

Pojekt Home-Lab

Spis treści

1. Cel projektu	2
2. Architektura Sieciowa	3
2.1 Szczegółowy opis architektury	4
3. Główne komponenty laboratorium	5
4. Etapy realizacji projektu	6
4.1. Instalacja oraz konfiguracja hypervisora (Proxmox)	6
4.2. Instalacja oraz konfiguracja zapory pfSense	9

Autor: Kamil Iskra
Rzeszów, 16.06.2025r.
Ver. 1.0

1. Cel projektu

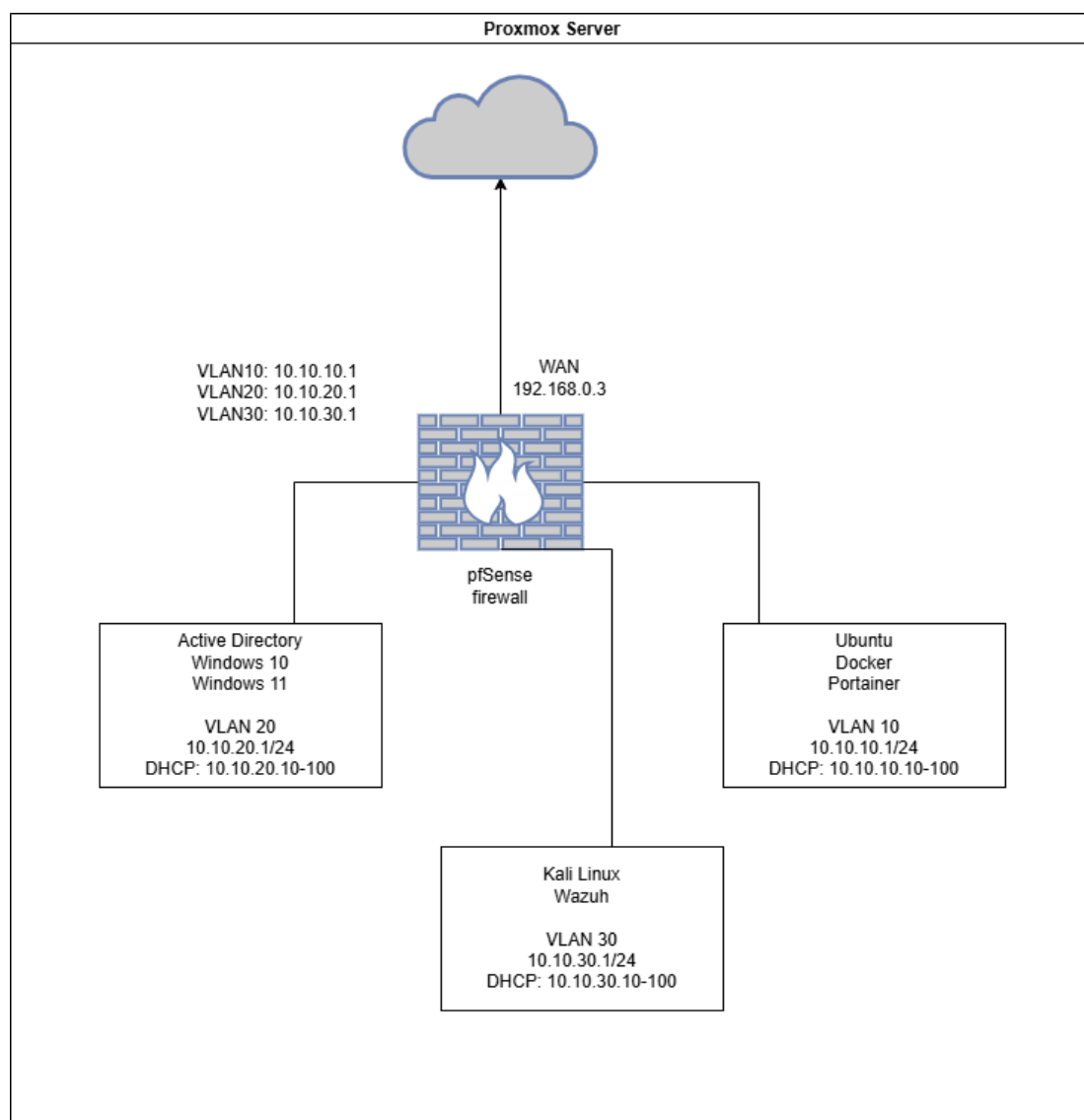
Projekt „Home-Lab” to kompleksowy projekt mający na celu praktyczne zdobycie umiejętności i naukę nowych technologii z zakresu cyberbezpieczeństwa, administracji sieciami / systemami, automatyzacji zadań oraz sztucznej inteligencji. Jest to przykład praktycznego wykorzystania różnorodnych narzędzi i konfiguracji, umożliwiających m.in. zarządzanie infrastrukturą, skanowanie podatności, monitorowanie sieci, wykrywanie zagrożeń oraz reagowanie na incydenty.

2. Architektura Sieciowa

Całe środowisko laboratoryjne jest zbudowane na platformie wirtualizacyjnej Proxmox. Jego centralnym punktem jest firewall pfSense, przy pomocy którego sieć jest podzielona na kilka podsieci. Segmentacja odbywa się za pomocą VLAN-ów (Virtual Local Area Network), co pozwala na ich izolację:

- **VLAN 10 (10.10.10.0/24):** podsieć dla maszyn Linux i kontenerów (Docker).
- **VLAN 20 (10.10.20.0/24):** podsieć z maszynami Windows.
- **VLAN 30 (10.10.30.0/24):** podsieć dla narzędzi bezpieczeństwa i monitoringu.

Tak zaplanowana architektura umożliwi łatwą rozbudowę w przyszłości np. poprzez utworzenie dodatkowych VLAN-ów.



Rys. 1 – Schemat sieci.

2.1 Szczegółowy opis architektury

- Serwer **Proxmox** będzie hostował wszystkie maszyny wirtualne laboratorium.
- Interfejs WAN zapory **pfSense** połączony z siecią domową (statyczny adres IP: 192.168.0.3/24)
- Interfejs LAN zapory **pfSense** (vbr1 w Proxmox) będzie trunkiem dla wszystkich wewnętrznych VLANów laboratorium. Został stworzony jako mostek (Linux Bridge) w Proxmox.
- Segmentacja VLAN:
 - **VLAN 10** (Docker / Kontenery): 10.10.10.0/24
 - Adres IP: 10.10.10.1
 - Zakres DHCP: 10.10.10.10-100
 - **VLAN 20** (Środowisko Windows): 10.10.20.0/24
 - Adres IP: 10.10.20.1
 - Zakres DHCP: 10.10.20.10-100
 - **VLAN 30** (Narzędzia bezpieczeństwa): 10.10.30.0/24
 - Adres IP: 10.10.30.1
 - Zakres DHCP: 10.10.30.10-100

3. Główne komponenty laboratorium

1. Zapora sieciowa (Firewall):

- pfSense: Główna zapora sieciowa, zarządzająca ruchem i segmentacją sieci.

2. Docker / Kontenery – VLAN 10:

- Ubuntu Server: Host dla kontenerów Docker.
- Docker: Platforma konteneryzacji.
- Portainer: Narzędzie do zarządzania kontenerami.

3. Środowisko Windows (Windows Server, Active Directory) – VLAN 20:

- Windows Server 2022: Kontroler domeny (AD, Group Policy, DHCP, DNS).
- Windows 10: Maszyna kliencka.
- Windows 11: Maszyna kliencka.

4. Narzędzia bezpieczeństwa – VLAN 30:

- Kali Linux: Maszyna do ataków i testów penetracyjnych.
- Wazuh: Rozwiązanie SIEM/XDR.
- Nessus: Skaner podatności.

4. Etapy realizacji projektu

4.1. Instalacja oraz konfiguracja hypervisora (Proxmox)

Kluczowym elementem każdego laboratorium jest wybór odpowiedniego systemu, który zostanie zainstalowany na fizycznym sprzęcie. W tym wypadku wybór padł na platformę Proxmox Virtual Environment. Istotną zaletą tego rozwiązania jest to, że opiera się na zmodyfikowanym jądrze Debiana oraz jest rozwiązaniem open source z aktywną społecznością. System został zainstalowany na sprzęcie o specyfikacji:

Model: Lenovo PC ThinkCentre M920x Tiny USFF

Procesor: Intel® Core™ i7-9700 @ 3.00GHz (8 rdzeni)

Pamięć operacyjna: 64 GB RAM DDR4 3200MHz

Dysk: 1 x Samsung PM9B1 NVMe 512 GB, 2 x WD SN580 2TB NVMe

Karta dźwiękowa: Zintegrowana Realtek® ALC233VB2 High Definition (HD) Audio

Karta sieciowa: Zintegrowana Intel® I219-V Gigabit Ethernet 10/100/1000 Mbit/s

Karta graficzna: Zintegrowana Intel® UHD Graphics 630

Chipset: Intel® Q370

Porty rozszerzeń:

2 x SODIMM

1 x SATA

1 x M.2 PCIe 2230 (dla WLAN)

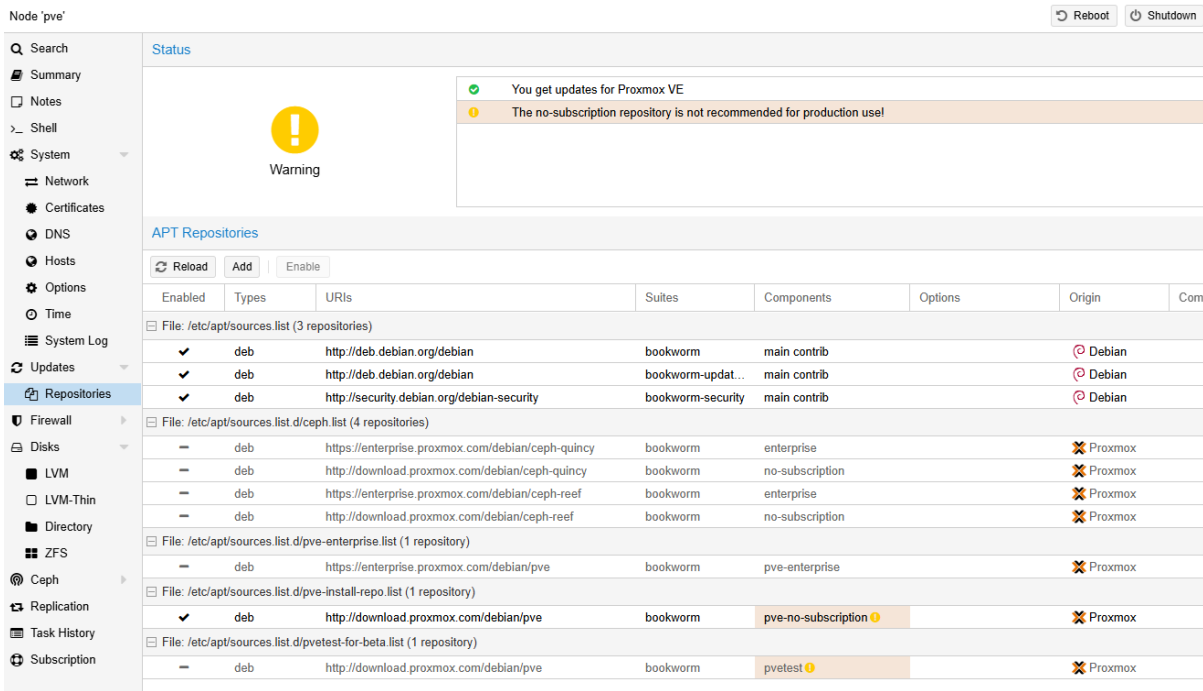
1 x M.2 PCIe 2280

1 x M.2 PCIe 2280 / 2242



Rys. 2 – Lenovo PC ThinkCentre M920x Tiny USFF.











Proces instalacji nie różni się znacząco od typowej instalacji systemu Linux. Uwagi natomiast wymaga konfiguracja Proxmox po zakończeniu instalacji. Pierwszą rzeczą jest konfiguracja repozytorium pakietów i aktualizacja systemu.



Rys. 3 – Konfiguracja repozytorium pakietów w Proxmox.

Dyski zostały wykorzystane następująco:

- Dysk Samsung PM9B1 NVMe 512 GB został przeznaczony w całości na system Proxmox oraz na magazynowanie obrazów instalacyjnych maszyn wirtualnych.
- Dwa dyski WD SN580 2TB NVMe zostały przeznaczone pod wirtualne maszyny, dyski zostały połączone w RAID1 (Mirroring) w celu zapewnienia bezpieczeństwa przed utratą danych w przypadku awarii jednego dysku. Zastosowany został system plików ZFS.

Reload	Show S.M.A.R.T. values	Initialize Disk with GPT	Wipe Disk				
Device	Type	Usage	Size	GPT	Model	Serial	S.M.A.R.T.
 /dev/nvme0n1	nvme	partitions	512.11 GB	Yes	PM9B1 NVMe Samsung 512GB	S6MZNFMW702050	PASSED
 /dev/nvme0n...	partition	BIOS boot	1.03 MB	Yes			
 /dev/nvme0n...	partition	EFI	1.07 GB	Yes			
 /dev/nvme0n...	partition	ZFS	511.04 GB	Yes			
 /dev/nvme1n1	nvme	partitions	2.00 TB	Yes	WD Blue SN580 2TB	24401W804826	PASSED
 /dev/nvme1n...	partition	ZFS	2.00 TB	Yes			
 /dev/nvme1n...	partition	ZFS reserved	8.39 MB	Yes			
 /dev/nvme2n1	nvme	partitions	2.00 TB	Yes	WD Blue SN580 2TB	24401W804804	PASSED
 /dev/nvme2n...	partition	ZFS	2.00 TB	Yes			
 /dev/nvme2n...	partition	ZFS reserved	8.39 MB	Yes			

Rys. 4 – Konfiguracja dysków.

Status: tank0

Reload

Health

ONLINE

Errors

No known data errors

Devices

Name	Health	READ	WRITE	CKSUM
<div> <div></div> <div>tank0</div> </div>	<div> <div></div> <div>ONLINE</div> </div>	0	0	0
<div> <div></div> <div>mirror-0</div> </div>	<div> <div></div> <div>ONLINE</div> </div>	0	0	0
<div> <div></div> <div>/dev/disk/by-id/nvme-WD_Blue_SN580_2TB_24401W804826-part1</div> </div>	<div> <div></div> <div>ONLINE</div> </div>	0	0	0
<div> <div></div> <div>/dev/disk/by-id/nvme-WD_Blue_SN580_2TB_24401W804804-part1</div> </div>	<div> <div></div> <div>ONLINE</div> </div>	0	0	0

Rys. 4 – Konfiguracja dysków – ZFS.

W celu robienia backupu maszyn wirtualnych podmontowany został zewnętrzny zasób sieciowy (exos-backup) przez protokół SMB/CIFS. Zasób dostępny z lokalnej sieci LAN.

Edit: SMB/CIFS

General

Backup Retention

ID:

exos-backup

Nodes:

All (No restrictions)

Server:

192.168.0.100

Enable:

☒

Username:

backup

Content:

Backup

Password:

Domain:

Share:

proxmox

Subdirectory:

Preallocation:

Default

?

Help

Advanced

☒

OK

Rys. 5 – Konfiguracja backupu.

4.2. Instalacja oraz konfiguracja zapory pfSense