Redsocks in Aktion

Natürlich! Ich werde Sie durch die Einrichtung eines Shadowsocks-Proxys auf Ihrem Mac-Computer und die Konfiguration Ihres OpenWRT-Routers führen, um den gesamten Datenverkehr aller angeschlossenen Geräte über diesen Proxy zu leiten. Diese Einrichtung umfasst die folgenden Hauptschritte:

1. Einrichten des Shadowsocks-Clients auf macOS (mit Shadowsocks-NG oder Clash)
2. Konfigurieren von macOS, um externe Proxy-Verbindungen zuzulassen
3. Zuweisen einer statischen IP-Adresse zu Ihrem Mac
4. Installieren und Konfigurieren von Redsocks auf OpenWRT
5. Umleiten des OpenWRT-Datenverkehrs über den macOS-Proxy
6. Testen der Proxy-Einrichtung

Lassen Sie uns jeden Schritt im Detail betrachten.

---

1. Einrichten des Shadowsocks-Clients auf macOS

Sie können entweder Shadowsocks-NG oder Clash als Ihren Shadowsocks-Client verwenden. Im Folgenden finden Sie Anleitungen für beide.

Option A: Verwendung von Shadowsocks-NG

Shadowsocks-NG ist ein beliebter und benutzerfreundlicher Shadowsocks-Client für macOS.

Schritt 1: Shadowsocks-NG herunterladen und installieren

1. Laden Sie Shadowsocks-NG herunter:
    - Besuchen Sie die Shadowsocks-NG GitHub Releases-Seite.
    - Laden Sie die neueste `.dmg`-Datei herunter.
2. Installieren Sie die Anwendung:
    - Öffnen Sie die heruntergeladene `.dmg`-Datei.
    - Ziehen Sie die ShadowsocksX-NG-App in Ihren Anwendungsordner.

3. Starte Shadowsocks-NG:
    - Öffne ShadowsocksX-NG aus deinem Anwendungsordner.
    - Möglicherweise musst du der App die notwendigen Berechtigungen in den Systemeinstellungen erteilen.

Schritt 2: Shadowsocks-NG konfigurieren

1. Einstellungen öffnen:
    - Klicken Sie auf das ShadowsocksX-NG-Symbol in der Menüleiste.
    - Wählen Sie “ShadowsocksX-NG öffnen” > “Einstellungen”.
2. Fügen Sie einen neuen Server hinzu:
    - Navigieren Sie zum Tab “Servers”.
    - Klicken Sie auf die Schaltfläche “+”, um einen neuen Server hinzuzufügen.
3. Importieren Sie die Shadowsocks-URL:
    - Kopieren Sie Ihre Shadowsocks-URL:

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

    - Importmethode:
        - Klicken Sie auf “Importieren”.
        - Fügen Sie Ihre Shadowsocks-URL ein.
        - Shadowsocks-NG sollte die Serverdetails automatisch analysieren und ausfüllen.
4. Richten Sie den lokalen Proxy ein:
    - Stellen Sie sicher, dass “SOCKS5-Proxy aktivieren” ausgewählt ist.
    - Notieren Sie sich den lokalen Port (standardmäßig ist dies normalerweise `1080`).
5. Speichern und Aktivieren:
    - Klicken Sie auf “OK”, um den Server zu speichern.
    - Schalten Sie den Schalter “Shadowsocks aktivieren” auf EIN.

Option B: Verwendung von Clash

Clash ist ein vielseitiger Proxy-Client, der mehrere Protokolle unterstützt, darunter auch Shadowsocks.

Schritt 1: Clash herunterladen und installieren

1. Clash für macOS herunterladen:
   - Besuchen Sie die Clash GitHub Releases-Seite.
   - Laden Sie das neueste Clash für macOS-Binary herunter.
2. Installieren Sie die Anwendung:
   - Verschieben Sie die heruntergeladene Clash-Anwendung in Ihren Anwendungsordner.
3. Clash starten:
   - Öffnen Sie Clash aus Ihrem Anwendungsordner.
   - Möglicherweise müssen Sie die erforderlichen Berechtigungen in den Systemeinstellungen erteilen.

Schritt 2: Clash konfigurieren

1. Konfigurationsdatei öffnen:
   - Clash verwendet eine YAML-Konfigurationsdatei. Sie können diese mit einem Texteditor wie TextEdit oder Visual Studio Code erstellen oder bearbeiten.
2. Fügen Sie Ihren Shadowsocks-Server hinzu:
   - Erstellen Sie eine Konfigurationsdatei (z.B. `config.yaml`) mit folgendem Inhalt:

```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"

rules:
   - MATCH,Default
```

Notizen:
 - `port` und `socks-port` definieren die HTTP- und SOCKS5-Proxy-Ports, die Clash überwacht.
 - `allow-lan: true` erlaubt es Geräten im LAN, den Proxy zu nutzen.
 - Der Abschnitt `proxies` enthält die Details Ihres Shadowsocks-Servers.
 - `proxy-groups` und `rules` bestimmen, wie der Datenverkehr geroutet wird.

3. Starte Clash mit der Konfiguration:
    - Starte Clash und stelle sicher, dass es deine `config.yaml`-Datei verwendet.
    - Möglicherweise musst du den Konfigurationspfad beim Starten von Clash angeben.
4. Überprüfen Sie, ob der Proxy läuft:
    - Stellen Sie sicher, dass Clash aktiv ist und mit Ihrem Shadowsocks-Server verbunden ist.
    - Überprüfen Sie das Menüleistensymbol auf den Status.

---

2. Konfiguration von macOS, um externe Proxy-Verbindungen zu ermöglichen

Standardmäßig binden Shadowsocks-Clients den Proxy an `localhost` (`127.0.0.1`), was bedeutet, dass nur der Mac den Proxy nutzen kann. Um Ihrem OpenWRT-Router die Nutzung dieses Proxys zu ermöglichen, müssen Sie den Proxy an die LAN-IP des Macs binden.

Für Shadowsocks-NG:

1. Einstellungen öffnen:
    - Klicken Sie auf das ShadowsocksX-NG-Symbol in der Menüleiste.
    - Wählen Sie “ShadowsocksX-NG öffnen” > “Einstellungen”.
2. Gehen Sie zum Reiter “Erweitert”:
    - Navigieren Sie zum Reiter “Erweitert”.
3. Setzen Sie die Abhör-Adresse:
    - Ändern Sie die “Listen Address” von `127.0.0.1` auf `0.0.0.0`, um Verbindungen von jeder Schnittstelle zuzulassen.
    - Alternativ können Sie die LAN-IP des Macs angeben (z.B. `192.168.1.xxx`).
4. Speichern und Neustarten von Shadowsocks-NG:
    - Klicken Sie auf “OK”, um die Änderungen zu speichern.
    - Starten Sie den Shadowsocks-NG-Client neu, um die neuen Einstellungen zu übernehmen.

Für Clash:

1. Konfigurationsdatei bearbeiten:
    - Stellen Sie sicher, dass die Einstellung `allow-lan: true` in Ihrer `config.yaml` aktiviert ist.
2. An alle Schnittstellen binden:
    - In der Konfiguration bindet die Einstellung `allow-lan: true` den Proxy in der Regel an alle verfügbaren Schnittstellen, einschließlich des LANs.
3. Clash neu starten:
    - Starten Sie den Clash-Client neu, um die Änderungen zu übernehmen.

---

3. Zuweisen einer statischen IP-Adresse zu Ihrem Mac

Um eine konsistente Verbindung zwischen Ihrem OpenWRT-Router und dem Mac sicherzustellen, weisen Sie Ihrem Mac eine statische IP-Adresse in Ihrem lokalen Netzwerk zu.

Schritte zur Zuweisung einer statischen IP auf macOS:

1. Systemeinstellungen öffnen:
    - Klicken Sie auf das Apple-Menü und wählen Sie “Systemeinstellungen”.
2. Navigieren Sie zu den Netzwerkeinstellungen:
    - Klicken Sie auf “Netzwerk”.
3. Wählen Sie Ihre aktive Verbindung:
    - Wählen Sie im linken Seitenmenü “Wi-Fi” oder “Ethernet” aus, je nachdem, wie Ihr Mac mit dem Router verbunden ist.
4. IPv4-Einstellungen konfigurieren:
    - Klicken Sie auf “Erweitert...”.
    - Gehen Sie zum Tab “TCP/IP”.
    - Ändern Sie “IPv4 konfigurieren” von “Mit DHCP” auf “Manuell”.
5. Statische IP-Adresse einrichten:
    - IP-Adresse: Wählen Sie eine IP außerhalb des DHCP-Bereichs Ihres Routers, um Konflikte zu vermeiden (z.B. `192.168.1.xxx`).
    - Subnetzmaske: Typischerweise `255.255.255.0`.
    - Router: Die IP-Adresse Ihres Routers (z.B. `192.168.1.1`).
    - DNS-Server: Sie können die IP Ihres Routers oder einen anderen DNS-Dienst wie `8.8.8.8` verwenden.
6. Einstellungen anwenden:
    - Klicken Sie auf “OK” und dann auf “Übernehmen”, um die Änderungen zu speichern.

---

4. Installation und Konfiguration von Redsocks auf OpenWRT

Redsocks ist ein transparenter SOCKS-Umleiter, der es ermöglicht, Netzwerkverkehr über einen SOCKS5-Proxy zu routen. Wir werden Redsocks verwenden, um den Datenverkehr von OpenWRT über den auf Ihrem Mac laufenden Shadowsocks-Proxy umzuleiten.

Schritt 1: Redsocks installieren

1. Paketlisten aktualisieren:

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

2. Installiere Redsocks:

   ```
   opkg install redsocks
   ```

   Falls Redsocks in Ihrem OpenWRT-Repository nicht verfügbar ist, müssen Sie es möglicherweise manuell kompilieren oder ein alternatives Paket verwenden.

Schritt 2: Redsocks konfigurieren

1. Erstellen oder Bearbeiten der Redsocks-Konfigurationsdatei:

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

2. Fügen Sie die folgende Konfiguration hinzu:

```
 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;  # Lokaler Port, auf dem
Redsocks lauschen soll        ip = xxx.xxx.xxx.xxx;  # Statische IP des Macs        port
= xxxxx;          # Lokaler SOCKS5-Proxy-Port von Shadowsocks-NG        type = socks5;
login = "";           # Falls Ihr Proxy eine Authentifizierung erfordert        password
= "";    }
```

Notizen: - `local_port`: Der Port, den Redsocks für eingehende Verbindungen von iptables-Umleitungen überwacht. - `ip` und `port`: Verweisen auf den Shadowsocks SOCKS5-Proxy Ihres Macs (`xxx.xxx.xxx.xxx:xxxxx` basierend auf den vorherigen Schritten). - `type`: Auf `socks5` setzen, da Shadowsocks einen SOCKS5-Proxy bereitstellt.

3. Speichern und Beenden:
    - Drücken Sie `ESC`, geben Sie `:wq` ein und drücken Sie `Enter`.
4. Protokolldatei erstellen:

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

Schritt 3: Starten Sie den Redsocks-Dienst

1. Redsocks beim Systemstart aktivieren:

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

2. Starte Redsocks:

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

3. Überprüfen, ob Redsocks läuft:

```
ps | grep redsocks
```

Sie sollten einen Redsocks-Prozess laufen sehen.

---

5. Umleitung des OpenWRT-Datenverkehrs über den macOS-Proxy

Nachdem Redsocks auf OpenWRT eingerichtet ist, konfigurieren Sie iptables, um den gesamten ausgehenden TCP-Datenverkehr über Redsocks umzuleiten, der ihn wiederum über den Shadowsocks-Proxy Ihres Macs routet.

Schritt 1: iptables-Regeln konfigurieren

1. Fügen Sie iptables-Regeln hinzu, um den Datenverkehr umzuleiten:

   ```
   # Leite den gesamten TCP-Datenverkehr an Redsocks weiter (außer den Datenverkehr zum Proxy selbst)
   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
   ```

Wende die REDSOCKS-Kette auf den gesamten ausgehenden Verkehr an iptables -t nat -A OUTPUT -p tcp -j REDSOCKS iptables -t nat -A PREROUTING -p tcp -j REDSOCKS “‘

Erklärung: - Erstelle eine neue Kette: `REDSOCKS` - Proxy-Verkehr ausschließen: Stelle sicher, dass der Verkehr, der für den Proxy selbst bestimmt ist, nicht umgeleitet wird. - Anderen TCP-Verkehr umleiten: Leite anderen TCP-Verkehr an den Port weiter, den Redsocks abhört (`12345`).

2. iptables-Regeln speichern:

Um diese Regeln über Neustarts hinweg beizubehalten, fügen Sie sie der Firewall-Konfiguration hinzu.

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

Fügen Sie die iptables-Regeln hinzu:

```
# Leite den gesamten TCP-Datenverkehr an Redsocks weiter (außer 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
```

Die REDSOCKS-Kette anwenden iptables -t nat -A OUTPUT -p tcp -j REDSOCKS iptables -t nat -A PREROUTING -p tcp -j REDSOCKS “‘

Speichern und Beenden: - Drücken Sie `ESC`, geben Sie `:wq` ein und drücken Sie `Enter`.

3. Firewall neu starten, um die Änderungen zu übernehmen:

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

Schritt 2: Überprüfen, ob der Traffic umgeleitet wird

1. Überprüfen Sie die Redsocks-Protokolle:

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

   Sie sollten Protokolle sehen, die anzeigen, dass der Datenverkehr über Redsocks verarbeitet wird.

2. Test von einem Client-Gerät aus:

- Verbinden Sie ein Gerät mit Ihrem OpenWRT-Router.
- Besuchen Sie eine Website oder führen Sie eine Aktion aus, die das Internet nutzt.
- Überprüfen Sie, ob der Datenverkehr über den Shadowsocks-Proxy geleitet wird, indem Sie die externe IP-Adresse überprüfen (z. B. über WhatIsMyIP.com), um festzustellen, ob sie die IP des Proxys widerspiegelt.

---

6. Testen des Proxy-Setups

Stellen Sie sicher, dass das gesamte Setup wie vorgesehen funktioniert, indem Sie die folgenden Tests durchführen.

Schritt 1: Überprüfen der Shadowsocks-Verbindung auf dem Mac

1. Überprüfen Sie den Status des Shadowsocks-Clients:
   - Stellen Sie sicher, dass Shadowsocks-NG oder Clash aktiv mit dem Shadowsocks-Server verbunden ist.
   - Vergewissern Sie sich, dass der lokale Proxy (z.B. `xxx.xxx.xxx.xxx:xxxxx`) erreichbar ist.
2. Testen Sie den Proxy lokal:
   - Öffnen Sie auf Ihrem Mac einen Browser und konfigurieren Sie ihn so, dass er `localhost:1080` als SOCKS5-Proxy verwendet.
   - Besuchen Sie WhatIsMyIP.com, um zu bestätigen, dass die IP mit dem Shadowsocks-Server übereinstimmt.

Schritt 2: Überprüfen, ob der OpenWRT-Datenverkehr über den Proxy geleitet wird

1. Überprüfen Sie die externe IP von OpenWRT:
   - Besuchen Sie von einem Gerät, das mit OpenWRT verbunden ist, WhatIsMyIP.com, um zu sehen, ob die IP die IP des Shadowsocks-Servers widerspiegelt.
2. Überwachen Sie die Redsocks-Protokolle:
   - Auf OpenWRT überwachen Sie die Redsocks-Protokolle, um sicherzustellen, dass der Datenverkehr umgeleitet wird.

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

3. Bei Bedarf Fehlerbehebung durchführen:
    - Wenn der Datenverkehr nicht korrekt weitergeleitet wird:
        - Stellen Sie sicher, dass der Shadowsocks-Client auf dem Mac läuft und erreichbar ist.
        - Überprüfen Sie, ob die iptables-Regeln korrekt eingerichtet sind.
        - Überprüfen Sie die Firewall-Einstellungen sowohl auf dem Mac als auch auf OpenWRT.

Weitere Überlegungen

1. Sicherheit

- Sichern Sie Ihren Proxy:
    - Stellen Sie sicher, dass nur vertrauenswürdige Geräte auf den Proxy zugreifen können. Da Sie den gesamten Datenverkehr über Redsocks umleiten, sollten Sie sicherstellen, dass die Firewall Ihres Macs nur Verbindungen von Ihrem OpenWRT-Router zulässt.

Auf macOS:

- Gehen Sie zu Systemeinstellungen > Sicherheit & Datenschutz > Firewall.
- Konfigurieren Sie die Firewall so, dass eingehende Verbindungen auf dem Proxy-Port (`xxxxx`) nur von der IP des OpenWRT-Routers zugelassen werden.
- Authentifizierung:
    - Shadowsocks bietet bereits ein gewisses Maß an Sicherheit durch Verschlüsselung. Stellen Sie sicher, dass starke Passwörter und Verschlüsselungsmethoden verwendet werden.

2. Leistung

- Router-Ressourcen:

- Das Ausführen von Proxy-Diensten wie Redsocks kann zusätzliche CPU- und Speicherressourcen auf Ihrem OpenWRT-Router beanspruchen. Stellen Sie sicher, dass Ihr Router über ausreichende Ressourcen verfügt.

- Mac-Leistung:
  - Stellen Sie sicher, dass Ihr Mac eingeschaltet und mit dem Netzwerk verbunden bleibt, um die Verfügbarkeit des Proxys aufrechtzuerhalten.

3. Wartung

- Überwachung der Protokolle:
  - Überprüfen Sie regelmäßig die Protokolle von Redsocks und Shadowsocks auf ungewöhnliche Aktivitäten oder Fehler.
- Software aktualisieren:
  - Halten Sie OpenWRT, Redsocks und Ihren Shadowsocks-Client auf dem neuesten Stand, um von Sicherheitsupdates und Leistungsverbesserungen zu profitieren.

4. Alternative Ansätze

Während die Verwendung eines Macs als Zwischen-Proxy-Server möglich ist, sollten Sie die folgenden Alternativen in Betracht ziehen, die möglicherweise einfacher einzurichten sind:

- OpenWRT direkt als Shadowsocks-Client konfigurieren:
  - OpenWRT unterstützt Shadowsocks direkt über Pakete wie `shadowsocks-libev`. Dieser Ansatz macht einen Mac als Vermittler überflüssig.
- Verwenden Sie ein dediziertes Proxy/VPN-Gerät:
  - Geräte wie der Raspberry Pi können Proxy-Dienste ausführen und als dedizierte Gateways fungieren.

Fazit

Indem Sie die oben beschriebenen Schritte befolgt haben, haben Sie Ihren Mac als Shadowsocks-Proxy-Server eingerichtet und Ihren OpenWRT-Router so konfiguriert, dass

der gesamte Datenverkehr aller angeschlossenen Geräte über diesen Proxy geleitet wird. Dieses Setup verbessert die Privatsphäre und Kontrolle Ihres Netzwerks durch die Nutzung des Shadowsocks-Protokolls.

Zusammenfassung der wichtigsten Punkte:

1. Shadowsocks-Client auf dem Mac:
    - Shadowsocks-NG oder Clash mit der bereitgestellten Shadowsocks-URL installiert und konfiguriert.
    - Den Client so konfiguriert, dass er auf die LAN-IP des Macs hört.
2. Proxy-Zugänglichkeit:
    - Dem Mac eine statische IP zugewiesen, um einen konsistenten Proxy-Zugang zu gewährleisten.
    - Die macOS-Firewall so konfiguriert, dass eingehende Proxy-Verbindungen zugelassen werden.
3. OpenWRT-Konfiguration:
    - Installiert und konfiguriert Redsocks, um den gesamten ausgehenden TCP-Datenverkehr über den Shadowsocks-Proxy umzuleiten.
    - Notwendige iptables-Regeln angewendet, um die Datenverkehrsumleitung zu erzwingen.
4. Testen:
    - Überprüft, dass der Datenverkehr von verbundenen Geräten über den Shadowsocks-Proxy geleitet wird, indem die externen IP-Adressen überprüft wurden.

Empfehlungen:

- Stabilität sicherstellen: Halten Sie Ihren Mac mit Strom versorgt und verbunden, um die Verfügbarkeit des Proxys zu gewährleisten.
- Sicherheit an erster Stelle: Aktualisieren Sie regelmäßig alle Komponenten und überwachen Sie die Protokolle, um sich vor unbefugtem Zugriff zu schützen.
- Direkte Router-Konfiguration in Betracht ziehen: Für eine effizientere Einrichtung können Sie die Konfiguration von Shadowsocks direkt auf Ihrem OpenWRT-Router in Betracht ziehen.

Wenn Sie auf Probleme stoßen oder weitere Unterstützung bei bestimmten Konfigurationen benötigen, zögern Sie nicht, sich zu melden!

```
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 = ""; }
```