Redsocks の活用

もちろんです！Mac コンピュータを使用して Shadowsocks プロキシを設定し、OpenWRT ルーターを構成して、接続されたすべてのデバイスのトラフィックをこのプロキシ経由でルーティングする手順をご案内します。このセットアップには、以下の主要なステップが含まれます：

1. macOS に Shadowsocks クライアントを設定する（Shadowsocks-NG または Clash を使用）
2. macOS を外部プロキシ接続を許可するように設定する
3. Mac に静的 IP を割り当てる
4. OpenWRT に Redsocks をインストールして設定する
5. OpenWRT のトラフィックを macOS のプロキシ経由にリダイレクトする
6. プロキシ設定をテストする

各ステップについて詳しく見ていきましょう。

---

1. macOS での Shadowsocks クライアントの設定

Shadowsocks クライアントとして、Shadowsocks-NG または Clash のどちらかを使用できます。以下にそれぞれの設定手順を記載します。

オプション A: Shadowsocks-NG を使用する

Shadowsocks-NG は、macOS 向けの人気で使いやすい Shadowsocks クライアントです。

ステップ 1: Shadowsocks-NG をダウンロードしてインストールする

1. Shadowsocks-NG をダウンロードする：
    - Shadowsocks-NG GitHub Releases ページにアクセスします。
    - 最新の `.dmg` ファイルをダウンロードします。
2. アプリケーションをインストールする：
    - ダウンロードした `.dmg` ファイルを開きます。
    - ShadowsocksX-NG アプリを「アプリケーション」フォルダにドラッグします。
3. Shadowsocks-NG を起動する：

- アプリケーションフォルダから ShadowsocksX-NG を開きます。
- システム環境設定でアプリに必要な権限を付与する必要があるかもしれません。

ステップ 2: Shadowsocks-NG の設定

1. 設定を開く：
   - メニューバーの ShadowsocksX-NG アイコンをクリックします。
   -「ShadowsocksX-NG を開く」＞「設定」を選択します。
2. 新しいサーバーを追加:
   -「Servers」タブに移動します。
   -「+」ボタンをクリックして新しいサーバーを追加します。
3. Shadowsocks URL をインポートする:
   - Shadowsocks URL をコピー:

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

   - インポート方法:
     -「インポート」をクリック。
     - Shadowsocks URL を貼り付ける。
     - Shadowsocks-NG が自動的にサーバーの詳細を解析し、入力してくれるはずです。
4. ローカルプロキシを設定する：
   -「SOCKS5 プロキシを有効にする」にチェックが入っていることを確認します。
   - ローカルポート（デフォルトは通常 1080）をメモしておきます。
5. 保存して有効化:
   -「OK」をクリックしてサーバーを保存します。
   -「Shadowsocks を有効にする」スイッチを ON に切り替えます。

オプション B: Clash を使用する

Clash は、Shadowsocks を含む複数のプロトコルをサポートする多機能なプロキシクライアントです。

ステップ 1: Clash をダウンロードしてインストールする

1. Clash for macOS をダウンロード:
    - Clash GitHub Releases ページ にアクセスします。
    - 最新の Clash for macOS バイナリをダウンロードします。
2. アプリケーションをインストールする：
    - ダウンロードした Clash アプリケーションを「アプリケーション」フォルダに移動します。
3. Clash を起動する：
    - アプリケーションフォルダから Clash を開きます。
    - システム環境設定で必要な権限を付与する必要があるかもしれません。

ステップ 2: Clash の設定

1. 設定ファイルにアクセスする:
    - Clash は YAML 設定ファイルを使用します。TextEdit や Visual Studio Code などのテキストエディタを使って、作成または編集できます。
2. Shadowsocks サーバーを追加する:
    - 以下の内容で設定ファイル（例: `config.yaml`）を作成します:

```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"
```

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

rules:
  - MATCH,Default
```

メモ:
- `port` と `socks-port` は、ClashがリッスンするHTTPおよびSOCKS5プロキシポートを定義します。
- `allow-lan: true` は、LANデバイスがプロキシを使用できるようにします。
- `proxies` セクションには、Shadowsocksサーバーの詳細が含まれています。
- `proxy-groups` と `rules` は、トラフィックのルーティング方法を決定します。

3. 設定ファイルを使用して Clash を開始:
    - Clash を起動し、`config.yaml` ファイルを使用するように設定します。
    - Clash を起動する際に、設定ファイルのパスを指定する必要があるかもしれません。
4. プロキシが動作していることを確認する:
    - Clash がアクティブで、Shadowsocks サーバーに接続されていることを確認します。
    - メニューバーのアイコンでステータスを確認します。

---

2. macOS を外部プロキシ接続を許可するように設定する

デフォルトでは、Shadowsocks クライアントはプロキシを `localhost`（`127.0.0.1`）にバインドするため、Mac のみがこのプロキシを使用できます。OpenWRT ルーターがこのプロキシを使用できるようにするには、プロキシを Mac の LAN IP にバインドする必要があります。

Shadowsocks-NG の場合:

1. 設定を開く:
    - メニューバーの ShadowsocksX-NG アイコンをクリックします。

- 「ShadowsocksX-NG を開く」＞「設定」を選択します。

2. 詳細設定タブに移動：
   - 「詳細設定」タブに移動します。
3. リスニングアドレスの設定:
   - 「Listen Address」を `127.0.0.1` から `0.0.0.0` に変更し、任意のインターフェースからの接続を許可します。
   - または、Mac の LAN IP（例: `192.168.1.xxx`）を指定します。
4. Shadowsocks-NG を保存して再起動:
   - 「OK」をクリックして変更を保存します。
   - 新しい設定を適用するために、Shadowsocks-NG クライアントを再起動します。

Clash の場合:

1. 設定ファイルを編集する:
   - `config.yaml` 内で `allow-lan: true` 設定が有効になっていることを確認してください。
2. すべてのインターフェースにバインドする:
   - 設定で `allow-lan: true` を設定すると、通常、プロキシは LAN を含むすべての利用可能なインターフェースにバインドされます。
3. Clash を再起動：
   - 変更を適用するために Clash クライアントを再起動します。

---

3. Mac に静的 IP を割り当てる

OpenWRT ルーターと Mac 間の接続を安定させるために、ローカルネットワーク内で Mac に静的 IP を割り当ててください。

macOS で静的 IP を割り当てる手順:

1. システム環境設定を開く：
   - Apple メニューをクリックし、「システム環境設定」を選択します。

2. ネットワーク設定に移動します：
    - 「ネットワーク」をクリックします。
3. アクティブな接続を選択:
    - Mac がルーターに接続されている方法に応じて、左側のサイドバーから「Wi-Fi」または「Ethernet」を選択します。
4. IPv4 設定を構成する：
    - 「詳細...」をクリックします。
    - 「TCP/IP」タブに移動します。
    - 「IPv4 を構成」を「DHCP を使用」から「手動」に変更します。
5. 静的 IP アドレスの設定:
    - IP アドレス: ルーターの DHCP 範囲外の IP を選び、競合を防ぎます（例: `192.168.1.xxx`）。
    - サブネットマスク: 通常は `255.255.255.0`。
    - ルーター: ルーターの IP アドレス（例: `192.168.1.1`）。
    - DNS サーバー: ルーターの IP を使用するか、`8.8.8.8` のような他の DNS サービスを利用できます。
6. 設定を適用する：
    - 「OK」をクリックし、次に「適用」をクリックして変更を保存します。

---

4. OpenWRT への Redsocks のインストールと設定

Redsocks は、ネットワークトラフィックを SOCKS5 プロキシ経由でルーティングできる透過型の SOCKS リダイレクターです。ここでは、Redsocks を使用して、Mac 上で動作している Shadowsocks プロキシを介して OpenWRT のトラフィックをリダイレクトします。

ステップ 1: Redsocks のインストール

1. パッケージリストの更新:

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

2. Redsocks をインストール:

```
opkg install redsocks
```

もし OpenWRT のリポジトリに Redsocks が利用できない場合、手動でコンパイルするか、代替パッケージを使用する必要があるかもしれません。

ステップ 2: Redsocks の設定

1. Redsocks 設定ファイルの作成または編集:

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

2. 以下の設定を追加:

```
 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;  # Redsocksがリッスンするローカルポート
     ip = xxx.xxx.xxx.xxx;  # Macの静的IPアドレス
     port = xxxxx;          # Shadowsocks-NGのローカルSOCKS5プロキシポート
     type = socks5;
     login = "";           # プロキシが認証を必要とする場合
     password = "";
 }
```

メモ: - `local_port`: Redsocks が iptables のリダイレクトからの接続を待ち受けるポート。- `ip` と `port`: Mac の Shadowsocks SOCKS5 プロキシを指す (`xxx.xxx.xxx.xxx:xxxxx` は前の手順に基づく)。- `type`: Shadowsocks が提供する SOCKS5 プロキシであるため、`socks5` に設定。

3. 保存して終了:
    - `ESC` を押し、`:wq` と入力して、`Enter` を押します。

4. ログファイルの作成:

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

ステップ 3: Redsocks サービスを開始する

1. 起動時に Redsocks を有効にする:

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

2. Redsocks を起動:

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

3. Redsocks が動作していることを確認する:

```
ps | grep redsocks
```

Redsocks プロセスが実行されているのが確認できるはずです。

---

5. OpenWRT のトラフィックを macOS プロキシ経由にリダイレクトする

OpenWRT に Redsocks が設定されたので、iptables を設定して、すべての発信 TCP トラフィックを Redsocks 経由でリダイレクトし、それが Mac の Shadowsocks プロキシを経由するようにします。

ステップ 1: iptables ルールの設定

1. トラフィックをリダイレクトするための iptables ルールを追加:

```
# すべての TCP トラフィックを Redsocks にリダイレクト（プロキシ自体へのトラフィックを除く）
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
```

すべての発信トラフィックに REDSOCKS チェーンを適用する

```
iptables -t nat -A OUTPUT -p tcp -j REDSOCKS
iptables -t nat -A PREROUTING -p tcp -j REDSOCKS
```

説明: - 新しいチェーンを作成: `REDSOCKS` - プロキシトラフィックを除外: プロキシ自体へのトラフィックがリダイレクトされないようにします。- その他の TCP トラフィックをリダイレクト: 他の TCP トラフィックを Redsocks のリスニングポート（`12345`）に転送します。

2. iptables ルールの保存:

これらのルールを再起動後も永続的にするには、ファイアウォールの設定に追加してください。

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

iptables ルールを追加:

```
# すべての TCP トラフィックを Redsocks にリダイレクト（プロキシを除く）
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
```

REDSOCKS チェーンの適用

```
iptables -t nat -A OUTPUT -p tcp -j REDSOCKS
iptables -t nat -A PREROUTING -p tcp -j REDSOCKS
```

保存して終了: - `ESC` を押し、`:wq` と入力して、`Enter` を押します。

3. 変更を適用するためにファイアウォールを再起動:

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

ステップ 2: トラフィックがリダイレクトされていることを確認する

1. Redsocks のログを確認する:

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

Redsocks を介してトラフィックが処理されていることを示すログが表示されるはずです。

2. クライアントデバイスからのテスト:
    - OpenWRT ルーターにデバイスを接続します。
    - インターネットを使用するウェブサイトにアクセスするか、何らかのアクションを実行します。
    - 外部 IP アドレス（例：WhatIsMyIP.com）を確認して、トラフィックが Shadowsocks プロキシを経由していることを確認します。プロキシの IP が反映されているかどうかを確認します。

---

6. プロキシ設定のテスト

以下のテストを実行して、セットアップ全体が意図した通りに動作することを確認してください。

ステップ 1: Mac での Shadowsocks 接続を確認する

1. Shadowsocks クライアントのステータスを確認する：
    - Shadowsocks-NG または Clash が Shadowsocks サーバーにアクティブに接続されていることを確認します。
    - ローカルプロキシ（例：`xxx.xxx.xxx.xxx:xxxxx`）がアクセス可能かどうかを確認します。
2. プロキシをローカルでテストする：
    - Mac でブラウザを開き、SOCKS5 プロキシとして `localhost:1080` を使用するように設定します。
    - WhatIsMyIP.comにアクセスし、IP が Shadowsocks サーバーと一致することを確認します。

ステップ 2: OpenWRT のトラフィックがプロキシを経由していることを確認する

1. OpenWRT の外部 IP を確認する:

- OpenWRT に接続されたデバイスから、WhatIsMyIP.comにアクセスし、IP が Shadowsocks サーバーの IP を反映しているかどうかを確認します。

2. Redsocks のログを監視する:
   - OpenWRT 上で、Redsocks のログを監視し、トラフィックがリダイレクトされていることを確認します。

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

3. 必要に応じてトラブルシューティングを行う:
   - トラフィックが正しくルーティングされない場合:
     - Mac 上の Shadowsocks クライアントが実行中でアクセス可能であることを確認する。
     - iptables のルールが正しく設定されていることを確認する。
     - Mac と OpenWRT の両方のファイアウォール設定を確認する。

追加の考慮事項

1. セキュリティ

- プロキシのセキュリティを確保する:
  - 信頼できるデバイスのみがプロキシにアクセスできるようにします。すべてのトラフィックを Redsocks 経由でリダイレクトしているため、Mac のファイアウォールが OpenWRT ルーターからの接続のみを許可するように設定します。

macOS の場合:

- システム環境設定 > セキュリティとプライバシー > ファイアウォールに移動します。
- ファイアウォールを設定し、OpenWRT ルーターの IP からのみプロキシポート（`xxxxx`）への着信接続を許可します。
- 認証:
  - Shadowsocks は暗号化を通じてある程度のセキュリティを提供しています。強力なパスワードと暗号化方式を確保してください。

2. パフォーマンス

- ルーターのリソース:
  - Redsocks のようなプロキシサービスを実行すると、OpenWRT ルーターの CPU とメモリを余分に消費する可能性があります。ルーターに十分なリソースがあることを確認してください。
- Mac のパフォーマンス:
  - プロキシの可用性を維持するために、Mac が電源に接続され、ネットワークに接続されていることを確認してください。

3. メンテナンス

- ログの監視:
  - Redsocks と Shadowsocks のログを定期的にチェックし、異常な活動やエラーがないか確認します。
- ソフトウェアの更新:
  - OpenWRT、Redsocks、および Shadowsocks クライアントを最新の状態に保ち、セキュリティパッチやパフォーマンスの向上を活用しましょう。

4. 代替アプローチ

Mac を中間プロキシサーバーとして使用することは可能ですが、以下の代替案を検討することで、より簡単な設定ができるかもしれません：

- OpenWRT を直接 Shadowsocks クライアントとして設定する:
  - OpenWRT は `shadowsocks-libev` のようなパッケージを通じて直接 Shadowsocks をサポートしています。この方法では、Mac を仲介する必要がなくなります。
- 専用のプロキシ/VPN デバイスを使用する:
  - Raspberry Pi のようなデバイスはプロキシサービスを実行し、専用のゲートウェイとして機能させることができます。

結論

上記の手順に従うことで、Mac を Shadowsocks プロキシサーバーとして設定し、OpenWRT ルーターを構成して、接続されたすべてのデバイスのトラフィックをこのプロキシ経由でルーティングするようにしました。この設定により、Shadowsocks プロトコルを活用してネットワークのプライバシーと制御が強化されます。

要点のまとめ：

1. Mac での Shadowsocks クライアント：
    - 提供された Shadowsocks URL を使用して、Shadowsocks-NG または Clash をインストールおよび設定しました。
    - クライアントを Mac の LAN IP でリッスンするように設定しました。
2. プロキシのアクセシビリティ:
    - Mac に静的 IP を割り当て、プロキシへの一貫したアクセスを確保しました。
    - macOS のファイアウォールを設定し、着信プロキシ接続を許可しました。
3. OpenWRT の設定：
    - Redsocks をインストールし、すべての外向き TCP トラフィックを Shadowsocks プロキシ経由でリダイレクトするように設定しました。
    - トラフィックリダイレクトを強制するために必要な iptables ルールを適用しました。
4. テスト:
    - 接続されたデバイスからのトラフィックが Shadowsocks プロキシを経由していることを確認するため、外部 IP アドレスをチェックしました。

おすすめ：

- **安定性を確保する**: プロキシの可用性を維持するために、Mac の電源を入れ、接続を維持してください。
- **セキュリティを最優先に**: すべてのコンポーネントを定期的に更新し、ログを監視して不正アクセスから保護してください。
- **ルーターの直接設定を検討する**: より効率的なセットアップのために、OpenWRT ルーター上で直接 Shadowsocks を設定する方法を探ってみてください。

特定の設定で問題が発生したり、さらなるサポートが必要な場合は、お気軽にお問い合わせください！

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

この設定は、redsocks の基本的な設定を定義しています。以下に各設定項目の説明を示します：

- log_debug = on;: デバッグログを有効にします。
- log_info = on;: 情報ログを有効にします。
- log = "file:/var/log/redsocks.log";: ログを/var/log/redsocks.log ファイルに出力します。
- daemon = on;: redsocks をデーモンとして実行します。
- redirector = generic;: ジェネリックなリダイレクタを使用します。

この設定は、redsocks がバックグラウンドで動作し、ログを指定されたファイルに出力するように指示しています。

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