

# Zastosowania wirtualizacji na przykładzie instalacji zapór sieciowych



**Dominik Przybysz**

# Wirtualizacja - rodzaje

Cel – uruchomienie wielu wydajnych maszyn wirtualnych na  
?jednej? fizycznej

- Parawirtualizacja
- Pełna wirtualizacja
- Typ 1. - bare metal
- Typ 2.

# Wirtualizacja - zalety/wady

## Zalety

- Uniezależnienie od platformy sprzętowej
- Lepsza gospodarka zasobami – ograniczenie kosztów i ilości sprzętu
- Skalowalność
- Wysoka dostępność
- Możliwość tworzenia migawek
- Łatwość tworzenia kopii zapasowych i ich odtwarzania.

## Wady

- Wysokie koszty licencji
- Bezpieczeństwo (np. czy maszyny wirtualne aby na pewno się nie skomunikują)
- Komplikacja używanych technologii
- W wypadku problemu hipernadzorcy padają wszystkie maszyny wirtualne

# Wirtualizacja - zalety/wady

## Zalety

- Uniezależnienie od platformy sprzętowej
- Lepsza gospodarka zasobami – ograniczenie kosztów i ilości sprzętu
- Skalowalność
- Wysoka dostępność
- Możliwość tworzenia migawek
- Łatwość tworzenia kopii zapasowych i ich odtwarzania.

## Wady

- Wysokie koszty licencji
- Bezpieczeństwo (np. czy maszyny wirtualne aby na pewno się nie skomunikują)
- Komplikacja używanych technologii
- W wypadku problemu hipernadzorcy padają wszystkie maszyny wirtualne

<https://sekurak.pl/hej-admini-i-uzytkownicy-lepiej-latajcie-asap-wasze-instancje-vm-ware-grupa-ransomware-wykorzystuje-podatnosc-klasy-rce-zeby-przejmowac-hurtem-cale-farmy-vmek/>

# VirtualBox kontra VMware ESXi



- + otwarto źródłowy
  - + zadziała (prawie) na wszystkim
  - + działa na typowym Linux (typ 2)
  - skomplikowane przygotowanie do pracy produkcyjnej
  - niewygodne zarządzanie siecią
  - + podstawowe funkcjonalności bezpłatne
  - + funkcjonalność „teleport” bezpłatna
  - \* interfejs GUI / api
- wysokie wymagania sprzętowe
  - zdarzają się kompilacje przy instalacji
  - jest wyspecjalizowanym systemem operacyjnym o wąskiej funkcjonalności (typ 1)
  - + łatwy w konfiguracji
  - + ergonomiczne administrowanie siecią
  - + podstawowe funkcjonalności bezpłatne
  - \* interfejs webowy / api

# VirtualBox kontra VMware ESXi



- + otwarto źródłowy
- + zadziała (prawie) na wszystkim
- + działa na typowym Linux (typ 2)
- skomplikowane przygotowanie do pracy produkcyjnej
- niewygodne zarządzanie siecią
- + podstawowe funkcjonalności bezpłatne
- + funkcjonalność „teleport” bezpłatna
- \* interfejs GUI / api

- wysokie wymagania sprzętowe
- zdarzają się kompilacje przy instalacji
- \* jest wyspecjalizowanym systemem operacyjnym o wąskiej funkcjonalności (typ 1)
- + łatwy w konfiguracji
- + ergonomiczne administrowanie siecią
- + podstawowe funkcjonalności bezpłatne
- \* interfejs webowy / api

<https://www.dobreprogramy.pl/bachus/Cud-inzynierii-wirtualizacji-vMotion,91068.html>

# Interfejs VMware ESXi 6.5

The screenshot displays the VMware ESXi 6.5 web interface for host **dl360g5.dom.lan**. The interface is divided into several sections:

- Host Overview:** Shows the host name, version (6.5.0 Update 3), state (Normal), and uptime (7.23 days).
- Hardware:**
  - Manufacturer: HP
  - Model: ProLiant DL360 G5
  - CPU: 8 CPUs x Intel(R) Xeon(R) CPU L5420 @ 2.50GHz
  - Memory: 16 GB
  - Persistent Memory: 0 B
  - Virtual flash: 0 B used, 0 B capacity
- Networking:**
  - Hostname: dl360g5.dom.lan
  - IP addresses: 1. vmk0: 10.44.44.203, 2. vmk0: fe80::21b:78ff:feeb:554e
  - DNS servers: 1. 10.44.44.1, 2. 8.8.8.8
  - Default gateway: 10.44.44.1
  - IPv6 enabled: Yes
- Configuration:**
  - Image profile: (Updated) ESXi-6.5.0-20200604001-standard (VMware, Inc.)
  - vSphere HA state: Not configured
  - vMotion: Supported
- System Information:**
  - Date/time on host: Saturday, November 14, 2020, 14:27:23 UTC
  - Install date: Monday, January 16, 2017, 00:32:33 UTC
  - Asset tag: (empty)
  - Serial number: (empty)
  - BIOS version: P58
  - BIOS release date: Sunday, August 16, 2015, 02:00:00 +0200
- Performance summary last hour:** Shows a bar chart for CPU and memory usage. CPU usage is at 100%, and memory usage is at 16%.
- Recent tasks:** A table listing recent operations performed on the host.

Task	Target	Initiator	Queued	Started	Result	Completed
Power On VM	xubuntu-endpoint	root	11/14/2020 15:04:20	11/14/2020 15:04:20	Completed successfully	11/14/2020 15:04:23
Reconfig VM	xubuntu-endpoint	root	11/14/2020 15:04:15	11/14/2020 15:04:15	Completed successfully	11/14/2020 15:04:17
Power Off VM	xubuntu-endpoint	root	11/14/2020 15:04:05	11/14/2020 15:04:05	Completed successfully	11/14/2020 15:04:07
Reconfig VM	xubuntu-endpoint	root	11/14/2020 15:03:56	11/14/2020 15:03:56	Completed successfully	11/14/2020 15:03:57
Reconfig VM	xubuntu-endpoint	root	11/14/2020 15:03:41	11/14/2020 15:03:41	Completed successfully	11/14/2020 15:03:42
Power On VM	xubuntu-endpoint	root	11/14/2020 15:02:59	11/14/2020 15:02:59	Completed successfully	11/14/2020 15:03:02

# Wirtualizacja – inne rozwiązania



VMware Player



Linux  
**KVM**



**LXC**

**PROXMOX**





# Firewall - znaczenia

- Usługa / Program filtrujący pakiety

UFW      FirewallD      iptables      Windows Firewall      ...

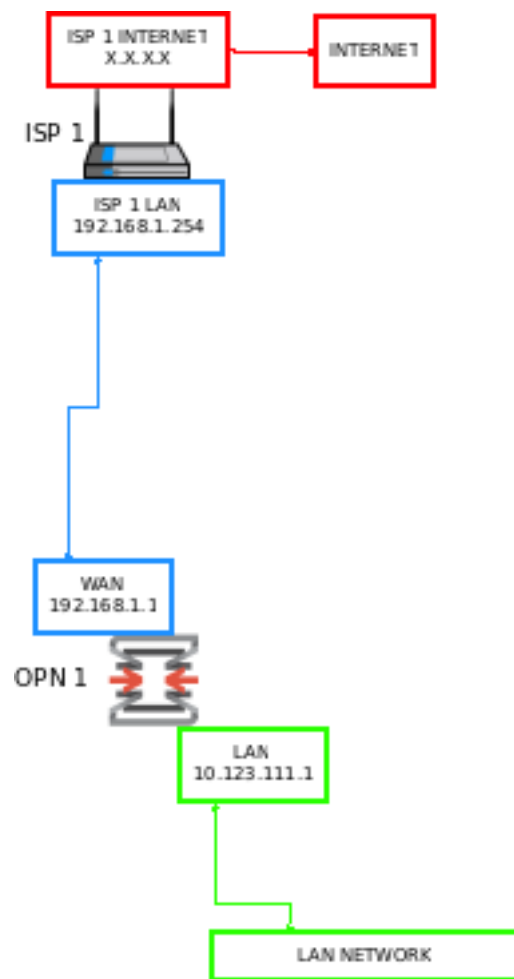
- Urządzenie sprzętowe filtrujące pakiety



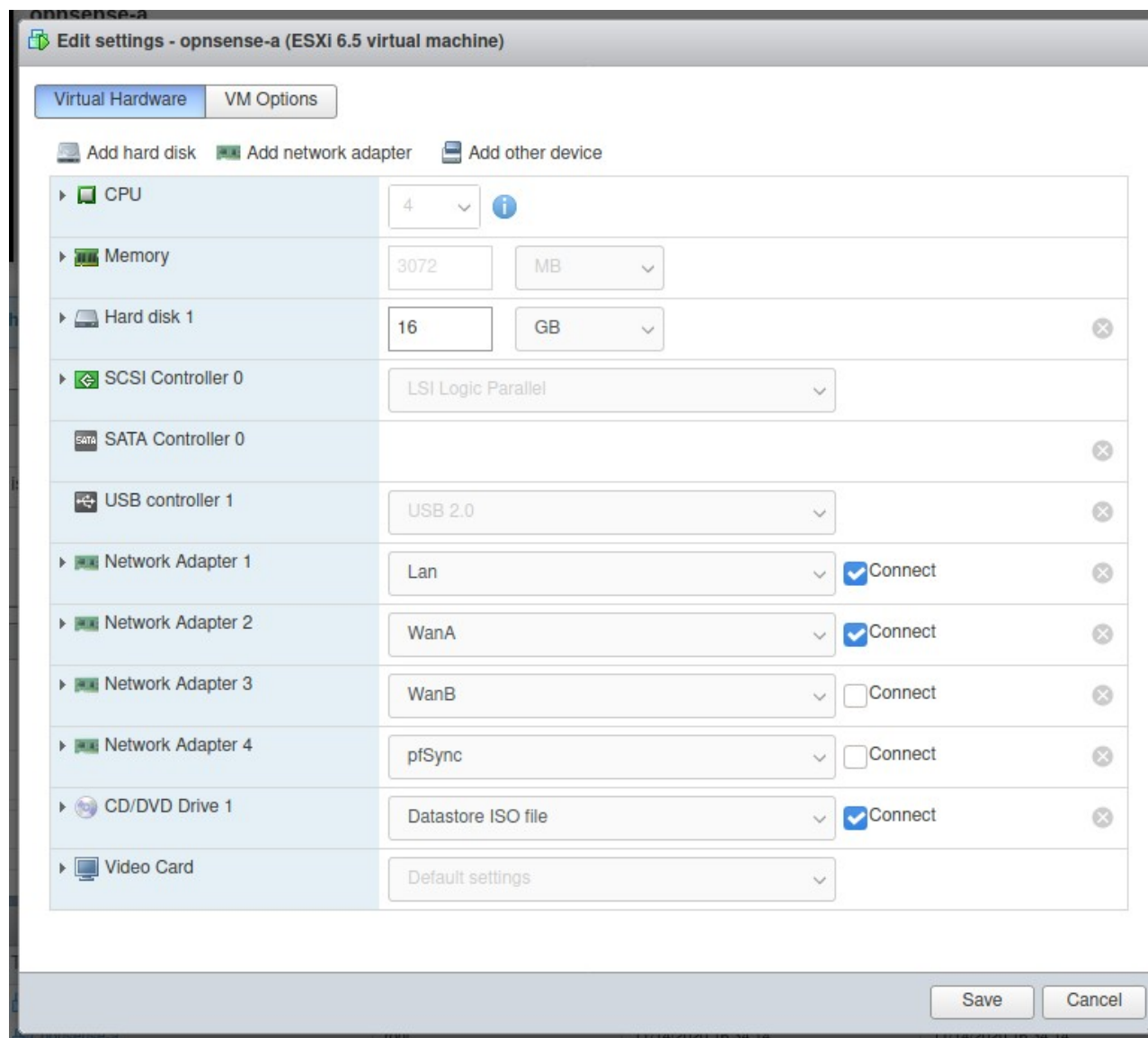
- Serwer z oprogramowaniem filtrującym pakiety



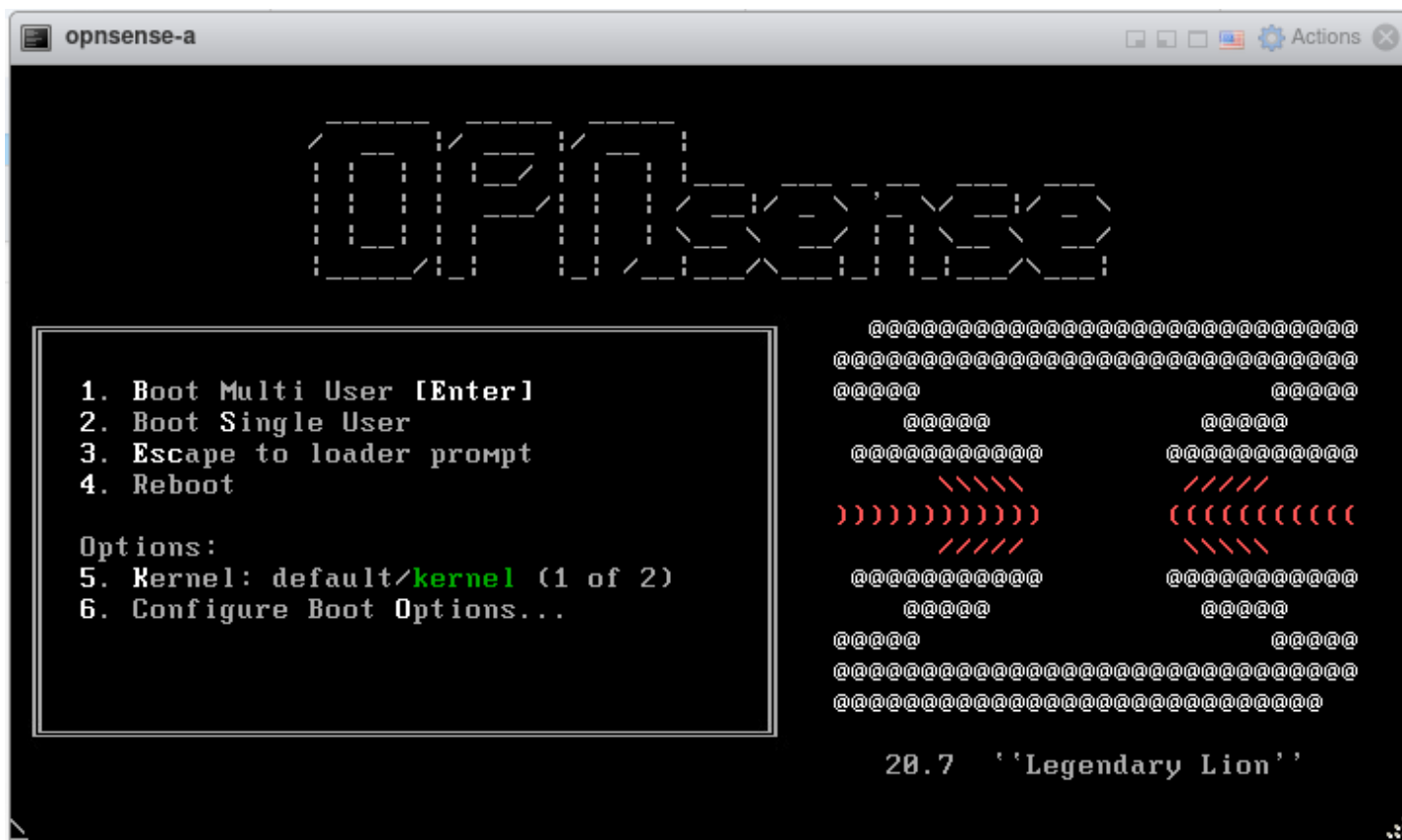
# OPNsense - konfiguracja



# OPNsense - instalacja



# OPNsense - instalacja



# OPNsense - instalacja

```
opnsense-a
F10=Refresh Display

                               @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                               @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                               @@@@@@
                               @@@@@@
                               @@@@@@@@@@@@@@@@@@
                               ///////////////
                               ((((((((((((((
                               \\\\\\\
                               @@@@@@@@@@@@@@@@@@
                               @@@@@@
                               @@@@@@
                               @@@@@@@@@@@@@@@@@@
                               @@@@@@@@@@@@@@@@@@

OPNsense 20.7

Welcome to the OPNsense 20.7 installer!

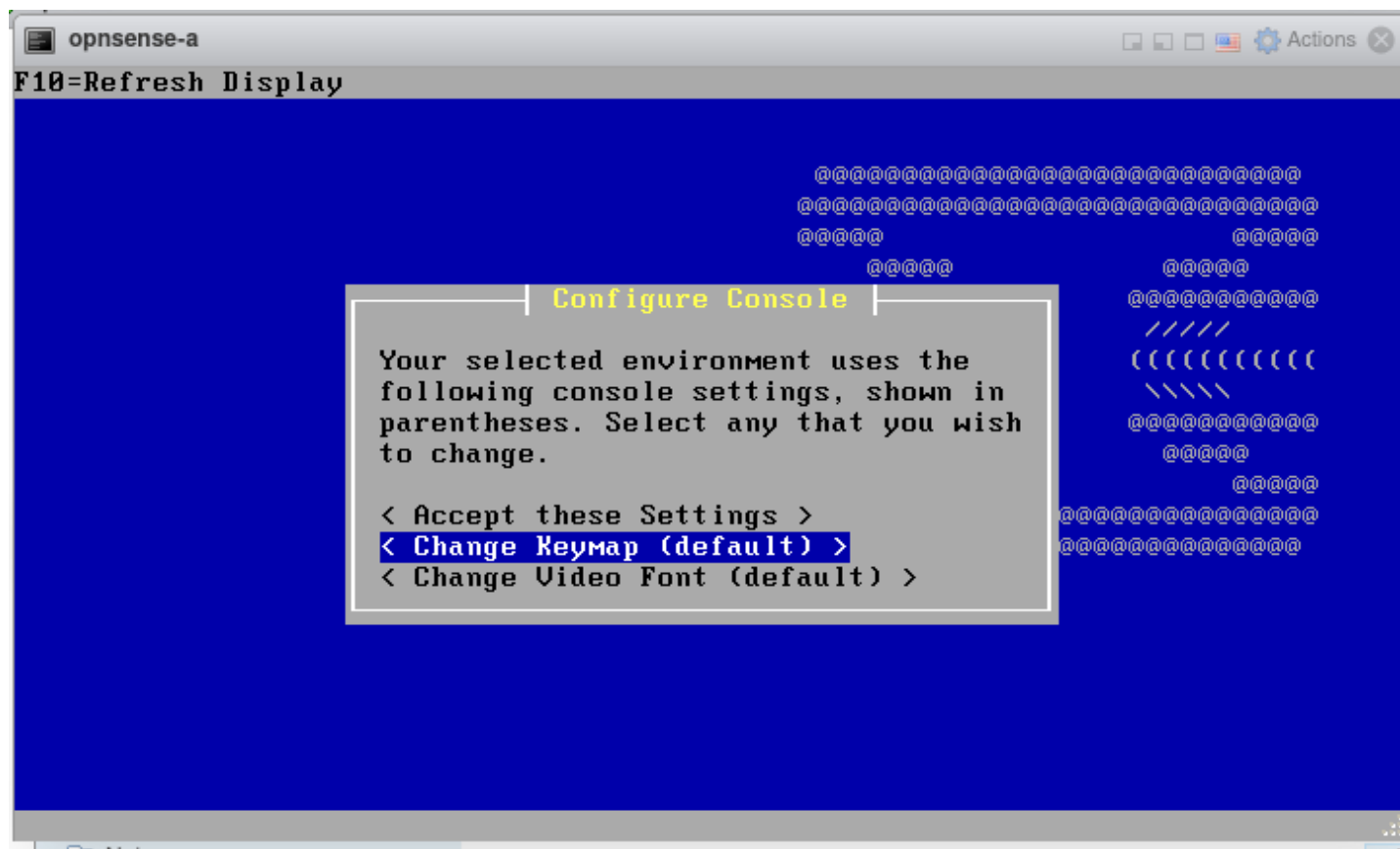
Before we begin, you will be asked a
few questions so that this installation
environment can be set up to suit your
needs.

You will then be presented a menu of
items from which you may select to
install a new system, with or without
importing a previous configuration.

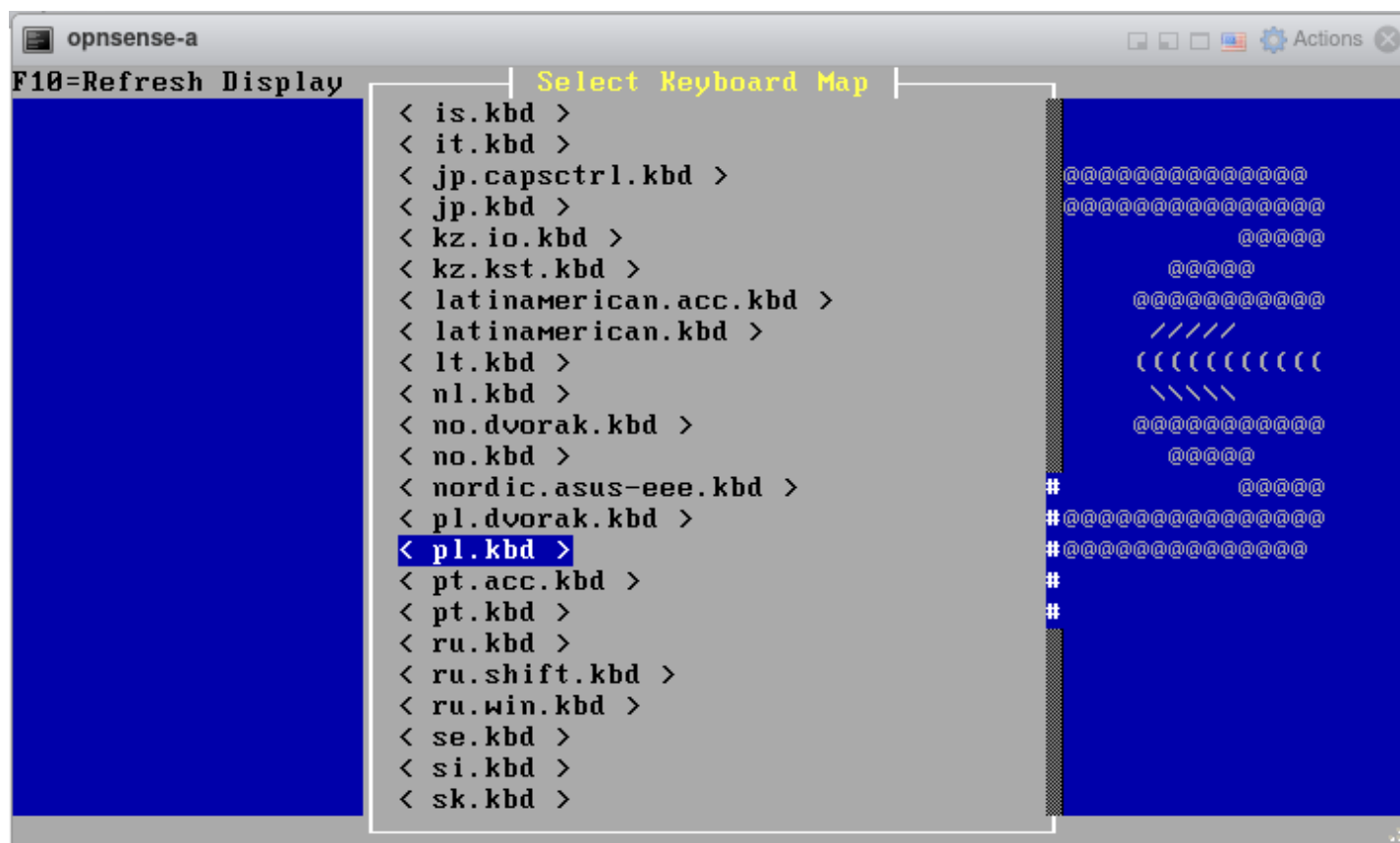
< Ok, let's go. >

Set up the installation environment and continue
```

# OPNsense - instalacja



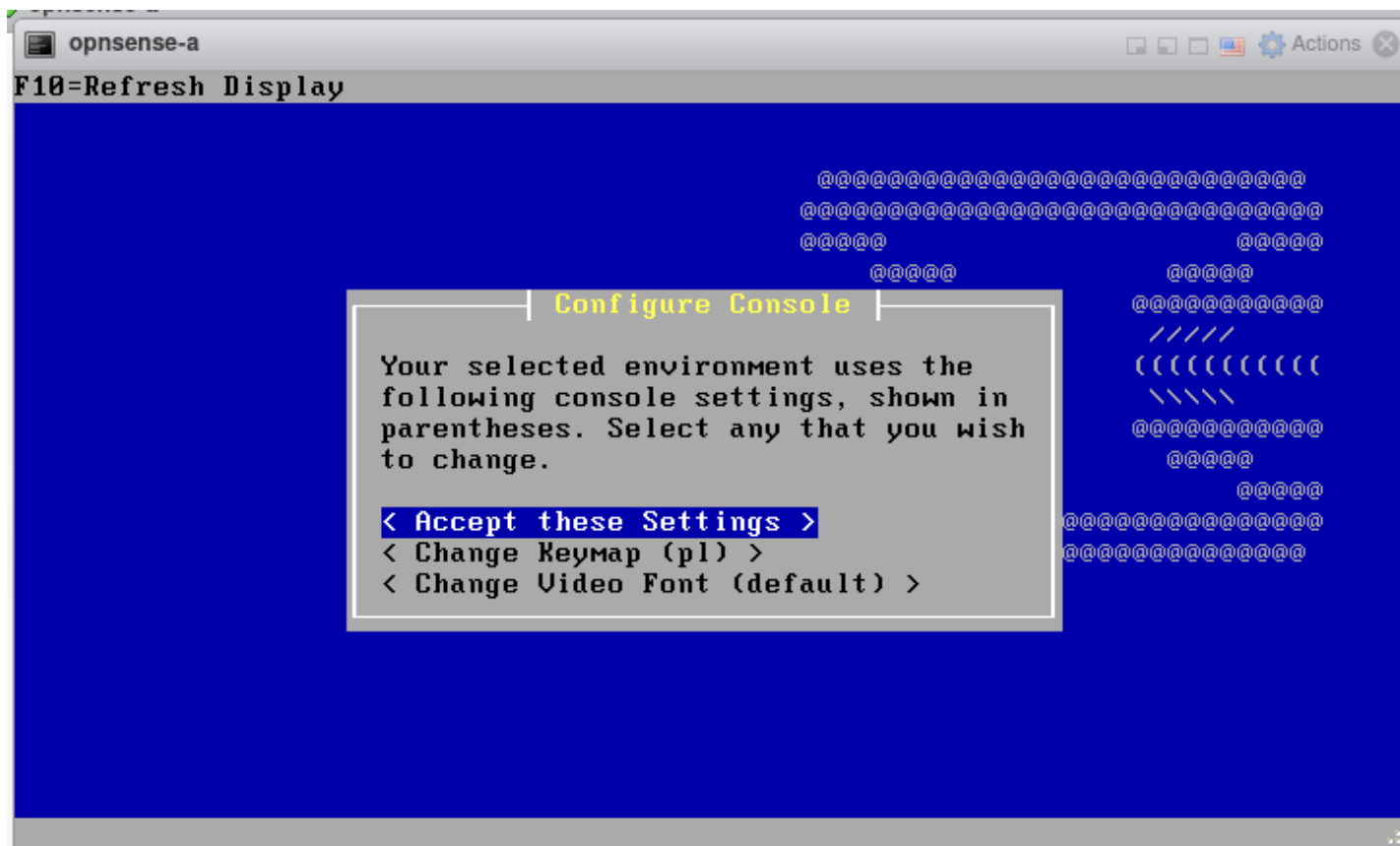
# OPNsense - instalacja



```
opnsense-a
F10=Refresh Display
Select Keyboard Map
< is.kbd >
< it.kbd >
< jp.capsctrl.kbd >
< jp.kbd >
< kz.io.kbd >
< kz.kst.kbd >
< latinamerican.acc.kbd >
< latinamerican.kbd >
< lt.kbd >
< nl.kbd >
< no.dvorak.kbd >
< no.kbd >
< nordic.asus-eee.kbd >
< pl.dvorak.kbd >
< pl.kbd >
< pt.acc.kbd >
< pt.kbd >
< ru.kbd >
< ru.shift.kbd >
< ru.win.kbd >
< se.kbd >
< si.kbd >
< sk.kbd >
```

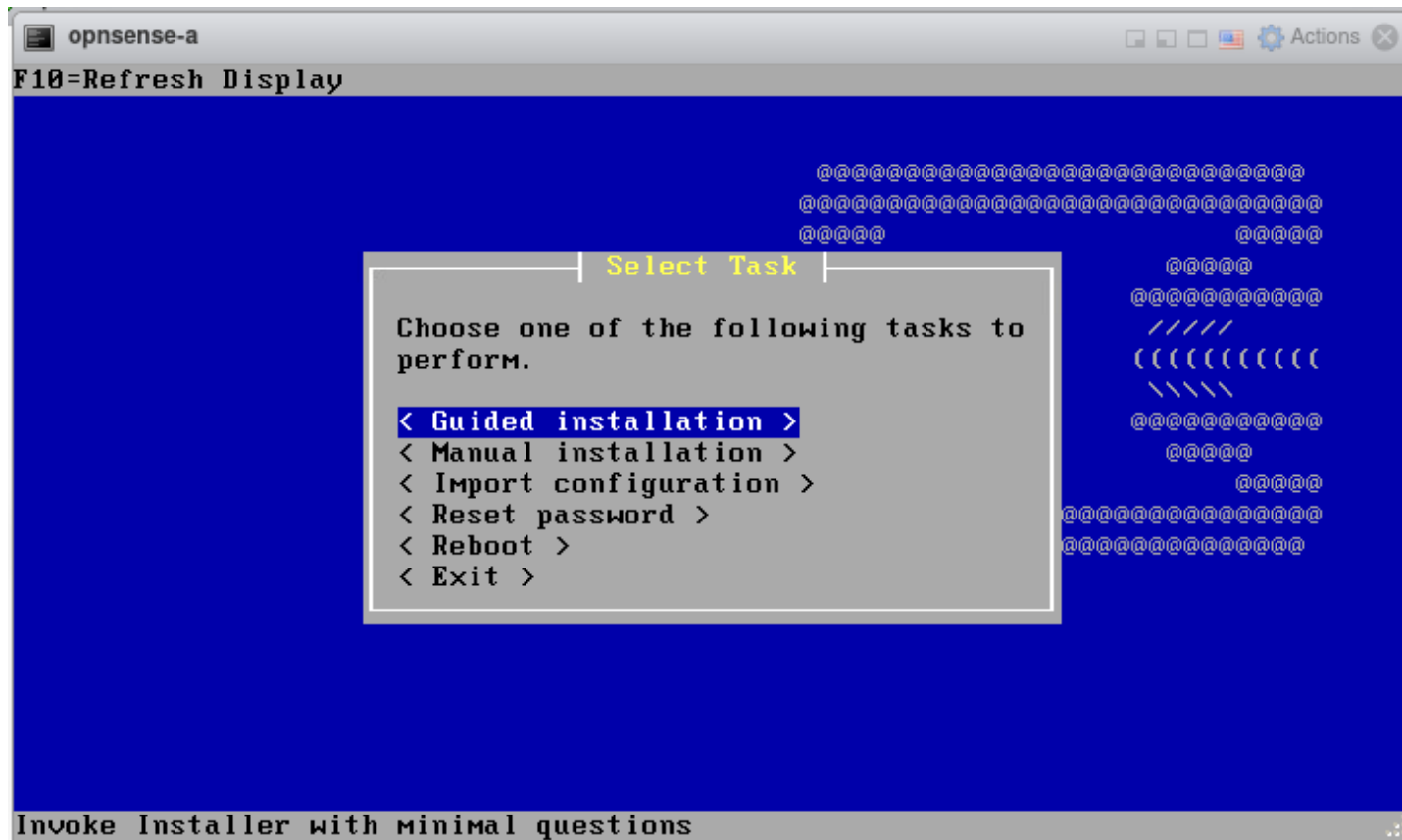
@@@@@@@@@@@@@@@@@  
@@@@@@@@@@@@@@@@@  
@@@@@  
@@@@@  
@@@@@@@@@@@@@  
/////  
((((((((((((((  
\\\\\\\\  
@@@@@@@@@@@@@  
@@@@@  
# @@@@@@  
# @@@@@@@@@@@@@@  
# @@@@@@@@@@@@@@  
#  
#

# OPNsense - instalacja

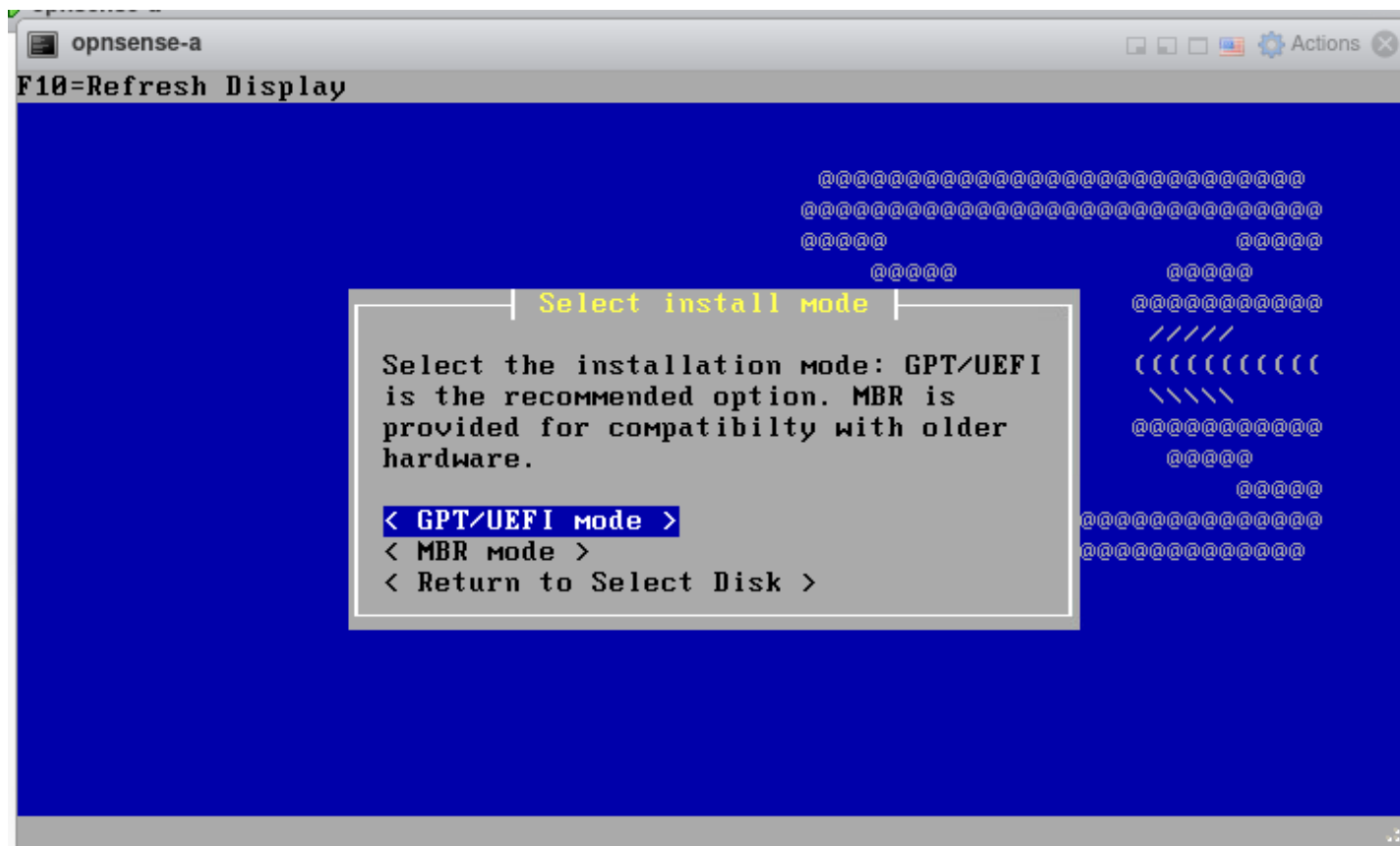




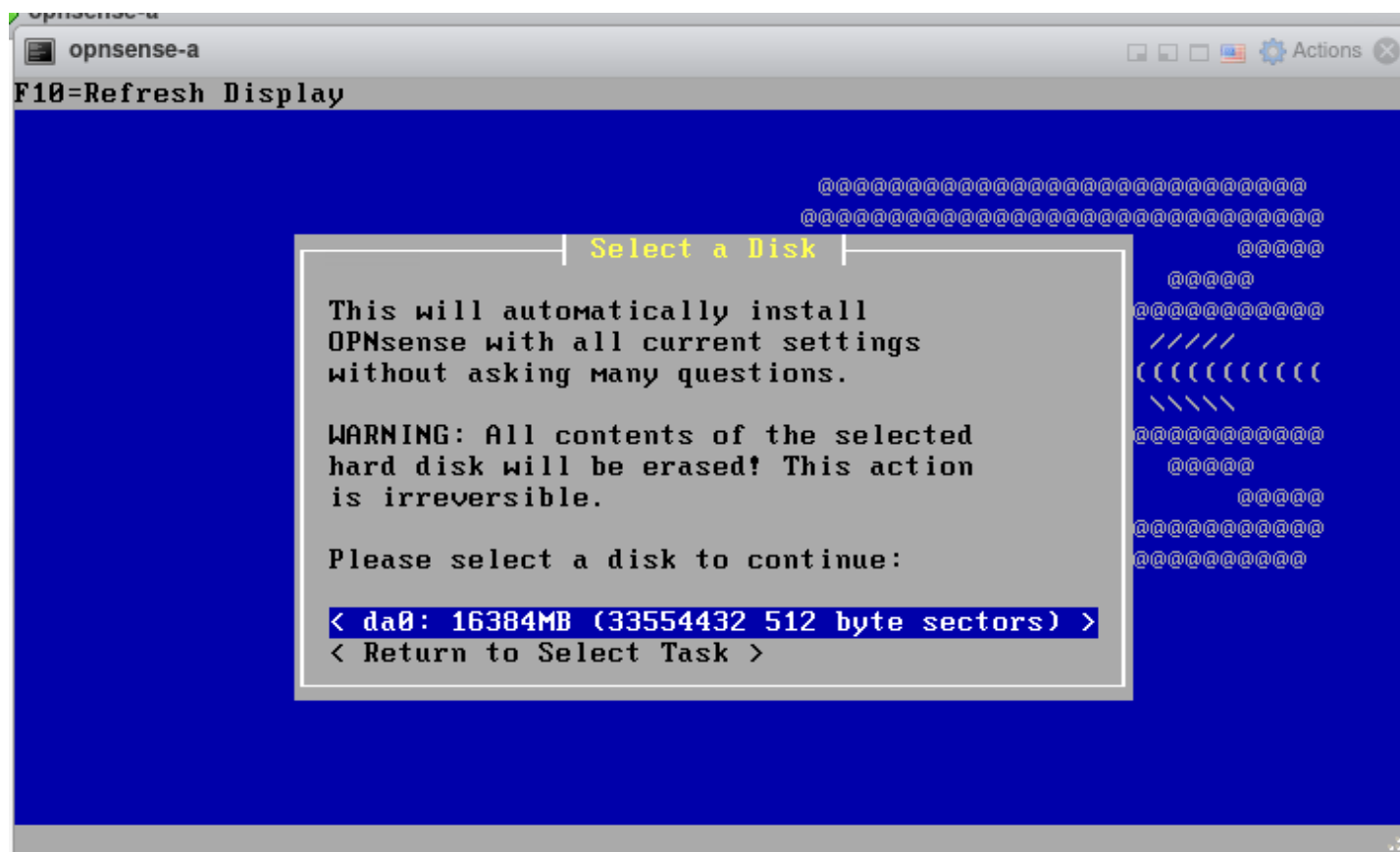
# OPNsense - instalacja



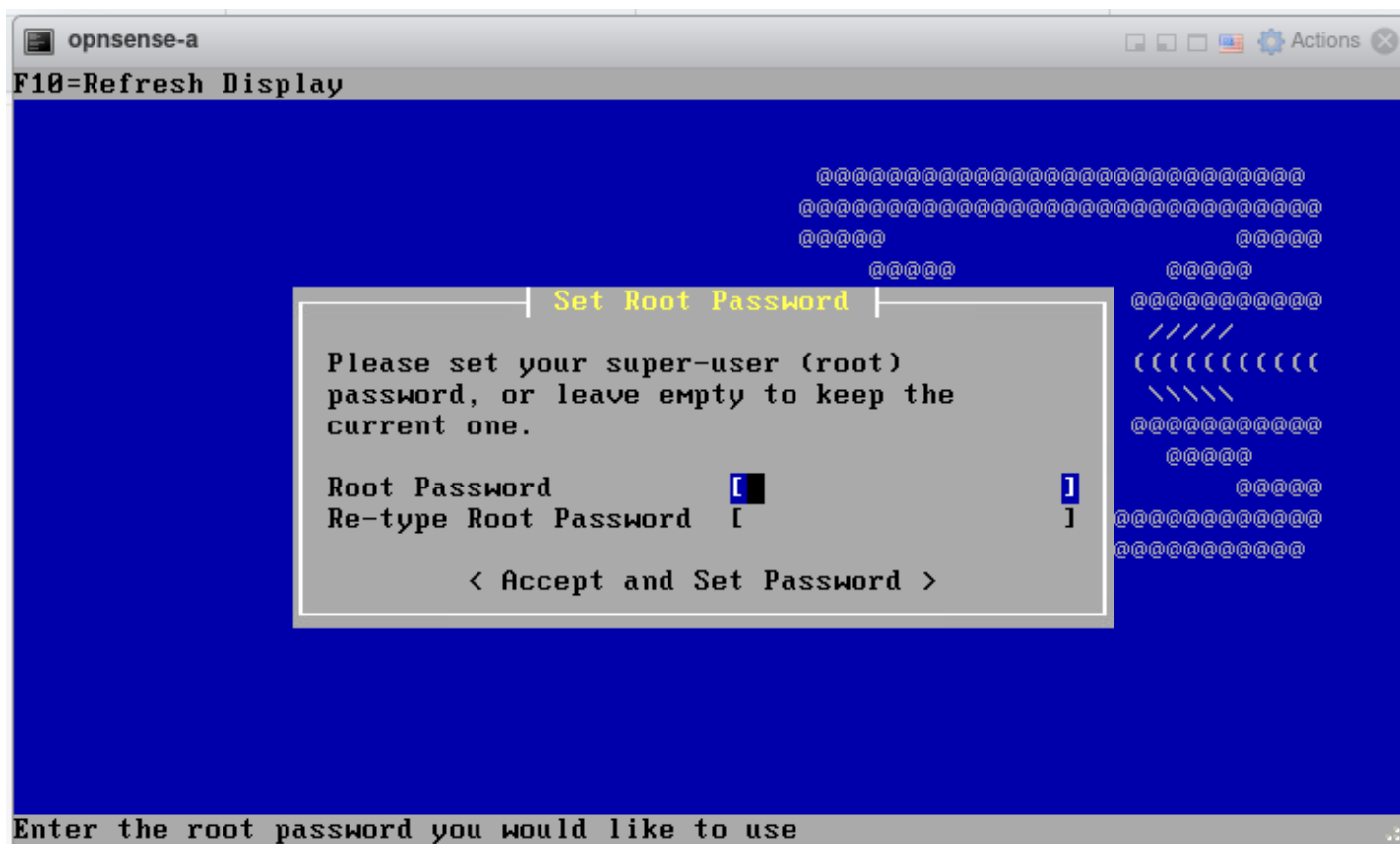
# OPNsense - instalacja



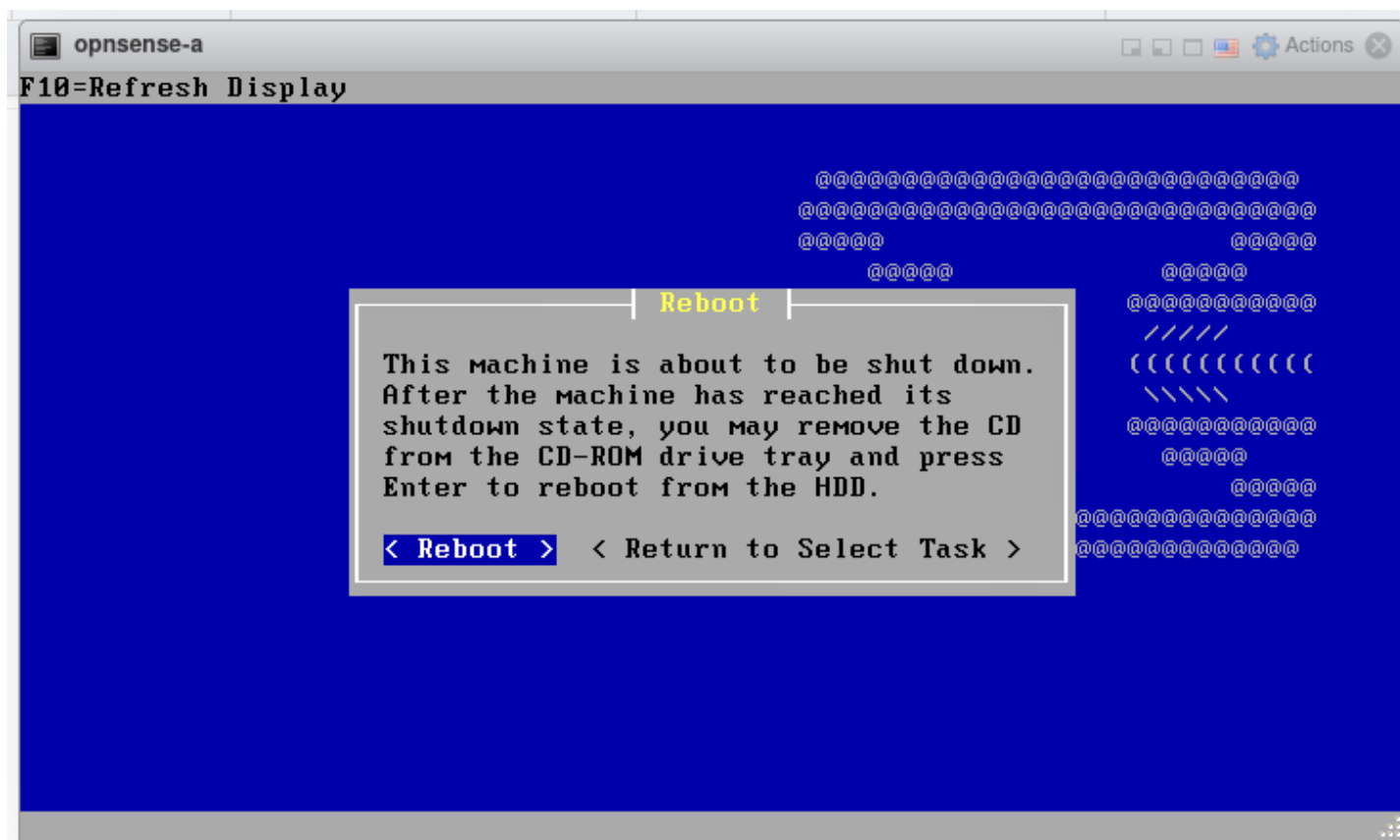
# OPNsense - instalacja



# OPNsense - instalacja



# OPNsense - instalacja



# OPNsense - instalacja

```
opnsense-a
Starting NTP service...deferred.
Starting Unbound DNS...done.
Generating RRD graphs...done.
Configuring system logging...done.
>>> Invoking start script 'newwanip'
Reconfiguring IPv4 on em1: OK
>>> Invoking start script 'freebsd'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Sat Nov 14 14:15:35 UTC 2020

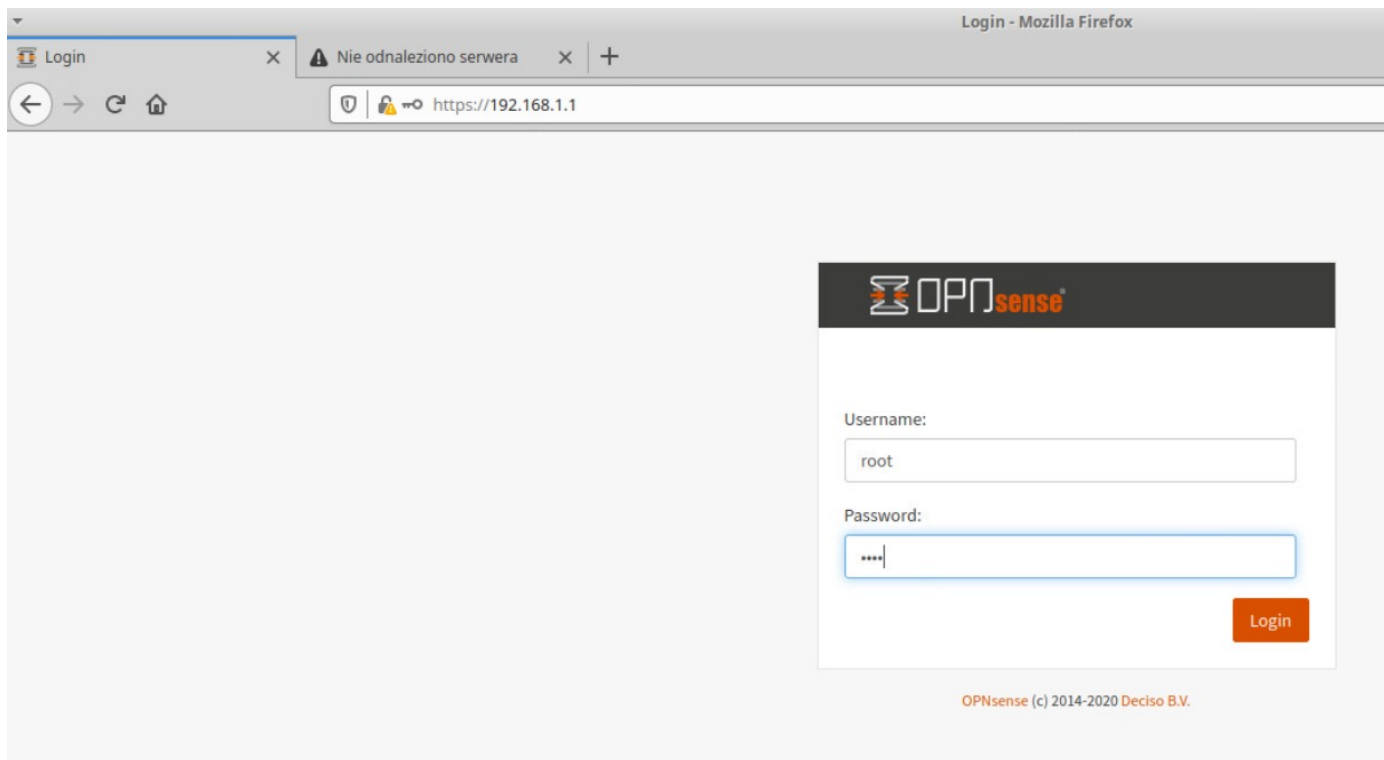
*** OPNsense.localdomain: OPNsense 20.7 (amd64/OpenSSL) ***

LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)     -> v4/DHCP4: 192.168.1.10/24

HTTPS: SHA256 F7 BF FC 12 34 B0 D7 8D 82 6C 6A F0 F6 14 D6 B7
          54 DF 32 7E D2 35 69 B9 26 98 CA 50 F9 AD 3F 41

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █
```

# OPNsense - konfiguracja



# OPNsense - konfiguracja

- DNSy np. 1.1.1.3 1.0.0.3
- wyłącznie nadpisywania DNS przez ustawienia interfejsów WAN
- Interfejs WAN: statyczne IP 192.168.1.1/24, brama 192.168.1.254 (? wpuszczenie ruchu sieci prywatnych)
- Interfejs LAN: statyczne IP 10.123.111.1/24



# Serwery DNS (źródło avlab.pl)

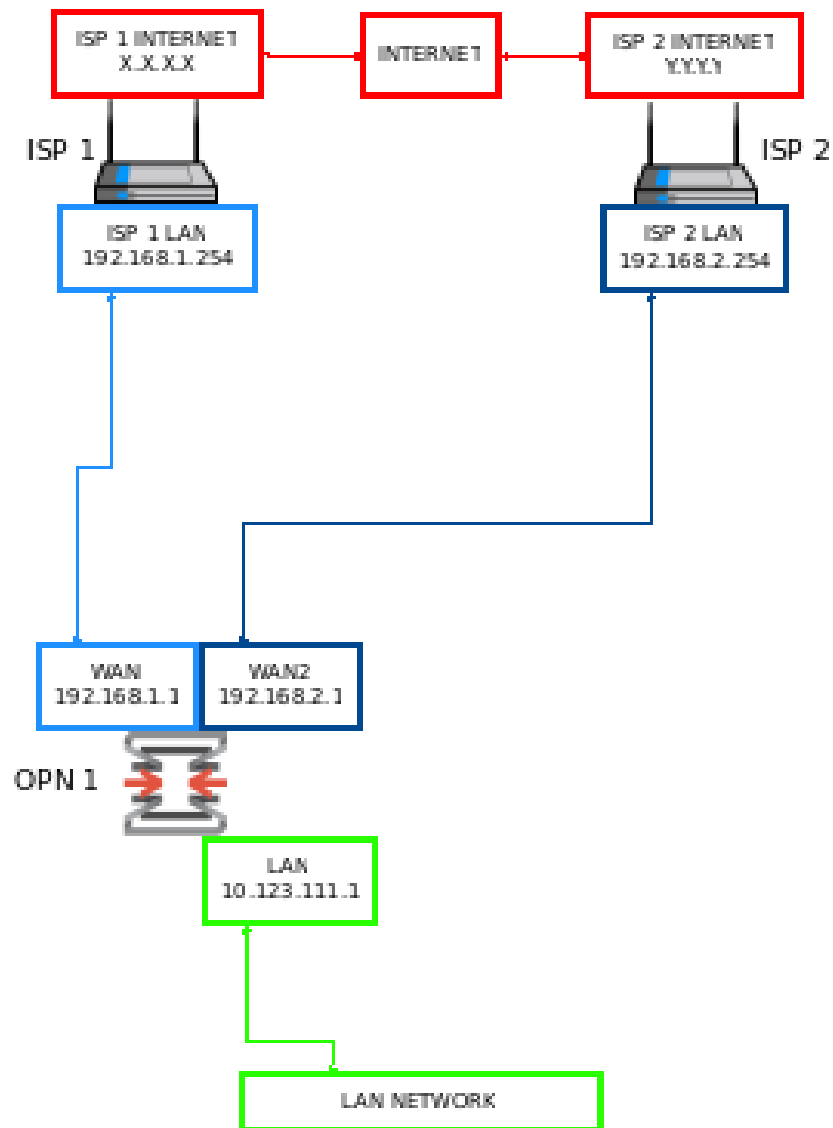
## Porównanie serwerów DNS

Nazwa	Adres	Pochodzenie	Filtrowanie kategorii np. pornografia, reklamy / ochrona przed malware i phishingiem	Wsparcie dla DNS- over-HTTPS (DoH)
Cloudflare	1.1.1.1 oraz 1.1.1.2, 1.0.0.2 (ochrona przed malware), 1.1.1.3, 1.0.0.3 (ochrona przed malware i filtr treści)	USA	NIE / (TAK)	TAK
Google Public DNS	8.8.8.8 i 8.8.4.4	USA	NIE / NIE	TAK
Cisco OpenDNS	208.67.222.222 i 208.67.220.220	USA	TAK / TAK	TAK
Quad9	9.9.9.9	USA	NIE / TAK	TAK
DNS.Watch	84.200.69.80 i 84.200.70.40	Niemcy	NIE / NIE	NIE
OpenNIC	192.71.245.208, 195.10.195.195, 176.126.70.119 i 91.217.137.37	USA	NIE / NIE	NIE
Comodo Secure DNS	8.26.56.26 i 8.20.247.20	USA	NIE / TAK	NIE
VeriSign Public DNS	64.6.64.6 i 64.6.65.6	USA	NIE / NIE	NIE
CleanBrowsing	185.228.168.168 i 185.228.169.168	USA	TAK / NIE	TAK
Alternate DNS	23.253.163.53 i 198.101.242.72	USA	TAK / NIE	NIE
AdGuard DNS	176.103.130.130 i 176.103.130.131	USA	TAK / TAK	TAK

# OPNsense - konfiguracja

```
user@xubuntu2:~$ traceroute wp.pl
traceroute to wp.pl (212.77.98.9), 30 hops max, 60 byte packets
 1  opn-a.test.lan (10.123.111.1)  0.328 ms  0.259 ms  0.218 ms
 2  192.168.1.254 (192.168.1.254)  0.731 ms  0.996 ms  0.907 ms
 3  10.44.44.1 (10.44.44.1)  1.192 ms  1.115 ms  1.078 ms
 4  195.187.156.227 (195.187.156.227)  5.302 ms  5.265 ms  5.060 ms
 5  195.187.156.1 (195.187.156.1)  5.446 ms  5.324 ms  5.156 ms
 6  212.127.88.106 (212.127.88.106)  5.606 ms  2.920 ms  3.001 ms
 7  * * *
 8  * * *
 9  *^C
user@xubuntu2:~$
```

# Dual WAN



# Dual WAN

- Ustawić monitor IP na pierwszej bramie, np. 8.8.8.8 – włączyć monitorowanie
- Przypisać drugi interfejs WAN
- Uruchomić interfejs z IP statycznym 192.168.2.2/24 dodając bramę multi WAN 192.168.2.254 (zastosować zmiany)
- Ustawić monitor IP na drugiej bramie, np. 1.1.1.1 (zastosować zmiany)
- Dodać grupę bram składającą się z obu bram z ważnością 1. i 2. przełączaną przez brak łączności lub duże opóźnienie (zastosować zmiany)
- Wyedytować regułę na interfejsie LAN kierując ruch wychodzący na grupę WAN (zastosować zmiany)
- Dodać regułę kierującą ruch do naszego firewalla na domyślną bramę

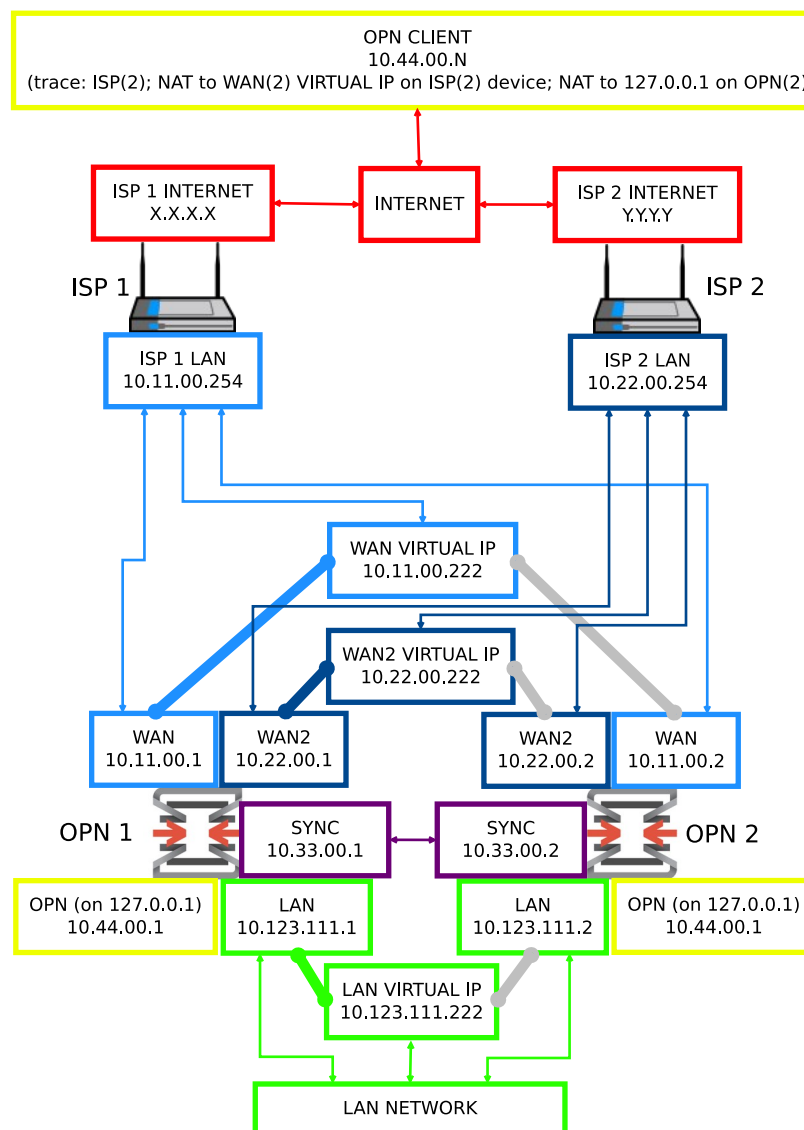
# Dual WAN

Name	Interface	Protocol	Priority	Gateway	Monitor IP	RTT	RTTd	Loss	Status	Description
<input type="checkbox"/> WAN_GW	WAN	IPv4	255 (upstream)	192.168.1.254	8.8.8.8	5.1 ms	2.1 ms	56.0 %	Offline	WAN Gateway
<input checked="" type="checkbox"/> WAN_DHCP6 (active)	WAN	IPv6	254			~	~	~	Online	Interface WAN_DHCP6 Gateway
<input checked="" type="checkbox"/> WANB_GWv4 (active)	WANB	IPv4	255	192.168.2.254	1.1.1.1	5.4 ms	1.9 ms	0.0 %	Online	

```
Terminal - user@xubuntu2:~
Plik Edycja Widok Terminal Karty Pomoc
user@xubuntu2:~$ traceroute wp.pl
traceroute to wp.pl (212.77.98.9), 30 hops max, 60 byte packets
 1  opn-a.test.lan (10.123.111.1)  0.266 ms  0.206 ms  0.191 ms
 2  192.168.1.254 (192.168.1.254)  0.883 ms  0.770 ms  0.703 ms
 3  10.44.44.1 (10.44.44.1)  1.014 ms  0.956 ms  0.886 ms
 4  195.187.156.227 (195.187.156.227)  2.393 ms  2.327 ms  2.290 ms
 5  195.187.156.1 (195.187.156.1)  2.256 ms  2.339 ms  2.277 ms
^C
user@xubuntu2:~$ traceroute wp.pl
traceroute to wp.pl (212.77.98.9), 30 hops max, 60 byte packets
 1  opn-a.test.lan (10.123.111.1)  0.321 ms  0.257 ms  0.263 ms
 2  192.168.2.254 (192.168.2.254)  1.069 ms  1.502 ms  1.427 ms
 3  10.44.44.1 (10.44.44.1)  3.093 ms  3.153 ms  3.060 ms
 4  195.187.156.227 (195.187.156.227)  2.966 ms  2.941 ms  3.116 ms
 5  195.187.156.1 (195.187.156.1)  3.239 ms  3.179 ms  3.065 ms
^C
user@xubuntu2:~$
```

```
Terminal - user@xubuntu2:~
Plik Edycja Widok Terminal Karty Pomoc
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=164 ttl=57 time=3.62 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=165 ttl=57 time=4.39 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=166 ttl=57 time=4.01 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=167 ttl=57 time=4.25 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=168 ttl=57 time=4.26 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=169 ttl=57 time=6.11 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=170 ttl=57 time=5.20 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=171 ttl=57 time=4.30 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=172 ttl=57 time=4.53 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=173 ttl=57 time=5.14 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=174 ttl=57 time=4.53 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=175 ttl=57 time=6.06 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=176 ttl=57 time=5.07 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=177 ttl=57 time=4.66 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=178 ttl=57 time=3.84 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=179 ttl=57 time=5.40 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=180 ttl=57 time=3.91 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=181 ttl=57 time=3.96 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=182 ttl=57 time=4.26 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=183 ttl=57 time=3.48 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=184 ttl=57 time=4.52 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=185 ttl=57 time=4.29 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=186 ttl=57 time=4.03 ms
```

# Co by tu skomplikować?





**Dziękuję za uwagę**