SOCKS5 revisited

Effektive Zugriffe auf Kunden- und Testumgebungen

Sicher und flexibel in fremden Netzen arbeiten – ohne das eigene Netzwerk umzubauen

Andreas Plöger
secom consulting und bergwerk IT.

secom secure communications consulting

Das Problem

Wie greifen wir sicher auf fremde Netzwerke zu?

Typische Situationen:

- Arbeiten beim **Kunden**
- Zugriff auf **Dev-, Test- und Staging-Umgebungen**
- Gleiche IP-Adressen in unterschiedlichen Umgebungen
- Unterschiedliche Netzwerke gleichzeitig nutzen

Die Idee: SOCKS5

SOCKS5 –"Kommunikation über Bande"

Der eigene Rechner baut eine Verbindung zu einem socks-Server auf. Dieses Gateway übernimmt anschließend die Verbindung zum Zielsystem.

Das eigene Netzwerk muss dafür nicht umkonfiguriert werden – nur der Prozess. Keine root-Rechte.

Die Anwendung muss SOCKS unterstützten.

Nicht nur für HTTP, sondern grundsätzlich für alle TCP- und UDP-Verbindungen.

Z.B.: apt install microsocks

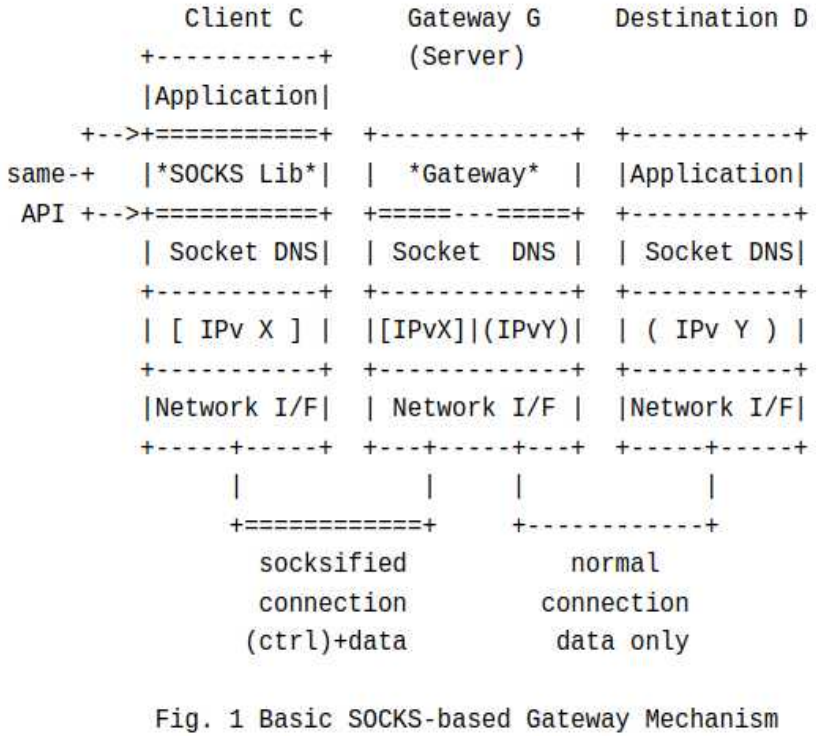


Fig. 1 Basic SOCKS-based Gateway Mechanism

Quelle: rfc3089

SOCKS ist nicht neu

Ein alter Ansatz mit neuen Einsatzmöglichkeiten

- SOCKS1: **1989**
- SOCKS5: seit **1996**
- Früher beispielsweise als Alternative zu ISDN-Routern
- Heute weiterhin relevant – unter anderem bei VPNs (z.B. NordVPN), TOR
- ... und SSH

```
ISDNPKT kostet 178,00 inkl. MwSt IPSWITCH kostet 348,00 inkl. MwST
ISDNPKT + IPSWITCH Bundle: 498,00 inkl. MwSt.  ISDNPKT + IPSWITCH +
TELES.S0 Bundle 888,00 DM inkl. MwSt

Das "PLUS"-Paket, inkl. SNMP (MIB-II + Herstellererweiterungen),
verfuegbar ab CeBIT 94: ISDNPKT + IPSWITCH+ + TELES.S0 Bundle:
1.398,00 DM inkl. MwSt.  beinhaltet kostenlosen Upgrade auf die PLUS-
Version des ISDNPKT, die Mitte April verfuegbar sein wird.
```

SOCKS5 über SSH

Mit SSH wird SOCKS5 besonders interessant

SSH bietet neben klassischen Tunneln (-L und -R) auch einen **dynamischen Tunnel**:

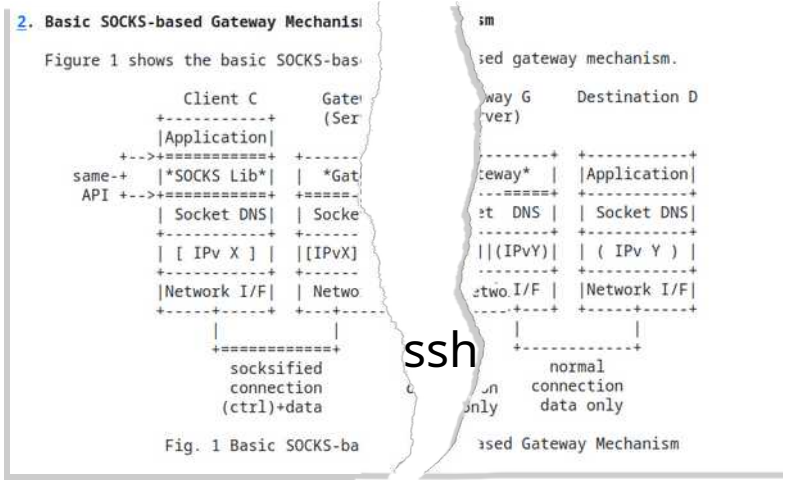
ssh -D 4711

Dadurch entsteht ein SOCKS5-Proxy auf dem eigenen Rechner.

Prinzip:

Laptop → SOCKS5 → SSH-Server → Zielnetz

Der Einstiegspunkt liegt lokal, der Ausgangspunkt im Zielnetz.



Warum nicht einfach VPN?

VPN funktioniert – aber nicht immer ideal

Einrichtung des VPN genügt nicht ....

- Routing auf dem eigenen Rechner verändern
- DNS verändern

Verführt dazu, das mit openvpn zu erledigen.

= unhygienisch

unhygienisch?

Szenario: Ein Angreifer hat sich im Kundennetz festgesetzt und wir sollen helfen.

- Wollen wir unser Routing und unsere Namensauflösung von einem potentiell verseuchten Kundensystem ändern lassen?
- *... „roter Teppich" ...*
- Konflikte

```
11:41:02 net_route_v4_add: 217.92.194.61/32 via 192.168.100.2 dev [
11:41:02 net_route_v4_add: 171.20.17.0/24 via 10.81.234.1 dev [NULL
11:41:02 net_route_v4_add: 217.92.194.61/32 via 192.168.100.2 dev [
11:41:02 sitnl_send: rtnl: generic error (-17): File exists
11:41:02 NOTE: Linux route add command failed because route exists
```

```
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_c
    link/none
    inet 10.1.70.23/24 brd 10.1.70.255 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::d4a:b325:1398:80d5/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
root@chromec:~#
```

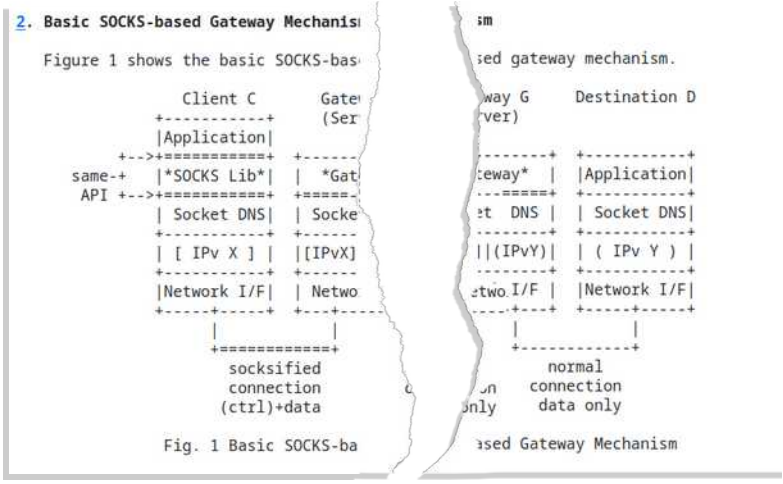
```
bergwerk@bwsnjumphost:~$ nmap 10.1.70.23
Starting Nmap 7.93 ( https://nmap.org ) at 2026-09-09
Nmap scan report for 10.1.70.23
Host is up (0.029s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.57 se
```

Der große Vorteil bei ssh+socks: Isolation

Jedes Zielnetz bleibt für sich

Mit SOCKS5:

- eigenes Routing bleibt unverändert
- eigene Namensauflösung bleibt unverändert
- also rückwirkungsfrei
- Verbindungen bleiben sauber voneinander getrennt, mehrere Zielnetze können ohne Konflikte parallel genutzt werden



Besonders interessant für **Dev / Test / Staging**, wenn dort dieselben IP-Adressen und DNS-Namen wie in der Produktion verwendet werden.

Wie sieht das beim Kunden aus?

Einfacher Aufbau

Der Kunde:

1. stellt SSH-Server bereit, hinterlegt meinen öffentlichen SSH-Key
2. erlaubt unsere feste IP-Adresse für SSH
3. richtet Port-Weiterleitung ein

Der Aufwand ist minimal!

Wir:

ssh -D 4711 admin@kunde.de

→ SOCKS5 läuft lokal auf Port 4711.

Verwendung von SOCKS5 - Web

Im Web-Browser: Verbindungs-/Proxy-Einstellung SOCKS5 127.0.0.1:4711

besser: proxy.pac

```
if(dnsDomainIs(host, ".kunde1.local"))
   return "SOCKS5 127.0.0.1:4711";
 if(dnsDomainIs(host, ".kunde2.local") || isInNet(host, "10.0.0.0", "255.0.
   return "SOCKS5 127.0.0.1:4712";
else
   return "DIRECT";
```

heikel: Syntaxfehler finden. 'ssh -v'. Vergleich mit funktionierender Vor-Version.

ggf. mehrere firefox-Profile ('firefox -P') mit eigenen Proxy-Einstellungen

Was kann ich damit machen?

SOCKS5 ist nicht nur für den Browser

Beispiel

Web-browser | SSH | RDP | Git

+ weitere Anwendungen mit SOCKS-Unterstützung

Für mehrere Kunden können unterschiedliche SOCKS5-Ports verwendet werden.

Verwendung von SOCKS5 - openssh

1 Answer

Sorted by: Highest score (default)

1

OpenSSH client does not have support for SOCKS protocol. It does not make sense to implement it in OpenSSH itself, because there are other specialized tool (`netcat`) doing it and OpenSSH can work with them (using `ProxyCommand`).

It is the logic of UNIX philosophy:

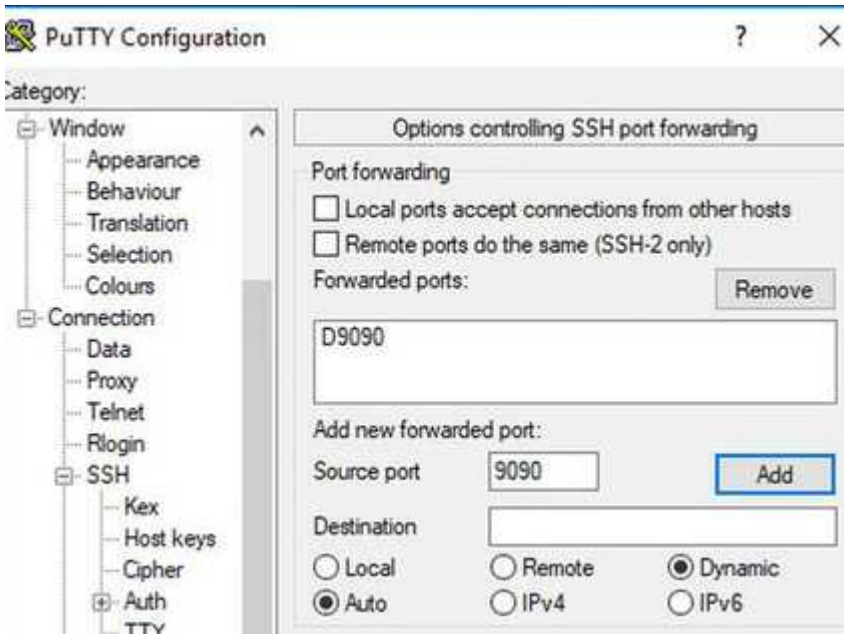
> Smaller programs are not only easier to write, optimize, and maintain; they are easier to delete when deprecated.

Quelle: https://superuser.com/questions/1229506/openssh-as-a-socks5-proxy-client

also:

```
Host bw-xxx
  Hostname xxx.berg45.de
  ProxyCommand /usr/bin/nc -x 127.0.0.1:5000 %h %p
```

~~Verwend~~Einrichtung von SOCKS5 - putty



Verwendung von SOCKS5 – rdp und vnc

Client entsprechend aussuchen, z.B. xfreerdp

Verwendung von SOCKS5 - git

eher nicht per (reverse - siehe unten) SOCKS, sondern 'ssh -R', das funktioniert natürlich weiter!

Verwendung von SOCKS5 - sonst

notfalls:
tsocks
Socksify
'ssh -L' funktioniert natürlich weiter

Reverse SOCKS5

Der nächste Schritt

Neuere OpenSSH-Versionen ermöglichen auch **Reverse SOCKS5** tunnel.

Das ist interessant für Umgebungen, die beispielsweise keinen direkten Internetzugang haben.

Bisher:

SSH remote Tunnel → zentraler Squid → Internet

Neu:

SSH reverse SOCKS5 → direkter Zugriff über den Tunnel ohne Squid

Rückblick

SOCKS5 statt Netzwerkumbau

Die wichtigsten Punkte:

- ✓ kann/sollte VPN ersetzen
- ✓ Originales Routing und DNS des Zielnetzes, eigener Rechner bleibt unverändert
- ✓ Wirkliche Einbahnstraße
- ✓ Zielnetze sind sauber voneinander getrennt
  Ideal für Kunden-, Dev-, Test- und Staging-Umgebungen
- ✓ SSH bringt SOCKS5 bereits mit
- ✓ Jede Anwendung erlaubt/erfordert eigene Konfiguration
- ✓ Wenig Infrastruktur auf Kundenseite notwendig

Fragen und Antworten