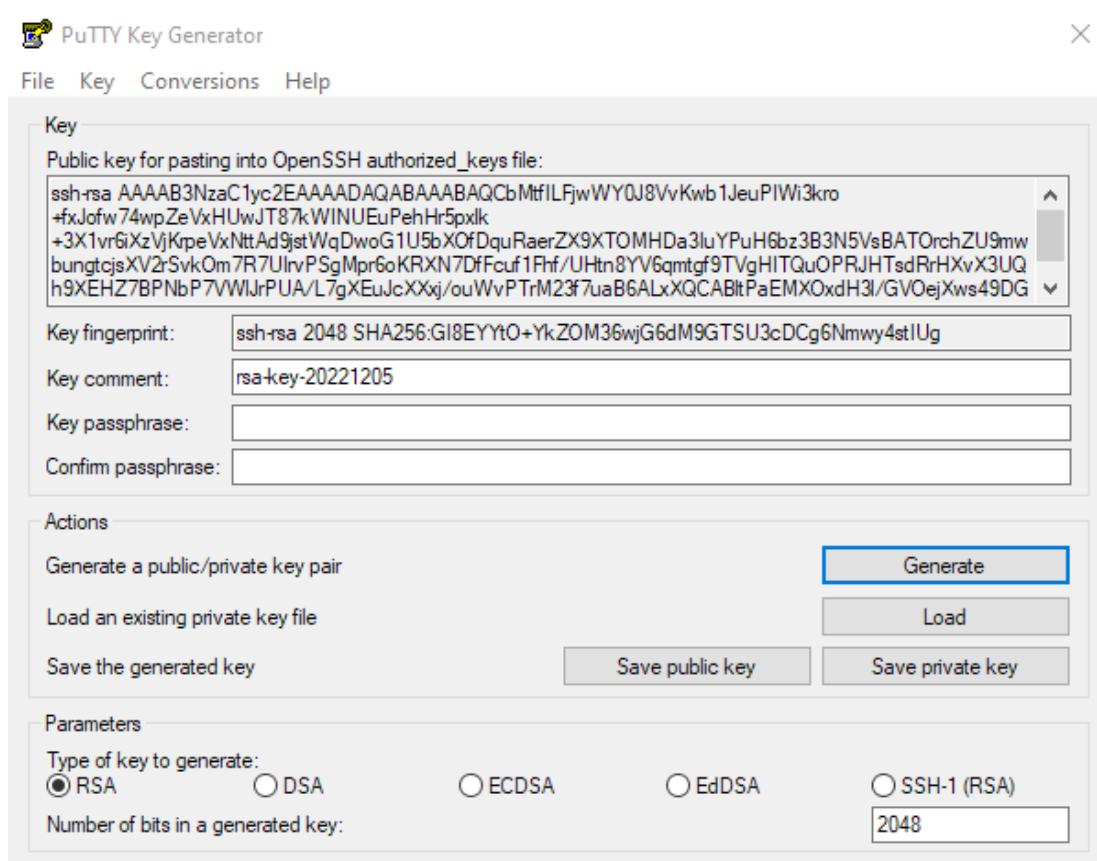


Wygenerowanie klucza ssh za pomocą putty



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

```
root@ubuntu: ~
```

```
GNU nano 4.8          /etc/ssh/sshd_config      Modified
```

```
# Authentication:  
  
#LoginGraceTime 2m  
#PermitRootLogin prohibit-password  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
  
#PubkeyAuthentication yes  
  
# Expect .ssh/authorized_keys2 to be disregarded by default in future.  
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2  
  
#AuthorizedPrincipalsFile none  
  
#AuthorizedKeysCommand none  
#AuthorizedKeysCommandUser nobody  
  
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
```

At the bottom of the terminal window, a menu bar displays keyboard shortcuts:

- ^G Get Help
- ^O Write Out
- ^W Where Is
- ^K Cut Text
- ^J Justify
- ^C Cur Pos
- ^X Exit
- ^R Read File
- ^A Replace
- ^U Paste Text
- ^T To Spell
- ^L Go To Line

Edycja pliku .ssh/authorized_keys – wklejenie wcześniej skopiowanego klucza



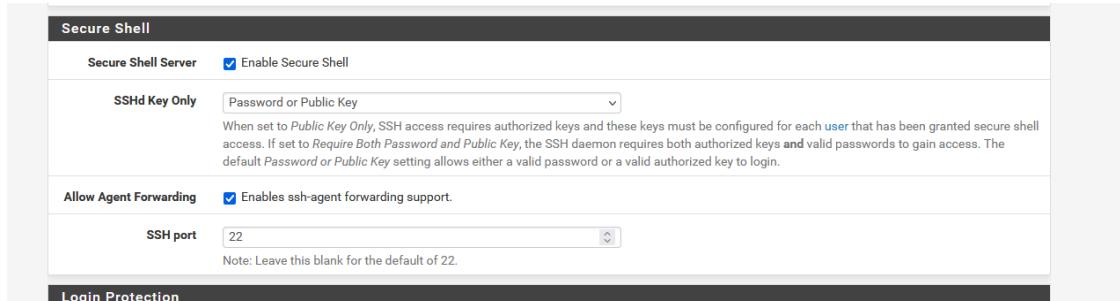
root@ubuntu: ~

```
GNU nano 4.8          .ssh/authorized_keys
SSH-rsa AAAAB3NzaC1yc2EAAAQABAAQCbMtfILFjwWY0J8VvKwb1JeuPIWi3kro+fxJofw74>
```

[Read 1 line]

^G Get Help **^O** Write Out **^W** Where Is **^K** Cut Text **^J** Justify **^C** Cur Pos
^X Exit **^R** Read File **^|** Replace **^U** Paste Text **^T** To Spell **^** Go To Line

Zaznaczenie odpowiednich ustawień w pfsensie



Secure Shell

Secure Shell Server Enable Secure Shell

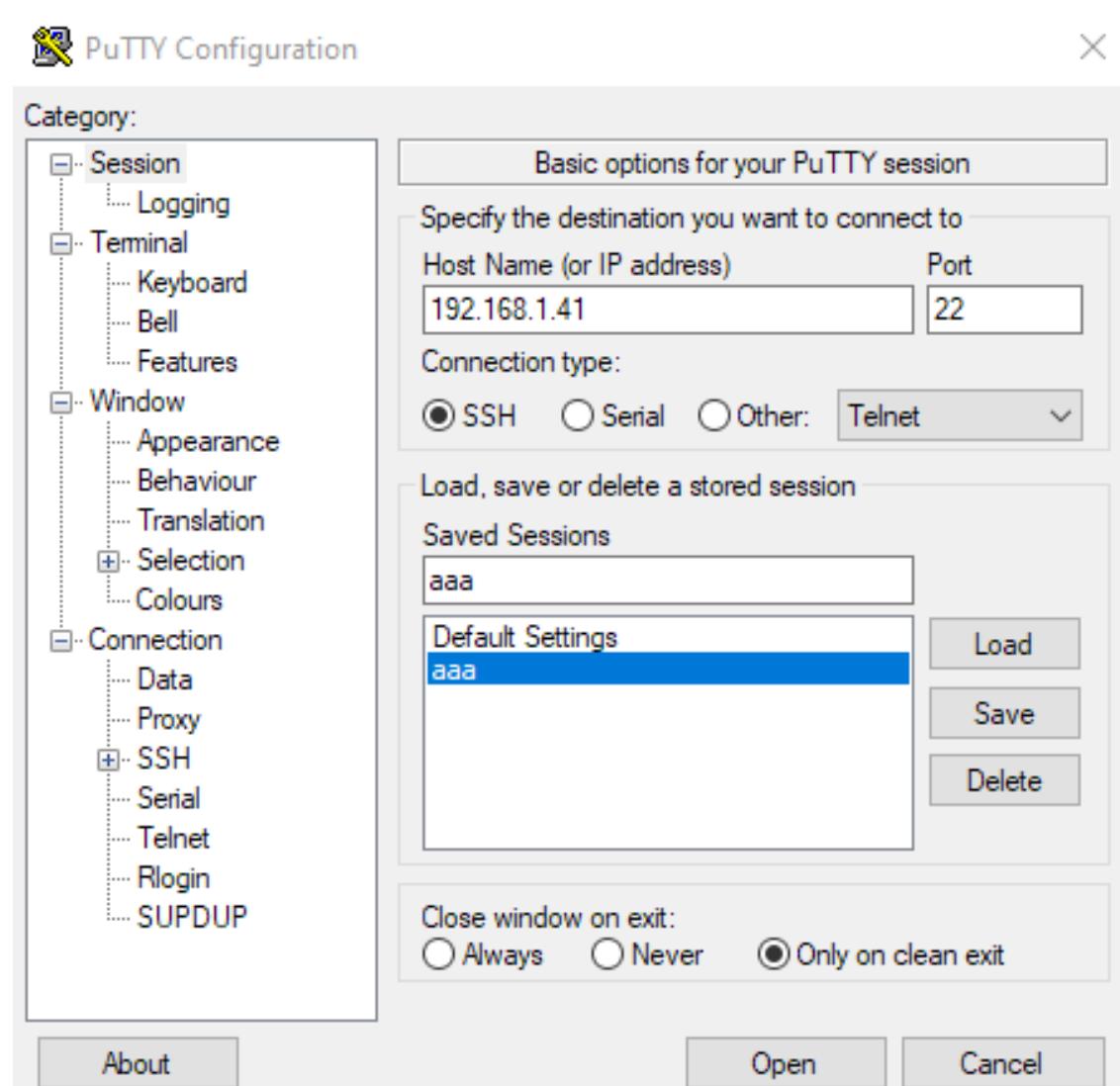
SSHD Key Only When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

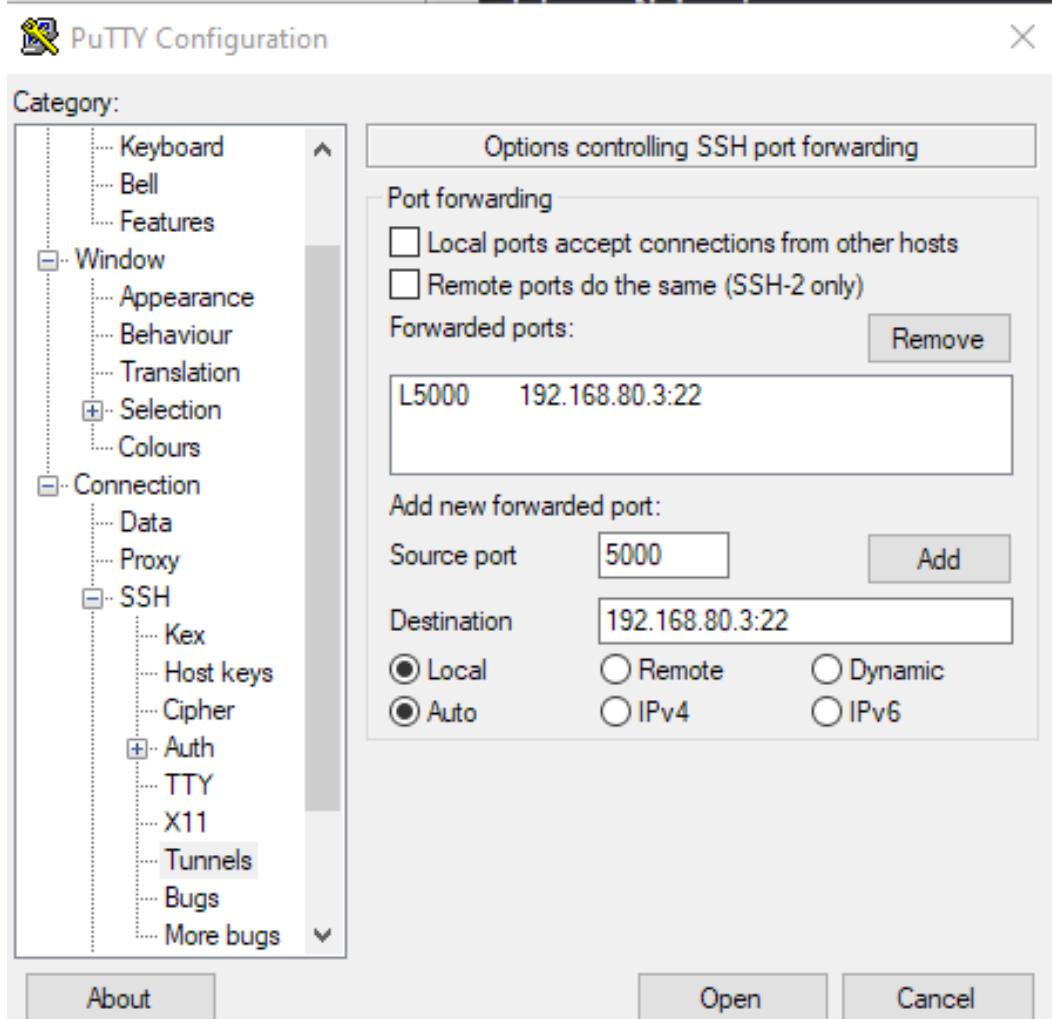
Allow Agent Forwarding Enables ssh-agent forwarding support.

SSH port Note: Leave this blank for the default of 22.

Login Protection

Przekierowanie ip na localhost:5000





```
192.168.1.41 - PuTTY
[ 1] login as: root
[ 2] Keyboard-interactive authentication prompts from server:
| Password for root@pfSense.home.arp:
[ 3] End of keyboard-interactive prompts from server
VirtualBox Virtual Machine - Netgate Device ID: lf3152cee3516768a493

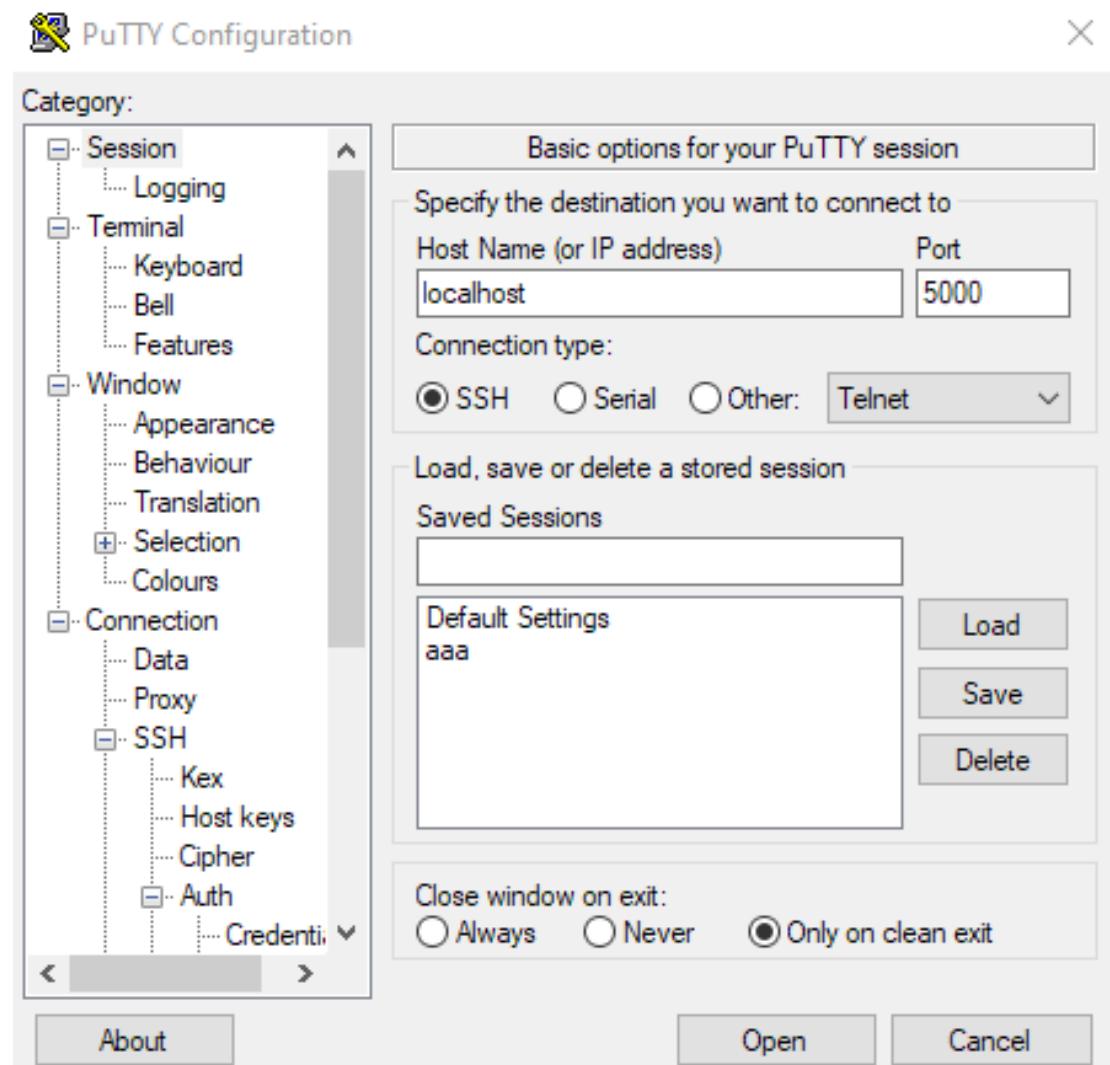
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.41/24
LAN (lan)      -> em1      -> v4: 192.168.80.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

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
 - Credentials
 - GSSAPI
 - TTY
 - X11

Credentials to authenticate with

Public-key authentication

Private key file for authentication:

Certificate to use with the private key:

Plugin to provide authentication responses

Plugin command to run

Udane zalogowanie na roota

```
root@ubuntu: ~
[1] login as: root
[2] Authenticating with public key "rsa-key-20221205"
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information as of pon, 5 gru 2022, 12:53:19 UTC

 System load: 0.04           Processes:          207
 Usage of /:   52.1% of 17.52GB  Users logged in:    1
 Memory usage: 32%           IPv4 address for enp0s3: 192.168.80.3
 Swap usage:  0%

 * 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

37 updates can be applied immediately.
26 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

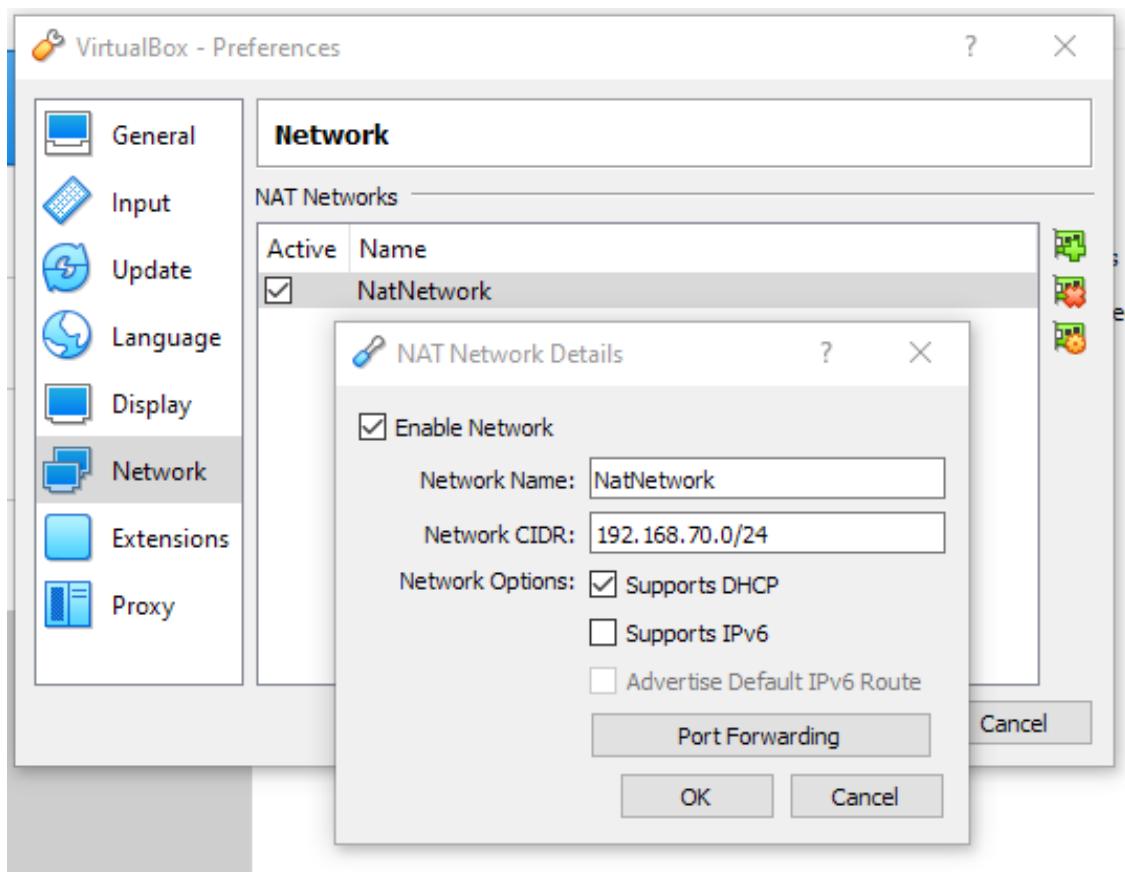
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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.

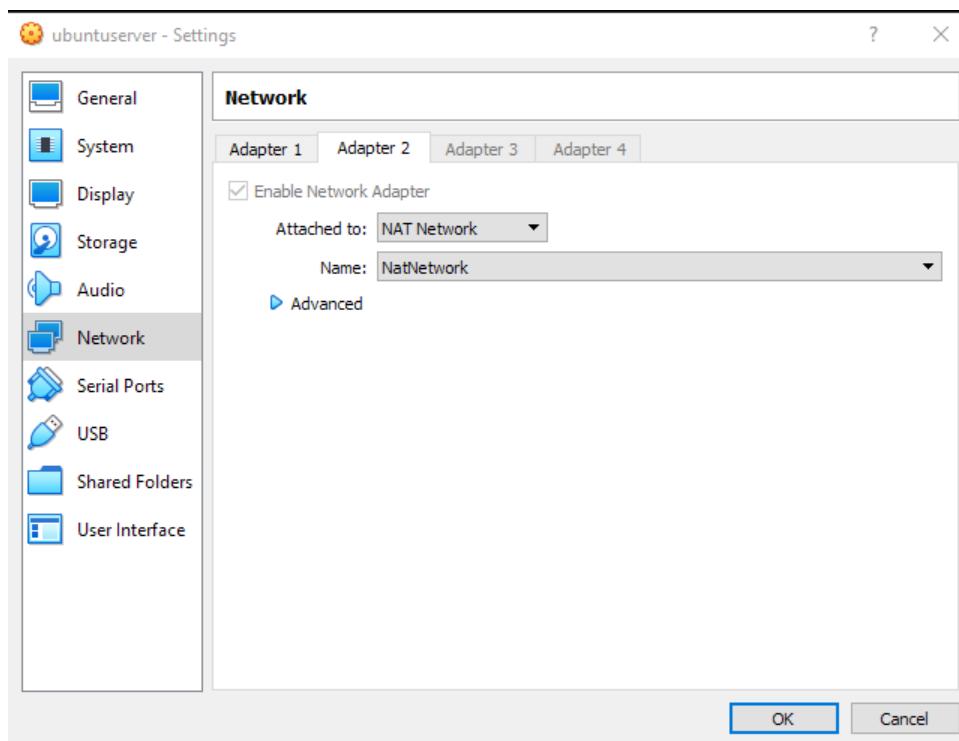
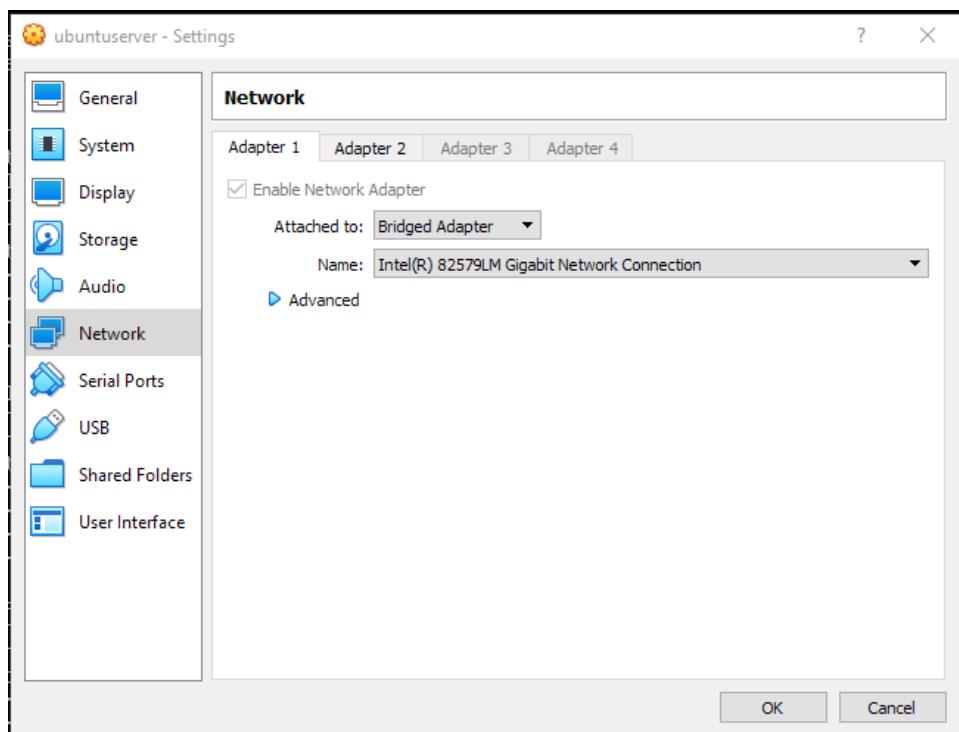
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@ubuntu:~#
```

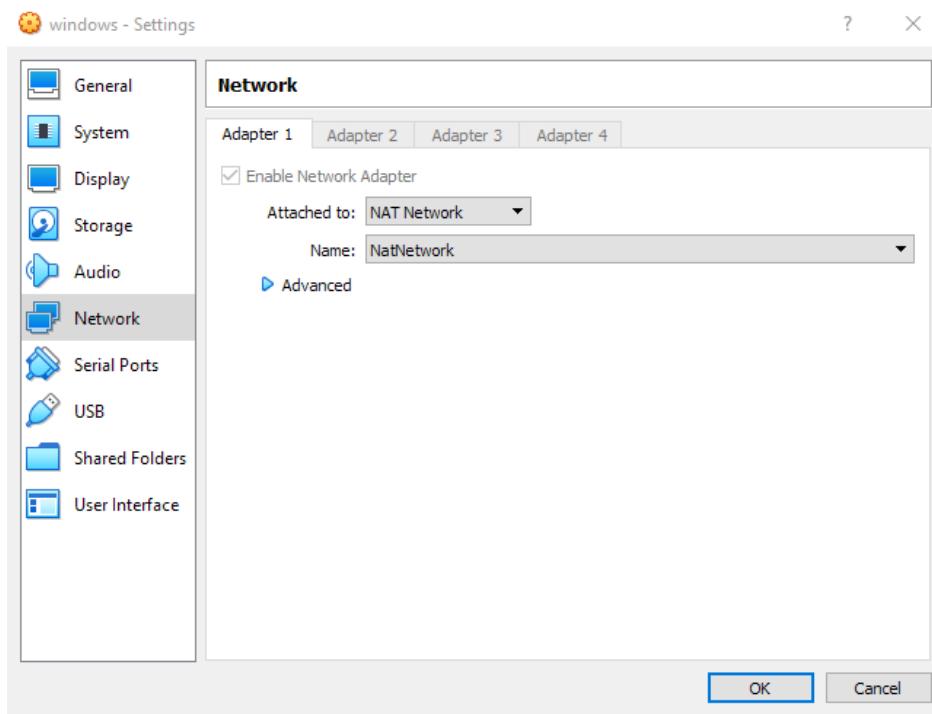
Utworzenie sieci Nat w virtual boxie i przypisanie do niej klienta Windowsa i nowy serwer ubuntu



Karty sieciowe serwera



Karta sieciowa klienta



Adresy serwera

```
ubuntu@ubuntuserver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Swap usage: 0%           IPv4 address for enp0s8: 10.0.3.15

50 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

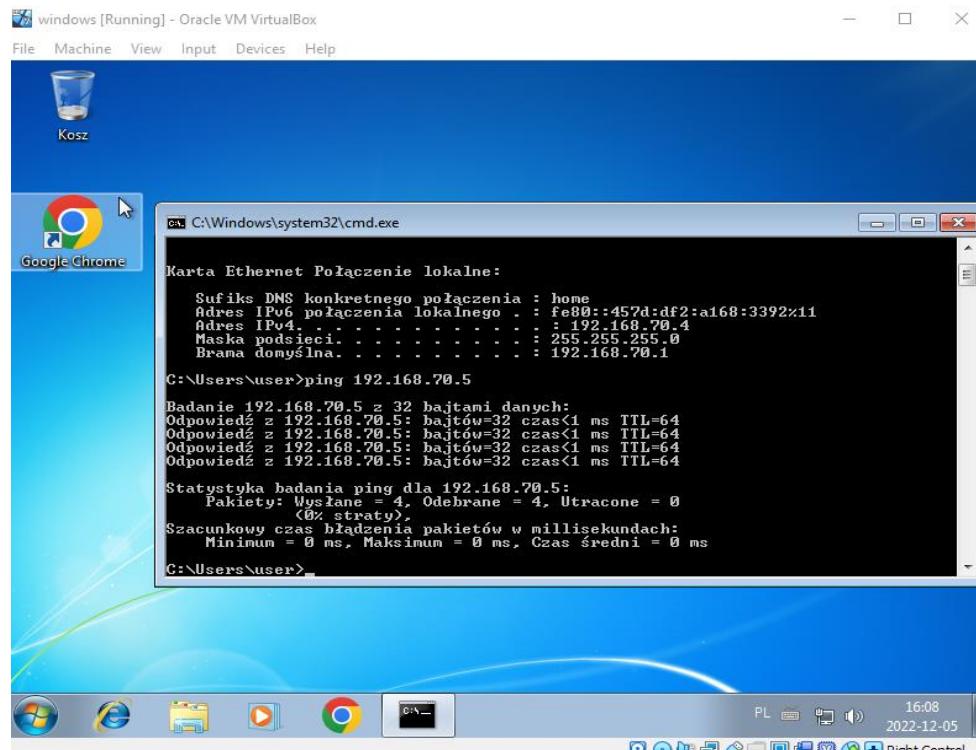
Last login: Mon Dec  5 14:53:59 UTC 2022 on tty1
user@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.44  netmask 255.255.255.0  broadcast 192.168.1.255
          inet6 fe80::a00:27ff:fe32:c0c2  prefixlen 64  scopeid 0x20<link>
            ether 08:00:27:32:c0:c2  txqueuelen 1000  (Ethernet)
              RX packets 12  bytes 1472 (1.4 KB)
              RX errors 0  dropped 3  overruns 0  frame 0
              TX packets 12  bytes 1504 (1.5 KB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.70.5  netmask 255.255.255.0  broadcast 192.168.70.255
          inet6 fe80::a00:27ff:fe13:626e  prefixlen 64  scopeid 0x20<link>
            ether 08:00:27:13:62:6e  txqueuelen 1000  (Ethernet)
              RX packets 53  bytes 8268 (8.2 KB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 10  bytes 1392 (1.3 KB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
          inet6 ::1  prefixlen 128  scopeid 0x10<host>
            loop  txqueuelen 1000  (Local Loopback)
              RX packets 80  bytes 5920 (5.9 KB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 80  bytes 5920 (5.9 KB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

user@ubuntu:~$
```

Adres klienta i sprawdzenie, czy widzi on serwer poprzez pingowanie



Sprawdzenie czy gospodarz widzi serwer

```
C:\Users\admin>ping 192.168.1.44

Pinging 192.168.1.44 with 32 bytes of data:
Reply from 192.168.1.44: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.44:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin>
```

Sprawdzenie statusu ssh

```
user@ubuntu:~$ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-12-05 15:05:58 UTC; 3min 57s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 652 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 691 (sshd)
   Tasks: 1 (limit: 1030)
  Memory: 4.4M
    CPU: 56ms
   CGroup: /system.slice/ssh.service
           └─691 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 05 15:05:57 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Dec 05 15:05:58 ubuntu sshd[691]: Server listening on 0.0.0.0 port 22.
Dec 05 15:05:58 ubuntu sshd[691]: Server listening on :: port 22.
Dec 05 15:05:58 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
user@ubuntu:~$ _
```

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

```
ubuntu@ubuntuserver:~$ nano /etc/ssh/sshd_config
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes

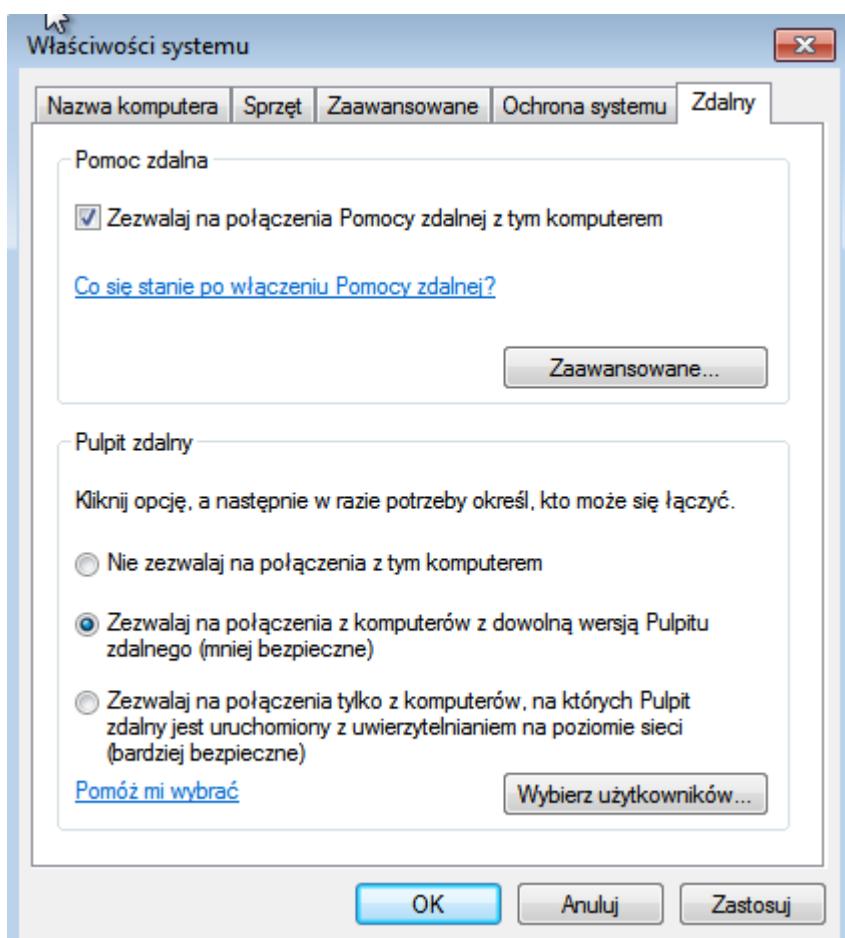
#AllowAgentForwarding yes
#AllowTcpForwarding yes
GatewayPorts yes_
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no

^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^- Go To Line M-E Redo
                                         Right Control ...
```

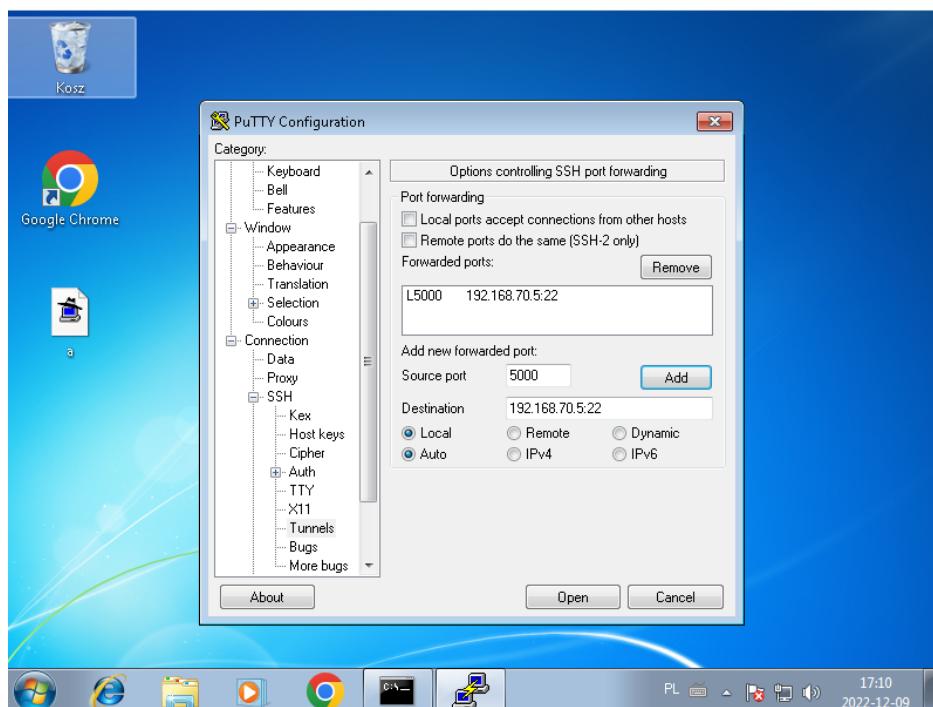
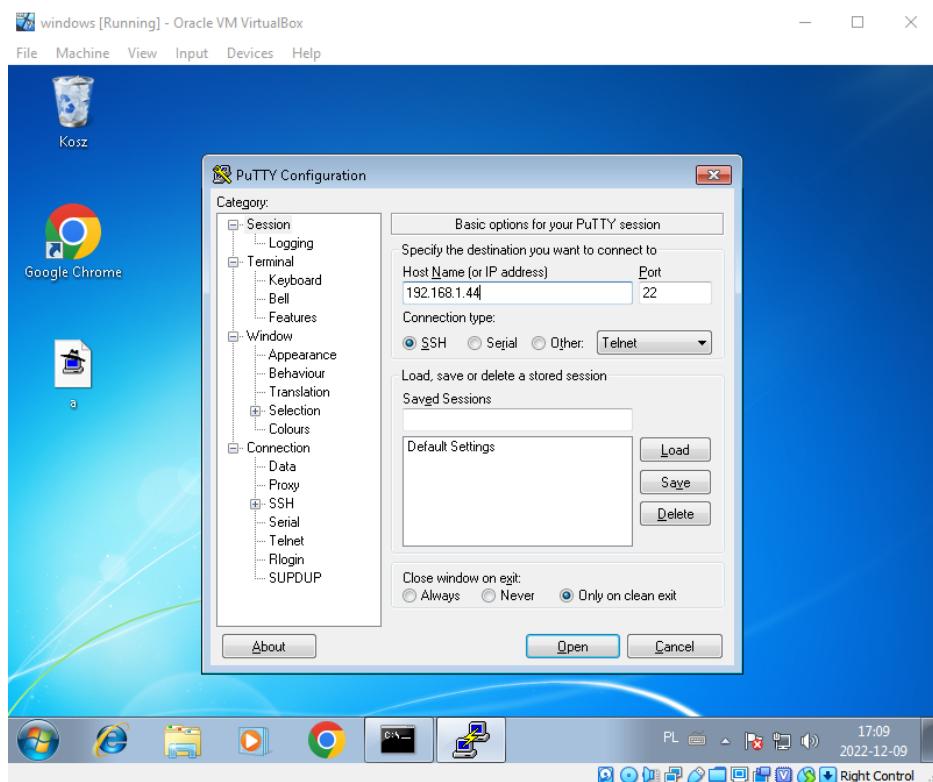
Sprawdzenie statusu firewalla, przez to, że jest inactive to nie będzie sprawiał żadnych problemów z pulpitem zdalnym

```
user@ubuntu:~$ sudo ufw status
Status: inactive
user@ubuntu:~$ _
```

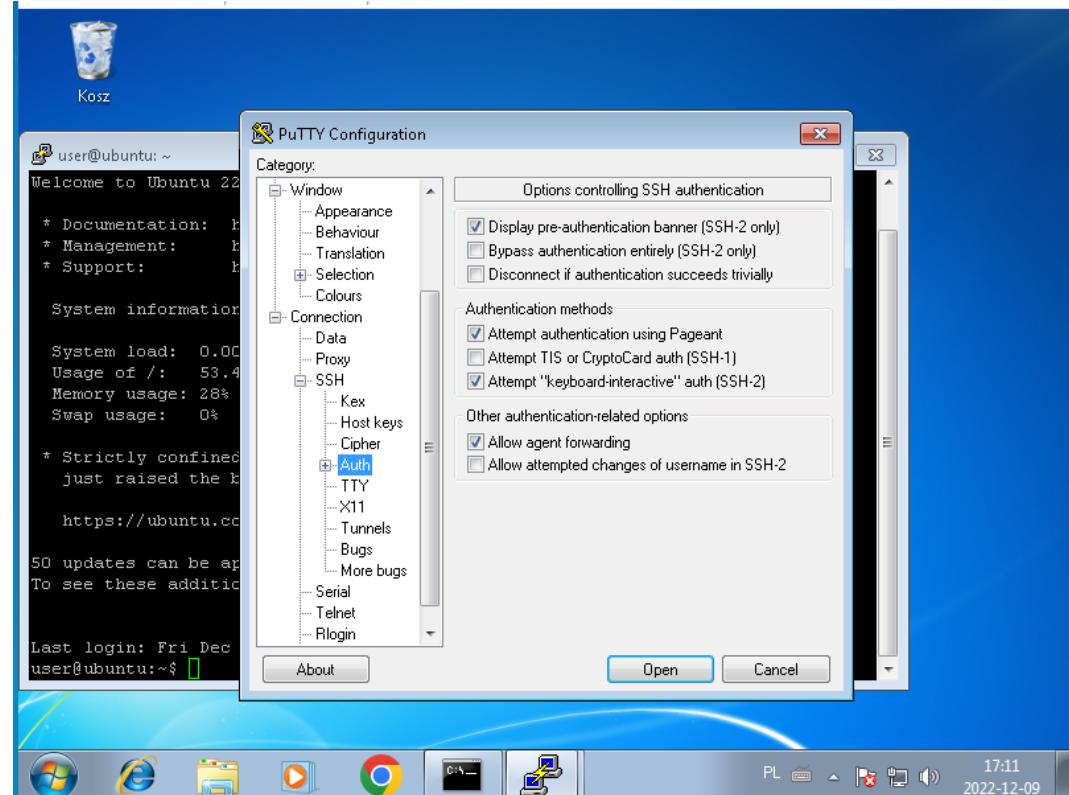
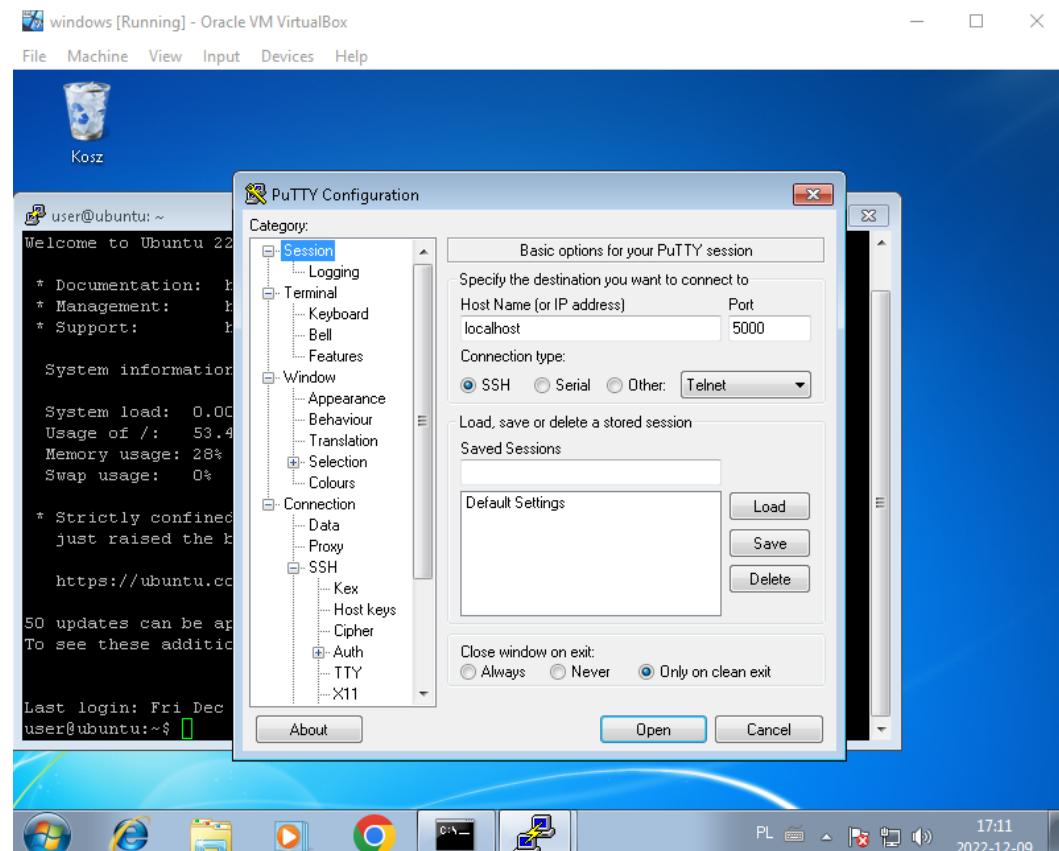
Zezwolenie na kliencie na łączenie się pulpitem zdalnym

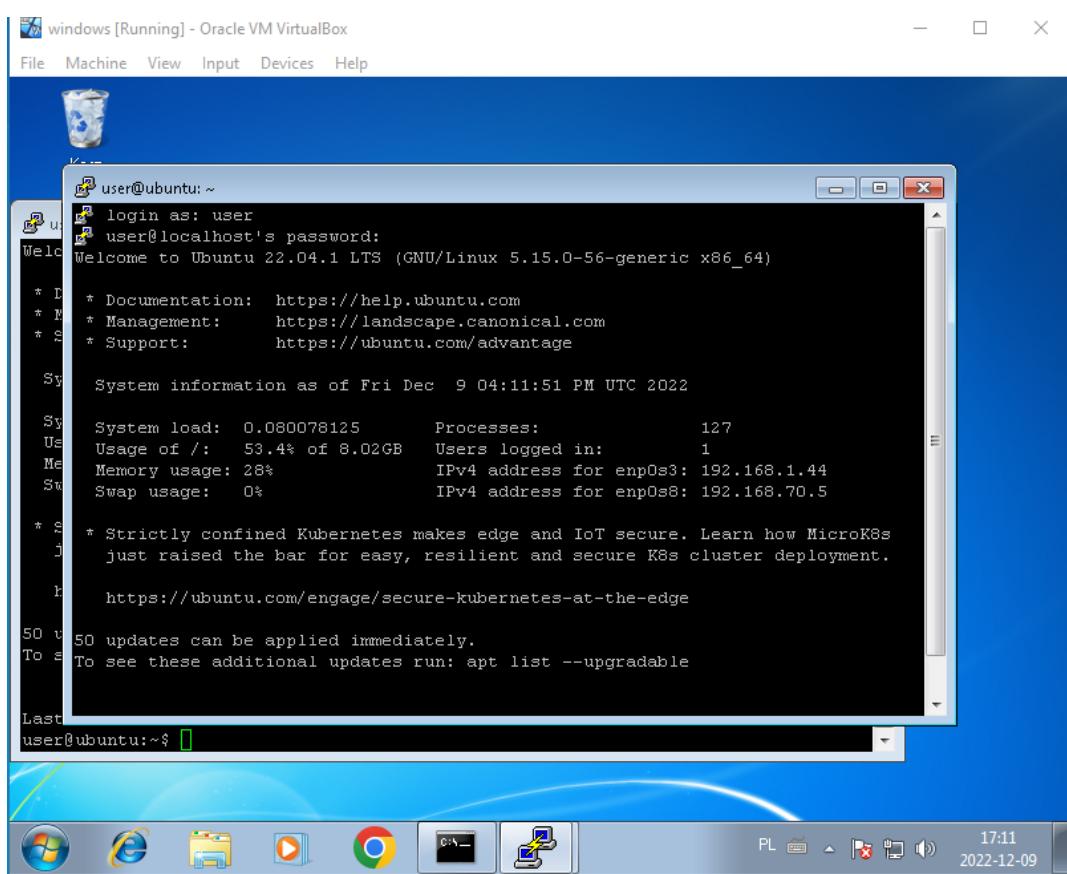
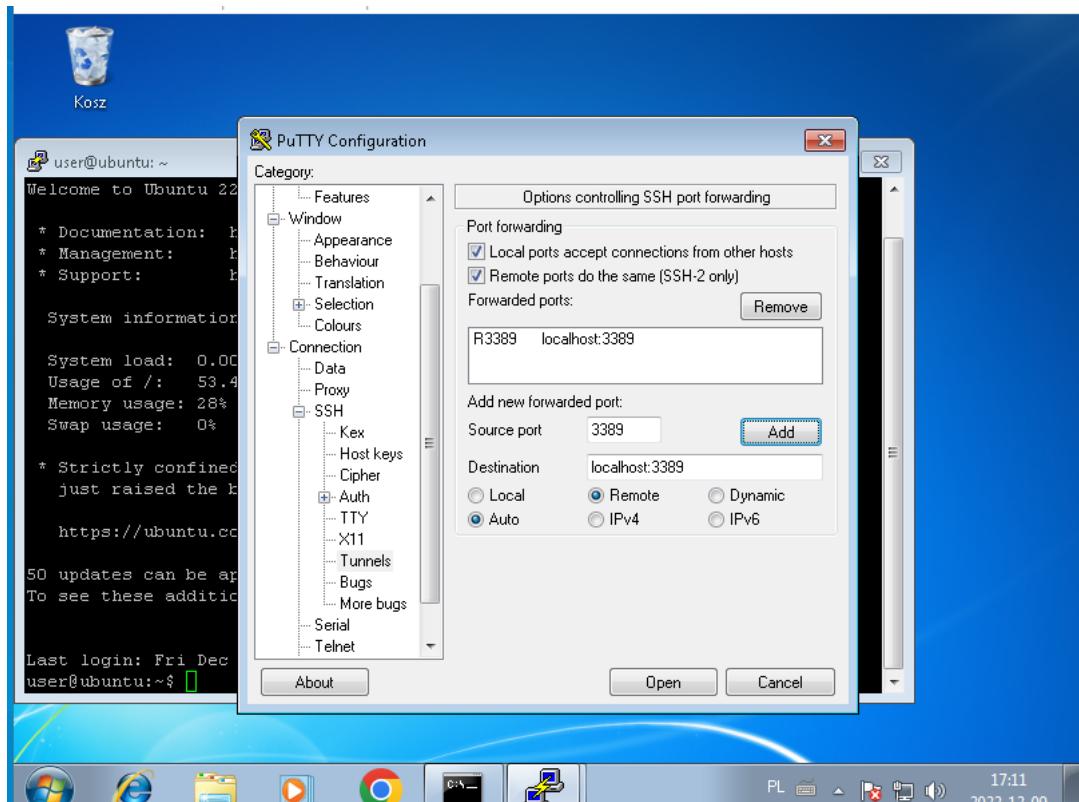


Otwarcie portu 5000

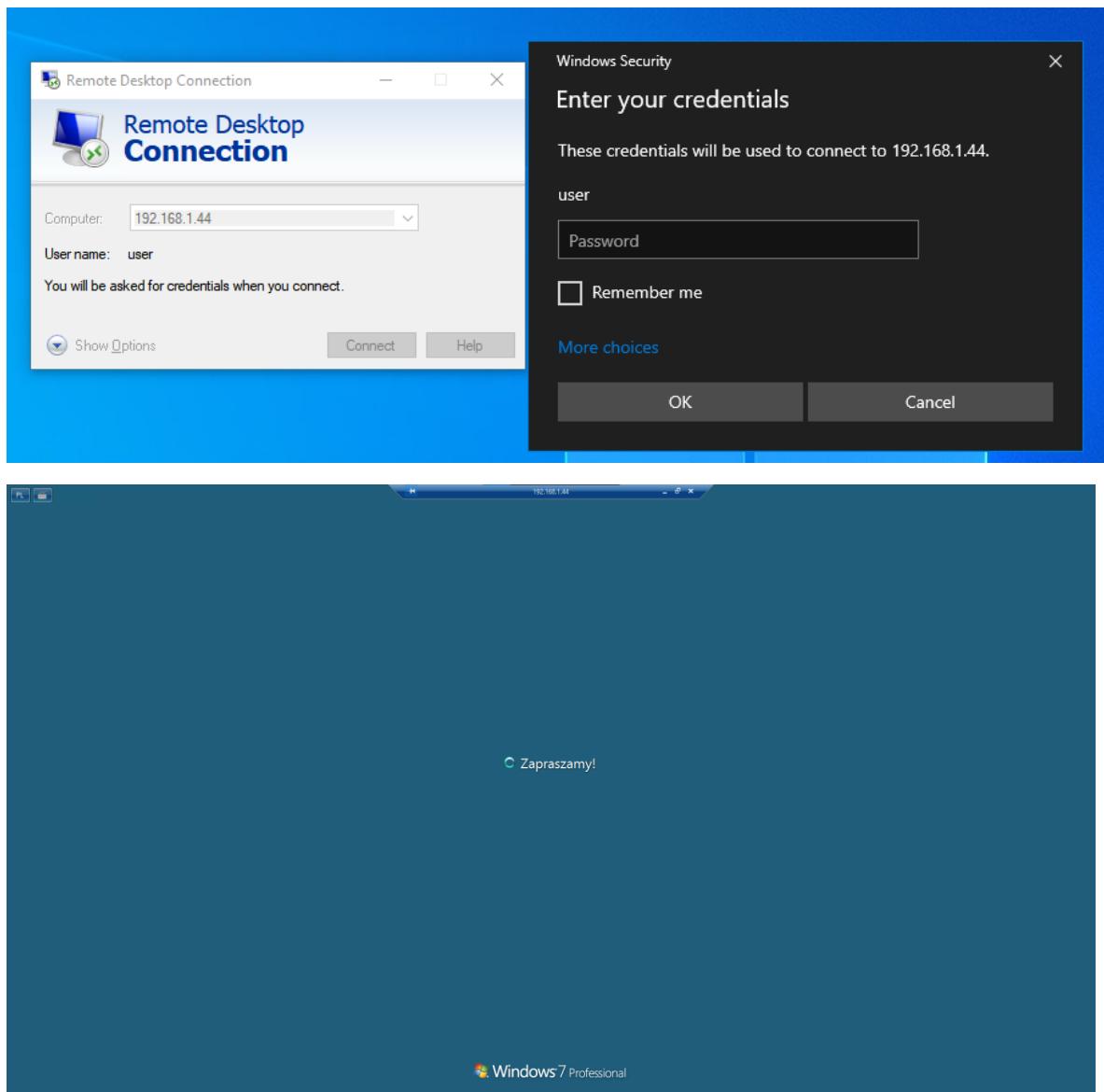


Wystawienie na porcie 5000 usługi zdalnego pulpitu, czyli 3389

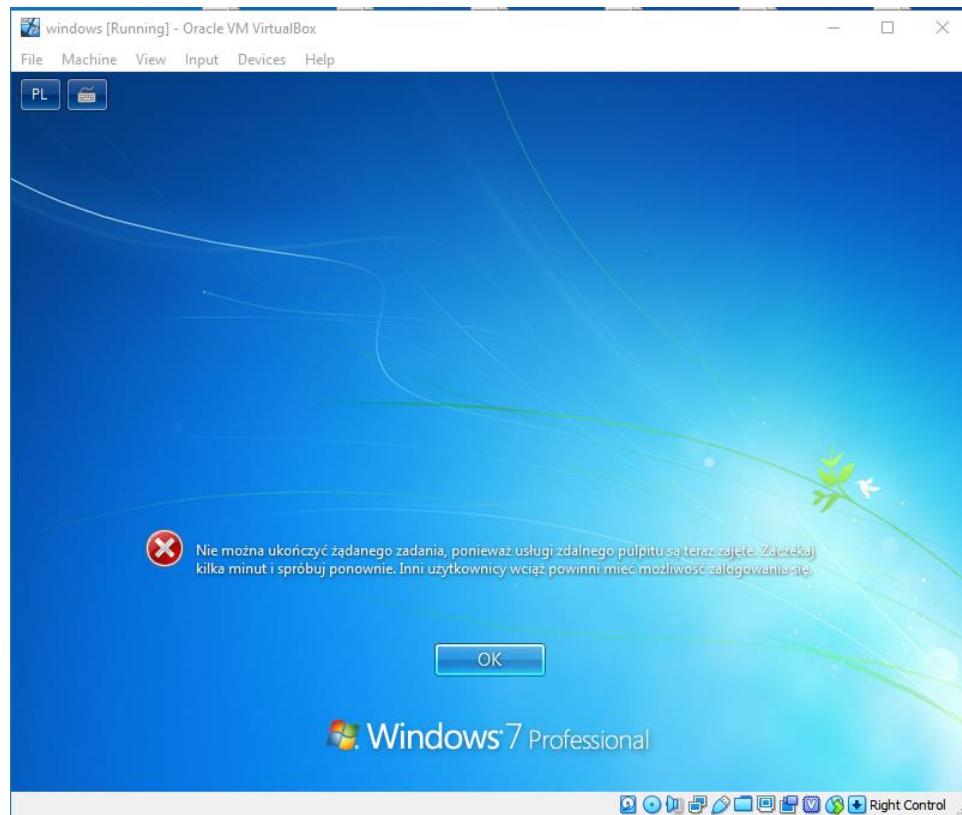
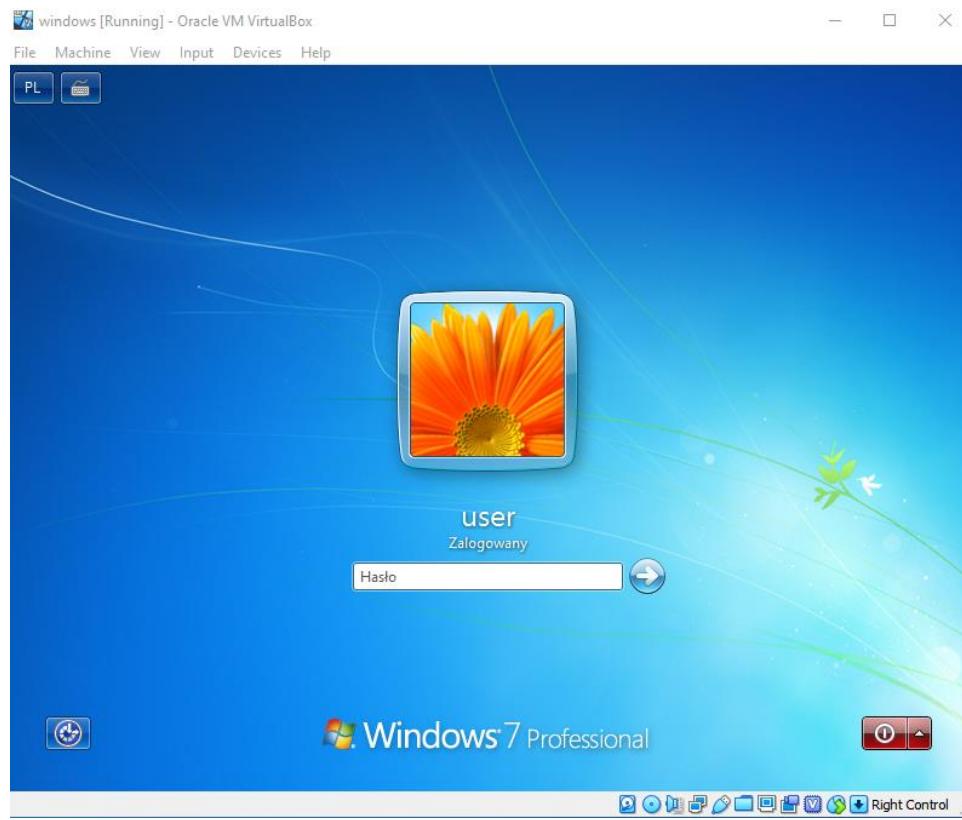




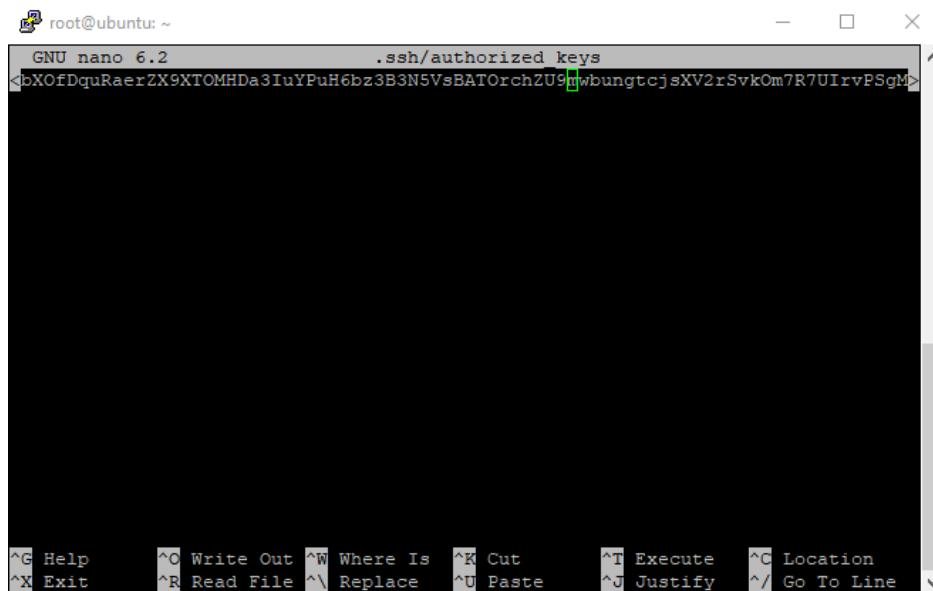
Próba połączenia się gospodarza przez pulpit zdalny



W czasie korzystania z pulpitu zdalnego nie możliwe jest używanie klienta



Wpisanie klucza ssh do pliku .ssh/authorized_keys

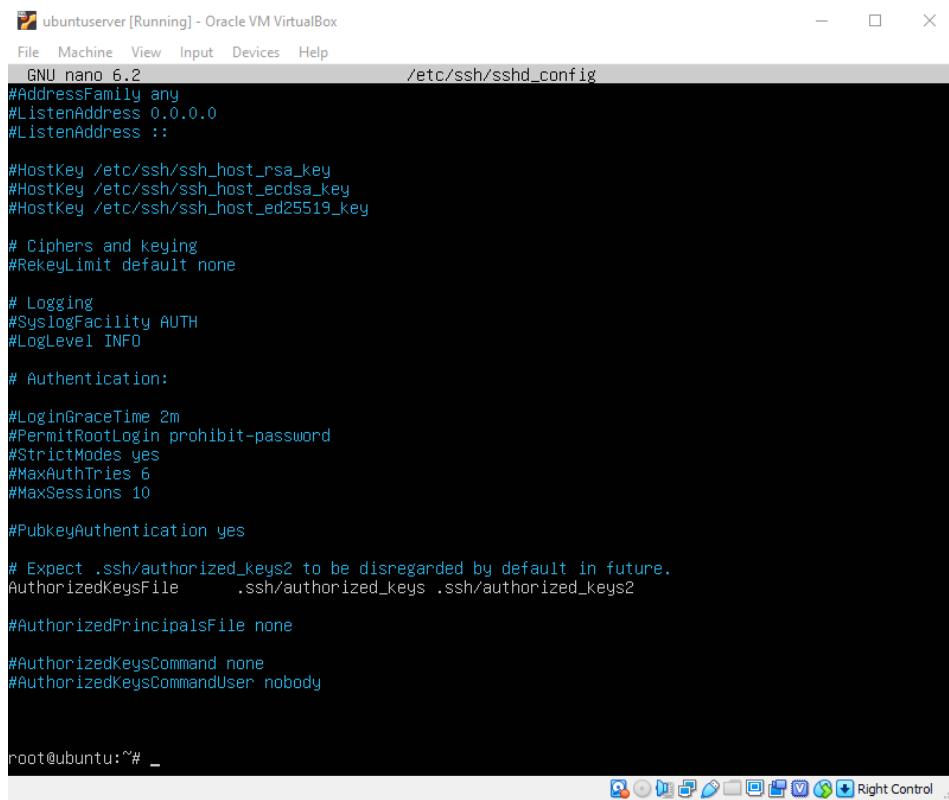


root@ubuntu: ~

```
GNU nano 6.2          .ssh/authorized_keys
<bxOfDquRaerZX9XTOMHDa3IuYPuH6bz3B3N5VsBATOrch2U9gbungtcjsXV2rSvkOm7R7UIrvPSgM>
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

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



ubuntuserver [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
GNU nano 6.2          /etc/ssh/sshd_config
#AddressFamily any
#ListenAddress 0.0.0.0
#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
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

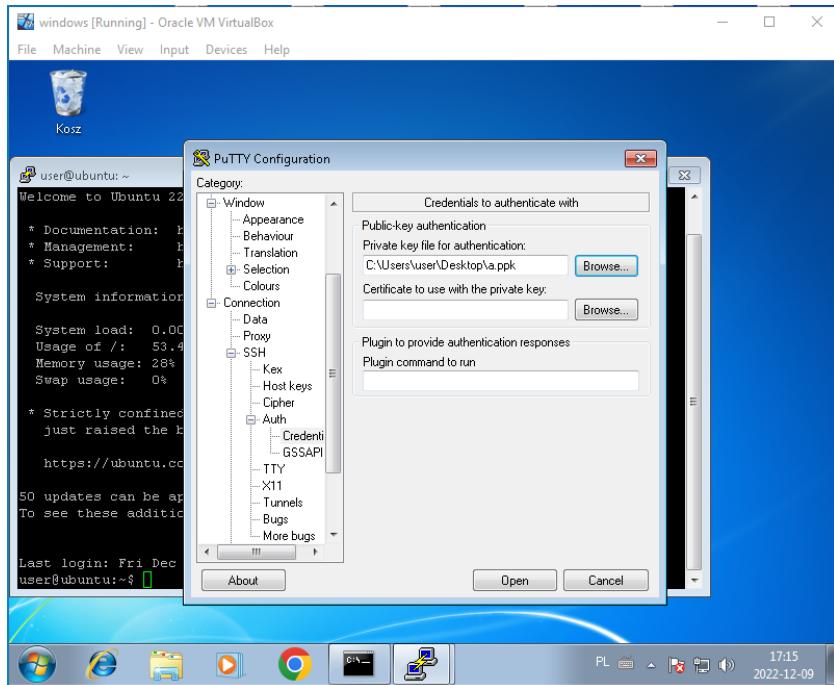
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

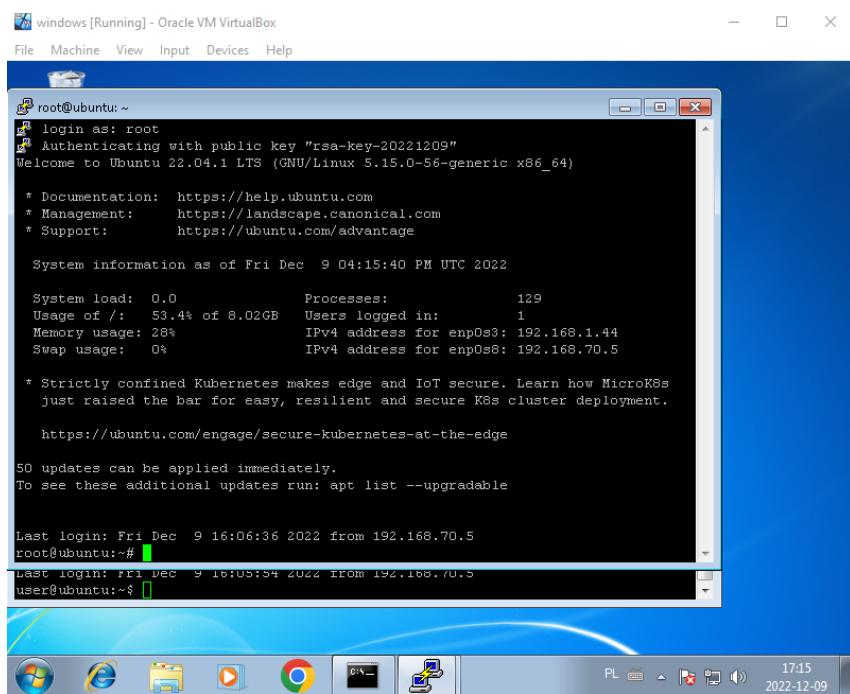
root@ubuntu:~# -
```

Right Control

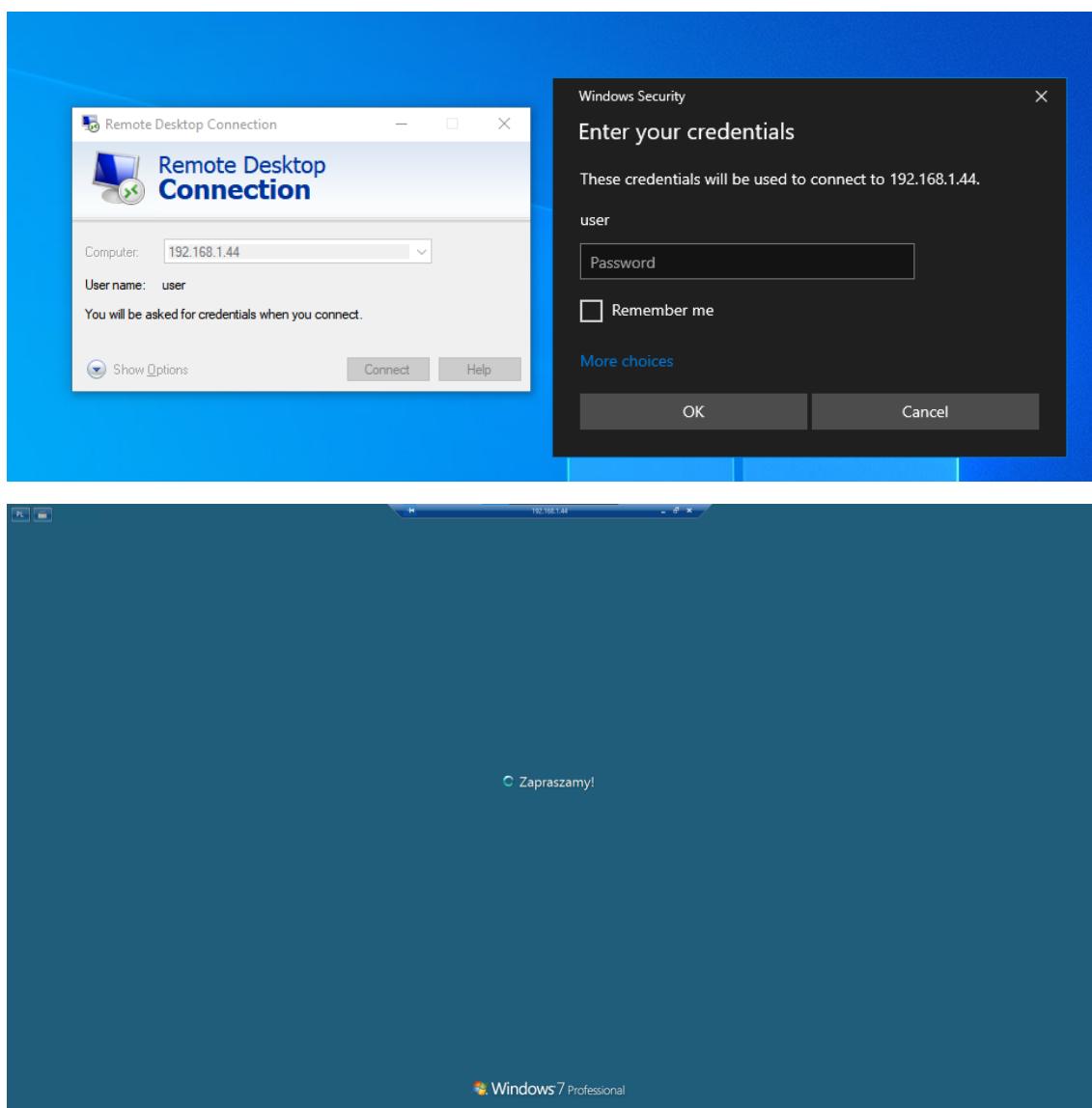
Zaznaczenie pliku z kluczem przy wystawianiu usługi pulpitu zdalnego na port 5000



Udane wystawienie bez potrzeby wpisywania hasła do roota



Sprawdzenie czy pulpit zdalny działa



Karty znajdujące się na serwerze

pfsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Starting CRON... done.
Starting package OpenVPN Client Export Utility...done.
pfSense 2.5.1-RELEASE amd64 Mon Apr 12 07:50:14 EDT 2021
Bootup complete
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) 9) pfTop
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Disable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell
Enter an option: []

Instalacja VPN

System / Package Manager / Package Installer
pfSense-pkg-openvpn-client-export installation successfully completed.
Installed Packages Available Packages Package Installer
Package Installation
--> NOTICE:
The p7zip port currently does not have a maintainer. As a result, it is
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:
<https://bugs.freebsd.org/bugzilla>
More information about port maintainership is available at:
<https://docs.freebsd.org/en/articles/contributing/#ports-contributing>
>>> Cleaning up cache... done.
Success

VPN / OpenVPN / Servers
Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export
OpenVPN Servers
Interface Protocol / Port Tunnel Network Mode / Crypto Description Actions
WAN UDP4 / 1194 192.168.1.0/24 Mode: Remote Access (SSL/TLS + User Auth)
(TUN) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC
Digest: SHA256 D-H Params: 2048 bits
+ Add

Ustawienia na zainstalowanym VPN

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

General Information

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Server mode Remote Access (User Auth)

Backend for authentication Local Database

Protocol UDP on IPv4 only

Device mode tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2).

Interface WAN
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port 1194
The port used by OpenVPN to receive client connections.

Description
A description may be entered here for administrative reference (not parsed).

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.

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.

TLS Key
2048 bit OpenVPN static key

-----BEGIN OpenVPN Static key V1-----
2bF1e34e170a0d2f4fc3c3d23f6b7263
51127d3e2e5a27c7d9939f7e7f6ee9d4
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 VPN1

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 VPN2 (Server: Yes, CA: VPN1, In Use)

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 Negotiation	<input type="checkbox"/> 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	<div style="display: flex; align-items: center;"> <div style="flex-grow: 1;"> <p>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)</p> </div> <div style="margin-left: 20px;"> <p>AES-256-CBC AES-128-GCM CHACHA20-POLY1305</p> </div> </div>
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	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> 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	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	<input checked="" type="checkbox"/> Allow communication between clients connected to this server
Duplicate Connection	<input type="checkbox"/> 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	

Client Settings

Dynamic IP Allow connected clients to retain their connections if their IP address changes.

Topology Subnet – One IP address per client in a common subnet

Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Ping settings

Inactive 0 Causes OpenVPN to exit after n seconds of inactivity on the TUN/TAP device. The time length of inactivity is measured since the last incoming or outgoing tunnel packet. 0 disables this feature.

Ping method keepalive – Use keepalive helper to define ping configuration

keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
 ping = interval
 ping-restart = timeout*2
 push ping = interval
 push ping-restart = timeout

Interval 10

Timeout 60

Advanced Client Settings

DNS Default Domain Provide a default domain name to clients

DNS Server enable Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

Block Outside DNS Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Force DNS cache update Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.

Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
 EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Username as Common Name Use the authenticated client username instead of the certificate common name (CN). When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

UDP Fast I/O Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

Exit Notify Disabled

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. In Peer-to-Peer Shared Key or with a /30 Tunnel Network, this value controls how many times this instance will attempt to send the exit notification.

Send/Receive Buffer Default

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KB and test higher and lower values.

Gateway creation Both IPv4 only IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level default

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
 Default through 4: Normal usage range
 5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
 6-11: Debug info range

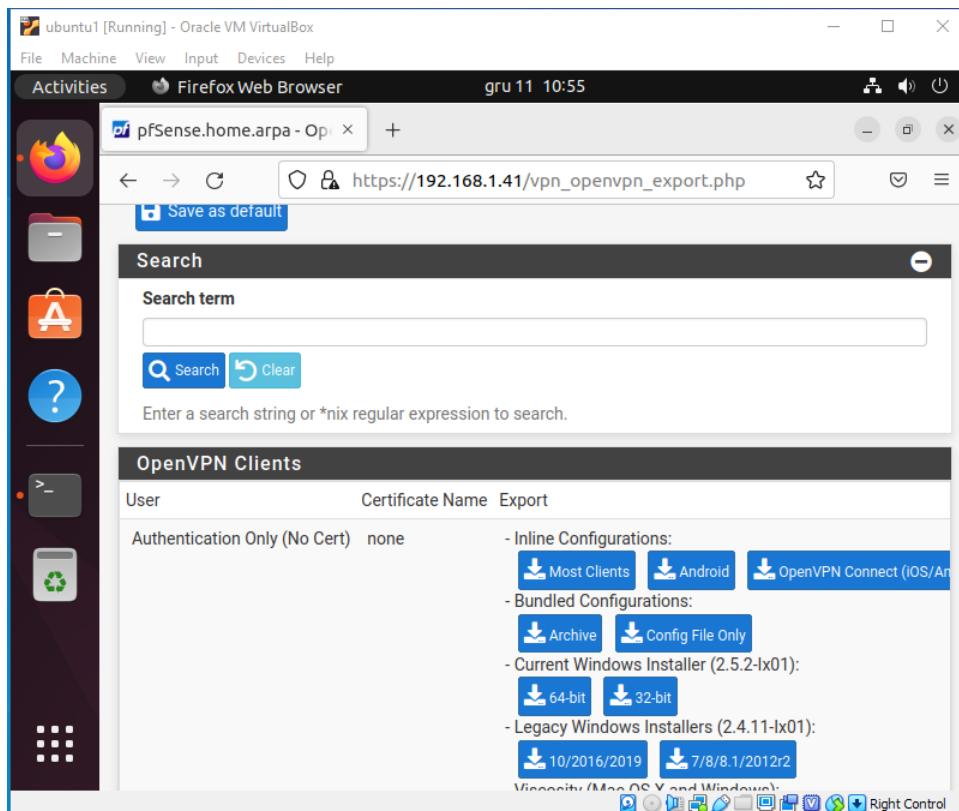
Ustawienia IP na kliencie i gospodarzu

```

admin1@admin1-VirtualBox: ~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.3 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopid 0x10<br/>
loop0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.4 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.2 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopid 0x10<br/>
loop1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.5 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>
admin2@admin2-VirtualBox: ~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.3 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopid 0x10<br/>
loop0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.4 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.2 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopid 0x10<br/>
loop1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.80.5 netmask 255.255.255.0 broadcast 0.0.0.0
                inet6 fe80::2a0f:87ff:fe0c:7769 prefixlen 64 scopid 0x20<br/>

```

Pobieranie pliku OpenVPN z serwera



Uruchamianie VPN na komputerze admin1

```
admin1@admin1-VirtualBox:~/Desktop$ sudo openvpn pfSense-UDP4-1194-  
config.ovpn  
[sudo] password for admin1:  
2022-12-11 10:56:48 DEPRECATED OPTION: ncp-disable. Disabling cipher negotiation is a deprecated debug feature that will be removed in OpenVPN 2.6  
2022-12-11 10:56:48 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers or change --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.  
2022-12-11 10:56:48 OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar 22 2022  
2022-12-11 10:56:48 library versions: OpenSSL 3.0.2 15 Mar 2022, LZ 0 2.10  
Enter Auth Username: admin  
Enter Auth Password: *****  
2022-12-11 10:56:54 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.41:1194  
2022-12-11 10:56:54 UDPv4 link local: (not bound)  
2022-12-11 10:56:54 UDPv4 link remote: [AF_INET]192.168.1.41:1194  
2022-12-11 10:56:54 [VPN2] Peer Connection Initiated with [AF_INET] 192.168.1.41:1194  
2022-12-11 10:56:55 TUN/TAP device tun0 opened  
2022-12-11 10:56:55 net_iface_mtu_set: mtu 1500 for tun0  
2022-12-11 10:56:55 net_iface_up: set tun0 up  
2022-12-11 10:56:55 net_addr_v4_add: 192.168.1.2/24 dev tun0
```

Łączenie się za pomocą ssh do admina2

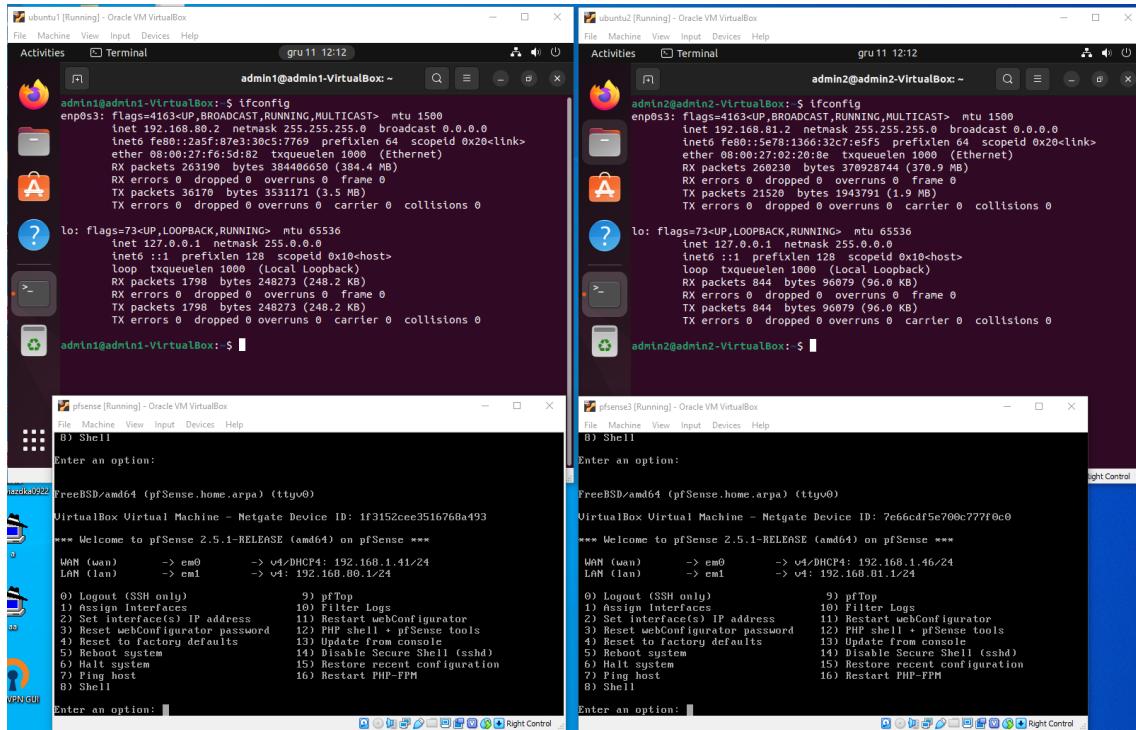
```
admin1@admin1-VirtualBox:~$ ssh admin2@192.168.80.2
admin2@192.168.80.2's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * 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

Last login: Sun Dec 11 11:21:52 2022 from 192.168.80.4
admin2@admin2-VirtualBox:~$
```

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

System / Certificate Manager / CAs

?

CAs Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
						 Add

Zaznaczenie, że certyfikatowi można ufać

System / Certificate Manager / CAs / Edit

CAs Certificates Certificate Revocation

Create / Edit CA

<u>Descriptive name</u>	VPN_CA	
<u>Method</u>	Create an internal Certificate Authority	
<u>Trust Store</u>	<input checked="" type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.	
<u>Randomize Serial</u>	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.	
Internal Certificate Authority		
<u>Key type</u>	RSA	
<u>Key Length</u>	2048	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
<u>Digest Algorithm</u>	sha256	The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
<u>Lifetime (days)</u>	3650	
<u>Common Name</u>	vpn-ca	

Internal Certificate Authority		
<u>Key type</u>	RSA	
<u>Key Length</u>	2048	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
<u>Digest Algorithm</u>	sha256	The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
<u>Lifetime (days)</u>	3650	
<u>Common Name</u>	vpn-ca	
The following certificate authority subject components are optional and may be left blank.		
<u>Country Code</u>	PL	
<u>State or Province</u>	e.g. Texas	
<u>City</u>	e.g. Austin	
<u>Organization</u>	IT_ORG	
<u>Organizational Unit</u>	IT_UNIT	
Save		

Utworzony certyfikat

System / Certificate Manager / CAs

CAs Certificates Certificate Revocation

Search

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN_CA	✓	self-signed	0	OU=IT_UNIT, O=IT_ORG, CN=vpn-ca, C=PL i Valid From: Sun, 11 Dec 2022 11:40:41 +0000 Valid Until: Wed, 08 Dec 2032 11:40:41 +0000		Edit Delete View Download

Add

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

The screenshot displays two vertically stacked configuration forms within a web-based management interface.

Top Form (Create / Edit CA):

- Descriptive name:** VPN_CA_INT
- Method:** Create an intermediate Certificate Authority
- Trust Store:** Add this Certificate Authority to the Operating System Trust Store
- Randomize Serial:** Use random serial numbers when signing certificates

Bottom Form (Internal Certificate Authority):

- Signing Certificate Authority:** VPN_CA
- Key type:** RSA
- Key Length:** 2048
- Digest Algorithm:** sha256
- Lifetime (days):** 3650

Common Name: vpn-ca-int

Subject Components (Optional):

- Country Code: PL
- State or Province: e.g. Texas
- City: e.g. Austin
- Organization: IT_ORG
- Organizational Unit: IT_UNIT

Save Button: A blue button labeled "Save" with a disk icon.

Pobranie obydwóch certyfikatów

A file manager interface showing the contents of the "Downloads" folder.

Name	Date modified	Type	Size
VPN_CA_INT	12/11/2022 12:43 PM	Security Certificate	2 KB
VPN_CA	12/11/2022 12:43 PM	Security Certificate	2 KB

Importowanie certyfikatów na zdalną bramę VPN

The screenshot shows two screenshots of the pfSense Certificate Manager interface.

Top Screenshot: Shows the 'CAs' tab selected in the 'Certificate Manager' section. It includes a search bar and a table listing Certificate Authorities. A red box highlights a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager."

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions	
VPN_CA			1	-----BEGIN CERTIFICATE-----MIIDDCCAbyAuIBAgIIQ+uzdhLxrCAwDQYJKoZIhvNAQELBQAwQTEPMA0GAIUEAxMgdnbUJMNMQswCQDVQQGewJQTEPEMA0GAIUEChQGSVRFt1JHMRAuOgYDVQQLFAdJVF9Vtk1UMB4OTIyMTIxMjExNDA0MVoXDTMyNTIvODExNDA0-----			Edit

Bottom Screenshot: Shows the 'Create / Edit CA' form for a new CA named 'VPN_CA'. The 'Method' is set to 'Import an existing Certificate Authority'. The 'Trust Store' checkbox is checked. The 'Randomize Serial' checkbox is unchecked. The 'Existing Certificate Authority' section contains a large text area with a PEM certificate. The 'Certificate Private Key (optional)' section has a text area for pasting a private key. The 'Next Certificate Serial' field is empty.

https://192.168.1.46/system_cmanager.php?act=new

System / Certificate Manager / CAs / Edit

Create / Edit CA

Descriptive name	VPN_CA_INT
Method	Import an existing Certificate Authority
Trust Store	<input checked="" type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.
Existing Certificate Authority	
Certificate data	-----BEGIN CERTIFICATE----- MIIDTCAPmgAwIBAgIBATANBgkqhkiG9w0BAQsFADBBMQ8wDQYD VQQFeUzCg4t Y2ExCzIjBgNVBAYTAjBMMQ8wDQYDVQQKFAZJVF9PUkcxEDAO8gNV BAsUB0LUx1V0 SVQqHnCNh]1XHfExMTETHzEwhcNHzIxHfA4HTE0HzEwBFHBRh -----END CERTIFICATE-----
Certificate Private Key (optional)	<input type="text"/>
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).	
Next Certificate Serial	<input type="text"/> 1
Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.	
Save	

Utworzono kopie certyfikatów

https://192.168.1.46/system_cmanager.php

System / Certificate Manager / CAs

Search

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN_CA	X	self-signed	1	OU=IT_UNIT, O=IT_ORG, CN=vpn-ca, C=PL Valid From: Sun, 11 Dec 2022 11:40:41 +0000 Valid Until: Wed, 08 Dec 2032 11:40:41 +0000		
VPN_CA_INT	X	VPN_CA	0	OU=IT_UNIT, O=IT_ORG, CN=vpn-ca-int, C=PL Valid From: Sun, 11 Dec 2022 11:43:13 +0000 Valid Until: Wed, 08 Dec 2032 11:43:13 +0000		

+ Add

Utworzenie w centralnej bramie certyfikatu bramy centralne w zakładce Certificates

https://192.168.1.41/system_certmanager.php

pfSense COMMUNITY EDITION

System / Certificate Manager / Certificates

Search

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (637b500dbe3f9)	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-637b500dbe3f9 Valid From: Mon, 21 Nov 2022 10:16:45 +0000 Valid Until: Sun, 24 Dec 2023 10:16:45 +0000	webConfigurator	

+ Add/Sign

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

The screenshot shows the 'Certificates' tab selected in the 'System / Certificate Manager / Certificates / Edit' menu. The 'Internal Certificate' section is active. The 'Method' dropdown is set to 'Create an internal Certificate'. The 'Descriptive name' field contains 'Certyfikat VPN'. Under 'Internal Certificate', the 'Certificate authority' is set to 'VPN_CA_INT', 'Key type' is 'RSA', and 'Key length' is '2048'. The 'Digest Algorithm' is 'sha256'. The 'Lifetime (days)' is set to '365'. The 'Common Name' is '192.168.1.41'. The 'Country Code' is 'PL'. Below these fields, optional subject components like 'City', 'Organization', and 'Organizational Unit' are listed. The 'Certificate Attributes' section includes an 'Attribute Notes' note about adding attributes to certificates and requests. It shows a 'Certificate Type' of 'Server Certificate' and an 'Alternative Names' entry for 'FQDN or Hostname' with a 'Type' of 'Value'. A green 'Add' button is available for more entries, and a blue 'Save' button is at the bottom.

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

The screenshot shows the pfSense Certificate Manager interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main page title is "System / Certificate Manager / Certificates / Edit". Below it, there are tabs for "CAs", "Certificates" (which is selected), and "Certificate Revocation".

The current form is titled "Add/Sign a New Certificate" and specifies "Method: Create a Certificate Signing Request". The "Descriptive name" is set to "Certyfikat VPN remote".

The "External Signing Request" section contains the following fields:

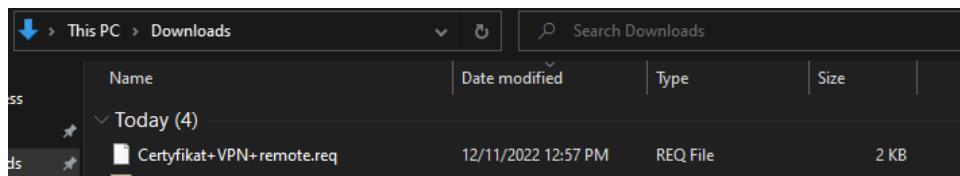
- Key type:** RSA
- Length:** 2048 (bits)
- Digest Algorithm:** sha256
- Common Name:** 192.168.1.46
- Country Code:** PL
- State or Province:** e.g. Texas
- City:** e.g. Austin

Below these fields, a note states: "The following certificate subject components are optional and may be left blank."

The "Certificate Attributes" section includes:

- Attribute Notes:** "The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode." "For Certificate Signing Requests, These attributes are added to the request but they may be ignored or changed by the CA that signs the request." "If this CSR will be signed using the Certificate Manager on this firewall, set the attributes when signing instead as they cannot be carried over."
- Certificate Type:** User Certificate
- Alternative Names:** FQDN or Hostname: Value (with a delete button)
- Add:** + Add
- Save:** (button)

Pobranie utworzonego certyfikatu



Zimportowanie pobranego certyfikatu do bramy centralnej

A screenshot of the pfSense web interface, specifically the 'System / Certificate Manager / Certificates / Edit' section. The page title is 'Add/Sign a New Certificate'. There are two tabs: 'CAs' and 'Certificates', with 'Certificates' being the active tab. Under 'Certificates', there is another tab 'Certificate Revocation'. The main form has a 'Method' dropdown set to 'Sign a Certificate Signing Request'. A 'Descriptive name' field contains 'Certyfikat VPN remote'. The 'Sign CSR' section includes a 'CA to sign with' dropdown set to 'VPN_CA_INT' and a 'CSR to sign' dropdown set to 'New CSR (Paste below)'. Below these dropdowns is a text area containing a long string of PEM-formatted CSR data, starting with '-----BEGIN CERTIFICATE REQUEST-----'. A note below the text area says 'Paste a Certificate Signing Request in X.509 PEM format here.' At the bottom of the form, there is a 'Key data' section with a large empty text area and a note ' Optionally paste a private key here. The key will be associated with the newly signed certificate in pfSense'. Finally, a 'Certificate Lifetime (days)' input field is set to '365' with a note explaining it represents the validity period in days.

/C2rL1dKXuu1psMLC14buJNu8HartbX31js=

-----END CERTIFICATE REQUEST-----

Paste a Certificate Signing Request in X.509 PEM format here.

Key data

Optional paste a private key here. The key will be associated with the newly signed certificate in pfSense

Certificate Lifetime (days) 365
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

When Signing a Certificate Request, existing attributes in the request cannot be copied. The attributes below will be applied to the resulting certificate.

Certificate Type User Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add  Save 

System / Certificate Manager / Certificates

Signed certificate Certyfikat VPN remote

CAs Certificates **Certificates** Certificate Revocation

Search

Search term Both  

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (637b500dbe3f9) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-637b500dbe3f9 	webConfigurator	   
Certyfikat VPN Server Certificate CA: No Server: Yes	VPN_CA_INT	OU=IT_UNIT, O=IT_ORG, CN=192.168.1.41, C=PL 		   
Certyfikat VPN remote User Certificate CA: No Server: No	VPN_CA_INT	OU=IT_UNIT, O=IT_ORG, CN=192.168.1.46, C=PL 		 



Pobranie utworzonego certyfikatu

This PC > Downloads

Search Downloads

Today (5)

Name	Date modified	Type	Size
Certyfikat+VPN+remote	12/11/2022 1:01 PM	Security Certificate	2 KB

Doklejenie pobranego pliku do certyfikatu CSR na bramie zdalnej

The screenshot shows the 'Certificates' tab selected in the pfSense Certificate Manager. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the 'Complete Signing Request for Certyfikat VPN remote' section is displayed. It contains two main sections: 'Signing request data' and 'Final certificate data'. The 'Signing request data' section shows a long string of base64-encoded data starting with '-----BEGIN CERTIFICATE REQUEST-----'. The 'Final certificate data' section shows a similar string ending with '-----END CERTIFICATE-----'. At the bottom of the page is a blue 'Update' button.

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

The screenshot shows the 'OpenVPN / Servers' configuration screen. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the 'General Information' section is visible, containing fields for 'Disabled' (unchecked), 'Server mode' (set to 'Peer to Peer (SSL/TLS)'), 'Protocol' (set to 'UDP on IPv4 only'), 'Device mode' (set to 'tun - Layer 3 Tunnel Mode'), 'Interface' (set to 'WAN'), 'Local port' (set to '1194'), and 'Description' (set to 'VPN gateway'). The 'Cryptographic Settings' section is also partially visible at the bottom.

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

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

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

ECDH Curve 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 <ul style="list-style-type: none"> 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) <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p>	<ul style="list-style-type: none"> AES-256-GCM AES-128-GCM CHACHA20-POLY1305 <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p>
--	---

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

Available Data Encryption Algorithms <ul style="list-style-type: none"> 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) <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p>	Allowed Data Encryption Algorithms <ul style="list-style-type: none"> AES-256-GCM AES-128-GCM CHACHA20-POLY1305 <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p>
--	---

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

Fallback Data Encryption Algorithm 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 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

Certificate Depth 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
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)
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)

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="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	<input type="text"/> 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	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	<input type="text" value="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)	<input type="text"/> 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.
IPv4 Remote network(s)	<input type="text" value="192.168.81.0/24"/> IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN's here. May be left blank for non site-to-site VPN.
IPv6 Remote network(s)	<input type="text"/> These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN's here. May be left blank for non site-to-site VPN.
Concurrent connections	<input type="text" value="10"/> Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	<input type="text" value="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.	

Po skonfigurowaniu OpenVPN należy skopiować klucz TLS

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

The screenshot shows two pages from the pfSense web interface related to OpenVPN clients.

Top Page (OpenVPN Clients):

- URL: https://192.168.1.46/vpn_openvpn_client.php
- Header: pfSense COMMUNITY EDITION
- Warning: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager."
- Breadcrumbs: VPN / OpenVPN / Clients
- Actions: Servers, Clients (selected), Client Specific Overrides, Wizards, Client Export, Shared Key Export
- Table Headers: Interface, Protocol, Server, Mode / Crypto, Description, Actions
- Buttons: + Add

Bottom Page (Edit Client Configuration):

- Breadcrumbs: VPN / OpenVPN / Clients / Edit
- Actions: Servers, Clients (selected), Client Specific Overrides, Wizards, Client Export, Shared Key Export
- General Information:**
 - Disabled: Disable this client
 - Description: Set this option to disable this client without removing it from the list.
- Server mode: Peer to Peer (SSL/TLS)
- Protocol: UDP on IPv4 only
- Device mode: tun - Layer 3 Tunnel Mode
 - Description: "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
 - "tap" mode is capable of carrying 802.3 (OSI Layer 2).
- Interface: WAN
 - Description: The interface used by the firewall to originate this OpenVPN client connection
- Local port:
- Server host or address: 192.168.1.41
 - Description: The IP address or hostname of the OpenVPN server.
- Server port: 1194
 - Description: The port used by the server to receive client connections.
- Proxy host or address:
 - Description: The address for an HTTP Proxy this client can use to connect to a remote server.
 - TCP must be used for the client and server protocol.
- Proxy port:

User Authentication Settings		
Username	<input type="text"/> Leave empty when no user name is needed	
Password	<input type="password"/> Leave empty when no password is needed	
Authentication Retry	<input type="checkbox"/> 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. i	
Cryptographic Settings		
TLS Configuration	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> Automatically generate a TLS Key.	
TLS Key	<pre>96f532ff5194c456c4982bdbddaa5d5 dc0d6d7299904b7b95014e492bb1b049 8a38dc32247e9e35fc820cc039f4d6ac 421a0ee0f5ae3570378e46d34ceb13e a277843db58ab8a2da0c68a819862b3 -----END OpenVPN Static key V1-----</pre> <p>Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.</p>	
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	<input type="text"/> VPN_CA_INT	
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation	
Client Certificate	<input type="text"/> Certyfikat VPN remote (CA: VPN_CA_INT)	
Peer Certificate Authority	<input type="text"/> VPN_CA_INT	
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation	
Client Certificate	<input type="text"/> Certyfikat VPN remote (CA: VPN_CA_INT)	
Data Encryption Negotiation	<input checked="" type="checkbox"/> 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	<pre>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)</pre> <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p>	<pre>AES-256-GCM AES-128-GCM CHACHA20-POLY1305</pre> <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p>
Fallback Data Encryption Algorithm	<input type="text"/> 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	<input type="text"/> 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	<input type="text"/> No Hardware Crypto Acceleration	

Tunnel Settings

IPv4 Tunnel Network	192.168.82.0/24	This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). The second usable address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.
IPv6 Tunnel Network		This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.
IPv4 Remote network(s)	192.168.81.0/24	IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN's here. May be left blank for non site-to-site VPN.
IPv6 Remote network(s)		These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN's here. May be left blank for non site-to-site VPN.
Limit outgoing bandwidth	Between 100 and 100,000,000 bytes/sec	Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second). Not compatible with UDP Fast I/O.
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.		
Topology	Subnet – One IP address per client in a common subnet	Specifies the method used to configure a virtual adapter IP address.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.	
Don't pull routes	<input type="checkbox"/> Bars the server from adding routes to the client's routing table	This option still allows the server to set the TCP/IP properties of the client's TUN/TAP interface.

Konfiguracja zasad firewalla na bramie zdalnej do OpenVPN

Firewall / Rules / OpenVPN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 /0 B	IPv4 *	*	*	*	*	*	none		OpenVPN wizard	
<input checked="" type="checkbox"/> 0 /0 B	IPv4 TCP/UDP	*	*	192.168.80.1	2222	*	none		NAT	

Add Add Save

Konfiguracja zasad firewalla na bramie centralnej do WAN i OpenVPN

Firewall / Rules / WAN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 /0 B	IPv4 UDP	*	*	192.168.80.2	22 (SSH)	*	none		NAT ssh	
<input checked="" type="checkbox"/> 1 /2.49 MiB	IPv4 TCP	*	*	*	*	*	none			
<input checked="" type="checkbox"/> 1 /14 KiB	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none		OpenVPN wizard	

Add Add Save

Firewall / Rules / OpenVPN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 /0 B	IPv4 *	*	*	*	*	*	none		OpenVPN wizard	
<input checked="" type="checkbox"/> 0 /0 B	IPv4 TCP/UDP	*	*	192.168.80.1	2222	*	none		NAT	

Add Add Save

Nadpisanie zasad dla konkretnego klienta

[VPN / OpenVPN / Client Specific Overrides](#)

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

CSC Overrides			
Disabled	Common Name	Description	Actions
			+ Add

[VPN / OpenVPN / Client Specific Overrides / Edit](#)

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

General Information	
Server List	OpenVPN Server 1: VPN gateway
Select the servers that will utilize this override. When no servers are selected, the override will apply to all servers.	
Disable	<input type="checkbox"/> Disable this override Set this option to disable this client-specific override without removing it from the list.
Common Name	192.168.1.46
Enter the X.509 common name for the client certificate, or the username for VPNs utilizing password authentication. This match is case sensitive.	
Description	VPN
A description for administrative reference (not parsed).	
Connection blocking	<input type="checkbox"/> Block this client connection based on its common name. Prevents the client from connecting to this server. Do not use this option to permanently disable a client due to a compromised key or password. Use a CRL (certificate revocation list) instead.

Tunnel Settings	
IPv4 Tunnel Network	192.168.82.0/24
The virtual IPv4 network used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.5/24). With subnet topology, enter the client IP address and the subnet mask must match the IPv4 Tunnel Network on the server. With net30 topology, the first network address of the /30 is assumed to be the server address and the second network address will be assigned to the client.	
IPv6 Tunnel Network	
The virtual IPv6 network used for private communications between this client and the server expressed using prefix (e.g. 2001:db9:1:1::10/64). Enter the client IPv6 address and prefix. The prefix must match the IPv6 Tunnel Network prefix on the server.	
IPv4 Local Network/s	192.168.80.0/24
These are the IPv4 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more CIDR networks. NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.	
IPv6 Local Network/s	
These are the IPv6 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more IP/PREFIX networks. NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.	
IPv4 Remote Network/s	192.168.81.0/24
These are the IPv4 client-side networks that will be routed to this client specifically using iroute, so that a site-to-site VPN can be established. Expressed as a comma-separated list of one or more CIDR ranges. May be left blank if there are no client-side networks to be routed. NOTE: Remember to add these subnets to the IPv4 Remote Networks list on the corresponding OpenVPN server settings.	
IPv6 Remote Network/s	
These are the IPv6 client-side networks that will be routed to this client specifically using iroute, so that a site-to-site VPN can be established. Expressed as a comma-separated list of one or more IP/PREFIX networks. May be left blank if there are no client-side networks to be routed. NOTE: Remember to add these subnets to the IPv6 Remote Networks list on the corresponding OpenVPN server settings.	
Redirect Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.

Sprawdzenie czy VPN działa na bramie centralnej

[Status / OpenVPN](#)

VPN gateway UDP:1194 Client Connections: 1

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Cipher
192.168.1.46	192.168.1.46:31778	192.168.82.2	2022-12-11 12:31:34	6 KiB	8 KiB	AES-256-GCM X

Status: ✓ Actions: [C](#) [O](#)

[Show Routing Table](#) - Display OpenVPN's internal routing table for this server.

Sprawdzenie czy VPN działa na bramie zdalnej

The screenshot shows the 'Status / OpenVPN' window. At the top, it says 'Client Instance Statistics'. Below is a table with the following data:

Name	Status	Connected Since	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
Client UDP4	up	Sun Dec 11 12:31:37 2022	192.168.1.46:31778	192.168.82.2	192.168.1.41:1194	8 KiB	7 KiB	

Klient jest w stanie pingować serwer

The terminal window title is 'ubuntu2 [Running] - Oracle VM VirtualBox'. The session name is 'gru 11 13:40'. The terminal prompt is 'admin2@admin2-VirtualBox: ~'. The user runs 'ifconfig' and 'ping' commands.

```
admin2@admin2-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.81.2 netmask 255.255.255.0 broadcast 0.0.0.0
        inet6 fe80::5e78:1366:32c7:e5f5 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:02:20:8e txqueuelen 1000 (Ethernet)
            RX packets 260230 bytes 370928744 (370.9 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 21520 bytes 1943791 (1.9 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 844 bytes 96079 (96.0 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 844 bytes 96079 (96.0 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

admin2@admin2-VirtualBox:~$ ping 192.168.80.2
PING 192.168.80.2 (192.168.80.2) 56(84) bytes of data.
64 bytes from 192.168.80.2: icmp_seq=1 ttl=64 time=0.681 ms
64 bytes from 192.168.80.2: icmp_seq=2 ttl=64 time=0.337 ms
64 bytes from 192.168.80.2: icmp_seq=3 ttl=64 time=0.293 ms
^C
--- 192.168.80.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2033ms
rtt min/avg/max/mdev = 0.293/0.437/0.681/0.173 ms
admin2@admin2-VirtualBox:~$
```

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

