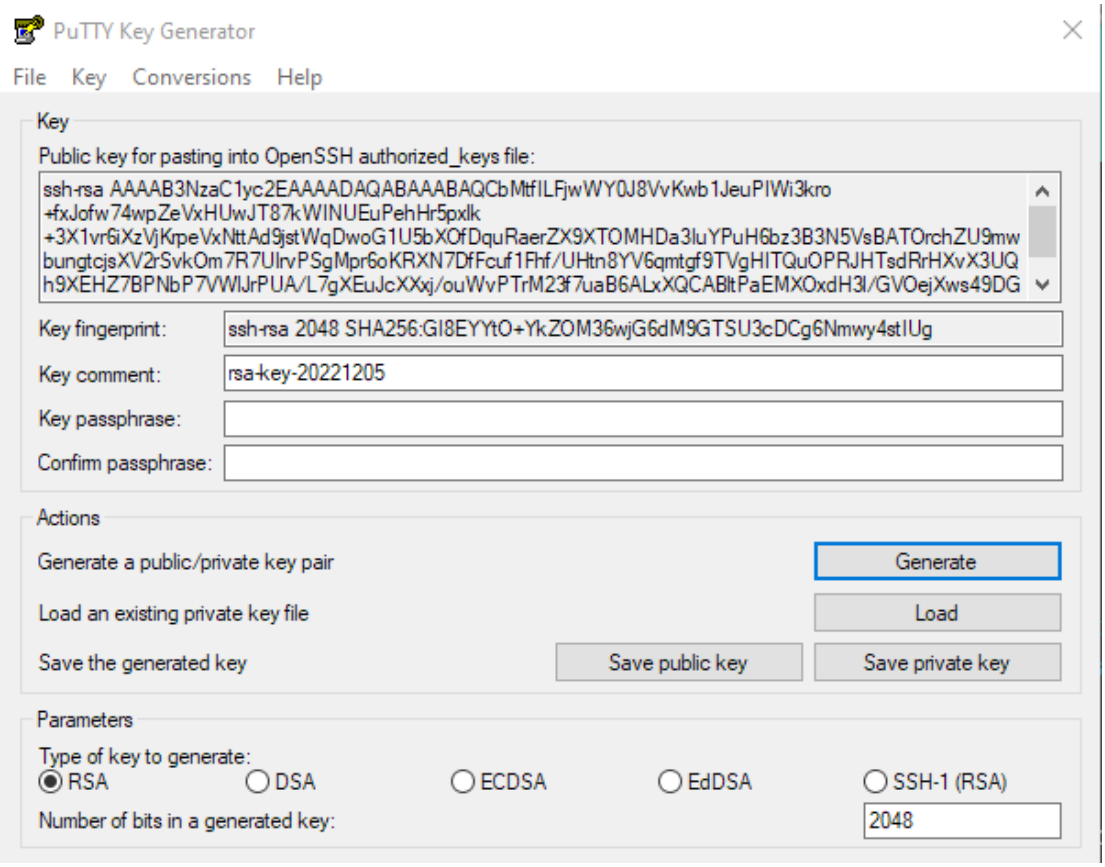
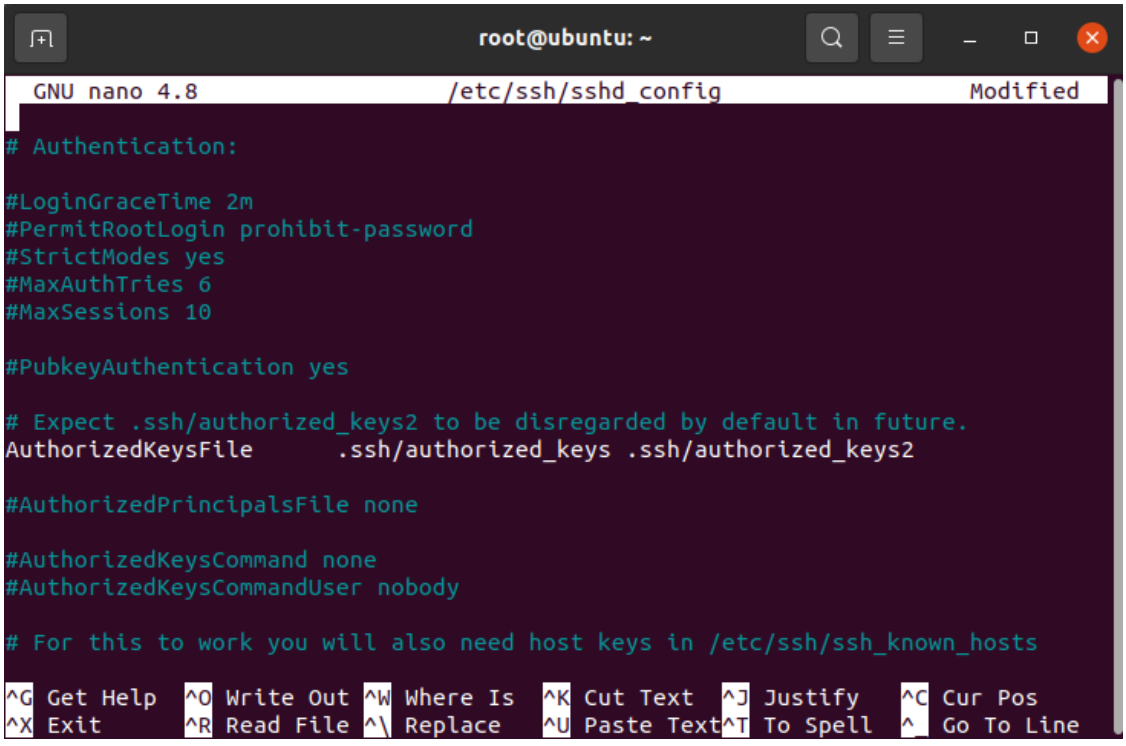
Wygenerowanie klucza ssh za pomocą putty

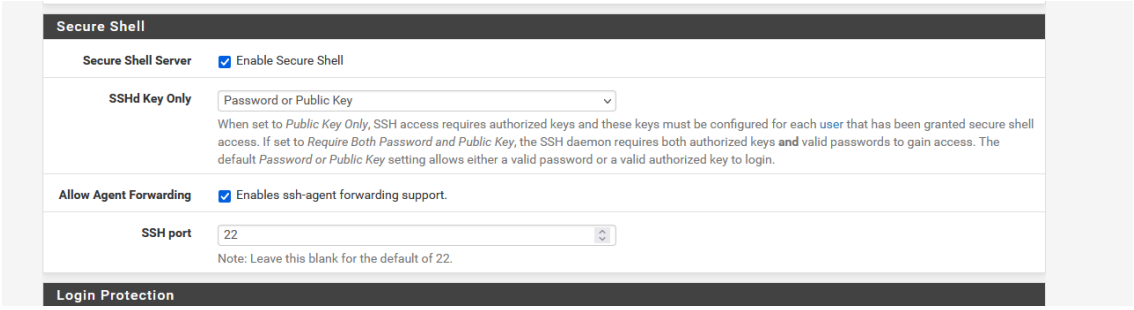


Edycja pliku /etc/ssh/sshd_config - umożliwienie odczytywania kluczy z pliku .ssh/authorized_keys

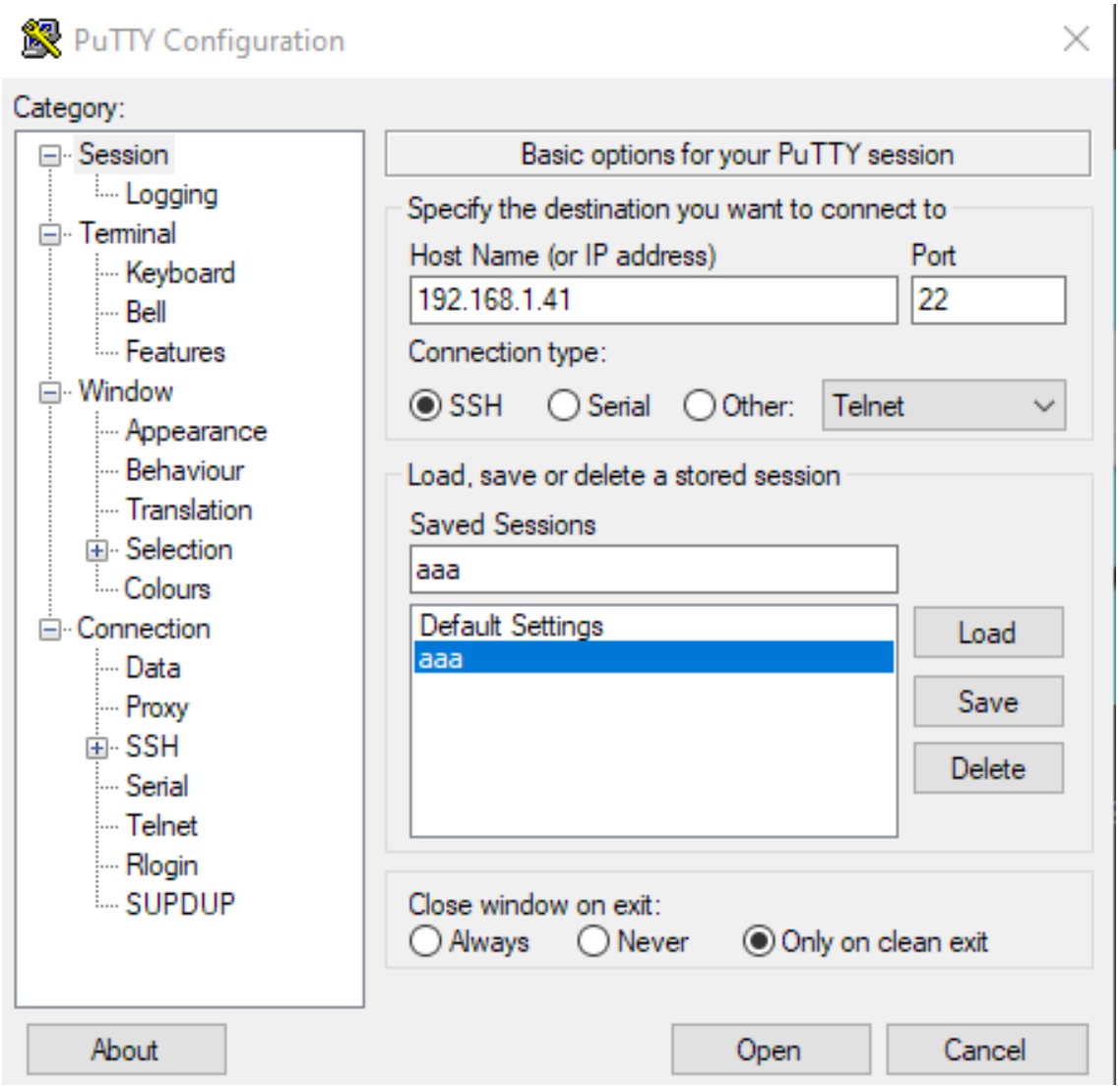


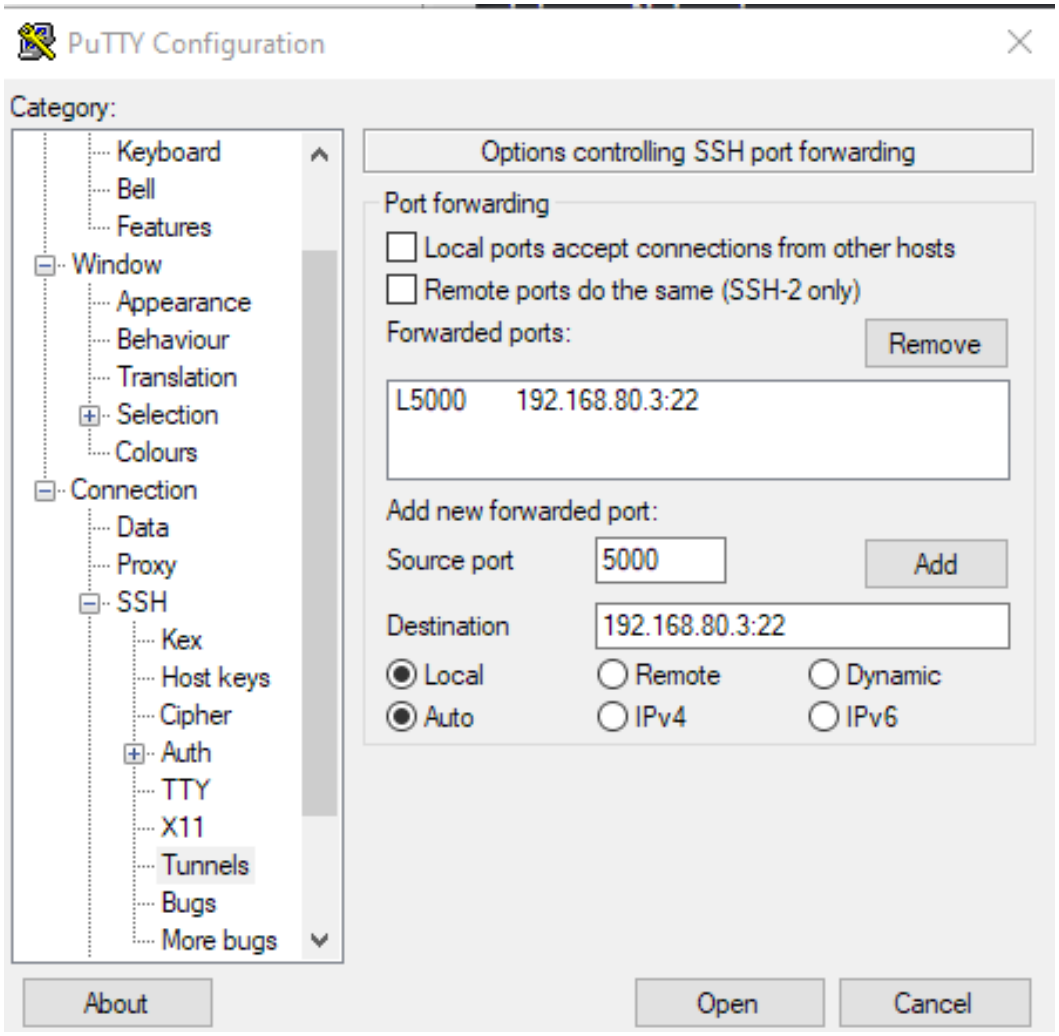
Edycja pliku .ssh/authorized_keys – wklejenie wcześniej skopiowanego klucza

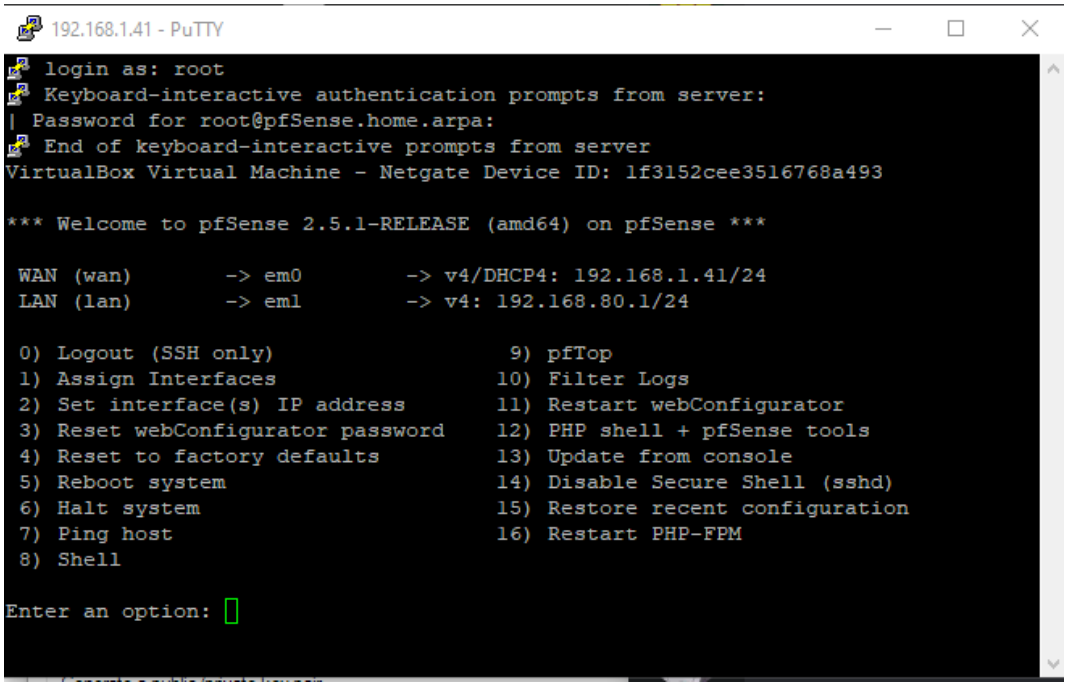
Zaznaczenie odpowiednich ustawień w pfsensie



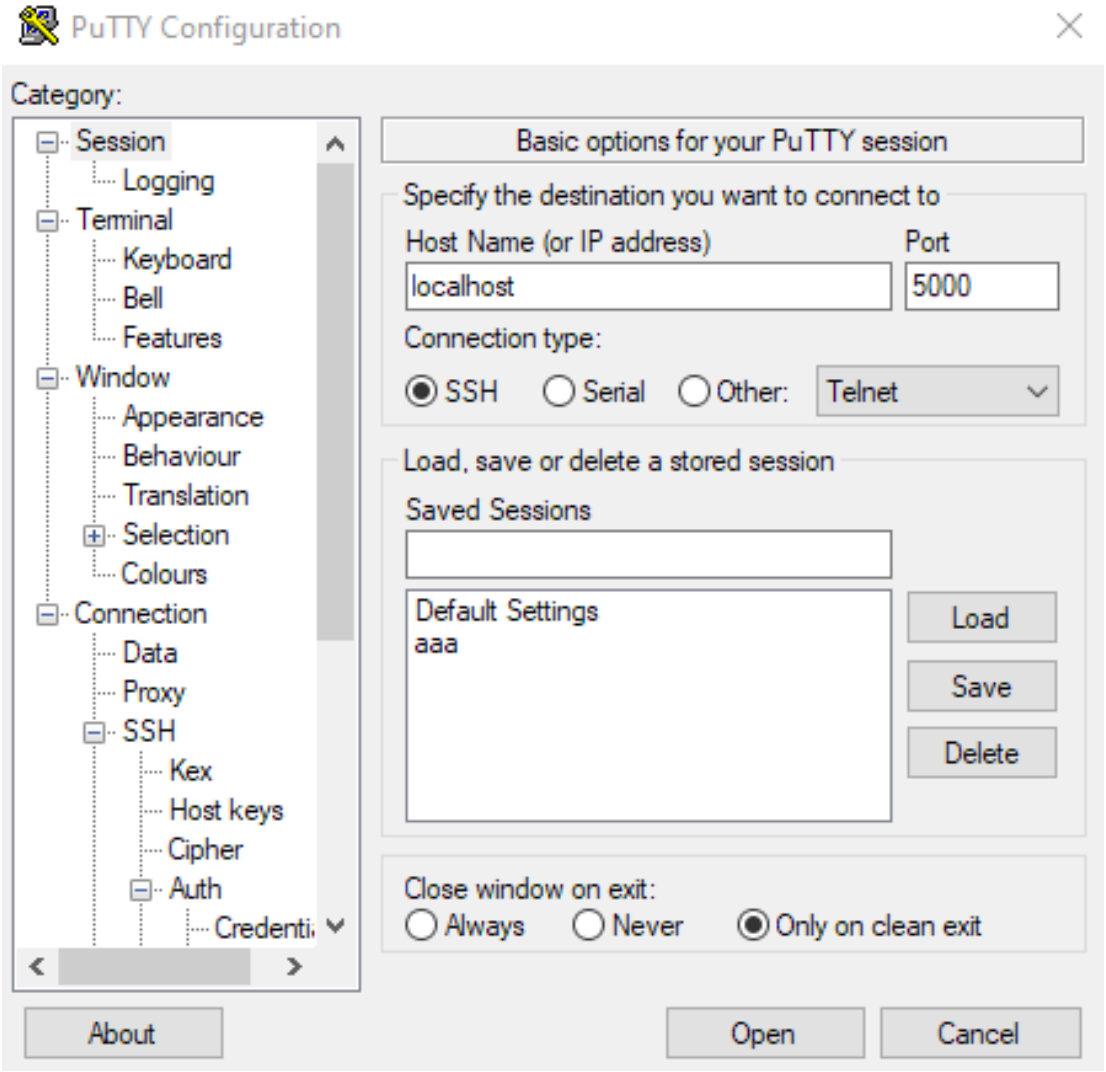
Przekierowanie ip na localhost:5000

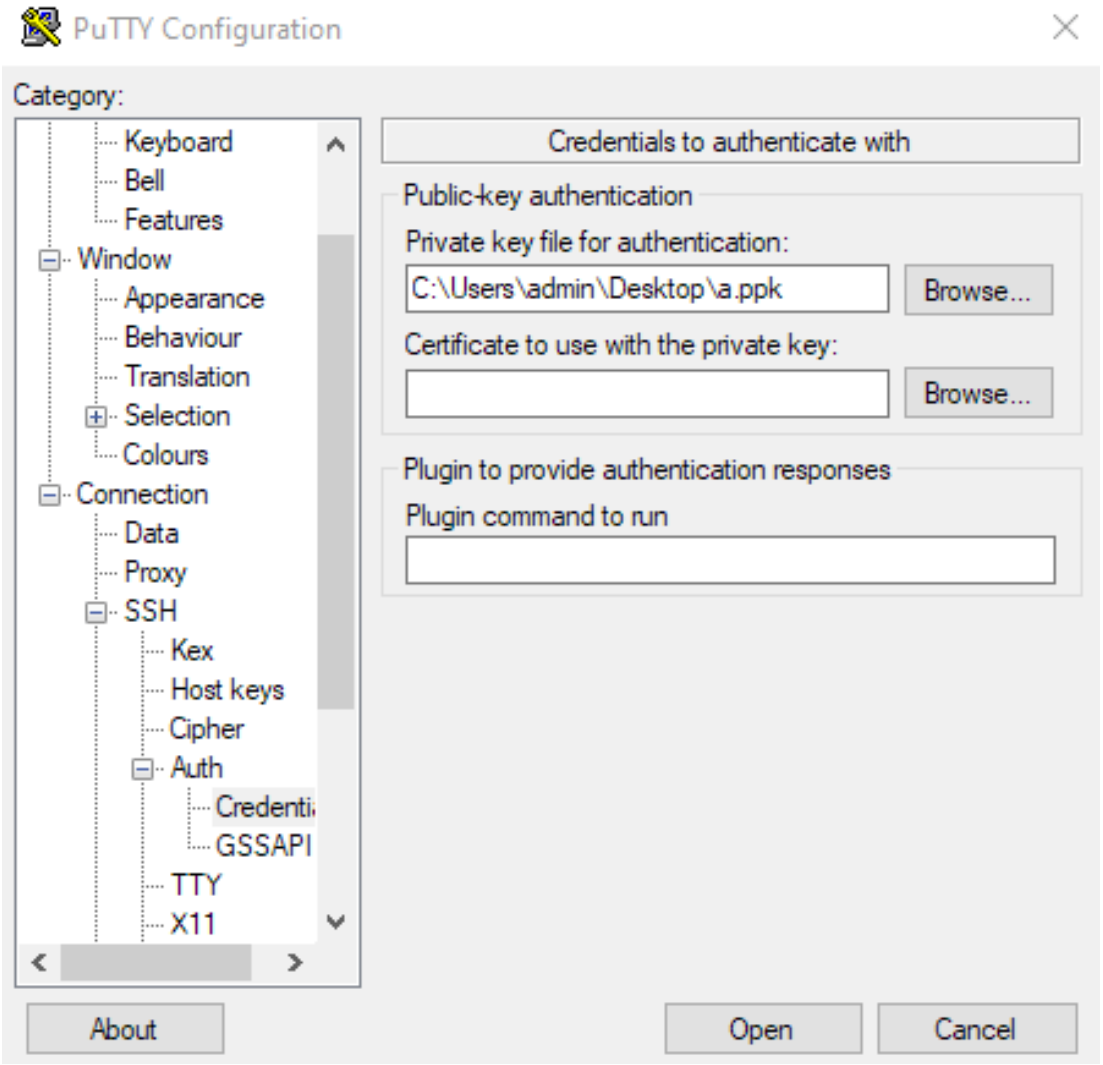



PuTTY Configuration
Category:
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
L5000 192.168.80.3:22
Add new forwarded port:
Source port
5000
Add
Destination
192.168.80.3:22
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Open
Cancel

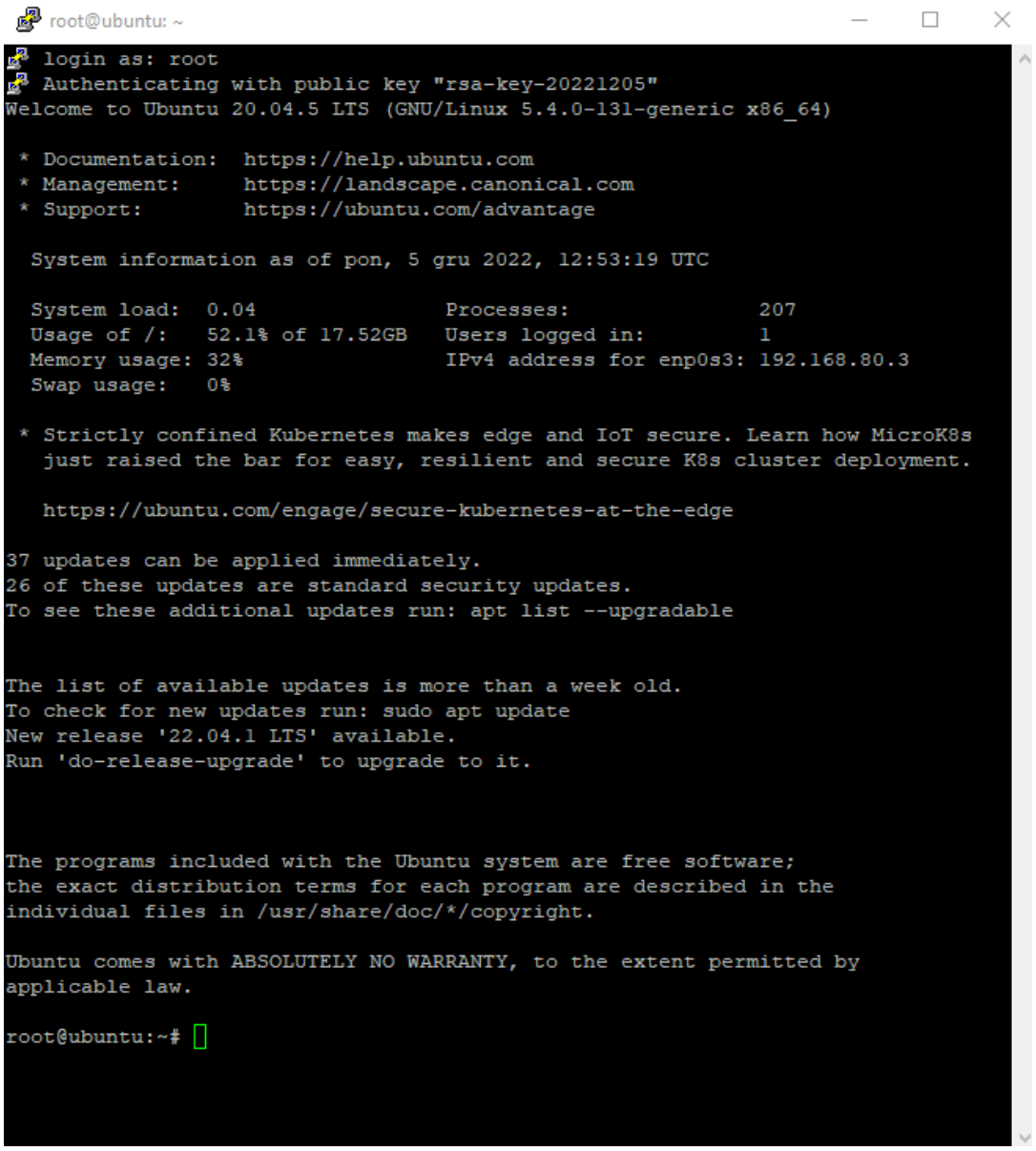

192.168.1.41 - PuTTY
login as: root
Keyboard-interactive authentication prompts from server:
Password for root@pfSense.home.arpa:
End of keyboard-interactive prompts from server
VirtualBox Virtual Machine - Netgate Device ID: 1f3152cee3516768a493
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.41/24
LAN (lan) -> em1 -> v4: 192.168.80.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

Zalogowanie się na port localhost:5000 przy użyciu klucza prywatnego, który został wcześniej dopisany na serwer do pliku authorized_keys

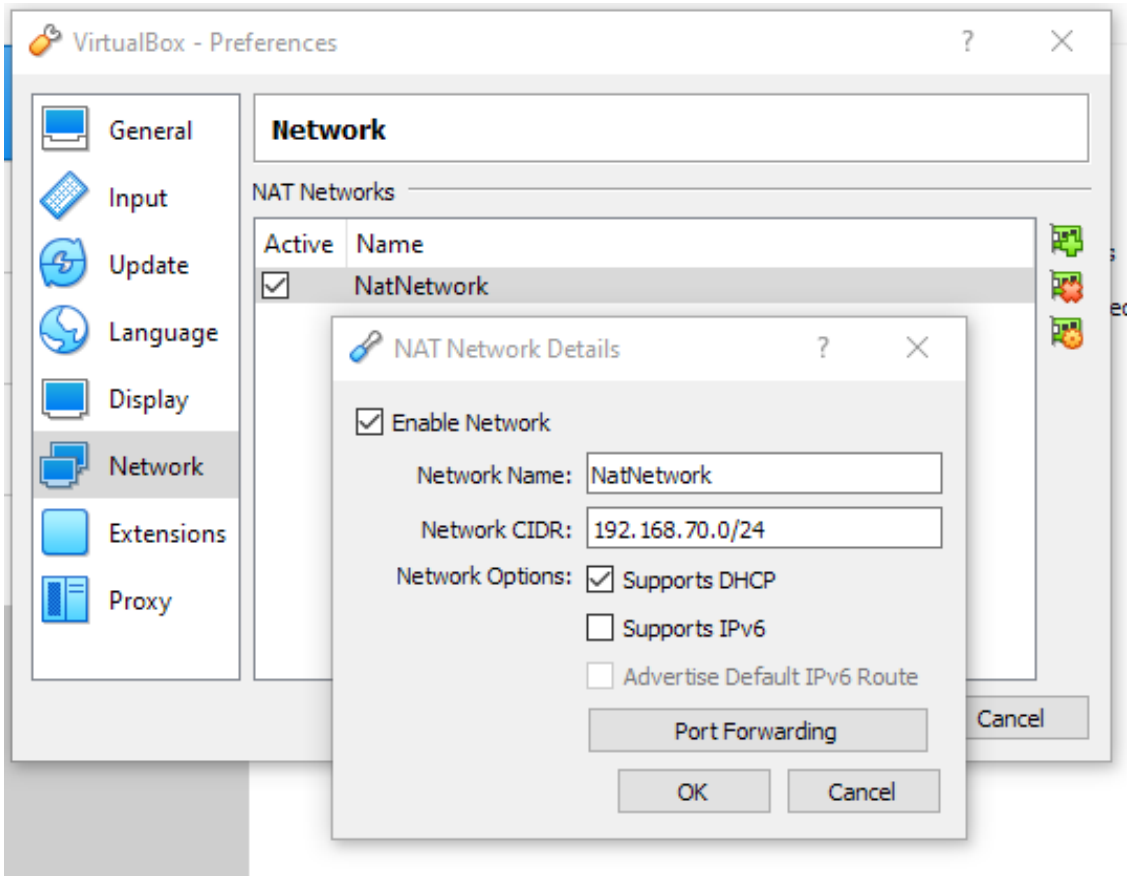



PuTTY Configuration
Category:
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
Credenti
GSSAPI
TTY
X11
Credentials to authenticate with
Public-key authentication
Private key file for authentication:
C:\Users\admin\Desktop\a.ppk
Browse...
Certificate to use with the private key:
Browse...
Plugin to provide authentication responses
Plugin command to run
About
Open
Cancel

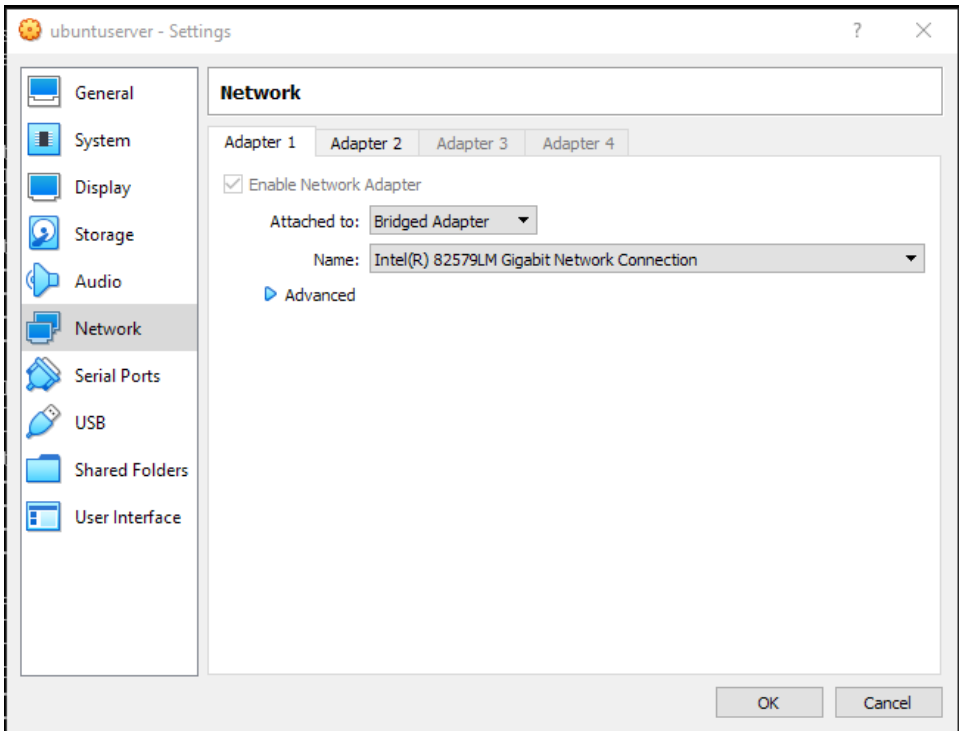
Udane zalogowanie na roota

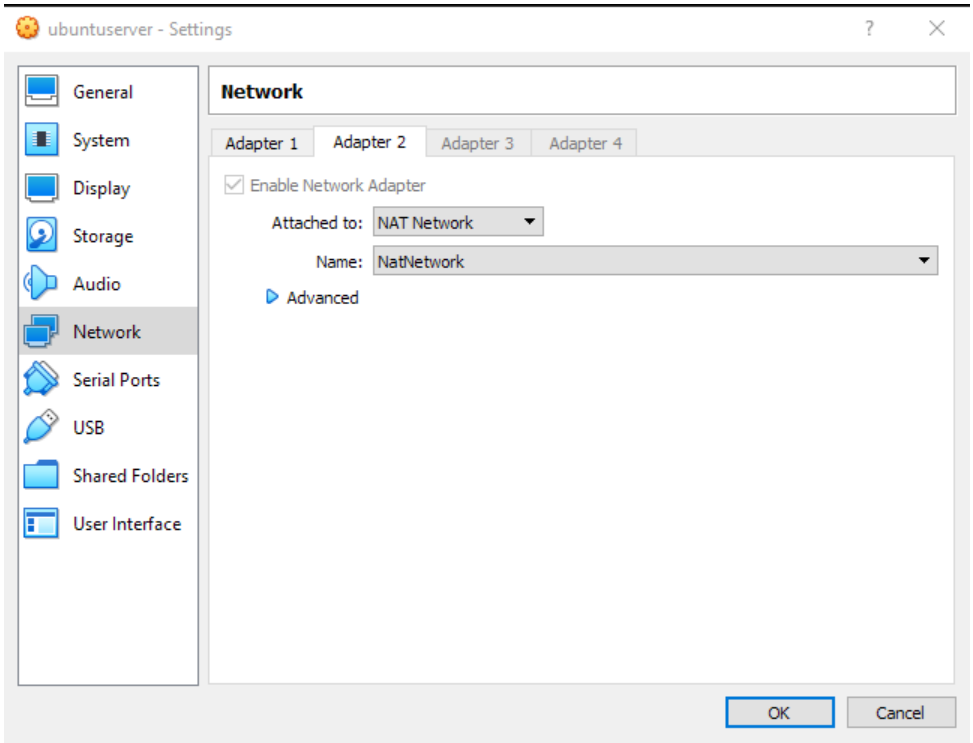


Utworzenie sieci Nat w virtual boxie i przypisanie do niej klienta Windowsa i nowy serwer ubuntu

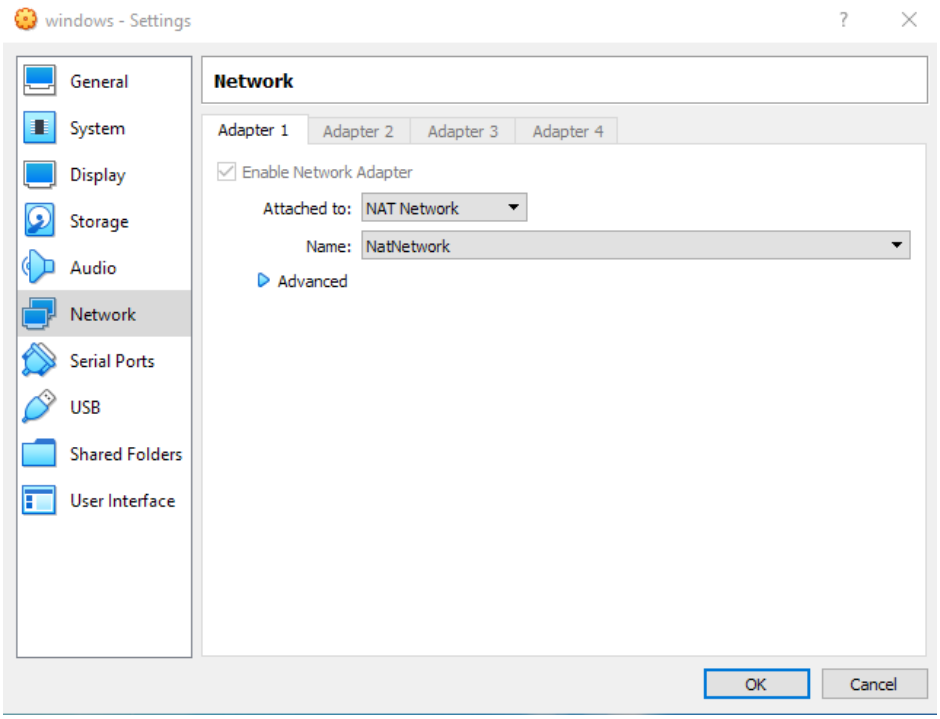


Karty sieciowe serwera

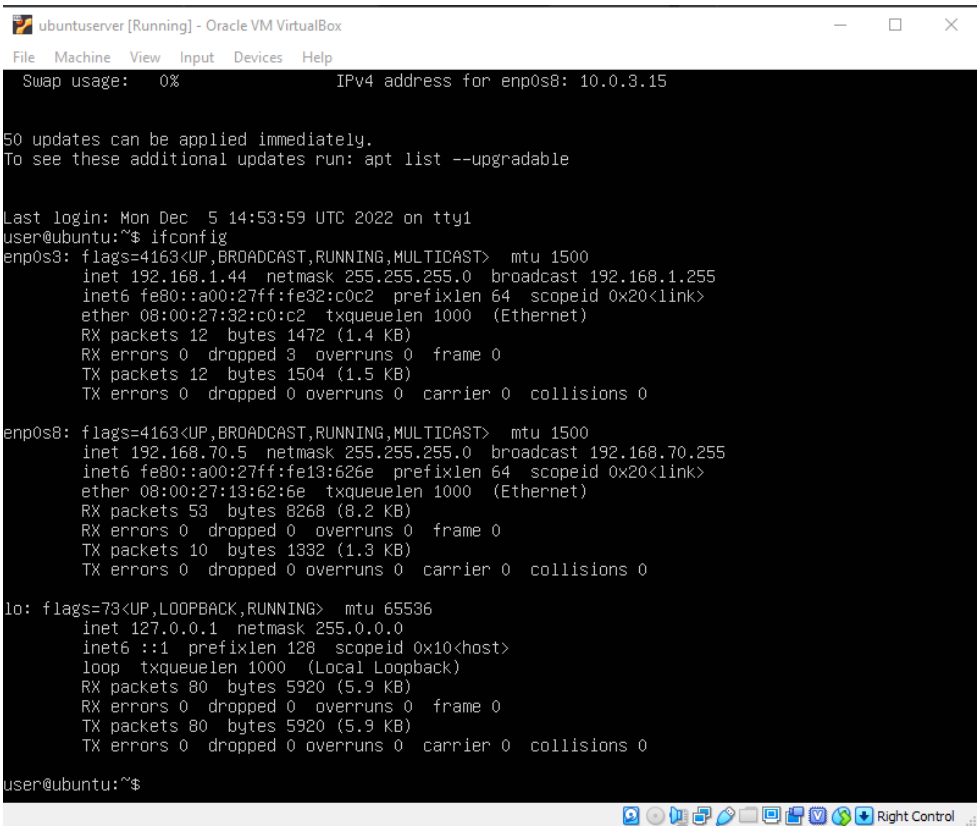




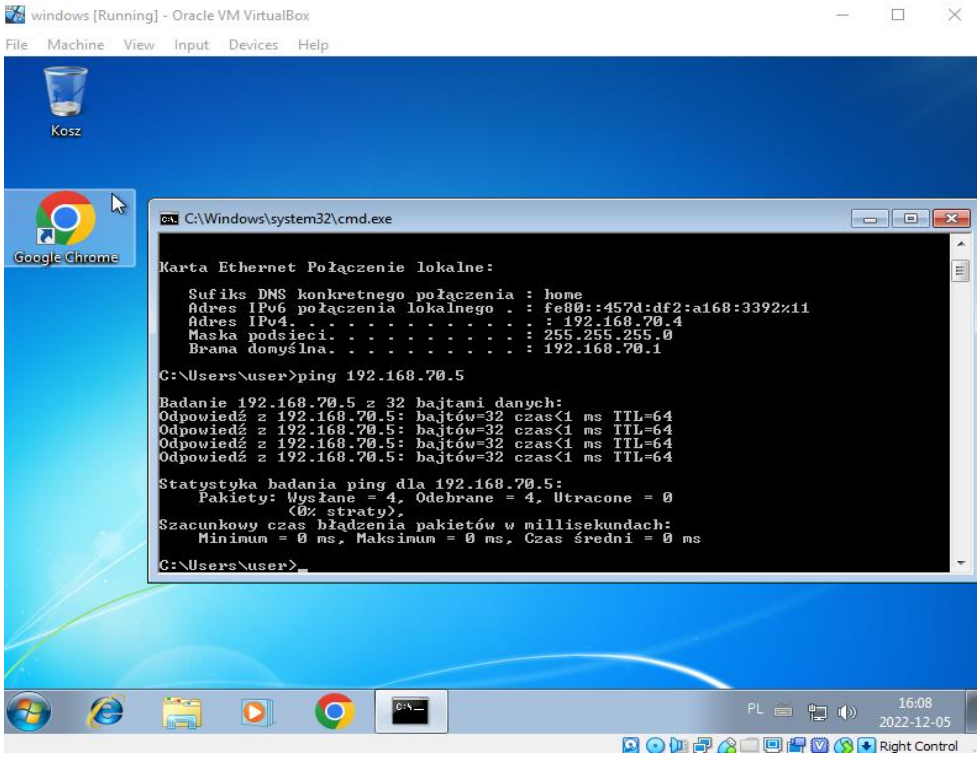
Karta sieciowa klienta



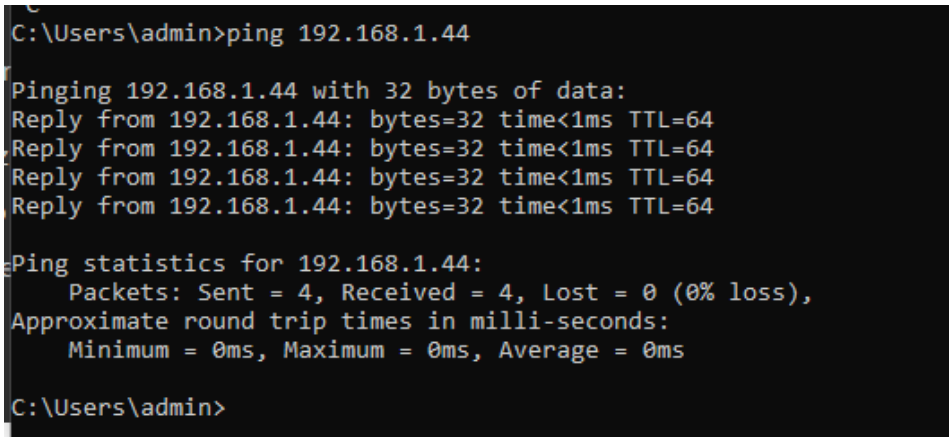
Adresy serwera



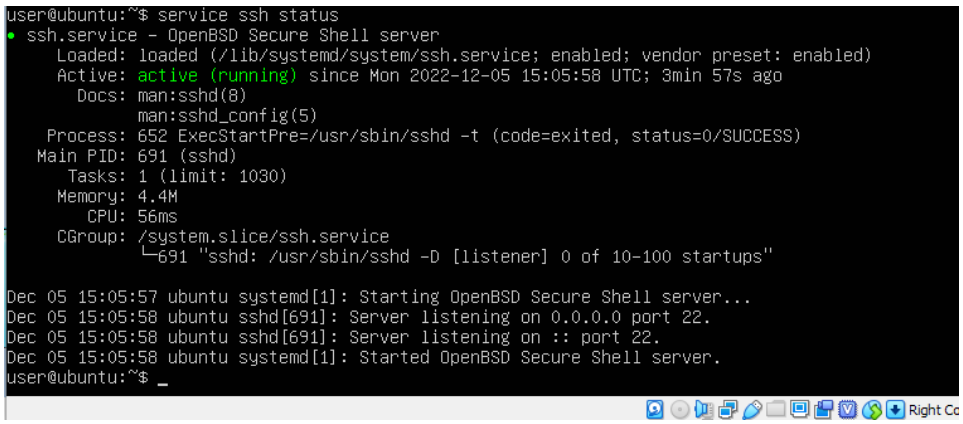
Adres klienta i sprawdzenie, czy widzi on serwer poprzez pingowanie



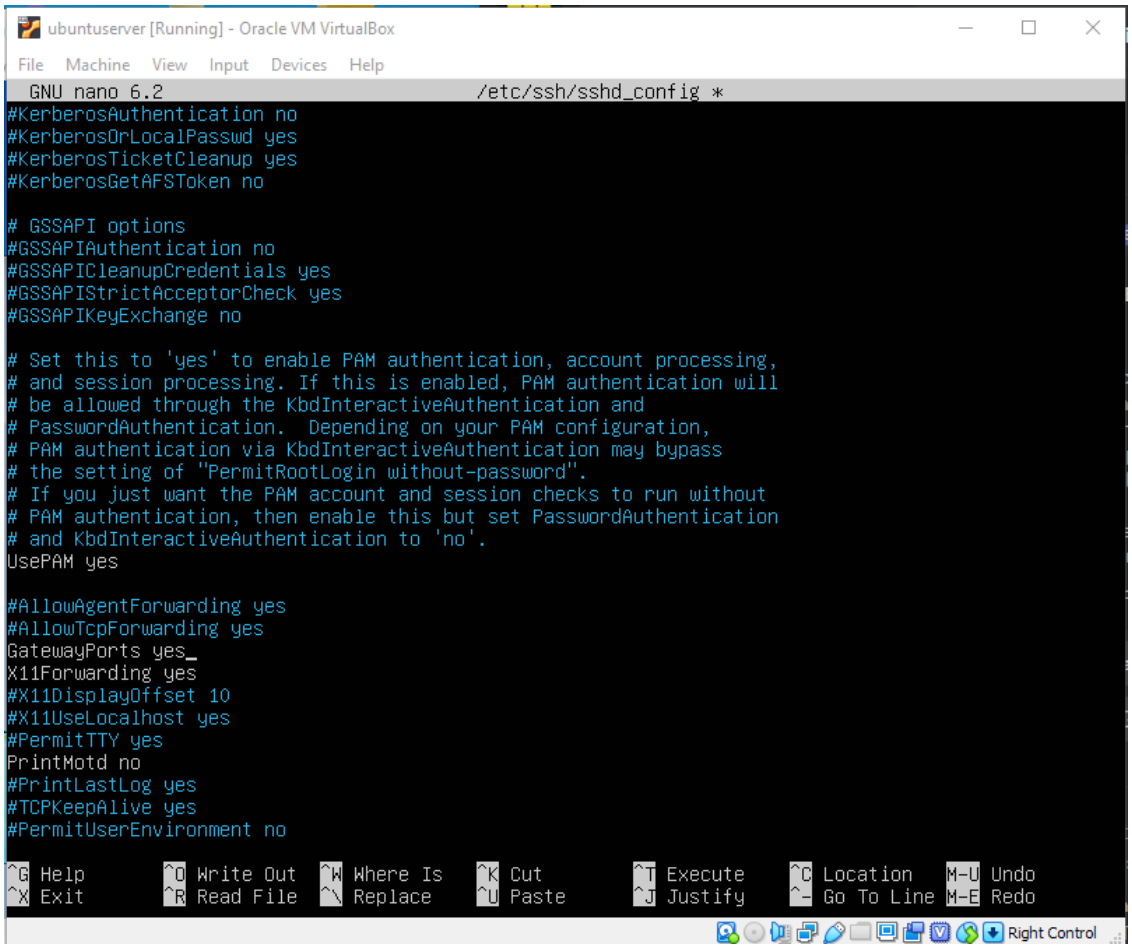
Sprawdzenie czy gospodarz widzi serwer



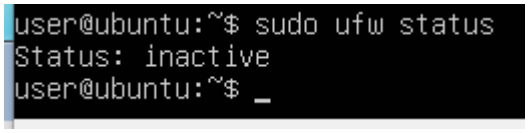
Sprawdzenie statusu ssh



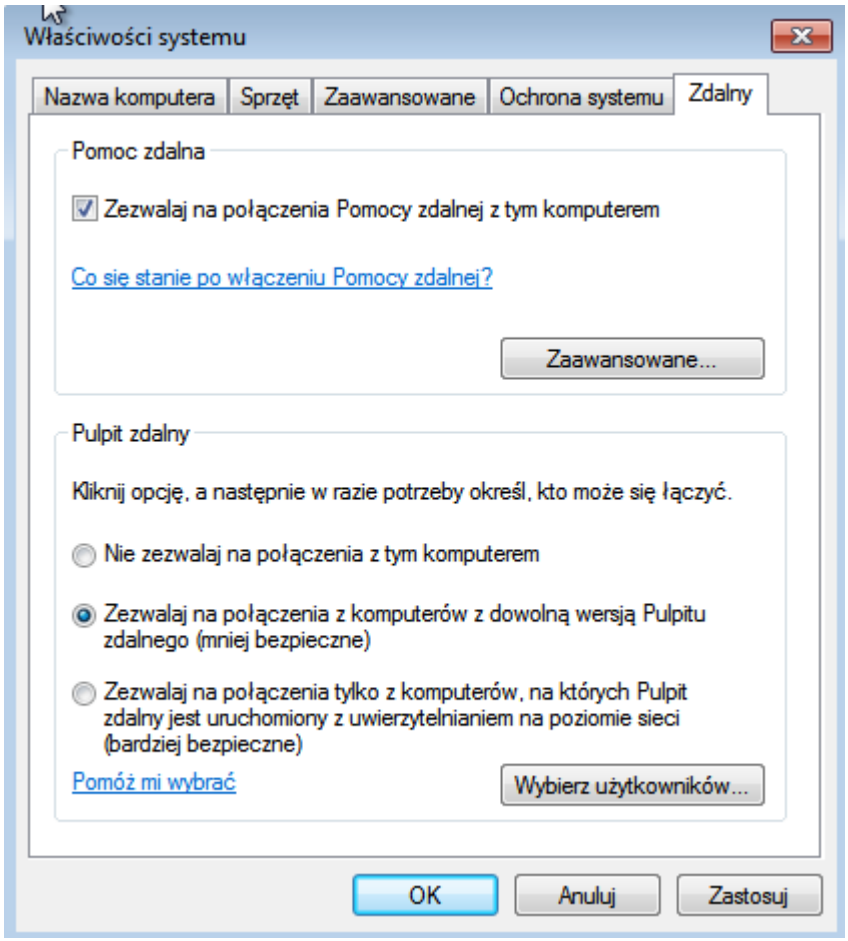
Edycja pliku /etc/ssh/sshd_config – odkomentowanie GatewayPorts Yes



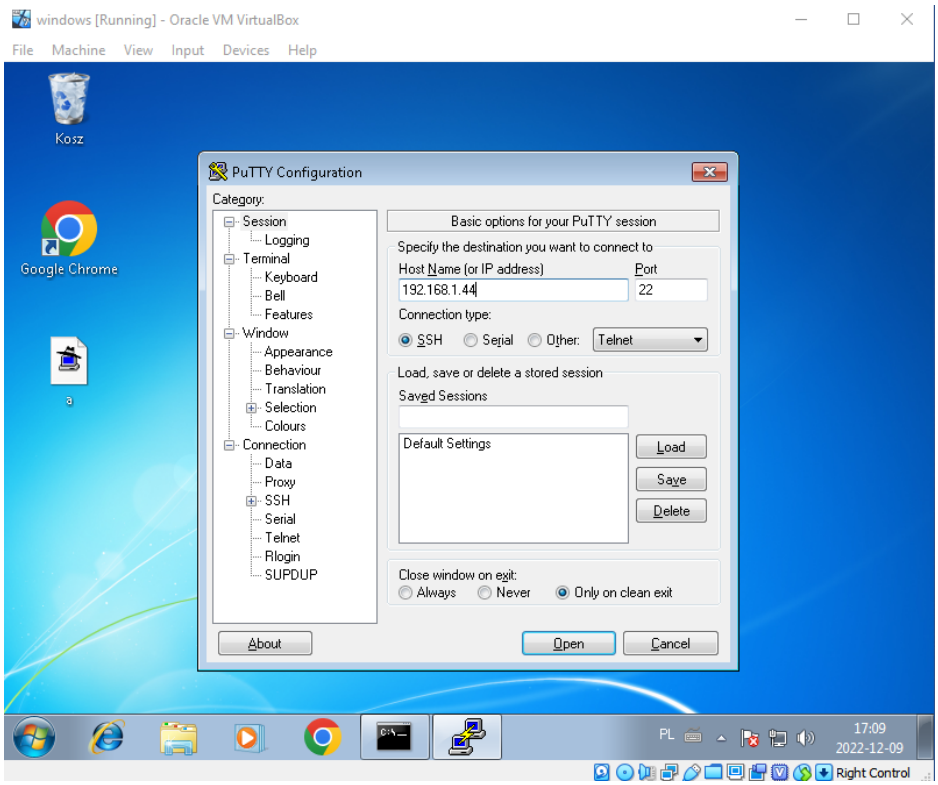
Sprawdzenie statusu firewalla, przez to, że jest inactive to nie będzie sprawiał żadnych problemów z pulpitem zdalnym

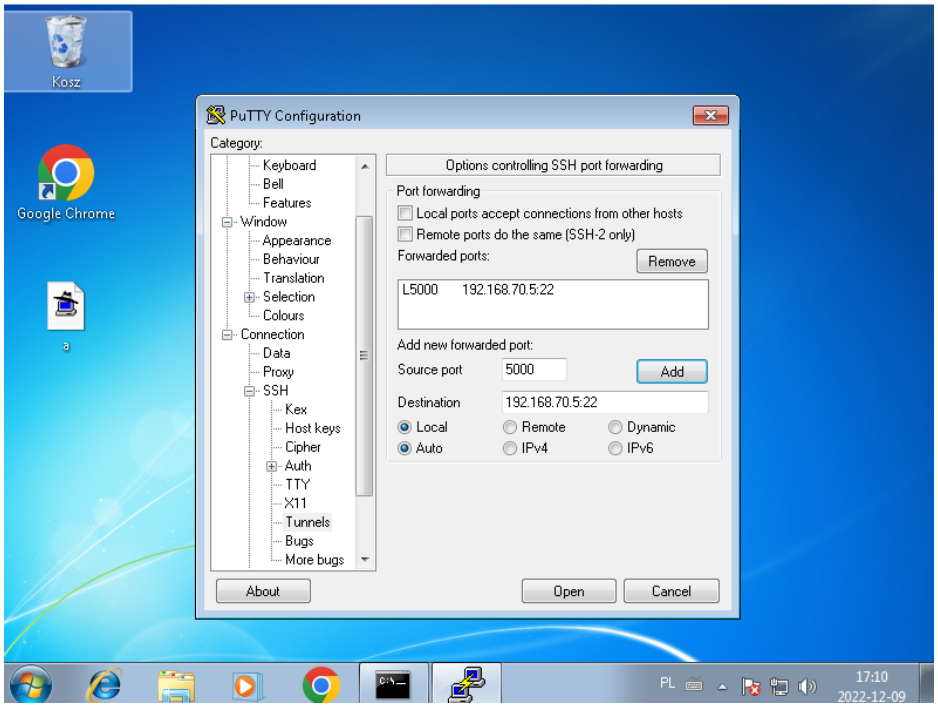


Zezwolenie na kliencie na łączenie się pulpitem zdalnym

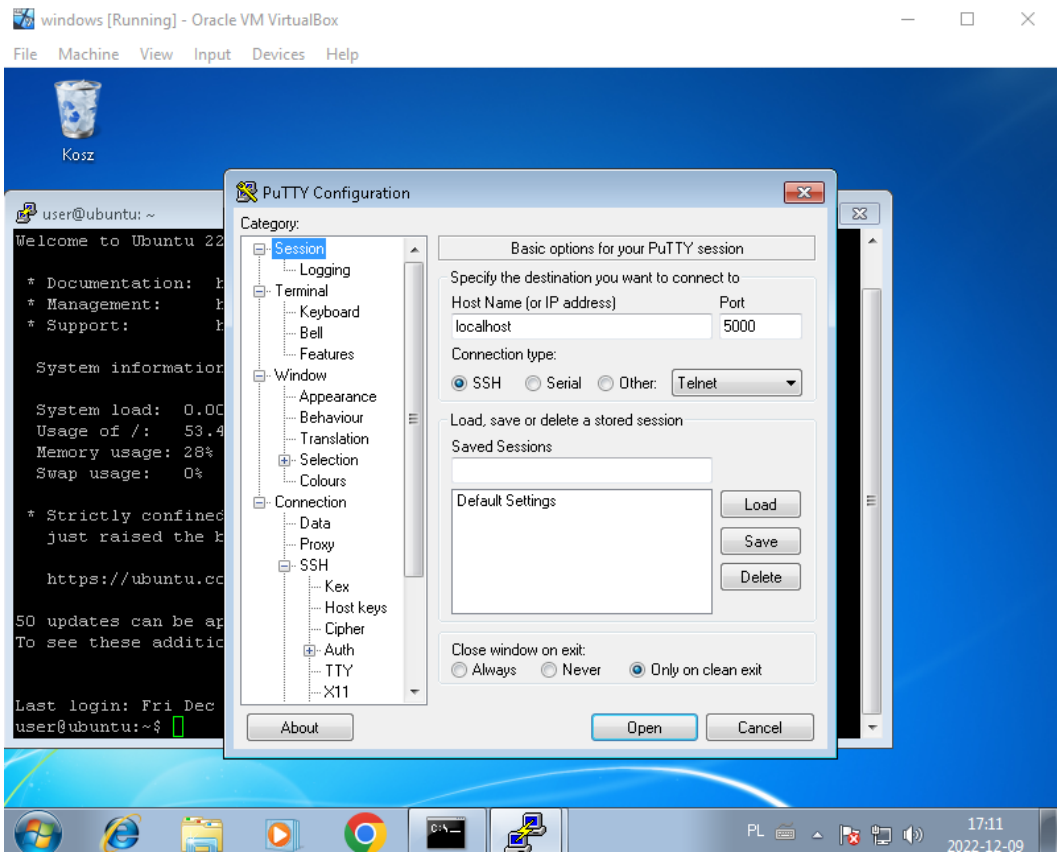


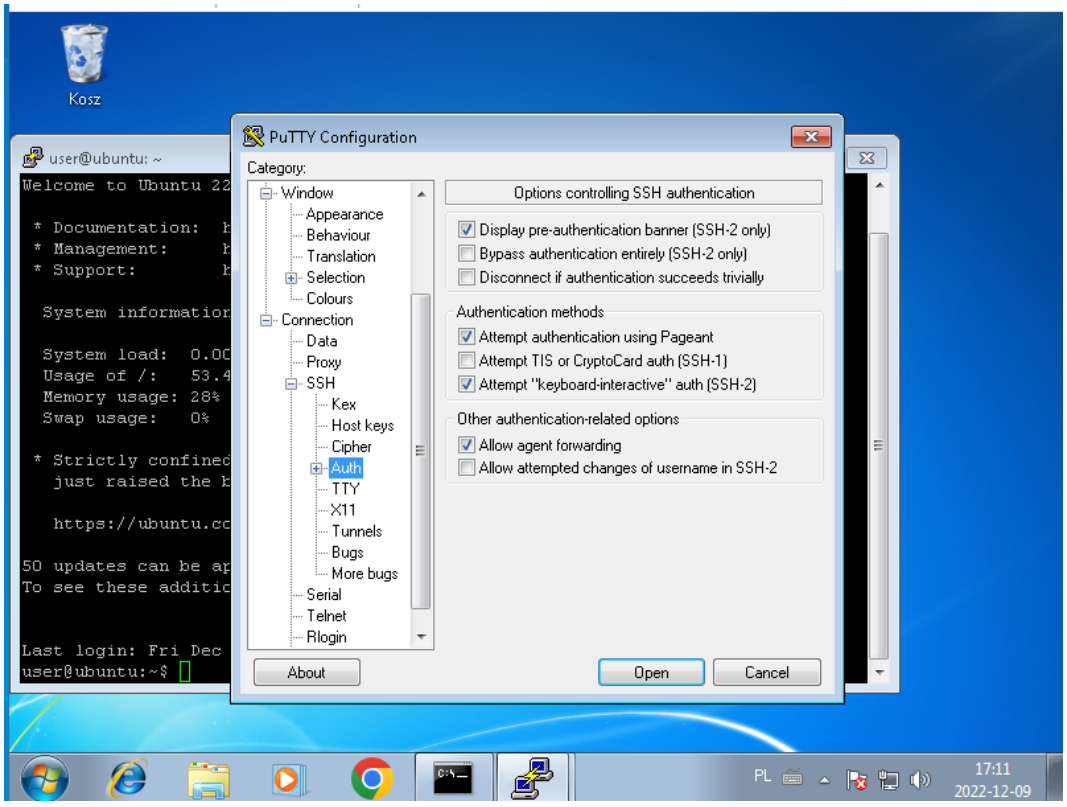
Otwarcie portu 5000

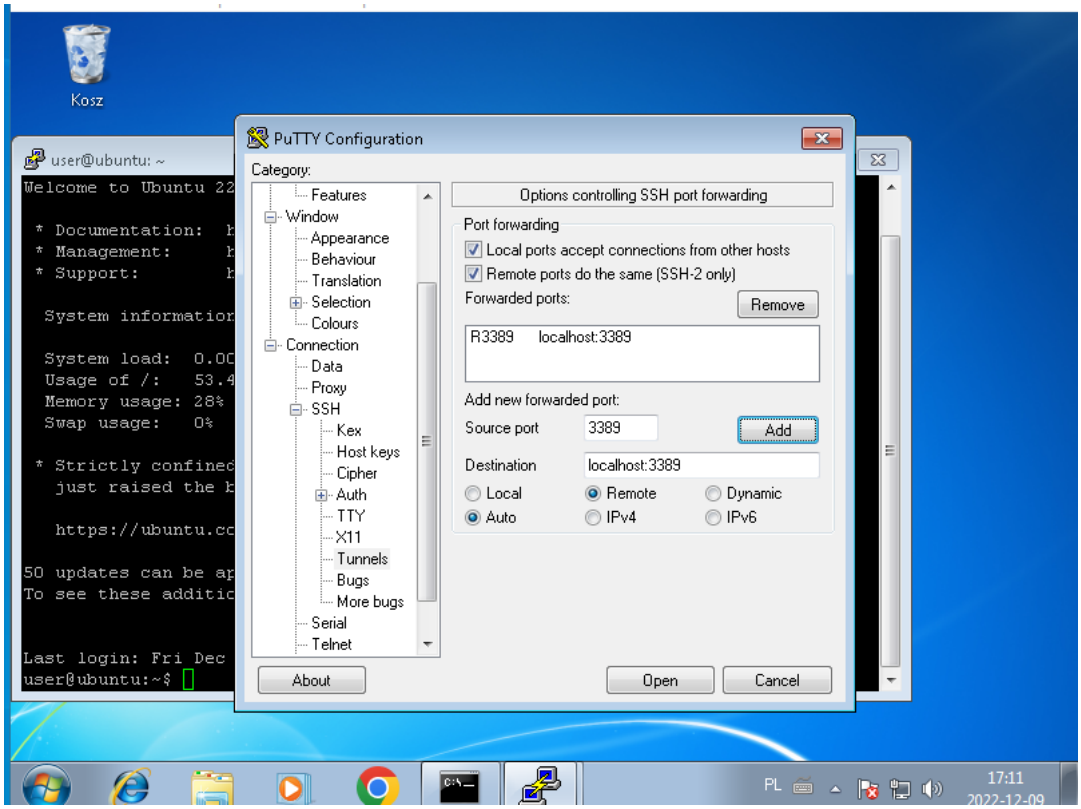


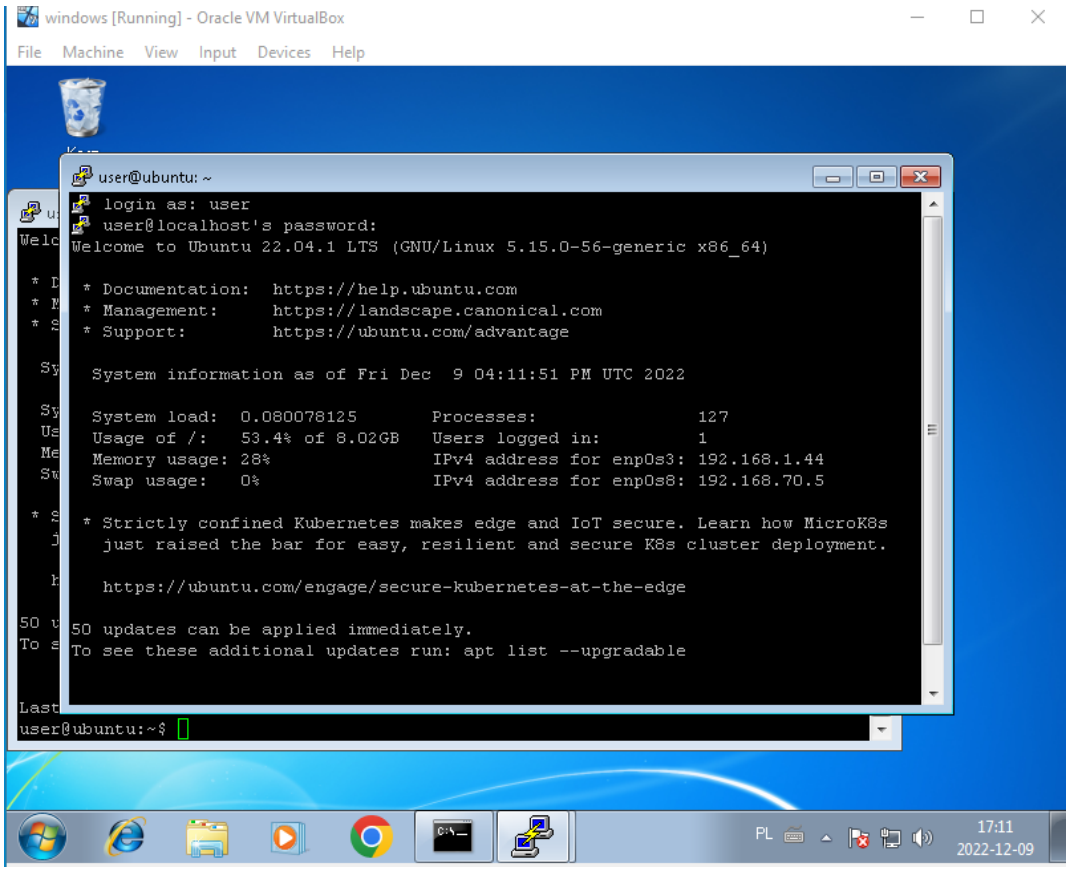


Wystawienie na porcie 5000 usługi zdalnego pulpitu, czyli 3389

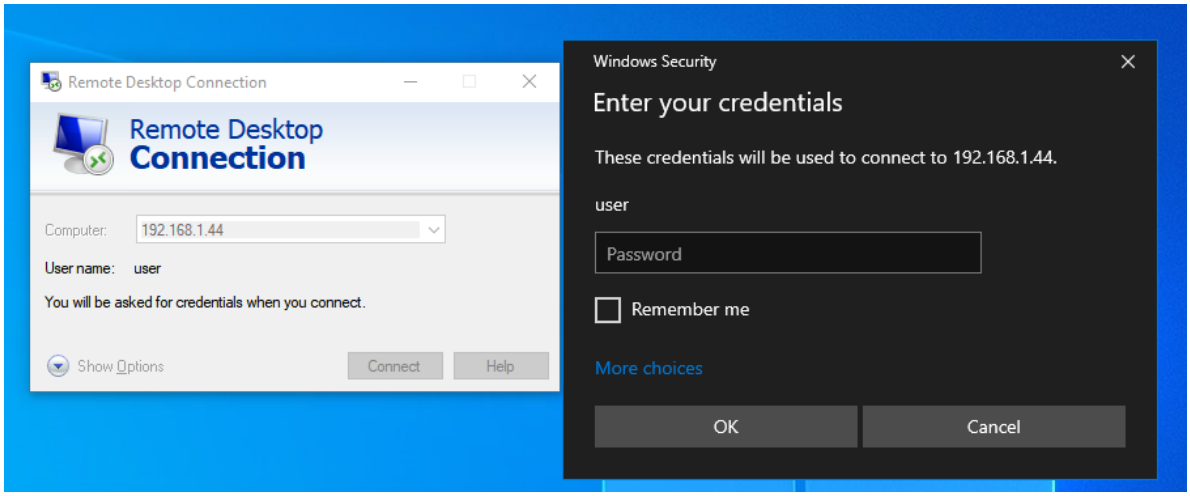


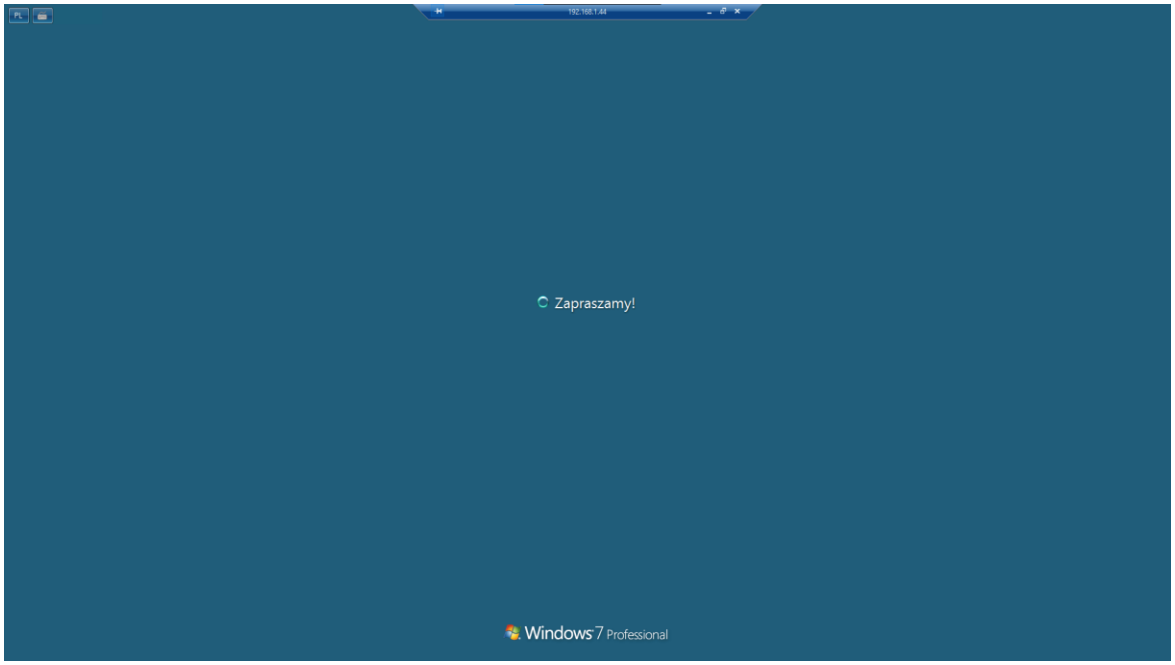



Kosz
user@ubuntu: ~
Welcome to Ubuntu 22
* Documentation:
* Management:
* Support:
System information
System load: 0.0
Usage of /: 53.4
Memory usage: 28%
Swap usage: 0%
* Strictly confined
just raised the b
https://ubuntu.co
50 updates can be ap
To see these additic
Last login: Fri Dec
user@ubuntu:~$
PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Serial
Telnet
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
R3389 localhost:3389
Add new forwarded port:
Source port
3389
Add
Destination
localhost:3389
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Open
Cancel
PL
17:11
2022-12-09

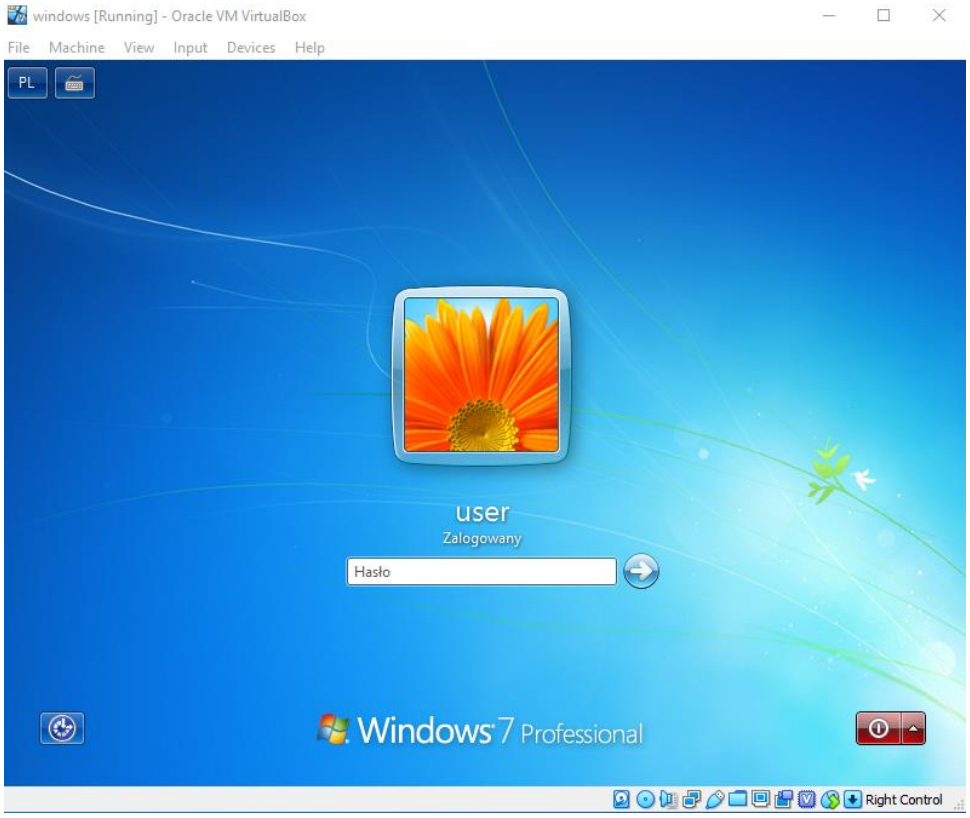

windows [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
user@ubuntu: ~
login as: user
user@localhost's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Fri Dec 9 04:11:51 PM UTC 2022
System load: 0.080078125 Processes: 127
Usage of /: 53.4% of 8.02GB Users logged in: 1
Memory usage: 28% IPv4 address for enp0s3: 192.168.1.44
Swap usage: 0% IPv4 address for enp0s8: 192.168.70.5
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
50 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
user@ubuntu:~$
PL
17:11
2022-12-09

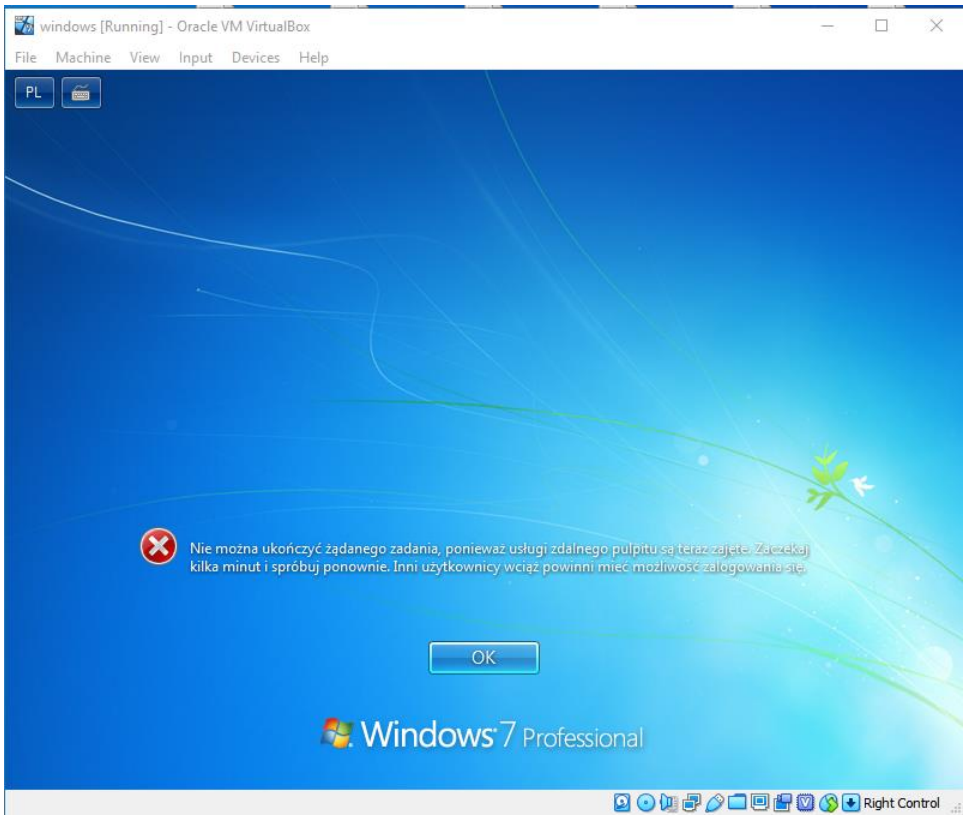
Próba połączenia się gospodarza przez pulpit zdalny



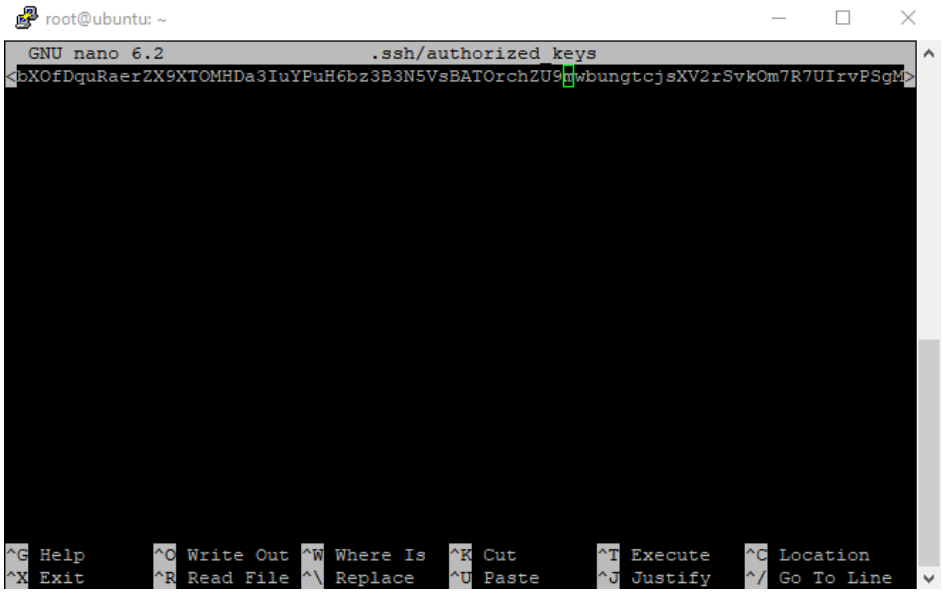


W czasie korzystania z pulpitu zdalnego nie możliwe jest używanie klienta

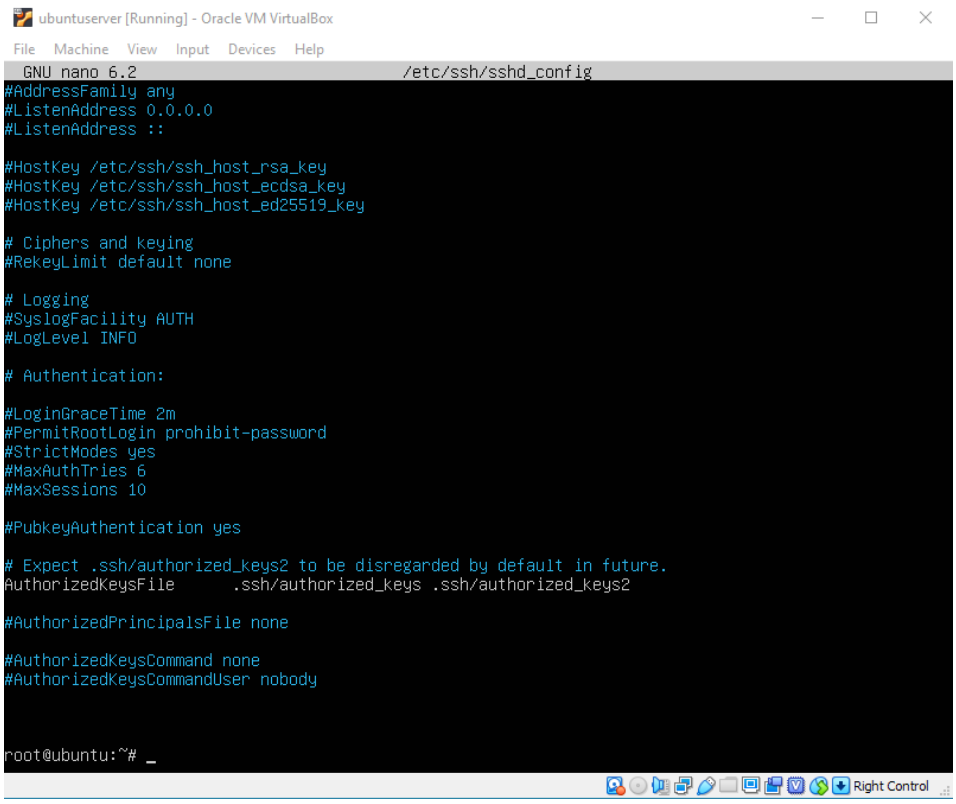




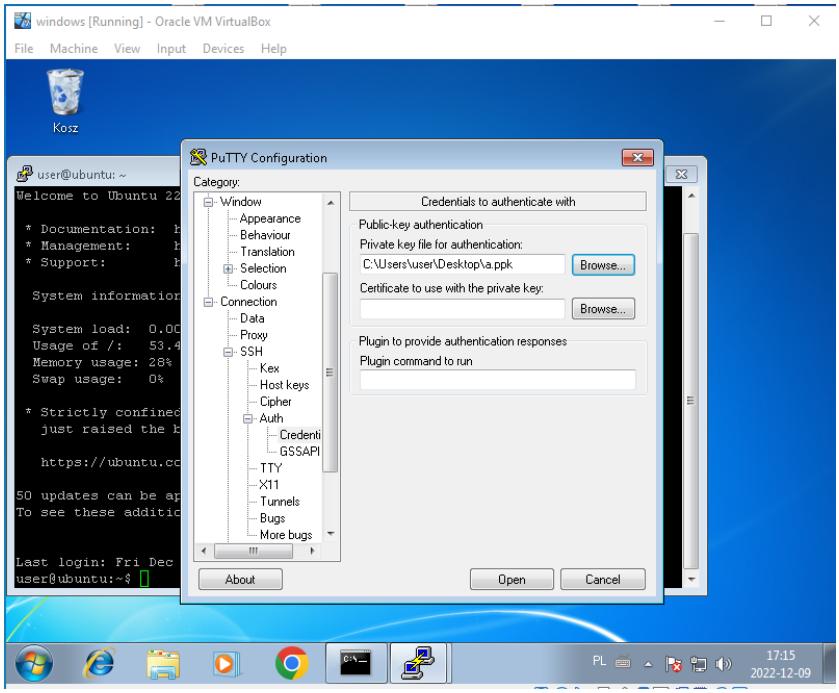
Wpisanie klucza ssh do pliku .ssh/authorized_keys



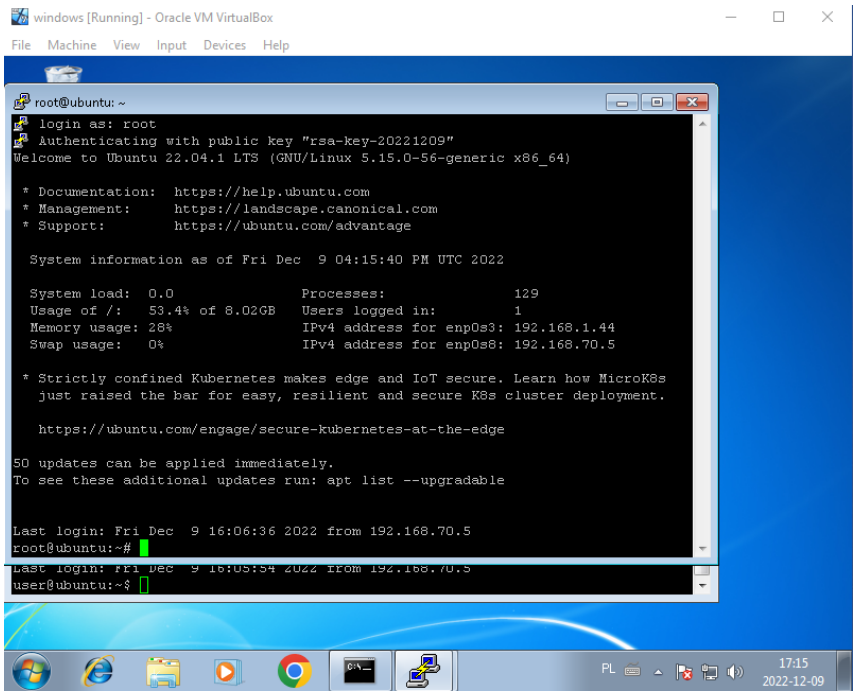
Edycja /etc/ssh/sshd_config - umożliwienie odczytywania kluczy z pliku .ssh/authorized_keys



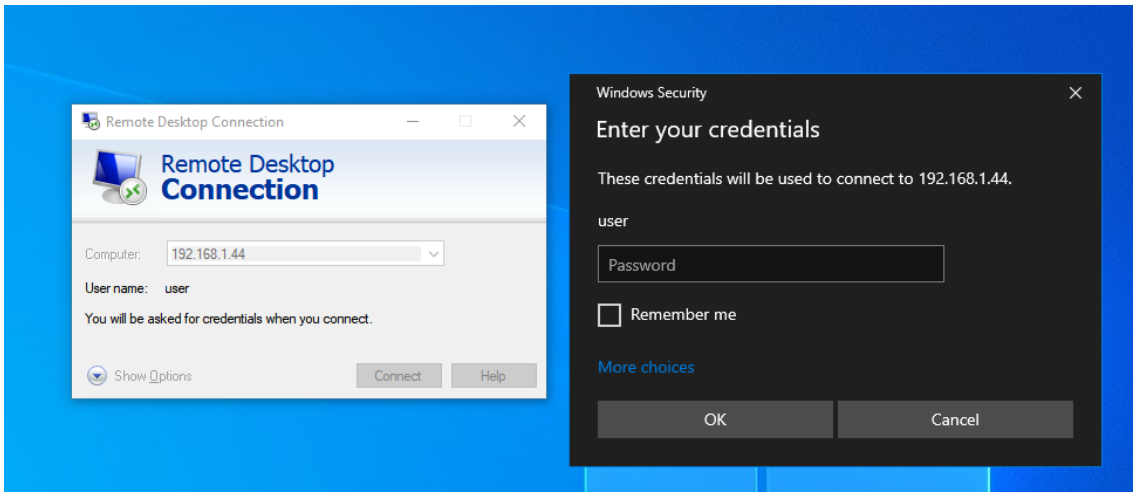
Zaznaczenie pliku z kluczem przy wystawianiu usługi pulpitu zdalnego na port 5000

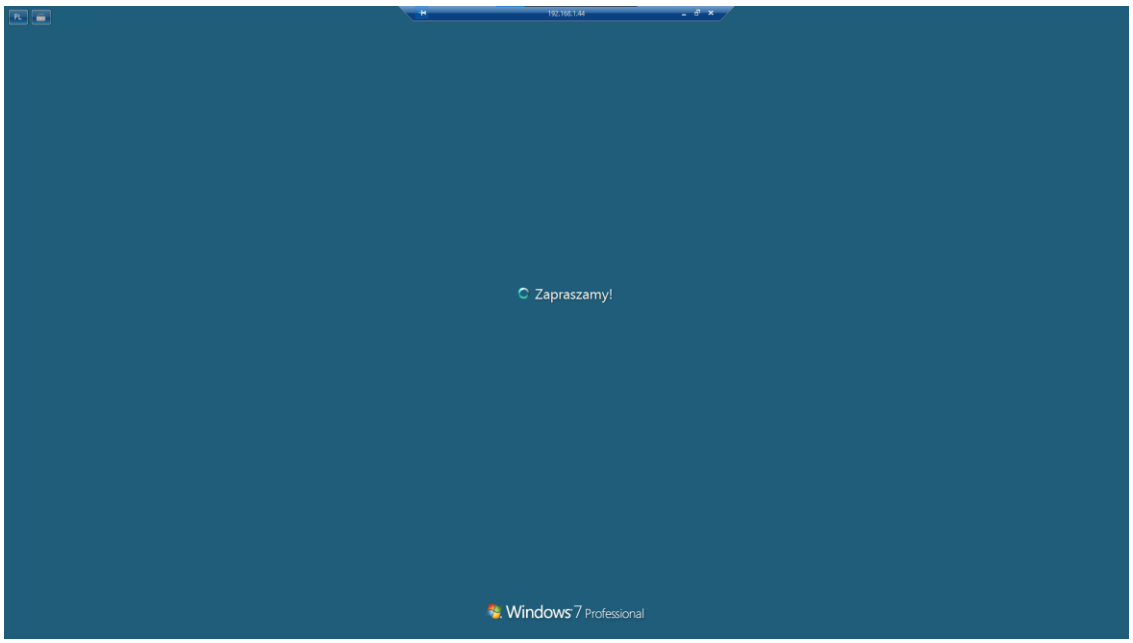


Udane wystawienie bez potrzeby wpisywania hasła do roota

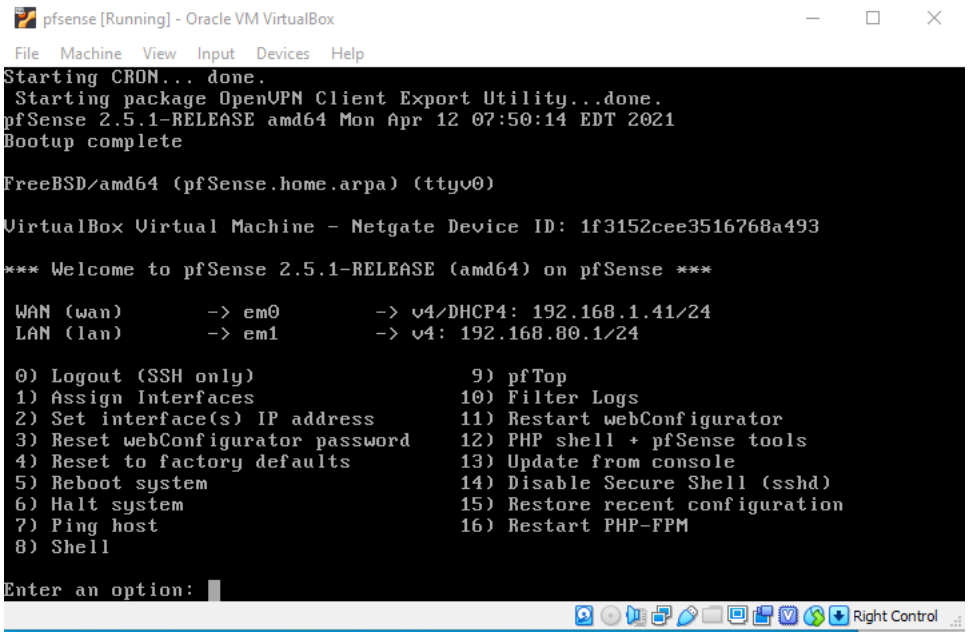


Sprawdzenie czy pulpit zdalny działa

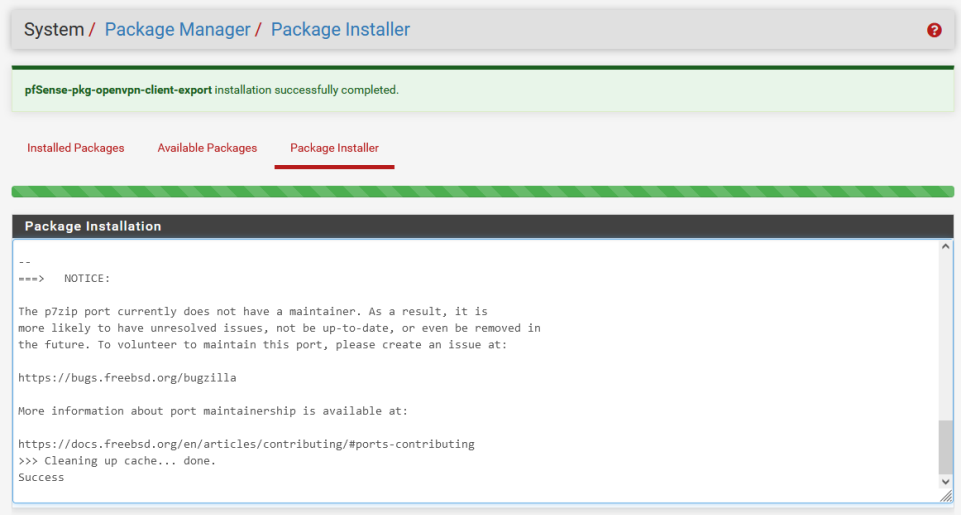


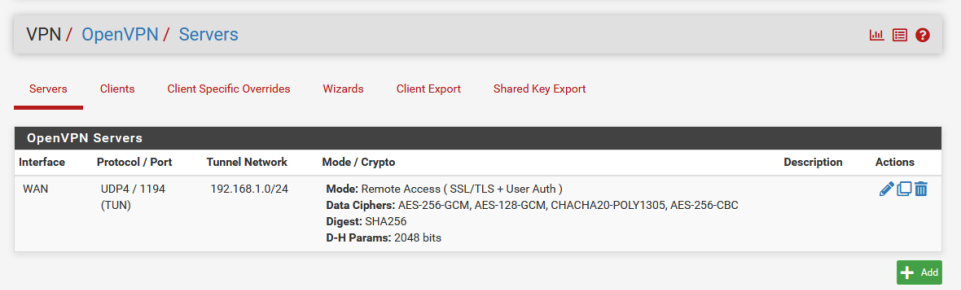


Karty znajdujące się na serwerze

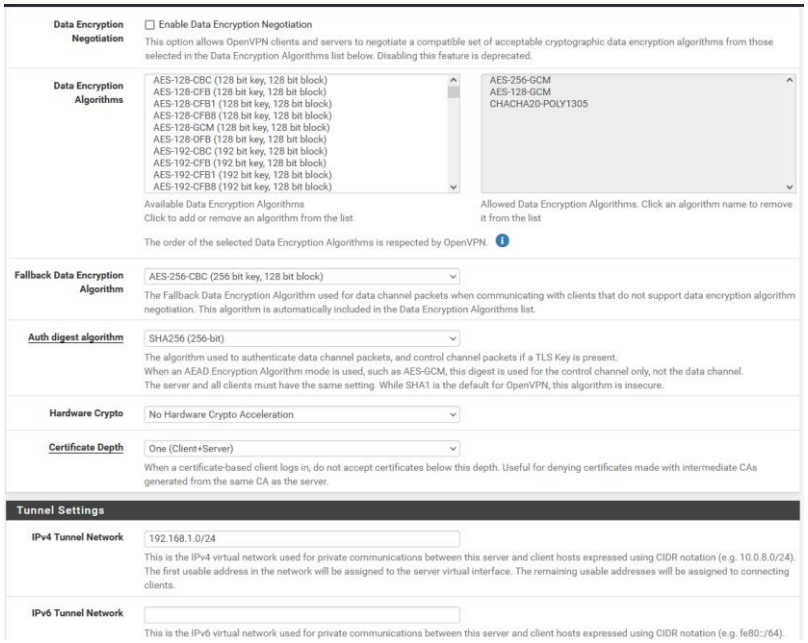


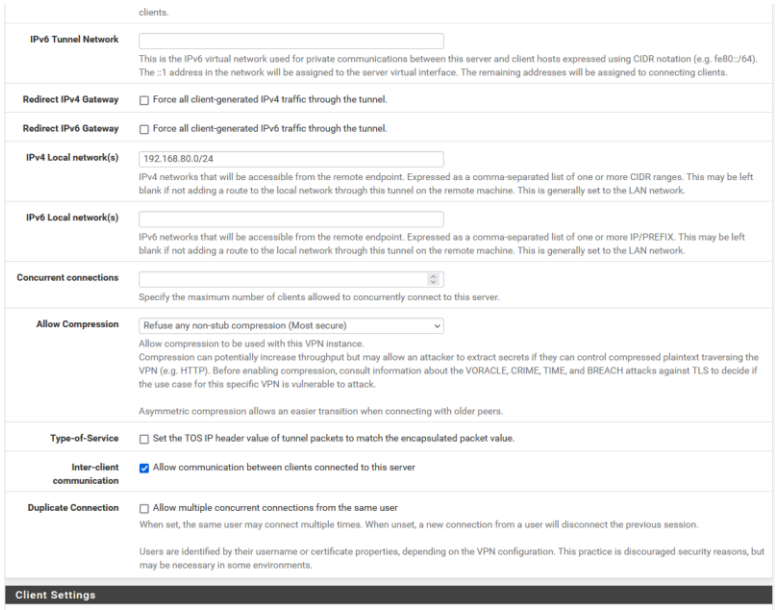
Instalacja VPN

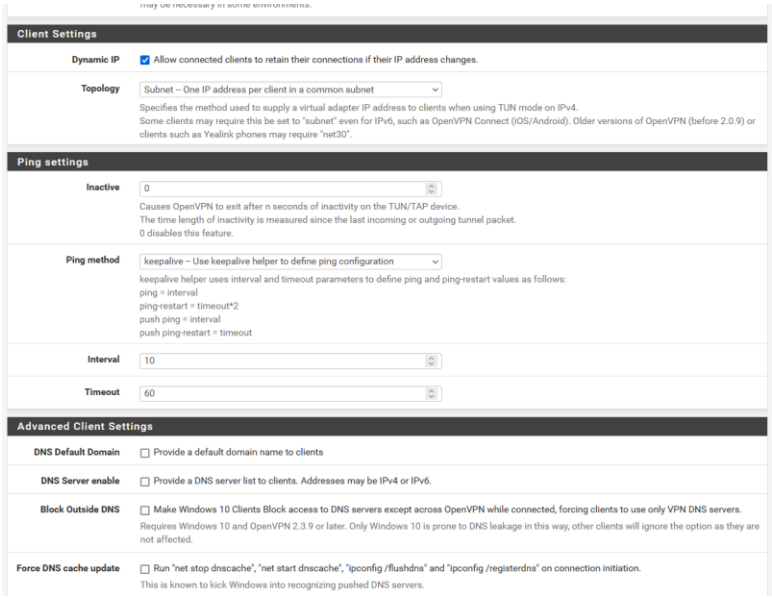


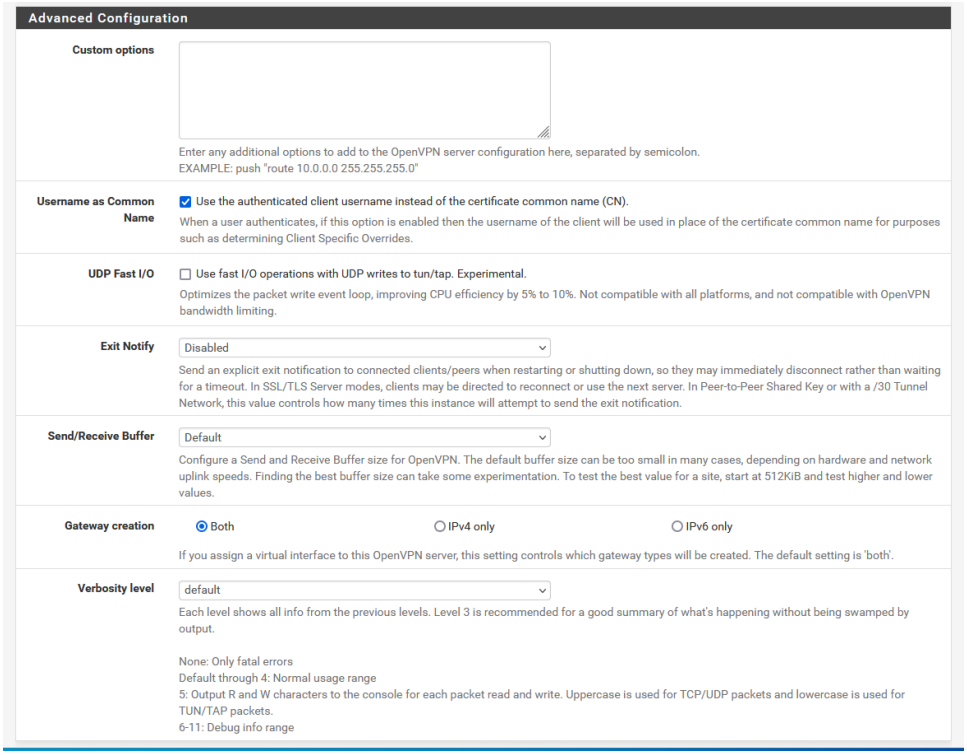


Ustawienia na zainstalowanym VPN

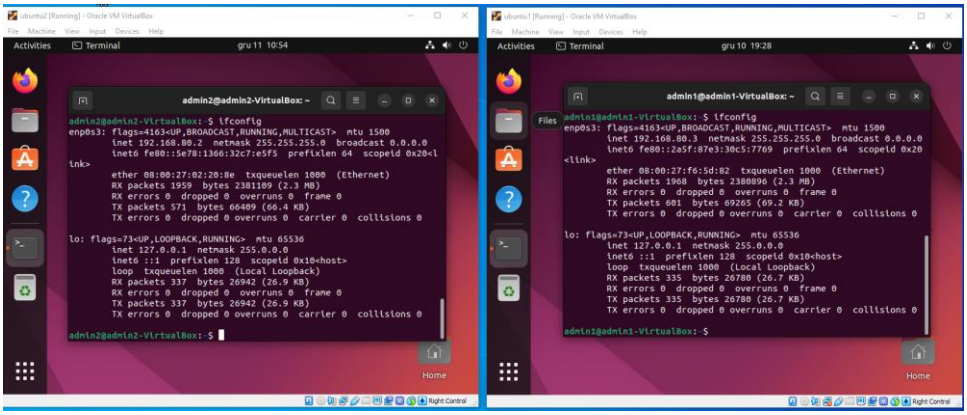

Data Encryption Negotiation
Enable Data Encryption Negotiation
This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.
Data Encryption Algorithms
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
The order of the selected Data Encryption Algorithms is respected by OpenVPN.
Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation. This algorithm is automatically included in the Data Encryption Algorithms list.
Auth digest algorithm
SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware Crypto
No Hardware Crypto Acceleration
Certificate Depth
One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
Tunnel Settings
IPv4 Tunnel Network
192.168.1.0/24
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network
This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64).


clients.
IPv6 Tunnel Network
This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)
192.168.80.0/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent connections
Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.
Asymmetric compression allows an easier transition when connecting with older peers.
Type-of-Service
Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication
Allow communication between clients connected to this server
Duplicate Connection
Allow multiple concurrent connections from the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.
Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.
Client Settings

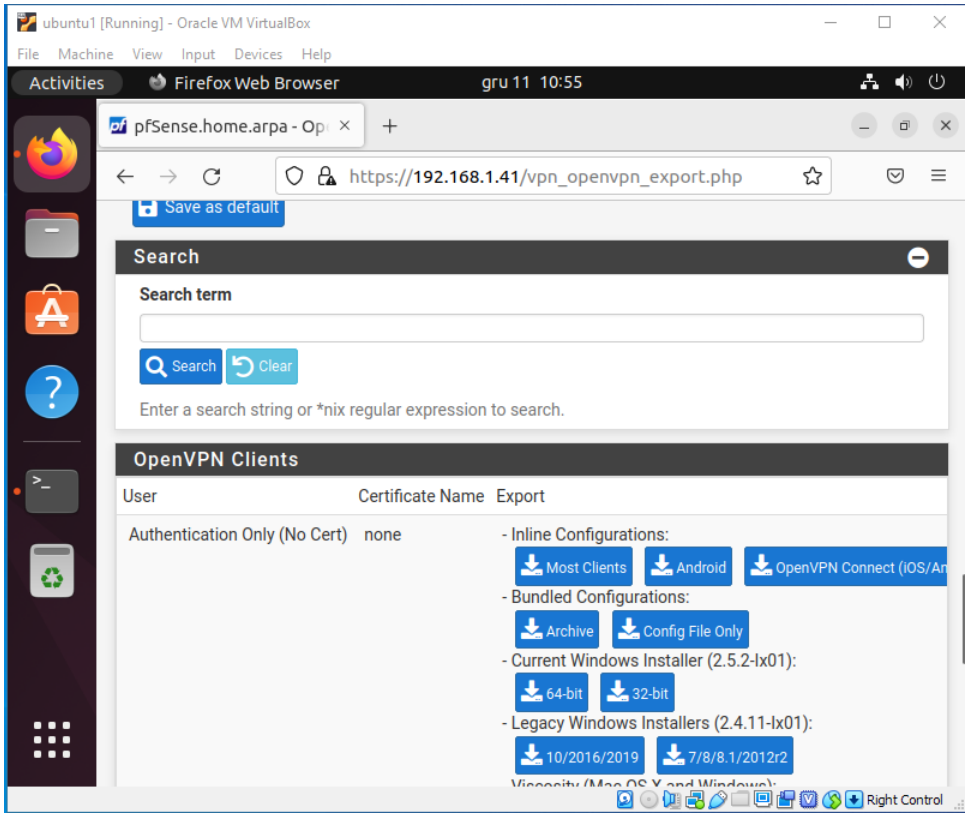




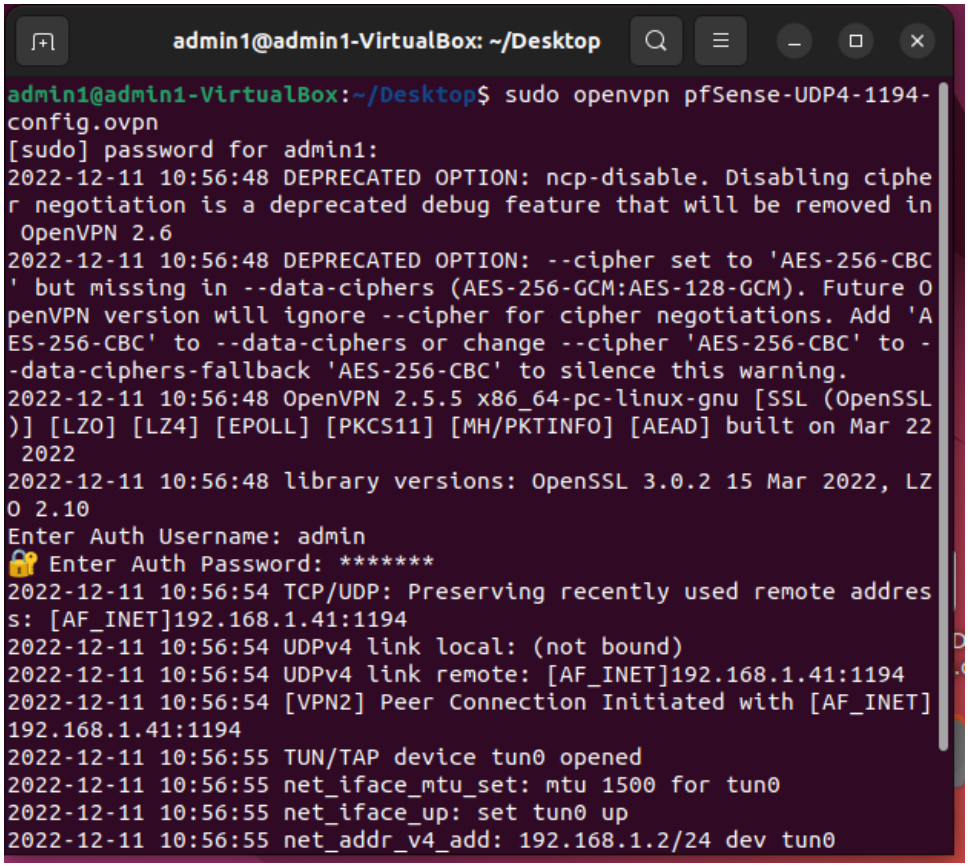
Ustawienia IP na kliencie i gospodarzu



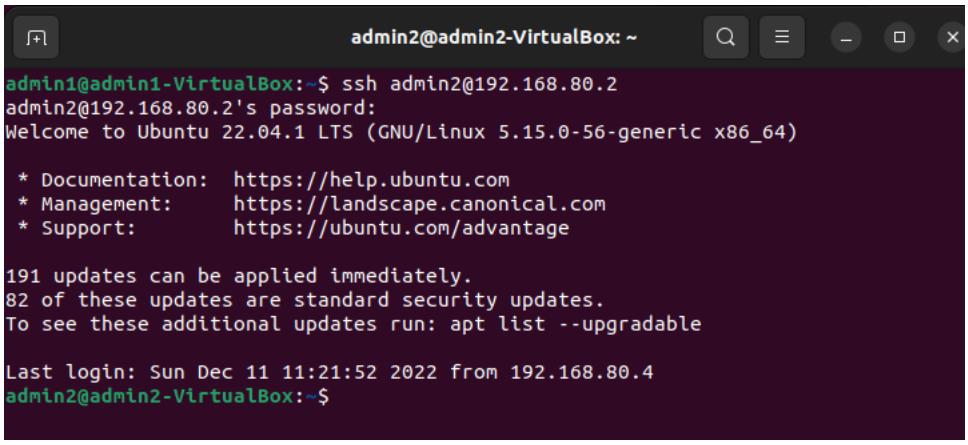
Pobieranie pliku OpenVPN z serwera



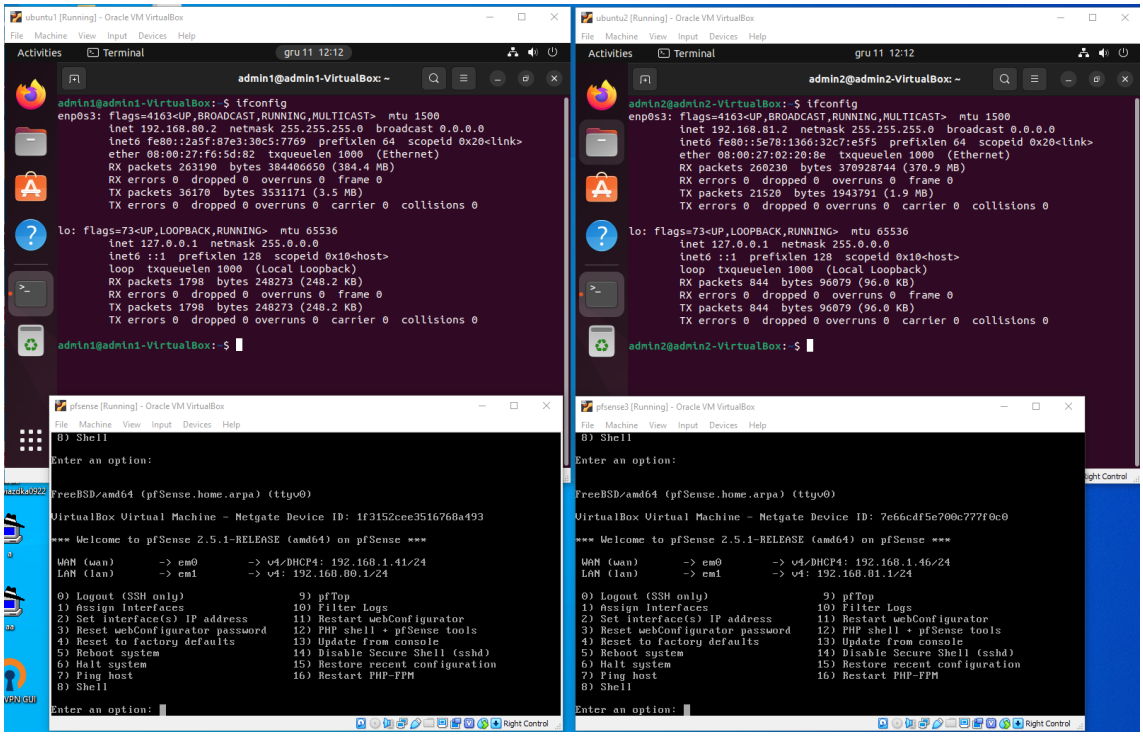
Uruchamianie VPN na komputerze admin1



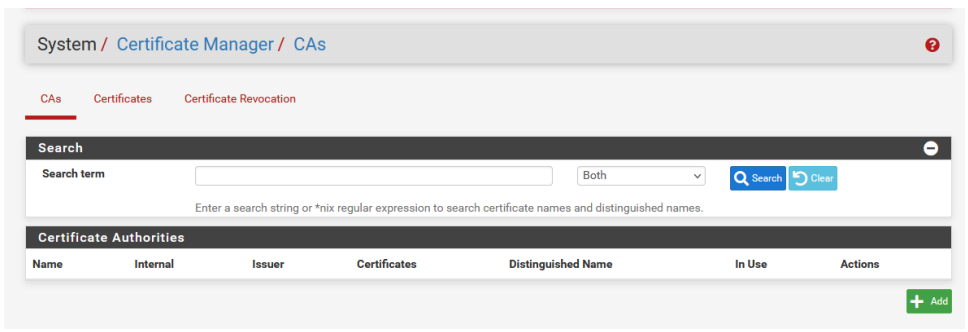
Łączenie się za pomocą ssh do admina2



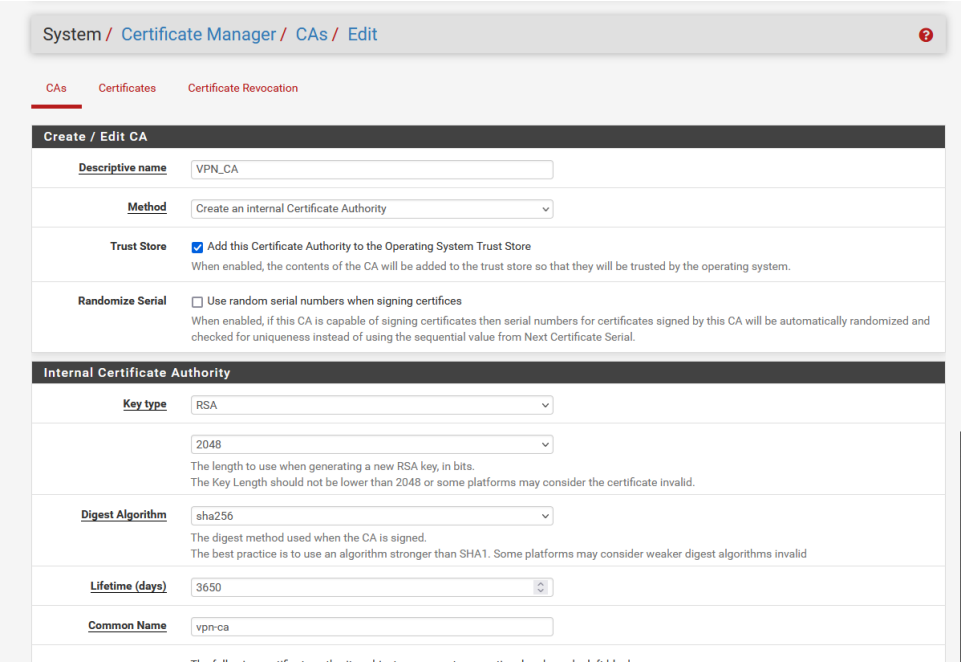
Wstępne ustawienia IP do połączenia peer-to-peer, admin1 pełni rolę serwera, admin2 pełni rolę klienta, 192.168.1.41 pełni rolę centralnej bramy, 192.168.1.46 pełni rolę zdalnej bramy

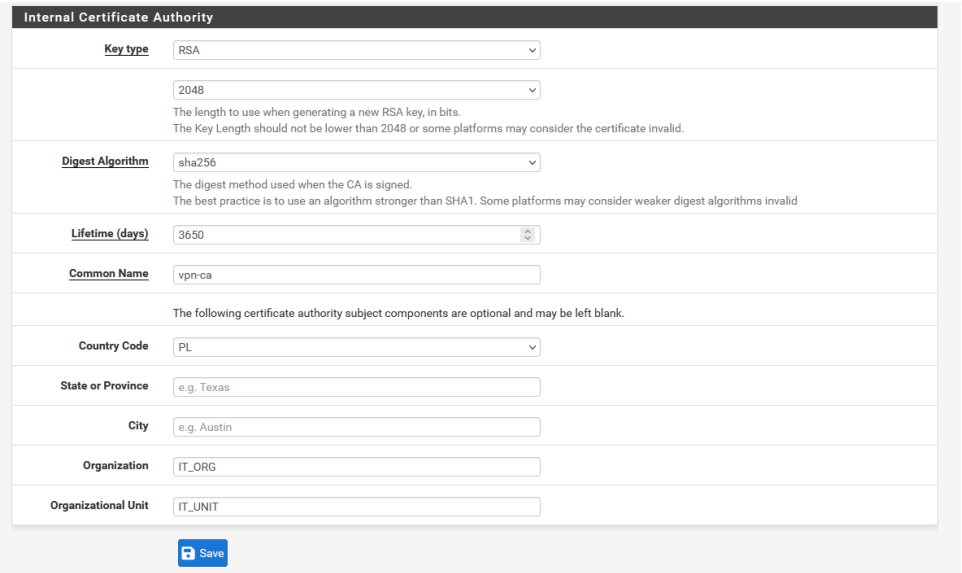


Tworzenie lokalnego certyfikatu na centralnej bramie VPN

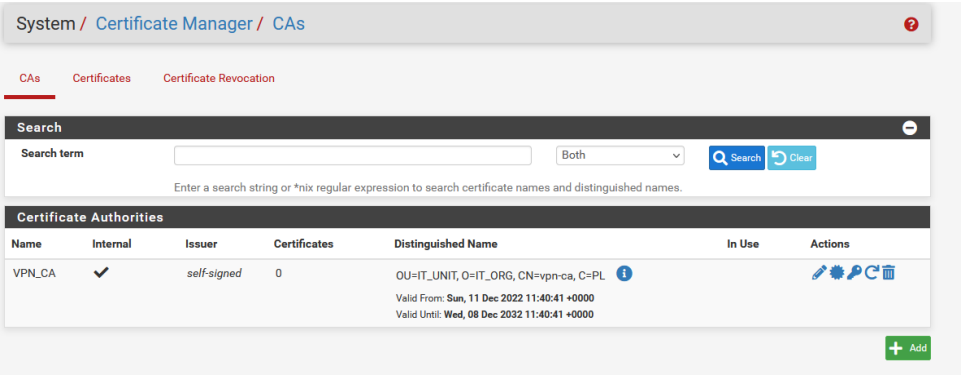


Zaznaczenie, że certyfikatowi można ufać

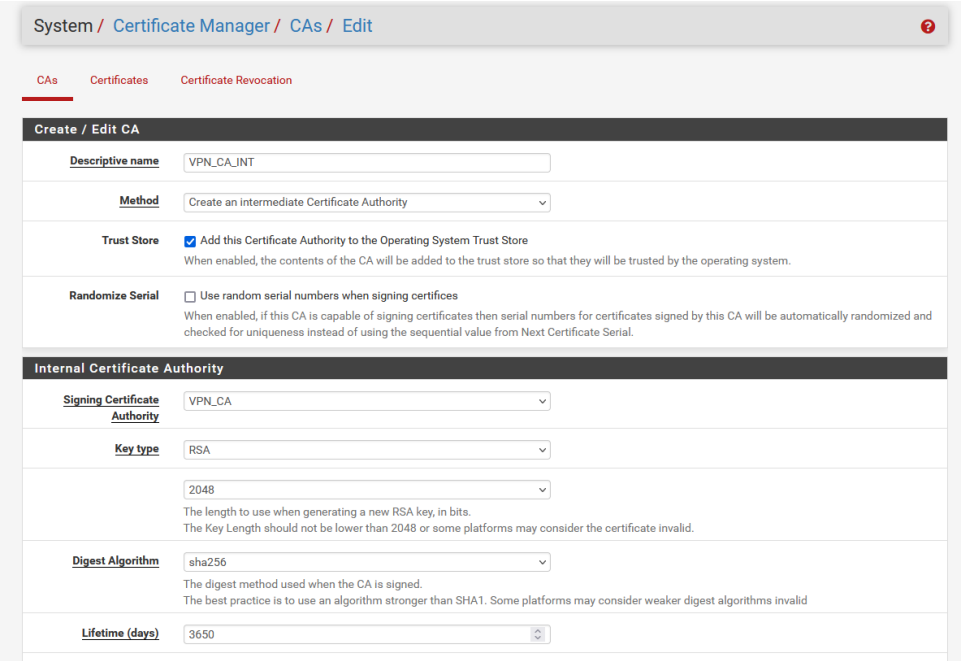


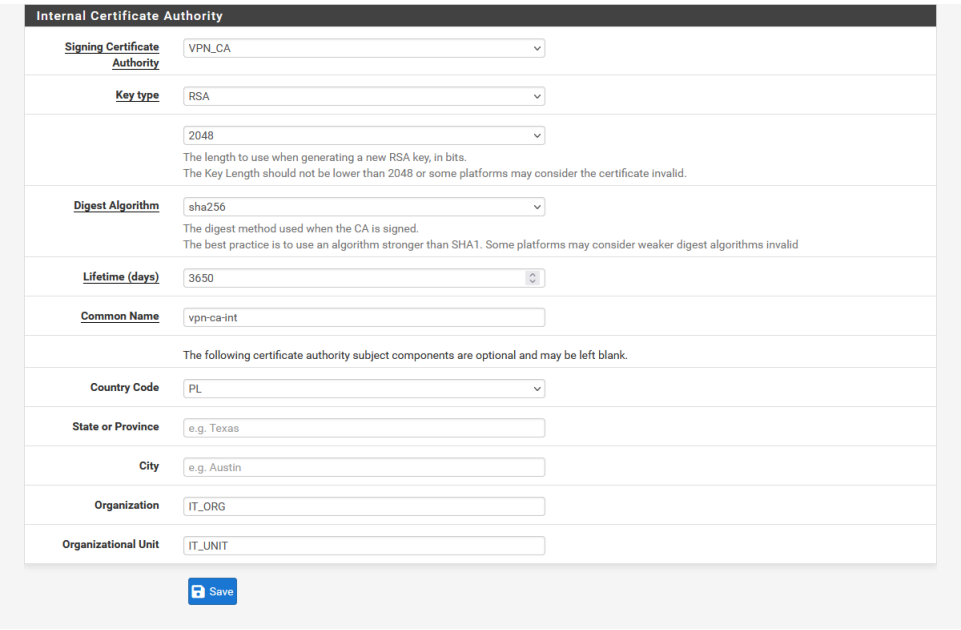


Utworzony certyfikat

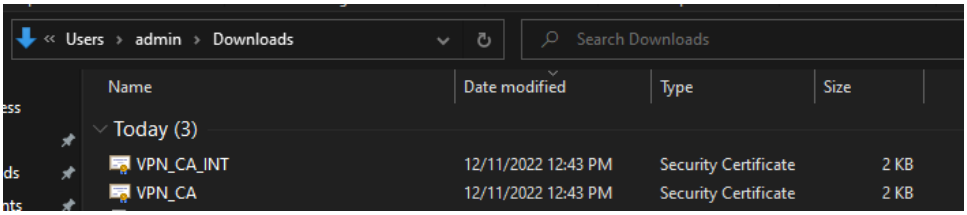


Tworzenie certyfikatu pośredniego, który jest podpisany przez utworzony wcześniej certyfikat VPN_CA

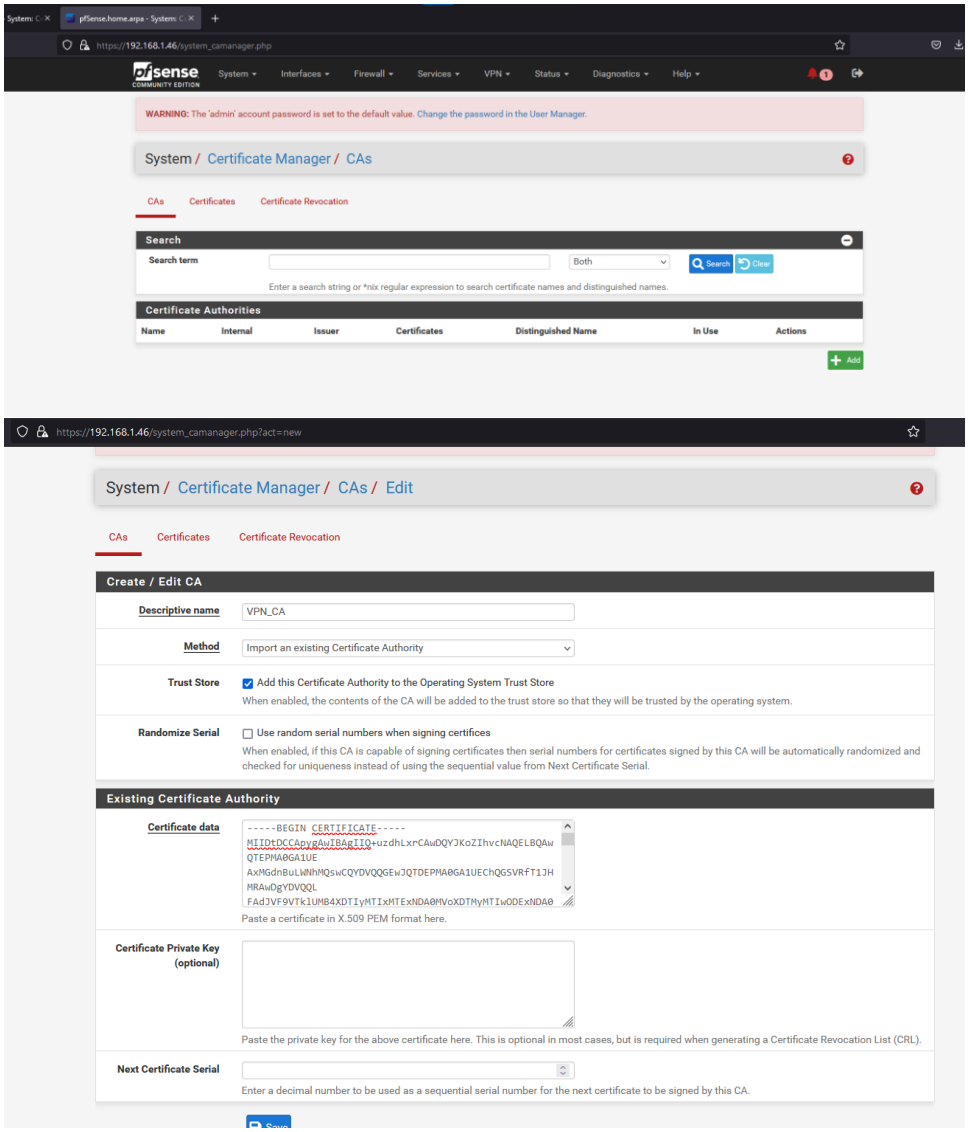


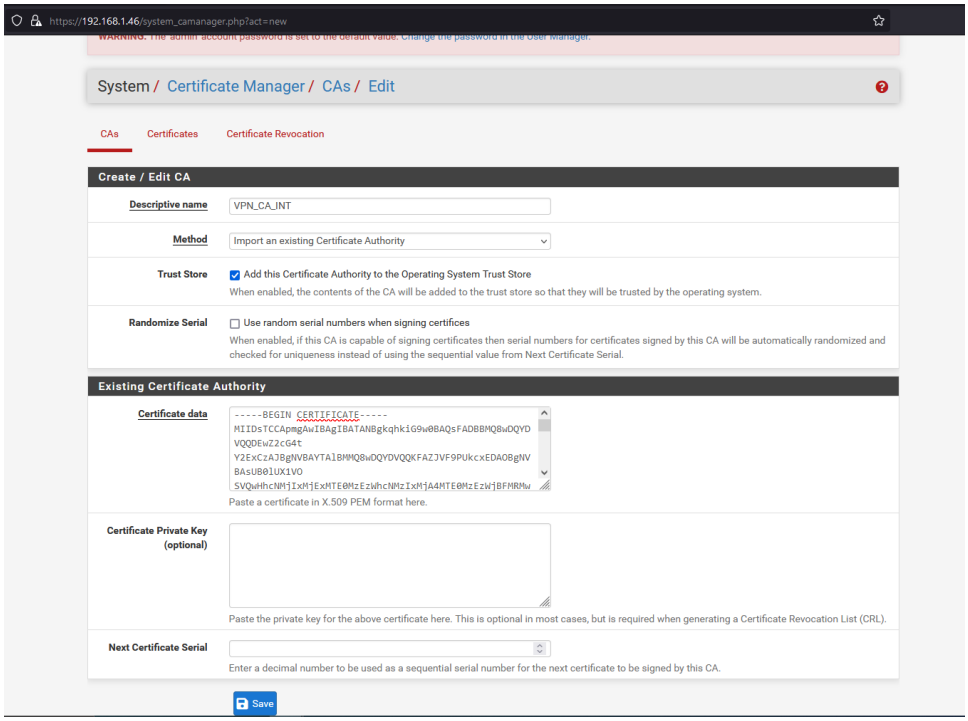


Pobranie obydwóch certyfikatów

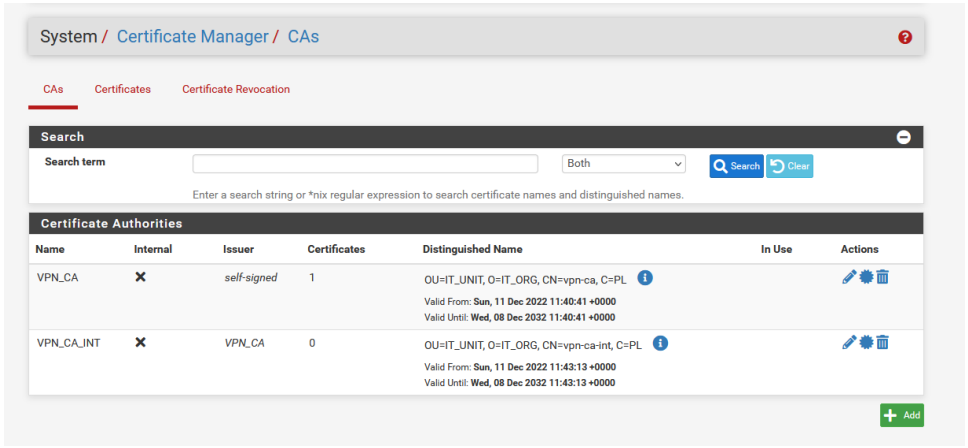


Importowanie certyfikatów na zdalną bramę VPN

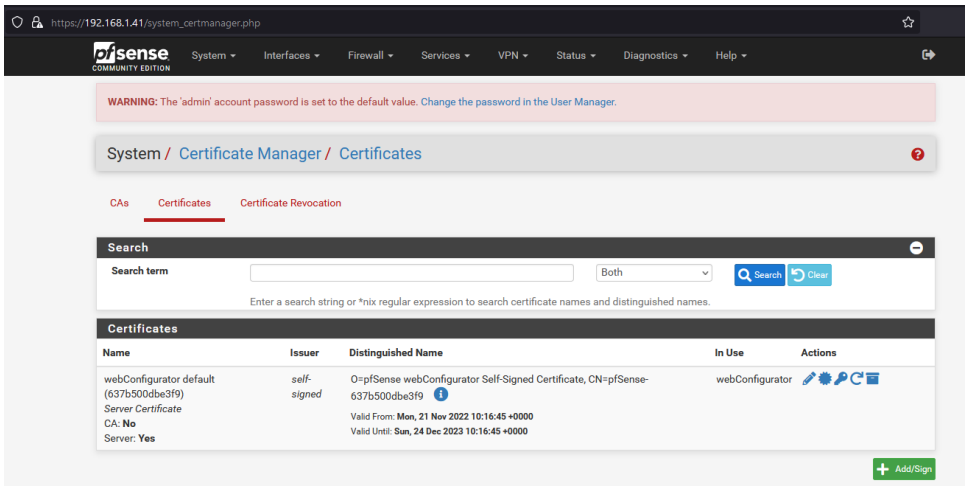




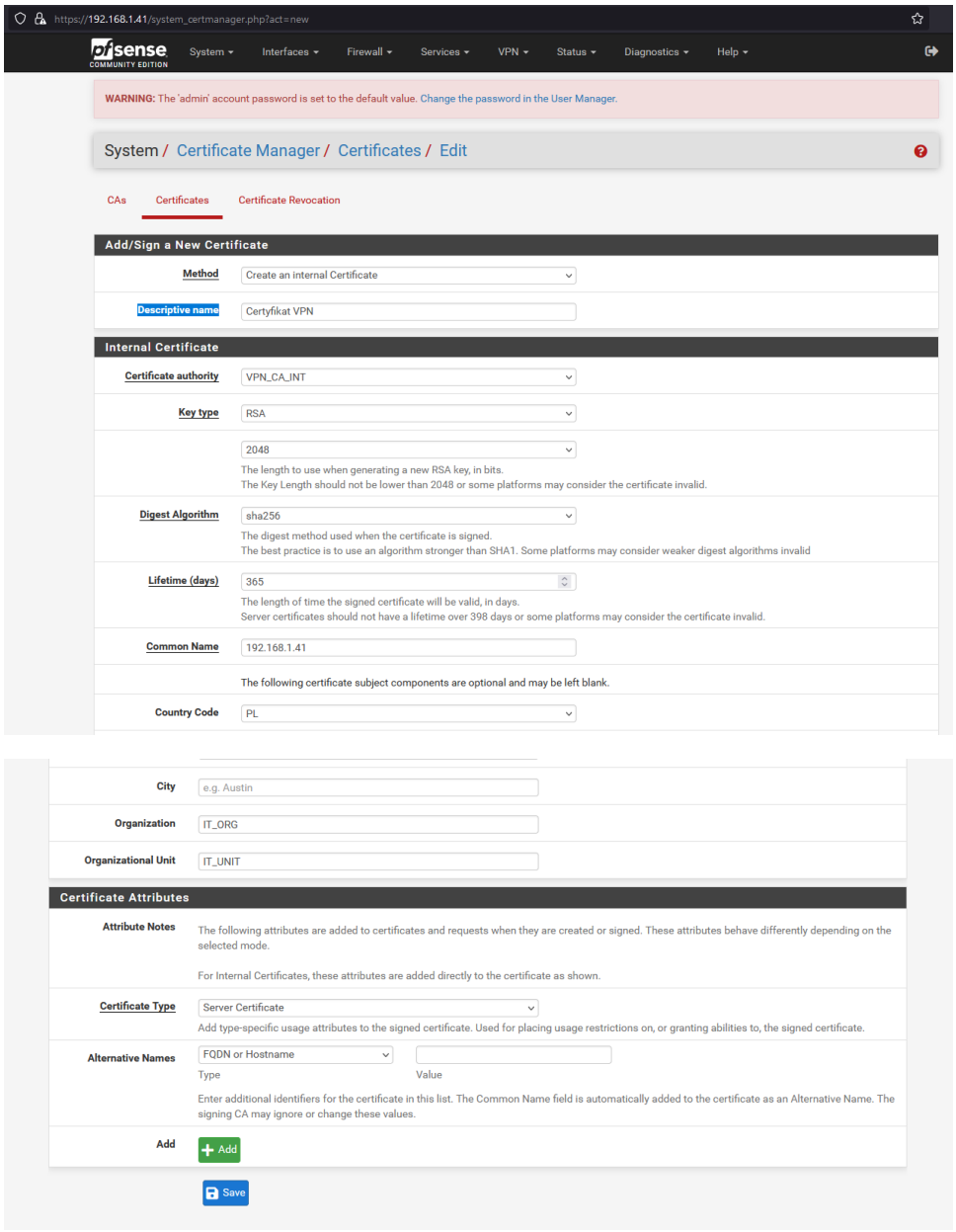
Utworzone kopie certyfikatów



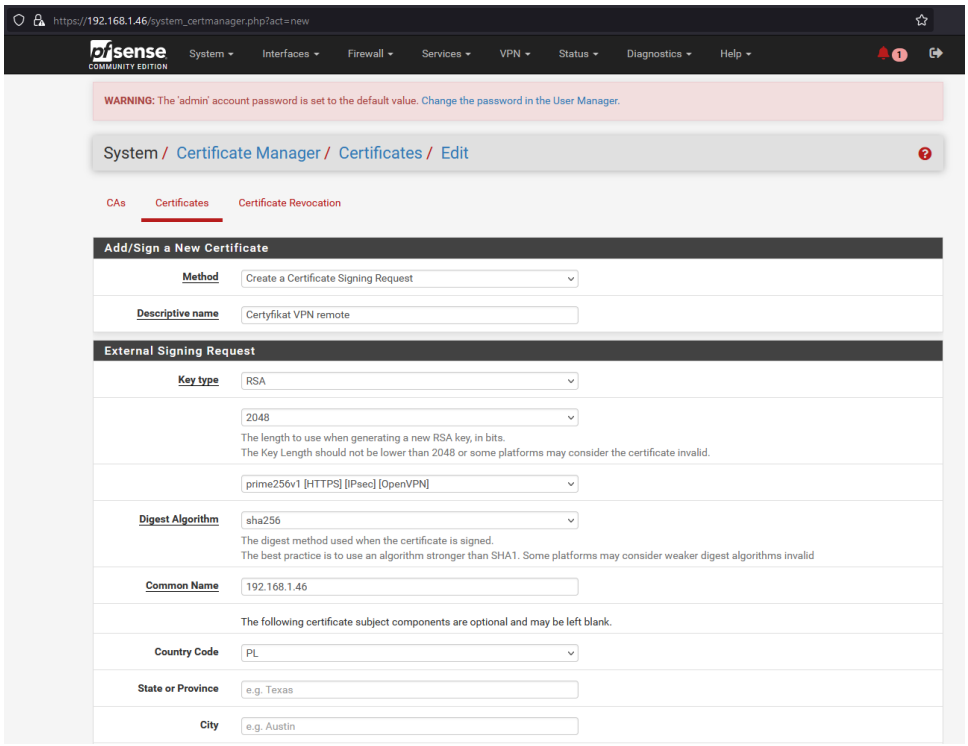
Utworzenie w centralnej bramie certyfikatu bramy centralne w zakładce Certificates

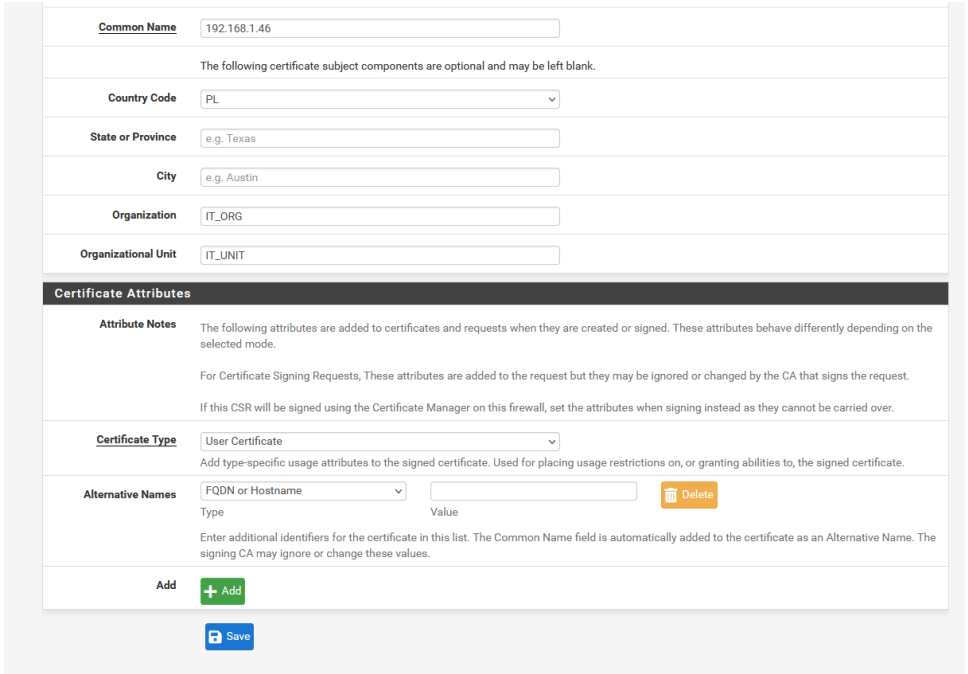


Zaznaczenie certyfikatu pośredniego, typ certyfikatu jako serwerowy, common name jako adres WAN

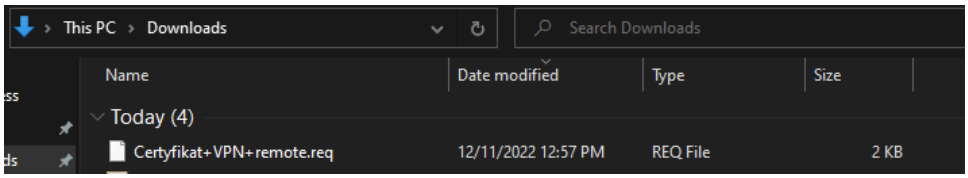


Utworzenie na bramie zdalnej certyfikat signing request, common name to adres WAN, typ certyfikatu to user

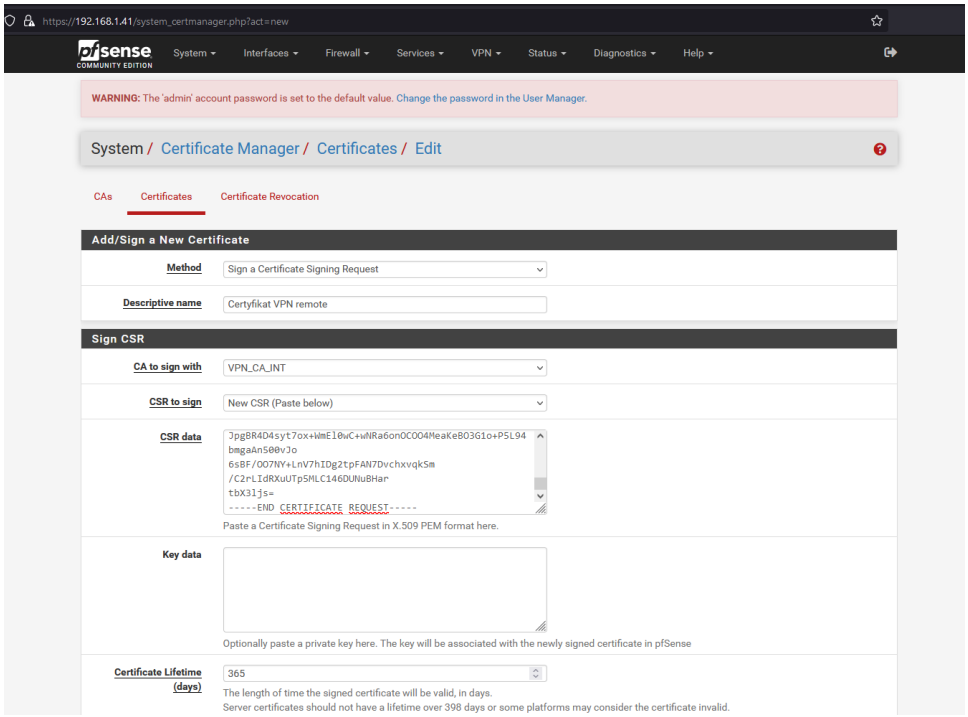


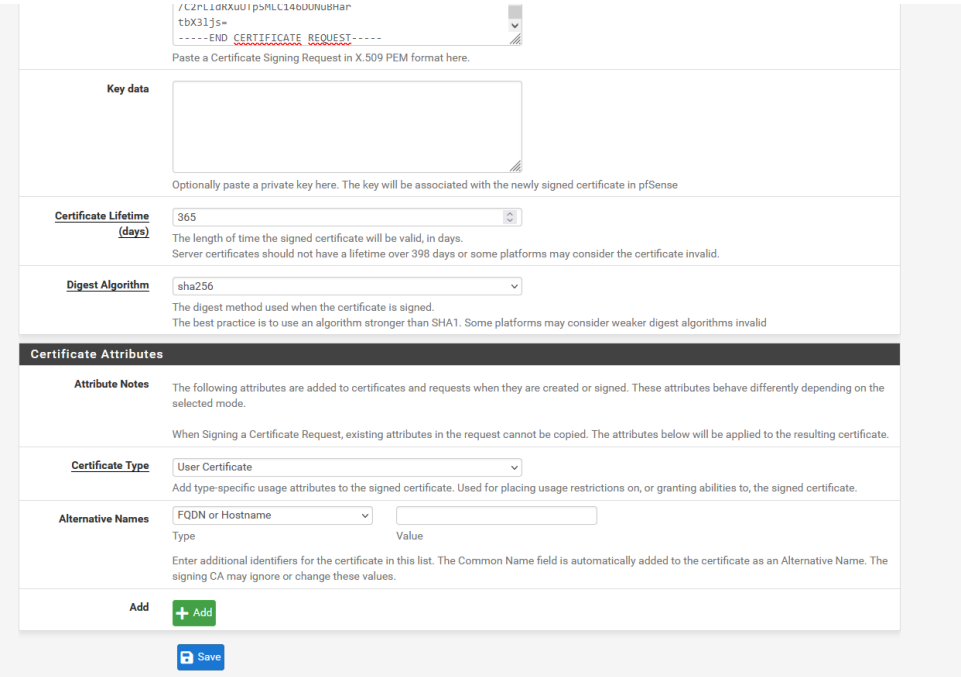


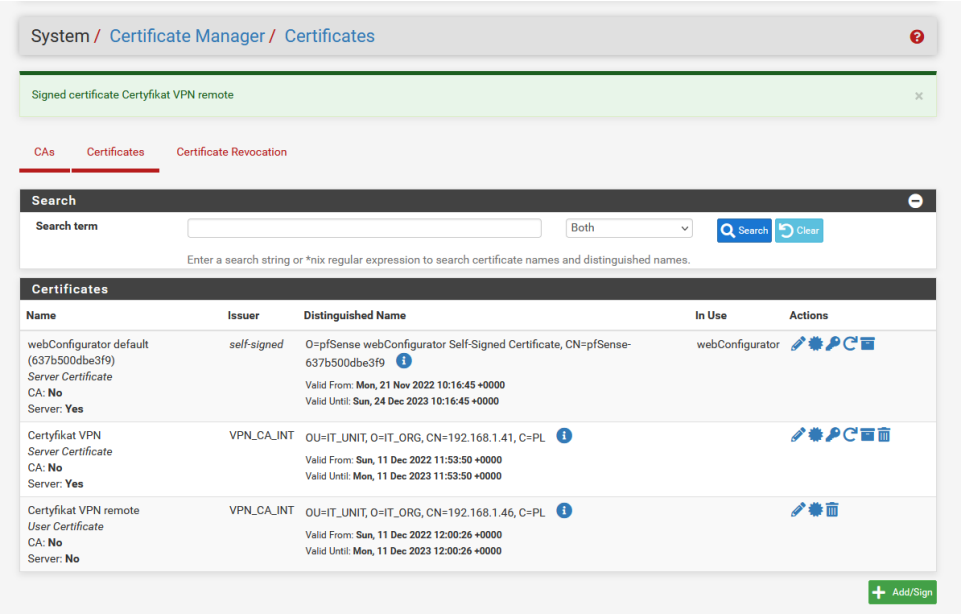
Pobranie utworzonego certyfikatu



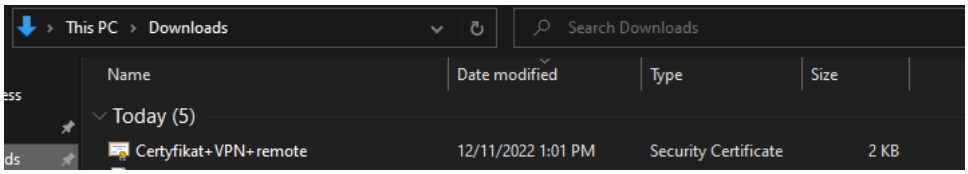
Zaimportowanie pobranego certyfikatu do bramy centralnej



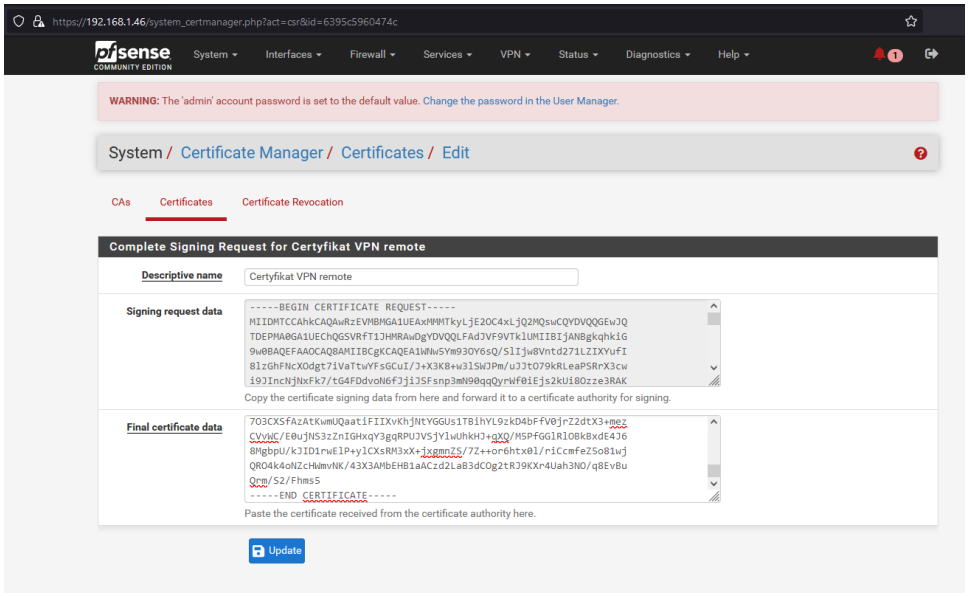




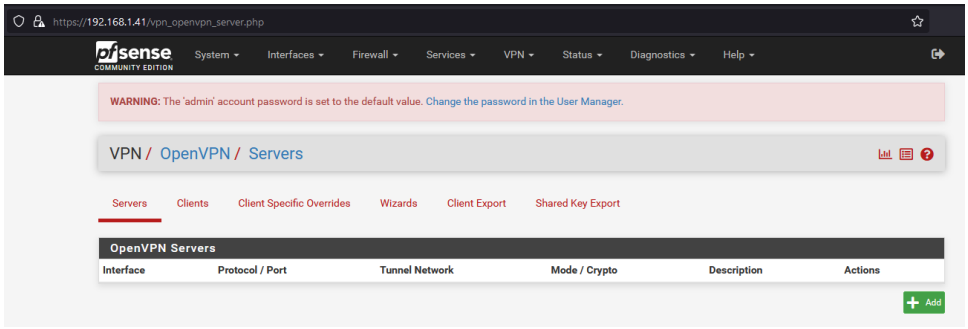
Pobranie utworzonego certyfikatu

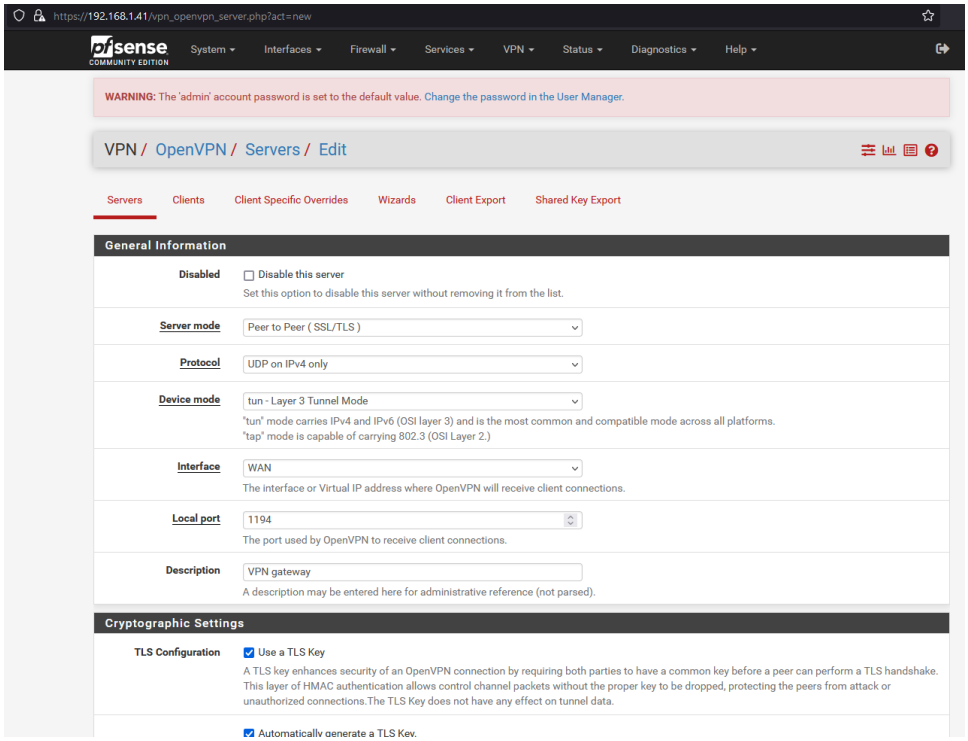


Doklejenie pobranego pliku do certyfikatu CSR na bramie zdalnej



Konfiguracja OpenVPN na bramie centralnej jako tunel między bramami wybrano 192.168.82.0/24





Cryptographic Settings

TLS Configuration

☑ Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.

☑ Automatically generate a TLS Key.

Peer Certificate Authority: VPN_CA_INT

Peer Certificate Revocation list: No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

OCSP Check: ☐ Check client certificates with OCSP

Server certificate: Certyfikat VPN (Server: Yes, CA: VPN_CA_INT)

DH Parameter Length: 2048 bit

Diffie-Hellman (DH) parameter set used for key exchange.

ECDH Curve: Use Default

The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Negotiation

☑ Enable Data Encryption Negotiation

This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

Data Encryption Algorithms

Available Data Encryption Algorithms	Allowed Data Encryption Algorithms
AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-CFB8 (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-192-CBC (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block)	AES-256-GCM AES-128-GCM CHACHA20-POLY1305

Click to add or remove an algorithm from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN.

Available Data Encryption Algorithms	Allowed Data Encryption Algorithms
AES-192-CFB (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block)	

Click to add or remove an algorithm from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN.

Fallback Data Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation. This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm: SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto: No Hardware Crypto Acceleration

Certificate Depth: Two (Client+Intermediate+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Tunnel Settings

IPv4 Tunnel Network: 192.168.82.0/24

This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network:

This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

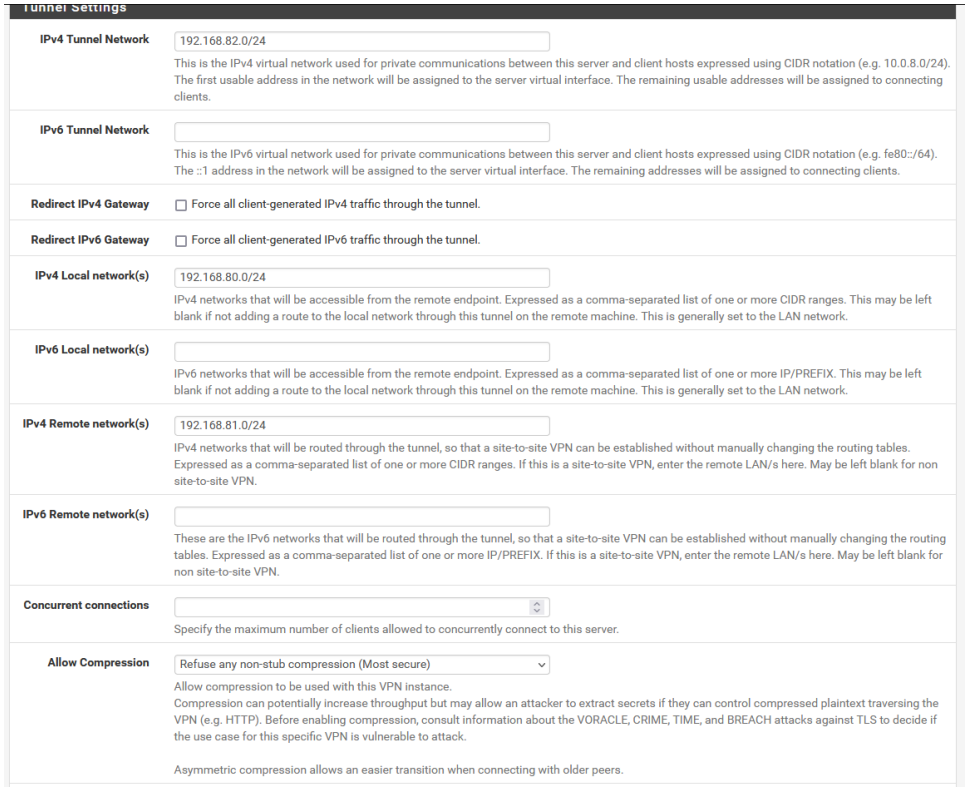
Redirect IPv4 Gateway: ☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway: ☐ Force all client-generated IPv6 traffic through the tunnel.

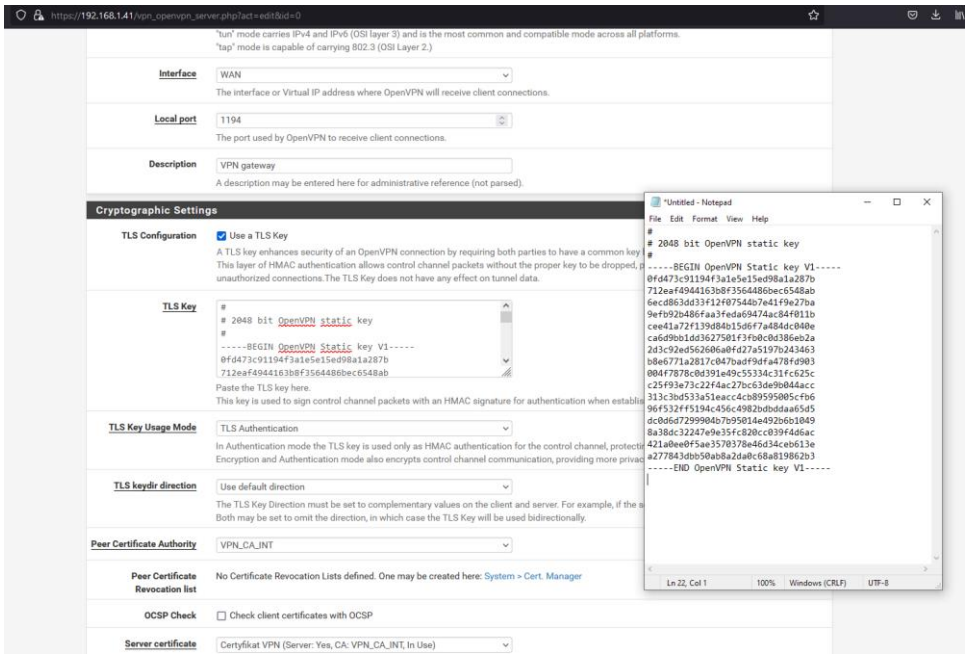
IPv4 Local network(s): 192.168.80.0/24

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

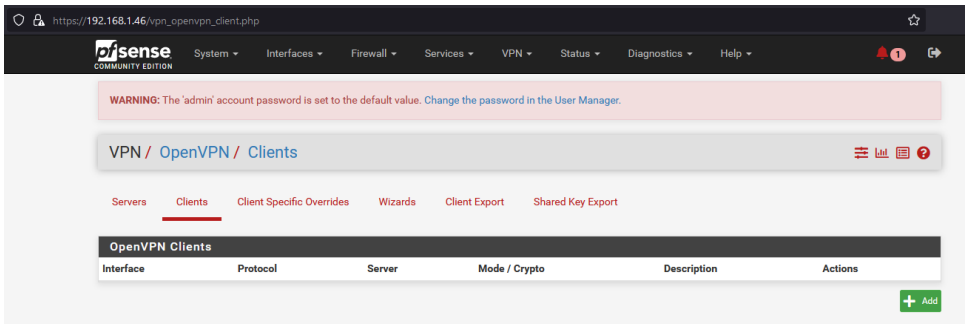
IPv6 Local network(s):

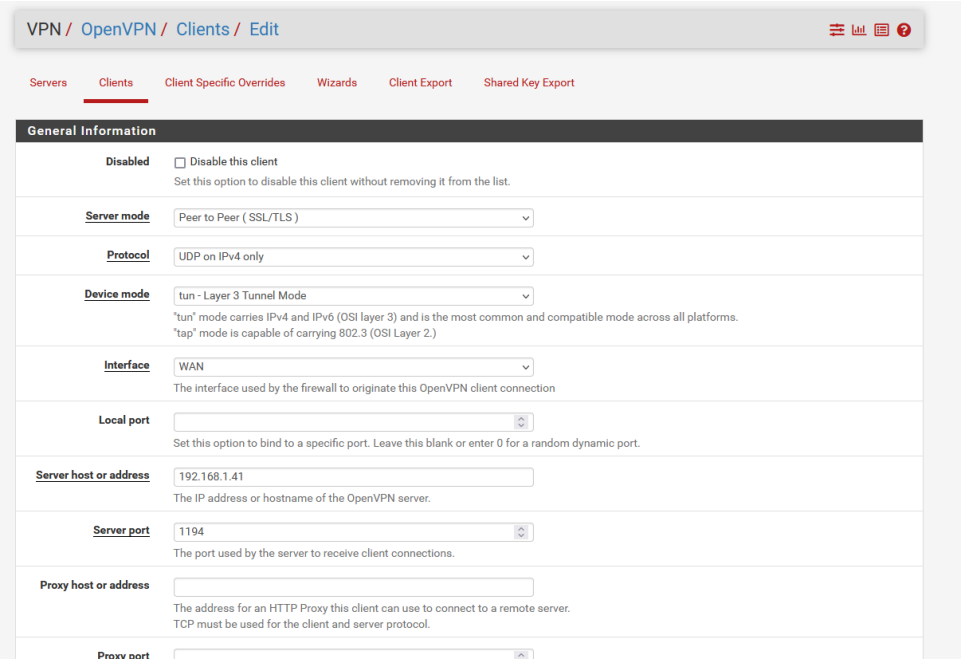


Po skonfigurowaniu OpenVPN należy skopiować klucz TLS



Konfiguracja OpenVPN na bramie zdalnej, należy skopiować zapisany wcześniej klucz TLS, zamiast generowania nowego





User Authentication Settings

Username

Leave empty when no user name is needed

Password

Leave empty when no password is needed

Authentication Retry

☐ Do not retry connection when authentication fails

When enabled, the OpenVPN process will exit if it receives an authentication failure message. The default behavior is to retry.

Cryptographic Settings

TLS Configuration

☑ Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.

☐ Automatically generate a TLS Key.

TLS Key

```
96f532ff5194c456c4982bdbddaa65d5
dc0d6d7299904b7b95014e492b6b1049
8a38dc32247e9e35fc820cc039f4d6ac
421a0ee0f5ae3570378e46d34ceb613e
a277843dbb50ab8a2da0c68a819862b3
-----END OpenVPN Static key V1-----
```

Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode

TLS Authentication

In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction

Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority

VPN_CA_INT

Peer Certificate Revocation list

No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation

Client Certificate

Certyfikat VPN remote (CA: VPN_CA_INT)

Peer Certificate Authority

VPN_CA_INT

Peer Certificate Revocation list

No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation

Client Certificate

Certyfikat VPN remote (CA: VPN_CA_INT)

Data Encryption Negotiation

☑ Enable Data Encryption Negotiation

This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

Data Encryption Algorithms

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

- AES-128-CBC (128 bit key, 128 bit block)
- AES-128-CFB (128 bit key, 128 bit block)
- AES-128-CFB1 (128 bit key, 128 bit block)
- AES-128-CFB8 (128 bit key, 128 bit block)
- AES-128-GCM (128 bit key, 128 bit block)
- AES-128-OFB (128 bit key, 128 bit block)
- AES-192-CBC (192 bit key, 128 bit block)
- AES-192-CFB (192 bit key, 128 bit block)
- AES-192-CFB1 (192 bit key, 128 bit block)
- AES-192-CFB8 (192 bit key, 128 bit block)

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

- AES-256-GCM
- AES-128-GCM
- CHACHA20-POLY1305

The order of the selected Data Encryption Algorithms is respected by OpenVPN.

Fallback Data Encryption Algorithm

AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation. This algorithm is automatically included in the Data Encryption Algorithms list.

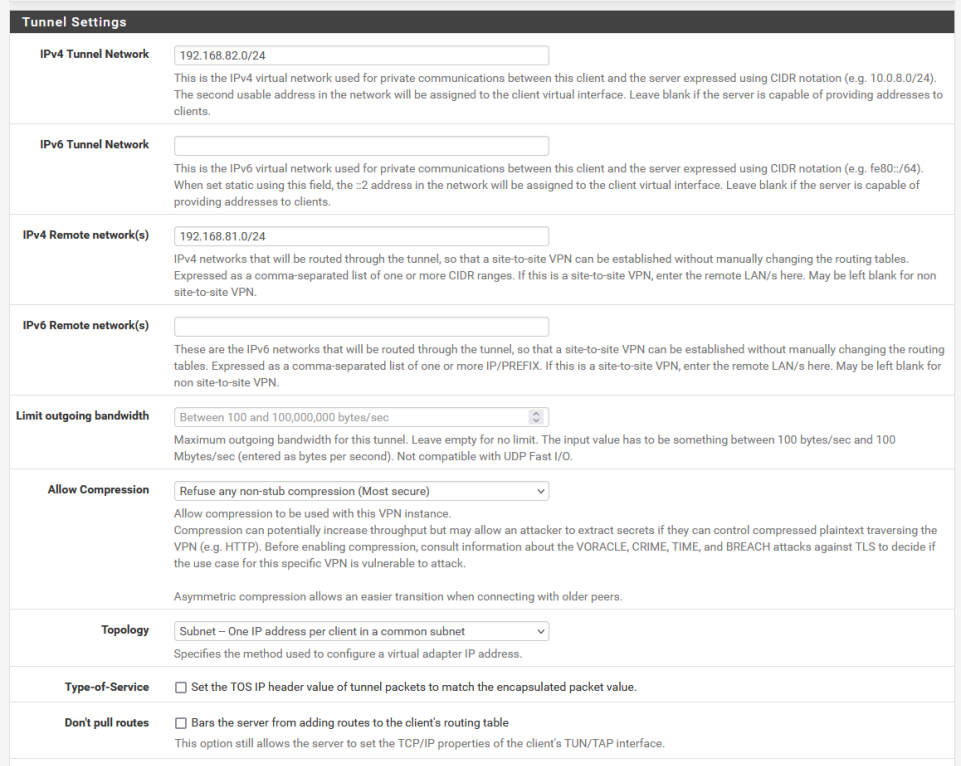
Auth digest algorithm

SHA256 (256-bit)

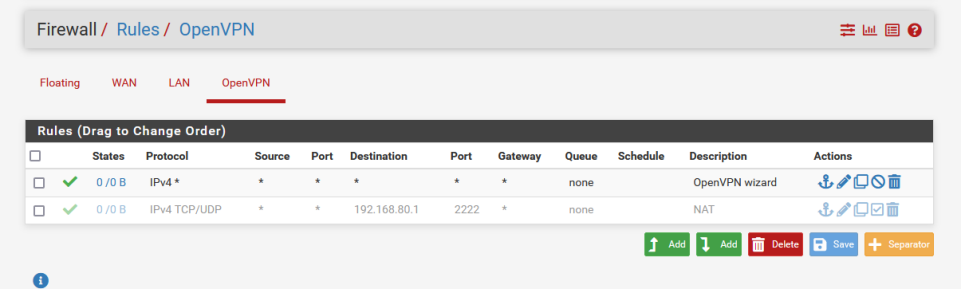
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto

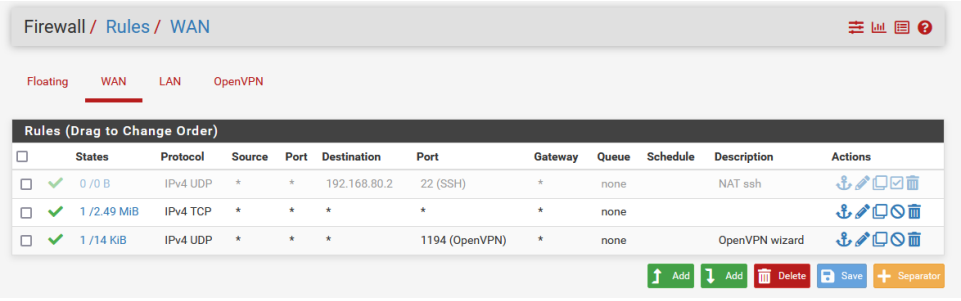
No Hardware Crypto Acceleration

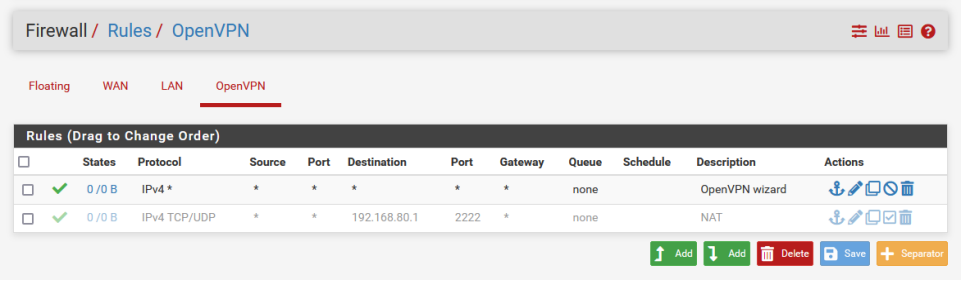


Konfiguracja zasad firewalla na bramie zdalnej do OpenVPN

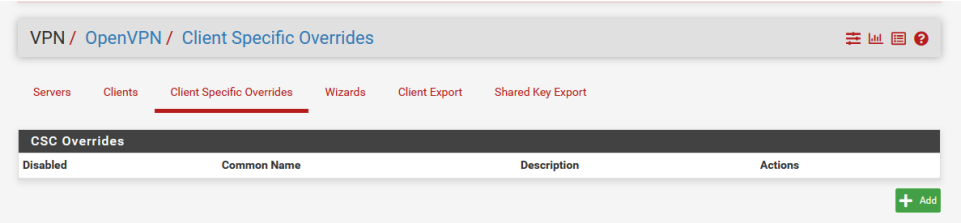


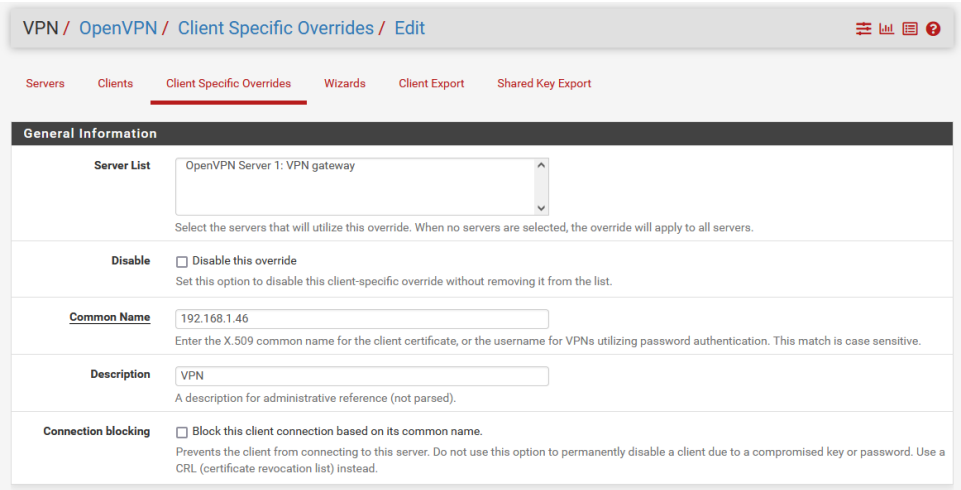
Konfiguracja zasad firewalla na bramie centralnej do WAN i OpenVPN

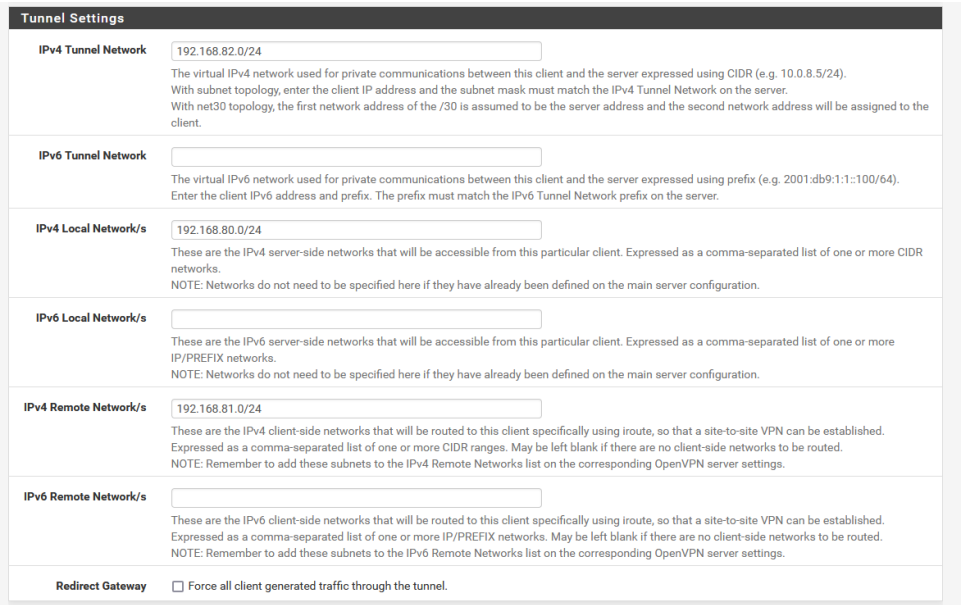




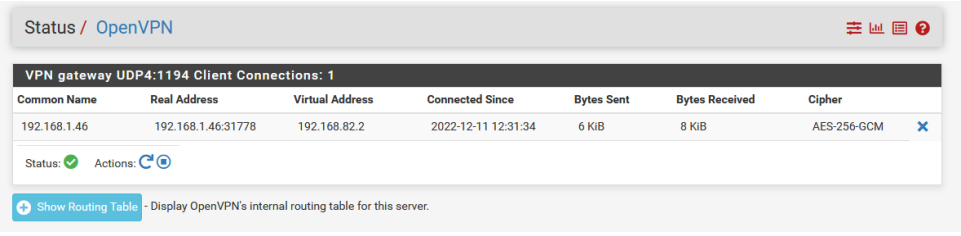
Nadpisanie zasad dla konkretnego klienta



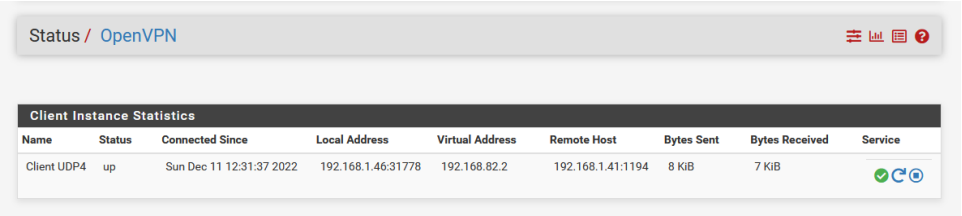




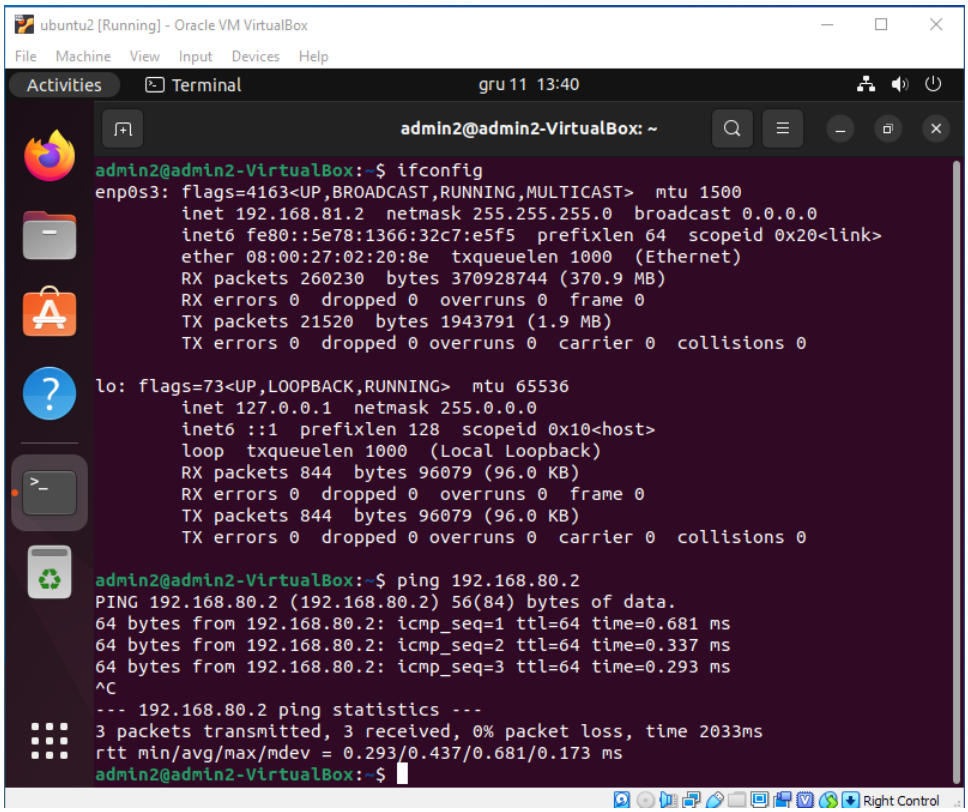
Sprawdzenie czy VPN działa na bramie centralnej



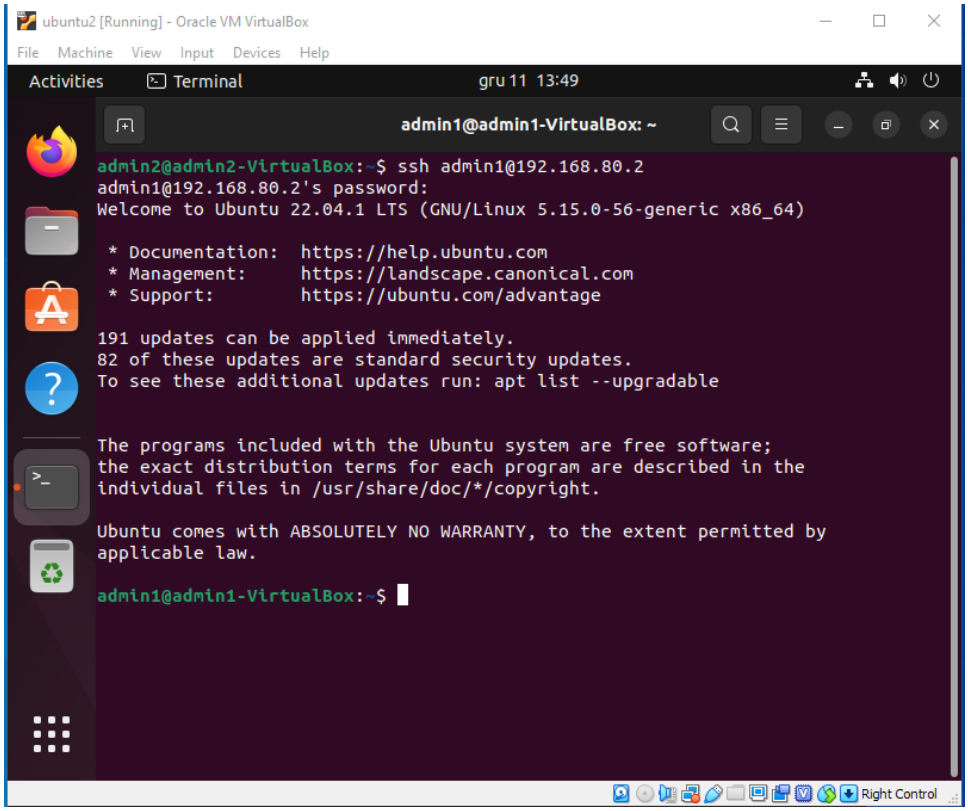
Sprawdzenie czy VPN działa na bramie zdalnej

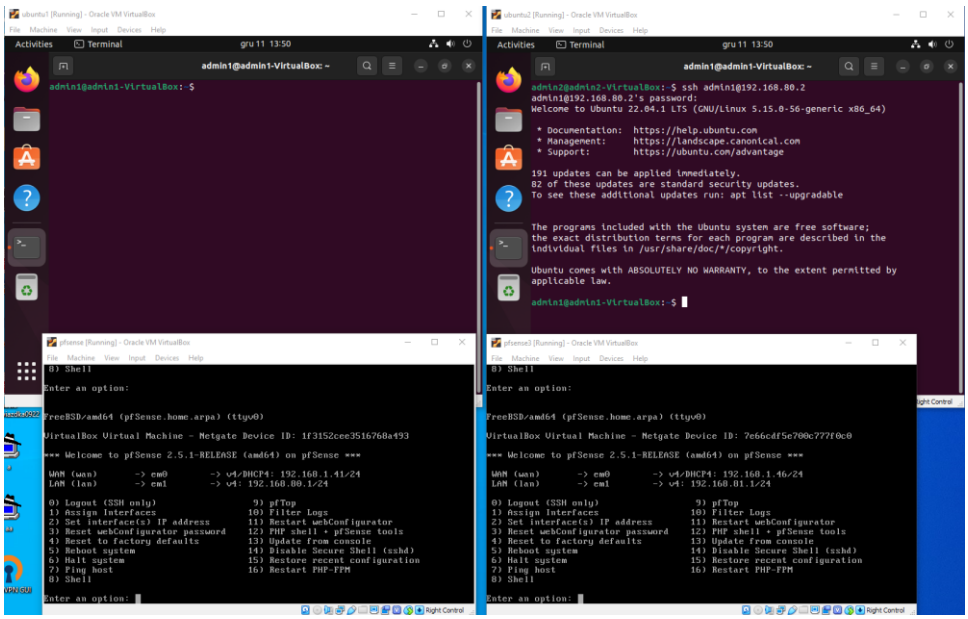


Klient jest w stanie pingować serwer



Udane połączenie ssh, należy pamiętać o edycji /etc/ssh/sshd_config, jeżeli występuje błąd acces denied (publickey) i zrestartować usługę ssh


ubuntu2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
gru 11 13:49
admin1@admin1-VirtualBox: ~
admin2@admin2-VirtualBox:~$ ssh admin1@192.168.80.2
admin1@192.168.80.2's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
191 updates can be applied immediately.
82 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
admin1@admin1-VirtualBox:~$
Right Control


admin1@admin1-VirtualBox: ~
admin2@admin2-VirtualBox:~$ ssh admin1@192.168.80.2
admin1@192.168.80.2's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)
191 updates can be applied immediately.
82 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Enter an option:
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 1f3152cee3516768a493
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.41/24
LAN (lan) -> em1 -> v4: 192.168.80.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 7e66c6f5e700c777f0c0
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.46/24
LAN (lan) -> em1 -> v4: 192.168.80.1/24
Enter an option: