

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.



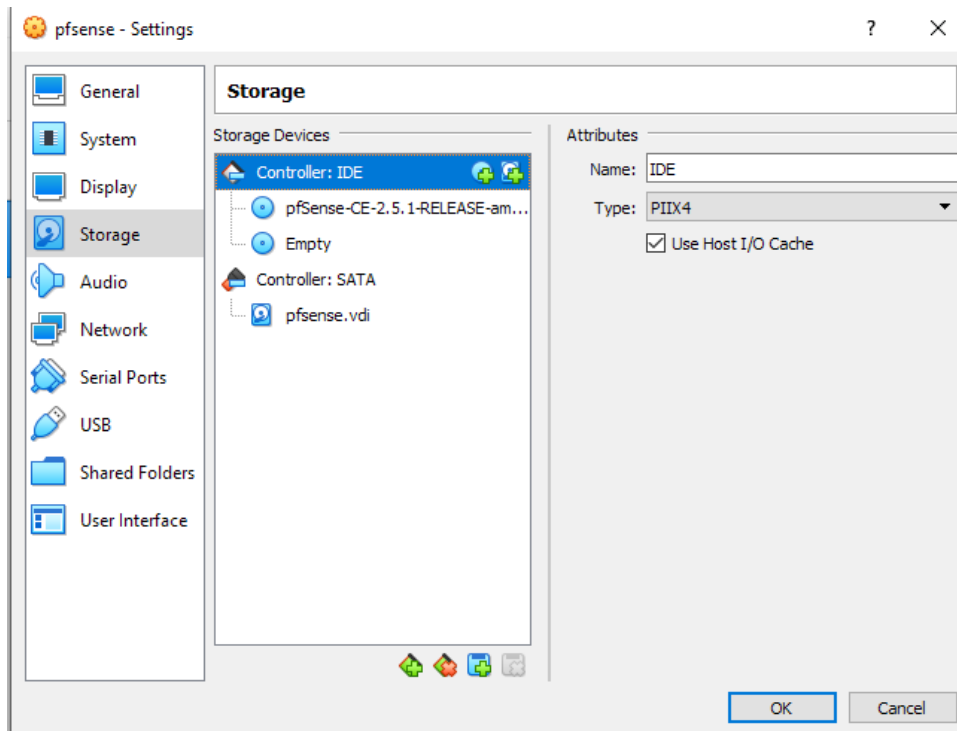
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.



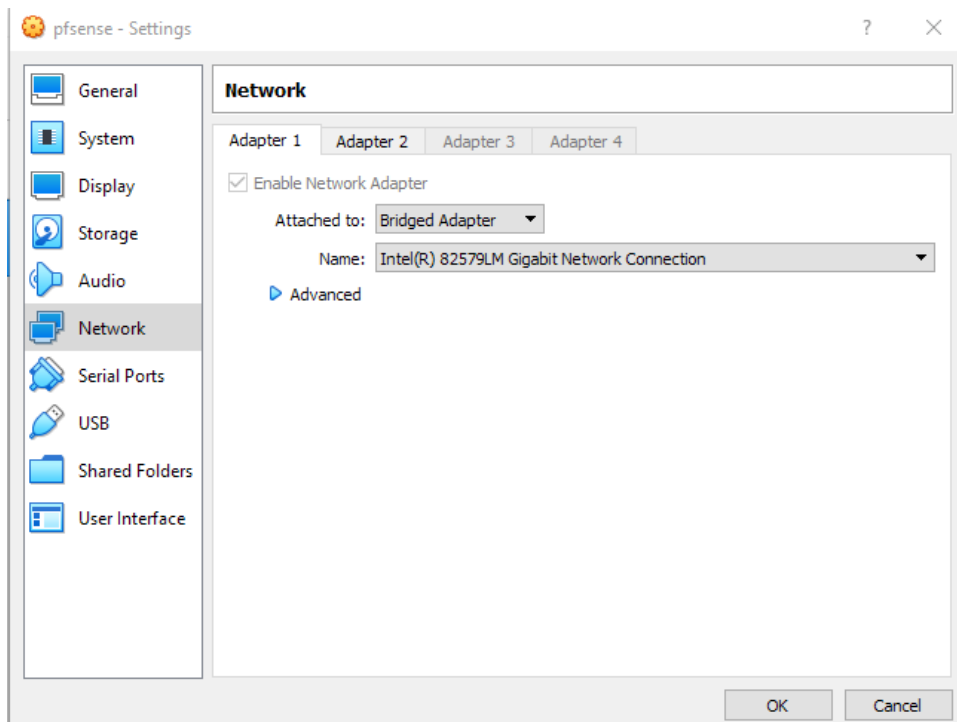
4.00 MB 2.00 TB

Create

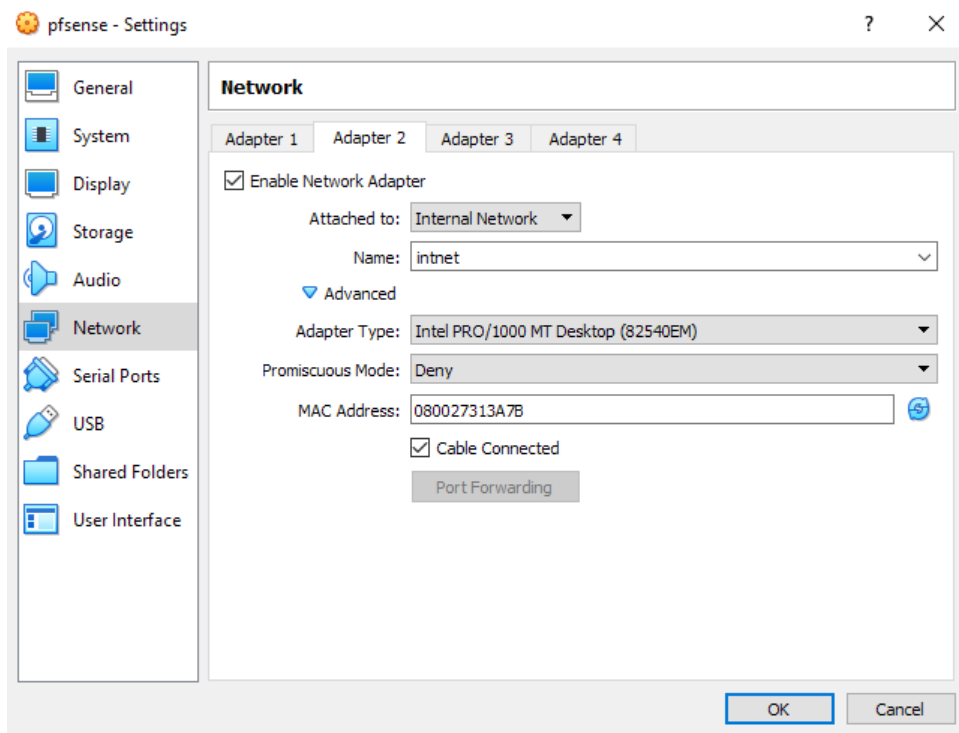
Cancel



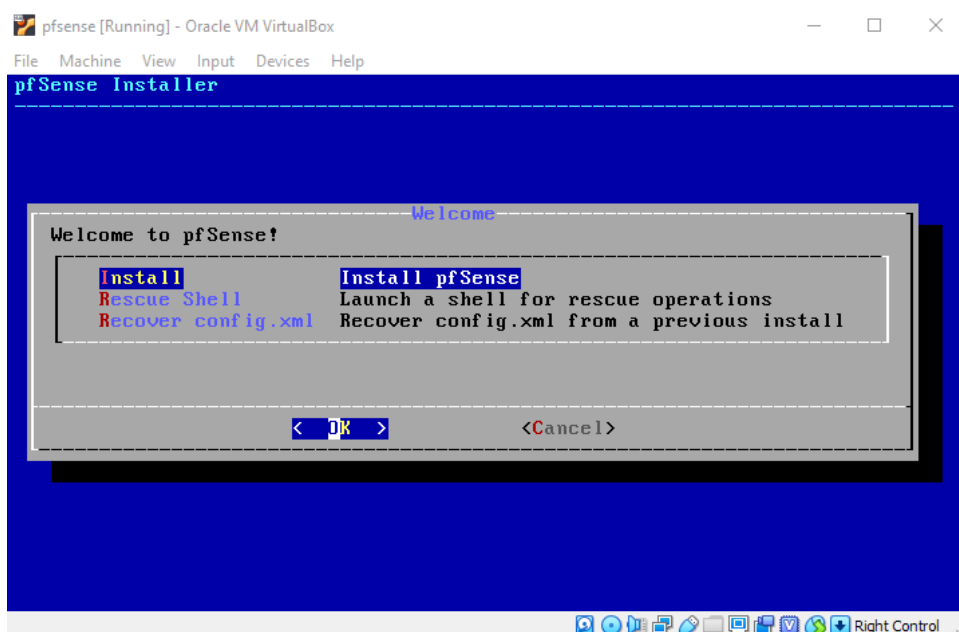
Pierwsza karta bridged



Druga karta siec wewnetrzna



Instalacja pfSense



Pierwsze uruchomienie

```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Starting syslog...done.
Starting CRON... done.
pfSense 2.5.1-RELEASE amd64 Mon Apr 12 07:50:14 EDT 2021
Bootup complete

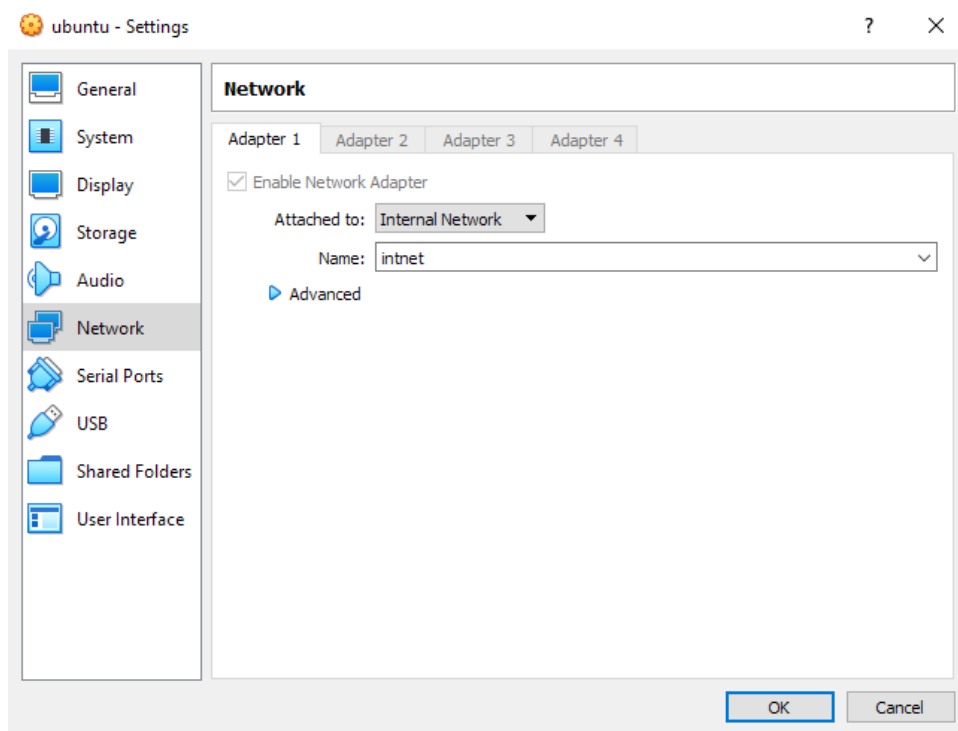
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 1f3152cee3516768a493
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

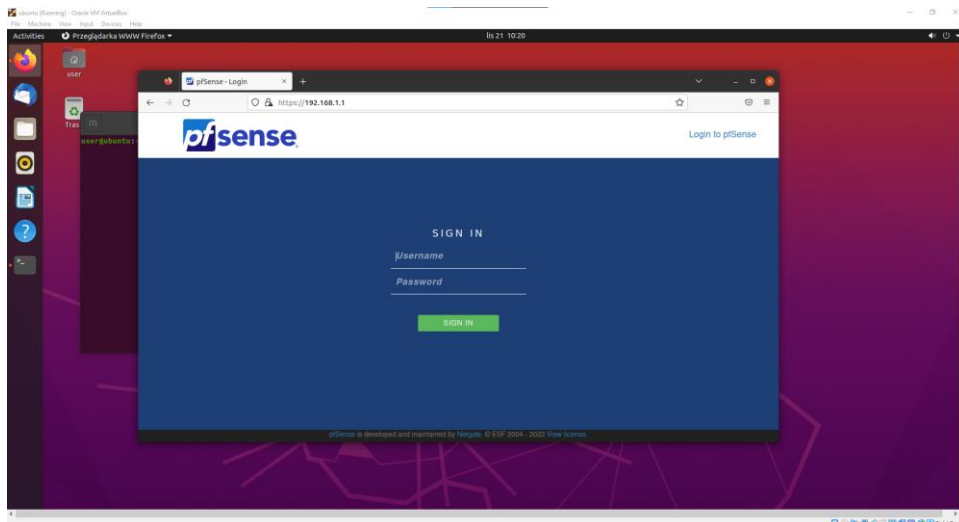
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: 
```

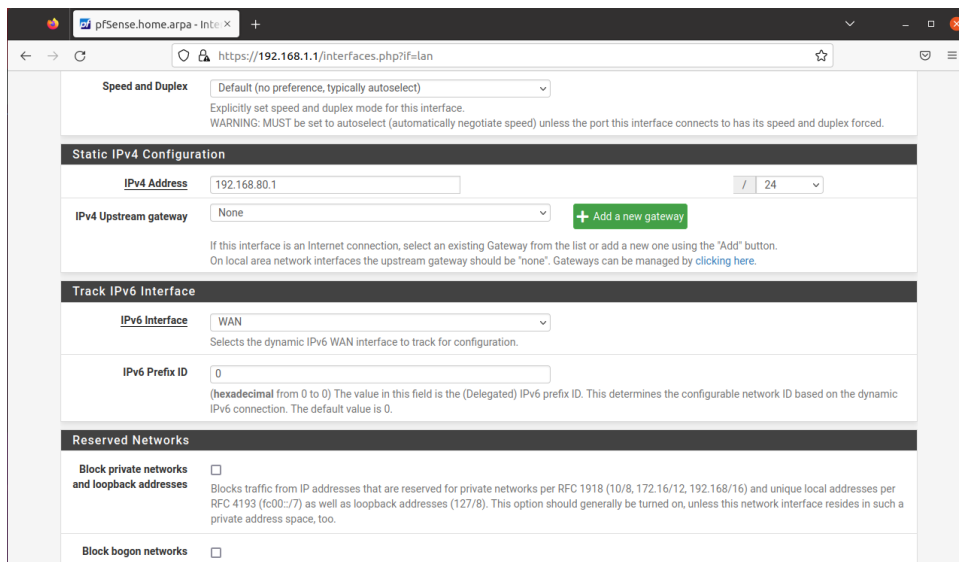
Siec wewnętrzna na drugiej maszynie – linuxie



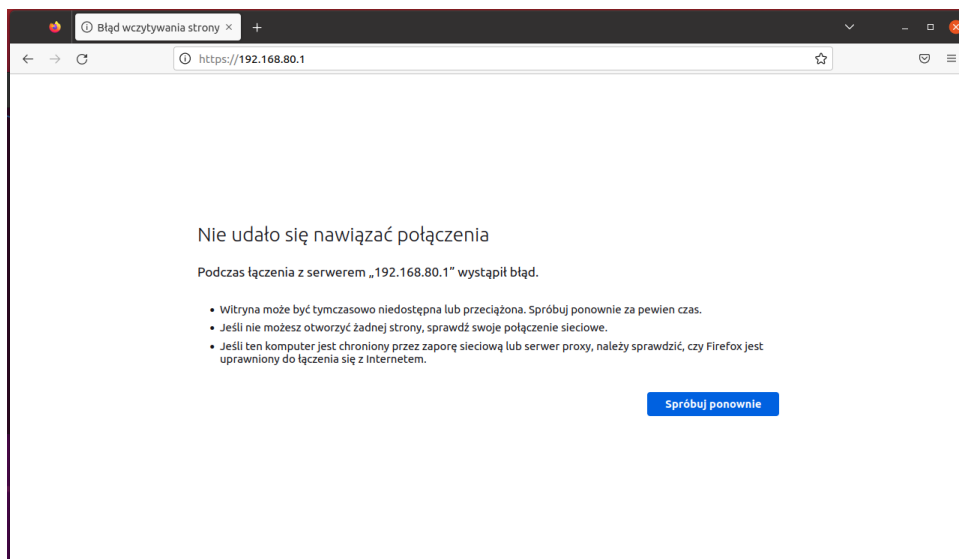
Logowanie się na pfsense z klienta



Zmiana adresu na 192.168.80.1



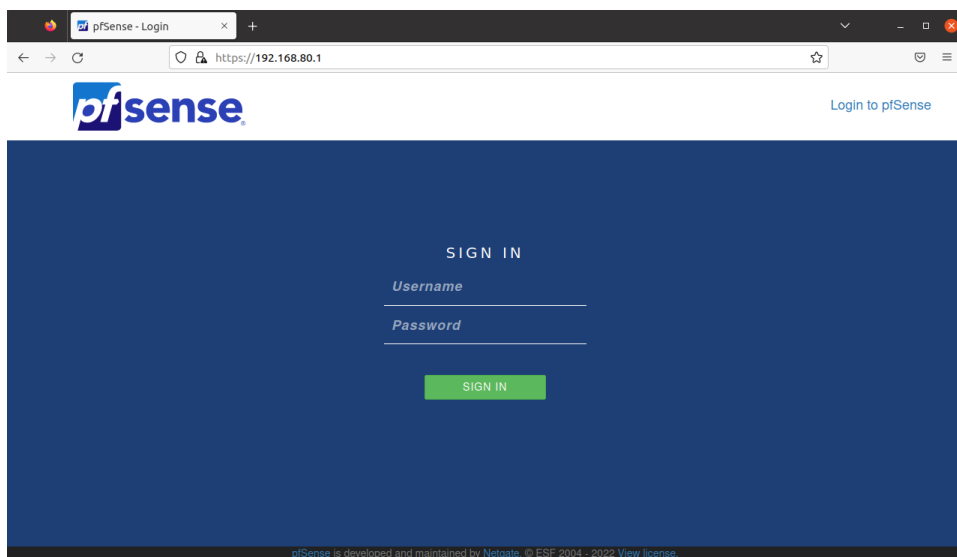
Nie można się na 192.168.80.1 połączyć po zmianie




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

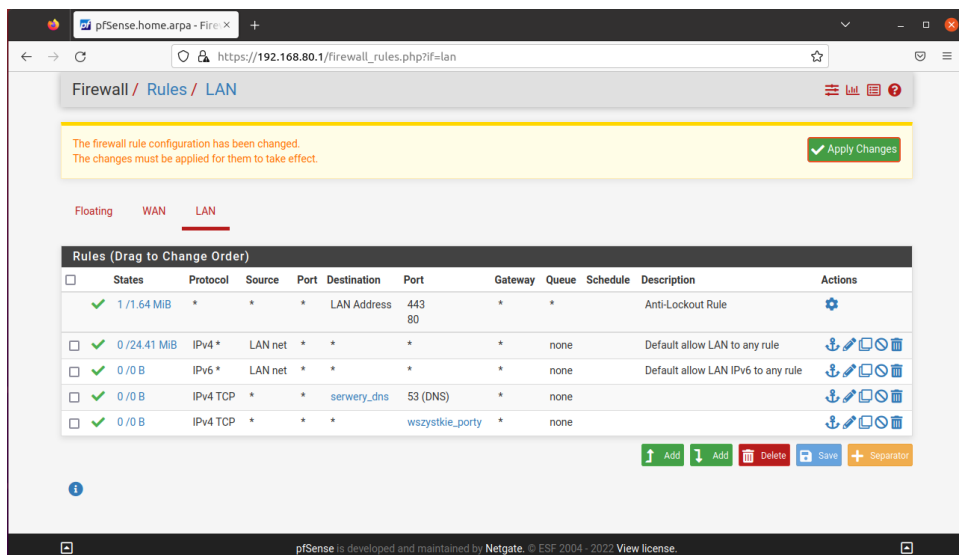


Utworzone aliasy

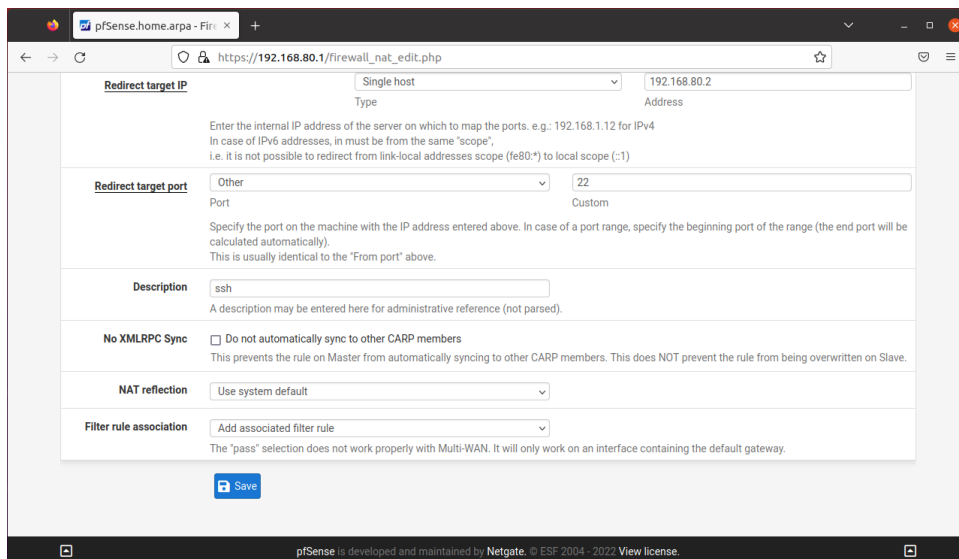
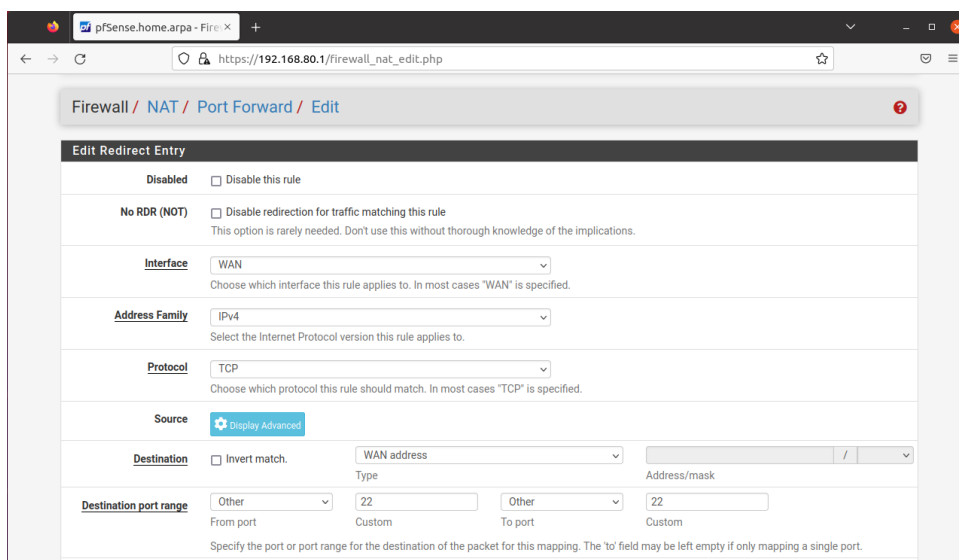
Firewall Aliases IP			
Name	Values	Description	Actions
servery_dns	4.4.8.8, 8.8.8.8		  

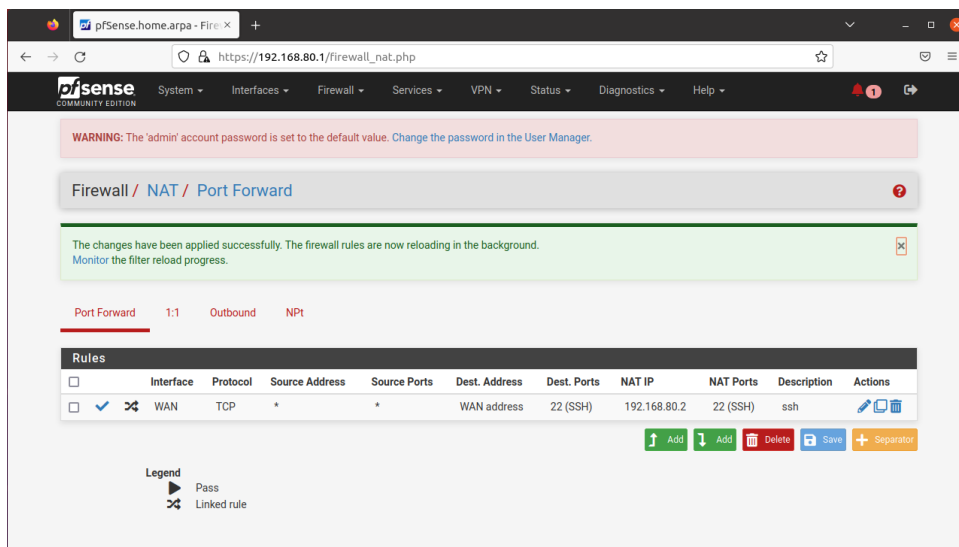
Firewall Aliases Ports			
Name	Values	Description	Actions
wszystkie_porty	80, 443, 123, 3389, 22		  

Utworzone zasady

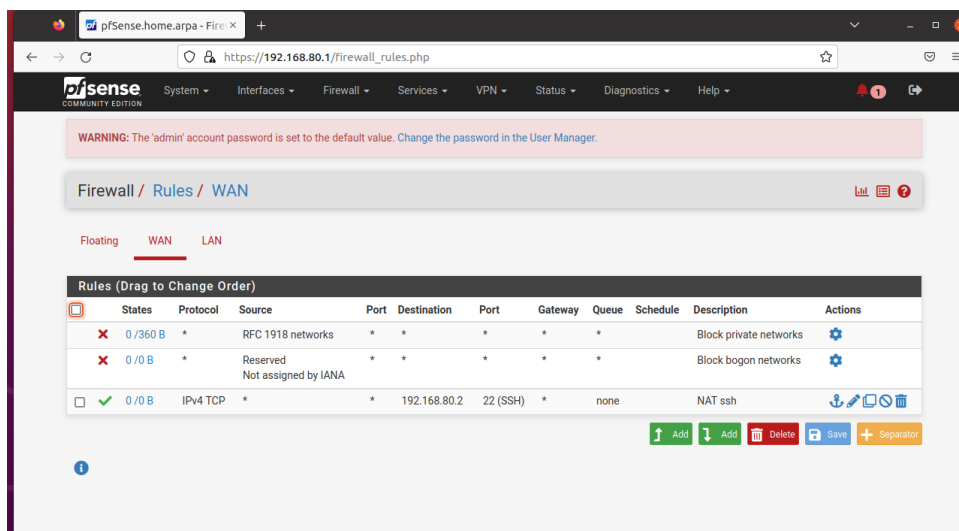


Umożliwianie zarządzaniem firewallem na adresie WAN





Automatycznie powstaje reguła na WAN



Wystawianie serwera ssh na porcie 2222

pfSense.home.arpa - Sys...
https://192.168.80.1/system_advanced_admin.php

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

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

System / [Advanced](#) / [Admin Access](#)

[Admin Access](#) Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

Protocol ☐ HTTP ☒ HTTPS (SSL/TLS)

SSL/TLS Certificate
Certificates known to be incompatible with use for HTTPS are not included in this list.

TCP port
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect ☐ Disable webConfigurator redirect rule
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

HSTS ☐ Disable HTTP Strict Transport Security
When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)

pfSense.home.arpa - Sys...
https://192.168.80.1/system_advanced_admin.php

Alternate Hostnames
Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks. Specify alternate hostnames by which the router may be queried, to bypass the DNS Rebinding Attack checks. Separate hostnames with spaces.

Browser HTTP_REFERER enforcement ☐ Disable HTTP_REFERER enforcement check
When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from [Wikipedia](#).

Browser tab text ☐ Display page name first in browser tab
When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.

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.

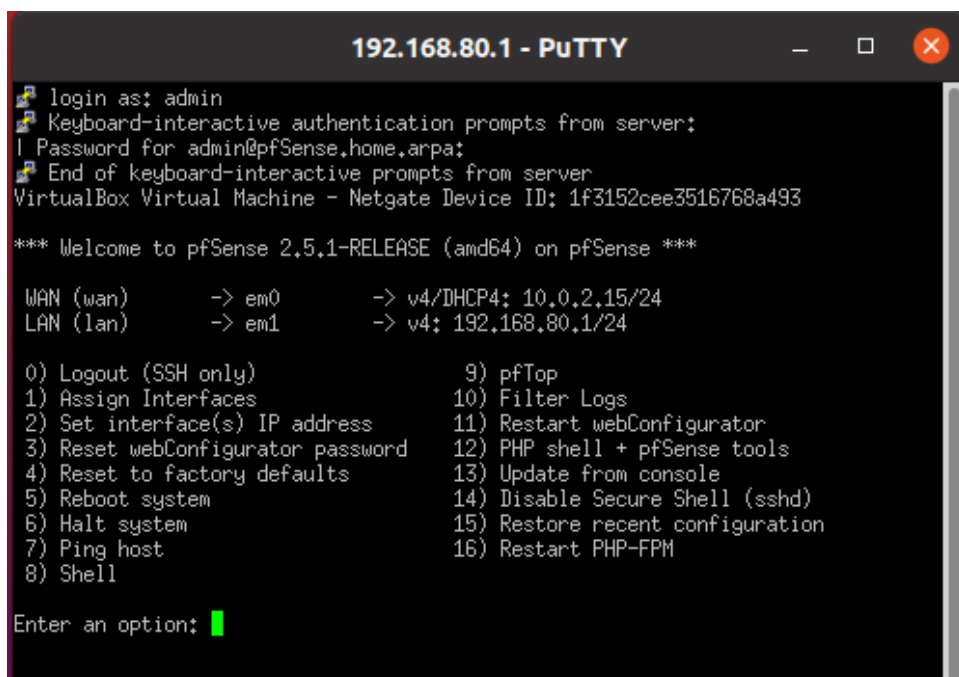
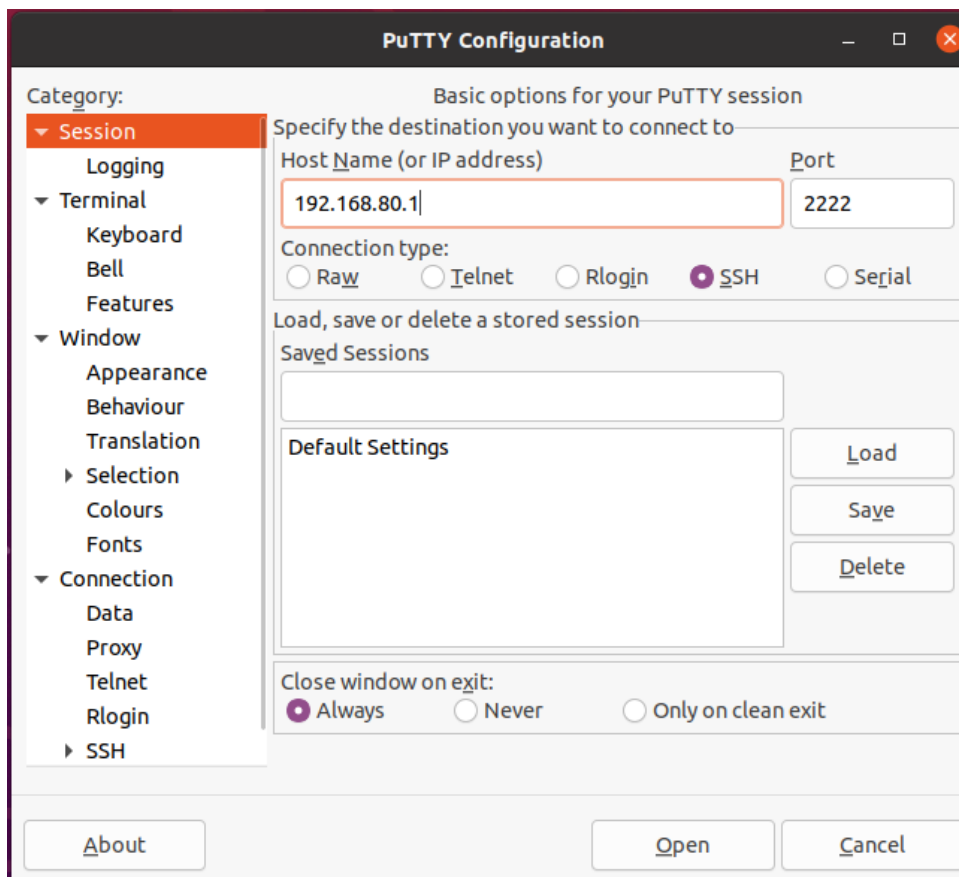
SSH port
Note: Leave this blank for the default of 22.

Login Protection

Threshold
Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.

Blocktime
Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.

Testowanie



Udane połączenie