Zastosowania wirtualizacji na przykładzie instalacji zapór sieciowych

Dominik Przybysz

Wirtualizacja - rodzaje

Cel – uruchomienie wielu wydajanych 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-vmware-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

vmware ESXi

- 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

vmware ESXi

- wysokie wymagania sprzętowe

- zdarzają się kompilacje przy instalacji

* jest wyspecjalizowanym systemem operacyjnym o wąskiej funkcjonalności (typ 1)

+ łatwy w konfiguracji

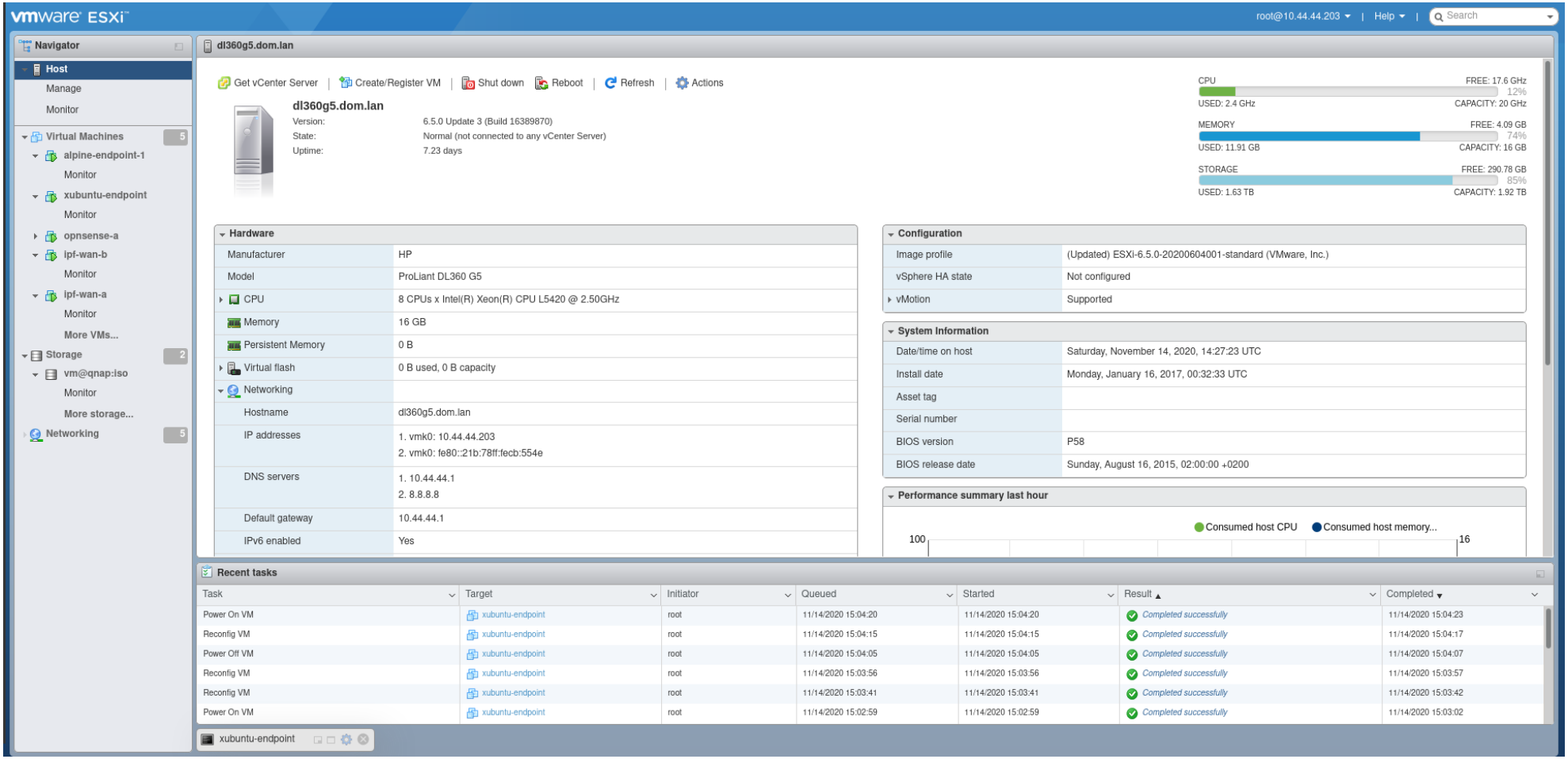
+ ergonomiczne administrowanie siecią

+ podstawowe funkcjonalności bezpłatne

* interfejs webowy / api

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

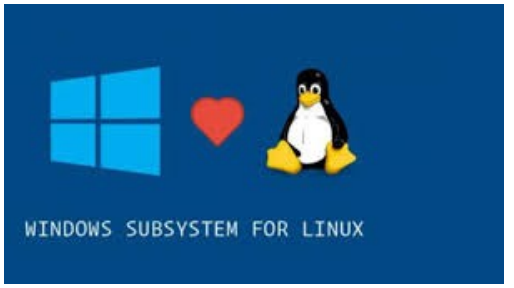
Interfejs VMware ESXi 6.5



Wirtualizacja – inne rozwiązania

Microsoft Hyper-V

VMware Player



Linux KVM

PROXMOX

LXC

docker

QEMU

Firewall - znaczenia

- Usługa / Program filtrujący pakiety

  UFW **FirewallD** **iptables** **Windows Firewall** **...**

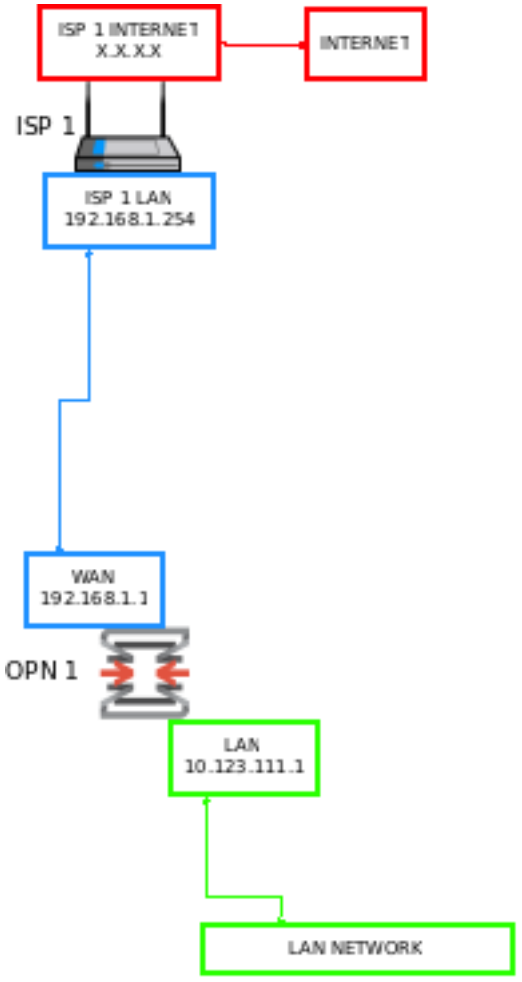
- Urządzenie sprzętowe filtrujące pakiety

- Serwer z oprogramowaniem filtrującym pakiety

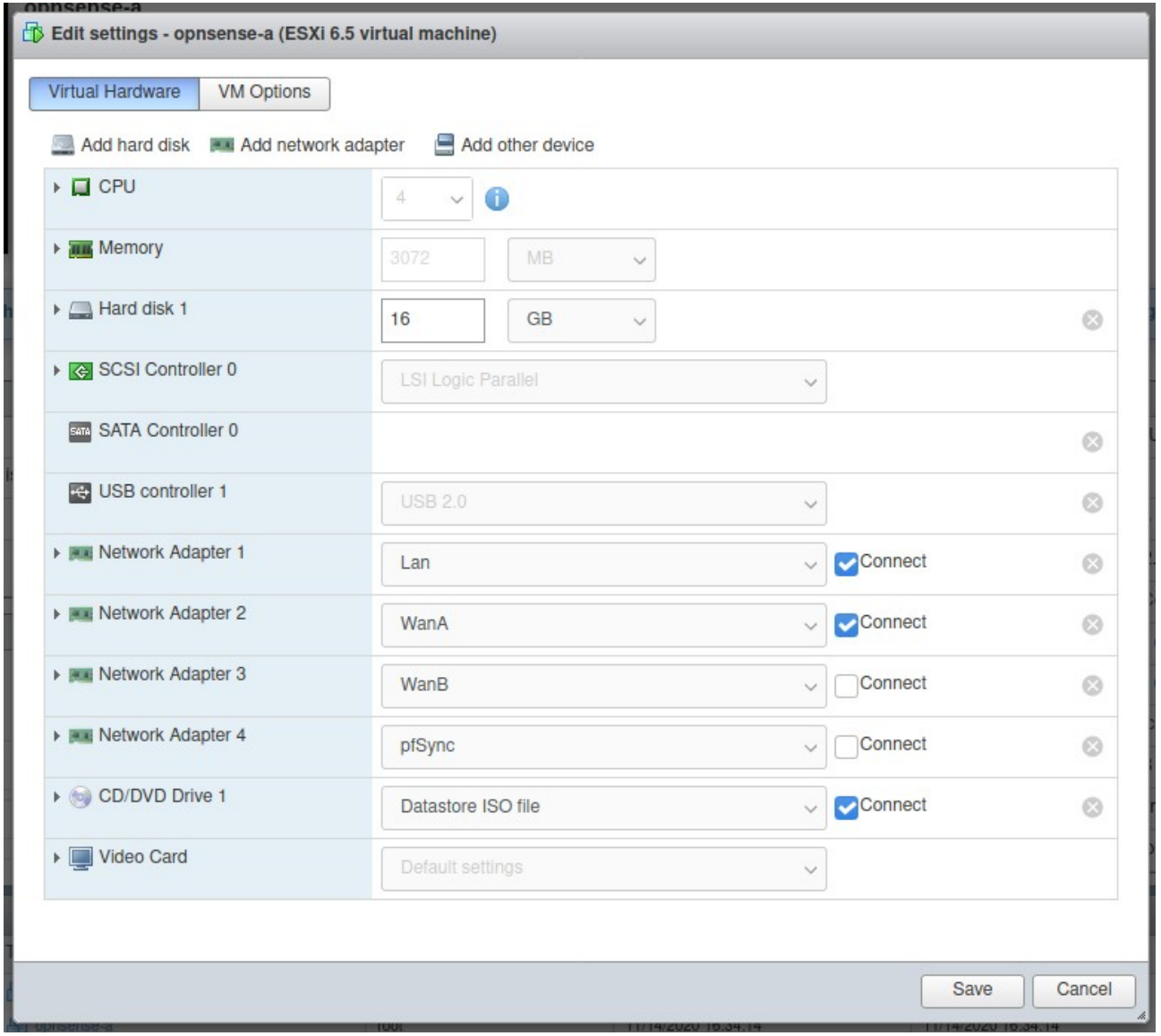
pfsense → OPNsense® Your next open source firewall

OpenWrt Wireless Freedom

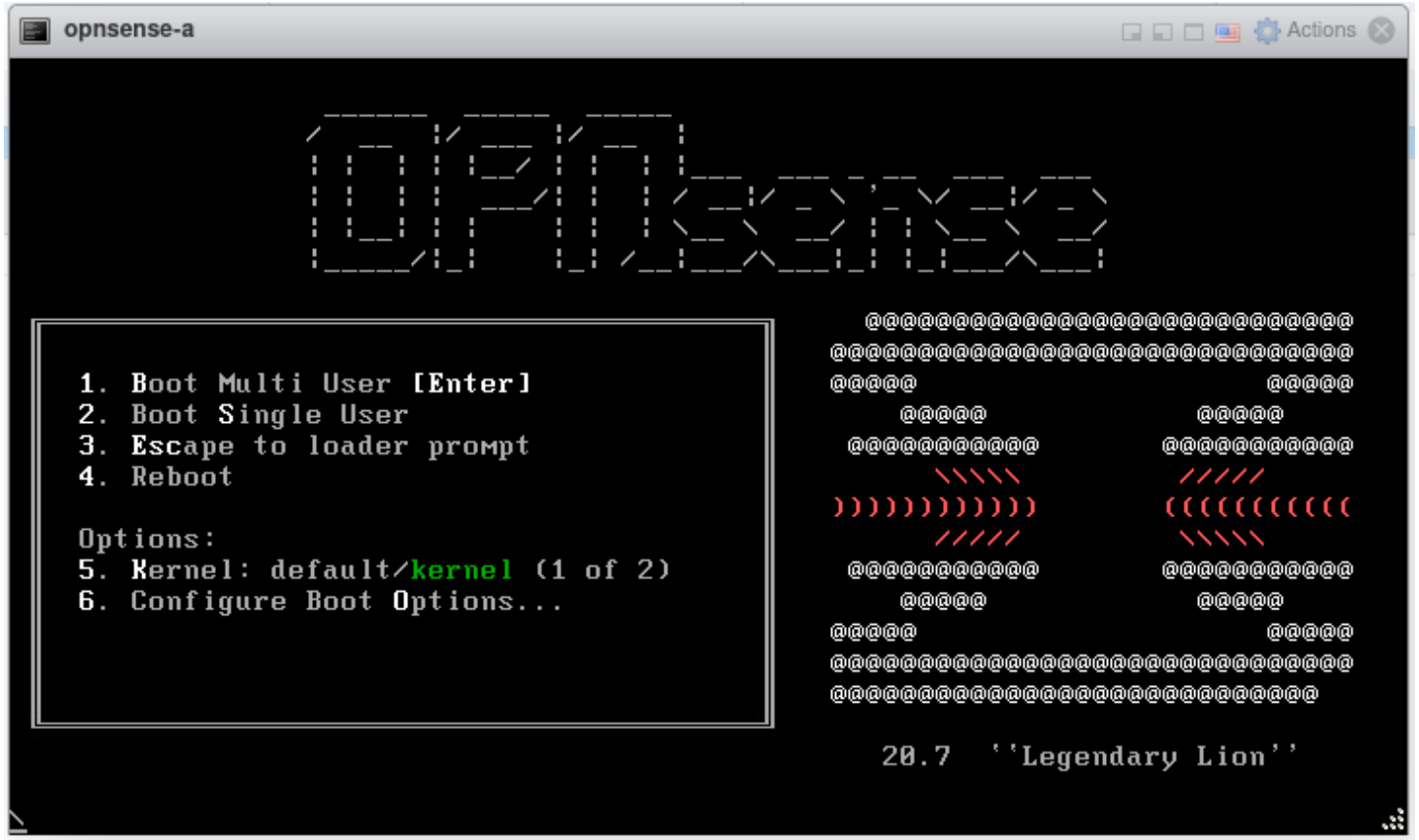
OPNsense - konfiguracja



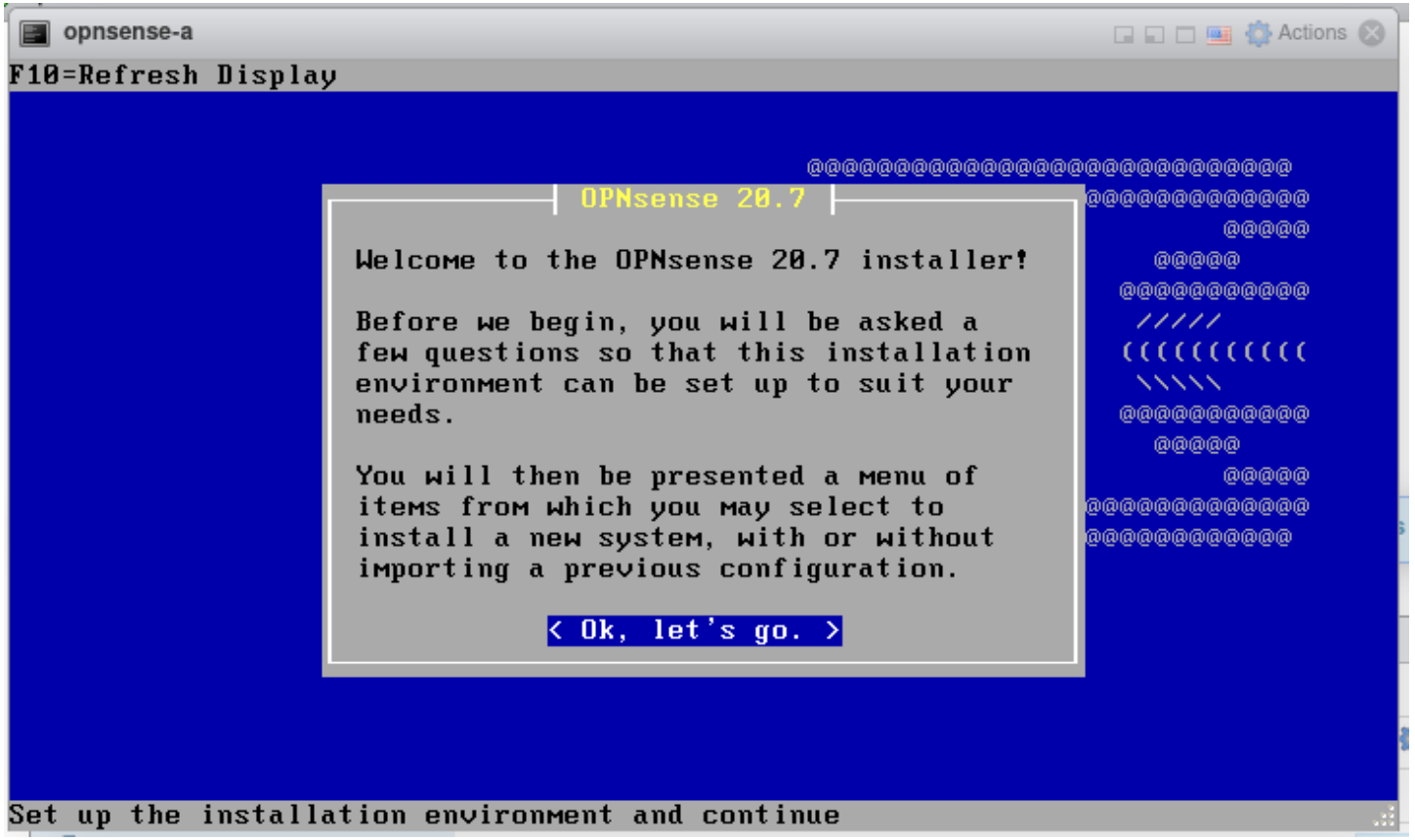
OPNsense - instalacja



OPNsense - instalacja

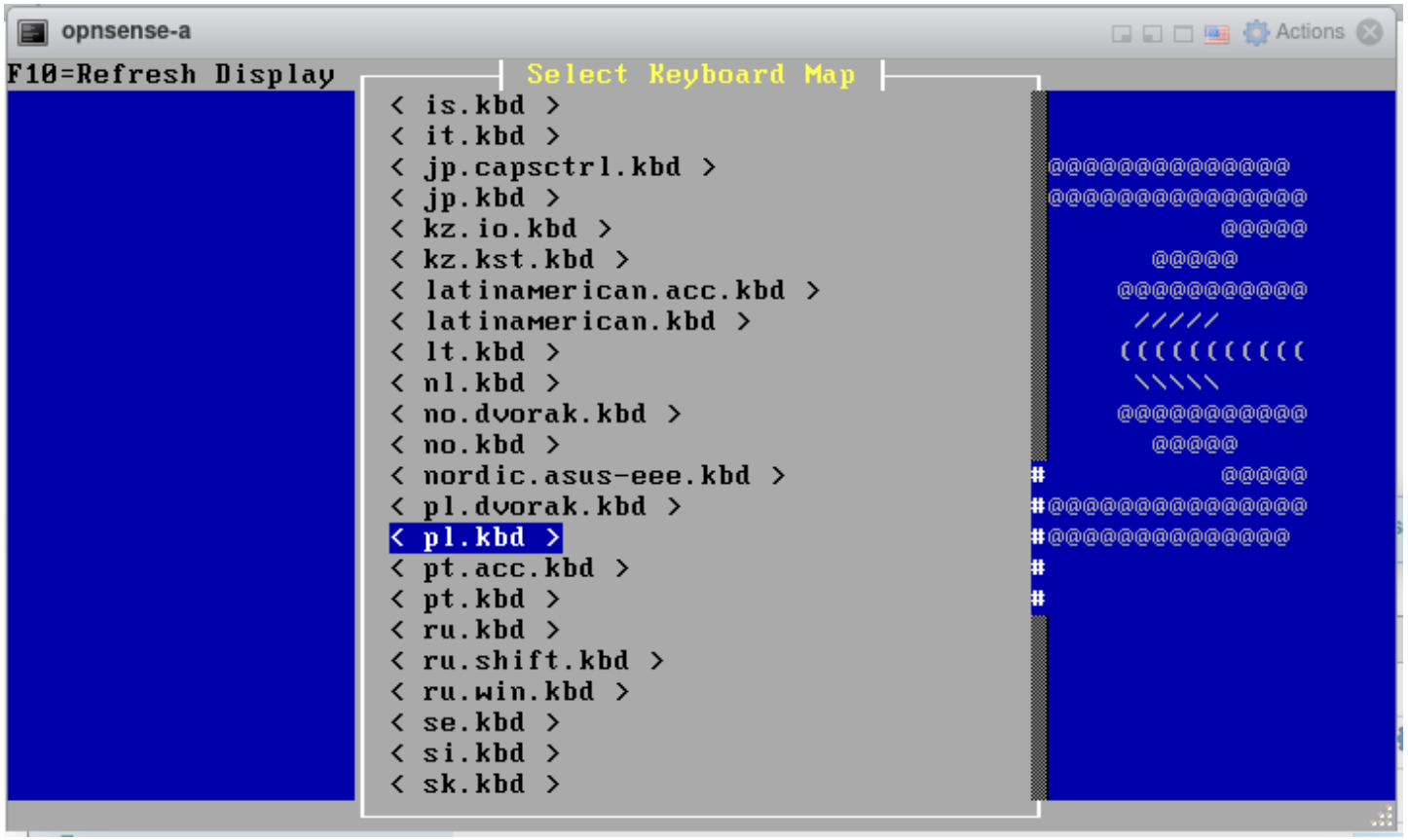


OPNsense - instalacja

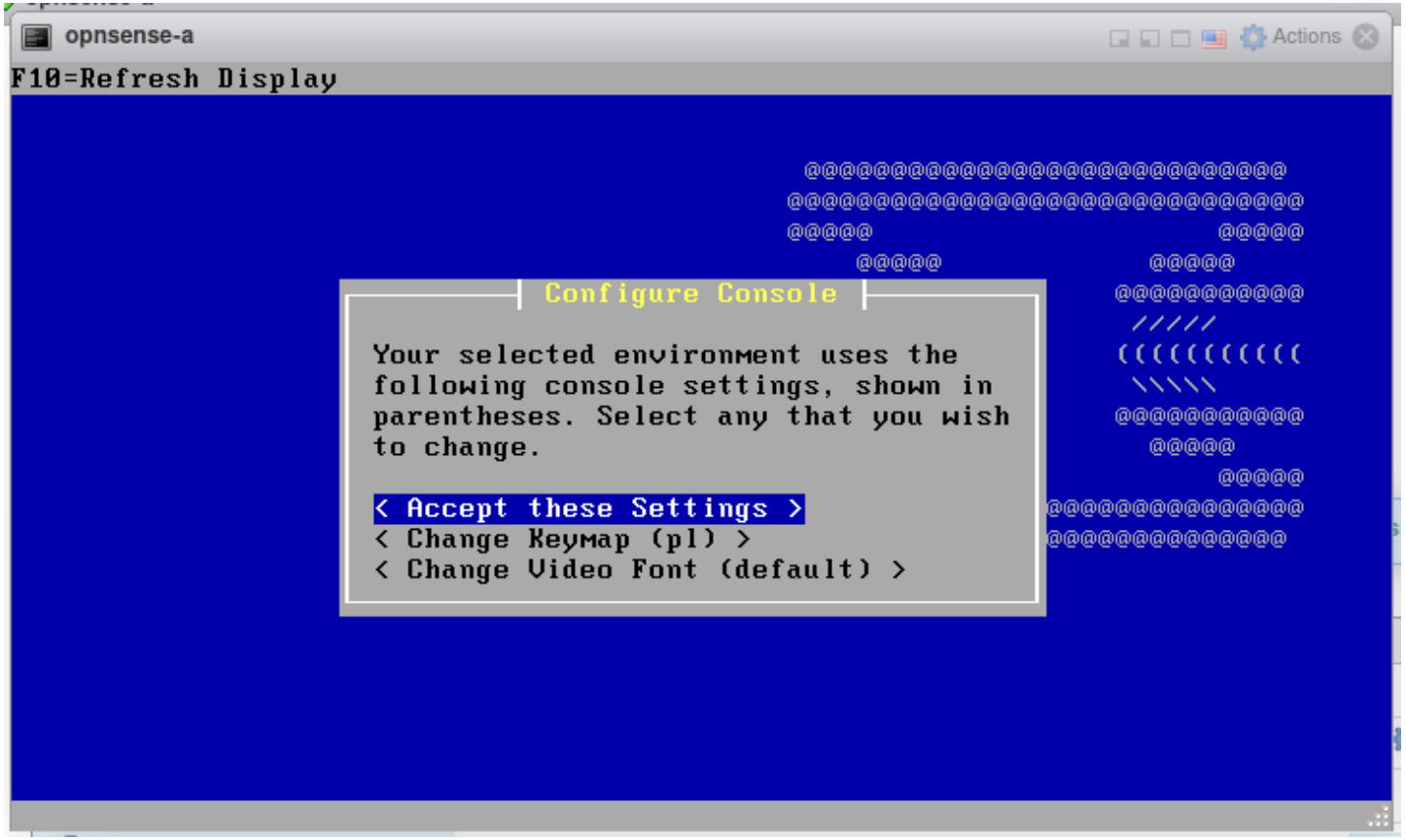


OPNsense - instalacja

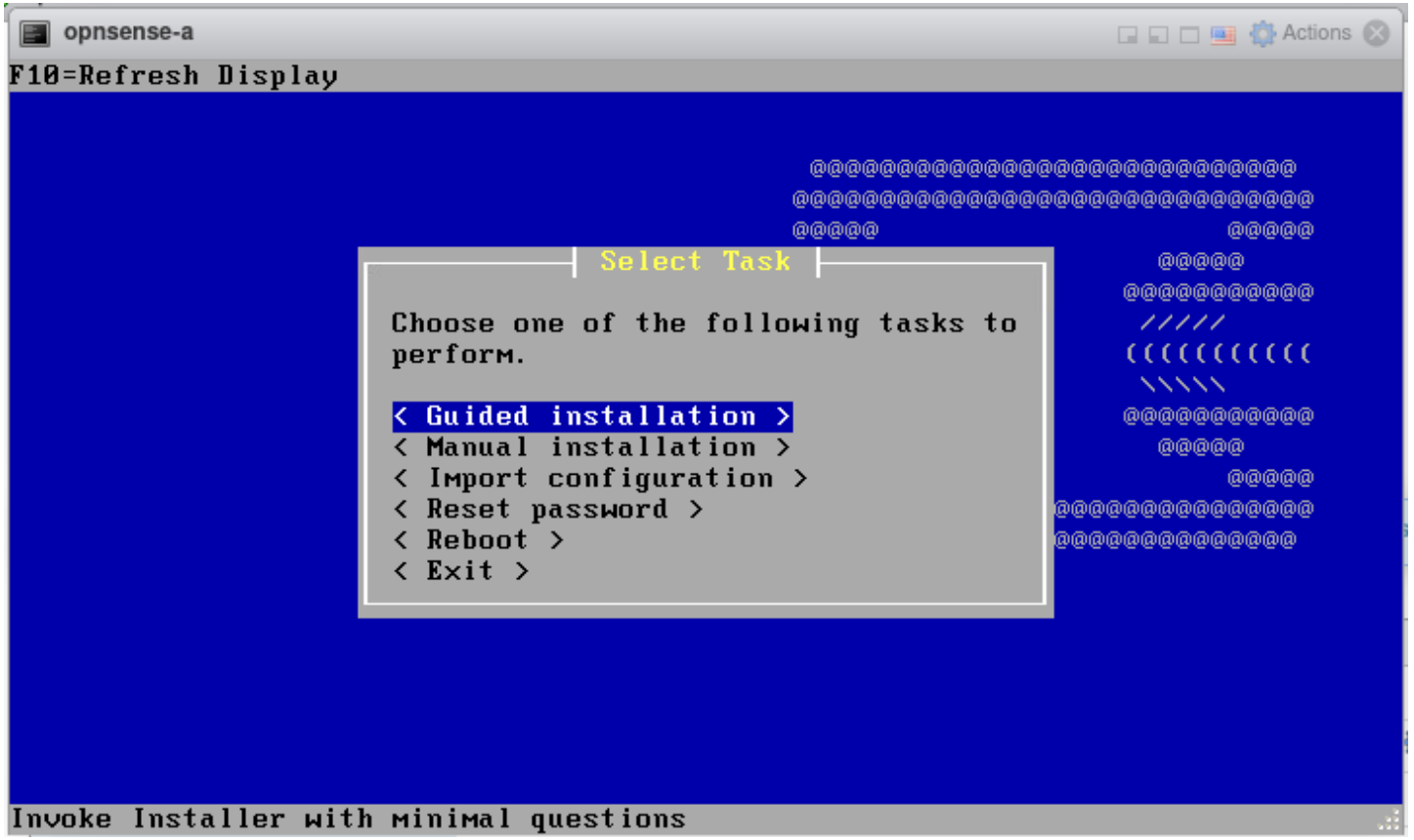
OPNsense - instalacja



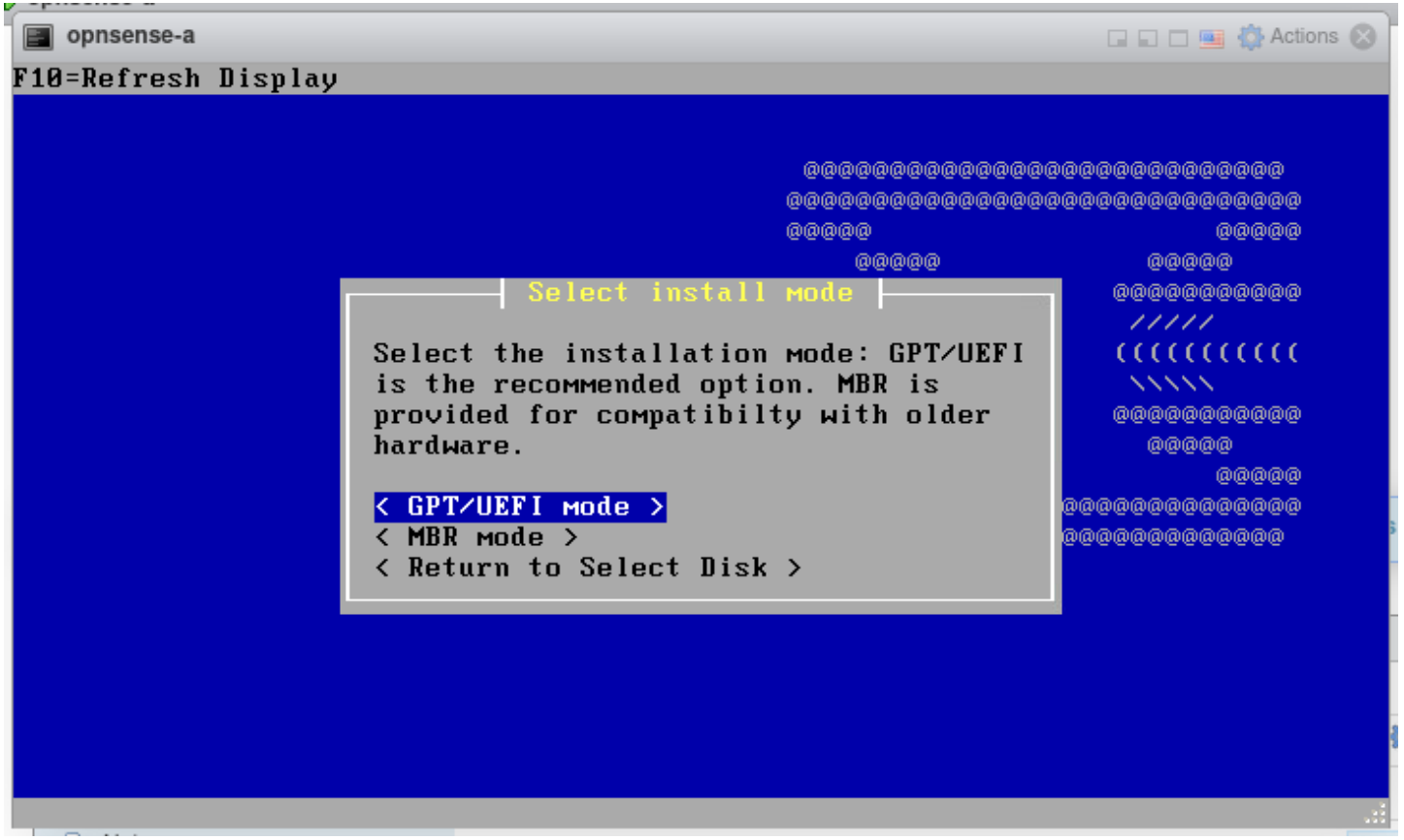
OPNsense - instalacja



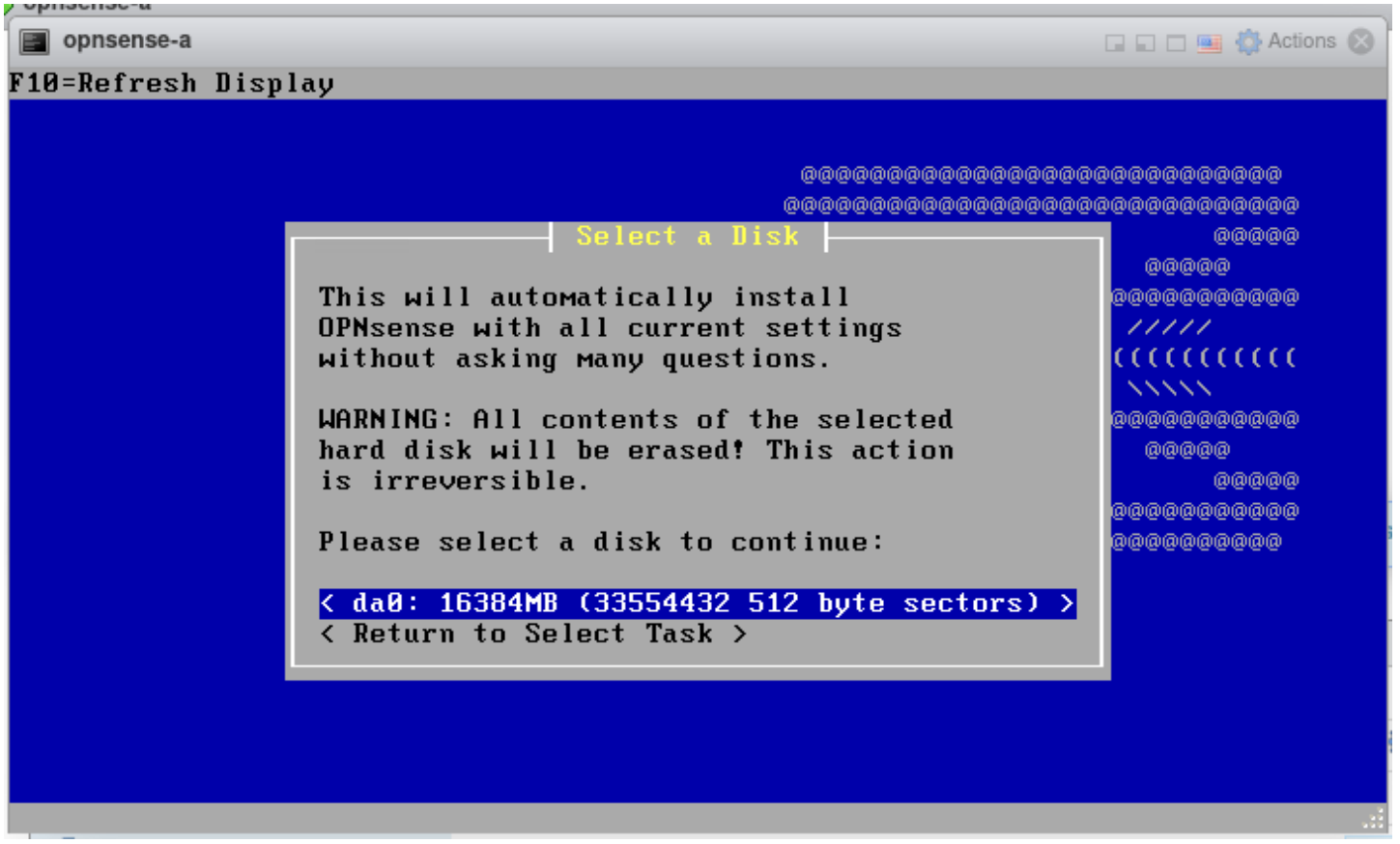
OPNsense - instalacja



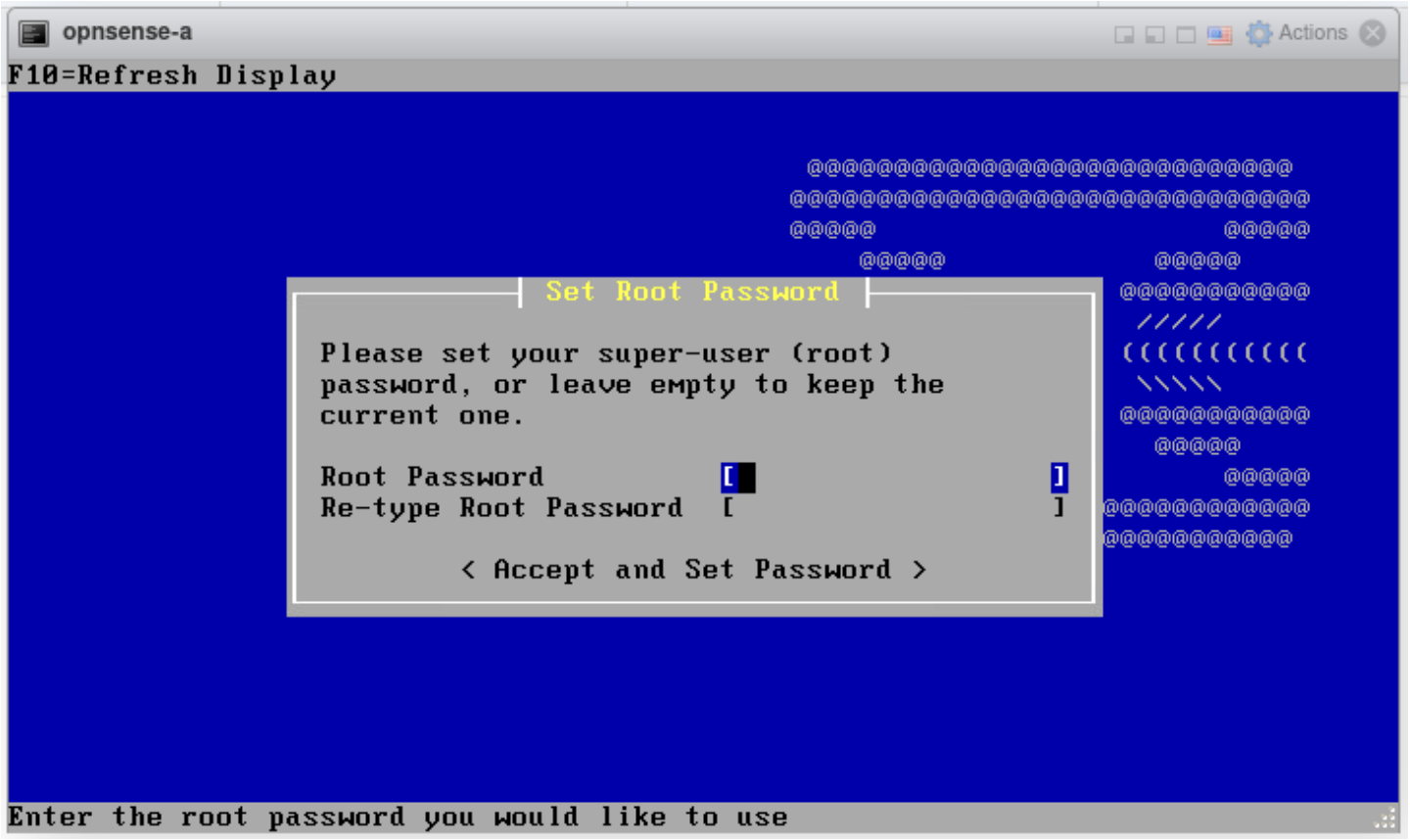
OPNsense - instalacja



OPNsense - instalacja

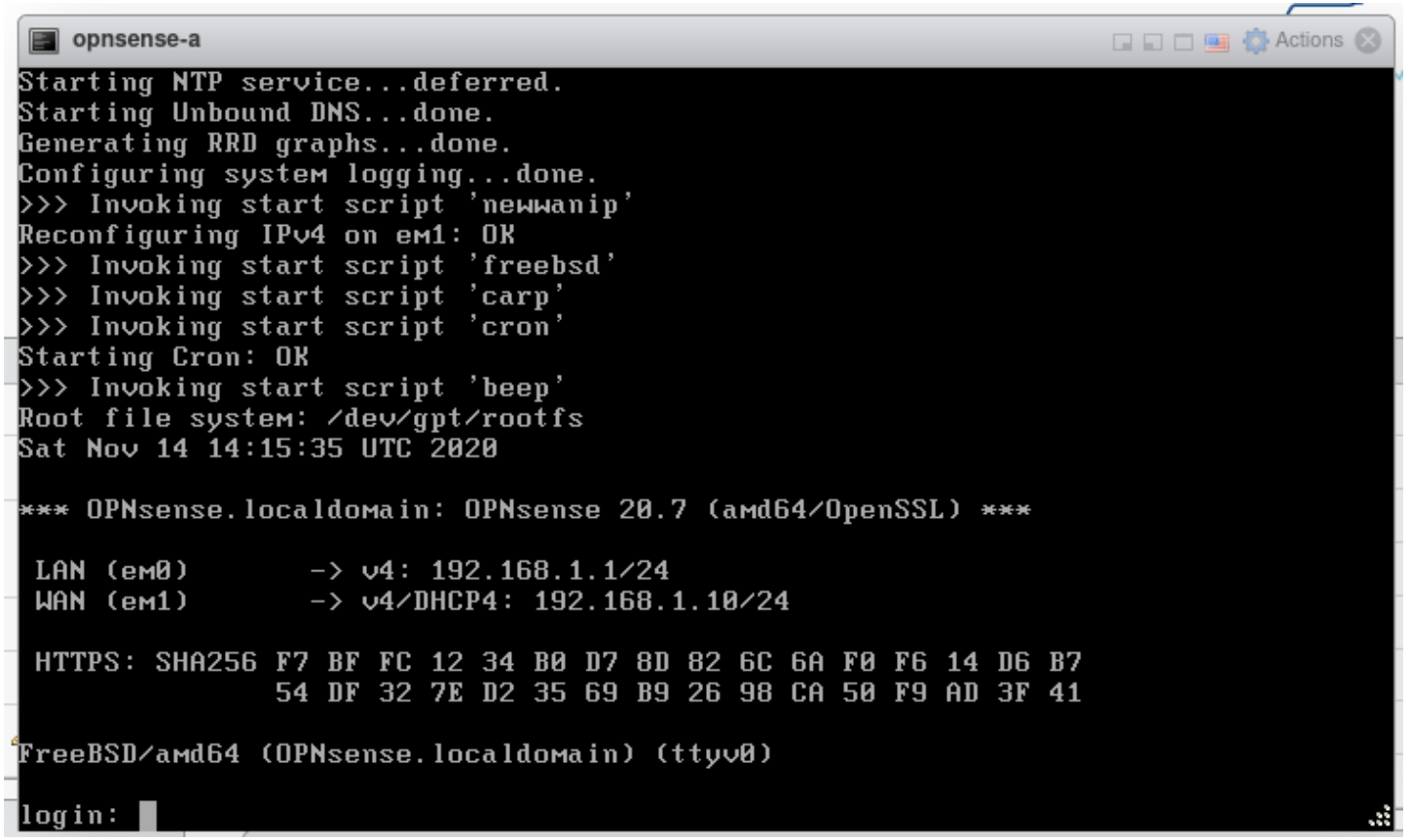


OPNsense - instalacja

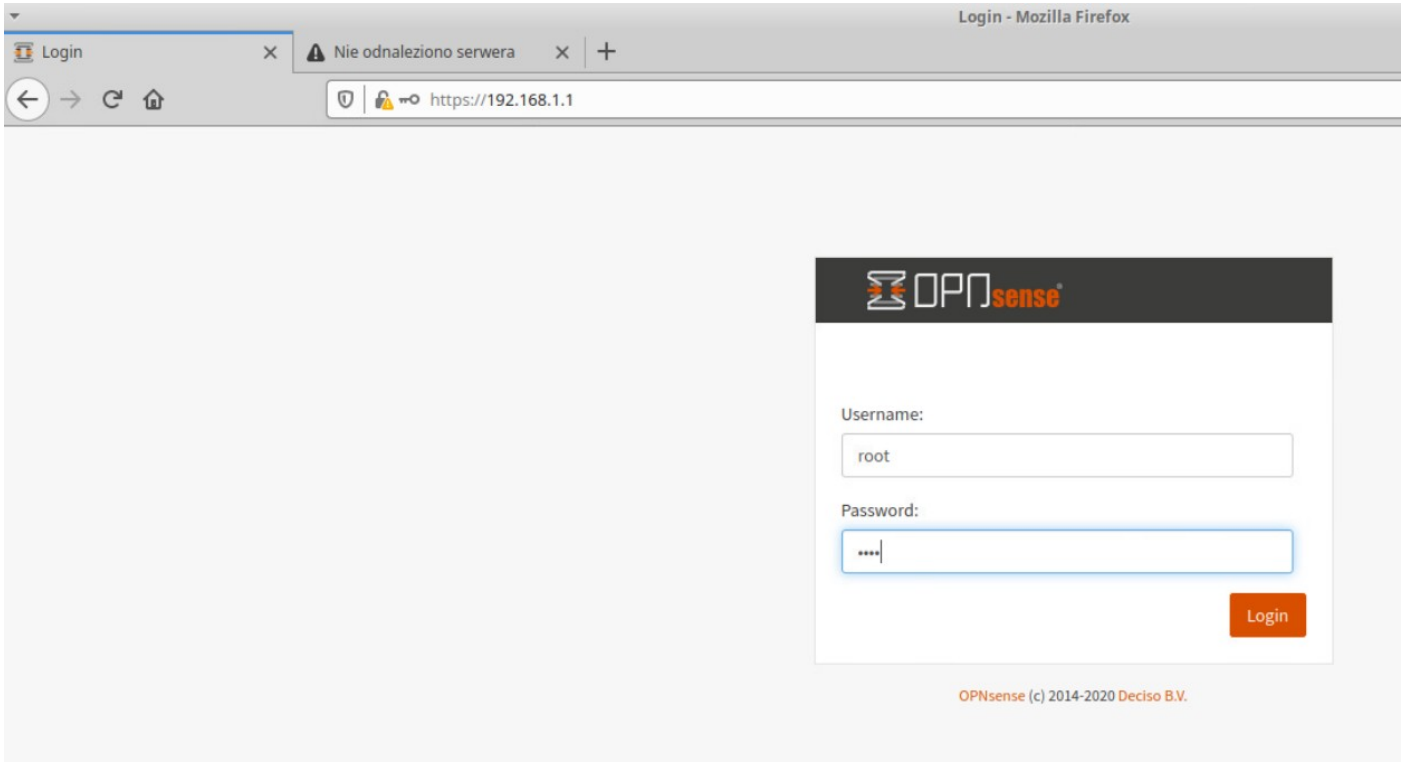


OPNsense - instalacja

OPNsense - instalacja



OPNsense - konfiguracja



OPNsense - konfiguracja

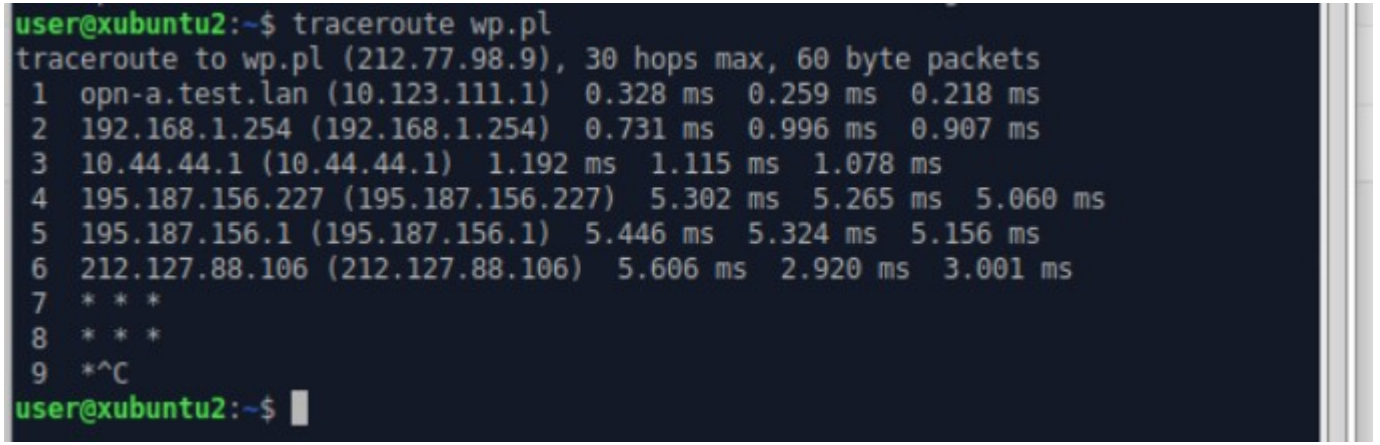
- DNSy np. 1.1.1.3 1.0.0.3
- wyłącznie nadpisywania DNS przez ustawienia interfejsów WAN
- Interfejs WAN: statyczne IP 192.168.1.1/24, brama 192.168.1.254 (? wpuszczenie ruchu sieci prywatnych)
- Interfejs LAN: statyczne IP 10.123.111.1/24

Serwery DNS (źródło avlab.pl)

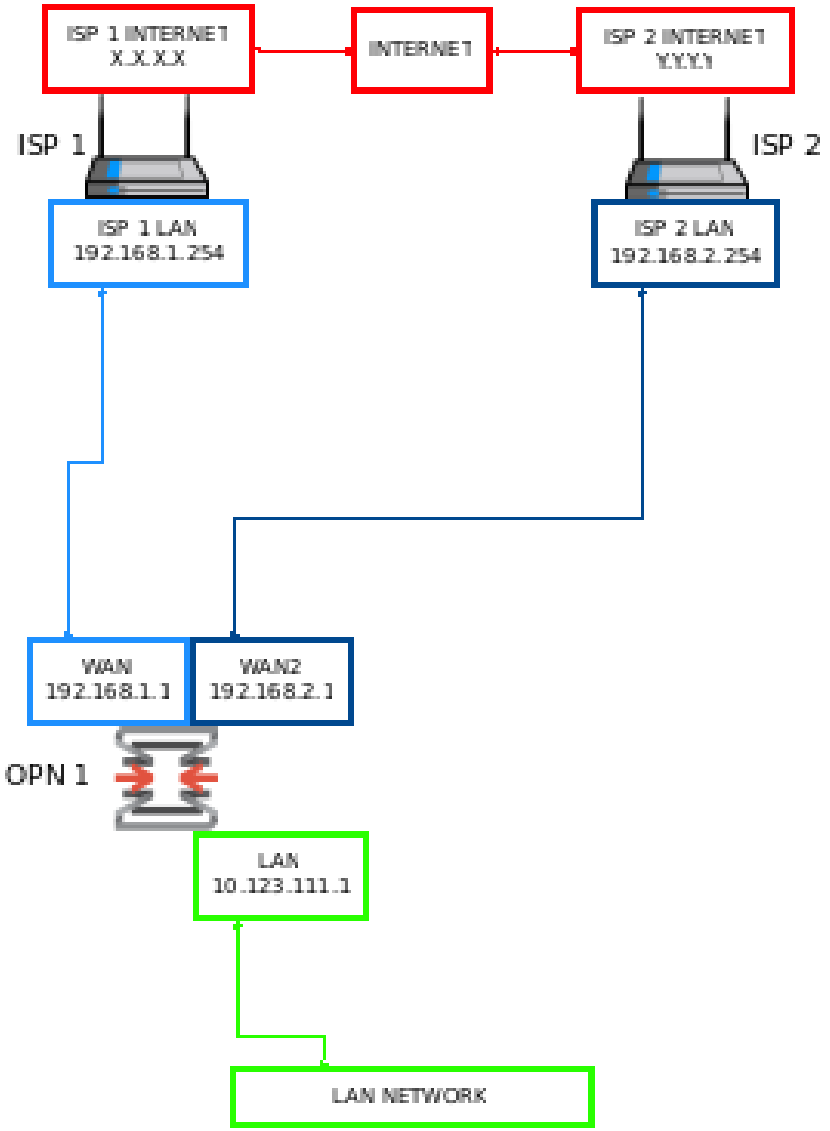
Porównanie serwerów DNS

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



Dual WAN

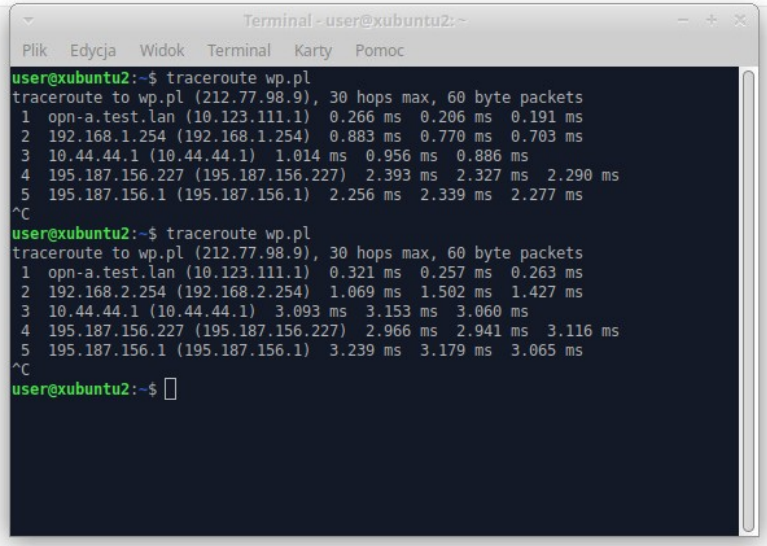

ISP 1 INTERNET
X.X.X.X
INTERNET
ISP 2 INTERNET
Y.Y.Y.Y
ISP 1
ISP 2
ISP 1 LAN
192.168.1.254
ISP 2 LAN
192.168.2.254
WAN
192.168.1.1
WAN2
192.168.2.1
OPN 1
LAN
10.123.111.1
LAN NETWORK

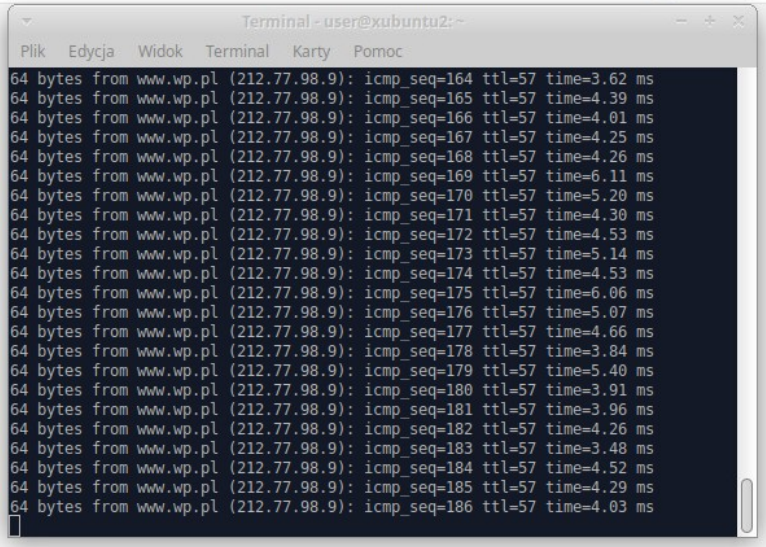
Dual WAN

- 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

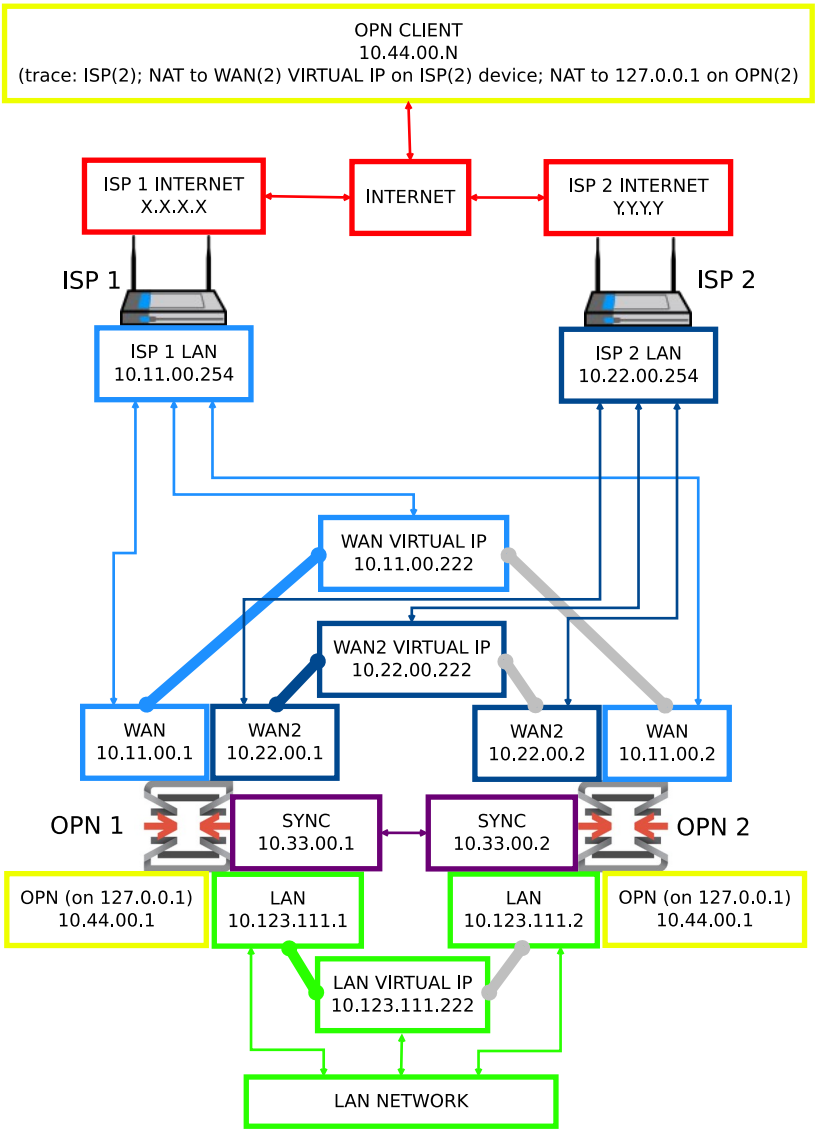
Dual WAN

	Name	Interface	Protocol	Priority	Gateway	Monitor IP	RTT	RTTd	Loss	Status	Description
☐	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
	WAN_DHCP6 **(active)**	WAN	IPv6	254			~	~	~	Online	Interface WAN_DHCP6 Gateway
☐	WANB_GWv4 **(active)**	WANB	IPv4	255	192.168.2.254	1.1.1.1	5.4 ms	1.9 ms	0.0 %	Online	





Co by tu skomplikować?



Dziękuję za uwagę