Firewall-Piercing mit httptunnel

(Port 80 benutzen, um Netzwerke über http-requests zu verbinden)

Man benötigt:

1. Einen Linux/Unix-Server im Internet, auf dem man den SERVER-Teil starten kann
2. Einen Linux-Unix-Client, mit dem man durch einen Firewall/Proxy ins Internet will, der aber nur Port 80 durchlässt und auch noch eine Proxy-Konfiguration erfordert (worst case)

Beispiel für einen „Webserver“ auf Port 8000 (geht ohne root). Dieser soll alle Verbindungen auf Port 22 (SSH) umleiten, und die Übersetzung vom SSH- ins HTTP-Protokoll verarbeiten:

Auf dem Server „meinserver.de“:

```
hts -F localhost:22 8000
```

Auf dem Client (hinter dem Firewall/Proxy):

```
htc -F 2222 meinserver.de:8000
```

Nun kann über den http-Tunnel eine Verbindung zum SSH-Server auf meinserver.de aufgebaut werden, indem man sich mit Port 2222 lokal verbindet!

ssh -p 2222 knopper@localhost

Wofür braucht man das?

- Betreiber eines Firewall hat diesen so konfiguriert, dass nur das gefährliche, unverschlüsselte http (Port 80) duchgelassen wird, ich möchte aber meine E-Mail lesen, ohne dass mein Passwort übers Netz geht!

- Nutzung anderer Dienste als reines http/https.

- Zwangsproxy umgehen bzw. kreativ nutzen.