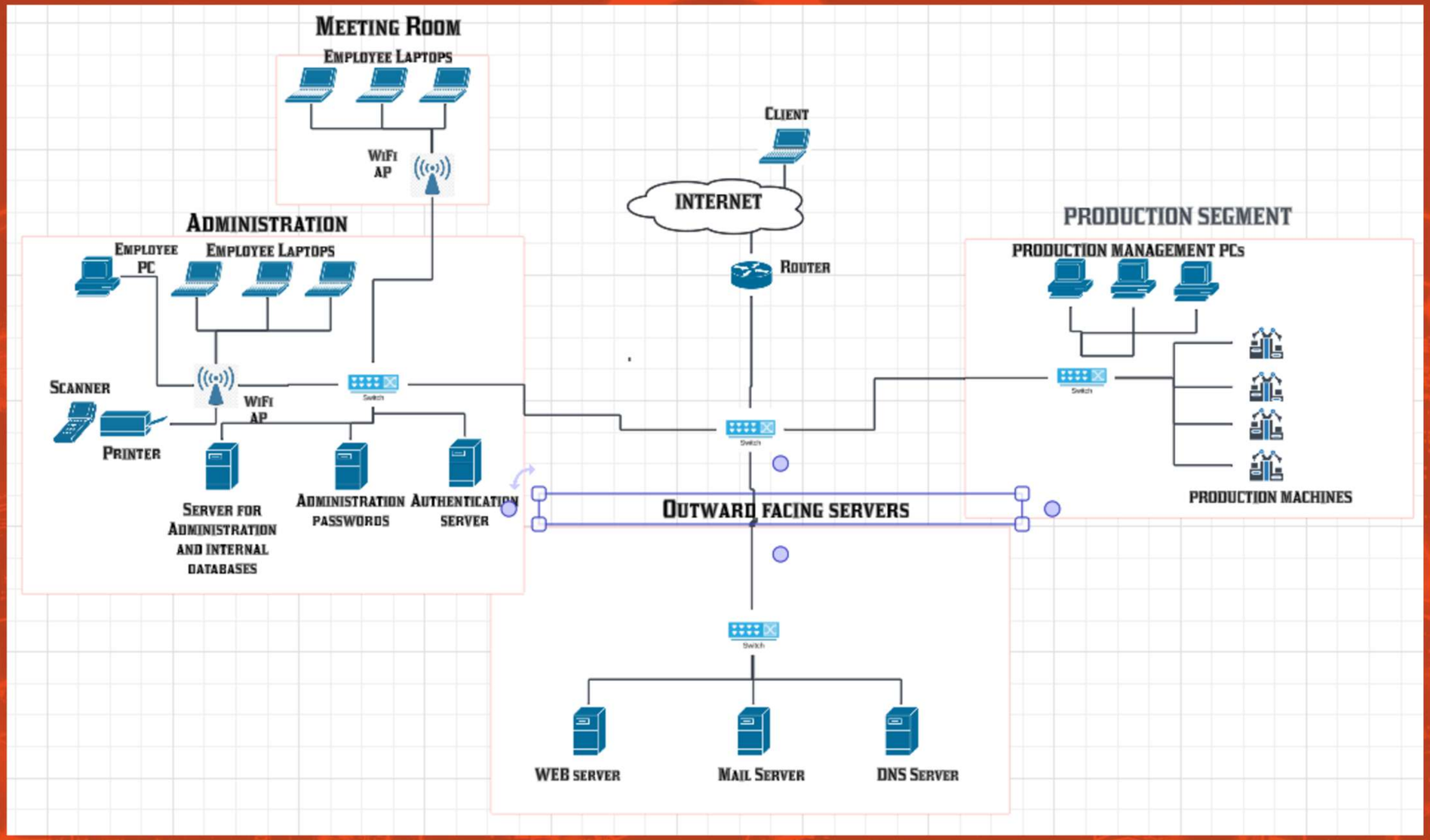
FIT1047 PART 2B

# ASSIGNMENT 4

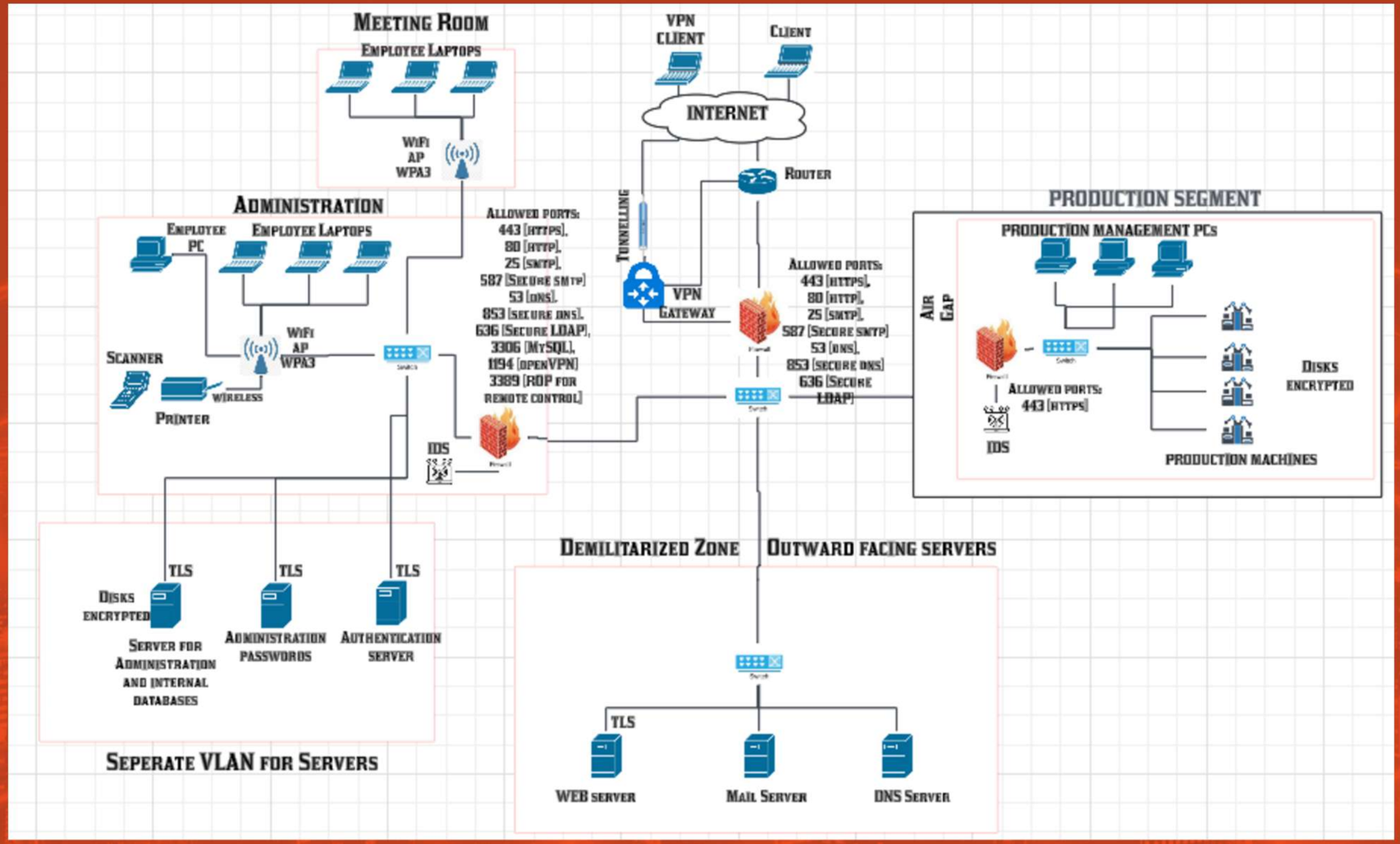
BY AMAN KARUKAPPADATH NISHAD
ID: 35087773

# INDEX

# NETWORK


MEETING ROOM
EMPLOYEE LAPTOPS
WIFI AP
CLIENT
INTERNET
ROUTER
ADMINISTRATION
EMPLOYEE PC
EMPLOYEE LAPTOPS
SCANNER
WIFI AP
PRINTER
SERVER FOR ADMINISTRATION AND INTERNAL DATABASES
ADMINISTRATION PASSWORDS
AUTHENTICATION SERVER
PRODUCTION SEGMENT
PRODUCTION MANAGEMENT PCS
PRODUCTION MACHINES
OUTWARD FACING SERVERS
WEB SERVER
MAIL SERVER
DNS SERVER

# NETWORK WITH SECURITY

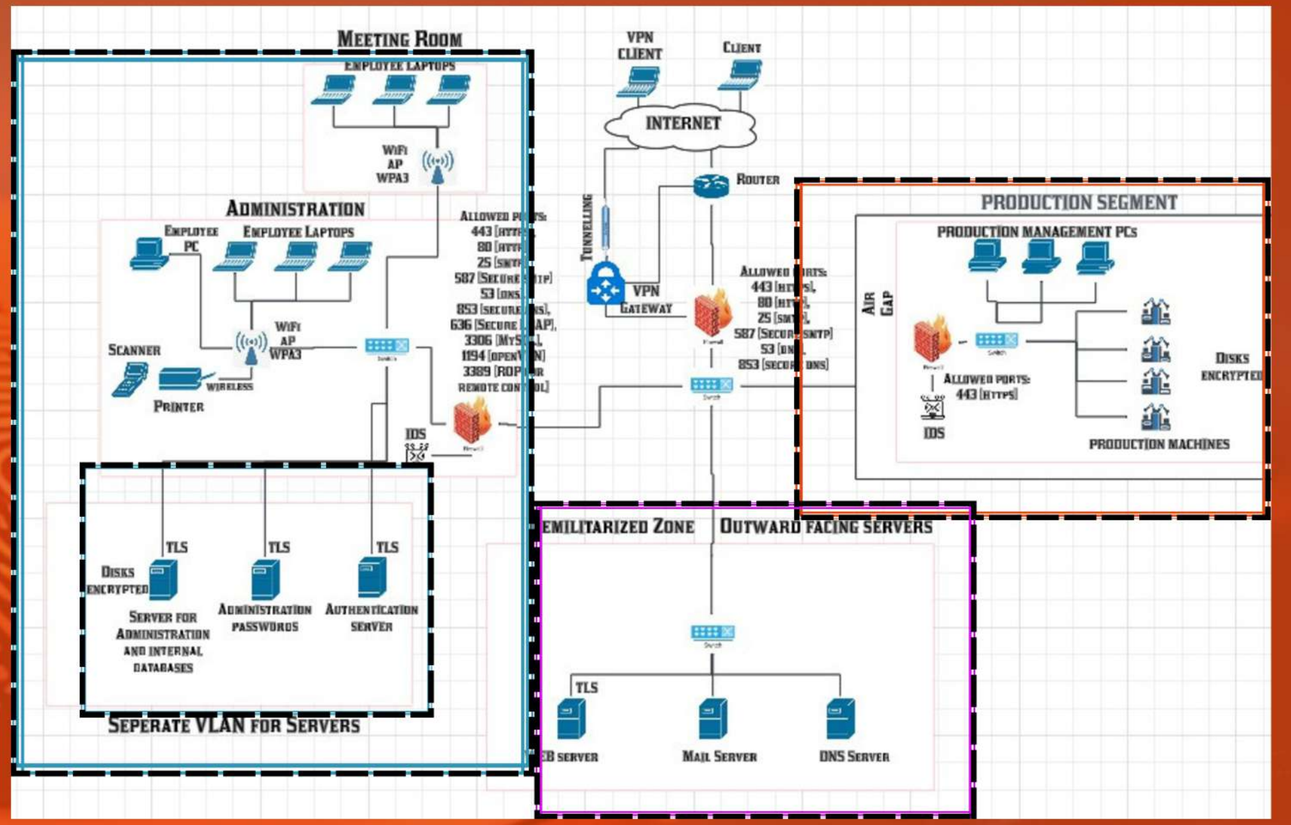


# VLANS & SEGMENTATION

The network uses three main VLANs: Administration (servers and office equipment), DMZ (outward-facing servers), and Production (manufacturing systems) – each separated for enhanced security.

Also a serperate VLAN is kept for the servers in administration as followed from the NIST framework of best practices

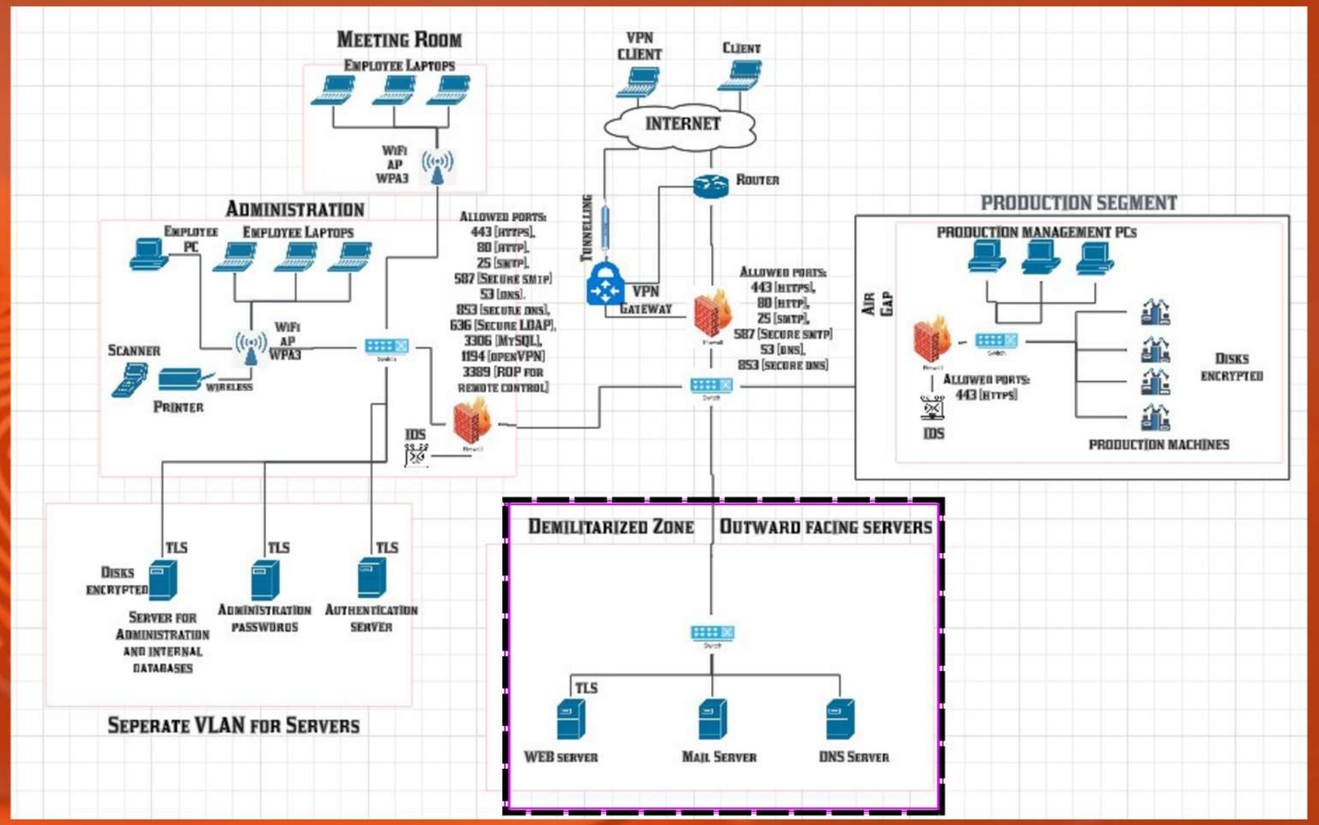
Reduces the risk of internal threats spreading across segments. Strengthening this setup with access controls can prevent unauthorized internal access.



# DEMILITARIZED ZONE

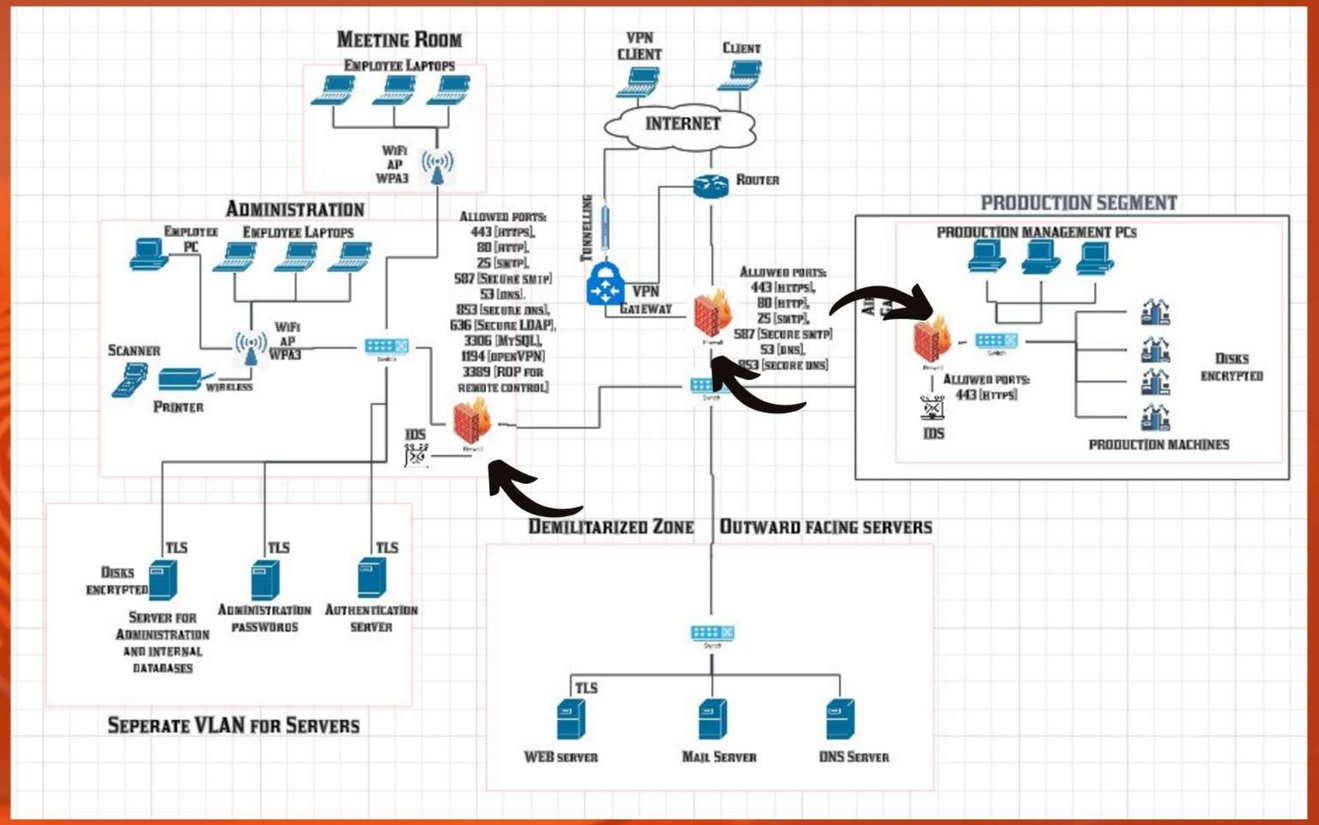
The DMZ hosts public servers for external users, isolating them from the internal network to reduce security risks.

A DMZ is a network segment that allows external access to public services while protecting the internal network from direct exposure.



# FIREWALL

A firewall acts as a protective barrier that monitors and controls network traffic, allowing safe communications within your organization while defending against threats from the outside internet.



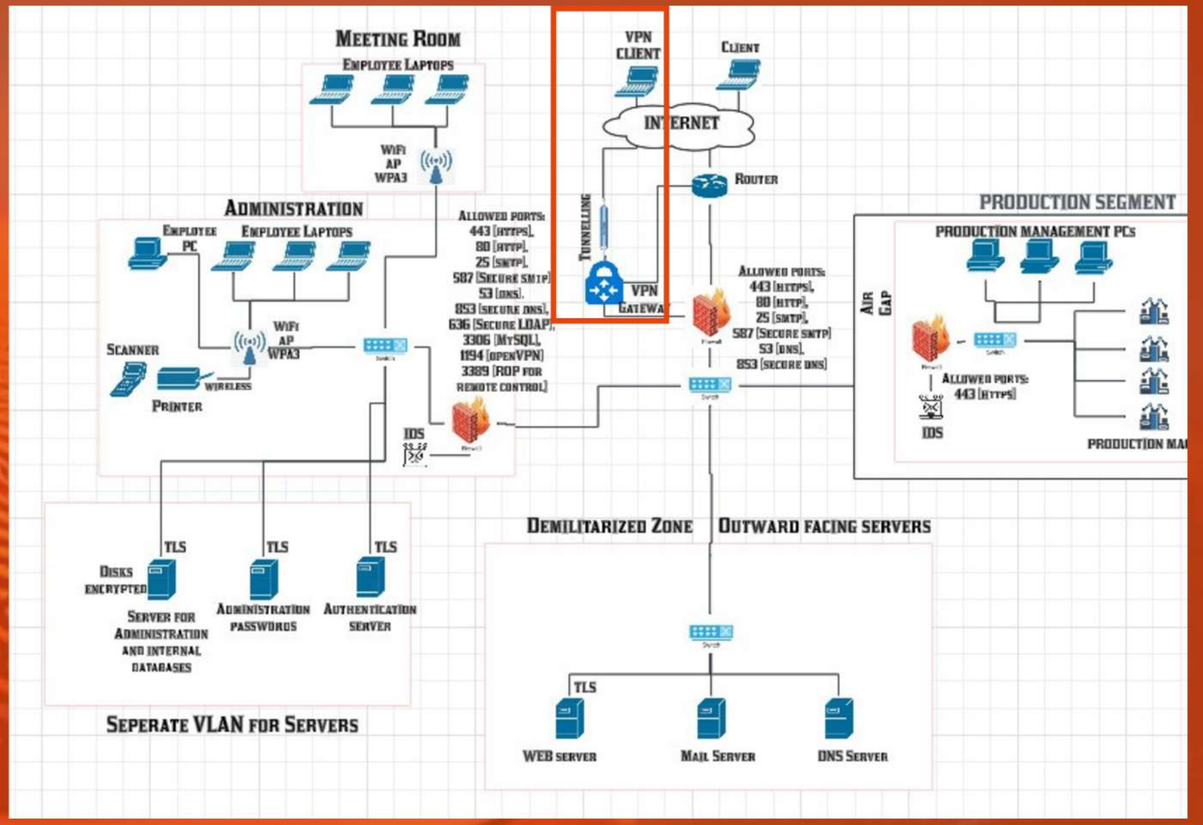

## Firewalls used:

- Perimeter Firewall
- Administration Firewall
- Production Firewall
- DMZ firewall (Perimeter Firewall)

# VPN CLIENT & GATEWAY

**VPN Client: "Software/Device that creates an encrypted connection between your device and your organization's network, ensuring secure remote access."**

**VPN Gateway: "The secure entry point that verifies remote connections and manages access to an organization's network resources."**

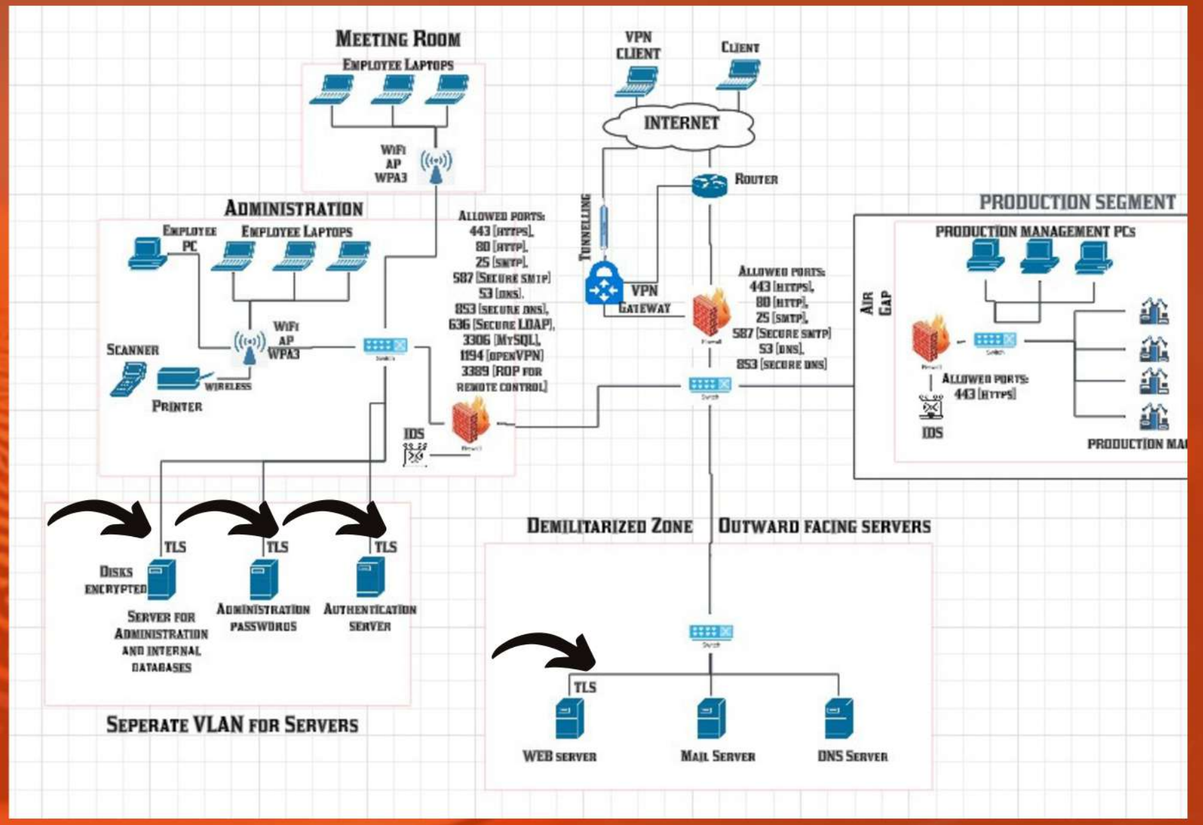


# TRANSPORT LAYER SECURITY [TLS]

Web Server in the DMZ: TLS secures connections between external users and the web server, encrypting data in transit to prevent interception and ensuring a secure connection.

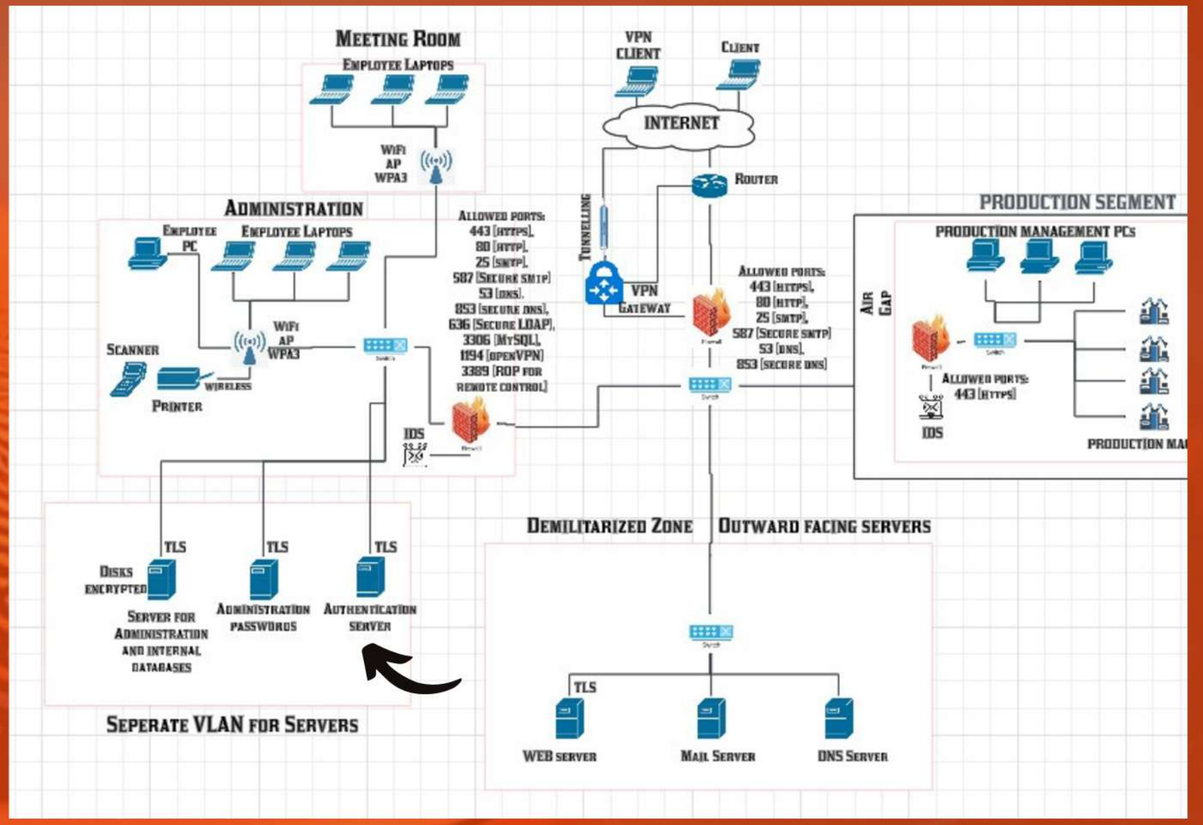
Internal Administration and Production Segments: TLS can secure data exchanged between sensitive systems, such as between the authentication server and user devices, to protect login credentials and other internal database content etc

Ensures data confidentiality, protecting sensitive information from insider threats.



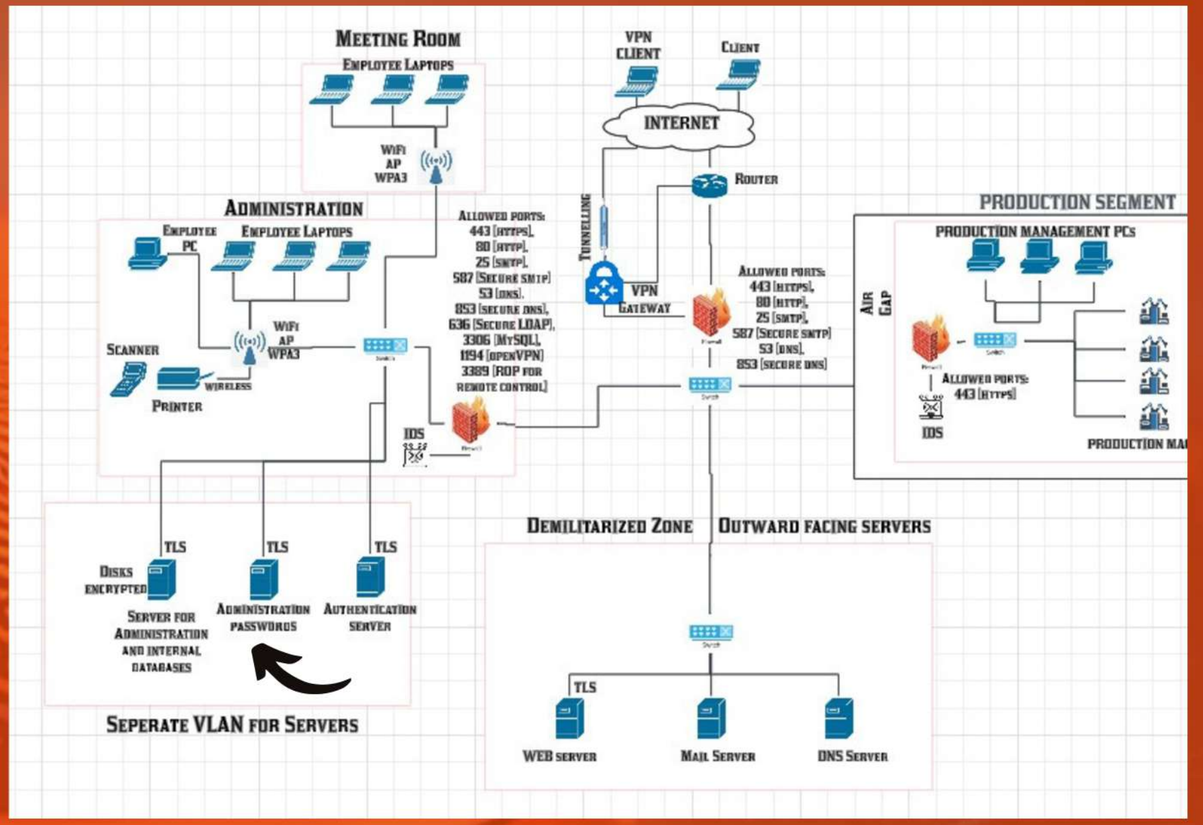
# AUTHENTICATION SERVER

The authentication server is the network's security guard – it checks and verifies user identities before granting them access to sensitive resources. Using standard security protocols, it ensures only authorized users can enter specific network areas, acting as a central checkpoint for all access requests.



# SECURE SEEDED STORAGE OF PASSWORDS

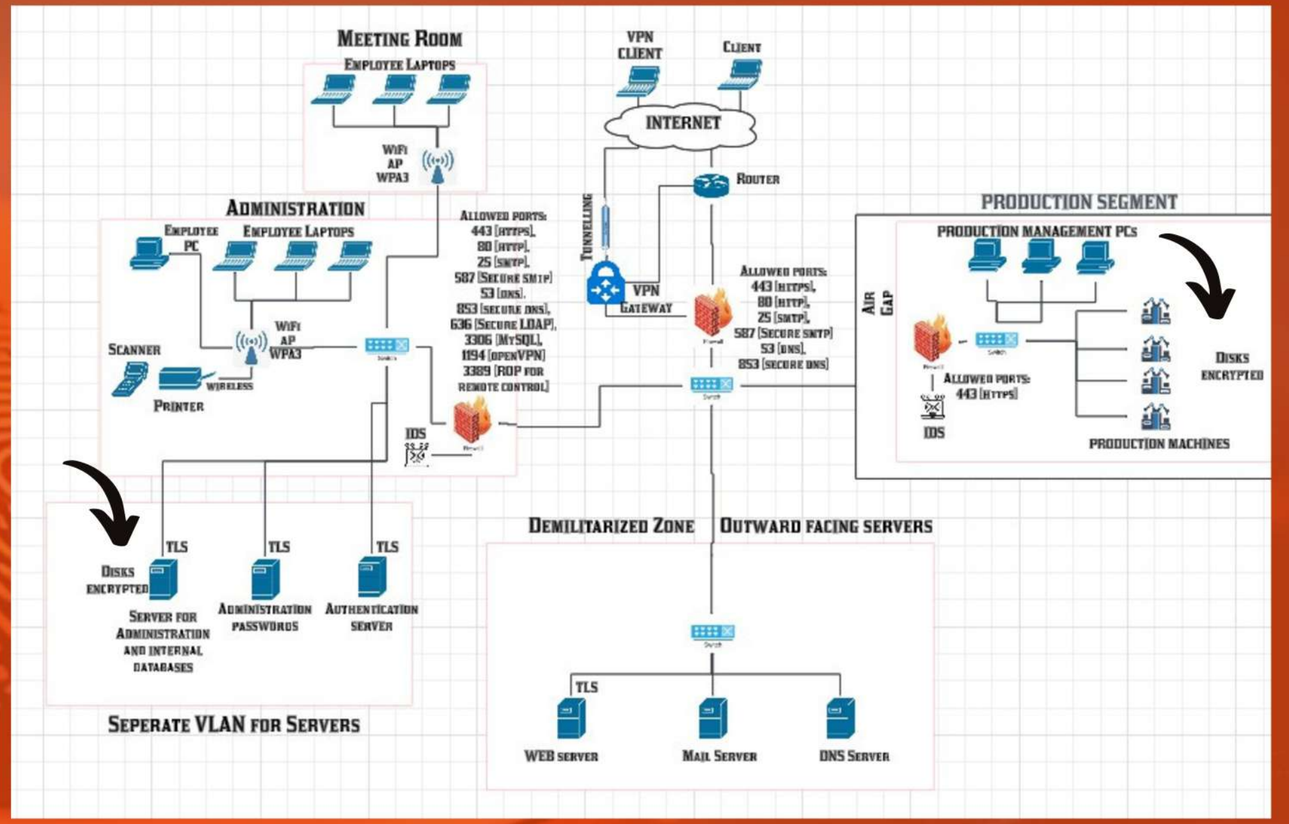
The administration passwords server protects user passwords through encryption techniques like hashing and salting, safeguarding access to sensitive network areas. This security is vital since compromised passwords could give attackers full network access.



# DISK ENCRYPTION

Disk encryption protects stored data on your database and production servers, making it unreadable without proper authentication.

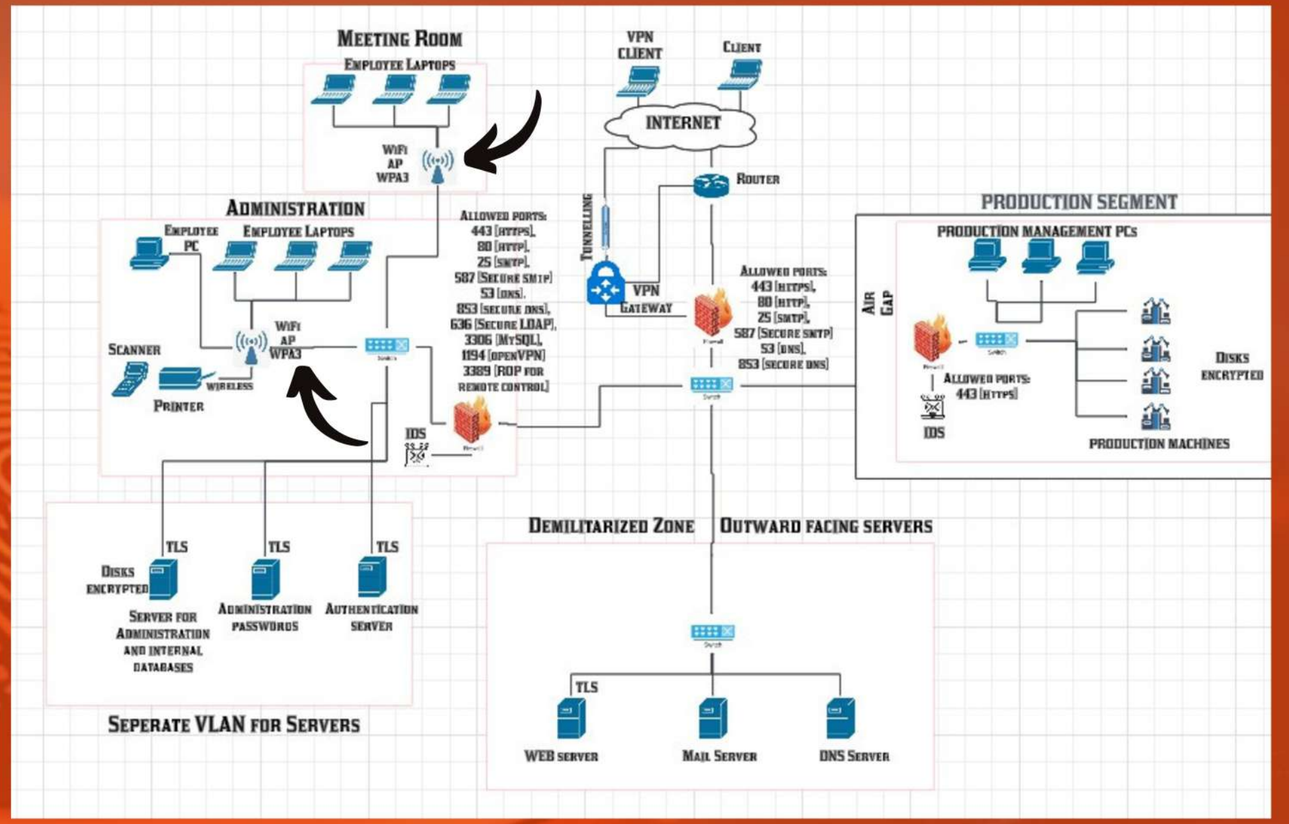
A security measure that converts stored data into encrypted code, ensuring only authorized users with decryption keys can access sensitive information.



# WPA3 ENCRYPTION

In the network, WPA3 secures the wireless connections in the Meeting Room and Administration areas, protecting data transmitted between laptops and WiFi access points.

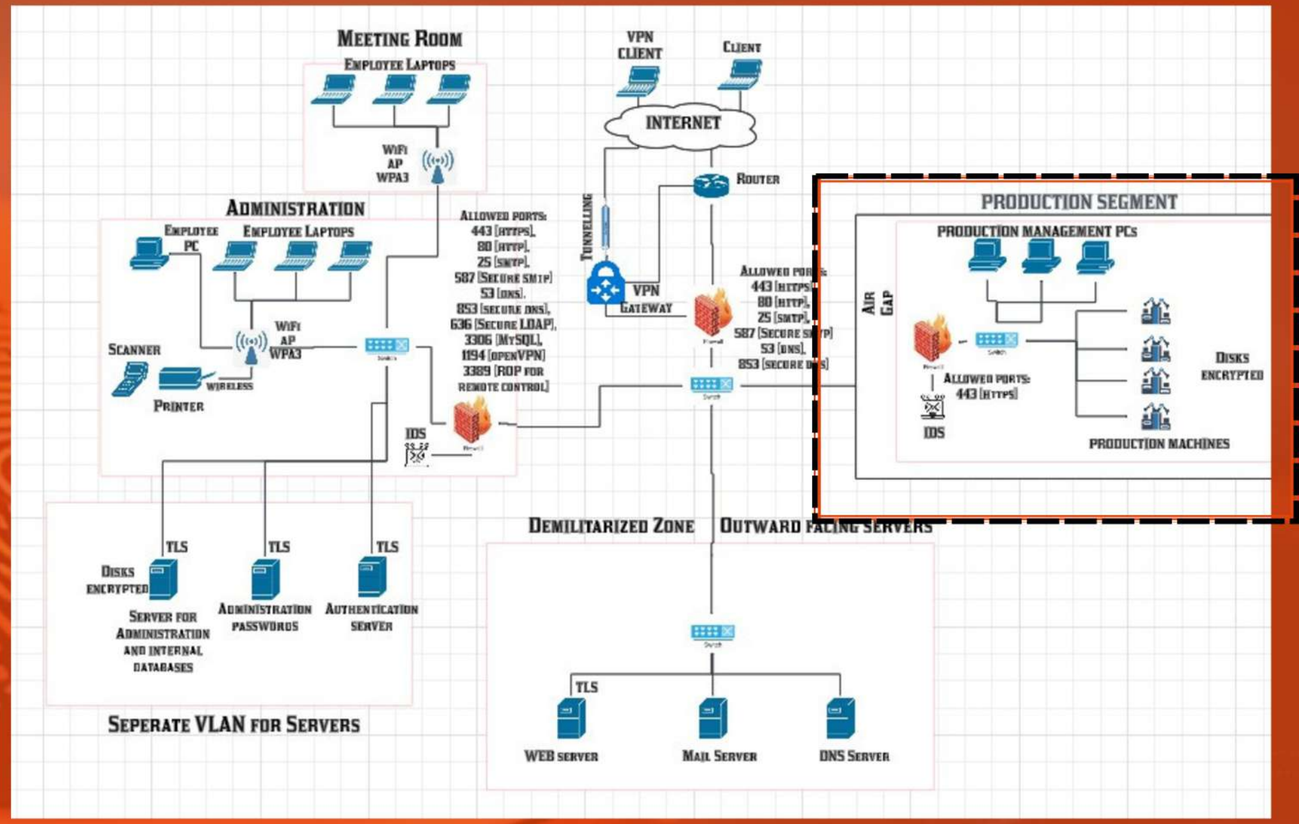
WPA3 is the latest WiFi security protocol that provides stronger encryption and protection against password-guessing attacks, making wireless networks significantly harder to hack.



# AIR GAPS

In the network, the air gap physically isolates the Production Segment from other network areas, preventing any unauthorized data flow or cyber attacks from reaching critical production machines.

An air gap is a security measure that physically disconnects a network or system from all other networks, including the internet, creating an uncrossable security barrier.

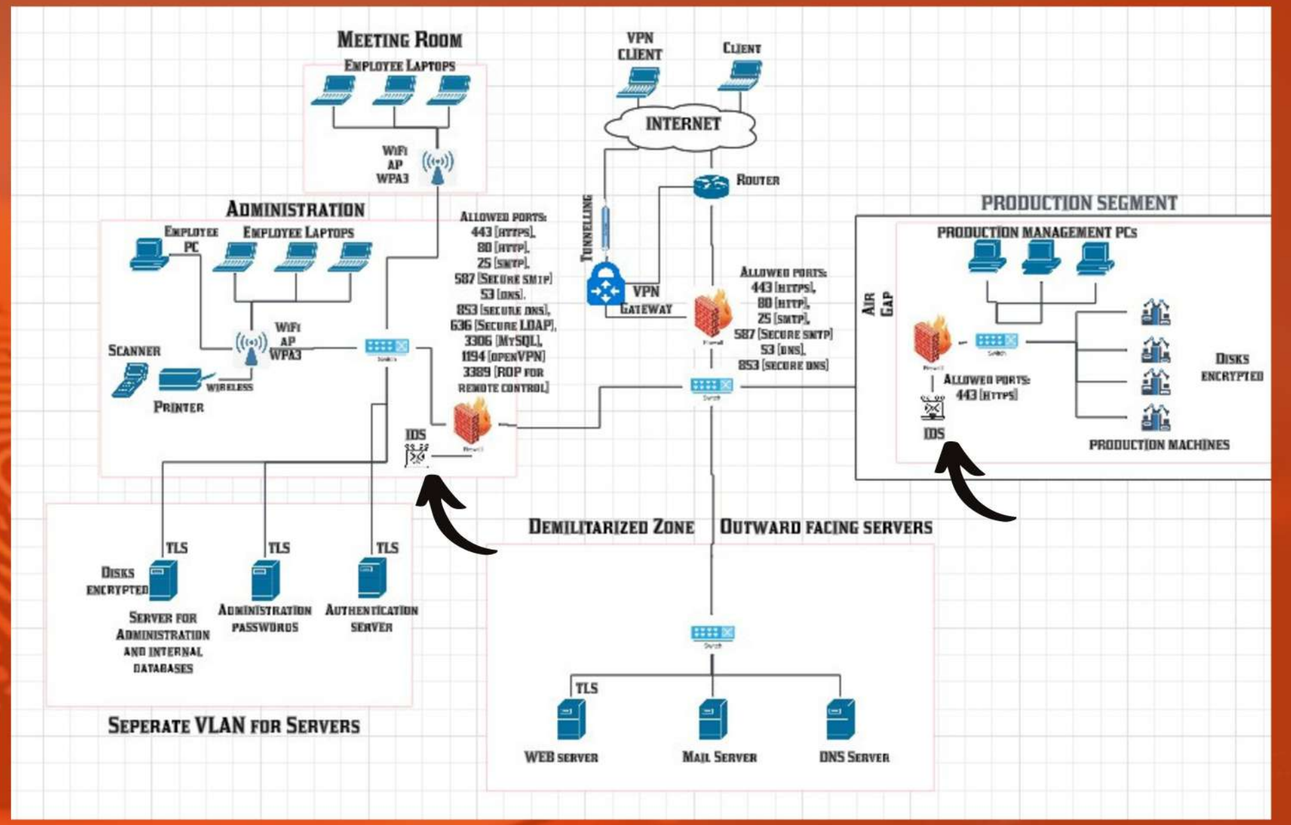


# INTRUSION DETECTION SYSTEM

In the network, IDS monitors traffic at key points – between internet and internal networks, and before the Production Segment – alerting when suspicious activities or potential attacks take place.

An IDS is a security tool that constantly watches network traffic for suspicious patterns or behaviors, acting like a security camera for your network data.

The Administration segment has an IDS, which can monitor traffic and detect suspicious activities. If configured properly, this IDS can serve as an internal threat detection tool by alerting on unusual patterns from internal sources.




THANK
YOU.

# REFERENCES

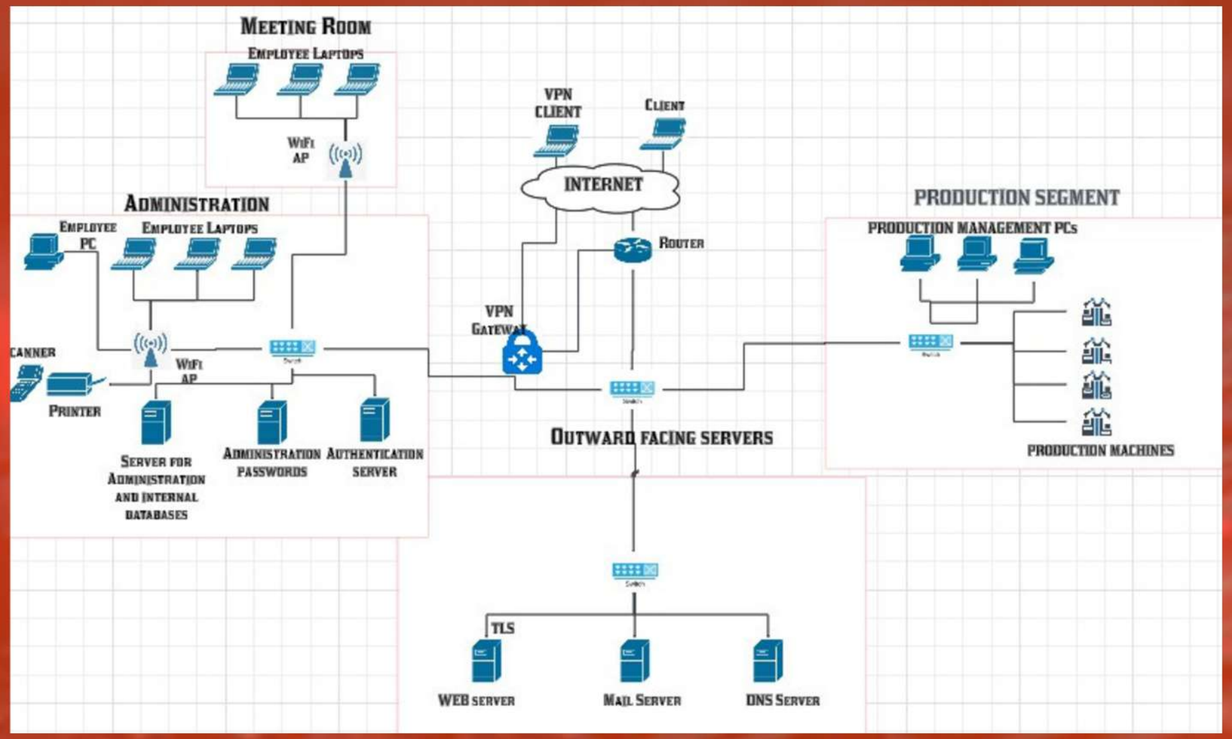

- National Security Agency. (2022, June 15). Network infrastructure security guidance (CTR publication). https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

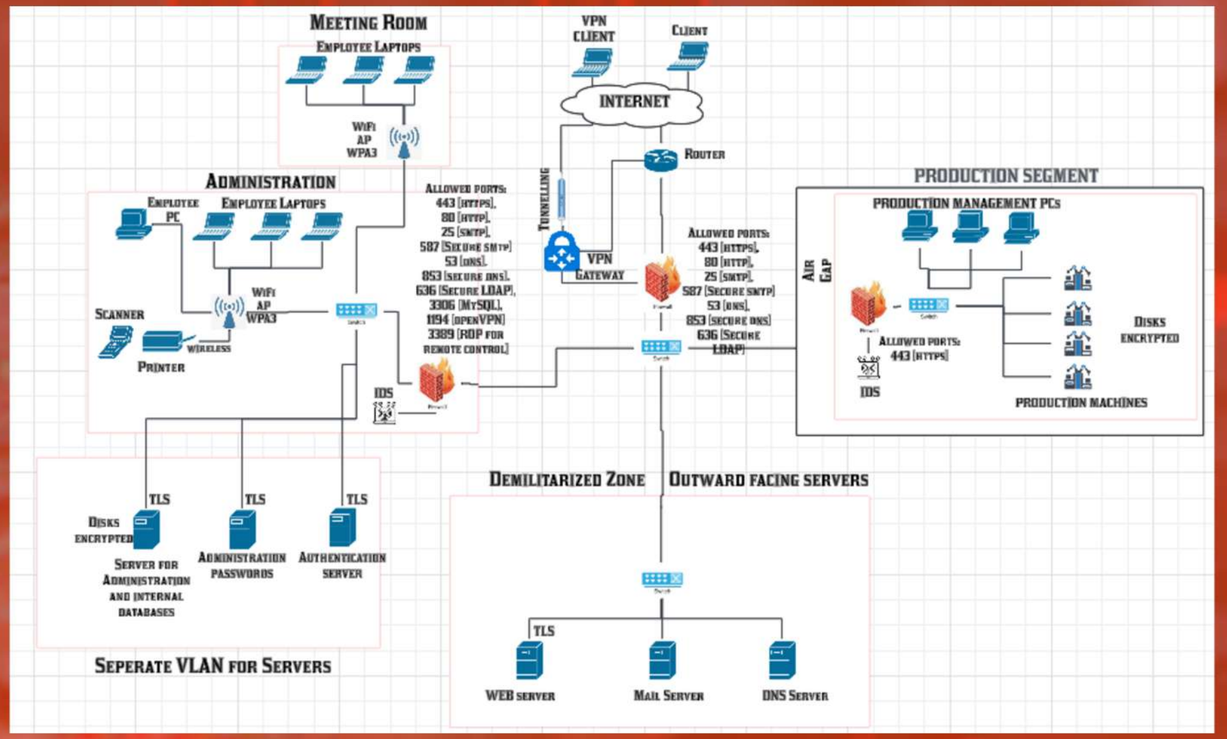
- Palo Alto Networks. (2023). Best practices for enterprise network segmentation. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

- NIST. (2022). Guidelines on firewalls and firewall policy https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901083

- I acknowledge the use of ChatGPT for this task in the following manner:
    a. In order to understand the different security controls and their implementations

# APPENDIX


MEETING ROOM
EMPLOYEE LAPTOPS
WIFI AP
ADMINISTRATION
EMPLOYEE PC
EMPLOYEE LAPTOPS
WIFI AP
PRINTER
SERVER FOR ADMINISTRATION AND INTERNAL DATABASES
ADMINISTRATION PASSWORDS
AUTHENTICATION SERVER
VPN CLIENT
CLIENT
INTERNET
ROUTER
VPN GATEWAY
OUTWARD FACING SERVERS
TLS
WEB SERVER
MAIL SERVER
DNS SERVER
PRODUCTION SEGMENT
PRODUCTION MANAGEMENT PCS
PRODUCTION MACHINES


MEETING ROOM
EMPLOYEE LAPTOPS
WIFI AP WPA3
ADMINISTRATION
EMPLOYEE PC
EMPLOYEE LAPTOPS
SCANNER
WIRELESS
PRINTER
WIFI AP WPA3
IDS
ALLOWED PORTS:
443 [HTTPS],
80 [HTTP],
25 [SMTP],
587 [SECURE SMTP]
53 [DNS],
853 [SECURE DNS],
636 [SECURE LDAP],
3306 [MySQL],
1194 [OPENVPN]
3389 [RDP FOR REMOTE CONTROL]
TLS
DISKS ENCRYPTED
SERVER FOR ADMINISTRATION AND INTERNAL DATABASES
ADMINISTRATION PASSWORDS
AUTHENTICATION SERVER
SEPERATE VLAN FOR SERVERS
VPN CLIENT
CLIENT
INTERNET
ROUTER
TUNNELLING
VPN GATEWAY
ALLOWED PORTS:
443 [HTTPS],
80 [HTTP],
25 [SMTP],
587 [SECURE SMTP]
53 [DNS],
853 [SECURE DNS],
636 [SECURE LDAP]
DEMILITARIZED ZONE
OUTWARD FACING SERVERS
TLS
WEB SERVER
MAIL SERVER
DNS SERVER
PRODUCTION SEGMENT
AIR GAP
PRODUCTION MANAGEMENT PCS
ALLOWED PORTS:
443 [HTTPS]
IDS
DISKS ENCRYPTED
PRODUCTION MACHINES