SOLENT UNIVERSITY   
**Department of Science and Engineering**

BSc (Hons) **CYBER SECURITY MANAGEMENT**

**Network Management - COM615**

**Data Centre Case Study**

**Academic Year 2024-2025**

**FRANCIS BAAFI**

**Portfolio –** Assignment 1

**Tutor: Neville Palmer [10/01/2025]**

**Table of Contents**

[**Introduction 5**](#_75wp514yobbw)

[**SLA/KPI 6**](#_wg7bmbq2q1d6)

[**Requirements 7**](#_pwqw6h5mj2fk)

[Requirements Gathering 7](#_swcrayebzt6m)

[1.0 - Layered Security Approach 8](#_22o920i0ilbi)

[There must be a layered security approach 8](#_4ivhsxo8droo)

[1.1 - Understand the client's expectations around the scope of security layers (e.g., perimeter, application, endpoint). 8](#_bl8k68skc6hj)

[The following Security layers must be implemented: 8](#_43w2fgw1z4xg)

[1.1.1 Perimeter 8](#_wsymqueu3nrg)

[1.1.2 Application 8](#_a0468pgqt3fw)

[1.1.3 Endpoint 8](#_7svu0c7naymj)

[2.0 - Access Control Policies 8](#_71hxdnnkp9yd)

[2.1 - The following access policies must be implemented for network devices: 8](#_gmc6qf30uydm)

[2.1.1 - Identity based 8](#_5081mwk1yuww)

[2.1.2 - Role based 8](#_h2hpwqb1yeu8)

[3.0 - Encryption Standards 9](#_ba8usgos59pa)

[3.1 - The following data encryption must be implemented for data: 9](#_hwzjl6fi7e1t)

[3.1.1 At rest 9](#_ge4lqfs4rq4a)

[3.1.2 In transit 9](#_7ftmnrm2yjvj)

[3.2 - Data encryption must be provided for data at rest and data in transit 9](#_11bcx7s5iqt)

[4.0 - Switch Security 10](#_f8tjrinm24bu)

[4.1 - There must be protection against the following attacks: 10](#_n4dplbwuwe3o)

[4.1.1 - DHCP 10](#_2bkf17jm8i2)

[4.1.2 - ARP 10](#_l66czh4pku0)

[4.1.3 - MAC Table Attacks (using DHCP Snooping and ARP Inspection) 10](#_n07jh55j34dn)

[4.2 - Implementing Spanning Tree Protocols (STP) 10](#_kq2w3cajwbr)

[4.2.1 - There must be protection against STP attacks 10](#_fjbb4ppvcnsf)

[4.3 - Trunking and VLANs (Creating Sub-interfaces) to segment the network (Microsegmentation) 10](#_g9vyass64gdn)

[4.3.1 - VLANs must be implemented to segment the network 10](#_knnguqdjf1jv)

[4.4 - Integrating Web Application firewalls as a layer of defence for Web Servers 10](#_xxs4kfilgbib)

[4.4.1 - There must be a web application firewall to protect the web server 10](#_df4ilk3wcjpx)

[5.0 - Security Enhancements 11](#_7bmm3yhdy847)

[5.1 - Need for securing network devices and customer systems. 11](#_yf7j7chacrio)

[5.1.1 - There must be network device security and endpoint security 11](#_ffxtv0ido9pq)

[5.2 - Implementation of IDS/IPS solutions for attack detection and prevention. 11](#_t4r4zlrvqbvx)

[5.3 - Implementing Syslog and SIEM for Events Logging and monitoring 11](#_uloiorx43o9y)

[5.3.1 - A syslog server must be implemented 11](#_ncdqwt5memq9)

[5.3.2 - SIEM must be implemented on the network 11](#_zetfzhtni9y7)

[5.4 - Implement NAT to block Private IP Addresses from roaming the Internet 11](#_x4yxd1xurf54)

[5.4.1 - NAT must be implemented on routers to hide private addresses from the internet 11](#_eb5opnmjjyro)

[**Group Contribution 12**](#_ex2mbw23xkk)

[**Plan 12**](#_qu59z67izel3)

[Perimeter Security 13](#_63afww9tsuum)

[Access Control & Authentication 13](#_eu7b33ah6ydm)

[Data Protection & Encryption 13](#_ov4tn0voapb)

[Network Segmentation 13](#_l24e18zhh718)

[Monitoring & Logging 13](#_cy2a0hy9gt94)

[Compliance 14](#_lk4ws28mtli6)

[**Technical Network Security (Solutions) 15**](#_irf5uoxddm2)

[Initial Topology of Data Centre 15](#_7z7nn7gaa4ea)

[Basic Security 16](#_wucd2n64vggv)

[**Research & Literature 17**](#_bgok35wv6gly)

[**Practical Experiment (Solutions) 18**](#_fz0xhlufx7lc)

[Basic Security 18](#_84x85p19hqk5)

[1.1 - Understand the client’s expectations around the scope of security layers (e.g. Perimeter, Application and endpoint). 20](#_z20kjumsvqto)

[1.1.1 - Perimeter Security 20](#_w5o4rb2s5nwk)

[2.1.1 - Identity-based Access Control 22](#_mwt4k5w3etez)

[2.1.2 - Role-based access control 24](#_lxmx84nd4zac)

[3.1.1 - Data at Rest 25](#_fje4cu71cllk)

[3.1.2 - Data in Transit 26](#_1pabgw58mie0)

[4.1.1 - DHCP 27](#_v6015idjulj4)

[4.1.2 - ARP 28](#_uu3bwlljhe6k)

[4.1.3 - MAC 28](#_37w6gfexkp55)

[4.3.1 - VLANs must be implemented to segment the network 29](#_e3qs7wegjmja)

[4.4.1 - There must be a web application firewall to protect the web server 31](#_e6lu1lotbmlz)

[5.2 - Implementation of IDS/IPS solutions 32](#_cev4a9n1pjx)

[5.3.1 - Syslog Server must be implemented 33](#_wr3wf1nm8gm2)

[5.4.1 - NAT must be implemented on routers to hide private addresses from the internet 33](#_tbk3nx9ep1ky)

[**Secured Network Topology 34**](#_ebskxiwjtwjg)

[**Summary of Solutions & Conclusions 34**](#_d6do4fqo1rv5)

[**Recommendations for further work 34**](#_nfdegwupzqko)

[**Appendix 36**](#_h29c5tcigi8z)

[Appendix A - PLAN 36](#_4q1nf53gu945)

[Appendix B 36](#_i75t2xwl0p8m)

[Perimeter Security 36](#_xibvfzidrkwh)

[Access Control & Authentication 37](#_siksuxuxlece)

[Data Protection & Encryption 37](#_rwb1q3a9bguv)

[Network Segmentation 37](#_l6tard1508ls)

[Monitoring & Logging 37](#_2w48ityhbnot)

[Compliance 38](#_7xurucgukrn5)

[Appendix C - Initial Topology of Data Centre 38](#_l8i5ppx8aeg8)

[Appendix D - Basic Security 38](#_4j1marc1oewj)

[Appendix E - Perimeter Security 39](#_viuvkhl93p2l)

[Appendix F - Identity-based access control 39](#_v2p080w467gc)

[Appendix G - Data in transit 39](#_p6i5qrb5ntxe)

[Appendix H - There must be a web application firewall to protect the web server 39](#_7i3tgv4t07uw)

[Appendix I - Syslog Server must be implemented 40](#_e7pgs1678re)

[**Supporting Evidence 41**](#_g7rsoci3crfa)

# Introduction

In this Project, I have been assigned the role of enhancing the security posture of the Data Centre we provide to our customers. As previously mentioned in the case study, recently there has been an upsurge in demand for working from home Georgiadou, Anna; Mouzakitis, Spiros; Askounis, Dimitris, (2022). (especially after COVID-19), there has been an increase in business and interest in the services we provide for Cloud Computing Solutions.

Our company Name is Danson Data Solutions & Associates Ltd. We are a cloud based Data Centre, aiming to supply approximately 100-150 customers, supporting 1000 simultaneous connections with cloud based services. We provide a variety of services ranging from Infrastructure as a Service to Platform and even Software for small businesses. Our main objective is to adapt our services to our customer demands, M. F. Bari; R. Boutaba; R. Esteves; L. Z. Granville; M. Podlesny; M. G. Rabbani; Q. Zhang; M. F. Zhani, (2013). also enhancing and hardening our security postures with various standards and compliances, when integrating new systems into our network.

My role within the team takes responsibility in Network Security, Z. Chen; F. Han; J. Cao; X. Jiang; S. Chen, (2013). in which I have been tasked to ensure personnel who have been authorised have provision and limited access to the data centre through cloud computing, and implementing security measures to reduce risks of exposure to loopholes within cloud computing, which may affect the data centre for our customers. In this assignment I will be mentioning the different security measures implemented to strengthen the security posture of our data centre as they become more scalable.

The area for investigation and concern was security should involve a defence in depth approach for both the customer side and the provider side (Data Centre and Customer IT Systems), as we have identified that security of network devices and systems should be improved.

# SLA/KPI

The Service level Agreements between Danson Data Centre and our clients, will define the expectations, obligations and key performance indicators, established for both parties. El-Awadi,Radwa; Abu-Rizka,Mohamed, (2015). The main aim of implementing Service Level Agreements is to ensure both parties can come to an understanding and agreement on service standards, performances and responsibilities.

1. Service Availability (Uptime Guarantee) must be as follows:

* Percentage of time the data centre services will be available to the clients
  + Tier 1 - (99.9%) Uptime in 1 Year
  + Tier 2 – (99.99%) Uptime in 1 Year
  + Tier 3 – (99.999%) Uptime in 1 Year
* Logs and reports monitored monthly, and provided to the clients
* Remediation if uptime falls below the agreed level, the clients should be entitled to financial compensation or service credits

1. Response Time for Incidents and Technical Issues must be as follows:

* This is the maximum amount of time it will take our team to respond to unavailability of services after it has been detected, issuing a ticket and resolving issue immediately
* Incident Response Time prioritisation levels
  + P1 - (Crucial): Complete outage - 15 minutes to respond to incident
  + P2 - (High): Major service impact - 30 minutes to respond to incident
  + P3 - (Medium): Moderate service degradation - 1 hour response
  + P4 - (Low): Minor issues - 4 hours response

1. Backup and Data Recovery

* There must be regular backups of data, being able to restore back to previous state in the case of a security breach or event
* Must be a retention policy to define how long backups will be stored and available for recovery
* Must be a Disaster Recovery plan for restoring services in a security event

1. Maintenance of systems and Scheduled Downtime

* When there is regular maintenance for where services will be unavailable
* Clients must be notified of the expected timelines of unavailability in good time for the clients to prepare for scheduled and emergency maintenance

# Requirements

## Requirements Gathering

**Stakeholders Interviews:**

We engaged our stakeholders to clarify and expand on their needs and requirements.

**Technical Assessments:**

Multiple assessments of current network security were tested via Penetration testing to understand state of security posture and to identify areas of improvement.

**Documentation:**

Results were documented, permitting for the development of requirements for client review, and established agreement on prioritising what must be included from a security perspective.

## 

## 

## 1.0 - Layered Security Approach

### There must be a layered security approach

After some careful consideration and analysis of the current security posture of the network, I have integrated requirements to enforce a more layered security approach on the network

### 1.1 - Understand the client's expectations around the scope of security layers (e.g., perimeter, application, endpoint).

Our services are scalable, based on clients requirements, enabling us to adapt to their needs. Hagos, Desta Haileselassie, (2016). This may make some modifications to the network topology due to the services a client may want, amount of applications running on their network, and endpoint devices. All of these require specific security measures which may not be applicable to other networks due to the infrastructure of the topology. E.g. Some clients may want to host a web server which will require Web Application Firewalls Z. Ghanbari; Y. Rahmani; H. Ghaffarian; M. H. Ahmadzadegan, (2015). while other clients may not need web services hosted.

### The following Security layers must be implemented:

#### 1.1.1 Perimeter

#### 1.1.2 Application

#### 1.1.3 Endpoint

## 2.0 - Access Control Policies

### 2.1 - The following access policies must be implemented for network devices:

Configuring access controls and policies are a crucial part in securing network devices. Access will be granted, Samarati, Pierangela; De Vimercati, Sabrina Capitani, (2000). on certain systems based on your identity for verification of users and role based access, based on the users job role. Osborn, Sylvia; Sandhu, Ravi; Munawer, Qamar, (2000).

#### 2.1.1 - Identity based

#### 2.1.2 - Role based

## 3.0 - Encryption Standards

### 3.1 - The following data encryption must be implemented for data:

#### 3.1.1 At rest

#### 3.1.2 In transit

For network security assurance we will address data at rest and in transit techniques to our clients. Where data is stored when not in use, and the type of encryption (AES256) El Adib, Samir; Raissouni, Naoufal, (2012), when data is being transmitted on the network (TLS).

Enforce Data encryption at rest and in transit for comprehensive protection across all layers

### 3.2 - Data encryption must be provided for data at rest and data in transit

## 4.0 - Switch Security

Integrating and configuring switch security is essential as the switches have direct connectivity with the servers and systems we provide to our client (according to the initial topology), if they have been breached or compromised it could potentially affect the availability of our servers, which could cause data loss and other malicious intended attacks.

### 4.1 - There must be protection against the following attacks:

#### 4.1.1 - DHCP

#### 4.1.2 - ARP

#### 4.1.3 - MAC Table Attacks (using DHCP Snooping and ARP Inspection)

### 4.2 - Implementing Spanning Tree Protocols (STP)

#### 4.2.1 - There must be protection against STP attacks

### 4.3 - Trunking and VLANs (Creating Sub-interfaces) to segment the network (Microsegmentation)

#### 4.3.1 - VLANs must be implemented to segment the network

VLANs are required to segment the overall network structure into smaller networks, each client assigned a specific VLAN (Network). Mehdizadeha, Abbas; Suinggia, Kevin; Mohammadpoorb, Mojtaba; Haruna, Harlina, (2017).

For public facing servers, we have agreed to allocate them to a Demilitarized Zone, isolating public facing services from the rest of the network for security reasons. Rababah, Baha; Zhou, Shikun; Bader, Mansour, (2018).

### 4.4 - Integrating Web Application firewalls as a layer of defence for Web Servers

#### 4.4.1 - There must be a web application firewall to protect the web server

Due to research, and statistics, Web Servers are a common avenue an attacker would exploit (infiltrate/exfiltrate data). Implementing another layer of security both in front and behind the web servers, enables a stronger security posture.

## 5.0 - Security Enhancements

### 5.1 - Need for securing network devices and customer systems.

Integrating endpoint security and network device security ensuring our services are always available securely for our clients.

#### 5.1.1 - There must be network device security and endpoint security

### 5.2 - Implementation of IDS/IPS solutions for attack detection and prevention.

IDS will be used to detect and alert network administrators of any abnormal behaviour on the network and IPS will be used to Block and prevent certain packets and ports from roaming the LAN. Ashoor, Asmaa Shaker; Gore, Sharad, (2011).

### 5.3 - Implementing Syslog and SIEM for Events Logging and monitoring

A syslog server will be configured for events logging and monitoring.

#### 5.3.1 - A syslog server must be implemented

#### 5.3.2 - SIEM must be implemented on the network

### 5.4 - Implement NAT to block Private IP Addresses from roaming the Internet

#### 5.4.1 - NAT must be implemented on routers to hide private addresses from the internet

This will be configured at the router to prevent private IP addresses from roaming the internet, by changing it to public IP addresses. Bansal, Anchit; Goel, Priyanka, (2017).

NAT will be implemented to prevent the shortages of IP addresses

Each private devices will be mapped using a subnet which will be differentiated by port numbers

Each company will be given their own public address because of VLANs

# Group Contribution

As a group we all had our various topics in which we deployed to contribute to this assignment. We agreed to have regular meetings to update our teammates of our progress in our individual tasks. I had uploaded the initial topology of our network infrastructure and the requirements to harden the Network Security posture of the topology. I also discussed with my group the various customer requirements relevant to the frail network topology, which allowed me to carry out this assignment to harden the security posture of the Data centre. This Group contribution was carried out using Trello which enabled each individual to upload their requirements and other useful information, to allow the rest of the team to access.

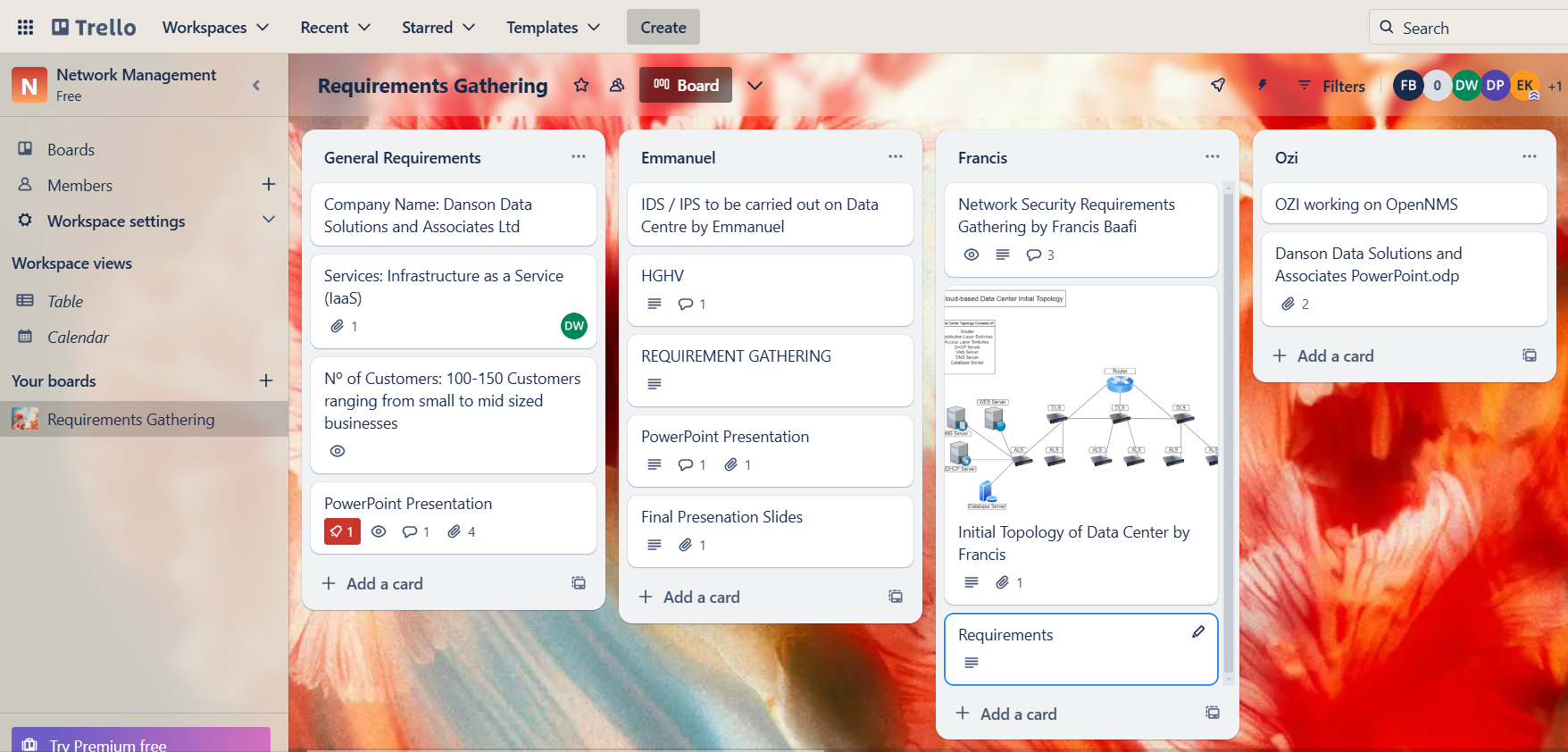
****

Figure 1

# Plan

Analysis of current network topology will be done to assess the current security posture of our network. As our network will be versatile and scalable to customer demands, I will need to address various security measures for the different services that we are providing, also ensuring we provide sufficient security for the network. We will be addressing the following layers of security:

* I will configure access lists and policies based on which users will be granted access to network devices.
* I will implement AAA and Parser views, for verification before access is fully granted. Users will have access based on roles and identity.
* I will configure VLANs to split the overall network structure into smaller segments of the network.
* I will configure devices to protect against STP Attacks
* I will configure firewalls and Zone based policy firewalls
* I will Implement IDS/IPS Solutions
* I will configure NAT

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (A) \***

## Perimeter Security

According to Requirement 1.1.1, I will address the following aspects:

For security of the Web Server I will implement a Web Application Firewall (WAF), whereby policies will be set on the firewall to block specific ports and to protect web applications.

As a layer of defence Internet facing Servers, will be isolated from the network and held in a DMZ separating these services from internal systems limiting reach of potential attacks.

Implementing microsegmentation permits the network architect to obtain granular control over traffic between servers and applications. In the case of our Data Centre each client will have their own VLANs and have the option to microsegment their services and systems hosted on our network.

Honeypots are a form of studying behavioural characteristics of attackers. We will implement this within the DMZ, copying the topology of the servers, and configuring meaningless or null values in those servers.

## Access Control & Authentication

According to Requirement 2.0, I will need to implement access control lists and policies, to permit certain personnel to access systems and services. Access will be granted based on identity or roles.

## Data Protection & Encryption

According to Requirement 3.0, I will be addressing encryption techniques implemented to ensure data is kept safe in transit, at rest and when data is stored. This will be addressed using AES256 and when data is transmitted we will use TLS.

## Network Segmentation

According to requirement 4.3 and also requirement 1.1.1, I will be addressing microsegmentations in the form of VLANs. Essentially this will be implemented to isolate the various networks that we obtain via the number of customers we have and limit their access to only their company specific systems.

## Monitoring & Logging

According to Requirements 5.3, I will implement syslog servers for events monitoring and logging. This will be a centralised server which will be monitoring every device integrated into our network.

## Compliance

When integrating the design of the network I will be correlating with the following compliance and regulatory legislations:

* NIST
* ISO 27001/2
* GDPR
* PII

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (B) \***

# 

# 

# 

# 

# 

# 

# Technical Network Security (Solutions)

## Initial Topology of Data Centre

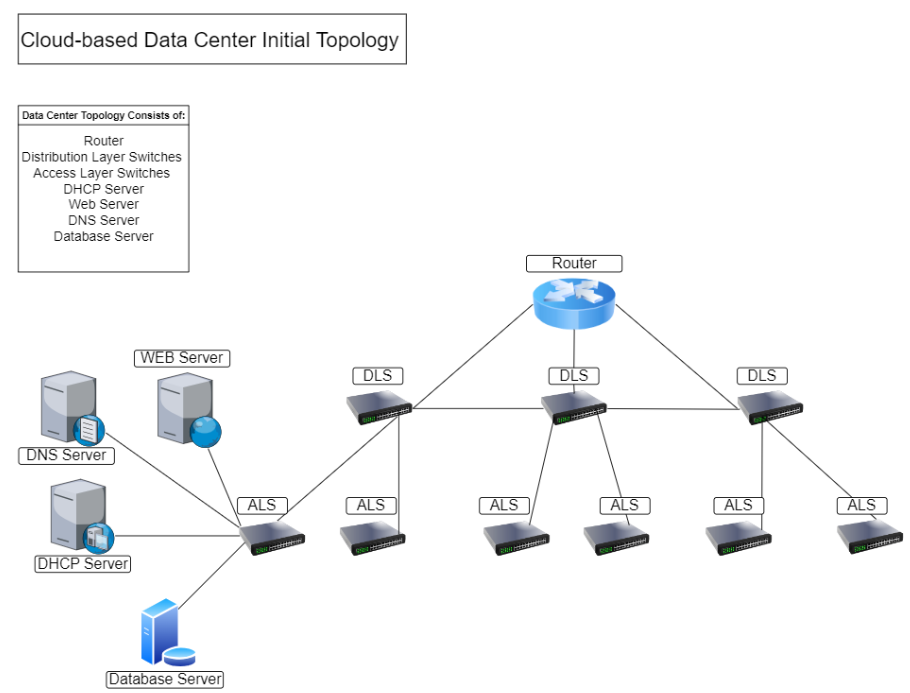


Figure 2

After some careful evaluation, the initial networking topology of our cloud-based Data Centre was designed. This is the current blueprint of our topology in which as a Networking Security Architect, I can see there are multiple flaws within this topology needing to be attended to before we can go live and launch our services to our various customers. In this assignment I am tasked with integrating security policies and procedures to our network to safeguard our customers and their data, as discussed in the SLAs and KPIs.

The initial topology consists of:

* **1 Router** - For WAN connectivity
* **3 Distribution Layer Switches (DLS)** - Located between the router and access layer switches used to aggregate data from multiple access switches
* **6 Access Layer Switches (ALS) 2 per DLS** - Located at the LAN side of topology, used to connect end devices to network, in this case servers.
* **4 Servers (Web, DHCP, DNS and Database)** - Initiate traffic to the core of the network and other devices requesting to use service.

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (C) \***

## Basic Security

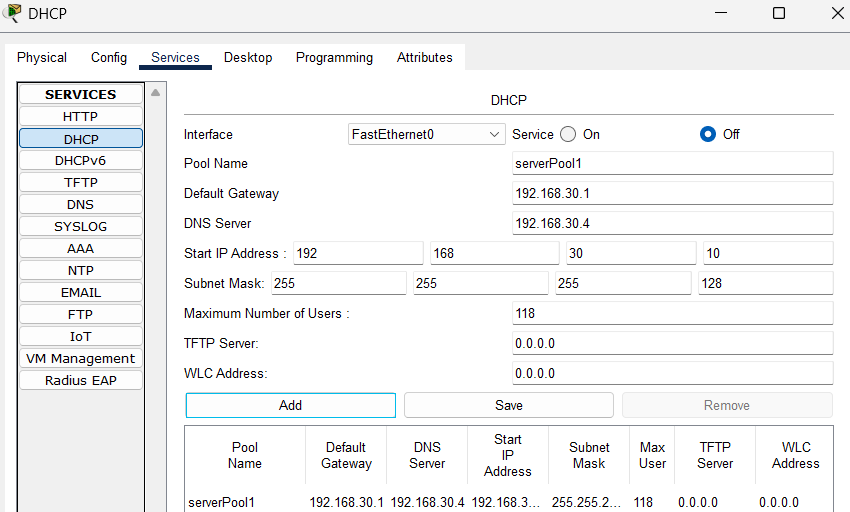


Figure 3

Configuring a DHCP Server (192.168.30.3), limiting address range to 118 available hosts /25 subnets. As a network architect limiting IP addresses is essential as we will only be hosting for 100 customers meaning there would be 18 addresses left over.

In this case I have allocated an address range from 192.168.30.3 (DHCP) - 192.168.30.9 to all servers implemented in this network design.

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (D) \***

# Research & Literature

ASHOOR, A.S. and S. GORE, 2011. Difference between intrusion detection system (IDS) and intrusion prevention system (IPS). *Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011 4.* Springer, pp.497–501 - **Established difference between IPS/IDS**

BANSAL, A. and P. GOEL, 2017. Simulation and analysis of network address translation (NAT) & port address translation (PAT) techniques. *Int.Journal of Engineering Research and Application,* 7(7), 50–56 - **This reference helped me to understand the concept of NAT**

EL ADIB, S. and N. RAISSOUNI, 2012. AES encryption algorithm hardware implementation: throughput and area comparison of 128, 192 and 256-bits key. *International Journal of Reconfigurable and Embedded Systems (IJRES),* 1(2), 67–74 - **This Reference enabled me to understand the comparison of AES encryption Keys**

EL-AWADI, R. and M. ABU-RIZKA, 2015. A Framework for Negotiating Service Level Agreement of Cloud-based Services. *Procedia Computer Science,* 65, 940–949 - **For Service Level Agreements of Cloud-based Data Centres**

GEORGIADOU, A., S. MOUZAKITIS and D. ASKOUNIS, 2022. Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal,* 35(2), 486–505 - **Referenced to Introduction showing the popularity of working from home since COVID-19**

HAGOS, D.H., 2016. Software-defined networking for scalable cloud-based services to improve system performance of hadoop-based big data applications. *International Journal of Grid and High Performance Computing (IJGHPC),* 8(2), 1–22 -

M. F. BARI *et al.,* 2013. Data Center Network Virtualization: A Survey. *IEEE Communications Surveys & Tutorials,* 15(2), 909–928

MEHDIZADEHA, A. *et al.,* 2017. Virtual Local Area Network (VLAN): Segmentation and Security. *The Third International Conference on Computing Technology and Information Management (ICCTIM2017).* Pp.89 - **Importance of Network Segmentation and VLANs**

OSBORN, S., R. SANDHU and Q. MUNAWER, 2000. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security (TISSEC),* 3(2), 85–106 - **Role-based access control**

RABABAH, B., S. ZHOU and M. BADER, 2018. Evaluation the Performance of DMZ. *International Journal of Wireless and Microwave Technologies,* 1(1), 1–13 - **Effectiveness of Integrating DMZ**

SAMARATI, P. and S.C. DE VIMERCATI, 2000. Access control: Policies, models, and mechanisms. *International school on foundations of security analysis and design.* Springer, pp.137–196 - **Understanding Access Control Policies**

Z. CHEN *et al.,* 2013. Cloud computing-based forensic analysis for collaborative network security management system. *Tsinghua Science and Technology,* 18(1), 40–50

Z. GHANBARI *et al.,* 2015. Comparative approach to web application firewalls. *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI).* Pp.808–812 - **Web Application Firewalls**

# Practical Experiment (Solutions)

## Basic Security

This isn't a requirement, but as i have built this network from the roots, i have decided to show the basic network configurations made on these devices

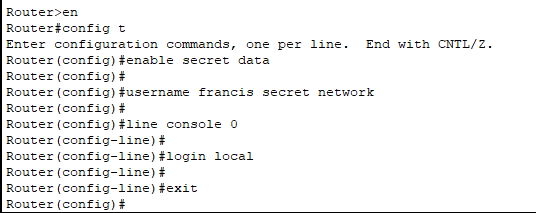


Figure 0.1 - Creating enabled or Privileged user

To prevent unauthorised access, an administrative user was created for the network configurations, with the ***username*** of ***francis*** and ***password*** of ***network*** and ***secret*** of ***data*** to get into config mode.

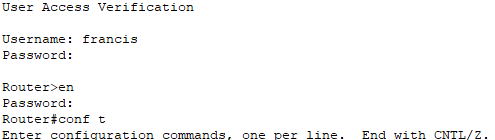


Figure 0.2 - User Verification

shows user verification to access config mode.

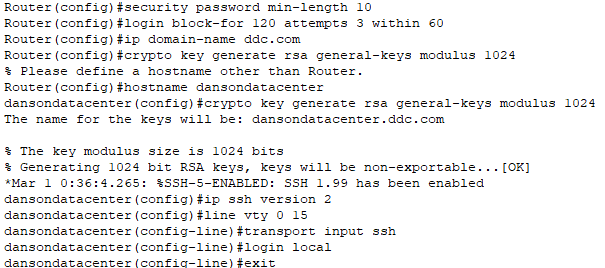


Figure 0.3 - Setting min password length, timeouts and SSH Version 2

According to NIST, they recommend users to set a minimum password length of 10 characters (***security password min-length 10***). I had also set up blocking login attempts to 3 unsuccessful attempts within the space of 1 minute (timeout) (***login block-for 120 attempts 3 within 60***). SSH was configured for remote access, implementing version 2 which is more secure (***ip ssh version 2***).

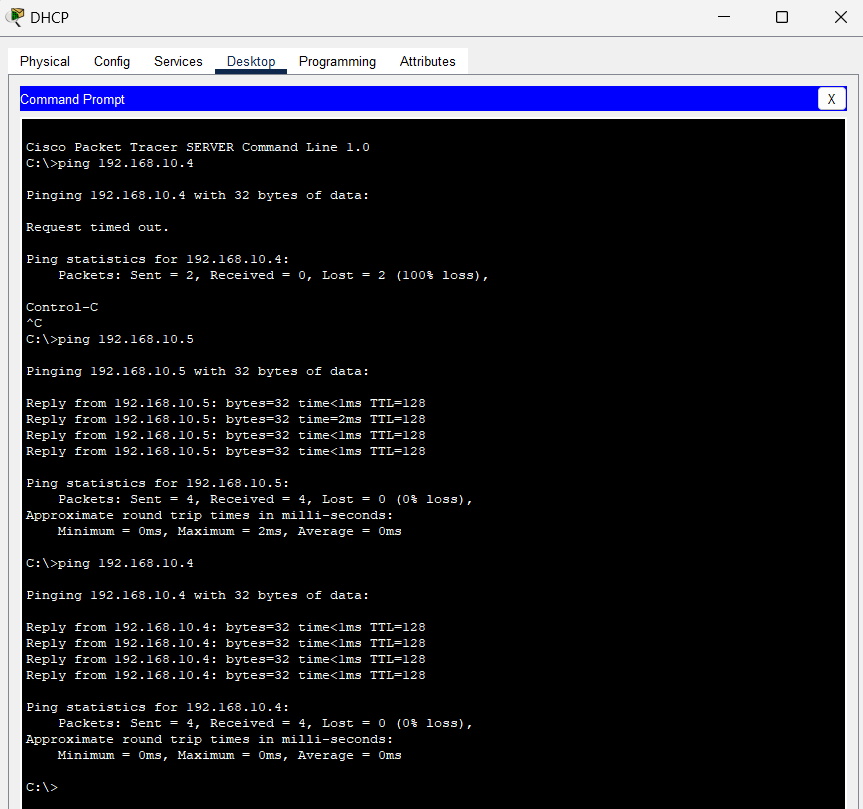


Figure 0.4 - Verifying connectivity between servers

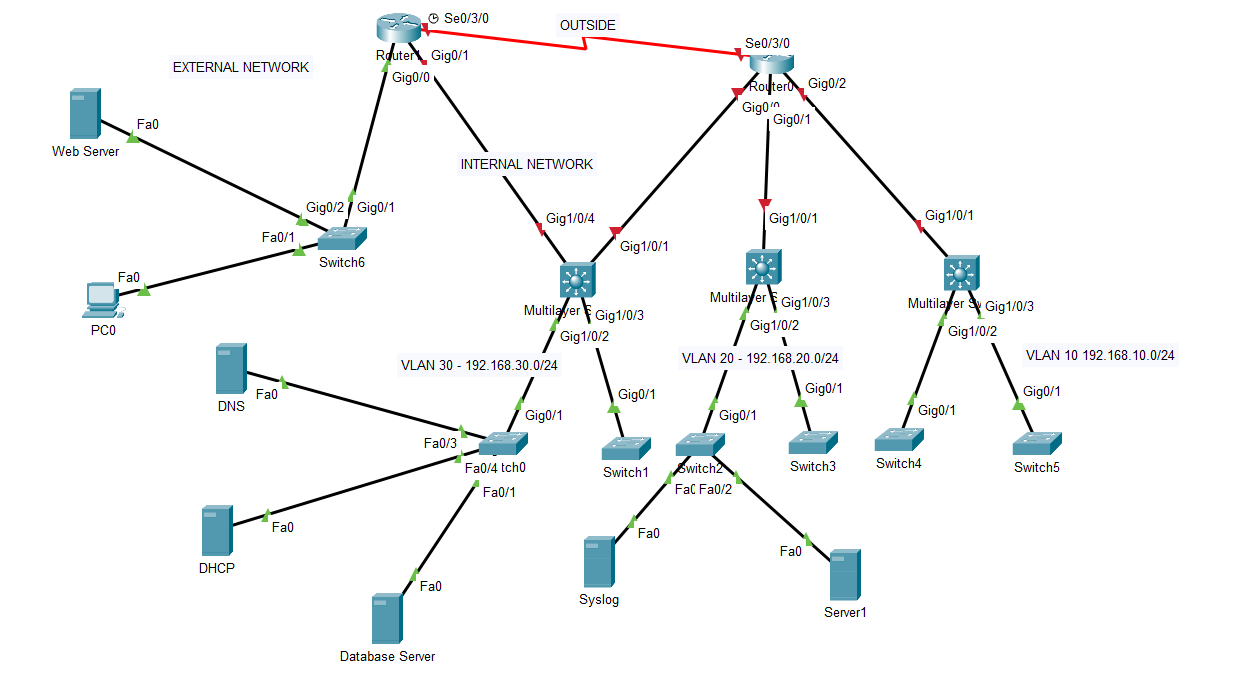
Pinging Servers to establish connectivity

## 1.1 - Understand the client’s expectations around the scope of security layers (e.g. Perimeter, Application and endpoint).

### 1.1.1 - Perimeter Security

I have split the network into different VLANs with each customer assigned their own network (different default gateways). Here are the following VLANs configured on the network for 3 different customers: (VLAN 20 will be used by one of our teams for monitoring purposes)

* VLAN 10 - 192.168.10.0 / 24 - Netmask - 255.255.255.0 - Wildcard - 0.0.0.255
* VLAN 20 - 192.168.20.0 / 24 - Netmask - 255.255.255.0 - Wildcard - 0.0.0.255
* VLAN 30 - 192.168.30.0 / 24 - Netmask - 255.255.255.0 - Wildcard - 0.0.0.255

Figure 1.1.1 - Assigning VLANs

I have configured access lists to prevent conflict between these VLANs.Each VLAN has been configured to block any access coming from another VLAN. For instance in Figure 1.1.1, you can see I have configured VLAN 20 to block any access to the network from VLAN 30. This has been implemented so that other customers cannot access unauthorised services of another customer, and also to reduce the impact of a security breach on the network by isolating and segmenting overall network structure.

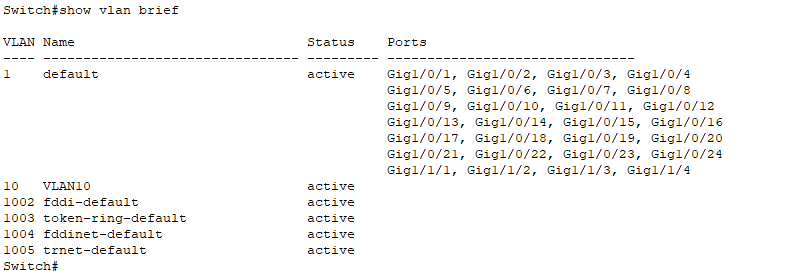
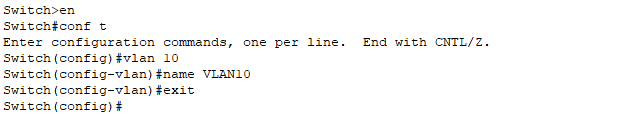


Figure 1.1.2 - Configuring VLANs on Multi-layer Switches

As previously stated each client willing to integrate their systems to our network will be assigned their own VLAN. In this case Figure 1.1.2 shows the configuration of VLAN 10, which has been activated, ready to have ports assigned to it.

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (E) \***

### 2.1.1 - Identity-based Access Control

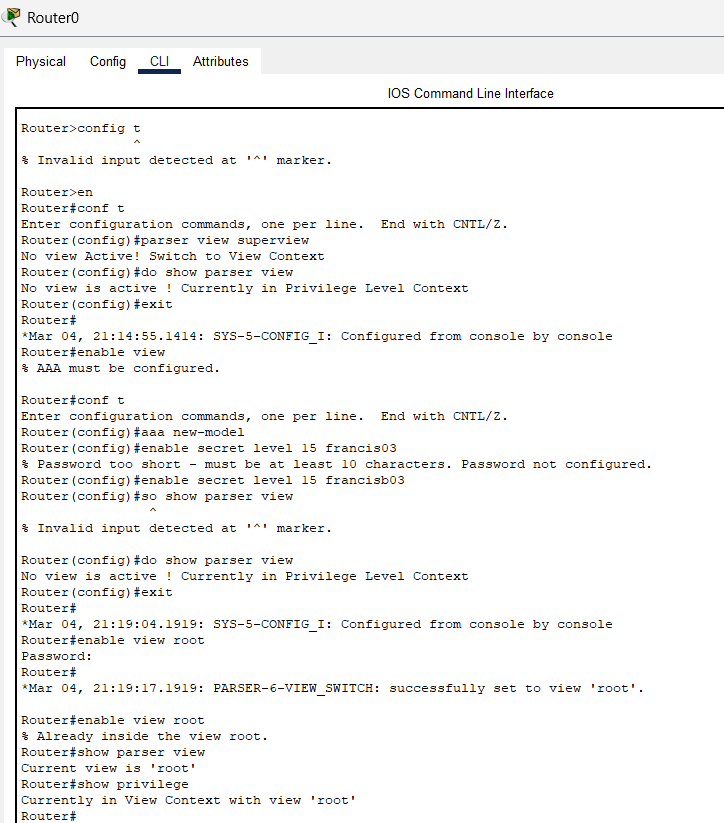


Figure 2.1.1 A - Activating Parser view

In this figure you can see that I have activated parser views. AAA had been configured as an additional layer of security to grant access to an entity of the network. I have created a policy whereby each client we have on our network will be assigned their own network security agent who takes care of configuration management and ensuring security posture and availability is at the level we intended, according to our SLA.

In Figure 2.1.1 A ***privilege level 15*** has been configured with a ***password*** of ***francisb03*** for the Network Security Agent.

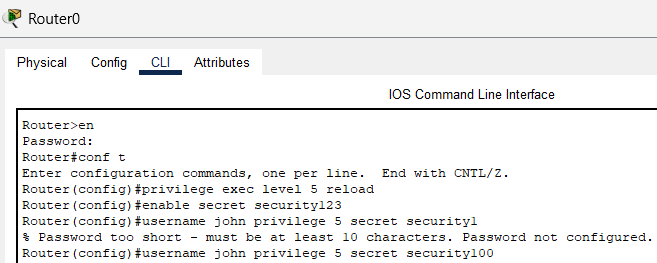


Figure 2.1.1 B - Configuring privilege level 5

Privilege level 5 users will be assigned to our support engineer who would be the first line support to troubleshoot any issues and view system configurations rather than escalating issues to higher levels, but not have the ability to modify critical settings. For instance checking for monitoring performance metrics, viewing interface status and checking logs.

As you can see in the Figure 2.1.1 B the ***username John*** has been assigned Privilege level 5 with the password of ***security100***, also have the ***reload*** command protected with the ***secret*** of ***security123***

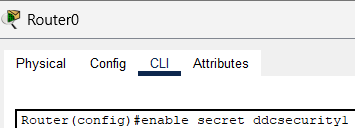


Figure 2.1.1 C - Protection of privilege level 15

Password protection for privilege level 15 user was configured. ***enable secret ddcsecurity1***

### 2.1.2 - Role-based access control

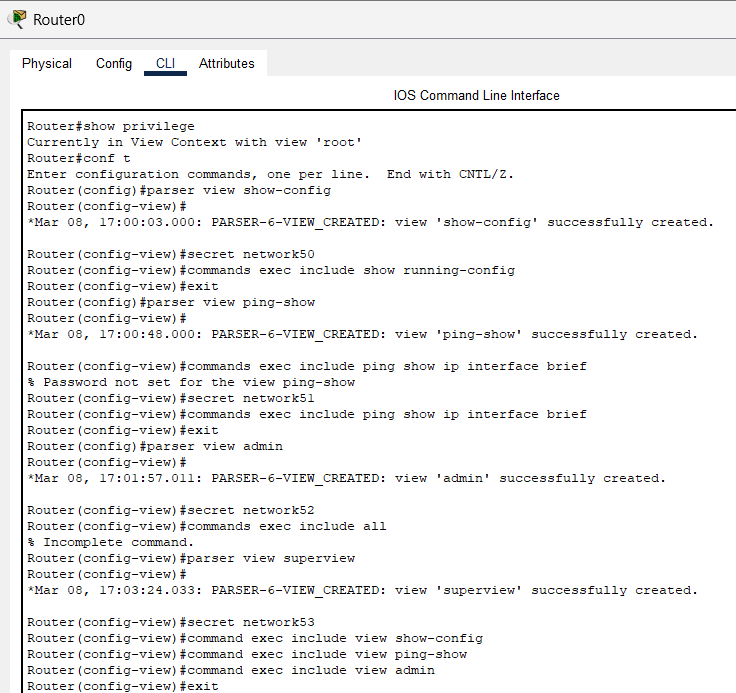


Figure 2.1.2 A - Configuring role-based views

Referring to parser view activation mentioned previously in figure 2.1.1 A It was vital in enabling configuration of role-based views.

1. ***show-config*** enables users to only have access to show configurations of network devices.
2. ***ping-show*** enables a user view that can only ping and display IP interface addresses.
3. ***admin*** enables the user to have full access.
4. ***superview*** includes all the three views above and enables multiple user views to combine into a single view, allowing users to access commands permitted in each view, without having to revert.

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (F) \***

### 3.1.1 - Data at Rest

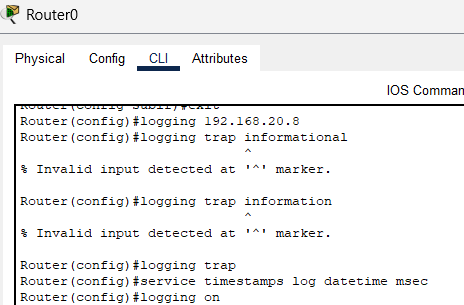


Figure 3.1.1 A - Redirecting log traffic to syslog server

This figure shows the configuration of a secured syslog server (192.168.20.8).

***service timestamps log datetime msec*** command will display every log, the time and the date in the syslog message. The IP address of the syslog server is configured as the host ***logging host 192.168.20.8***, the router has also been configure to include debugging messages ***logging trap debugging***

### 3.1.2 - Data in Transit

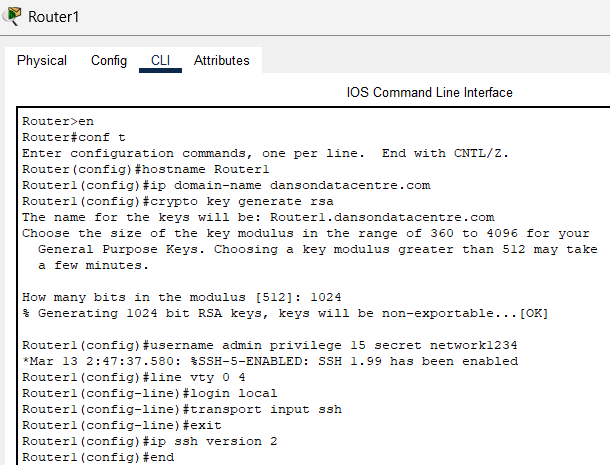


Figure 3.1.2 A - Data in transit (SSH)

As a form of data in transit I have decided to configure SSH to protect data in transit by encrypting the communications between devices.

Configuring version 2 of SSH which is more secure ***ip ssh version 2***

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (G) \***

### 4.1.1 - DHCP

Here, I will initiate protective measures against DHCP Snooping Attacks, as shown in the figure below:

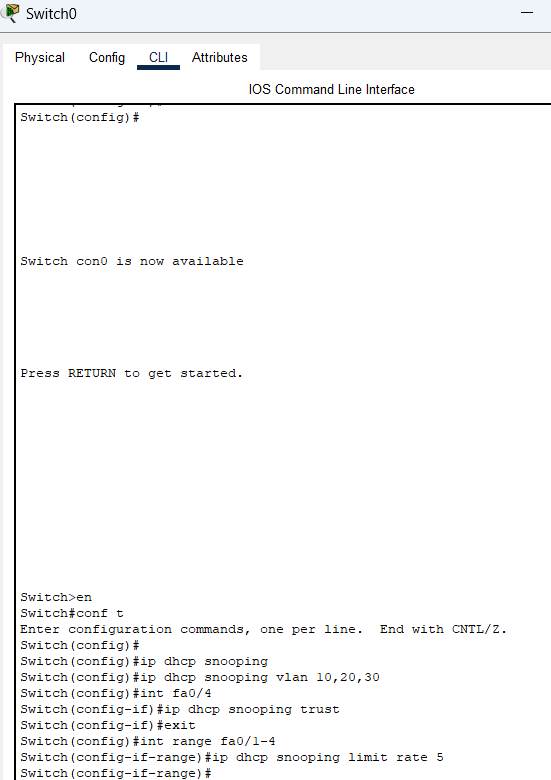


Figure 4.1.1 A - Protection against DHCP Snooping

Figure 4.1.1 A shows that DHCP Snooping has been configured and enabled on the following VLANs (10,20,30) ***ip dhcp snooping vlan 10,20,30***. I had marked the ***interface fa0/4*** connected to the legitimate DHCP server as the trusted connection ***ip dhcp snooping trust***, also initiating that the limit rate should be 5 packets at a time from untrusted interfaces ***ip dhcp snooping limit rate 5***, to reduce overload of packets which could lead to DDoS.

### 4.1.2 - ARP

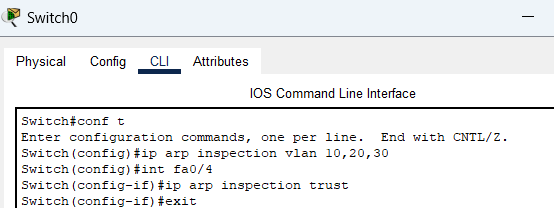


Figure 4.1.2 A - Protecting against ARP attacks

I have enabled Dynamic ARP inspection ***ip arp inspection trust*** to verify ARP packets against DHCP Spoofing.

### 4.1.3 - MAC

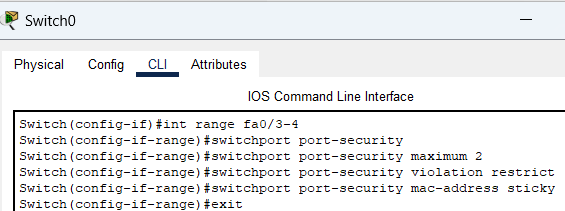


Figure 4.1.3 - Protecting against MAC attacks

I implemented these pre configurations to this switch as it has no ports open or interfaces assigned to it. I have done these pre config to essentially ensure that when devices are assigned to these ports they will already have port security activated on it.

### 4.3.1 - VLANs must be implemented to segment the network

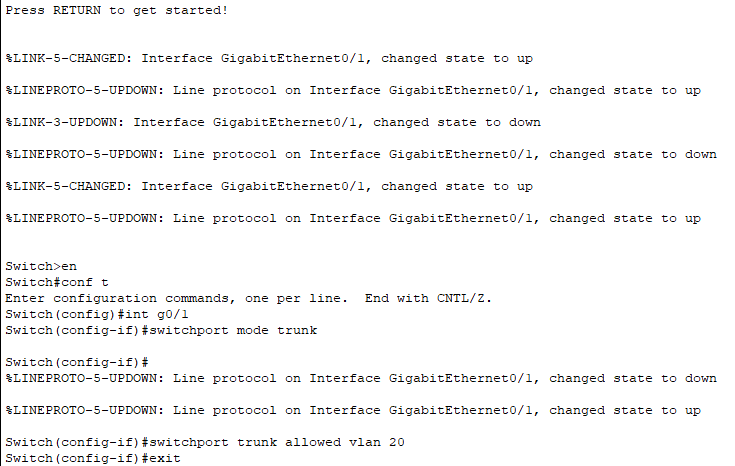
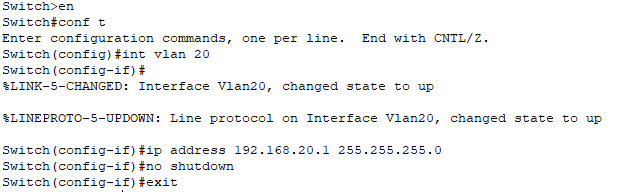


Figure 4.3.1 A - Assigning Ports for VLAN Trunking

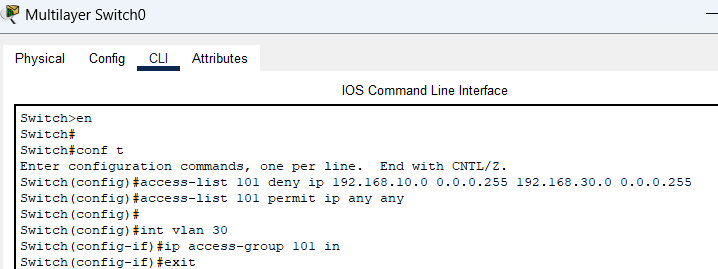
On each switch I had assigned a port that will be used for trunking ***int g0/1 | switchport mode trunk***. I have configured the switch in such a way that will control which VLAN will be permitted to pass through the designated trunk port. From a security perspective it restricts traffic for other VLANs other than VLAN 20 and only carries traffic specifically for VLAN 20. This ultimately reduces unnecessary traffic and improves security.

Figure 4.3.1 B - Configuring Inter-VLANs on Multi-layer Switches

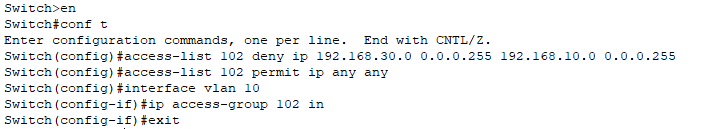
I have created a Switch Virtual Interface for VLAN 20 that provides connectivity for devices within the Specified VLAN. I had assigned the Default Gateway Address of ***192.168.20.1*** with a subnet mask of ***255.255.255.0 (/24)*** used for devices in VLAN 20 that need to communicate outside of VLAN 20.

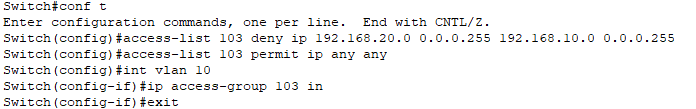
Here in these figures, I have configured the multilayer switches to have ACLs to control access between VLANs and restrict access.

Blocking VLAN 10 from accessing VLAN 30

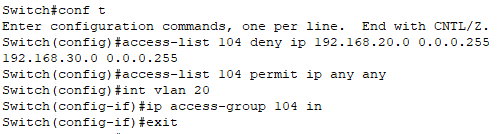


Blocking VLAN 30 from accessing VLAN 10:



Blocking VLAN 20 from accessing VLAN 10:

Blocking VLAN 20 from accessing VLAN 30:



Blocking VLAN 10 from accessing VLAN 20:

Blocking VLAN 30 from accessing VLAN 20:



### 4.4.1 - There must be a web application firewall to protect the web server

I decided to implement an access-list / firewall with specific rules to allow and block traffic to maintain security.

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (H) \***

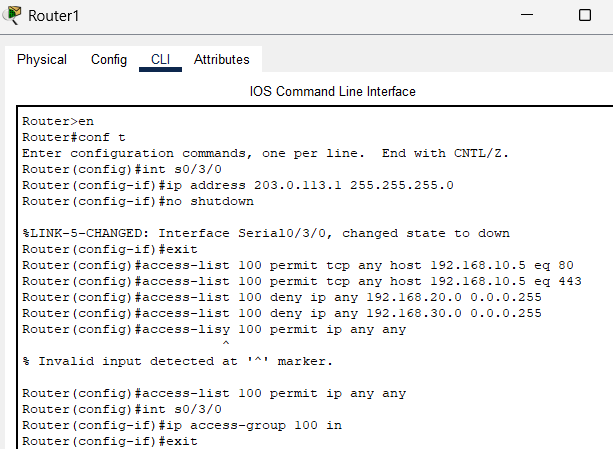


Figure 4.4.1 A - Firewall for Web server

In this figure above you can see that I had assigned an ***IP address*** of ***203.0.113.1*** to the ***interface S0/3/0*** as this is primarily used to test the network security. The subnet mask was ***/24*** which is ***255.255.255.0***

Then I had to configure a set of rules for the firewall on ***Router 1***. I allowed ***HTTP*** and ***HTTPS*** traffic to the web server ***(192.168.10.5) access-list 100 permit tcp any host 192.168.10.5 eq 80 & 443***.

I had then decided as a security professional to prevent any conflict between the internal network and other VLANs, I would block any traffic to the internal network, as the DMZ, according to the topology, is completely isolated from the internal network. ***Access-list 100 deny ip any 192.168.20.0 0.0.0.255 &192.168.30.0 0.0.0.255.***

Then I configured to permit all other outbound traffic ***access-list 100 permit ip any any***.

I proceeded to apply the access list to the external ***interface S0/3/0 ip access-group 100 in***

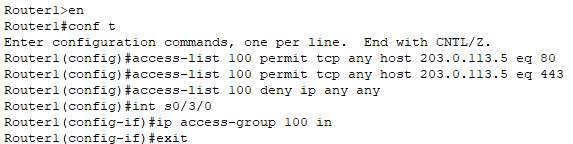


Figure 4.4.1 B - Access list to protect web server in DMZ

According to requirement 1.1.2 this figure show application security

This only permits HTTP(S) traffic ***access-list 100 permit tcp any host 203.0.113.5 eq 80 & 443***

***access-list 100 deny ip any any*** Blocks traffic to the web server from any external sources

### 5.2 - Implementation of IDS/IPS solutions



Figure 5.2 - IDS Configuration

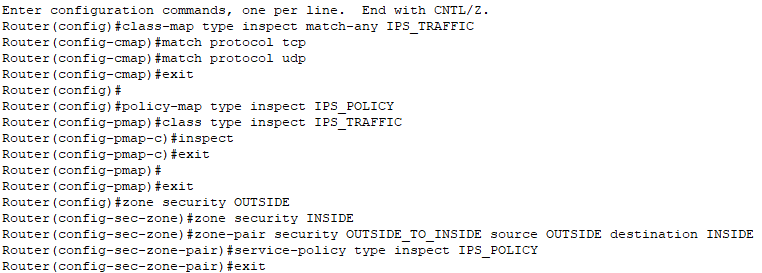


Figure 5.2 - IPS Configuration using Zone based policy firewall

Here two zones have been created ***INSIDE*** and ***OUTSIDE***

The zone pairs specify how the traffi*c flows between the* ***OUTSIDE*** *and* ***INSIDE*** *Zones* ***source OUTSIDE destination INSIDE***

The policy map dictates how the traffic is inspected within the flow

***Class map*** defines traffic to inspect

***Policy map*** applies rules to inspect the traffic

### 5.3.1 - Syslog Server must be implemented

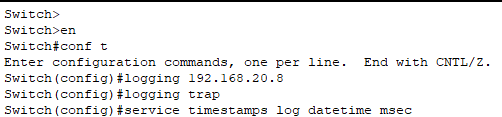


Figure 5.3.1 - Configuring Syslog server

According to requirement 5.3.1, a Syslog server must be implemented. In this figure you can see that the syslog server address 192.168.20.8 has been assigned to each switch. This is done so that all logs are monitored by a centralised syslog server to monitor any events and traffic on all of the devices integrated into the overall network.

**\* FOR MORE INFORMATION ON THIS, LOOK IN APPENDIX (I) \***

### 5.4.1 - NAT must be implemented on routers to hide private addresses from the internet

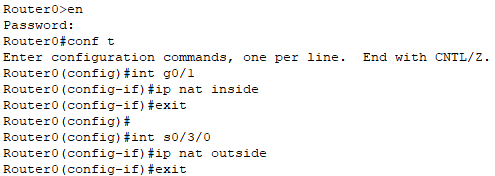


Figure 5.4.1 A - Configuring zones for interfaces



Figure 5.4.1 B - Configuring Static NAT



Figure 5.4.1 C - Configuring Dynamic NAT

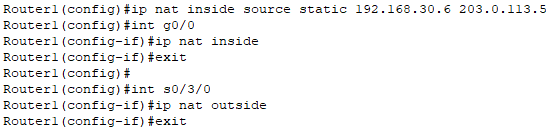


Figure 5.4.1 D - Configuring Static NAT for DMZ

# Secured Network Topology

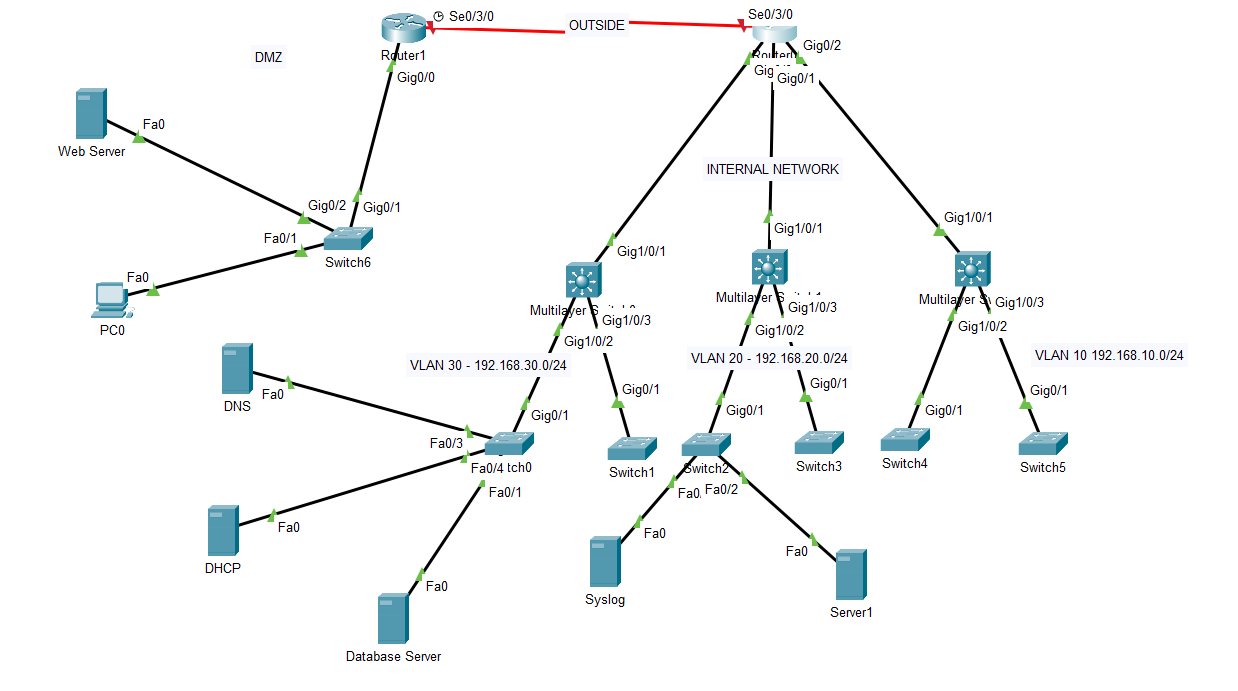


Figure 4

# Summary of Solutions & Conclusions

Overall I believe that the integration of these solutions shown, has really improved the networking security of our data center. I have maintained the overall core structure of the network but also with diligent research been able to implement and include more to the initial topology, increasing the level of security. This was just the first stages of development of this project, and we will be aiming to improve in the near future. This was completed by configuring:

Basic Security

Perimeter, Endpoint & Application Security

Identity-based & Role-based Access Control

Securing data at Rest & Transit

VLANs & Switch Security

Implementing Syslog

# Recommendations for further work

After being able to complete this project, I went on to take a further evaluation and analysis of the newly updated network topology from a security network security architecture perspective and realised there were still areas for improvement to tighten and security posture. Here are the following elements of recommendation:

1. Upgrading Syslog to SIEM - This can prove vital for the overall development of the business. Being able to configure SIEM into the network allows for more customers who want to host different systems to be integrated into the network and still have advanced real-time monitoring even if they have various different systems. According to Requirement 5.3.2, I recommended that SIEM must be implemented on the network.
2. Integrating Web Application firewalls (WAFs) - Due to Cisco Packet tracer not suitable to carry out this specific requirement 4.4, I deviated to just implement a normal Cisco firewall as a layer of defence for the web server. However, I do recommend in the future to implement Web application firewalls which are specified to block and permit traffic relevant to web servers. This is specified to detect against application threats (Layer 7 in OSI Model) WAFs provide targeted protection for web applications by filtering, monitoring, and blocking HTTP/S traffic. Web application firewalls can be used to protect against web specific attacks such as cross-site scripting and SQL injection.
3. Implementing OWASP and Threat Intelligence - As another security mechanism, implementing OWASP and other threat intelligence sources can enable the company to use a more proactive approach to prevent any attacks and breaches surfing the internet. OWASP, especially as we are host web services, lists the top 10 web application attacks around the world. Additionally we can implement Common Vulnerability Exposure, to see the most common vulnerabilities online and provide ways in which you can mitigate or prevent it from infecting our clients systems.
4. For Identity-based Access control policies - They could implement a RADIUS, LDAP or Active Directory, which can be used to verify who is trying to access resources and then assign the appropriate permissions based on their identity
5. Centralised configuration management system - To automatically push configurations to multiple devices
6. Patch management - To frequently update the operating systems on all endpoints to mitigate vulnerabilities

# Appendix

## Appendix A - PLAN

Analysis of current network topology will be done to assess the current security posture of our network. As our network will be versatile and scalable to customer demands, I will need to address various security measures for the different services that we are providing, also ensuring we provide sufficient security for the network. We will be addressing the following layers of security:

* I will also configure access lists and policies based on which users will be granted access to network devices.
* I will implement AAA and Parser views, for verification before access is fully granted. Users will have access based on roles and identity.

I will configure VLANs to split the overall network structure into smaller segments of the network. This is to isolate different services from each other. Also this will be configured in a way that completely isolates different segments from the network structure, if a device in a VLAN is compromised the attack span will be limited to that specific VLAN reducing risk of other services from being compromised or breached due to an attack.

## Appendix B

### Perimeter Security

According to Requirement 1.1.1, I will address the following aspects:

Security for the Web Server I will implement a Web Application Firewall (WAF). Policies will be set on the firewall to block specific ports and to protect web applications by filtering, monitoring and blocking malicious traffic that could compromise Web servers hosted by our clients.

As a layer of defence Internet facing Servers, will be isolated from the network and held in a DMZ. This separates these services from internal systems limiting reach of potential attacks. This is primarily implemented to not disrupt services provided to customers, if the internal network is under maintenance or compromised, affecting availability and violating the SLA Uptime Service Availability.

Network Segmentation in the form of VLANs are required to separate network structure based on data sensitivity (similar to DMZ), user roles and network functions. This can aid to contain an attack if one segment has been compromised, preventing the spread to other networks. Implementing microsegmentation permits the network architect to obtain granular control over traffic between servers and applications. In the case of our Data Centre each client will have their own VLANs and have the option to microsegment their services and systems hosted on our network.

Honeypots are a form of studying behavioural characteristics of attackers. We will implement this within the DMZ, copying the topology of the servers, and configuring meaningless or null values in those servers (dummy data). I have decided to implement this as stats show that attackers aim to breach internet facing services such as Web Server and DNS Servers (REF). This enables me and my network security team to observe how they behave when breaching a system and put mitigation factors in place on our legitimate servers to enhance our overall security posture.

Zero Trust Network Architecture enforces strict verification of for users and devices irrespective of their location, access level and Security Clearance. This is because zero trust doesn't trust any user on the network internally or remotely. Endpoint detection and response solutions will be used to monitor endpoints for suspicious behaviour. leading on from zero trust, insider threats have become so common over the years (REF) and implementing endpoint detection allows for a rapid response to potential breaches and compromised systems within the perimeter.

Physical Security Controls will be implemented at the core and perimeter of the data centre, through access controls like biometrics, bollards, badges, fences etc. to ensure only authorised personnel can access sensitive areas. We will also undergo 24/7 surveillance and monitoring to detect unauthorised physical access

### Access Control & Authentication

According to Requirement 2.0, I will need to implement access control lists and policies, to permit certain personnel to access systems and services. Access will be granted based on identity or roles.

### Data Protection & Encryption

According to Requirement 3.0, I will be addressing encryption techniques implemented to ensure data is kept safe in transit, at rest and when data is stored. This will be addressed using AES256 and when data is transmitted we will use TLS.

### Network Segmentation

According to requirement 4.3 and also requirement 1.1.1, I will be addressing microsegmentations in the form of VLANs. Essentially this will be implemented to isolate the various networks that we obtain via the number of customers we have and limit their access to only their company specific systems. This is done to prevent unauthorised security breaches and spread of malicious intent from an intruder on the overall network.

### Monitoring & Logging

According to Requirements 5.3, I will implement syslog servers for events monitoring and logging. This will be a centralised server which will be monitoring every device integrated into our network. SIEM will not be implemented due to some technical difficulties in the lab, but I will recommend that they implement it soon as it provides real-time security monitoring and can collect logs for different systems while syslog only has logs from specific systems.

### Compliance

When integrating the design of the network I will be correlating with the following compliance and regulatory legislations:

* NIST
* ISO 27001/2
* GDPR
* PII

## Appendix C - Initial Topology of Data Centre

* **1 Router** - For WAN connectivity, Operates at Layer 3 of OSI Model handling IP Addressing, Routing protocols and subnetting.
* **3 Distribution Layer Switches (DLS)** - Located between the router and access layer switches used to aggregate data from multiple access switches, forwarding traffic from access layer switches to core network and vice versa. Includes advanced routing and switching capabilities such as VLAN and load balancing.
* **6 Access Layer Switches (ALS) 2 per DLS** - Located at the LAN side of topology, used to connect end devices to network, in this case servers.
* **4 Servers (Web, DHCP, DNS and Database)** - Initiate traffic to the core of the network and other devices requesting to use service.

## Appendix D - Basic Security

Configuring a DHCP Server (192.168.30.3), limiting address range to 118 available hosts /25 subnets. As a network architect limiting IP addresses is essential as we will only be hosting for 100 customers meaning there would be 18 addresses left over. Our services are also scalable so therefore if there is more demand from customers we can increase the range of ip addresses allocated by the DHCP.

Subnetting helps logically separate network segments, to improve network management security. /25 enables for 126 usable addresses excluding network and broadcast. In this case I have allocated an address range from 192.168.30.3 (DHCP) - 192.168.30.9 to all servers implemented in this network design. They will be statically configured as their addresses should remain consistent, ensuring users, applications and network devices can connect reliably. Security protocols, firewalls, and access controls can be better configured with static IPs. For example, network policies and access rules often use specific IP addresses for whitelisting and other access controls.

## Appendix E - Perimeter Security

I have configured access lists to prevent conflict between these VLANs.Each VLAN has been configured to block any access coming from another VLAN. For instance here in Figure 1.1.1, you can see I have configured VLAN 20 to block any access to the network from VLAN 30. This has been implemented so that other customers cannot access unauthorised services of another customer, and also to reduce the impact of a security breach on the network by isolating and segmenting overall network structure. An example of this is if an attacker has compromised the DNS Server of one customer via DDoS, it will only affect that customer's services instead of the whole network.

## Appendix F - Identity-based access control

In figure 2.1.1 A ***privilege level 15*** has been configured with a ***password*** of ***francisb03***. This user (Network Security Agent) has level 15 privilege and root user views meaning they have the ability to modify and configure new views and add or remove commands from the views.

## Appendix G - Data in transit

This figure show the configuration of a secured syslog server (192.168.20.8). This is beneficial for data at rest as it ensure the confidentiality, integrity and authenticity of logs when stored on syslog server. Maintaining logs are extremely essential for observing network and user behaviour to be vital in a forensic investigation. Ensuring logs are kept secured at rest and aren't tampered with gives accurate readings when analysing and monitoring events on the network. These can be used to prevent malicious attacks as they can be spotted and mitigated or prevented before severity escalates.

(Additional Information) SSH protect data in transit by:

ensuring all data over the network is encrypted, including commands and files. This prevents unauthorised users from intercepting data (MiTM)

Requires secured authentication methods such as passwords and public/private key pairs, before a connectivity is established, permitting authorised users to access the communication channel.

SSH also ensures the integrity of data used is maintained via the usage of cryptographic hash functions

SSH also creates a secure tunnel for other protocols such as SFTP and less secured protocols like Telnet to protect data in transit.

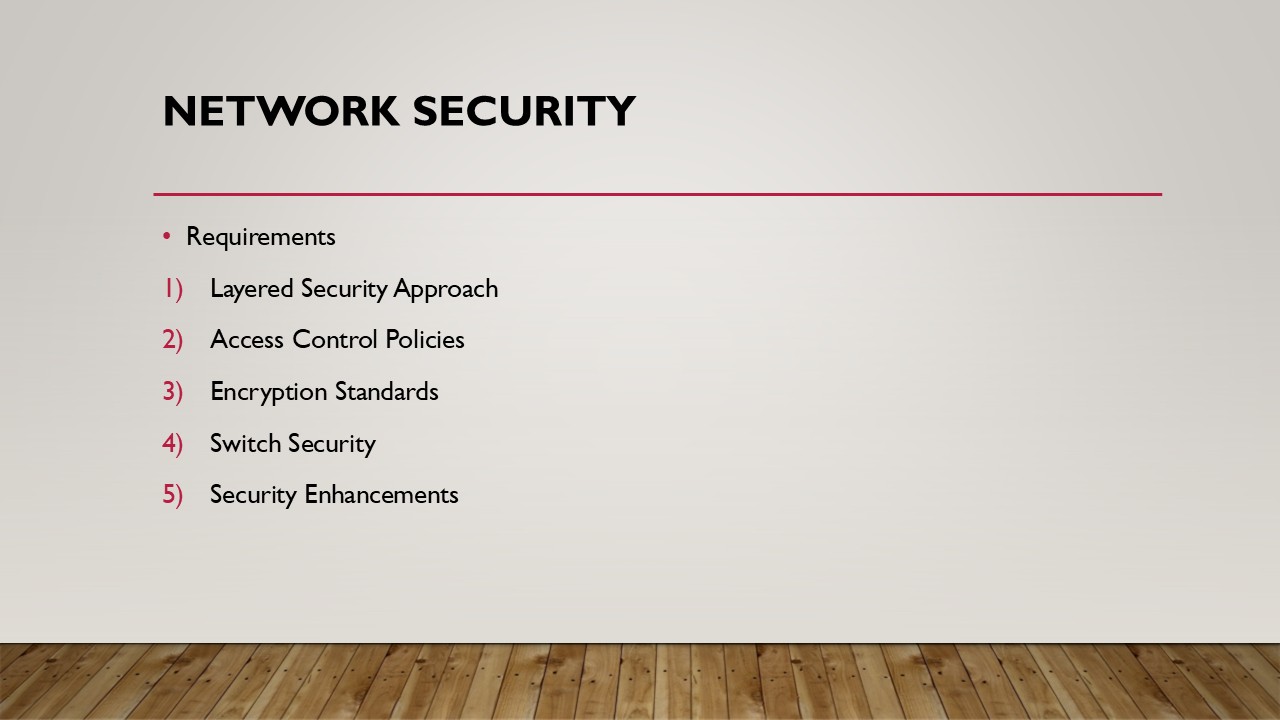
## Appendix H - There must be a web application firewall to protect the web server

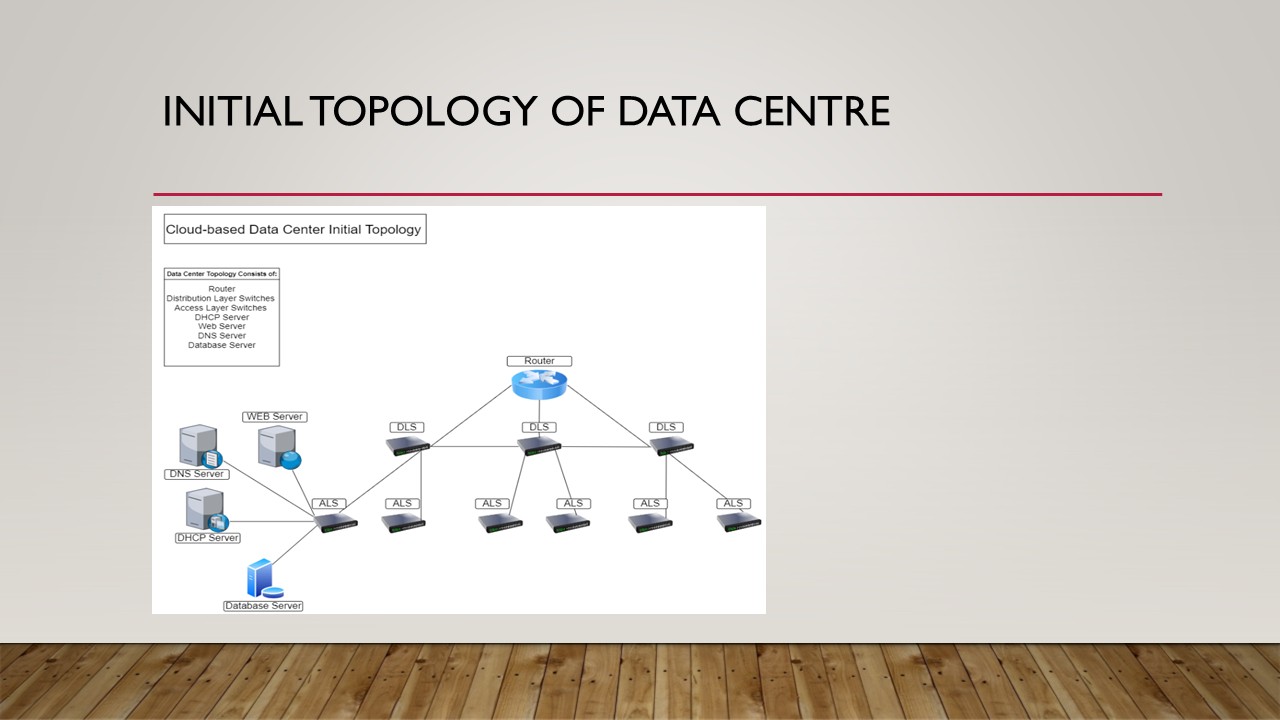
Cisco packet tracer did not allow me to create a Web Application Firewall, so I have added that to further work and recommendations section which could be implemented later on using different platforms and tools. Instead I decided to implement an access-list / firewall with specific rules to allow and block specific traffic to maintain security and integrity of the web server within the DMZ.

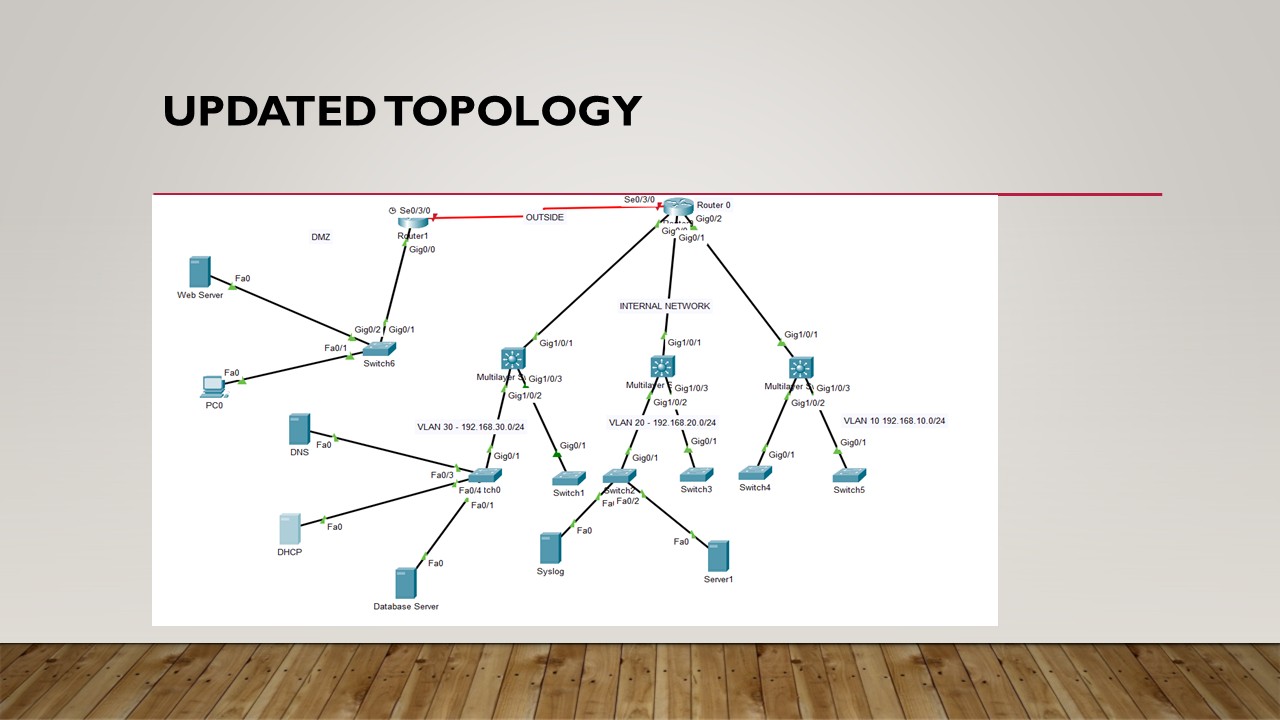
## Appendix I - Syslog Server must be implemented

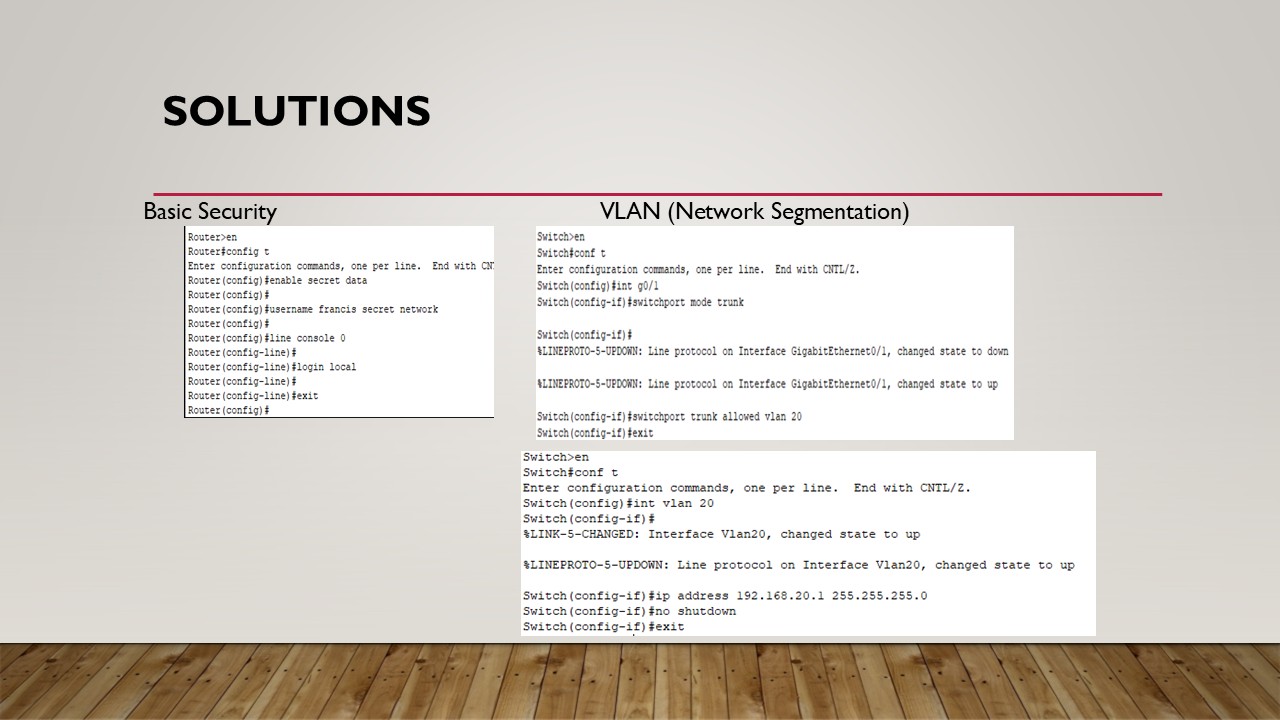
According to requirement 5.3.1, a Syslog server must be implemented. In this figure you can see that the syslog server address 192.168.20.8 has been assigned to each switch. This is done so that all logs are monitored by a centralised syslog server to monitor any events and traffic on all of the devices integrated into the overall network. This configuration was completed on each of the switches, an external syslog server was assigned for the DMZ as I have designed the network in such a way that the DMZ has no direct connection with the internal network. Syslog is much more secure than TLS.

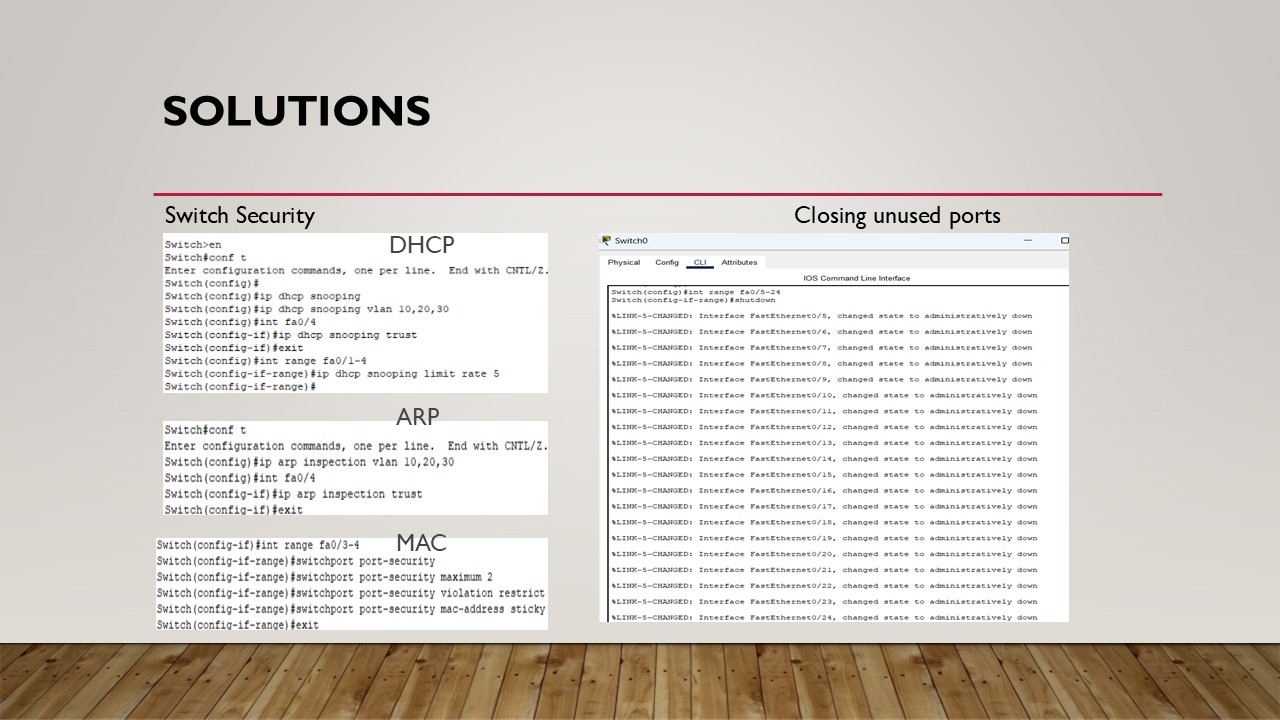
# Supporting Evidence

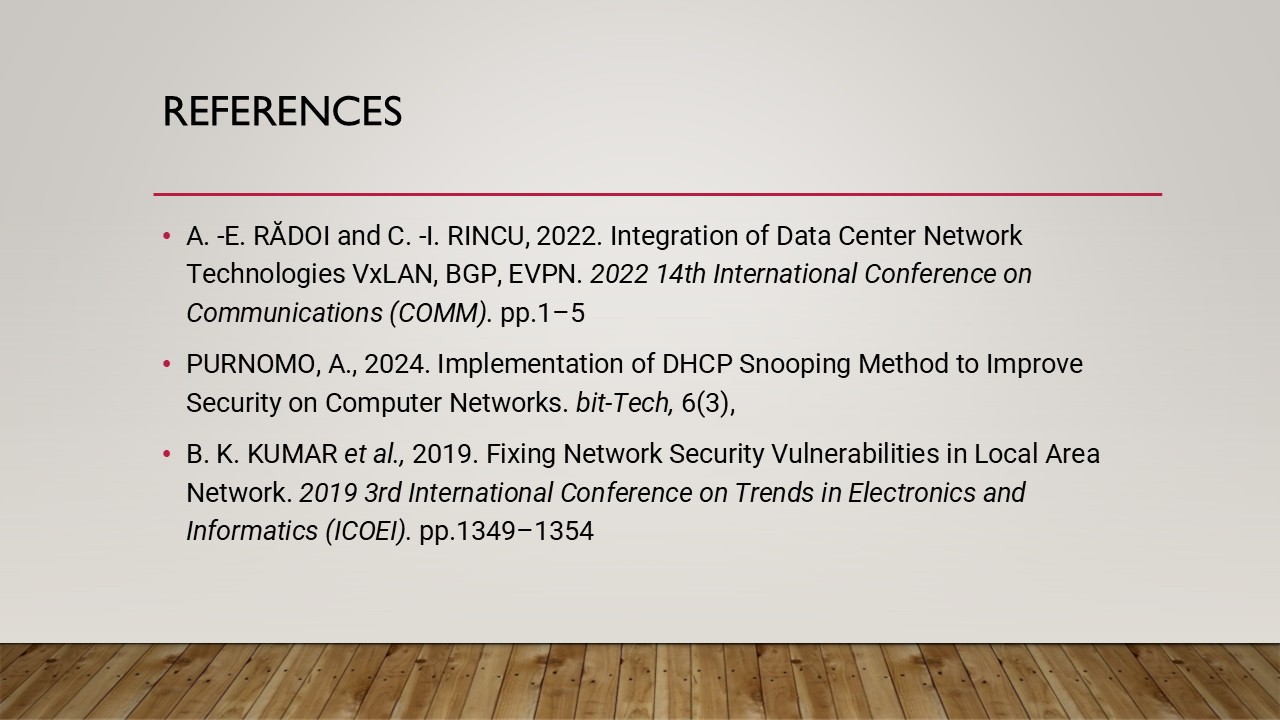












# 