Proxy over SSH

I wanted to tunnel my SSH SOCKS5 proxy out to Wi-Fi, here's a little how to, DNS included:

```
# Create the SOCKS5 proxy bound to 127.0.0.1:9050
ssh -N -D 9050 socksproxy@123.1.2.3

# Verify
[0] % \ss -tulpn | \grep 9050
tcp   LISTEN 0      128                                127.0.0.1:9050       0.0.0.0:*
users:(("ssh",pid=1407523,fd=5))
tcp   LISTEN 0      128                                    [::1]:9050          [::]:*
users:(("ssh",pid=1407523,fd=4))

# Verify in Firefox that the proxy indeed works
# -> It does
```

Create a network for systemd-networkd:

```
File: /etc/systemd/network/wlan0.network
————————————————————————————————————

[Match]
Name=wlan0

[Network]
Address=10.42.0.1/24
DHCPServer=yes

[DHCPServer]
DNS=10.42.0.1
Domain=lan
```

Create an AP profile for iwd:

```
File: /var/lib/iwd/socks.ap
———————————————————————

[Settings]
SSID=Socks
```

```
Security=psk
Passphrase=password
```

Create the AP:

```
[iwd]# device wlan0 set-property Powered on
[iwd]# device wlan0 set-property Mode ap
[iwd]# ap wlan0 start-profile Socks
```

Create the iptables rules:

```
# Option 1) (DNS over TCP won't work with this setup)
iptables -t nat -N VSOCKS
iptables -t nat -A VSOCKS -p tcp -j REDIRECT --to-ports 12345
iptables -t nat -A PREROUTING -s 10.42.0.0/24 -p tcp -j REDIRECT --to-ports 12345
```

```
# Option 2
iptables -t nat -N VSOCKS

# 1) Don't touch DNS traffic (TCP) - let local DNS server handle it
iptables -t nat -A VSOCKS -p tcp --dport 53 -j RETURN

# 2) Also don't redirect traffic destined to the local resolver IP (cloudflared)
iptables -t nat -A VSOCKS -d 10.42.0.1 -j RETURN

# (optional) also ignore localhost if you have any local services
iptables -t nat -A VSOCKS -d 127.0.0.1 -j RETURN

# 3) Redirect remaining TCP to vsocks
iptables -t nat -A VSOCKS -p tcp -j REDIRECT --to-ports 12345

# 4) Hook the chain for clients from your AP network
iptables -t nat -D PREROUTING -s 10.42.0.0/24 -p tcp -j REDIRECT --to-ports 12345 2>/dev/null
|| true
iptables -t nat -A PREROUTING -s 10.42.0.0/24 -p tcp -j VSOCKS
```

Run cloudflared on the same host as vsocks to enable DNS proxying:

```
sudo cloudflared proxy-dns \
  --address 10.42.0.1 --port 53 \
  --upstream https://1.1.1.1/dns-query \
```

```
  --upstream https://1.0.0.1/dns-query socks5://127.0.0.1:9050
```

Run vsocks:

```
vsocks 0.0.0.0:12345 127.0.0.1:9050


[vsck] VSocks - ver. 1.05.1a
[vsck] load: A:0/0 B:0/0 *:1/256
```

Revision #3
Created 2025-09-15 16:47:27 UTC by C0rn3j
Updated 2025-09-19 20:17:45 UTC by C0rn3j