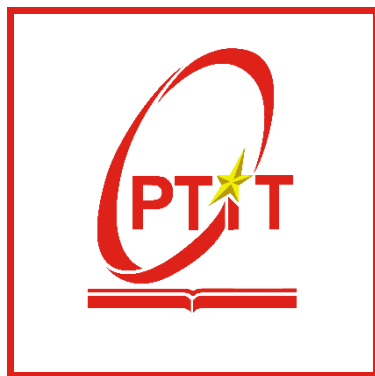


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



THỰC TẬP CƠ SỞ

**Bài 5: Cài đặt, cấu hình mạng doanh nghiệp với
Pfsense firewall**

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

Hà Nội – 3/2024

Môn học Thực tập cơ sở

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

I. Lý thuyết

1. Các chế độ mạng trong VMWare Network

❖ Mạng Bridged

Như tên cho thấy, đây là mạng Cầu nối, có nghĩa là máy ảo của bạn sẽ hoạt động như một máy ảo độc lập được kết nối với bộ chuyển mạch hoặc bộ định tuyến vật lý của bạn. Trong VM này sẽ trực tiếp lấy Địa chỉ IP từ Máy chủ DHCP có trong cơ sở hạ tầng của bạn. Nếu bạn sử dụng mạng cầu nối, máy ảo sẽ là thành viên đầy đủ trong mạng. Nó có quyền truy cập vào các máy khác trên mạng và có thể liên lạc với các máy khác trên mạng như thể nó là một máy tính vật lý trên mạng.

❖ Mạng NAT

Đây là mạng mặc định được sử dụng và chỉ định khi bạn tạo máy ảo. Trong trường hợp NAT, máy ảo của bạn không có địa chỉ IP riêng trên mạng bên ngoài. Thay vào đó, một mạng riêng biệt được thiết lập trên máy chủ. Máy ảo của bạn nhận được một địa chỉ trên mạng đó từ máy chủ DHCP ảo VMware. Thiết bị VMware NAT truyền dữ liệu mạng giữa một hoặc nhiều máy ảo và mạng bên ngoài. Nó xác định các gói dữ liệu đến dành cho từng máy ảo và gửi chúng đến đúng đích.

❖ Mạng Host-only

Điều này được sử dụng khi bạn muốn tạo một mạng hoàn toàn biệt lập để máy ảo của bạn không thể nhìn thấy mạng hoặc Internet khác. Mạng chỉ dành cho máy chủ cung cấp kết nối mạng giữa máy ảo và máy chủ, sử dụng bộ điều hợp Ethernet ảo hiển thị với hệ điều hành máy chủ. Cách tiếp cận này có thể hữu ích nếu bạn cần thiết lập một mạng ảo bị cô lập.

2. Giới thiệu về Pfsense

Để bảo vệ hệ thống mạng thì ta có nhiều giải pháp như sử dụng router cisco, dùng firewall cứng, firewall mềm của microsoft như ISA ...

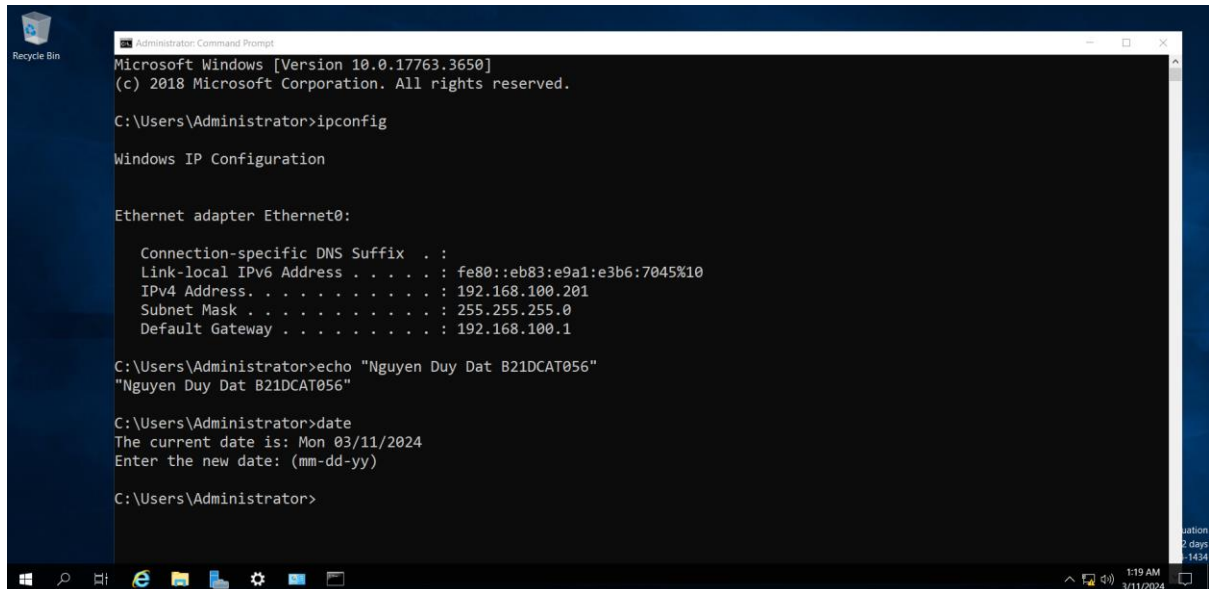
Những thiết bị như trên rất tốn kinh phí vì vậy đối với các doanh nghiệp vừa và nhỏ thì giải pháp firewall mềm mã nguồn mở là một phương án hiệu quả. Pfsense là một ứng dụng có chức năng định tuyến vào tường

lửa mạng và miễn phí dựa trên nền tảng FreeBSD có chức năng định tuyến và tường lửa rất mạnh. Pfsense được cấu hình qua giao diện GUI trên nền web nên có thể quản lý một cách dễ dàng. Nó hỗ trợ lọc theo địa chỉ nguồn, đích, cũng như port nguồn hay port đích đồng thời hỗ trợ định tuyến và có thể hoạt động trong chế độ bridge hay transparent. Nếu sử dụng pfsense là gateway, ta cũng có thể thấy rõ việc hỗ trợ NAT và port forward trên pfsense cũng như thực hiện cân bằng tải hay failover trên các đường mạng.

II. Cài đặt

1. Cấu hình topo mạng

- IP máy Windows Server



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

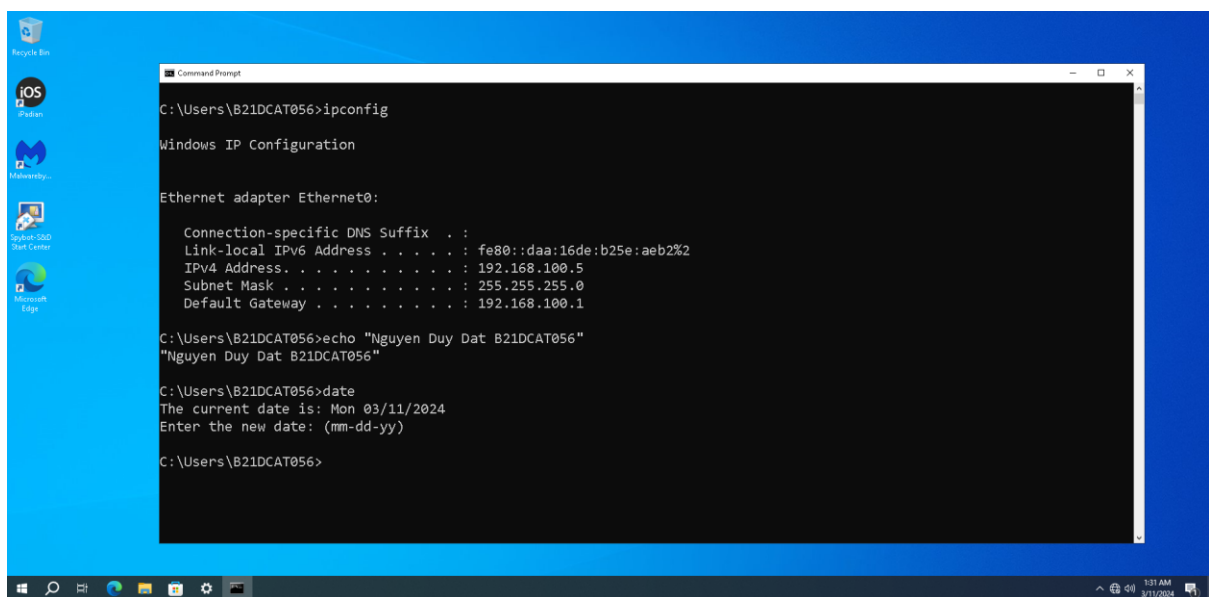
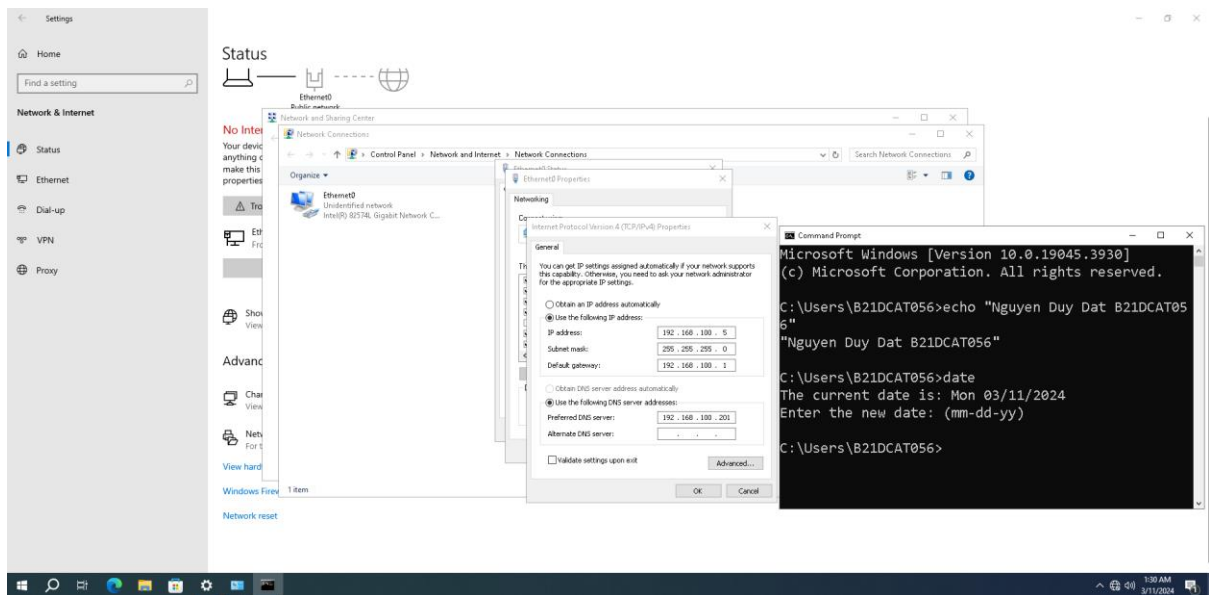
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::eb83:e9a1:e3b6:7045%10
    IPv4 Address. . . . . : 192.168.100.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

C:\Users\Administrator>echo "Nguyen Duy Dat B21DCAT056"
"Nguyen Duy Dat B21DCAT056"

C:\Users\Administrator>date
The current date is: Mon 03/11/2024
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>
```

- IP máy Windows 10



- IP máy Ubuntu

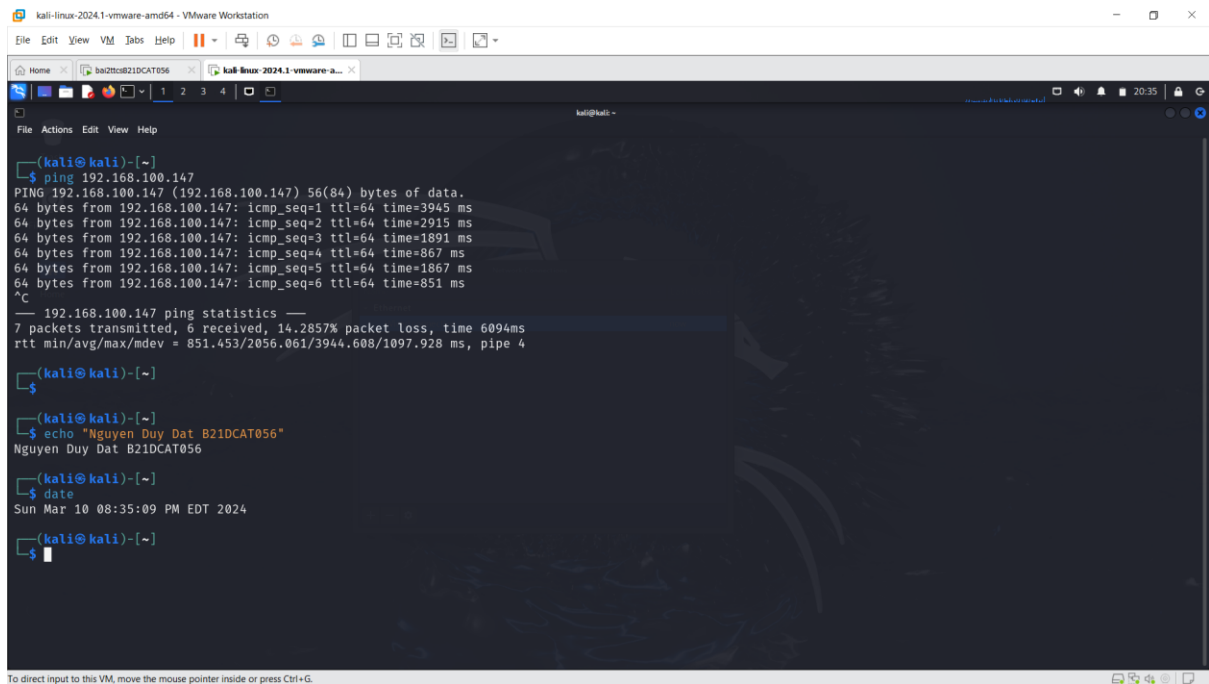
```
Activities Terminal Thg 3 11 07:23
datnd@NguyenDuyDat-B21DCAT056:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        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:29:4f:25:8d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.147/24 brd 192.168.100.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::2cfa:c972:363f:6443/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
datnd@NguyenDuyDat-B21DCAT056:~$
datnd@NguyenDuyDat-B21DCAT056:~$
datnd@NguyenDuyDat-B21DCAT056:~$
datnd@NguyenDuyDat-B21DCAT056:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
datnd@NguyenDuyDat-B21DCAT056:~$ time

real    0m0.000s
user    0m0.000s
sys     0m0.000s
datnd@NguyenDuyDat-B21DCAT056:~$ date
Thứ hai, 11 Tháng 3 năm 2024 07:23:42 +07
datnd@NguyenDuyDat-B21DCAT056:~$
```

- IP máy Kali

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali:~$ ip addr
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:29:34:b7:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.3/24 brd 192.168.100.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::8e26:c043:8d12:dcba/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
kali@kali:~$
kali@kali:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
kali@kali:~$
kali@kali:~$ date
Sun Mar 10 08:32:41 PM EDT 2024
kali@kali:~$
```

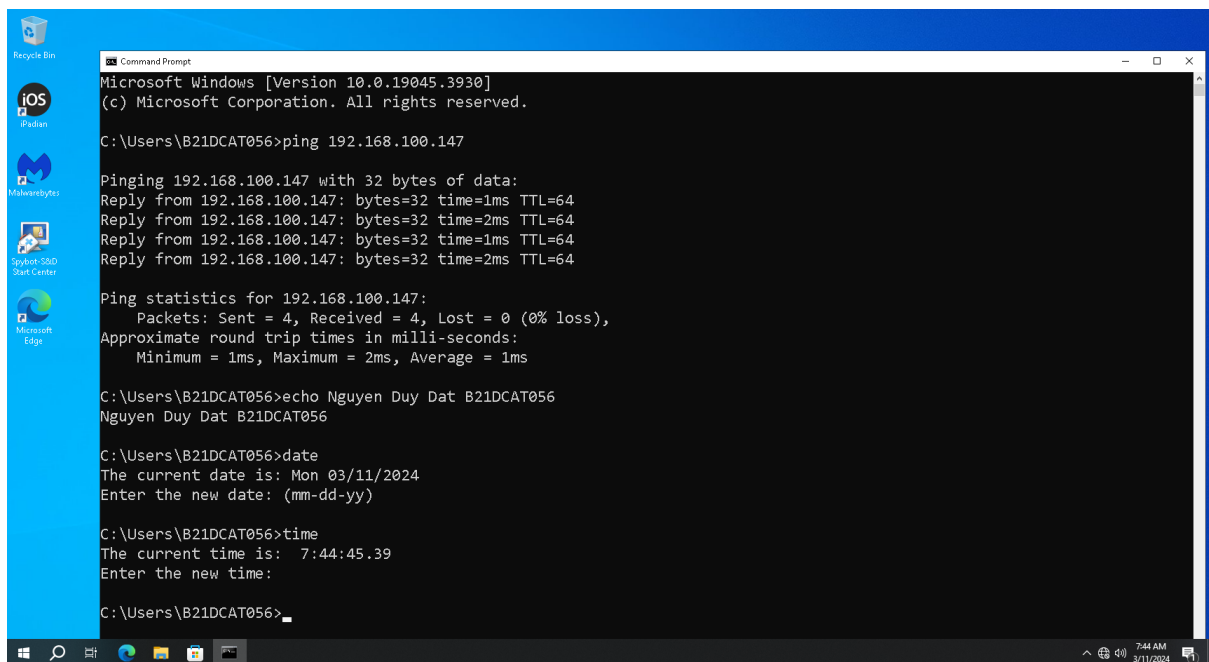
- Ping từ Kali Internal đến Ubuntu Internal



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
(kali@kali)-[~]
$ ping 192.168.100.147
PING 192.168.100.147 (192.168.100.147) 56(84) bytes of data:
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=3945 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=2915 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=1891 ms
64 bytes from 192.168.100.147: icmp_seq=4 ttl=64 time=867 ms
64 bytes from 192.168.100.147: icmp_seq=5 ttl=64 time=1867 ms
64 bytes from 192.168.100.147: icmp_seq=6 ttl=64 time=851 ms
^C
--- 192.168.100.147 ping statistics ---
7 packets transmitted, 6 received, 14.2857% packet loss, time 6094ms
rtt min/avg/max/mdev = 851.453/2056.061/3944.608/1097.928 ms, pipe 4
(kali@kali)-[~]
$
(kali@kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
(kali@kali)-[~]
$ date
Sun Mar 10 08:35:09 PM EDT 2024
(kali@kali)-[~]
$
```

- Ping từ máy Windows 10 đến Ubuntu Internal



The screenshot shows a Windows 10 Command Prompt window with the following commands and output:

```
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\B21DCAT056>ping 192.168.100.147

Pinging 192.168.100.147 with 32 bytes of data:
Reply from 192.168.100.147: bytes=32 time=1ms TTL=64
Reply from 192.168.100.147: bytes=32 time=2ms TTL=64
Reply from 192.168.100.147: bytes=32 time=1ms TTL=64
Reply from 192.168.100.147: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.100.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

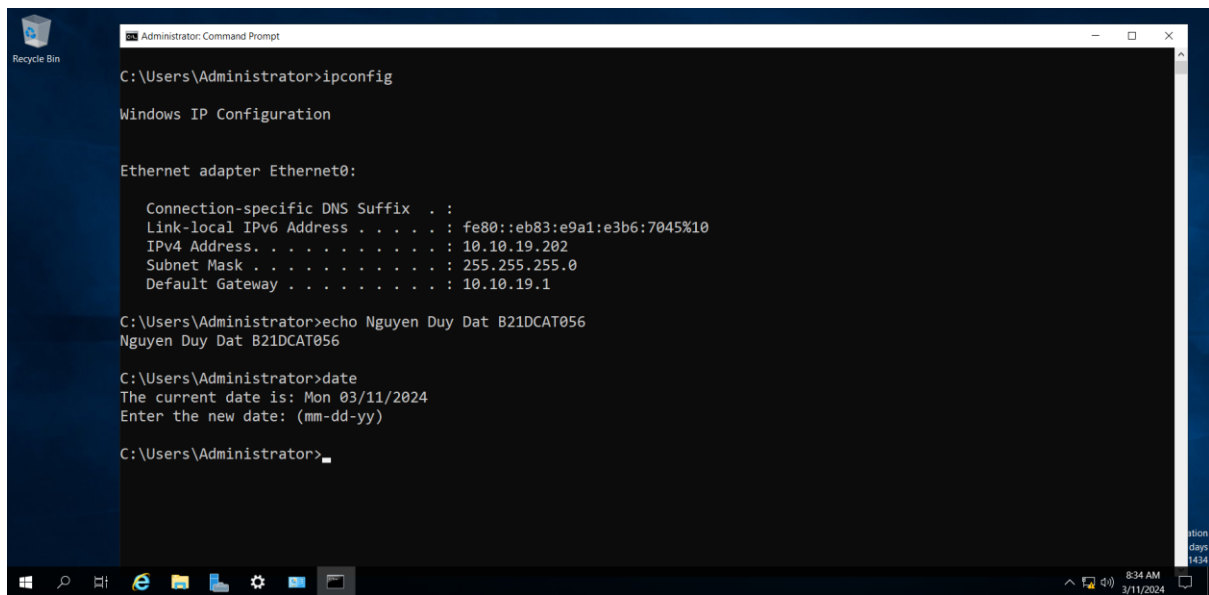
C:\Users\B21DCAT056>echo Nguyen Duy Dat B21DCAT056
Nguyen Duy Dat B21DCAT056

C:\Users\B21DCAT056>date
The current date is: Mon 03/11/2024
Enter the new date: (mm-dd-yy)

C:\Users\B21DCAT056>time
The current time is: 7:44:45.39
Enter the new time:

C:\Users\B21DCAT056>
```

- IP máy Windows Server External



```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

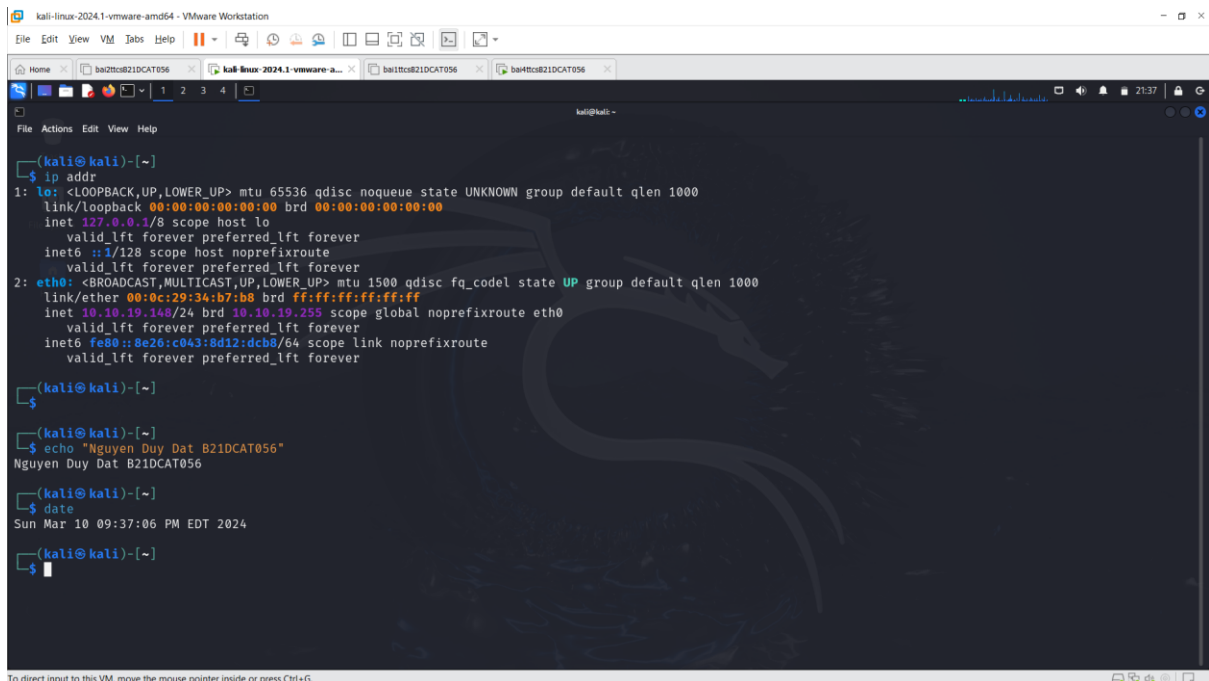
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::eb83:e9a1:e3b6:7045%10
    IPv4 Address. . . . . : 10.10.19.202
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.19.1

C:\Users\Administrator>echo Nguyen Duy Dat B21DCAT056
Nguyen Duy Dat B21DCAT056

C:\Users\Administrator>date
The current date is: Mon 03/11/2024
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>
```

- IP máy Kali External



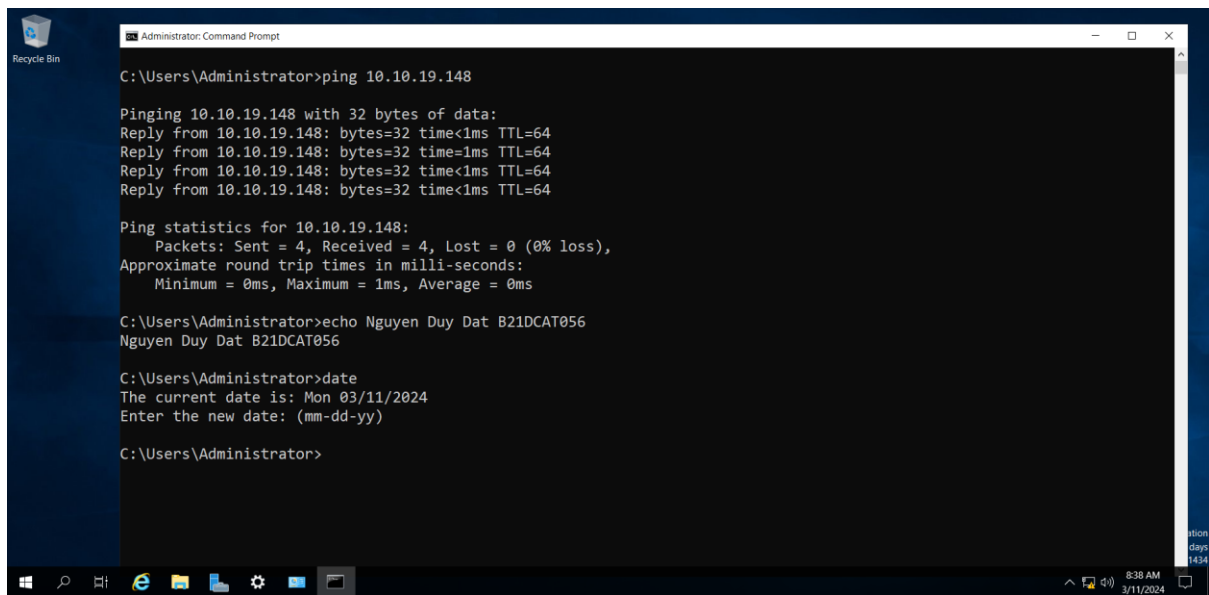
```
(kali@kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        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:29:34:b7:b8 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
    inet6 fe80::8e26:c043:8d12:dc88/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
└─$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@kali)-[~]
└─$ date
Sun Mar 10 09:37:06 PM EDT 2024

(kali@kali)-[~]
└─$
```

- Ping từ máy Windows Server External đến Kali External



```
C:\Users\Administrator>ping 10.10.19.148

Pinging 10.10.19.148 with 32 bytes of data:
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64

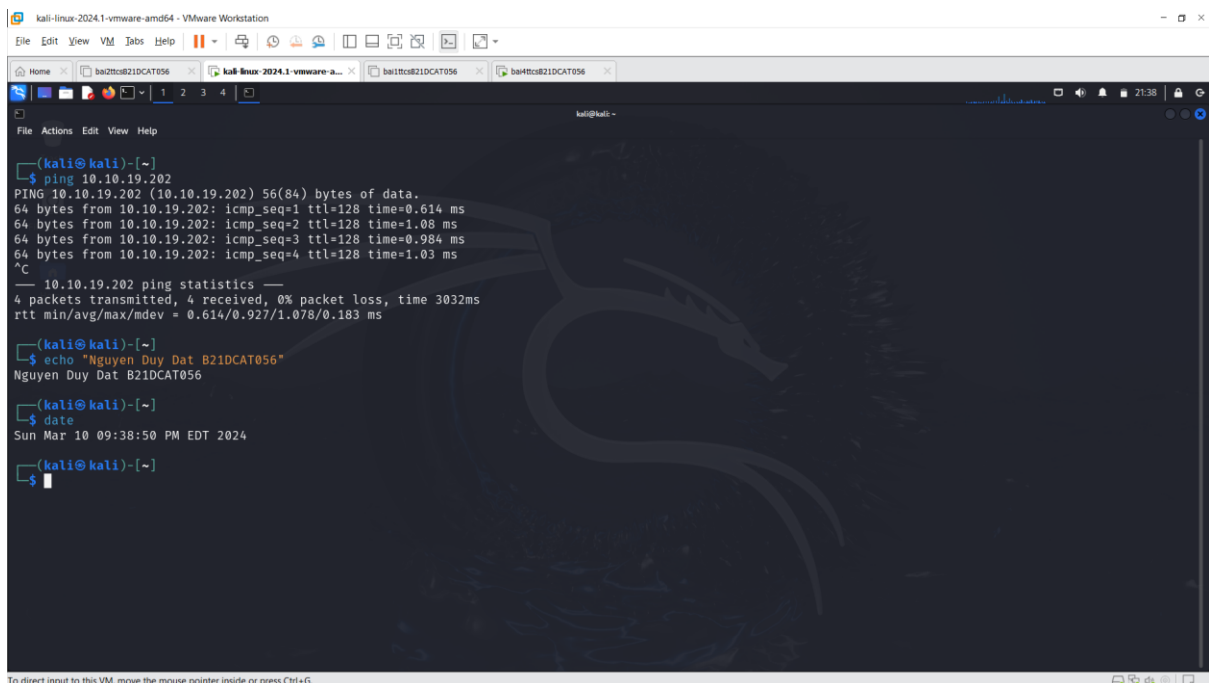
Ping statistics for 10.10.19.148:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>echo Nguyen Duy Dat B21DCAT056
Nguyen Duy Dat B21DCAT056

C:\Users\Administrator>date
The current date is: Mon 03/11/2024
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>
```

- Ping từ máy Kali External đến Windows Server External



```
kali@kali:~$ ping 10.10.19.202
PING 10.10.19.202 (10.10.19.202) 56(84) bytes of data:
64 bytes from 10.10.19.202: icmp_seq=1 ttl=128 time=0.614 ms
64 bytes from 10.10.19.202: icmp_seq=2 ttl=128 time=1.08 ms
64 bytes from 10.10.19.202: icmp_seq=3 ttl=128 time=0.984 ms
64 bytes from 10.10.19.202: icmp_seq=4 ttl=128 time=1.03 ms
^C
--- 10.10.19.202 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.614/0.927/1.078/0.183 ms

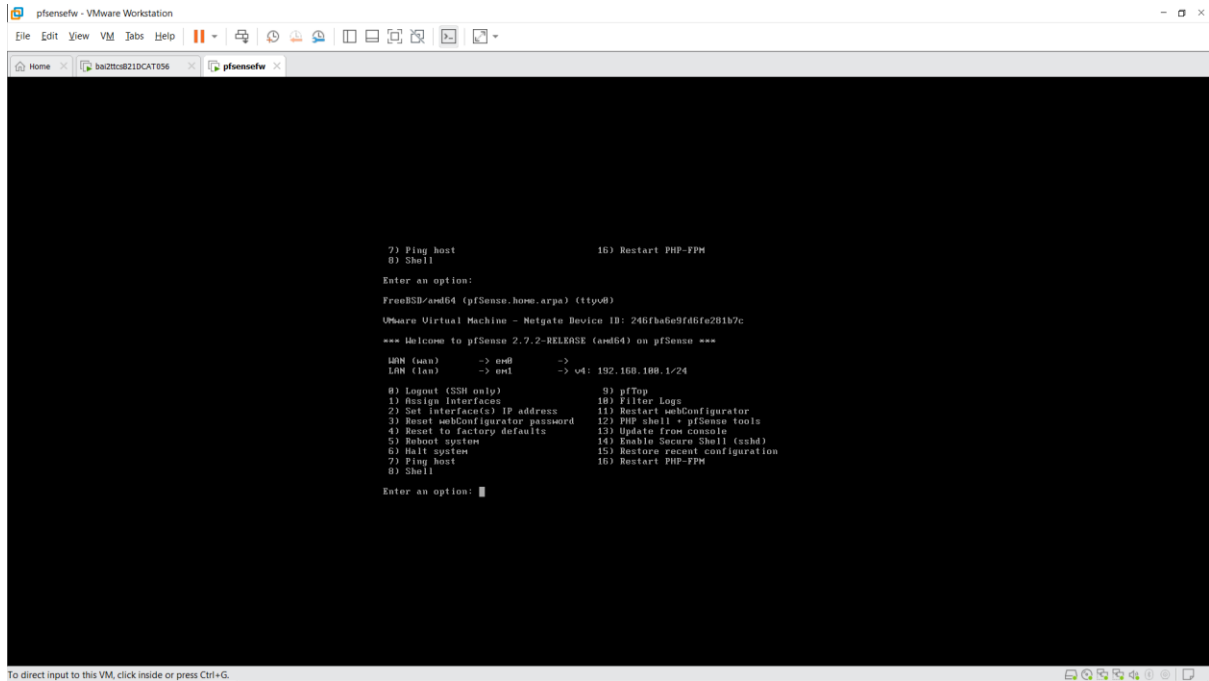
kali@kali:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

kali@kali:~$ date
Sun Mar 10 09:38:50 PM EDT 2024

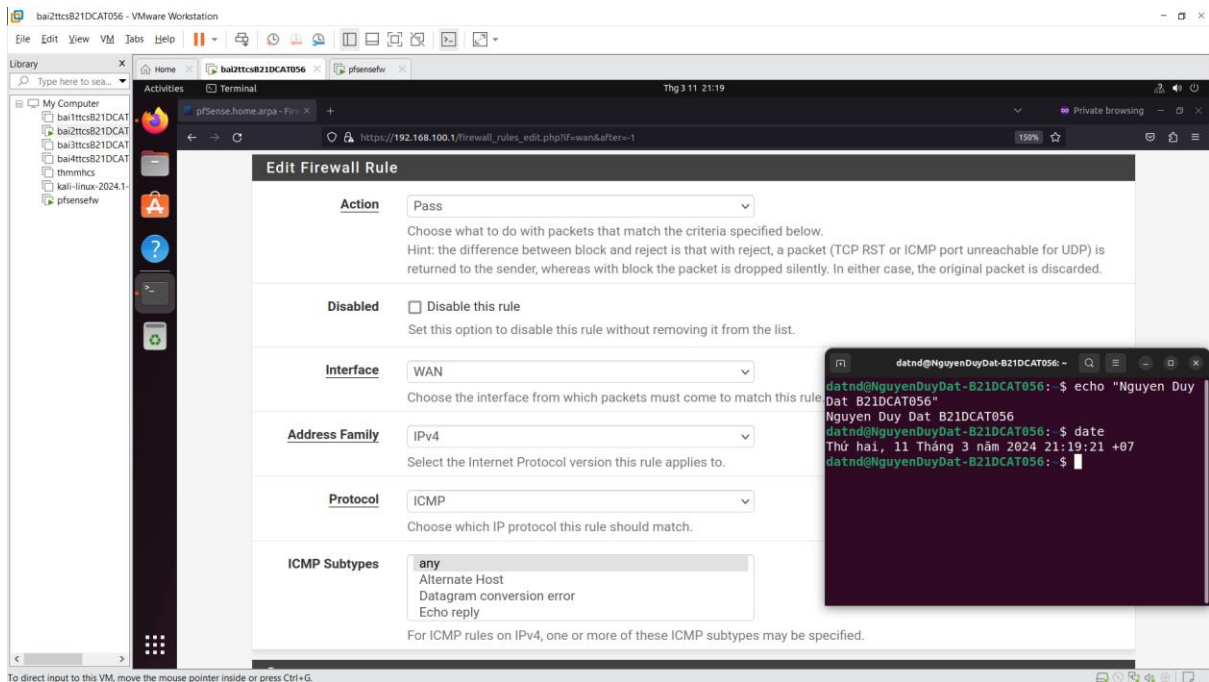
kali@kali:~$
```


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

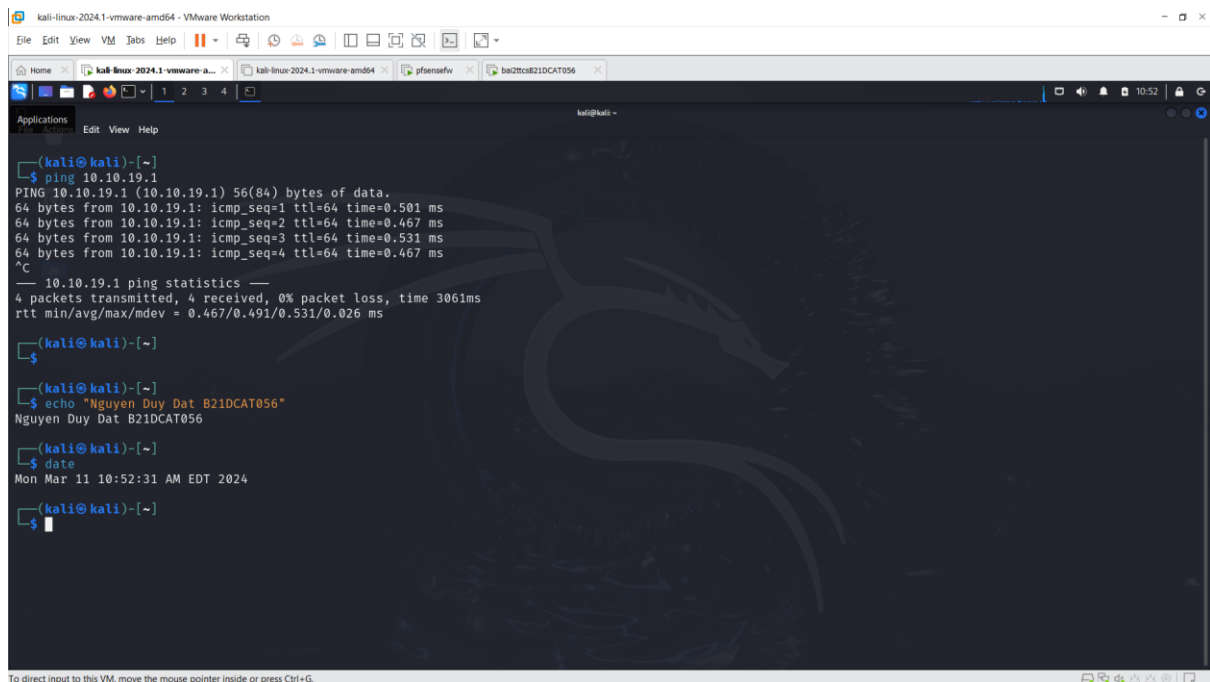
- Cài Pfsense



- Trên máy Linux victim ở mạng trong, vào <http://192.168.100.1> để cấu hình pfsense qua giao diện web.



- Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Kali attack ở mạng ngoài.



```
(kali@kali)-[~]
$ 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=0.501 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.467 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=0.531 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=0.467 ms
^C
-- 10.10.19.1 ping statistics --
4 packets transmitted, 4 received, 0% packet loss, time 3061ms
rtt min/avg/max/mdev = 0.467/0.491/0.531/0.026 ms

(kali@kali)-[~]
$
(kali@kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@kali)-[~]
$ date
Mon Mar 11 10:52:31 AM EDT 2024

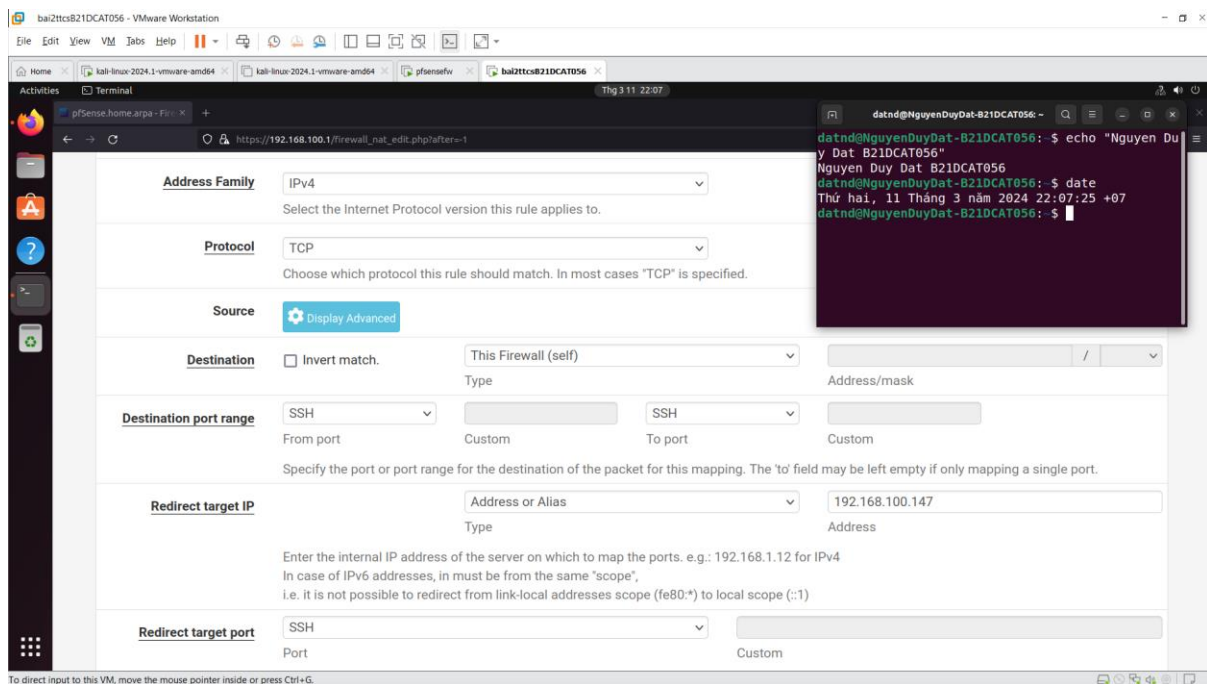
(kali@kali)-[~]
$
```

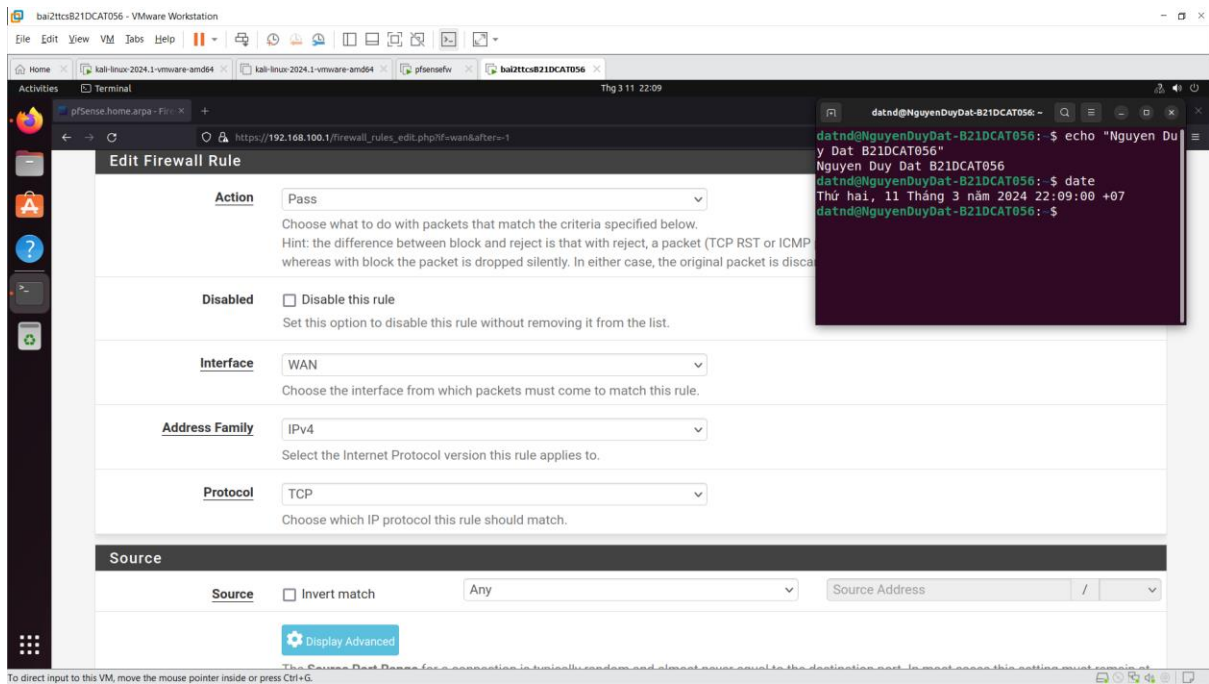
Trả lời câu hỏi: Mặc định, pfSense không mở cổng nào ở giao diện WAN. Có thể kiểm tra bằng cách nmap từ Kali External.

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.

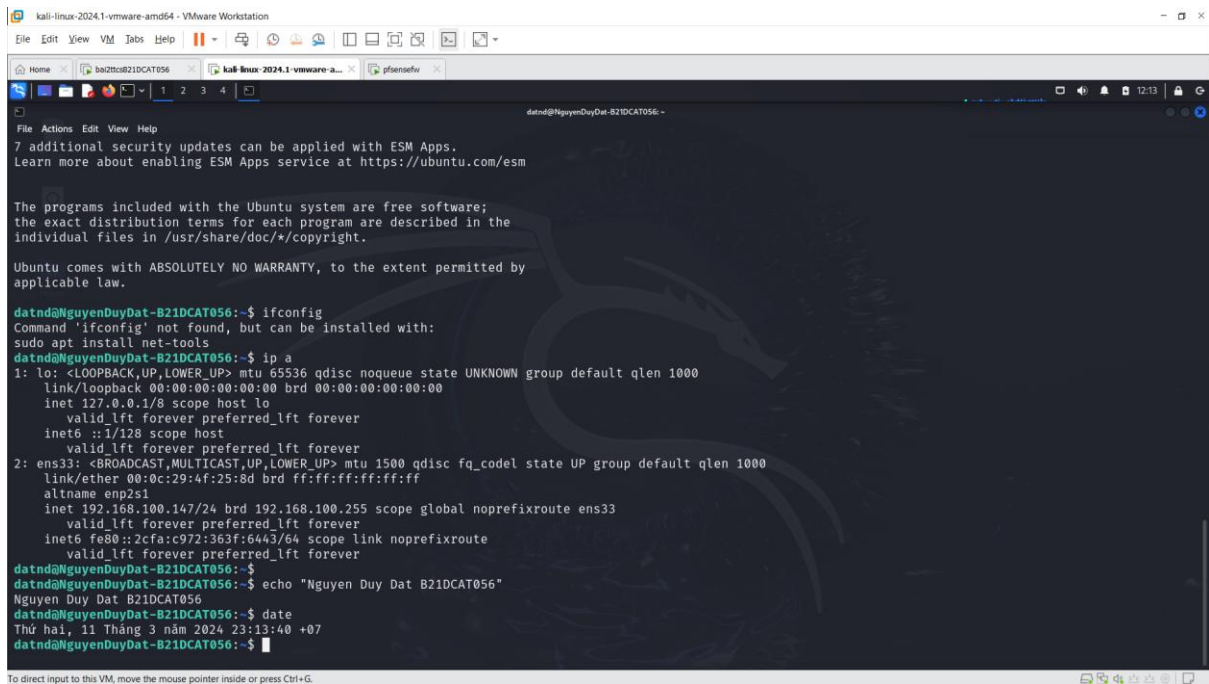
3. Cài đặt pfSense firewall cho phép chuyển hướng lưu lượng

- Cấu hình cho phép cổng SSH trên IP 192.168.100.147 (Máy Linux victim mạng Internal) được truy cập từ bên ngoài thông qua port forwarding. Nghĩa là khi các máy khách từ mạng 10.10.19.0/24 kết nối với địa chỉ IP của tường lửa pfSense của 10.10.19.1, chúng sẽ được chuyển hướng đến máy Linux victim trong mạng Internal

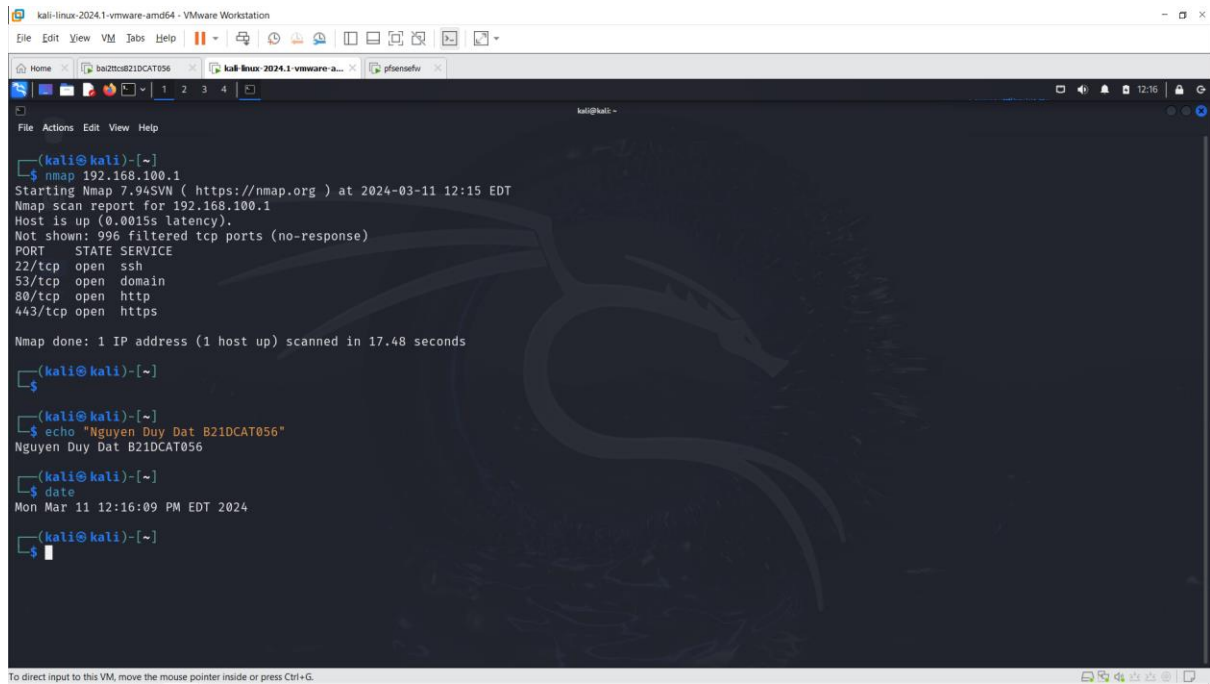




- Kiểm tra bằng cách truy cập ssh tới 10.10.19.1, rồi gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147 hay không?



- Kiểm tra các cổng được phép truy cập trên mạng Internal bằng cách gõ lệnh trên máy Kali Linux trong mạng Internal: `nmap 192.168.100.1`



The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the output of the `nmap 192.168.100.1` command, showing open ports 22/tcp (ssh), 53/tcp (domain), 80/tcp (http), and 443/tcp (https). It also shows the output of `echo "Nguyen Duy Dat B21DCAT056"` and `date`.

```
(kali@kali)-[~]
$ nmap 192.168.100.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 12:15 EDT
Nmap Scan report for 192.168.100.1
Host is up (0.0015s 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 17.48 seconds

(kali@kali)-[~]
$
(kali@kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
(kali@kali)-[~]
$ date
Mon Mar 11 12:16:09 PM EDT 2024
(kali@kali)-[~]
$
```