Configuration Raspberry Pi 5 - DMZ avec Routeur Teltonika RUT956 et Serveur Android

# 1. Introduction

L’objectif est de configurer un Raspberry Pi 5 comme un point d’accès sécurisé dans une zone démilitarisée (DMZ) pour filtrer le trafic réseau entre un routeur GSM (Teltonika RUT956) et un réseau d’entreprise. Ce système doit jouer le rôle de pare-feu avancé, créer un hotspot WiFi sécurisé, surveiller et filtrer les connexions Ethernet, WiFi, Bluetooth et GSM, et intégrer un honeypot pour détecter les tentatives de connexion malveillantes. Le serveur Android doit être surveillé et protégé, avec des outils de bannissement automatique des IP/MAC via Fail2Ban et arpwatch.

# 2. Matériel requis

• Raspberry Pi 5 avec Raspberry Pi OS  
• Routeur GSM Teltonika RUT956  
• Clé USB GSM ou modem intégré  
• Carte SD avec Raspberry Pi OS  
• Câble Ethernet pour la connexion avec le routeur  
• Modules Bluetooth et WiFi (si non intégrés au Raspberry Pi)

# 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 Balena Etcher.  
2. Démarrez le Raspberry Pi, connectez-vous et mettez à jour le système :

sudo apt update && sudo apt upgrade

3. Installer les pilotes USB/GSM :

sudo apt install usb-modeswitch

## b) Configuration réseau (Ethernet et WiFi)

1. Vérifiez la reconnaissance de la clé USB GSM :

lsusb

2. Configurez l’Ethernet avec ifconfig :

sudo ifconfig eth0 up

# 4. Configuration du routeur Teltonika RUT956

1. Accédez à l’interface du routeur via 192.168.1.1.  
2. Configurez le WAN dans Network > WAN (Ethernet, cellulaire).  
3. Redirigez le trafic vers le Raspberry Pi en DMZ dans Network > Firewall > Port forwarding.  
4. Limitez les ports autorisés vers le Raspberry Pi (HTTP, HTTPS, SSH).

# 5. Configuration du Raspberry Pi en point d'accès

1. Installez hostapd et dnsmasq :

sudo apt install hostapd dnsmasq

2. Créez la configuration hostapd pour le point d’accès :

interface=wlan0  
driver=nl80211  
ssid=RaspberryPi\_Hotspot  
hw\_mode=g  
channel=7  
wpa=2  
wpa\_passphrase=SuperSecurePassword

3. Configurez dnsmasq pour le DHCP WiFi :

interface=wlan0  
dhcp-range=192.168.4.2,192.168.4.20,255.255.255.0,24h

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

1. Ajoutez des règles pour sécuriser les ports ouverts :

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 80 -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

2. Sauvegardez les règles iptables :

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

# 7. Mise en place d’un honeypot avec Cowrie

1. Installez Cowrie pour surveiller les accès non autorisés :

sudo apt install git python3-venv  
git clone https://github.com/cowrie/cowrie  
cd cowrie  
python3 -m venv cowrie-env  
source cowrie-env/bin/activate  
pip install -r requirements.txt  
cp etc/cowrie.cfg.dist etc/cowrie.cfg  
./start.sh

# 8. Surveillance des connexions et bannissement

## a) Fail2Ban pour bannir les IPs suspectes

1. Installez Fail2Ban pour protéger le serveur Android :

sudo apt install fail2ban

2. Configurez Fail2Ban dans /etc/fail2ban/jail.local :

[android-server]  
enabled = true  
port = 8080  
filter = android-server  
logpath = /var/log/syslog  
maxretry = 3  
bantime = 3600

## b) Surveillance des MACs avec arpwatch

1. Installez arpwatch pour détecter les MACs :

sudo apt install arpwatch

2. Configurez arpwatch pour bannir les MACs suspectes avec iptables. Exemple :

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

# 9. Conclusion

Cette configuration permet de protéger un réseau d’entreprise avec un Raspberry Pi jouant un rôle de DMZ sécurisé. Le routeur Teltonika RUT956 gère la connectivité, tandis que Fail2Ban et arpwatch assurent la surveillance et le bannissement des IP et MAC malveillantes. Le honeypot Cowrie capture les tentatives de connexion non autorisées pour analyse.