GPN24

Besser Tunneln mit SSH

2026-06-06 20:00–21:00, ZKM Kubus

gpn24.de

Gulasch at the scale of chaos.

(Martin) Leyrer

martin@leyrer.priv.at

https://martin.leyrer.priv.at

@leyrer@23.social

https://media.ccc.de/search?p=leyrer

- Der Leyrer / Du Leyrer / Dem Leyrer sein ...
- „Du Martin“ ist auch OK, Siezen verwirrt mich
- Sammelt alte Hardware (NeXTCube anyone?)
- #GPN24

Sven Guckes

https://www.guckes.net/

GPN20: Besser leben mit SSH

- https://media.ccc.de/v/gpn20-8-besser-leben-mit-ssh
- https://martin.leyrer.priv.at/static/talks2022.html

No Usernames

```
Host demo
    HostName ssh-server.example.com
    User gulasch
```

Tippfaul

```
ssh gulasch@ssh.example.com
```

```
ssh demo
```

ssh-keygen

```
$ ssh-keygen -t ed25519 \
    -a 420 \
    -f ~/.ssh/demo.ed25519 \
    -C "Dem leyrer sein key (gpn20)"
```

~/.ssh/config

```
Host demo
    HostName ssh.example.com
    User gulasch
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519
```

Connect without passphrase

```
ssh-add ~/.ssh/demo.ed25519

ssh demo
```

Sane Defaults

```
Host demo bastion
    HostName ssh.example.com
    User gulasch
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519
…
Host *
    IdentitiesOnly yes
    UseRoaming no
    SendEnv LANG LC_*
    Compression yes
```

Elegant “Jumping”

```
Host demo bastion
    HostName ssh.example.com
    User gulasch
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519
Host internal
    HostName target.local
    ProxyJump bastion
    User gulasch
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519
```

GPN21: Noch besser leben mit SSH

- https://media.ccc.de/v/gpn21-28-noch-besser-leben-mit-ssh
- https://martin.leyrer.priv.at/static/talks2023.html

TPM für SSH

```
Host gulasch
  HostName ssh-server.example.com
  User gulasch
    PKCS11Provider /usr/lib/…/libtpm2_pkcs11.so.1
    PasswordAuthentication no
```

Securing SSH keys with

YubiKey Security Keys U2F

2FA (TOTP)

```
sudo apt-get install libpam-google-authenticator
```

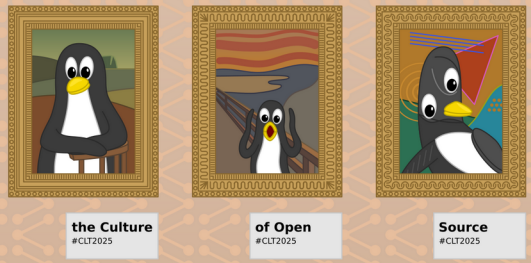
```
/etc/pam.d/sshd:
auth required pam_google_authenticator.so
/etc/ssh/sshd_config:
KbdInteractiveAuthentication yes
```

Als User am Server (!) ausführen: `google-authenticator`

CLT25: OpenSSH, das neue Zeug

- https://media.ccc.de/v/clt25-331-openssh-das-neue-zeug
- https://martin.leyrer.priv.at/static/talks2025.html

Lyrische Lesung des OpenSSH Changelogs

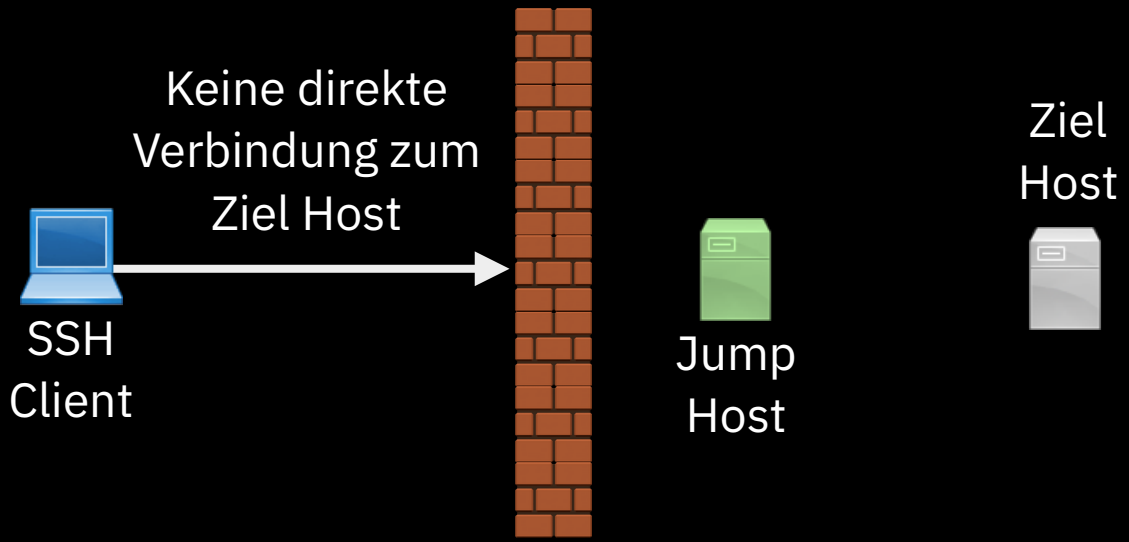


Chemnitzer Linux-Tage
22. und 23. März 2025

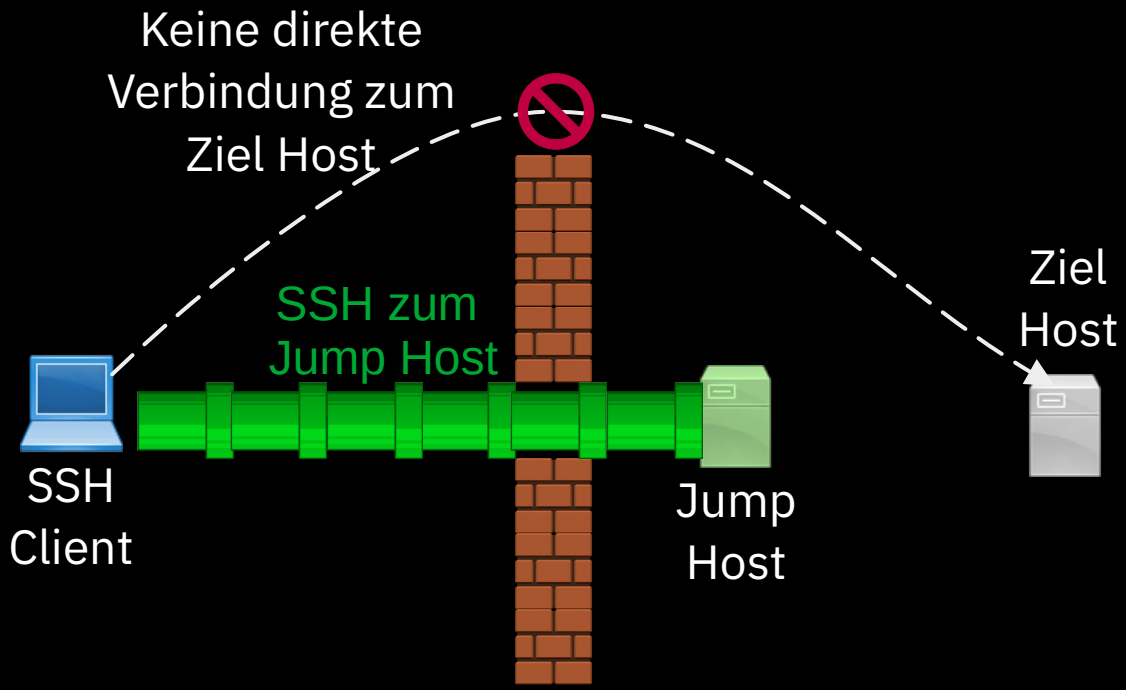
Besser Tunneln mit SSH

Bastion/Jump Hosts

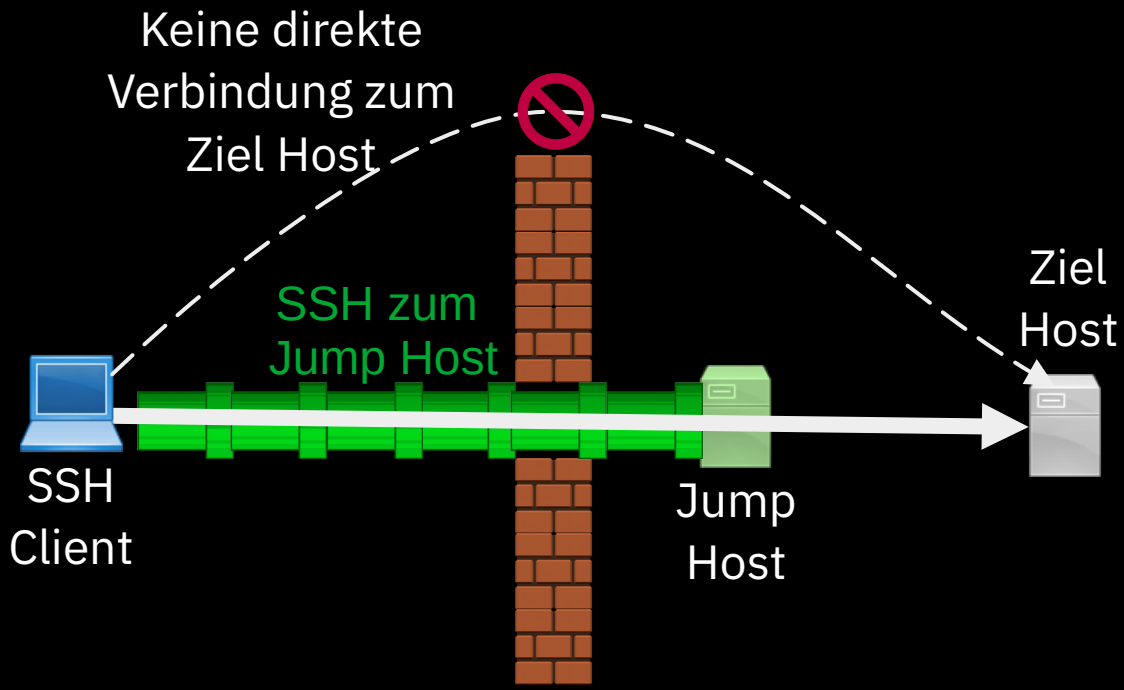
Warum Jump Hosts?



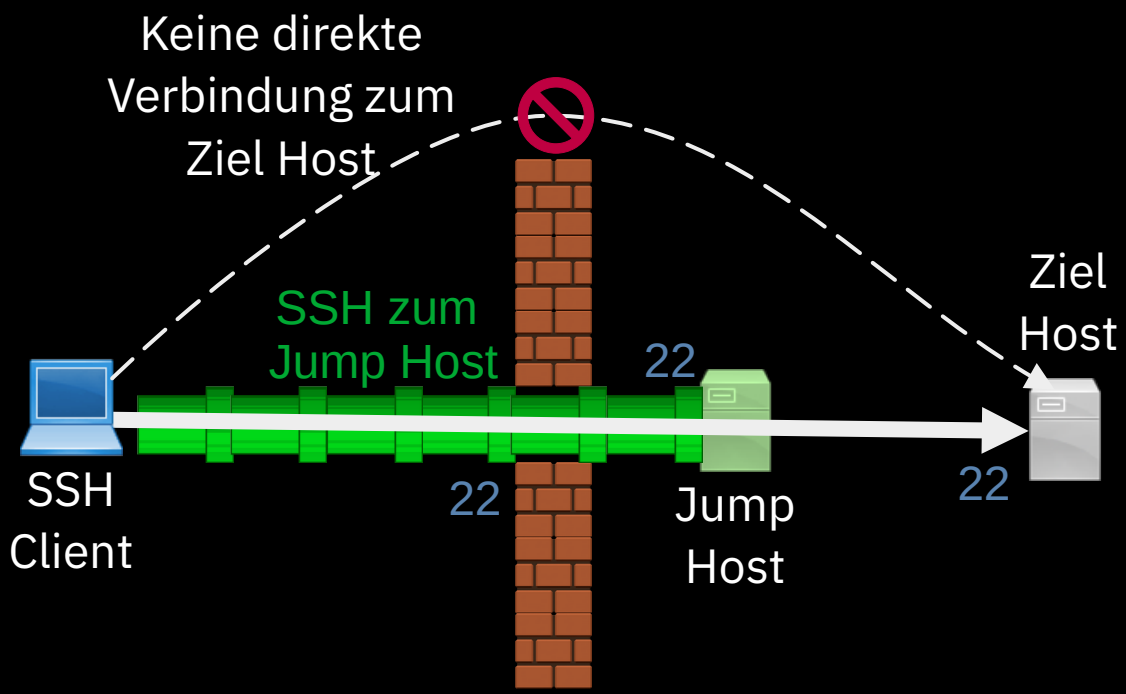
Tunnel zum Jump Host



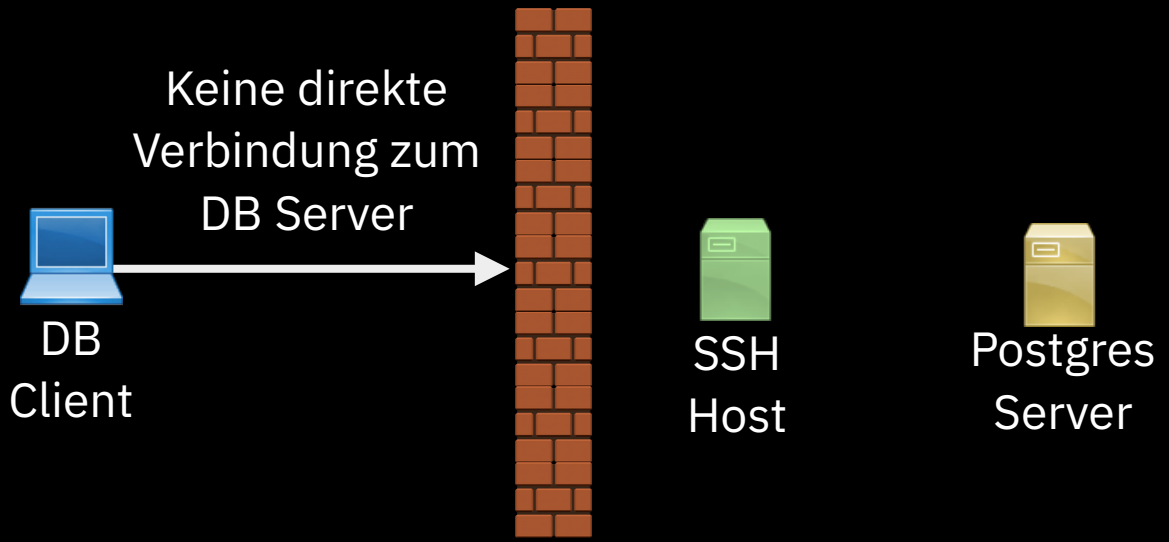
Tunnel über den Jump Host



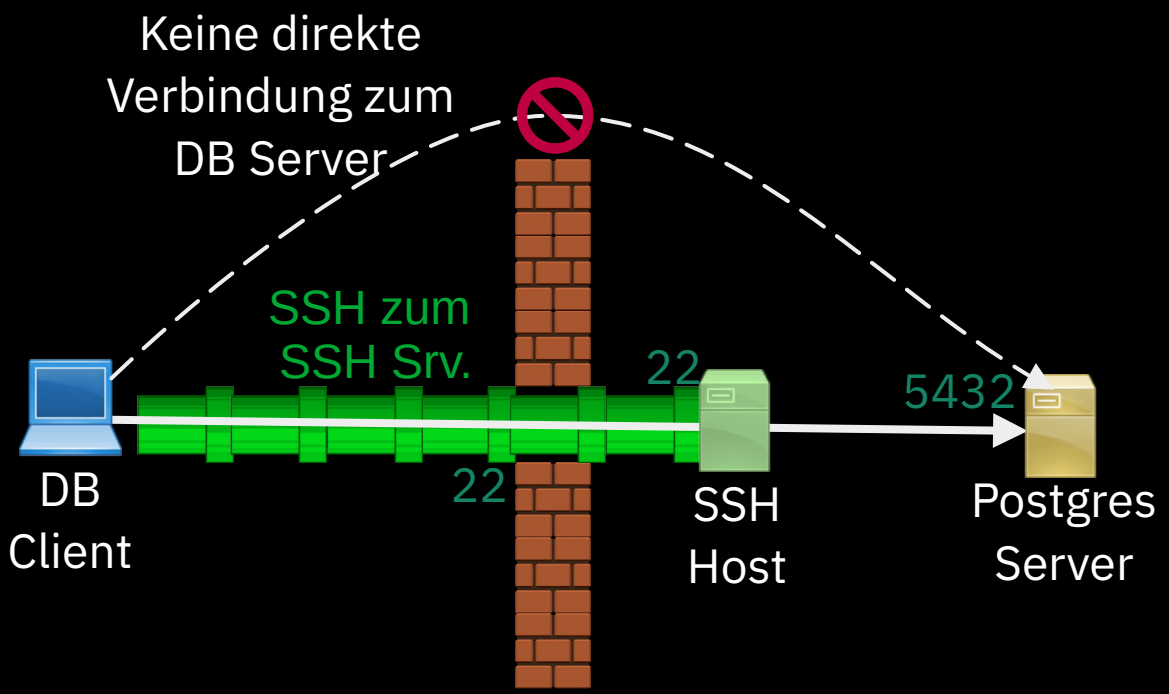
SSH only


Keine direkte
Verbindung zum
Ziel Host
SSH zum
Jump Host
22
22
22
SSH
Client
Jump
Host
Ziel
Host

Ziel ist kein SSH Host?



„Local“ Forwarding



Local Forwarding manuell

```
ssh -L \
    local_port:
    destination_server:
    destination_port \
user@ssh_server
```

Local Forwarding manuell

```
ssh -L \
  15432:postgres.example.com:5432 \
  gulasch@ssh.example.com
```

Local Forwarding mit ~/.ssh/config

```
Host demo
    HostName ssh.example.com
    User gulasch
    IdentityFile ~/.ssh/demo.ed25519
    LocalForward 15432 postgres.example.com:5432
```

Multiple Local Forwardings manuell

```
ssh -L \
    15432:postgres.example.com:5432 \
    -L 8080:localhost:80 \
    gulasch@ssh.example.com
```

Multiple Local Forwardings mit ~/.ssh/config

```
Host demo
    HostName ssh.example.com
    User gulasch
    IdentityFile ~/.ssh/demo.ed25519
    LocalForward 15432 postgres.example.com:5432
    LocalForward 8080 localhost:80
```

DEMO

Localhost ist wer?

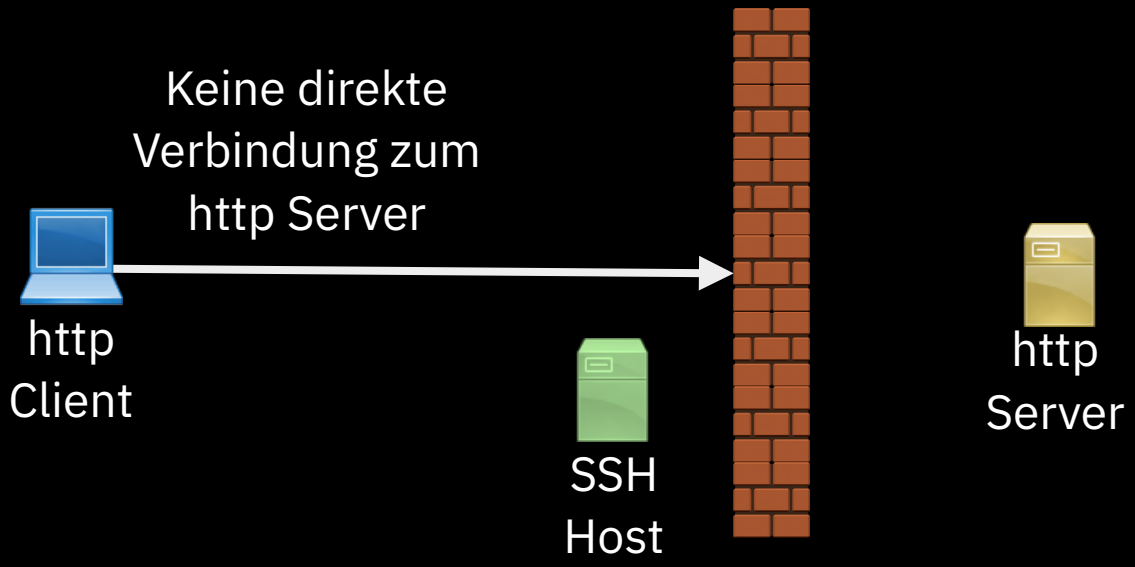

```
Host demo
    HostName ssh.example.com
    User gulasch
    IdentityFile ~/.ssh/demo.ed25519
    LocalForward 15432 postgres.example.com:5432
    LocalForward 8080 localhost:80
```

Auflösung: Localhost ist wer?

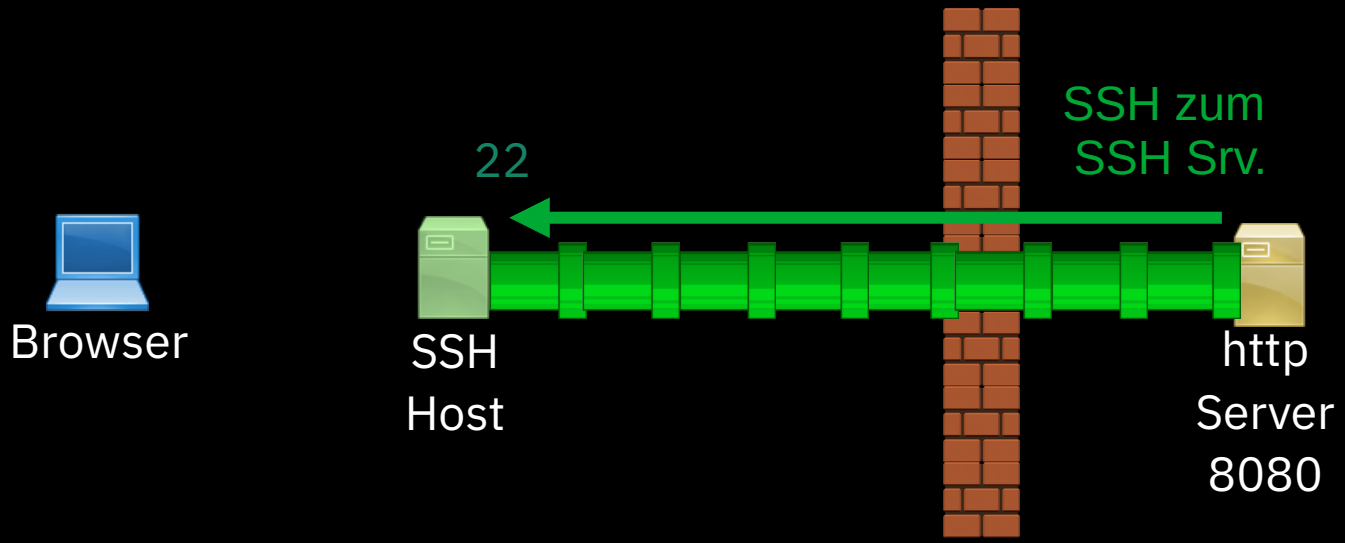
```
Host demo
    HostName ssh.example.com
    User gulasch
    IdentityFile ~/.ssh/demo.ed25519
    LocalForward 15432 postgres.example.com:5432
    LocalForward 8080 localhost:80
```

Remote Forwarding

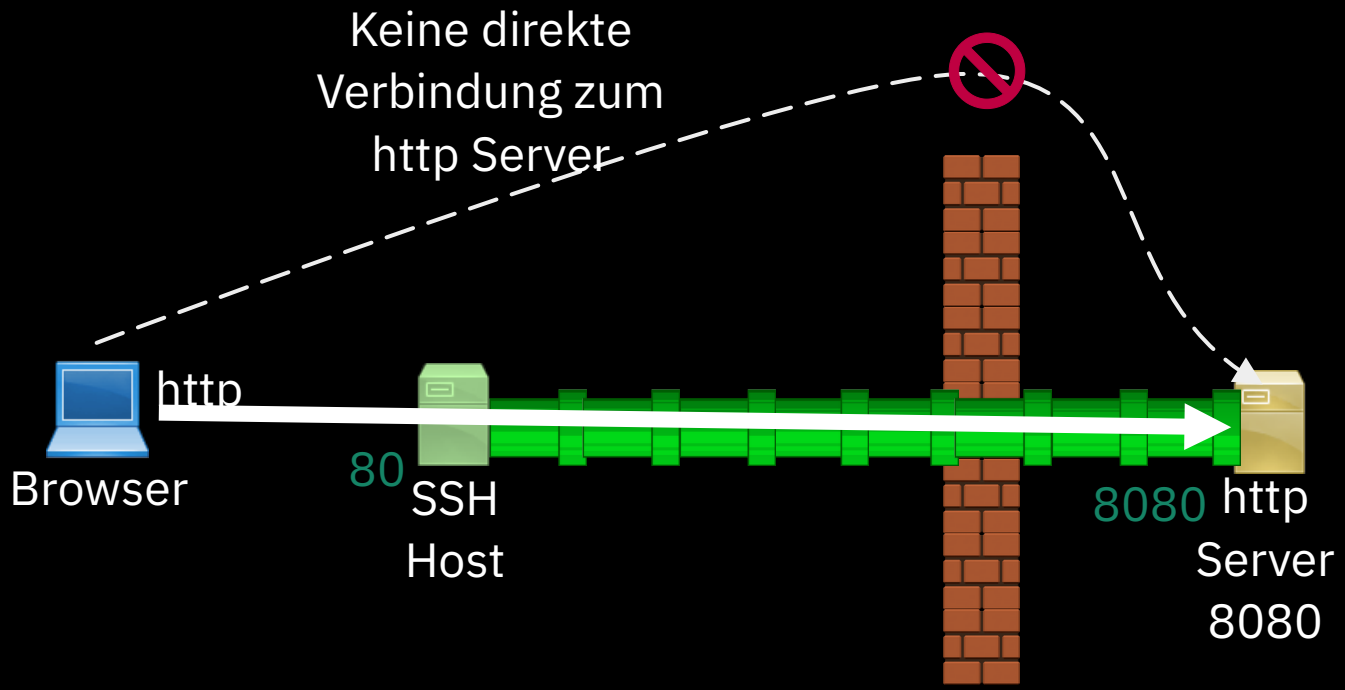
Ziel nicht erreichbar, SSH schon



Remote Port - SSH



Remote Port Forwarding



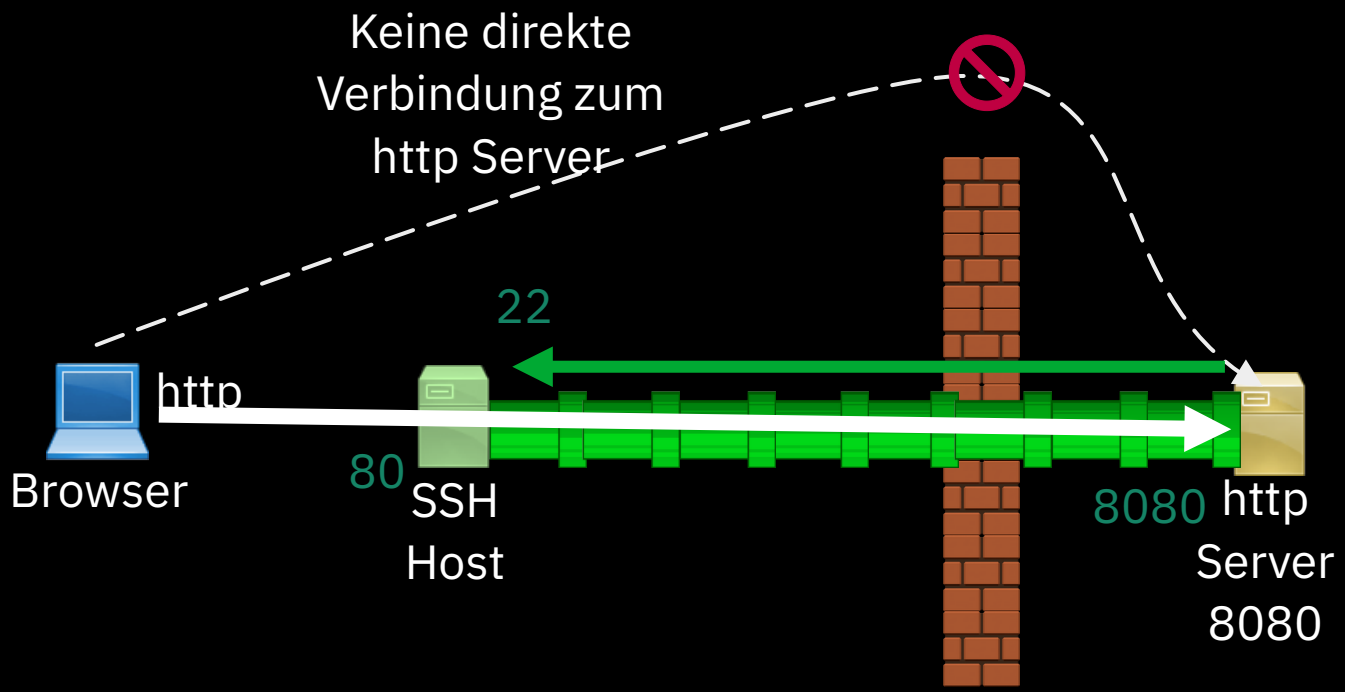
Remote Forwarding manuell

```
ssh -R \
    remote_port:
    destination_server:
    destination_port \
user@ssh_server
```

Remote Forwarding manuell

```
ssh -R 8081:localhost:8080 \
    gulasch@ssh.example.com
```

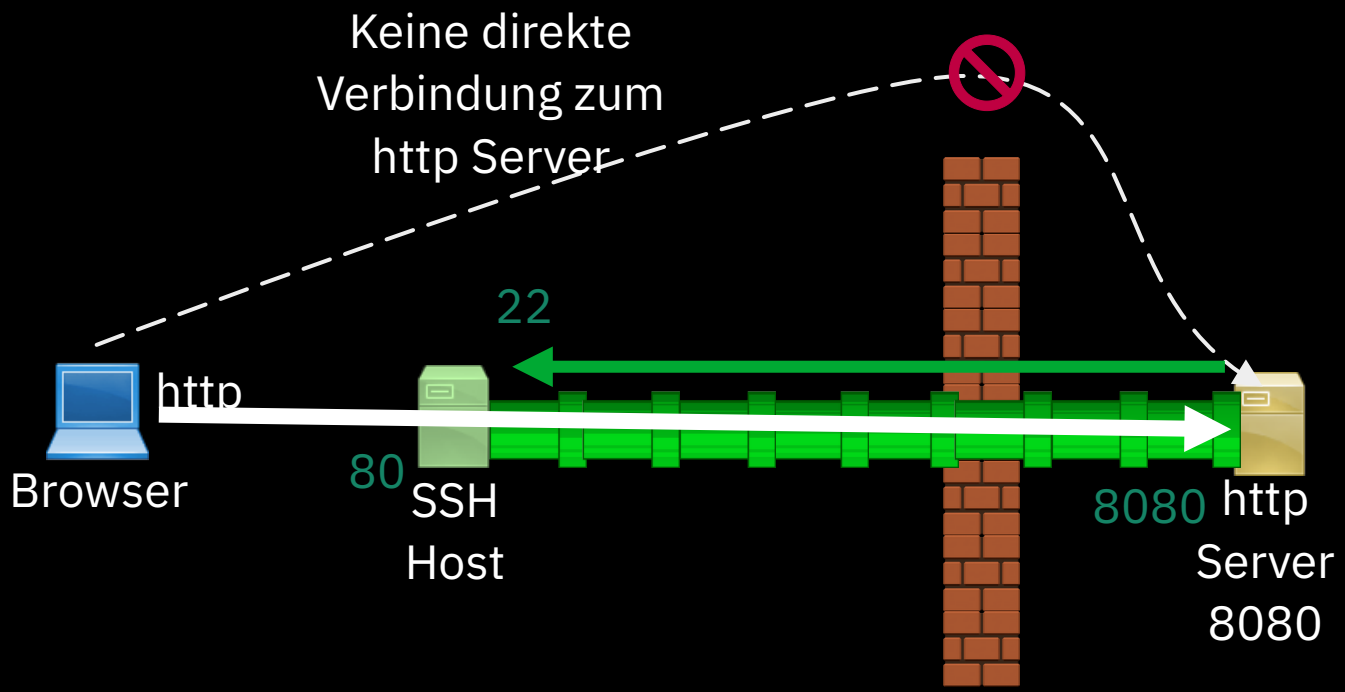
Remote Port Forwarding



Remote Forwarding mit ~/.ssh/config

```
Host demo
    HostName ssh.example.com
    User gulasch
    IdentityFile ~/.ssh/demo.ed25519
    RemoteForward 8081 localhost:8080
```

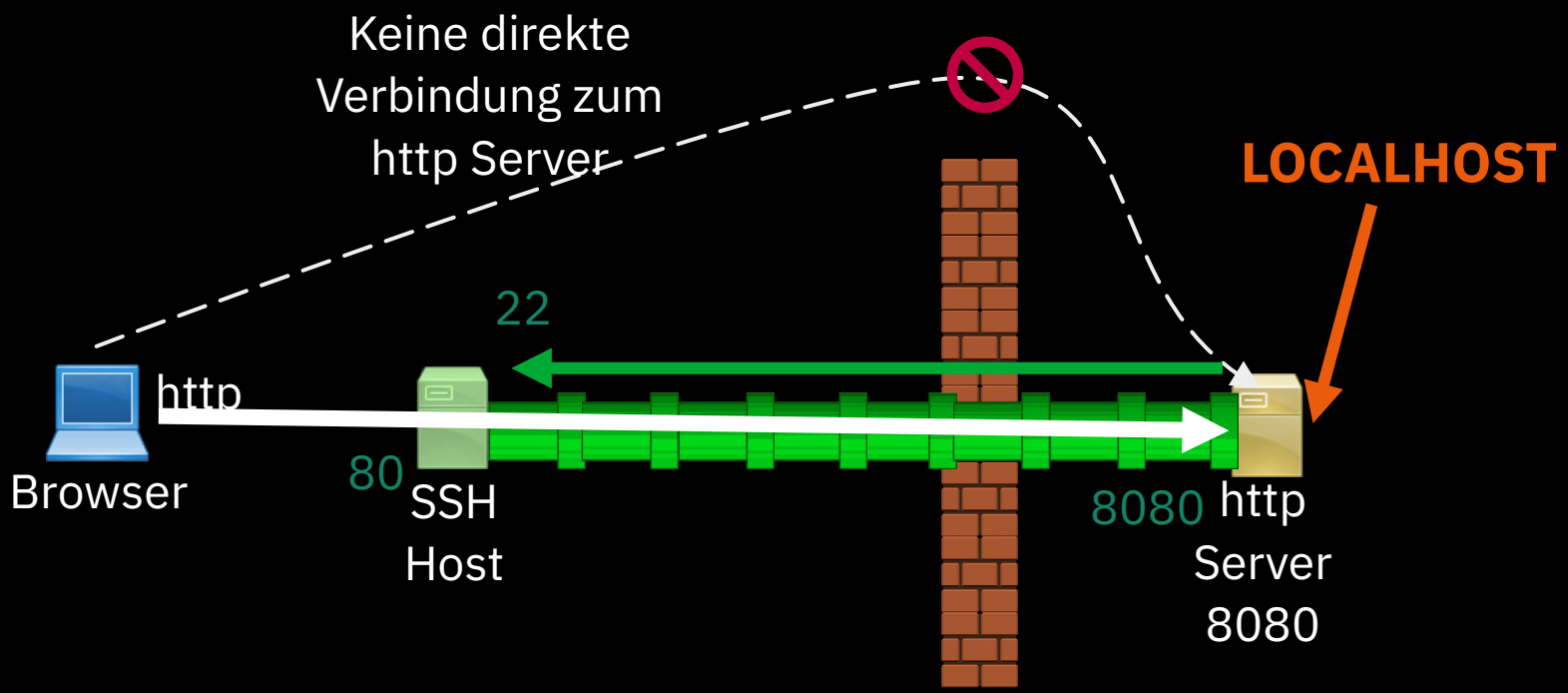
Remote Port Forwarding



Localhost ist wer?


```
Host demo
    HostName ssh.example.com
    User gulasch
    IdentityFile ~/.ssh/demo.ed25519
    RemoteForward 80 localhost:8080
```

Auflösung localhost



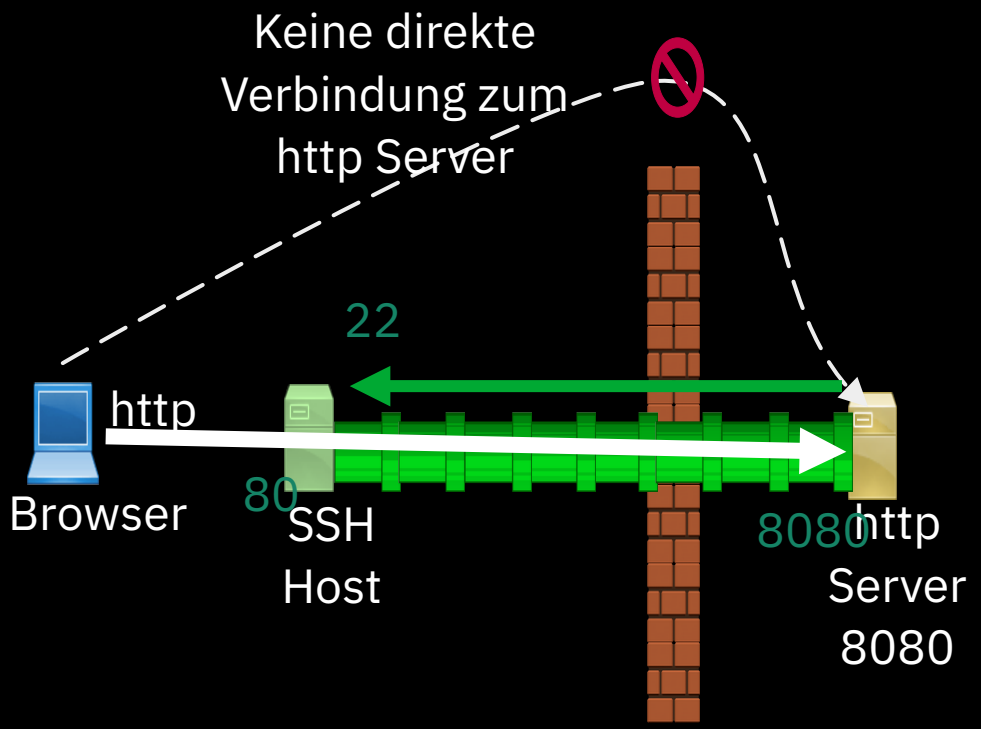
Local vs. Remote

- Immer aus Sicht des SSH Clients
  - SSH Client: „Du musst du die Dinge auch aus meiner Perspektive sehen.“
- **Local**: Der Port ist beim SSH Client
- **Remote**: Der Port ist beim SSH Ziel

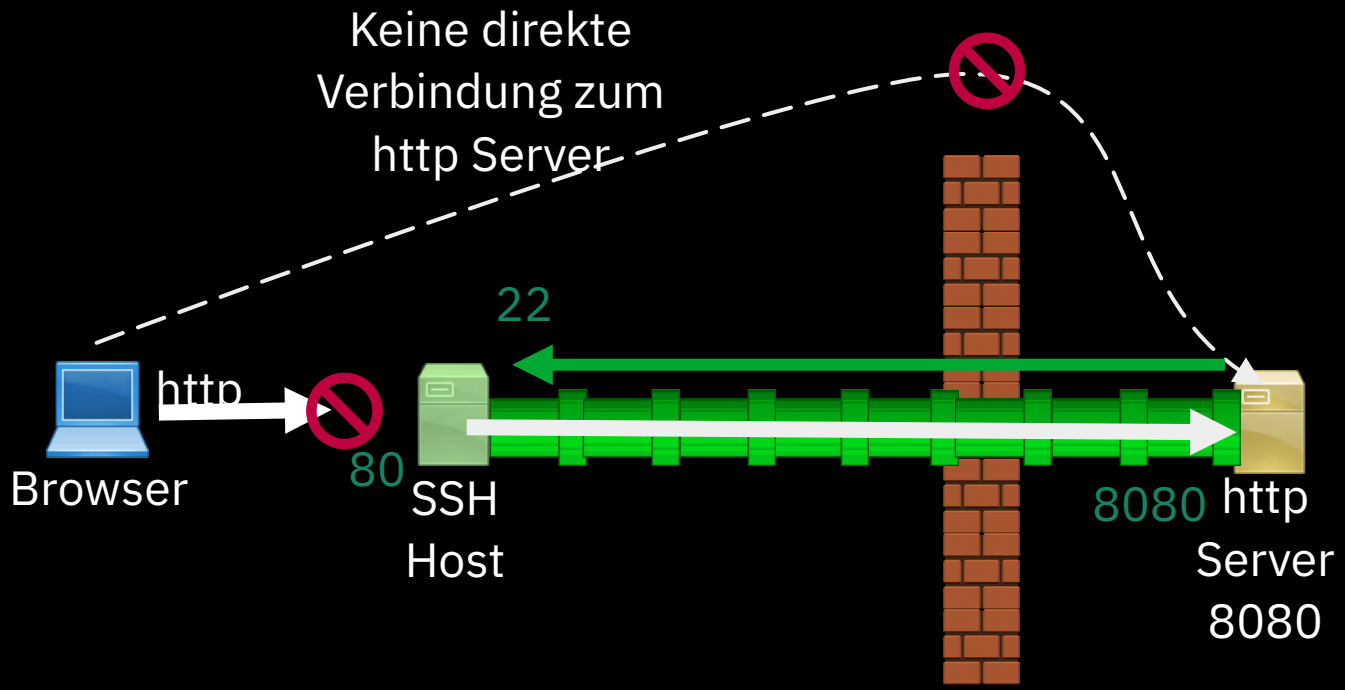
Beichte: Nicht per default

- „By default, sshd(8) binds remote port forwardings to the loopback address (only).“

- „GatewayPorts“ notwendig. Siehe „man 7 sshd_config“



Default remote port forwarding



Caveat Emptor !

- Port Forwarding kann Sicherheitsprobleme schaffen!
- Server Settings schärfen!
  - GatewayPorts
  - AllowTCPForwarding
- Firewallregeln: wer darf, ...

Dynamic Forwarding

(poor persons VPN)

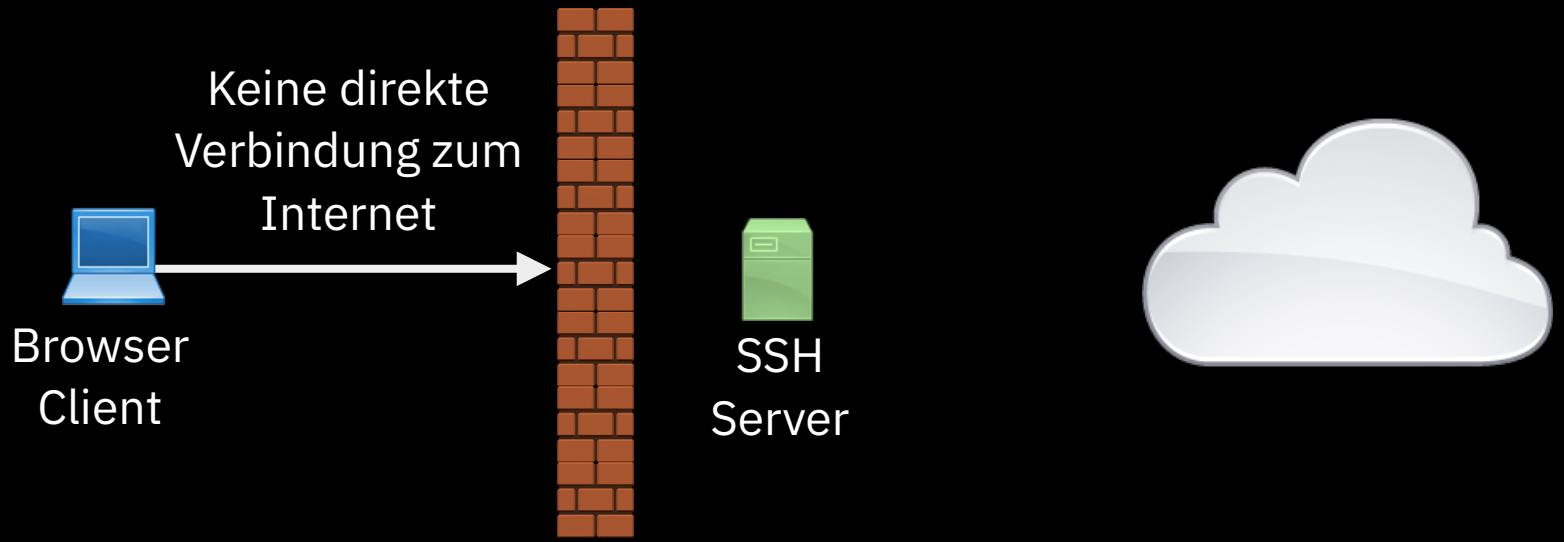
Sponsored by BlahajVPN

https://www.reddit.com/r/BLAHAJ/comments/1e42h5u/haj_on_the_computer_he_doesnt_know_how_to_turn_it/#lightbox

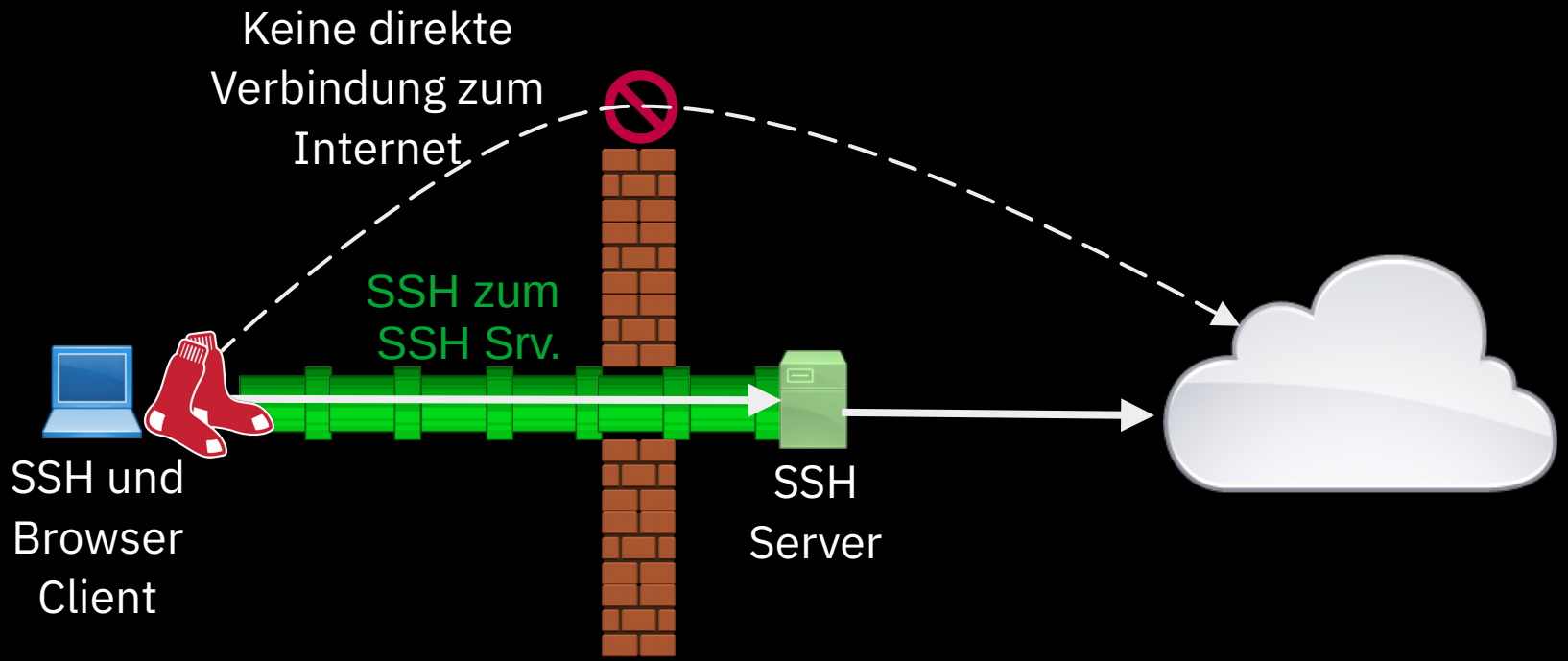
Dynamic Port Forwarding

- Erstellt einen SOCKS-Proxy, der den Netzwerkverkehr über einen SSH-Tunnel weiter bzw. „ins Internet“ leitet.
- Applikation muss SOCKS Proxies unterstützen
- Quasi ein VPN

Dynamic Port Forwarding – Warum?



Dynamic Port Forwarding



Dynamic Forwarding manuell

```
ssh -D  local_port \
    user@ssh_server
```

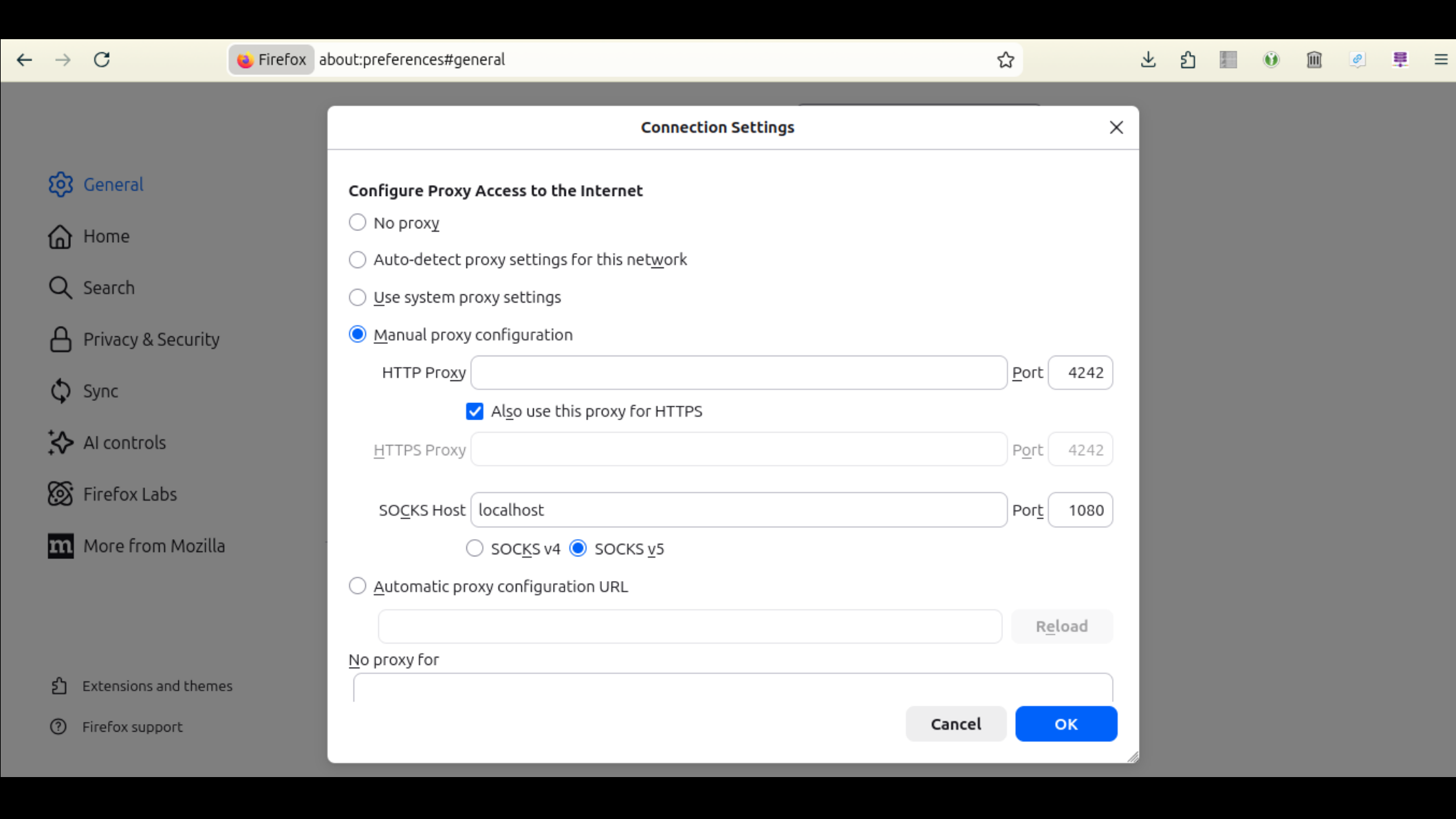
Dynamic Forwarding manuell

```
ssh -D  1080 \
    gulasch@ssh.example.com
```

DEMO

Wir tunneln nach Stockholm

```
ssh -N -D 1080 \
    gulasch-vpnjantit.com@
    se1.vpnjantit.com
```


Firefox
about:preferences#general
General
Home
Search
Privacy & Security
Sync
AI controls
Firefox Labs
More from Mozilla
Extensions and themes
Firefox support
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
Port
4242
Also use this proxy for HTTPS
HTTPS Proxy
Port
4242
SOCKS Host
localhost
Port
1080
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Cancel
OK

whatismyipaddress.com

WhatIs MyIPAddress .com

Enter Keywords or IP Address...

Search

ABOUT PRESS BOOK PODCAST CONTACT

MY IP | IP LOOKUP | HIDE MY IP | VPNS ▾ | TOOLS ▾ | LEARN ▾

My IP Address is:

IPv4: ? **193.148.59.245**

IPv6: ? **Not detected**

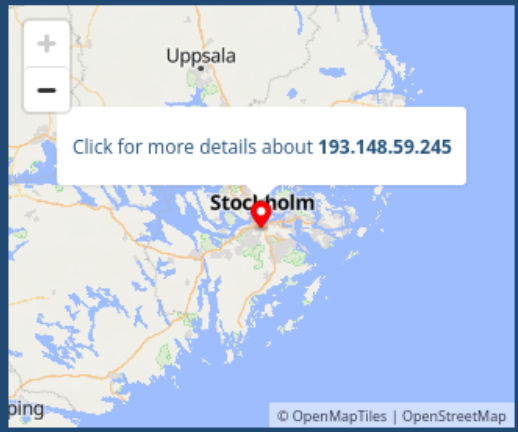
My IP Information:

ISP:	Baykov Ilya Sergeevich
Services:	VPN Server
City:	Stockholm
Region:	Stockholms lan
Country:	Sweden

Looks like you're using a VPN!

RATE YOUR VPN

Show Complete IP Details



Location not accurate?

Update My IP Location

Ende ???

„Danke“, 9er ….

9er
@9er@chaos.social

@leyrer erzählst du morgen auch was zu poor man's wireguard? (ssh -o tunnel=ethernet)

05 Jun 2026, 18:42 ·

https://chaos.social/@9er/116698497378781733

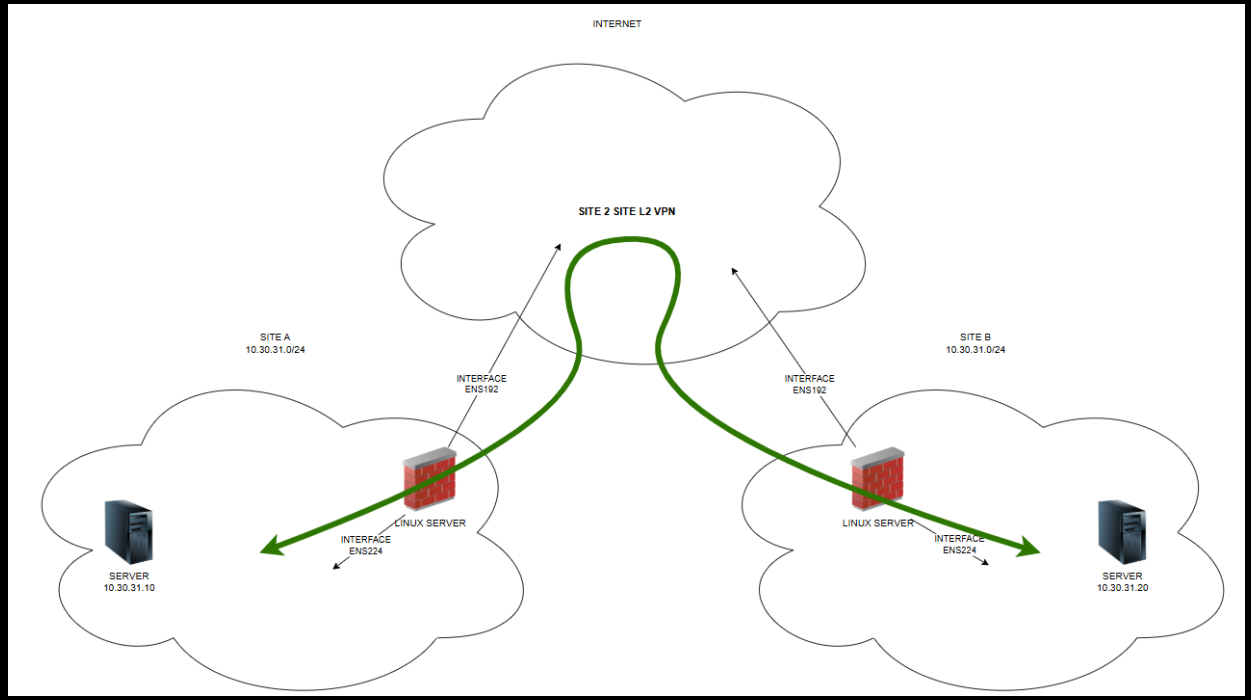
Layer 2 Tunnel mit OpenSSH

```
ssh -f -o Tunnel=ethernet \
   -o TunnelDevice=0:0 \
   -w 0:0 \
   root@SSH_SERVER
```

sshd_conf

- PermitRootLogin yes
- PermitTunnel yes

Ondrej Žilinec



https://www.cievo.sk/2025/01/17/easy-layer-2-site-to-site-vpn-2/comment-page-1/

Fragen ?

- Martin Leyrer
- https://martin.leyrer.priv.at
- leyrer@23.social

Solange man selbst redet, erfährt man nichts.

– Marie Freifrau Ebner von Eschenbach, österreichische Schriftstellerin

Quellen

- Mario pipe.png: https://en.wikipedia.org/wiki/File:Mario_pipe.png
- Super Mario Bros. – Overworld Block.svg: https://commons.wikimedia.org/wiki/File:Super_Mario_Bros._%E2%80%93_Overworld_Block.svg
- RedSoxPrimary HangingSocks.svg: https://en.wikipedia.org/wiki/File:RedSoxPrimary_HangingSocks.svg
- CISCO Network Topology Icons: https://www.cisco.com/c/en/us/about/brand-center/network-topology-icons.html