

# Pojekt Home-Lab

---

## Spis treści

1. Cel projektu .....	2
2. Architektura Sieciowa .....	3
2.1. Szczegółowy opis architektury .....	3
3. Główne komponenty laboratorium .....	5
4. Etapy realizacji projektu.....	6
4.1. Instalacja oraz konfiguracja hypervisor (Proxmox) .....	6
4.1.1. Konfiguracja metody backupu z wykorzystaniem Proxmox Backup Server .....	8
4.2. Instalacja oraz konfiguracja zapory sieciowej pfSense .....	9
4.2.1. Tworzenie maszyny wirtualnej dla pfSense oraz instalacja systemu .....	9
4.2.2. Konfiguracja maszyny wirtualnej pfSense .....	10
4.2.3. Szczegółowy opis konfiguracji zapory .....	11
4.3. Instalacja serwera Ubuntu, Dockera, Portainera.....	12
4.3.1. Tworzenie maszyny wirtualnej dla Ubuntu oraz instalacja systemu .....	12
4.3.2. Instalacja Dockera na Ubuntu Server .....	13
4.3.3. Instalacja Portainera (Ubuntu + Docker) .....	14
4.3.4. Konfiguracja sieci dla kontenerów Docker .....	15
4.4. Budowa serwera Wazuh .....	17
4.4.1. Tworzenie maszyny wirtualnej oraz instalacja systemu bazowego (Ubuntu) .....	17
4.4.2. Instalacja Wazuh.....	17
4.4.3. Instalacja agentów Wazuh.....	19
4.5. Budowa kontrolera domeny (Windows Server 2022).....	22
4.5.1. Tworzenie maszyny wirtualnej oraz instalacja Windows Server 2022 .....	22
4.5.2. Podstawowa konfiguracja systemu Windows Server 2022 po instalacji .....	23
4.5.3. Uruchomienie ról: Active Directory Domain Services (AD DS), DHCP i DNS.....	25
4.5.4. Przeniesienie usługi DHCP z pfSense do Windows Server 2022 .....	27
4.6. Budowa maszyny klienckiej Windows (Windows 10) .....	28
4.6.1. Tworzenie maszyny wirtualnej oraz instalacja Windows 10 .....	28
4.6.2. Podłączenie do domeny oraz weryfikacja poprawności połączenia .....	30
5. Podsumowanie .....	31

## **1. Cel projektu**

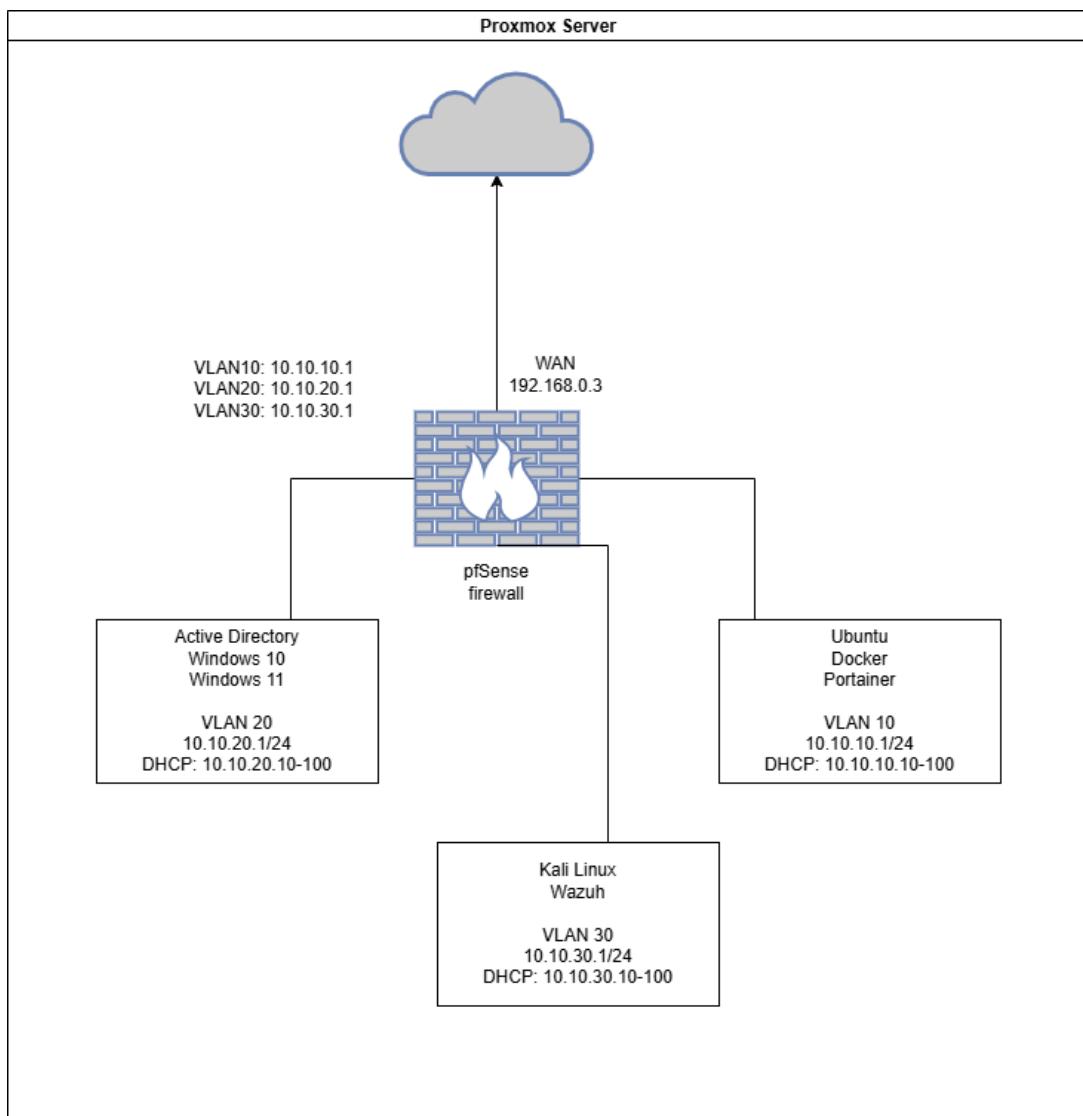
Projekt "Home-Lab" to kompleksowy projekt mający na celu praktyczne zdobycie umiejętności i naukę nowych technologii z zakresu cyberbezpieczeństwa, administracji sieciami / systemami, automatyzacji zadań oraz sztucznej inteligencji. Jest to przykład praktycznego wykorzystania różnorodnych narzędzi i 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 umożliwia 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** (vmbr1 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**

- **Zapora sieciowa (Firewall):**
  - pfSense: Główna zapora sieciowa, zarządzająca ruchem i segmentacją sieci.
- **Docker / Kontenery – VLAN 10:**
  - Ubuntu Server: Host dla kontenerów Docker.
  - Docker: Platforma konteneryzacji.
  - Portainer: Narzędzie do zarządzania kontenerami.
- **Środowisko Windows (Windows Server, Active Directory) – VLAN 20:**
  - Windows Server 2022: Kontroler domeny (AD, Group Policy, DHCP, DNS).
  - Windows 10: Maszyna kliencka.
- **Narzędzia bezpieczeństwa – VLAN 30:**
  - Kali Linux: Maszyna do ataków i testów penetracyjnych.
  - Wazuh: Rozwiązanie SIEM/XDR.

## 4. Etapy realizacji projektu

### 4.1. Instalacja oraz konfiguracja hypervisor (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)

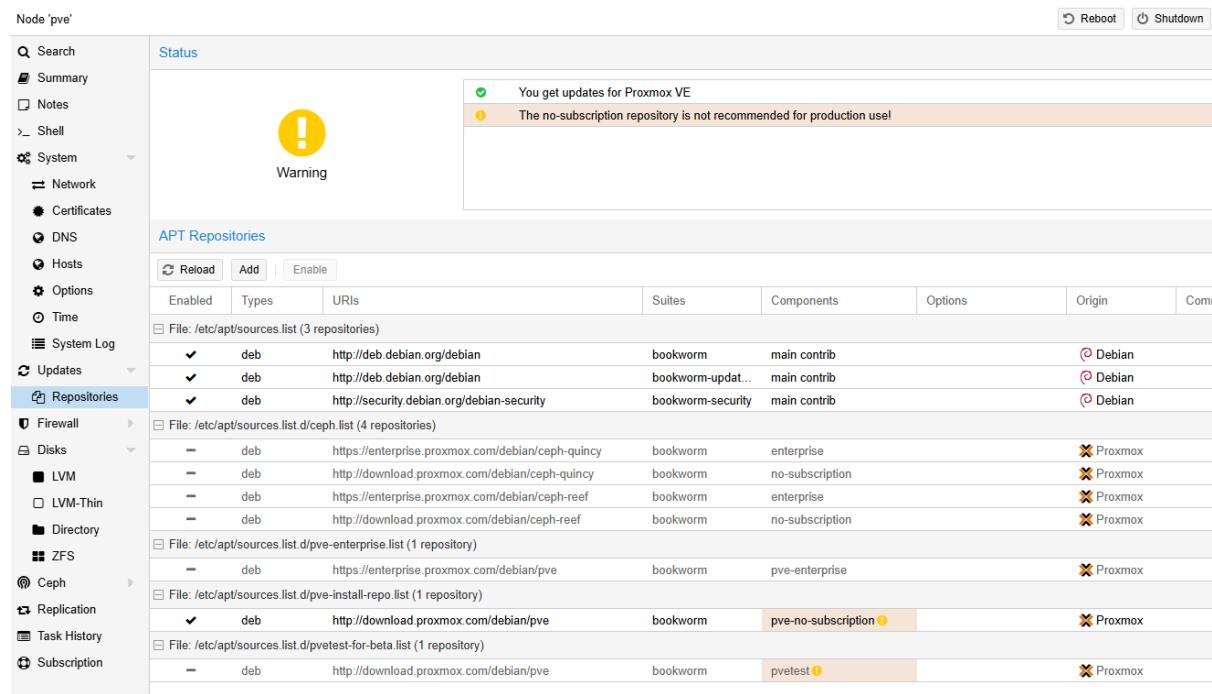
1 x M.2 PCIe 2280

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.

Disk Configuration							
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/nvme0n1p1	partition	BIOS boot	1.03 MB	Yes			
/dev/nvme0n1p2	partition	EFI	1.07 GB	Yes			
/dev/nvme0n1p3	partition	ZFS	511.04 GB	Yes			
/dev/nvme1n1	nvme	partitions	2.00 TB	Yes	WD Blue SN580 2TB	24401W804826	PASSED
/dev/nvme1n1p1	partition	ZFS	2.00 TB	Yes			
/dev/nvme1n1p2	partition	ZFS reserved	8.39 MB	Yes			
/dev/nvme2n1	nvme	partitions	2.00 TB	Yes	WD Blue SN580 2TB	24401W804804	PASSED
/dev/nvme2n1p1	partition	ZFS	2.00 TB	Yes			
/dev/nvme2n1p2	partition	ZFS reserved	8.39 MB	Yes			

Rys. 4 – Konfiguracja dysków.

Status: tank0					
<input type="button" value="Reload"/> <input type="button" value="Edit"/>					
Health		<span style="color: green;"> ONLINE</span>			
Errors		No known data errors			
Devices					
Name		Health	READ	WRITE	CKSUM
tank0	-	<span style="color: green;"> ONLINE</span>	0	0	0
mirror-0	-	<span style="color: green;"> ONLINE</span>	0	0	0
/dev/disk/by-id/nvme-WD_Blue_SN580_2TB_24401W804826-part1		<span style="color: green;"> ONLINE</span>	0	0	0
/dev/disk/by-id/nvme-WD_Blue_SN580_2TB_24401W804804-part1		<span style="color: green;"> ONLINE</span>	0	0	0

Rys. 5 – 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:	<input checked="" type="checkbox"/>
Username:	backup	Content:	Backup
Password:	*****	Domain:	
Share:	proxmox	Subdirectory:	
Preallocation:	Default		
<input type="button" value="Help"/> <input type="button" value="Advanced"/> <input type="button" value="OK"/>			

Rys. 6 – Konfiguracja backupu.

#### 4.1.1. Konfiguracja metody backupu z wykorzystaniem Proxmox Backup Server

W ramach rozbudowy laboratorium oraz złożoności całego projektu rozwinięty został system backupu całego środowiska. Do tego celu zostało wykorzystane dedykowane rozwiązanie w postaci systemu Proxmox Backup Server (PBS). PBS został zainstalowany na osobnej fizycznej maszynie.

## 4.2. Instalacja oraz konfiguracja zapory sieciowej pfSense

### 4.2.1. Tworzenie maszyny wirtualnej dla pfSense oraz instalacja systemu

ID VM: 200

Nazwa: pfSense

OS: Użycie pobranego obrazu ISO pfSense (pfSense-CE-2.7.2-RELEASE-amd64.iso)

Dysk: 50 GB (vm-drives).

CPU: 4 rdzenie.

RAM: 8 GB.

Interfejsy sieciowe:

net0: podłączony do vmbr0 (WAN).

net1: podłączony do vmbr1 (LAN).

Virtual Machine 200 (pfSense) on node 'pve'		No Tags 			
	Add	Remove	Edit	Disk Action	Revert
Summary					
Console					
Hardware					
Cloud-Init					
Options					
Task History					
Monitor					
Backup					
Replication					
Snapshots					
Firewall					
Permissions					
Memory	8.00 GiB				
Processors	4 (1 sockets, 4 cores) [host]				
BIOS	Default (SeaBIOS)				
Display	Default				
Machine	Default (i440fx)				
SCSI Controller	VirtIO SCSI single				
Hard Disk (scsi0)	vm-drives:200/vm-200-disk-0.qcow2,iothread=1,size=50G				
Network Device (net0)	virtio=BC:24:11:93:E0:C5,bridge=vmbr0,firewall=1				
Network Device (net1)	virtio=BC:24:11:2B:AD:9A,bridge=vmbr1,firewall=1				

Rys. 7 – Konfiguracja maszyny wirtualnej pfSense.

	Summary	<a href="#">Edit</a>	<a href="#">Revert</a>
	Name	pfSense	
	Start at boot	Yes	
	Start/Shutdown order	order=any	
	OS Type	Linux 6.x - 2.6 Kernel	
	Boot Order	scsi0	
	Use tablet for pointer	Yes	
	Hotplug	Disk, Network, USB	
	ACPI support	Yes	
	KVM hardware virtualization	Yes	
	Freeze CPU at startup	No	
	Use local time for RTC	Default (Enabled for Windows)	
	RTC start date	now	
	SMBIOS settings (type1)	uuid=4f318fb3-3d2f-48ed-b837-b9a481576d0f	
	QEMU Guest Agent	Enabled	
	Protection	No	
	Spice Enhancements	none	
	VM State storage	Automatic	
	AMD SEV	Default (Disabled)	

Rys. 8 – Konfiguracja maszyny wirtualnej pfSense (2).

#### 4.2.2. Konfiguracja maszyny wirtualnej pfSense

Po zainstalowaniu systemu pierwszym krokiem jaki należy zrobić jest konfiguracja interfejsów sieciowych. Tak jak to już wcześniej zostało skonfigurowane maszyna posiada dwa interfejsy sieciowe: WAN oraz LAN. W pfSense są one oznaczone odpowiednio `vtnet0` oraz `vtnet1`.

```

QEMU Guest - Netgate Device ID: 2e8ce3397f538cef95b6

*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4: 192.168.0.3/24
LAN (lan)      -> vtnet1      -> v4: 10.10.1.1/24
VLAN10 (opt1)  -> vtnet1.10  -> v4: 10.10.10.1/24
VLAN20 (opt2)  -> vtnet1.20  -> v4: 10.10.20.1/24
VLAN30 (opt3)  -> vtnet1.30  -> v4: 10.10.30.1/24

.0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address       11) Restart GUI
3) Reset admin account and 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

```

Rys. 9 – Konfiguracja interfejsów sieciowych w pfSense.

Po skonfigurowaniu interfejsów sieciowych istnieje możliwość zarządzania zaporą z poziomu panelu WWW.

The screenshot shows the pfSense web interface with the following details:

**System Information**

- Name: pfSense.home.arpa
- User: admin@192.168.0.226 (Local Database)
- System: QEMU Guest  
Netgate Device ID: 2e8ce3397f538cef95b6
- BIOS: Vendor: SeaBIOS  
Version: rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org  
Release Date: Tue Apr 1 2014
- Version: 2.7.2-RELEASE (amd64)  
built on Wed Dec 6 21:10:00 CET 2023  
FreeBSD 14.0-CURRENT
- CPU Type: QEMU Virtual CPU version 2.5+  
4 CPUs: 1 package(s) x 4 core(s)  
AES-NI CPU Crypto: Yes (inactive)  
QAT Crypto: No
- Hardware crypto: Inactive
- Kernel PTI: Enabled

**Interfaces**

Interface	Duplex	IP Address
WAN	10Gbase-T <full-duplex>	192.168.0.3
LAN	10Gbase-T <full-duplex>	10.10.1.1
VLAN10	10Gbase-T <full-duplex>	10.10.10.1
VLAN20	10Gbase-T <full-duplex>	10.10.20.1
VLAN30	10Gbase-T <full-duplex>	10.10.30.1

**Interface Statistics**

	WAN	LAN	VLAN10	VLAN20	VLAN30
Packets In	1267	0	0	0	0
Packets Out	1559	5	4	4	5
Bytes In	431 KiB	0 B	0 B	0 B	0 B
Bytes Out	907 KiB	416 B	344 B	344 B	416 B
Errors In	0	0	0	0	0
Errors Out	0	0	0	0	0
Collisions	0	0	0	0	0

Rys. 10 – Panel zarządzania pfSense.

Na powyższych zrzutach ekranu widoczne są już utworzone i skonfigurowane VLANy. Każdy z nich posiada połączenie z siecią zewnętrzną Internet oraz zapewnioną komunikację między sobą. Natomiast domyślnie zapora blokuje ruch z zewnątrz. Aby możliwy był dostęp do VLAN-ów z zewnątrz i tym samym do hostowanych w nich usług konieczne jest zezwolenie na ruch przez dodanie odpowiednich reguł.

The screenshot shows the pfSense web interface with the following details:

**Rules (Drag to Change Order)**

Actions	Description	Queue	Gateway	Port	Destination	Protocol	States	Source
		none	*	*	*	IPv4 *	✓ 8/4.12 MiB	192.168.0.0/24

**Actions**

- Add
- Up
- Down
- Delete
- Toggle
- Copy
- Save
- Separator

Rys. 11 – Reguła pfSense zezwalająca na ruch z zewnątrz.

#### 4.2.3. Szczegółowy opis konfiguracji zapory

##### 1. Konfiguracja VLANów w pfSense (przez interfejs webowy):

- Przejście do Interfaces -> Assignments -> VLANs.
- Dodanie VLANów:
  - VLAN 10: Parent interface vtnet1 (LAN), VLAN tag 10.

- VLAN 20: Parent interface vtnet1 (LAN), VLAN tag 20.
  - VLAN 30: Parent interface vtnet1 (LAN), VLAN tag 30.
- Przypisanie interfejsów do VLANów (Interfaces -> Assignments):
  - Dodanie OPT1 dla VLAN 10 na vtnet1.
  - Dodanie OPT2 dla VLAN 20 na vtnet1.
  - Dodanie OPT3 dla VLAN 30 na vtnet1.
- Konfiguracja interfejsów dla VLANów:
  - OPT1 (VLAN10): Włączenie, zmiana nazwy na VLAN10, adres IPv4 statyczny 10.10.10.1/24.
  - OPT2 (VLAN20): Włączenie, zmiana nazwy na VLAN20, adres IPv4 statyczny 10.10.20.1/24.
  - OPT3 (VLAN30): Włączenie, zmiana nazwy na VLAN30, adres IPv4 statyczny 10.10.30.1/24.

## 2. Konfiguracja reguł zapory dla VLANów w pfSense:

- Przejście do Firewall -> Rules.
- Dla każdego nowo utworzonego interfejsu VLAN (VLAN10, VLAN20, VLAN30):
  - Skopiowanie domyślnej reguły "Allow LAN to any" z interfejsu LAN.
  - Zmiana źródła (Source) z "LAN subnets" na odpowiedni "[NazwaVLAN] subnets".
- Dodanie reguły na interfejsie WAN zezwalającej na ruch z zewnętrz.

## 3. Konfiguracja serwera DHCP dla VLANów w pfSense:

- Przejście do Services -> DHCP Server.
- Dla każdego interfejsu VLAN (VLAN10, VLAN20, VLAN30):
  - Włączenie serwera DHCP.
  - Ustawienie zakresu adresów (np. dla VLAN10: od 10.10.10.10 do 10.10.10.100).
  - Dodanie serwerów DNS: 10.10.X.1 (gdzie X to numer VLAN) oraz 1.0.0.2, 1.1.1.1, 8.8.8.8.

## 4.3. Instalacja serwera Ubuntu, Dockera, Portainera

### 4.3.1. Tworzenie maszyny wirtualnej dla Ubuntu oraz instalacja systemu

ID VM: 202

Nazwa: docker

OS:Ubuntu Server 22.04. (Live).

Dysk: 250 GB (vm-drives).

CPU: 6 rdzeni.

RAM: 16 GB.

Interfejs sieciowy: podłączony do vmbr1 (LAN) z tagiem VLAN 10.

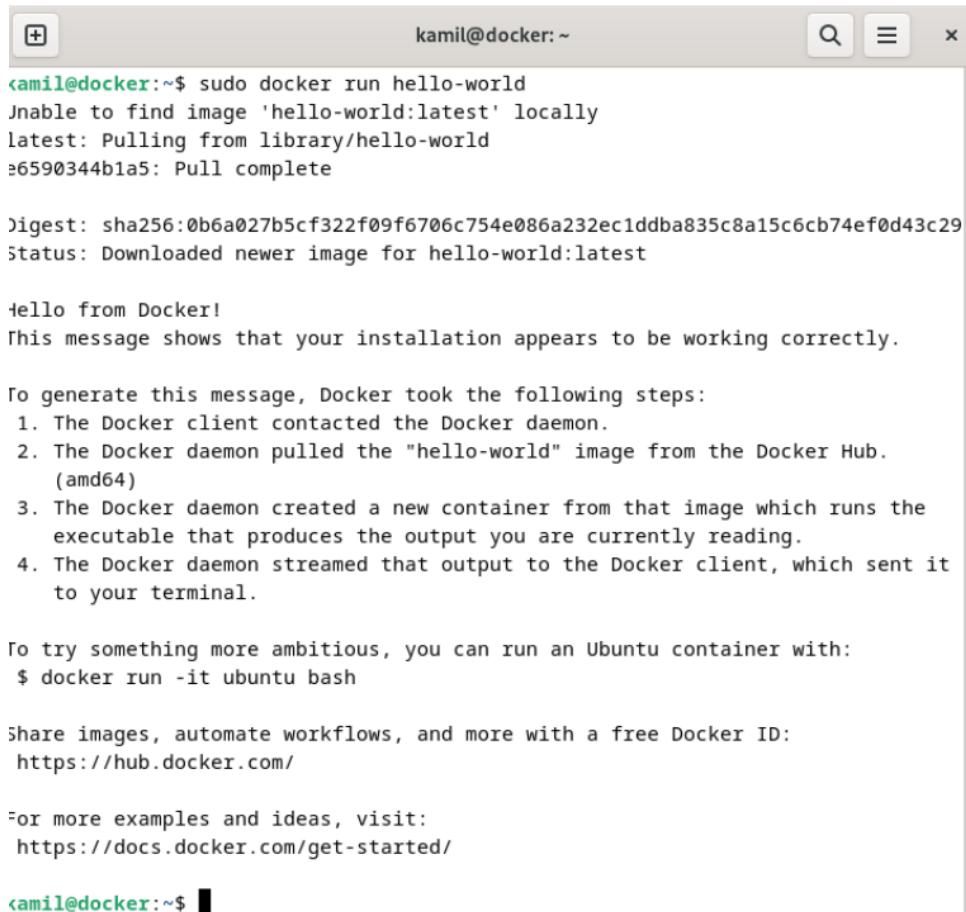
Instalacja z ustawieniami domyślnymi + dodatkowo instalacja usługi serwera ssh.

Adres IP maszyny przydzielony przez DHCP (10.10.10.10).

#### 4.3.2. Instalacja Dockera na Ubuntu Server

Instalacja zgodnie z dokumentacją – <https://docs.docker.com/engine/install/ubuntu/>

```
#Run the following command to uninstall all conflicting packages:  
for pkg in docker.io docker-doc docker-compose docker-compose-v2 podman-docker  
containerd runc; do sudo apt-get remove $pkg; done  
  
# Add Docker's official GPG key:  
sudo apt-get update  
sudo apt-get install ca-certificates curl  
sudo install -m 0755 -d /etc/apt/keyrings  
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o  
/etc/apt/keyrings/docker.asc  
sudo chmod a+r /etc/apt/keyrings/docker.asc  
  
#1. Set up Docker's apt repository.  
# Add the repository to Apt sources:  
echo \  
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc]  
https://download.docker.com/linux/ubuntu \  
  $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}") stable" | \  
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  
sudo apt-get update  
  
#2. Install the Docker packages.  
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin  
docker-compose-plugin  
  
#3. Verify that the installation is successful by running the hello-world image:  
sudo docker run hello-world
```



```
kamil@docker:~$ sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
e6590344b1a5: Pull complete

Digest: sha256:0b6a027b5cf322f09f6706c754e086a232ec1ddba835c8a15c6cb74ef0d43c29
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/
kamil@docker:~$
```

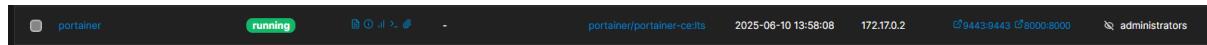
Rys. 12 – Weryfikacja instalacji i działania Dockera.

#### 4.3.3. Instalacja Portainera (Ubuntu + Docker)

Tak jak w przypadku Dockera, instalacja Portainera zgodnie z oficjalną dokumentacją – <https://docs.portainer.io/start/install-ce/server/docker/linux>

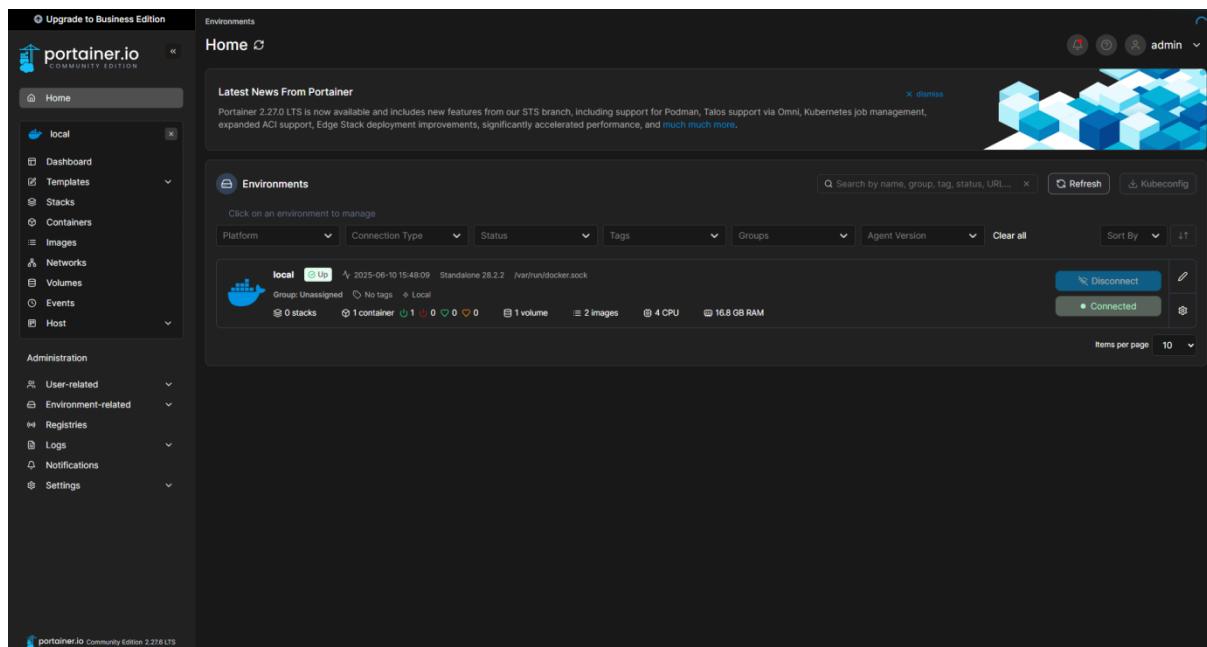
```
#First, create the volume that Portainer Server will use to store its database:
sudo docker volume create portainer_data

#Then, download and install the Portainer Server container:
sudo docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v
/var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data
portainer/portainer-ce:lts
```



Rys. 13 – Uruchomiony kontener - Portainer.

Dostęp do interfejsu webowego Portainera dostępny w sieci z przeglądarki pod adresem **10.10.10.10:9443** (domyślny port portainera).



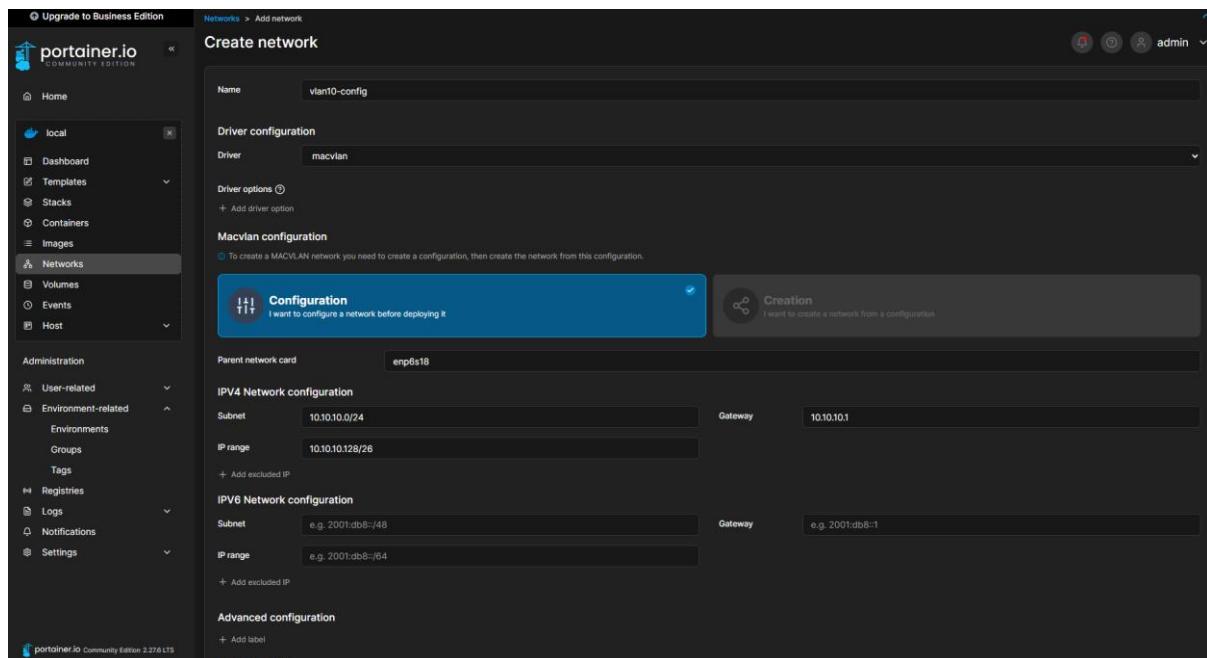
Rys. 14 – Panel Portainera.

#### 4.3.4. Konfiguracja sieci dla kontenerów Docker

MacVLAN umożliwia każdemu kontenerowi Docker posiadanie własnego, unikalnego adresu MAC i adresu IP w sieci hosta, co sprawia, że wyglądają one jak indywidualne urządzenia w sieci LAN. Jest to idealne rozwiązań do skanowania podatności na poziomie sieci.

Konfiguracja sprowadza się do dwóch kroków:

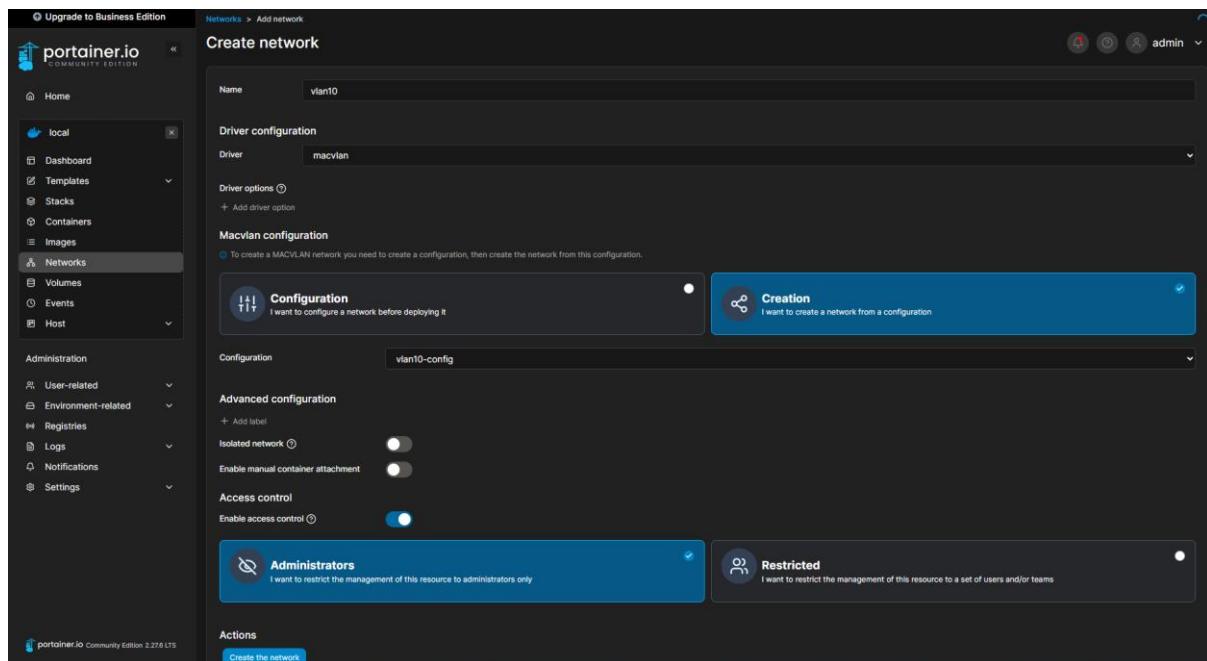
1. Utworzenia konfiguracji:
  - Networks → Add network
  - Name: vlan10-config (nazwa konfiguracji)
  - Driver: macvlan
  - Macvlan configuration: Configuration: „I want to configure a network before deploying it”
  - Parent network card (Nadrzędna karta sieciowa): nazwa interfejsu hosta enp6s18
  - IPv4 Network configuration:
    - Subnet: 10.10.10.0/24 (Cała podsieć VLAN 10)
    - Gateway: 10.10.10.1 (brama pfSense dla VLAN 10)
    - IP range: (Zakres adresów IP wewnętrznych podsieci 10.10.10.0/24, który nie jest zarezerwowany dla serwera DHCP pfSense dla hostów VM) 10.10.10.128/26 (zapewnia to adresy IP od .129 do .190 dla kontenerów – 62 hosty)
    - Create the Network



Rys. 15 – Portainer – vlan10-config.

## 2. Wdrożenie konfiguracji:

- Networks → Add network
- Name: vlan10 (nazwa wdrożenia)
- Driver: macvlan
- Macvlan configuration: „Creation: I want to create a network from a configuration”
- Configuration: vlan10-config (wybór sieci konfiguracyjnej)
- Create the network



Rys. 16 – Portainer – vlan10.

## 4.4. Budowa serwera Wazuh

Wazuh to darmowa platforma SIEM (Security Information and Event Management) oraz XDR (Extended Detection and Response) typu open-source, która pomaga organizacjom wykrywać zagrożenia, monitorować bezpieczeństwo i zachować zgodność.

### 4.4.1. Tworzenie maszyny wirtualnej oraz instalacja systemu bazowego (Ubuntu)

Wazuh został zainstalowany na bazowym systemie Ubuntu Server 24.04 w taki sam sposób jak w rozdziale 4.3.

ID VM: 205

Nazwa: wazuh

OS:Ubuntu Server 24.04. (Live).

Dysk: 200 GB (vm-drives).

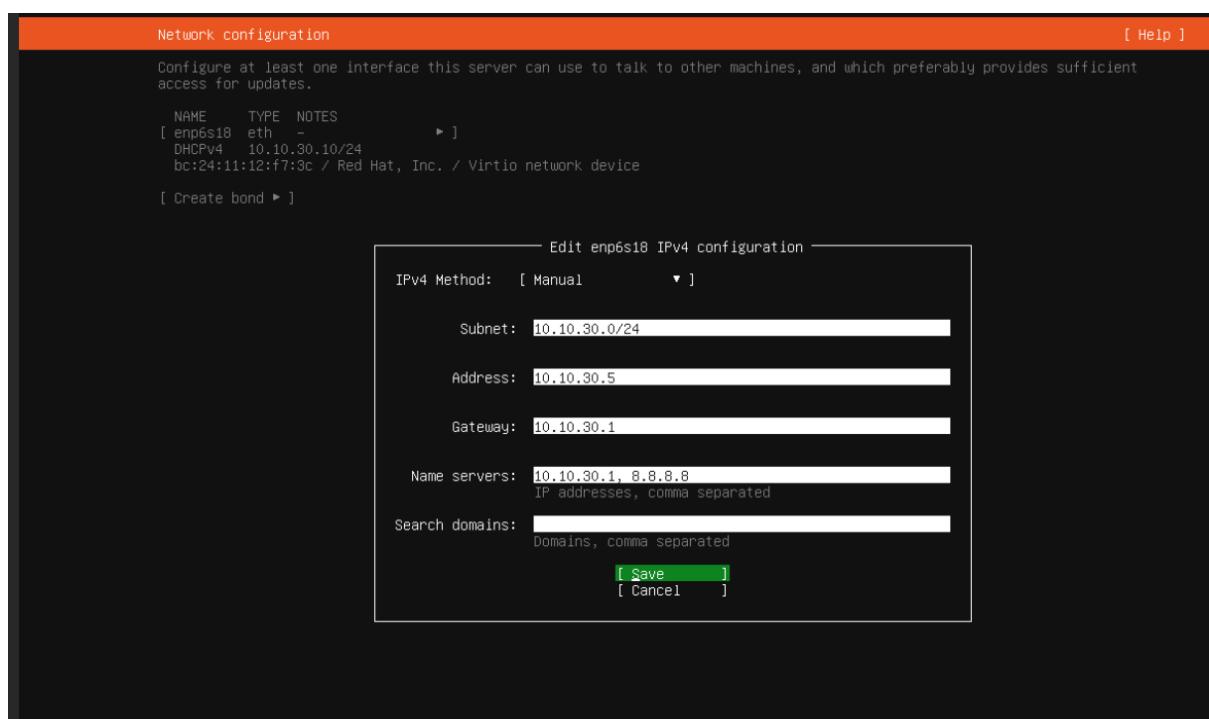
CPU: 8 rdzeni.

RAM: 8 GB.

Interfejs sieciowy: podłączony do vmbr1 (LAN) z tagiem VLAN 30.

Instalacja z ustawieniami domyślnymi + dodatkowo instalacja usługi serwera ssh.

Adres IP maszyny ustawiony statycznie na 10.10.30.5.



Rys. 17 – Instalacja Ubuntu – konfiguracja sieci.

### 4.4.2. Instalacja Wazuh

Instalacja Wazuh na Ubuntu jest bardzo prosta i sprowadza się do uruchomienia skryptu instalacyjnego **wazuh-install.sh**.

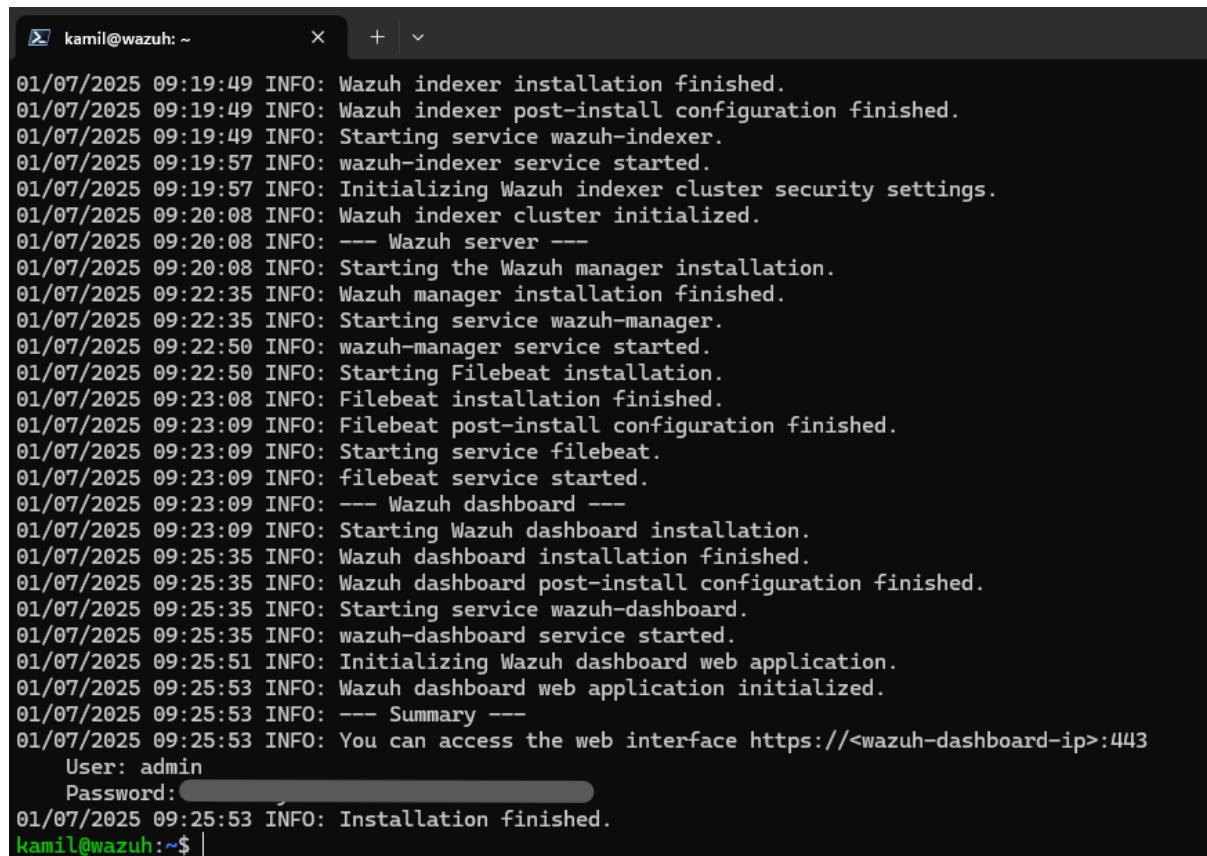
Sposób instalacji jest dokładnie przedstawiony w oficjalnej dokumentacji:  
<https://documentation.wazuh.com/current/quickstart.html>

i polega na wykonaniu jednego polecenia:

```
curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

To polecenie pobiera skrypt instalacyjny Wazuh i uruchamia go z flagą **-a**, która instaluje wszystkie komponenty (Manager, Indexer, Dashboard) na jednym serwerze.

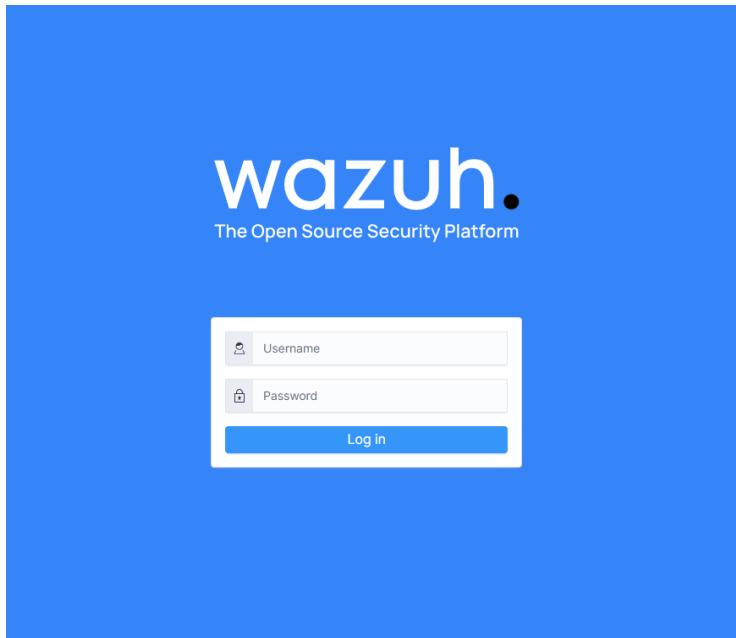
**Ważne** na tym etapie jest zachowanie hasła do panelu webowego przedstawionego przez instalator.



The screenshot shows a terminal window titled 'kamil@wazuh: ~'. It displays a log of Wazuh installation steps. The log includes messages about indexer installation, manager installation, filebeat installation, and dashboard installation. It also shows a summary and a note about accessing the web interface. At the bottom, it asks for a user and password, and then states that the installation is finished.

```
01/07/2025 09:19:49 INFO: Wazuh indexer installation finished.
01/07/2025 09:19:49 INFO: Wazuh indexer post-install configuration finished.
01/07/2025 09:19:49 INFO: Starting service wazuh-indexer.
01/07/2025 09:19:57 INFO: wazuh-indexer service started.
01/07/2025 09:19:57 INFO: Initializing Wazuh indexer cluster security settings.
01/07/2025 09:20:08 INFO: Wazuh indexer cluster initialized.
01/07/2025 09:20:08 INFO: --- Wazuh server ---
01/07/2025 09:20:08 INFO: Starting the Wazuh manager installation.
01/07/2025 09:22:35 INFO: Wazuh manager installation finished.
01/07/2025 09:22:35 INFO: Starting service wazuh-manager.
01/07/2025 09:22:50 INFO: wazuh-manager service started.
01/07/2025 09:22:50 INFO: Starting Filebeat installation.
01/07/2025 09:23:08 INFO: Filebeat installation finished.
01/07/2025 09:23:09 INFO: Filebeat post-install configuration finished.
01/07/2025 09:23:09 INFO: Starting service filebeat.
01/07/2025 09:23:09 INFO: filebeat service started.
01/07/2025 09:23:09 INFO: --- Wazuh dashboard ---
01/07/2025 09:23:09 INFO: Starting Wazuh dashboard installation.
01/07/2025 09:25:35 INFO: Wazuh dashboard installation finished.
01/07/2025 09:25:35 INFO: Wazuh dashboard post-install configuration finished.
01/07/2025 09:25:35 INFO: Starting service wazuh-dashboard.
01/07/2025 09:25:35 INFO: wazuh-dashboard service started.
01/07/2025 09:25:51 INFO: Initializing Wazuh dashboard web application.
01/07/2025 09:25:53 INFO: Wazuh dashboard web application initialized.
01/07/2025 09:25:53 INFO: --- Summary ---
01/07/2025 09:25:53 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: [REDACTED]
01/07/2025 09:25:53 INFO: Installation finished.
kamil@wazuh:~$ |
```

Rys. 18 – Instalacja Wazuh.



Rys. 19 – Okno logowania do panelu Wazuh.

#### 4.4.3. Instalacja agentów Wazuh

Agenci Wazuh zostaną zainstalowani na maszynach: Kali Linux, Docker oraz pfSense. Umożliwi to zbieranie logów z tych maszyn przez serwer Wazuh.

##### Instalacja agenta na Kali Linux

Przełączanie się na użytkownika Root

```
sudo -i
```

Dodanie repozytorium Wazuh Agent (zgodnie z dokumentacją:  
<https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html> -> sekcja "Deploy a Wazuh agent", zakładka APT):

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor | tee /usr/share/keyrings/wazuh.gpg > /dev/null
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
apt-get update
```

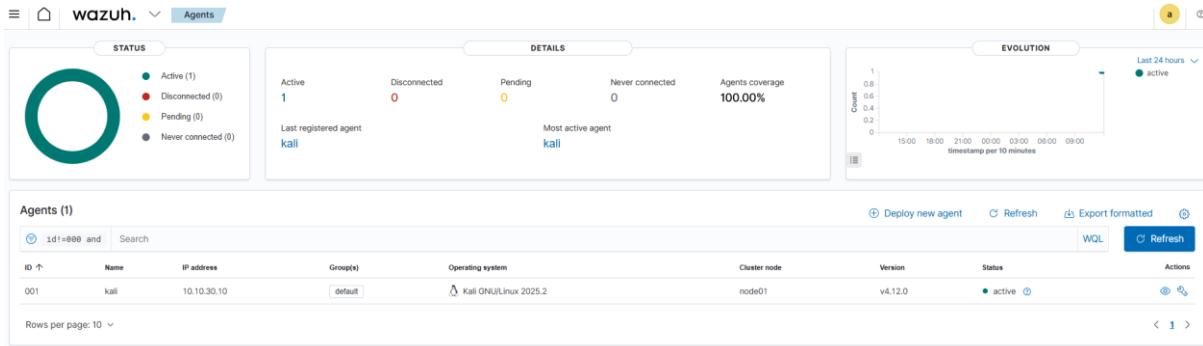
Instalacja agenta Wazuh, wskazując adres IP serwera Wazuh:

```
WAZUH_MANAGER='10.10.30.5' apt-get install wazuh-agent
```

Uruchomienie usługi agenta Wazuh:

```
systemctl daemon-reload  
systemctl enable wazuh-agent  
systemctl start wazuh-agent
```

Po poprawnej instalacji agent będzie widoczny w panelu managera Wazuh.



Rys. 20 – Agent Wazuh widoczny w panelu managera po instalacji.

### Instalacja agenta na maszynie z kontenerami Docker

Procedura instalacji agenta wygląda identycznie jak w przypadku instalacji na maszynie z Kali Linux. Wymagana jest jednak konfiguracja w celu szczegółowego monitorowania kontenerów. Dodatkowo zgodnie z dokumentacją należy:

```
pip3 install docker==7.1.0 urllib3==1.26.20 requests==2.32.2 --break-system-packages

# Add the following configuration to the Wazuh agent configuration file
/var/ossec/etc/ossec.conf to enable the Docker listener
nano /var/ossec/etc/ossec.conf

<wodle name="docker-listener">
  <disabled>no</disabled>
</wodle>

# Restart the Wazuh agent to apply the changes:
systemctl restart wazuh-agent
```

Poza tym w managerze Wazuh należy włączyć opcję monitorowania kontenerów:

Settings → Modules → Threat Detection and Response → Docker listener → ON

### Instalacja agenta na porcie pfSense

W tym przypadku procedura wygląda trochę inaczej z racji tego, że pfSense to FreeBSD.

```

cd /usr/local/etc/pkg/repos/
nano pfSense.conf
nano FreeBSD.conf

# Change the following lines to pfSense.conf and FreeBSD.conf
FreeBSD: { enabled: true }

pkg update

pkg search wazuh-agent

pkg install wazuh-agent-4.12.0 # or the latest version

cp /etc/localtime /var/ossec/etc/

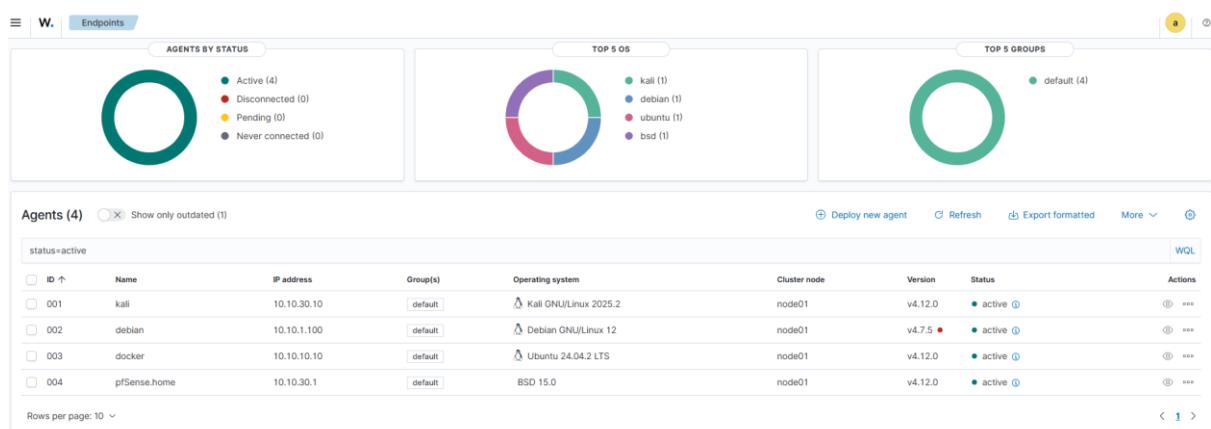
nano /var/ossec/etc/ossec.conf
# Change the following lines to ossec.conf
<server>
  <address>10.10.30.5</address>
  <port>1514</port>
</server>

# Enable the Wazuh agent service
sysrc wazuh_agent_enable="YES"

ln -s /usr/local/etc/rc.d/wazuh-agent /etc/rc.d/wazuh-agent.sh

service wazuh-agent start

```



Rys. 21 – Lista zainstalowanych i uruchomionych agentów.

## 4.5. Budowa kontrolera domeny (Windows Server 2022)

### 4.5.1. Tworzenie maszyny wirtualnej oraz instalacja Windows Server 2022

ID VM: 206

Nazwa: winsrv2022

OS: Windows Server 2022

Dysk: 200 GB (vm-drives).

CPU: 6 rdzeni.

RAM: 8 GB.

Interfejs sieciowy: podłączony do vmbr1 (LAN) z tagiem VLAN 20.

Memory	8.00 GiB
Processors	6 (1 sockets, 6 cores) [x86-64-v2-AES]
BIOS	OVMF (UEFI)
Display	Default
Machine	pc-q35-9.2+pve1
SCSI Controller	VirtIO SCSI single
Hard Disk (scsi0)	vm-drives:206/vm-206-disk-1.qcow2,iothread=1,size=200G
Network Device (net0)	rtl8139=BC:24:11:A2:E4:38,bridge=vmbr1,firewall=1,tag=20
EFI Disk	vm-drives:206/vm-206-disk-0.qcow2,eftype=4m,pre-enrolled-keys=1,size=528K
TPM State	vm-drives:206/vm-206-disk-2.raw,size=4M,version=v2.0

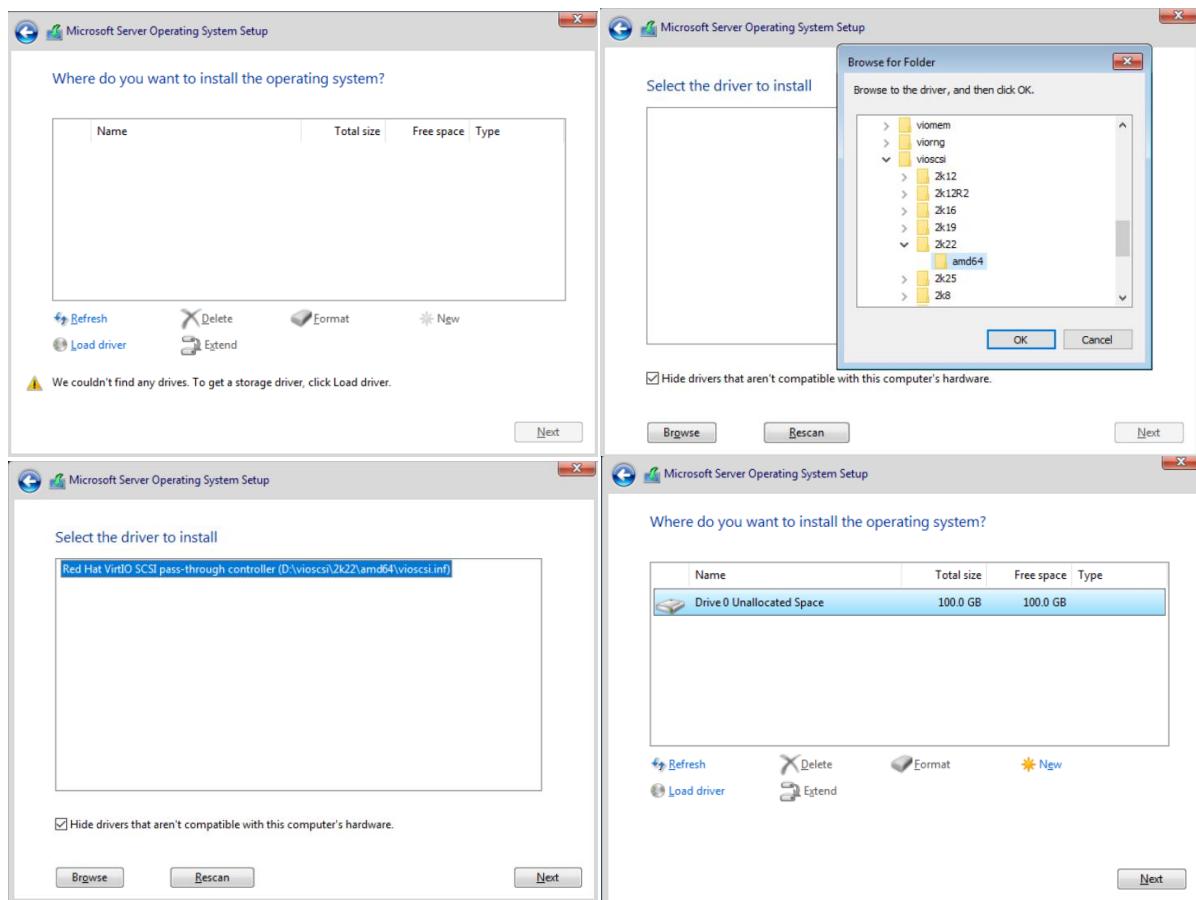
Rys. 22 – Konfiguracja maszyny wirtualnej Windows Server 2022.

Name	winsrv2022
Start at boot	Yes
Start/Shutdown order	order=any
OS Type	Microsoft Windows 11/2022/2025
Boot Order	scsi0, net0
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
KVM hardware virtualization	Yes
Freeze CPU at startup	No
Use local time for RTC	Default (Enabled for Windows)
RTC start date	now
SMBIOS settings (type1)	uuid=5caf71ff-321a-44dd-9906-d6fff704ddf2
QEMU Guest Agent	Default (Disabled)
Protection	No
Spice Enhancements	none
VM State storage	Automatic
AMD SEV	Default (Disabled)

Rys. 23 – Konfiguracja maszyny wirtualnej Windows Server 2022 (2).

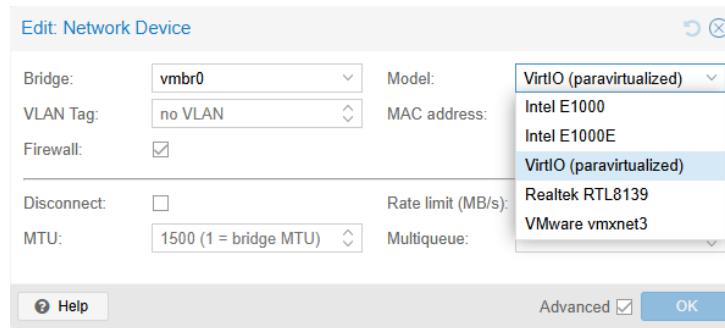
Zainstalowana wersja systemu to dokładnie *Standard Evaluation (Desktop Experience)*. Podczas instalacji wystąpił problem w postaci niewykrycia przez instalator podłączonego

dysku do maszyny wirtualnej. Rozwiązaniem tego problemu jest załadowanie odpowiednich sterowników kontrolera SCSI (virtio-win-0.1.266.iso).



Rys. 24 – Problem z wykrywaniem dysku podczas instalacji Windows Server 2022.

Po instalacji okazało się, że problem występuje także z interfejsem sieciowym – domyślny model urządzenia sieciowego w Proxmox (VirtIO) nie jest rozpoznawany przez system Windows. Rozwiązaniem w tym wypadku jest prosta zmiana typu urządzenia w konfiguracji maszyny wirtualnej (np. na Realtek RTL8139).



Rys. 25 – Zmiana modelu karty sieciowej maszyny z Windows Server 2022.

#### 4.5.2. Podstawowa konfiguracja systemu Windows Server 2022 po instalacji

##### 1. Konfiguracja statycznego adresu IP:

Adres IP: 10.10.20.10

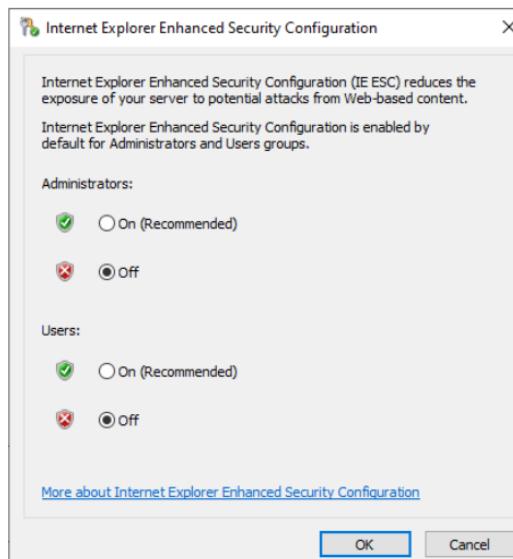
Maska podsieci: 255.255.255.0

Brama domyślna: 10.10.20.1 (Adres IP pfSense dla tej sieci VLAN)

## 2. Zmiana nazwy komputera: winsrv2022

### 3. Wyłączenie IE Enhanced Security Configuration:

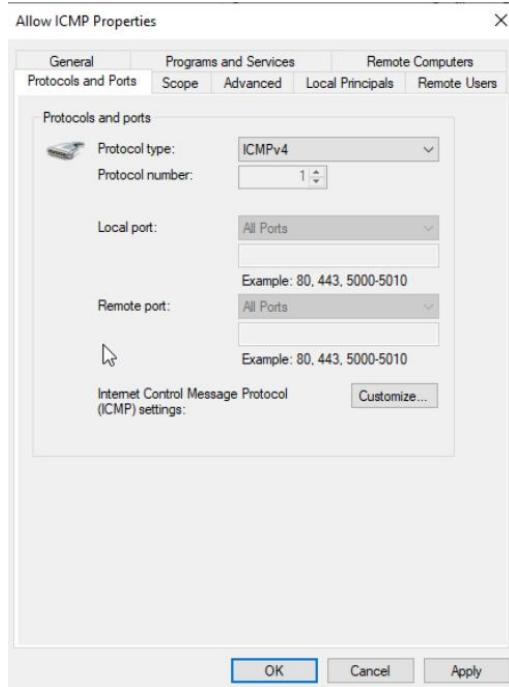
IE ESC ma za zadanie znacząco zwiększyć bezpieczeństwo podczas przeglądania stron w Internet Explorerze, jednak przy świadomym korzystaniu oraz środowisku serwerowym gdzie dostęp mają z reguły świadome osoby ta opcja sprawia więcej problemów niż pożytku.



Rys. 26 – Wyłączenie IE ESC w Windows Server 2022.

### 4. Zezwalanie na ruch ICMP przez zaporę systemową:

ICMP służy do kontroli transmisji danych w sieci, dostarczając informacje o błędach i statusie sieci. W celu włączenia lub wyłączenia możliwości odpowiadania na żądania ICMP (ping), należy przejść do Zapory systemu Windows Defender, sekcji "Ustawienia zaawansowane" i odnaleźć odpowiednie reguły ruchu przychodzącego.



Rys. 27 – Zezwolenie na ruch ICMP.

#### 4.5.3. Uruchomienie ról: Active Directory Domain Services (AD DS), DHCP i DNS

Po ponownym uruchomieniu i zalogowaniu się jako administrator w Menagerze Serwerów należy przejść do Manage → Add Roles and Features.

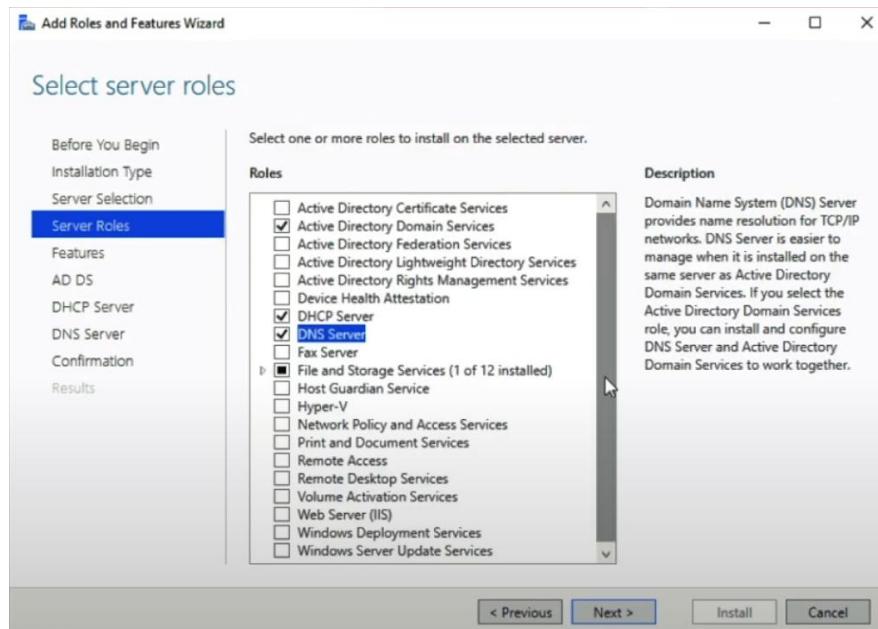
Zaznaczyć następujące role:

"Active Directory Domain Services" – po zaznaczeniu, wyskoczy okno z prośbą o dodanie wymaganych funkcji "Add Features"

"DHCP Server" – jw., wyskoczy okno, należy kliknąć "Add Features"

"DNS Server" – jw., wyskoczy okno, należy kliknąć "Add Features"

Należy potwierdzić wybór oraz kliknąć *Install*. Proces może zająć chwilę czasu, a serwer może się zrestartować.



Rys. 28 – Dodanie ról do serwera: AD DS., DHCP, DNS.

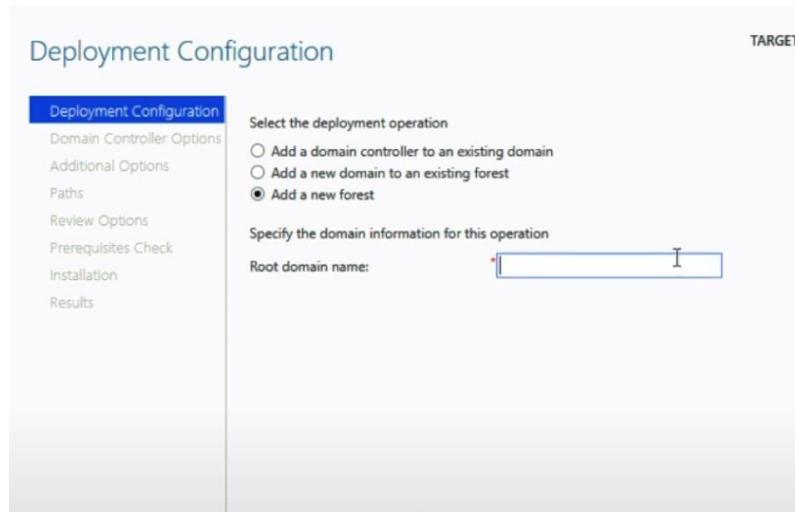
### Podniesienie serwera do rangi kontrolera domeny (Promoting to Domain Controller)

Po zakończeniu instalacji ról, należy kliknąć ikonę flagi (powiadomień) w prawym górnym rogu Menagera Serwerów, następnie "Promote this server to a domain controller" (Podnieś ten serwer do rangi kontrolera domeny).

Po restarcie na ekranie "Konfiguracja wdrożenia" (Deployment Configuration):

Wybrać opcję "Dodaj nowy las" (Add a new forest).

Nazwa domeny głównej (Root domain name): kamil.local



Rys. 29 – Ustawienie domeny.

W zakładce "Opcje dodatkowe" (Additional Options): należy sprawdzić nazwę domeny NetBIOS (powinna być taka jak część nazwy domeny głównej przed kropką, czyli w tym wypadku *kamil*).

Serwer zostanie automatycznie ponownie uruchomiony po zakończeniu instalacji.

#### 4.5.4. Przeniesienie usługi DHCP z pfSense do Windows Server 2022

Przejęcie roli serwera DHCP przez serwer Windows dla podsieci VLAN20 – z racji tego, że jest to sieć wydzielona tylko dla maszyn Windows.

Pierwszy krok to oczywiście wyłączenie usługi serwera DHCP na pfSense:

Services → DHCP Server → VLAN20 → Disable "Enable DHCP server on VLAN20 interface"

The screenshot shows the pfSense web interface for managing the DHCP Server. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is 'Services / DHCP Server / VLAN20'. The tabs at the top of the page are 'Settings', 'WAN', 'LAN', 'VLAN10', 'VLAN20' (which is highlighted in red), and 'VLAN30'. The 'General Settings' section contains the following configuration:

- DHCP Backend: Kea DHCP
- Enable:  Enable DHCP server on VLAN20 interface (this checkbox is circled in yellow)
- Deny Unknown Clients: Allow all clients

Below these settings, there are sections for 'Ignore Client Identifiers' (unchecked) and 'DNS Registration' (set to 'Track server'). The 'Primary Address Pool' section shows the following details:

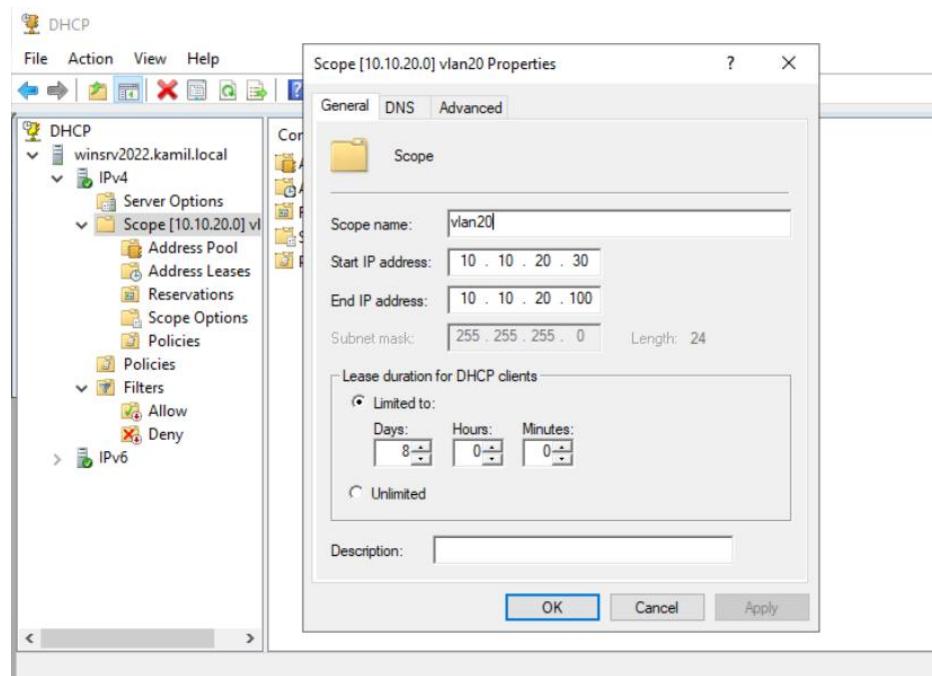
- Subnet: 10.10.20.0/24
- Subnet Range: 10.10.20.1 - 10.10.20.254
- Address Pool Range: From 10.10.20.10 To 10.10.20.100

A note at the bottom of the pool section states: "The specified range for this pool must not be within the range configured on any other address pool for this interface."

Rys. 30 – Wyłączenie usługi DHCP na pfSense dla VLAN20.

Następnie utworzenie nowego Scope w usłudze DHCP na Windows Server 2022.

DHCP → IPv4 → New Scope



Rys. 31 – VLAN20 na Windows Server 2022.

## 4.6. Budowa maszyny klienckiej Windows (Windows 10)

### 4.6.1. Tworzenie maszyny wirtualnej oraz instalacja Windows 10

ID VM: 207

Nazwa: win10

OS: Windows 10 64-bit

Dysk: 100 GB (vm-drives).

CPU: 6 rdzeni.

RAM: 8 GB.

Interfejs sieciowy: podłączony do vmbr1 (LAN) z tagiem VLAN 20.

Add	Remove	Edit	Disk Action	Revert
Memory	8.00 GiB			
Processors	6 (1 sockets, 6 cores) [host]			
BIOS	UEFI			
Display	Default			
Machine	pc-q35-9.2+pve1			
SCSI Controller	VirtIO SCSI single			
Hard Disk (scsi0)	vm-drives:207/vm-207-disk-1.qcow2,iothread=1,size=100G			
Network Device (net0)	rtl8139=BC:24:11:EC:75:EF,bridge=vmbr1,firewall=1,tag=20			
EFI Disk	vm-drives:207/vm-207-disk-0.qcow2,eftype=4m,pre-enrolled-keys=1,size=528K			
TPM State	vm-drives:207/vm-207-disk-2.raw,size=4M,version=v2.0			

Rys. 32 – Konfiguracja maszyny wirtualnej Windows 10.

Name	win10
Start at boot	No
Start/Shutdown order	order=any
OS Type	Microsoft Windows 11/2022/2025
Boot Order	scsi0
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
KVM hardware virtualization	Yes
Freeze CPU at startup	No
Use local time for RTC	Default (Enabled for Windows)
RTC start date	now
SMBIOS settings (type1)	uuid=7f721081-8287-43b1-8542-f6e131038807
QEMU Guest Agent	Enabled
Protection	No
Spice Enhancements	none
VM State storage	Automatic
AMD SEV	Default (Disabled)

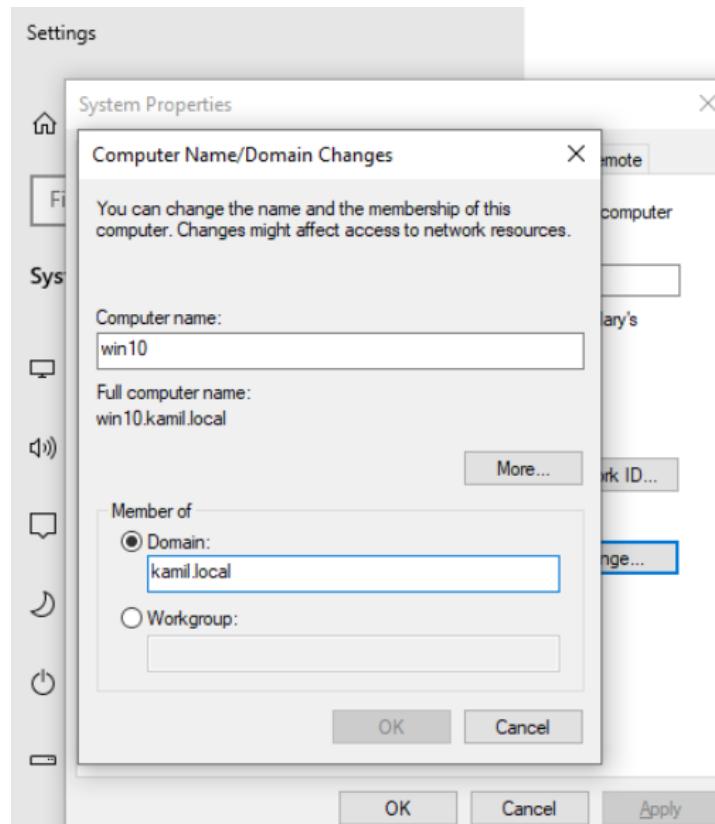
Rys. 33 – Konfiguracja maszyny wirtualnej Windows 10 (2).

Instalacja z ustawieniami domyślnymi. Wystąpiły te same problemy jak w przypadku instalacji Windows Server, czy problem z wykrywaniem dysku oraz adaptera sieciowego.

#### 4.6.2. Podłączenie do domeny oraz weryfikacja poprawności połączenia

Podłączenie do domeny można zrealizować z poziomu:

"This PC" → "Properties" → "Advanced system settings" → "Computer Name" → "Change" → wybrać opcję "Domain" i wprowadź nazwę swojej domeny (kamil.local). Następnie należy podać poświadczenie administratora domeny i konieczny będzie restart systemu.



Rys. 34 – Dołączanie komputera do domeny.

Weryfikacja poprawności połączenia do domeny oraz otrzymania adresacji przez serwer DHCP.

```
C:\Users\kamiliskra>ipconfig /all
Windows IP Configuration

Host Name . . . . . : win10
Primary Dns Suffix . . . . . : kamil.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : kamil.local

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : kamil.local
Description . . . . . : Realtek RTL8139C+ Fast Ethernet NIC
Physical Address . . . . . : BC-24-11-EC-75-EF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::167b:7687:ae18:5943%6(PREFERRED)
IPv4 Address. . . . . : 10.10.20.30(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, August 1, 2025 12:21:42 PM
Lease Expires . . . . . : Saturday, August 9, 2025 12:21:43 PM
Default Gateway . . . . . : 10.10.20.1
DHCP Server . . . . . : 10.10.20.10
DHCPv6 IAID . . . . . : 247211025
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-F9-CD-17-BC-24-11-EC-75-EF
DNS Servers . . . . . : 10.10.20.10
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\kamiliskra>
```

Rys. 35 – Weryfikacja poprawności konfiguracji Windows 10.

## 5. Podsumowanie

Podczas realizacji projektu, zbudowano elastyczną i skalową architekturę sieciową opartą na platformie wirtualizacyjnej Proxmox, wykorzystującą firewall pfSense do segmentacji sieci za pomocą VLANów (VLAN 10 dla Linux/Docker, VLAN 20 dla Windows, VLAN 30 dla narzędzi bezpieczeństwa). Takie podejście nie tylko zapewnia izolację poszczególnych środowisk, ale także otwiera drogę do łatwej rozbudowy o dodatkowe podsieci i komponenty w przyszłości. W trakcie realizacji projektu napotkano na typowe wyzwania techniczne, takie jak problemy z wykrywaniem dysków czy interfejsów sieciowych podczas instalacji systemów Windows na maszynach wirtualnych czy też konieczność specyficznej konfiguracji agenta Wazuh na środowisku Docker. Wszystkie te problemy zostały skutecznie zdiagnozowane i rozwiązane.