Secure Network Design

By: Antonio, Jessica, Steve, Tommy, Alexys

Summary

1 Introduction

2 Team Member Roles

3 Project Goals

4 Project Constraints & Requirements

5 Network Design Overview

6 IP Addressing and VLANs

7 Core Security Principles

8 DMZ Design and Purpose

9 Access Control List (ACL)

10 RADIUS Authentication

11 Estimated Hardware Budget

Introduction

This project simulates the implementation of a complete network redesign for a growing company setting up a new office.

The design is developed in alignment with the client's goals and constraints, ensuring all specified criteria are met.

Key priorities include security, scalability, and cost-effectiveness.

Team members roles

Team Leader: Steve
Responsible for setting up Trello, managing deadlines, overseeing final deliverables, and providing support across both teams.

Blue Team (Jessica & Tommy) – Topology and Connectivity
Tasks include designing the network topology, configuring VLANs, IP addressing, routers, and servers.

Green Team (Antonio & Alexys) – Security and Documentation
Responsible for developing the IP addressing table, creating documentation and presentation slides, and selecting appropriate hardware.

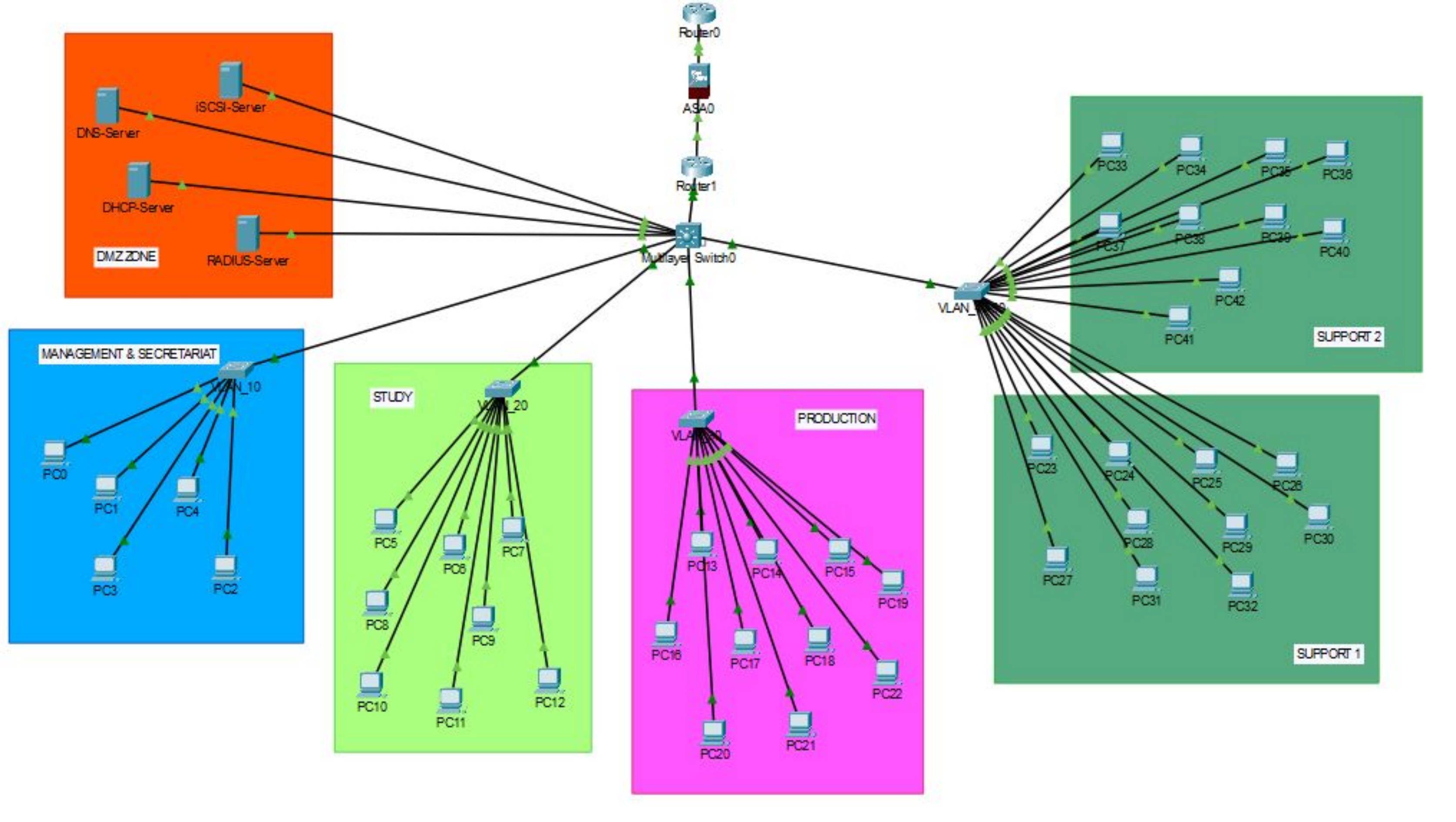
Project Goals

- **Design a secure and modern network**
- **Simulate a network design (GNS3 / Packet Tracer)**
- **Ensure strong security**
- **Create detailed documentation**
- **Demonstrate and justify Design Choices**
- **Ensure network functionality**

Project Constraints / Requirement

- Project deadline: 7 days
- Simulation tools: (GNS3 or Pka)
- Must include (DNS Server, DHCP server, DMZ concept with Vlan configuration and ACLs and ISCSI storage server)
- Centralized authentication via RADIUS server
- GNS3 (Packet tracer) Simulation and documentation reports
- 5 Departments: Management, Study, Production, Support A & B

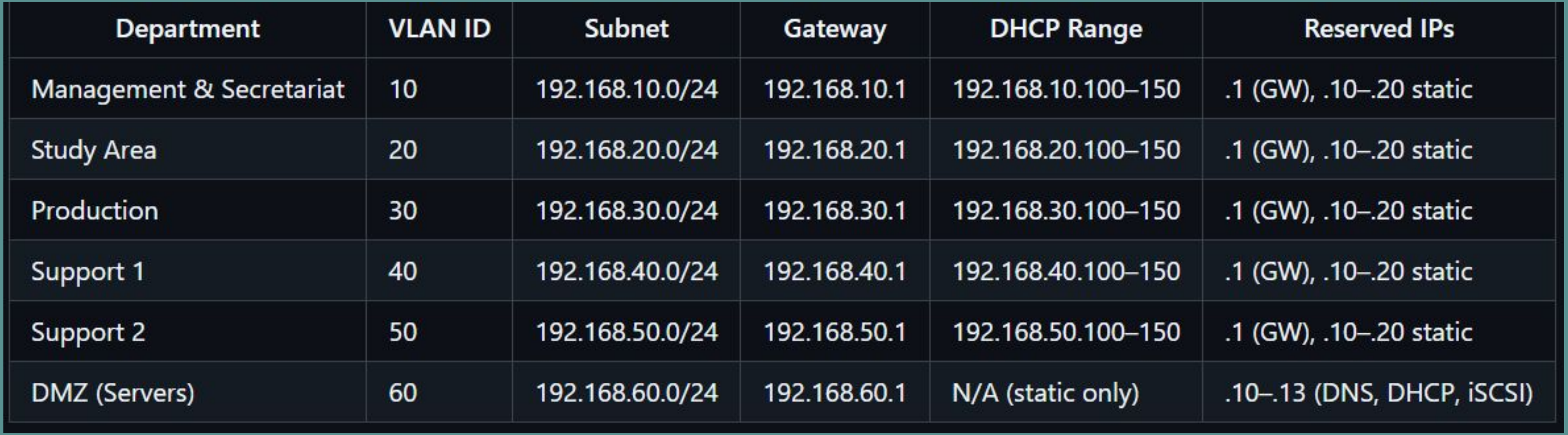
Network design Overview



Network design Overview

- 6 VLAN : 5 INTERNAL + 1 DMZ
- Inter-Vlan routing and ACLs on Layer 3 devices
- ALL Servers placed in a secured DMZ VLAN
- ISCSI access restricted to management only

IP Addressing & Vlans



Department	VLAN ID	Subnet	Gateway	DHCP Range	Reserved IPs
Management & Secretariat	10	192.168.10.0/24	192.168.10.1	192.168.10.100–150	.1 (GW), .10–.20 static
Study Area	20	192.168.20.0/24	192.168.20.1	192.168.20.100–150	.1 (GW), .10–.20 static
Production	30	192.168.30.0/24	192.168.30.1	192.168.30.100–150	.1 (GW), .10–.20 static
Support 1	40	192.168.40.0/24	192.168.40.1	192.168.40.100–150	.1 (GW), .10–.20 static
Support 2	50	192.168.50.0/24	192.168.50.1	192.168.50.100–150	.1 (GW), .10–.20 static
DMZ (Servers)	60	192.168.60.0/24	192.168.60.1	N/A (static only)	.10–.13 (DNS, DHCP, iSCSI)

Core security principales

- DMZ VLAN for exposed infrastructure
- VLAN segmentation to isolate departments
- ACLs to strictly control inter-Vlan traffic
- Statics IP for all critical assets
- Future-proofing with centralized RADIUS

DMZ Design & purpose

- VLAN 60 contains all core servers
- Acts as a buffer between users & VlANs and infrastructure
- Limited access via ACLs:
  - DNS / DHCP available to all
  - ISCSI available to only management
- Increases control & reduces attack surface
- Future-proofing with centralized RADIUS

Access Control list (ACLs)

- All traffic denied by default
- Allows DNS (UDP 53), DHCP, ISCSI as needed
- No lateral access between user VLANs
- Tested via ping/dns resolution between VLANs

RADIUS Authentication

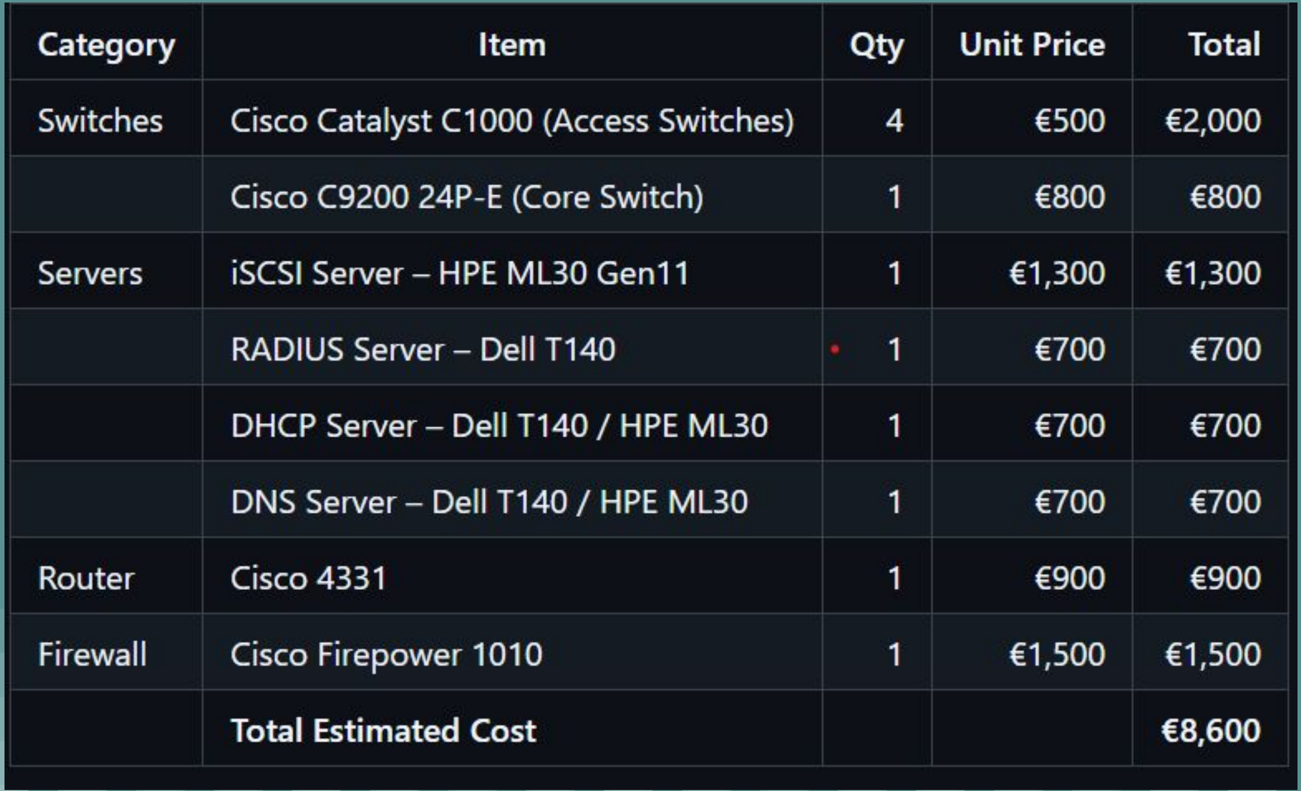
- RADIUS (Remote Authentication Dial-In User Service) provides centralized authentication for network devices
- Configured on switches/routers for both console and VTY (ssh/Telnet) access

RADIUS Authentication

Ensures:

- Secure admin login with user/password
- centralized control of credentials
- Auditing of login attempts
- Reduces risk from weak or local-only credentials

Estimated Hardware Budget



Category	Item	Qty	Unit Price	Total
Switches	Cisco Catalyst C1000 (Access Switches)	4	€500	€2,000
	Cisco C9200 24P-E (Core Switch)	1	€800	€800
Servers	iSCSI Server – HPE ML30 Gen11	1	€1,300	€1,300
	RADIUS Server – Dell T140	1	€700	€700
	DHCP Server – Dell T140 / HPE ML30	1	€700	€700
	DNS Server – Dell T140 / HPE ML30	1	€700	€700
Router	Cisco 4331	1	€900	€900
Firewall	Cisco Firepower 1010	1	€1,500	€1,500
	Total Estimated Cost			**€8,600**

Estimated Hardware Budget

- **Consider Refurbished Hardware: Mid range servers and network devices are often available at 60% to 80% discounts in the refurbished market**

- **While choosing the right device budget and functionality wise, we made sure to choose non End of life or End of services hardware that could be a security hazard.**

- **Where the estimated retail price for the budget is *€8,600* , the use of refurbished hardware could decrease the price to *€3,000***