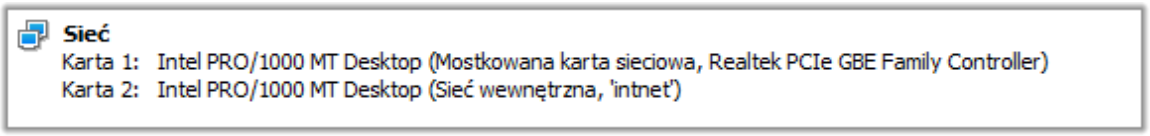
Serwer SSH

1. Na maszynie z US przywracamy czystą migawkę (może być ta z konfiguracji kart sieciowych), **pierwszą sieciówkę** konfigurujemy jako **zmostkowaną**, **drugą** jako **wewnętrzną intnet** (tak jak w poprzednim ćwiczeniu)



2. Przygotowujemy sobie jakąś drugą maszynę na testy (7,10, XP) sieciówka **wewnetrzna intnet**
3. Uruchamiamy Ubuntu, konfigurujemy kartę sieciową (tak aby adresacja pasowała do naszej sieci domowej) i **końcówka adresu IP** to był **nasz numer z dziennika**. Druga sieciówka to 192.168.X.1/24. U mnie niech to będzie:

   pierwsza sieciówka

   IP:10.39.100.X

   M:255.0.0.0

   B:10.0.0.1

   DNS:8.8.8.8

   druga sieciówka:

   IP:192.168.X.1

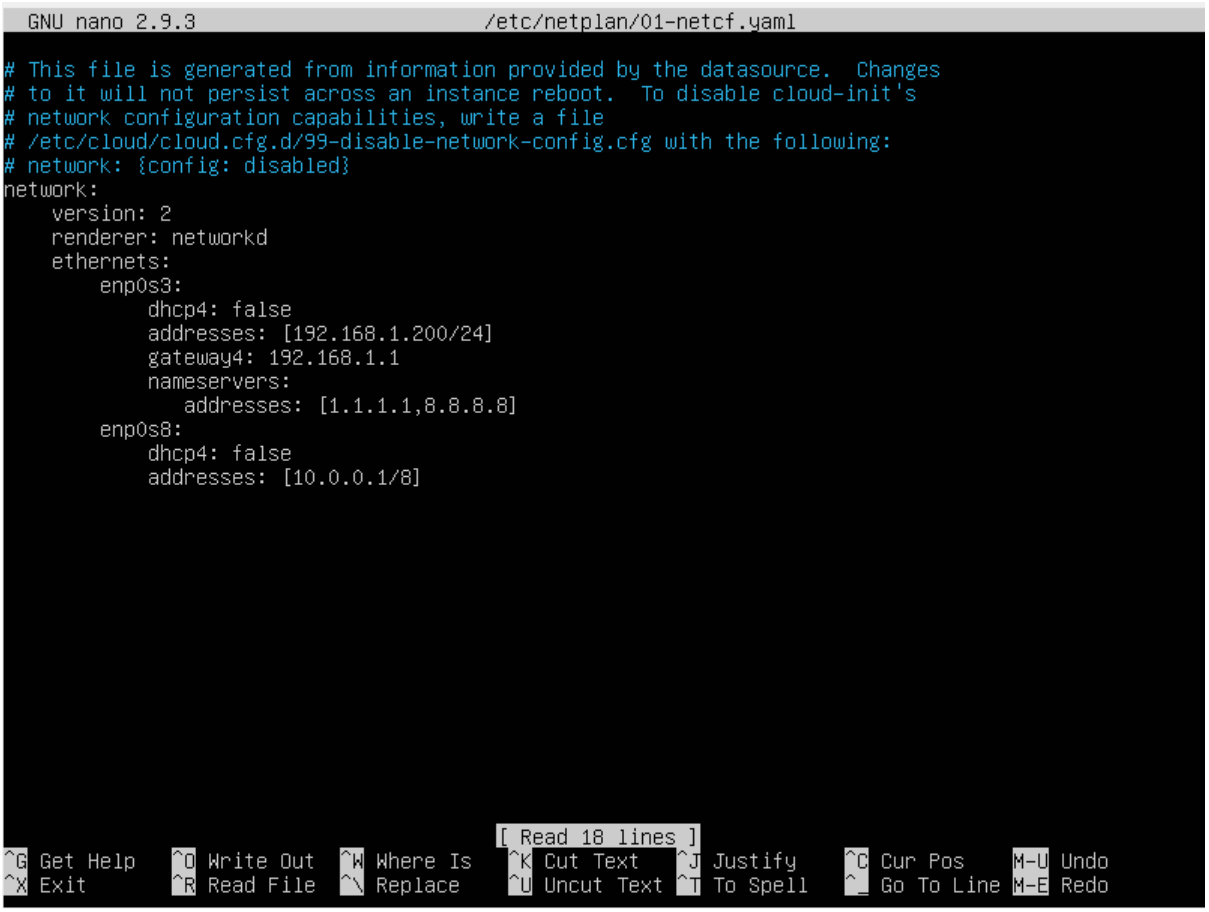
   M:255.255.255.0

   cd /etc/netplan/

   nano 01-netcf.yaml

   modyfikujemy ustawienia

   netplan apply



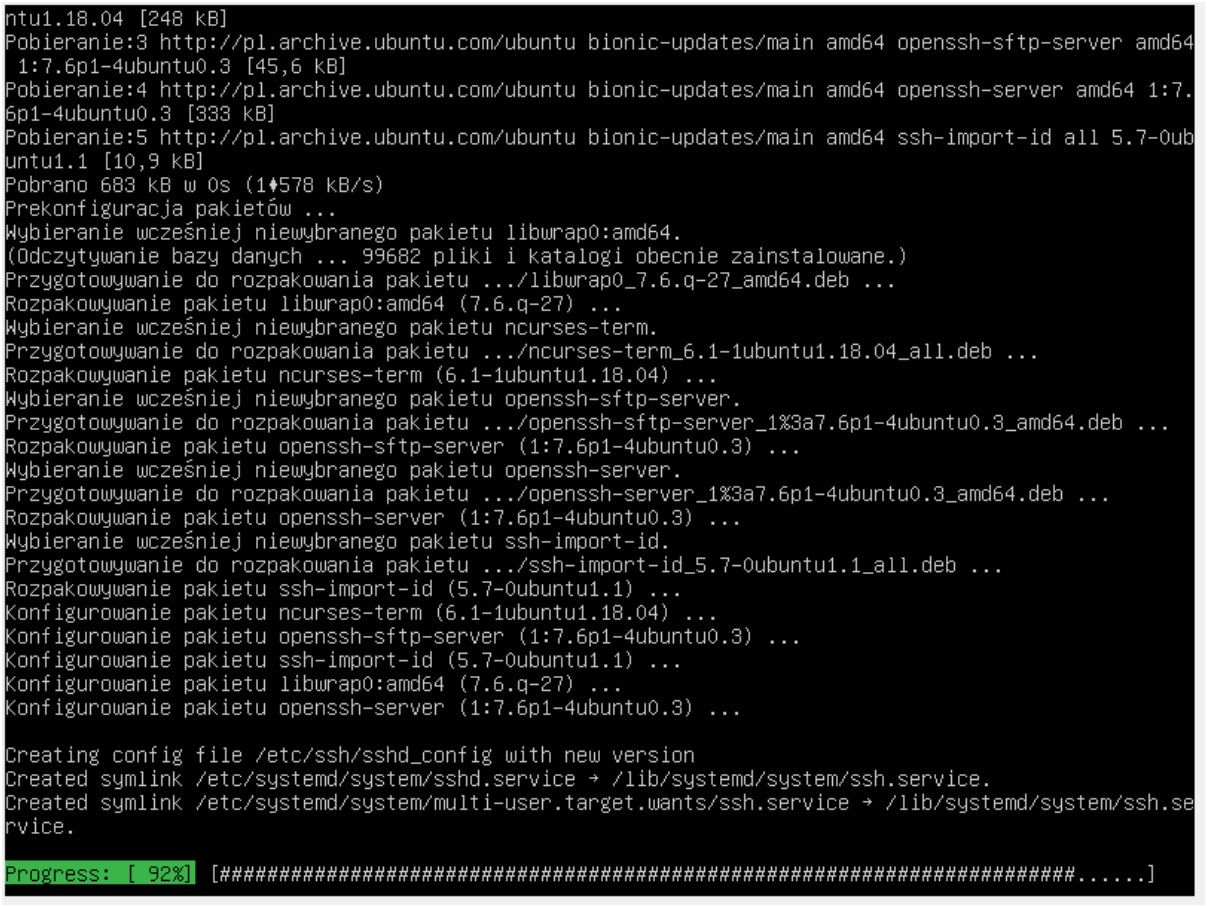
4. Uaktualniamy liste zawartości repozytoriów przed instalacją serwera SSH
(od Ubuntu 16.04 w górę możemy używać apt update zamiast apt-get update, tak samo przy instalacji wystarczy apt install zamiast apt-get install)

apt update

```
root@jkubuntu:/etc/netplan# apt update
Stary:1 http://pl.archive.ubuntu.com/ubuntu bionic InRelease
Stary:2 http://pl.archive.ubuntu.com/ubuntu bionic-updates InRelease
Stary:3 http://pl.archive.ubuntu.com/ubuntu bionic-backports InRelease
Stary:4 http://pl.archive.ubuntu.com/ubuntu bionic-security InRelease
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
38 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@jkubuntu:/etc/netplan#
```

5. Instalujemy serwer ssh - użyjemy pakietu **openssh-server**

   apt install openssh-server

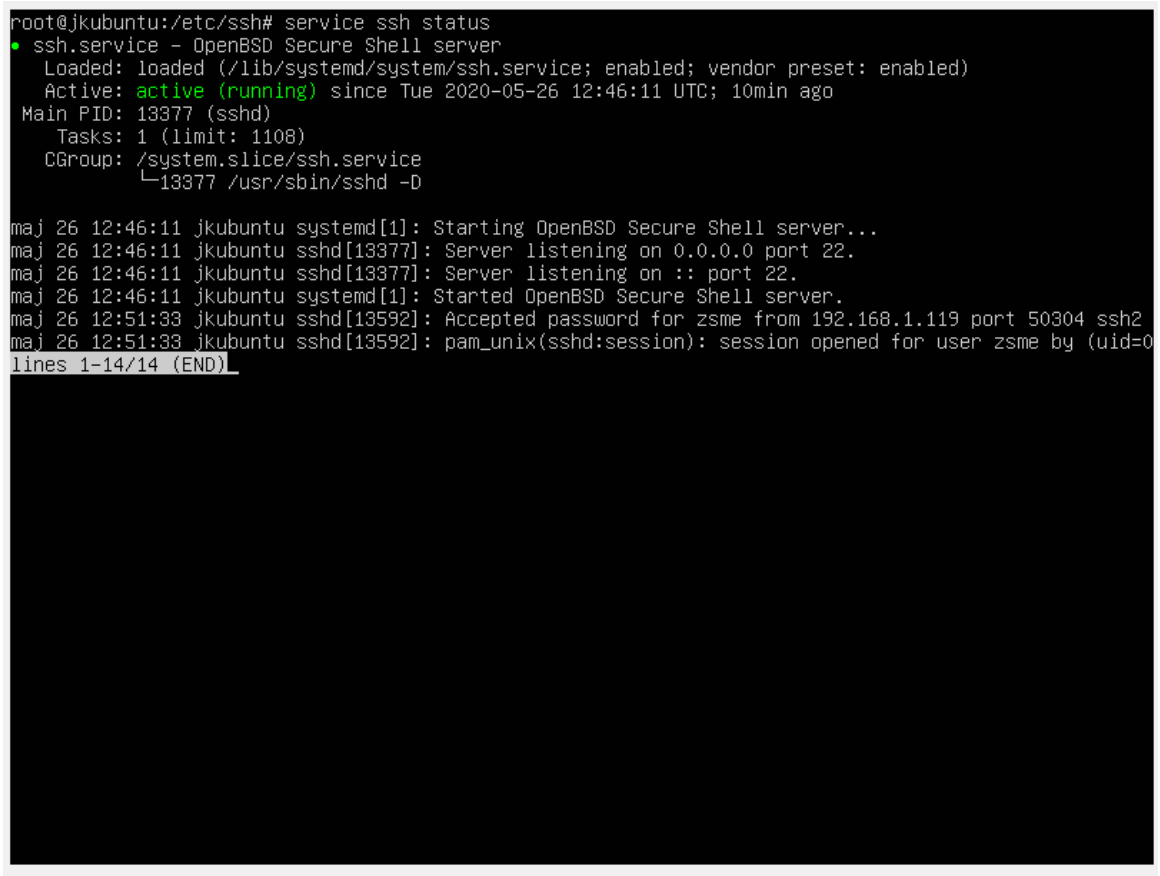


(jak widzimy, polecenie apt install pokazuje nam pasek postępu instalacji)

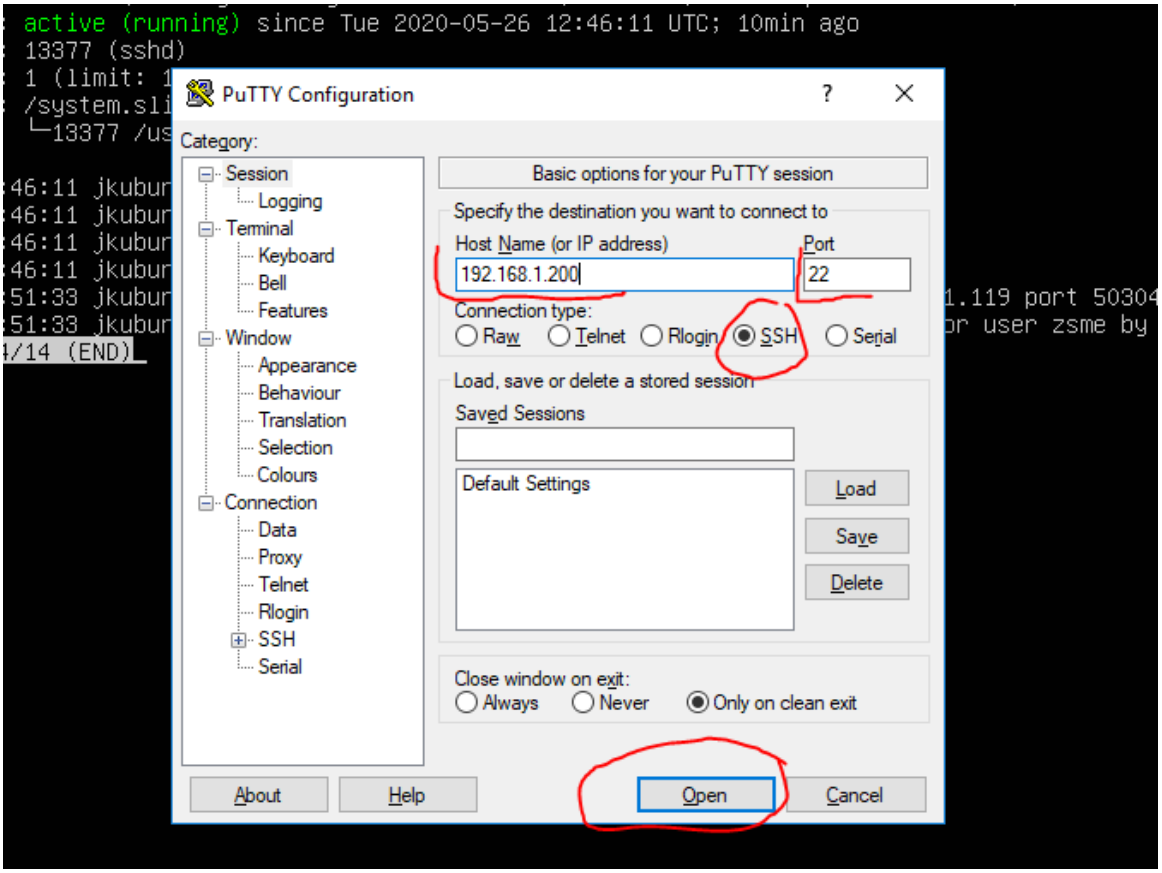
6. Nasz serwer zaraz po instalacji powinien działać i pozwalać na podłączenie się na domyślnym 22 porcie. Możemy to sprawdzić przy pomocy polecania:

   service ssh status
   lub
   systemctl status ssh

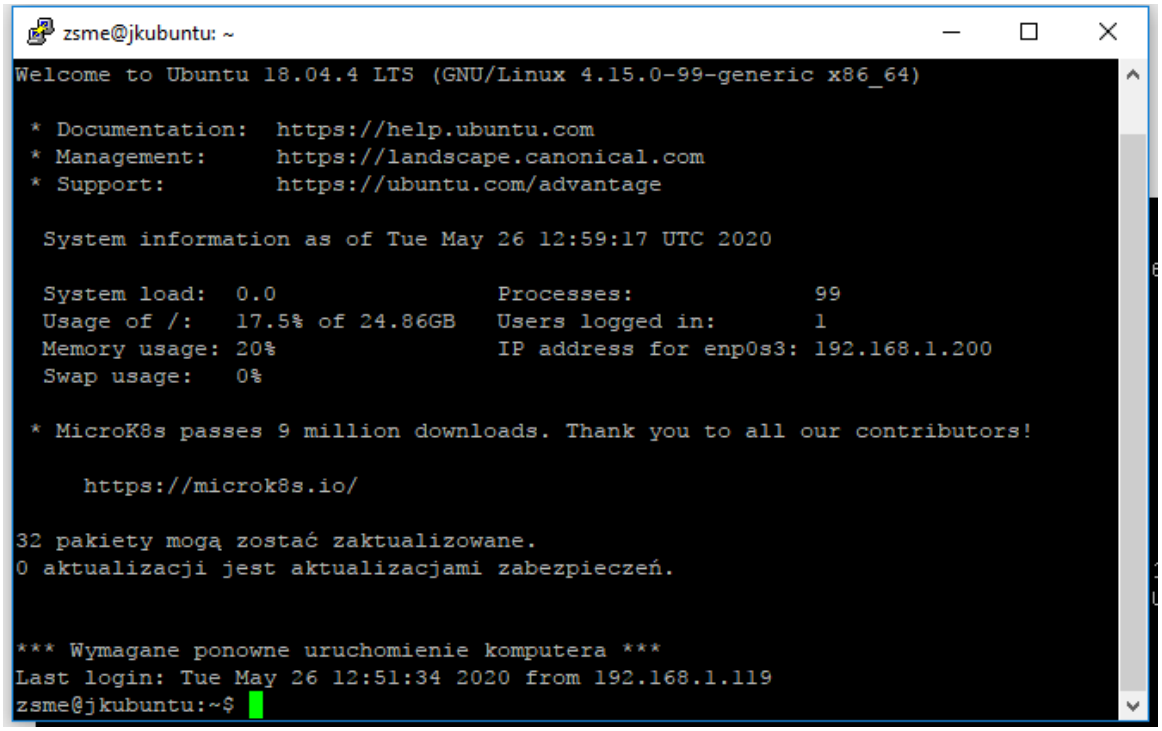
(żeby wyjść z polecenia używamy Ctrl + C)



7. Powinniśmy być się w stanie podłączyć na adres naszego serwera na domyślnym 22 porcie. Uruchamiamy Putty i zestawiamy połączenie:



i po podłączeniu i zalogowaniu:



8. Konfiguracja naszego serwera SSH znajduje się w katalogu **/etc/ssh** w pliku **sshd_config**

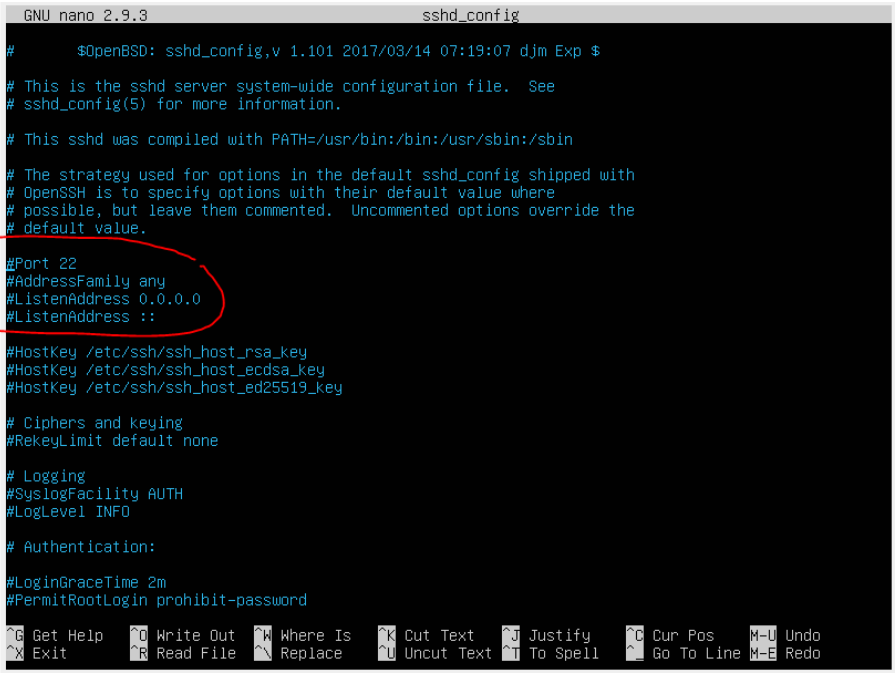
Przed zmianą konfiguracji zróbmy sobie oczywiście **kopie pliku konfiguracyjnego**, żeby w

razie wtopy można go było łatwo przywrócić:

cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bac

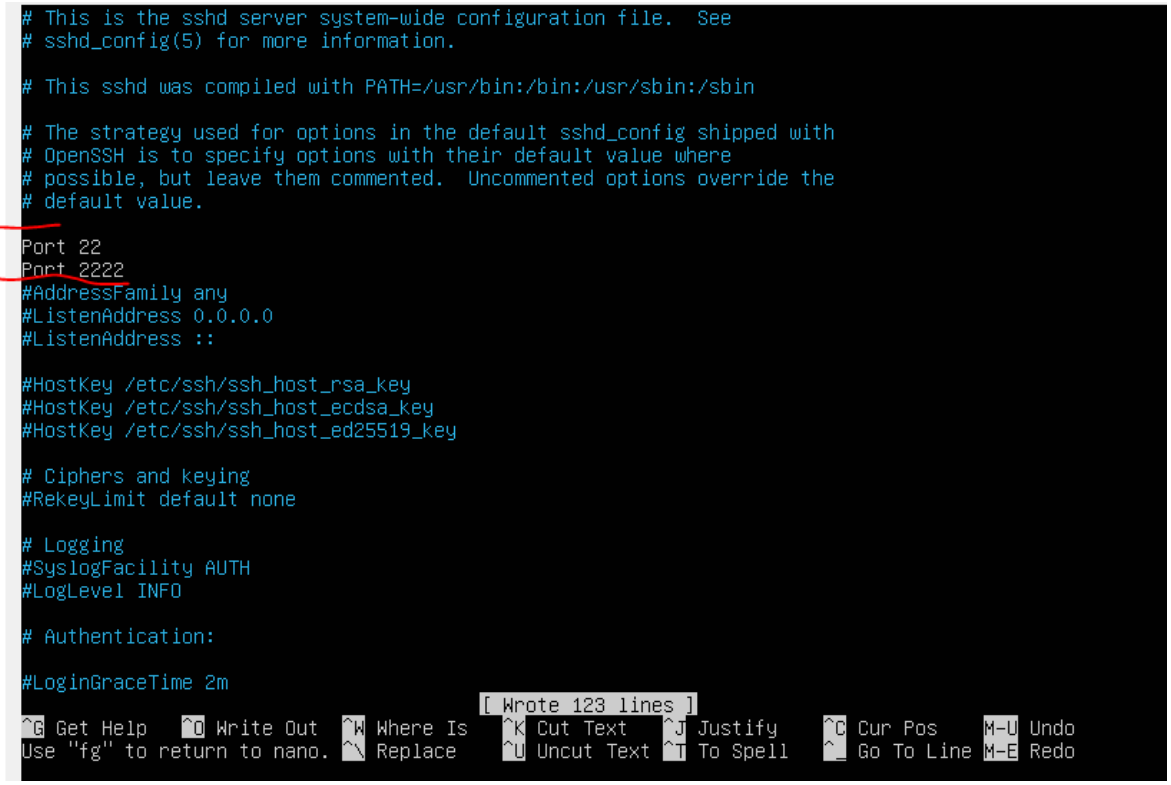
otwieramy w edytorze plik konfiguracyjny

nano /etc/ssh/sshd_config



najczęściej będzie nasz interesowała opcja wybrania adresu na którym ma działać serwer oraz portu

Możemy dopisać dodatkowe porty na których ma nasłuchiwać nasz serwer, zmienić domyślny port - całość polega na odkomentowaniu odpowiedniej linijki i ewentualnie dopisania żądanych ustawień - załóżmy, że chcemy, żeby oprócz domyślnego portu serwer działał tez na porcie 2222:



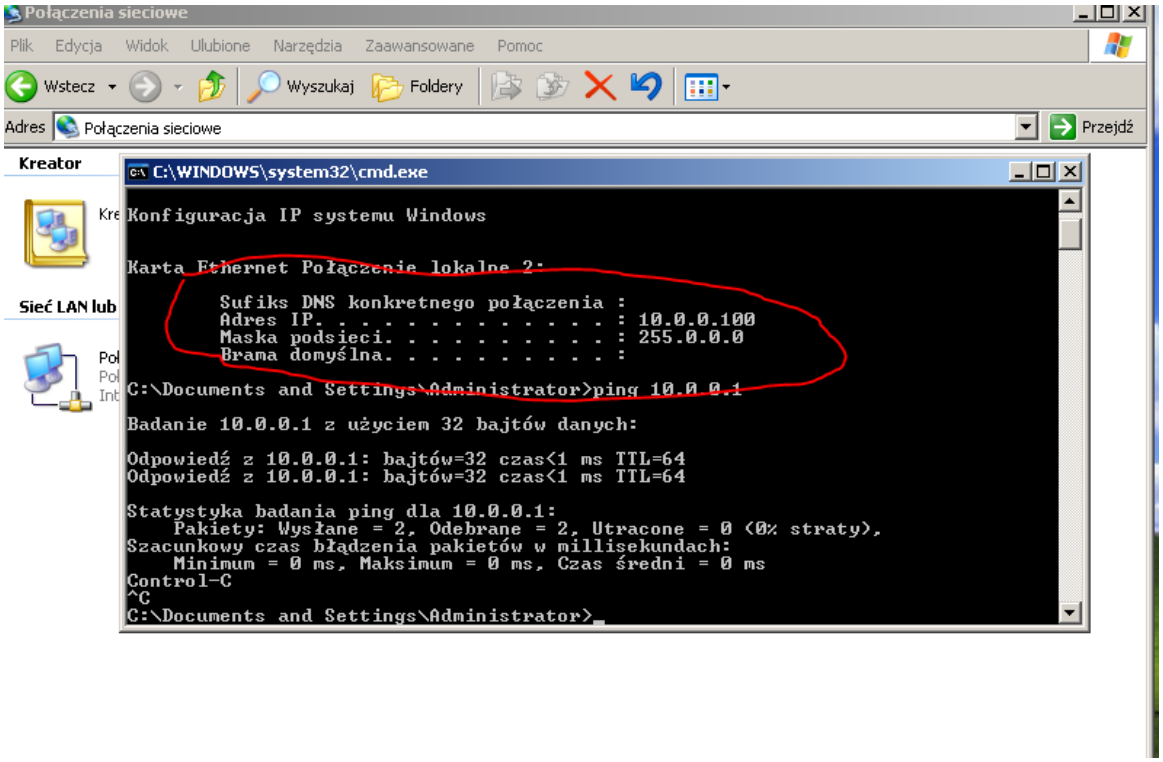
oczywiście, żeby nasze zmiany miały skutek musimy zrestartować usługę poleceniem:

service ssh restart
lub
systemctl restart ssh

Serwer powinien pozwalać teraz na połączenia na porcie 22 i 2222

9. Przygotujmy sobie teraz maszynę testową - ja użyje Windowsa XP – najpierw uruchomię go z kartą sieciową zmostkowaną, żeby mieć internet, ściągnę Putty (32bity, bo to XP)

Po ściągnięciu Putty, zmieniamy typ sieciówki na wewnętrzną i ustawiamy adresację na pasująca do drugiej karty sieciowej na naszym serwerze, czyli na przykład 10.0.0.100/8

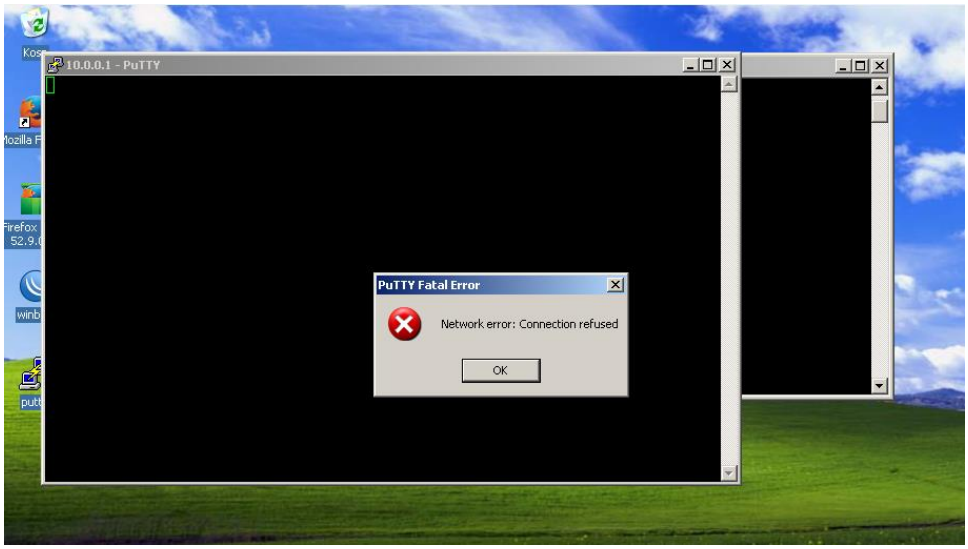


10. Możemy ustawić na jakim adresie/adresach IP ma nasłuchiwać nasz serwer – domyślnie nasłuchuje na wszystkich (powinien Was wpuścić i z komputera gospodarza i z komputera testowego na obu ustawionych portach) – odkomentowanie odpowiedniej linijki i wpisanie adresu spowoduje, że serwer będzie nasłuchiwał tylko na jednym adresie:

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port 22
Port 2222
#AddressFamily any
ListenAddress 192.168.1.200
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
                                [ Wrote 123 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
Use "fg" to return to nano.  ^\ Replace  ^U Uncut Text  ^T To Spell  ^_ Go To Line  M-E Redo

[3]+  Stopped                 nano sshd_config
root@jkubuntu:/etc/ssh# systemctl restart ssh
root@jkubuntu:/etc/ssh# _
```

Oczywiście po zapisaniu restartujemy za każdym razem usługę ssh (service ssh restart)

Teraz próbując zalogować się z komputera testowego na adres 10.0.0.1 serwer powinien odrzucić połączenie:



11. Możemy ręcznie dopisać drugi adres w konfiguracji – tutaj dodatkowo podałem port 3333 – przy takiej notacji serwer będzie zezwalał na łączenie się na tym adresie tylko na porcie 3333 pomijając te ustawione wyżej:

Oczywiście po restarcie usługi ssh i próbie polaczenia się z komputera testowego na 10.0.0.1:22 serwer odrzuci polaczenie a na 10.0.0.1:3333 pozwoli się połączyć.

12. Blokada lub zezwalanie na dostęp użytkowników/grup

Możemy też chcieć zablokować lub zezwalać na dostęp określonych użytkowników/grup

Musimy wtedy w naszym configu użyć odpowiednich zmiennych (działają zgodnie z nazwami):

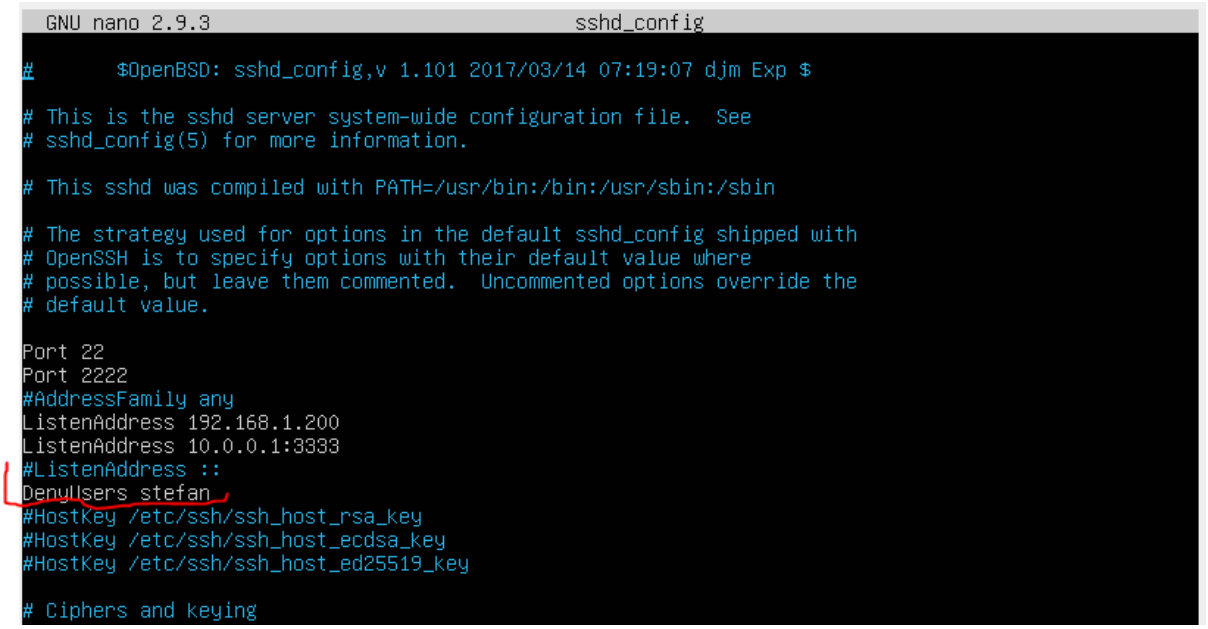
```
DenyUsers user1 user2 user3
DenyGroups group1 group2
```

AllowUsers user1 user2
AllowGroups group1 group2

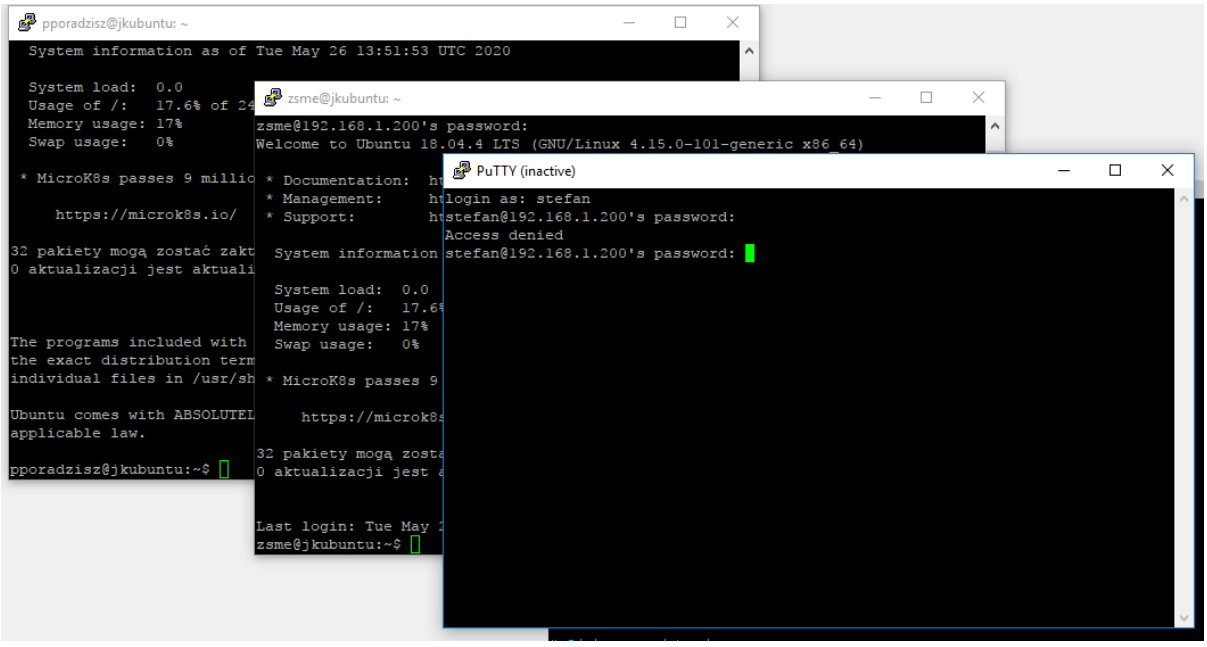
Załóżmy na serwerze testowe konto **inazwisko** z hasłem **123qwe** oraz **stefan** z hasłem **123qwe**

adduser pporadzisz
adduser stefan

I teraz spróbujmy ustawić tak, że konta iznazwisko i zsme są wpuszczane na serwer konto stefan nie:



restartujemy serwer SSH i sprawdzamy:



Podobnie oczywiście będzie działało to z grupami.