Fiche Technique : Projet de Hotspot Raspberry Pi 5

# 1. Aperçu

Cette fiche technique décrit les étapes et les composants impliqués dans la création d'un hotspot WiFi et Bluetooth entièrement fonctionnel et sécurisé à l'aide d'un Raspberry Pi 5. Le projet comprend le filtrage réseau, la gestion des adresses IP/MAC, la configuration d'un pare-feu, et des options pour intégrer une surveillance basée sur l'IA pour améliorer la sécurité.

# 2. Exigences Matérielles

Le projet nécessite les composants matériels suivants :

- Raspberry Pi 5 (ou Raspberry Pi 4 pour des configurations alternatives)  
- Adaptateur WiFi USB (si vous n'utilisez pas le WiFi intégré)  
- Dongle Bluetooth (si nécessaire)  
- Accélérateur IA Hailo-8L (en option pour des fonctionnalités avancées d'IA)  
- Carte MicroSD (32 Go ou plus)  
- Câble Ethernet (pour les connexions filaires)  
- Alimentation pour Raspberry Pi 5

# 3. Logiciels et Paquets

Les logiciels et paquets suivants sont nécessaires pour configurer le hotspot, la surveillance réseau et le filtrage :

- Raspberry Pi OS (version Lite ou Desktop)  
- hostapd (pour créer le point d'accès WiFi)  
- dnsmasq (pour les services DHCP)  
- iptables (pour le pare-feu et le filtrage IP/MAC)  
- bluez (pour la gestion du Bluetooth)  
- fail2ban (pour surveiller et bannir les IPs)  
- arpwatch (pour surveiller les adresses MAC)  
- nmap (pour scanner les appareils réseau)  
- En option : pilotes et SDK Hailo-8L (pour l'accélération IA)

# 4. Configuration et Paramétrage

## 4.1 Mise à Jour du Système et Installation des Pilotes

Mettez à jour le système et installez les pilotes nécessaires pour gérer les interfaces réseau (USB, WiFi, et Bluetooth).

Commandes :  
```bash  
sudo apt update && sudo apt upgrade -y  
sudo apt install usb-modeswitch ethtool hostapd dnsmasq iptables python3 bluetooth bluez -y  
```

## 4.2 Création d'un Point d'Accès WiFi et Bluetooth Sécurisé

Configurez le Raspberry Pi comme un hotspot WiFi et Bluetooth sécurisé. La configuration implique la mise en place de hostapd pour l'accès WiFi et de bluez pour le Bluetooth. Cette section couvre les fichiers de configuration clés et la gestion des services.

## 4.3 Filtrage Réseau et Gestion des Adresses IP/MAC

Cette section explique comment filtrer le trafic à l'aide d'iptables et gérer les adresses IP et MAC pour des raisons de sécurité. Le blocage des appareils suspects ou non autorisés peut être effectué via le filtrage IP et MAC.

## 4.4 Configuration du Pare-feu (iptables)

iptables est configuré comme le pare-feu principal pour contrôler le trafic entrant et sortant. Les règles du pare-feu devraient être configurées pour bloquer tout accès non autorisé tout en autorisant les services clés comme SSH et HTTP.

Commandes :  
```bash  
sudo iptables -F  
sudo iptables -P INPUT DROP  
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT # SSH  
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP  
```

# 5. Surveillance et Améliorations de la Sécurité

## 5.1 Fail2Ban et arpwatch

Fail2Ban surveille les journaux d'authentification et bannit les adresses IP présentant une activité suspecte. arpwatch est utilisé pour surveiller les adresses MAC afin de détecter les appareils qui se connectent au réseau. Ensemble, ces outils améliorent la sécurité en détectant et en réagissant aux menaces en temps réel.

## 5.2 Surveillance Réseau Basée sur l'IA (avec Hailo-8L)

Avec l'accélérateur IA Hailo-8L, une surveillance et un filtrage du réseau basés sur l'IA avancée peuvent être implémentés. Cela permet de détecter les anomalies, d'analyser les menaces de manière prédictive et d'effectuer une inspection approfondie des paquets (DPI) pour améliorer la sécurité.

# 6. Améliorations Optionnelles

- \*\*Intégration de l'IA Hailo-8L\*\* : Ajoutez des fonctionnalités avancées d'IA pour l'analyse prédictive du réseau et la détection des menaces.  
- \*\*Intégration d'un VPN\*\* : Sécurisez davantage le trafic du hotspot avec une solution VPN comme WireGuard ou OpenVPN.  
- \*\*Segmentation réseau\*\* : Créez des zones réseau isolées pour différents types d'appareils (IoT, invités, etc.).

# 7. Conclusion

Ce projet de Hotspot Raspberry Pi 5 fournit une solution complète pour la mise en place d'un point d'accès réseau sécurisé, gérable et extensible. Que ce soit pour un usage personnel, professionnel ou IoT, le système garantit la sécurité avec des fonctionnalités avancées de filtrage, de surveillance et des capacités basées sur l'IA pour offrir un environnement réseau hautement sécurisé.