Cahier des Charges : Proxy TCP pour TPE Multi-Sites

1. Contexte et Objectifs

1.1 Contexte

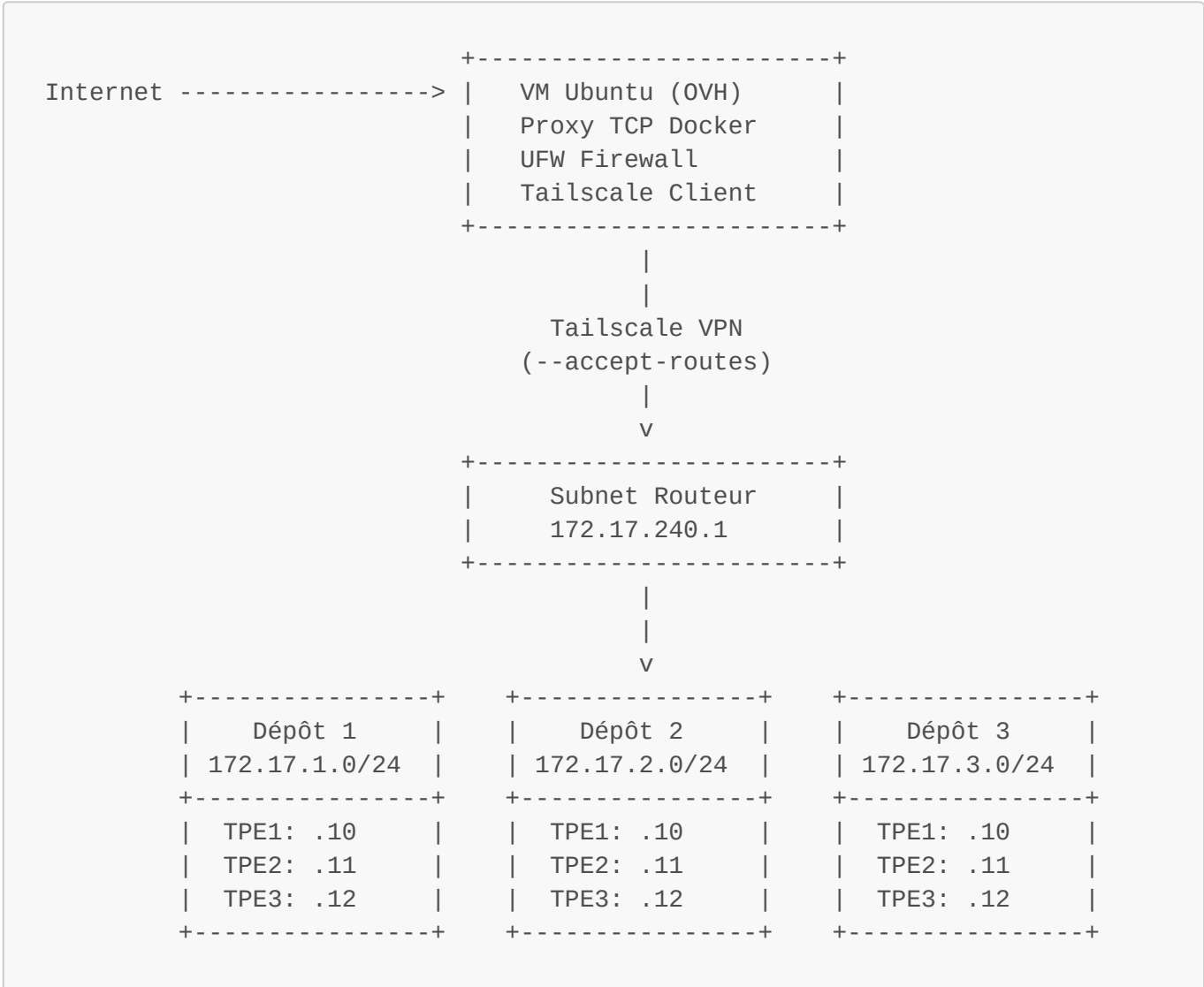
Mise en place d'une solution de redirection de ports TCP pour permettre l'accès à des TPE situés dans différents dépôts, chacun ayant son propre réseau local.

1.2 Objectifs

- Permettre l'accès distant aux TPE via une VM centralisée
- Sécuriser les accès par filtrage IP
- Faciliter la maintenance et la surveillance

2. Architecture Technique

2.1 Vue d'ensemble



2.2 Infrastructure

VM Centrale (OVH)

- Ubuntu 22.04 LTS
- Docker + Docker Compose
- UFW (Pare-feu)
- Ports exposés : 10001-17299
- Tailscale Client avec --accept-routes
- Connexion au subnet routeur 172.17.240.1

Configuration Tailscale

```
# Installation de Tailscale
curl -fsSL https://tailscale.com/install.sh | sh

# Connexion avec l'option accept-routes
tailscale up --accept-routes

# Vérification de la connexion et des routes
tailscale status
ip route
```

Réseaux des Dépôts

- Dépôt 1 : 172.17.1.0/24
- Dépôt 2 : 172.17.2.0/24
- Dépôt 3 : 172.17.3.0/24
- etc.

3. Configuration Détaillée

3.1 Configuration Docker Compose

```
version: '3.8'

services:
  # Dépôt 01
  depot01-tpe01:
    image: ralphi2811/tcp-proxy:latest
    command: 172.17.1.10 8888
    ports:
      - "10101:8888"
    restart: always

  depot01-tpe02:
    image: ralphi2811/tcp-proxy:latest
    command: 172.17.1.11 8888
    ports:
      - "10102:8888"
```

```
    restart: always

  # Dépôt 22
  depot22-tpe01:
    image: ralphi2811/tcp-proxy:latest
    command: 172.17.22.10 8888
    ports:
      - "12201:8888"
    restart: always

  depot22-tpe02:
    image: ralphi2811/tcp-proxy:latest
    command: 172.17.22.11 8888
    ports:
      - "12202:8888"
    restart: always

  # Ajouter d'autres TPE selon le même modèle
```

3.2 Convention de Nommage des Ports

Format : 1XXYY

- 1 : préfixe fixe
- XX : numéro du dépôt sur 2 chiffres (01-72)
- YY : numéro du TPE dans le dépôt sur 2 chiffres (01-99)

Exemple :

- 10101 : Dépôt 01, TPE 01
- 10102 : Dépôt 01, TPE 02
- 12201 : Dépôt 22, TPE 01

4. Sécurité

4.1 Configuration UFW

```
# Configuration de base
ufw default deny incoming
ufw default allow outgoing

# SSH (à adapter avec votre IP)
ufw allow from VOTRE_IP_ADMIN to any port 22

# TPE Dépôt 01
ufw allow from IP_AUTORISEE to any port 10101
ufw allow from IP_AUTORISEE to any port 10102

# TPE Dépôt 22
ufw allow from IP_AUTORISEE to any port 12201
ufw allow from IP_AUTORISEE to any port 12202
```

```
# Activation
ufw enable
```

4.2 Matrice de Flux

```
Source        Destination   Port     Protocol  Description
-----------   ------------ --------- --------  -----------
IP_ADMIN      VM           22        TCP      SSH Admin
IP_AUTORISEE  VM           1XXYY     TCP      Accès TPE (XX=dépôt, YY=TPE)
```

5. Surveillance et Maintenance

5.1 Logs à Surveiller

- Logs Docker : `/var/log/docker/`
- Logs UFW : `/var/log/ufw.log`
- Logs Système : `journalctl`

5.2 Commandes de Surveillance

```
# État des conteneurs
docker ps

# Logs d'un TPE spécifique
docker logs depot1-tpe1

# Connexions actives
netstat -tunlp

# Règles UFW
ufw status numbered

# État Tailscale
tailscale status
tailscale netcheck

# Routes
ip route show
ip route show table 52  # Table de routage Tailscale
```

6. Plan de Déploiement

1. Installation VM
    - Déploiement Ubuntu 22.04 LTS
    - Mise à jour système

- Installation Docker et Docker Compose
- Installation Tailscale
- Configuration Tailscale avec --accept-routes

2. Configuration Réseau

- Configuration UFW
- Vérification des routes Tailscale vers le subnet 172.17.240.1
- Test connectivité vers les dépôts via Tailscale

3. Déploiement Services

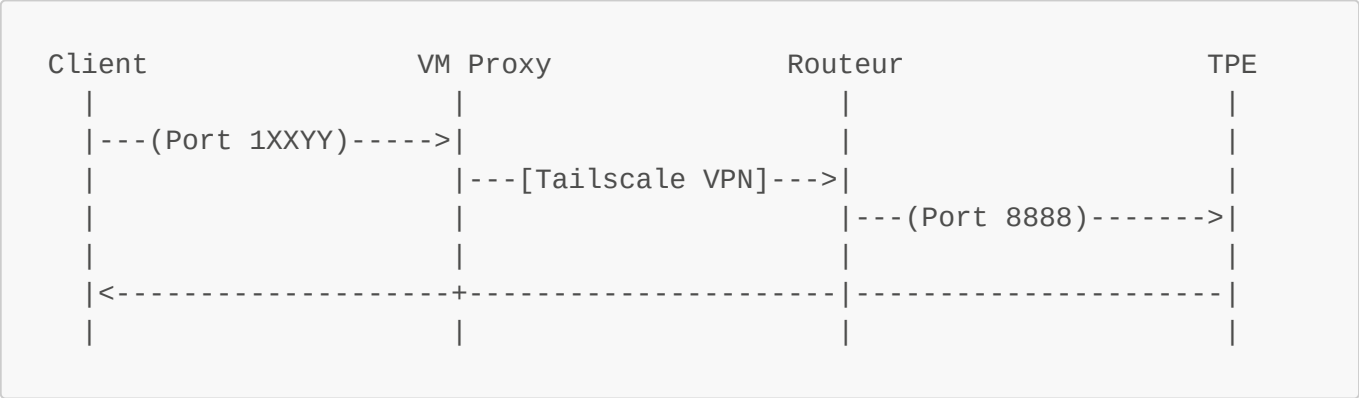
- Déploiement docker-compose.yml
- Test de chaque redirection

4. Validation

- Tests d'accès depuis les IP autorisées
- Vérification des logs
- Tests de charge (optionnel)

7. Documentation

7.1 Schéma de Flux Détaillé



Note: Le trafic entre la VM et les TPE passe par le tunnel Tailscale et est routé via le subnet 172.17.240.1

7.2 Tableau des TPE

Dépôt	Réseau	TPE	IP	Port Public
01	172.17.1.0/24	TPE01	.10	10101
01	172.17.1.0/24	TPE02	.11	10102
22	172.17.22.0/24	TPE01	.10	12201
22	172.17.22.0/24	TPE02	.11	12202

8. Support et Contact

- Support Technique : Raphaël Auberlet

- Contact Urgence : Raphaël Auberlet
- Documentation : https://github.com/ralphi2811/tcp-proxy-docker