

Netzwerktechnik Dokumentation

Table of Contents

| | |
|---------------------------------|---|
| 1. Overview | 1 |
| 1.1. IP-Adressen: | 1 |
| 1.2. SSH | 1 |
| 2. Grundausrüstung | 2 |
| 2.1. SSH | 2 |
| 2.2. UFW | 3 |
| 2.3. Sudo | 3 |
| 2.4. Unattended upgrades: | 4 |
| 2.5. User | 4 |
| 3. Router | 5 |
| 4. DNS | 5 |
| 5. Webserver | 5 |
| 6. Lubuntu | 6 |
| 6.1. RDC | 6 |
| 6.2. SSH | 6 |
| 7. PFSense | 6 |
| 8. Proxy | 7 |

1. Overview

1.1. IP-Adressen:

Die IP-Adressen der CT und Vms:

- Router: 10.9.8.214
- Router außen: 10.9.8.250
- Pi-Hole: 10.9.8.209
- Nginx: 10.9.8.210
- Lubuntu: 10.9.8.211
- Pfsense: 10.9.8.212
- Proxy: 10.9.8.213

1.2. SSH

eine SSH Verbindung sollte jederzeit mit allen der Instanzen möglich sein:

Diese läuft bei allen Maschinen auf Port 2022

```
ssh root@<IP-ADDR> -p 2022

# Root access wird bald abgeschaltet, daher:

ssh user@<IP_ADDR> -p 2022
```

2. Grundausrüstung

Es wurden (bis auf die Lubuntu installation) Debian Container verwendet aus folgenden Gründen:

- Effizienter als Virtuelle Maschinen
- Bereits Erfahrung im Arbeiten mit Debian

Diese sind wie folgt hardwaretechnisch ausgestattet:

- 2 CPU threads (für Parallelisierung)
- 512 MB Arbeitsspeicher
- 1 - 2 Netzwerkinterfaces
- 8 GB Boot drive

Jeder der einzelnen virtuellen Maschinen / Container hat eine gewisse Grundausrüstung, und dazu gehören:

2.1. SSH

Eine SSH Verbindung kann jederzeit zu allen Containern und Vms aufgebaut werden. Dies ermöglicht schnelles und effizientes Arbeiten.

Installation von SSH:

```
sudo apt-get update
sudo apt install && apt upgrade -y

sudo apt install openssh-server
sudo systemctl enable ssh
sudo systemctl start ssh

vi /etc/ssh/sshd_config
```

Diese wird dann noch mit passenden Einstellungen konfiguriert.

SSH kann allerdings bereits mit der default Configuration funktionieren.

```
ssh <USERNAME>@<HOST>
```

```
# z.B:
```

```
ssh test@10.0.0.8 -p 2022
```



Derzeit werden die SSH Server auf Port 2022 umgelegt.

Um den Port umzulegen, muss dies auch in systemctl umconfiguriert werden:

```
nano /lib/systemd/system/ssh.socket
```

```
# Dort die folgende Line Abändern:
```

```
ListenStream=22 ①
```

① 22 mit neuem Port ersetzen!

Wenn dies nicht erledigt wird, startet der ssh Server oft nicht automatisch. Dieser läuft allerdings leider in keinen Fehler, sondern wird einfach als "loaded" angezeigt, was zur Verwirrung führen kann.

2.2. UFW

Alle Ports wurden mithilfe von UFW gesichert und abgedreht. Pings werden zukünftig ebenfalls ausgeschaltet.

Die benötigten Ports sind dann allerdings freigegeben, sodass z.B die SSH-Verbindungen funktionieren.

Diese können mit folgendem Befehl eingesehen werden:

Aufgrund der Komplexität der Firewall beim Router musste die Firewall dort aktuell deaktiviert werden. An einer Lösung wird gearbeitet.

```
sudo ufw status
```

```
# ports freigeben:
```

```
sudo ufw allow 22①
```

① Portnummer

2.3. Sudo

Da dies mit Debian nicht mehr vorinstalliert ist, wurde dies einfach auf die Container hinzugefügt.

Dies vereinfacht das zukünftige Anlegen und Arbeiten mit Benutzer.

```
apt install sudo
```

2.4. Unattended upgrades:

Unattended upgrades wurde installiert, dass der Server updates automatisch installiert.

Installieren:

```
sudo apt install unattended-upgrades apt-listchanges bsd-mailx
```

Configurieren:

```
sudo dpkg-reconfigure -plow unattended-upgrades
# dann auf "yes"

sudo vim /etc/apt/apt.conf.d/50unattended-upgrades

#Unkommentieren von folgenden Lines:

Unattended-Upgrade::Mail "mctom.spdo@gmail.com";

Unattended-Upgrade::Automatic-Reboot "true";

# -----

sudo vim /etc/apt/listchanges.conf

#Config:

email_address=mctom.spdo@gmail.com
```

Testen der Configuration:

```
sudo unattended-upgrades --dry-run
```

2.5. User

erstellen eines neuen Users:

```
sudo adduser user
```

hinzufügen zur Sudogruppe:

```
usermod -aG sudo user
```

3. Router

Am Router CT sind 2 Netzwerkkarten angebracht. Jeder der einen Netzwerkkarten befindet sich in einem Netzwerk.

Damit der Container zwischen diesen zwei Interfaces routet, muss dieser configure werden:

Dazu muss man einfach das folgende File editieren:

```
vi /etc/sysctl.conf

net.ipv4.ip_forward = 1 ①
echo 1 > /proc/sys/net/ipv4/ip_forward ②
reboot ③
```

- ① Diese Zeile auskommentieren
- ② Da Debian dies standardmäßig ausgeschaltet hat, müssen wir dies einschalten
- ③ Man könnte ebenfalls gewisse Teile reloaden, allerdings ist in diesem Fall ein reboot schneller, ale dies zu recherchieren.

4. DNS

Als DNS wurde PI-hole verwendet.

Zum Installieren wurde einfach der die offizielle Dokumentation verwendet:

[Installation von PI-hole](#)

Das Passwort für das Webinterface wurde ebenfalls auf das Standartpasswort geändert. Hierfür wurde folgender Befehl verwendet:

```
pihole -a -p
```

5. Webserver

Nginx wurde als Webserver verwendet. Derzeit ist dort allerdings nur die Standard webpage gehostet.

Eine eigene Seite hat derzeit keine Priorität und wird aktuell nach hinten verschoben.

6. Ubuntu

Eine VM mit Ubuntu Desktop wurde eingerichtet, und in das Netzwerk eingebunden. Zu dieser kann jederzeit eine SSH oder RDP Verbindung aufgebaut werden



Der Bildschirmschoner sollte deaktiviert werden.

6.1. RDP

Auf Ubuntu wurde eine RDP (Remote Desktop Connection) eingerichtet, sodass hier ebenfalls ein schnelles und einfaches Arbeiten möglich ist.

Hierfür wurde XRDP verwendet:

```
sudo apt install xrdp
```

Dies wurde ebenfalls konfiguriert und eingerichtet.

Die remote Verbindung kann dann einfach mit den folgenden Daten aufgebaut werden:

```
IP: 10.9.8.211  
Username: thelast  
Password: <PASSWORD>
```

6.2. SSH

Die SSH Verbindung wurde gleich wie bei allen anderen Maschinen eingerichtet.

7. PFSense

Da PFSense ein eigenes ISO benötigt, und dieses nicht einfach auf einem normalen Linux laufen kann, wurde dies beim Prof. Angefragt, da wir dies nicht selbst auf den Server hochladen dürfen.

Da das ISO bereits auf dem Server zur Verfügung steht, wurde bereits damit begonnen, dieses zu installieren und fertig zu machen. In der nächsten Stunde ist geplant, daran weiterzuarbeiten.

Installation:

Für die Installation von PFSense werden zwei Netzwerkkarten benötigt, denn eine wird für das normale Netzwerk verwendet und die andere Karte wird für ein internes Vlan verwendet.

vtnet0 → Netzwerkkarte für das externe Netzwerk

8. Proxy

Der Proxy CT wurde angelegt und vorbereitet, an einer Proxy installation wird aktuell noch gearbeitet.

Installations Schritte

```
sudo apt-get update  
  
sudo apt-get install squid
```

Konfiguration

```
sudo nano /etc/squid/squid.conf
```

Für mehr Information und Konfigurationen

<https://phoenixnap.com/kb/setup-install-squid-proxy-server-ubuntu>