Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

«Безпека комп'ютерних мереж»

Лабораторна робота №6
«Мережні екрани»
Варіант 2

Виконала:
студентка групи ФБ-95
Гурджия Валерія Вахтангівна

Київ-2022

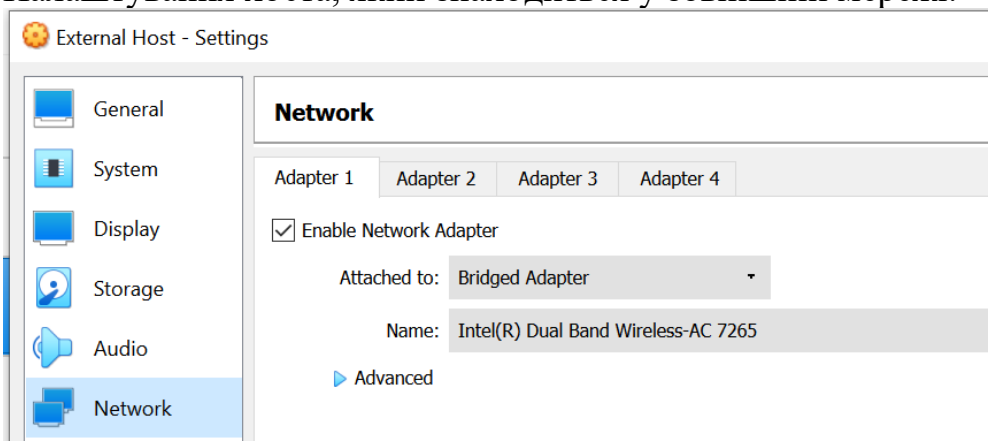
Завдання:

Є 2 мережі: зовнішня та внутрішня.

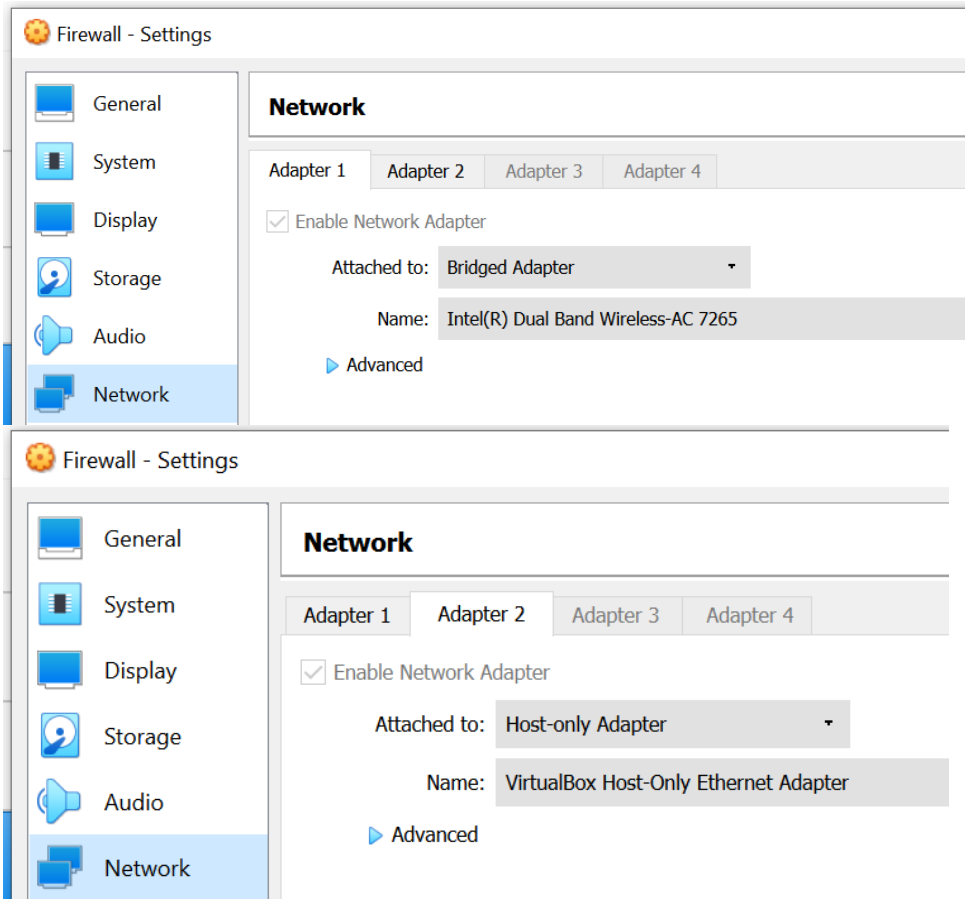
1) Зі зовнішніх мереж заборонити пінгувати хости внутрішньої мережі, але дозволити хостам внутрішньої мережі пінгувати зовнішні адреси.
2) Із зовнішніх мереж дозволити доступ лише до Web та FTP-серверів внутрішньої мережі.
3) Із зовнішніх мереж заборонити встановлювати з'єднання з деяким (одним) хостом внутрішньої мережі, однак цей хост повинен мати доступ до хостів у зовнішніх мережах.

1. Налаштування внутрішньої та зовнішньої мереж.
У зовнішній мережі знаходиться одна віртуальна машина External Host («Bridged Adapter»).
У внутрішній мережі знаходяться дві віртуальних машини, одна з яких має з'єднання з зовнішньою мережею, має тип «Host-only Adapter» та «Bridged Adapter». Віртуальна машина, яка належить лише до внутрішньої мережі, має тип мережевого адаптера «Host-only Adapter».

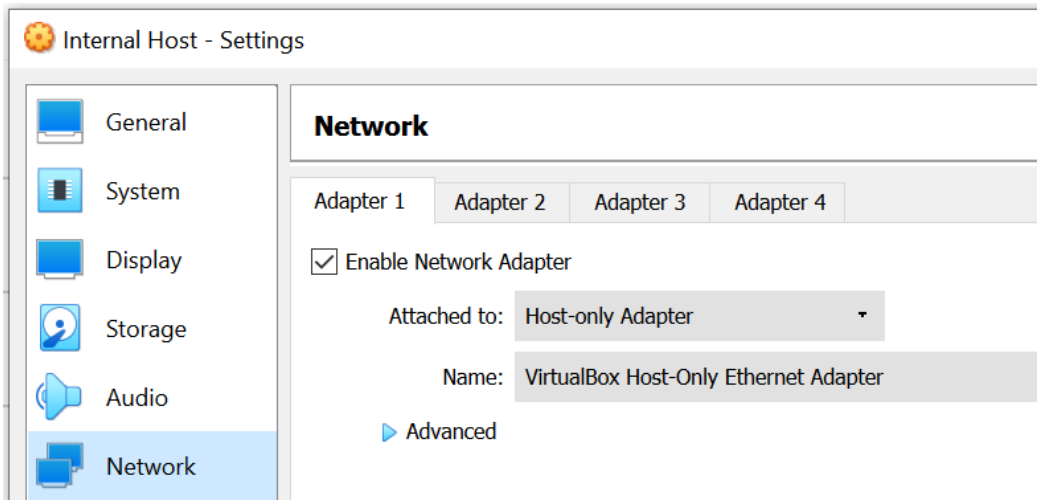
Налаштування хоста, який знаходиться у зовнішній мережі.



Налаштування хоста, який знаходиться у внутрішній мережі та має зв'язок з зовнішньою.



Налаштування хоста, який знаходиться у внутрішній мережі.



IP-адреса хоста зовнішньої мережі

```
lera@external-host:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.96  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::a0ad:72b9:a4f9:7572  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9f:1a:2b  txqueuelen 1000  (Ethernet)
        RX packets 68  bytes 16370 (16.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 125  bytes 14278 (14.2 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 150  bytes 12600 (12.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 150  bytes 12600 (12.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IP-адреси firewall

```
lera@firewall:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.97  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::1f0f:8f04:ce63:20ea  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:79:11:6a  txqueuelen 1000  (Ethernet)
        RX packets 153  bytes 22653 (22.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 166  bytes 17344 (17.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::41af:b11b:9ef6:247a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:57:fa:2a  txqueuelen 1000  (Ethernet)
        RX packets 41  bytes 6213 (6.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41  bytes 5130 (5.1 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 178  bytes 15070 (15.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 178  bytes 15070 (15.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IP-адреса хоста внутрішньої мережі

```
lera@internal-host:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::7a8d:16f2:cfab:75ef  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e9:d3:04  txqueuelen 1000  (Ethernet)
        RX packets 29  bytes 4918 (4.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 51  bytes 6085 (6.0 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 510  bytes 38066 (38.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 510  bytes 38066 (38.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Проведемо деякі налаштування

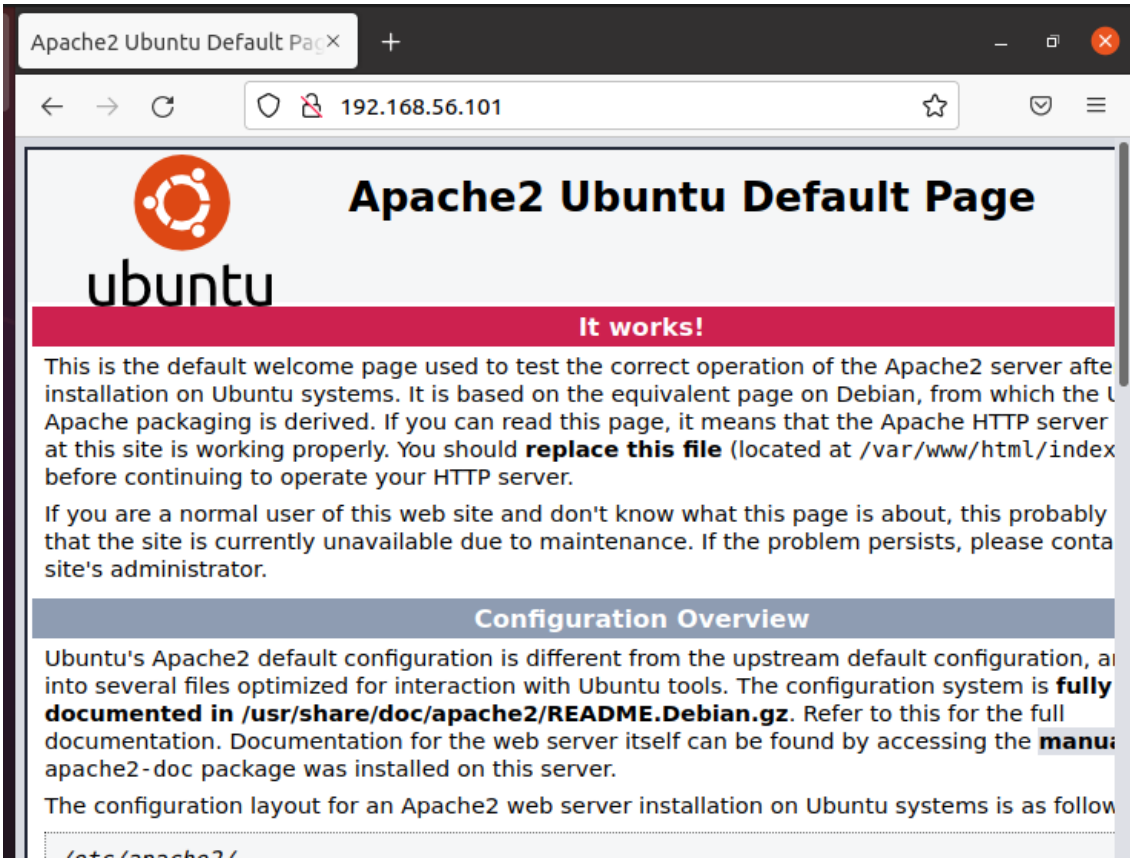
```
lera@external-host:~$ sudo ip route add 192.168.56.0/24 via 192.168.3.97
[sudo] password for lera:
lera@external-host:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.3.1     0.0.0.0         UG    100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
192.168.3.0     0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
192.168.56.0    192.168.3.97    255.255.255.0   UG    0      0        0 enp0s3
```

```
lera@internal-host:~$ sudo route add default gw 192.168.56.102
[sudo] password for lera:
lera@internal-host:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.56.102  0.0.0.0         UG    0      0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
192.168.56.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
```

```
root@firewall:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@firewall:~# iptables -t nat -A POSTROUTING -j MASQUERADE
root@firewall:~# iptables -F
root@firewall:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.3.1     0.0.0.0         UG    100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s8
192.168.3.0     0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
192.168.56.0    0.0.0.0         255.255.255.0   U     101    0        0 enp0s8
```

Запустимо WEB сервер apache2 на внутрішню мережу.

```
lera@internal-host:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor pres>
     Active: active (running) since Tue 2022-06-14 21:12:45 EEST; 7min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 661 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU>
   Main PID: 723 (apache2)
      Tasks: 55 (limit: 1087)
     Memory: 5.4M
     CGroup: /system.slice/apache2.service
             ├─723 /usr/sbin/apache2 -k start
             ├─726 /usr/sbin/apache2 -k start
             └─727 /usr/sbin/apache2 -k start

чер 14 21:12:45 internal-host systemd[1]: Starting The Apache HTTP Server...
чер 14 21:12:45 internal-host apachectl[686]: AH00558: apache2: Could not reli>
чер 14 21:12:45 internal-host systemd[1]: Started The Apache HTTP Server.
lines 1-16/16 (END)
```



Та FTP сервер vsftpd

```
lera@internal-host:~$ sudo systemctl status vsftpd
[sudo] password for lera:
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor prese>
     Active: active (running) since Tue 2022-06-14 21:12:45 EEST; 6min ago
    Process: 679 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited>
   Main PID: 684 (vsftpd)
      Tasks: 1 (limit: 1087)
     Memory: 676.0K
     CGroup: /system.slice/vsftpd.service
             └─684 /usr/sbin/vsftpd /etc/vsftpd.conf

чер 14 21:12:45 internal-host systemd[1]: Starting vsftpd FTP server...
чер 14 21:12:45 internal-host systemd[1]: Started vsftpd FTP server.
lines 1-12/12 (END)
```

За допомогою nmap перевірили, які порти є відкритими у внутрішній мережі.

```
root@internal-host-1:~# nmap 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-14 20:41 EEST
Nmap scan report for 192.168.56.101
Host is up (0.00013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 08:00:27:E9:D3:04 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@internal-host-1:~#
```

Видалимо всі правила

```
root@internal-host-1:~# iptables -F
root@internal-host-1:~#
```

Зі зовнішніх мереж заборонити пінгувати хости внутрішньої мережі, але дозволити хостам внутрішньої мережі пінгувати зовнішні адреси.

```
root@firewall:~# iptables -A INPUT -p icmp -s 192.168.56.0/24 -d 192.168.3.0/24 -j ACCEPT
root@firewall:~# iptables -A OUTPUT -p icmp -s 192.168.56.0/24 -d 192.168.3.0/24 -j ACCEPT
root@firewall:~# iptables -A INPUT -p icmp -s 192.168.3.0/24 -d 192.168.56.0/24 --icmp-type echo-request -j DROP
root@firewall:~# iptables -A FORWARD -p icmp -d 192.168.56.0/24 --icmp-type echo-request -j DROP
root@firewall:~#
root@firewall:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  192.168.56.0/24      192.168.3.0/24
DROP       icmp --  192.168.3.0/24       192.168.56.0/24      icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             192.168.56.0/24      icmp echo-request

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  192.168.56.0/24      192.168.3.0/24
```

Спробували пропінгувати зовнішню мережу із внутрішньої

```
lera@internal-host:~$ ping -c 4 192.168.3.96
PING 192.168.3.96 (192.168.3.96) 56(84) bytes of data.
64 bytes from 192.168.3.96: icmp_seq=1 ttl=63 time=1.32 ms
64 bytes from 192.168.3.96: icmp_seq=2 ttl=63 time=2.62 ms
64 bytes from 192.168.3.96: icmp_seq=3 ttl=63 time=2.35 ms
64 bytes from 192.168.3.96: icmp_seq=4 ttl=63 time=1.03 ms

--- 192.168.3.96 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.032/1.830/2.617/0.668 ms
```

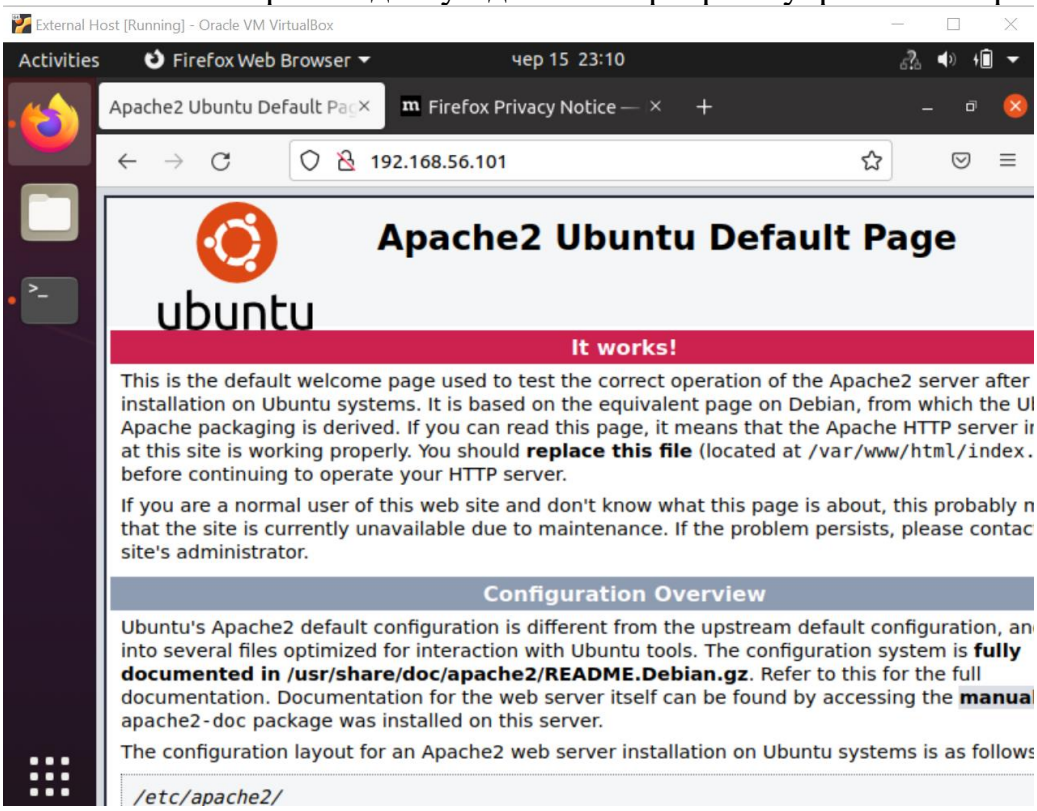
Спробували пропінгувати внутрішню мережу із внутрішньою

```
lera@external-host:~$ ping -c 3 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.

--- 192.168.56.101 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2042ms
```

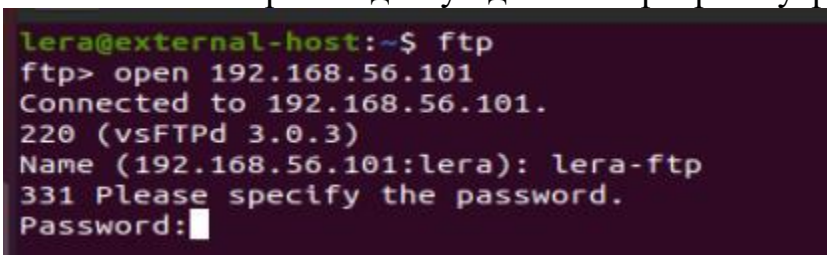
Із зовнішніх мереж дозволити доступ лише до Web та FTP-серверів внутрішньої мережі.

```
root@firewall:~# iptables -A FORWARD -p tcp --dport 80 -s 192.168.3.0/24 -d 192.168.56.0/24 -j ACCEPT
root@firewall:~# iptables -A FORWARD -p tcp --dport 21 -s 192.168.3.0/24 -d 192.168.56.0/24 -j ACCEPT
root@firewall:~#
root@firewall:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  192.168.56.0/24      192.168.3.0/24
DROP       icmp --  192.168.3.0/24       192.168.56.0/24      icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             192.168.56.0/24      icmp echo-request
ACCEPT     tcp  --  192.168.3.0/24       192.168.56.0/24      tcp dpt:http
ACCEPT     tcp  --  192.168.3.0/24       192.168.56.0/24      tcp dpt:ftp

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  192.168.56.0/24      192.168.3.0/24
```

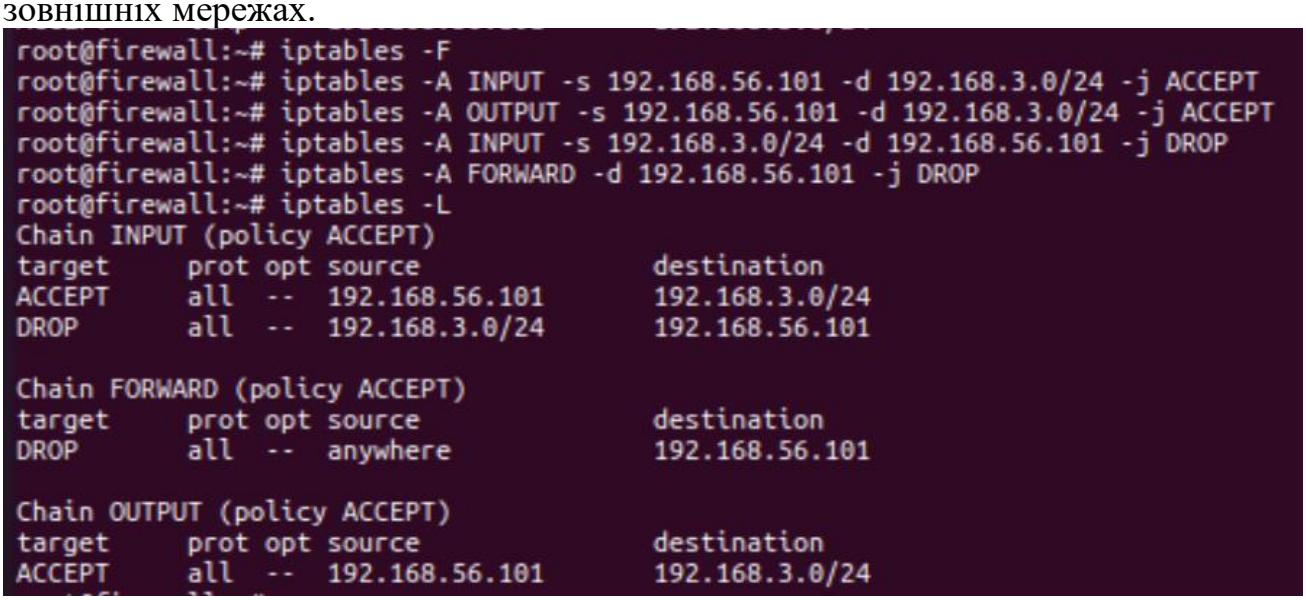
Із зовнішньої мережі є доступ до Web сервера внутрішньої мережі



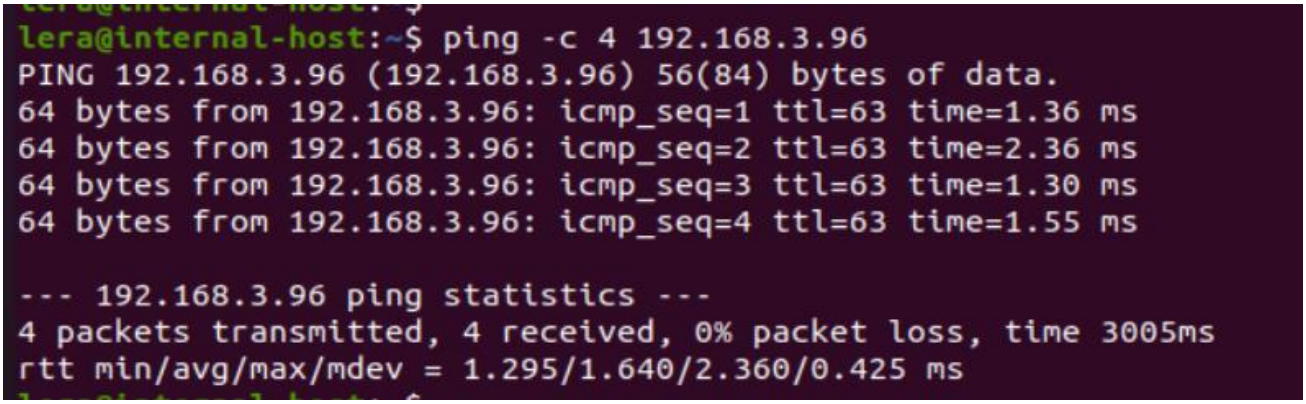
Із зовнішньої мережі є доступ до FTP сервера внутрішньої мережі



Із зовнішніх мереж заборонити встановлювати з'єднання з деяким (одним) хостом внутрішньої мережі, однак цей хост повинен мати доступ до хостів у зовнішніх мережах.



Спробували з’єднатись до хоста зовнішньої мережі із внутрішнього хоста 192.168.56.101



Спробували з’єднатись до хоста внутрішньої мережі 192.168.56.101 із зовнішньої мережі