD-01#
```

Figure 20

The user is local and his password is MD5 encrypted:

```
11   SW-RAD-01(config)#enable secret 5 $1$SpMm$eALjeyED.WSZs0naLNv22/
12   SW-RAD-01(config)#username admin secret 5 $1$SpMm$eALjeyED.WSZs0naLNv22/
```

Figure 21

The implementation fulfils the requirements because it is using SSH for remote access, username and hashed passwords for strong authentication and a physical security for access control (badge, pin, visual authentication).

4.12 Device Security best practices

Once again, following Cisco's guide on security[4], device security best practice is required because of:

- Legal obligations
- Protection of unauthorized access to network devices
- Protect against service attacks and breaking device integrity
- Data breach

Device security can be implemented as a central, network wide service using Radius. The implementation fulfils the requirements and is justified because Radius is an integrated standard solution for Cisco devices.

[4] Available from: https://www.cisco.com/c/en/us/products/security/product-listing.html

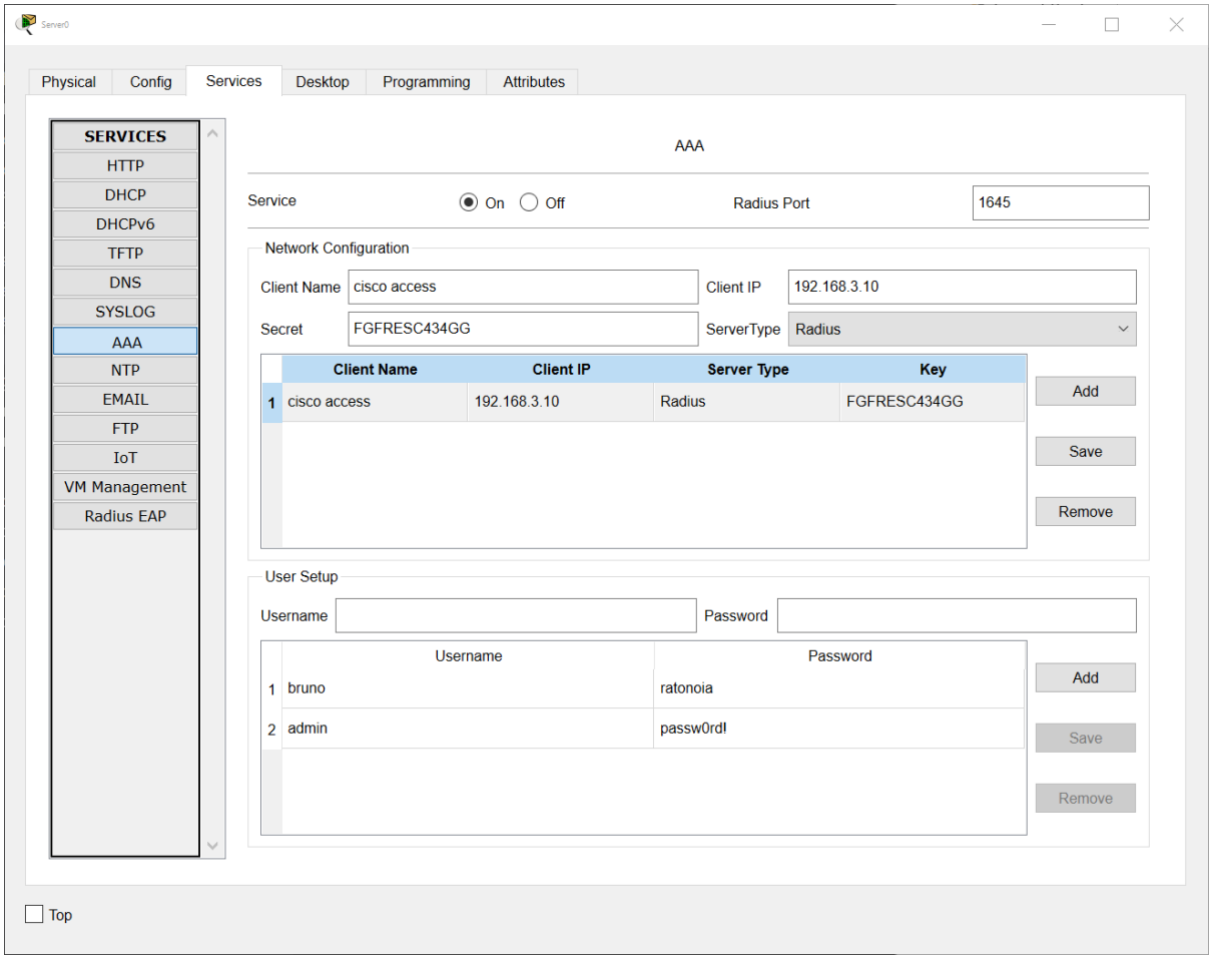


Figure 22: Device Security

Device security is enforced using a separated, protected management network and to avoid clear-text methods like telnet. Using ssh is mandatory, and if the device allows, using key based logins are preferred to username/password since, since password adequate strenghts is difficult to enforce. Further security measures are configured for the cisco router access:

```
3   enable secret 5 $1$SpMm$eALjeyED.WSZs0naLNv22/
4   no ip cef
5   ip routing
6   no ipv6 cef
7   username admin privilege 15 secret 5 $1$SpMm$eALjeyED.WSZs0naLNv22/
8   ip ssh version 2
9   ip ssh authentication-retries 2
10  ip ssh time-out 60
```

Figure 23

- Hashed encrypted passwords
- Only latest SSH version allowed
- Restricted retries
- Automated logout after a short time
- All logs of login and modifications should be logged and forwarded to a central security logging system

Figure 24

Figure 25

Even better access control is possible with Radius. Proof of concept implementation will be referred in the next chapter.

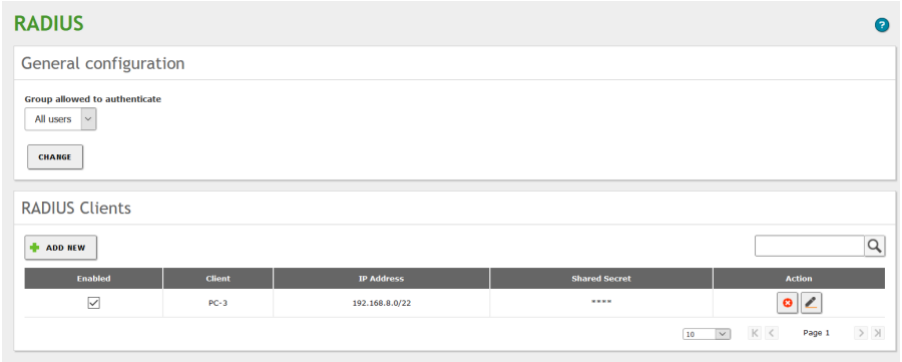


Figure 26

5 NETWORK SERVICES

This chapter is a proof-of-concept for DPL case that intends to show different network services. The administrative base is a virtual machine setup in Virtualbox, based on standard, well established opensource components like Ubuntu Linux, Netfilter, Samba, OpenVPN, Quagga, Nginx. Zentyal, which is based on Ubuntu was the solution used to summarize all configuration tasks into a single integrated dashboard. Zentyal server acts also as a router. Following its documentation and tutorial to configure routing[5] the different VLAN's from the networking chapter are connected with virtual ethernet adapters as follows:

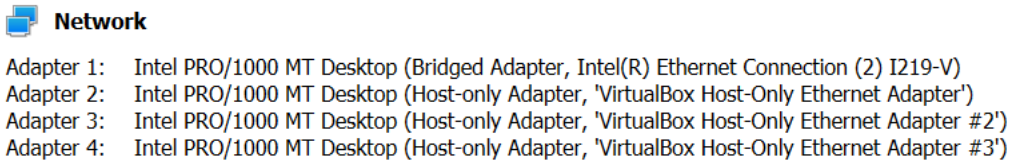


Figure 27: virtual machine network adapters.

5.1 Inbound and Outbound security

Network security controlling in- and outbound traffic is enforced and defined by using a firewall solution. DPL requires an opensource solution that shows the allowed connections graphically for a better overview. The firewall implementation works with the following parameters:

- Zentyal acts as a firewall server;
- An internal website delivers a website to the outside partner YAC (Yet Another Company) and to DPL's Research and Development division only;
- A detailed list of inbound and outbound security is provided (Mail, Web, ssh, DNS, ICMP, file transfer);
- All failed connections are logged;

[5] Configuring routing with Zentyal. Available from: https://doc.zentyal.org/5.1/en/routing.html

For inbound connection we allow the following firewall connections. Reasons are given in the description field. The order is important:

Decision	Source	Service	Description
↑	Any	dpl webserver 8080	DPL Webserver allowed
↑	Any	openVPN	VPN allowed for Data Collaboration
↑	Any	Zentyal Webadmin	remote admin allowed
⛔	Any	RADIUS	no Radius allowed
⛔	Any	Any ICMP	no Ping allowed
⛔	Any	Any TCP	no TCP allowed

Figure 28: inbound connections.

As for outbound connections we allow the following firewall connections. The reasons you can find in the description field:

Decision	Destination	Service	Description
↑	Any	openVPN	open VPN is allowed
↑	Any	Proxy	web proxy is allowed
↑	Any	SSH	ssh outbound is allowed
↑	Any	HTTPS	https outbound is allowed
⛔	Any	Any	deny everything else

Figure 29: outbound connections.

5.2 Automatic IPv4 address allocation

Automatic IPv4 address allocation is usually serviced with the industrial standard protocol DHCP (Kerravala, 2018). For the proof-of-concept implementation, we rely on Zentyal, which is available as an open-source community edition. The network design we need to fulfill the requirements is the following:

- Zentyal acts as DHCP server

- A Linux client on an internal network consumes DHCP and DNS dpl.ie from central service
- The DNS search domain should be dpl.ie
- The user PC's must be on an internal network; separated from the internet

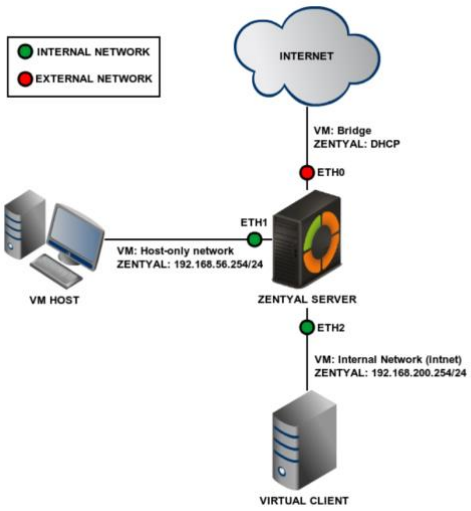


Figure 30: Figure: schematic connections of virtual networks.

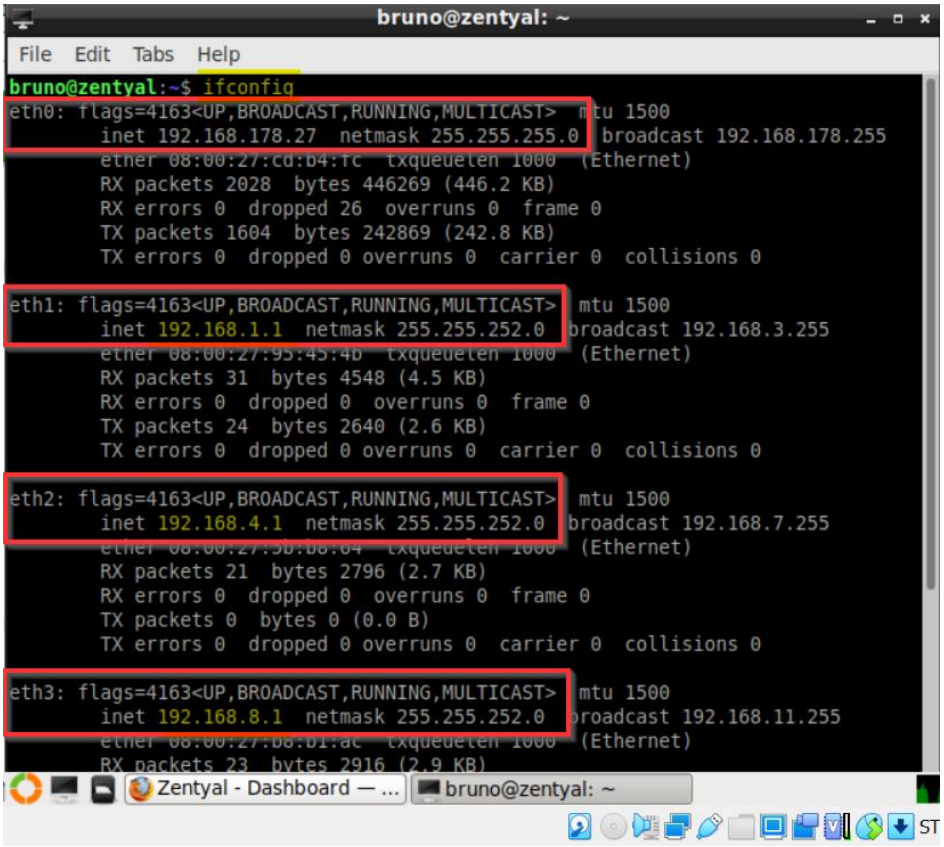


Figure 31: Zentyal server network configuration

For each interface we can apply a different DHCP range for each DPL division:

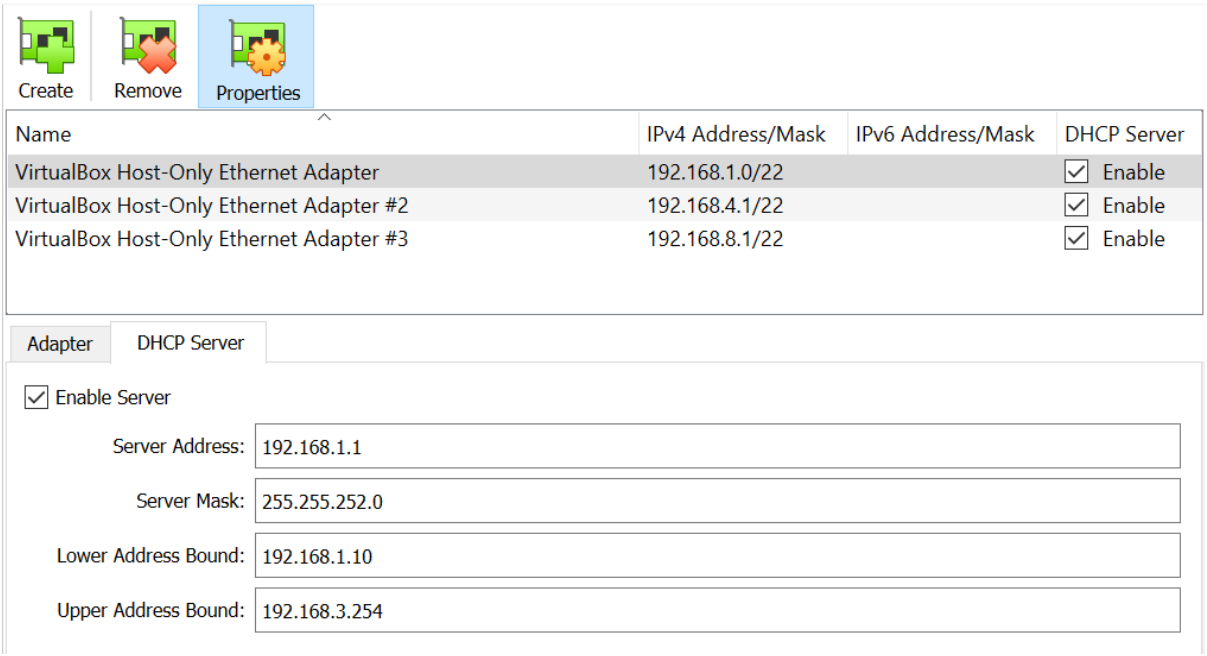


Figure 32

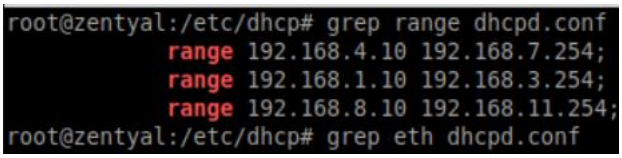


Figure 33

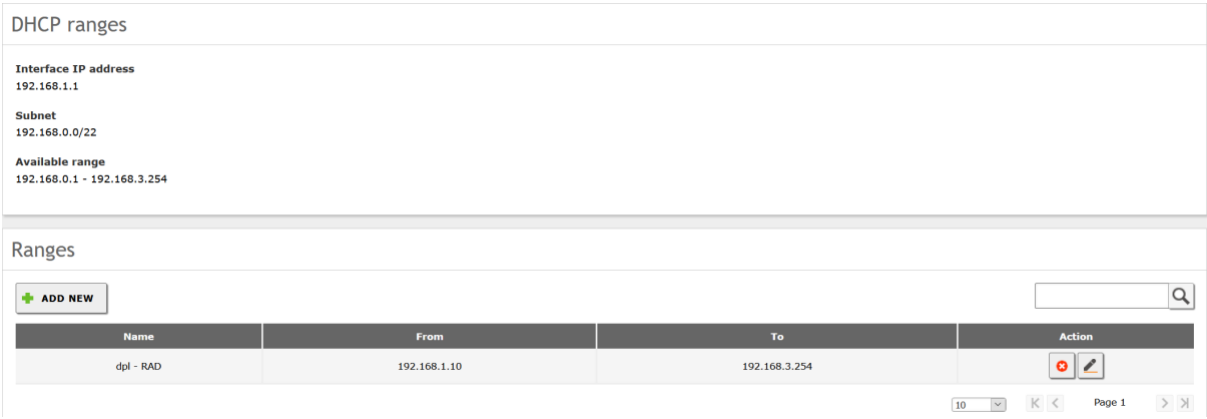


Figure 34

The PC and Linux desktop clients can then be setup with DHCP based on DPL's needs. The DNS also works, Internet access works and routing is configured:

```
adminuser@ubuntu:~$ ip route
default via 192.168.8.1 dev enp0s17 proto dhcp metric 100
169.254.0.0/16 dev enp0s17 scope link metric 1000
192.168.8.0/22 dev enp0s17 proto kernel scope link src 192.168.8.10 me
adminuser@ubuntu:~$
```

```
adminuser@ubuntu:~$ nslookup dpl.ie
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   dpl.ie
Address: 192.168.178.27
Name:   dpl.ie
Address: 192.168.1.1
```

Figure 26:

Clients get their IP from the preconfigured DHCP ranges according to their virtual network adapter in VirtualBox:

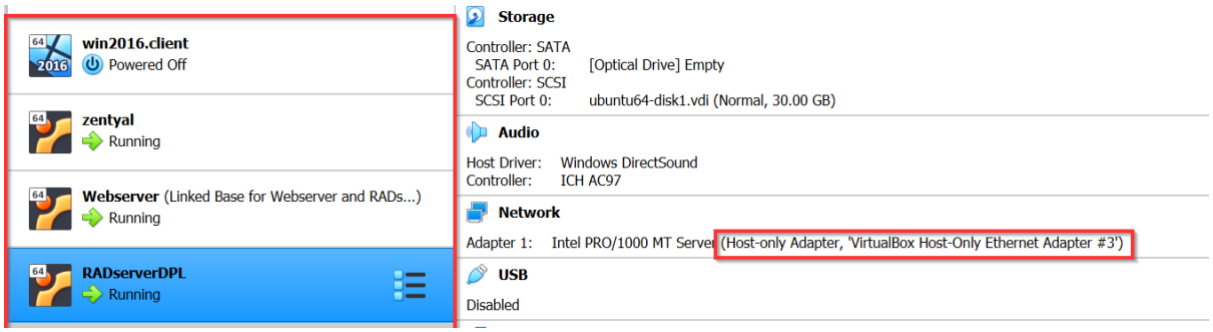


Figure 27: RAD department network configuration.

5.3 Web Server services

The webserver has to be accessible to the internal network of DPL and to the partner company YAC. There is a default gateway and a proxy configured for outgoing traffic:

Gateways List

ADD NEW

Enabled	Name	IP address	Interface	Weight	Default
☑	dhcp-gw-eth0	192.168.178.1	eth0	1	✔

Figure 35: Gateway lists

A static route enables the RAD division to access the webserver on the host-only network:

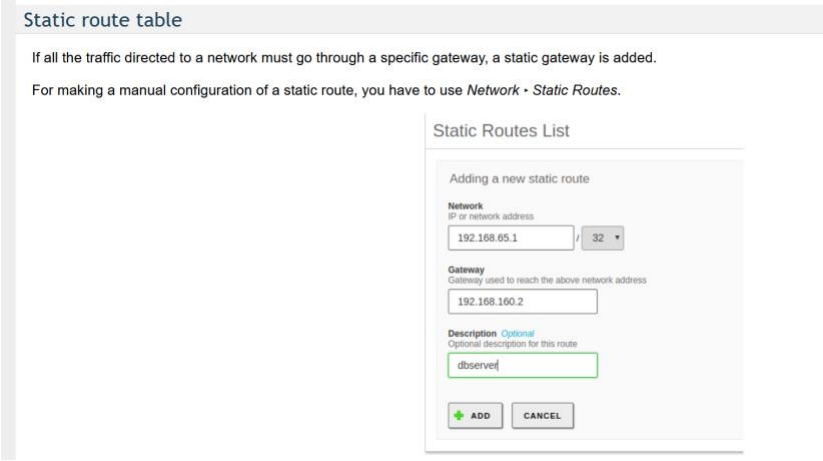


Figure 36: Static route table.

5.4 Custom intranet portal design

A custom intranet portal using Ubuntu 20 and Apache 2.42 was generated. The web server configuration is implemented as virtual apache host listening on its own port 8080 and having its own document root. These settings are standard entries for sites-available and ports.conf as shown below:

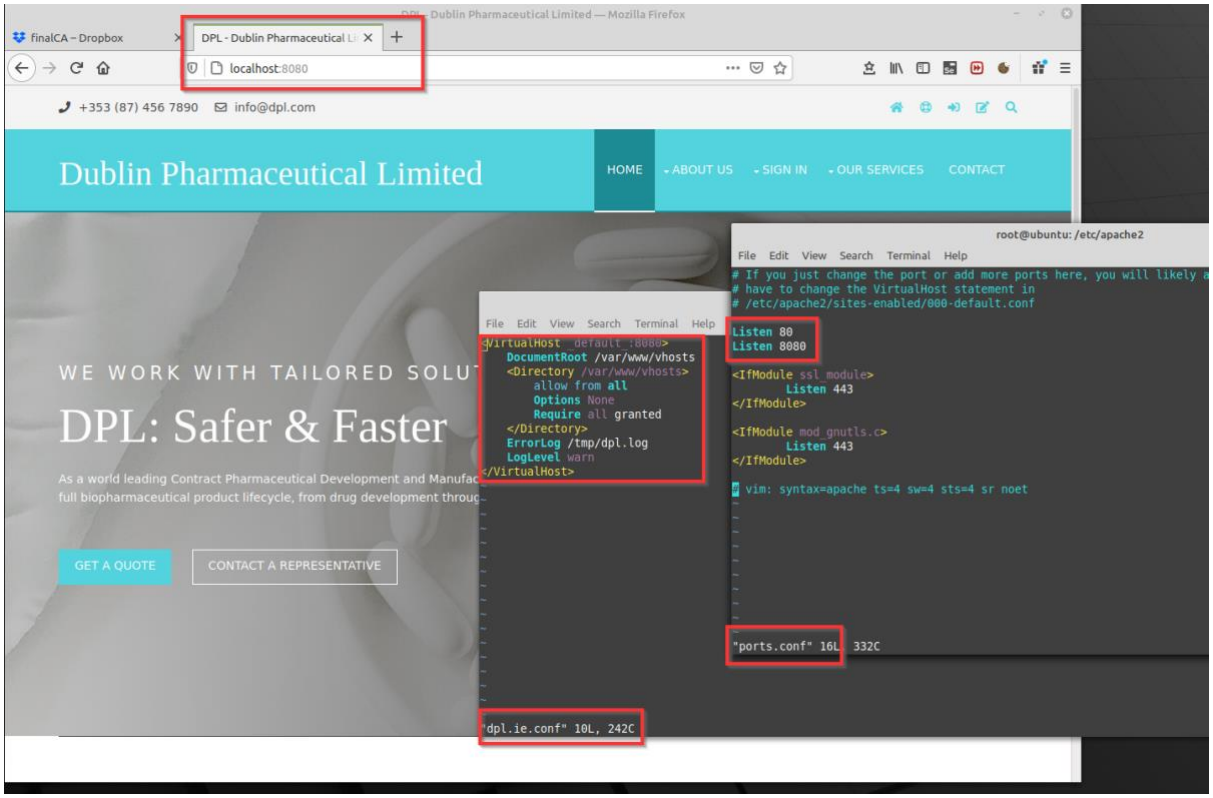


Figure 37: Intranet portal

HostIP and port 8080 is only available for the partner site and for research and development, as every other access is blocked on the firewall.

5.5 Remote Access services

There is VPN to be used for remote access services. The VPN Server configuration looks like this:

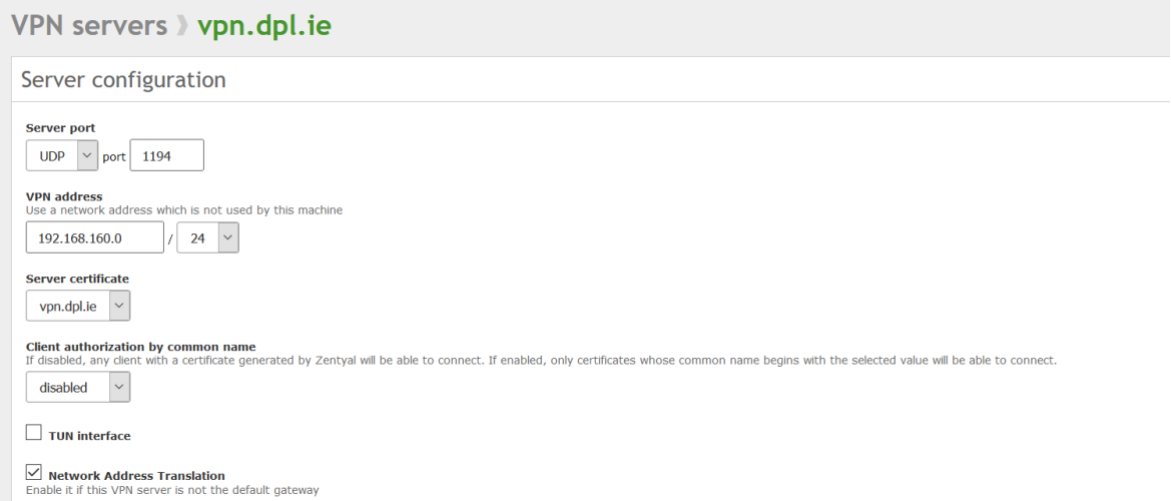


Figure 38

5.6 Secure File Transfer capabilities

First of all, there is SFTP or FTPS available to the same as FTP with increased security (Chan 2019). Each technique has specific pros and cons and it depends on what has to be established. But Chan (2019) estates that FTPS is a good choice when you have a server that supports FTP (but not SSH/SFTP) and need more security. It may also be helpful when transferring files from mobile devices such as phones and tablets to an FTP server. But if the server has the capability to use SFTP, that is the best option. As Zentyal server is able to provide FTP forced over SSL, that is the one we are using.

> Data breaches are becoming more common, and even the largest companies are getting hacked. Breaches can cost your company millions of dollars, so it makes sense to use the highest level of security when transferring files. And SFTP provides that. (Chan 2019).

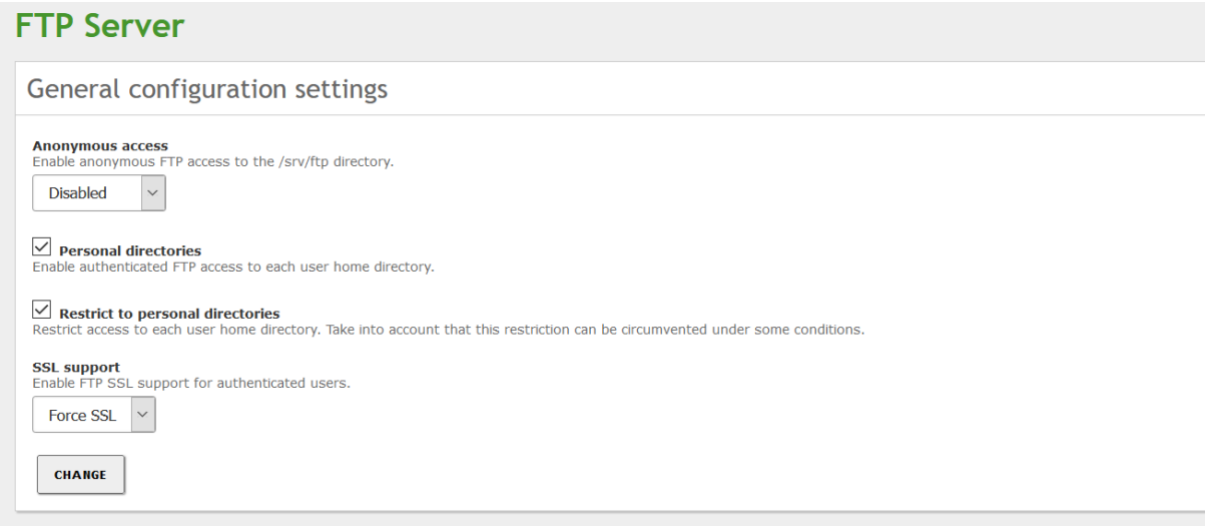


Figure 39: SFTP example in Zentyal/

For Windows Clients we have a secure file share available provided by Zentyal. Authentication is established and secured by Kerberos, a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. You can use LDAP over SSL/TLS to secure communication between the Virtual Machine LDAP client and the LDAP server. The valid Kerberos ticket can be viewed with klist command.

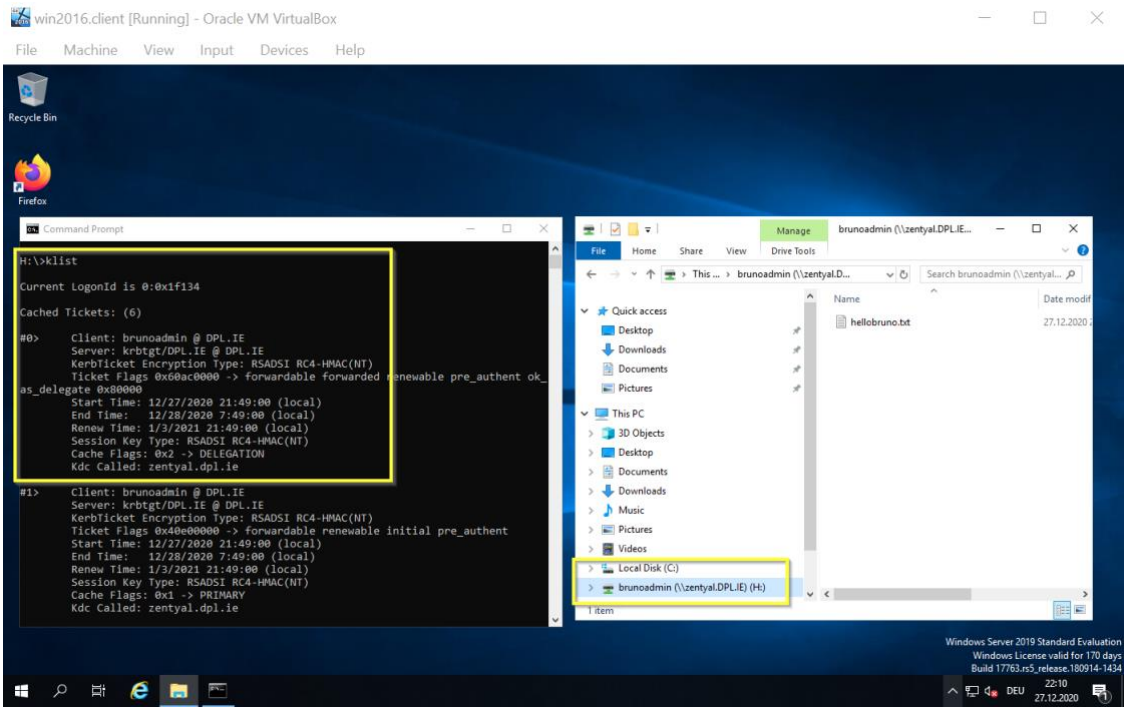


Figure: Kerberos secured File share and transfer access

5.7 Account management home directories

The same requirements are safe to assume again, like using Zentyal community edition. As mentioned, Zentyal is Ubuntu Linux based, highly optimized, tuned and opensource. The installation can be achieved using virtualization.

5.7.1 Windows 2019 Data Center joining Zentyal Primary Domain Controller

We have a goal of having a Windows 2019 Domain Controller to join the Primary Domain Controller running on Zentyal. For so, the DNS domain needs to be configured:

Figure 40

Second, the LDAP tree has to be filled. On the left side, you can see the tree, with our "local" domain as the root. There are several *Organizational Units* already created:

• **Computers**: Hosts joined to the domain, both servers and desktops, this section is useful for inventory reasons and also to apply host-based rules.
• **Groups**: Generic OU container node for the groups in your organization.
• **Users**: Generic OU container node for the users in your organization.
• **Domain Controllers**: Servers that replicate this directory information, they can also take on the different FSMO roles of a Samba4/Active Directory domain.

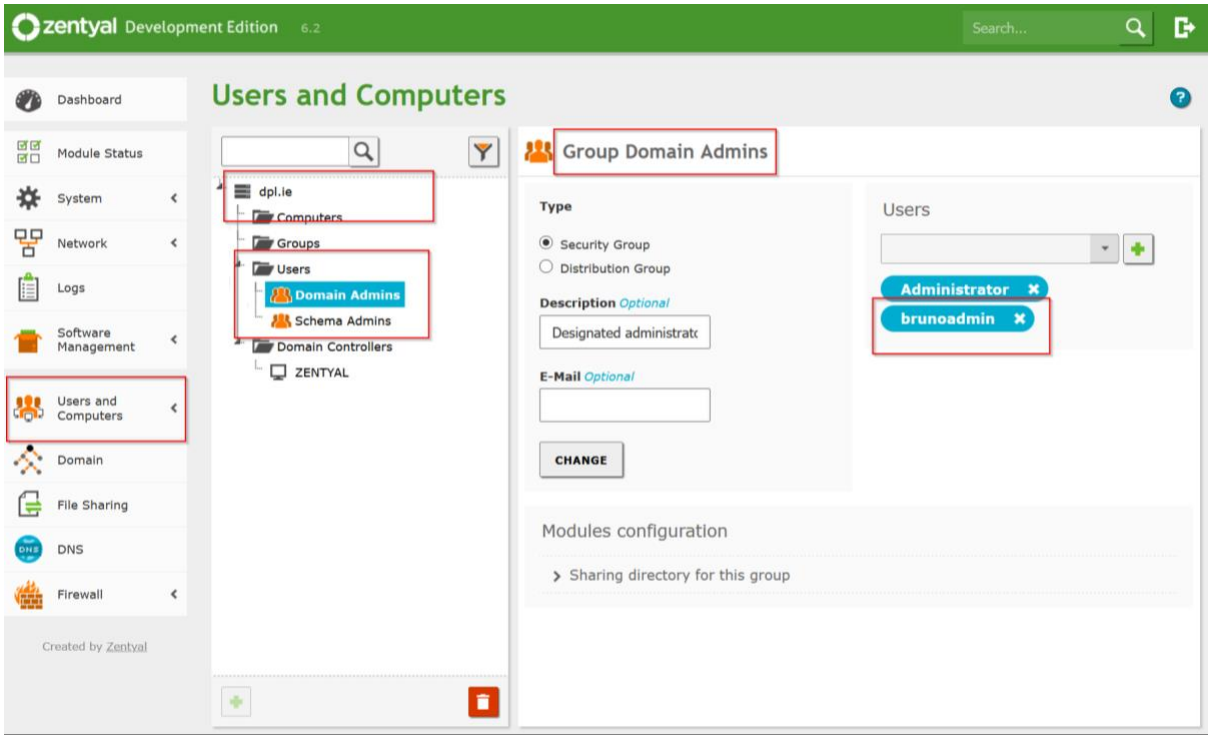


Figure 41

Windows joining the Domain on Primary Domain Controller:

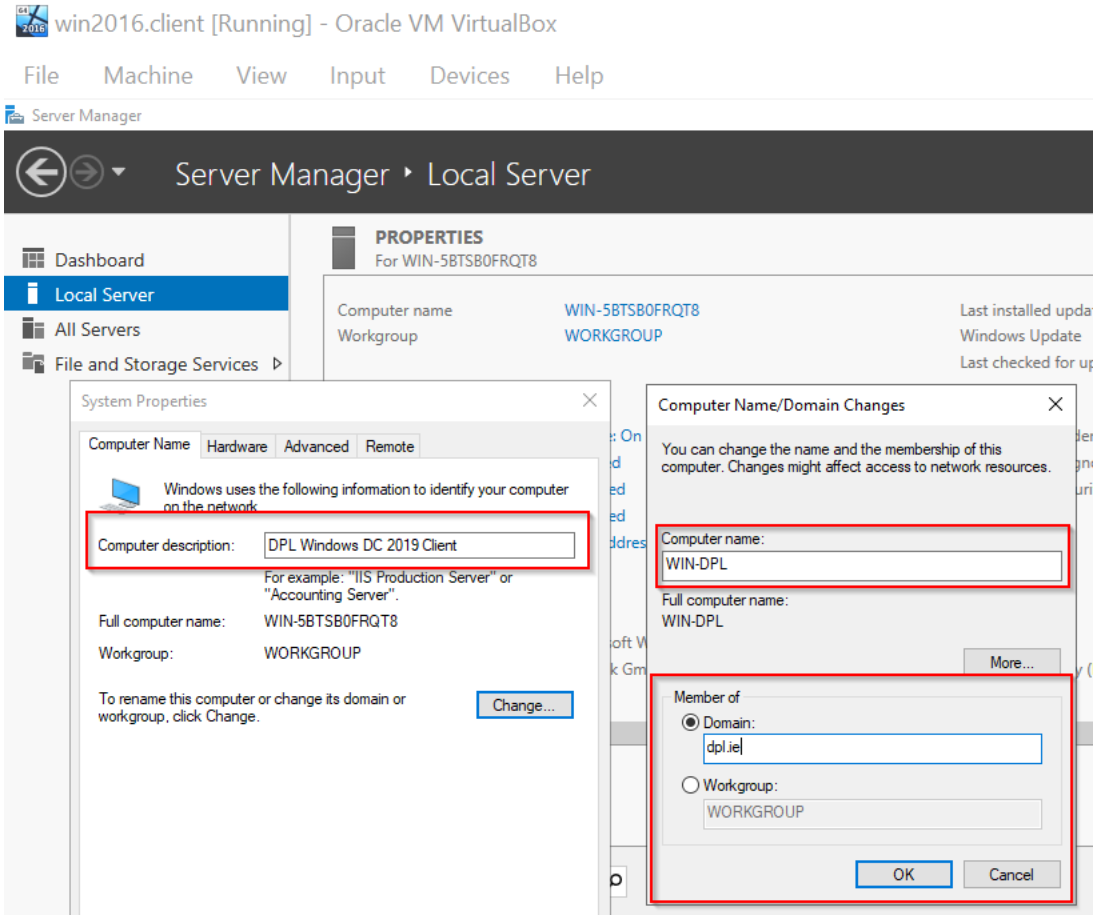


Figure 42

Log in as brunoadmin. Password: 1234

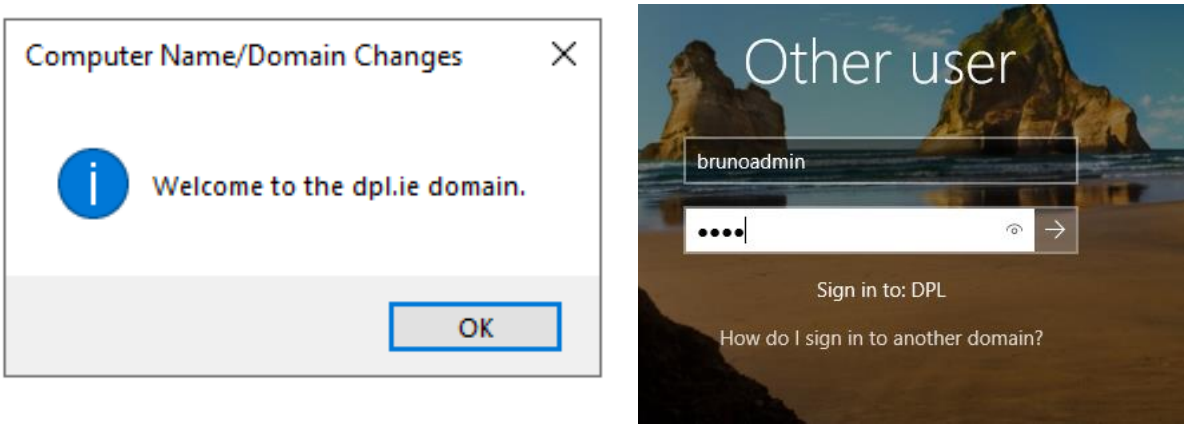
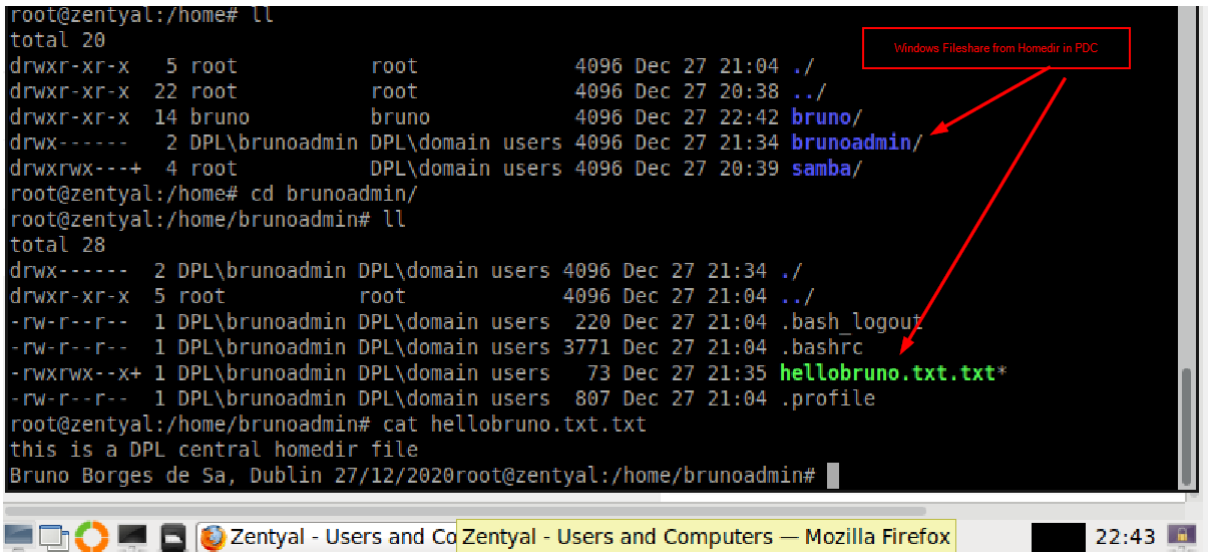


Figure 43: Login as administrator.

5.7.2 Home Directory file sharing between Client and Server

Here is a proof-of-concept of file sharing between Zentyal and Windows Client working. The domain users from DPL can connect and have access to files and vice versa.



DATA COLLABORATION

5.8 Cloud Network & Virtualization Infrastructure

5.8.1 Requirements

Most legacy business-to-business collaboration projects are network based on VPN (virtual private network). Typically, companies use a VPN to give remote employees access to internal applications and data, or to create a single shared network between multiple office locations. In both cases, the ultimate goal is to prevent web traffic - particularly traffic containing proprietary data - from being exposed on the open Internet (Cloudflare n.d.).

While this is established technology, there are high costs associated due to administration, availability and infrastructure. Connecting into a cloud provides big advantages such as:

- Global access
- Transparent billing and no upfront costs
- Flexibility and agility
- Security

In order to exchange data, there are solutions on different layers available:

• Function layer: direct API exchange
• Application layer: data exchange APUI based, but with complete Application
• OS / File layer: data exchange with file sharing (copy, sharing, transfer)
• Network layer: classical VPN connection

We could setup a hybrid connectivity between DPL, YAC and Gcloud by activating a VPN connection. A virtual private network lets us securely connect our Google Compute Engine resources to our own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity.

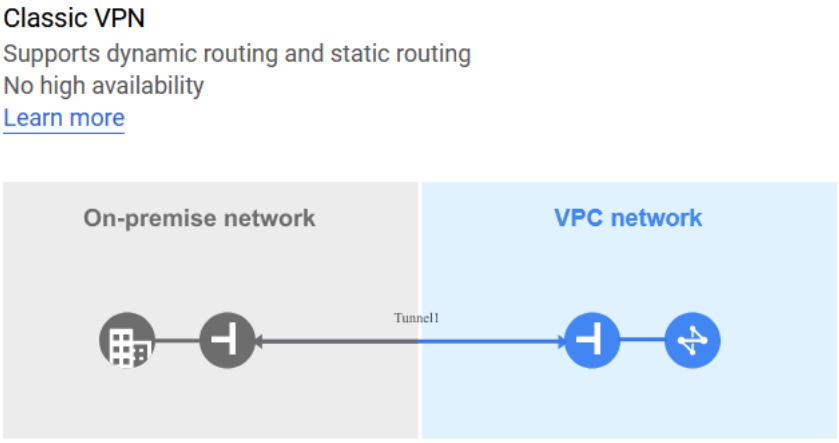


Figure 43

Since the complete code as a Proof-of-concept was provided for the data collaboration project between DPL and YAC, we can gain a lot from application layer data exchange, since we are much closer to business logic and transactions. We do not need to care for physical network, OS, user access, data files and so on.

The goal for data collaboration to be deployed into the cloud is:

- complexity due to Network Security and Data Center infrastructure
- Speed up implementation time providing common access to the shared environment
- Retain global access
- Share common datasets in centralized database and avoid synchronization

5.8.2 Design Virtual Private Cloud

The network layout as designed in chapter networking and implemented in chapter virtualization can be defined using cloud technologies. Strating now from Google Cloud (n.d.) documentation, the designed collab networks for data collaboration including DPL and YAC according to the specifications.

The node servers (backend) are running in the Google Cloud, as well as the front servers. I setup the DB on MongoDB cloud, since the pre-imaged MongoDB in Google involved some cost related implications.

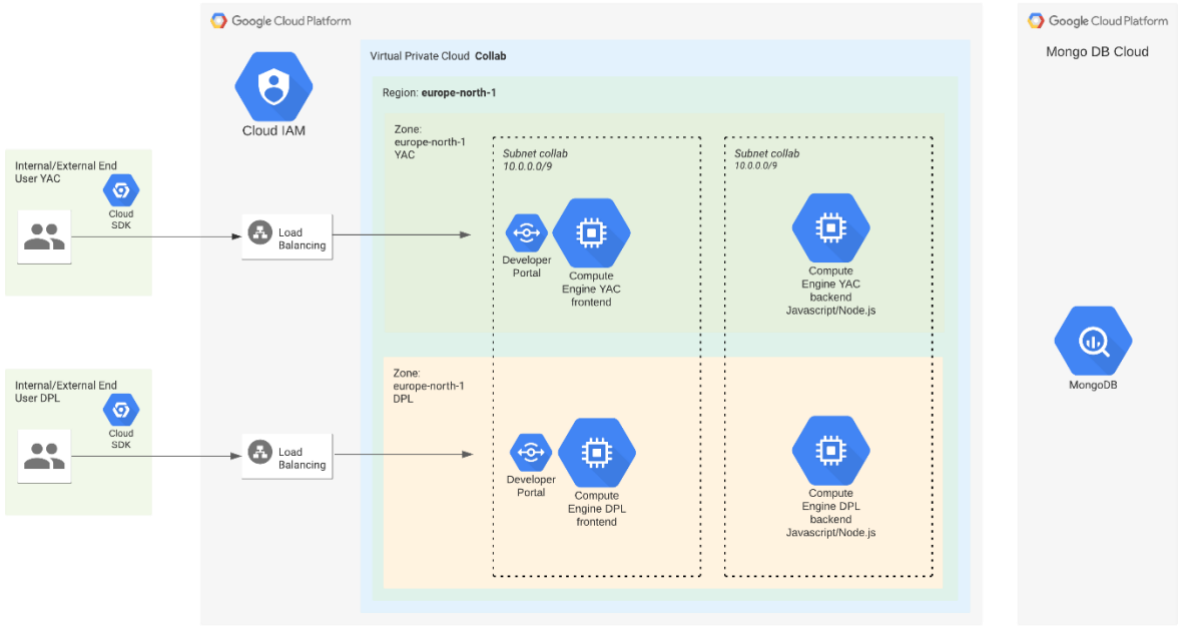


Figure 44: Network Design in Google Cloud

5.8.3 Implementation

Following below on how the Virtual Private Cloud, which can be considered as a legacy data center for a company, were set up and then added networking, firewall and servers (compute engines, Debian based).

Firewall CREATE FIREWALL REFRESH CONFIGURE LOGS DELETE

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed in the App Engine Firewall rules section.

collab Filter table

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network
collab-egress-mongodb	Egress	Apply to all	IP ranges: 0.0.0.0/0	tcp:27017	Allow	1000	collab
collab-8080	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:8080	Allow	1000	collab
collab-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	collab
collab-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	collab
collab-allow-ping	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1000	collab
collab-mongodb-servers-icmp	Ingress	collab-mongodb-servers-tier	Tags: collab-mongodb-deployment	icmp	Allow	1000	collab
collab-mongodb-servers-tcp-27017	Ingress	collab-mongodb-servers-tier	Tags: collab-mongodb-deployment	tcp:27017	Allow	1000	collab
collab-mongodb-servers-tcp-27018	Ingress	collab-mongodb-servers-tier	Tags: collab-mongodb-deployment	tcp:27018	Allow	1000	collab
collab-mongodb-servers-tcp-27019	Ingress	collab-mongodb-servers-tier	Tags: collab-mongodb-deployment	tcp:27019	Allow	1000	collab
ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,3000	Allow	1000	collab
allow-collaborator	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:8080	Allow	1000	default

Some considerations:

- Server 1: dpl nodejs server backend with mongodb access
- Server 2: yac nodejs server backend with mongodb assess
- Server 3: dpl nodejs server frontend with access to backend
- Server 4: yac nodejs server frontend with access to backend
- Server 5: MongoDB for database

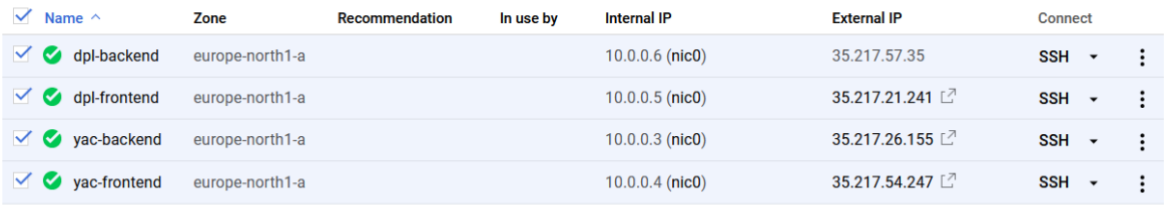


Figure 45: Servers

Integration and automation are key enablers for getting a seamless and quick entry into an enterprise. Selling much more licenses is good business and keeps competition away. Google helps here and enforces this with its command line-based framework as part of the SDK. Therefore, SDK was installed for the cloud shell according to the documentation[6].

[6] [6]Cloud SDK Documentation. Quickstart: Getting started with Cloud SDK. Available from: https://cloud.google.com/sdk/docs/quickstart?hl=en-GB

```
Brunos-MBP:~ brunoborges$ ./google-cloud-sdk/bin/gcloud init
Welcome! This command will take you through the configuration of gcloud.

Your current configuration has been set to: [default]

You can skip diagnostics next time by using the following flag:
  gcloud init --skip-diagnostics

Network diagnostic detects and fixes local network connection issues.
Checking network connection...done.
Reachability Check passed.
Network diagnostic passed (1/1 checks passed).

You must log in to continue. Would you like to log in (Y/n)?  Y

Your browser has been opened to visit:

    https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=325
55940559.apps.googleusercontent.com&redirect_uri=http%3A%2F%2Flocalhost%3A8085
%2F&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+http
s%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googlea
pis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcom
pute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=eloeNNh2K
uWnqbjNUt2DN6i5Ruxe5f&access_type=offline&code_challenge=T5cpzboJkVuJx4q8q4tcJ
84sl6pzsU6NOUmmAxqwxok&code_challenge_method=S256

You are logged in as: [borgesdesa@gmail.com].

Pick cloud project to use:
 [1] buoyant-valve-290916
 [2] electric-autumn-290920
 [3] stately-lambda-290919
 [4] Create a new project
Please enter numeric choice or text value (must exactly match list
```

Figure 46: Installing Google Cloud SDK.

Figure 47: Creating template for VM.

```
gcloud compute instances create dpl-server-2 --source-instance-
template=dpl-instance-template -zone=us-central1-a
```

Figure 48: Creating VM with CLI.

For Windows, first remove the default script execution lock first with "Set-ExecutionPolicy unrestricted" logged as administrator.

```
PS C:\Users\admin\Desktop> gcloud compute instances create dpl-server-2 --source-instance-template=dpl-instance-template --zone=us-central1-a

python.exe : Created
[https://www.googleapis.com/compute/v1/projects/electric-autumn-290920/zones/us-central1-a/instances/dpl-server-2].
At C:\Program Files (x86)\Google\Cloud SDK\google-cloud-sdk\bin\gcloud.ps1:117 char:3
+   & "$cloudsdk_python" $run_args_array
+   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (Created [https:.../dpl-server-2].:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

WARNING: Some requests generated warnings:
 - Disk size: '25 GB' is larger than image size: '10 GB'. You might need to resize the root repartition manually if the
operating system does not support automatic resizing. See
https://cloud.google.com/compute/docs/disks/add-persistent-disk#resize_pd for details.
NAME          ZONE           MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
dpl-server-2  us-central1-a  e2-micro                   10.128.0.5   34.67.6.8    RUNNING

PS C:\Users\admin\Desktop>
```

Figure 49

Default region is set during “init” of gcloud SDK, install beta tools for SSH access through command: $ google-cloud-sdk/bin/gcloud components install beta.

By clicking SSH button at VM, the key will be copied from metadata to VM. Every resource needs to be allowed within Identity and Access Management (IAM):

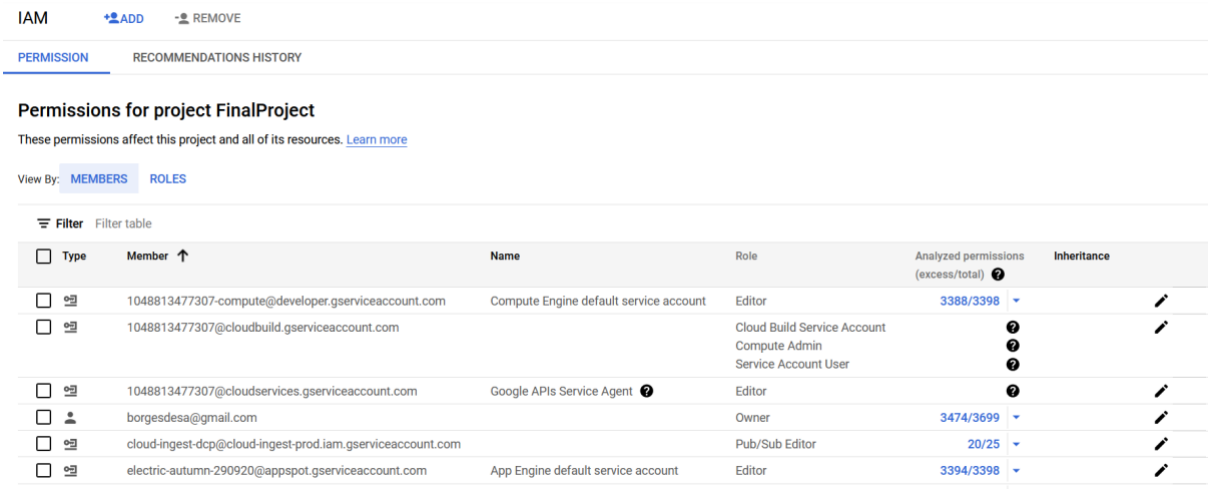


Figure 50: Permissions

Find below the whole picture of the cloud setup between the data base, application backend and frontend servers, including additional access like postman, to show API responses, and compass, to show collections and documents in the data base.

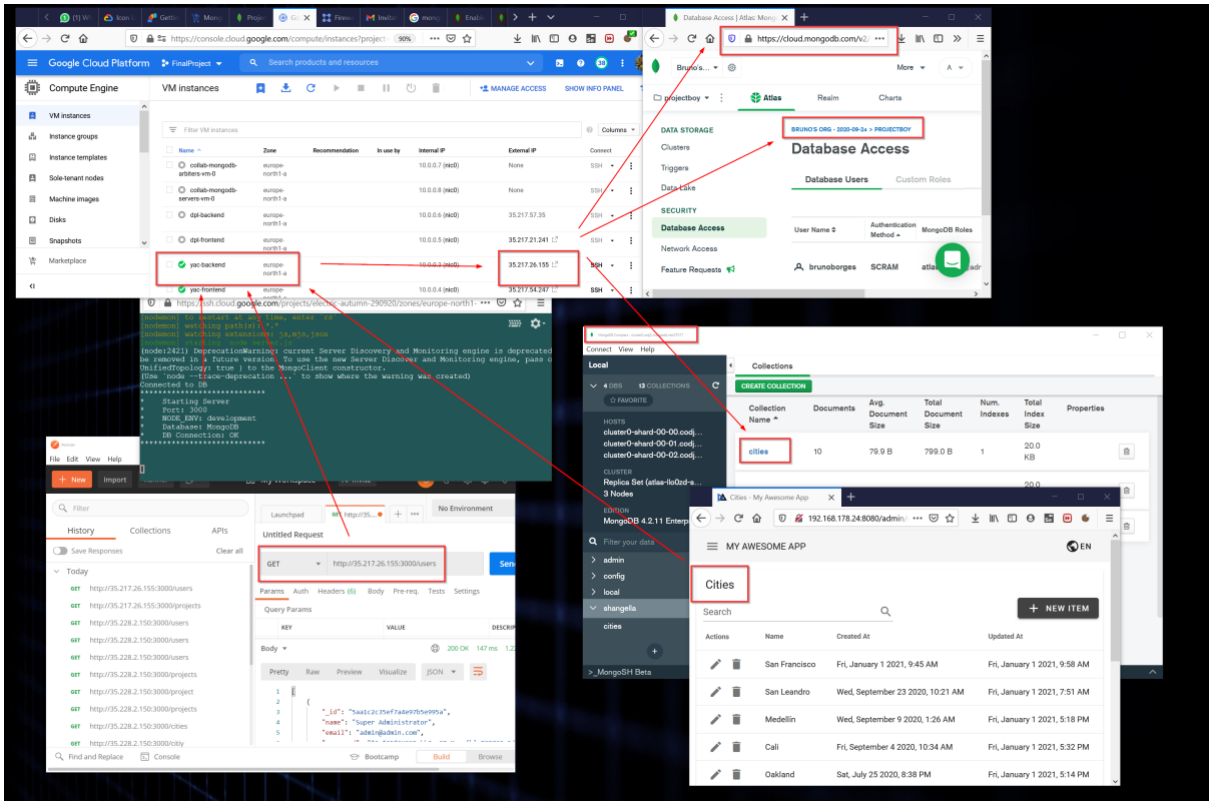


Figure 51: Cloud setup with front-end and backend.

5.9 Data Collaboration Application

5.9.1 Development Environment

Nodejs has been installed to run the application. It was previously developed and adapted for this project on Visual Studio Code. The source is referenced in the Appendix chapter.

In the front-end some links and names were changed to fit DPL while the main layout was maintained. The backend on the other hand had only the address and credentials changed so it can connect to our data base built in MongoDB.

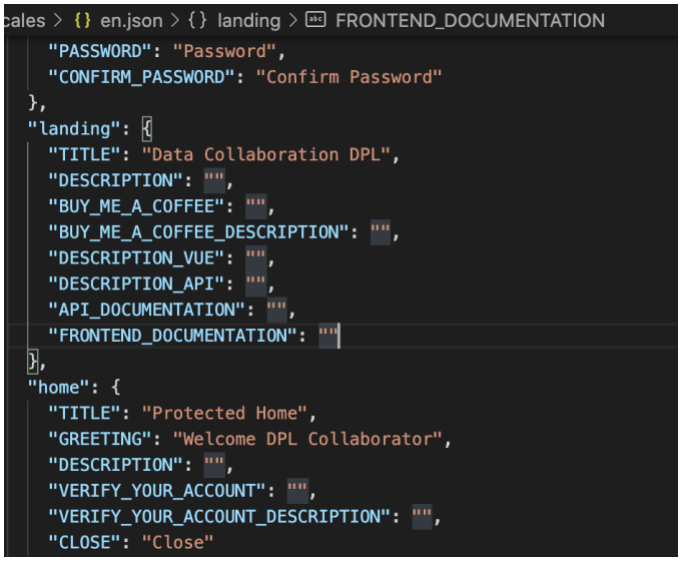


Figure 52: Frontend code.

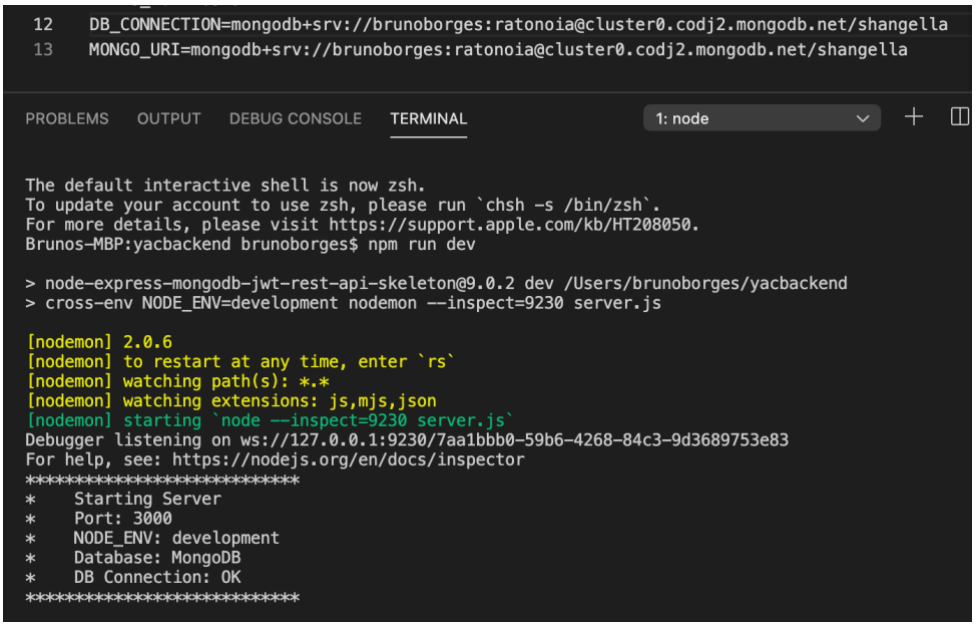


Figure 53: Backend connection to the database.

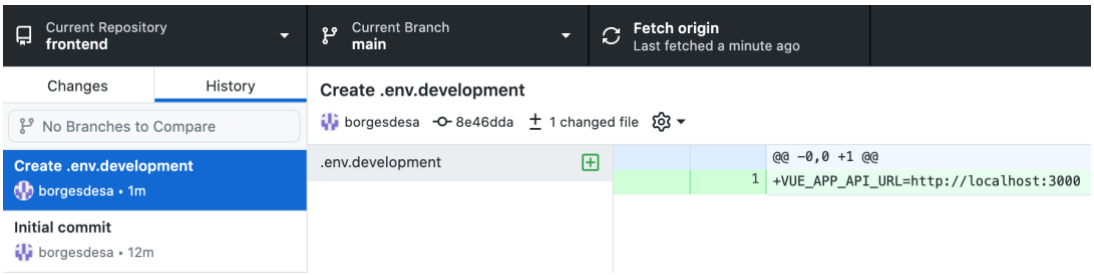


Figure 54: Development push from Github Desktop into repository.

5.9.2 Production Environment

Our proof of concept is based on the final setup with 4 different VM's. The external IP's of the 2 frontend servers are used for the access to the productive servers

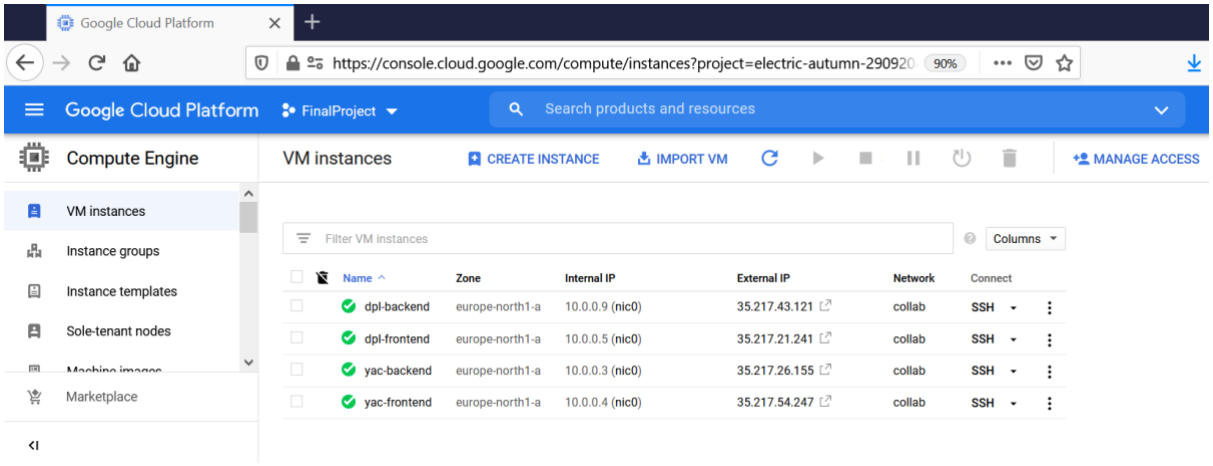


Figure 55: VM instances.

Networking is based on Virtual private cloud network, which consists of classical network functions like routes, gateways, firewalls and subnets.

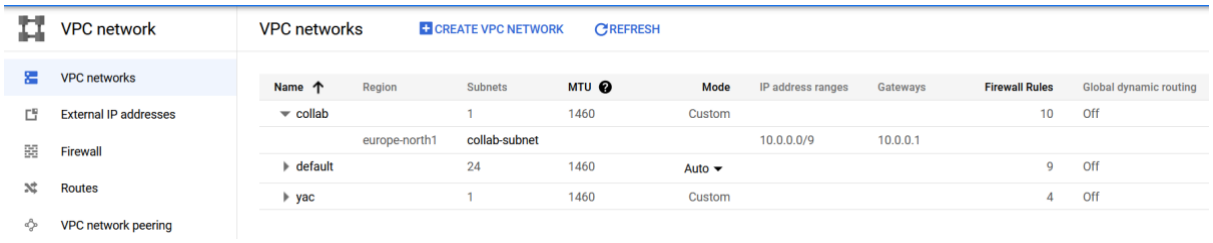


Figure 56: Networking.

The code used in the front and backend are JavaScript based and use Vue framework to generate the template in HTML and CSS files, which makes it more complex to edit and modify, especially in this project that has a tight deadline. For this reason, the layout was minimally changed according to the time available on our planning to make it reasonably appropriate. These are the portals running on the frontend VM's for the data collaboration project:

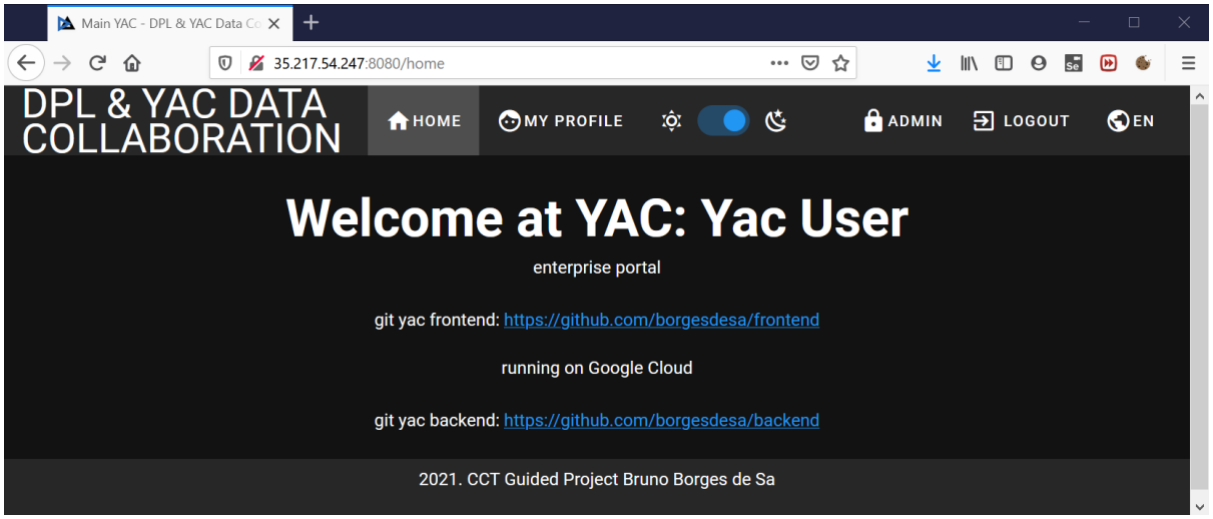


Figure 57

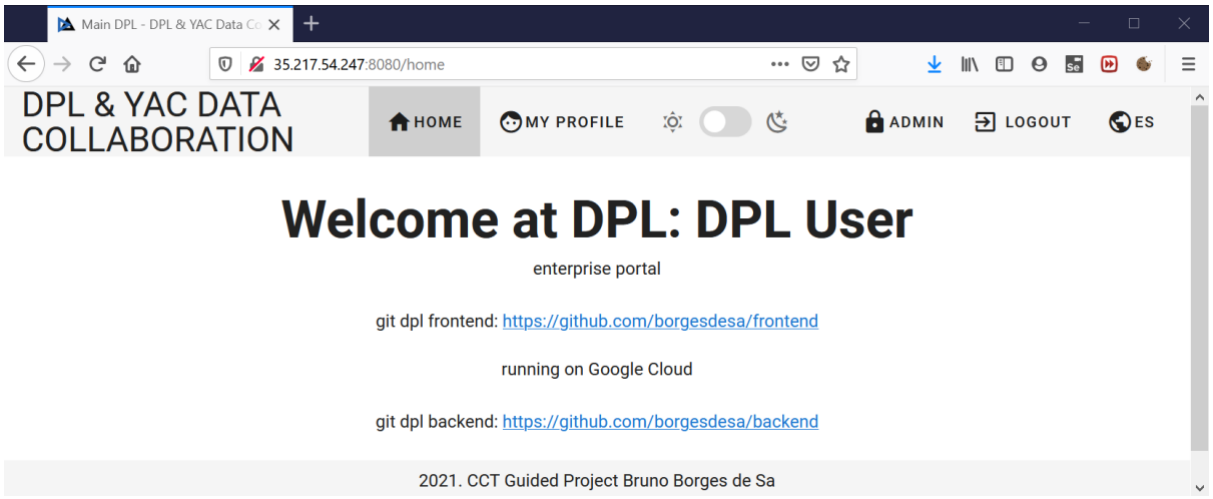


Figure 58

Next step is to login is enterprise user and start adding data, stored in the MongoDB. The backend is providing 2 routes to data: users and cities.

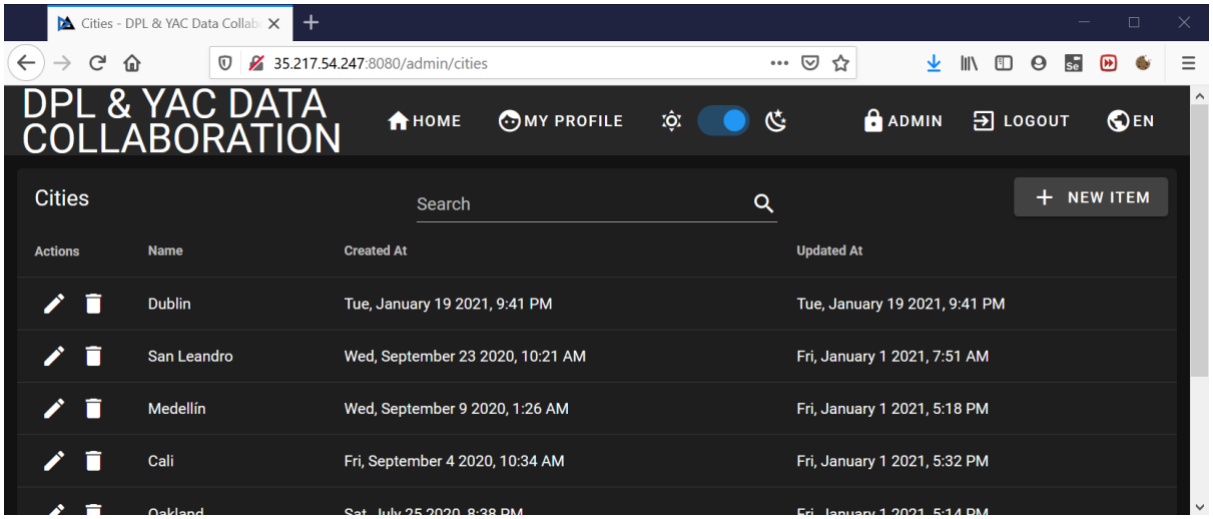


Figure 59

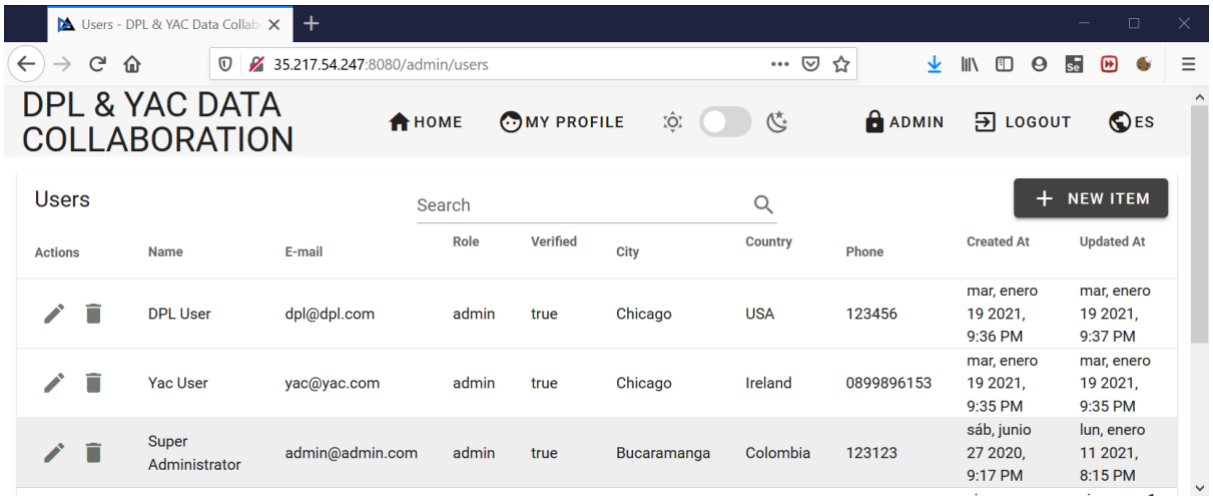


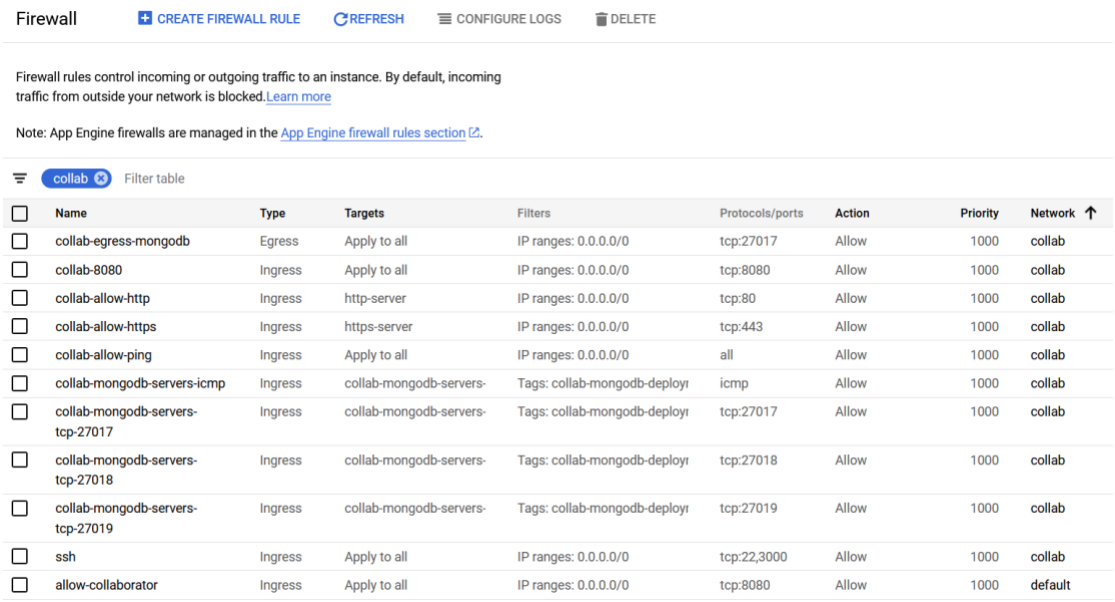
Figure 60

As you can see, there are three different users available:

- DPL User (adding data from DPL)
- YAC User (adding data from YAC)
- Super User (administration of Database)

Cities can be added, modified and deleted (CRUD) as data records, therefore the most basic database operations are possible.

As for Security is enforced by Google (spam protection, denial of service protection, brute force attack protection) and our own firewall configuration:



Firewall CREATE FIREWALL RULE REFRESH CONFIGURE LOGS DELETE

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed in the App Engine firewall rules section.

collab Filter table

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network
collab-egress-mongodb	Egress	Apply to all	IP ranges: 0.0.0.0/0	tcp:27017	Allow	1000	collab
collab-8080	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:8080	Allow	1000	collab
collab-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	collab
collab-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	collab
collab-allow-ping	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1000	collab
collab-mongodb-servers-icmp	Ingress	collab-mongodb-servers-	Tags: collab-mongodb-deployr	icmp	Allow	1000	collab
collab-mongodb-servers-tcp-27017	Ingress	collab-mongodb-servers-	Tags: collab-mongodb-deployr	tcp:27017	Allow	1000	collab
collab-mongodb-servers-tcp-27018	Ingress	collab-mongodb-servers-	Tags: collab-mongodb-deployr	tcp:27018	Allow	1000	collab
collab-mongodb-servers-tcp-27019	Ingress	collab-mongodb-servers-	Tags: collab-mongodb-deployr	tcp:27019	Allow	1000	collab
ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,3000	Allow	1000	collab
allow-collaborator	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:8080	Allow	1000	default

Figure 61

Billing is transparent and only OpEx are due based on dynamic usage of CPU, memory, storage buckets, networking and maybe solutions. Some functions are ‘for free’ like API or JavaScript Functions. Complete solutions like databases or storage transfers are available:

Figure 62: Fig. Billing for the cloud platform during the Guided Project for CCT.

6 WHAT IS NEXT

Most of the goals in this essay were successfully achieved, this is only the beginning of a great journey. In another scenario where time and even knowledge were not an issue, it would be great to have worked with platforms that are largely used in enterprises. Cisco, for instance, is a great platform but quite legacy these days.

Nevertheless, it has been a great journey and a huge learning opportunity, especially regarding JavaScript and Google Cloud, so complex and relevant. It is also why Google Cloud was chosen for the Data Collaboration chapter, stepping away from the opensource requirement, which, at this point wouldn't seem realistic enough without these two big names when it comes to networking. Other providers were considered, like Microsoft Azure, but due to fees conditions it didn't seem as appealing as Google.

A great next step to me is getting further on covering cloud services, especially Kubernetes. The main reason, among many others, is the Application-centric management. It raises the level of abstraction from running an OS on virtual hardware to running an application on a container runtime using logical resources.

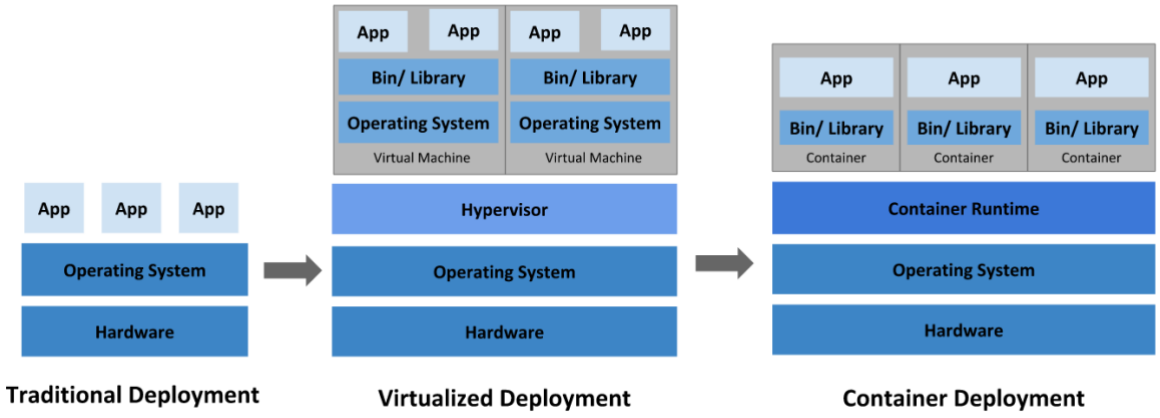


Figure 63: Going back in time in deployment. Available from: https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/

For the next years, I will keep on going my deep dive into JavaScript. The power of JavaScript is that the language itself is a link for all the modules and frameworks. It is widespread and knowhow gained will stay precious and stable, while product knowhow itself will not. Either way, I feel deeply grateful to have had this opportunity to get to know and integrate so many different things into such a big project.

7 APPENDIX: CODE LISTINGS

Cisco Packet Tracer network design: https://drive.google.com/file/d/13bIslURBP7wL9R2qYq0FDigLzNfKEWr7/view?usp=sharing (username: admin, password: password);

DPL intranet portal: https://drive.google.com/drive/folders/1TlzH5K9QX-83wEAuTftjX-iPVhvqhjs8?usp=sharing;

Back end solution: https://github.com/borgesdesa/backend;

Front end solution: https://github.com/borgesdesa/frontend;

Front end Skeleton: https://github.com/davellanedam/vue-skeleton-mvp;

Back end Basic Project Skeleton: https://github.com/davellanedam/node-express-mongodb-jwt-rest-api-skeleton;

Google Cloud VM front end instances: http://35.217.21.241:8080/, http://35.217.54.247:8080/;

8 REFERENCES

Caroll, A. (n.d.). *Data center redundancy.* Lifeline Data Centers. [online]. Available from: https://lifelinedatacenters.com/data-center/data-center-redundancy-what-you-need-to-know/ [accessed 3 December 2020].

CiscoStudents (2010). *Packet Tracer Tutorial #1* [online]. YouTube. Available from: https://www.youtube.com/watch?v=VqMeJ-WH4E0 [accessed 3 Jan. 2021].

Cloudflare (n.d.). *Business VPN uses and limitations* [online]. Cloudflare UK. Available from: https://www.cloudflare.com/en-gb/learning/access-management/what-is-a-business-vpn/ [accessed 10 January 2021].

Chan, M. (2019). *FTP, FTPS, and SFTP - what are the differences?* [online]. Thorn Technologies. Available from: https://www.thorntech.com/2019/07/ftp-ftps-sftp-differences/ [accessed 12 January 2021].

Contact Centre World (2017). *10 Questions to Ask Your VoIP Service Provider.* - VoIP Supply – Contact Centre World Blog [online]. Available from: https://www.contactcenterworld.com/company/blog/voip-supply/?id=e1429897-af56-4039-bb32-fd698218c13a [accessed 4 January 2021].

Data Center Knowledge (2015). *Six Facts in High-Availability Data Center Design*. Data Center Knowledge [online]. Available from: https://www.datacenterknowledge.com/archives/2015/09/30/six-facts-in-high-availability-data-center-design. [accessed 10 December 2020].

Emesowum, H, Paraskelidis, A & Adda, M. (2017). *Fault Tolerance Improvement for Cloud Data Center*. Journal of Communications [online]. Available from: https://www.researchgate.net/publication/322127191_Fault_Tolerance_Improvement_for_Cloud_Data_Center [accessed 12 December 2020].

Google Cloud. (n.d.). *VPC network overview* [online]. Google Cloud. Available from: https://cloud.google.com/vpc/docs/vpc [accessed 12 January 2021]

Google Developers. (n.d.). *Public DNS* [online]. Google Developers. Available from: https://developers.google.com/speed/public-dns [accessed 23 January 2021].

Hostinger. (2017). *How Does SSH Work* [online]. Hostinger Tutorials. Available from: https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work. [accessed 23 January 2021]

Kerravala, Z. (2018). *DHCP defined and how it works* [online]. Network World. Available from: https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html. [accessed 4 January 2021].

Kubernetes (2014). *What is Kubernetes* [online]. Kubernetes. Available from: https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/ [accessed 25 January 2021].

Liu, V. (2016). *Improving Fault Tolerance and Performance of Data Center Networks*. University of Washington. Washington.

Lotz, M. (2018). *Waterfall vs. Agile: Which Methodology is Right for Your Project?* Segue Technologies [online]. Available from: https://www.seguetech.com/waterfall-vs-agile-methodology/ [accessed 25 November 2020].

Lucidchart. (2017). *The 5 Steps of the Strategic Planning Process*. Lucidchart [online]. Available from: https://www.lucidchart.com/blog/5-steps-of-the-strategic-planning-process. [accessed 4 December 2020].

MIT. (2019). *Kerberos: The Network Authentication Protocol* [online]. Massachusetts Institute of Technology. Available at: https://web.mit.edu/kerberos/ [accessed 9 January 2021]

Microsoft Docs (2020). *Dynamic Host Configuration Protocol (DHCP)* [online]. Microsoft. Available from: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top [accessed 5 January 2021]

Network Computing (n.d.). *Cisco Retains Enterprise Infrastructure Market Dominance* [online]. Available from: https://www.networkcomputing.com/data-centers/cisco-retains-enterprise-infrastructure-market-dominance [Accessed 2 Jan. 2021].

OmniSci. (n.d.). *What is Edge Network?* [online]. OmniSci. Available from: https://www.omnisci.com/technical-glossary/edge-network [accessed 19 January 2021].

Oracle. (n.d.). *High Availability Concepts and Best Practices*. Oracle [online]. Available from: https://docs.oracle.com/cd/A91202_01/901_doc/rac.901/a89867/pshavdtl.htm [accessed 19 November 2020].

Packet Tracer Network (n.d.). *Cisco Packet Tracer 7.x tutorials* [online]. Packet Tracer Network. Available at: https://www.packettracernetwork.com/tutorials/ [accessed 3 Jan. 2021].

Reid, D. (2007). *VLAN How To: Segmenting a small LAN.* Small Net Builder [online]. Availabla from: https://www.smallnetbuilder.com/lanwan/lanwan-howto/30071-vlan-how-to-segmenting-a-small-lan?start=5 [Accessed 3 December].

Team Gantt. (2019). *Online Gantt Chart Software*. Team Gantt [online]. Available from: https://www.teamgantt.com/ [Accessed 27 November 2020].

Thurner, S., Klimek, P. & Hanel, R. (2020). *A network-based explanation of why most COVID-19 infection curves are linear*. Proceedings of the National Academy of Sciences [online]. Available from: https://www.pnas.org/content/117/37/22684 [Accessed 17 January 2020].

VoIP Insider. (2017). *10 Questions to Ask Your VoIP Service Provider*. [online]. VOIP Supply. Available at: https://www.voipsupply.com/blog/voip-insider/10-questions-to-ask-your-voip-service-provider/ Accessed 23 December 2020].

Zentyal Community (n.d.). *Zentyal 5.1 Official Documentation* [online]. Zentyal. Available from: https://doc.zentyal.org/5.1/en/index.html [Accessed 3 January 2021].