

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO THỰC HÀNH

Bài 5: Cài đặt, cấu hình mạng doanh nghiệp với Pfsensefirewall

Họ và tên: Vũ Thành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cương

Hà Nội, 2024

Mục lục

I. Tìm hiểu lý thuyết.....	2
1. Mạng ảo	2
2. pfSense.....	2
II. Mô tả cài đặt & kết quả.....	2
1. Cấu hình topo mạng	2
2. Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP.....	20
3. Cài đặt cấu hình pfSense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal	25
III. Tài liệu tham khảo.....	31

I. Tìm hiểu lý thuyết:

1. Mạng ảo:

- Mạng ảo cho phép giao tiếp giữa nhiều máy tính, máy ảo (VM), máy chủ ảo hoặc các thiết bị khác trên các vị trí văn phòng và trung tâm dữ liệu khác nhau. Trong khi mạng vật lý kết nối các máy tính thông qua cáp và phần cứng khác, mạng ảo mở rộng các khả năng này bằng cách sử dụng quản lý phần mềm để kết nối máy tính và máy chủ qua Internet.
- Mạng ảo cho phép các thiết bị trên nhiều địa điểm hoạt động với các khả năng tương tự như mạng vật lý truyền thống. Điều này cho phép các trung tâm dữ liệu trải dài trên các vị trí địa lý khác nhau và cung cấp cho quản trị viên mạng các tùy chọn mới và hiệu quả hơn, như khả năng dễ dàng sửa đổi mạng khi nhu cầu thay đổi mà không cần phải thay đổi hay mua mới phần cứng; linh hoạt hơn trong việc cung cấp mạng cho các nhu cầu và ứng dụng cụ thể; và khả năng di chuyển công việc trên cơ sở hạ tầng mạng mà không ảnh hưởng đến dịch vụ, bảo mật và tính khả dụng.
- VMWare cung cấp tính năng tạo và cấu hình mạng ảo thông qua giao diện Virtual Network Editor.


2. pfSense:

- pfSense là phần mềm máy tính tường lửa / bộ định tuyến mã nguồn mở dựa trên FreeBSD.
- pfSense có thể được cài đặt trên máy tính vật lý hoặc máy ảo để tạo tường lửa / bộ định tuyến chuyên dụng cho mạng.
- pfSense có cung cấp giao diện đồ họa (GUI) qua giao diện HTTP, giúp quản trị viên cấu hình tường lửa dễ dàng hơn.

II. Mô tả cài đặt & kết quả:

1. Cấu hình topo mạng:

- Trước hết, mở VMWare Virtual Network Editor, sau đó tạo hai mạng ảo là vmnet1 và vmnet2 với dải IP 192.168.100.0 và 10.10.19.0.
- Có thể sử dụng host-only mà không cần NAT vì các máy ảo không cần kết nối với các trang web thật như Google, Bing, v.v.


Virtual Network Editor
✕

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.100.0
VMnet2	Host-only	-	Connected	Enabled	10.10.19.0

Add Network...
Remove Network
Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)
Bridged to: Automatic Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

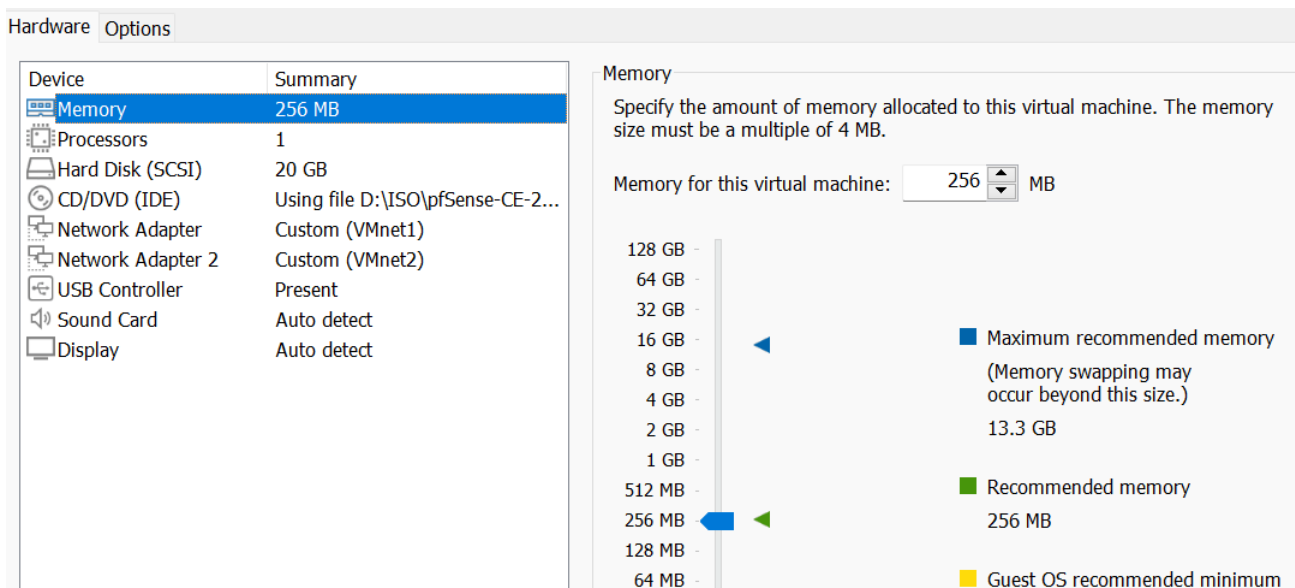
☒ Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet2

☒ Use local DHCP service to distribute IP address to VMs DHCP Settings...

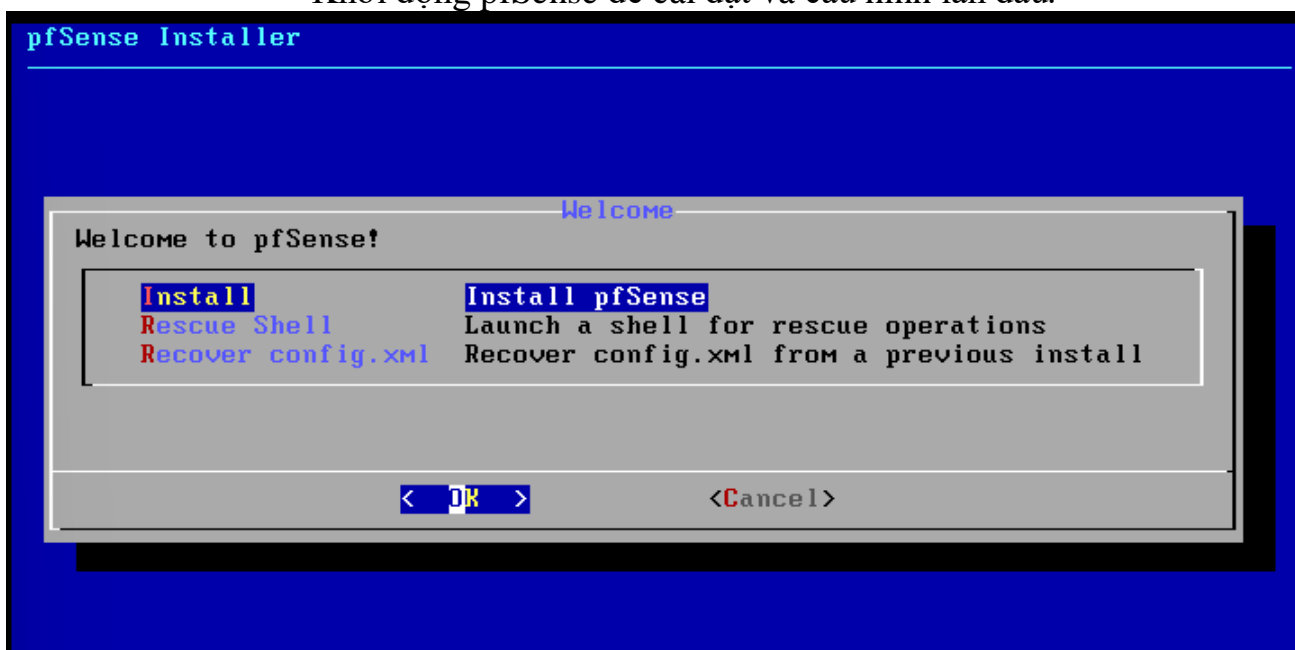
Subnet IP: 10 . 10 . 19 . 0 Subnet mask: 255 . 255 . 255 . 0

Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help

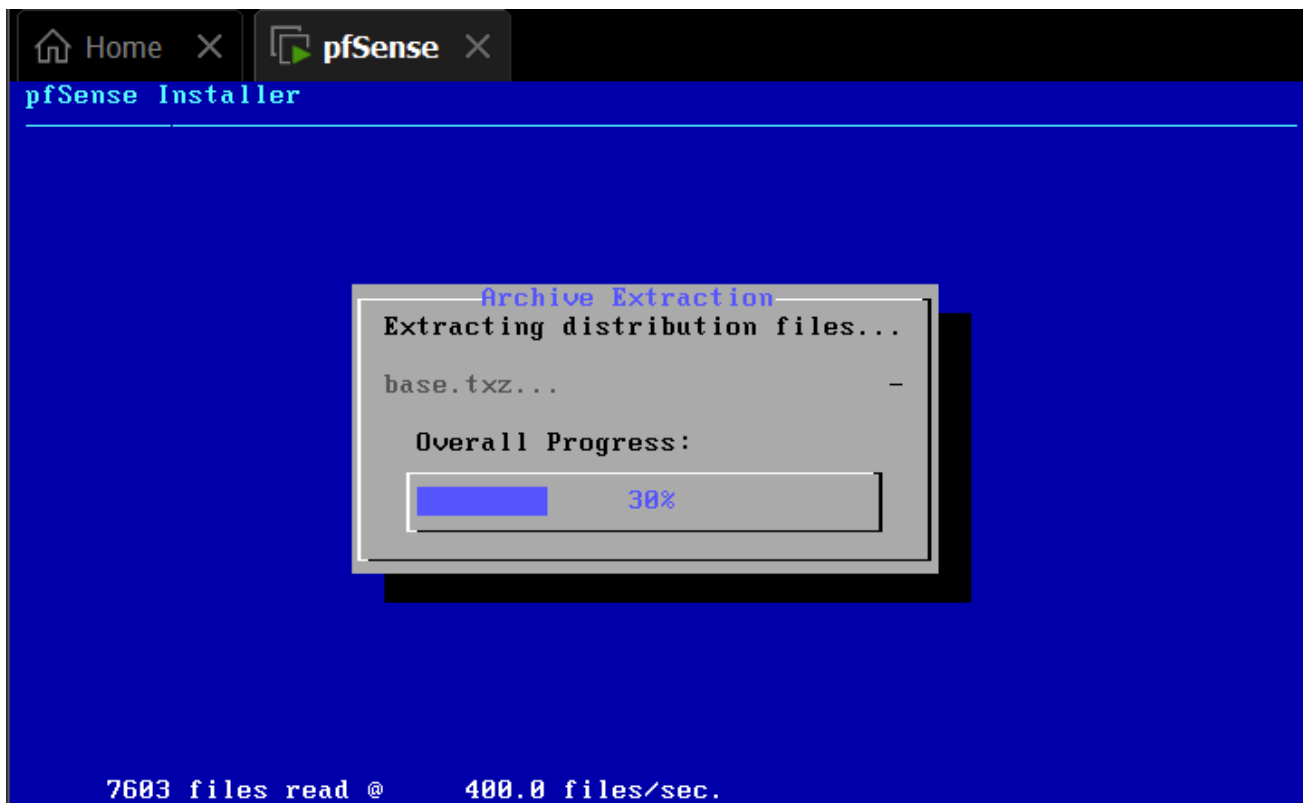
- Tiếp theo, cài đặt pfSense. Thao tác cài đặt trên VMWare tương tự như khi thực hiện bài thực hành 1 đến 4.
- Ở mục Edit virtual machine settings, chọn Add, chọn Network Adapter để thêm một card mạng cho pfSense. Cài đặt pfSense kết nối tới vmnet1 và vmnet2 như hình dưới.



- Khởi động pfSense để cài đặt và cấu hình lần đầu.



- Chọn Install, chọn cấu hình filesystem rồi chờ đợi cài đặt.



- Sau khi cài đặt thành công, khởi động lại pfSense và bắt đầu cấu hình địa chỉ IP tĩnh cho pfSense.
- Bấm 2 để mở tính năng cấu hình IP. Sau đó bấm 1 hoặc 2 để chọn WAN (mạng ngoài) hoặc LAN (mạng riêng).
- Điền địa chỉ IP của từng mạng: với WAN là 10.10.19.1, với LAN là 192.168.100.1
- Điền subnet là 24. Tắt DHCP Server trên pfSense vì đã có DHCP Server ảo của VMWare.

```

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

```

```

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

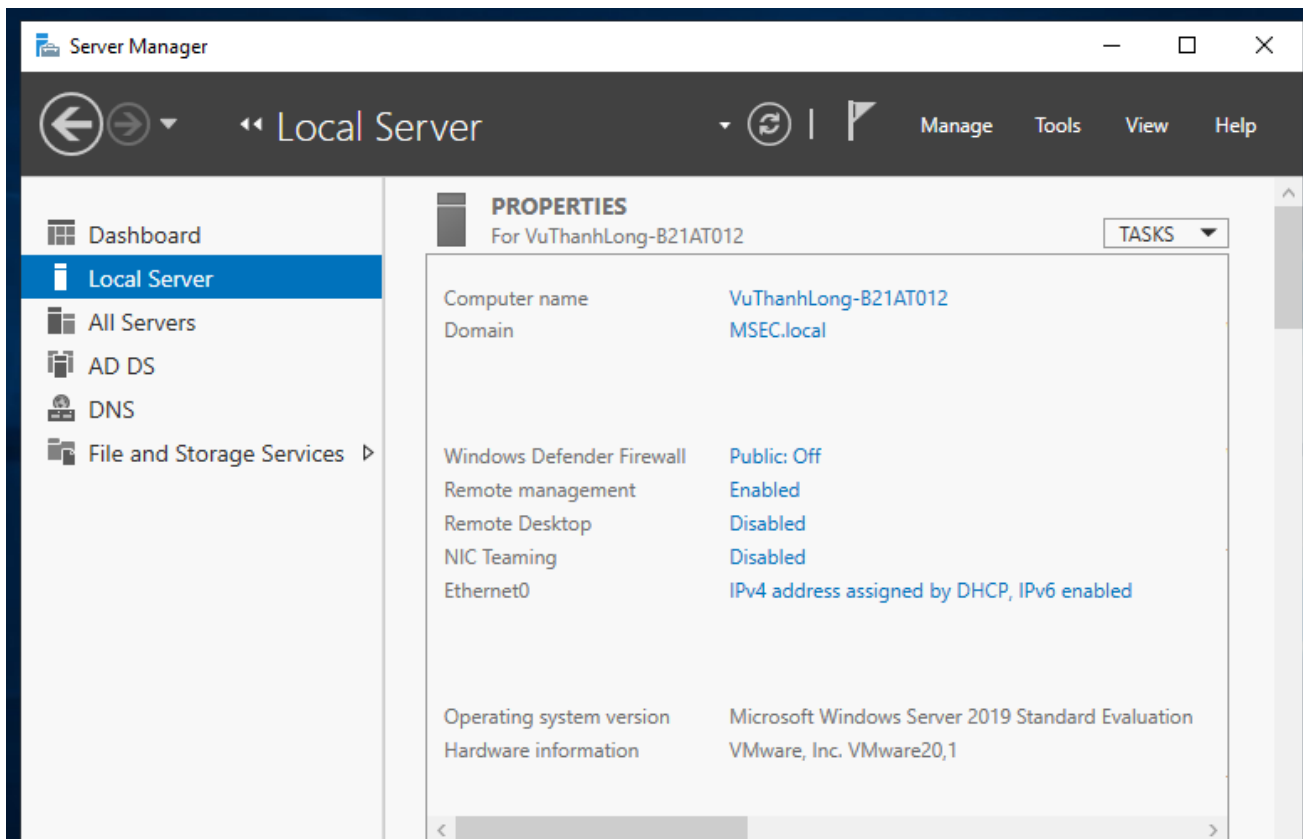
The IPv4 WAN address has been set to 10.10.19.1/24

Press <ENTER> to continue.

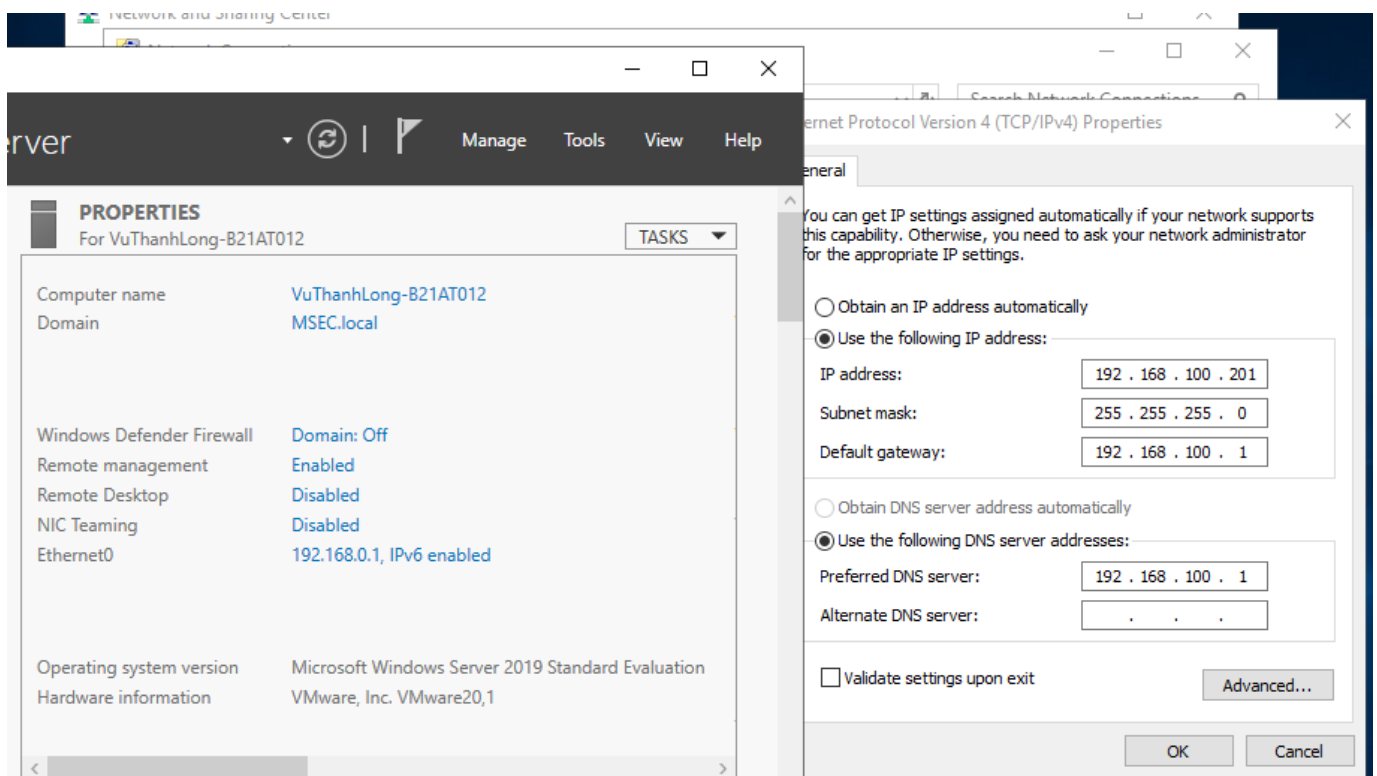
```

Sau đó, cấu hình lại network adapter trên cái máy ảo là vmnet1 và vmnet2 tương ứng với yêu cầu đề bài.

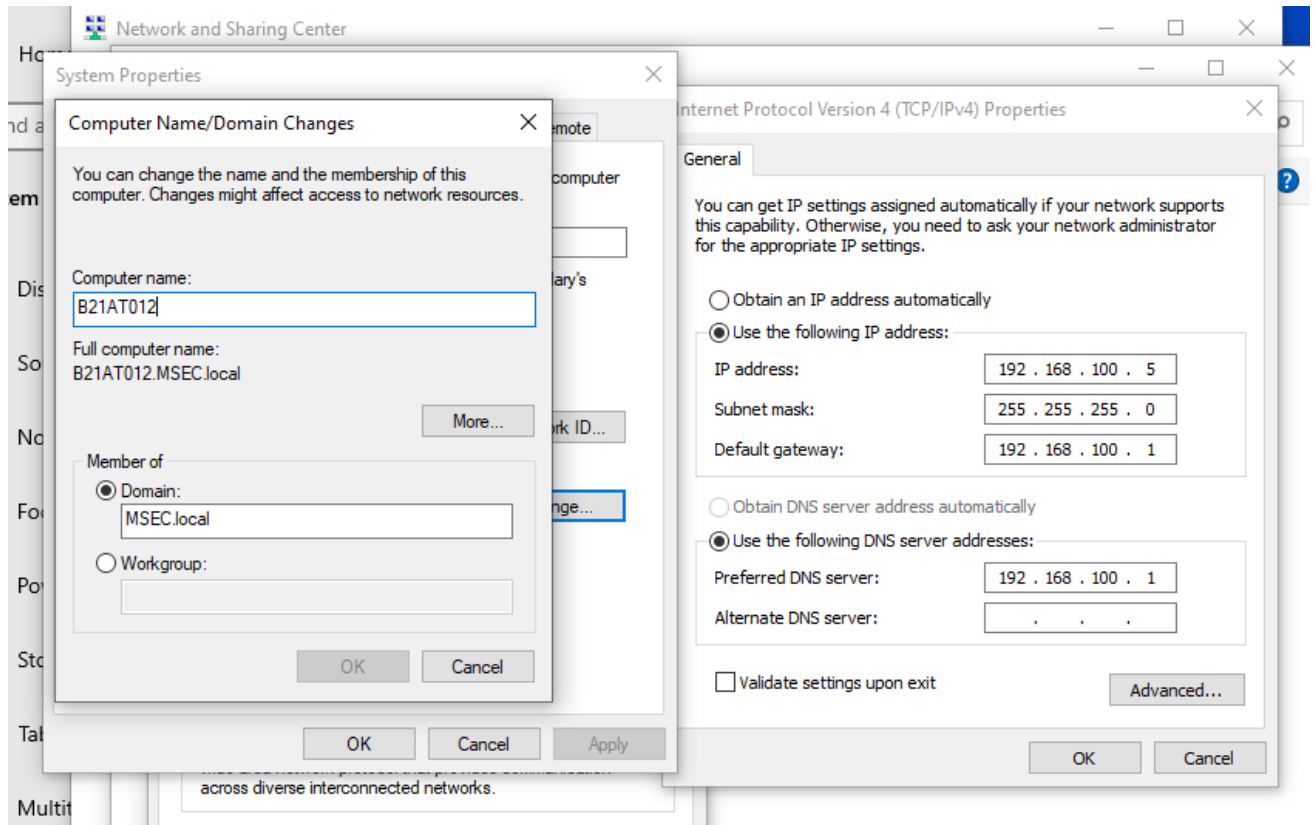
- Trên máy chủ Windows Server Internal, tạo Domain là MSEC.local.



- Cấu hình địa chỉ IP tĩnh, subnet mask, gateway và DNS của Windows Server Internal như hình dưới (bằng cách vào Control Panel, Network Connection, Change Adapter Options).



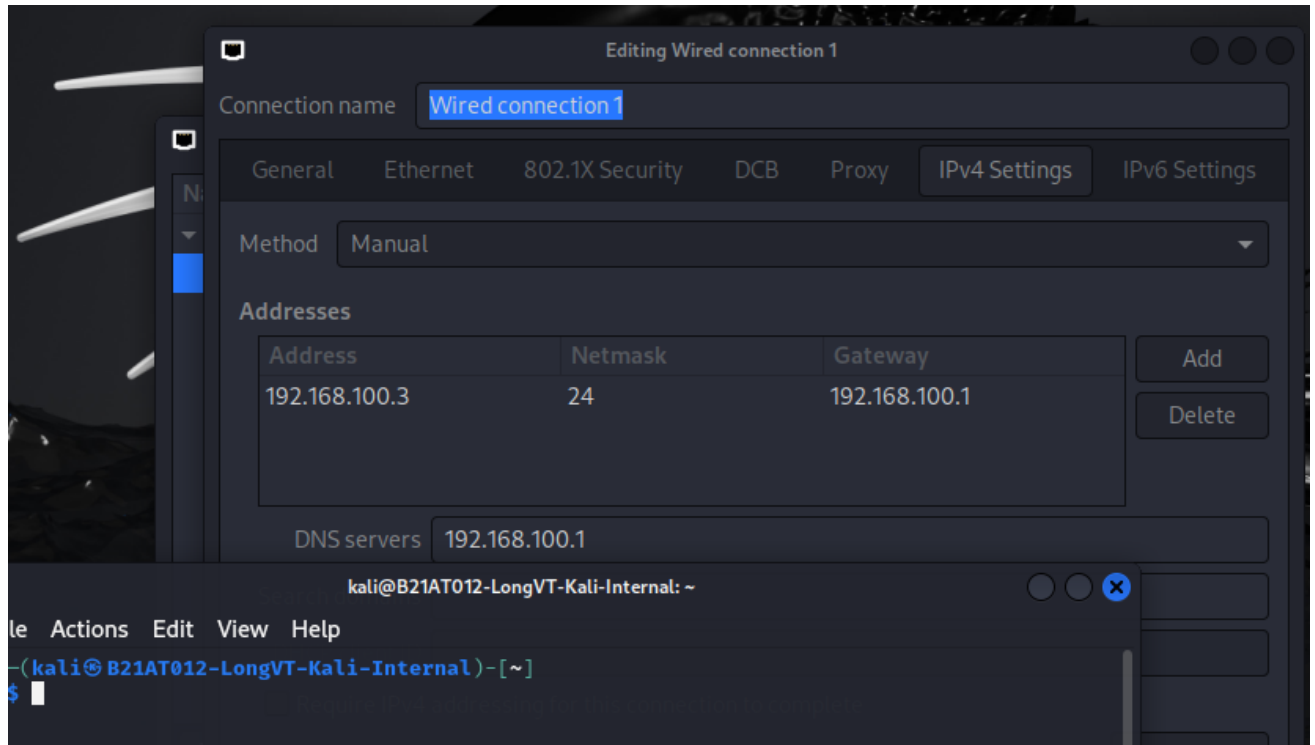
- Trên máy trạm Windows 10, cấu hình nó gia nhập MSEC.local (thao tác như bài 4) và cài đặt IP tĩnh như hình dưới.



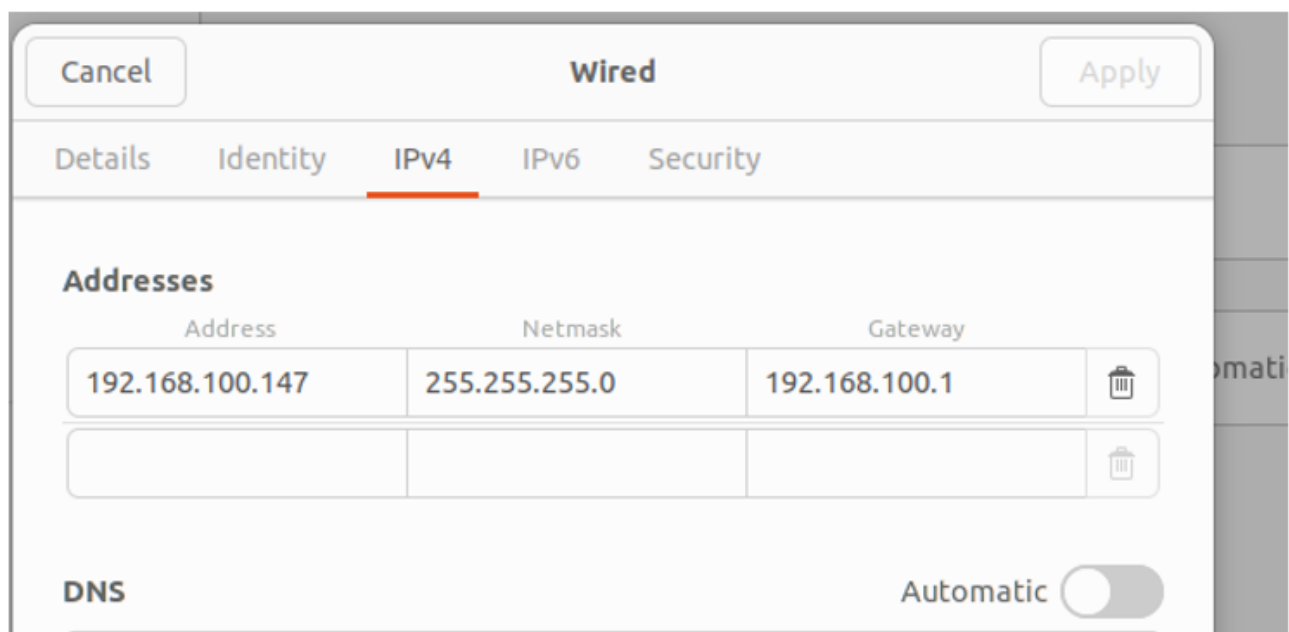
- Trên máy Ubuntu và Kali internal, chạy lệnh **sudo apt install realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin oddjob oddjob-mkhomedir packagekit** để cài đặt các package cần thiết cho việc gia nhập domain.
- Sau đó, chạy **realm discover MSEC.local** và **realm join MSEC.local** để gia nhập domain.

```
(root@ B21AT012-LongVT-Kali-Internal)-[/home/kali]
# realm join MSEC.local
Password for Administrator:
Home
(root@ B21AT012-LongVT-Kali-Internal)-[/home/kali]
#
```

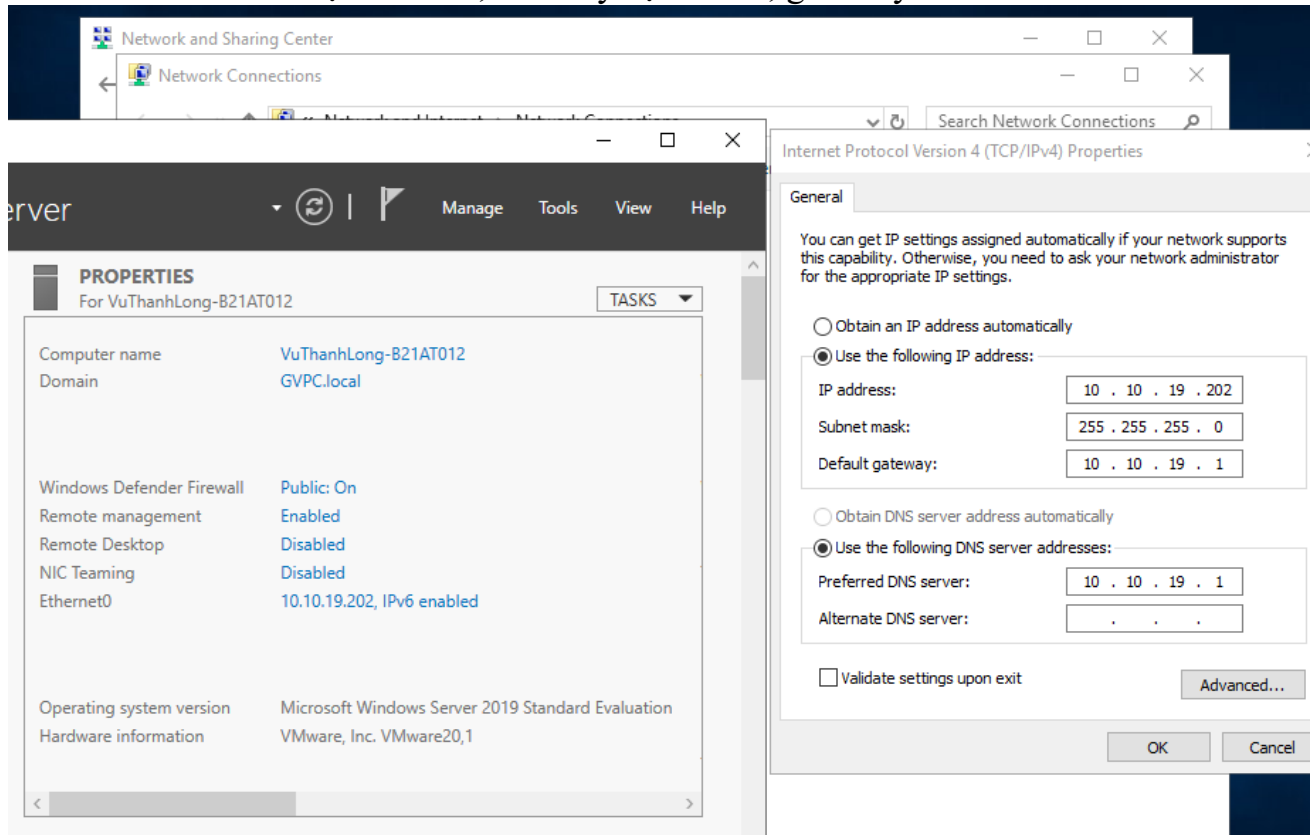
- Cấu hình IP tĩnh cho Kali internal bằng cách chuột phải vào biểu tượng mạng ở góc trên bên phải màn hình, rồi chọn Edit Connection:

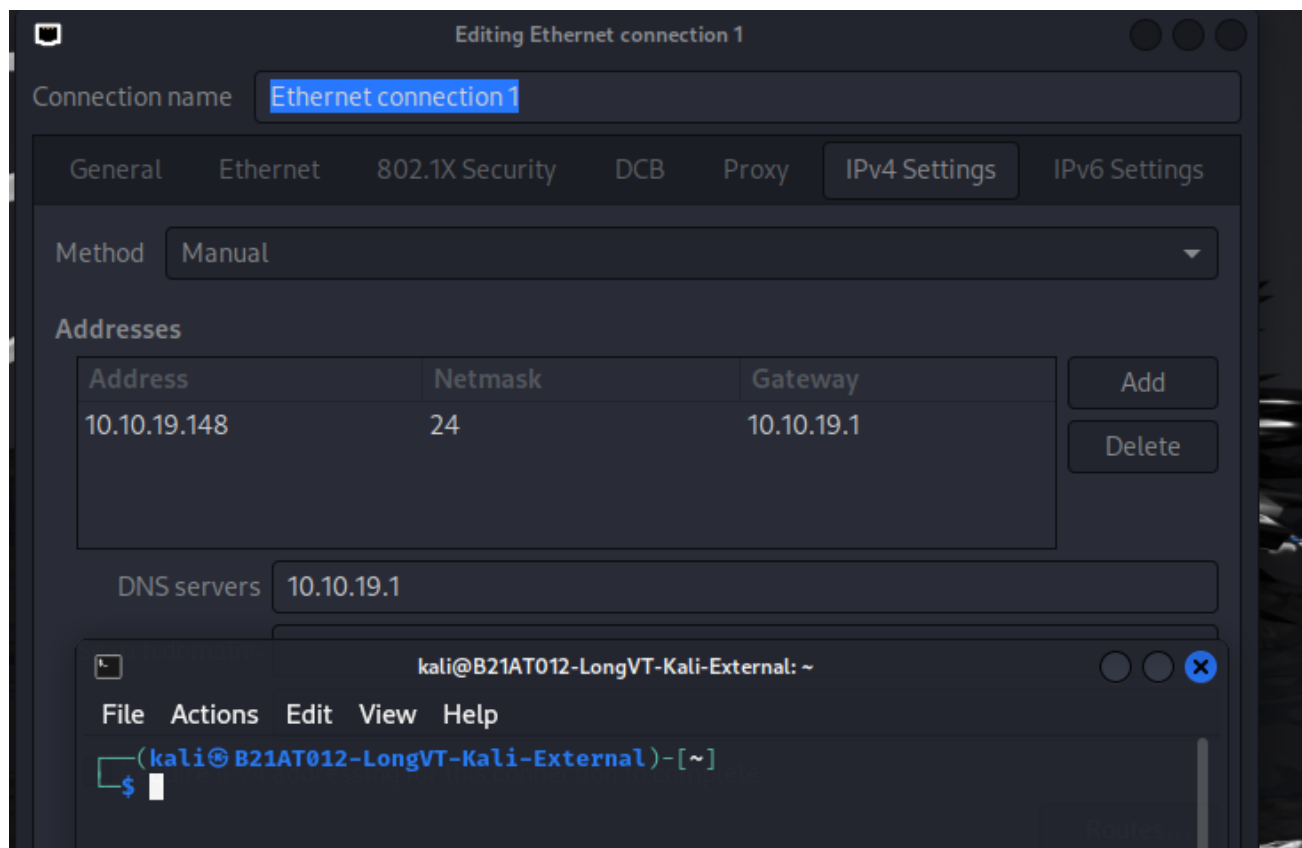


- Cấu hình địa chỉ IP tĩnh cho Ubuntu Internal bằng cách vào Settings, Network, bấm vào biểu tượng hình bánh răng, chọn IPv4:

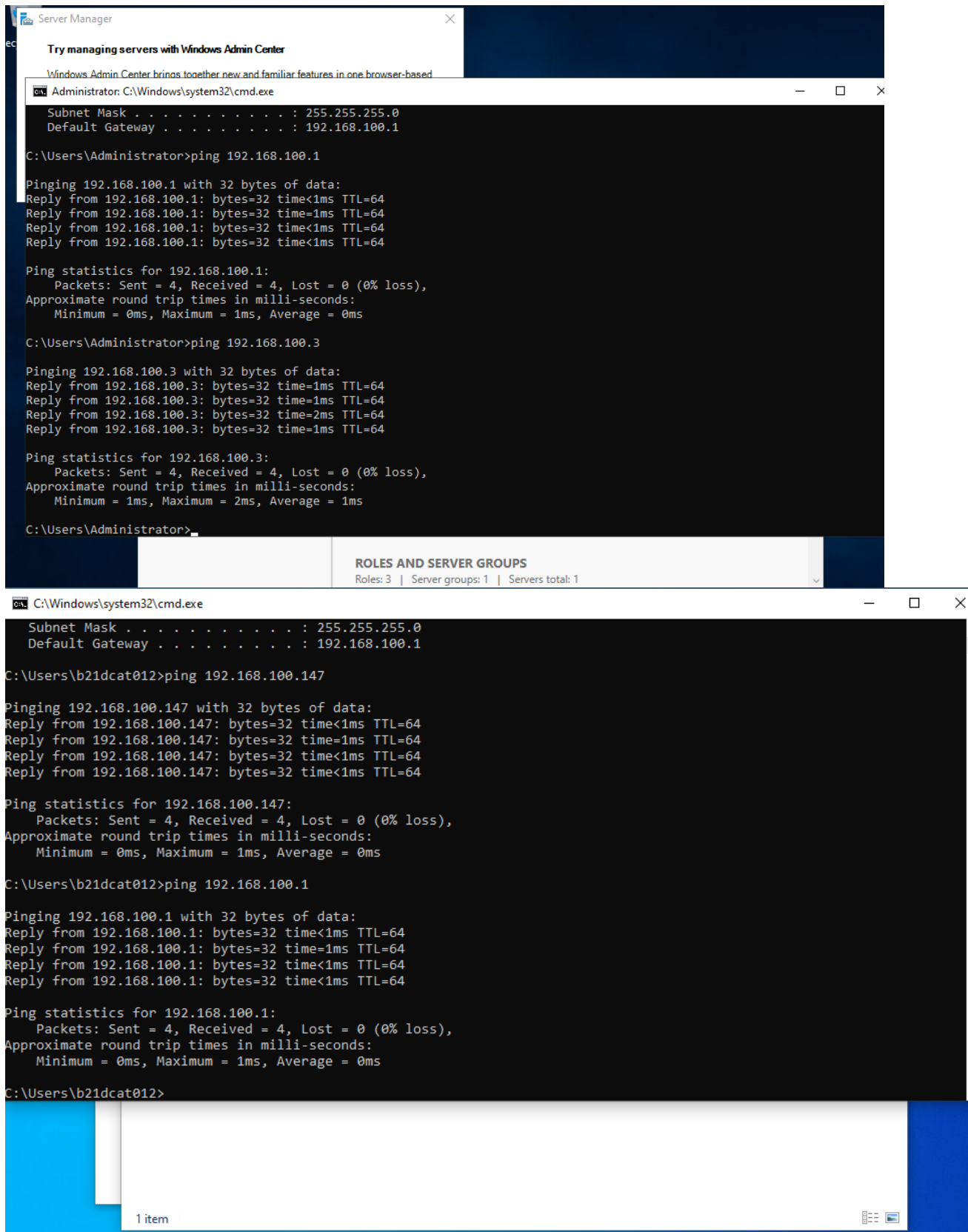


- Trên Windows Server External và Kali External, thao tác tương tự như trên, chỉ thay địa chỉ IP, gateway và DNS.



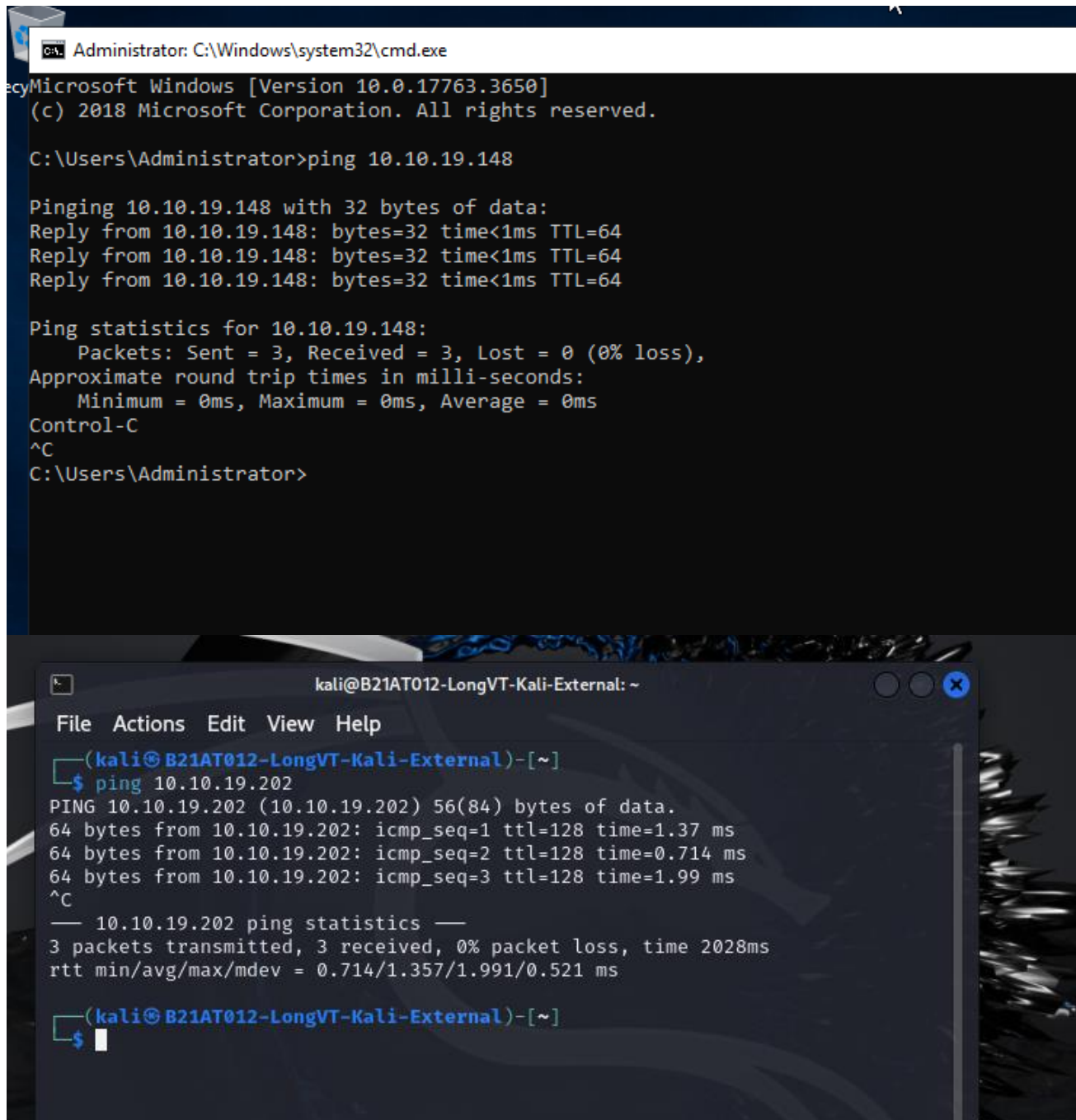


- Kiểm tra bằng cách ping cho các máy tính trên cùng mạng Internal:



```
longvt@b21dcat012: ~  
longvt@b21dcat012:~$ ping 192.168.100.201  
PING 192.168.100.201 (192.168.100.201) 56(84) bytes of data.  
64 bytes from 192.168.100.201: icmp_seq=1 ttl=128 time=1.32 ms  
64 bytes from 192.168.100.201: icmp_seq=2 ttl=128 time=0.555 ms  
64 bytes from 192.168.100.201: icmp_seq=3 ttl=128 time=1.62 ms  
64 bytes from 192.168.100.201: icmp_seq=4 ttl=128 time=0.750 ms  
64 bytes from 192.168.100.201: icmp_seq=5 ttl=128 time=1.21 ms  
^C  
--- 192.168.100.201 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4023ms  
rtt min/avg/max/mdev = 0.555/1.090/1.616/0.385 ms  
longvt@b21dcat012:~$ ping 192.168.100.3  
PING 192.168.100.3 (192.168.100.3) 56(84) bytes of data.  
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.860 ms  
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.960 ms  
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.852 ms  
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=1.73 ms  
64 bytes from 192.168.100.3: icmp_seq=5 ttl=64 time=0.637 ms  
^C  
--- 192.168.100.3 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4020ms  
rtt min/avg/max/mdev = 0.637/1.006/1.725/0.374 ms  
longvt@b21dcat012:~$
```

- Kiểm tra bằng cách ping cho các máy tính trên cùng mạng External (hình dưới):

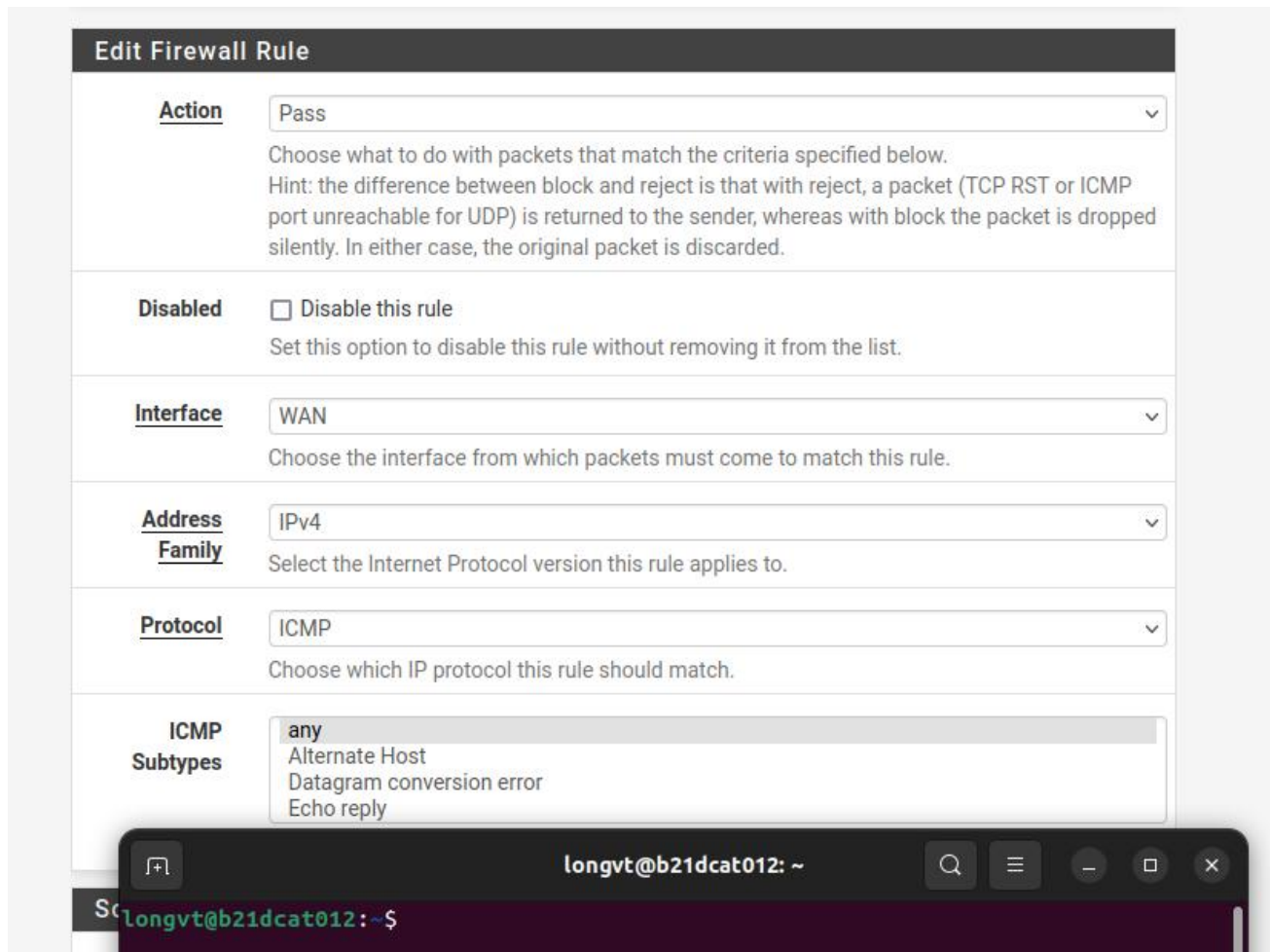


- Cuối cùng là cấu hình máy Linux Sniffer. Ở giao diện cấu hình máy ảo VMWare chọn 2 Network Adapter là vmnet1 và vmnet 2 cho Linux Sniffer.
- Khi khởi động Sniffer, chạy `ifconfig` thấy có 2 địa chỉ IP của mạng Internal và External.


```
kali@B21AT012-LongVT-Kali-Sniffer: ~  
File Actions Edit View Help  
  
(kali@B21AT012-LongVT-Kali-Sniffer)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:0d:ce:67 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.100.129/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0  
        valid_lft 1730sec preferred_lft 1730sec  
    inet6 fe80::216e:9b73:20ae:aa45/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:0d:ce:71 brd ff:ff:ff:ff:ff:ff  
    inet 10.10.19.131/24 brd 10.10.19.255 scope global dynamic noprefixroute eth1  
        valid_lft 1730sec preferred_lft 1730sec  
    inet6 fe80::8520:e2c1:46b3:3094/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

2. Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP:

- Trên máy Ubuntu Internal dùng Firefox vào <http://192.168.100.1> để cấu hình pfSense. Điền tên tài khoản và mật khẩu mặc định.
- Giao diện web của pfSense hiển thị. Chọn Firewall, chọn Rules, trên tab WAN bấm Add rule để thêm một luật mới.
- Mục Action chọn Pass để cho phép một hành động xảy ra. Mục Interface chọn WAN vì gói tin ping đến từ mạng ngoài. Mục Protocol chọn ICMP.
- Source chọn any, còn Destination chọn This firewall (self).
- Tóm lại, luật này miêu tả gói tin ICMP đi từ WAN đến pfSense sẽ được cho phép.



- Sau khi thêm luật mới, bấm Interfaces -> WAN và bỏ chọn Block private networks để cho phép các thiết bị ở mạng ngoài ping được vào địa chỉ IP mạng trong.

The screenshot shows the pfSense configuration interface. The top section is titled "Static IPv4 Configuration". It includes a field for "IPv4 Address" set to "10.10.19.1" with a subnet mask of "24". Below this is the "IPv4 Upstream gateway" section, currently set to "None", with a green button labeled "+ Add a new gateway". A descriptive text block explains that for Internet connections, an existing gateway should be selected or added, while for local area networks, it should be "none". It also notes that selecting an upstream gateway treats the interface as a WAN type interface and provides a link to manage gateways.

The bottom section is titled "Reserved Networks". It contains two options: "Block private networks and loopback addresses" (unchecked) and "Block bogon networks" (checked). Descriptive text for each option explains what they block and when they should be used. A note mentions that the update frequency of bogon lists can be adjusted in the settings.

Overlaid on the bottom right is a terminal window titled "longvt@b21dcat012: ~". It shows the command prompt "longvt@b21dcat012:~\$" and a cursor, indicating a shell session.

- Thực hiện ping thử từ Kali External đến địa chỉ IP ngoài của pfSense:

```
kali@B21AT012-LongVT-Kali-External: ~
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-External)-[~]
$ ping 10.10.19.1
PING 10.10.19.1 (10.10.19.1) 56(84) bytes of data.
64 bytes from 10.10.19.1: icmp_seq=1 ttl=64 time=0.569 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=1.39 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=1.07 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=1.27 ms
^C
— 10.10.19.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3023ms
rtt min/avg/max/mdev = 0.569/1.075/1.385/0.312 ms

(kali@B21AT012-LongVT-Kali-External)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:60:2c:1f brd ff:ff:ff:ff:ff:ff
    inet 10.10.19.148/24 brd 10.10.19.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
```

- **Trả lời câu hỏi:** Mặc định, pfSense không mở cổng nào ở giao diện WAN.

```
kali@B21AT012-LongVT-Kali-External: ~
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-External)-[~]
$ nmap 10.10.19.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 05:46 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds

(kali@B21AT012-LongVT-Kali-External)-[~]
$
```

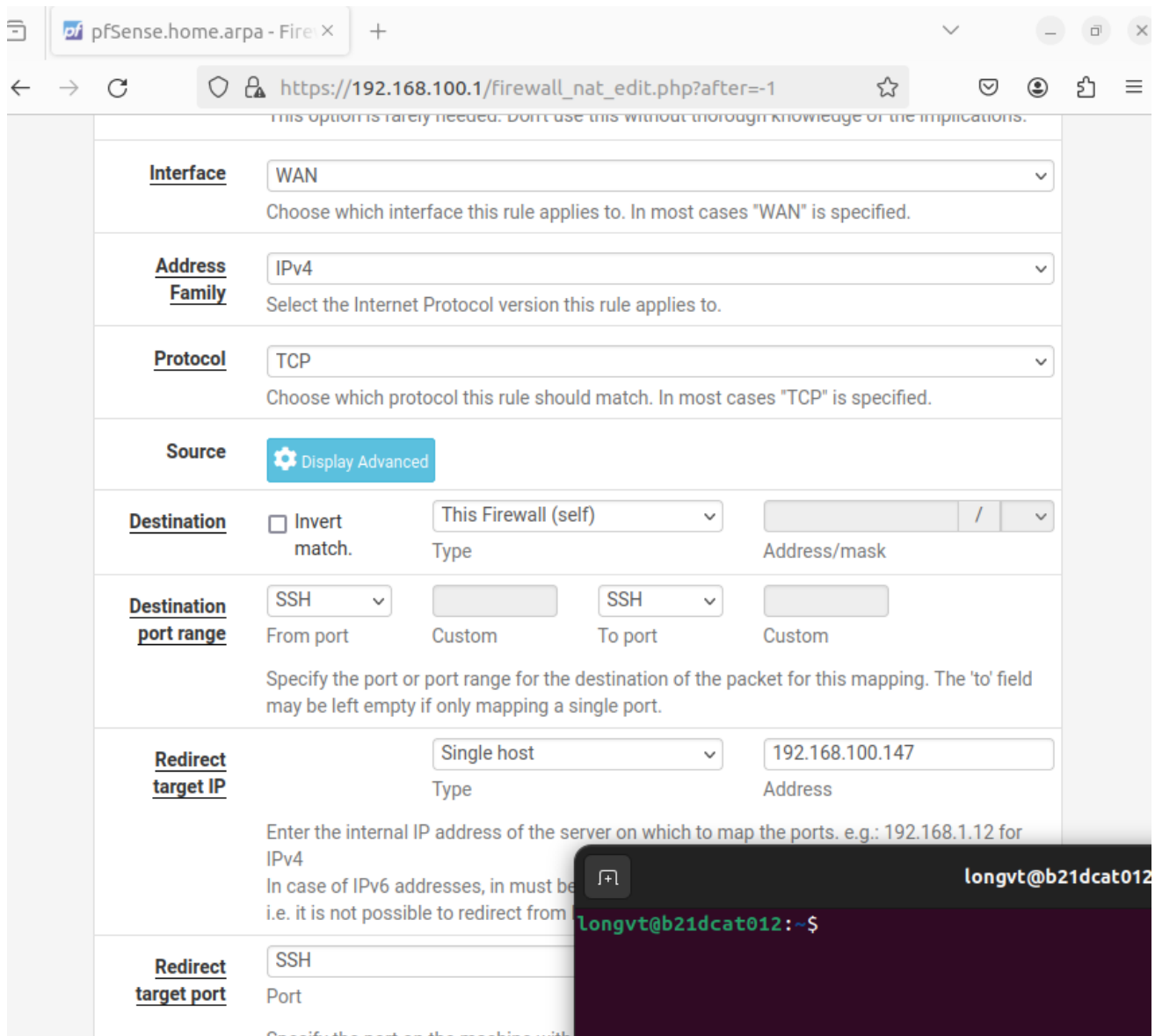
- **Trả lời câu hỏi:** Mặc định, ở giao diện LAN, pfSense mở cổng 53 cho dịch vụ DNS Server và cổng 80 để cho phép máy trạm truy cập giao diện web qua http.

```
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ nmap 192.168.100.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 05:45 EDT
Nmap scan report for pfSense.home.arpa (192.168.100.1)
Host is up (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

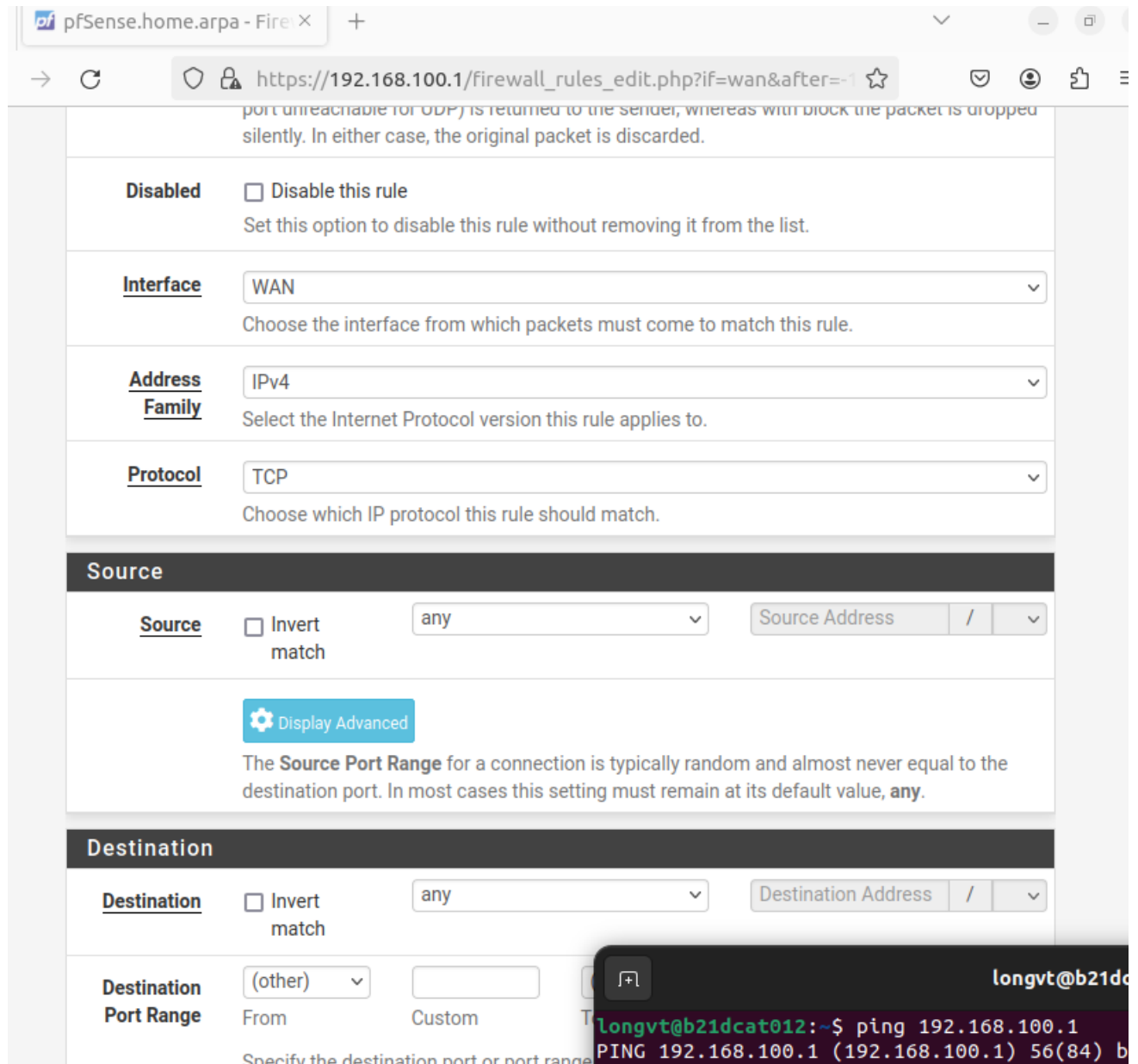
Nmap done: 1 IP address (1 host up) scanned in 4.45 seconds

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$
```

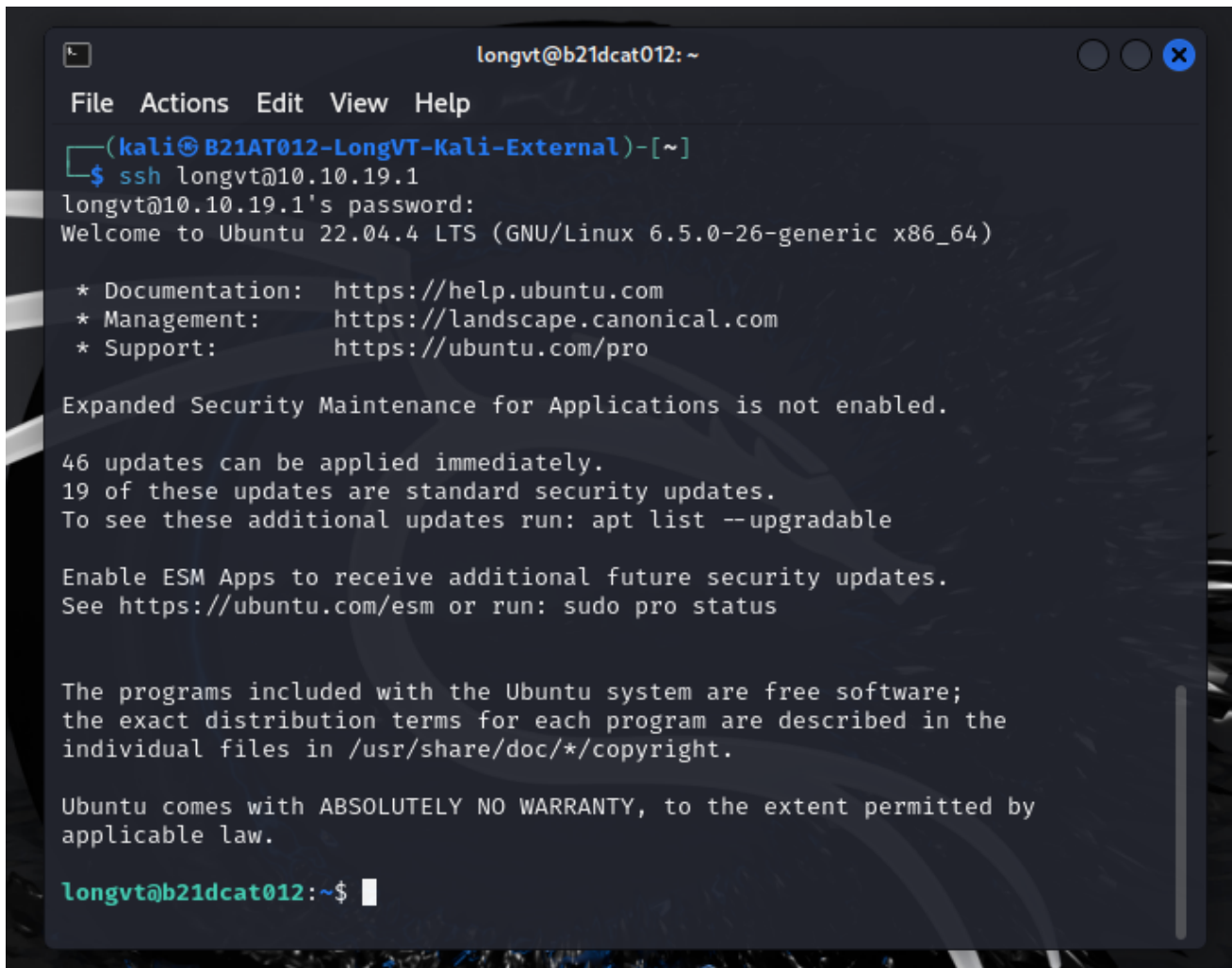
3. Cài đặt cấu hình pfSense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal:
 - Trên giao diện chính của pfSense, chọn Firewall chọn NAT, chọn Port Forward.
 - Thêm một luật mới như sau:
 - Mục Interface chọn WAN, Protocol chọn TCP (hoặc any).
 - Destination chọn This firewall vì lưu lượng phải đến pfSense rồi mới được chuyển hướng.
 - Destination port chọn 22, là cổng mặc định của SSH.
 - Redirect Target IP chọn Single host rồi điền địa chỉ IP của máy mà mình muốn chuyển hướng lưu lượng đến. Chọn 192.168.100.147 là địa chỉ IP của Ubuntu Internal.
 - Redirect target port chọn SSH.



- Ngoài ra, ở mục Firewall Rules cần tạo thêm luật mới cho phép các gói tin TCP từ mạng External đi vào được mạng Internal.



– Thực hiện SSH trên Kali Linux External:



```
longvt@b21dcat012: ~  
File Actions Edit View Help  
(kali@B21AT012-LongVT-Kali-External)-[~]  
$ ssh longvt@10.10.19.1  
longvt@10.10.19.1's password:  
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-26-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
Expanded Security Maintenance for Applications is not enabled.  
  
46 updates can be applied immediately.  
19 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
longvt@b21dcat012:~$
```

- Chạy lệnh ifconfig trên SSH, thấy địa chỉ IP là 192.168.100.147


```
longvt@b21dcat012: ~  
File Actions Edit View Help  
applicable law.  
  
longvt@b21dcat012:~$ whoami  
longvt  
longvt@b21dcat012:~$ hostname  
b21dcat012.MSEC.local  
longvt@b21dcat012:~$ ifconfig  
Command 'ifconfig' not found, but can be installed with:  
sudo apt install net-tools  
longvt@b21dcat012:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP  
group default qlen 1000  
    link/ether 00:0c:29:db:11:c7 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.100.130/24 brd 192.168.100.255 scope global dynamic noprefix  
route ens33  
        valid_lft 895sec preferred_lft 895sec  
    inet 192.168.100.147/24 brd 192.168.100.255 scope global secondary nopref  
ixroute ens33  
        valid_lft forever preferred_lft forever
```

- Dùng nmap trên Kali internal quét cổng mở trên pfSense, thấy vẫn chỉ mở 2 cổng là 53 và 80.


```
kali@B21AT012-LongVT-Kali-Intern
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ nmap 192.168.100.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 07:04 EDT
Nmap scan report for pfSense.home.arpa (192.168.100.1)
Host is up (0.0051s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$
```

Tài liệu tham khảo:

- VMWare Virtual Network Editor KB:
<https://kb.vmware.com/s/article/1018697>
- pfSense Documentation: <https://docs.netgate.com/pfsense/en/latest/>