SSH-Tunnel

Ingo Blechschmidt
<iblech@web.de>

LUGA

8. Juni 2005

Problem

- Keine Möglichkeit der Verbindungsaufnahme zu Computern hinter einem NAT-Gateway für außenstehende Computer
- Err, keine NAT-Gateways bei IPv6
- Problem gelöst, vielen Dank für die Aufmerksamkeit!

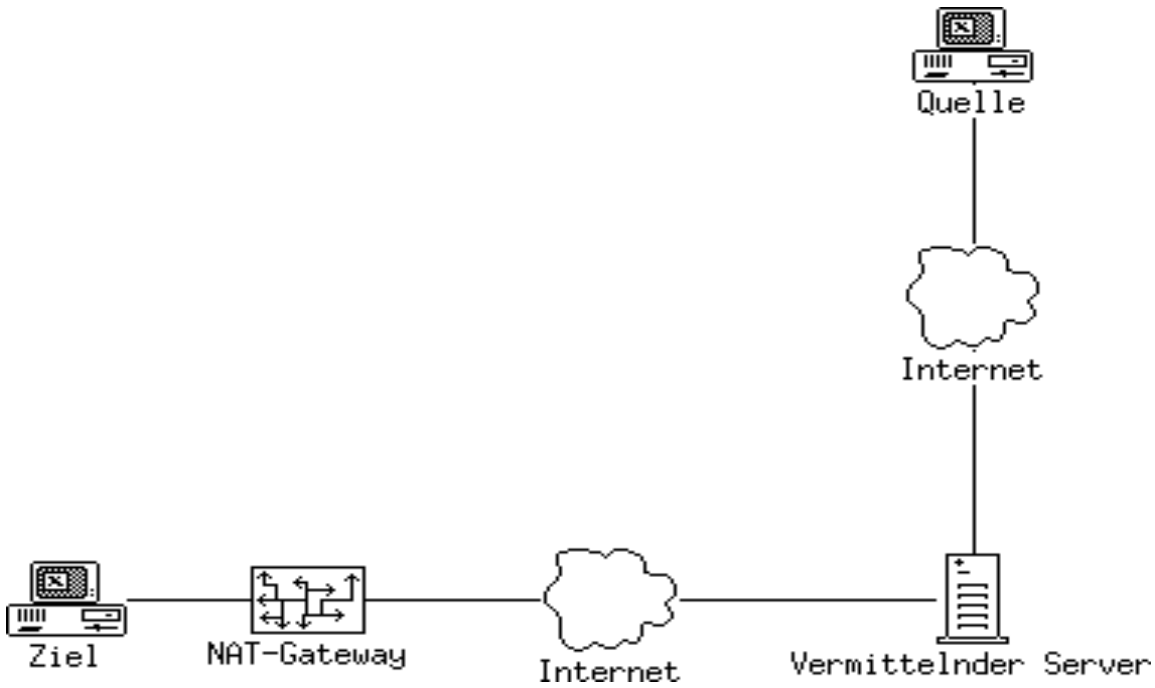
Problem

- Keine Möglichkeit der Verbindungsaufnahme zu Computern hinter einem NAT-Gateway für außenstehende Computer
- Err, keine NAT-Gateways bei IPv6
- Problem gelöst, vielen Dank für die Aufmerksamkeit!

Inhalt

Lösungsidee

- Bei IPv4: Keine direkte Ansprechmöglichkeit von Computern hinter einem NAT-Gateway wegen Fehlen von öffentlichen IP-Adressen
- Lösung: SSH-Tunnel



Init-Skript

```
#!/bin/sh

case "$1" in
  start)
    echo -n "Establishing SSH tunnels..." >&2
    su tunnel -c '/home/tunnel/tunnel.sh 20000' &
    su tunnel -c '/home/tunnel/tunnel.sh 20001' &
    su tunnel -c '/home/tunnel/tunnel.sh 20002' &
    echo "done." >&2;;
  stop)
    [...];;
  *)
    [...];;
esac
```

Init-Skript

```
#!/bin/sh

case "$1" in
  start)
    [...] ;;
  stop)
    echo -n "Stopping SSH tunnels..." >&2
    killall tunnel.sh          # hacky
    sleep 2
    killall -9 tunnel.sh       # hacky
    echo "done." >&2;;
  *)
    [...] ;;
esac
```

Init-Skript

```
#!/bin/sh

case "$1" in
  start)
    [...] ;;
  stop)
    [...] ;;
  *)
    echo "Usage: $0 start|stop" >&2
    exit 1;;
esac
```

Konfiguration von SSH

- Keine Möglichkeit von Passworteingaben $\Rightarrow$ SSH-Schlüssel zur Authentifizierung
- Hinzufügen des neuen Schlüssels zur Liste erlaubter Keys auf dem vermittelnden Server

Konfiguration von SSH

Auf dem Rechner hinter dem NAT-Gateway

```
tunnel@hinter-nat $ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/tunnel/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/tunnel/.ssh/id_dsa.
Your public key has been saved in /home/tunnel/.ssh/id_dsa.pub.
The key fingerprint is:
45:ab:b7:8c:b6:b3:4b:76:3b:20:93:78:28:0c:61:25 tunnel@hinter-nat
```

Wichtig: Keine Passphrase!

Konfiguration von SSH

Auf dem vermittelnden Server

```
tunnel@verm-server $ cat >> ~/.ssh/authorized_keys
command="/home/tunnel/sleep.sh",
  no-pty,
  no-X11-forwarding,
  no-agent-forwarding
  [Inhalt von hinter-nat:~tunnel/.ssh/id_dsa.pub]
```

- `command="[...]"`:
  Nutzung des Accounts **nur** für's Tunneln, **kein** Shell-Zugriff
- `no-pty`:
  Keine Alloziierung von Pseudo Terminals (Ressourcenschonung)
- `no-X11-forwarding`, `no-agent-forwarding`:
  Erneut: Nutzung ausschließlich für's Tunneln

sleep.sh

- Verhindern von möglichen Problemen bei Nichtbenutzung des Tunnels
- Alle fünf Minuten Ausgabe des aktuellen Datums ⇒
- SSH-Verbindung immer aktiv

verm-server:/home/tunnel/sleep.sh

```
echo -e "This account may only be used for
  port forwarding.\r"

while :; do
  sleep 300
  echo -e "`date`: Still alive.\r"
done
```

Kernskript

hinter-nat:/home/tunnel/tunnel.sh

```
#!/bin/sh

[ "$1" ] || {
  echo "Usage: $0 port"
  exit 1
}

while :; do
  ssh -T -R $1:localhost:22 \
    tunnel@verm-server '/home/tunnel/sleep.sh'
  sleep 30
done
```

Kernskript

- `ssh -T`:
  „Danke, aber wir brauchen kein Pseudo Terminal.“
- `ssh -R $1:localhost:22`:
  Tunnel `verm-server:$1` → `localhost:22`
- `sleep 30`:
  Kein Flooding des Netzes, Schonung des Prozessors (ansonsten evtl. ständiges Forken!)

Aktive Kontrolle

hinter-nat:/home/tunnel/tunnel-check.sh

```
#!/bin/sh

nc -z -w 20 verm-server 20000 || {
  sleep 10
  nc -z -w 20 verm-server 20000 || {
    killall ssh            # hacky!
    sleep 2
    killall -9 ssh         # hacky!
  }
}
```

Start von `tunnel-check.sh` per Cron alle fünf Minuten

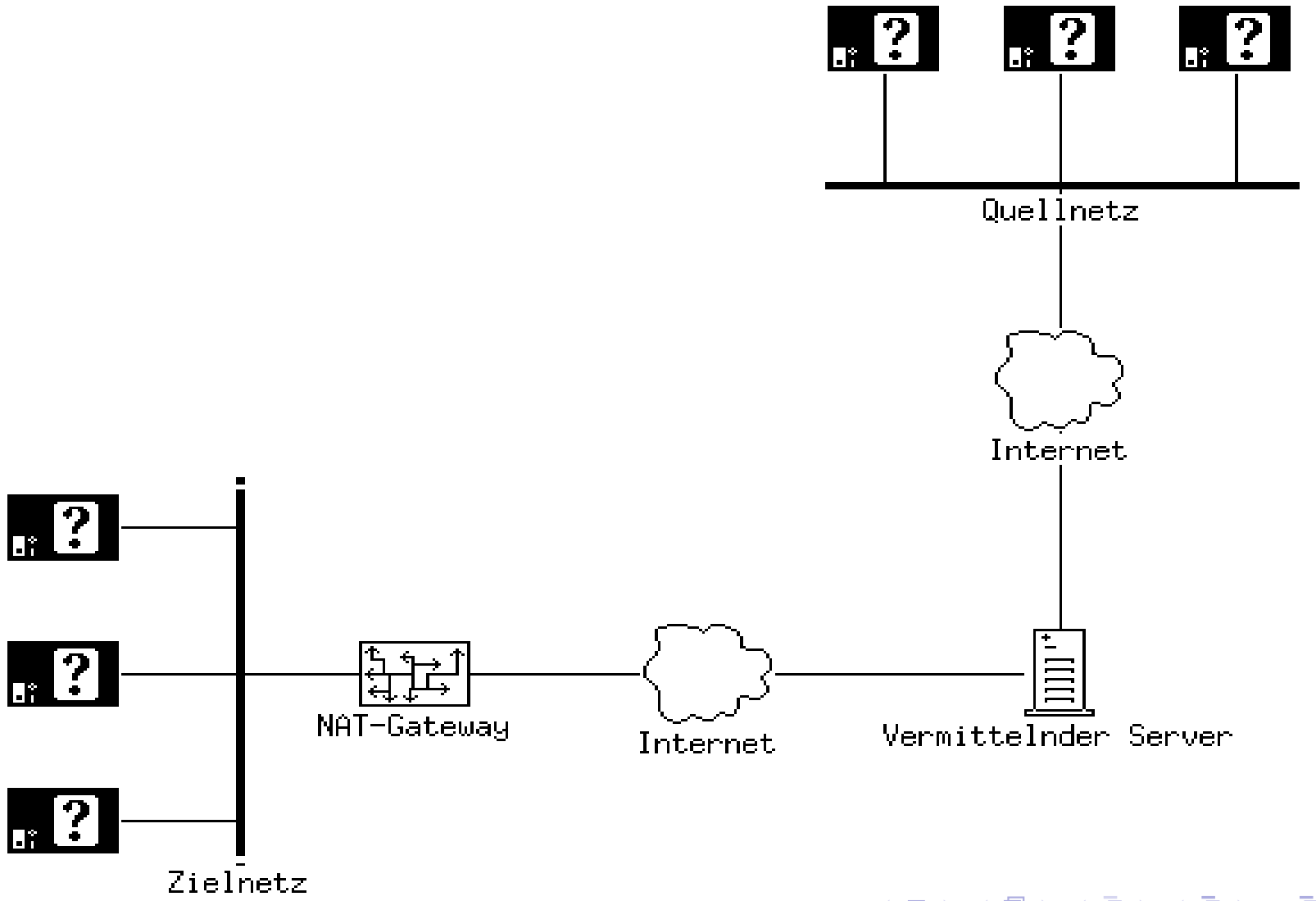
Problem und Lösungsidee

- Weiterleitung nur eines Ports ungenügend
- Wunsch nach **transparenter** Weiterleitung ganzer Netze
- Lösung: Point-to-Point Protocol Daemon (pppd)

Funktionsweise des pppd

- Bereitstellen von einfacher Byte-Übertragung durch beliebige untere Schicht („Modem“, „ISDN“, „Funk“, DNS (!), SSH)
- Bereitstellen von IP durch die pppd auf beiden Seiten
- Neues Interface: ppp$N$

Netzwerkdiagramm



Umsetzung

- Simpel: Ersetzen des SSH-Aufrufs in `tunnel.sh` durch `vpn-pppssh` von `http://www.tldp.org/HOWTO/ppp-ssh/configclient.html#AEN305`
- (Fertig.)

Umsetzung

- Simpel: Ersetzen des SSH-Aufrufs in `tunnel.sh` durch `vpn-pppssh` von `http://www.tldp.org/HOWTO/ppp-ssh/configclient.html#AEN305`
- (Fertig.)

Ausstehende Probleme

- Manuelle Eingriffe erforderlich zur Installation und (Um-)Konfigurierung der Tunnel
- (Kleiner) Overhead durch SSH und PPP (aber: Verschlüsselung!)
- Trotzdem: Stabile Tunnel mit Neuaufbau möglich

Einzige cleane Lösung

- Einmalige Installation von IPv6 auf den Routern
- `# modprobe ipv6`
- Fertig.

Ausstehende Probleme

- Manuelle Eingriffe erforderlich zur Installation und (Um-)Konfigurierung der Tunnel
- (Kleiner) Overhead durch SSH und PPP (aber: Verschlüsselung!)
- Trotzdem: Stabile Tunnel mit Neuaufbau möglich

Einzige cleane Lösung

- Einmalige Installation von IPv6 auf den Routern
- `# modprobe ipv6`
- Fertig.