

Setup Virtual Machines

- Netzwerkkarte 1: Bridge - automatische Erkennung
- Netzwerkkarte 2: Privat auf meinem Mac
- net-tools auf allen installieren
- tcpdump auf allen installieren
- iptables auf allen installieren
- iptables-persistent auf allen installieren

```
apt update && apt upgrade -y
```

```
apt install net-tools tcpdump iptables iptables-persistent -y
```

1. Firewall erstellen

1. IP: 10.10.10.2
2. ssh installieren

3. Webserver erstellen

1. IP: 10.10.10.3
2. apache2 installieren

4. Adminserver erstellen

1. IP: 10.10.10.4
2. ssh installieren

Nach Software-Installation die Interfaces ins Internet auf Webserver und Admin deaktivieren!

Netzwerkkonfiguration (/etc/network/interfaces)

```
# Webserver
```

```
auto ens256
iface ens256 inet static
    address 10.10.10.3
    gateway 10.10.10.2
    netmask 255.255.255.0
```

```
# Firewall
```

```
auto ens256
iface ens256 inet static
    address 10.10.10.2
    netmask 255.255.255.0
```

Adminserver

```
auto ens256
iface ens256 inet static
    address 10.10.10.4
    gateway 10.10.10.2
    netmask 255.255.255.0
```

Firewall-Regeln

Firewall-Maschine:

```
iptables -A PREROUTING -t nat -i ens256 -p tcp --dport 80 -j DNAT --to 10.10.10.3:80
```

```
iptables -A PREROUTING -t nat -i ens256 -p tcp --dport 22 -j DNAT --to 10.10.10.4:22
```

Commands

Enable ip-forwarding (auf der Firewall):

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Persistieren vom ip-forwarding: In Datei /etc/sysctl.conf

netstat:

```
netstat -rn
```

tcpdump:

```
tcpdump -i <INTERFACE> port <PORT>
```

iptables Regeln anzeigen:

```
iptables -L PREROUTING -t nat
```

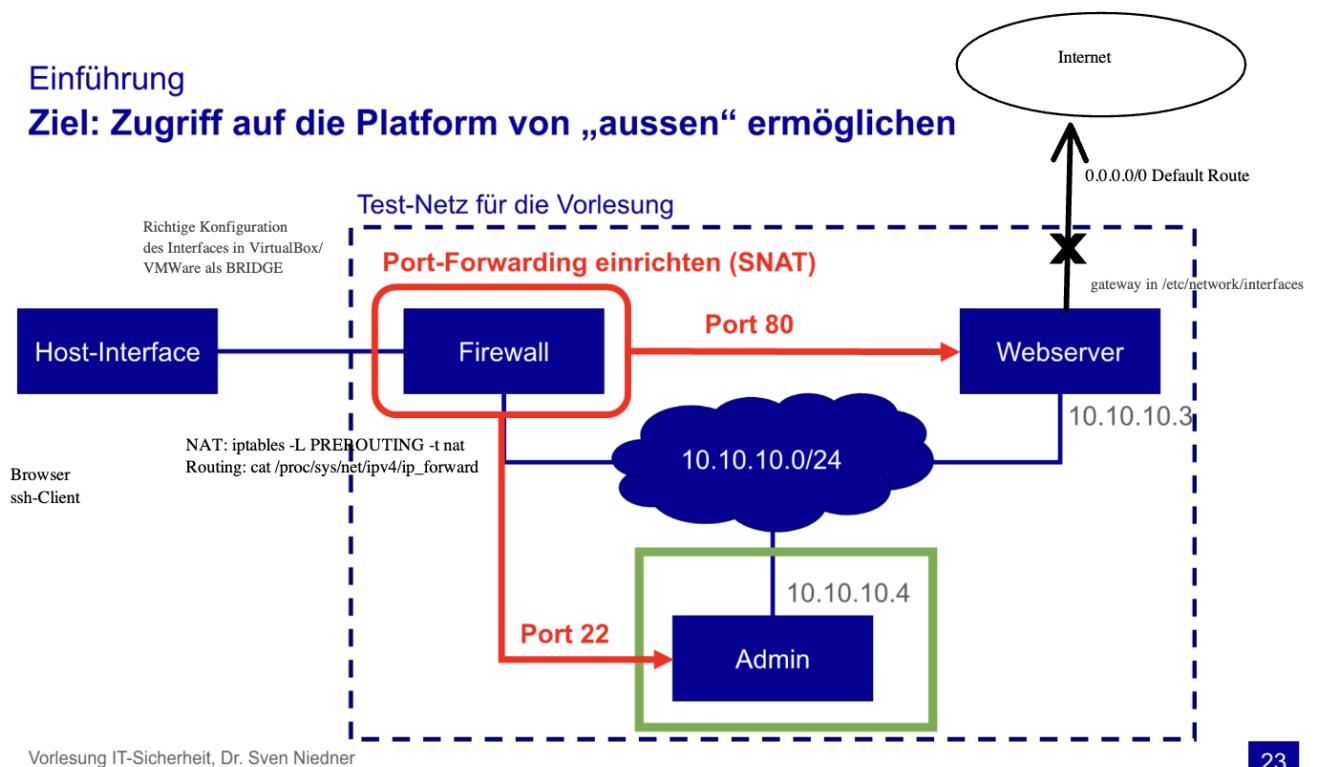
VMs Internet geben (auf Firewall):

```
iptables -t nat -A POSTROUTING -o <PUBLIC-INTERFACE-NAME> -j MASQUERADE
```

Schaubild

Einführung

Ziel: Zugriff auf die Plattform von „ausen“ ermöglichen



Vorlesung IT-Sicherheit, Dr. Sven Niederer

23

Revision #12

Created 16 August 2024 07:32:04 by Max

Updated 16 August 2024 12:04:05 by Max