SECURITY CONTROLS

SECURITY ARCHITECT

FOO KAI YAN
33085625

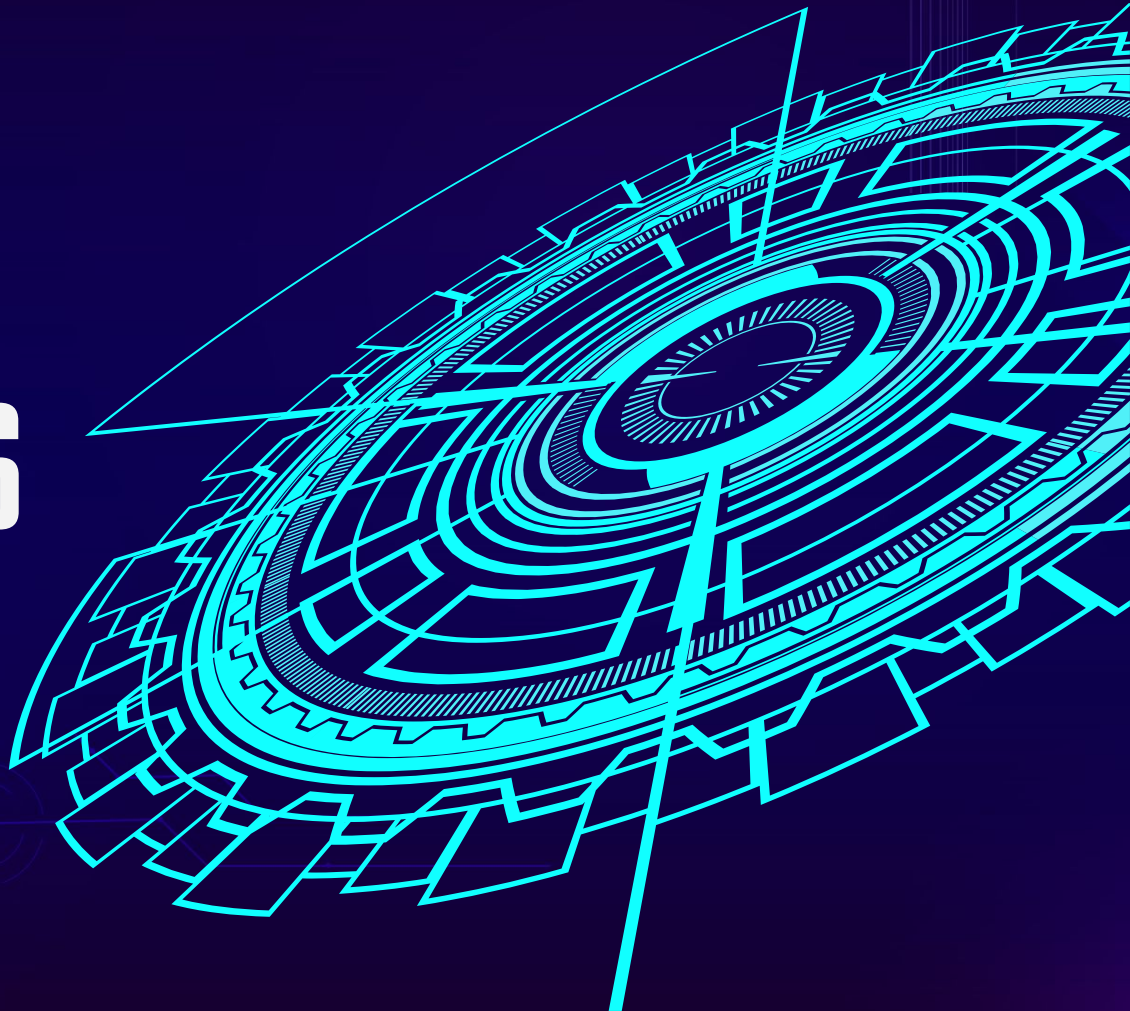
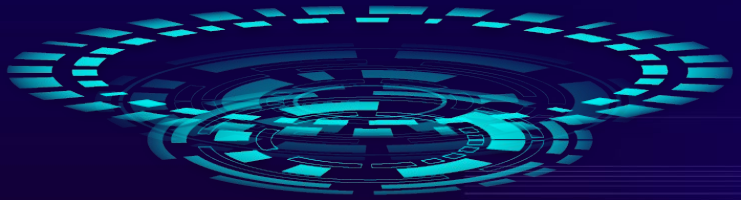


TABLE OF CONTENTS

INTRODUCTION

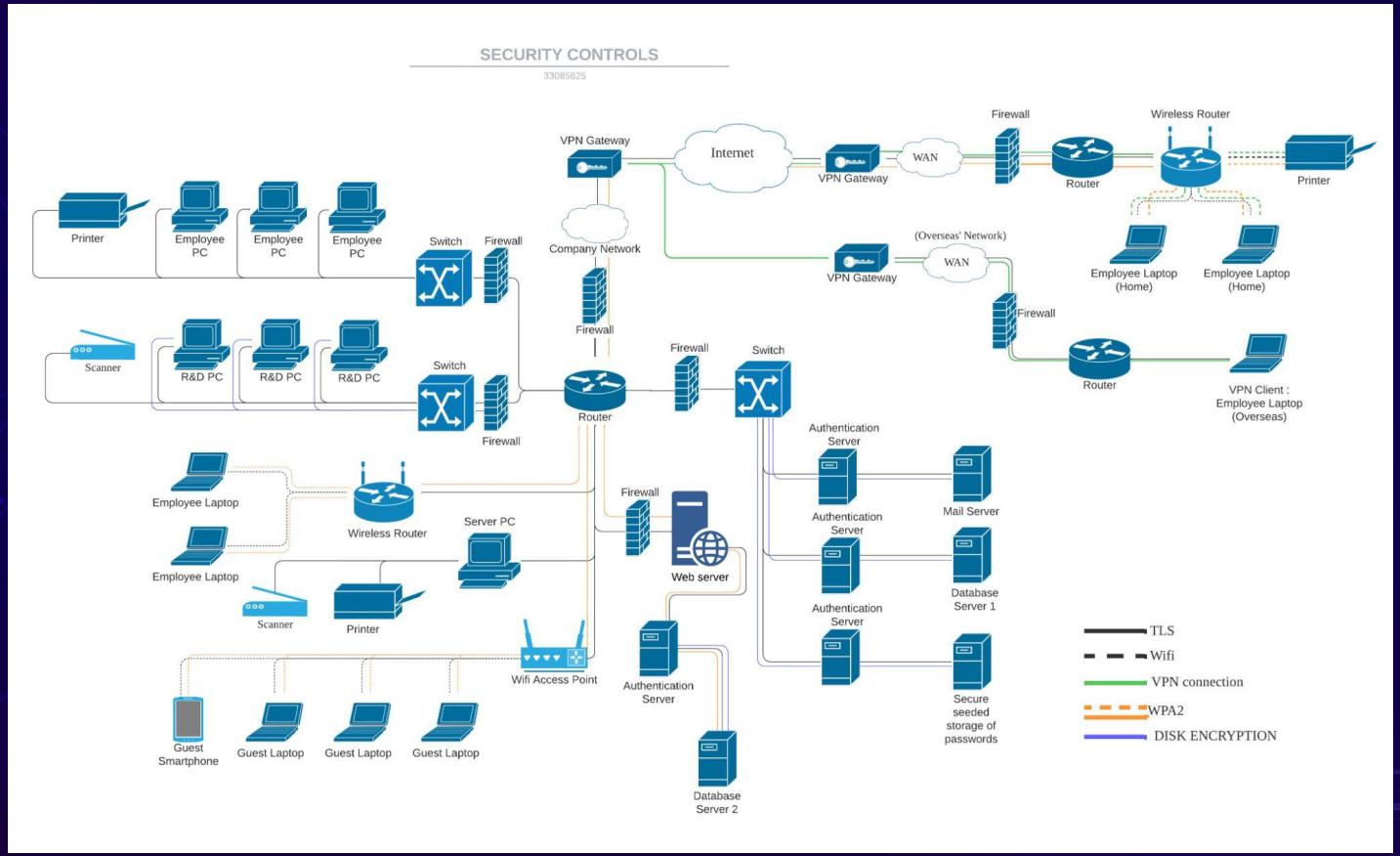
ROLE : SECURITY ARCHITECT

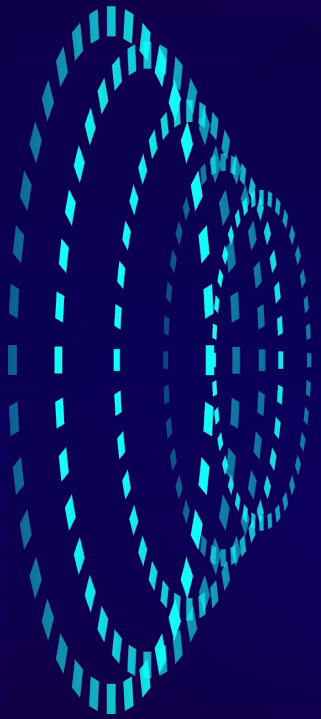
PURPOSE : USE A LIST OF SECURITY CONTROLS TO CONNECT A NUMBER OF ENTITIES TO THE INTERNAL NETWORK WHILST ENSURING THE ORGANISATION IS PROTECTED FROM INTERNAL AND EXTERNAL ADVERSARIES



DIAGRAM

MADE WITH LUCIDCHART





FIREWALLS

- FIRST LINE OF NETWORK SECURITY DEFENCE
- MONITOR ONGOING NETWORK TRAFFIC
- ALLOW OR BLOCK SPECIFIC TRAFFIC BASED ON ESTABLISHED SECURITY RULES
- PREVENT HACKING, VIRUS ATTACK, SPYWARE
- BARRIER BETWEEN PUBLIC AND PRIVATE INTERNET
- NETWORK-BASED FIREWALLS
  - STOP UNAUTHORISED ACCESS TO ORGANISATION'S NETWORK
  - PREVENT UNNECESSARY NETWORK TRAFFIC

RETRIEVED FROM :

https://www.miradore.com/blog/hard-drive-encryption-full-disk-encryption/

https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet

RETRIEVED FROM :
https://cloud.google.com/vmware-engine/docs/concepts-vpn-gateways
https://www.techradar.com/vpn/remote-access-vpn

VPN GATEWAY

- PROVIDE SECURE CONNECTION BETWEEN SERVER & CLIENT
- EACH GATEWAY CAN SUPPORT MULTIPLE CONNECTIONS
- VIRTUAL TUNNEL BETWEEN COMPANY'S NETWORK & EMPLOYEES' DEVICE
- PROTECTED BY ENCRYPTION & SECURITY PROTOCOLS
  - PRIVATE & SECURE
- DATA SECURITY
  - INFORMATION OBTAINED BY HACKERS ARE USELESS DUE TO NO DECRYPTION KEY

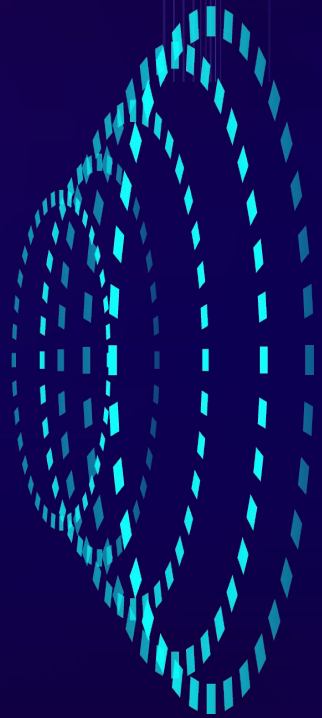
VPN CLIENTS

- VPN CLIENT INITIATED THE CONNECTION WITH VPN SERVER
- SOFTWARE ON CLIENT'S DEVICE
- SECURELY ACCESS DATA AND RESOURCES IN COMPANY'S VPN SERVER

RETRIEVED FROM :
https://www.dummies.com/article/technology/information-technology/networking/general-networking/network-administration-vpn-servers-and-clients-184879/

TLS

- TRANSPORT LAYER SECURITY
- PROTECT CONFIDENTIALITY & INTEGRITY OF DATA-IN-TRANSIT
- PASSWORDS, PERSONAL CORRESPONDENCE, STAFFS PERSONAL INFORMATION
- RESILIENCE AGAINST UNAUTHORISED TAMPERING OF DATA
- ENCRYPT COMMUNICATION SENT
  - ASYMMETRIC & SYMMETRIC ENCRYPTION
    - PROTECT CONFIDENTIALITY & INTEGRITY OF DATA-IN-TRANSIT
    - ASYMMETRIC = ESTABLISH SECURE SESSION
    - SYMMETRIC = EXCHANGE DATA WITHIN SECURE SESSION



RETRIEVED FROM :

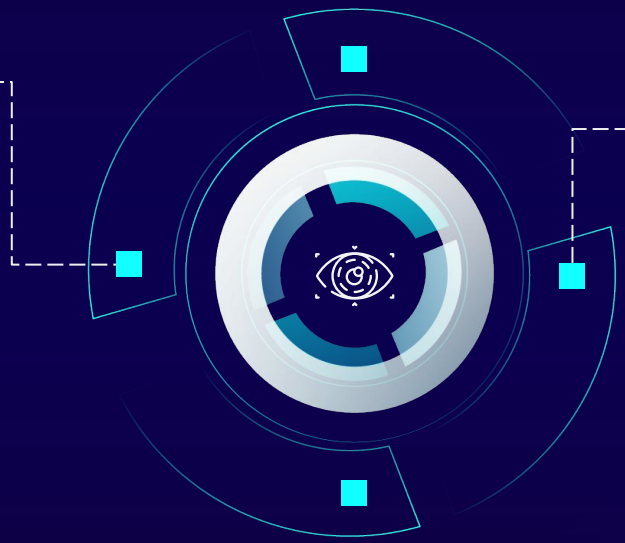
https://www.techtarget.com/searchsecurity/definition/Transport-Layer-Security-TLS

https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

RETRIEVED FROM :
https://www.okta.com/uk/identity-101/authentication-server/

AUTHENTICATION SERVER

- MANAGE PROCESSES THAT ALLOWS ACCESS TO NETWORK, APPLICATION OR SYSTEM
- IDENTIFY IMPOSTERS
- PROTECT CRITICAL ASSETS
- VERIFY EMPLOYEES' RIGHTS TO ACCESS FILES & DATA
- USERNAME/PASSWORD COMBINATION METHODS:
  - SINGLE-FACTOR
  - MULTIFACTOR



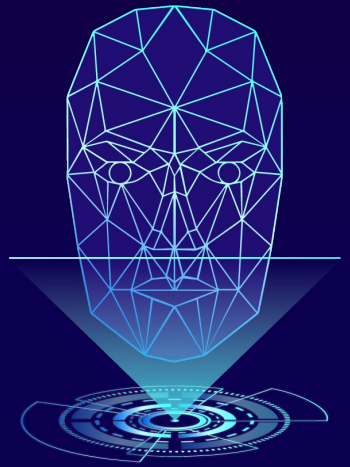
SECURE SEEDED STORAGE OF PASSWORDS

- STORAGE SPACE FOR ALL RELEVANT ACCOUNT PASSWORDS
- PASSWORD ENCRYPTED & DECRYPTED USING AES-256
- SAFE AGAINST BRUTE FORCE ATTACK FROM HACKERS

RETRIEVED FROM :
https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

DISK ENCRYPTION

- CONVERT DATA TO UNREADABLE CODE TO PREVENT UNAUTHORISED PERSON FROM DECIPHERING IT
- DATA THAT GOES IN DISK
- ENCRYPT USING HARDWARE OR DISK ENCRYPTION SOFTWARE
- PROTECT A DISK IN THE EVENT OF THEFT OR ACCIDENTAL LOSS
- ENCODING DATA, SYSTEM FILES
- TYPES
  - FULL DISK ENCRYPTION
  - FILE-LEVEL ENCRYPTION



RETRIEVED FROM :
https://www.miradore.com/blog/hard-drive-encryption-full-disk-encryption/

RETRIEVED FROM :

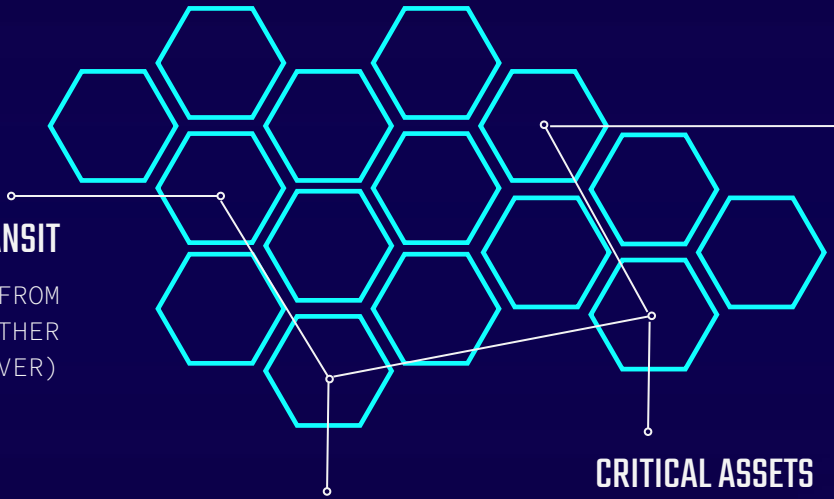
https://www.avast.com/c-wep-vs-wpa-or-wpa2

https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/

WPA2 ENCRYPTION

- ENSURE DATA SENT & RECEIVED IS ENCRYPTED
- SECURED, SHARES PASSWORD WITH ENTITIES OF THE SAME NETWORK
- ENTITIES WITH PASSWORD CAN ONLY ACCESS IT
- IF AUTHENTICATION WAS IMPLEMENTED POORLY, HACKERS CAN EASILY ACCESS THE SHARED DATA
  - POOR CHOOSING OF PASSWORDS
  - LONG PASSWORD TO CREATE SECURE NETWORK

APPENDIX



DATA-IN-TRANSIT

DATA ACTIVELY MOVING FROM ONE LOCATION TO ANOTHER (Eg. CLIENT ↔ SERVER)

MASTER PASSWORD

THE ONLY IMPORTANT PASSWORD AS IT CAN HELP ACCESS & RECOVER ALL ACCOUNTS' PASSWORDS NO MATTER WHAT DEVICE IS USED

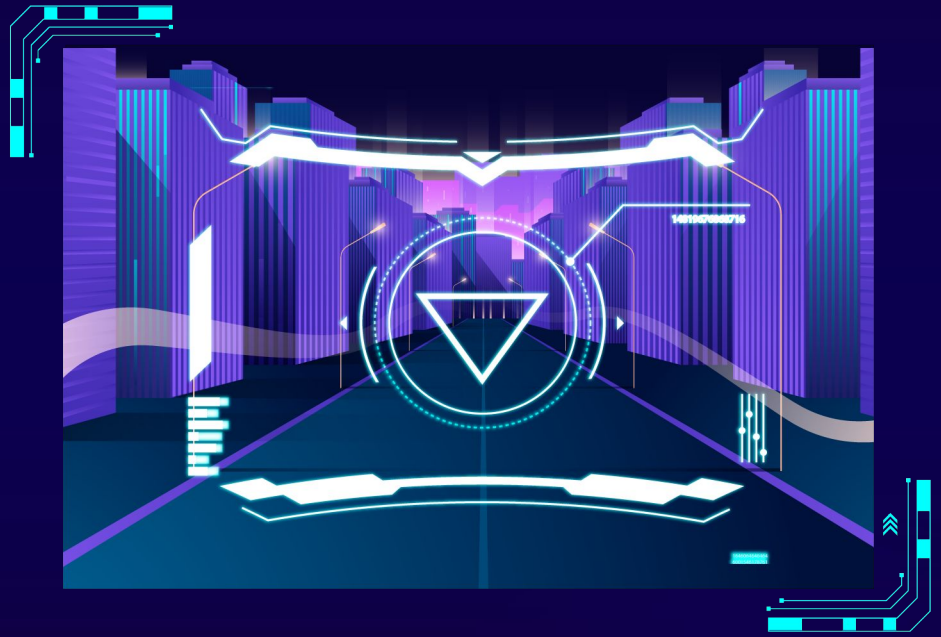
SPYWARE

MALWARE INSTALLED ON TECHNOLOGICAL DEVICES WITHOUT USERS' KNOWLEDGE

CRITICAL ASSETS

COMPANY'S ESSENTIAL RESOURCES TO MAINTAIN OPERATIONS AND ACHIEVE COMPANY'S MISSION (Eg. FINANCIAL DATA, PATENTS, COPYRIGHTS)

THANK YOU



THE NETWORK DIAGRAM *(BIGGER PICTURE)* ON THE NEXT SLIDE

SECURITY CONTROLS

33085625