

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**  
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**

-----



**MÔN HỌC: THỰC TẬP CƠ SỞ**  
**BÁO CÁO BÀI THỰC HÀNH SỐ 5**

**Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu**  
**Sinh viên thực hiện : Nguyễn Nhật Minh**  
**Mã sinh viên : B21DCAT132**

**Hà Nội, tháng 2 năm 2024**

# **Môn học Thực tập cơ sở**

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

### **1. Mục đích**

Các công ty thường bảo vệ hệ thống mạng bằng cách sử dụng tường lửa phần cứng hoặc phần mềm để kiểm soát lưu lượng mạng truy cập. Một số loại lưu lượng nhất định có thể bị chặn hoặc cho phép đi qua tường lửa. Việc hiểu cách thức hoạt động của tường lửa và mối quan hệ của nó với các mạng bên trong và bên ngoài sẽ rất quan trọng để có hiểu biết về bảo mật mạng.

Bài thực hành này giúp sinh viên có thể tự cài đặt, xây dựng một mạng doanh nghiệp với tường lửa để kiểm soát truy cập. Mạng mô phỏng môi trường mạng doanh nghiệp này có thể sử dụng trong các bài lab về ATTT sau này.

### **2. Nội dung**

#### **1. Tìm hiểu về cấu hình mạng trong Vmware**

Trong VMware, cấu hình mạng trong phần mềm mô phỏng VMware thường được thực hiện thông qua VMware Workstation hoặc VMware vSphere (đối với môi trường ảo hóa doanh nghiệp). Dưới đây là một số khái niệm và khả năng cấu hình mạng trong các sản phẩm VMware phổ biến:

##### **a) VMware Workstation:**

- VMware Workstation cung cấp một công cụ có tên là Virtual Network Editor cho phép người dùng tùy chỉnh cấu hình mạng ảo cho các máy ảo. Bạn có thể thiết lập các mạng ảo riêng biệt và xác định cách chúng kết nối với mạng vật lý
- Trong cài đặt của mỗi máy ảo, bạn có thể cấu hình các thiết lập mạng cho từng adapter, bao gồm cấu hình IP, DHCP, DNS, và các thiết lập mạng khác.

##### **b) VMware vSphere**

- Trong môi trường vSphere, mạng ảo được quản lý thông qua các vSwitches. VSwitches là các thành phần quan trọng trong việc kết nối máy ảo với mạng vật lý và giúp kiểm soát lưu lượng mạng.
- Port Groups được sử dụng để định cấu hình và quản lý các kết nối mạng cho máy ảo. Chúng cho phép bạn xác định VLANs, cung cấp chế độ truy cập mạng khác nhau cho các máy ảo, và thiết lập các chính sách bảo mật.

Trong cả hai trường hợp, bạn có thể cấu hình các tính năng mạng như VLANs, trunking, bonding (hoặc teaming), Quality of Service (QoS), và các tính năng bảo mật khác. Điều này cho phép bạn tạo ra môi trường mạng ảo tương tự như một mạng vật lý, với khả năng tùy chỉnh và kiểm soát cao.

## 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

### **Một số tính năng của pfsense:**

#### 2.1 Aliases

Trong pfsense, firewall không thể có 1 rule gồm nhiều nhóm IP hoặc 1 nhóm port. Vì vậy, điều ta cần làm là gom nhóm các IP, Port hoặc URL vào thành 1 alias . Một alias sẽ cho phép thay thế 1 host, 1 dải mạng, nhiều IP riêng biệt hay 1 nhóm port, URL ... Alias giúp ta tiết kiệm được phần lớn thời gian nếu bạn sử dụng một cách chính xác như thay vì sử dụng hàng loạt rule để thiết lập cho nhiều địa chỉ, ta có thể sử dụng 1 rule duy nhất để gom nhóm lại.

#### 2.2 NAT

Pfsense có hỗ trợ nat static dưới dạng nat 1:1. Điều kiện để thực hiện được nat 1:1 là ta phải có IP public. Khi thực hiện nat 1:1 thì IP private được nat sẽ luôn ra ngoài bằng IP public tương ứng và các port cũng tương ứng trên IP public.

Pfsense hỗ trợ nat outbound mặc định với Automatic outbound NAT rule generation. Để cấu hình thủ công, ta chọn Manual Outbound NAT rule generation (AON - Advanced Outbound NAT) và xóa các rule mặc định của pfsense đi đồng thời cấu hình thêm các rule outbound.

#### 2.3 Firewall Rules

Là nơi lưu trữ tất cả các luật ra, vào trên pfsense. Mặc định PfSense cho phép mọi kết nối ra, vào (tại cổng LAN có sẵn rule any à any). Ta phải tạo các rule để quản lý mạng bên trong.

#### 2.4 Traffic shaper

Đây là tính năng giúp quản trị mạng có thể tinh chỉnh, tối ưu hóa đường truyền trong pfsense. Trong pfsense, 1 đường truyền băng thông sẽ chia ra các hàng khác nhau.

Pfsense cũng hỗ trợ giới hạn tốc độ download/upload của 1 IP hoặc 1 dải IP với ta thiết lập thông số tại phần limiter. Firewall pfsense hỗ trợ chặn những ứng dụng chạy trên layer 7 – application trong mô hình OSI như sip, ftp, http ... trong phần Layer

#### 2.5 VPN

Một tính năng khác không thể thiếu đối với các gateway là VPN. Pfsense cũng hỗ trợ VPN qua 4 giao thức: IPSec, L2TP, PPTP và OpenVPN.

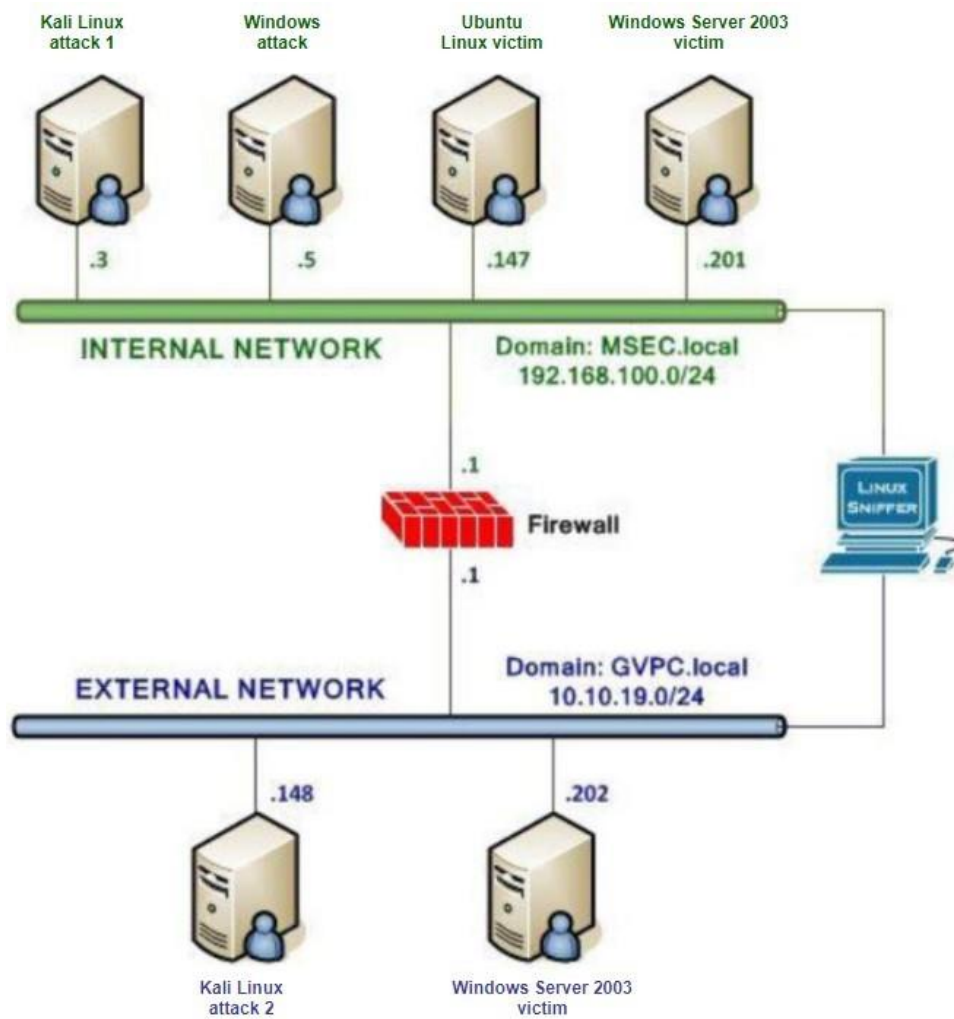
## 2.6 Monitor bằng thông

Pfsense có rất nhiều plugin hỗ trợ monitor bằng thông. Sau đây là 1 số plugin thông dụng: RRD Graphs, Lightsquid, BandwidthD, Ntop

Hoàn toàn miễn phí, giá cả là ưu thế vượt trội của tường lửa pfsense. Tuy nhiên, rẻ không có nghĩa là kém chất lượng, tường lửa pfsense hoạt động rất ổn định với hiệu năng cao, tối ưu hóa mã nguồn và hệ điều hành. Vì vậy pfsense không cần phần cứng phải mạnh. Pfsense hoạt động như một thiết bị mạng tổng hợp với đầy đủ tính năng và sẵn sàng bất cứ lúc nào. Pfsense hỗ trợ rất nhiều plugin để thiết lập thêm các tính năng hữu ích mà người dùng thấy cần thiết. Như vậy, tường lửa pfSense là sự kết hợp hoàn hảo và mạnh mẽ, đem lại sự hợp lý cho các nhà tài chính, và sự tin tưởng cho các nhà quản trị.

## 3. Chuẩn bị

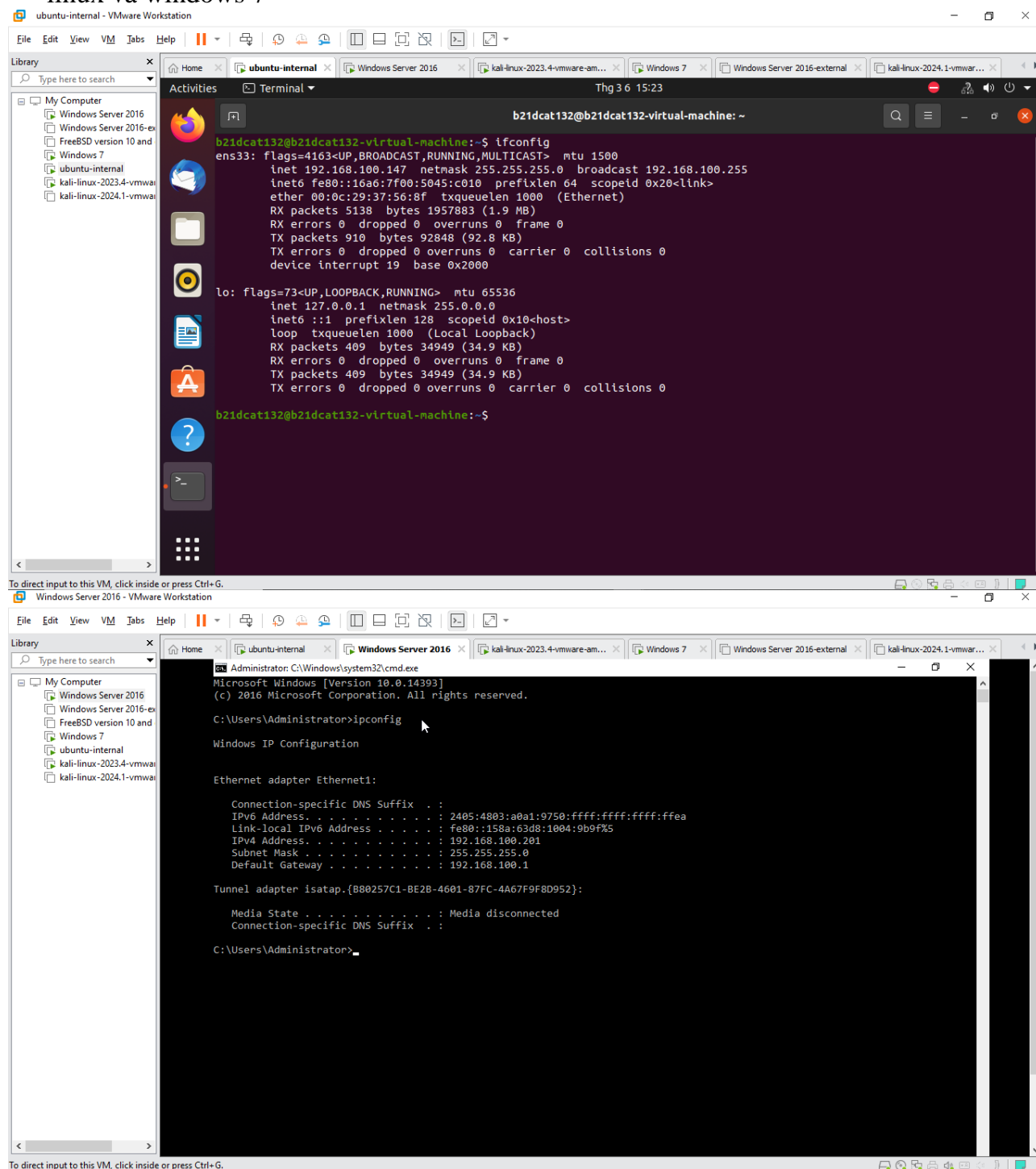
- Phần mềm Vmware
- Các file máy ảo bao gồm kali, linux, windows server và máy trạm
- File cài đặt tường lửa pfsense
- Ta cần cấu hình theo topo mạng sau:

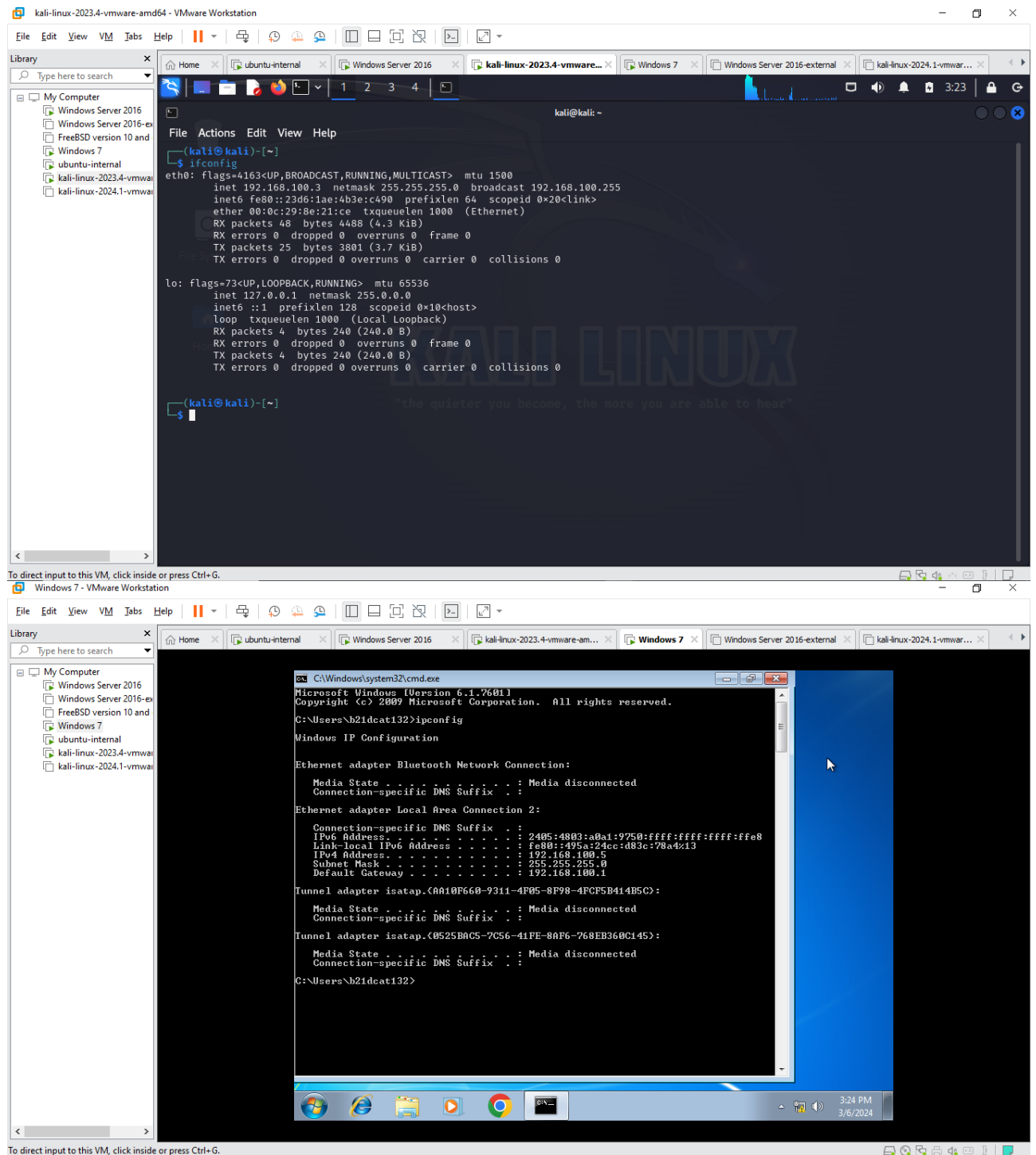


## 4. Thực hành

### 4.1. Cài các máy ảo theo topo và ping thành công

- Đầu tiên ta sẽ cài 4 máy ảo phía internal: lần lượt là ubuntu, windows server 2016, kali linux và windows 7





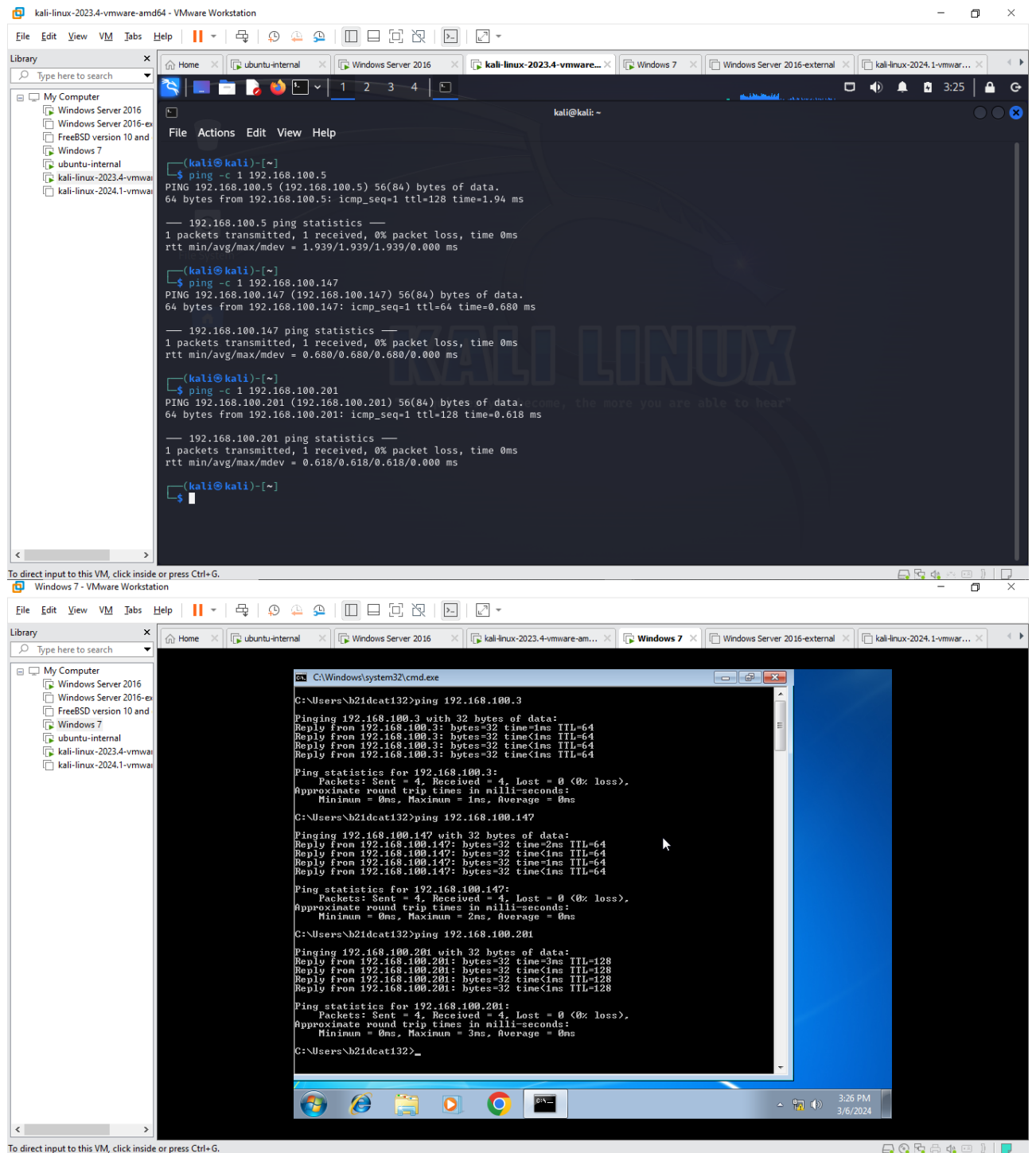
## - Tiến hành ping để kiểm tra kết nối giữa các máy trong internal

The screenshot displays two virtual machines in a VMware Workstation environment. The top window shows the 'ubuntu-internal' VM with a terminal window open, displaying the results of ping tests to three internal IP addresses. The bottom window shows the 'Windows Server 2016' VM with a command prompt open, also displaying successful ping results to the same three IP addresses.

```
b21dcat132@b21dcat132-virtual-machine: ~  
b21dcat132@b21dcat132-virtual-machine:~$ ping -c 1 192.168.100.3  
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=0.919 ms  
  
--- 192.168.100.3 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.919/0.919/0.919/0.000 ms  
b21dcat132@b21dcat132-virtual-machine:~$ ping -c 1 192.168.100.5  
PING 192.168.100.5 (192.168.100.5) 56(84) bytes of data:  
64 bytes from 192.168.100.5: icmp_seq=1 ttl=128 time=0.815 ms  
  
--- 192.168.100.5 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.815/0.815/0.815/0.000 ms  
b21dcat132@b21dcat132-virtual-machine:~$ ping -c 1 192.168.100.201  
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=3.74 ms  
  
--- 192.168.100.201 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 3.742/3.742/3.742/0.000 ms  
b21dcat132@b21dcat132-virtual-machine:~$
```

```
Administrator: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
  
C:\Users\Administrator>ping 192.168.100.3  
  
Pinging 192.168.100.3 with 32 bytes of data:  
Reply from 192.168.100.3: bytes=32 time<1ms TTL=64  
Reply from 192.168.100.3: bytes=32 time<1ms TTL=64  
Reply from 192.168.100.3: bytes=32 time<1ms TTL=64  
Reply from 192.168.100.3: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.100.3:  
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>ping 192.168.100.5  
  
Pinging 192.168.100.5 with 32 bytes of data:  
Reply from 192.168.100.5: bytes=32 time<1ms TTL=128  
Reply from 192.168.100.5: bytes=32 time<1ms TTL=128  
Reply from 192.168.100.5: bytes=32 time<1ms TTL=128  
Reply from 192.168.100.5: bytes=32 time<1ms TTL=128  
  
Ping statistics for 192.168.100.5:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\Users\Administrator>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<1ms TTL=64  
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64  
Reply from 192.168.100.147: bytes=32 time=3ms 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:
```





## - Tiếp theo cài kali và winserver 2016 phía external và tiến hành ping để kiểm tra kết nối

The image shows two virtual machines in a VMware Workstation environment. The top window is 'Windows Server 2016-external', and the bottom window is 'kali-linux-2024.1-vmware-amd64'.

**Windows Server 2016-external Command Prompt:**

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2405:4803:a0a1:9750:ffff:ffff:ffff:ffe3
    Link-local IPv6 Address . . . . . : fe80::789c:5fa3:1c0d:2bc6%5
    IPv4 Address. . . . . : 10.10.19.202
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.19.1

Tunnel adapter isatap.{8D011DE7-BEF8-4353-8A63-29F8246E988D}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

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 = 0ms, Average = 0ms

C:\Users\Administrator>
```

**kali-linux-2024.1-vmware-amd64 Terminal:**

```
kali@kali: ~
File Actions Edit View Help
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.148 netmask 255.255.255.0 broadcast 10.10.19.255
    inet6 fe80::40c5:c5c4:6dac:6015 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:2a:db:97 txqueuelen 1000 (Ethernet)
    RX packets 681 bytes 42956 (41.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 49 bytes 5000 (4.8 KiB)
    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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 30 bytes 2184 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 2184 (2.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

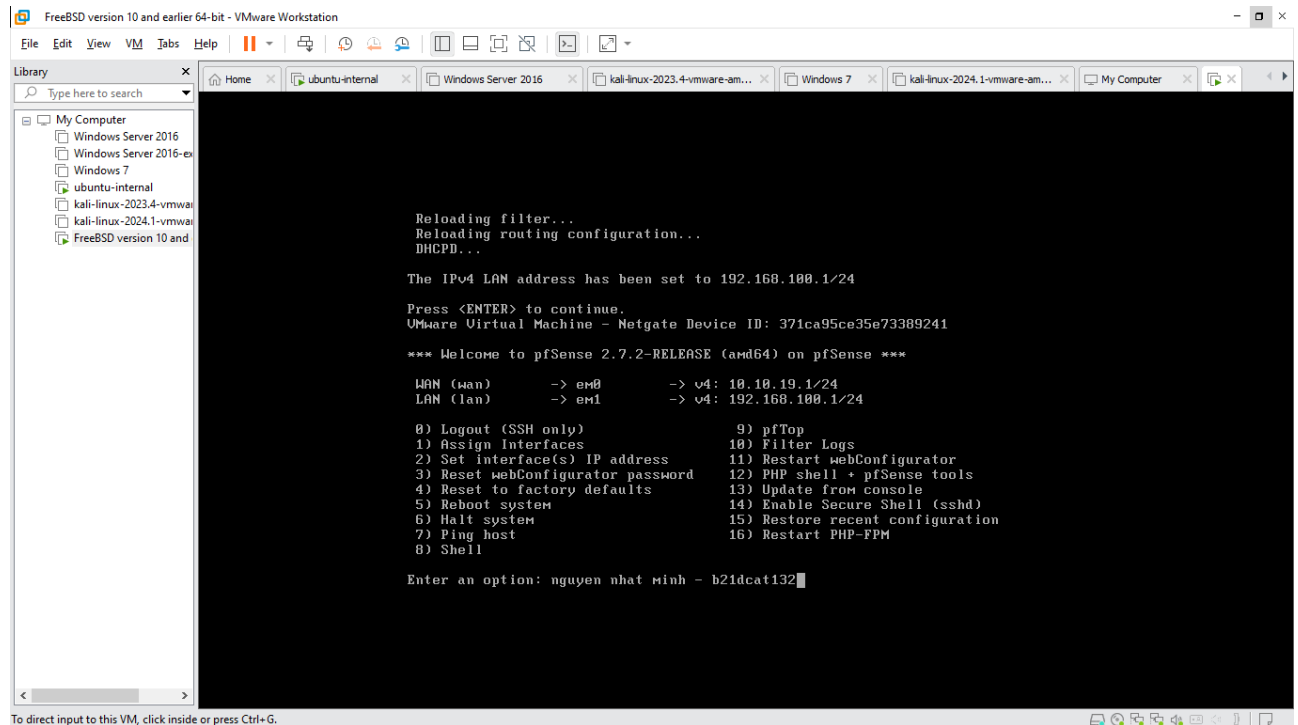
(kali@kali)~$ ping -c 4 10.10.19.202
PING 10.10.19.202 (10.10.19.202) 56(84) bytes of data.
64 bytes from 10.10.19.202: icmp_seq=1 ttl=128 time=1.10 ms
64 bytes from 10.10.19.202: icmp_seq=2 ttl=128 time=3.02 ms
64 bytes from 10.10.19.202: icmp_seq=3 ttl=128 time=3.36 ms
64 bytes from 10.10.19.202: icmp_seq=4 ttl=128 time=2.71 ms

--- 10.10.19.202 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.102/2.546/3.355/0.864 ms

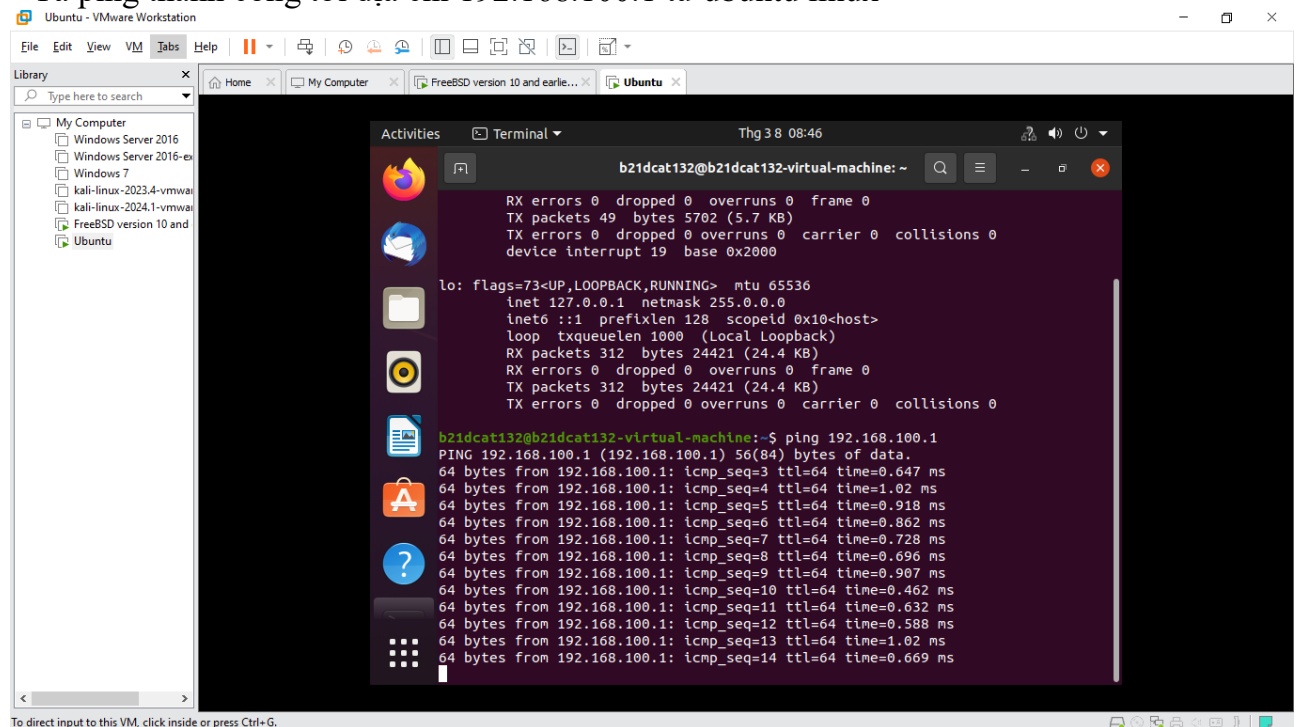
(kali@kali)~$
```

## 4.2. Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

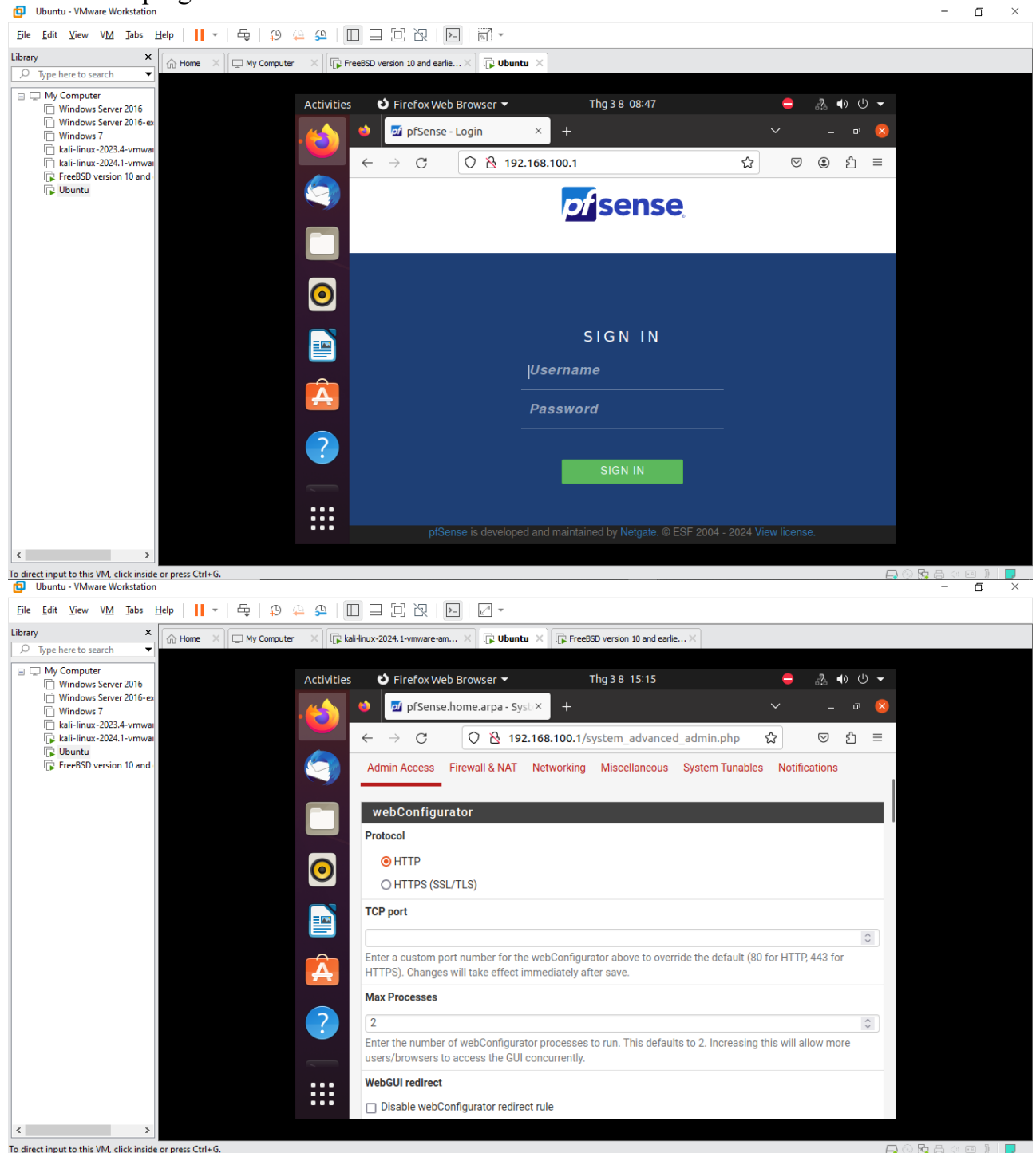
- Từ file iso của Pfsense cài đặt và cấu hình thành công

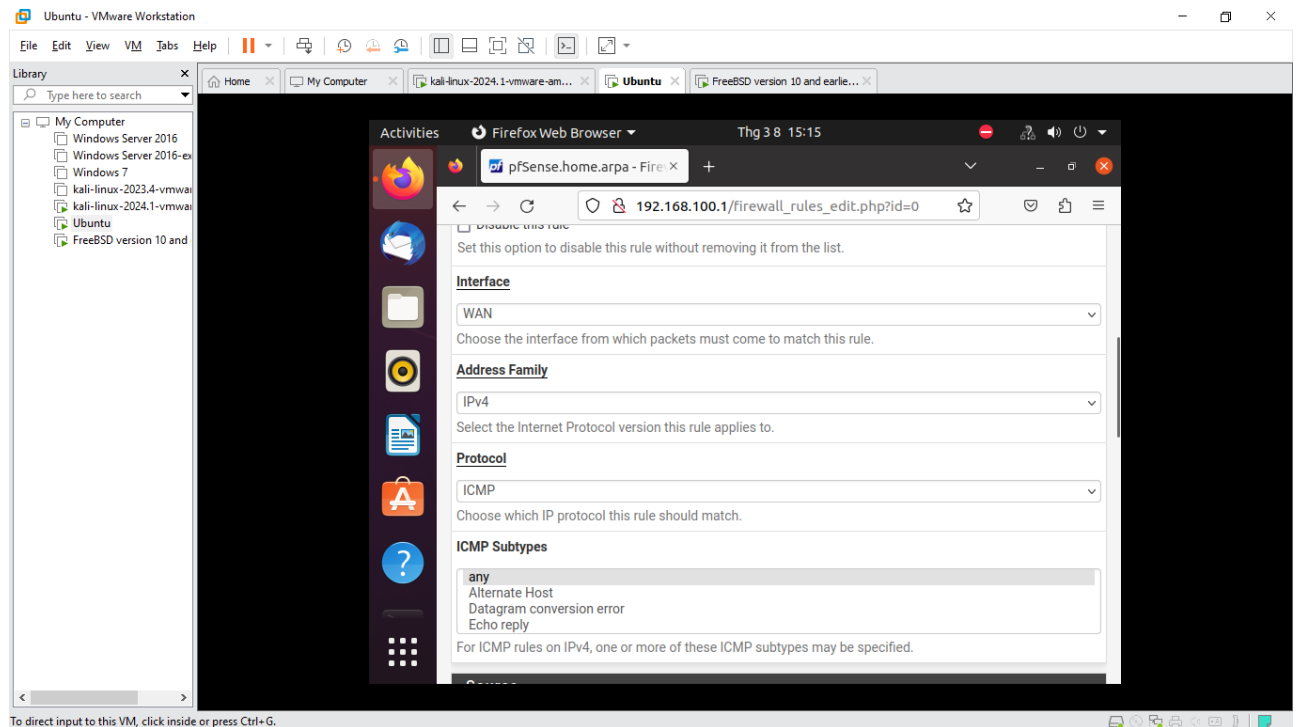


## - Ta ping thành công tới địa chỉ 192.168.100.1 từ ubuntu linux

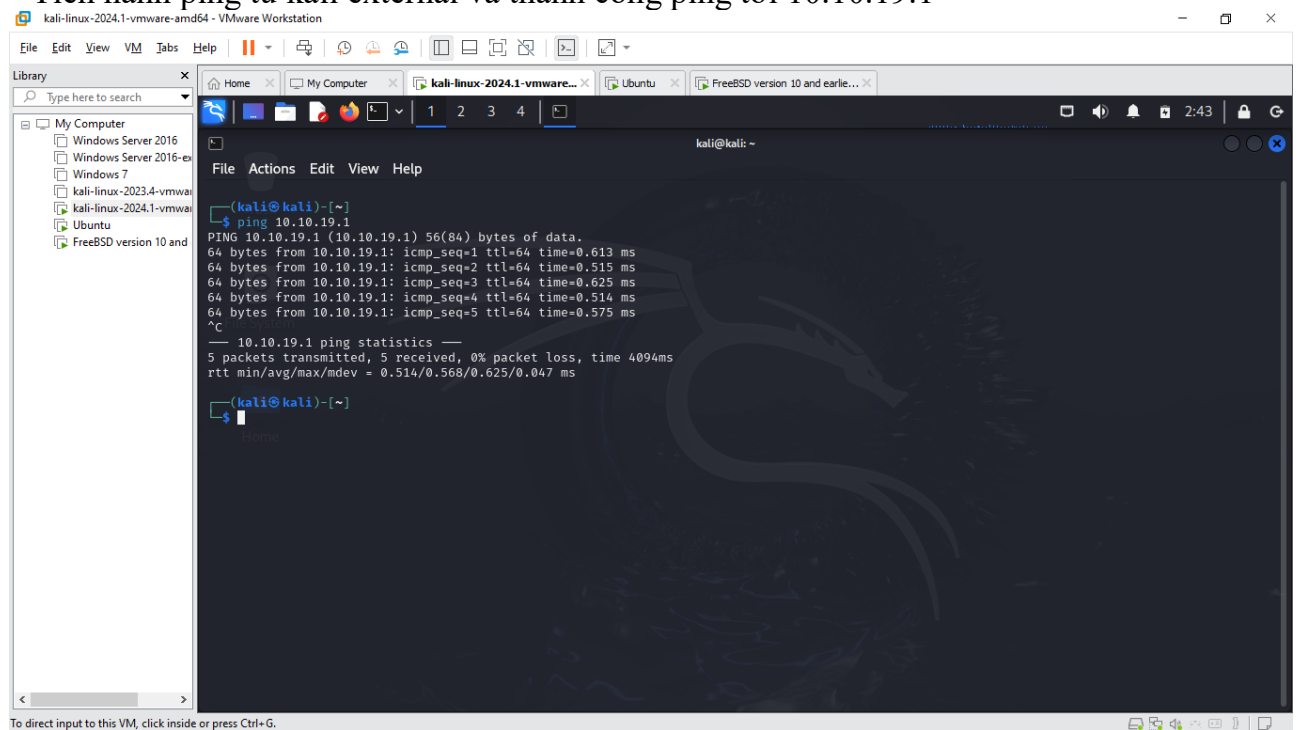


- Vào firefox truy cập tới địa chỉ 192.168.100.1 để cấu hình ICMP cho phép máy kali external ping tới 10.10.19.1





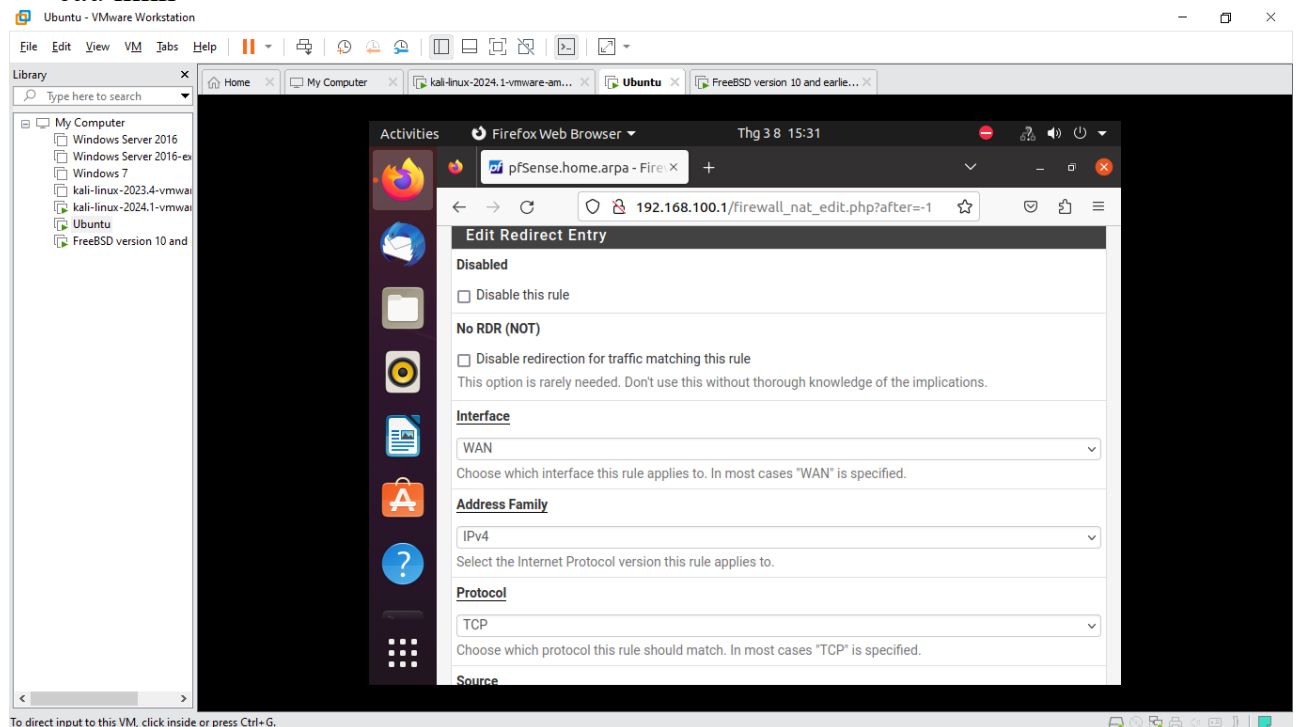
- Tiến hành ping từ kali external và thành công ping tới 10.10.19.1

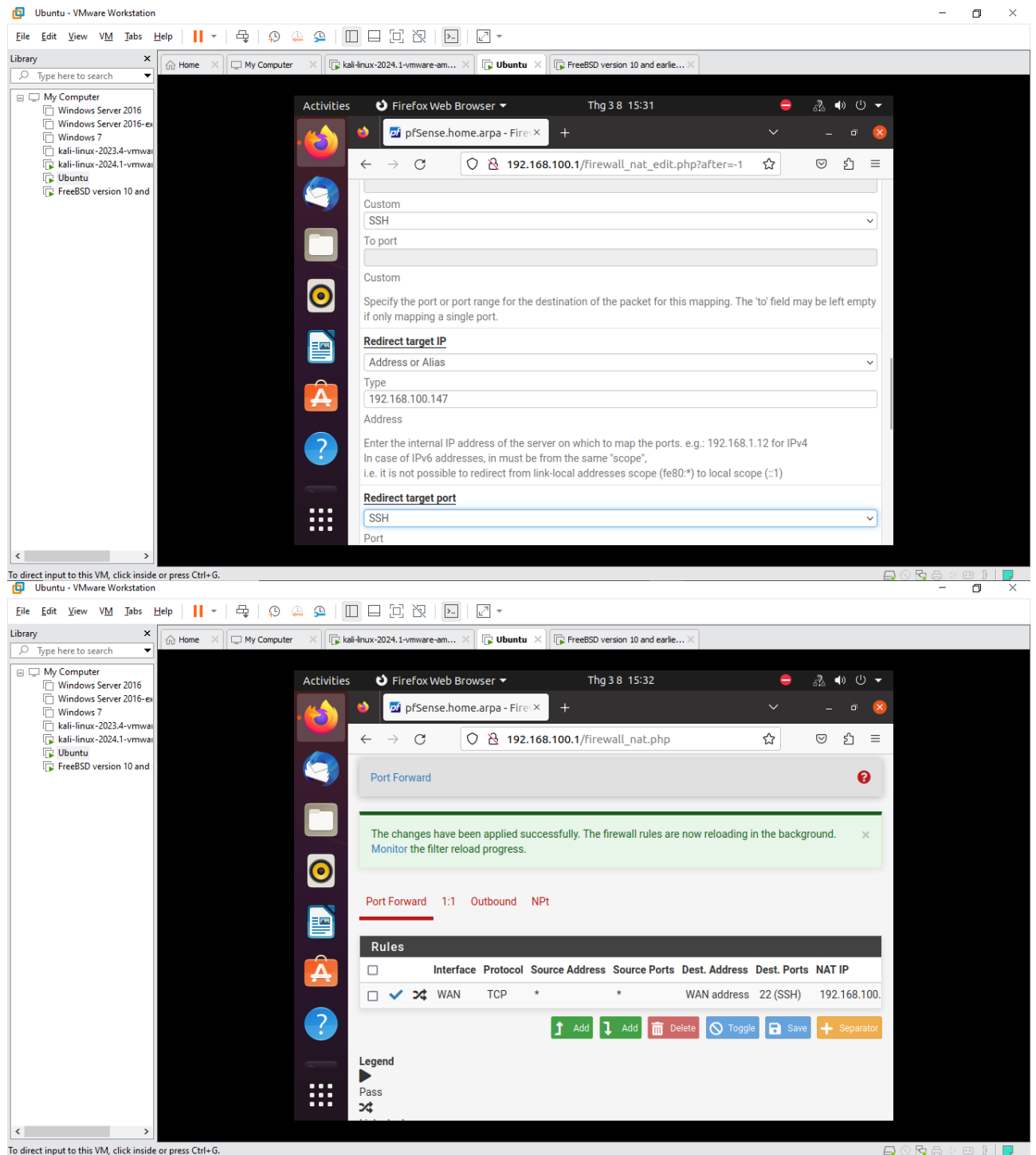


- Theo mặc định có bao nhiêu cổng mở trên giao diện mạng trong của pfsense:  
Mặc định, ở giao diện LAN, pfSense mở cổng 53 cho dịch vụ DNS Server và cổng 443 để cho phép máy trạm truy cập giao diện web qua https và có cổng 80 cho http
- Theo mặc định có bao nhiêu cổng TCP mở trên giao diện mạng ngoài của pfsense:  
Mặc định pfsense không mở cổng nào ở giao diện WAN

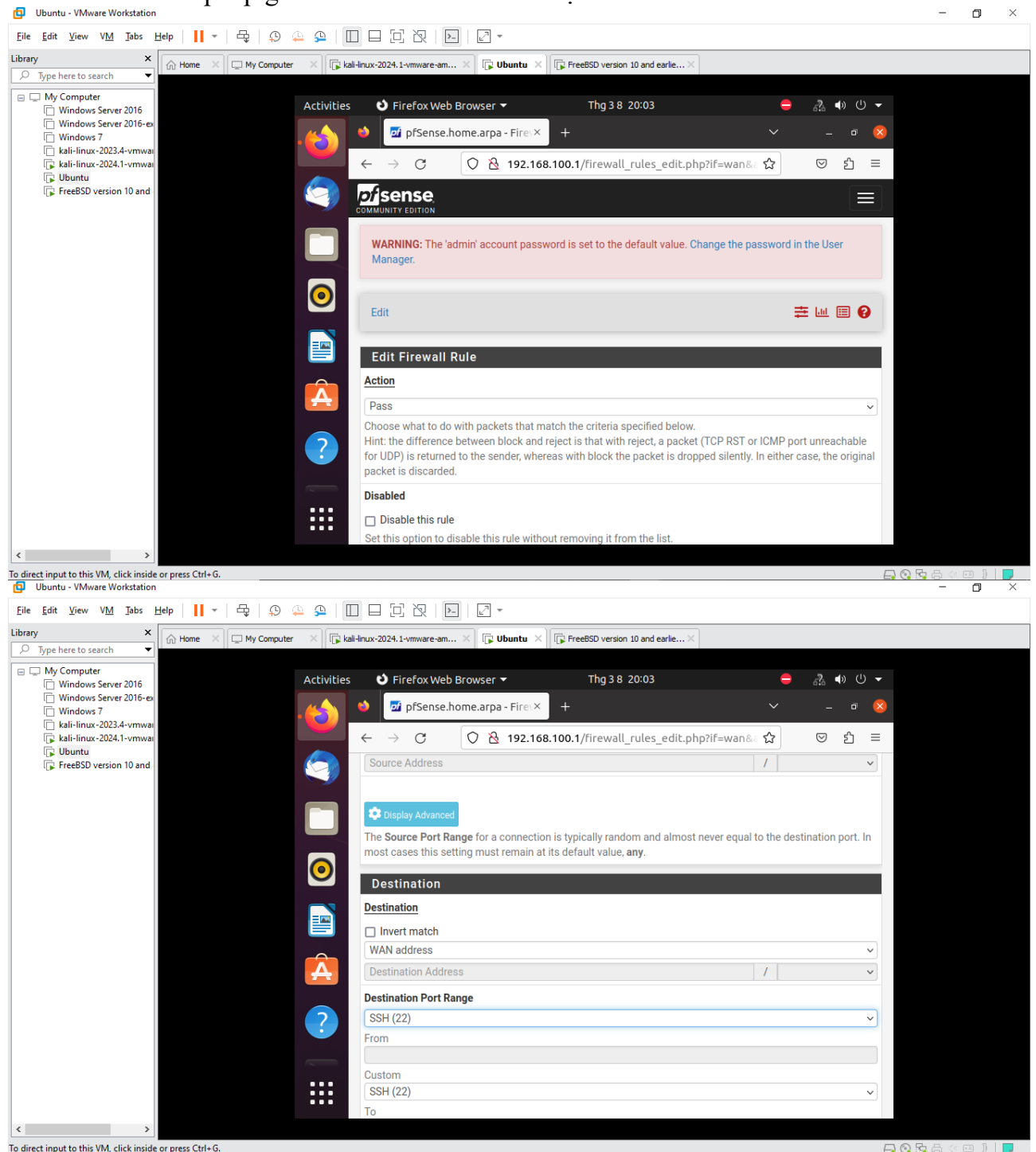
#### 4.3. Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

- Trên giao diện của pfsense vào firewall/NAT/Port Forward tiến hành add rules mới để cấu hình





## - Thêm rules cho phép giao thức TCP kết nối tới địa chỉ WAN





- Cấu hình thành công ta sẽ có 2 rules ở giao diện Firewall WAN

Rules (Drag to Change Order)										
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Descrip
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	WAN address	22 (SSH)	*	none	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.100.147	22 (SSH)	*	none	NAT

- Truy cập ssh tới ubuntu internal thành công và đã thành công

```

kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
  Windows Server 2016
  Windows Server 2016-es
  Windows 7
  kali-linux-2023.4-vmwa
  kali-linux-2024.1-vmwa
  Ubuntu
  FreeBSD version 10 and
b21dcat132@b21dcat132-virtual-machine:~
File Actions Edit View Help
(kali@kali)~$ ssh b21dcat132@10.10.19.1
b21dcat132@10.10.19.1's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-67-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

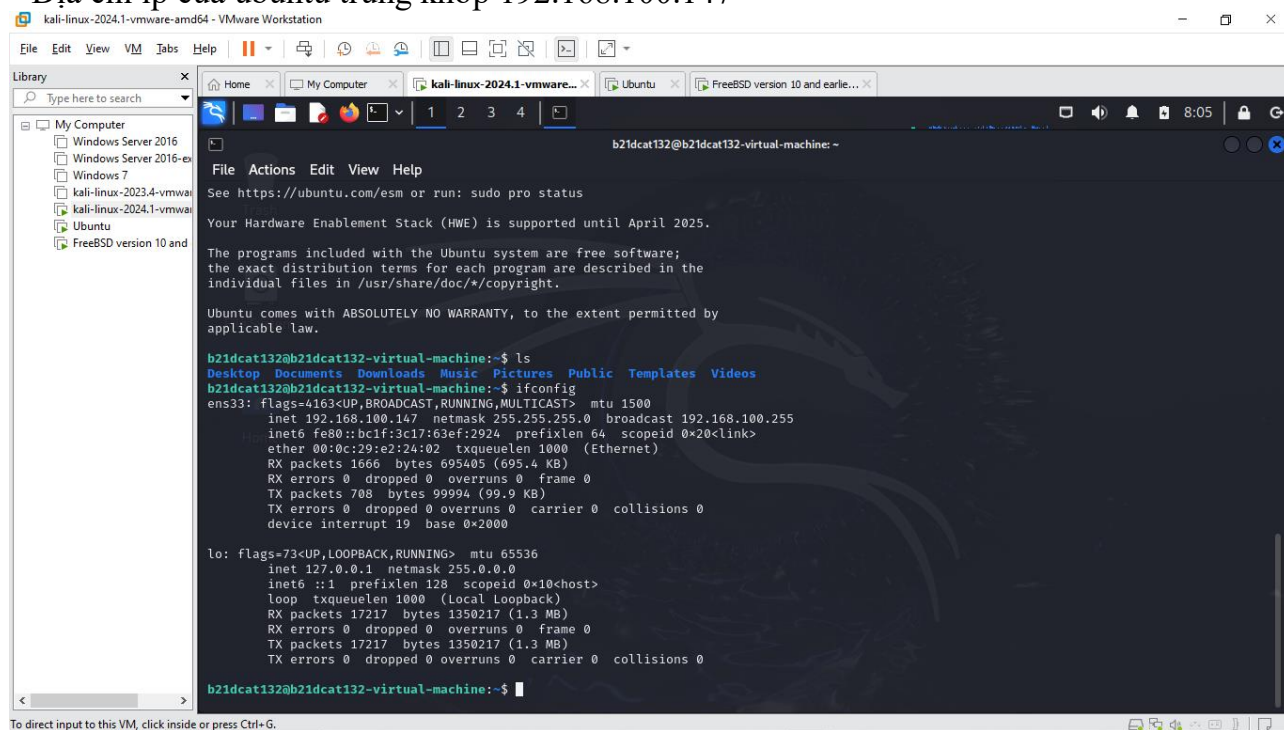
Your Hardware Enablement Stack (HWE) is supported until April 2025.

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.

b21dcat132@b21dcat132-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
To direct input to this VM, click inside or press Ctrl+G.
  
```

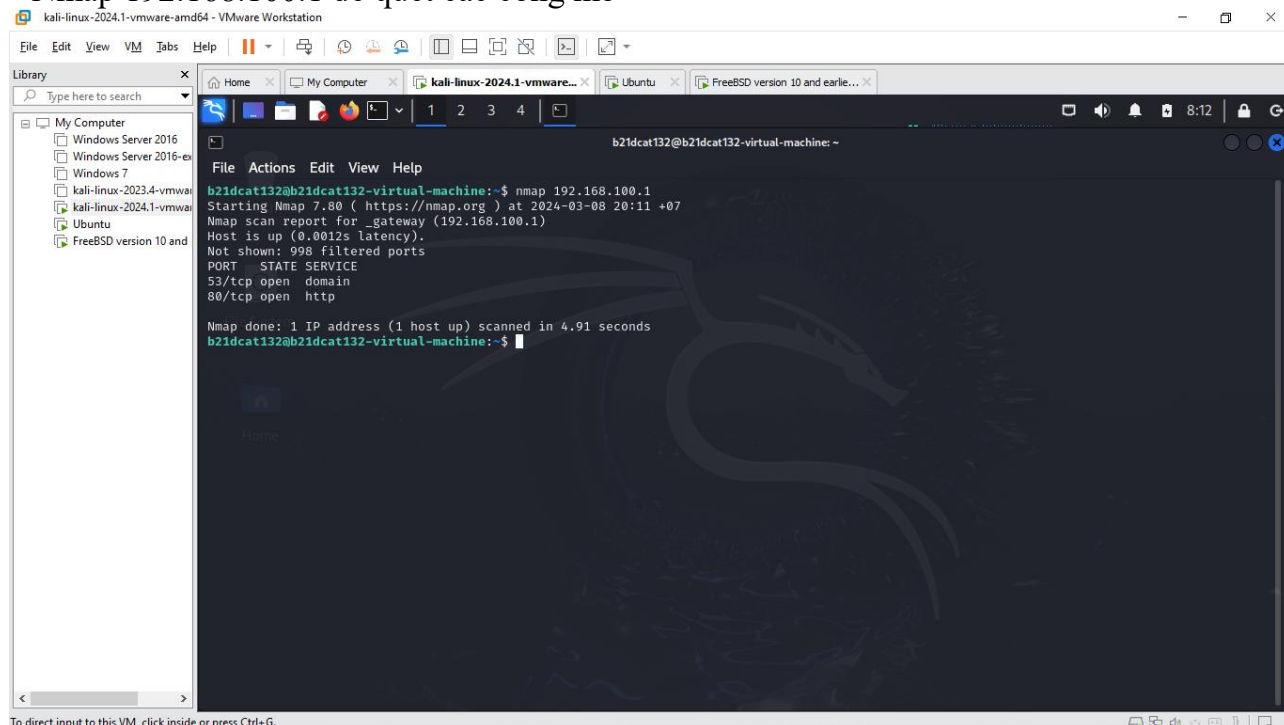
## - Địa chỉ ip của ubuntu trùng khớp 192.168.100.147



```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows Server 2016
Windows Server 2016-es
Windows 7
kali-linux-2023.4-vmwa
kali-linux-2024.1-vmwa
Ubuntu
FreeBSD version 10 and
b21dcat132@b21dcat132-virtual-machine: ~
File Actions Edit View Help
See https://ubuntu.com/esm or run: sudo pro status
Your Hardware Enablement Stack (HWE) is supported until April 2025.
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.
b21dcat132@b21dcat132-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
b21dcat132@b21dcat132-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.147 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::bc1f:3c17:63ef:2924 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:a2:24:02 txqueuelen 1000 (Ethernet)
    RX packets 1666 bytes 695405 (695.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 708 bytes 99994 (99.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 17217 bytes 1350217 (1.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17217 bytes 1350217 (1.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
b21dcat132@b21dcat132-virtual-machine:~$
```

To direct input to this VM, click inside or press Ctrl+G.

## - Nmap 192.168.100.1 để quét các cổng mở

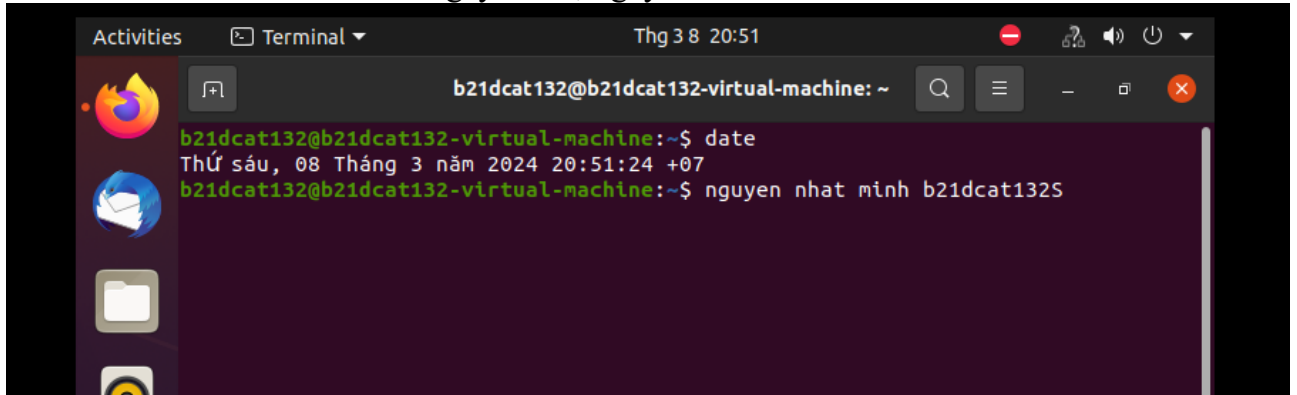


```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows Server 2016
Windows Server 2016-es
Windows 7
kali-linux-2023.4-vmwa
kali-linux-2024.1-vmwa
Ubuntu
FreeBSD version 10 and
b21dcat132@b21dcat132-virtual-machine: ~
File Actions Edit View Help
b21dcat132@b21dcat132-virtual-machine:~$ nmap 192.168.100.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-08 20:11 +07
Nmap scan report for _gateway (192.168.100.1)
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
b21dcat132@b21dcat132-virtual-machine:~$
```

To direct input to this VM, click inside or press Ctrl+G.

## 5. Kết quả

Bài thực hành hoàn thành vào ngày thứ 6, ngày 08/03/2024



The screenshot shows a terminal window titled "b21dcat132@b21dcat132-virtual-machine: ~". The terminal output is as follows:

```
b21dcat132@b21dcat132-virtual-machine:~$ date
Thứ sáu, 08 Tháng 3 năm 2024 20:51:24 +07
b21dcat132@b21dcat132-virtual-machine:~$ nguyen nhat minh b21dcat132S
```