

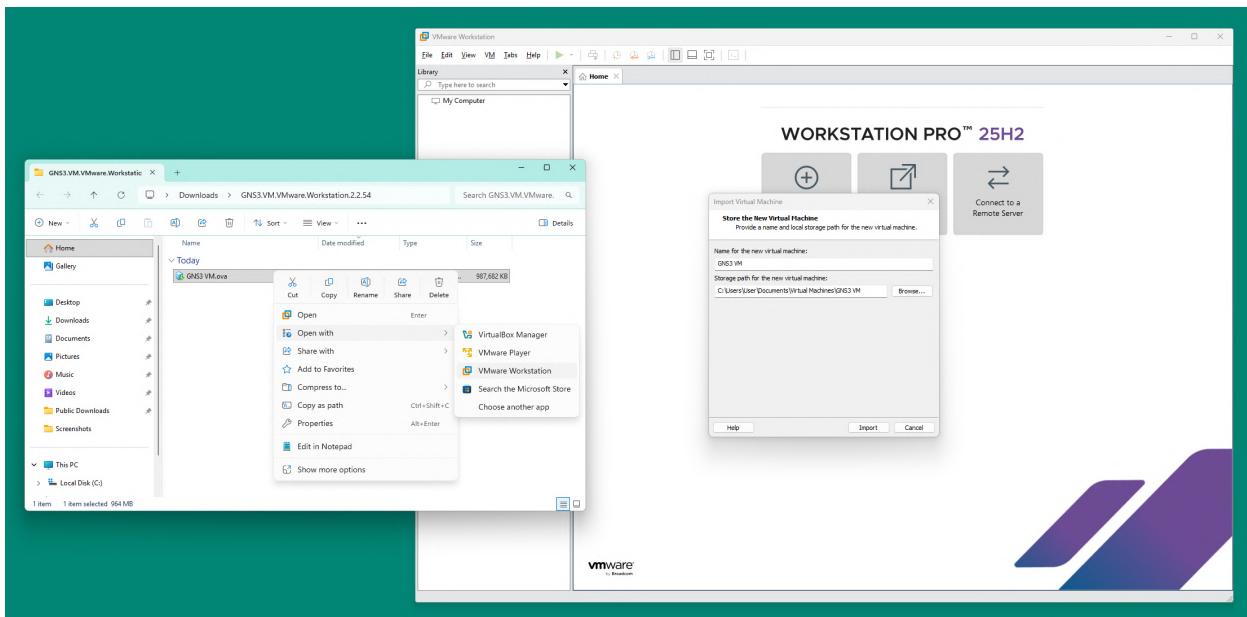
Bartosz Bieniek

gr. 7, st. 1, sem. 3, Informatyka RMS

Zadanie 1. Konfiguracja środowiska GNS3.

Środowisko GNS3 składa się z dwóch głównych komponentów – aplikacji graficznej oraz (opcjonalnej) maszyny wirtualnej GNS3. Zainstalowanie tej drugiej umożliwia między innymi na emulację przeróżnych urządzeń sieciowych, dzięki zawartym w niej dodatkowych narzędziach.

Instalację warto rozpocząć od pobrania maszyny wirtualnej, ponieważ w trakcie konfigurowania środowiska graficznego zostaniemy poproszeni o wskazanie istniejącej GNS3 VM. Istnieje możliwość wyboru obrazu dla środowiska Virtual Box, jednak wykorzystywana przez GNS3 zagnieźdzona wirtualizacja może nie być obsługiwana lub działać bardzo powoli. Z tego powodu wybrałem wersję pod VMware Workstation.

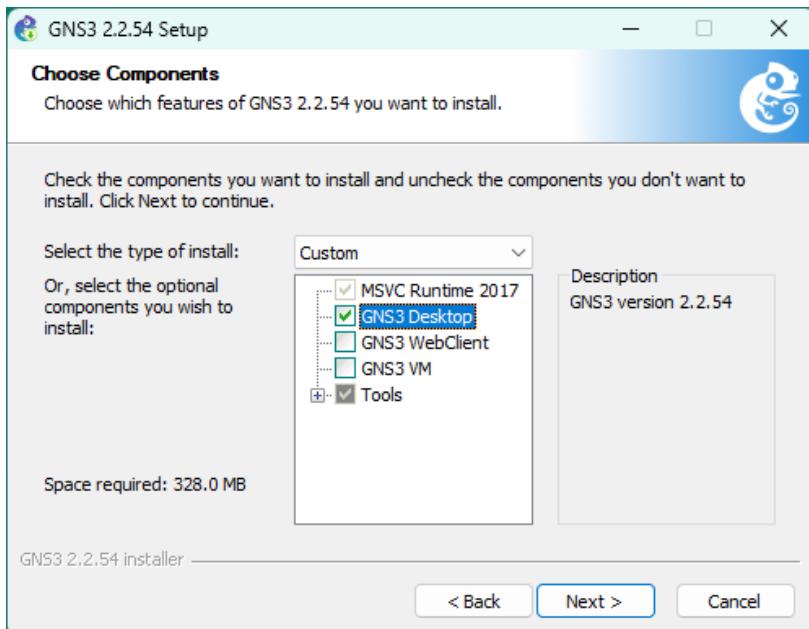


Zrzut ekranu 1 Import maszyny wirtualnej GNS3 VM do VMware Workstation Pro.

Pobraną maszynę wirtualną możemy zaimportować do VMware Workstation, klikając na plik .ova prawym myszy i wybierając „Open with VMWare Workstation”.

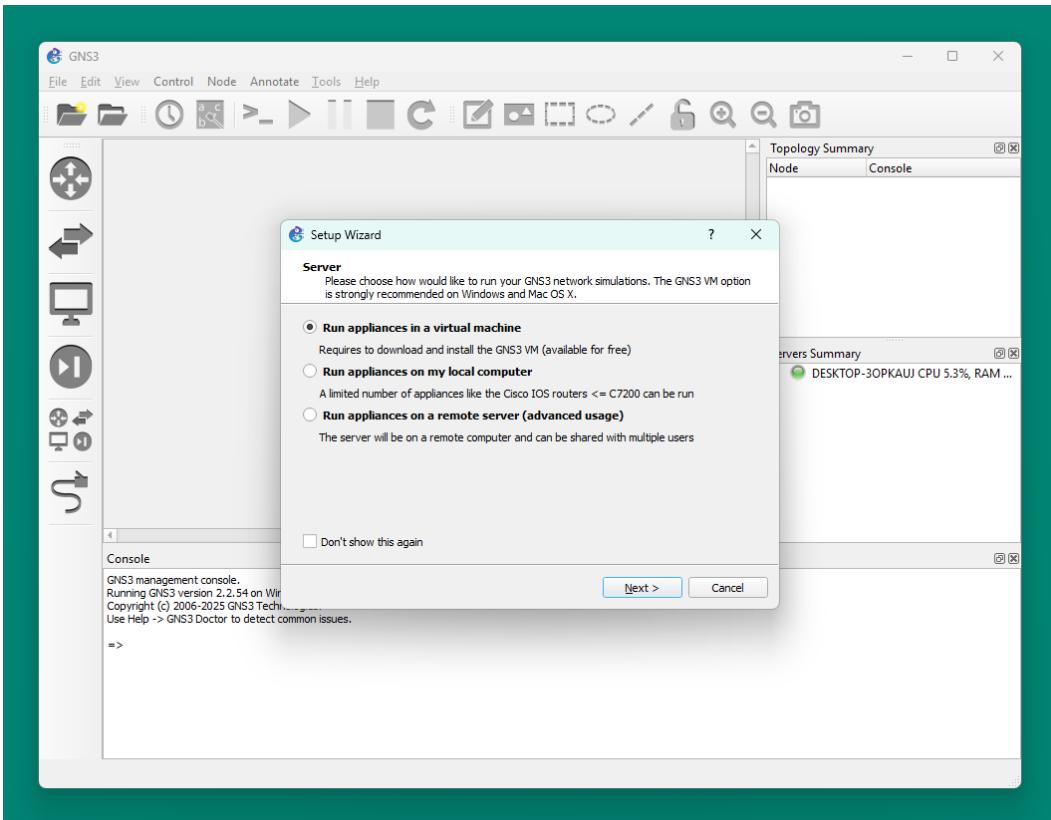
Aby przydzielić zasoby sprzętowe, należy po imporcie wejść w ustawienia maszyny i dobrać parametry w zależności od potrzeb. Na „czystą” GNS3 VM należy przewidzieć co najmniej 700 MB pamięci RAM, plus po około 500 MB na każdy działający w niej kontener. Ponieważ planuję wykorzystać trzy kontenery i kilka urządzeń sieciowych, zdecydowałem się przydzielić 4 GB pamięci oraz 4 rdzenie procesora.

Następnie uruchomiłem instalator „GNS3 All-in-one”, zaznaczając jedynie instalację aplikacji GNS3 Desktop oraz niezbędnych narzędzi. W trakcie procesu będą otwierały się programy instalacyjne dodatkowych narzędzi, które wystarczy jedynie „przeklikać”.



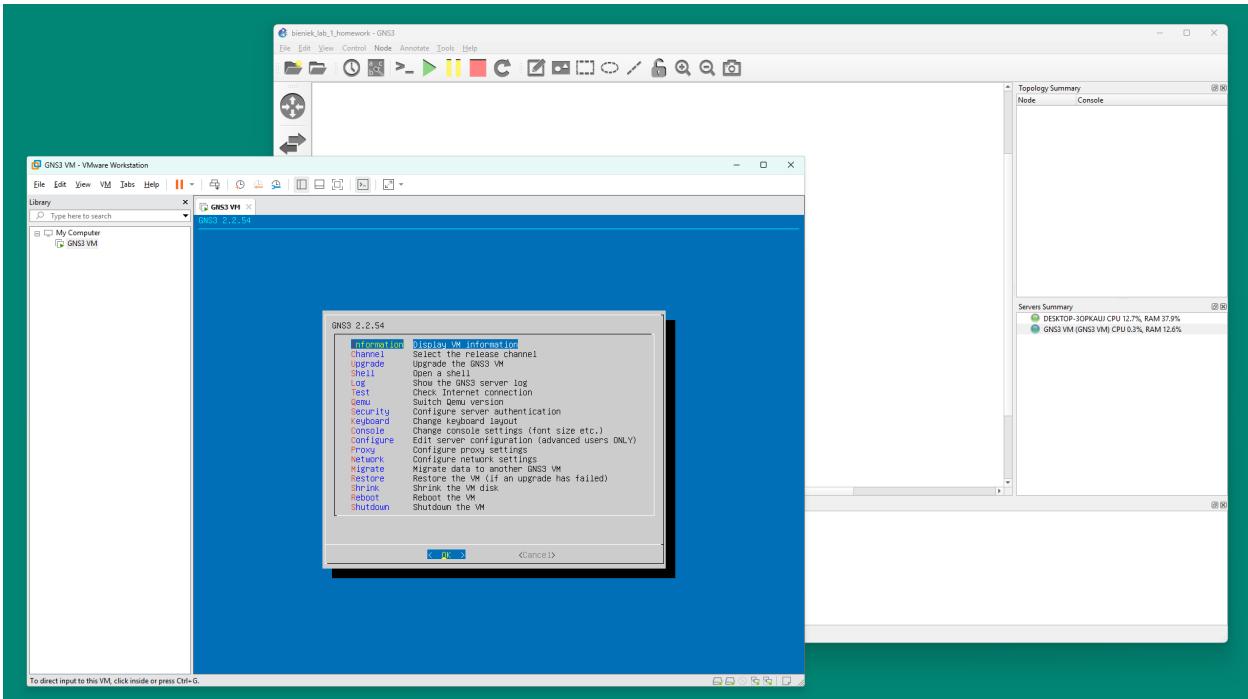
Zrzut ekranu 2 Wybór komponentów w instalatorze GNS3 All-in-one.

Przy pierwszym uruchomieniu programu GNS3 wyświetli się „Setup Wizard”, pozwalający skonfigurować najważniejsze opcje. W pierwszym kroku należy zaznaczyć uruchamianie wirtualnych urządzeń sieciowych wewnętrz GNS3 VM (oczywiście jeżeli ją zainstalowaliśmy), a następnie wybrać z listy jej nazwę. Pozwoli to na automatyczne startowanie maszyny wirtualnej razem ze środowiskiem GNS3.



Zrzut ekranu 3 Wybór sposobu uruchamiania symulacji sieciowych.

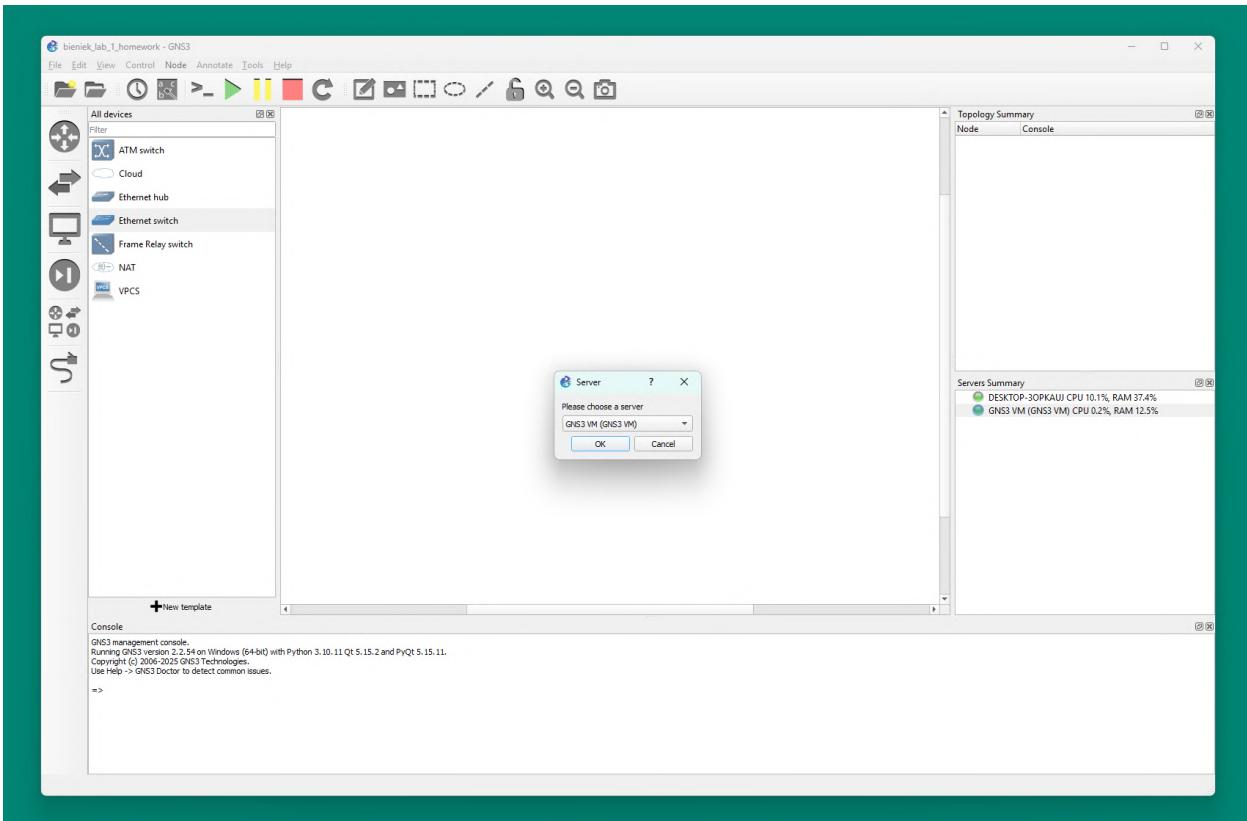
Po tak przeprowadzonej instalacji, maszyna wirtualna GNS3 VM powinna automatycznie wystartować.



Zrzut ekranu 4 Maszyna wirtualna GNS3 VM uruchomiona w programie VMware Workstation Pro.

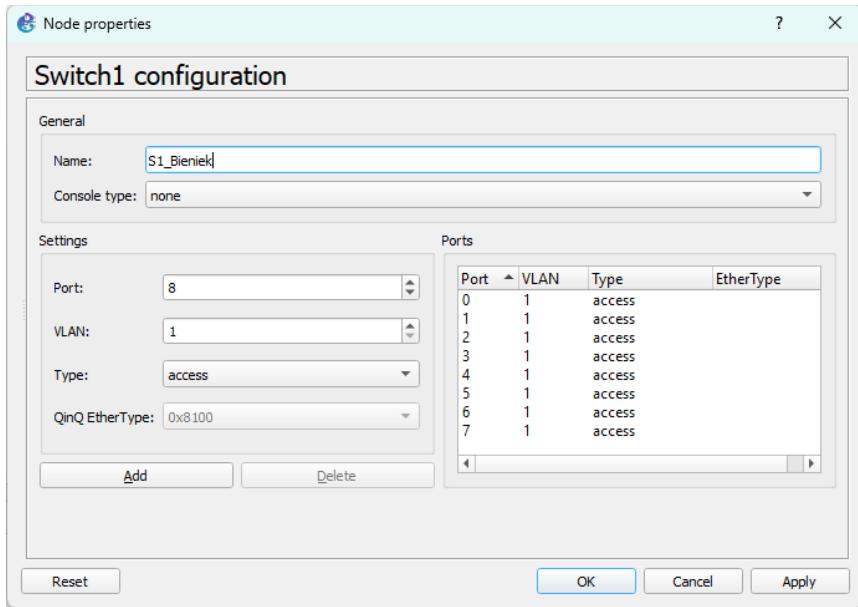
Zadanie 2. Utworzenie topologii sieciowej.

Rozpoczniemy od dodania przełącznika sieciowego. Przeciągając wybrane urządzenie z zasobnika do edytora, zostaniemy zapytani o „serwer” który ma je obsłużyć. Ponieważ planuję uruchamiać inne urządzenia i kontenery wewnątrz GNS3 VM, wybiorę tę właśnie opcję, aby uniknąć problemów z ich komunikacją.



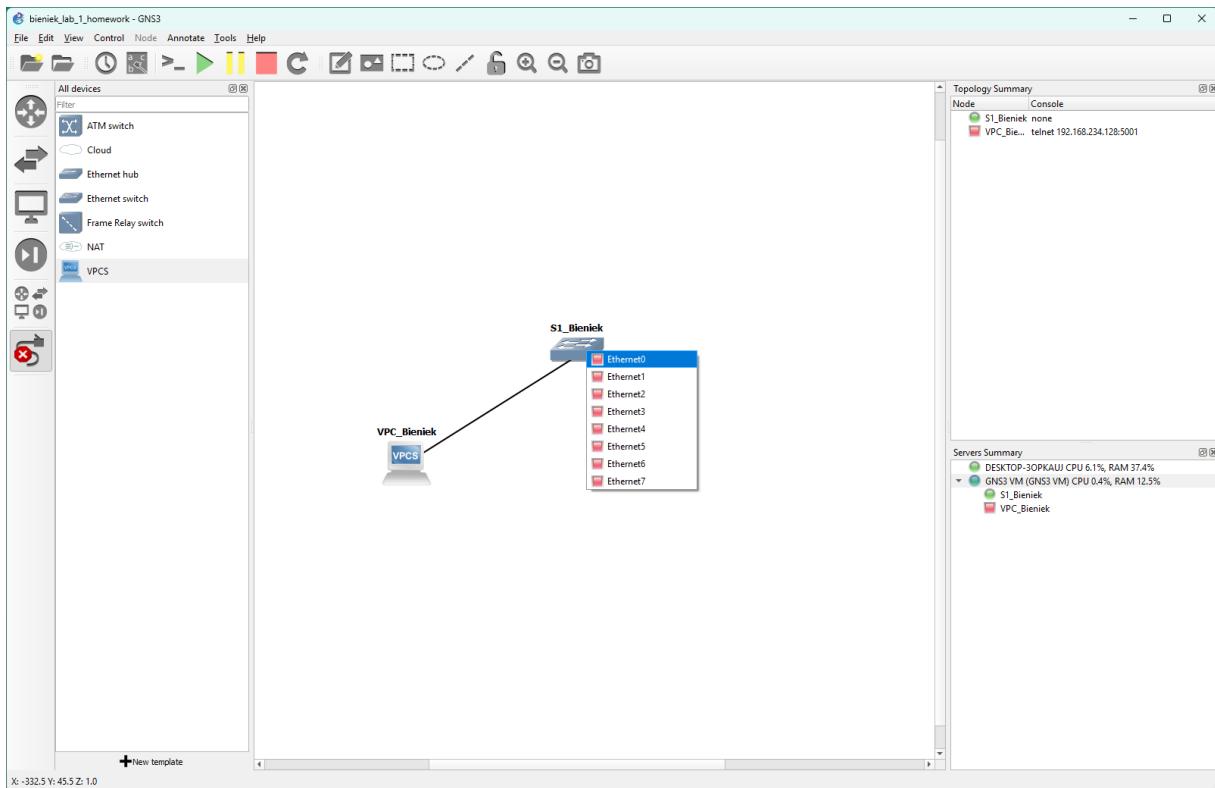
Zrzut ekranu 5 Otwarty zasobnik z urządzeniami sieciowymi oraz pytanie o wybór serwera, do którego ma zostać dołączony przełącznik sieciowy.

Ilość portów, wirtualnych sieci (VLAN) oraz opis urządzenia można dowolnie zmieniać, klikając na nie prawym przyciskiem myszy i wybierając opcję „Configure”.



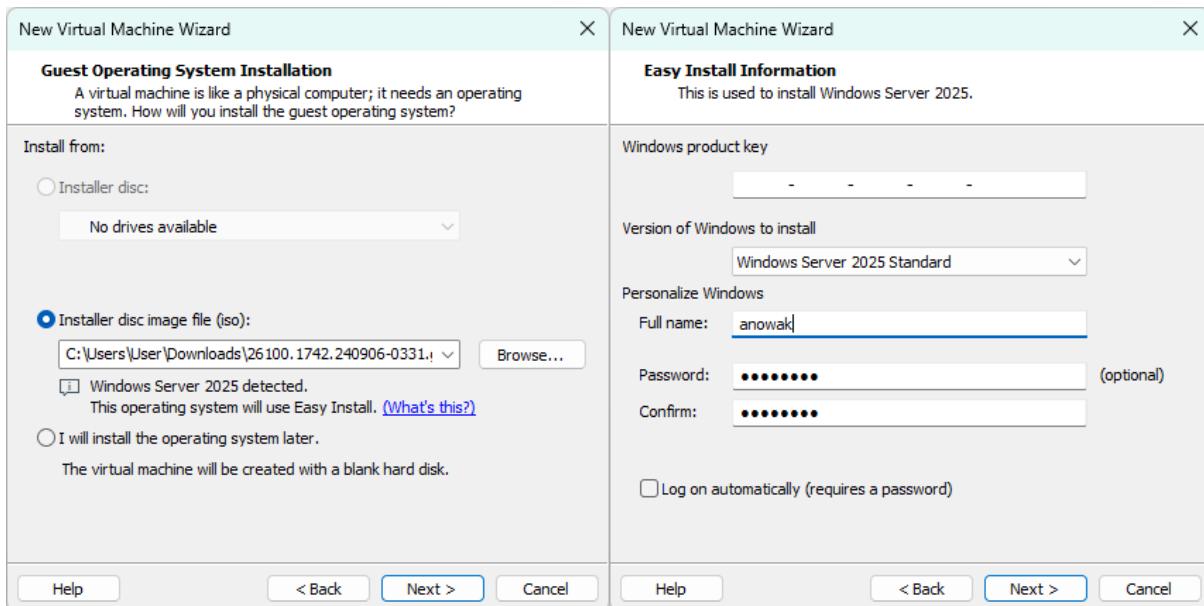
Zrzut ekranu 6 Konfiguracja przełącznika sieciowego w GNS3.

W identyczny sposób dodałem również wirtualny komputer (VPC), który podłączyłem kablem do portu *Ethernet0* na przełączniku. Takie urządzenie zawiera jedynie najpotrzebniejsze narzędzia sieciowe, które pozwalają między innymi na prostą konfigurację jego adresu, pobranie danych z usługi DHCP, czy ustawienie adresu serwera DNS.



Zrzut ekranu 7 Podłączanie VPC (wirtualnego komputera) do przełącznika sieciowego.

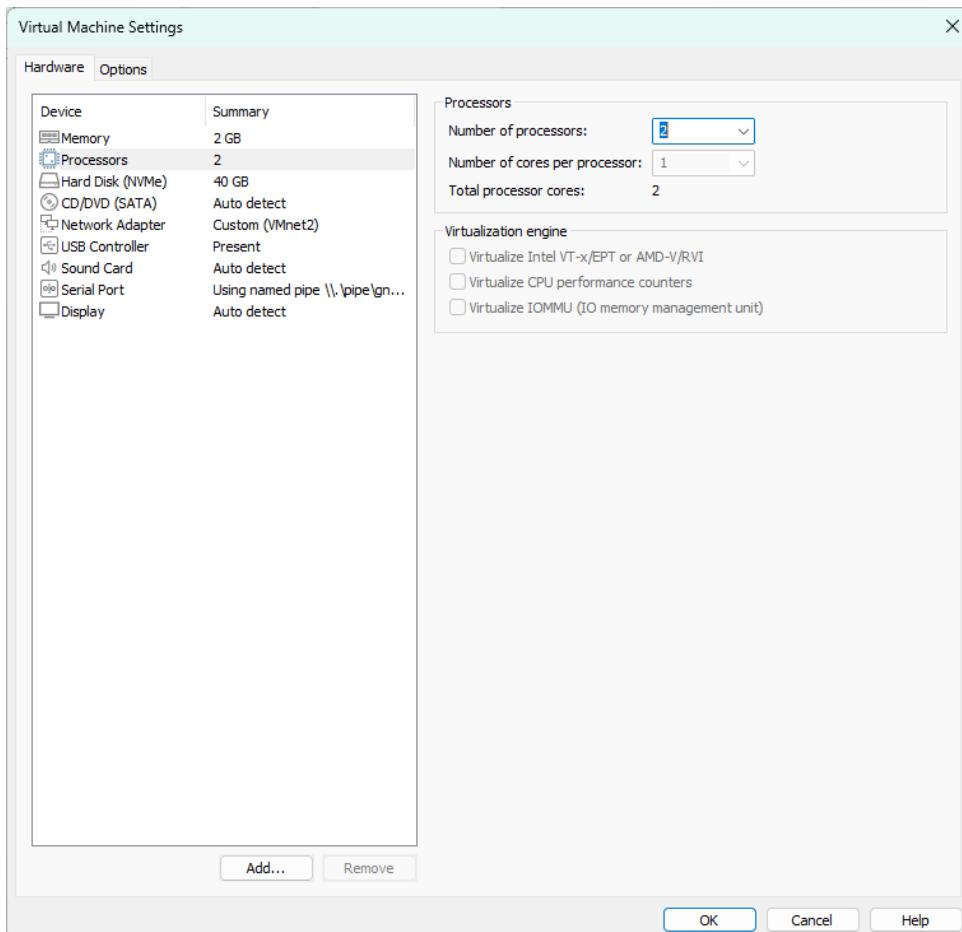
Dodajmy teraz do GNS maszynę wirtualną z systemem Windows Server 2025, wykorzystując w tym celu oprogramowanie VMware Workstation. Z górnego menu narzędzia do wirtualizacji wybieramy „File” → „New Virtual Machine” i zaznaczamy konfigurację „Typical”. W kolejnym kroku wybieramy lokalizację obrazu systemu z dysku. Kreator automatycznie rozpoznał system Windows Server 2025, dzięki czemu w następnym kroku będziemy mogli zawczasu podać klucz licencyjny, wersję systemu, czy login i hasło użytkownika. W trakcie instalacji te dane zostaną automatycznie uzupełnione, co pozwala zaoszczędzić czas.



Zrzut ekranu 8 Konfiguracja procesu instalacji przy użyciu rozwiązania Easy Install.

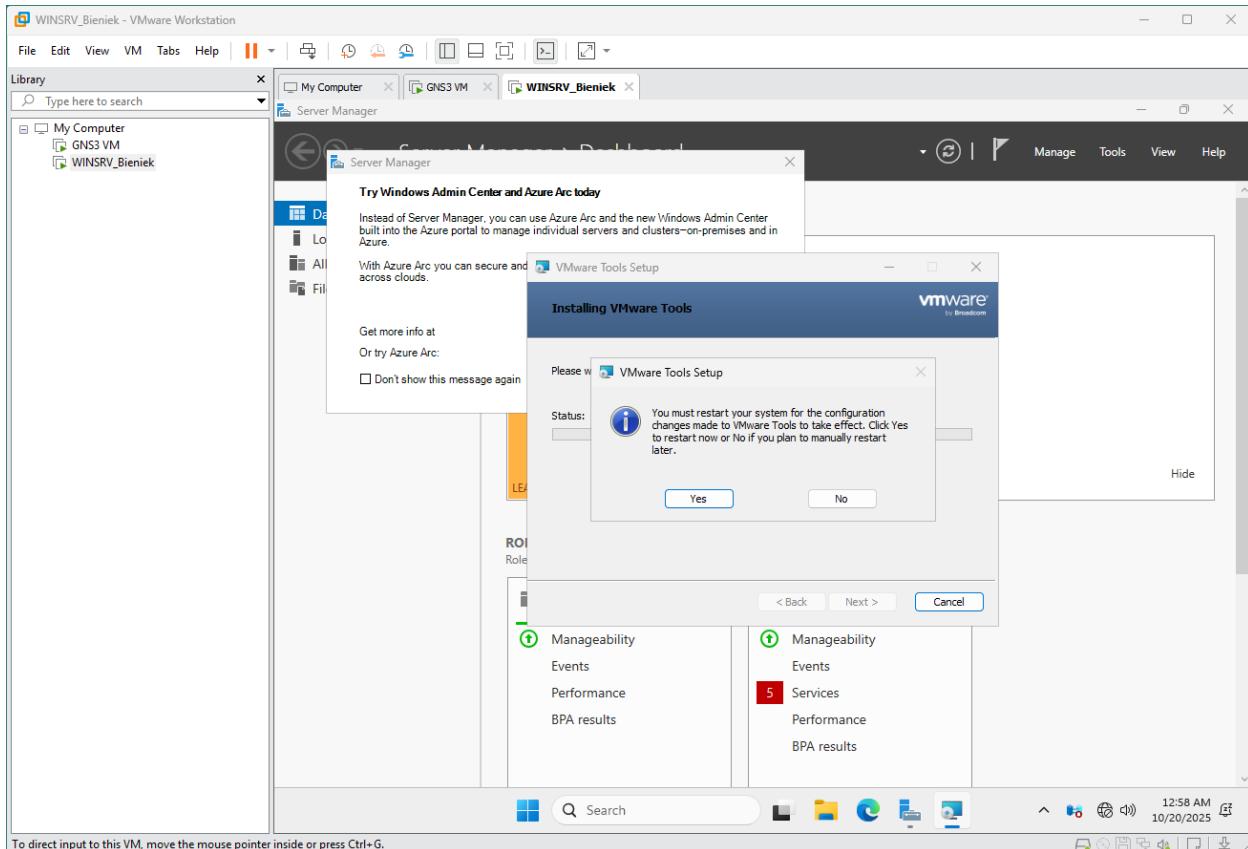
Na koniec podajemy nazwę i lokalizację zapisu plików VM oraz przydzielamy przestrzeń dyskową.

Za pomocą przycisku „Customize Hardware...” możemy przejść do szczegółowej konfiguracji sprzętu, aby na przykład zwiększyć ilość przydzielonej pamięci RAM, czy ilość procesorów. Minimalnym wymaganiem systemu Windows Server 2025 jest 2 GB, stąd pozostaną przy takiej wartości, aby zmieścić się jeszcze z pozostałymi maszynami. Zwiększę jednak ilość przydzielonych procesorów do dwóch.



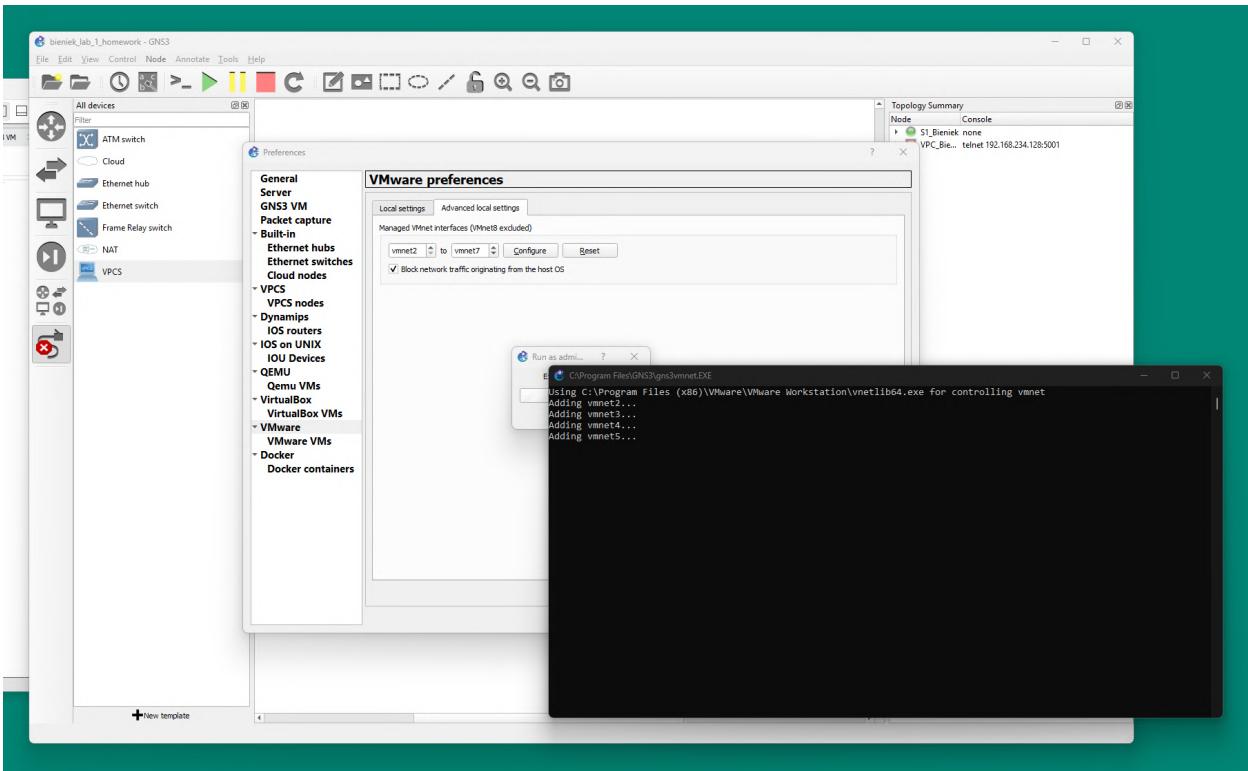
Zrzut ekranu 9 Konfiguracja zasobów sprzętowych maszyny wirtualnej z systemem Windows Server 2025.

Następnie zapisujemy zmiany, uruchamiamy maszynę wirtualną i przechodzimy proces instalacji systemu. Po jej zakończeniu i uruchomieniu się systemu, VMware Workstation automatycznie instaluje dodatki gościa pozwalające na współdzielenie schowka, synchronizację czasu, czy ulepszone przechodzenie kurSORA i klawiatury między systemem gościa i gospodarza.



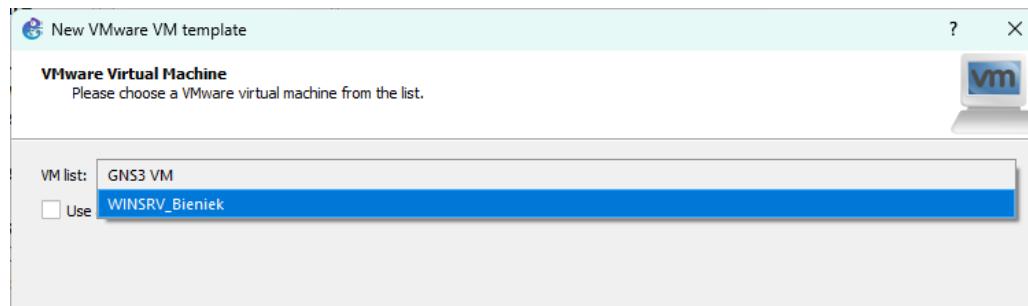
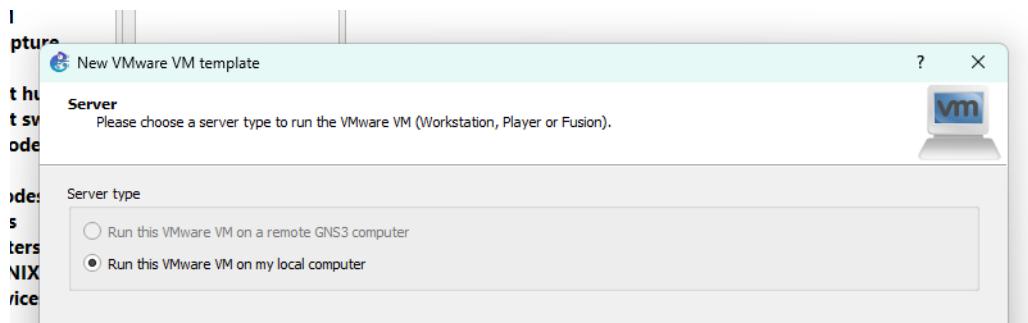
Zrzut ekranu 10 System Windows Server 2025 po zakończeniu instalacji.

Zanim dodamy tak utworzoną maszynę wirtualną do GNS, musimy w pierwszej kolejności skonfigurować interfejsy sieciowe, dzięki którym będzie odbywała się między nimi komunikacja. W tym celu z górnego menu wybieramy „Edit” → „Preferences” → „VMware” → „Advanced local settings” i wybieramy zakres sieci, które zostaną do tego celu wykorzystane. Sieci `vmnet1` oraz `vmnet8` są już zajęte, stąd wybór zakres od `vmnet2` do `vmnet7` włącznie, co w zupełności pozwoli mi na zrealizowanie zadania. Ponieważ wskazane sieci jeszcze nie istnieją, wybieramy „Configure”, które automatycznie je utworzy.



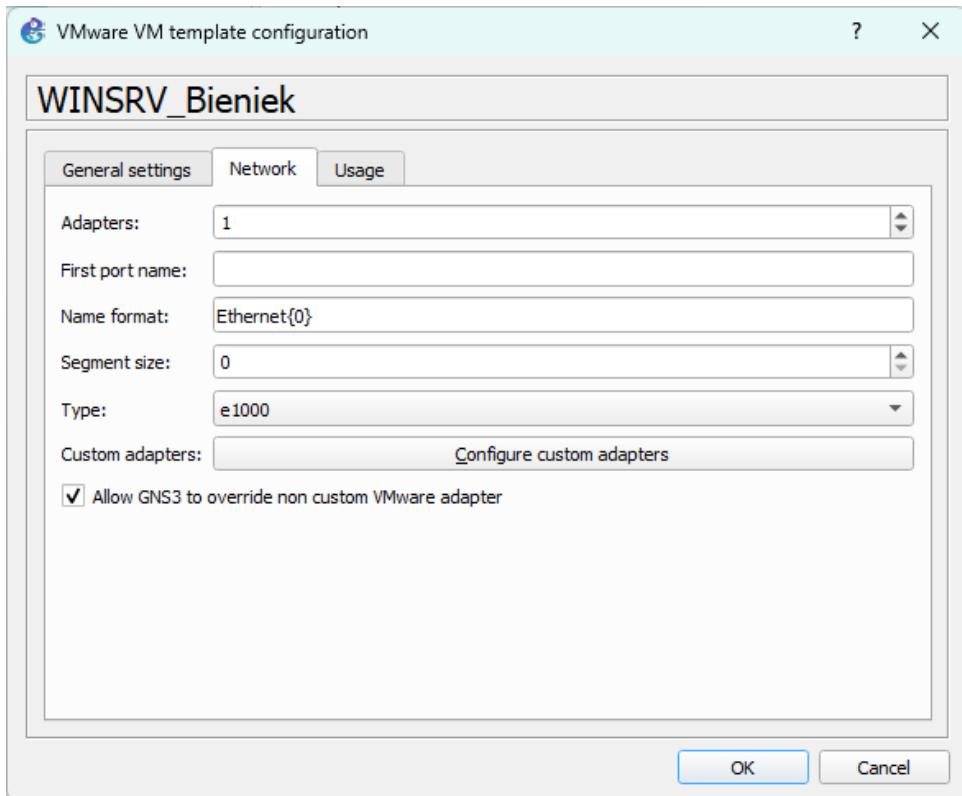
Zrzut ekranu 11 Tworzenie sieci wirtualnych dla maszyn wirtualnych działających pod VMware Workstation.

Teraz możemy już dodać wcześniejszą utworzoną maszynę wirtualną. W tym celu przechodzę do zakładki „VMware VMs” w prawym panelu i wybieram opcję „New” na dole okna. Następnie przechodzę przez kreator wybierając po drodze z listy odpowiednią maszynę.



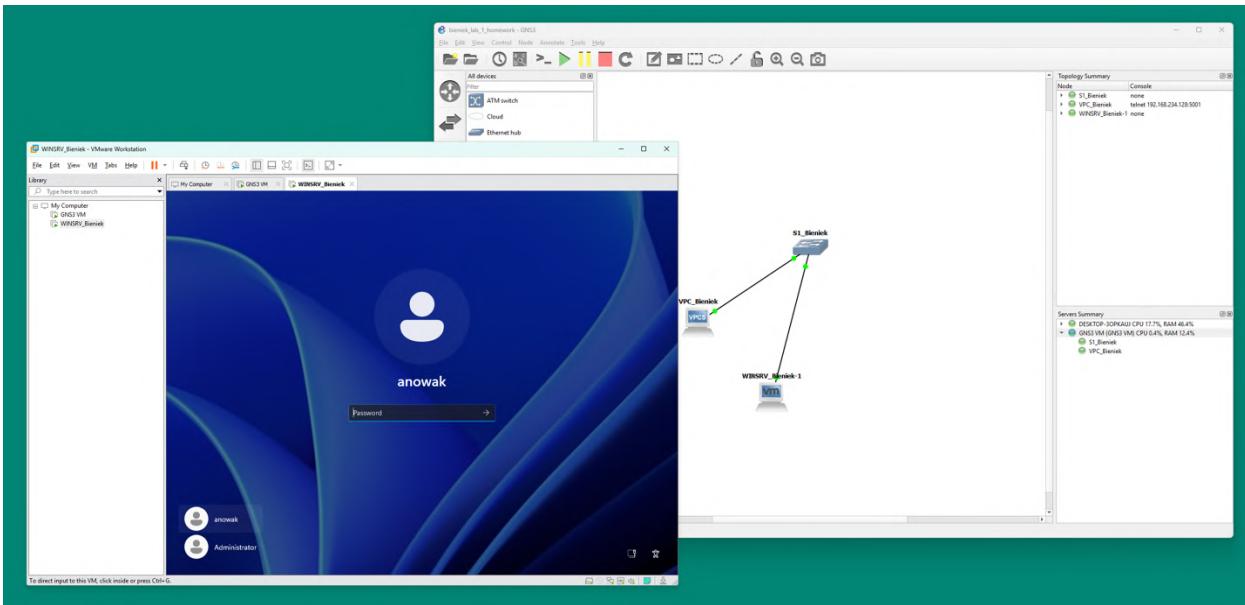
Zrzut ekranu 12 Kreator szablonu maszyny wirtualnej uruchamianej pod VMware Workstation Pro w GNS3.

Aby umożliwić komunikację sieciową między GNS-em, a maszynami wirtualnymi tworzonymi według zdefiniowanego właśnie szablonu, należy w opcjach szablonu (otwartych poprzez kliknięcie „Edit” na dole okna) zaznaczyć „Allow GNS3 to override non custom VMware adapter.



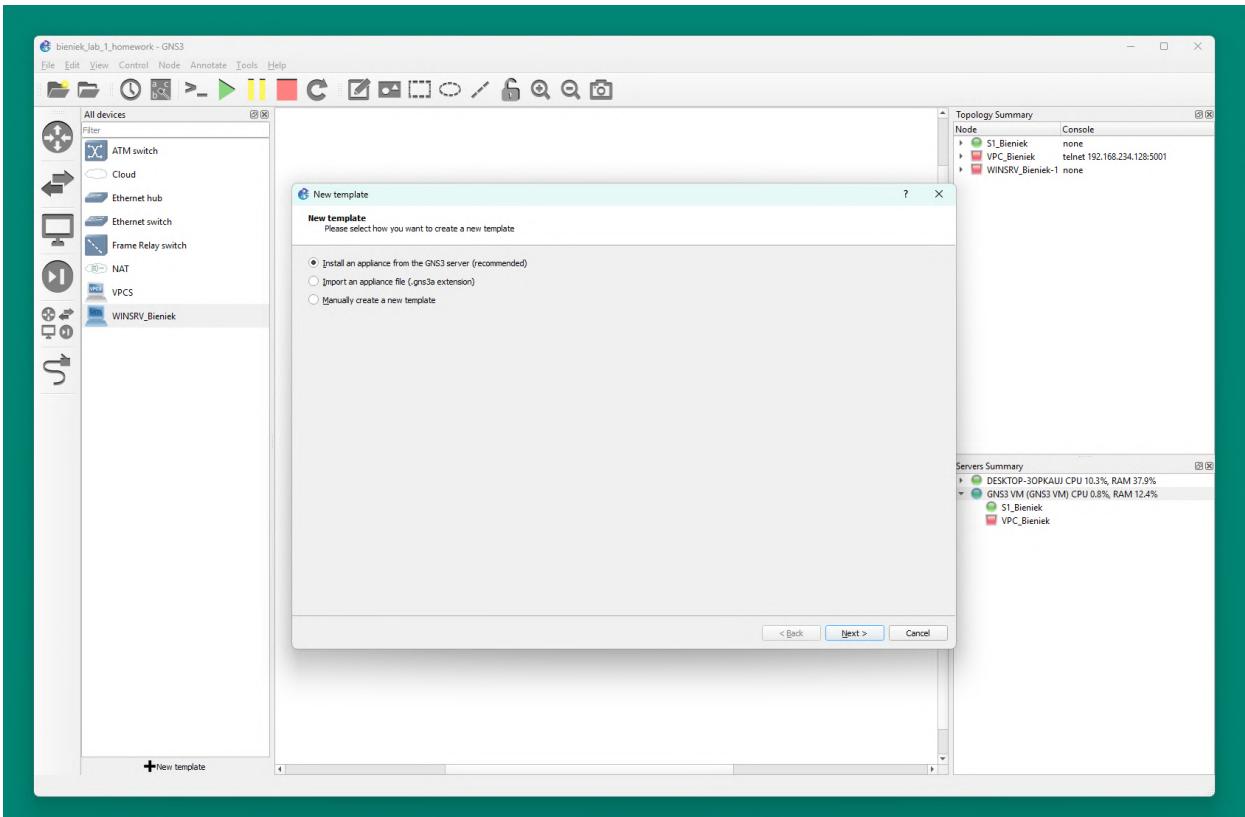
Po zapisaniu konfiguracji przyciskiem „OK” i wyjściu z ustawień, możemy teraz dodać maszynę wirtualną do naszej sieci. Postępujemy w identyczny jak wcześniej sposób – z lewego panelu wybieramy odpowiedni szablon, przeciągamy go na planszę i łączymy kablem.

Aby uruchomić maszynę wirtualną, w **programie GNS** klikamy prawym myszy na urządzenie i wybieramy „Start”. Gdybyśmy zrobili to z poziomu programu do wirtualizacji, GNS nie wykryłby, że maszyna działa i nie moglibyśmy się do niej podłączyć.



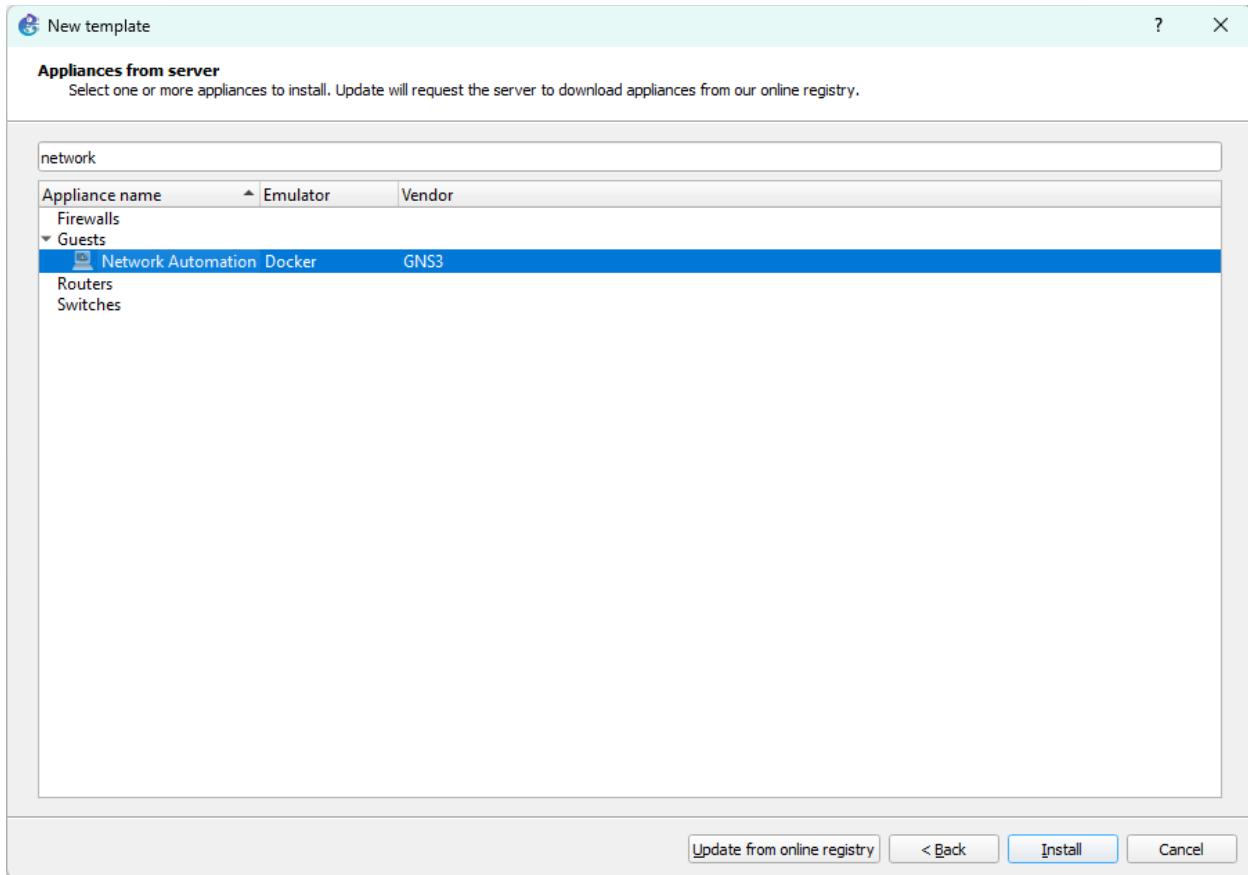
Zrzut ekranu 13 Uruchomiona z poziomu GNS maszyna wirtualna z systemem Windows Server 2025.

Do naszej sieci dodamy następnie kontener Network Automation, który znajduje się na serwerze GNS3. W tym celu klikamy w „New template” na dole lewego panelu i wybieramy „Install an appliance from the GNS3 server (recommended)”.



Zrzut ekranu 14 Instalacja kontenera znajdującego się na serwerze GNS3.

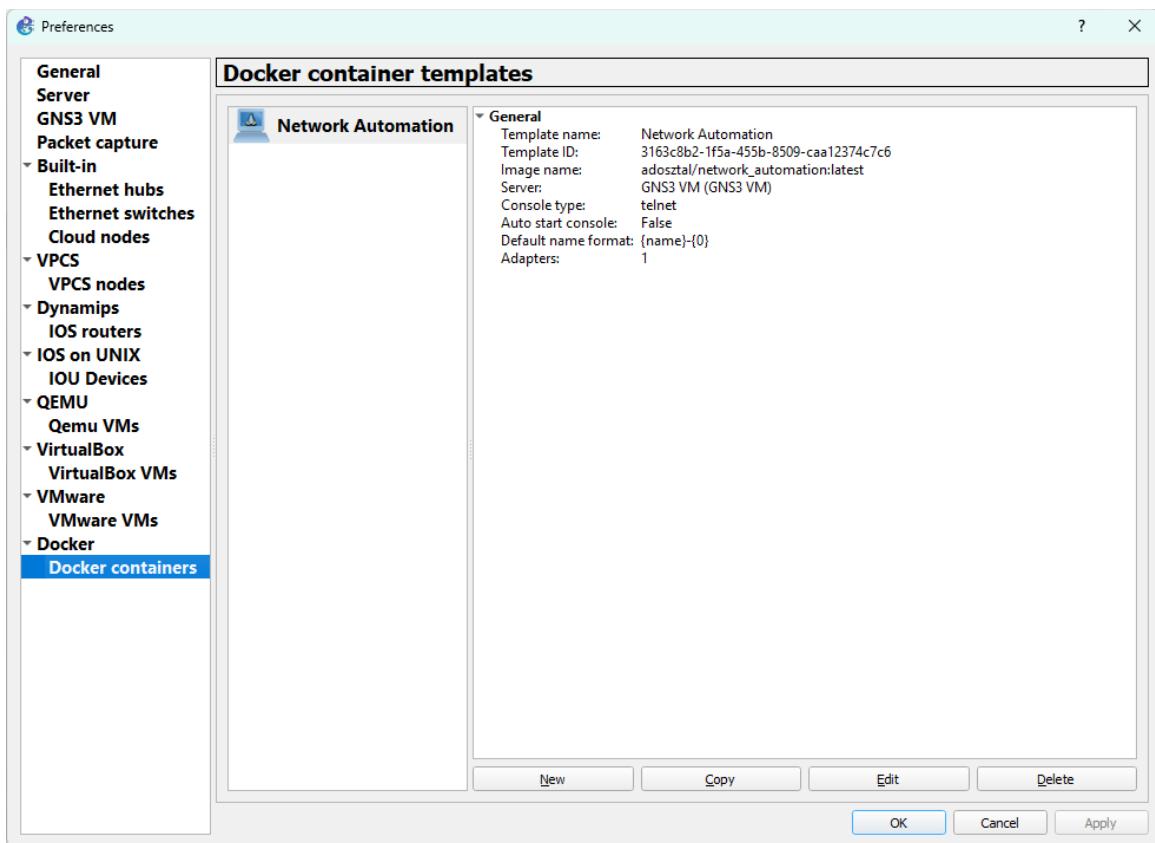
Następnie odszukujemy na liście odpowiednią pozycję (możemy skorzystać z pola wyszukiwania na górze okna) i klikamy „Install”.



Zrzut ekranu 15 Kontener "Network Automation" widoczny na liście pobranej z serwera GNS3.

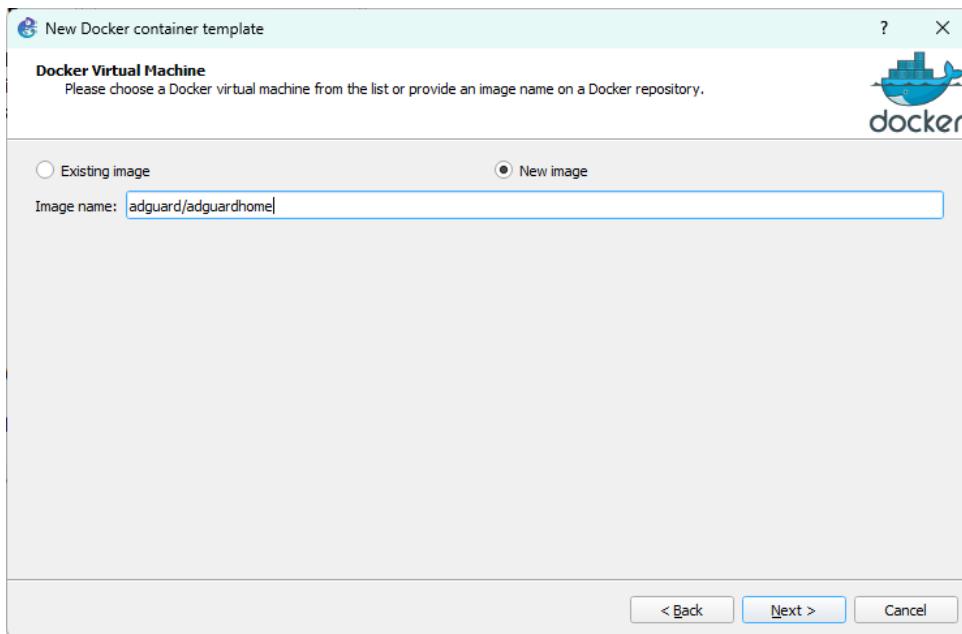
Tak utworzone urządzenie przeciągamy na planszę i łączymy kablem do kolejnego wolnego w przełączniku portu.

Nieco inaczej będzie wyglądał proces instalacji własnego kontenera, na przykład *adguardhome*. W tym celu wybieramy „New template” → „Manually create a new template”, które przeniesie nas do zakładki „Docker” w ustawieniach.



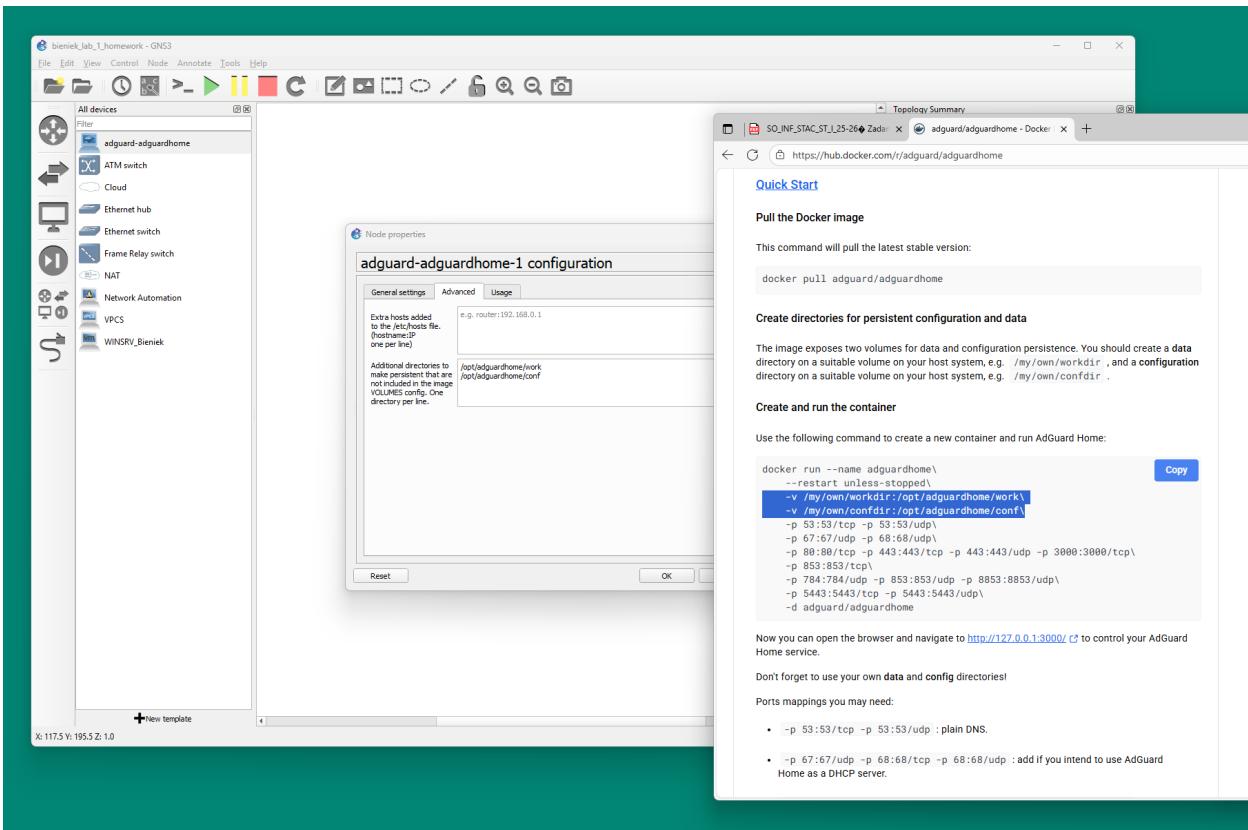
Zrzut ekranu 16 Zakładka "Docker" w ustawieniach projektu. Widoczny jest wcześniej dodany kontener.

Na dolnym pasku klikamy „New” i przechodzimy do drugiego kroku, w którym wybieramy opcję „New image” oraz wpisujemy nazwę obrazu. Aby ją poznać, możemy wykorzystać rejestr Dockera, znajdujący się pod adresem <https://hub.docker.com>.



Zrzut ekranu 17 Wybór nazwy obrazu kontenera do pobrania.

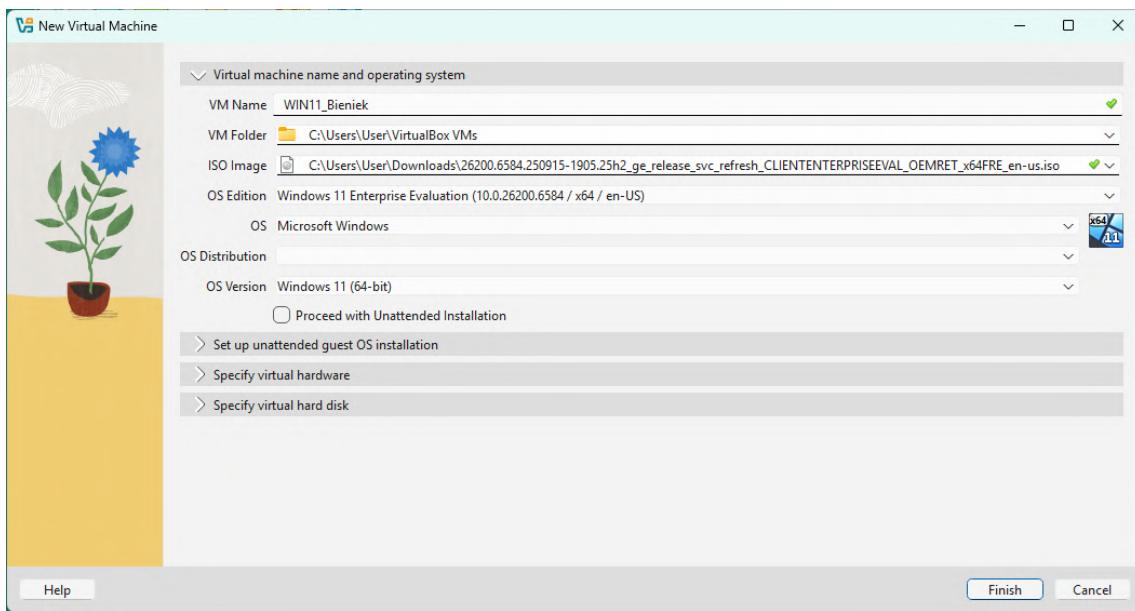
Przechodzimy przez resztę konfiguratora nie dokonując żadnych zmian. Uruchamiane przy pomocy Dockera kontenery są tworzone za każdym razem od nowa, co powoduje, że tracimy zapisane w nim dane. W GNS3 istnieje jednak opcja pozwalająca na automatyczne zapisywanie i przywracanie zawartości pod wskazaną w kontenerze ścieżką, w przypadku gdy nie zostało to już skonfigurowane w obrazie. W tym celu z dolnego paska wybieramy „Edit”, przechodzimy do zakładki „Advanced” i wypełniamy pole „Additional directories to make persistent [...]”. Aby poznać konkretne ścieżki pod którymi zapisywane są przez daną aplikację dane, musimy sprawdzić jej konfigurację. W przypadku adguardhome, są to foldery `/opt/adguardhome/work` i `/opt/adguardhome/conf`.



Zrzut ekranu 18 Konfiguracja folderów, których zawartość będzie przechowywana nawet po starcie nowego kontenera. Wycinek z dokumentacji aplikacji, prezentujący ścieżki zapisu danych.

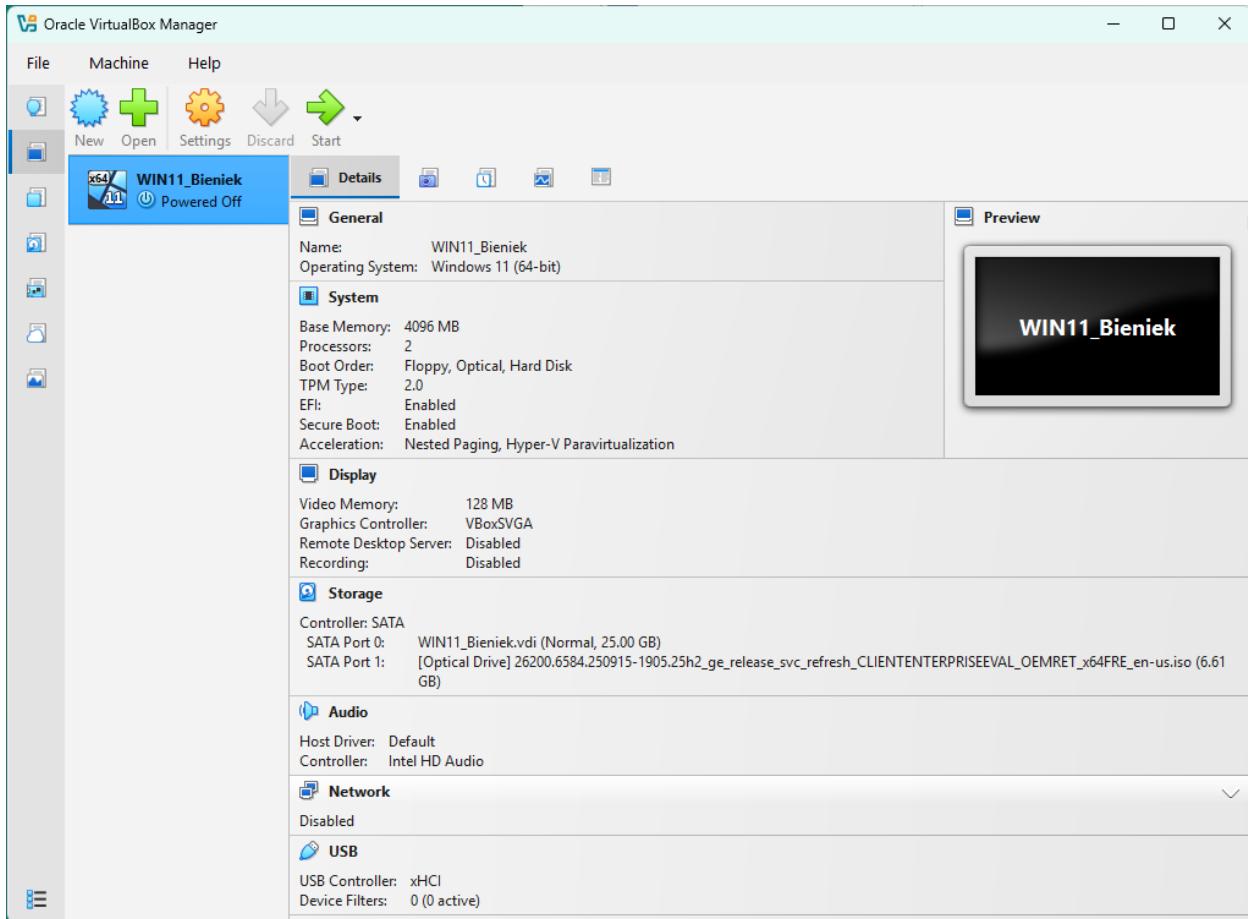
W sposób identyczny jak wcześniej, podłączamy do naszej sieci kontener. Na koniec dodamy do jeszcze maszynę wirtualną z Windowsem 11 Enterprise, działającą pod oprogramowaniem Oracle VirtualBox.

Z górnego paska wybieramy opcję „New” i podajemy nazwę maszyny, lokalizację zapisu, wybieramy obraz systemu oraz przydzielamy ilość pamięci RAM i przestrzeń dyskową. Minimalnym wymaganiem co do pamięci operacyjnej systemu Windows 11 są 4 GB, stąd tyle właśnie przydzielę. Ograniczę również wielkość dysku do 25 GB.



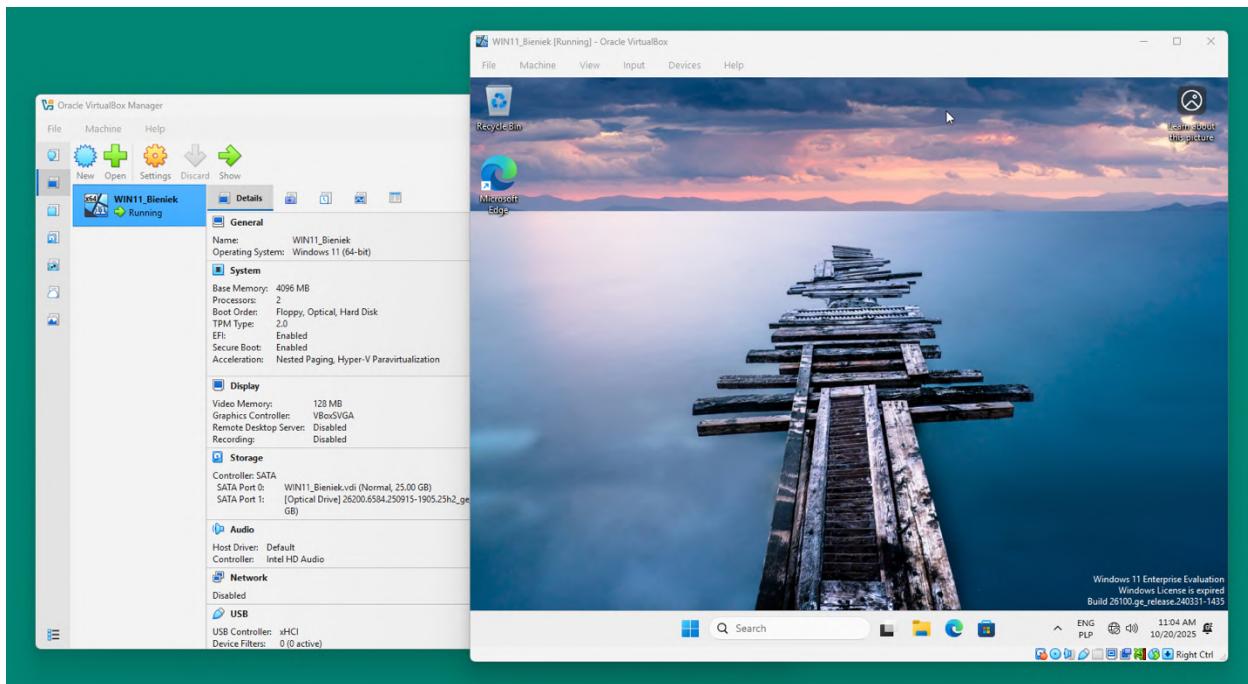
Zrzut ekranu 19 Konfiguracja nazwy maszyny wirtualnej, folderu, w którym zostanie zapisana oraz wybór obrazu systemu.

Ze względu na to, że będę chciał w trakcie instalacji utworzyć konto lokalne, zawczasu wyłączę adapter sieciowy w ustawieniach maszyny wirtualnej.



Zrzut ekranu 20 Podsumowanie konfiguracji maszyny wirtualnej z systemem Windows 11 Enterprise w Oracle VirtualBox.

Następnie przechodzę przez proces instalacji systemu.

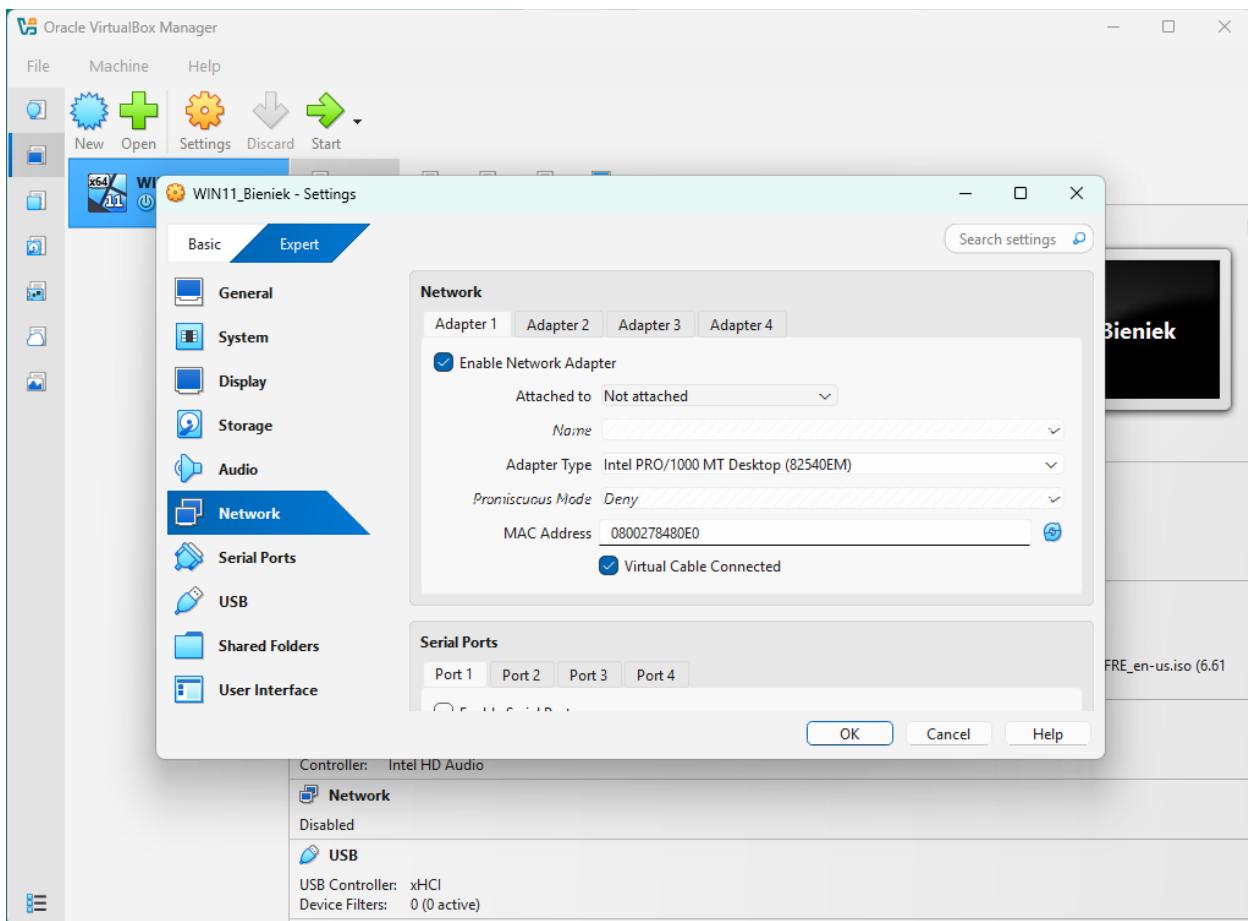


Zrzut ekranu 21 Zainstalowany system Windows 11 Enterprise.

Istnieją dwie opcje podłączenia utworzonej w VirtualBox maszyny wirtualnej do sieci w GNS.

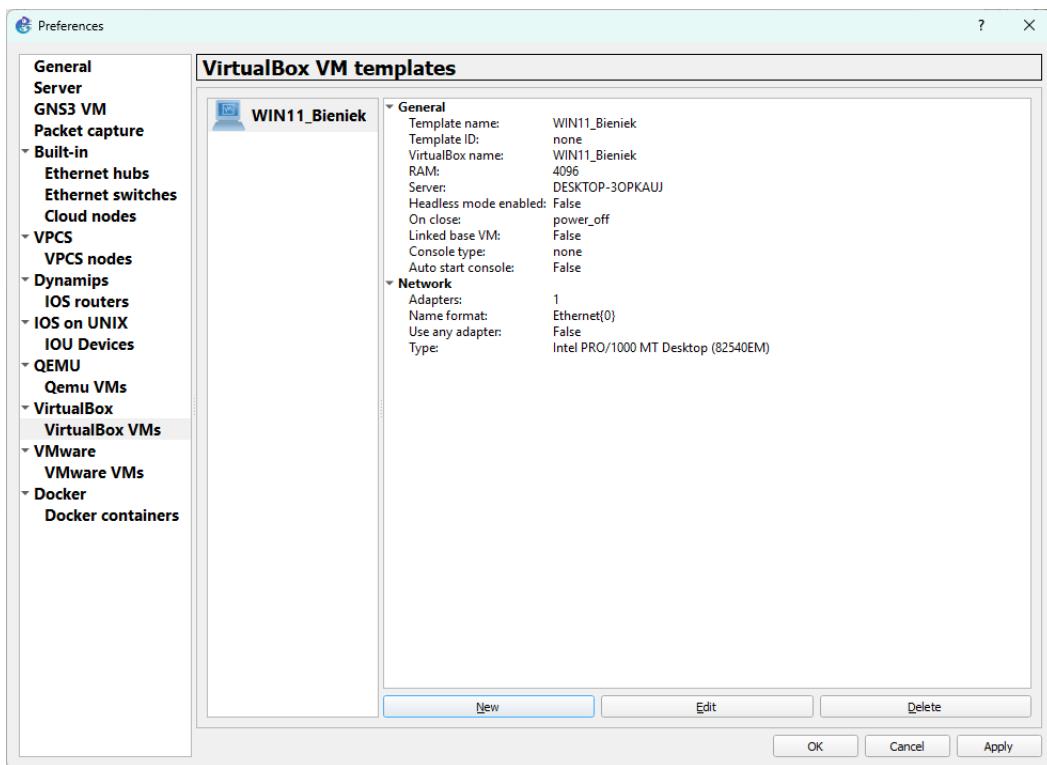
1. Wybrać opcję „Not attached” w ustawieniach adaptera, wówczas GNS sam rozpozna wolny interfejs i się do niego podłączy.
2. Wybrać opcję „Host-only Adapter”, wybrać (lub utworzyć nową) sieć typu Host-only i skorzystać z obiektu chmury w GNS.

Na potrzeby tego zadania skorzystam z pierwszej opcji.



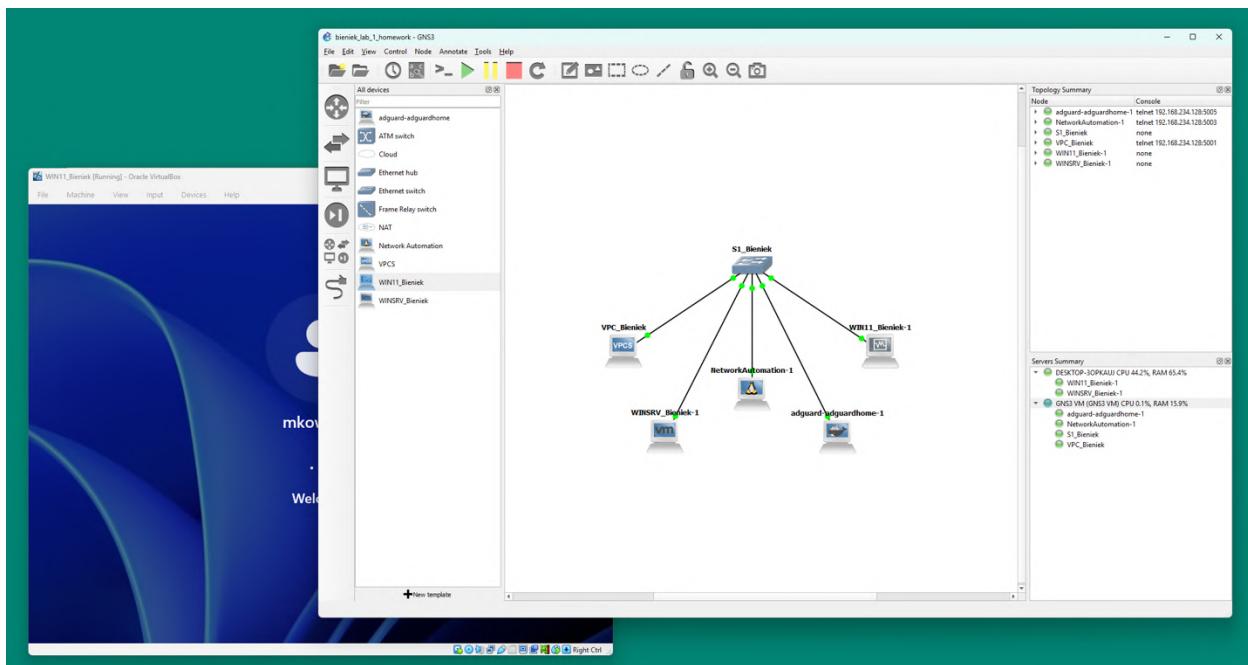
Zrzut ekranu 22 Ustawienie adaptera w trybie "Not attached" w ustawieniach maszyny wirtualnej w VirtualBox.

Aby dodać tak utworzoną maszynę wirtualną do GNS, należy ponownie wejść w „Edit” → „Preferences” → „VirtualBox VMs” i kliknąć przycisk „New”. W kolejnych krokach należy z listy wybrać nazwę utworzonej przed chwilą VM i zakończyć konfigurację przyciskiem „Finish”.



Zrzut ekranu 23 Podsumowanie szablonu maszyny wirtualnej VirtualBox w ustawieniach GNS.

Możemy teraz dodać maszynę wirtualną do sieci przeciągając ją na planszę, połączyć kablem do przełącznika i uruchomić wybierając opcję „Start” z menu kontekstowego, dostępnego po kliknięciu prawym przyciskiem myszy na urządzenie.



Zrzut ekranu 24 Utworzona topologia sieciowa. Widoczna w tle uruchamiająca się maszyna wirtualna z systemem Windows 11 Enterprise, działająca pod oprogramowaniem VirtualBox.

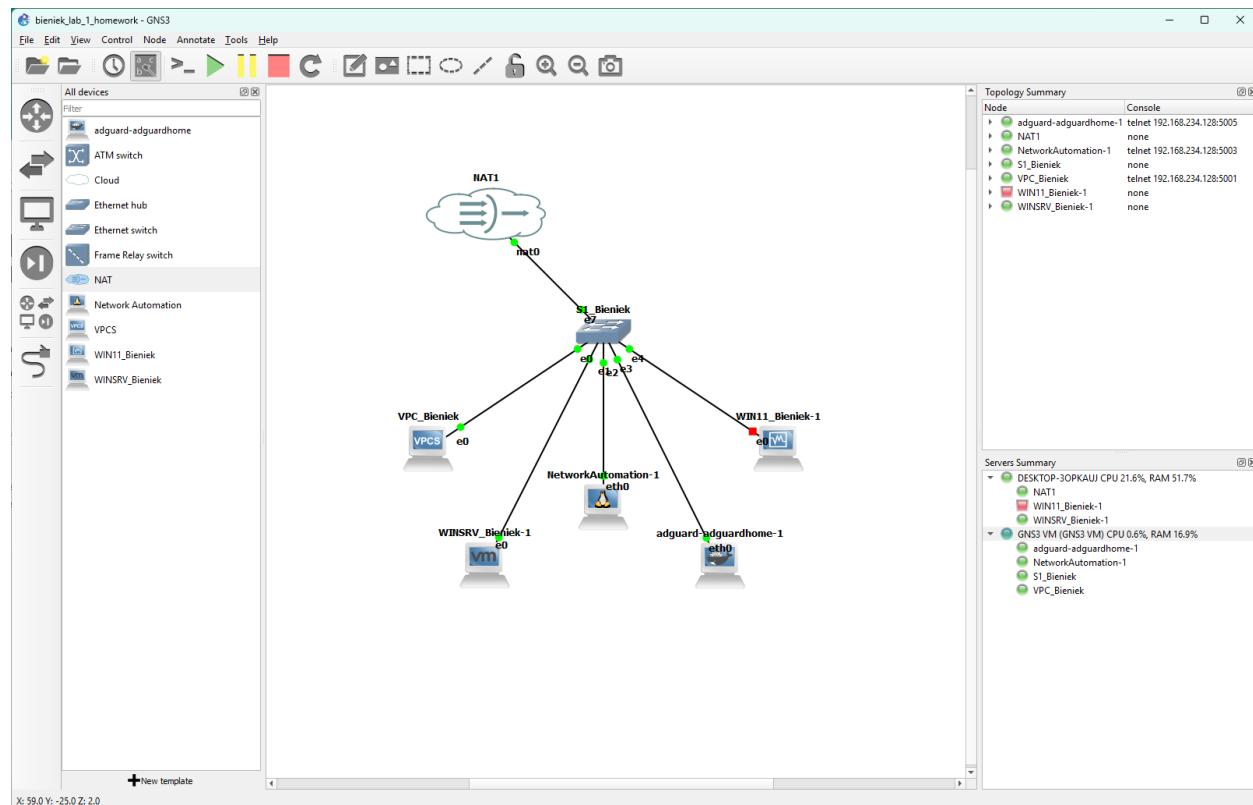
Zadanie 3. Konfiguracja połączenia z internetem.

Połączenie z siecią internet możemy wykonać na dwa sposoby.

1. „Chmura NAT” zachowuje się jak router z usługami NAT i DHCP. Pozwala podłączonym do niej urządzeniom uzyskać dostęp do internetu przez stos sieciowy komputera gospodarza (lub GNS3 VM).
2. Obiekt „Chmury” działa w pewnej mierze jak kabel sieciowy i pozwala na bezpośrednie podłączenie urządzeń do wybranego interfejsu sieciowego na komputerze gospodarza (lub GNS3 VM). W tym miejscu warto zaznaczyć, że możemy wybrać również wirtualne interfejsy sieciowe – na przykład takie, które zostały utworzone przez oprogramowanie VirtualBox. W odróżnieniu od pierwszej opcji, urządzenia będą one widoczne jako osobne urządzenia w wybranej sieci.

Do podłączenia urządzeń do internetu wykorzystam pierwszy sposób.

Na początku dodajmy do projektu obiekt „chmury NAT” i jako serwer wybierzmy nasz komputer – w końcu chcemy udostępnić nasze łącze sieciowe, a nie te, które posiada GNS3 VM.



Przejdźmy teraz do konfiguracji kolejnych urządzeń.

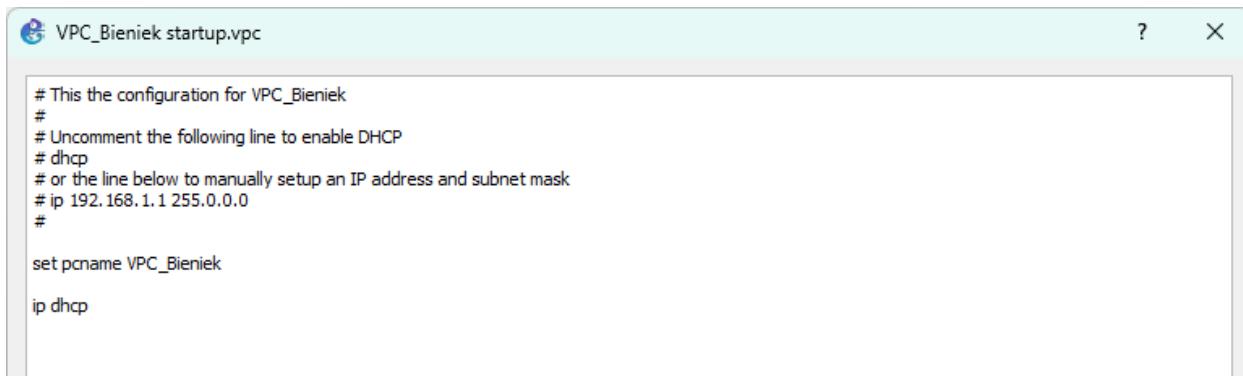
Konfiguracja sieciowa komputera VPC.

Aby ustawienia VPC przetrwały ponowne uruchomienia sprzętu, zmienimy konfigurację startową. W tym celu musimy go najpierw wyłączyć (prawy myszy → „Stop”), a następnie wybrać pozycję „Edit config” z menu kontekstowego.

Na końcu konfiguracji dodajemy linijkę z poleceniem

```
ip dhcp
```

które spowoduje automatyczne pobranie danych adresowych z serwera DHCP.

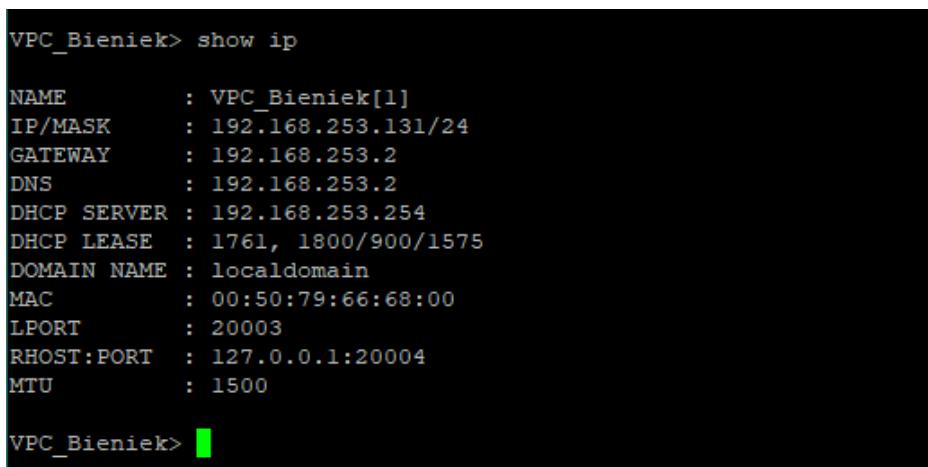


```
# This is the configuration for VPC_Bieniek
#
# Uncomment the following line to enable DHCP
# dhcp
# or the line below to manually setup an IP address and subnet mask
# ip 192.168.1.1 255.0.0.0
#
set pcname VPC_Bieniek
ip dhcp
```

Zrzut ekranu 26 Plik konfiguracyjny VPC. Dodano linijkę pobierającą dane adresowe z serwera DHCP przy starcie urządzenia.

Plik zapisujemy przyciskiem „Save” na dole okna, VPC uruchamiamy i przechodzimy do terminala, aby sprawdzić, czy dane adresowe zostały poprawnie pobrane. W tym celu wydamy poniższe polecenie.

```
show ip
```



```
VPC_Bieniek> show ip

NAME      : VPC_Bieniek[1]
IP/MASK   : 192.168.253.131/24
GATEWAY   : 192.168.253.2
DNS       : 192.168.253.2
DHCP SERVER : 192.168.253.254
DHCP LEASE  : 1761, 1800/900/1575
DOMAIN NAME : localdomain
MAC       : 00:50:79:66:68:00
LPORT     : 20003
RHOST:PORT : 127.0.0.1:20004
MTU       : 1500

VPC_Bieniek>
```

Zrzut ekranu 27 Wynik działania polecenia show ip. Dane adresowe zostały pomyślnie pobrane z serwera DHCP.

Jak widać, urządzeniu został przydzielony adres IP.

Konfiguracja sieciowa kontenerów.

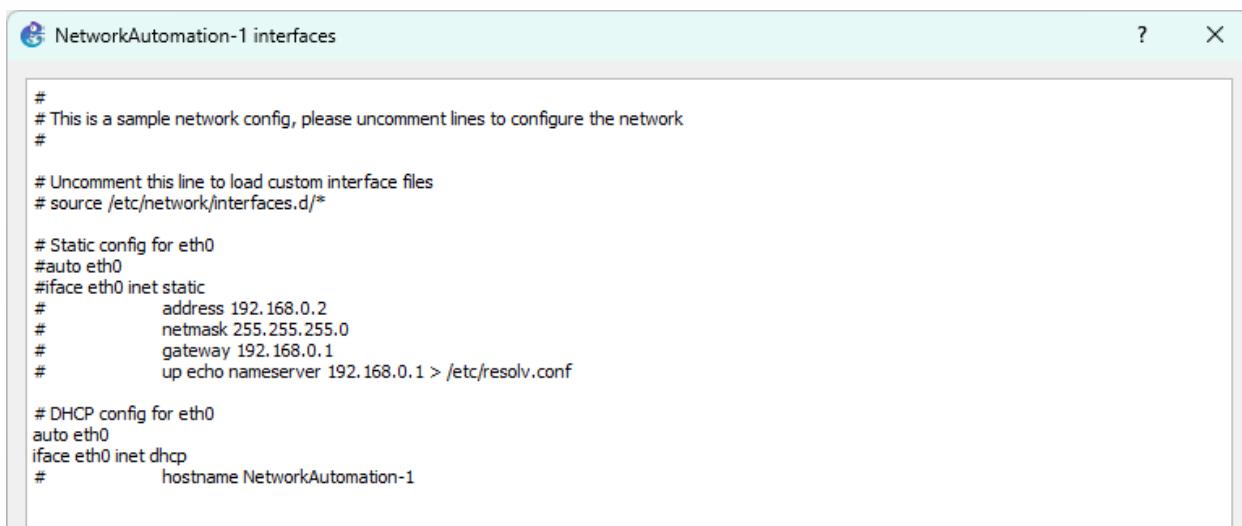
W przypadku kontenerów, postępujemy w podobny sposób. Na początku wyłączamy maszynę, po czym wybieramy z menu kontekstowego opcję „Edit config”. Skrypt konfiguracyjny nieco różni się od tego, z którym mieliśmy do czynienia w przypadku VPC, bowiem formatem przypomina stare pliki konfiguracyjne sieci pod Debianem, przed przejściem na systemd-networkd.

Na początku dodajemy polecenie uruchamiające wybrany interfejs sieciowy przy starcie systemu.

```
auto eth0
```

Następnie konfigurujemy dla niego automatyczne pobranie danych adresowych z serwera DHCP.

```
iface eth0 inet dhcp
```



```
# This is a sample network config, please uncomment lines to configure the network
#
# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*
#
# Static config for eth0
#auto eth0
#iface eth0 inet static
#        address 192.168.0.2
#        netmask 255.255.255.0
#        gateway 192.168.0.1
#        up echo nameserver 192.168.0.1 > /etc/resolv.conf
#
# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
#        hostname NetworkAutomation-1
```

Zrzut ekranu 28 Konfiguracja sieciowa kontenera.

Powysze kroki powtarzamy dla obydwu kontenerów – NetworkAutomation-1 oraz adguard-adguardhome-1.

Aby zweryfikować przydzielenie adresu IP z serwera DHCP dla pierwszego z nich musimy najpierw doinstalować pakiet *net-tools*, zawierający polecenie *ifconfig*.

```
apt update && apt install net-tools
```

```
root@NetworkAutomation-1:~# apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libbatml libmnl0 libxtables12
Use 'apt autoremove' to remove them.
The following packages will be upgraded:
  net-tools
1 upgraded, 0 newly installed, 0 to remove and 175 not upgraded.
Need to get 192 kB of archives.
After this operation, 8192 B disk space will be freed.
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 net-tools amd64
60+git20180626.aebd88e-lubuntul.3 [192 kB]
2% [1 net-tools 5508 B/192 kB 3%]
Fetched 192 kB in 1s (304 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
(Reading database ... 24087 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-lubuntul.3_amd64.deb
.
Unpacking net-tools (1.60+git20180626.aebd88e-lubuntul.3) over (1.60+git20180626
aebd88e-lubuntul) ...
Setting up net-tools (1.60+git20180626.aebd88e-lubuntul.3) ...
root@NetworkAutomation-1:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.253.132  netmask 255.255.255.0  broadcast 192.168.253.255
        ether 02:42:ee:a6:d6:00  txqueuelen 1000  (Ethernet)
          RX packets 27595  bytes 41096713 (41.0 MB)
          RX errors 0  dropped 28  overruns 0  frame 0
          TX packets 13149  bytes 725214 (725.2 KB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 0  bytes 0 (0.0 B)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 0  bytes 0 (0.0 B)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

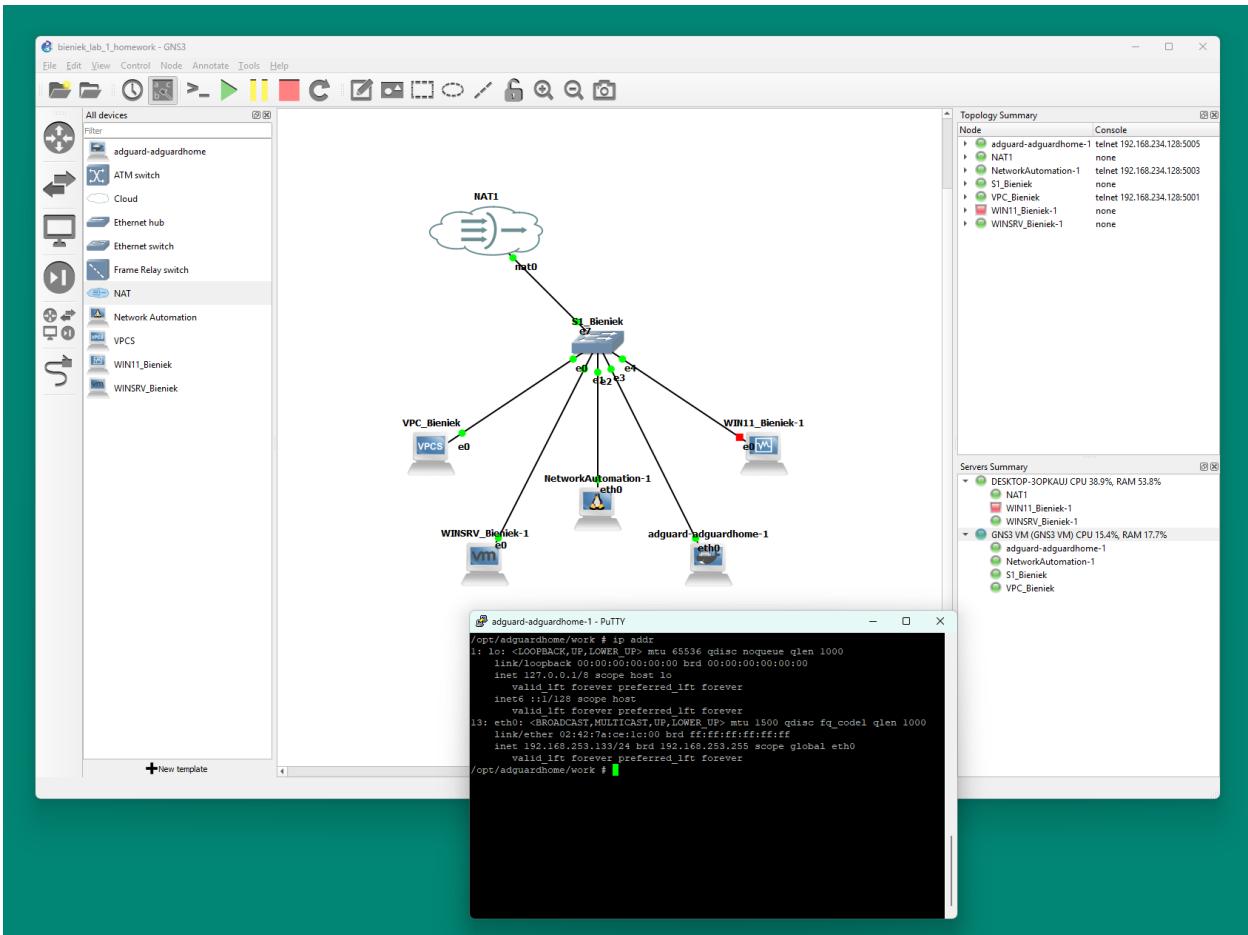
root@NetworkAutomation-1:~#
```

Zrzut ekranu 29 Instalacja pakietu net-tools i wynik wykonania polecenia ifconfig.

Jak widać, kontenerowi został automatycznie przydzielony adres IP, należący do tej samej sieci co komputer VPC.

W przypadku kontenera z oprogramowaniem *adguard*, polecenie wyświetlające konfigurację sieciową dotyczącą adresów IP jest już zainstalowane.

`ip addr`

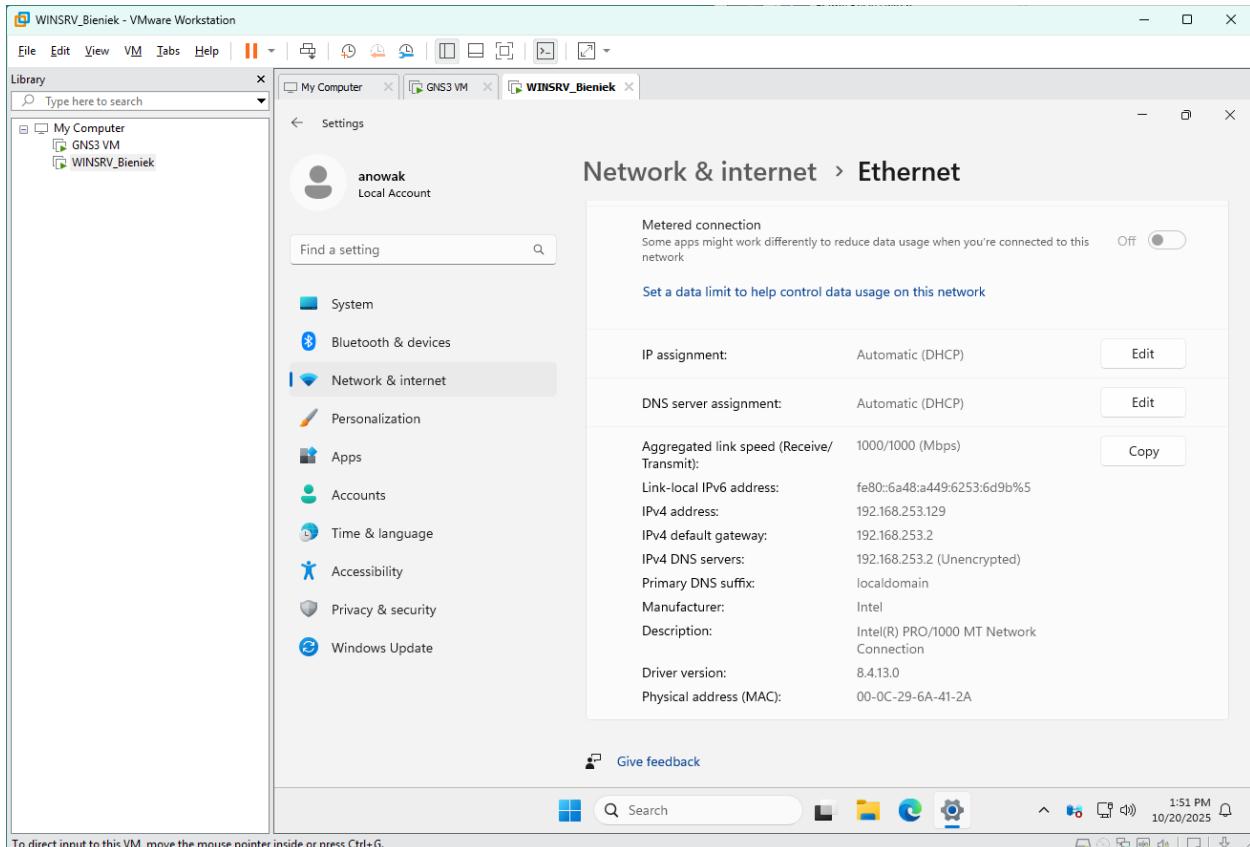


Zrzut ekranu 30 Konfiguracja sieciowa kontenera adguard-adguardhome-1. Dane adresowe przydzielone z serwera DHCP.

Tutaj również został automatycznie przydzielony adres IP.

Konfiguracja sieciowa maszyny wirtualnej z systemem Windows Server 2025.

W przypadku maszyn wirtualnych, ich stan jest zapisywany na dysku komputera gospodarza. Stąd, wszelkie zmiany wystarczy wprowadzić wewnątrz działającego systemu.



Zrzut ekranu 31 Ustawienia sieciowe w systemie Windows Server 2025. Dane adresowe uzyskane z serwera DHCP.

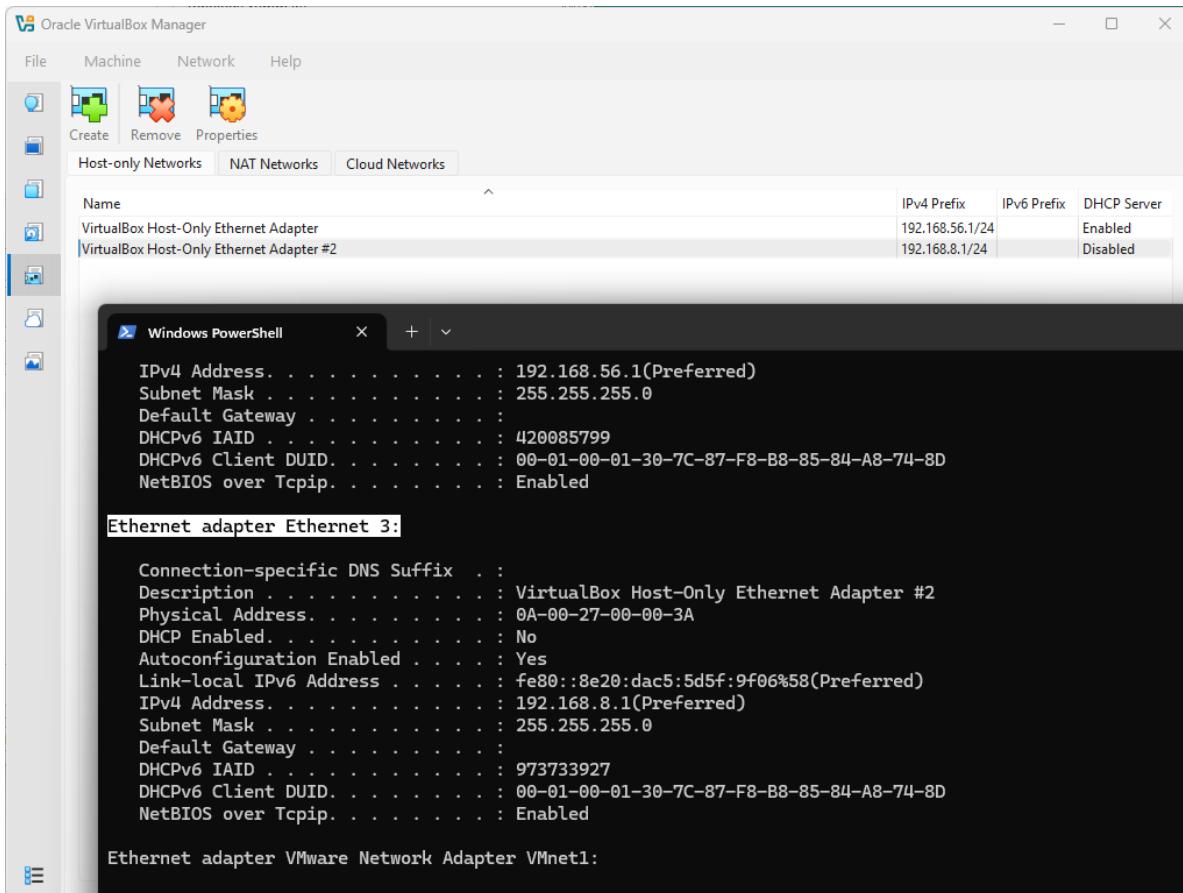
W moim przypadku Windows automatycznie uzyskał dane z usługi DHCP. Gdyby tak się jednak nie stało należy w terminalu wydać polecenie

```
ipconfig /renew
```

Konfiguracja sieciowa maszyny wirtualnej z systemem Windows 11 Enterprise.

Dla zobrazowania działania obiektu „chmury” (bez NAT) w GNS3, maszynę wirtualną podłączymy do sieci w niestandardowy sposób. Zamiast uruchamiać ją z poziomu GNS, co automatycznie konfiguruje ustawienia na niepodłączonym interfejsie, zrobimy to bezpośrednio z poziomu VirtualBox. Aby zapewnić połączenie sieciowe, w programie do wirtualizacji utworzymy nową sieć izolowaną, którą podłączymy przez obiekt „chmury” do GNS.

Rozpoczniemy od utworzenia w oprogramowaniu VirtualBox nowej sieci typu host-only (izolowanej). Ważne jest, aby nie uruchamiać w niej usługi DHCP, ponieważ doprowadziłybyśmy za chwilę do sytuacji, w której w jednej sieci GNS działałyby dwa różne serwery przydzielające adresy.

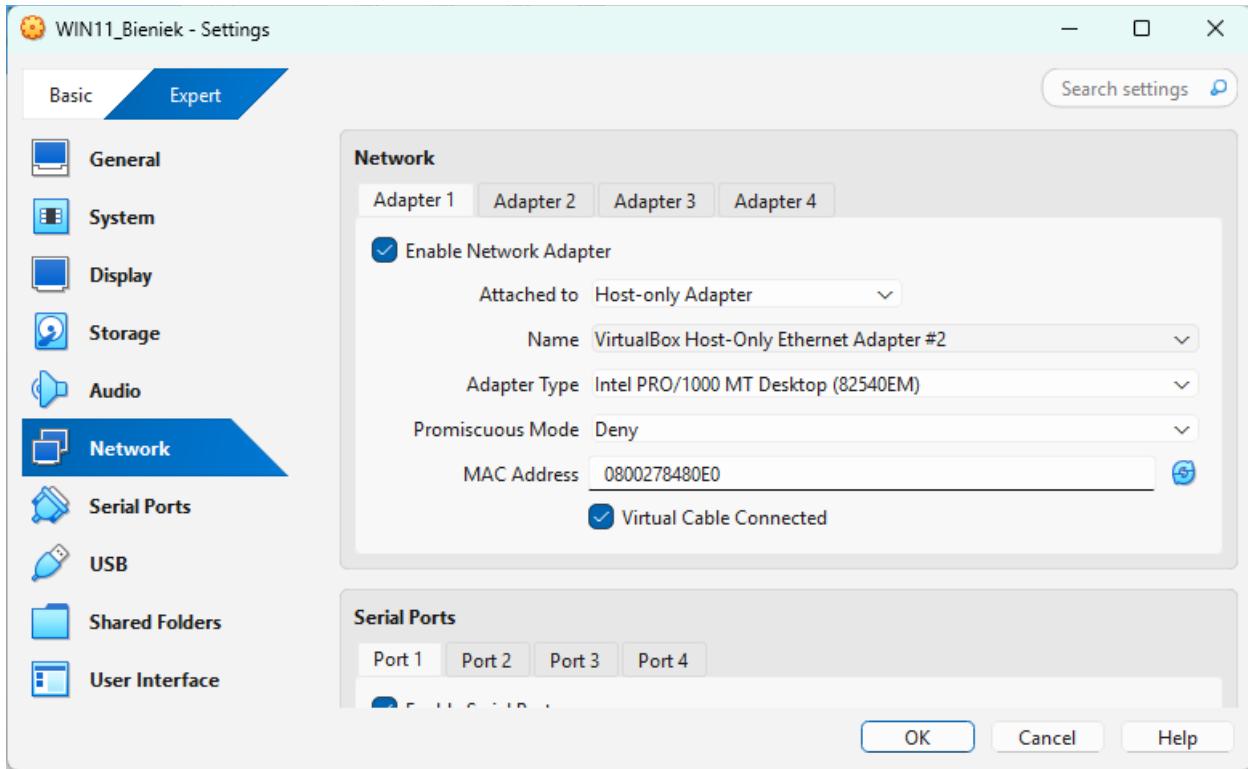


Zrzut ekranu 32 Utworzona w oprogramowaniu VirtualBox sieć izolowana z wyłączonym serwerem DHCP. W terminalu widoczny jest utworzony na jej potrzeby wirtualny adapter.

Zwrócić uwagę, że tak utworzona sieć wyświetla się w systemie gospodarza jako wirtualny interfejs sieciowy. Aby go odnaleźć, możemy wykonać poniższe polecenie i odszukać właściwą pozycję na podstawie opisu adaptera.

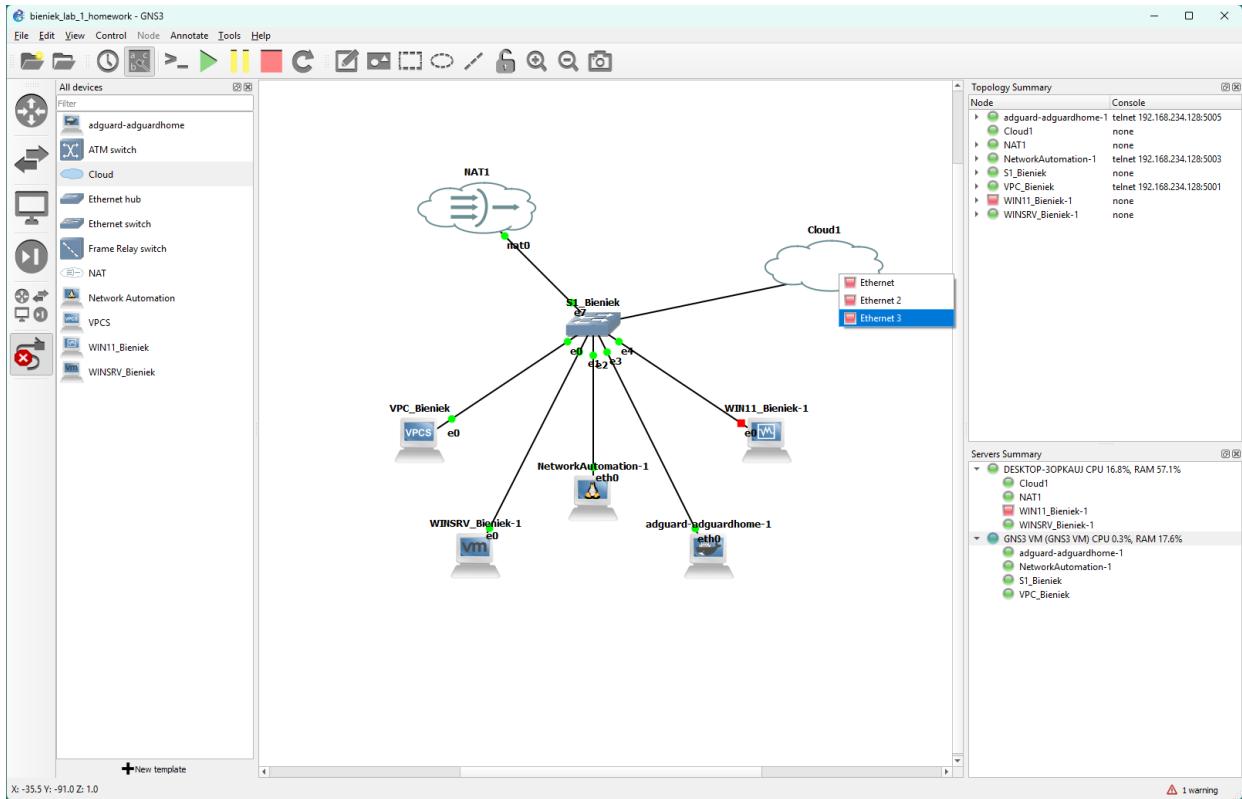
```
ipconfig /all
```

Następnie przechodzimy do ustawień maszyny wirtualnej i podłączamy ją do nowo utworzonej sieci.



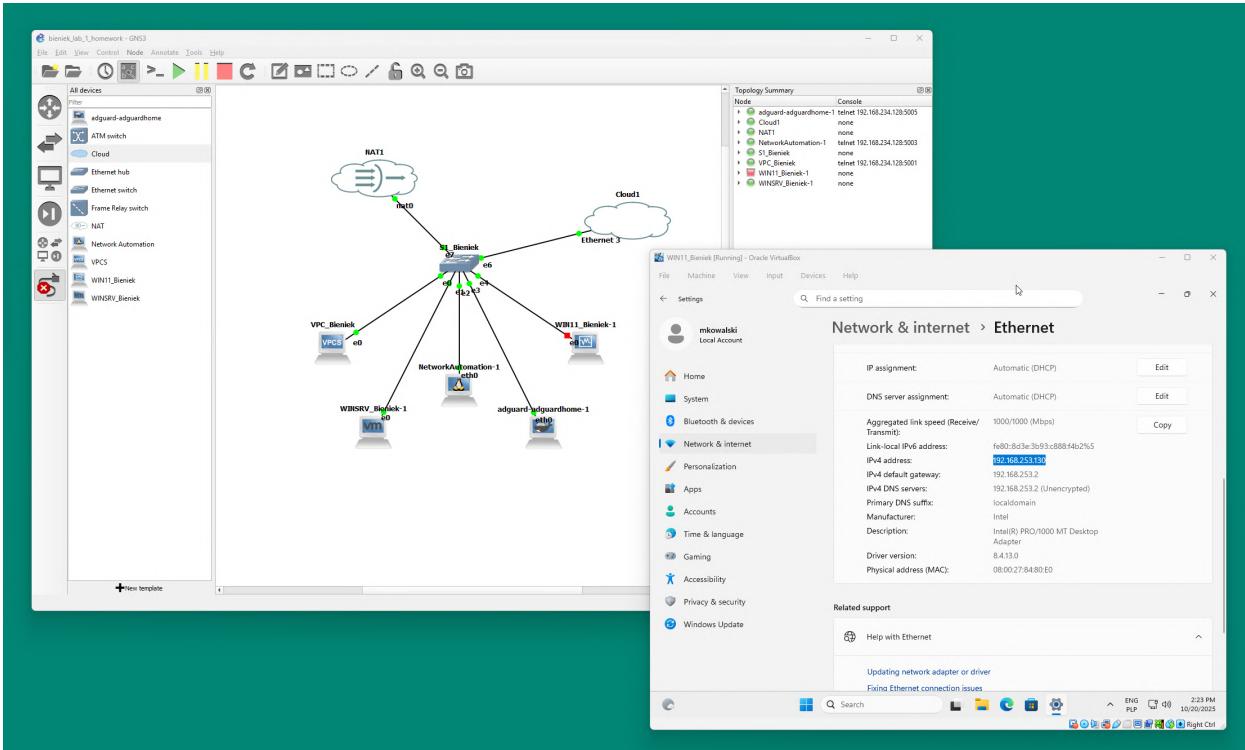
Zrzut ekranu 33 Podłączenie maszyny wirtualnej do utworzonej sieci izolowanej.

Jedynie co pozostało, to zapisać zmiany i dodać do GNS obiekt „chmury”, podłączając go z właściwego interfejsu (w moim przypadku Ethernet 3) z przełącznikiem.



Zrzut ekranu 34 Dodanie do GNS obiektu chmury (bez NAT).

Na koniec uruchommy maszynę z poziomu VirtualBox i sprawdźmy konfigurację sieciową.



Zrzut ekranu 35 Konfiguracja sieciowa maszyny wirtualnej Windows 11 Enterprise. Adres przydzielony z usługi DHCP działającej na „chmurze (NAT)”.

Jak widać maszyna wirtualna uzyskała dane adresowe przy użyciu usługi DHCP, działającej w „chmurze (NAT)”.

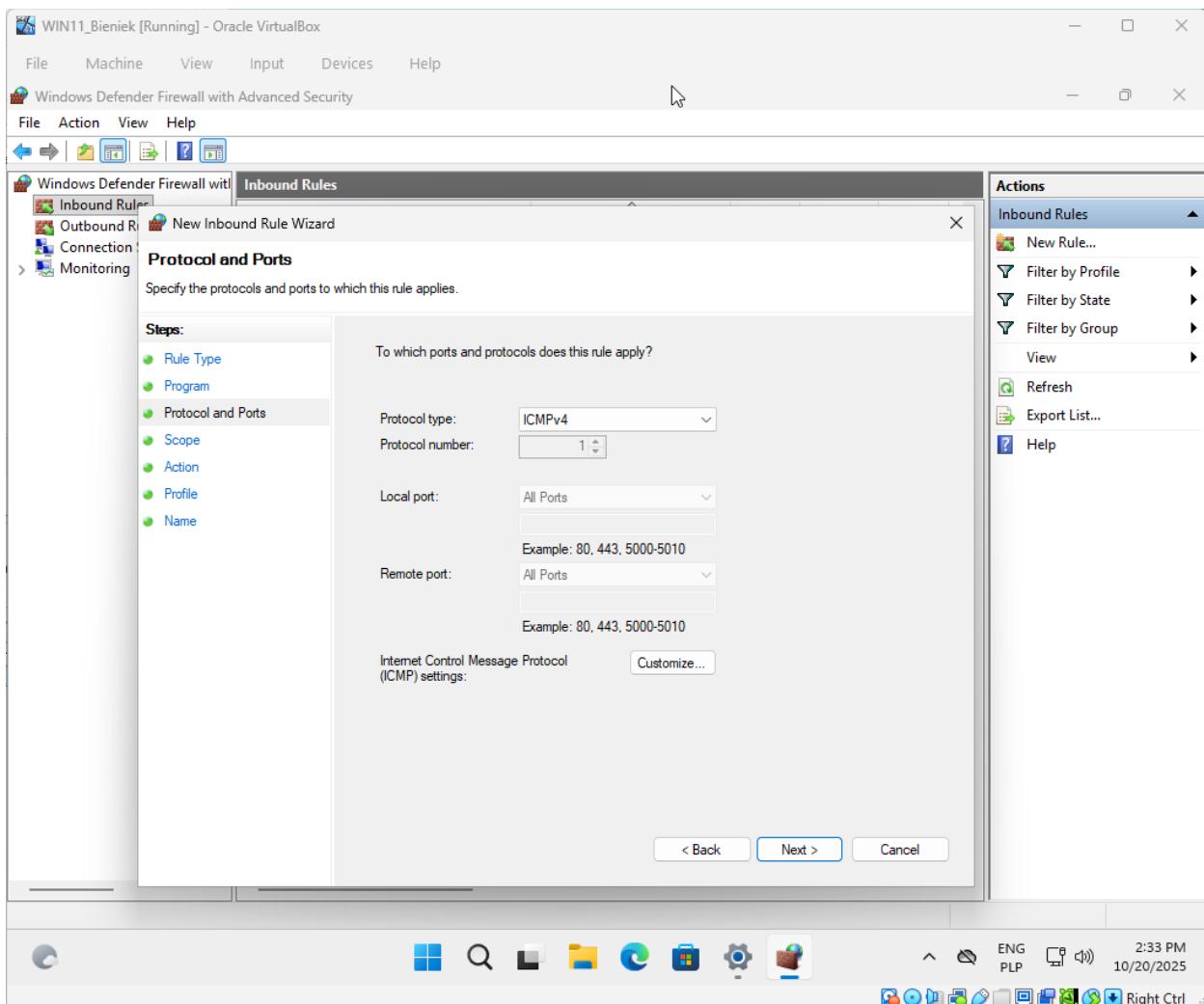
Zadanie 4. Weryfikacja komunikacji sieciowej.

W ramach poprzedniego zadania sprawdziliśmy już poprawność automatycznego przydzielania adresów przez usługę DHCP. Zobaczmy zatem, czy w naszej sieci możliwa jest także komunikacja między komputerami. W tym celu wykorzystamy narzędzie *ping*.

Konfiguracja zapory ogniwowej w systemie Windows.

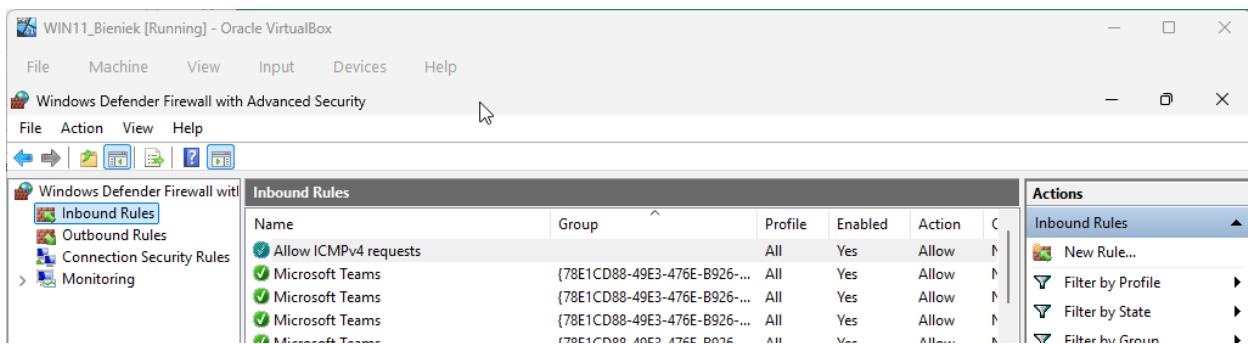
Należy pamiętać, że pod systemem Windows, zapytania *ping* są domyślnie odrzucane przez zaporę ogniwową. Stąd, należy skonfigurować zasadę, która pozwoli na otrzymywanie takich pakietów.

W tym celu przechodzimy do ustawień zapory ogniwowej dla połączeń przychodzących i tworzymy nową regułę. Wskazujemy typ „Custom” i w zakładce dotyczącej protokołów wybieramy z listy */ICMPv4*.



Zrzut ekranu 36 Dodawanie nowej zasady zapory ogniewej, zezwalającej na odbieranie zapytań ping.

Na koniec przechodzimy do sekcji „Name”, w której wskazujemy nazwę i zapisujemy.



Zrzut ekranu 37 Skonfigurowana reguła widoczna na liście zasad dla połączeń przychodzących.

Powyższe czynności powtarzamy zarówno dla komputera z systemem Windows Server 2025, jak i Windows 11 Enterprise.

Weryfikacja poprawności komunikacji między urządzeniami i internetem.

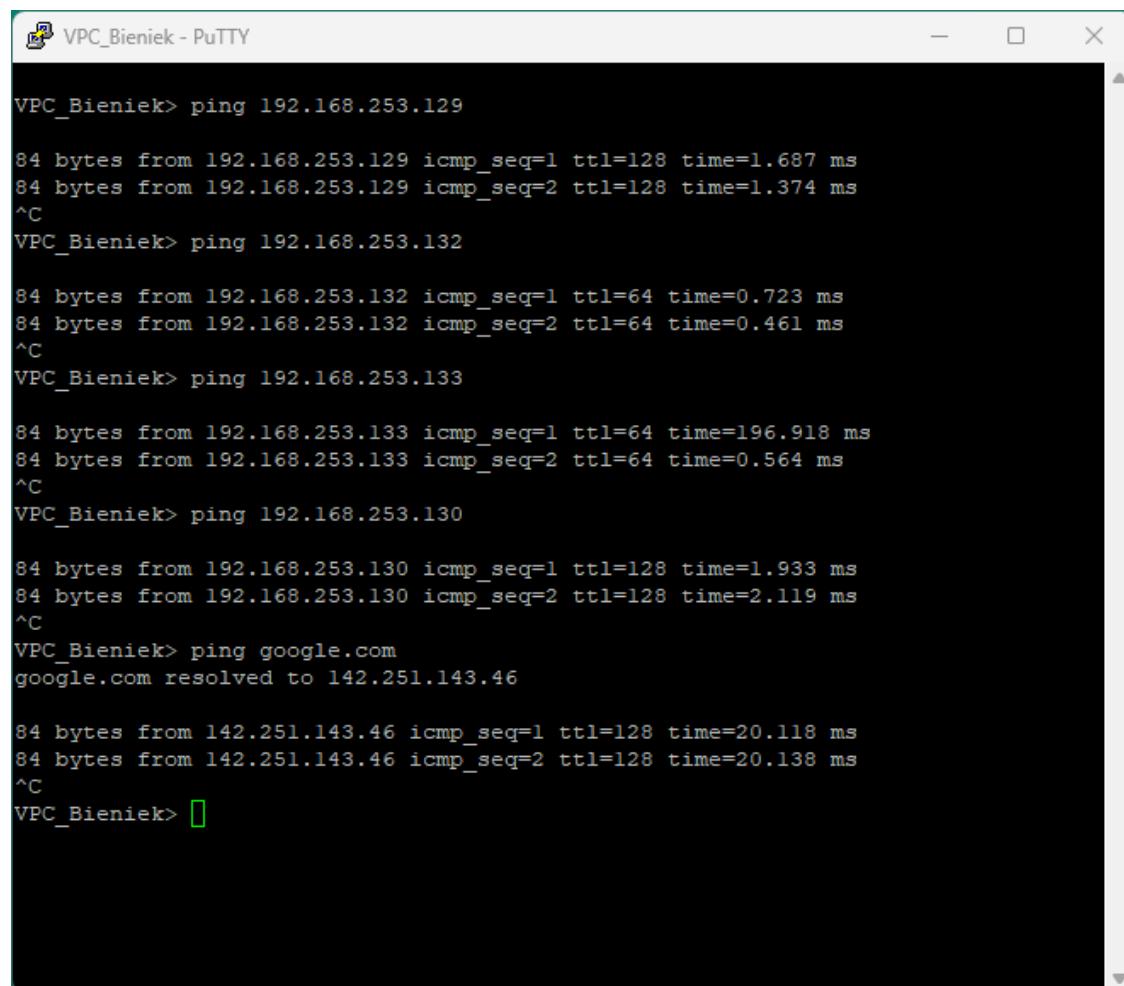
Do sprawdzenia możliwości komunikacji między komputerami oraz siecią internet skorzystamy z polecenia ping.

```
ping adres_ip_lub_nazwa_mnemoniczna
```

Dla ułatwienia, poniżej zamieszczam tabelkę z adresami IP przydzielonymi przez DHCP w poprzednim zadaniu.

Nazwa obiektu	Adres IP
VPC_Bieniek	192.168.253.131
WINSRV_Bieniek-1	192.168.253.129
NetworkAutomation-1	192.168.253.132
adguard-adguardhome-1	192.168.253.133
WIN11_Bieniek-1	192.168.253.130

Tabela 1 Przydzielone przez usługę DHCP adresy urządzeń.



```
VPC_Bieniek> ping 192.168.253.129
84 bytes from 192.168.253.129 icmp_seq=1 ttl=128 time=1.687 ms
84 bytes from 192.168.253.129 icmp_seq=2 ttl=128 time=1.374 ms
^C
VPC_Bieniek> ping 192.168.253.132
84 bytes from 192.168.253.132 icmp_seq=1 ttl=64 time=0.723 ms
84 bytes from 192.168.253.132 icmp_seq=2 ttl=64 time=0.461 ms
^C
VPC_Bieniek> ping 192.168.253.133
84 bytes from 192.168.253.133 icmp_seq=1 ttl=64 time=196.918 ms
84 bytes from 192.168.253.133 icmp_seq=2 ttl=64 time=0.564 ms
^C
VPC_Bieniek> ping 192.168.253.130
84 bytes from 192.168.253.130 icmp_seq=1 ttl=128 time=1.933 ms
84 bytes from 192.168.253.130 icmp_seq=2 ttl=128 time=2.119 ms
^C
VPC_Bieniek> ping google.com
google.com resolved to 142.251.143.46
84 bytes from 142.251.143.46 icmp_seq=1 ttl=128 time=20.118 ms
84 bytes from 142.251.143.46 icmp_seq=2 ttl=128 time=20.138 ms
^C
VPC_Bieniek>
```

Zrzut ekranu 38 Pomyślna próba komunikacji komputera VPC_Bieniek ze wszystkimi urządzeniami w sieci i internetem (tutaj serwerami Google).

The screenshot shows a VMware Workstation interface with a single VM named "WINSRV_Bieniek". Inside the VM, there are two open PowerShell windows. The top window is titled "Windows PowerShell" and shows the output of several ping commands. The first command is "ping 192.168.253.131", which returns three replies from the same IP address with a round-trip time of 1ms each. The second command is "ping 192.168.253.132", which also returns three replies from the same IP address with a round-trip time of 3ms each. The third command is "ping 192.168.253.133", which returns three replies from the same IP address with a round-trip time of 5ms each. The bottom window is also titled "Windows PowerShell" and shows the output of a ping command to "google.com" at IP [142.251.143.46]. The ping returns three replies from the same IP address with a round-trip time of 21ms each. Both windows show the standard Windows taskbar at the bottom with icons for File Explorer, Edge, and Control Panel.

```
PS C:\Users\anowak> ping 192.168.253.131
Pinging 192.168.253.131 with 32 bytes of data:
Reply from 192.168.253.131: bytes=32 time=1ms TTL=64
Reply from 192.168.253.131: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.253.131:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
PS C:\Users\anowak> ping 192.168.253.132

Pinging 192.168.253.132 with 32 bytes of data:
Reply from 192.168.253.132: bytes=32 time=3ms TTL=64
Reply from 192.168.253.132: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.253.132:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
Control-C
PS C:\Users\anowak> ping 192.168.253.133

Pinging 192.168.253.133 with 32 bytes of data:
Reply from 192.168.253.133: bytes=32 time=5ms TTL=64
Reply from 192.168.253.133: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.253.133:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms
Control-C
PS C:\Users\anowak> ping 192.168.253.130

Pinging 192.168.253.130 with 32 bytes of data:
Reply from 192.168.253.130: bytes=32 time=7ms TTL=128
Reply from 192.168.253.130: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.253.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 7ms, Average = 6ms
Control-C
PS C:\Users\anowak> ping google.com

Pinging google.com [142.251.143.46] with 32 bytes of data:
Reply from 142.251.143.46: bytes=32 time=22ms TTL=128
Reply from 142.251.143.46: bytes=32 time=21ms TTL=128

Ping statistics for 142.251.143.46:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 22ms, Average = 21ms
Control-C
PS C:\Users\anowak>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Zrzut ekranu 39 Pomyślna próba komunikacji serwera WINSRV_Bieniek-1 ze wszystkimi urządzeniami w sieci i internetem (tutaj serwerami Google).

```
root@NetworkAutomation-1: ~
root@NetworkAutomation-1:~# ping 192.168.253.131
PING 192.168.253.131 (192.168.253.131) 56(84) bytes of data.
64 bytes from 192.168.253.131: icmp_seq=1 ttl=64 time=0.576 ms
64 bytes from 192.168.253.131: icmp_seq=2 ttl=64 time=0.726 ms
^C
--- 192.168.253.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.576/0.651/0.726/0.075 ms
root@NetworkAutomation-1:~# ping 192.168.253.129
PING 192.168.253.129 (192.168.253.129) 56(84) bytes of data.
64 bytes from 192.168.253.129: icmp_seq=1 ttl=128 time=1.74 ms
64 bytes from 192.168.253.129: icmp_seq=2 ttl=128 time=1.50 ms
^C
--- 192.168.253.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.497/1.617/1.737/0.120 ms
root@NetworkAutomation-1:~# ping 192.168.253.133
PING 192.168.253.133 (192.168.253.133) 56(84) bytes of data.
64 bytes from 192.168.253.133: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 192.168.253.133: icmp_seq=2 ttl=64 time=0.776 ms
^C
--- 192.168.253.133 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.776/0.993/1.210/0.217 ms
root@NetworkAutomation-1:~# ping 192.168.253.130
PING 192.168.253.130 (192.168.253.130) 56(84) bytes of data.
64 bytes from 192.168.253.130: icmp_seq=1 ttl=128 time=6.33 ms
64 bytes from 192.168.253.130: icmp_seq=2 ttl=128 time=3.08 ms
^C
--- 192.168.253.130 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.076/4.703/6.331/1.627 ms
root@NetworkAutomation-1:~# ping google.com
PING google.com (142.251.143.46) 56(84) bytes of data.
64 bytes from ber07s04-in-f14.le100.net (142.251.143.46): icmp_seq=1 ttl=128 time=19.9 ms
64 bytes from ber07s04-in-f14.le100.net (142.251.143.46): icmp_seq=2 ttl=128 time=20.0 ms
64 bytes from ber07s04-in-f14.le100.net (142.251.143.46): icmp_seq=3 ttl=128 time=20.0 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 19.889/19.971/20.013/0.057 ms
root@NetworkAutomation-1:~#
```

Zrzut ekranu 40 Pomyślna próba komunikacji kontenera NetworkAutomation-1 ze wszystkimi urządzeniami w sieci i internetem (tutaj serwerami Google).

```
adguard-adguardhome-1 - PuTTY  
/opt/adguardhome/work # ping 192.168.253.130  
PING 192.168.253.130 (192.168.253.130): 56 data bytes  
64 bytes from 192.168.253.130: seq=12 ttl=128 time=2.405 ms  
64 bytes from 192.168.253.130: seq=13 ttl=128 time=2.015 ms  
64 bytes from 192.168.253.130: seq=14 ttl=128 time=4.182 ms  
64 bytes from 192.168.253.130: seq=15 ttl=128 time=2.325 ms  
^C  
--- 192.168.253.130 ping statistics ---  
16 packets transmitted, 4 packets received, 75% packet loss  
round-trip min/avg/max = 2.015/2.731/4.182 ms  
/opt/adguardhome/work # clear  
/opt/adguardhome/work # ping 192.168.253.131  
PING 192.168.253.131 (192.168.253.131): 56 data bytes  
64 bytes from 192.168.253.131: seq=0 ttl=64 time=1.452 ms  
64 bytes from 192.168.253.131: seq=1 ttl=64 time=0.812 ms  
^C  
--- 192.168.253.131 ping statistics ---  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 0.812/1.132/1.452 ms  
/opt/adguardhome/work # ping 192.168.253.129  
PING 192.168.253.129 (192.168.253.129): 56 data bytes  
64 bytes from 192.168.253.129: seq=0 ttl=128 time=3.933 ms  
64 bytes from 192.168.253.129: seq=1 ttl=128 time=1.972 ms  
^C  
--- 192.168.253.129 ping statistics ---  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 1.972/2.952/3.933 ms  
/opt/adguardhome/work # ping 192.168.253.132  
PING 192.168.253.132 (192.168.253.132): 56 data bytes  
64 bytes from 192.168.253.132: seq=0 ttl=64 time=0.792 ms  
64 bytes from 192.168.253.132: seq=1 ttl=64 time=0.692 ms  
^C  
--- 192.168.253.132 ping statistics ---  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 0.692/0.742/0.792 ms  
/opt/adguardhome/work # ping 192.168.253.130  
PING 192.168.253.130 (192.168.253.130): 56 data bytes  
64 bytes from 192.168.253.130: seq=0 ttl=128 time=2.268 ms  
64 bytes from 192.168.253.130: seq=1 ttl=128 time=1.968 ms  
^C  
--- 192.168.253.130 ping statistics ---  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 1.968/2.118/2.268 ms  
/opt/adguardhome/work # ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8): 56 data bytes  
64 bytes from 8.8.8.8: seq=0 ttl=128 time=10.871 ms  
64 bytes from 8.8.8.8: seq=1 ttl=128 time=11.637 ms  
^C  
--- 8.8.8.8 ping statistics ---  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 10.871/11.254/11.637 ms  
/opt/adguardhome/work #
```

Zrzut ekranu 41 Pomyślna próba komunikacji komputera NetworkAutomation-1 ze wszystkimi urządzeniami w sieci i internetem.

```
WIN11_Bieniek [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows PowerShell × + ⌂
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\mkowalski> ping 192.168.253.131
Pinging 192.168.253.131 with 32 bytes of data:
Reply from 192.168.253.131: bytes=32 time=2ms TTL=64
Reply from 192.168.253.131: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.253.131:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
Control-C
PS C:\Users\mkowalski> ping 192.168.253.129

Pinging 192.168.253.129 with 32 bytes of data:
Reply from 192.168.253.129: bytes=32 time=2ms TTL=128
Reply from 192.168.253.129: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.253.129:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
Control-C
PS C:\Users\mkowalski> ping 192.168.253.132

Pinging 192.168.253.132 with 32 bytes of data:
Reply from 192.168.253.132: bytes=32 time=2ms TTL=64
Reply from 192.168.253.132: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.253.132:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
Control-C
PS C:\Users\mkowalski> ping 192.168.253.133

Pinging 192.168.253.133 with 32 bytes of data:
Reply from 192.168.253.133: bytes=32 time=1ms TTL=64
Reply from 192.168.253.133: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.253.133:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
PS C:\Users\mkowalski> ping google.com

Pinging google.com [142.250.186.206] with 32 bytes of data:
Reply from 142.250.186.206: bytes=32 time=13ms TTL=128
Reply from 142.250.186.206: bytes=32 time=12ms TTL=128

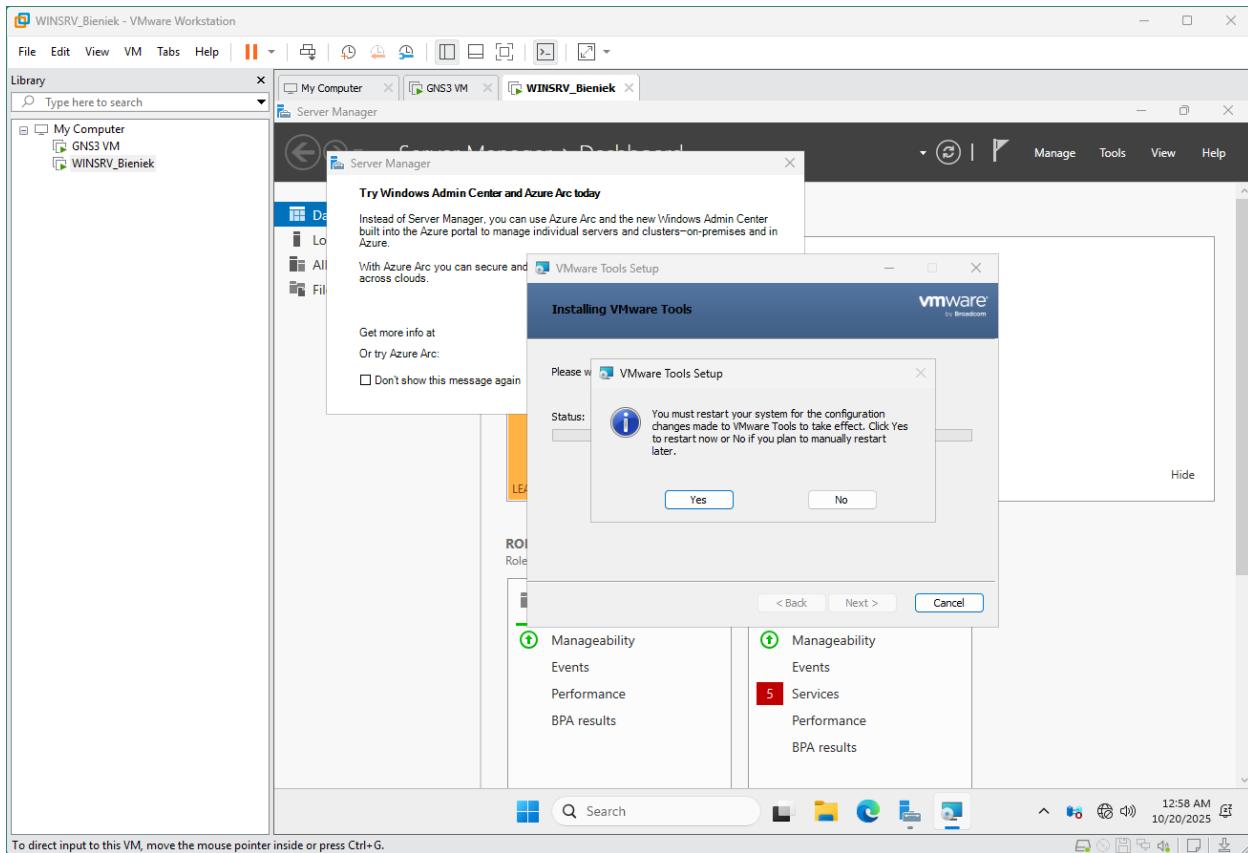
Ping statistics for 142.250.186.206:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 13ms, Average = 12ms
Control-C
PS C:\Users\mkowalski>
```

Zrzut ekranu 42 Pomyślna próba komunikacji komputera WIN11_Bieniek ze wszystkimi urządzeniami w sieci i internetem (tutaj serwerami Google).

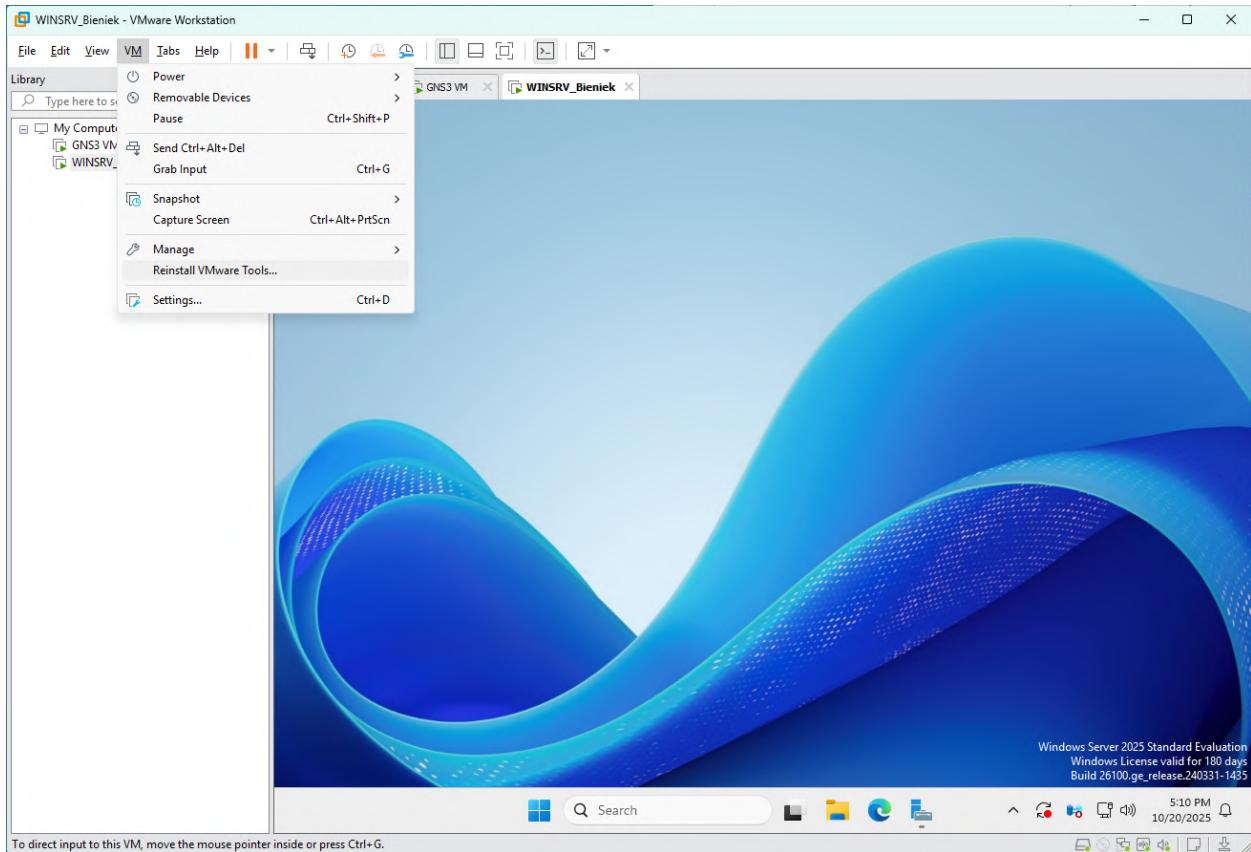
Zadanie 5. Instalacja dodatków gościa oraz wykonanie migawek.

Dodatki gościa umożliwiają między innymi płynne przechodzenie myszki i klawiatury między systemem w maszynie wirtualnej, a tym zainstalowanym na komputerze gospodarza. Dzięki nim możliwe jest też odpowiednie skalowanie obrazu i dostosowywanie się wielkości wirtualnego monitora do rozmiarów okna z maszyną wirtualną.

W przypadku instalacji systemu Windows Server 2025 pod oprogramowaniem VMware Workstation, dodatki gościa zostały automatycznie zainstalowane przy pierwszym uruchomieniu systemu.

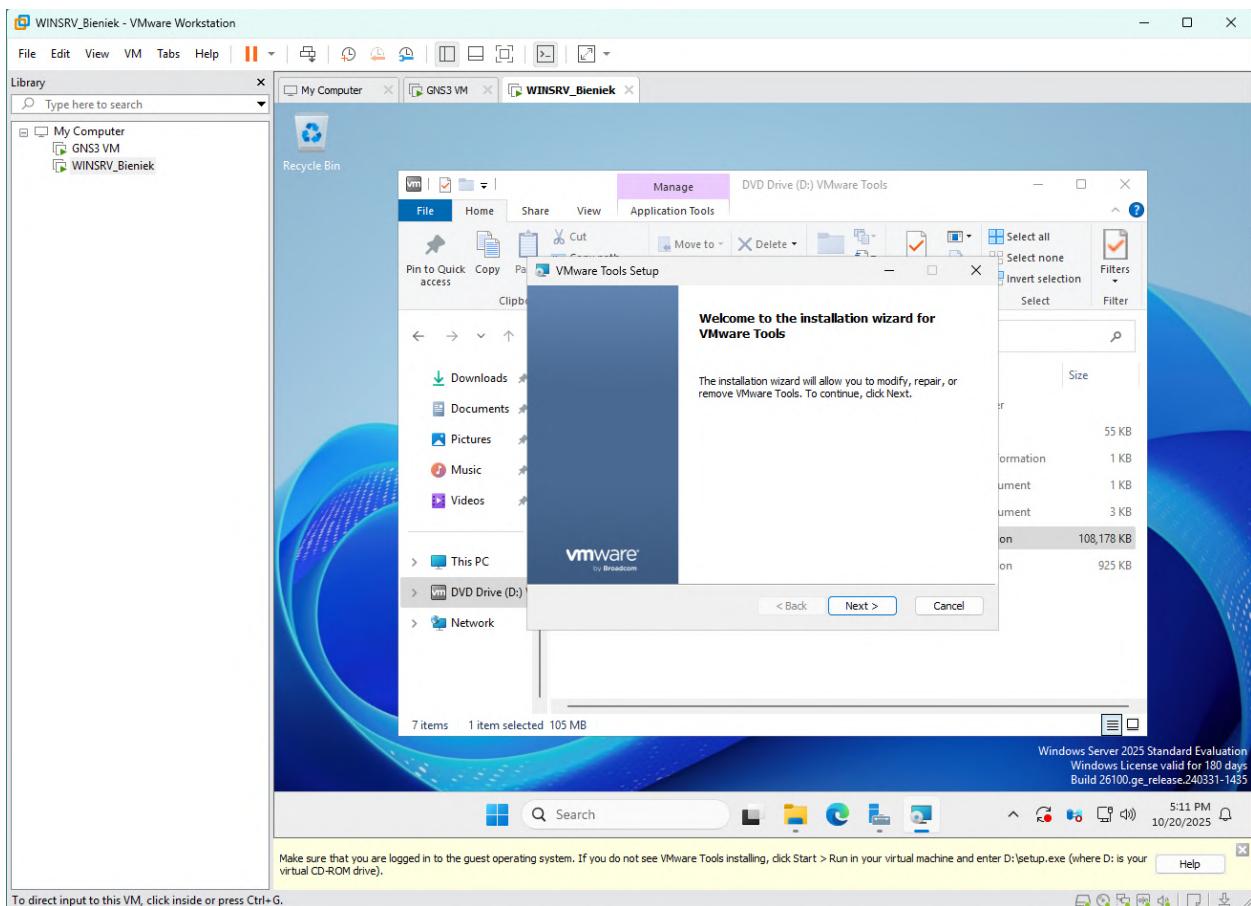


Zrzut ekranu 10 Gdyby nastąpiła taka potrzeba, możemy je przeinstalować wybierając podczas działania maszyny wirtualnej z górnego paska „VM” → „Reinstall VMware Tools...”.



Zrzut ekranu 43 Menu z widoczną opcją do przeinstalowania dodatków gościa w oprogramowaniu VMware Workstation.

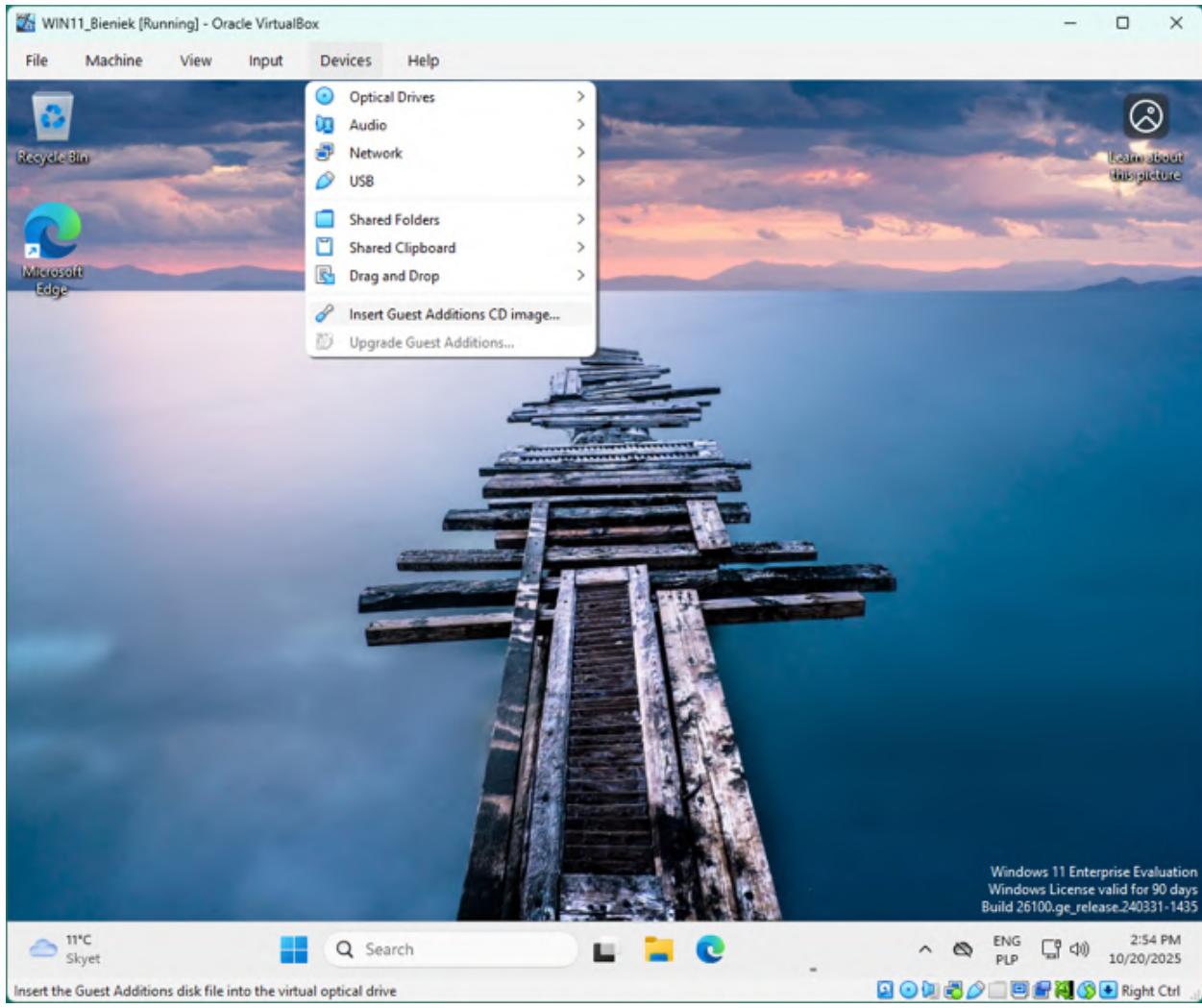
Do systemu zostanie wówczas dołączona wirtualna płytką DVD z instalatorem dodatków gościa, który należy uruchomić.



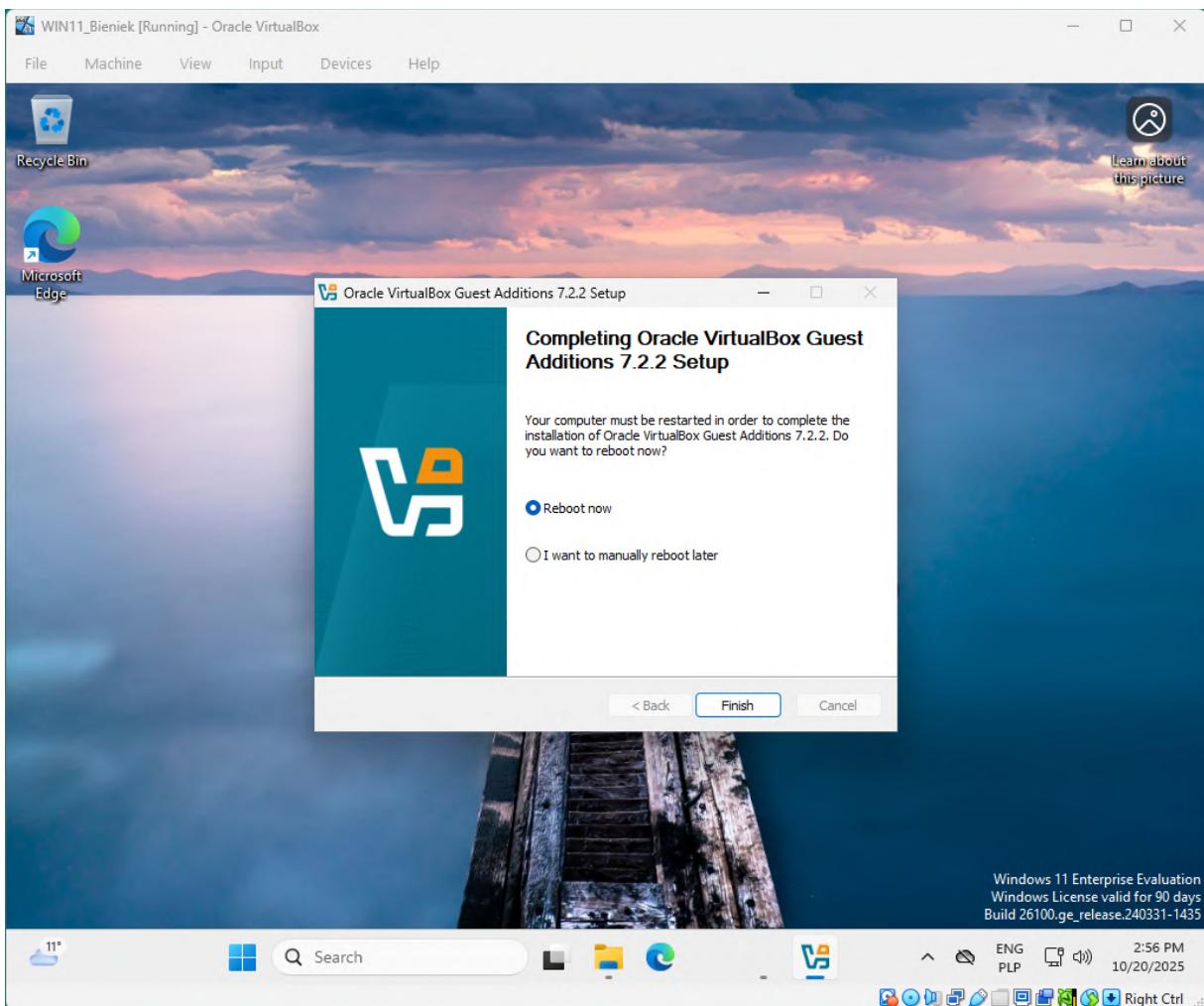
Zrzut ekranu 44 Instalator dodatków gościa w maszynie wirtualnej pod kontrolą oprogramowania VMware Workstation.

Jeżeli dodatki gościa nie byłyby wcześniej zainstalowane, po ukończeniu instalacji zostaniemy poproszeni o ponowne uruchomienie maszyny wirtualnej.

Proces ten wygląda praktycznie identycznie w oprogramowaniu VirtualBox. Z górnego paska narzędzi wybieramy „Devices” → „Insert Guest Additions CD image...”, a następnie uruchamiamy instalator z wirtualnej płytki CD.

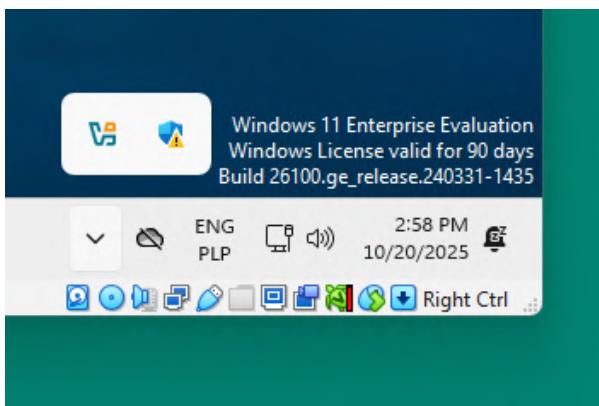


Zrzut ekranu 45 Menu z widoczną opcją do przeinstalowania dodatków gościa w oprogramowaniu Oracle VirtualBox.



Zrzut ekranu 46 Instalator dodatków gościa w maszynie wirtualnej pod kontrolą oprogramowania VirtualBox.

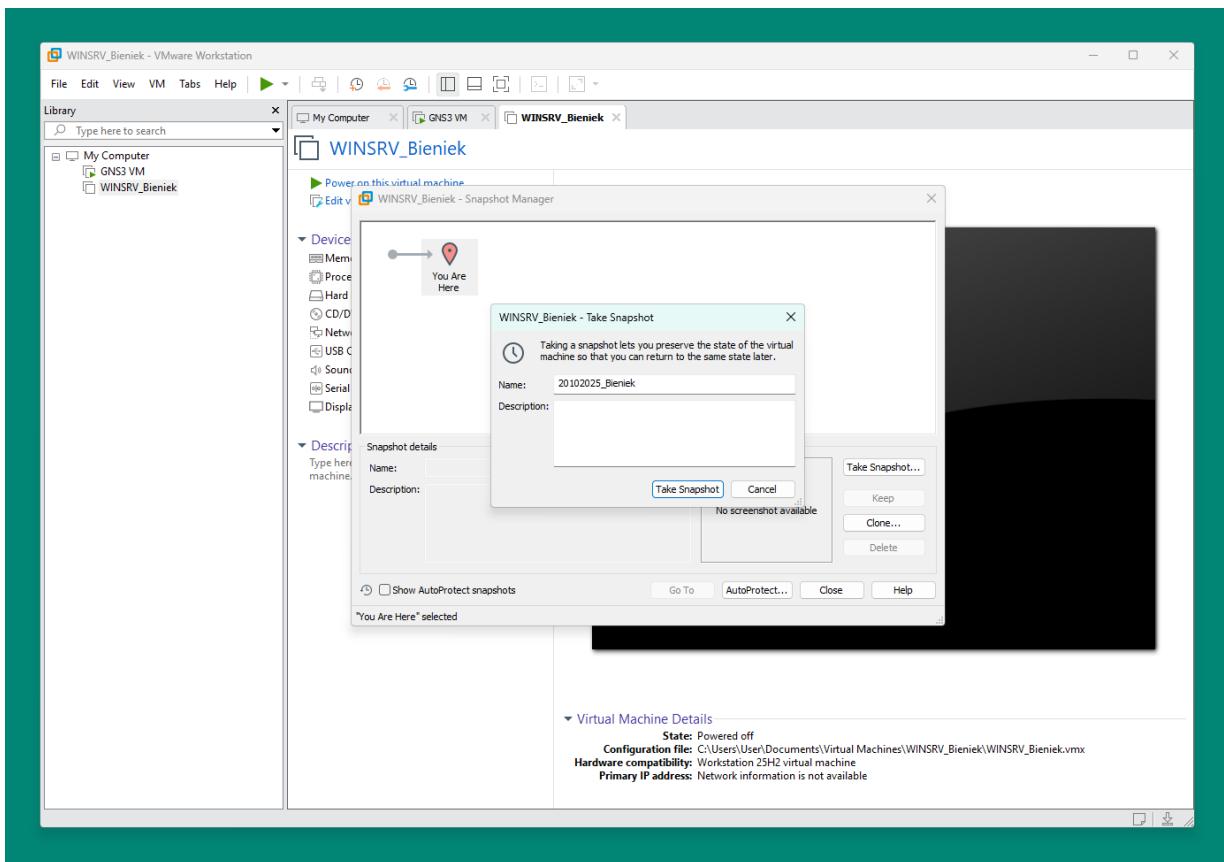
Jest to pierwszy raz, kiedy w tej maszynie zostały zainstalowane dodatki gościa. Stąd, do ich zadziałania wymagany jest restart wirtualizowanego systemu. Po ponownym uruchomieniu maszyny wirtualnej, na pasku narzędzi powinna pojawić się ikonka dodatków gościa (ikonka VirtualBox).



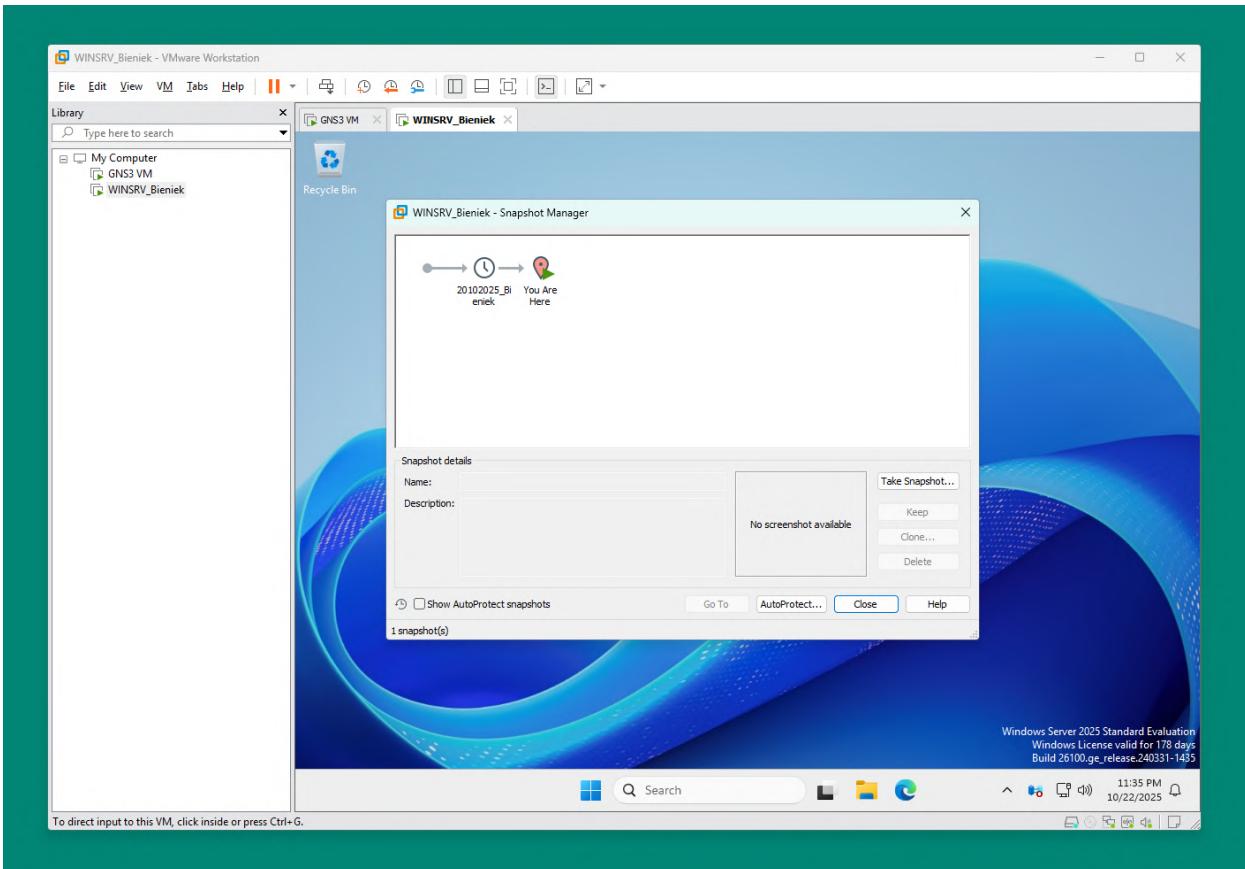
Zrzut ekranu 47 Ikonka oprogramowania VirtualBox widoczna na pasku narzędzi, wskazująca na działanie dodatków gościa.

Na tym etapie warto utworzyć migawki maszyn wirtualnych, aby po wprowadzeniu w przyszłości zmian, można było cofnąć się do stanu obecnego (w miarę czystego).

W środowisku VMware Workstation, wybieramy interesującą nas maszynę wirtualną z listy po lewej stronie. Następnie klikamy na nią prawym przyciskiem myszy i przechodzimy do „Snapshot” → „Snapshot Manager”. W otwierającym się okienku wybieramy „Take Snapshot...”, nadajemy nazwę migawki i zatwierdzamy.

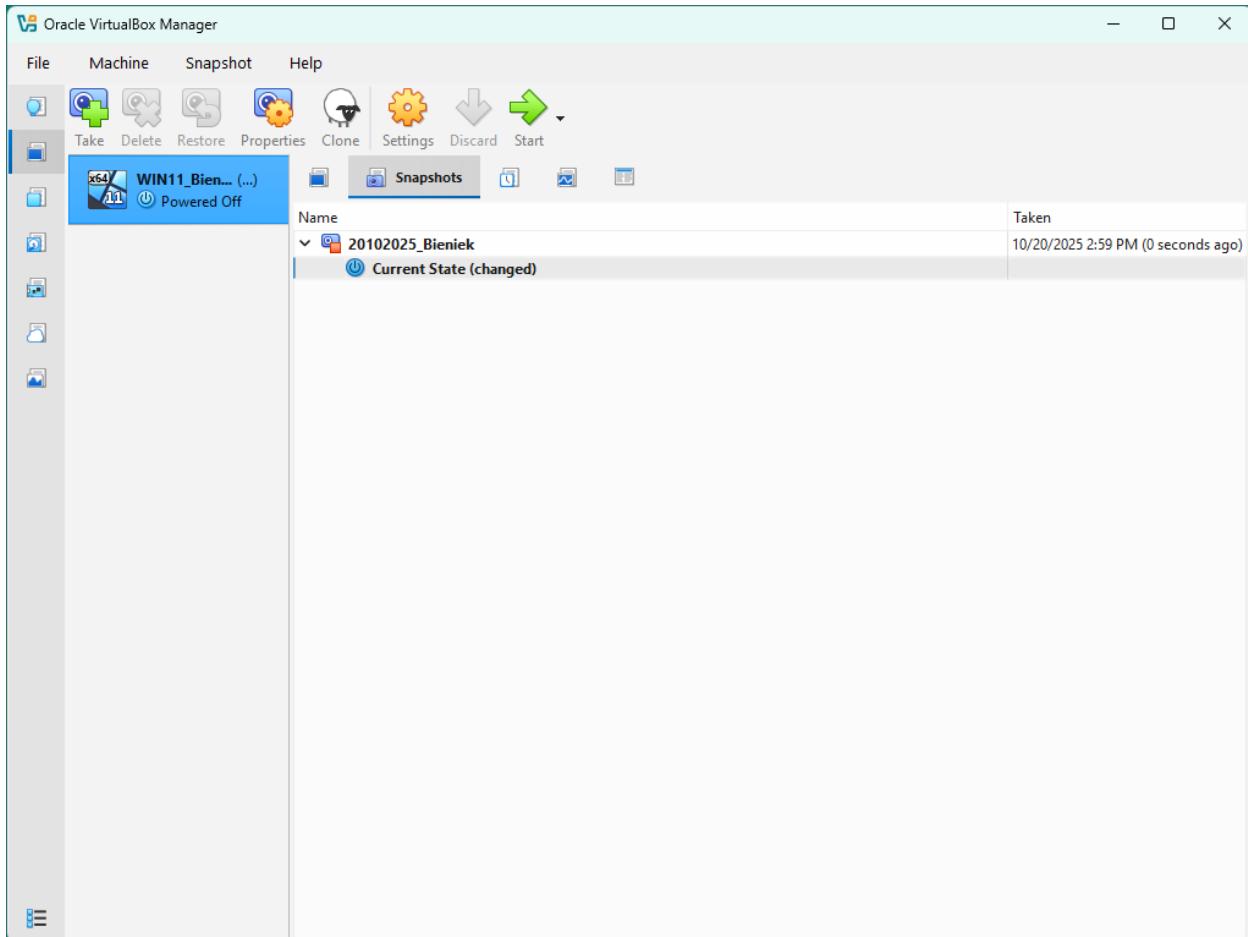


Zrzut ekranu 48 Tworzenie nowej migawki systemu w VMware Workspace.



Zrzut ekranu 49 Utworzona w programie VMware Workstation migawka maszyny wirtualnej.

W przypadku VirtualBox cały proces przebiega bardzo podobnie. Przechodzimy do zakładki „Snapshots” w prawym panelu i klikamy na przycisk „Take” z górnego menu. Następnie podajemy nazwę i zapisujemy migawkę.



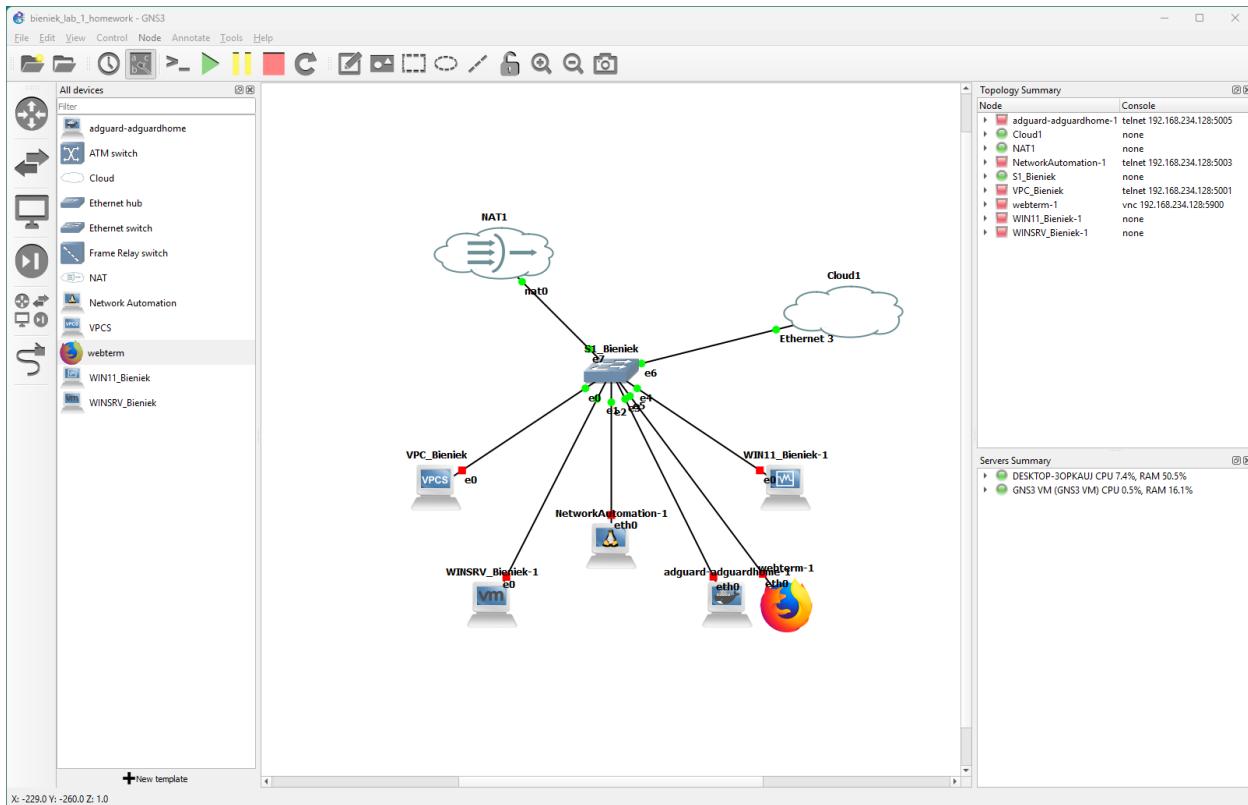
Zrzut ekranu 50 Utworzona migawka systemu w VirtualBox.

Zadanie 6. Konfiguracja AdGuard Home.

Oprogramowanie AdGuard Home działa jako serwer DNS i umożliwia między innymi filtrowanie i przepisywanie zapytań DNS. Zaprezentujmy jego działanie dodając wpis kierujący nazwę `winsrv.bieniek.pl` na adres maszyny wirtualnej z systemem Windows Server 2025.

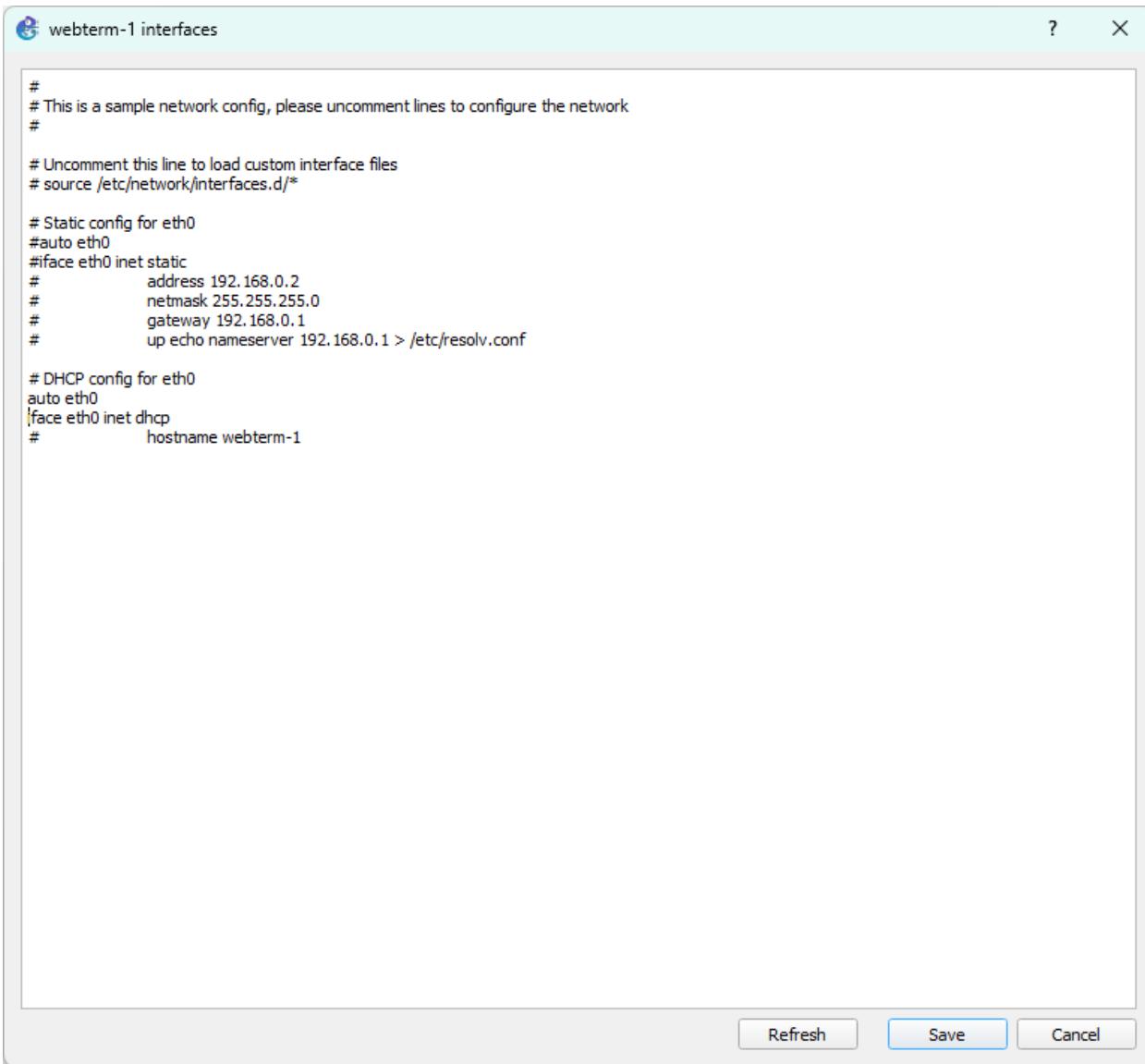
W rzeczywistości obydwu komputerom przypisaliśmy stałe adresy IP, jednak ze względu na brak kontroli nad „chmurą NAT”, w tym nad usługą DHCP, musimy skorzystać z adresów dynamicznych.

Usługą AdGuard Home można zarządzać z poziomu strony internetowej. Aby z niej skorzystać, w pierwszej kolejności dodajemy do naszej sieci kontener z przeglądarką internetową. W tym celu tworzymy nowy szablon wybierając przycisk „New template” na dole lewego zasobnika, a następnie wybieramy opcję „Install an appliance from the GNS3 server”. Do wyboru mamy dwie opcje – Firefox (webterm) lub Chromium. Ja postanowiłem wybrać pierwszą, po czym dodałem szablon przyciskiem „Install”. Tak utworzone „urządzenie” przeciągamy na planszę i łączymy kablem do wolnego portu przełącznika.



W dodanym w ten sposób kontenerze musimy włączyć interfejs sieciowy i aktywować pobieranie danych adresowych z usługi DHCP. W tym celu klikamy na niego prawym przyciskiem myszy, wybieramy opcję „Edit config” i na końcu pliku umieszczamy poniższe linijki.

```
auto eth0
iface eth0 inet dhcp
```

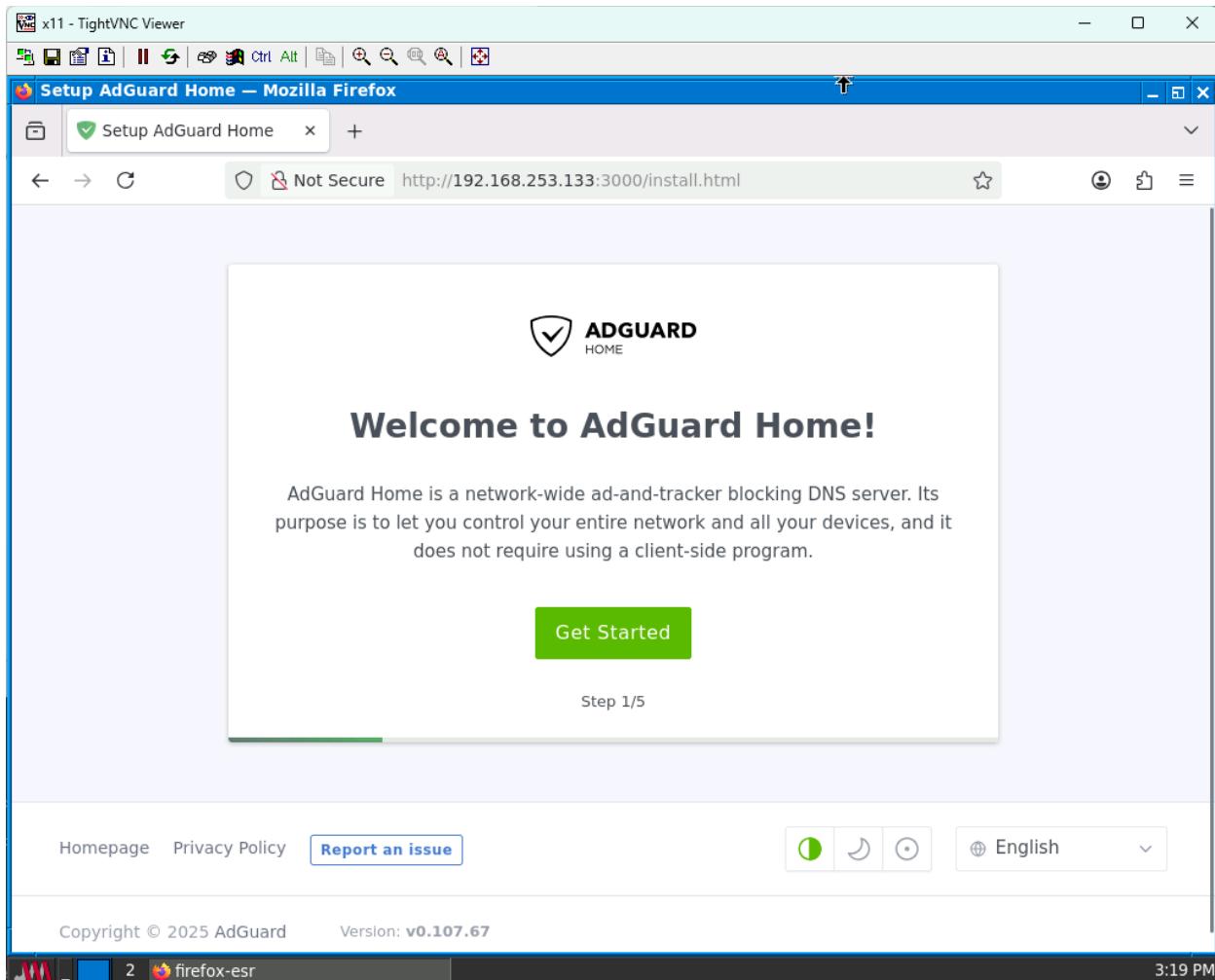


Zrzut ekranu 52 Konfiguracja sieciowa kontenera z przeglądarką internetową Mozilla Firefox (webterm).

Na koniec uruchamiamy kontener z serwerem AdGuard Home oraz webterm. Aby otworzyć okno przeglądarki i skonfigurować usługę, klikamy prawym myszy na ten ostatni i wybieramy opcję „Terminal”.

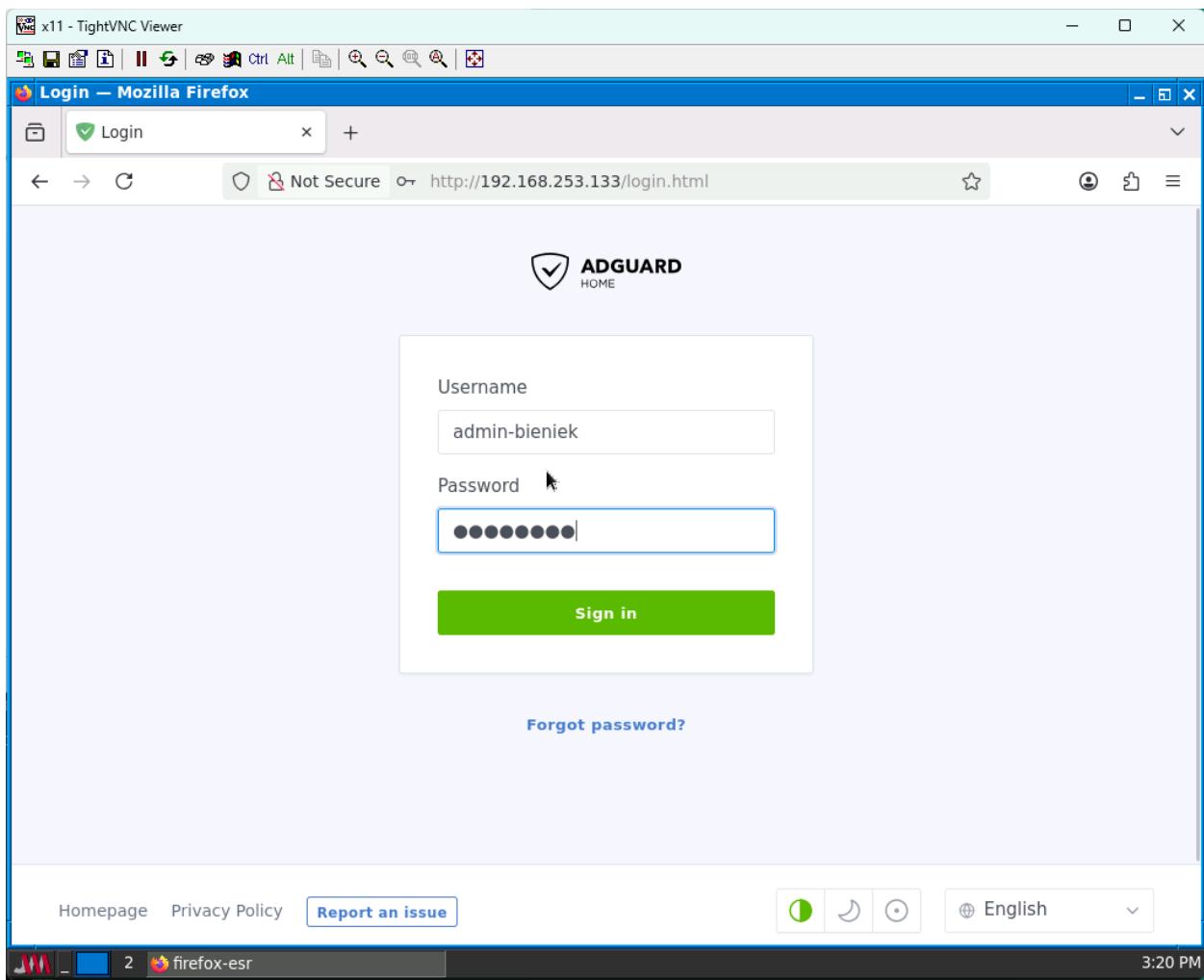
Konfiguracja AdGuard Home.

Przy pierwszym uruchomieniu AdGuard Home musimy przejść podstawową konfigurację. W tym celu wpisujemy w przeglądarce wskazany w terminalu kontenera adres, po czym uzupełniamy wszystkie wymagane pola.



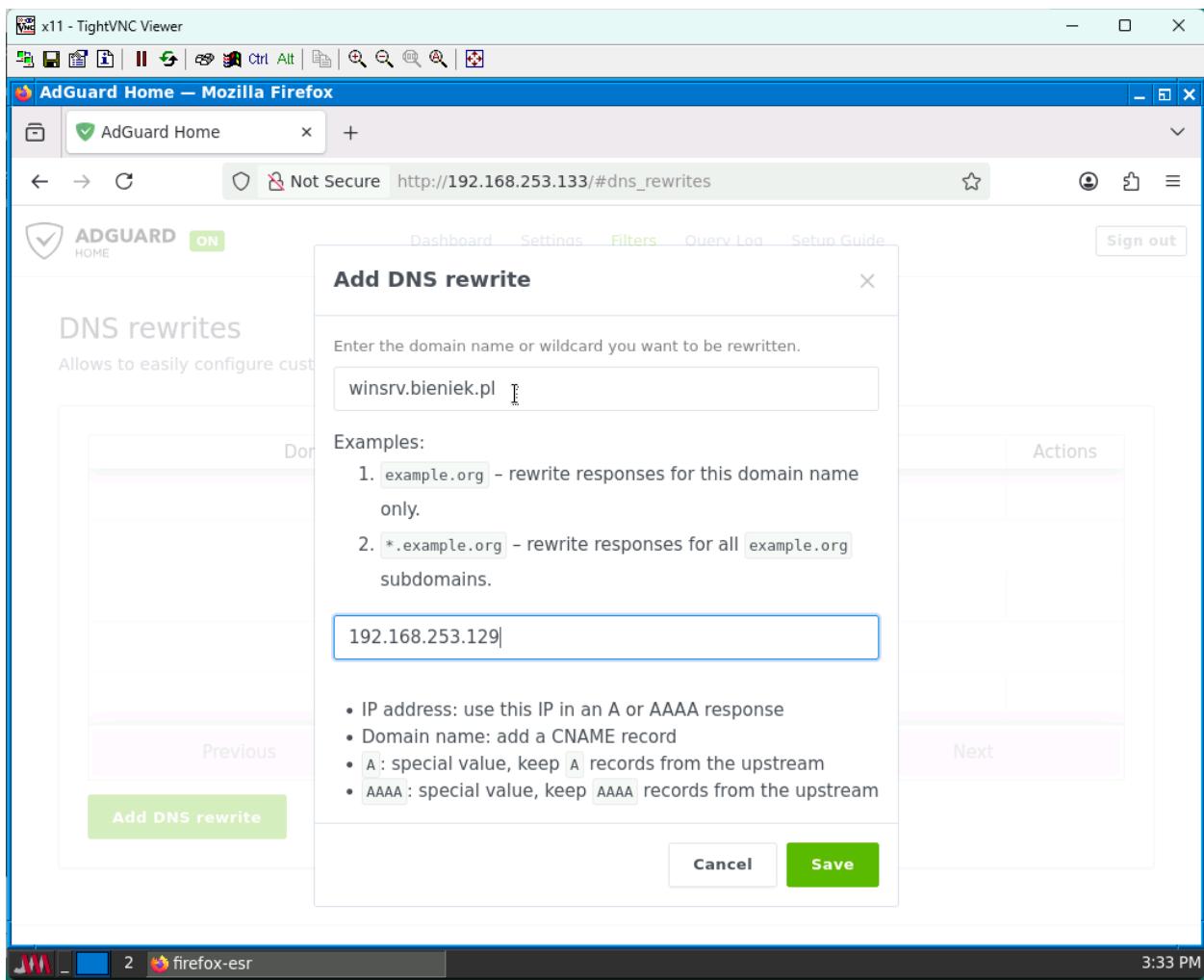
Zrzut ekranu 53 Ekran konfiguracji usługi AdGuard Home.

Po zakończonej konfiguracji klikamy przycisk „Open Dashboard” i logujemy się do panelu administracyjnego.



Zrzut ekranu 54 Ekran logowania do panelu administracyjnego AdGuard Home.

W celu zaprezentowania sposobu działania AdGuard Home dodamy przekierowanie nazwy `winsrv.bieniek.pl` na adres maszyny wirtualnej z systemem Windows Server 2025. W tym celu przechodzimy do zakładki „Filters” → „DNS rewrites” i dodajemy nowy rekord.

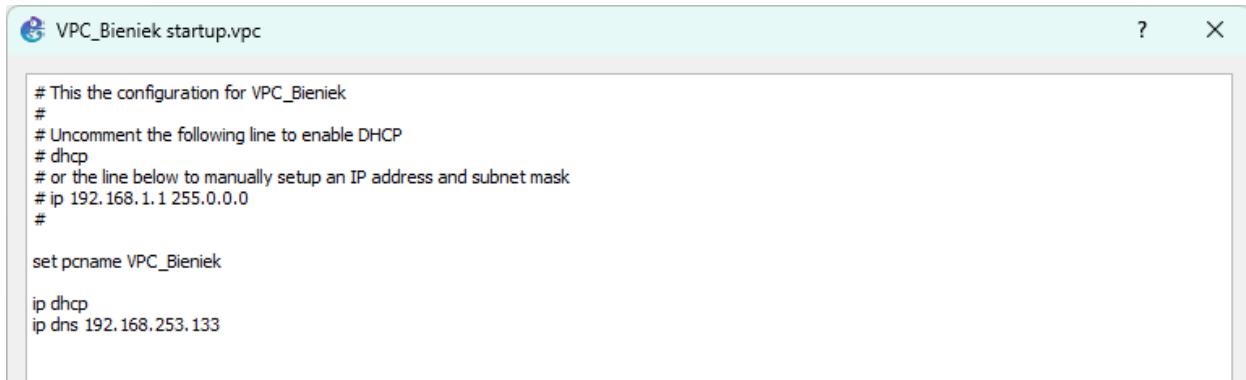


Zrzut ekranu 55 Ekran konfiguracji rekordu w zakładce przepisywania DNS.

Konfiguracja adresu serwera DNS w pozostałych komputerach w sieci.

Zaczniemy od konfiguracji komputera VPC. W tym celu klikamy prawym przyciskiem myszy na urządzenie i wybieramy opcję „Edit config”. Na końcu pliku konfiguracyjnego dodajemy poniższą linijkę, gdzie wskazany adres to adres kontenera AdGuard Home.

```
ip dns 192.168.253.133
```

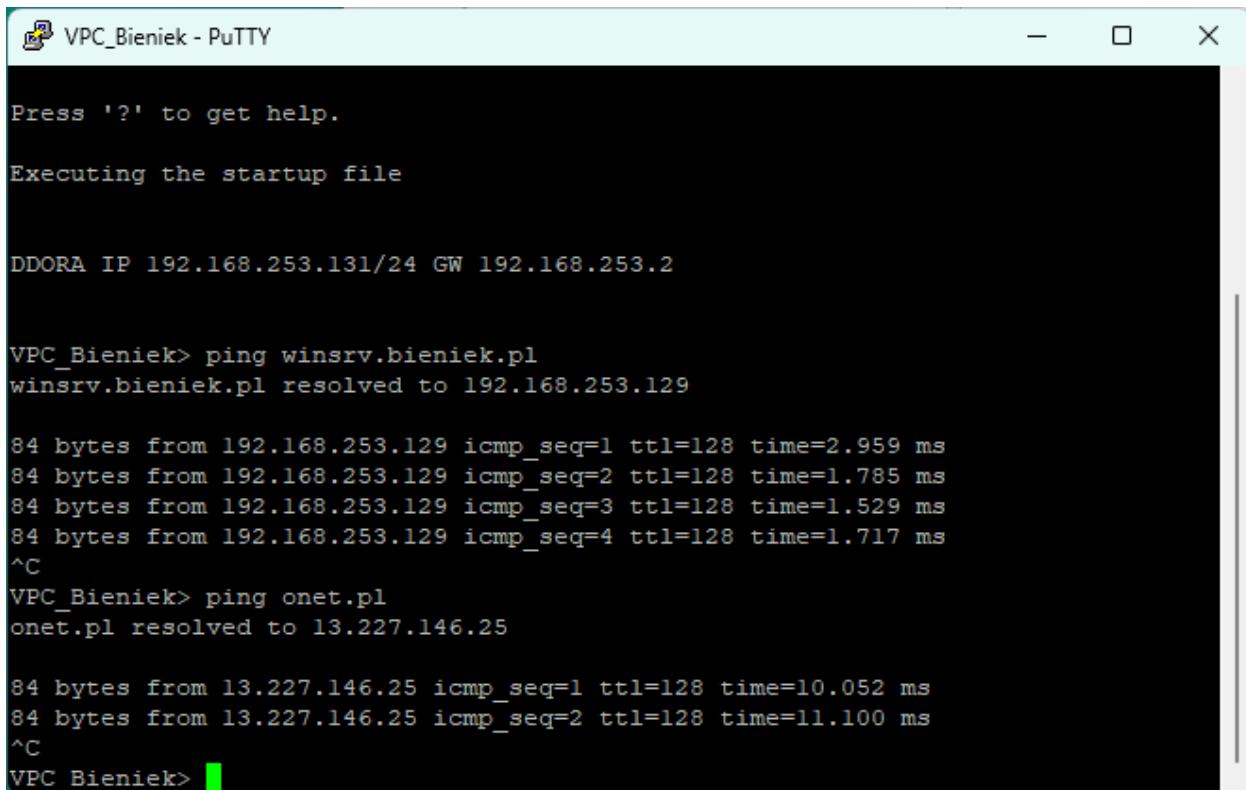


```
# This is the configuration for VPC_Bieniek
#
# Uncomment the following line to enable DHCP
# dhcp
# or the line below to manually setup an IP address and subnet mask
# ip 192.168.1.1 255.0.0.0
#
set pcname VPC_Bieniek

ip dhcp
ip dns 192.168.253.133
```

Po uruchomieniu maszyny możemy przetestować poprawność konfiguracji DNS.

Wykorzystamy do tego polecenie ping i sprawdzimy, czy system rozpoznaje nazwę winsrv.bieniek.pl oraz dowolną domenę publiczną.



```
Press '?' to get help.

Executing the startup file

DDORA IP 192.168.253.131/24 GW 192.168.253.2

VPC_Bieniek> ping winsrv.bieniek.pl
winsrv.bieniek.pl resolved to 192.168.253.129

84 bytes from 192.168.253.129 icmp_seq=1 ttl=128 time=2.959 ms
84 bytes from 192.168.253.129 icmp_seq=2 ttl=128 time=1.785 ms
84 bytes from 192.168.253.129 icmp_seq=3 ttl=128 time=1.529 ms
84 bytes from 192.168.253.129 icmp_seq=4 ttl=128 time=1.717 ms
^C

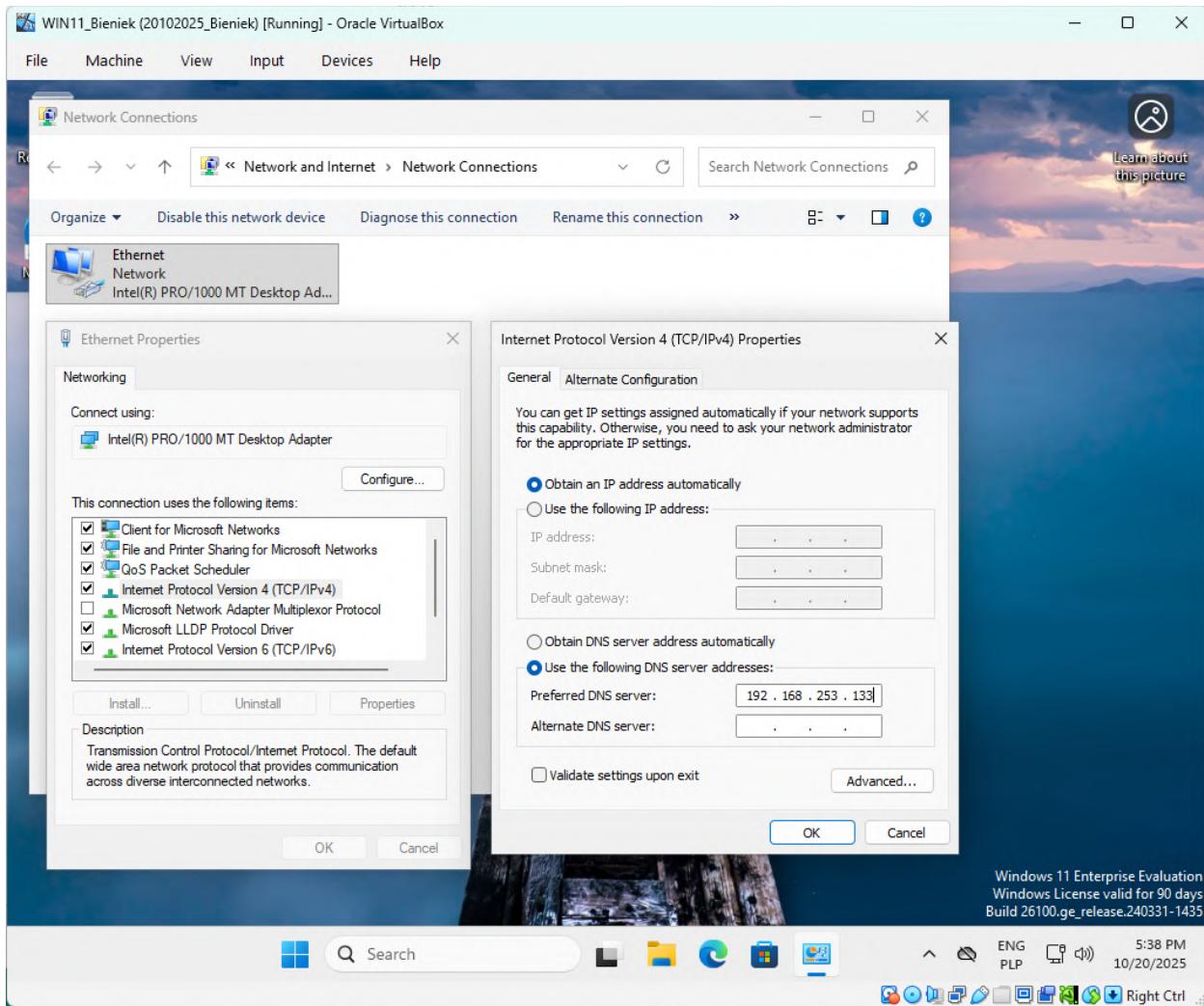
VPC_Bieniek> ping onet.pl
onet.pl resolved to 13.227.146.25

84 bytes from 13.227.146.25 icmp_seq=1 ttl=128 time=10.052 ms
84 bytes from 13.227.146.25 icmp_seq=2 ttl=128 time=11.100 ms
^C

VPC_Bieniek>
```

Zrzut ekranu 56 Sprawdzenie za pomocą polecenia ping konfiguracji DNS dla komputera VPC. Obie nazwy zostały poprawnie przepisane na adresy IP.

W przypadku komputerów z systemem Windows, wchodzimy we właściwości interfejsu sieciowego, a następnie z listy aktywnych elementów zaznaczamy „Internet Protocol Version 4 (TCP/IPv4)” i klikamy przycisk „Properties”. W sekcji dotyczącej konfiguracji DNS wybieramy „Use the following DNS server addresses:” i w polu „Preferred DNS server:” wpisujemy adres kontenera z uruchomioną usługą AdGuard Home, po czym zapisujemy zmiany. Proces powtarzamy dla obydwu maszyn z systemem Windows w naszej sieci.



Zrzut ekranu 57 Konfiguracja adresu serwera DNS w systemie Windows 11 Enterprise.

Podobnie jak wcześniej, z poziomu terminala poleceniem `ping` możemy sprawdzić, czy konfiguracja DNS działa poprawnie.



WIN11_Bieniek (20102025_Bieniek) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Windows PowerShell

```
PS C:\Users\mkowalski> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Users\mkowalski> ping winsrv.bieniek.pl

Pinging winsrv.bieniek.pl [192.168.253.129] with 32 bytes of data:
Reply from 192.168.253.129: bytes=32 time=5ms TTL=128
Reply from 192.168.253.129: bytes=32 time=2ms TTL=128
Reply from 192.168.253.129: bytes=32 time=2ms TTL=128
Reply from 192.168.253.129: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.253.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 2ms
PS C:\Users\mkowalski> ping onet.pl

Pinging onet.pl [13.227.146.64] with 32 bytes of data:
Reply from 13.227.146.64: bytes=32 time=12ms TTL=128
Reply from 13.227.146.64: bytes=32 time=11ms TTL=128
Reply from 13.227.146.64: bytes=32 time=10ms TTL=128
Reply from 13.227.146.64: bytes=32 time=11ms TTL=128

Ping statistics for 13.227.146.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 12ms, Average = 11ms
PS C:\Users\mkowalski>
```

Zrzut ekranu 58 Sprawdzenie za pomocą polecenia ping konfiguracji DNS dla komputera z systemem Windows 11 Enterprise. Obie nazwy zostały poprawnie przepisane na adresy IP.

The screenshot shows a Windows PowerShell window titled "Windows PowerShell" running on a Windows Server 2025 VM named "WINSRV_Bieniek". The window displays the following command and its output:

```
PS C:\Users\anowak> ipconfig /flushdns
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

PS C:\Users\anowak> ping winsrv.bieniek.pl

Pinging winsrv.bieniek.pl [192.168.253.129] with 32 bytes of data:
Reply from 192.168.253.129: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.253.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\anowak> ping google.com

Pinging google.com [142.250.186.206] with 32 bytes of data:
Reply from 142.250.186.206: bytes=32 time=12ms TTL=128
Reply from 142.250.186.206: bytes=32 time=12ms TTL=128
Reply from 142.250.186.206: bytes=32 time=12ms TTL=128
Reply from 142.250.186.206: bytes=32 time=11ms TTL=128

Ping statistics for 142.250.186.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 12ms, Average = 11ms
PS C:\Users\anowak>
```

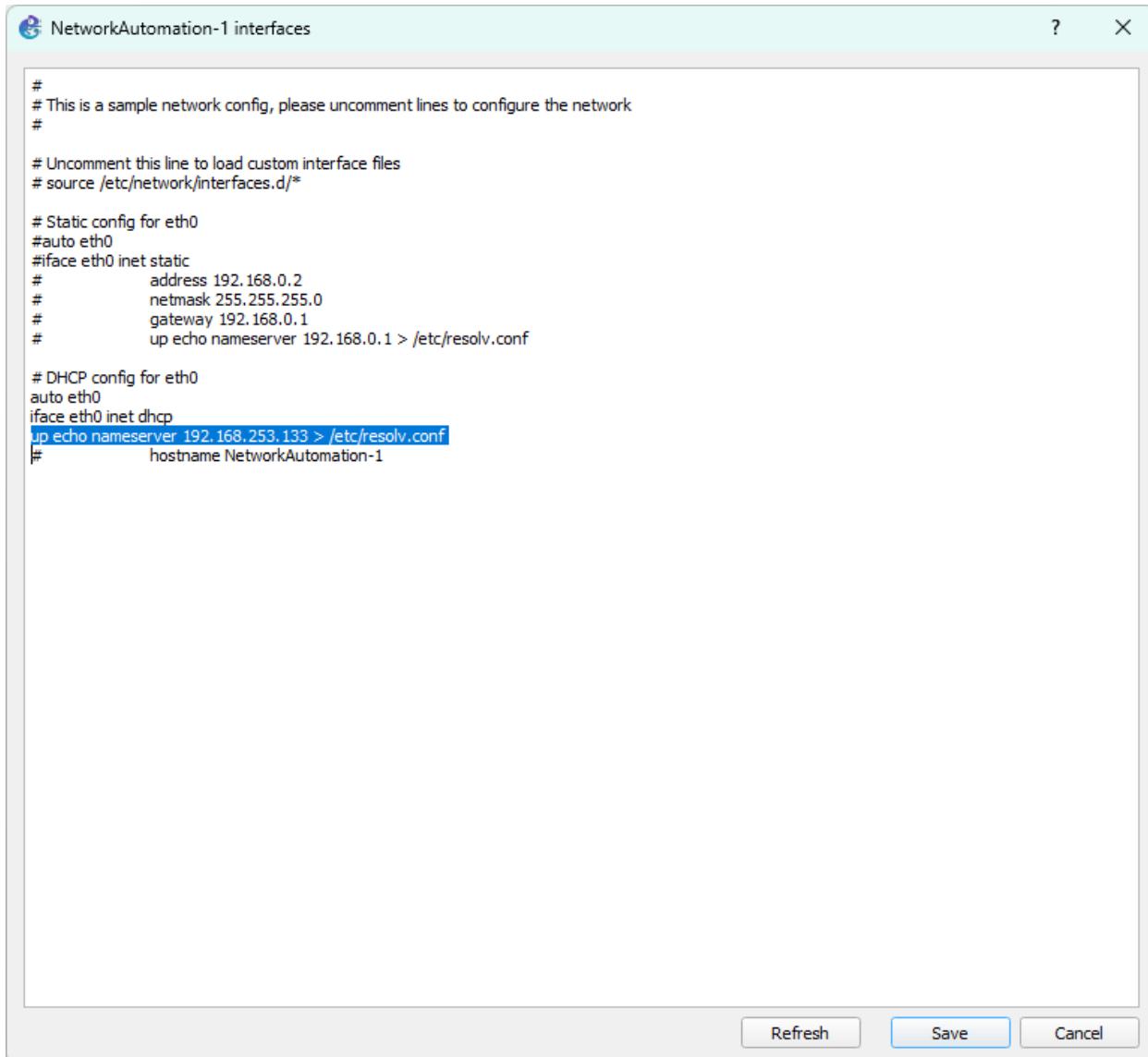
Zrzut ekranu 59 Sprawdzenie przy pomocy polecenia ping konfiguracji DNS dla komputera z systemem Windows Server 2025. Obie nazwy zostały poprawnie przepisane na adresy IP.

Jak można zauważyc, nazwy mnemoniczne są tłumaczone na adresy IP przy wykorzystaniu serwera DNS AdGuard Home w obydwu komputerach z systemem Windows.

Jako ostatni skonfigurujemy kontener NetworkAutomation. W tym celu otwieramy jego plik konfiguracyjny i na końcu dodajemy poniższe polecenie.

```
up echo nameserver 192.168.253.133 > /etc/resolv.conf
```

Po uruchomieniu interfejsu sieciowego nadpisze ono zawartość wskazanego pliku konfiguracyjnego DNS linijką „nameserver 192.168.253.133”.

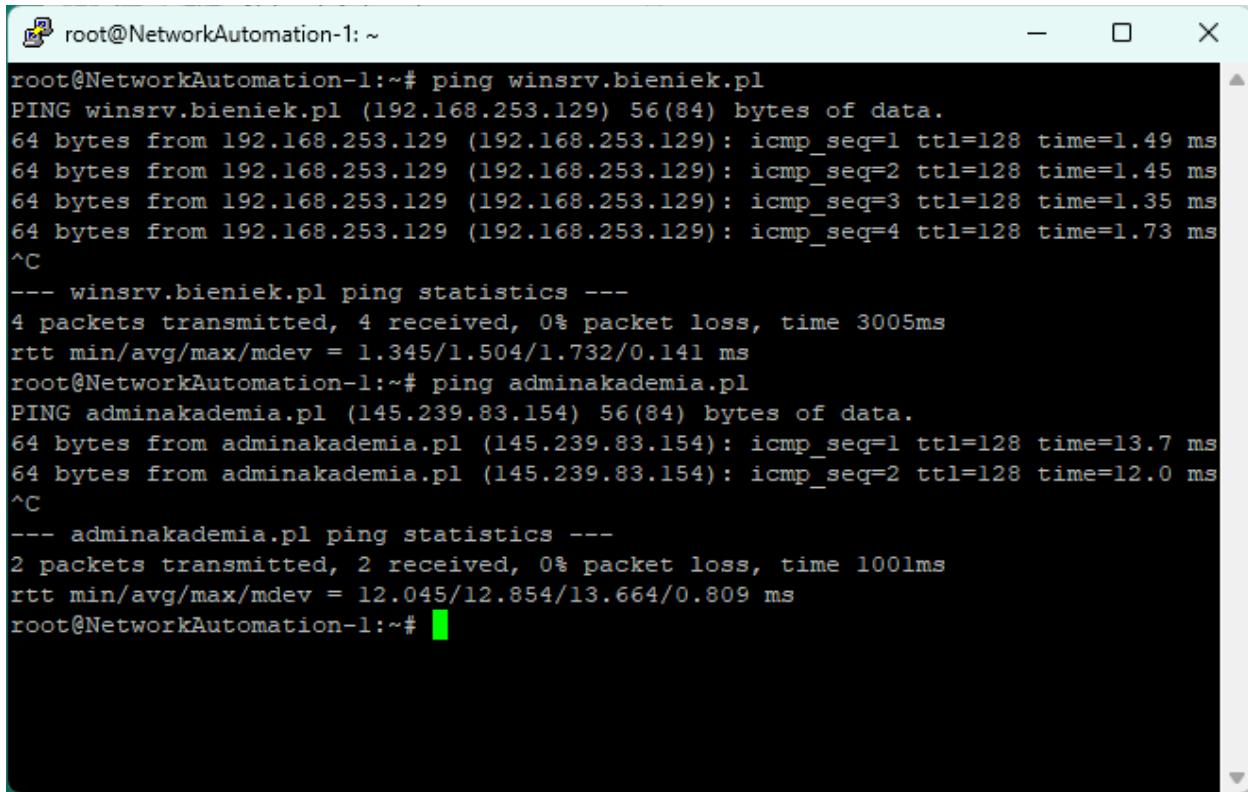


The screenshot shows a window titled "NetworkAutomation-1 interfaces". The main area contains a text editor with the following configuration:

```
# This is a sample network config, please uncomment lines to configure the network
#
# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*
#
# Static config for eth0
#auto eth0
#iface eth0 inet static
#       address 192.168.0.2
#       netmask 255.255.255.0
#       gateway 192.168.0.1
#       up echo nameserver 192.168.0.1 > /etc/resolv.conf
#
# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
up echo nameserver 192.168.253.133 > /etc/resolv.conf
#       hostname NetworkAutomation-1
```

At the bottom of the window are three buttons: "Refresh", "Save" (highlighted in blue), and "Cancel".

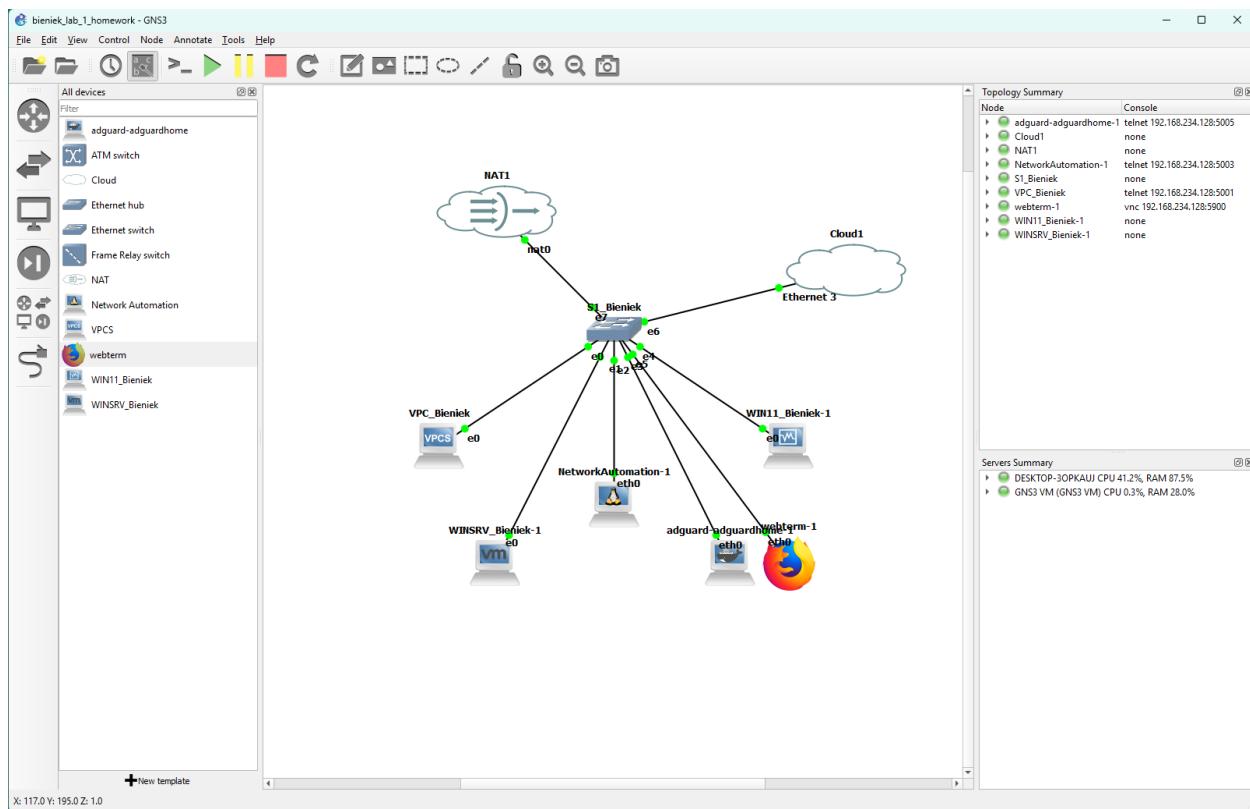
Zrzut ekranu 60 Plik konfiguracyjny kontenera NetworkAutomation-1.



```
root@NetworkAutomation-1:~# ping winsrv.bieniek.pl
PING winsrv.bieniek.pl (192.168.253.129) 56(84) bytes of data.
64 bytes from 192.168.253.129 (192.168.253.129): icmp_seq=1 ttl=128 time=1.49 ms
64 bytes from 192.168.253.129 (192.168.253.129): icmp_seq=2 ttl=128 time=1.45 ms
64 bytes from 192.168.253.129 (192.168.253.129): icmp_seq=3 ttl=128 time=1.35 ms
64 bytes from 192.168.253.129 (192.168.253.129): icmp_seq=4 ttl=128 time=1.73 ms
^C
--- winsrv.bieniek.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.345/1.504/1.732/0.141 ms
root@NetworkAutomation-1:~# ping adminakademia.pl
PING adminakademia.pl (145.239.83.154) 56(84) bytes of data.
64 bytes from adminakademia.pl (145.239.83.154): icmp_seq=1 ttl=128 time=13.7 ms
64 bytes from adminakademia.pl (145.239.83.154): icmp_seq=2 ttl=128 time=12.0 ms
^C
--- adminakademia.pl ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 12.045/12.854/13.664/0.809 ms
root@NetworkAutomation-1:~#
```

Zrzut ekranu 61 Sprawdzenie za pomocą polecenia ping konfiguracji DNS dla kontenera NetworkAutomation-1. Obie nazwy zostały poprawnie przepisane na adresy IP.

Tak jak w przypadku pozostałych urządzeń, również tutaj nazwy mnemoniczne zostały poprawnie przetłumaczone na adresy IP.



Zrzut ekranu 62 Kompletna topologia sieciowa.