Projet de Création d’un Hotspot DMZ Sécurisé avec Vérification Temporelle Optimale et Monitoring

# 1. Introduction

L'objectif de ce projet est de configurer un Raspberry Pi 5 comme point d'accès sécurisé dans une zone démilitarisée (DMZ) pour contrôler les connexions réseau via Ethernet, WiFi, Bluetooth et 5G. Le Raspberry Pi sera connecté à un routeur GSM, supportant la 5G pour la domotique, et inclura Fast USB et Fast Ethernet pour des performances optimales. Des logiciels de monitoring assureront la vérification des tentatives d'accès, et un compte administrateur sera créé pour permettre aux techniciens d'accéder en toute sécurité au système.

# 2. Matériel requis

• Raspberry Pi 5 avec Raspberry Pi OS  
• Routeur GSM 5G (ex. Teltonika RUT956)  
• Clé USB GSM ou modem intégré avec support 5G  
• Câble Fast Ethernet  
• Carte SD pour Raspberry Pi  
• Modules WiFi et Bluetooth  
• Système de domotique compatible 5G (optionnel)

# 3. Configuration du Raspberry Pi 5

## a) Mise à jour et installation des pilotes

1. Téléchargez Raspberry Pi OS et flashez la carte SD avec un utilitaire comme Balena Etcher.  
2. Démarrez le Raspberry Pi, connectez-vous au terminal, et mettez à jour le système avec la commande :

sudo apt update && sudo apt upgrade

3. Installer les pilotes nécessaires pour les périphériques USB et Ethernet :

sudo apt install usb-modeswitch ethtool

## b) Configuration réseau (Ethernet, WiFi, GSM 5G)

1. Vérifiez que la clé USB GSM 5G est détectée avec :

lsusb

2. Configurez l’Ethernet pour Fast Ethernet avec ethtool :

sudo ethtool -s eth0 speed 1000 duplex full

3. Configurez la connexion 5G pour le routeur Teltonika via l’interface WAN ou PPP.  
Accédez à l'interface du routeur et configurez le WAN en sélectionnant la connectivité 5G.

# 4. Configuration du Raspberry Pi en Point d'accès sécurisé

1. Installez hostapd et dnsmasq pour le hotspot WiFi sécurisé :

sudo apt install hostapd dnsmasq

2. Configurez le fichier de configuration hostapd :

interface=wlan0  
driver=nl80211  
ssid=DMZ\_Secure\_Hotspot  
hw\_mode=g  
channel=6  
wpa=2  
wpa\_passphrase=StrongPassword123

3. Configurez dnsmasq pour la gestion DHCP du WiFi :

interface=wlan0  
dhcp-range=192.168.50.10,192.168.50.100,255.255.255.0,24h

# 5. Création d’un Compte Administrateur Sécurisé

1. Créez un compte administrateur sécurisé pour permettre aux techniciens d'accéder à la DMZ en connexion hardware :

sudo adduser admin\_tech  
sudo usermod -aG sudo admin\_tech

2. Assurez-vous que le compte admin n’est accessible que via SSH sécurisé ou via connexion physique avec mot de passe fort.

# 6. Mise en place du Pare-feu avec iptables

1. Configurez des règles iptables pour filtrer les connexions en DMZ :

sudo iptables -F  
sudo iptables -P INPUT DROP  
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

2. Enregistrez les règles pour les rendre persistantes :

sudo sh -c 'iptables-save > /etc/iptables/rules.v4'

# 7. Monitoring des Connexions et Vérification Temporelle

1. Installez arpwatch pour surveiller les connexions et repérer les tentatives d'accès :

sudo apt install arpwatch

2. Configurez arpwatch pour surveiller les adresses MAC suspectes et générer des alertes. Pour bannir une MAC suspecte :

sudo iptables -A INPUT -m mac --mac-source XX:XX:XX:XX:XX:XX -j DROP

# 8. Surveillance Avancée avec Fail2Ban

1. Installez Fail2Ban pour bannir automatiquement les IP suspectes :

sudo apt install fail2ban

2. Configurez Fail2Ban dans /etc/fail2ban/jail.local pour surveiller les services critiques comme SSH et HTTP :

[sshd]  
enabled = true  
port = 22  
filter = sshd  
logpath = /var/log/auth.log  
maxretry = 3  
bantime = 600  
  
[http-auth]  
enabled = true  
port = 80  
logpath = /var/log/apache2/access.log  
maxretry = 3  
bantime = 600

# 9. Conclusion

En suivant ces étapes, un environnement sécurisé pour un réseau d'entreprise est établi avec un Raspberry Pi en tant que contrôleur de DMZ. La vérification temporelle des accès, la gestion des tentatives d'intrusion, ainsi que la protection offerte par Fail2Ban et arpwatch garantissent une surveillance continue et active. Le routeur Teltonika et la connectivité 5G offrent une flexibilité et une performance accrue pour des applications comme la domotique.