

Netzwerktechnik

Mag. Ing. Thomas Höllerer

2021/22

HTL Krems

Felix Schneider

25.05.2022

Inhaltsverzeichnis:

1	Aufgabenstellung.....	3
1.1	Debian Expert Install aufsetzen.....	3
1.2	Debian Server Pakete installieren	3
2	Vorbereitungen	3
2.1	Debian Expert Install aufsetzen.....	3
3	Übungsdurchführung	4
3.1	Virtuelle Debian Maschine	4
3.2	Aptitude + Putty	11
3.3	wichtige Befehle zum Herausfinden von Informationen	14
3.4	Virtuelle Windows Maschine	17
3.5	Virtuelle Debian Maschine Kopie	20
3.6	Windows Internet.....	27
3.7	DHCP Server.....	28
3.8	Firewall	31
3.9	IPv6.....	35
3.10	Apache2.....	38
3.11	Samba.....	39
3.12	DNS-Server	42
4	Notizen	48
4.1	DNS.....	48
5	Abbildungsverzeichnis.....	49
6	Codeverzeichnis.....	51
7	Ergebnisse.....	52
8	Kommentar.....	52

1 Aufgabenstellung

1.1 Debian Expert Install aufsetzen

Wir legen eine neue virtuelle Maschine mithilfe der Software **VMWare Workstation Player** an und setzen darauf eine Debian Maschine ohne grafische Oberfläche auf. Dafür verwenden wir eine ISO-Datei mit Debian Version 11.0.0.

Wir benötigen einen root- und einen normalen Benutzeraccount.

1.2 Debian Server Pakete installieren

2 Vorbereitungen

2.1 Debian Expert Install aufsetzen

Die **ISO-Datei** kann man vom Internet herunterladen:

- 64-Bit-Version: <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-11.1.0-amd64-netinst.iso>
- 32-Bit-Version: <https://cdimage.debian.org/debian-cd/current/i386/iso-cd/debian-11.1.0-i386-netinst.iso>

Die App **VMWare Workstation 16 Pro Player** kann hier heruntergeladen werden:

- <https://www.vmware.com/go/getworkstation-win>

3 Übungsdurchführung

3.1 Virtuelle Debian Maschine

3.1.1 Virtuelle Maschine erstellen

Um eine virtuelle Maschine zu erstellen, öffnen Sie die App VMWare Workstation Player und drücken auf Player → File → New Virtual Maschine...

Anschließend wählen Sie in dem Fenster, das aufgegangen ist, „Installer disc image file (iso):“ aus und suchen nach der auf ihrem Computer installierten Debian 11 ISO-Datei. Wählen Sie diese aus und klicken Sie auf „Next→“.

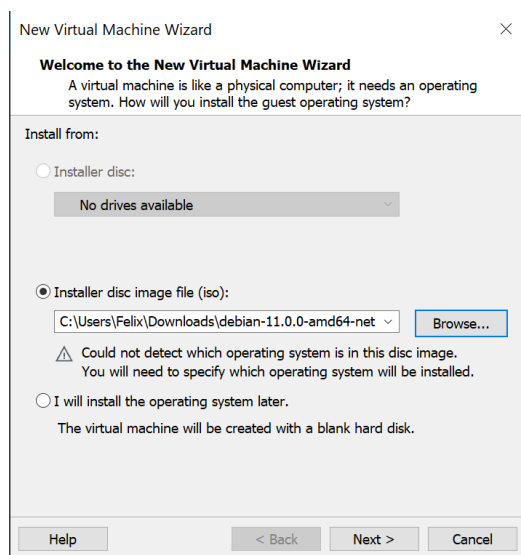


Abbildung 1: ISO Datei auswählen

Wählen Sie beim nächsten Fenster „Linux“ bei „Guest operating system“ und „Debian 10.x 64-bit“ unter „Version“ aus. Wenn Sie über einen 32-bit Rechner verfügen, wählen Sie statt „Debian 10.x 64-bit“ „Debian 10.x 32-bit“ aus. Klicken Sie auf Next→.

zusätzliche Informationen: Auch wenn Sie eine Debian 11 ISO File heruntergeladen haben und virtuell eingelegt haben, wählen wir hier Debian 10 aus, weil dies die letzte Version ist, die VMWare unterstützt (Stand 2021).

Beim nächsten Fenster geben Sie einen sinnvollen Namen der neuen virtuellen Maschine ein. Dieser wird nach Abschluss der Erstellung in der List in VMWare Workstation Player angezeigt. Außerdem wählen Sie den Speicherort der Installation. Beachten Sie, dass Sie ein Laufwerk mit genügend Speicherkapazität auswählen sollten!

Anschließend werden Sie aufgefordert, die Speicherkapazität der Virtuellen Maschine einzustellen. Es wird empfohlen mindestens die empfohlene Größe des Speichers einzuhalten. Wenn die empfohlene Größe also 20GB beträgt, sollten Sie keine 18GB verwenden, sondern mindestens 20GB, besser mehr als weniger. Beachten Sie hierbei, dass Sie nicht zu viel Kapazität freigeben, sondern nur maximal so viel wie auf dem vorhin eingestellten Laufwerk verfügbar ist. Die Kapazität wird nicht direkt von der Virtuellen Maschine verwendet, erst wenn der Speicherplatz benötigt wird.

Außerdem können Sie wählen, ob Sie diese Kapazität in einer einzigen Datei speichern möchten oder in mehreren kleineren Dateien speichern möchten. Das Teilen der virtuellen Disk hat den Vorteil,

dass die einzelnen Dateien kleiner sind, dadurch können Sie auch FAT32 als Speicherart verwenden. FAT32 hat nämlich eine Dateigrößenbegrenzung von 4GB.

3.1.2 Hardwareeinstellungen konfigurieren

Konfigurieren Sie die Hardwareeinstellungen folgendermaßen:

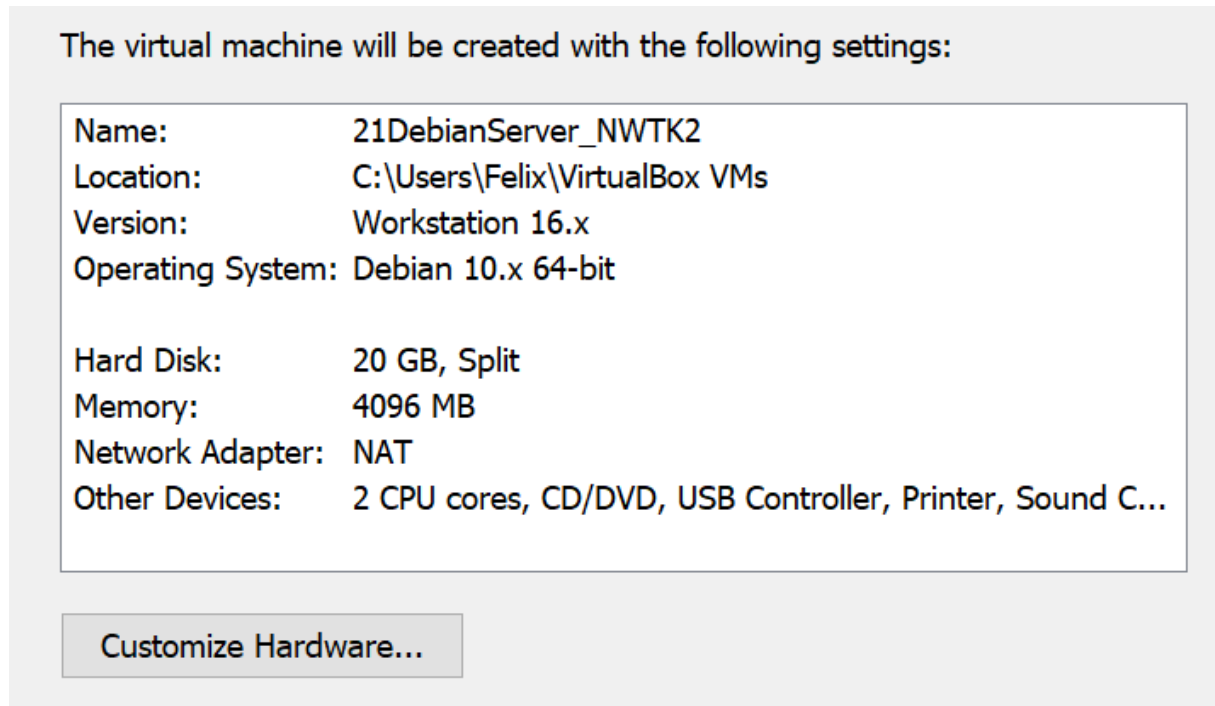


Abbildung 2: Hardwareeinstellungen

Wichtig sind hierbei folgende Einstellungen:

- der Arbeitsspeicher bzw. RAM → Sie müssen nicht 4GB wählen; mind. 2GB wird empfohlen
- der Netzwerkadapter: damit Sie ins Internet kommen benötigen Sie eine Netzwerkkarte mit NAT
- Wenn Sie eine bessere Performance wollen, können Sie (falls Ihr Computer das unterstützt) mehrere CPU-Kerne hinzufügen

zusätzliche Informationen: NAT – Network Address Translation – ersetzt die IP-Adresse der Virtuelle Maschine mit der IP-Adresse des Hosts. Somit kommen Sie ins Internet. Ein außenstehender PC kann nicht unterscheiden, ob der Internetzugriff vom Host oder der Virtuelle Maschine kommt (die IP-Adressen sind ja identisch). Über die Portnummer kann der Host allerdings das Paket wieder zur Virtuellen Maschine zurückleiten.

3.1.3 Expert Install starten

Starten Sie die gerade eben neu erstellte Virtuelle Maschine. Die Virtuelle Maschine lädt nun Daten der ISO Datei, dies kann ca. eine Minute dauern. Wenn die Daten fertig geladen sind, erscheint ein Fenster mit verschiedenen Optionen. Wählen Sie „Advanced options“ und anschließend „Expert Install“ aus.

Die Installation wurde jetzt gestartet. Das Protokoll führt Sie nun durch die einzelnen Schritte, die Sie durchführen müssen, um die Installation zu vollenden.

3.1.4 Sprache und Tastatur auswählen

Als erstes wählen Sie die richtige Sprache aus. **Mit den Pfeiltasten können Sie navigieren, mit Enter wählen Sie dann die Option aus.** Wählen Sie „Choose language“ aus und suchen Sie nach Ihrer Sprache (wahrscheinlich German, ansonsten würden Sie dieses Protokoll nicht lesen 😊). Anschließend werden Sie nach dem Land und dem Gebietsschema gefragt, hier wählen Sie bitte jeweils das Land oder Gebiet aus, in dem Sie wohnen.

zusätzliche Information: UTF-8, die Kodierung für Unicode Zeichen, ist in allen deutschsprachigen Ländern gleich. Jedoch variiert die Kennung.

Nachdem die Sprache konfiguriert wurde, werden Sie jetzt „Tastatur konfigurieren“ auswählen und das Layout Ihrer Tastatur heraussuchen.

3.1.5 Installer-Komponenten vom Installationsmedium laden

Laden Sie das Installationsmedium, das erkannt wurde, und binden Sie dieses ohne zusätzliche Komponenten ein.



Abbildung 3: Medium einbinden/laden

3.1.6 Netzwerk einrichten

Wieder im Hauptmenü zurück, klicken Sie auf „Netzwerk-Hardware erkennen“. Wenn keine Fehlermeldung auftritt, wurde die Netzwerk-Hardware erfolgreich erkannt und Sie können „Netzwerk einrichten“ aufrufen.

Sie wollen das Netzwerk automatisch einrichten, für die Wartezeit und den Rechnernamen am besten die voreingestellten Einträge so lassen, wie sie sind, und als Domain-Name **<IhrenNamen>.local** eintragen.



Abbildung 4: Name der Domain eingeben

zusätzliche Information: Der Domain-Name endet mit .local, weil Sie ein privates Netzwerk aufbauen wollen und .local auf den Rechner selbst verweist.

3.1.7 Benutzer und Passwörter einrichten

Als nächstes richten Sie Benutzer mit zugehörigem Passwort ein. Es wird empfohlen Shadow-Passwörter zu verwenden, eine Methode, die die verschlüsselten Passwörter in der /etc/shadow-Datei speichert und nicht, wie früher, in der /etc/passwd-Datei.

zusätzliche Information: Das war nämlich eine Sicherheitslücke, wenn Programme einen Benutzernamen oder bestimmte Gruppen herausfinden wollten. Diese Informationen stehen nämlich ebenfalls verschlüsselt in der /etc/passwd-Datei. Das bedeutet, wenn ein Programm die entschlüsselte /etc/passwd-Datei ausgelesen hat, stand das Passwort direkt dabei (unverschlüsselt!). Bei Shadow-Passwörtern steht das Passwort dann in /etc/shadow.

```
/etc/passwd
Informationen zu den Benutzerkonten

/etc/shadow
verschlüsselte Informationen zu den Benutzerkonten

/etc/shadow-
Sicherungskopie von /etc/shadow

Beachten Sie, dass diese Datei von Werkzeugen der Shadow-Werkzeugsammlung verwendet
wird, aber nicht von allen sonstigen Programmen zur Benutzer- und Passwortverwaltung.
```

Abbildung 5: Shadow-Passwörter

Erlauben Sie die Anmeldung als root, Sie können auf der Virtuellen Maschine sowieso nicht viel kaputt machen. Geben Sie ein sicheres Root-Passwort ein und bestätigen Sie dieses im nächsten Schritt. Erstellen Sie auch mindestens ein normales Benutzerkonto, für den Fall, dass Sie sich mit dem Root-Account nicht einloggen können.

Es ist wichtig, dass man neben dem root-Account zusätzlich auch noch ein Benutzerkonto anlegt, für den Fall, wenn man mit dem root-Account nicht einsteigen kann, hat man immer noch die Möglichkeit mit dem Benutzerkonto einzusteigen.

3.1.8 Uhr einstellen

Im nächsten Schritt stellen Sie die Uhr ein. Verwenden Sie kein NTP (Network Time Protocol), weil der Host die Uhrzeit bereits richtig eingestellt hat. Anschließend müssen Sie nur noch Ihre Zeitzone auswählen.

3.1.9 Festplatte partitionieren

Der nächste große Schritt ist die Festplattenpartitionierung. Klicken Sie hierzu vorerst auf „Festplatten erkennen“, wodurch das Installationsprogramm nach Festplatten sucht. Anschließend wählen Sie „Festplatten partitionieren“ und „manuell“ aus.

Nun sollten Sie ungefähr so eine Auswahl sehen:

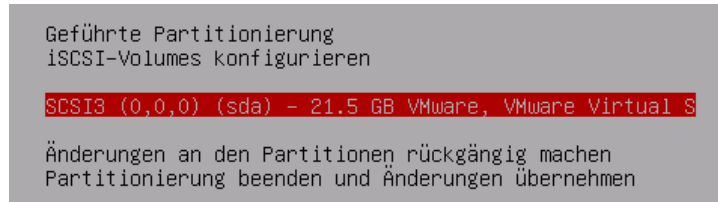


Abbildung 6: Übersicht – Festplatte partitionieren

Wählen Sie die gefundene Festplatte aus und erstellen Sie eine neue leere Partitionstabelle. Der Partitions-Typ soll msdos sein, Sie können allerdings auch andere Typen verwenden. Wie Sie dann sehen können, hat die Festplatte eine neue Partitionstabelle bekommen:



Abbildung 7: Partitionstabelle

Wählen Sie diese (rot hinterlegt) aus und erstellen Sie darauf eine neue Partition.

Die Größe dieser Partition kann hierbei ruhig die gesamte Größe der Virtuellen Maschine betragen.



Abbildung 8: Größe der Partition

Erstellen Sie diese Partition mit dem Typen „primär“.

zusätzliche Information: Dies bedeutet, dass die Partitionierung nicht nur logisch getrennt wird, sondern mit Dateien. Außerdem stellt dieser Typ sicher, dass das Betriebssystem von der Partition booten kann. Aus diesem Grund sollte die erste Partition immer primär sein.

Die Partition sollte das Ext4-Journaling-Dateisystem nutzen, root (/) als Einbindungspunkt haben, 5% oder mehr reservierte Blöcke beinhalten und Boot-Flag aktiviert haben.

zusätzliche Information: Es ist wichtig, dass mindestens 5% der Partition für ext-Dateisysteme reserviert sind, weil im Falle des Volllaufens der Festplatte die Anmeldung mit root ansonsten nicht mehr möglich wäre. Für mehr Informationen: <https://wiki.ubuntuusers.de/ext/>

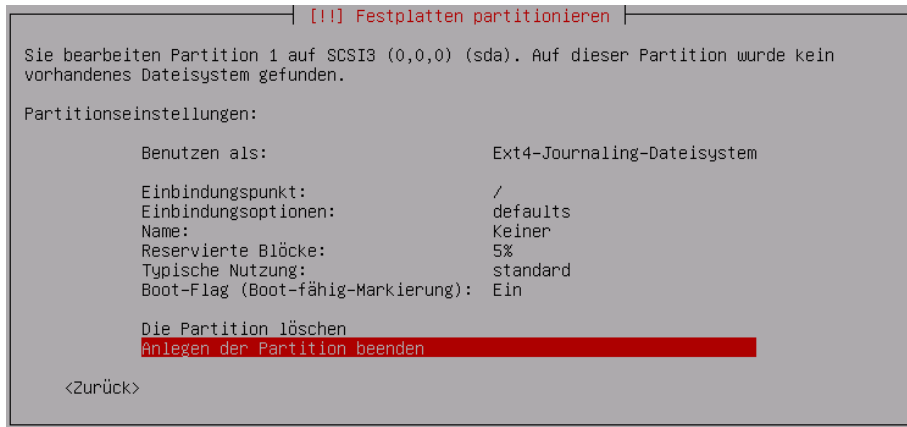


Abbildung 9: Partitionseinstellungen

Anschließend beenden Sie das Anlegen der Partition und speichern die Änderungen der Partitionierung. Kehren Sie zum Partitionierungsmenü zurück und schreiben Sie die Änderungen auf die Festplatte.

3.1.10 Basissystem installieren

Der nächste Schritt ist das Basissystem. Wählen Sie diesen Kernel aus:

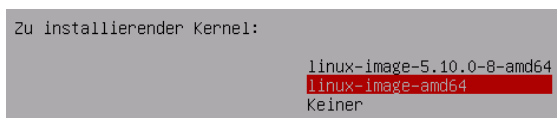


Abbildung 10: Kernel des Basissystems

Installieren Sie die Treiber **generisch**.

zusätzliche Information: Treiber generisch zu installieren, bedeutet, dass alle verfügbaren Treiber eingebunden werden. Treiber angepasst zu installieren, bedeutet, dass nur die Treiber installiert werden, die für das System gebraucht werden. Dadurch, dass Sie später noch weiter Zusatzpakete installieren wollen, ist es einfacher, wenn Sie bereits im Vorhinein alle verfügbaren Treiber installieren und danach nicht suchen müssen.

3.1.11 Paketmanager konfigurieren

Nun konfigurieren Sie den Paketmanager. Der Paketmanager von Debian heißt **apt**. Sie lesen kein weiteres Installationsmedium ein und verwenden den Netzwerkspiegel.

zusätzliche Information: Der Netzwerkspiegel bzw. Spiegelserver ist der Server, von dem sich apt seine Pakete installiert. Es wird daher empfohlen einen Spiegelserver in der Nähe, also im gleichen Land zu verwenden, damit das Downloaden schneller funktioniert.

Als Datei-Download-Protokoll verwenden Sie am besten http, weil es keine Probleme mit Firewalls verursacht. Anschließend wählen Sie einen netztopologisch gesehen, sinnvollen Spiegelserver aus. Verwenden Sie keinen Proxy, es sei denn, Sie benötigen einen, um ins Internet zu kommen. Damit Sie später alle Softwarepakete sehen können, wählen Sie die Option „<Ja>“ aus, wenn Sie nach „Non-free-Software“ gefragt werden. Paketdepots sollten Sie aktivieren. Verwenden Sie folgende Dienste (mit * markiert):

ACHTEN Sie darauf, dass mit Enter zum nächsten Fenster springen und mit Leertaste die einzelnen Dienste aktivieren bzw. deaktivieren können!

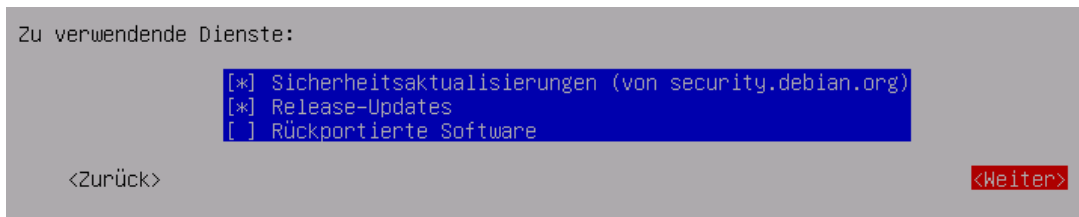


Abbildung 11: Dienste auswählen

3.1.12 Software auswählen und installieren

Dieser Schritt ist optional.

Automatische Updates können Sie deaktivieren und an der Paketverwendungserfassung wollen Sie auch nicht teilnehmen. Zusätzliche Software müssen Sie auch keine installieren. Natürlich können Sie bei allen 3 Auswahlmöglichkeiten auch auf ja klicken oder Zusatzsoftware installieren. Sie benötigen sie allerdings nicht.

3.1.13 den GRUB-Bootloader installieren

Im Gegensatz zum vorherigen Schritt ist dieser Schritt wieder unbedingt notwendig.

Installieren Sie den GRUB-Bootloader auf dem primären Laufwerk /dev/sda und deaktivieren Sie die Erzwingung von EFI.

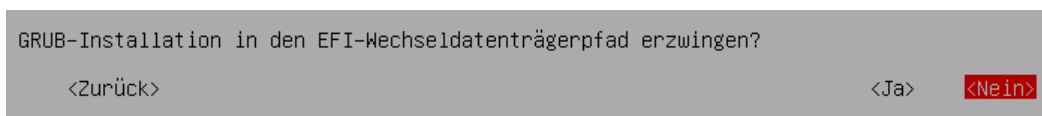


Abbildung 12: EFI Erzwingung deaktivieren

3.1.14 Installation abschließen

Schlussendlich müssen Sie nur noch die Installation abschließen. Stellen Sie ein, dass die Systemzeit nicht auf UTC eingestellt werden soll. Bestätigen Sie den Neustart und warten Sie, bis die Virtuelle Maschine neu gestartet hat.

Überprüfen Sie, ob Sie sich mit root anmelden können und fahren Sie anschließend die Virtuelle Maschine herunter.



Abbildung 13: Root-Anmeldung möglich

3.2 Aptitude + Putty

Öffnen Sie die Datei `/etc/apt/sources.list`.

```
root@debian:/etc/apt# nano sources.list
```

Code 1: `# nano sources.list`

Überprüfen Sie, ob die beiden Zeilen, in denen „cdrom“ vorkommt, auskommentiert sind. Das sollten Zeile 1 und 3 sein. Die Zeilen sind dann auskommentiert, wenn eine Raute (#) am Beginn steht.



```
GNU nano 5.4 sources.list
# deb cdrom:[Debian GNU/Linux 11.0.0 _Bullseye_ - Official amd64 NETINST 20210814-10:07]/ bullseye >
#deb cdrom:[Debian GNU/Linux 11.0.0 _Bullseye_ - Official amd64 NETINST 20210814-10:07]/ bullseye m>
deb http://deb.debian.org/debian/ bullseye main non-free contrib
deb-src http://deb.debian.org/debian/ bullseye main non-free contrib
deb http://security.debian.org/debian-security bullseye-security main contrib non-free
deb-src http://security.debian.org/debian-security bullseye-security main contrib non-free
# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates_and_backports
deb http://deb.debian.org/debian/ bullseye-updates main contrib non-free
deb-src http://deb.debian.org/debian/ bullseye-updates main contrib non-free
# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
```

Abbildung 14: `sources.list`

3.2.1 Aptitude installieren

Aktualisieren Sie die Datenbank mit „`apt-get update`“.

```
root@debian:/etc/apt# apt-get update_
```

Code 2: `# apt-get update`

Installieren Sie Aptitude.

zusätzliche Information: Aptitude ist ein Programm, mit dem Sie ganz einfach Zusatzpakete installieren können. Der große Vorteil im Gegensatz zu Apt ist, dass Aptitude Ihnen vor der Installation eine Liste aller Pakete auflistet, die neben dem vom Ihnen ausgewählten Paket installiert werden müssen.

```
root@debian:/etc/apt# apt-get install aptitude
```

Code 3: `# apt-get install aptitude`

Führen Sie Aptitude aus.

```
root@debian:/etc/apt# aptitude_
```

Code 4: `# aptitude`

Nun sollte sich ein Fenster öffnen, das ungefähr so aussieht:

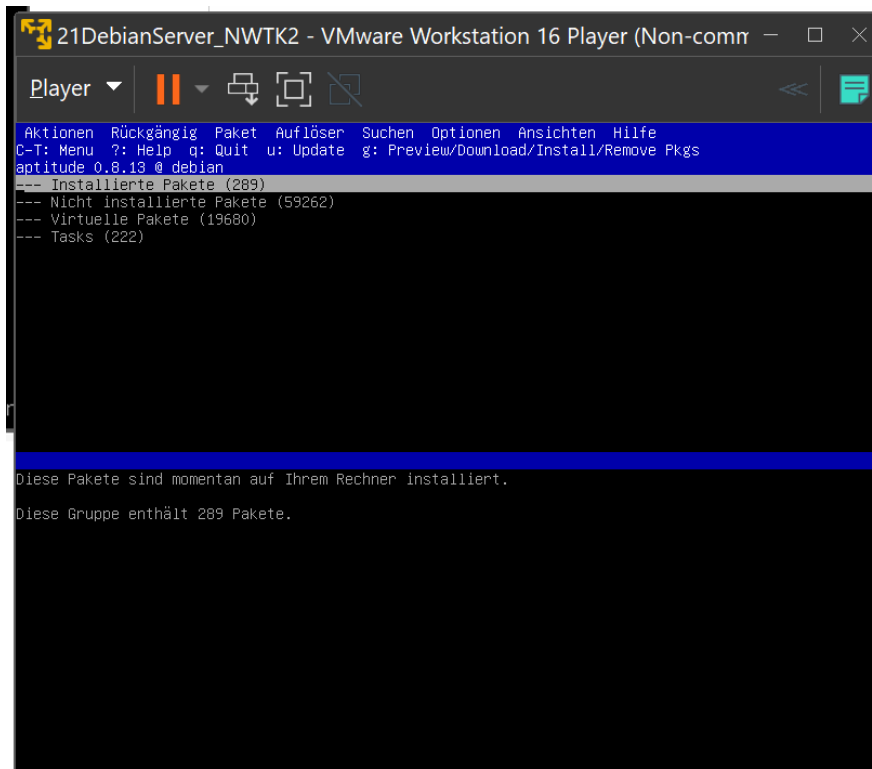


Abbildung 15: Aptitude

Hier haben Sie eine Liste mit den wichtigsten Aktionen:

- STRG+T: Menu
- q: beendet die Software Aptitude
- u: aktualisiert die Datenbank
- U: zeigt Ihnen alle Pakete an, die aktualisiert werden können
- /: öffnet ein Fenster, wo Sie nach Paketnamen suchen können
- n: springt zum nächsten Paket
- +: markiert ein Paket zum Installieren mit i (zusammenhängende Pakete werden mit iA markiert)
- g: installiert alle markierten Pakete

Unter den Aktionen können Sie sich Ihre installierten Pakete auflisten lassen. Außerdem kann man über das Menu Minesweeper spielen.

3.2.2 Openssh und man-db installieren

Öffnen Sie Aptitude, suchen Sie nach „openssh“, springen Sie die Pakete durch, bis Sie das „openssh“-Paket gefunden haben und markieren Sie dieses mit +. Installieren Sie diese Pakete.

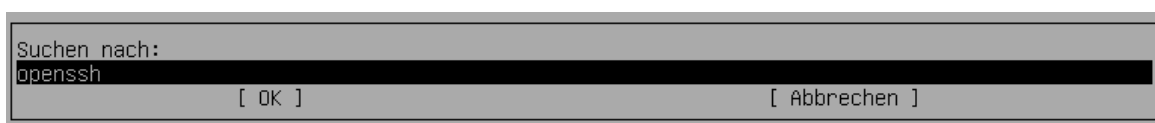


Abbildung 16: nach openssh suchen

Das gleiche Prinzip der Installation führen Sie nun bei man-db ebenfalls durch.

3.2.3 Putty einrichten

Wenn Sie mit VMWare öfters arbeiten, haben Sie vielleicht schon bemerkt, dass es schwierig ist, zwischen dem Fenster der Virtuellen Maschine und Windows bzw. dem laufenden Betriebssystem schnell zu wechseln. Aus diesem Grund ist **Putty** sehr hilfreich. So können Sie viel einfacher zwischen den Fenstern wechseln.

Laden Sie Putty über einen dieser Links herunter:

- 64-Bit-Version: <https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe>
- 32-Bit-Version: <https://the.earth.li/~sgtatham/putty/latest/w32/putty.exe>

Falls die Links nicht mehr funktionieren sollten, suchen Sie im Internet nach putty.org → Download → und suchen Sie sich die für Sie passende Version heraus.

Öffnen Sie die putty.exe Datei über den Explorer. Schreiben Sie in das Feld „Host Name (or IP address)“ die IP-Adresse der Virtuellen Maschine ein. Diese finden Sie mit dem „[ip -c a](#)“-Befehl heraus.

Wählen Sie als Verbindungstyp SSH und speichern Sie diese Einstellungen am besten unter einem sinnvollen Namen.

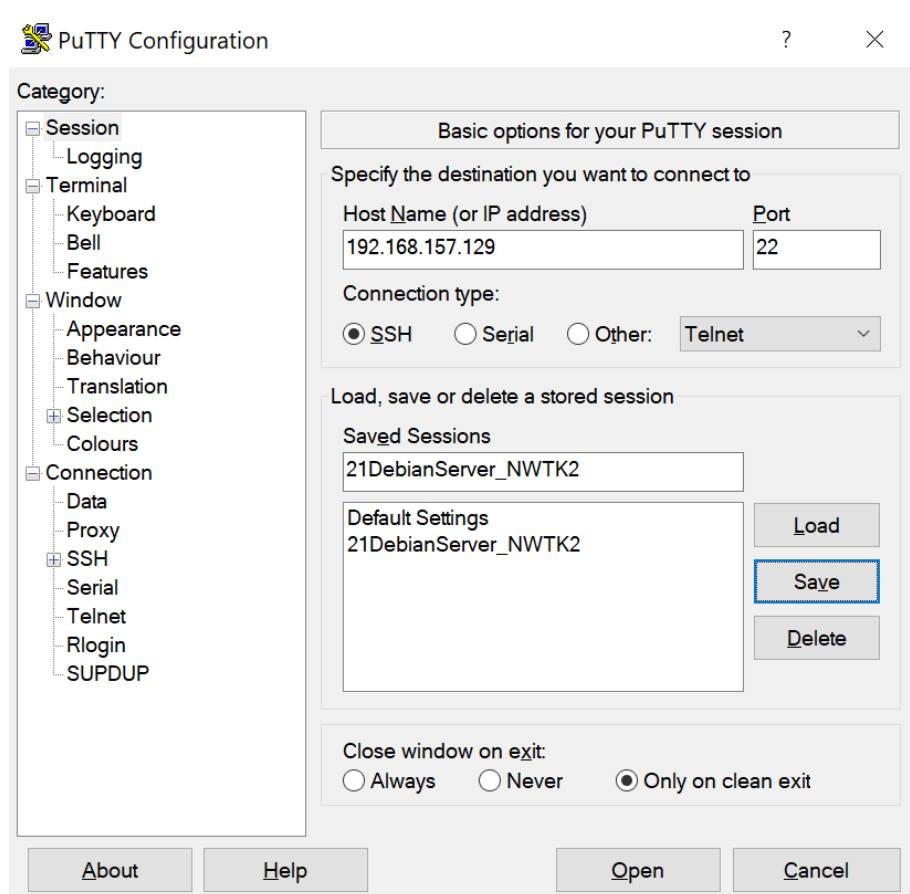


Abbildung 17: Putty Configuration

Nachdem Sie auf „Open“ geklickt haben, öffnet sich ein Fenster. Versuchen Sie einmal, sich mit dem root-Account anzumelden. Sie werden merken, dass dies nicht möglich ist, weil in der sshd_config-Datei nicht eingeschaltet ist, dass man sich mit dem root-Benutzer anmelden kann. Aus diesem Grund war es auch wichtig, dass Sie mindestens einen normalen Benutzeraccount erstellen.

Melden Sie sich nun mit dem Benutzerkonto an. Führen Sie den Befehl

```
felix@debian:~$ su - root
```

Code 5: `# su - root`

aus und geben Sie Ihr Passwort ein, um root-Berechtigungen zu erhalten.

zusätzliche Information: Den Bindestrich benötigen Sie, damit Sie auch root-Befehle ausführen können.

Öffnen Sie die Datei `/etc/ssh/sshd_config`.

```
root@debian:/etc/ssh# nano sshd_config
```

Code 6: `# nano sshd_config`

Entfernen Sie die Raute `#` in der Zeile „PermitRootLogin yes“ bzw. ändern Sie das „no“ auf ein „yes“.

Starten Sie den SSH-Service neu, indem Sie diesen Befehl eingeben:

```
root@debian:/etc/ssh# /etc/init.d/ssh restart
```

Code 7: `# /etc/init.d/ssh restart`

Anschließend können Sie sich mit dem root-Account anmelden.

3.2.4 SSH Verbindung herstellen

Um eine SSH Verbindung aufbauen zu können, benötigen Sie einen Benutzernamen, dessen Passwort und die IP-Adresse der Virtuellen Maschine.

```
PS C:\Users\Felix> ssh root@192.168.157.128
root@192.168.157.128's password:
```

3.3 wichtige Befehle zum Herausfinden von Informationen

3.3.1 ip -c a

```
root@debian:~# ip -c a
```

Code 8: `# ip -c a`

Mit diesem Befehl können Sie IP-Adressen herausfinden. Egal, ob decimal oder hexadecimal, die Antwort finden Sie mit diesem Befehl. Wegen dem „-c“ sind alle IP-Adressen in pink bzw. orange. Das „a“ ist die Kurzschreibweise für address.

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:8b:14:f9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.157.128/24 brd 192.168.157.255 scope global dynamic ens33
        valid_lft 1768sec preferred_lft 1768sec
    inet6 fe80::20c:29ff:fe8b:14f9/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:8b:14:03 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.10.21.1/24 brd 10.10.21.255 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe8b:1403/64 scope link
        valid_lft forever preferred_lft forever
```

Abbildung 18: ip -c a Ausgabe

3.3.2 route -n

```
root@debian:/etc/ssh# route -n
```

Code 9: # route -n

Mit diesem Befehl können Sie herausfinden, welche IP-Adressen über welche Router auf welchen Interfaces hinaus gehen. Hierbei können Router auf andere Rechner, also IP-Adressen bzw. Ziele, verweisen.

Ziel	Router	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.157.2	0.0.0.0	UG	0	0	0	ens33
192.168.157.0	0.0.0.0	255.255.255.0	U	0	0	0	ens33

Abbildung 19: route -n Ausgabe

3.3.3 more [path]

```
root@debian:~# more /etc/resolv.conf
```

Code 10: # more /etc/resolv.conf

Mit diesem Befehl kann man den DNS-Server des Rechners und die Domain herausfinden.

```
domain localdomain
search localdomain
nameserver 192.168.157.2
```

Abbildung 20: more /etc/resolv.conf Ausgabe

```
root@debian:~# more /etc/network/interfaces
```

Code 11: # more /etc/network/interfaces

Mit diesem Befehl kann man herausfinden, welche Netzwerkkarte welche IP-Adresse, Subnetzmaske und Gateway hat.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo ens33 ens37
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

iface ens37 inet static
    address 10.10.21.1
    netmask 255.255.255.0
```

Abbildung 21: `more/etc/network/interfaces` Ausgabe

3.3.4 `tail -f [path]`

```
root@debian:~# tail -f /var/log/syslog
```

Code 12: `# tail -f /var/log/syslog`

Mit diesem Befehl kann man sich immer die aktuellen log-Einträge ansehen. Das bedeutet, dass auf dem Fenster, wo man den Befehl aktiv ausführt, immer die neuesten Zeilen der syslog-Datei stehen. Sie können das Auslesen der syslog-Datei mit STRG+C beenden und zur Console zurückkehren.

zusätzliche Information: In dieser Datei stehen alle Meldungen bzw. Warnungen mit Ausnahme von Meldungen der auth oder authpriv Facilities. Diese Datei eignet sich daher gut zur Analyse von vielen Problemen.

```
Nov  7 13:34:36 debian systemd-networkd[1180]: ens33: Gained carrier
Nov  7 13:34:41 debian dhclient[1272]: DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 11
Nov  7 13:34:42 debian dhclient[1272]: DHCPOFFER of 192.168.157.128 from 192.168.157.254
Nov  7 13:34:42 debian dhclient[1272]: DHCPREQUEST for 192.168.157.128 on ens33 to 255.255.255.255 p
Nov  7 13:34:42 debian dhclient[1272]: DHCPACK of 192.168.157.128 from 192.168.157.254
Nov  7 13:34:42 debian dhclient[1272]: bound to 192.168.157.128 -- renewal in 696 seconds.
Nov  7 13:34:47 debian kernel: [17937.428501] e1000: ens33 NIC Link is Down
Nov  7 13:34:47 debian systemd-networkd[1180]: ens33: Lost carrier
Nov  7 13:34:51 debian kernel: [17941.495287] e1000: ens33 NIC Link is Up 1000 Mbps Full Duplex, Flo
Nov  7 13:34:51 debian systemd-networkd[1180]: ens33: Gained carrier
```

Abbildung 22: Beispiel für Ausgabe von `# tail -f /var/log/syslog`

3.3.5 `tracert -d [ip-address]`

```
C:\Users\Felix>tracert -d 192.168.157.2

Routenverfolgung zu 192.168.157.2 über maximal 30 Hops

 1      1 ms    <1 ms    <1 ms    10.10.21.1
 2      2 ms     4 ms     2 ms    192.168.157.2

Ablaufverfolgung beendet.

C:\Users\Felix>
```


tracert -d 192.168.157.2 zeigt die Routenverfolgung bis zum Ziel.

3.4 Virtuelle Windows Maschine

3.4.1 Virtuelle Windows Maschine aufsetzen

Laden Sie sich eine Windows 10 - ISO-Datei, oder wenn Sie wollen Windows 11 - ISO-Datei, vom Internet oder von hier: <https://www.microsoft.com/de-de/software-download/windows11> herunter.

Erstellen Sie eine neue Virtuelle Maschine in VMWare mit sinnvollem Namen, genügend RAM und Festplattenspeicher und fügen Sie die heruntergeladene ISO-Datei ein. Führen Sie den Installationsprozess durch.

3.4.2 Virtuelle Debian Maschine fürs Pinggen einrichten

Als zweites schließen Sie die Virtuelle Debian Maschine, falls diese noch läuft. Gehen Sie in die Einstellungen der Virtuellen Debian Maschine und fügen Sie eine zweite Netzwerkkarte hinzu.

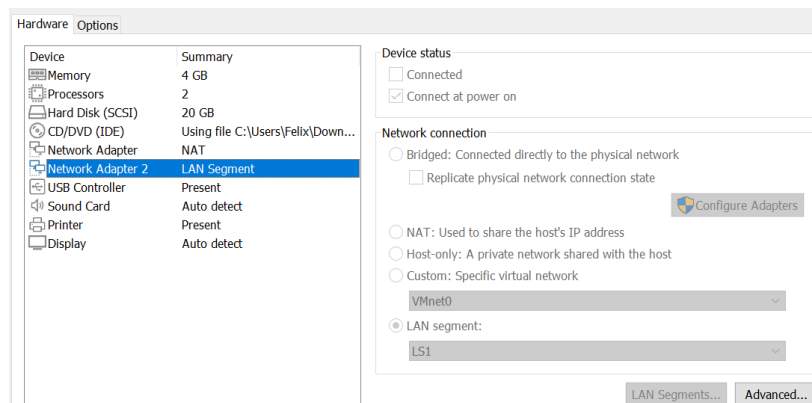


Abbildung 23: LAN Segment

Diese soll auf „LAN segment“ gestellt werden. Geben Sie dem Segment einen Namen, speichern Sie und fahren Sie die Virtuelle Debian Maschine wieder hoch.

Als nächstes ändern Sie auf der Virtuellen Debian Maschine die „/etc/network/interfaces“-Datei. Öffnen Sie die Datei mit „nano“ mit Root-Berechtigungen, um den Inhalt der Datei ändern zu können.

```
root@debian:~# nano /etc/network/interfaces
```

Code 13: # nano /etc/network/interfaces

Sie werden feststellen, dass diese Datei bereits einige geschriebene Zeilen beinhaltet. Das sind Voreinstellungen.

Sie müssen jetzt die Netzwerkeinstellungen von der neuen Netzwerkkarte hinzufügen. Um herauszufinden, wie die Netzwerkkarte heißt benötigen Sie den Befehl `ip -c a`. In hellblau bzw. türkis sehen Sie die Netzwerkkarten. Die Netzkarte, die Sie noch konfigurieren müssen, hat noch keine IP-Adresse. Konfigurieren Sie sie statisch mit IP-Adresse und Subnetzmaske.

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo ens33 ens37
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

iface ens37 inet static
    address 10.10.21.1
    netmask 255.255.255.0
```

Abbildung 24: /etc/network/interfaces

Außerdem schreiben Sie den Namen dieser Netzwerkkarte bei der Zeile „auto lo“ hinten dazu, damit die Änderungen bei Ausführung des Befehls „service networking restart“ auch übernommen werden.

zusätzliche Informationen: „iface“ schreiben Sie, weil Sie ein Interface konfigurieren. „ens37“ ist bei mir der Name der Netzwerkkarte. Als Protokoll verwenden Sie am besten „inet“ und weil Sie die IP-Adresse statisch, also per Hand, eintragen wollen, schreiben Sie „static“.

Als nächstes starten Sie das Netzwerk neu. Dies können Sie mit mehreren verschiedenen Befehlen erzielen. Hier zwei Beispiele:

```
root@debian:~# /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.
root@debian:~# _
```

Code 14: # /etc/init.d/networking restart

```
root@debian:~# service networking restart
root@debian:~# _
```

Code 15: # service networking restart

3.4.3 Windows Einstellungen konfigurieren

3.4.3.1 IPv4 Konfiguration

Auf der Virtuellen Windows Maschine müssen Sie die IPv4-Adresse, die Subnetzmaske und das Gateway, also den Router, richtig konfigurieren, damit eine Verbindung überhaupt stattfinden kann.

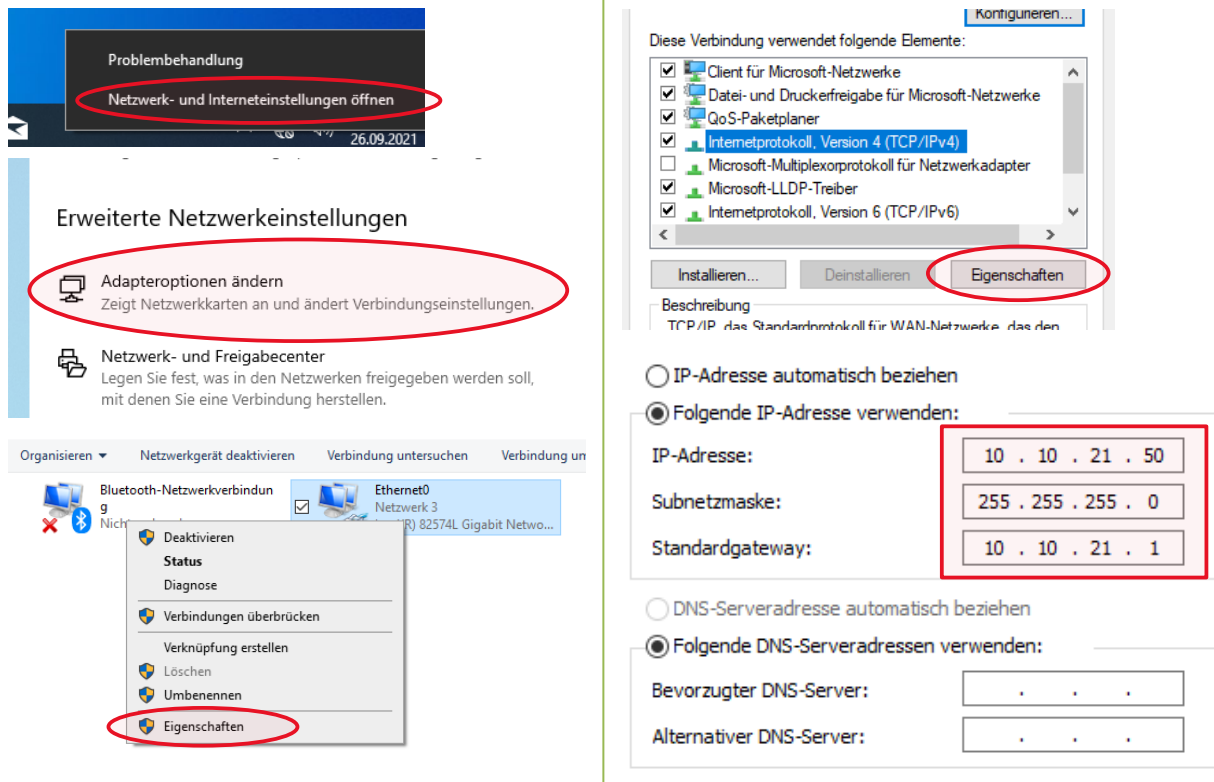


Abbildung 25: IPv4-Adressen Einstellungen Windows

Zu beachten ist hierbei, dass die dritte Dekade der IPv4-Adresse und des Standardgateways mit der IPv4-Adresse der Virtuellen Debian Maschine übereinstimmen (Interface ens37).

Mit dem Befehl „ipconfig“ können Sie Ihre Einstellungen auf Ihre Korrektheit prüfen.

```
C:\Users\Felix>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Ethernet0:

    Verbindungsspezifisches DNS-Suffix:
    Verbindungslokale IPv6-Adresse . . : fe80::5d6:4a2f:2baf:fab8%6
    IPv4-Adresse . . . . . : 10.10.21.50
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 10.10.21.1

Ethernet-Adapter Bluetooth-Netzwerkverbindung:

    Medienstatus. . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix:

C:\Users\Felix>
```

Abbildung 26: ipconfig
Code 16: # ipconfig

Damit wir von Debian Windows auch pingen können, müssen wir die Windows Firewall deaktivieren. Dies folgt in den nächsten Schritten:

3.4.3.2 Firewall deaktivieren

Im nächsten Schritt müssen Sie die Firewall der Virtuellen Windows Maschine deaktivieren, weil ansonsten diese die Pakete möglicherweise nicht von der Virtuellen Debian Maschine zu der Virtuellen Windows Maschine durchlässt.

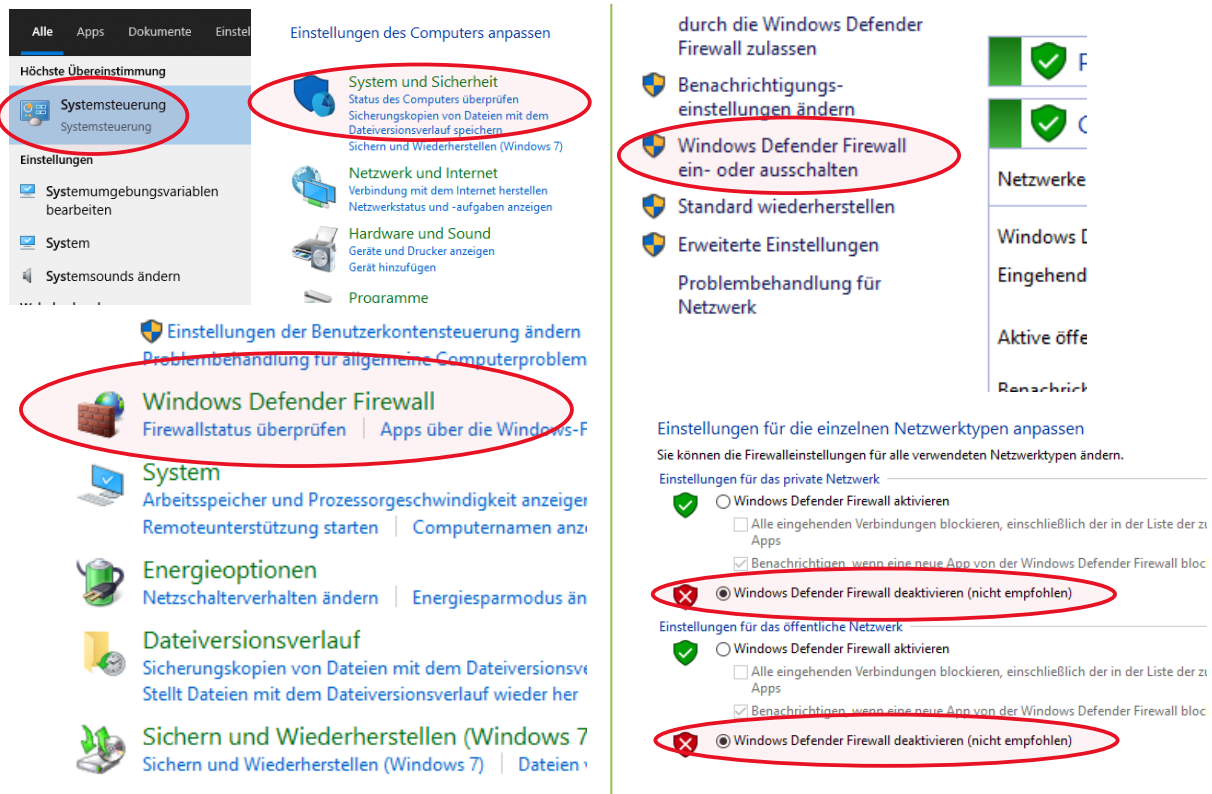


Abbildung 27: Firewall deaktivieren

Wenn wir die Netzwerkkonfigurationen auf der Virtuellen Debian Maschine neu starten, sollte das Ping in beide Richtungen funktionieren.

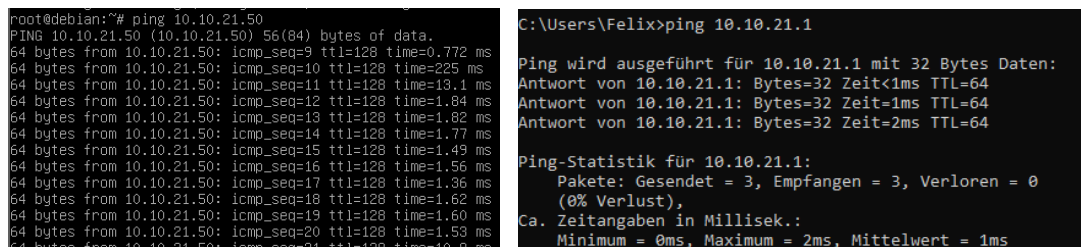


Abbildung 28 (links): Debian – ping Windows

Abbildung 29 (rechts): Windows – ping Debian

3.5 Virtuelle Debian Maschine Kopie

3.5.1 Virtuelle Debian Maschine klonen

Klonen Sie die Virtuelle Debian Maschine. Dies können Sie erreichen, indem Sie folgende Schritte befolgen:

Tätigen Sie einen Rechtsklick auf die Virtuelle Maschine in VMWare Workstation Player und klicken Sie auf „Settings...“ beziehungsweise „Einstellungen...“. Klicken Sie auf die Abteilung „Hard Disk (SCSI)“ und kopieren Sie den Pfad, wo die Virtuelle Debian Maschine gespeichert ist (im Bild rot markiert).

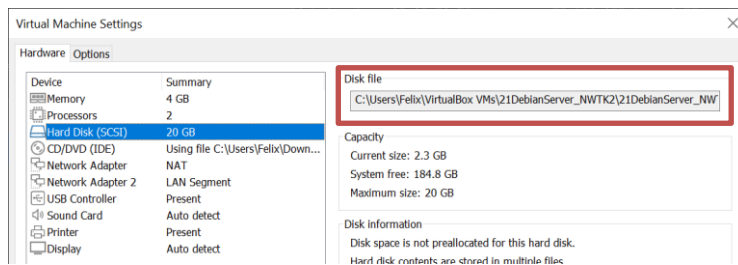


Abbildung 30: Pfad der Virtuellen Debian Maschine finden

Öffnen Sie Ihren Explorer und fügen Sie den kopierten Pfad in die Adressleiste ein. Wichtig ist, dass Sie anschließend den Namen am Ende der Adressleiste und die Dateierweiterung löschen, ansonsten starten Sie die Virtuelle Debian Maschine. Drücken Sie dann Enter und Sie werden zu dem Ordner geführt, indem sich die Virtuelle Debian Maschine befindet.

In diesem Ordner befindet sich eine Datei, die den Namen der Virtuellen Debian Maschine und die Dateierweiterung „.vmdk“ enthält. Diese Datei ist im nachstehenden Bild grau hinterlegt.

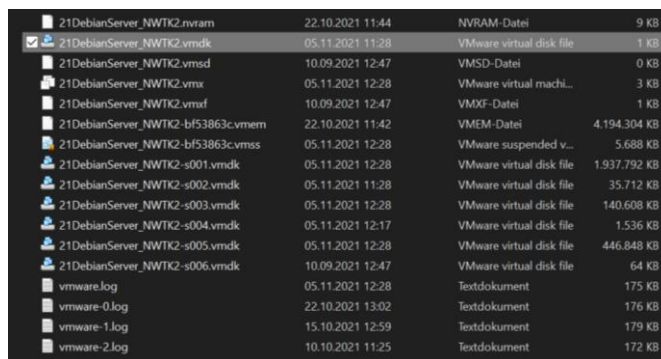


Abbildung 31: Virtuelle Debian Maschine - Datei

Kopieren Sie diese Datei in einen anderen Ordner und benennen Sie die Datei um, sodass der Name der neuen Virtuellen Debian Maschine drinnen steht, zum Beispiel: „21DebianClient_NWTK2.vmdk“. Führen Sie die Datei aus.

Wenn Sie gefragt werden, ob Sie die Virtuelle Debian Maschine Kopie verschoben oder kopiert haben, klicken Sie auf kopiert, damit die neue Virtuelle Debian Client Maschine eine neue eigene MAC-Adresse bekommt.

Schließen Sie die Virtuelle Debian Client Maschine wieder und öffnen Sie die Einstellungen. Entfernen Sie das virtuelle LAN-Segment, das Sie bei der ersten Virtuellen Debian Maschine hinzugefügt haben.

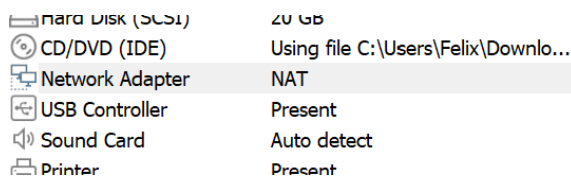


Abbildung 32: LAN-Segment entfernen

3.5.2 Webserver einrichten

Richten Sie einen Webserver auf der Virtuellen Debian Client Maschine ein, den Sie auf den anderen Virtuellen Maschinen erreichen, indem Sie folgende Schritte befolgen.

3.5.2.1 Apache2 installieren

Laden Sie über Aptitude das Apache2-Paket, das PHP-Paket und alle zugehörigen Pakete auf der Virtuellen Debian Client Maschine herunter.

3.5.2.2 Skript PHP schreiben

Damit Sie von der Virtuellen Windows Maschine über einen Webserver die Virtuelle Debian Client Maschine erreichen können und eine IP-Adresse angezeigt bekommen, müssen Sie sich ein PHP-Skript schreiben.

Erstellen Sie die Datei „/var/www/html/ip.php“ und fügen Sie den untenstehenden PHP-Code in diese Datei ein.

```
root@debian:~# nano /var/www/html/ip.php
```

Code 17: # nano /var/www/html/ip.php

```
GNU nano 5.4
<?php
$ip = $_SERVER["REMOTE_ADDR"];
$host = gethostbyaddr($ip);

echo "IP Adresse: $ip<br>";
echo "Hostname: $host";
?>
```

Abbildung 33: ip.php

3.5.3 Virtuelle Debian Client Maschine mit Virtuelle Windows Maschine verbinden

Es gibt zwei Möglichkeiten, wie Sie die Virtuelle Debian Client Maschine mit der Virtuelle Windows Maschine verbinden können:

- [NAT MASQUERADE](#)
- [Route IP-Weiterleitung](#)

NAT MASQUERADE verändert die IP-Adresse des Paketes und schickt es anschließen zu dieser Adresse. Die Route IP-Weiterleitung leitet das Pakete an die IP-Adresse weiter, die in der Tabelle eingetragen ist.

3.5.3.1 NAT MASQUERADE

Das ist der grundsätzliche Aufbau des neuen Netzwerks, wenn Sie NAT verwenden. In den folgenden Schritten werden Sie die Einstellungen dementsprechend konfigurieren.

zusätzliche Information: MASQUERADE ändert die ursprüngliche Quelladresse des Pakets in eine routbare IP-Adresse um.

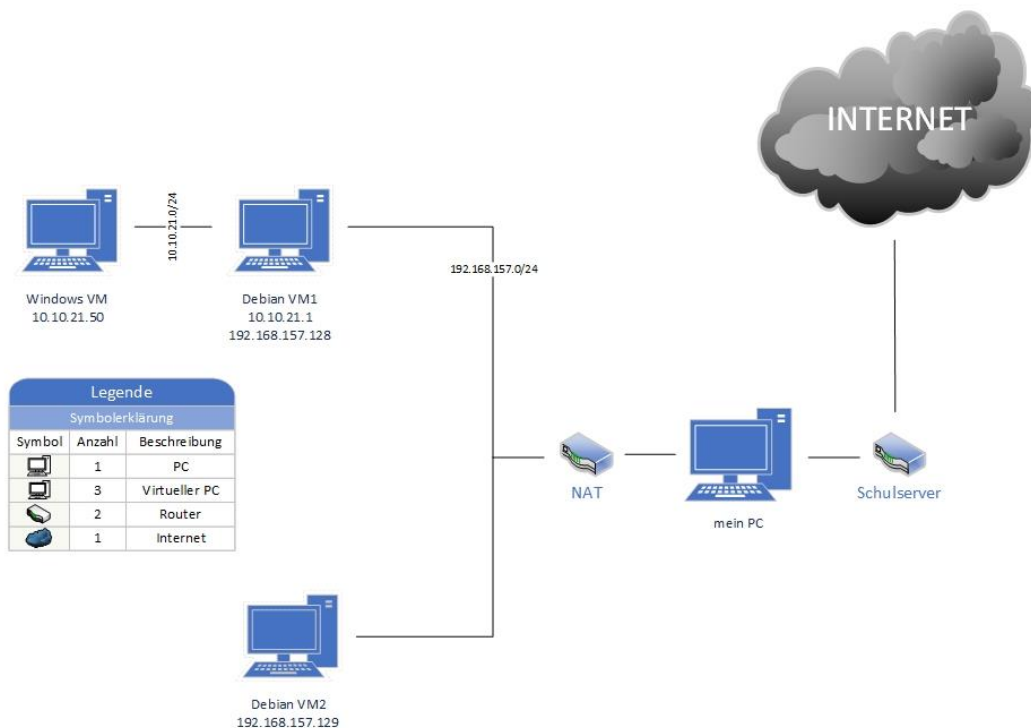


Abbildung 34: Netzwerkaufbau NAT

3.5.3.1.1 „iptables“ installieren

Als erstes installieren Sie das „iptables“-Paket mittels Aptitude.

3.5.3.1.2 Nat richtig einstellen

Damit NAT richtig funktioniert, muss MASQUERADE auf alle Pakete vom Interface ens33 in der POSTROUTING-Chain auf MASQUERADE umgestellt werden. Iptables weiß dann automatisch, was es zu tun hat. Damit Sie das erreichen benötigen Sie folgenden Befehl:

```
root@debian:~# iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
root@debian:~# _
```

Code 18: # iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

Zur Kontrolle, ob Masquerade nun aktiviert ist, tippen Sie den Befehl „iptables -t nat -L“ ein. Dieser zeigt Ihnen die aktuellen IP-Tabelle-Einstellungen. In der letzten Zeile des Bildes sehen Sie, dass Masquerade für alle Pakete aktiviert ist.

```
root@debian:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source          destination

Chain INPUT (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source          destination
MASQUERADE all  --  anywhere        anywhere
```

Abbildung 35: IP-Tabellen-Einstellungen

Code 19: # iptables -t nat -L

Wenn Sie glauben, die IP-Tabellen-Einstellungen kaputt gemacht zu haben, verwenden Sie den Befehl „iptables -t nat -F“, um die IP-Tabellen-Einstellungen für NAT zurückzusetzen.

3.5.3.1.3 Webserver erreichen

Öffnen Sie auf der Virtuellen Windows Maschine einen Browser Ihrer Wahl und tippen Sie die IP-Adresse der Virtuellen Debian Client Maschine, aus der kopierten Virtuellen Debian Maschine, in die URL-Leiste. Fügen Sie dann noch ein „/ip.php“ an, damit auch die Datei, die Sie [vorhin](#) erstellt haben, aufrufen.

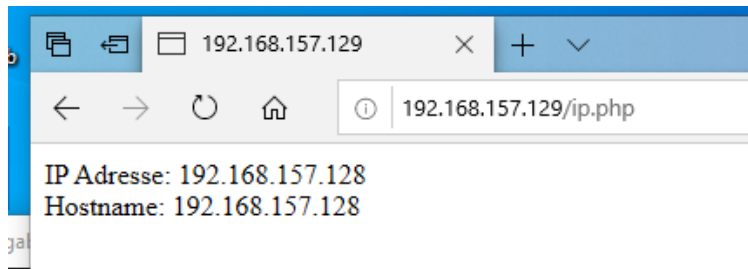


Abbildung 36: Webserver erreichen NAT

3.5.3.2 Route IP-Weiterleitung

Das ist der grundsätzliche Aufbau des neuen Netzwerks, wenn Sie die Routing Variante verwenden. In den folgenden Schritten werden Sie die Einstellungen dementsprechend konfigurieren.

zusätzliche Information: ROUTING sucht in einer internen Tabelle nach der Zieladresse des Paketes. Wenn diese gefunden wurde, schickt Routing das Paket an die andere IPv4-Adresse, die in der Tabelle neben der Zieladresse steht.

3.5.3.2.1 IPv4-Adressen aktivieren

Damit die Variante mittels Router funktioniert, müssen Sie als allererstes, IPv4-Adressen am Router aktivieren. Öffnen Sie hierzu die Datei „/etc/sysctl.conf“ und einkommentieren Sie die Zeile „net.ipv4.ip_forward=1“, indem Sie die Raute am Beginn der Zeile löschen.

```
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

Abbildung 37: sysctl.conf - net.ipv4.ip_forward=1

Speichern Sie die Datei mit STRG+O und verlassen Sie die Datei mit STRG+X. Mit dem Befehl „sysctl -p“ können Sie sich alle Zeilen, die nicht kommentiert sind, der Datei „sysctl.conf“ ausgeben lassen.

```
root@debian:~# sysctl -p
net.ipv4.ip_forward = 1
```

Code 20: # sysctl -p

3.5.3.2.2 Routing-Tabelle einstellen

Mit dem Befehl „[route -n](#)“ können Sie sich diese Routing-Tabelle anzeigen lassen.

Wenn Sie einen neuen Eintrag in die Tabelle machen wollen, verwenden Sie den Befehl „route add -net [Ziel-IP-Adresse des Pakets]/[Subnetzmaske] gw [neue Ziel-IP-Adresse des Routers]“

```
root@debian:~# route add -net 10.10.21.0/24 gw 192.168.157.128
root@debian:~#
```

Code 21: # route add -net 10.10.21.0/24 gw 192.168.157.128

Damit sich die Virtuelle Debian Klon Maschine mit der Virtuellen Windows Maschine verbindet, stellen Sie die Router-Tabelle-Einstellungen der Virtuellen Debian Maschine so ein:

```
root@debian:~# route -n
Kernel-IP-Routentabelle
Ziel          Router        Genmask         Flags Metric Ref    Use Iface
0.0.0.0        192.168.157.2 0.0.0.0         UG    0      0      0 ens33
10.10.21.0     0.0.0.0       255.255.255.0   U      0      0      0 ens37
192.168.157.0 0.0.0.0       255.255.255.0   U      0      0      0 ens33
root@debian:~#
```

Abbildung 38: Route-Einstellungen von Virtueller Debian Maschine

Die Virtuelle Debian Klon Maschine – Router-Tabellen-Einstellungen müssen Sie so einstellen:

```
Kernel-IP-Routentabelle
Ziel          Router        Genmask       Flags Metric Ref    Use Iface
0.0.0.0        192.168.157.2 0.0.0.0       UG    0      0      0 ens33
10.10.21.0     192.168.157.128 255.255.255.0 UG    0      0      0 ens33
192.168.157.0 0.0.0.0       255.255.255.0 U      0      0      0 ens33
root@debian:/var/www/html# _
```

Abbildung 39: Route-Einstellungen von Virtuelle Debian Klon Maschine

3.5.3.2.3 Webserver erreichen

Öffnen Sie auf der Virtuellen Windows Maschine einen Browser Ihrer Wahl und tippen Sie die IP-Adresse der Virtuellen Debian Client Maschine, als der kopierten Virtuellen Debian Maschine, in die URL-Leiste. Fügen Sie dann noch ein „/ip.php“ an, damit auch die Datei, die Sie [vorhin](#) erstellt haben, aufrufen.



IP Adresse: 10.10.21.50
Hostname: 10.10.21.50

3.6 Windows Internet

Damit Sie in der Virtuellen Windows Maschine Internetzugang haben tragen Sie in den IPv4-Einstellungen einen DNS-Server ein. Wichtig ist hierbei nur der bevorzugte DNS-Server, es funktioniert auch ohne den alternativen DNS-Server-Eintrag.

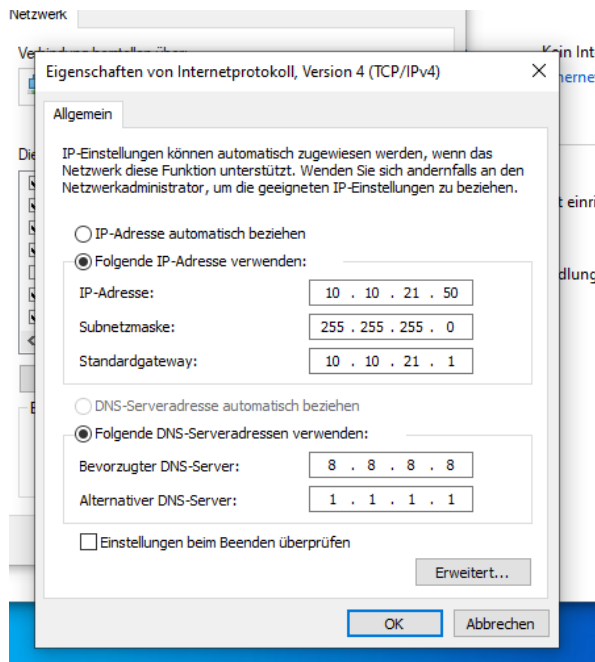


Abbildung 40: Virtuelle Windows Maschine DNS-Server

WICHTIG: Dies funktioniert nur bei der [NAT Methode](#). Bei der [ROUTING Methode](#) funktioniert die Weiterleitung logischerweise nicht!

3.7 DHCP Server

3.7.1 DHCP Server konfigurieren

3.7.1.1 isc-dhcp-server Paket installieren

Installieren Sie mithilfe von Aptitude das „isc-dhcp-server“-Paket und alle dazugehörigen Pakete auf der Virtuellen Debian Maschine.

3.7.1.2 Interface einstellen

Schreiben Sie in die „/etc/default/isc-dhcp-server“-Datei bei INTERFACESv4="" zwischen die Anführungszeichen ihre Netzwerkkarte, die zur Virtuellen Windows Maschine führt.

```
# Separate interface
INTERFACESv4="ens37"
INTERFACESv6=""
```

Abbildung 41: Netzwerkkarte DHCP einstellen

3.7.1.3 dhcpd.conf Datei

In der „/etc/dhcp/dhcpd.conf“ stellen Sie folgende Einstellungen um:

1. die Domain-Name **Servers** sind 8.8.8.8 und 1.1.1.1
2. die Domain-Name ist grundsätzlich egal
3. Entkommentieren Sie **authoritative**, weil der DHCP Server der einzige DHCP Server in dem Netzwerk ist
4. Stellen Sie das Subnetz so ein:

```
subnet 10.10.21.0 netmask 255.255.255.0 {
    range 10.10.21.100 10.10.21.150;
    option routers 10.10.21.1;
}
```

Abbildung 42: Subnetz DHCP einstellen

3.7.1.4 DHCP Server neu starten

Starten Sie den DHCP Service neu, indem Sie diesen Befehl schreiben:

```
root@debian:~# systemctl restart isc-dhcp-server.service
root@debian:~# _
```

Code 22: # systemctl restart isc-dhcp-server.service

3.7.2 Virtuelle Windows Maschine auf DHCP umstellen

3.7.2.1 umstellen

Navigieren Sie auf der Virtuellen Windows Maschine zu den Netzwerkeinstellungen des IPv4-Protokolls und schalten Sie „IP-Adresse automatisch beziehen“ ein. In anderen Worten ist dies die DHCP-Einstellung.

☒ IP-Adresse automatisch beziehen

☐ Folgende IP-Adresse verwenden:

IP-Adresse:	...
Subnetzmaske:	...
Standardgateway:	...

Abbildung 43: IP-Adresse automatisch beziehen

3.7.2.2 überprüfen

Um festzustellen, ob die Einstellungen richtig konfiguriert wurden und DHCP funktioniert, lassen Sie sich die IP-Adresse der Virtuellen Windows Maschine anzeigen:

```
C:\Users\Felix>ipconfig /all
```

Code 23: # ipconfig /all

```
Ethernet-Adapter Ethernet0:
Verbindungsspezifisches DNS-Suffix: felix.net
Beschreibung. . . . . : Intel(R) 82574L Gigabit Network Connection
Physische Adresse . . . . . : 00-0C-29-81-0B-73
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . . : fe80::5d6:4a2f:2baf:fab8%6(Bevorzugt)
IPv4-Adresse . . . . . : 10.10.21.100(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Freitag, 19. November 2021 12:17:50
Lease läuft ab. . . . . : Freitag, 19. November 2021 12:27:50
Standardgateway . . . . . : 10.10.21.1
DHCP-Server . . . . . : 10.10.21.1
DHCPv6-IAID . . . . . : 117443625
DHCPv6-Client-DUID. . . . . : 00-01-00-01-28-DF-5A-EC-00-0C-29-81-0B-73
DNS-Server . . . . . : 8.8.8.8
                  . . . . . : 1.1.1.1
NetBIOS über TCP/IP . . . . . : Aktiviert

Ethernet-Adapter Bluetooth-Netzwerkverbindung:
```

Abbildung 44: Ausgabe der Interneteinstellungen Windows

3.7.3 syslog

Sie können auch auf der Virtuellen Debian Maschine in der /var/log/syslog-Datei nachsehen, ob DHCP Pakete ein- und ausgegangen sind.

```
root@debian:~# tail -f /var/log/syslog
Nov 19 12:15:46 debian isc-dhcp-server[10099]: Starting ISC DHCPv4 server: dhcpd.
Nov 19 12:15:46 debian systemd[1]: Started LSB: DHCP server.
Nov 19 12:16:59 debian dhclient[2404]: DHCPREQUEST for 192.168.157.128 on ens33 to 192.168.157.254 port 67
Nov 19 12:16:59 debian dhclient[2404]: DHCPACK of 192.168.157.128 from 192.168.157.254
Nov 19 12:16:59 debian dhclient[2404]: bound to 192.168.157.128 -- renewal in 743 seconds.
Nov 19 12:17:01 debian CRON[10133]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Nov 19 12:17:50 debian dhcpd[10114]: DHCPDISCOVER from 00:0c:29:81:0b:73 via ens37
Nov 19 12:17:51 debian dhcpd[10114]: DHCPOFFER on 10.10.21.100 to 00:0c:29:81:0b:73 (DESKTOP-9DUA28D) via ens37
Nov 19 12:17:51 debian dhcpd[10114]: DHCPREQUEST for 10.10.21.100 (10.10.21.1) from 00:0c:29:81:0b:73 (DESKTOP-9DUA28D) via ens37
Nov 19 12:17:51 debian dhcpd[10114]: DHCPACK on 10.10.21.100 to 00:0c:29:81:0b:73 (DESKTOP-9DUA28D) via ens37
```

Abbildung 45: Syslog-Datei Ausgabe

3.7.4 Virtuelle Windows Maschine mittels MAC-Adresse IP-Adresse zuordnen

3.7.4.1 dhcpd.conf konfigurieren

Die Datei dhcpd.conf müssen Sie folgendermaßen konfigurieren:

Wie Sie sehen können weisen Sie dem Windows Client dann immer eine fixe IP-Adresse mithilfe der MAC-Adresse zu. Die MAC-Adresse der Virtuellen Windows Maschine finden Sie mit dem Befehl „ipconfig /all“ heraus.

```
# This is a very basic subnet declaration.

subnet 10.10.21.0 netmask 255.255.255.0 {
    range 10.10.21.100 10.10.21.150;
    option routers 10.10.21.1;

    #Virtuelle Windows Maschine immer gleiche IP-Adresse
    host winclient {
        hardware ethernet 00:0C:29:81:0B:73;
        fixed-address 10.10.21.50;
    }
}
```

Abbildung 46: dhcpd.conf mit fixer Adresse

3.7.4.2 Virtuelle Windows Maschine IPv4-Konfiguration erneuern

Mit dem Befehl „ipconfig /renew“ holt sich die Virtuelle Windows Maschine die neue IPv4-Adresse.

```
Ethernet-Adapter Ethernet0:

    Verbindungsspezifisches DNS-Suffix: felix.net
    Verbindungslokale IPv6-Adresse . . : fe80::5d6:4a2f:2baf:fab8%6
    IPv4-Adresse . . . . . : 10.10.21.50
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 10.10.21.1
```

Abbildung 47: IP-Konfiguration Virtuelle Windows Maschine

3.8 Firewall

3.8.1 iptables Befehl und Co.

3.8.1.1 Konfiguration in Datei speichern

„iptables-save -f <Dateiname>“ speichert die aktuelle iptables-Konfiguration in die neue Datei.

```
root@debian:/etc/iptables# iptables-save -f iptables2.rules
root@debian:/etc/iptables# ls
empty.rules  iptables2.rules  iptables.rules
```

Abbildung 48: iptables-Konfiguration speichern

3.8.1.2 Konfiguration aus Datei laden

„iptables-restore <Dateiname>“ ladet die Konfigurationen aus der Datei in die aktuelle Konfiguration.

```
root@debian:/etc/iptables# iptables-restore iptables.rules
root@debian:/etc/iptables# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            state RELATED,ESTABLISHED
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    tcp  --  anywhere              anywhere               tcp dpt:http
ACCEPT    tcp  --  anywhere              anywhere               tcp dpt:https
ACCEPT    tcp  --  anywhere              anywhere               tcp dpt:ssh

Chain FORWARD (policy DROP)
target     prot opt source                destination            state RELATED,ESTABLISHED
ACCEPT    all  --  anywhere              anywhere
ACCEPT    all  --  10.10.21.50           anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Abbildung 49: iptables-Konfiguration laden

3.8.2 Firewall konfigurieren (iptables)

3.8.2.1 Iptables konfigurieren

Führen Sie folgende Befehle durch:

```
# alles löschen
iptables -t filter -F
iptables -t nat -F

# default policy
iptables -t filter -P INPUT DROP
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -t filter -P FORWARD DROP
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# loopback
iptables -t filter -A INPUT -i lo -j ACCEPT

# http, https
iptables -t filter -A INPUT -p tcp --dport 80,443 -j ACCEPT

# proxy
iptables -t filter -A INPUT -p tcp --dport 3128 -s 10.10.10.0/24 -j ACCEPT

# ssh
iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT

# masquerade (nat)
iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

# forwarding
iptables -t filter -A FORWARD -s 10.10.10.50 -j ACCEPT

# port-forwarding
iptables -t nat PREROUTING -p tcp --dport 3389 -j DNAT --to-destination 10.10.10.50:3389
```

Abbildung 50: Firewall iptables Befehle

3.8.2.2 Iptables-Konfiguration speichern

Speichern Sie die aktuelle Konfiguration ([Konfiguration in Datei speichern](#)).

```
# Generated by iptables-save v1.8.7 on Fri Nov 26 12:46:09 2021
*filter
:INPUT DROP [2:573]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [3:726]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -s 10.10.21.50/32 -j ACCEPT
COMMIT
# Completed on Fri Nov 26 12:46:09 2021
# Generated by iptables-save v1.8.7 on Fri Nov 26 12:46:09 2021
*nat
:PREROUTING ACCEPT [31:2234]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [3:726]
:POSTROUTING ACCEPT [1:328]
-A PREROUTING -p tcp -m tcp --dport 3389 -j DNAT --to-destination 10.10.21.50:3389
-A POSTROUTING -o ens33 -j MASQUERADE
COMMIT
# Completed on Fri Nov 26 12:46:09 2021
```

Abbildung 51: Datei mit Konfiguration (iptables)

3.8.2.3 laden der Konfiguration

Sie können nun die Konfiguration immer nach dem Hochfahren der Virtuellen Debian Server Maschine laden ([Konfiguration aus Datei laden](#)).

```
root@debian:/etc/iptables# iptables-restore iptables.rules
root@debian:/etc/iptables#
```

Code 24: # iptables-restore iptables.rules

3.8.2.4 Autoladen der Konfiguration

Damit Sie nicht jedes Mal nach dem Hochfahren die Konfiguration per Hand laden müssen, können Sie auch einstellen, dass diese automatisch geladen wird, und die Firewall somit automatisch konfiguriert ist. Dies wird mithilfe eines „systemd“-Service umgesetzt.

Erstellen Sie eine neue Datei: „/etc/systemd/system/iptables.service“. Schreiben Sie den Inhalt des folgenden Screenshots ab.

zusätzliche Informationen: Bei [Unit] werden allgemeine Beschreibungen hinzugefügt und festgelegt, in welcher Reihenfolge der Service ausgeführt werden soll. Bei [Service] wird eingestellt, welcher Service dahinter ausgeführt wird. [Install] managed, von welchem Target der Service ausgeführt werden soll.

```
[Unit]
Description=iptables firewall service
After=network.target

[Service]
Type=oneshot
ExecStart=/sbin/iptables-restore /etc/iptables/iptables.rules
RemainAfterExit=true
ExecStop=/sbin/iptables-restore /etc/iptables/empty.rules

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

Abbildung 52: /etc/systemd/system/iptables.service

Anschließend können Sie den Service neu laden. Starten Sie den Service nun entweder per Hand oder stellen Sie ein, dass er jedes Mal beim Starten ausgeführt wird.

```
root@debian:/etc/systemd/system# systemctl daemon-reload
```

Code 25: # systemctl daemon-reload

```
root@debian:/etc/systemd/system# systemctl start iptables.service
```

Code 26: # systemctl start iptables.service

```
root@debian:/etc/systemd/system# systemctl enable --now iptables.service
Created symlink /etc/systemd/system/multi-user.target.wants/iptables.service → /etc/systemd/system/iptables.service.
```

Code 27: # systemctl enable --now iptables.service

3.8.2.5 Firewall testen

Testen Sie die Firewall, indem Sie die Regeln, die Sie konfiguriert haben, ausprobieren. Zum Beispiel sollten Sie die Virtuelle Debian Maschine von der Virtuellen Windows Maschine nicht pingen.

```
C:\Users\Felix>ping 192.168.157.128

Ping wird ausgeführt für 192.168.157.128 mit 32 Bytes Daten:
STRG-C
^C
C:\Users\Felix>
```

Abbildung 53: not-ping Debian

3.8.3 Firewall konfigurieren (nftables)

Eine andere Variante, wie man die Firewall konfigurieren kann ist **NFTABLES**. Dazu muss man eine .conf-Datei erstellen, in der alle Regeln festgelegt werden. nftables verwendet hier ein wenig ein anderes Aussehen als iptables.

3.8.3.1 nftables.conf konfigurieren

```

Filter
table inet filter {
    chain INPUT {
        type filter hook input priority filter
        policy drop
        ct state established,related accept
        iifname "lo" accept
        ip protocol icmp accept
        tcp dport 80 accept
        tcp dport 443 accept
        tcp dport 22 accept
    }

    chain FORWARD {
        type filter hook forward priority filter
        policy drop
        ct state established,related accept
        ip saddr 10.10.21.50 accept
    }
}

# NAT
table ip nat {
    chain PREROUTING {
        type nat hook prerouting priority dstnat
        policy accept
        tcp dport 3389 counter packets 0 bytes 0 dnat to 10.10.21.50:3389
    }

    chain POSTROUTING {
        type nat hook postrouting priority srcnat
        policy accept
        oifname "ens33" masquerade
    }
}
~

```

Abbildung 54: Firewall NFTABLES Konfiguration

3.8.3.2 nftables.conf ersetzen

Nun müssen Sie im Ordner „/etc“ die alte nftables.conf (dort stehen noch die Konfigurationen von iptables drinnen) durch die neue nftables.conf (obirger SS) ersetzen. Machen Sie vorher jedoch eine Kopie der alten nftables.conf-Datei, z.B.: nftables.conf.bak

3.8.3.3 iptables stoppen

Falls Sie Probleme mit iptables haben, weil sich eventuell irgendetwas in einem .service-File verändert haben und iptables nun neu laden will, führen Sie diesen Befehl aus:

```
root@debian:/etc# systemctl daemon-reload
```

Code 28: # systemctl daemon-reload

Deaktivieren Sie iptables mit diesem Befehl:

```
root@debian:/etc# systemctl disable --now iptables
```

Code 29: # systemctl disable --now iptables

3.8.3.4 nftables starten

Um nftables zu aktivieren, führen Sie diesen Befehl durch:

```
root@debian:/etc# systemctl enable --now nftables
```

Code 30: # systemctl enable --now nftables

Kontrollieren Sie auch, ob die Regeln der Firewall nun richtig konfiguriert sind.

```
root@debian:/etc# nft list ruleset
```

Code 31: # nft list ruleset

Der Output dieses Befehls sollten die eingestellten Regeln sein.

3.8.3.5 nftables stoppen

Mithilfe dieses Befehls kann man die NFTABLES-Regeln löschen. Beim nächsten Hochfahren werden die Regeln allerdings wieder ausgeführt, weil sie immer noch aktiviert sind.

```
root@debian:/etc# nft flush ruleset
```

Code 32: # nft flush ruleset

3.9 IPv6

3.9.1 Virtuelle Debian Server Maschine IPv6-Adresse zuweisen

Die Virtuelle Debian Maschine (also der Server) muss eine statische IPv6-Adresse bekommen (auf der richtigen Netzwerkkarte).

```
iface ens37 inet6 static
    address fc00::1
```

Abbildung 55: IPv6-Adresse Server (statisch) (/etc/network/interfaces)

3.9.2 Netzwerkkarte IPv6 erlauben

Damit IPv6 funktioniert, muss man in der „/etc/default/isc-dhcp-server“ einstellen, welche Interfaces (Netzwerkkarten) verwendet werden.

```
# Separate multiple interfaces
INTERFACESv4="ens37"
INTERFACESv6="ens37"
```

Abbildung 56: /etc/default/isc-dhcp-server

3.9.3 DHCPv6 konfigurieren

Konfigurieren Sie DHCPv6 indem Sie in der Datei /etc/dhcp/dhcpd6.conf zwei Dinge ändern.

- Schreiben Sie eine beliebige Domain in die Options hinein.

```
# Global definitions for name server address(es) and domain search list
option dhcp6.name-servers 3ffe:501:ffff:100:200:ff:fe00:3f3e;
option dhcp6.domain-search "felixnet.local";
```

Abbildung 57: /etc/dhcp/dhcpd6.conf

- Entkommentieren Sie am Ende der Datei das folgende Subnetz und geben Sie den Adressbereich ein:

```
# A third subnet behind a relay agent chain
subnet6 fc00:: /64 {
    range6 fc00::100 fc00::150;

    range6 fc00:: temporary;

    prefix6 fc00:: fc00:10:: /64;
}
```

Abbildung 58: /etc/dhcp/dhcpd6.conf

3.9.3.1 radvd installieren und konfigurieren

Laden Sie mit Aptitude das radvd Paket herunter. Erstellen Sie in „/etc“ eine Datei namens „radvd.conf“.

Eine Beispieldatei von radvd.conf finden Sie in „/usr/share/doc/radvd/examples/radvd.conf.example“.

zusätzliche Informationen: Durch die radvd-Konfiguration wird im Netzwerk fc00 eine stateful IP-Konfiguration vorgegeben.

```
interface ens37 {  
    AdvSendAdvert on;  
  
    AdvManagedFlag on;  
    AdvOtherConfigFlag on;  
  
    prefix fc00::/64 {  
        AdvOnLink on;  
        AdvAutonomous off;  
    };  
};
```

Abbildung 59: /etc/radvd.conf

3.9.3.2 Firewall anpassen

Damit man nun auch wirklich pingen kann, muss man in der NFTABLES Firewall-Konfiguration noch ein bisschen etwas umändern, nämlich 2 neue Zeilen (markiert) hinzufügen:

```
# Filter  
table inet filter {  
    chain INPUT {  
        type filter hook input priority filter  
        policy drop  
        iifname "lo" accept  
  
        icmp type { * } accept  
        icmpv6 type { * } accept  
  
        ct state established,related accept  
  
        tcp dport 80 accept  
        tcp dport 443 accept  
        tcp dport 22 accept  
    }  
  
    chain FORWARD {  
        type filter hook forward priority filter  
        policy drop  
        ct state established,related accept  
        ip saddr 10.10.21.50 accept  
    }  
}
```

Abbildung 60: Firewall anpassen

3.9.3.3 Windows überprüfen

Um sicherzustellen, dass IPv6-DHCP funktioniert, starten Sie die Virtuelle Windows Maschine und überprüfen Sie die IPv6-Adressen. Hier sollte nun eine Adresse aus dem angegebenen Adressbereich stehen.

```
Verbindungsspezifisches DNS-Suffix: felix.net
IPv6-Adresse. . . . . : fc00::150
Verbindungslokale IPv6-Adresse . : fe80::5d6:4a2f:2baf:fab8%6
IPv4-Adresse . . . . . : 10.10.21.50
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 10.10.21.1
```

Abbildung 61: Windows IPv6-Adresse

3.9.3.4 Ping

```
C:\Users\Felix>ping fc00::1

Ping wird ausgeführt für fc00::1 mit 32 Bytes Daten:
Antwort von fc00::1: Zeit=1ms
Antwort von fc00::1: Zeit=1ms
Antwort von fc00::1: Zeit=1ms
Antwort von fc00::1: Zeit=1ms

Ping-Statistik für fc00::1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms
```

Abbildung 62: IPv6-Adressen pingen

3.10 Apache2

Apache2 ist ein Webserver, der in unserem Fall auf der Debian Server Maschine laufen soll. Mithilfe dieses Webserver können wir überprüfen, ob das, was wir in der Theorie gelernt haben auch stimmt, nämlich: Muss man bei URLs wirklich eckige Klammern ([]) um die IPv6-Adresse herumschreiben, damit WWW das als IPv6-Adresse erkennt? Ansonsten würde es nämlich ein Problem geben, weil der Port bereits Doppelpunkte (:) als Trennzeichen verwendet.

Installieren Sie Apache2 mittels Aptitude und überprüfen Sie, ob Sie auf der Virtuellen Windows Maschine diesen Webserver erreichen.

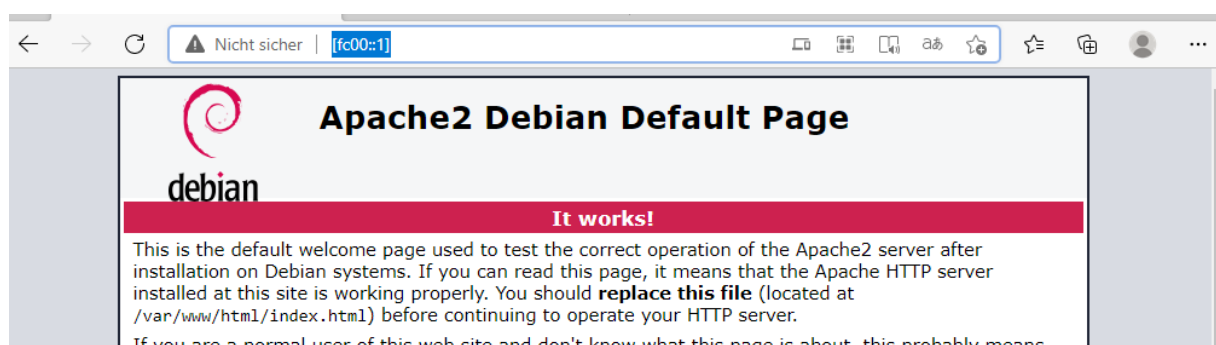


Abbildung 63: URL-Pfad IPv6

3.11 Samba

Samba ist das Standardprogramm für die Interoperabilität von Windows mit Linux und Unix. Seit 1992 bietet Samba sichere, stabile und schnelle Datei- und Druckdienste für alle Clients, die das SMB/CIFS-Protokoll verwenden, wie z.B. alle Versionen von DOS und Windows, OS/2, Linux und viele andere.

3.11.1 Installation

Als erstes muss man mithilfe von Aptitude das Samba-Paket installieren.

3.11.2 Shared Folder

Anschließend erstellen wir einen Media-Ordner. In diesem Ordner befinden sich später alle Dateien, die öffentlich geteilt werden wollen. Dieser Ordner bekommt alle Berechtigungen, sodass jeder darin herumschreiben, lesen und ausführen kann.

```
root@debian:/etc/samba# mkdir -p /media/samba/storage
root@debian:/etc/samba# useradd -U -r smbguest
root@debian:/etc/samba# chown smbguest:smbguest /media/samba/storage/
```

Abbildung 64: Shared Folder erstellen

3.11.3 Konfiguration

```
[global]
    workgroup = WORKGROUP
    map to guest = Bad User
    guest account = smbguest
    interfaces = 10.10.21.1/24 fc00::1/64

[public]
    path = /media/samba/storage/
    public = yes
    writable = yes
    browseable = yes
    comment = smb public share
    create mask = 666
    directory mask = 777
```

Abbildung 65: Samba public folder

3.11.4 Samba Service neu starten

Samba können Sie mit diesem Befehl neu starten:


zusätzliche Informationen: Das d am Ende steht bei Services immer für Daemon.

```
root@debian:/etc/samba# systemctl restart smbd
```

Code 33: # systemctl restart smbd

3.11.5 Unsichere Gastanmeldungen aktivieren

Bei Windows Education Versionen muss man anschließend noch unsichere Gastanmeldungen aktivieren, damit die Verbindung mit einem „\public“-Folder hergestellt werden kann.

Diese Aktion kann folgendermaßen durchgeführt werden:  + R drücken, damit ein unten links ein kleines Fenster aufpoppt, wo Sie gpedit.msc hineinschreiben. Das ist die schnellste Variante, die lokalen Gruppenrichtlinien bei Windows zu öffnen.

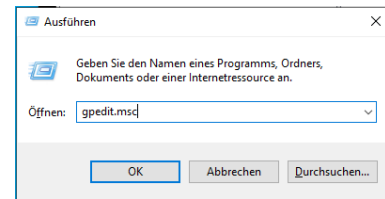


Abbildung 66: gpedit.msc

Anschließend klicken Sie die im Screenshot gelb markierten Ordner an und aktivieren Sie schlussendlich die unsicheren Gastanmeldungen. Somit sollte der UNC-Pfad funktionieren.

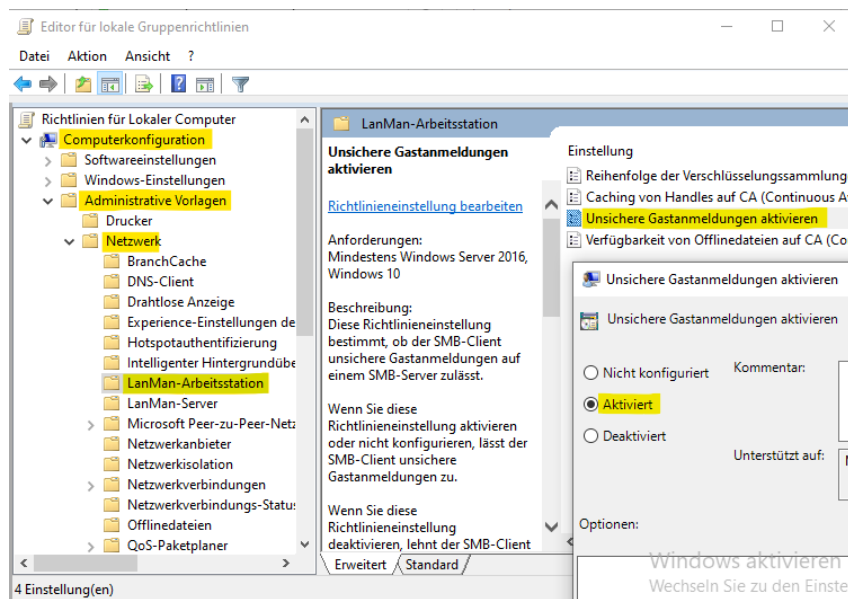


Abbildung 67: unsichere Gastanmeldungen aktivieren

3.11.6 Fileshare funktioniert

Um zu überprüfen, ob der Fileshare funktioniert, gehen Sie zur Virtuellen Windows Maschine und tippen Sie im Explorer die IPv6-Adresse der Virtuellen Debian Server Maschine mit Bindestrichen (-) statt Doppelpunkten (:) ein. Anschließend sollten Sie Zugriff auf den Shared Folder erhalten.

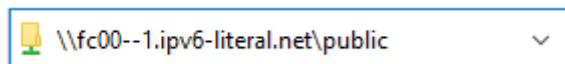


Abbildung 68: IPv6-UNC-Pfad

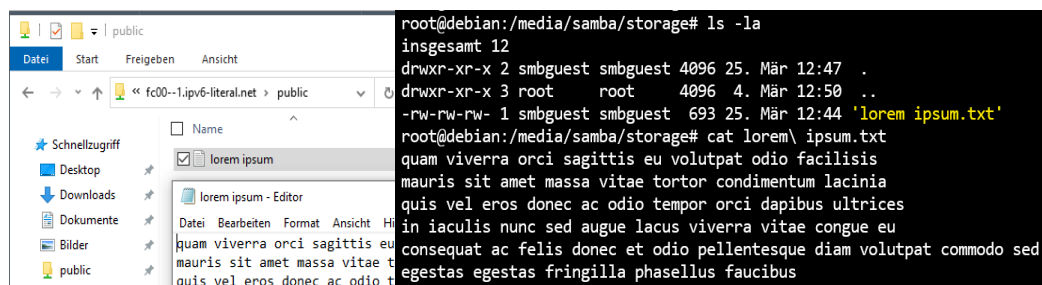


Abbildung 69: SAMBA funktioniert

3.11.7 Firewallrules anpassen

Damit die Firewall auch eine verbindungsorientierte TCP-Verbindung auf Port 445 zulässt, müssen Sie noch die grau hinterlegte Zeile bei Ihren NFTABLES-Rules hinzufügen:

```
# Filter
table inet filter {
    chain INPUT {
        type filter hook input priority filter
        policy drop
        iifname "lo" accept

        icmp type { * } accept
        icmpv6 type { * } accept

        ct state established,related accept

        tcp dport 80 accept
        tcp dport 443 accept
        tcp dport 22 accept
        tcp dport 445 accept
    }

    chain FORWARD {
        type filter hook forward priority filter
        policy drop
        ct state established,related accept
        ip saddr 10.10.21.50 accept
    }
}
```

Abbildung 70: Firewall anpassen

3.12 DNS-Server

3.12.1 Konfiguration

3.12.1.1 Options-Datei

Konfigurieren Sie die „/etc/bind/named.conf.options“ – Datei, damit DNS funktioniert. Dort können Sie auch einstellen, dass Sie einen Forwarder benötigen.

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        1.1.1.1;
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on      { 127.0.0.1; 10.10.21.1; };
    listen-on-v6   { ::1; fc00::1; };
};
```

Abbildung 71: /etc/bind/named.conf.options

3.12.1.2 named.conf.local

Damit die Zonendateien auch gefunden werden können, müssen Sie in der named.conf.local die Zonen einbinden.

```
zone "schneider.local" {
    type master;
    file "/etc/bind/zones/db.schneider.local";
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.c.f.ip6.arpa" {
    type master;
    file "/etc/bind/zones/db.fc00.ip6.arpa";
};

zone "21.10.10.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.21.10.10.in-addr.arpa";
};
```

Abbildung 72: /etc/bind/named.conf.local

3.12.1.3 Forward Zone

In der Forward Zone (db.schneider.local) stehen alle Umwandlungen von Namen in IP-Adressen drinnen.

```

; BIND data file for schneider.local
;
$TTL      86400
$ORIGIN    schneider.local.
@         IN      SOA      ns.schneider.local. root.schneider.local. (
                                04           ; Serial
                                604800        ; Refresh
                                86400         ; Retry
                                2419200       ; Expire
                                604800 )      ; Negative Cache TTL
;
@         IN      NS       ns
@         IN      MX       200      mail
@         IN      MX       100      mail6
;
; IPv4
;
ns        IN      A        10.10.21.1
www       IN      CNAME    ns
mail      IN      CNAME    ns
;
; IPv6
;
ns6       IN      AAAA     fc00::1
www6      IN      CNAME    ns6
mail6     IN      CNAME    ns6
;
; intern clients
;
win       IN      A        10.10.21.50
win6      IN      AAAA     fc00::150
;
; extern clients
;
deb       IN      A        192.168.157.129

```

Abbildung 73: /etc/bind/zones/db.schneider.local

Wie man sehen kann, funktioniert diese Zone:

```

root@debian:/etc/bind/zones# named-checkzone schneider.local db.schneider.local
zone schneider.local/IN: schneider.local/MX 'mail6.schneider.local' is a CNAME (illegal)
zone schneider.local/IN: schneider.local/MX 'mail.schneider.local' is a CNAME (illegal)
zone schneider.local/IN: loaded serial 4
OK

```

Abbildung 74: Forward-Zone funktioniert

<pre> > ns Server: ns.schneider.local Address: fc00::1 Name: ns.schneider.local Address: 10.10.21.1 </pre>	<pre> > www.schneider.local Server: ns.schneider.local Address: fc00::1 Name: ns.schneider.local Address: 10.10.21.1 Aliases: www.schneider.local </pre>	<pre> > mail6.schneider.local Server: ns.schneider.local Address: fc00::1 Name: ns6.schneider.local Address: fc00::1 Aliases: mail6.schneider.local </pre>
--	--	--

Abbildung 75: Überprüfung

3.12.1.4 IPv4 Reversed Lookup Zone

In der IPv4 Reversed Lookup Zone (db.21.10.10.in-addr.arpa) stehen alle Umwandlungen von IP-Adressen in Namen drinnen. Diese soll dann ungefähr so aussehen:

```
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
$ORIGIN 21.10.10.in-addr.arpa.
@        IN      SOA     ns.schneider.local. root.schneider.local. (
                                02           ; Serial
                                604800        ; Refresh
                                86400         ; Retry
                                2419200       ; Expire
                                604800 )      ; Negative Cache TTL
;
@        IN      NS      ns.schneider.local.
;
1        IN      PTR      ns.schneider.local.
50       IN      PTR      ns.schneider.local.
```

Abbildung 76: /etc/bind/zones/db.21.10.10.in-addr.arpa

Wie man sehen kann, funktioniert die IPv4 Reverse Lookup Zone ebenfalls:

```
root@debian:/etc/bind/zones# named-checkzone 21.10.10.in-addr.arpa db.21.10.10.in-addr.arpa
zone 21.10.10.in-addr.arpa/IN: loaded serial 2
OK
root@debian:/etc/bind/zones#
```

Abbildung 77: IPv4 Reversed Lookup Zone funktioniert

<pre>> 10.10.21.1 Server: ns.schneider.local Address: fc00::1 Name: ns.schneider.local Address: 10.10.21.1</pre>	<pre>> 10.10.21.50 Server: ns.schneider.local Address: fc00::1 Name: ns.schneider.local Address: 10.10.21.50</pre>
--	--

Abbildung 78: Überprüfung

3.12.1.6 DHCP anpassen

In der „/etc/dhcp/dhcpd.conf“ – Datei müssen Sie den Domain-Namen eintragen:

```
# option definitions common to all supported networks...  
option domain-name "schneider.local";  
option domain-name-servers 8.8.8.8, 1.1.1.1;
```

Abbildung 82: /etc/dhcp/dhcpd.conf

Auch bei IPv6 müssen Sie den Server eintragen: „/etc/dhcp/dhcpd6.conf“

```
# Global definitions for name server address(es) and domain search list  
option dhcp6.name-servers fc00::1;  
option dhcp6.domain-search "schneider.local";
```

Abbildung 83: /etc/dhcp/dhcpd6.conf

3.12.2 DNS-Server selbst nutzen

3.12.2.1 `/etc/network/interfaces`

Damit der DNS-Server selbst auch die Zonendateien am DNS-Server nutzen kann, muss man in der Datei „`/etc/network/interfaces`“ die beiden markierten Zeilen hinzufügen, damit in der „`/etc/resolv.conf`“ – Datei vom DNS-Server der Server selbst eingetragen ist.

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo ens33 ens37
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

iface ens37 inet static
    address 10.10.21.1
    netmask 255.255.255.0
    dns-nameserver 127.0.0.1
    dns-search schneider.local

iface ens37 inet6 static
    address fc00::1
    netmask 64
```

Abbildung 84: `/etc/network/interfaces`

3.12.2.2 `resolvconf` installieren

Installieren Sie den Manager der Datei „`/etc/resolv.conf`“ → `resolvconf`

```
root@debian:~# aptitude install resolvconf
```

Code 34: `# aptitude install resolvconf`

3.12.2.3 `/etc/resolv.conf`

Überprüfen Sie die Datei „`/etc/resolv.conf`“.

```
nameserver 127.0.0.1
search schneider.local localdomain
```

Abbildung 85: `/etc/resolv.conf`

Nun sollte der Server selbst auch DNS-Abfragen auflösen können.

4 Notizen

4.1 DNS

zone: schneider.local.

router: www.schneider.local –ipv4

www6.schneider.local –ipv6

mail.schneider.local

mail6.schneider.local

windows:

win.schneider.local

win6.schneider.local

2te Debian Rechner:

deb.schneider.local

deb6.schneider.local

Paket: bind9

/etc/bind/named.conf.local

Zonendateien: /etc/bind/zones/db.schneider.local

 /etc/bind/zones/21.10.10.in-addr.arpa

 /etc/bind/zones/21.168.192.in-addr.arpa

/etc/bind/named.conf.options --forwarder

5 Abbildungsverzeichnis

Abbildung 1: ISO Datei auswählen	4
Abbildung 2: Hardwareeinstellungen	5
Abbildung 3: Medium einbinden/laden.....	6
Abbildung 4: Name der Domain eingeben	7
Abbildung 5: Shadow-Passwörter	7
Abbildung 6: Übersicht – Festplatte partitionieren.....	8
Abbildung 7: Partitionstabelle.....	8
Abbildung 8: Größe der Partition	8
Abbildung 9: Partitionseinstellungen	9
Abbildung 10: Kernel des Basissystems	9
Abbildung 11: Dienste auswählen	10
Abbildung 12: EFI Erzwingung deaktivieren.....	10
Abbildung 13: Root-Anmeldung möglich	10
Abbildung 14: sources.list	11
Abbildung 15: Aptitude	12
Abbildung 16: nach openssh suchen.....	12
Abbildung 17: Putty Configuration	13
Abbildung 18: ip -c a Ausgabe	15
Abbildung 19: route -n Ausgabe	15
Abbildung 20: more /etc/resolv.conf Ausgabe	15
Abbildung 21: more/etc/network/interfaces Ausgabe	16
Abbildung 22: Beispiel für Ausgabe von # tail -f /var/log/syslog	16
Abbildung 23: LAN Segment	17
Abbildung 24: /etc/network/interfaces	18
Abbildung 25: IPv4-Adressen Einstellungen Windows.....	19
Abbildung 26: ipconfig	19
Abbildung 27: Firewall deaktivieren	20
Abbildung 28 (links): Debian – ping Windows	20
Abbildung 29 (rechts): Windows – ping Debian	20
Abbildung 30: Pfad der Virtuellen Debian Maschine finden	21
Abbildung 31: Virtuelle Debian Maschine - Datei	21
Abbildung 32: LAN-Segment entfernen	21
Abbildung 33: ip.php.....	22
Abbildung 34: Netzwerkaufbau NAT	23
Abbildung 35: IP-Tabellen-Einstellungen	23
Abbildung 36: Webserver erreichen NAT	24
Abbildung 37: sysctl.conf - net.IPv4.ip_forward=1	25
Abbildung 38: Route-Einstellungen von Virtueller Debian Maschine.....	25
Abbildung 39: Route-Einstellungen von Virtuelle Debian Klon Maschine	26
Abbildung 40: Virtuelle Windows Maschine DNS-Server	27
Abbildung 41: Netzwerkkarte DHCP einstellen.....	28
Abbildung 42: Subnetz DHCP einstellen	28
Abbildung 43: IP-Adresse automatisch beziehen.....	29
Abbildung 44: Ausgabe der Interneteinstellungen Windows	29
Abbildung 45: Syslog-Datei Ausgabe	29
Abbildung 46: dhcpd.conf mit fixer Adresse	30
Abbildung 47: IP-Konfiguration Virtuelle Windows Maschine	30
Abbildung 48: iptables-Konfiguration speichern.....	31
Abbildung 49: iptables-Konfiguration laden	31
Abbildung 50: Firewall iptables Befehle	32

Abbildung 51: Datei mit Konfiguration (iptables)	32
Abbildung 52: /etc/systemd/system/iptables.service	33
Abbildung 53: not-ping Debian.....	33
Abbildung 54: Firewall NFTABLES Konfiguration	34
Abbildung 55: IPv6-Adresse Server (statisch) (/etc/network/interfaces).....	35
Abbildung 56: /etc/default/isc-dhcp-server	36
Abbildung 57: /etc/dhcp/dhcpd.conf	36
Abbildung 58: /etc/dhcp/dhcpd.conf	36
Abbildung 59: /etc/radvd.conf	37
Abbildung 60: Firewall anpassen	37
Abbildung 61: Windows IPv6-Adresse	38
Abbildung 62: IPv6-Adressen pingen	38
Abbildung 63: URL-Pfad IPv6	38
Abbildung 64: Shared Folder erstellen.....	39
Abbildung 65: Samba public folder.....	39
Abbildung 66: gpedit.msc.....	40
Abbildung 67: unsichere Gastanmeldungen aktivieren	40
Abbildung 68: IPv6-UNC-Pfad	40
Abbildung 69: SAMBA funktioniert	40
Abbildung 70: Firewall anpassen	41
Abbildung 71: /etc/bind/named.conf.options.....	42
Abbildung 72: /etc/bind/named.conf.local	42
Abbildung 73: /etc/bind/zones/db.schneider.local	43
Abbildung 74: Forward-Zone funktioniert	43
Abbildung 75: Überprüfung.....	43
Abbildung 76: /etc/bind/zones/db.21.10.10.in-addr.arpa	44
Abbildung 77: IPv4 Reversed Lookup Zone funktioniert	44
Abbildung 78: Überprüfung.....	44
Abbildung 79: /etc/bind/zones/db.fc00.ip6.arpa	45
Abbildung 80: IPv6 Reversed-Lookup Zone funktioniert.....	45
Abbildung 81: Überprüfung.....	45
Abbildung 82: /etc/dhcp/dhcpd.conf	46
Abbildung 83: /etc/dhcp/dhcpd6.conf	46
Abbildung 84: /etc/network/interfaces	47
Abbildung 85: /etc/resolv.conf.....	47

6 Codeverzeichnis

# nano sources.list.....	11
# apt-get update.....	11
# apt-get install aptitude	11
# aptitude.....	11
# su - root.....	14
# nano sshd_config.....	14
# /etc/init.d/ssh restart.....	14
# ip -c a.....	14
# route -n	15
# more /etc/resolv.conf	15
# more /etc/network/interfaces	15
# tail -f /var/log/syslog.....	16
# nano /etc/network/interfaces.....	17
# /etc/init.d/networking restart.....	18
# service networking restart.....	18
# ipconfig	19
# nano /var/www/html/ip.php.....	22
# iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE.....	23
# iptables -t nat -L	24
# sysctl -p	25
# route add -net 10.10.21.0/24 gw 192.168.157.128	25
# systemctl restart isc-dhcp-server.service	28
# ipconfig /all	29
# iptables-restore iptables.rules.....	32
# systemctl daemon-reload	33
# systemctl start iptables.service	33
# systemctl enable --now iptables.service	33
# systemctl daemon-reload	35
# systemctl disable --now iptables	35
# systemctl enable --now nftables	35
# nft list ruleset	35
# nft flush ruleset	35
# systemctl restart smbd	39
# aptitude install resolvconf	47

7 Ergebnisse

Funktionierender Debian Server und angeschlossenen Windows und Debian Client. Folgende Protokolle / Programme wurden verwendet:

- DHCP (IPv4 + IPv6)
- Firewall (iptables + nftables)
- Apache2 + PHP
- Samba
- DNS

8 Kommentar

Die Konfiguration der Firewall haben Clemens Schlipfinger und ich nicht mit einem Shell-Script gemacht, sondern mit einem SystemD-Service.