Redsocks en Acción

¡Por supuesto! Te guiaré a través de la configuración de un proxy Shadowsocks utilizando tu computadora Mac y configurando tu router OpenWRT para enrutar todo el tráfico de los dispositivos conectados a través de este proxy. Esta configuración implica los siguientes pasos principales:

1. Configuración del Cliente Shadowsocks en macOS (Usando Shadowsocks-NG o Clash)
2. Configuración de macOS para Permitir Conexiones de Proxy Externas
3. Asignación de una IP Estática a tu Mac
4. Instalación y Configuración de Redsocks en OpenWRT
5. Redirección del Tráfico de OpenWRT a Través del Proxy en macOS
6. Prueba de la Configuración del Proxy

Profundicemos en cada paso en detalle.

---

1. Configuración del Cliente Shadowsocks en macOS

Puedes usar Shadowsocks-NG o Clash como cliente de Shadowsocks. A continuación, se encuentran las instrucciones para ambos.

Opción A: Usando Shadowsocks-NG

Shadowsocks-NG es un cliente de Shadowsocks popular y fácil de usar para macOS.

Paso 1: Descargar e instalar Shadowsocks-NG

1. Descargar Shadowsocks-NG:
    - Visita la página de lanzamientos de Shadowsocks-NG en GitHub.
    - Descarga el archivo `.dmg` más reciente.
2. Instala la aplicación:
    - Abre el archivo `.dmg` que descargaste.
    - Arrastra la aplicación ShadowsocksX-NG a la carpeta de Aplicaciones.

3. Inicia Shadowsocks-NG:
    - Abre ShadowsocksX-NG desde la carpeta de Aplicaciones.
    - Es posible que necesites otorgar los permisos necesarios a la aplicación en Preferencias del Sistema.

Paso 2: Configurar Shadowsocks-NG

1. Abrir Preferencias:
    - Haz clic en el ícono de ShadowsocksX-NG en la barra de menú.
    - Selecciona “Abrir ShadowsocksX-NG” > “Preferencias”.
2. Añadir un Nuevo Servidor:
    - Navega a la pestaña “Servers”.
    - Haz clic en el botón “+” para añadir un nuevo servidor.
3. Importa la URL de Shadowsocks:
    - Copia tu URL de Shadowsocks:

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

    - Método de importación:
        - Haz clic en “Importar”.
        - Pega tu URL de Shadowsocks.
        - Shadowsocks-NG debería analizar automáticamente y completar los detalles del servidor.
4. Configura el Proxy Local:
    - Asegúrate de que la opción “Habilitar Proxy SOCKS5” esté marcada.
    - Toma nota del Puerto Local (por defecto suele ser `1080`).
5. Guardar y Activar:
    - Haz clic en “Aceptar” para guardar el servidor.
    - Cambia el interruptor “Habilitar Shadowsocks” a ON.

Opción B: Usando Clash

Clash es un cliente proxy versátil que admite múltiples protocolos, incluyendo Shadowsocks.

Paso 1: Descargar e Instalar Clash

1. Descargar Clash para macOS:
    - Visita la página de lanzamientos de Clash en GitHub.
    - Descarga el binario más reciente de Clash para macOS.
2. Instala la aplicación:
    - Mueve la aplicación Clash descargada a tu carpeta de Aplicaciones.
3. Iniciar Clash:
    - Abre Clash desde la carpeta de Aplicaciones.
    - Es posible que necesites otorgar los permisos necesarios en Preferencias del Sistema.

Paso 2: Configurar Clash

1. Acceder al Archivo de Configuración:
    - Clash utiliza un archivo de configuración en formato YAML. Puedes crearlo o editarlo utilizando un editor de texto como TextEdit o Visual Studio Code.
2. Agrega tu servidor Shadowsocks:
    - Crea un archivo de configuración (por ejemplo, `config.yaml`) con el siguiente contenido:

```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
```

```
Notas:
- `port` y `socks-port` definen los puertos de proxy HTTP y SOCKS5 en los que Clash escuchará.
- `allow-lan: true` permite que los dispositivos de la LAN utilicen el proxy.
- La sección `proxies` incluye los detalles de tu servidor Shadowsocks.
- `proxy-groups` y `rules` determinan cómo se enruta el tráfico.
```

3. Iniciar Clash con la Configuración:
   - Inicia Clash y asegúrate de que utilice tu archivo `config.yaml`.
   - Es posible que necesites especificar la ruta de la configuración al iniciar Clash.
4. Verificar que el Proxy esté en Funcionamiento:
   - Asegúrate de que Clash esté activo y conectado a tu servidor Shadowsocks.
   - Revisa el ícono en la barra de menú para verificar el estado.

---

2. Configurar macOS para Permitir Conexiones de Proxy Externas

Por defecto, los clientes de Shadowsocks enlazan el proxy a `localhost` (`127.0.0.1`), lo que significa que solo la Mac puede usar el proxy. Para permitir que tu router OpenWRT use este proxy, necesitas enlazar el proxy a la IP LAN de la Mac.

Para Shadowsocks-NG:

1. Abrir Preferencias:

- Haz clic en el ícono de ShadowsocksX-NG en la barra de menú.
- Selecciona “Abrir ShadowsocksX-NG” > “Preferencias”.

2. Ve a la pestaña Avanzado:
   - Navega hasta la pestaña “Avanzado”.
3. Configurar la Dirección de Escucha:
   - Cambia la “Dirección de Escucha” de `127.0.0.1` a `0.0.0.0` para permitir conexiones desde cualquier interfaz.
   - Alternativamente, especifica la IP LAN del Mac (por ejemplo, `192.168.1.xxx`).
4. Guardar y Reiniciar Shadowsocks-NG:
   - Haz clic en “Aceptar” para guardar los cambios.
   - Reinicia el cliente Shadowsocks-NG para aplicar la nueva configuración.

Para Clash:

1. Editar el archivo de configuración:
   - Asegúrate de que la opción `allow-lan: true` esté habilitada en tu archivo `config.yaml`.
2. Vincular a Todas las Interfaces:
   - En la configuración, establecer `allow-lan: true` normalmente vincula el proxy a todas las interfaces disponibles, incluyendo la LAN.
3. Reiniciar Clash:
   - Reinicia el cliente de Clash para aplicar los cambios.

---

3. Asignar una IP estática a tu Mac

Para garantizar una conectividad constante entre tu router OpenWRT y el Mac, asigna una dirección IP estática a tu Mac dentro de tu red local.

Pasos para Asignar una IP Estática en macOS:

1. Abre las Preferencias del Sistema:

- Haz clic en el menú de Apple y selecciona “Preferencias del Sistema”.

2. Navega a la Configuración de Red:
   - Haz clic en “Red”.
3. Selecciona tu conexión activa:
   - Elige “Wi-Fi” o “Ethernet” en la barra lateral izquierda, dependiendo de cómo tu Mac esté conectado al router.
4. Configurar los ajustes de IPv4:
   - Haz clic en “Avanzado...”.
   - Ve a la pestaña “TCP/IP”.
   - Cambia “Configurar IPv4” de “Usar DHCP” a “Manualmente”.
5. Configurar una Dirección IP Estática:
   - Dirección IP: Elija una IP fuera del rango DHCP de su router para evitar conflictos (por ejemplo, `192.168.1.xxx`).
   - Máscara de Subred: Normalmente `255.255.255.0`.
   - Router: La dirección IP de su router (por ejemplo, `192.168.1.1`).
   - Servidor DNS: Puede usar la IP de su router o otro servicio DNS como `8.8.8.8`.
6. Aplicar Configuración:
   - Haz clic en “Aceptar” y luego en “Aplicar” para guardar los cambios.

---

4. Instalación y Configuración de Redsocks en OpenWRT

Redsocks es un redireccionador transparente de SOCKS que te permite enrutar el tráfico de red a través de un proxy SOCKS5. Utilizaremos Redsocks para redirigir el tráfico de OpenWRT a través del proxy Shadowsocks que se ejecuta en tu Mac.

Paso 1: Instalar Redsocks

1. Actualizar las listas de paquetes:

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

2. Instalar Redsocks:

```
opkg install redsocks
```

Si Redsocks no está disponible en tu repositorio de OpenWRT, es posible que necesites compilarlo manualmente o utilizar un paquete alternativo.

Paso 2: Configurar Redsocks

1. Crear o Editar el Archivo de Configuración de Redsocks:

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

2. Agrega la Siguiente Configuración:

```
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;  # Puerto local para que Redsocks escuche        ip = xxx.xxx.xxx.xxx;  # IP estática del Mac        port = xxxxx;  # Puerto local del proxy SOCKS5 de Shadowsocks-NG        type = socks5;        login = "";           # Si tu proxy requiere autenticación        password = "";    }
```

Notas: - `local_port`: El puerto en el que Redsocks escucha las conexiones entrantes desde redirecciones de iptables. - `ip` y `port`: Apuntan al proxy SOCKS5 de Shadowsocks en tu Mac (`xxx.xxx.xxx.xxx:xxxxx` según los pasos anteriores). - `type`: Configúralo como `socks5`, ya que Shadowsocks proporciona un proxy SOCKS5.

3. Guardar y Salir:
   - Presiona `ESC`, escribe `:wq`, y presiona `Enter`.
4. Crear Archivo de Registro:

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

Paso 3: Iniciar el Servicio de Redsocks

1. Habilitar Redsocks para que se Inicie al Arrancar:

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

2. Iniciar Redsocks:

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

3. Verifica que Redsocks esté en ejecución:

```
ps | grep redsocks
```

Deberías ver un proceso de Redsocks en ejecución.

---

5. Redirigiendo el Tráfico de OpenWRT a Través del Proxy de macOS

Ahora que Redsocks está configurado en OpenWRT, configura iptables para redirigir todo el tráfico TCP saliente a través de Redsocks, que a su vez lo enruta a través del proxy Shadowsocks de tu Mac.

Paso 1: Configurar las reglas de iptables

1. Agregar reglas de iptables para redirigir el tráfico:

```
# Redirigir todo el tráfico TCP a Redsocks (excepto el tráfico al propio 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
```

Aplicar la cadena REDSOCKS a todo el tráfico saliente iptables -t nat -A OUTPUT -p tcp -j REDSOCKS iptables -t nat -A PREROUTING -p tcp -j REDSOCKS “‘

Explicación: - Crear una Nueva Cadena: `REDSOCKS` - Excluir Tráfico del Proxy: Asegurarse de que el tráfico destinado al propio proxy no sea redirigido. - Redirigir Otro Tráfico TCP: Redirigir otro tráfico TCP al puerto de escucha de Redsocks (`12345`).

2. Guardar las reglas de iptables:

Para que estas reglas sean persistentes después de reinicios, agrégalas a la configuración del firewall.

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

Agrega las reglas de iptables:

```
# Redirigir todo el tráfico TCP a Redsocks (excepto el 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
```

Aplicar la cadena REDSOCKS iptables -t nat -A OUTPUT -p tcp -j REDSOCKS iptables -t nat -A PREROUTING -p tcp -j REDSOCKS “‘

Guardar y Salir: - Presiona `ESC`, escribe `:wq` y presiona `Enter`.

3. Reinicia el Firewall para Aplicar los Cambios:

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

Paso 2: Verificar que el tráfico esté siendo redirigido

1. Verificar los registros de Redsocks:

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

Deberías ver registros que indiquen que el tráfico está siendo procesado a través de Redsocks.

2. Prueba desde un dispositivo cliente:
    - Conecta un dispositivo a tu router OpenWRT.
    - Visita un sitio web o realiza una acción que utilice internet.
    - Verifica que el tráfico se enrute a través del proxy Shadowsocks comprobando la dirección IP externa (por ejemplo, a través de WhatIsMyIP.com) para ver si refleja la IP del proxy.

6. Prueba de la Configuración del Proxy

Asegúrate de que toda la configuración funcione como se espera realizando las siguientes pruebas.

Paso 1: Verificar la conexión de Shadowsocks en Mac

1. Verificar el estado del cliente Shadowsocks:
   - Asegúrate de que Shadowsocks-NG o Clash estén conectados activamente al servidor Shadowsocks.
   - Verifica que el proxy local (por ejemplo, `xxx.xxx.xxx.xxx:xxxxx`) sea accesible.
2. Prueba el Proxy Localmente:
   - En tu Mac, abre un navegador y configúralo para usar `localhost:1080` como el proxy SOCKS5.
   - Visita WhatIsMyIP.com para confirmar que la IP coincide con la del servidor Shadowsocks.

Paso 2: Verificar que el tráfico de OpenWRT se enrute a través del proxy

1. Verificar la IP Externa de OpenWRT:
   - Desde un dispositivo conectado a OpenWRT, visita WhatIsMyIP.com para ver si la IP refleja la IP del servidor Shadowsocks.
2. Monitorear los registros de Redsocks:
   - En OpenWRT, monitorea los registros de Redsocks para asegurarte de que el tráfico se esté redirigiendo correctamente.

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

3. Solucionar problemas si es necesario:
   - Si el tráfico no se está enrutando correctamente:
     - Asegúrate de que el cliente Shadowsocks en Mac esté en ejecución y sea accesible.
     - Verifica que las reglas de iptables estén configuradas correctamente.
     - Revisa la configuración del firewall tanto en Mac como en OpenWRT.

Consideraciones Adicionales

1. Seguridad

- Asegura tu Proxy:
  - Asegúrate de que solo dispositivos de confianza puedan acceder al proxy. Dado que estás redirigiendo todo el tráfico a través de Redsocks, asegúrate de que el firewall de tu Mac solo permita conexiones desde tu router OpenWRT.

En macOS:

- Ve a Preferencias del Sistema > Seguridad y Privacidad > Firewall.
- Configura el firewall para permitir conexiones entrantes en el puerto del proxy (`xxxxx`) solo desde la IP del router OpenWRT.
- Autenticación:
  - Shadowsocks ya proporciona un cierto nivel de seguridad a través del cifrado. Asegúrate de utilizar contraseñas fuertes y métodos de cifrado robustos.

2. Rendimiento

- Recursos del Router:
  - Ejecutar servicios de proxy como Redsocks puede consumir CPU y memoria adicionales en tu router OpenWRT. Asegúrate de que tu router tenga recursos suficientes.
- Rendimiento del Mac:
  - Asegúrate de que tu Mac permanezca encendida y conectada a la red para mantener la disponibilidad del proxy.

3. Mantenimiento

- Monitoreo de Registros:
  - Revisa periódicamente los registros de Redsocks y Shadowsocks en busca de actividades inusuales o errores.
- Actualizar Software:

- Mantén OpenWRT, Redsocks y tu cliente de Shadowsocks actualizados para beneficiarte de parches de seguridad y mejoras de rendimiento.

4. Enfoques Alternativos

Si bien es factible usar una Mac como servidor proxy intermediario, considera las siguientes alternativas para configuraciones potencialmente más simples:

- Configurar OpenWRT directamente como cliente de Shadowsocks:
  - OpenWRT admite Shadowsocks directamente a través de paquetes como `shadowsocks-libev`. Este enfoque elimina la necesidad de un intermediario con Mac.
- Usa un Dispositivo Dedicado de Proxy/VPN:
  - Dispositivos como Raspberry Pi pueden ejecutar servicios de proxy y actuar como puertas de enlace dedicadas.

Conclusión

Siguiendo los pasos descritos anteriormente, has configurado tu Mac como un servidor proxy Shadowsocks y has configurado tu router OpenWRT para enrutar todo el tráfico de los dispositivos conectados a través de este proxy. Esta configuración mejora la privacidad y el control de tu red al aprovechar el protocolo Shadowsocks.

Resumen de Puntos Clave:

1. Cliente Shadowsocks en Mac:
   - Instalé y configuré Shadowsocks-NG o Clash con la URL de Shadowsocks que proporcionaste.
   - Configuré el cliente para que escuche en la dirección IP LAN del Mac.
2. Accesibilidad del Proxy:
   - Asigné una IP estática a la Mac para garantizar un acceso consistente al proxy.
   - Configuré el firewall de macOS para permitir conexiones entrantes al proxy.
3. Configuración de OpenWRT:

- Instalé y configuré Redsocks para redirigir todo el tráfico TCP saliente a través del proxy Shadowsocks.
- Apliqué las reglas necesarias de iptables para hacer cumplir la redirección del tráfico.

4. Pruebas:
    - Verifiqué que el tráfico de los dispositivos conectados se enruta a través del proxy Shadowsocks comprobando las direcciones IP externas.

Recomendaciones:

- **Garantiza la Estabilidad**: Mantén tu Mac encendida y conectada para asegurar la disponibilidad del proxy.
- **Seguridad Primero**: Actualiza regularmente todos los componentes y monitorea los registros para protegerte contra accesos no autorizados.
- **Considera la Configuración Directa del Router**: Para una configuración más simplificada, explora la posibilidad de configurar Shadowsocks directamente en tu router OpenWRT.

Si encuentras algún problema o necesitas más ayuda con configuraciones específicas, ¡no dudes en contactarnos!

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

El bloque de configuración anterior define la configuración base para `redsocks`. Aquí está la traducción al español de los comentarios:

- `log_debug = on;`: Activa los registros de depuración.
- `log_info = on;`: Activa los registros de información.
- `log = "file:/var/log/redsocks.log";`: Especifica la ubicación del archivo de registro.
- `daemon = on;`: Ejecuta `redsocks` en modo demonio (en segundo plano).
- `redirector = generic;`: Define el tipo de redireccionador como genérico.

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