Rückwärts-SSH-Tunnel für Management von Standort-Servern

Für einige Standorte haben wir keinen Zugriff auf den WAN-Router. Um bei versehentlichen Aussperren durch Änderungen der VLANs und Interfaces keinen Vor-Ort-Termin vereinbaren zu müssen, konfigurieren wir diese Server mit einem Rückwärts-SSH-Tunnel.

Hierfür wird ein neues Benutzerkonto „reverse" mit eingeschränkten Rechten angelegt.

Übersicht

Quellserver (Standortserver)	Zielserver	Port
BEZ-Server-Keller (Hypervisor)	Gateway Parad0x	26662
LAFP-Server-Geb2	Gateway Parad0x	26663
ALG-Server	Gateway Parad0x	26664

Verbindung aufbauen

Um zum Stanbdortserver zu kommen, geht man wie folgt vor:

- SSH-Key-Agent nutzen (Windows z. B. Pageant)
- SSH-Verbindung zum Zielserver des Reverse-Tunnels aufbauen (z. B. Gateway Parad0x für Management von BEZ-Server-Keller)
- SSH-Verbindung zu localhost mit Port des Reverse-Tunnels aufbauen (Port: Siehe Übersichtstabelle)

```
ssh -pPORTNUMMER localhost
```

Vorlage systemd-Dienstdatei

Port muss jeweils angepasst werden. Jeder Port kann nur einmal vergeben werden.

```
[Unit]
Description=AutoSSH reverse tunnel service for parad0x.ffmsl.de 26662 -> 22
After=network.target

[Service]
Environment="AUTOSSH_GATETIME=0"
ExecStart=/usr/bin/autossh -M 0 -o "ExitOnForwardFailure=yes" -o "ServerAliveInterval 30" -o
"ServerAliveCountMax 3" -NR 26662:127.0.0.1:22 reverse@parad0x.servers.freifunk-muensterland.de -i /root/.ssh
/id_rsa

[Install]
WantedBy=multi-user.target
```

Diese Datei in "/etc/systemd/system/autossh.service" ablegen. Mit "ssh-keygen" ein SSH-Schlüssel-Paar generieren und den öffentlichen Teil auf Parad0x ablegen.

Tunnel aktivieren:

```
chmod +x /etc/systemd/system/autossh.service
systemctl daemon-reload
systemctl start autossh.service
```

Und nun testen.

Konfiguration (Beispiel Parad0x)

Serverseitig (auf parad0x.servers.ffmsl.de) durchgeführt

```
useradd -d /home/reverse -m -N -s /bin/false reverse
```

Pro Standort wird ein SSH-Schlüssel generiert und der öffentliche Teil auf Parad0x in /home/reverse/.ssh/authorized_keys abgelegt.

Nach dem Konfigurieren, muss einmalig manuell eine Verbindung aufgebaut werden, damit der Hostkey bekannt wird. (Beim Erstlogin mit Yes bestätigen)