Redsocks en Action

Bien sûr ! Je vais vous guider pour configurer un proxy Shadowsocks sur votre ordinateur Mac et configurer votre routeur OpenWRT afin de router tout le trafic des appareils connectés via ce proxy. Cette configuration comprend les étapes principales suivantes :

1. Configuration du client Shadowsocks sur macOS (en utilisant Shadowsocks-NG ou Clash)
2. Configuration de macOS pour autoriser les connexions proxy externes
3. Attribution d'une adresse IP statique à votre Mac
4. Installation et configuration de Redsocks sur OpenWRT
5. Redirection du trafic d'OpenWRT via le proxy macOS
6. Test de la configuration du proxy

Plongeons dans chaque étape en détail.

---

1. Configuration du client Shadowsocks sur macOS

Vous pouvez utiliser soit Shadowsocks-NG, soit Clash comme client Shadowsocks. Voici les instructions pour les deux.

Option A : Utilisation de Shadowsocks-NG

Shadowsocks-NG est un client Shadowsocks populaire et convivial pour macOS.

Étape 1 : Télécharger et installer Shadowsocks-NG

1. Téléchargez Shadowsocks-NG :
    - Rendez-vous sur la page des versions de Shadowsocks-NG sur GitHub.
    - Téléchargez le dernier fichier `.dmg`.
2. Installez l'application :
    - Ouvrez le fichier `.dmg` téléchargé.
    - Faites glisser l'application ShadowsocksX-NG dans votre dossier Applications.
3. Lancez Shadowsocks-NG :

- Ouvrez ShadowsocksX-NG depuis votre dossier Applications.
- Vous pourriez avoir besoin d'accorder à l'application les permissions nécessaires dans les Préférences Système.

Étape 2 : Configurer Shadowsocks-NG

1. Ouvrir les Préférences :
   - Cliquez sur l'icône de ShadowsocksX-NG dans la barre de menus.
   - Sélectionnez "Ouvrir ShadowsocksX-NG" > "Préférences".
2. Ajouter un nouveau serveur :
   - Accédez à l'onglet "Servers".
   - Cliquez sur le bouton "+" pour ajouter un nouveau serveur.
3. Importer l'URL de Shadowsocks :
   - Copiez votre URL Shadowsocks :

     `ss://[ENCRYPTED_PASSWORD]@xxx.xxx.xxx.xxx:xxxxx/?outline=1`

   - Méthode d'importation :
     - Cliquez sur "Importer".
     - Collez votre URL Shadowsocks.
     - Shadowsocks-NG devrait automatiquement analyser et remplir les détails du serveur.
4. Configurez le proxy local :
   - Assurez-vous que l'option "Activer le proxy SOCKS5" est cochée.
   - Notez le port local (par défaut, il est généralement `1080`).
5. Enregistrer et Activer :
   - Cliquez sur "OK" pour enregistrer le serveur.
   - Basculez l'interrupteur "Activer Shadowsocks" sur ON.

Option B : Utilisation de Clash

Clash est un client proxy polyvalent qui prend en charge plusieurs protocoles, notamment Shadowsocks.

Étape 1 : Télécharger et installer Clash

1. Téléchargez Clash pour macOS :
   - Rendez-vous sur la page des versions de Clash sur GitHub.
   - Téléchargez la dernière version binaire de Clash pour macOS.
2. Installer l'Application :
   - Déplacez l'application Clash téléchargée vers votre dossier Applications.
3. Lancez Clash :
   - Ouvrez Clash depuis votre dossier Applications.
   - Vous pourriez avoir besoin d'accorder les permissions nécessaires dans les Préférences Système.

Étape 2 : Configurer Clash

1. Accéder au fichier de configuration :
   - Clash utilise un fichier de configuration au format YAML. Vous pouvez le créer ou le modifier à l'aide d'un éditeur de texte comme TextEdit ou Visual Studio Code.
2. Ajoutez votre serveur Shadowsocks :
   - Créez un fichier de configuration (par exemple, `config.yaml`) avec le contenu suivant :

```yaml
port: 7890
socks-port: 7891
allow-lan: true
mode: Rule
log-level: info

    proxies:
      - name: "MyShadowsocks"
        type: ss
        server: xxx.xxx.xxx.xxx
        port: xxxxx
        cipher: chacha20-ietf-poly1305
        password: "xxxxxx"
```

```
    proxy-groups:
      - name: "Default"
        type: select
        proxies:
          - "MyShadowsocks"
          - "DIRECT"

règles :
  - MATCH,Default
```

Notes :
- `port` et `socks-port` définissent les ports HTTP et SOCKS5 sur lesquels Clash écoutera pour le proxy
- `allow-lan: true` permet aux appareils du réseau local d'utiliser le proxy.
- La section `proxies` inclut les détails de votre serveur Shadowsocks.
- `proxy-groups` et `rules` déterminent comment le trafic est acheminé.

3. Démarrer Clash avec la Configuration :
   - Lancez Clash et assurez-vous qu'il utilise votre fichier `config.yaml`.
   - Vous pourriez avoir besoin de spécifier le chemin de configuration lors du démarrage de Clash.
4. Vérifiez que le proxy fonctionne :
   - Assurez-vous que Clash est actif et connecté à votre serveur Shadowsocks.
   - Vérifiez l'icône dans la barre de menus pour connaître l'état.

---

2. Configuration de macOS pour Autoriser les Connexions Proxy Externes

Par défaut, les clients Shadowsocks lient le proxy à `localhost` (`127.0.0.1`), ce qui signifie que seul le Mac peut utiliser le proxy. Pour permettre à votre routeur OpenWRT d'utiliser ce proxy, vous devez lier le proxy à l'adresse IP LAN du Mac.

Pour Shadowsocks-NG :

1. Ouvrez les Préférences :
    - Cliquez sur l'icône de ShadowsocksX-NG dans la barre de menu.
    - Sélectionnez "Ouvrir ShadowsocksX-NG" > "Préférences".
2. Accédez à l'onglet Avancé :
    - Rendez-vous dans l'onglet "Avancé".
3. Définir l'adresse d'écoute :
    - Modifiez l'"Adresse d'écoute" de `127.0.0.1` à `0.0.0.0` pour autoriser les connexions depuis n'importe quelle interface.
    - Alternativement, spécifiez l'adresse IP LAN du Mac (par exemple, `192.168.1.xxx`).
4. Enregistrez et redémarrez Shadowsocks-NG :
    - Cliquez sur "OK" pour enregistrer les modifications.
    - Redémarrez le client Shadowsocks-NG pour appliquer les nouveaux paramètres.

Pour Clash :

1. Modifier le fichier de configuration :
    - Assurez-vous que le paramètre `allow-lan: true` est activé dans votre fichier `config.yaml`.
2. Se lier à toutes les interfaces :
    - Dans la configuration, définir `allow-lan: true` lie généralement le proxy à toutes les interfaces disponibles, y compris le LAN.
3. Redémarrer Clash :
    - Redémarrez le client Clash pour appliquer les modifications.

---

3. Attribuer une adresse IP statique à votre Mac

Pour garantir une connectivité constante entre votre routeur OpenWRT et le Mac, attribuez une adresse IP statique à votre Mac au sein de votre réseau local.

Étapes pour attribuer une adresse IP statique sur macOS :

1. Ouvrez les Préférences Système :
    - Cliquez sur le menu Apple et sélectionnez “Préférences Système”.
2. Accédez aux paramètres réseau :
    - Cliquez sur “Réseau”.
3. Sélectionnez votre connexion active :
    - Choisissez “Wi-Fi” ou “Ethernet” dans la barre latérale gauche, selon la manière dont votre Mac est connecté au routeur.
4. Configurer les paramètres IPv4 :
    - Cliquez sur “Avancé...”.
    - Allez dans l’onglet “TCP/IP”.
    - Changez “Configurer IPv4” de “Utiliser DHCP” à “Manuellement”.
5. Configurer une adresse IP statique :
    - Adresse IP : Choisissez une IP en dehors de la plage DHCP de votre routeur pour éviter les conflits (par exemple, `192.168.1.xxx`).
    - Masque de sous-réseau : Généralement `255.255.255.0`.
    - Routeur : L’adresse IP de votre routeur (par exemple, `192.168.1.1`).
    - Serveur DNS : Vous pouvez utiliser l’IP de votre routeur ou un autre service DNS comme `8.8.8.8`.
6. Appliquer les paramètres :
    - Cliquez sur “OK”, puis sur “Appliquer” pour enregistrer les modifications.

---

4. Installation et Configuration de Redsocks sur OpenWRT

Redsocks est un redirecteur de sockets transparent qui vous permet de router le trafic réseau via un proxy SOCKS5. Nous allons utiliser Redsocks pour rediriger le trafic d’OpenWRT à travers le proxy Shadowsocks fonctionnant sur votre Mac.

Étape 1 : Installer Redsocks

1. Mettre à jour les listes de paquets :

```
ssh root@<router_ip>
opkg update
```

2. Installez Redsocks :

   ```
   opkg install redsocks
   ```

   Si Redsocks n'est pas disponible dans votre dépôt OpenWRT, vous devrez peut-être le compiler manuellement ou utiliser un paquet alternatif.

Étape 2 : Configurer Redsocks

1. Créez ou modifiez le fichier de configuration de Redsocks :

   ```
   vi /etc/redsocks.conf
   ```

2. Ajoutez la configuration suivante :

   ```
   base {
       log_debug = on;
       log_info = on;
       log = "file:/var/log/redsocks.log";
       daemon = on;
       redirector = iptables;
   }
   ```

```
redsocks {        local_ip = 0.0.0.0;        local_port = 12345;  # Port local sur lequel
Redsocks doit écouter        ip = xxx.xxx.xxx.xxx;  # IP statique du Mac        port =
xxxxx;          # Port local du proxy SOCKS5 de Shadowsocks-NG        type = socks5;
login = "";           # Si votre proxy nécessite une authentification        password =
"";    }
```

Notes : - `local_port` : Le port sur lequel Redsocks écoute pour les connexions entrantes redirigées par iptables. - `ip` et `port` : Pointent vers le proxy SOCKS5 Shadowsocks de votre Mac (`xxx.xxx.xxx.xxx:xxxxx` basé sur les étapes précédentes). - `type` : Définissez-le sur `socks5` car Shadowsocks fournit un proxy SOCKS5.

3. Enregistrer et quitter :
    - Appuyez sur `ESC`, tapez `:wq`, puis appuyez sur `Entrée`.
4. Créer un fichier de journal :

```
touch /var/log/redsocks.log
chmod 644 /var/log/redsocks.log
```

Étape 3 : Démarrer le service Redsocks

1. Activer Redsocks pour qu'il démarre au démarrage :

```
/etc/init.d/redsocks enable
```

2. Démarrez Redsocks :

```
/etc/init.d/redsocks start
```

3. Vérifiez que Redsocks est en cours d'exécution :

```
ps | grep redsocks
```

Vous devriez voir un processus Redsocks en cours d'exécution.

---

5. Rediriger le trafic d'OpenWRT via le proxy macOS

Maintenant que Redsocks est configuré sur OpenWRT, configurez iptables pour rediriger tout le trafic TCP sortant via Redsocks, qui à son tour le route via le proxy Shadowsocks de votre Mac.

Étape 1 : Configurer les règles iptables

1. Ajouter des règles iptables pour rediriger le trafic :

```
# Rediriger tout le trafic TCP vers Redsocks (sauf le trafic vers le proxy lui-même)
iptables -t nat -N REDSOCKS
iptables -t nat -A REDSOCKS -d xxx.xxx.xxx.xxx -p tcp --dport xxxxx -j RETURN
iptables -t nat -A REDSOCKS -p tcp -j REDIRECT --to-ports 12345
```

Appliquer la chaîne REDSOCKS à tout le trafic sortant iptables -t nat -A OUTPUT -p tcp -j REDSOCKS iptables -t nat -A PREROUTING -p tcp -j REDSOCKS “‘

Explication : - Créer une nouvelle chaîne : `REDSOCKS` - Exclure le trafic du proxy : S’assurer que le trafic destiné au proxy lui-même n’est pas redirigé. - Rediriger les autres trafics TCP : Transférer les autres trafics TCP vers le port d’écoute de Redsocks (`12345`).

2. Sauvegarder les règles iptables :

Pour rendre ces règles persistantes après un redémarrage, ajoutez-les à la configuration du pare-feu.

```
vi /etc/firewall.user
```

Ajoutez les règles iptables :

```
# Rediriger tout le trafic TCP vers Redsocks (sauf le proxy)
iptables -t nat -N REDSOCKS
iptables -t nat -A REDSOCKS -d xxx.xxx.xxx.xxx -p tcp --dport xxxxx -j RETURN
iptables -t nat -A REDSOCKS -p tcp -j REDIRECT --to-ports 12345
```

Appliquer la chaîne REDSOCKS iptables -t nat -A OUTPUT -p tcp -j REDSOCKS iptables -t nat -A PREROUTING -p tcp -j REDSOCKS “‘

Enregistrer et quitter : - Appuyez sur `ESC`, tapez `:wq`, puis appuyez sur `Entrée`.

3. Redémarrez le pare-feu pour appliquer les modifications :

```
/etc/init.d/firewall restart
```

Étape 2 : Vérifier que le trafic est redirigé

1. Vérifier les journaux de Redsocks :

```
cat /var/log/redsocks.log
```

Vous devriez voir des logs indiquant que le trafic est traité par Redsocks.

2. Test depuis un appareil client :

- Connectez un appareil à votre routeur OpenWRT.
- Visitez un site web ou effectuez une action qui utilise Internet.
- Vérifiez que le trafic est routé via le proxy Shadowsocks en vérifiant l'adresse IP externe (par exemple, via WhatIsMyIP.com) pour voir si elle reflète l'IP du proxy.

---

6. Tester la configuration du proxy

Assurez-vous que l'ensemble de la configuration fonctionne comme prévu en effectuant les tests suivants.

Étape 1 : Vérifier la connexion Shadowsocks sur Mac

1. Vérifier l'état du client Shadowsocks :
   - Assurez-vous que Shadowsocks-NG ou Clash est activement connecté au serveur Shadowsocks.
   - Vérifiez que le proxy local (par exemple, `xxx.xxx.xxx.xxx:xxxxx`) est accessible.
2. Testez le proxy localement :
   - Sur votre Mac, ouvrez un navigateur et configurez-le pour utiliser `localhost:1080` comme proxy SOCKS5.
   - Visitez WhatIsMyIP.com pour vérifier que l'adresse IP correspond à celle du serveur Shadowsocks.

Étape 2 : Vérifier que le trafic d'OpenWRT est acheminé via le proxy

1. Vérifier l'IP externe d'OpenWRT :
   - À partir d'un appareil connecté à OpenWRT, visitez WhatIsMyIP.com pour voir si l'IP reflète celle du serveur Shadowsocks.
2. Surveiller les logs de Redsocks :
   - Sur OpenWRT, surveillez les logs de Redsocks pour vous assurer que le trafic est bien redirigé.

```
tail -f /var/log/redsocks.log
```

3. Dépannage si nécessaire :

- Si le trafic n'est pas correctement acheminé :
  - Assurez-vous que le client Shadowsocks sur Mac est en cours d'exécution et accessible.
  - Vérifiez que les règles iptables sont correctement configurées.
  - Vérifiez les paramètres du pare-feu sur Mac et OpenWRT.

Considérations supplémentaires

1. Sécurité

- Sécurisez votre proxy :
  - Assurez-vous que seuls les appareils de confiance peuvent accéder au proxy. Étant donné que vous redirigez tout le trafic via Redsocks, veillez à ce que le pare-feu de votre Mac n'autorise que les connexions provenant de votre routeur OpenWRT.

Sur macOS :

- Allez dans Préférences Système > Sécurité et Confidentialité > Pare-feu.
- Configurez le pare-feu pour autoriser les connexions entrantes sur le port du proxy (`xxxxx`) uniquement depuis l'IP du routeur OpenWRT.
- Authentification :
  - Shadowsocks offre déjà un certain niveau de sécurité grâce au chiffrement. Assurez-vous d'utiliser des mots de passe robustes et des méthodes de chiffrement solides.

2. Performances

- Ressources du routeur :
  - L'exécution de services de proxy comme Redsocks peut consommer des ressources supplémentaires en CPU et en mémoire sur votre routeur OpenWRT. Assurez-vous que votre routeur dispose de ressources suffisantes.
- Performances du Mac :
  - Assurez-vous que votre Mac reste allumé et connecté au réseau pour maintenir la disponibilité du proxy.

3. Maintenance

- Surveiller les journaux :
  - Vérifiez régulièrement les journaux de Redsocks et Shadowsocks pour détecter toute activité inhabituelle ou erreur.
- Mettre à jour les logiciels :
  - Maintenez OpenWRT, Redsocks et votre client Shadowsocks à jour pour profiter des correctifs de sécurité et des améliorations de performances.

4. Approches Alternatives

Bien qu'il soit possible d'utiliser un Mac comme serveur proxy intermédiaire, voici quelques alternatives à considérer pour des configurations potentiellement plus simples :

- Configurer directement OpenWRT en tant que client Shadowsocks :
  - OpenWRT prend en charge Shadowsocks directement via des paquets comme `shadowsocks-libev`. Cette approche élimine le besoin d'un intermédiaire Mac.
- Utiliser un appareil dédié pour le proxy/VPN :
  - Des appareils comme le Raspberry Pi peuvent exécuter des services de proxy et servir de passerelles dédiées.

Conclusion

En suivant les étapes décrites ci-dessus, vous avez configuré votre Mac en tant que serveur proxy Shadowsocks et configuré votre routeur OpenWRT pour acheminer tout le trafic des appareils connectés via ce proxy. Cette configuration améliore la confidentialité et le contrôle de votre réseau en exploitant le protocole Shadowsocks.

Points Clés à Retenir :

1. Client Shadowsocks sur Mac :
   - Installé et configuré Shadowsocks-NG ou Clash avec l'URL Shadowsocks fournie.
   - Configuré le client pour écouter sur l'adresse IP LAN du Mac.

2. Accessibilité du Proxy :
    - Attribué une IP statique au Mac pour garantir un accès proxy constant.
    - Configuré le pare-feu de macOS pour autoriser les connexions proxy entrantes.
3. Configuration d'OpenWRT :
    - J'ai installé et configuré Redsocks pour rediriger tout le trafic TCP sortant via le proxy Shadowsocks.
    - J'ai appliqué les règles iptables nécessaires pour appliquer la redirection du trafic.
4. Test :
    - Vérifié que le trafic des appareils connectés passe par le proxy Shadowsocks en vérifiant les adresses IP externes.

Recommandations :

- Assurer la stabilité : Gardez votre Mac alimenté et connecté pour maintenir la disponibilité du proxy.
- Sécurité avant tout : Mettez régulièrement à jour tous les composants et surveillez les journaux pour vous protéger contre les accès non autorisés.
- Envisagez une configuration directe du routeur : Pour une configuration plus simplifiée, explorez la configuration de Shadowsocks directement sur votre routeur OpenWRT.

Si vous rencontrez des problèmes ou avez besoin d'une assistance supplémentaire pour des configurations spécifiques, n'hésitez pas à nous contacter !

```
base {
    log_debug = on;
    log_info = on;
    log = "file:/var/log/redsocks.log";
    daemon = on;
    redirector = generic;
}

redsocks {     local_ip = 0.0.0.0;     local_port = 7891;     ip = xxx.xxx.xxx.xxx;
port = xxxxx;     type = http-connect;     login = "";     password = ""; }
```