Assignment 4 (Part 2) – Cybersecurity

CHEW YANG XUAN (33520496)

MONASH University

MALAYSIA

Yang Xuan

Chew

33520496

STUDENT

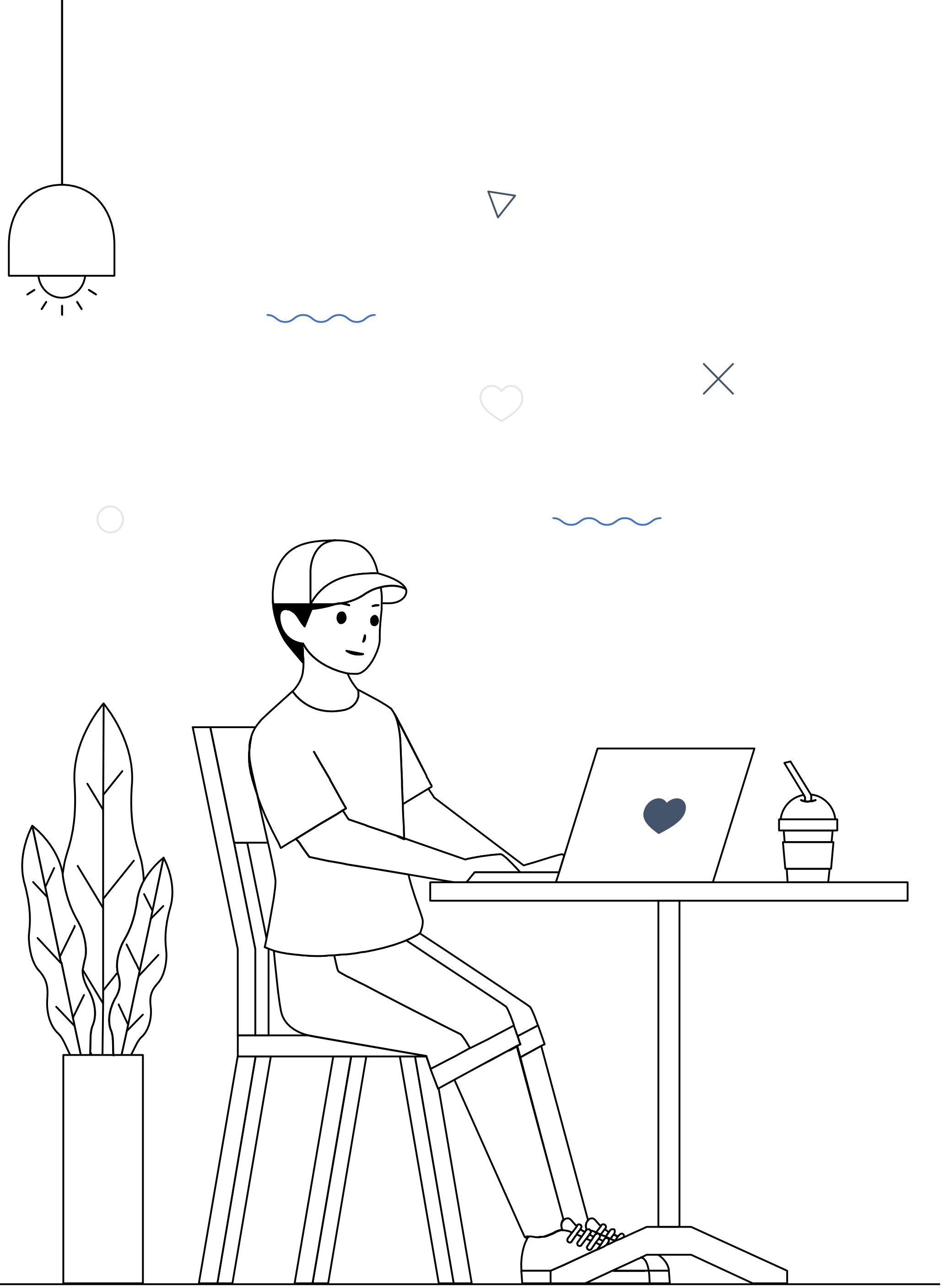
Issue: 1

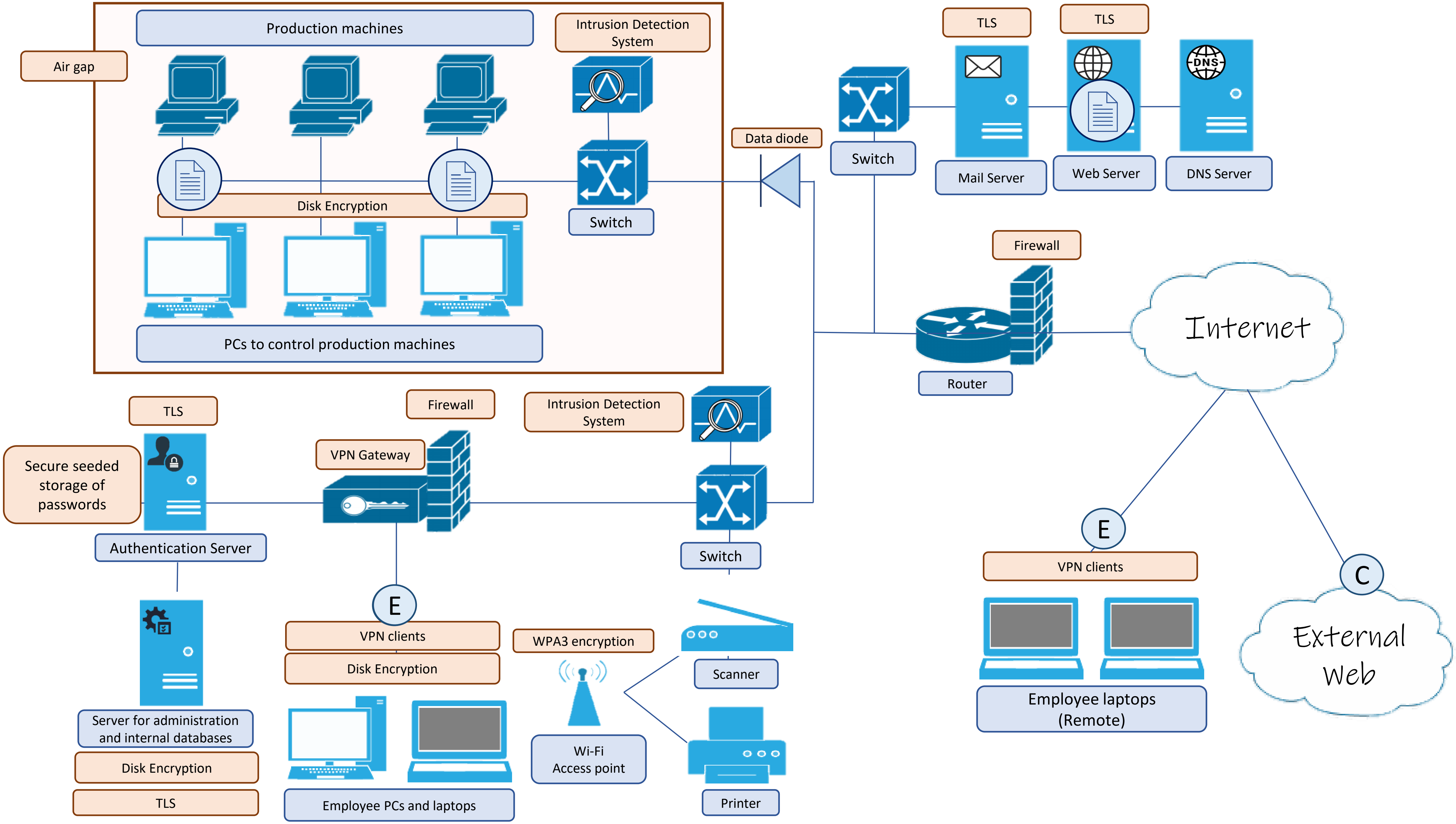
Expiry

31/03/2029

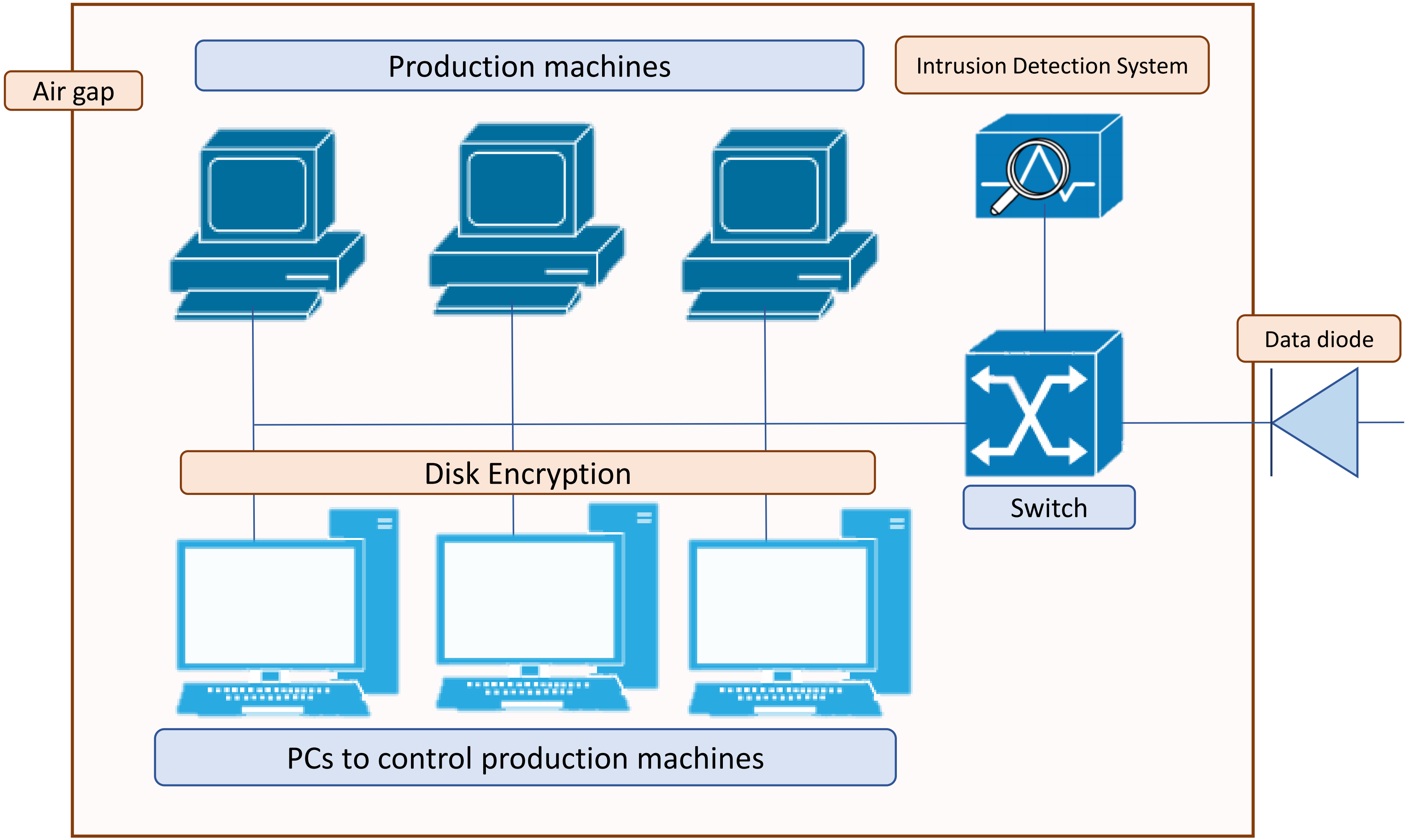
01

Network Diagram




Production machines
Intrusion Detection System
Air gap
Disk Encryption
Switch
PCs to control production machines
Data diode
TLS
TLS
Switch
Mail Server
Web Server
DNS
DNS Server
Firewall
Router
Internet
TLS
Firewall
Intrusion Detection System
Secure seeded storage of passwords
VPN Gateway
Authentication Server
Switch
E
VPN clients
Disk Encryption
WPA3 encryption
Scanner
Wi-Fi Access point
Printer
Server for administration and internal databases
Disk Encryption
TLS
Employee PCs and laptops
E
VPN clients
Employee laptops (Remote)
C
External Web

Production network



Air gap

Production machines

Intrusion Detection System

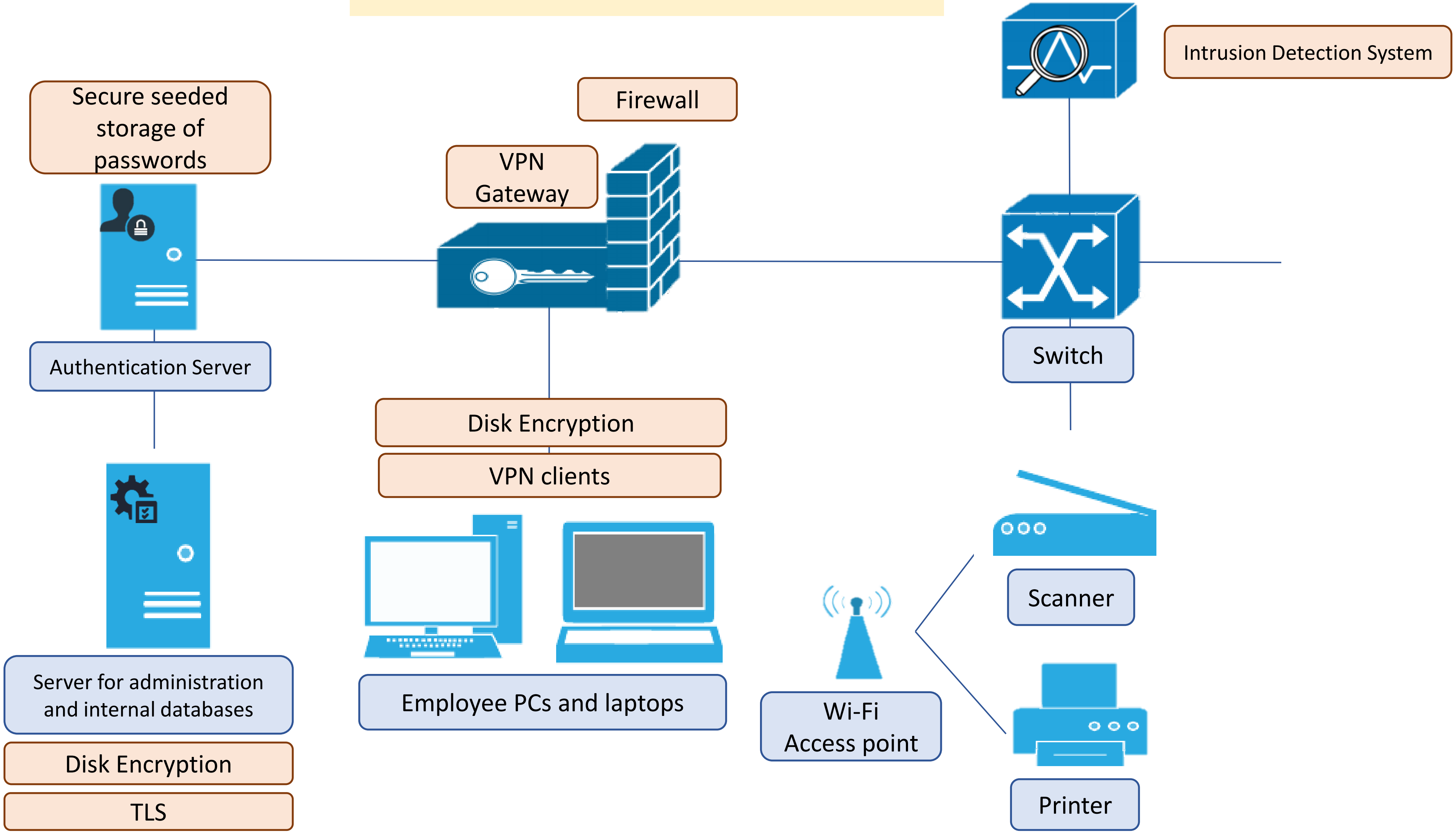
Data diode

Disk Encryption

Switch

PCs to control production machines

Administration network



Intrusion Detection System

Firewall

Secure seeded storage of passwords

VPN Gateway

Authentication Server

Switch

Disk Encryption

VPN clients

Scanner

Server for administration and internal databases

Employee PCs and laptops

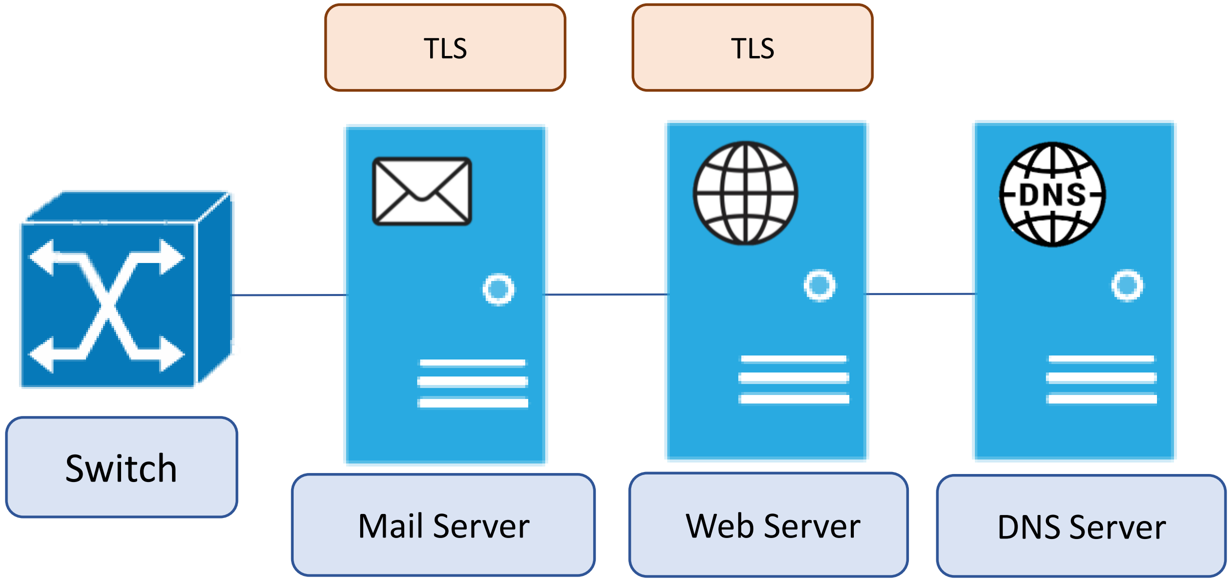
Wi-Fi Access point

Printer

Disk Encryption

TLS

Outward Facing Server



02

Security controls

Firewalls

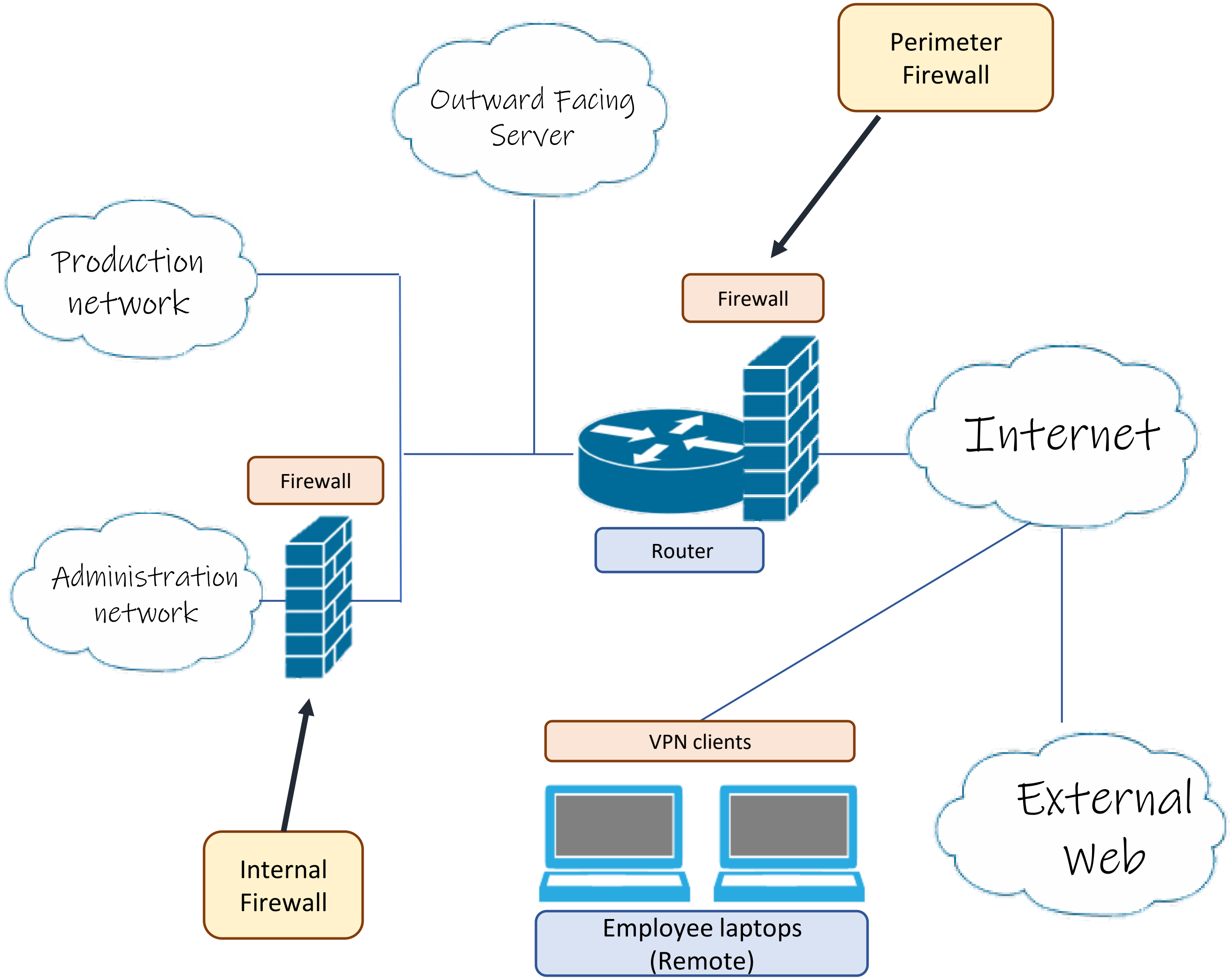
- First level defense
- Monitor network traffic and block suspicious traffic (Cisco, 2023)
- Port number for Perimeter Firewall:
  - Port 443 : HTTPS
  - Port 80 : HTTP
  - Port 22 : SSH
  - Port 587 : SMTP
  - Port 53 : DNS
  - Port 500 : IPSec

Web Server

Mail Server

DNS Server

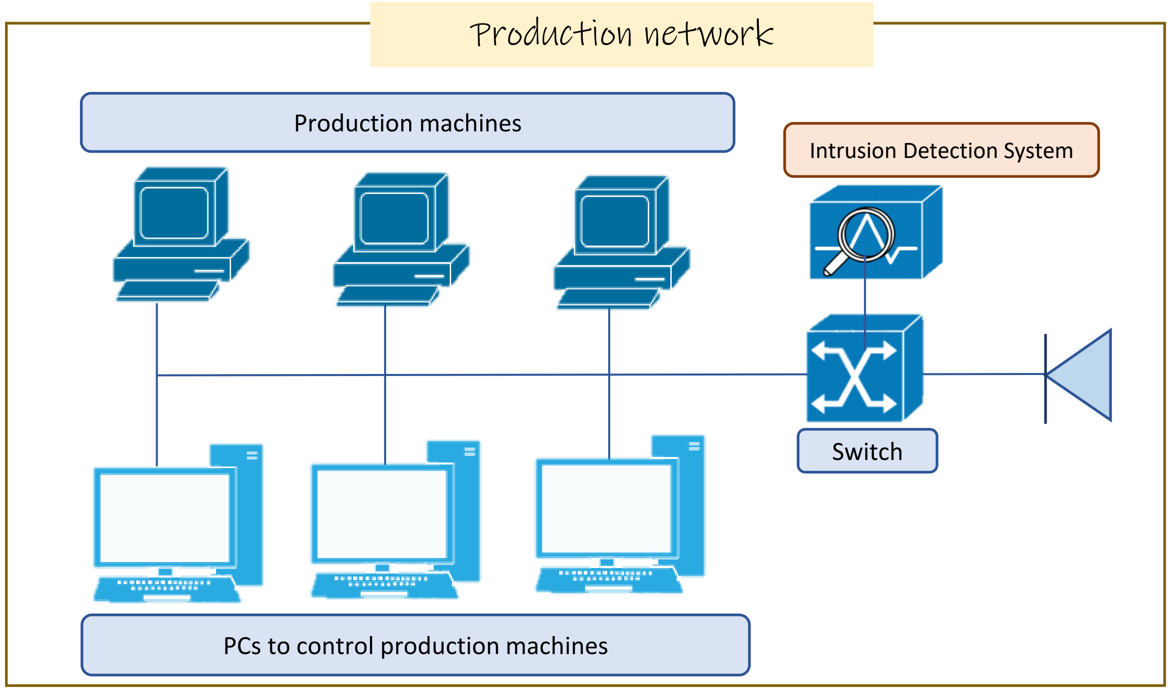
- Port number for Internal Firewall (Administration Network):
  - Port 1433 : Database Engine
  - Port 500 : IPSec



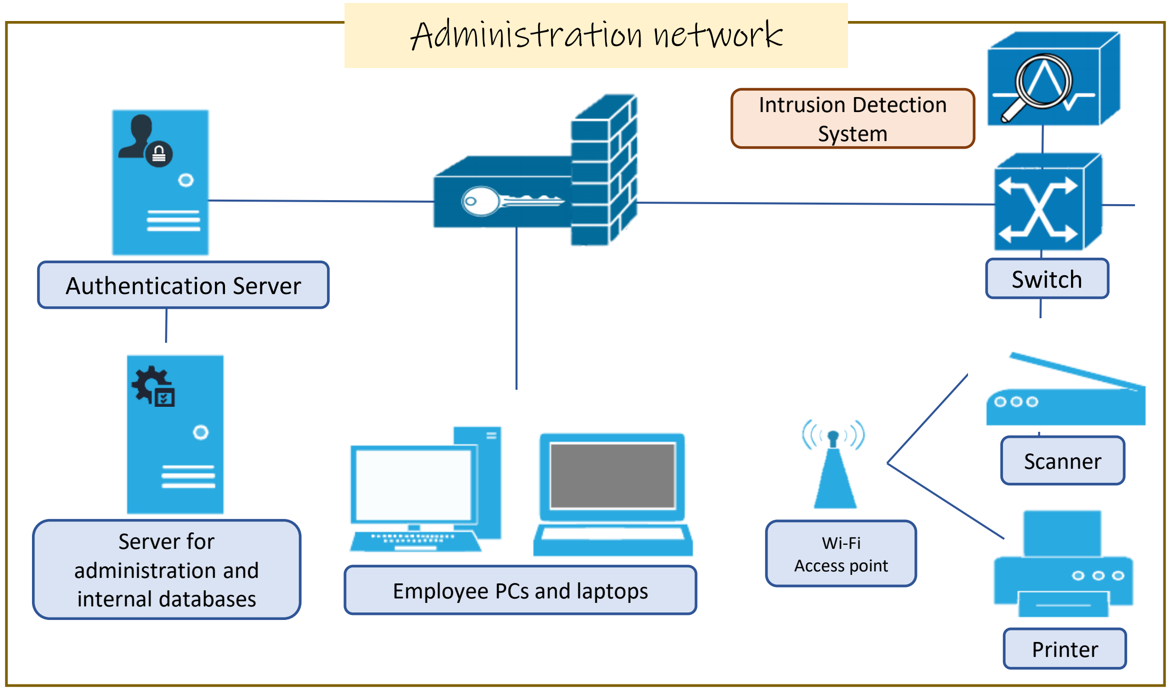
Intrusion Detection System

- Second level defense
- System that monitors network traffic for any unusual or concerning behavior and raise alerts when upon detection (Lutkevich, 2022)
- Anomaly-based detection
  - Identifying unknown attacks
- Signature-based detection
  - Identifying known attacks
- Reactions:
  - Drop abnormal network packets and initiate alarm
  - Block traffic from some IP address
  - Correct fragmentation within data streams
  - Trigger alerts for human acknowledgement

(Rudolph & Tack, n.d.)



Production network
Production machines
Intrusion Detection System
Switch
PCs to control production machines

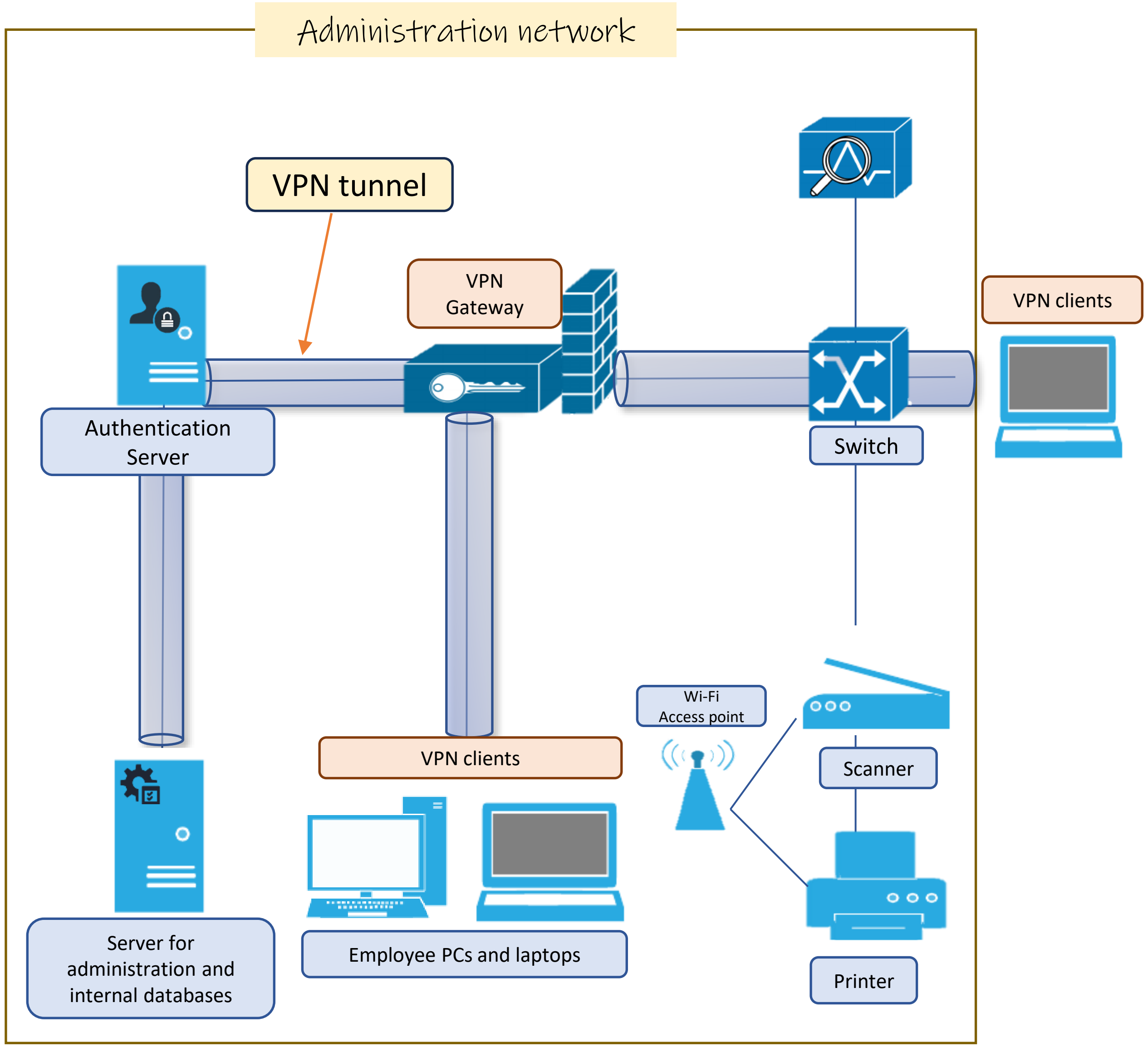


VPN Gateway

- Connect devices or networks together in a VPN infrastructure (Rouse, 2014)
- Create secure connection between employee and server for administration and internal databases
- Encrypt the message → Security purpose

VPN Clients

- Software which establish connection between devices and VPN server (Anton, 2023)
- Enhance privacy and confidentiality
- Safeguard data from eavesdropping or interception by establish an encrypted tunnel in between (Timmerman, 2023)



TLS

- Security protocol to establish a shared key to protect messages using symmetric encryption (Rudolph, n.d.)

TLS
Web Server

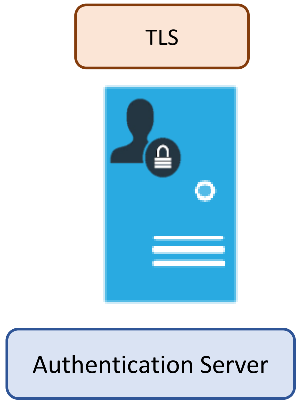
- Enable client to connect to a secure website (SSL/TLS connection)
- Ensure authentication using method of certificate (SHA)
- SHA >> hashing data and certificates

(Jena, 2023)

TLS
Mail Server

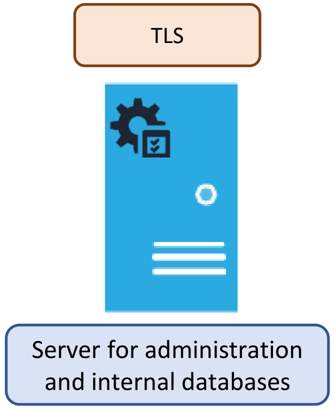
- Enable secure email transmission through secure channel
- Encrypted email contents using asymmetric encryption
- Ensure integrity and privacy

(Agari, 2021)



- Enable secure remote access communication with employee
- Protect confidentiality using Diffie-Hellman Key Exchange (DHKE)
- DHKE >> Secure key exchange

(Nakov, 2018)



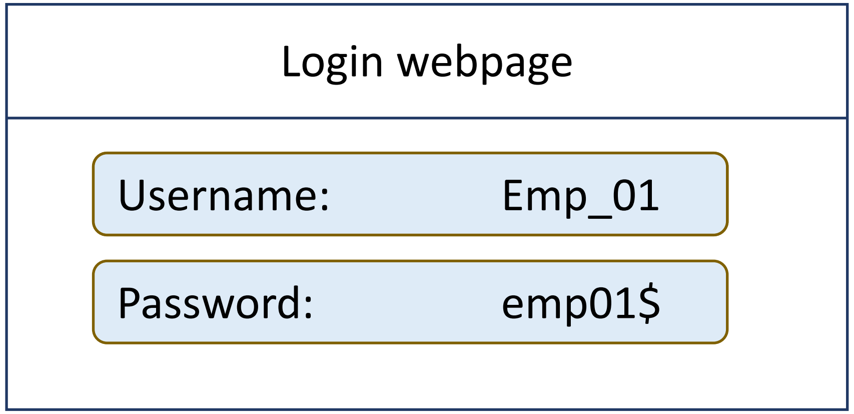
- Enable secure data transmission
- Ensure integrity by using Message Authentication Code (MAC)
- MAC >> ensure message does not change during transmission

(Sheldon, 2023)

Secure seeded storage of passwords

- Method of storing passwords
- Implemented on Authentication Server >> Provide access control to employee only
- Each employee >> own username and passwords
- Store password using Salted hash
- Protection towards identical passwords

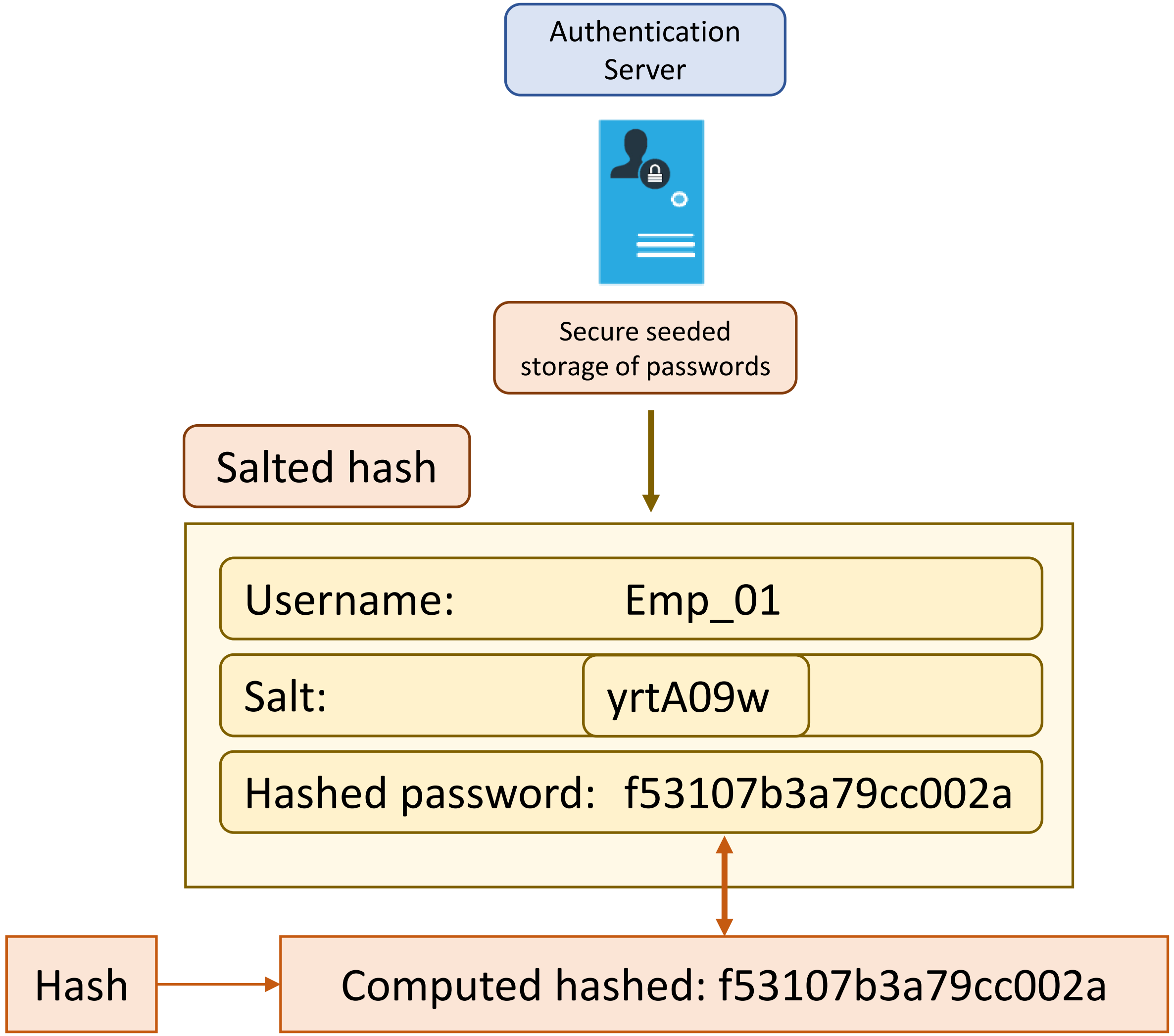
(Arias, 2018)



Login webpage

Username: Emp_01

Password: emp01$



Authentication Server

Secure seeded storage of passwords

Salted hash

Username: Emp_01

Salt: yrtA09w

Hashed password: f53107b3a79cc002a

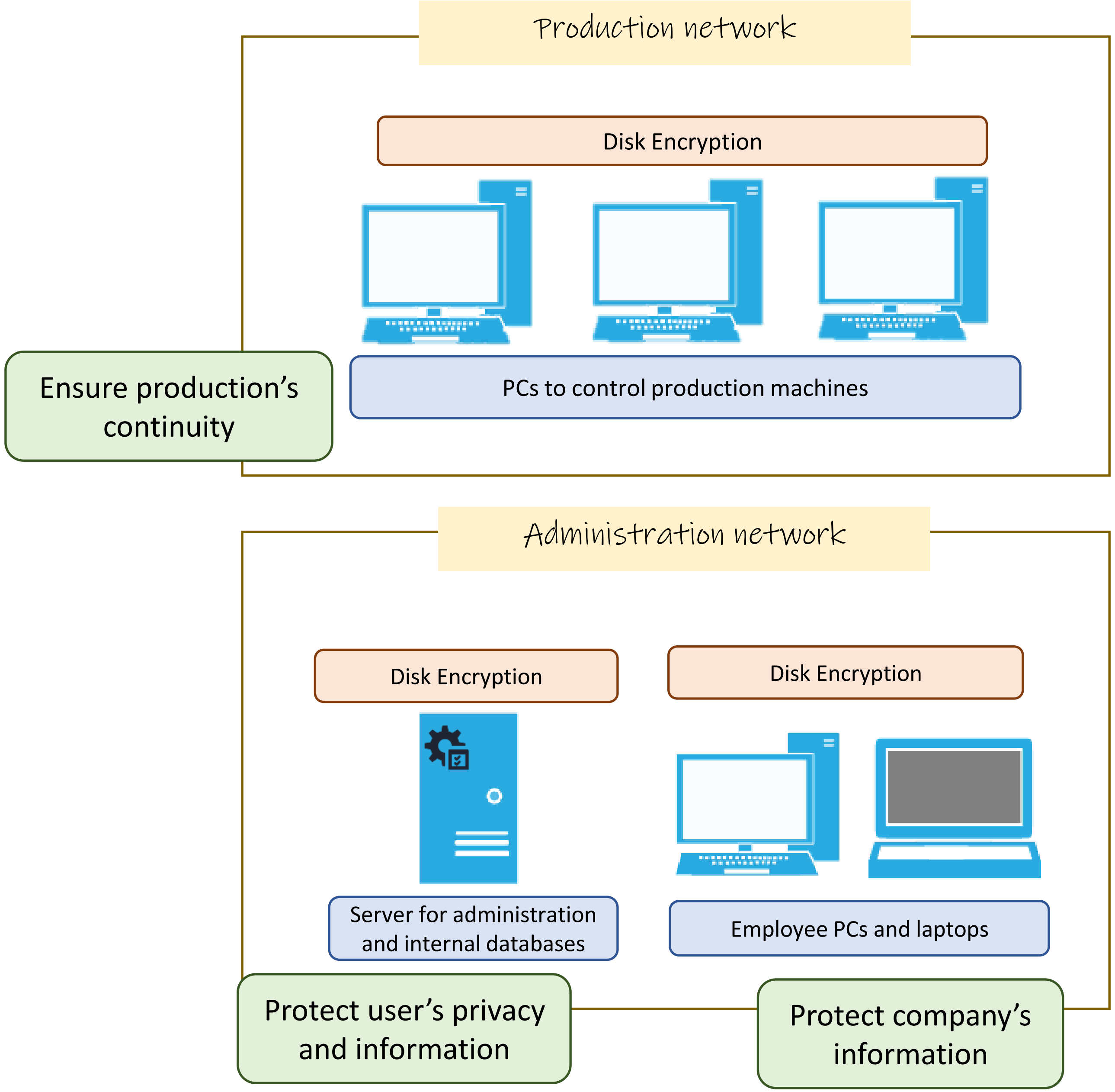
Hash

Computed hashed: f53107b3a79cc002a

Disk Encryption

- Encrypt data on a disk
- Provide protection against unauthorized access
- Utilize Advanced Encryption Standard (AES) for encryption
- Ensure confidentiality of the data
- Attackers unable to gain the information without the encryption key

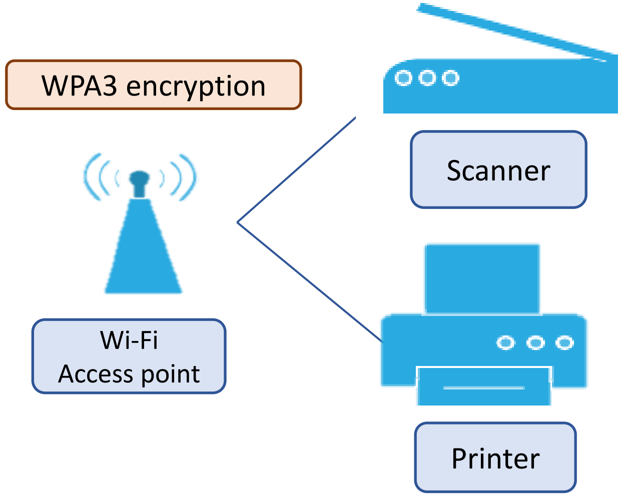
(Rimkiene, 2020)


Production network
Disk Encryption
PCs to control production machines
Ensure production's continuity
Administration network
Disk Encryption
Disk Encryption
Server for administration and internal databases
Employee PCs and laptops
Protect user's privacy and information
Protect company's information

WPA3 Encryption

- Use AES method
- Ensure data transmitted over a Wi-Fi network is secured
- Protect confidentiality and integrity of the data

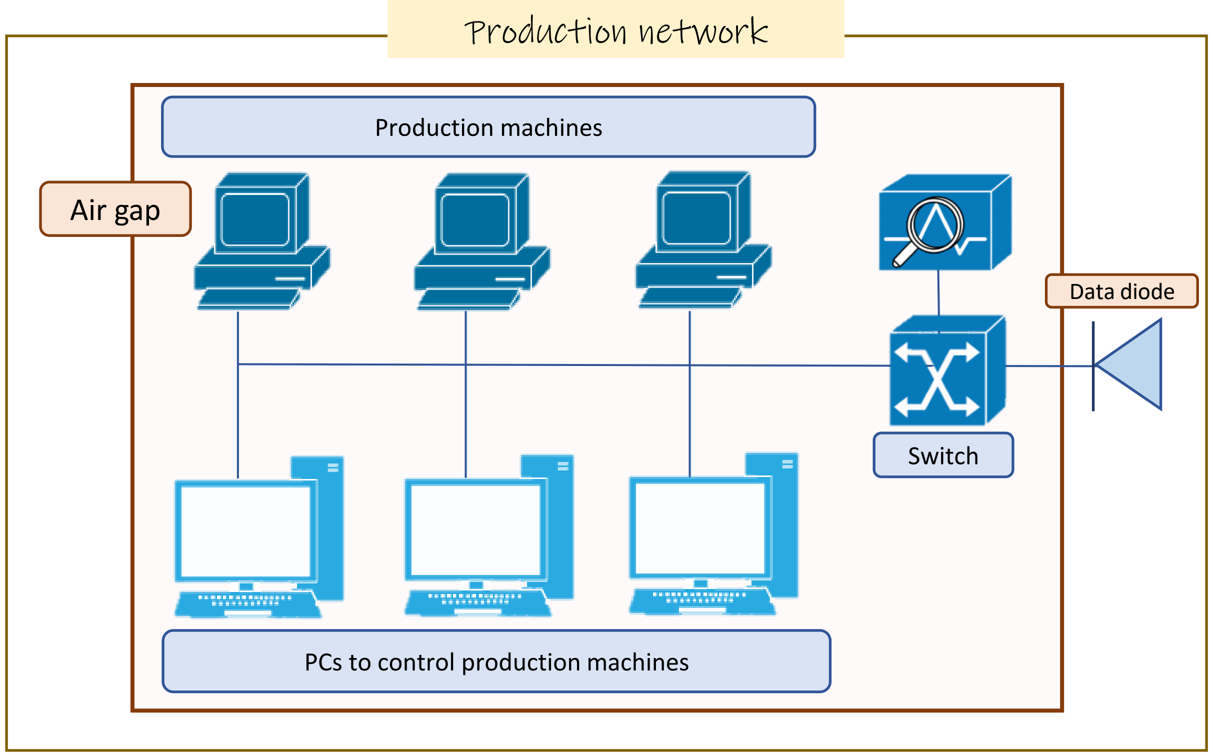
(Gillis, 2023)



Air gaps

- Isolates local area network from other networks (Rouse, 2022)
- Reduce the potential for security breaches
- Implements a data diode to allow data transfers to the PCs controlling the production machines

(Advenica, 2023)



References

Advenica. (2023, October 24). Data diodes - an effective alternative to air gaps | Advenica. *Advenica.com*. https://advenica.com/de/node/1200

Agari. (2021, June 21). *TLS Email Encryption: What It Is & How to Check if Your Email Is Using It*. Agari; Fortra. https://www.agari.com/blog/transport-layer-security-tls-emailencryption

Anton, P. (2023, August 9). *What is a VPN client? How it simplifies VPN use - Atlas VPN*. Atlasvpn.com. https://atlasvpn.com/blog/what-is-vpn-client

Arias, D. (2018, May 3). *Adding Salt to Hashing: A Better Way to Store Passwords*. Auth0. https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

Cisco. (2023). *What Is a Firewall?* Cisco. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Gillis, A. S. (2023, April). *What is WPA3? - Definition from WhatIs.com*. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/WPA3

Jena, B. K. (2023, August 29). *What Is SHA-256 Algorithm: How it Works & Applications | Simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

Lutkevich, B. (2022, October). *What is an intrusion detection system (IDS)? Definition from SearchSecurity*. TechTarget. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

Nakov, S. (2018, November). *Diffie–Hellman Key Exchange - Practical Cryptography for Developers*. Nakov.com. https://cryptobook.nakov.com/key-exchange/diffie-hellman-key-exchange

References

Rimkiene, R. (2020, December 11). *What is AES Encryption and How Does It Work?* CyberNews. https://cybernews.com/resources/what-is-aes-encryption/

Rouse, M. (2014, September 2). *What is a VPN Gateway? - Definition from Techopedia*. Techopedia.com. https://www.techopedia.com/definition/30755/vpn-gateway

Rouse, M. (2022, June 9). *What is an Air Gap? - Definition from Techopedia*. Techopedia.com. https://www.techopedia.com/definition/17037/air-gap

Rudolph, C. (n.d.). *Security Protocols: Transport Layer Security [Lecture Notes]*. Moodle@MU. https://shorturl.at/kAPQ6

Rudolph, C., & Tack, G. (n.d.). *Network Security: Intrusion detection and prevention [Lecture Notes]*. Moodle@MU. https://shorturl.at/qRS48

Sheldon, R. (2023, August). *What is message authentication code (MAC)? - Definition from WhatIs.com*. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/message-authentication-code-MAC

Timmerman, C. (2023, September 13). *What is an eavesdropping attack? | IPVanish*. Www.ipvanish.com. https://shorturl.at/nrCJK

Whitmore, C. (2023, June 20). *What are VPN ports? Everything you need to know | NordVPN*. Nordvpn.com. https://nordvpn.com/blog/what-are-vpn-ports/#:~:text=Default%20VPN%20ports%20depend%20on

Thanks!