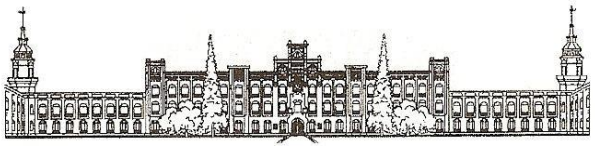

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»
ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

Лабораторна робота №8

з дисципліни «Системне програмне забезпечення»

«Конфігурування VPN»

Виконав студент IV курсу

групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

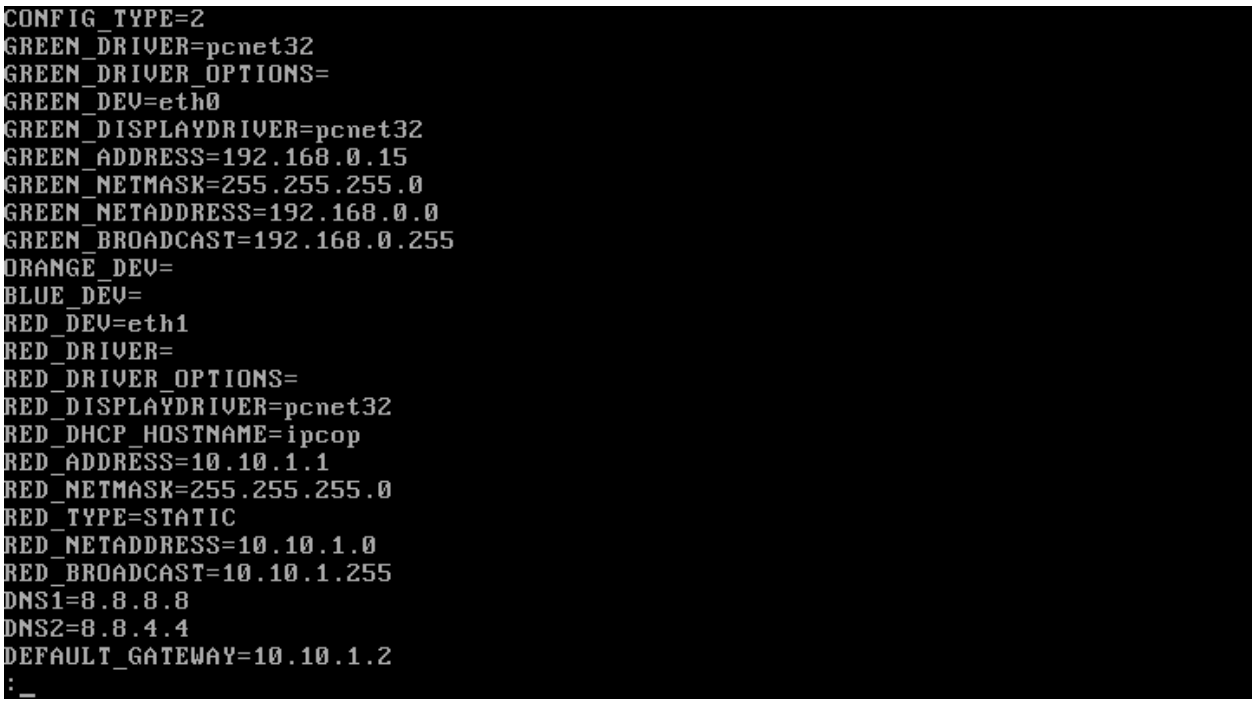

Рис. 1 – Налаштування мережевих інтерфейсів IPCop 1 (GREEN та RED).

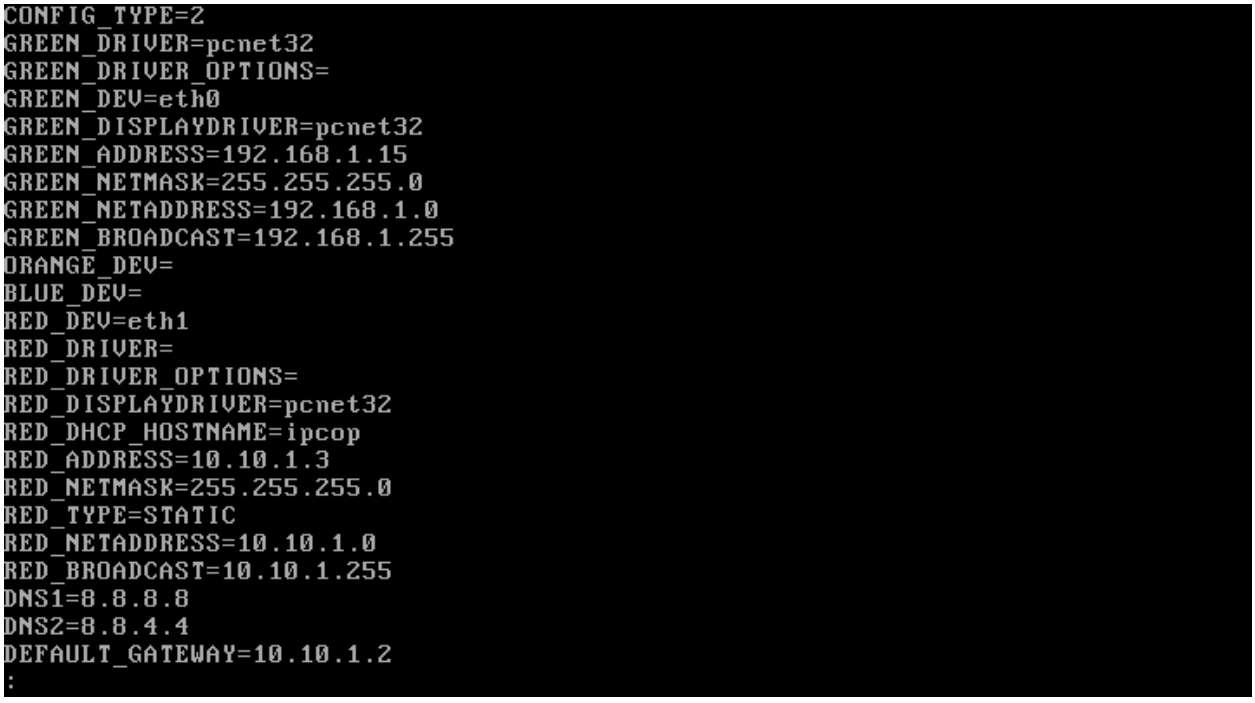

Рис. 2 – Налаштування мережевих інтерфейсів IPCop 2 (GREEN та RED).

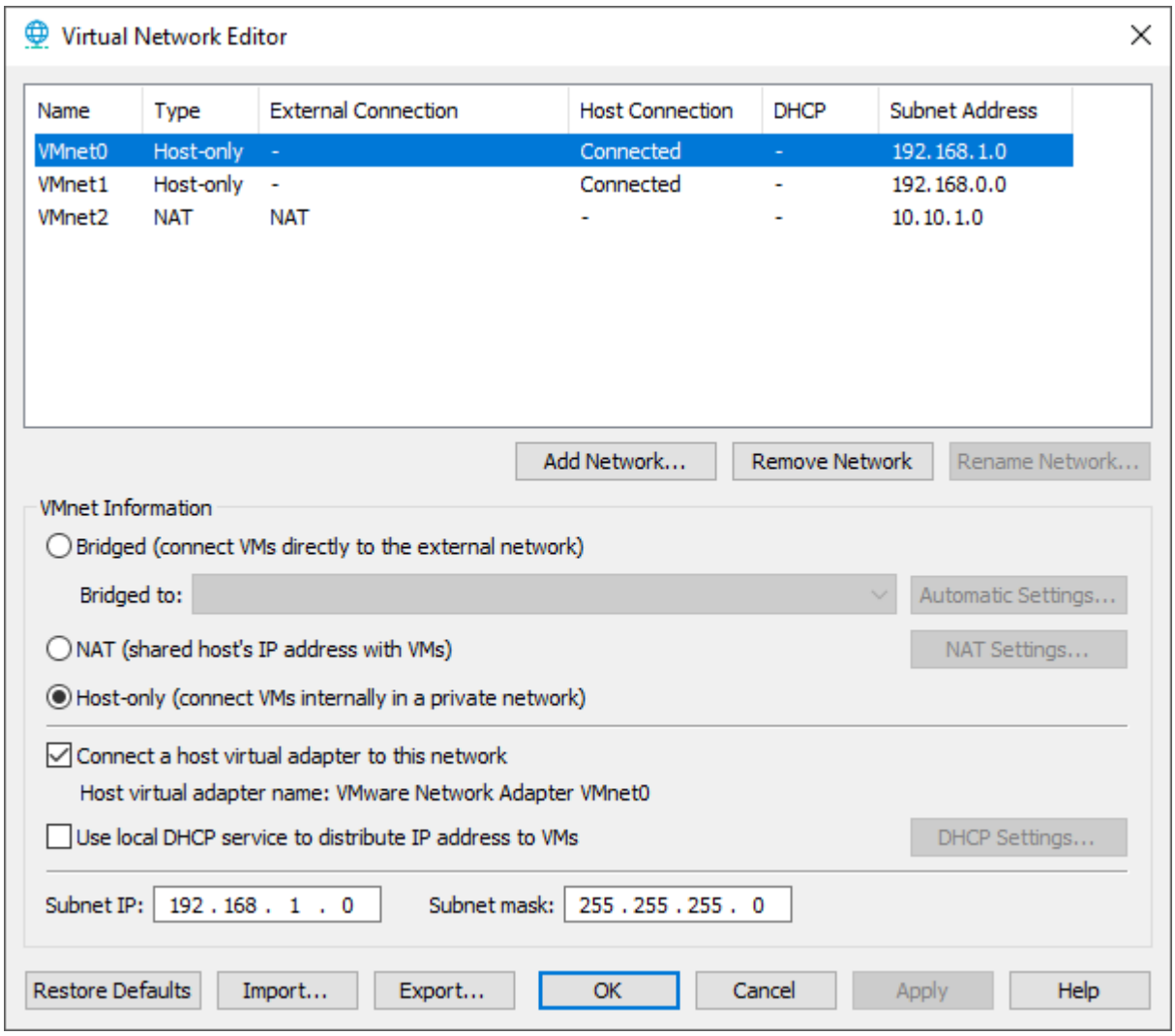

Рис. 3 – Налаштування Virtual Network Editor у VMware для мережевих сегментів.

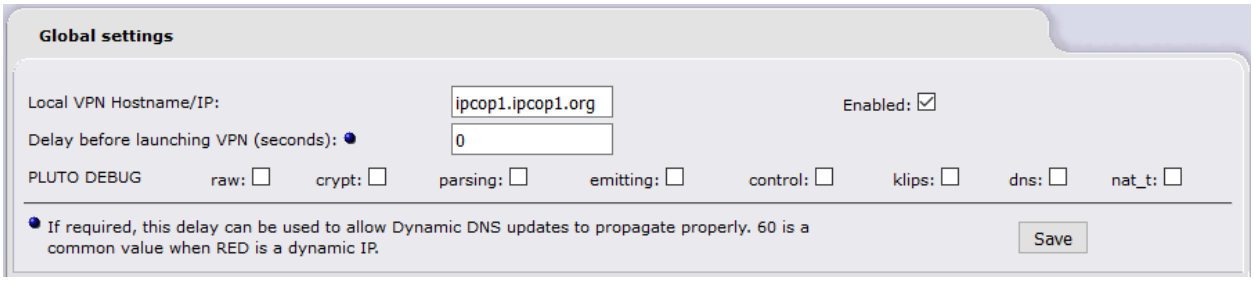

Рис. 4 – Глобальні налаштування VPN для IPCop 1 (hostname/IP).

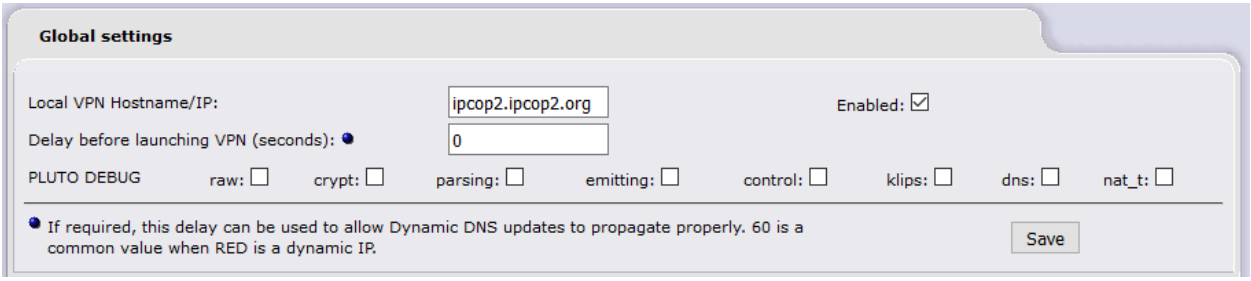

Рис. 5 – Глобальні налаштування VPN для IPCop 2 (hostname/IP).

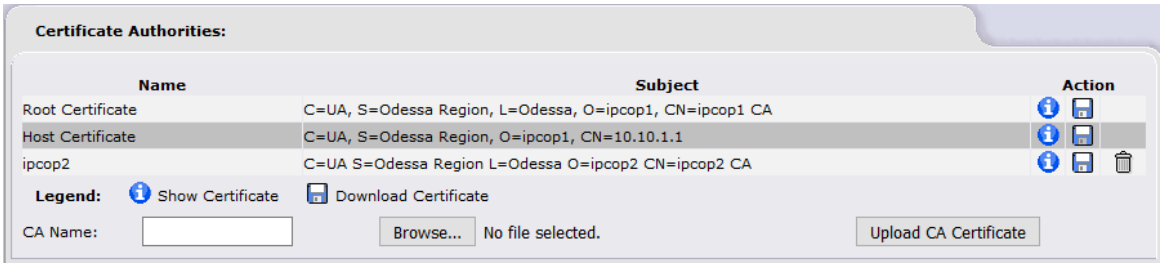

Рис. 6 – Список сертифікатів IPCop 1 (Root Certificate, Host Certificate, CA IPCop 2).

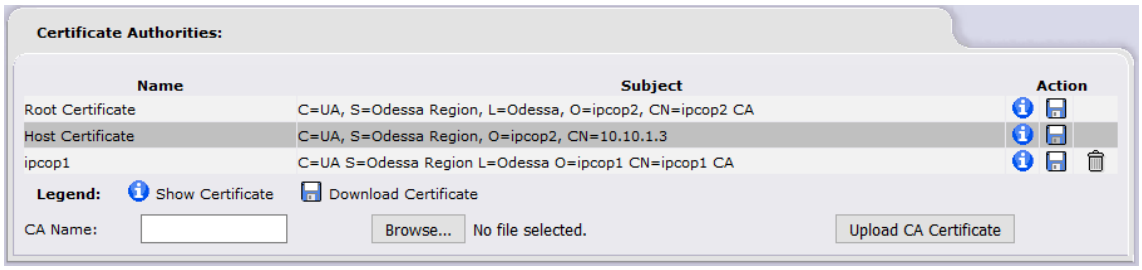

Рис. 7 – Список сертифікатів IPCop 2 (Root Certificate, Host Certificate, CA IPCop 1).

```
root@ipcop1:~ # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.10.1.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.10.1.0       0.0.0.0         255.255.255.0   U     0      0        0 ipsec0
0.0.0.0         10.10.1.2       0.0.0.0         UG    0      0        0 eth1
root@ipcop1:~ # ping 10.10.1.3
PING 10.10.1.3 (10.10.1.3): 56 data bytes
64 bytes from 10.10.1.3: icmp_seq=0 ttl=64 time=0.246 ms
64 bytes from 10.10.1.3: icmp_seq=1 ttl=64 time=0.176 ms
64 bytes from 10.10.1.3: icmp_seq=2 ttl=64 time=0.215 ms
64 bytes from 10.10.1.3: icmp_seq=3 ttl=64 time=0.277 ms
64 bytes from 10.10.1.3: icmp_seq=4 ttl=64 time=0.277 ms
--- 10.10.1.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.176/0.238/0.277/0.039 ms
```

Рис. 8 – Таблиця маршрутизації та результат пінгу з IPCop 1 до IPCop 2 (IP 10.10.1.3).

```
root@ipcop2:~ # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.10.1.0       0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.10.1.0       0.0.0.0         255.255.255.0   U     0      0        0 ipsec0
0.0.0.0         10.10.1.2       0.0.0.0         UG    0      0        0 eth1
root@ipcop2:~ # ping 10.10.1.1
PING 10.10.1.1 (10.10.1.1): 56 data bytes
64 bytes from 10.10.1.1: icmp_seq=0 ttl=64 time=0.181 ms
64 bytes from 10.10.1.1: icmp_seq=1 ttl=64 time=0.139 ms
64 bytes from 10.10.1.1: icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from 10.10.1.1: icmp_seq=3 ttl=64 time=0.172 ms
--- 10.10.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.139/0.170/0.190/0.000 ms
root@ipcop2:~ #
```

Рис. 9 – Таблиця маршрутизації та результат пінгу з IPCop 2 до IPCop 1 (IP 10.10.1.1).

Висновки

У процесі виконання лабораторної роботи було налаштовано VPN-з'єднання між двома віртуальними машинами на базі IPCop. Були створені сертифікати Root Certificate та Host Certificate для кожного вузла, а також проведений обмін CA-сертифікатами між вузлами для забезпечення взаємної довіри. Налаштовано мережеві інтерфейси для GREEN і RED зон на кожному IPCop, а також маршрутизація в середовищі VMware через Virtual Network Editor.

Під час тестування було успішно встановлено з'єднання між вузлами, що підтверджується позитивними результатами пінгів між підмережами (IP 10.10.1.1 та 10.10.1.3). Дані про активні тунелі та маршрути були перевірені на обох IPCop, що свідчить про правильну конфігурацію IPsec VPN.

Отримані результати демонструють можливість використання IPCop для створення безпечних тунелів у корпоративних або домашніх мережах. Робота дозволила закріпити навички конфігурування VPN, управління сертифікатами та налагодження маршрутизації у віртуальному середовищі.