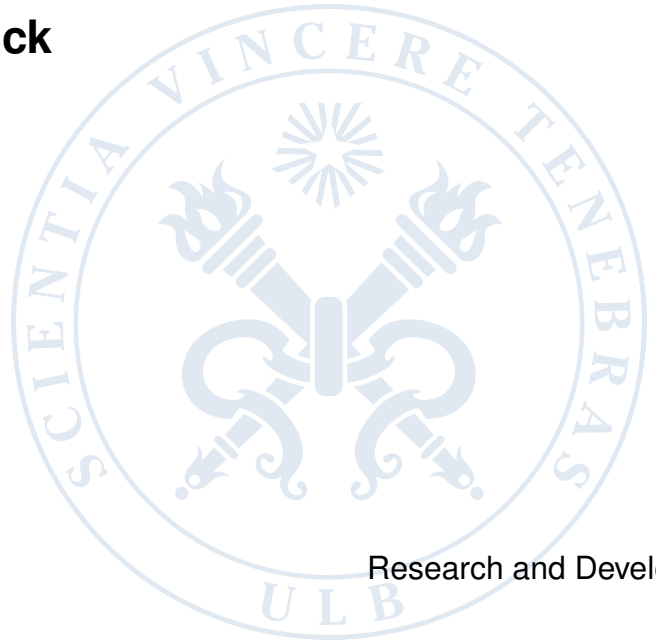
# Deployable Wi-Fi Mesh

## Security Analysis in the context of Military Operation and Festival Management

**Detry Pierrick**



Research and Development project owner:
Cyber Defence Lab

Master thesis submitted under the supervision of
Debatty Thibault

in order to be awarded the Degree of
Master in Cybersecurity
Cryptanalysis and Forensics

Academic year
2024 – 2025

I hereby confirm that this thesis was written independently by myself without the use of any sources beyond those cited, and all passages and ideas taken from other sources are cited accordingly.



18/08/2025

**Title: Deployable Wi-Fi Mesh**

Author: Detry Pierrick
Master in Cybersecurity – Cryptanalysis and Forensics
Academic year: 2024 – 2025

## Abstract

This master's thesis evaluates the feasibility and security of a rapidly deployable Wi-Fi mesh network for temporary environments (e.g., remote military camps and large outdoor festivals). By using solar-powered access points, the architecture enables rapid deployment in the field and significantly reduces installation time compared to traditional wired setups, while maintaining security. This specific design necessitates the use of lightweight, resource-efficient services, given the limited constraints. The study analyzes a Proof of Concept (PoC) developed at the Cyber Defence Lab (CyLab) and proposes a design with targeted mitigations for the most important vulnerabilities.

A literature review covers wireless topologies (repeater-based, mesh, and ad-hoc), along with general and wireless network security. Methodologically, the thesis applies STRIDE for threat modeling, a FAIR-inspired approach for quantitative risk assessment, and maps adversary techniques using MITRE CAPEC. Specific risks (e.g. identity spoofing, deauthentication-based denial of service, and rogue 'evil twin' access points) are assessed in parallel with broader network vulnerabilities. To mitigate these, the work introduces, among other measures, an Intrusion Detection System (IDS) capability and a Security Incident and Event Management (SIEM) capability as baseline controls, comparing candidate implementations to select options suitable for portable and resource-limited deployments.

The initial PoC prioritized functionality over security, exposing typical wireless weaknesses (e.g., management-frame manipulation and weak identity guarantees under WPA2-PSK). The improved design introduces network segmentation (VLANs with policy enforcement), stronger authentication methods, intrusion detection and, where hardware permits, WPA3 with Protected Management Frames (PMF). These measures reduce the attack surface, improve threat detection, and increase operational resilience, without compromising the mesh's rapid-deployment objective. Overall, the results demonstrate that a deployable Wi-Fi mesh can be both agile and defensible when designed with lightweight, field-appropriate controls.

**Keywords:** Wi-Fi, Mesh, Temporary network, Security analysis

# Preface

The pace at which organisations operate continues to accelerate. In military logistics and large public events, this creates a constant pressure to establish network connectivity as quickly as possible. This thesis was motivated by that reality: to examine whether a deployable Wi-Fi mesh network can significantly reduce connection times compared with traditional wired installations while preserving essential security. The aim is not to replace wired networks in terms of raw throughput, but to approach their operational readiness (being faster to set up while avoiding excessive risks).

This work was conducted within the academic context of the Royal Military Academy and in collaboration with the Cyber Defence Lab (CyLab). I visited CyLab's network laboratories to test hardware configurations underlying the PoC evaluated in this thesis.

I hope that these results will serve as a basis for future field deployments of cable-free connectivity when time is short, and that they will be refined through operational experience.

# Acknowledgements

I would like to express my sincere gratitude to the Royal Military Academy for granting me the opportunity to conduct and present this thesis. I am especially thankful to my promotor, Professor Thibaut Debatty, for his valuable guidance, availability, and continuous support throughout the preparation of this work.

I am also deeply grateful to my family, friends, and partner for their encouragement and support until the very end.

# Table of Contents

**Abstracts** **I**
Abstract . . . . . I
**Preface** **II**
**Table of Contents** **V**
**List of Figures** **VI**
**List of Tables** **VI**
**List of Abbreviations** **VII**
**1 Introduction** **1**
1.1 Motivations . . . . . 1
1.2 Project statement & contributions . . . . . 1
1.3 Organisation of this document . . . . . 2
**2 Literature review, state of the art (SotA), definitions and notations** **3**
2.1 Wired vs. Wireless Networks . . . . . 3
2.2 Wireless Network Topologies and Technologies . . . . . 4
2.2.1 Repeater-Based Wireless Networks . . . . . 4
2.2.2 Wireless Mesh Networks . . . . . 5
2.2.3 Ad-Hoc Networks . . . . . 6
2.2.4 Comparison of Deployment Models . . . . . 8
2.3 Security Challenges in Networked Systems . . . . . 9
2.3.1 Threat Modeling . . . . . 10
STRIDE . . . . . 10
Data Flow Diagram (DFD) . . . . . 10
Cyber Kill Chain and Advanced Persistent Threats (APTs) . . 11
Threat Intelligence Frameworks: ATT&CK and CAPEC . . . . 11
Risk assessment with FAIR . . . . . 12
Manage the risks . . . . . 15
Cyber Resilience . . . . . 16
2.3.2 Network Security . . . . . 16
Firewall . . . . . 16
Honeypots . . . . . 17
Network Segmentation . . . . . 17
2.3.3 Monitoring & Logging . . . . . 18
Logging and Event Collection . . . . . 18
Security Information and Event Management (SIEM) . . . . . 19
2.3.4 Wi-Fi Specific Security Considerations . . . . . 19
Wi-Fi Encryption Standards: WPA2, WPA3 . . . . . 19
Deauthentication Attacks . . . . . 20
Evil Twin Wi-Fi Attack . . . . . 21

**3 Initial Proof of Concept** **23**
3.1 Context . . . 23
3.1.1 Problem statement . . . 23
3.2 Requirements . . . 23
3.2.1 Hardware . . . 23
3.2.2 Software . . . 24
3.3 Network Architecture . . . 24
3.4 Preliminary testing . . . 26
3.5 Security posture . . . 26

**4 Security Analysis** **27**
4.1 Scope — What are we working on? . . . 27
4.1.1 Context and Scenario . . . 27
4.1.2 Data Flow Diagram . . . 29
4.1.3 Network Architecture . . . 29
4.2 Threats and risks — What can go wrong? . . . 30
4.2.1 Threat Modeling . . . 30
4.3 Mitigations — What are we going to do about it? . . . 41
4.4 Validation — Did we do a good job? . . . 56
4.4.1 Risk summary . . . 56

**5 Proof of Concept Improvement** **58**
5.1 Intrusion Detection System (IDS) Selection: Snort vs. Suricata vs. Zeek 58
5.2 Security Information and Event Management (SIEM) Selection: Elastic Stack vs. Splunk vs. Security Onion . . . 59
5.3 Key Improvements . . . 61
5.4 Requirements . . . 62

**6 Future Work** **65**

**7 Conclusions** **66**

**Bibliography** **74**

**Appendices** **75**

**A Q&A with a Security Coordinator at Couleur Café Festival** **75**
A.1 Q&A . . . 76

# List of Figures

2.1 Mesh Topology Example . . . 6
2.2 Factor Analysis for Information Risk (FAIR) risk model. . . . 13
2.3 Vulnerability matrix (Threat Capability (TCap) vs. Control Strength (CS)). . . . 14
2.4 Loss Event Frequency matrix (Threat Event Frequency (TEF) vs. Vulnerability). . . . 14
2.5 Risk matrix (Loss Event Frequency (LEF) vs. Probable Loss Magnitude (PLM)). . . . 15

2.6 Sequence Diagram of a Deauthentication Attack . . . . . 21

3.1 Initial PoC network layout (gateway AP/router with satellite nodes and portable power) [51]. . . . . 25

4.1 Data Flow Diagram (DFD) of the initial PoC (festival scenario) . . . . 29
4.2 Initial PoC network architecture (festival scenario). . . . . 30

5.1 Final Network Architecture . . . . . 62

# List of Tables

2.1 Comparison between wired and wireless networks . . . . . 4
2.2 Comparison of wireless network topologies . . . . . 9
2.3 STRIDE Threats per DFD Element . . . . . 10
2.4 Threat Capability scale. . . . . 13
2.5 Control Strength scale. . . . . 13
2.6 Threat Event Frequency (TEF) scale. . . . . 14
2.7 Probable Loss Magnitude buckets used in this thesis. . . . . 14
2.8 Selected differences between Wi-Fi Protected Access 3 (WPA3) and Wi-Fi Protected Access 2 (WPA2), based on [6, 67]. . . . . 20

3.1 Hardware components of the initial PoC . . . . . 24
3.2 Software components of the initial PoC . . . . . 24

4.1 Risk summary per threat: baseline vs. residual (after selected treatments) . . . . . 56
4.2 Resilience levers, effects, and threat coverage . . . . . 57

5.1 Hardware Components Used in the PoC Deployment . . . . . 63
5.2 Software Components Used in the PoC Deployment . . . . . 64

# List of Abbreviations

| | |
|---|---|
| AP | Access Point |
| API | Application Programming Interface |
| APT | Advanced Persistent Threat |
| ARP | Address Resolution Protocol |
| BSSID | Basic Service Set Identifier |
| CAPEC | Common Attack Pattern Enumeration and Classification |
| CIA | Confidentiality Integrity Availability |
| CS | Control Strength |
| DDoS | Distributed Denial of Service |
| DFD | Data Flow Diagram |
| DHCP | Dynamic Host Configuration Protocol |
| DoS | Denial of Service |
| DPI | Deep Packet Inspection |
| DWFM | Deployable Wi-Fi Mesh |
| FAIR | Factor Analysis for Information Risk |
| HIDS | Host-based Intrusion Detection System |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IT | Information Technology |
| KVM | Kernel-based Virtual Machine |
| LAN | Local Area Network |
| LEF | Loss Event Frequency |
| MAC | Medium Access Control |
| MANET | Mobile Ad-hoc Network |
| MDBF | Mean Distance Between Failures |
| MitM | Man in the Middle |
| NIDS | Network-based Intrusion Detection System |
| NSM | Network Security Monitoring |
| NTP | Network Time Protocol |
| PLM | Probable Loss Magnitude |
| PMF | Protected Management Frames |
| PoC | Proof of Concept |
| PoE | Power over Ethernet |
| PSK | Pre-Shared Key |
| SIEM | Security Incident and Event Management |
| SSID | Service Set Identifier |
| TCap | Threat Capability |
| TEF | Threat Event Frequency |
| VLAN | Virtual Local Area Network |
| VM | Virtual Machine |
| VoIP | Voice over IP |

| | |
|---|---|
| Vuln | Vulnerability |
| WDS | Wireless Distribution System |
| WEP | Wired Equivalent Privacy |
| WIDS | Wireless Intrusion Detection System |
| WLAN | Wireless Local Area Network |
| WMN | Wireless Mesh Network |
| WPA | Wi-Fi Protected Access |
| WPA2 | Wi-Fi Protected Access 2 |
| WPA3 | Wi-Fi Protected Access 3 |

# Chapter 1
# Introduction

## 1.1 Motivations

In scenarios such as military operations and large-scale events, it can be valuable to have the option to rapidly deploy a network with minimal infrastructure while preserving baseline security. This thesis explores the feasibility of a **Deployable Wi-Fi Mesh (DWFM)** solution built around solar-powered Wi-Fi Access Points (APs), portable servers (e.g., flyaway racks), and a lean security stack.

The objective is to analyse and improve a PoC designed to be:

1. quickly deployable,
2. easily manageable,
3. secure and resilient.

By eliminating most data cabling to endpoints, preconfiguring essential services (firewall, monitoring, access control) and templating device images, a deployable mesh network can reduce installation time compared to traditional wired deployments while maintaining a defensible security posture.

Using wireless instead of wired changes the threat surface: the broadcast medium introduces Wi-Fi–specific risks (e.g., spoofing, deauthentication, and "evil twin" AP) in addition to general network threats. Accordingly, the design leverages WPA3 with PMF where supported, network segmentation, and centralised monitoring with an IDS to maintain visibility and limit lateral movement. Segmentation over Wi-Fi is achieved by mapping role-based Service Set Identifiers (SSIDs) to Virtual Local Area Networks (VLANs), trunking these to the firewall, and enforcing inter-VLAN policy. Bandwidth management (prioritisation) protects critical services such as payments and security video under congestion. These principles guide the analysis and improvements developed in later chapters.

## 1.2 Project statement & contributions

The objective is to investigate the security challenges of a deployable Wi-Fi mesh, assess risks using STRIDE and a FAIR-inspired, semi-quantitative approach, and propose a secure, easily deployable design with low operational overhead.

The scope is temporary, cable-light deployments that prioritise availability, and observability (e.g., festivals, exercises). Endpoints include cameras, administrative devices, and payment terminal. No full field trial was performed.

What this thesis provides:

- A structured threat model (STRIDE with DFD) and a FAIR-inspired, semi-quantitative risk assessment tailored to the PoC's operational context, with CAPEC mappings to representative adversary techniques.

- An Enhanced architecture introducing VLAN-based segmentation with inter-VLAN policy enforcement, centralised logging and monitoring, and an intrusion detection capability, with WPA3 and Protected Management Frames (802.11w) where supported.
- An evaluation of IDS (Snort, Suricata, Zeek) and SIEM/monitoring options with emphasis on portability and resource footprint, resulting in field-tailored software and curated detections.
- An improved PoC moving from locally managed Wireless Distribution System (WDS) links to a controller-managed mesh (Netgear Insight Premium), with deployment guidance and templated configurations for rapid setup.
- Configuration artefacts (e.g., a pfSense backup including Network Time Protocol (NTP), failover, VLAN segmentation, and IDS integration), plus installation notes to reproduce the improved design, provided in the accompanying GitHub repository.

Future work includes a live field pilot with metrics, environmental and weatherisation validation (panel/AP placement, mounting, ingress protection), endpoint power distribution beyond APs, and a formal red-team pentest. These items are prioritised in Chapter 6 (*Future Work*).

## 1.3 Organisation of this document

This thesis is organised as follows. Chapter 2 surveys the literature on wired versus wireless networking, wireless network topologies (repeater-based, mesh, and ad hoc) and the security frameworks used throughout (STRIDE/DFD, Cyber Kill Chain, ATT&CK/CAPEC and FAIR), as well as core controls (firewalls, IDS/Intrusion Prevention System (IPS), SIEM, Wi-Fi protections). Chapter 3 documents the initial PoC (context, requirements, architecture, preliminary tests, and baseline security posture) built with locally managed APs and WDS-style links. Chapter 4 develops the security analysis, defining scope and assumptions, modelling data flows using a DFD, applying STRIDE with a FAIR-inspired assessment, and deriving mitigations under a cyber-resilience lens. Chapter 5 presents the improved solution: a controller-managed mesh (via Netgear Insight Premium), network segmentation, centralised logging and monitoring, and IDS/SIEM integration, with deployment guidance. Chapter 6 outlines future work, including a live pilot, adversarial testing (pentest), environmental placement and weatherisation of APs and solar panels, power delivery for endpoints, broader threat coverage, and log-integrity protections. Chapter 7 concludes with a synthesis of findings, an answer to the research question, and a summary of contributions and limitations.

# Chapter 2
# Literature review, state of the art (SotA), definitions and notations

This chapter surveys the literature to provide the conceptual and technical foundations for a secure DWFM. It contextualises the problem within wireless networking, clarifies terminology and notation, and situates the work in the state of the art. We first contrast wired and wireless media to frame the core trade-offs in bandwidth, latency, reliability, and deployment effort. We then review wireless topologies (repeater-based, mesh, and ad hoc/Mobile Ad-hoc Networks (MANETs)) highlighting where each is most suitable and the implications for a rapidly deployable design.

Because deployable networks must be deployable quickly, withstand environmental constraints, be simple to configure, and remain secure, we examine the security properties and threats specific to Wi-Fi (e.g., spoofing, deauthentication, "evil twin"), alongside general network risks. We introduce the analysis frameworks used throughout the thesis (STRIDE with DFD, ATT&CK/CAPEC, FAIR) and synthesise the network security mechanisms most relevant to the design: firewalls, IDS/IPS, honeypots, network segmentation, and monitoring and logging.

In summary, this chapter clarifies terminology, contrasts relevant wireless topologies, and reviews security frameworks and controls for deployable meshes.

## 2.1 Wired vs. Wireless Networks

Before focusing on wireless technologies, it is useful to distinguish the two broad categories of network transmission media: wired and wireless. Each type of network offers distinct characteristics that influence performance, security, reliability, and deployment complexity.

Wired networks rely on physical cabling (e.g., Ethernet or fiber-optic) interconnect devices, while wireless networks use radio spectrum (e.g., Wi-Fi) to transmit data through the air. These differences play a critical role in how networks are deployed and managed.

Table 2.1 presents a comparative overview of wired and wireless networks across several important technical dimensions [30, 37, 72].

| Aspect | Wired network | Wireless network |
|---|---|---|
| **Bandwidth and latency** | High speed, low latency and predictable throughput | Lower and more variable throughput. Shared spectrum and contention reduce capacity. |
| **Reliability** | Not affected by RF interference, failures are usually cable or port faults | Sensitive to interference, congestion, obstacles and placement. Link quality varies with environment and load. |
| **Security exposure** | Physical access is usually required to tap links. Layer 2 attacks remain possible. Segmentation is enforced in switches and the firewall. | Traffic is exposed over the air. Strong authentication and encryption are required. Use WPA3 with Protected Management Frames and 802.1X where possible, and consider WIDS. |
| **Mobility** | Limited to physical connection | Native mobility within coverage, roaming between APs is supported. |
| **Installation and cost** | Higher effort for pathway planning and cable pulls | Faster to deploy for temporary sites, focus on AP placement and quick mounting |
| **Scalability and capacity** | Scales with switch fabric and cabling, capacity additions are predictable | Constrained by shared spectrum and channel reuse. AP density is limited by co-channel interference. |
| **Cabling** | Extensive data cabling, Power over Ethernet (PoE) or separate power runs | Minimal data cabling. Power cabling for APs and some endpoints is still required unless battery or solar is used. |

Table 2.1: Comparison between wired and wireless networks

## 2.2 Wireless Network Topologies and Technologies

Designing a wireless network to cover a specific area can involve various technological approaches, depending on performance requirements, environmental constraints, budget, and scalability. Among the most common solutions [36] are **repeater-based configurations**, **wireless mesh networks**, and **ad-hoc networks**. Each of these topologies presents distinct advantages and trade-offs in terms of coverage, reliability, complexity, and deployment flexibility.

This section first introduces repeater-based networks as a basic form of wireless extension, followed by a discussion of wireless mesh networks and ad-hoc networks, which offer greater flexibility and scalability.

### 2.2.1 Repeater-Based Wireless Networks

Repeater-based networks represent one of the most straightforward methods for wireless extension. A repeater receives a wireless signal from an existing AP, amplifies it, and retransmits it to reach areas with weak or no signal. This approach is particularly useful in small-scale environments or where deploying additional wired APs is impractical [31,56].

Repeaters serve as a basic form of wireless extension, effectively increasing the coverage

area of a single access point without requiring complex configuration or infrastructure changes. However, this simplicity comes with trade-offs.

- **Advantages:** Easy to configure. Requires minimal equipment. Cost-effective for basic range extension.

- **Limitations:** Introduces additional latency. Reduces available bandwidth by approximately half at each hop. Lacks dynamic routing, redundancy, or advanced management features.

### 2.2.2 Wireless Mesh Networks

A Wireless Mesh Network (WMN) consists of multiple interconnected nodes that collaboratively provide seamless and resilient wireless coverage. Unlike traditional networks that rely on a central access point, WMNs distribute traffic dynamically across multiple paths, enhancing fault tolerance and coverage consistency [35, 74].

The IEEE 802.11s standard, developed by Task Group S, specifically addresses mesh networking for Wireless Local Area Networks (WLANs). This amendment introduces wireless frame forwarding and routing capabilities at the Medium Access Control (MAC) layer, differentiating it from IP-based WMNs that rely on higher layers for multihop communication. The 802.11s concept aims to make WMNs appear like traditional Local Area Network (LAN) segments, forming single broadcast domains for transparent support of protocols like Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and Spanning Tree Protocol [4, 32].

Mesh routing protocols are designed to optimize bandwidth usage by dynamically selecting efficient paths and avoiding congested links. This contributes to better overall throughput and network performance, especially in dense or high-traffic environments.

The 802.11s standard defines specific components:

- **Mesh Nodes:** Devices that form the mesh backbone by forwarding data and managing network traffic between nodes.

- **Mesh Clients:** End-user devices, such as smartphones and laptops, that connect to the network through mesh nodes.

- **Gateways:** Nodes that connect the mesh network to external networks, such as the Internet.

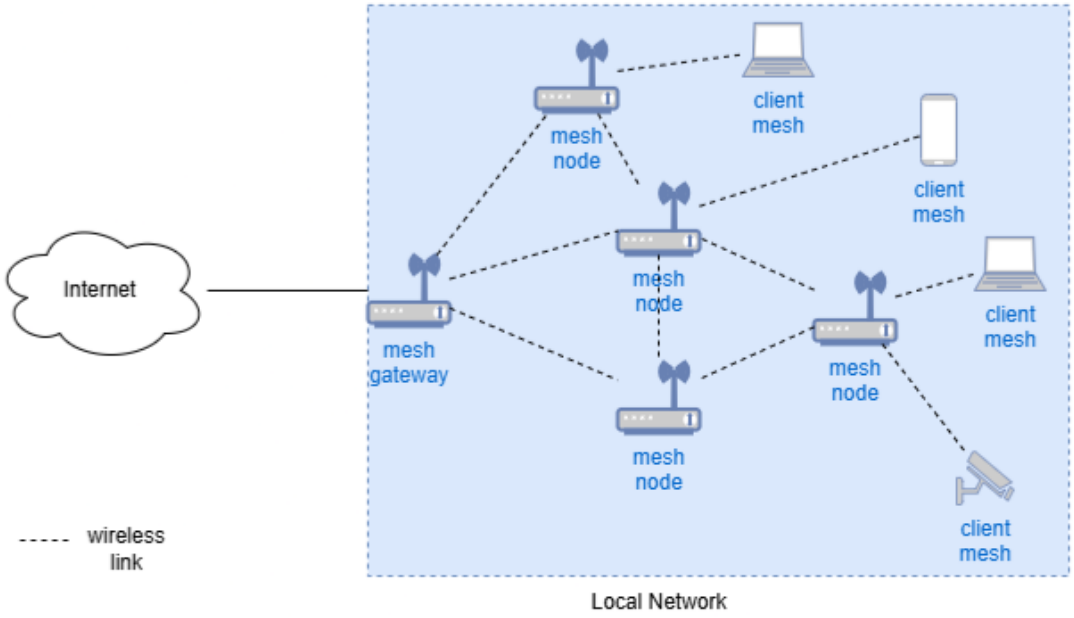



Figure 2.1: Mesh Topology Example

### Use Cases of Wireless Mesh Networks

Wireless mesh networks are particularly valuable in scenarios where traditional wired or single-hop wireless solutions are inadequate. Notable applications include:

- **Disaster and Emergency Response:** IEEE 802.11s mesh networks provide a rapidly deployable and cost-effective communication infrastructure when conventional systems are unavailable. They enable first responders to quickly establish connectivity in remote or disaster-stricken areas, facilitating timely coordination and data exchange [9, 23].
- **Extending WLAN Coverage:** Mesh networks allow for the flexible and scalable expansion of WLANs beyond the reach of wired infrastructure. They are effective in indoor environments, such as multi-floor buildings, and support large-scale urban deployments through self-organizing, multi-hop topologies [10, 39].

In conclusion, mesh networks represent a significant advancement in wireless communication, offering robust, adaptable, and self-managing solutions for a wide range of demanding use cases.

### 2.2.3 Ad-Hoc Networks

Ad-hoc networks are decentralized wireless systems that operate without fixed infrastructure or centralized administration. The term *ad hoc*, Latin for "for this purpose," reflects their ability to be deployed spontaneously in response to immediate communication needs [75]. Devices in such networks—ranging from laptops and smartphones to IoT sensors—communicate directly in a peer-to-peer fashion, forming a dynamic and self-organizing topology.

Each node in an ad-hoc network typically functions both as a host and a router, enabling multi-hop communication. When two nodes are not within direct range, data is relayed through intermediate nodes. This self-configuring and self-healing nature allows the network to adapt to node mobility, failures, or environmental changes [58].

Routing in ad-hoc networks is particularly challenging due to frequent topology changes and limited resources. Protocols such as AODV (Ad hoc On-Demand Distance Vector) and DSR (Dynamic Source Routing) are widely used to establish efficient routes with minimal overhead [20]. These protocols are reactive, initiating route discovery only when needed, which conserves bandwidth and energy.

Unlike mesh networks, ad-hoc networks are not governed by a unified standard. Instead, they rely on a variety of routing protocols and implementations, which can vary depending on the application domain and device capabilities. Bandwidth efficiency in ad-hoc networks is highly dependent on the routing protocol and network density, and may degrade under high mobility or congestion.

Ad-hoc networks can be:

- **Homogeneous:** All nodes have similar capabilities.
- **Heterogeneous:** Nodes vary in power, range, and processing capacity.

### Mobile Ad-Hoc Networks (MANETs)

MANETs are a subclass of ad-hoc networks where mobile nodes autonomously establish and maintain wireless communication. Their infrastructure-free and decentralized nature makes them ideal for scenarios requiring rapid deployment and adaptability. Common applications include:

- **Military and Tactical Operations:** MANETs are crucial for battlefield communication where infrastructure is unavailable or compromised. They support high mobility, frequency diversity, and secure multicast communication [57].
- **Disaster Relief:** Used to restore communication in areas affected by natural disasters where traditional infrastructure is damaged [63].
- **Environmental Monitoring:** Deployed in forests, oceans, or urban areas for sensor data collection and surveillance [63].
- **Vehicular Networks (VANETs):** Enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication for traffic safety and autonomous driving [59].

Other related architectures include Smartphone Ad Hoc Networks (SPANs) and Wireless Sensor Networks (WSNs), each tailored to specific use cases and device capabilities.

### Advantages and Limitations

Ad-hoc networks offer several advantages:

- Rapid and flexible deployment

- Cost-efficiency (no infrastructure required)
- Scalability and fault tolerance

However, they also face critical limitations:

- **Security vulnerabilities:** Susceptible to spoofing, eavesdropping, and denial-of-service attacks.
- **Resource constraints:** Limited battery, processing power, and bandwidth.
- **Routing complexity:** Frequent topology changes increase protocol overhead and latency.
- **Interference and range limitations:** Especially in dense or noisy environments.

Despite these challenges, ad-hoc networks remain a foundational concept in wireless communication, with ongoing research focused on improving their efficiency, security, and scalability.

### 2.2.4 Comparison of Deployment Models

The table below highlights the key differences [1, 3, 5, 7, 18, 70, 72]:

Table 2.2: Comparison of wireless network topologies

| Aspect | Repeater-based networks | Wireless mesh networks (WMNs) | Ad hoc / MANET |
|---|---|---|---|
| **Infrastructure** | Central AP with one or more repeaters/extenders | Gateways and mesh nodes, controller optional depending on vendor | No fixed infrastructure, peers form links on demand |
| **Routing** | Layer-2 bridging to the uplink AP, no independent routing in repeaters | Dynamic L2/L3 routing in the mesh (e.g., 802.11s HWMP or vendor-specific) | Network-layer MANET routing (e.g., OLSR, AODV, DSR) |
| **Deployment complexity** | Very low for quick range extension | Moderate to high (site survey, channel planning, controller policies) | Low to moderate (node configuration and peering) |
| **Scalability** | Limited hop count and single uplink path | High with self-healing and multiple paths when designed well | Moderate control-plane overhead grows with size |
| **Bandwidth efficiency** | Single-radio hops share airtime, effective throughput typically halves per hop | Per-hop airtime cost mitigated by multi-radio/multi-channel designs, still lower than wired backbones | Variable contention and hidden terminals can reduce capacity |
| **Fault tolerance** | Low path failure breaks coverage beyond the repeater | High redundant paths enable self-healing around failed nodes/links | Moderate some self-healing depending on protocol |
| **Typical use cases** | Small venues and basic coverage extension | Campus/municipal Wi-Fi, temporary events, emergency response | Tactical and disaster relief networks, IoT/sensor swarms |
| **Standardisation** | 802.11 WDS and vendor-specific implementations | IEEE 802.11s meshes and vendor-managed meshes | 802.11 IBSS plus IETF MANET protocols (no single IEEE mesh standard for MANET) |

## 2.3 Security Challenges in Networked Systems

Wireless networks broaden the attack surface because communications occur over a shared medium and endpoints can be reached from outside the physical perimeter. In addition to general network risks, this includes Wi-Fi–specific exposures.

To analyse these risks at a high level, we refer to established threat-modelling and risk frameworks. Specifically, we use STRIDE with a DFD to structure threat identification, relate threats to observed techniques via threat intelligence (e.g., MITRE ATT&CK/CAPEC), and apply a FAIR-inspired, semi-quantitative view to prioritise them. We then outline the

security building blocks used to mitigate the identified threats.

### 2.3.1 Threat Modeling

Threat modeling is a structured approach to identifying potential security issues within a system. It helps anticipate how an attacker might compromise a system and guides the implementation of appropriate countermeasures [55]. One of the most widely used methodologies for threat modeling is STRIDE, which is often applied in conjunction with DFDs to visualize and analyze system components and interactions.

#### STRIDE

The STRIDE model [44] provides a taxonomy that classifies threats into six categories:

- **S – Spoofing Identity:** Illegitimately accessing the system by impersonating another user or device.
- **T – Tampering with Data:** Unauthorized modification of data, configurations, or network traffic.
- **R – Repudiation:** Performing actions without the ability to trace or prove responsibility, often due to insufficient logging or auditing.
- **I – Information Disclosure:** Exposure of confidential data to unauthorized parties, typically through interception or misconfiguration.
- **D – Denial of Service (DoS):** Disrupting the availability of services by overloading the system or attacking key components.
- **E – Elevation of Privilege:** Gaining unauthorized access rights by exploiting vulnerabilities or misconfigurations.

Using STRIDE provides a systematic way to enumerate vulnerabilities across assets and trust boundaries and establishes a clear basis for deriving security requirements and countermeasures.

#### Data Flow Diagram (DFD)

To apply STRIDE effectively, it is common to use a **Data Flow Diagram (DFD)** [54] to model the system's architecture. A DFD represents the flow of data between different components, such as external entities, processes, data stores, and communication channels. Each of these elements can be analyzed for specific STRIDE threats using the **STRIDE-per-element** approach [22].

Table 2.3: STRIDE Threats per DFD Element

| DFD Element | S | T | R | I | D | E |
|---|---|---|---|---|---|---|
| **External Entity** | v | | v | | | |
| **Process** | v | v | v | v | v | v |
| **Data Store** | | v | | v | v | |
| **Data Flow** | | v | ? | v | v | |

**Legend:** S = Spoofing, T = Tampering, R = Repudiation, I = Information Disclosure, D = Denial of Service, E = Elevation of Privilege

By systematically applying STRIDE to each element in the DFD, security analysts can identify and prioritise threats, guiding the implementation of mitigations such as authentication, encryption, access control, and logging.

### Cyber Kill Chain and Advanced Persistent Threats (APTs)

While STRIDE helps categorise the types of threats a system may face, the Cyber Kill Chain model, developed by Lockheed Martin, outlines the typical stages of a cyberattack. This model is particularly relevant in understanding multi-step attacks such as APT. [41]

The Cyber Kill Chain consists of the following stages:

1. **Reconnaissance:** Gathering information about the target system or environment.
2. **Weaponization:** Crafting a malicious payload tailored to exploit a specific vulnerability.
3. **Delivery:** Transmitting the payload to the target (e.g., via email, USB, website).
4. **Exploitation:** Triggering the vulnerability to execute malicious code.
5. **Installation:** Installing malware or backdoors to maintain access.
6. **Command and Control (C2):** Establishing communication between the attacker and the compromised system.
7. **Actions on Objectives:** Executing the final goal, such as data exfiltration or disruption.

**Definition**

**Command and Control (C2)** refers to the communication channel established by an adversary to remotely manage compromised systems within a target network. A C2 server, controlled by the attacker, allows infected machines to receive instructions or exfiltrate stolen data. To evade detection, malware often embeds domain names or IP addresses and uses widely used protocols like HTTPS to mimic legitimate traffic. [45]

**Advanced Persistent Threats (APTs):** APTs are stealthy, long-term cyberattacks that typically use the Kill Chain stages. They are often conducted by well-resourced attackers and may target mesh networks to maintain undetected access, intercept communications, or manipulate devices such as cameras or access points. APTs are especially concerning in temporary, wireless-heavy environments like deployable mesh networks, where visibility and control may be limited.

Understanding both STRIDE and the Cyber Kill Chain provides a comprehensive foundation for analysing, detecting, and mitigating potential attacks in an infrastructure.

### Threat Intelligence Frameworks: ATT&CK and CAPEC

To further enhance threat modeling and risk assessment, threat intelligence frameworks like MITRE ATT&CK and CAPEC offer detailed knowledge about adversarial behavior and tactics.

**MITRE ATT&CK:** The MITRE ATT&CK[1] (Adversarial Tactics, Techniques, and Common Knowledge) framework is a curated knowledge base of adversary tactics and techniques based on real-world observations. It maps out how attackers operate during and after a compromise, aligning closely with the stages of the Cyber Kill Chain.

Each technique in ATT&CK includes:

- Description of the behavior
- Known threat actors using it
- Detection strategies
- Potential mitigations

**Common Attack Pattern Enumeration and Classification (CAPEC):** [2] A publicly maintained catalogue of known attack patterns that describes how adversaries execute attacks. CAPEC focuses on preconditions, execution steps, and intended outcomes, and it links patterns to relevant weaknesses and mitigations. .

**Summary:** Using ATT&CK and CAPEC alongside STRIDE and the Cyber Kill Chain enables a multi-dimensional view of threats:

- **STRIDE** categorises threat types.
- **Cyber Kill Chain** describes the attacker workflow.
- **ATT&CK** shows real-world tactics and techniques.
- **CAPEC** explains reusable attack patterns and methodology.

This comprehensive approach helps in building resilient architectures and identifying potential vulnerabilities specific to wireless mesh network environments.

### Risk assessment with FAIR

Risk assessment approaches range from qualitative (expert judgement) to quantitative (numerical estimates). In this thesis, we follow the method of [41], which is based on the FAIR framework (Factor Analysis of Information Risk), to structure and semi-quantitatively assess risk. Concretely, we use FAIR's canonical factors with ordinal ratings (e.g., VL, L, M, H, VH) rather than exact probabilities. This provides consistency and traceability across threats while remaining practical for a deployable PoC. All tables and heatmaps below are adapted from [41]. See also the FAIR Institute overview.[3] While more quantitative models can offer greater precision, they still rely on estimates and assumptions.

**From STRIDE to FAIR.** STRIDE (with the DFD) identifies *what* can go wrong and *where*. FAIR then estimates *how likely* and *how severe* those events are by rating the factors below, leading to a final risk magnitude.

Figure 2.2 shows the FAIR decomposition we use to rate each scenario.

[1] `https://attack.mitre.org/`
[2] `https://capec.mitre.org/`
[3] `https://www.fairinstitute.org/what-is-fair`

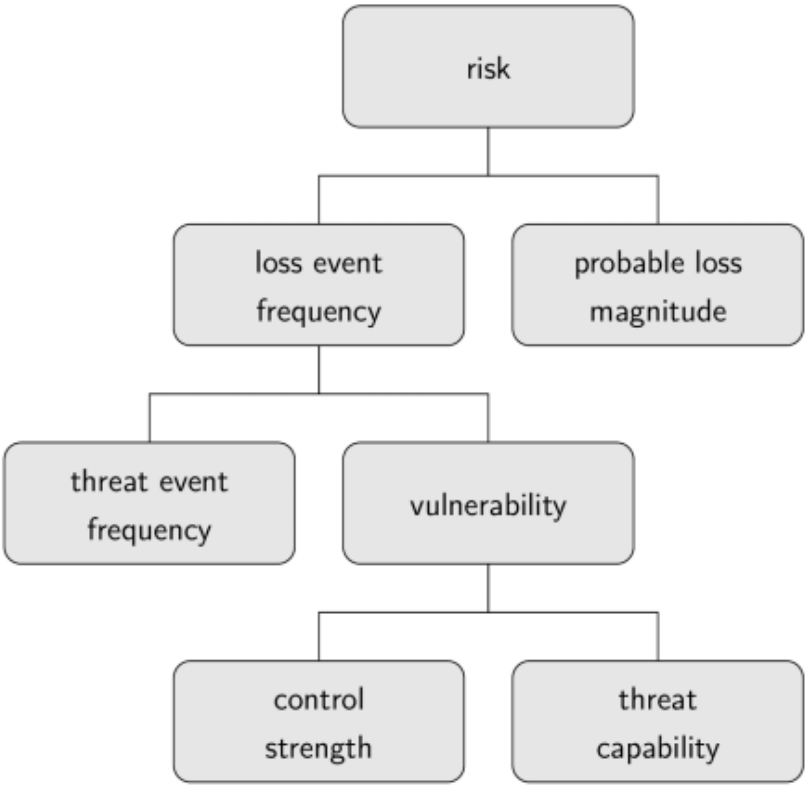



Figure 2.2: FAIR risk model.

**Threat Capability (TCap).** Level of force/skill/resources the threat agent can apply.

| Rating | Description |
|---|---|
| Very High (VH) | top 2% of the overall threat population |
| High (H) | top 16% of the overall threat population |
| Moderate (M) | average (between top 16% and bottom 16%) |
| Low (L) | bottom 16% of the overall threat population |
| Very Low (VL) | bottom 2% of the overall threat population |

Table 2.4: Threat Capability scale.

**Control Strength (CS).** Difficulty the environment imposes on the threat agent.

| Rating | Description |
|---|---|
| Very High (VH) | stops all but the top 2% of threat agents |
| High (H) | stops all but the top 16% |
| Moderate (M) | effective against the average threat agent |
| Low (L) | only stops the bottom 16% |
| Very Low (VL) | only stops the bottom 2% |

Table 2.5: Control Strength scale.

**Vulnerability (Vuln).** Probability a threat event becomes a loss event, derived from TCap vs. CS.

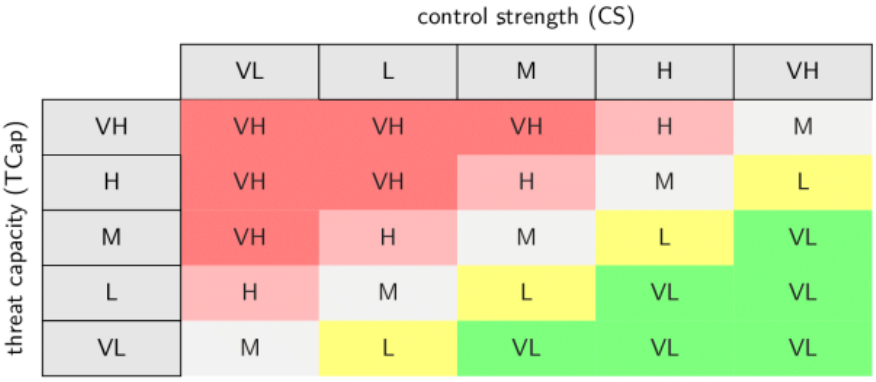



Figure 2.3: Vulnerability matrix (TCap vs. CS).

**Threat Event Frequency (TEF).** Expected frequency of relevant threat actions.

| Rating | Per year (events/yr) |
|---|---|
| Very High (VH) | $> 100$ |
| High (H) | 10–100 |
| Moderate (M) | 1–10 |
| Low (L) | 0.1–1 |
| Very Low (VL) | $< 0.1$ |

Table 2.6: Threat Event Frequency (TEF) scale.

**Loss Event Frequency (LEF).** Frequency of realized loss, driven by  and Vulnerability.

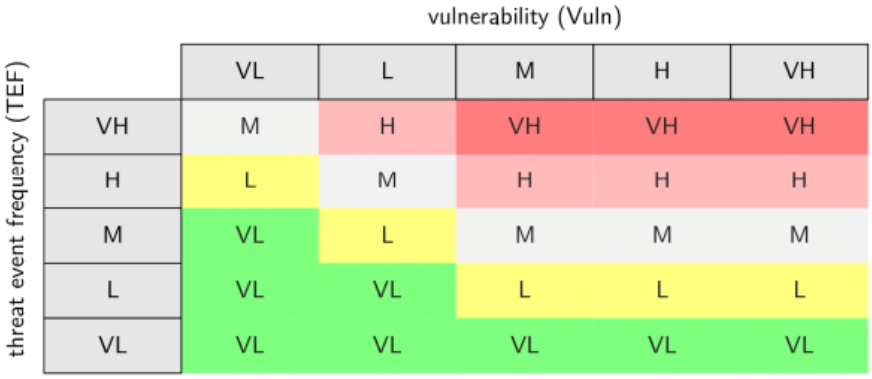



Figure 2.4: Loss Event Frequency matrix (TEF vs. Vulnerability).

**Probable Loss Magnitude (PLM).** Estimated impact of a realized loss (order-of-magnitude buckets).

| Magnitude | Range (EUR order of magnitude) |
|---|---|
| Severe (Sv) | $\geq 10.000.000$ |
| High (H) | 1.000.000 – 9.999.999 |
| Significant (Sg) | 100.000 – 999.999 |
| Moderate (M) | 10.000 – 99.999 |
| Low (L) | 1.000 – 9.999 |
| Very Low (VL) | $< 1.000$ |

Table 2.7: Probable Loss Magnitude buckets used in this thesis.

**Risk.** Combined function of LEF and PLM. In the heatmap below, **C** denotes *Critical*. Colors follow the usual convention (yellow = Low, grey = Medium, light red = High and red = Critical).

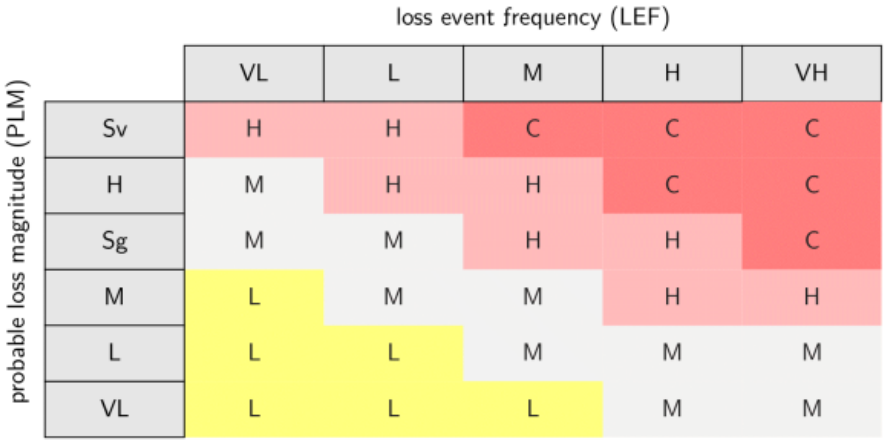



Figure 2.5: Risk matrix (LEF vs. PLM).

### Manage the risks

Once risks have been assessed using the FAIR methodology, organizations must decide how to respond to them. Risk management strategies are typically categorized into four main approaches [24, 47]:

- **Risk Avoidance** – *Eliminate the risk entirely.* This involves changing business processes, technologies, or practices to remove the conditions that give rise to the risk.
- **Risk Mitigation** – *Reduce the likelihood or impact of the risk.* This is achieved by implementing technical, administrative, or physical controls to lower the probability of a threat event or its potential consequences.
- **Risk Transfer** – *Shift the risk to a third party.* This can be done through mechanisms such as insurance, outsourcing, or contractual agreements that assign responsibility for certain risks to external entities.
- **Risk Acceptance** – *Acknowledge and tolerate the risk.* This is appropriate when the cost of mitigation exceeds the expected loss, or when the risk falls within the organization's defined risk tolerance.

The choice of strategy depends on the organization's risk appetite, regulatory requirements, and available resources. In practice, a combination of these strategies is often employed to achieve a balanced and cost-effective risk posture [40].

To support this process, a risk treatment plan is typically developed. This plan maps each identified risk to a response strategy, assigns responsibilities, and defines implementation timelines. It should be reviewed regularly to reflect changes in the threat landscape and organizational priorities.

### Cyber Resilience

Cyber resilience is broadly defined as an entity's ability to continue operating amid, and recover from, adverse cyber events. According to NIST, it is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources" [62].

In practical terms, cyber resilience means preparing for incidents, maintaining critical functions during disruptions, and restoring normal operations quickly with minimal impact on users or mission objectives. The concept extends traditional cybersecurity—focused on prevention and detection—by explicitly assuming some attacks or failures will succeed and by emphasising robustness and rapid recovery. A cyber-resilient system therefore couples protective controls with business-continuity and disaster-recovery disciplines so that essential services can continue during and after an incident [16].

## 2.3.2 Network Security

Network security is an indispensable component of modern infrastructure. It protects confidentiality, integrity, and availability by monitoring, detecting, preventing, responding to, and recovering from unauthorised activity or anomalies that could compromise systems and data.

This section explores building blocks that play a central role in defending networks against a range of attacks.

### Firewall

A firewall, as described in [27], is a fundamental network security component that monitors and filters traffic based on predefined rules, thereby forming a barrier between trusted internal systems and untrusted external networks. Firewalls can be hardware-based, software-based, or a hybrid of both, and typically evaluate packets using criteria such as IP addresses, ports, and protocols.

Firewalls serve as a foundational defense layer, protecting against threats such as unauthorized access, malware, and data exfiltration. Modern firewalls have evolved beyond simple packet filtering to include features like IPS, Deep Packet Inspection (DPI), and AI-driven threat detection to address increasingly sophisticated attacks in hybrid and cloud-based environments.

Examples of widely used firewall solutions include open-source tools like pfSense and OPNsense, as well as proprietary options such as Cisco ASA, FortiGate, and Palo Alto Networks firewalls.

### Intrusion Detection & Prevention System

Intrusion detection is the process of identifying suspicious activities within a monitored environment. To achieve this, IDS are employed. These systems can be categorised by the environment they monitor and by the method they use to detect anomalies [65].

**Monitored environment types:**

- **Host-based Intrusion Detection System (HIDS).** An agent on a host monitors local activity (e.g., file/process events, Application Programming Interface (API) calls, host networking). HIDS offers deep system visibility but must be tailored per platform, which can be challenging in heterogeneous or legacy environments [65].
- **Network-based Intrusion Detection System (NIDS).** A NIDS observes traffic at strategic points in the network (e.g., via a tap or SPAN/mirror port) to monitor multiple devices without host agents, but it lacks host-level context [65].

**Detection approaches.**

- **Signature-based detection.** Observed data are matched against known attack patterns or signatures, from byte strings to rule sets. Effective for known threats but blind to novel attacks [61].
- **Anomaly-based detection.** A model of "normal" behaviour is learned and significant deviations are flagged. Powerful for unknown threats but prone to false positives due to legitimate variability and overlap with malicious behaviour [21, 71].

**Challenges in intrusion detection.** Intrusion detection is a difficult classification problem with class overlap, base-rate issues, and concept drift, which helps explain continued reliance on signatures and protocol-aware heuristics to control false alarms [71].

**Intrusion Prevention System (IPS).** Traditional NIDS are passive (alert-only). IPS adds enforcement—for example, dropping traffic inline or dynamically updating firewall policy to block attacks in real time, so tuning and safeguards are required to avoid collateral blocking [65].

### Honeypots

A honeypot is a deliberately deployed non-operational asset in an information environment, designed to attract and mislead attackers while isolating malicious activity from production systems [28]. Since legitimate users have no reason to interact with such systems, any activity is likely indicative of hostile intent, making honeypots effective for reducing false positives in intrusion detection.

An example of implementation is Honeyd [60], a virtual honeypot framework capable of simulating multiple operating systems and network services. Honeyd is designed to deceive reconnaissance tools such as Nmap or Xprobe and has been used in scenarios like network decoys, worm detection, and spam mitigation.

### Network Segmentation

Network segmentation divides a larger network into smaller, controlled zones, each with tailored security policies and access controls [13, 19]. By limiting the flow of traffic between segments whether through VLANs, , or firewalls this strategy enhances security, performance, and compliance [26, 73].

Segmentation significantly enhances security by containing breaches and limiting the lateral movement of attackers between zones. It also contributes to performance optimization by reducing network congestion through the isolation of high-traffic domains. Furthermore, segmentation enables more granular access control and supports regulatory compliance by enforcing least-privilege principles. From an operational perspective, it facilitates better monitoring and incident response by allowing focused analysis and quicker detection of anomalies within specific network areas.

### 2.3.3 Monitoring & Logging

#### Logging and Event Collection

Logging is a foundational element of any monitoring strategy. It involves the systematic collection of event data from diverse sources such as operating systems, applications, network devices, and security appliances [53]. These logs provide critical visibility into system behavior, user activity, and potential security incidents.

There are two primary methods for collecting logs. Many modern systems support native log forwarding, allowing them to transmit events directly to a centralized collector. In environments where this is not feasible, agent-based solutions can be deployed to extract logs locally and forward them securely.

However, effective logging is not simply a matter of collecting everything. A well-designed logging strategy must balance the volume of data with its operational and security value. Prioritising high-value logs—such as authentication events, privilege escalations, or configuration changes—helps reduce noise and ensures that critical signals are not lost in a flood of irrelevant data. Retention policies should also be defined based on the intended use of the logs, whether for short-term debugging or long-term forensic analysis [52].

To support automated analysis and correlation, logs should follow a structured format and include contextual metadata such as timestamps, event types, source identifiers, and user or process IDs. Time synchronization across systems, typically enforced via NTP, is essential to maintain coherent event timelines.

Beyond individual log entries, the ability to correlate events across systems is vital for detecting complex attack patterns. For example, a failed login attempt on one server followed by a successful login on another may indicate lateral movement. Correlation enables analysts to reconstruct attack paths, trace user sessions, and identify root causes [64].

Because logs are often targeted by attackers seeking to cover their tracks, the logging infrastructure itself must be secured. Common threats include log flooding (to obscure malicious activity), false event injection (to mislead analysts), and log tampering or deletion. To mitigate these risks, organizations should authenticate log sources, protect log servers through segmentation and access controls, and store logs in tamper-evident formats such as append-only files or write-once media. Regular audits of log integrity and access history further enhance resilience.

In summary, logging is not merely a technical necessity but a strategic capability.

When properly implemented, it supports operational monitoring, threat detection, incident response, and regulatory compliance.

#### Security Incident and Event Management (SIEM)

Modern Information Technology (IT) environments generate vast volumes of data from diverse sources, including system logs, firewall events, authentication attempts, and intrusion detection alerts. Analyzing these data streams in isolation is inefficient and often leads to fragmented visibility. To address this challenge, organizations rely on SIEM systems.

A SIEM platform aggregates, correlates, and analyzes data from multiple sources to provide a unified view of an organization's security posture [25]. It acts as a central nervous system for security operations, enabling faster detection of suspicious behavior and more effective incident response.

The core capabilities of a SIEM typically include log aggregation, event correlation, real-time alerting, and historical analysis. By linking related events across systems, SIEMs can identify complex attack patterns that would otherwise go unnoticed [34]. Additionally, they support compliance efforts by maintaining audit trails and generating reports aligned with regulatory requirements.

However, the effectiveness of a SIEM depends not only on its technical features but also on how it is configured and used. A common pitfall is assuming that a visually rich dashboard guarantees situational awareness. In practice, the value of a SIEM is determined by the quality of ingested data, the relevance of correlation rules, and the alignment of detection logic with the organization's specific threat landscape [33].

To maximize its utility, a SIEM should be configured around risk-based use cases. Each identified threat scenario should be mapped to relevant data sources, detection rules, and predefined response actions. This approach ensures that the SIEM contributes meaningfully to cyber situational awareness and supports timely, informed decision-making during security incidents.

### 2.3.4 Wi-Fi Specific Security Considerations

#### Wi-Fi Encryption Standards: WPA2, WPA3

Wi-Fi security has evolved significantly over the years through the introduction of various encryption protocols. The first widely adopted standard was Wired Equivalent Privacy (WEP), introduced in 1997. Due to its numerous security flaws, it was soon replaced by Wi-Fi Protected Access (WPA) in 2003 as a temporary solution. Just a year later, in 2004, WPA2 became the new standard, offering improved security with the introduction of AES-based encryption. Most Wi-Fi networks today still rely on WPA2. However, in 2018, WPA3 was introduced to address the growing security demands of modern wireless networks. WPA3 offers enhanced protection against brute-force attacks and provides better encryption for open networks [6]. While adoption of WPA3 is increasing, WPA2 remains the most widely used protocol.
Comparison table can be found in table 2.8

| Aspect | WPA3 | WPA2 |
|---|---|---|
| **Cryptography** | Enterprise 192-bit security suite (CNSA-aligned; e.g., AES-256-GCMP, SHA-384) in WPA3-Enterprise 192-bit mode | AES-CCMP (128-bit) per 802.11i |
| **Password security** | SAE (WPA3-Personal) is resistant to offline dictionary attacks and provides forward secrecy | PSK handshake (WPA2-PSK) is vulnerable to offline guessing when a capture is obtained |
| **Open networks** | Enhanced Open / OWE: link encryption without passwords | Traditional "open" networks: no over-the-air encryption |
| **Forward secrecy** | Supported (SAE; and WPA3-Enterprise with appropriate EAP/TLS settings)* | Not in WPA2-Personal; possible in WPA2-Enterprise with EAP-TLS using ephemeral key exchange |
| **Management frames** | PMF (802.11w) required by WPA3 certification; mitigates deauth/disassoc spoofing | PMF optional in WPA2 and must be explicitly enabled |

Table 2.8: Selected differences between WPA3 and WPA2, based on [6, 67].

**Definition**

**Forward Secrecy** (also known as **Perfect Forward Secrecy**) is a cryptographic property, that ensures the compromise of long-term keys, does not compromise past session keys. This means that even if an attacker later obtains a server's private key, they cannot retroactively decrypt previously recorded encrypted communications. [80]

### Deauthentication Attacks

Deauthentication attacks [11] are a form of DoS targeting IEEE 802.11 wireless networks. These networks rely on deauthentication frames to legitimately terminate connections between clients and access points. However, a critical vulnerability arises from the fact that these management frames are not authenticated in WPA2 and earlier standards.

An attacker can exploit this weakness by forging deauthentication frames, thereby forcing connected users to disconnect from the network. This type of attack is commonly used to disrupt services or to capture the WPA/WPA2 4-way handshake, which can later be used in offline password-cracking attempts. Tools such as `aireplay-ng -0`[4] automate this process, making it relatively simple to execute with the right hardware and access. [78]

[4] `https://www.aircrack-ng.org/`

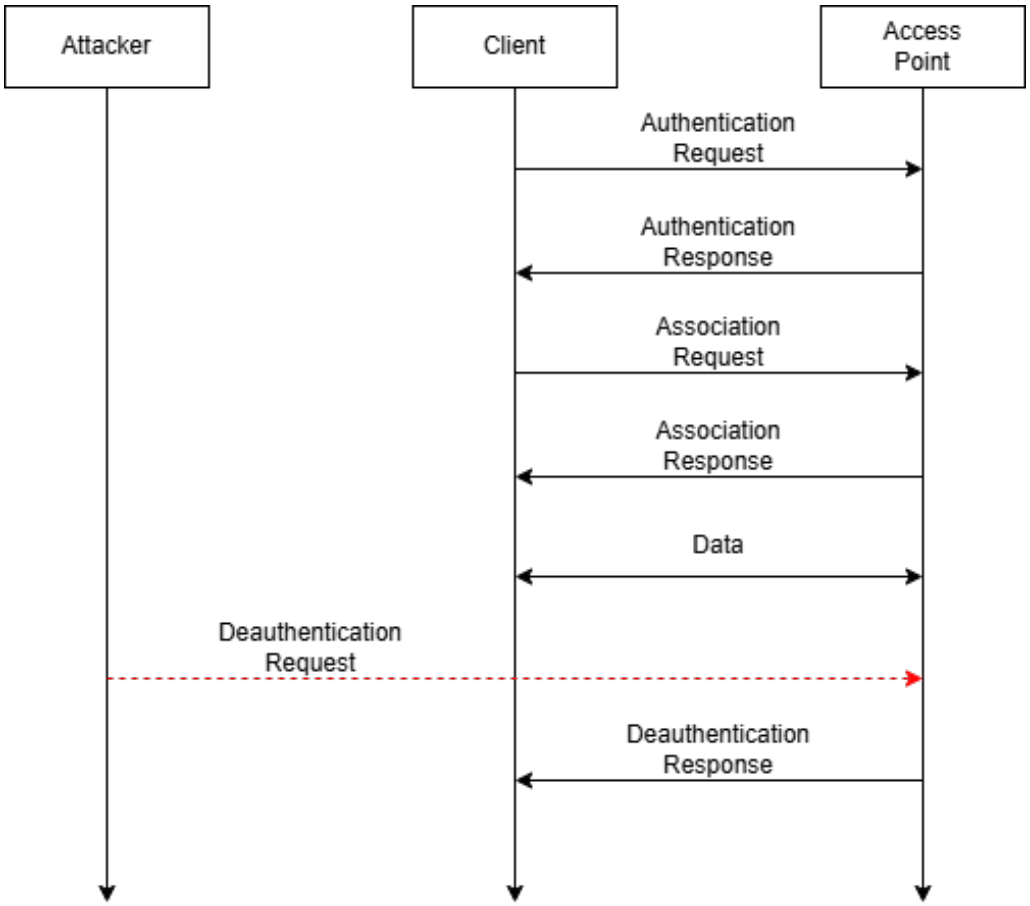



Figure 2.6: Sequence Diagram of a Deauthentication Attack

As shown in Figure 2.6, the client initially connects to the access point through a standard authentication and association process. Once the connection is established and data is being exchanged, an attacker sends a forged deauthentication frame to the access point. Since the 802.11 standard does not require authentication for management frames, the AP accepts the frame and terminates the connection with the client. This form of attack is commonly used as a precursor to further exploits such as man-in-the-middle or denial-of-service attacks.

**Definition**

A **Man in the Middle (MitM)** attack is a type of cyberattack where an adversary covertly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. [46]

**Mitigation:** To counteract such attacks, the IEEE 802.11w amendment was introduced to provide protection for management frames, including deauthentication and disassociation frames [2] [17]. Additionally, WPA3-Enterprise includes mandatory support for PMF significantly improving resistance against this class of attacks [82].

### Evil Twin Wi-Fi Attack

An Evil Twin attack [12] involves setting up a rogue access point that mimics the SSID and appearance of a legitimate Wi-Fi network. Unsuspecting users may connect to the

fake AP, believing it to be genuine, thereby exposing their traffic to interception or manipulation.

This attack is particularly dangerous in public or temporary deployments, where users may not verify the authenticity of the network. Once connected, attackers can perform MitM attacks, capture credentials, or inject malicious content.

**Mitigation:** To defend against Evil Twin attacks:

- Use WPA3 with Opportunistic Wireless Encryption (OWE) to protect open networks.
- Educate users to verify network names and avoid connecting to unsecured or unfamiliar SSIDs.
- Deploy Wireless Intrusion Detection System (WIDS) to detect rogue APs.
- Implement certificate-based authentication (e.g., EAP-TLS) in enterprise environments.

# Chapter 3
# Initial Proof of Concept

This chapter presents the initial PoC as published on the Cyber Defence Lab (CyLab[1]) blog, which serves as the technical foundation for the security analysis conducted in this thesis.

All relevant documentation for this solution is provided in [51]. Although the original context of the PoC differs slightly from the intended use case of this thesis, it provides a valuable baseline for assessing and improving the system's security posture.

## 3.1 Context

This PoC was designed to deploy a resilient Wi-Fi network in austere environments where resources such as electricity and Internet access may be limited [51]. The deployment therefore addresses the following environmental and logistical constraints:

- **Autonomous power supply.** The system must operate independently of the electrical grid (e.g., using a battery/solar pack).
- **Self-sufficient mesh network.** The infrastructure must support reliable inter-node communication without external dependencies.
- **Ruggedised hardware.** Equipment must be weather-resistant and capable of withstanding harsh environmental conditions.
- **Local-only management.** Due to operational constraints (intermittent Internet), the Netgear APs were configured via the local web interface rather than the Insight cloud platform. This limits available features, such as some controller-managed mesh capabilities and WPA3/PMF over WDS links.

### 3.1.1 Problem statement

A key limitation of the initial setup is the reliance on local device management due to intermittent or unavailable WAN connectivity. As a result, the Netgear APs were administered via the local web interface rather than the Insight controller, preventing use of controller-managed features (e.g., native mesh path selection, centralised RF management, and some WPA3/PMF options on WDS links). Consequently, the deployment used WDS bridging between APs, which extends coverage but is not a controller-managed mesh.

## 3.2 Requirements

### 3.2.1 Hardware

The following hardware components were used in the PoC:

[1] `https://www.cylab.be/`

Table 3.1: Hardware components of the initial PoC

| Component | Role and description |
|---|---|
| NETGEAR WAX610[2] | Indoor Wi-Fi AP acting as the mesh gateway. |
| NETGEAR WAX610Y[3] (×5) | Outdoor-rated Wi-Fi APs extending wireless coverage. |
| NETGEAR GS728TPP | Managed PoE switch interconnecting the management host and the gateway AP. |
| Mobisun Pro Air[4] (×5) | Portable battery/solar packs providing autonomous power. |
| PoE injectors (×5) | Supply PoE power to the WAX610Y outdoor APs. |
| Starlink[5] terminal | Satellite backhaul providing Internet connectivity. |
| Management PC | Hosts the Kernel-based Virtual Machine (KVM) hypervisor and virtualised services (e.g., firewall, Security Onion). |

### 3.2.2 Software

The software stack includes:

Table 3.2: Software components of the initial PoC

| Software | Role and description |
|---|---|
| KVM[6] | Hypervisor for hosting the virtualised services (e.g., pfSense, Security Onion, Checkmate). |
| pfSense[7] | Open-source firewall/router. |
| Security Onion[8] | Network security monitoring and intrusion detection (e.g., Zeek, Suricata, full packet capture (PCAP), dashboards). |
| Checkmate[9] | Open-source server and service monitoring, deployed as a Docker container for health checks, dashboards, and alerting. |

## 3.3 Network Architecture

Figure 3.1 shows the initial PoC topology. For clarity, the model labels in the figure ("LBR20" gateway and "RBS50Y" satellites) correspond to the hardware used in this thesis: Netgear WAX610 (gateway) and WAX610Y (satellites). We use the WAX610/WAX610Y naming throughout.

At the core of the system, a management PC runs a KVM hypervisor hosting:

- **pfSense** — firewalling and captive-portal access control;

[2] https://www.netgear.com/be/business/wifi/access-points/wax610/
[3] https://www.netgear.com/be/business/wifi/access-points/wax610y/
[4] https://mobisun.com/en/product/portable-solar-panel-with-battery-and-socket-230v-300w-148-wh-40000mah/
[5] https://www.starlink.com/
[6] https://linux-kvm.org/page/Main_Page
[7] https://www.pfsense.org/
[8] https://securityonionsolutions.com/
[9] https://checkmate.so/

- **Security Onion** — network security monitoring and intrusion detection.

Additionally, a Docker container runs **Checkmate** for host/service monitoring and alerting.

**Scope note**

At the time of writing, the software components were installed, but no firewall policy beyond the captive portal and no monitoring/IDS tuning had been defined. These configurations were outside the scope of the initial PoC.

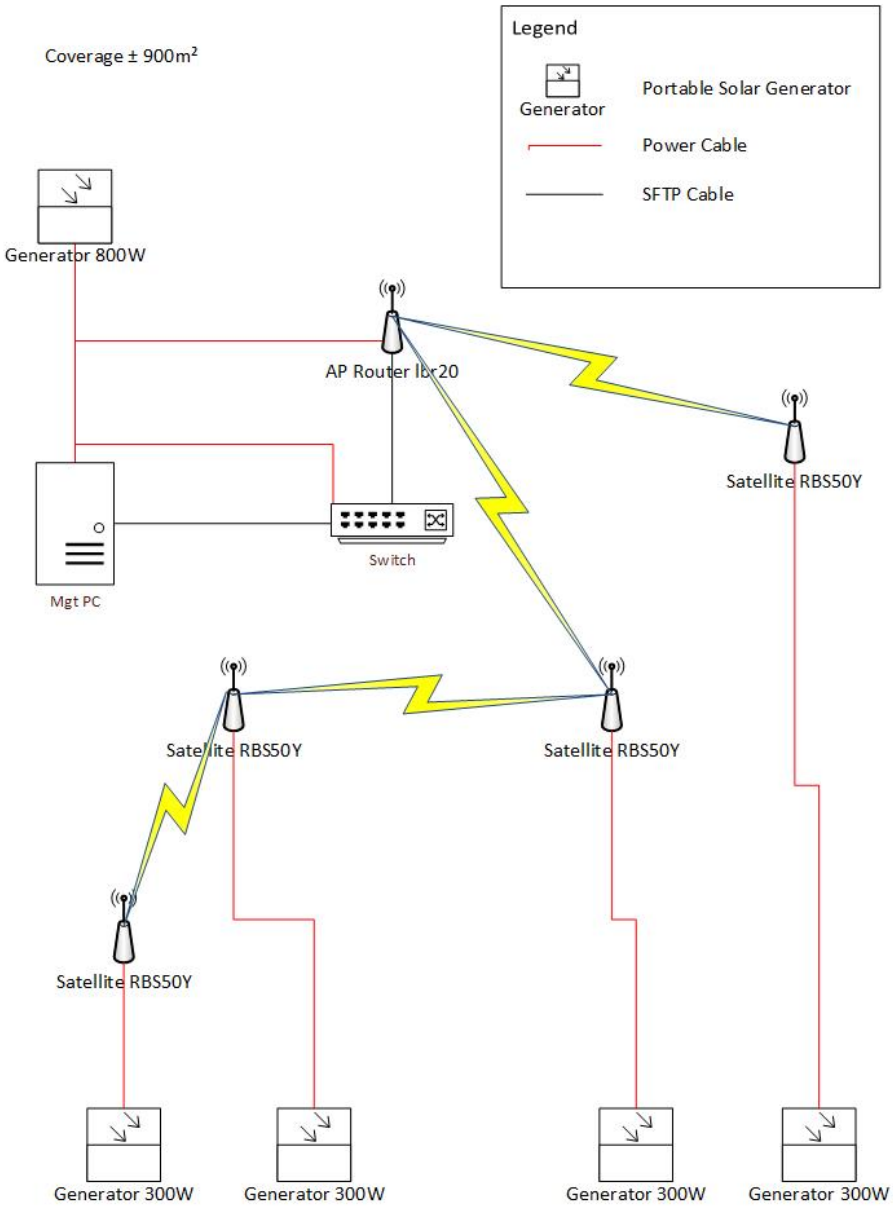



Figure 3.1: Initial PoC network layout (gateway AP/router with satellite nodes and portable power) [51].

The Starlink terminal provides the Internet backhaul and connects to the access switch, which in turn provides the upstream link to the firewall (so all client traffic is routed through it). The switch also facilitates future expansion by accommodating additional servers and services.

All infrastructure components are powered by portable solar-battery systems, enabling autonomous operation without grid power.

## 3.4 Preliminary testing

Several tests were conducted to evaluate the performance and limitations of the initial setup:

- **Battery endurance.** The portable battery pack sustained the system for approximately 7 hours. A full recharge from a mains outlet took about 1.5 hours. Solar charging performance was not tested. In particular, charge-while-operating (solar input with the APs and backhaul active) was not evaluated [51].
- **Wi-Fi coverage.** Signal strength measurements were taken with a threshold of $-70$ dBm, considered acceptable for stable client connectivity [42][10]. Measured distances to reach this threshold were:
  - *Outdoor (open space):* $\sim$ 26 metres.
  - *Indoor (with walls):* $\sim$ 12 metres.
  - *Indoor (open space):* $\sim$ 15 metres.

## 3.5 Security posture

The current security configuration is minimal:

- **Wi-Fi security.** WPA2-PSK. WPA3 is not available on WDS links.
- **Access control.** pfSense captive portal enabled for client onboarding.
- **Firewall policy.** Default policy only. No bespoke allow or deny rules.
- **Monitoring and logging.** No centralised logging or alerting. IDS installed but not tuned.
- **Segmentation.** No network segmentation. Single flat broadcast domain.

This baseline configuration provides a starting point for the security analysis and improvement process described in the following chapters.

[10] Coverage depends on radios, mounting height, channel conditions and interference. The values below are indicative and not a site-survey guarantee.

# Chapter 4
# Security Analysis

This chapter analyses the security of the initial PoC network described in the previous chapter. The aim is to assess its resilience against credible threats and to identify improvements across confidentiality, integrity, and availability, with availability prioritised for deployable environments.

A security analysis follows four guiding questions [54]:

1. **Scope — What are we working on?** Clarify purpose, operational context, assets, and system boundaries.

2. **Threats and risks — What can go wrong?** Identify threats and vulnerabilities, then evaluate likelihood and impact.

3. **Mitigations — What are we going to do about it?** Define controls and design changes to reduce risk to acceptable levels.

4. **Validation — Did we do a good job?** Define success criteria and evidence, execute acceptance checks and pilots, and compare residual risk against baseline using the methods and tables in the Validation section.

## 4.1 Scope — What are we working on?

### 4.1.1 Context and Scenario

The analysis concerns a temporary, deployable Wi-Fi network for event operations at a festival, rather than public Internet access. The network supports staff workloads such as press communications, Wi-Fi cameras, point-of-sale terminals, administration, and security monitoring, as identified during an interview with a former security coordinator for a festival (Annex A.1). Coverage is provided by wireless access infrastructure with backhaul via satellite (e.g., Starlink) or alternative links including 4G, 5G, or fibre. The primary goals are rapid setup, ease of operation in the field, and continuity of service under environmental and logistical constraints.

**Important remark**

This analysis focuses on a temporary, staff-only network for festival management that does not handle highly confidential or classified data. The design targets rapid deployment and basic mission support under field constraints. The same fundamental threats considered here (for example spoofing, rogue access points, deauthentication, and denial of service) also apply to non-classified military field networks, so many findings generalise. However, deployments that process classified information or require higher assurance need additional controls and accreditation that are out of scope for this thesis.

The initial PoC uses a WDS (repeater-style) topology to extend coverage. The main design goals are:

- rapid deployment and ease of configuration.
- operational resilience in harsh or remote environments.
- basic security monitoring and segmentation capabilities.

**Assumptions & limitations.**

- The network does not handle highly confidential or classified data. Typical traffic includes camera feeds, administrative access and payment connectivity.
- Backhaul may use Starlink, 4G/5G or fibre. Intermittent outages are expected.
- Camera footage is not archived in the PoC; only security logs are retained locally (Annex A.1).
- Physical protection is basic due to field conditions. Device loss or tampering is plausible.
- Payment terminals use end-to-end TLS to the acquirer. The event network does not intercept or terminate these sessions.

Availability is prioritised over confidentiality and integrity for this deployment, as indicated during the interview (Annex A.1). Because the system does not process sensitive or classified data, maintaining continuous operation is the most critical requirement.

**Actors and primary uses (Annex A.1).**

- **Physical Security.** Real-time viewing of on-site IP camera streams (local only, no Internet required).
- **Point-of-sale.** Card transactions via Internet payment gateways (requires reliable WAN access).
- **Press and communications.** Social media posting and press connectivity (best-effort Internet access).
- **IT/Administration.** Network configuration, monitoring, and troubleshooting (privileged access to management services).

**Environmental constraints.**

- Solar/battery power, variable RF conditions, and weather.
- Intermittent backhaul over satellite, 4G/5G or fibre, with variable latency and throughput and the risk of congestion during peak periods.

**Success criteria.**

- *Continuous local operations* during backhaul loss (for example, on-site camera viewing remains functional).
- *Controlled degradation* under node or power failures (the mesh reroutes with minimal service interruption).
- *Service prioritisation/QoS* so critical traffic (for example, payments and security video) keeps working during congestion.
- *Monitoring* to detect problems early and support a timely response.
- *Network segmentation* to contain incidents and make lateral movement harder.

### 4.1.2 Data Flow Diagram

The following DFD (Figure 4.1) captures external entities, trust boundaries, core processes, and data stores, and serves as the basis for a STRIDE analysis of each DFD element in the subsequent risk analysis.

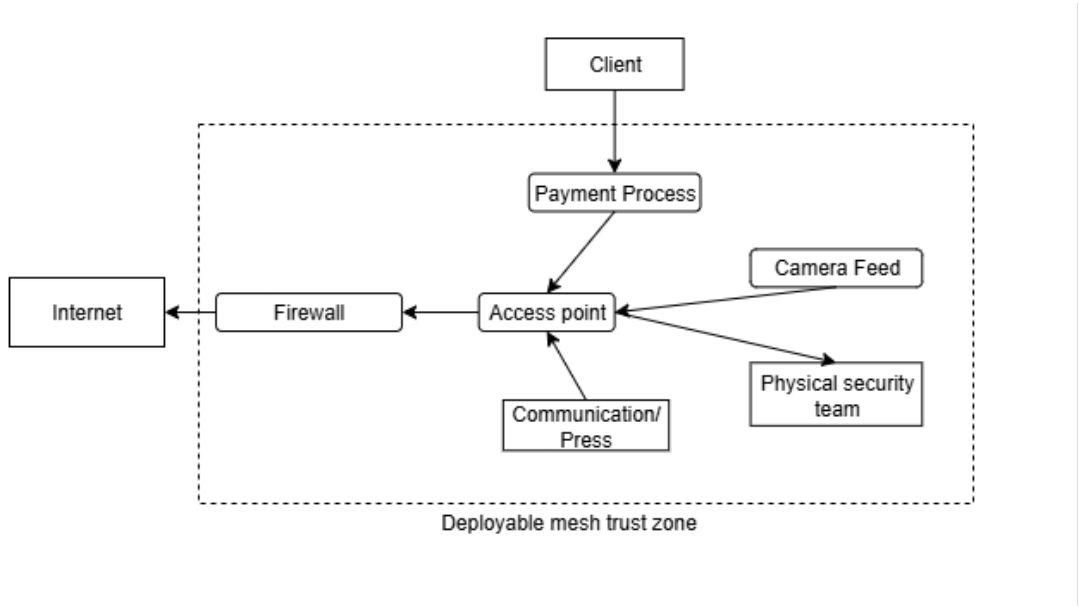



Figure 4.1: DFD of the initial PoC (festival scenario)

### 4.1.3 Network Architecture

Figure 4.2 illustrates the current architecture of the PoC network under the festival scenario.

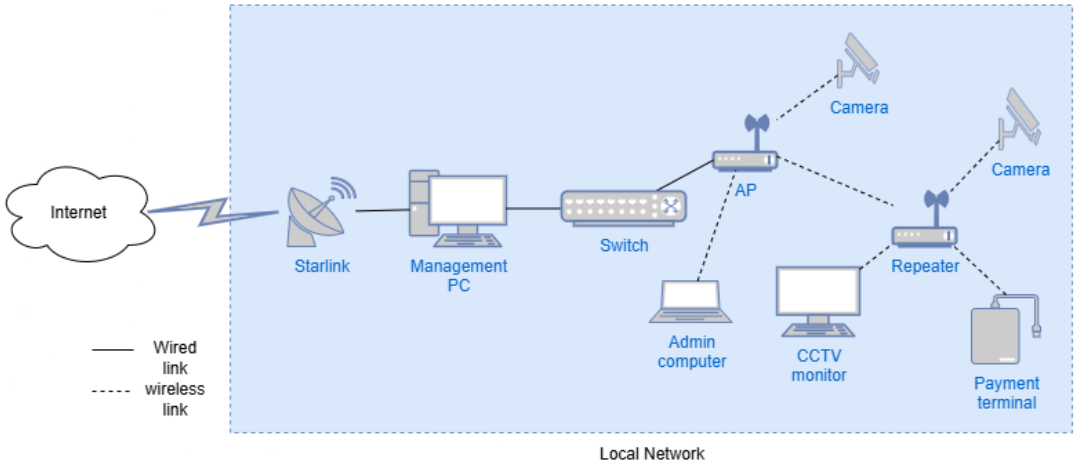



Figure 4.2: Initial PoC network architecture (festival scenario).

**Architecture constraint**

The initial PoC uses AP-local web configuration with WDS/repeater links (no mesh). This reduces self-healing and central visibility, raising availability and admin risks. The remediation (controller-managed mesh) is detailed in Section 5.3.

## 4.2 Threats and risks — What can go wrong?

In this section, we identify threats relevant to the PoC. While many apply to any Wi-Fi deployment, the constraints of a rapidly deployable mesh introduce additional risks that must be considered. We evaluate risks for each element of the DFD (Figure 4.1).

### 4.2.1 Threat Modeling

To structure the analysis, we apply STRIDE methodology in conjunction with the DFD. For each DFD element, we consider Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. We then assess likelihood and impact before proposing mitigations. However, some credible, multi-step (campaign-style) threats cut across several components and do not map cleanly to a single STRIDE instance.

**Threat 1: Spoofing the Identity of a User/Device on the Network (S–Spoofing)**
Associated CAPEC: CAPEC-151 – Identity Spoofing[1]

An attacker impersonates a legitimate user or device on the wireless network to gain unauthorized access, bypassing access controls and reaching internal services. This is feasible in environments relying solely on WPA2-Pre-Shared Key (PSK) (AES) without per-user credentials (e.g., 802.1X/EAP). Note that captive portals and MAC filtering *do not* provide cryptographic identity and are insufficient to prevent spoofing once the PSK is known.

[1] `https://capec.mitre.org/data/definitions/151.html`

To estimate the **Control Strength** (CS), we refer to Table 2.5. With only a shared WPA2-PSK and no individual authentication, all clients present the same secret. If that secret is leaked or guessed, impersonation becomes trivial. We therefore rate CS as **Low**.

The **Threat Capability** (TCap) is assessed as **Moderate** (Table 2.4). The attacker must be within radio range and either know the PSK or obtain it (e.g., social disclosure) or successfully mount an offline dictionary/brute-force attack after capturing a handshake (common with tools such as Aircrack-ng or Hashcat).

Combining **Low** CS with **Moderate** TCap yields **High** Vuln (Fig. 2.3).

For **Threat Event Frequency** (TEF), proximity is required and success depends on key leakage/guessing; nevertheless, shared-key environments are routinely targeted. We rate TEF as **Moderate** (Table 2.6).

Using Fig. 2.4, a **High** Vuln with **Moderate** TEF results in a **Moderate** LEF.

Regarding **Probable Loss Magnitude** (PLM, Table 2.7), successful spoofing could enable access to internal services, lateral movement, or traffic capture. Given the PoC's scope (operational but not highly sensitive assets), we estimate **Moderate** impact.

Combining LEF (**Moderate**) with PLM (**Moderate**), the overall **Risk Magnitude** is **Moderate** (Fig. 2.5).

**Operational assumption — temporary PSK rotation**

Because this network is *ephemeral*, the WPA2-PSK for field SSIDs is rotated at each deployment (never reused), with high-entropy values (e.g., $\geq 16$ random characters, preferably 20+) distributed just in time to authorized users. This shortens the attacker's window and raises the cost of offline guessing.

Under this assumption:

- **TCap: M → L**.
- **Vuln (Fig. 2.3):** with **CS = L** and **TCap = L**, moves to **M**.
- **TEF (Table 2.6): M → L** if rotation is enforced with truly random keys.
- **LEF (Fig. 2.4): L**. With **PLM = M**, overall risk still **M** (Fig. 2.5).

**Threat 2: Spoofing the Identity of an Access Point (S–Spoofing)** Associated CAPEC: CAPEC-615 – Evil Twin Wi-Fi Attack[2]

An attacker stands up a rogue ("evil twin") access point that impersonates a legitimate SSID/Basic Service Set Identifier (BSSID) and optionally its channel, often with stronger signal and with deauthentication to force clients to reconnect. If the WPA2-PSK is known or recovered via offline cracking after a handshake or PMKID capture, victims may auto-associate to the impostor AP. This enables MitM for credential capture and session hijacking or phishing, and it can disrupt availability.

To estimate the **Control Strength** (CS), we refer to Table 2.5. In the initial PoC, SSIDs use WPA2-PSK. There is no enterprise authentication (802.1X/EAP with server

[2] `https://capec.mitre.org/data/definitions/615.html`

certificate validation) and PMF is *not* present. Given the lack of per-AP cryptographic authenticity and the ability to inject management frames (deauthentication or disassociation), we rate CS as **Low**.

The **Threat Capability** (TCap) is **High** (Table 2.4). Commodity tooling and inexpensive radios (e.g., `airbase-ng`) make SSID/BSSID cloning, lure beacons, deauthentication forcing, and handshake capture straightforward for an attacker in proximity.

Combining **Low** CS with **High** TCap yields **Very High** Vuln (Fig. 2.3).

For **Threat Event Frequency** (TEF), crowded venues and the attacker's proximity requirement justify a **Moderate** rating (Table 2.6). Such attempts are plausible during public events, and detection is difficult in WPA2-only deployments without dedicated monitoring.

Using Fig. 2.4, **Very High** Vuln with **Moderate** TEF results in a **Moderate** LEF.

Regarding **Probable Loss Magnitude** (PLM, Table 2.7), consequences include credential harvesting (e.g., portal logins if present), traffic interception except where end-to-end TLS is enforced, and service disruption. Given the PoC's scope (operational data and no long-term video storage), we estimate **Moderate** impact.

Combining LEF (**Moderate**) and PLM (**Moderate**), the overall **Risk Magnitude** is **Moderate** (Fig. 2.5).

**Operational assumption — WPA2-only hygiene (no PMF, no WIDS)**

For each deployment, SSID names and PSKs are unique and not reused across events, PSKs are high entropy and rotated per event, and auto-join is disabled on admin devices. These practices shorten attacker windows and frustrate deauthentication-assisted lures even without PMF or wireless IDS.

Under this assumption:

- **TCap: H** $\rightarrow$ **M** when PSKs are strong and rotated and devices avoid auto-join.
- **Vuln (Fig. 2.3):** with **CS** = **L** and **TCap** = **M**, moves from **Very High** to **High**.
- **TEF (Table 2.6):** remains **M** due to the absence of dedicated monitoring.
- **LEF (Fig. 2.4):** remains **Moderate**. With **PLM** = **M**, overall risk remains **Moderate** (Fig. 2.5).

**Threat 3: Integrity of the Logs (T–Tampering)** Associated CAPEC: CAPEC-268 – Audit Log Manipulation[3] and CAPEC-93 – Log Injection–Tampering–Forging[4]

An attacker or malicious insider modifies or deletes log entries to conceal unauthorized activity. This undermines forensic evidence and makes incident response and accountability unreliable.

[3] `https://capec.mitre.org/data/definitions/268.html`
[4] `https://capec.mitre.org/data/definitions/93.html`

For **Control Strength** (CS, Table 2.5), if logs are stored only locally and lack integrity controls such as cryptographic signing or append-only storage, CS is **Low**. Local logs on systems where administrators have shell access are especially exposed.

For **Threat Capability** (TCap, Table 2.4), common tools and native OS privileges make alteration of plaintext logs straightforward once elevated access is obtained. We assess TCap as **Moderate**.

With **Low** CS and **Moderate** TCap, the **Vulnerability** (Vuln) is **High** (Fig. 2.3).

For **Threat Event Frequency** (TEF, Table 2.6), targeted log tampering is less common in low-profile environments and usually accompanies a broader intrusion. We rate TEF as **Low**. Using Fig. 2.4, **LEF = Low**.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Low**. Losing trustworthy logs degrades detection and post-incident analysis even if core services continue to run.

Combining LEF (**Low**) with PLM (**Low**), the overall **Risk Magnitude** is **Low** (Fig. 2.5).

**Threat 4: Integrity of the Camera Feed (T–Tampering)** Associated CAPEC: CAPEC-216 – Communication Channel Manipulation[5]

An attacker tampers with video feeds from surveillance cameras by disrupting streams such as jamming or disconnecting a camera or by altering content such as injecting fake footage or disabling the feed during malicious activity. This degrades situational awareness and can hinder monitoring or post-event analysis. Typical vectors include weak RTSP or RTP configurations, ARP or DNS spoofing to redirect streams, or replacing the viewing station endpoint.

To estimate the **Control Strength** (CS), we refer to Table 2.5. If camera streams use plaintext RTSP or RTP and there is no health monitoring to detect anomalies or gaps, CS is **Low**. Cameras that rely on unprotected management interfaces are especially exposed.

Given the prevalence of freely available tooling to intercept or spoof RTSP streams, the **Threat Capability** (TCap) is **Moderate** (Table 2.4).

Combining **Low** CS with **Moderate** TCap yields **High** Vuln (Fig. 2.3).

For **Threat Event Frequency** (TEF), proximity or network access is required and attacks are usually targeted. In a public and temporary venue with unattended devices, attempts are plausible but not routine. We rate TEF as **Low** (Table 2.6).

Using Fig. 2.4, **High** Vuln with **Low** TEF gives a **Low** LEF.

The **Probable Loss Magnitude** (PLM, Table 2.7) depends on operational reliance on live video. In this deployment, impact is **Moderate** due to loss of awareness and delayed response.

With **LEF = Low** and **PLM = Moderate**, the overall **Risk Magnitude** is **Low** (Fig. 2.5).

[5] `https://capec.mitre.org/data/definitions/216.html`

**Operational assumption — encrypted camera-to- streams**
If camera streams use TLS or SRTP such as RTSP over TLS or SRTP and the enforces device authentication, **CS** improves to **Moderate** which reduces **Vuln** to **Moderate**. **TEF** remains **Low** so **LEF** becomes **VL/L**. With **PLM** = **Moderate**, overall risk can drop toward **Very Low or Low**.

**Threat 4b: Physical Tampering of Camera Hardware (T/D–Tampering, DoS)** An attacker obstructs, damages, or removes a camera, or cuts or disconnects its *power cabling* (PoE or DC), causing loss of video. This results in a localized denial of service and loss of situational awareness.

For **Control Strength** (CS, Table 2.5), if mounts, housings, and *power or network cabling* are not hardened or supervised, CS is **Low**. Devices within easy reach and those without tamper switches or link health monitoring are especially exposed.

For **Threat Capability** (TCap, Table 2.4), only proximity and simple tools are required, so TCap is **Moderate**.

With **Low** CS and **Moderate** TCap, the **Vulnerability** (Vuln) is **High** (Figure 2.3).

For **Threat Event Frequency** (TEF, Table 2.6), in festival settings with crowd presence and periodic staff patrols, targeted physical tampering is plausible but not routine. We rate TEF as **Low**.

Using Figure 2.4, **Low** TEF with **High** Vuln yields a **Low** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Moderate** due to loss of situational awareness.

Combining LEF (**Low**) with PLM (**Moderate**), the **Risk Magnitude** is **Low** (Figure 2.5).

**Threat 5: Repudiation by an Administrator (R–Repudiation)** Associated CAPEC: CAPEC-268 – Audit Log Manipulation[6] and CAPEC-93 – Log Injection–Tampering–Forging[7]

An administrator performs a critical action on the system such as modifying firewall rules, disabling a control, or deleting logs and later denies responsibility. Without reliable and tamper-resistant auditing, attribution becomes difficult and accountability and incident response are undermined.

For **Control Strength** (CS, Table 2.5), monitoring components are installed but not configured and there is no enforced, tamper-evident audit trail for administrative actions. We rate CS as **Low**.

For **Threat Capability** (TCap, Table 2.4), the threat actor is an administrator with privileged knowledge and the ability to disable or clear local evidence. We assess TCap as **High**.

With **Low** CS and **High** TCap, the **Vulnerability** (Vuln) is **Very High** (Fig. 2.3).

[6] `https://capec.mitre.org/data/definitions/268.html`
[7] `https://capec.mitre.org/data/definitions/93.html`

For **Threat Event Frequency** (TEF, Table 2.6), malicious administrator activity is uncommon in this context though mistakes or policy violations followed by denial are plausible in low-oversight tests. We rate TEF as **Low**.

Using Fig. 2.4, **Very High** Vuln with **Low** TEF results in a **Low** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Moderate**. Undetected administrator changes can degrade the security posture, cause outages, or enable data exposure.

Combining LEF (**Low**) with PLM (**Moderate**), the overall **Risk Magnitude** is **Moderate** (Fig. 2.5).

**Threat 6: Information Disclosure via Wireless Sniffing (I–Information Disclosure)** Associated CAPEC: CAPEC-157 – Sniffing Attacks[8], CAPEC-158 – Sniffing Network Traffic[9], CAPEC-117 – Interception[10]

Because communications occur over a wireless medium, an attacker may attempt to intercept data in transit using packet-sniffing tools. Without encryption, this could expose credentials, configuration data, or user activity. In the initial PoC, wireless links use WPA2 encryption and most application traffic such as web administration and user-facing services uses HTTPS. Even if packets are captured, payloads are not readable without the correct keys and a captured handshake. These measures significantly reduce the chance of meaningful data exposure, although traffic analysis such as device identification by MAC address and flow timing remains possible.

To estimate the **Control Strength** (CS), we refer to Table 2.5. Modern link-layer encryption combined with application-layer encryption provides strong protection against casual sniffing and raises the effort required for a successful attack. Risks remain if weak passphrases are used, devices are misconfigured, or older ciphers are allowed. We therefore rate CS as **High**.

For **Threat Capability** (TCap, Table 2.4), sniffing tools such as `Wireshark` and `Aircrack-ng` are widely available and easy to operate. Without key compromise and a captured handshake, these tools are ineffective against properly encrypted payloads. We rate TCap as **High**.

Combining **High** CS with **High** TCap yields **Moderate** Vuln (Fig. 2.3).

For **Threat Event Frequency** (TEF, Table 2.6), opportunistic sniffing by any nearby attacker is plausible, but the probability of obtaining useful unencrypted data is minimal when WPA2 and HTTPS are correctly configured. We rate TEF as **Low**.

Using Fig. 2.4, **Moderate** Vuln with **Low** TEF results in **Low** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Low**. Even if traffic is captured, properly encrypted payloads are unlikely to yield exploitable information, though limited metadata exposure may occur.

With LEF **Low** and PLM **Low**, the resulting **Risk Magnitude** is **Low** (Fig. 2.5).

[8] `https://capec.mitre.org/data/definitions/157.html`
[9] `https://capec.mitre.org/data/definitions/158.html`
[10] `https://capec.mitre.org/data/definitions/117.html`

**Threat 7: Denial of Service—Wi-Fi Deauthentication Attack (D–Denial of Service)** Associated CAPEC: CAPEC-604 – Wi-Fi Jamming[11]

An attacker forges 802.11 deauthentication or disassociation frames so clients drop from the AP, disrupting availability. This is a management-frame abuse rather than RF noise flooding but for users the outcome is the same loss of connectivity [78].

**Control Strength** (CS) is **Low** (Table 2.5) on SSIDs without PMF. WPA2 without PMF leaves deauthentication and disassociation frames unauthenticated, so clients accept forged frames [2].

**Threat Capability** (TCap) is **Moderate** (Table 2.4). The attacker needs proximity and common tools such as `aireplay-ng` or Scapy to craft frames [78].

Combining **Low** CS with **Moderate** TCap yields **High** Vuln (Fig. 2.3).

**Threat Event Frequency** (TEF) is **Low** (Table 2.6). Intent and physical presence are required and opportunistic attacks at a small festival are uncommon.

Using Fig. 2.4, **High** Vuln with **Low** TEF gives **Low** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Low**. Impact is transient connectivity loss rather than data compromise.

With **LEF** = **Low** and **PLM** = **Low**, the overall **Risk Magnitude** is **Low** (Fig. 2.5).

**Note on scope**

Forged deauthentication and disassociation is distinct from broadband RF jamming where an adversary transmits noise. PMF mitigates forged frames but cannot stop true RF jamming. RF jamming is treated separately as a DoS variant in Threat 7b.

**Threat 7b: Denial of Service—RF Jamming / Interference (D–Denial of Service)** Associated CAPEC: CAPEC-604 – Wi-Fi Jamming[12]

An attacker or harsh RF conditions emit broadband noise or sustained transmissions on the operating channel(s), degrading signal-to-noise ratio and blocking client and AP communications. Unlike management-frame spoofing, this is a *physical-layer* denial of service and cryptographic controls such as PMF do not prevent it. WLAN guidance notes that jamming is difficult to fully prevent and resilience is achieved through RF planning, monitoring, and failover [66].

**Control Strength** (CS, Table 2.5) is **Low** when channels and transmit power are static and there is no automated RF response such as channel change, band steering, or path/backhaul failover.

**Threat Capability** (TCap, Table 2.4) is **Moderate**. Proximity and low-cost tools such as software-defined radios or commodity devices configured to transmit continuously are sufficient.

Combining **Low** CS with **Moderate** TCap yields **High** Vuln (Fig. 2.3).

[11] `https://capec.mitre.org/data/definitions/604.html`
[12] `https://capec.mitre.org/data/definitions/604.html`

**Threat Event Frequency** (TEF, Table 2.6) is **Low**. Deliberate on-site action is required and opportunistic jamming at a small festival is uncommon.

Using Fig. 2.4, **High** Vuln with **Low** TEF results in **Low** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Moderate** because availability is a priority in this context.

With LEF **Low** and PLM **Moderate**, the overall **Risk Magnitude** is **Low** (Fig. 2.5).

**Threat 8: Denial of Service—Service Saturation Inside the Network (D–Denial of Service)** Associated CAPEC: CAPEC-125 – Flooding[13] and CAPEC-130 – Excessive Allocation[14]

A device or service such as a camera stream, misconfigured client, or bulk upload consumes excessive bandwidth and degrades other critical services on shared links. In a network with limited backhaul capacity, sustained high-rate traffic of a service can impact adjacent services.

**Control Strength** (CS, Table 2.5) is **Low** when there is no quality-of-service policy or rate limiters and no VLAN-scoped shaping or per-SSID or per-client caps.

**Threat Capability** (TCap, Table 2.4) is **Moderate** because no sophisticated attacker is required and ordinary devices can saturate links through misconfiguration or peak use.

Combining **Low** CS with **Moderate** TCap yields **High** Vuln (Fig. 2.3).

**Threat Event Frequency** (TEF, Table 2.6) is **Moderate** where high-bandwidth services operate by default and are not rate limited.

Using Fig. 2.4, **High** Vuln with **Moderate** TEF results in **Moderate** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Moderate** due to service slowdown, loss of responsiveness, or brief outages of critical components.

With LEF **Moderate** and PLM **Moderate**, the overall **Risk Magnitude** is **Moderate** (Fig. 2.5).

**Threat 9: Elevation of Privilege (E–Elevation of Privilege)** Associated CAPEC: CAPEC-233 – Privilege Escalation[15]

An attacker or unauthorized user exploits a vulnerability or misconfiguration to gain higher privileges than initially granted. Elevated access enables actions such as altering configurations, accessing restricted data, or disabling security controls. Typical avenues include default or shared credentials, exposed administrative services, unpatched firmware, weak role separation, and overly broad ACLs.

**Control Strength** (CS, Table 2.5) is **Low** when role-based access control is not enforced, default accounts remain, administrative interfaces are reachable from non-IT networks, or logging is incomplete.

**Threat Capability** (TCap, Table 2.4) is **Moderate**. Public exploits, misconfiguration scanners, and common techniques such as weak password guessing or web admin flaws are widely available, though a foothold or misconfiguration is often required.

[13] `https://capec.mitre.org/data/definitions/125.html`
[14] `https://capec.mitre.org/data/definitions/130.html`
[15] `https://capec.mitre.org/data/definitions/233.html`

Combining **Low** CS with **Moderate** TCap yields **High** Vuln (Fig. 2.3).

**Threat Event Frequency** (TEF, Table 2.6) is **Moderate**. Once an actor has any network presence, privilege escalation is routinely attempted as part of intrusion playbooks.

Using Fig. 2.4, **High** Vuln with **Moderate** TEF results in **Moderate** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Moderate**. Elevated privileges can change security posture, interrupt services, or expose operational data, although the scope is limited by the PoC's modest asset sensitivity.

With LEF **Moderate** and PLM **Moderate**, the overall **Risk Magnitude** is **Moderate** (Fig. 2.5).

#### Threat 10: Insider Threat

A legitimate user such as an administrator or technician abuses or mishandles granted access, intentionally or accidentally disrupting services, altering configurations, or degrading test integrity. In this network, where data sensitivity is modest, availability and operational reliability are the primary concerns.

**Control Strength** (CS, Table 2.5) is **Moderate** when per-user accounts exist but role scoping, detailed activity logging, or behavior monitoring are incomplete.

**Threat Capability** (TCap, Table 2.4) is **High** because insiders understand procedures and assets and may already possess elevated privileges.

Combining **Moderate** CS with **High** TCap yields **High** Vuln (Fig. 2.3).

**Threat Event Frequency** (TEF, Table 2.6) is **Moderate**. Mistakes and policy deviations occur in small and fast-moving teams, and temporary staff turnover can increase error rates.

Using Fig. 2.4, **High** Vuln with **Moderate** TEF results in **Moderate** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Low**. Effects are mainly service disruption, configuration drift, or invalid test results rather than large financial or reputational harm.

With LEF **Moderate** and PLM **Low**, the overall **Risk Magnitude** is **Moderate**. (Fig. 2.5).

#### Threat 11: Advanced Persistent Threat (APT)

A user inside the network may unknowingly enable an attacker to gain long-term and covert access, for example through a phishing link. Once inside, the adversary may move laterally, exfiltrate data, or plant backdoors for continued control.

**Control Strength** (CS, Table 2.5) is **Low** under the baseline assumptions of limited anti-phishing controls, no endpoint EDR, and only basic email filtering. Social engineering remains difficult to fully prevent without layered defenses.

**Threat Capability** (TCap, Table 2.4) is **High** for well-resourced and persistent actors who use phishing, privilege escalation, lateral movement, and covert C2.

With **Low** CS and **High** TCap, the **Vulnerability** (Vuln) is **High** (Fig. 2.3).

**Threat Event Frequency** (TEF, Table 2.6) is **Moderate**. Phishing attempts are common, though successful multi-step compromise still requires several conditions to align.

Using Fig. 2.4, **High** Vuln with **Moderate** TEF gives **Moderate** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **High** due to potential long dwell time, service disruption, and data exposure if a foothold is achieved.

With LEF **Moderate** and PLM **High**, the overall **Risk Magnitude** is **High** (Fig. 2.5).

#### Threat 12: Access Point Failure

An AP fails due to hardware defect, environmental stress such as rain, dust, or heat, or loss of power. Outdoor units for example WAX610Y are weather resistant IP55 and designed for outdoor temperature ranges, while indoor units such as WAX610 are not [50]. In sparse or repeater-style topologies, a single AP outage can remove coverage or break a backhaul hop.

**Control Strength** (CS, Table 2.5) is **Low** when APs are deployed without redundancy, health monitoring, or appropriate environmental rating and protection for the location.

**Threat Capability** (TCap, Table 2.4) is **Low to Moderate**. No special skill is required for environmental or power related outages and physical disruption or accidental disconnection is plausible in field conditions.

With **Low** CS in single path and non self healing layouts and **Low to Moderate** TCap, the **Vulnerability** (Vuln) is **High** (Fig. 2.3).

**Threat Event Frequency** (TEF, Table 2.6) is **Low**. Outright device failure is infrequent over a short festival deployment, though exposure to weather and ad hoc power can raise the chance.

Using Fig. 2.4, **High** Vuln with **Low** TEF results in **Low** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Low**. Impact is mostly localized loss of Wi Fi or a mesh hop and not data compromise.

With LEF **Low** and PLM **Low**, the overall **Risk Magnitude** is **Low** (Fig. 2.5).

**Context note — WDS vs mesh**

In a controller managed mesh with overlapping coverage and multi hop path selection, single node loss is typically self healed by rerouting [4, 39]. In a WDS or repeater chain or with minimal overlap, a node failure can still partition the network.

**Context note — MTBF availability**

Vendor documentation for the selected models (*WAX610* and *WAX610Y*) does not list mean time between failures (MTBF). [50]

#### Threat 13: Battery Depletion in Access Points

Battery-powered APs may run out of energy during operation, particularly under high traffic load or during poor charging conditions such as overcast weather for solar. This causes partial or complete loss of wireless coverage in affected areas and disrupts connectivity for users and services.

**Control Strength** (CS, Table 2.5) is **Low**. There is no battery state monitoring, no predictive alerting, and no explicit redundancy in AP placement to compensate for power loss.

**Threat Capability** (TCap, Table 2.4) is **Very Low** because this is a non-malicious operational failure mode rather than an adversarial action.

Given **Low** CS and the environment's dependence on continuous power, the resulting **Vulnerability** () is assessed as **High** (Fig. 2.3).

**Threat Event Frequency** (TEF, Table 2.6) is **Moderate**. Depletion can recur during extended poor weather or sustained peak usage without load management.

Using Fig. 2.4, **Low** Vuln with **Moderate** TEF yields **Low** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Moderate**. Impact is localized to the coverage area of the affected AP, though effects are more pronounced in critical zones.

With LEF **Low** and PLM **Moderate**, the overall **Risk Magnitude** is **Moderate** (Fig. 2.5).

#### Threat 14: Backhaul Connectivity Loss

If the backhaul link (4G/5G, satellite, or fibre) fails, the network loses Internet connectivity even though the local mesh remains up. Causes include weather effects on satellite links, carrier outages, CPE or modem failure, cabling faults, or misconfiguration. In a festival scenario, this can disrupt payment processing and press or communications, while local-only services such as on-site camera viewing remain available.

**Control Strength** (CS, Table 2.5) is **Low**. The current PoC lacks dual-WAN failover, path diversity, and automated uplink health checks.

**Threat Capability** (TCap, Table 2.4) is **Moderate**. This is typically a non-malicious failure driven by environmental or provider issues rather than an active attacker.

With **Low** CS and **Moderate** TCap, the **Vulnerability** (Vuln) is **High** (Fig. 2.3).

**Threat Event Frequency** (TEF, Table 2.6) is **Moderate**. Remote or congested deployments can see periodic uplink interruptions due to weather, RF congestion, or equipment faults.

Using Fig. 2.4, **High** Vuln with **Moderate** TEF yields **Moderate** LEF.

**Probable Loss Magnitude** (PLM, Table 2.7) is **Significant** where Internet access is essential for payments or live external coordination. Local services are less affected but business-critical functions may halt.

With LEF **Moderate** and PLM **Significant**, the overall **Risk Magnitude** is **High** (Fig. 2.5). Backhaul is a single point of failure and requires redundancy and failover to be addressed.

**Future work**

Develop a simple dashboard to show primary and backup backhaul status, indicate which zones are bandwidth-prioritized during failover, and allow on-the-fly bandwidth reallocation.

## 4.3 Mitigations — What are we going to do about it?

**Risk Treatment for Threat 1: Spoofing the Identity of a User/Device (S–Spoofing)**

**Goal**
Reduce the feasibility of joining the network with a shared secret and improve accountability of who and what connects.

**Preferred control** *when supported*
Adopt WPA2/WPA3 Enterprise 802.1X with a RADIUS server for example FreeRADIUS on pfSense to enforce per user or per device credentials [67, 82]. Map roles to VLANs for example admin, cameras, payments, comms using RADIUS attributes. This removes the shared key and enables revocation and audit.

**Baseline controls** *with WPA2-PSK*

- **Strong rotating PSKs** Use high entropy PSKs $\geq$ 16–20 random characters and rotate for each deployment. Never reuse across events.
- **Per SSID VLAN isolation** Place PSK only clients on dedicated SSIDs and VLANs with deny by default pfSense rules for example cameras $\rightarrow$ only and payments $\rightarrow$ gateway IPs only and no lateral movement.
- **Client isolation on APs** Enable wireless client isolation on PSK SSIDs so peers cannot communicate directly.
- **Limit ciphers and features** Allow only AES CCMP. Require PMF where devices support it [50, 82].
- **Tight DHCP and addressing** Restrict DHCP scopes to expected counts and optionally reserve leases for known MAC addresses to reduce blast radius.
- **Management hygiene** Restrict APs and pfSense administration to the IT VLAN, use strong admin credentials, and disable SSID administration over wireless.

**Monitoring and detection**

- **AP side alerts** Enable built in rogue AP or client detection and association anomaly alerts such as duplicate MAC or excessive authentication failures on WAX610 or WAX610Y.
- **Central log collection** Forward AP and pfSense logs and RADIUS accounting if 802.1X is used to the central collector or SIEM see Chapter 5.
- **IDS building block** Deploy a network IDS sensor for association or authentication anomalies and east west policy violations. The specific IDS is selected in Chapter 5.

**Migration path**

1. *Now* Enforce strong per event PSK rotation and enable client isolation and segment PSK SSIDs into least privilege VLANs with pfSense rules.

2. *Next* Stand up FreeRADIUS on pfSense and move the IT or Admin SSID to WPA2 Enterprise for example PEAP or EAP TTLS and optionally use WPA3 Transition for newer devices [67].

3. *Then* Expand 802.1X to payments or comms where supported and consider dynamic VLAN assignment via RADIUS.

**Notes on scope and cost**
All measures above are compatible with pfSense and WAX610 or WAX610Y per vendor datasheet [50]. Baseline steps rotation and isolation and VLAN rules are low cost and fast to roll out. 802.1X adds account management overhead but delivers the strongest identity assurance.

**Cross reference**
The need for an  is recorded here as a control category. The concrete selection for example Suricata vs Snort vs Zeek is justified in Chapter 5 after a focused comparison.

**Decision**
Implement the baseline controls (high-entropy per-event PSKs, per-SSID VLAN isolation, client isolation, and PMF where supported) and record residual **Moderate** risk for the PoC. Reassess to **Low** once privileged SSIDs migrate to 802.1X (WPA2/WPA3-Enterprise) with server certificate validation and PMF required, and PSK use is confined to low-privilege segments. Central monitoring should flag authentication anomalies (e.g., repeated failures, duplicate MAC) to support early detection and tuning.

**Risk Treatment for Threat 2: Spoofing the Identity of an Access Point**

**Goal**
Reduce the likelihood and impact of evil twin attacks by strengthening client and AP authentication, limiting the blast radius for PSK clients, and enabling basic wireless threat detection.

**Preferred controls** *when supported*

- **WPA3 with PMF** Enable WPA3 on capable SSIDs with PMF set to required. For mixed WPA2/WPA3 SSIDs, set PMF to optional so legacy devices can still join while modern clients gain protection.
- **802.1X for the IT admin SSID** Use WPA2 Enterprise or WPA3 Enterprise with 802.1X on pfSense FreeRADIUS. Enforce server certificate validation on client devices to prevent credential capture on a rogue AP.

**Baseline controls** *deployable immediately*

- **Per event identity hygiene** Rotate SSID names and PSKs per event and use long random passphrases. Avoid reusing names like Festival Admin across events to make cloning less convincing.
- **Segmentation and least privilege** Map each SSID to a dedicated VLAN on pfSense and apply deny by default rules between VLANs. PSK VLANs should not reach management interfaces. Camera SSID allows only camera to viewing station flows and no Internet. Payment SSID allows only the required egress to payment gateways. Admin SSID reaches management services only through the firewall.

- **Client isolation** Enable client isolation on PSK SSIDs to block peer to peer traffic.
- **Protected admin path** For management traffic, prefer a tunnel from admin laptops to pfSense so that even if an admin joins a rogue SSID, the management plane still requires authentication and TLS certificate checks.

**Detection and response**

- **Rogue AP detection** Enable rogue AP detection in Netgear Insight and mark known BSSIDs as authorized so the controller can alert on look alikes.
- **Operational alerts** Configure pfSense and APs email or webhook alerts for rogue AP events. Keep a short on site runbook to verify and shut down suspicious SSIDs during the event.

**Device hygiene**

- On admin devices, disable auto join for public SSIDs and remove outdated SSIDs before the event.

**Decision**
With PMF on capable clients, per event SSIDs and PSKs, 802.1X for admin access, and VLAN isolation for PSK clients, the likelihood of successful evil twin exploitation is materially reduced and the impact is confined to low privilege segments, which means that the residual risk becomes **Low**. Some residual risk remains for legacy WPA2 PSK devices that cannot validate a RADIUS server certificate. We accept this residual risk for the PoC and document a migration path toward wider WPA3 and 802.1X coverage in Chapter 5.

**Risk Treatment for Threat 3: Integrity of the Logs (Tampering)**

**Goal**
Preserve basic auditability and deter casual log tampering with minimal overhead appropriate to the assessed Low risk.

**Baseline safeguards** *deployable immediately*

- Restrict pfSense administrative access with no shared credentials and HTTPS only GUI and MFA if available and disable shell access for non admin users.
- Ensure time accuracy with NTP on pfSense and APs so log timestamps are reliable.
- Enable log rotation on pfSense and retain a short window locally and after each rotation export archives to removable media and store a simple `sha256sum` manifest alongside them.

**Monitoring and alerts**

- Add a basic alert if the logging service stops or the log partition fills.

**Revisit trigger**
If incident reconstruction becomes a requirement, if any integrity issue is observed, or if a central sensor for example Security Onion is introduced, upgrade to remote log forwarding

and integrity marking for example central syslog or a SIEM with TLS and signed archives. Until then, local retention with the above hygiene remains proportionate to the assessed Low risk.

**Decision**
Implement the baseline safeguards and **accept** residual **Low** risk for this PoC.

### Risk Treatment for Threat 4: Integrity of the Camera Feed (Tampering)

**Goal**
Reduce the risk of stream manipulation or injection by hardening camera transport and strictly limiting who can communicate with cameras and the  in a real time only setting.

**Baseline controls** *deployable immediately*

- **Segmentation and allow listing** Place cameras in a dedicated Camera VLAN. On pfSense, permit only flows from the Camera VLAN to the NVR IPs and to required services such as NTP or DHCP. Prefer SRTP or RTSP over TLS for streams where supported. Deny Internet egress by default for the Camera VLAN.
- **Management hardening** Restrict camera admin interfaces to the Admin VLAN via pfSense rules. Enforce HTTPS for management, use unique strong credentials per device, remove default accounts, and disable unsolicited cloud or P2P access if present.
- **Health monitoring and logging** Configure the NVR or lightweight pfSense scripts to alert when a camera stops responding or when stream quality drops. Forward alerts to the central logger or SIEM if present. Sync time via a single NTP source for reliable correlation.
- **Wireless note** If any cameras are wireless, use WPA2 today with strong PSKs and client isolation on the camera SSID. *Future work* Prefer WPA3 with PMF when devices support it.

**Decision**
Given the assessed **Risk Magnitude = Low** and real time only use, we *accept the residual risk* after applying the above controls. Camera model selection will *require* secure streaming support, otherwise the device is out of scope for this PoC.

**Notes on scope and cost**
VLAN allow listing and management hardening are configuration only. Encrypted streaming support is a selection criterion for the camera or  and does not add separate licensing.

### Risk Treatment for Threat 4b: Physical Tampering of Camera Hardware

**Goal**
Deter and detect physical interference with cameras and keep useful coverage during incidents.

**Measures** *low cost, compatible with pfSense*

- **Vandal resistance and placement** Use tamper resistant mounts or housings and place cameras out of easy reach with overlapping fields of view.

- **Cable and power protection** Where any local power or network lead is exposed, protect the short run with a lockable box and conduit or sleeve to deter unplugging or cutting.
- **Basic monitoring** Configure a simple heartbeat or ping check and alert on loss of video or device offline.
- **Built in tamper detection** Enable camera tamper or cover detection and alert on trigger when supported.

**Decision**
Risk magnitude remains **Low** and we *accept the residual risk* after applying the above measures.

**Risk Treatment for Threat 5: Repudiation by an Administrator**

**Goal**
Establish reliable attribution for privileged actions and make tampering with evidence difficult to perform and easy to detect.

**Preferred control**
Use **per user admin identities** with **2FA** and **off box audit trails**. On pfSense, create individual admin accounts with least privilege in User Manager, enable TOTP for GUI logins, and disable any shared admin. Bind the GUI to the management interface only and disable the GUI on WAN. Forward pfSense and AP logs to a remote collector or SIEM with time sync across all devices. This aligns with OWASP guidance on logging and monitoring [52, 53].

**Baseline controls** *deployable immediately*

- **Per user admin accounts and least privilege** in pfSense User Manager. No shared credentials for GUI, SSH, or VPN.
- **RADIUS backed admin auth** with FreeRADIUS on pfSense for GUI and VPN where applicable. Enforce 2FA for human logins.
- **Remote logging** Enable syslog export on pfSense and WAX610 or WAX610Y to a lightweight collector or Security Onion. Ensure NTP on all nodes for consistent timestamps [34, 53].
- **Tamper evidence** Rotate logs daily on the collector and compute a hash manifest stored read only. Keep off device backups of pfSense `config.xml` with versioning.
- **Change tracking** Enable pfSense notifications for firewall rule edits, user changes, and IDS rule updates. Archive diffs with timestamps.
- **Harden remote access** Disable SSH password logins, require keys, and disable direct root login. Restrict management access to the IT VLAN only.

**Monitoring and detection** *lightweight*

- **Collector alerts** Basic alerts for admin login events, failed logins, config changes, and service restarts [25, 34].

- **AP and RADIUS logs** Forward WAX610 or WAX610Y and FreeRADIUS accounting logs to the same collector for correlation [50].

**Migration path** *pragmatic*

1. *Now* Create per user admins and least privilege roles. Enable TOTP for the GUI. Forward pfSense and AP logs off box. Enable NTP on all nodes.
2. *Next* Enforce RADIUS for admin and VPN access with 2FA. Archive and hash seal daily log bundles on the collector.
3. *Then* Centralize analytics in the selected SIEM from Chapter 5. Add dashboards and alerts for privileged events and configuration drift.

**Notes on scope and cost**
The steps above use built in pfSense features, FreeRADIUS, and native syslog on WAX610 or WAX610Y [50]. They are low cost and suitable for a temporary deployment. A full SIEM increases effort but improves detection and forensic quality [25, 34].

**Decision**
Implement the baseline controls and **accept** residual **Moderate** risk for the PoC. The centralized SIEM choice and any RADIUS alternatives are finalised in Chapter 5.

**Risk Treatment for Threat 6: Information Disclosure via Wireless Sniffing**

**Goal**
Keep traffic unintelligible to passive observers on the RF medium.

**Baseline controls** *deployable immediately*

- **No open SSIDs** Use WPA2 at minimum with AES-CCMP only. Disable WEP, TKIP, and WPS on WAX610 and WAX610Y [50].
- **Protected Management Frames** Require PMF on WPA3 SSIDs and set PMF to optional on mixed WPA2/WPA3 SSIDs [67, 82].
- **Per event PSK rotation** For PSK SSIDs, use high entropy passphrases and rotate at each deployment.
- **Encrypt management and media** Enforce HTTPS for device administration and SSH key authentication. For cameras, require SRTP or RTSP over TLS. Block clear text management and media protocols from camera and IT VLANs at the firewall.
- **TLS hygiene for Internet flows** Allow only TLS based egress from payment and comms VLANs by pfSense rules. Prefer HSTS capable services for admin portals.

**Monitoring** *lightweight*

- Enable AP security logs and alerts for cipher downgrades and association anomalies. Forward pfSense and AP logs to the central collector when available.

**Migration path** *pragmatic*

1. *Now* Disable legacy ciphers and WPS. Enable PMF. Enforce HTTPS and SSH. Rotate PSKs per event.
2. *Next* Enable WPA3 Transition on capable SSIDs and update client devices. Enforce SRTP or RTSP over TLS on cameras.
3. *Then* Migrate internal SSIDs to WPA3 only as device support permits [67].

**Decision**
With the above in place and given the assessed **Risk Magnitude = Low**, we **accept the residual risk**. A full WPA3 only posture remains a stretch goal to be pursued as legacy devices are phased out.

**Risk Treatment for Threat 7: Denial of Service — Wi-Fi Deauthentication Attack**

**Goal**
Limit the feasibility and impact of forged deauthentication or disassociation frames and keep critical operations usable during brief wireless outages.

**Preferred control** *future work*
Adopt WPA3 with **PMF** so management frames are authenticated and clients ignore forged deauthentication or disassociation packets [2, 82]. Use WPA3 only for high value SSIDs as device support allows. In mixed WPA2/WPA3 SSIDs, set PMF to required on WPA3 only SSIDs and optional on mixed mode so capable devices gain full protection [67]. The WAX610 and WAX610Y support these features [50].

**Baseline controls** *deployable immediately with WPA2 only*

- **Wire critical endpoints** Prefer Ethernet for the NVR or viewing station, payment gateway uplink, and admin workstation to remove them from Wi Fi deauthentication impact.
- **Reduce service impact** Keep DNS and NTP local, use long DHCP lease times, and configure applications to retry gracefully so micro outages do not stall sessions.
- **Client hygiene** On admin devices, disable auto join to public SSIDs and prefer the 5 GHz band. Keep PSK rotation per event to limit attacker preparation time.
- **Segmentation** Ensure the admin and payment paths traverse the firewall with least privilege so any brief client drops do not expose additional services.
- **Band agility** Allow automatic channel change on APs to escape incidental interference. This does not stop targeted deauthentication but can shorten incidental disruption.

**Monitoring** *lightweight*
Enable AP event logging and alerts for abnormal deauthentication or association failures and forward AP and pfSense logs to the collector when present [50]. During events, keep a short runbook to verify on site if repeated drops are observed.

**Decision**
With the baseline in place and the assessed **Risk Magnitude = Low**, we **accept the**

**residual risk** for the PoC. We plan a gradual move to WPA3 with PMF as legacy devices are retired.

**Risk Treatment for Threat 7b: RF Jamming / Interference**

**Goal**
Reduce susceptibility to single channel interference and recover service quickly when a channel is impaired.

**Low effort controls** *pfSense + WAX610/WAX610Y compatible*

- **Prefer 5 GHz and narrow channels** Use 5 GHz where possible and keep channels at 20 MHz in dense or temporary deployments to maximize non overlapping choices and reduce co channel contention [14, 15].
- **Enable automatic channel and power management** Allow the controller to select less congested channels and adjust power. Where supported, systems can switch away from impaired channels and steer clients accordingly [14].
- **Distribute SSIDs across bands** Put best effort traffic for example comms or press on one band and critical ops for example camera viewing on the other to avoid one RF domain taking down all use cases [14].
- **Simple placement diversity** Place APs so adjacent cells use different channels and avoid single points where one jammer blocks all coverage [14].
- **Backhaul resilience** Configure pfSense gateway groups for WAN failover so a local RF issue does not compound with backhaul instability [49].

**Monitoring and response** *lightweight*

- Enable controller or AP alerts for high channel utilization and DFS events and where supported jammed channel detection. Investigate and if needed force a channel change [14].
- Keep a short runbook to verify on site, rotate channel, temporarily move critical SSIDs to the alternate band, and document the event.

**Decision**
With the above low cost measures, **Risk Magnitude remains Low**. Residual risk is accepted for the PoC and documented as operationally tolerable during short lived deployments.

**Risk Treatment for Threat 8: Denial of Service — Service Saturation Inside the Network**

**Goal**
Preserve availability by preventing any one SSID, VLAN, or device from monopolizing shared links.

**Preferred control**
Combine **per SSID caps in Netgear Insight** with **per VLAN shaping on pfSense**.

Map each service class to its own SSID/VLAN on the WAX610 or WAX610Y, enforce bandwidth limits per SSID in Insight, and apply simple limiters on pfSense at the VLAN gateway. This provides clear isolation and predictable ceilings for heavy producers like video streams [13, 50].

**Baseline controls** *deployable immediately*

- **Per SSID VLANs** One SSID per role for example cameras, payments, comms or press, and IT. Tag to distinct VLANs. Deny by default between VLANs on pfSense [13, 50].
- **Per SSID bandwidth caps in Insight** Set reasonable up and down limits for each SSID so a single segment cannot saturate backhaul or mesh uplinks [50].
- **pfSense limiters per VLAN** Apply a simple upload and download limiter on each VLAN interface. Reserve headroom for critical services by giving their VLAN a higher ceiling.
- **Guest and comms hygiene** Optionally cap per client on the comms or guest SSID in Insight. Block bulk protocols not needed for the event on those VLANs.

**Monitoring and detection** *lightweight*

- **Insight usage charts** Watch SSID utilization and enable threshold alerts on unusual spikes [50].
- **pfSense graphs and logs** Track interface queues and limiter statistics. Alert if WAN or mesh uplink stays above a chosen utilization for several minutes.

**Migration path** *pragmatic*

1. *Now* Map SSIDs to VLANs. Enable per SSID caps in Insight. Add pfSense limiters per VLAN with conservative ceilings.
2. *Next* Tune ceilings after observing real traffic. Raise caps for payments and IT. Lower caps for comms or guest if they crowd the link.
3. *Then* If needed, add a simple priority queue so payment control traffic keeps low latency during peaks.

**Notes on scope and cost**
All measures use built in features of WAX610 or WAX610Y and pfSense. No extra hardware or licenses are required [50]. VLAN segmentation follows standard good practice for limiting blast radius and contention [13].

**Decision**
Implement the baseline controls. Residual risk is expected to drop from **Moderate** to **Low** once caps and limiters are tuned. We accept the remaining risk for the PoC and document tuning guidance for operations.

**Risk Treatment for Threat 9: Elevation of Privilege**

**Goal**
Prevent easy escalation by tightening access to the management plane, enforcing least privilege, keeping devices patched, and detecting and attributing privileged actions.

**Baseline controls** *deployable immediately*

- **Management plane isolation** Bind pfSense GUI and SSH and AP management to the *IT/Admin VLAN* only. Block reachability from all other VLANs with deny by default rules [13].
- **Per user admin accounts** No shared admin. Create individual pfSense users with minimal required privileges and enable TOTP for GUI logins. Apply the same model for Netgear Insight admins [52, 53].
- **Strong auth hardening** Disable SSH password logins on pfSense, require keys, and disable direct root login. On APs, disable remote management from non management networks.
- **Firmware and OS updates** Apply current pfSense releases and WAX610 or WAX610Y firmware via Insight before each event. Avoid end of life builds [50].
- **Service minimization** Remove unused packages and disable unneeded services on pfSense and on APs.

**Preferred controls** *when feasible*

- **RADIUS backed admin auth** Use FreeRADIUS on pfSense for GUI and VPN administration with 2FA. Keep per user accounting logs for attribution [53].
- **Config integrity** Keep versioned off device backups of `config.xml`. Alert on configuration changes and failed admin logins.

**Monitoring and detection** *lightweight*

- **Central logs** Forward pfSense and AP admin or auth logs to the collector or SIEM selected in Chapter 5. Ensure NTP sync for consistent timestamps [25, 34, 50].
- **Change and event alerts** Enable pfSense notifications for privilege changes, user edits, firmware updates, and service restarts.

**Migration path** *pragmatic*

1. *Now* Restrict management to the IT VLAN, remove shared admin, enable TOTP, and patch pfSense and AP firmware.
2. *Next* Enforce RADIUS with 2FA for admin and VPN access and centralize logs off box with basic alerts.
3. *Then* Add per role pfSense privileges and periodic config audits and integrate privileged event dashboards in the chosen SIEM.

**Notes on scope and cost**
All steps use built in pfSense features, Netgear Insight, and FreeRADIUS with no new hardware required [50]. Measures are low overhead and suitable for a temporary deployment.

**Decision**
Implement the baseline controls. Residual risk becomes **Low** for legacy or third party components. This is accepted for the PoC with the migration path documented for higher assurance deployments.

**Risk Treatment for Threat 10: Insider Threat**

**Goal**
Reduce the chance and blast radius of insider misuse and make actions attributable and reviewable.

**Baseline controls** *deployable immediately*

- **Per user authentication** Tie pfSense and management access to unique identities via FreeRADIUS and prohibit shared admin accounts for GUI, SSH, and VPN.
- **Least privilege** Restrict administrative roles to essential tasks only and separate day to day operations from high risk configuration changes.
- **Management plane isolation** Expose pfSense GUI and SSH and AP management only on the IT or Admin VLAN and block access from all other VLANs with deny by default rules.
- **Change hygiene** Version and back up `config.xml` before changes and require a quick peer check for high impact edits such as firewall rules, NAT, or VLANs.
- **Join or leave discipline** Use time bound accounts for temporary staff and disable them at teardown.

**Monitoring and detection**

- **IDS or IPS building block** Deploy a network IDS or IPS sensor to observe inter VLAN traffic and the management plane for policy violations and patterns associated with insider misuse. Start in IDS mode and consider enabling IPS only on the management VLAN for high confidence rules. The concrete engine such as Zeek, Snort, or Suricata is selected in Chapter 5 after comparison.
- **Central logs** Forward pfSense, AP, and RADIUS accounting logs to the collector or SIEM and enable NTP on all nodes and alert on admin logins, failed logins, and configuration changes.

**Preferred controls** *when feasible*

- **2FA for admins** Enable TOTP for the pfSense GUI and require 2FA for VPN and Insight admin users.
- **Separation of duties** Distinct roles for network admins versus camera operators and provide read only views where practical.

- **SIEM correlation** Add dashboards and alerts for privileged events and configuration drift once the SIEM from Chapter 5 is in place.

**Decision**
With per user authentication, least privilege roles, management plane isolation, and an IDS or IPS sensor monitoring privileged paths, the residual risk is acceptable for the PoC. Record residual **Moderate** risk due to inherent human factors and plan to tighten with 2FA, SIEM correlation, and selective IPS enforcement after the tooling choices in Chapter 5.

**Risk Treatment for Threat 11: Advanced Persistent Threat (APT)**

**Goal**
Contain multi step campaigns, prevent easy lateral movement, and shorten attacker dwell time in a temporary availability first deployment.

**Preferred controls** *identity centric access and tight egress governance*

- **Per user identities with MFA** for all admin access for example pfSense GUI using FreeRADIUS where possible and replace any shared admin with least privilege individual accounts.
- **Egress allow listing** at pfSense to limit command and control opportunities [45]. Permit only required destinations and protocols per VLAN for example DNS to the resolver, NTP, payment gateways, and software update sites and deny all other outbound by default.

**Baseline controls** *deployable immediately*

- **Segmentation and least privilege** Map roles to VLANs and enforce deny by default inter VLAN rules. Allow only explicit flows for example Camera VLAN to and IT VLAN to management IPs.
- **Admin hygiene** Bind management services to the IT or Admin VLAN, require  for remote admin, disable SSH passwords, and keep devices time synced with NTP.
- **Hardening at the edge** Remove default credentials on access points and cameras, use HTTPS for management, and disable unused services.

**Monitoring and detection** *lightweight*

- **IDS or IPS building block** Place a sensor at the inter VLAN choke to detect policy violations and suspicious east west traffic. The specific engine for example Suricata, Snort, or Zeek is selected in Chapter 5.
- **Log and correlate** Forward pfSense, AP, and RADIUS logs to the central collector or SIEM for privileged events and anomalous connections [34, 53].
- **DNS visibility** Log and review DNS queries from user VLANs to spot beaconing and unusual domains [45].

**Migration path** *pragmatic*

1. *Now* Enforce VLAN segmentation with deny by default, add basic egress allow lists, require  for admin, and enable per user admin accounts with MFA.

2. *Next* Deploy the IDS or IPS sensor and central log collector and add alerts for inter VLAN policy violations, unusual DNS, and new admin accounts.

3. *Then* Expand per user Wi Fi with 802.1X where devices support it and refine egress rules to only the destinations observed as necessary during the event.

**Notes on scope and cost**
All steps are compatible with pfSense and the WAX610 or WAX610Y. Baseline segmentation and egress allow listing are low cost and effective in a temporary setting. Central analytics improves detection quality but can remain lightweight for the PoC [34].

**Decision**
Implement the baseline controls. With segmentation, egress allow lists, and basic monitoring, we expect a reduction from **High** to **Moderate** risk for the PoC. Residual risk is accepted and revisited if higher sensitivity assets are introduced.

**Risk Treatment for Threat 12: Mesh Node Failure**

**Goal**
Maintain service when an individual AP or node fails and reduce environment related outages.

**Baseline controls** *low effort, compatible with pfSense + WAX610/WAX610Y*

- **Right device, right place** Deploy *WAX610Y* outdoors for IP55 and outdoor temperature or humidity ranges and keep *WAX610* indoors only. Protect short power leads and connectors [50].

- **Overlap for resilience** Plan RF so each critical area has coverage from $\geq 2$ APs. Avoid single hop chokepoints. Prefer a controller managed mesh to allow automatic reroute on node loss [4, 39].

- **Simple health checks** Enable Netgear Insight and pfSense reachability checks such as ping or HTTP to each AP. Alert on AP offline and on backhaul degradation.

- **Power hygiene** Add strain relief and weather protection for local DC runs. Use surge protection where feasible. Verify solar or battery budget with margin for overcast periods.

- **Spares on site** Keep 1–2 pre provisioned APs and power kits to swap failed nodes quickly.

**Monitoring and response**

- **Alarms and runbook** Alert on AP down and backhaul down. Document a 3–5 step swap procedure and alternate mounting points to restore overlap fast.

- **Periodic verification** Before doors open, run a brief walk test to confirm overlapping coverage and mesh paths. Re check after any site changes.

**Migration path**

1. *Now* Ensure overlapping coverage and enable basic Insight or pfSense availability alerts.

2. *Next* Move from WDS or repeater chains to a controller managed mesh for self healing path selection see Chapter 5 [4, 39].

**Decision**
With outdoor rated hardware where needed, overlapping coverage, basic health monitoring, and on site spares, the **Risk Magnitude remains Low**. We *accept* the residual risk for the PoC.

**Risk Treatment for Threat 13: Battery Depletion in Access Points**

**Goal**
Maintain coverage and graceful service under AP power loss in a solar or battery setup without native battery telemetry.

**Baseline controls** *deployable now with pfSense and WAX610/WAX610Y*

- **Overlapping coverage** Place APs so every critical area can reach at least two APs. Validate overlap with a quick site walk and RSSI check before the event.

- **Simple health checks** Use Netgear Insight AP offline alerts if available. In parallel, add a pfSense script or gateway monitor that pings each AP management IP and emails on failure.

- **Load trimming on APs** Disable nonessential SSIDs during low use hours using SSID schedules. Keep only the critical SSIDs up when battery is expected to be lowest.

- **Service shaping** Cap bandwidth on noncritical SSIDs in Insight and prefer lower bitrate camera profiles during the event to reduce airtime and AP workload.

- **Spare power** Stage at least one fully charged spare pack for each pair of APs. Document a swap procedure and label cabling for quick changeover.

- **Solar placement** Mount panels with proper tilt and avoid shading. Do a morning and afternoon visual check for unexpected shadowing from temporary structures.

**Optional enhancements** *for longer deployments*

- **Smart power sources** Prefer battery or UPS models with basic telemetry such as SNMP, an API, or Bluetooth in future iterations so remaining capacity can be monitored centrally.

- **Brownout cues** If power telemetry is unavailable, use indirect signals such as AP CPU load and association count trends to trigger manual SSID shedding or a battery swap playbook.

- **Tier the sites** Put higher capacity packs on critical APs and plan a nightly top up for noncritical APs when feasible.

**Decision**
Implement the baseline controls above and the residual risk becomes **Low** for this PoC even if the current battery model lack of telemetry. Revisit with smart batteries or inline meters if multi day uptime becomes a hard requirement.

**Risk Treatment for Threat 14: Backhaul Connectivity Loss**

**Goal**
Remove the single point of failure on the  and keep a minimum viable service during outages.

**Preferred control**
Configure **dual  failover on pfSense** using *Gateway Groups*. Monitor the primary  with health checks and fail over automatically to a backup link when loss or latency crosses a threshold. Use *diverse last mile technologies* for example Starlink plus 4G or 5G to avoid correlated failures.

**Baseline controls** *deployable immediately*

- **Gateway monitoring** Enable  monitoring on pfSense and set a Tier 1 primary and Tier 2 backup gateway group. Trigger on packet loss and high RTT, not just link down.
- **Local resilience** Keep critical local services working without the Internet. Allow on site camera viewing, local  and DHCP, and admin access to continue during backhaul loss.
- **Prioritization on backup** Apply a simple traffic shaper or limiters so that backup bandwidth is reserved first for *payments* and *IT admin*, then for comms or guest.
- **Health and alerting** Enable GUI, email, or webhook alerts for gateway up or down and failover events. Add a basic synthetic check to an external payment endpoint if applicable.

**Alternative**
If pfSense is not available, a dedicated multi  router for example SMB class with failover and policy routing can provide similar functionality at higher cost and with less flexibility.

**Migration path** *pragmatic*

1. *Now* Add a secondary  for example 4G or 5G. Create a gateway group with the primary at Tier 1 and the backup at Tier 2. Turn on alerts and test failover.
2. *Next* Add simple  so payment and admin VLANs are prioritized on the backup link. Document runbook steps for manual reprioritization during incidents.
3. *Then* Consider limited load sharing when both links are up and add out of band management for remote recovery.

**Notes on scope and cost**
Dual  and gateway monitoring are built into pfSense so there is no extra licensing. The main trade off is reduced capacity while on the backup link which is mitigated by per VLAN prioritization.

**Decision**
Implement pfSense dual  failover with diverse backhaul and lightweight . Accept residual risk of reduced bandwidth during failover with payment and IT traffic prioritized to maintain essential operations.

## 4.4 Validation — Did we do a good job?

This section validates that the selected treatments reduce risk to acceptable levels for a temporary, availability-first deployment.

### 4.4.1 Risk summary

The table below summarises, for each threat, the *baseline* risk (before controls) and the *residual* risk expected once the selected treatments in the Mitigations section are in place.

Table 4.1: Risk summary per threat: baseline vs. residual (after selected treatments)

| # | Threat | Baseline Risk | Residual Risk |
|---|---|---|---|
| 1 | Spoofing identity of a user/device | Moderate | Low |
| 2 | Spoofing identity of an AP (evil twin) | Moderate | Low |
| 3 | Integrity of the logs | Low | Low |
| 4 | Integrity of the camera feed | Low | Low |
| 4b | Physical tampering of camera hardware | Low | Low |
| 5 | Repudiation by an administrator | Moderate | Moderate |
| 6 | Information disclosure via wireless sniffing | Low | Low |
| 7 | DoS — Wi-Fi deauthentication attack | Low | Low |
| 7b | DoS — RF jamming / interference | Low | Low |
| 8 | DoS — Service saturation inside the network | Moderate | Low |
| 9 | Elevation of privilege | Moderate | Low |
| 10 | Insider threat | Moderate | Moderate |
| 11 | Advanced persistent threat (APT) | High | Moderate |
| 12 | Mesh node/access point failure | Low | Low |
| 13 | Battery depletion in access points | Moderate | Low |
| 14 | Backhaul connectivity loss | High | Moderate |

- Residual **Moderate** indicates risk has been reduced but not eliminated. Further reduction is planned via the documented migration paths (e.g. broader 802.1X, tighter egress, refined QoS/SIEM correlation).
- Biggest improvements: T11 (APT) and T14 (Backhaul) fall from **High** to **Moderate** due to segmentation/egress controls and dual-WAN failover.
- Low risks (e.g. T3, T4/4b, T6, T7/7b, T12) remain **Low** and are accepted for the PoC given low PLM and short deployment duration.

**Validation method.** Residual figures were derived using the FAIR-style approach (control strength → vulnerability, vulnerability + TEF → LEF, and LEF + PLM → risk) then sanity-checked via the acceptance checks below.

### Acceptance checks (evidence)

- **AP/node loss** — power off one WAX610Y: clients re-associate to a neighbouring AP, coverage degrades but persists (T12).

- **WAN failover** — disable WAN1: pfSense promotes WAN2 within the target interval, payment/test endpoints remain reachable (T14).
- **Segmentation** — inter-VLAN probes from guest: blocked by deny-by-default rules, only allow-listed flows pass (T8/T9/T10/T11).
- **Monitoring pipeline** — generate benign test alerts (port scan/synthetic pcap): Suricata/Zeek events and pfSense logs appear in Security Onion with correct timestamps and fields.
- **Local-first** — pull uplink: local DNS/auth and NVR remain usable, admin access via IT VLAN maintained (T14).

### Resilience levers and effects

Table 4.2: Resilience levers, effects, and threat coverage

| **Lever** | **Effect** | **Threats** |
|---|---|---|
| Mesh overlap | Clients fail over to another AP | T12, T13 |
| Dual, diverse | Backhaul fails over to backup | T14 |
| Segmentation | Faults stay in their VLAN | T8, T9, T10, T11 |
| Local-first services | DNS, auth, NVR work offline | T14 |

### Remaining gaps and outcome

**Gaps:** single pfSense node as a core dependency, no battery telemetry on current packs, and limited resilience to wide-area RF jamming.
**Outcome:** compared to the initial design, the network now degrades gracefully under node or backhaul faults and keeps core operations available while issues are remediated.

# Chapter 5
# Proof of Concept Improvement

In the previous chapter, we identified security weaknesses in the initial PoC deployable network and proposed mitigations. Based on that analysis, this chapter narrows the focus to two critical decision points: selecting the IDS and choosing a centralized log analysis/SIEM platform. For each, we compare viable options, evaluate them against the constraints of a temporary festival deployment (modest hardware, limited ops overhead, mixed client capabilities), and justify the final selection.

Our evaluation criteria include detection coverage and rule ecosystem, performance on pfSense-class hardware, ease of deployment and tuning, interoperability with VLAN segmentation and RADIUS authentication, quality of alerts and logs for incident response, and overall operational cost for a short-lived event network. The outcome is an open-source IDS on the pfSense firewall (Snort, optional inline IPS) and an integrated SIEM/Network Security Monitoring (NSM) platform (Security Onion Standalone) for correlation and dashboards (see Figure 5.1 for the final design context). Other improvements (e.g., VLAN segmentation, SSID authentication models, bandwidth controls, and dual-WAN failover) are already addressed in the security analysis and are only referenced here where they interact with the IDS/SIEM choices.

## 5.1 Intrusion Detection System (IDS) Selection: Snort vs. Suricata vs. Zeek

### Comparative Analysis of Candidate IDS Solutions

An intrusion detection system was needed to continuously monitor network traffic for signs of malicious activity or policy violations. We evaluated three open-source IDS options for integration into our network: Snort, Suricata, and Zeek (formerly Bro). Each has distinct characteristics:

- **Snort**: A classic rule-based Network IDS (NIDS) known for its extensive signature repository and long history in industry [38, 61]. Snort operates primarily single-threaded (until Snort3, which introduced multi-threading), inspecting packets against a database of known threat signatures. It is well-supported on pfSense via an official plugin package [48], simplifying deployment on our firewall platform. On the downside, Snort can become resource-intensive under heavy throughput due to its single-threaded nature – this architecture is a known performance bottleneck that can lead to high packet drop rates if not carefully tuned [81]. In multi-core hardware environments, Snort cannot natively utilize multiple cores (Snort2.x), so CPU scaling is limited, although running multiple Snort instances or using Snort 3 can partially mitigate this [69]. On pfSense, Snort can also run inline as an IPS that blocks matching traffic, but false positives will be blocked too and can disrupt legitimate flows.

- **Suricata**: A modern NIDS that, unlike Snort, is designed with multi-threading (and even optional GPU acceleration for pattern matching) in mind [79]. Suricata can

often handle higher traffic volumes by parallelizing packet processing across CPU cores, leading to better throughput and scalability on multi-core servers [69, 81]. It is compatible with the same rule syntax as Snort (e.g., Emerging Threats and Snort VRT rule sets) [81], and a Suricata package is also available for pfSense [48]. This makes it a strong alternative, promising better performance in high-bandwidth environments. However, Suricata's memory and CPU footprint can be higher – studies have noted that Suricata achieves its greater throughput at the cost of increased resource utilization compared to Snort [69]. In practice, its detection efficacy is very similar to Snort when using the same rules, since both engines rely on an identical set of signatures for known threats [69]. Integration into pfSense is slightly less mature (Snort's package has been available longer on pfSense), but Suricata is still well-supported. On pfSense, Suricata can also run inline as an IPS that blocks matching traffic, but any false positives will be blocked too and may disrupt legitimate flows.

- **Zeek (Bro)**: A network monitoring and IDS framework that differs from Snort/-Suricata by focusing on detailed traffic logging and anomaly detection rather than purely signature matching. Zeek passively monitors network flows and generates rich logs (for queries, HTTP sessions, TLS handshakes, etc.), enabling identification of suspicious behaviors via custom policy scripts [43]. It excels at providing context for forensic analysis and long-term trend monitoring. However, Zeek is not available as a plug-and-play package on pfSense – deploying it would require a separate server or virtual machine tapping into the network traffic. Zeek's output is also more log-oriented (needing aggregation and analysis via a SIEM or log management system to derive actionable alerts), and it does not perform inline packet blocking by itself (Zeek operates in IDS mode only, with no built-in IPS capability) [81]. Given our resource constraints and need for an easily integrated solution, using Zeek would introduce significant complexity for this project.

**IDS Selection—Conclusion.** We select Snort on the existing pfSense firewall. This choice reflects our constraints and priorities: (i) tight pfSense integration with a mature GUI package, (ii) sufficient performance for our moderate, event-scale traffic, (iii) comparable detection for known threats when using community rule feeds, (iv) low operational overhead (no extra sensor host), and (v) strong documentation and community. We acknowledge Suricata offers better multi-core scalability and would be preferred if throughput or rule volume grows materially, while Zeek excels at rich, contextual telemetry and could be added later on a separate host to enrich the SIEM. Additionally, Snort on pfSense can run inline as an IPS, giving a clear path from IDS-only to selective prevention on high-confidence rules. This is a plus for future adaptation, provided we stage the change carefully and tune to minimize false positives since blocked packets will interrupt legitimate flows.

## 5.2 Security Information and Event Management (SIEM) Selection: Elastic Stack vs. Splunk vs. Security Onion

### Comparative Analysis of Candidate SIEM Solutions

In addition to real-time intrusion alerts, a centralized logging and analysis capability was needed to aggregate events from the firewall, IDS, authentication system, and APs, and to support monitoring and triage. We considered:

- **Elastic Stack (ELK)**: Elasticsearch, Logstash, and Kibana with Beats provide a flexible open-source stack for log aggregation and search. ELK can ingest pfSense logs and Snort alerts, index them, and present custom dashboards in Kibana for queries like Wi-Fi associations or IDS alerts per VLAN [29]. The approach is cost-effective and highly adaptable to bespoke views. The trade-off is integration effort on our portable server where we must size JVM memory, design index lifecycle policies, and tune parsers. For small deployments ELK is feasible and widely used for network security monitoring [8]. Time-to-value can be slower because packet capture, NIDS engines, and content correlation need to be assembled rather than enabled out of the box.

- **Splunk**: Splunk offers powerful search, correlation, and alerting with many device integrations and a polished interface. It would ingest pfSense logs and Snort alerts with relatively little configuration and provides strong built-in content for dashboards. The free tier's daily ingest limit (~500 MB) is easy to exceed in an event setting and enterprise licensing costs are significant [76, 77]. A separate server or Virtual Machine (VM) must be sized for anticipated volume. Given budget constraints and our preference for open-source where possible, Splunk is technically attractive but not a practical fit for this PoC.

- **Security Onion**: Security Onion bundles Suricata and Zeek with an Elastic-based UI and curated dashboards for network security monitoring [8]. The *Standalone* profile is designed for small sites and PoCs and includes documented guidance for CPU, RAM, and SSD storage [68]. Packet capture, NIDS, parsing, storage, and dashboards are pre-wired which shortens deployment time and reduces custom plumbing. One host with a SPAN or TAP feed can deliver alerts and rich protocol metadata quickly. This overlaps with a separate Snort deployment but yields faster operational visibility in a temporary, deployable context.

*Snort on pfSense — integration options.*

- **Hybrid**: Keep Snort inline on pfSense as a narrow IPS for high-confidence rules while Security Onion runs passively for deeper detection and hunting. This preserves limited auto-blocking at the edge and keeps most detection in monitor mode to avoid over-blocking.

- **Passive only**: Disable Snort on pfSense and rely on Security Onion's Suricata and Zeek for detection with pfSense used for manual containment. Operations are simpler and there are no inline drops. Response becomes a documented playbook action instead of automatic blocking.

*SIEM Selection — Conclusion.* We select **Security Onion (Standalone)** for this PoC. It provides integrated NIDS, rich protocol telemetry, and Elastic-backed search with minimal integration effort which suits a portable, time-boxed deployment [8, 68]. We will forward pfSense logs and RADIUS accounting to Security Onion to unify network and authentication visibility. Splunk is ruled out due to cost [76, 77]. ELK remains a viable alternative but requires more custom assembly for equivalent network security monitoring. For future adaptation we can retain Snort on pfSense in selective IPS mode or migrate fully to Security Onion's sensor stack as needs evolve.

## 5.3 Key Improvements

- **Transition from WDS to true mesh architecture:** The original PoC relied on Wireless Distribution System (WDS) bridging due to limited configuration options. The improved design uses the Netgear Insight cloud management platform to create a true mesh network with dynamic path selection and centralized management. This greatly enhances reliability and simplifies deployment of multiple APs, as the mesh can self-optimize links and provide seamless coverage (whereas WDS was prone to manual configuration and single-point failures).

- **Redundant internet connectivity:** The pfSense firewall now supports dual WAN uplinks (e.g., a primary fibre link and a backup 4G/Starlink connection). In case the primary internet link fails, traffic automatically fails over to the backup, preserving connectivity for critical services. This redundancy is crucial for an event scenario to maintain point-of-sale systems and safety communications even if one ISP link goes down.

- **Network segmentation via VLANs:** Each user group or service zone is assigned a unique VLAN, which is mapped to a dedicated SSID on the Wi-Fi. This strict Layer-2 isolation contains broadcast domains and limits lateral movement between segments. Implementing such network segmentation is a known best practice to limit the scope of attacks and prevent malware from spreading freely across the network. Inter-VLAN traffic is minimized and tightly controlled through firewall rules on pfSense. All traffic between VLANs must pass through the firewall, where we enforce access policies.

- **Granular firewall policy enforcement:** We implemented detailed access control lists on pfSense to regulate traffic between segments. For instance, client devices on the public guest VLAN cannot reach any internal server VLANs; IoT devices (e.g., IP cameras or payment terminals) are restricted to only communicate with their designated servers or out to the internet, but not with client subnets. These policies enforce the principle of least privilege across the network, ensuring that each segment only has the access necessary for its function. Any inter-segment traffic that is required (such as the FreeRADIUS server receiving authentication requests from the Wi-Fi APs, or point-of-sale terminals reaching a payment gateway) is explicitly defined in firewall rules; all other cross-VLAN traffic is blocked by default.

- **Bandwidth management:** Per-SSID bandwidth limits (configured via the Netgear Insight management for the WAX610 APs) ensure no single wireless network can monopolize the available throughput. We applied rate limiting on the guest SSID in particular, so that public users cannot consume all bandwidth at the expense of operational networks. This prevents guest traffic from affecting the performance of mission-critical services. Conversely, higher priority or guaranteed bandwidth can be allocated to critical SSIDs (e.g., cameras, payment system). Together with pfSense's traffic shaping capabilities, this keeps performance steady for important applications even under heavy overall load.

- **Intrusion detection across all VLANs with optional inline prevention:** We centralize detection in **Security Onion**. Its *Suricata* and *Zeek* sensors observe traffic from all VLANs via a switch port mirror or a hypervisor tap and send alerts and rich

metadata to the Security Onion Console. This makes a dedicated IDS on pfSense less critical for visibility. We retain **Snort on pfSense** as an *optional* inline IPS on selected paths for example the IT or Admin VLAN or WAN egress. We start in alert only mode to tune rules and then enable drop on a small set of high confidence signatures to reduce false positives. All alerts are forwarded to Security Onion for unified triage and correlation.

- **Centralized threat monitoring and log correlation (Security Onion):** We deploy **Security Onion (Standalone)** as the SIEM/NSM platform to aggregate network telemetry and logs in one place. pfSense firewall/DHCP/DNS events and FreeRADIUS accounting are forwarded (syslog/Beats), and Netgear Insight/AP syslogs are ingested as well. Security Onion's *Suricata* and *Zeek* provide signature alerts and rich protocol metadata. We retain Snort on pfSense in selective inline IPS mode and forward its alerts to Security Onion for unified triage. In the Security Onion Console (Elastic-backed dashboards), we correlate signals (e.g., a client that triggers Suricata signatures, shows unusual Zeek DNS, and has repeated RADIUS failures), enabling faster detection/response during the event. Centralized retention supports post-event audit and forensics from a single console.

This chapter thus presents the final version of the solution, which incorporates these improvements to create a more resilient and manageable architecture. The updated network design is illustrated in Figure 5.1.

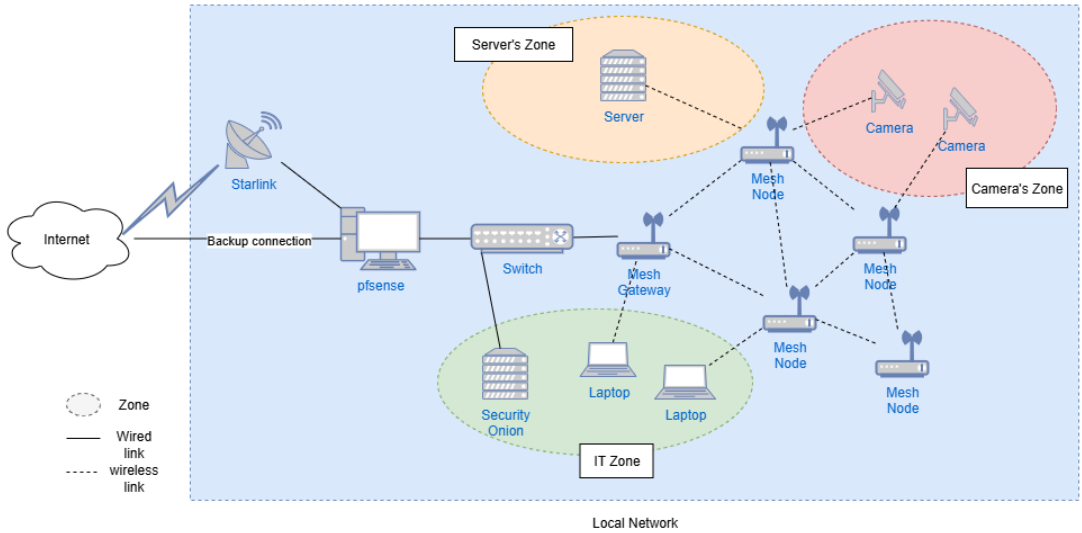



Figure 5.1: Final Network Architecture

## 5.4 Requirements

To implement the above solution, we utilized the following hardware and software components:

## Hardware Components

| Component | Role and Description |
|---|---|
| NETGEAR WAX610[1] | Indoor Wi-Fi 6 access point acting as the mesh gateway and root node. Provides primary wireless coverage and a wired uplink to the pfSense firewall. |
| NETGEAR WAX610Y[2] (×5) | Outdoor-rated Wi-Fi 6 access points that extend field coverage. These nodes form a mesh with the gateway AP to cover the venue. Powered from battery via PoE injector. |
| Managed L2 Switch with VLANs and SPAN[3] | Interconnects pfSense, the gateway AP, the on-site server, and backhaul CPE. Must support 802.1Q VLAN tagging. Provides a SPAN/mirror port feeding Security Onion's capture interface with no IP. Layer 2 only is sufficient because inter-VLAN routing is done on pfSense. |
| Portable Server | On-site virtualization host running KVM. Consolidates services: pfSense VM, Security Onion SIEM/IDS VM, and future VMs. |
| Mobisun Pro Portable Battery[4] (×5) | Portable battery systems with solar panels that power outdoor WAX610Y APs and other equipment where mains power is unavailable. Each connects to a PoE injector for the AP. |
| PoE Injectors (×5) | Power over Ethernet injectors sized to the AP power budget per the vendor datasheet. Provide power over a short Ethernet run to each outdoor AP. |
| Fibre | Primary backhaul (WAN1) where available. |
| LTE/5G Router | Primary or secondary backhaul (WAN1/WAN2) for pfSense multi-wan failover/load-balancing. |
| Starlink Terminal[5] | Primary or secondary satellite backhaul (WAN1/WAN2). Connect to a dedicated pfSense wan interface for automatic failover. |

Table 5.1: Hardware Components Used in the PoC Deployment

[1] `https://www.netgear.com/business/wifi/access-points/wax610/`
[2] `https://www.netgear.com/business/wifi/access-points/wax610y/`
[3] Any switch supporting IEEE 802.1Q and port mirroring
[4] `https://mobisun.com/en/product/portable-solar-panel-with-battery-and-socket-230v-300w-148-wh-40000mah/`
[5] `https://www.starlink.com/`

### Software Components

| Software Component | Host Platform | Role and Description |
|---|---|---|
| KVM[6] | Portable Server | Production hypervisor hosting the pfSense VM and the Security Onion VM, low overhead and headless operation |
| pfSense[7] | VM on KVM | Open source firewall/router; network core for routing, NAT, and security policy enforcement. Also provides DHCP, DNS resolver, and *local* NTP. **Example VM sizing (PoC):** ≥2 vCPU / 4 GB RAM / 20 GB disk[8]. Add CPU/RAM if enabling inline IPS or heavy packages. |
| Snort (optional IPS)[9] | pfSense (package) | Optional inline IPS on selected paths for example IT or Admin VLAN or WAN egress. Starts in alert only mode, can selectively drop high confidence signatures, forwards alerts to Security Onion for unified triage |
| FreeRADIUS[10] | pfSense (package) | Centralized authentication, enforces WPA2/WPA3 Enterprise 802.1X on staff or management SSIDs where supported with per user credentials and accounting |
| Local NTP Service | pfSense (ntpd) | Authoritative *local* time source for APs, cameras, servers, and admin laptops. Peers with public NTP when WAN is up, during outages provides holdover so logs stay aligned |
| Multi WAN Failover | pfSense | Dual WAN configuration with automatic failover between primary ISP and secondary for example Starlink or 4G or 5G |
| Security Onion[11] | VM on KVM | All-in-one NSM/monitoring/IDS distro (Suricata, Zeek, Elastic). **Standalone sizing (PoC):** ≥4–8 vCPU / 24–32 GB RAM / fast SSD ≥200 GB and **two NICs** (mgmt + capture)[12]. Ingests pfSense syslog, Snort alerts, FreeRADIUS accounting, and AP/Insight logs for correlation. |
| NETGEAR Insight (Premium)[13] | Cloud / Mobile App | Cloud management for WAX610 and WAX610Y APs: mesh configuration, SSIDs, VLANs, per SSID bandwidth limits, and AP status or alerts |

Table 5.2: Software Components Used in the PoC Deployment

**Contribution**

The configuration steps for pfSense (Snort, failover, NTP, VLANs) and Netgear WAX610/WAX610Y access points (mesh setup, SSIDs, bandwidth limits) are available at the following GitHub repository:
`https://github.com/Fufuches/Deployable-Wi-Fi-Mesh`

[6] `https://www.linux-kvm.org/`
[7] `https://www.pfsense.org/`
[8] `https://docs.netgate.com/pfsense/en/latest/hardware/size.html`
[9] `https://www.snort.org/`
[10] `https://www.freeradius.org/`
[11] `https://www.securityonionsolutions.com/software`
[12] `https://docs.securityonion.net/en/2.4/hardware.html`
[13] `https://www.netgear.com/insight/`

# Chapter 6
# Future Work

This work shows that a deployable Wi-Fi mesh can reduce installation time while keeping a defensible security posture. To progress from laboratory feasibility to reliable field operations, we outline the following priorities.

1. **Powering endpoints, not just APs.** The prototype assumed solar-powered access points. However, *end devices* (cameras, laptops, point-of-sale terminals) still need power. Future work should design and validate a solution. A deployable mesh reduces data cabling, but some power cabling remains unavoidable.

2. **Real-world pilot and metrics.** Conduct a live pilot (festival or military exercise) to quantify client density limits, multi-hop throughput, latency, roaming performance, and mean time to recovery (MTTR) after AP or backhaul loss. Tie measurements to service objectives (e.g., payments, security video) and validate energy budgets under realistic duty cycles (insolation/shading, temperature, charging profiles).

3. **Adversarial testing (penetration test).** Execute red-team drills on the deployed network to uncover vulnerabilities (e.g., evil-twin, deauthentication, basic jamming). Use the results to tune IDS/IPS rules, alert thresholds, and response playbooks, and verify that mitigations (e.g., WPA3 with PMF, segmentation) measurably reduce impact and detection time.

4. **Broaden the threat model.** Incorporate findings from the red-team report, add any missed threats, and update/validate mitigations.

5. **Placement, weather, and robustness.** Develop deployment guides for solar panels and APs (height, antenna orientation, channel plan). Validate environmental resilience: IP-rated enclosures, strain relief, UV-resistant cabling, thermal behaviour, ingress protection, and tamper-resistant mounting suitable for crowds and adverse weather.

6. **Protecting logs and observability.** Treat the logging stack as a protected asset. Implement mutually authenticated, encrypted log transport; append-only or retention-locked storage; cryptographic integrity (e.g., hash chaining/HMAC). Maintain disciplined time synchronisation (NTP), strict role-based access, and offline/immutable backups. Add detections for log flooding and false-event injection, and define procedures to preserve forensic data during power loss or device swaps. Consider off-site log replication to an external server or cloud storage with bandwidth-aware buffering.

7. **Improve power.** Add smart batteries/inline meters for APs (telemetry + alerts).

These steps move the system from proof-of-concept to repeatable field readiness: powering the full ecosystem (not only APs), validating performance and mitigations under real conditions, hardening against environment and broader threats, and ensuring that visibility data remain trustworthy when it matters most.

# Chapter 7
# Conclusions

This thesis examined whether a deployable Wi-Fi mesh can reduce time to setup in temporary environments while maintaining a defensible security posture. Starting from a functional but minimally secured PoC, a threat-driven analysis (STRIDE with a FAIR-inspired, semi-quantitative assessment) guided a hardening plan built around segmentation, centralised logging and monitoring, intrusion detection, and (where supported) WPA3 with PMF.

With far fewer data cables to pull, pre-configured images and templated policies bring the mesh online much faster than traditional wired builds. Candidate IDS and SIEM options were compared with an emphasis on portability and resource footprint; in the final design we deployed Security Onion (Standalone) for SIEM/NSM and retained Snort on pfSense as an optional inline IPS on selected paths, giving a clear route from monitoring to selective prevention.

A deployable Wi-Fi mesh is not a universal replacement for wired backbones. It excels when time-to-service, portability, and moderate client density are the dominant constraints. For high-throughput or deterministic-latency scenarios, wired (or hybrid) designs remain preferable. The mesh should therefore be viewed as a complementary approach that trades sustained capacity for speed and flexibility.

Two pragmatic caveats frame these conclusions. First, power: although access points were validated with solar/battery operation, endpoints (cameras, laptops, point-of-sale terminals) still require careful power distribution, safe DC runs, and brown-out policies. The mesh reduces data cabling, not the need for power cabling. Second, external validity: no live field trial was performed. Endurance and coverage measurements were obtained in controlled conditions and should be confirmed under real duty cycles, client densities, and weather.

A note on management and topology is important. The initial PoC relied on local AP configuration with WDS-style links, which limited self-healing and central policy. In the improved PoC, a controller-managed mesh (via Netgear Insight Premium) was adopted, enabling proper mesh formation, centralised configuration, and better roaming behaviour. While this removes the earlier WDS constraint and improves manageability, it introduces new aspects to validate in the field (e.g., controller availability during backhaul loss and vendor-specific feature coverage).

The research question can therefore be answered conditionally: a deployable Wi-Fi mesh can provide rapid, defensible connectivity for temporary sites when designed with threat-driven controls, segmentation, WPA3 with PMF where available, and strong observability through central logging and intrusion detection. Suitability depends on user density, backhaul quality, energy budget, and data sensitivity.

The principal limitation was the absence of a field pilot. This motivates the next steps set out in the *Future Work* chapter: validate the design in a live pilot with explicit service objectives, conduct adversarial testing to measure the effectiveness of mitigations,

harden deployment logistics (mounting, weatherisation, solar placement), plan power for endpoints, roaden the threat model (e.g., jamming, supply-chain and insider risks, backhaul trust), and protect log integrity and retention.

In conclusion, this work contributes a concise, threat-driven plan for securing deployable Wi-Fi meshes: retain rapid setup, and enforce least privilege between services, so that agility is achieved without compromising resilience.

# Bibliography


[1] Ietf manet working group — charter and rfcs, https://datatracker.ietf.org/wg/manet/about/ [Cited on page 8.]

[2] Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 4: Protected management frames. IEEE Std 802.11w-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, and IEEE Std 802.11y-2008) pp. 1–111 (2009) [Cited on pages 21, 36, and 47.]

[3] 802.11s mesh networking. Tech. rep., CWNP (2011) [Cited on page 8.]

[4] Ieee standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 10: Mesh networking. IEEE Std 802.11s-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011) pp. 1–372 (2011) [Cited on pages 5, 39, 53, and 54.]

[5] Ieee std 802.11s-2011: Mesh networking amendment (2011) [Cited on page 8.]

[6] Wpa3 will enhance wi-fi security. Tech. rep., National Security Agency (2018) [Cited on pages VI, 19, and 20.]

[7] Design considerations — wireless mesh constraints. Tech. rep., Cisco Systems (2020) [Cited on page 8.]

[8] AlgoSec: 9 Best Network Security Monitoring Providers for Identifying Cybersecurity Threats. AlgoSec Blog. https://www.algosec.com/blog/network-security-monitoring-tools (2024), [Accessed 30-07-2025] [Cited on page 60.]

[9] Ashraf, U., Khwaja, A., Qadir, J., Avallone, S., Yuen, C.: Wimesh: Leveraging mesh networking for disaster communication in poor regions of the world. CoRR abs/2101.00573 (2021) [Cited on page 6.]

[10] Camp, J.D., Knightly, E.W.: The ieee 802.11s extended service set mesh networking standard. IEEE Communications Magazine 46(8), 120–126 (2008) [Cited on page 6.]

[11] CAPEC: Capec-604: Wi-fi jamming, https://capec.mitre.org/data/definitions/604.html, [Accessed 02-06-2025] [Cited on page 20.]

[12] CAPEC: Capec-615: Evil twin wi-fi attack, https://capec.mitre.org/data/definitions/615.html, [Accessed 10-06-2025] [Cited on page 21.]

[13] Cisco: What is network segmentation?, https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html, [Accessed 27-06-2025] [Cited on pages 17, 49, and 50.]

[14] Cisco Meraki: Wi-fi channel planning best practices. Meraki Documentation (2018), https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Wi-Fi_Channel_Planning_Best_Practices, auto RF, channel/power selection, and reacting to jammed channels [Cited on page 48.]

[15] Cisco Meraki: Wi-fi 6: The next generation of wireless. White Paper (2019), https://meraki.cisco.com/lib/pdf/meraki_whitepaper_wifi6.pdf, notes 20 MHz operation is effective with OFDMA and in dense deployments [Cited on page 48.]

[16] Cisco Systems: What Is Cyber Resilience? https://www.cisco.com/site/us/en/learn/topics/security/what-is-cyber-resilience.html, [Accessed 29-06-2025] [Cited on page 16.]

[17] Cisco Systems: Cisco 802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3 (2013), https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.html [Cited on page 21.]

[18] Cisco Systems: Connect Multiple Access Points Together through Wireless Distribution System (WDS) (2019) [Cited on page 8.]

[19] Cloudflare: What is network segmentation?, https://www.cloudflare.com/en-gb/learning/access-management/what-is-network-segmentation/, [Accessed 27-06-2025] [Cited on page 17.]

[20] Corson, S., Macker, J.: Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations. RFC Editor (RFC 2501) (1999) [Cited on page 7.]

[21] Denning, D.E.: An intrusion-detection model. IEEE Transactions on Software Engineering SE-13(2) (1987) [Cited on page 17.]

[22] Drata: Using the stride threat model: Tutorial best practices, https://drata.com/grc-central/risk/guide-stride-threat-model, [Accessed 27-06-2025] [Cited on page 10.]

[23] Ertürk, M.A., Aydin, M.A., Vollero, L., Setola, R.: Ieee 802.11s mesh network analysis for post disaster communication. In: Boyaci, A., Ekti, A.R., Aydin, M.A., Yarkan, S. (eds.) International Telecommunications Conference. pp. 53–59. Springer Singapore, Singapore (2019) [Cited on page 6.]

[24] FAIR Institute: What is fair? (2023), https://www.fairinstitute.org/what-is-fair, accessed: 2025-07-09 [Cited on page 15.]

[25] Filkins, B.: An evaluator's guide to nextgen siem (2019), https://www.sans.org/media/vendor/evaluator-039-s-guide-nextgen-siem-38720.pdf, [Accessed 27-06-2025] [Cited on pages 19, 45, 46, and 50.]

[26] FireMon: The top 8 benefits of network segmentation, https://www.firemon.com/blog/network-segmentation-benefits/, [Accessed 27-06-2025] [Cited on page 17.]

[27] Fortinet: What is a firewall?, https://www.fortinet.com/resources/cyberglossary/firewall, [Accessed 19-05-2025] [Cited on page 16.]

[28] Fortinet: What is a honeypot? (2025), https://www.fortinet.com/resources/cyberglossary/what-is-honeypot [Cited on page 17.]

[29] Gashi, A.: Forwarding Snort logs to ELK stack. Medium (Cyber Academy Institute). https://medium.com/@armendgashx/forwarding-snort-logs-to-elk-stack-371232699e7f (2020), [Accessed 30-07-2025] [Cited on page 60.]

[30] Gast, M.S.: 802.11 Wireless Networks: The Definitive Guide. O'Reilly, 2 edn. (2005), foundational reference on 802.11 operation and security [Cited on page 3.]

[31] Georgas, I., Petropoulos, I., Voudouris, K., Tsiakas, P., Athanasopoulos, N., Cohen, M.V.H., Cyzs, B., Agapiou, G., Rigas, A.: Relay vs. repeater architectures in wimax. In: Mobile Multimedia Communications. pp. 229–241. Springer (2010) [Cited on page 4.]

[32] Henry, J., Burton, M.: 802.11s mesh networking (2011) [Cited on page 5.]

[33] Institute, S.: A practical application of sim/sem/siem: Automating threat identification (2021), https://www.sans.org/white-papers/1781/, [Accessed 27-06-2025] [Cited on page 19.]

[34] Institute, S.: Successful siem and log management strategies for audit and compliance (2022), https://www.sans.org/white-papers/33528/, [Accessed 27-06-2025] [Cited on pages 19, 45, 46, 50, 52, and 53.]

[35] Joaquin, L.: What is a mesh wifi network and how does it work?, https://www.tp-link.com/ph/blog/1835/what-is-a-mesh-wifi-network-and-how-does-it-work-/, [Accessed 18-06-2025] [Cited on page 5.]

[36] Johnson, A.: 31 Days Before your CCNA Exam: A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam. Cisco Press (2020) [Cited on page 4.]

[37] Kurose, J.F., Ross, K.W.: Computer Networking: A Top-Down Approach. Pearson, 8 edn. (2020) [Cited on page 3.]

[38] Lee, B.: Suricata vs snort: Which is the best ids? https://www.virtualizationhowto.com/2023/10/suricata-vs-snort-which-is-the-best-ids/ (2024), article published Oct 2023, updated 16 Aug 2024; Accessed: 14 Aug 2025 [Cited on page 58.]

[39] Lin, Y.D., Chang, S.L., Yeh, J.H., Cheng, S.Y.: Indoor deployment of ieee 802.11s mesh networks: Lessons and guidelines. Ad Hoc Networks 9(8), 1404–1413 (2011), recent advances on practical aspects of Wireless Mesh Networks [Cited on pages 6, 39, 53, and 54.]

[40] Martin-Vegue, T.: Six levers that quietly change your risk (2022), https://www.fairinstitute.org/blog/six-levers-that-quietly-change-your-risk, fAIR Institute Blog [Cited on page 15.]

[41] Mees, W.: Pragmatic cybersecurity. Independently published (2020) [Cited on pages 11 and 12.]

[42] metageek: Wi-fi signal strength basics, https://www.metageek.com/training/resources/wifi-signal-strength-basics/, [Accessed 19-05-2025] [Cited on page 26.]

[43] Michael, T.: Snort vs suricata vs zeek: Which open-source ids is best for 2025? https://tolumichael.com/snort-vs-suricata-vs-zeek/ (2025), [Accessed 29-07-2025] [Cited on page 59.]

[44] Microsoft: Threats - microsoft threat modeling tool (2022), https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN, [Accessed 27-06-2025] [Cited on page 10.]

[45] MITRE ATTCK®: Command and control, tactic ta0011 - enterprise, https://attack.mitre.org/tactics/TA0011, [Accessed 12-05-2025] [Cited on pages 11 and 52.]

[46] National Institute of Standards and Technology: Man-in-the-middle attack (mitm), https://csrc.nist.gov/glossary/term/man_in_the_middle_attack, [Accessed 19-05-2025] [Cited on page 21.]

[47] National Institute of Standards and Technology: Risk management framework (rmf) for information systems and organizations (2022), https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final, nIST Special Publication 800-37 Rev. 2 [Cited on page 15.]

[48] Netgate: Ids / ips (snort and suricata packages) — pfsense documentation. https://docs.netgate.com/pfsense/en/latest/packages/snort/ids-ips.html (2024), [Accessed 29-07-2025] [Cited on pages 58 and 59.]

[49] Netgate: Multi-wan (2024), https://docs.netgate.com/pfsense/en/latest/multiwan/index.html, gateway groups for failover and load balancing [Cited on page 48.]

[50] Netgear: Data sheet | wax610, wax610y, https://www.downloads.netgear.com/files/GDC/WAX610/WAX610_WAX610Y_DS.pdf?_ga=2.68151316.486267366.1733138210-1291023599.1732791289, [Accessed 02-06-2025] [Cited on pages 39, 41, 42, 46, 47, 49, 50, 51, and 53.]

[51] Otto, K.: How to set up a proof of concept Wi-Fi mesh network, https://cylab.be/blog/416/how-to-set-up-a-proof-of-concept-wi-fi-mesh-network, [Accessed 18-06-2025] [Cited on pages VI, 23, 25, and 26.]

[52] OWASP Foundation: Owasp top 10: A09:2021 - security logging and monitoring failures (2021), https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/, [Accessed 27-06-2025] [Cited on pages 18, 45, and 50.]

[53] OWASP Foundation: Logging cheat sheet (2023), https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html, [Accessed 27-06-2025] [Cited on pages 18, 45, 50, and 52.]

[54] OWASP Foundation: Threat modeling cheat sheet (2023), https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html, [Accessed 27-06-2025] [Cited on pages 10 and 27.]

[55] OWASP Foundation: Threat modeling process (2023), https://owasp.org/www-community/Threat_Modeling_Process, [Accessed 27-06-2025] [Cited on page 10.]

[56] Pahlavan, K., Krishnamurthy, P.: Evolution and impact of wi-fi technology and applications: A historical perspective. International Journal of Wireless Information Networks 28, 3–19 (2021) [Cited on page 4.]

[57] Patel, Z., Khanpara, P., Valiveti, S., Raval, G.: The evolution of ad hoc networks for tactical military communications: Trends, technologies, and case studies. In: Proceedings of the Third International Conference on Sustainable Expert Systems. pp. 331—-346. Springer (2023) [Cited on page 7.]

[58] Perkins, C., Royer, E.: Ad-hoc on-demand distance vector routing. In: Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications. pp. 90–100 (1999) [Cited on page 7.]

[59] Pranav, A., Jain, A., Ali, M.M., Raj, M., Gupta, U.: A comparative analysis of optimized routing protocols for high-performance mobile ad hoc networks. In: Proceedings of the Third International Conference on Computing and Communication Networks. pp. 95—-108. Springer (2024) [Cited on page 7.]

[60] Provos, N.: Honeyd - a virtual honeypot daemon (2004), http://www.honeyd.org/ [Cited on page 17.]

[61] Roesch, M.: Snort: Lightweight intrusion detection for networks. In: Proceedings of the 13th USENIX Systems Administration Conference (LISA '99). Seattle, WA, USA (1999) [Cited on pages 17 and 58.]

[62] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R.: NIST SP 800-160 Vol.2 Rev.1: Developing Cyber-Resilient Systems – A Systems Security Engineering Approach. Tech. rep., National Institute of Standards and Technology (2021) [Cited on page 16.]

[63] Roy, R.R.: Mobile ad hoc networks. In: Handbook of Mobile Ad Hoc Networks for Mobility Models, pp. 3–22. Springer (2010) [Cited on page 7.]

[64] SANS Institute: Syslog-ng and siem integration for security monitoring (2022), https://www.sans.org/white-papers/401/, [Accessed 27-06-2025] [Cited on page 18.]

[65] Scarfone, K., Mell, P.: Guide to intrusion detection and prevention systems (idps). Special Publication 800-94, National Institute of Standards and Technology (NIST) (2007) [Cited on pages 16 and 17.]

[66] Scarfone, K., Sexton, J.: Guidelines for securing wireless local area networks (wlans). NIST Special Publication 800-153 (2012), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf, discusses WLAN DoS risks and management-frame protections [Cited on page 36.]

[67] SecureW2: Wpa3 vs wpa2: What's the difference?, https://www.securew2.com/blog/wpa3-vs-wpa2, [Accessed 19-05-2025] [Cited on pages VI, 20, 41, 42, 46, and 47.]

[68] Security Onion Project: Security Onion 2.4 Documentation – Hardware Requirements (Standalone Deployment). https://docs.securityonion.net/en/2.4/hardware.html (2025), [Accessed 30-07-2025] [Cited on page 60.]

[69] Shah, S.A.R., Issac, B.: Performance comparison of intrusion detection systems and application of machine learning to snort system. Future Generation Computer Systems 80 (2018) [Cited on pages 58 and 59.]

[70] SmallNetBuilder: Everything you need to know about wireless bridging and repeating — part 1: Wds (2010), https://www.smallnetbuilder.com/wireless/wireless-howto/everything-you-need-to-know-about-wireless-bridging-and-repeating-part-1-wds/ [Cited on page 8.]

[71] Sommer, R., Paxson, V.: Outside the closed world: On using machine learning for network intrusion detection. In: IEEE Symposium on Security and Privacy (S&P) (2010) [Cited on page 17.]

[72] Souppaya, M., Scarfone, K.: Guidelines for securing wireless local area networks (wlans). Special Publication 800-153, NIST (2012) [Cited on pages 3 and 8.]

[73] Splunk: What is network segmentation? a complete guide, https://www.splunk.com/en_us/blog/learn/network-segmentation.html, [Accessed 27-06-2025] [Cited on page 17.]

[74] Team, N.O.: Wifi extender vs. mesh wifi: Which is right for you?, https://www.netgear.com/hub/technology/wifi-extender-vs-mesh-wifi-which-is-better/, [Accessed 18-06-2025] [Cited on page 5.]

[75] Toh, C.K.: Ad Hoc Mobile Wireless Networks: Protocols and Systems. Prentice Hall (2001) [Cited on page 6.]

[76] Tunggal, A.T.: Splunk vs ELK: Which Works Best For You? UpGuard Blog. https://www.upguard.com/blog/splunk-vs-elk (2025), [Accessed 30-07-2025] [Cited on page 60.]

[77] Udasi, A.: Breaking Down Splunk Costs for SREs and DevOps Teams. Last9 Blog. https://last9.io/blog/breaking-down-splunk-costs/ (2025), [Accessed 30-07-2025] [Cited on page 60.]

[78] Ugnė Zieniūtė: What is a deauthentication attack, and how does it work?, https://nordvpn.com/blog/deauthentication-attack/, [Accessed 19-05-2025] [Cited on pages 20 and 36.]

[79] VDA Labs: Lessons for the enterprise from running suricata ids at home (updated 2025). https://www.vdalabs.com/lessons-for-the-enterprise-from-running-suricata-at-home/ (2025), [Accessed 29-07-2025] [Cited on page 58.]

[80] VMware: Perfect forward secrecy definition, https://www.vmware.com/topics/perfect-forward-secrecy, [Accessed 19-05-2025] [Cited on page 20.]

[81] Waleed, A., Jamali, A.F., Masood, A.: Which open-source ids? snort, suricata or zeek. Computer Networks 213 (2022) [Cited on pages 58 and 59.]

[82] Wi-Fi Alliance: Security, https://www.wi-fi.org/discover-wi-fi/security, [Accessed 19-05-2025] [Cited on pages 21, 41, 46, and 47.]

# Appendix A

# Q&A with a Security Coordinator at Couleur Café Festival

The following transcript presents the insights of a security coordinator from the Couleur Café festival. To remain faithful to the original contribution, the introductory remarks he shared in French are provided here alongside their English translation. This is followed by the bilingual Q&A table.

## Introductory remarks

**Original (French):**

> Il y a de multiples utilisateurs et de multiples besoins qui peuvent différer d'un utilisateur à l'autre.
>
> Pour ce qui concerne la sécurité, la garantie d'avoir une connexion dans tous les cas de figure est une priorité absolue.
>
> Je n'ai personnellement jamais obtenu d'avoir accès au réseau Starlink qui peut assurer la connexion quand le réseau Proximus défaille. J'ai eu l'expérience une panne Internet généralisée pendant un événement. Le cas d'une situation de crise aigue a déjà provoqué la saturation des réseaux par l'usage intensif des festivaliers, bloquant ainsi son fonctionnement pour l'organisateur.
>
> Il y a donc deux critères à prendre en compte:
>
> 1. Un réseau suffisamment dimensionné pour absorber le déroulement « normal » en fonction de tous les utilisateurs.
> 2. Un réseau de secours en cas de saturation en situation de crise ou de panne des infrastructures Proximus.
>
> Parmi les utilisateurs citons:
>
> - les paiements aux bars,
> - les paiements aux restaurants,
> - la presse présente sur le site du festival,
> - les retransmissions filmées,
> - la communication interne entre différents organisateurs de l'événement, etc.

**Translation (English):**

> There are multiple users and multiple needs, which may differ from one user to another.

Regarding security, ensuring a connection under all circumstances is an absolute priority.

I personally never had access to the Starlink network, which can provide connectivity when the Proximus network fails. I have experienced a generalized Internet outage during an event. In the case of an acute crisis situation, intensive use by festival-goers has already caused network saturation, blocking its proper functioning for the organizer.

Therefore, two criteria must be taken into account:

1. A network sufficiently dimensioned to handle "normal" operations for all users.
2. A backup network in case of saturation during a crisis or failure of the Proximus infrastructure.

Among the users are:

- payments at the bars,
- payments at the restaurants,
- the press present on the festival site,
- live broadcasts,
- internal communication between different event organizers, etc.

## A.1 Q&A

| | |
|---|---|
| **Q: Le réseau joue-t-il un rôle dans la coordination des équipes de sécurité ?**<br>A: Oui, dans la mesure où un certain nombre de données sont à consulter. Non, dans la mesure où les communications entre les acteurs de terrain se font à l'aide de radios (Walkie-Talkie). | **Q: Does the network play a role in coordinating the security teams?**<br>A: Yes, to the extent that certain data must be consulted. No, as field communications are done via radios (walkie-talkies). |
| **Q: Quels types d'équipements sont généralement connectés au réseau pendant l'événement ? (Caméras, caisses, ordinateurs, tablettes, etc.)**<br>A: C'est ici que l'analyse des besoins est à faire ... En tous cas, les caméras sont en réseau et utilisées pour la sécurité. | **Q: What types of equipment are typically connected to the network during the event? (Cameras, cash registers, computers, tablets, etc.)**<br>A: This requires a needs analysis... In any case, cameras are networked and used for security. |
| **Q: Les images captées par les caméras de sécurité sont-elles enregistrées ? Si oui, sont-elles stockées localement ou dans le cloud ?**<br>A: Non. | **Q: Are the images captured by security cameras recorded? If so, are they stored locally or in the cloud?**<br>A: No. |

| | |
|---|---|
| **Q: Utilisez-vous des connexions de secours (4G/5G, satellite) en cas de panne du réseau principal ?**<br>A: Le réseau principal est doublé en suffisance pour ne pas lâcher. En cas de panne du réseau de distribution, seule la solution satellite fonctionne. | **Q: Do you use backup connections (4G/5G, satellite) in case of main network failure?**<br>A: The main network is sufficiently duplicated to avoid failure. In case of distribution network failure, only the satellite solution works. |
| **Q: Auriez-vous une idée du temps nécessaire pour déployer l'infrastructure réseau lors d'un tel événement (installation des câbles, équipements, etc.) ?**<br>A: Difficile à dire mais plus d'une semaine. | **Q: Do you have an idea of how long it takes to deploy the network infrastructure for such an event (installing cables, equipment, etc.)?**<br>A: Hard to say, but more than a week. |
| **Q: En 2007, lors de l'incendie : comment les communications réseau ont-elles été utilisées pour gérer cet incident ?**<br>A: 2007 est une année pendant laquelle les réseaux étaient absents. | **Q: In 2007, during the fire: how was network communication used to manage the incident?**<br>A: 2007 was a year when networks were absent. |
| **Q: Pensez-vous qu'une solution basée sur un réseau Wi-Fi Mesh aurait du sens dans un environnement comme un festival ?**<br>A: Pas la moindre idée. | **Q: Do you think a Wi-Fi Mesh solution would make sense in a festival environment?**<br>A: No idea at all. |
| **Q: Quels sont selon vous les besoins principaux en matière de connectivité pour assurer la sécurité physique d'un festival ? (Fiabilité, vitesse, sécurité, portée, mobilité. . . )**<br>A: C'est, je crois, une question également trop technique pour moi. Cependant, la fiabilité reste la qualité indispensable. | **Q: In your opinion, what are the main connectivity requirements to ensure physical security at a festival? (Reliability, speed, security, coverage, mobility. . . )**<br>A: I believe this is also a too technical question for me. However, reliability remains the key quality. |
| **Q: Avez-vous rencontré des limites ou des frustrations avec le réseau existant ?**<br>A: Non. | **Q: Have you encountered any limitations or frustrations with the existing network?**<br>A: No. |
| **Q: Quelles informations provenant de l'équipe IT ou réseau aimeriez-vous recevoir pour assurer au mieux la sécurité sur le terrain ?**<br>A: La date à laquelle le réseau est utilisable et son niveau de fiabilité. | **Q: What information from the IT or network team would you like to receive to ensure optimal security coordination?**<br>A: The date when the network becomes usable and its reliability level. |
| **Q: Par exemple : seriez-vous intéressé par des alertes en cas d'instabilité du réseau ou de coupure de connexion ?** | **Q: For example: would you be interested in alerts in case of network instability or connection loss?** |

| | |
|---|---|
| A: J'aimerais qu'il n'y ait pas de coupures du réseau que nous utilisons et je suis informé par l'équipe IT des pannes ou des problèmes. | A: I would prefer there are no network outages, and I am informed by the IT team in case of failures or issues. |
| **Q: Dans l'idéal, que devrait permettre un réseau Wi-Fi sécurisé et fiable pour faciliter votre travail de coordination ?** | **Q: Ideally, what should a secure and reliable Wi-Fi network enable to facilitate your coordination work?** |
| A: La circulation d'informations est limitée au bureau de coordination et de sécurité. Tous les autres contacts passent par radio ou oralement. | A: Information flow is limited to the coordination and security office. All other contacts go through radio or oral communication. |