

# Firewall connection

ssh connection to system

```
~ via @ v20.6.1
> ssh 172.18.10.177
The authenticity of host '172.18.10.177 (172.18.10.177)' can't be established.
ECDSA key fingerprint is SHA256:C6ktLibweBUwA5tmuo3DZ8c2qbLdcbUpy+DXXBmM+Og.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.18.10.177' (ECDSA) to the list of known hosts.
jakob@172.18.10.177's password:
>>> ~
>>> ~
```

bash

1

ssh 172.18.10.177

## setup firewall

add a rule to allow tcp a tcp connection from host system

```
>>> ~ sudo ufw allow proto tcp from 172.18.9.39 to 172.18.10.177
Rules updated
>>> ~ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
>>> ~
```

```
sudo ufw allow proto tcp from
172.18.9.39 to 192.168.56.103
```

# applications

## netcat

simulate a server on port 25565 using netcat

```
>>> ~ netcat -l 25565
```

```
netcat -l 25565
```

## rules

set a rule to allow ssh connections  
(will skip if rule already exists)

```
>>> ~ sudo ufw allow ssh  
Skipping adding existing rule  
Rules updated (v6)  
>>> ~
```

```
sudo ufw allow ssh
```

set a rule to allow tcp connections on port 25565

```
>>> ~ sudo ufw allow 25565/tcp  
Rules updated  
Rules updated (v6)  
>>> ~
```

```
sudo ufw allow 25565/tcp
```

enable logging

```
>>> ~ sudo ufw logging on
Logging enabled
>>> ~ sudo ufw logging high
Logging enabled
>>> ~ |
```

```
sudo ufw logging on
```

```
sudo ufw logging high
```

## enable the ufw

```
sudo ufw enable
```

## nmap

send nmap command to test all ports on the server

```
PS C:\Users\jakob> nmap -p- -Pn 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-19 11:32 W. Europe Standard Time
Nmap scan report for 192.168.56.103
Host is up (0.0034s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
5355/tcp   open  llmnr
5432/tcp   open  postgresql
25565/tcp  open  minecraft
MAC Address: 08:00:27:B9:97:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.93 seconds
PS C:\Users\jakob>
```

```
nmap -p- -Pn 192.168.56.103
```

## logs

```
>>> journalctl | grep -i ufw
Dez 19 12:02:39 jakob-archcraft dbus-daemon[344]: [system] Activating via systemd: service name='org.freedesktop.home1'
unit='dbus-org.freedesktop.home1.service' requested by ':1.45' (uid=0 pid=1900 comm="sudo ufw logging on")
Dez 19 12:02:42 jakob-archcraft sudo[1900]:    jakob : TTY=pts/2 ; PWD=/home/jakob ; USER=root ; COMMAND=/usr/bin/ufw lo
gging on
Dez 19 12:03:19 jakob-archcraft dbus-daemon[344]: [system] Activating via systemd: service name='org.freedesktop.home1'
unit='dbus-org.freedesktop.home1.service' requested by ':1.46' (uid=0 pid=1943 comm="sudo ufw disable")
Dez 19 12:03:19 jakob-archcraft sudo[1943]:    jakob : TTY=pts/2 ; PWD=/home/jakob ; USER=root ; COMMAND=/usr/bin/ufw di
sable
Dez 19 12:03:24 jakob-archcraft dbus-daemon[344]: [system] Activating via systemd: service name='org.freedesktop.home1'
unit='dbus-org.freedesktop.home1.service' requested by ':1.47' (uid=0 pid=2119 comm="sudo ufw logging on")
Dez 19 12:03:24 jakob-archcraft sudo[2119]:    jakob : TTY=pts/2 ; PWD=/home/jakob ; USER=root ; COMMAND=/usr/bin/ufw lo
gging on
Dez 19 12:03:39 jakob-archcraft dbus-daemon[344]: [system] Activating via systemd: service name='org.freedesktop.home1'
unit='dbus-org.freedesktop.home1.service' requested by ':1.48' (uid=0 pid=2141 comm="sudo ufw logging high")
Dez 19 12:03:39 jakob-archcraft sudo[2141]:    jakob : TTY=pts/2 ; PWD=/home/jakob ; USER=root ; COMMAND=/usr/bin/ufw lo
gging high
>>> ~ |
```

## Bonus

go to sshd\_config

```
sudo nano /etc/ssh/sshd_config
```

## disable root login

change PermitRootLogin to no

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

## enable PubkeyAuthentication

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
```

## disable PasswordAuthentication

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

make connection over ssh  
keys

generate key on host

```
PS C:\Users\jakob> ssh-keygen.exe
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\jakob\.ssh/id_rsa):
C:\Users\jakob\.ssh/id_rsa already exists.
Overwrite (y/n)? n
PS C:\Users\jakob>
```

ssh-keygen.exe

## copy key to server

```
PS C:\Users\jakob> cat C:\Users\jakob\.ssh\id_rsa.pub | ssh 192.168.56.103 "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_
keys"
jakob@192.168.56.103's password:
PS C:\Users\jakob>
```

```
cat C:\Users\jakob\.ssh\id_rsa.pub |
ssh 192.168.56.103 "mkdir -p ~/.ssh
&& cat >> ~/.ssh/authorized_keys"
```

## change port of ssh

in sshd\_config

```
# default value.
|
Port 4
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

## restart ssh

```
systemctl reboot ssh
```

## connect

```
~ via 📶 v20.6.1  
> ssh -p 4 192.168.56.103  
>>> 📁 ~
```

```
ssh -p 4 192.168.56.103
```

## only allow internal connection to port 25565

```
>>> 📁 ~ sudo ufw allow from 192.168.56.0/24 to any port 25565  
[sudo] password for jakob:  
Rules updated  
>>> 📁 ~
```

```
sudo ufw allow from 192.168.56.0/24  
to any port 25565
```

## server with port 25565 running on special user

```
>>> 📁 ~ sudo useradd -s /usr/sbin/nologin server25565  
>>> 📁 ~ sudo -u server25565 nc -l 25565  
|
```

```
sudo useradd -s /usr/sbin/nologin  
server25565
```

```
sudo -u server25565 nc -l 25565
```