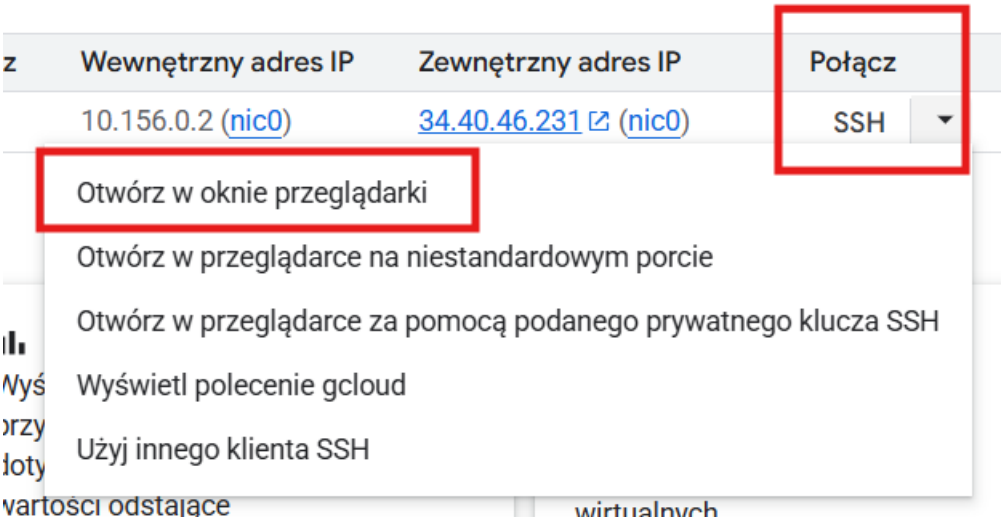
Wchodzimy po SSH do terminalu naszej Instancji VM.



Zmieniamy plik konfiguracyjny interfejsów sieciowych w Linuxie za pomocą edytora nano. Ścieżka do pliku poniżej. Wykonujemy komendę

sudo nano /etc/network/interfaces

```
root@juniper-lab-26-27-2005:/etc# cd network
root@juniper-lab-26-27-2005:/etc/network# ls
if-down.d  if-post-down.d  if-pre-up.d  if-up.d  interfaces  interfaces.d
root@juniper-lab-26-27-2005:/etc/network# nano interfaces
```

Jesteśmy w edycji pliku.

Przechodzimy kursorem do eth1 lub eth2. - to interfejsy Cloud 1 i 2 w panelu EVE.

```
  GNU nano 6.2                                      interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
iface eth0 inet manual
auto pnet0
iface pnet0 inet dhcp
    pre-up ip link set dev eth0 up
    bridge_hw eth0
    bridge_ports eth0
    bridge_stp off

# Cloud devices
iface eth1 inet manual
auto pnet1
iface pnet1 inet manual
    bridge_ports eth1
    bridge_stp off

iface eth2 inet manual
auto pnet2
iface pnet2 inet manual
    bridge_ports eth2
    bridge_stp off

iface eth3 inet manual
```

Założenia:

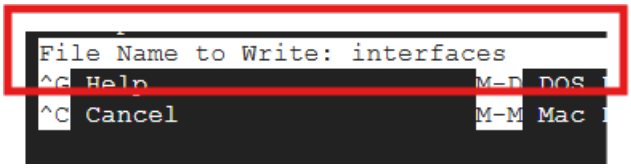
- pnet0 — dostęp do Internetu (DHCP).
- pnet2 — statyczny adres 172.16.100.100/24, działa jako interfejs lokalny.
- Chcesz, aby komputery w podsieci pnet2 (172.16.100.0/24) wychodziły do Internetu przez pnet0.

Dopisujemy dodatkowe wiersze jak poniżej. Uwaga zapis jest wrażliwy na wszelkie błędy składni oraz spacje. Wszystko musi być zgodne tak jak poniżej. Dla celów tego Labu proszę ustawienie adresacji tak jak na screenie.

```
iface eth2 inet manual
auto pnet2
iface pnet2 inet static
    address 172.16.100.100
    netmask 255.255.255.0
    dns-nameservers 8.8.8.8
    bridge_ports eth2
    bridge_stp off
```

Edycję pliku zapisujemy kolejno sekwencją skrótów:

1. CTRL + O



2. Enter
3. CTRL + X

Możemy sprawdzić czy się zapisało wchodząc jeszcze raz do pliku nano interfaces
Wychodzimy CTRL + X

Sprawdzamy poprawność zmian w pliku konfiguracji. Po pierwszej komendzie dajemy Enter , aby nie czeka na odwrócenie zmian.

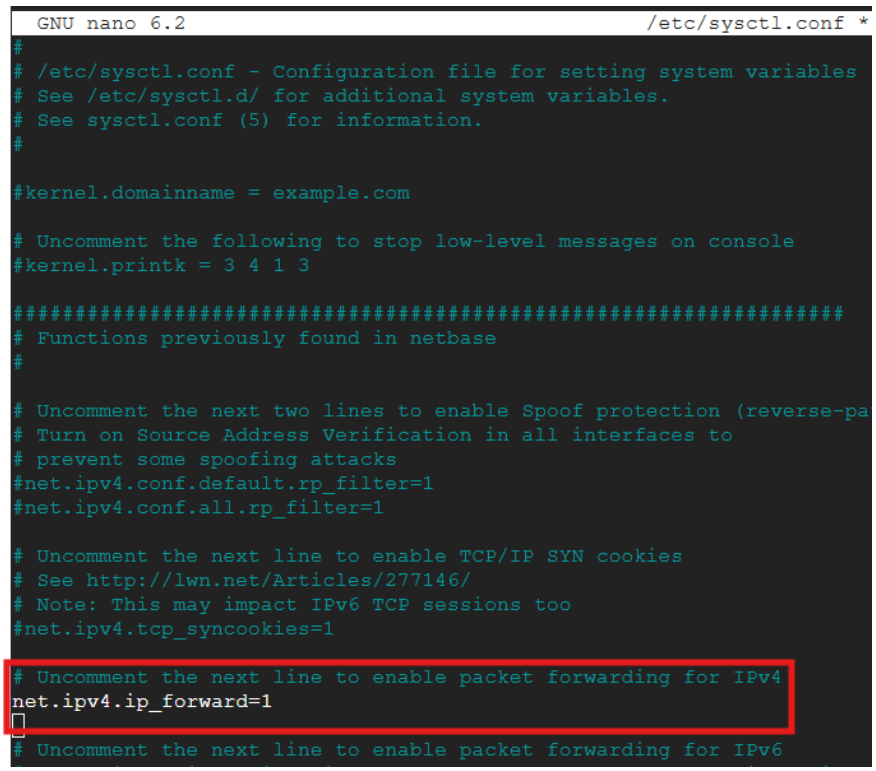
```
root@juniper-lab-26-27-2005:/etc/network# nano interfaces
root@juniper-lab-26-27-2005:/etc/network# netplan try
Do you want to keep these settings?


Press ENTER before the timeout to accept the new configuration


Changes will revert in 117 seconds
Configuration accepted.
root@juniper-lab-26-27-2005:/etc/network# netplan apply
root@juniper-lab-26-27-2005:/etc/network#
```

Włącz przekazywanie IPv4 na stałe komendą:

sudo nano /etc/sysctl.conf

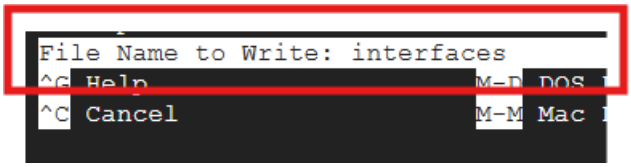
Odkomentuj usuwając znak # w linii:

net.ipv4.ip_forward = 1



Edycję pliku zapisujemy kolejno sekwencją skrótów:

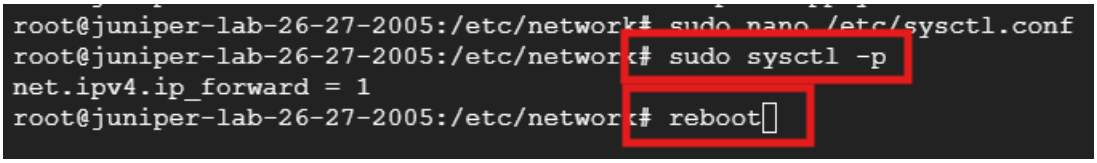
1. CTRL + O



2. Enter
3. CTRL + X

Możemy sprawdzić czy się zapisało wchodząc jeszcze raz do nano /etc/sysctl.conf
Wychodzimy CTRL + X

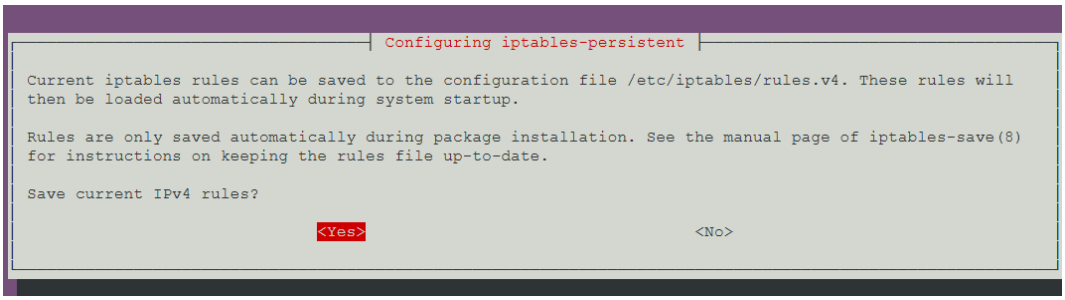
Wprowadzamy zmiany natychmiast:
sudo sysctl -p



Zerwie połączenie terminalu. Ponownie łączymy się SSH.
Wchodzimy na Roota: sudo -i

Zainstaluj pakiet iptables-persistent. Oczywiście spod roota.
Komendy wykonujemy osobno, czekając na rezultat!
apt update
apt install iptables-persistent

Wyskoczy okno gdzie dajemy Yes. Dalej nastąpi instalacja. Czekamy na wynik.



Teraz ustaw reguły NAT w iptables
Zakładamy, że pnet0 to interfejs z dostępem do Internetu, a pnet2 to sieć lokalna (172.16.100.0/24): Tworzymy NAT - maskarada dla ruchu wychodzącego przez pnet0

iptables -t nat -A POSTROUTING -s 172.16.100.0/24 -o pnet0 -j MASQUERADE

Zezwól na przekazywanie pakietów z pnet2 do pnet0. Zezwól na ruch powrotny
iptables -A FORWARD -i pnet2 -o pnet0 -j ACCEPT

iptables -A FORWARD -i pnet0 -o pnet2 -m state --state ESTABLISHED,RELATED -j ACCEPT

Zapisz reguły I wykonaj restart.
iptables-save | sudo tee /etc/iptables/rules.v4

Reboot

```
root@juniper-lab-26-27-2005:~# iptables -t nat -A POSTROUTING -s 172.16.100.0/24 -o pnet0 -j MASQUERADE
root@juniper-lab-26-27-2005:~# iptables -A FORWARD -i pnet2 -o pnet0 -j ACCEPT
root@juniper-lab-26-27-2005:~# iptables -A FORWARD -i pnet0 -o pnet2 -m state --state ESTABLISHED,RELATED -j ACCEPT
root@juniper-lab-26-27-2005:~# iptables-save | sudo tee /etc/iptables/rules.v4
# Generated by iptables-save v1.8.7 on Tue May 27 20:27:52 2025
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -i pnet2 -o pnet0 -j ACCEPT
-A FORWARD -i pnet0 -o pnet2 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -m string --hex-string "|03786d6c05636973636f03636f6d|" --algo bm --to 65535 -j DROP
COMMIT
# Completed on Tue May 27 20:27:52 2025
# Generated by iptables-save v1.8.7 on Tue May 27 20:27:52 2025
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 172.16.100.0/24 -o pnet0 -j MASQUERADE
COMMIT
# Completed on Tue May 27 20:27:52 2025
root@juniper-lab-26-27-2005:~# reboot
```

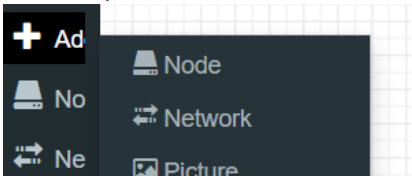
Przechodzimy do EVE-NG. W panelu Google Cloud klikamy na nasz adres publiczny. Jeżeli strona się nie otwiera to zmieniamy na http://nasz adres ip

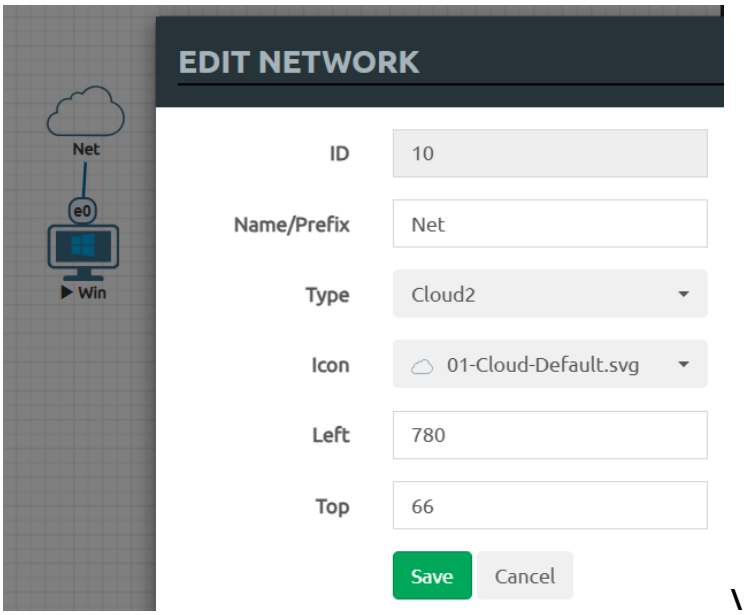
Domyślnie przeglądarka próbuje otworzyć przez https, gdzie nie mamy certyfikatu.
Zmieniamy na http.

Logujemy się danymi:
Login: admin
Password: eve
Z listy wybieramy Html5 console

Testujemy połączenie z EVE-NG do internetu.

Szyki test możemy wykonać przez dodanie Network (chmurki z wybranym interfejsem Cloud2).





Nasz interfejs łączymy z PC, gdzie kartę sieciową adresujemy statycznie. Oczywiście maszynę Windows musimy włączyć. Po ustawieniu adresu możemy wykonać ping do np. hostu wp.pl