PROTECTING LEGACY SYSTEMS

DAVID COLLINS

ABOUT ME

- I work at SEPTA (Philadelphia area public transit)
- My previous experience: Linux sysadmin, Windows sysadmin, network engineer
- My current role: Security engineer
- Email: david@decollins.com
- GitHub: https://github.com/dcollins42

PROTECTING LEGACY SYSTEMS

- Things I Will Talk About
  - Network Segmentation
  - Virtual Desktop Infrastructure (VDI)
  - Local virtualization
  - Legacy Wi-Fi
  - Reverse Proxies
  - Case Studies

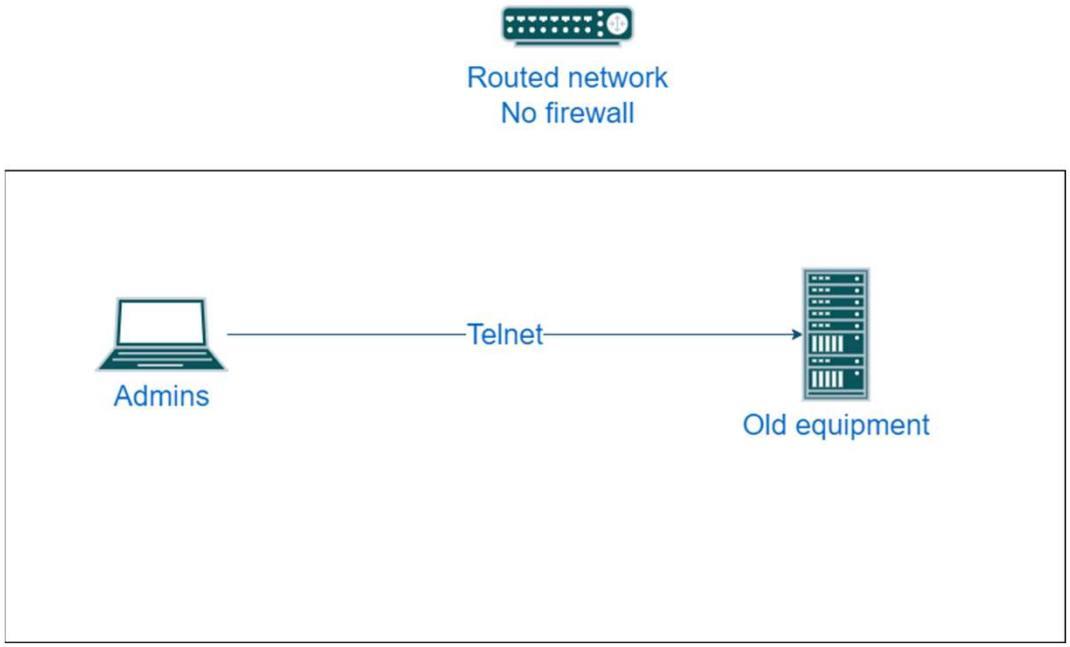
BASIC PROTECTIONS

- Basic Protections
  - Network segmentation
  - Firewall with ingress and egress filtering
  - Endpoint Detection and Response (EDR)
  - Updated operating system and software
  - Zero Trust-ish

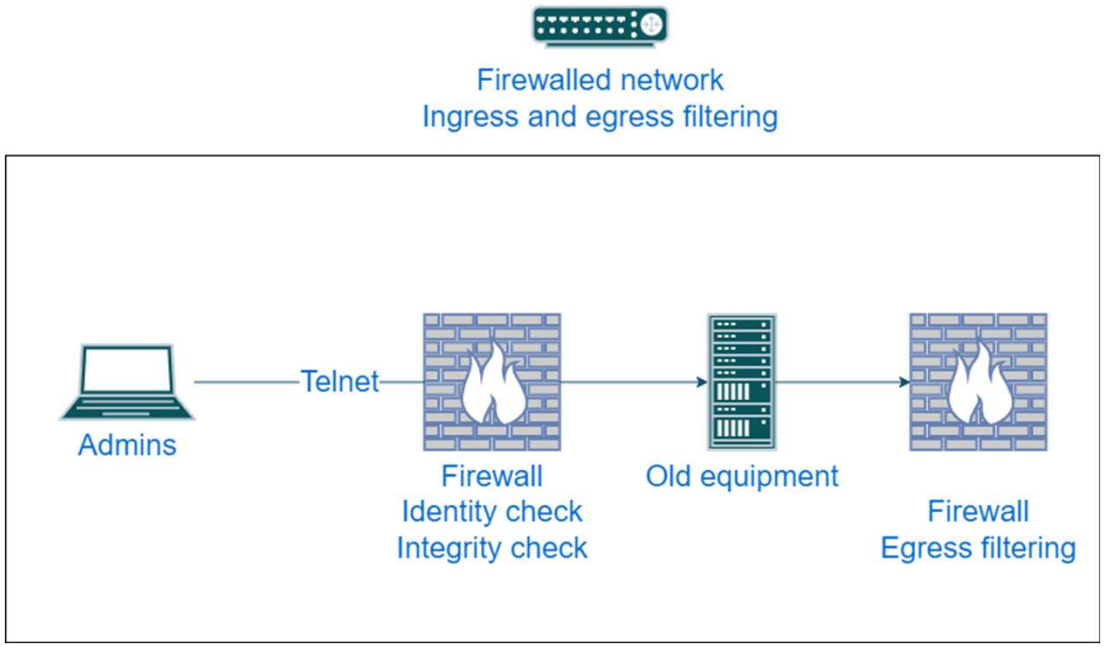
NETWORK SEGMENTATION

- Network segmentation
  - Isolate systems into granular VLANs
  - Only allow necessary communication between VLANs
  - Filter both ingress and egress traffic

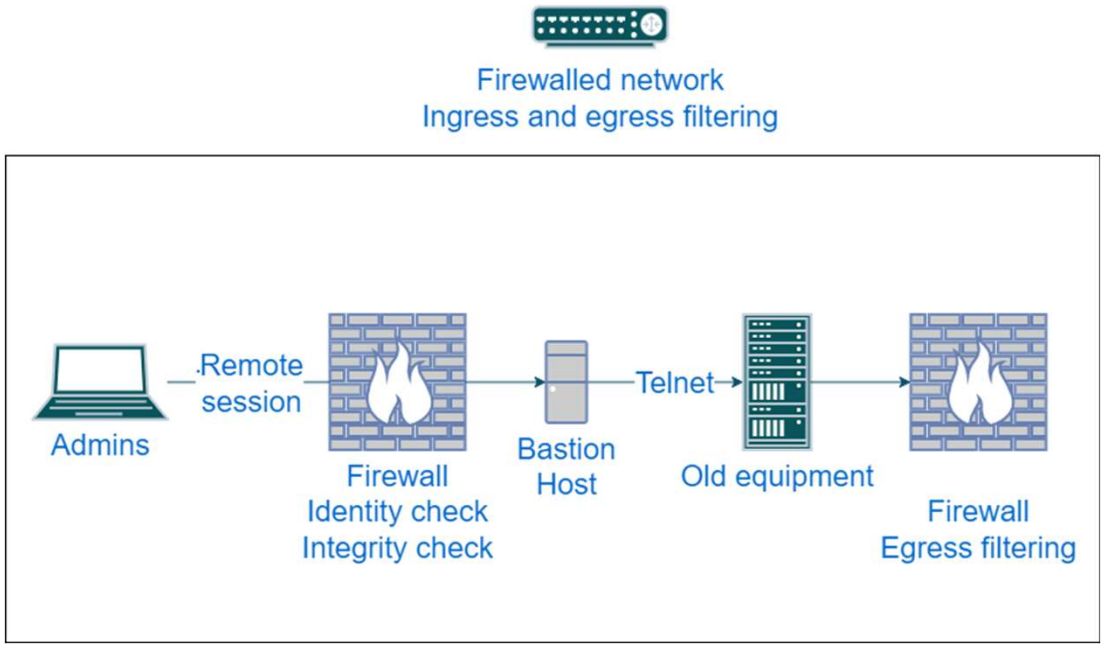
NETWORK SEGMENTATION



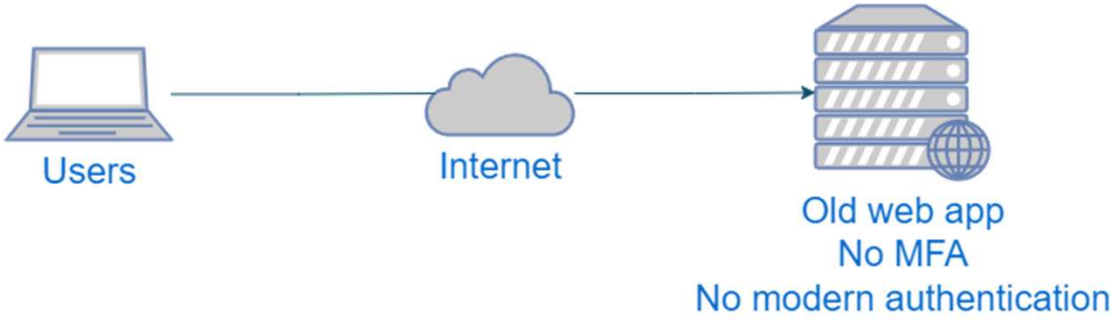
NETWORK SEGMENTATION



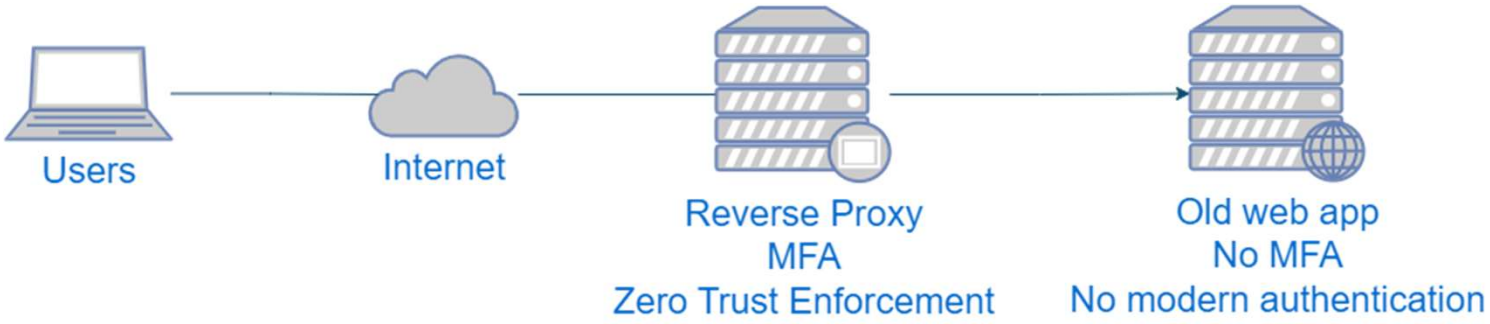
NETWORK SEGMENTATION



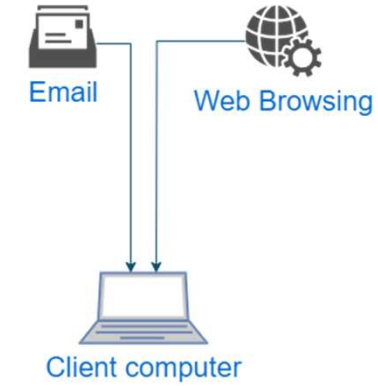
REVERSE PROXY



REVERSE PROXY

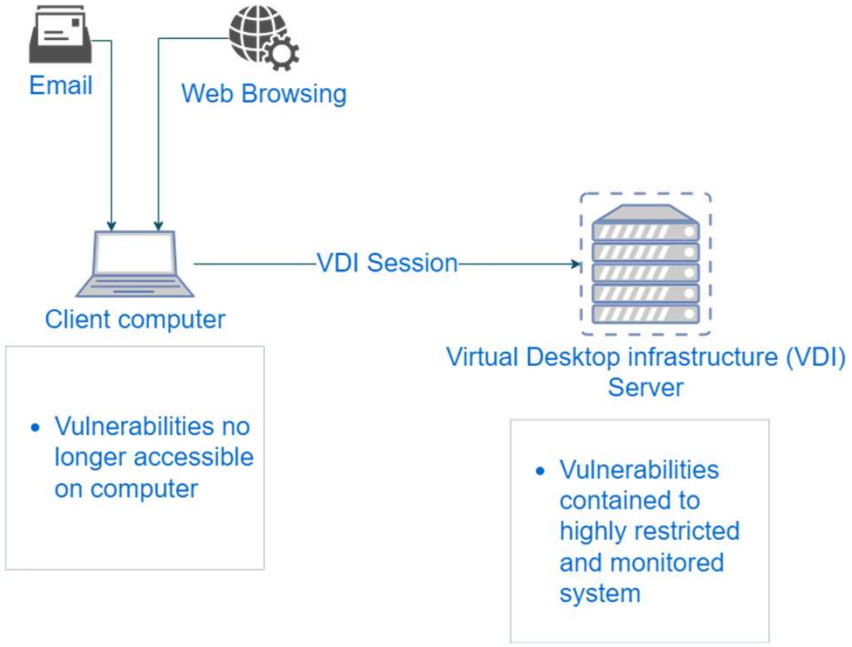


VDI

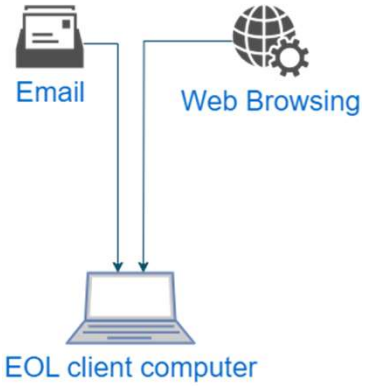


- Old application running locally
- Vulnerabilities accessible on computer

VDI

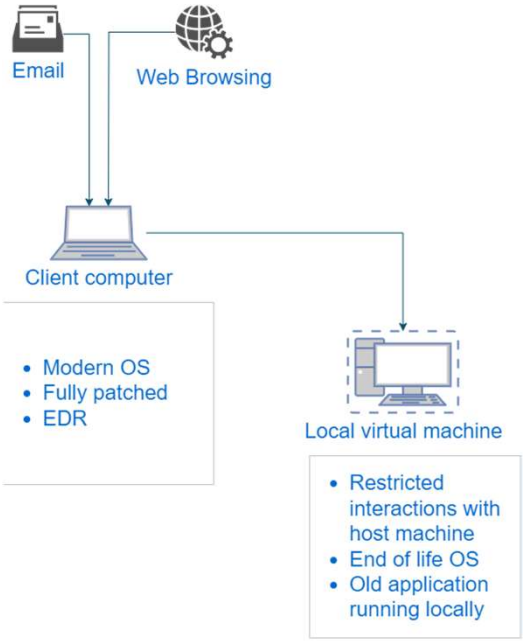

Email
Web Browsing
VDI Session
Client computer
Virtual Desktop infrastructure (VDI) Server
• Vulnerabilities no longer accessible on computer
• Vulnerabilities contained to highly restricted and monitored system

LOCAL VIRTUALIZATION

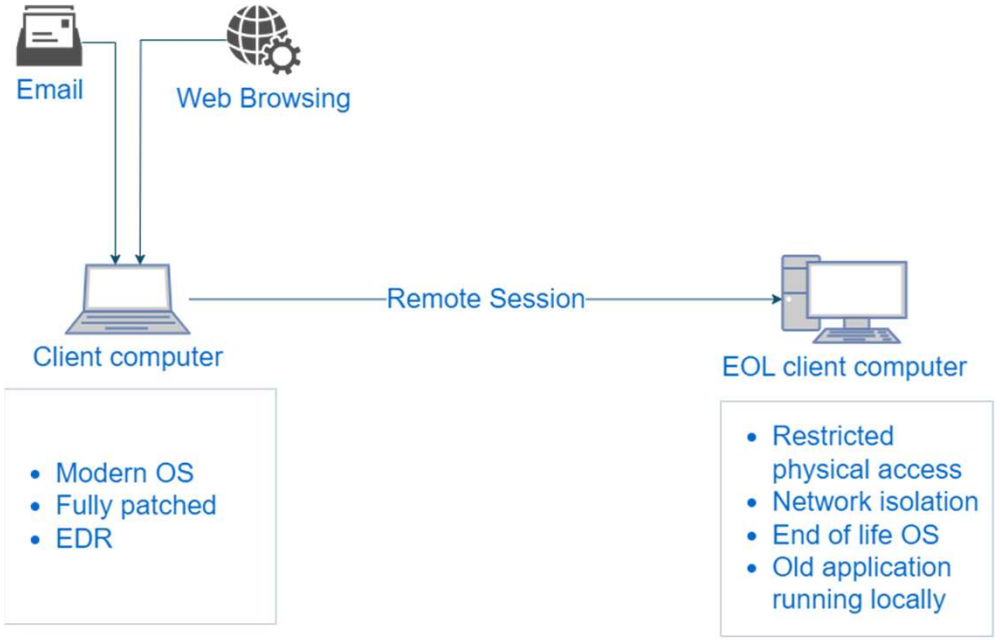


- End of life OS
- Old application running locally
- No EDR

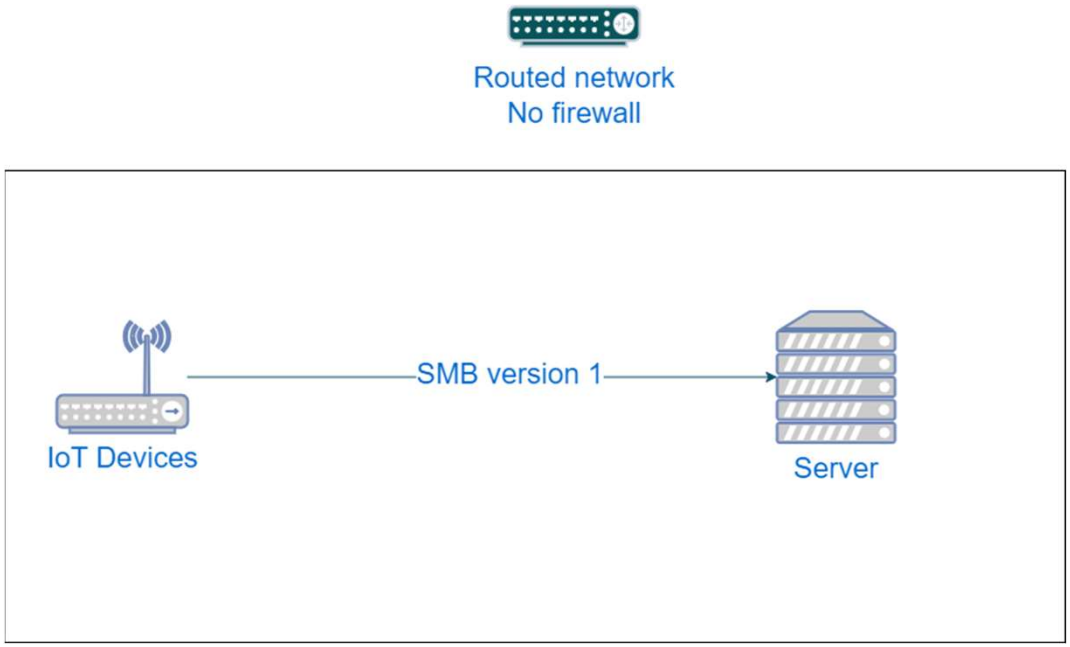
LOCAL VIRTUALIZATION



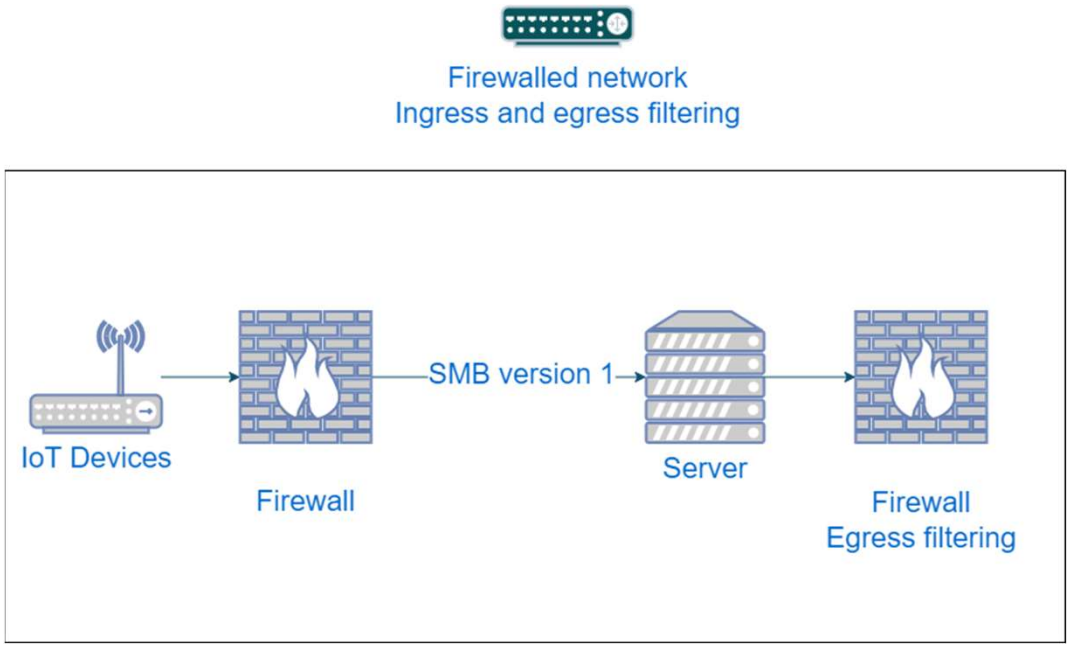
LOCAL VIRTUALIZATION



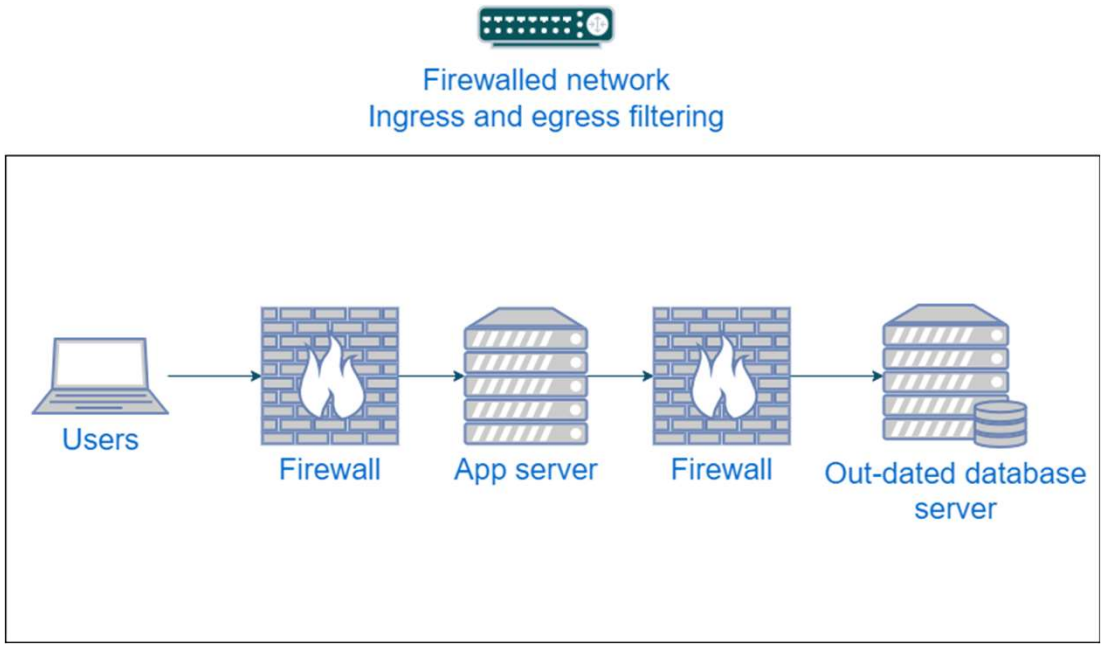
IOT SERVER


Routed network
No firewall
IoT Devices
SMB version 1
Server

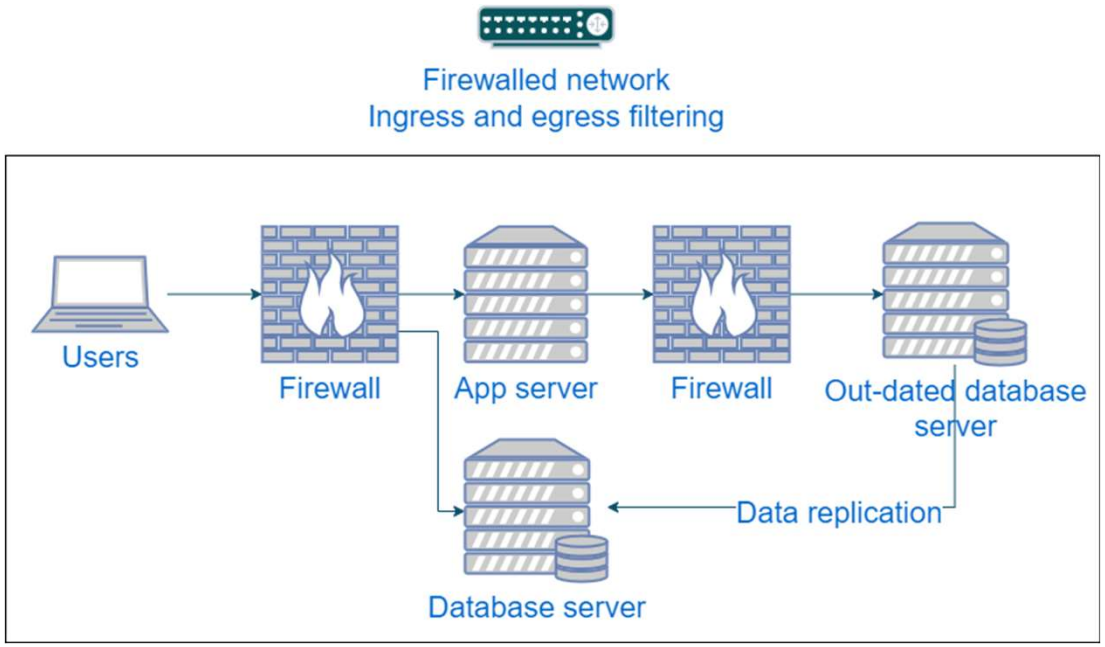
IOT SERVER


Firewalled network
Ingress and egress filtering
IoT Devices
Firewall
SMB version 1
Server
Firewall
Egress filtering

DATABASE SERVER



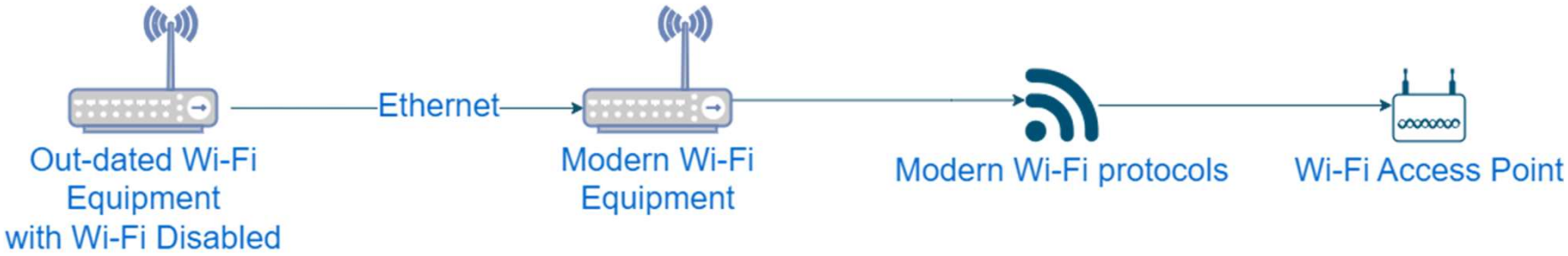
DATABASE SERVER



WI-FI


Out-dated Wi-Fi Equipment
Vulnerable Wi-Fi protocols
Wi-Fi Access Point

WI-FI


Ethernet
Out-dated Wi-Fi Equipment with Wi-Fi Disabled
Modern Wi-Fi Equipment
Modern Wi-Fi protocols
Wi-Fi Access Point

QUESTIONS?

- Questions?