

Tworzenie wirtualnej maszyny pfsense


? ✕


← Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:  ▼

Type: ▼ 

Version: ▼

Expert Mode

Next


Cancel

? ✕

← Create Virtual Hard Disk

File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.



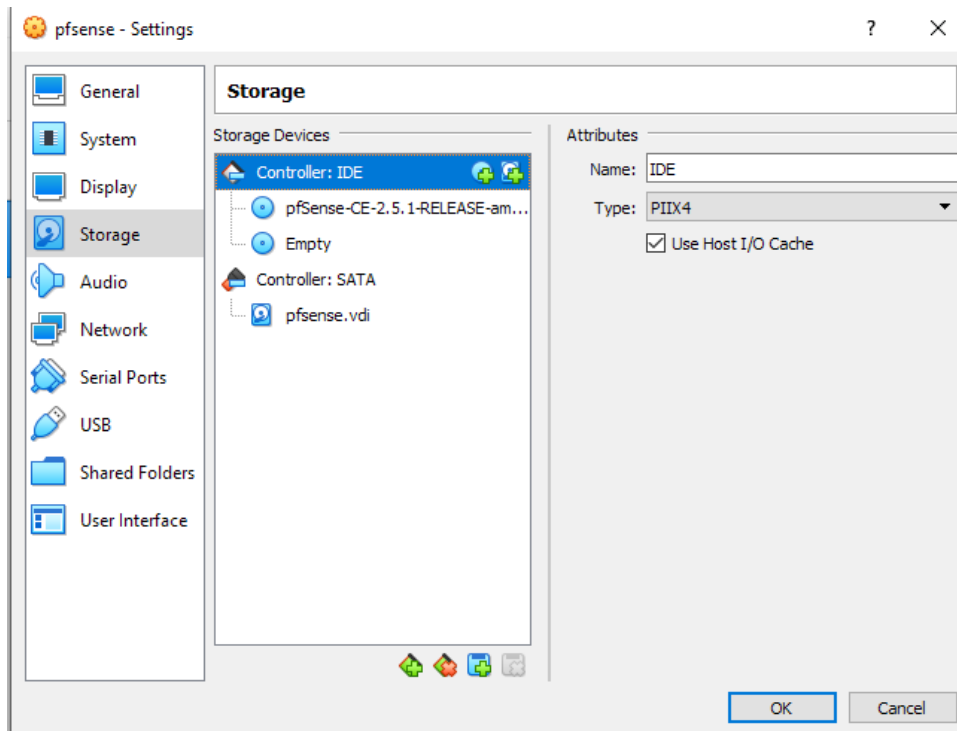
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.



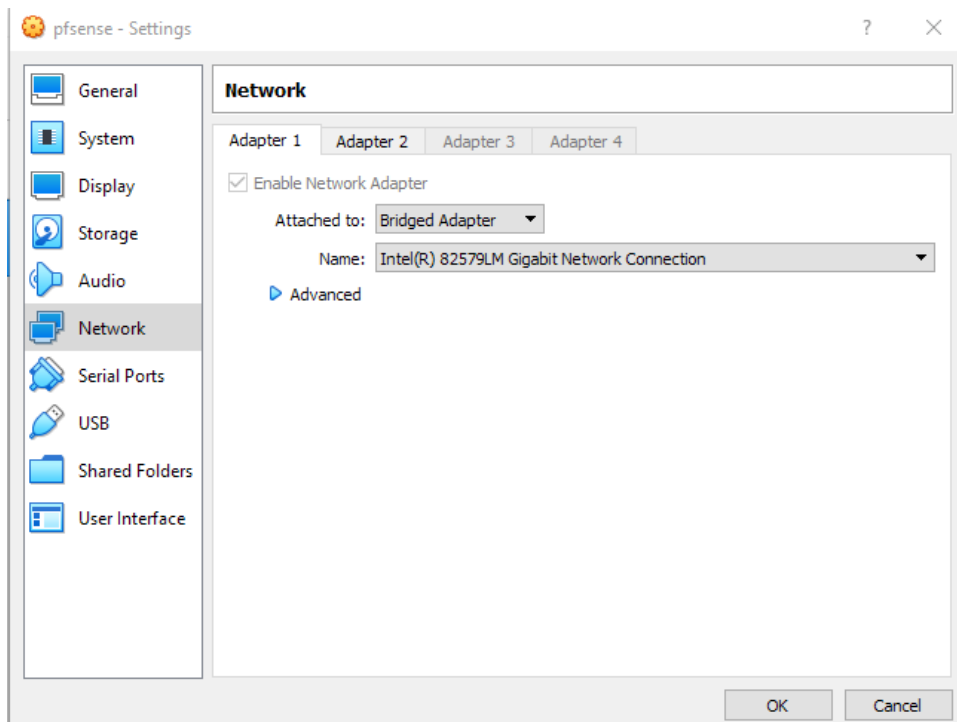
4.00 MB 2.00 TB

Create

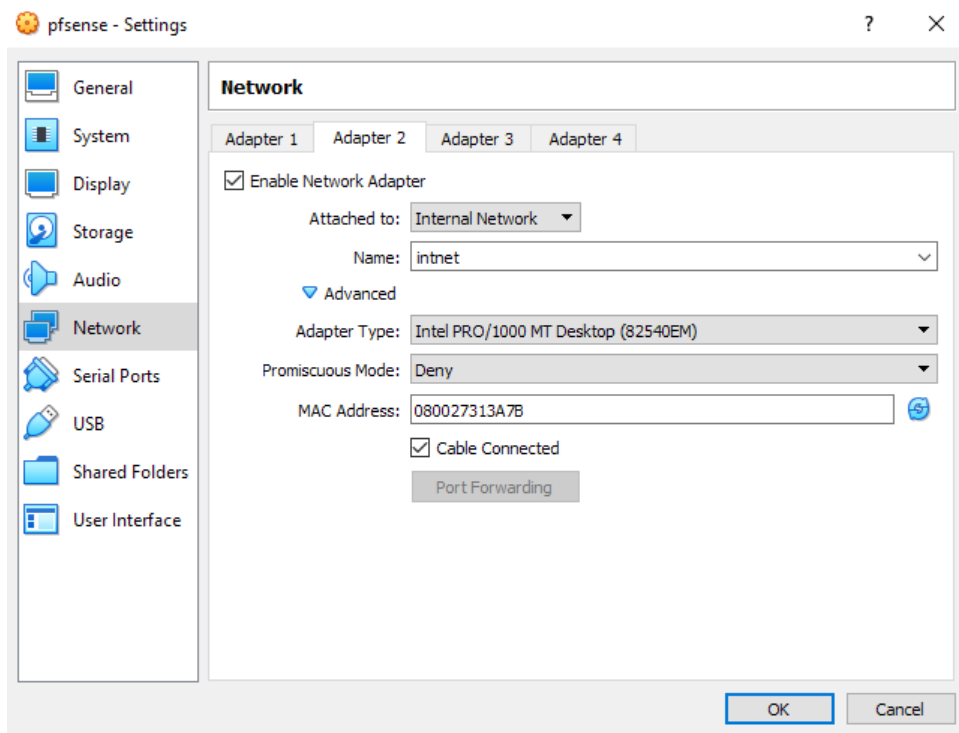
Cancel



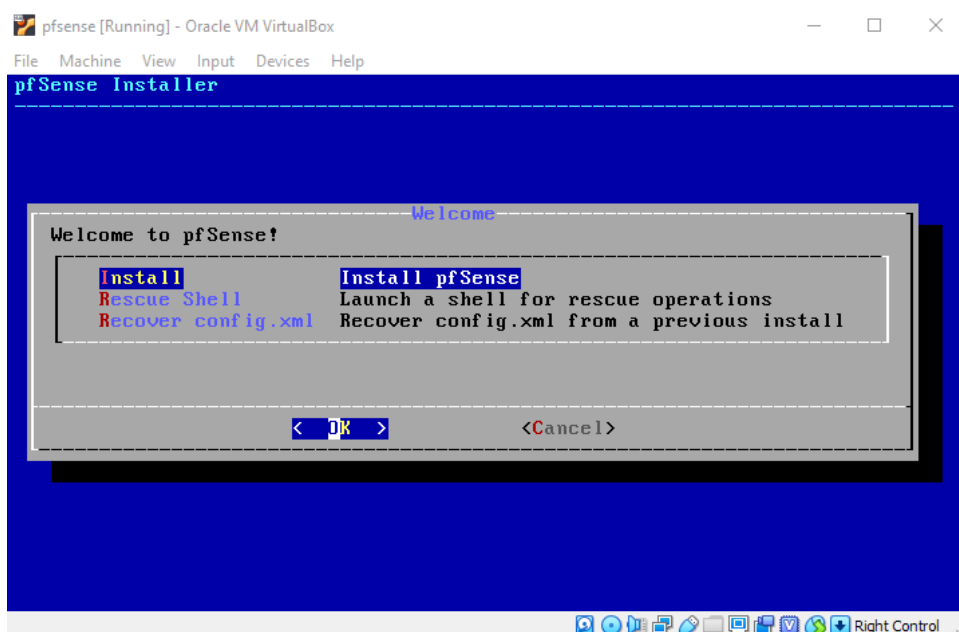
Pierwsza karta bridged



Druga karta siec wewnetrzna



Instalacja pfSense



Pierwsze uruchomienie

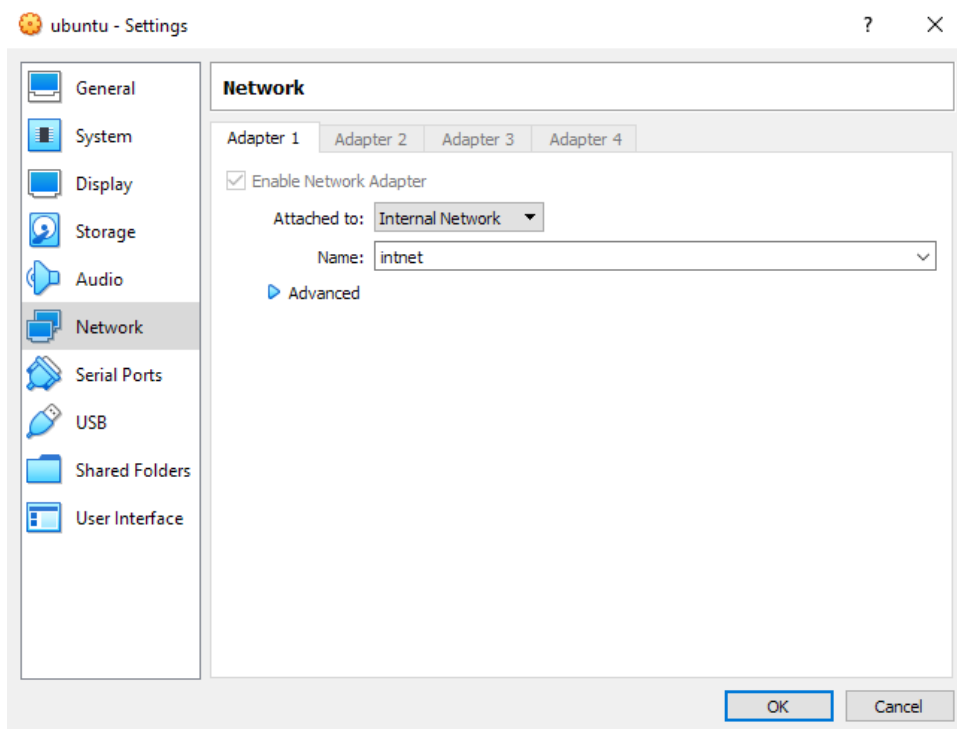
```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 1f3152cee3516768a493
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

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

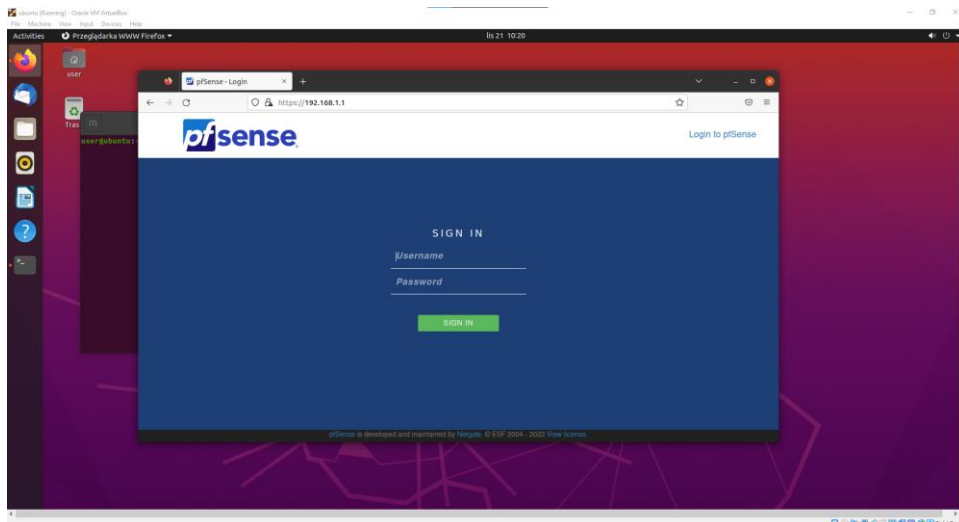
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Disable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

Enter an option: 
```

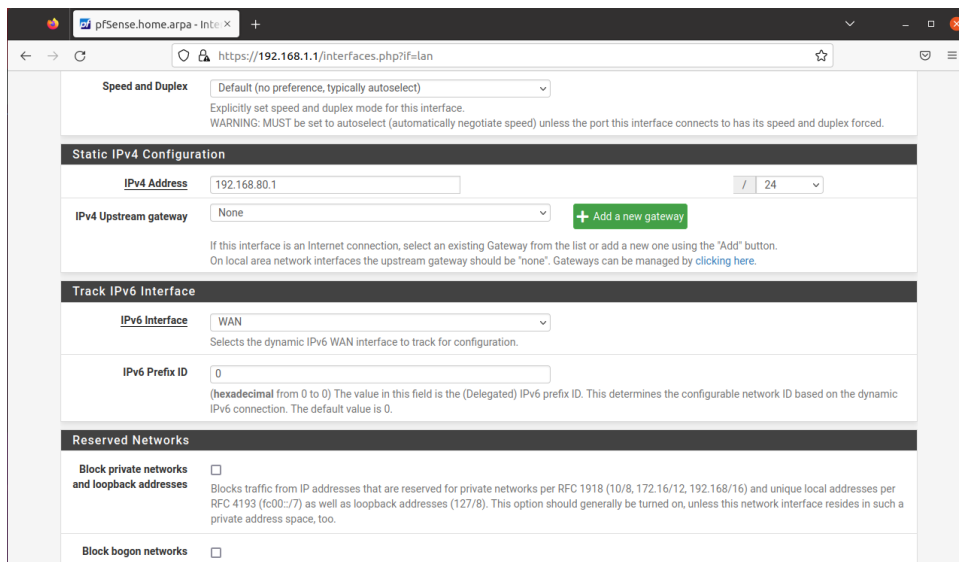
Siec wewnętrzna na drugiej maszynie – linuxie



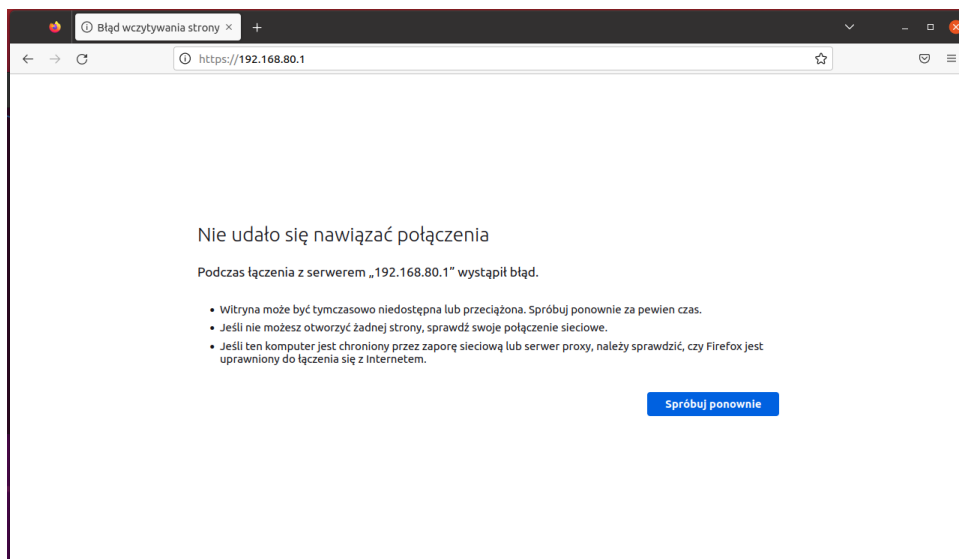
Logowanie się na pfsense z klienta



Zmiana adresu na 192.168.80.1



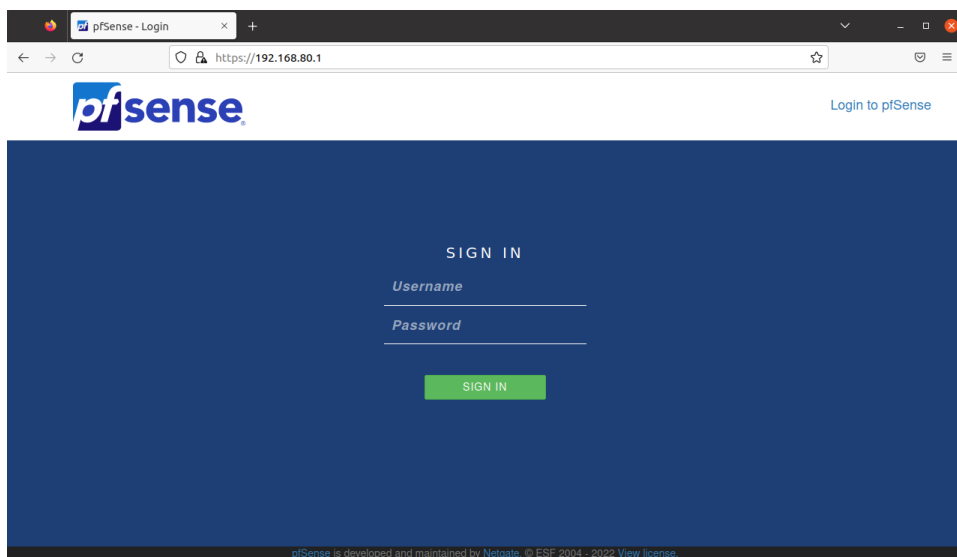
Nie można się na 192.168.80.1 połączyć po zmianie




Zmiana adresu klienta



```
user@ubuntu: ~  
user@ubuntu:~$ sudo ip addr add 192.168.80.2/24 dev enp0s3  
[sudo] password for user:  
user@ubuntu:~$
```

Teraz można się zalogować na serwer



Utworzone aliasy

Firewall Aliases IP			
Name	Values	Description	Actions
servery_dns	4.4.8.8, 8.8.8.8		  

Firewall Aliases Ports			
Name	Values	Description	Actions
wszystkie_porty	80, 443, 123, 3389, 22		  

Utworzone zasady

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / LAN

FloatingWANLAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/0 B	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	serwery_dns	53 (DNS)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	wszystkie_porty	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

Umożliwianie zarządzaniem firewallem na adresie WAN

Odblokowanie dwóch opcji w interfaces WAN

Use IPv4 connectivity as parent interface	<input type="checkbox"/> Request a IPv6 prefix/information through the IPv4 connectivity link
Request only an IPv6 prefix	<input type="checkbox"/> Only request an IPv6 prefix, do not request an IPv6 address
DHCPv6 Prefix Delegation size	<div>64</div> <div>The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.</div>
Send IPv6 prefix hint	<input type="checkbox"/> Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	<input type="checkbox"/> Start DHCP6 client in debug mode
Do not wait for a RA	<input type="checkbox"/> Required by some ISPs, especially those not using PPPoE
Do not allow PD/Address release	<input type="checkbox"/> dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent
Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> <div>Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.</div>
Block bogon networks	<input type="checkbox"/> <div>Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.</div>
Save	

Wpisanie DNS serwerów, które są przepuszczane przez zasady firewalla

From To

Additional Pools

Add [+ Add pool](#)

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Actions

Servers

WINS servers

WINS Server 1

WINS Server 2

DNS servers

4.4.8.8

8.8.8.8

DNS Server 3

DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

OMAPI

OMAPI Port

OMAPI Port

Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.

OMAPI Key

OMAPI Key

Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.

☐ Generate New Key

Generate a new key based on the selected algorithm.

Wystawianie serwera ssh na porcie 2222

Edycja pliku /etc/ssh/sshd_config

```

root@ubuntu: /
GNU nano 4.8 /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

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

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

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

Include /etc/ssh/sshd_config.d/*.conf

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa key

```

Wrote 124 lines

^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

Ustawienie forwardingu

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match.
Type Address/mask

Destination port range
From port To port
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

https://192.168.80.1/firewall_nat_edit.php?id=0

Destination port range
From port To port
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

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

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Filter rule association
[View the filter rule](#)

Rule Information

Created	11/21/22 10:39:20 by admin@192.168.80.2 (Local Database)
Updated	11/22/22 18:09:58 by admin@192.168.80.3 (Local Database)

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / NAT / Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

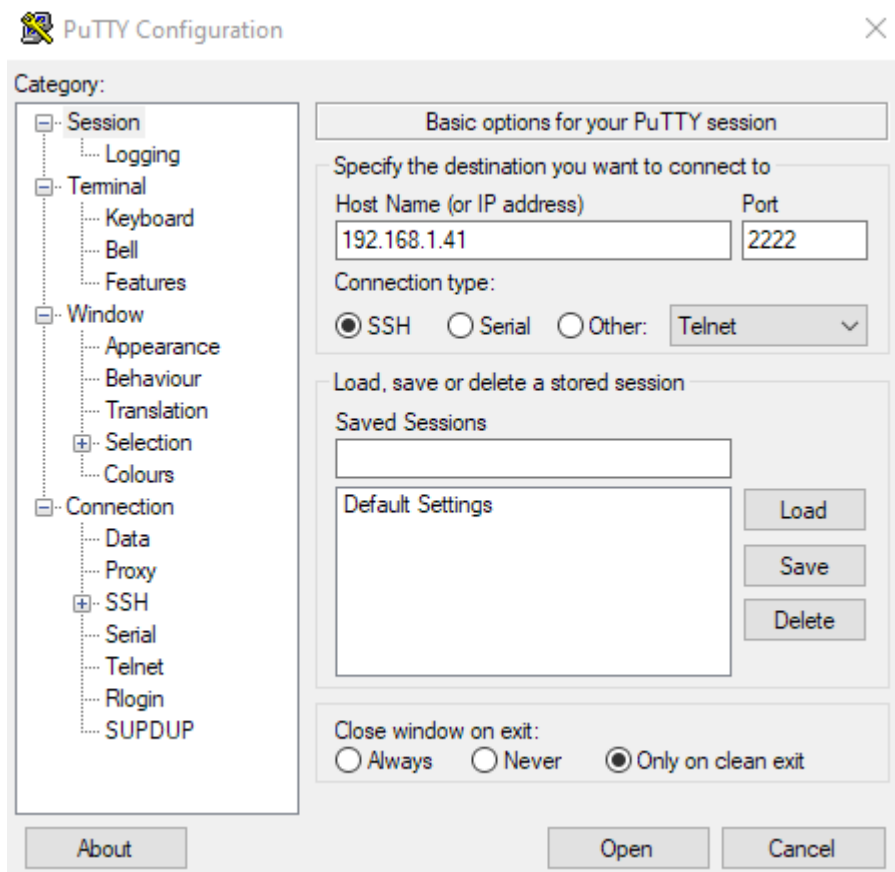
Port Forward 1:1 Outbound NPT

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	2222	192.168.80.2	2222	ssh	Edit Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Legend
▶ Pass

Testowanie



Udane zalogowanie

```
user@ubuntu: ~  
login as: user  
user@192.168.1.41's password:  
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 wto, 22 lis 2022, 18:14:19 UTC  
  
System load:  0.28      Processes:    216  
Usage of /:   49.9% of 17.52GB  Users logged in: 1  
Memory usage: 45%      IPv4 address for enp0s3: 192.168.80.2  
Swap usage:   0%        IPv4 address for enp0s3: 192.168.80.3  
  
* 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  
  
Last login: Wed Oct 12 10:39:09 2022  
user@ubuntu:~$
```