University of Derby

CYBER-PHYSICAL SMART OFFICE: IMPLEMENTATION STRATEGY

Module: 7CS093 Securing Networks

AUT-2025

Created by:

DK0069 (Med Student)

100827271

100828960

Project Scope & Scenario

Scenario: As a CPS Architect for Siemens Technologies UK, this pilot project demonstrates a secure, industrial-grade Smart Office environment.

Key Objectives:

Design: Integrate physical sensors with enterprise IT and "Siemens Cloud Edge."

Secure: Mitigate internal/external threats using AAA, VPNs, and Firewalls.

Connectivity: Establish secure Branch-to-HQ communication for remote CPS control.

Concept: The Cyber-Physical System (CPS)

Definition: A Cyber-Physical System (CPS) integrates sensing, computation, control, and networking into physical objects and infrastructure, connecting them to the Internet and to each other.

The "Smart Office" Vision:

Convergence: Merges the physical office (locks, lights, HVAC) with the digital world (cloud analytics, servers).

Automation: Devices react dynamically to environmental changes (e.g., Anemometer triggering actions) without manual intervention.

Connectivity: Seamless communication between local sensors, the enterprise network, and external cloud services.

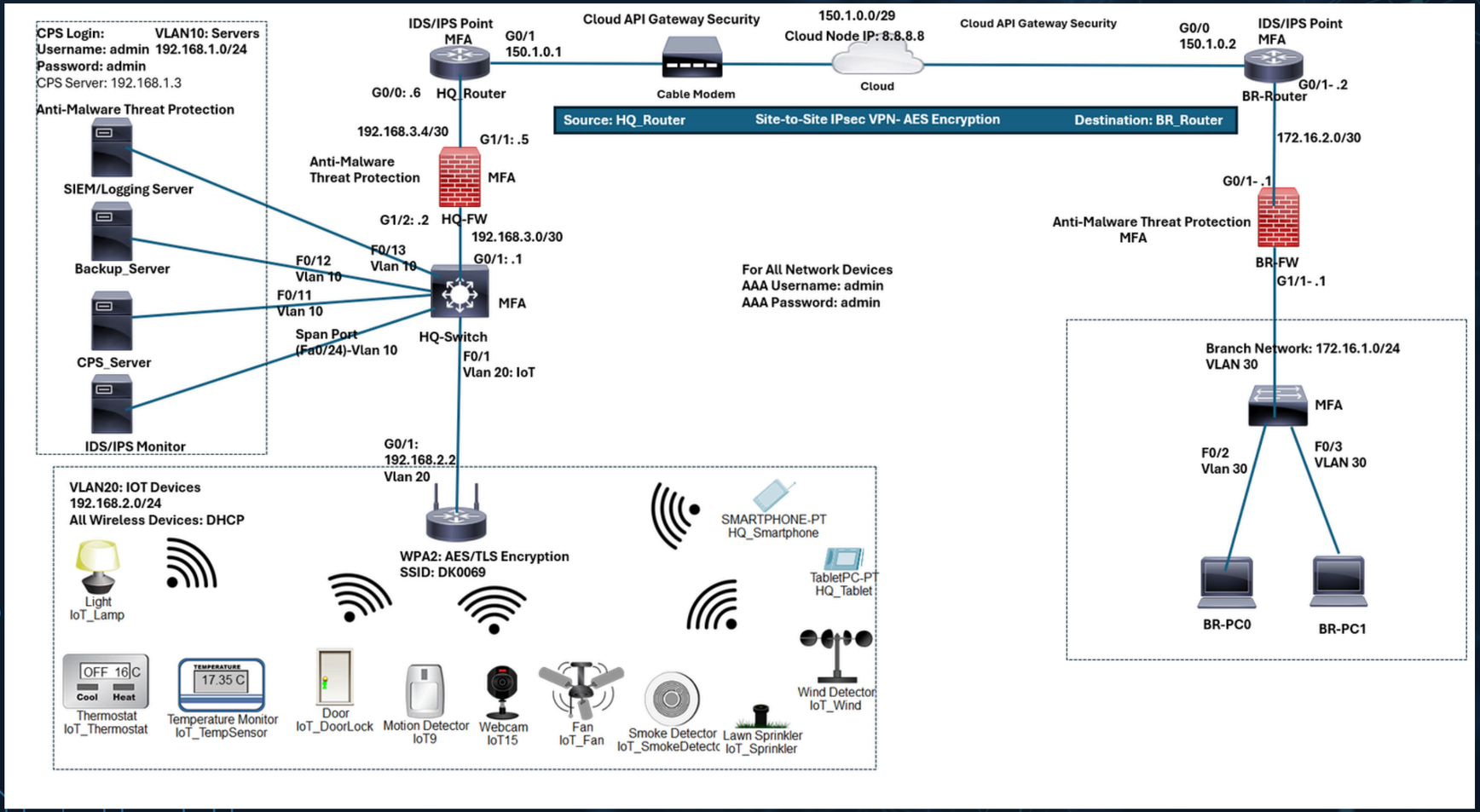
Architectural Layers of the Smart Office

1. Physical Layer (Perception):
Consists of sensors (Motion, Smoke, Temperature) and actuators (Fan, Sprinkler, Door Lock) that interact with the physical environment.

2. Network Layer (Transmission):
Secure transport infrastructure using VLAN segmentation (separating IoT from IT), AES-encrypted Wi-Fi, and IPsec VPNs for secure transit.

3. Application Layer (Processing):
Centralized logic residing on the CPS Registration Server and Siemens Cloud Edge for data analysis, decision making, and remote control via tablets/smartphones.

Smart Office Network Topology



Smart Office Network Topology

Smart Devices Implemented:

Environment: Thermostat, Ceiling Fan, Anemometer (Wind Detector), Sprinkler.

Security: Smart Door Lock, Motion Detector, Smoke Detector, CCTV Camera.

Lighting: Smart Lamp (Dimmable).

Core Infrastructure:

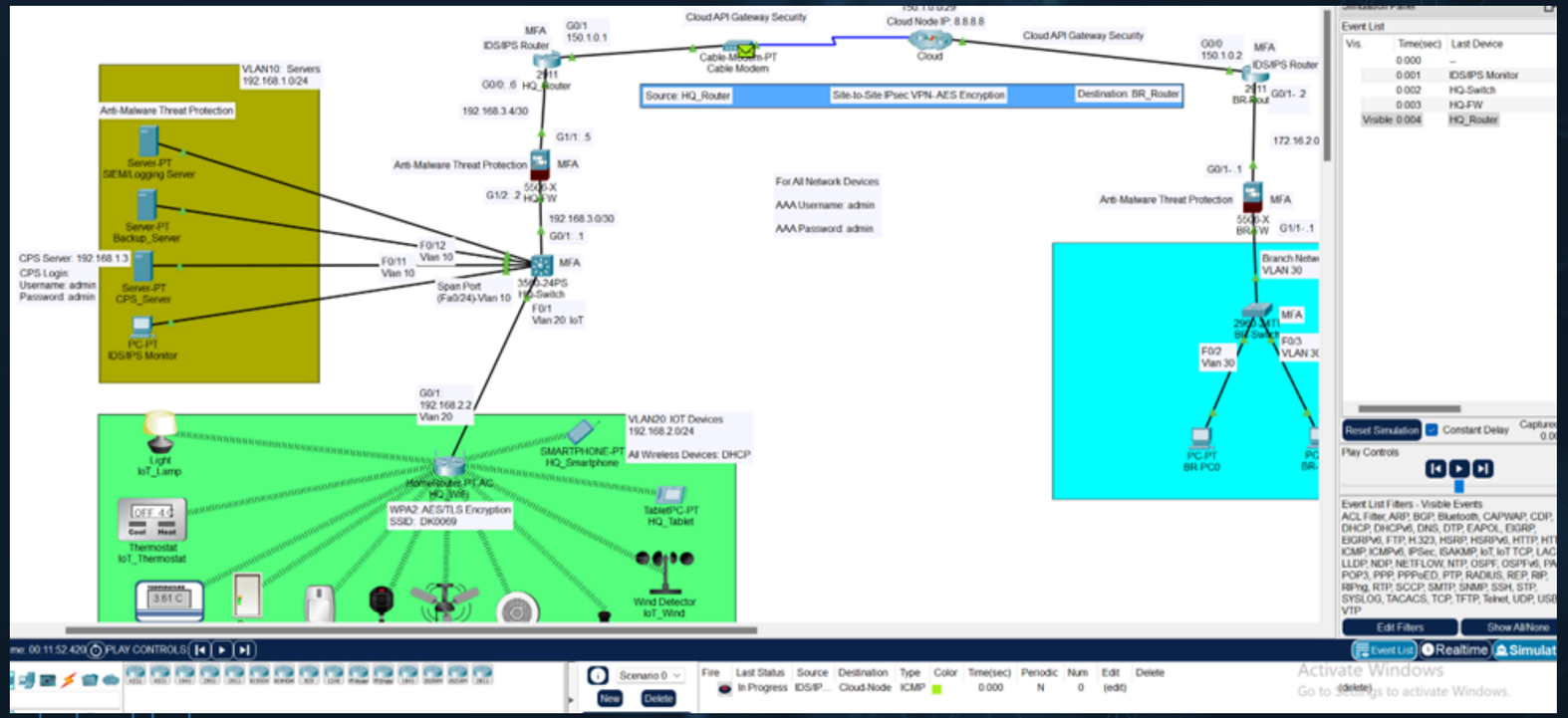
Wireless: Router using WPA2-PSK (AES) encryption.

Management: CPS Registration Server and External Backup Server.

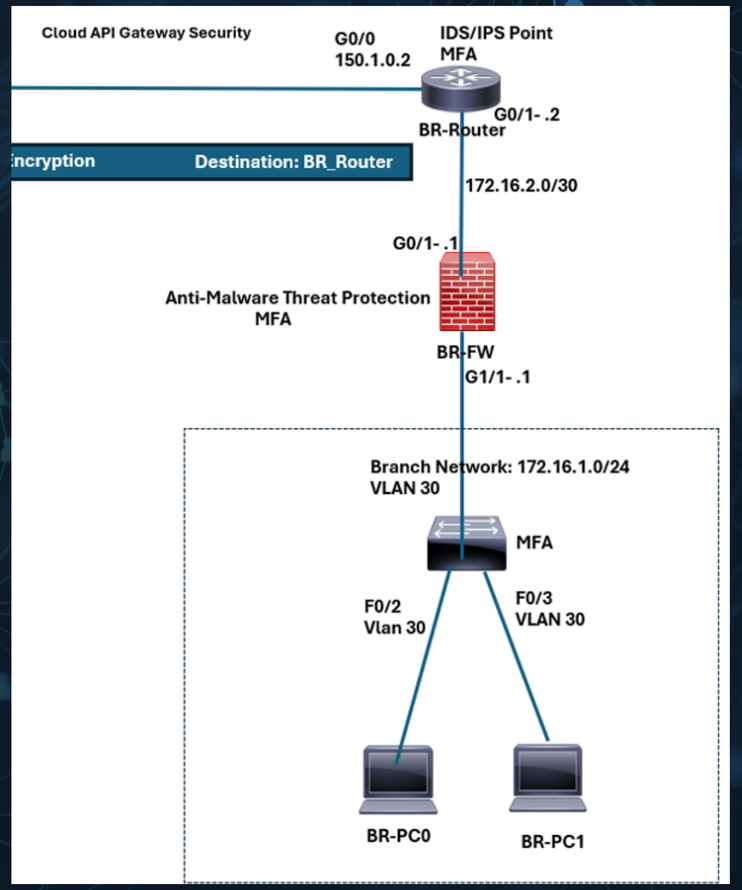
Cloud: Connection to "Siemens Cloud Edge" Cluster via Cable Modem.

Protocol Analysis

Application Layer: HTTP/HTTPS (for IoT web interface control).
DHCP for dynamic IoT IP Addressing.
Transport Layer: TCP (reliable delivery for device commands) or UDP (fast streaming for CCTV).
Network Layer: IP (Routing packets via OSPF between HQ and Cloud).
Link Layer: Ethernet (802.3) and Wi-Fi (802.11) frames carrying the data.



Branch Office Extension



Connectivity Strategy:

Site-to-Site VPN: IPsec tunnel established between HQ and Branch routers.

Encryption: AES encryption ensures data confidentiality over the public internet.

Routing: OSPF configured to share routes dynamically between the two sites.

Outcome: Seamless communication enabling the Branch PC to communicate with the HQ IoT network.

IP Addressing & VLAN Segmentation

Segmentation Strategy:

VLAN 10 (Servers): Isolated critical infrastructure (Siemens Log Server, CPS Server).

VLAN 20 (IoT): Dedicated network for smart devices to prevent congestion and improve security.

VLAN 30 (Branch): Separate broadcast domain for remote office traffic.

Benefit: Prevents broadcast storms and restricts lateral movement if an IoT device is compromised.

IP Addressing & VLAN Segmentation

S/N	Network Segment	VLAN	Network Address /IP Address	Subnet Mask	Valid IP Range	Default Gateway
HQ						
1	HQ Servers	10	192.168.1.0	255.255.255.0	192.168.1.1-192.168.1.254	192.168.1.1
2	HQ IoT	20	192.168.2.0	255.255.255.0	192.168.2.1-192.168.2.254	192.168.2.1
3	HQ-Switch to HQ_FW	NA	192.168.3.0	255.255.255.252	192.168.3.1-192.168.3.2	NA
4	HQ_FW to HQ_Router	NA	192.168.3.4	255.255.255.252	192.168.3.5-192.168.3.6	NA
5	HQ_Router to Cloud	NA	150.1.0.0	255.255.255.248	150.1.0.1-150.1.0.6	NA
BRANCH						
6	Branch	30	172.16.1.0	255.255.255.0	172.16.1.1 – 172.16.1.254	NA
7	BR-FW to BR-Router	NA	172.16.2.0	255.255.255.252	172.16.2.1 – 172.16.2.2	NA
8	BR-Router to Cloud	NA	150.1.0.0	255.255.255.248	150.1.0.1-150.1.0.6	NA
Server / End Device						
9	SIEM /Logging	10	192.168.1.253	255.255.255.0	192.168.1.1-192.168.1.254	192.168.1.1
10	Backup Server	10	192.168.1.2	255.255.255.0	192.168.1.1-192.168.1.254	192.168.1.1
11	CPS Server	10	192.168.1.3	255.255.255.0	192.168.1.1-192.168.1.254	192.168.1.1
12	IDS/IPS Monitor	10	192.168.1.254	255.255.255.0	192.168.1.1-192.168.1.254	192.168.1.1
13	Cloud Node	NA	8.8.8.8	255.0.0.0	8.0.0.1-8.255.255.254	8.8.8.1

Threat Landscape Analysis

External Threats:

- DDoS attacks on the Gateway.
- Man-in-the-Middle (MitM) attacks on the WAN link.
- Brute-force attacks against authentication gateways.

Internal & CPS Threats:

Rogue Devices: Unauthorized sensors connecting to the network.

Sensor Manipulation: e.g., Spoofing temperature data to trigger HVAC errors.

Insider Misuse: Unauthorized employee accessing control panels.

Further threat modeling and remediation actions in regards to network security will be presented on the next part of the project

Thank you for your time!